Sterling Integrator

UNIX/Linux Cluster Environment Installation Guide

Version 5.1

Sterling Integrator

UNIX/Linux Cluster Environment Installation Guide

Version 5.1

Note
Before using this information and the product it supports, read the information in "Notices" on page 89.

Copyright

This edition applies to Version 5 Release 1 of Sterling Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2000, 2013.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2000, 2013

Chapter 1. UNIX/Linux Cluster Environment Installation Overview

Sterling Integrator Installation Overview

Use the guide to install Sterling Integrator 5.1 in a UNIX/Linux cluster environment.

This guide contains the following information:

- Before You Begin the Installation
- Configure the Database
- Install the Software
- Validate the Installation
- Post Installation Configuration
- Installation Maintenance
- Configure Non-English Environment
- User Documentation
- Install Perimeter Servers
- Uninstall the Software
- Sterling Integrator with Gentran:Server for UNIX
- Troubleshooting Tips

Prerequisite Knowledge for Installation

Before you being the installation, you should be knowledgeable on the following topics:

- Application servers
- Operating system on which you plan to install
- Database administration
- VI or another text editor
- System Requirements for this release

Intended Audience

This document is intended for use by:

- System Administrators
- Installation Engineers
- Database Administrators

Assumptions for this Guide

The procedures in this guide are accurate as of the publication date and are specific to Sterling Integrator 5.1.

© Copyright IBM Corp. 2000, 2013

Chapter 2. Before You Begin the Installation

Before You Begin the Installation

Before you begin the installation, you need to:

- Perform some system verification tasks
- Perform some operating system verification tasks
- Gather some information and complete the preinstallation checklist

System Verification Tasks

Before you begin an installation, you need to:

#	System Verification Tasks	Your Notes
1	Use the system requirements to verify that your system hardware and software meet the requirements specified for this release. Verify you have the correct: • Patches required by Java™ for the operation system • Version of the JDK • Absolute path to JDK and patches For HP, you must run the HP JConfig utility to obtain the required patches and kernel modifications.	
2	Verify the file system has adequate free disk space.	
3	Verify the following: • An operating system user account exists on the host server. • User account has permissions to execute the commands for the operating environment.	
4	Verify that your database has been installed and configured. If you are going to manually apply DDL statements, you need to complete the data base schema work before you begin the installation.	
5	If you are using a non-English environment, confirm that you are using the appropriate character set.	

© Copyright IBM Corp. 2000, 2013

Operating System Verification

Before you begin the installation, you need to verify your operating system configuration, by using the following checklist:

For the Operating System	Operating System Configuration Checklist	Your Notes
HP-UX Operating System	Establish these settings: • Verify kernel parameters and establish the following minimum settings by running kctune command: – kctune max_thread_proc 1024 – kctune maxdsiz 2147483648 – kctune maxdsiz_64bit 8589934592 – kctune maxssiz 369098752 – kctune maxssiz_64bit 536870912 • Run ulimit utility, verify, and establish the following minimum settings: – ulimit -d = 2097152 (in kilobytes) or higher – ulimit -s = 360448 (in kilobytes) or higher	

For the Operating System	Operating System Configuration Checklist	Your Notes

AIX Operating System	You must specify the name of the installation directory name. The installation process creates the directory and beneath it, a directory called “install”.
	
	To ensure that */install_dir*/install has the necessary permissions, AIX users must run the following command on the parent directory of */install_dir*/install before installation:
	`chmod -R a-s <absolute path>/install_dir_parent`
	
	Where *install_dir_parent* is the directory in which */install_dir*/install will be created.
	
	For example, to specify
	
	AIX_1/applications/test1/*my_install* as your installation directory, you could run the command from the AIX_1/applications directory (directly above the test1 directory):
	`chmod -R a-s test1`
	
	Or from another location on the file system:
	`chmod -R a-s /AIX_1/applications/test1`
	
	This ensures that when the *my_install* directory is created during installation, it inherits the correct permissions from test1.
	
	The ncargs value specifies the maximum allowable size of the ARG/ENV list (in 4K byte blocks) when running exec() subroutines. Set ncargs value to 16 or higher.
	
	To display the current value of ncargs, enter `lsattr -El sys0 -a ncargs`.
	
	To change the current value of ncargs, enter `chdev -l sys0 -a ncargs=NewValue`.
	
	Note: The lsattr and chdev command options are –El (lowercase L) and –l (lowercase L) respectively.
	
	Change the following default entries in the /etc/security/limits file:
	• fsize = -1
	• core = 2097151
	• cpu = -1
	• data = 262144
	• rss = 65536
	• stack = 65536
	• nofiles = 4096	

For the Operating System	Operating System Configuration Checklist	Your Notes
Linux Operating System	You need to disable SELinux by enter the following: `/etc/sysconfig/selinux: SELINUX=disabled` Ensure that /etc/hosts has short-names first for all entries. For example, 127.0.0.1localhostlocalhost.localdomain If the base locale is English, verify: • that the LANG variable is en_US • LANG variable is exported	
RedHat Enterprise Linux Operating System	Make the following system changes: • If the base locale for the system is English, edit the /etc/sysconfig/i18n file by changing the SUPPORTED variable from en_US.utf8 to en_US. You can also allow multiple support using the following format: en_US.utf8:en_US • Save and close the /etc/sysconfig/i18n file. Edit the /etc/security/limits.conf file by adding the following lines: – `* hard nofile 8196` – `* soft nofile 4096` – `* hard memlock 3000000` – `* soft memlock 3000000` – `* hard nproc 16000` – `* soft nproc 16000` – `* hard stack 512000` – `* soft stack 512000` This updates the system ulimits. For nofile, the recommended value is unlimited. • Save and close the /etc/security/limits.conf file. • Reboot the system.	
Solaris Operating System	Set the following entries in the /etc/security/limits file: `nofiles = 4096` (recommended value is unlimited) `set rlim_fd_max=4096 (limit is 65535)` - hard limit `set rlim_fd_cur=4096` - soft limit • To make the setting effective as the hard limit, reboot the server or run the following command: `kill -1 inetd` • To make the setting effective as the soft limit, use the parent shell configuration (for example, .profile). Then, reboot the server.	

Installation Checklist for UNIX/Linux Cluster Environment

The preinstallation checklist contains the items you need to gather and tasks you need to complete prior to installing the Sterling Integrator in a cluster environment. The checklist contains:

- Brief descriptions for tasks, while more detailed procedures are provided after the checklist
- Information you need to gather to complete the installation

You may want to make a copy of the following checklist and use it to record the information you collect.

The cluster environment does not support the following items:

- MySQL database
- AS2 Edition

#	Preinstallation Checklist	Node 1	Node 2	Node 3	Your Notes
1	Determine which installation method you are going to use: • GUI- based • Text-based • Silent Installation				
2	Decide which type of security certificates you will use: • The default self-signed SSL (Secure Sockets Layer) certificate that is automatically installed. • A Certificate Authority-related certificate that you install before installing Sterling Integrator.				
3	If you are using an Oracle, Microsoft SQL Server, or DB2 database, decide if you are going to manually or automatically apply Database Definition Language (DDL) Statements (schema) to the database.				
4	Determine if the database password need to be encrypted.				
5	Record the Hostname on which you plan to install Sterling Integrator.				
6	Record the Directory Name where you plan to install Sterling Integrator.				
7	Record the Login to host machine.				
8	Record the Password to the host machine.				

#	Preinstallation Checklist	Node 1	Node 2	Node 3	Your Notes
9	Record the path to the JDBC drivers.				
10	Record the path to the installation wizard and file name.				
11	Record the path to JDK.				
12	Record the path to the License File.				
13	Record the path to JCE file.				
14	Record the Host IP address.				
15	Record the Initial Port Number.				
16	Record the System passphase.				
17	Record the Database vendor name.				
18	Record the Database user name.				
19	Record the Database password.				
20	Record the Database (catalog) name.				
21	Record the Database host name.				
22	For Oracle and Microsoft SQL Server, record the Path and file name for the JDBC Driver.				
23	For DB2 , record the absolute paths and file names for two JDBC drivers.				

Verify Your System Meets the System Requirements

Before you begin the installation, verify that your system meets the hardware and software requirements specified for this release. The hardware requirements listed are the minimum required. Your system requirements will exceed these if you are running other applications on the same machine as the Sterling Integrator.

The installation strictly enforces the following *System Requirements*:

- Operating system version must match requirement exactly.
- The minimum patch level for the operating system is enforced, but you can apply higher patch levels.
- JDK version must match requirement exactly.

- The disk space is a minimum for the installation. The system should be separately sized to handle whatever load is going to be put on the system.
- Database version must match exactly.
- JDBC driver version supports exact matches and wildcard matches.

If any of the these requirements are not met, the installation will fail. If the installation fails, review the installation log for a list of non-compliant items.

Multicast Ports: Node to Node Communications

Cluster nodes are configured to communicate with each other using JGroups, an open source toolkit that provides flexibility for protocol configuration. JGroups provides rich open management features, along with multiple protocol support. JGroups supports multicast (UDP) and TCP-based communication protocols.

When JGroups is configured to use multicast (UDP), all cluster nodes communicate with each other on a specific IP address and port. The multicast ports are configured based on the installation base port. All clusters that are on the same subnet configured on the same base port will send multicasting messages on the same multicast IP address and port.

To avoid this, each Sterling Integrator cluster on the same subnet needs to be configured on different base ports. Install your clusters on different port ranges or on different network segments with multicast forwarding restricted, so that they will not interfere with each other. The default multicast address used is 239.255.166.17. This address is configurable, with a port range of 10 ports, starting with the multicast base port for the instance.

All nodes participating in the same cluster must be installed on the same multicast base port (the multicastBasePort property in the noapp.properties file). This is usually computed from the system base (non-multicast) port, but can be configured separately in the noapp.properties file, to allow different nodes in a cluster to be installed at different (non-multicast) port ranges. Also, all the nodes in the cluster should be installed in the same subnet.

For node to node communications, the properties are defined in jgroups_cluster.properties. The attributes used to define communications are:

- property_string - default value is UDP.
- distribution_property_string - default value is TCP. This attribute should never be set to UDP.

If you want to change the communication for cluster multicast from the UDP protocol to TCP, you need to change the value of the property_string property in the jgroups_cluster.properties.in file (after backing up the file), and then run the `setupfiles.cmd` command. You can make this change right after the installation or after you have started running the cluster. If you change the file after starting the cluster, you need to stop all nodes of the cluster, make the change on each node, and then re-start your cluster.

To change the communication for cluster multicast from the UDP protocol to TCP, use the following value for the property_string property in the jgroups_cluster.properties.in file:

```
property_string=TCP(start_port=any_available_port_number):
TCPPING (initial_hosts=this_instance_host_ip[start_port_number],
theothernode_instance_host_ip[theothernode_start_port_number];port_range=2;
```

```
timeout=5000;num_initial_members=3;up_thread=true;down_thread=true):
VERIFY_SUSPECT(timeout=1500):
pbcast.NAKACK(down_thread=true;up_thread=true;gc_lag=100;retransmit_timeout=3000):
pbcast.GMS(join_timeout=5000;join_retry_timeout=2000;shun=false;print_local_addr=
true;down_thread=true;up_thread=true)
```

For more information about UDP, TCP, and JGroups communications, refer to the *Sterling Integrator Clustering* documentation.

Security Certificates

Before you begin the installation, you must decide which of the following security certificates you will use:

- The default self-signed SSL (Secure Sockets Layer) certificate that is automatically generated by the installation.
- A Certificate Authority-related certificate that you generate before installing the software.

If you install with the default SSL certificate, but you later want to switch to a CA-related certificate, you can make that change using the sslCert property in the noapp.properties.in file.

Port Numbers

During installation, you are prompted to specify the initial port number. Port number guidelines are:

- A range of 200 consecutive open ports between 1025 and 65535 are required for this installation.
- The initial port number represents the beginning port number in the range.
- Make sure that port numbers in the port range are not used by any other applications on your system.

After your installation, refer to the */install_dir*/install/properties/sandbox.cfg file for all of the port assignments.

UNIX Accounts

In a UNIX or Linux environment, create one UNIX administrative account on the host server for all of the installations. For example, if you want to create a test environment and a production environment, create one UNIX account on the host server. For more information about creating UNIX accounts, see your operating system documentation.

License File

After your company signed the sales contract with Sterling Commerce, Sterling Commerce creates a license file containing information about your company, your system, and the packages (components) that your company selected to use, such as services, maps, and adapters.

Your first license file is a temporary keyfile that is e-mailed to you after you purchase Sterling Integrator. It allows you to run the software and all of the licensed features for a limited period. Before the keyfile expires, you must replace

the temporary key with a permanent key Failure to either extend your temporary keyfile or replace it with a permanent keyfile will result in the keyfile expiry and Sterling Integrator will fail to start.

The permanent license keyfile contains your specific operating system and the IP address of your system, and is valid for 20 years from the date of issue.

The permanent license file contains a single or multiple IP addresses in your computing environment. If you change an IP address in your computing environment that is present in your license file, the software will cease to operate. You should take necessary precautions to avoid this potential outage, including notifying the appropriate contacts within your organization (Information technology and related departments) and include the license file updates in your computing environment change plans.

Obtain a License File

About this task

To obtain a license file:

Procedure

1. Navigate to the Sterling Commerce Customer Center (https://customer.sterlingcommerce.com).
2. Click **Support Center > Sterling Integrator > Key Requests**.
3. Enter the following information:
   - Company Name
   - Contact Name
   - Phone Number
   - Fax number
   - Email Address
   - Requested Key Type (Permanent or Temporary)
   - PSP number - The PSP Number (unique number that identifies a licensed software asset in your Sterling Integrator installation) is present in the temporary or previous version of the keyfile you received from Sterling Commerce.
   - CD Key (if no PSP number is present in your license key)
   - Order Number
   - Product
   - Platform
   - Environment
   - IP Addresses
   - Previous IP Address
   - Sterling Account Executive
   - Comments
4. Click **Submit**.

   Your new keyfile will be generated and delivered to you as an attachment to an email. Save this attachment and record the absolute path. This will be used during the install process.

Install the License Key

About this task

To install the license key from the command line:

Procedure

1. When you receive the permanent license keyfile, make a copy of it, and keep the copy in a safe place.
2. Stop Sterling Integrator.
3. Copy your license keyfile to the machine where Sterling Integrator is installed.
4. Navigate to */install_dir*/bin.
5. Enter `./AddLicenseSet.sh` <*path*>. Where <*path*> is the path to the license keyfile.
6. Start Sterling Integrator.

   You can also install or update your license file from the Licenses screen (**Operations > System > Licenses**).

Download the JCE Distribution File for the IBM JDK 1.6

About this task

The Java Cryptography Extension (JCE) is a set of Java packages from IBM that provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms.

If you are installing the software outside of the United States, check to see if you can get the JCE unlimited strength jurisdiction policy files. The unlimited strength jurisdiction policy files can only be exported to countries to which the United States permits the export of higher-level encryption.

To obtain the zip file for the IBM JDK 1.6:

Procedure

1. Open your browser and navigate to https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk.
2. Enter your `IBM ID` and `password`. If you do not have an IBM ID, follow the IBM registration instructions.
3. Click **Sign in**.
4. Select the **Unrestricted JCE Policy files for SDK for all newer versions** and click **Continue**.
5. Review your personal information and the license agreement.
6. Select the **I agree** check box and click **I confirm** to continue.
7. Click **Download now**.
8. Save the unrestricted.zip file to your system.
9. Record the directory and the zip file name. You will need this information during the installation process.

Download the JCE Distribution File for the SUN JDK 1.6

About this task

The Java Cryptography Extension (JCE) is a set of Java packages from Sun Microsystems, Inc. or IBM that provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. By default, the software uses the limited strength JCE file that is included in the JDK that you use during the installation. Installing unlimited strength JCE file will overwrite the limited strength JCE file.

If you are installing the software outside of the United States, check to see if you can get the JCE unlimited strength jurisdiction policy files. The unlimited strength jurisdiction policy files can only be exported to countries to which the United States permits the export of higher-level encryption.

To obtain this file for the Sun JDK 1.6:

Procedure

1. Open your browser and navigate to http://java.sun.com/javase/downloads/index.jsp.
2. At the bottom of the page (Additional Resources), locate the **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6** and click **Download**.
3. Click the jce_policy-6.zip link start the download.
4. Save the jce_policy-6.zip file to your system.
5. Record the directory and the zip file name. You will need this information during the installation process.

Chapter 3. Configure the Database

Supported Database Servers in a Cluster Environment

In a UNIX/Linux cluster environment, the Sterling Integrator can support the following databases:

- Oracle®.
- DB2.
- Microsoft SQL Server - In this document, where ever Microsoft SQL Server (MSSQL) is mentioned, it applies to both 2005 and 2008 depending on which version you have installed. If the information is specific to one version or the other version, the version is specifically stated.

Only a non-clustered installation can use the MySQL database. See *System Requirements* for supported version information.

You must install, create, and configure a database so that each Sterling Integrator instance has a dedicated schema and login for the database.

Database Information You Need Before you Install Sterling Integrator in a Cluster Environment

Before you begin to install Sterling Integrator, you need to install and configure your database. Review and gather the following information. An "x" indicates the information is required.

Information to Gather	Oracle	DB2	Microsoft SQL Server	Record Information Here
Database User Name	x	x	x	
Database Password	x	x	x	
Database Catalog Name	x	x	x	
Database Host	x	x	x	
Database Port	x	x	x	
JDBC Driver #1	x	x	x	
JDBC Driver #2		x		
Use BLOB data?	x		x	
Enable Multibyte Support?	x	x	x	

Database Sizing and Capacity Planning

Database sizing is designed to give you estimates of the database growth and to assist in planning the disk requirements.

There are many factors to consider when estimating the amount of disk space that will be required for the Sterling Integrator. As a result, trying to consider all growth factors is impractical because the user may not know the answers to many questions that are required to do a detailed forecast. Over the years the cost of

© Copyright IBM Corp. 2000, 2013

disks has dramatically decreased, and the capacity and speed of disks has increased. The method of how information system managers order disk capacity has also changed, from purchasing disk arrays that are dedicated to a particular database server and project, to the concept of SANS (Storage Area Network).

The Sterling Integrator provides a methodology to estimate your initial disk requirements. Consider the confidence that you have in your data estimates when making the final purchase decision and adjust accordingly. After the initial purchase and production deployment, disk growth should be tracked for future purchase forecasts.

You should track your actual database storage usage and the number of database records regularly. Correlating these two metrics enabled you to plan your future disk requirements. Moreover, determining the average amount of space used for each order line or shipment line, enables you to accurately predict your future growth requirements.

Database Definition Language (DDL) Statements

When you install Sterling Integrator, you can manually apply Database Definition Language (DDL) statements to your database tables instead of requiring the installation process to do it directly. This option is not available for MySQL databases.

This feature increases database security by reducing the database permissions of the Sterling Integrator database user. The rights to database objects can be reserved for a secure user like a customer database administrator (DBA). A business can require that only a DBA with the proper permissions can make database changes.

If you:	Then
Choose to manually apply the DDL statements	Before you begin the installation, you will need to manually create the database schema using the SQL files in the */install_dir*/install/repository/scripts directory. You need to apply the DDL statements in a specific order. To find an example of the correct order, run an installation where the database schema was applied automatically and then look in the installation log file. The installation process will validate the database with a Sterling Integrator tool called DBVerify and warn you if there are issues, and will exit the installation.
Choose NOT to manually apply the DDL statements	The installation will apply the DDL statements.

Configure DB2 with Sterling Integrator

DB2 Database Configuration Checklist

Before you begin:

- If you do not have the DB2 installed, follow the procedures in the DB2 Installation manual.
- The installation script creates tables and indexes. Certain tables require a page size of 32K. You should have a table space to accommodate such tables. DB2

automatically places tables and indexes in the available tablespaces using its internal logic. You can move the tables to a different tablespace after the installation is complete.

- If you are reinstalling the software, be aware that data in your existing database will be deleted. To prevent this, either back up the existing database or save it under a different name.
- After creating and configuring your database, recycle the database. Then stop and restart to apply the changes.

Use the following checklist to configure DB2 for Sterling Integrator:

#	DB2 Database Configuration Checklist	Your Notes
1	Create the database. Refer to the DB2 documentation on creating the database, including creating a schema repository, login, and tablespace. Be sure to install the correct version and patches. See System Requirements for supported version information.	
2	Install Client Components, Compilers, and Fix Pack.	
3	Review the DB2 Parameters.	
4	Ensure the DB2 User Privileges are set.	
5	Install JDBC Drivers for DB2.	

Install DB2 Client Components, Compilers, and Fix Pack

About this task

The Sterling Integrator uses stored procedures for DB2. You must install or set up the following components:

Procedure

1. Install the Administration client.
2. Install the necessary fix pack after you install the client components and compilers. Otherwise, the clients will overwrite the fix pack binaries.
3. Set the path for the compiler by using the **db2set** command.

What to do next

For more information about these tasks, see the IBM documentation.

DB2 Parameters

The following parameters settings are required for your DB2 database:

Parameter	Value
DB2_SKIPDELETED	ON
DB2_SKIPINSERTED	ON
DB2_NUM_CKPW_DAEMONS	0
DB2LOCK_TO_RB	STATEMENT

Parameter	Value
LOCKLIST	AUTOMATIC
MAXLOCKS	AUTOMATIC If AUTOMATIC is not support, then 100
Database code page	UTF-8

For additional information, see the Performance Management documentation.

DB2 Database User Privileges

The DBADM role is required for performing administrative operations in DB2 database.

Install JDBC Drivers for DB2

About this task

For DB2, install the appropriate DB2 JDBC Type 4 driver and any correlating patches. See *System Requirements* for supported version information.

You can obtain these files from the IBM Web site. After you obtain this JDBC driver, record the absolute path to its location on your system. You must supply this absolute path during installation.

If the JDBC driver provided by your database vendor is distributed among multiple files, you must place all the files that comprise the JDBC driver into one .jar file. Follow these steps to create one .jar file:

Procedure

1. Identify all the vendor database jar files for the JDBC driver.
2. Create a temporary working directory (`mkdir wd; cd wd`).
3. Extract the contents of each file used for the JDBC driver using the jar utility into the temporary working directory (`jar xvf <jdbc.jar>` for each supplied jar file). Various Sterling Integrator scripts, such as the one used for loading the factory defaults, specify a DB_DRIVER. The DB_DRIVER specified must include all of these JAR files. The DB_DRIVER setting is located in sandbox.cfg.
4. Bundle the files in the temporary working directory into one file using the jar utility (`jar cvf new.jar*`).
5. Record the absolute path to the .jar file you created on the Preinstallation Checklist.

   The type-4 driver does not require a separate Java listener running on the database server. Instead, connect directly to the DB2 port.

Configure Oracle with Sterling Integrator

Oracle Database Configuration Checklist

About this task

You can use an Oracle database for maintaining information on Sterling Integrator.

Before you begin:

- If you are reinstalling the software, be aware that data in your existing database will be deleted. To prevent this, either back up the existing database or save it under a different name.
- After creating and configuring your database, recycle the database. Then stop and restart to apply the changes.

Use the following checklist to configure Oracle for Sterling Integrator:

#	Oracle Database Configuration Checklist	Your Notes
1	Create the database. Refer to the Oracle documentation on creating the database, including creating a schema repository, login, and tablespace. Be sure to install the correct version and patches. See *System Requirements* for supported version information.	
2	Configure an Oracle Instance.	
3	Configure Oracle Rollback.	
4	Install the Oracle JDBC Driver.	
5	Enable Failover in a Multiple Node Oracle RAC Database Cluster.	
6	After Sterling Integrator is installed, if you want to encrypt the data traffic, perform one of the following tasks: • Configure Sterling Integrator for Data Traffic Encryption • Configure Sterling Integrator for Data Traffic Encryption with SSL	

Configure an Oracle Instance

About this task

Before you begin:

- You must have the Oracle database installed. Ensure you have installed the correct versions and patches. See *System Requirements* for supported version information.
- Ensure that the user responsible for creating and modifying the Oracle database has a specified quota (extent) assigned in the tablespace, even if the user was assigned an unlimited tablespace. Otherwise, the installer may throw the error *ORA-09150: no privileges on tablespace name*.

To configure the Oracle database:

Procedure

1. Run the create instance procedure. Use AL32UTF8 as the character set.
2. Configure the INIT<INSTANCE_NAME>.ORA file. The following parameter settings are required:

Parameter	Parameter Definition	Value
OPEN_CURSORS	Number of open cursors	Greater than or equal to 2000
SHARED_POOL_SIZE	Shared pool size	Greater than or equal to 90000000
LARGE_POOL_SIZE	Large pool size	Greater than or equal to 614400
JAVA_POOL_SIZE	Java pool size	Greater than or equal to 20971520
PROCESSES	Number of processes	Greater than or equal to 500 Must be greater than the number of connections required by Sterling Integrator (sum of transactional or local and NoTrans pools in jdbc.properties), and operational management tools.
LOG_BUFFER	Log buffer	Greater than or equal to 163840
DB_BLOCK_SIZE	Database block size	Greater than or equal to 8192
NLS_LENGTH_SEMANTICS	NLS Length semantics	CHAR When you change the multi-byte character set to CHAR, Oracle reserves space equivalent to "n" characters, which is more than "n" bytes.
SGA_MAX_SIZE	SGA maximum size	1 GB to *n* GB, depending on the amount of physical memory on your database server. If the server is running only this database, up to 80% of physical memory.
SGA_TARGET	SGA components total size	1 GB to *n* GB, depending on the amount of physical memory on your database server. If the server is running only this database, up to 80% of physical memory.
PGA_AGGREGATE_TARGET	PGA target aggregate memory	1 GB to *n* GB, depending on the amount of physical memory on your database server. If the server is running only this database, up to 80% of physical memory.
cursor_sharing	Cursor sharing	exact
timed_statistics	Timed Statistics	true
optimizer_mode	Optimizer mode	All_rows
db_cache_size	Database cache size	Greater than or equal to 19200

3. Identify or create a tablespace for user tables and indexes.
4. Create a user. Unless specifically stated for a given task, the user does not require database administrator (DBA) privileges.
5. Grant permissions to the user. The following permissions are required for the administrative user for creating and modifying the Oracle database: GRANT "CONNECT" TO SI_USER ALTER USER SI_USER DEFAULT ROLE "CONNECT" GRANT CREATE SEQUENCE TO SI_USER GRANT CREATE TABLE TO SI_USER GRANT CREATE TRIGGER TO SI_USER GRANT SELECT ON CTXSYS.CTX_USER_INDEXES TO SI_USER GRANT SELECT ON SYS.DBA_DATA_FILES TO SI_USER GRANT SELECT ON

SYS.DBA_FREE_SPACE TO SI_USER GRANT SELECT ON SYS.DBA_USERS TO SI_USER GRANT SELECT ON SYS.V_$PARAMETER TO SI_USER GRANT SELECT ANY DICTIONARY TO SI_USER GRANT ALTER SESSION TO SI_USER GRANT CREATE SESSION TO SI_USER

6. If you are using Oracle AQ, grant the AQ_ADMINISTRATOR_ROLE permission.

Configure Oracle Rollback

About this task

You can rollback changes in Oracle using AUTO UNDO management. It is recommended that you use this option. This will avoid any manual monitoring of UNDO segments.

If a server is upgraded from Oracle 8i, set the UNDO_MANAGEMENT=AUTO parameter in init< SID>.ora. Your database administrator needs to determine the UNDO_RETENTION setting. Ensure that the file system, which has the UNDOTBS1 tablespace, has enough space to use the AUTOGROW setting.

Install the Oracle JDBC Driver

The Sterling Integrator requires the appropriate JDBC driver for Oracle Database. These drivers are thin client based pure Java JDBC drivers. See *System Requirements* for supported version information. The supported versions of the JDBC driver will build the correct Sterling Integrator directory structure.

Enable Failover in a Multiple Node Oracle RAC Database Cluster

About this task

To enable failover in a multiple node Oracle RAC database cluster in UNIX/Linux:

Procedure

1. Navigate to */install_dir*/install/properties directory to modify the sandbox.cfg file.
2. In the sandbox.cfg file, add a new property for ORACLE_JDBC_URL, which contains the Oracle RAC connection URL.

   The following example shows the suggested URL form and the way it is organized to connect using Service Name or System ID (SID). You can use either one of these identifiers when adding a URL, however, be aware that Oracle plans to depricate use of SID.

   The property value must be one string of text starting with ORACLE_JDBC_URL=. Your database administrator (DBA) can modify this URL as needed.

   ```
   jdbc:oracle:thin:@
     (DESCRIPTION=
       (ADDRESS_LIST=
         (FAILOVER=ON)
         (LOAD_BALANCE=OFF)
         (ADDRESS=(PROTOCOL=TCP)(HOST=myhost1)(PORT=1521))
         (ADDRESS=(PROTOCOL=TCP)(HOST=myhost2)(PORT=1521))
       )
         (CONNECT_DATA = (SERVER = DEDICATED)(SERVICE_NAME = myservicename OR mySID))
       )
   ```

3. Navigate to */install_dir*/install/bin.

4. Enter `./setupfiles.sh`.

Data Traffic Encryption in Oracle Database 11g

You can encrypt transactions between Sterling Integrator and Oracle Database 11*g*. This prevents anyone outside the system from viewing the data while it tracks between the Sterling Integrator and the database.

The following is a list of important aspects of enabling database encryption with Sterling Integrator:

- The default configuration for encryption at installation is no encryption. If you want to have your database transactions to be encrypted, you must perform the tasks provided in this topic.
- The encryption can be enabled at any time.
- Once you enable encryption, it applies to all database transactions between Sterling Integrator and the database.

System performance may be impacted when encryption is enabled. The extent of this impact will depend on your hardware, database configuration, transaction volume, and the relative amount of processing time spent by the system against other activities.

Addition information on data traffic configuration can be found in the Oracle® documentation, which can be accessed from http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf.

Before You Encrypt Data Traffic for Oracle 11g Database

Consider the following when configuring database traffic encryption:

- Sterling Integrator must be installed in TCP (clear) mode before you can configure encryption.
- You should perform these changes to your database prior to installing Sterling Integrator.
- You should configure wallets for encryption only mode even if the wallet used is empty. Enable auto login for all wallets.
- If you want to use SSL for encryption only, it is recommended to follow the instructions in the Oracle *CASE #1: USE SSL FOR ENCRYPTION ONLY* section of the Oracle documentation. It is not necessary to configure certificates for the wallet. In this mode, Diffie-Hellman ciphers are used and neither the server nor the client is authenticated through SSL. You must authenticate by using a username and a password. However, if you are running Sterling Integrator on a platform that requires an IBM JDK, you cannot use this mode, as IBM JSSE TrustManager does not permit anonymous ciphers. You must configure wallets with certificates.
- If you want to use SSL for encryption and for server authentication, it is recommended to follow the instructions in the Oracle *CASE #2: USE SSL FOR ENCRYPTION AND SERVER AUTHENTICATION* section of the Oracle documentation.
- If you want to use SSL for encryption and for server authentication of both tiers, it is recommended to follow the instructions in the Oracle *CASE #3: USE SSL FOR ENCRYPTION AND AUTHENTICATION OF BOTH TIERS* section of the Oracle documentation, depending on how you intend to configure client and/or server authentication.

- Once you configure your database for data traffic encryption, the database accepts both TCP (clear) and TCPS (encrypted) connections.
- There is a known issue in Oracle Database 11*g* when the listener is configured only for TCPS. The lsnrctl utility (that is used to start/stop DB listeners) attempts to contact the listener, which is enabled first. You should define the address list of the listener to contact either TCP or IPC before contacting TCPS.

Configure Sterling Integrator for Data Traffic Encryption in Oracle

About this task

Use this procedure if you want to enable data traffic encryption only, with anonymous authentication, and not SSL authentication.

If you want to use SSL for encryption only, it is recommended to follow the instructions in the Oracle *CASE #1: USE SSL FOR ENCRYPTION ONLY* section of the Oracle documentation. It is not necessary to configure certificates for the wallet. In this mode, Diffie-Hellman ciphers are used and neither the server nor the client is authenticated through SSL. You must authenticate by using a username and a password. However, if you are running Sterling Integrator on a platform that requires an IBM JDK, you cannot use this mode, as IBM JSSE TrustManager does not permit anonymous ciphers. You must configure wallets with certificates.

However, if you are running Sterling Integrator on a platform that requires an IBM JDK, you cannot use this mode, as IBM JSSE TrustManager does not permit anonymous ciphers. You must configure wallets with certificates.

This procedure is applicable only if you are running Sterling Integrator on a platform that requires Sun JDK. The IBM JSSE TrustManager does not permit anonymous ciphers.

If your Sterling Integrator is a cluster installation, you will need to perform this procedure on each node, starting with node 1.

Procedure

1. Install Sterling Integrator in TCP (clear) mode.
2. Stop Sterling Integrator.
3. Navigate to `/install_dir/install/properties`.
4. Open the customer_overrides.properties file and add the following additional database connection information:

   ```
   jdbcService.oraclePool.prop_oracle.net.ssl_cipher_suites=
   (SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_
   MD5,SSL_DH_anon_WITH_DES_CBC_SHA)
   jdbcService.oraclePool.prop_oracle.net.ssl_server_dn_match=false
   ```

   If you have a container configured, ensure that the same database information is added to the customer_overrides.properties.in file. To locate the file, navigate to */install_dir*/install/properties/nodexACy. Where *x* gives the node number and *y* gives the container number. Perform this step for all the containers configured in the system.
5. Repeat Step 4 for the following Oracle connection pools by changing only the poolname:
   - oraclePool_local

- oraclePool_NoTrans
- oracleArchivePool
- oracleUIPool

If you have any other database pools, you will need to add the properties for those pools.

6. Open the sandbox.cfg file and change the database connection information as shown:

```
ORACLE_JDBC_URL= jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)
(HOST=<DB host>)(PORT=<TCPS port as configured in DB config section above>))
(CONNECT_DATA=(SERVICE_NAME=<service name>)))
```

Make sure you enter the HOST, PORT, and SERVICE_NAME.

7. Open the activemqconfig.xml.in file and modify the following database connection information:
   - Remove or comment out the following default ActiveMQ database configuration information:

```
<bean id="gis-ds" class="org.apache.commons.dbcp.BasicDataSource"
destroy-method="close" singleton="true" lazy-init="default"
autowire="default" dependency-check="default"
SCIOverrideName="persistence-bean">
<property name="driverClassName">
<value>oracle.jdbc.driver.OracleDriver</value>
</property>
<property name="url">
#:ifdef ORACLE_JDBC_URL
<value>&ORACLE_JDBC_URL;</value>
#:else
<value>jdbc:oracle:thin:@&ORA_HOST;:&ORA_PORT;:&ORA_DATA;</value>
#:endif
</property>
 <property name="username">
<value>&ORA_USER;</value>
</property>
<property name="password">
<value>&ORA_PASS;</value>
</property>
<property name="maxActive">
<value>32</value>
</property>
</bean>
```

   - Add the following ActiveMQ database configuration information:

```
<bean id="gis-ds"
class="oracle.jdbc.pool.OracleDataSource" destroy-method="close"
singleton="true" lazy-init="default"
autowire="default"
dependency-check="default">
<property name="URL"><value>&ORACLE_JDBC_URL;</value></property>
<property name="user"><value>&ORA_USER;</value></property>
<property name="password"><value>&ORA_PASS;</value></property>
<property name="connectionProperties"><value> oracle.net.ssl_cipher_suites:
(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA, SSL_DH_anon_WITH_RC4_128_MD5,
SSL_DH_anon_WITH_DES_CBC_SHA)
oracle.net.ssl_client_authentication: false
oracle.net.ssl_version: 3.0
driverClassName:oracle.jdbc.driver.OracleDriver
maxActive: 32
</value>
 </property>
</bean>
```

8. Navigate to */install_dir*/install/bin.

9. Enter ./setupfiles.sh.
10. Restart Sterling Integrator. All the database connections from Sterling Integrator are now connected through TCPS (encrypted) mode.

Configure Sterling Integrator for Data Traffic Encryption with SSL Authentication in Oracle

About this task

Use this procedure to enable data traffic encryption and SSL authentication. This procedure is applicable if you are running Sterling Integrator on a platform that requires either Sun JDK or IBM JDK.

The example in this procedure uses 2-way SSL authentication. It is recommended to follow the instructions in the Oracle *CASE #2: USE SSL FOR ENCRYPTION AND SERVER AUTHENTICATION* section of the Oracle documentation.

You can also configure 1-way SSL authentication. If you want to use SSL for encryption and for server authentication of both tiers, it is recommended to follow the instructions in the Oracle *CASE #3: USE SSL FOR ENCRYPTION AND AUTHENTICATION OF BOTH TIERS* section of the Oracle documentation. For more information about 1-way SSL authentication, refer to Oracle® documentation, which can be accessed from http://www.oracle.com/technology/tech/java/sqlj_jdbc/pdf/wp-oracle-jdbc_thin_ssl.pdf.

If your Sterling Integrator is a cluster installation, you will need to perform this procedure on each node, starting with node 1.

Procedure

1. Install Sterling Integrator in TCP (clear) mode.
2. Stop Sterling Integrator.
3. Navigate to */install_dir*/install/properties.
4. Open the customer_overrides.properties file and add additional database connection information:

```
jdbcService.oraclePool.prop_javax.net.ssl.trustStore=/.../path/
.../ClientKeyStore.jks
jdbcService.oraclePool.prop_javax.net.ssl.trustStoreType=JKS
jdbcService.oraclePool.prop_javax.net.ssl.trustStorePassword=password
jdbcService.oraclePool.prop_oracle.net.ssl_version=3.0
jdbcService.oraclePool.prop_javax.net.ssl.keyStore=/.../path/
.../ClientKeyStore.jks
jdbcService.oraclePool.prop_javax.net.ssl.keyStoreType=JKS
jdbcService.oraclePool.prop_javax.net.ssl.keyStorePassword=password
```

5. Repeat step 4 for the following Oracle connection pools by changing only the poolname:
   - oraclePool_local
   - oraclePool_NoTrans
   - oracleArchivePool
   - oracleUIPool

   If you have any other database pools, you will need to add the properties for those pools.
6. Open the sandbox.cfg file and change the database connection information to:

```
ORACLE_JDBC_URL= jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)
(HOST=<DB host>)(PORT=<TCPS port as configured in DB config section above>))
(CONNECT_DATA=(SERVICE_NAME=<service name>)))
```

7. Navigate to */install_dir*/install/activemq/conf.
8. Open the activemqconfig.xml.in file and modify the database connection information:
   - Remove or comment out the following default ActiveMQ database configuration information:

     ```
     #:ifdef ORACLE
     <bean id="gis-ds" class="org.apache.commons.dbcp.BasicDataSource"
     destroy-method="close" singleton="true" lazy-init="default"
     autowire="default" dependency-check="default"
     SCIOverrideName="persistence-bean">
     <property name="driverClassName">
     <value>oracle.jdbc.driver.OracleDriver</value>
     </property>
     <property name="url">
     #:ifdef ORACLE_JDBC_URL
     <value>&ORACLE_JDBC_URL;</value>
     #:else
     <value>jdbc:oracle:thin:@&ORA_HOST;:&ORA_PORT;:&ORA_DATA;</value>
     #:endif
     </property>
     <property name="username">
     <value>&ORA_USER;</value>
     </property>
     <property name="password"><value>&ORA_PASS;</value>
     </property>
     <property name="maxActive"><value>32</value>
     </property>
     </bean>
     #:endif
     ```

   - Add the following ActiveMQ database configuration information:

     ```
     <bean id="gis-ds"
     class="oracle.jdbc.pool.OracleDataSource" destroy-method="close"
     singleton="true" lazy-init="default" autowire="default"
     dependency-check="default">
     <property name="URL"><value>&ORACLE_JDBC_URL;</value></property>
     <property name="user"><value>&ORA_USER;</value></property>
     <property name="password"><value>&ORA_PASS;</value></property>
     <property name="connectionProperties"><value>
     javax.net.ssl.trustStore: /.../path/.../ClientKeyStore.jks
     javax.net.ssl.trustStoreType:JKS
     javax.net.ssl.trustStorePassword:password
     oracle.net.ssl_version:3.0
     javax.net.ssl.keyStore: /.../path/.../ClientKeyStore.jks
     javax.net.ssl.keyStoreType:JKS
     javax.net.ssl.keyStorePassword: password
     driverClassName:oracle.jdbc.driver.OracleDriver
     maxActive:32
     </value>
     </property>
     </bean>
     ```

9. Enter ./setupfiles.sh.
10. Restart Sterling Integrator. All the database connections from Sterling Integrator are now connected through TCPS (encrypted) mode.

Configure Microsoft SQL Server with Sterling Integrator

Microsoft SQL Server Database Configuration Checklist

About this task

You can use an Microsoft SQL Server database for maintaining information in the Sterling Integrator.

Before you begin:

- If you are reinstalling the software, be aware that data in your existing database will be deleted. To prevent this, either back up the existing database or save it under a different name.
- After creating and configuring your database, recycle the database. Then stop and restart to apply the changes.

Use the following checklist to configure Micrsoft SQL Server for Sterling Integrator:

#	Microsoft SQL Server Database Configuration Checklist	Your Notes
1	If you do not have Microsoft SQL Server installed, follow the installation procedures in the SQL server installation manual. Refer to the Microsoft SQL server documentation on creating the database, including creating a schema repository, login, and tablespace. Be sure to install the correct version and patches. See *System Requirements* for supported version information.	
2	For Microsoft SQL 2005, install the Microsoft SQL 2005 Server Service Pack and Hotfix.	
3	Ensure the Microsoft SQL Database parameters are set.	
4	Review the Microsoft SQL Server Database user privileges.	
5	Configure Snapshot for Microsoft SQL Server.	
6	Install the Microsoft SQL Server JDBC driver.	

Microsoft SQL Server Database User Privileges

In Microsoft SQL Server, you must grant DBO (Database Owner) permission to the user. The DB_DDLADMIN role is required for creating objects in the SQL Server database.

Microsoft SQL Server Database Parameters

To create a database, ensure that the collation property you select supports all the characters for your database. The following parameter settings are required in your Microsoft SQL Server database:

Parameter	Value
Collation Setting	SQL_Latin1_General_CP850_BIN
Sort order	Binary
Security authentication	SQL Server and Windows
Torn Page Detection	Off

Install Microsoft SQL Server 2005 Service Pack and Hotfix

About this task

Before you begin:

- Ensure that Named Pipes & TCP/IP protocols are enabled in the network utility of the SQL Server.
- For SQL Server 2005, do not use case-sensitive column names in the database. Case-sensitive names will prevent the SQL Server 2005 System Management Console from loading.

To install Microsoft SQL Server 2005, Service Pack 2 and hotfixes:

Procedure

1. Install the Microsoft SQL Server 2005 base release.
2. Install the Microsoft SQL Server 2005 Service Pack 2. You can download it from http://www.microsoft.com/downloads/details.aspx?familyid=D07219B2-1E23-49C8-8F0C-63FA18F26D3A&displaylang=en.
3. Apply the cumulative hotfix package. You can download it from http://support.microsoft.com/default.aspx?scid=kb;EN-US;933097.
4. Apply the GDR2 hotfix. You can download it from http://support.microsoft.com/kb/934459/. The Microsoft SQL Server 2005 version is now 9.00.3159.

Install the JDBC Driver in Microsoft SQL Server

About this task

Sterling Integrator requires the correct Microsoft SQL Server driver. See *System Requirements* for supported version information.

Go to the Microsoft web site to download the driver and any appropriate patches.

Procedure

1. Download sqljdbc_*version_language*.tar.gz to a temporary directory.
2. To unpack the zipped tar file, navigate to the directory where you want the driver unpacked and type the following command: `gzip -d sqljdbc_version_language.tar.gz`
3. To unpack the tar file, move to the directory where you want the driver installed and type the following command: `tar –xf sqljdbc_version_language.tar`

After the package unpacks, you can find out more information about using this driver by opening the JDBC Help System in the */absolutePath*/sqljdbc_*version*/*language*/help/default.htm file. This will display the help system in your Web browser.

4. When the Sterling Integrator installation asks for the location of the JDBC drivers, specify the extracted jar file created after unpacking the archive (usually named sqljdbc.jar). The JDBC driver version is the same as the version of the drivers downloaded from Microsoft.

Configure Snapshot for Microsoft SQL Server

About this task

The snapshot feature in Microsoft SQL Server allows you to view a read-only copy of the database even when it is locked. Configuring the snapshot feature can also reduce deadlocks.

Enter the following command to enable the snap shot feature:

```
ALTER DATABASE db_name SET READ_COMMITTED_SNAPSHOT ON;
```

Database Password Management

Database Passwords

A password is used by the system to connect to its database. The password is stored as clear text in a system property file. If the security policies at your company require you to encrypt these passwords, you can do so after you install the system. Encrypting these passwords is optional.

Database Passwords Encryption Methods

Database passwords are encrypted using one of two methods, OBSCURED or ENCRYPTED. The encryption method is decided by the value of the encryptionPrefix in propertyEncryption.properties or propertyEncryption.properties_platform_security_ext file.

Encrypt Database Passwords

About this task

To encrypt the database password:

Procedure

1. Stop the Sterling Integrator.
2. Navigate to */install_dir*/install/bin.
3. Enter `./enccfgs.sh`.
4. Enter `./setupfiles.sh`.
5. Enter `./deployer.sh`.
6. Enter `./run.sh` to start the Sterling Integrator.
7. Enter your passphrase.

Decrypt Database Passwords

About this task

To decrypt the database password:

Procedure

1. Stop the Sterling Integrator.
2. Navigate to */install_dir*/install/properties.
3. Open the sandbox.cfg file.
4. Copy the encrypted password from the database_PASS property.

   Use the text that appears after the database_PASS= text. For example, if database_PASS= OBSCURED:123ABCxyz321, you would copy the text OBSCURED:123ABCxyz321. (OBSCURED is the encryption method for the password.)
5. Navigate to */install_dir*/install/bin.
6. Enter `./decrypt_string.sh encrypted _password`.

   For encrypted_password, use the text that you copied in Step 4.

   You are prompted for the system passphrase.

   After you enter the passphrase, your decrypted password appears.
7. Navigate to */install_dir*/install/properties.
8. Edit the sandbox.cfg file to replace the encrypted password with the password that was returned in Step 6.
9. You need to decrypt the entries for YANTRA_DB_PASS and DB_PASS. Repeat Steps 4 to 8 to decrypt these entries. You should also decrypt any passwords present in the property files. Encrypted passwords typically reside in the following property files:
   - sandbox.cfg
   - apservsetup
   - jdbc.properties/.in
   - customer_overrides.properties/.in
10. Navigate to */install_dir*/install/bin.
11. Enter `./setupfiles.sh`.
12. Enter `./deployer.sh`.
13. Enter `./run.sh` to start the Sterling Integrator.
14. Enter your passphrase.

Chapter 4. Install the Software

General UNIX/Linux Installation Information

Caution: Sterling Integrator should be installed behind a company firewall for security purposes. See the Perimeter Server and Security topics in the Sterling Integrator documentation library for more information on secure deployment options.

Use one of the following methods to install your system:

- GUI-Based
- Text-Based
- Silent Install File

The following are some general installation guidelines:

- If you are on Linux, do not use any soft or symbolic links in the path to the SCIInstallWizard.jar file.
- If you are using FTP to copy the files, verify that your session is set to binary mode.
- The installation directory must have adequate free disk space.
- The installation directory must not already exist because the installation process creates it.
- If you are using AIX with the DB2 database, the directory path cannot be longer than 108 bytes.
- The directory path to SI.jar cannot include any spaces.

General Wizard Information

The installation wizard provides:

- The option of either entering the paths or selecting the paths and files (**Select File** button).
- For every screen in the GUI-Based installation wizard, you need to click **Next** to move to the next step the wizard. The click Next step is not represented in each step in the procedure.
- For every screen in the Text-Based installation wizard, you need to press **Enter** to move to the next step the wizard. The press **Enter** step is not represented in each step in the procedure.

Guidelines for a UNIX/Linux Cluster Environment Installation

The cluster environment does not support the following items:

- MySQL database
- AS2 Edition

The following are some installation guidelines for cluster environments:

- You need a valid Sterling Integrator license for multiple IP addresses of all nodes where the Sterling Integrator will be installed and configured as a cluster.
- All nodes must use the same database.
- All nodes must use the same passphrase.

© Copyright IBM Corp. 2000, 2013

- All nodes must use the same operating system.
- When installing nodes on different machines, the initial port numbers must be the same. Installing nodes are different machines helps you take advantage of cluster features such as, reliability, availability, scaliablity, and failover.
- When installing nodes on the same machine, you must install node 2 and higher in different directories. Each initial port must be at least 200 higher or lower than the initial port for the other nodes.
- You must install the nodes sequentially, one at time, starting with the first node.
- After installing the nodes, you must start the nodes sequentially, one at a time, starting with the first node.
- Clustering is not supported for systems that use a MySQL database.

Guidelines for IPv6 Addresses

Before using an IPv6 address during an installation, see *IPv6 Capabilities* section in *System Requirements*.

Consider the following IPv6 address information when planning the installation:

- If you use an IPv6 address, use a fully qualified address that includes square brackets around the address, and a zero (0) between colons where there are no other numbers. For example, use [fe80:0:0:0:213:72ff:fe3c:21bf] instead of fe80::213:72ff:fe3c:21bf.
- If you are installing with IPv6 address, comment the Host Name mapping to IPv4 address and retain the mapping to IPv6 address in the host file located in /etc/sysconfig/networking/profiles/default/hosts directory.
- You must install using a host name, not an IPv6 address, otherwise the Lightweight JDBC adapter and Graphical Process Modeler (GPM) will not work.
- If you are using an Oracle database, do not use an IP v6 address for the host name.
- If you are using an IPv6 address and are going to configure Sterling Integrator as a dual stack host, after you complete the installation, you will need to add the IPv6 address (as the admin_host.3 property) to the noapp.properties_platform_ifcresources_ext .in file.

Install Using the GUI-Based Method in a UNIX/Linux Cluster Environment

About this task

Before you begin:

- You should have completed the *Preinstallation Checklist for UNIX/Linux*.
- The license file must reside on the host machine on which the application is being installed. If you saved the license file to a Windows client, transfer the license file to the host.
- If you are using an IPv6 address, review the *Guidelines for IPv6 Addresses.*
- *install_dir* refers to the installation directory where the new software will be installed. Do not use any pre-existing directory name or an old version of the Sterling Integrator installation directory. If you do, you could inadvertently overwrite the existing installation. You should create a new installation directory before you begin the installation.
- *parent_install* is the directory one level above the *install_dir* directory.

- Ensure that the *parent_install* directory has the proper permissions set using the chmod command.
- If you are installing Sterling Integrator on VMware, provide the IP address of the virtual machine, not the IP address of the VMware host. For example, if 10.251.124.160 is the IP address of the VMware host and 10.251.124.156 is the IP address of the Windows 2003 server it is hosting, you should use 10.251.124.156 as the correct IP address to install Sterling Integrator.
- The installation creates subsequent ports based on the initial port number. For all of the port assignments, see the */install_dir*/install/properties/sandbox.cfg file.

To install Sterling Integrator, refer to your pre-installation checklist and follow these steps:

Procedure

1. From the installation media, copy SCIInstallWizard.jar and SI.jar to a UNIX/Linux directory.
2. Log in to a Windows machine.
   a. Start X server in your UNIX/Linux server using an X Windows client tool.
   b. Log in to your UNIX/Linux environment.
   c. Set the display to use your server as a client using the following command: `export DISPLAY=server:0.0`
3. Navigate to your working directory. For example, cd *parent_install*.
4. Enter: `/path_to_java/bin/java -jar /absolutePath/SCIInstallWizard.jar`

   The program verifies support for your operating system and JDK. It also verifies that your operating system is patched to the required level.

   The installation wizard is displayed.
5. Click **Next** to start the installation wizard.
6. Review the License conditions and click **Accept** to accept the terms.
7. Enter the full path to the JDK directory.
8. Enter the full path to the license file.

   If you have not installed a license file, you can minimize this window, obtain the license file, and then return to the installation process.
9. Enter the full path to your JCE file.
10. Enter the path to installation directory. If the directory does not exist, click **Yes** at the prompt *The directory does not exist, create it?*. The installer creates the installation directory.

    This installation directory is referred to as *install_dir*. Below the installation directory, install_dir, the installer creates a directory named install. This directory contains the installation files.
11. Enter the path to the Sterling Integrator install jar file.
12. Enter the explicit IP address for the server or use the default value of localhost.
13. Enter the initial port number or use the default value of 8080.
14. Enter your system passphrase.
15. Re-enter the system passphrase.
16. Enter the administrative e-mail address to which you want system alert messages sent.

17. Enter the SMTP mail server (IP address or host name) that you want to use for system alert messages and other administrative notices.
18. If you want to enable FIPS (Federal Information Processing Standards) mode, select the checkbox. The default is disable FIPS mode.
19. Select the database that you want to use (Oracle, Microsoft SQL Server, or DB2).
20. Select all options that apply to this node:

Choices:	Action
This installation is an upgrade from a prior version.	Do not select this option.
This installation is for a cluster node 2 or higher	• For node 1: Do not select the check box. • For node 2 or higher: Select the check box.
(Skip for MySQL) Apply database schema automatically?	• If yes, no action required. The default is to automatically apply the DDL statements. • If you want to manually create the database schema, then clear the **Apply database schema automatically** check box. After the installation wizard stops, you must perform these additional steps: 1. Manually create the database schema. 2. Rename or delete the *install_dir* directory. 3. Start the installation wizard again. When you are executing the scripts, it is important to execute the SQL scripts in a particular order. The SQL script order is dependant on the database configured with your system. See the database documentation for further information. **Important:** In version 5.1 of Sterling Integrator, there is an issue with this feature and the installation wizard. For information on the corrective workaround, see InQuira Article NFX11576.
Verbose install?	• By default, the check box is not selected. • Select the checkbox to generate the installation log. The events that occur during the installation are recorded in InstallSI.log file.

21. Enter the database connection information.
    - Database user name
    - Database password (and confirmation)
    - Database catalog name
    - Database host name
    - Database port
    - (Oracle and Microsoft SQL Server only) Absolute path and file name for one JDBC driver file
    - (DB2 only) Absolute paths and file names for two JDBC driver files

Use the Type-4 JDBC driver. This type of driver converts JDBC calls into the network protocol used directly by DB2, allowing a direct call from Sterling Integrator to the DB2 server.

- (Oracle only) Select the check box to select the data type to use for caching. Select either the default BLOB (binary large object) columns data type or the Long Raw data type.

  You can significantly improve performance by enabling the cache on the BLOB data object in Oracle. For more information, refer to the Sterling Integrator documentation for slow performance in Oracle.

22. Review and confirm the database information.
23. Review the default **Install Actions**. The following check boxes are automatically selected and you can not clear them:
    - Verify Operating System is supported
    - Verify the selected JDK is supported
    - Install Components
    - Save install files
    - Clean Up Files
24. Select the appropriate JDK. By default, the 64-bit JDK is selected. By default, the 64-bit JDK is selected.
25. If you want to create a desktop icon for launching Sterling Integrator, select the check box . By default, the check box is not selected.
26. Click **Next** to continue.

    The Installation Progress screen appears. You can click **Show Details** to confirm your installation information before starting the installation.
27. Click **Install**.

    The Installation Progress screen shows the general progress of the installation through different stages. For more information about these stages, click **Show Details**.

    For more detailed information about the installation, you can also refer to the */install_dir*/PreInstallSI.log file.

    The installation completes automatically. When the installation is finished, the system displays a dialog box with the message `Installation Wizard completed. Please see the installation guide for next steps.`

    Installation information is in the following log files:
    - ant.install.log (in the *install_dir* directory)
    - InstallSI.log (in the *install_dir*/install directory)
28. If you are using the AIX operating system and are using IPv6:
    - Navigate to the */install_dir*/install/properties
    - Add the following to the sandbox.config file: `IPV4STACK=false`
    - Navigate to the */install_dir*/install/bin
    - Enter ./setupfiles.sh
29. Install each subsequent node, from node 2 onwards. Navigate to your working directory. For example, cd *parent_install* directory.
30. You need to start the installation wizard for the additional node, enter: `/path_to_java/bin/java -jar /absolutePath/SCIInstallWizard.jar`

    The program verifies support for your operating system and JDK. It also verifies that your operating system is patched to the required level. You will follow the same steps as you did for node 1 until you get to Step 21. When prompted, **This installation is for a cluster node 1 or higher**, enter **true**.

31. If you installed multiple nodes on the same machine or used different base ports for node 2 onward, you need to complete the following additional steps:

Step	Action	Your Notes
1	Navigate to /*install_dir*/install/properties for node 1.	
2	In the noapp.properies_platform_ifcresources_ext file, record the value for multicastBasePort.	
3	In the jgroup_cluster.properties file, record the values for the mcast_port parameters of the property_string and lock.protocolStack properties.	
4	For each subsequent node, you need to perform the remaining steps.	
5	Navigate to /install_dir/install/properties for each node (node 2 and higher).	
6	In the noapp.properies_platform_ifcresources_ext.in file, update the value of the multicastBasePort to match the value for node 1. For example, replace the string &MULTICAST_NODE_PORT1; with the port number 45460. • (before) multicastBasePort= &MULTICAST_NODE_PORT1; • (after) multicastBasePort=45460	
7	In the jgroups_cluster.properties.in and jgroups_cluster.properties_fifo_ext.in files, update all occurrances of mcast_port to match the values for node 1.	
8	After you have updated the attributes for all of the nodes, enter: /install_dir/install/bin/setupfiles.sh for node 2 and higher.	

32. Determine if you need to apply a patch to the installation. Refer to *Installation Maintenance* for information on how to install the latest patch.

Install Using the Text-Based Method in a UNIX/Linux Cluster Environment

About this task

Before you begin:

- You should have completed the *Preinstallation Checklist for UNIX or Linux*.
- The license file must reside on the host machine on which the application is being installed. If you saved the license file to a Windows client, transfer the license file to the host.
- If you are using an IPv6 address, review the Guidelines for IPv6 Addresses.
- *install_dir* refers to the installation directory where the new software will be installed. Do not use any pre-existing directory name or an old version of the Sterling Integrator installation directory. If you do, you could inadvertently overwrite the existing installation. You should create a new installation directory before you begin the installation.

- *parent_install* is the directory one level above the *install_dir* directory.
- Ensure that the *parent_install* directory has the proper permissions set using the chmod command.
- If you are installing Sterling Integrator on VMware, provide the IP address of the virtual machine, not the IP address of the VMware host. For example, if 10.251.124.160 is the IP address of the VMware host and 10.251.124.156 is the IP address of the Windows 2003 server it is hosting, you should use 10.251.124.156 as the correct IP address to install Sterling Integrator.
- If at any time you wish to go back and change any input previously entered, you will have to re-start the installation. You can abort the installation by pressing **Ctrl** + **C** and then re-starting the installation.
- The installation program validates the initial port number and confirms that you have enough disk space for the installation. These port assignments are written to the */install_dir*/install/properties/sandbox.cfg file.

To install Sterling Integrator, refer to your pre-installation checklist and follow the steps below:

Procedure

1. From the installation media, copy SCIInstallWizard.jar and SI.jar to a UNIX/Linux directory.
2. Navigate to your working directory. For example, cd *parent_install*.
3. Enter: `/path_to_java/bin/java -jar /absolutePath/SCIInstallWizard.jar`
4. Press **Enter** to start the installation.
5. Press **Enter** to review the license agreement. You can page through the agreement by entering `n` and pressing **Enter** at each page or you can go directly to the end of the agreement, press **Enter** until you reach the *Do you accept the license?*
6. Press **Enter** to accept the license agreement. Default value is Y.
7. Enter the full path of your JDK directory.

   Use the */absolutePath* part of the */absolutePath*/bin/java section of your installation command.
8. Enter the full path to the License file.
9. Enter the full path to unlimited strength JCE policy file.
10. Enter the full path name to the installation directory. This must be a newly created directory or the installation will later fail. If the installation directory does not exist, when prompted enter `Y` to create the directory.

    This installation directory is referred to as *install_dir*. Below the installation directory, *install_dir*, the installer creates a directory named install. This directory contains the installation files.
11. Enter the path to your installable jar file.
12. Enter an explicit IP address or host name. Default is localhost.
13. Enter the initial port number. Default is 8080.
14. Enter your system passphrase.
15. Enter your system passphrase again to confirm it.
16. Enter the administrative e-mail address to which you want system alert messages sent.
17. Enter the SMTP mail server host name that you want to use for system alert messages and other administrative notices.
18. Do you want to use FIPS (Federal Information Processing Standards) mode?

- If yes, enter **true**.
- If no, press **Enter**. Default value is false.

19. Enter the number of the database vendor (Oracle, Microsoft SQL Server, or DB2).
20. At the *This installation is an upgrade from a prior version* prompt, press **Enter** to continue as a new installation. Default is false.
21. For node 1, enter **false** (default) at the *This installation is for a cluster node 2 or higher* and press **Enter**. For node 2 and higher, enter **true** and press **Enter**.
22. (Skip for MySQL) At the *Apply database schema automatically?* prompt:
    - To automatically apply the database schema, press **Enter**. The default is to automatically apply the DDL statements.
    - To manually create the database schema, enter `false`. After the installation wizard stops, you must perform these additional steps:
      a. Manually create the database schema.
      b. Rename or delete the *install_dir* directory.
      c. Start the installation wizard again.

    When you are executing the scripts, it is important to execute the SQL scripts in a particular order. The SQL script order is dependant on the database configured with your system. See the database documentation for further information.

    Important: In version 5.1 of Sterling Integrator, there is an issue with this feature and the installation wizard. For information on the corrective workaround, see InQuira Article NFX11576.
23. Do you want to installation information to be stored in the InstallSI.log file (*Verbose Install*)?
    - If no, press **Enter**. (Default value is false).
    - If yes, enter `true`. The events are recorded in InstallSI.log file.
24. Configure your database by entering the following information:
    - Database user name
    - Database password (and confirmation)
    - Database catalog name
    - Database host name
    - Database host port number
    - (Oracle and Microsoft SQL Server only) Absolute path and file name for one JDBC driver
    - (DB2 only) Absolute paths and file names for two JDBC drivers.

      Use the Type-4 JDBC driver. This type of driver converts JDBC calls into the network protocol used directly by DB2, allowing a direct call from Sterling Integrator to the DB2 server.
    - (Oracle only) At the **What Datatype would you like to use?** prompt, choose a data type for caching (BLOB or Long Raw).

      To use caching for BLOB (binary large object) columns, enter 1 (the default value). You can significantly improve performance by enabling the cache on the BLOB data object in Oracle. For more information, refer to the documentation for slow performance in Oracle.

      To use the Long Raw data type, enter 2.
25. Review the Database Information.
26. Is this a 32 or 64-bit JDK?

- If you are using a 32-bit JDK, enter 1.
- If you are using a 64-bit JDK (default value), press **Enter**.

27. Do you want to create a desktop icon for accessing Sterling Integrator?
    - If yes, enter **true** at the **Create Desktop Icons (Windows & Linux)** prompt.
    - If no, press **Enter**. Default value is false.

    The installation automatically continues.

    The screen displays the progress of your installation. You can follow more detailed progress of your installation through the PreInstallSI.log file in your installation directory. If the installation stops, check the PreInstallSI.log for details.
28. When the installation is finished, the system displays the following message:

    ```
    BUILD SUCCESSFUL
    Installation Wizard completed.
     Please see the installation guide for next steps.
    ```

    Installation information is in the following log files:
    - ant.install.log (in the *install_dir* directory)
    - InstallSI.log (in the *install_dir*/install directory)
29. If you are using the AIX operating system and are using IPv6:
    - Navigate to the /*install_dir*/install/properties
    - Add the following to the sandbox.config file: `IPV4STACK=false`
    - Navigate to the /*install_dir*/install/bin
    - Enter ./setupfiles.sh
30. Install each subsequent node, from node 2 onwards. Navigate to your working directory. For example, cd *parent_install* directory.
31. You need to start the installation wizard for the additional nodes, enter: `/path_to_java/bin/java -jar /absolutePath/SCIInstallWizard.jar`

    The program verifies support for your operating system and JDK. It also verifies that your operating system is patched to the required level. You will follow the same steps as you did for node 1 until you get to Step 21. When prompted, **This installation is for a cluster node 1 or higher**, enter **true**.
32. If you installed multiple nodes on the same machine or used different base ports for node 2 onward, you need to complete the following additional steps:

Step	Action	Your Notes
1	Navigate to install_dir/install/properties for node 1.	
2	In the noapp.properies_platform_ifcresources_ext file, record the value for multicastBasePort.	
3	In the jgroup_cluster.properties file, record the values for the mcast_port parameters of the property_string and lock.protocolStack properties.	
4	For each subsequent node, you need to perform the remaining steps.	
5	Navigate to install_dir/install/properties for each node (node 2 and higher).	

Step	Action	Your Notes
6	In the noapp.properies_platform_ifcresources_ext.in file, update the value of the multicastBasePort to match the value for node 1. For example, replace the string &MULTICAST_NODE_PORT1; with the port number 45460. • (before) multicastBasePort= &MULTICAST_NODE_PORT1; • (after) multicastBasePort=45460	
7	In the jgroups_cluster.properties.in and jgroups_cluster.properties_fifo_ext.in files, update all occurrances of mcast_port to match the values for node 1.	
8	After you have updated the attributes for all of the nodes, enter: /install_dir/install/bin/setupfiles.sh for node 2 and higher.	

33. Determine if you need to apply a patch to the installation. Refer to *Installation Maintenance* for information on how to install the latest patch.

Silent Installation

The silent installation method automates part of the installation process and limits your manual interaction with the installation program. To use the silent installation method, you will need to first create a silent install file using a text editor.

Create the Silent Installation File in a UNIX/Linux Cluster Environment

About this task

The following entries correlate to prompts in the Install Using the Text-Based method procedure. The silent install file must contain the entries marked as required in the following table. Record the file name and location, as you will use this information during the installation.

Create a silent installation file with the following variables:

Silent Install File Entry	Description
ACCEPT_LICENSE	(Required) Indicates if the user accepts the license agreement. Default: YES
JVM_LOC	(Required) Full path to JDK directory.
LICENSE_FILE_PATH	(Required) Full path to a valid license file. Example: */absolutePath*/Full_License.xml
SI_LICENSE_AVAILABLE	(Optional) Indicates if a license is being passed in and is required for the installation. Default: YES

Silent Install File Entry	Description
JCE_DIST_FILE	(Required) Full path to unlimited strength JCE policy file. If present, this file will overwrite the JCE file in the JDK. Example: */absolutePath*/unrestrict123.zip
INSTALL_DIR	(Required) Directory that includes the bin subdirectory (where many commands are stored) and the properties subdirectory (where many properties are stored).The INSTALL_DIR property cannot point to a pre-existing directory, or the installation will fail. It can include the following: • The installation directory that you specify during an interactive installation. • The subdirectory "install". Although you can enter your own path, the */install_dir*/install path matches the path that is created during an interactive installation.
REINIT_DB	(Required) Indicates if database should be initialized. • For node 1 of a cluster, this property is true. • For node 2 and higher of a cluster, this property is false. Default: true
CLUSTER	(Required) Indicates if this is the second or higher node of a cluster installation. Valid values: • true - This is the second or higher node of a cluster installation. • false (default) - This is the first node of a cluster or a single node (non-cluster) installation.
INSTALL_IP	(Required) Host name or IP address. Valid values: • localhost (default) • (your IP address or host name) If you are installing Sterling Integrator on VMware, provide the IP address of the virtual machine, not the IP address of the VMware host. For example, if 10.251.124.160 is the IP address of the VMware host and 10.251.124.156 is the IP address of the Windows 2003 server it is hosting, you should use 10.251.124.156 as the correct IP address to install Sterling Integrator. **CAUTION:** **Before applying an IPv6 address, see** *IPv6 Capabilities* **section in the** *System Requirements***.** If you use an IPv6 address, use a fully qualified address that includes square brackets around the address, and a zero (0) between colons where there are no other numbers. For example, use [fe80:0:0:0:213:72ff:fe3c:21bf] instead of fe80::213:72ff:fe3c:21bf. If you are installing with IPv6 address, comment the Host Name mapping to IPv4 address and retain the mapping to IPv6 address in the host file located in /etc/sysconfig/networking/profiles/default/ hosts directory. You must install using a host name, not an IPv6 address, otherwise the Lightweight JDBC adapter and Graphical Process Modeler (GPM) will not work.

Silent Install File Entry	Description
PORT1	(Required) Base port for ASI server. Ports are assigned consecutively from this port. Example: 12345 Default: 8080
APSERVER_PASS	(Required) Passphrase used to secure all encrypted data in database.
SI_ADMIN_MAIL_ADDR	(Required) E-mail address for the administrative user. Example: abc@xyz.com
SI_ADMIN_SMTP_HOST	(Required) Valid SMTP host through which the system can e-mail the administrative user. Example: mail.xyz.com
FIPS_MODE	(Optional) Indicates if you are using FIPS (Federal Information Processing Standards) mode. Valid values: • true - Enable FIPS mode. • false (default) - Disable FIPS mode.
DB_VENDOR	(Required) Database vendor. Valid values: • Oracle • MSSQL2005 (use this value for Microsoft SQL 2005 and 2008) • DB2 • MySQL (default)
DB_CREATE_SCHEMA	(Required) Indicates if you want the database schema automatically created. Valid values: • true (default) - Automatically create the schema. • false - Manually create the schema. If you create the database schema manually, restart the installation procedure in a new installation directory. You can delete the installation directory created earlier.
DEBUG	(Optional) Records events that occur during the installation in InstallSI.log file. Valid values: • true - records events that occur during the installation. • false (default) - does not record the events that occur during installation.
DB_USER	(Required) Database user name. Example: abcd_123_1
DB_PASS	(Required) Database password. Example: xyz
DB_DATA	(Required) Database catalog name. Example: abcd
DB_HOST	(Required) Database host name. Example: abcd Default: localhost

Silent Install File Entry	Description
DB_PORT	(Required) Database port. Example: 1234
DB_DRIVERS	(Required) Full path to JDBC driver files. If DB_VENDOR is: • Oracle or MSSQL, specify one driver. • DB2, specify two drivers. If you specify more than one driver, use colons (:) to separate the file names. Examples: • *JDBC_driver_dir*/db2jdbc.jar • *JDBC_driver_dir*/db2_1_jdbc.jar:*JDBC_driver_dir*/db2_2_jdbc.jar
ORACLE_USE_BLOB	(Required if DB_VENDOR=Oracle) Indicates the data type to use for caching. • true (default) - BLOB (binary large object) • false - Long Raw
MSSQL2005	(Required for Microsoft SQL Server 2005) This attribute is case-sensitive. • Set this attribute to the default value of true. • (All other servers) Do not include this attribute.
JDK64BIT	Indicates if a 32-bit or 64-bit JDK is being used. Refer to the *System Requirements* to determine the type of JDK for your operating system. Valid values: • true (default) - 64-bit • false - 32-bit
Icons	(Required) Indicates whether to create a desktop icon for accessing Sterling Integrator. Valid values: • true - Create a desktop icon. • false (default) - Do not create a desktop icon.

The following entries do not directly correlate to prompts in the installation procedure. Use these entries to customize or document your installation.

Silent Install File Entry	Description
IPV4STACK	(Required for AIX) Set this parameter to false. For example: IPV4STACK=false
DB_DRIVERS_VERSION	(Optional) Free form version string for JDBC driver. This is informational only. Example: 8_1_5
LOAD_FACTORY_SETUP	(Optional) Indicates whether factory setup should be loaded during installation. To manually set LOAD_FACTORY_SETUP to false after an installation where LOAD_FACTORY_SETUP=true (the default value), change LOAD_FACTORY_SETUP to false in sandbox.cfg file. Valid values: • true (default).- loads factory setup during installation. • false - does not load factory setup during installation. Run loadDefaults command after installation.

Silent Install File Entry	Description
CONFIG_GS	(Optional) Indicates whether integration with Gentran Server should be configured. Default: No
NO_DBVERIFY	(Optional) Valid values are true or false. When set to true during installation and installservice, dbverify will not be run. This means that the Sterling Integrator will not generate DDL to make the database like the XML entity repository.

Install with a Silent Installation File in a UNIX/Linux Cluster Environment

About this task

Before you begin:

- *parent_install* is the directory one level above the *install_dir* directory.
- *install_dir* refers to the installation directory where the new software will be installed. Do not use any pre-existing directory name or an old version of the Sterling Integrator installation directory. If you do, you could inadvertently overwrite the existing installation. You should create a new installation directory before you begin the installation.
- If you are using AIX and IPv6, you must set the IPV4STACK parameter to false in the silent installation file.

To install Sterling Integrator using a silent installation file:

Procedure

1. From the installation media, copy SI.jar to a UNIX/Linux directory.
2. Set up your silent installation file and record the file location.
3. Navigate to your working directory. For example, cd *parent_install*.
4. To start the installation, enter:

   ```
   /absolutePath/bin/java -jar /absolutePath/SI.jar -f
   /absolutePath/SilentInstallFile
   ```

   The installation starts. You can follow the progress of the installation on screen.

   The installation program verifies support for your operating system and JDK. It also verifies that you have enough space for the installation.

   When the installation is finished, the system displays the following message:

   ```
   Installation has completed successfully.
   ```

5. (Skip this step if you are applying database schema automatically.) If you are going to manually create the database schema, the installation will stop. After it has stopped, you need to perform the following steps:
   a. Manually create the database schema.
   b. Rename or delete the *install_dir* directory.
   c. Start the silent installation again.

   When you are executing the scripts, it is important to execute the SQL scripts in a particular order. The SQL script order is dependant on the database configured with your system. See the database documentation for further information.

Important: In version 5.1 of Sterling Integrator, there is an issue with this feature and the installation wizard. For information on the corrective workaround, see InQuira Article NFX11576.

6. If you are installing nodes on separate machines, copy the silent install file for node 1 into a new silent install file and then set REINIT_DB=false and set CLUSTER=true. This REINIT_DB=false prevents the database from being re-initialized. After you have the silent install files for node 2 and higher, proceed to Step 8.
7. If you are installing multiple nodes on the same machine, copy the silent install file for node 1 into a new silent install file and then set REINIT_DB=false, set CLUSTER=true, use a different installation directory for each node (INSTALL_DIR) and make sure that the initial port for each node is 100 port numbers higher or lower than node 1. After you have the silent install files for node 2 and higher, proceed to Step 7.
8. To start the installation of nodes 2 and higher of the cluster, enter:

   ```
   /absolutePath/bin/java -jar /absolutePath/SI.jar -f
   /absolutePath/SilentInstallFile - cluster
   ```

9. If you installed multiple nodes on the same machine or used different base ports for node 2 onward, you need to complete the following additional steps:

Step	Action	Your Notes
1	Navigate to */install_dir*/install/properties for node 1.	
2	In the noapp.properies_platform_ifcresources_ext file, record the value for multicastBasePort.	
3	In the jgroup_cluster.properties file, record the values for the mcast_port parameters of the property_string and lock.protocolStack properties.	
4	For each subsequent node, you need to perform the remaining steps.	
5	Navigate to */install_dir*/install/properties for each node (node 2 and higher).	
6	In the noapp.properies_platform_ifcresources_ext.in file, update the value of the multicastBasePort to match the value for node 1. For example, replace the string &MULTICAST_NODE_PORT1; with the port number 45460. • (before) multicastBasePort= &MULTICAST_NODE_PORT1; • (after) multicastBasePort=45460	
7	In the jgroups_cluster.properties.in and jgroups_cluster.properties_fifo_ext.in files, update all occurrances of mcast_port to match the values for node 1.	
8	After you have updated the attributes for all of the nodes, enter: */install_dir*/install/bin/setupfiles.sh for node 2 and higher.	

10. Determine if you need to apply a patch to the installation. Refer to *Installation Maintenance* for information on how to install the latest patch.

Chapter 5. Validate the Installation

Validate the Installation Checklist in a Cluster Environment

As part of the installation, you need to run the following tests to ensure that the software installation was successful. Complete the following tasks:

#	Validate Installation Task	Completed
1	Verify the Cluster Environment Settings in Property Files.	
2	Configure the Nodes in the Cluster.	
3	Start a Cluster.	
4	Access Sterling Integrator.	
5	Validate the Installation.	
6	Verify the Cluster is Running from the User Interface.	
7	Stop a Node (Hard Stop or Soft Stop) or Stop the Cluster.	

Verify the Cluster Environment Settings in Property Files

About this task

To verify the cluster environment is correct, check these property settings on node 2:

Procedure

1. Verify that CLUSTER=true is in the sandbox.cfg property file.
2. Verify that CLUSTER=true is in the centralops.properties property file.
3. Verify that CLUSTER=true is in the noapp.properties property file.
4. Verify that cluster_env property=true is in the ui.properties property file.

Configure the Nodes in the Cluster

About this task

The first time you configure a cluster, you need to use the startCluster command with true option (startCluster.sh nodeNumber true). Initial configuration should be the only time you need to use the startcluster command. However. if you should need to use the command again, use the startcluster command with the false option (startCluster.sh nodeNumber false). The false option prevents any configuration changes from affecting the system, especially after installation of a patch or hot fix.

To configure the nodes, starting with node 1:

Procedure

1. Navigate to */install_dir*/install/bin.

© Copyright IBM Corp. 2000, 2013

2. Enter `./startCluster.sh <nodeNumber> <true or false>`. Where <nodeNumber> is the number of the node, true performs database updates and false prevents database updates. For example for node 1, enter `./startCluster.sh 1 true`.
3. If you are starting node 2 or higher, enter your passphrase. For node 1, you are not prompted to enter your passphrase.
4. After the cluster has started, the following message is displayed:

   ```
   BUILD SUCCESSFUL
   Total time nn minutes nn seconds
   Done with ant script
   Running setup files
   ```

   You can proceed to the next node after the command line prompt appears.

What to do next

After all the nodes are configured, the following message is displayed:

```
Deployment to application server successful.
```

Start the Cluster

About this task

You need to perform this task for each node.

To start the cluster:

Procedure

1. Navigate to */install_dir*/install/bin.
2. Enter `./run.sh`.
3. Enter your passphrase.
4. The final startup processes run, concluding with the following message: `Open your Web browser to http://host:port/dashboard`

   where *host:port* is the IP address and port number where Sterling Integrator resides on your system.

   Depending on system load, it may take several minutes for the UI to be ready.
5. Record the URL address so that you can access Sterling Integrator.

What to do next

Note: If you need to release all the locks in a cluster and both nodes are down, use the restart parameter for Node 1. For example:

For Node 1, enter:

```
./run.sh restart
```

For Nodes 2 and higher, enter:

```
./run.sh
```

Access Sterling Integrator

About this task

To log in to Sterling Integrator:

Procedure

1. Open a browser window and enter the address displayed at the end of startup. The login page displays.
2. Enter the default user ID (`admin`) and password (`password`). The default login is at an administrative level. One of your first tasks as an administrator is to change the administrative password and to register other users with other levels of permission.

Validate the Installation

About this task

Validate the installation by testing a sample business process:

Procedure

1. From the Administration Menu, select **Business Process > Manager**.
2. In the Process Name field, enter `Validation_Sample_BPML` and click **Go!**
3. Click **execution manager**.
4. Click **execute**.
5. Click **Go!** The `Status: Success` message displays in the upper left side of the page.

Verify the Cluster is Running from the User Interface

About this task

To verify the cluster is running from the User Interface (UI):

Procedure

1. From the UI, from the **Administration Menu**, select **Operations > System > Troubleshooter**. Ensure you can view the Business Process Queue Usage information for each node.
2. From the UI, from the **Administration Menu**, select **Operations > System > Troubleshooter**. Ensure you can view the JNDI Tree for each node.
3. From the UI, from the **Administration Menu**, select **Operations > System > Troubleshooter**. Ensure you can view the host, state, status, adapters, and memory usage information for each node.
4. From the UI, from the **Administration Menu**, select **Operations > System > Troubleshooter**. Ensure you can view the adapter status for each node.

Stop a Node in a Cluster Environment (Soft Stop)

About this task

A soft stop halts the system after all the business processes finish running. In a cluster environment, you need to perform this task on each node, starting with node 1.

Running the soft stop command in a clustered environment suspends all of the scheduled business processes. It is recommended to run the hard stop command when stopping individual nodes of a cluster.

To soft stop in a UNIX or Linux environment:

- You can select **Operations > System > Troubleshooter** and click **Stop the System**.
- You can perform the soft stop from the command line interface.

To run a soft stop, from the command line:

Procedure

1. Navigate to */install_dir*/install/bin.
2. Enter `./softstop.sh`.
3. Enter your passphrase.

Stop a Node in the Cluster Configuration (Hard Stop)

About this task

You can stop a single node Sterling Integrator in an UNIX or Linux cluster environment.

To run a hard stop, perform this task for each node:

Procedure

1. Navigate to */install_dir*/install/bin.
2. Enter `./hardstop.sh`.

Stop the Cluster

About this task

To stop the cluster:

Procedure

1. From the Administration Menu, select **Operations > System > Troubleshooting**.
2. Click **Stop the System**.

Chapter 6. Post Installation Configuration

Post Installation Configuration Checklist for Cluster Environment

After you have installed the Sterling Integrator, you need to complete the post installation configuration checklist. Review all tasks, but note, some tasks may not be required for your installation.

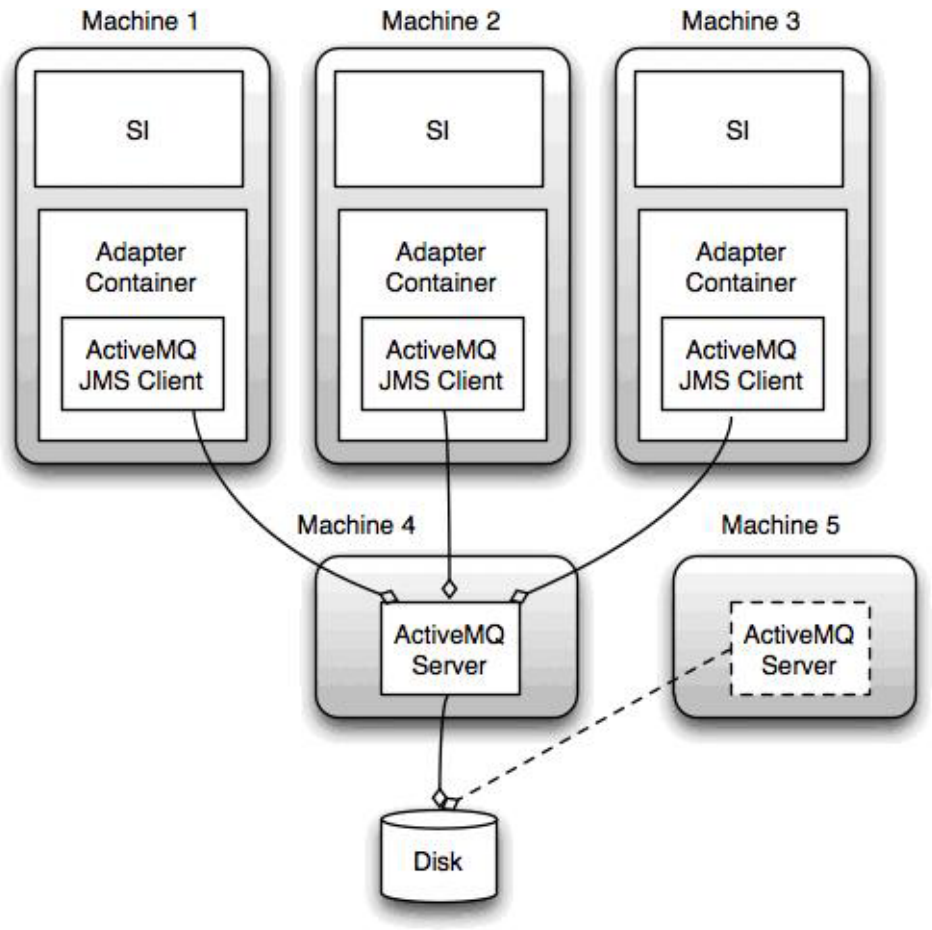
#	Post Installation Configuration Checklist	Your Notes
1	For security purposes, change all default user ID passwords immediately after the installation is completed. See the *Update My Account Information* task in the documentation library.	
2	Configure ActiveMQ for a cluster environment.	
3	If you are using an IPv6 address in a dual stack configuration, complete the *Add the IPv6 Address for the Dual Stack Configuration* task.	
4	Download Sterling Integrator Tools.	
5	Determine if you need to modify any Property Files.	
6	Configure Shared File System as Document Storage.	
7	Add host[port] from all the nodes to the jgroups_cluster.property.in for each node.	
8	If you are using an IPv6 address, you need to complete the *Update the sandbox.cfg File for IPv6 Address* task.	
9	Configure Customer Overrides File with a Firewall between Nodes.	

JMS Cluster Configuration for Failover

To allow proper JMS execution and failover in the Sterling Integrator 5.1 cluster environment, you must configure an external ActiveMQ using the *Configure ActiveMQ for a Cluster Environment* task.

The following diagram illustrates how the ActiveMQ can be configured to increase availability and failover.

© Copyright IBM Corp. 2000, 2013



Configure ActiveMQ for a Cluster Environment

About this task

To configure the ActiveMQ for the cluster environment:

Procedure

1. Download the ActiveMQ 5.2 from http://activemq.apache.org/activemq-520-release.html for the appropriate OS.
2. Deploy an instance of ActiveMQ 5.2. This can be on the same machine as Sterling Integrator or on a separate machine.
3. Navigate to */install_dir*/install/properties.
4. Copy the activemq.xml file to the AMQ conf directory. This file configures the ActiveMQ to:
   - Use failover clustering
   - Use the SI database for storage
   - Configures the AMQ port usage

   By default, ActiveMQ is configured to listen at the Sterling Integrator base port + 64 and the ActiveMQ interface will be at base port + 65 (http://server:base port + 66/admin). The port can be changed by editing the config file.

5. Navigate to */install_dir*/install/properties.
6. On each Sterling Integrator application node and each Sterling Integrator container node, the queue configuration must be re-directed to utilize the ActiveMQ cluster. In each node, add the following to the customer_overrides.properties:

   For FIFO Processing:

   ```
   fifo.broker.username=
   fifo.broker.password=
   fifo.broker.url=failover:(tcp://amq_master_hostname:amq_master_port,
   tcp://amq_slave_hostname:amq_slave_port)
   ```

   For adapters running in separate JVM containers:

   ```
   iwfcqueue.username=
   iwfcqueue.password=
   iwfcqueue.protocol_config=failover:(tcp://amq_master_hostname:amq_master_port,
   tcp://amq_slave_hostname:amq_slave_port)
   ```

7. Start the ActiveMQ instances. To start ActiveMQ, it is necessary to supply the activemq.hostname property with the hostname for the current system. For example:

   ```
   activemq -Dactivemq.hostname=ExampleHostname
   ```

   See http://activemq.org for additional information about running an ActiveMQ instance.
8. Start Sterling Integrator.

Add the IPv6 Address for Dual Stack Configuration

About this task

If you are using IPv6 and have Sterling Integrator configured in a dual stack, you need to add the IPv6 address to the admin host list.

To add the IPv6 address:

Procedure

1. Navigate to the installation directory that contains the noapp.properties file.
2. Open the noapp.properties_platform_ifcresources_ext .in file.
3. Add following line to the properties file:

   ```
   admin_host.3=FULL_IPv6_ADDRESS
   ```

   Where FULL_IPv6_ADDRESS is the IPv6 address of the machine. (Make sure you surround the IPv6 address with square brackets.)
4. Save and close the file.
5. Run the setupfiles.sh.
6. Start Sterling Integrator.

Download Sterling Integrator Tools

Sterling Integrator includes tools that run on a desktop or personal computer. After you install, you can install the following tools:

- Map Editor and associated standards
- Graphical Process Modeler (GPM)
- Web Template Designer

- (If licensed) MESA Developer Studio plug-ins, including, MESA Developer Studio Software Development Kit (SDK) and MESA Developer Studio Skin Editor
- If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.

Conflicting IP addresses can cause problems when you download a desktop tool.

Property Files Configuration

Property files contain properties that control the operation of the Sterling Integrator. For example, the REINT_DB property in the sandbox.cfg file controls whether or not a database is initialized when you install Sterling Integrator.

By modifying the values of these properties, you can customize the Sterling Integrator to suit your business and technical needs. Most property files are in the:

- For UNIX, /*install_dir*/install/properties directory
- For Windows, *install_dir*\install\properties directory

After installing the Sterling Integrator, most property files and scripts do not need any further configuration for basic operation. However, if you want to customize any specific operations, for example setting a different logging level - you will need to edit (or in some cases, create) certain property or .xml files.

Before changing any property files, refer to Working with Property Files documentation for general information about how to work with Property Files.

Areas where you might need to make specific property files changes after an installation include:

- LDAP user authentication
- Prevention of cross-site script vulnerabilities
- Logging configuration
- Process-specific property file settings
- Securing the Interop Servlet

Configure Shared File Systems as Document Storage

About this task

To configure the shared file systems as document storage:

Procedure

1. Navigate to /*install_dir*/install/properties.
2. Open the jdbc.properties.in file.
3. Update the value of the *document_dir* attribute to point to the shared files system directory where you store documents.
4. Save and close the file.
5. Navigate to /*install_dir*/install/bin.
6. Enter `./setupfiles.sh`.
7. Restart the Sterling Integrator.

Add host[port] From all the Nodes to the jgroups_cluster.property.in for Each Node

About this task

Complete this task for both vertical and horizontal clusters. You will need to complete this task for each node, starting with node 1.

Before you begin, it is important to note that you should never override mcast_addr in the jgroup_cluster.properties.

To add the host [port] to the jgroups_cluster.property.in file:

Procedure

1. Navigate to the properties file directory for the node.
2. Determine the initial_hosts port for each node:
   - Navigate to the properties file directory for the node.
   - Find the initial_hosts from the jgroups_cluster.property (initial_hosts=host{port}).
   - Record the value from the initial_hosts for each node.
3. Open the jgroups_cluster.property.in file.
4. Add the initial_hosts property to the file. For example, if node 1 is on host1 and node 2 is on host2. For node 1, you would add:

   ```
   initial_hosts=host1[port1],host2[port2]
   ```

   For node 2, you would add:

   ```
   initial_hosts=host2[port2],host1[port1]
   ```
5. Save and close the file.

Update the sandbox.cfg file for an IPv6 address

About this task

Before you begin, it is important to note that you should never override mcast_addr in the jgroup_cluster.properties.

To update the sandbox.cfg file for an IPv6 address (complete this task for each node in the cluster):

Procedure

1. Navigate to the properties file directory for each node.
2. Open the sandbox.cfg file.
3. Add the following line to the file.

   ```
   IPV4STACK=false
   ```
4. Save and close the file.
5. Navigate to the bin directory for your installation.
6. Enter setupfiles.sh (UNIX) or setupfiles.cmd (Windows).

Services and Adapters Associated with Node 1 in a Cluster

The following service and adapters are associated with node 1 in the cluster:

- Schedule
- FileSystem
- CmdLine
- CDServerAdapter
- CDAdapter
- CDRequesterAdapter
- CEUServerAdapter
- HttpServerAdapter
- B2B_HTTP_COMMUNICATIONS_ADAPTER
- HTTP_COMMUNICATIONS_ADAPTER
- HTTPClient Adapter
- FTPClientAdapter
- FtpServerAdapter
- SFTPClientAdapter

The following services have storage set to database:

- HttpServerAdapter
- CEUServerExtractrServiceType
- CDSERVER_ADAPTER

The default storage for all of the workflows is set to database.

Configure Customer Overrides File with a Firewall between Nodes

About this task

If you have configured a firewall between nodes that blocks ports outside of the port range assigned to Sterling Integrator, perform the following task on all nodes:

Procedure

1. Navigate to the Sterling Integrator installation directory.
2. Navigate to the properties directory and locate (or create, if necessary) the customer_overrides.properties file.
3. Open the customer_overrides.properties file using a text editor.
4. Add the following properties:

   ```
   noapp.jnp_host= <host_name>
   noapp.jnprmiport=<port_number_1>
   noapp.jnprmiport2=<port_number_2>
   noapp.useSocketFactories=true
   noapp.jndirmiport=<port_number_3>
   ops.jnp_host= <host_name>
   ops.jnprmiport=<port_number_1>
   ops.useSocketFactories=true
   ops.jndirmiport=<port_number_2>
   ops.jnprmiport2=<port_number_3>
   ```

   This increases the number of threads used by the system.
5. Save and close the customer_overrides.properties file.
6. Stop Sterling Integrator and restart it to apply the changes.

Chapter 7. Installation Maintenance

Installation Maintenance for a UNIX/Linux Cluster Environment

From time to time, you will need to apply either a patch or a hotfix to your Sterling Integration installation:

- All nodes in the cluster must be patched to the same level. You must stop all nodes in the cluster before installing a patch, then install the patch on each node.
- Patches contain cumulative fixes for a specific version of Sterling Integrator. Because each patch contains the fixes from previous patches, you only need to install the most recent patch. You should periodically check the web site to verify that you have the most recent patch.
- Hot-fix is one or more fixes applied to a specific existing patch.

It is possible to apply patches to nodes while other nodes are processing. However a patch containing any of the following, requires the entire cluster to be down:

- Critical cluster functionality
- Engine-related changes
- Changes to the database

You can preserve your custom changes to system resources (like workflow definitions and maps) when you update your system. During updates, the system can identify when you make a custom change versus when the system makes a change through an upgrade or patch.

When a patch, installation or upgrade is performed, a baseline record of system resources is created. This baseline is not affected by any subsequent customer changes. When another patch is installed, the resources in this baseline are compared to the resources in the existing system. If a baseline and existing resource are not the same, it means that the existing resource was customized and is not overwritten by the patch.

During an update, the baseline is updated with new system resource information, but not with custom changes to resources.

Determine if You need to Apply a Maintenance Patch in UNIX/Linux Environment

About this task

Patches contain cumulative fixes for a specific version of Sterling Integrator. Patch files are available at:

https://customer.sterlingcommerce.com.

Because each patch contains the fixes from previous patches, you only need to install the most recent patch. Patch files are named using the following naming convention:

si_<*release number*>_build_<*build number*>.jar

© Copyright IBM Corp. 2000, 2013

Information about a patch is located in a PDF file with a similar name. The naming convention for PDF files containing information about a particular patch is:

si_<*release number*>_build_<*build number*>_patch_info.pdf

Before you install the patch, review the following items:

- Preserve your custom changes to system resources.
- The patch installation may use one or more patch property override files. These files will be named *propertyFile_patch*.properties. Do not alter these files.
- Property changes made directly in *.properties or *.properties.in files may be overwritten during the patch installation. Properties overridden using the customer_overrides.properties file are not affected. Sterling Commerce recommends that you maintain property file changes using (when possible) the customer_overrides.properties file. For more information about this file, refer to the property file documentation.
- If you edited any of the cdinterop files, you must back them up before applying the patch. The cdinterop files do not have initialization (*.in) files. After applying the patch, use the backup version of the files in your patched installation. These files include the following files: cdinterop-proxy-records.properties; cdinterop-spoe-auth.properties; cdinterop-spoe-policy.properties; and cdinterop-user-records.properties.
- Information about the patch installation is automatically logged to /*install_dir*/install/logs/InstallService.log.
- If you would need to rollback a patch, see the *Patch Changes Report*.
- During patch installation, the dbVerify utility compares the list of standard indexes with those present in the database and drops the custom indexes. You should recreate the custom indexes after the patch installation is complete.

Install a Maintenance Patch in UNIX/Linux Cluster Environment

About this task

You will need to install the patch on each node in the cluster.

To install the latest patch for Sterling Integrator in a UNIX/Linux cluster environment:

Procedure

1. Navigate to https://customer.sterlingcommerce.com/user/login.aspx.
2. Login using your email address and password.
3. Download the most recent patch file for your version of Sterling Integrator and record the absolute path to the downloaded file. Do not rename the file. If you use FTP, you must use Binary mode.
4. Verify that the database server is up and ready to accept connections.
5. Stop Sterling Integrator.
6. Perform a full backup of the Sterling Integrator installation directory, including all subdirectories.
7. Perform a backup of the database.
8. If you edited any property files, ensure that the associated properties.in files have the most current changes. Property files will be overwritten with the contents of the associated properties.in files during the patch installation.
9. Is the database password encrypted? If Yes, decrypt the password.

10. Navigate to the bin directory where Sterling Integrator is installed. Enter: `cd /install_dir/install/bin`
11. Enter: `./InstallService.sh <path>/si_<release number>_build_<build number>.jar`

    If the patch attempts to modify the database schema and the modification fails, you will receive an error message about the failure. The message will provide the error message code from the database and the SQL command that failed. The failure information is also logged to the system.log file (in the /*install_dir*/install directory) and to the patch.log file.
12. Press **Enter** to continue.
13. If you want to accept the license agreement, enter `Y`.
14. Enter the passphrase.

    Information about the patch is displayed. After the patch has been applied, the following message is displayed: Deployment to application server successful
15. If you decrypted the database password, re-encrypt the password.
16. Enter `./startCluster.sh 1` to reconfigure the cluster after installing the patch.
17. Start Sterling Integrator.

    If you are using a perimeter server in the DMZ, you will to need to review the information on how to apply a patch to the perimeter server.

Preserve Custom Configuration Changes in the Cluster Environment (startCluster.sh)

About this task

As part of a default cluster configuration, certain values in the database for service or adapter configurations, and default document storage, need to be updated to get the cluster working. The default settings do not include a shared or mounted file system with a line of sight from all cluster nodes. Certain service or adapter configurations are forcibly deployed on node 1 and the default document storage type is set up to "Database" for all business processes.

To keep these custom configuration changes from being overwritten, you can run the following cluster configuration script:

```
./startCluster.sh nodeNumber true/false
```

Where:

- nodeNumber is the cluster node number
- True performs database updates (True is the default)
- False prevents database updates

The first time you configure a cluster, you need to have the option set to true. After the first configuration, you can use the false option. The false option prevents any configuration changes from affecting the system, especially after installation a patch or hot fix.

Apply a critical fix pack (stopping the whole cluster)

About this task

You will need to install the patch on each node in the cluster.

To apply a critical fix pack, where the entire cluster needs to be down:

Procedure

1. Stop the cluster.
2. Navigate to */install_dir*/install/bin.
3. Enter the following command for each node, starting with node 1: `./InstallServices.sh fixpack_dir/fixpackFilename.jar`.
4. Open the `sandbox.cfg` file and change REINT_DB as follows:
   - For node 1, REINT_DB=True
   - For node 2 or higher, REINT_DB=False, this prevents the database updates from repeating during the fix pack installation on each node.
5. Configure the node in the cluster, enter `./startCluster.sh nodeNumber false`
6. Start the cluster.

Apply a critical fix pack (stopping one node at a time)

About this task

To apply a fix pack, where the you stop one node at a time:

CAUTION:
Only use this update method if there are no database changes in the fix pack. Check the release notes for each fix pack for this information.

Procedure

1. Starting with node 1, navigate to */install_dir*/install/bin.
2. Stop the node.
3. After the processes stop, enter the following command: `./InstallServices.sh fixpack_dir/fixpackFilename.jar`.
4. Navigate to */install_dir*/install/properties.
5. Open the `sandbox.cfg` file and change REINT_DB as follows:
   - For node 1, REINT_DB=True
   - For node 2 or higher, REINT_DB=False, this prevents the database updates from repeating during the fix pack installation on each node.
6. Configure the node in the cluster, enter `./startCluster.sh nodeNumber false`
7. Repeat steps 1 to 6 for each node.

Applying a critical fix pack (stopping the whole cluster, starting one node at a time)

About this task

You must install the fix pack on each node in the cluster.

To apply a critical fix pack, where the entire cluster must be down:

Procedure

1. Stop the entire cluster.
2. Starting with node 1, do the following for each node:
   a. Navigate to /*install_dir*/install/bin.
   b. Enter the following command for each node, starting with node 1: `./InstallServices.sh fixpack_dir/fixpackFilename.jar`
   c. Open the `sandbox.cfg` file and change REINT_DB as follows:
      - For node 1, REINT_DB=True
      - For node 2 or higher, REINT_DB=False, this setting prevents the database updates from repeating during the fix pack installation on each node.
   d. Configure the node in the cluster enter `./startCluster.sh nodeNumber false`

Install a Hot-Fix in UNIX/Linux Cluster Environment

About this task

After you install the Sterling Integrator you may need to install a hot-fix. A hot-fix is one or more fixes applied to a specific existing patch. In a cluster environment, you need to apply the hot-fix to node 1 first and then to the subsequent nodes.

Before you can install a hot-fix developed for your company, you must have completed the following:

- Received the file name of the ccaseid.jar to install from Sterling Commerce Customer Support
- Created a full backup of the Sterling Integrator
- Created a full backup of your database
- Preserve your custom changes to system resources.

To install a hot-fix:

Procedure

1. Log in to the computer that you are installing the hot-fix on.
2. If the database password was encrypted, decrypt the password.
3. Enter `ftp theworld.stercomm.com.`
4. Enter your user name and password. If you do not know your user name and password, contact Sterling Commerce Customer Support.
5. Enter `bin` and press **Enter** to select Binary as your transfer mode.
6. At the FTP prompt, enter `get` *`ccaseid`*`.jar`, where *ccaseid* includes the ID number you received from Customer Support.
7. Stop the Sterling Integrator.
8. Navigate to /*install_dir*/install/bin.
9. Enter `./installService.sh` */absolutePath/ccaseid*.jar to install the hot-fix.
   You may need to complete this step twice depending on the patch. Read the output from the InstallService.sh script carefully to see if you need to complete this step twice.
10. If you decrypted the database password, re-encrypt the password.
11. Start the Sterling Integrator.
12. In the /*install_dir*/install/bin directory, enter `./dump_info.sh` to verify that the hot-fix was successfully installed.

13. After installing the hot-fix in node, enter `./startCluster.sh nodeNumber` to configure the node.
14. After node 1 is completed, open the sandbox.cfg file and change REINT_DB to false. False prevents the database updates from repeating on each node's patch installation.
15. Repeat steps 1 to 13 for the remaining nodes.

Uninstalling an interim fix

Uninstalling an interim fix is a manual process. IBM support must first determine what is included in the interim fix you want to remove, and then manually backout the changes one at a time. The complexity of this process, therefore, can vary greatly.

If you must remove an interim fix, contact IBM support by creating a PMR (Problem Management Record)

DB Checksum Tool

A checksum is a simple redundancy check used to detect errors in data. In Sterling Integrator 5.1, a verification process is used to compare the checksum between the existing default resource and the resource added after applying a patch or upgrading. The DB Checksum tool, a resource difference tool generates a granular report of the changes in the system that was not permitted to be set as defaults.

The DB Checksum tool generates the difference in resource checksum between the default resource and the latest system resource from the database.

Perform a Checksum

About this task

To run the DB Checksum tool:

Procedure

1. Navigate to */install_dir*/install/bin.
2. Enter:

   ./db_checksum_tool.sh [-d] [-i [1 | 2 | 3 | 4 | 5]] [-r [wfd | map | schema | sii | template]] [-o <output file>] [-g]

   Where:

   -d is the mode to dump the difference of resource checksum between the default resource and latest system resource.

   -i is the resource type integer (optional).

   1 is WFD.

   2 is MAP.

   3 is SCHEMA.

   4 is SII.

   5 is TEMPLATE.

   -r is the resource name (optional). For example, wfd, map, schema, sii, or template.

   -o is the file name to output all the messages (optional).

   -g is the file name that lists all the ignored resources (optional).

-h is the help screen.

The DB Checksum tool performs the relevant checksum operation based on the command options and generates the output message.

Patch Changes Report

The Patch Changes Report is used to obtain information if you need to rollback a patch. The patch report can be found in the installation directory patch_reports folder. The report contains the following patch information:

- Patch ID
- Patch Changes
- Number of files deleted
- Number of JARs removed
- Number of JARs added
- Number of files added
- Number of files changed
- Number of properties added
- Number of business processes added
- Number of service instances added
- Number of service definitions added
- Number of templates added
- Number of reports added
- Number of maps added
- Number of schemas added
- Number of business rules added

For example, the installation directory patch_reports folder contains the file Patch_Report.html. When you open this html file, you can view the patch information.

Example: Patch Changes Report

The following is an example of a Patch Changes Report.

```
Summary of Changes
Patch ID: Platform_2.0
Patch Changes: 1287
Number of Files Deleted: 0
Number of JARs Removed: 2
Number of JARs Added: 0
Number of Files Added: 3
Number of Files Changed: 3
Number of Properties Added: 4
Number of BPs Added: 4
Number of Service Instances Added: 2
Number of Service Definitions Added: 3
Number of Templates Added: 0
Number of Reports Added: 0
Number of Maps Added: 3
Number of Schemas Added: 3
Number of Business Rules Added: 0

_____________________________________
List of JARs Removed:
JAR Removed: /SAMPLE_INSTALL_1/jar/jaf/1_0_2/activation.jar
Time: Wed May 13 15:23:08 EDT 2009
JAR Removed: /SAMPLE_INSTALL_1/jar/commons_logging/1_0_3/commons-logging-api.jar
```

```
Time: Wed May 13 15:23:08 EDT 2009

_____________________________________________
List of Files Added:
File Added: /SAMPLE_INSTALL_1/bin/sql/fix_db2_schema.sql
Time: Wed May 13 15:21:30 EDT 2009
File Added: /SAMPLE_INSTALL_1/bin/sql/fix_db2iseries_schema.sql
Time: Wed May 13 15:21:30 EDT 2009
File Added: /SAMPLE_INSTALL_1/bin/errorQueueManager.sh.in
Time: Wed May 13 15:21:30 EDT 2009

_____________________________________________
List of Files Changed:
File Changed: /SAMPLE_INSTALL_1/properties/lang/en/Reports_en.properties
File Changed: /SAMPLE_INSTALL_1/properties/lang/es/Reports_es.properties
File Changed: /SAMPLE_INSTALL_1/properties/lang/fr/Reports_fr.properties

_____________________________________________
List of Properties Added:
Property Added: /SAMPLE_INSTALL_1/properties/filesToRemove.txt
Property Added: /SAMPLE_INSTALL_1/properties/filesToRemove.txt.in
Property Added: /SAMPLE_INSTALL_1/properties/csr.properties.sample
Property Added: /SAMPLE_INSTALL_1/properties/csr.properties.sample.in

_____________________________________________
List of BPs Added:
BP Added: Schedule_AssociateBPsToDocs.bpml version: 4
Time: Wed May 13 15:23:07 EDT 2009
BP Added: Recovery.bpml version: 17
Time: Wed May 13 15:23:07 EDT 2009
BP Added: Schedule_AutoTerminateService.bpml version: 10
Time: Wed May 13 15:23:07 EDT 2009
BP Added: Schedule_DBMonitorService.bpml version: 1
Time: Wed May 13 15:23:08 EDT 2009

_____________________________________________
List of Service Instances Added:
Service Instance Added: RetentionProcessor version: 2
Time: Wed May 13 15:23:28 EDT 2009
Service Instance Added: MESAHttpServerAdapter version: 1
Time: Wed May 13 15:25:11 EDT 2009

_____________________________________________
List of Service Definitions Added:
Service Definition Added: LockServiceType
Time: Wed May 13 15:22:58 EDT 2009
Service Definition Added: XAPIServiceType
Time: Wed May 13 15:22:59 EDT 2009
Service Definition Added: CleanLockServiceType
Time: Wed May 13 15:22:59 EDT 2009

_____________________________________________
List of Templates Added:
Template Added: Normalize
Time: Wed May 13 15:23:26 EDT 2009
Template Added: Derive
Time: Wed May 13 15:23:26 EDT 2009

_____________________________________________
List of Maps Added:
Map Added: IBMPutResponseToXML
Time: Wed May 13 15:24:05 EDT 2009
Map Added: http_headers
Time: Wed May 13 15:24:36 EDT 2009
Map Added: OracleHttpHeaders
Time: Wed May 13 15:24:51 EDT 2009

_____________________________________________
List of Schemas Added:
Schema Added: E5_V20_Acknowledge_Result.dtd from file: E5_V20_Acknowledge_Result
Time: Wed May 13 15:24:36 EDT 2009
Schema Added: E5_V20_Acknowledge_Submit.dtd from file: E5_V20_Acknowledge_Submit
Time: Wed May 13 15:24:36 EDT 2009
Schema Added: E5_V20_APIs_Result.dtd from file: E5_V20_APIs_Result
Time: Wed May 13 15:24:36 EDT 2009
```

Chapter 8. Configure Non-English Environment

Non-English Environment Checklist

You can install the Sterling Integrator in an English or a non-English environment. The base language for the Configurator can be switched only once. Use the following checklist change to a non-english environment:

#	Non-English Environment Checklist	Your Notes
1	Install the Sterling Integrator Language Pack.	
2	Load the Sterling Integrator Language Pack Factory Defaults.	
3	Load the Sterling Integrator Language Pack translators.	
4	Configure Encodings.	
5	Configure Locales.	

Language Settings

Language settings for Java applications involve both character sets and encoding:

- A character set is a set of characters (letters, numbers, and symbols such as #, $, and &) that are recognized by computer hardware and software.
- An encoding is a representation of data in a particular character set. An encoding set is a group of encodings.

For information about basic and extended encoding sets, see java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html.

The default encoding set includes:

- UTF-8 (default)
- IS0-8859-1
- ISO-8859-5
- US-ASCII
- ISO_8859-1
- EUC-JP
- UTF-16
- ISO-2022-JP

The Sterling Integrator provides two property files that contain supported encoding sets. These properties files reside in the */install_dir*/install/properties directory.

- encodings.properties – Contains the default encoding set used in the user interface.
- encodings_large.properties – Contains all supported encoding sets.

You are not limited to the encodings in the encoding.properties file. The Sterling Integrator enables you to configure the encodings properties files to expand the number of encodings you can use.

© Copyright IBM Corp. 2000, 2013

Install the Language Pack

About this task

Before installing the language pack be sure that you have successfully installed Sterling Integrator.

To install Sterling Integrator language pack:

Procedure

1. Insert the language CDs into your CD-ROM drive.
2. Navigate to the directory that is appropriate for your operating system.
   - If you are using AIX, open the AIX directory.
   - If you are using HP-UX, open the HP directory.
   - If you are using Solaris, open the Sun directory.
   - If you are using Red Hat Linux, open the Linux directory.
   - If you are using SUSE Linux, open the Linux directory.
3. Enter `./setup.bin`.

Load the Language Pack Translations

About this task

Prior to loading the Sterling Integrator Language Pack factory defaults, be sure that you have successfully completed all instructions in the database chapter.

To load the language pack translation with custom localization literals:

Procedure

1. Run the LocalizedStringReconciler tool in the IMPORT mode from the */install_dir*/install/bin directory. Enter: `./ant.sh -f localizedstringreconciler.xml import -Dsrc=/install_dir/database/FactorySetup/XMLS` This tool first inserts the value specified in the *<from_language>*_*<from_country>*_ycplocalizedstrings_*<to_language>* *<to_country>* .properties file present in the */install_dir*/database/FactorySetup/XMLS/<language>_<country> directory into the database.

   The basefilename refers to the file present in the /database/FactorySetup/XMLS directory, for which the translations are to be imported into the database.
2. Verify that your locale settings such as currency, time format, and date are correct.

Configure Encodings

About this task

To configure your encoding set:

Procedure

1. Stop the Sterling Integrator and wait for shutdown to complete.
2. Navigate to */install_dir*/install/properties.
3. Open the encodings_large.properties file.
4. Select the encodings you want to add to the encodings.properties file.

5. Open the encodings.properties.in file.
6. At the end of the encodings.properties.in file, add the encodings you selected from the encodings_large.properties file. When adding encodings from one file to the other, first copy the encodings as they appear in the encodings_large.properties file. After adding the new encodings, ensure that the index numbers are consecutive. If the index numbers are not consecutive, change the index number or numbers as needed. For example, encoding54 cannot follow encoding6. In this example, change encoding54 to encoding7.

   The first name in the definition (before the comma) is the name that will appear in the Sterling Integrator user interface. You can change this name to make it more descriptive. For example: encoding4 = 819,ISO8859_1 may be changed to encoding4 = WesternEurope,ISO8859_1. ISO8859_1 is the Java canonical name and should not be changed.
7. Update the first line in the encodings.properties.in file (numberof). Change *numberof* to the number of encodings added to the file. For example, if the current value is numberof = 6 and you add 5 new encodings, the new value is numberof = 11.

   numberof indicates the total number of encodings located in the file. You must update numberof to ensure that the encodings you added will be visible in the user interface.
8. Navigate to /*install_dir*/install/bin.
9. Enter `./setupfiles.sh`.
10. Start Sterling Integrator.

Configure Locale

About this task

The Sterling Integrator runs in any locale that Java supports. If you want to run the in a non-default locale, then configure your environment to the specific locale you want to use.

To configure locale (default is English):

Procedure

1. Enter `local-a`. A list of locales is displayed.
2. Enter `export LANG <locale>`. Where <locale> is the language, for example to set the locale to Japanese, locale = ja_JP.
3. Enter `export LC_ALL <locale>`. Some UNIX shells require the setenv command instead of the export command.

Chapter 9. User Documentation

Sterling Integrator User Documentation

The user documentation is available via an online documentation site on the Web. Providing the documentation in an online environment allows for frequent updates of content based on user feedback and usability.

We also understand the need for a printed copy of documentation. You can print topics of information using your Internet browser, or you can download documents in PDF format. You also have the option to request a documentation CD.

Access the Online Documentation

About this task

You can also access the Documentation site by opening your Internet browser and entering the following URL:

http://www.sterlingcommerce.com/Documentation/SI51/homepage.htm

After you are in the documentation library, you can:

- Enter a word or phrase and search the entire library for information.
- Move through a hierarchy of contents pages to identify the topic you want to read or print.
- Print topics by using your browser's Print function.
- Download entire documents in PDF format. To download PDF documents, click the Documentation in PDF Format link from the main online documentation page.

To access the Documentation site from within Sterling Integrator or one of its tools, select the Help  icon. The application must reside on a computer that supports Internet access and an Internet browser.

Request a Documentation CD

About this task

You can request a CD that contains all the documentation found on the Documentation site. To submit a request, go to the following URL:

http://support.sterlingcommerce.com/forms/Gentran_GIS_UpgradeRequest.aspx

© Copyright IBM Corp. 2000, 2013

Chapter 10. Install/Configure Perimeter Servers

Perimeter Server Overview

A perimeter server is an optional software tool for communications management. A perimeter server can be installed in a demilitarized zone (DMZ). A DMZ is a computer host or small network inserted as a neutral zone between a company's private network and their public network. A perimeter server requires a corresponding perimeter client.

The perimeter server manages the communications flow between outer layers of your network and the TCP-based transport adapters. A perimeter server can solve problems with network congestion, security, and scalability, especially in high-volume, Internet-gateway environments.

Installation Guidelines for Perimeter Servers with Sterling Integrator

The installation program installs a perimeter client and a local mode server. The local mode server is useful for testing purposes or in environments that do not require a secure solution. However, if you require high-volume, secure connections, you must install a perimeter server in a remote zone, either a more secure or less secure network than your integration server.

Consider the following before you install a perimeter server:

- Licensing for a perimeter server is determined by the licensing restrictions on the corresponding B2B adapters.
- Each perimeter server is limited to two TCP/IP addresses:
  - Internal interface is the TCP/IP address that the perimeter server uses to communicate with the Sterling Integrator.
  - External interface is the TCP/IP address that the perimeter server uses to communicate with trading partners. To use additional TCP/IP addresses, install additional perimeter servers.
- You can have multiple perimeter servers installed on the same computer interacting with one instance of Sterling Integrator. To install a perimeter server on a computer with an existing instance, install the new perimeter server in a different installation directory.
- The combination of internal TCP/IP address and port must be unique for all perimeter servers installed on one computer.
  - If a perimeter server is installed using the wildcard address, then all ports must be unique. The assigned ports are not available for use by adapters that use the server or any other perimeter server on that computer.
  - The internal and external interface may use the same TCP/IP address. However, the port used by the perimeter server is not available to the adapters that use the server.

Perimeter Server Installation Methods

You can install perimeter server either in silent mode or in interactive mode. The default installation mode is silent. In the silent mode, you should specify the details in a silent file, whereas in the interactive mode, you should enter the value each time a prompt appears.

© Copyright IBM Corp. 2000, 2013

Perimeter Server Information Gathering Checklist

Before you install the perimeter server, you need to gather the following information and answer the following questions:

Perimeter Server Information Gathering Checklist	Your Notes
Path to java	
Path to the Sterling Integrator installation directory	
Will this perimeter server be installed in a less secure network?	
TCP/IP address or the DNS address that the perimeter server will listen on.	
Listening port for the perimeter server.	
Local port that the perimeter server will use to connect to Sterling Integrator. Port number must be higher than 1024.	

Perimeter Server Security Vulnerabilities

When the Sterling Integrator is deployed with a remote perimeter server in a more secure network zone, there is a security vulnerability. An intruder may compromise the host where the proxy resides, and take over the persistent connection to the perimeter server residing in the more secure zone. If this happens, the perimeter server will relay all the intruder's network requests past the firewall into this internal zone.

To prevent an intrusion, limit the activities the remote perimeter server can perform on behalf of the proxy to specifically those activities that the proxy needs to do for its operation.

Control these limitations by using a configuration residing in the secure network zone with the remote perimeter server, inaccessible by the proxy that could become compromised.

Install a Perimeter Server in a More Secure Network in a UNIX or Linux Environment

About this task

Before you begin:

- Sterling Integrator 5.1 needs to be installed.
- You should have completed the Perimeter Server Information Gathering Checklist.

To install a perimeter server in a more secure network in a UNIX or Linux environment using the interactive mode:

Procedure

1. Enter: `/path_to_java/java -jar /install_dir/install/packages/ps_4500.jar –interactive`

The installation program verifies the operating system, required patch level, and the location and version of the JDK.

2. Enter the full path name for the Sterling Integrator 5.1 installation directory and press Enter.

   If there is an existing installation in the directory you specify, you can update it using the same settings. Enter yes, and installation will proceed without additional entries.
3. Enter `yes` to confirm that the installation directory is correct.

   The program verifies the amount of available disk space.
4. Is this server in a less secure network than the integration server, enter `no`.

   This installation is for a more secure network.
5. Will this perimeter server need to operate on specific network interface:
   - Enter `yes` to select from a list network interfaces available.
   - Enter `no.`
6. Enter the TCP/IP address or DNS name that the integration server will listen on for the connection from this perimeter server.
7. Enter `yes` to confirm the TCP/IP address or DNS name.
8. Enter the port that the integration server will listen on for the connection from this server. The port number must be higher than 1024.
9. Enter the local port number that the perimeter server will use for the connection to the integration server.

   The port number must be higher than 1024, except specify a port of zero if you want the operating system to select any unused port.
10. Enter `yes` to confirm the port number.

    After the installation is complete, the following messages are displayed:

    ```
    Installation of Perimeter Service is finished
    To start this Perimeter Server change to the install directory and run
    the startup script.
    You will also need to configure this server in your integration server
    (SI) UI.
    ```

Install a Perimeter Server in a Less Secure Network in a UNIX or Linux Environment

About this task

To install a perimeter server in a UNIX or Linux environment in interactive mode:

Procedure

1. Copy the ps_4500.jar installation files from the installation CD (or from another location) to a UNIX/Linux directory. If you are using FTP to copy the file, make sure your session is set to binary mode.
2. Enter: `/`*`path_to_java`*`/java -jar /`*`install_dir`*`/install/packages/ps_4500.jar –interactive`

   The program verifies the operating system, required patch level, and the location and version of the JDK.
3. Enter the full path name of the installation directory.
4. If there is an existing installation in the directory you specify, you can update it using the same settings. Answer the question:

`There is an existing install at that location, update it while keeping existing settings?`

If **yes**, the installation will proceed without additional entries.

Note: If you want to change any of the settings, you must use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that does not contain a valid installation. The existing installation must be Sterling Integrator 5.0 or later.

5. Confirm that the installation directory is correct.

   The program verifies the amount of available disk space.
6. Answer the question:

   `Is this server in a less secure network than the integration server?`

   Yes
7. Answer the question:

   `Will this server need to operate on specific network interfaces?`

   If **yes**, the program returns a list of the network interfaces available on your host. Select the interfaces for the server to use.
8. Enter the TCP/IP address or DNS name for the internal interface to use to communicate with the integration server (Sterling Integrator). Press Enter to use a wildcard for this address.
9. Verify the TCP/IP address or DNS name for the internal interface.
10. Enter the TCP/IP address or DNS name for the external interface to use to communicate with trading partners. Press Enter to use a wildcard for this address.
11. Verify the TCP/IP address or DNS name for the external interface.
12. Enter the port that the perimeter server will listen on for the connection from integration server (Sterling Integrator). The port number must be higher than 1024.
13. Verify the port.

    When the perimeter server is installed, the following message is displayed:

    `Installation of Perimeter Service is finished`
14. Change to the installation directory.
15. Enter `./startupPs.sh` to start the perimeter server.

Silent Installation Method for an External Perimeter Server

You can install an external perimeter server using a silent install file. The perimeter server can be installed on the same machine where you have installed the Sterling Integrator or on a separate machine. It is recommended to install the perimeter server on an separate machine.

To use the silent installation method, you first create the silent install file and then you use to complete the installation.

Create the Silent Installation File for an External Perimeter Server

About this task

Create a silent installation file with the following variables:

Entry	Description
INSTALL_DIR	(Required) The installation directory that stores perimeter server files and related directories. This directory must exist prior to running the silent install.
REVERSE_CONNECT	(Optional) Determines if the perimeter server is to be installed in a more secure network zone. Valid values: • Y - more secure network zone • N - less secure network zone
PS_PORT	(Required) Determines the perimeter server port to interact with the system.
PS_SECURE_IF	(Required) Determines the TCP/IP address or DNS name for the internal interface to communicate with the integration server (Sterling Integrator). You can use a wildcard (*) for this address.
PS_EXTERNAL_IF	(Required) Determines the TCP/IP address or DNS name for the external interface to communicate with the trading partners. You can use a wildcard (*) for this address.
REMOTE_ADDR	(Optional) Determines the remote perimeter server address. (Not required if REVERSE_CONNECT=N)
REMOTE_PORT	(Optional) Determines the remote perimeter server port. (Not required if REVERSE_CONNECT=N)
MAX_JVM_HEAP	(Required) Determines the maximum Java heap size allocated to the JVM.

Install an External Perimeter Server with a Silent Installation File

About this task

Before you begin, you should have already created the silent install file.

To install the external perimeter using a silent installation file:

Procedure

1. From the installation media, copy SI.jar to a UNIX/Linux directory.
2. Set up your silent installation file and record its location.
3. Navigate to your working directory.
4. To start the installation, enter:

   ```
   /absolutePath/bin/java -jar /install_dir/install/
   packages/ps_4500.jar -f silent.txt
   ```

   The installation starts. You can follow the progress of the installation on screen.

   The installation program verifies support for your operating system and JDK. It also verifies that you have enough space for the installation.

   When the installation is finished, the system displays the following message:

   ```
   Installation has completed successfully.
   ```

5. Determine if you need to apply any maintenance patches to the installation. Refer to *Installation Maintenance* to install the latest patch.

Install Patches in a Remote Perimeter Server UNIX or Linux Environment

About this task

Remote perimeter servers are not automatically updated by a service pack or patch. You must reinstall the perimeter server using the new perimeter server installation file supplied with the service pack or patch.

To update a Remote Perimeter Server:

Procedure

1. Update your installation with the latest maintenance patch. Obtain the maintenance patch file from the Sterling Commerce Support on Demand web site, at https://support.sterlingcommerce.com. These patches have a name that identifies a build number. For example, si_43_build_4307.jar. For more information, refer to the maintenance patch documentation.
2. Locate your perimeter server patch file in the */install_dir*/install/packages directory of your installation. For maintenance patches, obtain the file from the Sterling Commerce Support on Demand Web site, at https://support.sterlingcommerce.com. These patch files have a name that identifies a version number. For example, ps_2006.jar.
3. Copy the file to a directory on the remote server.
4. Stop the perimeter server, enter `./stopPs.sh`.
5. To begin the installation, enter : `/absolutePath/bin/java -jar filename.jar -interactive`

   absolutePath is the directory name where the Java version is installed.

   The program verifies the operating system, required patch level, and the location and version of the JDK.
6. Enter the full path to the installation directory. If you do not want to change any settings for your perimeter server, specify the same directory where the remote perimeter server was originally installed.
7. Answer the question:

   `There is an existing install at that location, update it while keeping existing settings?`

   If **yes**, the installation will proceed without additional entries.

   Note: If you want to change any of the settings, you must use a new directory, or delete the old installation before performing the new installation. You cannot overwrite an existing installation, and you cannot use an existing directory that does not contain a valid installation. The existing installation must be Sterling Integrator 5.0 or later.

   When the perimeter server is installed, the following message is displayed:

   `Installation of Perimeter Service is finished`
8. Change to the installation directory.
9. Enter `./startupPs.sh` to start the perimeter server.

Grant Permissions for Specific Activities for a Perimeter Server

About this task

Before you begin:

- Remote perimeter server must be installed for a more secure zone.
- Know what permissions you want to grant
- Understand the content of the restricted.policy file.The first two grant sections in the restricted.policy file are required for correct perimeter server operation. Do not modify these sections.

Procedure

1. Install a remote perimeter server, choosing the option for a more secure network zone.
2. At the installation prompt *Is this server in a less secure network than the integration server?*, select **No**, which is the option for a more secure network zone.
3. Navigate to the perimeter server installation directory.
4. Open the restricted.policy file.
5. Add permission lines for each back-end server that you intend to allow the proxy to access. There are commented out examples for each type of server.

   The first two grant sections are required for correct perimeter server operation. Do not modify these sections.

   For example, you can grant permission to a target FTP Server. In the example, servers are configured to listen on the following ports: 33001 (for FTP), 33002 (for HTTP), and 1364 (for C:D). These port numbers can be edited.

   ```
   // To restrict or permit the required Host/Server to communicate with the
   PS, update the "ftphost/htttphost/snode" with that of the Server IP and
   provide the appropriate PORT number where the Server will listen. //
    // For each target FTP Server
    // permission java.net.SocketPermission "10.117.15.87:33001", "connect"; //
    Control connection.
    // permission java.net.SocketPermission "10.117.15.87:lowPort-highPort",
   "connect"; // Passive data connections.
    // 10.117.15.87 indicates IP of the FTP Server for which the permission is
   granted by PS for communicating with client //
    // For each target HTTP Server
    //
    // permission java.net.SocketPermission "10.117.15.87:33002", "connect";
    // 10.117.15.87 indicates IP of the HTTP Server for which the permission
   is granted by PS for communicating with client //

    // For each target C:D snode
    //
    // permission java.net.SocketPermission "snode:1364", "connect";
    //  10.117.15.87 indicates IP of the Connect Direct Node for which
   the permission is granted by PS for communication //
   ```

6. In the perimeter server installation directory, there is the perimeter server settings file called remote_perimeter.properties. Edit it to change the "restricted" setting to a value of true to turn on restrictions.
7. In the future, any attempt by the perimeter server to access disallowed network resources will be rejected and logged in the perimeter server log written to the perimeter server installation directory.

Perform DNS Lookup on Remote Perimeter Server

About this task

By default, a perimeter server performs DNS lookup in the main server JVM. If you have limited DNS in your secure area, you can configure the remote perimeter server to look up trading partner addresses in the DMZ.

To enable DNS lookup to occur at the remote perimeter server, edit the remote_perimeter.properties file and change the following parameter:

Property Name	Description
<*psname*>.forceRemoteDNS	Forces resolution of DNS names at remote PS. Value is true or false.

Start Perimeter Servers in UNIX or Linux

About this task

To start a perimeter server in UNIX or Linux:

Procedure

1. Navigate to the perimeter server installation directory.
2. Enter `./startupPs.sh`.

Stop Perimeter Servers in UNIX or Linux

About this task

To stop a perimeter server in UNIX or Linux:

Procedure

1. Navigate to the perimeter server installation directory.
2. Enter `./stopPs.sh`.

Chapter 11. Uninstall the Software in a Cluster Environment

Uninstall the Sterling Integrator from a UNIX/Linux Cluster Environment

About this task

When you uninstall the Sterling Integrator, the Sterling Integrator is automatically removed from the server.

Additionally, you may perform the following tasks:

- Manually remove the JDK that was installed
- Manually remove any desktop tools that were downloaded
- Free any database space in Oracle, Microsoft SQL Server, or DB2 databases

To uninstall the Sterling Integrator from a UNIX/Linux cluster environment, perform the following procedure on each node, starting with node 1:

Procedure

1. Stop the Sterling Integrator and wait for shutdown to complete. If you begin removing files before all business processes and the Sterling Integrator are stopped, you may be unable to remove the Sterling Integrator successfully.

   To stop the Sterling Integrator, navigate to */install_dir*/install/bin and run the following command:

   ```
   ./hardstop.sh
   ```

2. Back up the file system and database.

   This step is optional. However, by backing up the file system and database, you are ensured that the Sterling Integrator is completely recoverable.

3. Remove the installation directory by entering the following command in the parent directory of your installation directory: `rm -rf install_dir`
4. If you use an Oracle, Microsoft SQL Server, or DB2 database, these remain intact even after you remove the Sterling Integrator from the server. If you no longer want to reference the data, contact your database administrator about removing unwanted tables and recovering the database space where the Sterling Integrator used to reside.
5. (Optional) To remove the JDK, review and perform the uninstall procedure for the JDK you are using.
6. After you remove the Sterling Integrator from the server, you can remove Eclipse, and any tools that were downloaded to the desktop, including the following:
   - Map Editor and associated standards

     Refer to the *Map Editor Guide* for information about removing the Map Editor.
   - Graphical Process Modeler

     Refer to the *Graphical Process Modeler Guide* for information about removing the Graphical Process Modeler.
   - Web Template Designer

© Copyright IBM Corp. 2000, 2013

Refer to the *Web Extensions Guide* for information about removing the Web Template Designer.

- (If licensed) MESA Developer Studio plug-ins, including:
  - MESA Developer Studio Software Development Kit (SDK)
  - MESA Developer Studio Skin Editor

  Refer to the *MESA Developer Studio* guide for information about removing MESA Developer Studio.
- (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.

  Refer to the *MESA Developer Studio* guide for information about removing Reporting Services.

Chapter 12. Sterling Integrator with Gentran:Server for UNIX

Gentran:Server for UNIX and Sterling Integrator Overview

Sterling Integrator has the ability to access information located in Gentran:Server for UNIX version 5.3 or 6.0. You can configure this immediately following the installation or at a later date.

By configuring Sterling Integrator to run with Gentran:Server for UNIX, you can:

- View data from your Gentran trading partners
- Start or stop Gentran:Server data managers
- View which data managers are running
- View, search, and track Gentran:Server Life Cycle event records

The following restrictions apply:

- You must have an UNIX or Linux environment
- You must be using one of the following Gentran:Server for UNIX products:
  - Gentran:Server for UNIX with Process Control Manager (PCM)
  - Gentran:Server for UNIX with EC Workbench (ECW)
  - Gentran:Server for UNIX with Advanced Data Distribution (ADD)

Install and Configure Attunity® Data Connect

About this task

If you want Sterling Integrator to use the trading partner information in your Gentran:Server for UNIX, you must install and configure Attunity Data Connect. The Attunity Data Connect software provides JDBC access to the Gentran DISAM database fields where the trading partner information is stored.

To install and configure Attunity Data Connect:

Procedure

1. Install Attunity Data Connect 3.3 or later using the installation procedures provided with the Attunity Data Connect software.
2. Ensure the Attunity Data Connect software runs as expected.
3. Create a new DISAM data source and refresh the Attunity Data Connect server. See the Attunity Data Connect documentation for the procedure.
4. Locate the following metadata description files in the */install_dir*/tp_import/gentran/disam_mapping directory:

Find this file	Replace this string $YOUR_DATASOURCE with ..	Replace this string $YOUR_GENTRAN with ..
TP_MAST.XML	the name of the data source for your Gentran:Server for UNIX system	the path to the root directory of Gentran:Server for UNIX

© Copyright IBM Corp. 2000, 2013

Find this file	Replace this string $YOUR_DATASOURCE with ..	Replace this string $YOUR_GENTRAN with ..
TRADACOM.XML	the name of the data source for your Gentran:Server for UNIX system	the path to the root directory of Gentran:Server for UNIX
ORGANIZATION.XML	the name of the data source for your Gentran:Server for UNIX system	the path to the root directory of Gentran:Server for UNIX
TP_MISC.XML	the name of the data source for your Gentran:Server for UNIX system	the path to the root directory of Gentran:Server for UNIX

5. Run the Attunity Data Connect Dictionary (ADD) Editor.
6. Select the DISAM data source you created in Step 3.
7. Import the metadata description files you updated in Step 4. See the Attunity Data Connect documentation for the procedure.
8. Verify that the metadata description files are included in the list of tables.
9. Save your changes.
10. Exit the Attunity Data Connect Dictionary (ADD) Editor.

Configure Sterling Integrator To Run with Gentran:Server for UNIX

About this task

To configure Sterling Integrator to run with Gentran:Server for UNIX:

Procedure

1. Set the umask to 002 in Sterling Integrator.
2. Is Sterling Integrator installed on a different computer than Gentran:Server for UNIX?
   - If No, then continue to Step 3.
   - If Yes, then NFS mount the $EDI_ROOT of Gentran:Server for UNIX onto the Sterling Integrator host. Continue to Step 3.
3. Verify that the remote shell (rsh or remsh) is working. If you are unable to use the rsh/rmesh shell and can only use ssh shell, change the GS_RSHELL variable located in sandbox.cfg file.
4. Navigate to */install_dir*/bin.
5. Stop the Sterling Integrator, enter `./softstop.sh`. If you are in a clustered environment, softstop suspends all the scheduled business processes. It is recommended to run a hardstop when stopping individual nodes in a cluster.
6. Enter `./configGSUnix.sh`. This command starts the configuration.
7. Press **Enter** to continue the configuration.
8. If you currently use Gentran Life Cycle and want to configure Tracking and Ops, then you need to enter the following the database information:
   - Database vendor
   - Absolute path to the JDBC drivers
   - Database user name
   - Database password
   - Database (catalog) name

- Database host name using either the IP address or name of the computer where the data base is installed
- Database port number

9. Is Gentran:Server for UNIX installed on the same computer as Sterling Integrator?
   - If Yes, enter EDI_ROOT for the local computer and continue with next step.
   - If No, enter the host name where Gentran:Server for UNIX is installed, and the EDI root where Gentran:Server for UNIX is mounted. Verify the EDI root is installed.
10. Enter the version number for Gentran:Server for UNIX.
    - Enter 1 for version 5.3.
    - Enter 2 for version 6.0.
11. If you want to configure Sterling Integrator to view Trading Partner Administration, then you need to enter the following Gentran:Server for UNIX database information:
    - Absolute path to the JDBC drivers (for example, /attunity_install_dir/java
    - Database user name
    - Database password
    - Database (catalog) name
    - Database host name where Attunity Data Connect is installed
    - Attunity port number
12. Enter `yes` and press **Enter** to continue the configuration. After the installation completed, the following message is displayed: *Deployment to the application server successful.*
13. Enter `./run.sh`.

Gentran:Server for UNIX and Sterling Integrator Migration Information

When you are migrating maps and setting up processes in Sterling Integrator from Gentran:Server for UNIX, Gentran:Server for UNIX now displays translation errors, if any, in the envelope segments and does not process the erroneous envelope segments.

Gentran:Server for UNIX 6.0 and 6.1 allowed EDI envelope segments (ISA, GS, ST, SE, GE, IEA, UNB, UNH, UNT, and UNZ) with errors to be processed successfully. This has been corrected and Gentran:Server for UNIX now issues translation errors when using X12 or EDIFACT deenvelope processes. The functional acknowledgments display the errors in the envelope segments.

The following examples illustrate scenarios where Gentran:Server for UNIX allowed successful processing of EDI segments with errors:

- Gentran:Server for UNIX did not display an error when the segment count in the UNT or SE segments did not reflect the correct count of segments in a transaction.
- Gentran:Server for UNIX did not display an error when the use of segment delimiters in the Map Input properties did not match the data. The user could not specify a delimiter in a map with multiple data files that used different delimiters. The user had to use the Syntax Record and specify the positions of the delimiters.

Chapter 13. Troubleshooting Tips

Troubleshooting Tips for Cluster Environment

Situation	Message or Symptom	Explanation/Resolution
Installing	You encounter errors or problems during installation.	**Explanation** The installation creates several log files that you can use to diagnose problems like the failure of an installation. **Resolution** Examine the log files generated during installation: • ant.install.log (in the *parent_install* directory) • */install_dir*/PreInstallSI.log • */install_dir*/InstallSI.log
Installing	When you entered an absolute path during installation, a message indicated that the command was not found.	**Explanation** You entered an incorrect path. Check the information entered. **Resolution** Enter the correct path.
Installing	The license file cannot be found.	**Explanation** • You did not obtain the license file. • The license file is corrupt. • You downloaded the license file to a PC but have not moved it to the server. **Resolution** You need to obtain the license file. If the license file resides on a PC, save the license file to the server.

© Copyright IBM Corp. 2000, 2013

Situation	Message or Symptom	Explanation/Resolution
Installing a desktop tool or resource	Cannot download any of the following: • Map Editor and associated standards • Graphical Process Modeler • Web Template Designer • (If licensed) MESA Developer Studio plug-ins, including: – MESA Developer Studio Software Development Kit (SDK) – MESA Developer Studio Skin Editor • (If licensed) Reporting Services, which requires MESA Developer Studio if you want to use the plug-ins to create fact models and custom reports.	**Explanation** When you install the Sterling Integrator, system files are created that contain an internal IP address. If you install the Sterling Integrator behind a firewall, and your firewall is configured to accept an external IP address from a client computer, you may not be able to download the desktop tools and resources. The firewall will reject the internal IP address from a client residing outside of the firewall. **Resolution** Modify the system files that contain the invalid IP address. Follow these steps: 1. Navigate to */install_dir*/install/bin. 2. Enter the following command followed by the external IP address: `./patchJNLP.sh external_IP_address` 3. Stop the Sterling Integrator. 4. Restart the Sterling Integrator.
Installing	Memory and ulimit errors.	**Explanation** The installation fails with memory and ulimit errors. **Resolution** • Refer to the *Viewing and Editing Performance Configuration Settings* in the *Performance Management* documentation. Modify your memory setting accordingly. • Refer to the *Operating System Configuration Checklist* and tune the ulimit settings.
Accessing the URL	Attempts to access the URL for Sterling Integrator display the message: Page cannot be displayed	See the information on *Changes to Network Inteface Bindings* to update either the property file or the dashboard.

Situation	Message or Symptom	Explanation/Resolution
Node status on a dual-stack machine	Displays **Node went down** status in Node Status page, but the node is up and running.	**Explanation** Sterling Integrator is configured using an IPv4 address on a dual-stack machine. The Node Status page displays Node went down status, but the node is up and running. **Resolution** Modify the noapp.properties and jgroups_cluster.properties.in files by performing the following: 1. Identify the IPv6 address of the host machine from the /etc/hosts file. 2. Navigate to the /install_dir/properties directory. 3. Edit noapp.properties.in file and add the IPv6 address: admin_host.2 = <IPv6 address> 4. Edit jgroups_cluster.properties.in and modify the following: &HOST_NAME=<IPv6 address> mcast_addr=FFFF::<IPv4 address 5. Run the ./setupfiles.sh script to apply the changes.
Installing (HP-UX 11.31)	When entering your email address the @ key is not recognized.	**Explanation** The @ key is being mapped to kill or eol, it needs to be mapped to another character. **Resolution** This resolution only applies to HP-UX 11.31. Map the @ key to another character. Note: If you need want to see what the key is mapped to, use the stty -a command.
Cluster Installation	Cluster is not working properly and your machine is running dual-stack - ipv4 and ipv6.	**Explanation** You can see the node went down from User Interface, but the node is running. **Resolution** • Find your ipv6 address in the /etc/hosts file and update noapp.properties.in file admin_host.2 = <ipv6_address>. • Edit jgroups_cluster.properties.in file and replace &HOST_NAME with the ipv6 address string and change mcast_addr=FFFF::239.255.166.17. • Enter setupfiles.sh.

Notices

This information was developed for products and services offered in the U.S.A.

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

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

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

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

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be

© Copyright IBM Corp. 2000, 2013

incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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

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

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

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

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

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

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

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2011. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2011.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

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

Product Number:

Printed in USA