Connect:Direct Enterprise Deployment Guide

Contents

Managed File Transfer enterprise deployment solution....1

Enterprise deployment overview....3
Requirements for enterprise deployment....4

Steps for planning an enterprise deployment....4
Identify the target systems....4
Create deployment groups for enterprise deployment....5
Security overview....6
Create an installation package for each group....6
Test each package....7
Deploy each group package....7

Use the Connect:Direct silent installation for enterprise deployment....7
Connect:Direct for UNIX silent installation....7
Sterling Connect:Direct for UNIX silent installation options file and command-line parameters....8
cdinstall_a script operation....18
Basic installation and configuration....18
Installing Connect:Direct for UNIX....18
Upgrading or applying a fix pack to Connect:Direct for UNIX....18
Uninstalling Connect:Direct for UNIX....19
Complete installation and configuration....19
Installing Connect:Direct for UNIX with optional files....19
Upgrading or applying a fix pack to Connect:Direct for UNIX with optional files....20
Configuring and monitoring Connect:Direct for UNIX with Control Center....20
Connect:Direct for Microsoft Windows silent installation....20
Sterling Connect:Direct for Microsoft Windows deployment options....21
Installation executable silent operation....25
Installing Connect:Direct for Microsoft Windows....25
Upgrading Connect:Direct for Microsoft Windows....26
Applying a fix pack to Connect:Direct for Microsoft Windows....26
Uninstalling Connect:Direct for Microsoft Windows....26
Configuring and monitoring Connect:Direct for Microsoft Windows with Control Center....27

Tivoli Endpoint Manager overview....27
Getting Started with the CreateTEMTasks utility....27
CTTU data file....28
CTTU properties file....28
CTTU tasks file....29
Connect:Direct for UNIX tasks file....29
Connect:Direct for Microsoft Windows tasks file....31
Sample tasks file....33
Running the CTTU....33
Running the TEM tasks....34

Connect:Direct for UNIX deployment messages....36

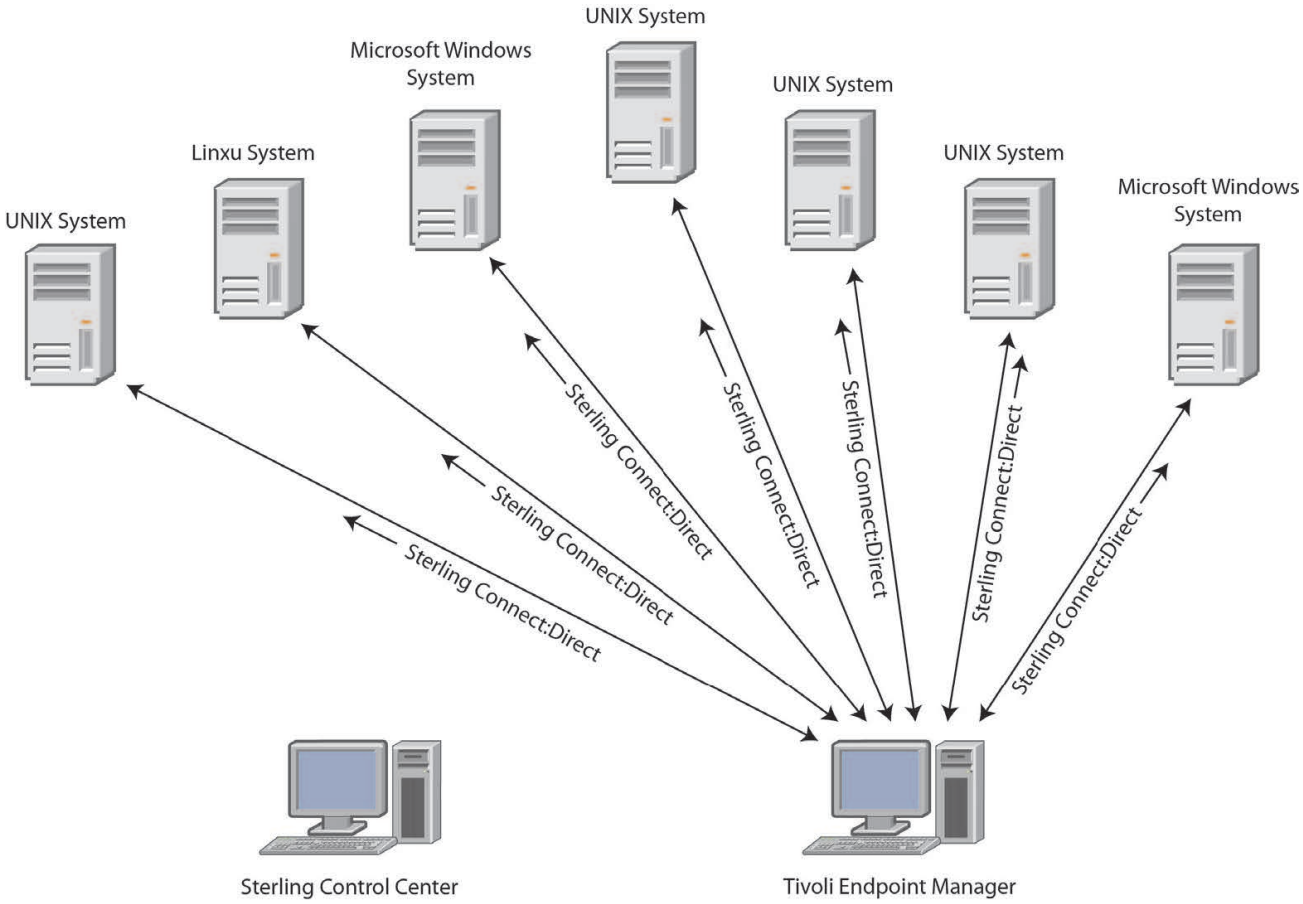
Configure new nodes in Control Center....41
Importing certificates....41

Creating server node entries..... 42

Troubleshooting..... 42

Managed File Transfer enterprise deployment solution

Deploying a Managed File Transfer (MFT) solution across your organization is a major step that you can take toward a comprehensive data movement strategy. The IBM® enterprise deployment solution helps your organization adopt a customer-centric MFT architecture to realize the full potential of an MFT solution.



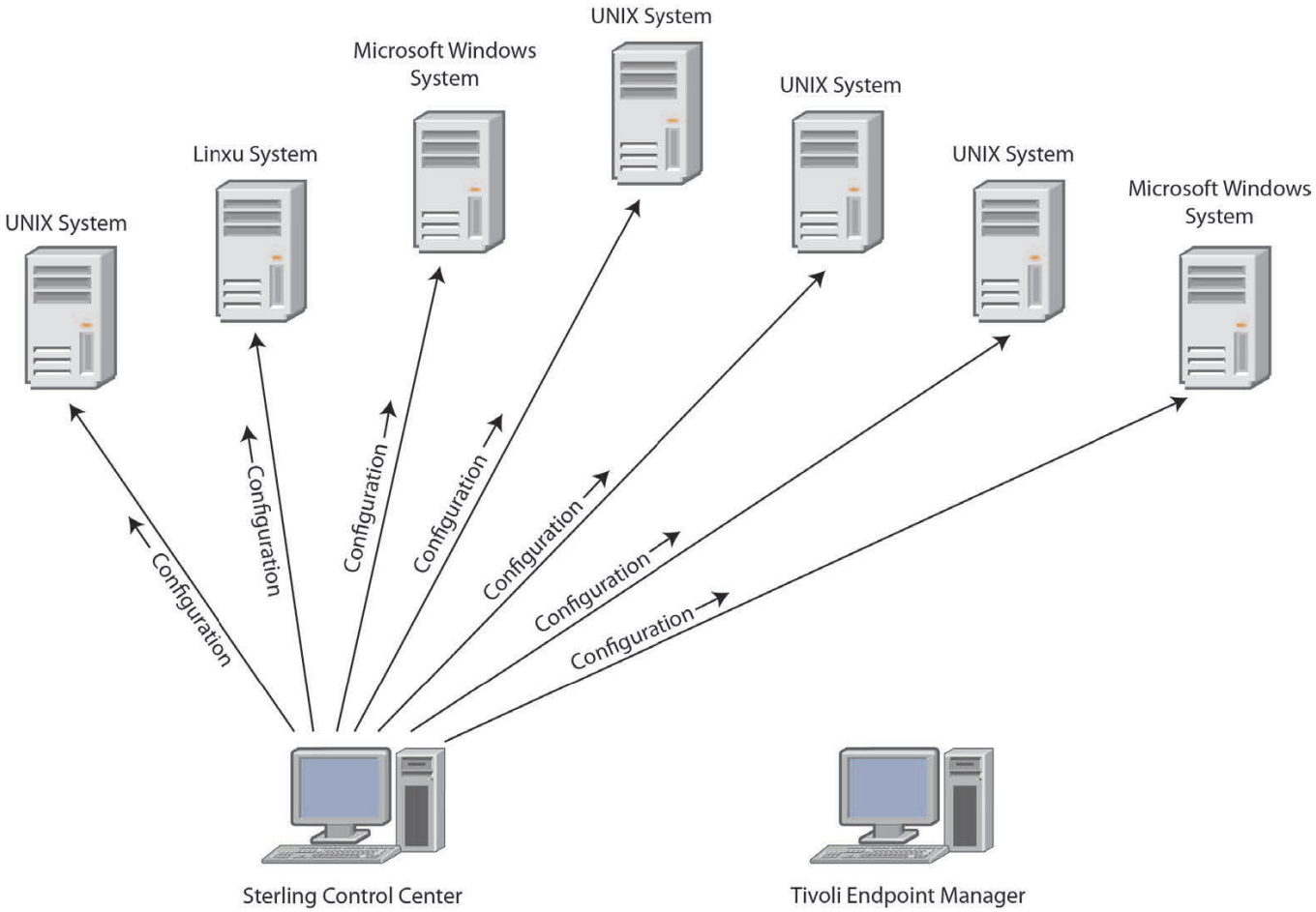
Connect:Direct

Automate the deployment of Connect:Direct® for UNIX and Connect:Direct for Microsoft Windows across your enterprise with the IBM Connect:Direct installation. Automated deployment of Connect:Direct,

coupled with the configuration and monitoring capabilities of Control Center, enables the following benefits:

- Reduced total cost of ownership
- Improved operational efficiencies
- Improved governance and auditability over the data that is being moved

Connect:Direct is point-to-point (peer-to-peer) file-based integration middleware that is meant for 24x365 unattended operation, which provides assured delivery, high-volume, and secure data exchange within and between enterprises. It is optimized for high performance and throughput. It also moves files that contain any type of data (text, EDI, binary, digital content, image) across multiple hardware types and operating systems, disparate file systems, and disparate media. It is used by many industries throughout the world to move large volumes of data and for connecting to remote offices.



Control Center

After you deploy Connect:Direct across your enterprise, use Control Center to configure and monitor your Connect:Direct nodes from a central location.

Control Center is a centralized monitoring and management system. It gives operations personnel the capability to continuously monitor business activities across the enterprise for the following server types:

- Connect:Direct
- Connect:Direct File Agent
- IBM Connect:Enterprise®
- IBM B2B Integrator
- IBM File Gateway
- IBM Connect:Express
- IBM QuickFile
- Many FTP servers

In addition, you can manage the configurations and licenses of Connect:Direct servers.

Tivoli Endpoint Manager

IBM Tivoli® Endpoint Manager delivers an easy-to-manage, quick-to-deploy solution that provides unified, real-time visibility to install, upgrade, patch, and uninstall applications, such as Connect:Direct, across all endpoints from a single console. It offers the following capabilities:

- Single intelligent agent for continuous endpoint self-assessment and policy enforcement
- Real-time visibility and control from a single management console
- Manage hundreds of thousands of endpoints regardless of location, connection type, or status. Endpoints include network-attached servers and desktops, Internet-connected notebooks, mobile devices, and specialized equipment such as point-of-sale (POS) devices, ATMs, and self-service kiosks.
- Support heterogeneous hardware and operating systems: Microsoft® Windows®, UNIX®, Linux® and Mac operating systems

Enterprise deployment overview

As the number of Connect:Direct for UNIX and Connect:Direct for Microsoft Windows installations increases, so does the time and effort that is needed for new installations and upgrades. Especially when administrators perform these operations one installation at a time.

Silent installations on individual systems

You can use an installation script for Connect:Direct for UNIX to silently and automatically install the product. The silent installation for Connect:Direct for Microsoft Windows supports enterprise deployment.

Automated installations on multiple systems

Instead of performing silent installations one system at a time, you can automate deployment on multiple systems with a single installation package. Use these installation solutions with existing software deployment systems, such as the Tivoli Endpoint Manager.

Then, you can use IBM Control Center for post-installation configuration and monitoring tasks. Although it is possible to combine installation and configuration in a single step, in this document the installation and configuration are treated as separate steps. During installation, perform the minimum configuration that is required to allow Control Center to establish a secure connection with Connect:Direct. Then, use Control Center for production configuration and subsequent configuration updates.

Another tool that you can use for post-installation and ongoing configuration management of Connect:Direct servers is the Control Center API (CCAPI). Use the CCAPI, a Java program, to programmatically create and maintain Connect:Direct server objects for large-scale efficiency.

These objects include:

- Functional authorities
- Initialization parameters
- Netmap nodes
- Netmap modes
- Netmap communication paths
- Connect:Direct Secure Plus nodes
- Connect:Direct Secure Plus key certificates
- Connect:Direct Secure Plus trusted certificates
- Connect:Direct Secure Plus cipher suites
- User proxies

Requirements for enterprise deployment

To automate the Connect:Direct deployment, your environment must meet the following requirements:

- A software deployment tool, such as IBM Tivoli Endpoint Manager, to create a deployment package and distribute it to the target systems
- A test environment to test a deployment before you deploy to your production environment
- Control Center to perform post-installation configuration (optional)

Steps for planning an enterprise deployment

To ensure a successful enterprise deployment, you can create and follow a detailed deployment plan.

To plan for an enterprise deployment, follow these steps:

1. Identify the attributes of systems where you plan to install Connect:Direct. Attributes can include operating system type and the attributes of the Connect:Direct servers, such as users and netmaps.
2. Define one or more groups of systems with common attributes.
3. Create a deployment package for each group of systems.
4. Incorporate site-specific security considerations.
5. Deploy and verify the installation package for each group on a test system with identical deployment attributes.
6. Deploy and verify each group deployment package on all systems in the group.

Identify the target systems

Take an inventory of the systems where you plan to deploy Connect:Direct.

You must identify the operating system and hardware because each platform has a different installation program that requires a unique deployment package.

Refer to the following table for an example of how you might organize attribute information.

Attribute	System 1	System 2	System 3	System 4	System 5	System 6
Owning organization	IT	IT	DEV	TEST	APPDEV	APPDEV
Hardware architecture	x86	x86	Sparc	x86	x86	x86
Operating system	Microsoft Windows	Microsoft Windows	Solaris	Linux	Linux	Linux
Ports	11363, 11364	11363, 11364	default (1363, 1364)	default (1363, 1364)	default (1363, 1364)	default (1363, 1364)
Initparm	Win-Std-Init	Win-Std-Init	Dev-Init	Test-Init	APP1_Init	APP1_Init
Netmap	Win-Std-Net	Win-Std-Net	Dev-Net	Test-Net	APP1_Net	APP1_Net
Userfile	IT-General-User	IT-General-User	Dev-User	Test-User	APP1_User	APP1_User
Xlate tables	na	na	na	na	APP1_XLATE	APP1_XLATE
Installation directory	default	default	`/development/cdu/cdu001`	`/test/cdu/test001`	`/appdev/cdu/app1`	`/appdev/cdu/app1`
Authorization type	ID and password	ID and password	Secure Point of Entry	Secure Point of Entry	Secure Point of Entry	Secure Point of Entry
Certificates	Single keycert for all nodes	Single keycert for all nodes	Single keycert for all nodes	Single keycert for all nodes	Unique keycert for each node	Unique keycert for each node
Connect:Direct administrator user ID	cdadmin	cdadmin	cdadmin	cdadmin	cdadmin	cdadmin

Create deployment groups for enterprise deployment

Group systems according to their common attributes to determine a set of systems where you can deploy a single package for each Connect:Direct node in that group. The larger the deployment group, the less work that is required to deploy to all the systems in that group.

The following table provides an example of a starting point for grouping instances of Connect:Direct with common characteristics.

Attributes	Group 1	Group 2	Group 3	Group 4
Owning organization	IT	DEV	Test	AppDev
Number of systems	2	1	1	2
Operating system	Microsoft Windows	Solaris	Linux	Linux
System architecture	x86	Sparc	x86	x86
Ports	11363, 11364	default (1363, 1364)	31363, 31364	default (1363, 1364)

Attributes	Group 1	Group 2	Group 3	Group 4
Initparm	Win-Std-Init	Dev-Init	Test-Init	APP1_Init
Netmap	Win-Std-Net	Dev-Net	Test-Net	APP1_Net
Userfile	IT-General-User	Dev-User	Test-User	APP1_User
XLATE tables	na	na	na	APP1_Xlate
Install directory	`C:\Program Files (x86)\Sterling Commerce \Connect Direct v4.6.00`	`/ development/cd u/cdu001`	`/test/cdu/ cdu001`	`/appdev/cdu/ cdu001`
Authorization type	ID and password	Secure Point of Entry	Secure Point of Entry	Secure Point of Entry
Certificates	Single keycert for all nodes	Single keycert for all nodes	Unique keycert for each node	Unique keycert for each node
Connect:Direct administrator user ID	cdadmin	cdadmin	cdadmin	cdadmin

Security overview

You must implement security and encryption to the degree appropriate for your deployment and environment. Review the following tasks that you must take to ensure a secure deployment.

You must set up the Connect:Direct administrator user ID on all target systems.

In order for Control Center to establish a secure connection with the Connect:Direct nodes after they are installed, install the nodes with a keycert. You must also configure the Secure+ .Client record to use the keycert. If you establish a secure connection from a client, you can safely complete more security configuration tasks. These configuration tasks include adding users and updating keycerts, with the Connect:Direct API. For more information, see the *IBM Sterling Control Center Getting Started Guide*.

For ease of deployment, use a single keycert for all the nodes in a group during deployment. A single keycert facilitates a secure connection so that you can use Control Center to apply production keycerts to the deployed nodes. For more information, see the *IBM Sterling Control Center Configuration Management Guide*.

CAUTION: Encrypt the keycert passphrase to keep it protected. Decrypt the keycert passphrase immediately before you install a Connect:Direct node.

Tip: If you use Tivoli Endpoint Manager for deployment, the passphrase is encrypted for you.

Create an installation package for each group

No matter which deployment tool you use, you must provide it with the files that make up a Connect:Direct silent installation.

For Connect:Direct for UNIX, the `cdinstall_a`, `cdinstall`, and `cpio` archive files are required. If you do more than a basic installation, you might also need the options file, Connect:Direct Secure Plus configuration command file, other keycerts, `initparm.cfg` file, `netmap.cfg` file, and `userfile.cfg` file. For more information, see “ Connect:Direct for UNIX silent installation” on page 7.

For Connect:Direct for Microsoft Windows, you must include the installation executable. The options `cd_srv.ini` file, keycert file, `initparm.cfg` file, `netmap.cfg` file, and `userfile.cfg` file are

optional. For more information, see “Connect:Direct for Microsoft Windows silent installation” on page 20.

Test each package

Choose a test system for installing the newly created installation package. It must have the same attributes as the systems in the group for which the package was created.

Each deployment tool has its own error report mechanism. However, you can use the return code from the Connect:Direct silent installation and the installation log to assist with troubleshooting.

Deploy each group package

After you successfully test the deployment package, you can deploy it to a group of production or test systems.

Connect:Direct for UNIX does some minimal deployment validation. For additional validation, you can use Control Center to access each Connect:Direct node by using a secure connection to do the following tasks:

- Verify that each deployed Connect:Direct node is up and running and connectable by Control Center
- Validate the initial configuration of each Connect:Direct node

For more information, see the *IBM Sterling Control Center System Administration Guide*.

Use the Connect:Direct silent installation for enterprise deployment

The following sections provide step-by-step instructions for command-line deployment of Connect:Direct for UNIX and Connect:Direct for Microsoft Windows by starting their silent installations.

Connect:Direct for UNIX silent installation

The following installation and configuration files are required for a silent installation of Connect:Direct for UNIX:

- `cdinstall_a` script
- `cdinstall` script
- `cpio` file (installation archive)
- key certificate
- Options file (unless you specify all parameters on the command line)

On the command line, you can specify parameters, such as the parameters in the following list:

- key certificate passphrase
- Connect:Direct server port
- Connect:Direct client port
- Connect:Direct administrator user ID

Refer to “Sterling Connect:Direct for UNIX silent installation options file and command-line parameters” on page 8 for a description of the options file and command-line parameters. The options file and command-line parameters are important when you do not use Control Center for configuration tasks or an enterprise deployment tool.

Attention: Command-line parameters override the settings in the options file.

The `cdinstall_a` script provides the essential installation and configuration capabilities for deploying Connect:Direct for UNIX. This script uses the `cdinstall` and `cdcust` scripts.

The `cdinstall_a` script reads the options file, command-line arguments, or both for the necessary arguments that are needed for execution. This information includes the deployment command to run: install, upgrade, or uninstall, the installation directory for Connect:Direct, the platform-specific `cpio` file, and other information.

Refer to "cdinstall_a script operation" on page 18 for a detailed description of how `cdinstall_a` operates. This information is essential if you do not use Control Center for configuration tasks or an enterprise deployment tool.

Restriction: Different UNIX and Linux operating systems have different command-line length limitations. An effective method for silent installations is to use an options file to specify your parameters instead of the command line.

The following installation and configuration files are optional for a silent installation of Connect:Direct for UNIX:

- Connect:Direct Secure Plus configuration command file (permits extended configuration of Connect:Direct Secure Plus)
- `initparm.cfg`
- `netmap.cfg`
- `userfile.cfg`
- Xlate tables (the file extension must be `.sxlt`)

  Note: The silent install requires the original pre-compiled .sxlt files to import. Re-naming an existing .xlt file to .sxlt does not work because the silent install does the compile process during the install.
- More key certificate files to use with the Connect:Direct Secure Plus configuration command line (the file extension must be `.pem`, `.cer`, or `.crt`)

Refer to the *IBM Connect:Direct for UNIX Administration Guide* for more information about `.cfg` files and xlate tables.

Refer to the *IBM Connect:Direct Secure Plus for UNIX Administration Guide* for more information about the Connect:Direct Secure Plus configuration command file and key certificate files.

Sterling Connect:Direct for UNIX silent installation options file and command-line parameters

The options file contains shell script variables. `cdinstall_a` "source includes" the options file into its execution environment so that the variables are available. However, it will do so only after it runs a security check that UNIX or Linux commands are not specified as values for the parameter variables or as individual commands. This guards against a code injection attack.

This point is important because `cdinstall_a` is started under the root account. Therefore, the administrator can run arbitrary commands without `cdinstall_a`. However, other users or applications without root privileges can initiate an automated installation. These users or applications might specify UNIX or Linux commands in the options file, which would be processed under root. This situation creates a security issue.

The following table lists and describes these variables. If you do not specify the full path of the files in the installation package, then the path defaults to the directory where `cdinstall_a` was started. For example, the path name for the `cpio` file defaults to the package directory where `cdinstall_a` is located if you do not explicitly specify a path.

Variable name	Command-line arguments	Default value	Description
cdai_installCmd=<`install	upgrade	uninstall`>	--installCmd	None. Required parameter.	Specifies the type of processing to use.
cdai_cpioFile=*<cpio file name>*	--cpioFile	cdunix	The installation `cpio` name. If it is in a different directory than the package directory, the full path must be specified.
cdai_installDir=*<target installation directory>*	--installDir	None. Required parameter.	Where to install Sterling Connect:Direct. The administrator can choose any accessible location, but the full path must be specified
cdai_localNodeName=*<Sterling Connect:Direct local name>*	--localNodeName	Host name (required for installation only).	Name to assign to the local Sterling Connect:Direct. Name is shortened to 16 characters if necessary. Specify `uname` to ensure that the host name of the system is used.
cdai_acquireHostnameOrIP=*<h | fqn | ip4 | ip6 | string>*	--acquireHostnameOrIP	*h* (required for installation only).	Specify host name, fully qualified domain name, IP v4 address, or IP v6 address. Any other strings are interpreted as IP addresses or names. • *h*=host name • *fqn*=fully qualified domain name • *ip4*=IPv4 address • *ip6*=IPv6 address String can be `0.0.0.0`, `0:0:0:0:0:0:0:0`, `::`, `192.168.0.100`, or other valid IP address.

Variable name	Command-line arguments	Default value	Description
cdai_serverPort=*<port number>*	--serverPort	1364	Sterling Connect:Direct to Sterling Connect:Direct
cdai_clientPort=*<port number>*	--clientPort	1363	CLI/API port
cdai_rpcPort=*<port number>*	--rpcPort	1367	TCP/IP port to listen for a PMGR RPC client request. Specify this port when you are engaging in silent installation over HP UX Itanium and Sun SPARC-Solaris platforms.
cdai_localCertFile=*<certfile>*	--localCertFile	None. (required for installation only).	Keycert file for Sterling Connect:Direct local node and client
cdai_localCertPassphrase=*<passphrase>*	--localCertPassphrase	None. (required for installation only).	Passphrase for keycert file
cdai_adminUserid=*<user ID>*	--adminUserid	None. (required for installation only).	System user ID to use for the Sterling Connect:Direct administrator user ID
cdai_trace=y|n	--trace	n	Enables display of debugging information

Variable name	Command-line arguments	Default value	Description

cdai_spConfig=<*file name*>	--spConfig	None.	Customized text file to update Sterling Connect:Direct parameter file as necessary. To create a parameter file, you can enter a list of commands in the spConfig text file, similarly to this example:
			`sync netmap`
			`path=/sci/silent_install/netmap.cfg`
			`name=*`
			`;`
			`Import KeyCert`
			`File="/sci/silent_install/keycert.txt"`
			`Passphrase=password`
			`Label=myKeyCert`
			`ImportMode=Add`
			`;`
			The silent install script points to this text file.
			If **cdai_spConfig** is not specified, then only basic Sterling Connect:Direct configuration is used with the key certificate and trusted root files.

Variable name	Command-line arguments	Default value	Description
cdai_ignoreExistingInstallDir=y|n	--ignoreExistingInstallDir	n	y causes cdinstall_a to ignore an existing target installation directory and proceed with the installation. n causes cdinstall_a to fail if the target installation directory exists. Use y with caution when you are engaging in automated deployment across multiple systems.

Variable name	Command-line arguments	Default value	Description
cdai_allowUmaskReset=y|n	--allowUmaskReset	y	This variable has no effect if the default umask of the adminUserid is 22 or less. If the default umask of the adminUserid is greater than 22, y causes cdinstall_a to reset the umask of the adminUserid to 22. Setting the variable to n in that case causes cdinstall_a to proceed with the more restrictive than recommended umask setting.  **CAUTION:** If the installation procedure proceeds with an umask setting that is more restrictive than the recommended value, some users might not have the necessary permissions to use Sterling Connect:Direct for UNIX.

Variable name	Command-line arguments	Default value	Description
cdai_verifyUpgrade=y|n	--verifyUpgrade	y	An upgrade command fails if pre-existing configuration files don't pass the configuration check or if the sample.cd process fails to complete successfully. This happens even when the configuration errors or sample.cd operation failure is considered tolerable. This variable allows users to choose whether to verify an upgrade or not.

Variable name	Command-line arguments	Default value	Description
cdai_trustedRootCertFile=*<trusted root file>*	--trustedRootCertFile	None.	This variable allows users to deploy a custom trusted root certificate file. If cdai_trustedRootCertFile is specified, then the automated installation arbitrarily uses this file as the trusted root certificate file. If cdai_trustedRootCertFile is not specified, then the automated installation procedure customizes and uses the default trusted root certificate file that is included in the Sterling Connect:Direct for UNIX installation file. The default trusted root certificate file is customized by adding the certificate portion of the deployed keycert file and any other deployed certificates to it. **Note:** This variable applies only to Sterling Connect:Direct for UNIX 4.1.0.

Variable name	Command-line arguments	Default value	Description
cdai_keystoreFile=<*keystore file*>	--keystoreFile	None.	If cdai_keystoreFile is specified, then the automated installation uses this file as the keystore file. If it is not specified, then the automated installation procedure uses the default keystore file that is created during the installation. In either case, the keystore file is customized by adding the certificate portion of the deployed keycert file and any other deployed certificates to it. **Note:** This variable applies only to Sterling Connect:Direct for UNIX 4.2.0 and later.
cdai_keystorePassword=<*keystore password*>	--keystorePassword	None. (always required for the installation command, but only required for the upgrade command when you are upgrading a version before Sterling Connect:Direct for UNIX 4.2.0).	Password for keystore file. Minimum 3 characters, maximum 80 characters. A keystore is created or updated with this password during the silent installation. This parameter is required if cdai_installCmd is *install* or *upgrade*. It is not required for an *uninstall*. **Note:** This variable applies only to Sterling Connect:Direct for UNIX 4.2.0 and later.

Variable name	Command-line arguments	Default value	Description
cdai_localCertLabel=*<certificate label name>*	--localCertLabel	Client-API	If cdai_localCertLabel is specified, the specification is used to label the keycert for use in basic Secure+ configurations for secure client connections. If it is not specified, the default label is used. **Note:** This variable applies only to Sterling Connect:Direct for UNIX 4.2.0 and later.
cdai_asperaLicenseFile=*<aspera license file>*	--asperaLicenseFile	None	For an installation that uses FASP, this variable allows deployment of the required license file. **Note:** This variable applies only to Sterling Connect:Direct for UNIX 4.2.0.3 and later.
cdai_installFA=y|n	--installFA	n	This variable enables file agent installation. If cdai_installFA is not specified , then file agent installation is ignored.

The following options file includes sample values for each variable:

```
cdai_trace="y"
cdai_installCmd="install"
cdai_cpioFile="/netshare/cdu/aix/cdunix"
cdai_installDir="/test/cdu/test001"
cdai_spConfig=spcmds.txt
cdai_localNodeName=uname
cdai_localNodeName=prod1.tul.company.com
cdai_acquireHostnameOrIP=ip4
cdai_serverPort=13364
cdai_clientPort=13363
cdai_localCertFile="keycert.txt"
cdai_localCertPassphrase="password"
cdai_adminUserid=kstep1
```

cdinstall_a script operation

cdinstall_a is a script that acts as a “wrapper” script for cdinstall to set up an installation environment. It also starts other installation and customization shell scripts and the following executables: cdinstall, cdcust, ndmxlt, and spcli.sh.

The command-line arguments have the same name as the parameters in the options file except the prefix cdai_ is removed. For example, the command-line argument for cdai_installCmd in the options file is --installCmd and cdai_cpioFile becomes --cpioFile.

If you specify both an options file and command-line arguments, then the command-line arguments override the corresponding values in the options file.

Restriction: Different UNIX and Linux operating systems have different command-line length limitations. The best practice for silent installations is to use an options file to specify your parameters instead of the command line.

To start cdinstall_a with an options file, use the following syntax:

```
$ cdinstall_a –f <options file>
```

To start cdinstall_a with command-line arguments, refer the following example:

```
$ cdinstall_a –-installCmd upgrade –-cpioFile <file name> --installDir <CDU install dir>
```

Basic installation and configuration

A basic installation includes only the basic installation steps with the required deployment and installation files.

Important: Log on as root before you start the cdinstall_a script. If the root password is unavailable, but root authority can be properly acquired per your company's security policies via a utility like sudo, then acquire root authority via the utility and then execute cdinstall_a script.

Installing Connect:Direct for UNIX

Complete the following procedure to perform a basic installation of Connect:Direct for UNIX:

Procedure

1. Create the options file to install Connect:Direct for UNIX.
2. Log in to the target system as root.

   Note: If the root password is unavailable, but root authority can be properly acquired per your company's security policies via a utility like sudo, then acquire root authority via the utility and then execute cdinstall_a script.
3. Make a deployment directory on the target system to stage the installation files.
4. Copy cdinstall_a, cdinstall, the cpio file, keycert file, and the options file to the deployment directory. You can put the cpio file on a network file system instead of the deployment directory.
5. Run cdinstall_a.
6. Review the log file in the deployment directory (cdaiLog.txt).

Upgrading or applying a fix pack to Connect:Direct for UNIX

Complete the following procedure to perform a basic upgrade or fix pack application of Connect:Direct for UNIX:

Procedure

1. Copy and modify the installation options file for the upgrade.
2. Log in to the target system as root.

3. Copy `cdinstall_a`, `cdinstall`, the `cpio` file, and the options file to the deployment directory. You can copy the `cpio` file to a network file system instead of the deployment directory.
4. Run `cdinstall_a`.
5. Review the log file in the deployment directory (`cdaiLog.txt`).

Uninstalling Connect:Direct for UNIX

Complete the following procedure to uninstall Connect:Direct for UNIX:

Procedure

1. Copy and modify the installation options file and copy `cdinstall_a` to the deployment directory.
2. Log in to the target system as root.
3. Run `cdinstall_a`.
4. Review the log file in the deployment directory (`cdaiLog.txt`).
5. If `cdinstall_a` fails:
   a) Stop Connect:Direct with the command-line interface (or issue `kill -9 <cdpmgr pid>`).
   b) Under the root ID, issue `rm -rf <Sterling Connect:Direct install directory>`.
6. Remove the deployment directory and contents.

Complete installation and configuration

The complete, script-only installation and configuration include the basic installation steps. Optionally, you can add any combination of more keycerts, Connect:Direct configuration files, the Connect:Direct Secure Plus configuration command file, and Xlate tables.

After installation, you can use Control Center to do more configuration of your Connect:Direct nodes. This configuration includes updating netmaps with other newly installed nodes and applying production keycerts to the deployed nodes.

Installing Connect:Direct for UNIX with optional files

Complete the following procedure for a complete, script-only installation of Connect:Direct for UNIX:

Procedure

1. Create the options file to install Connect:Direct.
2. Create one of more of the following optional files:
   - More keycert files
   - Connect:Direct `initparm.cfg`, `netmap.cfg`, or `userfile.cfg` files. You can use one or more of these files.

     Note: If the silent installation options file includes port numbers different from the port numbers that are specified in the optional `.cfg` files, the silent installation overrides the options file parameters and uses the parameters from the optional `.cfg` files.
   - Connect:Direct Secure Plus configuration command file
   - Xlate tables
3. Log in to the target server.
4. Create a deployment directory.
5. Copy the `cdinstall_a`, `cdinstall`, keycert file, `cpio` file, options file, and other files to the deployment directory. You can put the `cpio` file on a network file system instead of the deployment directory.
6. Run `cdinstall_a`.
7. Review the log file in the deployment directory (`cdaiLog.txt`).

Upgrading or applying a fix pack to Connect:Direct for UNIX with optional files

Complete the following procedure to perform a complete, script-only upgrade, or fix pack application of Connect:Direct for UNIX:

Procedure

1. Copy and modify the installation options file.
2. Log in to the target server as root.
3. Copy `cdinstall_a`, `cdinstall`, the `cpio` file, and the options file to the deployment directory. You can copy the `cpio` file to a network file system instead of the deployment directory.
4. Run `cdinstall_a`.
5. Review the log file in the deployment directory (`cdaiLog.txt`).

Configuring and monitoring Connect:Direct for UNIX with Control Center

After you deploy Connect:Direct for UNIX by any of the previous methods, use Control Center to quickly complete more configuration and to monitor the new Connect:Direct nodes. Control Center provides full functionality for configuring, monitoring, and analyzing your Connect:Direct servers.

About this task

Complete the following procedure to configure and monitor Connect:Direct nodes with Control Center.

Procedure

1. Configure secure connections from Control Center to the new Connect:Direct nodes with unique keycerts for each node. For more information, see the *IBM Sterling Control Center System Administration Guide*.
2. Perform post-deployment configuration on these nodes.
   - Add new Connect:Direct nodes to the netmaps of the existing nodes.
   - Add Connect:Direct nodes to the netmaps of new nodes.
   - Update the functional authorities on each node.
   - Update the user proxies on each node.

   For more information, see the *IBM Sterling Control Center Configuration Management Guide*.

Connect:Direct for Microsoft Windows silent installation

The installation file for a silent installation of Connect:Direct for Microsoft Windows is an executable (`.exe`).

On the command line for the installation executable, you can specify parameters, such as the parameters in the following list:

- Database password
- keycert passphrase
- Connect:Direct server port
- Connect:Direct client port
- Connect:Direct administrator user ID

For more information about the installation executable, see “Installation executable silent operation” on page 25.

The Connect:Direct server supports the use of an INI file, which can specify the value of installation properties. If you plan to use the `cd_srvr.ini` file to manage a silent installation, change the parameters of the INI file that is provided with Connect:Direct for Microsoft Windows to specify site-specific information.

You can use the Connect:Direct for Microsoft Windows Configuration Utility (CdConfig.exe) to extract and validate configuration information from an existing master node.

- To extract netmap configuration, run the following command:

```
CDConfig.exe /q /mC:\Configurations\MyNetmap.cfg
```

- To extract user configuration, run the following command:

```
CDConfig.exe /q /uC:\Configurations\MyUserAuth.cfg
```

- To extract initialization parameters, run the following command:

```
CDConfig.exe /q /pC:\Configurations\MyInitparms.cfg
```

Attention: If a parameter is defined in both the cd_srvr.ini file and on the command line, the parameter in the cd_srvr.ini file overrides the command-line parameter.

Important: Some parameters must be defined at the command line, such as ADDLOCAL, REMOVE, and INSTALLDIR.

Refer to "Sterling Connect:Direct for Microsoft Windows deployment options" on page 21 for more information about installation parameters that can be specified in the cd_srvr.ini file or on the command line. This is important when you do not use Control Center for configuration tasks or an enterprise deployment tool.

After installation, you can use Control Center to complete the configuration of your Connect:Direct nodes.

Sterling Connect:Direct for Microsoft Windows deployment options

The following table describes the installation parameters that can be specified in the cd_srvr.ini file or on the command line.

Restriction: Values in the cd_srvr.ini file are case-sensitive. Use the appropriate case when you edit the file.

Attention: Parameters that are specified on the command line do not override parameters in cd_srvr.ini. Parameters in cd_srvr.ini override parameters that are specified on the command line. It is a safe practice to specify parameters either in cd_srvr.ini or the command line but not both.

Parameter name	Default value	Description
CD_SETUP_TYPE	Default	Specify Default to perform a new installation. Specify Upgrade to upgrade releases.
CD_AGENT_PORT	1365	Specify the Agent port details here to configure the Agent listening port that Control Center Director will use to communicate with the Agent.
CD_OSA_REST_URL URL	None	Provide the Event Repository URL to configure the Control Center Director Open Server Architecture (OSA) URL, the target location where Agent posts all the events to Control Center Director.

Parameter name	Default value	Description
CD_NODENAME	First 16 characters of server name.	The name to assign to the Sterling Connect:Direct node that is installed. Limited to 16 characters and converted to uppercase.
CD_UPGRADE_NODE	First node of most recent version installed.	Applies only if `CD_SETUP_TYPE=Upgrade` is specified. Example: `CD_UPGRADE_NODE=V3.3.02\MyNode`
CD_UPGRADE_KEEPSRC_FLAG	Uninstall previous version.	Whether to keep the previous version or not during an upgrade.
CD_HOST_IP	First IP address found on the server.	Listening IP address to accept incoming Sterling Connect:Direct server connections. `0.0.0.0` means listen on all interfaces.
CD_HOST_PORT	1364	Listening port to accept incoming Sterling Connect:Direct server connections.
CD_API_IP	First IP address found on the server.	Listening IP address to accept incoming Sterling Connect:Direct client connections. `0.0.0.0` means listen on all interfaces.
CD_API_PORT	1363	Listening port to accept incoming Sterling Connect:Direct client connections.
CD_SNA_FLAG	Disabled	Specify 1 to enable SNA support.
CD_SNA_LUNAME	If already installed, previous LU name. Otherwise, first 8 characters of server name.	Translated to uppercase. Ignored if **CD_SNA_FLAG** is not set.
CD_SNA_NETID	None	Any valid string. Translated to uppercase. Ignored if **CD_SNA_FLAG** is not set.
CD_SNA_MODE	NDM624K	Any valid string. Translated to uppercase. Ignored if **CD_SNA_FLAG** is not set.
CD_SNMP_FLAG	Disabled	1 enables SNMP trap agent.

Parameter name	Default value	Description
CD_EVENTLOG_FLAG	Disabled.	1 enables Sterling Connect:Direct event logging.
CD_ACTIVEDIR_FLAG	Disabled	1 registers the client IP address to Active Directory.
CD_NOTIFY_TYPE	NT BROADCAST	NT BROADCAST or SMTP. Specifies type of process completion notification.
CD_NOTIFY_SMTP_HOST	None.	SMTP server host name or IP address.
CD_NOTIFY_SMTP_PORT	25	SMTP server port.
CD_NOTIFY_SMTP_SENDER	None.	
CD_NOTIFY_SMTP_AUTHENTICATE	Disabled	1 = enable.
CD_NOTIFY_SMTP_USERID	None.	SMTP user ID.
CD_NOTIFY_SMTP_PWD	None.	SMTP password.
CD_USERAUTH_FILE	None.	Path to user auth file to import. You can use the Sterling Connect:Direct for Microsoft Windows Configuration Utility to extract the configuration from an existing node.
CD_NETMAP_FILE	None.	Path to netmap to import. You can use the Sterling Connect:Direct for Microsoft Windows Configuration Utility to extract the configuration from an existing node.
CD_INITPARMS_FILE	None.	Path to initparms to import. You can use the Sterling Connect:Direct for Microsoft Windows Configuration Utility to extract the configuration from an existing node.
CD_DATABASE_TYPE	SOLIDDB	Use for TCQ and Statistics databases. Can specify MSSQL or MYSQL also.
CD_SOLIDDB_PORT	23460	Listening port.
CD_SOLIDDB_USERID	root	User ID for database.
CD_SOLIDDB_PWD	None.	Password.

Parameter name	Default value	Description
CD_SQL_SERVER	None	Host name or IP address of DB server.
CD_SQL_AUTHENTICATION	Disabled.	1 = enable.
CD_SQL_USERID	None.	User ID for DB.
CD_SQL_PWD	None.	Password for DB.
CD_MYSQL_HOST	LocalHost	Host name or IP address of DB server.
CD_MYSQL_PORT	1366	Listening port of DB server.
CD_MYSQL_USERID	root	User ID for DB.
CD_MYSQL_PWD	None.	Optional.
CD_SVC_ACCOUNT	None.	Name of service account, which is specified in DomainName\UserName format, to log in with.
CD_SVC_ACCOUNT_PWD	None.	Password for login service account.
CD_NETMAP_CHECK	Y	Scope of netmap checking. Y, L, R, N.
CD_NODE_CHECK	B	Method of Sterling Connect:Direct node checking. A, B, C.
CD_KEYSTORE_FILE=	cdkeystore.kdb	Specifies the file name for Secure+ KeyStore file. The file name should not include a path and will be created in the Secure+ certificates directory.
CD_KEYSTORE_PWD=password	None.	Specifies the password for Secure+ KeyStore file. The password is required when Secure+ is installed.
CD_CLIENT_CIPHERSUITES	(TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA)	List of cipher suites to enable.
CD_ADMIN_USERID	ID of user performing install.	Specify different value if you are installing under system account.

The following `cd_srvr.ini` file includes sample values for each parameter:

Restriction: Values in the `cd_srvr.ini` file are case-sensitive. Use the appropriate case when you edit the file.

```
 [Server]
CD_SETUP_TYPE=default
CD_NODENAME=CD.WINDOWS
CD_HOST_IP=0.0.0.0
CD_HOST_PORT=1364
CD_API_IP=0.0.0.0
CD_API_PORT=1363
CD_EVENTLOG_FLAG=1
CD_NOTIFY_TYPE=NT BROADCAST
CD_USERAUTH_FILE=C:\Configurations\MyUserAuth.cfg
CD_NETMAP_FILE=C:\Configurations\MyNetmap.cfg
CD_INITPARMS_FILE=C:\Configurations\MyInitparms.cfg
CD_SOLIDDB_PORT=23460
CD_SOLIDDB_USERID=root
CD_SOLIDDB_PWD=solidpasswd
CD_SVC_ACCOUNT=.\cdsvcuser
CD_SVC_ACCOUNT_PWD=syspasswd
CD_NETMAP_CHECK=Y
CD_CLIENT_KEYCERT_FILE=c:\certs\clientKeycert.pem
CD_CLIENT_KEYCERT_PWD=passwd
CD_CLIENT_CIPHERSUITES=(TLS_RSA_WITH_AES_256_CBC_SHA,
                        TLS_RSA_WITH_AES_128_CBC_SHA)
CD_ADMIN_USERID=cdadmin
```

Installation executable silent operation

There are four types of operations: Install, upgrade, apply fix pack, and uninstall.

The following example illustrates how to use the installation executable file for a new installation:

```
<Drive:\path>Setup.exe /s /v"ADDLOCAL=ALL REMOVE=Symbols
CD_SRVR_INI_FILE=\"C:\MyFiles\cd_srvr.ini\" /qn /l*vx \"C:\cdinstall.log\""
```

Tip: You can specify the `CD_SOLIDDB_PWD` in the `cd_srvr.ini` file.

The following example illustrates how to use the installation executable for an upgrade installation (`CD_SETUP_TYPE=Upgrade`):

```
<Drive:\path>Setup.exe /s /v"ADDLOCAL=ALL REMOVE=Symbols
CD_SRVR_INI_FILE=\"C:\MyFiles\cd_srvr.ini\" /qn /l*vx \"C:cdupgrade.log\""
```

Tip: You can specify the `CD_SOLIDDB_PWD` and `CD_SETUP_TYPE` in the `cd_srvr.ini` file.

The following example illustrates how to use the installation executable for a fix pack installation (`SEPATCH_ONLY_FLAG=1`):

```
<Drive:\path><Fix Pack executable> /v"SEPATCH_ONLY_FLAG=1 /qn /l*vx C:\temp\fpinstall.log" /s
```

The following example illustrates how to use the installation executable to uninstall (`/x`) Connect:Direct for Microsoft Windows.

Important: The uninstall works only with the same version of the installer executable as the instance that is being uninstalled.

```
<Drive:\path><setup.exe> /v"/qn /l*vx C:\temp\uninstall.log" /s /x
OR
<Drive:\path>< Fix Pack executable > /v"/qn /l*vx C:\temp\uninstall.log" /s /x
```

Installing Connect:Direct for Microsoft Windows

Complete the following procedure to perform a basic installation of Connect:Direct for Microsoft Windows:

Procedure

1. If needed, edit the `cd_srvr.ini` file with a text editor.

2. Log in to the target server as a Microsoft Windows administrator.
3. Create a deployment directory on the target system to stage the installation files.
4. Copy the installation executable file, `keycert` file, and `cd_srvr.ini` file (if needed) to the deployment directory. You can optionally put the installation executable file on a network share.
5. For Connect:Direct for Microsoft Windows version 4.6.0.2 or later, run the installation executable with the following syntax:

```
<Installation executable name> /v"ADDLOCAL=ALL REMOVE=SNMP,Symbols
CD_SRVR_INI_FILE=\"C:\My Files\cd_srvr.ini\" CD_SOLIDDB_PWD=<password>
/qn /l*v C:\Windows\temp\cdinstall.log\" /w /s
```

   Restriction: If you want to use the `cd_srvr.ini` file, add it to the command.
6. Review the log file (`C:\Windows\temp\cdinstall.log`).

Upgrading Connect:Direct for Microsoft Windows

Complete the following procedure to perform a basic upgrade of Connect:Direct for Microsoft Windows:

Procedure

1. If needed, copy the `cd_srvr.ini` file for the upgrade.
2. Log in to the target server.
3. Copy the installation executable file and `cd_srvr.ini` file (if needed) to the deployment directory. You can optionally put the installation executable file on a network share.
4. For Connect:Direct for Microsoft Windows version 4.6, run the installation executable with the following syntax:

```
<Installation executable name> /v"ADDLOCAL=ALL REMOVE=SNMP,Symbols CD_SETUP_TYPE=Upgrade
CD_SRVR_INI_FILE=\"C:\My Files\cd_srvr.ini\" CD_SOLIDDB_PWD=<password> /qn /l*v
C:\Windows\temp\cdinstall.log\" /w /s
```

   Restriction: If you want to use the `cd_srvr.ini` file, add it to the command.
5. Review the log file (`C:\Windows\temp\cdinstall.log`).

Applying a fix pack to Connect:Direct for Microsoft Windows

Complete the following procedure to apply a fix pack application of Connect:Direct for Microsoft Windows:

Procedure

1. Log in to the target server.
2. Copy the fix pack executable to the deployment directory

   You can optionally make the fix pack executable file available on a network share.
3. For Connect:Direct for Microsoft Windows version 4.6, run the fix pack executable with the following syntax:

```
<Fix pack executable name> /v"SEPATCH_ONLY_FLAG=1 /qn /l*v
C:\Windows\temp\cdinstall.log\" /w /s
```

4. Review the log file (`C:\Windows\temp\cdinstall.log`).

Uninstalling Connect:Direct for Microsoft Windows

Complete the following procedure to uninstall Connect:Direct for Microsoft Windows:

Procedure

1. Copy the installation executable file to the deployment directory or a network share.
2. Log in to the target system.

3. For Connect:Direct for Microsoft Windows version 4.6, run the installation executable file with the following syntax:

```
<Installation executable name> /v"/qn /lv* C:\cduninstall.log" /s /x
```

4. Review the log file.
5. Remove the deployment directory and contents.

Configuring and monitoring Connect:Direct for Microsoft Windows with Control Center

After you deploy Connect:Direct for Microsoft Windows by any of the previous methods, use Control Center to quickly complete configuration and to monitor the new Connect:Direct nodes. Control Center provides full functionality for configuring, monitoring, and analyzing your Connect:Direct servers.

About this task

Complete the following procedure to configure and monitor Connect:Direct nodes with Control Center.

Procedure

1. Configure secure connections from Control Center to the new Connect:Direct nodes. For more information, see *IBM Sterling Control Center System Administration Guide*.
2. Perform post-deployment configuration on these nodes.
   - Add new Connect:Direct nodes to the netmaps of the existing nodes.
   - Add Connect:Direct nodes to the netmaps of new nodes.
   - Update the functional authorities on each node.
   - Update the user proxies on each node.

   For more information, see *IBM Sterling Control Center Configuration Management Guide*.

Tivoli Endpoint Manager overview

You can use IBM Tivoli Endpoint Manager (TEM) to deploy Connect:Direct across computers in your enterprise. You can also use TEM to upgrade and uninstall Connect:Direct.

Requirements

If you want to use TEM to deploy, upgrade, and uninstall Connect:Direct, you must install the following software:

- IBM Tivoli Endpoint Manager Server and Console, version 9.0 or later.
- IBM Tivoli Endpoint Manager agent, version 9.0 or later, must be installed on every computer on which you want to install, upgrade, or uninstall Connect:Direct.
- CreateTEMTasks utility

Getting Started with the CreateTEMTasks utility

The CreateTEMTasks utility (CTTU) creates TEM tasks that are used by a TEM console operator to deploy, upgrade, and uninstall Connect:Direct for UNIX and Connect:Direct for Microsoft Windows across the enterprise. The CTTU also provides a TEM task to start the Connect:Direct for Microsoft Windows service.

Before you begin

The CTTU is a Java based application and requires Java Runtime Environment (JRE), version 1.6 or later.

About this task

The CTTU must use a secure connection to the TEM server. Before you can run the CTTU, you must add the TEM server public certificate to the JKS truststore used by the CTTU. You can add the certificate by using the following procedure on Microsoft Windows:

Procedure

1. Make a copy of the `cacerts` truststore file for the JRE. The truststore file is usually in the *<install directory>*`/jre/lib/security` directory of your JRE.
2. Put your copy of the `cacerts` truststore file in a directory that contains no other files.
3. Download a copy of the TEM server public certificate. If you use a Firefox browser, use the following procedure:
   a) Type the URL of the TEM server in the following format: `https://`*<TEM server address>*`:`*<TEM port>*.
   A "This Connection is Untrusted" message is displayed.

   Attention: 52311 is the default port the TEM server listens on for connections. If your TEM server is configured to listen on a different port, use that value.

   b) Click **Add Exception...**.
   The "Add Security Exception" window opens.
   c) Click **View...**
   d) Click the **Details** tab.
   e) Click **Export...**.
   f) Save the certificate.

   Tip: Alternately, you can use OpenSSL to obtain a copy of the TEM server public certificate. Issue the command: `s_client -showcerts -connect` *<server>*`:52311`, where *<server>* must be replaced with the TEM server address. Copy the certificate from the console.
4. Open a Command Prompt.
5. Use the Java keytool utility to add the certificate to your copy of the `cacerts` file with the following command:

```
keytool -import -alias tem -keystore <file pathname to cacerts copy>
-file <file pathname to TEM server public certificate> -trustcacerts
```

6. When prompted, enter the password for the truststore file. The default value is `changeit`.

CTTU data file

The CTTU utilizes two data files:

- A properties file containing connection information for the TEM server. This file usually does not change for different tasks.
- A tasks file containing one line of information, in CSV form, for each TEM task.

CTTU properties file

The CTTU properties file contains the following connection information:

- User ID to access the TEM server (**`temUserID`**)
- Password to access the TEM server (**`temPassword`**)
- The TEM server host address (**`temHost`**)
- The TEM server port (**`temPort`**)

- The file path name of the truststore that is used by the CTTU (**trustStorePathname**)
- The password for the truststore that is used by the CTTU (**trustStorePassword**)
- The file path name for the data file that contains information for the TEM tasks (**tasksPathName**)

The following sample properties file specifies connection information that is used by the CTTU to connect to a TEM server.

```
temUserID=user1
temPassword=Abc123
temHost=server01.proddomain.com
temPort=52311
trustStorePathname=c:/cacerts
trustStorePassword=changeit
tasksPathname=c:/Users/PROD_ADMIN/Desktop/TEM/data/tasks.txt
```

Attention: If any values specified contain a backslash ("\"), you must specify two of them or they are used as an escape character.

Attention: You can specify a single forward slash as a file separator character, rather than two backslashes, for both UNIX and Microsoft Windows.

CTTU tasks file

The tasks file contains one line of information, in CSV form, for each TEM task you create.

The first two values in each line must contain:

- The name of the TEM task
- The file path name to the TEM task skeleton

Subsequent values for each line depend upon the task or function to accomplish. If you distribute more files as a part of the TEM task, the path names for those files must follow the TEM task skeleton path name.

Attention: In the tasks file, blank lines and lines that begin with # are ignored by the CTTU.

Connect:Direct for UNIX tasks file

The tasks file can be used to install, upgrade, or uninstall Connect:Direct for UNIX.

Installations

For Connect:Direct for UNIX installations, specify the file path name for the `cpio` file for the third value. For the fourth value, specify the file path name for the key certificate of the installation. Specify the file path names for the `cdinstall_a` and `cdinstall` installation scripts for the fifth and sixth values. You can specify more file path names and, if you specify them, they must correspond to one of the default values for the optional installation files. For example, if you specify one or more additional file path names, use one of the following file names:

- `initparm.cfg`
- `netmap.cfg`
- `userfile.cfg`

Note: The options file is not needed with TEM deployment. The CTTU creates an options file during the installation.

Table 1. TEM tasks file parameters and sample values for Connect:Direct for UNIX installations

Position	Parameter	Sample values
1	Name of TEM task	`Install CDU AIX test 3-18`

Table 1. TEM tasks file parameters and sample values for Connect:Direct for UNIX installations (continued)		
Position	**Parameter**	**Sample values**
2	File path name to the TEM task skeleton (`cdunix-install.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdunix-install.bes`
3	File path name for the `cpio` file	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdunix`
4	File path name for the key certificate of the installation	`C:\Users\IBM_ADMIN\Desktop\TEM\ CTTU \iden_keycert.pem`
5	File path name for the `cdinstall_a` installation script	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM \cdinstall_a`
6	File path name for the `cdinstall` installation script	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM \cdinstall`
7 - n	File path name for an optional installation file	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM \netmap.cfg`

Upgrades

For Connect:Direct for UNIX upgrades, specify the file path name of the `cpio` file for the third value. Do not specify a value for the fourth value because key certificates are not used during the upgrade process. Specify the file path names for the `cdinstall_a` and `cdinstall` installation scripts for the fifth and sixth values. Do not specify more file path names.

Table 2. TEM tasks file parameters and sample values for Connect:Direct for UNIX upgrades		
Position	**Parameter**	**Sample values**
1	Name of TEM task	`Upgrade CDU AIX test 3-18`
2	File path name to the TEM task skeleton (`cdunix-upgrade.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdunix-upgrade.bes`
3	File path name for the `cpio` file	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdunix`
4	Leave the value for this parameter empty (a comma indicates an empty value)	
5	File path name for the `cdinstall_a` installation script	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM \cdinstall_a`
6	File path name for the `cdinstall` installation script	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM \cdinstall`

Uninstalls

Do not specify values for the third and fourth values for Connect:Direct for UNIX uninstalls. Specify the file path name for `cdinstall_a` for the fifth value. Do not specify more file path names.

Table 3. TEM tasks file parameters and sample values for Connect:Direct for UNIX uninstalls		
Position	**Parameter**	**Sample values**
1	Name of TEM task	`Uninstall CDU AIX test 3-18`

Table 3. TEM tasks file parameters and sample values for Connect:Direct for UNIX uninstalls (continued)		
Position	**Parameter**	**Sample values**
2	File path name to the TEM task skeleton (`cdunix-uninstall.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdunix-uninstall.bes`
3	Leave the value for this parameter empty (a comma indicates an empty value)	
4	Leave the value for this parameter empty (a comma indicates an empty value)	
5	File path name for the `cdinstall_a` installation script	`C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdinstall_a`

Connect:Direct for Microsoft Windows tasks file

The tasks file can be used to install, upgrade, apply a fix pack, or uninstall Connect:Direct for Microsoft Windows, or start the Connect:Direct for Microsoft Windows service.

Installations

For Connect:Direct for Microsoft Windows installations, specify the file path name for the installation executable for the third value. For the fourth value, specify the file path name for the key certificate file of the installation. You might, optionally, specify file path names for the following configuration files as additional values:

- `Initparms.cfg`
- `Map.cfg`
- `User.cfg`

Table 4. TEM tasks file parameters and sample values for Connect:Direct for Microsoft Windows installations		
Position	**Parameter**	**Sample values**
1	Name of TEM task	`Install CDW test 3-18`
2	File path name to the TEM task skeleton (`cdwindows-install.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-install.bes`
3	File path name for the installation executable	`C :\Users\IBM_ADMIN\Desktop\TEM\Windows\4.6.0.3-SterlingConnectDirectforMicrosoftWindows-x86-fp0003.exe`
4	File path name for the key certificate of the installation	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\iden_keycert.pem`
5 - 7	File path name for optional configuration files	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\user.cfg`

Upgrades

For Connect:Direct for Microsoft Windows upgrades, specify the file path name for the installation executable for the third value. Do not specify additional file path names.

Table 5. TEM tasks file parameters and sample values for Connect:Direct for Microsoft Windows upgrades		
Position	**Parameter**	**Sample values**
1	Name of TEM task	`Upgrade CDW test 3-18`
2	File path name to the TEM task skeleton (`cdwindows-upgrade.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-upgrade.bes`
3	File path name for the installation executable	`C:\Users\IBM_ADMIN\Desktop\TEM\Windows\4.6.0.3-SterlingConnectDirectforMicrosoftWindows-x86-fp0003.exe`

Fix packs

For Connect:Direct for Microsoft Windows fix pack applications, specify the file path name for the installation executable for the third value. Do not specify additional file path names.

Table 6. TEM tasks file parameters and sample values for Connect:Direct for Microsoft Windows fix packs		
Position	**Parameter**	**Sample values**
1	Name of TEM task	`Fixpack CDW test 3-18`
2	File path name to the TEM task skeleton (`cdwindows-fixpack_application.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-fixpack_application.bes`
3	File path name for the installation executable	`C:\Users\IBM_ADMIN\Desktop\TEM\Windows\4.6.0.3-SterlingConnectDirectforMicrosoftWindows-x86-fp0003.exe`

Uninstalls

For Connect:Direct for Microsoft Windows uninstalls, do not specify any additional values.

Table 7. TEM tasks file parameters and sample values for Connect:Direct for Microsoft Windows uninstalls		
Position	**Parameter**	**Sample values**
1	Name of TEM task	`Uninstall CDW test 3-18`
2	File path name to the TEM task skeleton (`cdwindows-uninstall.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-uninstall.bes`

Start Connect:Direct for Microsoft Windows service

To start Connect:Direct for Microsoft Windows service, do not specify any additional values.

Table 8. TEM tasks file parameters and sample values to start Connect:Direct for Microsoft Windows service		
Position	**Parameter**	**Sample values**
1	Name of TEM task	`Start CDW test 3-18`
2	File path name to the TEM task skeleton (`cdwindows-start.bes`)	`C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-start.bes`

Sample tasks file

The following sample data file contains six lines: one for each task.

```
Install CDU AIX test 3-18,C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdunix-install.bes,
C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdunix,C:\Users\IBM_ADMIN\Desktop\TEM\
CTTU\iden_keycert.pem,C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdinstall_a,C:\U
sers\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdinstall

Upgrade CDU AIX test 3-18,C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdunix-upgrade.bes,
C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdunix,,C:\Users\IBM_ADMIN\Desktop\TEM
\cdu4101\IBM\cdinstall_a,C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdinstall

Uninstall CDU AIX test 3-18,C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdunix-uninstall.
bes,,,C:\Users\IBM_ADMIN\Desktop\TEM\cdu4101\IBM\cdinstall_a

Install CDW test 3-18,C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-install.bes,C
:\Users\IBM_ADMIN\Desktop\TEM\Windows\CDWindows.4602.20130226-1853.exe,C:\Users\I
BM_ADMIN\Desktop\TEM\CTTU\iden_keycert.pem

Upgrade CDW test 3-18,C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-upgrade.bes,C
:\Users\IBM_ADMIN\Desktop\TEM\Windows\CDWindows.4602.20130226-1853.exe

Uninstall CDW test 3-18,C:\Users\IBM_ADMIN\Desktop\TEM\CTTU\cdwindows-
uninstall.bes
```

Running the CTTU

Use this information to create TEM tasks by running the CTTU.

Before you begin

When the CTTU distribution file is unarchived, the directory that is created for the CTTU contains all required `.jar` files, configuration files, and the `runCTTU.bat` or `runCTTU.sh` file. If needed, edit the `runCTTU.bat` file or `runCTTU.sh` file, and update the value for **propertiesPathname** to the file path name of your TEMTask properties file. The `runCTTU.bat` file contains the following command and parameters:

```
java -DpropertiesPathname="TEMTask.properties" -Dlog4j.configuration=file:conf\CTTU.
log4j -classpath lib\log4j-1.2.16.jar;lib\componentCommon.jar;lib\xalan.jar;lib\
commons-httpclient-3.1.jar;lib\jdom.jar;lib\com.ibm.ws.org.apache.commons.codec
.1.4_1.0.0.jar;lib\commons-logging.jar;lib\SCCenter.jar;. com.sterlingcommerce.
scc.tem.CreateTEMTasks
```

About this task

To run the CTTU, use the following procedure:

Procedure

1. Open a Command Prompt
2. Go to the directory where the `runCTTU.bat` or `runCTTU.sh` file is located
3. Type `runCTTU` (Microsoft Windows) or `runCTTU.sh` (UNIX/Linux) and press **Enter**

Results

As the CTTU creates each TEM task, it writes the task ID value to the console.

The following output is an example of what is written to the console:

```
C:\CTTU>java -DpropertiesPathname="TEMTask.properties" -Dlog4j.configuration=fil
e:conf\CTTU.log4j -classpath lib\log4j-1.2.16.jar;lib\componentCommon.jar;lib\xa
lan.jar;lib\commons-httpclient-3.1.jar;lib\jdom.jar;lib\com.ibm.ws.org.apache.co
mmons.codec.1.4_1.0.0.jar;lib\commons-logging.jar;lib\SCCenter.jar;. com.sterlin
gcommerce.scc.tem.CreateTEMTasks
Tue Apr 16 10:22:57 CDT 2013  Create TEM Tasks Utility beginning...
Tue Apr 16 10:22:58 CDT 2013  Adding files for Task ~Install CDW test 1
```

```
Tue Apr 16 10:22:58 CDT 2013  Initiating upload of the following file to TEM: C:
\CDWin4603\CDWindows\CDWindows.4602.20130327-0943.exe
Tue Apr 16 10:23:51 CDT 2013  File uploaded successfully.
Tue Apr 16 10:23:51 CDT 2013  Initiating upload of the following file to TEM: C:
\CDWin4603\CDWindows\user1_1024_fips_keycert.txt
Tue Apr 16 10:23:51 CDT 2013  File uploaded successfully.
Tue Apr 16 10:23:51 CDT 2013  Adding Task ~Install CDW test 1 to TEM server...
Tue Apr 16 10:23:52 CDT 2013  Task added successfully - id = 90
```

Running the TEM tasks

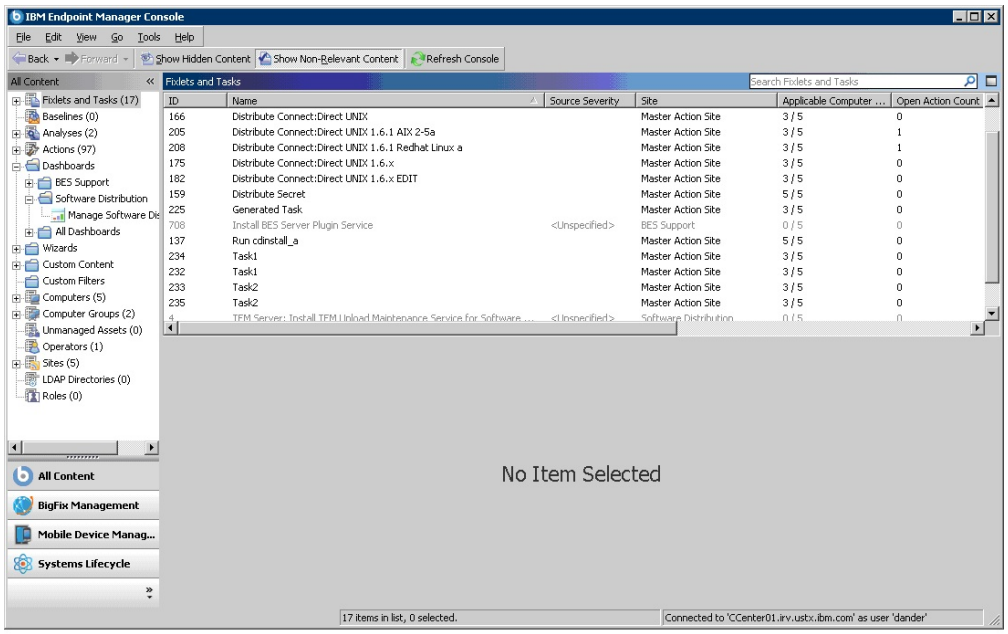
After the CTTU creates the TEM tasks, use the TEM console to run the TEM tasks. These tasks can install, upgrade, apply a fix pack, or uninstall Connect:Direct, or start the Connect:Direct service on systems that contain the TEM client.

About this task

Use the following procedure to run the TEM tasks:

Procedure

1. Start the TEM console.



2. Click the **All Content** domain button that is located beneath the **Domain Panel**.
3. Select **Fixlets and Tasks** in the **Domain Panel**.

   The **List Panel** displays a list of relevant fixlets and tasks. This is where tasks created by the CTTU appear.

   Attention: Tasks that are created by the CTTU are added to the **Master Action Site**.

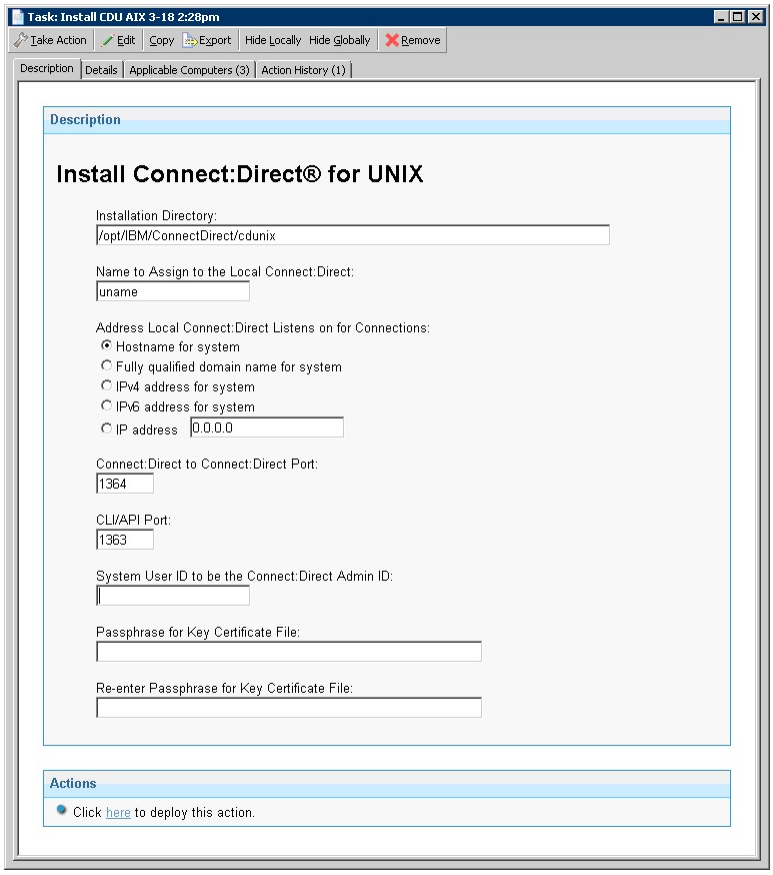
   Attention: If you do not select **Show Non-Relevant Content**, the tasks that are created by the CTTU do not appear in the list until they are determined relevant for one or more of the computers that are managed by TEM. There might be a delay before tasks are determined relevant for all systems.

Attention: You might see multiple tasks that are created with the same name. You can add the ID column to the display and sort the tasks by ID to find specific tasks.

4. Select a specific task.

   A **Task** window displays.

   Attention: The task that is displayed in the **Task** window depends on the selected task. In the following figure, the user selected the TEM task to perform Connect:Direct for UNIX installations.

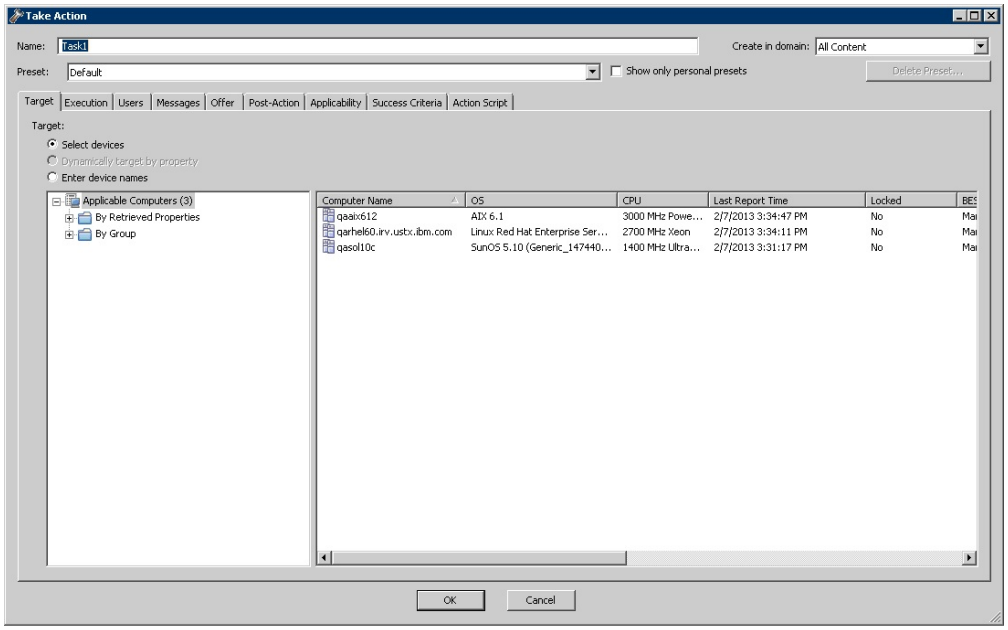


5. On the **Description** tab, enter the appropriate values for your task. For example, to install Connect:Direct for UNIX, enter the following values:

   - **Installation Directory:** the directory where you want to install Connect:Direct
   - **Name to Assign to the Local Connect:Direct:** The name can include up to 16 characters. If you specify uname, the host name of the server where Connect:Direct is installed is used for the name.
   - **Address Local Connect:Direct Listens on for Connections:** Select one of the following options to determine the address the local Connect:Direct listens on:
     - **Hostname for system**
     - **Fully qualified domain name for system**
     - **IPv4 address for system**
     - **IPv6 address for system**
     - Specify **IP address** for system
   - **Connect:Direct to Connect:Direct Port:** port that is used for Connect:Direct to Connect:Direct communications.
   - **CLI/API Port:** port that is used for client connections.
   - **System User ID to be the Connect:Direct Admin ID:** the system User ID that is used for the Connect:Direct administration ID.

- **Passphrase for Key Certificate File:**

6. Click **here** to deploy the task.
   The **Take Action** window displays.



   Initially, the **Take Action** window displays all relevant computers. In the previous figure, the task makes all UNIX and Linux computers with a compatible TEM client relevant.

7. Select the computers for this task.

   Attention: If the task is a UNIX installation, you must select the computers from the list that are compatible with the CPIO file associated with the task. The task relevance ensures only that UNIX and Linux servers are relevant. It does not ensure that only systems appropriate for the CPIO file to be deployed are relevant.

8. You can select any other execution options in other tabs, such as when to schedule the action on the **Execution** tab.
9. Click **OK** to initiate the task.

Connect:Direct for UNIX deployment messages

There are two types of messages that are shown in the following tables. The first table contains informational messages. The second table contains error messages in addition to comments about correcting the error.

These messages are written to the log file named `cdaiLog.txt`, in the deployment directory. A file named `exitStatusFile.txt` contains the completion message ID and descriptive text from the `cdinstall_a` installation in addition to other information.

The following table contains `cdinstall_a` informational messages:

Message ID	Message text
CDAI000I	Connect:Direct for UNIX automated installation operation started.
CDAI001I	Connect:Direct automated installation completed.

Message ID	Message text
CDAI010I	Debug message. Actual message text is supplied on logging call.
CDAI011I	Start of display of variables from options file.
CDAI012I	End of display of variables from options file.
CDAI013I	Backup of current installation started.
CDAI014I	Backup of current installation completed.
CDAI015I	Restore of current installation started.
CDAI016I	Restore of current installation completed.
CDAI017I	Connect:Direct successfully uninstalled.
CDAI018I	Performing writable installation.
CDAI019I	Performing upgrade installation.
CDAI020I	Performing uninstall.
CDAI021I	Configuring Secure+.
CDAI022I	Verifying installation.
CDAI023I	Copying deployment directory contents to writable directory.
CDAI024I	Copying deployment directory complete.
CDAI025I	Execution started in writable deployment directory.
CDAI026I	Execution completed in writable deployment directory.
CDAI027I	Copying output files from writable deployment directory.
CDAI028I	Start of log records from writable deployment directory.
CDAI029I	Building xlate tables started.
CDAI030I	Building xlate tables completed.
CDAI031I	Start of display of environment info.
CDAI032I	End of display of environment info.
CDAI033I	cdinstall_a exiting.
CDAI034I	Connect:Direct for UNIX failed to start.
CDAI035I	Extracting admin userid from idInfoFile.
CDAI036I	Extracting local node name from idInfoFile.
CDAI037I	Admin userid determined. Override ignored.
CDAI038I	Local node determined. Override ignored.
CDAI039I	Options File.
CDAI040I	Resolved Variables.
CDAI041I	Variables Used During:

Message ID	Message text
CDAI042I	Copied configuration files. Verifying installation again.

The following table contains cdinstall_a error messages:

Message ID	Message text	Comments
CDAI000E	usage: cdinstall_a [-f <options file>] [cmd line args]	Check spelling/syntax in options file and/or command-line arguments.
CDAI001E	Connect:Direct automated installation failed.	Check other error messages that describe the specific error.
CDAI002E	Invalid argument found.	Check spelling/syntax in options file and/or command-line arguments.
CDAI003E	Options file parameter not specified.	Required options file or command-line parameter was not specified.
CDAI004E	Options file does not exist.	Check spelling, path, etc.
CDAI005E	Base installation and configuration failed.	Check other error messages that describe the specific error.
CDAI006E	Setting root attributes failed.	Connect:Direct installation directory might not be on local file system.
CDAI007E	Secure+ configuration failed.	Check Connect:Direct Secure Plus error messages.
CDAI008E	Must not install under root id.	
CDAI009E	Backup of current installation failed.	Check other error messages that describe the specific error.
CDAI010E	Restore of current installation failed.	Check other error messages that describe the specific error.
CDAI011E	Executable code not allowed as value for variable.	Cannot specify option file parameters that are enclosed in ` characters or for Linux, use the `$(...)` expression. These notations would allow injection of arbitrary UNIX and Linux commands.
CDAI012E	cdinstall_a must run under root id.	Log in under root before you run `cdinstall_a`.
CDAI013E	Invalid admin userid.	The admin user ID is not a defined user ID.

Message ID	Message text	Comments
CDAI014E	Could not copy certificates to Secure+ certificates directory.	Make sure that certificates are readable and the installation directory and Connect:Direct Secure Plus subdirectorys are writable.
CDAI015E	Upgrade installation and configuration failed.	Check other error messages that describe the specific error.
CDAI016E	No keycert for S+ install.	`cdai_localCertFile` must be specified.
CDAI017E	Restore of installation directory failed.	Check other error messages that describe the specific error.
CDAI018E	File does not exist or is unreadable.	Make sure that the file in question is available or readable.
CDAI019E	Install directory should not exist for new install.	The admin specified `cdai_installCmd="install"` but the Connect:Direct installation directory exists. Change the directory name or change the command to `upgrade` or `uninstall` as appropriate.
CDAI020E	Shutdown of Connect:Direct failed.	Check other error messages that describe the specific error.
CDAI021E	Connect:Direct not installed. Cannot uninstall.	Check installation directory spelling.
CDAI022E	Connect:Direct installation verification failed.	Check the `cdaiLog.txt` file for other errors. View the Connect:Direct statistics for other clues.
CDAI023E	Error building xlate tables.	Check syntax of Xlate tables in question.
CDAI024E	Copying log/output files to work subdirectory failed.	Verify permissions are correct.
CDAI025E	cdinstall_a exiting with error.	Check other error messages that describe the specific error.
CDAI026E	Deletion of C:D installation directory failed.	Check permissions on directory.
CDAI027E	Invalid parameter in options file or on command line.	Correct the spelling and/or syntax.
CDAI028E	Install cmd specified but C:D already installed.	Change command to `upgrade` or `uninstall` if either is the intended action.
CDAI029E	Upgrade cmd specified but C:D is not installed.	Change **`cdai_installCmd`** to `install` and rerun.

Message ID	Message text	Comments
CDAI030E	Uninstall cmd specified but C:D is not installed.	Nothing left to do.
CDAI031E	IAcquiring net info failed. ip4|6: link addresses defined?	Correct spelling/syntax errors in **cdai_acquireHostnameOrIP** parameter value.
CDAI032E	Passphrase missing for keycert.	Specify cdai_localCertPassphrase.
CDAI033E	No cmd line arguments specified.	Specify an options file or the minimum required individual command-line arguments that are needed for the command that is being run.
CDAI034E	Connect:Direct for UNIX failed to start.	Check other log errors. View Connect:Direct statistics records.
CDAI035E	mkdir failed for directory:	Check spelling.
CDAI036E	Invalid exit code returned. cmd=	Report
CDAI037E	idInfoFile.txt missing. setting cdadmin to dir owner id.	Can occur if you are upgrading a Connect:Direct installation that is not originally installed with the automated installation mechanism.
CDAI038E	No cdadmin userid in id file. Trying alternate settings.	Can occur if you are upgrading a Connect:Direct installation that is not originally installed with the automated installation mechanism.
CDAI039E	No local node name. Trying alternate settings.	Can occur if you are upgrading a Connect:Direct installation that is not originally installed with the automated installation mechanism.
CDAI040E	No cdamind userid.. Trying alternate settings.	Can occur if you are upgrading a Connect:Direct installation that is not originally installed with the automated installation mechanism.
CDAI041E	Local node name not specified.	Specify cdai_localNodeName.
CDAI042E	Invalid local node name specified.	Specify cdai_localNodeName correctly.
CDAI043E	Not a valid text file. Trying Win2unix conversion. File:	A possible Microsoft Windows text file was detected (for example, initparm.cfg). Converting to UNIX text format.
CDAI044E	Win2unix text conversion failed. File:	Text file still incorrect after you convert to UNIX text format.

Message ID	Message text	Comments
CDAI045E	cdamind userid cannot read/write into install directory.	User ID cdadmin not allowed to create/write into Connect:Direct installation directory. Choose a different directory for installation.
CDAI046E	No usable IPv6 address configured.	IPv6 addressing was selected but the system has no IPv6 addresses configured. Try IPv4 addresses instead.
CDAI047E	Upgrade installation and configuration of Secure+ failed.	Check the `cdaiLog.txt` log file for more information.
CDAI048E	Invalid characters found in local node name.	Specify a Connect:Direct node name with correct characters.
CDAI049E	C:D config file copy to cfg/<nodename> directory failed.	Check permissions on the config files and view `cdaiLog.txt` for more information about the error.

Configure new nodes in Control Center

After you deploy your Connect:Direct servers, you can use Control Center to complete more configuration tasks and to monitor those servers.

There are two tasks you must complete so that Control Center can securely communicate with Connect:Direct servers.

1. Import root certificates from each Connect:Direct server into the Control Center truststore file.
2. Create new Control Center node entries with connection information for each Connect:Direct node.

Importing certificates

Complete the following procedure to import root certificates from a Connect:Direct server into the Control Center truststore:

Procedure

1. Locate the existing Control Center truststore or create a new one.

   Note: If you create a truststore, use the `configCC.bat` or shell script to configure Control Center to use it.
2. Create a truststore file that contains CA information in JKS format on the Control Center engine.
3. If a truststore file in JKS format is not available, use the default truststore file (`cacerts`) in the *<Sterling Control Center installation directory>*`/jre/lib/security` directory. This truststore file contains authentication information for most CAs.
4. Import the root certificate of the Connect:Direct server into the truststore on the Control Center engine. Use the **Import to Trust Store** feature of IBM Certificate Wizard.
5. Configure the Control Center engine for a secure connection.

   For more information about creating a truststore, see the *Configure a Secure Connection* section of the *IBM Sterling Control Center Getting Started Guide*.

Creating server node entries

Complete the following procedure to create Connect:Direct node entries:

Procedure

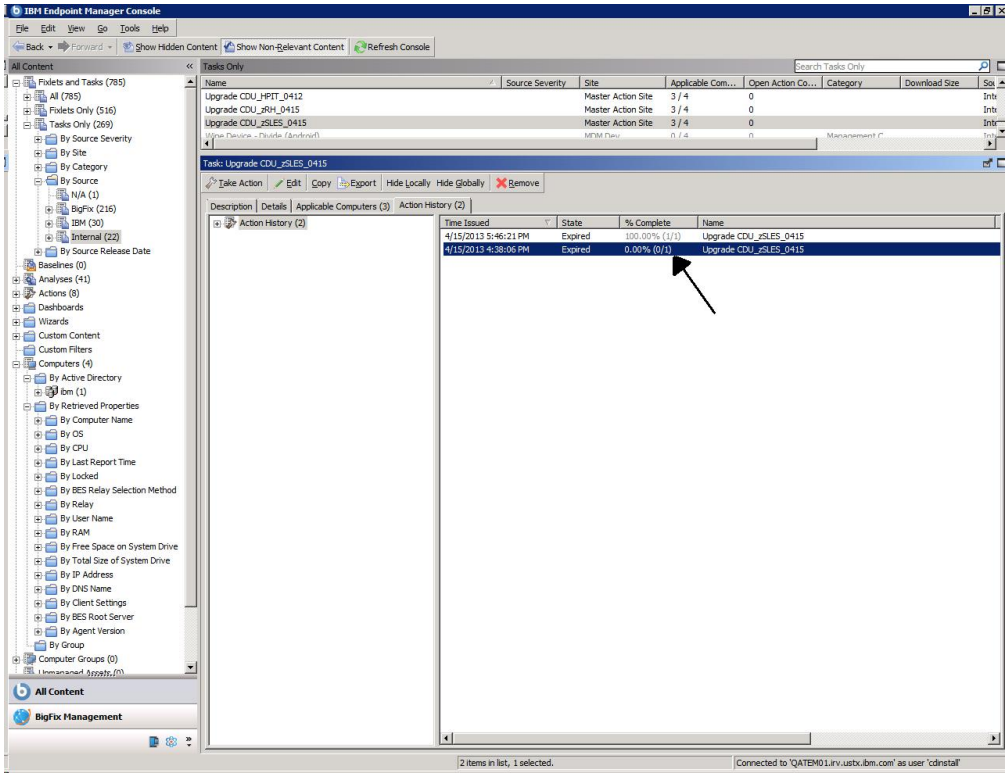
1. Start the Control Center console.
2. Select **Manage** > **Add Server**. The **Add Server** wizard displays.
3. Type the server name or alias and an optional description.
4. Click **Next**.
5. Select the server type **Connect:Direct with TCP/IP API**.
6. Complete the requested information on the **Connection** page of the **Add Server** wizard for Connect:Direct servers.
7. Optionally, add this server to a server group by selecting a group name in **Groups** and moving it to **Selected Groups** by clicking **>**.

Troubleshooting

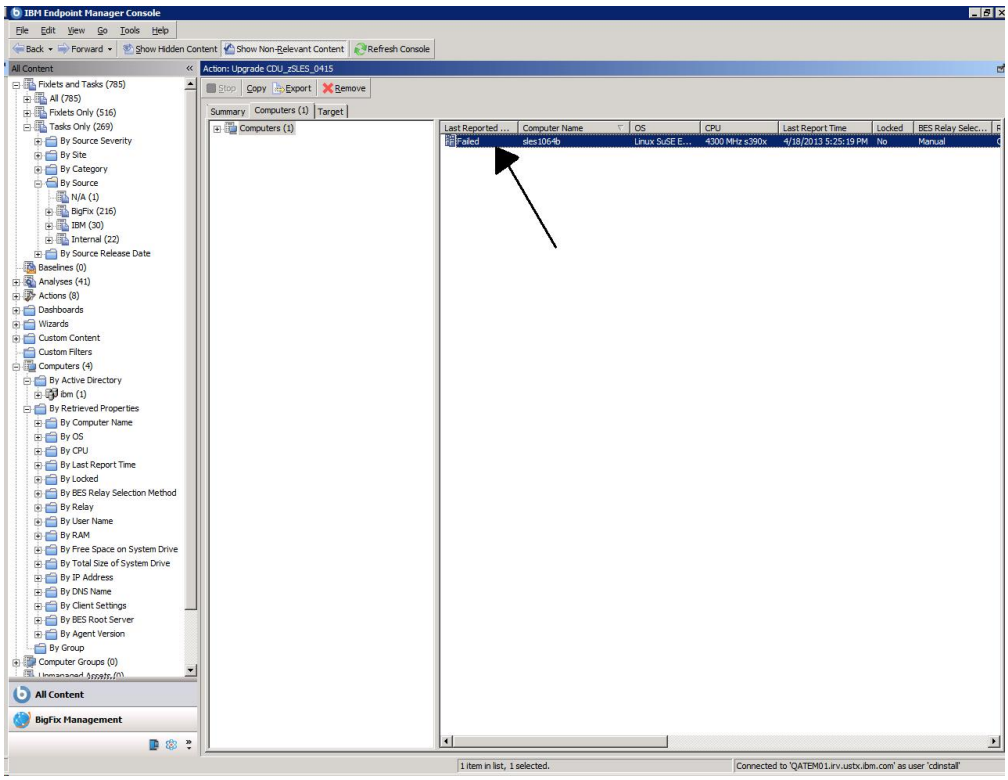
If a Connect:Direct installation fails when you use TEM, diagnose the problem from the TEM server console.

Procedure

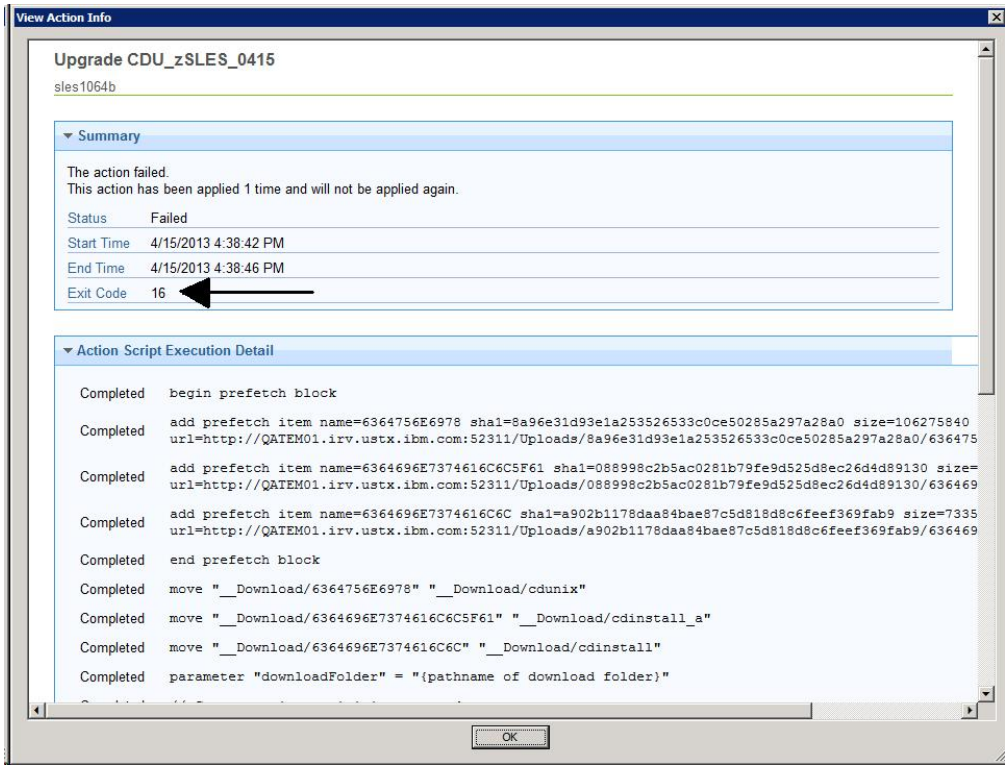
1. Start the TEM console.
2. Click the **All Content** domain button that is located beneath the **Domain** Panel.
3. Select **Fixlets and Tasks** > **Tasks Only** > **Internal** and find the specific task that failed.



4. Double-click the failed task to open the Action **Summary**.
5. Select the **Computers** tab and locate the failed action information.



6. Double-click the failed action report. A **View Action** window opens with detailed information about the task.
7. Locate the **Exit Code**.



8. Match the **Exit Code** with the Connect:Direct message ID for enterprise deployment. Refer to the deployment messages in this document.

   For example, if the **Exit Code** is 16, the **Exit Code** for Connect:Direct for UNIX is `CDAI016E - No keycert for S+ install.`