IBM Connect:Direct Web Services 6.1

Documentation

This edition applies to Version 5 Release 3 of IBM® Connect:Direct and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Release Notes

The IBM® Connect:Direct® Web Service Release Notes document supplements IBM Connect:Direct Web Service documentation. Release notes are updated with each release of the product and contains product requirements, as well as other information pertinent to installing and implementing Connect:Direct Web Services.

New Features and Enhancements

Connect:Direct Web Services and its related software have the following features and enhancements:

FixPack 4 (v6.1.0.4)

New Features and Enhancements
To install this software, you should go to the Fix Central website and install the latest available fix pack. • With this release, web console has following enhancements: – You have access to human readable certificate to ease troubleshooting. – Name and path of currently used Keystore and Truststore will be visible. • Keystore/Truststore password encryption key will be generated automatically. For more information, refer “Changing Keystore/Truststore using Web Console” on page 45. • Support for different Keystore and Key Certificate passwords is extended. • IBM Connect:Direct Web Service support is extended for configurable **Password Exit**. For more information refer to, Connect:Direct Windows Release Notes for Fix Pack 2 (6.1.0.2).

FixPack 3 (v6.1.0.3)

New Features and Enhancements

To install this software, you should go to the Fix Central website and install the latest available fix pack.

- The `log4j.properties` file is changed to `log4j2.yaml` file. For more information, refer "Configuring Logs" on page 54.
- IBM Connect:Direct Web Service support is extended for Connect:Direct Windows users to configure:
  - **Allow No-Password Local Connections** and **Allow Process to run using Service Account** in Functional Authority.
    - Navigate to **Settings** > **Users** > **Create New Functional Authority** > **Authentication (Settings)** > to configure these properties.
  - **Allow Process to run using Service Account** in User Proxy.
    - Navigate to **Settings** > **Users** > **Create New Remote User Id** > **Process Permissions** > to configure this property.

    For more information, refer Connect:Direct for Windows(v6.1.0) Release Notes.
- IBM Connect:Direct Web Service support is extended for Connect:Direct Windows and Unix users to configure Install Agent properties for installing new Connect:Direct servers from IBM Control Center Director:
  - Navigate to **Settings** > **Initialization Parameter**:
    - Install Agent
    - License Information

    For more information, refer Connect:Direct for Windows (Fix Pack 1 v6.1.0.1) and Connect:Direct for UNIX(Fix Pack 1 v6.1.0.1) Release Notes.

FixPack 2 (v6.1.0.2)

New Features and Enhancements

Connect:Direct Web Services 6.1.0.2 has the following features and enhancements. To install this software, you should go to the Fix Central website and install the latest available fix pack.

- The Java version is upgraded to 8.0.6.10.
- With this fix pack, support to Windows server 2019 is added. For more information, see "Minimum Hardware and Software Requirements" on page 4.

FixPack 1 (v6.1.0.1)

New Features and Enhancements

Connect:Direct Web Services 6.1.0.1 has the following features and enhancements. To install this software, you should go to the Fix Central website and install the latest available fix pack.

- **Connect:Direct Web Services support extended for Connect:Direct UNIX and Windows users to cache certificate validation responses from External Authentication Server**

  With this fix pack Connect:Direct UNIX and Windows can be configured via IBM Connect:Direct Web Service to cache certificate validation responses from External Authentication Server when it interfaces External Authentication Server during a TLS session. This option is available under Web Console using any of the following UI paths:

  – **Settings >Secure + > Local Records> .SEAServer> View details/Edit**> **Caching Details** to modify caching SEAS certificate validation response settings for the External Authenticator.

  – **Settings >Secure + > Secure Partners** file menu option. Select a External Authenticator node entry and click **Edit** to modify caching SEAS certificate validation response settings.

    For more details see the following resources:

    - Connect:Direct for Windows v6.1.0 Release Notes
    - Connect:Direct for UNIX v6.1.0 Release Notes

- **Partner security settings extended to include TLS 1.3 protocol support**

  Connect:Direct Secure Plus for Windows, UNIX, and z/OS extended its security settings to include TLS 1.3 protocol support with v6.1. With this fix pack, **IBM Connect:Direct Web Service** partner security settings have been extended to include TLS 1.3 protocol support to ensure secure data transfer between the PNODE and SNODE.

  – To configure security settings and enable TLS 1.3 protocol, click **Partners> Add Partners>Add Partner Details** to display **Add new Partner** form.

  – From the **Security** drop-down list, select **Custom Security** to view **Custom Security Type** form. To enable TLS 1.3 go to **Select Security Protocol>TLS 1.3**.

  – **Cipher Suites** is also updated to display TLS 1.3 supported cipher suites.

- **Upgrade support available on Solaris SPARC 10 platform**

  With this Fix Pack, upgrade support is available for IBM Connect:Direct Web Service users upgrading from v6.0.0.X to v6.1.0.1 on Solaris SPARC 10 platform.

Base Release (v6.1)

New Features and Enhancements

Connect:Direct Web Services 6.1 has the following features and enhancements:

- **Web Console support now available for Connect:Direct for z/OS users**

  Connect:Direct Web Services now extends support for Web Console to Connect:Direct users signed in from Connect:Direct for z/OS. z/OS users can also continue to access Web Services via. its RESTful API interface.

- **Connect:Direct Secure Plus support**

  Support added to configure and maintain Connect:Direct Secure Plus environment. IBM Connect:Direct Secure Plus for UNIX, Windows and z/OS provide enhances security for Connect:Direct using cryptography to secure data during transmission. This option is available under Web Console> **Settings >Secure + > Secure Partners** file menu option.

  The following Connect:Direct Secure Plus functionalities are available via Connect:Direct Web Console:

  – View, modify, delete, and create an Alias for Secure Plus .Local, .SEAServer, Remote node records.

  – Support introduced to filter node records basis security configuration. This option is available under **Secure Partners**>**Filters**.

- **Web Console support available to manage Keystore/Truststore**

  With v6.1, IBM Connect:Direct Web Service now extends its web console capabilities to:

  – support import and export of base64-encoded ASCII certificates into an existing Keystore/Trust Store. For more information see, "Add/Import a certificate(s) to IBM Connect:Direct Web Service Keystore/Trust Store" on page 46

  – configure IBM Connect:Direct Web Service to use a different Keystore/Truststore For more information see, "Changing Keystore/Truststore using Web Console" on page 45

  For a UI walk-through on these new Web Console capabilities see, YouTube> IBM Connect:Direct.

- **Detailed certificate view available under Certificate tab**

  With v6.1 **Certificate** tab is enhanced for Connect:Direct Web Services users to display certificate attributes in a summary, detailed, and tree navigational view. This option is available Web Services users under **Settings**>**Secure+**>**Certificates**>**Key Certificates** or **Trusted Certificates**.

  With v6.1 **Certificate** tab is now available for Web Services Administrator to display certificate attributes in a summary, detailed, and tree navigational view. This option is available to Admin user under **Certificates**>**Key Certificates** or **Trusted Certificates**.

- **Enhanced Statistics view**

  Filtered searches in the **Statistics** view can result in a large number of entries being returned, possibly even all entries. Setting a search limits improve overall server performance by limiting how many entries are returned. With this release Connect:Direct Web Services administrators can set search limit by modifying the `statistics.search.limit` property. For more information see, "Configuring application.properties" on page 50.

  Statistics view displays data in local time while the Swagger UI displays all statistics data in UTC format, by default, unless time zone is offset if provided from the Swagger UI.

  Note: Statistics view displays transfer activity statistics showing results narrowed to the past 15 minutes.

Minimum Hardware and Software Requirements

IBM Connect:Direct Web Service and its related software require the following hardware and software. For detailed Software Product Compatibility Reports for Connect:Direct Web Services see, https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.

Table 1.	
Hardware	**Software**
For a **UNIX** operating system: • **RAM (min.)** - 4 GB • **Disk Space (min.)** - 250 GB	IBM Connect:Direct Web Service can be installed on the following 64-bit Operating Systems: • RedHat Enterprise Linux Server 7.2 and above • RedHat Enterprise Linux Server 8.x and above • IBM AIX 7.1 and 7.2 • SuSE Any point release of SuSE Linux Enterprise Server version 12.x • zSeries SuSE Any point release of SuSE Linux Enterprise Server version 12.x • zSeries Red Hat Any point release of Red Hat Enterprise Linux version 7.x • Solaris SPARC 10 to level 11 and above • Solaris SPARC 11 • MS-Windows server 2012 • MS-Windows server 2012 R2 • MS-Windows server 2016 • MS-Windows server 2019 • MS-Windows 8 • MS-Windows 10
For a **Windows** operating system: • **RAM (min.)** - 4 GB • **Disk Space (min.)** - 250 GB	

Browser Compatibility

The following table shows the browser versions compatible with the IBM Connect:Direct Web Console:

Table 2. Compatible browser with version	
Browser	**Version supported**
Google Chrome (recommended)	88.0.4324.104 (Official Build) (64-bit)
Mozilla Firefox	83.0 (64-bit)
Microsoft Edge	44.18362.449.0 and above
Microsoft Edge (Chromium)	88.0.705.56 (Official Build) (64-bit)

Note: Recommended Web Console resolution is: 1366 * 768p (desktop applications only).

The application is best viewed when the zoom is set to a default 100% in the browser setting.

Note: IBM Connect:Direct Web Console displays content only in English language. The Web Console displays Date/Time information in user's local time zone.

Known Limitations and Restrictions

IBM Connect:Direct Web Services has the following known restrictions:

- Upgrade from Connect:Direct Web Services v5.3 (1.0.0) is currently not supported. To upgrade from v5.3 (1.0.0), uninstall v5.3 and then install v6.0.
- Currently, Connect:Direct Web Console content is only available in English language.

- Upgrade is not supported from v6.0.0.X to v6.1.0.0 on Solaris SPARC 10 platform.

Security Considerations

You should evaluate security consideration as per their enterprise policy and should take necessary steps to harden it.

- It is recommended that Connect:Direct Web Services and PostgreSQL database be installed on the same system.
- Connect:Direct Web Services PostgreSQL database does not support data encryption in the current release.
- For security reasons, it is recommended that you change the default administrator password immediately after your first login. To change the administrator password, use **Reset Password** option under the **Admin** view.
- If you configure and integrate your own Keystore/Truststore other than the default one, you will be responsible its security and protection.

Upgrading Guidelines

Observe the following guidelines for upgrading IBM Connect:Direct Web Service from an earlier version.

- Before you perform any upgrade procedure, create backup copies of the following IBM Connect:Direct Web Service database and system files. Taking a backing of the following files will helps you preserve your data and restore the previous set up in case of a failed upgrade.

  Note: The file path given below are relative to the installation directory.
- If in any case upgrade installation is corrupted, you have the option to re-install the earlier version, replace the backup files and restart the services manually.

Table 3. Connect:Direct Web Services system files

File Name	Path
application.properties	/mftws/BOOT-INF/classes
hiddenFile	/mftws/BOOT-INF/classes
ssl-server.jks	/mftws/BOOT-INF/classes
trustedKeystore.jks	/mftws/BOOT-INF/classes
script utilities	/bin
uninstall.sh	/UninstallerData
log4j2.yaml **Note:** For users upgrading from a version <v6.1.0.3 backup log4j.properties file.	/mftws/BOOT-INF/classes
silentInstall.properties	/mftws/BOOT-INF/classes

* for users upgrading from v6.0.0.5 and above

** for users upgrading from a version <= v6.0.0.4

Table 4. Connect:Direct Web Services database files upgrading from a version <v6.0.0.4

File Name	Path
Redis	/redis

Table 5. Connect:Direct Web Services database files for users upgrading from v6.0.0.5 and above users	
File Name	**Path**
PostgreSQL	/PostgreSQL

Upgrading Connect:Direct Web Services on zLinux and AIX systems

Observe the following guidelines only when you upgrade from **v6.1.0.0 to v6.1.0.1**.

Note: Do not log into the Connect:Direct Web Services application until the database backup and restore scripts complete all of its processes as described below.

1. Ensure that the following two scripts are placed inside the same directory other than the installation directory. These scripts come bundled in installer .tar.gz file.

```
backup.sh
restore.sh
```

2. Issue the following command to initiate database backup.

   Note: Ensure that the PostgreSQL database password, hostname, and port entries must match the database connection details provided at v6.1.0.0 fresh install.

```
bash-5.0# ./backup.sh

Enter absolute path of PostgreSQL bin directory:
/usr/bin

Enter PostgreSQL Password:

Enter PostgreSQL Hostname:
localhost

Enter PostgreSQL Port:
5432
```

3. Initiate the upgrade process as described in “Upgrading Web Services on AIX” on page 32 and “Upgrading Web Services on zLinux” on page 34.
4. Execute the following command to initiate database restore.

```
bash-5.0# ./restore.sh

Enter absolute path of PostgreSQL bin directory:
/usr/bin

Enter PostgreSQL Password:

Enter PostgreSQL Hostname:
localhost

Enter PostgreSQL Port:
5432
```

5. The upgrade process is complete. You can now login to the application via. Web Console or RESTful API interface.

Chapter 2. Product overview

The following section describes how to plan, install, and manage IBM Connect:Direct Web Service.

About IBM Connect:Direct Web Service

Web Services technology is widely gaining popularity and is increasingly used to provide access to business functions over the internet. Web Services enable external applications to be integrated more rapidly, easily, and with much reduced costs than ever before.

IBM Connect:Direct Web Service targets transforming the Managed File Transfer market with a modern user experience and help your business by:

- Reducing the operating cost
- Deploying solutions rapidly
- Opening new opportunities by enabling easy integration with other Web service-based applications

IBM Connect:Direct Web Service extends a Web-based User Interface (Web Console) and a RESTful API-based interface to Connect:Direct users.

- **Web Console**

  The IBM® Connect:Direct Web console, or simply the Web Console, is your web interface to IBM Connect:Direct. It provides a single point of access to manage operational and administrative tasks necessary to monitor and control Connect:Direct processes. To access the Web console, install Connect:Direct Web Services on your preferred Operation System. For more information see, “Installation and Configuration Worksheet” on page 11.

- **RESTful API Interface**

  The Representational State Transfer (REST) Application Programming Interface (API) is useful when you want to integrate IBM® Connect:Direct Web Services with other solutions or develop custom applications by using the RESTful APIs.

Web Console Interface

The IBM Connect:Direct Web Service extends a light and clean Web-based User Interface (Web Console) to Connect:Direct users to create, submit, and view Connect:Direct processes from a web browser.

The Web Console provides the following features as a standard:

- A light and clean user interface that presents clear, uncluttered menus and displays.
- Accessed using a Web browser that connects to Connect:Direct Web Server. For more information on browser support see, “Browser Compatibility” on page 5.
- Control what information can be amended, and where and how these amendments are made.
  - Example, you can make sure that the user must confirm an operation that is required, or that data has to be changed. Or, add safety by providing a confirmation panel asking the user to confirm that an action is to be performed.
- An easy-to-use interface to complete operational and administrative tasks necessary to monitor and control Connect:Direct processes.
- Provides a complete audit trail of data transmission through extensive statistics and logs.

  The Web Console logically bundles all these tasks under the following views:

  - **User Functions**

Use the **User Functions** view to complete Connect:Direct operational tasks.

The **User Functions** view includes tabs such as Partners, Transfers, Statistics, and Settings. These tabs have linked menus that facilitate all Connect:Direct operational tasks such as View and Change the network map or initialization parameters.

- **Admin Functions**

  Use **Admin Functions** view to perform tasks such as, Add node information from the IBM Connect:Direct Web Console itself.

To access the Web Console, complete the Web Services installation and configuration tasks on your preferred Operation System.

What to do next:

- "Installation and Configuration Worksheet" on page 11
- Chapter 4, "Configuration settings for IBM Connect:Direct Web Service ," on page 43
- "Accessing Web Console" on page 40

RESTful API Interface

The IBM Connect:Direct Web Service also extends a RESTful API interface to Connect:Direct.

You can use the Representational State Transfer (**REST**) Application Programming Interface (**API**) to make HTTPS queries and integrate IBM Connect:Direct with other solutions.

RESTful APIs users can issue commands via. browser interface, REST client (Postman), CLI interface (cURL), and scripts that run automatically from a remote client - making scripting common actions easier.

For more information on using IBM Connect:Direct RESTful APIs see, Chapter 5, "Using RESTful APIs with IBM Connect:Direct," on page 55.

Web Console Getting Started Videos

To learn more about the Connect:Direct Web Console, its functions and capabilities access the collection of videos on YouTube> IBM Connect:Direct.

Chapter 3. Installing, Uninstalling, and Upgrading IBM Connect:Direct Web Service

Use information provided in the following sections to install, upgrade, and uninstall Connect:Direct Web Services on a UNIX, Windows, or AIX platform.

Installation and Configuration Worksheet

The following sections outlines the steps to set up IBM Connect Direct Web Services. This workflow also describes how to plan, configure, uninstall, and troubleshoot the IBM Connect:Direct Web Service .

The table lists the necessary installation and configuration tasks that you must perform to complete the installation.

Task	For more information, see the following sections in this guide
Installing IBM Connect:Direct Web Service	"Installing on UNIX" on page 11 "Installing on Windows" on page 26 "Installing on AIX" on page 30
Configuring a secure connection between IBM Connect:Direct Web Console and a IBM Connect:Direct server	"Establishing a Secure Connection between IBM Connect:Direct and IBM Connect:Direct Web Service " on page 43
Configuring the property files that control system-wide IBM Connect:Direct Web Console properties.	"Configuring application.properties" on page 50
Configuring Web Services Logs	"Connect:Direct Web Services Logs" on page 53

Installing, Upgrading, and Uninstalling on UNIX

Use information in the following sections to install, upgrade, and uninstall Connect:Direct Web Services on a UNIX platform.

Installing on UNIX

Before you begin

- Review the system requirements. For more information, see "Minimum Hardware and Software Requirements" on page 4.
- Make sure you have added firewall rules for inbound and outbound connections between Web Services and Connect Direct Server. Firewall rules must allow inbound connections to the specified Web Services port. Connect Direct server must also have its API port open for web service.
- Note that upgrade from Connect:Direct Web Services v5.3 (1.0.0) is not available. To upgrade from v5.3 (1.0.0), you must first uninstall it and then install v6.0. For more information, see "Uninstalling on UNIX" on page 21.

Procedure

To install the Connect:Direct Web Services from command line on a UNIX Operating System follow the steps given below.

Note: Do not install as root. If you do not have sufficient privileges, use `chmod a+x` to execute the script. Ensure that you login to the same functional account to upgrade and install Connect:Direct Web Services.

1. If you have downloaded the software from IBM Passport Advantage go to the download folder.

   Note: Passport Advantage provides access to your IBM software purchases, so you can download products directly to the computers where you want to install them. For information on the how to download software using Passport Advantage see, Passport Advantage.

2. Untar the installer .tar.gz file.

   ```
   % tar -zxvf IBM_CDWebServices_$version_Linux_x64.tar.gz
   ```

   Note: $VERSION refers to the IBM Connect:Direct Web Service version number.

   The following files are extracted:

   ```
   MFTWebServicesInstall.bin
   MFTWebServicesInstall.sh
   silentInstall.properties
   ```

3. Confirm that you have sufficient privileges to run the following script file.

   ```
   % ./MFTWebservicesInstall.sh
   ```

4. The installation menu appears.

```
Preparing to install
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...
===============================================
MFTWebServices (created with InstallAnywhere)
-------------------------------------------------------------------------------
Preparing CONSOLE Mode Installation...
===============================================
Introduction
-------------------------------------------------------------------------------
Welcome to the installation wizard for MFTWebServices.
This wizard guides you through the installation of MFTWebServices.
You are strongly recommended to quit all programs before continuing with this
installation.
Respond to each prompt to proceed to the next step in the installation.
You may cancel this installation at any time by typing 'quit'.
Licensed Materials - Property of IBM Corp. © IBM Corporation and other(s).
2018.
```

5. Enter the absolute installation path and press **ENTER** to confirm the location.

```
Choose Install Folder
---------------------------
Where would you like to install?
Default Install Folder: $HOME/MFTWebServices
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
```

6. Enter Secure port number details that Connect:Direct Web Server uses to connect to the Web Service and press **ENTER** to continue.

```
Port for Web Server
-------------------------
Enter the ConnectDirectWebServices secure sever port.
eg. https://<hostname:port>/cdws-doc/signOn.html
https://<hostname:port>/cdws-ui/index.html
Secure Port (Default: 9443):
```

7. Enter the PostgreSQL Database Server port number and press **ENTER** to continue.

```
Port for PostgreSQL
---------------------
Enter PostgreSQL Port
PostgreSQL Port (Default: 5432):
Password for PostgreSQL
---------------------
This installation requires a password to continue.
Please Enter the password:
PRESS <ENTER> TO CONTINUE:
```

8. Pre-Installation summary appears.
   Press **ENTER** to continue.

```
Pre-Installation Summary
--------------------------------
Review the following information before you continue the installation:
Product Name:
MFTWebServices
Install Folder:
$HOME/MFTWebServices
Web Server Port
9443
PostgreSQL Port
5432
Version
<$VERSION>
Disk Space Information (for Installation Target):
Required: 345 MegaBytes
Available: 5,000.26 MegaBytes
PRESS <ENTER> TO CONTINUE:
```

9. Certification Generation information screen appears. Press **ENTER** to continue.

```
Generate Certificate
--------------------------
User can generate two types of certificate:
1. DEFAULT Certificate: The certificate is generated through default values of the system.
2. SELF SIGNED Certificate: The certificate is generated by taking input from the user.
Note: After successful installation, user can add a third party or any other
certificate in existing Keystore/Truststore.
User can also add a new Keystore/Truststore.
Please refer IBM CDWS documentation for more details
Press Enter to proceed.
```

10. Enter the Certificate option serial number for the certificate type that you would like to use or generate a - Default, or Self-Signed certificate.

    Note: When installation is complete, users can add a CA-signed certificate or any other certificate in existing Keystore/Truststore. Users can also add a new Keystore/Truststore. For more information, see "Configuring Keystore/Truststore" on page 43.

```
Choose certificate type
-----------------------------
1. DEFAULT
2. SELF SIGNED
Enter Your Choice: (Default: 1): 1
```

If you enter [1], Default Certificate details display. Press **ENTER** to continue.

```
Certificate Details
-----------------------
The Certificate will be generated with following details:
_____________________________________________________________
Keystore NAME: ssl-server.jks
KEYSIZE: 2048
CERTIFICATE LABEL: connectdirectwebservices
CERTIFICATE EXPIRY TIME: 365 days
ORGANIZATION: OrganizationName
LOCALITY: Irving
STATE: Texas
COUNTRY: US
EMAIL ID: noreply@noreply.com
ALGORITHM: SHA256withRSA
COMMON NAME: <hostname>
PRESS <ENTER> TO CONTINUE:
```

A Default Certificate is generated.

```
Certificate Generated Successfully.
Keystore NAME: ssl-server.jks
CERTIFICATE LABEL: connectdirectwebservices
PATH: /$HOME/MFTWebServices/mftws/BOOT-INF/classes/ssl-server.jks
ALGORITHM: SHA256withRSA
PRESS <ENTER> TO CONTINUE:
============================================================
Please Wait
------------------------------------------------------------
.....
Installation Completed
------------------------------------------------------------
Installation and Certificate generation is complete.
MFTWebServices-<$version> has been successfully installed to:
/$HOME/MFTWebServices

MFTWebservices User Interface is available at :
https://<hostname:port>/cdws-ui/index.html
MFTWebservices API reference is available at : https://<hostname:port>/cdws-doc/signOn.html
PRESS <ENTER> TO EXIT THE INSTALLER:
```

11. If you enter [2], user is prompted to set the Keystore password.

```
Enter Password
----------------------
Certificate Generation requires Password.
Please Enter the Password:
```

Note: Keystore password should not include any of these special characters, o "%^{}|<>~'!`.

12. Enter the Keystore password again to confirm the user input in the previous step.

```
Confirm Password
---------------------------
Please Enter the Password again:
```

13. Answer the following prompts related to Self-Signed Certificate details.

```
Certificate Label
----------------------
Enter Certificate Label (Default: connectdirectwebservices):
================================================
Certificate Expiry Time
------------------------------
Enter Certificate expiry time(MAX value: 3649 days) (Default: 365):
================================================
Common Name(CN)
--------------------------
Enter Common Name(CN) (Default: <hostname>)
================================================
Organization Name
-------------------------
Enter name of the organization (Default: organizationname):
================================================
Locality Name
--------------------
Enter name of the locality (Default: Irving):
================================================
State Name
---------------
Enter name of the State (Default: Texas):
================================================
Country Name
--------------------
Enter Country Name (Default: US):
================================================
Enter E-mail Address
---------------------------
Enter E-mail Address: (Default: noreply@noreply.com):
```

Table below describes self-signed certificate field, descriptions, example, and default values.

Table 6. Self-Signed Certificate generation entries and descriptions

Entry	Description	Example value	Default Value
Certificate label	Any descriptive name to identify the certificate.	mycertificatename	connectdirectwebservices

Table 6. Self-Signed Certificate generation entries and descriptions (continued)			
Entry	**Description**	**Example value**	**Default Value**
Certificate Expiry Time	Enter the certificate expiration time in days	278 days	365 days Max value: 3649 days
Common Name (CN)	Identifies the host name associated with the certificate	yourdomain	<*hostname*>
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC. **Note:** Do not abbreviate or use any of these symbols: ! @ # $ % ^ * ( ) ~ ? > < / \.	MyOrganizationName Inc.	organizationname
Locality	The city where your organization is located.	Irving	Irving
State	The state/region where your organization is located. **Note:** Do not use abbreviations.	Texas	Texas
Country	The two-letter ISO code for the country where your organization is location.	US	US
E-mail ID	An email address used to contact your organization.	support@mydomain.com	noreply@noreply.com

14. Self-Signed certificate details display. Press **ENTER** to continue.

```
Certificate Details
------------------------
The certificate will be generated with following details:
_____________________________________________________
Keystore NAME: ssl-server.jks
KEYSIZE: 2048
CERTIFICATE LABEL:connectdirectwebservices
CERTIFICATE EXPIRY TIME: 365
CN: <hostname>
ORGANIZATION: MyOrganization
LOCALITY: Irving
STATE: Texas
COUNTRY: US
EMAIL ID: noreply@noreply.com
ALGORITHM: SHA256withRSA
FQDN: <hostname>
PRESS <ENTER> TO CONTINUE:
```

15. A Self-Signed Certificate is generated successfully. Installation is complete. Press **ENTER** to exit the installation screen.

```
Certificate Generated Successfully.
Keystore NAME: ssl-server.jks
CERTIFICATE LABEL: connectdirectwebservices
PATH: /$HOME/MFTWebServicesDoc/mftws/BOOT-INF/classes/ssl-server.jks
ALGORITHM: SHA256withRSA
PRESS <ENTER> TO CONTINUE:
============================================================
Please Wait
------------------------------------------------------------
.....
============================================================
Installation Completed
------------------------------------------------------------
Installation and Certificate generation is complete.
ConnectDirectWebServices-<$VERSION> has been successfully installed to:
/$HOME/MFTWebServices
MFTWebServices User Interface is available at :
https://<hostname:port>/cdws-ui/index.html
MFTWebServices API reference is available at :
https://<hostname:port>/cdws-doc/signOn.html
PRESS <ENTER> TO EXIT THE INSTALLER
```

16. Press **ENTER** to exit the installation screen.

What to do next

1. Chapter 4, “Configuration settings for IBM Connect:Direct Web Service ,” on page 43
2. “Logging in” on page 39

Directory Structure

The following figure illustrates IBM Connect:Direct Web Service directory structure after a successful installation:

```
|---- bin
|---- mftws/BOOT-INF/classes
|---- doc
|---- Encryption
|---- jre
|---- license
|---- logs
|---- PostgreSQL
|---- RestLogs
|---- UninstallerData
|---- README.txt
```

Uninstalling on UNIX

About this task

To uninstall the IBM Connect:Direct Web Service follow the steps given below.

Procedure

Confirm that you have an executable permission to run the **`uninstall.sh`**. If you do not have sufficient privileges, use `chmod a+x` to execute the script.

Before you initiate the uninstall process, create backup copies of the IBM Connect:Direct Web Service database and system files listed here.

1. Change the IBM Connect:Direct Web Service installation directory and issue the following at command line:

   ```
   % cd your_Installation_directory/UninstallerData/
   ```

2. To complete the uninstall process, run the **uninstall.sh** script.

   Note: If you do not have sufficient privileges, use `chmod a+x` to execute the script.

   ```
   ./uninstall.sh
   ==================0============================
   ConnectDirectWebServices (created with InstallAnywhere)
   -------------------------------------------------------------------------------
   Preparing CONSOLE Mode Uninstallation...
   ===============================================
   ```

```
Uninstall MFTWebServices
---------------------------------------------
About to uninstall...
MFTWebServices
This will remove features installed by InstallAnywhere.
PRESS <ENTER> TO CONTINUE: [Hit The Enter Key]
==========================================
```

```
Uninstalling...
===============================
```

```
Uninstall Complete
------------------------
All items were successfully uninstalled.
================================
```

Upgrading from a previous release on UNIX

Observe the following guidelines to upgrade IBM Connect:Direct Web Service from a previous release.

Upgrade Guidelines

Observe the following guidelines:

- You must plan the upgrade activity during a planned maintenance window.
- Before you perform any upgrade procedure, create backup copies of Connect:Direct Web Services database and system files. For details see, “Upgrading Guidelines” on page 6.
- A Connect:Direct user cannot perform any operation on IBM Connect:Direct Web Services during the upgrade process.

  Note: IBM Connect:Direct Web Services will restart during this process. It is recommended that you stop any instance of Web Services, if running.

Upgrading Web Services on UNIX

About this task

To upgrade the IBM Connect:Direct Web Services from command line on UNIX follow the steps given below.

Procedure

Log on to the UNIX system and ensure that you have executable privileges required to upgrade the software. You can create an account specifically for this purpose.

Note: Ensure that you login to the same functional account to upgrade and install Connect:Direct Web Services. The screen shots given below are examples and not definitive of what you see on your screen.

On upgrading installer with different user getting error message

1. Untar the installer .tar.gz file.

```
% tar -zxvf IBM_CDWebServices_$CurrentVersion_Linux_x64.tar.gz
```

Note: $VERSION refers to the IBM Connect:Direct Web Service version number.

The following files are extracted:

```
MFTWebservicesInstall.bin
MFTWebservicesInstall.sh
silentInstall.properties
```

2. Confirm that you have sufficient privileges to run the following script file.

```
% ./MFTWebservicesInstall.sh
```

Note: If you do not have sufficient privileges, use `chmod a+x` to execute the script.

3. The installation menu appears. Enter the instance option serial number to upgrade and press **ENTER** to confirm.

```
Specify the instance that you want to upgrade.
1. $HOME/MFTWebServices
Enter 1 for first instance, 2 for second instance, and so on:
===============================================
MFTWebServices (created with InstallAnywhere)
-------------------------------------------------------------------------------
Preparing CONSOLE Mode Installation...
===============================================
Please Wait
-----------------
.....................................................................................
=========================================
```

4. Read the upgrade guideline screen displayed and press **ENTER** to continue.

```
Upgrade Guidelines
---------------------------
Welcome to the upgradation wizard for MFTWebServices.
This wizard is going to guide you through the upgradation of
MFTWebServices.
You are strongly recommended to quit all programs before continuing with this
upgrade.
Respond to each prompt to proceed to the next step in the upgrade.
Licensed Materials - Property of IBM Corp. © IBM Corporation and other(s).
2018.
PRESS <ENTER> TO CONTINUE:
```

5. The Upgrade Notice displays. Read the Upgrade Notice and press **ENTER** to continue.

```
Upgrade Notice
----------------------
The existing installation of MFTWebServices in
$HOME/MFTWebServices is going to be upgraded.
The existing library files will be uninstalled, but all configuration data
such as properties file, Keystore, Truststore and configuration files will be
retained.
Before you proceed with the upgrade, backup your existing configuration data.
During MFTWebServices upgrade , the installer is going to attempt to backup
your existing configuration data.
Note: During Upgrade the user will not be able to login or perform any
operation on MFTWebServices.
Do not 'quit' before Upgrade process is completed.
PRESS <ENTER> TO CONTINUE:
```

6. Configuration data backup begins.

```
==========================================
Backup of Configuration data
------------------------------------------
Configuration data backup is successful
==========================================
```

7. User is one step away from Upgrade. The pre-upgrade summary is displayed.
   Press **ENTER** to continue.

```
===============================================
Pre-Upgrade Summary
-------------------------------
Review the following information before you continue the upgrade:
Product Name:
MFTWebServices
Install Folder:
$HOME/MFTWebServices
Install Set:
Typical
Base Upgrade Version
6.0.0.5
Product will be upgraded to
6.1
Disk Space Information (for Installation Target):
Required: 345 MegaBytes
Available: 4,634.47 MegaBytes
PRESS <ENTER> TO CONTINUE:
```

8. Old version of the IBM Connect:Direct Web Service is removed before the new version is installed.

```
===============================================
Please Wait
--------------------
Uninstalling older installation : ConnectDirectWebServices-6.0.0.5
===============================================
```

9. Upgrade to a new version is complete. The following output is displayed:

```
Upgrade Complete
----------------------------
ConnectDirectWebServices-6.0.0.5 has been successfully upgraded to
ConnectDirectWebServices-6.1 and located at:
$HOME/MFTWebServices
PRESS <ENTER> TO EXIT THE INSTALLER:
```

Installing, Upgrading, and Uninstalling on Windows

Use information in the following sections to install, upgrade, and uninstall Connect:Direct Web Services on a Windows platform.

Installing on Windows

Before you begin

Before you begin, see “Minimum Hardware and Software Requirements” on page 4.

Make sure you have added firewall rules for inbound and outbound connections between Web Services and Connect Direct Server. Firewall rules must allow inbound connections to the specified Web Services port. Connect Direct server must also have its API port open for web service.

Procedure

To install IBM Connect:Direct Web Service on a Windows platform follow the steps given below.

1. If you downloaded the software from IBM Passport Advantage, double-click ***IBM_CDWebServices_<version>_Windows_X64.exe*** from the download folder.

   Note: For information on the how to download software using Passport Advantage see, Passport Advantage.

   Installation Folder window appears. This window serves as a welcome screen with a **Guided Setup** on the left. The Guided Step up is an installation status panel. As you complete each task, the status panel is updated. Click **Next.**
2. In the **Installation Folder** window, use the default location or click **Choose** and specify a different location. Click **Restore Default Folder** to choose the default location.
3. Click **Next** to continue.
4. The **Ports** window appears. Enter the following:
   a. **Secure Port** that the Web Services uses to connect to the Web Server. For example,

   ```
   https://<hostname:port>/cdws-doc/signOn.html
   https://<hostname:port>/cdws-ui/index.html

   Default: 9443
   ```

   b. Enter PostgreSQL database connection details. For example:

   ```
   Default: 5342
   Password:<password>
   ```
5. Click **Next** to continue.
6. In the **Pre-Installation Summary** window, review the information, and then click **Install**.
7. **Generate Certificate** window appears.

   This window informs the user of two certificate generation options available to the user.

   Click **Next** to continue.
8. Choose **Certificate** window appears. This window provides users two options that can be used to generate a certificate:

   a) Default Certificate

   b) Self-Signed Certificate

   Note: When installation is complete, users can add a CA-signed certificate or any other certificate in the existing Keystore/Truststore. User can also add a new Keystore/Truststore. For more information, see “Configuring Keystore/Truststore” on page 43.
9. Select **Default** option to generate a Default certificate. Click **Next** to continue
10. The **Certificate Details** window appears. This window displays Default certificate details. To generate a Default Certificate, click **Next.**
11. A Default certificate is generated and **Installation Complete** screen appears. Click **Done**.

12. Alternatively, select **Self-Signed** option to generate a User-Defined certificate.
13. The **Keystore** screen appears. Set the **Keystore password** to generate a self-signed certificate. Click **Next**.
14. Enter the **Keystore password** again to confirm the user input. Click **Next.**
15. The **Self-Signed Certificate** screen appears. Enter certificate details in the fields, as applicable. To generate a Self-Signed Certificate **Next**.

    Table below describes self-signed certificate field, descriptions, example, and default values.

Table 7. Self-Signed Certificate generation field descriptions

Fields	Description	Example value	Default Value
Certificate label	Any descriptive name to identify the certificate.	mycertificatename	connectdirectwebservices
Certificate Expiry Time	Enter the certificate expiration date in days	278 days	365 days Max value: 3649 days
Common Name (CN)	Identifies the host name associated with the certificate	yourdomain	<*hostname*>
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC. **Note:** Do not abbreviate or use any of these symbols: ! @ # $ % ^ * ( ) ~ ? > < / \.	MyOrganizationName Inc.	organizationname
Locality	The city where your organization is located.	Irving	Irving
State	The state/region where your organization is located. **Note:** Do not use abbreviations.	Texas	Texas
Country	The two-letter ISO code for the country where your organization is location.	US	US
E-mail ID	An email address used to contact your organization.	support@mydomain.com	noreply@noreply.com

16. Self-Signed certificate details summary window appears. Click **Next** to continue.
17. A Self-Signed certificate is generated and Click **Next** to continue.
18. **Installation Complete** screen appears. Click **Done**.

What to do next

1. Chapter 4, “Configuration settings for IBM Connect:Direct Web Service ,” on page 43

2. “Logging in” on page 39

Directory Structure

The following figure illustrates IBM Connect:Direct Web Service directory structure after a successful installation on a Windows Operating System:

```
|---- bin
|---- mftws
|---- Encryption
|---- jre
|---- license
|---- logs
|---- PostgreSQL
|---- RestLogs
|---- sampleRestClientScripts
|---- Uninstall_MFTWebServices
|---- clear-syslog
|---- README.txt
```

Uninstalling on Windows

About this task

The Connect:Direct Web Services Uninstall program removes the application, its components, program items, and Server/Registry settings.

Procedure

To uninstall the IBM Connect:Direct Web Service program and all its utilities follow the procedure give below.

Before you initiate the uninstall process, create backup copies of the IBM Connect:Direct Web Service database and system files listed here.

1. Click **Start** > **Programs** > **Settings** > **Control Panel** > **Add-Remove Programs**.
2. Select *MFTWebservices* and click **Remove**.
3. Click **Yes** to confirm the removal of this program.
4. Click **Finish**.
5. Click **OK** to close the **Add/Remove Programs Properties** dialog box.

Upgrading Web Services on Windows

Procedure

To upgrade the IBM Connect:Direct Web Service on a Windows platform follow the steps given below.

Note: Before you perform any upgrade procedure, create backup copies of Connect:Direct Web Services database and system files. For details see, “Upgrading Guidelines” on page 6.

1. If you downloaded the software from IBM Passport Advantage, double-click **IBM_CDWebServices_<new_version>_Windows_X64.exe** from the download folder.

Note: For information on the how to download software using Passport Advantage see, Passport Advantage.

The **Upgrade Confirmation** window appear.

2. Click **Upgrade** to continue with the upgrade.
3. The **Upgrade Guidelines** window appears. This window serves as a welcome screen with a **Guided Setup** on the left. The Guided Step up is an upgrade status panel. As you complete each task, the status panel is updated. Click **Next.**
4. Read the upgrade guideline screen displayed and press **ENTER** to continue.
5. Click **Next** to continue.
6. The **Ports** window appears. Enter the following:
   - **PostgreSQL database port**. For example:

PostgreSQL database Port Default: 5432

7. Click **Next** to continue.
8. In the **Pre-Installation Summary** window, review the information, and then click **Next**.
9. The **Upgrade Guideline** screen displays. Click **Next** to continue.
10. The **Upgrade Notice** displays. Click **Next** to continue.
11. **Configuration data** backup begins.
12. User is one step away from Upgrade and the **Pre-upgrade** summary displays.
    Click **Upgrade** to continue.
    Old version of the IBM Connect:Direct Web Services is removed before the new version is installed.

Installing, Upgrading, and Uninstalling on AIX

Use information in the following sections to install, upgrade, and uninstall Connect:Direct Web Services on IBM AIX platform.

Installation Prerequisites

About this task

Before you install IBM Connect:Direct Web Service on AIX complete the following procedure to initialize and configure PostgreSQL database.

Note: This procedure only applies for IBM Connect:Direct Web Service v6.0.0.5 and above users.

Procedure

1. Invoke the following command to list all PostgreSQL database packages:

```
yum list postgresql*
```

2. Invoke the following command to install PostgreSQL v9.2 database.

```
yum install postgresql-server
```

3. Invoke the following command to initialize and configure a PostgreSQL database.

a. The PostgreSQL data directory contains all data files required to configure and initialize the database. Variable **PGDATA** is used to reference this directory. The default data directory is `/var/lib/pgsql/data`.

b. To initialize the database, create a directory and use `chown` command to assign all privileges to that directory.

   Add a PostgreSQL database user to the PostgreSQL group using the `chown -R` command, with data directory, logged in as a PostgreSQL user.

```
root@zrh07xxd var]# mkdir AIXPostgres
[root@zrh07xxd var]# chown -R 777/var/AIXPostgres/
[root@zrh07xxd var]# chown -R postgres:postgres/var/AIXPostgres/
[root@zrh07xxd var]# cd AIXPostgres/
[root@zrh07xxd testpg]# su - postgres
Last login: Tue Dec 17 12:59:14 CST 2019 on pts/2
```

c. Invoke the `initdb` command from the bin folder and define the directory created in the steps above followed by argument -D.

d. Use `-W -A` arguments to prompt user for password-based authentication.

```
bash-5.0$ ./initdb -U postgres -D "/var/AIXPostgres" -W -A md5
The files belonging to this database system will be owned by user "postgres".
This user must also own the server process.

The database cluster will be initialized with locale "en_US".
The default database encoding has accordingly been set to "LATIN1".
The default text search configuration will be set to "english".
Data page checksums are disabled.
Enter new superuser password:
Enter it again:

fixing permissions on existing directory /var/AIXPostgres... ok
creating subdirectories ... ok
selecting default max_connections ... 100
selecting default shared_buffers ... 128MB
selecting default timezone ... CST6CDT
selecting dynamic shared memory implementation ... posix
creating configuration files ... ok
running bootstrap script ... ok
performing post-bootstrap initialization ... ok
syncing data to disk ... ok

Success. You can now start the database server using:

    ./pg_ctl -D /var/AIXPostgres -l logfile start
```

Installing on AIX

Before you begin

Connect:Direct Web Services on AIX requires the following system libraries to be installed:

- `libatomic.a`
- `libgcc_s.a`

Make sure you add firewall rules for inbound and outbound connections between Web Services and Connect Direct Server. Firewall rules must allow inbound connections to the specified Web Services port. Connect Direct server must also have its API port open for web service.

Make sure you also add firewall rules for inbound and outbound connections between Web Services and PostgreSQL database.

Note: Ensure that you install using **Root Privilege**.

Attention: For Connect:Direct Web Services v6.0.0.5 and above to run with PostgreSQL on AIX platforms, users must create a dedicated PostgreSQL database instance and then configure Connect:Direct Web Services to use it while it is being installed.

If for some reason the database is corrupted, or you lose the database password, follow the instructions described here "PostgreSQL database Password management" on page 72.

About this task

Follow the procedure given below to prepare and complete installation on AIX.

Procedure

1. Download the appropriate `libgcc` RPM from https://www.ibm.com/developerworks/aix/library/aix-toolbox/alpha.html.
   a. For AIX 7.1, download the following RPM:

   ```
   libgcc-6.3.0-2.aix7.1.ppc.rpm
   ```

   b. For AIX 7.2, download the following RPM:

   ```
   libgcc-8.1.0-2.aix7.2.ppc.rpm
   ```

2. When the `libgcc` RPM is installed, copy the `libatomic.a` and `libgcc_s.a` libraries to /**usr**/**lib** directory.
   a. For AIX 7.1 copy from

   ```
   /opt/freeware/lib/gcc/powerpc-ibm-aix7.1.0.0/6.3.0/ppc64/
   ```

   b. For AIX 7.2 copy from

   ```
   /opt/freeware/lib/gcc/powerpc-ibm-aix7.2.0.0/8.1.0/ppc64/
   ```

3. If you have downloaded the Web Services for AIX installation software from Fix Central or Passport Advantage go to the download folder.
4. Untar the installer .tar.gz file.

   ```
   % tar -zxvf IBM_CDWebServices_<$version>_AIX_x86.tar.gz
   ```

   Note: $VERSION refers to the IBM Connect:Direct Web Service version number.
5. To continue installing follow the steps described in "Installing on UNIX" on page 11.

Uninstalling on AIX

About this task

To uninstall the IBM Connect:Direct Web Service on AIX, execute the **uninstallAIX.sh** script. For more information see, "Uninstalling on UNIX" on page 21.

Before you initiate the uninstall process, create backup copies of the IBM Connect:Direct Web Service database and system files listed here.

Upgrading Web Services on AIX

About this task

To upgrade the IBM Connect:Direct Web Service on IBM AIX follow the steps given below. Before you perform any upgrade procedure, create backup copies of Connect:Direct Web Services database and system files. If you are upgrading from v6.1.0.0 to v6.1.0.1 see , “Upgrading Guidelines” on page 6.

Procedure

1. Untar the installer .tar.gz file.

```
% tar -zxvf IBM_CDWebServices_<$NEW_VERSION>_AIX_x86.tar.gz
```

   Note: $NEW_VERSION refers to the IBM Connect:Direct Web Service version number.

2. To continue the Upgrade procedure see, “Upgrade Guidelines” on page 22 and “Upgrading Web Services on UNIX” on page 22.

Installing, Upgrading, and Uninstalling on zLinux

Use information in the following sections to install, upgrade, and uninstall Connect:Direct Web Services on IBM zLinux platform.

Installation Prerequisites

About this task

Before you install IBM Connect:Direct Web Service on zLinux complete the following procedure to initialize and configure PostgreSQL database.

Note: This procedure only applies for IBM Connect:Direct Web Service v6.0.0.5 and above users.

Procedure

1. Invoke the following command to list all PostgreSQL database packages:

```
yum list postgresql*
```

2. Invoke the following command to install PostgreSQL v9.2 database.

```
yum install postgresql-server
```

3. Invoke the following command to initialize and configure a PostgreSQL database.
   a. The PostgreSQL data directory contains all data files required to configure and initialize the database. Variable **PGDATA** is used to reference this directory. The default data directory is `/var/lib/pgsql/data`.
   b. To initialize the database create a directory and use `chown` command to assign all privileges to that directory.

      Add a PostgreSQL database user to the PostgreSQL group using the `chown -R` command, with data directory, logged in as a PostgreSQL user.

```
root@zrh07xxd var]# mkdir zlinuxPostgres
[root@zrh07xxd var]# chown -R 777/var/zlinuxPostgres/
[root@zrh07xxd var]# chown -R postgres:postgres/var/zlinuxPostgres/
[root@zrh07xxd var]# cd zlinuxPostgres/
[root@zrh07xxd testpg]# su - postgres
Last login: Tue Dec 17 12:59:14 CST 2019 on pts/2
```

c. Invoke the `initdb` command from the bin folder and define the directory created in the steps above followed by argument -D.

d. Use `-W -A` arguments to prompt user for password-based authentication.

```
bash-5.0$ ./initdb -U postgres -D "/var/zlinuxPostgres" -W -A md5
The files belonging to this database system will be owned by user "postgres".
This user must also own the server process.

The database cluster will be initialized with locale "en_US".
The default database encoding has accordingly been set to "LATIN1".
The default text search configuration will be set to "english".
Data page checksums are disabled.
Enter new superuser password:
Enter it again:

fixing permissions on existing directory /var/zlinuxPostgres... ok
creating subdirectories ... ok
selecting default max_connections ... 100
selecting default shared_buffers ... 128MB
selecting default timezone ... CST6CDT
selecting dynamic shared memory implementation ... posix
creating configuration files ... ok
running bootstrap script ... ok
performing post-bootstrap initialization ... ok
syncing data to disk ... ok

Success. You can now start the database server using:

    ./pg_ctl -D /var/zlinuxPostgres -l logfile start
```

Installing on zLinux

Before you begin

Connect:Direct Web Services on zLinux requires the following system libraries to be installed:

Note: Ensure that you install using **Root Privilege**.

Make sure you add firewall rules for inbound and outbound connections between Web Services and Connect Direct Server. Firewall rules must allow inbound connections to the specified Web Services port. Connect Direct server must also have its API port open for web service.

Make sure you also add firewall rules for inbound and outbound connections between Web Services and PostgreSQL database.

Attention: For Connect:Direct Web Services v6.0.0.5 and above to run with PostgreSQL on zLinux platforms, users must create a dedicated PostgreSQL database instance and then configure Connect:Direct Web Services to use it while it is being installed.

If for some reason the database is corrupted, or you lose the database password, follow the instructions described here “PostgreSQL database Password management” on page 72.

About this task

Follow the procedure given below to prepare and complete installation on zLinux.

Procedure

1. If you have downloaded the Web Services for zLinux installation software from Fix Central or Passport Advantage go to the download folder.
2. Untar the installer .tar.gz file.

```
% tar -zxvf IBM_CDWebServices_<$version>_zLinux_x64.tar.gz
```

   Note: $VERSION refers to the IBM Connect:Direct Web Service version number.
3. To continue installing follow the steps described in, “Installing on UNIX” on page 11.

Uninstalling on zLinux

About this task

To uninstall the IBM Connect:Direct Web Service on AIX, execute the **uninstallZLinux.sh** script. For more information see, “Uninstalling on UNIX” on page 21.

Before you initiate the uninstall process, create backup copies of the IBM Connect:Direct Web Service database and system files listed here.

Upgrading Web Services on zLinux

About this task

To upgrade the IBM Connect:Direct Web Service on IBM zLinux follow the steps given below. Before you perform any upgrade procedure, create backup copies of Connect:Direct Web Services database and system files. If you are upgrading from v6.1.0.0 to v6.1.0.1 see , “Upgrading Guidelines” on page 6.

Procedure

1. Untar the installer .tar.gz file.

```
% tar -zxvf IBM_CDWebServices_<$new_version>_zLinux_x64.tar.gz
```

   Note: $new_version refers to the IBM Connect:Direct Web Service version number.
2. To continue the Upgrade procedure see, “Upgrade Guidelines” on page 22 and “Upgrading Web Services on UNIX” on page 22.

Silent Install and Silent Upgrade for Connect:Direct Web Services

Connect:Direct Web Services administrators can use procedures defined in the following sections to run an unattended install with minimal user interaction. Silent installs can be used for repetitive installs in your deployment.

Installation and Upgrade Considerations

Recommendation: You can silently upgrade an installation only if the installation was performed using the silent installation method

- Ensure that the installation executable file, script, and `silentInstall.properties` file are placed in the same directory. Also, do not rename these files.
- The same `silentInstall.properties` file that was used to perform silent installation must be used to upgrade Connect:Direct Web Services to a different version.

- When you upgrade from version < 6.0.0.5 the user must update database properties that is, Redis properties (REDIS_PORT) must be replaced with changed PostgreSQL properties (POSTGRES_PORT and POSTGRESQL_PASSWORD) in the `silentInstall.properties` file.

A Silent install is implemented in two steps:

1. Supply values in the `silentInstall.properties` file included in software package, Fix Pack 3 (v6.0.0.3) and above.

   `silentInstall.properties` file defines the installation configuration that you would normally enter during an interactive installation process (console-mode installation). The `silentInstall.properties` file is subsequently used to silently install Connect:Direct Web Services.

   Before you begin

   The following Connect:Direct Web Services minimum version levels are required to perform silent installation:

   Table 8.

Product	**Minimum Version**
IBM Connect:Direct Web Services	Fix Pack 3 (v6.0.0.3)

   The following table lists script files to be used by Operating Systems to perform unattended installation.

   Table 9. Silent Installer script name by OS

Operating System	**Silent installation script name**
Windows	MFTWebServices.bat
RedHat	MFTWebServicesInstall.sh
zLinux	MFTWebServicesInstallzLinux.sh
SuSe	MFTWebServicesInstallSuse.sh
AIX	MFTWebServicesInstallAIX.sh
Solaris 10	MFTWebServicesInstallSolaris10.sh
Solaris 11	MFTWebServicesInstallSolaris.sh

2. To perform silent installation see the following examples:

   UNIX environment (RHEL)

   When executing the `MFTWebServicesInstall.sh`, pass the argument `silent` to the script.

   ```
   [user@SolQA-02 CDWS_6.1.0.1]$ ./MFTWebServicesInstall.sh silent
   Installing Webservices...
   Installer installed/upgraded correctly.
   Please refer INSTALLATION_DIRECTORY/README.txt for getting started with MFTWebservices.
   Press any key to continue.....
   ```

   WINDOWS environment

   To install in a Windows environment, execute the `MFTWebservices.bat` file available in the download folder.

   ```
   C:\Users\Administrator\Desktop\CDWS_Installer\CDWS_6.1.0.0_01_05_2020>MFTWebservices.bat
   Installing Webservices...
   "Exit Code: 0"
   Installer installed/upgraded correctly.
   Please refer INSTALLTION_DIRECTORY/README.txt for getting started with MFTWebservices.
   Press any key to continue . . .
   ```

Error Handling during Silent Install

- If you encounter problems when performing a silent installation review the log file, **failure.txt**, available inside the `logs` directory at the same location where you have installed Connect:Direct Web Services.
- If silent installation does not begin:
  - Cleanup the registry settings in the .com.zero.registry.xml

    In UNIX environment, this file is located in `/var` for Root users and `$HOME/`for non-root users. In Windows, this file is located in `C:\Program Files\Zero G Registry`.
  - Edit the Zero G registry file to remove entries that begin with **MFTWebServices** and delete any entries beginning with the following tag:

    ```
    <product name="MFTWebServices">...</product>
    ```
  - Attempt silent installation again.

Connect:Direct Web Services Silent Install and Silent Upgrade Example

Procedure

1. Download the installation package from Fix Central and navigate to the directory where the installation package is downloaded.

   The following files will be used to perform Silent Installation:

   - `silentInstall.properties`
   - `MFTWebservices.exe`
   - `MFTWebservices.bat` (for Windows)
   - `MFTWebServicesInstall.sh` (for UNIX)
2. Modify the `silentInstall.properties` file based on your requirements.

Table 10. Parameters for Windows-based Silent installation

Parameters	Mandatory/ Optional	Description
`CERTIFICATE_TYPE_NEW`	M	This attribute stores value for certificate type to be used for secured communication. Possible values: • 0 for a Self-signed • 1 for a Default
`CERTIFICATE_TYPE_NEW_1`	M	This attribute should store the following values: • No value (blank) If the administrator elects to generate a self-signed certificate • Default Certificate If the administrator elects to generate the default certificate

Table 10. Parameters for Windows-based Silent installation (continued)

Parameters	Mandatory/ Optional	Description
CERTIFICATE_TYPE_NEW_2	M	This attribute should store the following values: • No value (blank) If the administrator elects to generate a default certificate • Self Signed Certificate If the administrator elects to use a self-signed certificate
CERTIFICATE_TYPE_NEW_BOOLEAN_1	M	This attribute should store the following values: • 0 for a Self-Signed Certificate • 1 for a Default certificate
CERTIFICATE_TYPE_NEW_BOOLEAN_2	M	This attribute should store the following values: • 0 for a Default certificate • 1 for a Self-Signed Certificate
USER_INSTALL_DIR	M	The directory where the installer will get installed. Example: `/root/MFTWebServices`
SSL_PORT	M	Port number used to communicate with the Jetty server.
POSTGRES_PORT	M	Port number used to communicate with the PostgreSQL database. **Note:** This property is mandatory if you are upgrading from IBM Connect:Direct Web Service **v6.0.0.4** to a higher version.
POSTGRESQL_PASSWORD	M	A Base64 password used to connect to the PostgreSQL database. Password considerations: • Password value 'postgres' is not allowed • Minimum and maximum length should be 8 characters and 80 characters respectively. • must contain at least 1 Alphabet and at least 1 non-Alphabet • Should not include blank spaces **Note:** This property is mandatory if you are upgrading from IBM Connect:Direct Web Service **v6.0.0.4** to a higher version.

Table 11. Attributes for UNIX-based Silent installation

Parameters	Mandatory/ Optional	Description
CERTIFICATE_TYPE	M	This attribute should store the following values: • 1 for a Default certificate • 2 for a Self-Signed Certificate
USER_INSTALL_DIR	M	The directory where the installer will get installed. Example: `/root/MFTWebServices`
SSL_PORT	M	Port number used to communicate with the Jetty server.
POSTGRES_PORT	M	Port number used to communicate with the PostgreSQL database. **Note:** This property is mandatory if you are upgrading from IBM Connect:Direct Web Service **v6.0.0.4** to a higher version.
POSTGRESQL_PASSWORD	M	An Base64 password used to connect to the PostgreSQL database. Password considerations: • Password value 'postgres' is not allowed • Minimum and maximum length should be 8 characters and 80 characters respectively. • must contain at least 1 Alphabet and at least 1 non-Alphabet • Should not include blank spaces **Note:** This property is mandatory if you are upgrading from IBM Connect:Direct Web Service **v6.0.0.4** to a higher version.

Table 12. Common conditional parameters and parameters not to be edited

Parameters	Mandatory/ Optional	Description
Read-Only parameters		
INSTALLER_UI	Use default value	Do not modify this attribute.
CHOSEN_INSTALL_SET	Use default value	Do not modify this attribute.
Conditional Parameters		
Keystore_PASS	O	This attribute should store a Base64 password to the Keystore where the certificate will be placed.
CONFIRM_PASS	O	This attribute should store the same value as Keystore_PASS attribute.
CERTIFICATE_LABEL	O	This attribute should store the certificate label or alias of the certificate entered in lower case.

Table 12. Common conditional parameters and parameters not to be edited (continued)		
Parameters	**Mandatory/ Optional**	**Description**
CERTIFICATE_EXPIRY_TIME	O	This attribute should store the expiry time in days. Value entered should be greater than 0.
COMMON_NAME	O	This attribute should store the Common Name of the certificate. Values not allowed: • Special characters • IP addresses, Port numbers • "http:// or https://"
ORGANISATION	O	This attribute should store an Organization Name that must be registered with some authority at the national, state, or city level. Use the legal name under which your organization is registered. Do not use an abbreviated form or use any of these symbols: ! @ # $ % ^ * ( ) ~ ? > < / \.
LOCALITY	O	This attribute should store the name of locality/ city where the organization is located.
STATE	O	This attribute should store the name of state where the organization is located.
COUNTRY	O	This attribute should store country code in the standard format where the organization is located.
EMAIL_ID	O	This attribute should store e-mail ID for the support group.

Logging in

What to do next

After you have successfully installed and configured the IBM Connect:Direct Web Service, the **Installation and Certificate Complete** screen displays URLs to access the Web Console and RESTful APIs and connect to IBM Connect:Direct.

These URLs are also available inside the README file under the installation directory.

Installation and Certificate Complete Screen Display

```
Installation and Certificate generation is complete.
ConnectDirectWebServices-Version has been successfully installed to: $USER_INSTALL_DIR$

ConnectDirectWebservices User Interface is available at :
https://<hostname:port>/cdws-ui/index.html
ConnectDirectWebservices API reference is available at :
https://<hostname:port>/cdws-doc/signOn.html
```

The following sections describe post installation steps.

Accessing Web Console

About this task

After you have installed and configured Web Services, log in to the Web Console to verify the installation and to administer the Connect:Direct Web Server.

Before you begin, ensure that the Web Console and Web server are running.

Procedure

1. Launch a web browser and enter the following URL to connect to the IBM Connect:Direct Web Console.

   ```
   https://<hostname:port>/cdws-ui/index.html
   ```

   The Web Console login page displays.
2. At the **Admin Functions** login tab, type the default ID and password (admin/admin) and click **Log in**.

   Administrator can now manage (add, modify, or remove) IBM Connect:Direct user nodes.
3. Log in to the **User Functions** tab to complete operational tasks such as, Add, Modify,or Delete Netmap entries or Initialization Parameters (initparms).

   Note: For security reasons, it is recommended that you change the default administrator password immediately after your first login. To change the administrator password, use **Reset Password** option under the **Admin** view.

   Note: For more information on how to use the Web Console to complete Connect:Direct tasks, click **Help**. Getting Started and feature videos are also available at YouTube> IBM Connect:Direct.

Accessing RESTful API interface

Launch any supported browser and enter the following URL to validate Connect:Direct RESTful APIs.

```
https://<hostname:port>/cdws-doc/signOn.html
```

For more information see, Chapter 5, “Using RESTful APIs with IBM Connect:Direct,” on page 55.

Password Reset for a Web Administrator

About this task

The Password Reset utility resets the password for a Web Admin user account for IBM Connect:Direct Web Service. The following information explains when you might need it, how to access the utility, and its parameters.

A Web Admin user account could be locked under circumstances such as:

- Failed login attempts
- Lapses in security policies preventing a Web Admin user from retaining the current password

To help resolve such situations use the Password Reset utility, `ResetDefaultCDWSAdminPassword`, available in the `/usr/bin` directory.

Note: Administrator privileges are required to execute the `ResetDefaultCDWSAdminPassword` script.

Note: With v6.0.0.5, password reset utility name is now changed to `ResetDefaultCDWSAdminPassword`. IBM Connect:Direct Web Service users who are on an older release that is, prior to v6.0.0.5 can continue to use `thecleanAdminRedisDataAdminKey`.

Procedure

Use the following commands to work with the Password Reset utility.

a. For IBM Connect:Direct Web Service installed on Windows, navigate to *$INSTALLATION_DIR$\bin* and execute:

```
ResetDefaultCDWSAdminPassword.bat
```

b. For IBM Connect:Direct Web Service installed on Linux, Solaris, AIX, or a ZLinux platform, navigate to *$CDWS_INSTALLATION_DIR$\bin* and execute:

```
./ResetDefaultCDWSAdminPassword.sh
```

Chapter 4. Configuration settings for IBM Connect:Direct Web Service

After you have completed installing the IBM Connect:Direct Web Service use the information defined in the following sections to complete configuration settings.

Establishing a Secure Connection between IBM Connect:Direct and IBM Connect:Direct Web Service

To establish a secure connection between IBM Connect:Direct Web Service and a IBM Connect:Direct server, make sure that you have added a IBM Connect:Direct certificate to the Web Services Truststore.

IBM Connect:Direct Web Service Key Store/Truststore supports base64-encoded ASCII certificates. It does not support binary-encoded X.509 certificates.

Pre-requisites

Obtain a IBM Connect:Direct Certificate and follow the steps given below to add it to Web Service's Truststore.

1. Navigate to the following directory:

```
% CDWS_Installation_Directory/jre/bin
```

2. Issue the following command and press **ENTER:**

```
Linux
./ikeycmd -cert -import -db <CD_Keystore> -target <CDWS_Keystore> -target_pw
<CDWS_KeystorePassword> -label <label of CD certificate> -pw <CD_KeystorePassword>

Windows
ikeycmd -cert -import -db <CD_Keystore> -target <CDWS_Keystore> -target_pw
<CDWS_KeystorePassword> -label <label of CD certificate> -pw <CD_KeystorePassword>
```

Note: Provide complete path of *<CD_Keystore>* and *<CDWS_Keystore>* if the Keystore is not present under the current folder.

Configuring Keystore/Truststore

To establish a secure connection between Connect:Direct, Connect:Direct Web Services and other clients, you need a Keystore and Truststore that contains necessary keys and digital certificates. IBM Connect:Direct Web Service, by default is installed and configured with a default Keystore/Truststore and certificates. To use a different Keystore and Truststore see, “Changing Keystore/Truststore using Web Console” on page 45 and “Changing Keystore/Truststore using a CLI procedure” on page 44.

Note: The following software/tool are required to implement some Keystore/Truststore management procedures described in the following sections.

- **OpenSSL**

  An SSL/TLS toolkit and cryptographic library. Download it from here.

- **IKEYCMD**

  A Java-based tool that can be used to manage keys, certificates and certificate requests. IKEYCMD is installed with the IBM Connect:Direct Web Service installation package at `/installdirectory/jre/bin`.

- **Keytool**

  Java **Keytool** is a key and certificate management utility. Keytool is installed with the IBM Connect:Direct Web Service installation package at `/installdirectory/jre/bin`.

Resetting the Keystore/Truststore/Key Certificate password and syncing with Connect:Direct Web Services

The default password for Truststore/Keystore is **changeit**. It is recommended to change this password after installation. To do this, follow these steps:

1. Use the following command to manually reset the Keystore/Truststore/Key Certificate password:

   Command to change Keystore/Truststore password

   ```
   keytool -storepasswd -Keystore <path_of_Keystore/Truststore_with_name>
   Enter Keystore password:
   New Keystore password:
   ```

   Command to change Key Certificate password

   ```
   keytool -keypasswd -Keystore <path_of_Keystore/Truststore_with_name> -alias
   <key_certificate_alias>
   Enter Keystore password:
   Enter key password for <key_certificate_alias>:
   New key password for <key_certificate_alias>:
   Re-enter new key password for <key_certificate_alias>:
   Password change successful for alias <key_certificate_alias>
   ```

2. Go to the following path: `<Installation_dir/mftws/BOOT-INF/classes>` and run `ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar` to sync the new password with CDWS.

   Note: Ensure that you have CDWS admin password ready and the database service is up before running the `ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar` utility.

3. Depending on your environment type, issue one of the following commands:
   - In Windows, stop and start *MFTWebservices* from the Task manager for changes to take effect.
   - In UNIX, issue the following command to stop and start *MFTWebServices* for changes to take effect.

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

Changing Keystore/Truststore using a CLI procedure

This procedure describes steps to follow to configure IBM Connect:Direct Web Service to use a different Keystore using a command line procedure.

Note: This procedure overrides the Web Services' default Keystore/Truststore settings.

1. Navigate to following directory:

```
$CDWS_installation_directory/mftws/BOOT-INF/classes
```

2. Run the **CDWS_installation_directory/jre/bin/java -jar ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar** and enter the following details:

```
Enter Admin Password:
Please Select from below options:
1. Type K and Enter to Change Keystore OR Sync Keystore Password with CDWS.
2. Type T and Enter to Change Truststore OR Sync Truststore Password with CDWS.
3. Type C and Enter to Sync Key Certificate Password with CDWS.
4. Type Q and Enter to Exit.
Enter your Choice: K
Enter the complete path of Keystore: (including fileName(.jks)):
Enter Keystore Password:
Confirm Password:
Keystore details updated successfully
Press Y to Continue OR Q to Exit:Q
Exiting the Utility.
```

Note:

- Ensure that you have CDWS admin password ready and the database service is up before running the `ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar` utility.
- If changed keystore contains key certificate with different password, you must sync the new password with CDWS using this utility.

3. To update the **application.properties** file navigate to following directory:

```
% cd $Installation_directory/mftws/BOOT-INF/classes
```

4. Edit **application.properties** file and replace the value *server.ssl.key-alias* with <Label of Certificate> to be used by Connect:Direct Web Services.
5. Issue the following commands for changes to take effect.
   - In Windows environment, stop and start `MFTWebservices` from the Task manager for changes to take effect.
   - In UNIX environment, issue the following command to stop and start `MFTWebServices.`

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

Changing Keystore/Truststore using Web Console

About this task

This procedure describes steps to follow to configure IBM Connect:Direct Web Service to use a different Key Store. Before you begin the procedure, you must ensure that the Keystore is located on the same machine where IBM Connect:Direct Web Service is installed.

Procedure

1. Login to the Web Console as an Admin user.
2. Click **Certificates** > **Change Keystore** to display Keystore configuration properties.
3. Enter the complete absolute path of the changed **Keystore**.

   Note: You must not provide an empty Keystore path.
4. Enter the changed Keystore password in **Keystore Password**.

   Note: The encryption key that will be used to encrypt the **Keystore Password** is automatically generated from backend.
5. Enter the **Key Certificate Password**. For release 6.1.0.4 and later Keystore and Key Certificate passwords can be different. However, all the Key Certificates must have the same password.

To configure IBM Connect:Direct Web Service to use a different Truststore, click **Certificates** > **Change trust store** and follow the same procedure as described above. For a UI walk-through of this feature see, YouTube> IBM Connect:Direct.

Add/Import a certificate(s) to IBM Connect:Direct Web Service Keystore/ Trust Store

Follow the procedure given below to add a certificate into an existing Keystore/Truststore.

With v6.1, IBM Connect:Direct Web Service now extends its web console capabilities to support import and export certificates into an existing Key Store/Truststore. To use this feature, login as an Admin user and click **Certificates**> **Key Certificate/Trust Certificate** > **Import**. For a UI walk-through of this feature see, YouTube> IBM Connect:Direct.

Note: IBM Connect:Direct Web Service Key Store/Truststore supports base64-encoded ASCII certificates. It does not support binary-encoded X.509 certificates.

For importing certificate(s) from CLI follow these steps:

1. Navigate to following directory:

```
% cd $Installation_directory/jre/bin
```

2. Follow the steps below to import the certificate into Keystore.

   a. Execute the following OpenSSL command to create a **PKCS12** (.**p12**) file. Administrator is prompted to enter **key.pem** pass phrase if the key is found to be encrypted.

```
openssl pkcs12 -export -name <Certificate_Alias_Name> -in <PEM_Certificate> -inkey
<key.pem> -out <Keystore_NAME>.p12
Enter pass phrase for key.pem:
Enter Export Password:
Verifying - Enter Export Password:
```

   b. Issue the following commands to import the certificate into Keystore.

      Input parameter considerations:

      - **<sourceKeystore>** value should match <**Keystore_NAME>**
      - **<sourceKeystorePassword>** value should match the Export password supplied in step above

```
UNIX
./ikeycmd -cert -import -db <sourceKeystore> -target <CDWS_Keystore> -target_pw
<CDWS_KeystorePassword> -label <Certificate_Alias_Name> -pw
<sourceKeystorePassword>

Windows
ikeycmd -cert -import -db <sourceKeystore> -target <CDWS_Keystore> -target_pw
<CDWS_KeystorePassword> -label <Certificate_Alias_Name> -pw
<sourceKeystorePassword>
```

   c. Edit **application.properties** file and change the value of `server.ssl.key-alias` property with `<Certificate_Alias_Name>` to be used by Connect:Direct Web Services.

   d. Issue the following commands for changes to take effect.

      - For Windows, stop and start *MFTWebservices* from the Task manager for changes to take effect.
      - For UNIX, issue the following command to stop and start *MFTWebServices*:

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

3. Adding a Trusted certificate.

a. Invoke the following commands to add a Trusted Certificate:

```
UNIX
./ikeycmd -cert -add -db <CDWS_Truststore> -pw <CDWS_TruststorePassword> -label
<LabelName> -file <Certificate to be added>

Windows
ikeycmd -cert -add -db <CDWS_Truststore> -pw <CDWS_TruststorePassword> -label
<LabelName> -file <Certificate to be added>
```

b. Issue the following commands for changes to take effect.

- For Windows, stop and start *MFTWebservices* from the Task manager for changes to take effect.
- For UNIX, issue the following command to stop and start *MFTWebServices* for changes to take effect:

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

Note: IBM Connect:Direct Web Service, provides two options to configure Keystore/Truststore at the installation time:

- For default keystore, use password changeit for keystore and keycert password.
- For self-signed certificate, use the password provided at the time of installation for keystore as well as key certificate.

Attention: The password change of Keystore/Truststore is not possible using webconsole. If you change Keystore/Truststore password then you must sync the changed password with CDWS using `ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar`.

Import Key Certificate with different password using Web Console

You won't be able to upload a Key certificate with password different than existing key certificate password via IBM Connect:Direct Web Service Web Console. If you still want to use those certificates, you have to Import Key Certificate with different passwords. To do this from web console:

1. Login as an Admin user.
2. Go to **Certificates**> **Key Certificate**> **View**> **Delete all existing Key Certificates from existing Keystore**.
3. Go to **Certificates**> **Key Certificate/Trust Certificate** > **Import** and import new Key Certificate in that Keystore in the same session.
4. Edit `application.properties` file and change the value of `server.ssl.key-alias` property with Certificate Label to be used by Connect:Direct Web Services.
5. Depending on your environment type, issue one of the following commands:
   - In Windows, stop and start *MFTWebservices* from the Task manager for changes to take effect.
   - In UNIX, issue the following command to stop and start *MFTWebServices* for changes to take effect.

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

Alternative approach

If you do not wish to delete the old certificates, rather change their passwords and import the new certificates, follow these steps:

1. Update the Key Certificate password using following keytool command:

```
keytool -keypasswd -Keystore <path_of_Keystore/Truststore_with_name> -alias
<key_certificate_alias>
```

```
Enter Keystore password:
Enter key password for <key_certificate_alias>:
New key password for <key_certificate_alias>:
Re-enter new key password for <key_certificate_alias>:
Password change successful for alias <key_certificate_alias>
```

2. Run following utility to sync the new password with CDWS:

```
java -jar ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar
Enter Admin Password:
Please Select from below options:
1. Type K and Enter to Change Keystore OR Sync Keystore Password with CDWS.
2. Type T and Enter to Change Truststore OR Sync Truststore Password with CDWS.
3. Type C and Enter to Sync Key Certificate Password with CDWS.
4. Type Q and Enter to Exit.
Enter your Choice: K
Enter the complete path of Keystore: (including fileName(.jks)):
Enter Keystore Password:
Confirm Password:
Keystore details updated successfully
Press Y to Continue OR Q to Exit:Q
Exiting the Utility.
```

Attention: Use the above command to update CDWS with new password if you forgot Keystore/ Truststore password. However, you cannot recover Keystore password because of security reasons.

3. Depending on your environment type, issue one of the following commands:
   - In Windows, stop and start *MFTWebservices* from the Task manager for changes to take effect.
   - In UNIX, issue the following command to stop and start *MFTWebServices* for changes to take effect.

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

4. Follow the steps mentioned in Add/Import a certificate(s) to IBM Connect:Direct Web Service Keystore/ Truststore .

Adding a new Keystore and Key Certificate

If you wish to import a Key Certificate with a different password, you can add a new Key Store with a new Key Certificate:

1. Create a new Keystore with a new Key Certificate.
2. Change the Keystore from Web Console or using following utility:

```
java -jar ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar
Enter Admin Password:
Please Select from below options:
1. Type K and Enter to Change Keystore OR Sync Keystore Password with CDWS.
2. Type T and Enter to Change Truststore OR Sync Truststore Password with CDWS.
3. Type C and Enter to Sync Key Certificate Password with CDWS.
4. Type Q and Enter to Exit.
Enter your Choice: K
Enter the complete path of Keystore: (including fileName(.jks)):
Enter Keystore Password:
Confirm Password:
Keystore details updated successfully
Press Y to Continue OR Q to Exit:Q
Exiting the Utility.
```

3. Edit `application.properties` file and change the value of `server.ssl.key-alias` property with Key Certificate Alias to be used by Connect:Direct Web Services.
4. Depending on your environment type, issue one of the following commands:
   - In Windows, stop and start *MFTWebservices* from the Task manager for changes to take effect.
   - In UNIX, issue the following command to stop and start *MFTWebServices* for changes to take effect.

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

Sample Use Case: Adding a PEM Certificate with key into IBM Connect:Direct Web Service Keystore

Follow the procedure given below to add a PEM formatted (.crt) certificate into Web Service's Key Store.

With v6.1, IBM Connect:Direct Web Service extends its web console capabilities to support Keystore/Truststore management. For a UI walk-through on how to add a PEM certificate into IBM Connect:Direct Web Service Keystore see, YouTube> IBM Connect:Direct.

Ensure that you've installed OpenSSL before you begin configuring the Keystore/Truststore. For the OpenSSL 3.0.0 release, and later releases derived from that, the Apache License v2 applies. Any release made before OpenSSL 3.0.0, the dual OpenSSL and SSLeay license applies.

1. Obtain the PEM-encoded certificate.
2. Execute the following OpenSSL command to create a **PKCS12** (.**p12**) file.

```
openssl pkcs12 -export -name <Certificate_Alias_Name> -in <PEM_Certificate> -inkey
<PEM_KEY> -out <Keystore_NAME>.p12
```

3. Execute the following command to import the **PKCS12** (.**p12**) certificate into a JKS Keystore.

```
keytool -importKeystore -destKeystore <NEW_JKS_Keystore_NAME> -deststoretype jks
-srcKeystore <PKCS12_KESTORE_NAME> -srcstoretype pkcs12 -alias <Certificate_Alias_Name>
```

4. Import the CA-signed certificate into the IBM Connect:Direct Web Service Keystore.

```
OS: Unix
./ikeycmd -cert -import -db <NEW_JKS_Keystore_NAME> -target <CDWS_Keystore> -target_pw
<CDWS_KeystorePassword>-label <Certificate_Alias_Name> -pw
<NEW_JKS_Keystore_PASSWORD>


OS: Windows
ikeycmd -cert -import -db <NEW_JKS_Keystore_NAME> -target <CDWS_Keystore> -target_pw
<CDWS_KeystorePassword>-label <Certificate_Alias_Name> -pw
<NEW_JKS_Keystore_PASSWORD>
```

5. Edit **application.properties** file and change the value of `server.ssl.key-alias` property with `<Certificate_Alias_Name>` to be used by Connect:Direct Web Services.
6. Execute the `ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar` file available at `mftws/BOOT-INF/classes`.

```
java -jar ChangeKeystoreTruststoreAndUpdatePassword-0.1.jar
Enter Admin Password:
Please Select from below options:
1. Type K and Enter to Change Keystore OR Sync Keystore Password with CDWS.
2. Type T and Enter to Change Truststore OR Sync Truststore Password with CDWS.
3. Type C and Enter to Sync Key Certificate Password with CDWS.
4. Type Q and Enter to Exit.
Enter your Choice: K
Enter the complete path of Keystore: (including fileName(.jks)):
Enter Keystore Password:
Confirm Password:
Keystore details updated successfully
Press Y to Continue OR Q to Exit:Q
Exiting the Utility.
```

7. Depending on your environment type, issue one of the following commands:
   - In Windows, stop and start *MFTWebservices* from the Task manager for changes to take effect.

- In UNIX, issue the following command to stop and start *MFTWebServices* for changes to take effect.

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

Configuring application.properties

To configure property files that control system-wide Connect:Direct Web Services properties follow the steps given below:

1. Navigate to the following directory:

```
% cd $Installation_Directory/mftws/BOOT-INF/
classes
```

2. Modify *application.properties* and save after making necessary changes.

Configuration Items	Description
accessKey.connectionTimeInactivityLimit	Configure access token inactivity time in minutes Default: 60 min
accessKey.connectionTimeMaxLimit	Configure access token maximum timeout in minutes Default: 1440 min
accessKey.maxConnectionNumber	Configure maximum number of Connect:Direct node connections Default value is 100
cdserver.http.enabled	By default a HTTPS connection is enabled. Set this to TRUE to enable a HTTP connection. Default: False
cdserver.http.port	To configure HTTP Port Default: 9090
certificate.finger.print	A unique identifier to identify a certificate in a user-friendly manner. Default: null
server.ssl.enabled-protocols	To enable/disable legacy protocols. Where protocols can be TLSv1, TLSv1.1, TLSv1.2 Default: TLSv1.2
server.ssl.key-alias	Alias that identifies the key in the Keystore Default: ibmconnectdirectwebservices
server.port	Port on which Connect:Direct Web Services is running. Default value: 9443 This is a Web Server secure port.

Configuration Items	Description
spring.datasource.url	To configure Connect:Direct Web Services to communicate with Postgres server running on a given port. Default value: 5432 **Note:** This value is set during installation and should not be modified without due consideration.
statistics.limit	Maximum statistics records to be displayed. -1 displays the entire stat listing.
statistics.search.limit	This property limits the number of transfer statistics results that are displayed in Web Console>**Statistics** view when a user applies any filters. Search limits improve overall server performance by limiting how many entries are returned when a user attempts a filtered search through the transfer statistics. This property is set to a default of 2000.
thread.pool.max.size	Defines the maximum tasks of threads that can ever be created. Default: 100
thread.pool.core.size	Minimum number of tasks to keep alive without timing out. Default: 100
thread.pool.queue.size	Number of tasks that are queued while all other threads are in use. Default: 100

3. Issue the following commands depending on environment type.
   - In Windows environment, stop and start *MFTWebservices* from Task manager for changes to take effect.
   - In UNIX environment, issue the following command to stop and start *MFTWebServices*:

```
% ./$CDWS_INSTALLATION_DIR$/bin/stopWebservice.sh
% ./$CDWS_INSTALLATION_DIR$/bin/startWebservice.sh
```

Certificate-based Authentication

IBM® Connect:Direct Web Services uses the following two client authentication methods to establish the identity of the requesting REST client and determine whether that client is authorized to connect to Connect:Direct server using the credentials supplied:

- Username/password-based authentication
- Certificate-based authentication

Passwords configured are set to expire at some interval and must be changed. Any time the password is changed it results in tedious password management routine in a large deployment.

To ease password management routines for REST client over a TLS connection, Connect:Direct Web Services extends its client authentication process to allow certificate-based authentication.

The following sections explore certificate-based authentication in the context of Web Service's RESTful API interface.

Configuring Certificate based Authentication

About this task

The following sections list tasks that you need to perform by interface, to enable certificate-based authentication in your Connect:Direct deployment.

Procedure

1. Configuring **REST Client** for certificate-based authentication
   a. Import Connect:Direct Web Service's self-signed or CA certificate into REST client's Truststore.
   b. Create/Import REST client's identity certificate that is, Self-signed/CA-signed certificate into the client's Keystore.
   c. Add the following header parameter when you form a Web Service JSON request with the REST client:

      ```
      CertificateAuthentication=true
      ```

2. Configuring **Connect:Direct Web Services** for certificate-based authentication
   a. Import REST client's self-signed or CA certificate into Connect:Direct Web Service's Truststore.
   b. Add REST client certificate fingerprint in `application.properties` file in the following format.

      If the **Common Name**=myvalidcertificate.com and

      Fingerprint=7F:87:9C:53:4A:EA:89:D6:3F:0D:31:15:12:F4:89:ED:0A:1A:A6:F6:
      8B:85:3B:72:FF:2F:44:70:00:59:57:7B

      Then `certificate.finger.print` value should be:

      `certificate.finger.print= myvalidcertificate.com; 7F:87:9C:53:4A:EA:89:`
      `D6:3F:0D:31:15:12:F4:89:ED:0A:1A:A6:F6:8B:85:3B:72:FF:2F:44:70:00:59:57:7B`

      Note: To obtain fingerprint value issue commands defined below:

      Using OpenSSL

```
openssl x509 -noout -fingerprint -sha256 -inform pem -in cert.pem
(Only SHA-256 is supported)
```

      Using iKeyMan CLI interface

```
./ikeycmd -cert -details -db /<CDWS_Installation_Directory>/<cdws_Keystore> -label <username>
 -pw <password>
Label: myvalidcertificate
Key Size: 2048
Version: X509 V3
Serial Number: 5D 36 B8 9D
Issued by: CN=myvalidcertificate.com, O=Orgname, L=locationName, ST=StateName, C=CountryName
Subject: CN=myvalidcertificate.com, O=Orgname, L=locationName, ST=StateName, C=CountryName
Valid: From: Tuesday, July 23, 2019 1:04:53 PM IST To: Thursday, July 22, 2021 1:04:53 PM IST
Fingerprint:
    SHA1: AC:59:F7:0F:AC:EB:B0:1F:43:08:BF:D6:57:1E:4A:7B:60:2C:78:58
    SHA256: D5:6B:45:97:F9:E1:84:5E:B9:D4:2B:99:32:4A:69:8E:12:C1:53:82:BD:7B:F0:E7:ED:F6:8B:5A:
            29:9C:E2:B6
    HPKP: mzJLrZbXK0B9dZ+BmX+vwCVvl2YTPOnei144ubbAZCQ=
```

c. Add/Import Connect:Direct Server's self-signed/CA certificate into Connect:Direct Web Service's Truststore. With v6.1, IBM Connect:Direct Web Service now extends its web console capabilities to support import and export certificates into an existing Truststore. To use this feature, login as an Admin users and click **Certificates**> **Trust Certificate** > **Import**.

3. Configure **Connect:Direct Server** to enable certificate-based authentication. For more information see, Configure Certificate Authentication for Client API Connections.

   Note: Restart Connect:Direct Web Services for changes to take effect.

   Example cURL command format

   Invoke cURL commands in the following format, when using certificate-based authentication method, to sign into Connect:Direct Server:

   Example 1

```
curl -s -i -H 'CertificateAuthentication:true' -H 'X-XSRF-TOKEN:Y2hlY2tpdA==' -H
"Content-Type: application/json" -X POST -d '{"ipAddress":"'<CD_Node_IP>'",
"protocol":"<TLS1.2|TLS1.1|TLS1.0|SSL>","port":'<Port>'}'
--cacert /home/user/cdws_cert/ibmcdws.pem --cert ./cert.pem --key key.pem
https://<CDWS_HOSTNAME>:<CDWS_Port>/cdwebconsole/svc/signon
```

   Example 2

```
curl -s -i -H 'CertificateAuthentication:true' -H 'X-XSRF-TOKEN:Y2hlY2tpdA==' -H
"Content-Type: application/json" -X POST -d '{"ipAddress":"'<CD_Node_IP>'",
"protocol":"<TLS1.2|TLS1.1|TLS1.0|SSL>","port":'<Port>'}'
--cacert /home/user/cdws_cert/ibmcdws.pem
--cert ./ssl-client.p12 https://<CDWS_HOSTNAME>:<CDWS_Port>/cdwebconsole/svc/signon
```

Connect:Direct Web Services Logs

IBM Connect:Direct Web Services creates installation and RESTful API activity logs for tuning and diagnostic purpose.

This section describes four types of log families in Connect:Direct Web Services:

1. **REST API logs**

   The REST API log is a repository of error conditions that are detected on each node, as well as operational events such as User Sign-In and Sign-Out.

   To edit log4j.properties for Framework and REST API logs to gather diagnostic information, see “Configuring Logs” on page 54.

2. **AIJ logs**

   The AIJ logs contain information that helps you to troubleshoot the connection issues related to CDAIJ and Connect:Direct node. It contains commands issued with results.

These logs are set to OFF by default, to enable recording AIJ logs, set `cdaij.trace` to TRUE in `application.properties`.

3. **Installer logs**

   Help diagnose and troubleshooting installer related abnormal events.

The activity logs are stored inside the following folders located under your installation folder.

Table 13.

Log Family	Location

Installer logs	**Windows**
	`$CDWS_INSTALLATION_DIR$/logs`
	UNIX
	`CDWS_INSTALLATION_DIR$/UninstallerData/logs`

CDWS and AIJ logs	**Windows** `$CDWS_INSTALLATION_DIR$/RestLogs` **UNIX** `$CDWS_INSTALLATION_DIR$/RestLogs`

Configuring Logs

Depending on your logging requirements you can configure detailed logs supported by IBM Connect:Direct Web Services using the common log properties file, **log4j2.yaml**.

The **log4j2.yaml** file can be found in, `$CDWS_INSTALLATION_DIR$/mftws/BOOT-INF/classes/`.

Example **log4j2.yaml** files

```
configuration:
    properties:
    property:
      # Common log properties to change as per user requirements
      # Log level settings control the quantity of messages sent to product trace logs
      # Web Services supports the following log levels: ERROR, INFO, DEBUG, ALL, and OFF
      - name: RestLogLevel
        value: "INFO"
      - name: RestLogFilePath
        value: "../RestLogs"
      - name: RestLogPattern
        value: "%d{yyyy-MM-dd HH:mm:ss} %-5p - %m%n"
```

Log level settings are controlled by RestLogLevel property. Possible values are ERROR, INFO, DEBUG, ALL, and OFF.

Note: RestLogLevel property must be set to ‘DEBUG’ to start recording logs.

After completing configuring the logs restart the Connect:Direct Web Services for changes to come into effect.

Chapter 5. Using RESTful APIs with IBM Connect:Direct

IBM Connect:Direct Web Service RESTful APIs enables external business applications to integrate with IBM Connect:Direct. The Web Services RESTful APIs support Read, Create, Update/Replace, and Delete (CRUD) operations on resources using standard HTTP GET, POST, PUT, and DELETE methods and output resource data in a JavaScript Object Notation (JSON) format.

IBM Connect:Direct Web Service provide APIs for corresponding Connect:Direct functions such as, submitting a file transfer process, process control, fetching statistics , netmap update for remote nodes , user authorization , user proxy , secure plus configuration, and controlling tracing.

The RESTful APIs can be directly invoked through the following means so as to seamlessly integrated with external business applications:

- **Browser Interface**
  - Web Services RESTful API documentation can be accessed in a web browser using the Swagger UI.
  - Swagger is REST API documentation framework that helps developers design, build and consume the RESTful Web services.
- **REST Clients** (e.g POSTMAN)
- **Command Line Interface (cURL)**
- **Scripts-based RESTful API invocation**

Note: Ensure a secure connection with Connect:Direct server before executing the Secure Plus APIs. For more information and example scenarios see the sections that follow.

Using Browser Interface to validate RESTful APIs

Procedure

Follow the procedure below to access the Web Services RESTful APIs via. a browser interface.

- IBM Connect:Direct Web Service automatically generates RESTful API documentation during API creation.
- RESTful API documentation lists all RESTful API resources and operations that can be called on those resources.

1. Click the URL **`https://<CDWS_IPAddress:Port>/cdws-doc/signOn.html.`**

2. The page prompts for the following details:

- *IP/Hostname*: Enter the Connect:Direct Server IP address
- *Port*: Enter the Connect:Direct Server Port
- *UserID*: Enter the User ID used to connect to the Connect:Direct Server
- *Password*: Enter the Password to connect to the Connect:Direct Server
- *Protocol*: Enter the connection protocol method. Possible values could be TCPIP, SSL, TLS1.0, TLS1.1, TLS1.2.

3. Click **Sign In**.

Using REST Client to validate RESTful APIs

A third-party application, such as Postman, can be used to make REST API calls. Postman is available for download at https://www.getpostman.com/ and is used in the example procedures in the following sections.

Sign On

Sign On is required to use all IBM Connect:Direct Web Service RESTful APIs.

Note: Ensure that the authorization header is included each time a RESTful API is invoked for authentication.

Sign On procedure

1. Make a **POST** request to the URL **https://<CDWS_IPAddress:Port>/cdwebconsole/svc/signon**.
2. Encode the IBM® Connect:Direct user name and password into Base64. To encode the username and password use URL **https://<CDWS_IPAddress:Port>/cdws-doc/base64encode.html**.

   For example, encoded password for *admin:password123* becomes *YWRtaW46cGFzc3dvcmQxMjM=*.
3. Set the Request Header to:

```
Authorization
Basic <Encoded_Password from step 2 e.g. YWRtaW46cGFzc3dvcmQxMjM=>

Content-Type
application/json; charset=iso-8859-1

X-XSRF-TOKEN
Y2hlY2tpdA== (fixed for the first time)
```

4. Set the Request body and submit the request

```
{
"ipAddress":"CDNODE IP",
"port":1363,
"protocol":"TCPIP || TLS1.0 || TLS1.1 || TLS1.2"
}
```

5. Complete the Request body as follows:

```
POST /cdwebconsole/svc/signon HTTP/1.1
Host: <CDWS_IPAddress:Port>
Content-Type: application/json; charset=utf-8
X-XSRF-TOKEN: Y2hlY2tpdA==
Authorization: Basic QWRtaW5pc3RyYXRvcjpNc3dAMTIzIQ==
Cache-Control: no-cache

{
    "ipAddress":"172.20.186.35",
    "protocol":"tcpip",
    "port":1363
}
```

6. Response message received as follows:

```
[
    {
        "messageCode": 200,
        "message": "Signon is successful",
        "version": "CDWS_VERSION",
        "nodeName": "CD_NODE_NAME"
    }
]
```

7. User receives an Authorization and XSRF token in response header that can be used to execute other RESTful APIs.

```
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuMzU6MTM2MzplMDI
0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1NTcxMjcyMTJ9.ME_mni-wgm
rzVL214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3JYo1REs1w
XSRF:
809ab7e8-c6be-41ac-84f1-b4f8db246d9e
```

Example 1: Submit a Process using REST API

Workflow

The following example describes steps to execute a Submit Process Control RESTful API using POST method.

1. Call the **SignOn** API and get the authorization token and XSRF-TOKEN token from the header in the response.

```
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYu
MzU6MTM2MzplMDI0Y
jAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1NTcxMjcyMTJ9.ME_mni-wgmrzVL
214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3JYo1REs1w

XSRF:
809ab7e8-c6be-41ac-84f1-b4f8db246d9e
```

2. Submit a **POST** request at the following URL:

```
https://<CDWS_IPAddress:Port>/cdwebconsole/svc/processcontrolcriterias
```

3. Call the API with the Authorization header:

```
Authorization:<Authorization_Token_From_Step_1>
```

4. Call the API with the XSRF header as X-XSRF-TOKEN:

```
X-XSRF-TOKEN : <XSRF_Token_From_Step_1>
```

5. Set the content type to:

```
Content-Type: application/json; charset=utf-8
```

6. Set the request body to:

```
{
  "processFile": "C:\Users\Administrator\Desktop\test.cdp"
}
```

7. Complete request body as follows:

```
POST /cdwebconsole/svc/processcontrolcriterias HTTP/1.1
Host: <CDWS_IPAddress:Port>
Content-Type: application/json
X-XSRF-TOKEN: 809ab7e8-c6be-41ac-84f1-b4f8db246d9e
Authorization: eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4x
ODYuMzU6MTM2MzplMDI0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1
NTcxMjcyMTJ9.ME_mni-wgmrzVL214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-z
gS6J8JiL2GJrG3JYo1REs1w
Cache-Control: no-cache
{
"processFile": "C:\\Users\\Administrator\\Desktop\\CDWS_AutoInstall\\cd_proc
ess_dir \\test.cdp"
}
```

8. Response received as follows:

```
{
 "messageCode": 201,
 "message": "The process has been successfully submitted with
  processNumber '126'"
}
```

Example 2: Select Statistics for a Process using REST API

Workflow

The following example describes steps to execute a Select Statistics Services RESTful API using GET method.

1. Call the **SignOn** API and get the authorization token and XSRF-TOKEN token from the header in the response.

```
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuMzU6MTM2MzplMD
I0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1NTcxMjcyMTJ9.ME_mni-
wgmrzVL214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3JYo1REs1w

XSRF:
809ab7e8-c6be-41ac-84f1-b4f8db246d9e
```

2. Submit a **GET** request at the following URL with process number generated in “Example 1: Submit a Process using REST API” on page 57:

```
https://<CDWS_IPAddress:Port>/cdwebconsole/svc/selectstatistics?
processNumber= 126
```

3. Call the API with the Authorization header:

```
Authorization: <Authorization _Token_From_Step_1>
```

4. Call the API with the XSRF header as X-XSRF-TOKEN:

```
X-XSRF-TOKEN : <XSRF_Token_From_Step_1>
```

5. Set the content type to:

```
Content-Type: application/json; charset=utf-8
```

6. Complete the request body as follows:

```
Get /cdwebconsole/svc/selectstatistics?processNumber=126 HTTP/1.1
Host: <CDWS_IPAddress:Port>
Content-Type: application/json
X-XSRF-TOKEN: 809ab7e8-c6be-41ac-84f1-b4f8db246d9e
Authorization: eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4
xODYuMzU6MTM2MzplMDI0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOj
E1NTcxMjcyMTJ9.ME_mni-wgmrzVL214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk
-zgS6J8JiL2GJrG3JYo1REs1w
Cache-Control: no-cache
```

7. Response received as follows:

```
 {
        "stopTime": "Mon May 06 12:41:32 IST 2019",
        "submitNode": "CDWLT-025",
        "msgShortText": "The submit of the process succeeded.",
        "recordCategory": "CAPR",
        "startTime": "Mon May 06 12:41:32 IST 2019",
        "recordId": "SUBP",
        "conditionCode": 0,
        "submitter": "Administrator",
        "messageId": "LCCA013I",
        "logDateTime": "Mon May 06 12:41:32 IST 2019",
        "processName": "PP",
        "processNumber": 127,
        "secondaryNode": "CDWLT-025"
    }
```

Sign Out

Workflow

Sign Out is required to close an active session.

1. Call the **SignOn** API and get the authorization token and XSRF-TOKEN token from the header in the response.

```
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuMzU6MTM2MzplMDI0Y
jAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1NTcxMjcyMTJ9.ME_mni-wgmrzVL
214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3JYo1REs1w
XSRF:
809ab7e8-c6be-41ac-84f1-b4f8db246d9e
```

2. Submit a DELETE request at the following:

```
URL https://<CDWS_IPAddress:Port>/cdwebconsole/svc/SignOut
```

3. Call the API with the Authorization header:

```
Authorization: <Authorization Token_From_Step_1>
```

4. Call the API with the XSRF header as X-XSRF-TOKEN:

```
X-XSRF-TOKEN : <XSRF_Token_From_Step_1>
```

5. Set the content type to:

```
Content-Type: application/json; charset=utf-8
```

6. Set the request body as follows:

```
{
"userAccessToken": "<Access_Token_From_Step_1>"
}
```

7. Complete the request body as follows:

```
Delete /cdwebconsole/svc/signout HTTP/1.1
Host: 172.20.186.34:9443
Content-Type: application/json
Authorization: eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuMz
U6MTM2MzplMDI0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1NTcxMjcyMTJ9.
ME_mni-wgmrzVL214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3JYo1R
Es1w
X-XSRF-TOKEN: 809ab7e8-c6be-41ac-84f1-b4f8db246d9e
Cache-Control: no-cache
{"userAccessToken": "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xO
DYuMzU6MTM2MzplMDI0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1NTcxMjcy
MTJ9.ME_mni-wgmrzVL214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3J
Yo1REs1w"}
```

8. Response received as follows:

```
 {
    "signOut": true,
    "userId": "Administrator"
}
```

Using command line (cURL) to validate RESTful APIs

cURL is a command-line tool for getting or sending files using URL syntax. The following procedure describes the format and syntax used when making Web Services REST API requests with cURL.

Listed below are scripts validated on the following cURL executable versions by OS:

Table 14. Supported cURL executable versions

OS	cURL executable version
Windows	v7.64.1
Linux	v7.29.0
Solaris	v7.59.0
zLinux	v7.29.0
AIX	v7.64.1

SignOn

About this task

Sign On is required to use all IBM Connect:Direct Web Service RESTful APIs.

Note: Ensure that the authorization header is included each time a RESTful API is invoked for authentication.

Procedure

1. Encode the IBM® Connect:Direct user name and password into Base64. To encode the username and password use URL in the following format:

```
https://<CDWS_IPAddress:Port>/cdws-doc/base64encode.html
```

2. Set the Request Header to:

```
Authorization
Basic <Encoded_Password>' -H '

Content-Type
application/json" -X POST -d
'{"ipAddress":"CDNodeIp","protocol":" TCPIP || TLS1.0 || TLS1.1 ||
TLS1.2","port":'1363'}'-k

X-XSRF-TOKEN
<Y2hlY2tpdA== (fixed for signon request )>'-H
```

3. Complete the Request body as follows:

```
curl -s -i -H ' Authorization: Basic <Encoded_Password>' -H
'X-XSRF-TOKEN:<Y2hlY2tpdA== (fixed for signon request )>' -H
"Content-Type: application/json"-X POST -d '{"ipAddress":"CDNodeIp",
"protocol":" TCPIP || TLS1.0 || TLS1.1 ||TLS1.2","port":'1363'}'-k
https://<CDWS_IPAddress:Port>/cdwebconsole/svc/signon
```

4. Response message received as follows:

```
HTTP/1.1 200 OK
Date: Tue, 14 May 2019 07:46:03 GMT

Set-Cookie:
XSRF-TOKEN=1086bae5-3073-4a8f-afbe-b3d3199d6812;Path=/;Secure;

HttpOnly _csrf:
1086bae5-3073-4a8f-afbe-b3d3199d681

osType: WINDOWS

Content-Type:application/json;charset=iso-8859-1

Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuNz
Q6MTM2Mzo1NmIwNDFkZS0yYmI1LTQyMTUtOGI4OC02ZjMwYzU1NmE2NTUiLCJleHAiOjE1
NTc4MjIzNjN9.z2la7UyfICFWkMtaO8xJ6kv2Llth-u8kRLXH8tIOTsKm_82jeNE-Rdl2q
fQGUlRdl2qifQGUlT4gOs9BhyWAN4JGPde5Fo5g

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Cache-Control: no-cache, no-store,must-revalidate,max-age=0

Pragma: no-cache

Strict-Transport-Security: max-age=31536000 ;includeSubDomains

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff Content-Security-Policy: default-src 'self'

X-Content-Type-Options:nosniff

X-Frame-Options: DENY

Set-Cookie:JSESSIONID=node01jk2nfvlk2nyjq4ubgnot3j7r4.node0;Path=/;Secure;HttpOnly

Content-Length:70
[
    {
        "messageCode": 200,
        "message": "Signon is successful",
        "version": "CDWS_VERSION_NO",
        "nodeName": "CD_NODE_NAME"
    }
]
```

5. User receives an Authorization. jsessionid, and XSRF token in response header that can be used to execute other RESTful APIs.

```
XSRF-TOKEN=1086bae5-3073-4a8f-afbe-b3d3199d6812;Path=/;Secure;
HttpOnly _csrf:1086bae5-3073-4a8f-afbe-b3d3199d6812

Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJhZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuNz
Q6MTM2Mzo1NmIwNDFkZS0yYmI1LTQyMTUtOGI4OC02ZjMwYzU1NmE2NTUiLCJleHAiOjE1
NTc4MjIzNjN9.z2la7UyfICFWkMtaO8xJ6kv2Llth-u8kRLXH8tIOTsKm_82jeNE-Rdl2
qifQGUlRdl2qifQGUlT4gOs9BhyWAN4JGPde5Fo5g

JSESSIONID=node01jk2nfvlk2nyjq4ubgnot3j7r4.node0;Path=/;Secure;HttpOnly
```

Example 1: Submit a Process using cURL

About this task

The following example describes steps to execute a Submit Process Control RESTful API using cURL.

Procedure

1. Call the **SignOn** API and get the authorization token, jsessionID, and XSRF-TOKEN token from the header in the response.

```
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuMzU6
MTM2MzplMDI0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHA
iOjE1NTcxMjcyMTJ9.ME_mniwgmrzVL214ijhxNzU-bgHw9bv-Ktz8WL84ljpEYtgm89jf
H7ehspyk-zgS6J8JiL2GJrG3JYo1REs1w

XSRF:
809ab7e8-c6be-41ac-84f1-b4f8db246d9e

JSessionID:
node04p0v71bx6q46u2qthvr32htv3.node0
```

2. Submit a **cURL** request at the following URL

```
https://<CDWS_IPAddress:Port>/cdwebconsole /svc/processcontrolcriterias
```

3. Call the API with the XSRF header as X-XSRF-TOKEN:

```
X-XSRF-TOKEN: <XSRF_Token_From_Step_1>
```

4. Set the content type to:

```
Content-Type: application/json
```

5. Set the request body to:

```
"processFile":"<processFilePathWithName>"
```

6. Complete request body as follows:

```
curl -s -i --cookie'
XSRFTOKEN=<XSRF_TOKEN_FROM_RESPONSE_HEADER>;
JSESSIONID=<JSESSIONID_FROM_RESPONSE_HEADER>;' -H '
Authorization:<AUTHORIZATION_TOKEN_ FROM_RESPONSE_HEADER> ' -H '
Content-Type: application/json' -H
'X-XSRF-TOKEN: <XSRF_TOKEN_FROM_RESPONSE_HEADER>' -X
POST -d'{"processFile":"<processFilePathWithName>"}' -k
```

7. Response received as follows:

```
[
{
 "messageCode" : 201,
 "message" : "The process has been
successfully submitted with processNumber '10'"
}
]
```

Example 2: Select Statistics for a Process using cURL

About this task

The following example describes steps to execute a Submit Select Statistics RESTful API using cURL.

Procedure

1. Call the **SignOn** API and get the authorization token, jsessionID, and XSRF-TOKEN token from the header in the response

```
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4x
ODYuMzU6MTM2MzplMDI0YjAzZC03NzkwLTQxMjItOTZkOC1iZjg5Mm
Y5NDcxM2MiLCJleHAiOjE1NTcxMjcyMTJ9.ME_mni-wgmrzVL214ijhxNz
U-bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3JYo1REs1w

XSRF:
809ab7e8-c6be-41ac-84f1-b4f8db246d9e

JSessionID:
node04p0v71bx6q46u2qthvr32htv3.node0
```

2. Submit a **cURL** request at the following URL

```
https://<CDWS_IPAddress:Port>/cdwebconsole/svc/processcontrolcriterias
```

3. Call the API with the XSRF header as X-XSRF-TOKEN:

```
X-XSRF-TOKEN : <XSRF_Token_From_Step_1>
```

4. Set the content type to:

```
Content-Type: application/json
```

5. Set the request body to:

```
"processFile":"<processFilePathWithName>"
```

6. Complete request body as follows:

```
curl -s -i --cookie ''XSRF-TOKEN=<XSRF_TOKEN_FROM_RESPONSE_HEADER>;
JSESSIONID=<JSESSIONID_FROM_RESPONSE_HEADER>; ' -H '
Authorization:<AUTHORIZATION_TOKEN_ FROM_RESPONSE_HEADER> ' -H '
Content-Type: application/json' -H 'X-XSRF-TOKEN: <XSRF_TOKEN_FROM_RESPONSE_HEADER>'
GET -k https://<CDWS_IPAddress:Port>/cdwebconsole/svc/selectstatistics?processNumber=10
```

7. Response received as follows:

```
[
{
"stopTime": "Mon May 06 12:41:32 IST 2019",
"submitNode": "CDWLT-025",
"msgShortText": "The submit of the process succeeded.",
 "recordCategory": "CAPR",
 "startTime": "Mon May 06 12:41:32 IST 2019",
 "recordId": "SUBP",
 "conditionCode": 0,
 "submitter": "Administrator",
 "messageId": "LCCA013I",
 "logDateTime": "Mon May 06 12:41:32 IST 2019",
 "processName": "PP",
 "processNumber": 10,
 "secondaryNode": "CDWLT-025"
 }
]
```

Sign Out

About this task

This procedure describes process to Sign Out.

Procedure

1. Call the **SignOn** API and get the authorization token, XSRF-TOKEN token, and JSESSION ID from the header in the response

   .

```
Authorization:
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJBZG1pbmlzdHJhdG9yOjE3Mi4yMC4xODYuMzU6MTM2MzplMDI0YjAzZC
03NzkwLTQxMjItOTZkOC1iZjg5MmY5NDcxM2MiLCJleHAiOjE1NTcxMjcyMTJ9.ME_mni-wgmrzVL214ijhxNzU-
bgHw9bv-Ktz8WL84ljpEYtgm89jfH7ehspyk-zgS6J8JiL2GJrG3JYo1REs1w
XSRF:
809ab7e8-c6be-41ac-84f1-b4f8db246d9e
JSessionID:
node04p0v71bx6q46u2qthvr32htv3.node0
```

2. Submit a DELETE request at the following:

```
 https://<CDWS_IPAddress:Port>/cdwebconsole/svc/signout
```

3. Call the API with the Authorization header:

```
Authorization: <Authorization Token_From_Step_1>
```

4. Call the API with the XSRF header as X-XSRF-TOKEN:

```
X-XSRF-TOKEN : <XSRF_Token_From_Step_1>
```

5. Call the API with the JSESSEION ID:

```
JSESSION ID : <JESSIONID_From_Step_1>
```

6. Set the content type to:

```
Content-Type: application/json
```

7. Set the request body as follows:

```
{
"userAccessToken": "<Access_Token_From_Step_1>"
}
```

8. Complete the request body as follows:

```
curl -s -i --cookie 'XSRF-TOKEN=<XSRF_TOKEN_FROM_RESPONSE_HEADER>;
JSESSIONID=<JSESSIONID_FROM_RESPONSE_HEADER>; ' -H '
Authorization:<AUTHORIZATION_TOKEN_ FROM_RESPONSE_HEADER> ' -H '
Content-Type: application/json' -H 'X-XSRF-TOKEN: <XSRF_TOKEN_FROM_RESPONSE_HEADER>'
-X DELETE -d '{"userAccessToken":"<AUTHORIZATION_TOKEN_ FROM_RESPONSE_HEADER> "}'
-k
```

9. Response received as follows:

```
{
 "signOut" : true,
 "userId" : "administrator"
}
```

Sample Scripts to invoke RESTful APIs

IBM Connect:Direct Web Service sample scripts can be used to invoke RESTful APIs . These scripts run from a remote client - making scripting common actions easier and can be customized to suit your business requirements.

JavaRESTClient.java and PythonRESTClient.py are sample Java and Python program, which invokes following APIs programmatically:

1. SignOn to CD Node
2. Submit a Process
3. Select the Process Stats
4. SignOut from CD Node

Java and Python scripts come packaged with the installer. To access the scripts, go to `<INSTALLATION_PATH>/SampleRESTClientScripts` directory.

HTTP Codes

The following table lists HTTP status codes that convey the results of a Web Services RESTful APIs request.

Table 15. HTTP return codes

HTTP code	**Description**
HTTP/1.1 200 OK	"OK" success code for requests other than creations and deletions
HTTP/1.1 201 OK	"Created" success code for a POST request
HTTP/1.1 500 Internal Server Error	The request failed due to internal error (Internal Server Error)
HTTP/1.1 404 Not Found	The requested resource couldn't be found.
HTTP/1.1 401 Unauthorized	(Unauthorized) The session ID or access token used has expired or is invalid. The response body contains the message and errorCode. The user must be logged in to make this API request. Check the value of the Authorization HTTP request header
HTTP/1.1 503 Service Unavailable	Service unavailable A backend error has occurred.
HTTP/1.1 400 Bad Request	The request couldn’t be understood, usually because the JSON body contains an error. The API request is invalid or improperly formed. Consequently, the API server could not understand the request.
HTTP/1.1 403 Forbidden	The request has been refused. Verify that the logged-in user has appropriate permissions. If the request syntax is correct, but the server is not able to find the item it. The requested operation is forbidden and cannot be completed

Supported RESTful APIs and methods matrix

REST API methods Matrix by Configuration Objects

The following matrix provides a consolidated view of operations supported by IBM Connect:Direct Web Service RESTful APIs.

RESTful API	Create (POST)	Read (GET)	Update/Replace (PUT)	Delete (DELETE)
Init Parms	N	Y	Y	N
List Directories	N	Y	N	N
Message Lookup	N	Y	N	N
Native	Y	N	N	N
Netmap Description	Y	Y	N	N
Netmap Node	Y	Y	Y	Y
Netmap Path	Y	Y	Y	Y
Process Control Services - Submit/Change/Select/ Suspend/Delete Process	Y	Y	Y	Y
Secure Plus CipherSuites	N	Y	N	N
Secure Plus Node Service	Y	Y	Y	Y
Secure Plus Key Certificate	Y	Y	Y	Y
Secure Plus Trusted Certificate	Y	Y	Y	Y
Select Statistics	N	Y	N	N
Stop Node	Y	N	Y	N
Tracing	N	Y	Y	N
Translation	N	Y	Y	N
User Authority	Y	Y	Y	Y
User Proxy	Y	Y	Y	Y

Chapter 6. Connect:Direct Web Services Troubleshooting

Use the following table to help troubleshoot problems with Connect:Direct Web Services:

Problem	Possible Cause	Solution
Connect:Direct Web Console fails to load	Cookies disabled in your browser settings and/or browser's local storage is persistent.	Enable browser cookie, local storage, clear the cache, and reload the page.
Upgrade fails	A previous attempt to uninstall Connect:Direct version was unsuccessful.	Cleanup the registry settings in the .com.zero.registry.xml: • Backup your installation data located in your <CDWSInstallDirecory> • This file is located in `/var/` for Root users and `$HOME/`for non-root users • It is recommended to create a back up of Zero G registry file before you proceed. • Edit the Zero G registry file to remove entries that begin with **MFTWebServices** product name. • Delete any entries beginning with tag `<product name="MFTWebServices">...</product>` • Attempt to re-install or upgrade.
Connect:Direct Web Console fails to load	Web Services is not accessible	Ensure firewall rules have been added for inbound and outbound connections between Web Services and Connect Direct Server. Firewall rules must allow inbound connections to the specified Web Services port. Connect Direct server must also have its API port open for web service.
Connect:Direct Web Services is not accessible	A network or firewall restriction	Ensure firewall rules are added on all the machines hosting Connect:Direct server(s).

Problem	Possible Cause	Solution
Connect:Direct server stops with the following error message: `CD server is in stop state.`	• Connect:Direct node in stop state or, • Number of API connection reached maximum or, • A firewall Restriction	Ensure that the Connect:Direct Server is running and verify: • The API address and port number used to establish client sessions with this Connect:Direct Server • The Maximum API connections limit has reached. Close an open API connection to continue using the IBM Connect:Direct Web Services • If a Firewall restriction is in place and that the machine hosting Connect:Direct Web Services to Connect:Direct server is attached to the network
Web Admin user account is locked.	• Failed login attempts • Lapses in security policies preventing a Web Admin user from retaining the current password.	Execute the Password Reset utility, `ResetDefaultCDWSAdminPassword`. For more information see, “Password Reset for a Web Administrator” on page 40.
Certificate-based authentication fails	This possibly occurred due to domain name and the Subject Alternative Name (SAN) or common name mismatch of the SSL certificate.	• When using certificate generated at installation, verify if the common-name is configured with the correct hostname value. • When using an external certificate, verify if either one of the following two conditions is met: – the common-name is configured with the correct hostname value – the IP Address/Hostname should match Subject Alternative Names (SAN) as defined in SSL certificate
Reference to PostgreSQL database may remain in the Registry after Connect:Direct Web Services for Windows is successfully uninstalled.		• Start the Registry editor (`regedit.exe`) • Locate the current control set and delete the related values **HKEY_LOCAL_MACHINE > Control Set > Services and delete >PostGreSQL - MFTWebServices** • Quit the Registry editor • Restart your system
All services were up and running but unable to access Connect:Direct Web Console.	This possibly occurred due to firewall settings. The settings are blocking connection attempts to Web services application.	Contact your system administrator.

Problem	Possible Cause	Solution

Connect:Direct Web Services fails to start after installation/upgrade is complete.
Upon inspecting the RESTful APIs logs the following error is displayed:
`org.postgresql.util .PSQLException: FATAL: password authentication: failed for user "postgres"`
	This issue possibly occurs when you're executing PostgreSQL password reset procedures for Connect:Direct Web Services running zLinux and AIX platforms.	1. Stop *MFTWebservices*
		2. Go to <Installation_Directory>/mftws/BOOT-INF/classes and invoke the following command to apply password changes to Web services:
		`java -jar ChangeDatabasePassword-0.1.jar Enter New Postgres Password>: Confirm Password>: Password Updated Successfully.`
		3. Launch Connect:Direct Web Services using the following utility:
		`./startWebserviceZLinux.sh`

	The default PostGreSQL password is changed in the Connect:Direct Web Services configuration settings. The modified password must also be updated for this user in PostgreSQL.	See, *Reset PostgreSQL Database connection password procedure using default password* described here, “PostgreSQL database Password management” on page 72.
Reset PostgreSQL Database using old password.		Follow *Reset PostgreSQL Database connection password procedure using old password* described here, “PostgreSQL database Password management” on page 72.
Change PostgreSQL Database in case of forgotten password		Follow *Reset PostgreSQL database connection in case of forgotten password* described here, “PostgreSQL database Password management” on page 72.

Problem	Possible Cause	Solution
Unable to import Connect:Direct z/OS certificates through Web Services.	• To complete Connect:Direct Secure Plus configuration environment, only base64 encoded pem certificates of Connect:Direct z/OS can be imported into Connect:Direct Web Services' Truststore through the Web Console. • Importing Connect:Direct z/OS key certificate through Connect:Direct Web Console supports base64-encoded PKCS12 ASCII key certificate. • Importing trust certificates into Connect:Direct z/OS Keystore supports base64 encoded certificates through the Web Console.	For a binary key certificate in Base64 ASN.1 DER format, follow the steps below convert the binary certificate into a base64 encoded PKCS12 ASCII key certificate: • Convert PKCS12 to base64 and save output into a pem file `cat cert.p12 | base64 >> cert.pem` • Add `-----BEGIN CERTIFICATE-----` in the beginning and `-----END CERTIFICATE-----` at the end of file cert.pem. The key certificate file is ready to import into Connect:Direct z/OS Keystore via Web Console.

PostgreSQL database Password management

Follow the procedures given below to manage PostgreSQL database passwords.

Reset PostgreSQL Database connection password procedure using old password

For Connect:Direct Web Services v6.0.0.5 users running zLinux/AIX platform, follow the steps given below to reset the PostgreSQL password to a new value.

1. Connect to the instance where PostgreSQL is installed.
2. Login as a PostgreSQL user with root privileges that is, `su – postgres`
3. Add the following line to the `pg_hba.conf` file to allow a user on the system to connect to local PostgreSQL database.

```
host  all  postgres  127.0.0.1/32   trust
```

4. Enter the current password used to connect to the PostgreSQL database.

```
PGPASSWORD=<current password>
```

5. Issue the following command to connect to the PostgreSQL database.

```
./psql -U postgres -p <PostgreSQL PORT>
```

6. Issue the following command to set the password to a new value.

```
ALTER USER <postgres_user> WITH PASSWORD <'new_password'>;
```

7. Issue the following command to stop the Web Services.

```
./stopWebserviceZLinux.sh in /<Installation_Directory>/bin/
./stopWebserviceAIX.sh in /<Installation_Directory>/bin/
```

8. Go to /<Installation_Directory>/mftws/BOOT-INF/classes and invoke the following command to apply password changes to Web services.

```
java -jar ChangeDatabasePassword-0.1.jar
```

9. Launch Connect:Direct Web Services using the following utility:

```
./startWebserviceZLinux.sh
./startWebserviceAIX.sh
```

This utility is available in the /<Installation_Directory>/jre/bin/ directory.

Reset PostgreSQL Database connection password procedure using default password

For Connect:Direct Web Services users running Windows/UNIX platform, follow the steps given below to reset the PostgreSQL password to a new value.

1. Navigate to the following directory.

Windows

```
Installation_Directory/PostgreSQL/bin
```

UNIX

```
Installation_Directory/PostgreSQL/pgsql/bin
```

2. Execute the following command to connect to PostgreSQL database.

```
psql.exe -U postgres -p <port_number>
Enter Password as 'postgres'
```

3. Execute the following command to change the PostgreSQL password that was entered when Web Services was installed.

```
ALTER USER postgres WITH PASSWORD 'new_password';
```

Reset PostgreSQL database connection in case of forgotten password

1. Connect to the instance where PostgreSQL is installed.
2. Login as a PostgreSQL user with root privileges that is, su – postgres.
   a. Go to the /var/<FolderName_where_database_initialised > directory where PostgreSQL database is installed.
   b. Take a backup of the pg_hba.conf file that controls the client authentication. Create a backup file with name such as, pg_**hbkp**.conf file.
3. Add the following line to the pg_hba.conf file to allow a user on the system to connect to local PostgreSQL database.

```
host  all  postgres  127.0.0.1/32   trust
```

4. Go to the bin directory and issue the following commands to restart PostgreSQL server:

```
run ./pg_ctl -m fast -D /var/< FolderName_where_database_initialised> stop
run ./pg_ctl -D /var/< FolderName_where_database_initialised> start
```

5. Issue the following command to connect to the PostgreSQL database server:

```
./psql -U postgres -p <PostgreSQL PORT>
```

6. Issue the following command to change the password of the PostgreSQL server:

```
ALTER USER postgres WITH PASSWORD 'very_secure_password';
```

7. Restore the pg_hba.conf file, restart the PostgreSQL server, and connect to the PostgreSQL database server with new password.
8. Invoke stopWebserviceZLinux.sh/stopWebserviceAIX.sh utility available in the /<Installation_Directory>/bin/ to stop the Web Services on the machine where it is currently installed.
9. Go to /<Installation_Directory>/mftws/BOOT-INF/classes and invoke the following command to apply password changes to Web services.

```
java -jar ChangeDatabasePassword-0.1.jar
```

10. Launch Connect:Direct Web Services using the following utility:

```
./startWebserviceZLinux.sh
./startWebserviceAIX.sh
```

This utility is available in the /<Installation_Directory>/jre/bin/java directory.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

Trademarks

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

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

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

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

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

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

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

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

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

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

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

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

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

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

Part Number:

(1P) P/N: