Information Engineering Technology

Install Guide - Remote Install

Release 8.8.0

© Information Engineering Technology Ltd 2021

Table Of Contents

Introduction

The GuardIEn System Updating facilities and the Construction Assistant provide a variety of options for installing generated code. If you wish to install the code on a different machine to the GuardIEn server you will have to configure the system to perform a *remote install*.

The GuardIEn Remote Install software is used to manage the installation of Gen generated code on a remote platform. A remote platform is any platform that is not on the same machine as the GuardIEn server. For example, GuardIEn on a UNIX server might generate code for installation on another UNIX server, a Windows server or MVS (CSE to MVS).

GuardIEn on the host encyclopaedia also provides facilities for executing certain system updating steps on a remote MVS machine (MVS to MVS). Note that a remote generation option is also available for the host encyclopaedia that utilises a Studio Developer workstation to automate the generation non-MVS code from models on the host encyclopaedia. This option for remote generation is not covered in this document.

When the generated code is to be installed on a remote platform, the GuardIEn remote install software needs to be installed on the remote machine.

The installation of the remote software is a two-stage process:

1) The remote installation software is prepared on a windows workstation
2) The remote installation software is then transferred to the remote installation machine and installed there

Pre-Requisites for a GuardIEn CSE server

- GuardIEn or Construction Assistant
- Gen client/server encyclopaedia with construction server and cross generation option for Windows
- Remote shell (rsh) and remote copy (rcp) utilities or secure shell (ssh/scp)
- FTP client (Microsoft FTP client for Windows or UNIX FTP client)
- FTP server (required for use with MVS builds only)

Pre-Requisites for Windows Build

- Gen Build Tool
- Remote Shell and Remote Copy Daemon, such as DeniComp's WRSHDNT
- Pre-compiler, compiler and other system software required by the Gen Build Tool

Pre-Requisites for UNIX Build

- Gen implementation toolset (IT)
- Remote Shell and Remote Copy Daemon or Secure Shell Daemon
- Pre-compiler, compiler and other system software required by the Gen IT

Pre-Requisites for CSE to MVS Build

- Gen runtimes
- COBOL Compiler and other runtimes and utilities required for compiling and linking Gen generated code. Note that whilst the Gen runtimes are required, the Gen MVS IT is not utilised.
- IBM TCP/IP FTP or Tectia SSH server capable of receiving FTP/sftp requests from the CSE and also transferring files to the CSE.
- In addition, the batch jobs are submitted from the CSE by using FTP or sftp to a Tectia SSH server.

Pre-Requisites for MVS to MVS Installation

- Gen SLIB dataset if MFS Gen required
- COBOL Compiler and other runtimes and utilities required for compiling and linking Gen generated code. Note that whilst the Gen runtimes are required, the Gen MVS IT is not utilised.
- IBM TCP/IP FTP capable of receiving FTP requests from the GuardIEn MVS machine and also transferring files between the two machines.
- In addition, the batch jobs are submitted using TCP/IP FTP or ssh to a Tectia SSH server

Prepare Software

All IET software is available for download from the IET support centre: https://support.iet.co.uk. Software is secured on the web site, so you will need register and then request access.

The following files should be downloaded into a temporary directory e.g. c:\temp\gdninst\

File Name	Description
GDRMTxxx.EXE	Setup program (xxx is the GuardIEn release, i.e. 880)

The next step is to prepare the remote installation software on your workstation.

- Execute GDRMTxxx.EXE. This is a self-extracting file that will then automatically launch a set-up program. Provide answers to the questions in the following dialogs:

Choose Destination Location

The GuardIEn remote install software is normally prepared on your C: drive in \Program Files under a sub-directory of \GuardIEn Remote Install. You may choose a different path during the set-up if you wish

Select Installation Targets

The remote installation software can support remote installation on Windows, UNIX and MVS. Select which platform(s) you wish to install the remote installation software on.

The following dialogs will depend on which platform(s) have been selected

Select Gen Version

Specify whether you are using Gen 6.5 or earlier, Gen r7.* , Gen 8.0, Gen 8.5 or Gen 8.6.

UNIX Install

Select UNIX Operating System

Specify the UNIX operating system.

- The IT home directory is the root directory for the IT and should contain a file called p3270keys.

Specify UNIX Parameters

Provide the path for the IT (Gen Implementation Toolset) home and scripts directories.

- The IT home directory is the root directory for the IT and should contain a file called p3270keys.
- The IT scripts directory is normally a scripts sub-directory located below IT home.

Specify GuardIEn and Oracle Paths

Provide a name for the path where the GuardIEn remote install software is to be installed on the UNIX server.

Provide the name for the Oracle home path, i.e. the value of $ORACLE_HOME

CSE to MVS Install

JES Version

Select whether you are using JES2 or JES3

Cobol Version

Select the major release level of COBOL

MVS Installation Info

Provide a dataset prefix (high level qualifier) for the GuardIEn remote install datasets on MVS. For example, if you want to install the GuardIEn datasets to GDN.RMTINST.CTLLIB etc, then set the dataset prefix to GDN.RMTINST (do not enter a trailing '.').

Provide the disk unit value for permanent datasets, i.e. 3390, DISK, etc.

MVS Gen Libraries

Provide the dataset names for the Gen libraries. These are either the names of the Gen Host Encyclopaedia or IT datasets. If you are using Gen r8.0 or above, then two panels are displayed. The first asks for the two Gen load libraries (software and runtime) and the second for the skeleton and sample libraries. For Gen r7 and earlier, one panel asks for the load, skeleton and sample libraries.

DB2 Load Library

Provide the dataset names for the following:

- DB2 Load – the DB2 load library containing the DB2 runtime and utility programs

MVS Runtime Libraries

Provide the dataset names for the following MVS runtime libraries:

- COBOL – the COBOL compiler library, for example IGY340.SIGYCOMP
- LE/370 – this is the LE/370 runtime library, typically CEE.SCEELKED
- ISPLINK – the ISPF link library containing the ISPLINK module

ISPF Libraries (1) & (2)

Provide the dataset names for the following ISPF runtime libraries. Note that these are the runtime libraries required to execute ISPF and not the Gen libraries.

- Panel – the ISPF Panel library
- Skeleton – the ISPF skeleton library
- Table – the ISPF table library
- Message – the ISPF message library

TP Load Library

Provide the dataset name for the TP monitor load library that contains the TP monitor runtimes required for linking online transactions. This is usually the CICS or IMS load library, i.e. CICS.SDFHLOAD or IMS.RESLIB.

Select CICS Support

If you wish to install support for the CICS newcopy support, then check the Install CICS support checkbox.

CICS Libraries

Provide the dataset names for the following CICS runtime library.

- EXCI – the CICS external interface library.

MVS to MVS Install

MVS Installation Info

Provide a dataset prefix (high level qualifier) for the GuardIEn remote install datasets on MVS. For example, if you want to install the GuardIEn datasets to GDN.RMTINST.CTLLIB etc, then set the dataset prefix to GDN.RMTINST (do not enter a trailing '.').

Provide the disk unit value for permanent datasets, i.e. 3390, DISK, etc.

MVS Gen Libraries

Provide the dataset names for the Gen SLIB dataset. These are either the names of the Gen Host Encyclopaedia or IT datasets.

DB2 Runtime Libraries

Provide the dataset names for the following runtime libraries:

- DB2 Load – the DB2 load library containing the DB2 runtime and utility programs

Installing Remote Software

Once the setup program has completed, you will need to transfer and install the remote install software on the remote installation machine(s).

Configuring CSE to Windows Installs

The software to manage remote installation on a windows machine is located in the \windows directory.

The following steps are performed to configure a remote Windows installation server.

1) Decide which user account will be used to perform the install (for example a user called iefinst might be created for this purpose
2) Create a directory on the windows build server to contain the GuardIEn remote installation software (i.e. c:\GuardIEn\RemoteInstall)
3) Copy the contents of the \windows sub-directory of the GuardIEn remote install software on your workstation to the windows build server.
4) Install and configure a *remote shell daemon* that supports remote copy (rcp) and remote shell (rsh). If you do not have a remote shell daemon (since this is not included with Windows) you may want to consider using *Winsock RSHD* (*Remote Shell Daemon*) from *Denicomp Systems*, which is a shareware product that IET has used. See *www.denicomp.com* for more details.
5) When the remote shell is executed, it is important that the PATH and other environment variables are correctly set to be able to invoke the Gen Build Tool.
6) In addition, the directory created on the build server will also need to be in the PATH and a variable called GDRMT needs to be set to this path. Most remote shell daemons commonly allow you to define what environment variables are set for the remote shell. The rsh.var file contains examples of the variables that would need to be set.
7) Enable remote shell access for the iefinst user from the CSE server. Your remote shell will indicate how this is performed.

Configuring CSE to UNIX Installs

The software to manage remote installation on a windows machine is located in the \UNIX directory.

The following steps are performed to configure a remote UNIX installation server.

When transferring files between machines, remember to use ASCII transfer except when transferring the binary executables.

1) Decide which user account will be used to perform the install (for example a user called iefinst might be created for this purpose
2) Create the server directory where the code is to be installed. You should use a single directory to contain the source code, object code, remote files and other files.
3) Create a GuardIEn Home directory, e.g. /apps/gdn/home (these are required for Gen 6.5 or earlier only)
4) Create a directory called UNIX beneath this, e.g. /apps/gdn/home/UNIX (these are required for Gen 6.5 or earlier only)
5) Create a GuardIEn scripts directory, e.g. /apps/gdn/scripts
6) Create a GuardIEn bin directory, e.g. /apps/gdn/bin
7) From your CSE server, transfer the contents of the GuardIEn Remote Install UNIX/home/UNIX directory to the installation server home/UNIX directory
8) Edit the .tgt files in the UNIX directory and check that the default locations of the IEFAE, SCRIPT and EXTERNAL_LIB tokens have correct values for your server (these are required for Gen 6.5 or earlier only)
9) Transfer the contents of the GuardIEn Remote Install UNIX\script to the remote server /scripts directory. Make the script executable (i.e. chmod +x *)

10) Transfer as an executable file (i.e. using binary file transfer) the appropriate gdckfile executable from the GuardIEn Remote Install UNIX\bin files to the remote server /bin directory. For HP-UX copy gdckfile.hpux. For AIX, copy gdckfile.aix. For HP IA64 Itanium, copy gdckfile.hpux.itanium.

11) Rename the gdckfile.aix/hpux/itanium file to gdckfile (i.e. with no extension). Make the gdckfile executable (chmod +x gdckfile). Repeat for gdfparse.

12) Copy the gdckfile & gdfparse programs from the /bin directory to a location on the remote installation server where it can be found in the PATH of a remote shell, for example /usr/bin or the home directory of the iefinst user. You might need your UNIX system administrator to do this.

13) Enable remote shell access for the iefinst user from the CSE server. This is normally accomplished by creating an entry in the .rhosts file in the iefinst user's home directory. An example .hosts entry for access from a CSE server called cse1 by the userid on the CSE called ency would be:

    cse1 ency # allow access from machine cse1 user ency

Note that GuardIEn assumes that the remote shell program is called rsh on NT and remsh on UNIX. For UNIX, check that your CSE server operating system uses remsh and not rsh or resh (which is restricted shell on HP-UX for example).

Configuring CSE to MVS Installs

The software to manage remote installation on a windows machine is located in the \CSE2MVS directory.

The configuration of the MVS server involves the following steps:

- Edit the cse2mvs.jcl file and insert a valid jobcard at the top of the file, replacing the first line (//JOBNAME JOB)
- Transfer the cse2mvs.jcl file as an ASCII file to the host to an FB 80 dataset. This can either be a sequential dataset or a member in an existing partitioned dataset. This file contains national language characters (i.e. $) that need to be transferred to codepage 037 on the host, so if your ascii file transfer defaults are not for codepage 037, amend the ftp transfer to use this codepage.
- Transfer the mvsinst.seq file as a BINARY file to the host to an FB 80 sequential dataset named <PREFIX>.MVSINST where <PREFIX> is the same prefix that you entered for the GuardIEn remote install software.
- Submit the JCL file on the host and check the return codes from each of the steps.

The job will create the following datasets:

Dataset Name	Purpose
<PREFIX>.LOADLIB	Load Library
<PREFIX>.CTLLIB	Control Card and CLISTs
<PREFIX>.PROCLIB	JCL Procedures

- Once the job has completed, check the job output to ensure that all of the steps completed successfully
- Edit the PROCLIB(GDNIRSPF) dataset and check that the ISPF datasets allocate are sufficient to execute an ISPF task.

```
//ISPPLIB  DD DSN=<ISPFPRFX>.ISPPLIB,DISP=SHR
//ISPSLIB  DD DSN=<ISPFPRFX>.ISPSLIB,DISP=SHR
//ISPMLIB  DD DSN=<ISPFPRFX>.ISPMLIB,DISP=SHR
```

Specify the *ISPF libraries* used at your site. At least one entry is required in each ISPF library type, although you may need further datasets. Please note that the ISPF libraries are the libraries that contain the ISPF software itself.

- If you are using a UNIX CSE server or the Windows FTP daemon expects the directories to be specified in UNIX style, create a system parameter with a code of FTPSTYLE and set the text value to UNIX.
- When using UNIX style path names with a Windows IIS FTP server, you should also configure a virtual directory for the drive with the same name as the drive, for example a virtual directory called “C” using the path “c:\”.

CICS NEW COPY or PHASEIN

If you are using the CICS new copy procedure to deploy changed application load modules into CICS, then you also need to install the GNSE transaction in the target CICS region. The CICS new copy is performed by executing the GNSEBTCH program in batch which communicates to the GNSE server in CICS to perform the new copy.

By default, the GuardIEn mechanism for automating the deployment of changed CICS load modules utilises a CICS NEW COPY via load module GNSE deployed into CICS. However, if preferred, this behaviour can be altered to invoke a CICS PHASEIN by deployment of a different version of the GNSE module that is also supplied with the remote installation. To activate, you will need to firstly rename the GuardIEn LOADLIB member GNSE to GNSEO and then rename member GNSE2 to GNSE. This ensures the CICS PHASEIN call replaces the default CICS NEW COPY invocation within GNSE.

To deploy GNSE into CICS, complete the following tasks for EACH CICS region where you will be deploying your application code via GuardIEn.

- Copy the GNSE load module from the LOADLIB into your CICS program library.
- Define the GNSE transaction using CICS resource definition. The parameters are:

```
DEFINE TRANS(GNSE) GROUP(GDNGD) DE(GUARDIEN CICS NEW COPY SERVER)
    PROGRAM(GNSE) TWASIZE(8) TASKDATALOC(ANY) TRANCLASS(DFHTCL00)

DEFINE PROGRAM(GNSE) GROUP(GDNGD) DE(GUARDIEN NEW COPY SERVER)
    LANGUAGE(LE370) DATALOCATION(ANY)
```

Note that a different GROUP can be used.

- The GuardIEn CICS new copy server uses the CICS EXCI interface to establish the communication between the batch program and CICS. The CICS inter-region communication (IRC) needs to be open and CICS needs to have multi-region operation (MRO) enabled. You also need to ensure that your CICS system has a generic EXCI *CONNECTION* defined and an EXCI *SESSIO*N defined to use this connection.
- By default the GuardIEn mechanism for automating the deployment of changed CICS load modules utilises the standard mirror transaction (CSMI) as defined to DFHMIRS to invoke a CICS NEW COPY or PHASEIN via the GuardIEn batch job (GNSEBTCH). For most sites use of CSMI will be acceptable although should you need to utilise a separate and discrete mirror transaction then GNSE may itself be used, defined as a transaction based on CSMI. To do this GNSE will have to be defined with the necessary authorities to run CSMI requests otherwise you will encounter security errors when the GNSEBTCH batch job attempts to invoke GNSE via the mirror transaction. To activate this functionality, you firstly rename the existing GuardIEn LOADLIB member GNSEBTCH to GNSEBTCO and then rename member GNSEBTC2 to GNSEBTCH. This ensures a TRANSID with the GNSE transaction is passed into CICS instead of the default CSMI.

Character Translation

The installation process transfers the generated source code from the CSE to MVS using FTP. If the FTP server is not configured to correctly translate the ascii to ebcdic for the specific codepage, then the GuardIEn server needs to be configured to ensure that national language and special characters are correctly converted. Consult the Remote Installs user guide for details.

Configuring MVS to MVS Installs

The software to manage remote installation on a windows machine is located in the \MVS2MVS directory.

The configuration of the MVS server involves the following steps:

- Edit the mvs2mvs.jcl file and insert a valid jobcard at the top of the file, replacing the first line (//JOBNAME JOB)
- Transfer the mvs2mvs.jcl file as an ASCII file to the host to an FB 80 dataset. This can either be a sequential dataset or a member in an existing partitioned dataset.
- Submit the JCL file on the host and check the return codes from each of the steps.

The job will create the following datasets:

Dataset Name	Purpose
<PREFIX>.CTLLIB	Control Card and CLISTs
<PREFIX>.PROCLIB	JCL Procedures

Documentation

The documentation for remote installation is the *Remote Builds* document located in the GuardIEn client \doc directory

Testing the Windows/UNIX Remote Install Server

The following steps are performed to test that the remote server is available using rcp/rsh utilities or the secure shell alternatives.

Test Remote Shell

If you are using the standard remote shell utilities, perform these tests.

Test RCP

From the CSE server, attempt to copy a file to the remote server using remote copy, using the form:

rcp <source_file> <host>.<user>:<remote_file>
e.g.:
rcp test.txt 19.150.50.100.iefinst:/home/iefinst/test.txt

Test RSH

From the CSE server, try and invoke gdckfile, using the form:

rsh <host> -l <userid> gdckfile <file name to check>
e.g.:
rsh 19.150.50.100 -l iefinst gdckfile /apps/gdn/scripts/gdremrmt

On a UNIX CSE you may have to use remsh instead of rsh.

Test Secure Shell

If you are using Secure Shell, perform these tests. You cannot use password or command line authentication from the GuardIEn server and will therefore need to enable public key authentication. See the GuardIEn documentation for further details of SSH support in GuardIEn.

Test SCP

From the CSE server, attempt to copy a file to the remote server using remote copy, using the form:

scp <source_file> <user>@<host>:<remote_file>
e.g.:
scp test.txt iefinst@19.150.50.100:/home/iefinst/test.txt

Test SSH

From the CSE server, try and invoke gdckfile, using the form:

ssh <host> -l <userid> gdckfile <file name to check>
e.g.:
ssh 19.150.50.100 -l iefinst gdckfile /apps/gdn/scripts/gdremrmt