Backup and Recovery

This chapter explains how to maintain the Cisco Prime Network Registrar databases.

Backing Up Databases

Because the Cisco Prime Network Registrar databases do a variety of memory caching and can be active at any time, you cannot rely on third-party system backups to protect the database. They can cause backup data inconsistency and an unusable replacement database.

For this purpose, Cisco Prime Network Registrar provides a shadow backup utility, cnr_shadow_backup. Once a day, at a configurable time, Cisco Prime Network Registrar takes a snapshot of the critical files. This snapshot is guaranteed to be a consistent view of the databases.

Recommendation

When upgrading to 10.0 (or later) from a pre-10.0 version of CPNR and when there are significant number of DHCPv6 leases (and/or DHCPv6 lease history records), customers SHOULD schedule a DHCP database dump and load (see Using the cnrdb_util Utility , on page 14) to reduce the size of the DHCPv4 database after the upgrade. The upgrade does NOT reduce the size of the original dhcp.ndb database when the DHCPv6 leases (active + history) are moved to the new dhcp6.ndb and the only way to reduce the size of the original database is to do a dump and load. Viewing the size of the dhcp6.ndb file (using the ls (Unix) or dir (Windows) commands) will give you an estimate as to the size by which the database can be reduced.

Related Topics

Syntax and Location, on page 2

Backup Strategy, on page 2

Syntax and Location

Be sure to understand that the notation “.../data/db” in the following sections refers to directories in the Cisco Prime Network Registrar product data location path, depending on the operating system:

- **Windows**—“.../data” means the data directory, which by default is **C:\NetworkRegistrar\{Local | Regional}\data**.
- **Linux**—“.../data” means the data directory, which by default is **/var/nwreg2/{local | regional}/data**.

Cisco Prime Network Registrar database utility programs mentioned in the following sections are located in the “.../bin” directory, which you run as its full path name:

- **Windows**—“.../bin/*program* ” means the program file in the bin directory, which by default is **C:\Program Files\Network Registrar\{Local | Regional}\bin***program* for a 32-bit OS and **C:\Program Files (x86)\Network Registrar\{Local | Regional}\bin***program* for a 64-bit OS.
- **Linux**—“.../bin/*program*” means the program file in the bin directory, which by default is **/opt/nwreg2/local/usrbin/***program* or **/opt/nwreg2/regional/usrbin/***program*.

Note Use only the approved utilities for each type of database. In Windows, if you want to run the utility from outside the installed path, you must set the CNR_HOME environment variable.

Backup Strategy

The backup strategy involves either:

- Making CCM perform a nightly shadow backup for you (See the Setting Automatic Backup Time, on page 3) and using the shadow backups for permanent backup and then doing an explicit backup - either using the cnr_shadow_backup utility and backing up the backup files (*.bak DBs)

  or

Shutting down Cisco Prime Network Registrar and performing a backup using TAR or other similar tools.

Manual Backup (Using cnr_shadow_backup utility)

Use the cnr_shadow_backup utility to back up the following databases:

- **CNRDB databases**—...data/dhcp, ...data/dns/csetdb, ...data/dns/rrdb, ...data/cdns, ...data/leasehist, ...data/lease6hist, ...data/subnetutil, ...data/mcd, ...data/replica, and ...data/ccm/ndb

Note If you change the location of the data directory, you must edit the **cnr.conf** file, which is located in .../conf (see Modifying the cnr.conf File). Change the **cnr.datadir** variable to the full path to the data directory. For example, the following is the default value on Windows:

```
cnr.datadir=C:\\NetworkRegistrar\\{Local|Regional}\\data
```

The most basic component of a backup strategy is the daily shadow backup. When problems occur with the operational database, you might need to try recovering based on the shadow backup of the previous day. Therefore, you must recognize and correct any problems that prevent a successful backup.

The most common problem is disk space exhaustion. To get a rough estimate of disk space requirements, take the size of the .../data directory and multiply by 10. System load, such as usage patterns, application mix, and the load on Cisco Prime Network Registrar itself, may dictate that a much larger reserve of space be available.

You should regularly archive existing shadow backups (such as to tape, other disks, or other systems) to preserve them for possible future recovery purposes.

Caution Using a utility on the wrong type of database other than the one recommended can cause database corruption. Use only the utilities indicated. Also, never use the database utilities on the operational database, only on a copy.

Related Topics

Setting Automatic Backup Time, on page 3

Performing Manual Backups, on page 3

Using Third-Party Backup Programs with cnr_shadow_backup, on page 4

Setting Automatic Backup Time

You can set the time at which an automatic backup should occur by editing the **cnr.conf** file (in .../conf). Change the **cnr.backup-time** variable to the hour and minute of the automatic shadow backup, in 24-hour *HH*:*MM* format, then restart the server agent. For example, the following is the preset value:

```
cnr.backup-time=23:45
```

Note You must restart Cisco Prime Network Registrar for a change to **cnr.backup-time** to take effect.

Performing Manual Backups

You can also initiate a manual backup with the cnr_shadow_backup utility, which requires root privileges. Enter the cnr_shadow_backup command at the prompt to perform the backup.

Note To restore DHCP data from a failover partner that is more up to date than a backup, see Restoring DHCP Data from a Failover Server, on page 16.

Using Third-Party Backup Programs with cnr_shadow_backup

You should avoid scheduling third-party backup programs while cnr_shadow_backup is operating. Third-party backup programs should be run either an hour earlier or later than the cnr_shadow_backup operation. As described in Setting Automatic Backup Time, on page 3, the default shadow backup time is daily at 23:45.

Configure third-party backup programs to skip the Cisco Prime Network Registrar operational database directories and files, and to back up only their shadow copies.

The operational files are listed in Backup Strategy, on page 2. On Linux, Cisco Prime Network Registrar also maintains lock files in the following directories:

- Cisco Prime Network Registrar server processes—/var/nwreg2/local/temp/np_destiny_trampoline or /var/nwreg2/regional/temp/np_destiny_trampoline

The lock files are recreated during a reboot. These files are important while a system is running. Any maintenance process (such as virus scanning and archiving) should exclude the temporary directories, operational database directories, and files.

Windows does not maintain lock files, but uses named-pipes instead.

Backing Up CNRDB Data

In the case of the CNRDB databases, the cnr_shadow_backup utility copies the database and all log files to a secondary directory in the directory tree of the installed Cisco Prime Network Registrar product. For:

- **DHCP**—The operational database is in the .../data/dhcp/ndb, .../data/dhcp/ndb6, and .../data/dhcp/clientdb directories, with the log files in the .../data/dhcp/ndb/logs and .../data/dhcp/ndb6/logs directories. The shadow copies are in the .../data.bak/dhcp/ndb, .../data.bak/dhcp/ndb6, and.../data.bak/dhcp/clientdb directories.
- **DNS**—The operational database is in the .../data/dns/rrdb directory. The important operational components are the High-Availability (HA) DNS is in the .../data/dns/hadb directory, with log files in the .../data/dns/hadb/logs directory.The shadow copies are in the .../data.bak/dns directory.
- **CDNS—**The operational database is in the .../data/cdns directory. The shadow copies are in the .../data.bak/cdns directory.
- **CCM**—The operational database and log files are in the .../data/ccm/ndb directory. The shadow copies are in the .../data.bak/ccm directory.
- **MCD change log**—The operational database and log files are in the .../data/mcd/ndb directory. The shadow copies are in the .../data.bak/mcd directory. MCD Change Log database may not exist if there are no change log entries. Also, the database is deleted when the MCD change log history is trimmed or when there is no MCD change log data to begin with.
- **Lease history**—The operational database and log files are in the .../data/leasehist and .../data/lease6hist directories. The shadow copies are in the .../data.bak/leasehist and .../data.bak/lease6hist directories.
- **DHCP utilization**—The operational database and log files are in the .../data/subnetutil directory. The shadow copies are in the .../data.bak/subnetutil directory.

- **Replica**—The operational database and log files are in the .../data/replica directory.

The file names are:

- **Database**—dhcp.ndb, dhcp6.ndb, clientdb.ndb, dns.ndb, and the *.db files used by CCM.
- **Log files**—log.0000000001 through log.9999999999. The number of files varies with the rate of change to the server. There are typically only a small number. The specific filename extensions at a site vary over time as the database is used. These log files are not humanly readable.

Backing Up All CNRDBs Using tar or Similar Tools

This section describes the procedure for backing up all Cisco Prime Network Registrar databases using tar or similar tools.

Step 1 Shut down Cisco Prime Network Registrar.

Backups cannot be done using tar or similar tools if Cisco Prime Network Registrar is running.

Step 2 Back up the entire data directory and subdirectories:

```
> /var/nwreg2/local/data or /var/nwreg2/regional/data
> /opt/nwreg2/*/conf
```

Step 3 Restart Cisco Prime Network Registrar when the backup is complete.

Note Technically the backups do not need to include the *.bak directories (and subdirectories of those directories) as those contain nightly shadow backups. However, unless your available storage space is severely limited, we recommend a full backup of the entire data directory (and subdirectories) including the shadow backups.

Database Recovery Strategy

Cisco Prime Network Registrar uses the CNRDB database. The following table lists the types of CNRDB database that must be backed up and recovered.

Table 1: Cisco Prime Network Registrar Databases for Recovery

Subdirectory	Cluster	Type	Description
mcd	local	CNRDB	MCD change log data. Only exists for upgrades from pre 8.0 databases as long as there is MCD change log history that has not been trimmed.

Subdirectory	Cluster	Type	Description
ccm	local, regional	CNRDB	Central Configuration Management database. Stores local centrally managed cluster and the SNMP server data.
dns	local	CNRDB	DNS database. Stores zone state information, names of protected RRs, and zone configuration data for the DNS server.
cdns	local	CNRDB	Caching DNS database. Stores the initial DNSSEC root trust anchor and root hints.
dhcp[1]	local	CNRDB	DHCP database. Stores lease state data for the DHCP server.
dhcpeventstore	local		Queue that Cisco Prime Network Registrar maintains to interact with external servers, such as for LDAP and DHCPv4 DNS Update interactions. Recovery is not necessary.
tftp	local		Default data directory for the TFTP server. Recovery is not necessary.
replica	regional	CNRDB	Stores replica data for the local clusters.
lease6hist	regional	CNRDB	DHCPv6 lease history database.
leasehist	regional	CNRDB	DHCPv4 lease history database.
subnetutil	regional	CNRDB	DHCP Utilization database which includes databases for subnets and prefixes separately.

[1] Restoring the DHCP databases (.../data/dhcp/ndb and .../data/dhcp/ndb6) from a backup is NOT RECOMMENDED. This is because, this data is constantly changing as the DHCP server is running (because of client activity and lease expirations either on this server or its partner). Therefore, restoring the DHCP ndb/ndb6 databases would set the clock back in time for the server, but not for clients. Hence,

it is best to retain the DHCP server databases rather than recovering it, or if recovery is needed, delete it and recover the current leases from the partner via failover (see Restoring DHCP Data from a Failover Server, on page 16).

The general approach to recovering a Cisco Prime Network Registrar installation is:

1. Stop the Cisco Prime Network Registrar server agent.
2. Restore or repair the data.
3. Restart the server agent.
4. Monitor the server for errors.

After you are certain that you executed a successful database recovery, always manually execute the cnr_shadow_backup utility to make a backup of the current configuration and state.

Recovering CNRDB Data from Backups

If there are any indications, such as server log messages or missing data, that database recovery was unsuccessful, you may need to base a recovery attempt on the current shadow backup (in the Cisco Prime Network Registrar installation tree). To do this:

Step 1 Stop the Cisco Prime Network Registrar server agent.

Step 2 Move the operational database files to a separate temporary location.

Step 3 Copy each .../data/*name* .bak directory to .../data/*name* ; for example, copy .../data/ccm.bak to .../data/ccm.

Note If you set the cnr.dbrecover variable to false in the cnr.conf file to disable recovery during the cnr_shadow_backup nightly backup, you must also do a recovery as part of these steps.

Step 4 Rename the files.

The CNRDB database maintains centrally managed configuration data that is synchronized with the server configuration databases.

Step 5 Create a new data directory and then untar or recover the backed up directory.

We recommend that you run the DB directory and recovery tools to ensure that the databases are good.

Note Ensure that the logs subdirectory is present in the same directory or the logs path is mentioned in the DB_CONFIG file.

Step 6 Restart the server agent.

Note If the recovery fails, perhaps because the current shadow backup is simply a copy of corrupted files, use the most recent previous shadow backup. This illustrates the need to regularly archive shadow backups. You cannot add operational log files to older shadow backup files. All data added to the database since the shadow backup was made will be lost.

After a successful database recovery, initiate an immediate backup and archive the files using the cnr_shadow_backup utility (see Performing Manual Backups, on page 3).

Recovering All CNRDBs Using tar or Similar Tools

This section describes the procedure for recovering all Cisco Prime Network Registrar databases using tar or similar tools.

Step 1 Shut down Cisco Prime Network Registrar. Run **/etc/init.d/nwreglocal stop** (for RHEL/CentOS 6.x) or **systemctl stop nwreglocal** (for RHEL/CentOS 7.x) to ensure that Cisco Prime Network Registrar is down.

Step 2 Rename the active data directory (such as mv data old-data).

Note You must have sufficient disk space for twice the size of the data directory (and all the files in it and its subdirectories). If you do not have sufficient disk space, move the active data directory to another drive.

Step 3 Create a new data directory and then untar or recover the backed up directory.

We recommend that you run the CNRDB directory and recovery tools to ensure that the databases are good.

Step 4 Start Cisco Prime Network Registrar.

Note Technically the restores do not need to include the *.bak directories (and subdirectories of those directories) as those contain nightly shadow backups. However, unless your available storage space is severely limited, we recommend a full restore of the entire data directory (and subdirectories) including the shadow backups.

Recovering Single CNRDB from tar or Similar Tools

This section describes the procedure for recovering single database using tar or similar tools.

Step 1 Shut down Cisco Prime Network Registrar. Run **/etc/init.d/nwreglocal stop** (for RHEL/CentOS 6.x) or **systemctl stop nwreglocal** (for RHEL/CentOS 7.x) to ensure that Cisco Prime Network Registrar is down.

Step 2 Rename the active data directory (such as mv data old-data).

Note You must have sufficient disk space for twice the size of the data directory (and all the files in it and its subdirectories). If you do not have sufficient disk space, move the active data directory to another drive.

Step 3 Create a new data directory and then untar or recover only the files in that directory (and its subdirectories) from the backup.

We recommend that you run the CNRDB integrity and recovery tools to ensure that the CNRDB are good.

Step 4 Repeat **Step 2** to **Step 3** for other DBs that have to be recovered.

Step 5 Start Cisco Prime Network Registrar.

Virus Scanning While Running Cisco Prime Network Registrar

If you have virus scanning enabled on your system, it is best to configure it to exclude certain Cisco Prime Network Registrar directories from being scanned. Including these directories might impede Cisco Prime

Network Registrar operation. The ones you can exclude are the .../data, .../logs, and .../temp directories and their subdirectories.

Troubleshooting Databases

The following sections describe troubleshooting the Cisco Prime Network Registrar databases.

Related Topics

Using the cnr_exim Data Import and Export Tool, on page 9

Using the cnrdb_recover Utility, on page 12

Using the cnrdb_verify Utility, on page 13

Using the cnrdb_checkpoint Utility, on page 13

Using the cnrdb_util Utility , on page 14

Restoring DHCP Data from a Failover Server, on page 16

Using the cnr_exim Data Import and Export Tool

The cnr_exim data import and export tool now supports the following for a user not constrained to a specific tenant:

- Exporting all the data
- Exporting the data specific to a tenant either with or without the core data
- Exporting and importing license related data
- Importing all of the data
- Importing the data specific to a tenant and optionally mapping it to a new tenant either with or without the core data. This allows you to build a base configuration for new tenants. When specifying tenant tags, the imported data is used to find the old tenant id and the current configuration is used to find the new tenant id.

Some of the advantages that come with the use of multi-tenant architecture are that you can move configurations for a tenant from one cluster to another to export a tenant template data and them import that data as another tenant.

Note A user constrained to a specific tenant can only export or import data for that tenant.

The cnr_exim tool also serves to export unprotected resource record information. However, cnr_exim simply overwrites existing data and does not try to resolve conflicts.

Note You cannot use cnr_exim tool for import or export of data from one version of Cisco Prime Network Registrar to another. It can be used only for import or export of data from or to the same versions of Cisco Prime Network Registrar.

Before using the cnr_exim tool, exit from the CLI, then find the tool on:

- **Windows**—...\bin\cnr_exim.exe
- **Linux**—.../usrbin/cnr_exim

You must reload the server for the imported data to become active.

Note that text exports are for reading purposes only. You cannot reimport them.

The text export prompts for the username and password (the cluster defaults to the local cluster). The syntax is:

```
> cnr_exim -e exportfile [-N username -P password -C cluster]
```

To export (importable) raw data, use the **–x** option:

```
> cnr_exim -e exportfile -x
```

To export DNS server and zone components as binary data in raw format, use the **–x** and **–c** options:

```
> cnr_exim -e exportfile -x -c "dnsserver,zone"
```

The data import syntax is (the import file must be in raw format):

```
> cnr_exim -i importfile [-N username -P password -C cluster]
```

You can also overwrite existing data with the **–o** option:

```
> cnr_exim -i importfile -o
```

The following table describes all the qualifying options for the cnr_exim tool.

Table 2: cnr_exim Options

Option	Description
–a	Allows exporting and importing of protected or unprotected RRs. Valid *values* are: **protectedRR**, **unprotectedRR**, and **none** **Export**: All RRs are exported by default, so you must explicitly specify the export of protected or unprotected RRs using the option "-a protectedRR", "-a unprotectedRR", or "-a none". If this option is not specified, all RRs are exported. **Import:** All RRs are imported by default, so you must explicitly specify the import of protected or unprotected RRs using the option "-a protectedRR" or " -a unprotectedRR". If this option is not specified, all RRs are imported.

Option	Description
–c	Imports or exports Cisco Prime Network Registrar components, as a quoted, comma-delimited string. Use **–c help** to view the supported components. User are not exported by default; you must explicitly export them using this option, and they are always grouped with their defined groups and roles. Secrets are never exported. **Note** After you import administrator names, you must set new passwords for them. If you export groups and roles separately from usernames (which are not exported by default), their relationship to usernames is lost.
–C *cluster*	Imports from or exports to the specified cluster. Preset to **localhost**.
–e *exportfile*	Exports the configuration to the specified file.
–h	Displays help text for the supported options.
–i *importfile*	Imports the configuration to the specified file. The import file must be in raw format.
–N *username*	Imports or exports using the specified username.
–o	When used with the **–i** (import) option, overwrites existing data.
–p *port*	Port used to connect to the SCP server.
–P *password*	Imports or exports using the specified password.
–t *exportfile*	Specifies a file name to export to, exports data in s-expression format.
–v	Displays version information
–x	When used with the **–e** (export) option, exports binary data in (importable) raw format.
–d	Specifies the directory path of cnr_exim log file.
–f	Specifies the source tenant. Valid for export and import.
–g	Specifies the destination tenant. Valid for import only. The tenant-id can not be changed when exporting data, only when the data is imported.)

Option	Description
–b	Specifies that the core (base) objects are to be included in the import/export. This includes all objects either with an explicit tenant-id of 0 and those that have no tenant-id attribute.
–w	Specifies the view tag to export. This option allows the user to export zone and RRs data which has the same view tag as mentioned in “w” option. All other objects will not take this option into consideration and will be exported as earlier if it is used.

Using the cnrdb_recover Utility

The **cnrdb_recover** utility is useful in restoring the Cisco Prime Network Registrar databases to a consistent state after a system failure. You would typically use the **–c** and **–v** options with this command (The following table describes all of the qualifying options). The utility is located in the installation bin directory.

Table 3: cnrdb_recover Options

Option	Description
–c	Performs a catastrophic recovery instead of a normal recovery. It not only examines all the log files present, but also recreates the .ndb (or .db) file in the current or specified directory if the file is missing, or updates it if is present.
–e	Retains the environment after running recovery, rarely used unless there is a DB_CONFIG file in the home directory.
–h *dir*	Specifies a home directory for the database environment. By default, the current working directory is used.
–t	Recovers to the time specified rather than to the most current possible date. The time format is *[[CC]YY]MMDDhhmm[***.***ss]* (the brackets indicating optional entries, with the omitted year defaulting to the current year).
–v	Runs in verbose mode.
–V	Writes the library version number to the standard output, and exits.

In the case of a catastrophic failure, restore a snapshot of all database files, along with all log files written since the snapshot. If not catastrophic, all you need are the system files at the time of failure. If any log files are missing, **cnrdb_recover –c** identifies the missing ones and fails, in which case you need to restore them and perform the recovery again.

Use of the catastrophic recovery option is highly recommended. In this way, the recovery utility plays back all the available database log files in sequential order. If, for some reason, there are missing log files, the recovery utility will report errors. For example, the following gap in the log files listed:

```
log.0000000001
log.0000000053
```

results in the following error that might require you to open a TAC case:

```
db_recover: Finding last valid log LSN:file:1 offset 2411756
db_recover: log_get: log.0000000002: No such file or directory
db_recover: DBENV->open: No such for or directory
```

Using the cnrdb_verify Utility

The **cnrdb_verify** utility is useful for verifying the structure of the Cisco Prime Network Registrar databases. The command requires a file parameter. Use this utility only if you are certain that there are no programs running that are modifying the file. The following table describes all its qualifying options. The utility is located in the installation bin directory. The syntax is described in the usage information when you run the command:

```
C:\Program Files\Network Registrar\Local\bin>cnrdb_verify

usage: cnrdb_verify [-NoqV] [-h dir] [-P password] file
```

Table 4: cnrdb_verify Options

Option	Description
–h *dir*	Specifies a home directory for the database environment. By default, the current working directory is used.
–N	Prevents acquiring shared region locks while running, intended for debugging errors only, and should not be used under any other circumstances.
–o	Ignores database sort or hash ordering and allows **cnrdb_verify** to be used on nondefault comparison or hashing configurations.
–P *password*	User password, if the file is protected.
–q	Suppresses printing any error descriptions other than exit success or failure.
–V	Writes the library version number to the standard output, and exits.

Using the cnrdb_checkpoint Utility

The **cnrdb_checkpoint** utility is useful in setting a checkpoint for the database files so as to keep them current. The utility is located in the installation bin directory. The syntax is described in the usage information when you run the command:

```
C:\Program Files\Network Registrar\Local\bin>cnrdb_checkpoint ?

usage: cnrdb_checkpoint [-1Vv] [-h home] [-k kbytes] [-L file] [-P password][-p min]
```

Using the cnrdb_util Utility

The cnrdb_util utility is useful for dumping and loading CPNR databases. In addition, you can use this utility to shadow backup and recover the CPNR databases, to clear the log files, as well as to change the database page size.

The utility is located on the following directory:

- **Window** — *(installation directory)*\bin\cnrdb_util.bat
- **Linux** — *(installation directory)*/usrbin/cnrdb_util

Important It is strongly recommended that a backup be done before performing any operation on the CPNR databases. If existing backup files are to be retained, they must be backed up as well.

The cnrdb_util utility runs in two modes.

- **Interactive mode** - Prompts the user for operations and options.
- **Batch mode** - Requires information (both operation and options) as arguments while executing this utility.

The syntax is described in the usage information when you run the command:

```
./cnrdb_util -h
```

The following tables describe all of the qualifying operations and options.

Table 5: cnrdb_util Operations

Operation	Description
–d	Dump one or all CPNR databases.
–l	Load one or all CPNR databases.
–b	Create shadow backup of all CPNR databases.
–r	Recover one or all CPNR databases from shadow backup.
–c	Cleanup sleepycat log files in one or all CPNR databases.
–h	Display help text for the supported options.

Important You can perform only one operation at a time.

Table 6: cnrdb_util Options

Option	Description
-m { local | regional }	Specifies the CPNR installation mode. If not specified, this information is read from the cnr.conf file. If the file is not found, local mode is used by default.
-prog path	Specifies the path to the dump, load, or shadow backup executable. If not specified, this will be derived from the CPNR installation path.
-db_pagesize number	Specifies the size of database pages (in bytes) to be used when creating new databases. The minimum page size is 512 bytes and the maximum page size is 64K bytes, and must be a power of two. If no page size is specified, a page size is selected based on the underlying filesystem I/O block size. (A page size selected in this way has a lower limit of 512 bytes and an upper limit of 16K bytes.) Usually the default is appropriate. However, large page sizes may not have good performance. 4096 and 8192 are typically good sizes. You can determine the page size of the database by using the **cnrdb_stat** utility.
-n { ccm | dhcp | dns | mcd | leasehist | lease6hist | replica | subnetutil | all }	Specifies the name of the source database for the '-d' dump, '-l' load, or '-r' recover operation. If not specified, the operation will be performed on all databases present in database path. This option is not applicable for the '-b' backup operation. • Valid database names for local mode are { ccm | dhcp | dns | mcd | all } • Valid database names for regional mode are { ccm | dns | leasehist | lease6hist | replica | subnetutil | all }
-s	Specifies that this program should attempt to stop the CPNR Server Agent, if it is running.
-out path	Specifies the destination path for output files. If not specified, the source db path is used. This option is not applicable for the '-b' backup and '-c' cleanup operations.

Important If the source and target directories are the same, the Dump and Load operations will delete the source files when the target files are created. This is done to minimize the disk space requirements when a dump/load operation is run to recapture the unused space in large database files.

Note The Dump operation will dump each database to a file in the specified location using the database file name appended by '.dbdump'. The Load operation will only load database files if a *.dbdump file is found; the name of the database file is the name without '.dbdump'.

Restoring DHCP Data from a Failover Server

You can restore DHCP data from a failover server that is more current than the result of a shadow backup. Be sure that the failover partner configurations are synchronized. Also, ensure that the following steps are run on the bad failover partner (i.e., the one whose database is bad) and that you want to restore to.

On Windows

1. Set the default path; for example:

```
SET PATH=%PATH%;.;C:\PROGRA~1\NETWOR~1\LOCAL\BIN
```

2. Stop the server agent:

```
net stop "Network Registrar Local Server Agent"
```

3. Delete the eventstore, ndb, and logs directories:

```
del C:\NetworkRegistrar\Local\data\dhcpeventstore\*.*
del C:\NetworkRegistrar\Local\data\dhcp\ndb\dhcp.ndb
del C:\NetworkRegistrar\Local\data\dhcp\ndb\logs\*.*
del C:\NetworkRegistrar\Local\data\dhcp\ndb6\dhcp6.ndb
del C:\NetworkRegistrar\Local\data\dhcp\ndb6\logs\*.*
```

Warning When removing either DHCP databases, BOTH MUST be removed - the DHCPv4 (data/dhcp/ndb) or DHCPv6 (data/dhcp/ndb6) lease databases. Removing only one (and leaving the other) is unsupported and may produce unpredictable results.

4. Restart the server agent:

```
net start "Network Registrar Local Server Agent"
```

On Linux

1. Stop the server agent:

   - RHEL/CentOS 6.x:

   ```
   /etc/init.d/nwreglocal stop
   ```

   - RHEL/CentOS 7.x:

   ```
   systemctl stop nwreglocal
   ```

2. Determine the processes running:

```
/opt/nwreg2/local/usrbin/cnr_status
```

3. Kill the remaining processes:

   ```
   kill -9 pid
   ```

4. Delete the eventstore, ndb, and logs directories:

   ```
   rm /var/nwreg2/data/dhcpeventstore/*.*

   rm -r /var/nwreg2/data/dhcp/ndb/
   rm -r /var/nwreg2/data/dhcp/ndb6/
   ```

Warning When removing either DHCP databases, BOTH MUST be removed - the DHCPv4 (data/dhcp/ndb) or DHCPv6 (data/dhcp/ndb6) lease databases. Removing only one (and leaving the other) is unsupported and may produce unpredictable results.

5. Restart the server agent:

   - RHEL/CentOS 6.x:

     ```
     /etc/init.d/nwreglocal start
     ```

   - RHEL/CentOS 7.x:

     ```
     systemctl start nwreglocal
     ```