

Network Registrar Data Backup and Recovery Strategies

Document ID: 50107

Introduction

Network Registrar Databases

DHCP Data

DNS Data

CCM Data

Backup and Recovery

DHCP

DNS

CCM

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides an overview of Network Registrar databases used for:

- DHCP lease storage
- DNS authoritative data
- CCM configuration management

This document presents different backup and recovery strategies for each type of data, based on operational considerations.

Network Registrar Databases

The Network Registrar databases include two types of embedded databases and sequential access files that are managed through the host file system. Most server data is stored in high-performance embedded databases using Berkeley DB distributed by Sleepycat Software. Configuration data is split between newer Sleepycat databases and the original Raima database distributed by Bristol Technologies.

The original Raima database is generally referred to as the MCD database, while the collection of Sleepycat configuration databases is generally referred to as the CCM database. The small amount of server data still stored in the Raima database is referred to as MCD state data, to distinguish it from the MCD configuration data managed by the CCM server. A few data items used by the Server Agent are also stored in the Raima database. These are not managed by the CCM server and are configured during installation.

Both the Sleepycat and Raima databases use transaction logs to save changes as they are committed to the databases. These are stored in associated logs subdirectories in the database directory tree. When the database performs its database checkpoints, these transactions are incorporated into the main database file, and the logs are marked redundant. The redundant logs are trimmed periodically by the servers.

It is critical that any snapshot of a given database also include all its current transaction logs. Any inconsistency between these files compromises the integrity of the database. Because the servers operate in a concurrent, multi-threaded environment, a database snapshot can only be reliably made using file system

copy commands when the servers are stopped. For this reason, you are provided the `mcshadow` utility to pause the servers while making backup copies of the server databases. The `mcshadow` utility runs automatically on a nightly basis, or you can run it manually at any time. For details on how to use the `mcshadow` utility, refer to the section on Performing Manual Backups on page 7–2 of the *Network Registrar User's Guide*.

You can export and re–import configuration data with the `cnr_exim` utility. You can use this utility to save the configuration to a simple text file in either a readable text or hexadecimal format. You must use the hexadecimal format to re–import the configuration. Whenever you export the configuration, you should export both file types concurrently. For details on how to use the `cnr_exim` utility, refer to the section on Using the `cnr_exim` Data Import and Export Tool on page 7–10 of the *Network Registrar User's Guide*.

DHCP Data

The DHCP lease database is the primary data store of the DHCP server. This database was converted to a Sleepycat database structure in version 5.0. Starting with version 6.1, both active and historical lease data are stored in a single, private, embedded Sleepycat database. The database file **`dhcp.ndb`** and its associated transaction logs are stored within the database directory tree at:

```
datadir/dhcp/ndb/
```

In versions 5.5 and 6.0, an independent Sleepycat database is used to store the historical lease data. The location of this database is configured when you enable the feature. Earlier versions do not save any historical lease data.

The DHCP server maintains a persistent event queue to store pending DNS updates or LDAP lookup events. The event queue is stored as a set of special–purpose transaction logs within the database directory tree at:

```
datadir/dhcpeventstore
```

A small amount of failover state information is stored as MCD state data. Although persisted, the data is not essential, and can be recreated from the lease data through failover re–synchronization.

All DHCP configuration data is managed in the MCD database through the CCM server.

DNS Data

The DHCP lease database is the primary data store for the DHCP server. This database was converted to a Sleepycat database structure in version 5.0. Starting with version 6.1, both active and historical lease data are stored in a single, private, embedded Sleepycat database. The database file, **`dhcp.ndb`**, and its associated transaction logs are stored within the database directory tree at:

```
datadir/dhcp/ndb/
```

The zone checkpoint files are stored at:

```
datadir/dns/zchk/
```

The DNS server maintains two cache databases that are stored as flat files in the DNS database directory. The AUTHZONE database is a cache of the authoritative zones and resource records for the server. The AUTHZONE.db is generated from the zone checkpoint files and combined with any new history stored in the changeset database after the last checkpoint was saved. This secondary data store formulates answers to authoritative queries that are not already present in the in–memory cache for the server. You can improve

server reload performance if this cache is present at startup so that it does not need to be recreated. The CACHE database is a persistent cache of the in–memory cache for the server, which is used to handle query responses. You do not have to use the CACHE.db, and you can disable it to improve performance.

A small amount of zone transfer state information is stored as MCD state data. Although persisted, the data is not essential. You can restart any zone transfers that are interrupted after the standard protocol.

All DNS configuration data are managed in the MCD database through the CCM server.

CCM Data

The CCM server:

- Manages the server configuration data stores in the MCD database
- Maintains primary data stores for local and regional CCM management functions

Local Cluster Databases

The local CCM database is the local CCM primary data store for the server. This is a new set of Sleepycat databases introduced in version 6.0. It defines:

- Management data for the local cluster configuration
- Change history for configuration objects
- A persistent queue of any propagation tasks that are pending

Propagation tasks are used to synchronize related data changes, such as CCM zone edits. You must perform these changes on the copy of the zone data stored in MCD of the server. The database files (*.db files) and their associated transaction logs are stored within the database directory tree at:

```
datadir/ccm/ndb
```

The local MCD database defines the configuration data for all servers (DHCP, DNS, and TFTP). The servers read this configuration data at startup or on reload and initialize their in–memory data structures. Changes to the configuration data are made using the management interfaces serviced by the CCM server. This ensures that the CCM databases used to present the management view of the configuration remain synchronized with the MCD database. The MCD database (**mcddb.*** files) and its associated transaction logs are stored within the database directory tree at:

```
datadir/db/
```

With Version 6.0, the CCM server maintains the change history for the MCD database and a persistent queue of any propagation tasks that are pending in a secondary Sleepycat data store. The database files (*.db files) and their associated transaction logs are stored within the database directory tree at:

```
datadir/mcd/ndb
```

Regional Cluster Databases

The regional CCM database is the primary data store for the regional CCM server. Similar to the local CCM database, the regional server defines the management data for the regional cluster configuration and change history for configuration objects.

The database files (*.db files) and their associated transaction logs are stored within the database directory tree at:

```
datadir/ccm/ndb
```

The regional CCM server manages several secondary data stores. This is a new set of Sleepycat databases introduced in version 6.1. For each local cluster managed by the regional server:

- Replica database stores a cached copy of the local server configuration
- Subnet Utilization database stores aggregated subnet utilization data collected from each local DHCP server
- Lease History database stores aggregated historical lease data collected from each local DHCP server

These three sets of database files (*.db files) and their associated transaction logs are stored within the database directory tree, respectively at:

```
datadir/replica  
datadir/subnetutil  
datadir/leasehist
```

The regional MCD database contains only the Server Agent configuration set during installation. Since this data is not managed by the CCM server, there is no secondary data store for change history. The MCD database (mcddb.* files) and its associated transaction logs are stored within the database directory tree at:

```
datadir/db/
```

Backup and Recovery

DHCP

Best practice for DHCP is to run the servers with DHCP failover enabled in a simple, server-wide failover configuration. A daily mcshadow backup and cnr_exim export of the main partner is sufficient for this configuration.

With DHCP failover enabled, a backup of the DHCP server databases is not needed. In the event that either the main or backup DHCP server fails, you can reconstitute its configuration and current lease state from the failover partner. Starting with version 6.1, you can resynchronize the DHCP failover configuration to or from the main or backup server using the regional CCM server failover configuration feature. The local CCM server failover configuration feature supports resynchronization from the main server only. If the regional CCM server is not available, you can use the cnr_exim utility to recover the configuration from the backup server. Once the failover configuration is restored between the two servers, the lease database automatically uses the the failover protocol to resynchronize. For details on how to use CCM server failover configuration features, refer to the section on Creating a Main and Backup Server Configuration on page 16–6 of the *Network Registrar User's Guide*.

You can use the same procedure to recover from a catastrophic configuration error. If both servers were misconfigured to the point where you cannot unravel the changes, the best recovery strategy is to roll back to the most recent *cnr_exim* export.

If both servers fail completely, only the main partner should be restored from the database backup. Refer to the sections on Recovering Data from Backups starting on page 7–4 of the *Network Registrar User's Guide*. Restore the backup partner by resynchronizing its configuration and lease database from the main server.

Because any backup that is restored is out of date with the current state of the network, you must enable the scope attribute `ping-clients` so that the server does not inadvertently hand out duplicate addresses. For details, refer to the web UI online help, or the Scope Command section on page 2–93 of the *Network Registrar CLI Reference*. The addresses are marked `policy attribute unavailable-timeout` if they are found to be used. The setting by default is 24 hours, but you should set it to a small value (for example, 1 hour), so that the addresses can be reused once these unknown clients obtain a new lease. For details, see the web UI online help, or the Policy Command section on page 2–82 of the *Network Registrar CLI Reference*. The servers should be left in this configuration for a full lease period to bring the DHCP lease database up-to-date.

DNS

DNS primary authoritative data may be relatively static or highly dynamic. In either case, a daily `mcshadow` backup of primary servers and daily `cnr_exim` exports of each primary, secondary, or caching server configuration should be saved. Restoring from backup may be sufficient for relatively static configurations. For more dynamic environments, consider other strategies.

If you configure a primary server to accept DNS updates, consider a high-availability (HA) cluster solution to assure uninterrupted servicing of updates. Alternatively, if a maintenance outage is acceptable, you can reconstruct the primary server from a current secondary server using the `cnr_zone_recovery` utility. An example of acceptable maintenance outage would be if you only accept administrative changes, or if DNS updates are performed by the DHCP server and queued pending the availability of the DNS server. Enable `Notify` and `IXFR` to ensure that the secondary server is always current if you use this approach. For details, refer to the sections on Enabling Incremental Zone Transfers (IXFR) and Enabling `Notify` on pages 10–5 and 10–6 of the *Network Registrar User's Guide*.

Note: Although the `cnr_zone_recovery` utility is compatible with servers starting with version 6.0, it is only found in the Network Registrar software distribution beginning with version 6.1.1. For more information, refer to the `cnr_zone_recovery` Tool section on pages 7–15 through 7–18 of the *Network Registrar User's Guide*.

To restore a secondary or caching server, the configuration should simply be rebuilt from the most recent `cnr_exim` export. The server should then restore its dynamic data from the primary server or rebuild its cache, respectively. If a server was misconfigured to the point where the changes are not easy to unravel, the best recovery strategy is to roll back to the `cnr_exim` export.

CCM

CCM configuration and management data is typically less dynamic, and daily `mcshadow` backups and `cnr_exim` export of the regional CCM server are sufficient for most deployments. (The local CCM server `mcshadow` backup and `cnr_exim` export are performed as part of the DHCP and/or DNS server backups.) Historical subnet use and lease history databases should be archived periodically to secondary media if these records are required. Older records will be trimmed from these databases once they exceed the configured age.

If the server was misconfigured to the point where the changes are not easy to unravel, the best recovery strategy is to roll back to the most recent `cnr_exim` export.

When restoring from backup, the regional CCM database could precipitate a gap in the history data collected. To avoid this, the period of data saved at the local DHCP should be greater than the backup interval. You should save at least two days of history locally to cover this gap. When the historical databases are restored from backup, the CCM server will request all data from its most current entries to the present.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Network Management
Network Infrastructure: Network Management
Virtual Private Networks: Network and Policy Management

Related Information

- **Technical Support – Cisco Systems**

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 26, 2007

Document ID: 50107
