

Recommended CNR Settings and Management

Document ID: 13390

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Standard Configuration

Recommendations for Configuration and Setup

- Initial Planning and Setup

- General System Configuration

- DHCP Configuration

- DNS Configuration

- TFTP Configuration

- CNR LDAP Configuration

- LDAP Server Tuning Parameters

Routine Procedures

Immediate Actions When Facing a Problem

- Analyze Log Files

- Check for LDAP Problems

- Verify CNR's Internal Databases

- Check DNS Data With nslookup

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This article has two purposes. First, it contains recommendations on how to configure the Cisco Network Registrar (CNR) for optimum performance and stability and how to monitor your CNR installation. Second, it contains recommendations on how you should react if a problem does occur. In the ideal case, you will read this article and act on the configuration and monitoring recommendations before any problems occur. By doing so, you will avoid problems. If you are reading this article for the first time because you have a problem with CNR, go immediately to the Immediate Actions When Facing a Problem section. For further explanation of the recommendations, please refer to the CNR User Guides and Command References.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Standard Configuration

The configuration recommendations offered here represent a starting point. If your system is configured differently from this, review your settings. Your configuration may have developed from earlier versions of CNR. CNR 5.0 and later versions provide much-improved performance compared to earlier versions, but parameter changes should be made to achieve the maximum benefit. The focus of this document is on large service provider environments, but many of the recommendations apply to other CNR environments as well. This document assumes that:

- You are a service provider running a broadband network with 10,000 subscribers or more.
- You are using CNR 5.0.3 or later.
- You are using Lightweight Directory Access Protocol (LDAP). CNR runs without LDAP, but many service providers use LDAP.
- Your network has medium IP address saturation.
- You run CNR on UNIX servers. Most of the recommendations apply equally to Windows NT, but most service providers run CNR on UNIX servers, so where UNIX and NT differ, the UNIX example is used.
- You have upstream connections to other systems (such as billing, customer care, or provisioning) that are running on other servers.
- Dynamic Domain Name System (DDNS) is not active at your site (most service providers do not use DDNS).

Recommendations for Configuration and Setup

Initial Planning and Setup

- Plan and document IP address allocation.
- Separate disk-intensive operations: put your primary DHCP server on a different machine than your LDAP server and primary DNS server.
- Document your Cable Modem Termination System (CMTS) configuration; make sure the CMTS and CNR configurations match.
- Prepare disaster recovery plans.
- Document your network topology.
- Note the Cisco IOS® Software versions of CMTSs.

The most effective steps to long term health of your network are: a) plan your configuration, b) record those plans, and c) record the changes when changes are planned and made. Documenting the reasons for choices can help during future planning sessions.

General System Configuration

- Use safe failover. Simple failover, where one server is main for all scopes, and the other server is backup for all scopes (as opposed to symmetrical failover, where both servers are main and backup at the same time, depending on the individual scope), is highly recommended, as it *simplifies greatly* the administration tasks.
- Turn on Simple Network Management Protocol (SNMP) traps. These examples are for illustration:

```
nrcmd> trap enable address-conflict
nrcmd> trap enable dhcp-failover-config-mismatch
nrcmd> trap enable other-server-not-responding
nrcmd> trap set free-address-low-threshold=15%
nrcmd> trap set free-address-high-threshold=30%
nrcmd> trap enable free-address-low
```

- Be sure you have adequate RAM (512 MB or greater).
- Be sure the data partition is large enough (2.5 GB or greater).
- Use separate partitions for logs and data.
- Ensure high-speed, low-latency connections between servers; verify interface settings.

SNMP traps enable you to monitor the DHCP server from a network monitor. Be sure to configure the traps on the DHCP server, configure the monitor to receive and display them, and obviously be sure to pay attention to the monitor.

Configuring a production system requires trade-offs of cost against system effectiveness. We suggest these values assuming about 100,000 subscribers on E250-class systems running failover. Use of many policies, client-classes, scopes, request and response buffers, DHCP extensions, and other complications affects memory needs and the performance.

The log partition (`/var/nwreg2`) should be increased if the number and size of logs is increased.

DHCP Configuration

- Set the request and response buffers for optimal throughput. Note that these recommendations have changed for CNR 5.0.

```
nrcmd> DHCP set max-dhcp-requests=500
nrcmd> DHCP set max-dhcp-responses=2000
```

- Cable modem lease time = 604800 (7 days) or more.
- Customer Premises Equipment (CPE) lease time: as long as possible (see note for trade-offs).
- Increase DHCP and TFTP log sizes:

```
nrcmd> server DHCP serverLogs nlogs=15 logsize=10M
nrcmd> server DNS serverLogs nlogs=15 logsize=10M
nrcmd> server TFTP serverLogs nlogs=10 logsize=10M
```

- Configure log settings that provide enough detail to identify problems, but do not generate excessive detail (which makes it difficult to distinguish problems and puts unnecessary load on the server). These are recommended settings that are generally applicable. Adjust your settings if necessary to deal with issues in your network:

- ◆ Activity-summary
- ◆ Default
- ◆ No-failover-activity
- ◆ Enable defer-lease-extensions
- ◆ Set last-transaction-time-granularity = $1/2$ lease interval
- ◆ Disable allow-client-lease-override for policies offering production leases.
- ◆ Enable fall-back-to-local; when LDAP is unavailable, CNR uses local data:

```
nrcmd> session set visibility=3
nrcmd> dhcp enable fallback-to-local-client-data
nrcmd> session set visibility=5
```

- If using CNR 5.5 or later, configure the client-cache capability to reduce the LDAP queries by half.

```
nrcmd> dhcp set client-cache-count=2000
nrcmd> dhcp set client-cache-ttl=5
```

To make the most effective use of CNR's throughput capability, there should be three to four times as many response buffers as request buffers. The system only uses as many buffers as it needs. As lease times become shorter, more response buffers are required.

Note: Lease times should be made as long as is practical. Cable modem leases come from a private address space (usually net-10), and the modems seldom move around to different locations on the net. These leases should be made a week or longer. CPE leases, on the other hand, come from the public address space, and CPEs (in particular, laptops) do move around. Here the lease duration must be set to match the habits of your user population. Longer leases reduce the load on the DHCP server. When using short leases (less than 8 hours), increase the response buffers to 2500.

Disable `allow-client-lease-override` to ensure that clients adhere to the lease times specified in your CNR configuration some clients attempt to override the specified setting.

Enable `fall-back-to-local` to keep your network operating in the event of an LDAP server failure. With this setting, the DHCP server continues to satisfy lease requests even though the LDAP server is not responding. The server will not have access to the specific client information that is stored in the LDAP server, so it will satisfy each request with a default setting. You must configure a default that is reasonable for your network.

Finally, the `client-cache` feature keeps in memory the client data retrieved from LDAP, so that the DHCP server needs to query LDAP only once during the discovery-offer-request-ack cycle, speeding up the DHCP server performance.

DNS Configuration

1. Enable the incremental transfer feature:

```
nrcmd> dns enable ixfr-enable
```

2. Enable notify. Refer to the CNR CLI Command References for the arguments you need to enable notify.
3. Put primary and secondary DNS servers on separate network segments.
4. Configure clients to query a secondary DNS server.

Secondary DNS servers receive their data from the primary server one of two ways: a) "full zone transfer," or b) "notify/ixfr" (incremental transfer). Using notify/ixfr reduces the number of records that must be transferred from the primary to the secondary servers. This is critical when the name space is relatively dynamic.

TFTP Configuration

- Set `initial-packet-timeout` to 2:

```
nrcmd> tftp set initial-packet-timeout = 2
```

- If using CNR 5.5 or later, enable TFTP file caching to improve performance:

```
nrcmd> tftp set home-directory=/var/nwreg2/data/tftp
nrcmd> tftp set file-cache-directory=CacheDir
nrcmd> tftp set file-cache-max-memory-size=32000
nrcmd> tftp enable file-cache
nrcmd> tftp reload
```

TFTP file caching keeps the cable modem configuration files stored in memory, avoiding reads to disk every time a cable modem requests a configuration file. A file cache directory needs to be created in the hard drive (CacheDir in the example above), and a maximum size is assigned. Choose the size taking into account the total amount of RAM in your system and the number of different configuration files needed.

The TFTP protocol does not require the client to send a final acknowledgment (ACK) packet on receipt of a file. If no ACK is received, the server must hold the client connection for the timeout period, which limits its capacity to service new requests. If your TFTP server has the resource capacity, you can also increase the

value of **max-tftp-packets** to support a greater number of client connections. The default value for this parameter is 512. The maximum value is 1000.

CNR LDAP Configuration

These settings show a configuration where CNR is writing lease updates to LDAP. If possible, design your network so this is not necessary. It is shown here to provide recommendations if you must write lease updates. Optimize LDAP connections by using separately tunable READ/WRITE LDAP objects. (Each object gets its own group of threads).

```
# Create and Configure a New LDAP Create/Update object
ldap LDAP-Write create csrc-ldap
ldap LDAP-Write set password=changeme
ldap LDAP-Write set port=389
ldap LDAP-Write set preference=1
ldap LDAP-Write setEntry query-dictionary csrcclientclass=client-class-name
ldap LDAP-Write set reactivate-interval=60s
ldap LDAP-Write set search-filter=
(&(macaddress=%s)(|(csrcclassname=Computer)(csrcclassname=Modem)))
ldap LDAP-Write set search-path=csrcprogramname=csrc,o=NetscapeRoot
ldap LDAP-Write set username=
"uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot"
ldap LDAP-Write set can-query=disabled
ldap LDAP-Write set can-create=enabled
ldap LDAP-Write set can-update=enabled
ldap LDAP-Write set connections=2
ldap LDAP-Write set limit-requests=enabled
ldap LDAP-Write set max-requests=8
ldap LDAP-Write set timeout=30s

### Create and Configure a New LDAP Read object
ldap LDAP-Read create csrc-ldap
ldap LDAP-Read set password=changeme
ldap LDAP-Read set port=389
ldap LDAP-Read set preference=1
ldap LDAP-Read setEntry query-dictionary csrcclientclass=client-class-name
ldap LDAP-Read set reactivate-interval=60s
ldap LDAP-Read set search-filter=
(&(macaddress=%s)(|(csrcclassname=Computer)(csrcclassname=Modem)))
ldap LDAP-Read set search-path=csrcprogramname=csrc,o=NetscapeRoot
ldap LDAP-Read set username=
"uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot"
ldap LDAP-Read set can-query=enabled
ldap LDAP-Read set can-create=disabled
ldap LDAP-Read set can-update=disabled
ldap LDAP-Read set connections=3
ldap LDAP-Read set limit-requests=enabled
ldap LDAP-Read set max-requests=12
ldap LDAP-Read set timeout=3s
```

The configuration shown includes having CNR write lease updates to LDAP. You may want to do this to make it possible for applications to query LDAP for current lease information, but you should try to avoid structuring your application so that this is necessary. If you need to make information available about the state of the lease for an IP address you can use the NRCMD lease command to obtain the MAC address, expiration and other information about the current status of the lease.

LDAP directories are designed to be read quickly and efficiently, but writing to an LDAP directory is inefficient. If you configure CNR to write lease information to LDAP, LDAP becomes a bottleneck to overall system performance. If you must configure LDAP lease writes, use the recommended settings. Note that CNR access to LDAP has been optimized through the use of separate "read" and "update LDAP" objects. Note also the 30 second write timeout. With a shorter timeout you run the risk of LDAP writes timing out when LDAP

is under heavy load. Then CNR retries the write, which adds additional load to LDAP.

The total number of connections to your LDAP server should not exceed the maximum number of available threads. If your LDAP server supports multiple threads per connection, the optimal number of connections is the total number of threads divided by the number of threads per connection.

LDAP Server Tuning Parameters

- Create indexes for lookup fields.
- Configure cache size to increase the number of entries cached in memory, although the cache should not exceed one third of available memory.
- Configure maximum threads to increase the number of simultaneous connections that can be supported, although this should not exceed one half of available resources.
- Configure log settings that provide enough detail to identify problems but do not generate excessive detail (which makes it difficult to distinguish problems and puts unnecessary load on the server).
- Use separate partitions for logs and data.

Specific LDAP server implementations vary. Refer to your server documentation to implement these suggestions.

Routine Procedures

- Regularly back up the CNR databases. Refer to the User Guides for instructions. You should back up the CNR databases at least once a day. Retain backup files for at least two weeks.
- Regularly back up LDAP.
- Regularly back up and archive logs.
- After changes are made to CNR, ensure that the configuration of main and backup servers in a failover scenario remains consistent. Use the **cnrFailoverConfig -compare** tool in CNR versions 5.5 and earlier, or compare the configurations using the WebUI in CNR 6.0 and later.
- When network topology changes are planned, set the DHCP renew and lease times to small values.
- Monitor IP address usage (use SNMP traps).
- Monitor system usage (memory, disk, CPU, and swap). The utility **top** is useful for this purpose.
- Periodically review logs to become familiar with the normal cases. Understanding normal logs lets you handle problems more quickly.
- Periodically review logs for exceptions: `grep` for "error", "warn", or "connect" (for example, in UNIX, use **grep -i warn name_dhcp_1_log**).

DHCP Safe-failover requires that the configuration settings for a scope be identical on the primary and backup server for that scope. Be sure, when you make a change to a setting, that you make the change on both servers. Periodically use **cnrFailoverConfig -compare** or WebUI in CNR 6.0 and above to check to make sure there are no differences.

Network topology changes or IP address allocation changes can make it necessary for clients to get a different address. You must plan for a period of time when some clients on a subnet have an address from the old range and some have renewed and gotten an address from the new range. You can reduce the amount of time during which both sets of addresses are active by reducing the length of leases before you make the change so that all of the clients have short-duration leases. This ensures that they must renew their leases frequently and therefore pick up a lease from the new range soon after you make the change. Be sure not to set the lease time so short that leases run out while you stop and start the server to make the change. After you have made the change, be sure to restore the original lease period so that you do not increase the load on the server.

The most effective approach to resolving problems is avoiding them. Following the recommendations outlined above keeps your administrators in tune with your operation and enables you to avoid serious

problems. When problems appear (such as I/O wait time increases or memory usage increases for no known reason), follow up with the logs. Review recent changes to your physical environment or CNR configuration to see if that could be the source of the problems.

The CNR logs are your friends. When starting to use CNR, upgrading CNR, or changing the CNR configuration, use the **grep** command described to check the logs for any issues. Then work backwards in the log to understand when and how the issue arose, and fix the problem.

Immediate Actions When Facing a Problem

- **Do not** reboot CMTS unless requested to do so by Cisco support staff (applies to cable environments only).
- **Do not** restart CNR unless requested to do so by Cisco support staff.
- **Do not** disable safe failover unless requested to do so by Cisco support staff.
- **Do not** reload, restart, or disrupt CNR in any way with safe failover resynchronization in progress.
- **Do** copy the log files to a directory where they will not be overwritten. If CNR crashed, copy the core file to a directory where it will not be overwritten.
- **Do** use:

```
nrcmd> server dhcp getRelatedServers
```

to isolate safe failover misconfiguration.

- **Do** look at the logs for exceptions. Check particularly the start-up sequence (this may be in an old log): **grep** for "error", "warn", or "connect" (e.g. **grep -i error name_dhcp_1_log***).

When you face a problem, it is crucial that you cause no further harm while isolating and fixing the initial problem. Rebooting a CMTS or restarting CNR creates immediate load spikes during a time when the system is already fragile. The objective is to have your system fully functional again in the shortest period of time. The elapsed time until your last action counts; the time to your first action does not count. In other words, do not take quick action just for the sake of quick action. Think before you act.

Start a log of all steps taken and all changes made anywhere in the system: DHCP, DNS, or TFTP servers, and changes made to any CMTS or cable modem. Describe the problem and log, in detail, just the observable behavior.

Analyze Log Files

Collect the logs (`/var/nwreg2/logs`). Analyze these, looking for errors or warnings. Use a text editor to further analyze errors of interest. Starting from the error, search back in the log for all entries relating to the MAC address, IP address, or domain name associated with the error.

You may need to turn on additional logging to diagnose DHCP problems. The DHCP server supports an extensive range of logging capabilities. Refer to the CNR CLI Command References for a list of logging options and an explanation of each. Be careful, since each log message places load on the server. You must make a trade-off between the amount of information you ask CNR to log and server performance.

Check for LDAP Problems

The problem may be with the LDAP server. CNR builds a queue of requests to the LDAP server. If the LDAP server cannot keep up with the load, the queue builds up. Look in the `/var/nwreg2/data/dhcpeventstore` directory. Event store files are fixed in size, so if the queue is building up, CNR creates more files. If there is more than one file in the directory, this indicates that the queue is backing up. The same queue is used to queue requests to the DNS server, so if the queue is backing up, and you are using DDNS, it could be filling

with requests to the DNS server. To determine whether the problem is with LDAP, turn on additional CNR LDAP interface logging. Enable the log flags **ldap-create-detail**, **ldap-query-detail**, and **ldap-update-detail**. The log message include time stamps that help you determine whether LDAP is the system bottleneck.

Verify CNR's Internal Databases

If you suspect the problem may be that one or more of CNR's internal databases has lost integrity, refer to the CNR User Guides to learn how to run the database validity check utilities. If one of these utilities indicates a problem, continue to follow the directions in the User Guides to resolve it.

Check DNS Data With nslookup

The utility **nslookup** is included both with UNIX systems and with Windows NT. It can be used to interrogate a DNS server and therefore is useful in verifying the data stored by the server. The documentation for your operating system provides detailed information on its capabilities.

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

- [Cisco CNS Network Registrar Tech Notes](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 26, 2005

Document ID: 13390
