

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[标准配置](#)

[配置和设置推荐](#)

[初始计划和设置](#)

[一般系统配置](#)

[DHCP 配置](#)

[DNS 配置](#)

[TFTP 配置](#)

[CNR IDAP 配置](#)

[LDAP 服务器调整参数](#)

[常规程序](#)

[遇到问题时应立即采取的措施](#)

[分析日志文件](#)

[检查 LDAP 问题](#)

[验证 CNR 的内部数据库](#)

[用nslookup检查DNS数据](#)

[相关信息](#)

简介

此条款有两个目的。首先，它包含关于如何配置Cisco网络认证(CNR)最佳性能和稳定性的和如何的建议监控您的CNR安装。其次，它包含关于您如何的建议应该起反应，如果问题发生。理想的状况，在所有问题发生前，您在配置和监视推荐上将读此条款和操作。通过这样执行，您将避免问题。如果第一次阅读此条款，因为您有一问题CNR，请立即去[即时动作，当面对Problem部分时](#)。对于建议的进一步说明，请参考CNR[用户指南](#)和[命令参考](#)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

标准配置

提供的配置推荐此处代表起点。如果您的系统配置与此不同，请查看您的设置。您的配置可能从CNR更早版本开发。CNR 5.0及以上版本提供很大改进的性能与更早版本比较，但是应该做参数改变达到最大优点。本文焦点在大服务提供商环境，但是许多建议应用对其他CNR环境。本文假设那：

- 您是服务提供商运行宽带网络的以10,000个用户或更多。
- 您使用CNR 5.0.3或以后。
- 您使用轻量级目录访问协议(LDAP)。CNR运行，不用LDAP，但是许多服务提供商使用LDAP。
- 您的网络有中等IP地址饱和。
- 您运行在UNIX服务器的CNR。大多建议同等适用与Windows NT，但是多数服务提供商运行在UNIX服务器的CNR，因此UNIX和NT有所不同的地方，使用UNIX示例。
- 您有对在其他服务器运行的其他系统的上行联系(例如计费、用户关怀或者供应)。
- 动态域名系统(DDNS)不是活跃的在您的站点(多数服务提供商不使用DDNS)。

配置和设置推荐

初始计划和设置

- 规划和文档IP地址分配。
- 独立的磁盘密集操作：比您的LDAP服务器和主DNS服务器放置您的主要的DHCP服务器在一个不同的计算机。
- 描述您的有线调制解调器终端系统(CMTS)配置;确保CMTS和CNR配置匹配。
- 准备灾难恢复计划。
- 描述您的网络拓扑。
- 注释CMTS Cisco IOS软件版本。

对您的网络长期健康的最有效的步骤是：当变动计划并且做时， a)计划您的配置， b)记录那些规划和c)记录更改。在未来规划会话期间，描述选择的原因可帮助。

一般系统配置

- 请使用安全故障切换。简单故障切换，一个服务器为所有范围是主要和另一个服务器为所有范围是备份(与对称故障切换相对，两个服务器主要，并且备份同时，根据单个范围)，是高度推荐的，因为非常地简单化管理任务。
- 启动简单网络管理协议(SNMP)陷阱。这些示例是为说明：

```
nrcmd> trap enable address-conflictnrcmd> trap enable dhcp-failover-config-mismatchnrcmd> trap enable other-server-not-respondingnrcmd> trap set free-address-low-threshold=15%nrcmd> trap set free-address-high-threshold=30%nrcmd> trap enable free-address-low
```
- 请务必您有足够的RAM (512 MB或更加极大)。
- 请务必数据分区足够大(2.5 GB或更加极大)。
- 请使用单独的分区日志和数据。
- 保证服务器之间的高速，低潜伏期连接;验证接口设置。

SNMP陷阱使您监控从网络监控器的DHCP服务器。请务必配置在DHCP服务器的陷阱，配置监视器接收和显示他们和明显地是肯定注意监视器。

配置生产系统要求开销交换系统效率。建议这些值假设大约E250-class系统的我们100,000个用户运行故障切换。使用许多策略、客户端类别、范围、请求和答复缓冲区、DHCP扩展和其他复杂化影响内存需要和性能。

应该增加日志分区(/var/nwreg2)，如果数量和大小日志增加。

DHCP 配置

- 设置最佳吞吐量的请求和答复缓冲区。注意这些建议为CNR5.0更改。`nrcmd> DHCP set max-dhcp-requests=500``nrcmd> DHCP set max-dhcp-responses=2000`
- 有线调制解调器租用时间= 604800 (7天)或更多。
- 客户端前置设备(CPE)租用时间：越久越好(请参阅注意关于交换)。
- 增加DHCP和TFTP日志大小：`nrcmd> server DHCP serverLogs nlogs=15 logsize=10M``nrcmd> server DNS serverLogs nlogs=15 logsize=10M``nrcmd> server TFTP serverLogs nlogs=10 logsize=10M`
- 配置提供足够的细节识别问题的日志设置，但是请勿生成在服务器上使困难区分问题并且把多余的负载放)的过多的详细信息(。这些是通常可适用的推荐的设置。如果需要，调节您的设置处理在您的网络的问题：行为总结默认无故障切换活动`defer-lease-extensions Enable (event)``last-transaction-time-granularity集= 1/2租期间隔``allow-client-lease-override禁用`提供制作租期的策略的。`fall-back-to-local Enable (event)`;当LDAP不可用时，CNR使用本地数据
：`nrcmd> session set visibility=3``nrcmd> dhcp enable fallback-to-local-client-data``nrcmd> session set visibility=5`
- 如果曾经CNR 5.5或以上，配置客户端缓存功能由半减少LDAP查询。`nrcmd> dhcp set client-cache-count=2000``nrcmd> dhcp set client-cache-ttl=5`

要做最有效的使用CNR的吞吐量功能，应该有三到四次许多答复缓冲区作为请求缓冲区。当需要，系统只使用许多缓冲区。作为租期计时变得更短，更多答复缓冲区要求。

注意：租期时间，只要是实用的，应该做。有线调制解调器租期来自专用地址空间(通常net-10)，并且调制解调器很少搬到网的不同位置。应该做这些租期周或更加长。另一方面，CPE租期来自公共地址空间和CPE (特别是，膝上型计算机)移动。此处必须设置租约期限匹配您的用户群习性。长期租赁减少在DHCP服务器的负载。当曾经短租期(少于8个小时)时，请增加答复缓冲区到2500。

禁用`allow-client-lease-override`保证客户端遵守在您的CNR配置方面指定的租期时代？一些客户端尝试改写指定的设置。

在LDAP服务器失败情形下，启用`fall-back-to-local`继续您的网络操作。使用此设置，DHCP服务器继续满足租期请求，即使LDAP服务器不响应。服务器不会访问在LDAP服务器存储的特定客户端信息，因此对默认设置将满足每请求。您必须配置为您的网络是合理的默认。

最后，一次只在`discovery-offer-request-ack`周期期间，客户端缓存功能在客户端数据从LDAP获取的内存保留，因此DHCP服务器需要查询LDAP，加速DHCP服务器性能。

DNS 配置

1. 启用增量传输功能：`nrcmd> dns enable ixfr-enable`
2. Enable (event)通知。参考您需要启用通知的参数的[CNR CLI命令参考资料](#)。
3. 把主备DNS服务器放在独立的网络分段上。
4. 配置客户端查询辅助DNS服务器。

辅助DNS服务器接收他们的从主服务器两种方式一的数据：a) “全双工区域传输”，或b) “通知/ixfr” (递增转移)。使用请通知/ixfr减少必须从主要的转接到辅助服务器的记录数。当名称空间相对动态时，这是关键。

TFTP 配置

- **initial-packet-timeout**集到2 : `nrcmd> tftp set initial-packet-timeout = 2`
- 如果曾经CNR 5.5或以上，使TFTP文件高速缓冲存储改进性能：`nrcmd> tftp set home-directory=/var/nwreg2/data/tftpnrcmd> tftp set file-cache-directory=CacheDirnrcmd> tftp set file-cache-max-memory-size=32000nrcmd> tftp enable file-cachenrcmd> tftp reload`

在有线调制解调器请求配置文件时候，TFTP文件高速缓冲存储在内存保留有线调制解调器配置文件存储，避免读到磁盘。文件缓存目录在硬盘驱动器(在以上示例的CacheDir需要创建)，并且一个最大大小分配。选择考虑到总量在您的系统和需要的不同的配置文件数量的RAM的大小。

TFTP协议不要求客户端发送在文件的收据的一最终确认(ACK)数据包。如果ACK没有接收，服务器必须拿着客户端连接为超时周期，限制其能力服务新建的请求。如果您的TFTP server有资源产能，您能也增加值**max-tftp-packets**支持客户端连接一个更加了不起的编号。此参数的默认值是512。最大值是1000。

CNR IDAP 配置

这些设置显示配置CNR写入租期更新对LDAP的地方。若可能，请设计您的网络不如此这是必要的。它显示此处提供建议是否必须写入租期更新。通过使用个别调整的读取/写入LDAP对象，最优化LDAP连接。(每个对象获得其线索的自己的组)。

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

显示的配置包括有CNR写入租期更新对LDAP。您也许要执行此成为可能为了应用程序能查询LDAP当前租赁信息，但是您应该设法避免构造您的应用程序，以便这是必要的。如果需要做关于租期的状态的有用的资料IP地址的您能使用nrcmd lease命令得到MAC地址、有效期和其他信息关于租期的当前状态。

LDAP目录设计读迅速和高效，但是对LDAP目录的文字是效率低的。如果配置CNR写入租赁信息到LDAP，LDAP变为瓶颈对整个系统性能。如果必须配置LDAP租期写入，使用推荐的设置。注意对LDAP的CNR访问通过独立的“读的”使用，并且“请更新LDAP”对象优化。注意30秒也写入超时。使用您冒LDAP之险的一更短的超时写入定时，当LDAP在重载下时。然后CNR再试写入，添加额外的开销到LDAP。

连接总数对您的LDAP服务器的不应该超出可用的线索最大。如果您的LDAP服务器支持多个线索每连接，连接最佳数量是线索数量分开的线索的总数每连接。

LDAP 服务器调整参数

- 创建查找字段的索引。
- 配置缓存容量增加在内存缓存的条目数量，虽然缓存不应该超过可利用的内存的三分之一。
- 配置最大线程数增加可以支持同时连接的数量，虽然这不应该超出可用资源一半的。
- 配置提供足够的细节识别问题的日志设置，但是请勿生成在服务器上使困难区分问题并且把多余的负载放)的过多的详细信息(。
- 请使用单独的分区日志和数据。

特定LDAP服务器实施变化。参考您的服务器文档实现这些建议。

常规程序

- 请有规律备份CNR数据库。参考[用户指南](#)关于说明。您应该至少一天一次备份CNR数据库。保留备份文件至少两周。
- 请有规律备份LDAP。
- 正常备份和归档日志。
- 在变动做对CNR后，请保证主和备份服务器的配置在故障切换方案依然是一致。请使用 `cnrFailoverConfig` -在CNR版本5.5和以下的[比较工具](#)或者比较配置使用在CNR 6.0的WebUI及以后。
- 当网络结构更改计划时，设置DHCP更新并且租用时期对小值。
- 监控IP地址使用情况(使用SNMP陷阱)。
- 监控系统用法(内存、磁盘、CPU和交换)。工具[顶部](#)为此是有用的。
- 周期地请检查日志熟悉正常案件。了解正常日志让您迅速处理问题。
- 周期地例外的复核日志：error、"warn"或者"Connect"的grep (例如，在UNIX，使用`grep -i warn name_dhcp_1_log`)。

DHCP安全故障切换要求范围的配置设置是相同的在该范围的主要和备份服务器。请务必，当您做出变化对设置时，您在两个服务器做变动。周期地使用`cnrFailoverConfig` -[比较](#)或在CNR 6.0的WebUI以上检查确保那里是没有差异。

网络结构更改或IP地址分配更改能使必要为了客户端能得到一个不同的地址。您必须一段时间计划，当子网的一些客户端有从旧有范围时的一个地址，并且一些从新的范围更新了并且得到了地址。您可以减少期间两套地址通过减少长度是活跃的租期的时间在，在您做变动前，以便所有客户端有持续时间租期。这保证他们必须更新他们的租期频繁地并且选择从新的范围的一租期，在您做变动后。请务必不如此设置被耗尽的租期的租用时间短，当您中断并且启动服务器做变动时。在您做了变动后，请务必恢复原始租赁期限，以便您不增加在服务器的负载。

对解决的问题的最有效的方法避免他们。在概述的建议之后以上保持您的管理员与您的操作一致并且使您避免严重问题。当问题出现(例如I/O等待时间增加或内存使用增加为未知原因)，请进一步进行日志。如果那可能是问题的来源，请检查对您的物理环境或CNR配置的最近更改发现。

CNR日志是您的朋友。当开始使用CNR，升级CNR或者更改CNR配置，使用描述的[grep命令](#)检查日志所有问题。然后向后请工作在日志了解问题何时并且怎样出现了，并且解决问题。

[遇到问题时应立即采取的措施](#)

- 请勿重新启动CMTS，除非请求的由Cisco技术支持人员如此执行(适用于仅电缆环境)。
- 请勿重新启动CNR，除非请求的由Cisco技术支持人员如此执行。
- 请勿禁用安全故障切换，除非请求的由Cisco技术支持人员如此执行。
- 请勿重新加载，重新启动或者打乱CNR用所有方式以进展中安全故障切换的再同步。
- 请复制日志文件对他们不会覆盖的目录。如果CNR失败了，请复制内核文件对不会覆盖的目录。
- 请使用：`nrCmd> server dhcp getRelatedServers`隔离安全故障切换误配置。
- 请查看日志为例外。检查特殊启动顺序(这可能在一本旧有日志)：error、"warn"或者"Connect"的(即`grep 我错误 name_dhcp_1_log*`) grep。

当您面对问题时，是关键的不导致进一步害处，当隔离和修复最初的问题时。当系统已经是易碎的，重新启动CMTS或重新启动CNR创建立即负载阻止在时候。目标再将有您的系统功能完备的在最短的时期。直到您的上一操作计数的消逝的时间;对您的第一操作的时间不计数。换句话说，为了快速着想请勿采取快速动作。在您操作前，请认为。

开始做的所有步骤采取的和所有变化日志任何地方在system:上DHCP、DNS或者做的TFTP服务器和变动对任何CMTS或有线调制解调器。描述问题和日志，详细，可测的行为。

[分析日志文件](#)

收集日志(/var/nwreg2/logs)。分析这些，寻找错误或警告。请使用文本编辑进一步分析错误利益。由错误开始，请搜索在日志的上一步所有条目与MAC地址、IP地址或者域名相关关联与错误。

您可能需要打开另外的记录日志诊断DHCP问题。DHCP服务器支持各种各样的日志功能。参考日志选项列表和其中每一的说明的[CNR CLI命令参考资料](#)。因为每日志消息在服务器，放置负载小心。您必须做在您请求CNR记录和服务器性能的信息量之间的一个折衷方案。

[检查 LDAP 问题](#)

问题可能是LDAP服务器。CNR构件请求队列到LDAP服务器。如果LDAP服务器不能跟上负载，队列加强。查找在/var/nwreg2/data/dhcpeventstore目录。事件存储文件在大小上修复，因此，如果队列加强，CNR创建更多文件。如果有超过在目录的一个文件，这表明队列备份。同一个队列用于排队请求到DNS服务器，因此，如果队列备份和您使用DDNS，它可能填充用请求到DNS服务器。要确定问题是否是LDAP，请打开另外的CNR LDAP接口记录日志。启用日志标志**ldap-create-detail**，**ldap-query-detail**和**ldap-update-detail**。日志消息包括时间戳帮助您确定LDAP是否是系统瓶颈。

[验证 CNR 的内部数据库](#)

如果怀疑问题可能是一个或很多CNR的内部数据库丢失完整性，参考CNR[用户指南](#)学习如何运行数据库有效性检查工具。如果这些工具之一指示一问题，请继续跟随在[用户指南的](#)方向解决它。

[用nslookup检查DNS数据](#)

工具nslookup包括用UNIX系统和与Windows NT。它可以用于询问DNS服务器并且是有用的在验证服务器存储的数据。您的操作系统的文档在其功能提供详细信息。

[相关信息](#)

- [Cisco CNS网络注册程序技术说明](#)
- [技术支持 - Cisco Systems](#)