建議的CNR設定和管理

目錄

簡介

本文有兩個目的。首先，它包含有關如何配置Cisco Network Registrar(CNR)以獲得最佳效能和穩定性以及如何監控CNR安裝的建議。第二，它包含關於在發生問題時如何反應的建議。在理想情況下，您將在出現任何問題之前閱讀本文並根據配置和監控建議採取行動。這樣可以避免問題。如果您是第一次閱讀此文，因為CNR有問題，請立即轉至遇到問題時的立即操作部分。有關建議的進一步說明，請參閱CNR用戶指南和命令參考。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

標準配置

此處提供的配置建議是一個起點。如果您的系統配置與此不同，請檢視您的設定。您的配置可能是由早期版本的CNR開發的。與早期版本相比，CNR 5.0及更高版本提供了更好的效能，但應更改引數以實現最大收益。本文檔重點介紹大型服務提供商環境，但許多建議也適用於其他CNR環境。本檔案假設：

- 您是一家運營寬頻網路的服務提供商，擁有10,000名或以上的使用者。
- 您使用的是CNR 5.0.3或更高版本。
- 您正在使用輕量型目錄訪問協定(LDAP)。CNR運行不帶LDAP，但許多服務提供商使用LDAP。
- 您的網路具有中等的IP地址飽和度。
- 您在UNIX伺服器上運行CNR。大多數建議同樣適用於Windows NT，但大多數服務提供商在UNIX伺服器上運行CNR，因此在UNIX和NT不同的情況下，使用UNIX示例。
- 您有到其他伺服器上運行的其他系統（如計費、客戶服務或調配）的上游連線。
- 動態域名系統(DDNS)在您的站點上處於非活動狀態（大多數服務提供商不使用DDNS）。

配置和設定建議

初始規劃和設定

- 規劃和記錄IP地址分配。
- 獨立的磁碟密集型操作：將主DHCP伺服器置於與LDAP伺服器和主DNS伺服器不同的電腦上。
- 記錄您的纜線資料機終端系統(CMTS)組態；確保CMTS和CNR配置匹配。
- 準備災難恢復計畫。
- 記錄網路拓撲。
- 注意CMTS的Cisco IOS®軟體版本。

實現網路長期正常運行的最有效步驟包括：a)規劃您的配置，b)記錄這些計畫，以及c)在計畫和做出更改時記錄更改。記錄選擇的原因有助於在未來的規劃會議中進行選擇。

常規系統配置

- 使用安全故障轉移。強烈建議使用簡單故障轉移，即一台伺服器為所有範圍的主要，另一台伺服器為所有範圍進行備*份(與對稱故障轉移*相反，兩台伺服器同時為主和備份，具體取決於各個範圍)，因為它極大地簡化了管理任務。
- 開啟簡單網路管理協定(SNMP)陷阱。以下範例舉例說明：

```
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
```

- 請確保您有充足的RAM（512 MB或更高）。
- 確保資料分割槽足夠大（2.5 GB或更高）。
- 對日誌和資料使用單獨的分割槽。
- 確保伺服器之間的高速、低延遲連線；驗證介面設定。

SNMP陷阱使您能夠從網路監視器監視DHCP伺服器。請務必在DHCP伺服器上配置陷阱，將監控器配置為接收和顯示這些陷阱，並且請務必注意監控器。

配置生產系統需要在成本與系統有效性之間進行權衡。我們建議這些值，假設運行故障切換的E250類系統上有大約10萬使用者。使用許多策略、客戶端類、範圍、請求和響應緩衝區、DHCP擴展以及其他複雜因素會影響記憶體需求和效能。

如果日誌數量和大小增加，應增加日誌分割槽(/var/nwreg2)。

DHCP配置

- 設定請求和響應緩衝區以實現最佳吞吐量。請注意，對於CNR 5.0，這些建議已更改。

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

- 電纜數據機租用時間= 604800（7天）或更多。
- 客戶端裝置(CPE)租賃時間：儘可能長（有關折衷方案，請參閱註釋）。
- 增加DHCP和TFTP日誌大小：

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

- 配置日誌設定，該設定提供足夠詳細資訊以識別問題，但不會生成過多的詳細資訊（這導致難以區分問題並將不必要的負載置於伺服器上）。 這些是通常適用的建議設定。如有必要，請調整您的設定，以處理網路問題：活動摘要預設No-failover-activity啟用defer-lease-extensionsSet last-transaction-time-granularity = *1/2租用間隔*為提供生產租賃的策略禁用allow-client-lease-override。支援回退到本地；當LDAP不可用時，CNR使用本地資料：

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

- 如果使用CNR 5.5或更高版本，請配置客戶端快取功能以將LDAP查詢減少一半。

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

為了最有效地利用CNR的吞吐量能力，響應緩衝區的數量應該是請求緩衝區的3到4倍。系統僅使用所需的任意數量的緩衝區。隨著租用時間的縮短，需要更多的響應緩衝區。

注意：只要切實可行，就應設定租用時間。纜線資料機租賃來自私人位址空間（通常為net-10），而資料機很少會移動到網路上的不同位置。這些租約應為期一週或更長時間。另一方面，CPE租賃來自公共地址空間，而CPE（尤其是筆記型電腦）確實會移動。此處必須設定租期以符合使用者群體的習慣。租用時間越長，DHCP伺服器的負載越低。使用短租約（少於8小時）時，將響應緩衝區增加到2500。

禁用allow-client-lease-override以確保客戶端遵守在CNR配置中指定的租用時間 — 某些客戶端嘗試覆蓋指定的設定。

啟用回退到本地功能，以便在LDAP伺服器出現故障時保持網路正常運行。通過此設定，即使

LDAP伺服器沒有響應，DHCP伺服器仍繼續滿足租用請求。伺服器將無權訪問儲存在LDAP伺服器中的特定客戶端資訊，因此它將使用預設設定滿足每個請求。您必須設定適用於您網路的預設值。

最後，客戶端快取功能將從LDAP檢索到的客戶端資料保留在記憶體中，因此DHCP伺服器只需在discovery-offer-request-ack週期中查詢LDAP一次，從而提高了DHCP伺服器效能。

DNS配置

1. 啟用增量傳輸功能：
   ```
   nrcmd> dns enable ixfr-enable
   ```
2. 啟用通知。有關需要啟用通知的引數，請參閱CNR CLI命令參考。
3. 將主DNS伺服器和輔助DNS伺服器放在不同的網段上。
4. 配置客戶端以查詢輔助DNS伺服器。

輔助DNS伺服器通過兩種方式之一從主伺服器接收其資料：a)「全區傳輸」或b)「通知/ixfr」（增量傳輸）。 使用notify/ixfr可以減少必須從主伺服器傳輸到輔助伺服器的記錄的數量。這在名稱空間相對動態時非常重要。

TFTP配置

- 將initial-packet-timeout設定為2:
  ```
  nrcmd> tftp set initial-packet-timeout = 2
  ```
- 如果使用CNR 5.5或更高版本，請啟用TFTP檔案快取以提高效能：
  ```
  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檔案快取將電纜數據機配置檔案儲存在記憶體中，避免每次電纜數據機請求配置檔案時都讀取磁碟。需要在硬碟中建立一個檔案快取目錄（在上面的示例中為CacheDir），並分配一個最大大小。根據系統中RAM的總量和所需的不同配置檔案的數量選擇大小。

TFTP協定不要求客戶端在收到檔案時傳送最終確認(ACK)資料包。如果未收到ACK，伺服器必須在超時期限內保持客戶端連線，這限制了伺服器為新請求提供服務的能力。如果TFTP伺服器具有資源容量，您還可以增加max-tftp-packets的值以支援更多數量的客戶端連線。此引數的預設值為512。最大值為1000。

CNR LDAP配置

這些設定顯示CNR正在向LDAP寫入租用更新的配置。如果可能，請設計您的網路，這樣就不需要了。此處顯示的內容旨在提供如果您必須寫入租用更新的建議。通過使用單獨可調的讀/寫LDAP對象最佳化LDAP連線。（每個對象都有自己的執行緒組）。

```
# 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
```

顯示的配置包括對LDAP進行CNR寫租用更新。您可能希望這樣做，以使應用程式能夠查詢LDAP以獲取當前租賃資訊，但您應儘量避免構建應用程式，以便這是必要的。如果您需要提供有關IP地址租用狀態的資訊，可以使用NRCMD lease命令來獲取MAC地址、到期日期以及租用當前狀態的其他資訊。

LDAP目錄設計為可快速高效地讀取，但寫入到LDAP目錄效率低下。如果將CNR配置為向LDAP寫入租用資訊，則LDAP將成為整體系統效能的瓶頸。如果必須配置LDAP租用寫入，請使用建議的設定。請注意，CNR對LDAP的訪問已通過使用單獨的「讀取」和「更新LDAP」對象進行了最佳化。另請注意30秒的寫入超時。使用較短的超時時間，在LDAP負載較重時，您將面臨發生LDAP寫入超時風險。然後CNR重試寫入，這會向LDAP新增更多負載。

與LDAP伺服器的連線總數不應超過可用執行緒的最大數量。如果LDAP伺服器支援每個連線有多個執行緒，則最佳連線數是將執行緒總數除以每個連線的執行緒數。

LDAP伺服器調整引數

- 為查詢欄位建立索引。
- 配置快取大小以增加記憶體中快取的條目數，但快取不應超過可用記憶體的三分之一。
- 配置最大執行緒以增加可支援的併發連線數，雖然這不應超過可用資源的一半。
- 配置日誌設定，該設定提供足夠詳細資訊來識別問題，但不會生成過多的詳細資訊（這導致難以區分問題並將不必要的負載置於伺服器上）。
- 對日誌和資料使用單獨的分割槽。

具體的LDAP伺服器實施各不相同。請參閱您的伺服器文檔以實施這些建議。

例行程式

- 定期備份CNR資料庫。有關說明，請參閱使用手冊。您應該每天至少備份CNR資料庫一次。將備份檔案保留至少兩週。
- 定期備份LDAP。
- 定期備份和歸檔日誌。
- 對CNR進行更改後，確保故障切換場景中主伺服器和備份伺服器的配置保持一致。在CNR 5.5及更低版本中使用**cnrFailoverConfig -compare**工具，或者在CNR 6.0及更高版本中使用WebUI比較配置。
- 規劃網路拓撲更改時，將DHCP續訂和租用時間設定為較小的值。
- 監控IP地址使用情況（使用SNMP陷阱）。
- 監控系統使用情況（記憶體、磁碟、CPU和交換）。 實用程式**top**對此很有用。
- 定期檢視日誌，熟悉正常情況。通過瞭解普通日誌，可以更快地處理問題。
- 定期檢視異常日誌：grep表示「error」、「warn」或「connect」(例如，在UNIX中，使用**grep -i warn name_dhcp_1_log**)。

DHCP安全故障轉移要求作用域的配置設定在該作用域的主伺服器和備份伺服器上相同。在對設定進行更改時，請確保在兩個伺服器上都進行了更改。定期使用**cnrFailoverConfig -compare**或CNR 6.0及更高版本中的WebUI進行檢查以確保沒有差異。

網路拓撲更改或IP地址分配更改可能會使客戶端必須獲取其他地址。您必須規劃一段時間，使子網中的某些客戶端具有舊範圍的地址，而某些客戶端已更新並獲得新範圍的地址。您可以在更改之前縮短租用時間，以便所有客戶機都具有短期租用，從而縮短這兩組地址處於活動狀態的時間量。這可以確保他們必須頻繁續訂租約，因此在您做出更改後很快會從新範圍中選擇租約。請勿將租用時間設定得過短，以便在停止並啟動伺服器進行更改時租期結束。進行更改後，請務必恢復原始租用期，以便不增加伺服器上的負載。

解決問題最有效的方法是避免這些問題。遵循上述建議可使管理員與您的操作保持同步，從而避免出現嚴重問題。當出現問題時（例如I/O等待時間增加或記憶體使用率因未知原因而增加），請跟蹤日誌。檢視您的物理環境或CNR配置最近發生的更改，確定這些更改是否可能是問題的根源。

CNR日誌是您的朋友。開始使用CNR、升級CNR或更改CNR配置時，請使用所述的**grep**命令檢查日誌中是否存在任何問題。然後在日誌中向後工作，以瞭解出現問題的時間和方式，並修復問題。

面臨問題時立即採取的操作

- ***除非思科***支援人員要求重新啟動CMTS，否則不要重新啟動CMTS（僅適用於電纜環境）。
- ***除非思科***支援人員要求重新啟動CNR，否則不要重新啟動CNR。
- ***除非思科***支援人員要求安全故障轉移，否則不要禁用安全故障轉移。
- ***在進行安***全故障切換重新同步時，請勿以任何方式重新載入、重新啟動或中斷CNR。
- ***請***將日誌檔案複製到不會覆蓋的目錄中。如果CNR崩潰，請將核心轉儲檔案複製到不會覆蓋它的目錄中。
- Do use:

  ```
  nrcmd> server dhcp getRelatedServers
  ```

  隔離安全故障切換配置錯誤。
- ***請***檢視日誌以發現異常。請特別檢查啟動順序（這可能位於舊日誌中）：grep for "error"、"warn"或"connect"(例如**grep -i error name_dhcp_1_log***)。

當您面臨問題時，隔離和修復最初的問題時不要造成進一步的傷害，這一點至關重要。重新啟動

CMTS或重新啟動CNR會在系統已脆弱時立即產生負載峰值。目的是讓您的系統在最短時間內重新完全正常工作。上一次操作計數所用的時間；第一次操作的時間不算。換句話說，不要為了快速行動而採取快速行動。行動前先思考。

啟動一個日誌，記錄系統中任何位置執行的所有步驟和所做的所有更改：DHCP、DNS或TFTP伺服器，以及對任何CMTS或電纜數據機所做的更改。描述問題並詳細記錄可觀察行為。

分析日誌檔案

收集日誌(/var/nwreg2/logs)。 分析這些資訊，查詢錯誤或警告。使用文本編輯器進一步分析感興趣的錯誤。從錯誤開始，在日誌中重新搜尋與錯誤關聯的MAC地址、IP地址或域名相關的所有條目。

您可能需要開啟其他日誌記錄來診斷DHCP問題。DHCP伺服器支援廣泛的日誌記錄功能。請參閱CNR CLI命令參考以瞭解日誌記錄選項清單和每個日誌記錄選項的說明。請小心，因為每個日誌消息都會在伺服器上放置負載。您必須在要求CNR記錄的資訊量與伺服器效能之間進行權衡。

檢查LDAP問題

問題可能是LDAP伺服器。CNR生成到LDAP伺服器的請求隊列。如果LDAP伺服器無法跟上負載，則隊列將建立。在/var/nwreg2/data/dhcpeventstore目錄中查詢。事件儲存檔案的大小是固定的，因此，如果隊列正在增加，CNR將建立更多檔案。如果目錄中有多個檔案，則表示隊列正在備份。相同的隊列用於排隊DNS伺服器的請求，因此，如果隊列正在備份，而您正在使用DDNS，則隊列可能包含對DNS伺服器的請求。要確定問題是否與LDAP有關，請開啟其他CNR LDAP介面日誌記錄。啟用日誌標誌**ldap-create-detail**、**ldap-query-detail**和**ldap-update-detail**。日誌消息包含時間戳，可幫助您確定LDAP是否是系統瓶頸。

檢驗CNR的內部資料庫

如果您懷疑問題可能是一個或多個CNR內部資料庫丟失了完整性，請參閱CNR User Guides以瞭解如何運行資料庫有效性檢查實用程式。如果其中某個實用程式指示出現問題，請繼續按照使用手冊中的說明解決問題。

使用nslookup檢查DNS資料

UNIX系統和Windows NT中都包含實用程式**nslookup**。它可用於查詢DNS伺服器，因此可用於驗證伺服器儲存的資料。作業系統文檔提供了有關其功能的詳細資訊。

相關資訊

- 《Cisco CNS Network Registrar技術說明》
- 技術支援 - Cisco Systems