Empfohlene CNR-Einstellungen und -Verwaltung

Inhalt

Einführung

Dieser Artikel hat zwei Ziele. Zunächst enthält es Empfehlungen zur Konfiguration des Cisco Network Registrar (CNR) für optimale Leistung und Stabilität sowie zur Überwachung Ihrer CNR-Installation. Zweitens enthält es Empfehlungen, wie Sie reagieren sollten, wenn ein Problem auftritt. Im Idealfall lesen Sie diesen Artikel und befolgen Sie die Konfigurations- und Überwachungsempfehlungen, bevor Probleme auftreten. Auf diese Weise vermeiden Sie Probleme. Wenn Sie diesen Artikel zum ersten Mal lesen, weil Sie ein Problem mit CNR haben, fahren Sie sofort mit dem Abschnitt "Sofortige Maßnahmen bei Problemen" fort. Weitere Erläuterungen zu den Empfehlungen finden Sie in den CNR-Benutzerhandbüchern und Befehlsreferenzen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Standardkonfiguration

Die hier angebotenen Konfigurationsempfehlungen stellen einen Ausgangspunkt dar. Wenn Ihr System anders konfiguriert ist, überprüfen Sie Ihre Einstellungen. Ihre Konfiguration wurde möglicherweise aus früheren CNR-Versionen entwickelt. CNR 5.0 und neuere Versionen bieten im Vergleich zu früheren Versionen eine deutlich verbesserte Leistung, aber Parameteränderungen sollten vorgenommen werden, um den größtmöglichen Nutzen zu erzielen. Der Schwerpunkt dieses Dokuments liegt auf großen Umgebungen von Service Providern, aber viele Empfehlungen gelten auch für andere CNR-Umgebungen. In diesem Dokument wird davon ausgegangen, dass

- Sie sind ein Service Provider, der ein Breitbandnetzwerk mit mindestens 10.000 Teilnehmern betreibt.
- Sie verwenden CNR 5.0.3 oder höher.
- Sie verwenden LDAP (Lightweight Directory Access Protocol). CNR wird ohne LDAP ausgeführt, aber viele Service Provider verwenden LDAP.
- Ihr Netzwerk hat eine mittlere IP-Adressensättigung.
- Sie führen CNR auf UNIX-Servern aus. Die meisten Empfehlungen gelten gleichermaßen für Windows NT, aber die meisten Dienstanbieter führen CNR auf UNIX-Servern aus. Wenn UNIX und NT sich also unterscheiden, wird das UNIX-Beispiel verwendet.
- Sie verfügen über Upstream-Verbindungen zu anderen Systemen (z. B. Rechnungsstellung, Kundenbetreuung oder Bereitstellung), die auf anderen Servern ausgeführt werden.
- Dynamisches Domain Name System (DDNS) ist an Ihrem Standort nicht aktiv (die meisten Service Provider verwenden DDNS nicht).

Empfehlungen für Konfiguration und Einrichtung

Erste Planung und Einrichtung

- Zuweisung von IP-Adressen planen und dokumentieren.
- Separate speicherintensive Operationen: den primären DHCP-Server auf einem anderen Computer als den LDAP-Server und den primären DNS-Server.
- Dokumentieren Sie die CMTS-Konfiguration (Cable Modem Termination System). Stellen Sie sicher, dass die CMTS- und CNR-Konfigurationen übereinstimmen.
- Erstellen Sie Disaster Recovery-Pläne.
- Dokumentieren Sie Ihre Netzwerktopologie.
- Beachten Sie die Cisco IOS® Software-Versionen der CMTSs.

Die effektivsten Schritte für einen langfristigen Netzwerkstatus sind: a) planen Sie Ihre Konfiguration, b) zeichnen Sie diese Pläne auf, und c) zeichnen Sie die Änderungen auf, wenn Änderungen geplant und vorgenommen werden. Die Dokumentation der Gründe für die Auswahl kann bei zukünftigen Planungssitzungen hilfreich sein.

Allgemeine Systemkonfiguration

- Sicheres Failover verwenden Ein einfaches Failover, bei dem ein Server für alle Bereiche die Hauptrolle spielt und der andere Server Backup für alle Bereiche (im Gegensatz zu einem symmetrischen Failover, bei dem beide Server - je nach Umfang - gleichzeitig die Hauptleitung und die Sicherung sind), wird dringend empfohlen, da es *die* Verwaltungsaufgaben *erheblich vereinfacht*.
- Aktivieren Sie SNMP-Traps (Simple Network Management Protocol). Diese Beispiele dienen als Beispiel:

```
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
```

- Stellen Sie sicher, dass Sie über ausreichend RAM (512 MB oder mehr) verfügen.
- Stellen Sie sicher, dass die Datenpartition groß genug ist (2,5 GB oder größer).
- Verwenden Sie separate Partitionen für Protokolle und Daten.
- Sicherstellung von Hochgeschwindigkeitsverbindungen mit niedriger Latenz zwischen Servern Überprüfen der Schnittstelleneinstellungen

SNMP-Traps ermöglichen Ihnen, den DHCP-Server von einem Netzwerkmonitor aus zu überwachen. Konfigurieren Sie die Traps auf dem DHCP-Server, konfigurieren Sie den Monitor so, dass er sie empfängt und anzeigt, und achten Sie auf den Monitor.

Die Konfiguration eines Produktionssystems erfordert Kompromisse zwischen Kosten und Systemeffektivität. Wir schlagen vor, diese Werte unter der Annahme von ca. 100.000 Teilnehmern auf Systemen der E250-Klasse mit Failover zu verwenden. Die Verwendung vieler Richtlinien, Clientklassen, Bereiche, Anforderungs- und Antwortpuffer, DHCP-Erweiterungen und anderer Komplikationen wirkt sich auf Speicheranforderungen und Leistung aus.

Die Protokoll-Partition (/var/nwreg2) sollte erhöht werden, wenn Anzahl und Größe der Protokolle erhöht werden.

DHCP-Konfiguration

- Legen Sie die Anforderungs- und Antwortpuffer für einen optimalen Durchsatz fest. Beachten Sie, dass diese Empfehlungen für CNR 5.0 geändert wurden.

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

- Leasedauer für Kabelmodem = 604800 (7 Tage) oder mehr
- Customer Premises Equipment (CPE)-Leasedauer: so lange wie möglich (siehe Mitteilung zu den Kompromissen).
- Erhöhen Sie die Größe von DHCP- und TFTP-Protokollen:

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

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

- Konfigurieren Sie Protokolleinstellungen, die genügend Details bereitstellen, um Probleme zu identifizieren, jedoch keine übermäßige Detailgenauigkeit generieren (wodurch es schwierig ist, Probleme zu unterscheiden und unnötiges Laden auf dem Server zu verursachen). Dies sind empfohlene Einstellungen, die allgemein gültig sind. Passen Sie ggf. Ihre Einstellungen an, um Probleme in Ihrem Netzwerk zu beheben:AktivitätsübersichtStandardKeine Failover-AktivitätDefer-Lease-Erweiterungen aktivierenFestlegen der Granularität für die letzte Transaktion = *1/2-Leasingintervall*Deaktivieren Sie das allow-client-lease-override für Richtlinien, die Produktions-Leasing anbieten.Möglichkeit der Rückfallsicherung an den lokalen Benutzer; Wenn LDAP nicht verfügbar ist, verwendet CNR lokale Daten:
```
nrcmd> session set visibility=3
nrcmd> dhcp enable fallback-to-local-client-data
nrcmd> session set visibility=5
```

- Wenn Sie CNR 5.5 oder höher verwenden, konfigurieren Sie die Client-Cache-Funktion, um die LDAP-Abfragen um die Hälfte zu reduzieren.
```
nrcmd> dhcp set client-cache-count=2000
nrcmd> dhcp set client-cache-ttl=5
```

Um den Durchsatz von CNR so effektiv wie möglich zu nutzen, sollte es drei- bis viermal so viele Antwortpuffer geben wie Anforderungspuffer. Das System verwendet nur so viele Puffer, wie es benötigt. Je kürzere Leasingzeiten, desto mehr Response-Puffer sind erforderlich.

Hinweis: Leasingzeiten sollten so lange wie möglich erfolgen. Die Leasingraten für Kabelmodems stammen aus einem privaten Adressraum (normalerweise netto-10), und die Modems bewegen sich selten an verschiedenen Stellen im Netz. Diese Leasingverträge sollten eine Woche oder länger abgeschlossen werden. CPE-Leasing hingegen kommt aus dem öffentlichen Adressraum, und CPEs (insbesondere Laptops) bewegen sich um. In diesem Fall muss die Leasedauer so festgelegt werden, dass sie den Gewohnheiten Ihrer Benutzerpopulation entspricht. Längere Leasing-Zeiträume reduzieren die Auslastung des DHCP-Servers. Wenn Sie kurze Leasing-Zeiträume (weniger als 8 Stunden) nutzen, erhöhen Sie die Response-Puffer auf 2500.

Deaktivieren Sie allow-client-lease-override, um sicherzustellen, dass die Clients die in Ihrer CNR-Konfiguration angegebenen Leasedauer einhalten - einige Clients versuchen, die angegebene Einstellung zu überschreiben.

Aktivieren Sie die Option "fallback-to-local", um den Betrieb Ihres Netzwerks im Falle eines LDAP-Serverausfalls aufrechtzuerhalten. Bei dieser Einstellung erfüllt der DHCP-Server weiterhin Leasinganforderungen, obwohl der LDAP-Server nicht antwortet. Der Server hat keinen Zugriff auf die spezifischen Client-Informationen, die auf dem LDAP-Server gespeichert sind. Daher erfüllt er jede Anforderung mit einer Standardeinstellung. Sie müssen einen Standard konfigurieren, der für Ihr Netzwerk angemessen ist.

Schließlich behält die Client-Cache-Funktion die vom LDAP abgerufenen Client-Daten im Arbeitsspeicher, sodass der DHCP-Server LDAP nur einmal während des Discovery-Offer-Request-Back-Zyklus abfragen muss, wodurch die Leistung des DHCP-Servers beschleunigt wird.

DNS-Konfiguration

1. Aktivieren Sie die Funktion für die inkrementelle Übertragung:

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

2. Benachrichtigung aktivieren. Informationen zu den Argumenten, die Sie für die Benachrichtigung aktivieren müssen, finden Sie unter CNR CLI-Befehlsreferenzen.
3. Platzieren Sie primäre und sekundäre DNS-Server in separaten Netzwerksegmenten.
4. Konfigurieren von Clients zum Abfragen eines sekundären DNS-Servers

Sekundäre DNS-Server erhalten ihre Daten auf zwei Arten vom primären Server: a) "Vollzonenübertragung" oder b) "Benachrichtigung/ixfr" (inkrementelle Übertragung). Durch die Verwendung von notify/ixfr wird die Anzahl der Datensätze reduziert, die vom primären auf die sekundären Server übertragen werden müssen. Dies ist besonders wichtig, wenn der Name Leerzeichen relativ dynamisch ist.

TFTP-Konfiguration

- Legen Sie **das Timeout für das Startpaket** auf 2 fest:
  ```
  nrcmd> tftp set initial-packet-timeout = 2
  ```

- Wenn Sie CNR 5.5 oder höher verwenden, aktivieren Sie TFTP-Datei-Caching, um die Leistung zu verbessern:
  ```
  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
  ```

Beim Caching der TFTP-Datei werden die Konfigurationsdateien für das Kabelmodem im Speicher gespeichert. So wird vermieden, dass sie bei jedem Anfordern einer Konfigurationsdatei auf der Festplatte gelesen werden. Auf der Festplatte muss ein Dateicache-Verzeichnis erstellt werden (im obigen Beispiel CacheDir), und es muss eine maximale Größe zugewiesen werden. Wählen Sie die Größe unter Berücksichtigung der gesamten RAM in Ihrem System und der Anzahl der benötigten Konfigurationsdateien aus.

Beim TFTP-Protokoll muss der Client beim Empfang einer Datei kein ACK-Paket (Final Bestätigungs) senden. Wenn kein ACK empfangen wird, muss der Server die Client-Verbindung für den Timeout-Zeitraum halten, wodurch seine Kapazität zur Bearbeitung neuer Anfragen eingeschränkt wird. Wenn Ihr TFTP-Server über die erforderliche Ressourcenkapazität verfügt, können Sie auch den Wert von **max-tftp-Paketen** erhöhen, um eine größere Anzahl von Clientverbindungen zu unterstützen. Der Standardwert für diesen Parameter ist 512. Der Maximalwert ist 1000.

CNR-LDAP-Konfiguration

Diese Einstellungen zeigen eine Konfiguration an, in der CNR Lease-Updates für LDAP schreibt. Wenn möglich, sollten Sie Ihr Netzwerk so gestalten, dass dies nicht erforderlich ist. Es wird hier gezeigt, um Empfehlungen zu geben, wenn Sie Lease-Updates schreiben müssen. Optimieren Sie LDAP-Verbindungen, indem Sie LDAP-Objekte, die getrennt einstellbar sind, für Lese-/SCHREIBEN verwenden. (Jedes Objekt erhält seine eigene Threadgruppe).

```
# 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
```

Die angezeigte Konfiguration beinhaltet CNR-Lease-Updates für LDAP. Sie können dies tun, damit Anwendungen LDAP für aktuelle Leasinginformationen abfragen können. Sie sollten jedoch versuchen, eine Strukturierung der Anwendung zu vermeiden, damit dies erforderlich ist. Wenn Sie Informationen über den Leasingstatus einer IP-Adresse bereitstellen müssen, können Sie den Befehl NRCMD Lease verwenden, um die MAC-Adresse, das Ablaufdatum und andere Informationen über den aktuellen Leasingstatus abzurufen.

LDAP-Verzeichnisse sind so konzipiert, dass sie schnell und effizient gelesen werden können. Das Schreiben in ein LDAP-Verzeichnis ist jedoch ineffizient. Wenn Sie CNR so konfigurieren, dass Leasing-Informationen in LDAP geschrieben werden, wird LDAP zu einem Engpass der allgemeinen Systemleistung. Wenn Sie LDAP Lease Writes konfigurieren müssen, verwenden Sie die empfohlenen Einstellungen. Beachten Sie, dass der CNR-Zugriff auf LDAP mithilfe separater "Read"- und "Update LDAP"-Objekte optimiert wurde. Beachten Sie auch das Schreibtimeout für 30 Sekunden. Bei einer kürzeren Zeitüberschreitung besteht das Risiko, dass das LDAP-Timing bei starker LDAP-Last ausgeführt wird. Dann versucht CNR den Schreibvorgang neu, wodurch LDAP zusätzliche Last hinzugefügt wird.

Die Gesamtzahl der Verbindungen zum LDAP-Server darf die maximale Anzahl der verfügbaren Threads nicht überschreiten. Wenn der LDAP-Server mehrere Threads pro Verbindung unterstützt, ist die optimale Anzahl der Verbindungen die Gesamtzahl der Threads dividiert durch die Anzahl der Threads pro Verbindung.

LDAP-Server-Optimierungsparameter

- Erstellen von Indizes für Suchfelder.
- Konfigurieren Sie die Cache-Größe, um die Anzahl der im Arbeitsspeicher zwischengespeicherten Einträge zu erhöhen. Der Cache sollte jedoch ein Drittel des verfügbaren Arbeitsspeichers nicht überschreiten.
- Konfigurieren Sie maximale Threads, um die Anzahl der unterstützten gleichzeitigen Verbindungen zu erhöhen. Dies sollte jedoch nicht mehr als die Hälfte der verfügbaren Ressourcen betragen.
- Konfigurieren Sie Protokolleinstellungen, die genügend Details bereitstellen, um Probleme zu identifizieren, jedoch keine übermäßige Detailgenauigkeit generieren (wodurch es schwierig ist, Probleme zu unterscheiden und unnötiges Laden auf dem Server zu verursachen).
- Verwenden Sie separate Partitionen für Protokolle und Daten.

Bestimmte LDAP-Serverimplementierungen variieren. Informationen zur Umsetzung dieser Vorschläge finden Sie in der Serverdokumentation.

Routineverfahren

- Sichern Sie regelmäßig die CNR-Datenbanken. Anweisungen hierzu finden Sie in den Benutzerhandbüchern. Sie sollten die CNR-Datenbanken mindestens einmal täglich sichern. Speichern Sie die Sicherungsdateien mindestens zwei Wochen lang.
- Regelmäßiges Sichern von LDAP.
- Regelmäßige Sicherung und Archivierung von Protokollen
- Nachdem an CNR Änderungen vorgenommen wurden, stellen Sie sicher, dass die Konfiguration der Haupt- und Backup-Server in einem Failover-Szenario konsistent bleibt. Verwenden Sie das Tool **cnrFailoverConfig-Comparison** in CNR 5.5 und früher, oder vergleichen Sie die Konfigurationen mithilfe der WebUI in CNR 6.0 und höher.
- Wenn Änderungen an der Netzwerktopologie geplant sind, legen Sie die DHCP-Erneuerungs- und Leasedauer auf kleine Werte fest.
- Überwachen der IP-Adressverwendung (SNMP-Traps verwenden)
- Überwachung der Systemauslastung (Arbeitsspeicher, Festplatte, CPU und Austausch). Das Dienstprogramm **oben** ist für diesen Zweck nützlich.
- Überprüfen Sie die Protokolle regelmäßig, um sich mit den Normalfällen vertraut zu machen. Durch das Verständnis normaler Protokolle können Probleme schneller behoben werden.
- Regelmäßige Überprüfung von Protokollen auf Ausnahmen: grep für "error", "warn" oder "connect" (in UNIX verwenden Sie beispielsweise **grep -i warn name_dhcp_1_log**).

DHCP Safe-Failover erfordert, dass die Konfigurationseinstellungen für einen Bereich auf dem primären und dem Backup-Server für diesen Bereich identisch sind. Stellen Sie sicher, dass Sie beim Ändern einer Einstellung die Änderung auf beiden Servern vornehmen. Verwenden Sie regelmäßig **cnrFailoverConfig-Vergleich** oder WebUI in CNR 6.0 und höher, um sicherzustellen, dass keine Unterschiede bestehen.

Änderungen an der Netzwerktopologie oder Änderungen bei der IP-Adresszuweisung können es für Clients erforderlich machen, eine andere Adresse zu erhalten. Sie müssen einen Zeitraum planen, in dem einige Clients in einem Subnetz eine Adresse aus dem alten Bereich haben, andere jedoch eine neue Adresse erhalten haben. Sie können die Zeitdauer, während der beide Adresssätze aktiv sind, verkürzen, indem Sie die Leasingdauer vor der Änderung verkürzen, sodass alle Kunden über Leasing mit kurzer Laufzeit verfügen. Dadurch wird sichergestellt, dass sie ihre Leasing-Verträge regelmäßig erneuern müssen und daher unmittelbar nach der Änderung ein Leasing aus dem neuen Angebot abholen können. Stellen Sie sicher, dass die Leasedauer

nicht so kurz ist, dass Leasingverträge auslaufen, während Sie anhalten und den Server starten, um die Änderung vorzunehmen. Nachdem Sie die Änderung vorgenommen haben, stellen Sie sicher, dass Sie den ursprünglichen Leasing-Zeitraum wiederherstellen, damit Sie die Last auf dem Server nicht erhöhen.

Der effektivste Ansatz zur Lösung von Problemen besteht darin, diese zu vermeiden. Die Befolgung der oben genannten Empfehlungen hält Ihre Administratoren stets auf dem Laufenden und hilft Ihnen, ernsthafte Probleme zu vermeiden. Wenn Probleme auftreten (z. B. eine Verlängerung der E/A-Wartezeit oder eine Erhöhung der Speichernutzung ohne bekannten Grund), führen Sie eine weitere Protokollierung durch. Überprüfen Sie die jüngsten Änderungen an Ihrer physischen Umgebung oder an der CNR-Konfiguration, um festzustellen, ob dies die Ursache für die Probleme sein könnte.

Die CNR-Protokolle sind Ihre Freunde. Wenn Sie CNR verwenden, CNR aktualisieren oder die CNR-Konfiguration ändern möchten, verwenden Sie den beschriebenen Befehl **grep**, um die Protokolle auf Probleme zu überprüfen. Arbeiten Sie dann im Protokoll rückwärts, um zu verstehen, wann und wie das Problem auftrat, und beheben Sie das Problem.

Sofortige Maßnahmen bei Problemen

- *Starten **Sie** CMTS **nur** dann neu*, wenn dies vom Support-Team von Cisco angefordert wurde (gilt nur für Kabelumgebungen).
- *Starten **Sie** CNR **nur** neu*, wenn Sie vom Cisco Support-Team dazu aufgefordert werden.
- *Deaktivieren **Sie kein** sicheres Failover, es sei denn, Sie werden von den Support-Mitarbeitern von Cisco dazu aufgefordert.*
- ***Laden Sie** CNR **nicht** neu, starten Sie ihn neu oder unterbrechen Sie ihn, wenn eine sichere Failover-Resynchronisierung ausgeführt wird.*
- ***Kopieren Sie** die Protokolldateien in ein Verzeichnis, in das sie nicht überschrieben werden. Wenn CNR abstürzt, kopieren Sie die Core-Datei in ein Verzeichnis, in dem sie nicht überschrieben wird.*
- ***Nicht** anwenden:*
  ```
  nrcmd> server dhcp getRelatedServers
  ```
  um eine sichere Failover-Fehlkonfiguration zu isolieren.
- ***Sehen Sie sich** die Protokolle auf Ausnahmen an. Überprüfen Sie insbesondere die Startsequenz (dies kann in einem alten Protokoll sein): grep für "error", "warn" oder "connect" (z.B. **grep -i error name_dhcp_1_log***).

Wenn Sie ein Problem haben, ist es wichtig, dass Sie bei der Isolierung und Behebung des ursprünglichen Problems keinen weiteren Schaden anrichten. Ein Neustart eines CMTS oder ein Neustart von CNR führt zu sofortigen Auslastungsspitzen während einer Zeit, in der das System bereits instabil ist. Ziel ist es, Ihr System innerhalb kürzester Zeit wieder voll funktionsfähig zu machen. Die verstrichene Zeit, bis Ihre letzte Aktion zählt. die Zeit bis zur ersten Aktion zählt nicht. Mit anderen Worten: Lassen Sie nicht schnell handeln, nur um schnell zu handeln. Denken Sie, bevor Sie handeln.

Starten Sie ein Protokoll aller durchgeführten Schritte und aller Änderungen, die an einem beliebigen Ort im System vorgenommen wurden: DHCP-, DNS- oder TFTP-Server sowie Änderungen an CMTS- oder Kabelmodem. Beschreiben Sie das Problem, und protokollieren Sie detailliert nur das beobachtbare Verhalten.

Protokolldateien analysieren

Erfassen Sie die Protokolle (/var/nwreg2/logs). Analysieren Sie diese, und suchen Sie nach Fehlern oder Warnungen. Verwenden Sie einen Texteditor, um Fehler von Interesse weiter zu analysieren. Suchen Sie nach allen Einträgen, die sich auf die MAC-Adresse, die IP-Adresse oder den Domänennamen beziehen, die dem Fehler zugeordnet sind, ab dem Fehler im Protokoll.

Möglicherweise müssen Sie die zusätzliche Protokollierung aktivieren, um DHCP-Probleme zu diagnostizieren. Der DHCP-Server unterstützt eine breite Palette von Protokollierungsfunktionen. Eine Liste der Protokollierungsoptionen und eine Erläuterung dazu finden Sie unter CNR CLI-Befehlsreferenzen. Seien Sie vorsichtig, da jede Protokollmeldung die Last auf den Server legt. Sie müssen einen Kompromiss zwischen der Menge an Informationen, die Sie bei CNR für die Protokollierung und die Serverleistung fragen, eingehen.

Auf LDAP-Probleme prüfen

Das Problem kann beim LDAP-Server auftreten. CNR erstellt eine Warteschlange mit Anforderungen an den LDAP-Server. Wenn der LDAP-Server mit der Last nicht mithalten kann, wird die Warteschlange erstellt. Suchen Sie im Verzeichnis /var/nwreg2/data/dhcpeventstore. Die Größe der Ereignisspeicherdateien ist festgelegt. Wenn die Warteschlange also aufgebaut ist, erstellt CNR weitere Dateien. Wenn mehr als eine Datei im Verzeichnis vorhanden ist, weist dies darauf hin, dass die Warteschlange eine Sicherung durchführt. Dieselbe Warteschlange wird für die Warteschlange von Anfragen an den DNS-Server verwendet. Wenn also die Warteschlange gesichert wird und Sie DDNS verwenden, können Anfragen an den DNS-Server gesendet werden. Um zu bestimmen, ob das Problem mit LDAP auftritt, aktivieren Sie die zusätzliche CNR-LDAP-Schnittstellenprotokollierung. Aktivieren Sie die Protokollflags **ldap-create-detail**, **ldap-query-detail** und **ldap-update-detail**. Die Protokollmeldung enthält Zeitstempel, mit denen Sie ermitteln können, ob LDAP der Systemengpass ist.

Überprüfen der internen CNR-Datenbanken

Wenn Sie vermuten, dass eine oder mehrere interne Datenbanken von CNR die Integrität verloren haben, lesen Sie die CNR-Benutzerhandbücher, um zu erfahren, wie Sie die Dienstprogramme zur Überprüfung der Datenbankvalidierung ausführen. Wenn eines dieser Dienstprogramme auf ein Problem hinweist, befolgen Sie die Anweisungen in den Benutzerhandbüchern, um dieses Problem zu beheben.

Überprüfen von DNS-Daten mit nslookup

Das Dienstprogramm **nslookup** ist sowohl in UNIX-Systemen als auch in Windows NT enthalten. Sie kann zum Abfragen eines DNS-Servers verwendet werden und ist daher hilfreich bei der Überprüfung der vom Server gespeicherten Daten. Die Dokumentation für Ihr Betriebssystem enthält detaillierte Informationen zu den Funktionen.

Zugehörige Informationen

- Cisco CNS Network Registrar Tech Notes
- Technischer Support - Cisco Systems