Aanbevolen CNR-instellingen en -beheer

Inhoud

Inleiding

Dit artikel heeft twee doelen. Eerst bevat het aanbevelingen over hoe u de Cisco Network Registrar (CNR) kunt configureren voor optimale prestaties en stabiliteit en hoe u uw CNR-installatie kunt bewaken. Ten tweede bevat het aanbevelingen over hoe u moet reageren als er een probleem optreedt. In het ideale geval zal u dit artikel lezen en reageren op de configuratie en controle aanbevelingen voordat er problemen optreden. Door dit te doen, zult u problemen vermijden. Als u dit artikel voor het eerst leest omdat u een probleem hebt met CNR, ga dan onmiddellijk naar de afdeling Onmiddellijke handelingen wanneer u een probleem tegenkomt. Raadpleeg voor meer informatie over de aanbevelingen de CNR-gebruikershandleidingen en opdrachtreferenties.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Standaard configuratie

De configuratie aanbevelingen die hier worden aangeboden vormen een uitgangspunt. Als uw systeem anders is geconfigureerd dan dit, herzie uw instellingen. Uw configuratie kan zijn gebaseerd op eerdere versies van CNR. CNR 5.0 en latere versies bieden veel verbeterde prestaties in vergelijking met eerdere versies, maar parameterveranderingen moeten worden aangebracht om het maximale voordeel te bereiken. Dit document is gericht op grote serviceprovider-omgevingen, maar veel van de aanbevelingen zijn ook van toepassing op andere CNR-omgevingen. In dit document wordt ervan uitgegaan dat:

- U bent een serviceprovider die een breedbandnetwerk runt met 10.000 abonnees of meer.
- U gebruikt CNR 5.0.3 of hoger.
- U gebruikt Lichtgewicht Directory Access Protocol (LDAP). CNR werkt zonder LDAP, maar veel dienstverleners gebruiken LDAP.
- Uw netwerk heeft een gemiddelde IP adresverzadiging.
- U voert CNR uit op UNIX-servers. De meeste aanbevelingen zijn ook van toepassing op Windows NT, maar de meeste serviceproviders draaien CNR op UNIX-servers, dus waar UNIX en NT verschillen, wordt het UNIX-voorbeeld gebruikt.
- U hebt stroomopwaartse verbindingen met andere systemen (zoals facturering, klantenservice of provisioning) die op andere servers worden uitgevoerd.
- Dynamic Domain Name System (DDNS) is niet actief op uw site (de meeste serviceproviders gebruiken DDNS).

Aanbevelingen voor configuratie en installatie

Eerste planning en installatie

- Toewijzing van plan en documentinvoer en toewijzing van IP-adressen.
- Schijfintenintensieve bewerkingen: Zet uw primaire DHCP-server op een andere machine dan uw LDAP server en primaire DNS server.
- Document uw CMTS-configuratie (Cable Modem Termination System); Zorg ervoor dat de CMTS- en CNR-configuraties overeenkomen.
- Maak rampenherstelplannen op.
- Document uw netwerktopologie.
- Let op de Cisco IOS®-softwareversies van CMTS's.

De meest effectieve stappen naar een gezondheid op lange termijn van uw netwerk zijn: a) plan

uw configuratie , b) registreer die plannen en c) registreer de veranderingen wanneer veranderingen worden gepland en gemaakt . Het documenteren van de redenen voor keuzes kan tijdens toekomstige planningssessies helpen.

Algemene systeemconfiguratie

- Gebruik veilige failover. Eenvoudige failover, waarbij één server is hoofd voor alle scopen, en de andere server back-up is voor alle scopen (in plaats van symmetrische failover, waarbij beide servers tegelijkertijd hoofdondersteuning en back-up hebben, afhankelijk van het individuele bereik), wordt ten zeerste aanbevolen, omdat deze beheertaken *aanzienlijk vereenvoudigt*.
- Zet Simple Network Management Protocol (SNMP)-traps aan. Deze voorbeelden zijn ter illustratie:

```
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
```

- Zorg ervoor dat u voldoende RAM (512 MB of meer) hebt.
- Zorg ervoor dat de gegevensdeling groot genoeg is (2,5 GB of groter).
- Gebruik afzonderlijke partities voor logbestanden en gegevens.
- zorgen voor snelle, laaglatente verbindingen tussen servers; controleer de interface-instellingen.

SNMP-traps stellen u in staat om de DHCP-server vanaf een netwerkmonitor te controleren. Vergeet niet de vallen op de DHCP-server te configureren, de monitor te configureren om ze te ontvangen en weer te geven, en uiteraard aandacht te besteden aan de monitor.

Voor het configureren van een productiesysteem zijn kostenbatten nodig in vergelijking met de effectiviteit van het systeem. We stellen deze waarden voor als we uitgaan van ongeveer 100.000 abonnees op E250-klasse systemen die overvallen. Het gebruik van veel beleid, client-klassen, bereik, verzoek- en responsbuffers, DHCP-uitbreidingen en andere complicaties beïnvloedt de geheugenbehoeften en de prestaties.

De logverdeling (/var/nwreg2) moet worden verhoogd als het aantal en de grootte van stammen wordt verhoogd.

DHCP-configuratie

- Stel de aanvraag- en responsbuffers in voor een optimale doorvoersnelheid. Deze aanbevelingen zijn gewijzigd voor CNR 5.0.

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

- De huurtijd van de kabelmodems is = 604800 (7 dagen) of meer.
- CPE-leasetijd (Customer Premises Equipment) zo lang mogelijk (zie nota voor "trade-offs").
- Vergroot de bestandsgrootte van DHCP en TFTP:

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

- Configureer loginstellingen die voldoende details geven om problemen te identificeren, maar geen excessieve details genereren (wat het moeilijk maakt om problemen te onderscheiden en onnodige belasting op de server plaatst). Dit zijn aanbevolen instellingen die algemeen toepasbaar zijn. Pas de instellingen indien nodig aan om problemen in uw netwerk aan te pakken:Samenvatting van de activiteitStandaardGeen failover-activiteitUitgestelde-leaseextensies inschakelenStel het laatste-transactie-tijd-granulariteit in = *1/2 lease*intervalSchakel z.g.g.-leaseoping uit voor beleid dat productieleases aanbiedt.terugval naar de lokale omgeving mogelijk maken; wanneer LDAP niet beschikbaar is, gebruikt CNR lokale gegevens:
  ```
  nrcmd> session set visibility=3
  nrcmd> dhcp enable fallback-to-local-client-data
  nrcmd> session set visibility=5
  ```

- Indien CNR 5.5 of later wordt gebruikt, moet u de client-cache configureren om de LDAP-vragen met de helft te verminderen.
  ```
  nrcmd> dhcp set client-cache-count=2000
  nrcmd> dhcp set client-cache-ttl=5
  ```

Om de doorvoercapaciteit van CNR optimaal te benutten, moeten er drie tot vier keer zoveel buffers zijn als gevraagde buffers. Het systeem gebruikt alleen zoveel buffers als het nodig heeft. Naarmate de leasetijden korter worden, zijn er meer buffers nodig.

Opmerking: De leasetijden moeten zo lang worden gemaakt als praktisch mogelijk is. De huurders van de kabelmodems komen van een privé adresruimte (gewoonlijk net-10), en de modems bewegen zich zelden rond aan verschillende plaatsen op het net. Deze leaseovereenkomsten moeten een week of langer worden gesloten. CPE-leases daarentegen komen uit de publieke adresruimte en CPE's (met name laptops) bewegen zich wel. Hier moet de leasetijd worden ingesteld om de gewoontes van uw gebruikerspopulatie te evenaren. Langere leases verminderen de lading op de DHCP-server. Wanneer u korte leases gebruikt (minder dan 8 uur), verhoog u de buffers voor respons op 2500.

Schakel de lease-override uit om ervoor te zorgen dat klanten de leasetijden in acht nemen die in uw CNR-configuratie zijn gespecificeerd. Sommige klanten proberen de gespecificeerde instelling te omzeilen.

Schakel de terugval-naar-locaal in om uw netwerk actief te houden in het geval van een LDAP server-storing. Met deze instelling blijft de DHCP-server voldoen aan leaseaanvragen, ook al reageert de LDAP-server niet. De server heeft geen toegang tot de specifieke client informatie die opgeslagen wordt op de LDAP server, dus zal elk verzoek voldoen aan een standaardinstelling. U moet een standaard configureren die redelijk is voor uw netwerk.

Ten slotte houdt de client-cache optie in het geheugen van de clientgegevens die van LDAP zijn opgehaald, zodat de DHCP-server LDAP slechts eenmaal hoeft te vragen tijdens de discovery-offer-request-ack cyclus, waardoor de DHCP-serverprestaties worden versneld.

DNS-configuratie

1. Schakel de optie incrementele overdracht in:
   ```
   nrcmd> dns enable ixfr-enable
   ```

2. Inschakelen voor kennisgeving Raadpleeg de cnr CLI Opdrachtreferenties voor de argumenten die u moet opgeven.
3. Plaats primaire en secundaire DNS servers op afzonderlijke netwerksegmenten.
4. Configureer klanten om een secundaire DNS-server te vragen.

Secundaire DNS-servers ontvangen hun gegevens op een van de twee manieren van de primaire server: a) "volledige overdracht van zone" of b) "kennisgeving/ixfr" (incrementele overdracht). Met de aanmelding/ixfr wordt het aantal records verminderd dat van de primaire naar de secundaire servers moet worden overgedragen. Dit is van cruciaal belang wanneer de naamruimte relatief dynamisch is.

TFTP-configuratie

- Stel **de begintijd in** op 2:
  ```
  nrcmd> tftp set initial-packet-timeout = 2
  ```

- Als u CNR 5.5 of hoger gebruikt, schakelt u TFTP-bestandsindeling in om de prestaties te verbeteren:
  ```
  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-bestandsopberging houdt de kabelmodemconfiguratiebestanden in het geheugen opgeslagen en vermijdt leest aan schijf telkens wanneer een kabelmodembestand om een configuratiebestand vraagt. Er moet een bestands cache-map worden aangemaakt in de harde schijf (CacheDir in het bovenstaande voorbeeld) en er moet een maximale grootte worden toegewezen. Kies de grootte rekening houdend met het totale aantal RAM in uw systeem en het aantal verschillende configuratiebestanden dat nodig is.

Het TFTP-protocol vereist niet dat de client na ontvangst van een bestand een laatste ontvangstbevestiging (ACK) pakje verstuurt. Als geen ACK wordt ontvangen, moet de server de client verbinding bewaren voor de tijdelijke periode, die zijn capaciteit beperkt om nieuwe verzoeken te bedienen. Als uw TFTP-server over de resource capaciteit beschikt, kunt u ook de waarde van **max-tftp-pakketten** verhogen om een groter aantal client-verbindingen te ondersteunen. De standaardwaarde voor deze parameter is 512. De maximale waarde is 1000.

Configuratie CNR LDAP

Deze instellingen tonen een configuratie waar CNR leaseupdates aan LDAP schrijft. Indien mogelijk, ontwerp uw netwerk zodat dit niet nodig is. Hier wordt getoond om aanbevelingen te verstrekken als u huurupdates moet schrijven. Optimaliseer LDAP-verbindingen door afzonderlijk afstelbare LEES-/SCHRIJFSDP-objecten te gebruiken. (Elk object krijgt een eigen groep draden).

```
# 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
```

De configuratie die wordt getoond, omvat de aanwezigheid van CNR-afschrijvingsupdates aan LDAP. U kunt dit doen om het voor toepassingen mogelijk te maken om LDAP te vragen voor actuele leaseinformatie, maar u moet proberen te voorkomen dat uw toepassing zo wordt gestructureerd dat dit nodig is. Als u informatie beschikbaar moet maken over de staat van de lease voor een IP-adres, kunt u de NRCMD-huuropdracht gebruiken om het MAC-adres, de verloopdatum en andere informatie over de huidige status van de lease te verkrijgen.

De LGO-gidsen zijn ontworpen om snel en efficiënt te kunnen lezen, maar schrijven naar een LDAP-directory is niet efficiënt. Als u CNR aanpast om leaseinformatie aan LDAP te schrijven, wordt LDAP een knelpunt voor de algehele systeemprestaties. Als u LDAP lease-documenten moet configureren gebruikt u de aanbevolen instellingen. Merk op dat CNR-toegang tot LDAP is geoptimaliseerd door gebruik te maken van afzonderlijke "lees"- en "update LDAP"-objecten. Opmerking: ook de 30 seconden durende afschrijvingsperiode. Met een kortere tijdslimiet loopt u het risico dat LDAP de timing uitschrijft wanneer LDAP zwaar belast is. CNR probeert de schrijfmachine opnieuw in te voeren, wat een extra lading aan LDAP toevoegt.

Het totale aantal verbindingen op uw LDAP-server mag niet groter zijn dan het maximale aantal beschikbare draden. Als uw LDAP server meerdere draden per verbinding ondersteunt, is het optimale aantal verbindingen het totale aantal draden gedeeld door het aantal draden per verbinding.

Instellingen LDAP-server

- indexen maken voor lookup-velden.
- Configureer cachegrootte om het aantal items dat in het geheugen is opgeslagen te verhogen, hoewel de cache niet groter moet zijn dan een derde van het beschikbare geheugen.

- Configureer maximale draden om het aantal gelijktijdige verbindingen te verhogen dat kan worden ondersteund, hoewel dit niet meer dan de helft van de beschikbare bronnen mag bedragen.
- Configureer loginstellingen die voldoende details geven om problemen te identificeren maar geen excessieve details genereren (wat het moeilijk maakt om problemen te onderscheiden en onnodige belasting op de server plaatst).
- Gebruik afzonderlijke partities voor logbestanden en gegevens.

De specifieke LAN server implementaties variëren. Raadpleeg uw serverdocumentatie om deze suggesties te implementeren.

Routinemethoden

- Maak regelmatig een back-up van de CNR-databases. Raadpleeg de gebruikershandleidingen voor meer informatie. U dient ten minste eenmaal per dag een back-up te maken van de CNR-databases. Bewaar de back-upbestanden gedurende ten minste twee weken.
- Doe regelmatig een back-up van LDAP.
- Maak regelmatig back-ups en archiveblogs.
- Zorg er na wijzigingen in CNR voor dat de configuratie van de hoofd- en reserveservers in een failoverscenario consistent blijft. Gebruik het **cnrFailoverConfig -** vergelijk het gereedschap in CNR-versies 5.5 en eerder, of vergelijk de configuraties met WebUI in CNR 6.0 en hoger.
- Wanneer de veranderingen van de netwerktopologie gepland zijn, plaats DHCP vernieuwde en huurde tijden aan kleine waarden.
- Controleer IP-adresgebruik (gebruik SNMP-trap).
- Systeemgebruik bewaken (geheugen, schijf, CPU en swap). De nutsvoorziening **top** is nuttig voor dit doel.
- Regelmatig opnieuw bekijken wordt geregistreerd om vertrouwd te raken met de normale gevallen. Door de normale logbestanden te begrijpen, kunt u problemen sneller oplossen.
- Regelmatig opnieuw bekeken logbestanden voor uitzonderingen: grep voor "error", "waarschuwing" of "connect" (bijvoorbeeld in UNIX, gebruik **grep -i om name_dhcp_1_log te waarschuwen**).

DHCP Safe-failover vereist dat de configuratie instellingen voor een bereik identiek zijn op de primaire en reserveserver voor dat bereik. Zorg ervoor, wanneer u een instelling verandert, dat u de verandering op beide servers aanbrengt. Gebruik **CnrFailoverConfig -vergelijk** of WebeiUI in CNR 6.0 en hoger om te controleren of er geen verschillen zijn.

Veranderingen in netwerktopologieën of IP-adrestoewijzing kunnen het voor klanten noodzakelijk maken om een ander adres te krijgen. U moet een periode plannen wanneer sommige cliënten op een netwerk een adres van de oude bereik hebben en sommigen een adres van de nieuwe bereik vernieuwd en gekregen hebben. U kunt de hoeveelheid tijd verminderen gedurende welke beide reeksen adressen actief zijn door de lengte van huurcontracten te verminderen alvorens u de verandering maakt zodat alle cliënten huurcontracten van korte duur hebben. Dit zorgt ervoor dat ze hun leaseovereenkomsten regelmatig moeten verlengen en daarom een leaseovereenkomst uit de nieuwe range moeten halen kort nadat u de verandering hebt doorgevoerd. Stel de leasetijd niet zo kort in, dat de leaseovereenkomsten verlopen terwijl u stopt en de server start om de wijziging aan te brengen. Nadat u de wijziging hebt aangebracht, kunt u de oorspronkelijke leaseperiode herstellen zodat u de lading niet op de server verhoogt.

De meest effectieve benadering van het oplossen van problemen is het vermijden ervan. Volgens

de hierboven uiteengezette aanbevelingen houdt uw beheerders zich bij uw werking aan en stelt u in staat ernstige problemen te voorkomen. Als er problemen verschijnen (zoals een verlenging van de I/O-wachttijd of een toename van het geheugengebruik om een ongekende reden), neem dan contact op met de logbestanden. Bekijk recente wijzigingen in uw fysieke omgeving of configuratie van CNR om te zien of dat de bron van de problemen zou kunnen zijn.

De CNR-blogs zijn je vrienden. Wanneer u CNR start, CNR opwaardering of de configuratie van de CNR wijzigt, gebruikt u de beschreven **grep**-opdracht om de logbestanden op problemen te controleren. Werk dan terug in het logboek om te begrijpen wanneer en hoe de kwestie ontstond, en los het probleem op.

Onmiddellijke acties bij problemen

- Herstart CMTS ***niet*** tenzij verzocht door Cisco-ondersteuningspersoneel (is alleen van toepassing op kabelomgevingen).
- ***Start CNR niet opnieuw***, tenzij dit door het Cisco-ondersteuningspersoneel wordt gevraagd.
- *Schakel* ***geen*** veilige failover uit tenzij u dit door Cisco-ondersteuningspersoneel hebt gevraagd.
- *Herladen, opnieuw opstarten of verstoren CNR* ***niet*** *op enige manier* met een veilige failover-resynchronisatie in uitvoering.
- ***Kopieer*** de logbestanden naar een map waarin ze niet overschreven zullen worden. Als CNR is opgeslagen, kopieert u het kernbestand naar een map waarin het niet wordt overschreven.
- Gebruik:
  ```
  nrcmd> server dhcp getRelatedServers
  ```

  om veilige failover-configuratie te isoleren.
- Bekijk de blogs voor uitzonderingen. Controleer in het bijzonder de startvolgorde (dit kan in een oud logbestand voorkomen): grep voor "error", "waarschuwing" of "connect" (bijvoorbeeld **grip -i error name_dhcp_1_log***).

Wanneer u een probleem tegenkomt, is het van cruciaal belang dat u geen verdere schade veroorzaakt, terwijl u het aanvankelijke probleem isoleert en repareert. Wanneer u een CMTS opnieuw start of wanneer CNR opnieuw wordt opgestart, worden er direct belastingspieken gecreëerd terwijl het systeem al fragiel is. Het doel is dat uw systeem in de kortste tijd weer volledig functioneert. De tijd die is verstreken tot uw laatste handeling telt; de tijd tot uw eerste actie telt niet . Met andere woorden, niet snel handelen alleen om snel te kunnen optreden. Denk voordat je iets doet.

Start een logbestand met alle stappen die u hebt ondernomen en alle wijzigingen die u ergens in het systeem hebt aangebracht: DHCP-, DNS- of TFTP-servers en wijzigingen aangebracht in een CMTS- of kabelmodem. Beschrijf het probleem en log, in detail, enkel het waarneembare gedrag.

Logbestanden analyseren

Verzamel de stammen (/var/nwreg2/boomstammen). Analyseer deze, op zoek naar fouten of waarschuwingen. Gebruik een teksteditor om belangfouten verder te analyseren. Om te beginnen met de fout, zoek terug in het logbestand voor alle items die betrekking hebben op het MAC-adres, IP-adres of domeinnaam die aan de fout is gekoppeld.

Het kan nodig zijn om extra loggen aan te zetten om DHCP-problemen te diagnosticeren. De DHCP-server ondersteunt een uitgebreid scala aan houtkapmogelijkheden. Raadpleeg de

referenties van de CNR CLI-opdracht voor een lijst met houtkapopties en een verklaring voor elke opdracht. Wees voorzichtig, want elk logbericht plaatst de lading op de server. U moet een uitruil maken tussen de hoeveelheid informatie die u CNR vraagt om de prestaties van de logger en de server te registreren.

Raadpleeg voor LDAP-problemen

Het probleem kan zijn met de LDAP server. CNR stelt een reeks verzoeken aan de LDAP server op. Als de LDAP-server niet de lading kan bijhouden, wordt de wachtrij uitgebreid. Kijk in de /var/nwreg2/data/dhcpeventstore folder. Event Store-bestanden zijn van een bepaalde grootte gemaakt, dus als de wachtrij wordt aangelegd, creëert CNR meer bestanden. Als er meer dan één bestand in de map staat, duidt dit erop dat de wachtrij een back-up maakt. Dezelfde wachtrij wordt gebruikt om verzoeken aan de DNS-server in een wachtrij te plaatsen, zodat als de wachtrij een back-up maakt en u DDNS gebruikt, het bestand kan worden ingevuld met verzoeken aan de DNS-server. Om te bepalen of het probleem met LDAP is, schakelt u de extra CNR LDAP-interfacevastlegging in. Schakel het **aldap-creatie-detail**, het **ldap-query-detail** en het **ldap-update-detail in**. Het logbericht bevat tijdstempels waarmee u kunt bepalen of LDAP het systeemknelpunt is.

Controleer de interne databases van CNR

Als u vermoedt dat het probleem kan zijn dat een of meer van de interne databases van CNR onherroepelijk zijn geworden, raadpleegt u de gebruikershandleidingen van CNR om te leren hoe de hulpprogramma's voor de geldigheid van de gegevensbank moeten worden beheerd. Als een van deze hulpprogramma's op een probleem wijst, volg de aanwijzingen in de gebruikershandleidingen om het op te lossen.

DNS-gegevens met nslookup controleren

Het nutsbedrijf is zowel met UNIX-systemen als met Windows NT meegeleverd. Het kan worden gebruikt om een DNS server te ondervragen en is daarom handig om de gegevens te controleren die door de server zijn opgeslagen. De documentatie voor uw besturingssysteem bevat gedetailleerde informatie over de mogelijkheden.

Gerelateerde informatie

- Tech Notes over Cisco NCS Network Registrar
- Technische ondersteuning - Cisco-systemen