Impostazioni e gestione CNR consigliate

Sommario

Introduzione

Questo articolo ha due finalità. In primo luogo, contiene raccomandazioni su come configurare Cisco Network Registrar (CNR) per ottenere prestazioni e stabilità ottimali e su come monitorare l'installazione di CNR. In secondo luogo, contiene raccomandazioni su come reagire se si verifica un problema. Nel caso ideale, leggere questo articolo e seguire le raccomandazioni relative alla configurazione e al monitoraggio prima di riscontrare eventuali problemi. In questo modo, eviterete i problemi. Se stai leggendo questo articolo per la prima volta perché hai un problema con CNR, vai immediatamente alla sezione Azioni immediate quando si affronta un problema. Per ulteriori informazioni sulle raccomandazioni, consultare le guide per l'utente e i riferimenti ai comandi CNR.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione standard

I suggerimenti di configurazione forniti rappresentano un punto di partenza. Se il sistema è configurato in modo diverso, verificare le impostazioni. È possibile che la configurazione sia stata sviluppata dalle versioni precedenti di CNR. CNR 5.0 e versioni successive offrono prestazioni notevolmente migliorate rispetto alle versioni precedenti, ma è necessario apportare modifiche ai parametri per ottenere il massimo vantaggio. Il presente documento è incentrato sugli ambienti dei provider di servizi di grandi dimensioni, ma molte delle raccomandazioni sono valide anche per altri ambienti CNR. Il presente documento presuppone che:

- Il provider di servizi esegue una rete a banda larga con 10.000 o più utenti.
- Si sta utilizzando CNR 5.0.3 o versione successiva.
- Si sta utilizzando il protocollo LDAP (Lightweight Directory Access Protocol). CNR viene eseguito senza LDAP, ma molti provider di servizi utilizzano LDAP.
- La saturazione dell'indirizzo IP della rete è media.
- CNR viene eseguito sui server UNIX. La maggior parte dei suggerimenti si applica allo stesso modo a Windows NT, ma la maggior parte dei provider di servizi esegue CNR su server UNIX, pertanto se UNIX e NT differiscono, viene utilizzato l'esempio UNIX.
- Sono disponibili connessioni upstream ad altri sistemi (ad esempio fatturazione, assistenza clienti o provisioning) in esecuzione su altri server.
- Il servizio DNS (Dynamic Domain Name System) non è attivo nel sito (la maggior parte dei provider di servizi non utilizza il servizio DNS).

Consigli per la configurazione e l'installazione

Pianificazione e configurazione iniziali

- Pianificare e documentare l'allocazione degli indirizzi IP.
- Operazioni a uso intensivo del disco separate: posizionare il server DHCP primario su un computer diverso dal server LDAP e dal server DNS primario.
- Documentare la configurazione del sistema di terminazione del modem via cavo (CMTS); accertarsi che le configurazioni CMTS e CNR corrispondano.
- Preparare piani di ripristino di emergenza.
- Documentare la topologia di rete.
- Prendere nota delle versioni software Cisco IOS® dei CMTS.

I passaggi più efficaci per garantire l'integrità a lungo termine della rete sono: a) pianificare la configurazione, b) registrare tali piani e c) registrare le modifiche quando vengono pianificate e apportate. Documentare i motivi delle scelte può essere di aiuto durante le sessioni di

pianificazione future.

Configurazione generale del sistema

- Utilizzare il failover sicuro. Il failover semplice, in cui un server è il server principale per tutti gli ambiti e l'altro è il backup per tutti gli ambiti (a differenza del failover simmetrico, in cui entrambi i server sono principali e il backup contemporaneamente, a seconda dell'ambito individuale), è altamente consigliato, in quanto *semplifica notevolmente* le attività di amministrazione.
- Attivare le trap SNMP (Simple Network Management Protocol). Questi esempi sono a scopo illustrativo:

```
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
```

- Accertarsi di disporre di una RAM adeguata (almeno 512 MB).
- Assicurarsi che la partizione dati sia sufficientemente grande (2,5 GB o superiore).
- Utilizzare partizioni separate per i registri e i dati.
- Garantire connessioni ad alta velocità e bassa latenza tra i server; verificare le impostazioni dell'interfaccia.

Le trap SNMP consentono di monitorare il server DHCP da un monitor di rete. Accertarsi di configurare le trap sul server DHCP, configurare il monitor in modo che le riceva e le visualizzi e, ovviamente, prestare attenzione al monitor.

La configurazione di un sistema di produzione richiede compromessi tra costi e efficacia del sistema. Questi valori vengono suggeriti presupponendo che circa 100.000 sottoscrittori su sistemi di classe E250 eseguano il failover. L'utilizzo di molti criteri, classi client, ambiti, buffer di richiesta e risposta, estensioni DHCP e altre complicazioni influiscono sulle esigenze di memoria e sulle prestazioni.

La partizione dei log (/var/nwreg2) deve essere aumentata se si aumentano il numero e le dimensioni dei log.

Configurazione DHCP

- Impostare i buffer di richiesta e risposta per una velocità effettiva ottimale. Queste raccomandazioni sono state modificate per CNR 5.0.

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

- Durata del lease del modem via cavo = 604800 (7 giorni) o superiore.
- Durata del leasing di apparecchiature per la sede del cliente (CPE): quanto più a lungo possibile (cfr. nota per gli svantaggi).
- Aumentare le dimensioni del registro DHCP e 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
```

- Configurare le impostazioni di registro che forniscono dettagli sufficienti per identificare i problemi, ma non generano dettagli eccessivi (il che rende difficile distinguere i problemi e carica inutilmente il server). Si tratta delle impostazioni consigliate generalmente applicabili. Se necessario, modificare le impostazioni per risolvere i problemi della rete:Riepilogo attivitàPredefinitoNessuna attività di failoverAbilita estensioni per il lease differitoImposta la granularità dell'ultima transazione = *1/2 intervallo di lease*Disabilitare la sostituzione del lease client-client per i criteri che offrono lease di produzione.Possibilità di fallback su sistemi locali; quando LDAP non è disponibile, CNR utilizza i dati locali:
```
nrcmd> session set visibility=3
nrcmd> dhcp enable fallback-to-local-client-data
nrcmd> session set visibility=5
```

- Se si utilizza CNR 5.5 o versioni successive, configurare la funzionalità cache del client in modo da ridurre della metà le query LDAP.
```
nrcmd> dhcp set client-cache-count=2000
nrcmd> dhcp set client-cache-ttl=5
```

Per utilizzare al meglio la capacità di throughput del CNR, dovrebbe esistere un numero di buffer di risposta da tre a quattro volte superiore rispetto ai buffer di richiesta. Il sistema utilizza solo il numero di buffer necessario. Con la riduzione dei tempi di lease, sono necessari più buffer di risposta.

Nota: i tempi di locazione devono essere rispettati finché è possibile. I lease dei modem via cavo provengono da uno spazio di indirizzi privato (generalmente net-10) e i modem si spostano raramente in posizioni diverse sulla rete. Questi contratti di locazione dovrebbero essere di una settimana o più. I contratti di leasing CPE, d'altro canto, provengono dallo spazio degli indirizzi pubblici e i CPE (in particolare i notebook) si spostano. La durata del lease deve essere impostata in modo da corrispondere alle abitudini degli utenti. Lease più lunghi riducono il carico sul server DHCP. Se si utilizzano leasing brevi (inferiori a 8 ore), aumentare i buffer di risposta fino a 2500.

Disabilitare allow-client-lease-override per garantire che i client rispettino i tempi di lease specificati nella configurazione CNR. Alcuni client tentano di ignorare l'impostazione specificata.

Possibilità di eseguire il fallback a un sito locale per mantenere la rete operativa in caso di guasto del server LDAP. Con questa impostazione, il server DHCP continua a soddisfare le richieste di lease anche se il server LDAP non risponde. Il server non avrà accesso alle informazioni specifiche del client memorizzate nel server LDAP, quindi soddisferà ogni richiesta con un'impostazione predefinita. È necessario configurare un valore predefinito ragionevole per la rete.

Infine, la funzione di cache del client mantiene in memoria i dati del client recuperati da LDAP, in modo che il server DHCP debba eseguire una query LDAP una sola volta durante il ciclo discovery-offer-request-ack, velocizzando le prestazioni del server DHCP.

Configurazione DNS

1. Abilitare la funzione di trasferimento incrementale:
```
nrcmd> dns enable ixfr-enable
```

2. Abilita notifica. Fare riferimento ai riferimenti ai comandi CNR CLI per gli argomenti da abilitare per la notifica.
3. Posizionare i server DNS primario e secondario su segmenti di rete separati.

4. Configurare i client per eseguire query su un server DNS secondario.

I server DNS secondari ricevono i dati dal server primario in uno dei due modi seguenti: a) "trasferimento di zona completo" o b) "notifica/ixfr" (trasferimento incrementale). L'utilizzo di notifica/ixfr riduce il numero di record che devono essere trasferiti dal server principale a quello secondario. Questo è fondamentale quando lo spazio dei nomi è relativamente dinamico.

Configurazione TFTP

- Impostare **initial-packet-timeout** su 2:

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

- Se si utilizza CNR 5.5 o versioni successive, abilitare la memorizzazione nella cache dei file TFTP per migliorare le prestazioni:

```
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
```

La cache dei file TFTP mantiene i file di configurazione del modem via cavo archiviati in memoria, evitando la lettura su disco ogni volta che un modem via cavo richiede un file di configurazione. È necessario creare una directory della cache dei file sul disco rigido (CacheDir nell'esempio precedente) e assegnare una dimensione massima. Scegliere le dimensioni tenendo conto della quantità totale di RAM presente nel sistema e del numero di file di configurazione necessari.

Il protocollo TFTP non richiede che il client invii un pacchetto di conferma finale (ACK) alla ricezione di un file. Se non viene ricevuto alcun ACK, il server deve mantenere la connessione client per il periodo di timeout, che ne limita la capacità di soddisfare nuove richieste. Se il server TFTP dispone della capacità di risorse, è inoltre possibile aumentare il valore dei **pacchetti max-tftp** per supportare un numero maggiore di connessioni client. Il valore predefinito per questo parametro è 512. Il valore massimo è 1000.

Configurazione LDAP CNR

Queste impostazioni mostrano una configurazione in cui CNR sta scrivendo gli aggiornamenti del lease su LDAP. Se possibile, progettare la rete in modo che non sia necessario. In questa sezione vengono forniti suggerimenti per la scrittura di aggiornamenti del lease. Ottimizzare le connessioni LDAP utilizzando oggetti LDAP di LETTURA/SCRITTURA regolabili separatamente. Ogni oggetto ottiene il proprio gruppo di thread.

```
# 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
```

La configurazione mostrata include la scrittura degli aggiornamenti del lease CNR su LDAP. È possibile eseguire questa operazione per consentire alle applicazioni di eseguire query su LDAP per ottenere informazioni sul lease correnti, ma è consigliabile evitare di strutturare l'applicazione in modo da renderlo necessario. Per rendere disponibili informazioni sullo stato del lease per un indirizzo IP, è possibile utilizzare il comando NRCMD lease per ottenere l'indirizzo MAC, la scadenza e altre informazioni sullo stato corrente del lease.

Le directory LDAP sono progettate per essere lette in modo rapido ed efficiente, ma la scrittura in una directory LDAP è inefficiente. Se si configura CNR per scrivere le informazioni sul lease su LDAP, LDAP diventa un collo di bottiglia per le prestazioni complessive del sistema. Se è necessario configurare le scritture di lease LDAP, utilizzare le impostazioni consigliate. Notare che l'accesso CNR a LDAP è stato ottimizzato mediante l'uso di oggetti "read" e "update LDAP" separati. Notare anche il timeout di scrittura di 30 secondi. Con un timeout più breve si corre il rischio di timeout delle scritture LDAP quando il carico di LDAP è elevato. CNR riprova quindi la scrittura, aggiungendo ulteriore carico a LDAP.

Il numero totale di connessioni al server LDAP non deve superare il numero massimo di thread disponibili. Se il server LDAP supporta più thread per connessione, il numero ottimale di connessioni è il numero totale di thread diviso per il numero di thread per connessione.

Parametri di ottimizzazione server LDAP

- Creare indici per i campi di ricerca.
- Configurare le dimensioni della cache per aumentare il numero di voci memorizzate nella cache, anche se la cache non deve superare un terzo della memoria disponibile.
- Configurare il numero massimo di thread per aumentare il numero di connessioni simultanee che possono essere supportate, anche se non deve superare la metà delle risorse disponibili.
- Configurare le impostazioni di registro che forniscono dettagli sufficienti per identificare i problemi ma non generano dettagli eccessivi (il che rende difficile distinguere i problemi e carica inutilmente il server).

- Utilizzare partizioni separate per i registri e i dati.

Le implementazioni specifiche del server LDAP possono variare. Per implementare questi suggerimenti, consultare la documentazione del server.

Procedure di routine

- Eseguire regolarmente il backup delle banche dati CNR. Consultare le Guide per l'utente per istruzioni. È consigliabile eseguire il backup dei database CNR almeno una volta al giorno. Conservare i file di backup per almeno due settimane.
- Eseguire regolarmente il backup di LDAP.
- Eseguire regolarmente il backup e l'archiviazione dei registri.
- Dopo aver apportato modifiche al CNR, assicurarsi che la configurazione dei server principale e di backup in uno scenario di failover rimanga coerente. Utilizzare lo strumento **cnrFailoverConfig -compare** in CNR versione 5.5 e precedenti oppure confrontare le configurazioni utilizzando WebUI in CNR 6.0 e versioni successive.
- Quando sono pianificate modifiche alla topologia di rete, impostare i tempi di rinnovo e lease DHCP su valori ridotti.
- Monitorare l'utilizzo degli indirizzi IP (utilizzare trap SNMP).
- Monitoraggio dell'utilizzo del sistema (memoria, disco, CPU e swap). A tale scopo, è utile **posizionare** il **coperchio dell'**utilità.
- Esaminare periodicamente i registri per acquisire familiarità con i casi normali. La comprensione dei registri normali consente di gestire i problemi più rapidamente.
- Esaminare periodicamente i registri per individuare le eccezioni: grep per "error", "warn" o "connect" (ad esempio, in UNIX, utilizzare **grep -i warn name_dhcp_1_log**).

Per il failover sicuro di DHCP è necessario che le impostazioni di configurazione per un ambito siano identiche nel server primario e nel server di backup per tale ambito. Quando si apporta una modifica a un'impostazione, assicurarsi di apportare la modifica in entrambi i server. Utilizzare periodicamente **cnrFailoverConfig -compare** o WebUI in CNR 6.0 e versioni successive per verificare che non vi siano differenze.

Le modifiche della topologia di rete o dell'allocazione degli indirizzi IP possono rendere necessario per i client ottenere un indirizzo diverso. È necessario pianificare un periodo di tempo in cui alcuni client su una subnet hanno un indirizzo del vecchio intervallo e altri hanno rinnovato e ottenuto un indirizzo dal nuovo intervallo. È possibile ridurre la quantità di tempo durante la quale entrambi i set di indirizzi sono attivi riducendo la durata dei lease prima di apportare la modifica in modo che tutti i client abbiano lease di breve durata. In questo modo, i clienti devono rinnovare spesso i contratti di leasing e, subito dopo aver apportato la modifica, devono acquistare un contratto di leasing dalla nuova gamma. Assicurarsi di non impostare la durata del lease in modo che i lease si esauriscano mentre si arresta e si avvia il server per apportare la modifica. Dopo aver apportato la modifica, assicurarsi di ripristinare il periodo di lease originale in modo da non aumentare il carico sul server.

L'approccio più efficace per risolvere i problemi è evitarli. Seguendo i suggerimenti sopra descritti, gli amministratori sono in sintonia con le operazioni e consentono di evitare problemi gravi. Quando si verificano dei problemi (ad esempio un aumento dei tempi di attesa I/O o dell'utilizzo della memoria per motivi sconosciuti), completare i log. Esaminare le modifiche recenti apportate all'ambiente fisico o alla configurazione CNR per verificare se è questa la causa dei problemi.

I registri CNR sono tuoi amici. Quando si inizia a utilizzare CNR, ad aggiornare CNR o a

modificare la configurazione di CNR, usare il comando **grep** descritto per verificare la presenza di eventuali problemi nei log. Quindi lavorare all'indietro nel registro per capire quando e come il problema è sorto e risolvere il problema.

Azioni immediate nell'affrontare un problema

- ***Non*** riavviare CMTS a meno che non sia richiesto dal personale di assistenza Cisco (solo per ambienti cablati).
- ***Non*** riavviare CNR a meno che non sia richiesto dal personale di supporto Cisco.
- ***Non*** disabilitare il failover sicuro se non richiesto dal personale di supporto Cisco.
- ***Non*** ricaricare, riavviare o interrompere CNR in alcun modo con la risincronizzazione sicura del failover in corso.
- ***Non*** copiare i file di registro in una directory in cui non verranno sovrascritti. In caso di arresto anomalo del CNR, copiare il file di base in una directory in cui non verrà sovrascritto.
- ***Non*** utilizzare:
  ```
  nrcmd> server dhcp getRelatedServers
  ```
  per isolare la configurazione errata del failover sicuro.
- ***Esaminare*** i registri per individuare le eccezioni. Controllare in particolare la sequenza di avvio (potrebbe trovarsi in un registro precedente): grep per "error", "warn" o "connect" (ad esempio, **grep -i error name_dhcp_1_log***).

Quando devi affrontare un problema, è fondamentale che non causi ulteriori danni mentre isoli e risolvi il problema iniziale. Il riavvio di un CMTS o di un CNR determina picchi di carico immediati in un momento in cui il sistema è già fragile. L'obiettivo è di ripristinare la piena funzionalità del sistema nel minor tempo possibile. Tempo trascorso per il conteggio dell'ultima azione. il tempo necessario per la prima azione non viene contato. In altre parole, non agite rapidamente solo per il gusto di agire rapidamente. Pensa prima di agire.

Avvia un registro di tutte le operazioni effettuate e di tutte le modifiche apportate in qualsiasi punto del sistema: Server DHCP, DNS o TFTP e modifiche apportate a qualsiasi modem CMTS o via cavo. Descrivere il problema e annotare nel dettaglio solo il comportamento osservabile.

Analizza file registro

Raccogliere i registri (/var/nwreg2/logs). Analizzare questi elementi, cercando errori o avvisi. Utilizzare un editor di testo per analizzare ulteriormente gli errori di interesse. A partire dall'errore, cercare nuovamente nel log tutte le voci relative all'indirizzo MAC, all'indirizzo IP o al nome di dominio associati all'errore.

Potrebbe essere necessario attivare la registrazione aggiuntiva per diagnosticare i problemi DHCP. Il server DHCP supporta un'ampia gamma di funzionalità di registrazione. Per un elenco delle opzioni di log e una spiegazione di ciascuna di esse, consultare la guida di riferimento dei comandi CNR CLI. Prestare attenzione, in quanto ogni messaggio di registro comporta il caricamento sul server. È necessario trovare un compromesso tra la quantità di informazioni che si chiede al CNR di registrare e le prestazioni del server.

Verifica problemi LDAP

Il problema potrebbe essere dovuto al server LDAP. CNR crea una coda di richieste al server

LDAP. Se il server LDAP non riesce a gestire il carico, la coda viene creata. Cercare nella directory /var/nwreg2/data/dhcpeventstore. Poiché le dimensioni dei file dell'archivio eventi sono fisse, in caso di creazione della coda CNR verranno creati altri file. Se nella directory sono presenti più file, significa che è in corso il backup della coda. La stessa coda viene utilizzata per accodare le richieste al server DNS, quindi se la coda è in fase di backup e si utilizza il servizio DNS, potrebbe essere occupato da richieste al server DNS. Per determinare se il problema è relativo a LDAP, attivare la registrazione aggiuntiva dell'interfaccia LDAP di CNR. Abilitare i flag di log **ldap-create-detail**, **ldap-query-detail** e **ldap-update-detail**. Il messaggio di log include timestamp che consentono di determinare se LDAP è il collo di bottiglia del sistema.

Verifica dei database interni di CNR

Se si sospetta che uno o più database interni di CNR abbiano perso l'integrità, consultare le Guide per l'utente di CNR per informazioni su come eseguire le utilità di controllo della validità del database. Se una di queste utilità indica un problema, continuare a seguire le istruzioni riportate nelle Guide per l'utente per risolverlo.

Controlla dati DNS con nslookup

L'utilità **nslookup** è inclusa sia nei sistemi UNIX che in Windows NT. Può essere utilizzato per interrogare un server DNS ed è pertanto utile per verificare i dati archiviati dal server. La documentazione del sistema operativo fornisce informazioni dettagliate sulle relative funzionalità.

Informazioni correlate

- Note tecniche su Cisco CNS Network Registrar
- Supporto tecnico – Cisco Systems