Configurações e gerenciamento de CNR recomendados

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Conventions
Configuração padrão
Recomendações de configuração e instalação
Planejamento e configuração iniciais
Configuração geral do sistema
Configuração DHCP
Configuração DNS
Configuração de TFTP
Configuração LDAP de CNR
Parâmetros de ajuste de servidor de LDAP
Procedimentos de rotina
Ações imediatas ao enfrentar um problema
Analisar arquivos de log
Verificar problemas de LDAP
Verifique os banco de dados internos de CNR
Verificar dados DNS com nslookup
Informações Relacionadas

Introduction

Esse artigo tem dois objetivos. Em primeiro lugar, contém recomendações sobre como configurar o Cisco Network Registrar (CNR) para desempenho ideal e estabilidade e sobre como monitorar a instalação do CNR. Em segundo lugar, contém recomendações sobre como você deve reagir se um problema efetivamente ocorrer. Em uma situação ideal, você lerá este artigo e seguirá as recomendações de configuração e monitoramento antes que algum problema ocorra. Com isso, você evitará problemas. Se você estiver lendo este artigo pela primeira vez porque tem um problema com o CNR, vá imediatamente para a seção Ações imediatas ao enfrentar um problema. Para obter mais explicações sobre as recomendações, consulte os Guias do Usuário CNR e Referências de Comando.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configuração padrão

As recomendações de configuração aqui oferecidas representam um ponto de partida. Se o seu sistema estiver com uma configuração diferente, revise as suas configurações. Sua configuração pode ter se desenvolvido de versões anteriores do CNR. O CNR 5.0 e as versões posteriores proporcionam um desempenho muito melhor, em comparação com as versões anteriores, mas devem ser feitas alterações de parâmetro para se obter o máximo de benefício. O foco deste documento é em amplos ambientes de provedores de serviços, mas muitas das recomendações aplicam-se também a outros ambientes de CNR. Este documento pressupõe que:

- Você é um provedor de serviços executando uma rede de banda larga com 10.000 ou mais assinantes.
- Você está usando o CNR 5.0.3 ou posterior.
- Você está usando o protocolo LDAP (Lightweight Directory Access Protocol). O CNR é executado sem LDAP, mas muitos provedores de serviços usam LDAP.
- Sua rede tem saturação de endereço IP médio.
- Você executa CNR em servidores UNIX. A maioria das recomendações se aplica igualmente ao Windows NT, mas a maioria dos provedores de serviços executa o CNR em servidores UNIX, de modo que, onde o UNIX e o NT são diferentes, o exemplo UNIX é usado.
- Você tem conexões de upstream com outros sistemas (como cobrança, atendimento ao cliente ou configuração) que estão sendo executados em outros servidores.
- O DDNS (Dynamic Domain Name System) não está ativo no seu local (a maioria dos provedores de serviços não usa DDNS).

Recomendações de configuração e instalação

Planejamento e configuração iniciais

- Planejar e documentar a alocação de endereços IP.
- Operações separadas que exigem muito do disco: coloque seu servidor DHCP principal em uma máquina diferente do servidor LDAP e do servidor DNS primário.
- Documentar a configuração do Cable Modem Termination System (CMTS); certifique-se de que as configurações de CMTS e CNR sejam compatíveis.
- Preparar planos de recuperação de desastre.
- Documente sua topologia de rede.

- Observe as versões do software Cisco IOS® dos CMTSs.

As etapas mais eficazes para a integridade da sua rede a longo prazo são: a) planeje sua configuração, b) registre esses planos e c) registre as alterações quando as alterações forem planejadas e feitas. Documentar as razões das escolhas pode ser útil em sessões futuras de planejamento.

Configuração geral do sistema

- Use failover seguro. O failover simples, em que um servidor é principal para todos os escopos, e o outro servidor é o backup para todos os escopos (ao contrário do failover simétrico, em que ambos os servidores são principais e o backup ao mesmo tempo, dependendo do escopo individual), é altamente recomendado, pois *simplifica bastante* as tarefas de administração.
- Ative as interceptações SNMP (Simple Network Management Protocol). Estes exemplos são ilustrativos:

```
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
```

- Verifique se você tem RAM adequada (512 MB ou mais).
- Verifique se a partição de dados é grande o suficiente (2,5 GB ou maior).
- Use partições separadas para logs e dados.
- Garanta conexões de alta velocidade e baixa latência entre servidores; verifique as configurações da interface.

Os desvios de SNMP permitem monitorar o servidor DHCP a partir de um monitor de rede. Não se esqueça de configurar os desvios no servidor DHCP, configurar o monitor para recebê-los e exibi-los e, obviamente, não deixe de prestar atenção no monitor.

Configurar um sistema de produção exige compensações de custos em relação à eficiência do sistema. Sugerimos esses valores supondo aproximadamente 100.000 assinantes em sistemas da classe E250 executando failover. O uso de muitas políticas, classes de clientes, escopos, buffers de solicitação e resposta, extensões DHCP e outras complicações afetam as necessidades de memória e o desempenho.

A partição de registro (/var/nwreg2) deverá ser aumentada se o número e o tamanho dos registros aumentarem.

Configuração DHCP

- Defina os buffers de solicitação e resposta para o ritmo de transferência ideal. Observe que estas recomendações mudaram no CNR 5.0.

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

- Tempo de concessão do modem a cabo = 604800 (7 dias) ou mais.
- Tempo de leasing de equipamentos nas instalações do cliente (CPE): o máximo possível (ver nota para as compensações).
- Aumente os tamanhos de log de 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
```

- Defina as configurações de log que fornecem detalhes suficientes para identificar problemas, mas não geram detalhes excessivos (o que dificulta a distinção de problemas e coloca carga desnecessária no servidor). Essas são configurações recomendadas que são geralmente aplicáveis. Ajuste as configurações, caso seja necessário lidar com questões na sua rede:Activity-summaryPadrãoNão há atividade de failoverEnable defer-lease-extensionsDefinir a granularidade da última transação = *intervalo de locação de 1/2*Desative allow-client-lease-override para políticas que oferecem leasing de produção.Habilitar fallback-to-local; quando o LDAP não está disponível, o CNR usa dados locais:
```
nrcmd> session set visibility=3
nrcmd> dhcp enable fallback-to-local-client-data
nrcmd> session set visibility=5
```

- Se estiver usando o CNR 5.5 ou posterior, configure a capacidade de cache do cliente para reduzir as consultas LDAP pela metade.
```
nrcmd> dhcp set client-cache-count=2000
nrcmd> dhcp set client-cache-ttl=5
```

Para usar o recurso de transferência de CNRs da forma mais eficiente, deve haver uma quantidade de buffers de resposta de três a quatro vezes maior do que a quantidade de buffers de requisições. O sistema usa apenas quantos buffers precisar. À medida que os tempos de leasing se tornam mais curtos, mais buffers de resposta são necessários.

Observação: os tempos de leasing devem ser feitos o quanto for prático. Os arrendamentos de modem a cabo são originários de um espaço de endereço privado (em geral, net-10), e os modems raramente movem-se para locais diferentes na rede. Essas concessões devem ser feitas por uma semana ou mais. Os arrendamentos de CPE, por outro lado, vêm do espaço de endereço público e os CPEs (em particular, laptops) se movem. Aqui, a duração do aluguel deve ser definida para corresponder aos hábitos de sua população de usuários. Concessões mais longas reduzem a carga no servidor DHCP. Ao usar concessões curtas (menos de 8 horas), aumente os buffers de resposta para 2500.

Desative allow-client-lease-override para garantir que os clientes atendam aos tempos de leasing especificados na configuração do CNR — alguns clientes tentam substituir a configuração especificada.

Habilite fall-back-to-local para manter o sistema operacional em caso de falha no servidor de LDAP. Com essa configuração, o servidor DHCP continua a atender às solicitações de concessão mesmo que o servidor LDAP não esteja respondendo. O servidor não terá acesso às informações de cliente específicas armazenadas no servidor de LDAP; por isso, ele atenderá a cada requisição com uma configuração padrão. Você deve configurar um padrão razoável para sua rede.

Finalmente, o recurso de cache de cliente mantém na memória os dados do cliente recuperados do LDAP, de modo que o servidor DHCP precisa consultar o LDAP apenas uma vez durante o ciclo discovery-offer-request-ack, acelerando o desempenho do servidor DHCP.

Configuração DNS

1. Habilite o recurso de transferência incremental:
   ```
   nrcmd> dns enable ixfr-enable
   ```

2. Habilitar notificação. Consulte as Referências de Comando CLI do CNR para obter os argumentos necessários para ativar a notificação.
3. Coloque servidores DNS primários e secundários em segmentos de rede separados.
4. Configurar clientes para consultar um servidor DNS secundário.

Os servidores DNS secundários recebem seus dados do servidor primário de duas maneiras: a) "transferência total da zona", ou b) "notificação/ixfr" (transferência incremental). O uso de notificação/ixfr reduz o número de registros que devem ser transferidos do servidor primário para o secundário. Isso é crítico quando o espaço do nome é relativamente dinâmico.

Configuração de TFTP

- Defina **initial-packet-timeout** como 2:
  ```
  nrcmd> tftp set initial-packet-timeout = 2
  ```

- Se estiver usando o CNR 5.5 ou posterior, ative o cache de arquivos TFTP para melhorar o desempenho:
  ```
  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
  ```

O cache de arquivos TFTP mantém os arquivos de configuração do modem a cabo armazenados na memória, evitando leituras em disco sempre que um modem a cabo solicita um arquivo de configuração. Um diretório de cache de arquivos precisa ser criado no disco rígido (CacheDir no exemplo acima) e um tamanho máximo é atribuído. Escolha o tamanho levando em conta a quantidade total de RAM no seu sistema e o número de diferentes arquivos de configuração necessários.

O protocolo TFTP não exige que o cliente envie um pacote de confirmação final (ACK) ao receber um arquivo. Se nenhum ACK for recebido, o servidor deverá manter a conexão do cliente por um período de tempo limite, o que limita sua capacidade de atender novas solicitações. Se o servidor TFTP tiver a capacidade do recurso, você também poderá aumentar o valor de **max-tftp-packets** para suportar um número maior de conexões de clientes. O valor padrão deste parâmetro é 512. O valor máximo é 1000.

Configuração LDAP de CNR

Essas definições mostram uma configuração em que o CNR está gravando atualizações de concessão no LDAP. Se for possível, projete sua rede para que isso não seja necessário. Ele é mostrado aqui para fornecer recomendações se você deve gravar atualizações de leasing. Otimizar conexões LDAP usando objetos LDAP de LEITURA/GRAVAÇÃO ajustáveis separadamente. (Cada objeto recebe seu próprio grupo de segmentos).

```
# 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
```

A configuração mostrada inclui fazer com que o CNR grave atualizações de aluguel no LDAP. É possível que você queira fazer isso para permitir que os aplicativos consultem o LDAP sobre informações de uso atuais, mas você deve tentar evitar estruturar o aplicativo de modo que isso seja necessário. Se você precisar disponibilizar informações sobre o estado do arrendamento para um endereço IP, poderá usar o comando de arrendamento de NRCMD para obter o endereço MAC, a expiração e outras informações sobre o status atual do arrendamento.

Os diretórios LDAP são projetados para serem lidos de forma rápida e eficiente, mas gravar para um diretório LDAP é ineficiente. Se você configurar o CNR para gravar informações de concessão no LDAP, o LDAP se tornará um gargalo para o desempenho geral do sistema. Se tiver que configurar gravações de uso do LDAP, use as configurações recomendadas. Observe que o acesso CNR ao LDAP foi otimizado por meio do uso de objetos de leitura e atualizar LDAP em separado. Observe também o tempo limite de escrita de 30 segundos. Com um intervalo de parada mais curto, é possível correr o risco do LDAP gravar o intervalo de parada quando o LDAP Depois, o CNR faz uma nova tentativa de gravação, o que adiciona carga extra ao LDAP.

O número total de conexões com o servidor LDAP não deve exceder o número máximo de segmentos disponíveis. Se o servidor LDAP suportar vários threads por conexão, o número ideal de conexões é o número total de threads divididos pelo número de threads por conexão.

Parâmetros de ajuste de servidor de LDAP

- Criar índices para campos de pesquisa.

- Configure o tamanho do cache para aumentar o número de entradas no cache de memória, embora o cache não deva exceder um terço da memória disponível.
- Configurar os segmentos máximos para aumentar o número de conexões simultâneas que podem ser suportadas, embora esse número não possa exceder metade dos recursos disponíveis.
- Defina as configurações de log que fornecem detalhes suficientes para identificar problemas, mas não geram detalhes excessivos (o que dificulta a distinção de problemas e coloca carga desnecessária no servidor).
- Use partições separadas para logs e dados.

As implementações específicas do servidor LDAP variam. Consulte a documentação do servidor para implementar essas sugestões.

Procedimentos de rotina

- Faça backup regular dos bancos de dados CNR. Consulte os Guias do Usuário para obter instruções. Você deve fazer backup dos bancos de dados CNR pelo menos uma vez por dia. Mantenha os arquivos de backup por pelo menos duas semanas.
- Faça backup regular do LDAP.
- Fazer backup e arquivar registros regularmente.
- Depois de fazer alterações no CNR, certifique-se de que a configuração dos servidores principal e de backup em um cenário de failover permaneça consistente. Use a ferramenta **cnrFailoverConfig -compare** nas versões 5.5 e anteriores do CNR ou compare as configurações usando a WebUI no CNR 6.0 e posterior.
- Quando alterações na topologia da rede forem planejadas, defina os tempos de renovação e liberação para valores pequenos.
- Monitore o uso de endereços IP (use interceptações SNMP).
- Monitore o uso do sistema (memória, disco, CPU e troca). A **parte superior** do utilitário é útil para este fim.
- Periodicamente, revise os registros para ficar familiarizado com os casos normais. A compreensão dos registros normais permite que você trate os problemas mais rapidamente.
- Analise periodicamente os logs para obter exceções: grep para "error", "warn" ou "connect" (por exemplo, no UNIX, use **grep -i warn name_dhcp_1_log**).

DHCP Safe-failover exige que os ajustes de configuração de um escopo sejam idênticos nos servidores principal e de backup para esse escopo. Certifique-se de que, ao alterar uma configuração, você faça a alteração em ambos os servidores. Use periodicamente **cnrFailoverConfig -compare** ou WebUI no CNR 6.0 ou superior para verificar se não há diferenças.

Alterações na topologia da rede ou alterações na alocação de endereços IP podem tornar necessário que os clientes obtenham um endereço diferente. Deve ser feito um plano para um período em que alguns clientes de uma sub-rede têm um endereço da faixa antiga e alguns clientes foram renovados e obtiveram um endereço da nova faixa. É possível reduzir a quantidade de tempo durante o qual os dois conjuntos de endereços estão ativos reduzindo a duração das concessões antes de fazer a alteração de modo que todos os clientes tenham concessões de curta duração. Isso garante que eles devem renovar seus aluguéis com frequência e, portanto, pegar um leasing do novo intervalo logo após a alteração. Certifique-se de não definir o tempo de concessão tão curto que os arrendamentos acabam enquanto você interrompe e inicia o servidor para fazer a alteração. Depois de fazer a alteração, certifique-se de restaurar o período de concessão original para que você não aumente a carga no servidor.

A abordagem mais efetiva para solucionar problemas é evitá-los. Seguir as recomendações descritas acima mantém seus administradores em sintonia com sua operação e permite que você evite problemas graves. Quando surgirem problemas (como aumento do tempo de espera de E/S ou aumento do uso da memória sem motivo conhecido), faça o acompanhamento dos registros. Revise as recentes alterações do ambiente físico ou da configuração do CNR para ver se essa pode ser a origem dos problemas.

Os registros CNR são seus amigos. Ao iniciar o uso do CNR, ou ao fazer a atualização do CNR, ou quando alterar a configuração do CNR, use o comando grep descrito, para verificar os logs de qualquer emissão. Em seguida, trabalhe para trás no registro para entender quando e como o problema surgiu e corrigir o problema.

Ações imediatas ao enfrentar um problema

- ***Não*** reinicialize o CMTS a menos que solicitado pela equipe de suporte da Cisco (aplica-se somente a ambientes de cabo).
- ***Não reinicie o CNR, a menos se solicitado pela equipe de suporte da Cisco.***
- ***Não desabilite o failover seguro, a menos que isso seja solicitado pela equipe de suporte Cisco.***
- ***Não*** recarregue, reinicie ou interrompa o CNR de nenhuma forma com a ressincronização segura de failover em andamento.
- ***Copie os arquivos de registro para um diretório em que não sejam sobrescritos.*** Se o CNR travou, copie o arquivo central em um diretório em que não seja substituído.
- ***Use:***
  ```
  nrcmd> server dhcp getRelatedServers
  ```

  para isolar a configuração incorreta de failover seguro.
- ***Procure exceções nos registros.*** Verifique principalmente a sequência de inicialização (que pode estar em um log antigo): grep para "error", "warn" ou "connect" por exemplo, grep -i error name_dhcp_1_log*).

Quando você enfrenta um problema, é crucial que você não cause mais danos ao isolar e corrigir o problema inicial. Reiniciar um CMTS ou reiniciar o CNR cria picos de carga imediatos durante um tempo em que o sistema já está frágil. O objetivo é ter o sistema plenamente funcional novamente no menor período de tempo. O tempo decorrido até a última ação ser contada; o tempo para sua primeira ação não conta. Por outras palavras, não tomem medidas rápidas só por uma ação rápida. Pense antes de agir.

Inicie um log de todas as etapas e todas as alterações feitas em qualquer lugar do sistema: Servidores DHCP, DNS ou TFTP e alterações feitas em qualquer CMTS ou modem a cabo. Descreva o problema e registre, em detalhes, apenas o comportamento que pode ser observado.

Analisar arquivos de log

Colete os registros (/var/nwreg2/logs). Analise isso procurando erros ou avisos. Use um editor de texto para analisar ainda mais os erros de interesse. Começando do erro para trás, procure no registro todas as entradas relativas ao endereço MAC, ao endereço IP ou ao nome de domínio associados ao erro.

Talvez seja necessário ativar o registro adicionar para diagnosticar problemas de DHCP. O servidor DHCP oferece suporte a uma ampla gama de recursos de registro. Consulte as

Referências de Comandos CLI do CNR para obter uma lista de opções de registro e uma explicação de cada uma delas. Tenha cuidado, pois cada mensagem de registro coloca carga no servidor. Você deve fazer uma troca entre a quantidade de informações que solicita ao CNR para registrar e o desempenho do servidor.

Verificar problemas de LDAP

O problema pode ser com o servidor do LDAP. O CNR cria uma fila de solicitações para o servidor LDAP. Se o servidor LDAP não conseguir acompanhar a carga, a fila será acumulada. Examine o diretório /var/nwreg2/data/dhcpeventstore. Os arquivos do repositório de eventos são corrigidos em tamanho, de modo que, se a fila estiver acumulando, o CNR criará mais arquivos. Se houver mais de um arquivo no diretório, isso indica que a fila está fazendo backup. A mesma fila é usada para colocar solicitações em fila no servidor DNS, de modo que, se a fila estiver fazendo backup e você estiver usando DDNS, ela poderá estar preenchendo solicitações ao servidor DNS. Para determinar se o problema está no LDAP, ative o registro de interface CNR LDAP adicional. Habilite os flags de log ldap-create-detail, ldap-query-detail e ldap-update-detail. A mensagem de log inclui datadores que ajudam a determinar se o LDAP é o gargalo do sistema.

Verifique os banco de dados internos de CNR

Se você suspeitar que o problema pode ser que um ou mais bancos de dados internos do CNR tenham perdido a integridade, consulte os Guias do Usuário CNR para saber como executar os utilitários de verificação de validade do banco de dados. Se um desses utilitários indicar um problema, continue seguindo as instruções nos Guias do usuário para resolvê-lo.

Verificar dados DNS com nslookup

O utilitário **nslookup** está incluído em sistemas UNIX e com Windows NT. Pode ser usado para interrogar um servidor DNS e, por isso, é útil na verificação dos dados armazenados pelo servidor. A documentação para o seu sistema operacional fornece informações detalhadas sobre os seus recursos.

Informações Relacionadas

- Notas técnicas do Cisco CNS Network Registrar
- Suporte Técnico - Cisco Systems