Contenido

Introducción

Este artículo tiene dos objetivos. Primero, contiene recomendaciones sobre cómo configurar Cisco Network Registrar (CNR) para un rendimiento y estabilidad óptimos y cómo monitorear su instalación de CNR. Segundo, contiene recomendaciones acerca de cómo debe reaccionar si ocurre un problema. En una situación ideal, usted leerá este artículo y seguirá las recomendaciones de configuración y control antes de que haya problemas. Al hacer esto, evitará problemas. Si usted está leyendo este artículo por primera vez porque usted tiene un problema con el CNR, vaya inmediatamente a las acciones inmediatas al hacer frente a una sección de problemas. Para la explicación adicional de las recomendaciones, refiera por favor a los guías del usuario y a las referencias de comandos CNR.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configuración estándar

Las recomendaciones para la configuración ofrecidas aquí representan un punto de partida. Si su sistema no está configurado de esta manera, revise sus configuraciones. Su configuración puede haberse desarrollado a partir de versiones anteriores de CNR. Las versiones 5.0 ó posteriores de CNR proporcionan un desempeño muy mejorado en comparación con las versiones anteriores, pero deben efectuarse los cambios de parámetros para maximizar los beneficios. Este documento hace hincapié en los entornos de grandes proveedores de servicios, pero muchas de las recomendaciones también se aplican a otros entornos de CNR. Este documento asume eso:

- Usted es un prestador de servicios a cargo de una red de banda ancha con 10.000 suscriptores o más.
- Usted está utilizando CNR 5.0.3 o más adelante.
- Utiliza el Protocolo ligero de acceso a directorios (LDAP). El CNR se ejecuta sin el LDAP, pero muchos proveedores de servicio utilizan el LDAP.
- Su red tiene saturación media de la dirección IP.
- Con servidores UNIX se ejecuta CNR. La mayor parte de las recomendaciones se aplican igualmente al Windows NT, pero la mayoría de los proveedores de servicio ejecutan el CNR en los servidores Unix, así que donde diferencian UNIX y NT, se utiliza el ejemplo de Unix.
- Cuenta con conexiones ascendentes en otros sistemas (como facturación, atención al cliente o abastecimiento) que se ejecutan en otros servidores.
- El Sistema de nombres de dominio (DNS) dinámico (DDNS) no es activo en su sitio (la mayoría de los proveedores de servicio no utilizan el DDNS).

Recomendaciones para la configuración e instalación

Planificación y configuración inicial

- Asignación de IP Address del plan y del documento.
- Operaciones disco-intensivas separadas: ponga a su servidor DHCP primario en una diversa máquina que su servidor LDAP y servidor DNS principal.
- Documente su configuración del Sistema de terminación del cablemódem (CMTS); asegúrese de que las configuraciones de CMTS y CNR coincidan.
- Prepare planes de recuperación ante catástrofes.
- Documente la tipología de red.
- Observe las versiones de software de Cisco IOS® de los CMTS.

Los pasos más eficaces a la salud a largo plazo de su red son: a) planea su configuración, b) expediente esos planes, y c) expediente los cambios cuando se planean y se realizan los cambios. La documentación de los motivos de la elección puede ser útil durante las futuras sesiones de planificación.

Configuración del sistema general

- Use una conmutación por error segura. El fallo simple, donde está principal un servidor para todos los alcances, y el otro servidor es de reserva para todos los alcances (en comparación con la Conmutación por falla simétrica, donde están principales ambos servidores y de reserva al mismo tiempo, dependiendo del alcance individual), se recomienda altamente, pues *simplifica grandemente las* tareas de la administración.
- Gire los desvíos del Simple Network Management Protocol (SNMP). Estos ejemplos están para el ejemplo:`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**`
- Esté seguro que usted tiene RAM adecuado (512 MB o mayor).
- Esté seguro que la división de los datos es bastante grande (2.5 GB o mayores).
- Use particiones separadas para registros y datos.
- Asegure de alta velocidad, las conexiones de la latencia baja entre los servidores; verifique las configuraciones de las interfaces.

Las trampas de SNMP le permiten controlar el servidor DHCP desde un monitor de red. Asegúrese de configurar las trampas en el servidor DHCP, de configurar el monitor para que las reciba y las muestre, y obviamente asegúrese de prestar atención al monitor.

Configurar un sistema de producción requiere los equilibrios de costar contra la efectividad del sistema. Sugerimos estos valores si se asume que cerca de 100,000 suscriptores en los sistemas que ejecutan la recuperación de fallas. E250-class. El uso de muchas directivas, los clientes class, los alcances, los buffers de la solicitud y de la respuesta, las extensiones DHCP, y otras complicaciones afecta a las necesidades de la memoria y al funcionamiento.

La partición de registros (/var/nwreg2) deberá incrementarse si el número y el tamaño de registros aumenta.

Configuración DHCP

- Configure los búfers de pedido y de respuesta para un rendimiento óptimo. Tenga en cuenta que estas recomendaciones han cambiado para CNR 5.0.`nrcmd> **DHCP set max-dhcp-requests=500**nrcmd> **DHCP set max-dhcp-responses=2000**`
- Tiempo de validez del módem de cable = 604800 (7 días) o más.
- Tiempo de validez del Customer Premises Equipment (CPE): todo el tiempo posible (véase la nota para los equilibrios).
- Aumente los tamaños del registro del DHCP y 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**`
- Configure las configuraciones de registro que proporcionan bastante detalle para identificar los problemas, pero no genere el detalle excesivo (que hace difícil distinguir los problemas y pone la carga innecesaria en el servidor). Éstas son las configuraciones recomendadas que son generalmente aplicables. Si es necesario, ajuste su configuración para atender los problemas en su red:Actividad-resumenPredeterminadoActividad sin fallasHabilitar defer-lease-extensionsFije el último-transacción-tiempo-granularity del = *intervalo del arriendo 1/2*Inhabilite la permitir-cliente-arriendo-invalidación para las directivas que ofrecen los arriendos de la producción.Habilite caída-detrás-a-local; cuando el LDAP es inasequible, el CNR utiliza los datos locales:`nrcmd> **session set visibility=3**nrcmd> **dhcp enable fallback-to-**`

local-client-datanrcmd> **session set visibility=5**

- Si usa el CNR 5.5 o más adelante, configura la capacidad del caché del cliente para reducir las interrogaciones LDAP por la mitad.nrcmd> **dhcp set client-cache-count=2000**nrcmd> **dhcp set client-cache-ttl=5**

Para utilizar de manera más efectiva la capacidad de rendimiento de los CNR, debería haber tres o cuatro veces más búfers de respuesta que búfers de solicitud. El sistema utiliza solamente tantos buffers mientras que necesita. Mientras que los Tiempos de validez llegan a ser más cortos, se requieren más buffers de la respuesta.

Nota: Los tiempos de validez deben extenderse hasta tanto sean prácticos. Los alquileres de cablemódem provienen de un espacio de dirección privada (por lo general, red-10) y es muy raro que los módems se trasladen a diversos lugares de la red. La valides debería establecerse en una semana o más. Los arriendos del CPE, por otra parte, venidos del espacio de dirección pública, y de CPEs (particularmente, las laptopes) se mueven alrededor. Aquí el tiempo de validez se debe fijar para hacer juego los hábitos de su población de usuarios. Los arrendamientos prolongados reducen la carga en el servidor DHCP. Si utiliza arrendamientos cortos (de menos de 8 horas), aumente los búfers de respuesta a 2500.

¿Inhabilite la permitir-cliente-arriendo-invalidación para asegurarse de que los clientes se adhieren a los Tiempos de validez especificados en su configuración de CNR? algunos clientes intentan reemplazar la configuración especificada.

Habilite la opción fall-back-to-local (recurrir a local) para mantener su red en funcionamiento en el caso de una falla en un servidor LDAP Con esta configuración, el servidor DHCP continúa satisfaciendo las solicitudes del arriendo aunque no está respondiendo el servidor LDAP. El servidor no tendrá acceso a la información específica del cliente almacenada en el servidor LDAP, por lo que cubrirá cada solicitud con una configuración predeterminada. Usted debe configurar un valor por defecto que sea razonable para su red.

Finalmente, la característica del caché del cliente mantiene la memoria que los datos del cliente extrajeron del LDAP, de modo que el servidor DHCP necesite preguntar el LDAP solamente una vez durante el ciclo detección-oferta-petición-ACK, acelerando el funcionamiento del servidor DHCP.

Configuración de DNS

1. Habilite la función de transferencia gradual:nrcmd> **dns enable ixfr-enable**
2. El permiso notifica. Refiera a las referencias del comando CLI CNR para los argumentos que usted necesita habilitar notifica.
3. Ponga a los servidores DNS principales y secundarios en los segmentos de red separados.
4. Configure a los clientes para preguntar a un servidor DNS secundario.

Los servidores DNS secundarios reciben sus datos del servidor primario uno de dos maneras: a) la “transferencia de zona completa,” o b) “notifica/ixfr” (transferencia ampliada). Usando notifique/ixfr reduce la cantidad de registros que se debe transferir del primario a los servidores secundarios. Esto es crítico cuando el espacio para nombre es relativamente dinámico.

Configuración de TFTP

- Fije el **Initial-packet-timeout a** 2:nrcmd> **tftp set initial-packet-timeout = 2**
- Si usa el CNR 5.5 o más adelante, habilita el archivo TFTP que oculta para mejorar el funcionamiento:nrcmd> **tftp set home-directory=/var/nwreg2/data/tftp**nrcmd> **tftp set file-**

```
cache-directory=CacheDirnrcmd> tftp set file-cache-max-memory-size=32000nrcmd> tftp enable
file-cachenrcmd> tftp reload
```

El almacenamiento en memoria inmediata del archivo TFTP mantiene los archivos de configuración de cablemódem salvados en la memoria, evitando lee al disco cada vez que un módem de cable pide un archivo de configuración. Un directorio de caché del archivo necesita ser creado en la unidad de disco duro (CacheDir en el ejemplo anterior), y se asigna un tamaño máximo. Elija el tamaño que tiene en cuenta la cantidad total de RAM en su sistema y el número de diversos archivos de configuración necesarios.

El protocolo TFTP no requiere al cliente enviar un paquete del reconocimiento final (ACK) en el recibo de un archivo. Si no se recibe ningún ACK, el servidor debe llevar a cabo la conexión cliente para el período de agotamiento del tiempo de espera, que limita su capacidad de mantener las nuevas peticiones. Si su servidor TFTP tiene la capacidad de recursos, usted puede también aumentar el valor del **Max-tftp-packets** para soportar un mayor número de conexiones cliente. El valor predeterminado para este parámetro es 512. El valor máximo es 1000.

Configuración de CNR LDAP

Estos parámetros muestran una configuración en la que CNR escribe actualizaciones de arrendamiento en el LDAP. Si es posible, diseñe su red para que esto no sea necesario. Se muestra aquí para proporcionar las recomendaciones si usted debe escribir las actualizaciones del arriendo. Optimice las conexiones LDAP usando los objetos por separado armoniosos del READ/WRITE LDAP. (Cada objeto consigue su propio grupo de hilos).

```
nrcmd> tftp set home-directory=/var/nwreg2/data/tftpnrcmd> tftp set file-cache-
directory=CacheDirnrcmd> tftp set file-cache-max-memory-size=32000nrcmd> tftp enable file-
cachenrcmd> tftp reload
```

La configuración presentada incluye hacer que CNR escriba actualizaciones de arrendamiento en el LDAP. Quizás quiera hacer esto para permitir que las aplicaciones consulten a LDAP por la información de arrendamiento actual aunque debe tratar de evitar estructurar su aplicación para que esto sea necesario. Si necesita que la información sobre el estado de arrendamiento para una dirección IP esté disponible, puede usar el comando NRCMD lease para obtener la dirección MAC, el vencimiento y más información sobre el estado actual del arrendamiento.

Los directorios LDAP fueron diseñados para ser leídos rápida y eficientemente, pero la escritura en directorios LDAP es ineficiente. Si usted configura el CNR para escribir la información sobre arrendamiento al LDAP, el LDAP se convierte en un embotellamiento al funcionamiento general del sistema. Si debe configurar escrituras de arrendamiento LDAP, utilice las configuraciones recomendadas. Tenga en cuenta que el acceso CNR a LDAP se ha optimizado a través del uso de objetos de "leer" y "actualizar LDAP" separados. Asimismo, observe el tiempo de espera de escritura de 30 segundos. Con un tiempo de espera más corto corre el riesgo de que las escrituras de LDAP se suspendan cuando el LDAP está bajo carga pesada. Luego, CNR vuelve a intentar escribir y esto genera una carga adicional en LDAP.

La cantidad total de conexiones a su servidor LDAP no debería exceder la cantidad máxima de secuencias disponibles. Si su servidor LDAP soporta los varios subprocesos por la conexión, la cantidad óptima de conexiones es el número total de hilos divididos por el número de hilos por la conexión.

Parámetros de ajuste del servidor LDAP

- Cree los índices para los campos de las operaciones de búsqueda.

- Configure el tamaño de la memoria caché para aumentar la cantidad de entradas almacenadas en la memoria caché, a pesar de que ésta no debe exceder un tercio de la memoria disponible.
- Configure secuencias máximas para aumentar el número de conexiones simultáneas que se pueden admitir, aunque éste no debería consumir más de la mitad de los recursos disponibles.
- Configure las configuraciones de registro que proporcionan bastante detalle para identificar los problemas pero no genere el detalle excesivo (que hace difícil distinguir los problemas y pone la carga innecesaria en el servidor).
- Use particiones separadas para registros y datos.

Las implementaciones de servidor LDAP específicas varían. Refiera a su documentación del servidor para implementar estas sugerencias.

Procedimientos de rutina

- Sostenga regularmente las bases de datos CNR. Refiera a los guías del usuario para las instrucciones. Usted debe sostener las bases de datos CNR por lo menos una vez al día. Conserve los archivos de respaldo al menos por dos semanas.
- Sostenga regularmente el LDAP.
- Regularmente salvaguardia y registros del archivo.
- Después de que los cambios se realicen al CNR, asegúrese de que la configuración del principal y los servidores de backup en un escenario de falla siga siendo constantes. Utilice el **cnrFailoverConfig - compare la** herramienta en las versiones de CNR 5.5 y anterior, o compare las configuraciones usando el WebUI en CNR 6.0 y posterior.
- Cuando se programan cambios en la topología de la red, establezca los tiempos de renovación y arrendamiento de DHCP en valores reducidos.
- Monitoree el uso de la dirección IP (SNMP traps del uso).
- Monitoree la utilización del sistema (memoria, disco, CPU, e intercambio). **El top** utilitario es para este propósito útil.
- Periódicamente revise los registros para familiarizarse con los casos normales. La comprensión de los registros normales le deja manejar los problemas más rápidamente.
- Periódicamente registros del estudio para las excepciones: grep para el “error”, “advierta”, o “Conectar” (por ejemplo, en UNIX, **grep del** uso **- advierto el name_dhcp_1_log**).

La conmutación por error segura DHCP requiere que los parámetros de configuración para un alcance sean idénticos en el servidor primario y de respaldo para ese alcance. Esté seguro, cuando usted realiza un cambio a una configuración, que usted realiza el cambio en ambos servidores. Periódicamente **cnrFailoverConfig del** uso **- compare** o el WebUI en CNR 6.0 y arriba marcar para aseegurarse allí no es ninguna diferencia.

Los cambios de los cambios de la topología de red o de la asignación de IP Address pueden hacerlo necesario para que los clientes consigan un diverso direccionamiento. Debe planificar un periodo de tiempo en el cual algunos clientes en una subred tengan una dirección del rango viejo y algunos hayan renovado y obtenido una dirección del rango nuevo. Puede reducir la cantidad de tiempo durante el cual ambas direcciones son activadas reduciendo la duración de validez antes que realice el cambio para que todos los clientes tengan una duración de validez corta. Esto se asegura de que deban renovar sus arriendos con frecuencia y por lo tanto para escoger para arriba un arriendo del nuevo rango pronto después de que usted realice el cambio. Esté seguro de no fijar el cortocircuito del Tiempo de validez tanto como los arriendos ejecutados hacia fuera

mientras que usted para y enciende el servidor para realizar el cambio. Después de que usted haya realizado el cambio, esté seguro de restablecer el período de arrendamiento original de modo que usted no aumente la carga en el servidor.

El método más efectivo para resolver problemas es evitarlos. Después de las recomendaciones delineadas arriba guarda a sus administradores en armonía con su operación y le permite para evitar los problemas graves. Cuando aparecen los problemas (por ejemplo los aumentos o el uso de la memoria del tiempo de espera entrada-salida aumenta por ninguna razón sabida), siga con los registros. Revise los cambios recientes en su entorno físico o en la configuración de CNR para verificar si pueden ser la fuente de los problemas.

Los registros CNR son sus amigos. Cuando comienza a utilizar CNR, a actualizarlo o a cambiar su configuración, use el comando grep descripto para verificar que los registros no tengan errores. Entonces trabaje al revés en el registro para entender cuando y cómo se presentó el problema, y repare el problema.

Acciones inmediatas cuando se enfrenta un problema

- No reinicie el CMTS a menos que sea pedido para hacer tan por el equipo de soporte técnico de Cisco (se aplica a los entornos de cable solamente).
- No reinicie el CNR, salvo que el personal de asistencia de Cisco se lo solicite.
- No inhabilite el modo a prueba de fallos, salvo que así lo solicite el personal de soporte de Cisco.
- No recargue, recomience, o interrumpa el CNR de cualquier manera con la resincronización de la falla segura en curso.
- Copie los archivos de registro en un directorio donde no se los pueda sobrescribir. Si CNR sufrió una caída, copie el archivo central en un directorio en el que no sea sobrescrito.
- Debe utilizar:`nrcmd> server dhcp getRelatedServers`para aislar el misconfiguration de la falla segura.
- Busque en el registro las excepciones. Marque determinado la secuencia de lanzamiento (esto puede estar en un registro viejo): grep para el “error”, “advierta”, o “Conectar” (e.g **error name_dhcp_1_log* del** grep-yo**).**

Cuando usted hace frente a un problema, es crucial que usted no causa ningún otro daño mientras que aísla y repara el problema inicial. Reiniciar un CMTS o el recomienzo del CNR crea los puntos inmediatos de la carga durante una época en que el sistema es ya frágil. El objetivo es que su sistema vuelva a funcionar en su totalidad en la menor cantidad de tiempo. El tiempo transcurrido hasta sus cuentas más recientes de la acción; el tiempo a su primera acción no cuenta. Es decir no tome la acción rápida apenas por la acción rápida. Piense antes de actuar.

Comience un registro de todas las medidas tomadas y de todos los cambios realizados dondequiera en el sistema: DHCP, DNS, o servidores TFTP, y cambios realizados a cualquier CMTS o módem de cable. Describa el problema y registre, en detalle, sólo la conducta observable.

Analizar archivos de registro’

Recoja los registros (/var/nwreg2/logs). Analícelos buscando errores o advertencias. Utilice un editor de textos para analizar más lejos los errores de interés. Comenzando por el error, revise todas las entradas del registro que relacionan al error con la dirección MAC, con la dirección IP o con el nombre del dominio.

Puede ser necesario encender la registración adicional para diagnosticar los problemas del DHCP. El servidor DHCP soporta una extensa gama de capacidades de registro. Refiera a las referencias del comando CLI CNR para una lista de opciones de registro y una explicación de cada uno. Tenga cuidado, ya que cada mensaje del registro coloca carga en el servidor. Usted debe hacer un equilibrio entre la cantidad de información que usted pide que el CNR registren y el rendimiento del servidor.

Verifique si hay problemas de LDAP

Es posible que el problema pertenezca al servidor de LDAP. El CNR construye una cola de las peticiones al servidor LDAP. Si el servidor LDAP no puede continuar con la carga, la cola se acumula. Mire en el directorio de /var/nwreg2/data/dhcpeventstore. Los archivos del almacén del evento se reparan de tamaño, así que si la cola se está acumulando, el CNR crea más archivos. Si hay más de un archivo en el directorio, éste indica que la cola está sosteniendo. La misma cola se utiliza para hacer cola las peticiones al servidor DNS, así que si la cola está sosteniendo, y usted está utilizando el DDNS, él podría llenar de las peticiones al servidor DNS. Para determinar si el problema está con el LDAP, gire la registración adicional de la interfaz LDAP CNR. Habilite los indicadores de registro ldap-create-detail, ldap-query-detail y ldap-update-detail. El mensaje del registro incluye los sellos de fecha/hora que ayuda que usted determina si el LDAP es el embotellamiento del sistema.

Verificar las bases de datos internas de CNR

Si usted sospecha el problema puede ser que uno o más de las bases de datos internas CNR han perdido la integridad, refiere a los guías del usuario CNR para aprender cómo funcionar con las utilidades de la comprobación de validez de la base de datos. Si una de estas utilidades indica un problema, continúe siguiendo las direcciones en los guías del usuario para resolverlo.

Marque los datos de DNS con el nslookup

Utilidad nslookup se incluye con los sistemas Unix y con el Windows NT. Puede ser utilizado para interrogar un servidor DNS y, en consecuencia, es útil para verificar los datos almacenados por el servidor. La documentación para su sistema operativo proporciona información detallada acerca de sus capacidades.

Información Relacionada

- Recomendación técnica de Cisco Network Registrar CNS
- Soporte Técnico - Cisco Systems