Contenu

Introduction

Cet article a deux buts. D'abord, il contient des recommandations concernant la façon configurer le Cisco Network Registrar (le CNR) pour la performance optimale et la stabilité et la façon surveiller votre installation CNR. En second lieu, il contient des recommandations concernant la façon dont vous devriez réagir si un problème se pose. Dans le cas idéal, vous lirez ces article et acte suivant les recommandations de configuration et de surveillance avant que tous les problèmes se posent. Ce faisant, vous éviterez des problèmes. Si vous lisez cet article pour la première fois parce que vous avez un problème avec le CNR, allez immédiatement aux actions immédiates en faisant face à une section Problème. Pour davantage d'explication des recommandations, référez-vous s'il vous plaît aux guides utilisateurs et aux références de commandes CNR.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration standard

Les recommandations de configuration offertes ici représentent un point commençant. Si votre système est configuré différemment de ceci, passez en revue vos configurations. Votre configuration a pu s'être développée à partir des versions antérieures du CNR. Le CNR 5.0 et les versions ultérieures fournissent la représentation beaucoup-améliorée comparée aux versions antérieures, mais des modifications de paramètre devraient être apportées pour réaliser l'avantage maximum. Le centre de ce document est sur de grands environnements de fournisseur de services, mais plusieurs des recommandations s'appliquent à d'autres environnements CNR aussi bien. Ce document suppose cela :

- Vous êtes un fournisseur de services exécutant un réseau haut débit avec 10,000 abonnés ou plus.
- Vous utilisez le CNR 5.0.3 ou plus tard.
- Vous utilisez le Protocole LDAP (Lightweight Directory Access Protocol). Le CNR s'exécute sans LDAP, mais beaucoup de fournisseurs de services utilisent le LDAP.
- Votre réseau a la saturation moyenne d'adresse IP.
- Vous dirigez le CNR sur des serveurs Unix. La plupart des recommandations s'appliquent également à Windows NT, mais à la plupart de CNR de passage de fournisseurs de services sur des serveurs Unix, ainsi où l'UNIX et le NT diffèrent, l'exemple UNIX est utilisé.
- Vous entretenez les relations en amont à d'autres systèmes (tels que la facturation, l'assistance à la clientèle, ou le ravitaillement) qui s'exécutent sur d'autres serveurs.
- Le Dynamic Domain Name System (DDNS) n'est pas en activité à votre site (la plupart des fournisseurs de services n'utilisent pas DDNS).

Recommandations pour la configuration et l'installation

Planification initiale et installation

- Allocation d'adresse IP de plan et de document.
- Exécutions disque-intensives distinctes : mettez votre serveur DHCP primaire sur un ordinateur différent que votre serveur LDAP et serveur de DNS principal.
- Documentez votre configuration du système de terminaison par modem câble (CMTS) ; correspondance assurez-vous CMTS et CNR configurations.
- Préparez les plans de Reprise sur sinistre.
- Documentez votre topologie du réseau.
- Notez les versions de logiciel de Cisco IOS® de CMTSs.

Les étapes les plus efficaces aux santés à long terme de votre réseau sont : a) prévoient votre configuration, b) enregistrement ces plans, et c) enregistrement les modifications quand des modifications sont prévues et apportées. La documentation des raisons pour des choix peut aider pendant les sessions de plan futur.

Configuration de système général

- Basculement de coffre-fort d'utilisation. Le Basculement simple, où un serveur est principal pour toutes les portées, et l'autre serveur est de sauvegarde pour toutes les portées (par opposition au Basculement symétrique, où les deux serveurs sont principaux et de sauvegarde en même temps, selon la portée individuelle), est fortement recommandé, car elle *simplifie considérablement les* tâches de gestion.
- Activez les déroutements de Protocole SNMP (Simple Network Management Protocol). Ces exemples sont pour l'illustration :`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**`
- Soyez sûr que vous avez la RAM adéquate (512 Mo ou plus grands).
- Soyez sûr que la partition de données est assez grande (2.5 Go ou plus grands).
- Partitions distinctes d'utilisation pour des logs et des données.
- Assurez la haute vitesse, des connexions de faible latence entre les serveurs ; vérifiez les paramètres d'interface.

Les déroutements SNMP te permettent de surveiller le serveur DHCP d'une surveillance réseau. Soyez sûr de configurer les déroutements sur le serveur DHCP, de configurer le moniteur pour recevoir et de les afficher, et d'être évidemment sûr de prêter l'attention au moniteur.

Configurer un système de production exige des compromis de coûter contre l'efficacité de système. Nous proposons ces valeurs assumant environ 100,000 abonnés sur des systèmes E250-class exécutant le Basculement. L'utilisation de beaucoup de stratégies, de client-classes, de portées, de mémoires tampons de demande et de réponse, d'extensions DHCP, et d'autres complications affecte les besoins de mémoire et la représentation.

La partition de log (/var/nwreg2) devrait être augmentée si le nombre et la taille de logs est augmenté.

Configuration DHCP

- Placez les mémoires tampons de demande et de réponse pour le débit optimal. Notez que ces recommandations ont changé pour le CNR 5.0.`nrcmd> **DHCP set max-dhcp-requests=500**nrcmd> **DHCP set max-dhcp-responses=2000**`
- Durée de bail de modem câble = 604800 (7 jours) ou plus.
- Durée de bail de la CPE (CPE) : aussi longtemps que possible (voir la note pour des compromis).
- Des tailles augmentez DHCP et TFTP log :`nrcmd> **server DHCP serverLogs nlogs=15 logsize=10M**nrcmd> **server DNS serverLogs nlogs=15 logsize=10M**nrcmd> **server TFTP serverLogs nlogs=10 logsize=10M**`
- Configurez les configurations de log qui fournissent assez de détail pour identifier des problèmes, mais ne générez pas le détail excessif (qui le rend difficile de distinguer des problèmes et met le chargement inutile sur le serveur). Ce sont des configurations recommandées qui s'appliquent généralement. Ajustez vos configurations s'il y a lieu pour traiter des questions dans votre réseau :Activité-résuméPar défautNO--Basculement-activitéReporter-bail-extensions d'enableFixez la dernier-transaction-temps-finesse = *intervalle de bail de 1/2*Autoriser-client-bail-dépassement de débronchement pour des stratégies offrant des baux de production.Chute-de retour-à-gens du pays d'enable ; quand le LDAP est indisponible, le CNR utilise des données locales :`nrcmd> **session set**`

`visibility=3`nrcmd> **`dhcp enable fallback-to-local-client-data`**nrcmd> **`session set visibility=5`**

- Si utilisant le CNR 5.5 ou plus tard, configurent la capacité de client-cache pour réduire les requêtes de LDAP par moitié.nrcmd> **`dhcp set client-cache-count=2000`**nrcmd> **`dhcp set client-cache-ttl=5`**

Pour faire l'utilisation la plus efficace de la capacité du débit du CNR, il devrait y avoir trois à quatre fois autant de mémoires tampons de réponse comme mémoires tampons de demande. Le système utilise seulement autant de mémoires tampons pendant qu'il a besoin. Pendant que les durées de bail deviennent plus courtes, plus de mémoires tampons de réponse sont exigées.

Remarque: Des durées de bail devraient être faites tant que est pratique. Les baux de modem câble proviennent un espace d'adressage privé (habituellement net-10), et les Modems se déplacent rarement autour aux endroits différents sur le net. Ces baux devraient être faits une semaine ou plus long. Les baux CPE, d'autre part, proviennent l'espace adresse d'annonce publique, et CPEs (en particulier, des ordinateurs portables) se déplacent autour. Ici la durée de bail doit être placée pour apparier les habitudes de votre population d'utilisateurs. Les baux plus à long terme réduisent le chargement sur le serveur DHCP. En utilisant sous peu des baux (moins de 8 heures), augmentez les mémoires tampons de réponse à 2500.

Désactivez l'autoriser-client-bail-dépassement pour s'assurer que les clients adhèrent aux durées de bail spécifiées dans votre configuration CNR ? tentative de quelques clients d'ignorer la configuration spécifiée.

Permettez aux chute-de retour-à-gens du pays de continuer votre réseau fonctionner en cas d'une panne de serveur LDAP. Avec cette configuration, le serveur DHCP continue à satisfaire des demandes de bail quoique le serveur LDAP ne réponde pas. Le serveur n'aura pas accès aux informations spécifiques de client qui sont stockées dans le serveur LDAP, ainsi elles satisferont chaque demande avec une valeur par défaut. Vous devez configurer un par défaut qui est raisonnable pour votre réseau.

En conclusion, la caractéristique de client-cache maintient dans la mémoire que les données de client ont récupéré du LDAP, de sorte que le serveur DHCP doive questionner le LDAP seulement une fois pendant le cycle détection-offre-demande-ACK, accélérant la représentation de serveur DHCP.

Configuration DNS

1. Activez la fonctionnalité de transfert incrémentale :nrcmd> **`dns enable ixfr-enable`**
2. L'enable annoncent. Référez-vous aux références de commandes CNR CLI pour les arguments que vous devez activer annoncez.
3. Mettez les serveurs DNS principaux et secondaires sur des segments de réseau indépendant.
4. Configurez les clients pour questionner un serveur de DNS secondaire.

Les serveurs de DNS secondaire reçoivent leurs données du serveur primaire un de deux manières : a) le « plein transfert de zone, » ou b) « annoncent/ixfr » (transfert par étapes). Utilisant annoncez/ixfr réduit le nombre d'enregistrements qui doivent être transférés du primaire vers les serveurs secondaires. C'est essentiel quand l'espace de nom est relativement dynamique.

Configuration TFTP

- Placez l'initiale-paquet-**délai d'attente à** 2 :nrcmd> **`tftp set initial-packet-timeout = 2`**
- Si utilisant le CNR 5.5 ou plus tard, permettent à la mise en cache de fichier TFTP d'améliorer

la représentation :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 mise en cache de fichier TFTP maintient les fichiers de configuration de modem câble enregistrés dans la mémoire, évitant lit au disque chaque fois qu'un modem câble demande un fichier de configuration. Un répertoire de cache de fichier doit être créé dans le disque dur (CacheDir dans l'exemple ci-dessus), et une taille maximale est assignée. Choisissez la taille prenant en considération la quantité totale de RAM dans votre système et le nombre de différents fichiers de configuration requis.

Le protocole TFTP n'exige pas du client d'envoyer un paquet final de l'accusé de réception (ACK) à la réception d'un fichier. Si aucun ACK n'est reçu, le serveur doit tenir la connexion client pour le délai d'inactivité, qui limite sa capacité d'entretenir de nouvelles demandes. Si votre serveur TFTP a la capacité de ressource, vous pouvez également augmenter la valeur des maximum-tftp-**paquets** pour prendre en charge un plus grand nombre de connexions client. La valeur par défaut pour ce paramètre est 512. La valeur maximale est 1000.

Configuration de LDAP CNR

Ces configurations affichent à une configuration où le CNR écrit des mises à jour de bail au LDAP. Si possible, concevez votre réseau ainsi que ce n'est pas nécessaire. On lui affiche ici pour fournir des recommandations si vous devez écrire des mises à jour de bail. Optimisez les connexions de LDAP à l'aide des objets LECTURE/ÉCRITURE séparément réglables de LDAP. (Chaque objet obtient son propre groupe de thread).

```
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 configuration illustrée inclut avoir le CNR écrivent des mises à jour de bail au LDAP. Vous pouvez vouloir faire ceci pour permettre aux applications pour questionner le LDAP pour les informations en cours de bail, mais vous devriez essayer d'éviter de structurer votre application de sorte que ce soit nécessaire. Si vous devez faire les informations disponibles au sujet de l'état du bail pour une adresse IP vous pouvez utiliser la commande de bail NRCMD d'obtenir l'adresse MAC, l'expiration et d'autres informations sur l'état actuel du bail.

Des répertoires LDAP sont conçus pour être lus rapidement et efficacement, mais l'écriture à un répertoire LDAP est inefficace. Si vous configurez le CNR pour écrire les informations de bail au LDAP, le LDAP devient un étranglement à la performance globale du système. Si vous devez configurer le bail de LDAP écrit, utilise les configurations recommandées. Notez que le CNR accèdent à au LDAP a été optimisé par l'utilisation « lue » et des objets distincts « mettez à jour LDAP ». La note également les 30 seconde écrivent le délai d'attente. Avec un délai d'attente plus court que vous courez le risque de LDAP écrit la synchronisation quand le LDAP est sous la charge lourde. Alors le CNR relance l'inscription, qui ajoute le chargement supplémentaire au LDAP.

Le nombre total de connexions à votre serveur LDAP ne devrait pas dépasser le nombre maximal de thread disponibles. Si votre serveur LDAP prend en charge des fils multiples par connexion, le nombre optimal de connexions est le nombre total de thread divisés par le nombre de thread par connexion.

Paramètres de accord de serveur LDAP

- Créez les index pour des champs de consultation.
- Configurez la taille de mise en cache pour augmenter le nombre d'entrées cachées dans la mémoire, bien que le cache ne devrait pas dépasser un tiers de la mémoire disponible.
- Configurez les thread maximum pour augmenter le nombre de connexions simultanées qui peuvent être prises en charge, bien que ceci ne devrait pas dépasser un demi- de ressources disponibles.
- Configurez les configurations de log qui fournissent assez de détail pour identifier des problèmes mais ne générez pas le détail excessif (qui le rend difficile de distinguer des problèmes et met le chargement inutile sur le serveur).
- Partitions distinctes d'utilisation pour des logs et des données.

Les réalisations de serveur LDAP spécifiques varient. Référez-vous à votre documentation de serveur pour implémenter ces suggestions.

Procédures courantes

- Sauvegardez régulièrement les bases de données CNR. Référez-vous aux guides utilisateurs pour des instructions. Vous devriez sauvegarder les bases de données CNR au moins une fois par jour. Retenez les fichiers de sauvegarde pendant au moins deux semaines.
- Sauvegardez régulièrement le LDAP.
- Sauvegardez régulièrement et des logs d'archives.
- Après que des modifications soient apportées au CNR, assurez-vous que la configuration des serveurs principaux et de sauvegarde dans un scénario de Basculement demeure cohérente. Utilisez le **cnrFailoverConfig - comparez l'**outil dans des versions 5.5 et antérieures CNR, ou comparez les configurations utilisant le WebUI au CNR 6.0 et plus tard.
- Quand des modifications de topologie du réseau sont prévues, placez le DHCP renouvellent et des durées de bail à de petites valeurs.
- Surveillez l'utilisation d'adresse IP (déroutements SNMP d'utilisation).
- Surveillez l'utilisation de système (mémoire, disque, CPU, et échange). **Le dessus** de service est utile à cet effet.
- Périodiquement l'examen se connecte pour se familiariser avec les cas normaux. La compréhension des logs normaux vous permet de traiter des problèmes plus rapidement.
- Périodiquement logs d'examen pour des exceptions : grep pour la « erreur », « avertissez », ou « connectez » (par exemple, dans l'UNIX, **grep d'**utilisation **- j'avertis name_dhcp_1_log**).

Le Coffre--Basculement DHCP exige que les paramètres de configuration pour une portée soient identiques sur le serveur primaire et de sauvegarde pour cette portée. Soyez sûr, quand vous modifiez une configuration, que vous apportez la modification sur les deux serveurs. Périodiquement **cnrFailoverConfig d'**utilisation **- comparez** ou WebUI au CNR 6.0 et vérifier en haut pour s'assurer là ne sont aucune différence.

La topologie du réseau change ou les modifications d'allocation d'adresse IP peuvent la rendre nécessaire pour que les clients obtiennent une adresse différente. Vous devez prévoir pendant une période où quelques clients sur un sous-réseau ont une adresse de la vieille plage et certains ont renouvelé et ont une adresse de la nouvelle gamme. Vous pouvez réduire la durée pendant laquelle les deux ensembles d'adresses sont en activité en réduisant la longueur de baux avant que vous apportiez la modification de sorte que tous les clients aient des baux de court-durée. Ceci s'assure qu'ils doivent renouveler leurs baux fréquemment et donc pour sélectionner un bail de la nouvelle gamme peu après que vous apportiez la modification. Soyez sûr de ne pas placer le short de durée de bail ainsi qui des baux épuisés tandis que vous cessez et mettez en marche

le serveur pour apporter la modification. Après que vous ayez apporté la modification, soyez sûr de restaurer la période d'origine de bail de sorte que vous n'augmentiez pas le chargement sur le serveur.

L'approche la plus efficace à résoudre des problèmes les évite. Après les recommandations tracées les grandes lignes ci-dessus garde vos administrateurs en accord avec votre exécution et te permet d'éviter des sérieux problème. Quand les problèmes apparaissent (comme des augmentations de temps d'attente E/S ou des augmentations d'utilisation de mémoire pour aucune raison connue), continuez avec les logs. Passez en revue les changements récents à votre environnement physique ou à configuration CNR pour voir si ce pourrait être la source des problèmes.

Les logs CNR sont vos amis. En commençant à utiliser le CNR, en promouvant le CNR, ou en changeant la configuration CNR, utilisez la commande de **grep** décrite pour vérifier les logs pour toutes les questions. Travaillez alors vers l'arrière dans le log pour comprendre quand et comment la question a surgi, et réparez le problème.

Actions immédiates en faisant face à un problème

- Ne redémarrez pas CMTS à moins que demandé de faire ainsi par le personnel de support de Cisco (s'applique aux environnements câblés seulement).
- Ne redémarrez pas le CNR à moins que demandé de faire ainsi par le personnel de support de Cisco.
- Ne désactivez pas le Basculement sûr à moins que demandé de faire ainsi par le personnel de support de Cisco.
- Ne rechargez pas, redémarrez, ou perturbez le CNR de quelque façon avec la resynchronisation sûre de Basculement en cours.
- Copiez les fichiers journal sur un répertoire où ils ne seront pas remplacés. Si le CNR tombait en panne, copiez le fichier image mémoire sur un répertoire où il ne sera pas remplacé.
- L'utilisez :`nrcmd> server dhcp getRelatedServers`pour isoler la mauvaise configuration sûre de Basculement.
- Regardez les logs pour des exceptions. Contrôle en particulier la séquence de lancement (ceci peut se produire dans un vieux log) : grep pour la « erreur », « avertissez », ou « connectez » (par exemple **erreur name_dhcp_1_log* de** grep-je**).**

Quand vous faites face à un problème, il est crucial que vous n'entraîniez aucun autre mal tout en isolant et réparant le problème initial. La réinitialisation d'un CMTS ou redémarrer le CNR crée les pics immédiats de chargement pendant un moment où le système est déjà fragile. L'objectif est d'avoir votre système entièrement - fonctionnel de nouveau pendant la période la plus courte. Le temps écoulé jusqu'à vos derniers comptes d'action ; le temps à votre première action ne compte pas. En d'autres termes, ne prenez pas une mesure rapide juste dans l'intérêt de l'action rapide. Pensez avant que vous agissiez.

Commencez un log de toutes les mesures prises et de tous les changements faits n'importe où du système : Serveurs DHCP, de DN, ou TFTP, et modifications apportées à tout CMTS ou modem câble. Décrivez le problème et le log, en détail, juste le comportement observable.

Analysez les fichiers journal

Collectez les logs (/var/nwreg2/logs). Analysez ces derniers, en recherchant des erreurs ou des avertissements. Employez un éditeur de texte pour analyser plus loin des erreurs d'intérêt. À partir

de l'erreur, le recherchez de retour dans le log pour toutes les entrées concernant l'adresse MAC, l'adresse IP, ou le nom de domaine associé avec l'erreur.

Vous pouvez devoir activer se connecter supplémentaire pour diagnostiquer des problèmes DHCP. Le serveur DHCP prend en charge une gamme étendue de capacités se connectantes. Référez-vous aux références de commandes CNR CLI pour une liste de se connecter des options et une explication de chacun. Faites attention, puisque chaque message de log place le chargement sur le serveur. Vous devez faire un compromis entre la quantité d'informations que vous demandez au CNR pour se connecter et à la performance des serveurs.

Vérifiez les problèmes de LDAP

Le problème peut être avec le serveur LDAP. Le CNR construit une file d'attente des demandes au serveur LDAP. Si le serveur LDAP ne peut pas suivre le chargement, la file d'attente s'accumule. Regardez dans le répertoire de /var/nwreg2/data/dhcpeventstore. Des fichiers de mémoire d'événement sont réparés dans la taille, ainsi si la file d'attente s'accumule, le CNR crée plus de fichiers. S'il y a plus d'un fichier dans le répertoire, ceci indique que la file d'attente sauvegarde. La même file d'attente est utilisée pour aligner des demandes au serveur DNS, ainsi si la file d'attente sauvegarde, et vous utilisez DDNS, il pourriez remplir de demandes au serveur DNS. Pour déterminer si le problème est avec le LDAP, activez se connecter supplémentaire d'interface de LDAP CNR. Activez les indicateurs de log LDAP-créer-**détail**, LDAP-requête-**détail**, et LDAP-mise à jour-**détail**. Le message de log incluent les groupes date/heure qui vous aident à déterminer si le LDAP est l'étranglement de système.

Vérifiez les bases de données internes du CNR

Si vous suspectez le problème peut être qu'un ou plusieurs des bases de données internes du CNR a perdu l'intégrité, se rapportent aux guides utilisateurs CNR pour apprendre comment exécuter les utilitaires de contrôle de validité de base de données. Si un de ces utilitaires indique un problème, continuez à suivre les directions dans les guides utilisateurs pour le résoudre.

Données de DN de contrôle avec le nslookup

Le nslookup de service est inclus avec des systèmes Unix Et avec Windows NT. Il peut être utilisé pour interroger un serveur DNS et est donc utile en vérifiant les données enregistrées par le serveur. La documentation pour votre système d'exploitation fournit les informations détaillées sur ses capacités.

Informations connexes

- Notes en tech de Network Registrar de Cisco CNS
- Support technique - Cisco Systems