Dispositif Cisco NAC (Clean Access) 4.x : Configurer les paramètres Syslog pour l'enregistrement des événements

Contenu

Introduction

Ce document décrit comment configurer les configurations de Syslog afin de se connecter les événements à un serveur externe dans l'appliance du Cisco Network Admission Control (NAC), autrefois connue sous le nom de Cisco Clean Access (CA).

Conditions préalables

Conditions requises

Ce document suppose que le gestionnaire de Cisco Clean Access (CAM) et des serveurs de Cisco Clean Access (CAS) sont installés et fonctionnent correctement.

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de Cisco NAC qui exécute la version de logiciel 4.0 et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Interprétation des journaux d'événements

Cliquez sur les **journaux d'événements** joignent dans le module de **surveillance** afin de visualiser l'événement basé sur Syslog ouvre une session la console d'admin. Il y a trois onglets de journaux d'événements :

- **Logs de vue**
- **Configurations de logs**
- **Configurations de Syslog**

Logs de vue

Figure 1
L'onglet de logs de vue inclut ces informations :

- Statistiques de système pour les serveurs de Clean Access, qui sont générés chaque heure par défaut.
- L'activité d'utilisateur, avec des temps de connexion d'utilisateur, des temps de déconnexion, a manqué des tentatives de connexion, et plus.
- Événements de configuration réseau, qui incluent des modifications au Contrôle d'accès au support (MAC) ou fonction émulation IP le répertorie, et ajout ou suppression des serveurs de Clean Access.
- Événements de gestion de la commutation pour hors bande (OOB), qui incluent quand des déroutements de linkdown sont reçus, et quand un port change en le RÉSEAU LOCAL virtuel authentique ou d'Access (VLAN).
- Modifications ou mises à jour aux contrôles de Clean Access, aux règles, et à l'antivirus/à liste des produits pris en charge d'AntiSpyware.
- Modifications à la configuration de Protocol de dynamic host configuration de Clean Access Server (DHCP).

Des statistiques de système sont générées pour chaque CAS géré par Clean Access Manager chaque heure par défaut. Voyez qu'en configurant la commande logging on de Syslog pour changer combien de fois les contrôles du système se produisent.

Remarque: Les événements les plus récents apparaissent d'abord dans la colonne d'événements.

Le tableau 1 décrit la navigation, des capacités de recherche, et le Syslog réel affiché sur la vue se connecte.

Tableau 1 :

	Colonne	Description
Navigation	**D'abord/précédent/ensuite/dernier**	Page de ces liens de navigation par le journal d'événements. Les événements les plus

		récents apparaissent d'abord dans la colonne d'événements. **Le dernier** lien t'affiche les événements les plus anciens dans le log. Un maximum de 25 entrées est affiché à une page.
	Colonne	Cliquez sur une en-tête des colonnes, telle que le type ou la catégorie, afin de trier le journal d'événements par cette colonne.
Critères de recherche	**Type**	La recherche par ces critères de colonne de type, et cliquent sur alors la **vue** : • En tapent • Panne • Les informations • Succès
	Catégorie	La recherche par ces critères de colonne de catégorie, et cliquent sur alors la **vue** : • Authentification [1] • Gestion • Client • Clean Access Server • Clean Access • SW_Management, si OOB est activé • Divers • DHCP
	Heure	La recherche par ces critères de temps, et cliquent sur alors la **vue** : • Dans un délai d'une heure • Dans un jour • Dans les deux jours • Dans un délai d'une semaine • Lorsque • Il y a une heure • Il y a un jour • Il y a deux jours • Il y a une semaine
	Recherche en texte de log	Tapez le texte désiré de recherche et cliquez sur la **vue**.
Contrôles	**Vue**	Après que les critères de recherche désirés soit choisis, cliquez sur la **vue** afin d'afficher les résultats.

	Remettez à l'état initial la vue	Si vous cliquez sur la **vue de remise**, elle restaure la vue par défaut, dans laquelle des logs dans un jour sont affichés.
	Effacement	Si vous cliquez sur Delete, il retire les événements filtrés à l'aide des critères de recherche à travers le nombre de pages applicables. L'effacement retire des événements filtrés de la mémoire de Clean Access Manager. Autrement, le journal d'événements persiste par l'arrêt normal du système. Utilisez l'indicateur d'événement de filtre affiché dans la figure 1 afin de visualiser le nombre total d'événements filtrés qui sont sujets à la suppression.
Affichage d'état	**Type**	• Alerte () = panne — indique une erreur ou un événement autrement inattendu • Indicateur vert () = succès — indique un événement réussi ou normal d'utilisation, tel que l'activité réussie de procédure de connexion et de configuration • Indicateur jaune () = les informations — indique les informations de performance du système, telles que les informations de chargement et l'utilisation de mémoire
	Catégorie	Indique le module ou le composant système qui ont initié l'événement de log. Pour une liste, référez-vous à la **catégorie** sous la section de critères de recherche. Notez que, par défaut, des statistiques de système sont générées chaque heure pour chaque Clean Access Server qui est gérée par Clean Access Manager.
	Heure	Affiche la date et l'heure (hh :

		millimètre : solides solubles) de l'événement, avec les événements les plus récents d'abord dans la liste.
	Événement	Affiche l'événement pour le module, avec les événements les plus récents répertoriés d'abord. Voir le tableau 2 - La colonne d'événement met en place pour un exemple d'un événement de Clean Access Server.

Notes de bas de page - Tableau 1

1 Les entrées d'authentication-type peuvent fournisseur inclure élément « : type> de <provider, Point d'accès : NON APPLICABLE, réseau : NON APPLICABLE. » Afin de continuer à fournir le support pour le client sans fil existant de la fin de vie (EOL), si actuel et préconfiguré dans le gestionnaire, le « Point d'accès : NON APPLICABLE, réseau : Les » champs NON-DÉTERMINÉ fournissent des informations de MAC et d'Identifiant SSID (Service Set Identifier) du Point d'accès (AP) respectivement pour le client existant.

Exemple de journal d'événements

Le tableau 2 explique l'exemple typique d'événement de santés de Clean Access Server :

```
CleanAccessServer 2006-04-03 15:07:53 192.168.151.55 System Stats:
 Load factor 0 (max since reboot: 9) Mem Total: 261095424 bytes Used: 246120448
 bytes Free: 14974976 bytes Shared: 212992 bytes Buffers: 53051392 bytes Cached:
 106442752 bytes CPU User: 0% Nice: 0% System: 97% Idle: 1%
```

Tableau 2 - Champs de colonne d'événement

Valeur	Description
`CleanAccessServer`	Clean Access Server signale l'événement
`2006-04-03 15:07:53`	Date et heure de l'événement
`192.168.151.55`	Adresse IP de signaler Clean Access Server
`Densité d'occupation 0`	La densité d'occupation indique le nombre de paquets qui attendent d'être traités par Clean Access Server, c.-à-d., le chargement en cours qui est manipulé par CAS. Quand la densité d'occupation se développe, c'est une indication que les paquets attendent dans la file d'attente à traiter. Si la densité d'occupation dépasse 500 pour n'importe quelle à période cohérente, telle que cinq minutes, ceci indique que Clean Access Server a une charge élevée régulière du trafic/de paquets d'arrivée. Soyez concerné si ce nombre grimpe jusqu'à 500 ou plus élevé.
`(maximum depuis`	Le nombre maximal de paquets dans la file d'attente en même temps. En d'autres termes,

<table>
<tr><td>la réinitialisation : <n>)</td><td>le chargement maximum manipulé par Clean Access Server.</td></tr>
<tr><td>Total de Mem : 261095424 octets
Utilisé : 246120448 octets
Libre : 14974976 octets
Partagé : 212992 octets
Mémoires tampons : 53051392 octets
Caché : 106442752 octets</td><td>Ce sont les statistiques d'utilisation de mémoire. Il y a six nombres affichés ici :
• mémoire totale
• mémoire utilisée
• mémoire disponible
• mémoire partagée
• mémoire tampon
• antémémoire</td></tr>
<tr><td>Utilisateur CPU : 0%
Gentil : 0%
Système : 97%
Inactif : 1%</td><td>Ces nombres indiquent le chargement de processeur CPU sur le matériel, dans les pourcentages. Ces quatre nombres indiquent le temps passé par le système dans l'utilisateur, gentil, le système, et les processus de veille.
Remarque: Le temps passé par la CPU dans le processus de système est en général plus grand que 90 pour cent sur Clean Access Server. Ceci indique un système sain.</td></tr>
</table>

Limitez le nombre d'événements loggés

Le seuil de journal d'événements est le nombre d'événements à enregistrer dans la base de données de Clean Access Manager. Le nombre maximal d'événements de log gardés sur le CAM, par défaut, est 100,000. Vous pouvez spécifier un seuil de journal d'événements de jusqu'à 200,000 entrées à enregistrer dans la base de données de CAM à la fois. Le journal d'événements est un log circulaire. Les entrées les plus anciennes sont remplacées quand le log passe le seuil de journal d'événements.

Afin de changer le nombre maximal d'événements :

1. Cliquez sur l'**onglet de configuration de logs** dans les pages de **surveillance > de journaux d'événements**.
2. Introduisez le nouveau nombre dans les domaines **maximum de journaux d'événements**.
3. Cliquez sur **Update**.

Configurez se connecter de Syslog

Des statistiques de système sont générées chaque heure, par défaut, pour chaque Clean Access Server qui est géré par Clean Access Manager. Par défaut, des journaux d'événements sont écrits au CAM. Vous pouvez réorienter des journaux d'événements de CAM à un autre serveur, tel que votre propre serveur de Syslog.

Supplémentaire, vous pouvez configurer combien de fois vous voulez que le CAM se connecte les informations d'état du système. Afin de faire ceci, placez la valeur dans le domaine d'**intervalle de log de santés de Syslog**. Le par défaut est de **60** minutes.

Afin de configurer se connecter de Syslog :

1. Choisissez la **surveillance > les journaux d'événements > les configurations de Syslog**.
2. Écrivez l'adresse IP du serveur de Syslog dans la zone adresse d'**adresse du serveur de Syslog**. Le par défaut est **127.0.0.1**.
3. Entrez dans le port pour le serveur de Syslog dans le domaine de **port de serveur de Syslog**. Le par défaut est **514**.
4. Entrez dans combien de fois vous voulez que le CAM se connecte les informations d'état du système, en quelques minutes, dans le domaine d'**intervalle de log d'états du système**. Le par défaut est de **60** minutes. Cette configuration détermine comment fréquemment des statistiques de CAS sont ouvertes une session le journal d'événements.
5. **Mise à jour de** clic afin de sauvegarder vos modifications.**Remarque:** Après que vous installiez votre serveur de Syslog dans le CAM, vous pouvez tester votre configuration. Afin de faire ceci, fermez une session et connectez-vous de nouveau dans la console d'admin de CAM. Ceci génère un événement de Syslog. Si l'événement de CAM n'est pas vu sur votre serveur de Syslog, assurez-vous que le serveur de Syslog reçoit le Protocole UDP (User Datagram Protocol) 514 paquets et qu'ils ne sont pas bloqués ailleurs sur votre réseau.**Remarque:** Configurer de plusieurs serveurs de Syslog n'est pas possible car il n'est pas pris en charge. Vous pouvez seulement expédier à un serveur de Syslog.

Fichiers journal

Le journal d'événements se trouve dans la table de base de données de Clean Access Manager et est nommé table de log_info. répertorie d'autres logins Clean Access Manager.

Tableau 3

Fichier	Description
`/var/log/messages`	Startup
`/var/log/dhcplog`	Relais DHCP, logs DHCP
`/tmp/perfigo-log0.log.*`	Le service de Perfigo se connecte pour 3.5(4) et plus tôt [1]
`/perfigo/logs/perfigo-log0.log.*`	Le service de Perfigo se connecte pour 3.5(5) et plus tard [1,2]
`/perfigo/logs/perfigo-redirect-log0.log.0`	erreurs liées au certificat de connexion CAM/CAS
`/var/nessus/logs/nessusd.messages`	Logs embrochables de test de Nessus

`/perfigo/control/apache/logs/*`	Certificats de la couche de sockets de sécuriser (SSL), journaux des erreurs d'Apache
`/perfigo/control/tomcat/logs/localhost *.`	Tomcat, réorientent, JavaServer pagine les logs (JSP)
`/var/log/ha-log`	Haute disponibilité de logs pour le CAM et le CAS

Notes de bas de page - Tableau 3

1. 0 au lieu de * affiche le log le plus récent.

2. Des événements de gestion de la commutation pour des notifications reçues par le CAM des Commutateurs sont écrits seulement aux logins le système de fichiers (/perfigo/logs/perfigo-log0.log.0). En outre, ces événements sont écrits au disque seulement quand le niveau de log est placé aux INFORMATIONS ou plus correct.

Informations connexes

- Page de support d'appareils de Cisco NAC
- Support et documentation techniques - Cisco Systems