Contenu

Introduction

Ce document fournit les pratiques recommandées pour administrer (CS) l'ACS Cisco Secure pour l'application UNIX. Les recommandations présentées dans ce document sont basées sur des expériences de conception et de déploiement par les ingénieurs de développement de Cisco (De).

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- configurant et gérant le CS ACS pour l'UNIX

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 2.3(5) du CS ACS UNIX

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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Liste des pratiques recommandées

Est ci-dessous une liste des pratiques recommandées recommandées.

Étapes

Procédez comme suit :

1. Assurez-vous que la base de données SQLAnywhere ne dépasse pas 5000 profils utilisateurs.
2. Les enregistrements des comptes ne devraient pas dépasser 50,000 enregistrements dans les tables de comptabilité.
3. Exécutez le journal d'utilitaire d'AcctExport.
4. Si le débit de transaction est très élevé, et il y a du trafic énorme de comptabilité tels qu'il y a plus de 50,000 enregistrements des comptes, alors exécutez AcctExport deux fois ou trois fois basé sur le chargement.
5. Assurez-vous qu'il y a disque adéquat et espace de swapping disponible sur le boîtier Solaris.
6. Exécutez le mensuel d'utilitaire de dbunload. Ceci aidera à réduire la taille de la base de données de CSUnix.
7. Le csecure.db devrait ne jamais dépasser 1 Go d'espace disque.
8. Si le csecure.db dépasse dans la taille très rapidement, alors assurez-vous que le dbunload est exécuté plus fréquemment.
9. Si l'AAA de rayon n'est pas utilisé en CS, est-ce qu'alors ceci peut être désactivé avec l'aide de ? Indicateur R dans /etc/rc2.d/S80Ciscosecure.
10. Au délai d'exécution, des erreurs de DBServer, y compris les erreurs produites dans l'interface à la base de données, sont signalées dans les fichiers journal/le fichier <date> de csdb_. N'importe quelles erreurs ou informations inattendues de crash de Java Virtual Machine sont fichier ouvert une session du log/dbserver.log. Vérifiez ces fichiers pour toutes les erreurs.
11. Si l'AAAServer tombe en panne, les fichiers image mémoire veulent se trouvent dans le $BASEDIR/corefiles. Vérifiez l'existence des fichiers image mémoire éventuels.
12. Sauvegarde la base de données régulièrement (quotidien ou hebdomadaire), basé sur les besoins des clients.
13. Pour une meilleure représentation, désactivez la fonctionnalité de journalisation de csuslog. Ceci augmentera rigoureusement la représentation.
14. La valeur d'ulimit devrait être 4096 dans /etc/system, /etc/rc2.d/S80Ciscosecure $BASEDIR/bin/DBServer.sh
15. Retirez csecure.log régulièrement. Avant de retirer csecure.log, le CS devrait être arrêté.
16. Manuellement n'ajoutez pas/modifiez/effacement les tables de base de données directement - utilisez seulement les méthodes prises en charge.
17. Archivez le répertoire $BASEDir/logfiles une fois par mois.
18. Archivez les fichiers de /var/log/csuslog régulièrement, et équilibrez la taille en émettant le **cat /dev/null > csuslog de** commande. Si le fichier est supprimé, le Syslog ne fonctionnera pas, et par conséquent le log ne sera pas réorienté au fichier de csuslog.
19. Questions de serveur DNS : Si le système cible a des DN configurés, ou si le système d'exploitation solaris a été configuré en tant que serveur DNS, le soin particulier doit être pris pour assurer que la représentation et les exécutions de DN sont complètement opérationnelles.Si le système Solaris de cible de serveur ACS de CS a des DN activés, il pourrait y avoir des questions de représentation ou d'authentification pour le CS ACS. Le CS ACS n'appelle pas directement un serveur DNS ; cependant, les appels de système d'exploitation solaris ? gethostbyadd_r ? et pourrait indirectement appeler le serveur DNS,

si configuré pour faire ainsi. Vérifiez le fichier de /etc/nsswitch.conf pour une telle configuration. Si l'exécution de résolution de nom de domaine de DN ne fonctionne pas ou est lente, ceci affecte directement le CS ACS.

20. Tout en exécutant des outils tels que le dbbackup et le dbunload, le CHEMIN devrait être correctement placé. Autrement, les outils peuvent ne pas fonctionner correctement. $BASEDIR/utils/bin/env_setup peut être utilisé pour placer le chemin. Ce fichier contient toutes les variables environnementales exigées et d'autres détails de chemin.
21. Les paramètres de MaxConnection et de ConnectionLicense devraient être placés afin de répondre aux besoins basés sur le nombre d'authentifications et le nombre de transactions que le CSU peut manipuler. MaxConnection peut être placé à une valeur maximum de 50, si le DB utilisé est SqlAnyWhere. Augmentez le ConnectionLicense dans $BASEDIR/config/CSConfig.ini, et augmentez également la valeur de MaxConnection dans $BASEDIR/CSU/libdb.conf à une valeur deux moins que le ConnectionLicense basé sur le chargement.
22. En employant les scripts automatisés pour ouvrir une session aux Routeurs et aux Commutateurs, et pour exécuter des commandes, routeur régulier intermédiaire/commandes du commutateur de commandes de **sommeil d'**endroit d'il est conseillé de. Ceci aide se propage le chargement et évite des conflits de ressource dans le serveur de CS.
23. De plus, ces scripts automatisés devraient correctement clôturer des sessions de telnet (même dans le cas de toutes pannes de commande) pour assurer des ressources ne sont pas verrouillés au serveur de CS.

Informations connexes

- CiscoSecure ACS pour l'UNIX, 2.3(5) documentation technique
- Support produit de Cisco Secure Access Control Server pour Unix
- Support et documentation techniques - Cisco Systems