Configuration de l'authentification des requêtes HTTP avec CE exécutant ACNS 5.0.1 et Microsoft Active Directory

Contenu

Introduction

Cette configuration d'échantillon t'affiche que comment installer un Cisco Content Engine pour exécuter une recherche de base de données de Protocole LDAP (Lightweight Directory Access Protocol) de Répertoire actif pour laisser/limitez les utilisateurs pour accéder à des ressources web.

Une base de données de Répertoire actif est une base de données utilisateur d'un serveur de Windows 2000. Cette base de données peut être questionnée pour l'authentification par des protocoles de LDAP. Typiquement, un client satisfait de LDAP d'engine questionne la base de données utilisateur d'un serveur LDAP et obtient les qualifications de l'utilisateur, telles que l'expiration du compte d'utilisateur, des privilèges, et les groupes auxquels l'utilisateur appartient. En application de Cisco et logiciel 5.0 du système de Réseau de diffusion de contenu (ACNS), on permet également au le client satisfait de LDAP d'engine pour authentifier et autoriser un utilisateur configuré dans un Répertoire actif distant dans une base de données du serveur de Windows 2000.

Pour utiliser le Répertoire actif de Miscrosoft en tant que serveur LDAP pour l'authentification avec l'engine satisfaite, il y a un certain spécifique fait un pas vous doit prendre. Par défaut, la Microsoft Active Directory ne permet pas des requêtes anonymes de LDAP. Pour faire des requêtes de LDAP ou parcourir le répertoire, un client de LDAP doit lier au serveur LDAP utilisant le nom unique (DN) d'un compte qui appartient au groupe d'administrateur du système Windows.

Pour installer la Microsoft Active Directory en tant que votre serveur LDAP, vous devez déterminer le pleins DN et mot de passe d'un compte dans le groupe d'administrateurs. Par exemple, si l'administrateur de Répertoire actif crée un compte dans le répertoire d'utilisateurs des utilisateurs

de Répertoire actif et panneau de configuration de Windows Nt/2000 d'ordinateurs et le domaine de DN est sns.cisco.com, le DN en résultant a la structure suivante : cn=<adminUsername>, cn=users, dc=sns, dc=cisco, dc=com

Le LDAP a été inventé pour préserver les meilleures qualités offertes par X.500 tout en réduisant les frais d'administration. Le LDAP fournit un Directory Access Protocol ouvert s'exécutant au-dessus du TCP/IP. Il retient le modèle de données X.500 et il est extensible à une taille globale et aux millions d'entrées pour un investissement modeste en matériel et infrastructure réseau. Le résultat est une solution globale de répertoire qui est assez abordable pour être utilisée par les petits organismes, mais qui peut également être mesuré pour prendre en charge le plus grand des entreprises.

Une engine LDAP-activée de moteur de cache/contenu authentifie des utilisateurs avec un serveur LDAP. Avec une requête de HTTP, l'engine satisfaite obtient un ensemble de qualifications de l'utilisateur (user-id et mot de passe), et les compare contre ceux dans un serveur LDAP. Quand l'engine satisfaite authentifie un utilisateur par le serveur LDAP, un enregistrement de cette authentification est enregistré localement dans la RAM satisfaite d'engine (cache d'authentification). Tant que l'entrée d'authentification est gardée, les tentatives ultérieures d'accéder au contenu Internet restreint par cet utilisateur n'exigent pas des consultations de serveur LDAP. Le par défaut est de 480 minutes, le minimum est de 30 minutes, et le maximum est de 1440 minutes (24 heures). C'est l'intervalle de temps entre le dernier accès Internet de l'utilisateur et la suppression de cette entrée d'utilisateur du cache d'autorisation, forçant la ré-authentification avec le serveur LDAP.

L'authentification LDAP de supports de moteur de cache pour le mode proxy et l'accès transparent du mode (WCCP). Dans le mode proxy, le moteur de cache utilise l'ID utilisateur du client comme clé pour la base de données d'authentification, alors qu'en mode transparent, le moteur de cache utilise l'adresse IP du client comme clé pour la base de données d'authentification. Le moteur de cache emploie l'authentification (nonencrypted) simple pour communiquer avec le serveur LDAP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Cisco Content Engine 7325 ACNS s'exécutant 5.0.1
- Le Microsoft Windows 2000 avance le serveur avec le Répertoire actif

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.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

Cisco Content Engine 7325 (version de logiciel 5.0.1 de Cisco ACNS)

```
hostname V5CE7325
!
!
http authentication cache timeout 5
http proxy incoming 80 8080
!
ip domain-name cisco.com
!
interface GigabitEthernet 1/0
 ip address 10.48.67.23 255.255.254.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
ip default-gateway 10.48.66.1
!
primary-interface GigabitEthernet 1/0
!
!
no auto-register enable
!
!
multicast accept-license-agreement
!
!
ip name-server 10.48.66.123

username admin password 1 CfxnDoKDWrBds
username admin privilege 15
!

ldap server base "dc=sns,dc=cisco,dc=com"
 !--- This is the base DN of the starting point for !---
the search in the LDAP database. ldap server userid-
attribute cn !—-- Searching for the CN of the user. ldap
server host 10.48.66.217 primary !--- The LDAP server's
IP address number. ldap server administrative-dn
"cn=Administrator,cn=users,dc=sns,dc=cisco,dc=com" !---
This is the DN of the admin user. ldap server
administrative-passwd **** !--- This is the password for
```

```
the admin-user. ldap server version 3 !—-- Use LDAP
version 3 for active directory. ldap server active-
directory-group enable !—-- Allows users based on their
group memberships. ldap server enable ! authentication
login local enable primary authentication configuration
local enable primary ! access-lists 300 permit groupname
internet access-lists 300 deny groupname any !—--
Defines what user groups are allowed. ! access-lists
enable ! ! cdm ip 10.48.67.25 cms enable ! ! end
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **show ldap** — Cette commande montre les détails de la configuration. L'exemple de sortie de commande est affiché ci-dessous.

```
Allow mode:     disabled
Base DN:        dc=sns,dc=cisco,dc=com
Filter:         <none>
Retransmits:    2
Timeout:        5 seconds
UID Attribute:  cn
Group Attribute:         memberOf
Administrative DN:       cn=Administrator,cn=users,dc=sns,dc=cisco,dc=com
Administrative Password: ****
LDAP version:   3
LDAP port:      389
Server            Status
---------------   ---------
10.48.66.217      primary
<none>            secondary
```

- **show access-lists** — Cette commande montre le Listes de contrôle d'accès (ACL) qui sont activés.
- **HTTP-authcache d'exposition** — Cette commande affiche le cache d'authentification. L'exemple de sortie de commande est affiché ci-dessous.

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

- **mettez au point le suivi d'en-tête de https** — Cette commande te permet pour visualiser et dépanner la demande reçue par l'engine satisfaite.
- **HTTP-demande de debug authentication** — Cette commande te permet pour visualiser et dépanner la procédure d'authentification. Des exemples de sortie de commande sont affichés ci-dessous.**Authentification réussie**

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
```

```
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

Demande défectueuse quand l'utilisateur n'est pas un membre de groupe Internet

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

Demande défectueuse quand l'utilisateur n'existe pas dans la base de données de LDAP

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Centre de logiciel réseau de Réseau de diffusion de contenu (clients enregistrés seulement)
- Support et documentation techniques - Cisco Systems