Configuración de la autenticación de petición HTTP utilizando CE con ACNS 5.0.1 y Microsoft Active Directory

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Configurar](#)
[Configuraciones](#)
[Verificación](#)
[Troubleshooting](#)
[Información Relacionada](#)

Introducción

Esta configuración de muestra le explica cómo configurar un Motor de contenido de Cisco para realizar una búsqueda en la base de datos del Protocolo ligero de acceso a directorios (LDAP) de Active Directory y permitir/restringir el acceso de usuarios a los recursos de Web.

Una base de datos del Active Directory es una base de datos de usuarios de a Windows 2000 Server. Esta base de datos puede consultarse con fines de autenticación mediante protocolos LDAP. Generalmente, un cliente LDAP motor de contenido solicita una base de datos de usuarios del servidor LDAP y obtiene las credenciales del usuario, como el vencimiento de la cuenta del usuario, los privilegios y los grupos a los que el usuario pertenece. En el software Cisco Application y Content Networking System (ACNS) 5.0, el cliente Motor de contenidos LDAP también puede autenticar y autorizar a un usuario configurado en un Directorio activo remoto dentro de una base de datos del servidor Windows 2000.

Para utilizar Microsoft Active Directory como el servidor LDAP para la autenticación con el motor de contenido, debe seguir algunos pasos específicos. Por abandono, el Microsoft Active Directory no permite las interrogaciones anónimas LDAP. Para hacer las interrogaciones LDAP u hojear el directorio, un cliente LDAP debe atar al servidor LDAP que usa el Nombre distintivo (DN) de una cuenta que pertenezca al Grupo del administrador del Sistema Windows.

Para configurar Microsoft Active Directory como el servidor LDAP, necesita determinar el DN completo y la contraseña de una cuenta en el grupo Administrators (administradores). Por ejemplo, si el administrador del Active Directory crea una cuenta en la carpeta del usuario del panel de control de Windows Nt/2000 de los usuarios de directorio activo y computadora y el dominio DNS es sns.cisco.com, el DN resultante tiene la estructura siguiente:

cn=<adminUsername>, cn=users, dc=sns, dc=cisco, dc=com

LDAP fue inventado para preservar las más mejores cualidades ofrecidas por X.500 y al mismo tiempo reducir los costos administrativos. LDAP ofrece un protocolo de acceso libre al directorio que se ejecuta sobre TCP/IP. Conserva el modelo de datos X.500 y se puede ampliar a un tamaño global y a millones de entradas para una inversión moderada en la infraestructura de hardware y de red. El resultado es una solución de directorio global lo suficientemente accesible como para ser utilizada por pequeñas organizaciones, pero con capacidad de ampliación para empresas de mayor tamaño.

Un motor caché habilitado para LDAP / Content Engine autentica a los usuarios con un servidor LDAP. Con una consulta HTTP, Content Engine obtiene credenciales del usuario (identificación y contraseña de usuario) y la compara con las del servidor LDAP. Cuando el Content Engine autentica a un usuario a través del servidor LDAP, un expediente de esa autenticación se salva localmente en el RAM del Content Engine (caché de la autenticación). Mientras que se mantenga la entrada de autenticación, los intentos subsecuentes para acceder al contenido restringido de Internet por parte de ese usuario no requieren la búsqueda de servidores LDAP. El valor predeterminado es 480 minutos, el mínimo es 30 minutos y el máximo es 1440 minutos (24 horas). Es un intervalo de tiempo entre el último acceso del usuario a Internet y el retiro de la entrada de ese usuario del caché de autorización forzándolo a la reautenticación con el servidor LDAP.

El motor de la memoria caché admite la autenticación LDAP para el acceso en modo proxy y en modo transparente (WCCP). En el modo de representación, el motor del caché utiliza el userid del cliente como clave para la base de datos de autenticación, mientras que en el modo transparente, el motor del caché utiliza la dirección IP del cliente como clave para la base de datos de autenticación. El Cache Engine utiliza una autentificación simple (no cifrada) para comunicarse con el servidor LDAP.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Motor de contenido de 7325 de Cisco que ejecuta ACNS 5.0.1
- El Microsoft Windows 2000 avanza el servidor con el Active Directory

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las

convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Configuraciones

Motor de contenido Cisco 7325 (versión 5.0.1 del software ACNS de Cisco)

```
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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **ldap de la demostración** — Este comando muestra los detalles de la configuración. A continuación, se incluye un resultado de ejemplo del comando

```
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
```

- **listas de acceso de la demostración** — Este comando muestra el Listas de control de acceso (ACL) se habilita que.
- show http-authcache: este comando muestra la memoria caché de autenticación. A continuación, se incluye un resultado de ejemplo del comando

```
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
```

- debug https header trace - este comando le permite visualizar y resolver los problemas relativos a la solicitud recibida por el Content Engine (Motor de contenido).
- debug authentication http-request: este comando permite consultar y solucionar problemas del proceso de autenticación. Las salidas del comando de ejemplo se muestran a continuación.**Autenticación exitosa**

```
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
```

Solicitud fallida cuando el usuario no es un miembro del grupo de 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
```

Fallo de solicitud cuando el usuario no existe en la base de datos 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
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Centro del software de Content Networking (sólo para clientes registrados)
- Soporte Técnico y Documentación - Cisco Systems