Configurando a Autenticação de Requisições HTTP com o CE Executando o ACNS 5.0.1 e o Microsoft Active Directory

Índice

Introdução

Esse exemplo de configuração mostra como configurar um Cisco Content Engine para executar uma pesquisa de banco de dados do protocolo LDAP, a fim de permitir/restringir o acesso dos usuários aos recursos da web.

Um base de dados do diretório ativo é uma base de dados de usuário de um servidor do Windows 2000. Esse banco de dados pode ser consultado para fins de autenticação pelos protocolos LDAP. Geralmente, um cliente de LDAP do Content Engine consulta um banco de dados de usuário do servidor LDAP e obtém as credenciais de usuário, como os privilégios de vencimento de conta de usuário, e grupos aos quais o usuário pertence. No software Cisco Application and Content Networking System (ACNS) 5.0, o cliente LDAP Content Engine também pode autenticar e autorizar um usuário configurado em um Active Directory remoto de um banco de dados de servidor Windows 2000.

Para usar o Microsoft Active Directory como o servidor LDAP para autenticação com o Content Engine, existem alguns passos específicos que devem ser executados. À revelia, o microsoft ative directory não permite perguntas anônimas LDAP. Para fazer perguntas LDAP ou consultar o diretório, um cliente de LDAP deve ligar ao servidor ldap usando o nome destacado (DN) de uma conta que pertença ao grupo de administrador do sistema Windows.

Para definir o Microsoft Active Directory como seu servidor LDAP, é necessário determinar o DN completo e a senha de uma conta no grupo de Administradores. Por exemplo, se o administrador do diretório ativo cria uma conta na pasta de usuários dos usuários de diretório ativo e Control Panel de Windows Nt/2000 dos computadores e o domínio de DNS são sns.cisco.com, o DN resultante tem a seguinte estrutura: cn=<adminUsername>, cn=users, dc=sns, dc=cisco, dc=com

O LDAP foi criado para preservar as melhores qualidades oferecidas pelo X.500, ao mesmo tempo em que reduz os custos administrativos. O LDPA oferece um protocolo de acesso de diretório aberto em execução sobre TCP/IP. Mantém o modelo de dados X.500 e é escalonável para um tamanho global e milhões de entradas para um investimento modesto em hardware e infra-estrutura de rede. O resultado é uma solução de diretório global acessível o suficiente para ser usada por pequenas organizações, mas que também pode ser escalonada para suportar a maior das empresas.

Um Cache Engine/Content Engine habilitado para LDAP autentica os usuários por meio de um servidor de LDAP. Com uma consulta HTTP, o Content Engine obtém um conjunto de credenciais do usuário (ID de usuário e senha) e as compara com as do servidor LDAP. Quando o Content Engine autentica um usuário através do servidor ldap, um registro dessa autenticação está armazenado localmente no Content Engine RAM (esconderijo da autenticação). Enquanto a entrada de autenticação é mantida, as tentativas subseqüentes de acesso a conteúdo restrito de Internet por tal usuário não exigem pesquisas de servidor LDAP. O padrão é 480 minutos, o mínimo é 30 minutos e o máximo é 1.440 minutos (24 horas). Esse é o intervalo de tempo entre o último acesso à Internet do usuário e a remoção da entrada desse usuário do cache de autorização, forçando a reautenticação com o servidor LDAP.

O Mecanismo de Cache suporta a autenticação LDAP para o modo de proxy e o acesso ao modo transparente (WCCP). No modo de proxy, o motor do esconderijo usar o userid do cliente como uma chave para a base de dados de autenticação, quando no modo transparente, o motor do esconderijo usa o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente como uma chave para a base de dados de autenticação. O Cache Engine utiliza a autenticação simples (não criptografada) para comunicar-se com o servidor de LDAP.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Content Engine 7325 executando ACNS 5.0.1
- O Microsoft Windows 2000 avança o server com diretório ativo

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Configurações

Cisco Content Engine 7325 (versão do software Cisco ACNS 5.0.1)

```
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
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **ldap da mostra** — Este comando mostra os detalhes da configuração. A saída de exemplo de comando está mostrada abaixo.

```
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 acesso da mostra** — Este comando mostra o Access Control Lists (ACLs) que é permitido.
- show http-authcache esse comando exibe o cache de autenticação. A saída de exemplo de comando está mostrada abaixo.

```
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 - esse comando permite exibir e solucionar o problema de solicitação recebida pelo Content Engine.
- debug authentication http-request - Este comando permite que você exiba e faça Troubleshooting do processo de autenticação. Os exemplos de saída de comando são mostrados a seguir.**Autenticação bem sucedida**

```
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
```

Falha da requisição quando o usuário não for um membro do 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
```

A solicitação falha quando o usuário não existe no banco de dados 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Centro de software de rede de conteúdo (somente clientes registrados)
- Suporte Técnico e Documentação - Cisco Systems