配置HTTP请求认证使用运行ACNS 5.0.1和Microsoft Active Directory的CE

目录

简介

此配置示例显示您如何设置Cisco内容引擎执行活动目录轻量级目录访问协议(LDAP)数据库查寻准许/请限制用户访问Web资源。

活动目录数据库是Windows 2000服务器的用户数据库。此数据库可以由LDAP协议为认证的目的查询。一般，内容引擎LDAP客户端查询LDAP服务器的用户数据库并且获取用户凭据，例如用户帐户有效期，权限和的组用户属于。在Cisco应用和内容联网系统(ACNS) 5.0软件方面，内容引擎LDAP客户端也允许验证和授权在一远程活动目录的一个用户配置的在Windows 2000服务器数据库。

要使用Miscrosoft活动目录作为LDAP服务器验证与内容引擎，有您必须采取的一些特定步骤。默认情况下， Microsoft Active Directory不允许匿名LDAP查询。要做LDAP查询或浏览目录， LDAP客户端必须绑定到LDAP服务器使用属于windows系统的管理员组帐户的特有名(DN)。

要设置Microsoft Active Directory作为您的LDAP服务器，您需要确定一个帐户的全双工DN和密码在管理员组的。例如，如果活动目录管理员创建在激活目录用户和计算机Windows NT/2000控制面板的用户文件夹的一个帐户，并且DNS域是sns.cisco.com，发生的DN有以下结构：cn=<adminUsername>， cn=users， dc=sns， dc=cisco， dc=com

LDAP被发明保留X.500提供的最好的质量，当降低管理开销时。LDAP提供运行TCP/IP的一个开放目录访问协议。它保留X.500数据模型，并且是可扩展对一个全局大小和数百万条目一次普通的投资的在硬件和网络基础设施。结果是足够价格合理由小组织使用，但是能也被扩展支持最大企业的全球目录解决方案。

一支持LDAP的Cache Engine/内容引擎验证用户用LDAP服务器。使用HTTP查询，内容引擎从用户获取一套凭证(用户ID和密码)，并且对那些比较他们在LDAP服务器。当内容引擎通过LDAP服务器时验证用户，该验证记录在内容引擎RAM (验证缓存)存储本地。只要验证条目保持，随后的尝试由

该用户访问限制互联网内容不要求LDAP服务器查找。默认是480分钟，最低是30分钟，并且最大数量是1440分钟(24个小时)。这是在用户的最后该用户输入之间互联网访问和删除的时间间隔从授权缓存，强制再验证用LDAP服务器。

Cache Engine支持代理模式和透明(WCCP)模式访问的LDAP认证。在代理模式， Cache Engine使用客户端的userid作为密钥身份验证数据库，而在透明模式， Cache Engine使用客户端IP地址作为密钥身份验证数据库。Cache Engine使用简单(非加密的)验证与LDAP服务器联络。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco内容引擎7325运行的ACNS 5.0.1
- Microsoft Windows 2000提前有活动目录的服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置

Cisco内容引擎7325 (Cisco ACNS软件版本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
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **show ldap** —此命令显示配置的详细信息。示例命令输出如下所示。

```
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** —此命令显示启用的访问控制列表(ACL)。
- **show http-authcache** —此命令显示验证缓存。示例命令输出如下所示。

```
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** —此命令允许您查看和排除故障内容引擎接收的请求。
- **debug authentication http-request** —此命令允许您查看和排除故障认证过程。示例命令输出如下所示。**成功认证**

```
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
```

失败的请求，当用户不是互联网组的成员

```
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
```

失败的请求，当用户在LDAP数据库不存在

```
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
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 内容网络软件中心(注册用户)
- 技术支持和文档 - Cisco Systems