Настройка аутентификации запросов HTTP при помощи CE Running ACNS 5.0.1 и Microsoft Active Directory

Содержание

Введение

В данном примере конфигурации описано настройку модуля содержимого Cisco для выполнения поиска в базе данных протокола LDAP для предоставления или ограничения доступа пользователей к веб-ресурсам.

База данных Active Directory является базой данных пользователей Сервера Windows 2000. Протоколы LDAP могут послать к данной базе запросы в целях проверки подлинности. Обычно клиент модуля содержимого LDAP запрашивает базу данных пользователя сервера LDAP и получает учетные данные пользователя, такие как срок действия записи пользователя, привилегии и группы, к которым принадлежит пользователь. В программном обеспечении Cisco Application and Content Networking System (ACNS) 5.0 клиенту Content Engine LDAP также разрешено выполнять аутентификацию и авторизацию пользователя, включенного в удаленный каталог Active Directory в базе данных сервера Windows 2000.

Чтобы использовать Miscrosoft Active Directory в качестве сервера LDAP для проверки подлинности на Content Engine, необходимо выполнить следующие действия. По умолчанию Microsoft Active Directory не позволяет анонимные запросы LDAP. Чтобы сделать запросы LDAP или просмотреть каталог, клиент LDAP должен связать с Сервером LDAP с помощью Составного имени (DN) учетной записи, которая принадлежит Группе администраторов Системы Windows.

Чтобы настроить Microsoft Active Directory в качестве сервера LDAP, необходимо определить полное DN и пароль учетной записи группы "Администраторы". Например, если администратор Active Directory создает учетную запись в Папке Пользователи Windows NT Пользователей и компьютеров Active Directory/2000 панель управления, и Домен DNS

является sns. cisco . com, получающийся DN имеет следующую структуру: cn=<adminUsername>, cn=users, dc=sns, dc=cisco, dc=com

Облегченный протокол службы каталогов введен для сохранения лучших характеристик, предлагаемых X 500 и сокращения административных расходов. LDAP – это облегченный протокол доступа к каталогам по каналам TCP/IP. Он поддерживает модель данных X.500 и он масштабируем до глобального размера и миллионов записей при скромном инвестировании в оборудование и сетевую инфраструктуру. В результате получается решение для глобального каталога, достаточно доступное по цене для малого бизнеса, и в то же время масштабируемое настолько, что его могут использовать самые крупные предприятия.

Cache Engine с включенным LDAP / Content Engine проверяет пользователей с помощью LDAP-сервера. С помощью запроса HTTP Content Engine получает набор учетных данных от пользователя (идентификатор и пароль) и сравнивает их с данными на LDAP-сервере. Когда Модуль контента аутентифицирует пользователя через Сервер LDAP, запись той аутентификации сохранена локально в ОЗУ Модуля контента (опознавательный кэш). На время хранения записи проверки последующие попытки доступа к запрещенному содержимому Интернета этим пользователем не требуют поисков сервера LDAP. Значение по умолчанию составляет 480 минут, минимальное – 30 минут, а максимальное – 1440 минут (24 часа). Это временной интервал между последним доступом пользователя в сеть Интернет и удалением записи об этом пользователе из кэша авторизации, принуждающий к повторной аутентификации с помощью сервера LDAP.

Cache Engine поддерживает аутентификацию LDAP при доступе в режиме прокси и прозрачном режиме (WCCP). В то время как в прозрачном режиме, Cache Engine использует IP-адрес клиента в качестве ключа для базы данных проверки подлинности, в режиме proxy Cache Engine использует идентификатор пользователя клиента в качестве ключа для базы данных проверки подлинности. Устройство Cache Engine использует простую аутентификацию (без шифрования) для взаимодействия с сервером LDAP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Процессор содержимого Cisco 7325, использующий ACNS 5.0.1
- Сервер усовершенствования Microsoft Windows 2000 с Active Directory

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Конфигурации

Cisco Content Engine 7325 (программное обеспечение Cisco ACNS версии 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
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **show ldap** — Эта команда показывает подробные данные конфигурации. Ниже представлен пример выходных данных команды.

```
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** команда показывает Списки контроля доступа (ACL), которые включены.
- **show http-authcache – данная команда отображает кэш проверки подлинности.** Ниже представлен пример выходных данных команды.

```
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 - данная команда позволяет просматривать и устранять ошибки запроса, полученного модулем содержимого.**
- **debug authentication http-request – Позволяет наблюдать процесс аутентификации и устранять его неполадки.** Примеры выходов команд приведены ниже.**Успешная аутентификация**

```
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
```

Запрос не выполнен, так как пользователь не является членом группы Интернета

```
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
```

Запрос, не выполненный по причине не существования пользователя в базе данных 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
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Центр программного обеспечения для Управления Контентом
- Cisco Systems – техническая поддержка и документация