Contents

Introduction

External user database configuration (WINDOWS) with ACS 4.2 + Router config

Design

External User Database Authentication Process

When ACS attempts user authentication with an external user database, it forwards the user credentials to the external user database. The external user database passes or fails the authentication request from ACS. On receiving the response from the external user database, ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the external user database.

end user---------->>>>>>>>>> AAA client (switch/router/AP/ASA)---------->>>>>>>>>>>>ACS 4.2

Configuration on ACS

Configuring a Windows External User Database

To configure ACS to authenticate users against the Windows user database in the trusted domains of your network:

Step 1 click External User Databases.

Step 2 Click Database Configuration.

ACS will show all possible external user database types.

Step 3 Click Windows Database.

If no Windows database configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 4 Click Configure.

Step 5 As needed, configure the options in:

?Dialin Permission

?Windows Callback

?Unknown User Policy

?Domain List

?MS-CHAP Settings

?Windows EAP Settings

?Windows Authentication Configuration

It helps in configuring a workstation name for ACS authentications to the Windows Active Directory.

?Default: "CISCO"?Choose f you want CISCO as the workstation name.

?Local: machine-name?Choose it if you want to use your local machine name as the workstation name.

?User defined workstation name?Choose if you have defined your own workstation name.

Step 6 Click Submit.

== Concept of Authentication with Windows User Databases ==

ACS forwards user credentials to a Windows database by passing the user credentials to the Windows operating system of the computer that is running ACS for Windows or the Solution Engine remote agent. The Windows database passes or fails the authentication request from ACS.

ACS for Windows only: When receiving the response from the Windows database agent ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the Windows database.

Solution Engine only: When receiving the response from the Windows database, the remote agent forwards the response to ACS, and ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the Windows database.

ACS grants authorization based on the ACS group to which the user is assigned. While you can determine the group to which a user is assigned information from the Windows database, it is ACS that grants authorization privileges.

To further control access by a user, you can configure ACS to also check the setting for granting dial-in permission to the user. This setting is labeled Grant dialin permission to user in Windows NT and Allow access in the Remote Access Permission area in Windows 2000 and Windows 2003 R2. If this feature is disabled for the user, access is denied; even if the username and password are typed correctly.

Configuration on ROUTER

Configure AAA Authentication for Login and authorization for exec

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the login authentication command in line configuration mode. AAA services must also be configured.

Configuration Procedure In this example, the router is configured to retrieve users' passwords from a TACACS+ server when users attempt to connect to the router.

From the privileged EXEC (or "enable") prompt, enter configuration mode and enter the commands to configure the router to use AAA services for authentication:

```
       router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login default  group tacacs+ local
router(config)#aaa authorization exec default group tacacs if-authenticated
router(config)#tacacs-server host 192.168.1.1
router(config)#tacacs-server key cisco
```

```
Switch to line configuration mode using the following commands. Notice that the prompt changes to
```

```
router(config)#line vty 0 4
router(config-line)#
 router(config-line)#login authentication default
 router(config-line)# authorization exec default
```

Note: By default IOS device works on default method list, You only need to define login authentication or exec authorization under line method, when using named method list.

```
Exit configuration mode.
```

```
router(config-line)#end
router#
```

Show running-config

Verify the Configuration

Examine the configuration of the router to verify that the commands have been properly entered:

```
show running-config - displays the current configuration of the router.
```

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
```

```
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
!

!--- Lines omitted for brevity




...
!
tacacs-server host 192.168.1.1
tacacs-server key letmein
!
line con 0
line 1 8
line aux 0
line vty 0 4
!
end
```

Do a test authentication using your windows credentials and it will work.

Related Information

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/UsrDb.htm