ACS 5.x and later: Integration with Microsoft Active Directory Configuration Example

Contents

Introduction

This document provides a sample configuration to integrate Microsoft Active Directory with Cisco Secure Access Control System (ACS) 5.x and later. ACS uses Microsoft Active Directory (AD) as an external identity store to store resources such as users, machines, groups, and attributes. ACS authenticates these resources against AD.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Windows Active Directory Domain to be used needs to be fully configured and operational.
- Use Microsoft Windows Server 2003 Domain, Microsoft Windows Server 2008 Domain or Microsoft Windows Server 2008 R2 Domain as these are supported by ACS 5.x.**Note:** Integration of Microsoft Windows Server 2008 R2 Domain with ACS is supported from ACS 5.2 and later.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure ACS 5.3

- Microsoft Windows Server 2003 Domain

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Windows Active Directory provides many features that are used in the daily network usage. The integration of ACS 5.x with AD allows the use of the existing AD users, machines and their group mapping.

ACS 5.x integrated with AD provides these features:

1. Machine Authentication
2. Attribute Retrieval for Authorization
3. Certificate Retrieval for EAP-TLS Authentication
4. User and Machine Account Restriction
5. Machine Access Restrictions
6. Dial-in Permissions Check
7. Callback Options for Dial-in users
8. Dial-in Support Attributes

Configuration

Configure ACS 5.x Application Deployment Engine (ADE-OS)

Before you integrate ACS 5.x to the AD, ensure that the **TimeZone, Date & Time** on the ACS matches with that on the AD primary domain controller. Also, define the DNS server on the ACS in order to be able to resolve the domain name from the ACS 5.x. Complete these steps in order to configure ACS 5.x Application Deployment Engine (ADE-OS):

1. SSH to the ACS appliance and enter the CLI credentials.
2. Issue the **clock timezone** command in config mode as shown in order to configure the **TIMEZONE** on the ACS in order to match with that on the domain controller.

   ```
   clock timezone Asia/Kolkata
   ```

   Note: Asia/Kolkata is the timezone used in this document. You can find your specific timezone by exec mode **show timezones** command.
3. In case your AD domain controller is synchronized with an NTP server that resides in your network, it is highly recommended to use the same NTP server on the ACS. If you do not have NTP server, then skip to **step 4**. These are the steps to configure NTP server:NTP server can be configured with the **ntp server <ip address of the NTP server>** command in config mode as shown.

```
ntp server 192.168.26.55
The NTP server was modified.
If this action resulted in a clock modification, you must restart ACS.
```

Refer to ACS 5.x: Cisco ACS Synchronization with NTP Server Configuration Example for more information on NTP configuration.

4. In order to configure date and time manually use the **clock set** command in **exec mode**. An example is shown here:

```
clock set Jun 8 10:36:00 2012
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....................
Stopping Runtime......
Stopping Database....
Cleanup.....
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
```

5. Now verify the **Timezone, Date** and **Time** with the **show clock** command. The output of show clock command is shown here:

```
acs51/admin# show clock
Fri Jun  8 10:36:05 IST 2012
```

6. Configure DNS on ACS with the **<ip name-server <ip address of the DNS>** command in **config mode** as shown here:

```
ip name-server 192.168.26.55
```

Note: The DNS IP address is provided by your Windows domain administrator.

7. Issue the **nslookup <domain name>** command in order to verify the domain name reachability as shown.

```
acs51/admin#nslookup MCS55.com
Trying "MCS55.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;MCS55.com.                     IN      ANY

;; ANSWER SECTION:
MCS55.com.              600     IN      A       192.168.26.55
MCS55.com.              3600    IN      NS      admin-zq2ttn9ux.MCS55.com.
MCS55.com.              3600    IN      SOA     admin-zq2ttn9ux.MCS55.com.
   hostmaster.MCS55.com. 635 900 600 86400 3600

;; ADDITIONAL SECTION:
admin-zq2ttn9ux.MCS55.com. 3600 IN      A       192.168.26.55

Received 136 bytes from 192.168.26.55#53 in 0 ms
```

Note: If the **ANSWER SECTION** is empty, then contact your windows domain administrator to find out the correct DNS server for the domain.

8. Issue the **ip domain-name <domain name>** command in order to configure **DOMAIN-NAME** on the ACS as shown here:

```
ip domain-name MCS55.com
```

9. Issue the **hostname <hostname>** command in order to configure **HOSTNAME** on the ACS as shown here:

```
hostname acs51
```

Note: Due to NETBIOS limitations, ACS hostnames must contain less than or equal to 15 characters.

10. Issue the **Write memory** command in order to save the configuration to ACS.

Join ACS 5.x to AD

Complete these steps in order to join ACS5.x to AD:

1. Choose **Users and Identity Stores > External Identity Stores > Active Directory** and provide the Domain Name, AD account (Username) and its Password and click on **Test Connection**.**Note:** AD account required for domain access in ACS should have either of these:Add workstations to domain user right in corresponding domain.Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is created before joining ACS machine to the domain.**Note:** Cisco recommends that you disable the lockout policy for the ACS account and configure the AD infrastructure to send alerts to the admin if a wrong password is used for that account. This is because if you enter a wrong password, ACS does not create or modify its machine account when it is necessary and therefore possibly deny all authentications.**Note:** The Windows AD account, which joins ACS to the AD domain, can be placed in its own Organizational Unit (OU). It resides in its own OU either when the account is created or later on with a restriction that the appliance name must match the name of the AD account.
2. This screen shot shows that the test connection to the AD is successful. Then click **OK**.**Note:** Centrify configuration gets affected and sometimes gets disconnected when there is a slow response from the server while you test the ACS connection with the AD domain. However, it works fine with the other applications.
3. Click **Save Changes** for the ACS to join AD.
4. Once the ACS has successfully joined the AD Domain, it shows in the connectivity status.**Note:** When you configure an AD identity store, ACS also creates:A new dictionary for that store with two attributes: ExternalGroups and another attribute for any attribute retrieved from the Directory Attributes page.A new attribute, IdentityAccessRestricted. You can manually create a custom condition for this attribute.A custom condition for group mapping from the ExternalGroup attribute; the custom condition name is AD1:ExternalGroups and another custom condition for each attribute selected in the Directory Attributes page, for example, AD1:cn.

Configure Access Service

Complete these steps in order to complete the Access Service configuration so that ACS can use the newly configured AD Integration.

1. Choose the service from where you would like the users to be authenticated from AD and click on **Identity**. Now click **Select** next to the Identity Source field.
2. Choose **AD1** and click **OK**.
3. Click **Save Changes**.

Verify

In order to verify AD authentication, send an authentication request from a NAS with AD

credentials. Ensure that the NAS is configured on the ACS and the request would be processed by the Access Service configured in the previous section.

1. After successful authentication from NAS log into the ACS GUI and choose **Monitoring and Reports > AAA Protocol > TACACS+Authentication**. Identify the passed authentication from the list and click on the **magnifying glass** symbol as shown.
2. You can verify from the steps that ACS has sent Authentication request to AD.

Related Information

- **Cisco Secure Access Control System**
- **Technical Support & Documentation - Cisco Systems**