ACS 5.x及更高版本 — 配置與Microsoft AD的整合

目錄

簡介

本文提供將Microsoft Active Directory與思科安全訪問控制系統(ACS)5.x及更高版本整合的示例配置。ACS使用Microsoft Active Directory(AD)作為外部身份庫來儲存資源，例如使用者、電腦、組和屬性。ACS根據AD對這些資源進行身份驗證。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 要使用的Windows Active Directory域需要完全配置且運行正常。
- 使用Microsoft Windows Server 2003域、Microsoft Windows Server 2008域或Microsoft Windows Server 2008 R2域，因為ACS 5.x支援這些域。**注意：**ACS 5.2及更高版本支援將Microsoft Windows Server 2008 R2域與ACS整合。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全ACS 5.3
- Microsoft Windows Server 2003域

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

Windows Active Directory提供了許多日常網路使用中使用的功能。ACS 5.x與AD的整合允許使用現有的AD使用者、電腦及其組對映。

與AD整合的ACS 5.x提供以下功能：

1. 機器驗證
2. 用於授權的屬性檢索
3. EAP-TLS驗證的證書檢索
4. 使用者和電腦帳戶限制
5. 電腦訪問限制
6. 撥入許可權檢查
7. 撥入使用者的回叫選項
8. 撥入支援屬性

組態

配置ACS 5.x應用部署引擎(ADE-OS)

將ACS 5.x整合到AD之前，請確保ACS上的**TimeZone、Date & Time**與AD主域控制器上的時間相匹配。此外，在ACS上定義DNS伺服器，以便能夠從ACS 5.x解析域名。完成以下步驟以配置ACS 5.x應用部署引擎(ADE-OS):

1. 通過SSH連線到ACS裝置並輸入CLI憑證。
2. 在配置模式下發出**clock timezone**命令，如下所示，以便在ACS上配置**TIMEZONE**，使其與域控制器上的配置相匹配。

   ```
   clock timezone Asia/Kolkata
   ```

   註：Asia/Kolkata是本文檔中使用的時區。您可以通過exec mode **show timezones** 命令找到您的特定時區。
3. 如果AD域控制器與位於網路中的NTP伺服器同步，強烈建議在ACS上使用同一個NTP伺服器。如果沒有NTP伺服器，請跳至**步驟4**。以下是配置NTP伺服器的步驟：NTP伺服器可以在配置**模式下使用ntp server <NTP server的ip地址>**命令進行配置，如下所示。

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

   請參閱ACS 5.x:Cisco ACS與NTP伺服器同步配置示例，瞭解有關NTP配置的詳細資訊。
4. 若要手動配置日期和時間，請在**exec**模式下使用**clock set**命令。以下提供範例：

   ```
   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. 現在使用**show clock**命令驗證**Timezone**、Date和**Time**。show clock命令的輸出如下所示：

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

6. 在配置模式下使用**<ip name-server <ip address of the DNS>命令在ACS上**配置DNS,如下所示：

```
ip name-server 192.168.26.55
```

注意：DNS IP地址由您的Windows域管理員提供。

7. 發出**nslookup <domain name>**命令以驗證域名的可達性，如圖所示。

```
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
```

注意：如果**ANSWER SECTION**為空，請與Windows域管理員聯絡以查詢該域的正確DNS伺服器。

8. 發出**ip domain-name <domain name>**命令，以便在ACS上配置**DOMAIN-NAME**，如下所示：

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

9. 發出**hostname <hostname>**命令，以便在ACS上配置**HOSTNAME**，如下所示：

```
hostname acs51
```

注意：由於NETBIOS限制，ACS主機名包含的字元數必須少於或等於15。

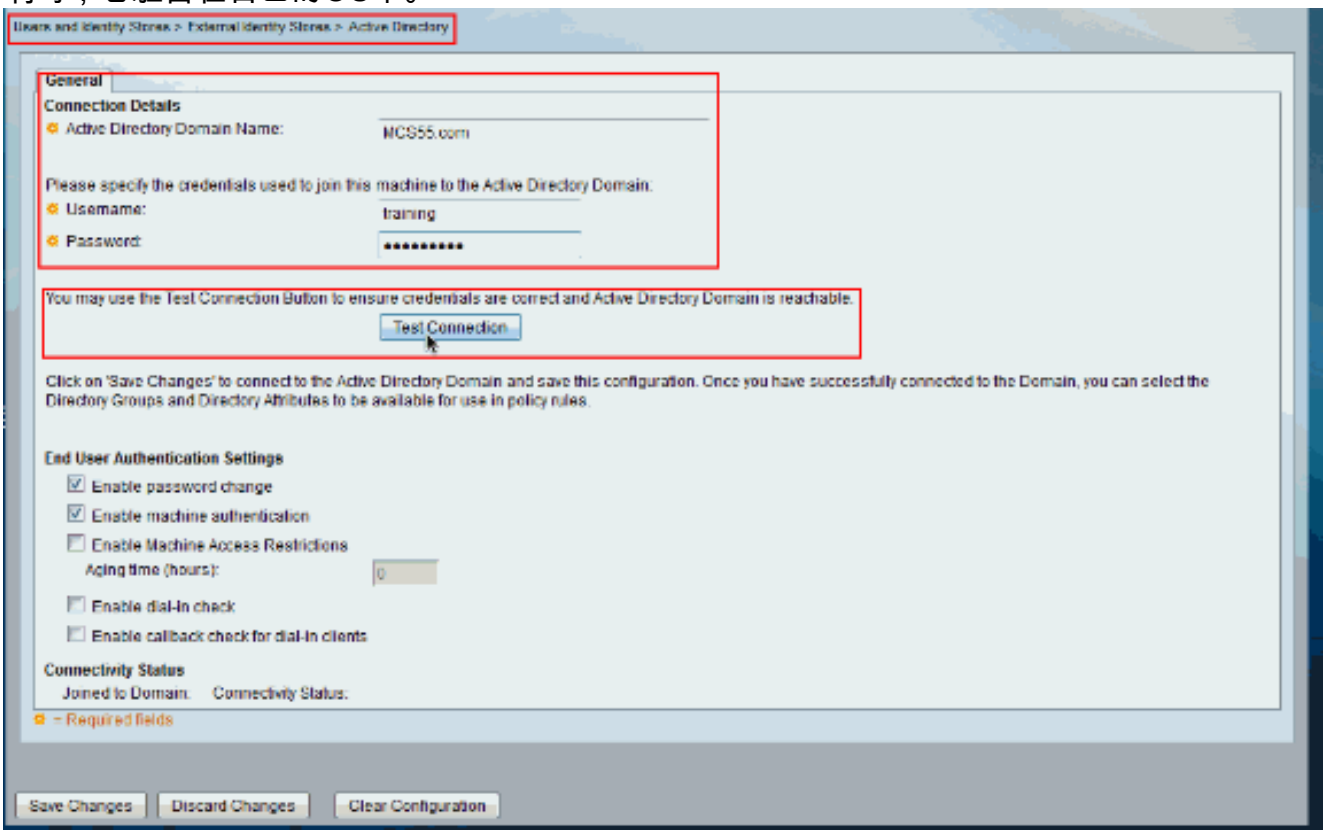
10. 發出**Write memory**命令，將組態儲存到ACS。

將ACS 5.x加入AD

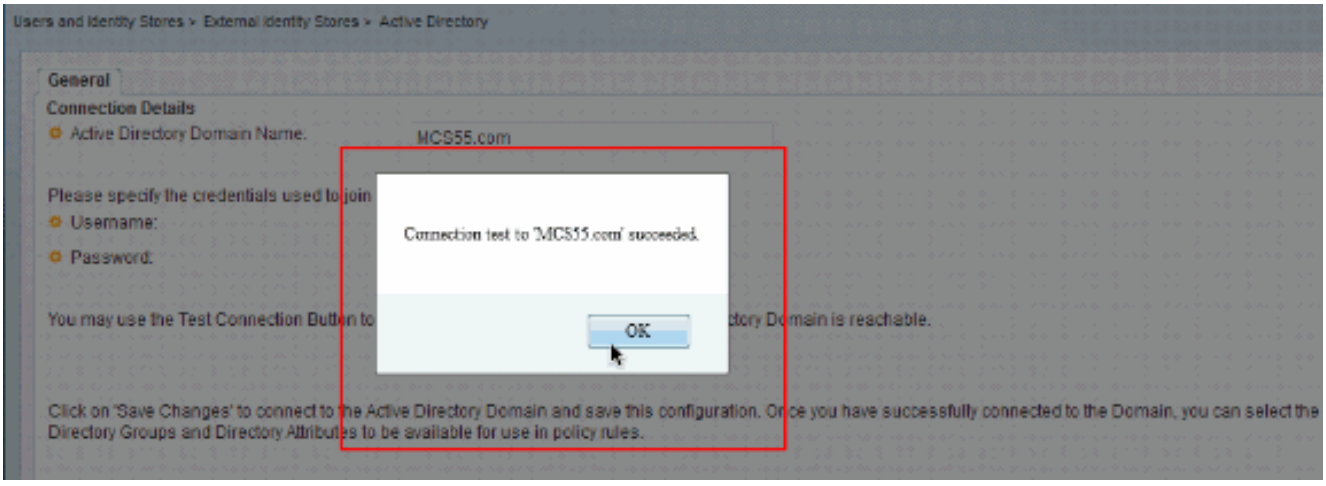
完成以下步驟，以便將ACS5.x加入AD:

1. 選擇**Users and Identity Stores > External Identity Stores > Active Directory**，提供域名、AD帳戶（使用者名稱）及其密碼，然後按一下**Test Connection**。**注意：在**ACS中訪問域所需的AD帳戶應具有以下任一項：將工作站新增到相應域中的域使用者許可權。在將ACS電腦加入域之前，在建立ACS電腦帳戶的相應電腦容器上建立電腦對象或刪除電腦對象許可權。**注意：**思科建議您禁用ACS帳戶的鎖定策略，並配置AD基礎設施，以便在該帳戶使用錯誤密碼時向管理員傳送警報。這是因為如果您輸入的密碼錯誤，ACS不會在必要時建立或修改其電腦帳戶，因此可能會拒絕所有身份驗證。**注意：**將ACS加入AD域的Windows AD帳戶可以置於自己

的組織單位(OU)中。 在建立帳戶時或在建立帳戶後設定裝置名稱必須與AD帳戶名稱匹配的限制時，它駐留在自己的OU中。

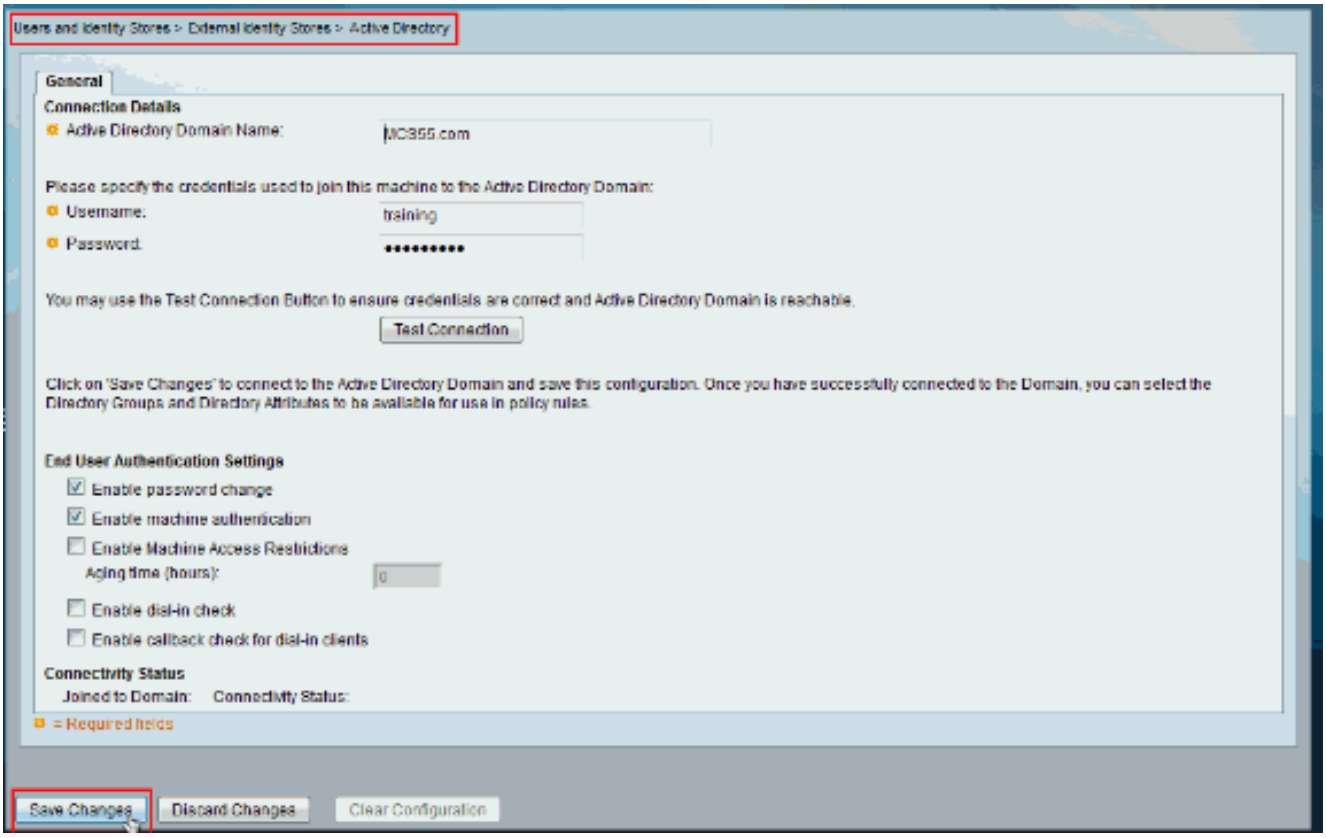


2. 此螢幕抓圖顯示與AD的測試連線成功。然後按一下**OK**。

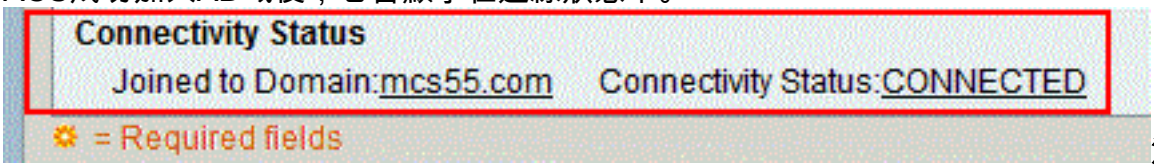


注意：測試與AD域的ACS連線時，如果伺服器響應緩慢，Centrify配置會受到影響，有時會斷開連線。但是，它與其他應用程式配合使用效果良好。

3. 按一下**Save Changes**以將ACS加入AD。



4. ACS成功加入AD域後，它會顯示在連線狀態中。

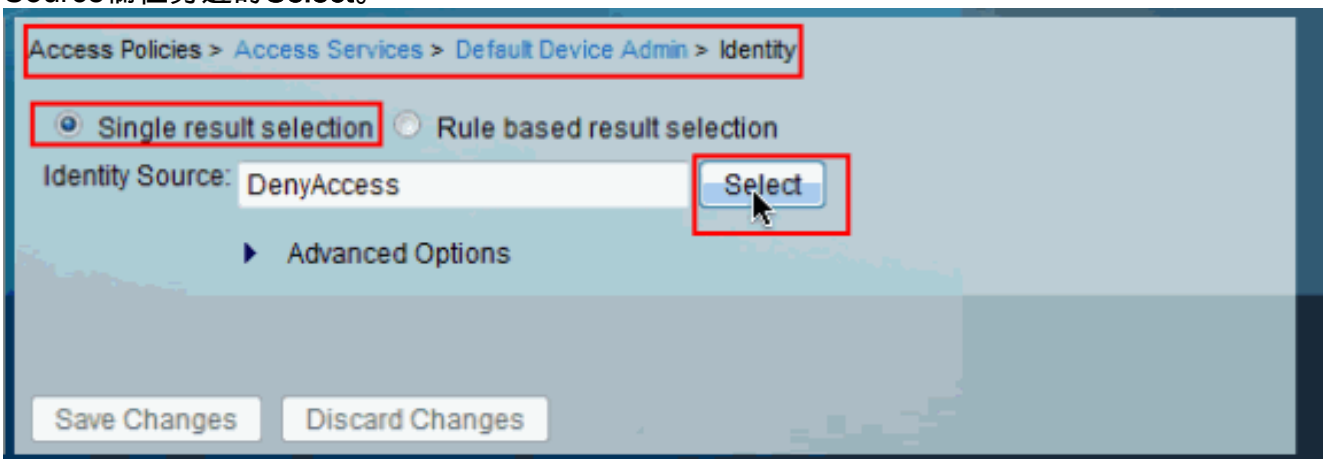


注意：配置AD身份庫時，ACS還會建立：該商店的新詞典具有兩個屬性：ExternalGroups和從「目錄屬性」(Directory Attributes)頁面檢索的任何屬性的另一個屬性。新屬性IdentityAccessRestricted。您可以手動建立此屬性的自定義條件。從ExternalGroup屬性進行組對映的自定義條件；自定義條件名稱為AD1:ExternalGroups，並且在「目錄屬性」頁中選定的每個屬性的另一個自定義條件，例如AD1:cn。

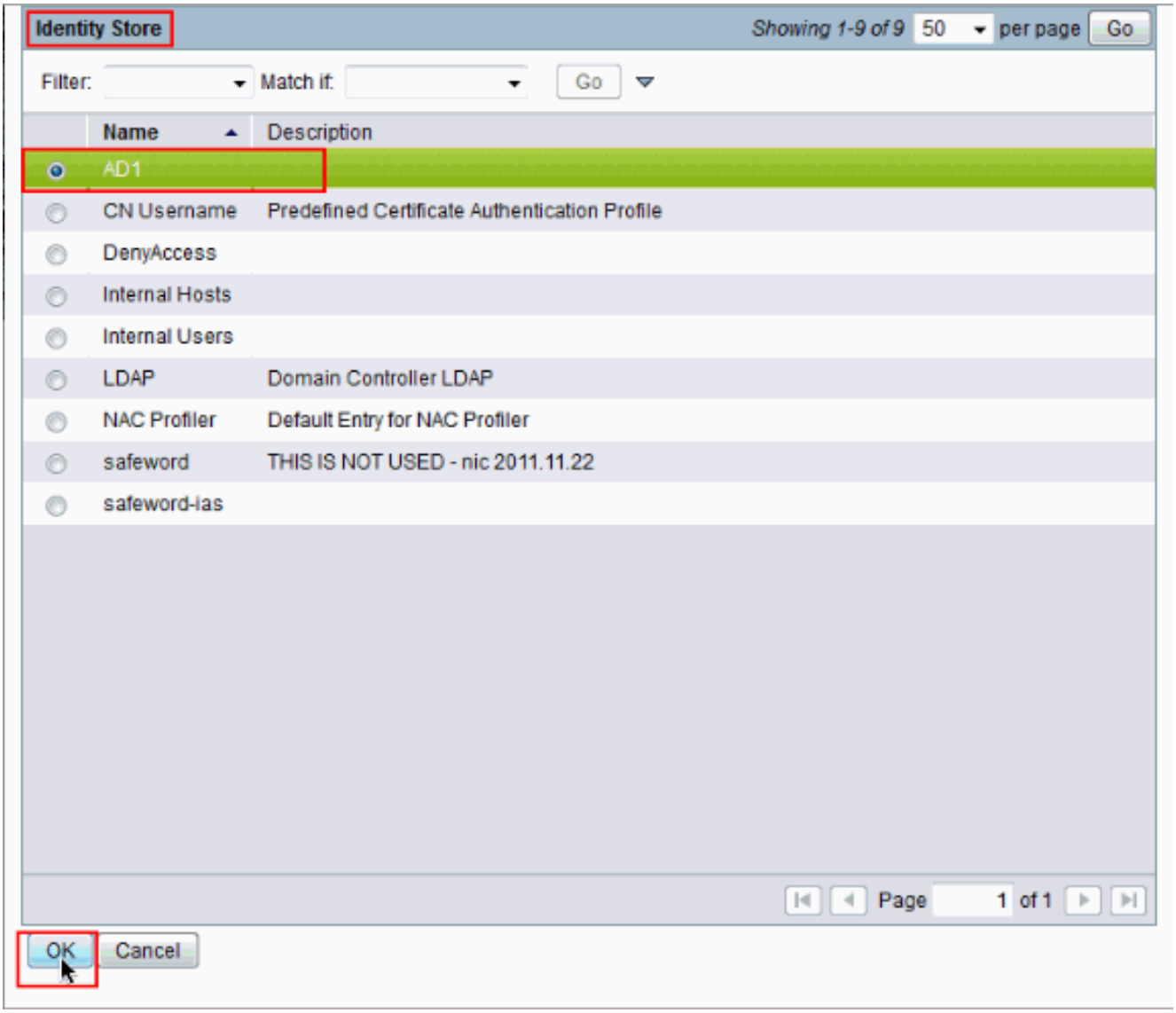
配置訪問服務

完成以下步驟即可完成訪問服務配置，以便ACS可以使用新配置的AD整合。

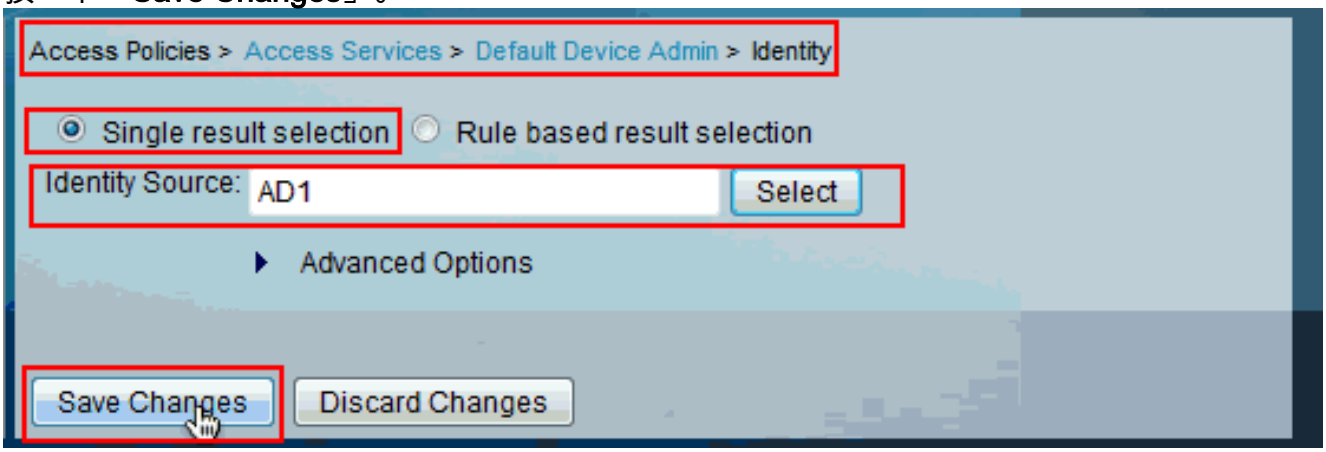
1. 選擇要從AD對使用者進行身份驗證的服務，然後按一下**Identity**。現在，點選Identity Source欄位旁邊的**Select**。



2. 選擇**AD1**，然後按一下**OK**。



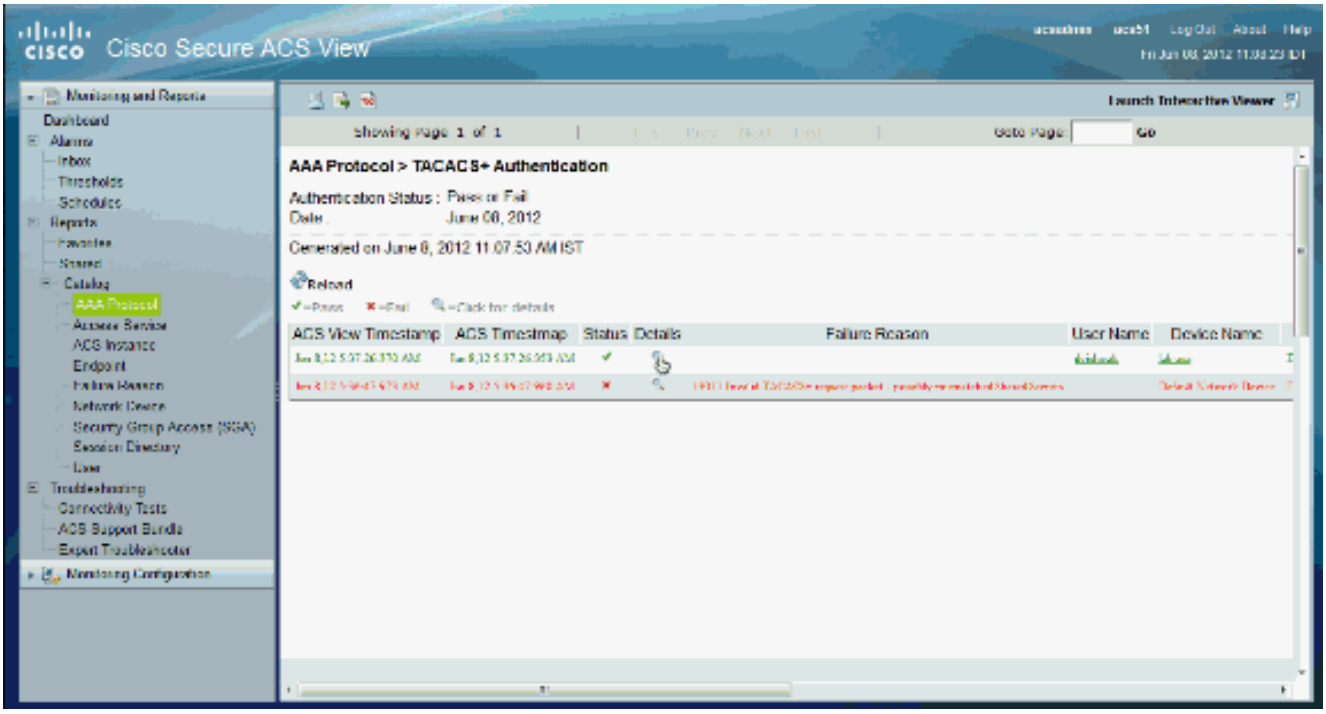
3. 按一下「**Save Changes**」。



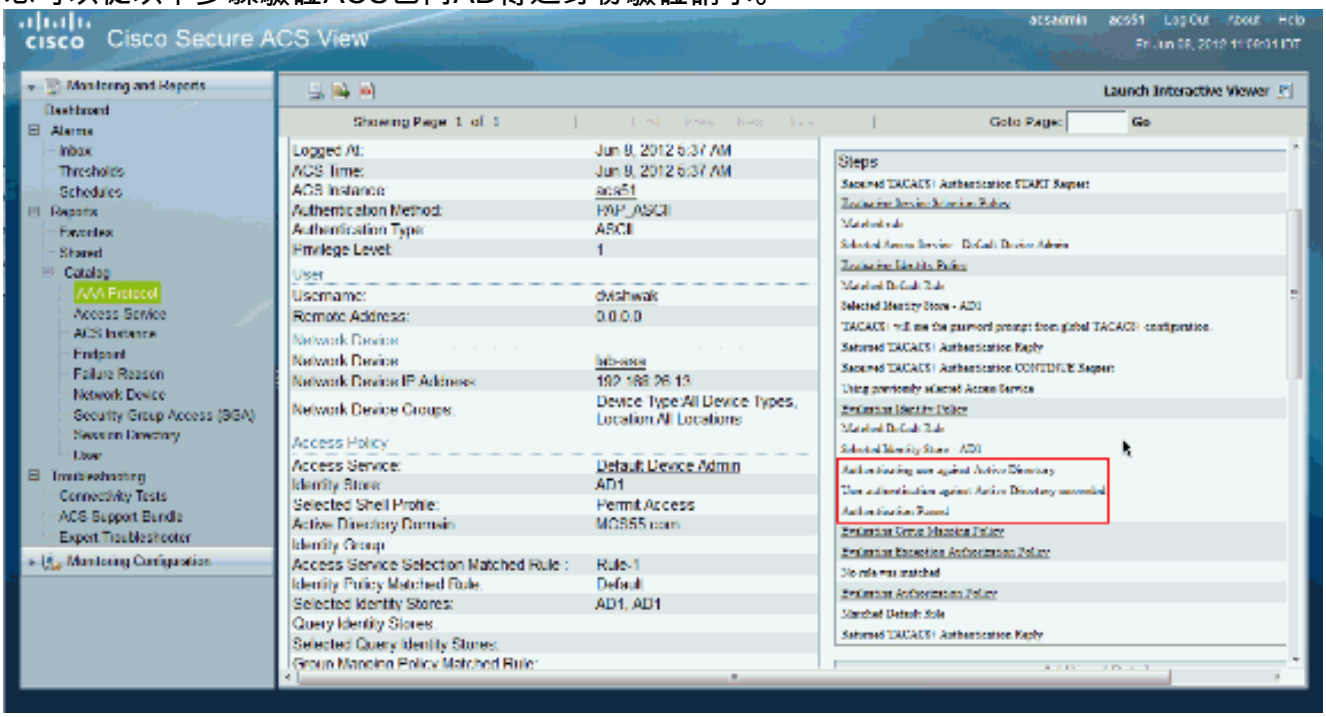
驗證

為了驗證AD身份驗證，請從NAS傳送帶有AD憑證的身份驗證請求。確保在ACS上配置了NAS，並且請求將由上一節中配置的訪問服務處理。

1. 成功從NAS進行身份驗證後，登入到ACS GUI，然後選擇**Monitoring and Reports > AAA Protocol > TACACS+Authentication**。從清單中識別通過身份驗證，然後按一下放**大鏡形**符號，如圖所示。



2. 您可以從以下步驟驗證ACS已向AD傳送身份驗證請求。



相關資訊

- 思科安全存取控制系統
- 技術支援與文件 - Cisco Systems