ACS 5.x及更高版本 — 配置與Microsoft AD的整合

```
目錄
```

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>背景資訊</u> <u>組態</u> 配置ACS 5.x應用部署引擎(ADE-OS)</u> <u>將ACS 5.x加入AD</u> <u>配置訪問服務</u> <u>驗證</u> 相關資訊

<u>簡介</u>

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。

<u>必要條件</u>

<u>需求</u>

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。

<u>採用元件</u>

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。

<u>慣例</u>

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。

<u>背景資訊</u>

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

<u>配置ACS 5.x應用部署引擎(ADE-OS)</u>

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<u>ACS 5.x:Cisco ACS與NTP伺服器同步配置示例</u>,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-zg2ttn9ux.MCS55.com. 3600 IN MCS55.com. SOA admin-zg2ttn9ux.MCS55.com. hostmaster.MCS55.com. 635 900 600 86400 3600 ;; ADDITIONAL SECTION: 192.168.26.55 admin-zq2ttn9ux.MCS55.com. 3600 IN A 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

- 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。

<u>將ACS 5.x加入AD</u>

服器。

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。

| a and a design of the second se | tive Directory | |
|--|---|---|
| and the second sec | | |
| General | | |
| Connection Details | | |
| Adve Directory Domain Name: | MCS55.com | |
| Places specify the production up adds in the | e montries to the Anti-o Disasters Dem | a ala: |
| Please specily the credentials used to join thi | s machine to the Active Directory Dom | nam. |
| - Gaemanne. | training | |
| o Password | | |
| | | |
| You may use the Test Connection Button to en | isure credentials are correct and Achiv | ve Directory Domain is reachable. |
| | Test Connection | |
| | <i>\$</i> | |
| Click on 'Save Changes' to connect to the Acti | ve Directory Domain and save this cor | nfiguration. Once you have successfully connected to the Domain, you can select the |
| Directory Groups and Directory Attributes to br | available for use in policy rules. | |
| | | |
| | | |
| End User Authentication Settions | | |
| End User Authentication Settings | | |
| End User Authentication Settings | | |
| End User Authentication Settings | | |
| End User Authentication Settings Image Image Image Image </td <td></td> <td></td> | | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): | D | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): Enable dial-in check | D | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): Enable dial-in check Enable caliback check for dial-in clients | D | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): Enable dial-in check Enable caliback check for dial-in clients Connectivity States | 0 | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): Enable dial-in check Enable callback check for dial-in client: Connectivity Status Joned to Domain Connectivity Status | 0 | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): Enable dial-in chack Enable caliback chack for dial-in clients Connectivity Status Joined to Domain: Connectivity Status: Previnced Tables | D 2 | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): Enable dial-in chack Enable caliback check for dial-in clients Connectivity Status Joined to Domain: Connectivity Status: Required fields | 0 | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Aging time (hours): Enable dial-in check Enable callback check for dial-in clients Connectivity Status Joined to Domain: Connectivity Status: Required fields | 0 | |
| End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictions Acing time (hours): Enable dial-in chack Enable caliback chack for dial-in clients Connectivity Status Joined to Domain: Connectivity Status: Required fields | 0 | |

2. 此螢幕抓圖顯示與AD的測試連線成功。然後按一下OK。

| General | | | | | | | | | | | | | | |
|--|---|------------|---------|-------|--------|--------|-------|-----------|----------|--------|-----|---|----------|--|
| Connection Details | | | | | | | | | | | | | | |
| Active Directory Domain Name. | MCS55.com | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| Please specify the credentials used to join | | | | | | | | | | | | | | |
| 6 Lisemana: | | | | | | | | | | | | | | |
| Coemane. | Connection test to 'MCS55.com' succeeded. | | | | | | | | | | | | | |
| Password: | | × 0 - 0 0 | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| You may use the Test Case added Butters to | | Acres De | o no o | | hoble | | | | | | | | | |
| rou may use the rest connection but in to | OK | citory Di | main i | sread | nable | 1.1.1 | | | | | | | | |
| in a sector i di na sa i a di di n <mark>a</mark> sa i | <u> </u> | 16.00 | | | | | | | | | | | | |
| | | 10000 | | | | | | | | | | | | |
| Click on 'Rays Channes' to connect to the Art | Directory Domain and caus this confin | unation Or | de veri | have | autopa | a stul | hinne | n e store | (to 10) | e Dain | ain | - | opla | |

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。

| Connection Details | | | | |
|---|-------------------------------------|--------------------------|-------------------|--|
| Active Directory Domain Name: | MC855.com | | | |
| Please specify the credentials used to joi | n this machine to the Active Dire | ctory Domain: | | |
| 0 Usemame: | training | | | |
| Password: | | | | |
| You may use the Test Connection Button t | to ensure credentials are correc | and Active Directory Dom | ain is reachable. | |
| | Test Connection | | | |
| Directory Groups and Directory Attributes | to be available for use in policy r | ules. | | |
| ind User Authentication Settings | | | | |
| Enable password change | | | | |
| Enable machine authentication | | | | |
| Enable Machine Access Restriction | ns | | | |
| Aging time (hours): | 0 | | | |
| Enable dial-in check | | | | |
| Enable caliback check for dial-in cl | ients | | | |
| Connectivity Status Joined to Domain: Connectivity Statu | 15: | | | |
| = Required helds | | | | |
| | | | | |
| ve Changes | Clear Configuration | | | |
| | | | | |
| ve Changes Discard Changes | Clear Configuration | | | |

➡ = Required fields 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**。

| Access Policies > / | Access Services > Default Device Admin > Identity |
|---------------------|---|
| Identity Source: | DenyAccess Select |
| The second second | Advanced Options |
| | |
| Save Changes | Discard Changes |

2. 選擇AD1,然後按一下OK。

| Filter: | • | Match if: | | • | Go | ~ | | | | | |
|--|--|---|--------------------------------|-------------------------------|------------------------|-----------------------------------|---------|--------|-----|--------|---|
| | Name 🔺 | Descripti | on | | | | | | | | |
| ۲ | AD1 | | | | | | | | | | |
| 0 | CN Username | Predefine | ed Certific | ate Authen | tication P | ofile | | | | | |
| 0 | DenyAccess | | | | | | | | | | |
| \odot | Internal Hosts | | | | | | | | | | |
| 0 | Internal Users | | | | | | | | | | |
| 0 | LDAP | Domain | Controller | LDAP | | | | | | | |
| 0 | NAC Profiler | Default E | ntry for N/ | AC Profiler | | | | | | | |
| 0 | safeword | THIS IS N | IOT USED |) - nic 201 | 1.11.22 | | | | | | |
| 0 | safeword-ias | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | ŀ | (🕘 Pa | ige | 1 of 1 | Þ |
| OK | Cancel | | | | | | • | t 🕘 Pa | ige | 1 of 1 | Þ |
| <u>оқ</u> | Cancel | I ges 」。 | | | | | H | t 💽 Pa | ige | 1 of 1 | Þ |
| ok :一下 Access | Cancel | Iges」。 | ices > D | efault Dev | vice Adm | in > Identit | [! | C Pa | ige | 1 of 1 | Þ |
| ок стр Access | Cancel | Iges」 ₀ cess Serv | ices > D | efault Dev | vice Adm | in > Identit | y | I I Pa | ige | 1 of 1 | Þ |
| <mark>ور بر</mark> مردوعة مردوعة | Cancel Save Chan Selicies > Acc Single result s | Iges」。 cess Serv election | ices > D | efault Dev le based | vice Adm d result : | in > Identit selection | y | (🚽 Pa | ige | 1 of 1 | Þ |
| ۲ Access Ident | Cancel Save Chan s Policies > Acc Single result s ity Source: AE | Iges」。 cess Serv election)1 | ices > D] ◯ Ru | efault Dev le based | vice Adm d result : | in > Identit selection Sele | y ct | I d Pa | ige | 1 of 1 | • |
| کردوءی Ident | Cancel Save Chan Second Single result s Table Source: AC | Iges」。 cess Serv election)1 Advanc | ices > D] ○ Ru ed Optic | efault Dev le based ons | vice Adm d result : | in ≻ Identit selection Sele | y ct | I I Pa | ige | 1 of 1 | Þ |

<u>驗證</u>

Save Changes

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。

Discard Changes

 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。

| cisco Cisco Secure A | CS View | daan ucabt Fa | Log Out About Jan 08, 2012 11.08 | Halp 123 IDI |
|--------------------------------|--|------------------|--|-----------------|
| - 💮 Monitoring and Reports | 1 B B | Launch | Interactive View | er 🔄 |
| E Alarma | Showing Page 1 of 1 I is Prev. Real Lind Gete Page | Ge | , | |
| - inbox | AAA Protocol > TACACS+ Authentication | | | i i |
| Schedules 10 Reports | Authentication Status : Passion Fail Date : June 00, 2012 | | | |
| - Havanies | Cenerated on June 8, 2012 11 07 53 AM IST | | | |
| E - Catalog AAA Protocol | | | | |
| Access Bervice ACS Instance | ACS View Timestamp ACS Timestmap Status Details Failure Reason | User Name | Device Name | |
| Endpoint | a., 8,12 5 07 26 370 AM 1., 8,12 5 37 26 263 AM 🖌 🦉 | distant. | Selected and the selected sele | I |
| - Falure Reason | len 8.12 5/64-376 MM 🛛 log 8/12 5.96-07.968 AVI 🖉 🧐 1911) Toost in TACACCe require particle provide researched Stand Servers | | Defect Veterals Base | - 1 |
| Securty Group Access (SGA) | | | | |
| . Session Directory | | | | |
| E Troubleshooting | | | | |
| - Connectivity Tasts | | | | |
| Expert Troubleshooter | | | | |
| 🕞 🏭 Nonitoring Configuration | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

2. 您可以從以下步驟驗證ACS已向AD傳送身份驗證請求。

| cisco Cisco Secure A | CS View | | Ex.Jun 08, 2012 11 06/01 IOT |
|---|---|--|---|
| * 🛐 Moniforing and Reports | 5 6 0 | | Launch Interactive Viewer 📳 |
| Dashtrond B_Alarma | Showing Page 1 of 1 | I SI RSW NOR INC. | Golo Page: Go |
| - Inbox Thresholds Schedules | Logged At: ACS Time: ACS Instance: | Jun 8, 2012 5:37 AM Jun 8, 2012 5:37 AM acs51 | Steps Second TACATSI Authorization START Super: Descript Article Stories Patient |
| - Facates - Stand H- Catalog | Authentication Type Finilege Levet | ASCI 1 | Marateal ade Schotel Assess Service - Dofad: Device Admin Instancine Menths Parlies |
| Access Service Access Service | Username: Remote Address: Network Davies | dvishwak 0.0.0.0 | Marshed Default 244 Selected Merity Store - AD1 TACAUS - will use the password prompt from global TACAUS - configuration. |
| Freijont Failure Reason Network Device | Network Device Network Device IP Address | lab-asa 192 168 26 13 Deste Time 20 Deste Dest | Setured TACACSI Anthenication Reply Secured TACACSI Anthenication CONTINUE Segree: Using previously selected Acoust Service |
| Security Group Access (SGA) Security Directory User | Network Device Groups. Access Policy | Location Al Locations | Zenimon Bettie Dile Manini Dalah Sala Selanta Betak Sala |
| Imitilexhoring Connectivity Tests ACS Second Bandle | Access Service: Identity Store Selected Shell Profile: | Default Device Admin AD1 Permit Access | Author densing our against Author Directory Dara authoritant against Author Directory accorded Author densing Record |
| Expert Troubleshooter | Active Directory Domain Identity Group Access Service Selection Matched Rule : | MC355.com Rule-1 | Preliminan Genes Massian Policy Preliminan Researces Archeolation Policy |
| | Identity Policy Matched Role. Selected Identity Stores: Query Identity Stores. Selected Query Identity Stores. | Default AD1, AD1 | Jon ma Hai anatheo Emilianai Aofondation Zolary Mandai Detaili Sola Sataras TACACSI Anthenication Reply |
| | Group Manoing Policy Matched Bule | | A 101 175 - 3 |

相關資訊

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