以 Tivoli Access Manager 6.0 配置單一登入網路社群

開機時以 WebSEAL 和 PDWebPI 單一登入網路社群

Vinayak Kawathekar (vinayak.kawathekar@in.ibm.com)，軟體工程師，IBM 印度軟體實驗室

原文刊載於：http://www-128.ibm.com/developerworks/tivoli/library/t-ecssotam/index.html

本文簡單說明以 Tivoli® Access Manager for e-Business，來進行網路社群單一登入 (e-community single sign-on, eCSSO) 的實施概念，同時會討論到配置、必備項目，以及實施 eCSSO 期間所遭遇問題的疑難排解要訣。

前言

跨 Tivoli Access Manager (TAM) 網域實施 SSO 的方法如下：

- 在大型分工組織中，每個分支都使用不同的 TAM 網域，以確實分隔不同群組的資料與使用者。
- 在包含許多事業夥伴組織的運作環境中，由於每個組織都有各自實施 TAM 安全的方法，因此使用者登錄和授權機制也五花八門。

在這種環境中，使用者可能需要在在不同網域之間移動，但不需每次進入不同網域時都需經過重新鑑別。這種跨網域功能是以不同網域之間的授信爲運作基礎，當通行個體已在其他特定網域中鑑別身分時，另一網域就能接受該個體，不需重新鑑別。

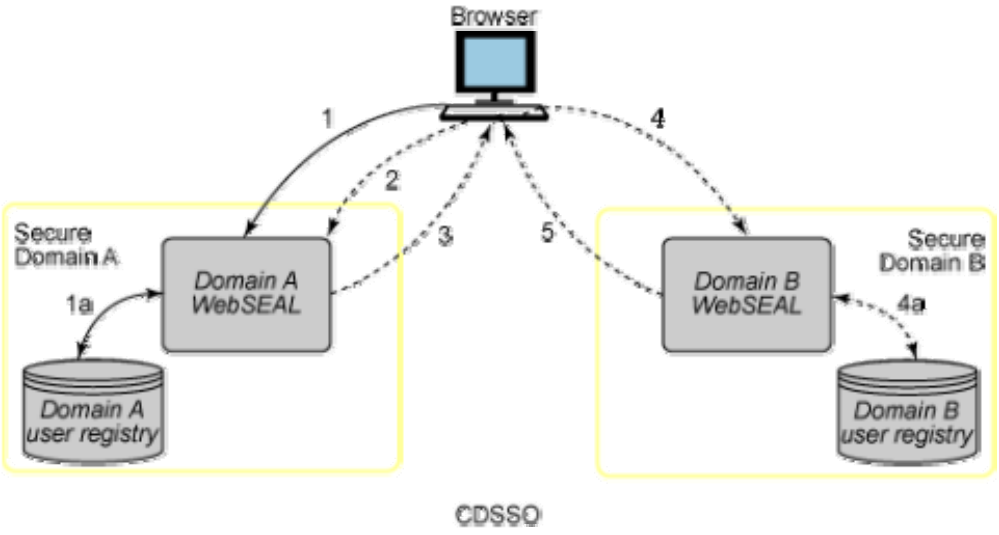
使用者存取受保護資源的權限，取決於使用者在該特定網域的認證等級，且在使用者成功鑑別身分後，才會建立這些認證。但在跨網域環境中，還需要另一種建立使用者認證的機制，以便在無法確實鑑別使用者的新網域中使用。WebSEAL 支援兩種不同類型的跨網域鑑別功能，可解決這個問題。

- 跨網域單一登入 (Cross domain single sign-on, CDSSO)
- 網路社群單一登入 (e-community single sign-on, eCSSO)

跨網域單一登入 (Cross domain single sign-on, CDSSO)

WebSEAL 可將安全網域中的已鑑別使用者身分，轉遞給另一個安全網域中的 WebSEAL 伺服器。接收端 WebSEAL 會針對提供的身分，傳送 WebSEAL 給其自身安全網域中的有效身分，從而完成身分對映。此功能也可視爲推送式鑑別模式。

使用 CDSSO 時，使用者可要求 WebSEAL 伺服器上的特定鏈結，然後將該要求和認證資訊傳送給不同 TAM 網域中的 WebSEAL 伺服器。不過，如果使用者想要直接存取目標網域，仍必須直接在該網域進行鑑別。



CDSSO 程序包含下列步驟：

1. 使用者先在 Domain A 中的 WebSEAL 伺服器上鑑別。
2. 在某個時點，使用者對 'pkmscdsso' 鏈結提出要求，而該鏈結則是包含 Domain B URL 的特定導向指令。這個導向指令會重新導向使用者，導至由 Domain B 中 WebSEAL 伺服器所控制的 URL。
3. 此時 Domain A WebSEAL 會建立包含加密認證的身分符記，並利用該符記將瀏覽器重新導至 Domain B WebSEAL。
4. Domain B WebSEAL 接收身分符記之後，便會解密其中的認證資訊，然後將使用者對映至某個 Domain B 身分（如圖 4a 所示），並建立瀏覽器階段作業。
5. 此時使用者已順利在兩部不同網域的 WebSEAL 伺服器之間建立階段作業，但卻只需登入一次。Domain B URL 經過處理後，會將結果傳送至瀏覽器。

由於已透過 Domain B WebSEAL 建立身分，因此不需要鑑別就能順利處理後續要求。

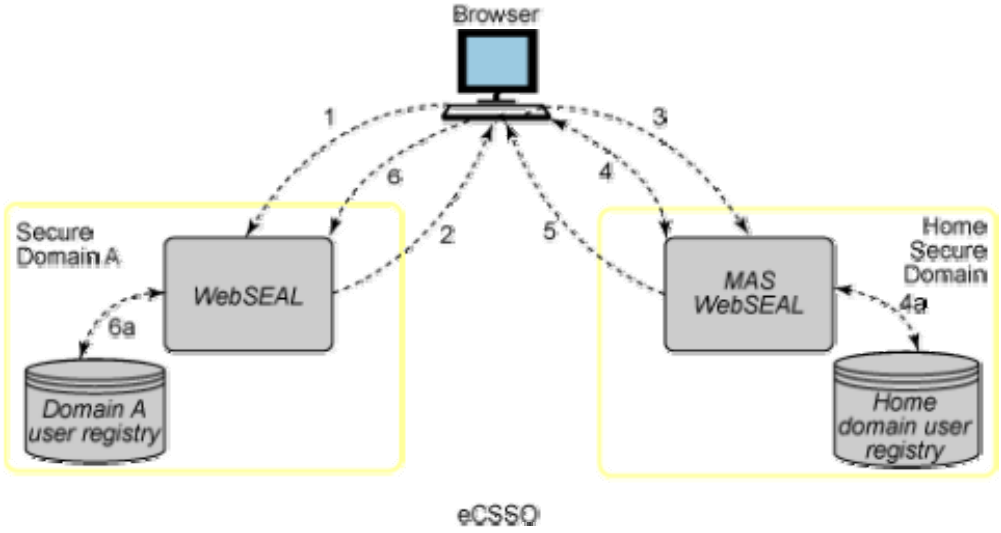
CDSSO 所採用的機制，是由某個安全網域中的 WebSEAL 伺服器，將類似於「介紹信」的資訊，傳送給另一個安全網域中的 WebSEAL 伺服器。

網路社群單一登入 (e-community single sign-on, eCSSO)

在 eCSSO 中，多個 TAM 網域被定義爲網路社群的一部分，並將其中一個網域指定爲「起始」(Home) 網域。起始網域擁有管制網路社群的商業協議，使用者加入網路社群時，其

相關驗證資訊（包括使用者名稱及鑑別用密碼）都由起始網域加以維護，這份協議可作爲管理所需的單一參考點。

當使用者在任一涉及網域中要求受保護資源時，會先在起始網域的「主要鑑別伺服器」(Master Authentication server, MAS) 上進行鑑別。完成起始鑑別之後，使用者便擁有在起始網域使用者登錄中建立的網路社群身分。如有需要，使用者的網路社群身分會透過網路社群中其他網域的「Web 安全伺服器」（WebSEAL 或 PDWebPI），陸續與本端身分進行對映。



eCSSO 程序包含下列步驟：

1. 使用者對網路社群中的受保護資源提出要求，而該資源是由社群中某網域 (Domain A) 的 WebSEAL 伺服器所控制，且這部 WebSEAL 尚未建立這位使用者的階段作業。
2. WebSEAL 伺服器使用 'voucher' 要求，將使用者重新導至 MAS。Voucher 要求中包含了特定導向指令 (pkmsvouchfor)，會要求 MAS 提供該使用者的身分資訊。
3. 瀏覽器將 voucher 要求轉遞給 MAS，
4. 並由 MAS 檢查使用者是否已在網路社群中完成鑑別。如果還沒進行，就會鑑別使用者，並對映至起始網域身分（如圖 4a 所示)。
5. 此時會建立一個認證用 (vouch-for) 符記，且 MAS 會將此符記傳回原本的 WebSEAL 伺服器，符記中包含了證明使用者身分的認證資訊。
6. 瀏覽器會將要求和認證用符記轉遞給原本的 WebSEAL，之後 WebSEAL 伺服器便會解密符記，並擷取使用者身分。WebSEAL 會將擷取的身分與本端網域中的適當 TAM 身分進行對映（如圖 6a 所示），並建立瀏覽器階段作業。

與 Domain A WebSEAL 建立好階段作業之後，通常不需再進行證明/驗證，即可順利處理後續要求。

CDSSO 與 eCSSO 的主要差異：

- eCSSO 模式支援使用直接 URL（我的最愛書籤）來存取資源，
- CDSSO 模式則仰賴特別配置的 'pkmscdsso' 鏈結。
- 在 eCSSO 中，WebSEAL 會從 MAS WebSEAL 拉取使用者認證資料；
- 在 CDSSO 中，WebSEAL 則是將使用者的認證資料，推送至使用者想要單一登入的另一部 WebSEAL。

想要參與跨網域單一登入機制的使用者，必須擁有有效的初始（起始）網域使用者帳號，然後再對映至每個參與遠端網域中的有效帳號。

這項對映作業的進行方式，可以是使用登錄在所有參與網域中的同一使用者名稱（一對一對映），或使用「跨網域對映架構」(Cross Domain Mapping Framework, CDMF)，來將某網域的使用者身分對映到另一網域中的相對應身分。（一對一或多對一對映）。

eCSSO 配置的必備項目

eCSSO 配置的必備項目包括：

- 爲了讓網路社群能夠順利運作，每部加入的 Web 安全伺服器，都必須向跨網域環境中的其他參與伺服器，顯示出完整的網域名稱 (FQDN)。
- 所有加入網路社群的 Web 安全伺服器必須使用同步的機器時間。
- 必須產生一個「cdsso 金鑰」：

TAM Web 安全伺服器必須加密驗證資料，並將其置於符記中。進行加密時，會使用位於 'pdwebrte/bin' 目錄中的 'cdsso_key_gen' 公用程式來產生金鑰，並以金鑰加密資料。每個加入網域中的每部 Web 安全伺服器都會共用這個金鑰。在設定網路社群時便會要求建立及散佈金鑰檔，您可以手動方式將這個金鑰檔，安全複製到每部加入的 Web 安全伺服器。

當網路社群中的 MAS WebSEAL 伺服器實例與參與 WebSEAL 伺服器實例，皆配置爲使用同一部機器上的相同網路介面時，該網路社群無法支援生產與測試用途。

WebSEAL 配置檔中的配置參數

若要編輯 WebSEAL 配置檔 'webseald.conf'：

1. 在 [authentication-mechanisms] 段落中指定 sso-create 和 sso-consume 程式庫，解除 sso-create 和 sso-consume 項目的註解，然後新增作業系統類型適用的外掛失效

接手 Cookie 程式庫名稱。

只有作爲 MAS 的特定 WebSEAL，才能指定 sso-create 參數。

作爲網路社群參與者的特定 WebSEAL 則只能指定 sso-consume 參數。

[authentication-mechanisms]

- sso-create = C:\Progra~1\Tivoli\PDWebRTE\lib\ssocreate.dll (Windows®)
- sso-create = /opt/pdwebrte/lib/libssocreate.so (Linux®)
- sso-consume = C:\Progra~1\Tivoli\PDWebRTE\lib\ssoconsume.dll (Windows)
- sso-consume = /opt/pdwebrte/lib/libssoconsume.so (Linux)

2. 指定要以「http、https、both 或 none」其中一種方式，來加入網路社群單一登入。

[e-community-sso]

- e-community-sso-auth = https

3. 網路社群名稱必須符合所接收的任何「認證用符記」或「網路社群 Cookie」。參與特定網路社群的所有 Web 安全伺服器都必須使用這個名稱。

[e-community-sso]

- e-community-name = ecomm

4. 若爲網路社群中的 MAS，此參數必須設爲 'yes'。將主要鑑別伺服器設爲 'yes' 之後，此伺服器就能接受來自其他 WebSEAL 實例的認證用要求，這些實例擁有的網域金鑰已列於 [e-community-domain-keys] 段落中。

[e-community-sso]

- is-master-authn-server = yes

5. 如果此特定 WebSEAL 不作爲 MAS，就必須在 [e-community-sso] 段落中設定其他參數，也就是該特定網路社群 MAS 的 FQDN。如果尚未執行本端網域登入，則登入嘗試將遞送給 MAS，並由此伺服器來證明使用者身分。主要驗證伺服器的網域金鑰必須列在 [e-community-domain-keys] 段落中。

   如果 e-community-sso-auth 允許使用 HTTP 通訊協定，且主要鑑別伺服器會在標準 HTTP 埠（埠 80）以外的其他埠上接聽 HTTP 要求，就必須在此處指定非標準埠號。如果此伺服器是主要鑑別伺服器，就可以忽略此參數。

   如果 e-community-sso-auth 允許使用 HTTPS 通訊協定，且主要鑑別伺服器會在標準 HTTPS 埠（埠 443）以外的其他埠上接聽 HTTPS 要求，就必須在此處指定非標準埠號。如果此伺服器是主要鑑別伺服器，就可以忽略此參數。

[e-community-sso]

- is-master-authn-server = no
- master-authn-server = MAS 的 FQDN
- master-http-port = MAS 的 http 埠號
- master-https-port = MAS 的 https 埠號

6. 此參數用來表示認證用符記的使用期限（以秒爲單位），且必須將參與 Web 安全伺服器之間的時間偏差納入考量。

[e-community-sso]

- vf-token-lifetime = 180

7. 這是認證用 URL 的指定元，用來指定伺服器根目錄的 URL 相對路徑。MAS 會使

用此路徑來建立參與 eCSSO 伺服器所需的認證用要求，以便區分認證用要求資訊與其他要求。依預設會使用 '/pkmsvouchfor'。

[e-community-sso]

- vf-url = /pkmsvouchfor

8. 此參數用來指定認證用引數，也就是包含於認證用回覆內容中的認證用符記名稱（作爲引數名稱）。MAS 使用此引數來建立認證用回覆，並用來識別傳入的要求，是否與加入 eCSSO 伺服器的認證用資訊相同。依預設會使用 'PD-VF'。

   [e-community-sso]

   - vf-argument = PD-VF

9. 此參數可指定網路社群的 Cookie 使用期限（以分鐘爲單位）。

   [e-community-sso]

   - ec-cookie-lifetime = 300

10. 啓用或停用 eCSSO 的無鑑別存取。設定爲 no 時，每個初始 eCSSO 要求都必須進行鑑別。預設值爲 yes。

    [e-community-sso]

    - ecsso-allow-unauth = yes

11. 若認證用符記中的字串必須使用 UTF-8 編碼，請指定此參數。當符記中的的使用者名稱或認證屬性未使用與 WebSEAL 伺服器相同的編碼頁時，就必須使用 UTF-8 進行編碼。如果您的符記必須在使用本端編碼頁的舊環境中交互運作，請將此屬性設定爲 'no'。

    [e-community-sso]

    - use-utf8 = yes

12. 這些是由 'cdsso_key_gen' 公用程式所產生的金鑰，會列出網路社群加入網域所使用的金鑰，其中包括 WebSEAL 伺服器的執行網域，並採用「依網域配對」方式共享，即項目的設定格式爲「網域名稱 = 金鑰檔」。

    [e-community-domain-keys]

    - in.ibm.com = /opt/pdwebrte/bin/ecsso.key

瞭解「認證用」(vouch-for) 符記：

- 此符記包含「認證用」成功或失敗狀態、使用者身分（若成功的話）、建立此符記的伺服器完整名稱、網路社群身分、以及建立時間。
- 有效「認證用」符記的持有者，可以使用此符記來建立伺服器階段作業（及一組認證），而不需特別在該伺服器上進行鑑別。
- 符記會使用共用的 Triple-DES 密鑰進行加密，因此能夠順利驗證其確實性。
- 加密的符記資訊並不會儲存在瀏覽器上，
- 且符記只能用來通行一次。接收端伺服器會使用此資訊，在其快取中建立使用者認證。伺服器則會在相同階段作業期間，使用這些認證來處理後續要求。
- WebSEAL 配置檔中會設定符記的使用期限（逾時），此值可能非常短（僅數秒），以避免遭受「重送攻擊」(replay attack)。

認證用符記的使用期限：

您必須考量加入網域之間的時間偏差。時間偏差是指加入網域中 Web 安全伺服器的相關系統時間差異。若差異接近 vf-token-lifetime 值，符記的實際使用期限就會大幅縮短。但若差異超過 vf-token-lifetime 值時，在某網域中有效的符記在其他網域中可能會無效。您應該視情況來調整 vf-token-lifetime。

然而，如果因爲時間偏差而必須設定較大的 vf-token-lifetime 值，將較爲容易遭受重送攻擊。在這種情況下，您應該考慮針對加入網域中的相關 Web 安全伺服器，並讓其系統時間維持同步。

瞭解網路社群 Cookie：

- 網路社群 Cookie 是 WebSEAL 伺服器所設定的網域專用 Cookie，儲存在使用者的瀏覽器記憶體中，並會隨著後續要求傳輸至相同網域中的其他 WebSEAL 伺服器。
- 網域專用 Ccookie 包含了「認證用」伺服器的名稱、網路社群身分、「認證用」伺服器的位置 (URL)、功能、及使用期限，但不包含使用者或安全資訊。
- WebSEAL 配置檔中會設定 Cookie 的使用期限（逾時）。遠端伺服器必須在使用期限內，提供使用者的「認證用」資訊。若超出 Cookie 使用期限，就會將使用者重新導至 MAS 進行再次鑑別。
- 關閉瀏覽器時，便會從記憶體中清除 Cookie。如果使用者在特定網域中登出，則網路社群 Cookie 會覆寫爲空白。這個動作可有效從瀏覽器移除 Cookie。

eCSSO 配置摘要 (WebSEAL)

情境實例：

- MAS WebSEAL 伺服器：
  - 主機名稱：mas.in.ibm.com
  - HTTP 埠：80

- HTTPS 埠：443

- 從屬 WebSEAL 伺服器：
  - 主機名稱：slave.in.ibm.com
  - HTTP 埠：80
  - HTTPS 埠：443

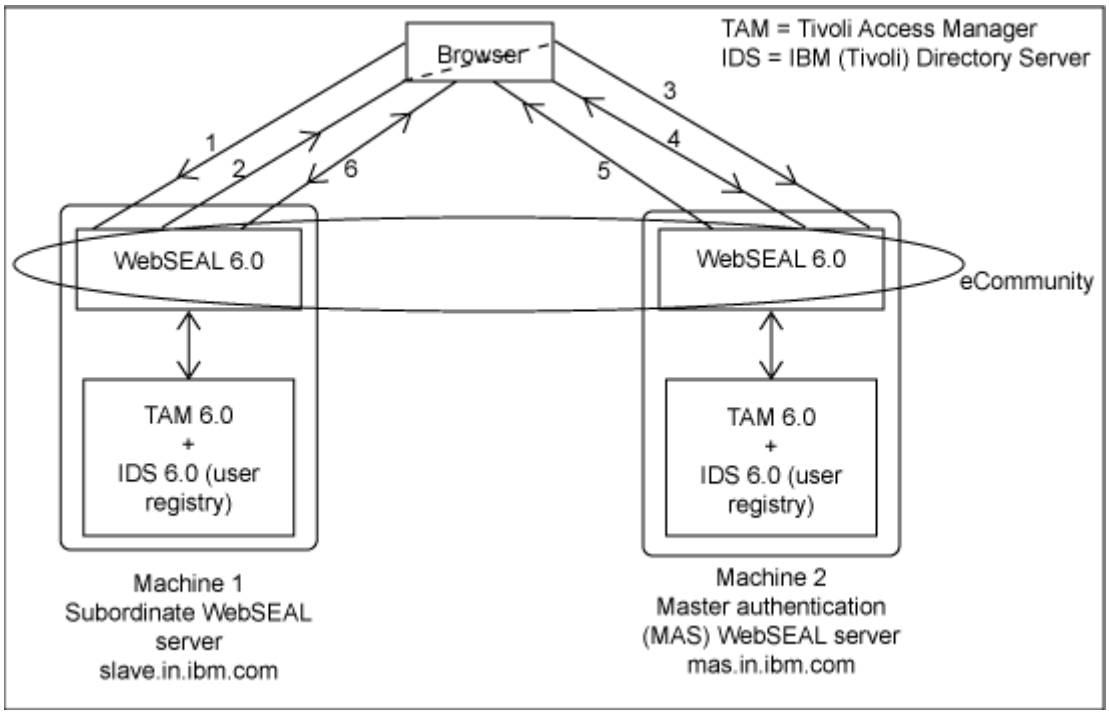
Webseald.conf (MAS)

- [forms]
  - forms-auth = https
- [authentication-mechanisms]
  - sso-create = /opt/pdwebrte/lib/libssocreate.so
- [e-community-sso]
  - e-community-sso-auth = https
  - e-community-name = ecomm
  - is-master-authn-server = yes
  - vf-token-lifetime = 180
  - vf-url = /pkmsvouchfor
  - vf-argument = PD-VF
  - ec-cookie-lifetime = 300
  - ecsso-allow-unauth = yes
  - use-utf8 = yes
- [e-community-domain-keys]
  - in.ibm.com = /opt/pdwebrte/bin/ecsso.key

Webseald.conf (Non-MAS)

- [forms]
  - forms-auth = https
  - [authentication-mechanisms]
  - sso-consume = /opt/pdwebrte/lib/libssoconsume.so
- [e-community-sso]
  - e-community-sso-auth = https
  - e-community-name = ecomm
  - is-master-authn-server = no
  - master-authn-server = mas.in.ibm.com
  - master-http-port = 80
  - master-https-port = 443
  - vf-token-lifetime = 180
  - vf-url = /pkmsvouchfor
  - vf-argument = PD-VF
  - ec-cookie-lifetime = 300
  - ecsso-allow-unauth = yes
  - use-utf8 = yes
- [e-community-domain-keys]
  - in.ibm.com = /opt/pdwebrte/bin/ecsso.key

運作方式：



1. 存取非 MAS（從屬）WebSEAL 所保護的資源：
   - https://slave.in.ibm.com/index.html
2. 從屬 WebSEAL 使用 'voucher' 要求，將使用者重新導至 MAS WebSEAL。
3. 瀏覽器轉遞 voucher 要求至 MAS。在步驟 1 按下 Enter 鍵之後，URL 就變更爲：
   - https://mas.in.ibm.com/pkmsvouchfor?ecomm&https://slave.in.ibm.com/index.html
4. 此時會顯示鑑別表單。若要進行鑑別，請提供在兩部伺服器登錄中共用的使用者名稱，以及特定使用者在 MAS（起始）網域中的密碼。此時使用者就完成鑑別，並會對映至一個「起始網域身分」。
5. 將建立一個認證用符記，且 MAS 會將使用者重新導至原本的（從屬）WebSEAL。
6. 瀏覽器會轉遞要求和認證用符記給原本的 WebSEAL，然後將使用者對映至「從屬網域身分」，再建立階段作業以處理要求。將提供受保護的頁面 'index.html'，且瀏覽器中的 URL 將變爲：
   - https://slave.in.ibm.com/index.html

PDWebPI 配置檔中的配置參數

若要編輯 PDWebPI 配置檔 'pdwebpi.conf'：

1. 解除 sso-create 和 sso-consume 項目的註解，然後新增作業系統適用的外掛失效接手 Cookie 程式庫名稱。
   在特定 PDWebPI 作爲 MAS 時，才可指定 sso-create 參數；在特定 PDWebPI 爲網路社群參與者時，才可指定 sso-consume 參數。

[authentication-mechanisms]

- sso-create = /opt/pdwebrte/lib/libssocreate.so
- sso-consume = /opt/pdwebrte/lib/libssoconsume.so

2. 配置檔中的 [common-modules] 段落，定義了所有鑑別方法的使用方式。若要讓外掛伺服器能在網路社群中運作，請在 authentication 和 pre-authzn 中指派 ecsso。當配置非 MAS 網路社群成員時，ecsso authentication 必須列在其他鑑別網目前面；也就是說，在鑑別模組清單中，必須先指定 ecsso，再指定其他鑑別網目。此外，如果有鑑別模組的鑑別層級高於預設值 1，則需優先於其他模組的 ecsso 模組，本身至少要指定爲與其相同的鑑別層級。

   [common-modules]

   - pre-authzn = acctmgmt
   - pre-authzn = ecsso
   - pre-authzn = forms
   - authentication = ecsso
   - authentication = forms
   - session = session-cookie

3. pdwebpi.conf 配置檔中的 [modules] 段落，定義了所有可用的鑑別機制，以及相關聯的共用程式庫名稱。必須確任網路社群 SSO 項目已存在：

   [modules]

   - ecsso = pdwpi-ecsso-module

4. 網路社群所有成員的 e-community-name 值必須相同。

   [ecsso]

   - e-community-name = ecommpdwebpi

5. 如果 is-master-authn-server 參數設定爲 'yes'，就必須解除 master-authn-server 參數的註解，並另行指定。此參數可指定網路社群 MAS 的完整網域名稱。請指定主要鑑別伺服器用來接收 HTTP 和 HTTPS 要求的埠號。如果埠號並非標準埠（http:80 和 https:443），就必須指定非標準埠號。

   [ecsso]

   - is-master-authn-server = yes

6. 如果 is-master-authn-server 參數設定爲 'no'，就必須解除 master-authn-server 參數的註解，並另行指定。此參數可指定網路社群 MAS 的完整網域名稱。請指定主要鑑別伺服器用來接收 HTTP 和 HTTPS 要求的埠號。如果埠號並非標準埠（http:80 和 https:443），就必須指定非標準埠號。

   [ecsso]

   - is-master-authn-server = no
   - master-authn-server = MAS 的 FQDN
   - master-http-port = MAS 的 http 埠號
   - master-https-port = MAS 的 https 埠號

7. 這些參數全部的預設值和說明皆爲 WebSEAL 中的資料相同。

   [ecsso]

- vf-token-lifetime = 180
- vf-url = /pkmsvouchfor
- vf-argument = PD-VF
- use-utf8 = true

8. 若使用者已執行登入但不成功，部署使用者名稱與密碼型鑑別網目的 MAS 可能會採取兩種方法：

   i. 提示使用者再次輸入認證，或
   ii. 立即將使用者重新導至原本試圖存取的伺服器，而不證明使用者身分。

   第二種做法是爲了強制使用者直接在從屬伺服器上進行鑑別。allow-login-retry 參數控制了 MAS 上的此項行爲。只有在 eCSSO 網路社群的 MAS 配置中，才可使用此參數。使用者可以嘗試重設過期密碼。在 MAS 上發生的其他登入失敗，如帳戶被鎖定，則無論 allow-login-retry 參數指定了什麼值，都會立即重新導至原本的從屬伺服器。依預設此參數設定爲 true。在本情境實例中，我們將此參數保留爲 'false'。

   [ecsso]

   - allow-login-retry = false

9. 配置檔 [ecsso-domain-keys] 的段落定義了金鑰檔位置，若要加密和解密 MAS 與遠端網域加入伺服器之間的符記，需要使用這些金鑰檔。配置 MAS 時，必須針對作爲主要伺服器的每個網域定義金鑰。配置非 MAS 的網路社群成員時，則必須定義用於網域和 MAS 的金鑰。您必須指定伺服器的完整網域名稱，以及金鑰檔位置的絕對路徑名稱。

   [ecsso-domain-keys]

   - in.ibm.com = /opt/pdwebrte/bin/ecsso.key

eCSSO configuration summary (PDWebPI)

情境實例：

MAS PDWebPI 伺服器：

- 主機名稱：mas.in.ibm.com
- MAS 保護的虛擬主機：
  - （**建議**：啓用 SSL，透過 https 進行存取）
    - mas.in.ibm.com:555
    - mas.in.ibm.com:666
    - mas.in.ibm.com:777
  - （未啓用 SSL，透過 http 進行存取）
    - mas.in.ibm.com:8080
    - mas.in.ibm.com:8081
    - mas.in.ibm.com:8082

從屬 PDWebPI 伺服器：

- 主機名稱：slave.in.ibm.com
- 從屬伺服器保護的虛擬主機：
  - （**建議**：啓用 SSL，透過 https 進行存取）
    - slave.in.ibm.com:555
    - slave.in.ibm.com:999
  - （未啓用 SSL，透過 http 進行存取）
    - slave.in.ibm.com:81
    - slave.in.ibm.com:82

pdwebpi.conf (MAS)

- [authentication-mechanisms]
  - sso-create = /opt/pdwebrte/lib/libssocreate.so
- [common-modules]
  - pre-authzn = acctmgmt
  - pre-authzn = ecsso
  - pre-authzn = forms
  - authentication = ecsso
  - authentication = forms
  - session = session-cookie
- [modules]
  - ecsso = pdwpi-ecsso-module
- [ecsso]
  - e-community-name = ecommpdwebpi
  - is-master-authn-server = yes
  - vf-token-lifetime = 180
  - vf-url = /pkmsvouchfor
  - vf-argument = PD-VF
  - allow-login-retry = false
  - use-utf8 = true
- [e-community-domain-keys]
  - in.ibm.com = /opt/pdwebrte/bin/ecsso.key

pdwebpi.conf (non-MAS)

- [authentication-mechanisms]
  - sso-consume = /opt/pdwebrte/lib/libssoconsume.so
  - [common-modules]
  - pre-authzn = acctmgmt
  - pre-authzn = ecsso
  - pre-authzn = forms
  - authentication = ecsso
  - authentication = forms
  - session = session-cookie
- [modules]
  - ecsso = pdwpi-ecsso-module
- [ecsso]
  - e-community-name = ecommpdwebpi
  - is-master-authn-server = no
  - master-authn-server = mas.in.ibm.com
  - master-http-port = 8080 //here, any port from 8080,8081,8082
  - master-https-port = 777 //here, any port from 555,666,777
  - vf-token-lifetime = 180
  - vf-url = /pkmsvouchfor
  - vf-argument = PD-VF
  - allow-login-retry = false
  - use-utf8 = true
- [e-community-domain-keys]
  - in.ibm.com = /opt/pdwebrte/bin/ecsso.key

運作方式：

運作方式與 WebSEAL 相同。

1. 存取從屬伺服器保護的物件：
   - https://slave.in.ibm.com:999/
     (MAS https port=777, Subordinate https port=999)
     或
   - http://slave.in.ibm.com:82/
     (MAS http port=8080, Subordinate http port=82)

2. 按下 Enter 鍵之後，將要求重新導至 MAS 進行鑑別，您將會看到 URL：
   - https://mas.in.ibm.com:777/pkmsvouchfor?ecommpdwebpi&https://slave.in.ibm.com:999/
     或
   - http://mas.in.ibm.com:8080/pkmsvouchfor?ecommpdwebpi&http://sla

ve.in.ibm.com:82/

顯示出鑑別表單。提供兩部伺服器登錄中共用的使用者名稱並順利登入之後，就會出現受保護 Web 伺服器的 index.html 頁面。顯示的 URL 可能如下：

- https://slave.in.ibm.com:999/?PD-VFHOST=mas.in.ibm.com&PD-VF=BAGs3DCBiQIBAQICAZoCAQICAQAEAAR4+P9LTzXDP6zq5ByZta55T+u6nPCe6g3JuJg1D/4zhKMP+RlGJL7TW5qophY1j0NYwxC26Q5a3pWdTlhQ76m/oNZSCNW3XOd9GxDTLB+qvVkpWrmKRyjOrV3llPOG8RBMO30/O6oWQgI2kMJBmYgPREDzb2AvR+9k
  或
- http://slave.in.ibm.com:82/?PD-VFHOST=mas.in.ibm.com&PD-VF=BAGs3DCBiQIBAQICAZoCAQICAQAEAAR4+P9LTzXDP6zq5ByZta55T+u6nPCe6g3Jw1yti3YVAD6dQdJz2U0QcezIr0fdd5ednuKNEuVGue6TO1Ysgy7I9V8J+ft7PP9TOcSrHD/O7/XB1ycYDjB6erOgjpo9Li/+9nVQlNqwAtHW/RrOgw0VPuZB152N0ljk

疑難排解

問題 1：當使用者存取從屬 WebSEAL 保護的資源時，要求使用者進行二次鑑別，無法只鑑別一次就存取。

1. 除錯：
   - 同時在 MAS 和從屬伺服器的 'webseald.conf' 檔中設定參數，然後重新啓動 WebSEAL 伺服器。
     - ba-auth = both
     - forms-auth = none

     同時在 MAS 和從屬伺服器的 'webseald.conf' 檔中設定上述兩個參數，然後重新啓動 WebSEAL 伺服器。
   - 存取從屬 WebSEAL 保護的資源。
   - 此時會要求您進行鑑別，首先是 MAS，之後是特定的從屬 WebSEAL。從基本鑑別蹦現視窗顯示的主機名稱，就能輕易發現這個問題。
2. 可能原因：
   - 若認證用符記在新網域（從屬 WebSEAL 的網域）無效，就可能發生這個問題。因爲從屬 WebSEAL 無法取得使用者的正確認證，因此會強制使用者再次進行鑑別。您可以讓參與 Web 安全伺服器的時間同步，使認證用符記的使用期限相對延長，即能解決這個問題。
   - 如果將 'cdsso_key_gen' 所產生的金鑰複製到其他 Web 安全伺服器時，金鑰遭到毀損，則用來加密和解密的金鑰已經不同，也就無法在從屬網域中正確解密符記資料。因此從屬 WebSEAL 將無法要求正確的使用者認證，導致使用者必

須在從屬網域中再次進行鑑別。重新產生金鑰，然後正確複製金鑰，就能解決這個問題。

3. 解決措施：
   - 同步化日期時，請使用指令 'date -u'（UNIX® 平台）來檢查日期，只使用 'date' 還不足夠。
     例如，在本情境實例中：
     - MAS:
       mas:~ # date
       Tue May 16 01:20:42 IST 2006
       mas:~ # date -u
       Mon May 15 19:52:39 UTC 2006
     - Subordinate:
       [root@slave ~]# date
       Tue May 16 01:21:33 IST 2006
       [root@slave ~]# date -u
       Mon May 15 19:52:41 UTC 2006
   - 'date -u' 輸出資料的所有欄位都必須相同，但不包括 'seconds' 部分。請使用相同指令 'date -u' 來修改日期：
     - Date -u MMDDhhmm (Month, Date, Hour, Minute)
   - 將日期同步之後，必須使用 'cdsso_key_gen' 公用程式來（重新）產生金鑰（在 MAS 上產生，並正確複製到加入 WebSEAL）。

問題 2：鑑別之後，瀏覽器出現粗體紅字的「找不到」錯誤訊息，而非顯示所需的受保護資源。

1. 除錯：
   - 這個錯誤發生在 eCSSO 運作方式步驟 4 之後。
   - 請檢查 MAS WebSEAL 的日誌檔，檔案位於 "/var/pdweb/log/msg__webseald-MAS.log"，其中可能會記錄下列錯誤：
     - DPWWA1993E Can't determine server domain name. Disabling e-community single-sign-on.
2. 可能原因：
   - 這個問題可能是主機名稱解析不當所導致。MAS 和從屬 WebSEAL 無法解析彼此的 FQDN。
3. 解決措施：
   - 若透過瀏覽器存取任何受保護資源，請務必使用所有 WebSEAL 伺服器的 FQDN， 切勿使用 IP 位址。
   - 檢查每部 Web 安全伺服器的主機名稱，以查看特定伺服器是否顯示 FQDN。請使用 "hostname --fqdn"（適用於 Linux）來進行這個動作，應該會傳回 Web 安

全伺服器的完整網域名稱。
例如，在本情境實例中：

- mas:~ # hostname
  mas
- mas:~ # hostname --fqdn
  mas.in.ibm.com

- 修改每部伺服器的 /etc/hosts 檔案，此檔案會顯示所有參與伺服器的 IP 位址與 FQDN。檢查 /etc/hosts 檔案的格式，
  例如，IP 位址 FQDN 短名稱
  - 9.XXX.YYY.31 slave.in.ibm.com slave
  - 9.XXX.YYY.52 mas.in.ibm.com mas
- 所有 WebSEAL 伺服器的這些 host 檔案必須使用相同格式。

問題 3：瀏覽器設定錯誤。

1. 可能原因：
   - 如果 MAS 未將瀏覽器重新導至原本所要求的 URL，且您的瀏覽器爲 Microsoft® Internet Explorer，則可能是網頁快取所導致的問題。
     在這種情況下，請配置瀏覽器，使其每次開啓儲存頁面時，都會檢查是否有較新版本。
2. 解決措施：
   - 工具 > 網際網路選項 > 一般 > Temporary Internet Files > 設定 >（選取）每次查閱畫面時。

問題 4：變更配置參數之後，無法啓動 WebSEAL 伺服器。

1. 除錯：
   - 檢查各個 WebSEAL 的日誌檔 "/var/pdweb/log/msg__webseald-XXX.log" 是否出現下列錯誤訊息：
     - DPWAD0454E Unable to configure the eCSSO authentication module for domain/host 'mas.in.ibm.com': status 0x13212075.
     - DPWWA1994E Disabling e-community single sign-on
     - DPWWA2079E Configuration of the SSO create and/or consume authentication module(s) failed: HPDIA0117E Can't select authentication mechanism.
     - DPWIV0164W Could not start background process .
2. 可能原因：
   - 未正確指定 sso-create 及/或 sso-consume 參數。
3. 解決措施：
   - 依照該特定 WebSEAL 伺服器所扮演的角色（MAS 或從屬伺服器），分別檢查這兩個配置參數設定（sso-create 或 sso-consume）。

sso-create 和 sso-consume 的共用程式庫會因平台而有所不同，請務必配置適當的程式庫。

問題 5：瀏覽器出現「無法顯示網頁」錯誤訊息，且瀏覽器中顯示的 URL 爲 "https://mas.in.ibm.com/pkmslogin.form"。

1. 除錯：
   - 這個錯誤發生在 eCSSO 運作方式步驟 4 之後。
   - 檢查 MAS WebSEAL 的日誌檔，其中可能會記載下列錯誤訊息：
     - DPWWA1990W The e-community name ecomm does not match the configured name ecomm1
     - DPWWA1978W Badly formed single sign-on URL
2. 可能原因：
   - 在加入 Web 安全伺服器中，可能未指定 'e-community-name' 參數，或此參數並非獨一無二。
3. 解決措施：
   - 檢查在加入 Web 安全伺服器的配置檔中，'e-community-name' 是否獨一無二。

問題 6：存取從屬 WebSEAL 保護的資源時，瀏覽器出現「無法顯示網頁」錯誤頁面。.

1. 除錯：
   - 這個錯誤發生在 eCSSO 運作方式步驟 1 之後。
2. 可能原因：
   - 從屬 WebSEAL 可能無法聯絡 MAS。
3. 解決措施：
   - 檢查從屬 WebSEAL 的配置檔，查看參數 'master-authn-server' 是否正確。
   - 檢查 Web 安全伺服器彼此之間是否能夠完成連線測試 (ping)，以及瀏覽器所在機器的 'hosts' 檔案是否已輸入所有 Web 安全伺服器項目。

問題 7：從屬 WebSEAL 不鑑別使用者，卻將使用者重新導至 MAS 以進行鑑別。

1. 除錯：
   - 瀏覽器無法如 eCSSO 運作方式步驟 3 所述，順利顯示重新導向 URL。
2. 可能原因：
   - 從屬 WebSEAL 可能無法透過指定的連接埠來聯絡 MAS。
3. 解決措施：
   - 檢查從屬 WebSEAL 的配置檔中，參數 'master-http-port' 和 'master-https-port' 是否正確。
   - 檢查從屬伺服器的 /etc/hosts 檔案，其輸入項目的格式應如問題 2 矯正措施 3 所述，爲「IP 位址 FQDN 短名稱」。

WebSEAL 追蹤

下列方法可以啓用 WebSEAL 追蹤：

- 使用檔案 '/opt/pdweb/etc/routing' 來取得追蹤輸出資料。您可以解除 'routing' 檔案最後一行的註解，來取得預設目錄 '/var/pdweb/log' 中的追蹤日誌檔。您可以選擇要取得所有 TAM 元件或特定元件的追蹤資料。
- 啓用元件追蹤（如 'pdweb.debug' 或 'pdweb.snoop'）之後，也可以取得要求和回應流程資訊。您可以透過 pdadmin 指令行來啓用這些追蹤功能：

下列擷取資料來自結合了 MAS 和從屬機器的 'pdweb.debug' 追蹤：

1. 要求（瀏覽器 ==> PD）:
    - GET / HTTP/1.1
    - host: slave.in.ibm.com

   回應（瀏覽器 <== PD）:
    - HTTP/1.1 302 Moved Temporarily
    - location: https://mas.in.ibm.com/pkmsvouchfor?ecomm&https://slave.in.ibm.com/
2. 要求（瀏覽器 ==> PD）:
    - GET /pkmsvouchfor?ecomm&https://slave.in.ibm.com/ HTTP/1.1
    - host: mas.in.ibm.com

   回應（瀏覽器 <== PD）:
    - HTTP/1.1 200 OK
3. 要求（瀏覽器 ==> PD）:
    - POST /pkmslogin.form HTTP/1.1
    - host: mas.in.ibm.com
    - referer: https://mas.in.ibm.com/pkmsvouchfor?ecomm&https://slave.in.ibm.com/

   回應（瀏覽器 <== PD）:
    - HTTP/1.1 302 Moved Temporarily
    - location: https://mas.in.ibm.com/pkmsvouchfor?ecomm&https://slave.in.ibm.com/
4. 要求（瀏覽器 ==> PD）:
    - GET /pkmsvouchfor?ecomm&https://slave.in.ibm.com/ HTTP/1.1
    - host: mas.in.ibm.com
    - referer: https://mas.in.ibm.com/pkmsvouchfor?ecomm&https://slave.in.ibm.com/

   回應（瀏覽器 <== PD）:

- HTTP/1.1 302 Moved Temporarily
- location: https://slave.in.ibm.com/?PD-VFHOST=mas.in.ibm.com&PD-VF=BAGs3DCBiQIBAQICAZoCAQICAQAEAAR4Ooqw+2wG/B48RFitmIsow0bGC+f4kHUk4/teEksl2aw9NILcxanvC1pkInkbd8Lb8QxRE4ufsG YMfYuMR8JesNQ7OG8SOnd/B97FWghLxn6gaMkDj4yzkdakJk2igEjB/qQR6rFgrzEduJ+QVdzaqlDHEV0xaGrJ

5. 要求（瀏覽器 ==> PD）：
   - GET /?PD-VFHOST=mas.in.ibm.com&PD-VF=BAGs3DCBiQIBAQICAZoCAQICAQAEAAR4Ooqw+2wG/B48R FitmIsow0bGC+f4kHUk4/teEksl2aw9NILcxanvC1pkInkbd8Lb8QxRE4ufsGYMfYuMR8JesNQ7OG8SOnd/B97FWghLxn6gaMkDj4yzkdakJk2igEjB/qQR6rFgrzEduJ+QVdzaqlDHEV0xaGrJHTTP/1.1
   - host: slave.in.ibm.com
   - referer: https://mas.in.ibm.com/pkmsvouchfor?ecomm&https://slave.in.ibm.com/

   回應（瀏覽器 <== PD）：
   - HTTP/1.1 302 Moved Temporarily
   - location: https://slave.in.ibm.com/

6. 要求（瀏覽器 ==> PD）：
   - GET / HTTP/1.1
   - host: slave.in.ibm.com
   - referer: https://mas.in.ibm.com/pkmsvouchfor?ecomm&https://slave.in.ibm.com/

   回應（瀏覽器 <== PD）：
   - HTTP/1.1 200 OK

擷取的輸出資料只會顯示這些 HTTP 標頭的屬性，這些標頭都是進行 eCSSO 配置除錯的重點。編號 1、5 和 6 的追蹤資料會記載在從屬 WebSEAL 伺服器上指定的追蹤日誌檔，編號 2、3 和 4 的追蹤資料則會記載在 MAS 上指定的追蹤日誌檔。HTTP 要求標頭的 'host' 屬性，指明了要求會重新導至哪部 WebSEAL 伺服器。上面所列的要求與回應流程，則是在使用 eCSSO 配置順利存取資源時，用來指明完整的後續動作。若使用 eCSSO 設定來存取資源卻發生問題，可以參考上述後續動作以找出失敗原因。

作者簡介

	Vinayak Kawathekar 主修電腦科學，已完成工學士學位。擔任 IBM 軟體工程師已有三年時間，並致力於發展 Tivoli Security 產品系列。