Tivoli Access Manager 環境裡的 Tivoli Directory Proxy Server：管理與疑難排解 Tivoli Access Manager 環境裡的 TDS 6.0 Proxy Server

等級：中級

Sunil K. Verma (sunverma@in.ibm.com)，IBM 印度系統軟體工程師
Varsha Sogani (varsha_sogani@in.ibm.com)，IBM 印度軟體實驗室系統軟體工程師

2008 年 3 月 24 日

假如您是在軟體產業工作，都很可能聽說過 LDAP 目錄伺服器。輕量型目錄存取通訊協定 (LDAP) 針對目錄的資訊存取及更新，定義了標準方法，使用將讀取權最佳化的主從架構模型來存取目錄。IBM® Tivoli® Access Manager (TAM) 使用 LDAP 目錄伺服器做爲使用者登錄，以儲存使用者與群組資訊。Tivoli Directory Server (TDS) Server 是隨 TAM 出貨的預設 LDAP 目錄伺服器。TDS 伺服器可配置爲後端伺服器，或者做爲 Proxy 伺服器。本文將讓您瞭解 TAM 如何運用 TDS Proxy 伺服器，同時也會提供建議，協助您管理及疑難排解 TAM 環境裡的 TDS Proxy 伺服器。

前言

TDS Proxy Server 是特殊類型的目錄伺服器，位於配送目錄的前端，提供有效率的要求遞送。TDS Proxy Server 會配置後端伺服器的連線資訊，並爲用戶端提供統一檢視 (TAM/WebSEAL)。TAM 提供統一的安全服務集，包括鑑別、授權、審核和記載。TAM WebSEAL 是多執行緒 Web 伺服器，可爲 TAM 保護的 Web 資源套用精細的安全原則。

本文針對 TAM 環境裡的 TDS Proxy Server，說明以下相關領域：

- 瞭解在 TAM 環境裡使用 TDS Proxy Server 的優點
- 瞭解「廣域管理群組」(Global Administration Group)
- 爲 TDS Proxy Server 配置失效接手和負載平衡
- 在網路架構放置 TDS Proxy Server
- 驗證 Access Manager 環境裡的 TDS Proxy Server
- 管理 TDS Proxy Server
- 部分已知問題、供 Proxy 使用的修正程式及 TechNotes
- 疑難排解 TDS Proxy Server
- TDS Proxy 6.1 的新增功能
- 總結

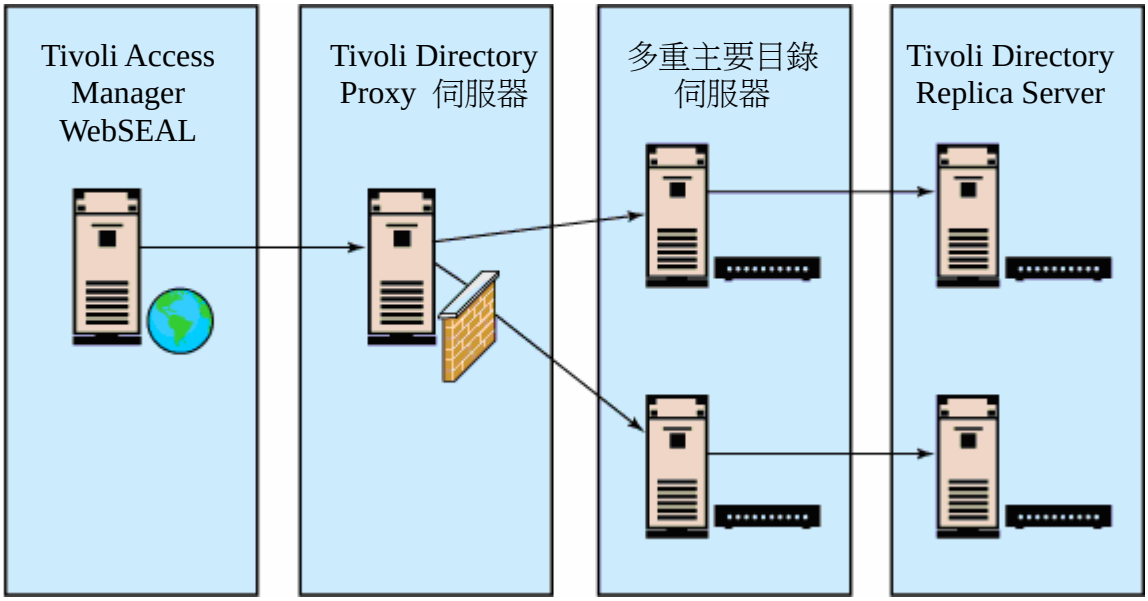
TDS Proxy Server 和 TDS 後端伺服器之間的差異：

- TDS Proxy 並未配置資料庫；後端伺服器擁有關聯資料庫。
- TDS Proxy 無法參與抄寫，但標準的後端伺服器則可以做到。

瞭解在 TAM 環境裡使用 TDS Proxy Server 的優點

在 TAM 環境裡，TDS Proxy Server 位於後端伺服器及用戶端（例如：WebSEAL Policy Server）之間，如圖 1 所示。

圖 1：



TDS Proxy Server 提供要求遞送、負載平衡、失效接手及分散式鑑別等功能，其優點如下：

- 可輕鬆配送及管理大量資料

TAM 需要儲存大量使用者資料時，配送及管理資料是最重要的考量。運用 TDS 的 Proxy 功能，即可在多個後端伺服器上配送大量資料，並且輕鬆進行管理。

- TDS Proxy Server 的要求遞送功能可提高效能

可以在分散式環境中，執行有效率的用戶端要求遞送，根據本身擁有的分割區資訊，將要求配送給分散式後端伺服器。Proxy 知道資料的配送方法，也知道如何讓 Proxy 從後端伺服器提取所要求的資料，再轉送至 WebSEAL 用戶端。對 WebSEAL 而言，Proxy 和後端目錄伺服器之間的互動是無形的。

- 使用 Proxy Server 達成延展性

客戶對目錄伺服器的需求隨時間不斷變化，目前，可儲存數千個登錄的目錄伺服器，在五年後將可儲存數以百萬計的登錄。在單一目錄伺服器上儲存數百萬個登錄並不容易，且可能降低效能，也會帶來硬體延展的問題。在這個情況下，Proxy Server 可因應這些效能及延展性的問題。

- 失效接手及負載平衡

Proxy 伺服器也可以做爲負載平衡器或失效接手管理器。雖然 TAM 本身擁有失效接手功能，且該功能已使用可用的 LDAP 後端伺服器，但 TDS Proxy Server 失效接手可提高效能與穩固性。請記住，Proxy 是爲讀取要求執行負載平衡，並爲更新要求執行失效接手。

- 高可用性

在 Proxy 伺服器之間採用失效接手，可避免單一失效點，從而確保高可用性。

瞭解廣域管理群組

使用者最常遇到的問題，是使用 admin DN (cn=root) 連結 TDS Proxy Server 時無法修改目錄資料。雖然 cn=root 是 Proxy 和後端伺服器的 admin DN（配置 Proxy 和後端伺服器時將 cn=root 設定爲 admin DN），但以 cn=root 連結 TDS Proxy 時，使用者僅是 Proxy 伺服器的管理者，而不是後端伺服器的管理者。這時，對後端伺服器而言，該使用者是匿名的。假如使用者以 cn=root 身分連結 Proxy 伺服器，並試圖修改後端伺服器登錄時，該使用者將遇到「Insufficient access」（存取權不足）的錯誤。換言之，cn=root 身分只能變更 Proxy 伺服器配置，而存取也僅限於擁有匿名存取權的端目錄登錄。

廣域管理群組就是用來確保，透過 Proxy 修改後端伺服器登錄時，能擁有正確的管理者專用權，存取後端伺服器。需要特別注意的是，即使您以廣域管理群組身分連結 Proxy，您並不具有下列專用權或：

- 後端伺服器配置設定的存取權
- 任何綱目資料的存取權
- 審核日誌的存取權 因此，本端管理者 cn=root 可以爲了安全目的，使用審核日誌來監控廣域管理群組成員的活動。

在 Proxy 環境裡，可於後端伺服器定義廣域管理群組，爲使用者提供管理權。TAM WebSEAL 並不會察知廣域管理群組。

爲廣域管理群組新增使用者的步驟

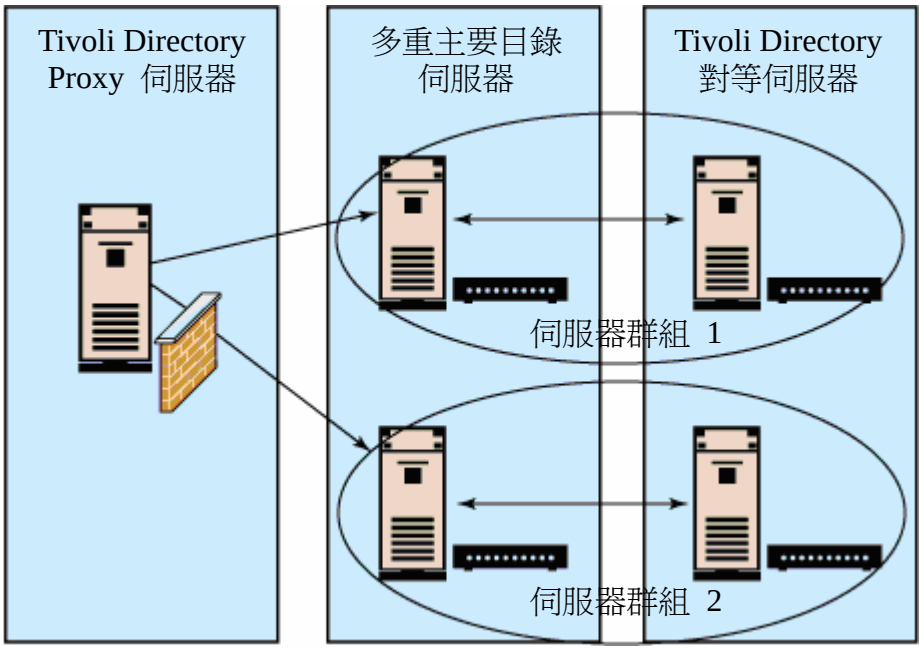
```
# idsldapadd -h hostname -p port_no -D cn=root -w root -f LDIF1
# idsldapadd -h hostname -p port_no -D cn=root -w root -f LDIF2

where LDIF1 contains:                    and where LDIF2 contains:
dn: cn=manager,cn=ibmpolicies   dn: globalGroupName=GlobalAdminGroup,cn=ibmpolicies
objectclass: person             changetype: modify
sn: manager                              add: member
cn: manager                              member: cn=manager,cn=ibmpolicies
userpassword: secret
```

Proxy 提供失效接手、負載平衡和高可用性

如前所述，TDS Proxy Server 可以做爲失效接手代理站，且能夠執行用戶端要求的負載平衡。Proxy 可察知指定分割區的所有主要伺服器，而且須使用其中之一個伺服器做爲最主要伺服器 (primary master)；在分割區資訊中找到的第一部主要伺服器，將選爲最主要伺服器。假如最主要伺服器因故關閉，Proxy 即可讓備用伺服器（對等伺服器）進行失效接手。

如果 Proxy 在啓動時無法連結一或多部後端伺服器，則 Proxy 只能以配置模式啓動，直到設定了伺服器群組。伺服器群組是在 Proxy 伺服器上定義的，用以從數部對等伺服器中取得至少一部線上後端伺服器，若群組中一或多部後端伺服器因故關閉時，Proxy 仍能繼續作業。根據圖 2，您可以輕鬆預想到伺服器群組 1 具有前兩部目錄伺服器，而伺服器群組 2 則由另外兩部目錄伺服器所組成；每個伺服器群組都擁有一部主要伺服器及一部對等伺服器。因此，若伺服器群組 1 的主要伺服器因故關閉，或無法使用時，Proxy 即可讓相同伺服器群組中的另一部對等伺服器進行失效接手。假如目前的線上伺服器無法執行所要求的作業，Proxy 伺服器將會回覆作業錯誤。

圖 2：



附註：
爲了獲得更好的效能，所有 TDS 後端伺服器和 TDS Proxy Server 應共用相同的關鍵隱藏檔。

TDS Proxy 上線後，會查詢每部後端伺服器的抄寫拓蹼，後端伺服器如果是指定分割區子樹狀結構中的主要伺服器，都將新增至 Proxy 的「可寫入」清單，而其他的後端伺服器則會新增至「可讀取」清單。爲了免於解決衝突，Proxy 會採用第一部「可寫入」伺服器，並且將所有更新要求傳送至該伺服器，直到該伺服器離線爲止。伺服器離線時，Proxy 將自動讓下一部可用的「可寫入」伺服器進行失效接手，並且繼續採用直到失效爲止。

附註：
在負載平衡的 Proxy 環境裡，若 Proxy 伺服器發生失效，傳送給它的第一個作業將會失敗，並回覆錯誤，所有後續作業將改傳至失效接手的 Proxy 伺服器。發生失敗的第一個作業將可以重試，但作業不會自動傳送至失效接手的伺服器。

Proxy 也察知指定分割區中的所有抄本，而且能爲線上抄本之間的讀取要求執行負載平衡。Proxy 將爲讀取要求執行負載平衡，另爲更新要求執行失效接手。Proxy 可傳送更新要求和讀取要求至適當的讀取／寫入伺服器和唯讀伺服器。

TDS Proxy 也可以傳送服務要求至尚未配送的目錄，但這些目錄必須是 TDS 6.0 的目錄，而且必須針對子樹狀結構，爲 Proxy 提供相關的分割點資訊。其中的技巧是設定多個分割點，但分割點僅可擁有一個分割。客戶的現行環境可能已安裝了 TDS 後端伺服器和抄寫伺服器設定，因此只需要負載平衡，而不需要資料配送。在這種情況下，採用 Proxy 伺服器可爲要求

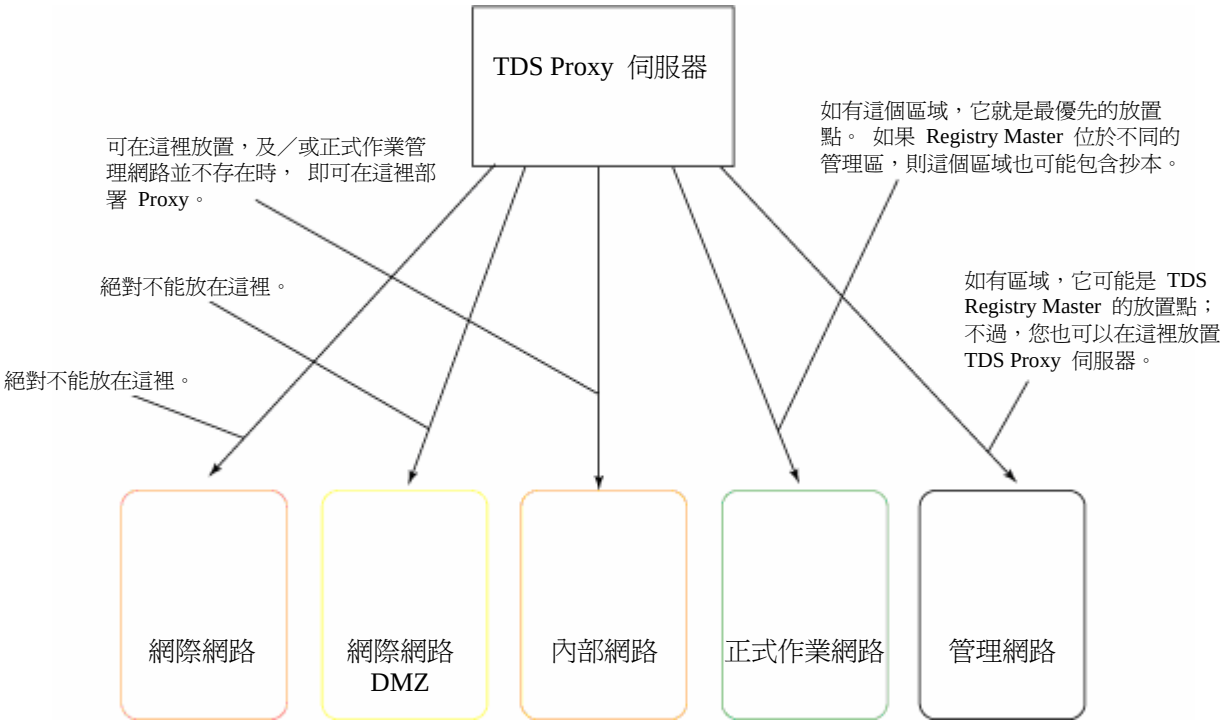
執行負載平衡，並提高效能。

Proxy 的高可用性：如有需要，可以使用負載平衡器，爲失效接手設定 TDS Proxy Server，以獲得高可用性，並解決單一失效點的問題。IBM WebSphere® Edge Server 之類的負載平衡器可以在 Proxy 伺服器之間，平衡 LDAP 讀取／寫入要求。負載平衡器經配置之後，僅傳送這些要求給一部 Proxy 伺服器。假如 Proxy 伺服器因網路故障而關閉或無法使用，負載平衡器將傳送要求給下一部可用的 Proxy 伺服器，直到第一部 Proxy 伺服器恢復可用爲止。此外，TDS Proxy Server 不能堆疊串接，即每部 Proxy 不能位於另一部 Proxy 之後，且不能向其後之 Proxy（位於另個網路區）遞送要求，由第二部 Proxy 遞送要求給後端伺服器。

在網路架構放置 TDS Proxy Server

本節將探討如何在網路架構下放置 TDS Proxy 伺服器。由於 WebSEAL 僅能察知 Proxy，而且沒有資訊可供後端伺服器使用，因此，WebSEAL 將與 TDS Proxy Server 互動以執行 LDAP 作業，而不是與 TDS 後端伺服器互動。這表示，TDS Proxy Server 必須可供 WebSEAL 存取，但不應透過網際網路存取，如圖 3 中的說明，網際網路屬於「非控制區」，網際網路 DMZ 和內部網路屬「控制區」，「正式作業網路」屬於「限制區」，而「管理網路」屬於「安全區」。

圖 3：



這些是 Proxy 伺服器可能方置的方式：

- Proxy 伺服器不應放置於「網際網路非控制區」。

- Proxy Server 絕對不能放置於「網際網路 DMZ 控制區」。
- 假如沒有正式作業或管理網路，則 Proxy Server 可以部署在「網際網路控制區」。
- 如有「正式作業」網路區，則這是最優先的 Proxy Server 放置點。
- 管理區是主要後端伺服器的邏輯放置點；不過，Proxy Server 也可以放置在這裡。

TDS Proxy Server 可以跨中繼網路區執行要求，例如，將屬於 DMZ 的 TDS 用戶端（此爲 WebSEAL）與屬於管理區或正式作業區的 TDS 後端伺服器及資料庫連結起來，兩者之間存在數個中繼網路區。

驗證 Access Manager 環境裡的 Proxy

於 TAM 環境安裝 Proxy 之後，我們建議您要驗證 TDS Proxy 和 Policy Server。在 Access Manager 環境驗證 Proxy 和 Policy Server 的基本步驟包括：

1) 驗證 TDS Proxy

a) 驗證 Proxy 是否已啓動和執行

```
# ibmdirctl -D <admin-dn> -w <admin-pwd> status
```

b) 在 Proxy 上爲後端伺服器的現有登錄執行 ldapsearch

```
#ldapsearch -D <Global_AdminGroup_member> -w <password> -p <port> -s sub -b "" \
objectclass=*
```

c) 透過 Proxy 新增登錄，並驗證後端是否已新增該登錄

```
# ldapadd -h <hostname> -D <Global_AdminGroup_member> -w <password> -p <port> -i \
<add.ldif>
where ldif file contains :
dn: cn=sunil,o=ibm,c=us
objectclass: person
cn: Sunil
sn: Verma
userpassword: password
-
dn: cn=sunil,cn=Users,secAuthority=default
objectclass: person
cn: Sunil
sn: Verma
```

```
userpassword: password
```

d) 在 Proxy、後端伺服器和抄本上使用 ldapsearch 進行檢查，以確保後端已適當新增登錄

```
Run below ldapsearch on proxy, master and replica server as well :
# ldapsearch -h <hostname> -D <Global_AdminGroup_member> -w <password> -p <port> -s sub \
-b "cn=sunil,o=ibm,c=us" objectclass=*
# ldapsearch -h <hostname> -D <Global_AdminGroup_member> -w <password> -p <port> -s sub \
-b "cn=sunil,cn=Users,secAuthority=default" objectclass=*
```

假如設定 Proxy 時，使用包含兩部主要後端伺服器的子樹狀結構型分割，則可以透過 Proxy 的子樹狀結構，新增一個測試登錄來進行驗證。例如，在一部後端伺服器上定義 o=ibm,c=us，並且在另一部伺服器上定義 secAuthority=default。在這兩部後端伺服器上應同時針對新增的登錄執行下一個 ldapsearch，以檢查是否已適當新增登錄。在主要伺服器上搜尋登錄之後，在抄本伺服器上應執行相同搜尋，以檢查登錄是否已抄寫。

在設置了 RDN 和雜湊型分割的情況下，登錄可新增至任何依賴雜湊演算法的伺服器，因此應在後端伺服器和抄本伺服器上執行搜尋以驗證 Proxy。

2) 驗證 Policy Server

a) Policy Server 是否已啓動和執行

```
# pd_start status
```

b) 檢查 ldap.conf 檔中的 Proxy 明細

```
--ldap.conf--
[ldap]
ldap-server = proxy IP Address
-------------
```

附註：ldap.conf 檔案應指向 Proxy，而不是後端伺服器或抄本伺服器

c) 登入 pdadmin

```
# pdadmin -a sec_master -p password
```

這是驗證的第一步，接下來即可執行指令以驗證環境，例如，運用使用者清單指令列出使用者。

d) 使用 pdadmin 新增使用者

```
# pdadmin> user create varsha cn=varsha,o=ibm,c=us Varsha Sogani
password
```

e) 檢查 Proxy 和後端抄本是否已新增登錄

```
# ldapsearch -h <hostname> -D <Global_AdminGroup_member> -w <password> -p <port> -s sub \
-b "cn=varsha,o=ibm,c=us" objectclass=*
# ldapsearch -h <hostname> -D <Global_AdminGroup_member> -w <password> -p <port> -s sub \
-b "cn=varsha,cn=Users,secAuthority=default" objectclass=*
```

管理 TDS Proxy

在 TAM 環境裡放置 TDS Proxy 並不表示無需調整後端伺服器。Tivoli Directory Server 是 LDAP 目錄，可在 DB2® 之上提供資料層，讓使用者有效率地組織、操作及擷取儲存於 DB2 資料庫的資料。若要調整最佳效能，最主要的關鍵在於根據工作量的本質，調整 LDAP 伺服器和 DB2 之間的關係。

下列手冊提供 IBM Tivoli Directory Server 及相關 IBM 資料庫的調整資訊。

調整手冊：*Performance Tuning Guide（效能調整手冊）*

IBM Redbooks®：*Performance Tuning for IBM Tivoli Directory Server（IBM Tivoli Directory Server 的效能調整）*

1) Proxy 的綱目管理

Proxy 完成配置後，其配置本身的綱目。Proxy 伺服器應擁有與後端伺服器相同的綱目定義，因爲 Proxy 伺服器.. 可同步處理 Proxy 伺服器與後端伺服器的綱目，已修改的綱目檔應從後端伺服器（例如：V3.modifiedschema）複製到 Proxy 伺服器。

附註：所有後端伺服器的綱目檔也應同步化。

2) 配置和綱目檔備份

資料庫或任何其他檔案若有備份程序，建議同時備份 ibmslapd.conf 和綱目檔。除了資料庫備份之外，配置和綱目檔也應及時備份，以在發生失效時，能夠再次適當配置 LDAP 伺服器。

部分已知問題、供 Proxy 使用的修正程式及 TechNotes

WebSEAL 配置使用 TDS Proxy Server 時，您可能會遇到一些問題。爲了在 TAM 環境裡使用 TDS Proxy Serve，我們建議 TDS Proxy 至少應該採用 Fix Pack Level 2 (FP02)。下列是目前已知的問題：

1) 配置 WebSEAL 使用 Tivoli Directory Server Proxy Server 6.0 時，WebSEAL 無法鑑別使用者。

WebSEAL 配置使用 TDS Proxy Server 時，您可能會遇到鑑別問題。最常見的問題是，配置 WebSEAL 使用 Tivoli Directory Server Proxy Server 6.0 時，WebSEAL 無法鑑別使用者，使用者可以成功連結 TDS Proxy 及主要 LDAP 伺服器，例如，使用者「sunil」可以連結 TDS Proxy 伺服器和主要後端伺服器的 「idsldapmodify -D cn=sunil,O=IBM,C=US -w password」。若要檢查特定的鑑別問題，首先要收集 IRA 追蹤資料。IRA 追蹤資料是從 WebSEAL 機器上收集的 LDAP 用戶端追蹤資料，用以尋找 LADP 回覆碼，協助找出問題原因。在此情況下，ldap_compare 如同預期順利執行，而 ira_cache_user_get_groups returns 'd2', 則指出使用者不屬於任何群組。

IRA 追蹤資料

```
2006-01-11-14:02:53.683+11:00I----- thread(3) trace.pd.ivc.ira:8 /project/am600 \
/build/am600/src/ivrgy/ira_cache.c:2092: CII EXIT
ira_cache_user_get_groups() with status:    0x000000d2
```

對主要後端伺服器和 Proxy 執行下列搜尋，以取得使用者的群組成員資格。搜尋結果差異甚大，說明如下：

```
# idsldapsearch -D cn=root -w password -h hostname -p port_no -b "cn=sunil,O=IBM,C=US" \
"objectclass=*" ibm-allgroups
LDAP Master Returned:
cn=sunil,O=IBM,C=US
LDAP Proxy Returned:
Did not return anything!
```

配置 WebSEAL 使用 LDAP Proxy 時，使用者鑑別作業可能會失敗，原因是無法順利完成 LDAP 搜尋，判定使用者的群組成員資料。當使用者新增至群組時，WebSEAL 鑑別即可順利執行。此外，新增使用者至群組後再次執行搜尋，即可成功執行 LDAP 搜尋，而 WebSEAL 鑑

別也可以順利執行。這是 TDS 6.0 中的錯誤，已透過 APAR IO03861 修正。

APAR IO03861：若要求 ibm-allGroups，Proxy 並未回覆 DN。這個測試已順利完成。我們可以驗證，沒有群組成員資格的使用者，現可透過指向 LDAP Proxy 的 WebSEAL 登入。用戶端要求 ibm-allGroups 屬性時，Proxy 不會回覆任何資料，對於不屬於任何群組的使用者而言，確實如此，但屬於某個群組成員的使用者，Proxy 將會回覆正確的 DN。不過，如果使用者並非任何群組的成員時，將不會回覆 DN，Proxy 必須回覆該使用者的 DN。

2) TDS 後端伺服器因故關閉時，TDS Proxy 伺服器並未讓其他可用的 TDS 後端伺服器執行失效接手。

TDS 後端伺服器機器因故關閉時，WebSEAL 未能從 Proxy 伺服器收到回應，原因是 Proxy 並未讓其他可用的 TDS 後端伺服器執行失效接手。在此種情況下，WebSEAL 使用者將無法執行鑑別。此外，使用 Policy Server 執行的使用者供應也將暫停，直至 Proxy 讓可用的後端伺服器執行失效接手。

6.0 版中的 TDS 失效接手是在後端伺服器關閉或停止執行時，用來處理異常狀況，但如果網路失效，TDS 將不會執行失效接手。假如 TDS 後端伺服器關閉，Proxy 上所有開啓的 Socket 將從 TCP 層取得 FIN 封包，Proxy 因此可以總結後端伺服器程序已關閉。

如果後端伺服器機器從網路離線或因故關閉，Proxy 上的 TCP 堆疊將不會從事件的後端伺服器獲得資訊，繼續等待（Proxy 程序也會因而繼續等待）。TCP 堆疊已有方法解決這類低階問題。TCP 是用來在網際網路上，做爲可靠的通訊協定，因此能夠解決網路層的問題，諸如不當的主機或路由器（預期會由 OSPF 尋找替代路由器以解決問題），其預設逾時是 7200 秒或兩小時。

驗證 TCP 逾時後會執行 TDS 失效接手：在保留作用中逾時後，TDS Proxy 伺服器具有回應力，且會列印錯誤訊息，在 TCP 逾時後則執行失效接手。以下是變更 tcp_keepalive_* 設定的方法（適用於 Linux®）。

```
# cd /proc/sys/net/ipv4
# ls -la tcp_keepalive_*
-rw-r--r--    1 root root 0 Nov 24 22:57 tcp_keepalive_intvl
-rw-r--r--    1 root root 0 Nov 24 22:57 tcp_keepalive_probes
-rw-r--r--    1 root root 0 Nov 24 22:57 tcp_keepalive_time
# echo 5 > tcp_keepalive_intvl
# echo 2 > tcp_keepalive_probes
# echo 15 > tcp_keepalive_time
```

3) 使用 W Webadmin GUI 來管理 Proxy 的密碼原則時，不同環境會出現不同行爲。

a) 如果在 Proxy 的 ibmslapd.conf 檔中僅定義一個 cn=pwdPolicy 分割（如下所示），則連結 Proxy 伺服器時，webadmin 不會隱藏 pwdpolicy 登錄：

```
dn: cn=pwdpolicy split, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory, cn=Schemas, \
cn=Configuration
cn: pwdpolicy split
ibm-slapdProxyNumPartitions: 1
ibm-slapdProxyPartitionBase: cn=pwdpolicy
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplitContainer

dn: cn=split1, cn=pwdpolicy split, cn=ProxyDB, cn=Proxy Backends, cn=IBM Directory,\
cn=Schemas, cn=Configuration
cn: split1
ibm-slapdProxyBackendServerDN: cn=Server1,cn=ProxyDB,cn=Proxy Backends, cn=IBM \
Directory, cn=Schemas,cn=Configuration
ibm-slapdProxyPartitionIndex: 1
objectclass: top
objectclass: ibm-slapdConfigEntry
objectclass: ibm-slapdProxyBackendSplit
```

b) 透過 Webadmin GUI 使用 cn=root 或其他使用者身分連結 Proxy 伺服器，且試圖執行變更時，您會從伺服器收到存取權不足的錯誤訊息，這情況是正確的。若要執行變更，您應使用廣域管理群組成員身分登入。

4) 若使用「idsslapd」指令啓動 Proxy Server 實例，Proxy 無法載入正確的程式碼或執行環境，而且無法適當運作。無法精確預測結果。

您可以使用「ibmslapd」指令或「idsslapd」別名啓動 TDS 6.0 伺服器，這兩個指令都可以在 /opt/IBM/ldap/V6.0/sbin 中執行 「包裝器 script」，爲伺服器實例起始環境並載入應用程式碼，取決於是一般的「RDBM」伺服器或「PROXY」伺服器。指令應該是相同的，然而，在「idsslapd」包裝器 (wrapper) script 中出現錯誤，以致無法爲 PROXY 伺服器實例載入正確的程式碼。

這個問題的暫行解決方法，是使用的副本或 V6.0/sbin/idsslapd 的 sym-link 取代

V6.0/sbin/ibmslapd script ，或者改用「ibmslapd」指令。

這個問題已在 APAR IO06919 中修正。

5) Proxy 的 APAR 修正

- IO07536：[僅 AIX®] 來自 openldap 用戶端的匿名 DIGEST-MD5 連結可能損毀 AIX 上的 TDS 6.0 Proxy Server
- IO07309：[僅 Linux] 在特許埠啓動 Proxy 時發生 GLPCOM027E 錯誤
- IO06919：[僅 AIX] 啓動 Proxy 伺服器實例時發生 GLPWRP002E 錯誤
- IO06918：使用「idsslapd」指令啓動 PROXY 伺服器時出現不穩定
- IO06323：Proxy 伺服器可能當機（死鎖）
- IO05509：後端伺服器關閉時，Proxy 伺服器核心異常終止
- IO05748：若啓用追蹤，Proxy 在執行 Compare（比較）作業時發生異常終止
- IO05579：Proxy 伺服器按每個作業洩漏 48 位元組
- IO05508：更正 Proxy supportedcontrol 和 ibm-supportedcapabilities
- IO05269：審核作業 ID 以對映 Proxy 要求和後端作業
- IO05276：Proxy 伺服器洩漏處理修改作業的記憶體
- IO05287：Proxy 伺服器在執行連結作業時，可能異常終止
- IO05261：若後端伺服器關閉，Windows® 上的 Proxy Server 大量耗用 CPU
- IO05092：「ldap_delete: operations error」刪除 Proxy 伺服器上的登錄
- IO05040：透過 Proxy 執行 Delete（刪除）或 modrdn 時可能回覆 LDAP_INSUFFICIENT_ACCESS
- IO04808：Proxy 伺服器承受壓力時可能當機（異常終止）
- IO04765：Proxy Server 的加強服務，爲每個順利開啓的 TCP 連線記載訊息
- IO03861：要求 ibm-allGroups 時，Proxy 並未回覆 DN
- IO03862：操作員並未執行任何特定動作，Proxy 卻當機
- IO04277：6.0 Proxy 不應傳送更新資料給「轉遞程式」伺服器
- IO04208：Proxy 在監控搜尋時回覆錯誤的 opscompleted 值
- IO03886：需要進一步的 Proxy 伺服器功能相關資訊
- IO03885：刪除成員時，Proxy 並未更新廣域管理群組
- IO03334：應擴大 Proxy 窗格中的預設連線儲存區大小
- IO02387：除了搜尋之外，Proxy 伺服器無法正確處理屬性
- IO02385：處理 Digest-MD5 鑑別時，Proxy 伺服器發生異常終止
- IO02378：處理 ibm-allgroups 搜尋時，Proxy 伺服器發生異常終止
- IO02369：加強 Proxy 伺服器，以在僅有 1 個分割區時，修改分割儲存器登錄
- IO02374：使用群組的 Acl 解決方案無法透過 Proxy 伺服器正確作業。
- IO02377：若由非管理員使用者執行呼叫，Compare（比較）、Delete（刪除）和 modrdn

作業無法透過 Proxy 正確作業

6) Proxy 上的 TechNotes

Linux：Proxy 並未在 389 埠上啓動；因爲錯誤碼 13（許可權遭拒）而執行失敗...

Proxy 的轉介追蹤：ITDS 6.0 Proxy 伺服器不提供轉介追蹤...

ITDS 6.0 Proxy 和後端 LDAP 伺服器 - 支援的延伸、控制項和功能...

Proxy 伺服器不支援 ibm-allgroups 的子樹狀結構型搜尋...

IBM Tivoli Directory Server 6.0 Proxy Server 和舊版的 IBM Tivoli Directory Server 不相容...

疑難排解 TDS Proxy

1) 發生作業失敗時需要檢查的基本日誌檔

使用具備後端伺服器的 Proxy 時，查看日誌檔中的錯誤訊息，可以解決許多問題和失敗。您可以使用日誌檔驗證適當行爲，遇到任何錯誤時，查看日誌檔都是首選的解決方法，日誌檔可讓您初步瞭解狀況。不過，只有管理員或管理群組的成員有權檢視或存取 Proxy 日誌資訊。

Proxy 日誌的預設日誌路徑：

UNIX® 路徑：instance-base-directory/idsslapd-<實例名稱>/logs

Windows 路徑：drive\idsslapd-<實例名稱>\logs

WebSEAL 的預設訊息日誌路徑：

UNIX 路徑：/var/pdweb/logs/msg__webseald-<實例名稱>.log

Windows 路徑：<安裝磁碟>\Tivoli\logs\

附註：ibmslapd.log 檔和 audit.log 檔都很常用，其審核日誌可用來提高目錄伺服器的安全，而 ibmslapd.log 可用來檢視伺服器的相關狀態與錯誤訊息。

如需日誌和日誌管理的詳細說明，請見 TDS 6.0 管理手冊。

如需針對日誌中的錯誤，採取適當動作，請見訊息手冊。

2) 無法透過日誌瞭解狀況時，收集詳細除錯資料的詳情

假如無法使用日誌解決問題，可在發生失敗時收集基本資訊。這些詳細資料有助「支援」團隊分析問題：

a) 在 Proxy 伺服器和後端伺服器上啓用 ASCII/Binary 追蹤。有關伺服器追蹤資料的收集步驟，請遵循以下的 TechNotes 鏈結：

如何在啓動時收集 ASCII 伺服器追蹤資料

如何收集動態的 ASCII 伺服器追蹤資料

如何在 ITDS 上收集並行的動態二進位和 ASCII 伺服器追蹤資料

b) LDAP 版本和修正套件等級明細：# ldapsearch -e output
我們建議您使用最新等級的修正套件：升級至最新的修正套件

c) 目錄下的所有日誌檔：

- /home-<實例名稱>/idsslapd-<實例名稱>/logs
- 和 /home/<實例名稱>/sqllib/db2dump/db2diag.log

d) Proxy 配置檔 - ibmslapd.conf：

/home/<實例名稱>/idsslapd-<實例名稱>/etc

e) 其他可收集的有用資訊：

- OS 詳細資訊
- DB2 修正套件詳細資料：db2level
- 抄寫明細？（像同層級、主要抄本)
- SSL 明細，是否啓用 SSL

f) 針對 WebSEAL 收集的其他資料

- webseald-<實例名稱>.conf
- msg__webseald-<實例名稱>.log

3) 檢查鑑別錯誤（登入遭拒）

配置 WebSEAL 使用 TDS Proxy Server 時，您可能會遭到鑑別問題。若要檢查特定的登入遭拒問題，首先請檢查及驗證使用者可順利連結 TDS Proxy 和主要 LDAP 伺服器。如果使用者可以連結 TDS Proxy 和主要 LDAP 伺服器，請尋找 WebSEAL 訊息日誌中的所有錯誤訊息。若要進一步探索問題，請收集 IRA 追蹤資料。IRA 追蹤資料是從 WebSEAL 機器上收集的 LDAP 用戶端追蹤資料，用以尋找 LADP 回覆碼，協助找出問題原因。

例如：WebSEAL 伺服器訊息日誌中所擷取的失敗登入 (/var/pdweb/log/msg__webseald-default.log)：

```
---------------------------------------
2007-09-20-07:55:29.772+00:00I----- 0x132120DD webseald WARNING ias authsvc pdauthn.cpp
1435 0x00002728
HPDIA0221W      Authentication for user testuser failed. You have used an invalid user name,
password or client certificate.
---------------------------------------
```

若要收集 IRA 追蹤資料：
請使用以下方法啓用 pd.ivc.ira 追蹤：
pdadmin> server task webseald-instance-name trace set pd.ivc.ira 9 file path=/tmp/pdweb.ira.out

使用以下方法停用 pd.ivc.ira 追蹤：
pdadmin> server task webseald-instance-name trace set pd.ivc.ira 0

顯示登入遭拒和 LDAP 伺服器回覆碼的 pd.ivc.ira 追蹤資料輸出部分：

```
---------------------------------------
2007-07-20-07:55:29.757+00:00I----- thread(4) trace.pd.ivc.ira:8 /project/am510/build/
am510/src/ivrgy/ira_auth.c:1417: CII ENTRY: ira_auth_passwd_compare() dn: cn=testuser,
o=ibm,c=us

2007-07-20-07:55:29.757+00:00I----- thread(4) trace.pd.ivc.ira:7 /project/am510/build/
am510/src/ivrgy/ira_entry.c:3053: ira_ldap_compare_s() DN: cn=testuser,o=ibm,c=us Attr
: userPassword
```

```
2007-07-20-07:55:29.758+00:00I----- thread(4) trace.pd.ivc.ira:7 /project/am510/build/
am510/src/ivrgy/ira_ldap.c:757: ira_ldap_compare_s(): No timeout - calling ldap_compare_s

2007-07-20-07:55:29.759+00:00I----- thread(4) trace.pd.ivc.ira:7 /project/am510/build/
am510/src/ivrgy/ira_ldap.c:767: ira_ldap_compare_s: Returning LDAP rc x5

2007-07-20-07:55:29.759+00:00I----- thread(4) trace.pd.ivc.ira:7 /project/am510/build/
am510/src/ivrgy/ira_entry.c:3060: LDAP rc: x5

2007-07-20-07:55:29.759+00:00I----- thread(4) trace.pd.ivc.ira:8 /project/am510/build/
am510/src/ivrgy/ira_auth.c:1427: CII EXIT ira_auth_passwd_compare() with rc:
0x00000031 LDAP_ERROR x5 "A compare operation returned false.".
---------------------------------------
```

針對登入失敗顯示 LDAP 回覆碼的 IRA 追蹤資料，即 x31「Invalid Credentials」（無效的認證）或 x5「A compare operation returned false」（對比操作得到錯誤回覆)。使用連結或比較的鑑別是由 webseald-default.conf 檔的 「auth-using-compare」參數所控制。

4) 配置 TAM Policy Server/WebSEAL 使用 Proxy 時，檢查存取控制：

Tivoli Access Manager 必須擁有適當的存取控制，才能管理 Suffix 中的使用者和群組；而使用者和群組定義是在 Suffix 中維護的。換言之，TDS 後端伺服器必須擁有適當的 Policy Server 和 WebSEAL 存取控制，才能執行 LDAP 作業。在 TDS Proxy 伺服器 上，無法修改和管理控制清單 (ACL) 的存取。使用 Proxy 伺服器時，是由後端伺服器強制執行存取控制。假如 ACL 是位於分割區分割點的最上層物件，請務必在每一部後端伺服器上建立及附加適當的 ACL。若要在後端伺服器上設定必要的 ACL，讓 Tivoli Access Manager 能夠管理分割區 Suffix，請使用 Tivoli Access Manager ivrgy_tool 公用程式和 add-acls 參數。

```
# ivrgy_tool -h 9.182.194.116 -p 3389 -D cn=root -w root -d add-acls default
ivrgy_tool: Attempting to add Access Control Lists (ACLs) to each suffix for domain \
"default".
  O=IBM,C=US
  SECAUTHORITY=DEFAULT
ivrgy_tool: IRA interface reports result (x'0'):
Request was successful.
```

TDS Proxy 6.1 的新增功能

1. **監控：**TDS 6.1 Proxy 支援其他監控搜尋，協助進一步監控 Proxy 所配置的分割區基礎，以及每一部後端伺服器上的個別求作業。此外，您還可以監控 Proxy 後端的作業總數。
2. **性能檢查：**TDS 6.1 Proxy Server 提供後端伺服器性能檢查和快速失效接手，可減少在失效接手狀況下的失敗作業數目。
3. **後端伺服器 的 Proxy 快速失效接手和分層優先順序：**在 TDS 6.1 Proxy Server 中，每個分割區皆可配置爲主要後端伺服器，方法是將後端伺服器群組成具有優先順序的分層。
4. **尋找登錄：**TDS 6.1 Proxy Server 容許管理員在儲存指定登錄的後端伺服器上，使用 Proxy 伺服器分割演算法尋找後端伺服器。
5. **支援 LDAP 交易：**Proxy 伺服器提供有限交易支援，交易中的所有作業都鎖定單一後端伺服器目標時，容許交易進行。
6. **密碼原則支援：**Proxy 伺服器現在提供完整的廣域密碼原則支援，而只要資料經過分割，就支援多重密碼原則。
7. **Proxy 伺服器配置：**Proxy 伺服器可以進行配置，連結後端伺服，成爲廣域管理群組的成員，在舊版中，他們必須以本端管理群組或 Root 管理者身分才能連結。
8. **Web Admin 支援 Proxy Server 群組：**在 TDS 6.1 中，可使用 Web 管理工具配置伺服器群組。
9. **自訂的 DN 分割演算法：**在 TDS 6.1 中，分割功能可以實作成外掛程式，而 ITDS Proxy Server 分割演算法則很容易取代。因此，ITDS Proxy Server 得以提高彈性和調適性。
10. **多執行緒配送目錄設定工具：**您可以在 ITDSv6.1 中建立 ddsetup 工具，以使用 Proxy 伺服器的配置檔並提高工具的效能。

總結

本文內容涵蓋 TDS Proxy 伺服器的管理、放置和疑難排解，以更充分地理解及管理 TDS Proxy 伺服器。文中也介紹了在 TAM 環境裡使用 TDS Proxy 伺服器的好處，還說明廣域管理群組。此外，也簡介了目前已知的 Proxy 伺服器問題。

鳴謝

特別感謝 Darshan R Donni 爲本文提供 TDS Proxy 的寶貴概念。

關於作者

Sunil 是軟體工程師，目前隸屬於 IBM 印度軟體實驗室第 2 級 Tivoli 安全團隊，他擁有工程學士（資訊科技）學位，主要研究領域包括企業級安全、單一登入 (SSO) 和服務導向架構 (SOA)；他擁有 ITIL Foundation 認證以及 Tivoli Access Manager for e-business V6.0 Implementation 認證。

Varsha Sogani 也是軟體工程師，目前隸屬於 IBM 印度軟體實驗室第 2 級 Tivoli 安全團隊，她擁有電腦科學工程學士（榮譽學位）。她是 IBM 認證的 Tivoli Directory Server 6.1、ITIL Foundation 和 DB2 UDB V8.1 Family Fundamentals 部署專家。