CA Spectrum®

Secure Domain Manager 使用者指南

9.4 版

ca technologies

本文件包含內嵌說明系統與文件 (以下稱爲「文件」)僅供您參考之用，且 CA 得隨時予以變更或撤銷。

未經 CA 事先書面同意，任何人不得對本「文件」之任何部份或全部內容進行影印、傳閱、再製、公開、修改或複製。 此「文件」爲 CA 之機密與專屬資訊，您不得予以洩漏或 用於任何其他用途，除非 (i) 您與 CA 已另立協議管理與本「文件」相關之 CA 軟體之使用；或 (ii) 與 CA 另立保密協議同意使用之用途。

即便上述，若您爲「文件」中所列軟體產品之授權使用者，則可列印或提供合理份數之「文件」複本，供您以及您的員工內部用於與該軟體相關之用途，但每份再製複本均須附上所有 CA 的版權聲明與說明。

列印或提供「文件」複本之權利僅限於軟體的相關授權有效期間。 如果該授權因任何原因而終止，您有責任向 CA 以書面證明該「文件」的所有複本與部份複本均已經交還 CA 或銷毀。

在相關法律許可的情況下，CA 係依「現狀」提供本文件且不做任何形式之保證，其包括但不限於任何針對商品適銷性、適用於特定目的或不侵權的暗示保證。 在任何情況下，CA 對於您或任何第三方由於使用本文件而引起的直接、間接損失或傷害，其包括但不限於利潤損失、投資損失、業務中斷、商譽損失或資料遺失，即使 CA 已被明確告知此類損失或損害的可能性，CA 均毋須負責。

「文件」中提及之任何軟體產品的使用均須遵守相關授權協議之規定，本聲明中任何條款均不得將其修改之。

此「文件」的製造商爲 CA。

僅授與「有限權利」。美國政府對其之使用、複製或公開皆受 FAR 條款 12.212，52.227-14 與 52.227-19(c)(1) - (2) 與 DFARS 條款 252.227-7014(b)(3) 中所設之相關條款或其後續條約之限制。

Copyright © 2014 CA. All rights reserved. 本文提及的所有商標、商品名稱、服務標章和公司標誌均爲相關公司所有。

CA Technologies 產品參考資料

本文件提及下列 CA Technologies 產品：

- CA Spectrum® (CA Spectrum)
- CA Spectrum® 安全網域管理員
- CA Spectrum® 安全網域連接器

連絡技術支援

如需線上技術協助及完整的地址清單、主要服務時間以及電話號碼，請洽「技術支援」，網址為：http://www.ca.com/worldwide。

目錄

第 1 章： 簡介 7

管理高安全網路的挑戰 7
重疊 IP 網域 8
封鎖 SNMP 和 ICMP 流量的防火牆 10
穿過不安全網路的 SNMP 流量 10
Secure Domain Manager 11
Secure Domain Manager 運作方式 12
Secure Domain Manager 架構 14
使用 Secure Domain Manager 的優點 15

第 2 章： 安裝和配置 Secure Domain Manager 程序 17

如何設定 Secure Domain Manager 程序 17
安裝和配置程序 17
在 SpectroSERVER 上設定 Secure Domain Manager 18
硬體建議 18
關於 SDConnector CPU 和記憶體使用量 18
安裝 SDConnector 程序 19
安裝檔案 20
使用憑證 21
升級時刪除舊的憑證檔 21
建立憑證 22
配置 SDConnector 程序設定 24
配置 SDManager 程序設定 27
在 Windows 上啓動、停止及重新啓動 SDConnector 程序 30
在 Solaris 和 Linux 上啓動、停止及重新啓動 SDConnector 程序 31

第 3 章： 使用 Secure Domain Manager 33

匯入 SDManager 配置檔 33
模型化 SDConnector 主機 34
SDConnector 模型化注意事項 35
SDConnector 模型化和 CA Spectrum 錯誤隔離 35
將安全網路網域中的裝置模型化 36
依 IP 建立模型 36

搜索 37
使用 SDConnector 主機來搜索裝置 37
關於維護裝置安全網域成員資格 38
存取 Secure Domain Manager 搜尋 39
檢查安全網域中的裝置存取性 39
檢視安全網域中的裝置 MIB 39
SDManager 模型資訊檢視 40
SDConnector 模型資訊檢視 42

第 4 章： 在容錯環境中設定程序 43

在容錯 SpectroSERVER 環境中設定 SDManager 43
容錯 SpectroSERVER (SDManager) 44
設定容錯 SDConnector 44
容錯 SDConnector 46

附錄 A： Secure Domain Manager 疑難排解 47

錯誤訊息 47
憑證無效錯誤 47
連接埠衝突 48
SDConnector 需要自訂的 SNMP 設陷連接埠 48
安裝問題 48

第 1 章： 簡介

本節包含以下主題：

管理高安全網路的挑戰 (位於 p. 7)
Secure Domain Manager (位於 p. 11)
Secure Domain Manager 運作方式 (位於 p. 12)
Secure Domain Manager 架構 (位於 p. 14)
使用 Secure Domain Manager 的優點 (位於 p. 15)

管理高安全網路的挑戰

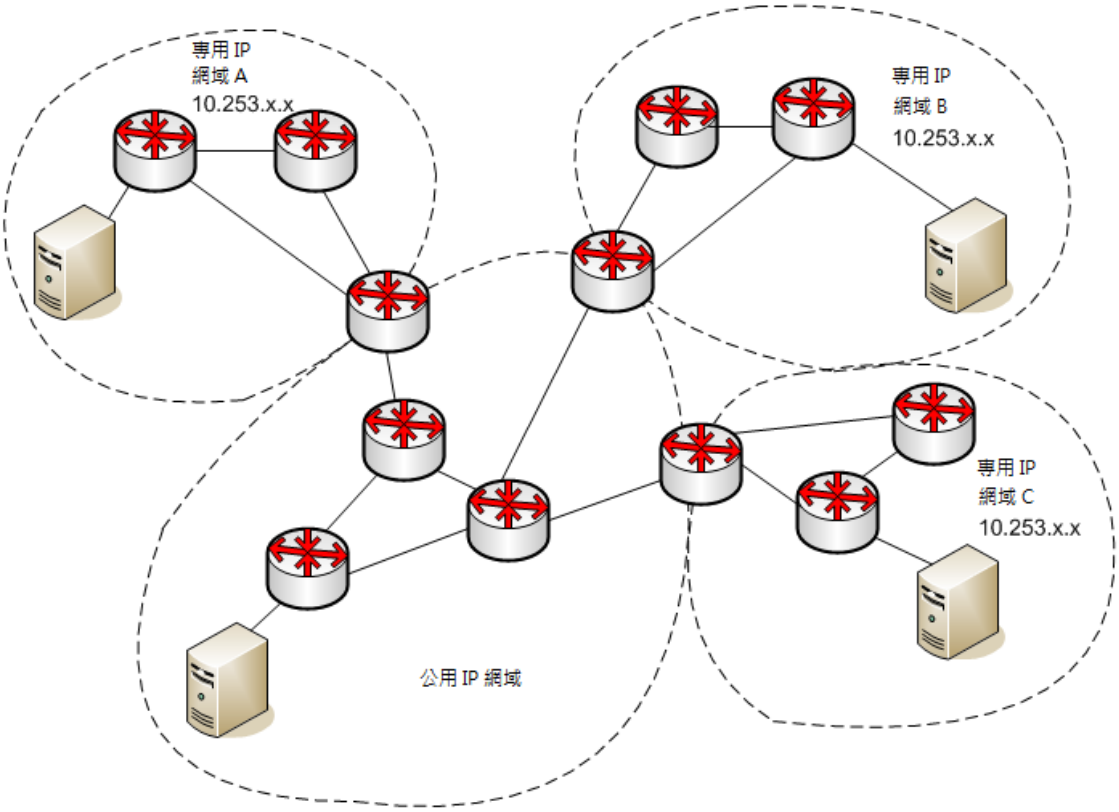
如今的電腦網路有更多安全保護。 在安全網路中管理裝置和應用程式的挑戰也隨之升高。 這些挑戰包括：

- 管理重疊 (或私人) IP 網域 (NAT 環境) 中的網路元素
- 管理防火牆 (已配置來封鎖 SNMP 和 ICMP 流量) 後面的網路元素
- 穿過不安全網路網域來管理網路元素

Secure Domain Manager 產品提供獨特的解決方案來克服這些管理挑戰。

重疊 IP 網域

下圖顯示的 NAT 網路包含一個公用 IP 網域和三個包含相同 IP 子網路的私人 IP 網域。



這些網域可能代表公司的受管理網路、大企業中剛收購的部門，或航空站裡受管理的無線熱點。

下列類型的 CA Spectrum 客戶面臨重疊 IP 的挑戰：

受管理服務提供者 (MSP)

MSP 使用 CA Spectrum 來管理其他組織的網路。 MSP 管理的客戶都使用私人 IP 常用的 IP 範圍，例如 10.x.x.x 或 172.16.x.x。 因此，MSP 必須解決管理重複或重疊 IP 位址的挑戰。 以往，此挑戰的解決之道是提供專用的 CA Spectrum 管理伺服器 (SpectroSERVER) 給每一個使用相同 IP 位址空間的客戶。

這樣造成兩個問題。 第一個是成本。 不論受管理環境的規模有多大或使用的重疊 IP 位址數量有多少，每一個客戶都需要有專用的管理伺服器。 第二個問題是管理。 MSP 要負責維護更多管理系統。 MSP 需要較不昂貴且有效率的作法來替代專用的管理系統，尤其是當有重疊 IP 位址的元素爲數很少，不值得花費成本在專用的管理伺服器時。

熱點 (Wi-Fi) 存取提供者

熱點存取提供者會在一些地點提供 Wi-Fi 連線，例如航空站、候機室、旅館房間及咖啡館。 每一個地點會配發相同的私人 IP 位址空間。 此作法可簡化配置、安裝及管理。 提供者可能有數百或數千個熱點。 爲了快速部署新的熱點，每一組在場所中建立熱點的設備都使用相同配置，包括 IP 位址空間。 熱點開始運作時，挑戰就變成主動管理熱點來維持最佳服務水準。

企業管理員

在組織合併或收購的情況下，企業管理人員通常必須合併個別建構的兩個完全不同的 IP 網路，而這經常會產生多個重疊 IP 位址。 在此情況下，新的 IT 組織現在必須管理合併後的網路，尤其是管理具有相同 IP 位址空間的網路。 要解決這項挑戰，一種方法是重新指派 IP 給每一個 IP 實體，以杜絕重複的 IP 位址。 但那樣的解決方案工程浩大，需要面對更多挑戰。

Secure Domain Manager 採取下列作法，讓這些客戶克服管理重疊 IP 網域的挑戰：

- MSP 只需在每位客戶的遠端網路中的主機機器上部署輕量型代理程式程序，而不需要部署和管理完整的 CA Spectrum 安裝。
- 熱點存取提供者和大型企業可以讓重疊的私人 IP 網域維持不變，同時利用輕量型代理程式程序來管理網路。

封鎖 SNMP 和 ICMP 流量的防火牆

防火牆提供許多網路環境中不可或缺的安全性。 管理防火牆後面的網路會面臨一些挑戰。 首先，網路管理員通常會配置防火牆來封鎖 SNMP 和 ICMP 流量，因爲這些流量可讓未經授權的來源窺探網路基礎架構。 其次，若要穿過高度安全的防火牆來管理網路元素，所需的配置很複雜。 因爲，防火牆上要識別並開放所有相關的主機和連接埠，才有完整的管理功能可用。

Secure Domain Manager 採取下列作法，讓網路管理員克服穿越安全防火牆來管理網路的挑戰：

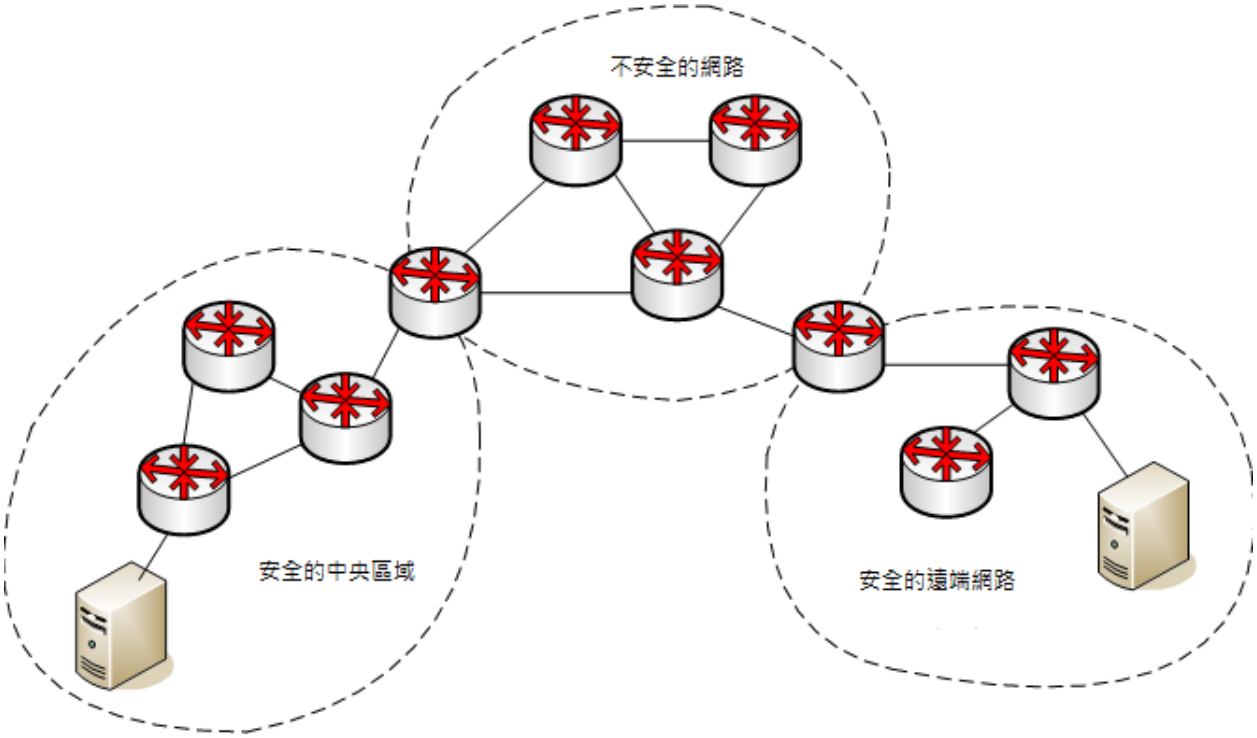
- 將 UDP 型 SNMP 和 ICMP 封包編碼成 TCP/IP 型通訊協定，以克服防火牆對 SNMP 和 ICMP 流量的限制。
- 將防火牆的配置簡化成開啓單一連接埠，以在一個妥善定義的連接埠上，允許 SNMP 和 ICMP 流量在兩個妥善定義的主機之間流動。

穿過不安全網路的 SNMP 流量

SNMPv1 和 SNMPv2 不是安全的通訊協定，因爲資料沒有加密，只要使用通訊協定解析程式就能檢視。 因此，不建議穿過不安全的網路來傳送這個流量。 想讓 SNMP 流量穿過不安全網路抵達您要管理的網路，就成爲一項挑戰。

下圖顯示「安全中心區域」中主機電腦上的網路管理系統，其負責管理「安全遠端網路」中的裝置。管理流量必須穿過「不安全的網路」區域。 在這部份的網路中，網路管理員要避免曝露不安全通訊協定封包內的資料，例如 SNMPv1 和 SNMPv2。

穿過不安全網路來傳送 SNMP



Secure Domain Manager 可讓網路管理員將 SpectroSERVER 主機和遠端受管理網路中的主機之間傳遞的管理流量加密。 此解決方案可在不安全的網路中安全地傳遞不安全的 SNMP 流量。 當流量穿越中間的不安全網路時，可確保資料安全性。

Secure Domain Manager

Secure Domain Manager 是 CA Spectrum 網路管理解決方案，可讓使用者管理安全網路中的裝置。 您不需要部署本機 SpectroSERVER 就可以管理裝置。 Secure Domain Manager 可透過安全連線來安全地傳遞 SNMP 和 ICMP 流量，讓您管理安全網域。 防火牆上只開啓單一連接埠，如此既可延伸管理範圍，同時又不影響既有的安全性原則。 此解決方案不會干擾使用者和用戶端應用程式，因此不需要執行更多管理工作。

Secure Domain Manager 運作方式

Secure Domain Manager 支援 SNMPv1、SNMPv2 及 SNMPv3 通訊。 它包含兩個不同的程序，即 SDManager 和 SDConnector：

SDManager

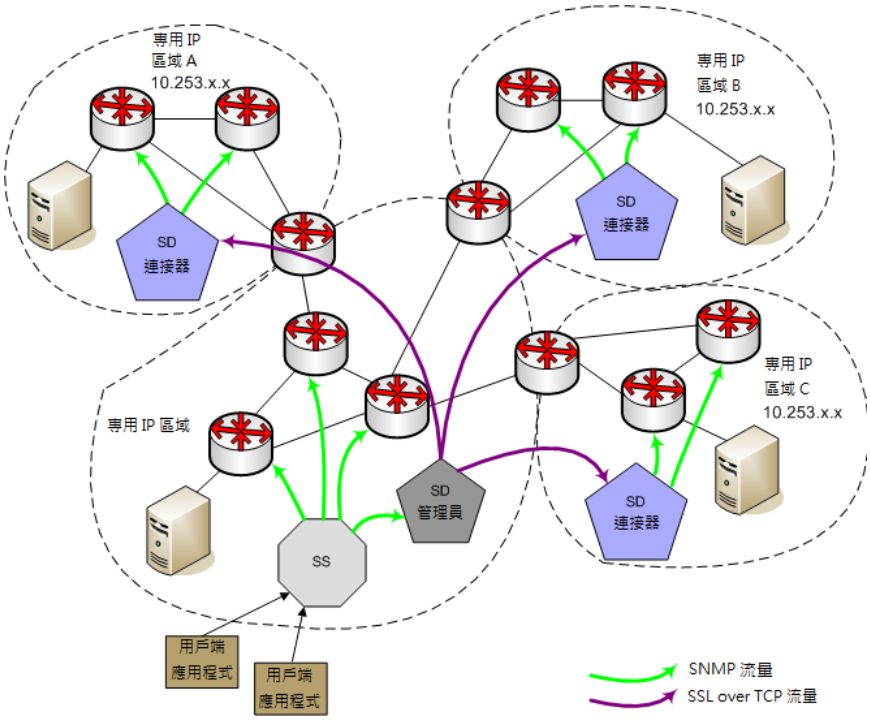
SDManager 是由 SpectroSERVER 載入的伺服器訊息程式庫。

SDConnector

SDConnector 是遠端程序，負責與 SpectroSERVER 上的 SDManager 通訊。 它在遠端私人網路中的主機機器上執行，能夠代表 SpectroSERVER (通常部署在私人 IP 區域中) 轉送 SNMP 和 ICMP 訊息，因此可以管理私人網路中的裝置。 SDConnector 是以配置檔 (sdc.config) 來配置，此檔案可能同時包含主要和備用 SpectroSERVER 資訊。 它是 Secure Domain Manager 解決方案的一部份。

下圖顯示如何在安全網路環境中部署這些程序。

使用 Secure Domain Manager 的 NAT 網路環境



附註：在與 SpectroSERVER 位於相同區域中，裝置是由 SNMP 管理，而不是 Secure Domain Manager。

當公用 IP 區域中的 SpectroSERVER 必須與遠端安全區域中的裝置通訊時，SpectroSERVER 會傳送要求給 SDManager。 SDManager 會將 SMNP 資料轉換成專用格式，並將資料傳送到裝置所在區域中的 SDConnector。 如果 SDManager 和 SDConnector 已配置爲搭配 SSL 來執行，則資料會加密，並利用 SSL over TCP 透過安全通道傳送到 SDConnector。 SDConnector 收到資料時，就會將資料轉換回 SNMP，並傳送要求給適當的裝置。

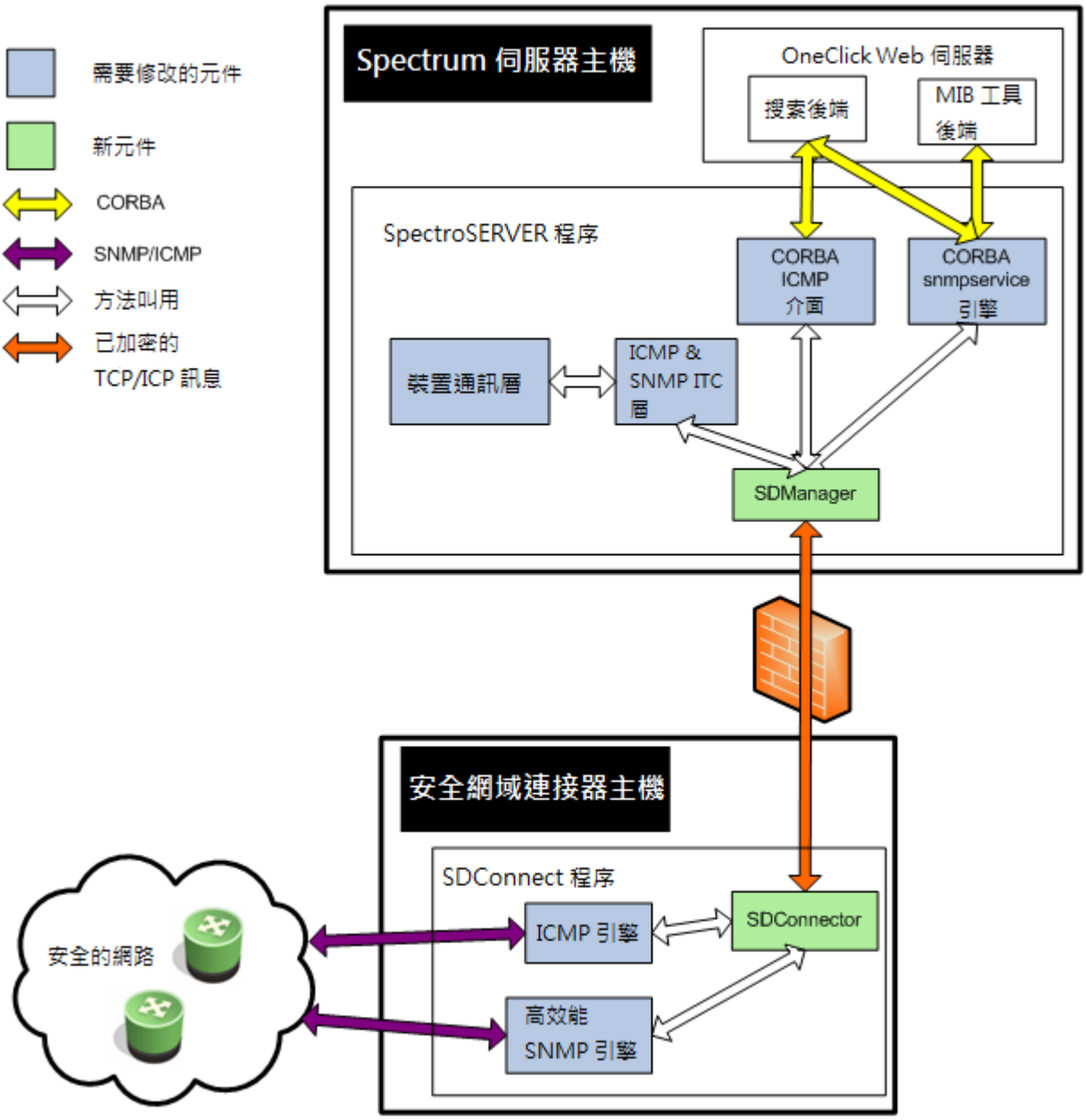
如果部署了防火牆，則運作方式相同。 網路管理員必須在每道防火牆建立一個「缺口」，專門供兩個公認主機使用。 在穿越多道防火牆的區域中，也可使用此解決方案來管理裝置。 若要啓用此通訊，請在每道防火牆開啓一個連接埠。 此連接埠必須是公認連接埠，可讓一對位於相鄰區域的公認主機使用 TCP 來通訊。

部署 Secure Domain Manager 來管理重疊 IP 網域時，每個 SDConnector 主機機器都必須有唯一公用 IP 位址。主機必須能夠與 SDConnector 所必須通訊的所有裝置通訊，包括 SpectroSERVER 主機機器及其管理的單一私人 IP 網域內的所有裝置。 此 SDConnector 主機可能是 NAT 後面由 NAT 靜態指派唯一 IP 位址的機器。 SpectroSERVER 使用 SDConnector 主機機器的唯一 IP 位址作爲額外鑑別器，以唯一識別具有相同私人 IP 位址的多個裝置。

附註：某些 CA Spectrum 產品無法管理重疊 IP 位址，例如 Network Configuration Manager (NCM) 和 IP 服務管理應用程式 (包括 Multicast Manager 和 Enterprise VPN Manager)。 不過，如果您在 SDConnector 上模型化這些應用程式的裝置，而不是在 SpectroSERVER 上，則仍然可以使用 Secure Domain Manager 來管理這些應用程式。 在這種配置中，可以爲每一個 SpectroSERVER 部署多個 SDConnector，只要 SDConnector 所管理的裝置不是被配置重疊的 IP 位址即可。 利用此方法，您還是可以在本機 SpectroSERVER 上模型化裝置，但這些裝置被配置的 IP 位址，不能與透過 SDConnector 管理的裝置上所配置的 IP 位址重疊。

Secure Domain Manager 架構

下圖說明 Secure Domain Manager 的運作方式：



使用 Secure Domain Manager 的優點

Secure Domain Manager 解決方案可透過下列方式強化 CA Spectrum 中的現有管理功能：

- 讓 CA Spectrum 與所有 SNMP 相容裝置通訊：SNMPv1、SNMPv2 和 SNMPv3
- 讓 CA Spectrum 與防火牆 (封鎖了 SNMP 和 ICMP 流量) 後面的裝置通訊
- 簡化防火牆配置。 因爲，只開啓一個缺口，讓兩個公認主機之間能夠透過一個公認連接埠來交換流量
- 讓 CA Spectrum 將 SNMP 和 ICMP 流量安全地送經不安全網路
- 讓 CA Spectrum 使用單一 SpectroSERVER 來管理重疊 IP 網域 (NAT 環境) 中的裝置
- 增強 [搜索] 功能來搜索和模型化安全環境中的裝置 (一次處理一個 IP 位址空間)

第 2 章： 安裝和配置 Secure Domain Manager 程序

本章說明如何安裝和配置 Secure Domain Manager 解決方案，過程中需要安裝和配置 SDConnector 及 SDManager。

本節包含以下主題：

如何設定 Secure Domain Manager 程序 (位於 p. 17)
硬體建議 (位於 p. 18)
安裝 SDConnector 程序 (位於 p. 19)
使用憑證 (位於 p. 21)
配置 SDConnector 程序設定 (位於 p. 24)
配置 SDManager 程序設定 (位於 p. 27)
在 Windows 上啓動、停止及重新啓動 SDConnector 程序 (位於 p. 30)
在 Solaris 和 Linux 上啓動、停止及重新啓動 SDConnector 程序 (位於 p. 31)

如何設定 Secure Domain Manager 程序

配置 Secure Domain Manager 的過程包括安裝和設定 Secure Domain Manager 程序，然後在 SpectroSERVER 上使用 OneClick 來設定它們。

安裝和配置程序

安裝和配置 Secure Domain Manager 程序需要下列步驟：

1. 在指定的主機上安裝 SDConnector 程序 (位於 p. 19)。

   附註：安裝核心 CA Spectrum 產品時會一起安裝 SDManager；不過，它必須包含在您公司所購買的套件中，才會產生作用。

2. (選用) 建立和部署 SSL 憑證 (位於 p. 21)以支援 SSL 加密。
3. 在 SDConnector 主機上，在 SDConnector 的配置檔中設定參數 (位於 p. 24)。
4. 在 SpectroSERVER 上，在 SDManager 的配置檔中設定參數 (位於 p. 27)。

在 SpectroSERVER 上設定 Secure Domain Manager

安裝並配置 SDConnector 和 SDManager 程序之後，在 SpectroSERVER 主機上使用 OneClick 來設定 Secure Domain Manager。 此設定包含下列步驟：

1. 匯入 SDManager 配置檔 (位於 p. 33)。
2. 將 SDConnector 主機模型化 (位於 p. 34)。
3. 將安全網域中您要管理的裝置模型化 (位於 p. 36)。

硬體建議

遵循這些建議來達成最佳的 Secure Domain Manager 效能：

- 爲了維持最佳的 SpectroSERVER 模型化容量，SpectroSERVER/SDManager 安裝電腦必須有兩顆 CPU：一個供 SpectroSERVER 專用，另一個專門處理 SDManager 功能。 如果 SDManager 和 SpectroSERVER 需要共用單一處理器來管理網路元素，則 SpectroSERVER 模型化容量會降低 40%。
- 建議以一部主機電腦來專門執行您部署的每一個 SDConnector 程序。 SDConnector 安裝系統需求與純 SpectroSERVER 的安裝需求相同。 多磁碟配置的特殊需求除外。

  附註：如需安裝需求的詳細資訊，請參閱《*管理指南*》。
- 一個 SDConnector 只連接一個 SDManager。 如果您的環境有需要的話，容錯 SpectroSERVER 中的兩個 SDManager 可以連接至單一 SDConnector。 如需詳細資訊，請參閱《在容錯環境中設定程序 (位於 p. 43)》。

關於 SDConnector CPU 和記憶體使用量

SDConnector 使用的 CPU 容量是 SpectroSERVER 管理裝置時所使用的一半。 如果 SpectroSERVER 電腦使用整個 CPU 的 50%，且所有裝置都是由 SDManager 管理，則在同等運算能力的系統上，SDConnector 使用大約 25% 的 CPU 容量。 主要差別是 SDConnector 不會使用太多記憶體。 如果只作爲 SDConnector，則 512 MB 的 RAM 就足夠，不過 RAM 當然是越多越好。

安裝 SDConnector 程序

在 CA Spectrum 中使用 Secure Domain Manager 功能來管理安全網路中的裝置和應用程式之前，請在安全網路中的主機電腦上安裝單一 SDConnector 程序。 Secure Domain Manager 不支援在相同的主機電腦上執行多個 SDConnector 程序。 安裝 SDConnector 時，您必須是系統管理使用者 (Windows 系統) 或根使用者 (Solaris 和 Linux 系統)。

附註：以最佳做法而言，在任何平台上升級 SDConnector 程序之前，請停止程序，甚至在必要時刪除程序。 停止或刪除程序可確保程序在升級之後正常執行。

安裝 SDConnector

1. 在您要執行 SDConnector 的非 SpectroSERVER 主機機器上，啓動平台適用的 CA Spectrum 安裝程式。

   附註：只能安裝與 SpectroSERVER 有相同運作環境的 SDConnector。 如果需要安裝其他運作環境的 SDConnector，請連絡 CA 支援。 如需啓動安裝程式的詳細資訊，請參閱《*安裝指南*》。

   [安裝] 對話方塊隨即開啓。

2. 選取 [安裝 CA 安全網域連接器]。

   [簡介] 對話方塊隨即開啓。

3. 按 [下一步] 繼續。

   [授權合約] 對話方塊隨即開啓。

4. 捲動並閱讀授權合約，接受合約，然後按 [下一步]。

   [目標位置] 對話方塊隨即開啓。

5. 按 [下一步]，將 SDConnector 安裝在預設目錄中。 預設目錄在 Windows 上是 C:\Program Files\CA\SDMConnector，在 Solaris 和 Linux 上則是 /usr/SDMConnector。

   若要將 SDConnector 安裝在預設資料夾以外的位置，請按一下 [選擇]，選取資料夾，然後按 [下一步]。 只有在本機進行的安裝才會顯示 [選擇] 按鈕 (不在本機進行的遠端安裝則不會顯示)。

   附註：無法將 SDConnector 安裝到名稱含有空格的目錄中。

   [安裝前摘要] 對話方塊隨即開啓。

6. 按一下 [安裝]。

   [安裝 SPECTRUM_SDM_Connector] 對話方塊隨即開啓。安裝 SDConnector 之後，狀態會變成 [安裝完成]，且 [完成] 按鈕會啓用。

7. 按一下 [完成]。

   對話方塊隨即關閉。

8. 在最初的 [安裝] 對話方塊中按一下 [關閉]。

   SDConnector 已安裝在此主機電腦上。 SDConnector 已安裝成服務，並會於系統每次重新啓動時自動啓動。

   附註：您也可以在 SDConnector 安裝到的目錄中檢查安裝記錄，以確認安裝順利完成。

安裝檔案

請注意以下在安裝過程中建立的目錄和檔案。

在 SpectroSERVER

CA Spectrum 安裝程序會在 SpectroSERVER 的 *<$SPECROOT>*/SDM 目錄中，安裝下列 Secure Domain Manager 目錄和檔案：

cert

此目錄是存放您爲 SDManager 建立之 SSL 憑證的儲存庫。

日誌

此目錄包含當您將配置檔匯入至 SpectroSERVER 時所產生的輸出記錄檔。已執行的工作的詳細資料， 包括任何發生的錯誤，都在記錄檔中。

README

此檔案提供如何在 SpectroSERVER 主機上配置 Secure Domain Manager 的詳細資料。

在 SDConnector 主機

SDConnector 安裝程序會在 SDConnector 主機上的 SDMConnector 目錄中安裝下列目錄和檔案：

bin

此資料夾包含以下用於 SDConnector 的項目：

cert

此目錄是存放您為 SDConnector 建立之 SSL 憑證的儲存庫。

README

此檔案提供如何在 SDConnector 主機上配置 SDConnector 程序的詳細資料。

SdmConnectorService[.exe]

SDConnector 的執行檔。

使用憑證

預設會載入 SDManager 和 SDConnector 的憑證。 這可讓您使用 SSL 加密，以保護 SDManager 與 SDConnector 主機之間透過不安全網路來傳輸的 ICMP 和 SNMP (SNMPv1、SNMPv2c 及 SNMPv3) 資料。 如果不想對您網路環境中的任何 SDManager 與 SDConnector 間連線使用 SSL 加密，請在 SDManager 和 SDConnector 的配置檔中加上 nonsecure 選項。 如需如何使用 nosecure 選項的詳細資訊，請參閱「配置 SDConnector 程序設定 (位於 p. 24)」。

升級時刪除舊的憑證檔

從 9.*x* 以前的版本升級至 Secure Domain Manager 時，請刪除舊的憑證檔。 此版本的 Secure Domain Manager 中無法使用舊的憑證 (9.*x* 以前)。 在 SDManager 主機的 *<$SPECROOT>*/SDM/srconf/mgr 目錄中，刪除預設為舊版 Secure Domain Manager 安裝的下列憑證檔：

- snmpricacert.pem：主要憑證授權單位
- dsspmastercert.pem：SDManager 憑證授權單位
- dsspremotecert.pem：SDConnector 憑證授權單位

建立憑證

Secure Domain Manager 使用數位憑證來確保安全性。 CA Spectrum 安裝會隨附預設憑證，您可以使用 CertGen 工具來建立網站專用憑證。

預設憑證

如果您要使用預設憑證，請勿執行任何動作。 所有預設檔案位於 <*$SPECROOT*>/SDM/cert 目錄，包括下列檔案：

SDMCA.pem

憑證授權單位。 將此檔案發佈給以任何產能使用安全網域管理員或安全網域連接器的任何電腦，此檔案可視爲信任的 CA 檔。

SDMCAKey.pem

CA 的私密金鑰。 可用來發行憑證，但不一定要發佈給任何機器。

SDMCert.p12

由 SDMCA.pem 簽署的應用程式憑證。 這是 SDManager 與 SDConnector 之間使用的憑證檔。 應該小心發佈給值得信任的電腦，並用來宣告這些電腦的身分識別。

CertGen[.exe]

此程式用來產生網站專用憑證授權單位、金鑰檔及憑證檔。 執行 CertGen -h 可檢閱所有可用的憑證選項。

openssl[.exe]

SSL 通訊協定的 OpenSSL 開放原始碼實作。

網站專用憑證

如果要建立網站專用憑證，請將預設憑證檔 (*.pem 和 *.p12) 移至硬碟上的其他位置。 執行下列程序來建立和部署自訂憑證。

建立網站專用憑證

建立網站專用憑證以加強安全性。 請在只有技術人員才能存取的單一電腦上建立這些憑證。 此電腦可以是 SDManager 主機。

重要！ 您必須具備系統管理員或根權限，才能建立 Secure Domain Manager 的 SSL 憑證。

請依循下列步驟:

1. 執行下列命令來建立憑證授權單位憑證，以及憑證授權單位憑證的私密金鑰：

   ```
   CertGen -t ca -c US
   ```

   此步驟只需要執行一次，爲組織建立必要的憑證授權單位憑證。

   建立的檔案如下：

   SDMCA.pem

   SDMCAKey.pem

   附註：Secure Domain Manager 隨附的預設憑證授權單位和金鑰檔是唯讀檔案。 如果發生權限錯誤，請檢查使用者權限，或將 SDMCA.pem 和 SDMCAKey.pem 移至其他位置，再重新執行命令。

2. 執行下列命令來建立 SDManager 的憑證：

   ```
   CertGen -t cert -c <國家/地區代碼>
   ```

   SDMCert.01.p12 檔便已建立完成。

3. (選用) 若要加強安全性，請使用 -p 選項加上密碼來產生憑證，如下所示：

   ```
   CertGen -t cert -p <密碼> -c <國家/地區代碼>
   ```

   在 sdc.config 檔和 sdm.config 檔中輸入密碼。

4. 將 SDMCert.01.p12 重新命名爲 SDMCert.p12。

   現在已可以使用新的網站專用憑證。

部署網站專用憑證

建立憑證檔之後，請執行下列工作：

- 將憑證檔部署在 SDManager 主機和 SDConnector 主機。
- 在 SDManager 主機上重新啟動 SpectroSERVER，並在 SDC 主機上重新啟動 SDConnector 程序。

若要部署憑證，請將您建立的 SDMCA.pem 檔，複製到 SDManager 主機電腦上的 *<$SPECROOT>*/SDM/cert 目錄，並複製到將與 SDManager 主機連線之 SDConnector 主機上 SDConnector 安裝下的 cert 目錄。 SDMCert.p12 檔應該由系統管理員 (或根使用者) 擁有。

重要！ 將 SDMCAKey.pem 檔保留在您打算建立更多憑證的電腦上。 限定僅授權人員才能使用此檔案。 此電腦可以是 SDManager 主機電腦，但這不是必要條件。

部署憑證之後，在 SDManager 主機上重新啟動 SpectroSERVER，並在 SDC 主機上重新啟動 SDConnector 程序。 如需重新啟動 SDConnector 程序的詳細資訊，請參閱在 Windows 上啟動、停止及重新啟動 SDConnector 程序 (位於 p. 30)或在 Solaris 和 Linux 上啟動、停止及重新啟動 SDConnector 程序 (位於 p. 31)。

配置 SDConnector 程序設定

本節說明您在 SDConnector 配置檔 (sdc.config) 中可設定的配置選項。啓動時會讀取此配置檔，同時會套用指定的選項。sdc.config 中只接受一行選項。以下是 sdc.config 檔中的範例行。 它指定 SDConnector 將接受來自 SDManager 的連線 (192.168.0.2)：

```
-accept 192.168.0.2
```

配置 SDConnector 設定

1. 在 SDConnector 主機機器的 SDMConnector\bin 目錄中，使用文字編輯器建立 (若已存在則開啓) 名稱爲 'sdc.config' 的檔案。
2. 根據您的特定需求，在檔案中以一行新增並指定下列選項的詳細資料：

   -accept remote_ipaddr:[local_port]

   接受在位址 *<ip>*、本機連接埠號碼 *<port>* 的主機上執行的 SDManager 所發出的連線。 連線必須來自指定的 IP 位址，否則會忽略連線嘗試。

   如果指定此選項，則與此 SDConnector 連線的 SDManager 必須在其配置檔 (sdm.config) 中，使用 -remoteconnect 選項來指定此 SDConnector *<ip>*。 另外，如果指定此選項，則無法連線 (-connect) 至該 SDManager。

-buffersize *<size>*

指定傳送和接收通訊端緩衝區的大小 (位元組)。

預設值：262,144 (256k，在大多數部署中應該足夠)

-certdir <*dir*>

針對不在預設目錄 (/cert) 中的 SSL 憑證 (應用程式憑證、私密金鑰及憑證授權單位憑證)，指定這些憑證的目錄。

如果指定 -nosecure 選項，則不會存取憑證。

-certpassword <passwd>

提供憑證密碼。 如果使用 Secure Domain Manager 隨附的預設憑證，則不需要提供 -certpassword。否則，請使用此選項來提供憑證密碼。如果密碼有空格，則必須以引號括住 (")。 CA Spectrum 假設應用程式憑證的密碼會加密。

附註：如果使用 -certpassword，則它必須是設定檔中第一個宣告的選項。

-connect remote_ipaddr:[remote_port]

與在 IP 位址 <*ip*>、連接埠 <*port*> 的主機上執行的 SDManager 連線。如果未指定 <*port*>，則假設為 6844。

如果指定此選項，則與此 SDConnector 連線的 SDManager 在其配置檔 (sdm.config) 中，必須使用 -remoteconnect 選項來指定此 SDConnector 的 IP 位址。

如果指定此選項，則此 SDConnector 無法接受 (-accept) 或接聽 (-listen) 來自指定的 SDManager (sdm.config) 的連線。

-keepalive <*n*>

變更當 SDManager 或 SDConnector 送出小型訊息來確認連線仍在作用中時的預設內部逾時 (以秒為單位)。 如果 SDManager 和 SDConnector 在 <*n*> 值的三倍之內沒有得到對方的回應，連線就會終止。

預設值：10 秒

-listen [port]

依預設，SDConnector 會在連接埠 6844 接聽來自任何 SDManager 的連線要求。 不過，如果指定任何 -connect 或 -accept 選項，則 SDConnector 依預設就不再接聽。

-listen 選項中指定的連接埠，優先於 -accept 選項中指定的連接埠。也就是說，如果 -listen 選項中指定連接埠，就不會確認該連接埠的來源 IP 位址。

附註：-listen 和 -listen6 互斥。

-listen6 [local_port]

在指定連接埠上接受來自任何 IPv6 SDManager 的連線。

附註：-listen 和 -listen6 互斥。

-loglevel fatal|error|warning|info|debug

指定要記錄的訊息類型。

預設值：warning (也包括 error 和 fatal)

-maxlogsize <*n*>

設定 sdmLog.log 大小上限 (MB)。

預設值：5M

最小值：1M

-nosecure

停用安全通訊端層 (SSL) 安全性 (預設為啓用)。 如果在任何 -connect 或 -accept 項目之前使用 -nosecure 選項，則所有連線都停用 SSL。 不然，您也可以在每個 -connect 或 -accept 項目之後指定 -nosecure 選項，如此此選項就只會套用於該項目。

如果要求 SSL 安全性，則會加密資料流，並強制執行相互密碼編譯驗證。 如果 SDManager 或 SDConnector 要求安全性，則該連線必須使用安全性。

-trappoll <*n*>

每隔 <*n*> 秒就轉送設陷至 SDManager。

預設值：15 秒

-withfips

指定以 FIPS 模式執行。 FIPS 模式預設為關閉。

附註：如果建立空的 sdc.config，SDConnector 會在連接埠 6844 接聽來自任何 SDManager 的連線；連線由 SDManager 啓動。

3. 儲存並關閉檔案。

   SDConnector 便已配置完成。

   附註：每次更新 sdc.config 檔，就必須重新啓動 SDConnector 程序。

配置 SDManager 程序設定

SDManager 配置檔 (sdm.config) 指定 SDManager 程序的運作設定。 SDManager 程序預設為停用。您必須建立 sdm.config 檔並根據需求加以配置，SDManager 程序才會運作。第一次配置 sdm.config 檔，或每次修訂其設定後，都必須將該檔案匯入至 CA Spectrum，才能讓 SDManager 設定在 SpectroSERVER 上生效。如需詳細資訊，請參閱「匯入 SDManager 配置檔 (位於 p. 33)」。 您可以在 SpectroSERVER 啓動之前或之後配置 sdm.config。

sdm.config 中只接受一行選項。 以下是 sdm.config 中的範例行。 它指定連線 (-remoteconnect) 至兩個 SDConnector (172.24.148.196 和 172.19.32.199)：

```
-remoteconnect 172.24.148.196 -remoteconnect 172.19.32.199
```

附註：如果使用 -nosecure 選項來啓動一或多個 SDConnector 程序，則必須在 SDManager 選項中為相對應的 -remoteconnect/-remoteaccept 項目指定相同的 -nosecure 選項，或直接在所有 -remoteconnect/-remoteaccept 項目之前指定 -nosecure，以停用所有連線的 SSL。

配置 SDManager 設定

1. 在 SpectroSERVER 主機機器的 *<SPECROOT>*\SDM 目錄中，使用文字編輯器建立 (若已存在則開啓) 名稱爲 'sdm.config' 的檔案。
2. 根據您的特定需求，在檔案中以一行新增並指定下列選項的詳細資料：

   -apiclientport [port]

   設定連接埠來接聽 API 用戶端連線。 此參數僅適用於獨立式 SDManager 程序。

   -buffersize *<size>*

   指定傳送和接收通訊端緩衝區的大小 (位元組)。

   預設值：262,144 (256k，在大多數部署中應該足夠)

   -certdir *<dir>*

   針對不在預設目錄 (/cert) 中的 SSL 憑證 (應用程式憑證、私密金鑰及憑證授權單位憑證)，指定這些憑證的目錄。

   如果指定 -nosecure 選項，則不會存取憑證。

   -certpassword <passwd>

   提供憑證密碼。 如果使用 Secure Domain Manager 隨附的預設憑證，則不需要提供 -certpassword。 否則，請使用此選項來提供憑證密碼。 如果密碼有空格，則必須以引號括住 (")。 CA Spectrum 假設應用程式憑證的密碼會加密。

   附註：如果使用 -certpassword，則它必須是設定檔中第一個宣告的選項。

   -clientServiceThreads *<n>*

   設定每個將會處理要求的用戶端將有的執行緒數目。 此參數僅適用於獨立式 SDManager 程序。

   -keepalive *<n>*

   變更當 SDManager 或 SDConnector 送出小型訊息來確認連線仍在作用中時的預設內部逾時 (以秒爲單位)。

   預設值：10 秒

   如果 SDManager 和 SDConnector 在 *<n>* 值的三倍之內沒有得到對方的回應，連線就會終止。

-loglevel fatal|error|warning|info|debug

指定要記錄的訊息類型。

預設值：warning (也包括 error 和 fatal)

-maxapiconnections *<n>*

將 API 用戶端連線數目上限設為 *<n>*。 此參數僅適用於獨立式 SDManager 程序。

-maxlogsize *<n>*

設定 sdmLog.log 大小上限 (MB)。

預設值：5M

最小值：1M

-nosecure

停用安全通訊端層 (SSL) 功能 (預設為啓用)。 如果在任何 -remoteconnect 或 -remoteaccept 項目之前使用 -nosecure 選項，則所有連線都停用 SSL。 不然，您也可以在每個 -remoteconnect 或 -remoteaccept 項目之後指定 -nosecure 選項，如此此選項就只會套用於該項目。

如果要求 SSL 安全性，則會加密資料流，並強制執行相互密碼編譯驗證。 如果 SDManager 或 SDConnector 要求安全性，則該連線必須使用安全性。

-remoteaccept (-rema) remote_ipaddr[:local_port]

接受在位址 *<ip>*、本機連接埠號碼 *<port>* 的主機上執行的 SDConnector 所發出的連線。 您必須指定 SDConnector 的公用 IP 位址。

如果指定此選項，則與此 SDManager 連線的 SDConnector 必須在其配置檔 (sdc.config) 中，使用 -connect 選項來指定此 SDManager 的 IP 位址。 另外，如果指定此選項，則無法連線 (-remoteconnect) 至 SDConnector (sdc.config)。

-remotebackup (-remb) remote_ipaddr[:remote_port]

在容錯 Secure Domain Manager 設定中，使用 SDConnector 的公用 IP 位址來指定備用 SDConnector。 如需詳細資訊，請參閱「在容錯環境中設定程序 (位於 p. 43)」。

-remoteconnect (-remc) remote_ipaddr[:remote_port]

與在 IP 位址 *<ip>*、*<port>* 的主機上執行的 SDConnector 連線。 如果未指定 *<port>*，則假設爲 6844。您必須指定 SDConnector 的公用 IP 位址。

如果指定此選項，則此 SDManager 連線到的 SDConnector 必須在其配置檔 (sdc.config) 中，使用 -accept 選項來指定此 SDManager，或使用 -listen 選項。 另外，如果指定此選項，則無法接受此配置檔中指定的 SDConnector 發出的連線 (-remoteaccept)。

-withfips

指定以 FIPS 模式執行。 FIPS 模式預設爲關閉。 如果將配置從 FIPS 模式變更爲非 FIPS (或相反方向)，則必須重新啓動應用程式。

附註：如果 sdm.config 檔是空的，SDManager 程序會停用。

3. 儲存並關閉 sdm.config 檔。

   SDManager 配置完成。

更多資訊：

匯入 SDManager 配置檔 (位於 p. 33)

在 Windows 上啓動、停止及重新啓動 SDConnector 程序

使用 [服務] 管理員來啓動、停止或重新啓動 SDConnector 程序。 SDConnector 程序會列在名稱「安全網域連接器」之下。

在 Solaris 和 Linux 上啓動、停止及重新啓動 SDConnector 程序

若要啓動 SDConnector 程序，請以 root 身分登入，開啓命令列主控台，然後輸入下列命令：

```
$ cd /etc/init.d

$ ./sdmconnector start
```

若要停止 SDConnector 程序，請發出 **./sdmconnector stop** 命令。

若要重新啓動 SDConnector 程序，請發出 **./sdmconnector restart** 命令。

第 3 章： 使用 Secure Domain Manager

本章說明如何將 SDManager 配置檔 (sdm.config) 匯入至 CA Spectrum，以及將安全網域中的 SDConnector 主機和裝置模型化。 本章也說明用來尋找 Secure Domain Manager 元件的 OneClick 工具。 這些元件用來 Ping 安全網域中的裝置。 Ping 裝置來檢視裝置 MIB，以及檢視 SDManager 和 SDConnector 模型的相關資訊。

本節包含以下主題：

匯入 SDManager 配置檔 (位於 p. 33)
模型化 SDConnector 主機 (位於 p. 34)
將安全網路網域中的裝置模型化 (位於 p. 36)
存取 Secure Domain Manager 搜尋 (位於 p. 39)
檢查安全網域中的裝置存取性 (位於 p. 39)
檢視安全網域中的裝置 MIB (位於 p. 39)
SDManager 模型資訊檢視 (位於 p. 40)
SDConnector 模型資訊檢視 (位於 p. 42)

匯入 SDManager 配置檔

在開始將 OneClick 用於 Secure Domain Manager 產品之前，以及每次要更新 SDManager 配置時，必須將 sdm.config 檔匯入至 CA Spectrum。 如需配置 sdm.config 參數的詳細資訊，請參閱設定 SDManager 程序設定 (位於 p. 27)。

附註：您可以在建立 SDConnector 主機的模型之前或之後匯入 SDManager 配置檔。不過，如果是在建立 SDConnector 主機的模型之前匯入 sdm.config 檔，則 CA Spectrum 會自動將主機模型化爲 SDConnectorProcess 模型類型。 如需模型化選項的詳細資訊，請參閱「模型化 SDConnector 主機 (位於 p. 34)」，包括如何將 SDConnector 模型化爲 Pingable 和 Host_Device 模型類型。

匯入 SDManager 配置檔

1. 在 OneClick 主控台的 [導覽] 面板中，按一下 Secure Domain Manager。
2. 按一下 [元件詳細資料] 面板中的 [資訊] 索引標籤，並展開 [配置] 子檢視。
3. 按一下 [匯入]。

   [匯入 Secure Domain Manager 配置] 確認對話方塊隨即開啓。

4. 按一下 [是]，確認您要匯入 SDManager 配置檔 (sdm.config)。

   [匯入 Secure Domain Manager 配置] 對話方塊會指出匯入是否順利開始。此對話方塊也提供資訊讓您檢查輸出記錄，以判斷匯入是否成功。SDM/Logs 目錄中的匯入記錄檔提供疑難排解資訊。匯入未成功時，可使用這些資訊來修正錯誤。

5. 按一下 [確定]。

   如果已正確匯入配置檔，[Secure Domain Manager 狀態] 欄位會顯示「已配置」。如果匯入的 sdm.config 檔中沒有引數來定義 SDManager 與 SDConnector 之間的連線建立方式，則 SDManager 會停用，而 [Secure Domain Manager 狀態] 欄位會顯示「未配置」。

   附註：編輯 sdm.config 檔時，如果 SpectroSERVER 未執行，則 SpectroSERVER 啓動時會自動匯入新的 sdm.config 檔。您可以檢查最新的記錄檔，以確認匯入是否成功。

模型化 SDConnector 主機

在 OneClick 拓撲檢視中使用 [依類型模型化] 選項，將 SDConnector 主機電腦模型化爲下列三種模型類型之一：

SDConnectorProcess

SDConnectorProcess 模型類型是 SDConnector 的預設模型類型。 此模型類型不允許您管理裝置狀態，但可讓您看到 OneClick Secure Domain Manager 模型階層中顯示的主機電腦，還能存取 SDConnector 模型資訊檢視 (位於 p. 42)中討論的檢視。

附註：讓 SDConnector 主機模型具有可清楚識別主機的有意義名稱。 模型名稱會出現在 OneClick 的 Secure Domain Manager 檢視中。

Host_Device

如果主機電腦執行 SNMP 代理程式，請使用 Host_Device 模型類型。

Pingable

如果主機電腦僅支援 ICMP，請使用 Pingable 模型類型。

如果您使用 Host_Device 或 Pingable 模型類型，則可以監控主機電腦的狀態。如需有關將 SDConnector 主機模型化爲 Host_Device 或 Pingable 模型以利用 CA Spectrum 錯誤隔離功能的詳細資訊，請參閱「SDConnector 模型化和 CA Spectrum 錯誤隔離 (位於 p. 35)」。

SDConnector 模型化注意事項

- 如果您未在最初匯入 SDManager 配置檔之前就建立 SDConnector 主機電腦的模型，CA Spectrum 預設會自動將該電腦模型化爲 SDConnectorProcess 類型類型。
- 如果想要將主機模型化爲 Pingable 或 Host_Device，請在匯入之前就將主機模型化爲想要的類型。 或者，也可以在匯入之後終結 SDConnectorProcess 模型。 然後，將主機模型化爲 Pingable 或 Host_Device。

  附註：如果使用 [依 IP 模型化] 選項來建立代表 SDConnector 主機的模型，但未先終結現有的 SDConnectorProcess 模型，CA Spectrum 會複製 SDConnectorProcess 模型，並貼到原先叫用 [依 IP 模型化] 選項的拓撲檢視中。
- 即使在 OneClick 中終結 SDConnector 主機模型，CA Spectrum 仍然可以使用實際的 SDConnector 進行裝置通訊。 若要終結 SDConnector，必須編輯 sdm.config 檔來移除 SDConnector，再重新匯入 SDManager 配置。
- 如果您不小心終結 SDConnectorProcess 模型，則下次匯入 SDManager 配置檔時，CA Spectrum 會重建模型。 如果終結 Pingable 或 Host_Device 模型，則您下次匯入 SDManager 配置檔時，CA Spectrum 會建立 SDConnectorProcess 模型。 如果要還原 Pingable 或 Host_Device 模型，請明確重建模型，再匯入配置檔。

SDConnector 模型化和 CA Spectrum 錯誤隔離

如「模型化 SDConnector 主機 (位於 p. 34)」所述，在模型化 SDConnector 時，您可以選擇下列其中一種模型類型：

- SDConnectorProcess
- Host_Device
- Pingable

建議將 SDConnector 主機模型化爲 Host_Device 或 Pingable 模型類型。 當遠端 SDConnector 程序關閉或中斷連線時，這些模型類型可讓 CA Spectrum 錯誤隔離正確運作。CA Spectrum 會將中斷原因隔離到 SDConnector 主機模型，幾乎可消除所有未解決的錯誤警報。

儘管如此，SDConnector 主機通常會連線至網路邊緣的交換器。 但是，它在邏輯上會作爲公用網域和安全網域區域之間的橋梁。請據此將它模型化。對於在公用網域和安全網域區域之間路由傳送流量的裝置，請將 SDConnector 主機模型放在代表這兩個裝置的模型之間。 下圖說明此連線，其中將 SDConnector 顯示爲 Host_Device 模型。

將安全網路網域中的裝置模型化

模型化 SDConnector 主機之後，接著將 SDConnector 主機所在安全網域中您要管理的網路裝置模型化。使用 OneClick 的 [依 IP 建立模型] 選項或 [搜索]，一次模型化一個網路裝置。 您可以將模型放在拓撲檢視中的任意處。 成功建立模型之後，CA Spectrum 就可以使用 SDConnector 程序來與它們通訊。

依 IP 建立模型

使用 OneClick 的 [依 IP 建立模型] 選項，將安全網域中的每個裝置模型化。

附註：如需在 OneClick 中模型化的詳細資訊，請參閱《*模型化與管理 IT 基礎結構管理員指南*》。

使用 [依 IP 模型化] 選項將安全網域中的裝置模型化

1. 在拓撲檢視中按一下 [依 IP 模型化] 選項。

   [依 IP 位址建立模型] 對話方塊隨即開啓。

2. 在 [網路位址] 欄位中，輸入您要模型化的裝置的網路位址。

3. 從 [安全網域] 下拉式清單中，選取您要模型化之裝置所在的安全網域中，執行 SDConnector 之主機的 IP 位址，或選取已配置給該 SDConnector 主機的名稱。

   附註：您可以在 OneClick 中變更主機模型名稱，以提供 SDConnector 主機的安全網域名稱。 如需將安全網域名稱當作可選選項的詳細資訊，請參閱「SDManager 模型資訊檢視 (位於 p. 40)」。

4. 在 [SNMP 通訊選項] 區段中，選取與您要管理的裝置相容的 SNMP 版本。

5. 按一下 [確定]。

搜索

使用 OneClick [搜索] 來搜索和模型化 SDConnector 主機所在安全網域中的所有裝置。 搜索具有重疊 IP 位址的裝置時，請記住下列重點：

- 每次搜索只能使用一個 SDConnector。
- 雖然可以使用第 2 層對應，但其有效性取決於 [來源位址] 和 [跨距樹狀目錄] 表格的正確性。
- [通訊協定選項] 設定：
  - 不使用第 3 層自動搜索對應。 在 [通訊協定選項] 對話方塊中，取消選取 [IP 位址表格] 和 [IP 路由表格]。
  - 不在 Cisco 或 Nortel 環境中使用「專屬搜索通訊協定」，因為它們會使用 IP 位址來表達鄰近項目關係。 在 [通訊協定選項] 對話方塊中，取消選取 [專屬搜索表格]。
  - 不使用 Pingable 對應。 在 [通訊協定選項] 對話方塊中，取消選取 [Pingable 的 ARP 表格]。

使用 SDConnector 主機來搜索裝置

請依循下列步驟:

1. 從主功能表中，依序按一下 [工具]、[公用程式]、[搜索主控台]。

   [搜索主控台] 隨即開啟。

2. 對於您要將其中裝置模型化的安全網域，完成「搜索」配置。

   附註：如需配置「搜索」的詳細資訊，請參閱《*模型化與管理 IT 基礎結構管理員指南*》。

3. 在 [配置] 索引標籤中按一下 [進階選項]。

   [進階選項] 對話方塊隨即開啓。

4. 從 [搜索選項] 區段的 [安全網域] 下拉式清單中，選取此安全網域中執行 SDConnector 之主機的 IP 位址，或選取已指定給該安全網域的名稱。

   附註：您可以在 OneClick 中變更主機模型名稱，以提供 SDConnector 主機的安全網域名稱。 如需將安全網域名稱當作可選選項的詳細資訊，請參閱「SDManager 模型資訊檢視 (位於 p. 40)」。

5. 按一下 [確定]。

   [進階選項] 對話方塊隨即關閉，並儲存您的變更。

6. 在 [搜索主控台] 按一下 [搜索]。

   您配置的搜索會開始執行。 搜索之後，在相對應的 SDConnector 主機圖示的 [安全網域連接器裝置表格] 中，檢視所有列出的裝置。

   附註：如果已使用 SDConnectorProcess 模型將執行遠端 SDConnector 程序的主機機器模型化，而您在該主機所在的網路區域上執行「搜索」，則搜索會使用 Host_Device 或 Pingable 模型，建立額外的主機模型。 您可以在此重複的模型建立後加以刪除，或者從此模型建立之前已設定的搜索結果中，篩選掉此模型。

關於維護裝置安全網域成員資格

在 NAT 環境中，使用多個 SDConnector 來管理相同 IP 範圍。 重複 IP 範圍存在時，CA Spectrum 無法判斷是哪個 SDConnector 必須管理每個裝置。因此，請指定這項資訊。

在 CA Spectrum 中搜索或模型化新的裝置時，您可以使用 OneClick [依 IP 模型化] 檢視或 OneClick [搜索] 來設定安全網域。 若要更新現有裝置模型的安全網域，請使用 OneClick 屬性編輯器來編輯 [安全網域位址] 屬性。 這樣會自動更新 [安全網域名稱]。當新的 SDManager 配置檔 (sdm.config) 匯入至 CA Spectrum 後，任何已被指派給舊安全網域的現有裝置，仍然是被指派至該舊的安全網域。 這些模型上可能產生紅色警報。

存取 Secure Domain Manager 搜尋

OneClick 包含各種預先定義的 Secure Domain Manager 搜尋選項。

若要存取 Secure Domain Manager 搜尋選項，請在 [OneClick 主控台] 的 [搜尋器] 索引標籤中，展開 Secure Domain Manager 資料夾。

這時會顯示預先定義供您使用的 Secure Domain Manager 搜尋。

檢查安全網域中的裝置存取性

使用 OneClick Ping 功能表選項來 Ping 安全網域中的裝置，以判斷是否可存取裝置。

附註：Ping 成功時，並不會顯示安全網域中被 Ping 的裝置所傳回的位元組數。

若要檢查安全網域中的裝置存取性，請在 [OneClick 主控台] 以滑鼠右鍵按一下您要評估存取性的裝置，然後按一下 Ping。

Ping 對話方塊隨即開啟，列出 Ping 要求的結果。 例如：

```
Secure reply from 10.254.1.5: icmp_seq=4. time =140. ms
```

如果此裝置不在安全網域中，則出現的結果如下：

```
64 bytes from 10.254.1.5: icmp_seq=4. time =140. ms
```

檢視安全網域中的裝置 MIB

使用 MIB 工具來檢視安全網域中的裝置 MIB。 首先，為裝置所在的安全網域指定 SDConnector。 下列程序說明如何指定 SDConnector。

附註：如需使用 MIB 工具的詳細資訊，請參閱《*憑證使用者指南*》。

請依循下列步驟:

1. 選取您要使用 MIB 工具來調查的裝置。
2. 以滑鼠右鍵按一下裝置，依序選取 [公用程式]、[MIB 工具]。

   「MIB 工具」隨即開啓。 [連絡準則] 中會預先填入裝置的所選 SNMP 連絡資訊。「MIB 工具」會嘗試連絡裝置。

   如果「MIB 工具」*無法*連絡裝置，則會出現錯誤訊息，而 [連絡狀態] 指標會變成紅色。

   如果「MIB 工具」*可以*連絡裝置，[連絡狀態] 指標會變成綠色。

   狀態對話方塊也會出現，其中顯示擷取及載入「MIB 工具」資料庫的進度。
3. 在 [連絡準則] 區段中，按一下 [進階選項]。

   [MIB 工具：進階選項] 對話方塊隨即出現。
4. 從 [安全網域] 下拉式清單中，選取適用的安全網域。
5. 按一下 [確定]。

   [進階選項] 對話方塊隨即關閉，並儲存您的變更。
6. 在 [連絡準則] 區段中按一下 [連絡]，確認「MIB 工具」可以成功連絡裝置。
7. 關閉「MIB 工具」。

   「MIB 工具」關閉，您也已指定裝置的 SDConnector。

SDManager 模型資訊檢視

在 [元件詳細資料] 面板的 [資訊] 索引標籤中，下列區段提供所選 SDManager 模型的相關資訊與配置控制：

一般資訊

[一般資訊] 區段提供 Secure Domain Manager 模型的標準資訊，例如模型類別和安全性字串。

配置

[配置] 區段包含下列內容：

匯入

將 SDManager 配置檔 (sdm.config) 匯入至 CA Spectrum。

Secure Domain Manager 狀態

指出 SDManager 的配置狀態，如下所示：

- **已配置**：指出已成功匯入檔案。
- **未配置**：指出從未匯入自訂或編輯的 sdm.config 檔、已匯入不含引數的 sdm.config 檔，或已匯入含有錯誤的 sdm.config 檔。

安全網域顯示選項

指定 CA Spectrum 是否顯示用來識別 SDConnector 主機 (及其網域) 或 SDConnector 主機 IP 位址的名稱。您可以從下拉式清單中選擇 [顯示安全網域名稱] 或 [顯示安全網域位址]。這會決定所有 OneClick 檢視中使用的 SDConnector 識別碼類型。

本機網域

指定針對本機管理的模型 (不在安全網域中的模型)，出現在 [安全網域] 欄中的文字。

預設值：直接管理

附註：只有已安裝 Secure Domain Manager 時，OneClick 清單中才會出現 [安全網域] 欄。

安全網域連接器清單

顯示所有目前正在遠端網路區域中執行 SDConnector 程序的主機機器。

下圖顯示所選 SDManager 模型的 [元件詳細資料] 面板範例：

更多資訊：

匯入 SDManager 配置檔 (位於 p. 33)

SDConnector 模型資訊檢視

[元件詳細資料] 面板的 [資訊] 索引標籤提供所選 SDConnector 的相關資訊。 [一般資訊] 和 [SPECTRUM 模型化資訊] 類別提供 SDConnector 模型的標準資訊。 還有一個模型類型編輯器區段包含下列子區段：

安全網域連接器裝置表格

[安全網域連接器裝置表格] 列出選取的 SDConnector 所管理的所有裝置。 它也可讓您列印、匯出及篩選裝置清單。 您可以在此清單中按一下裝置的 [名稱] 超連結，以直接瀏覽至拓撲檢視中的該裝置。

第 4 章： 在容錯環境中設定程序

本章說明如何設定 SDConnector，以連線至容錯 SpectroSERVER 環境中的主要和備用 SpectroSERVER 上的 SDManager。 本章也說明如何設定主要和備用 SDConnector。

本節包含以下主題：

在容錯 SpectroSERVER 環境中設定 SDManager (位於 p. 43)
設定容錯 SDConnector (位於 p. 44)

在容錯 SpectroSERVER 環境中設定 SDManager

在容錯 SpectroSERVER 環境中，請將 SDManager 同時安裝在主要 SpectroSERVER 和備用 SpectroSERVER 上。 與此 SDManager 通訊的每個 SDConnector，都會配置爲連線至主要與備用 SpectroSERVER。 如果主要 SpectroSERVER 失敗，備用 SpectroSERVER 會接管與每個 SDConnector 的通訊。

請依循下列步驟:

1. 在您要管理的每個安全網域上部署 SDConnector。

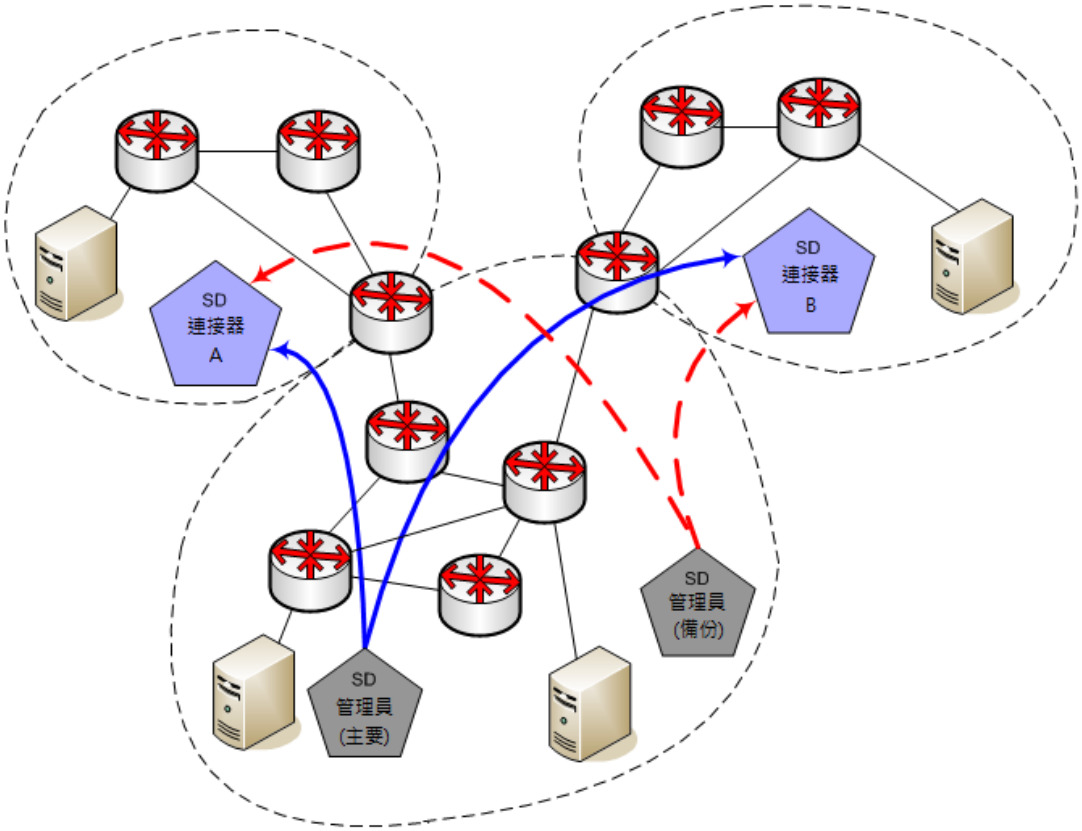
   附註：如需如何部署 SDConnector 的詳細指示，請參閱「安裝和配置 Secure Domain Manager 程序 (位於 p. 17)」。

2. 配置每個 SDConnector 以接受來自主要 SpectroSERVER 與備用 SpectroSERVER 的連線。 例如，分別是 172.24.1.2 和 172.24.3.4：

   ```
   -accept 172.24.1.2 -accept 172.24.3.4
   ```

容錯 SpectroSERVER (SDManager)

下圖顯示兩個 SDConnector 如何能連線至主要 SDManager，又能連線至備用 SDManager：



sdm.config 中同時對這兩個 SDManager 的配置設定：

```
-remoteconnect <SDConnector A 的 IP> -remoteconnect <SDConnector B 的 IP>
```

sdc.config 中同時對這兩個 SDConnector 的配置設定：

```
-accept <主要 SDManager 的 IP> -accept <備用 SDManager 的 IP>
```

設定容錯 SDConnector

Secure Domain Manager 是以個別 SDConnector 爲基礎來支援「備用」功能。備用 SDConnector 必須能夠管理主要 SDConnector 所管理的所有裝置，而不只是其中一部份。

當您將備用配置匯入至 CA Spectrum 時，系統不會自動將備用 SDConnector 模型化。 如果主要 SDConnector 關閉，備用功能就會*默默*接管。 不會有明顯跡象表示主要 SDConnector 已關閉。 另外，因爲備份並未模型化，所以不會出現在 OneClick 主控台的 [依 IP 模型化] 或 [搜索配置] 檢視中，也不會出現在「MIB 工具」中。

請依循下列步驟:

1. 對您要管理的每一個遠端網域，部署主要與備用 SDConnector。

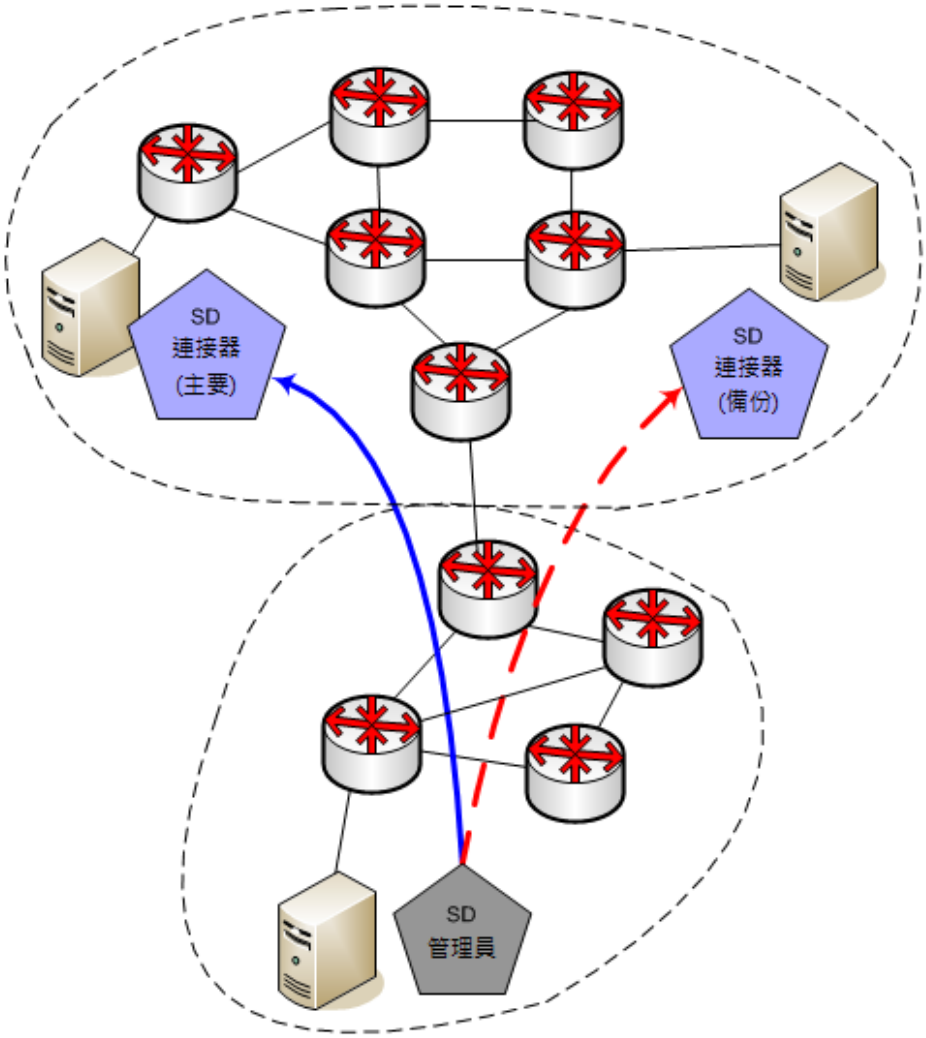
   附註：如需如何部署 SDConnector 的詳細指示，請參閱「安裝和配置 Secure Domain Manager 程序 (位於 p. 17)」。

2. 修改 sdm.config 檔，以配置 SDManager 來連線至主要與備用 SDConnector，如下列範例所示：

   `-remoteconnect <`*主要 SDC 的 IP*`> -remotebackup <`*備用 SDC 的 IP*`>`

容錯 SDConnector

下圖顯示兩個連線至單一 SDManager 的 SDConnector：



sdm.config 中對 SDManager 的配置設定：

```
-remoteconnect <主要 SDConnector 的 IP> -remotebackup <備用 SDConnector 的 IP>
```

sdc.config 中同時對這兩個 SDConnector 的配置設定：

```
-accept <SDManager 的 IP>
```

附錄 A： Secure Domain Manager 疑難排解

本節說明一些可能的 Secure Domain Manager 問題及其解決方案。

本節包含以下主題：

錯誤訊息 (位於 p. 47)
連接埠衝突 (位於 p. 48)
安裝問題 (位於 p. 48)

錯誤訊息

本節提供 Secure Domain Manager 錯誤訊息的相關資訊。 SDManager 錯誤出現在 SDManager.out 檔中；SDConnector 錯誤出現在終端機畫面。

憑證無效錯誤

適用於 Linux、Solaris 和 Windows

徵兆：

當憑證或安全性設定中出現不符時，就會出現下列 SDConnector 錯誤訊息：

`SdmEtpkiConnectEndpoint run()` 無效通訊端安全性。 將不嘗試連線至主機。

請確認憑證和安全性配置是否正確。

解決方案：

確認已部署 SSL 的機器是否有相符的憑證。

連接埠衝突

SDConnector 需要自訂的 SNMP 設陷連接埠

適用於 Linux、Solaris 和 Windows

如果需要變更 SDConnector 用來接聽 SNMP 設陷的設陷連接埠，請配置自訂的接聽連接埠。

附註：下列程序中使用連接埠 951 作爲新的自訂接聽連接埠的範例。

請依循下列步驟:

1. 修改 sdc.rc 檔，以配置 SDConnector 在自訂連接埠上接聽設陷，如下所示：

   ```
   snmp_trap_port = 951
   ```

2. 將電腦重新開機來重新啟動 SDConnector 程序。

   現在 SDConnector 會在連接埠 951 上接聽設陷。

安裝問題

有些 Windows 安裝上沒有安裝 SDConnector 服務。 或者，雖然已安裝，但未啟動。 那麼，請在 Windows 上手動安裝 SDConnector 服務。

請依循下列步驟:

1. 在命令提示字元中，切換至下列資料夾：

   <SDC 安裝目錄>/bin

2. 執行下列命令：

   ```
   SdmConnectorService.exe --install
   ```

3. 從 [服務] 視窗啟動服務，或執行下列命令：

   ```
   SdmConnectorService.exe --start
   ```