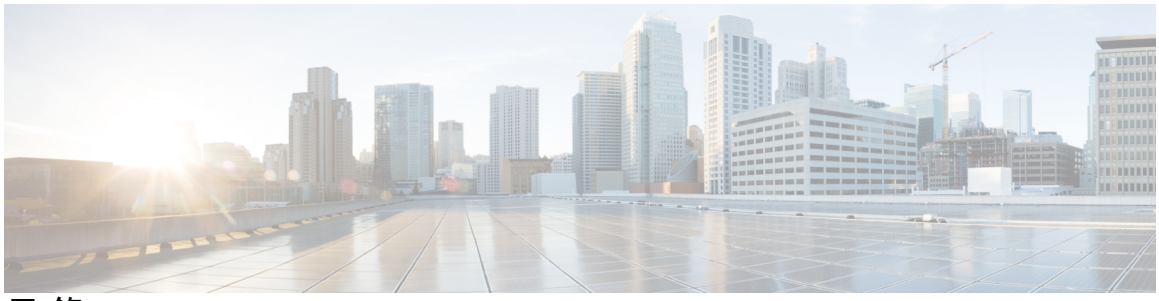
Cisco Unified Communications Manager 管理指南，版本 12.5(1)SU3

第一次發佈日期: 2020 年 8 月 13 日

上次修改日期: 2024 年 2 月 13 日

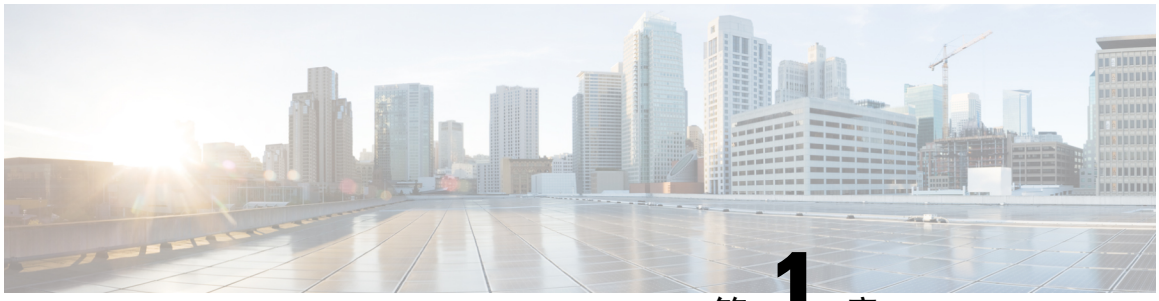
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



目錄

第 I 部分

管理概觀



第 1 章

管理概觀

Cisco Unified CM 管理概覽

Cisco Unified CM 管理是一個基於 Web 的應用程式，其爲 Cisco Unified Communications Manager 的主要管理和組態介面。 您可以使用 Cisco Unified CM 管理設定系統的各種項目，包括一般系統元件、功能、伺服器設定、通話路由規則、電話、一般使用者和媒體資源。

組態功能表

Cisco Unified CM 管理的組態視窗分爲下列功能表：

- 系統—使用此功能表底下的組態視窗設定一般系統設定，例如伺服器資訊、NTP 設定、日期與時間群組、地區、DHCP、LDAP 整合和企業參數。
- 通話路由—使用此標籤底下的組態視窗設定與 Cisco Unified Communications Manager 路由通話的方式相關的項目，包括路由型式、路由群組、搜尋引導、撥號規則、分區、通話搜尋範圍、目錄號碼和轉換型式。
- 媒體資源—使用此標籤下的組態視窗設定媒體資源群組、會議橋接器、通報器和轉碼器等項目。
- 進階功能—使用此標籤下的組態視窗設定語音信箱引導、留言和與通話控制代理設定檔等功能。
- 裝置—使用此標籤下的組態視窗設定裝置，例如電話、IP 電話服務、trunk、閘道、軟鍵範本和 SIP 設定檔。
- 應用程式—使用此標籤下的組態視窗下載及安裝外掛程式，例如 Cisco Unified JTAPI、Cisco Unified TAPI 和 Cisco Unified 即時監控工具。
- 使用者管理—使用「使用者管理」標籤下的組態視窗設定系統的一般使用者和應用程式使用者。

- 批量管理—使用「批量管理工具」一次匯入及設定大量一般使用者或裝置。
- 描述—按一下此功能表可存取線上說明系統。 線上說明系統包含可協助您在系統上設定各種組態視窗的檔案。

作業系統管理概覽

使用 Cisco Unified Communications 作業系統管理設定及管理您的作業系統，並執行下列管理工作：

- 檢查軟體和硬體狀態
- 檢查及更新 IP 位址
- 對其他網路裝置進行 ping
- 管理 NTP 伺服器
- 升級系統軟體和選項
- 管理節點安全性，包括 IPSec 和憑證
- 管理遠端支援帳戶
- 重新啓動系統

作業系統狀態

您可以檢查不同作業系統元件的狀態，包括下列：

- 叢集和節點
- 硬體
- 網路
- 系統
- 安裝的軟體和選項

作業系統設定

您可以檢視及更新下列作業系統設定：

- IP—更新安裝應用程式時您輸入的 IP 位址和 DHCP 用戶端設定。
- NTP 伺服器設定—設定外部 NTP 伺服器的 IP 位址；新增 NTP 伺服器。
- SMTP 設定—設定作業系統將用於傳送電子郵件通知的簡易郵件傳輸通訊協定 (SMTP) 主機。

作業系統安全性組態

您可以管理安全性憑證和 IPSec 設定。 您可以從 **Security** 功能表中，選擇下列安全性選項：

- Certificate Management—管理憑證和憑證簽署請求 (CSR)。 您可以顯示、上傳、下載、刪除及產生憑證。 透過憑證管理，您也可以監控節點上的憑證到期日。
- IPsec Management—顯示或更新現有 IPSec 原則；設定新的 IPSec 原則和關聯。

軟體升級

您可以升級作業系統上執行的軟體版本，或安裝特定軟體選項，包括 Cisco Unified Communications 作業系統地區設定安裝程式、撥號計劃和 TFTP 伺服器檔案。

您可以從**安裝/升級**功能表選項，從本機光碟或遠端伺服器升級系統軟體。 升級的軟體安裝於非作用中的分區，您可以重新啓動系統及切換分區，以讓系統開始在新的軟體版本執行。 如需詳細資訊，請參閱 *Upgrade Guide for the Cisco Unified Communications Manager*（Cisco Unified Communications Manager 升級指南）：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html。

附註 您需透過 Cisco Unified Communications 作業系統介面和 CLI 包含的軟體升級功能來執行所有軟體安裝和升級。 系統僅可上傳及處理 Cisco Systems 核准的軟體。 您無法安裝或使用第三方或 Windows 平台軟體應用程式。

服務

應用程式提供下列作業系統公用程式：

- 偵測—檢查與其他網路裝置的連線。
- 遠端支援—設定 Cisco 支援人員可用於存取系統的帳戶。 此帳戶會在您指定的天數後自動到期。

CLI

您可以從作業系統存取 CLI 或透過安全 Shell 連線至伺服器。 如需詳細資訊，請參閱 *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*（Cisco Unified Communications 解決方案的命令行介面參考指南）：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

經過驗證的網路時間通訊協定支援

12.0 (1) 版本即支援 Cisco Unified Communications Manager 的網路時間通訊協定 (NTP) 已驗證功能，新增此支援是爲了將 Cisco Unified Communications Manager 的 NTP 伺服器連線安全化。 舊版本中，Cisco Unified Communications Manager 至 NTP 伺服器的連線不安全。

此功能以對稱金鑰型驗證爲基礎，且受 NTPv3 和 NTPv4 伺服器支援。 Cisco Unified Communications Manager 僅支援 SHA1 加密。 NTP 4.2.6 版和更高版本可使用 SHA1 對稱金鑰支援。

- 對稱金鑰
- 沒有驗證

您可以透過管理 CLI 或 **Cisco Unified 作業系統管理**應用程式的 **NTP 伺服器清單**頁面檢查 NTP 伺服器的驗證狀態。

自動金鑰驗證的網路時間通訊協定支援

Cisco Unified Communications Manager 也支援透過自動金鑰功能（以公開金鑰基礎結構爲基礎的驗證）進行網路時間通訊協定 (NTP) 驗證。 此功能僅適用於發佈者節點。

Redhat 建議透過 Autokey 進行對稱金鑰驗證。 如需更多資訊，請參閱https://access.redhat.com/support/cases/#/case/01871532。

已新增此功能，因爲 Common Criteria 憑證是以 PKI 爲基礎的驗證的必需條件。

僅在 Cisco Unified Communication Manager 啓用通用條件模式時始可使用 NTP 伺服器上的 IFF 身分配置配置以 PKI 爲基礎的驗證。

您可以在 Cisco Unified Communications Manager 上啓用對稱金鑰或以 PKI 爲基礎的 NTP 驗證。

若您嘗試在啓用 PKI 的伺服器上啓用對稱金鑰，便會顯示下列警告訊息：

警告 使用 Autokey 的 NTP 驗證目前啓用中，需停用才能啓用對稱金鑰。 請使用「utils ntp auth auto-key disable」命令停用 NTP 驗證，然後重試此命令。

若您嘗試在啓用對稱金鑰的伺服器上啓用 Autokey，便會顯示下列警告訊息：

警告 使用對稱金鑰的NTP驗證目前啓用中，需停用才能啓用Autokey。 請使用「utils ntp auth symmetric-key disable」命令停用 NTP 驗證，然後重試此命令。

附註 NTP 伺服器需要 NTP 版本 4 和 RPM 版本 ntp-4.2.6p5-1.el6.x86_64.rpm 和更高版本。

您可以透過管理 CLI 或 Cisco Unified 作業系統管理應用程式的「NTP 伺服器清單」頁面檢查 NTP 伺服器的驗證狀態。

Cisco Unified Serviceability 概覽

Cisco Unified Serviceability是一個網頁式疑難排解工具，提供許多服務、警示和工具來協助系統管理員管理系統。 Cisco Unified Serviceability爲系統管理員提供的功能包括：

- Start and Stop Services（馬上啓動、馬上停止服務）—系統管理員可以設定各種協助各個系統管理員管理系統的服務。 例如，您可以透過允許系統管理員使用「即時監控工具」啓動 Cisco CallManager Serviceability RTMT 服務，從而監控系統的狀態。
- SNMP—SNMP 提供網路裝置（例如節點、路由器等）之間的管理資訊交換。 作爲 TCP/IP 通訊協定的一部分，SNMP 可讓管理員遠端管理網路效能、尋找及解決網路問題，以及計畫網路成長。
- 警示—警示提供執行階段狀態和系統狀態的資訊，以便讓您針對與系統相關的問題進行疑難排解。

- 追蹤—追蹤工具可協助您針對語音應用程式的問題進行疑難排解。
- Cisco Serviceability 回報工具—Cisco Serviceability 回報工具 會在 Cisco Unified Serviceability中產生每日報告。
- SNMP—SNMP 提供網路裝置（例如節點、路由器等）之間的管理資訊交換。 作爲 TCP/IP 通訊協定的一部分，SNMP 可讓管理員遠端管理網路效能、尋找及解決網路問題，以及計畫網路成長。
- CallHome—設定 Cisco Unified Communications Manager Call Home 功能，讓 Cisco Unified Communications Manager 進行通訊，以及將診斷警示、庫存和其他訊息傳送至 Smart Call Home 後端伺服器。

其他管理介面

透過使用 Cisco Unified Serviceability，您可以啓動可讓您使用下列其他管理介面的服務：

- 即時監控工具—即時監控工具是一個網頁式介面，可協助您監控系統狀態。 透過使用 RTMT，您可以檢視警示、計數器和包含系統狀態詳細資訊的報告。
- Dialed Number Analyzer（撥出號碼分析器）—撥出號碼分析器是 Web 型介面，可協助管理員使用撥號計畫進行疑難排解。
- Cisco Unified CDR 分析與報告—CDR 分析與報告會收集通話詳細資料記錄，這些記錄顯示已在系統上撥出的通話詳細資料。

如需如何使用 Cisco Unified Serviceability的詳細資訊，請參閱《*Cisco Unified Serviceability*管理指南》：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

Cisco Unified Reporting概覽

Cisco Unified Reporting Web 應用程式會產生疑難排解或檢查 Cisco Unified Communications Manager 叢集資料的報告。 您可於 Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service 主控台存取應用程式。

此工具提供輕鬆取得叢集資料概觀的方式。 工具會從現有來源收集資料、比較資料及回報不正確之處。 在 Cisco Unified Reporting中產生報告時，報告會將一或多部伺服器上的一或多個來源的資料合併爲一個輸出檢視。 例如，您可以檢視下列報告，以協助您管理系統：

- Unified CM 叢集概覽—檢視此報告可取得叢集的一個快照，包括 Cisco Unified Communications Manager 和 IM and Presence Service 的版本、伺服器主機和硬體詳細資料。
- 電話功能清單—若您在設定功能，可檢視此報告。 此報告提供支援 Cisco Unified Communications Manager 功能的電話清單。
- 無線路的 Unified CM 電話—檢視此報告可查看叢集中沒有電話線路的電話。

若需要 Cisco Unified 報告提供的報告完整清單，以及如何使用應用程式的說明，請參閱 *Cisco Unified Reporting Administration Guide*（*Cisco Unified* 報告管理指南）：http://www.cisco.com/c/en/us/support/

unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

災害復原系統概覽

災害復原系統 (DRS) 可從 Cisco Unified Communications Manager 管理叫用，提供完整的資料備份和還原功能。 災害復原系統可讓您執行定期排程自動備份或使用者叫用的資料備份。

DRS 會將其設定（備份裝置設定和排程設定）還原爲平台備份/還原的一部分。 DRS 會備份及還原 `drfDevice.xml` 和 `drfSchedule.xml` 檔案。 伺服器還原這些檔案時，您不需要重新設定 DRS 備份裝置和排程。

災害復原系統包含下列功能：

- 用於執行備份和還原工作的UI 。
- 用於執行備份及還原功能的分散式系統架構。
- 排程的備份。
- 將備份封存至實體磁帶機或遠端 SFTP 伺服器。

批量管理工具概覽

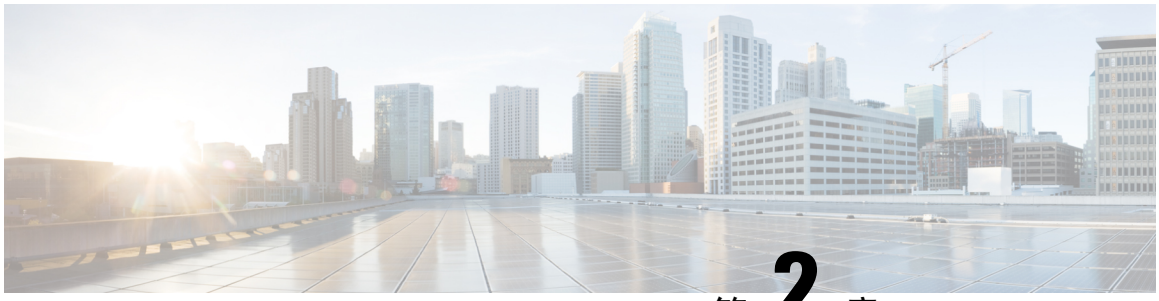
在 Cisco Unified CM 管理中，透過批量管理工具使用批量管理功能表和子功能表選項設定 Cisco Unified Communications Manager 中的實體。

Cisco Unified Communications Manager 批量管理工具 (BAT) 是一個網頁式應用程式，可讓管理員執行 Cisco Unified Communications Manager 資料庫的批量異動。 BAT 可讓您來同時新增、更新或刪除大量的類似電話、使用者或連接埠。 當您使用 Cisco Unified CM 管理時，每筆資料庫異動都需要個別的手動操作，而 BAT 則會將此流程自動化，並實現更快的新增、更新和刪除操作。

您可以使用 BAT 來處理以下類型的裝置和記錄：

- 新增、更新及刪除 Cisco IP 電話、閘道、電話、電腦電話介面 (CTI) 通訊埠和 H.323 用戶端
- 新增、更新及刪除使用者、使用者裝置設定檔、Cisco Unified Communications Manager Assistant 管理員和助理
- 新增或刪除強制授權代碼和用戶端事件代碼
- 新增或刪除代接來電群組
- 填入或取消填入地區對照
- 插入、刪除或匯出存取清單
- 插入、刪除或匯出遠端目的地和遠端目的地設定檔
- 新增基礎架構裝置

如需如何使用批量管理工具的詳細資訊，請參閱《*Cisco Unified Communications Manager* 批量管理指南》。



第 2 章

開始使用

登入管理介面

使用此流程以登入系統中的任何管理介面。

程序

步驟 1 在網頁瀏覽器中開啓 Unified Communications Manager 介面。

步驟 2 從**導覽**下拉式清單中選擇管理介面。

步驟 3 按一下 **Go (執行)** 。

步驟 4 輸入您的使用者名稱與密碼。

步驟 5 按一下 **登入**。

重設安全性密碼的管理員

若遺失管理員密碼而無法存取系統，請使用此流程重設密碼。

附註 要在 IM and Presence 節點上更改密碼請在重設系統管理員密碼之前在所有 IM and Presence 節點中停止 Cisco Presence Engine 服務。 密碼重設後，在所有節點中重新啓動 Cisco Presence Engine 服務。確保在維護期間執行此任務，因爲停止 PE 時可能會遇到狀態問題。

開始之前

- 您需要實際存取執行此流程的節點。
- 在任何時間點，當要求您插入 CD 或 DVD 媒體時，您需透過 VMWare 伺服器的 vSphere 用戶端安裝 ISO 檔案。 若需指引如何繼續操作，請參閱“將 DVD 或 CD 光碟機新增至虛擬機”https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.html。
- 叢集中所有節點的安全性密碼皆需符合。 請變更所有機器上的安全密碼，否則叢集節點不會進行通訊。

程序

步驟 1 使用下列使用者名稱和密碼登入發佈者節點上的 CLI：

a) 使用者名稱：**pwrecovery**

b) 密碼：**pwreset**

步驟 2 按任意鍵繼續。

步驟 3 若您的硬碟機中有有效 CD/DVD，或您已安裝 ISO 檔案，請將它從 VMWare 用戶端移除。

步驟 4 按任意鍵繼續。

步驟 5 將有效的 CD 或 DVD 插入硬碟機，或安裝 ISO 檔案。

附註 在此測試中，您需使用僅資料的硬碟或 ISO 檔案。

步驟 6 系統驗證最後一個步驟後，便會提示您輸入下列其中一個選項以繼續：

- 輸入 **a** 重設管理員密碼。
- 輸入 **s** 重設安全性密碼。

附註 變更安全性密碼後，您需重設叢集中的每個節點。 節點重新啟動失敗會導致系統服務問題和訂閱者節點管理視窗問題。

步驟 7 輸入新密碼，然後再次輸入以進行確認。

管理員憑證需以字母字元開頭，長度至少六個字元，可包含英數字元、連字符和底線。

步驟 8 系統驗證新密碼的長度後，便會重設密碼，並提示您按任意鍵結束密碼重設公用程式。

若要設定不同管理員密碼，請使用 **set password** CLI 命令。 如需詳細資訊，請參閱 *Command Line Interface Reference Guide for Cisco Unified Solutions*（Cisco Unified 解決方案的命令行介面參考指南）：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

關閉或重新啟動系統

如需關閉或重新啓動系統（例如，進行組態變更後），請使用此流程。

開始之前

若伺服器強制關閉並從虛擬機器重新啓動，檔案系統可能已損毀。 若要避免強制關機，請在此流程或從 CLI 執行**utils system shutdown** 後等待伺服器正確關閉。

附註 建議您以 utils system shutdown CLI 命令於虛擬機上關閉或重新啓動。 system-history.log 顯示命令項目，並被視爲正常關機。 若關閉或重新啓動是透過 vSphere Client 完成的，則將其視爲不正常的關閉，且該項目在 system-history.log 中不可用。 從 10.x 版開始，不支援自 vSphere Client 關機/重新啓動。

附註 若從 VMware 管理工具（vCenter 或嵌入式主機用戶端）強制關閉或重新啓動虛擬機，請執行以下操作：

- 從 12.5（1）SU3 或更早版本開始，這將是不正常的關閉/重新啓動，並且檔案系統可能已損壞。非正常關機將顯示在 system-history.log 中。 相反地我們建議您使用 utils system shutdown CLI 命令正常關閉/重新啓動（這將在系統歷史記錄中顯示爲正常關閉/重新啓動）。

程序

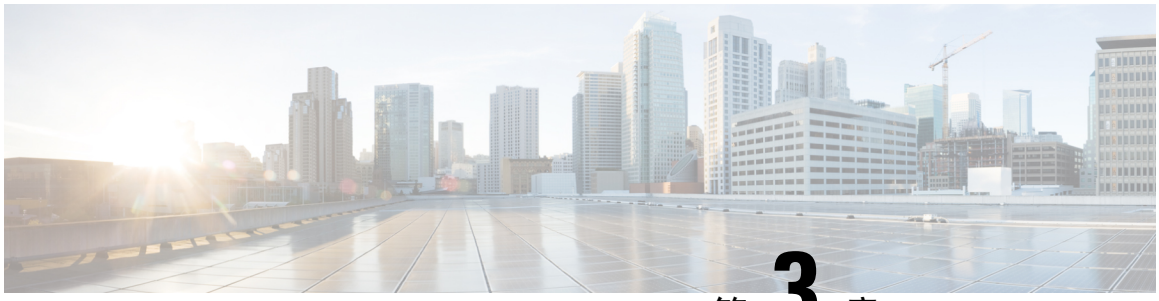
步驟 1 在 Cisco Unified OS Administration 中選擇 **設定** > **版本**。

步驟 2 請執行下列一項動作：

- 按一下**關閉**停止所有流程並關閉系統。
- 按一下**重新啟動**停止所有流程並重新啓動系統。

第 II 部分

管理使用者



第 3 章

管理使用者存取

使用者存取概覽

您可配置下列的項目以管理 Cisco Unified Communications Manager 的使用者存取：

- 存取控制群組
- 角色
- 使用者等級

存取控制群組概覽

存取控制群組是使用者與指派給這些使用者的角色的一個清單。 當您將一般使用者、應用程式使用者或管理員使用者指派給存取控制群組時，該使用者將取得與該群組關聯的角色的存取權限。 您可以將具有類似存取需求的使用者指派給僅具有他們所需的角色和權限的存取控制群組，來管理系統存取。

存取控制群組分爲兩類：

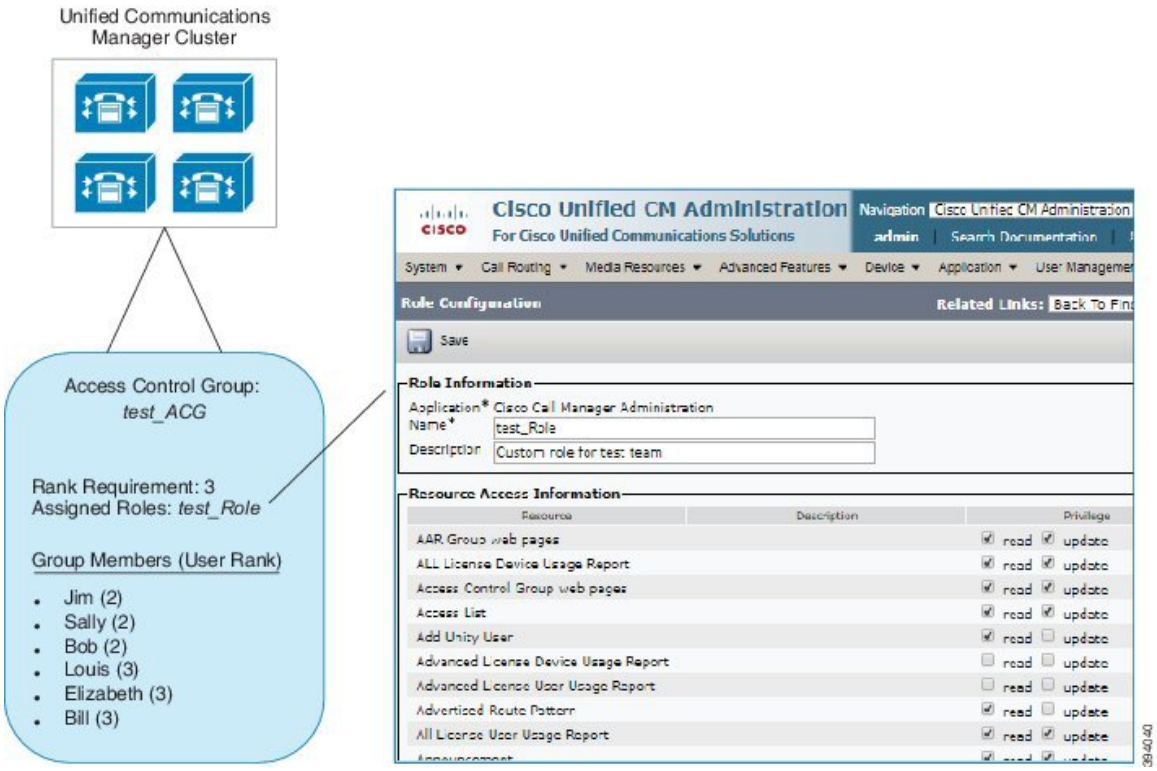
- 標準存取控制群組-爲預先定義的預設群組，其角色指派可以滿足常見的部署需求。 您不能在標準群組中編輯角色的指派， 除了本來就具有的修改使用者等級要求功能，您還可新增和刪除使用者， 有關標準存取控制群組及其相關角色的清單，請參閱標準角色和存取控制群組 ，第 28 頁上的。
- 自訂存取控制群組-當標準組都不包含滿足您需求的角色權限時，創建您自己的存取控制群組。

使用者等級框架爲可以指派使用者的存取控制群組提供了一組控制。 若要被指派到某存取控制群組，使用者需符合該群組的最低等級。 例如，只能將使用者等級爲 4 的一般使用者指定給最低等級要求介於 4 到 10 之間的存取控制群組。不能將這些使用者指定給最低等級爲 1 的群組。

範例-具有存取控制群組的角色權限

以下範例說明了一個叢集，在該叢集中測試團隊的成員被指派到**test_ACG**存取控制群組。 右側的螢幕截圖顯示了 test_Role 的存取設定，它是與存取控制群組關聯的角色。 另請注意，存取控制群組的最低等級要求爲 3。所有群組成員的等級必須介於 1-3 之間，才能加入群組。

圖 *1:* 存取控制群組的角色權限



角色概覽

使用者透過與使用者所屬的存取控制群組建立關聯的角色取得系統存取特權。 每個角色都包含一組附加到特定資源或應用程式的權限，例如 Cisco Unified CM 管理或 CDR 分析和回報。 對於諸如 Cisco Unified CM 管理之類的應用程式而言，角色可能包含允許您檢視或編輯應用程式中特定 GUI 頁面的權限。 您可以爲資源或應用程式指派三個等級的權限：

- 讀取-允許使用者檢視資源的設定。
- 更新-允許使用者編輯資源的設定。
- 無存取權限-若使用者無“讀取”或“更新”存取權限則其無權檢視或編輯既定資源的設定。

角色類型

設定使用者時，需確定要套用的角色，然後將使用者指派給包含該角色的存取控制群組。 Cisco Unified Communications Manager 中的角色主要有兩種：

- 標準角色-這些是預安裝的預設角色，旨在滿足常見部署的需求。 您不能編輯標準角色的權限。
- 自訂角色-若沒有標準角色具有您所需的權限，則您可建立自訂的角色。 另外，若您需要更細緻的存取控制級別，則可以套用進階設定來控制管理員編輯關鍵使用者設定的能力。（如需詳細資訊，請參閱下面的章節）。

進階角色設定

當您建立自訂角色時，您可以將詳細控制等級新增至**應用程式使用者**和**一般使用者組態**視窗中的選定欄位。

進階角色組態視窗可讓您配置對 Cisco Unified CM 管理的存取，同時限制對以下任務的存取：

- 新增使用者
- 編輯密碼
- 編輯使用者等級
- 編輯存取控制群組

下表詳述您可以透過此組態套用的其他控制項：

表 *1:* 進階資源存取資訊

進階資源	存取控制
權限資訊	控制用來新增或編輯存取控制群組的功能： • **檢視**—使用者可以檢視存取控制群組，但是無法新增、編輯或刪除存取控制群組。 • **更新**—使用者可以新增、編輯或刪除存取控制群組。 **附註** 若這兩個值都未選擇，則無法使用**權限資訊**區段。 **附註** 若您選擇**檢視**，**使用者可以為自己的使用者更新權限資訊**欄位設定爲**無**且被停用。 若您希望能夠編輯此欄位，則需設置**權限資訊**到**更新資料**。
使用者可以爲自己的使用者更新權限資訊	控制使用者編輯自己的存取權限的能力： • **是**—使用者可以更新自己的權限資訊。 • **否**—使用者無法更新自己的權限資訊。 但使用者可以查看或修改相同或較低級別使用者的權限資訊。 **附註** 若**權限資訊更新**選取方塊未勾選，則會將**使用者可更新自己使用者的權限資訊**欄位設定爲**無**並停用。

進階資源	存取控制
使用者等級	控制用來變更使用者等級的功能： • **檢視**—使用者可以檢視使用者等級，但無法變更使用者等級。 • **更新**—使用者可以變更使用者等級。 **附註** 若這兩個值都未選擇，則無法使用**使用者等級**區段。 **附註** 若您選擇**檢視**，**使用者可以將自己使用者**的等級欄位設定爲**無**並停用。 若您希望能夠編輯此欄位，則需將**使用者等級**設爲**更新**。
使用者可以爲自己的使用者更新使用者等級	控制使用者編輯自己的使用者等級的能力： • **是**—使用者可以更新自己的使用者等級。 • **否**—使用者無法更新自己的使用者等級。但使用者可以查看或修改相同或較低級別使用者的使用者等級。 **附註** 若**使用者等級更新**選取方塊未勾選，則會將**使用者可以更新自己使用者的使用等級**欄位會設定爲**無**並停用。
新增使用者	控制用來新增使用者的功能： • **是**—使用者可以新增使用者。 • **否**—無法使用**新增**按鈕。
密碼	控制變更密碼的功能： • **是**—使用者可以在**應用程式使用者資訊**區段底下變更使用者密碼。 • **否**—無法使用**應用程式使用者資訊**區段底下的**密碼**和**確認密碼**。

使用者等級概覽

「使用者等級存取控制」提供一組存取層級控制項，讓管理員提供給一般使用者或應用程式使用者。

佈建一般使用者或應用程式使用者時，管理員需爲每位使用者指定使用者等級。 管理員也可將使用者等級指派至各存取控制群組。 將使用者新增至存取控制群組時，管理員僅能將使用者指派到使用者的“使用者等級”已有滿足群組的等級要求的群組。 例如，管理員可以將使用者等級爲 3 的使用者指定給使用者等級要求介於 3 到 10 之間的存取控制群組。但是，管理員無法將該使用者指定給使用者等級要求爲 1 或 2 的存取控制群組。

管理員可以在**使用者等級組態視窗**，並在設定使用者和存取控制群組時可以使用該層次結構。 請注意，若您未配置使用者等級層次結構，或者在配置使用者或存取控制群組時僅不指定使用者等級設定，則會爲所有使用者和存取控制群組指派預設的使用者等級 1（最高排名可能）。

使用者存取必需條件

確保檢查您的使用者需求，以便您知道使用者需要什麼級別的存取權限。 您將要指派具有使用者所需存取權限的角色，但這些角色不提供對使用者不應存取的系統的存取權限。

建立新角色或存取控制群組前，請檢閱系統預先安裝的標準角色和存取控制群組，以檢查現有存取控制群組是否包含您的使用者需要的角色和權限。 如需詳細資訊，請參閱標準角色和存取控制群組，第 28 頁上的。

使用者存取組態工作流程

完成下列工作以配置使用者的存取。

開始之前

若要使用預設角色和存取控制群組，則可以跳過創建自訂角色和存取控制群組的任務。 您可以將使用者指派給現有的預設存取控制群組。

程序

	命令或動作	目的
步驟 1	配置使用者等級層次結構 ，第 19 頁上的	設定使用者等級層次結構。 請注意，若您跳過此任務，則會爲所有使用者和存取控制群組指派預設使用者等級 1（最高等級）。
步驟 2	建立自訂角色 ，第 20 頁上的	若預設角色沒有所需的存取權限，請創建自訂角色。
步驟 3	配置系統管理員進階角色 ，第 21 頁上的	選用。 自訂角色中的進階權限使您可以控制管理員編輯關鍵使用者設定的能力。
步驟 4	建立存取控制群組 ，第 21 頁上的	若預設的群組沒有所需的角色指派，您可建立自訂存取控制群組。
步驟 5	指派使用者至存取控制群組 ，第 22 頁上的	在標準或自訂存取控制群組中新增或刪除使用者。
步驟 6	設定存取控制群組的重疊權限原則 ，第 23 頁上的	選用。 若將使用者指派到具有衝突權限的多個存取控制群組，則使用此設定。

配置使用者等級層次結構

使用此流程可建立自訂使用者等級階層。

附註 若未配置使用者等級階層結構，則預設情況下將會爲所有使用者和存取控制群組指定一個使用者等級 1（可指定的最高等級）。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**使用者管理** > **使用者設定** > **使用者等級**。

步驟 2 按一下**新增**。

步驟 3 在**使用者等級**下拉式功能表中，選擇介於 1-10 之間的等級設定。 最高等級爲 1。

步驟 4 輸入**等級名稱**和**說明**。

步驟 5 按一下**儲存**。

步驟 6 重複此流程以新增其他使用者等級。
您可以將使用者等級指派給使用者和存取控制群組，以控制可以將使用者指派給哪些群組。

建立自訂角色

使用此流程可創建具有自訂特權的新角色。 若沒有具有所需確切權限的標準角色，則可能需要執行此操作。 建立角色有兩種方式：

- 點按**新增**按鈕以從零開始創建和配置新的角色。
- 若現有角色的存取權限接近您所需要的權限，則點按**複製**按鈕。 您可以將現有角色的特權複製到可編輯的新角色。

程序

步驟 1 在 Cisco Unified CM 管理中，按一下**使用者管理** > **使用者設定** > **角色**。

步驟 2 執行下列其中一項：

- 若要建立新的角色，請按一下**新增**。 選擇與該角色關聯的**應用程式**，然後點按**下一個**。
- 要自現有角色複製設定，請點按**尋找**並開啓現有角色。點按**複製**並輸入新角色的名稱。按一下**確定**。

步驟 3 輸入角色的**名稱**和**描述**。

步驟 4 請勾選各項資源方面的方塊：

- 若您希望使用者能夠檢視某項資源的設定，勾選**讀取**方塊。
- 若您希望使用者能夠編輯某項資源的設定，勾選**更新**方塊。
- 若要限制某項資源的存取則兩個方塊都請勿勾選。

步驟 5 按一下**允許存取全部**或**拒絕存取全部**按鈕可授予或移除此角色在頁面上顯示的所有資源的權限。

附註　若資源清單顯示在多個頁面上，此按鈕僅適用於目前頁面顯示的資源。 您需顯示其他頁面，並使用那些頁面上的按鈕來變更頁面所列的資源存取權。

步驟 6 點擊**儲存**。

配置系統管理員進階角色

您可透過“配置進階角色”在更詳細的等級上編輯自訂角色的權限。 您可在**一般使用者組態**和**應用程式使用者組態**視窗中控制管理員編輯以下關鍵設定的能力：：

- 編輯使用者等級
- 編輯存取控制群組之指定
- 新增使用者
- 編輯使用者的密碼

程序

步驟 1 在 Cisco Unified CM 管理中選擇 **使用者管理** > **使用者設定** > **角色**。
步驟 2 點按**尋找**並選擇一個自訂角色。
步驟 3 在**相關連結**中選擇**進階角色組態**然後點按**前往**。
步驟 4 在**資源網頁**中選擇**應用程式使用者網頁**或**使用者網頁**。
步驟 5 編輯設定。 如需有關欄位及其設定的描述，請參閱線上說明。
步驟 6 點擊**儲存**。

建立存取控制群組

若您需要建立新的存取控制群組，請執行此流程。 若沒有標準群組有您所需的角色和存取特權，則可能需要執行此操作。 有兩種創建自訂群組的方法：

- 點按**新增**按鈕以從零開始創建和配置新的存取控制群組。
- 若現有群組角色的指派與您所需要的相近，則點按**複製**按鈕。 您可以將設定從現有組複製到新的可編輯組。

程序

步驟 1 在「Cisco Unified CM 管理」中，選擇**使用者管理** > **使用者設定** > **存取控制群組**。
步驟 2 執行下列其中一項：

- 若要從零開始建立新的群組，請按一下**新增**。
- 要複製現有群組的設定，請點按**尋找**並開啓現有的存取控制群組。 點按**複製**並輸入新群組的名稱。 按一下**確定**。

步驟 3 爲存取控制群組輸入**名稱**。

步驟 4 在**可供使用的最低使用者等級**下拉式清單中，選擇可將使用者指派至此群組的最低使用者等級。 預設使用者等級爲 1。

步驟 5 按一下**儲存**。

步驟 6 指派角色給存取控制群組 您選擇的角色將指派給群組成員：

a) 在**相關連結**中選擇**指派角色給存取控制群組**，然後按一下**執行**。
b) 點按**尋找**搜尋現有角色。
c) 檢查您要新增的角色，然後點按**新增所選**。
d) 點擊**儲存**。

下一步

指派使用者至存取控制群組 ，第 22 頁上的

指派使用者至存取控制群組

在標準或自訂存取控制群組中新增或刪除使用者。 .

附註 您只可以爲存取控制群組新增使用者等級相同或高於最低使用者等級的使用者。

附註 若要從公司 LDAP 目錄同步新的使用者，且使用適當的權限創建了等級層次結構和存取控制群組，作爲 LDAP 同步的一部分，可將群組指定給已同步的使用者。 如需有關如何設定 LDAP 目錄同步的詳細資訊，請參閱 *Cisco Unified Communications Manager* 系統組態配置指南。

程序

步驟 1 選擇**使用者管理** > **使用者設定** > **存取控制群組**。

隨即顯示**尋找及列出存取控制群組**視窗。

步驟 2 按一下**尋找**並選擇您要更新使用者清單的存取控制群組。

步驟 3 在 **Available for Users with User Rank as**（**提供使用的使用者等級**）下拉式清單中，選擇讓使用者指派至此群組的最低使用者等級。

步驟 4 在**使用者**部分中，按一下**尋找**以顯示使用者清單。

步驟 5 若要將一般使用者或應用程式使用者新增至存取控制群組，請執行下列作業：

a) 按一下 **Add End Users to Access Control Group**（將一般使用者新增至存取控制群組）或 **Add App Users to Access Control Group**（將應用程式使用者新增至存取控制群組）。
b) 選擇您要新增的使用者。
c) 按一下**新增選擇的項目**。

步驟 6 若要從存取控制群組刪除使用者：

a) 選擇您要刪除的使用者。
b) 按一下**刪除選取的項目**。

步驟 7 點擊**儲存**。

設定存取控制群組的重疊權限原則

設定 Cisco Unified Communications Manager 如何處理受存取控制群組指派影響的重疊使用者權限。本節討論一般使用者指派至多個存取控制群組時，具有衝突角色與權限設定的情況。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**系統** > **企業參數**。

步驟 2 在 **User Management Parameters**（使用者管理參數）底下，爲 **Effective Access Privileges For Overlapping User Groups and Roles**（重疊使用者群組和角色的有效存取權限）設定下列其中一個值：

- **最大值**—代表所有重疊存取控制群組最大權限的有效權限。 此爲預設選項。
- **最小值**—代表所有重疊存取控制群組最小權限的有效權限。

步驟 3 點擊**儲存**。

檢視使用者權限報告

執行下列流程，以檢視現有一般使用者或現有的應用程式使用者的「使用者權限」報告。「使用者權限」報告會顯示存取控制群組、角色和指派給一般使用者或應用程式使用者的存取權限。

程序

步驟 1 在 Cisco Unified CM 管理中，執行下列其中一個步驟：

- 若爲一般使用者，請選擇**使用者管理** > **一般使用者**。
- 若爲應用程式使用者，請選擇**使用者管理** > **應用程式使用者**。

步驟 2 按一下**尋找**並選擇您要檢視存取權限的使用者。

步驟 3 從**相關連結**下拉式清單中，選擇 **User Privilege Report**（**使用者權限報告**），然後按一下**執行**。

「使用者權限」視窗會隨即顯示。

建立自訂服務台角色工作流程

某些公司希望服務台人員能擁有權限以執行特定管理工作。 遵循此工作流程中的步驟以設定服務台小組成員的角色和存取控制群組，以讓他們執行新增電話和新增一般使用者等工作。

程序

	命令或動作	目的
步驟 1	建立自訂服務台角色 ，第 24 頁上的	爲服務台小組成員建立自訂角色，並將新增電話和新增使用者等權限指派至角色。
步驟 2	建立自訂服務台存取控制群組 ，第 25 頁上的	爲「服務台」角色建立新的存取控制群組。
步驟 3	將服務台角色指派至存取控制群組 ，第 25 頁上的	將「服務台」角色指派至「服務台」存取控制群組。 「服務台」角色的權限會指派至任何指派至此存取控制群組的使用者。
步驟 4	將服務台成員指派至存取控制群組 ，第 26 頁上的	將自訂服務台角色的權限指派給服務台小組成員。

建立自訂服務台角色

執行此流程可建立自訂服務台角色，以讓您指派角色至組織中的服務台成員。

程序

步驟 1 在 Cisco Unified Communications Manager 管理中，選擇**使用者管理** > **使用者設定** > **角色**。

步驟 2 按一下**新增**。

步驟 3 從「應用程式」下拉式清單中，選擇您要指派至此角色的應用程式。 例如，**Cisco CallManager 管理**。

步驟 4 按**下一步**。

步驟 5 輸入新角色的**名稱**。 例如，**服務台**。

步驟 6 在 **Read and Update Privileges**（**讀取及更新權限**）底下，選擇您要爲服務台使用者指派的權限。 例如，若要讓服務台成員新增使用者和電話，請勾選「使用者」和「電話」頁面的**讀取**和**更新**方塊。

步驟 7 點擊**儲存**。

下一步

建立自訂服務台存取控制群組 ，第 25 頁上的

建立自訂服務台存取控制群組

開始之前

建立自訂服務台角色 ，第 24 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者設定** > **存取控制群組**。

步驟 2 按一下**新增**。

步驟 3 爲存取控制群組輸入名稱。 例如，**Help_Desk**。

步驟 4 點擊**儲存**。

下一步

將服務台角色指派至存取控制群組 ，第 25 頁上的

將服務台角色指派至存取控制群組

執行下列步驟，以「服務台」角色的權限設定「服務台」存取控制群組。

開始之前

建立自訂服務台存取控制群組 ，第 25 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者設定** > **存取控制群組**。

步驟 2 按一下**尋找**並選擇您爲服務台建立的存取控制群組。
存取控制群組組態視窗會隨即顯示。

步驟 3 在**相關連結**下拉式清單方塊中，選擇 **Assign Role to Access Control Group**（指派角色至存取控制群組）選項，然後按一下 **Go**（執行）。
Find and List Roles（尋找並列出角色）快顯視窗會隨即顯示。

步驟 4 按一下**指派角色至群組**按鈕。

步驟 5 按一下**尋找**並選擇服務台角色。

步驟 6 按一下**新增選擇的項目**。

步驟 7 點擊**儲存**。

下一步

將服務台成員指派至存取控制群組 ，第 26 頁上的

將服務台成員指派至存取控制群組

開始之前

將服務台角色指派至存取控制群組 ，第 25 頁上的

程序

步驟 1 在「Cisco Unified CM 管理」中，選擇**使用者管理** > **使用者設定** > **存取控制群組**。

步驟 2 按一下**尋找**，並選擇您建立的自訂服務台存取控制群組。

步驟 3 執行下列其中一個步驟:

- 若您的服務台小組成員已設爲一般使用者，請按一下**新增一般使用者至群組**。
- 若您的服務台小組成員已設爲應用程式使用者，請按一下**新增應用程式使用者至群組**。

步驟 4 按一下**尋找**並選擇服務台使用者。

步驟 5 按一下**新增選擇的項目**。

步驟 6 按一下**儲存**。
Cisco Unified Communications Manager 便會將您建立的自訂服務台角色的權限指派給服務台小組成員。

刪除存取控制群組

使用下列流程可刪除整個存取控制群組。

開始之前

刪除存取控制群組時，Cisco Unified Communications Manager 會從資料庫移除所有存取控制群組資料。 請確定您知道正在使用存取控制群組的角色。

程序

步驟 1 選擇**使用者管理** > **使用者設定** > **存取控制群組**。

Find and List Access Control Groups (尋找並列出存取控制群組) 視窗會隨即出現。

步驟 2 尋找您要刪除的存取控制群組。

步驟 3 按一下要刪除的存取控制群組的名稱。

您選擇的存取控制群組會隨即顯示。 清單會依字母順序顯示此存取控制群組中的使用者。

步驟 4 若要刪除整個存取控制群組，請按一下**刪除**。

對話方塊會隨即顯示，警告您無法復原刪除存取控制群組的動作。

步驟 5 若要刪除存取控制群組，請按一下**確定**；若要取消此動作，請按一下**取消**。若您按一下**確定**，Cisco Unified Communications Manager 便會從資料庫移除存取控制群組。

撤銷現有 OAuth 重新整理記號環

使用 AXL API 撤銷現有 OAuth 重新整理記號環。 例如，若員工離開公司，您可以使用此 API 撤銷該員工目前的重新整理記號環，使員工無法取得新的存取記號環，且無法再登入公司帳戶。 API 是以 REST 爲基礎的 API，且受 AXL 憑證保護。 您可以使用命令行工具叫用 API。 下列命令提供可用於撤銷重新整理記號環的 cURL 命令範例：

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

其中:

- `admin:password` 是 Cisco Unified Communications Manager 管理員帳戶的登入 ID 和密碼。
- `UCMaddress` 是 Cisco Unified Communications 管理員發佈者節點的 FQDN 或 IP 位址。
- `end_user` 是您要撤銷重新整理記號環的使用者的使用者 ID。

停用不活躍的使用者帳號

使用 Cisco 資料庫層監控服務以停用不活躍的使用者帳號：

若您未在指定的天數內登入Cisco Unified Communications Manager，則在計劃的維護任務期間 Cisco 資料庫層監控會將使用者帳號狀態更改爲不活躍。 停用的使用者將在後續審計記錄檔中自動進行審計。

開始之前

在 Cisco 資料庫層監控服務中所選定的伺服器中（**系統** > **服務參數**）輸入**維修時間**。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇 **系統** > **服務參數**。

步驟 2 在**伺服器**下拉式清單方塊中選擇一個伺服器。

步驟 3 在**服務**下拉式清單方塊中選擇**Cisco 資料庫層監控** 參數。

步驟 4 按一下**進階**。

步驟 5 在**停用已 X（天）未使用的使用者帳號**欄位中輸入天數， 例如，90。系統使用輸入的值作爲臨界值，以將帳戶狀態公布爲非作用中狀態。 要關閉自動停用，請輸入 0 爲值 。

附註 此爲必要欄位。 預設及最小值爲 0，單位爲天。

步驟 6 按一下**儲存**。

若使用者在所配置的天數（例如 90 天）內仍保持非活躍狀態則將被停用。 將會在審計記錄檔中建立一個項目，訊息顯示爲：userID>使用者被標記爲非活躍狀態”。

設定遠端帳戶

在 Unified Communications Manager 中配置遠端帳戶，讓 Cisco 支援可以暫時存取系統以進行疑難排解。

程序

步驟 1 在「Cisco Unified 作業系統管理」中選擇 **服務** > **遠端支援**。

步驟 2 在**帳戶名稱**欄位中，輸入遠端帳戶的名稱。

步驟 3 在 **Account Duration**（帳戶期間）欄位中，輸入帳戶期間天數。

步驟 4 按一下**儲存**。
系統產生一個加密的密碼短語。

步驟 5 請聯絡 Cisco 支援，以提供遠端支援帳戶名稱和複雜密碼。

標準角色和存取控制群組

下表摘要列出 Cisco Unified Communications Manager 中預先設定的標準角色和存取控制群組。 標準角色的權限爲預設設定。 此外，與標準角色相關聯的存取控制群組也是預設設定。

針對標準角色和相關聯的存取控制群組，您無法編輯權限或角色指派。

表 *2:* 標準角色、權限和存取控制群組

標準角色	角色的權限/資源	相關標準存取控制群組
標準 AXL API 存取	允許存取 AXL 資料庫 API	標準 CCM 超級使用者
標準 AXL API 使用者	授權登入權限以執行 AXL API。	
標準 AXL 唯讀 API 存取	可讓您依預設執行 AXL 唯讀 API（列出 API、取得 API、executeSQLQuery API）預設。	
標準管理報告工具管理	可讓您檢視及設定 Cisco Unified Communications Manager CDR 分析與報告 (CAR)。	標準 CAR 管理使用者、標準 CCM 超級使用者

標準角色	角色的權限/資源	相關標準存取控制群組
標準審計記錄管理	可讓您針對審計記錄功能執行下列工作： • 在 Cisco Unified Serviceability中檢視及設定「Audit Log Configuration」（審計記錄組態）視窗 • 檢視及設定 Cisco Unified Serviceability 中的追蹤，並收集即時監控工具審計記錄功能的追蹤 • 在 Cisco Unified Serviceability中檢視及啓動/停止 Cisco Audit Event（審計事件）服務 • 檢視及更新 RTMT 中的相關警示	標準審計使用者
Standard CCM Admin Users（標準 CCM 管理使用者）	授予 Cisco Unified Communications Manager 管理的登入權限。	Standard CCM Admin Users（標準 CCM 管理使用者）、Standard CCM Gateway Administration（標準 CCM 閘道管理）、Standard CCM Phone Administration（標準 CCM 電話管理）、Standard CCM Read Only（標準 CCM 唯讀）、Standard CCM Server Monitoring（標準 CCM 伺服器監控）、Standard CCM Super Users（標準 CCM 超級使用者）、Standard CCM Server Maintenance（標準 CCM 伺服器維護）、Standard Packet Sniffer Users（標準封包監聽器使用者）
標準 CCM 一般使用者	授予 Cisco Unified Communications 自助入口網站的一般使用者登入權限	標準 CCM 一般使用者

標準角色	角色的權限/資源	相關標準存取控制群組

標準 CCM 功能管理	能讓您在 Cisco Unified Communications Manager 管理中執行下列工作：
	• 使用批量管理工具檢視、刪除及插入下列項目：
	  • 用戶端事件代碼和強制授權代碼
	  • 代接來電群組
	• 在 Cisco Unified Communications Manager 管理中檢視及設定下列項目：
	  • 用戶端事件代碼和強制授權代碼
	  • 來電駐留
	  • 代接來電
	  • 即時會議號碼/型式
	  • 留言待聽取
	  • Cisco Unified IP 電話 服務
	  • 語音信箱引導、語音信箱連接埠精靈、語音信箱連接埠和語音信箱設定檔
		標準 CCM 伺服器維護

標準 CCM 閘道管理	能讓您在 Cisco Unified Communications Manager 管理中執行下列工作： • 在批量管理工具中檢視及設定閘道範本 • 檢視及設定閘道管理員、閘道和trunk	標準 CCM 閘道管理

標準角色	角色的權限/資源	相關標準存取控制群組

標準 CCM 電話管理	能讓您在 Cisco Unified Communications Manager 管理中執行下列工作：
	• 在批量管理工具中檢視及匯出電話
	• 在批量管理工具中檢視及插入使用者裝置設定檔
	• 在 Cisco Unified Communications Manager 管理中檢視及設定下列項目：
	  • BLF 快速撥號
	  • CTI 路由點
	  • 預設裝置設定檔或預設設定檔
	  • 目錄號碼和聯動線路
	  • 韌體載入資訊
	  • 電話按鈕範本或軟鍵範本
	  • 電話
	  • 在「電話組態」視窗中，按一下「Modify Button Items」（修改按鈕項目）按鈕，即可重新排序特定電話的電話按鈕資訊
		標準 CCM 電話管理

標準 CCM 路由計畫管理	能讓您在 Cisco Unified Communications Manager 管理中執行下列工作： • 檢視及設定應用程式撥號規則 • 檢視及設定通話搜尋範圍和分區 • 檢視及設定撥號規則，包括撥號規則型式 • 檢視及設定搜尋清單、搜尋引導和線路群組 • 檢視及設定路由過濾器、路由群組、路由搜尋清單、路由清單、路由型式和路由計畫報告 • 檢視及設定時期和時程 • 檢視及設定轉譯型式	

標準角色	角色的權限/資源	相關標準存取控制群組

標準 CCM 服務管理	能讓您在 Cisco Unified Communications Manager 管理中執行下列工作：
	• 檢視及設定下列項目：
	  • 通報器、會議橋接器和轉碼器
	  • 音訊來源和 MOH 伺服器
	  • 媒體資源群組和媒體資源群組清單
	  • 終止媒體點
	  • Cisco Unified Communications Manager Assistant 精靈
	• 在批量管理工具中檢視及設定「Delete Managers」（刪除管理員）、「Delete Managers/Assistants」（刪除管理員/助理）和「Insert Managers/Assistants」（插入管理員/助理）視窗
		標準 CCM 伺服器維護

標準角色	角色的權限/資源	相關標準存取控制群組

標準 CCM 系統管理	能讓您在 Cisco Unified Communications Manager 管理中執行下列工作：
	• 檢視及設定下列項目：
	  • 自動變更路由 (AAR) 群組
	  • Cisco Unified Communications Manager (Cisco Unified CM) 和 Cisco Unified Communications Manager 群組
	  • 日期與時間群組
	  • 裝置預設
	  • 裝置集區
	  • 企業參數
	  • 企業電話組態
	  • 位置
	  • 網路時間通訊協定 (NTP) 伺服器
	  • 外掛程式
	  • 執行精簡用戶端控制協定 (SCCP) 或作業階段啓始通訊協定 (SIP) 的電話的安全性設定檔；SIP trunk的安全性設定檔
	  • 遠端電話自我存活 (SRST) 參考
	  • 伺服器
	• 在批量管理工具中檢視及設定「工作排程器」視窗
		標準 CCM 伺服器維護

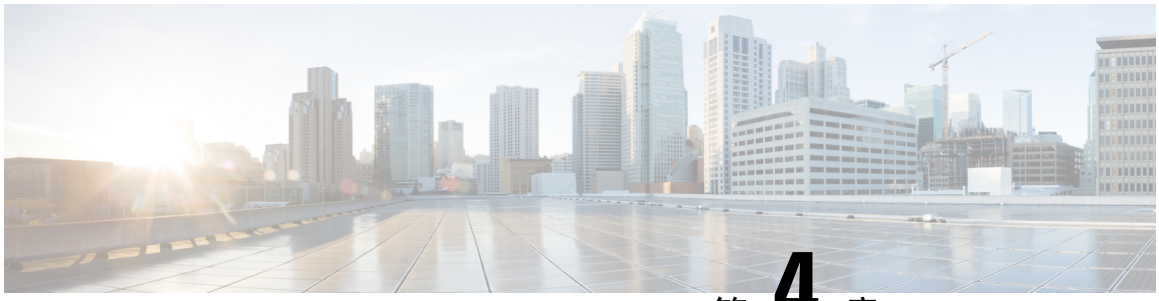
標準 CCM 使用者權限管理	可讓您在 Cisco Unified Communications Manager管理中檢視及設定應用程式使用者。	
標準 CCMADMIN 管理	可讓您存取 CCMAdmin 系統的所有層面	
標準 CCMADMIN 管理	可讓您檢視及設定 Cisco Unified Communications Manager 管理和批量管理工具中的所有項目。	標準 CCM 超級使用者
標準 CCMADMIN 管理	可讓您檢視及設定 Dialed Number Analyzer（撥出號碼分析器）中的資訊。	

標準角色	角色的權限/資源	相關標準存取控制群組
標準 CCMADMIN 唯讀	允許讀取所有 CCMAdmin 資源	
標準 CCMADMIN 唯讀	可讓您檢視 Cisco Unified Communications Manager 管理和批量管理工具中的組態。	標準 CCM 閘道管理、標準 CCM 電話管理、標準 CCM 唯讀、標準 CCM 伺服器維護、標準 CCM 伺服器監控
標準 CCMADMIN 唯讀	可讓您分析 Dialed Number Analyzer（撥出號碼分析器）中的路由組態。	
標準 CCMUSER 管理	允許存取 Cisco Unified Communications Self Care Portal。	標準 CCM 一般使用者
標準 CTI 允許通話監控	允許 CTI 應用程式/裝置監控通話	標準 CTI 允許通話監控
標準 CTI 允許來電駐留監控	允許 CTI 應用程式/裝置使用來電駐留。 **重要須知** 可用線路和駐留線路的最大數量不得超過 65,000。 如果總數超過 65,000，請從應用程式使用者中刪除 Standard CTI Allow Call Park Monitoring 角色或減少配置的駐留線路數量。	標準 CTI 允許來電駐留監控
標準 CTI 允許通話錄音	允許 CTI 應用程式/裝置錄製通話	標準 CTI 允許通話錄音
標準 CTI 允許來電號碼修改	允許 CTI 應用程式在通話期間轉換來電方號碼	標準 CTI 允許來電號碼修改
標準 CTI 允許控制所有裝置	允許控制所有可用 CTI 控制的裝置	標準 CTI 允許控制所有裝置
標準 CTI 可控制支援已連接轉接及會議的電話	允許控制所有支援已連接轉接及會議的 CTI 裝置	標準 CTI 可控制支援已連線轉接及會議之電話
標準 CTI 允許控制支援變換模式的電話	允許控制所有支援變換模式的 CTI 裝置	標準 CTI 允許控制支援變換模式的電話
標準 CTI 允許接收 SRTP 金鑰資料	允許 CTI 應用程式存取及分發 SRTP 金鑰資料	標準 CTI 允許接收 SRTP 金鑰資料
Standard CTI Enabled (啓用標準 CTI)	啓用 CTI 應用程式控制	Standard CTI Enabled (啓用標準 CTI)
標準 CTI 安全連線	啓用 Cisco Unified Communications Manager 的安全 CTI 連線	標準 CTI 安全連線

標準角色	角色的權限/資源	相關標準存取控制群組
標準 CUReporting	可讓應用程式使用者產生來自不同來源的報告	
標準 CUReporting	可讓您在 Cisco Unified 報告中檢視、下載、產生及上傳報告	標準 CCM 管理使用者、標準 CCM 超級使用者
標準 EM 驗證代理權限	管理應用程式的 Cisco Extension Mobility (EM) 驗證權限；與 Cisco Extension Mobility 互動的所有應用程式使用者皆需要（例如 Cisco Unified Communications Manager Assistant 和 Cisco Web Dialer）	標準 CCM 超級使用者、標準 EM 驗證代理權限
標準封包監聽	可讓您存取 Cisco Unified Communications Manager 管理以啓用封包監聽（擷取）。	標準封包監聽器使用者
標準 RealtimeAndTraceCollection	可讓您存取 Cisco Unified Serviceability和即時監控工具檢視，並使用下列項目： • 簡易物件存取通訊協 (SOAP) Serviceability AXL API • SOAP 通話錄音 API • SOAP 診斷入口網站（分析管理員）資料庫服務 • 設定審計記錄功能的追蹤 • 設定即時監控工具，包括收集追蹤	標準 RealtimeAndTraceCollection

標準角色	角色的權限/資源	相關標準存取控制群組
標準Serviceability	可讓您在 Cisco Unified Serviceability或即時監控工具中檢視及設定下列視窗： • 警示組態和警示定義（Cisco Unified Serviceability） • 審計追蹤（標示爲已讀/僅供檢視） • SNMP 的相關視窗（Cisco Unified Serviceability） • 追蹤組態及追蹤組態疑難排解（Cisco Unified Serviceability ） • 日誌分割監控 • 警示組態 (RTMT)、設定檔組態 (RTMT) 和追蹤集合 (RTMT) 可讓您檢視及使用 SOAP Serviceability AXL API、SOAP 通話記錄 API 和 SOAP 診斷入口網站（分析管理員）資料庫服務。 針對 SOAP 通話記錄 API，RTMT 分析管理員通話記錄權限是透過此資源控制。 針對SOAP診斷入口網站資料庫服務，RTMT分析管理員主控資料庫存取是透過此資源控制。	標準 CCM 伺服器監控、標準 CCM 超級使用者
標準Serviceability管理	Serviceability管理員可存取 Cisco Unified Communications Manager 管理中的「外掛程式」視窗，並從此視窗下載外掛程式。	
標準Serviceability管理	可讓您管理 Dialed Number Analyzer（撥出號碼分析器）Serviceability的所有層面。	
標準Serviceability管理	可讓您在 Cisco Unified Serviceability和即時監控工具中檢視及設定所有視窗。（「審計追蹤」僅支援檢視。） 可讓您檢視及使用所有 SOAP Serviceability AXL API。	
標準Serviceability唯讀	可讓您檢視 Dialed Number Analyzer（撥出號碼分析器）元件的所有Serviceability相關資料。	標準 CCM 唯讀

標準角色	角色的權限/資源	相關標準存取控制群組
標準Serviceability唯讀	可讓您在 Cisco Unified Serviceability和即時監控工具中檢視組態。（不包括審計組態視窗，該視窗是以「標準審計記錄管理」角色爲代表） 可讓您檢視所有 SOAP Serviceability AXL API、SOAP 通話記錄 API 和 SOAP 診斷入口網站（分析管理員）資料庫服務。	
標準系統服務管理	可讓您檢視、啓用及停止 Cisco Unified Serviceability中的服務。	
標準 SSO 組態管理員	可讓您管理 SAML SSO 組態的所有層面	
標準 Confidential Access Level 使用者	可讓您存取所有 Confidential Access Level 頁面	標準 Cisco 通話管理員管理
標準 CCMADMIN 管理	可讓您管理 CCMAdmin 系統的所有層面	標準 Cisco Unified CM IM and Presence 管理
標準 CCMADMIN 唯讀	允許讀取所有 CCMAdmin 資源	標準 Cisco Unified CM IM and Presence 管理
標準 CUReporting	可讓應用程式使用者產生來自不同來源的報告	標準 Cisco Unified CM IM and Presence 報告



第 4 章

管理一般使用者

一般使用者概覽

管理執行中的系統時，您可能需要更新系統中的已設定一般使用者清單。 這包括：

- 設定新使用者
- 爲新的一般使用者設定電話
- 爲一般使用者變更密碼或 PIN 碼
- 讓一般使用者可使用 IM and Presence Service

「Cisco Unified CM 管理」中的**一般使用者組態**視窗可讓您新增、搜尋、顯示及維護 Unified CM 一般使用者的資訊。 您也可以使用**快速使用者/電話新增**視窗快速設定新的一般使用者，並爲該一般使用者設定新電話。

一般使用者管理工作

程序

	命令或動作	目的
步驟 1	設定使用者範本 ，第 40 頁上的	若您未以包含通用線路和裝置範本的使用者設定檔設定系統，請執行這些工作以進行設定。 您可以將這些範本套用至任何新的一般使用者以快速設定新使用者和電話。

	命令或動作	目的
步驟 2	使用下列其中一種方法新增一般使用者 • 從 LDAP 匯入一般使用者 ，第 44 頁上的 • 手動新增一般使用者 ，第 45 頁上的	若您的系統與公司 LDAP 目錄同步，便可直接自 LDAP 匯入新的一般使用者。 否則，您可以手動新增及設定一般使用者。
步驟 3	執行下列其中一個工作以將電話指派至新的一般使用者或現有的一般使用者： • 新增一般使用者的新電話 ，第 46 頁上的 • 將現有的電話移至一般使用者 ，第 46 頁上的	您可以使用「Add New Phone」(新增電話)程序，使用通用裝置範本的設定爲一般使用者設定新電話。 您也可以使用「移動」流程指派已設定的現有電話。
步驟 4	變更一般使用者 PIN 碼 ，第 47 頁上的	（可任選）變更 Cisco Unified Communications Manager 管理中一般使用者的 PIN 碼。
步驟 5	變更一般使用者的密碼 ，第 47 頁上的	（可任選）變更 Cisco Unified Communications Manager 管理中一般使用者的密碼。
步驟 6	建立 Cisco Unity Connection 語音信箱 ，第 48 頁上的	（選用）在 Cisco Unified Communications Manager 管理中建立個別 Cisco Unity Connection 語音信箱。

設定使用者範本

執行下列工作可設定使用者設定檔和功能組範本。 新增一般使用者時，您可以使用線路和裝置設定來快速設定一般使用者和該使用者的電話。

程序

	命令或動作	目的
步驟 1	設定通用線路範本 ，第 41 頁上的	使用通常套用至目錄號碼的常用設定來設定通用線路範本。
步驟 2	設定通用裝置範本 ，第 41 頁上的	使用通常套用至電話的常用設定來設定通用裝置範本。
步驟 3	設定使用者設定檔 ，第 42 頁上的	將通用線路和通用裝置範本指派至使用者設定檔。 若您已設定自我佈建功能，便能爲使用此設定檔的使用者啓用自我佈建。
步驟 4	設定功能組範本 ，第 43 頁上的	將使用者設定檔指派至功能組範本。 若爲 LDAP 同步使用者，功能組範本會將使用者設定檔的設定關聯至一般使用者。

設定通用線路範本

通用線路範本使將通用設定輕鬆套用於新指派的目錄號碼碼變得容易。 配置不同的範本以滿足不同使用者群組的需求。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者/電話新增** > **通用線路範本**。

步驟 2 按一下**新增**。

步驟 3 設定**通用線路範本組態**視窗中的欄位。 如需有關欄位及其組態選項的詳細資訊，請參閱線上說明。

步驟 4 若您要部署具有替代號碼的全域撥號計畫複寫，請展開**企業替代號碼**和**+E.164替代號碼**部份，然後執行以下操作：

a) 點按**新增企業替代號碼**按鈕和/或**新增 + E.164 替代號碼**按鈕。

b) 新增您要用來指派至您的替代號碼的**號碼遮罩**。 例如，一個四位數的分機可能以 5XXXX 爲企業號碼遮罩而以 1972555XXXX 作爲 + E.164 替代號碼遮罩。

c) 在要指派替代號碼的位置指定分組。

d) 若您想透過 ILS 播發此號碼，請勾選**透過 ILS 在全球範圍內播發**方塊。 請注意，若您使用播發的型樣來彙總一系列替代號碼，您可能就不需播發個別的替代號碼。

e) 展開**PSTN 容錯移轉**部分然後選擇**企業號碼**或者**+ E.164 替代號碼**作爲在正常的通話路由失敗時使用 PSTN 容錯移轉。

步驟 5 點擊**儲存**。

下一步

設定通用裝置範本 ，第 41 頁上的

設定通用裝置範本

通用裝置範本可輕鬆將組態設定套用於新佈建的裝置。所提供的裝置使用通用裝置範本的設定。您可以配置不同的裝置範本以滿足不同使用者群組的需求。 您還可以將已配置的設定檔指派給該範本。

開始之前

設定通用線路範本 ，第 41 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中選擇**使用者管理** > **使用者/電話新增** > **通用裝置範本**。

步驟 2 按一下**新增**。

步驟 3 輸入下列必填的欄位。

a) 輸入 UDP 範本的**裝置描述**。

b) 在下拉式清單中選擇**裝置集區**。
c) 在下拉式清單中選擇**裝置安全性設定檔**。
d) 在此下拉式清單中選擇**SIP 設定檔**。
e) 在下拉式清單中選擇**電話按鈕範本**。

步驟 4 填妥**通用裝置範本組態**視窗中的欄位。 如需欄位的描述請參閱線上說明。

步驟 5 在**電話設定**中請填妥以下任選欄位：
a) 若您配置了**通用電話設定檔**，則您需指派設定檔。
b) 若您配置了**通用裝置組態**，則您需指派組態。
c) 若您配置了**功能控制原則**，則您需指派原則。

步驟 6 點擊**儲存**。

下一步

設定使用者設定檔 ，第 42 頁上的

設定使用者設定檔

將通用線路和通用裝置範本指派至使用者個人資料檔。 爲不同的使用者群組配置多個使用者個人資料檔。 您亦可爲使用此服務設定檔的使用者啓用自我佈建。

開始之前

設定通用裝置範本 ，第 41 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者設定** > **使用者設定檔**。

步驟 2 按一下**新增**。

步驟 3 輸入使用者個人資料檔的**名稱**和**描述**。

步驟 4 指派**通用裝置範本**以套用至使用者的**桌面電話**、**行動及桌上型裝置**和**遠端目標/裝置設定檔**。

步驟 5 指派**通用線路範本**以套用至此使用者個人資料檔中的使用者電話線路。

步驟 6 若要讓此使用者個人資料檔的使用者使用自我佈建功能，以佈建自己的電話，請執行下列作業:
a) 勾選 **Allow end user to provision their own phones(允許一般使用者佈建自己的電話)**方塊。
b) 在 **Limit Provisioning once End User has this many phones (當一般使用者有許多部電話時限制佈建)** 欄位中，輸入允許使用者佈建的電話數目上限。 最大值爲 20。
c) 選取 **允許佈建已指定給其他最終使用者的電話**選取方塊，以確定與此設定檔相關的使用者是否有許可權移轉或重新指定已經被其他使用者擁有的裝置。 預設未勾選此方塊。

步驟 7 如果您想讓與此使用者設定檔相關的Cisco Jabber使用者，能夠使用行動裝置和遠端存取功能，請選中**啟用行動裝置和遠端存取**選取方塊。

附註
- 此可勾選方塊預設爲勾選。 當您取消該選取方塊時，**使用者端原則**區段被停用，無服務使用者端原則選項被預設值選中。
- 僅使用 OAuth Refresh 登入的 Cisco Jabber 使用者需要進行此設定。 非 Jabber 使用者無需使用此設定來使用「Mobile and Remote Access」。 Mobile and Remote Access 功能僅適用於 Jabber Mobile and Remote Access使用者，不適用於任何其他端點或使用者端。

步驟 8 爲此使用者個人資料檔指派Jabber原則。 從**桌面使用者端原則**和**行動裝置使用者端原則**下拉式清單中，選擇以下選項之一：
- 無服務—此原則會停用所有 Cisco Jabber 服務的存取。
- 僅限 IM & Presence—此原則只會啓用即時訊息與目前狀態功能。
- IM & Presence、語音和視訊通話—此原則會針對擁有音訊或視訊裝置的所有使用者來啓用即時訊息、狀態、語音信箱和會議功能。 此爲預設選項。

附註 Jabber 桌面使用者端包括 Windows 版 Cisco Jabber 使用者和 Mac 版 Cisco Jabber 使用者。 Jabber 行動使用者端包括 iPhone 與 iPad 版 Cisco Jabber 使用者和 Android 版 Cisco Jabber 使用者。

步驟 9 如您希望此使用者個人資料檔中的使用者能透過 Cisco Unified Communications Self Care Portal 設定 Extension Mobility 或跨叢集 Extension Mobility 的登入時間上限，請勾選**允許一般使用者設定其 Extension Mobility 的登入時間上限**方塊。

附註 預設未勾選**允許一般使用者設定其 Extension Mobility 的登入時間上限**方塊。

步驟 10 點擊**儲存**。

下一步

設定功能組範本 ，第 43 頁上的

設定功能組範本

功能組範本可爲佈建的使用者快速配置電話、線路和功能，以協助您的系統部署過程。 若要自公司 LDAP 目錄同步使用者，請使用希望使用者在目錄同步使用的“使用者設定檔”和“服務配置檔”配置功能組範本。 您還可以透過此範本爲同步使用者啓用 IM and Presence Service。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者/電話新增** > **功能組範本**。

步驟 2 按一下**新增**。

步驟 3 輸入功能組範本的**名稱**和**說明**。

步驟 4 若要將本地叢集作爲所有使用此範本的使用者的主叢集，請勾選**主叢集**方塊。

步驟 5 若要讓使用此範本的使用者能夠交換即時訊息和在線狀態資訊，請勾選**為 Unified CM IM and Presence 啟用使用者**方塊。

步驟 6 在下拉式清單中選擇**服務配置檔**和**使用者設定檔**。

步驟 7 完成**功能組範本組態**視窗的其餘欄位。 如需欄位描述，請參閱線上說明。

步驟 8 按一下**儲存**。

下一步

新增一般使用者。 若您的系統與公司 LDAP 目錄整合，便可直接從 LDAP 目錄匯入使用者。 否則，請手動建立一般使用者。

- 從 LDAP 匯入一般使用者 ，第 44 頁上的
- 手動新增一般使用者 ，第 45 頁上的

從 LDAP 匯入一般使用者

執行下列流程以在公司 LDAP 目錄手動匯入新的一般使用者。 若 LDAP 同步組態包含功能群組範本，且具有包含通用線路和裝置範本的使用者個人資料檔，以及 DN 集區，則匯入流程將自動配置一般使用者和主要分機。

附註 初始同步發生後，您無法再將新的配置 (例如，新增功能群組範本) 新增至 LDAP 目錄同步中。 若要編輯現有的 LDAP 同步，則需使用批量管理或配置新的 LDAP 同步。

開始之前

此流程假設您已同步 Cisco Unified Communications Manager 和公司 LDAP 目錄。 LDAP 同步需包含具有通用線路和裝置範本的功能群組範本。

程序

步驟 1 在 Cisco Unified CM 管理中，選取**系統** > **LDAP** > **LDAP 目錄**。

步驟 2 按一下**尋找**，然後選擇要新增至使用者的 LDAP 目錄。

步驟 3 按一下 **Perform Full Sync**（**執行完整同步**）。
Cisco Unified Communications Manager 便會與外部 LDAP 目錄同步。 LDAP 目錄中的任何新的一般使用者皆會被匯入 Cisco Unified Communications Manager 資料庫。

下一步

若啓用使用者的自我佈建，則一般使用者可以使用自我佈建互動語音回應 (IVR) 佈建新的電話。 否則，請執行下列其中一個工作，以將電話指派給這位一般使用者:

- 新增一般使用者的新電話 ，第 46 頁上的

- 將現有的電話移至一般使用者 ，第 46 頁上的

手動新增一般使用者

執行下列流程以新增一般使用者，並爲該使用者設定存取控制群組和主要線路分機。

附註 確保已設定存取控制群組，該存取控制群組具有要爲其分配使用者的角色權限。 詳細資訊，請參閱“管理使用者存取”一章。

開始之前

確認您已配置包含通用線路範本的使用者個人資料檔。 若您需要配置新的分機，Cisco Unified Communications Manager 能使用通用線路範本的設定來配置主要分機。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者/電話新增** > **快速使用者/電話新增**。

步驟 2 輸入**使用者 ID**和**姓氏**。

步驟 3 在**功能群組範本**下拉式清單中，選擇功能群組範本。

步驟 4 按一下**儲存**。

步驟 5 在**使用者個人資料檔**下拉式清單中，確認選擇的使用者個人資料檔包含通用線路範本。

步驟 6 在**存取控制群組成員資格**區段中，按一下 **+** 圖示。

步驟 7 在 **User is a member of (使用者所屬群組)** 下拉式清單中，選擇存取控制群組。

步驟 8 在**主要分機**下方，按一下 **+** 圖示。

步驟 9 在**分機**下拉式清單中選擇顯示爲 **(可用)** 的目錄號碼。

步驟 10 若所有線路分機皆顯示爲 **(已使用)**，請執行下列步驟:

a) 按一下 **New... (新增...)** 按鈕。
ad d New Extension (新增分機) 快顯視窗會隨即顯示。
b) 在**目錄號碼**欄位中，輸入新的線路分機。
c) 在**線路範本**下拉式清單中選擇通用線路範本。
d) 按一下**確定**。
Cisco Unified Communications Manager 便會使用通用線路範本的設定來設定目錄號碼。

步驟 11 (可選) 完成**快速使用者/電話新增組態**視窗中的其他欄位。

步驟 12 按一下**儲存**。

下一步

執行下列其中一個程序，以將電話指派給這位一般使用者:

- 新增一般使用者的新電話 ，第 46 頁上的
- 將現有的電話移至一般使用者 ，第 46 頁上的

新增一般使用者的新電話

執行下列流程以爲新一般使用者或現有的一般使用者新增電話。 確定一般使用者的使用者設定檔包含通用裝置範本。 Cisco Unified Communications Manager 使用通用裝置範本的設定來設定電話。

開始之前

請執行下列其中一個流程以新增一般使用者：

- 手動新增一般使用者 ，第 45 頁上的
- 從 LDAP 匯入一般使用者 ，第 44 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中選擇**使用者管理** > **使用者/電話新增** > **快速/使用者電話新增**。

步驟 2 按一下**尋找**並選擇您要新增電話的一般使用者。

步驟 3 按一下**管理裝置**。
「管理裝置」視窗會隨即顯示。

步驟 4 按一下 **新增電話**。
「新增電話至使用者」快顯視窗會隨即顯示。

步驟 5 在**產品類型**下拉式清單中選擇電話機型。

步驟 6 在**裝置通訊協定**下拉式清單中選擇 SIP 或 SCCP 作爲通訊協定。

步驟 7 在**裝置名稱**文字方塊中，輸入裝置 MAC 位址。

步驟 8 在**通用裝置範本**下拉式清單中，選擇通用裝置範本。

步驟 9 若電話支援擴充模組，請輸入您所要部署的擴充模組數目。

步驟 10 若要使用 Extension Mobility 存取電話，請勾選 **In Extension Mobility (在 Extension Mobility 中)** 方塊。

步驟 11 按一下 **新增電話**。
「新增電話」快顯視窗即會關閉。 Cisco Unified Communications Manager 便會將電話新增至使用者並且使用通用裝置範本來配置電話。

步驟 12 若要另外再編輯電話組態，請按一下相對應的「鉛筆」圖示以在**電話組態**視窗中開啓電話。

將現有的電話移至一般使用者

執行此流程可將現有的電話移至新的一般使用者或現有的一般使用者。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**使用者管理** > **使用者/電話新增** > **快速使用者/電話新增**。

步驟 2 按一下**尋找**並選擇您要行動現有電話的使用者。

步驟 3 按一下**管理裝置**按鈕。

步驟 4 按一下 **Find a Phone to Move To This User (尋找電話以移至此使用者)** 按鈕。

步驟 5 選擇要移至此使用者的電話。

步驟 6 按一下 **Move Selected (行動選擇項目)**。

變更一般使用者 PIN 碼

程序

步驟 1 在 Cisco Unified Communications Manager 管理中，選擇**使用者管理** > **一般使用者**。
尋找和列出使用者視窗會隨即顯示。

步驟 2 若要選擇現有使用者，請在 **Find User Where** 欄位中指定適當的過濾器，按一下**尋找**來擷取使用者清單，然後從清單中選擇使用者。
一般使用者組態視窗會隨即顯示。

步驟 3 在 **PIN 碼**欄位中，連按兩下現有的加密 PIN 碼，然後輸入新 PIN 碼。 您至少需輸入指派的憑證原則中所指定的字元數下限（1-127 個字元）。

步驟 4 在 **確認 PIN 碼**欄位中，連按兩下現有的加密 PIN 碼，然後再次輸入新 PIN 碼。

步驟 5 按一下**儲存**。

附註 若在 Cisco Unity Connection 視窗中啓用**一般使用者 PIN 碼同步**勾選方塊，**應用程式伺服器組態** 您可以使用相同的一般使用者 PIN 碼登入 Extension Mobility、立即舉辦會議、行動連線和 Cisco Unity Connection 語音信箱。 一般使用者可以使用相同的 PIN 碼登入 Extension Mobility 及存取其語音信箱。

變更一般使用者的密碼

啓用 LDAP 驗證時，無法變更一般使用者的密碼。

程序

步驟 1 在 Cisco Unified Communications Manager 管理中，選擇**使用者管理** > **一般使用者**。
尋找和列出使用者視窗會隨即顯示。

步驟 2 若要選擇現有使用者，請在 **Find User Where** 欄位中指定適當的過濾器，按一下**尋找**來擷取使用者清單，然後從清單中選擇使用者。
一般使用者組態視窗會隨即顯示。

步驟 3 在**密碼**欄位中，連按兩下現有的加密密碼，然後輸入新密碼。 您至少需輸入指派的憑證原則中所指定的字元數下限（1-127 個字元）。

步驟 4 在**確認密碼**欄位中，連按兩下現有的加密密碼，然後再次輸入新密碼。

步驟 5 點擊**儲存**。

建立 Cisco Unity Connection 語音信箱

開始之前

- 您需針對語音留言設定 Cisco Unified Communications Manager。 如需配置 Cisco Unified Communications Manager 以使用 Cisco Unity Connection 的詳細資訊，請參閱《*Cisco Unified Communications Manager* 系統組態指南》：

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- 您需將裝置與主要分機號碼與一般使用者建立關聯。
- 您可以使用 Cisco Unity Connection 提供的匯入功能，而不必執行本節所述的流程。 如需有關如何使用匯入功能的相關資訊，請參閱 *User Moves, Adds, and Changes Guide for Cisco Unity Connection*（Cisco Unity Connection 的使用者移動、新增和變更指南）。

程序

步驟 1 在 Cisco Unified Communications Manager 管理中，選擇**使用者管理** > **一般使用者**。
尋找和列出使用者視窗會隨即顯示。

步驟 2 若要選擇現有使用者，請在 **Find User Where** 欄位中指定適當的過濾器，按一下**尋找**來擷取使用者清單，然後從清單中選擇使用者。
一般使用者組態視窗會隨即顯示。

步驟 3 確認主要分機號碼與此使用者關聯。

附註 您需定義主要分機；否則 Create Cisco Unity User（建立 Cisco Unity 使用者）連結不會顯示於**相關連結**下拉式清單中。

步驟 4 在**相關連結**下拉式清單中，選擇 Create Cisco Unity User（建立 Cisco Unity 使用者）連結，然後按一下**執行**。

Add Cisco Unity User（新增 Cisco Unity 使用者）對話方塊會隨即出現。

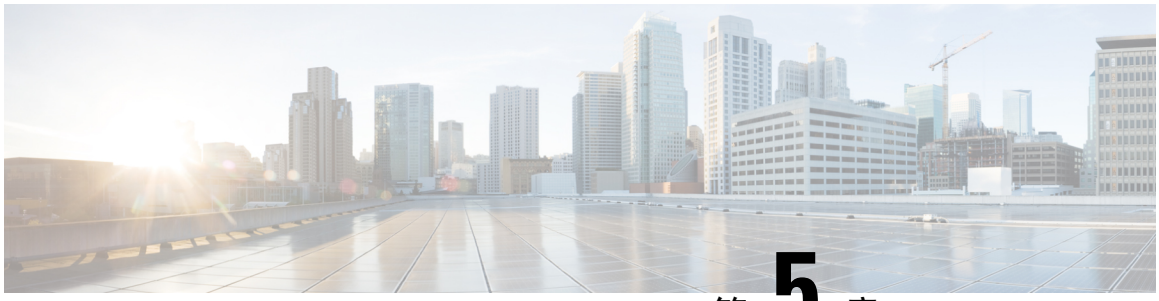
步驟 5 在**應用程式伺服器**下拉式清單中，選擇您要建立 Cisco Unity Connection 使用者的 Cisco Unity Connection 伺服器，然後按一下**下一步**。

步驟 6 在**使用者範本**下拉式清單中選擇您要使用的使用者範本。

步驟 7 按一下**儲存**。

信箱便會建立。 **一般使用者組態**視窗的**相關連結**下拉式清單中的連結會變更爲 Edit Cisco Unity User（編輯 Cisco Unity 使用者）。 您現在可以在 Cisco Unity Connection Administration 中檢視您所建立的使用者。

附註 整合 Cisco Unity Connection 使用者和 Cisco Unified Communications Manager 一般使用者後，您便無法編輯 Cisco Unity Connection 管理中的欄位，例如「別名」（Cisco Unified CM 管理中的使用者 ID）、「名字」、「姓氏」和「分機」（Cisco Unified CM 管理中的「主要分機」）。 您只能在 Cisco Unified CM 管理中更新這些欄位。



第 5 章

管理應用程式使用者

應用程式使用者概覽

「Cisco Unified CM 管理」中的**應用程式使用者組態**視窗可讓管理員新增、搜尋、顯示及維護 Cisco Unified Communications Manager 應用程式使用者的相關資訊。

Cisco Unified CM 管理預設包括下列應用程式使用者：

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

附註 「標準CCM超級使用者」群組中的管理員使用者可透過單一登錄其中一個應用程式存取Cisco Unified Communications Manager 管理、Cisco Unified Serviceability和 Cisco Unified Reporting。

應用程式使用者工作流程

程序

	命令或動作	目的
步驟 1	新增應用程式使用者 ，第 52 頁上的	新增應用程式使用者。
步驟 2	將裝置與應用程式使用者建立關聯 ，第 53 頁上的	指派裝置以與應用程式使用者相關聯。
步驟 3	將管理員使用者新增至 Cisco Unity 或 Cisco Unity Connection ，第 53 頁上的	將使用者以管理員使用者的身分新增至 Cisco Unity 或 Cisco Unity Connection。 您在 Cisco Unified CM 管理中設定應用程式使用者；然後在 Cisco Unity 或 Cisco Unity Connection 管理中爲使用者設定其他設定。
步驟 4	變更應用程式使用者的密碼 ，第 54 頁上的	變更應用程式使用者密碼。
步驟 5	管理應用程式使用者密碼憑證資訊 ，第 55 頁上的	變更或檢視憑證資訊，例如關聯的驗證規則、關聯的憑證原則，或應用程式使用者上次變更密碼的時間。

新增應用程式使用者

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **應用程式使用者**。

步驟 2 按一下**新增**。

步驟 3 配置**應用程式使用者組態**視窗中的欄位。 如需有關欄位及其組態選項的資訊，請參閱線上說明。

步驟 4 點擊**儲存**。

下一步

將裝置與應用程式使用者建立關聯 ，第 53 頁上的

將裝置與應用程式使用者建立關聯

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **應用程式使用者**。
尋找和列出使用者視窗會隨即顯示。

步驟 2 若要選擇現有使用者，請在 **Find User Where** 欄位中指定適當的過濾器，選擇**尋找**來擷取使用者清單，然後從清單中選擇使用者。

步驟 3 在**可用裝置**清單中，選擇您要與應用程式使用者關聯的裝置，然後按一下清單下方的「**下**」**箭頭**。
選擇的裝置會移至**受控裝置**清單。

附註　若要限制可用裝置清單，請按一下 **Find more Phones**（**尋找更多電話**）或 **Find more Route Points**（**尋找更多路由點**）按鈕。

步驟 4 若您按一下 **Find more Phones**（**尋找更多電話**）按鈕，便會顯示**尋找並列出電話**視窗。 執行搜尋以尋找要與此應用程式使用者關聯的電話。

爲每一部您要指派至應用程式使用者的裝置重複上述步驟。

步驟 5 若您按一下 **Find more Route Points**（**尋找更多路由點**）按鈕，便會顯示 **Find and List CTI Route Points**（**尋找並列出 CTI 路由點**）視窗。 執行搜尋以尋找要與此應用程式使用者關聯的 CTI 路由點。

爲每一部您要指派至應用程式使用者的裝置重複上述步驟。

步驟 6 點擊**儲存**。

將管理員使用者新增至 Cisco Unity 或 Cisco Unity Connection

若您將 Cisco Unified Communications Manager 與 Cisco Unity Connection 7.x 或更高版本整合，您可使用 Cisco Unity Connection 7.x 或更高版本的匯入功能而不必執行本節所述的流程。 如需有關如何使用匯入功能的相關資訊，請參閱 *User Moves, Adds, and Changes* Guide for Cisco Unity Connection（Cisco Unity Connection 7.x 或更高版本的使用者移動、新增和變更指南）。

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

Cisco Unity 或 Cisco Unity Connection 使用者與 Cisco Unified CM 應用程式使用者整合時，您無法編輯欄位。 您只能在 Cisco Unified Communications Manager 管理中更新這些欄位。

Cisco Unity 和 Cisco Unity Connection 會監控 Cisco Unified Communications Manager 的資料同步。 您可以在工具功能表中設定 Cisco Unity Administration 或 Cisco Unity Connection Administration 的同步時間。

開始之前

請確認您已爲計畫推送至 Cisco Unity 或 Cisco Unity Connection 的使用者定義適當的範本。

Create Cisco Unity User（**建立 Cisco Unity 使用者**）連結只會在您安裝及設定適當的 Cisco Unity 或 Cisco Unity Connection 軟體時顯示。 Cisco Unity 方面請參閱相關的 *Cisco Unified Communications Manager* 整合指南；Cisco Unity Connection 方面請參閱相關的 *Cisco Unified Communications Manager SCCP* 整合指南：

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **應用程式使用者**。

步驟 2 若要選擇現有使用者，請在 **Find User Where** 欄位中指定適當的過濾器，選擇**尋找**來擷取使用者清單，然後從清單中選擇使用者。

步驟 3 從**相關連結**下拉式清單中，選擇 **Create Cisco Unity Application User**（建立 Cisco Unity 應用程式使用者）連結，然後按一下**執行**。
Cisco Unity User（Cisco Unity 使用者）對話方塊會隨即出現。

步驟 4 從**應用程式伺服器**下拉式清單中，選擇您要建立 Cisco Unity 或 Cisco Unity Connection 使用者的 Cisco Unity 或 Cisco Unity Connection 伺服器，然後按一下**下一步**。

步驟 5 從**應用程式使用者**下拉式清單中，選擇您要使用的範本。

步驟 6 按一下**儲存**。
管理員帳戶是在 Cisco Unity 或 Cisco Unity Connection 中建立。 **應用程式使用者組態**視窗的「相關連結」中的連結會變更爲 **Edit Cisco Unity User**（**編輯 Cisco Unity 使用者**）。 您現在可以在 Cisco Unity Administration 或 Cisco Unity Connection Administration 中檢視您所建立的使用者。

變更應用程式使用者的密碼

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **應用程式使用者**。
尋找和列出使用者視窗會隨即顯示。

步驟 2 若要選擇現有使用者，請在 **Find User Where** 欄位中指定適當的過濾器，選擇**尋找**來擷取使用者清單，然後從清單中選擇使用者。
應用程式使用者組態視窗會顯示所選應用程式使用者的相關資訊。

步驟 3 在**密碼**欄位中，連按兩下現有的加密密碼，然後輸入新密碼。

步驟 4 在**確認密碼**欄位中，連按兩下現有的加密密碼，然後再次輸入新密碼。

步驟 5 點擊**儲存**。

管理應用程式使用者密碼憑證資訊

執行下列流程可管理應用程式使用者密碼的憑證資訊。 這可讓您執行管理責任，例如鎖定密碼、將憑證原則套用至密碼，或檢視資訊（例如最後登入嘗試失敗時間）。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **應用程式使用者**。
尋找和列出使用者視窗會隨即顯示。

步驟 2 若要選擇現有使用者，請在 **Find User Where** 欄位中指定適當的過濾器，選擇**尋找**來擷取使用者清單，然後從清單中選擇使用者。
應用程式使用者組態視窗會顯示所選應用程式使用者的相關資訊。

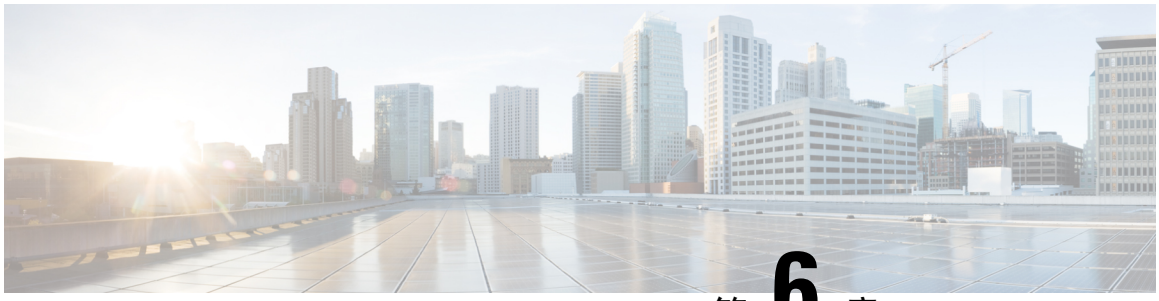
步驟 3 若要變更或檢視密碼資訊，請按一下**密碼**欄位旁的**編輯憑證**按鈕。
使用者 **Credential Configuration**（憑證組態）會隨即顯示。

步驟 4 配置 **Credential Configuration**（憑證組態）視窗中的欄位。 如需有關欄位及其組態選項的詳細資訊，請參閱線上說明。

步驟 5 若您變更任何設定，請按一下**儲存**。

第 III 部分

管理裝置



第 6 章

管理電話

電話管理概覽

本章描述如何管理網路中的電話。 本部分描述新增電話、將現有的電話移至另一位使用者、鎖定電話和重設電話等工作。

適用於您的電話機型的《Cisco IP 電話管理指南》包含特定於電話機型的配置資訊。

電話按鈕範本

“電話”按鈕範本是根據電話機型創建的。 某些電話機型不使用任何特定的電話按鈕範本，但是某些電話機型需要特定的範本，無論是單個範本還是裝置預設範本。

這**非尺寸安全電話的電話範本選擇**和**自動註冊舊版模式**企業參數**企業參數配置**頁指定使用的電話按鈕範本的類型。 如需有關欄位的詳細資訊請參閱線上說明。

表 *3:* 不同情況下的電話按鈕範本

非尺寸安全電話的電話範本選擇	自動註冊舊版模式	電話
創建一個個別的範本	False	透過通用裝置範本新增電話時，將創建單個電話按鈕範本。
使用裝置預設設定中的範本	False	未創建單個電話按鈕範本，它採用了裝置預設設定中的電話按鈕範本。
使用裝置預設設定中的範本	True	裝置集、電話範本、通話搜尋空間、電話按鈕範本的值皆取自裝置預設值。

非尺寸安全電話的電話範本選擇	自動註冊舊版模式	電話
創建一個個別的範本	True	裝置集、電話範本、通話搜尋空間、電話按鈕範本的值皆取自裝置預設值。 不會創建個別的範本。 自動註冊舊版模式具有優先權。

電話管理工作

程序

	命令或動作	目的
步驟 1	以一般使用者或不以一般使用者自範本新增電話 ，第 61 頁上的	自包含或不含一般使用者的範本新增電話。
步驟 2	手動新增電話 ，第 60 頁上的	不使用裝置範本而爲一般使用者新增電話。
步驟 3	以一般使用者身分自範本加入新的電話 ，第 62 頁上的	爲一般使用者新增電話，並指派通用裝置範本。
步驟 4	移動現有的電話 ，第 68 頁上的	將已設定的電話移至另一位一般使用者。
步驟 5	尋找主動登入的裝置 ，第 68 頁上的	搜尋特定裝置或列出使用者目前登入的所有裝置。
步驟 6	尋找遠端登入的裝置 ，第 69 頁上的	搜尋特定裝置或列出使用者遠端登入的所有裝置。
步驟 7	遠端鎖定電話 ，第 70 頁上的	某些電話可以遠端鎖定。 遠端鎖定電話時，電話將無法使用，直到您解除鎖定。
步驟 8	將電話重設成出廠預設值 ，第 70 頁上的	將電話重設爲原廠設定。
步驟 9	電話鎖定/清除報告 ，第 71 頁上的	搜尋遠端鎖定和/或遠端重設爲原廠預設設定的裝置。
步驟 10	檢視 LSC 狀態及爲電話產生 CAPF 報告 ，第 72 頁上的	搜尋電話的 LSC 到期狀態，並產生 CAPF 報告。

手動新增電話

執行下列流程以手動新增使用者的新電話。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**裝置** > **電話** > **尋找並列出電話**。

步驟 2 在**尋找並列出電話**頁面中點按**新增**以手動新增電話。

新增電話頁面將會顯示。

在**新增電話**頁面中，若您點按“點按此處使用通用裝置範本新增電話”超連結，頁面將被重新導向至**新增電話**頁面，您便可自範本新增電話（新增或不新增使用者）。 如需更多資訊，請參閱以一般使用者或不以一般使用者自範本新增電話 ，第 61 頁上的 。

步驟 3 在**產品類型**下拉式清單中選擇電話機型。

步驟 4 按**下一步**。
電話組態視窗隨即顯示。

步驟 5 在 **電話組態**頁面中的必需欄位中輸入值。 如需有關欄位的詳細資訊請參閱線上說明。

有關“產品特定配置”區域中欄位的其他資訊，請參閱適用於您的電話型號的 *Cisco IP* 電話管理指南。

步驟 6 點按**儲存**以儲存電話組態。

下一步

將現有的電話移至一般使用者 ，第 46 頁上的

以一般使用者或不以一般使用者自範本新增電話

執行下列流程，以新增或不新增使用者的方式從範本新增電話。 Cisco Unified Communications Manager 使用通用裝置範本的設定來設定電話。

開始之前

確保已在 Cisco Unified Communications Manager 中配置了通用裝置範本。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**裝置** > **電話** > **尋找並列出電話**。

步驟 2 在**尋找並列出電話**頁面中點按**自範本新增**以自裝置範本新增電話（新增或不新增一般使用者皆可）。

新增電話頁面將會顯示。

在**新增電話**頁面中，若您點按“點按這裡手動輸入所有電話設定”的超連結，頁面會重新導向至現有的**新增一個電話**頁面，讓您可手動新增電話。 如需更多資訊，請參閱手動新增電話 ，第 60 頁上的 。

步驟 3 從**電話類型（和通訊協定）**下拉式清單中選擇電話機型。

電話可支援多種通訊協定時，才會顯示通訊協定下拉式清單。

步驟 4 在 **名稱或 MAC 位址**文字方塊中，輸入名稱或 MAC 位址。

步驟 5 從**裝置範本**下拉式清單中，選擇通用裝置範本。

步驟 6 從**目錄號碼（線路 1）**下拉式清單中，選擇目錄號碼。

若下拉式清單中的目錄號碼超過下拉式清單上限，則**尋找**標籤會顯示。 按一下**尋找**，快顯對話方塊便會依據「尋找目錄號碼」準則開啓。

步驟 7 （可任選）若要建立新的目錄號碼並將其指派至裝置，請按一下**新增**，輸入目錄號碼，然後選擇通用線路範本。

您也可以使用關聯使用者的目錄號碼來建立電話，請移至**使用者管理** > **使用者/電話新增** > **快速使用者/電話新增**。

步驟 8 （選用）在**使用者**下拉式清單中，選擇您要新增電話的使用者。

附註 爲 Cisco 雙模式（行動）裝置新增使用者爲必要動作。

若此下拉式清單中的一般使用者數目超過下拉式清單上限，便會顯示**尋找**標籤。 按一下**尋找**，即可開啓包含「尋找一般使用者」條件的快顯對話方塊。

步驟 9 按一下**新增**。

附註 非尺寸的安全電話而言，將依下列的選項來建立電話範本：**非尺寸安全電話的電話範本選擇**和**企業參數組態**頁面上的**自動註冊舊版模式**參數。

隨即顯示新增成功訊息。 Cisco Unified Communications Manager 將新增電話而**電話組態編輯**頁面將會顯示。 有關欄位的更多資訊請參閱**電話組態**頁面上的線上說明。

下一步

將現有的電話移至一般使用者 ，第 46 頁上的

以一般使用者身分自範本加入新的電話

執行下列流程以新增一般使用者的新電話。

開始之前

您正在新增電話的一般使用者已設定包含通用裝置範本的使用者設定檔。 Cisco Unified Communications Manager 使用通用裝置範本的設定來設定電話。

- 一般使用者管理工作 ，第 39 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中選擇**使用者管理** > **使用者/電話新增** > **快速/使用者電話新增**。

步驟 2 按一下**尋找**並選擇您要新增電話的一般使用者。

步驟 3 按一下**管理裝置**。
「管理裝置」視窗會隨即顯示。

步驟 4 按一下 **新增電話**。
「新增電話至使用者」快顯視窗會隨即顯示。

步驟 5 在**產品類型**下拉式清單中選擇電話機型。

步驟 6 在**裝置通訊協定**下拉式清單中選擇 SIP 或 SCCP 作爲通訊協定。

步驟 7 在**裝置名稱**文字方塊中，輸入裝置 MAC 位址。

步驟 8 在**通用裝置範本**下拉式清單中，選擇通用裝置範本。

步驟 9 若電話支援擴充模組，請輸入您所要部署的擴充模組數目。

步驟 10 若要使用 Extension Mobility 存取電話，請勾選 **In Extension Mobility (在 Extension Mobility 中)** 方塊。

步驟 11 按一下 **新增電話**。
「新增電話」快顯視窗即會關閉。 Cisco Unified Communications Manager 便會將電話新增至使用者並且使用通用裝置範本來配置電話。

步驟 12 若要另外再編輯電話組態，請按一下相對應的「鉛筆」圖示以在**電話組態**視窗中開啓電話。

Collaboration Mobile Convergence 虛擬裝置概覽

CMC 裝置是一個虛擬裝置，代表與之關聯的遠端目標。 當企業電話撥話至 CMC 裝置時，通話將重新導向至遠端目標。此功能旨在建立裝置類型**Collaboration Mobile Convergence**與 Spark Remote Device 相同，幾乎不需自訂且具有以下優點。

- 支援 Cisco Unified Communications Manager 上的本機行動裝置，其功能類似於 Spark 遠端裝置。
- 充分利用作爲 Spark-RD 的功能，其中包括未來開發同等功能。
- 允許針對特定於行動裝置的用例進行自訂，例如將通話從“行動裝置”轉移至“桌面電話”，“從桌面電話轉移至行動電話”。（在“身份”頁面上新增 deskpickup 計時器並透過產品支援功能設定啓用該功能）。
- CMC 裝置可以包含在搜尋群組中。
- 能夠與 Spark 遠端裝置共用線路。
- 授權-從授權使用角度來看，算作一個單獨的裝置。 任何多裝置授權捆包皆應支援 CMC-RD。

CMC RD 裝置的授權調整

新增新的 CMC 裝置後將依照與使用者關聯的裝置的數目/類型消耗授權。 CMC 裝置消耗的授權類型取決於與之關聯的一般使用者所擁有的裝置數目。

- 若僅部署 CMC 裝置，請使用 Enhanced 授權
- 若要一併部署 CMC 裝置和 Spark RD，請使用 Enhanced 授權
- 若要一併部署 CMC 和實體裝置：Enhanced Plus 授權

- 若要一併部署 CMC、Spark RD 和實體裝置：Enhanced Plus 授權

新增 Collaboration Mobile Convergence 虛擬裝置

執行以下步驟，爲一般使用者新增 Cisco Collaboration Mobile Convergence（CMC）遠端裝置。

開始之前

您正在爲其新增電話的一般使用者需已有包含通用裝置範本的使用者設定檔。 Cisco Unified Communications Manager 使用通用裝置範本的設定來設定電話。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **電話**。

步驟 2 按一下 **新增**按鈕。

步驟 3 點按**點按此處手動輸入所有電話設定**連結。
新增新電話視窗會隨即顯示。

步驟 4 在**電話類型**下拉式清單中選擇 Cisco Collaboration Mobile Convergence 然後點按**下一個**。
電話組態視窗會隨即顯示。

步驟 5 在**所有者使用者 ID** 下拉式清單中，選擇要爲其創建裝置的一般使用者。

步驟 6 在**裝置集**下拉式清單中，選擇裝置集。

步驟 7 按一下**儲存**。
將彈出警告訊息，點按**應用配置**按鈕以使變更生效。 按一下**確定**。 裝置新增成功。

步驟 8 配置**目錄號碼**，點按新增的 CMC 裝置，輸入**目錄號碼**然後點按**儲存**。

步驟 9 若要爲新增的 CMC 裝置新增一個**遠端目標**，請在“身份”框中點按連結。

步驟 10 在“遠端目標配置”視窗中，輸入**姓名**、**目的地號碼**然後點按**儲存**。

附註　每一台 CMC 裝置僅能新增一個“遠端目標”。

步驟 11 若要更新現有的遠端目標，請輸入**新名稱**然後點擊**儲存**。

步驟 12 若要刪除現有的遠端目標，請點擊功能表中的“刪除”按鈕。
將出現來自網頁確認將永久刪除的訊息。 按一下**確定**。

步驟 13 若要自裝置頁面刪除 CMC 裝置，請勾選**裝置**方塊並在功能表中點擊**刪除選擇的裝置**。

CMC RD 功能互動

表 *4: CMC RD* 功能互動

功能	互動
共用線路處理	• 在具有關聯的CMC RD和Spark RD的共用桌面電話的設定中，當使用者以企業電話致電 CMC 裝置 DN 時，三個CMC RD、Spark RD、共用桌面電話皆會響鈴。 • 從任何遠端目標接聽通話，共用桌面電話上皆會顯示“遠端使用中”訊息。 • 從任何共用桌面電話接聽通話則兩個遠端目標電話（CMC RD 、 Spark RD 電話）的連線皆會中斷。
CMC 裝置可在通話管理員組（CMG）設定中使用	• 當CMC裝置與“通話管理員”群組關聯時，它僅在主伺服器關閉時始終在主伺服器上執行，並在通話管理員群組的下一個活動輔助伺服器上執行。 • 若主伺服器在通話流程中中斷，則仍保留正在進行的通話，且在通話結束後，CMC 裝置會註冊至輔助伺服器。 附註 當通話處於保留模式時，電話之間的媒體仍然保持活動狀態，但是除了斷開通話之外，無法執行其他任何操作。 • 若主伺服器最初處於關閉狀態，且在CMC裝置已註冊至輔助伺服器時發起了通話，然後在進行中的通話流程中主伺服器亦啓動，則通話將進入保留模式，而通話結束後CMC裝置將會註冊至主伺服器。
通話錨定	自CMC裝置撥出的所有基本傳入通話及“號碼至遠端目標的通話”都錨定在企業網路中。 配置CMC遠端裝置後，使用者可以自行動裝置撥出和接收通話，而所有通話都將錨定到企業： • 使用者可以從企業號碼直接撥話至CMC遠端目標。該通話錨定在企業網路中。 在這種情況下，桌面電話（CMC裝置的共用線路）不會響鈴，而是保留在**遠端連線使用**狀態。 • 使用者可自 CMC 遠端目標撥至任何企業號碼。 通話已錨定。 在這種情況下，桌面電話（CMC裝置的共用線路）保留在**遠端連線使用**狀態。

功能	互動
單一號碼聯絡	• 在“遠端目標”配置頁面中，若**啟用單一號碼聯絡**方塊未勾選，該通話不會延伸至 CMC RD，且該通話將被拒絕。 • 無論**啟用單一號碼聯絡**勾選方塊是否勾選，來自遠端目的地的來電和**號碼至遠端目的地**的輸出通話不會受到影響。 • 若與CMC裝置共用了桌面電話，且**啟用單一號碼聯絡**方塊未勾選，則通話將延伸至共用桌面電話但不延伸至 CMC RD。 附註 若**單一號碼存取語音信箱原則**設定爲**使用者控制**在發生到主要分機的**秘密轉接**時將**不會**觸發行動目的地號碼。僅主擴展將被觸發。 **使用者控制**設定：支援諮詢傳輸。**計時器控制**：語音郵件迴避原則同時支援“諮詢”和“盲目”轉移。
根據一天中的時間（ToD）進行通話路由	• 您可以使用“遠端目標”的“一天中的時間”組態來設定響鈴時間表（例如，您可以配置特定時間，例如星期一至星期五上午 9 點至下午 5 點之間）。 僅在那些時候，通話將被重新導向到您的“遠端目標”。 從企業電話到CMC號碼的通話將根據固定於“遠端目標”配置頁面中“響鈴時間表”進行路由。 響鈴時間表可以指定如下： • **每時每刻** – 通話隨時被路由。 沒有任何限制。 • **一周中的某幾日** – 僅在選定的特定日期路由通話。 • **特定的時間**-僅在選定的辦公時間內路由通話。確定有選擇時區。 • 在“振鈴”時間表中接聽電話時，將根據“遠端目標”組態頁面中“允許存取”或“阻止存取”清單中新增的電話號碼或模式，路由從企業電話到 CMC 號碼的通話。 • **允許存取清單**-僅當通話者號碼或模式在允許存取清單中時，目標才會響鈴。 • **阻止存取清單**-若通話者號碼或模式在“阻止存取”清單中，目標不會響鈴。 附註 在任何時間點，都僅能使用“允許存取清單”或“阻止存取清單”。

功能	互動
使用者區域設定	CMC 虛擬裝置使用在“電話配置”視窗中配置的區域設定來確定電話顯示和電話通知的區域設定。 此原則適用於常規通話以及對“立即會議”號碼的通話。 公告的部分而言，當以使用者區域設定中所選擇的語言來撥話（任何企業電話）和被撥話（CMC 裝置）的電話，通話和遠端目標上的公告均基於在“電話組態”頁面中選擇的使用者區域設定。 **附註** 例如，當自與 CMC 裝置建立關聯的**遠端目標**撥號至**立即舉辦會議的號碼**，該公告是基於在 CMC 裝置的“電話配置”頁面中選所擇的“使用者區域設定”。
HLogin 和 HLogout 的新存取代碼	此功能可幫助管理員使用新增的服務參數來設定 CMC 裝置的搜尋群組登錄和註銷號碼： • 搜尋群組登入的企業功能存取號碼。 • 搜尋群組登出的企業功能存取號碼。 當使用者在與 CMC 裝置關聯的 RD 上輸入 Hlogin 號碼時，僅在撥打與 CMC 裝置關聯的搜尋引導號碼時，通話才會被重新導向到 RD。 當使用者從與 CMC 裝置關聯的 RD 輸入登出登錄號碼時，在撥打與 CMC 裝置關聯的尋線開機號碼時，通話將不會重新導向到 RD。 預設情況下，CMC 裝置爲 Hloggedin。 在兩種情況下，都不會影響對 CMC 裝置的直接通話。
CMC 的遠端目標通話延伸基於在資料庫中所配置的 **振鈴定時器之前的延遲**	**若將 DB 中的振鈴定時器之前的延遲配置為 5000** • 企業電話至 CMC 號碼來電時，共用線路會振鈴，且通話會在五秒鐘後到達“遠端目標”。 • 企業電話至 CMC 號碼來電時，若共用線路在 5 秒鐘前應答通話，則該通話不會延伸到“遠端目標”。 • 企業電話至 CMC 號碼來電時，共用線路會振鈴，且若撥話方在五秒鐘前掛斷，則該通話不會延伸到“遠端目標”。 **若將 DB 中的振鈴定時器之前的延遲配置為 0** 從企業電話到 CMC 號碼的任何通話都將同時提醒遠端目標和共用線路。
批量管理工具（BAT）支援	爲 CMC 裝置提供了 BAT 支援

CMC RD 功能限制

表 *5: CMC RD* 功能限制

功能	限制
CMC 遠端目標關聯	下列限制適用於： • 您僅能將 CMC 裝置與一個遠端目標建立關聯。 . • 若一般使用者被刪除，則其關聯的 CMC 裝置和 RD（遠端目標）也將被刪除。 附註 無論**啟用移動性**方塊是否有勾選，CMC 和 RD 不受影響， 不會刪除 CMC 裝置。 附註 Cisco Unified Communications Manager 不支援 CMC 裝置的通話句柄保留。

移動現有的電話

執行下列流程以將設定的電話移至一般使用者。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**使用者管理** > **使用者/電話新增** > **快速使用者/電話新增**。

步驟 2 按一下**尋找**並選擇您要行動現有電話的使用者。

步驟 3 按一下**管理裝置**按鈕。

步驟 4 按一下 **Find a Phone to Move To This User (尋找電話以移至此使用者)** 按鈕。

步驟 5 選擇要移至此使用者的電話。

步驟 6 按一下 **Move Selected (行動選擇項目)**。

尋找主動登入的裝置

Cisco Extension Mobility 和 Cisco 跨叢集的Extension Mobility功能會儲存使用者主動登入之裝置的記錄。Cisco Extension Mobility功能的方面，主動登入的裝置報告會追蹤本地使用者主動登入的本地電話； Cisco跨叢集的Extension Mobility功能的方面，主動登入的裝置報告會追蹤遠端使用者主動登入的本地電話。

Unified Communications Manager 提供特定的搜尋視窗來搜尋使用者登入的裝置。請執行下列步驟來搜尋特定的裝置或列出使用者主動登入的所有裝置。

程序

步驟 1 選擇**裝置** > **電話**。

步驟 2 請在右上角的**相關連結**下拉式清單中，選取**主動登入裝置報告**，然後按一下**執行**。

步驟 3 若要尋找資料庫中所有已主動登入的裝置記錄，請確定此對話方塊爲空白，並繼續執行步驟 4。

若要過濾或搜尋記錄：

a) 在第一個下拉式清單中選擇搜尋參數。
b) 在第二個下拉式清單中選擇搜尋型樣。
c) 如果適用的話，請指定適當的搜尋文字。

附註 若要新增其他搜尋條件，請按一下 **+** 按鈕。 當您新增條件時，系統會搜尋符合您指定之所有條件的記錄。 若要移除條件，請按一下**(-)**按鈕來移除最後加入的條件，或按一下**清除過濾器**按鈕來移除所有加入的搜尋條件。

步驟 4 按一下**尋找**。

隨即顯示所有相符的記錄。 您可以變更在每個頁面上顯示的項目數，只要從每頁列數下拉式清單中選擇另一個值即可。

步驟 5 從顯示的記錄清單中，按一下您要檢視之記錄的連結。

附註 若要反轉排序順序，請在清單標頭中按一下向上或「下」箭頭（若可用的話）。

視窗將會顯示您選擇的項目。

尋找遠端登入的裝置

Cisco跨叢集的Extension Mobility功能會記錄使用者遠端登入的裝置。「遠端登入裝置」報告會追蹤屬於其他叢集，但由本機使用者以 EMCC 功能主動登入的電話。

Unified Communications Manager 提供特定搜尋視窗，讓您搜尋使用者遠端登入的裝置。 請遵循下列步驟來搜尋特定裝置或列出使用者遠端登入的所有裝置。

程序

步驟 1 選擇**裝置** > **電話**。

步驟 2 在右上角的**相關連結**下拉式清單中，選取**遠端登入裝置**，然後按一下**執行**。

步驟 3 若要尋找資料庫中所有遠端登入的裝置記錄，請確定此對話方塊爲空白，並繼續執行步驟 4。

若要過濾或搜尋記錄：

a) 在第一個下拉式清單中選擇搜尋參數。
b) 在第二個下拉式清單中選擇搜尋型樣。
c) 如果適用的話，請指定適當的搜尋文字。

附註 若要新增其他搜尋條件，請按一下 **+** 按鈕。 當您新增條件時，系統會搜尋符合您指定之所有條件的記錄。若要移除條件，請按一下**(–)**按鈕來移除最後加入的條件，或按一下清除過濾器按鈕來移除所有加入的搜尋條件。

步驟 4 按一下**尋找**。

隨即顯示所有相符的記錄。 您可以變更在每個頁面上顯示的項目數，只要從每頁列數下拉式清單中選擇另一個值即可。

步驟 5 從顯示的記錄清單中，按一下您要檢視之記錄的連結。

附註 若要反轉排序順序，請在清單標頭中按一下向上或「下」箭頭（若可用的話）。

視窗將會顯示您選擇的項目。

遠端鎖定電話

某些電話可以遠端鎖定。 遠端鎖定電話時，電話將無法使用，直到您解除鎖定。

若電話支援「遠端鎖定」功能，**鎖定**按鈕便會出現在右上角。

程序

步驟 1 選擇**裝置** > **電話**。

步驟 2 在**尋找並列出電話**視窗中輸入搜尋準則，然後按一下**尋找**以尋找特定的電話。

符合搜尋準則的電話清單會隨即顯示。

步驟 3 選擇要執行遠端鎖定的電話。

步驟 4 在**電話組態**視窗中，按一下**鎖定**。

若未註冊電話，便會顯示通知您電話將在下次註冊時鎖定的快顯視窗。 按一下**鎖定**。

裝置鎖定/抹除狀態部分會隨即顯示，包含最近的請求、是否擱置中和最近通知的相關資訊。

將電話重設成出廠預設值

某些電話支援遠端抹除功能。 當您遠端抹除電話時，此作業會將電話重設成原廠設定。 先前儲存在電話上的所有資料皆會抹除。

若電話支援遠端抹除功能，**抹除**按鈕便會出現在右上角。

⚠

注意 此作業無法復原。 您應該僅在確定將電話重設爲原廠設定時，才執行此作業。

程序

步驟 1 選擇**裝置** > **電話**。

步驟 2 在**尋找並列出電話**視窗中，輸入搜尋準則，然後按一下**尋找**以尋找特定電話。

符合搜尋準則的電話清單會隨即顯示。

步驟 3 選擇要執行遠端抹除的電話。

步驟 4 在**電話組態**視窗中，按一下**抹除**。

若未註冊電話，便會顯示通知您電話將在下次註冊時抹除的快顯視窗。 按一下**抹除**。

Device Lock/Wipe Status（**裝置鎖定/抹除狀態**）區段會隨即顯示，包含最近的請求、是否擱置中和最近通知的相關資訊。

電話鎖定/清除報告

Unified Communications Manager 提供特定搜尋視窗，讓您搜尋已透過遠端鎖定和或遠端清除的裝置。請遵循下列步驟來搜尋特定裝置，或列出所有遠端鎖定和/或遠端抹除的裝置。

程序

步驟 1 選擇**裝置** > **電話**。

「尋找並列出電話」視窗會隨即顯示。 啓用中（之前）的查詢記錄也可能會顯示於視窗中。

步驟 2 請在視窗右上角的**相關連結**下拉式清單中，選取 **Phone Lock/Wipe Report**（**電話鎖定/抹除報告**），然後按一下**執行**。

步驟 3 若要在資料庫中尋找所有遠端鎖定或遠端抹除的裝置記錄，請確保文字方塊爲空白；並移至步驟 4。

若要過濾或搜尋特定裝置的記錄：

a) 請從第一個下拉式清單中，選擇裝置作業類型以進行搜尋。
b) 在第二個下拉式清單中，選擇搜尋參數。
c) 在第三個下拉式清單中，選擇搜尋型樣。
d) 如果適用的話，請指定適當的搜尋文字。

附註 若要新增其他搜尋條件，請按一下 + 按鈕。 當您新增條件時，系統會搜尋符合您指定之所有條件的記錄。 若要移除條件，請按一下 － 按鈕來移除最後加入的條件，或按一下「清除過濾器」按鈕來移除所有加入的搜尋條件。

步驟 4 按一下**尋找**。

隨即顯示所有相符的記錄。 您可以變更在每個頁面上顯示的項目數，只要從每頁列數下拉式清單中選擇另一個值即可。

步驟 5 從顯示的記錄清單中，按一下您要檢視之記錄的連結。

附註 若要反轉排序順序，請在清單標頭中按一下向上或「下」箭頭（若可用的話）。

視窗將會顯示您選擇的項目。

檢視 LSC 狀態及為電話產生 CAPF 報告

使用此流程可在 Cisco Unified Communications Manager 介面中監控本地重要憑證 (LSC) 到期資訊。下列搜尋過濾器會顯示 LSC 資訊：

- LSC Expires（LSC 到期）—在電話上顯示 LSC 到期日。
- LSC Issued By（LSC 簽發者）—顯示簽發者名稱，這可能是 CAPF 或第三方。
- LSC Issuer Expires By（LSC 簽發者到期日）—顯示簽發者到期日。

附註 當新的裝置上未發行任何 LSC 時，**LSC Expires**（**LSC 到期**）和 **LSC Issuer Expires By**（**LSC 簽發者到期日**）欄位的狀態會設爲 “NA” 。

在升級至 Cisco Unified Communications Manager 11.5 (1) 前，將 LSC 發行給裝置時，**LSC Expires**（**LSC 到期**）和 **LSC Issuer Expires By**（**LSC 簽發者到期日**）欄位的狀態會設爲 “Unknown（不明）” 。

程序

步驟 1 選擇**裝置** > **電話**。

步驟 2 從第一個 **Find Phone where**（**尋找電話條件**）下拉式清單中，選擇下列其中一個條件：

- LSC Expires（LSC 到期）
- LSC Issued By（LSC 簽發者）
- LSC Issuer Expires By（LSC 簽發者到期日）

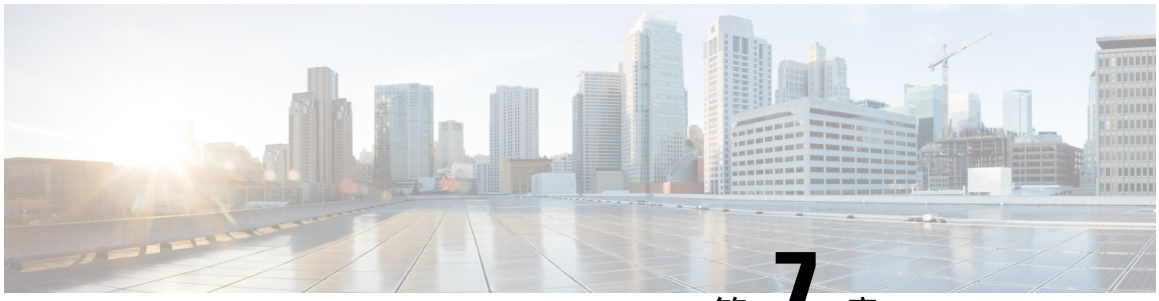
從第二個 **Find Phone where**（**尋找電話條件**）下拉式清單中，選擇下列其中一個條件：

- 之前
- 完全
- 之後
- 開頭爲
- 包含

- 結尾爲
- 完全
- 爲空白
- 不爲空白

步驟 3 按一下**尋找**。
隨即顯示找到的電話清單。

步驟 4 從**相關連結**下拉式清單中，選擇 **CAPF Report in File**（**檔案中的 CAPF 報告**），然後按一下**執行**。
報告便會隨即下載。



第 7 章

管理裝置韌體

裝置韌體更新概覽

裝置載入是 IP 電話、擬真視訊會議系統和其他佈建且註冊至 Cisco Unified Communications Manager 的裝置的軟體和韌體。 在安裝或升級期間，Cisco Unified Communications Manager 包含最新可用載入，視 Cisco Unified Communications Manager 的版本釋出時間而定。 Cisco 經常釋出更新的韌體，以引進新功能和軟體修正，您可以將電話更新爲較新的載入，而不需要等待包含該載入的 Cisco Unified Communications Manager 升級。

端點可升級至新版的軟體前，需能在端點可存取的位置下載新載入需要的檔案。 最常見位置是啓用 Cisco TFTP 服務的 Cisco UCM 節點，稱爲 “TFTP 伺服器” 。 某些電話還支援使用替代下載位置，稱爲“載入伺服器” 。

若要取得清單、檢視或下載已存在於任何伺服器的 TFTP 目錄中的檔案，您可以使用 CLI 命令「file list tftp」查看 TFTP 目錄中的檔案、「file view tftp」檢視檔案，或「file get tftp」取得 TFTP 目錄中的檔案備份。 如需詳細資訊，請參閱 *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*（Cisco Unified Communications 解決方案的命令行介面參考指南）。 您也可以使用網頁瀏覽器造訪 URL “http://<tftp_server>:6970/<filename>” 下載任何 TFTP 檔案。

提示 您可以將新的載檔套用至單一裝置，然後將之配置爲整個系統的預設。 此方法在測試時相當有用。但請記住，該類型的所有其他裝置皆使用舊的載入，直到您使用新載入更新整個系統的預設。

安裝裝置包或單個韌體

請安裝裝置套件以引進新的電話類型，並爲多種電話機型升級韌體。

- 現有裝置可以下列的選項安裝或升級：Cisco 選項套件 (COP) 檔案—COP 檔案包含韌體檔案和資料庫更新，所以安裝於發佈者時，除了安裝韌體檔案外，還會更新預設韌體。
- 僅韌體檔案—以 zip 檔案提供，包含應手動擷取並上傳至 TFTP 伺服器的適當目錄的個別裝置韌體檔案。

附註　請參閱「readme 」檔案取得特定於 COP 或韌體檔案包的安裝描述。

程序

步驟 1　從「Cisco Unified 作業系統管理」中，選擇**軟體升級** > **安裝/升級**。

步驟 2　在「軟體位置」區段中填入適用的值，然後按一下**下一步**。

步驟 3　在**Available Software**（**可用軟體**）下拉式清單中，選擇裝置套件檔案，然後按一下**Next**（**下一步**）。

步驟 4　確認 MD5 值是否正確，然後按一下 **Next**（**下一步**）。

步驟 5　在警告方塊中，確認您已選擇正確的韌體，然後按一下 **Install**（**安裝**）。

步驟 6　檢查是否已收到成功訊息。

附註　若您重新啓動叢集，請跳至步驟 8。

步驟 7　在正在執行服務的所有節點上重新啓動**Cisco TFTP**服務。

步驟 8　重設受影響的裝置以將裝置升級爲新載入。

步驟 9　在「Cisco Unified CM 管理」中，選擇**裝置** > **裝置設定** > **裝置預設**，然後將載入檔案（針對特定裝置）的名稱手動變更爲新載入。

步驟 10　按一下**儲存**，然後重設裝置。

步驟 11　在所有叢集節點上重新啓動**Cisco Tomcat**服務。

步驟 12　請執行下列其中一個步驟:

- 若執行的爲 11.5（1）SU4 或更低版本的 12.0 (1)或 12.0（1）SU1，請將叢集重新啓動。
- 若您執行的爲 11.5（1）SU5 或更高版本，或 12.0（1）SU2 或更高版本，請重新啓動**Cisco CallManager**發布者節點上的服務。 倘若您僅在訂閱者節點上執行**Cisco CallManager**服務，您可跳過此任務。

韌體安裝的潛在問題

以下是安裝裝置包後可能會遇到的一些潛在問題：

問題	原因/解決方法
新裝置不會註冊	這可能是由於裝置類型不相符而發生的。 這可能是由於： • 使用錯誤的裝置類型在“電話組態”視窗中新增了該裝置。 例如，選擇 Cisco DX80 作爲電話類型而未選擇 Cisco TelePresence DX80。 用正確的裝置類型重新配置裝置。 • **Cisco CallManager**服務無法辨識新的裝置類型。 在這種情況下，請重新啓動**Cisco CallManager**發布者節點上的服務。
端點未升級到新韌體	**可能的原因：** • 該裝置包未安裝在 TFTP 伺服器上。 結果，韌體無法透過電話下載。 • **Cisco TFTP**安裝後該服務未重新啓動，因此該服務未偵測到新的檔案。 確保將裝置包安裝在 TFTP 伺服器上
Cisco Unified CM 管理中的“電話組態”視窗顯示未下載的連結，其中圖標圖像應爲新裝置類型	重新啓動**Cisco Tomcat** CLI 上所有節點上的服務。

自系統移除未使用的韌體

Device Load Management（**裝置載入管理**）視窗可讓您從系統刪除未使用的韌體（裝置載入）和關聯的檔案以增加硬碟空間。 例如，您可以在升級前刪除未使用的載入，以避免硬碟空間不足導致的升級失敗。 某些韌體檔案可能具有**Device Load Management**（**裝置載入管理**）視窗中未列出的依存檔案。 刪除韌體時，依存檔案也會一併刪除。 然而，若依存檔案未關聯至其他韌體，便不會刪除。

附註 您需個別刪除叢集中各伺服器未使用的韌體。

開始之前

注意 刪除未使用的韌體前，請確保您刪除正確的載入。 若不執行DRS還原整個叢集，便無法還原刪除的載入。 我們建議您在刪除韌體前先進行備份。

確保不要刪除使用多個檔案負載的裝置的檔案。 例如，某些 CE 端點會使用多個負載。 但是，只有一個負載會在 **Device Load Management**（**裝置負載管理**） 視窗中被參照爲 **In Use**（**使用中**）。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇 **Software Upgrades**（軟體升級） > **Device Load Management**（裝置載入管理）。

步驟 2 指定搜尋準則，然後按一下**尋找**。

步驟 3 選擇您要刪除的裝置載入。 如有需要，可以選擇多個載檔。

步驟 4 按一下 **Delete Selected Loads**（刪除選擇的載入）。

步驟 5 點擊**確定**。

設定電話機型的預設韌體

使用此流程可爲特定電話機型設定預設韌體載入。 註冊新電話時，Cisco Unified Communications Manager 會嘗試將預設韌體傳送至電話，除非電話組態指定的**電話組態**視窗中指定覆寫韌體載入。

附註 針對個別電話，**電話組態**視窗中**電話載入名稱**欄位的設定會覆寫該特定電話的預設韌體載入。

開始之前

請確定韌體有載入至 TFTP 伺服器。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **裝置設定** > **裝置預設值**。
出現的**裝置預設組態**視窗會顯示 Cisco Unified Communications Manager 支援的不同電話機型的預設韌體載入。 韌體顯示在**載入資訊**一欄中。

步驟 2 在**裝置類型**底下，尋找您要指派預設韌體的電話機型。

步驟 3 在附帶的**載入資訊**欄位中，輸入韌體載入。

步驟 4 （可任選）爲該電話機型輸入預設**裝置集區**和預設**電話範本**。

步驟 5 點擊**儲存**。

設定電話的韌體載入

使用此流程可針對特定電話指派韌體載入。 若您想要使用不同於**裝置預設組態**視窗中指定的預設的韌體載入，可以執行此流程。

附註 若要爲多部電話指派版本，您可以使用「批量管理工具」，透過CSV檔案或查詢來設定**電話載入名稱**欄位。 如需詳細資訊，請參閱《*Cisco Unified Communications Manager* 批量管理指南》。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **電話**。

步驟 2 按一下**尋找**，然後選擇個別電話。

步驟 3 在**電話載入名稱**欄位中，輸入韌體的名稱。 針對這部電話，此處指定的韌體載入會覆寫**裝置預設組態**視窗中指定的預設韌體載入。

步驟 4 完成**電話組態**視窗中的其餘所有欄位。 如需有關欄位及其設定的說明，請參閱線上說明。

步驟 5 按一下**儲存**。

步驟 6 按一下**套用組態**以將變更的欄位推送到電話。

使用負載伺服器

若要讓電話從非 TFTP 伺服器的伺服器下載韌體更新，您可以在電話的**電話組態**頁面設定“負載伺服器”。 負載伺服器可能是另一個 Cisco Unified Communications Manager 或第三方伺服器。 第三方伺服器需能透過 TCP 連接埠 6970（建議）的 HTTP 或 UDP 型 TFTP 通訊協定提供電話要求的任何檔案。 某些電話機型僅支援 HTTP 韌體更新，例如 DX 系列 Cisco TelePresence 裝置。

附註 若要爲多部電話指派負載伺服器，您可以使用「批量管理工具」，透過CSV檔案或查詢來設定**負載伺服器**欄位。 如需詳細資訊，請參閱《*Cisco Unified Communications Manager* 批量管理指南》。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **電話**。

步驟 2 按一下**尋找**，然後選擇個別電話。

步驟 3 在**負載伺服器**欄位中，輸入替代伺服器的 IP 位址或主機名稱。

步驟 4 完成**電話組態**視窗中的其餘所有欄位。 如需有關欄位及其設定的說明，請參閱線上說明。

步驟 5 點擊**儲存**。

步驟 6 按一下**套用組態**以將變更的欄位推送到電話。

尋找具有非預設韌體載入的裝置

Unified Communications Manager中的「韌體載入資訊」視窗可讓您快速找到未針對其裝置類型使用預設韌體載入的裝置。

附註 每個裝置都可個別指定覆寫預設值的韌體載入。

請使用下列流程來找出未使用預設韌體載入的裝置。

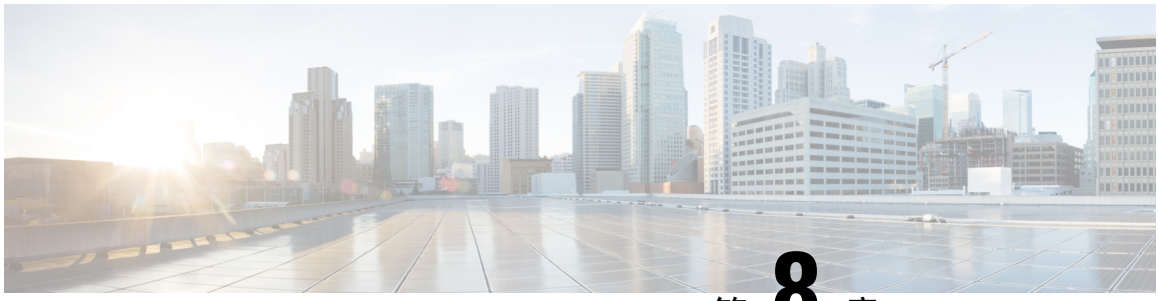
程序

步驟 1 選擇**裝置** > **裝置設定** > **韌體載入資訊**。

此頁面會更新，以顯示需要韌體載入的裝置類型清單。 對於每個裝置類型，「不使用預設載入的裝置」欄會連結到使用非預設載入之任何裝置的組態設定。

步驟 2 若要檢視使用非預設裝置載入之特定裝置類型的裝置清單，請在「不使用預設載入的裝置」欄中按一下該裝置類型的項目。

開啓的視窗會列出未執行預設韌體載入之特定裝置類型的裝置。



第 8 章

管理基礎架構裝置

管理基礎架構概覽

本章描述如何管理網路基礎架構裝置（例如交換器和無線存取點），以作爲Location Awareness功能的一部分。 啓用 Location Awareness 時，Cisco Unified Communications Manager 資料庫會儲存網路中交換器和存取點的狀態資訊，包括目前關聯至各交換器或存取點的端點清單。

基礎架構裝置對應的端點可協助 Cisco Unified Communications Manager 和 Cisco Emergency Responder 判斷來電者的實體位置。 例如，若行動用戶端在漫遊狀況撥出緊急通話時，Cisco Emergency Responder 會使用對應來判斷傳送緊急服務的地點。

儲存在資料庫的基礎架構資訊也可協助您監控基礎架構使用。 您可以在Cisco Unified Communications Manager 介面中檢視網路基礎架構裝置，例如交換器和無線存取點等等。 您也可以查看目前關聯至特定存取點或交換器的端點清單。 若未使用基礎架構裝置，您可以從追蹤停用基礎架構裝置。

管理基礎架構必需條件

您需設定 Location Awareness 功能，才可以於 Cisco Unified Communications Manager 介面管理無線基礎架構。 針對您的有線基礎架構，此功能會預設爲啓用。

有關配置詳細資訊，請參閱 Cisco Unified Communications Manager 功能組態指南。

您還需安裝網路基礎架構。 如需詳細資訊，請參閱基礎架構裝置（例如無線 LAN 控制器、存取點和交換器）隨附的硬體說明文件。

管理基礎架構工作流程

完成下列工作以監控及管理您的網路基礎架構裝置。

程序

	命令或動作	目的
步驟 1	檢視基礎架構裝置的狀態 ，第 82 頁上的	取得無線存取點或乙太網路交換器的目前狀態，包括關聯的端點清單。
步驟 2	停用基礎架構裝置的追蹤 ，第 82 頁上的	若您有非使用中的交換器或存取點，請將裝置標示爲非作用中。 系統會停止更新基礎架構裝置的關聯端點清單狀態。
步驟 3	啓用已停用的基礎架構裝置的追蹤 ，第 83 頁上的	初始化非作用中基礎架構裝置的追蹤。 Cisco Unified Communications Manager 便會開始以基礎架構裝置關聯端點清單的狀態更新資料庫。

檢視基礎架構裝置的狀態

使用此流程以在基礎架構裝置（例如無線存取點或乙太網路交換器）取得目前狀態。 您可以在Cisco Unified Communications Manager介面中檢視存取點或交換器的狀態，並查看關聯的端點的目前清單。

程序

步驟 1 在 Cisco Unified CM 管理中選擇 **advanced Features**（進階功能） > **Device Location Tracking Services**（裝置位置追蹤服務） > **Switches and Access Points**（交換器和存取點）。

步驟 2 按一下**尋找**。

步驟 3 按一下您要查看狀態的交換器或存取點。
Switches and Access Point Configuration（交換器和存取點組態）視窗便會顯示目前的狀態，包括目前關聯至存取點或交換器的端點清單。

停用基礎架構裝置的追蹤

使用此流程可爲特定基礎架構裝置移除追蹤，例如交換器或存取點。 您可以爲非使用中的交換器或存取點執行此操作。

附註 若移除基礎架構裝置的追蹤，則裝置會保留在資料庫中，但變成非作用中。 Cisco Unified Communications Manager 便不會再更新裝置的狀態，包括與基礎架構裝置關聯的端點清單。 您可以檢視從**相關鏈結**，在**交換機和存取點**視窗的下拉功能表中找到您的非活動交換機和存取點。

程序

步驟 1 在 Cisco Unified CM 管理中選擇 **advanced Features**（進階功能）> **Device Location Tracking Services**（裝置位置追蹤服務）> **Switches and Access Points**（交換器和存取點）。

步驟 2 按一下 **Find (尋找)**，然後選擇您要停止追蹤的交換器或存取點。

步驟 3 按一下 **Deactivate Selected** (停用選擇的項目)。

啟用已停用的基礎架構裝置的追蹤

使用此流程可起始已停用的非作用中基礎架構裝置的追蹤。一旦啓用交換器或存取點，Cisco Unified Communications Manager 便會開始動態追蹤狀態，包括關聯交換器或存取點的端點清單。

開始之前

需設定 Location Awareness。如需詳細資訊，請參閱《*Cisco Unified Communications Manager* 系統組態指南》中的「Location Awareness」一章。

程序

步驟 1 在 Cisco Unified CM 管理中選擇 **advanced Features**（進階功能）> **Device Location Tracking Services**（裝置位置追蹤服務）> **Switches and Access Points**（交換器和存取點）。

步驟 2 從**相關連結**選擇 **Inactive Switches and Access Points**（不活躍的交換器和存取點），然後按一下**執行**。

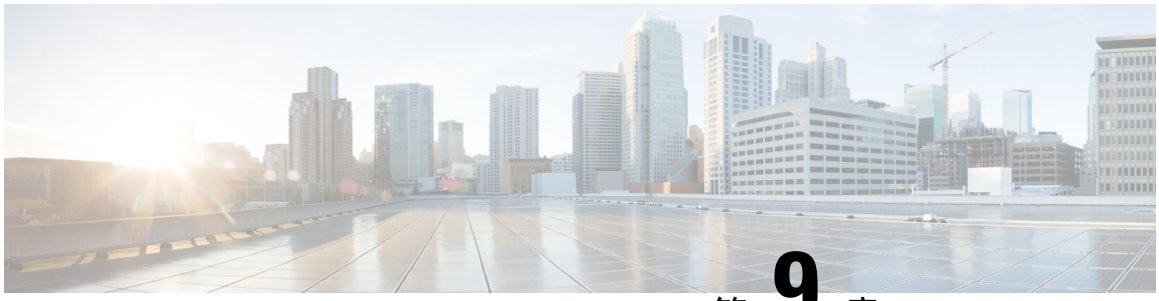
Find and List Inactive Switches and Access Points（尋找並列出不活躍的交換器和存取點）視窗便會顯示未追蹤的基礎架構裝置。

步驟 3 選擇要起始追蹤的交換器或存取點。

步驟 4 按一下 **Reactivate Selected**（重新啓用選擇項目）。

第 IV 部分

管理系統



第 9 章

監控系統狀態

檢視叢集節點狀態

使用此流程可在叢集中顯示節點資訊。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**顯示** > **叢集**。

步驟 2 檢閱**叢集**視窗中的欄位。 如需有關欄位的詳細資訊請參閱線上說明。

檢視硬體狀態

使用此流程可顯示系統硬體資源的硬體狀態和資訊。

程序

步驟 1 從 Cisco Unified 作業系統管理中，選擇**顯示** > **硬體**。

步驟 2 檢閱**硬體狀態**視窗中的欄位。 如需有關欄位的詳細資訊請參閱線上說明。

檢視網路狀態

使用此流程可顯示系統的網路狀態，例如乙太網路和 DNS 資訊。

顯示的網路狀態資訊視是否啓用「網路容錯」而定：

- 若啓用「網路容錯」，當乙太網路連接埠 0 失敗時，乙太網路連接埠 1 會自動管理網路通訊。
- 若啓用「網路容錯」，便會顯示網路連接埠乙太網路 0、乙太網路 1 和鍵結 0 的網路狀態資訊。
- 若未啓用「網路容錯」，只會顯示乙太網路 0 的狀態資訊。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**顯示** > **網路**。

步驟 2 檢閱**網路組態**視窗中的欄位。 如需有關欄位的詳細資訊請參閱線上說明。

檢視安裝的軟體

使用此流程可顯示軟體版本和安裝的軟體套件的相關資訊。

程序

步驟 1 從 Cisco Unified 作業系統管理中，選擇**顯示** > **軟體**。

步驟 2 檢閱 **Software Packages**（**軟體套件**）視窗中的欄位。 如需有關欄位的詳細資訊請參閱線上說明。

檢視系統狀態

使用此流程顯示整體系統狀態，例如地區設定、正常運作時間、CPU 使用和記憶體使用的資訊。

程序

步驟 1 從 Cisco Unified 作業系統管理中，選擇**顯示** > **系統**。

步驟 2 檢閱**系統狀態**視窗中的欄位。 如需有關欄位的詳細資訊請參閱線上說明。

檢視 IP 偏好設定

使用此流程可顯示系統可用的註冊連接埠清單。

程序

步驟 1 從 Cisco Unified 作業系統管理中，選擇**顯示** > **IP 偏好設定**。

步驟 2 (可選) 若要過濾或搜尋記錄，請執行下列其中一項工作：

- 從第一份清單中選擇搜尋參數。
- 從第二份清單中選擇搜尋型式。
- 如果適用的話，請指定適當的搜尋文字。

步驟 3 按一下**尋找**。

步驟 4 檢閱**系統狀態**視窗中顯示的欄位。 如需有關欄位的詳細資訊請參閱線上說明。

檢視最後登入詳細資料

當一般使用者（使用本機或 LDAP 憑證）與管理員登入 Cisco Unified Communications Manager 或 IM and Presence Service 的 Web 應用程式時，主要應用程式視窗會顯示上次成功和失敗登入的詳細資料。

使用 SAML SSO 功能登入的使用者只能檢視上次成功登入系統的資訊。 使用者可以參考身分識別提供者 (IdP) 應用程式來追蹤失敗 SAML SSO 登入的資訊。

下列 Web 應用程式會顯示嘗試登入資訊：

- Cisco Unified Communications Manager：
  - Cisco Unified CM 管理
  - Cisco Unified 報告
  - Cisco Unified Serviceability
- IM and Presence Service
  - Cisco Unified CM IM and Presence 管理
  - Cisco Unified IM and Presence 報告
  - Cisco Unified IM and Presence Service功能

只有管理員可以在 Cisco Unified Communications Manager 中登入及檢視下列 Web 應用程式的上次登入詳細資料：

- 災害復原系統

- Cisco Unified 作業系統管理

偵測節點

使用 Ping 公用程式偵測網路中的其他節點。 這些結果可協助您驗證或對裝置連線進行疑難排解。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇 **Services**（服務） > **Ping**（偵測）。

步驟 2 配置 **Ping Configuration**（偵測組態）視窗中的欄位。 如需有關欄位及其組態選項的詳細資訊，請參閱線上說明。

步驟 3 選擇 **Ping**（偵測）。

偵測結果會隨即顯示。

顯示服務參數

您可能需要比較屬於叢集中所有伺服器上特定服務的所有服務參數。 您可能也需要只顯示未同步的參數（也就是在不同伺服器中有不同值的服務參數）或是已從建議值修改的參數。

請使用下列流程，以針對叢集中所有伺服器的特定服務顯示服務參數。

程序

步驟 1 選擇**系統** > **服務參數**。

步驟 2 在伺服器下拉式清單方塊中選擇一個伺服器。

步驟 3 在服務下拉式清單方塊中，選擇要在叢集中所有伺服器上顯示服務參數的服務。

附註 「服務參數組態」視窗會顯示所有服務（啓用或非啓用）。

步驟 4 在顯示的「服務參數組態」視窗中，在相關連結下拉式清單方塊中選擇「Parameters for All Servers」（所有伺服器的參數）；然後按一下「執行」。

隨即顯示「Parameters for All Servers」（所有伺服器的參數）視窗。 此清單會針對目前的服務依字母順序顯示所有參數。 對於每個參數，都會在參數名稱旁邊顯示建議值。每個參數名稱底下皆會顯示包含此參數的伺服器清單。 每個伺服器名稱旁皆會顯示這部伺服器上目前用於此參數的值。

針對指定的參數，按一下伺服器名稱或目前參數值，可連接至對應的服務參數視窗，以變更該值。按一下「Previous」（上一個）和「Next」（下一個）可導覽「Parameters for All Servers」（所有伺服器的參數）視窗。

步驟 5 若要顯示未同步的服務參數，請在「相關連結」下拉式清單方塊中，選擇「Out of Sync Parameters for All Servers」（所有伺服器的未同步參數），然後按一下「Go」（執行）。

隨即顯示「Out of Sync Parameters for All Servers」（所有伺服器的未同步參數）視窗。 針對目前的服務，在不同伺服器上具有不同值的服務參數會以字母順序顯示。 對於每個參數，都會在參數名稱旁邊顯示建議值。每個參數名稱底下皆會顯示包含此參數的伺服器清單。 每個伺服器名稱旁皆會顯示這部伺服器上目前用於此參數的值。

針對指定的參數，按一下伺服器名稱或目前參數值，可連接至對應的服務參數視窗，以變更該值。按一下「Previous」（上一個）和「Next」（下一個）可導覽「Out of Sync Parameters for All Servers」（所有伺服器的未同步參數）視窗。

步驟 6 若要顯示已從建議值修改的服務參數，請在「相關連結」下拉式清單方塊中，選擇「Modified Parameters for All Servers」（所有伺服器的已修改參數），然後按一下「Go」（執行）。

隨即顯示「Modified Parameters for All Servers」（所有伺服器的已修改參數）視窗。 針對目前的服務，具有與建議值不同的值的服務參數會以字母順序顯示。 對於每個參數，都會在參數名稱旁邊顯示建議值。每個參數名稱底下皆會顯示其值與建立值相異的伺服器清單。 每個伺服器名稱旁皆會顯示這部伺服器上目前用於此參數的值。

針對指定的參數，按一下伺服器名稱或目前參數值，可連接至對應的服務參數視窗，以變更該值。按一下「Previous」（上一個）和「Next」（下一個）可導覽「Modified Parameters for All Servers」（所有伺服器的已修改參數）視窗。

配置網路 DNS

使用此流程來設定您的網路 DNS

附註 您還可在 Cisco Unified CM 管理中的 DHCP 組態視窗指派 DNS 主伺服器和輔助伺服器。

程序

步驟 1 登入命令行介面。

步驟 2 若要指派 DNS 伺服器，請在發布者節點上執行以下命令之一：

- 指定主要 DNS 伺服器 **run set network dns primary <ip_address>**
- 指定次要 DNS 伺服器 **run the set network dns secondary <ip_address>**

步驟 3 指派其他 DNS 選項：**run the set network dns options [逾時|秒] [嘗試次數|數目] [旋轉]**。

- 超時設定 DNS 逾時
- 秒數爲逾時會經之秒數

- 嘗試次數設定嘗試 DNS 請求的次數
- 數目表示嘗試次數
- 巡迴會導致系統在已配置的 DNS 伺服器之間旋轉並指派負載

例如，set network dns options timeout 60 attempts 4 rotate

執行此命令後，伺服器將重新開機。

第 10 章

警報

概覽

Cisco Unified Serviceability 和 Cisco Unified IM and Presence Serviceability警報提供有關執行階段狀態和系統狀態等資訊，因此您可以疑難排解與系統相關的問題。例如，辨識與災害恢復系統相關的問題。 警報資訊不只包括說明和建議操作，另包括應用程式名稱、電腦名稱等資訊，除了可以協助您排解疑難問題之外，還適用於叢集。

您可以將警報介面設定爲將警報資訊傳送到多個位置，而且每個位置都可以擁有自己的警報事件層級 (從除錯到緊急)。 您可以將警報導向 Syslog Viewer (本機 syslog) 、Syslog 檔案 (遠端 syslog) 、SDL 追蹤記錄檔案 (僅適用於 Cisco CallManager 和 CTIManager 服務) 或所有目的地。

當服務發出警報時，警報介面會將警報資訊傳送到已設定而且在警報定義之路由清單中指定的位置 (如 SDI 追蹤)。 系統可以轉發警報資訊 (如 SNMP 陷阱) ，也可以將警報資訊寫入其最終目的地 (如記錄檔案)。

您可以爲特定節點上的服務 (如 Cisco 資料庫層監控) 設定警報，也可以爲叢集中所有節點上的特定服務設定警報。

附註 Cisco Unity Connection SNMP 不支援陷阱。

提示 對於遠端 Syslog 伺服器，請勿指定 Unified Communications Manager 伺服器，因爲該伺服器不能接受來自其他伺服器的 syslog 訊息。

您可以使用 Cisco Unified 即時監控工具 (Unifed RTMT) 中的追蹤和記錄檔中心來收集傳送到 SDL 追蹤記錄檔案的警報 (僅適用於 Cisco CallManager 和 CTIManager 服務)。 您可以在 Unifed RTMT 中使用 SysLog Viewer 來查看傳送到本機 syslog 的警報資訊。

警報組態

您可以在 Cisco Unified Serviceability 中爲 Cisco 資料庫層監控 之類的服務設定警報。 接著，您可以設定系統傳送警報資訊的一或多個目的地位置，如 Syslog Viewer (本機 syslog)。 透過此選項，您可以執行以下操作：

- 爲特定伺服器或所有伺服器上的服務設定警報 (僅適用於 Unified Communications Manager 叢集)
- 爲設定的服務或伺服器設定不同的遠端 syslog 伺服器
- 爲不同的目的地設定不同的警報事件層級設定

透過 Cisco Unified Communications Manager 管理中的 Cisco Syslog Agent 企業參數，您可以使用以下兩個設定將達到或超過設定之臨界值的所有警報轉送到遠端 syslog 伺服器：遠端 syslog 伺服器名稱和 syslog 嚴重性。 若要存取這些 Cisco Syslog 代理參數，請前往組態適用的視窗：

Unified Communications Manager	在 Cisco Unified Communications Manager 管理中，選擇**系統** > **企業參數**。
Cisco Unity Connection	在 Cisco Unity Connection 管理中，選擇**系統設定** > **企業參數**。
Cisco IM and Presence	在 Cisco Unified Communications Manager IM and Presence 管理中，選擇**系統** > **企業參數**。

警報包括系統 (作業系統/硬體平台) 、應用程式 (服務) 和 安全警報。

附註 若在 Cisco Unified Serviceability 中同時設定了 Cisco Syslog 代理警報企業參數和應用程式 (服務) 警報，系統可以將同一警報傳送到遠端 syslog 兩次。

若爲應用程式警報啓用本機 syslog，唯有當警報同時超過本機 syslog 臨界值和企業臨界值時，系統才會將警報傳送到企業遠端 syslog 伺服器。

若您同時在 Cisco Unified Serviceability 中啓用遠端 syslog，系統將使用在 Cisco Unified Serviceability 中設定的應用程式臨界值將警報轉送到遠端 syslog 伺服器，這可能會導致警報傳送到遠端 syslog 伺服器兩次。

事件層級/嚴重性設定爲系統收集的警示和訊息提供一種過濾機制。 此設定有助於防止 Syslog 和追蹤檔案超載。 系統只會轉送超過設定之臨界值的警示和訊息。

若要深入瞭解警報和事件的附帶的嚴重性層級，請參閱警報定義 ，第 95 頁上的。

警報定義

用於參考，警報定義說明警報訊息：它們的含義以及如何從中復原。 您可在「警報定義」視窗中搜尋警報資訊。 按一下任何服務特定的警報定義時，會顯示警報資訊的說明 (包括已新增的任何使用者定義文字) 和建議的動作。

您可以搜尋Serviceability GUI 中顯示的所有警報的警報定義。 爲了幫助您疑難排解問題，存在於相應目錄中的定義包括警報名稱、說明、解釋、建議的操作、嚴重性、參數和監控器。

系統產生警報時，它會在警報資訊中使用警報定義名稱，讓您可以識別警報。 在警報定義中，您可以檢視路由清單，此清單指定系統可以傳送警報資訊的位置。 路由清單可能包括以下位置，這些位置與您可以在「警報組態」視窗中設定的位置相關：

- 僅限 Unified Communications Manager：SDL - 若爲此選項啓用警報，並在「警報組態」視窗中指定事件層級，則系統會將警報資訊傳送到 SDL 追蹤。
- SDI - 若爲此選項啓用警報，並在「警報組態」視窗中指定事件層級，則系統會將警報資訊傳送到 SDI 追蹤。
- 系統記錄檔 - 若爲此選項啓用警報、在「警報組態」視窗中指定事件層級，並爲遠端 Syslog 伺服器輸入伺服器名稱或 IP 位址 ，則系統會將警報資訊傳送到遠端 Syslog 伺服器。
- 事件記錄檔 - 若爲此選項啓用警報，並在「警報組態」視窗中指定事件層級，系統會將警報資訊傳送到本機 Syslog，您可以在 Cisco Unified 即時監控工具 (Unified RTMT) 中的 SysLog Viewer 檢視此警報資訊。
- 資料收集器 - 系統會將警報資訊傳送到即時資訊系統 (RIS 資料收集器) ，僅用於警示目的。 您無法在「警報組態」視窗中設定此選項。
- SNMP 陷阱 - 系統會產生 SNMP 陷阱。 您無法在「警報組態」視窗中設定此選項。

提示 若 SNMP 陷阱位置顯示在路由清單中，則系統會將警報資訊轉移到 CCM MIB SNMP 代理，此代理會根據 CISCO-CCM-MIB 中的定義產生陷阱。

若「警報組態」視窗中爲特定位置設定的警報事件層級等於或低於警報定義中列出的嚴重性，則系統會傳送警報。 例如，若警報定義中的嚴重性等於 WARNING_ALARM，並且在「警報組態」視窗中，將特定目標的警報事件層級設定爲「警示」、「注意」、「資訊」或「除錯」(這些是較低的事件層)，則系統會將警報傳送到對應目標。 若您將警報事件層級設定爲「緊急」、「警示」、「嚴重」或「錯誤」，則系統不會將警報傳送到對應位置。

對於每個警報定義，您可以包括其他說明或建議。所有管理員都可以存取新增的資訊。您可以直接在「警報詳細資料」視窗中顯示的「使用者定義的文字」窗格中輸入資訊。 標準水平和垂直捲軸支援捲動。 Cisco Unified Serviceability會將資訊新增至資料庫。

警報資訊

您可以檢視警報資訊，以判定是否存在問題。 您用來檢視警報資訊的方法取決於設定警報時選擇的目標。 您可以檢視傳送到 SDL 追蹤記錄檔的警報資訊 (僅適用於 Unified Communications Manager)，方法是使用 Unified RTMT 中的「追蹤和記錄檔中心」選項或使用文字編輯器。 您可以使用 Unified RTMT 中的 SysLog Viewer，檢視傳送到本機 Syslog 的警報資訊。

設定警報

請執行以下步驟來設定警報。

程序

步驟 1 在 Cisco Unified Communications Manager 管理、Cisco Unity Connection 管理或 Cisco Unified IM and Presence 管理中，設定 Cisco Syslog 代理企業參數，以將系統、應用程式 (服務) 和安全性警報/訊息傳送至您指定的遠端 Syslog 伺服器。 跳過此步驟以在 Cisco Unified Serviceability中設定應用程式 (服務) 警報/訊息。

步驟 2 在 Cisco Unified Serviceability中，爲您想要收集的應用程式 (服務) 警報資訊設定伺服器、服務、目的地和事件層級。

步驟 3 (選用) 將定義新增至警報。

- 所有服務都可以移至 SDI 記錄檔 (但也需在追蹤中進行設定)。
- 所有服務都可以移至 SysLog Viewer。
- 僅限 Unified Communications Manager：僅 Cisco CallManager 和 CiscoCTIManager 服務使用 SDL 記錄檔。
- 若要將 Syslog 訊息傳送到遠端 Syslog 伺服器，請檢查遠端 Syslog 目的地並指定主機名稱。若未設定遠端伺服器名稱，則 Cisco Unified 服務能力不會將 Syslog 訊息傳送到遠端 Syslog 伺服器。

提示 請勿將 Unified Communications Manager 伺服器設定爲遠端 Syslog 伺服器。

步驟 4 若選擇 SDL 追蹤檔案作爲警報目的地，請使用 Unified RTMT 中的「追蹤和記錄檔中心」選項收集追蹤並檢視資訊。

步驟 5 若選擇本機 Syslog 作爲警報目的地，請在 Unified RTMT 以 SysLog Viewer 檢視警報資訊。

步驟 6 如需說明和建議的動作，請參閱相應的警報定義。

警報服務設定

Syslog 代理企業參數

您可以設定 Cisco Syslog Agent 企業參數，以將超出設定臨界值的系統、應用程式和安全警報/訊息發送到指定的遠端 syslog 伺服器。 若要存取 Cisco Syslog 代理參數，請前往組態適用的視窗：

Unified Communications Manager	在 Cisco Unified Communications Manager 管理中，選擇**系統** > **企業參數**。
Cisco Unity Connection	在 Cisco Unity Connection 管理中，選擇**系統設定** > **企業參數**。
Cisco IM and Presence	在 Cisco Unified Communications Manager IM and Presence 管理中，選擇**系統** > **企業參數**。

接下來，設定遠端 Syslog 伺服器名稱 (遠端 Syslog 伺服器名稱 1、遠端 Syslog 伺服器名稱 2、遠端 Syslog 伺服器名稱 3、遠端 Syslog 伺服器名稱 4 和、遠端 Syslog 伺服器名稱 5) 和 Syslog 嚴重性。 在設定伺服器名稱時，請務必指定有效的 IP 地址。 Syslog 嚴重性適用於您設定的所有遠端 Syslog 伺服器。 接著按一下**儲存**。 要輸入有效值，請按一下 **?** 按鈕。 若未指定伺服器名稱，Cisco Unified Serviceability不會傳送 Syslog 訊息。

注意 在 Unified Communications Manager 中設定遠端 Syslog 伺服器時，請勿爲遠端 Syslog 伺服器名稱新增重複的項目。 若新增重複項目，則在向遠端 Syslog 伺服器傳送訊息時，Cisco Syslog 代理將忽略重複項目。

附註 不要將 Unified Communications Manager 設定爲遠端 Syslog 伺服器。 Unified Communications Manager 節點不接受來自其他伺服器的 Syslog 訊息。

設定警報服務

本節說明如何爲您透過 Cisco Unified Serviceability管理的功能或網路服務新增或更新警報。

附註 Cisco 建議您不要變更 SNMP 陷阱和目錄組態。

Cisco Unity Connection 也會使用 Cisco Unity Connection Serviceability中提供的警報。 您無法在 Cisco Unity Connection Serviceability中設定警報。 如需詳細資料，請參閱 *Cisco Unity Connection Serviceability* 管理指南。

如需如何使用標準登錄編輯器的詳細資訊，請參閱線上作業系統檔案。

程序

步驟 1 選擇**警示** > **組態**。

「警報組態」視窗隨即顯示。

步驟 2 在「伺服器」下拉式清單選擇要設定警報的伺服器，然後按一下**執行**。

步驟 3 從「服務群組」下拉式清單選擇要設定警報的服務類別 (如資料庫與管理服務) ，然後按一下**執行**。

提示 如需對應至服務群組的服務清單，請參閱服務群組。

步驟 4 從「服務」下拉式清單選擇要設定警報的服務，然後按一下**執行**。

只有支援服務群組和組態的服務會顯示。

提示 下拉式清單顯示活躍和不活躍的服務。

在「警報組態」視窗中，爲選擇的服務顯示具有事件層級的警報監控器清單。 此外，也會顯示「套用到所有節點」勾選方塊。

步驟 5 僅限 Unified Communications Manager：若想要這樣做，您可以將服務的警報組態套用到叢集中的所有節點，方法爲勾選**套用到所有節點**方塊，前提是您的組態支援叢集。

步驟 6 如「警報組態」設定中所述進行設定，其中包括監控器和事件層級的說明。

步驟 7 若要儲存您的組態，請按一下**儲存**按鈕。

附註 若要設定預設值，請按一下**設定預設**按鈕，然後按一下**儲存**。

下一步

提示 若「警報組態」視窗中爲特定目標設定的警報事件層級等於或低於警報定義中列出的嚴重性，則系統會傳送警報。 例如，若警報定義中的嚴重性等於 WARNING_ALARM，並且在「警報組態」視窗中，將特定目標的警報事件層級設定爲「警示」、「注意」、「資訊」或「除錯」(這些是較低的事件層) ，則系統會將警報傳送到對應目標。 若您將警報事件層級設定爲「緊急」、「警示」、「嚴重」或「錯誤」(這些是較高的嚴重等級) ，則系統不會將警報傳送到對應位置。

若要存取 Cisco Extension Mobility Application 服務、Cisco Unified Communications Manager Assistant 服務、Cisco Extension Mobility 服務和 Cisco Web Dialer 服務的警報定義，請如警報定義中所述，選擇「警報訊息定義」視窗中的 **JavaApplications** 目錄。

設定使用 Cisco Tomcat 的警報服務

以下服務使用 Cisco Tomcat 產生警報：

- Cisco Extension Mobility 應用程式

- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer

系統登入警報 AuthenticationFailed 也會使用 Cisco Tomcat。 若要爲這些服務產生警報，請執行以下程式。

程序

步驟 1 在 Cisco Unified Serviceability中，選擇**警報** > **組態**。

步驟 2 在「伺服器」下拉式清單選擇要設定警報的伺服器，然後按一下**執行**。

步驟 3 在「服務群組」下拉式清單中，選擇**平台服務**；然後，按一下**執行**。

步驟 4 在「服務」下拉式清單中，選擇 **Cisco Tomcat**然後，按一下**Go**。

步驟 5 僅限 Unified Commuications Manager：若想要這樣做，您可以將服務的警報組態套用至叢集中的所有節點，方法爲勾選**套用到所有節點**方塊，前提是您的組態支援叢集。

步驟 6 如「警報組態」設定中所述進行設定，其中包括監控器和事件層級的說明。

步驟 7 若要儲存您的組態，請按一下**儲存**按鈕。

服務群組

下表列出了與警報組態視窗中服務群組下拉式清單中的選項相對應的服務。

附註 並非所有列出的服務群組和服務都適用於所有系統組態。

表 *6:* 警報組態中的服務群組

服務群組	服務
CM 服務	Cisco CTIManager、Cisco CallManager、Cisco DHCP 監控服務、Cisco 已撥出號碼分析工具、Cisco 已撥出號碼分析工具伺服器、Cisco Extended Functions、Cisco IP 語音媒體串流 App、Cisco Messaging Interface、Cisco 耳機服務和 Cisco TFTP
CTI 服務	Cisco IP Manager Assistant 和 Cisco WebDialer Web 服務
CDR 服務	Cisco CAR Scheduler、Cisco CDR Agent 和 Cisco CDR Repository Manager
資料庫與管理服務	Cisco 批量佈建服務 和 Cisco 資料庫層監控
效能與監控服務	Cisco AMC Service 和 Cisco RIS Data Collector
安全性服務	Cisco 憑證授權單位代理功能和 Cisco 憑證到期監控程式

服務群組	服務
目錄服務	Cisco DirSync
備份與還原服務	Cisco DRF Local 和 Cisco DRF Master
系統服務	Cisco 追蹤收集服務
平台服務	Cisco Tomcat 和 Cisco Smart License Manager
位置追蹤服務	Cisco 無線控制器同步服務

警報組態設定

下表描述所有警報組態設定，即便服務可能不支援這些設定。

表 *7:* 警報組態設定

名稱	描述
伺服器	從下拉式清單選擇要設定警報的伺服器(節點)，然後按一下**執行**。
服務群組	Cisco Unity Connection 僅支援以下服務群組：資料庫與管理服務、效能監控服務、備份與還原服務、系統服務及平台服務。 從下拉式清單選擇要設定警報的服務類別 (如資料庫與管理服務)，然後按一下**執行**。
服務	從「服務」下拉式清單選擇要設定警報的服務，然後按一下**執行**。 只有支援服務群組和組態的服務會顯示。 **提示**　下拉式清單會顯示活躍和不活躍的服務。
僅適用於 Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service： 套用到所有節點	若要將服務的警報設定套用到叢集中的所有節點，請勾選方塊。
啓用本機 Syslog 警報	SysLog 檢視器能當做警報目的地。該程式會將錯誤記錄在 SysLog Viewer 的應用程式記錄檔中，並提供警報說明和建議動作。您可以從 Cisco Unified 即時監控工具存取 SysLog Viewer。 如需使用 SysLog Viewer 檢視記錄檔的相關資訊，請參閱 *Cisco Unified* 即時監控工具管理指南。

名稱	描述
啓用遠端 Syslog 警報	SysLog 檔案能當做警報目的地。 勾選此方塊可將 Syslog 訊息儲存在 Syslog 伺服器上並指定 Syslog 伺服器名稱。若啓用此目的地但未指定伺服器名稱，Cisco Unified 服務能力不會傳送 Syslog 訊息。 設定的 AMC 主要和容錯移轉收集器會使用遠端 syslog 設定。 收集器使用的遠端 syslog 設定是在各個節點上配置的設定。 若您只在 AMC 主要收集器上設定遠端 syslog，未在 AMC 容錯移轉收集器上設定遠端syslog，當容錯移轉發生在AMC主要收集器時，系統不會產生任何遠端 syslog。 您需在所有節點上配置完全相同的設定，才能將遠端 syslog 警報傳送到同一部遠端 syslog 伺服器。 當容錯移轉發生在 AMC 控制器或是當收集器組態變更爲其他節點時，系統會使用備份或新設定節點上的遠端 syslog 設定。 爲防止系統充斥過多警報，您可以勾選**排除端點警報**方塊。 這樣可以確保將端點電話相關事件記錄在單獨的檔案中。 唯有 CallManager 服務會顯示**排除端點警報**方塊，其預設值爲未勾選。當您勾選此方塊時亦需勾選**套用到所有節點**。端點警報的組態選項會列示在警報組態設定中。 **提示** 請勿將 Unified Communications Manager 或 Cisco Unified Communications Manager IM and Presence Service 節點指定爲目的地，因爲該節點不接受來自另一個節點的 syslog 訊息。
遠端 Syslog 伺服器	在每個「伺服器名稱1」、「伺服器名稱2」、「伺服器名稱3」、「伺服器名稱 4」和「伺服器名稱 5」欄位中，輸入要用於接受 syslog 訊息的遠端 syslog 伺服器名稱或 IP 位址。 例如，若要將警報傳送到 Cisco Unified Operations Manager，請將伺服器名稱指定爲 Cisco Unified Operations Manager。 **提示** 請勿將 Unified Communications Manager 或 Cisco Unified Communications Manager IM and Presence Service 節點指定爲目的地，因爲該節點不接受來自另一個節點的 syslog 訊息。
啓用 SDI 追蹤警報	SDI 追蹤庫能當做警報目的地。 若要記錄警報，請勾選此方塊，然後在所選服務的「追蹤組態」視窗中勾選「追蹤開啓」方塊。 如需在 Cisco Unified Serviceability「追蹤組態」視窗中組態設定的相關資訊，請參閱「設定追蹤參數」。

名稱	描述
僅限 Unified Communications Manager 和 Unified Communications Manager BE： 啓用 SDL 追蹤警報	SDL 追蹤庫能當做警報目的地。 此目的地僅適用於 Cisco CallManager 服務和 CTIManager 服務。 請使用追蹤 SDL 組態來設定此警報目的地。若要將警報記錄在SDL追蹤記錄檔中，請勾選此方塊，然後在所選服務的「追蹤組態」視窗中勾選「追蹤開啓」方塊。 如需在 Cisco Unified Serviceability「追蹤組態」視窗中組態設定的相關資訊，請參閱「設定追蹤參數」。
警報事件層級	在下拉式清單中選擇下列其中一個選項： **緊急** 此層級會將系統指定爲不可使用。 **警示** 此層級表示需要立即採取行動。 **嚴重** 系統偵測到嚴重情況。 **錯誤** 此層級表示存在錯誤情況。 **警示** 此層級表示偵測到警示情況。 **注意** 此層級指出正常但重要的情況。 **資訊** 此層級只會指出資訊訊息。 **除錯** 此層級指出Cisco技術支援中心工程師用於除錯的詳細事件資訊。

下表說明預設警報組態設定。

	本機 Syslog	遠端 Syslog	SDI 追蹤	SDL 追蹤
啓用警報	勾選	未勾選	勾選	勾選
警報事件層級	錯誤	已停用	錯誤	錯誤

排除端點警報	本機 Syslog	替代 Syslog	遠端 Syslog	Syslog 嚴重性和抑制警報	Syslog 陷阱
勾選	否	是	否	否	否

未勾選	否	是	是	是	是

警報定義和使用者定義的說明新增

本節提供程式資訊，爲Serviceability介面中顯示的警報定義搜尋、檢視和建立使用者資訊。

檢視警報定義和新增使用者定義的說明

本節說明如何搜尋和檢視警報定義。

提示 僅限 Unified Communications Manager 和 Cisco Unity Connection：您可以檢視 Cisco Unity Connection 服務能力中的 Cisco Unity Connection 警報定義。 您無法將使用者定義的說明新增到 Cisco Unity Connection Serviceability中的警報定義。

Cisco Unity Connection 也會使用 Cisco Unified Serviceability中的某些警報定義，並且需在 Cisco Unified Serviceability中檢視它們。 請注意，可以檢視與系統目錄中的目錄相關聯的警報。

開始之前

檢閱警報定義目錄的說明。

程序

步驟 1 選擇**報警** > **定義**。

步驟 2 請執行下列一項動作：

- 選擇警報，如下所示：
  - 從**尋找警報位置**下拉式清單中選擇警報目錄，例如，系統警報目錄或 IM and Presence 警報目錄。
  - 從**等於**下拉式清單中選擇特定的目錄名稱。
- 在**輸入警報名稱**欄位中輸入警報名稱。

步驟 3 選取「**尋找**」。

步驟 4 若警報定義存在多個頁面，請執行以下其中一個動作：

- 若要選擇另一個頁面，請選擇**警報訊息定義**視窗底端的適當導覽按鈕。
- 若要變更視窗中顯示的警報數目，請從**每頁列數**下拉式清單中選擇不同的值。

步驟 5 選擇您想要警報詳細資料的警報定義。

步驟 6 若想要將資訊新增至警報，請在**使用者定義的文字**欄位中輸入文字，然後選擇**儲存**。

提示　若您在**使用者定義的文字**欄位中新增文字，您可以隨時選擇**全部清除**以刪除您輸入的資訊。

步驟 7 選取**儲存**。

步驟 8 若想要返回**警報訊息定義**視窗，請從「相關連結」下拉式清單中選擇**返回尋找/列出警報**。

步驟 9 選擇**執行**。

系統警報目錄說明

下表包含系統警報目錄警報說明。 系統警報目錄支援 Unified Communications Manager 和 Cisco Unity Connection。

表 *8:* 系統目錄

名稱	描述
叢集管理員警報目錄	與叢集中伺服器之間的安全性關聯建立有關的所有叢集管理員警報定義
資料庫警報目錄	所有 Cisco 資料庫警報定義
災害復原系統警報目錄	所有災害復原系統警報定義
通用警報目錄	所有應用程式共用的所有通用警報定義
Java 應用程式	所有 Java 應用程式警報定義。 **提示**　您無法使用警報組態 GUI 設定 JavaApplications 警報。 對於 Un Communications Manager 和 Cisco Unity Connection，通常會在事 檔中設定警報爲；對於 Unified Communications Manager，您可以 些警報以產生 SNMP 設陷，以與 CiscoWorks LAN 管理解決方案 使用作業系統隨附的註冊表編輯器來檢視或變更警報定義和參數
Extension Mobility 警報目錄	Extension Mobility 警報
登入警報目錄	所有與登入有關的警報定義
記錄檔分割監控追蹤收集目錄	所有記錄檔分割監控和追蹤收集警報定義
RTMT 警報目錄	所有 Cisco Unified 即時監控工具警報定義
系統存取目錄	用於追蹤 SystemAccess 是否同時提供所有執行緒統計資料計數器和所 計資料計數器的所有警報定義。
服務管理員警報目錄	與服務的啓用、停用、啓動、重新啓動和停止相關的所有服務管理員警
TFTP 警報目錄	所有 Cisco TFTP 警報定義
信任驗證服務警報目錄	信任驗證服務警報

名稱	描述
測試警報目錄	用於從命令行介面 (CLI) 透過 SNMP 設限傳送測試警報的所有警報 詳細資訊，請參閱 *Cisco Unified* 解決方案的命令行介面參考指南。 **提示** Cisco Unity Connection SNMP 在 Unified Communications Mana Unity Connection 系統中均不支援設陷。
憑證監控警報目錄	所有憑證到期定義。
CTL 提供者警報目錄	憑證信任清單 (CTL) 提供者服務的警報
CDP 警報目錄	Cisco Discovery Protocol (CDP) 服務的警報
IMS 警報目錄	所有使用者驗證和認證定義。
SLM 警報目錄	Cisco Smart Licensing 警報

CallManager 警報目錄說明

本節中的資訊不適用於 Cisco Unity Connection。

下表包含 CallManager 警報目錄說明。

表 *9: CallManager* 警報目錄

名稱	描述
CallManager	所有 Cisco CallManager 服務警報定義
CDRRepAlarmCatalog	所有 CDRRep 警報定義
CARAlarmCatalog	所有 CDR 分析和回報警報定義
CEFAlarmCatalog	所有 Cisco Extended Functions 警報定義
CMIAlarmCatalog	所有 Cisco Messaging Interface 警報定義
CtiManagerAlarmCatalog	所有 Cisco 電腦電話整合 (CTI) 管理員警報定義
IpVmsAlarmCatalog	所有 IP Voice Media Streaming 應用程式警報定義
TCDSRVAlarmCatalog	所有 Cisco 電話通話發送器服務警報定義
電話	電話相關任務的警報，例如下載
CAPFAlarmCatalog	憑證授權單位代理功能 (CAPF) 服務的警報
SAMLSSOAlarmCatalog	SAML 單一登錄功能的警報。

IM and Presence 警報目錄說明

下表包含 IM and Presence Service警報目錄說明。

表 *10: IM and Presence Service*警報目錄

名稱	描述
CiscoUPSConfigAgent	將 IM and Presence Service IDS 資料庫中的組態變更通知 IM and Presence Service SIP Proxy的所有組態代理警報。
CiscoUPInterclusterSyncAgent	在用於叢集間路由的 IM and Presence Service之間同步化一般使用者資訊的所有叢集間同步代理。
CiscoUPSPresenceEngine	收集使用者可用性狀態和通訊功能之相關資訊的所有狀態引擎警報。
CiscoUPSSIPProxy	與路由，請求者識別和傳輸互連有關的所有 SIP Proxy 警報。
CiscoUPSSOAP	使用 HTTPS 提供進出外部使用者端之安全 SOAP 介面的所有簡易物件存取通訊協定 (SOAP) 警報
CiscoUPSSyncAgent	將 IM and Presence 資料與 Unified Communications Manager 資料保持同步的所有同步代理警報。
CiscoUPXCP	收集 IM and Presence Service上 XCP 元件和服務之狀態相關資訊的所有 XCP 警報。
CiscoUPServerRecoveryManager	與狀態備援群組中節點之間的容錯移轉和後援程式有關的所有伺服器復原管理員警報。
CiscoUPReplWatcher	監控 IDS 複寫狀態的所有 ReplWatcher 警報。
CiscoUPXCPConfigManager	與 XCP 元件相關的所有 Cisco XCP Config Manager 警報定義。

警報資訊，其中包括說明和建議的動作，還包括應用程式名稱、伺服器名稱和其他資訊，以協助您執行疑難排解，即使針對不在本機 IM and Presence Service節點上發生的問題也一樣。

如需 IM and Presence Service特定警報的詳細資訊，請參閱 *Cisco Unified Communications Manager* 上 *IM and Presence* 的系統錯誤訊息。

CiscoSyslog 檔案中的預設警報

下表包含預設警報說明，解說在沒有任何警報組態的情況下於 CiscoSyslog 檔案中觸發的警報：

表 *11: CiscoSyslog* 檔案中的預設警報

名稱	描述
CLM_IPSecCertUpdated	由於發生變更，因此已匯入叢集中對等節點的 IPSec 自我簽署憑證。
CLM_IPAddressChange	叢集中對等節點的 IP 位址已變更。
CLM_PeerState	叢集管理員與叢集中其他節點的作業階段狀態已變更爲目前狀態。
CLM_MsgIntChkError	叢集管理員收到一則未通過訊息完整性檢查的訊息。 這可能代表叢集中其他節點的安全密碼設定錯誤。
CLM_UnrecognizedHost	叢集管理員從非設定爲此叢集中節點的 IP 位址接收到一則訊息。
CLM_ConnectivityTest	叢集管理員偵測到網路錯誤。
ServiceActivated	此服務現在已啓動。
ServiceDeactivated	此服務現在已停用。
ServiceActivationFailed	無法啓動此服務。
ServiceDeactivationFailed	無法停用此服務。
ServiceFailed	服務突然終止。 服務管理員將嘗試重新啓動。
ServiceStartFailed	無法啓動此服務。 服務管理員將嘗試再次啓動服務。
ServiceStopFailed	重試幾次後依然無法停止指定的服務。 該服務將標記爲已停止。
ServiceRestartFailed	無法重新啓動指定的服務。
ServiceExceededMaxRestarts	無法啓動服務，即使達到重新啓動嘗試次數上限也無法啓動。
FailedToReadConfig	無法讀取組態檔案。 組態檔案可能已損毀。
MemAllocFailed	無法配置記憶體。
SystemResourceError	系統通話失敗。
ServiceManagerUnexpectedShutdown	意外終止後，服務管理員成功重新啓動。

名稱	描述
OutOfMemory	程式已向作業系統要求記憶體，不過沒有足夠的可用記憶體。
CREATE-DST-RULE-FILE-CLI	新的 DST 規則檔案會從 cli 產生。 需要重新啓動電話。不重新啓動電話將導致 DST 開始/停止日期錯誤。
CREATE-DST-RULE-FILE-BOOTUP	新的 DST 規則檔案會在啓動過程中產生。 需要重新啓動電話。不重新啓動電話將導致 DST 開始/停止日期錯誤。
CREATE-DST-RULE-FILE-CRON	新的 DST 規則檔案會從 cron 產生。 需要重新啓動電話。不重新啓動電話將導致 DST 開始/停止日期錯誤。
PermissionDenied	無法完成操作，因爲該程式無權執行。
ServiceNotInstalled	可執行檔案正在嘗試啓動，但是在服務控制管理員中未將其設定爲服務，因此無法啓動。 服務名稱爲 %s。
ServiceStopped	服務已停止。
ServiceStarted	服務已啓動。
ServiceStartupFailed	服務已啓動。
FileWriteError	無法寫入主要檔案路徑。

第 11 章

審計記錄檔

審計記錄檔

使用稽核記錄時，系統的組態變更會記錄在單獨的日誌檔中，以利稽核。

審計記錄 (標準)

啓用審計記錄檔但未選擇詳細審計記錄檔選項時，系統將設定爲標準審計記錄檔。

使用標準審計記錄檔時，系統的組態變更將記錄在單獨的記錄檔案中，以利審計。 顯示在服務能力 GUI 中控制中心 - 網路服務下的 Cisco Audit Event Service，能監視和記錄由使用者變更或因使用者操作而變更的任何系統組態。

您可以存取Serviceability GUI 中的**審計記錄檔組態**視窗，組態審計記錄檔的設定。

標準審計記錄檔包含以下幾個部分：

- 審計記錄檔框架 - 此框架包含一個 API，該 API 會使用警報庫將審計事件寫入審計記錄檔。 定義爲 GenericAlarmCatalog.xml 的警報目錄適用於這些警報。 不同的系統元件提供不同的記錄功能。

  以下範例顯示 Unified Communications Manager 元件可以用來傳送警報的 API：

```
User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3
EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
Successful Description: CallManager Service status is stopped
```

- 審計事件記錄 - 審計事件代表任何需要記錄的事件。 以下顯示審計事件的範例：

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

提示 請注意，審計事件記錄會集中處理且預設爲啓用。 名爲 Syslog Audit 的警報顯示器將寫入記錄檔。 預設情況下，記錄檔設定爲輪換。 若 AuditLogAlarmMonitor 無法寫入審計事件，AuditLogAlarmMonitor 會將此失敗視爲嚴重錯誤記錄在 syslog 檔案中。 警示管理員會連同 SeverityMatchFound 警示一同報告此錯誤。 即使事件記錄失敗，實際操作也會繼續進行。 在 Cisco Unified 即時監控工具中，所有審計記錄檔都可以從「追蹤和記錄檔中心」收集、檢視及刪除。

Cisco Unified Serviceability 標準事件記錄

Cisco Unified Serviceability會記錄以下事件：

- 啓動、停用、啓動或停止服務。
- 追蹤組態和警報組態變更。
- SNMP 組態變更。
- CDR 管理中的變更。 (僅適用於 Cisco Unified Communications Manager)
- 檢視Serviceability報告封存中的任何報告。 此記錄檔可在報告工具節點上檢視。 (僅適用於Unified Communications Manager)

Cisco Unified 即時監控工具標準事件記錄

Cisco Unified 即時監控工具會記錄以下事件，並加上審計事件警報：

- 警示組態
- 警示暫停
- 電子郵件組態
- 設定節點警示狀態
- 警示新增
- 新增警示動作
- 清除警示
- 啓用警示
- 移除警示動作
- 移除警示

Unified Communications Manager 標準事件記錄

Cisco CDR Analysis and Reporting (CAR) 會爲以下事件建立審計記錄檔：

- 載入程式排程
- 每日、每週和每月報告排程

- 郵件參數組態
- 撥號計劃組態
- 閘道組態
- 系統偏好設定組態
- 自動清除組態
- 評估引擎組態在某段期間、一日中某時、語音品質等方面的分數
- 服務品質組態
- 自動產生/警示預先產生的報告組態。
- 通知限制組態

Cisco Unified CM 管理標準事件記錄

系統會記錄 Cisco Unified Communications Manager 管理各個元件的以下事件：

- 使用者登入和登出
- 使用者角色成員資格更新 (新增使用者、刪除使用者、更新使用者角色)
- 角色更新 (新增、刪除或更新新角色)
- 裝置更新 (電話與閘道)
- 伺服器組態更新 (變更警報或追蹤組態、服務參數、企業參數、IP 位址、主機名稱、乙太網路設定及 Unified Communications Manager 伺服器新增或刪除)

Cisco Unified Communications Self Care Portal 標準事件記錄

記錄 Cisco Unified Communications Self Care Portal 的使用者登入和登出事件。

命令行介面標準事件記錄

記錄透過命令行介面發出的所有命令 (針對 Unified Communications Manager 和 Cisco Unity Connection)。

Cisco Unity Connection 管理標準事件記錄

Cisco Unity Connection 管理會記錄以下事件：

- 使用者登入和登出
- 所有組態變更，包括但不限於使用者、聯絡人、通話管理物件、網路、系統設定和電話
- 任務管理 (啓用或停用任務)
- 批量管理工具 (批量建立、批量刪除)
- 自訂鍵台對應 (對應更新)

Cisco Personal Communications Assistant (Cisco PCA) 標準事件記錄

Cisco Personal Communications Assistant 使用者端會記錄以下事件：

- 使用者登入和登出
- 透過 Messaging Assistant 變更的所有組態

Cisco Unity Connection Serviceability 標準事件記錄

Cisco Unity Connection Serviceability 會記錄以下事件：

- 使用者登入和登出
- 所有組態變更。
- 啓用、停用、啓動或停止服務。

使用代表狀態轉接 API 的 Cisco Unity Connection 使用者端事件記錄

使用代表狀態轉接 (REST) API 的 Cisco Unity Connection 使用者端會記錄以下事件：

- 使用者登入和登出 (使用者 API 驗證)。
- 使用 Cisco Unity Connection 佈建介面的 API 通話。

Cisco Unified IM and Presence Serviceability標準事件記錄

Cisco Unified IM and Presence Serviceability會記錄以下事件：

- 啓動、停用、啓動或停止服務。
- 追蹤組態和警報組態變更
- SNMP 組態變更
- 檢視Serviceability報告封存中任何報告 (這項記錄檔需在報告工具節點上檢視)

Cisco Unified IM and Presence 即時監控工具標準事件記錄

Cisco Unified IM and Presence 即時監控工具會記錄以下事件，並加上審計事件警報：

- 警示組態
- 警示暫停
- 電子郵件組態
- 設定節點警示狀態
- 警示新增
- 新增警示動作
- 清除警示

- 啓用警示
- 移除警示動作
- 移除警示

Cisco IM and Presence 管理標準事件記錄

系統會記錄 Cisco Unified Communications Manager IM and Presence 管理各個元件的以下事件：

- 管理員登入和登出 (登入和登出 IM and Presence 介面，如管理、作業系統管理、災害恢復系統和報告)
- 使用者角色成員資格更新 (新增使用者、刪除使用者、更新使用者角色)
- 角色更新 (新增、刪除或更新新角色)
- 裝置更新 (電話與閘道)
- 伺服器組態更新 (變更警報或追蹤組態、服務參數、企業參數、IP 位址、主機名稱、乙太網路設定及 IM and Presence 伺服器新增或刪除)

IM and Presence 應用程式標準事件記錄

系統會記錄 IM and Presence 應用程式各個元件的以下事件：

- 一般使用者登入和登出 IM 使用者端 (使用者登入、使用者登出和失敗的登入嘗試)
- 使用者進入和離開 IM 聊天室
- 建立和銷毀 IM 聊天室

命令行介面標準事件記錄

記錄所有透過命令行介面發出的命令。

審計記錄 (詳細)

詳細審計記錄檔是選用功能，用來記錄未儲存在標準 (預設) 審計記錄檔中的其他組態修改。 除了儲存在標準審計記錄檔中的所有資訊之外，詳細審計記錄檔還包括新增、更新和刪除的組態項目 (包括修改值)。 詳細審計記錄檔預設會停用，但是您可以在**審計記錄檔組態**視窗中予以啓用。

Audit Log Types

系統審計記錄檔

系統審計記錄檔會追蹤活動，例如建立、修改或刪除 Linux OS 使用者、篡改記錄檔，以及對檔案或目錄權限進行任何變更。 由於收集大量資料，因此預設爲停用這種類型的審計記錄檔。 若要啓用此功能，需使用 CLI 手動啓用 utils auditd。 在啓用系統審計記錄檔功能之後，可以透過即時監控工具

中的追蹤和記錄檔中心來收集、檢視、下載或刪除選擇的記錄檔。 系統審計記錄檔採用以下格式：`vos-audit.log`。

如需如何啓用此功能的相關資訊，請參閱 *Cisco Unified Communications* 解決方案的命令行介面參考指南。 如需如何從即時監控工具存取所收集記錄檔的相關資料，請參閱 *Cisco Unified* 即時監控工具管理指南。

應用程式審計記錄檔

應用程式審計記錄檔能監控及記錄由使用者所爲或因使用者操作而對系統產生的任何組態變更。

附註 應用程式審計記錄檔 (Linux auditd) 只能透過 CLI 啓用或停用。 除了透過即時監控工具收集 vos-audit.log 之外，您無法變更此類型審計記錄檔的任何設定。

資料庫審計記錄檔

資料庫審計記錄檔會追蹤與 Informix 資料庫存取相關聯的所有活動，例如登入。

審計記錄檔組態工作流程

完成以下工作以設定審計記錄。

程序

	命令或動作	目的
步驟 1	設定審計記錄 ，第 115 頁上的	在審計記錄組態視窗中設定審計記錄檔組態。 您可以設定是否要使用遠端審計記錄以及是否需要詳細審計記錄選項。
步驟 2	設定遠端審計記錄檔傳輸通訊協定 ，第 115 頁上的	選用。 若您設定了遠端審計記錄，請設定傳輸通訊協定。 正常操作模式下的系統預設值爲 UDP，但是您也可以設定 TCP 或 TLS
步驟 3	設定警示通知的電子郵件伺服器 ，第 116 頁上的	選用。 在 RTMT 中，設定電子郵件警示的電子郵件伺服器。
步驟 4	啓用電子郵件警示 ，第 116 頁上的	選用。 設定以下其中一個電子郵件警示： • 若您使用 TCP 設定了遠端審計記錄，請爲 **TCPRemoteSyslogDeliveryFailed** 警示設定電子郵件通知。 • 若您使用 TLS 設定了遠端審計記錄，請爲 **TLSRemoteSyslogDeliveryFailed** 警示設定電子郵件通知。

	命令或動作	目的
步驟 5	設定平台記錄的遠端審計記錄 ，第 117 頁上的	爲平台審計記錄和遠端伺服器記錄檔設定遠端審計記錄。 對於這些類型的審計記錄，需設定 FileBeat 使用者端和外部 Logstash 伺服器。

設定審計記錄

開始之前

遠端審計記錄而言，您需已經設定了遠端 Syslog 伺服器，並在每個叢集節點和遠端 Syslog 伺服器之間設定了 IPSec，包括到兩者之間任何閘道的連線。 有關 IPSec 組態，請參閱 *Cisco IOS* 安全性組態指南。

程序

步驟 1 在 Cisco Unified Serviceability中，選擇**工具** > **審計記錄組態**。

步驟 2 從**伺服器**下拉式功能表中，選擇叢集中的任何伺服器，然後按一下**執行**。

步驟 3 要記錄所有叢集節點，請勾選**套用至所有節點**方塊。

步驟 4 在**伺服器名稱**欄位中，輸入遠端 Syslog 伺服器的 IP 位址或完整網域名稱。

步驟 5 選用。 要記錄組態更新 (包括已修改的項目和已修改的值) ，請勾選**詳細審計記錄**方塊。

步驟 6 請完成**審計記錄檔組態**視窗中的其餘欄位。 如需有關欄位及其描述的詳細資訊，請參閱線上說明。

步驟 7 點擊**儲存**。

下一步

設定遠端審計記錄檔傳輸通訊協定 ，第 115 頁上的

設定遠端審計記錄檔傳輸通訊協定

使用此程式可以變更遠端審計記錄的傳輸通訊協定。 系統預設值爲 UDP，但您可以重新設定爲 TCP 或 TLS。

程序

步驟 1 登入命令行介面。

步驟 2 執行 **utils remotesyslog show protocol** 命令以確認設定了哪個通訊協定。

步驟 3 若需要變更此節點上的通訊協定，請執行以下作業：

- 要設定 TCP，請執行 **utils remotesyslog set protocol tcp** 命令。
- 要設定 UDP，請執行 **utils remotesyslog set protocol udp** 命令。

- 要設定 TLS，請執行 **utils remotesyslog set protocol tls** 命令。

  附註　在通用準則模式下，將實行嚴格的主機名稱驗證。 因此，需要使用與憑證相符的標準網域名稱 (FQDN) 組態伺服器。

步驟 4 若變更了通訊協定，請重新啓動節點。

步驟 5 在所有 Unified Communications Manager 和 IM and Presence Service 叢集節點上重複此過程。

下一步

設定警示通知的電子郵件伺服器 ，第 116 頁上的

設定警示通知的電子郵件伺服器

使用此流程設定您電子郵件伺服器的警示通知。

程序

步驟 1 在即時監控工具的系統視窗中，按一下**警示中心**。

步驟 2 選取**系統** > **工具** > **警示** > **設定電子郵件伺服器**。

步驟 3 在**郵件伺服器組態**快顯視窗中，輸入郵件伺服器的詳細資料。

步驟 4 點擊**確定**。

下一步

啓用電子郵件警示 ，第 116 頁上的

啟用電子郵件警示

若有設定 TCP 或 TLS 執行遠端審計記錄，請使用此程式設定電子郵件通知來通知您傳輸故障。

程序

步驟 1 在即時監控工動具**系統**區域中，按一下**警示中央**。

步驟 2 在**警示中央**視窗

- 若有使用 TCP 的遠端審計記錄，請選取 **TCPRemoteSyslogDeliveryFailed**
- 若有使用 TLS 的遠端審計記錄，請選取 **TLSRemoteSyslogDeliveryFailed**

步驟 3 選擇**系統** > **工具** > **警示** > **組態警示動作**。

步驟 4 在**警示動作**快顯視窗中，選取**預設**，並按一下**編輯**。

步驟 5 在**警示動作**快顯視窗中，**新增**收件者。

步驟 6 在快顯視窗中，輸入要傳送電子郵件警示的地址，然後按一下**確定**。

步驟 7 在**警示動作**快顯視窗中，請確定地址出現在**收件者**下方，且已勾選**啟用**方塊。

步驟 8 點擊**確定**。

設定平台記錄的遠端審計記錄

完成這些工作，以爲平台審計記錄、遠端支援記錄檔和批量管理 csv 檔案新增遠端審計記錄支援。對於這些類型的記錄檔，將使用 FileBeat 使用者端和 logstash 伺服器。

開始之前

確保已設定外部 Logstash 伺服器。

程序

	命令或動作	目的
步驟 1	設定 Logstash 伺服器資訊 ，第 117 頁上的	使用外部 Logstash 伺服器詳細資訊設定 FileBeat 使用者端，例如 IP 位址、連接埠和檔案類型。
步驟 2	設定 FileBeat 使用者端 ，第 117 頁上的	啓用 FileBeat 使用者端以進行遠端審計記錄。

設定 Logstash 伺服器資訊

使用此程式可使用外部 Logstash 伺服器資訊 (例如 IP 位址、連接埠號碼和可下載檔案類型) 設定 FileBeat 使用者端。

開始之前

確保已設定外部 Logstash 伺服器。

程序

步驟 1 登入命令行介面。

步驟 2 執行 **utils FileBeat configure** 命令。

步驟 3 按照提示設定 logstash 伺服器詳細資訊。

設定 FileBeat 使用者端

使用此程式可以啓用或停用 FileBeat 使用者端以上傳平台審計記錄檔、遠端支援記錄檔和批量管理 csv 檔案。

程序

步驟 1 登入命令行介面。

步驟 2 執行 **utils FileBeat status** 命令以確認是否啓用了 FileBeat 使用者端。

步驟 3 執行下列命令之一：

- 要啓用使用者端，請執行 **utils FileBeat enable** 命令。
- 要停用使用者端，請執行 **utils FileBeat disable** 命令。

附註　TCP 是預設的傳輸通訊協定。

步驟 4 選用。 若要使用 TLS 作爲傳輸通訊協定，請執行以下操作：

- 要啓用 TLS 作爲傳輸通訊協定，請執行 **utils FileBeat tls enable** 命令。
- 要停用 TLS 作爲傳輸通訊協定，請執行 **utils FileBeat tls disable** 命令。

附註　要使用 TLS，需將安全性憑證從 Logstash 伺服器上傳到 Unified Communications Manager 和 IM and Presence Service上的 tomcat 信任儲存中。

步驟 5 在各節點中重複此程式。

不要在所有節點上同時執行任何這些命令。

審計記錄檔組態設定

開始之前

請注意，只有具有審計角色的使用者才能變更審計記錄檔設定。 預設情況下 Unified Communications Manager 方面在全新的安裝和升級後，CCMAdministrator 擁有審計角色。 CCMAdministrator 可以將任何具有審計權限的使用者指派到 Cisco Unified Communications Manager 管理中「使用者群組組態」視窗的「標準審計使用者」群組。 若要這樣做，您可以將 CCMAdministrator 從「標準審計使用者」群組中移除 。

IM and Presence Service 而言，在全新安裝和升級後管理員將擁有審計角色，而且可以將任何具有審計權限的使用者指派到「標準審計使用者」群組。

Cisco Unity Connection而言，在安裝過程中建立的應用程式管理帳戶具有「審計管理員」角色，而且可以將其他管理使用者指派給該角色。 您也可以將「審計管理員」角色從該帳戶中移除。

「標準審計記錄檔組態」角色用於提供審計記錄檔刪除功能，以及讀取/更新以下各項目的存取權限：Cisco Unified 即時監控工具、IM and Presence 即時監控工具、追蹤收集工具、即時監控工具 (RTMT) 警示組態、Serviceability UI 中的控制中心 - 網路服務、RTMT 設定檔儲存、Serviceability UI 中的「審計組態」，以及稱爲審計追蹤的資源。

「標準審計記錄檔組態」角色用於提供審計記錄檔刪除功能，以及讀取/更新以下各項目的存取權限：Cisco Unified RTMT、追蹤收集工具、RTMT 警示組態、Cisco Unified Serviceability 中的控制中心 - 網路服務、RTMT 設定檔儲存、Cisco Unified Serviceability 中的「審計組態」，以及稱爲審計追蹤的資源。

Cisco Unity Connection 中的「審計管理員」角色提供在 Cisco Unified RTMT 中檢視、下載和刪除審計記錄檔的功能。

若要了解 Unified Communications Manager 中的角色、使用者和使用者群組，請參閱《*Cisco Unified Communications Manager* 管理指南》。

若要了解 Cisco Unity Connection 中的角色和使用者，請參閱《*Cisco Unity Connection* 的使用者移動、新增和變更指南》。

若要了解 IM and Presence 中的角色、使用者和使用者群組，請參閱《*IM and Presence Service*對 *Unified Communications Manager* 的設定與管理》。

下表描述可以在 Cisco Unified Serviceability「審計記錄檔組態」視窗中組態的設定。

表 *12:* 審計記錄檔組態設定

欄位	描述
選擇伺服器	
伺服器	選擇要設定審計記錄檔的目的地伺服器 (節點) ，然後按一下**執行**。
套用到所有節點	若要將審計記錄檔組態套用到叢集中的所有節點，請勾選**套用到所有節點**方塊。
應用程式審計記錄檔設定	
啓用審計記錄檔	勾選此方塊時，系統會爲應用程式審計記錄檔建立審計記錄檔。 Unified Communications Manager 而言，應用程式審計記錄檔支援 Unified Communications Manager 的 UI (如 Cisco Unified Communications Manager 管理) 的組態更新、Cisco Unified RTMT、Cisco Unified Communications Manager CDR 分析和回報 及Cisco Unified Serviceability。 IM and Presence Service而言，應用程式審計記錄檔支援 IM and Presence 的 UI (如 Cisco Unified Communications Manager IM and Presence 管理) 的組態更新、Cisco Unified IM and Presence RTMT和 Cisco Unified IM and Presence Serviceability。 Cisco Unity Connection 而言，應用程式審計記錄檔支援 Cisco Unity Connection UI 的組態更新，包括 Cisco Unity Connection 管理、Cisco Unity Connection Serviceability、Cisco Personal Communications Assistant 和使用 Connection REST API 的使用者端。 此設定預設會顯示爲已啓用。 **附註**　網路服務審計事件服務需處於執行中狀態。

欄位	描述
啓用清除	記錄檔分割顯示器(LPM)會查看「啓用清除」選項，以判斷是否需要清除審計記錄檔。 勾選此方塊時，只要共用分割硬碟使用率超過高水位標記，LPM 就會清除 RTMT 中的所有審計記錄檔案，不過您可以藉由取消勾選選擇方塊來停用清除。 若停用清除，審計記錄檔的數量將繼續增加，直到硬碟已滿。 此動作可能會導致系統中斷。 當您取消勾選「啓用清除」方塊時，系統將顯示訊息，描述停用清除的風險。 請注意，此選項可用於活躍的分區的審計記錄檔。 若審計記錄檔位於不活躍的分區，當硬碟使用率高於高水位標記時，系統將清除審計記錄檔。 您可以透過在 RTMT 中選擇**追蹤和記錄中心** > **審計記錄檔**來存取審計記錄檔。 **附註** 網路服務 Cisco Log Partitions Monitoring 工具需處於執行中狀態。
啓用記錄檔輪換	系統會讀取此選項來決定是否需要輪換審計記錄檔案還是要繼續建立新檔案。 檔案數目上限不能超過 5000。勾選「啓用輪換」方塊的情況下，在達到檔案數目上限後，系統會開始覆寫最舊的稽核日誌檔案。 **提示** 停用(未勾選)記錄檔輪換時，審計記錄檔將忽略「檔案數量上限」設定。
詳細審計記錄檔	勾選此方塊將啓用系統的詳細審計記錄檔。 詳細審計記錄檔提供的項目與一般審計記錄檔相同，不過還包括組態變更。 例如，審計記錄檔包括新增、更新和刪除的項目，包括修改後的值。
伺服器名稱	輸入要用於接受 syslog 訊息的遠端 syslog 伺服器名稱或 IP 位址。 若未指定伺服器名稱，Cisco Unified IM and Presence Serviceability 就不會傳送 syslog 訊息。 請勿將 Unified Communications Manager 節點指定爲目的地，因爲 Unified Communications Manager 不接受來自另一部伺服器的 syslog 訊息。 該做法僅適用於 IM and Presence Service。
遠端 Syslog 審計事件層級	爲遠端 syslog 伺服器選擇所需的 syslog 訊息嚴重性。 所有具有選定嚴重性層級或更高嚴重性層級的 syslog 訊息都會傳送到遠端 syslog。 該做法僅適用於 IM and Presence Service。
檔案數量上限	輸入記錄檔中包含的檔案數量上限。 預設設定指定 250。數目上限指定 5000。
檔案大小上限	輸入審計記錄檔的檔案大小上限。 檔案大小值需保持在 1 MB 到 10 MB 之間。 您需指定介於 1 到 10 之間的數值。

欄位	描述
接近記錄檔輪換覆寫的警示臨界值 (%)	當審計記錄檔接近即將遭到覆寫的程度時，系統可以提醒您。使用此欄位可以設定系統向您傳送警示的臨界值。 例如，若您使用 250 個 2 MB 檔案的預設設定和 80% 的警示臨界值，當審計記錄檔累積達 200 個檔案 (80%) 時，系統會向您傳送警報。若您想要保留審計歷程記錄，可以在系統覆寫記錄檔之前使用 RTMT 擷取記錄檔。RTMT 提供在收集檔案後刪除檔案的選項。 請輸入介於 1 到 99% 之間的值。預設值爲 80%。設定此欄位時，還需勾選**啟用記錄檔輪換**選項。 **附註** 分配給審計記錄檔的硬碟空間總數是最大檔案數乘以最大檔案大小。若硬碟上的審計記錄檔大小超過分配的硬碟空間總數百分比，系統會在警示中心發出警報。
資料庫審計記錄檔過濾器設定	
啓用審計記錄檔	勾選此方塊時，系統會爲 Unified Communications Manager 和 Cisco Unity Connection 資料庫建立審計記錄檔。請將此設定與「除錯審計層級」設定搭配使用，如此將能針對資料庫的某些方面建立記錄檔。
除錯審計層級	此設定允許您選擇要在記錄檔中審計資料庫的哪些方面。從下拉式清單方塊中，選擇下列其中一個選項。請注意，每個審計記錄檔過濾器層級都是累積的。 • **架構** - 追蹤對審計記錄檔資料庫設定所做的變更 (例如，資料庫表格中的列和行)。 • **行政工作** - 追蹤對 Unified Communications Manager 系統所做的所有管理變更 (例如，爲維護系統所做的任何變更)，再加上所有**架構**變更。 **提示** 大多數管理員保留「管理任務」設定的停用狀態。對於需要審計的使用者，請使用「資料庫更新」層級。 • **資料庫更新** - 追蹤對資料庫所做的所有變更，再加上所有**架構**變更和所有**管理工作**變更。 • **資料庫讀取** - 追蹤對系統的每次讀取，再加上所有架構變更、管理工作變更和資料庫更新變更。 **提示** 僅當您想快速查看 Unified Communications Manager、IM and Presence Service或 Cisco Unity Connection 系統時，才選擇「資料庫讀取」層級。此層級會佔用大量系統資源，因此只能在短時間內使用。
啓用審計記錄檔輪換	系統會讀取此選項來決定要輪換資料庫審計記錄檔案，還是要繼續建立新檔案。勾選「啓用審計輪換」選項方塊的情況下，在達到檔案數量上限之後，系統會開始覆寫最舊的審計記錄檔案。 取消勾選此設定方塊時，審計記錄檔會忽略「檔案數量上限」設定。

欄位	描述
檔案數量上限	輸入記錄檔中包含的檔案數量上限。請確認輸入的「檔案數量上限」設定值大於輸入的「記錄檔輪換時刪除的檔案數」設定值。 您可以輸入從 4 (最小) 到 40 (最大) 之間的數值。
記錄檔輪換時刪除的檔案數	輸入資料庫審計記錄檔輪換發生時系統可以刪除的檔案數量上限。 您可以在此欄位中輸入的最小值爲1。最大值比您輸入的「檔案數量上限」設定值小2。例如，若在「檔案數量上限」欄位中輸入40，可以在「記錄檔輪換時刪除的檔案數」欄位中輸入的最大數值爲 38。
設爲預設值	**設為預設值**按鈕能指定預設值。除非需要設定爲其他層級以進行詳細的疑難排解，否則建議您將審計記錄檔設定爲預設模式。**設為預設值**選項能大幅減少了記錄檔案佔用的硬碟空間。

注意 資料庫記錄啓用後可能會在短時間內產生大量資料，特別是若將除錯審計層級設定爲**資料庫更新**或**資料庫讀取**。在使用負荷繁重的期間內，這可能會嚴重影響效能。一般來說，我們建議您停用資料庫記錄。 若您需要啓用記錄功能來追蹤資料庫中的變更，我們只建議您在短時間內使用**資料庫更新**層級。 同樣，管理記錄確實會影響 Web UI 的整體效能，尤其是在輪詢資料庫項目時 (例如，從資料庫提取 250 部裝置)。

第 12 章

Call Home

Call Home

本章提供 Unified Communications Manager Call Home 服務的一個概觀，並說明如何配置 Unified Communications Manager Call Home 功能。 Call Home 功能允許通訊，並將診斷警示、庫存和其他訊息傳送到 Smart Call Home 後端伺服器。

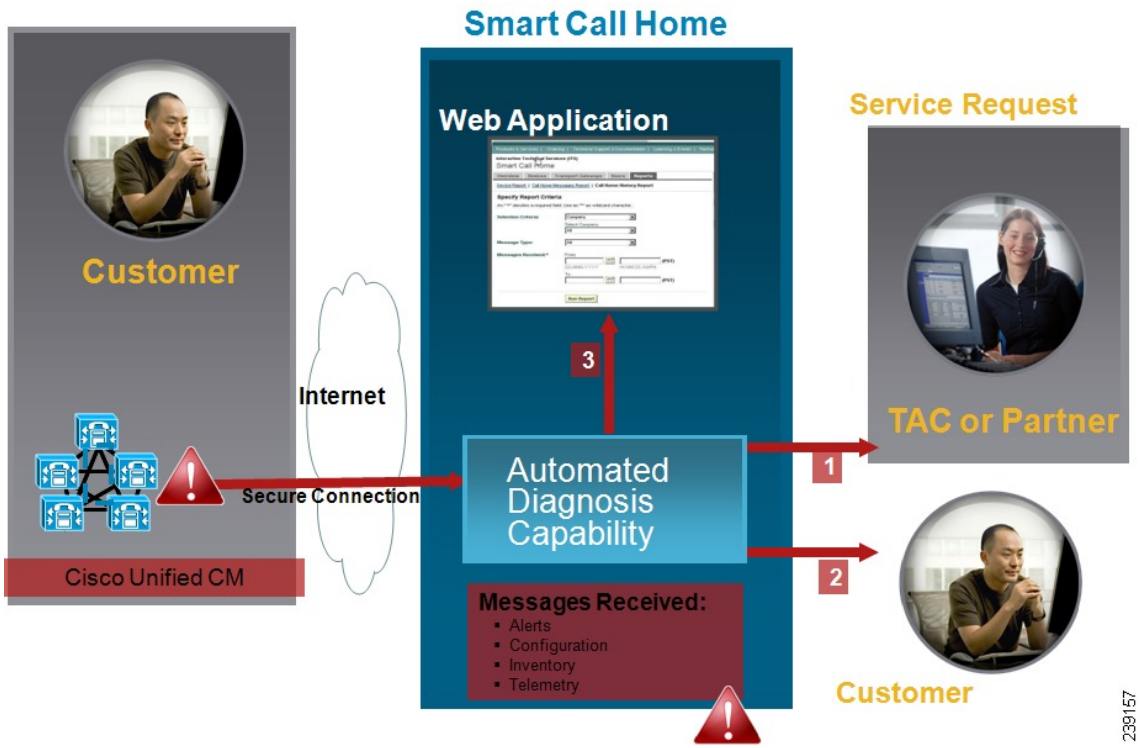
Smart Call Home

Smart Call Home 可在一系列 Cisco 裝置上提供主動診斷，即時警報和修復，以提高網路可用性及營運效率。 它從啓用了 Smart Call Home 的 Unified Communications Manager 接收和分析診斷警報、清單和其他訊息來完成此工作。 Unified Communications Manager 的這種特殊功能名爲 Unified Communications Manager Call Home。

Smart Call Home

- 透過以下方式主動且快速解決問題，從而提高網路可用性：
  - 透過連續監控、即時、主動警報和詳細診斷以快速識別問題。
  - 透過提供僅針對網路中特定類型的裝置警報，讓您意識到潛在的問題。 透過直接、自動與 Cisco 技術協助中心 (TAC) 的專家聯繫，可以更快地解決關鍵問題。
- 透過爲客戶提供以下能力來提高營運效率：
  - 透過減少疑難排解時間，更有效地使用員工資源。
- 針對所需資訊提供快速的網頁型存取，使客戶能夠：
  - 在一處檢閱所有通話訊息、診斷和建議。
  - 快速檢查服務請求狀態。
  - 檢視所有 Call Home 裝置的最新清單和組態資訊。

圖 *2: Cisco Smart Call Home* 概觀



Smart Call Home 包含執行以下工作的模組：

- 通知客戶 Call Home 訊息。
- 提供影響分析和補救步驟。

有關 Smart Call Home 的更多資訊，請參閱以下位置的 Smart Call Home 頁面：

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Smart Call Home 憑證更新資訊

從 Cisco 版本 10.5(2) 開始，管理員需爲任何更新請求手動上傳新憑證，以繼續支援 Smart Call Home 功能。 您可以透過 Cisco Unified Operating System 管理 Web GUI 上傳憑證。 前往**安全性 > 憑證管理 > 上傳憑證/憑證串鍊憑證鏈**。 選擇 **tomcat-trust** 作爲憑證用途，然後從儲存的目的地上傳憑證。

以下副檔名爲 .PEM 的憑證應上傳到 tomcat-trust。

附註 確保管理員複製整個字串，並包括 ----- BEGIN CERTIFICATE ----- 和 ----- END CERTIFICATE -----，將其貼到文字檔中，並使用副檔名儲存 .PEM。

-----BEGIN CERTIFICATE-----

MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x

GTAXBgNVBAoTEF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv

b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR
TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----

Anonymous Call Home

Anonymous Call Home 功能是 Smart Call Home 功能的子功能，該功能使 Cisco 可以匿名接收清查和遙測訊息。 啓用此功能可以讓您保持匿名身分。

以下是 Anonymous Call Home 的特性：

- Unified Communications Manager 只會將清查和遙測訊息傳送到 Smart Call Home 後端，不會傳送診斷和組態資訊。
- 它不會傳送任何與使用者相關的資訊 (例如，註冊的裝置和升級歷程記錄)。
- Anonymous Call Home 選項不需要向 Cisco 註冊 Smart Call Home 功能或取得授權。
- 清查和遙測訊息會定期 (每個月的第一天) 傳送到 Call Home 後端。
- 若將 Cisco Unified Communications Manager 設定爲使用 Anonymous Call Home，則**包括追蹤記錄檔和診斷資訊**選項會停用。

清查訊息包含有關叢集、節點和授權的資訊。

下表列出 Smart Call Home 和 Anonymous Call Home 的清查訊息。

表 *13: Smart Call Home* 和 *Anonymous Call Home* 的清查訊息

清查訊息	Smart Call Home	Anonymous Call Home
聯絡人電子郵件	適用	不適用
聯絡人電話號碼	適用	不適用
街道地址	適用	不適用
伺服器名稱	適用	不適用
伺服器 IP 位址	適用	不適用
授權伺服器	適用	不適用
作業系統版本	適用	適用
機型	適用	適用
序號	適用	適用
CPU 速度	適用	適用
RAM	適用	適用
儲存分割	適用	適用
韌體版本	適用	適用
BIOS 版本	適用	適用
BIOS 資訊	適用	適用
Raid 組態	適用	適用
活躍的服務	適用	適用

清查訊息	Smart Call Home	Anonymous Call Home
發佈者名稱	適用	不適用
發佈者 IP	適用	不適用
產品 ID	適用	適用
活躍的版本	適用	適用
不活躍的版本	適用	適用
產品簡稱	適用	適用

遙測訊息包含有關 Unified Communications Manager 叢集上可用之各種裝置類型的裝置數量 (IP 電話、閘道、會議橋接器等) 的資訊。 遙測資料包含整個叢集的裝置計數。

下表列出 Smart Call Home 和 Anonymous Call Home 的遙測訊息。

表 *14: Smart Call Home* 和 *Anonymous Call Home* 的遙測訊息

遙測會議	Smart Call Home	Anonymous Call Home
聯絡人電子郵件	適用	不適用
聯絡人電話號碼	適用	不適用
街道地址	適用	不適用
伺服器名稱	適用	不適用
CM 使用者人數	適用	不適用
序號	適用	適用
發佈者名稱	適用	不適用
裝置數量和型號	適用	適用
電話使用者人數	適用	適用
CM 通話活動	適用	適用
註冊裝置數	適用	不適用
升級記錄	適用	不適用
系統狀態	適用於主機名稱、日期、區域設定、產品版本、作業系統版本、授權 MAC、正常運作時間、MP Stat、已用記憶體、硬碟使用量、使用的作用中和停用分割及 DNS	適用於日期、區域設定、產品版本、作業系統版本、授權 MAC、正常運作時間、已用記憶體、硬碟使用量及使用的作用中和停用分割

組態訊息包含的資訊與每個涉及組態之資料庫表格的列數相關。 組態資料由整個叢集中每個表格的表格名稱和列數組成。

Smart Call Home 互動

若您直接與 Cisco Systems 簽訂了服務合約，則可以爲 Cisco Smart Call Home 服務註冊 Unified Communications Manager。 Smart Call Home 透過分析從 Unified Communications Manager 傳送的 Call Home 訊息並提供背景資訊和建議，可以快速解決系統問題。

Unified Communications Manager 的 Call Home 功能將以下訊息傳遞到 Smart Call Home 後端伺服器：

- 警示 - 包含與環境、硬體故障和系統效能有關的各種的警示資訊。 警示可以從 Unified Communications Manager 叢集內的任何節點產生。 警示詳細資訊包含節點和進行疑難排解所需的其他資訊，具體取決於警示類型。 請參閱與 Smart Call Home 互動有關的主題，以取得傳送到 Smart Call Home 後端伺服器的警示。

以下是 Smart Call Home 的警示。

預設情況下，Smart Call Home 每 24 小時處理一次警示。 在混合叢集 (Unified Communication Manager 和 Cisco Unified Presence) 中的 24 小時內重複出現同一警示，Smart Call Home 不會對其進行處理。

重要須知 48 年後，收集的資訊將從主 AMC 伺服器中刪除。 預設情況下，Unified Communications Manager 發佈者是主要 AMC 伺服器。

- **效能警示**
  - CallProcessingNodeCPUPegging
  - CodeYellow
  - CPUPegging
  - LowActivePartitionAvailableDiskSpace
  - LowAvailableVirtualMemory
  - LowSwapPartitionAvailableDiskSpace
- **資料庫 - 相關警示**
  - DBReplicationFailure
- **通話失敗警示**
  - MediaListExhausted
  - RouteListExhausted
- **當機 - 相關警示**
  - Coredumpfilefound

- CriticalServiceDown

組態、清查和遙測訊息會定期 (每個月的第一天) 傳送到 Call Home 後端。 這些訊息中的資訊讓 TAC 能夠提供及時和主動的服務，以幫助客戶管理和維護其網路。

Call Home 的必需條件

若要支援 Unified Communications Manager Call Home 服務，您需要以下各項：

- 與相對應的 Unified Communications Manager 服務合約相關聯的 Cisco.com 使用者 ID。
- 強烈建議同時爲 Unified Communications Manager Call Home 功能設定網域名稱系統 (DNS) 和簡易郵件傳輸通訊協定 (SMTP) 伺服器。
  - 需要進行 DNS 設定，才能使用安全網路 (HTTPS) 傳送 Call Home 訊息。
  - 需要進行 SMTP 設定，才能將 Call Home 訊息傳送到 Cisco TAC，或透過電子郵件將訊息的副本傳送到收件人清單。

存取 Call Home

若要存取 Unified Communications Manager Call Home，請移至 Cisco Unified Serviceability管理，並選擇 **CallHome** (**Cisco Unified Serviceability** > **CallHome** > **Call Home** 組態)。

Call Home 設定

下表列出預設 Unified Communications Manager Call Home 設定。

表 *15:* 預設 *Call Home* 設定

參數	預設值
Call Home	已啓用
使用指定方式將資料傳送給 Cisco Technical Assistance Center (TAC)	安全 Web (HTTPS)

若在安裝期間變更預設的 Smart Call Home 組態，相同的設定會反映在「Call Home」UI 中。

附註 若您選擇**電子郵件**傳輸方式，而且 SMTP 設定不是**安全網路 (HTTPS)** 選項的必要項目，就需具備 SMTP 設定。

Call Home 組態

在 Cisco Unified Serviceability中，選擇**Call Home** > **Call Home** 組態。

「Call Home 組態」視窗隨即會顯示。

附註　您還可以在安裝 Unified Communications Manager 時設定 Cisco Smart Call Home。

若在安裝期間設定 Smart Call Home 選項，Smart Call Home 功能將會啓用。 若您選擇**無**，在登入 Cisco Unified Communications Manager 管理時，系統會顯示一則提醒訊息。 我們準備了使用 Cisco Unified Serviceability 配置 Smart Call Home 或停用提醒的指示。

下表說明設定 Unified Communications Manager Call Home 時的設定。

表 *16: Unified Communications Manager Call Home* 組態設定

欄位名稱	描述
Call Home 訊息排程	顯示最後傳送Call Home訊息和下一則排定訊息的日期和時間。
Call Home*	在此下拉式清單中選擇下列其中一個選項： • **無**： 若您想要啓用或停用 Call Home，請選擇此選項。 管理員頁面會出現一則提醒訊息：`Smart Call Home 尚未設定。 若要設定 Smart Call Home 或停用提醒，請移至 Cisco Unified Serviceability> Call Home，或按一下此處。` • **停用**：若您想要停用 Call Home，請選擇此選項。 • **啟用 (Smart Call Home)**：若您在安裝期間選擇 Smart Call Home，此選項會啓用。 選擇此選項時，**客戶聯絡人詳細資料**下的所有欄位均會啓用。 採用相同組態的情況下，**傳送資料**選項也會啓用。 • **啟用 (Anonymous Call Home)**：若您想要在匿名模式下使用 Call Home，請選擇此選項。 選擇此選項時，**客戶聯絡人詳細資料**下的所有欄位均會停用。 採用相同組態的情況下，**傳送資料**中的「將副本傳送到以下電子郵件地址(用逗號分隔多個地址)」欄位會啓用，而且「Call Home」頁面中的「包括追蹤記錄檔和診斷資訊」會停用。 附註　若啓用 Anonymous Call Home，伺服器會將使用統計資料從伺服器傳送到 Cisco 系統。 這些資訊有助於 Cisco 了解有關產品的使用者體驗，以及推動產品發展方向。
客戶聯絡人詳細資料	
電子郵件地址*	輸入客戶的聯絡人電子郵件地址。 此爲必填欄位。
公司	(選填) 輸入公司名稱。 您最多可以輸入 255 個字元。

欄位名稱	描述
聯絡人姓名	(選填) 輸入客戶的聯絡人姓名。 您最多可以輸入 128 個字元。 聯絡人姓名可以包含英數字元和一些特殊字元，如點 (.)、底線 (_) 和連字型大小 (-)。
地址	(選填) 輸入客戶的地址。 您最多可以輸入 1024 個字元。
電話	(選填) 輸入客戶的電話號碼。
傳送資料	
使用指定方式將資料傳送給 Cisco Technical Assistance Center (TAC)	這是必填欄位。 從下拉式清單中，選擇下列其中一個選項將 Call Home 訊息傳送給 Cisco TAC： • **安全網路 (HTTPS)**：若要使用安全網路將資料傳送到 Cisco TAC，請選擇此選項。 • **電子郵件**：若要使用電子郵件將資料傳送到 Cisco TAC，請選擇此選項。 對於電子郵件，SMTP 伺服器需設定。 您可以看到已配置的 SMTP 伺服器主機名稱或 IP 位址。 附註 若您尚未配置 SMTP 伺服器，有一則警示訊息會出現。 • **透過代理的安全網路 (HTTPS)**：若要透過代理將資料傳送到 Cisco TAC，請選擇此選項。 目前，我們不支援代理層級的驗證。 設定此選項時會出現以下欄位： • **HTTPS 代理 IP/主機名稱***：輸入代理 IP/主機名稱。 • **HTTPS 代理連接埠***：輸入要通訊的代理連接埠號碼。
將副本傳送到以下電子郵件地址 (用逗號分隔多個地址)	勾選此方塊可將 Call Home 訊息的副本傳送到指定電子郵件地址。 您最多可以輸入 1024 個字元。
包括追蹤記錄檔和診斷資訊	勾選此方塊以啓動 Unified Communications Manager 來收集記錄檔和診斷資訊。 附註 唯有啓用 Smart Call Home 後，此選項才會處於作用狀態。 訊息包含警示產生時收集的診斷資訊以及追蹤訊息。若追蹤大小小於 3 MB，系統會將追蹤編碼並連同警示訊息一起傳送；若追蹤大於 3 MB，系統會將追蹤位置的路徑顯示在警示訊息中。

欄位名稱	描述
儲存	儲存 Call Home 組態。 **附註** 儲存 Call Home 組態後，使用者授權合約 (EULA) 訊息將會出現。 若是首次設定，您需接受授權合約。 **提示** 若要停用您啓動的 Call Home 服務，請從下拉式清單選擇**停用**選項，然後按一下**儲存**。
重設	重設爲上次儲存的組態。
儲存並立即 Call Home	儲存及傳送 Call Home 訊息。 **附註** 若訊息傳送成功，會出現一則 **Call Home 組態已儲存，而且所有 Call Home 訊息已成功傳送**訊息。

侷限

當 Unified Communications Manager 或 Cisco Unified Presence 伺服器關閉或無法連線時，適用下列限制：

- Smart Call Home 無法擷取上次傳送 Call Home 訊息和下次排定訊息的日期和時間。
- 在伺服器可以連線之前，Smart Call Home 不會傳送 Call Home 訊息。
- 當發佈者關閉時，Smart Call Home 將無法擷取庫存郵件的授權資訊。

以下限制由於警示管理員和收集器 (AMC) 所致：

- 若節點 A 上發生警示，並且主要 AMC 伺服器 (預設爲發佈者) 重新啓動，以及若同一節點在 24 小時內發生同一警示，則 Smart Call Home 會從節點 A 重新傳送警示資料。由於主要 AMC 已重新啓動，因此 Smart Call Home 無法識別已發生的警示。
- 若節點 A 上發生警示，並且您將主要 AMC 伺服器變更爲另一個節點，以及若同一節點在 24 小時內發生同一警示，則 Smart Call Home 會將其識別爲節點 A 上的全新警示，並傳送警示資料。
- 在少數案例下，主要 AMC 伺服器上收集的追蹤可能在主要 AMC 伺服器上駐留最多 60 小時。

以下是混合叢集 (Unified Communications Manager 和 IM and Presence) 案例中的限制：

- 像是 **CallProcessingNodeCpuPegging**、**媒體清單已用盡**、**路由清單已用盡**不適用於 IM and Presence。
- 若使用者將主要 AMC 伺服器變更爲 IM and Presence，則 Smart Call Home 無法爲**媒體清單已用盡**和**路由清單已用盡**產生叢集概觀報告。
- 若使用者將主要 AMC 伺服器變更爲 IM and Presence，則 Smart Call Home 無法爲**資料庫複寫**警示產生概觀報告。

Call Home 參考資料

如需 Smart Call Home 的詳細資訊，請參閱以下 URL：

- Smart Call Home 服務介紹

  http://www.cisco.com/en/US/products/ps7334/serv_home.html

第 13 章

Serviceability Connector

Serviceability Connector概覽

您可以使用 Webex Serviceability 服務簡化記錄檔的收集。 該服務可自動執行尋找、擷取和儲存診斷記錄和資料的任務。

此功能使用部署於您公司處所中的*Serviceability Connector*。 Serviceability Connector是在網路專用主機（連接器主機）上執行的軟體， 您可以在以下任何一個組件上安裝連接器：

- 企業計算平台（ECP）- 推薦

  ECP 使用 Docker 容器隔離、保護和管理其服務。 主機和 Serviceability Connector應用程式是自雲端安裝的。 您無需手動將其升級即可保持其更新狀態和安全狀態。

重要須知 我們建議使用 ECP。 我們未來的發展將集中在這個平台上。 如果您在 Expressway 上安裝 Serviceability Connector，某些新功能將無法使用。

- Cisco Expressway

您可以將可 Serviceability Connector 用於以下目的：

- 服務請求的自動記錄和系統資訊擷取
- Cloud-Connected UC 部署中 Unified CM 叢集的記錄檔收集

您可在這兩個用例使用相同的 Serviceability Connector。

使用 Serviceability 服務的好處

該服務具有下列的優點：

- 加快記錄檔收集速度。 TAC 工程師在執行問題診斷時可以擷取相關記錄檔。 他們可以避免請求額外記錄檔和等待手動收集和交付的延遲。 這種自動化可能會使您的問題解決時間減少個幾天。
- 與 TAC 的協作解決方案分析器及其診斷簽署資料庫一起使用。 系統會自動分析記錄檔，識別已知問題，並推薦已知的修復或解決方法。

與其他混合服務的差異

您可使用 Control Hub 像其他基於 Expressway 的混合服務一樣部署和管理 Serviceability Connector，如混合行事曆服務和混合通話服務等等， 其中有一些重要的差異：

該服務無使用者的功能。 TAC 爲該服務的主要使用者。 它可讓使用其他混合服務的組織受益，不使用其他混合服務的組織則爲服務的一般使用者。

若您已經在 Control Hub 中配置了組織，則可透過現有的組織管理員帳號啓用該服務。

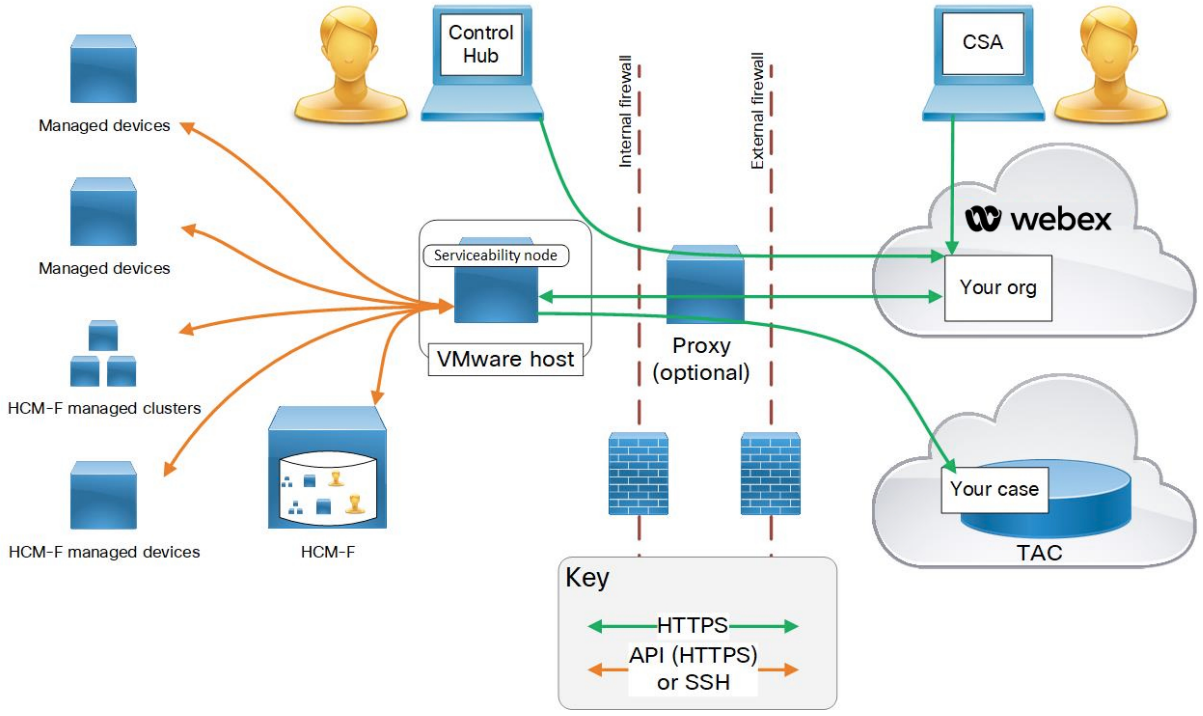
Serviceability Connector與直接向使用者提供功能的連接器具有不同的負載配置檔。 該連接器始終可用，因此 TAC 可以在必要時收集資料。 但隨時間的推移，其無穩定的負載。 TAC 代表手動啓動資料收集。 他們協商適當的收集時間，以最大程度地減少對同一基礎結構所提供的其他服務的影響。

Serviceability Connector運作方式的簡述

1. 您的管理員與 Cisco TAC 一起部署Serviceability 服務。 請參閱TAC 個案的部署架構 ，第 137 頁上的。
2. TAC 得知您的一台 Cisco 裝置有問題（開啓機箱時））。
3. TAC 代表使用協作解決方案分析器（CSA）Web 介面來請求 Serviceability Connector 自相關裝置收集資料。
4. 您的Serviceability連接器將請求轉換爲 API 命令以自受管理的裝置收集所請求的資料。
5. 您的Serviceability連接器透過加密連結收集、加密和上載資料，並將其上載到客戶體驗硬碟（CXD）然後再將該資料與您的服務請求建立關聯。
6. 將根據超過 1000 個診斷簽署的 TAC 資料庫對資料進行分析。
7. TAC 代表檢查結果，並在必要時檢查原始記錄檔。

TAC 個案的部署架構

圖 *3:* 在 ***Expressway*** 上使用 ***Service Connector*** 進行部署



元素	描述
受管理裝置	包括要向 Serviceability 服務提供記錄檔的任何裝置。 使用單一 Serviceability Connector 您可以新增達 150 個本地管理的裝置。 您可以從 HCM-F（託管協作中介實現）中匯入有關 HCS 客戶的受管裝置和叢集（具有更多裝置的資訊），請參閱https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Service）。 該伺服當前可與下列裝置一起使用： • 託管協作中介實現（HCM-F） • Cisco Unified Communications Manager • Cisco Unified CM IM and Presence Service • Cisco Expressway 系列 • Cisco TelePresence Video Communication Server (VCS) • Cisco Unified Contact Center Express （UCCX） • Cisco Unified Border Element （CUBE） • Cisco BroadWorks 應用程式伺服器（AS） • Cisco BroadWorks 配置檔案伺服器（PS） • Cisco BroadWorks 訊息伺服器（UMS） • Cisco BroadWorks 執行伺服器（XS） • Cisco Broadworks Xtended 服務平台（XSP）
您的管理員	使用 Cisco Webex Control Hub 註冊連接器主機並啓用「Serviceability 服務」。 該網址爲https://admin.webex.com而您需要您的“組織管理員”憑證。
連接器主機	承載管理連接器和 Serviceability Connector的企業計算平台（ECP）或 Expressway。 • ECP 或 Expressway 上的**管理連接器**和 Webex 中相對應的管理服務會管理您的註冊，保持連線不中斷，在需要時更新連接器，並回報狀態和警報。 • **Serviceability 連接器**-爲貴組織啓用 Serviceability 服務後，連接器主機（ECP 或 Expressway）會自 Webex 下載的一個小型應用程式。
Proxy	（可任選）若在啓動 Serviceability Connector 之後更改Proxy組態，則您亦需重新啓動 Serviceability Connector。
Webex 雲端	承載 Webex、Webex Calling、Webex Meetings 和 Webex Hybrid Services。

元素	描述
技術協助中心 (TAC)	包含： • TAC 代表使用 CSA 透過 Webex Cloud與您的 Serviceability Connector 進行通訊。 • TAC 個案管理系統，其中包含您的個案以及 Serviceability Connector 收集並上載到 Customer eXperience Drive 的相關記錄檔。

Serviceability Connector的 TAC 支援

有關Serviceability連接器的更多詳細資訊，請參閱https://www.cisco.com/go/serviceability或聯繫您的 TAC 代表。

第 14 章

簡易網路管理通訊協定

簡易網路管理通訊協定支援

SNMP (應用程式層通訊協定) 可協助在網路裝置 (例如節點和路由器) 之間交換管理資訊， 作爲 TCP/IP 套件的一部分，SNMP 可讓管理員遠端管理網路效能、尋找及解決網路問題，以及計畫網路成長。

您可以使用Serviceability GUI 來設定 SNMP 關聯設定，例如 V1、V2c 和 V3 的社區字串、使用者和通知目的地。 您設定的 SNMP 設定適用於本機節點。不過，若您的系統組態支援叢集，則您可以使用 SNMP 組態視窗中的“套用到所有節點”選項，將設定套用到叢集中的所有伺服器。

提示 僅限 Unified Communications Manager：您在 Cisco Unified CallManager 或 Unified Communications Manager 4.X 中指定的 SNMP 組態參數，在 Unified Communications Manager 6.0 及更新版本升級期間不會移轉。 您需在 Cisco Unified Serviceability中再次執行 SNMP 組態程式。

SNMP 支援 IPv4 和 IPv6，CISCO-CCM-MIB 包括 IPv4 和 IPv6 位址、偏好設定等等的欄和儲存空間。

SNMP 基本原理

SNMP 管理的網路包括三個關鍵元件：受管理裝置、代理和網路管理系統。

- 受管理裝置 - 包含 SNMP 代理並位於受管理網路上的網路節點。 受管理裝置會收集並儲存管理資訊，並透過使用 SNMP 使其可用。

  僅限 Unified Communications Manager 和 IM and Presence Service：在支援叢集的組態中，叢集中的第一個節點會充當受管理裝置。

- 代理 - 位於受管理裝置的網路受管理軟體模組。 代理包含管理資訊的本機知識，並將其轉換爲與 SNMP 相容的形式。

  主要代理和子代理元件用來支援 SNMP。 主要代理充當代理通訊協定引擎，並執行與 SNMP 請求相關的驗證、授權、存取控制和隱私功能。 同樣地，主要代理包含一些與MIB-II相關的管理資訊庫 (MIB) 變數。 在子代理完成必要的任務之後，主要代理也會連接和中斷連接子代理。 SNMP 主要代理接聽連接埠 161，並轉移廠商 MIB 的 SNMP 封包。

  Unified Communications Manager 子代理僅與本機 Unified Communications Manager 互動。 Unified Communications Manager 子代理會將陷阱和資訊訊息傳送到 SNMP 主要代理，並且 SNMP 主要代理會與 SNMP 陷阱接收器 (通知目的地) 進行通訊。

  IM and Presence Service子代理僅與本機 IM and Presence Service互動。 IM and Presence Service子代理會將陷阱和資訊訊息傳送到 SNMP 主要代理，並且 SNMP 主要代理會與 SNMP 陷阱接收器 (通知目的地) 進行通訊。

- 網路管理系統 (NMS) - SNMP 管理應用程式 (連同其執行所在的電腦) ，提供網路管理所需的大量處理和記憶體資源。 NMS 執行監控和控制受管理裝置的應用程式。 支援以下 NMS：
  - CiscoWorks LAN 管理解決方案
  - HP OpenView
  - 支援 SNMP 和 Unified Communications Manager SNMP 介面的第三方應用程式

SNMP 管理資訊庫

SNMP 允許存取管理資訊庫 (MIB)，該資訊庫是以階層式方式組織的資訊集合。 MIB 包含管理物件對象，這些物件由物件識別符識別。 包含管理裝置特定特徵的MIB物件包含一或多個物件執行個體 (變數)。

SNMP 介面提供下列 Cisco 標準 MIB：

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

請注意下列事項：

- Unified Communications Manager 不支援 CISCO-UNITY-MIB。
- Cisco Unity Connection 不支援 CISCO-CCM-MIB。
- IM and Presence Service 不支援 CISCO-CCM-MIB 和 CISCO-UNITY-MIB。

SNM分機代理駐留在伺服器中，並公開CISCO-CCM-MIB，它提供了有關伺服器已知裝置的詳細資訊。 對於叢集組態，SNMP 分機代理駐留在叢集的每個伺服器中。 CISCO-CCM-MIB 提供裝置資訊，例如裝置註冊狀態、IP 地址、說明和伺服器 (不是叢集，位於支援叢集的組態) 型號類型。

SNMP 介面還提供以下產業標準 MIB：

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

使用 CDP 子代理讀取 Cisco Discovery Protocol MIB、CISCO-CDP-MIB。 此 MIB 會讓 SNMP 管理裝置將自己公告給網路上的其他 Cisco 裝置。

CDP 子代理實作 CDP-MIB。 CDP-MIB 包含以下物件：

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

附註 CISCO-CDP-MIB 取決於以下 MIB 的存在：CISCO-SMI、CISCO-TC、CISCO-VTP-MIB。

SYSAPPL-MIB

使用系統應用程式代理從 SYSAPPL-MIB 取得資訊，例如已安裝的應用程式、應用程式元件和系統上正在執行的程式。

系統應用程式代理支援以下 SYSAPPL-MIB 物件群組：

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt

- sysApplElmtRun

表 *17: SYSAPPL-MIB* 命令

命令	說明
裝置相關查詢	
sysApplInstallPkgVersion	提供軟體製造商指派給應用程式套件的版本號碼。
sysApplElmPastRunUser	提供程式所有者的登入名稱(例如root)。
記憶體、儲存空間和與 CPU 相關的查詢	
sysApplElmPastRunMemory	提供以 KB 爲單位的最後已知的實際系統記憶體總量，該記憶體在終止之前分配給該程式。
sysApplElmtPastRunCPU	提供此程式耗用的總系統 CPU 資源的最後已知釐秒數 (以釐秒爲單位)。 **附註** 在多處理器系統上，該值可能會在實際(時鐘)時間的一釐秒中增加超過一釐秒。
sysApplInstallElmtCurSizeLow	提供以 2 ^ 32 位元組模數的目前檔案大小。 例如，對於一個檔案總大小爲 4,294,967,296 位元組的檔案，此變數的值爲 0；否則，該變數的值爲 0。對於檔案總大小爲 4,294,967,295 位元組的檔案，此變數爲 4,294,967,295。
sysApplInstallElmtSizeLow	提供以 2 ^ 32 位元組爲模數的已安裝檔案大小。 這是安裝後檔案在硬碟上的立即大小。 例如，對於一個檔案總大小爲 4,294,967,296 位元組的檔案，此變數的值爲 0；否則，該變數的值爲 0。對於檔案總大小爲 4,294,967,295 位元組的檔案，此變數爲 4,294,967,295。
sysApplElmRunMemory	提供以 KB 爲單位的實際系統記憶體總量，該記憶體目前分配給該程式。
sysApplElmRunCPU	提供此程式耗用的總系統 CPU 資源的釐秒數 (以釐秒爲單位)。 **附註** 在多處理器系統上，該值可能會在實際(時鐘)時間的一釐秒中增加超過一釐秒。
程式相關查詢	

sysApplElmtRunState	提供正在執行的程式目前狀態。 可能的值是正在執行(1)、可執行(2)，但在等待資源，例如CPU、正在等待(3)事件、結束(4) 或其他(5)。
sysApplElmtRunNumFiles	提供該程式月前開啓的一般檔案數。 傳輸連線 (通訊端) 不應包括在此值的計算中，也不包括特定作業系統的特殊檔案類型。
sysApplElmtRunTimeStarted	提供程式啓動的時間。
sysApplElmtRunMemory	提供以 KB 爲單位的實際系統記憶體總量，該記憶體目前分配給該程式。
sysApplElmtPastRunInstallID	提供已安裝元素表的索引。 該物件的值與 sysApplInstallElmtIndex 的值相同，該物件的應用程式元素的此項目表示先前執行的程式。
sysApplElmtPastRunUser	提供程式所有者的登入名稱(例如root)。
sysApplElmtPastRunTimeEnded	提供程式結束的時間。
sysApplElmtRunUser	提供程式所有者的登入名稱(例如root)。
sysApplRunStarted	提供啓動應用程式的日期和時間。
sysApplElmtRunCPU	提供此程式耗用的總系統 CPU 資源的釐秒數 (以釐秒爲單位)。 附註 在多處理器系統上，該值可能會在實際(時鐘)時間的一釐秒中增加超過一釐秒。
與軟體元件相關的查詢	
sysApplInstallPkgProductName	提供製造商指派給軟體應用程式套件的名稱。
sysApplElmtRunParameters	提供該程式的啓動參數。
sysApplElmtRunName	提供程式的完整路徑和檔案名。 例如，對於執行路徑爲「opt/MYYpkg/bin/myyproc」的程式「myyproc」，將傳回「/opt/MYYpkg/bin/myyproc」。
sysApplInstallElmtName	提供此元素的名稱，該名稱包含在應用程式中。
sysApplElmtRunUser	提供程式所有者的登入名稱(例如root)。

sysApplInstallElmtPath	提供安裝此元素的目錄完整路徑。 例如，對於目錄「/opt/EMPuma/bin」中安裝的元素，該值將爲「/opt/EMPuma/bin」。 大多數應用程式套件都包含有關套件中包含的元素資訊。 另外，元素通常安裝在套件安裝目錄下的子目錄中。 在套件資訊本身不包含元素路徑名稱的情況下，通常可以透過簡單搜尋子目錄來確定路徑。 若該元素未安裝在該位置，並且代理實作沒有其他可用資訊，則該路徑不明並會傳回Null。
sysApplMapInstallPkgIndex	提供此物件的值，並識別此程式所屬的應用程式已安裝軟體套件。 若可以確定該程式的父應用程式，則該物件的值與 sysApplInstallPkgTable 中與該程式所屬的已安裝應用程式相對應項目的 sysApplInstallPkgIndex 值相同。 但是，若無法確定父應用程式(例如，該程式不是特定已安裝應用程式的一部分)，則該物件的值爲「0」，表示該程式無法與應用程式相關聯，並且會傳回已安裝的軟體套件。
sysApplElmtRunInstallID	提供 sysApplInstallElmtTable 的索引。 該物件的值與 sysApplInstallElmtIndex 的值相同，該物件的應用程式元素的此項目表示正在執行的執行個體。 若此程式無法與已安裝的可執行檔相關聯，則該值應爲「0」。
sysApplRunCurrentState	提供正在執行的應用程式執行個體的目前狀態。 可能的值是正在執行(1)、可執行(2)，但在等待資源，例如CPU、正在等待(3)事件、結束(4) 或其他(5)。 此值基於對此應用程式執行個體的執行元素(請參見 sysApplElmRunState) 及其由 sysApplInstallElmtRole 定義的角色評估。 若一或多個應用程式的一或多個「必要」元素不再執行，則該代理實作可以偵測到該應用程式執行個體正在退出。 大多數代理實作將等到第二次內部輪詢完成後才能讓系統有時間啓動 REQUIRED 元素，然後再將應用程式執行個體標記爲退出。
sysApplInstallPkgDate	提供安裝在主機上的軟體應用程式的日期和時間。

sysApplInstallPkgVersion	提供軟體製造商指派給應用程式套件的版本號碼。
sysApplInstallElmtType	提供作爲已安裝應用程式一部分的元素類型。
日期/時間相關查詢	
sysApplElmtRunCPU	此程式耗用的總系統 CPU 資源的釐秒數 (以釐秒爲單位) 附註 在多處理器系統上，該值可能會在實際 (時鐘) 時間的一釐秒中增加超過一釐秒。
sysApplInstallPkgDate	提供安裝在主機上的軟體應用程式的日期和時間。
sysApplElmtPastRunTimeEnded	提供程式結束的時間。
sysApplRunStarted	提供啓動應用程式的日期和時間。

MIB-II

使用 MIB2 代理從 MIB-II 取得資訊。 MIB2 代理提供對 RFC 1213 中定義之變數 (例如介面、IP 等) 的存取，並支援以下物件群組：

- 系統
- 介面
- at
- ip
- icmp
- tcp
- udp
- snmp

表 *18: MIB-II* 命令

命令	說明
裝置相關查詢	
sysName	提供此管理節點的管理指派名稱。按照約定，此名稱是節點的標準網域名稱。若名稱不明，則該值爲零長度字串。

sysDescr	提供實體的文字說明。 該值應包括系統硬體類型，軟體作業系統和網路軟體的全名和版本識別。
SNMP 診斷查詢	
sysName	提供此管理節點的管理指派名稱。按照約定，此名稱是節點的標準網域名稱。若名稱不明，則該值爲零長度字串。
sysUpTime	提供自上次重新初始化系統的網路管理部分以來的時間 (以百分之一秒爲單位)。
snmpInTotalReqVars	提供由於接收到有效的 SNMP Get-Request 和 Get-Next PDU 而被 SNMP 通訊協定實體成功擷取的 MIB 物件總數。
snmpOutPkts	提供從 SNMP 實體傳遞到傳輸服務的 SNMP 訊息總數。
sysServices	提供一個值，指出此實體可能提供的服務集。該值是一個總和。該總和最初值爲零，然後對於該節點執行交易的範圍爲 1 到 7 的每一層 L，將總和增加爲 (L-1) 再加 2。 例如，作爲提供應用程式服務的主機節點的值將爲 4 (2 ^(3-1))。 相反地，作爲提供應用程式服務的主機節點的值將爲 72 (2^(4-1) + 2^(7-1))。 附註 在 Internet 通訊協定套件的內容中，計算：第 1 層實際 (例如中繼器) ，第 2 層資料連結/子網路 (例如橋接器) 、第 3 層內部網路 (支援 IP) 、第 4 層端到端 (支援 TCP) 、第 7 層應用程式 (支援 SMTP)。 對於包含 OSI 通訊協定的系統，您還可以計算第 5 層和第 6 層。
snmpEnableAuthenTraps	指示是否允許 SNMP 實體產生 authenticationFailure 設陷。 該物件值將覆蓋所有組態資訊。如此可提供一種可以停用所有 authenticationFailure 設陷的方法。 附註 Cisco 強烈建議將此物件儲存在非揮發性記憶體中，以便在網路管理系統的重新初始化期間保持不變。
Syslog 相關查詢	

snmpEnabledAuthenTraps	指示是否允許 SNMP 實體產生 authenticationFailure 設陷。 該物件值將覆蓋所有組態資訊。如此可提供一種可以停用所有 authenticationFailure 設陷的方法。 附註 Cisco 強烈建議將此物件儲存在非揮發性記憶體中，以便在網路管理系統的重新初始化期間保持不變。
日期/時間相關查詢	
sysUpTime	提供自上次重新初始化系統的網路管理部分以來的時間 (以百分之一秒爲單位)。

HOST-RESOURCES MIB

使用主機資源代理從 HOST-RESOURCES-MIB 取得值。 主機資源代理提供對主機資訊的 SNMP 存取，例如儲存資源，程式表格、裝置資訊和已安裝的軟體庫。 主機資源代理支援以下物件群組：

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

表 *19: HOST-RESOURCES MIB* 命令

命令	說明
裝置相關查詢	
hrFSMountPoint	提供此檔案系統根目錄的路徑名。
hrDeviceDescr	提供此裝置的文字說明，包括裝置製造商和版本，以及序號 (選用)。
hrStorageDescr	提供儲存類型和執行個體說明。
記憶體、儲存空間和與 CPU 相關的查詢	
hrMemorySize	提供主機包含的實際讀寫主記憶體 (通常爲 RAM) 數量。
hrStorageSize	提供儲存的大小 (以 hrStorageAllocationUnits 爲單位)。在可以進行此作業且在基礎系統上可行的情況下，可寫入此物件以允許遠端組態儲存區域的大小。 例如，您可以修改分配給緩衝集區的主記憶體量或分配給虛擬記憶體的硬碟空間量。

程式相關查詢	
hrSWRunName	提供此執行軟體的文字說明，包括製造商，版本和一般熟知的名稱。 若此軟體爲本機安裝，則需與相應的 hrSWInstalledName 中使用的字串相同。
hrSystemProcesses	提供此系統上目前已載入或正在執行的程式內容的數量。
hrSWRunIndex	爲主機上執行的每個軟體提供唯一的值。 盡可能使用系統的本機唯一識別號碼。
與軟體元件相關的查詢	
hrSWInstalledName	提供此已安裝軟體的文字說明，包括製造商，版本、一般熟知的名稱和序號 (選用)。
hrSWRunPath	提供從中載入該軟體的長期儲存(例如硬碟機)的位置說明。
日期/時間相關查詢	
hrSystemDate	提供主機的本機日期和時間。
hrFSLastPartialBackupDate	提供此檔案系統其中一部分複製到另一個儲存裝置以進行備份的最後日期。 此資訊對於確保定期執行備份很有用。 若此資訊不明，則此變變值將對應於 0000 年 1 月 1 日 00:00:00.0，其編碼爲 (hex)'00 00 01 01 00 00 00 00'。

CISCO-SYSLOG-MIB

Syslog 追蹤並記錄所有系統訊息，從參考資訊到嚴重資訊。 使用此 MIB，網路管理應用程式可以接收 syslog 訊息作爲 SNMP 設陷：

Cisco Syslog 代理透過以下 MIB 物件支援設陷功能：

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

附註 CISCO-SYSLOG-MIB 取決於 CISCO-SMI MIB 的存在。

表 *20: CISCO-SYSLOG-MIB* 命令

命令	說明

Syslog 相關查詢	
clogNotificationEnabled	指示在裝置產生系統記錄檔訊息時是否將傳送 clogMessageGenerated 通知。 停用通知不會阻止將系統記錄檔訊息新增到 clogHistoryTable。
clogMaxSeverity	指示將處理的系統記錄檔嚴重性層級。 代理將忽略嚴重性值大於此值的任何系統記錄檔訊息。 附註 嚴重性數值隨著嚴重性的降低而增加。例如，錯誤 (4) 比除錯 (8) 更嚴重。

CISCO-CCM-MIB/CISCO-CCM-CAPABILITY MIB

CISCO-CCM-MIB 包含有關 Unified Communications Manager 及其關聯裝置 (例如電話、閘道等) 的動態 (即時) 和已設定 (靜態) 資訊，這些資訊在此 Unified Communications Manager 節點上可見。 簡單網路管理通訊協定 (SNMP) 表包含像是 IP 位址、註冊狀態和型號類型之類的資訊。

SNMP 支援 IPv4 和 IPv6，CISCO-CCM-MIB 包括 IPv4 和 IPv6 位址、偏好設定等等的欄和儲存空間。

附註 Unified Communications Manager 在 CiscoUnified Communications Manager 系統中支援此 MIB。 IM and Presence Service 和 Cisco Unity Connection 不支援此 MIB。

要檢視 CISCO-CCM-MIB 和 MIB 定義的支援清單，請前往以下連結：

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

要在 Unified Communications Manager 版本中檢視 MIB 相依性和 MIB 內容 (包括過時的物件) ，請前往以下連結： http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

僅當 Cisco CallManager 服務已啓動並正在執行 (或在 Unified Communications Manager 叢集組態中爲本機 Cisco CallManager 服務) 且已啓動且正在執行時，才會填入動態表格。當 Cisco CallManager SNMP 服務執行時，將填入靜態表格。

表 *21: Cisco-CCM-MIB* 動態表格

表格	內容
ccmTable	該表格儲存本機 Unified Communications Manager 的版本和安裝 ID。還儲存有關本機 Unified Communications Manager 知道但會顯示“不明”版本詳細資訊的叢集中所有 Unified Communications Manager 的資訊。 若本機 Unified Communications Manager 處於關閉狀態，則該表格將保持空白，除了版本和安裝 ID 值。

表格	內容
ccmPhoneFailed、ccmPhoneStatusUpdate、ccmPhoneExtn、ccmPhone、ccmPhoneExtension	Cisco Unified IP 電話而言，ccmPhoneTable 中已註冊電話的數量應與 Unified Communications Manager /RegisteredHardware 電話 Perfmon 計數器一致。 ccmPhoneTable 爲每個已註冊、未註冊或拒絕的 Cisco Unified IP 電話 包含一個項目。 ccmPhoneExtnTable 使用組合索引、ccmPhoneIndex 和 ccmPhoneExtnIndex 來關聯 ccmPhoneTable 和 ccmPhoneExtnTable 中的項目。
ccmCTIDevice、ccmCTIDeviceDirNum	ccmCTIDeviceTable 將每個 CTI 裝置儲存爲一個裝置。 根據 CTI 路由點或 CTI 通訊埠的註冊狀態，Unified Communications Manager MIB 中的 ccmRegisteredCTIDevices、ccmUnregisteredCTIDevices 和 ccmRejectedCTIDevices 計數器會更新。
ccmSIPDevice	CCMSIPDeviceTable 將每個 SIP Trunk 儲存爲一個裝置。
ccmH323Device	ccmH323DeviceTable 包含 Unified Communications Manager 包含其資訊的 H.323 裝置清單 (在叢集組態情況下爲本機 Unified Communications Manager)。 H.323 電話或 H.323 閘道方面，ccmH.323DeviceTable 爲每個 H.323 裝置納入一個項目。 (H.323 電話和閘道未於 Cisco Unified Communications Manager 註冊。 準備好處理指定的 H.323 電話和閘道的通話時，Unified Communications Manager 會產生 H.323Started 警報。) 系統提供閘道管理員資訊作爲 H.323 Trunk 資訊的一部分。
ccmVoiceMailDevice、ccmVoiceMailDirNum	對於 Cisco uOne ActiveVoice，ccmVoiceMailDeviceTable 包括一個用於每個語音留言裝置的項目。 根據註冊狀態，Cisc MIB 中的 ccmRegisteredVoiceMailDevices、ccmUnregisteredVoiceMailDevices 和 ccmRejectedVoiceMailDevices 計數器會更新。
ccmGateway	ccmRegisteredGateways、ccmUnregistered 閘道和 ccmRejectedGateways 分別追蹤已註冊的閘道裝置或通訊埠數量、未註冊的閘道裝置或通訊埠數量以及拒絕的閘道裝置或通訊埠數目。 Unified Communications Manager 會在裝置或通訊埠層級產生警報。 基於 CallManager 警報的 ccmGatewayTable 包含裝置層級或連接埠層級的資訊。 每個已註冊、未註冊或拒絕的裝置或連接埠在 ccmGatewayTable 中都有一個項目。 具有兩個 FXS 連接埠和一個 T1 連接埠的 VG200 在 ccmGatewayTable 中具有三個項目。 ccmActiveGateway 和 ccmInActiveGateway 計數器追蹤活動 (已註冊) 和與 (未註冊或拒絕的) 閘道裝置或通訊埠失去聯繫的數量。 根據註冊狀態，ccmRegisteredGateways、ccmUnregisteredGateways 和 ccmRejectedGateways 計數器會更新。
ccmMediaDeviceInfo	該表包含所有嘗試至少在本機 Unified Communications Manager 中註冊的媒體裝置清單。
ccmGroup	該表包含 Unified Communications Manager 叢集中的 Unified Communications Manager 群組。

表格	內容
ccmGroupMapping	該表將叢集中的所有 Unified Communications Manager 對應到 Unified Communications Manager 群組。 當本機 Unified Communications Manager 節點關閉時，該表保持空白。

表 *22: CISCO-CCM-MIB* 靜態表格

表格	內容
ccmProductType	該表包含 Unified Communications Manager (或在 Unified Communications Manager 叢集組態的情況下爲叢集)支援的產品類型清單，包括電話類型、閘道類型、媒體裝置類型、H.323 裝置類型、CTI 裝置類型、語音留言裝置類型和 SIP 裝置類型。
ccmRegion、ccmRegionPair	ccmRegionTable 包含 Cisco Communications Network (CCN) 系統中所有地理位置分開區域的清單。 ccmRegionPairTable 包含 Unified Communications Manager 叢集的地理區域配對清單。 地理區域配對由來源區域和目的地區域定義。
ccmTimeZone	該表包含 Unified Communications Manager 叢集中所有時區群組的清單。
ccmDevicePool	該表包含 Unified Communications Manager 叢集中所有裝置集區的清單。 裝置集區由區域，日期/時間群組和 Unified Communications Manager 群組定義。

附註 CISCO-CCM-MIB 中的 “ccmAlarmConfigInfo” 和 “ccmQualityReportAlarmConfigInfo ” 群組定義了與所描述的通知相關的組態參數。

CISCO-UNITY-MIB

CISCO-UNITY-MIB 使用連線 SNMP 代理取得有關 Cisco Unity Connection 的資訊。

要檢視 CISCO-UNITY-MIB 定義，請前往以下連結，然後按一下 **SNMP V2 MIB**：

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

附註 Cisco Unity Connection 支援此 MIB。 Unified Communications Manager 和 IM and Presence Service 不支援此 MIB。

連線 SNMP 代理支援下物件。

表 *23: CISCO-UNITY-MIB* 物件

物件	描述
Cisco Unity 表格	下表包含有關Cisco Unity Connection 伺服器的一般資訊，例如主機名稱和版本號碼。
ciscoUnityPortTable	下表含有關Cisco Unity Connection語音留言通訊埠的一般資訊。
一般Unity使用情況資訊物件	該群組含有關Cisco Unity Connection 語音留言通訊埠容量和使用率的資訊。

SNMP 組態需求

系統不提供預設的SNMP組態。 安裝後需設定SNMP設定才能存取MIB資訊Cisco支援SNMP V1、V2c 和 V3 版本。

SNMP 代理透過社群名稱和驗證設陷阱提供安全性。 您需設定社群名稱才能存取 MIB 資訊。 下表提供了必要的 SNMP 組態設定。

表 *24: SNMP* 組態需求

組態	**Cisco Unified Serviceability**頁面
V1/V2c 社群字串	**SNMP** > **V1/V2c** > **社群字串**
V3 社群字串	**SNMP** > **V3** > **使用者**
MIB2 的系統聯絡人和位置	**SNMP** > **SystemGroup** > **MIB2 系統群組**
設陷目的地 (V1/V2c)	**SNMP** > **V1/V2c** > **通知目的地**
設陷目的地 (V3)	**SNMP** > **V3** > **通知目的地**

SNMP 版本 1 支援

SNMP 版本 1 (SNMPv1) 是 SNMP 的初始實作，依循管理資訊結構 (SMI) 的規格運作，其會透過諸如使用者資料包通訊協定 (UDP) 和網際網路通訊協定 (IP) 之類的通訊協定進行操作。

SNMPv1 SMI 定義高度結構化表格 (MIB)，用來將表格式物件 (亦即，包含多個變數的物件) 的執行個體分區。 這些表格包含零或多個進行索引編製的列，因此 SNMP 可以使用支援的命令擷取或更改整列。

使用SNMPv1，NMS可以發出請求，並且受管理裝置可以傳回回應。代理會使用陷阱操作，將重要事件以非同步方式通知 NMS。

在Serviceability GUI 中，您可以在 **V1/V2c Configuration** (V1/V2c 組態) 視窗中設定 SNMPv1 支援。

SNMP 版本 2c 支援

與 SNMPv1 一樣，SNMPv2c 依循管理資訊結構 (SMI) 的規格運作。 MIB 模組包含相互關聯的受管理物件的定義。 SNMPv1 中使用的操作類似於 SNMPv2 中使用的操作。 例如，SNMPv2 陷阱操作提供 SNMPv1 中使用的同一功能，但它使用不同的訊息格式並取代了 SNMPv1 陷阱。

SNMPv2c 中的 Inform 操作允許一個 NMS 將陷阱資訊傳送到另一個 NMS，然後從 NMS 接收回應。

在Serviceability GUI 中，您可以在 **V1/V2c Configuration** (V1/V2c 組態) 視窗中設定 SNMPv2c 支援。

SNMP 版本 3 支援

SNMP 版本 3 提供安全性功能，例如驗證 (驗證請求是否來自真實來源) 、隱私 (資料加密) 、授權 (驗證使用者是否允許請求的操作) 及存取控制 (驗證使用者是否可以存取請求的物件)。 爲了防止 SNMP 封包暴露在網路上，您可以使用 SNMPv3 設定加密。

附註 從12.5 (1) SU1版開始，Unified Communications Manager不支援MD5或DES加密方法。 新增 SNMPv3 使用者時，可以選擇SHA或AES作爲身份驗證協議。

SNMPv3 不使用 SNMPv1 和 v2 之類的社群字串，而是使用 SNMP 使用者。

在 Serviceability GUI 中，您可以在 **V3Configuration** 視窗中設定 SNMPv3 支援。

SNMP 服務

下表中的服務支援 SNMP 作業。

附註 SNMP 主要代理充當 MIB 介面的主要服務。 您需手動啓動 Cisco CallManager SNMP 服務。 安裝後，所有其他 SNMP 服務都應如常執行。

表 *25: SNMP* 服務

MIB	服務	視窗
CISCO-CCM-MIB	Cisco CallManager SNMP 服務	**Cisco Unified Serviceability** > **工作** > **控制中心 - 功能服務**。 選擇一個伺服器；然後，選擇效能和監控類別。
SNMP 代理	SNMP 主要代理	**Cisco Unified Serviceability** > **工作** > **控制中心 - 網路服務**。 選擇一個伺服器；然後，選擇平台服務類別。 **CiscoUnifiedIM and Presence Serviceability** > **工具** > **控制中心 - 網路服務**。 選擇一個伺服器；然後，選擇平台服務類別。
CISCO-CDP-MIB	CiscoCDP 代理	
SYSAPPL-MIB	系統應用程式代理	
MIB-II	MIB2 代理	
HOST-RESOURCES-MIB	主機資源代理	
CISCO-SYSLOG-MIB	Cisco Syslog 代理	
硬體 MIB	原生代理配接器	

MIB	服務	視窗
CISCO-UNITY-MIB	連線 SNMP 代理	**Cisco Unity Connection Serviceability** > **工具** > **服務管理**。 選擇一個伺服器；然後，選擇基本服務類別。

注意 停止任何 SNMP 服務都可能會導致資料遺失，因爲網路管理系統不再監控 Unified Communication Manager 或 Cisco Unity Connection 網路。 除非您的技術支援團隊建議您這樣做，否則請勿停止服務。

SNMP 社群字串和使用者

儘管 SNMP 社群字串不提供安全性，但它們會驗證對 MIB 物件的存取並充當內嵌密碼。 您只能針對 SNMPv1 和 v2c 設定 SNMP 社群字串。

SNMPv3 不使用社群字串。 版本 3 改用 SNMP 使用者。 這些使用者的作用與社群字串相同，但使用者可以提供安全性，因爲您可以爲他們設定加密或驗證。

在Serviceability GUI 中，不存在預設社群字串或使用者。

SNMP 陷阱和通知

SNMP 代理以設陷的形式向 NMS 傳送通知，或通知以識別重要的系統事件。 設陷不會收到來自目的地的確認，而通知則會收到確認。 您可以使用Serviceability GUI 中的 SNMP 通知目的地組態視窗來設定通知目的地。

附註 Unified Communications Manager 在 Unified Communications Manager 和 IM and Presence Service 系統中支援 SNMP 設陷。

對於 SNMP 通知，若啓用了相應的設陷阱旗標，則系統會立即傳送設陷。 對於 syslog 代理，警報和系統層級記錄檔訊息將傳送到 syslog 精靈進行記錄。 另外，某些標準的第三方應用程式會將記錄檔訊息傳送到 syslog 精靈進行記錄。 這些記錄檔訊息將本機記錄在 syslog 檔案中，並且會轉換爲 SNMP 設陷/通知。

下表包含傳送至已配置設陷目標的 Unified Communications Manager SNMP 設陷/通知訊息：

- Unified Communications Manager 失敗
- 電話失敗
- 電話狀態更新
- 閘道失敗
- 媒體資源清單已用盡
- 路由清單已用盡
- 閘道第 2 層級變更

- 品質報告
- 惡意來電
- 產生 Syslog 訊息

提示 在設定通知目的地之前，請確認所需的 SNMP 服務已啓動並正在執行。 另外，請確保已正確設定社群字串/使用者的權限。

您可以在Serviceability GUI 中選擇 **SNMP** > **V1/V2** > **通知目的地**或 **SNMP** > **V3** > **通知目的地**以設定 SNMP 設陷目的地。

下表提供了有關您在網路管理系統 (NMS) 上設定設陷/通知參數的資訊。 您可以在 NMS 上發出適當的命令來設定表格中的值，如支援 NMS 的 SNMP 產品檔案中所述。

附註 除了最後兩個參數外，表格中列出的所有參數都是 CISCO-CCM-MIB 的一部分。 最後兩個 clogNotificationsEnabled 和 clogMaxSeverity 構成 CISCO-SYSLOG-MIB 的一部分。

IM and Presence Service 方面，您只能在 NMS 上設定 clogNotificationsEnabled 和 clogMaxSeverity 設陷/通知參數。

***表 26: Cisco Unified Communications Manager* 設陷/通知組態參數**

參數名稱	預設值	產生設陷	組態建議
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	保留預設規格。
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change 儘管您可以在 Cisco Unified Communications Manager 管理中將 CiscoATA 186 裝置設爲電話，當 Unified Communications Manager 爲 CiscoATA 裝置傳送 SNMP 設陷時，會傳送閘道類型設陷。例如，ccmGatewayFailed。	無。 預設情況下將此設陷設定爲啓用。
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	將 ccmPhoneStatusUpdateAlarmInterval 設爲 30 到 3600 之間的值。

參數名稱	預設值	產生設陷	組態建議
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	將 ccmPhoneFailedAlarmInterval 設爲 30 到 3600 之間的值。
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	無。 預設情況下將此設陷設定爲啓用。
ccmQualityReportAlarmEnable	True	僅當在伺服器上啓動並執行 CiscoExtended Functions 服務，或者使用叢集組態 (僅適用於 Unified Communications Manager) 時在本機 Unified Communications Manager 伺服器上啓動並執行該服務，才會產生此設陷。 ccmQualityReport	無。 預設情況下將此設陷設定爲啓用。
clogNotificationsEnabled	False	clogMessageGenerated	要啓用設陷產生，請將 clogNotificationsEnable 設爲 True。
clogMaxSeverity	警示	clogMessageGenerated	當您將 clogMaxSeverity 設爲警示時，當應用程式產生至少具有警示嚴重性層級的 syslog 訊息時，將產生 SNMP 設陷。

SFTP 伺服器支援

對於內部測試，我們在 Cisco Prime Collaboration 部署 (PCD) 上使用 SFTP 伺服器 (這些由 Cisco 提供)，支援則由 Cisco TAC 提供。 請參考下表，瞭解有關 SFTP 伺服器選項的摘要：

表 *27: SFTP* 伺服器支援

SFTP 伺服器	支援說明
Cisco Prime Collaboration 部署上的 SFTP 伺服器	此伺服器是由 Cisco 提供及測試的 SFTP 伺服器，並完全由 Cisco TAC 支援。 版本相容性視您的 Emergency Responder 版本和 Cisco Prime Collaboration 部署而定。 請先參閱 Cisco Prime Collaboration 部署管理指南，再升級其版本 (SFTP) 或 Emergency Responder，以確保版本相容，
Technology Partner 的 SFTP 伺服器	這些伺服器是由第三方提供和測試。 版本相容性視第三方測試而定。 如您升級其 SFTP 產品和/或升級 Unified Communications Manager，請參閱 Technology Partner 頁面。

SFTP 伺服器	支援說明
其他第三方 SFTP 伺服器	這些伺服器由第三方提供，且不受 Cisco TAC 正式支援。 版本相容性爲以能力所及的最佳方式建立相容的 SFTP 版本和 Emergency Responder 版本。 附註 這些產品未經過 Cisco 的測試，我們不保證功能性，Cisco TAC 不支援這些產品。若需要完整測試及支援的 SFTP 解決方案，請使用 Cisco Prime Collaboration 部署或 Technology Partner。

SNMP 組態工作流程

完成這些工作以設定簡單網路管理通訊協定。您需確定要配置的 SNMP 版本，因爲工作可能會有所不同。您可以選擇 SNMP V1、V2c 或 V3。

開始之前

安裝和設定 SNMP 網路管理系統。

程序

	命令或動作	目的
步驟 1	啓動 SNMP 服務 ，第 160 頁上的	確認基本的 SNMP 服務正在執行。
步驟 2	根據您的 SNMP 版本，完成以下工作之一： • 設定 SNMP 社群字串 ，第 160 頁上的 • 設定 SNMP 使用者 ，第 162 頁上的	對於 SNMP V1 或 V2，請設定社群字串。 對於 SNMP V3，請設定 SNMP 使用者。
步驟 3	取得遠端 SNMP 引擎 ID ，第 165 頁上的	對於 SNMP V3，取得通知目的地組態中必要的遠端 SNMP 引擎位址。 附註 對於 SNMP V3，此程式是必需的，但對於 SNMP V1 或 V2c，此程式是可選的。
步驟 4	設定 SNMP 通知目的地 ，第 166 頁上的	對於所有 SNMP 版本，爲 SNMP Traps and Informs 設定通知目的地。
步驟 5	設定 MIB2 系統群組 ，第 170 頁上的	爲 MIB-II 系統群組設定系統聯絡人和系統位置。
步驟 6	CISCO-SYSLOG-MIB 陷阱參數 ，第 171 頁上的	設定 CISCO-SYSLOG-MIB 的陷阱設定。
步驟 7	CISCO-CCM-MIB 陷阱參數 ，第 171 頁上的	僅限 Unified Communications Manager：爲 CISCO-CCM-MIB 設定陷阱設定。

	命令或動作	目的
步驟 8	重新啓動 SNMP 主要代理 ，第 172 頁上的	完成 SNMP 組態後，重新啓動 SNMP 主代理。
步驟 9	在 SNMP 網路管理系統上，設定 Unified Communications Manager 陷阱參數。	

啟動 SNMP 服務

使用此程式可確保 SNMP 服務已啓動並正在執行。

程序

步驟 1 登入Cisco Unified Serviceability。

步驟 2 確認 **Cisco SNMP 主要代理**網路服務正在執行。 根據預設，CDP 服務啓動且執行中。

a) 選擇**工具** > **控制中心 - 網路服務**。
b) 選擇發佈者節點，然後按一下**確定**。
c) 確認 **Cisco SNMP 主要代理**服務正在執行。

步驟 3 開始使用 **Cisco Call Manager SNMP Service**。

a) 選擇**控制中心** > **服務啟動**。
b) 從**伺服器**下拉式清單中，選擇發佈者節點，然後按一下**執行**。
c) 確認 **Cisco Call Manager SNMP Service** 正在執行。 若未執行，請勾選相對應的方塊，然後按一下**儲存**。

下一步

若要設定 SNMP V1 或 V2c，設定 SNMP 社群字串 ，第 160 頁上的。

若要設定 SNMP V3，設定 SNMP 使用者 ，第 162 頁上的。

設定 SNMP 社群字串

若要部署 SNMP V1 或 V2c，請使用以下流程來設定 SNMP 社群字串。

附註 SNMP V1 或 V2c 需要使用此流程。 SNMP V3 請配置 SNMP 使用者而非社群字串。

程序

步驟 1 在 Cisco Unified Serviceability 中選擇**snmp** > **V1/V2c** > **社群字串**。

步驟 2 選擇**伺服器**然後按一下**尋找**來搜尋現有的社群字串。 (選用) 您可以輸入搜尋參數來尋找特定的社群字串。

步驟 3 執行下列其中一項：

- 要編輯現有的 SNMP 社群字串，請選擇該字串。
- 要新增社群字串，請按一下**新增**。

附註　要刪除現有社群字串，請選擇該字串，然後按一下**刪除所選**。 刪除使用者後，重新啓動Cisco SNMP 主要代理。

步驟 4 輸入**社群字串名稱**。

步驟 5 完成 **SNMP 社群字串組態**視窗中的欄位。 如需有關欄位及其設定的描述，請參閱 社群字串組態設定 ，第 161 頁上的。

步驟 6 從**存取權限**下拉式清單，爲此社群字串設定權限。

步驟 7 若要將這些設定套用到於所有叢集節點，請勾選**套用至所有節點**方塊。

步驟 8 按一下**儲存**。

步驟 9 按一下**確定**以重新啓動 SNMP 主要代理服務，讓變更生效。

下一步

設定 SNMP 通知目的地 ，第 166 頁上的

社群字串組態設定

下表描述社群字串組態設定。

表 *28:* 社群字串組態設定

欄位	描述
伺服器	「社群字串」組態視窗中的此設定能顯示爲唯讀，因爲您在執行尋找社群字串的程式中指定了伺服器選擇。 若要變更社群字串的伺服器，請執行尋找社群字串程式。
社群字串	輸入社群字串的名稱。 此名稱最多可包含 32 個英數字元、連字型大小 (-) 及底線字元 (_) 的任意組合。 **提示**　選擇外部人員難以得知的社群字串名稱。 編輯社群字串時，您不能變更社群字串的名稱。
接受來自任何主機的 SNMP 封包	若要接受來自任何主機的 SNMP 封包，請按一下此按鈕。

欄位	描述
僅接受來自這些主機的 SNMP 封包	若要接受來自特定主機的 SNMP 封包，請按一下單選按鈕。 在「主機名稱/IPv4/IPv6 位址」欄位中，輸入要接受 SNMP 封包的來源 IPv4 或 IPv6 位址，然後按一下**插入**。 IPv4 位址爲小數點十進位格式。 例如 10.66.34.23。 IPv6 位址爲冒號分隔十六進位格式。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。 針對要接受 SNMP 封包的每個來源位址重複此程式。 若要刪除位址，請從「主機 IPv4/IPv6 位址」清單方塊中選擇該位址，然後按一下**移除**。
存取權限	在下拉式清單方塊中，從以下清單選擇適當的存取層級： **ReadOnly** 社群字串只能讀取 MIB 物件的值。 **ReadWrite** 社群字串可以讀取和寫入 MIB 物件的值。 **ReadWriteNotify** 社群字串可以讀取及寫入MIB物件的值，還可以傳送陷阱和通知訊息的 MIB 物件值。 **NotifyOnly** 社群字串只能傳送陷阱和通知訊息的 MIB 物件值。 **ReadNotifyOnly** 社群字串可以讀取MIB物件的值，還可以傳送陷阱和通知訊息的值。 **None** 社群字串無法讀取、寫入或傳送陷阱資訊。 **提示** 若要變更陷阱組態參數，請使用 NotifyOnly、ReadNotifyOnly 或 ReadWriteNotify 權限設定社群字串。 IM and Presence Service 不支援 ReadNoticyOnly。
套用到所有節點	若要將使用者群組態套用到叢集中的所有節點，請勾選此方塊。 該欄位僅適用於 Unified Communications Manager 和 IM and Presence Service 叢集。

設定 SNMP 使用者

若要部署 SNMP V3，請使用以下程式來設定 SNMP 使用者。

附註　SNMP V3 需要使用此程式。 對於 SNMP V1 或 V2c，請改爲設定社群字串。

程序

步驟 1 在 Cisco Unified Serviceability中，選擇 **Snmp** > **V3** > **使用者**。

步驟 2 選擇**伺服器**然後按一下**尋找**搜尋現有的 SNMP 使用者。 (選用) 您可以輸入搜尋參數來尋找特定的使用者。

步驟 3 執行下列其中一項：

- 要編輯現有的 SNMP 使用者，請選擇該使用者。
- 若要新增 SNMP 使用者，請按一下**新增**。

附註　要刪除現有使用者，請選擇該使用者，然後按一下**刪除所選**。 刪除使用者後，重新啓動Cisco SNMP 主要代理。

步驟 4 輸入 **SNMP 使用者名稱**。

步驟 5 輸入 SNMP 使用者群組態設定。 如需有關欄位及其設定的描述，請參閱 SNMP V3 使用者群組態設定 ，第 164 頁上的。

提示　儲存組態，可以隨時按一下**全部清除**按鈕，刪除您爲視窗中所有設定輸入的所有資訊。

步驟 6 從**存取權限**下拉式清單中，設定要指派給該使用者的存取權限。

步驟 7 若要將此組態套用到於所有叢集節點，請勾選**套用至所有節點**方塊。

步驟 8 按一下**儲存**。

步驟 9 按一下**確定**以重新啓動 SNMP 主要代理。

附註　要使用您設定的使用者存取伺服器，請確保在NMS 上設定該使用者適當的驗證和隱私設定。

下一步

取得遠端 SNMP 引擎 ID ，第 165 頁上的

SNMP V3 使用者群組態設定

下表說明 SNMP V3 使用者群組態設定。

表 *29: SNMP V3* 使用者群組態設定

欄位	描述
伺服器	此設定顯示爲唯讀，因爲您在執行尋找通知目的地的程式時指定了伺服器。 要變更提供存取權限的伺服器，請執行以下步驟尋找 SNMP 使用者。
使用者名稱	在欄位中，輸入要爲其提供存取權限的使用者名稱。 此名稱最多可包含 32 個英數字元、連字型大小 (-) 及底線字元 (_) 的任意組合。 **提示** 輸入您已經爲網路管理系統 (NMS) 設定的使用者。 對於現有的 SNMP 使用者，此設定顯示爲唯讀。
需要驗證	若要要求驗證，請勾選方塊，在密碼和重新輸入密碼欄位中輸入密碼，然後選擇適當的通訊協定。 SNMPv3 密碼至少要 8 個字元長。 **附註** 若啓用了 FIPS 模式或增強安全性模式，請選擇 **SHA** 作爲通訊協定。
需要隱私	若勾選了需要驗證方塊，則可以指定隱私資訊。若想要求隱私，請勾選方塊，在密碼和重新輸入密碼欄位中輸入密碼，然後勾選適當的通訊協定方塊。 SNMPv3 密碼至少要 8 個字元長。 **附註** 若啓用了 FIPS 模式或增強安全性模式，請選擇 **AES128** 作爲通訊協定。
接受來自任何主機的 SNMP 封包	若要接受來自任何主機的 SNMP 封包，請按一下單選按鈕。
僅接受來自這些主機的 SNMP 封包	若要接受來自特定主機的 SNMP 封包，請按一下單選按鈕。 在「主機名稱/IPv4/IPv6 位址」欄位中，輸入要接受 SNMP 封包的來源 IPv4 或 IPv6 位址，然後按一下**插入**。 IPv4 位址爲小數點十進位格式。 例如 10.66.34.23。 IPv6 位址爲冒號分隔十六進位格式。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。 針對要接受 SNMP 封包的每個來源位址重複此程式。 若要刪除位址，請從「主機 IPv4/IPv6 位址」清單方塊中選擇該位址，然後按一下**移除**。

欄位	描述
存取權限	從下拉式清單方塊中，選擇下列其中一個存取層級選項： **ReadOnly** 您只能讀取 MIB 物件的值。 **ReadWrite** 您可以讀寫 MIB 物件的值。 **ReadWriteNotify** 您可以讀取和寫入 MIB 物件的值，以及傳發設陷的 MIB 物件值和通知訊息。 **NotifyOnly** 您只能傳送用於設陷和通知訊息的 MIB 物件值。 **ReadNotifyOnly** 您可以讀取 MIB 對象的值，還可以傳送陷阱值並通知訊息。 **None** 您無法讀取、寫入或傳送陷阱資訊。 **提示** 要變更設陷組態參數，請使用 NotifyOnly、ReadNotifyOnly 或 ReadWriteNotify 權限設定使用者。
套用到所有節點	要將使用者群組態套用到叢集中的所有節點，請勾選此方塊。 這僅適用於 Unified Communications Manager 和 IM and Presence Service叢集。

取得遠端 SNMP 引擎 ID

若要部署 SNMP V3，請使用此程式取得遠端 SNMP 引擎 ID，這是通知目的地組態所必需的。

附註 對於 SNMP V3，此程式是必需的，但對於 SNMP V1 或 2C，此程式是可選的。

程序

步驟 1 登入命令行介面。

步驟 2 執行 `utils snmp walk 1` CLI 命令。

步驟 3 輸入設定的社群字串 (使用 SNMP V1/V2) 或設定的使用者 (使用 SNMP V3)。

步驟 4 輸入伺服器的 IP 位址。 例如，針對 localhost 輸入 `127.0.0.1`。

步驟 5 輸入 `1.3.6.1.6.3.10.2.1.1.0` 作爲物件 ID (OID)。

步驟 6 對於檔案，輸入 檔案。

步驟 7 輸入 y。
系統輸出的 HEX-STRING 表示遠端 SNMP 引擎 ID。

步驟 8 在執行 SNMP 的每個節點上重複此程式。

下一步

設定 SNMP 通知目的地 ，第 166 頁上的

設定 SNMP 通知目的地

使用此程式爲 SNMP Traps and Informs 設定通知目的地。 您可以對 SNMP V1，V2c 或 V3 使用此程式。

開始之前

若尚未設定 SNMP 社群字串或 SNMP 使用者，請完成以下工作之一：

- 對於 SNMP V1/V2，請參閱 設定 SNMP 社群字串 ，第 160 頁上的
- 對於 SNMP V3，請參閱 設定 SNMP 使用者 ，第 162 頁上的

程序

步驟 1 從 Cisco Unifeid Serviceability中，選擇以下選項之一：

- 對於 SNMP V1/V2，選擇**snmp** > **V1/V2** > **通知目的地**
- 對於 SNMP V3，選擇**snmp** > **V3** > **通知目的地**

步驟 2 選擇**伺服器**然後按一下**尋找**搜尋現有的 SNMP 通知目的地。 (選用) 您可以輸入搜尋參數來尋找特定的目的地。

步驟 3 執行下列其中一項：

- 要編輯現有的 SNMP 通知目的地，請選擇通知目的地。
- 要新增 SNMP 通知目的地，請按一下**新增**。

附註 要刪除現有的SNMP通知目的地，請選擇目標，然後按一下**刪除所選**。 刪除使用者後，重新啓動 **Cisco SNMP 主要代理**。

步驟 4 從**主機 IP 位址**下拉式功能表中，選擇現有位址或按一下**新增**並輸入一個新的主機 IP 位址。

步驟 5 僅限 SNMP V1/V2。 **SNMP 版本**欄位中選擇 V1 或 V2C 單選按鈕，端看您設定的爲 SNMP V1 還是 V2c。

步驟 6 對於 SNMP V1/V2，請完成以下步驟：

a) 僅限 SNMP V2。 從**通知類型**下拉式功能表中，選擇**通知**或**陷阱**。

b) 選擇您設定的**社群字串**。

步驟 7 對於 SNMP V3，請完成以下步驟：

a) 從**通知類型**下拉式功能表中，選擇**通知**或**設陷**。

b) 從**遠端 SNMP 引擎 ID** 下拉式功能表，選擇現有的引擎 ID 或選擇**新增**並輸入新的 ID。

c) 從**安全性層級**下拉式功能表，指派適當的安全性層級。

步驟 8 若要將此組態套用到於所有叢集節點，請勾選**套用至所有節點**方塊。

步驟 9 按一下**插入**。

步驟 10 按一下**確定**以重新啓動 SNMP 主要代理。

範例

附註 有關通知目的地組態視窗中的欄位描述說明，請參閱以下主題之一：

- SNMP V1 和 V2c 的通知目的地設定 ，第 167 頁上的
- SNMP V3 的通知目的地設定 ，第 168 頁上的

下一步

設定 MIB2 系統群組 ，第 170 頁上的

SNMP V1 和 V2c 的通知目的地設定

下表描述了 SNMP V1/V2c 的通知目的地組態設定。

表 *30: SNMP V1/V2c* 的通知目的地組態設定

欄位	描述
伺服器	此設定顯示爲唯讀，因爲您在執行尋找通知目的地的程式時指定了伺服器。 要變更通知目的地的伺服器，請執行尋找社群字串的程式。
主機 IPv4/IPv6 位址	從下拉式清單方塊中，選擇設陷目的地的主機 IPv4/IPv6 位址或按一下**新增**。 若按一下**新增**，在「主機 IPv4/IPv6 位址」欄位中輸入設陷目的地的 IPv4/IPv6 位址。 對於現有的通知目的地，您無法修改主機 IP 位址組態。
主機 IPv4/IPv6 位址	在欄位中，輸入要從其接受 SNMP 封包的 IPv4 或 IPv6 位址。 IPv4 位址爲小數點十進位格式。 例如 10.66.34.23。 IPv6 位址爲冒號分隔十六進位格式。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。

欄位	描述
連接埠號碼	在欄位中，輸入目標伺服器上的接收 SNMP 封包的通訊埠號碼。
V1 或 V2c	在SNMP版本資訊窗格中，依您所使用的SNMP版本按一下適當的SNMP版本 (V1 或 V2c) 單選按鈕 。 • 若選擇 V1，請設定社群字串設定。 • 若選擇 V2c，請設定通知類型設定，然後設定社群字串。
社群字串	從下拉式清單方塊中，選擇要在此主機產生的通知訊息中使用的社群字串名稱。 僅顯示具有最低通知權限 (讀取與寫入通知或僅通知) 的社群字串。 若尚未設定社群字串的這些權限，則下拉式清單方塊中將不會顯示任何選項。如有必要，請按一下**建立新的 uiCommunity 字串**以建立社群字串。 僅 IM and Presence：僅顯示具有最低通知權限 (讀取與寫入通知、僅讀取通知或僅通知) 的社群字串。 若尚未設定社群字串的這些權限，則下拉式清單方塊中將不會顯示任何選項。如有必要，請按一下**建立新的社群字串**以建立社群字串。
通知類型	從下拉式清單方塊中，選擇適當的通知類型。
套用到所有節點	要將通知目的地組態套用到叢集中的所有節點，請勾選此方塊。 這僅適用於 Cisco Unified Communications Manager 和 IM and Presence Service 叢集。

SNMP V3 的通知目的地設定

下表描述了 SNMP V3 的通知目的地組態設定。

表 *31: SNMP V3* 的通知目的地組態設定

欄位	描述
伺服器	此設定顯示爲唯讀，因爲您在執行尋找 SNMP V3 通知目的地的程式時指定了伺服器。 要變更用於通知目的地的伺服器，請執行以下步驟尋找 SNMP V3 通知目的地並選擇其他伺服器。
主機 IPv4/IPv6 位址	從下拉式清單方塊中，選擇設陷目的地的主機 IPv4/IPv6 位址或按一下**新增**。 若按一下**新增**，在「主機 IPv4/IPv6 位址」欄位中輸入設陷目的地的 IPv4/IPv6 位址。 對於現有的通知目的地，您無法修改主機 IP 位址組態。

欄位	描述
主機 IPv4/IPv6 位址	在欄位中，輸入要從其接受 SNMP 封包的 IPv4 或 IPv6 位址。 IPv4 位址爲小數點十進位格式。 例如 10.66.34.23。 IPv6 位址爲冒號分隔十六進位格式。 例如 2001:0db8:85a3:0000:0000:8a2e:0370:7334 或 2001:0db8:85a3::8a2e:0370:7334。
連接埠號碼	在欄位中，輸入目的地伺服器上的接收通知的連接埠號碼。
通知類型	從下拉式清單方塊中選擇**通知**或**設陷**。 **提示** Cisco建議您選擇通知選項。通知功能會重新傳輸訊息直到系統確認爲止，因此比設陷更可靠。
遠端 SNMP 引擎 ID	若從「通知類型」下拉式清單方塊中選擇「通知」，則會顯示此設定。 在下拉式清單方塊中，選擇引擎 ID 或選擇**新增**。 若選擇「新增」，請在「遠端 SNMP 引擎 ID」欄位中輸入十六進位的 ID 值。
安全性層級	從下拉式清單方塊中，爲使用者選擇適當的安全性層級。 **noAuthNoPriv** 未設定驗證或隱私。 **authNoPriv** 已設定驗證，但未設定隱私。 **authPriv** 已設定驗證和隱私。
使用者資訊窗格	在窗格中，執行以下任務之一，以將通知目的地與使用者關聯或取消關聯。 1. 要建立新使用者，請按一下**建立新使用者**。 2. 要修改現有使用者，請按一下該使用者的單選按鈕，然後按一下**更新所選使用者**。 3. 要刪除使用者，請按一下該使用者的單選按鈕，然後按一下**刪除所選使用者**。 顯示的使用者會依您爲通知目的地設定的安全性層級而有所不同。
套用到所有節點	要將通知目的地組態套用到叢集中的所有節點，請勾選此方塊。 這僅適用於 Cisco Unified Communications Manager 和 IM and Presence Service 叢集。

設定 MIB2 系統群組

使用此程式爲 MIB-II 系統群組設定系統聯絡人和系統位置。 例如，您可以輸入 Administrator 555-121-6633 作爲系統聯絡人，輸入 SanJose，Bldg 23 2 樓作爲系統位置。 您可以對 SNMP V1，V2 和 V3 使用此程式。

程序

步驟 1 從 Cisco Unified Serviceability中，選擇 **Snmp** > **SystemGroip** > **MIB2 系統群組**。

步驟 2 從**伺服器**下拉式清單中選擇節點，然後按一下**執行**。

步驟 3 完成**系統聯絡人**和**系統位置**欄位。

步驟 4 若要將這些設定套用到於所有叢集節點，請勾選**套用至所有節點**方塊。

步驟 5 按一下**儲存**。

步驟 6 按一下**確定**以重新啓動 SNMP 主要代理服務

範例

附註 如需取得欄位說明，請參閱 MIB2 系統群組設定 ，第 170 頁上的

附註 您可以按一下**全部清除**以清除欄位。 若依序按一下**全部清除**和**儲存**，記錄將被刪除。

MIB2 系統群組設定

下表說明 MIB2 系統群組組態設定。

表 *32: MIB2* 系統群組組態設定

欄位	描述
伺服器	從下拉式清單方塊中，選擇要爲其設定聯絡人的伺服器，然後按一下**確定**。
系統聯絡人	輸入發生問題時通知的人員。
系統位置	輸入被識別爲系統聯絡人的人員位置。
套用到所有節點	選擇以將系統組態套用到叢集中的所有節點。 這僅適用於 Unified Communications Manager 和 IM and Presence Service叢集。

CISCO-SYSLOG-MIB 陷阱參數

請使用以下指導原則，在系統上設定 CISCO-SYSLOG-MIB 陷阱設定：

- 使用 SNMP Set 操作將 clogsNotificationEnabled (1.3.6.1.4.1.9.9.41.1.1.2) 設定爲 True；例如，例如，使用 net-snmp set 公用程式，利用以下命令從 linux 命令行將此 OID 設定爲 True：

```
snmpset -c <community string>-v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

  您也可以將任何其他 SNMP 管理應用程式用於 SNMP Set 操作。

- 使用 SNMP Set 操作來設定 clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) 值；例如，例如，使用 net-snmp set 公用程式，利用以下命令從 linux 命令行設定此 OID 值：

```
snmpset-c public-v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i
<value>
```

  輸入<value>設定的嚴重性編號。 嚴重性值隨嚴重性降低而增加。 值 1 (緊急) 表示最高嚴重性，值 8 (除錯) 表示最低嚴重性。 Syslog 代理會忽略任何大於指定值的訊息；例如，若要捕獲所有 Syslog 訊息，請使用值 8。

  嚴重性的值如下：

  - 1：緊急
  - 2：警示
  - 3：嚴重
  - 4：錯誤
  - 5：警示
  - 6：注意
  - 7：資訊
  - 8：除錯

  您也可以將任何其他 SNMP 管理應用程式用於 SNMP Set 操作。

附註 在記錄之前，Syslog 會截斷任何大於所指定 Syslog 緩衝區大小的陷阱訊息資料。 Syslog 陷阱訊息的長度限制等於 255 個位元組。

CISCO-CCM-MIB 陷阱參數

- 使用 SNMP Set 操作將 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) 設定爲 30-3600 範圍內的值；例如，使用 net-snmp set 公用程式，利用以下命令從 linux 命令行設定此 OID 值：

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

您也可以將任何其他 SNMP 管理應用程式用於 SNMP Set 操作。

- 使用 SNMP Set 操作將 ccmPhoneStatusUpdateAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.4) 設定爲 30-3600 範圍內的值；例如，使用 net-snmp set 公用程式，利用以下命令從 linux 命令行設定此 OID 值：

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
```

您也可以將任何其他 SNMP 管理應用程式用於 SNMP Set 操作。

CISCO-UNITY-MIB 陷阱參數

僅限 Cisco Unity Connection：儘管陷阱可由 Cisco Unity Connection 警報觸發，但 Cisco Unity Connection SNMP 代理不會啓用陷阱通知。 您可以在**警報** > **定義**畫面上檢視 Cisco Unity Connection 服務能力中的 Cisco Unity Connection 警報定義。

您可以使用 CISCO-SYSLOG-MIB 設定陷阱參數。

相關主題

CISCO-SYSLOG-MIB 陷阱參數 ，第 171 頁上的

重新啟動 SNMP 主要代理

完成所有 SNMP 組態後，重新啓動 SNMP 主代理 服務。

程序

步驟 1 在 Cisco Unified Serviceability 中選擇**工具** > **控制中心 - 網路服務**。

步驟 2 選擇**伺服器**然後按一下**執行**。

步驟 3 選擇 **SNMP 主要代理**。

步驟 4 按一下**重新啟動**。

SNMP 陷阱設定

使用 CLI 命令來設定可設定的 SNMP 陷阱設定。 爲 CISCO-SYSLOG-MIB、CISCO-CCM-MIB 和 CISCO-UNITY-MIB 提供 SNMP 陷阱組態參數和建議的組態提示。

設定 SNMP 陷阱

使用此程式設定 SNMP 陷阱。

開始之前

爲 SNMP 設定系統。 如需詳細資訊，請參閱SNMP 組態工作流程 ，第 159 頁上的。

確保對於 SNMP 社群字串 (對於 SNMP V1/V2) 或 SNMP 使用者 (對於 SNMP V3) 而言，**存取權限**均設爲以下設定之一：**ReadWriteNotify**、**ReadNotify**、**NotifyOnly**。

程序

步驟 1 登入到 CLI 並執行 `utils snmp test` CLI 命令，以確認 SNMP 是否正在執行。

步驟 2 遵循 產生 SNMP 設陷 ，第 173 頁上的 以產生特定 SNMP 陷阱 (例如，ccmPhoneFailed 或 MediaResourceListExhausted 陷阱)。

步驟 3 若未產生陷阱，請執行以下步驟：

- 在「Cisco Unified Serviceability」中，選擇**警報** > **組態**，然後選擇 **CM 服務**和 **Cisco CallManager**。
- 勾選**套用至所有節點**方塊。
- 在「本機系統記錄檔」下，將「警報事件層級」下拉式清單方塊設定爲**參考**。

步驟 4 重現陷阱並檢查對應的警報是否記錄在 CiscoSyslog 檔案中。

產生 SNMP 設陷

本節介紹了產生特定 SNMP 設陷類型的程式。 SNMP 需在伺服器上設定並執行，以便產生個別的設陷。 遵循 設定 SNMP 陷阱 ，第 173 頁上的 瞭解如何設定系統以產生 SNMP 設陷的說明。

附註 個別 SNMP 設陷的處理時間因您嘗試產生的設陷而異。 某些 SNMP 設陷可能最多需要幾分鐘才能產生。

表 *33:* 產生 *SNMP* 設陷

SNMP 設陷	程式
ccmPhoneStatusUpdate	要觸發 ccmPhoneStatusUpdate 設陷： **1.** 在 ccmAlarmConfig Info mib 表格中，設定 ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 或更高。 **2.** 登入 Cisco Unified Communications Manager 管理。 **3.** 若電話正使用中並已註冊至 Unified Communications Manager，請重設電話。 取消電話註冊，然後重新註冊，以產生 ccmPhoneStatusUpdate 設陷。
ccmPhoneFailed	要觸發 ccmPhoneFailed 設陷： **1.** 在 ccmAlarmConfigInfo mib 表格中，設定 ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) =30 或更高。 **2.** 在 Cisco Unified Communications Manager 管理中，將電話的 MAC 位址變更爲無效值。 **3.** 在 Cisco Unified Communications Manager 管理中，註冊電話。 **4.** 將電話設定爲指向 TFTP 伺服器 A，然後將電話插入其他伺服器。
ccmGatewayFailed	要觸發 ccmGatewayFailed SNMP 設陷： **1.** 確認 ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) 設爲 True。 **2.** 在 Cisco Unified Communications Manager 管理中，將閘道的 MAC 地址變更爲無效值。 **3.** 重新啓動閘道。
ccmGatewayLayer2Change	要在受監控的第 2 層級的工作閘道上觸發 ccmGatewayLayer2Change 設陷 (例如 MGCP 回傳負載) ： **1.** 在 ccmAlarmConfig Info mib 表格中，將 ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) 設定爲 True。 **2.** 在 Cisco Unified Communications Manager 管理中，將閘道的 MAC 地址變更爲無效值。 **3.** 重設閘道。

SNMP 設陷	程式
MediaResourceListExhausted	要觸發 MediaResourceListExhausted 設陷： **1.** 在 Cisco Unified Communications Manager 管理中，建立一個媒體資源群組，其中包含標準會議橋接資源 (CFB-2) 之一。 **2.** 建立一個包含您之前建立的媒體資源群組的媒體資源群組清單。 **3.** 在電話組態視窗中，將媒體資源群組清單欄位設定爲您建立的媒體資源群組清單。 **4.** 停止 IP 語音媒體串流服務。 此動作導致 ConferenceBridge 資源 (CFB-2) 停止工作。 **5.** 透過使用媒體資源群組清單的電話進行電話會議。「無會議橋接可用」訊息出現在電話螢幕中。
RouteListExhausted	要觸發 RouteListExhausted 設陷： **1.** 建立包含一個閘道的路由組。 **2.** 建立一個包含您剛建立之路由組的路由組清單。 **3.** 建立通過路由群組清單路由通話的唯一路由模式。 **4.** 將閘道取消註冊。 **5.** 撥出與其中一個電話相符的路由模式號碼。
MaliciousCallFailed	要觸發 MaliciousCallFailed 設陷： **1.** 建立一個包含所有可用「MaliciousCall」軟按鍵的軟按鍵範本。 **2.** 將新的軟按鍵範本指派給網路中的電話並重設電話。 **3.** 接通兩台電話。 **4.** 在通話過程中，選擇「MaliciousCall」軟按鍵。

SNMP 設陷	程式
ccmCallManagerFailed	**1.** 執行顯示程清單 CLI 命令以取得 CallManager 應用程式 ccm 的程式識艘別碼 (PID)。 此命令會傳多個程式及其 PID。 您特別務必取得 ccm 的 PID，因爲需停止此 PID 才能產生警報。 **2.** 執行 `delete process <pid>` 損毀 CLI 指令 **3.** 執行 CLI 命令。 產生內部錯誤時，將產生 CallManager 失敗警報。 這些內部錯誤可能包括由於缺少CPU而導致內部執行緒退出，讓CallManager伺服器暫停超過 16 秒以及計時器問題。 您無法手動產生此警報。 附註 產生 ccmCallManagerFailed 警報或設陷將關閉 CallManager 服務並產生核心檔案。 爲避免混淆，Cisco 建議您立即刪除核心檔案。
syslog messages as traps	要接收特定嚴重性以上的系統記錄檔訊息設陷，請在 clogBasic 表中設定以下兩個 mib 物件： **1.** 將 clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2) 設爲 True(1)。 預設值爲 false(2)。 例如，snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 **2.** 將 clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) 設爲大於您希望設陷的層級。 預設值爲警示 (5)。 所有警報嚴重性小於或等於設定嚴重性層級的系統記錄檔訊息均以設陷傳送。 例如，snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

SNMP 追蹤組態

對於 Unified Communications Manager，您可以在 Cisco Unified Serviceability的「追蹤組態」視窗中設定 Cisco CallManager SNMP 代理的追蹤，方法爲在「效能和監控服務」服務群組中選擇 Cisco CallManager SNMP 服務。 所有代理都有預設設定。 對於 Cisco CDP 代理和 Cisco Syslog 代理，您可以使用 CLI 變更叢集設定，如 *Cisco Unified* 解決方案的命令行介面參考指南。

對於 Cisco Unity Connection，您可以在 Cisco Unity Connection 服務能力的「追蹤組態」視窗中爲 Cisco Unity Connection SNMP 代理設定追蹤，方法爲選擇連線 SNMP 代理元件。

對 SNMP 進行疑難排解

檢閱本節以取後疑難排解提示。 確保所有功能和網路服務都在執行中。

問題

您無法從系統輪詢任何 MIB。

這種情況代表著社群字串或 snmp 使用者未在系統上設定，或者其與系統上設定的不符。 依預設，不會在系統上設定社群字串或使用者。

解決方案

使用 SNMP 組態視窗，檢查是否已在系統上適當地設定社群字串或 snmp 使用者。

問題

您無法從系統收到任何通知。

這種情況代表著未在系統上正確地設定通知目的地。

解決方案

驗證您是否已在「通知目的地 (V1/V2c 或 V3) 組態」視窗中適當地設定通知目的地。

第 15 章

服務

功能服務

使用Serviceability GUI 啓動、開始和停止 Cisco Unified Communications Manager 和 IM and Presence Service。 啓動能開啓和開始服務。 針對您要使用的所有功能，您需手動啓動功能服務。 如需服務啓動的建議，請參閱與服務啓動相關的主題。

附註 若您嘗試從 IM and Presence 節點存取 Unified Communications Manager 伺服器 (反之亦然) ，可能會遇到以下錯誤：「無法建立伺服器連線(無法存取遠端節點) 」。 若出現此錯誤訊息，請參閱《*Cisco Unified Communications Manager* 管理指南》。

附註 使用 IM and Presence 的裝置設定爲使用 Postgres 外部資料庫來支援持續聊天、合規和檔案傳輸。 但是，IM and Presence 伺服器與 Postgres 之間的連線缺少保護，資料通過時沒有任何檢查。 對於不支援 TLS 的服務或裝置，還有另一種方法可以提供安全通訊，就是透過設定安全通訊的標準通訊協定— IP Sec 來提供安全通訊，針對通訊作業階段的每個 IP 封包進行驗證和加密。

在**服務啟動**視窗啓動服務後，您無需在**控制中心 - 功能服務**視窗中啓動服務。 若該服務由於任何原因而無法啓動，您需在**控制中心 - 功能服務**視窗中啓動。

系統安裝後，不會自動啓動功能服務，您需要啓動功能服務才能使用Serviceability報告封存檔功能之類的組態功能。

僅限 Unified Communications Manager 和 Cisco Unified IM and Presence Service：若您要升級 Unified Communications Manager，升級之前在系統上啓動的服務會在升級後自動啓動。

啓動功能服務後，您可以使用產品的管理 GUI 修改服務參數設定：

- Cisco Unified Communications Manager 管理

- Cisco Unity Connection 管理

功能服務類別

在 Cisco Unified Serviceability中，**服務啟動**視窗和**控制中心 - 功能服務**視窗會將功能服務分爲以下幾類：

- 資料庫與管理服務
- 效能與監控服務
- CM 服務
- CTI 服務
- CDR 服務
- 安全性服務
- 目錄服務
- 語音品質報告服務

在 Cisco Unified IM and Presence Serviceability中，**服務啟動**視窗和**控制中心 - 功能服務**視窗會將功能服務分爲以下幾類：

- 資料庫與管理服務
- 效能與監控服務
- IM and Presence Service 服務

資料庫與管理服務

位置頻寬管理員

IM and Presence Service不支援此服務。

位置頻寬管理員服務會從一或多個叢集中設定的位置與連結資料聚集一個網路模型，決定每一對位置間的有效路徑，根據各通話類型的頻寬可用性決定是否承認每一對位置間的通話，以及扣除獲准的每個通話期間的頻寬 (保留)。

Cisco AXL Web 服務

Cisco AXL Web 服務可讓您修改資料庫項目，以及從使用 AXL 的使用者端應用程式執行預存程式。

在 IM and Presence Service系統中，此服務同時支援 Unified Communications Manager 和 Cisco Unity Connection。

Cisco UXL Web 服務

IM and Presence Service不支援此服務。

Cisco IP 電話通訊錄同步工具中的 TabSync 使用者端使用 Cisco UXL Web 服務來查詢 Unified Communications Manager 資料庫，這可確保 Cisco IP 電話通訊錄同步工具使用者只能存取與其相關的一般使用者資料。 Cisco UXL Web 服務能執行以下功能：

- 當一般使用者登入 Cisco IP 電話通訊錄同步工具時，透過驗證一般使用者的使用者名稱和密碼來進行驗證檢查。
- 藉由只允許目前登入 Cisco IP 電話通訊錄同步工具的使用者執行列出、擷取、更新、移除和新增聯絡人之類的功能，進行使用者授權檢查。

Cisco 批量佈建服務

該服務不支援 Cisco Unity Connection。

若您的組態支援叢集 (僅適用於 Unified Communications Manager) ，您只能在第一部伺服器上啓動 Cisco 批量佈建服務。 若您使用 Unified Communications Manager 批量管理工具來管理電話和使用者，需啓動此服務。

Cisco TAPS 服務

該服務不支援 Cisco Unity Connection 或 IM and Presence Service。

Cisco 的自動註冊電話支援工具 (TAPS) 服務支援 Cisco Unified Communications Manager 自動註冊電話工具，允許使用者在回應交互式語音回覆 (IVR) 提示後，於自動註冊的電話上上傳自訂組態。

若您的組態支援叢集 (僅適用於 Unified Communications Manager) ，請在第一部伺服器上啓動此服務。 當您要爲該工具建立空的 MAC 位址時，請務必在同一部伺服器上啓動 Cisco 批量佈建服務。

提示 Cisco Unified Communications Manager 自動註冊電話工具需仰賴 Cisco Customer Response Solutions (CRS)。 若要讓工具發揮設計的功能，請按照 CRS 檔案中的說明，檢查 CRS 伺服器是否已設定而且正在執行。

平台管理 Web 服務

平台管理 Web 服務是一種簡單物件存取通訊協定 (SOAP) API，可以在 Unified Communications Manager、IM and Presence Service 和 Cisco Unity Connection 上啓動，以允許 PAWS-M 伺服器升級系統。

重要須知 請勿在 PAWS-M 伺服器上啓動平台管理 Web 服務。

Performance and monitoring services

Cisco Serviceability 回報工具

Cisco Serviceability 回報工具 服務能產生每日報告。 如需詳細資訊，請參閱與Serviceability報告歸檔相關的主題。

若您的組態支援叢集 (僅適用於 Unified Communications Manager) ，請在叢集中的所有 Unified Communications Manager 伺服器上安裝此服務。 回報工具 會每天根據記錄的資訊產生報告。 您可以從 Cisco Unified Serviceability的「工具」功能表存取 回報工具 產生的報告。 每個摘要報告均包含不同的圖表，這些圖表顯示該特定報告的統計資料。 服務啓動後，最多需要 24 個小時來產生報告。

相關主題

Serviceability報告封存 ，第 261 頁上的

Cisco CallManager SNMP 服務

該服務不支援 IM and Presence Service和 Cisco Unity Connection。

該服務實現了 CISCO-CCM-MIB，將適用於 Unified Communications Manager 的佈建和統計資料等資訊的存取權限提供給 SNMP。

若您的組態支援叢集 (僅適用於 Unified Communications Manager) ，請在叢集中的所有伺服器上啓動此服務。

CM 服務

本節旨在說明 CM 服務，不適用於 IM and Presence Service和 Cisco Unity Connection。

Cisco CallManager

Cisco CallManager 服務爲 Unified Communications Manager 提供純軟體的通話處理以及訊號和通話控制功能。

提示 僅適用於 Unified Communications Manager 叢集：啓動此服務之前，請確認 Unified Communications Manager 伺服器是否顯示在 Cisco Unified Communications Manager 管理的「尋找和列出 Cisco Unified Communications Manager」視窗中。 若伺服器未顯示，請先新增 Unified Communications Manager 伺服器，然後再啓動此服務。 如需尋找及新增伺服器的相關資訊，請參閱《*Cisco Unified Communications Manager* 管理指南》。

僅適用於 Unified Communications Manager 叢集：若在「服務啓動」中停用 Cisco CallManager 或 CTIManager 服務，停用服務的 Unified Communications Manager 伺服器將不再存在於資料庫中，這代表著您無法選擇該 Unified Communications Manager 伺服器在 Cisco Unified Communications Manager 管理中進行組態操作，因爲它不會顯示在圖形UI (GUI) 中。 若您隨後在同一部 Unified Communications Manager 伺服器上重新啓動服務，資料庫會再次爲 Unified Communications Manager 建立項目並在伺服器名稱或 IP 位址前新增 “CM_” 首碼。例如，若您在 IP 位址爲 172.19.140.180 的伺服器上重新啓動 Cisco CallManager 或 CTIManager 服務，則 CM_172.19.140.180 將顯示在 Cisco Unified Communications Manager 管理中。 您現在可以在 Cisco Unified Communications Manager 管理中選擇加上新 “CM_” 首碼的伺服器。

以下服務需仰賴 Cisco CallManager 服務啓動：

- CM 服務
- CDR 服務

Cisco TFTP

Cisco 簡單檔案傳輸通訊協定 (TFTP) 會建置及提供與簡單檔案傳輸通訊協定 (簡化版本的 FTP) 一致的檔案。 Cisco TFTP 可提供內嵌元件可執行檔、鈴聲檔案和裝置組態檔案。

僅限 Unified Communications Manager：組態檔案包括一份 Unified Communications Manager 清單，供裝置 (電話和閘道) 建立連線 。 裝置啓動時，元件會向動態主機組態通訊協定 (DHCP) 伺服器查詢其網路組態資訊。 DHCP 伺服器會回覆裝置的 IP 位址、子網路遮罩、預設閘道、網域名稱系統 (DNS) 伺服器位址及 TFTP 伺服器名稱或位址。 裝置會向 TFTP 伺服器要求組態檔案。 組態檔案包含 Unified Communications Manager 的清單，以及裝置連接 Unified Communications Manager 時的 TCP 連接埠。 組態檔案包含 Unified Communications Manager 的清單，以及裝置連接 Unified Communications Manager 時的 TCP 連接埠。

Cisco Messaging Interface

Cisco Messaging Interface 允許您將簡化訊息台介面 (SMDI) 相容的外部語音留言系統與 Cisco Unified Communications Manager 連結。 SMDI 爲電話系統定義了一種方法，使其能將智能處理來電所需的資訊提供給語音留言系統。

Cisco Unified 行動語音存取服務

Cisco Unified 行動語音存取服務可以啓動 Cisco Unified Mobility 內的行動語音存取功能。行動語音存取是一種整合式語音回應 (IVR) 系統，能允許 Cisco Unified Mobility 使用者執行以下任務：

- 從行動電話撥打電話，就像從桌上型電話撥打電話一樣。
- 開啓 Cisco Unified Mobility。
- 關閉 Cisco Unified Mobility。

Cisco IP 語音媒體串流應用程式

Cisco IP 語音媒體串流應用程式服務爲 Unified Communications Manager 提供語音媒體串流功能，以與終止媒體點 (MTP)、會議、待話期間背景音樂 (MOH) 和通報器一起使用。 Cisco IP 語音媒體串流應用程式能將訊息從 Unified Communications Manager 轉發到處理即時通訊協定 (RTP) 串流的 IP 語音媒體串流驅動程式。

Cisco IP 語音媒體串流 應用程式服務不會爲涉及任何 IP Voice Media Streaming 應用程式元件 (如會議、MOH、通報器或 MTP) 的通話線路產生通話管理記錄 (CMR) 檔案。

Cisco CTIManager

Cisco CTI Manager 包含與應用程式互動的 CTI 元件。 此服務允許應用程式監控或控制電話和虛擬裝置，執行通話控制功能。

僅適用於 Unified Communications Manager 叢集：使用 CTI Manager，應用程式可以存取叢集中所有 Unified Communications Manager 的資源和功能，而且可以改善容錯移轉功能。 儘管叢集中可以有一個或多個處於作用狀態的 CTI Manager，不過一部伺服器上只能存在一個 CTI Manager。 一個應用程式 (JTAPI / TAPI) 可以同時連接多個 CTI Manager，不過應用程式一次只能使用一個連線來開啓具有終止媒體功能的裝置。

Cisco Extension Mobility

此服務支援 Cisco Extension Mobility 功能，可替該功能執行登入和自動登出功能。

Cisco 已撥出號碼分析工具

Cisco 已撥出號碼分析工具服務支援 Unified Communications Manager 已撥出號碼分析工具。 啓動後，此應用程式將消耗大量資源，因此請務必在離峰時段啓動此服務 (可能會出現少量通話處理中斷)。

僅適用於 Unified Communications Manager 叢集：Cisco 不建議您在叢集中的所有伺服器上啓動此服務。 Cisco 建議您只在通話處理活動最少的其中一部叢集伺服器上啓動此服務。

Cisco 已撥出號碼分析工具伺服器

Cisco 已撥出號碼分析工具伺服器服務以及 Cisco 已撥出號碼分析工具 服務均支援 Cisco Unified Communications Manager Dialed Number Analyzer。 唯有專門用於 Cisco 已撥出號碼分析工具服務的節點需要啓動此服務。

僅適用於 Unified Communications Manager 叢集：Cisco 不建議您在叢集中的所有伺服器上啓動此服務。 Cisco 建議您只在通話處理活動最少的其中一部叢集伺服器上啓動此服務。

Cisco DHCP 監控服務

Cisco DHCP 監控服務 能監控資料庫表格中 IP 電話的 IP 位址變更。 偵測到變更時，它會修改 /etc./dhcpd.conf 檔案並重新啓動 DHCPD 守護程式。

Cisco 叢集間查詢服務

叢集間查詢服務 (ILS) 能在叢集範圍內執行。 透過 ILS，您可以建立遠端 Unified Communications Manager 叢集的網路。 ILS 叢集探索功能使 Unified Communications Manager 可以連接遠端叢集，而無需管理員手動設定每個叢集之間的連線。 ILS 全域撥號計畫複寫功能使 ILS 網路中的叢集能夠與 ILS 網路中的其他叢集交換全域撥號計畫資料。

您可以從「ILS 組態」視窗啓動 ILS，該視窗可以在 Cisco Unified Communications Manager 管理中透過選擇**進階功能** > **ILS 組態**來存取。

Cisco UserSync 服務

Cisco UserSync 服務能將 Unified Communications Manager 一般使用者表格的資料同步到 LDAP 資料庫。

Cisco UserLookup Web 服務

Cisco UserLookup Web 服務能將商業電話 (透過外部閘道的通話) 路由到受話方的備用內部號碼，以避免撥打外部號碼的商業成本。

若 Unified Communications Manager 網路中的來電者在外部號碼上撥話，Unified Communications Manager 會檢查 LDAP 資料庫中是否有被撥話方的內部號碼。 若有內部號碼，系統會將通話路由到該內部號碼。 若在 LDAP 資料庫中找不到內部號碼，系統會將通話路由到原始 (外部) 號碼。

Cisco 耳機服務

若您使用相容的 Cisco IP 電話、Cisco Jabber 或其他 Cisco 裝置，Cisco 耳機服務可讓您管理 Cisco 耳機的庫存、組態更新及診斷資料。

附註 每當 Cisco CallManager 服務執行時，都應該在所有 Unified Communications Manager 節點上啓動 Cisco 耳機服務 。 請務必在要使用 Cisco Unified CM 管理介面管理耳機的 Unified Communications Manager 節點上啓動 Cisco 耳機服務。 當您啓用 Cisco 耳機服務時，Cisco CallManager 服務將會自動啓動。 若不需 Cisco CallManager 服務，請予以停用 。

IM and Presence Service

IM and Presence Service僅適用於 IM and Presence Service。

Cisco SIP Proxy

Cisco SIP Proxy服務負責提供 SIP 註冊器和代理功能。 這包括要求路由、要求者身分辨識及傳輸互連。

Cisco Presence 引擎

Cisco Presence 引擎能使用標準型 SIP 和 SIMPLE 介面來收集、彙總與分配使用者功能和屬性。 它能收集有關使用者可用性狀態和通訊功能的資訊。

Cisco XCP 文字會議管理員

Cisco XCP 文字會議管理員支援聊天功能。 聊天功能允許使用者在線上聊天室相互溝通。 它支援使用特定 (臨時) 和永久聊天室的聊天功能，這些聊天室將保留在 Cisco 支援的外部資料庫中，直到刪除爲止。

Cisco XCP 網路連線管理員

Cisco XCP 網路連線管理員服務讓使用瀏覽器的使用者端能夠連接 IM and Presence Service。

Cisco XCP 連線管理員

Cisco Unified Presence XCP 連線管理員使 XMPP 使用者端可以連接 Cisco Unified Presence 伺服器。

Cisco XCP SIP 聯盟連線管理員

Cisco XCP SIP 聯盟連線管理員支援透過 SIP 通訊協定與 Microsoft OCS 進行網域間聯盟。 當部署含括 IM and Presence Service版本 9.0 叢集和 Cisco Unified Presence 版本 8.6 叢集間的跨叢集連線時，您亦需啓用此服務。

Cisco XCP XMPP 聯盟連線管理員

Cisco XCP XMPP 聯盟連線管理員能透過 XMPP 通訊協定支援與第三方企業 (如 IBM Lotus Sametime、Cisco Webex Meeting Center 和 GoogleTalk) 的網域間聯盟，也支援透過 XMPP 通訊協定與其他 IM and Presence Service企業的網域間聯盟。

Cisco XCP 留言封存程式

Cisco XCP 訊息封存程式服務支援 IM 合規性功能。 IM 合規性功能可以記錄傳入和傳出 IM and Presence Service伺服器的所有訊息，包括點對點訊息，以及聊天功能之特定 (臨時) 和永久聊天室的訊息。 訊息會記錄至支援 Cisco 的外部資料庫。

Cisco XCP 目錄服務

Cisco XCP 目錄服務支援 XMPP 使用者端與 LDAP 目錄的整合，以允許使用者搜尋和新增 LDAP 目錄中的聯絡人。

Cisco XCP 驗證服務

Cisco XCP 驗證服務能處理所有來自連接 IM and Presence Service之 XMPP 使用者端的驗證要求。

CTI 服務

本節說明 CTI 服務，不適用於 Cisco Unity Connection 或 IM and Presence Service。

Cisco IP Manager Assistant

此服務支援 Cisco Unified Communications Manager Assistant。 服務啓動後，Cisco Unified Communications Manager Assistant 將能使管理員與助理更有效地合作。 Cisco Unified Communications Manager Assistant 兩種運作模式：代理線路支援及共用線路支援。

該功能包括通話路由服務、管理員電話功能增強，以及主要供助理使用的桌面介面。

服務可攔截撥給管理員的電話並將其路由至選定助理、管理員或由根據預先設定通話過濾器定義的其他目標。 管理員可以動態變更通話路由。例如，透過按電話上的軟體鍵，管理員可以指示服務將所有通話路由到助理，並可以接收這些通話的狀態。

Unified Communications Manager 使用者由管理員和助理組成。 路由服務能攔截管理員通話並適當地進行路由。 助理使用者可代表管理員處理通話。

Cisco WebDialer Web 服務

適用於 Cisco Unified Communications Manager 系統的 Cisco WebDialer Web 服務

Cisco Web Dialer提供按一下撥號功能。 它允許 Unified Communications Manager 叢集內的使用者使用網頁或桌面應用程式，向叢集內外的其他使用者發起通話。 Cisco Web Dialer 提供網頁，讓叢集中的使用者可以相互通話。 Cisco Web Dialer 包含兩個元件：Web Dialer 小服務程式和重新導向程式小服務程式。

重新導向程式 小服務程式 能將使用 Cisco Web Dialer 的能力提供給第三方應用程式。 重新導向程式 小服務程式 能爲 Cisco Web Dialer 使用者找到合適的 Unified Communications Manager 叢集，並將要求重新導向該叢集中的 Cisco Web Dialer。 重新導向程式 功能僅適用於 HTTP/HTML Web Dialer 用戶端應用程式，因爲它不適用於採用簡易物件存取通訊協定 (SOAP) 的 Web Dialer 應用程式。

自我佈建 IVR

隨著自我配置 IVR 服務的導入，Unified Communications Manager 上的自動註冊 IP 電話可以更快速指派給使用者。 當您從使用 IVR 服務的使用者分機撥打「自我佈建」頁面上所設定的 CTI RP DN 時，電話會連線到自我佈建 IVR 應用程式，並提示您提供自助式認證。 IVR 服務會根據您提供之自助式認證的驗證，將自動註冊的 IP 電話指定給使用者。

即便此服務已停用，您還是可以設定自我佈建，但管理員將無法使用 IVR 服務來指定 IP 電話給使用者。 預設會停用此服務。

若要啓用自我佈建 IVR 服務，您還需啓用 Cisco CTI Manager 服務。

如需詳細資訊，請參閱 *Cisco Unified Communications Manager* 管理指南。

CDR 服務

本節描述 CDR 服務，不適用於 IM and Presence Service和 Cisco Unity Connection。

CAR Web 服務

Cisco CAR Web 服務可載入 CAR 的 UI。CAR 是一種網頁式報告應用程式，可以透過使用 CDR 資料來產生 CSV 或 PDF 報告。

Cisco SOAP - CDROnDemand 服務

Cisco SOAP-CDROnDemand 服務是在 CDR 儲存庫伺服器上執行，而且採用 SOAP/HTTPS 的服務。它能依據使用者指定的時間間隔 (最長 1 小時) 接收索取 CDR 檔案名稱清單的 SOAP 要求，並傳回符合要求中指定之持續時間的檔案名稱清單。 該服務還能接收要求傳送特定 CDR/CMR 檔案，並在要求中指定檔案名稱和傳輸方法 (SFTP/FTP、伺服器名稱、登入資訊、目錄) 的要求。

若您使用的第三方計費應用程式會透過 HTTPS/SOAP 介面存取 CDR 資料，請啓動此服務。

Unified Communications Manager 12.x 和更高版本而言，CDR onDemand 服務預設爲未啓用。 若您要啓用 CDR onDemand 服務，應手動啓動服務。 在根層級執行以下命令以啓動 CDR onDemand 服務：`/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy8443`。

安全性服務

本節說明安全服務，不適用於 IM and Presence Service和 Cisco Unity Connection。

Cisco CTL Provider

僅限 Unified Communications Manager：以本機系統帳戶權限執行的 Cisco 憑證信任清單 (CTL) 提供者，提供與使用者端外掛程式 Cisco CTL Provider Utility 搭配使用的服務，可將叢集的安全模式從不安全變更爲混合模式。 當您安裝外掛程式時，Cisco CTL Provider 服務會爲 CTL 檔案擷取叢集中所

有 Unified Communications Manager 和 Cisco TFTP 伺服器的清單，其中包含叢集中安全性權杖和伺服器的清單。

您可以安裝和配置 Cisco CTL Client 或 **utils ctl** CLI 命令集 ，然後再啓動此服務，讓整個叢集的安全模式從不安全變更爲安全。

啓動服務後，Cisco CTL Provider 服務將還原爲預設 CTL 通訊埠，即 2444。 若您想要變更連接埠，請參閱《*Cisco Unified Communications Manager* 安全性指南》以獲得詳細資訊。

Cisco 憑證授權單位代理功能 (CAPF)

搭配 Cisco 憑證授權單位代理功能 (CAPF) 應用程式，CAPF 服務可以執行以下任務，視您的組態而定：

- 向支援的 Cisco Unified IP 電話型號發行本地重要憑證。
- 升級電話上的現有憑證。
- 擷取電話憑證以進行疑難排解。
- 刪除電話中的本地重要憑證。

附註 僅限 Unified Communications Manager：當您在即時監控工具 (RTMT) 中查看即時資訊時，CAPF 服務僅顯示第一部伺服器。

目錄服務

本節說明目錄服務，不適用於 IM and Presence Service和 Cisco Unity Connection。

Cisco DirSync

Unified Communications Manager：Cisco DirSync 服務可確保 Unified Communications Manager 資料庫儲存所有使用者資訊。 若您將整合的公司目錄 (如 Microsoft Active Directory 或 Netscape/iPlanet Directory) 與 Unified Communications Manager 搭配使用，Cisco DirSync 服務會將使用者資料移轉到 Unified Communications Manager 資料庫。 Cisco DirSync 服務不同步公司目錄中的密碼。

附註 具有重複電子郵件 ID 的使用者無法同步，而且管理員不會收到有關未同步使用者清單的通知。 這些 IDS 會顯示在 Unified RTMT 的 DirSync 錯誤記錄檔中。

Cisco Unity Connection ：當 Cisco Unity Connection 與 LDAP 目錄整合時，Cisco DirSync 服務會針對 Cisco Unity Connection 伺服器上 Unified Communications Manager 資料庫中有相應資料在 LDAP 目錄中的小部分使用者資料 (名字、姓氏、別名、電話號碼等) 進行同步處理。 另一個服務 (CuCmDbEventListener) 會將 Cisco Unity Connection 使用者資料庫中的資料，與 Unified Communications Manager 資料庫中的資料同步。 對於設定完成的 Cisco Unity Connection 叢集，Cisco DirSync 服務只會在發佈者伺服器上執行。

位置型追蹤服務

本節描述位置型追蹤服務。

Cisco 無線控制器同步服務

此服務支援位置感知功能，可提供網路無線存取點和關聯的行動裝置狀態。

此服務需正在執行以將 Unified Communications Manager 與 Cisco 無線存取點控制器同步。 當服務執行且設定了同步時，Unified Communications Manager 會將其資料庫與 Cisco 無線存取點控制器同步，並儲存該控制器管理的無線存取點的狀態資訊。 您可以將同步安排爲定期進行，讓資訊保持最新狀態。

附註 新增新的 Cisco 無線存取點控制器時，請確保此服務正在執行。

語音品質報告服務

本節說明語音品質報告程式服務，不適用於 IM and Presence Service和 Cisco Unity Connection。

Cisco Extended Functions

Cisco Extended Functions 服務提供 Unified Communications Manager 語音品質功能的支援，包括品質回報工具 (QRT)。 如需各個功能的詳細資訊，請參閱《*Cisco Unified Communications Manager* 系統組態設定指南》和《*Cisco Unified Communications Manager* 的 *Cisco Unified IP* 電話管理指南》。

網路服務

自動安裝的網路服務包括系統運作所需的服務，例如資料庫和平台服務。 由於這些服務是基本功能所需的服務，因此您無法在「服務啓用」視窗中啓用它們。 例如，若基於疑難排解目的需要這些服務，您可能需要在「控制中心 - 網路服務」視窗中停止和啓動 (或重新啓動) 網路服務。

在安裝您的應用程式之後，網路服務會自動啓動，如「控制中心 - 網路服務」視窗中所述。 Serviceability GUI 會將服務分類爲邏輯群組。

效能與監控服務

Cisco CallManager Serviceability RTMT

Cisco CallManager Serviceability RTMT 小服務程式 支援 IM and Presence 即時監控工具 (RTMT)，能讓您收集和查看追蹤、查看效能監控物件、處理警示及監控系統效能和效能計數器等。

Cisco RTMT 回報工具 小服務程式

Cisco RTMT 回報工具 小服務程式 允許您發佈 RTMT 報告。

Cisco 記錄檔分割監控工具

Cisco記錄檔分割監控工具服務支援記錄檔分割監控功能，能透過使用設定的臨界值和輪詢間隔來監控節點 (或叢集中所有節點) 上記錄檔分割的硬碟使用量。

Cisco Tomcat Stats 小服務程式

Cisco Tomcat Stats 小服務程式 允許您透過使用 RTMT 或 CLI 監控 Tomcat Perfmon 計數器。 除非您懷疑此服務使用過多資源 (如 CPU 時間) ，否則請勿停止服務。

Cisco RIS 資料收集工具

即時資訊伺服器 (RIS) 能維護裝置註冊狀態、效能計數器統計資料、產生的嚴重警報等即時資訊。 Cisco RIS Data Collector 服務能爲 IM and Presence 即時監控工具 (RTMT)、SOAP 應用程式等應用程式提供介面，以便擷取儲存在叢集中所有 RIS 節點的資訊。

Cisco AMC 服務

用於即時監控工具 (RTMT)的此服務 (警報管理器和收集器服務) 允許 RTMT 擷取伺服器 (或叢集中所有伺服器) 上存在的即時資訊。

Cisco 審計事件服務

Cisco 審計事件服務能以 Unified Communications Manager 或 IM and Presence 系統爲對象，監控和記錄由使用者或使用者動作所產生的任何管理組態變更。 Cisco 審計事件服務還能監控和記錄一般使用者事件，如登入、登出及 IM 聊天室的進入和退出。

備份與還原服務

Cisco DRF Master

這不適用於 IM and Presence Service。

CiscoDRF 主代理 服務支援 DRF 主代理，能搭配災害恢復系統 GUI 或 CLI 安排備份時程、執行還原、查看相依性、檢查作業狀態，以及在必要時取消作業。 Cisco DRF 主代理 還能爲備份和還原程式提供儲存媒體。

Cisco DRF Local

Cisco DRF Local 服務支援 Cisco DRF Local Agent，負責打理 DRF 主代理 的主要工作。 元件會向 Cisco DRF Loical Agent 註冊以使用災害復原架構。 Cisco DRF Loical Agent 會執行從 Cisco DRF 主代理 接收的命令。 Cisco DRF Loical Agent 會將狀態、記錄檔和命令結果傳送到 Cisco DRF 主代理。

系統服務

Cisco CallManager Serviceability

Cisco CallManager Serviceability服務支援 Cisco Unified Serviceability 和 IM and Presence ServiceServiceability GUI，這兩者是用於排解疑難問題和管理服務的 Web 應用程式/介面。 該服務會

自動安裝，供您存取Serviceability GUI。 若您在伺服器上停止此服務，在瀏覽該伺服器時將無法存取Serviceability GUI。

Cisco CDP

Cisco Discovery Protocol (CDP) 將語音應用程式通告給其他網路管理應用程式，讓網路管理應用程式 (如 SNMP 或 Cisco Unified Operations Manager) 爲語音應用程式執行網路管理任務。

Cisco 追蹤收集小服務程式

Cisco 追蹤收集小服務程式與 Cisco 追蹤收集服務一同 支援追蹤收集，並允許使用者使用 RTMT 查看追蹤。 如果在伺服器上停止此服務，則無法在該伺服器上收集或查看追蹤。

爲了使「SysLog 檢視器」和「追蹤和記錄檔中心」在 RTMT 中執行，Cisco Trace Collection 小服務程式和 Cisco 追蹤收集服務需在伺服器上執行。

Cisco 追蹤收集服務

Cisco 追蹤收集服務與 Cisco 追蹤收集小服務程式支援追蹤收集，並允許使用者使用 RTMT 查看追蹤。 如果在伺服器上停止此服務，則無法在該伺服器上收集或查看追蹤。

爲了使「SysLog 檢視器」和「追蹤和記錄檔中心」在 RTMT 中執行，Cisco Trace Collection 小服務程式和 Cisco 追蹤收集服務需在伺服器上執行。

提示 如有必要，Cisco 建議您先重新啓動 Cisco 追蹤收集服務，再重新啓動 Cisco Trace Collection 小服務程式，縮短初始化時間。

平台服務

A Cisco DB

A Cisco DB 服務支援 Unified Communications Manager 上的 Progres 資料庫引擎。 在 IM and Presence Service上，A Cisco DB 服務支援 IDS 資料庫引擎。

A Cisco DB 複寫器

僅限 Unified Communications Manager 和 IM and Presence：A Cisco DB 複寫器服務可確保叢集中第一部伺服器和後續伺服器之間的資料庫組態和資料同步作業。

Cisco Tomcat

Cisco Tomcat 服務支援 Web 伺服器。

SNMP 主要代理

該服務能成爲代理通訊協定引擎，提供與 SNMP 要求相關的驗證、授權、存取控制和隱私功能。

提示 在Serviceability GUI 中完成 SNMP 組態後，您需在**控制中心 - 網路功能**視窗重新啓動 SNMP 主要代理服務。

MIB2 代理

此服務將 RFC 1213 中定義的變數存取權限提供給 SNMP，這些變數能讀取和寫入系統、介面和 IP 等變數。

主機資源代理

此服務將主機資訊的存取權限提供給 SNMP，如儲存資源、進度表、裝置資訊和安裝的軟體庫。 該服務實現了 HOST-RESOURCES-MIB。

原生代理配接器

此服務支援廠商管理資訊庫 (MIB)，使您可以將 SNMP 要求轉送到系統上執行的另一個 SNMP 代理。

IM and Presence Service和 Unified Communications Manager 方面，該服務若安裝在虛擬機器上，將不會存在。

系統應用程式代理

此服務將系統上安裝和執行的應用程式存取權限提供給 SNMP。 這將納入 SYSAPPL-MIB。

Cisco CDP Agent

該服務使用 Cisco Discovery Protocol 將節點上網路連線資訊的存取權限提供給 SNMP。 該服務納入了 CISCO-CDP-MIB。

Cisco Syslog 代理

該服務支援收集各種 Unified Communications Manager 元件產生的 syslog 訊息。 該服務實現 CISCO-SYSLOG-MIB。

注意 停止任何 SNMP 服務都可能會導致資料遺失，因爲網路管理系統不再監視網路。 除非您的技術支援團隊建議您這樣做，否則請勿停止服務。

Cisco 憑證變更通知

此服務可在叢集中的所有節點之間自動同步 Tomcat、CallManager 和 XMPP 等元件的憑證。 在服務停止的情況下重新產生憑證時，您需將它們手動上傳到其他節點上的憑證信任。

平台管理 Web 服務

平台管理 Web 服務是一種簡單物件存取通訊協定 (SOAP) API，可以在 Unified Communications Manager、IM and Presence Service 和 Cisco Unity Connection 上啓動，以允許 PAWS-M 伺服器升級系統。

重要須知 請勿在 PAWS-M 伺服器上啓動平台管理 Web 服務。

平台通訊 Web 服務

平台通訊 Web 服務是一種代表狀態轉接通訊協定 (REST) API，可在 Unified Communications Manager、IM and Presence Service和Cisco Unity Connection 系統上執行。

附註 您無法手動啓動或停止**平台通訊 Web 服務**。

Cisco 憑證到期監控

該服務會定期檢查系統產生之憑證的到期狀態，並在憑證即將到期時傳送通知。 Unified Communications Manager 方面，您可以在 Cisco Unified 作業系統管理中管理使用此服務的憑證。 IM and Presence Service 方面，您可以在 Cisco Unified IM and Presence 作業系統管理中管理使用此服務的憑證。

Cisco 智慧型授權管理器

Cisco 智慧型授權管理員是只在發佈者上執行的網路服務。 它能管理 Unified Communications Manager 發佈者上的所有 Cisco 智慧型授權作業。 Cisco 智慧型授權管理員服務能向 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 報告產品的授權或權利使用情況，並從 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 取得授權狀態。

安全性服務

Cisco 憑證註冊服務

此服務可在線上第三方 CA 與憑證授權單位代理功能之間建立線上連線。 若要使用具有憑證授權單位代理功能的線上 CA 來簽署 LSC 憑證，您需啓動此服務。

Cisco 信任驗證服務

IM and Presence Service不支援此服務。

Cisco 信任驗證服務是在 CallManager 伺服器或專用伺服器上執行的服務，能代表電話和其他端點驗證憑證。 它能替憑證擁有者建立角色清單的關聯。 憑證或擁有者可以與一個或多個角色建立關聯。

電話和信任驗證服務之間的通訊協定允許電話要求驗證。 信任驗證服務會驗證憑證，並傳回與憑證相關聯的角色清單。 該通訊協定允許信任驗證服務驗證要求。反之，也允許電話驗證來自信任驗證服務的回應。 該通訊協定能保護要求和回應的完整性。 要求和回應的機密性則非必要。

Cisco 信任驗證服務的多個執行個體能在叢集中的不同伺服器上執行，以提供擴充能力。 這些伺服器不一定要是託管 Cisco Unified CallManager 的伺服器。 電話能取得網路中的信任驗證服務清單，並使用選擇演算法 (如循環法) 連接其中之一。 若聯絡的信任驗證服務沒有回應，電話將切換到清單中的下一個信任驗證服務。

資料庫服務

Cisco 資料庫層監控

Cisco 資料庫層監控 服務能監控資料庫層的各個方面。 該服務能處理變更通知和監控作業。

附註 Unified Communications Manager 使用智慧型統計資料更新功能「自動更新統計資料」，它能監控資料庫表格中的變更，以及只更新需要統計資料更新的表格。此功能可節省大量頻寬，尤其是在Unified Communications Manager 的 VMware 部署上。 自動更新統計資料是預設的索引方法。

SOAP 服務

Cisco SOAP 即時服務 API

僅限 IM and Presence Service：Cisco SOAP 即時服務 API 支援使用者端登入，以及利用第三方 API 處理狀態資料。

僅限 Unified Communications Manager 和 Cisco Unity Connection：Cisco SOAP 即時服務 API 使您可以收集裝置和 CTI 應用程式的即時資訊。 該服務還提供用於啓動、開始和停止服務的 API。

Cisco SOAP 效能監控 API

Cisco SOAP 效能監控 API 服務允許您透過 SOAP API 使用效能監控計數器，監控各種應用程式。例如，您可以監控每個服務的記憶體資訊、CPU 使用率和效能監控計數器。

Cisco SOAP 記錄檔收集 API

Cisco SOAP 記錄檔收集 API 服務允許您在遠端 SFTP 伺服器上收集記錄檔案及安排記錄檔案的收集排程。 您可以收集的記錄檔案包括 syslog、核心傾印檔案和 Cisco 應用程式追蹤檔案等。

SOAP 診斷入口資料庫服務

Cisco Unified 即時監控工具 (RTMT) 使用 SOAP 診斷入口資料庫服務來存取 RTMT Analysis Manager 託管資料庫。 RTMT 能根據操作員定義的過濾器選擇來收集通話記錄。 若該服務停止，RTMT 便無法從資料庫收集通話記錄。

CM 服務

本節說明 Unified Communications Manager CM 服務，不適用於 IM and Presence Service和 Cisco Unity Connection。

Cisco CallManager 個人通訊錄

Cisco CallManager 個人通訊錄服務支援 Cisco 個人通訊錄。

在 Cisco Business Edition 5000 系統中，此服務僅支援 Cisco Unified Communications Manager。

Cisco Extension Mobility 應用程式

Cisco Extension Mobility 應用程式服務允許您定義登入設定，如 Cisco Extension Mobility 功能之電話組態上的持續時間限制。

僅限 Unified Communications Manager：Cisco Extension Mobility 功能允許 Unified Communications Manager 叢集中的使用者登入叢集中的另一部電話，將該電話臨時設定爲他們自己的電話。 使用者登入後，電話會採用個人電話號碼、快速撥號、服務連結以及其他使用者特定的屬性。 登出後，電話將採用原始的使用者設定檔。

Cisco CallManager Cisco IP 電話服務

Cisco CallManager Cisco IP 電話服務會針對您在 Cisco Unified Communications Manager 管理中設定的 Cisco Unified IP 電話服務初始化服務 URL。

在 Cisco Business Edition 5000 系統中，此服務僅支援 Cisco Unified Communications Manager。

Cisco 使用者資料服務

Cisco 使用者資料服務使 Cisco Unified IP 電話能夠存取 Cisco Unified Communications Manager 資料庫中的使用者資料。 Cisco 使用者資料服務能提供支援給 Cisco 個人通訊錄。

Cisco 推送通知服務

Cisco 推送通知服務提供從 Cisco Unified Communications Manager 傳送來電推送通知給 Apple iOS 裝置的功能。 此服務能將推送通知訊息從 Cisco CallManager 服務轉送到 Cisco Collaboration Cloud。該服務還能管理用於傳送推送通知的存取權杖。

Cisco 耳機服務

若您使用相容的 Cisco IP 電話、Cisco Jabber 或其他 Cisco 裝置，Cisco 耳機服務可讓您管理 Cisco 耳機的庫存、組態更新及診斷資料。

附註 每當 Cisco CallManager 服務執行時，都應該在所有 Unified Communications Manager 節點上啓動 Cisco 耳機服務 。 請務必在要使用 Cisco Unified CM 管理介面管理耳機的 Unified Communications Manager 節點上啓動 Cisco 耳機服務。 當您啓用 Cisco 耳機服務時，Cisco CallManager 服務將會自動啓動。若不需 Cisco CallManager 服務，請予以停用 。

IM and Presence Service 服務

IM and Presence Service 服務僅適用於 IM and Presence Service。

Cisco 登入資料庫

Cisco 登入資料庫是一個即時資料庫，用於儲存 Cisco 使用者端設定檔代理的使用者端作業階段。

Cisco 路由資料庫

Cisco 路由資料庫是一個即時資料庫，用於儲存路由資訊的快取，以及爲 Cisco SIP Proxy 和 Cisco 使用者端設定檔代理指定的使用者。

Cisco 組態代理

Cisco 組態代理是一種變更通知服務，可將 IM and Presence Service IDS 資料庫中的組態變更通知 Cisco SIP Proxy。

Cisco 同步代理

Cisco 同步代理會將 IM and Presence 資料與 Unified Communications Manager 資料保持同步。 它會針對 IM and Presence 可能會需要的資料，將 SOAP 請求傳送到 Unified Communications Manager 並訂閱 Unified Communications Manager 的變更通知，同時更新 IM and Presence IDS 資料庫。

Cisco OAM 代理

Cisco OAM 代理服務會監控 IM and Presence Service IDS 資料庫中狀態引擎感興趣的組態參數。 在資料庫中進行變更時，OAM 代理會寫入組態檔，並將 RPC 通知傳送到狀態引擎。

Cisco 用戶端設定檔代理

Cisco 使用者端設定檔代理服務使用 HTTPS 提供進出外部使用者端的安全 SOAP 介面。

Cisco 叢集間同步代理

Cisco 叢集間同步代理服務提供以下各項：Unified Communications Manager 的 DND 傳播，以及 IM and Presence Service叢集之間用於叢集間 SIP 路由的同步一般使用者資訊。

Cisco XCP 路由器

XCP 路由器是 IM and Presence Service伺服器上的核心通訊功能。 它在 IM and Presence Service上提供 XMPP 型路由功能；它將 XMPP 資料路由到 IM and Presence Service上其他作用中的 XCP 服務，而且它會存取 SDNS，以允許系統將 XMPP 資料路由到 IM and Presence Service使用者。 XCP 路由器會管理使用者的 XMPP 作業階段，並在這些作業階段來回路由 XMPP 訊息。

在安裝 IM and Presence Service之後，系統預設爲開啓 Cisco XCP 路由器。

附註 若您重新啓動 Cisco XCP 路由器，IM and Presence Service會自動重新啓動所有作用中的 XCP 服務。請注意，您需選擇重新啓動選項，才能重新啓動 Cisco XCP 路由器。這與關閉和開啓 Cisco XCP 路由器不同。 若您關閉 Cisco XCP 路由器，而不是重新啓動此服務，IM and Presence Service會停止所有其他 XCP 服務。 隨後，當您開啓 XCP 路由器時，IM and Presence Service不會自動開啓其他 XCP 服務；您需要手動開啓其他 XCP 服務。

Cisco XCP 組態管理員

Cisco XCP 組態管理員會監控透過管理 GUI 進行的組態和系統拓撲變更 (以及從叢集間對等同步的拓撲變更)，這些變更會影響其他 XCP 元件 (例如，路由器和訊息封存器)，並視需要更新這些元件。Cisco XCP 組態管理員服務會爲管理員建立通知，指出 XCP 元件何時需要重新啓動 (由於這些變更)，並在重新啓動完成後自動清除通知。

Cisco 伺服器復原管理員

Cisco 伺服器復原管理員 (SRM) 服務會管理狀態備援群組中節點之間的容錯移轉。 SRM 會管理節點中的所有狀態變更；狀態變更是自動的，或由管理員起始 (手動)。 一旦開啓狀態備援群組中的高可用性，每個節點上的 SRM 就會與對等節點建立活動訊號連線，並開始監控關鍵程式。

Cisco IM and Presence 資料監控器

Cisco IM and Presence 資料監控器會監控 IM and Presence Service上的 IDS 複寫狀態。 其他 IM and Presence Service取決於 Cisco IM and Presence 資料監控器。 這些相關服務會使用 Cisco 服務，將啓動延遲到 IDS 複寫處於穩定狀態。

Cisco IM and Presence 資料監控器亦會檢查來自 Unified Communications Manager 的 Cisco 同步代理同步狀態。 相關的服務僅允許在 IDS 複寫已設定，且 IM and Presence 資料庫發佈者節點上的同步代理已完成從 Unified Communications Manager 同步之後啓動。 逾時之後，即使 IDS 複製及Sync Agent 尚未完成，發佈者節點上的 Cisco IM and Presence 資料監控器將允許相關服務啓動。

訂閱者節點上，Cisco IM and Presence 資料監控器延遲功能服務的啓動，直到成功建立 IDS 複製。Cisco IM and Presence 資料監控器僅延遲叢集中問題訂閱者節點上功能服務的啓動，由於只有一個問題節點，它不會延遲所有訂閱者節點上功能服務的啓動。 例如，若在 node1 及 node2 而不是在 node3 成功地建立 IDS 複製，Cisco IM and Presence 資料監控器可讓功能服務在 node1 及 node2 上啓動，但延遲功能服務則在 node3 上啓動。

Cisco Presence 資料庫

Cisco Presence 資料庫是用於儲存臨時狀態資料和訂閱的即時資料庫。

Cisco SIP 註冊資料庫

Cisco Presence SIP 註冊資料庫是用於儲存 SIP 註冊資料的即時資料庫。

Cisco RCC 裝置選擇

Cisco RCC 裝置選擇服務是用於遠端通話控制的 Cisco IM and Presence 使用者裝置選擇服務。

CDR 服務

本節描述 CDR 服務，不適用於 IM and Presence Service和 Cisco Unity Connection。

Cisco CDR Repository Manager

此服務能維護及移動從 Cisco CDR Agent 服務取得及產生的詳細通話記錄 (CDR)。 在支援叢集的系統中 (僅適用於 Unified Communications Manager) ，該服務位於第一部伺服器上。

Cisco CDR Agent

附註 Unified Communications Manager 能在 Cisco Unified Communications Manager 系統中支援 Cisco CDR Agent。

該服務不支援 IM and Presence Service和 Cisco Unity Connection。

Cisco CDR Agent 服務能將 Unified Communications Manager 產生的 CDR 和 CMR 檔案從本機主機傳輸到 CDR 儲存庫伺服器，其中 CDR Repository Manager 服務能通過 SFTP 連線執行。

此服務能將本機主機產生的 CDR 和 CMR 檔案傳輸到叢集中的 CDR 儲存庫伺服器。 CDR 儲存庫節點獨立伺服器中的CDR Agent，能透過SFTP連線將獨立伺服器產生的檔案傳輸到Cisco CDR Repository Manager。 CDR Agent 能維護及移動檔案。

爲了使該服務發揮功用，請在伺服器上啓動 Cisco CallManager 服務並確保其正在執行。 若您的組態支援叢集 (僅適用於 Unified Communications Manager) ，請在第一部伺服器上啓動 Cisco CallManager 服務。

Cisco CAR Scheduler

Cisco CDR 分析和回報 (CAR) Scheduler 服務不支援IM and Presence Service和Cisco Unity Connection。

Cisco CAR Scheduler 服務允許您安排與 CAR 相關的任務。例如，您可以安排報告產生或將 CDR 檔案載入 CAR 資料庫的時程。

Cisco SOAP-CallRecord 服務

預設情況下，Cisco SOAP-CallRecord 服務會在發佈者上作爲 SOAP 伺服器執行，因此使用者端可以通過 SOAP API 連接 CAR 資料庫。 這種連線是透過使用 CAR 連接器 (有單獨 CAR IDS 執行個體) 實現的。

Cisco CAR DB

Cisco CAR DB 能管理 CAR 資料庫的 Informix 執行個體，使 Service Manager 可以啓動或停止該服務，以及分別啓動或關閉 CAR IDS 執行個體。 這與用於維護 CCM IDS 執行個體的 Unified Communications Manager 資料庫相似。

預設情況下，Cisco CAR DB 服務會在發佈者上啓動 。 CAR DB 執行個體已安裝並在發佈者伺服器上主動執行，以維護 CAR 資料庫。 此網路服務只能在發佈者上使用，無法在訂閱者上使用。

管理服務

本節介紹管理服務，不適用於 Cisco Unity Connection。

Cisco CallManager 管理

IM and Presence Service和 Cisco Unity Connection 不支援 Cisco CallManager 管理服務。

Cisco CallManager 管理服務支援 Cisco Unified Communications Manager 管理，也就是您用來配置 Unified Communications Manager 設定的 Web 應用程式/介面。 安裝 Unified Communications Manager 之後，此服務將自動啓動，並允許您存取圖形UI (GUI)。 若您停止此服務，便無法在瀏覽該伺服器時存取 Cisco Unified Communications Manager 管理圖形UI 。

Cisco IM and Presence 管理員

Unified Communications Manager 和 Cisco Unity Connection 不支援 Cisco IM and Presence 管理服務。

Cisco IM and Presence 管理服務支援 Cisco Unified Communications Manager IM and Presence 管理，也就是您用來配置 IM and Presence Service設定的 Web 應用程式/介面。 安裝 IM and Presence Service之後，此服務會自動啓動，並允許您存取GUI。若您停止此服務，便無法在瀏覽該伺服器時存取Cisco Unified Communications Manager IM and Presence 管理 GUI。

Services setup

控制中心

在 Serviceability GUI 中的控制中心，您可以檢視狀態並一次啓動和停止一項服務。 若要啓動、停止和重新啓動網路服務，請存取「控制中心 - 網路服務」視窗。若要啓動、停止和重新啓動功能服務，請存取「控制中心 - 功能服務」視窗。

提示 使用「相關連結」下拉式清單方塊和「執行」按鈕，導覽到「控制中心」和「服務啓動」視窗。

僅限 Unified Communications Manager 和 IM and Presence：在叢集組態中，您可以檢視狀態，以及一次爲叢集中的一部伺服器啓動和停止服務。

僅限 Unified Communications Manager：啓動和停止功能服務會導致目前註冊到該服務的所有 Cisco Unified IP 電話和閘道失效，由其次要服務接手。 裝置和電話僅在無法向次要服務註冊時才需要重新啓動。 啓動和停止服務可能會導致其他已安裝並移至該 Unified Communications Manager 的應用程式 (例如會議橋接器或 Cisco Messaging Interface) 一併啓動和停止。

注意 僅限 Unified Communications Manager：停止服務也會停止該服務控制之所有裝置的通話處理。 服務停止後，從IP電話到另一IP電話的通話會保持啓動狀態；從IP電話到媒體閘道控制通訊協定 (MGCP) 閘道的進行中通話也會保持啓動狀態，但是其他類型的通話則會遭到捨棄。

設定服務

使用服務時，您可以執行以下任務：

程序

步驟 1 啓動您想要執行的功能服務。

步驟 2 設定適當的服務參數。

步驟 3 如有必要，請使用Serviceability GUI 追蹤工具對問題進行疑難排解。

服務啟動

附註 您可以啓用或停用多個功能服務，或從Serviceability GUI 中的「服務啓用」視窗中選擇要啓用的預設服務。 您可以從 IM and Presence 節點檢視、啓動和停止 Unified Communications Manager 服務，反之亦然。 您可能會遇到以下錯誤：「無法建立與伺服器的連線(無法存取遠端節點) 」。 若出現此錯誤訊息，請參閱 *Cisco Unified Communications Manager* 管理指南。

附註 從 Unified Communications Manager 6.1.1 版開始，一般使用者將再也無法存取 Cisco Unified Serviceability，以啓動和停止服務。

功能服務是以自動模式啓用，並且Serviceability GUI 會根據單一節點組態檢查是否有服務相依性。 當您選擇啓用功能服務時，系統會提示您選擇所有其他依賴該服務執行的服務 (若有的話)。 當您按一下**設定預設值**時，Serviceability GUI 會選擇要在伺服器上執行所需的那些服務。

僅限 Unified Communications Manager 和 IM and Presence Service：即使在支援叢集的組態中，此程式也是基於單一伺服器組態。

啓用服務會自動啓動服務。 您可以從控制中心啓動和停止服務。

Cisco Unified Communications Manager 的叢集服務啟動建議

在叢集中啓動服務之前，請查看下表提供的多伺服器 Unified Communications Manager 組態服務建議。

***表 34: Cisco Unified Communications Manager* 服務啟動建議**

服務/小服務程式	啟動建議
CM 服務	

服務/小服務程式	啟動建議
Cisco CallManager	該服務支援 Unified Communications Manager。 在「控制中心-網路服務」中，確認 Cisco RIS Data Collector 服務和資料庫層監聽在節點上執行。 **提示** 啟動此服務之前，請確認 Unified Communications Manager 伺服器是否顯示在 Unified Communications Manager 管理的 Unified Communications Manager「列示」視窗中。 若伺服器未顯示，請先新增 Unified Communications Mana 服器，然後再啟動此服務。 如需新增伺服器的相關資訊，請參閱《*Cisco Unified Communications Mana* 統組態設定指南》。
Cisco Messaging Interface	唯有使用透過伺服器連接的 USB 到序列配接器將 SMDI 與第三方語音信箱系統整啟動。
Cisco Unified 行動語音存取服務	若要使行動語音存取正常運作，您需先設定 H.323 閘道，使其指向第一個 VXML 之後在叢集的第一個節點上啟動此服務。 另外，請確認 Cisco CallManager 和 Cisc 服務在叢集中的某一部伺服器上執行，不一定要與執行 Cisco Unified 行動語音存的伺服器相同。
Cisco IP 語音媒體串流應用程式	若叢集中有多個節點，請在每個叢集的一或兩部伺服器上啟動。 您可以在待話期音樂的專用節點上啟動。 此服務要求您在叢集中的某個節點上啟動 Cisco TFTP。第一個節點或執行 Cisco CallManager 服務的任何節點上啟動此服務。
Cisco CTIManager	在 JTAPI/TAPI 應用程式將連接的每個節點上啟動。 CTIManager 啟動還需要在節動 Cisco CallManager 服務。 如需 CTIManager 和 Cisco CallManager 服務互動的詳訊，請參閱與 CM 服務相關的主題。
Cisco Extension Mobility	在叢集中的所有節點上啟動。
Cisco Extended Functions	在執行 Cisco RIS 資料收集工具的一或多部伺服器上啟動此服務，該服務支援品質具 (QRT)。 請務必在叢集中的節點上啟動 Cisco CTIManager 服務。
Cisco DHCP 監控服務	啓用 DHCP 監控服務後，它會偵測資料庫中影響 IP 電話 IP 位址的變更、修改 /etc/dhcpd.conf 檔案，以及使用更新的組態檔案停止和重新啓動 DHCPD 守護程式啓用 DHCP 的節點上啓動此服務。
Cisco 位置頻寬管理器	若您計劃使用 Cisco 位置通話許可控制功能來管理音訊和視訊通話的頻寬配置，此服務。 該服務能與 Cisco CallManager 服務搭配使用。 建議您在執行 Cisco CallM 服務的同一伺服器上執行 Cisco 位置頻寬管理器。 若位置頻寬管理器與 CallMana 務不在同一部伺服器上執行，請確認位置頻寬管理器群組的設定是否正確。
Cisco 叢集間查詢服務	若您計劃在多個 Unified Communications Manager 叢集之間傳播 URI 和數值路由資在參與此交換的叢集發佈者上啓動此服務。
Cisco 已撥出號碼分析工具伺服器	若叢集中有多個節點，請在 Cisco 已撥出號碼分析工具服務的某一個專用節點上服務。

服務/小服務程式	啟動建議
Cisco 已撥出號碼分析工具	若您打算使用 Unified Communications Manager 已撥出號碼分析工具，請啓動此服務該服務可能會消耗大量資源，因此請在通話處理活動最少的節點上或在離峰時段啓動服務。
Cisco TFTP	若叢集中有多個節點，請在Cisco TFTP服務的某一個專用節點上啓動此服務。 若您在集中的多個節點上啓動此服務，請設定選項 150。
Cisco 耳機服務	若您計劃從 Unified Communications Manager 管理 Cisco 耳機，請啓動此服務。 附註 每當 Cisco CallManager 服務執行時，都應該在所有 Unified Communications Mana節點上啓動 Cisco 耳機服務 。 請務必在要使用 Cisco Unified CM 管理介面管理機的 Unified Communications Manager 節點上啓動 Cisco 耳機服務。 當您啓用 Ci耳機服務時，Cisco CallManager 服務將會自動啓動。 若不需 Cisco CallManag服務，請予以停用 。
CTI 服務	
Cisco IP Manager Assistant	若您打算使用 Cisco Unified Communications Manager Assistant，請在叢集中的任兩部伺器 (主要和備份) 上啓動此服務。 確認 Cisco CTI Manager 服務已在叢集中啓動 。 如需 Cisco IP Manager Assistant 的詳細資料，請參閱 *Cisco Unified Communications Man* 功能設定指南。
Cisco WebDialer Web 服務	在每個叢集的某一個節點上啓動。
自我佈建 IVR	若要啓用自我佈建 IVR 服務，您還需啓用 Cisco CTI Manager 服務。 即便此服務已停用，您還是可以設定自我佈建，但管理員將無法使用 IVR 服務來指定電話給使用者。 預設會停用此服務。
CDR 服務	
Cisco SOAP-CDROnDemand 服務	您只能在第一部伺服器上啓動 Cisco SOAP-CDROnDemand 服務，而且 Cisco CDR Repos Manager 和 Cisco CDR Agent 服務需在同一部伺服器上執行。 Unified Communications Manager 12.x 和更高版本而言，CDR onDemand 服務預設爲未用。 若您要啓用 CDR onDemand 服務，應手動啓動服務。 在根層級執行以下命令以動 CDR onDemand 服務：`/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy84`
Cisco CAR Web 服務	您只能在第一部伺服器上啓動 Cisco CAR Web 服務，而且 Cisco CAR Scheduler 服務需啓動並在同一部伺服器上執行，此外，CDR存放庫管理員服務也需在同一部伺服器上行。
資料庫與管理服務	

服務/小服務程式	啟動建議
Cisco AXL Web 服務	安裝後，Cisco AXL Web 服務在所有叢集節點上預設爲啓用 。 Cisco 建議您一律 者節點上保持服務啓動狀態。 這樣能確保您可以設定依賴 AXL 的產品，例如 Un Provisioning Manager。 根據您的需要，您可以在特定訂閱者節點上，於 Cisco Unified Serviceability的「工 務」下啓動或停用服務。
Cisco 批量佈建服務	您只能在第一個節點上啓動 Cisco 批量佈建服務。 若您使用批量管理工具 (BAT) 話和使用者，需啓動此服務。
Cisco UXL Web 服務	此服務能執行驗證和使用者授權檢查。 Cisco IP 電話通訊錄同步工具中的 TabSyn 者端使用 Cisco UXL Web 服務來查詢 Cisco Unified Communications Manager 資料 若您計劃使用 Cisco IP 電話通訊錄同步工具，需在某一個節點 (最好是發佈者) 上 服務。 若您不使用 Cisco IP 電話通訊錄同步工具，Cisco 建議您停用此服務。 預 用此服務。
Cisco 平台管理 Web 服務	若您計劃使用 Cisco Prime Collaboration Deployment (PCD) 伺服器來管理升級、切 本、重新啓動或重新分配地址作業，需啓動此服務。 平台管理 Web 服務 (PAWS) 在通話管理員和 Prime Collaboration Deployment (PCD) 之間進行 SOAP 通訊。 若 有多個節點，您需在叢集中的每部伺服器上啓動此服務。
Cisco TAPS 服務	使用 Cisco Unified Communications Manager 自動註冊電話工具之前，您需在第一 上啓動此服務。 當您建立 Cisco Unified Communications Manager 自動註冊電話工 MAC 位址時，請務必在同一個節點上啓動 Cisco 批量佈建服務。
效能與監控服務	
Cisco Serviceability 回報工具	僅在第一個節點上啓動。 **附註** 即使您在其他節點上啓動服務，該服務也只會在第一個節點上產生報告。
Cisco CallManager SNMP 服務	若您使用 SNMP，請在叢集中的所有伺服器上啓動此服務。
安全性服務	
Cisco CTL Provider	在叢集中的所有伺服器上啓動。
Cisco 憑證授權單位代理功能 (CAPF)	僅在第一個節點上啓動。
目錄服務	
Cisco DirSync	僅在第一個節點上啓動。

IM and Presence Service的叢集服務啟動建議

⚠

注意 在開啓功能的任何服務之前，您需爲該功能完成 IM and Presence 上的所有必要組態。 請參閱每個 IM and Presence 功能的相關檔案。

在開啓叢集中的服務之前，請檢閱下表，其中爲多節點 IM and Presence 組態提供服務建議。

表 *35: IM and Presence Service*啟動建議

服務/小服務程式	行動
資料庫與管理服務	
Cisco AXL Web 服務	安裝後，Cisco AXL Web 服務在所有叢集節點上預設爲啓用 。 Cisco 建議您一律在 IM and Presence Service資料庫發佈者節點上保持服務啓動狀態。 這樣能確保您可以設定依賴 AXL 的產品。若設定叢集間通信，則需在設定爲遠端對等同步來源的子叢集中的兩個節點上啓用此服務。若未在兩個節點上啓用此服務，則在容錯移轉案例中，將失去狀態和 IM 功能。 根據您的需要，您可以在特定 IM and Presence 訂閱者節點上，於 Cisco Unified Serviceability的「功能服務」下啓動或停用服務。
Cisco 批量佈建服務	• 您僅在第一個節點上開啓 Cisco 批量佈建服務。 • 若使用批量管理工具 (BAT) 來管理使用者，則需開啓此服務。
效能與監控服務	
Cisco Serviceability 回報工具	僅在發佈者節點上開啓此服務。 **附註** 即使您在其他節點上開啓服務，該服務也只會在發佈者節點上產生報告。
IM and Presence Service	
Cisco SIP Proxy	在叢集中的所有節點上開啓此服務。
Cisco Presence 引擎	在叢集中的所有節點上開啓此服務。
Cisco 同步代理	在叢集中的所有節點上開啓此服務。

服務/小服務程式	行動
Cisco XCP 文字會議管理員	• 若您在 IM and Presence 上部署聊天功能，請開啓此服務。 • 在執行聊天功能的每個節點上開啓此服務。 附註 永久聊天功能需要外部資料庫。 若啓用永久聊天功能，則還需在啓動文字會議管理員服務之前設定外部資料庫。 若啓用永久聊天功能，但未設定外部資料庫，則文字會議管理員服務將不會啓動。 請參閱 *IM and Presence* 的資料庫設定指南 *Unified Communications Manager*。
Cisco XCP 網路連線管理員	• 若您整合 Web 使用者端與 IM and Presence，請開啓此服務。 • 在叢集中的所有節點上開啓此服務。
Cisco XCP 連線管理員	• 若您整合 XMPP 使用者端與 IM and Presence，請開啓此服務。 • 在叢集中的所有節點上開啓此服務。
Cisco XCP SIP 聯盟連線管理員	若部署以下任何組態，請開啓此服務： • 透過 IM and Presence 上 SIP 通訊協定的網域間聯盟。在執行 SIP 聯盟的每個節點上開啓此服務。 • IM and Presence 9.x 版叢集與 Cisco Unified Presence 8.6(x) 版叢集之間的叢集間部署。在 9.x 版叢集中的所有節點上開啓此服務。
Cisco XCP XMPP 聯盟連線管理員	• 僅在透過 IM and Presence 上的 XMPP 通訊協定部署網域間聯盟時，才開啓此服務。 • 在執行 XMPP 聯盟的每個節點上開啓此服務。 附註 在節點上開啓 XMPP 聯盟連線管理員服務之前，需在該節點上開啓 Cisco Unified Communications Manager IM and Presence 管理中的 XMPP 聯盟。 請參閱 *IM and Presence* 的網域間聯盟*Unified Communications Manager*。

服務/小服務程式	行動
Cisco XCP 留言封存程式	• 若您在 IM and Presence 上部署合規功能，請開啓此服務。 • 在執行 IM 合規功能的任何節點上開啓此服務。 附註 若在設定外部資料庫之前開啓訊息封存器，則服務將不會啓動。 另外，若無法連接外部資料庫，則服務將不會啓動。 請參閱 *IM and Presence* 的資料庫設定指南*Unified Communications Manager*。
Cisco XCP 目錄服務	• 若您將 IM and Presence 上的 XMPP 使用者端與 LDAP 目錄進行整合，請開啓此服務。 • 在叢集中的所有節點上開啓此服務。 附註 若在設定第三方 XMPP 使用者端的 LDAP 聯絡人搜尋設定之前開啓目錄服務，則服務將啓動，然後再次停止。 請參閱 *Unified Communications Manager* 上 *IM and Presence Service*的組態和管理。
Cisco XCP 驗證服務	• 若您整合 XMPP 使用者端與 IM and Presence，請開啓此服務。 • 在叢集中的所有節點上開啓此服務。

啟動功能服務

您可以在Serviceability GUI 中的**服務啟動**視窗中，啓動和停用功能服務。 顯示在**服務啟動**視窗中的服務在啓動之前不會啓動。

您只能啓動和停用功能服務 (而不是網路服務)。 您可以同時啓動或停用任意數量的服務。 某些功能服務依賴於其他服務，並且相關服務會在功能服務啓動之前被啓動。

提示 僅限 Unified Communications Manager 和 IM and Presence Service：在服務啓動視窗中啓動服務之前，請查看與叢集服務啓動建議相關的主題。

程序

步驟 1 選擇**工具** > **服務啟用**。

隨即顯示**服務啟用** (Service Activation) 視窗。

步驟 2 從**伺服器**下拉式清單中選擇伺服器 (節點) ，然後按一下**執行**。

您可以從以下位置存取 Unified Communications Manager 服務：IM and Presence Service 節點，反之亦然。 嘗試存取遠端節點時，可能會遇到以下錯誤：「無法建立到伺服器的連線 (無法連線到遠端節點) 」。 若出現此錯誤訊息，請參閱 *Cisco Unified Communications Manager* 管理指南。

步驟 3 執行以下動作之一以開啓或關閉服務：

a) 要開啓在單一伺服器上執行所需的預設服務，請選擇**設定為預設值**。

附註　此選項根據單一伺服器的組態選擇預設服務，並檢查服務相依性。

b) 要開啓所有服務，請勾選**檢查所有服務**。
c) 要開啓特定服務，請勾選您要開啓的服務的方塊
d) 要開啓特定服務，請勾選您要開啓的服務的方塊。

步驟 4 僅適用於 Unified Communications Manager 和 IM and Presence Service：叢集組態而言，請檢閱叢集服務啓動建議，然後勾選要啓動的服務旁邊的方塊。

步驟 5 勾選要啓用的服務的方塊後，按一下**儲存**。

提示　要停用已啓用的服務，請取消勾選要停用的服務旁的方塊；然後再按一下**儲存**。

提示　要取得服務的最新狀態，請按一下**重新整理**按鈕。

相關主題

Cisco Unified Communications Manager 的叢集服務啓動建議 ，第 200 頁上的
IM and Presence Service的叢集服務啓動建議 ，第 204 頁上的

在控制中心或 CLI 中啟動、停止和重新啟動服務

爲了執行這些任務，Serviceability GUI 提供兩個控制中心視窗。 若要啓動、停止和重新啓動網路服務，請存取**控制中心 - 網路服務**視窗。 若要啓動、停止和重新啓動功能服務，請存取**控制中心 - 功能服務**視窗。

提示　使用**相關連結**清單方塊和**執行**按鈕，導覽到「控制中心」和「服務啓動」視窗。

在控制中心啟動、停止和重新啟動服務

Serviceability GUI 中的控制中心允許您：

- 檢視狀態
- 重新整理狀態
- 啓動、停止和重新啓動特定伺服器上的功能和網路服務，或叢集組態中叢集內伺服器的功能和網路服務

服務停止時，直到服務停止後才能啓動。

⚠

注意 僅限 Unified Communications Manager：停止服務也會停止該服務控制之所有裝置的通話處理。 服務停止後，從 IP 電話到另一 IP 電話的通話會保持連線；從 IP 電話到媒體閘道控制通訊協定 (MGCP) 閘道的進行中通話也會保持連線，但是其他類型的通話則會遭到捨棄。

程序

步驟 1 根據您要啟動/停止/重新啟動/重新整理的服務類型，執行下列其中一項任務：

- 選擇**工具** > **控制中心 - 功能服務**。

  提示 需先啟動功能服務，然後才能啟動、停止或重新啟動它。

- 選擇**工具** > **控制中心 - 網路服務**。

步驟 2 在伺服器下拉式清單中選擇伺服器，然後按一下**執行**。

視窗即會顯示以下項目：

- 您選擇的伺服器的服務名稱。
- 服務群組。
- 服務狀態，例如 Started、Running、Not Running 等等。 (狀態欄)。
- 服務開始執行的確切時間。 (開始時間欄)。
- 服務已執行的時間量。 (啟動時間欄)。

步驟 3 您可以執行下列一項作業：

- 按一下您要啟動的服務旁邊的單選按鈕，然後按一下**啟動**。 狀態即會變更以反映更新的狀態。
- 按一下您要停止的服務旁邊的單選按鈕，然後按一下**停止**。 狀態即會變更以反映更新的狀態。
- 按一下您要重新啟動的服務旁的單選按鈕，然後按一下**重新啟動**。 訊息指出重新動可能需要一些時間。 按一下**確定**。
- 按一下**重新整理**以取得服務的最新狀態。
- 若要移至**服務啟用**視窗，或移至其他控制中心視窗，請從相關連結下拉式清單選擇選項，然後按一下**執行**。

使用命令行介面啟動、停止和重新啟動服務

您可以透過 CLI 啟動和停止某些服務。 如需您可以透過 CLI 啟動和停止的服務清單，以及如何執行這些任務的相關資訊，請參閱 *Cisco Unified* 解決方案命令行介面參考指南。

提示 您需從Serviceability GUI 中的控制中心啓動和停止大多數服務。

第 16 章

追蹤

追蹤

Cisco Unified Serviceability提供追蹤工具，以協助您疑難排解語音應用程式的問題。 Cisco Unified Serviceability支援 SDI (系統診斷介面) 追蹤、SDL (訊號通訊群組層) 追蹤 (若爲 Cisco CallManager 和 Cisco CTIManager 服務，僅適用於 Unified Communications Manager) 和 Log4J 追蹤 (若爲 Java 應用程式)。

您可以使用「追蹤組態」視窗，來指定要追蹤的資訊層級，以及要納入每個追蹤檔案中的資訊類型。

僅限 Unified Communications Manager：若服務是通話處理應用程式，例如 Cisco CallManager 或 Cisco CTIManager，則您可以在裝置 (例如電話和閘道) 上設定追蹤。

僅限 Unified Communications Manager 和：在「警報組態」視窗中，您可以將警報引導至各個位置，包括 SDL 追蹤記錄檔。 若您想要這樣做，可以在 Cisco Unified 即時監控工具 (Unified RTMT) 中設定警示的追蹤。

在您設定要納入各種服務之追蹤檔案中的資訊之後，您可以使用 Cisco Unified 即時監控工具 中的「追蹤和記錄中心」選項來收集及檢視追蹤檔案。

Cisco Unified IM and Presence Serviceability提供追蹤工具，以協助您疑難排解即時訊息和狀態應用程式的問題。 Cisco Unified IM and Presence Serviceability支援：

- SDI 追蹤
- Log4J 追蹤 (若爲 Java 應用程式)

您可以設定要追蹤的資訊層級 (除錯層級) 、要追蹤的資訊 (追蹤欄位) ，以及追蹤檔案的相關資訊 (例如，每項服務的檔案數、檔案大小，以及資料儲存在追蹤檔案中的時間)。 您可以設定單一服務的追蹤，也可以將該服務的追蹤設定套用至叢集中的所有伺服器。

在**報警組態**視窗中，您可以將警報引導至各個位置。 若您想要這樣做，可以在 IM and Presence Unified RTMT 中設定警示的追蹤。

在您設定要納入各種服務之追蹤檔案中的資訊之後，您可以使用 Unified RTMT 中的「追蹤和記錄中心」選項來收集及檢視追蹤檔案。 您可以爲可在叢集中任何 IM and Presence 節點上使用的任何功能

或網路服務設定追蹤參數。使用**追蹤組態**視窗，指定要追蹤以疑難排解問題的參數。若想要使用預定的疑難排解追蹤設定，而不是選擇自己的追蹤欄位，則您可以使用**疑難排解追蹤設定**視窗。

附註 啓用追蹤會降低系統效能，請務必僅爲疑難排解之目的啓用追蹤。 如需使用追蹤方面的協助，請聯絡 Cisco 技術協助中心 (TAC)。

追蹤組態

您可以爲Serviceability介面中顯示的任何功能或網路服務設定追蹤參數。 若有叢集，則您可以爲可在叢集中任何伺服器上使用的任何功能或網路服務設定追蹤參數。 使用追蹤組態視窗，指定要追蹤以疑難排解問題的參數。

您可以設定要追蹤的資訊層級 (除錯層級) 、要追蹤的資訊 (追蹤欄位) ，以及追蹤檔案的相關資訊 (例如，每項服務的檔案數、檔案大小，以及資料儲存在追蹤檔案中的時間)。 若具有叢集，則您可以設定單一服務的追蹤，也可以將該服務的追蹤設定套用至叢集中的所有伺服器。

若想要使用預定的疑難排解追蹤設定，而不是選擇自己的追蹤欄位，則您可以使用「疑難排解追蹤設定」視窗。 如需疑難排解追蹤的詳細資訊，請參閱追蹤設定。

在您設定要納入各種服務之追蹤檔案中的資訊之後，您可以使用 Unified RTMT 中的追蹤和記錄中心選項來收集追蹤檔案。 如需有關追蹤收集的詳細資訊，請參閱追蹤收集。

追蹤設定

「疑難排解追蹤設定」視窗允許您選擇要爲其設定預定疑難排解追蹤設定的服務。 在此視窗中，您可以選擇單一或多個服務，然後將這些服務的追蹤設定變更爲預定的追蹤設定。 若您有叢集，則可以在叢集中的不同伺服器上選擇服務，讓所選服務的追蹤設定變更爲預定的追蹤設定。 您可以選擇單一伺服器的特定啓動服務、伺服器的所有啓動服務、叢集中所有伺服器的特定啓動服務，或叢集中所有伺服器的所有啓動服務。 在視窗中，N/A 顯示在非作用中服務旁邊。

附註 功能或網路服務的預定疑難排解追蹤設定包括 SDL、SDI 和 Log4j 追蹤設定。 在套用疑難排解追蹤設定之前，系統會備份原始追蹤設定。 重設疑難排解追蹤設定時，會還原原始疑難排解。

將疑難排解追蹤設定套用至服務之後，若開啓「疑難排解追蹤設定」視窗，您爲疑難排解設定的服務會顯示爲勾選狀態。 在「疑難排解追蹤設定」視窗中，您可以將追蹤設定重設爲原始設定。

在將疑難排解追蹤設定套用至服務之後，「追蹤設定」視窗會顯示一則訊息，指出已爲該服務設定疑難排解追蹤。 若要重設服務的設定，您可以從「相關連結」下拉式清單方塊中選擇「疑難排解追蹤設定」選項。 該服務而言，「追蹤組態」視窗會將所有設定顯示爲唯讀，但追蹤輸出設定的部分參數 (例如檔案數上限) 除外。 即使在套用疑難排解追蹤設定之後，也可以修改這些參數。

追蹤收集

使用追蹤和記錄檔中心 (Cisco Unified 即時監控工具中的選項) ，來收集、檢視和壓縮各種服務追蹤或其他記錄檔。 搭配追蹤和記錄檔中心選項，您可以收集 SDL/SDI 追蹤、應用程式記錄檔、系統記錄檔 (例如事件檢視應用程式、安全性和系統記錄檔) 和損毀傾印檔案。

提示 不要使用 Windows 記事本來檢視收集的追蹤檔案，因爲 Windows 記事本無法適當地顯示換行符號。

附註 僅限 Unified Communications Manager：對於支援加密的裝置，安全即時傳輸通訊協定 (SRTP) 金鑰資料不會顯示在追蹤檔案中。

如需追蹤收集的詳細資訊，請參閱 *Cisco Unified* 即時監控工具管理指南。

被撥話方追蹤

「被撥話方追蹤」可讓您設定您想要追蹤的目錄號碼或目錄號碼清單。 您可以使用作業階段追蹤工具來要求以隨選方式追蹤通話。

如需詳細資訊，請參閱 *Cisco Unified* 即時監控工具管理指南。

設定追蹤組態

以下程式概述了爲Serviceability介面中的功能和網路服務設定和收集追蹤的步驟。

程序

步驟 1 執行下列其中一個步驟，設定「TLC 節流 CPU 目標」和「TLC 節流 IOWait 目標」服務參數 (Cisco RIS Data Collector 服務) 的值：

- Cisco Unified Communications Manager 管理和 Cisco Unified IM and Presence ：選擇 **系統** > **服務參數**，然後設定「TLC 節流 CPU 目標」和「TLC 節流 IOWait 目標」服務參數 (Cisco RIS Data Collector 服務) 的值。
- 僅限 Cisco Unity Connection：選擇 Cisco Unity Connection 管理中的**系統設定** > **服務參數**，然後設定「TLC 節流 CPU 目標」和「TLC 節流 IOWait 目標」服務參數 (Cisco RIS Data Collector 服務) 的值。

步驟 2 爲要爲其收集追蹤的服務設定追蹤設定。 若具有叢集，則您可以在叢集中的某部伺服器或所有伺服器上設定服務的追蹤。

若要設定追蹤設定，請選擇除錯層級和追蹤欄位，來選擇要包括在追蹤記錄檔中的資訊。

若想要在服務上執行預定的追蹤，請爲這些服務設定疑難排解追蹤。

步驟 3 在本機 PC 上安裝 Cisco Unified 即時監控工具。

步驟 4 若想要在指定的搜尋字串存在於受監控追蹤檔案時產生警報，請在 Unified RTMT 中啓用 LogFileSearchStringFound 警示。

您可以在 LpmTctCatalog 中找到 LogFileSearchStringFound 警報。 (選擇**警報** > **定義**。 在「尋找警報位置」下拉式清單方塊中，選擇**系統警報目錄**；在「等於」下拉式清單方塊中，選擇 **LpmTctCatalog**)。

步驟 5 若想要自動擷取警示的追蹤 (例如 CriticalServiceDown 和 CodeYellow) ，請於 Unified RTMT 中勾選「設定警示/內容」對話方塊中該警示的**啟用追蹤下載**方塊，然後再配置您想要下載所發生的頻率。

步驟 6 收集追蹤。

步驟 7 以適當的檢視器檢視記錄檔。

步驟 8 若啓用了疑難排解追蹤，請重設追蹤設定服務，以便還原原始設定。

附註 長時間啓用疑難排解追蹤會增加追蹤檔案件的大小，並可能影響服務的效能。

配置追蹤

本節提供配置追蹤設定的資訊。

附註 啓用追蹤會降低系統效能，請務必僅爲疑難排解之目的啓用追蹤。 如需使用追蹤方面的協助，請聯絡您的技術支援團隊。

設定追蹤參數

本節介紹如何爲透過Serviceability GUI 管理的功能和網路服務設定追蹤參數。

提示 Cisco Unity Connection而言，您可能需要在 Cisco Unified Serviceability和 Cisco Unity Connection Serviceability中執行追蹤以疑難排解 Cisco Unity Connection 問題。 如需如何在 Cisco Unity Connection Serviceability執行追蹤的相關資訊，請參閱 *Cisco Unity Connection Serviceability*管理指南。

程序

步驟 1 選擇**追蹤** > **組態**。

隨即顯示追蹤組態視窗。

步驟 2 從「伺服器」下拉式清單方塊中，選擇正在執行要設定追蹤之服務的伺服器，然後按一下**執行**。

步驟 3 從「服務群組」下拉式清單方塊中，爲要設定追蹤的服務選擇服務群組，然後按一下**執行**。

提示 追蹤組態表格中的服務群組會列出服務和追蹤程式庫，而這些程式庫對應至「服務群組」下拉式清單方塊中顯示的選項。

步驟 4 從「服務」下拉式清單方塊中，選擇要設定追蹤的服務，然後按一下**執行**。

下拉式清單方塊即會顯示活躍和不活躍的服務。

提示 僅限 Cisco Unity Connection：對於 Cisco CallManager 和 CTIManager 服務，您可以設定 SDL 追蹤參數。 若要這樣做，請開啓其中一個服務的「組態」視窗，然後按一下「相關連結」下拉式清單方塊旁邊的**執行**按鈕。

若已爲服務設定「疑難排解追蹤」，則視窗頂端會顯示一則訊息，指出已設定「疑難排解追蹤」功能，這表示系統停用「追蹤組態」視窗中的所有欄位，但「追蹤輸出設定」除外。 若要設定「追蹤輸出設定」，請移至步驟 11。若要重設「疑難排解追蹤」，請參閱「設定疑難排解追蹤設定」。

追蹤參數會針對您選擇的服務而顯示。 此外，也會顯示「套用到所有節點」勾選方塊 (僅適用於 Unified Communications Manager)。

步驟 5 僅限 Unified Communications Manager 和 IM and Presence：若想要這樣做，您可以將服務或追蹤程式庫的追蹤設定套用到叢集中的所有伺服器，方法爲勾選**套用至所有節點**方塊；前提是您的組態有支援叢集。

步驟 6 勾選**開啟追蹤**方塊。

步驟 7 僅限 Cisco Unity Connection：若要設定 SDL 追蹤參數，請移至步驟 10。

步驟 8 在**除錯追蹤層級**清單方塊中選擇您要追蹤的資訊層級，如「除錯追蹤層級設定」中所述。

步驟 9 爲您選擇的服務勾選**追蹤欄位**方塊，例如 Cisco 記錄檔分割監控工具追蹤欄位。

步驟 10 若服務沒有多個您可以在其中指定要啓動之追蹤的追蹤設定，請勾選**啟用所有追蹤**方塊。 若您選擇的服務具有多個追蹤設定，請勾選要啓用之追蹤勾選方塊旁邊的方塊，如追蹤欄位說明中所述。

步驟 11 若要限制追蹤檔案的數目和大小，請指定追蹤輸出設定。 如需說明，請參閱「追蹤輸出設定」。

步驟 12 若要儲存您的追蹤參數組態，請按一下**儲存**按鈕。

對於 Cisco Messaging Interface 以外的所有服務，追蹤組態的變更立即生效 (僅限 Unified Communications Manager)。 Cisco Messaging Interface 的追蹤組態變更會在 3 到 5 分鐘內生效。

附註 若要設定預設值，請按一下**設定預設**按鈕。

追蹤組態中的服務群組

下表列出了服務和追蹤程式庫，而這些程式庫對應至追蹤組態視窗中「服務群組」下拉式清單方塊顯示的選項。

表 *36:* 追蹤組態中的服務群組

服務群組	服務和追蹤程式庫	備註
Unified Communications Manager CM 服務	• Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP 電話服務 • Cisco DHCP 監控服務 • Cisco 已撥出號碼分析工具 • Cisco 已撥出號碼分析工具伺服器 • Cisco Extended Functions, Cisco Extension Mobility • Cisco Extension Mobility 應用程式 • Cisco IP 語音媒體串流應用程式 • Cisco Messaging Interface • Cisco TFTP • Cisco Unified 行動語音存取服務	對於 CM Service 群組中的大部分服務，您可以執行特定元件的追蹤，而不必爲該服務啓用所有追蹤。追蹤欄位說明列出了可以爲特定元件執行追蹤的服務。
Unified Communications Manager CTI 服務	• Cisco IP Manager Assistant • Cisco Web Dialer Web 服務	對於這些服務，您可以執行特定元件的追蹤，而不必爲該服務啓用所有追蹤；請參閱追蹤欄位說明。

服務群組	服務和追蹤程式庫	備註
Unified Communications Manager CDR 服務	• Cisco Unified Communications Manager CDR 分析與報告排程 • Cisco Unified Communications Manager CDR 分析與報告 Web 服務 • Cisco CDR Agent • Cisco CDR Repository Manager	您爲每個服務啓用所有追蹤，而不是爲特定元件執行追蹤。 在 Cisco Unified Communications Manager CDR 分析和回報中，當執行的報告引用預存流程時，Cisco Unified Communications Manager CDR 分析和回報會在預存流程的記錄開始之前，爲 Cisco Unified Communications Manager CDR 分析和回報排程服務和追蹤組態視窗中的 Cisco Unified Communication Manger CDR 分析和回報 Web 服務檢查已組態除錯層級。 Cisco Unified Communications Manager CDR 分析和回報會檢查預先產生的報告 Cisco Unified Communications Manager CDR 分析和回報排程服務的層級；隨需報告而言，Cisco Unified Communications Manager CDR 分析和回報則檢查 Cisco Unified Communications Manager CDR 分析和回報 Web 服務的層級。若從除錯追蹤層級下拉式清單方塊中選擇「除錯」，則將啓用預存程式記錄並繼續進行，直到自下拉式清單方塊中選擇另一個選項爲止。 以下 Cisco Unified Communications Manager CDR 分析和回報的報告會使用預存程式記錄：閘道使用率報告、路由和線路群組組使用率報告、路由/搜尋清單使用率報告、路由模式/搜尋引導使用率報告、電話會議詳細資訊報告、電話會議摘要報告、會議橋接使用率報告、語音留言使用率報告和 CDR 搜尋報告。

服務群組	服務和追蹤程式庫	備註
IM and Presence Service	• Cisco 用戶端設定檔代理 • Cisco 組態代理 • Cisco 叢集間同步代理 • Cisco 登入資料庫 • Cisco OAM 代理 • Cisco Presence 資料庫 • Cisco Presence 引擎 • Cisco IM and Presence 資料監控器 • Cisco 路由資料庫 • Cisco SIP Proxy • Cisco SIP 註冊資料庫 • Cisco 伺服器復原管理員 • Cisco 同步代理 • Cisco XCP 驗證服務 • Cisco XCP 組態管理員 • Cisco XCP 連線管理員 • Cisco XCP 目錄服務 • Cisco XCP 留言封存程式 • Cisco XCP 路由器 • Cisco XCP SIP 聯盟連線管理員 • Cisco XCP 文字會議管理員 • Cisco XCP 網路連線管理員 • Cisco XCP XMPP 聯盟連線管理員	請參閱 Cisco Unified IM and Presence Serviceability中有關功能和網路服務的主題，取得這些服務的相關說明。 • 對於這些服務，應該爲該服務啓用所有追蹤，而不是爲特定元件執行追蹤。

服務群組	服務和追蹤程式庫	備註
資料庫與管理服務	Unified Communications Manager 和 Cisco Unity Connection： • Cisco AXL Web 服務 • Cisco CCM DBL Web Library • Cisco CCMAdmin Web 服務 • Cisco CCMUser Web 服務 • Cisco 資料庫層監控 • Cisco UXL Web 服務 Unified Communications Manager • Cisco 批量佈建服務 • Cisco GRT 通訊 Web 服務 • Cisco 角色型安全性 • Cisco TAPS 服務 • Cisco Unified 回報 Web 服務 IM and Presence Service： • Cisco AXL Web 服務 • Cisco 批量佈建服務 • Cisco CCMUser Web 服務 • Cisco 資料庫層監控 • Cisco GRT 通訊 Web 服務 • Cisco IM and Presence 管理員 • Cisco Unified 回報 Web 服務 • 平台管理 Web 服務	選擇 Cisco CCM DBL Web 程式庫選項可啓動 Java 應用程式對資料庫存取的追蹤。 C++ 應用程式的資料庫存取：請按照 Cisco Extended Functions 追蹤欄位中的說明啓動對 Cisco 資料庫層監控 的追蹤。 選擇支援 Unified Communication Manager 的 Cisco 角色型安全性選項，將啓動使用者角色授權的追蹤。 資料庫和管理服務群組中的大多數服務您皆可啓用服務/程式庫的所有追蹤，而不必爲特定元件啓用追蹤。 Cisco 資料庫層監控而言，您可執行特定元件的追蹤。 **附註** 您可以在 Cisco Unified IM and Presence Serviceability UI 中控管服務記錄。 要變更記錄檔層級，請選擇系統服務群組和 Cisco CCMService Web 服務。

服務群組	服務和追蹤程式庫	備註
效能與監控服務	Unified Communications Manager 和 Cisco Unity Connection： • Cisco AMC 服務 • Cisco CCM NCS Web 程式庫 • CCM PD Web 服務 • Cisco CallManager SNMP 服務 • Cisco 記錄檔分割監控工具 • Cisco RIS 資料收集工具 • Cisco RTMT Web 服務 • Cisco 審計事件服務 • Cisco RisBean 程式庫 Unified Communications Manager： • Cisco CCM PD Web 服務 IM and Presence Service： • Cisco AMC 服務 • Cisco 審計事件服務 • Cisco 記錄檔分割監控工具 • Cisco RIS 資料收集工具 • Cisco RTMT Web 服務 • Cisco RisBean 程式庫	選擇 CCM NCS Web 程式庫選項可啓動 Java 使用者端對資料庫變更通知的追蹤。 選擇 Cisco Unity RTMT Web 服務選項可啓動 Unity RTMT 小服務程式的追蹤。執行此追蹤將爲 Unity RTMT 使用者端查詢建位伺服器端記錄檔。
Unified Communications Manager 安全性服務	• Cisco CTL Provider • Cisco 憑證授權單位代理功能 • Cisco 信任驗證服務	您爲每個服務啓用所有追蹤，而不是爲特定元件執行追蹤。
Unified Communications Manager 目錄服務	Cisco DirSync	您爲此服務啓用所有追蹤而不是爲特定的元件執行追蹤。
備份與還原服務	• Cisco DRF Local • 僅 Unified Communications Manager 和 Cisco Unity Connection：Cisco DRF Master	您爲每個服務啓用所有追蹤，而不是爲特定元件執行追蹤。

服務群組	服務和追蹤程式庫	備註
系統服務	Unified Communications Manager： • Cisco CCMRealm Web 服務 • Cisco CCMService Web 服務 • Cisco 通用 UI • Cisco 追蹤收集服務 IM and Presence Service： • Cisco CCMService Web 服務 • Cisco 追蹤收集服務	選擇 Cisco CCMRealm Web 服務選項可啓動登入驗證的追蹤。 選擇 Cisco 通用UI 選項可啓動對多個應用程式使用的通用代碼追蹤。例如，Cisco Unified 作業系統管理和 Cisco Unified Serviceability。 選擇 Cisco CCMService Web 服務選項可啓動對 Cisco Unified Serviceability Web 應用程式 (GUI) 的追蹤。 您爲每個選項/服務啓用所有追蹤，而不是爲特定元件執行追蹤。
SOAP 服務	• CiscoSOAP 網路服務 • CiscoSOAP 訊息服務	選擇 Cisco SOAP Web 服務選項將啓動 AXL Serviceability API 的追蹤。 您爲此服務啓用所有追蹤而不是爲特定的元件執行追蹤。
平台服務	Cisco Unified 作業系統管理 Web 服務	Cisco Unified 作業系統管理 Web 服務支援 Cisco Unified 作業系統管理，這是 Web 應用程式，可提供與平台相關的功能管理，例如憑證管理、版本設定以及安裝和升級。 您爲此服務啓用所有追蹤而不是爲特定的元件執行追蹤。

除錯追蹤層級設定

下表說明服務的除錯追蹤層級設定。

表 *37:* 除錯服務追蹤層級

層級	描述
錯誤	追蹤警報狀況和事件。 用於異常路徑中產生的所有追蹤。使用最少的 CPU 週期。
特殊	追蹤所有錯誤狀況，以及流程和裝置初始化訊息。
狀態轉換	追蹤所有特殊狀況，以及正常作業期間發生的子系統狀態轉換。 追蹤通話處理事件。
重要	追蹤所有狀態轉換狀況，再加上正常作業期間發生的媒體層事件。

層級	描述
進入/結束	**附註** 並非所有服務都使用此追蹤層級。 追蹤所有重要狀況以及例行的進入和結束點。
任意	追蹤所有進入/結束狀況以及低層級除錯資訊。
詳細	追蹤所有任意狀況以及詳細的除錯資訊。

下表說明小服務程式的除錯追蹤層級設定。

表 *38*: 小服務程式的除錯追蹤層級

層級	描述
嚴重	追蹤可能導致應用程式中止的極嚴重錯誤事件。
錯誤	追蹤警報狀況和事件。 用於異常路徑中產生的所有追蹤。
警示	追蹤可能有害的狀況。
資訊	追蹤大多數的小服務程式問題且對系統效能的影響極低。
除錯	追蹤所有狀態轉換狀況，再加上正常作業期間發生的媒體層事件。 開啓所有記錄的追蹤層級。

追蹤欄位說明

對於某些服務，您可以啓動特定元件的追蹤，而不必爲該服務啓用所有追蹤。 以下清單包括您可以爲特定元件啓動追蹤的服務。 按一下其中一個交互參照任務，可將您帶到適用的章節，其中會爲服務的每個追蹤欄位顯示說明。 若服務未存在於下列清單，則會在「追蹤組態」視窗中爲該服務顯示「啓用所有追蹤」勾選方塊。

以下服務適用於 Unified Communications Manager 和 Cisco Unity Connection：

- 資料庫層監控追蹤欄位
- Cisco RIS Data Collector 追蹤欄位

以下服務適用於 Unified Communications Manager：

- Cisco CallManager SDI 追蹤欄位
- Cisco CallManager SDL 追蹤欄位
- Cisco CTIManager SDL 追蹤欄位
- Cisco Extended Functions 追蹤欄位
- Cisco Extension Mobility 追蹤欄位

- Cisco IP Manager Assistant 追蹤欄位
- Cisco IP 語音媒體串流應用程式追蹤欄位
- Cisco TFTP 追蹤欄位
- Cisco Web Dialer Web 服務追蹤欄位

資料庫層監控追蹤欄位

下表說明 Cisco 資料庫層監控 追蹤欄位。 Cisco 資料庫層監控 服務支援 Unified Communications Manager 和 Cisco Unity Connection。

表 *39: Cisco* 資料庫層監控追蹤欄位

欄位名稱	描述
啓用 DB 程式庫追蹤	啓動 C ++ 應用程式資料庫程式庫追蹤。
啓用服務追蹤	啓動服務追蹤。
啓用 DB 變更通知追蹤	啓動 C++ 應用程式的資料庫變更通知追蹤。
啓用單元測試追蹤	請勿勾選此方塊。 Cisco 工程部將其用於測試目的。

Cisco RIS 資料收集工具追蹤欄位

下表說明 Cisco RIS 資料收集工具追蹤欄位。 Cisco RIS 資料收集服務支援 Unified Communications Manager 和Cisco Unity Connection。

表 *40: Cisco RIS* 資料收集工具追蹤欄位

欄位名稱	描述
啓用 RISDC 追蹤	啓動對 RIS 資料收集服務 (RIS) 的 RISDC 執行緒追蹤。
啓用系統存取追蹤	啓動 RIS 資料收集工具中系統存取程式庫的追蹤。
啓用連結服務追蹤	啓動 RIS 資料收集工具中連結服務的追蹤。
啓用 RISDC 存取追蹤	啓動RIS資料收集工具中RISDC存取程式庫的追蹤。
啓用 RISDB 追蹤	啓動RIS資料收集工具中RISDB程式庫的追蹤。
啓用 PI 追蹤	啓動 RIS 資料收集工具中 PI 程式庫的追蹤。
啓用 XML 追蹤	啓動對 RIS 資料收集服務的輸入/輸出 XML 訊息的追蹤。

欄位名稱	描述
啓用 Perfmon Logger 追蹤	啓動追蹤，以對 RIS 資料收集工具中的 Perfmon 資料進行疑難排解。 用於追蹤記錄檔的名稱，所記錄的計數器總數，應用程式和系統計數器以及執行個體的名稱，流程和執行緒CPU百分比的計算以及記錄檔變換轉和刪除出現的次數。

Cisco CallManager SDI 追蹤欄位

下表描述 Cisco CallManager SDI 追蹤欄位。 Cisco CallManager 服務支援 Unified Communications Manager。

表 *41: Cisco CallManager SDI* 追蹤欄位

欄位名稱	描述
啓用 H245 訊息追蹤	啓動 H245 訊息的追蹤。
啓用 DT-24+/DE-30+ 追蹤	啓動 ISDN 類型 DT-24+/DE-30+ 裝置追蹤的記錄。
啓用 PRI 追蹤	啓動主要速率介面 (PRI) 裝置的追蹤。
啓用 ISDN 轉譯追蹤	啓動 ISDN 訊息追蹤。 用於正常除錯。
啓用 H225 和閘道管理員追蹤	啓動 H.225 裝置的追蹤。 用於正常除錯。
啓用雜項追蹤	啓動其他裝置的追蹤。 **附註** 在正常系統作業期間，請勿勾選此方塊。
啓用會議橋接器追蹤	啓動會議橋接器的追蹤。 用於正常除錯。
啓用待話期間背景音樂追蹤	啓動待話期間背景音樂 (MOH) 裝置的追蹤。 用於追蹤 MOH 裝置狀態，例如向 Unified Communications Manager 註冊、與 Unified Communications Manager 取消註冊、資源分配處理成功或失敗。
啓用 Unified CM 即時資訊伺服器追蹤	啓動即時資訊伺服器使用的 Unified Communications Manager 即時資訊追蹤。
啓用 SIP 堆疊追蹤	啓動 SIP 堆疊的追蹤。 預設值爲已啓用。
啓用通報器追蹤	啓動通報器追蹤；通報器是使用 Cisco IP 語音媒體串流 應用程式服務的 SCCP 裝置，它可讓 Unified Communications Manager 播放預錄通告 (.wav 檔案) 和音調給 Cisco Unified IP 電話和閘道，以及其他可設定的裝置。

欄位名稱	描述
啓用 CDR 追蹤	啓動 CDR 的追蹤。
啓用類比 trunk 追蹤	啓動所有類比 trunk (AT) 閘道的追蹤。
啓用所有電話裝置追蹤	啓動電話裝置的追蹤。 追蹤資訊包括軟體電話裝置。 用於正常除錯。
啓用 MTP 追蹤	啓動終止媒體點(MTP)裝置的追蹤。 用於正常除錯。
啓用所有閘道追蹤	啓動所有類比和數位閘道的追蹤。
啓用轉接和雜項追蹤	啓動來電轉接和另一個可勾選方塊未涵蓋的所有子系統的追蹤。 用於正常除錯。
啓用 MGCP 追蹤	啓對媒體閘道控制通訊協定(MGCP)裝置的追蹤。用於正常除錯。
啓用媒體資源管理員追蹤	啓動媒體資源管理員 (MRM) 活動的追蹤。
啓用 SIP 通話處理追蹤	啓動 SIP 通話處理的追蹤。
啓用 SCCP 保持運作追蹤	在 Cisco CallManager 追蹤中啓動 SCCP 保持不中斷追蹤資訊的追蹤。 因爲每個 SCCP 裝置會每 30 秒回報一次保持不中斷訊息，而且每個保持不中斷訊息都會建立 3 行追蹤資料，所以勾選此方塊時，系統會產生大量追蹤資料。
啓用 SIP 保持運作 (REGISTER 重新整理) 追蹤	在 Cisco CallManager 追蹤中啓動 SIP 保持不中斷 (REGISTER 重新整理) 追蹤資訊的追蹤。 因爲每個 SIP 裝置會每 2 分鐘報告一次保持不中斷訊息，而且每個保持不中斷訊息都會建立多行追蹤資料，所以勾選此方塊時，系統會產生大量追蹤資料。

Cisco CallManager SDL 追蹤欄位

下表說明 Cisco CallManager SDL 追蹤過濾器設定。 Cisco CallManager 服務支援 Unified Communications Manager。

附註 除非 Cisco 工程師另有指示，否則 Cisco 建議您使用預設值。

表 *42: Cisco CallManager SDL* 組態追蹤過濾器設定

設定名稱	描述
啓用所有第 1 層追蹤。	啓動第 1 層的追蹤。
啓用詳細的第 1 層追蹤。	啓動詳細的第 1 層追蹤。
啓用所有第 2 層追蹤。	啓動第 2 層的追蹤。
啓用第 2 層介面追蹤。	啓動第 2 層介面追蹤。
啓用第 2 層 TCP 追蹤。	啓動第 2 層傳輸控制程式 (TCP) 追蹤。
啓用詳細的轉儲第 2 層追蹤。	啓動轉儲第 2 層的詳細追蹤。
啓用所有第 3 層追蹤。	啓動第 3 層的追蹤。
啓用所有通話控制追蹤。	啓動通話控制的追蹤。
啓用雜項輪詢追蹤。	啓動雜項輪詢的追蹤。
啓用雜項追蹤 (資料庫訊號)。	啓動雜項追蹤，如資料庫訊號。
啓用訊息轉譯訊號追蹤。	啓動訊息轉譯訊號的追蹤。
啓用 UUIE 輸出追蹤。	啓動使用者對使用者資訊元素 (UUIE) 輸出的追蹤。
啓用閘道訊號追蹤。	啓動閘道訊號的追蹤。
啓用 CTI 追蹤。	啓動 CTI 追蹤。
啓用網路服務資料追蹤	啓動網路服務資料追蹤。
啓用網路服務事件追蹤	啓動網路服務事件追蹤。
啓用 ICCP 管理追蹤	啓動 ICCP 管理追蹤。
啓用預設追蹤	啓動預設追蹤。

下表描述 Cisco CallManager SDL 組態特色。

表 *43: Cisco CallManager SDL* 組態追蹤特色

特色	描述
啓用 SDL 連結狀態追蹤。	啓動叢集內通訊通訊協定 (ICCP) 連結狀態的追蹤。
啓用低階 SDL 追蹤。	啓動低階 SDL 的追蹤。
啓用 SDL 連結輪詢追蹤。	啓動 ICCP 連結輪詢的追蹤。

特色	描述
啓用 SDL 連結訊息追蹤。	啓動 ICCP 原始訊息的追蹤。
啓用訊號資料傾印追蹤。	啓動訊號資料傾印的追蹤。
啓用關聯標籤對應追蹤。	啓動關聯標籤對應的追蹤。
啓用 SDL 處理狀態追蹤。	啓動 SDL 處理狀態的追蹤。
停用 SDL 追蹤的美化功能。	停用 SDL 美化功能的追蹤。 美化功能可以在追蹤檔案中新增標籤和空格，而無需執行後處理。
啓用 SDL TCP 事件追蹤。	啓動 SDL TCP 事件追蹤。

Cisco CTIManager SDL 追蹤欄位

下表說明 Cisco CTIManager SDL 追蹤過濾器設定。 Cisco CTIManager 服務支援 Unified Communications Manager。

提示 除非 Cisco 工程師另有指示，否則 Cisco 建議您使用預設值。

提示 從「服務群組」下拉式清單方塊選擇 CTIManager 服務時，「追蹤組態」視窗會顯示該服務的 SDI 追蹤。 若要爲 Cisco CTI Manager 服務啓動 SDI 追蹤，請在 Cisco CTIManager 服務的「追蹤組態」視窗中勾選**啟用所有追蹤**方塊。 若要存取「SDL 組態」視窗，請從「相關連結」下拉式清單方塊選擇 **SDL 組態**。Cisco CTIManager SDL 組態追蹤過濾器設定表格和 Cisco CTIManager SDL 組態追蹤特色表格中描述的設定即會出現。

表 *44: Cisco CTIManager SDL* 組態追蹤過濾器設定

設定名稱	描述
啓用雜項輪詢追蹤。	啓動雜項輪詢的追蹤。
啓用雜項追蹤 (資料庫訊號)。	啓動雜項追蹤，如資料庫訊號。
啓用 CTI 追蹤。	啓動 CTI 追蹤。
啓用網路服務資料追蹤	啓動網路服務資料追蹤。
啓用網路服務事件追蹤	啓動網路服務事件追蹤。
啓用 ICCP 管理追蹤	啓動 ICCP 管理追蹤。
啓用預設追蹤	啓動預設追蹤。

下表描述 Cisco CTIManager SDL 組態追蹤特色。

表 *45: Cisco CTIManager SDL* 組態特色

特色	描述
啓用 SDL 連結狀態追蹤。	啓動 ICCP 連結狀態的追蹤。
啓用低階 SDL 追蹤。	啓動低階 SDL 的追蹤。
啓用 SDL 連結輪詢追蹤。	啓動 ICCP 連結輪詢的追蹤。
啓用 SDL 連結訊息追蹤。	啓動 ICCP 原始訊息的追蹤。
啓用訊號資料傾印追蹤。	啓動訊號資料傾印的追蹤。
啓用關聯標籤對應追蹤。	啓動關聯標籤對應的追蹤。
啓用 SDL 處理狀態追蹤。	啓動 SDL 處理狀態的追蹤。
停用 SDL 追蹤的美化功能。	停用 SDL 美化功能的追蹤。 美化功能可以在追蹤檔案中新增標籤和空格，而無需執行後處理。
啓用 SDL TCP 事件追蹤	啓動 SDL TCP 事件追蹤。

Cisco Extended Functions 追蹤欄位

下表描述 Cisco Extended Functions 追蹤欄位。 Cisco Extended Functions 服務支援 Unified Communications Manager。

表 *46: Cisco Extended Functions* 追蹤欄位

欄位名稱	描述
啓用 QBE Helper TSP 追蹤	啓動電話服務供應商追蹤。
啓用 QBE Helper TSPI 追蹤	啓動 QBE Helper TSP 介面追蹤。
啓用 QRT 字典追蹤	啓動品質回報工具服務字典追蹤。
啓用 DOM Helper 追蹤	啓動 DOM Helper 追蹤。
啓用備援和變更通知追蹤	啓動資料庫變更通知追蹤。
啓用 QRT 報告處理程式追蹤	啓動品質回報工具報告處理程式追蹤。
啓用 QBE Helper CTI 追蹤	啓動 QBE Helper CTI 追蹤。
啓用 QRT 服務追蹤	啓動品質回報工具服務相關的追蹤。
啓用 QRT DB 追蹤	啓動 QRT DB 存取追蹤。
啓用範本對應追蹤	啓動標準範本對應和多重對應追蹤。
啓用 QRT 事件處理程式追蹤	啓動品質回報工具事件處理程式追蹤。

欄位名稱	描述
啓用 QRT 即時資訊伺服器追蹤	啓動品質回報工具即時資訊伺服器追蹤。

Cisco Extension Mobility 追蹤欄位

下表說明 Cisco Extension Mobility 追蹤欄位。 Cisco Extension Mobility 服務支援 Unified Communications Manager。

表 *47: Cisco Extension Mobility* 追蹤欄位

欄位名稱	描述
啓用 EM 服務追蹤	啓動 Extension Mobility 服務追蹤。

提示 當您啓動 Cisco Extension Mobility 應用程式服務的追蹤時，可以在 Cisco Extension Mobility 應用程式服務的「追蹤組態」視窗中勾選「啓用所有追蹤」方塊。

Cisco IP Manager Assistant 追蹤欄位

下表描述 Cisco IP Manager Assistant 追蹤欄位。 Cisco IP Manager Assistant 服務支援 Cisco Unified Communications Manager Assistant。

表 *48: Cisco IP Manager Assistant* 追蹤欄位

欄位名稱	描述
啓用 IPMA 服務追蹤1164	啓動 Cisco IP Manager Assistant 服務的追蹤。
啓用 IPMA Manager 組態變更記錄檔	啓動追蹤來記錄爲管理員和助理組態所做的變更。
啓用 IPMA CTI 追蹤	啓動 CTI Manager 連線的追蹤。
啓用 IPMA CTI 安全追蹤	啓動 CTIManager 安全連線的追蹤。

Cisco IP 語音媒體串流應用程式追蹤欄位

本節中的資訊不適用於 Cisco Unity Connection。

下表說明 Cisco IP 語音媒體串流應用程式追蹤欄位。 Cisco IP 語音媒體串流應用程式服務支援 Unified Communications Manager。

表 *49: Cisco IP* 語音媒體串流應用程式追蹤欄位

欄位名稱	描述
啓用服務初始化追蹤	啓動追蹤以取得初始化資訊。

欄位名稱	描述
啓用 MTP 裝置追蹤 Trace	啓動追蹤以監控處理的終止媒體點(MTP)訊息。
啓用裝置復原追蹤	啓動追蹤以取得有關 MTP、會議橋接器和 MOH 的裝置復原相關資訊。
啓用瘦小工作站訊息追蹤	啓動瘦小工作站通訊協定追蹤。
啓用 WinSock 2 級追蹤	啓動追蹤以取得有關 WinSock 的高階詳細資訊。
啓用待話期間背景音樂管理員追蹤	啓動追蹤以監控 MOH 音訊來源管理員。
啓用通報器追蹤	啓動追蹤以監控通報器。
啓用 DB 設定管理員追蹤	啓動追蹤以監控資料庫設定，以及 MTP、會議橋接器和 MOH 的變更。
啓用會議橋接器裝置追蹤	啓動追蹤以監控處理的會議橋接器訊息。
啓用裝置驅動程式追蹤	啓動裝置驅動程式追蹤。
啓用 WinSock 1 級追蹤	啓動追蹤以取得有關 WinSock 的低階一般資訊。
啓用待話期間背景音樂裝置追蹤	啓動追蹤以監控處理的 MOH 訊息。
啓用 TFTP 下載追蹤	啓動追蹤以監控 MOH 音訊來源檔案的下載。

Cisco TFTP 追蹤欄位

下表描述 Cisco TFTP 追蹤欄位。 Cisco TFTP 服務支援 Unified Communications Manager。

表 *50: Cisco TFTP* 追蹤欄位

欄位名稱	描述
啓用服務系統追蹤	啓動服務系統的追蹤。
啓用建構檔案追蹤	啓動構建檔案的追蹤。
啓用服務檔案追蹤	啓動服務檔案的追蹤。

Cisco Web Dialer Web 服務追蹤欄位

下表說明 Cisco Web Dialer Web 服務追蹤欄位。 Cisco Web Dialer Web 服務支援 Unified Communications Manager。

表 *51: Cisco Web Dialer Web* 服務追蹤欄位

欄位名稱	描述
啓用 Web Dialer 小服務程式 追蹤	啓動 Cisco Web Dialer 小服務程式的追蹤。
啓用重新導向程式小服務程式追蹤	啓動重新導向程式小服務程式的追蹤。

IM and Presence SIP Proxy服務追蹤過濾器設定

下表說明 IM and Presence SIP Proxy的服務追蹤過濾器設定。

表 *52: IM and Presence SIP Proxy*服務追蹤過濾器設定

參數	描述
啓用存取記錄檔追蹤	使用此參數可追蹤代理存取記錄檔；記錄代理收到的每個 SIP 訊息的第一行。
啓用驗證追蹤	使用此參數可追蹤驗證模組。
啓用行事曆追蹤	使用此參數可追蹤行事曆模組。
啓用 CTI 閘道追蹤	使用此參數可追蹤 CTI 閘道。
啓用 Enum 追蹤	使用此參數可追蹤 Enum 模組。
啓用方法/事件路由追蹤	使用此參數可追蹤方法/事件路由模組。
啓用號碼擴充追蹤	使用此參數可追蹤號碼擴充模組。
啓用剖析器追蹤	使用此參數可追蹤與依賴sipd 子 SIP 剖析器操作相關的剖析器訊息。
啓用隱私追蹤	使用此參數可以追蹤有關與私密請求的 PAI、RPID 和 Diversion 標頭處理的資訊。
啓用登錄追蹤	使用此參數可追蹤登錄模組。
啓用路由追蹤	使用此參數可追蹤路由模組。
啓用 SIPUA 追蹤	使用此參數可追蹤 SIP UA 應用程式模組。
啓用伺服器追蹤	使用此參數可追蹤伺服器。
啓用 SIP 訊息和狀態機器追蹤	使用此參數可以追蹤與每個 SIP 狀態機器運作相關的資訊。
啓用 SIP TCP 追蹤	使用此參數可追蹤與 TCP 服務進行之 SIP 訊息的 TCP 傳輸有關的資訊。
啓用 SIP TLS 追蹤	使用此參數可追蹤與 TCP 服務之 SIP 訊息的 TLS 傳輸有關的資訊。

參數	描述
啓用 SIP XMPP IM 閘道追蹤	使用此參數可追蹤 SIP XMPP IM 閘道。
啓用 Presence Web 服務追蹤	使用此參數可追蹤 Presence Web 服務。

IM and Presence 追蹤欄位說明

下表提供了支援對特定元件啓動追蹤的服務欄位說明。 對於某些服務，您可以啓動特定元件的追蹤，而不必爲該服務啓用所有追蹤。 若本章節內容未包含某項服務，「啓用所有追蹤」會在「追蹤組態」視窗中顯示該服務。

Cisco 存取記錄檔追蹤欄位

下表說明 Cisco 存取記錄檔追蹤欄位。

表 *53:* 存取記錄檔追蹤欄位

欄位名稱	描述
啓用存取記錄檔追蹤	開啓存取記錄檔追蹤。

Cisco 驗證追蹤欄位

下表說明 Cisco 驗證追蹤欄位。

表 *54:* 驗證追蹤欄位

欄位名稱	描述
啓用驗證追蹤	開啓驗證追蹤。

Cisco 行事曆追蹤欄位

下表說明 Cisco 行事曆追蹤欄位。

表 *55:* 行事曆追蹤欄位

欄位名稱	描述
啓用行事曆追蹤	開啓行事曆追蹤。

Cisco CTI 閘道追蹤欄位

下表說明 Cisco CTI 閘道追蹤欄位。

表 *56: CTI* 閘道追蹤欄位

欄位名稱	描述
啓用 CTI 閘道追蹤	開啓 CTI 閘道追蹤。

Cisco 資料庫層監控追蹤欄位

下表說明 Cisco 資料庫層監控 追蹤欄位。

表 *57: Cisco* 資料庫層監控追蹤欄位

欄位名稱	描述
啓用 DB 程式庫追蹤	開啓 C++ 應用程式的資料庫程式庫追蹤。
啓用服務追蹤	開啓服務追蹤。
啓用 DB 變更通知追蹤	啓動 C++ 應用程式的資料庫變更通知追蹤。
啓用單元測試追蹤	不要檢查。 Cisco 工程部將其用於測試目的。

Cisco Enum 追蹤欄位

下表說明 Cisco Enum 追蹤欄位。

表 *58: Enum* 追蹤欄位

欄位名稱	描述
啓用 Enum 追蹤	開啓 Enum 追蹤。

Cisco 方法/事件追蹤欄位

下表描述 Cisco 方法/事件追蹤欄位。

表 *59:* 方法/事件追蹤欄位

欄位名稱	描述
啓用方法/事件追蹤	開啓方法/事件追蹤。

Cisco 號碼擴充追蹤欄位

下表說明 Cisco 號碼擴充追蹤欄位。

表 *60:* 號碼擴充追蹤欄位

欄位名稱	描述
啓用號碼擴充追蹤	啓動號碼擴充追蹤。

Cisco 剖析器追蹤欄位

下表說明 Cisco 剖析器追蹤欄位。

表 *61:* 剖析器追蹤欄位

欄位名稱	描述
啓用剖析器追蹤	啓動剖析器追蹤。

Cisco 隱私追蹤欄位

下表說明 Cisco 隱私追蹤欄位。

表 *62:* 隱私追蹤欄位

欄位名稱	描述
啓用隱私追蹤	啓動隱私追蹤。

Cisco 代理追蹤欄位

下表說明 Cisco proxy 追蹤欄位。

表 *63:* 代理追蹤欄位

欄位名稱	描述
新增代理	開啓代理追蹤。

Cisco RIS 資料收集工具追蹤欄位

下表說明 Cisco RIS 資料收集工具追蹤欄位。

表 *64: Cisco RIS* 資料收集工具追蹤欄位

欄位名稱	描述
啓用 RISDC 追蹤	啓動對 RIS 資料收集服務 (RIS) 的 RISDC 執行緒追蹤。
啓用系統存取追蹤	啓動 RIS 資料收集工具中系統存取程式庫的追蹤。

欄位名稱	描述
啓用連結服務追蹤	啓動 RIS 資料收集工具中連結服務的追蹤。
啓用 RISDC 存取追蹤	啓動RIS資料收集工具中RISDC存取程式庫的追蹤。
啓用 RISDB 追蹤	啓動RIS資料收集工具中RISDB程式庫的追蹤。
啓用 PI 追蹤	啓動 RIS 資料收集工具中 PI 程式庫的追蹤。
啓用 XML 追蹤	啓動對 RIS 資料收集服務的輸入/輸出 XML 訊息的追蹤。
啓用 Perfmon Logger 追蹤	啓動追蹤，以對 RIS 資料收集工具中的 Perfmon 資料進行疑難排解。 用於追蹤記錄檔的名稱，所記錄的計數器總數，應用程式和系統計數器以及執行個體的名稱，流程和執行緒CPU百分比的計算以及記錄檔變換轉和刪除出現的次數。

Cisco 登錄追蹤欄位

下表說明 Cisco 登錄追蹤欄位。

表 *65:* 登錄追蹤欄位

欄位名稱	描述
啓用登錄追蹤	啓動登錄追蹤。

Cisco 路由追蹤欄位

下表說明 Cisco 路由追蹤欄位。

表 *66:* 路由追蹤欄位

欄位名稱	描述
啓用路由追蹤	啓動路由追蹤。

Cisco 伺服器追蹤欄位

下表說明 Cisco 伺服器追蹤欄位。

表 *67:* 伺服器追蹤欄位

欄位名稱	描述
啓用伺服器追蹤	啓動伺服器追蹤。

Cisco SIP 訊息和狀態機器追蹤欄位

下表說明 Cisco SIP 訊息和狀態機器追蹤欄位。

表 *68: SIP* 訊息和狀態機器追蹤欄位

欄位名稱	描述
啓用 SIP 訊息和狀態機器追蹤	啓動 SIP 訊息和狀態機器追蹤。

Cisco SIP TCP 追蹤欄位

下表說明 Cisco SIP TCP 追蹤欄位。

表 *69: SIP TCP* 追蹤欄位

欄位名稱	描述
啓用 SIP TCP 追蹤	啓動 SIP TCP 追蹤。

Cisco SIP TLS 追蹤欄位

下表說明 Cisco SIP TLS 追蹤欄位。

表 *70: SIP TLS* 追蹤欄位

欄位名稱	描述
啓用 SIP TLS 追蹤	啓動 SIP TLS 追蹤。

Cisco Web 服務追蹤欄位

下表說明 Cisco Web 服務追蹤欄位。

表 *71: Web* 服務追蹤欄位

欄位名稱	描述
啓用 Presence Web 服務追蹤	啓動 Presence Web 服務追蹤。

追蹤輸出設定

下表包含追蹤記錄檔說明。

注意 當您在追蹤組態視窗中變更最大檔案數或最大檔案大小設定時，系統將刪除目前檔案(即服務正在執行) 以外的所有服務記錄檔。若尚未啓動該服務，則系統會在您啓動該服務後立即刪除檔案。 在變更最大檔案數設定或最大檔案大小設定之前，若要保留記錄檔的記錄，請將服務記錄檔案下載並儲存到另一台伺服器；否則，請執行以下作業：要執行此工作，請使用 Unity RTMT 中的追蹤和記錄檔中心。

表 *72:* 追蹤輸出設定

欄位	描述
檔案數量上限	此欄位指定給定服務的追蹤檔總數。 Cisco Unified Serviceability自動將序號附加到檔案名以指出是哪個檔案，例如 cus299.txt。 當序列中的最後一個檔案已滿時，追蹤資料將開始覆蓋第一個檔案。 預設值因服務而異。
檔案大小上限 (MB)	此欄位會指定追蹤檔大小上限 (MB)。 預設值因服務而異。

追蹤設定疑難排解

疑難排解追蹤設定視窗

疑難排解追蹤設定視窗允許您在Serviceability GUI中選擇要爲其設定預定疑難排解追蹤設定的服務。在此視窗中，您可以選擇叢集中不同節點上的服務。 這會爲您選擇的所有服務填入追蹤設定變更。您可以選擇單一節點的特定作用中服務、節點的所有作用中服務、叢集中所有節點的特定作用中服務，或叢集中所有節點的所有作用中服務。 在視窗中，N/A 顯示在非作用中服務旁邊。

附註 IM and Presence 方面，IM and Presence 功能或網路服務的預定疑難排解追蹤設定包括 SDI 和 Log4j 追蹤設定。在套用疑難排解追蹤設定之前，系統會備份原始追蹤設定。 重設疑難排解追蹤設定時，會還原原始疑難排解。

將疑難排解追蹤設定套用至服務之後，若開啓**疑難排解追蹤設定**視窗，您爲疑難排解設定的服務會顯示爲勾選狀態。 在**疑難排解追蹤設定**視窗中，您可以將追蹤設定重設爲原始設定。

在將疑難排解追蹤設定套用至服務之後，**追蹤設定**視窗會顯示一則訊息，指出已爲該服務設定疑難排解追蹤。 若要重設服務的設定，您可以從**相關連結**下拉式清單中選擇「疑難排解追蹤設定」選項。 對於指定服務，**追蹤組態**視窗會將所有設定顯示爲唯讀，但追蹤輸出設定的部分參數 (例如，檔案數上限) 除外。

疑難排解追蹤設定

開始之前

檢視任務設定追蹤組態和設定追蹤參數。

程序

步驟 1 選擇**追蹤** > **疑難排解追蹤設定**。

步驟 2 從**伺服器**清單方塊中選擇要在其中疑難排解追蹤設定的伺服器。

步驟 3 選擇**執行**。

即會顯示服務清單。 不是作用中的服務顯示爲 N/A。

步驟 4 請執行下列一項動作：

a) 若要在您已從**伺服器**清單方塊中選擇的節點上監控特定服務，請勾選**服務**窗格中的服務。

例如，「資料庫與管理服務」、「效能與監控服務」或「備份與還原服務」窗格 (依此類推)。

此任務僅影響您從**伺服器**清單方塊中選擇的節點。

b) 若要在您已從**伺服器**清單方塊中選擇的節點上監控所有服務，請勾選**檢查所有服務**。

c) 僅限 Cisco Unified Communications Manager 和 IM and Presence 叢集：若要監控叢集中所有節點上的特定服務，請勾選**檢查所有節點上選擇的服務**。

此設定適用於服務活躍的叢集中的所有節點。

d) 僅限 Unified Communications Manager 和 IM and Presence 叢集：若要監控叢集中所有節點的所有服務，請勾選**檢查所有節點上的所有服務**。

步驟 5 選取**儲存**。

步驟 6 選擇以下其中一個按鈕來還原原始追蹤設定：

a) **重設疑難排解追蹤**—在您於「伺服器」清單方塊中選擇的節點上還原服務的原始追蹤設定；也會顯示爲您可以選擇的圖示。

b) 僅 Unified Communications Manager 和 IM and Presence 叢集：**重設所有節點上的疑難排解追蹤**—還原叢集中所有節點上服務的原始追蹤設定。

僅當您爲一個或多個服務設定疑難排解追蹤時，才會顯示「重設疑難排解追蹤」按鈕。

附註 長時間啓用疑難排解追蹤會增加追蹤檔案件的大小，並可能影響服務的效能。

在選擇**重設**按鈕之後，視窗會重新整理且服務方塊會顯示爲未勾選。

第 17 章

檢視使用記錄

使用記錄概覽

Cisco Unified Communications Manager 提供記錄，可讓您查看所配置的項目在系統中的使用方式。配置的項目包含裝置，以及系統層級設定，例如裝置集區、日期和時間群組以及路由計劃。

相依性記錄

針對下列目的使用相依性記錄：

- 尋找系統層級設定的相關資訊，例如伺服器、裝置集區、日期和時間群組。
- 決定資料庫中使用其他記錄的記錄。 例如，您可以決定使用特定通話搜尋範圍的裝置，例如 CTI 路由點或電話。
- 在刪除任何記錄前，顯示記錄之間的相依性。 例如，在您刪除分區前，可使用相依性記錄來檢視與之相關的通話搜尋範圍 (CSS) 和裝置。 您便可重新設定移除相依性的設定。

路由計畫報告

路由計畫報告可讓您檢視號碼、路由、在系統中設定的型式的部分或完整清單。 當您產生報告時，可以在報告中按一下「型式/目錄號碼」、「分區」或「Route Detail」（路由詳細資料）欄中的項目，存取各項目的組態視窗。

此外，路由計畫報告可讓您將報告資料儲存爲可匯入其他應用程式的 .CSV 檔案。 .CSV 檔案包含的資訊比網頁上的資訊還要詳細，包含電話的目錄號碼、路由型式、型式使用、裝置名稱和裝置描述。

Cisco Unified Communications Manager 使用路由計畫來路由傳遞內部通話和外部公用交換電話網路 (PSTN) 通話。 由於您的網路中可能有數筆記錄，Cisco Unified Communications Manager 管理可讓您根據特定準則尋找特定路由計畫記錄。

使用報告工作

程序

	命令或動作	目的
步驟 1	若要檢視路由計畫記錄並將之用於管理取消指派的目錄號碼，請參閱下列流程： • 檢視路由計畫記錄 ，第 240 頁上的 • 儲存路由計畫報告 ，第 241 頁上的 • 刪除未指定的目錄號碼 ，第 241 頁上的 • 更新取消指定的目錄號碼 ，第 242 頁上的	使用這些流程可尋找特定路由計畫記錄、將記錄儲存爲 .CSV 檔案及管理取消指派的目錄號碼。
步驟 2	若要使用相依性記錄，請參閱下列流程： • 檢視相依性記錄 ，第 243 頁上的	使用這些流程可尋找系統層級設定的相關資訊，並顯示資料庫中的記錄之間的相依性。

路由計畫報告工作流程

程序

	命令或動作	目的
步驟 1	檢視路由計畫記錄 ，第 240 頁上的.	檢視路由計畫記錄及產生自訂路由計畫報告。
步驟 2	儲存路由計畫報告 ，第 241 頁上的.	以 .csv 檔案格式檢視路由計畫報告。
步驟 3	刪除未指定的目錄號碼 ，第 241 頁上的.	從路由計畫報告刪除取消指派的目錄號碼。
步驟 4	更新取消指定的目錄號碼 ，第 242 頁上的.	更新設定路由計畫中取消指派的目錄號碼設定。

檢視路由計畫記錄

本節描述如何檢視路由計畫記錄。 由於您的網路中可能有數筆記錄，Cisco Unified Communications Manager管理可讓您根據特定準則尋找特定路由計畫記錄。 使用下列流程可產生自訂路由計畫報告。

程序

步驟 1 選擇**通話路由** > **路由計畫報告**。

步驟 2 若要尋找資料庫中的所有記錄，請確定此對話方塊爲空白，並執行步驟 3。

若要過濾或搜尋記錄

a) 在第一個下拉式清單中，選擇搜尋參數。
b) 在第二個下拉式清單中，選擇搜尋型樣。
c) 如果適用的話，請指定適當的搜尋文字。

步驟 3 按一下**尋找**。

隨即顯示全部或相符的記錄。 您可以變更在每個頁面上顯示的項目數，只要從「每頁列數」下拉式清單中選擇另一個值即可。

步驟 4 從顯示的記錄清單中，按一下您要檢視之記錄的連結。

視窗將會顯示您選擇的項目。

儲存路由計畫報告

本節包含如何在 .csv 檔案中檢視路由計畫報告的相關資訊。

程序

步驟 1 選擇**通話路由** > **路由計畫報告**。

步驟 2 從**路由計畫報告**視窗中的**相關連結**下拉式清單中選擇 **View In File**（**在檔案中檢視**），然後按一下**執行**。

在出現的對話方塊中，您可以儲存檔案或將檔案匯入至其他應用程式。

步驟 3 按一下**儲存**。

便會顯示另一個視窗，讓您將此檔案儲存至您選擇的位置。

附註 您也可以將檔案儲存爲不同的檔案名稱，但檔案名稱需包含 .CSV 副檔名。

步驟 4 選擇要儲存檔案的位置，然後按一下**儲存**。 此動作會將檔案儲存至您指定的位置。

步驟 5 找到您剛剛儲存的 .CSV 檔案，在其圖示按兩下即可檢視。

刪除未指定的目錄號碼

本節描述如何自路由計畫報告刪除取消指派的目錄號碼。 目錄號碼可以在Cisco Unified Communications Manager 管理中設定及移除。 從裝置移除目錄號碼或刪除電話時，目錄號碼仍存在於 Cisco Unified Communications Manager 資料庫中。 若要從資料庫刪除目錄號碼，請使用「路由計畫報告」視窗。

程序

步驟 1 選擇**通話路由** > **路由計畫報告**。

步驟 2 在「路由計畫報告」視窗中，使用三個下拉式清單指定列出所有取消指派 DN 的路由計畫報告。

步驟 3 有三種方式可刪除目錄號碼：

a) 按一下要刪除的目錄號碼。「目錄號碼組態」視窗顯示時，請按一下「刪除」。
b) 勾選您要刪除的目錄號碼旁的方塊。 按一下「刪除選擇的項目」 。
c) 若要刪除所有找到已取消指定的目錄號碼，請按一下「Delete All Found Items」（刪除所有找到的項目）。

警告訊息會向您確認是否刪除目錄號碼。

步驟 4 若要刪除目錄號碼，請按一下「確定」。 若要取消刪除請求，請按一下「取消」。

更新取消指定的目錄號碼

本節描述如何從路由計畫報告更新取消指派的目錄號碼設定。 目錄號碼可以在 Cisco Unified Communications Manager 管理中設定及移除。 從裝置移除目錄號碼時，目錄號碼仍存在於 Cisco Unified Communications Manager 資料庫中。 若要更新目錄號碼的設定，請使用「路由計畫報告」視窗。

程序

步驟 1 選擇**通話路由** > **路由計畫報告**。
步驟 2 在**路由計畫報告**視窗中，使用三個下拉式清單指定列出所有取消指派 DN 的路由計畫報告。
步驟 3 按一下要更新的目錄號碼。

附註 您可以更新目錄號碼的所有設定，除了目錄號碼和分區以外。

步驟 4 進行必要的更新，例如通話搜尋範圍或轉接選項。
步驟 5 按一下**儲存**。

「目錄號碼組態」視窗會重新顯示，目錄號碼欄位爲空白。

相依性記錄工作流程

程序

	命令或動作	目的
步驟 1	設定相依性記錄 ，第 243 頁上的.	使用此流程可啓用或停用相依性記錄。 此流程以低於一般優先順序執行，可能需要花費較長的時間才能完成；這是因爲撥號計畫的規模與複雜性、CPU 速度及其他應用程式的 CPU 需求所致。
步驟 2	檢視相依性記錄 ，第 243 頁上的.	啓用相依性記錄後，您便可從介面上的組態視窗存取相依性記錄。

設定相依性記錄

使用相依性記錄檢視 Cisco Unified Communications Manager 資料庫記錄之間的關係。 例如，在您刪除分區前，可使用相依性記錄來檢視與之相關的通話搜尋範圍 (CSS) 和裝置。

注意 相依性記錄會產生高CPU使用率。 此流程以低於一般優先順序執行，可能需要花費較長的時間才能完成；這是因爲撥號計畫的規模與複雜性、CPU 速度及其他應用程式的 CPU 需求所致。

若您啓用相依性記錄，且系統發生 CPU 使用率問題，您可以停用相依性記錄。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。

步驟 2 捲動至 **CCMAdmin 參數**區段，從 **Enable Dependency Records**（啓用相依性記錄）下拉式清單中，選擇下列其中一個選項：

- **True**—啓用相依性記錄。
- **False**—停用相依性記錄。

對話方塊會根據您選擇的選項顯示啓用或停用相依性記錄的結果相關訊息。 請閱讀訊息，再於此對話方塊中按一下**確定**。

步驟 3 按一下**確定**。

步驟 4 按一下**儲存**。
畫面上會顯示更新成功訊息，以確認變更。

檢視相依性記錄

啓用相依性記錄後，您便可從介面上的組態視窗存取相依性記錄。

開始之前

設定相依性記錄 ，第 243 頁上的

程序

步驟 1 從 Cisco Unified CM 管理，導覽至您要檢視記錄的組態視窗。

範例：

若要檢視裝置集區的相依性記錄，請選擇**系統** > **裝置集區**。

附註 您無法從**裝置預設**和**企業參數組態**視窗檢視相依性記錄。

步驟 2 按一下**尋找**。

步驟 3 按一下其中一個記錄。
組態視窗會隨即顯示。

步驟 4 從**相關連結**清單方塊中，選擇**相依性記錄**方塊，然後按一下**執行**。

附註 若未啓用相依性記錄，**Dependency Records Summary**（**相依性記錄摘要**）視窗便會顯示訊息，而不是記錄的相關資訊。

Dependency Records Summary（**相依性記錄摘要**）視窗會顯示資料庫中由其他記錄使用的記錄。

步驟 5 在此視窗中選擇下列其中一個相依性記錄按鈕：

- **Refresh**（**重新整理**）—使用目前的資訊更新視窗。
- **Close**（**關閉**）—關閉視窗，而不返回您點選「相依性記錄」連結的組態視窗。
- **Close and Go Back**（**關閉並返回**）—關閉視窗，且返回您點選「相依性記錄」連結的組態視窗。

第 18 章

管理企業參數

企業參數概覽

企業參數提供預設設定，可套用至整個叢集的所有裝置與服務。 例如，您的系統使用企業參數設定其裝置預設的初始值。

您無法新增或刪除企業參數，但可以更新現有的企業參數。 組態視窗會以不同種類列出企業參數；例如，CCMAdmin 參數、CCMUser 參數和 CDR 參數。

您可以在**企業參數組態**視窗中檢視參數組態的詳細說明。

⚠

注意 許多企業參數不需要變更。 請勿變更企業參數，除非您完全瞭解您要變更的功能，或 Cisco 技術援助中心 (TAC) 建議您變更。

檢視企業參數資訊

透過**企業參數組態**視窗中的內嵌內容存取企業參數的相關資訊。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。

步驟 2 您可以執行下列一項作業：

- 若要檢視特定企業參數的說明，請按一下參數名稱。
- 若要檢視所有企業參數的描述，請按一下？ 。

更新企業參數

使用此流程可開啓**企業參數組態**視窗及設定系統層級設定。

注意 許多企業參數不需要變更。 請勿變更企業參數，除非您完全瞭解您要變更的功能，或 Cisco 技術援助中心 (TAC) 建議您變更。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。

步驟 2 選擇您要變更的企業參數所需的值。

步驟 3 點擊**儲存**。

下一步

將組態套用至裝置 ，第 246 頁上的

將組態套用至裝置

透過此流程可使用您的設定來更新叢集中所有受影響的裝置。

開始之前

更新企業參數 ，第 246 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。

步驟 2 確認您的變更，然後按一下**儲存**。

步驟 3 選擇下列其中一個選項：

- 若想讓系統判斷要重新啓動的裝置，請按一下**套用組態**。 在某些情況下，裝置可能不需要重新啓動。 進行中的通話可能會中斷，但會保留接通的通話，除非裝置集區包含 SIP trunk。
- 若要重新啓動叢集中的所有裝置，請按一下**重設**。 我們建議您在非尖峰時段執行此步驟。

步驟 4 讀取確認對話後，按一下**確定**。

還原預設企業參數

若要將企業參數重設爲預設設定，請使用此流程。 某些企業參數包含建議的值，如組態視窗中的欄位所示；此流程使用這些值作爲預設設定。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。

步驟 2 按一下**設為預設值**。

步驟 3 讀取確認提示後，按一下**確定**。

第 19 章

管理伺服器

管理伺服器概覽

本章描述如何管理 Cisco Unified Communications Manager 節點的屬性、檢視狀態伺服器狀態，以及設定 Unified Communications Manager 伺服器的主機名稱。

伺服器刪除

本節介紹如何自Cisco Unified Communications Manager資料庫刪除伺服器，及如何將已刪除的伺服器新增回Cisco Unified Communications Manager叢集。

在Cisco Unified Communications Manager 管理中無法刪除叢集的第一個節點，但可刪除後續的節點。在「尋找和列出伺服器」視窗中刪除後續節點之前，Cisco UnifiedCM 管理會顯示以下訊息：“您將永久刪除一台或多台伺服器，此動作無法復原。 繼續嗎？” 。若點按「確定」，則伺服器將自 Cisco UnifiedCM 資料庫中刪除且無法使用。

提示 當您嘗試在「伺服器組態」視窗中刪除伺服器時，將顯示一條類似於上一段的訊息。 若點按「確定」，則伺服器將自 Cisco UnifiedCM 資料庫中刪除且無法使用。

刪除伺服器之前，請考慮下列的資訊：

- Cisco Unified Communications Manager 管理不允許您刪除叢集中的第一個節點，但您可刪除任何後續的節點。

- Cisco建議您不要刪除有執行Cisco Unified Communications Manager的任何節點，尤其在該節點上註冊了裝置（例如電話）的情況下更不要刪除。
- 儘管後續的節點的依賴項記錄存在，但這些記錄並不會阻止您刪除該節點。
- 若在要刪除的節點上配置了任何CiscoUnified Communications Manager通話駐留號碼，刪除會失敗。 在刪除節點之前，需刪除Cisco Unified Communications Manager 管理中的通話駐留號碼。
- 若Cisco Unified Communications Manager 管理中的組態欄位含有您打算要刪除的伺服器的 IP 位址或主機名稱，請在刪除伺服器之前更新組態。 若不執行此任務，則刪除伺服器後，依賴組態的功能可能無法正常運作；例如，若輸入服務參數、企業參數、服務URL、目錄URL、IP電話服務等的 IP 位址或主機名稱，請在刪除伺服器之前更新此組態。
- 例如，若如Cisco Unity、Cisco Unity Connection等等的應用程式 GUI 含有要刪除的伺服器的 IP 位址或主機名稱，請在刪除伺服器之前在相對應的GUI 中更新組態。 若不執行此任務，則刪除伺服器後，依賴於組態的功能可能無法正常運作。
- 刪除伺服器時，系統可能會自動刪除某些裝置，例如 MOH 伺服器。
- 在刪除節點之前，Cisco 建議您停用在後續節點上處於活動狀態的服務。 執行此任務可確保刪除節點後服務能夠正常運作。
- 對伺服器組態的變更要等到您重新啓動 Cisco Unified Communications Manager 之後才會生效。如需有關重新啓動 Cisco CallManager 服務的詳細資訊，請參閱 *Cisco Unified Serviceability*管理指南。
- 爲確保正確更新資料庫檔案，需在刪除伺服器、在線狀態或應用程式伺服器後重啓叢集。
- 刪除節點後，存取Cisco Unified 報告以驗證Cisco Unified Communications Manager已在叢集中刪除了該節點。 此外，存取 Cisco Unified Reporting、RTMT 或 CLI 以驗證資料庫複製正在現有節點之間進行；如有必要，請修復節點之間的資料庫複製。

附註 當從叢集中刪除訂閱者節點時，其憑證仍然存在於發布者節點和其他節點中。 管理員需手動刪除：

- 從各個叢集成員的信任庫中刪除的訂閱者節點的憑證。
- 來自已刪除的訂閱者節點的trust store中的每個其他叢集成員的憑證。

自叢集刪除 Unified Communications Manager 節點

使用下列流程可自 Cisco Unified Communications Manager 伺服器刪除檔案。

程序

步驟 1 在 Cisco Unified CM 管理中選擇 **系統** > **伺服器**。

步驟 2 點按**尋找**並選擇要刪除的節點。

步驟 3 按一下**刪除**。

步驟 4 當警告對話方塊指出此動作無法復原時，選擇**確定**。

步驟 5 關閉您所取消指定的節點的主虛擬機或伺服器。

自叢集中刪除 IM and Presence 節點

若您需要自 Presence 備援群組和叢集安全移除 IM and Presence Service 節點，請依此流程進行。

⚠

注意 移除節點會導致Presence備援群組中其餘節點的使用者服務中斷。 此流程僅應在維護視窗期間執行。

程序

步驟 1 在 **Cisco Unified CM 管理 > 系統 > Presence 備援群組**頁面，若「高線上狀態」爲啓用，請將它停用。

步驟 2 在 **Cisco Unified CM 管理 > 使用者管理 > Assign Presence Users (指派目前狀態使用者)**頁面，在您要移除的節點取消指派或移除所有使用者。

步驟 3 如要將節點從其狀態備援群組中移除，請從該狀態備援群組的**狀態備援群組組態**頁面上的「狀態伺服器」下拉式清單選擇**未選擇**。 當警告對話方塊指出取消指派節點會重新啓動Presence 備援群組中的服務時，選擇**確定**。

附註 您無法直接於 Presence 備援群組刪除發布者節點。 若要刪除發布者節點，請首先在發布者節點上取消指定使用者，然後完全刪除 Presence 備援群組。

但您可以將已刪除的 IM and Presence 節點重新新增回叢集中。 有關如何新增已刪除節點的更多資訊，請參閱將刪除的伺服器加回叢集，第 251 頁上的。 在這種情況下，當在 Cisco Unified CM 管理控制台的**系統 > 伺服器**螢幕會刪除的發佈方節點新增至伺服器時，系統會自動建立 **DefaultCUPSubcluster**。

步驟 4 在 **系統 > 伺服器**中刪除所取消指定的節點。 當警告對話方塊指出此動作無法復原時，選擇**確定**。

步驟 5 爲您取消指派的節點關閉主機 VM 或伺服器。

步驟 6 在所有節點上重新啓動 Cisco XCP 路由器： 服務。

將刪除的伺服器加回叢集

若您在 Cisco Unified Communications Manager 管理刪除後續節點 (訂閱者)，且您想要將它加回叢集，請執行下列流程。

程序

步驟 1 在 Cisco Unified Communications Manager 管理中，選擇**系統** > **伺服器**以新增伺服器。

步驟 2 將後續節點新增至 Cisco Unified Communications Manager 管理後，使用 Cisco 在軟體套件中提供的硬碟，於伺服器上執行安裝適用的版本。

提示 請確保您安裝的版本符合在發佈者節點上執行的版本。 若在發佈者節點上執行的版本與安裝檔案不符，請在安裝過程選擇「安裝期間升級」選項。 如需詳細資訊，請參閱 *Cisco Unified Communications Manager* 和 *IM and Presence Service*安裝指南。

步驟 3 安裝 Cisco Unified CM 後，請設定後續節點，如支援您的 Cisco Unified CM 版本的安裝檔案所述。

步驟 4 存取 Cisco Unified 報告、RTMT 或 CLI 以驗證資料庫複製正在現有節點之間進行；如有必要，請修復節點之間的資料庫複製。

在安裝前新增節點至叢集

使用 Cisco Unified Communications Manager 管理，在安裝前新增新節點至叢集。 您在新增節點時選擇的伺服器類型需符合您安裝的伺服器類型。

您需在第一個節點使用 Cisco Unified Communications Manager 管理設定新節點，再安裝新節點。 若要在叢集上安裝節點，請參閱 *Cisco Unified Communications Manager* 安裝指南。

針對 Cisco Unified Communications Manager 語音/語音伺服器，您在 Cisco Unified Communications Manager 軟體初始安裝期間新增的第一個伺服器會指定爲發佈者節點。 所有後續伺服器安裝或新增皆會指定爲訂閱者節點。 您新增至叢集的第一個 Cisco Unified Communications Manager IM and Presence 節點會指定爲 IM and Presence Service 資料庫發佈者節點。

附註 新增伺服器後，您無法使用 Cisco Unified Communications Manager 管理變更伺服器類型。 您需刪除現有的伺服器執行實例，然後再次新增新的伺服器，並選擇正確的伺服器設定。

程序

步驟 1 選擇 **系統** > **伺服器**。

尋找及列出伺服器視窗會隨即顯示。

步驟 2 按一下**新增**。

伺服器組態 - 新增伺服器視窗會隨即顯示。

步驟 3 在**伺服器類型**下拉式清單方塊中，選擇要新增的伺服器類型，然後按**下一步**。

- CUCM 視訊/語音

- CUCM IM and Presence

步驟 4 在**伺服器組態**視窗中，輸入適當的伺服器設定。

若需要伺服器的組態欄位描述，請參閱伺服器設定。

步驟 5 點擊**儲存**。

檢視狀態伺服器狀態

使用 Cisco Unified Communications Manager 管理，檢視 IM and Presence Service節點的關鍵服務狀態和自我診斷測試結果。

程序

步驟 1 選擇 **系統** > **伺服器**。

尋找及列出伺服器視窗會隨即顯示。

步驟 2 選擇伺服器搜尋參數，然後按一下**尋找**。

符合的記錄會隨即顯示。

步驟 3 選擇列於**尋找及列出伺服器**視窗中的 IM and Presence 伺服器。

伺服器組態視窗會隨即顯示。

步驟 4 按一下**伺服器組態**視窗 IM and Presence 伺服器資訊區段中的「狀態伺服器狀態」連結。

伺服器的**節點詳細資料**視窗會隨即顯示。

設定通訊埠

使用此流程可以更改用於連線的通訊埠設定，例如 SCCP 裝置註冊、SIP 裝置註冊和 MGCP 閘道連線。

附註 通常您無需更改預設通訊埠設定。 僅當您確實要更改預設值時才使用此流程。

程序

步驟 1 在 Cisco Unified Communications Manager 管理中選擇 **系統** > **Cisco Unified CM**。
尋找及列出 Cisco Unified CM視窗會隨即顯示。

步驟 2 輸入適當的搜尋準則，然後按一下**尋找**。
所有相符的 Cisco Unified Communications Manager 皆顯示。

步驟 3 選擇您想要檢視的**Cisco Unified CM**。
Cisco Unified CM 組態視窗隨即顯示。

步驟 4 導覽至**此伺服器的 Cisco Unified Communications Manager TCP 通訊埠設定**部分。

步驟 5 點擊**儲存**。

步驟 6 按一下**套用組態**。

步驟 7 點擊**確定**。

連接埠設定

欄位	描述
乙太網路電話通訊埠	系統會使用此 TCP 通訊埠來與網路上的Cisco Unified IP 電話（僅限 SCCP）通訊。 • 請接受預設通訊埠值 2000，除非您的系統上已使用此通訊埠。 選擇 2000 會將此通訊埠識別爲不安全。 • 請確定所有通訊埠輸入都是獨一無二的。 • 有效通訊埠號碼範圍爲 1024 到 49151。
MGCP 接聽通訊埠	系統會使用此 TCP 通訊埠來從其相關 MGCP 閘道偵測訊息。 • 請接受預設通訊埠 2427，除非您的系統上已使用此通訊埠。 • 請確定所有通訊埠輸入都是獨一無二的。 • 有效通訊埠號碼範圍爲 1024 到 49151。
MGCP 保持不中斷通訊埠	系統會使用此 TCP 連接埠與其相關 MGCP 閘道交換保持連線訊息。 • 請接受預設通訊埠 2428，除非您的系統上已使用此通訊埠。 • 請確定所有通訊埠輸入都是獨一無二的。 • 有效通訊埠號碼範圍爲 1024 到 49151。
SIP 電話通訊埠	此欄位會指定 Cisco Unified Communications Manager 用於聆聽 SIP 線路註冊（透過 TCP 與 UDP）的通訊埠號碼。

欄位	描述
SIP 電話安全通訊埠	此欄位會指定系統用於聆聽 SIP 線路註冊（透過 TLS）的通訊埠號碼。
SIP 電話 OAuth 通訊埠	此欄位會指定 Cisco Unified Communications Manager 用來從 Jabber 內部部署裝置透過 TLS（傳輸層安全性）聆聽 SIP 線路註冊的通訊埠號碼。 預設值爲 5090。範圍爲 1024 至 49151。
SIP Mobile and Remote Access OAuth 通訊埠	此欄位會指定 Cisco Unified Communications Manager 用來從透過 Expressway 的 Jabber 經由 MTLS（相互傳輸層安全性）聆聽 SIP 線路註冊的通訊埠號碼。 預設值爲 5091。範圍爲 1024 至 49151。

主機名稱組態

下表列出您可以爲 Unified Communications Manager 伺服器配置主機名稱的地方，允許主機名稱使用的字元數量以及建議主機名稱使用的第一個和最後一個字元。請注意，如果您沒有正確配置主機名稱，Unified Communications Manager 中的部分組件，例如作業系統、資料庫、安裝等元件可能無法按預期工作。

表 *73: Cisco Unified Communications Manager* 的主機名稱組態

主機名稱位置	允許的組態	允許的字元數	建議的主機名稱第一個字元	建議的主機名稱最後一個字元
主機名稱/IP 位址欄位 Cisco Unified Communications Manager 管理中的**系統** > **伺服器**。	您可以新增或變更叢集中的伺服器的主機名稱。	2-63	字母	英數字
主機名稱欄位 Cisco Unified Communications Manager 安裝精靈	您可以新增叢集中的伺服器的主機名稱。	1-63	字母	英數字
主機名稱欄位 Cisco Unified Communications 作業系統中的**設定** > **IP** > **乙太網路**	您可以變更 (非新增)叢集中的伺服器的主機名稱。	1-63	字母	英數字
設定網路主機名稱 主機名稱 命令行介面	您可以變更 (非新增)叢集中的伺服器的主機名稱。	1-63	字母	英數字

提示 主機名稱需遵循 ARPANET 主機名稱的規則。 您可以在主機名稱的第一個和最後一個字元之間輸入英數字元和連字符。

在任何位置設定主機名稱之前，請檢閱下列資訊：

- 「伺服器組態」視窗中的「主機名稱/IP 位址」欄位支援裝置對伺服器、應用程式對伺服器和伺服器對伺服器通訊，可讓您以小數點十進位的格式輸入 IPv4 位址或主機名稱。

  安裝 Unified Communications Manager 發佈者節點後，發佈者的主機名稱會自動顯示在此欄位。安裝 Unified Communications Manager 訂閱者節點前，請在 Unified Communications Manager 發佈者節點的此欄位中輸入訂閱者節點的 IP 位址或主機名稱。

  請僅在 Unified Communications Manager 可存取 DNS 伺服器以解析主機名稱爲 IP 位址時，在此欄位配置主機名稱；請確定您在 DNS 伺服器配置 Cisco Unified Communications Manager 的名稱和位址資訊。

提示 除了設定 DNS 伺服器的 Unified Communications Manager 資訊，您也會在 Cisco Unified Communications Manager 安裝期間輸入 DNS 資訊。

- Unified Communications Manager 發佈者節點安裝期間，您會輸入主機名稱，其爲必填欄位，以及發佈者節點的 IP 位址以設定網路資訊；也就是說，若您要使用靜態網路的話。

  Unified Communications Manager訂閱者節點安裝期間，您會輸入 Unified Communications Manager 發佈者節點的主機名稱和 IP 位址，以讓 Unified Communications Manager 驗證網路連線和發佈者至訂閱者的驗證。 此外，您需輸入訂閱者節點的主機名稱和IP位址。 Unified Communications Manager 安裝提示您輸入使用者伺服器的主機名稱時，請輸入 Cisco Unified Communications Manager 管理「伺服器組態」視窗中顯示的值；亦即，若您已在「主機名稱/IP 位址」欄位設定使用者伺服器的主機名稱。

Kerneldump 公用程式

Kerneldump 公用程式使您可以在受影響的電腦上本地收集故障轉儲記錄檔，而無需輔助伺服器。

在一個Unified Communications Manager叢集，您僅需要確保在伺服器上啓用了 kerneldump 公用程式，即可收集故障轉儲資訊。

附註 Cisco建議您在安裝後驗證 kerneldump 公用程式是否已啓用Unified Communications Manager以便進行更有效的疑難排解。 若您尚未這樣做，請先啓用 kerneldump 公用程式，然後再從受支援的裝置版本升級Unified Communications Manager。

重要須知 啓用或停用 kerneldump 公用程式需將節點重新啓動。 除非您位於可將結點重新啓動的視窗中，否則請不要執行 enable 命令。

Cisco Unified Communications 作業系統的指令行介面（CLI）可用於啓用、停用或檢查 kerneldump 公用程式的狀態。

使用以下流程來啓用核心轉儲公用程式：

使用公用程式收集的檔案

要檢視kerneldump公用程式崩潰資訊請使用*Cisco Unified RTMT*或命令行介面（CLI）。要使用*Cisco Unified RTMT*收集 kerneldump 記錄檔，請在“追蹤和記錄中心”中選擇“收集檔案”選項。在“選擇系統服務/應用程式”索引標籤中，選擇“Kerneldump 記錄檔”方塊。如需如何在*Cisco Unified RTMT* 存取所收集記錄檔的相關資料，請參閱 *Cisco Unified* 即時監控工具管理指南。

要使用 CLI 收集 kerneldump 記錄檔，請使用“檔案”崩潰目錄中檔案上的 CLI 命令， 位於“activelog”分區中。記錄檔檔案名稱開頭爲 kerneldump 用戶端的 IP 位址然後以檔案創建的日期爲結尾。如需 CLI 檔案命令的更多資訊請參閱 *Cisco Unified Solutions* 命令行介面參考指南。

啟用 Kerneldump 公用程式

使用此流程啓用 kerneldump 公用程式。萬一發生核心崩潰，該公用程式提供了一種收集和轉儲崩潰的機制。 您可以將公用程式配置爲將記錄檔轉儲到本地伺服器或外部伺服器。

程序

步驟 1 登入命令行介面。

步驟 2 完成以下的任一操作：

- 如要在本地伺服器上轉儲核心崩潰，請執行 `utils os kerneldump enable` CLI 指令。
- 要將核心崩潰傾印到外部伺服器，請執行 `utils os kerneldump ssh enable <ip_address>` CLI 指令再加上外部伺服器的 IP 位址。

步驟 3 重新啓動伺服器。

範例

附註 若您需要停用 kerneldump 公用程式，則可以執行 `utils os kernelcrash disable` CLI 指令以停用本地伺服器進行核心傾印，以及 `utils os kerneldump ssh disable <ip_address>` CLI 指令以在外部伺服器上停用該公用程式。

下一步

在 RTMT 中配置電子郵件警報以通知核心轉儲發生時機。 如需詳細資訊，請參閱 啓用核心轉儲的電子郵件警示 ，第 258 頁上的

有關 kerneldump 公用程式和疑難排解的更多資訊請參閱*Cisco Unified Communications Manager* 疑難排解指南。

啟用核心轉儲的電子郵件警示

使用此流程可配置 RTMT 以在發生核心轉儲時傳送電子郵件給管理員。

程序

步驟 1 選擇**系統** > **工具** > **警示** > **警示中心**。

步驟 2 在 **CoreDumpFileFound** 警示上按一下滑鼠右鍵，然後選擇**設定警示內容**。

步驟 3 按照精靈提示設定您的偏好準則：

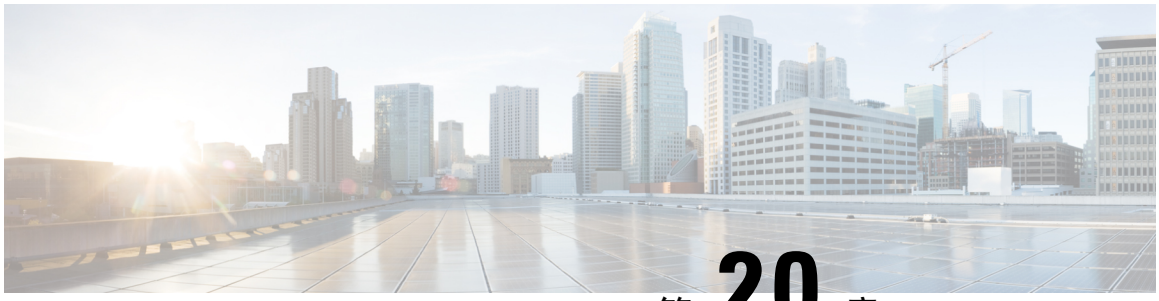
a) 在**警示內容：電子郵件通知**快顯視窗中，確定已勾選**啟用電子郵件**，然後按一下**設定** 以設定預設警示動作，動作即爲寄送電子郵件給管理員。
b) 按照提示進行，然後**新增**收件人電子郵件地址。 觸發此警示時，預設動作是透過電子郵件寄送到此地址。
c) 按一下**儲存**。

步驟 4 設定預設電子郵件伺服器：

a) 選擇**系統** > **工具** > **警示** > **設定電子郵件伺服器**。
b) 輸入電子郵件伺服器和連接埠資訊，以傳送電子郵件警示。
c) 輸入**傳送使用者 ID**。
d) 點擊**確定**。

第 V 部分

管理報告



第 20 章

Cisco Serviceability 回報工具

Serviceability報告封存

Cisco Serviceability 回報工具 服務會產生每日報告，其中包含圖表，這些圖表會顯示該特定報告的統計資料摘要。 Reporter 會根據記錄的資訊產生報告，每天一次。

使用Serviceability GUI，從**工具** > **Serviceability報告封存**檢視報告。 您需先啓動 Cisco Serviceability 回報工具 服務，然後才能檢視報告。 服務啓動後，最多需要 24 個小時來產生報告。

這些報告包含前一天的 24 小時資料。 新增到報告名稱的檢視報告顯示 回報工具 產生它們的日期；例如 AlertRep_mm_dd_yyyy.pdf。「Serviceability報告封存」視窗會使用此日期，僅顯示相關日期的報告。這些報告會從記錄檔中存在的資料產生，並附上前一天的時間戳記。 系統考慮目前日期和前兩天的記錄檔來收集資料。

報告中顯示的時間反映伺服器“系統時間”。

產生報告時，您可以從伺服器擷取記錄檔案。

附註 Cisco Unified 回報 Web 應用程式會將資料的快照檢視提供爲一個輸出，並執行資料檢查。 應用程式也允許您封存產生的報告。 如需詳細資訊，請參閱 *Cisco Unified* 回報管理指南。

叢集組態的Serviceability報告封存注意事項

本節僅適用於 Unified Communications Manager 和 IM and Presence Service。

- 因爲 Cisco Serviceability 回報工具 僅在第一部伺服器上作用中，所以任何時間，回報工具 僅會在第一部伺服器上產生報告，而不會在其他伺服器上產生報告。
- 報告中顯示的時間反映第一部伺服器“系統時間”。 若第一部伺服器和後續伺服器位於不同的時區，則第一部伺服器“系統時間”會顯示在報告中。
- 在爲報告收集數據時，將考慮叢集中伺服器位置之間的時區差異。

- 產生報告時，您可以從個別伺服器或從叢集中的所有伺服器中選擇記錄檔`。
- Cisco Unified 報告 Web 應用程式輸出和資料檢查包括來自所有可存取伺服器的叢集資料。

Cisco Serviceability 回報程式配置工作流程

完成這些任務以透過 Cisco Serviceability 回報程式設定每日系統報告。

程序

	命令或動作	目的
步驟 1	啓動 Cisco Serviceability 回報程式 ，第 262 頁上的	**Cisco Serviceability 回報程式** 服務需爲執行中以每日產生報告。
步驟 2	配置 Cisco Serviceability 回報程式設定 ，第 262 頁上的	爲 Cisco Serviceability 回報程式產生的每日報告配置計劃設定。
步驟 3	檢視每日報告封存 ，第 263 頁上的	系統產生每日報告後，請使用此任務檢視PDF檔案中的每日報告。

啟動 Cisco Serviceability 回報程式

使用此流程可透過以下方式開啓每日系統報告：**Cisco Serviceability 回報程式**。 該服務需爲**啟動**以產生報告。

程序

步驟 1 在 Cisco Unified Serviceability中，選擇**工具** > **服務啟用**。

步驟 2 選擇**伺服器**然後點按**移至**。

步驟 3 在**性能和監控服務**中檢查**Cisco Serviceability 回報程式**服務的狀態。

步驟 4 若服務正在執行中或已啓用，請選擇旁邊的單選按鈕，然後按一下**停止**。

附註 每天產生報告。 第一份報告最多可能需要 24 小時才能產生。

配置 Cisco Serviceability 回報程式設定

爲 Cisco Serviceability 回報程式 產生的每日報告配置計劃設定。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **服務參數**。

步驟 2 選擇執行 Cisco Serviceability 回報程式 的**伺服器**。

步驟 3 在**服務**下拉式清單中選擇 Cisco Serviceability 回報程式。

步驟 4 配置以下服務參數的設定：

- **RTMT 回報程式指定節點**—指定 RTMT 回報程式所執行的節點。 Cisco建議您指定一個非通話處理節點。
- **報告產生時間** - 指定報告於午夜0時後幾分鐘產生。 範圍是 0 – 1439，預設設定爲 30 分鐘。
- **報告刪除年紀**—將報告儲存在硬碟上的天數。 範圍是 0-30，預設設定爲 7 天。

步驟 5 點擊**儲存**。

檢視每日報告封存

一旦 Cisco Serviceability 回報程式 在產生每日報告，請使用此流程檢視 PDF 檔案中的報告。

程序

步驟 1 選擇**工具** > **服務能力報告封存**。

步驟 2 選擇要顯示報告的月份和年份。
顯示與月份相對應的天數清單。

步驟 3 點按要檢視所產生的報告的日期。

步驟 4 點按您要檢視的報告。

附註 若要檢視 PDF 報告，您的電腦中需安裝 Acrobat Reader。 若要下載 Acrobat Reader，請按一下 **Serviceability 報告封存**視窗底端的連結。

每日報告摘要

Cisco Serviceability 回報程式 每日會產生系統報告。

- 裝置統計資料報告
- 伺服器統計資料報告
- 服務統計資料報告
- 通話活動報告

- 警示摘要報告
- 效能保護報告

裝置統計資料報告

裝置統計資料報告不適用於 IM and Presence Service和 Cisco Unity Connection。

裝置統計資料報告提供以下折線圖：

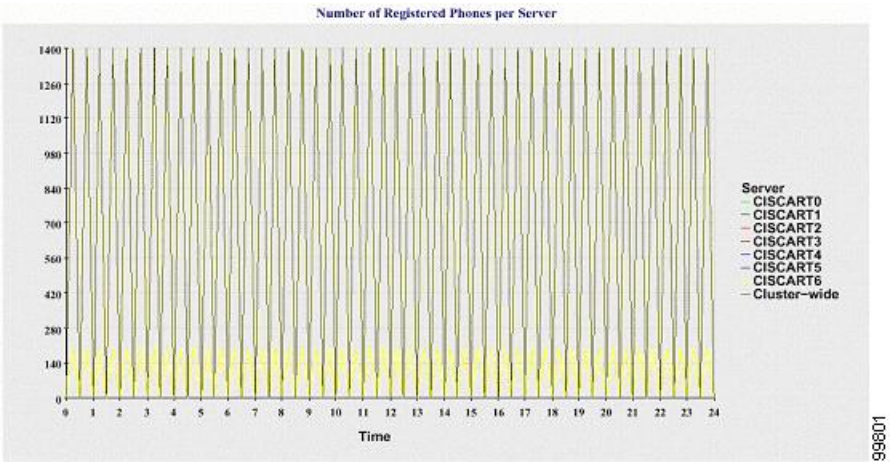
- 每部伺服器的已註冊電話數
- 叢集中的 H.323 閘道數
- 叢集中的 Trunk 數

每部伺服器的已註冊電話數

折線圖顯示每部 Unified Communications Manager 伺服器 (以及 Unified Communications Manager 叢集組態中的叢集) 的已註冊電話數。 圖表中的每一條線代表有可用資料之伺服器的資料，另一條線顯示全叢集資料 (僅適用於 Unified Communications Manager 叢集)。 圖表中的每個資料值代表 15 分鐘內註冊的平均電話數。 若伺服器未顯示任何資料，則 回報工具 不會產生代表該伺服器的線條。 若伺服器 (或 Unified Communications Manager 叢集組態中的所有伺服器) 沒有資料，則對於已註冊的電話，回報工具 不會產生圖表。 這時會顯示訊息“裝置統計資料報告沒有可用的資料”。

圖 *4:* 描述每部伺服器之已註冊電話數的折線圖

下圖顯示折線圖範例，代表 Unified Communications Manager 叢集組態中每部 Unified Communications Manager 伺服器的已註冊電話數。



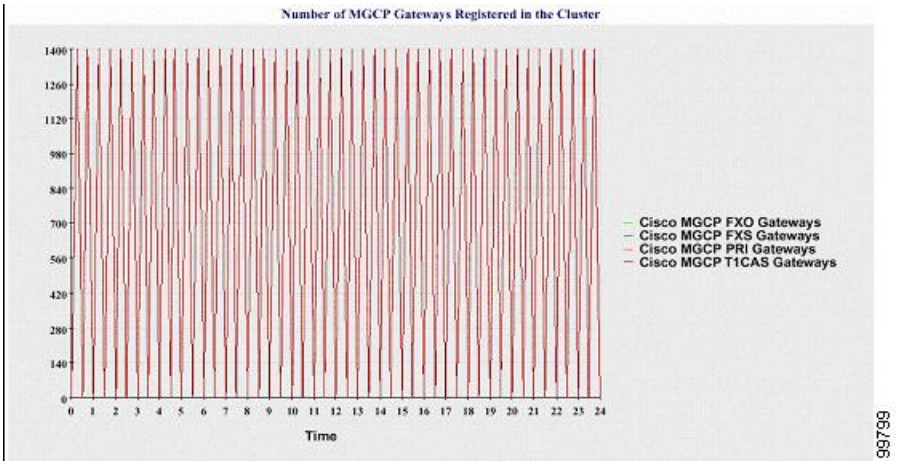
叢集中已註冊的 MGCP 閘道數

折線圖顯示已註冊的 MGCP FXO、FXS、PRI 和 T1CAS 閘道數。 每條線僅代表 Unified Communications Manager 伺服器 (或 Unified Communications Manager 叢集組態中的叢集) 的資料；因此，四條線顯示每種閘道類型的伺服器 (或全叢集) 詳細資料。 圖表中的每個資料值代表 15 分鐘內註冊的平均 MGCP 閘道數。 若伺服器 (或叢集中的所有伺服器) 的閘道沒有任何資料，則 回報工具 不會產生線條，代

表該特定閘道的資料。 若伺服器 (或叢集中的所有伺服器) 的所有閘道沒有任何資料，則 回報工具 不會產生圖表。

圖 *5:* 描述每個叢集之已註冊閘道數的折線圖

下圖顯示折線圖範例，代表 Unified Communications Manager 叢集組態中每個叢集的已註冊閘道數。

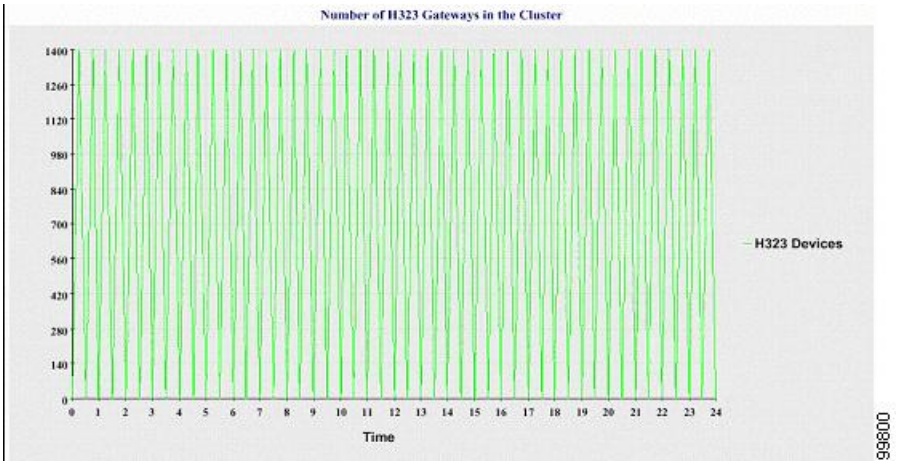


叢集中的 H.323 閘道數

顯示 H.323 閘道數的折線圖。 一條線代表 H.323 閘道的詳細資料 (或 Unified Communications Manager 叢集組態中的全叢集詳細資料)。 圖表中的每個資料值代表 15 分鐘內的平均 H.323 閘道數。 若伺服器 (或叢集中的所有伺服器) 的 H.323 閘道沒有任何資料，則 回報工具 不會產生圖表。

圖 *6:* 描述每個叢集之已註冊 *H.323* 閘道數的折線圖

下圖顯示折線圖範例，代表 Unified Communications Manager 叢集組態中每個叢集的 H.323 閘道數。



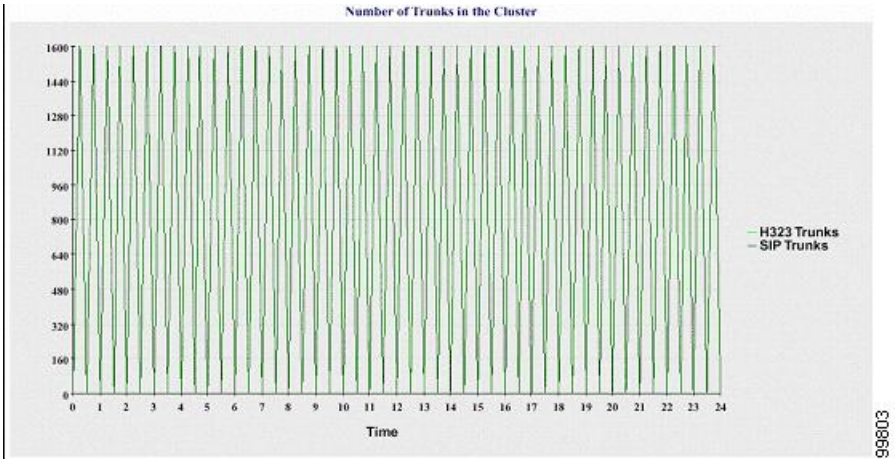
叢集中的 Trunk 數

顯示 H.323 和 SIP Trunk 數的折線圖。 兩條線代表 H.323 Trunk 和 SIP Trunk 的詳細資料 (或 Unified Communications Manager 叢集組態中的全叢集詳細資料)。 圖表中的每個資料值代表 15 分鐘內的平均 H.323 和 SIP Trunk 數。 若伺服器 (或叢集中的所有伺服器) 的 H.323 Trunk 沒有任何資料，則 回報工具 不會產生線條，代表 H.323 Trunk 的資料。 若伺服器 (或叢集中的所有伺服器) 的 SIP Trunk

沒有任何資料，則 回報工具 不會產生線條，代表 SIP Trunk 的資料。 若 Trunk 根本沒有資料，則 回報工具 不會產生圖表。

圖 *7:* 描述每個叢集之 *Trunk* 數的折線圖

下圖顯示折線圖範例，代表 Unified Communications Manager 叢集組態中每個叢集的 Trunk 數。



伺服器 (或叢集中的每部伺服器) 包含與檔案名稱型式 DeviceLog_mm_dd_yyyy_hh_mm.csv 相符的記錄檔。 下列資訊存在於記錄檔中：

- 伺服器 (或 Unified Communications Manager 叢集中的每部伺服器) 上的已註冊電話數
- 伺服器 (或 Unified Communications Manager 叢集中的每部伺服器) 上的已註冊 MGCP FXO、FXS、PRI 和 T1CAS 閘道數
- 伺服器 (或 Unified Communications Manager 叢集中的每部伺服器) 上的已註冊 H.323 閘道數
- SIP Trunk 和 H.323 Trunk 數

伺服器統計資料報告

伺服器統計資料報告提供以下折線圖：

- 每部伺服器的 CPU 百分比
- 每部伺服器的記憶體使用量百分比
- 每部伺服器最大分割區的硬碟使用量百分比

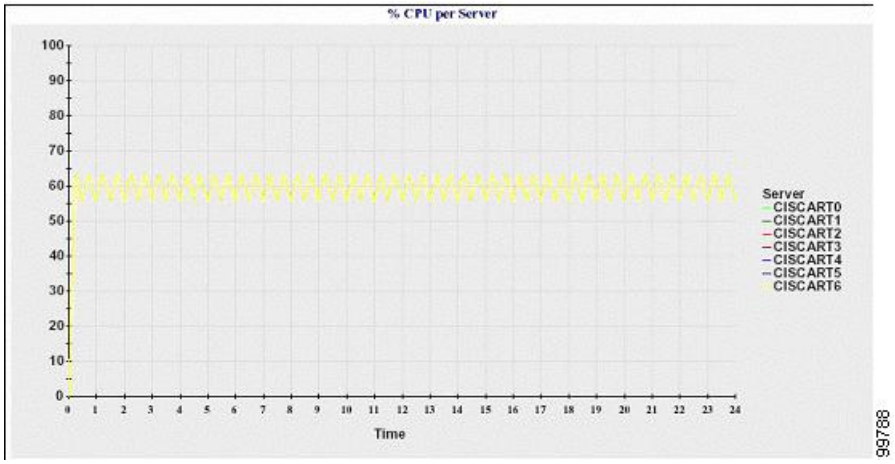
僅 Unified Communications Manager 和 IM and Presence Service 支援叢集特定統計資料。

每部伺服器的 CPU 百分比

折線圖顯示伺服器 (或叢集中的每部伺服器) 的 CPU 使用量百分比。 圖表中的線條代表有可用資料之伺服器的資料 (或代表叢集中每部伺服器的一條線)。 圖表中的每個資料值代表 15 分鐘內的平均 CPU 使用量。 若伺服器 (或叢集中的任一伺服器) 沒有任何資料，則 回報工具 不會產生線條，代表該伺服器。 若沒有要產生的線條，回報工具 不會建立圖表。 這時會顯示訊息“伺服器統計資料報告沒有可用的資料”。

圖 *8:* 描述每部伺服器的 *CPU* 百分比的折線圖

下圖顯示折線圖範例，代表 Unified Communications Manager 叢集組態中每部伺服器的 CPU 使用量百分比。

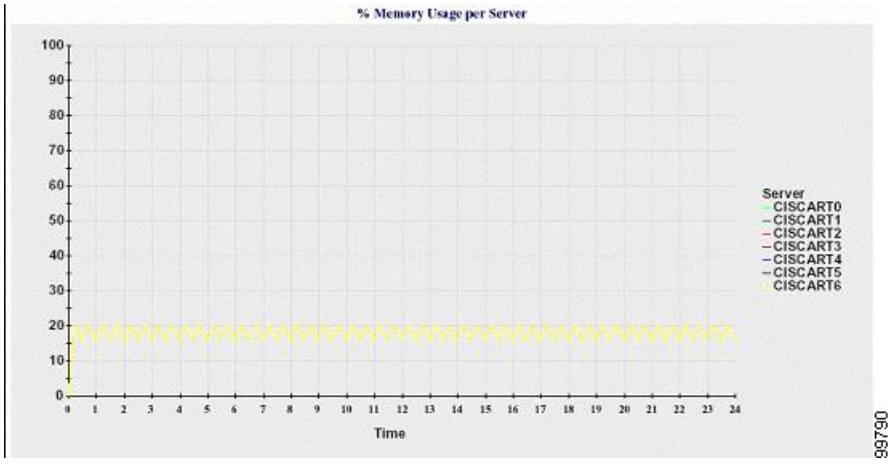


每部伺服器的記憶體使用量百分比

折線圖顯示 Unified Communications Manager 伺服器的記憶體使用量百分比 (%MemoryInUse)。 在 Unified Communications Manager 叢集組態中，叢集中有可用資料的每部伺服器都有一條線。 圖表中的每個資料值代表 15 分鐘內的平均記憶體使用量。 若沒有資料，則 回報工具 不會產生圖表。 若叢集組態中的任何伺服器都沒有資料，回報工具 不會產生線條，代表該伺服器。

圖 *9:* 描述每部伺服器的記憶體使用量百分比的折線圖

下圖顯示折線圖範例，代表叢集組態中每部 Unified Communications Manager 伺服器的記憶體使用量百分比。



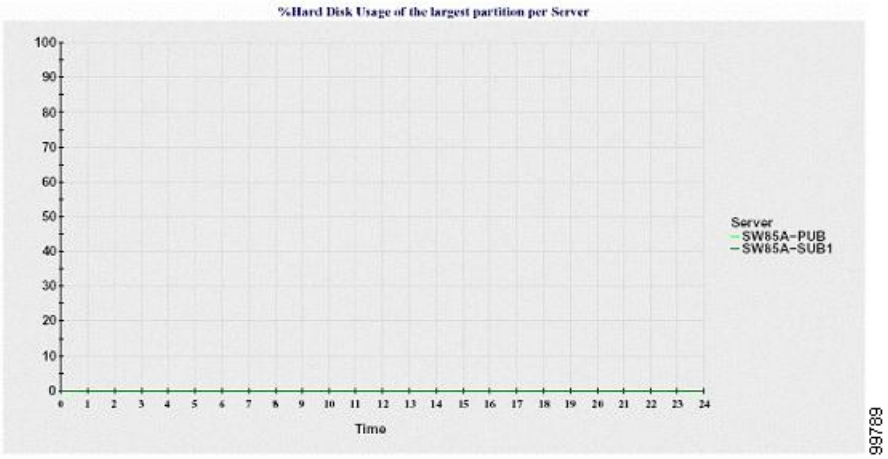
每部伺服器最大分割區的硬碟使用量百分比

折線圖顯示伺服器或叢集組態中每部伺服器上最大分割區的硬碟空間使用量百分比 (%DiskSpaceInUse)。 圖表中的每個資料值代表 15 分鐘內的平均硬碟使用量。 若沒有資料，則 回報

工具 不會產生圖表。 若叢集組態中的任一伺服器都沒有資料，回報工具 不會產生線條，代表該伺服器。

圖 *10*: 描述每部伺服器最大分割區的硬碟使用量百分比的折線圖

下圖顯示折線圖範例，代表 Unified Communications Manager 叢集組態中每部伺服器最大分割區的硬碟使用量百分比。



伺服器 (或叢集組態中的每部伺服器) 包含與檔案名稱型式 ServerLog_mm_dd_yyyy_hh_mm.csv 相符的記錄檔。 下列資訊存在於記錄檔中：

- 伺服器 (或叢集中的每部伺服器) 上的 CPU 使用量百分比
- 伺服器 (或叢集中的每部伺服器) 上的記憶體使用量百分比 (%MemoryInUse)
- 伺服器 (或叢集中的每部伺服器) 上最大分割區的硬碟使用量百分比 (%DiskSpaceInUse)

服務統計資料報告

服務統計資料報告不支援 IM and Presence Service和 Cisco Unity Connection。

服務統計資料報告提供以下折線圖：

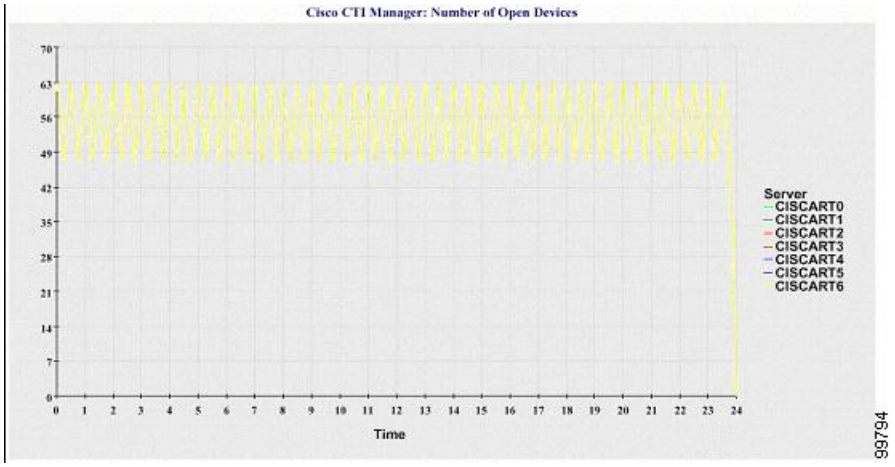
- Cisco CTI 管理員：開啓的裝置數
- Cisco CTI 管理員：開啓的線路數
- Cisco TFTP：請求數
- Cisco TFTP：中止的請求數

Cisco CTI 管理員：開啟的裝置數

折線圖顯示 CTI 管理員 (或 Unified Communications Manager 叢集組態中的每個 CTI 管理員) 的 CTI 開啓裝置數。 每個折線圖代表啓用服務的伺服器 (或 Unified Communications Manager 叢集中的每部伺服器) 的資料。 圖表中的每個資料值代表 15 分鐘內的平均 CTI 開啓裝置數。 若沒有資料，則 回報工具 不會產生圖表。 若 Unified Communications Manager 叢集組態中皆無任一部伺服器的資料，回報工具不會產生代表該伺服器的線條。 這時會顯示訊息“服務統計資料報告沒有可用的資料”。

圖 *11:* 描述 ***Cisco CTI*** 管理員的折線圖：開啟的裝置數

下圖顯示折線圖範例，顯示的爲 Unified Communications Manager 叢集組態中每個 Cisco CTI 管理員的開啓裝置數目。

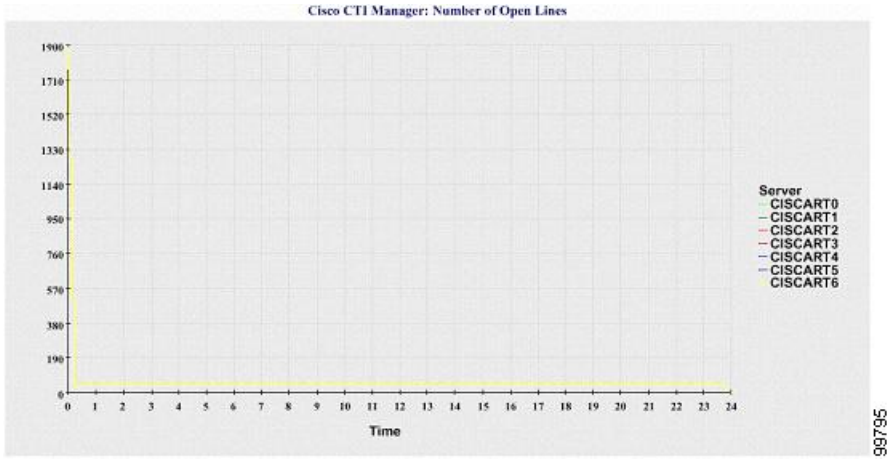


Cisco CTI 管理員：開啟的線路數

折線圖顯示 CTI 管理員 (或 Unified Communications Manager 叢集組態中的每個 CTI 管理員) 的 CTI 開啓線路數。 圖表中的線條代表啓用 Cisco CTI 管理員服務的伺服器的資料 (或表示 Unified Communications Manager 叢集組態中每部伺服器的一條線)。 圖表中的每個資料值代表 15 分鐘內的平均 CTI 開啓線路數。 若沒有資料，則 回報工具 不會產生圖表。 若 Unified Communications Manager 叢集組態中皆無任一部伺服器的資料，回報工具不會產生代表該伺服器的線條。

圖 *12:* 描述 ***Cisco CTI*** 管理員的折線圖：開啟的線路數

下圖顯示折線圖範例，代表 Unified Communications Manager 叢集組態中每個 Cisco CTI 管理員的開啓線路數。



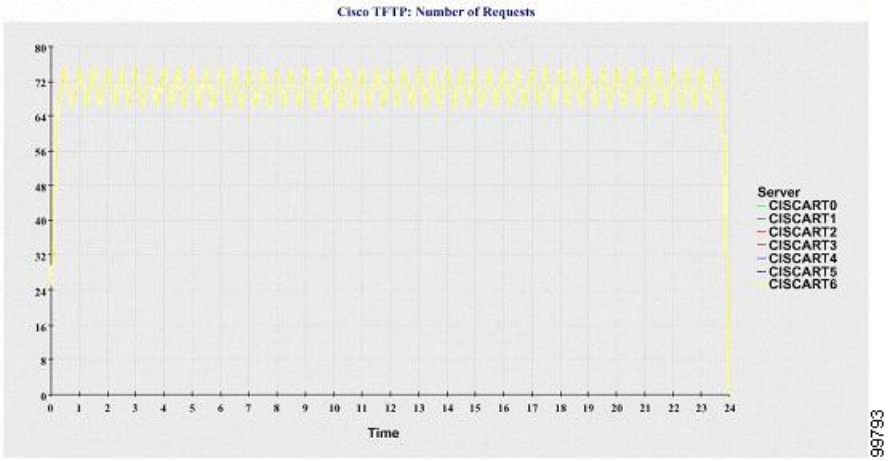
Cisco TFTP：請求數

折線圖顯示 TFTP 伺服器 (或 Unified Communications Manager 叢集組態中的每部 TFTP 伺服器) 的 Cisco TFTP 請求數量。 圖表中的線條代表啓用 Cisco TFTP 服務的伺服器的資料 (或表示 Unified

Communications Manager 叢集中每部伺服器的一條線)。 圖表中的每個資料值代表 15 分鐘內的平均 TFTP 請求數量。 若沒有資料，則 回報工具 不會產生圖表。 若 Unified Communications Manager 叢集組態中皆無任一部伺服器的資料，回報工具不會產生代表該伺服器的線條。

圖 *13:* 描述 *Cisco TFTP* 的折線圖：請求數

下圖顯示折線圖範例，其中代表每部 TFTP 伺服器的 Cisco TFTP 請求數量。

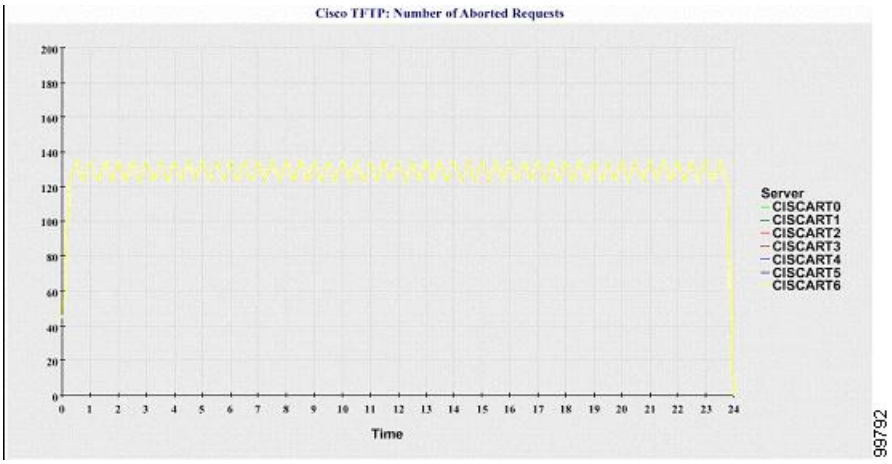


Cisco TFTP：中止的請求數

折線圖顯示 TFTP 伺服器 (或 Unified Communications Manager 叢集組態中的每部 TFTP 伺服器) 已中止的 Cisco TFTP 請求數量。 圖表中的線條代表啓用 Cisco TFTP 服務的伺服器的資料 (或表示 Unified Communications Manager 叢集中每部伺服器的一條線)。 圖表中的每個資料值代表 15 分鐘內的平均已中止 TFTP 請求數量。 若沒有資料，則 回報工具 不會產生圖表。 若 Unified Communications Manager 叢集組態中皆無任一部伺服器的資料，回報工具不會產生代表該伺服器的線條。

圖 *14:* 描述 *Cisco TFTP* 的折線圖：中止的請求數

下圖顯示折線圖範例，其中代表每部 TFTP 伺服器已中止的 Cisco TFTP 請求數量。



伺服器 (或 Unified Communications Manager 叢集中的每部伺服器) 包含符合檔案名稱型式 ServiceLog_mm_dd_yyyy_hh_mm.csv 的記錄檔。 下列資訊存在於記錄檔中：

- 對於每個 Cisco CTI 管理員 - 開啓的裝置數
- 對於每個 Cisco CTI 管理員 - 開啓的線路數
- 對於每部 Cisco TFTP 伺服器 - TotalTftpRequests
- 對於每部 Cisco TFTP 伺服器 - TotalTftpRequestsAborted

通話活動報告

通話活動報告不支援 IM and Presence Service和 Cisco Unity Connection。

通話活動報告提供以下折線圖：

- 叢集的 Unified Communications Manager 通話活動
- 叢集的 H.323 閘道通話活動
- 叢集的 MGCP 閘道通話活動
- MGCP 閘道
- 叢集的 Trunk 閘道通話活動

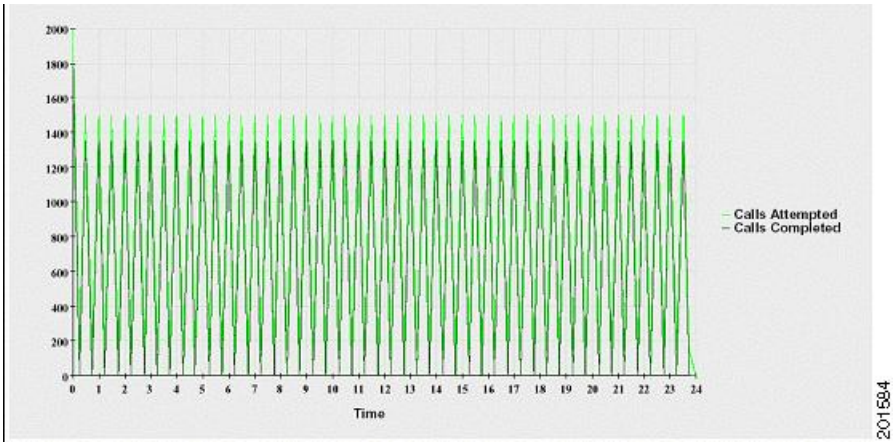
叢集的 Cisco Unified Communications Manager 通話活動

折線圖顯示已嘗試的 Unified Communications Manager 通話次數和已完成的通話次數。 在 Unified Communications Manager 叢集組態中，折線圖顯示整個叢集已嘗試和完成的通話次數。 圖表包括兩條線，一條表示已嘗試的通話次數，另一條則表示已完成的通話次數。 Unified Communications Manager 叢集組態中，每條線條代表叢集值，此值是叢集中所有伺服器 (有可用資料) 之值的總和。 圖表中的每個資料值代表在 15 分鐘內已嘗試的通話總次數或已完成的通話總次數。

若已完成的 Unified Communications Manager 通話沒有任何資料，則回報工具不會產生線條以代表已完成之通話的資料。 若已嘗試的 Unified Communications Manager 通話沒有任何資料，則回報工具不會產生線條以代表已嘗試之通話的資料。 在 Unified Communications Manager 叢集組態中，若叢集中的伺服器沒有資料，回報工具不會產生線條以代表已在該伺服器上嘗試或完成的通話。 若根本沒有用於 Unified Communications Manager 通話活動的資料，則回報工具不會產生圖表。 這時會顯示訊息“通話活動報告沒有可用的資料”。

圖 *15:* 描述叢集之 *Cisco Unified Communications Manager* 通話活動的折線圖

下圖顯示折線圖，其代表 Unified Communications Manager 叢集已嘗試和已完成的通話次數。

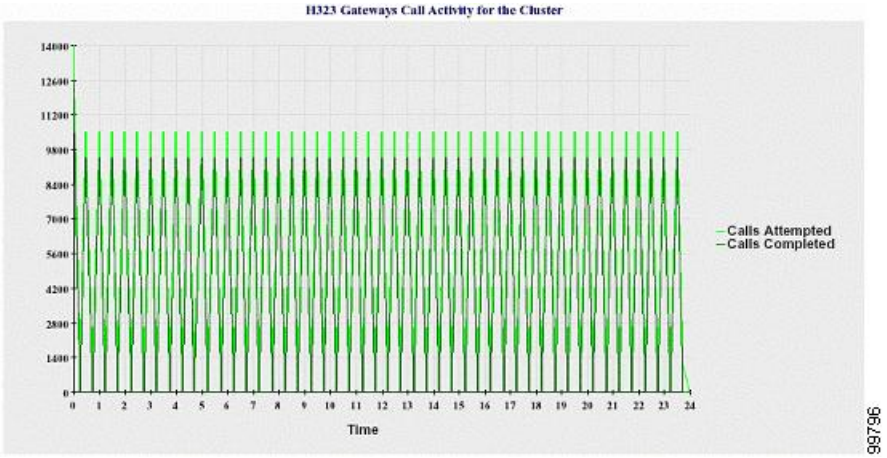


叢集的 H.323 閘道通話活動

折線圖顯示 H.323 閘道已嘗試的通話次數和已完成的通話次數。 在 Unified Communications Manager 叢集組態中，折線圖顯示整個叢集已嘗試和完成的通話次數。 圖表包括兩條線，一條表示已嘗試的通話次數，另一條則表示已完成的通話次數。 Unified Communications Manager 叢集組態中，每條線條代表叢集值，此值是叢集中所有伺服器 (有可用資料) 之值的總和。 圖表中的每個資料值代表在 15 分鐘內已嘗試的通話總次數或已完成的通話總次數。 若已完成的 H.323 閘道通話沒有任何資料，則回報工具不會產生線條以代表已完成之通話的資料。 若已嘗試的 H.323 閘道通話沒有任何資料，則回報工具不會產生線條以代表已嘗試之通話的資料。 在 Unified Communications Manager 叢集組態中，若叢集中的伺服器沒有資料，回報工具不會產生線條以代表已在該伺服器上嘗試或完成的通話。 若 H.323 閘道通話活動根本沒有資料，則 回報工具 不會產生圖表。

圖 *16:* 描述叢集的 *H.323* 閘道通話活動的折線圖

下圖顯示折線圖，其代表 Unified Communications Manager 叢集的 H.323 閘道通話活動。



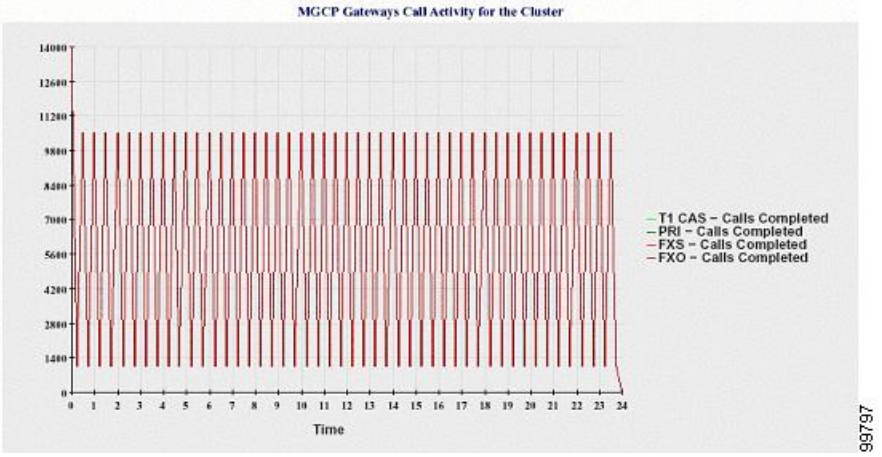
叢集的 MGCP 閘道通話活動

折線圖顯示 MGCP FXO、FXS、PRI 和 T1CAS 閘道在一小時內完成的通話次數。 在 Unified Communications Manager 叢集組態中，折線圖顯示整個 Unified Communications Manager 叢集已完成的通話次數。 圖表最多包含 4 條線，一條表示每種閘道類型 (有可用資料) 已完成的通話次數。 圖表

中的每個資料值代表在 15 分鐘內完成的通話總次數。 若閘道沒有任何資料，則回報工具不會產生線條，代表特定閘道已完成之通話的資料。 若所有閘道沒有資料，則回報工具不會產生圖表。

圖 *17:* 描述叢集的 *MGCP* 閘道通話活動的折線圖

下圖顯示折線圖，其代表 Unified Communications Manager 叢集的 MGCP 閘道通話活動。

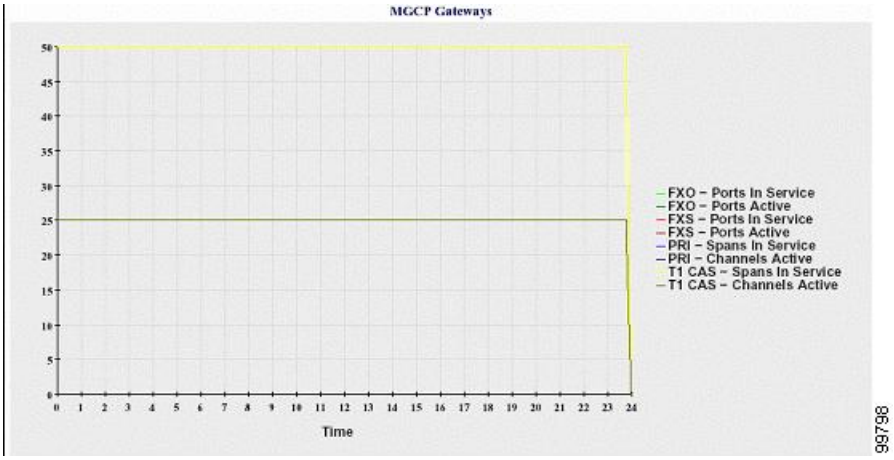


MGCP 閘道

折線圖顯示 MGCP FXO、FXS 閘道的「服務中通訊埠」和「活躍的通訊埠」的數目，以及 PRI、T1CAS 閘道的「服務中跨距」或「活躍的通道」的數目。 Unified Communications Manager 叢集組態中，折線圖顯示整個 Unified Communications Manager 叢集的資料。 圖表中有八條線，MGCP FXO 和 FXS 的「服務中通訊埠」數目各有兩條線，而 MGCP FXO 和 FXS 的「活躍的通訊埠」數目各有兩條線。 另外四條線爲 PRI 和 T1CAS 閘道的「服務中跨距」數目和「活躍的通道」數目所佔用。 Unified Communications Manager 叢集組態中，每條線條代表叢集值，此值是叢集中所有伺服器 (有可用資料) 之值的總和。 圖表中的每個資料值均代表 15 分鐘內「服務中通訊埠」、「活躍的通訊埠」、「服務中跨距」或「活躍的通道」的總數。 若沒有資料表示所有伺服器之閘道 (MGCP PRI、T1CAS)的「服務中跨距」或「活躍的通道」數目，則回報工具不會產生代表該特定閘道之資料的線條。

圖 *18:* 描繪 *MGCP* 閘道的折線圖

下圖顯示代表 MGCP 閘道的折線圖。

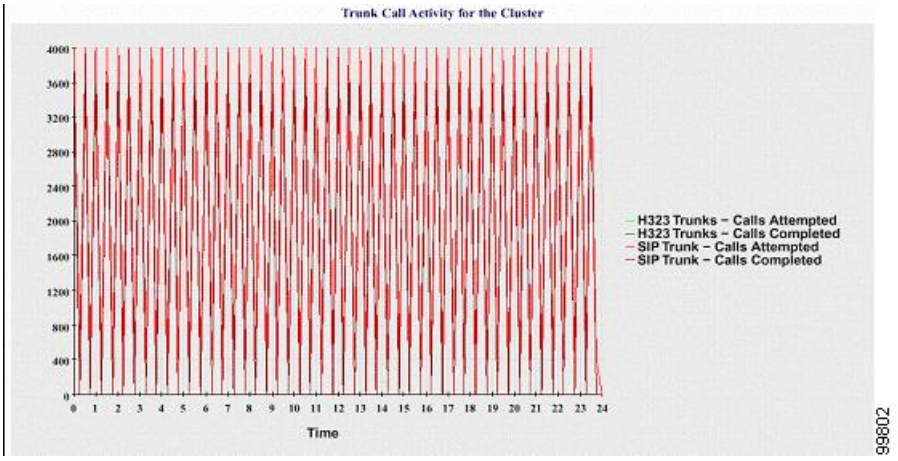


叢集的 Trunk 閘道通話活動

折線圖顯示 SIP Trunk 和 H.323 Trunk 在一小時內已嘗試的通話次數和已完成的通話次數。 Unified Communications Manager 叢集組態中，折線圖顯示整個 Unified Communications Manager 叢集已完成的通話次數和已嘗試的通話次數。 圖表中有四條線，兩條表示每個 SIP 和 H.323 Trunk (有可用資料) 已完成的通話次數，另兩條則表示已嘗試的通話次數。 Unified Communications Manager 叢集組態中，每條線條代表叢集值，此值是叢集中所有節點 (有可用資料) 之值的總和。 圖表中的每個資料值代表或在 15 分鐘內已完成的通話總次數或已嘗試的通話次數。 若 Trunk 沒有任何資料，則 回報工具 不會產生線條，代表特定 Trunk 已完成之通話i或已嘗試之通話的資料。 若兩種 Trunk 類型都沒有資料，則 回報工具 不會產生圖表。

圖 *19:* 描述叢集的 *Trunk* 通話活動的折線圖

下圖顯示折線圖，其代表 Unified Communications Manager 叢集的 Trunk 通話活動。



伺服器 (或 Unified Communications Manager 叢集組態中的每部伺服器) 包含符合檔案名稱型式 CallLog_mm_dd_yyyy_hh_mm.csv 的記錄檔。 下列資訊存在於記錄檔中：

- Unified Communications Manager (或 Unified Communications Manager 叢集中的每部伺服器) 已嘗試的通話和已完成的通話
- H.323 閘道 (或 Unified Communications Manager 叢集中每部伺服器的閘道) 已嘗試的通話和已完成的通話
- MGCP FXO、FXS、PRI 和 T1CAS 閘道 (或 Unified Communications Manager 叢集中每部伺服器的閘道) 已完成的通話
- PRI 和 T1CAS 閘道 (在 Unified Communications Manager 叢集中的每部伺服器中) 的服務中連接埠、MGCP FXO 和 FXS 閘道的作用中連接埠，以及服務中跨距
- H.323 Trunk 和 SIP Trunk 已嘗試的通話和已完成的通話

警示摘要報告

警示摘要報告提供了當天產生之警示的詳細資料。

僅 Unified Communications Manager 和 IM and Presence Service 支援叢集特定統計資料。

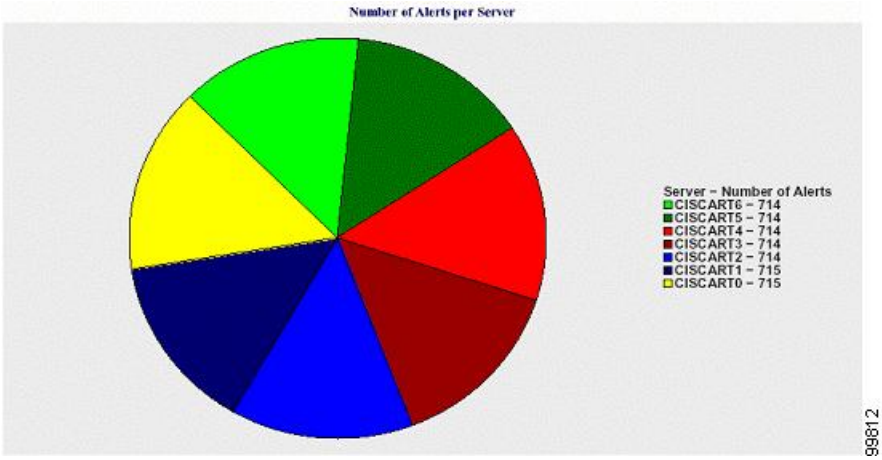
每部伺服器的警示數

圓形圖提供叢集中每個節點的警示數。此圖表顯示所產生之警示的全伺服器詳細資料。圓形圖的每個扇區代表爲叢集中特定伺服器產生的警示數。 此圖表包含的扇區與叢集中的伺服器 (回報工具會在當天爲其產生警示) 一樣多。 若一個伺服器沒有資料，則圖表中沒有扇區代表該伺服器。 若所有伺服器皆無資料，則回報工具不會產生圖表。 “當日未有產生任何警示”訊息即會顯示。

僅限 Cisco Unity Connection：圓形圖提供伺服器的警示數。 此圖表顯示所產生之警示的全伺服器詳細資料。 若伺服器沒有資料，則 回報工具 不會產生圖表。 訊息「當天沒有產生任何警示」即會顯示。

下圖顯示圓餅圖的範例，其代表 Unified Communications Manager 叢集中每部伺服器的警示數。

圖 *20:* 描述每部伺服器警示數的圓形圖

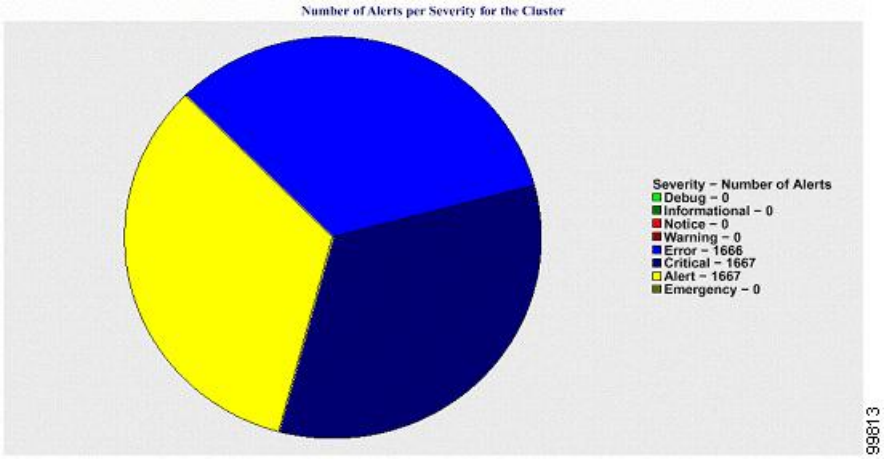


叢集的每個嚴重性的警示數

圓形圖顯示每個警示嚴重性的警示數。此圖表顯示所產生之警示的嚴重性詳細資料。圓形圖的每個扇區代表針對特定嚴重性類型產生的警示數。 此圖表提供的扇區與嚴重性 (回報工具 會在當天爲其產生警示) 一樣多。 若嚴重性沒有資料，則圖表中沒有扇區代表該嚴重性。 若沒有資料，則 回報工具 不會產生圖表。

下圖顯示圓餅圖的範例，其代表 Unified Communications Manager 叢集中各等嚴重性的警示數。

圖 *21:* 描述叢集每個嚴重性警示數的圓形圖

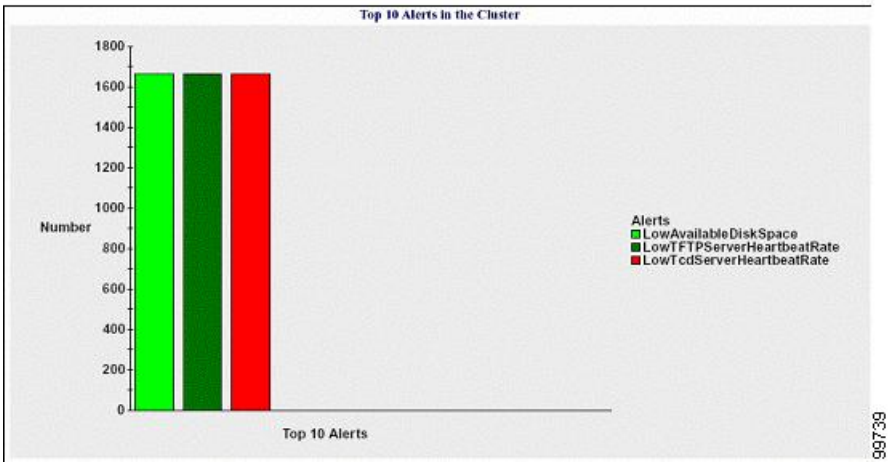


叢集中的十大警示

條形圖顯示特定警示類型的警示數。此圖表根據警示類型顯示所產生之警示的詳細資料。每列代表警示類型的警示數。此圖表會根據最高警示數依遞減排序僅顯示前十大警示的詳細資料。若特定警示類型沒有資料，則沒有條形代表該警示。 若任何警示類型沒有資料，則 RTMT 不會產生圖表。

下圖顯示圓餅圖的範例，其代表 Unified Communications Manager 叢集中前十大的警示。

圖 *22:* 描述叢集中前 *10* 大警示的條形圖



伺服器 (或叢集中的每部伺服器) 包含與檔案名稱型式 AlertLog_mm_dd_yyyy_hh_mm.csv 相符的記錄檔。 下列資訊存在於記錄檔中：

- 時間 - 發生警示的時間
- 警示名稱 - 描述性名稱
- 節點名稱 - 發生警示的伺服器
- 監控的物件 - 受監控的物件

- 嚴重性 - 此警示的嚴重性

效能保護報告

效能保護報告不支援 IM and Presence Service和 Cisco Unity Connection。

效能保護報告會提供一個摘要，其中包含不同的圖表，顯示該特定報告的統計資料。 Reporter 會根據記錄的資訊產生報告，每天一次。

效能保護報告提供有關最後七個預設監控物件的趨勢分析資訊，讓您可以追蹤 Cisco Intercompany Media Engine 的相關資訊。 此報告包括 Cisco IME 使用者端通話活動圖表，其中顯示 Cisco IME 使用者端的通話總數和後援通話率。

效能保護報告包含以下圖表：

- Cisco Unified Communications Manager 通話活動
- 已註冊電話和 MGCP 閘道的數量
- 系統資源用量
- 裝置和撥號計劃數量

Cisco Unified Communications Manager 通話活動

折線圖顯示已嘗試的通話次數和已完成的通話次數，作爲進行中通話次數每小時的增加率或減少率。 Unified Communications Manager 叢集組態的方面，會爲叢集中的每部伺服器繪製資料圖表。 此圖表包括三條線，一條表示已嘗試的通話次數、一條表示已完成的通話次數、一條則表示作用中通話。 若通話活動沒有資料，則回報工具不會產生圖表。

已註冊電話和 MGCP 閘道的數量

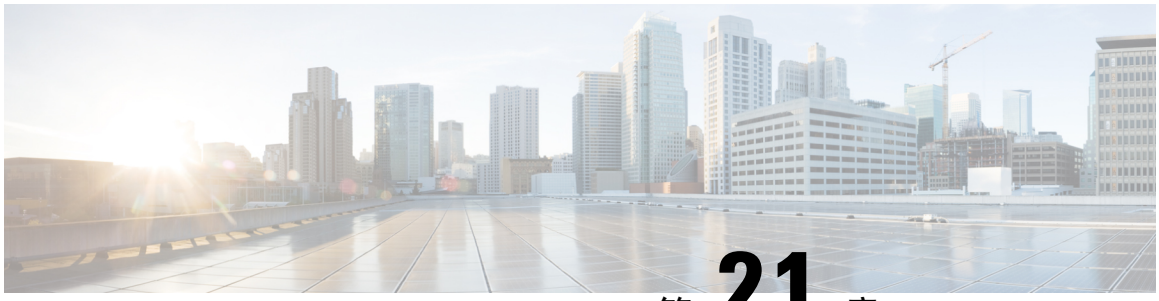
折線圖顯示已註冊電話和 MGCP 閘道數。 Unified Communications Manager 叢集組態的方面，此圖表顯示叢集中每部伺服器的資料。圖表包括兩條線，一條表示已註冊電話數，另一條表示 MGCP 閘道數。 若電話或 MGCP 閘道沒有資料，則回報工具不會產生圖表。

系統資源用量

折線圖顯示 CPU 負載百分比，以及用於伺服器 (或 Unified Communications Manager 叢集組態中的整個叢集) 的記憶體百分比 (以位元組爲單位)。 此圖表包括兩條線，一條表示 CPU 負載，一條表示記憶體使用量。 在 Unified Communications Manager 叢集中，每條線條代表叢集值，此值是叢集中所有伺服器 (有可用資料) 的平均值。 若電話或 MGCP 閘道沒有資料，則回報工具不會產生圖表。

裝置和撥號計劃數量

兩個表格顯示來自 Unified Communications Manager 資料庫，有關裝置數和撥號計劃元件數的資訊。 裝置表顯示 IP 電話、Cisco Unity Connection 連接埠、H.323 使用者端、H.323 閘道、MGCP 閘道、MOH 資源和 MTP 資源的數量。 撥號計劃表顯示目錄號碼和線路、路由型式以及轉譯型式的數量。



第 21 章

Cisco Unified 報告

合併資料報告

從 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service 主控台存取的 Cisco Unified 報告 Web 應用程式會產生合併報告，以供疑難排解或檢查叢集資料。

附註 除非另有說明，否則本指南中的資訊、附註和程式適用於 Unified Communications Manager 和 IM and Presence Service。

此工具提供輕鬆取得叢集資料概觀的方式。 工具會從現有來源收集資料、比較資料及回報不正確之處。 在 Cisco Unified 報告中產生報告時，報告會將一或多部伺服器上的一或多個來源的資料合併爲一個輸出檢視。 例如，您可以檢視報告中有關主機檔案之叢集中的所有伺服器。

Cisco Unified 報告 Web 應用程式在安裝時會部署到叢集中的所有節點。 報告是從資料庫記錄產生的。

附註 在 Cisco Business Edition 5000 伺服器上，Cisco Unified 報告應用程式只會擷取 Unified Communications Manager 的資料。 由於大小限制，該應用程式無法擷取 Cisco Unity Connection 的資料。 您可以使用該工具來收集有關 Unified Communications Manager 安裝的重要資訊。

用於產生報告的資料來源

應用程式從發佈者節點和每個訂閱者節點上的以下任何來源擷取資訊。

- RTMT 計數器

- CDR_CAR (僅適用於 Unified Communications Manager)
- Unified Communications Manager DB (僅適用於 Unified Communications Manager)
- IM and Presence DB (僅適用於 IM and Presence Service)
- 硬碟檔案
- 作業系統 API 通話
- 網路 API 通話
- 偏好設定
- CLI
- RIS

報告包含所有啓用中叢集的資料，這些資料可在產生報告時存取。 若發佈者節點上的資料庫已關閉，則可以爲啓用中的節點產生報告。 系統報告清單中的報告說明報告提供了報告的資訊來源。

支援的輸出格式

此版本支援報告的 HTML/CSV 輸出。 您可以在 Cisco Unified Reporting 中依報告名稱和日期和時間標記識別報告。該應用程式儲存最新的報告本機副本供您檢視。您可以按照“下載新報告”中的說明將最新報告的本機副本或新報告下載到硬碟上。 下載報告後，您可以重新命名下載的檔案或將其儲存在不同的資料夾中以進行識別。

系統需求

Cisco Tomcat 服務

Cisco Unified Reporting 在 Cisco Tomcat 服務上作爲應用程式執行，在您安裝 Unified Communications Manager 和 IM and Presence Service 時會啓動。 確保這些產品正在叢集的所有節點上執行。

HTTPS

報告子系統透過 HTTPS 使用 RPC 機制從其他節點收集資訊。 確保 HTTPS 連接埠已開啓，並且 Cisco Tomcat 服務正在節點上執行，以成功產生報告。

要啓用 HTTPS，需在連線過程中下載用於識別該節點的憑證。 您可以僅接受目前作業階段的節點憑證，也可以將憑證下載到信任的資料夾 (檔案) 以保護與該節點有關的目前和未來的作業階段。 信任資料夾會儲存所有受信任站台的憑證。 如需有關 HTTPS 的詳細資訊，請參閱《*Cisco Unified Communications Manager* 管理指南》中的“簡介”一章。

要存取該應用程式，請在瀏覽器視窗中存取管理介面。 CIsco Unified Reporting 使用 HTTPS 建立與瀏覽器的安全連線。

所需的存取權限

Cisco Unified 報告應用程式使用 Cisco Tomcat 服務驗證使用者，然後才允許存取 Web 應用程式。 只有授權的使用者才能存取 Cisco Unified 報告應用程式。 對於Unified Communications Manager，預設情況下，只有標準 CCM 超級使用者群組中的管理員使用者可以存取 Cisco Unified 報告以檢視和建立報告。

對於 Cisco Unified Communications Manager 和 IM and Presence 服務而言，標準 CUReporting 驗證角色的使用者可以存取 Cisco Unified 報告。

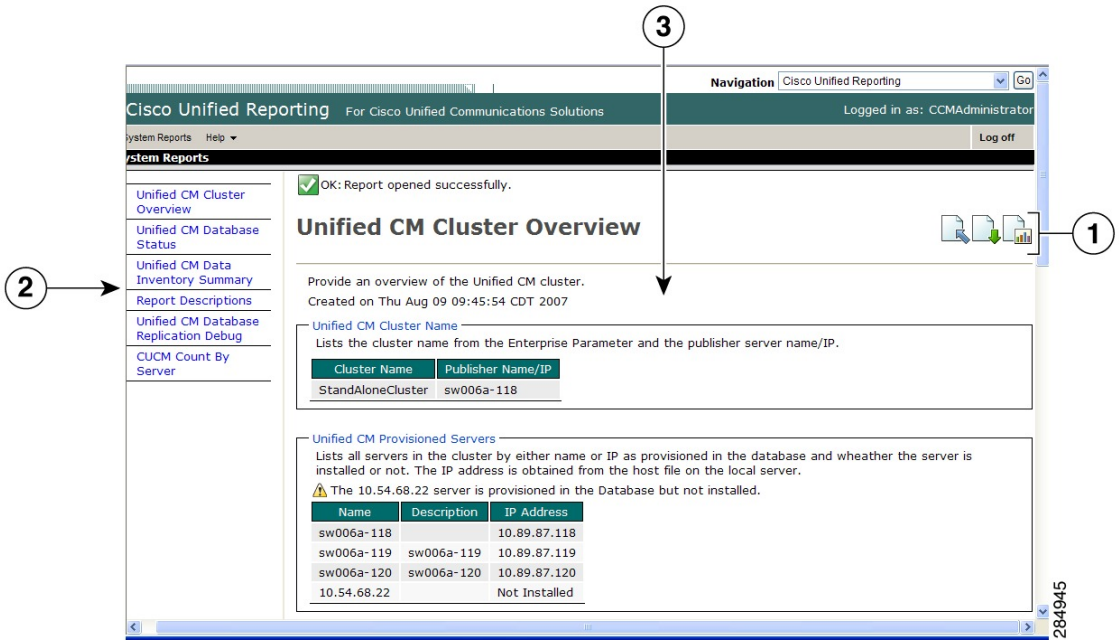
作爲授權的使用者，您可以使用 Cisco Unified 回報 UI 以檢視報告、產生新報告或下載報告。

附註 Unified Communications Manager方面，標準 CCM 超級使用者群組中的管理員使用者可以存取 Unified Communications Manager 管理導覽功能表中的管理應用程式，包括 Cisco Unified 報告，只需單一登入至其中一個應用程式。

UI 元件

下圖顯示用於 Cisco Unified 回報 的 UI 元件。

圖 *23: UI* 元件



1. 上傳、下載、產生圖示
2. 報告清單
3. 報告詳細資料

附註 報告類別、可用報告和報告資料因版本而異。

從管理介面登入

執行以下任一步驟，從管理介面登入至 Cisco Unified 報告。

- 若用 Unified Communications Manager，在 Cisco Unified CM 管理介面的導覽功能表中選擇 **Cisco Unified 報告**。
- 如果是 IM and Presence 服務，請選取 Cisco Unified CM IM and Presence 管理介面上導覽功能表中的 **Cisco Unified IM and Presence 報告**。

開始之前

確保您有權存取 Cisco Unified 報告應用程式。

當您登入 Cisco Unified 報告時，每個使用者上次成功的系統登入嘗試和上次不成功的系統登入嘗試以及使用者 ID、日期、時間和 IP 位址都會顯示在主要 Cisco Unified 報告視窗中。

支援的報告

本節詳細介紹了 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service 支援的報告。 您可以在 Cisco Unified Reporting 中依報告名稱和日期和時間標記識別報告。 Cisco Unified 回報會儲存最新報告的本機副本供您檢視。

Unified Communications Manager 報告

下表描述安裝了 Unified Communications Manager 後，顯示在 Cisco Unified 報告中的系統報告類型。

表 *74: Unified Communications Manager* 出現在 *Cisco Unified* 回報中的報告

報告	描述
具逾期憑證演算法的UCM使用者	提供一般使用者清單，這些使用者的密碼或PIN使用SHA1進行儲存和雜湊。
報告說明	提供有關顯示報告的疑難排解和詳細資訊。
安全性診斷工具	提供有關安全性元件資訊的摘要檢視。

報告	描述
Unified CM 叢集概觀	提供 Unified Communications Manager 叢集概觀。 該報告包括以下詳細資訊： • Unified Communications Manager 或 IM and Presence Service 叢集中安裝的版本 • 叢集中所有節點的主機名稱或 IP 位址 • 硬體詳細資訊摘要
Unified CM 資料摘要	提供 Unified Communications Manager 資料庫中存在的資料摘要，根據 Unified Communications Manager 管理中的功能表結構。 例如，若配置三個憑證原則，五個會議橋接和十個共用線路外觀，則可以在此報告中看到該類型的資訊。
Unified CM 資料庫複製除錯	提供資料庫複寫除錯資訊。 **提示** 產生此報告可能會讓 CPU 使用量激增，且叢集中的每個節點最多需要 10 秒的時間。
Unified CM 資料庫狀態	提供 Unified Communications Manager 資料庫執行狀況的快照。應在升級之前產生此報告，以確保資料庫狀況良好。
Unified CM 裝置計數摘要	依型號和通訊協定提供 Unified Communications Manager 資料庫中存在的裝置數量。
Unified CM 裝置分佈摘要	提供裝置如何在整個叢集中分佈的摘要；例如，此報告顯示哪些裝置與主要、次要和第三級節點關聯。
Unified CM 目錄 URI 和 GDPR 複製	提供系統上重複的使用者目錄URI、已學習的目錄URI、已學習的編號和已學習模式的詳細清單。
Unified CM Extension Mobility	提供以下內容的摘要：Cisco Extension Mobility 使用量；例如，具有 Cisco Extension Mobility 使用者登入的電話數量、與 Cisco Extension Mobiity 關聯的使用者等等。
Unified CM 地理位置原則	提供地理位置邏輯分割原則矩陣。
具有過濾器的 Unified CM 地理位置原則	針對選擇的地理位置原則提供地理位置邏輯分割原則矩陣。
不包含電話的 Unified CM 線路	提供不與電話關聯的線路清單。
Unified CM 多線路裝置	提供具有多線路狀態的電話清單。
Unified CM 電話類別	提供與通用裝置範本一起使用的給定類別中的電話型號清單。爲使用者啓用自我配置時，您可以爲每個類別提供範本來選擇允許任何或所有這些類別的電話。

報告	描述
Unified CM 電話功能清單	提供Unified Communications Manager管理中每種裝置類型中支援的功能清單。
Unified CM 電話地區設定安裝程式	提供已安裝的電話地區設定套件支援的 Cisco Unified IP 電話軔體版本清單。
包括不相符載入的 Unified CM 電話	提供具有不相符軔體載入的所有電話清單。
無線路的 Unified CM 電話	提供 Unified Communications Manager 資料庫中沒有與之關聯的所有電話清單。
Unified CM 共用線路	提供 Unified Communications Manager 資料庫中具有至少一個共用線路外觀的所有電話清單。
Unified CM Table 計數摘要	提供以資料庫爲中心的資料檢視。 該報告對於瞭解資料庫結構描述對管理員或 AXL API 開發人員十分有用。
Unified CM 使用者裝置數	提供有關關聯裝置的資訊；例如，此報告列出了沒有使用者的電話數量、擁有一部電話的使用者數量以及擁有一部以上電話的使用者數量。
Unified CM 使用者共用主要分機	提供共用系統上主要分機的使用者清單。
Unified CM VG2XX 閘道	提供閘道端點安全性設定檔的摘要。
Unified CM 語音信箱	提供 Unified Communications Manager 管理中與語音留言組態相關的摘要；例如，此報告列出已設的語音留言連接埠的數量、訊息等待指示器的數量、已設定語音留言設定檔的數量，與語音留言設定檔關聯的目錄號碼的數量等等。
Unified Confidential Access Level 矩陣	提供有關 Confidential Access Level 矩陣的所有資訊。

IM and Presence Service報告

下表描述在 Unified Communications Manager 上安裝 IM and Presence 服務後，顯示在 Cisco Unified 報告中的系統報告類型。

附註 從版本 10.0(1) 起，可從 Cisco Unified Communications Manager 節點取得 IM and Presence 叢集資訊。從 Cisco Unified Communications Manager，選擇 **Cisco Unified 報告** > **系統報告** > **Unified CM 叢集概觀**。

您可以在下表中檢視和產生任何報告類型。

表 *75:* 顯示在 *Cisco Unified* 報告中的 *IM and Presence* 服務報告

報告	描述
IM and Presence 資料庫複寫除錯	提供資料庫複寫除錯資訊。 **提示** 產生此報告可能會讓 CPU 使用量激增，且叢集中的每個節點最多需要 10 秒的時間。
IM and Presence 資料庫狀態	提供 IM and Presence Service資料庫執行狀況的快照。 應在升級之前產生此報告，以確保資料庫狀況良好。
IM and Presence 表格計數摘要	提供以資料庫爲中心的資料檢視。該報告證明了瞭解資料庫結構描述對管理員或 AXL API 開發人員十分有用。
IM and Presence 使用者作業階段報告	提供一或多個裝置的所有活躍使用者已登入之作業階段清單。
狀態組態報告	提供有關 IM and Presence Service使用者的組態資訊。 • 從 Cisco Unified Communications Manager 同步的使用者 • 可使用 IM and Presence Service的使用者 • 可使用 Microsoft 遠端通話控制的使用者 • 可使用 IM and Presence Service中行事曆資訊的使用者 請按一下**檢視詳細資料**在可排序的資料欄中查看使用者清單。
IM and Presence 叢集概觀	提供 IM and Presence Service叢集概觀。 例如，此報告可以告訴您叢集上安裝的 IM and Presence Service版本，叢集中所有節點的主機名稱或 IP 位址，硬體詳細資料摘要等資訊。
狀態限制警示報告	提供有關已達到或超過聯絡人或觀察者最大數量組態限制的使用者資訊。 請按一下**檢視詳細資料**在可排序的資料欄中查看使用者清單。
狀態使用情況報告	提供已登錄 XMPP 的使用者端和第三方 API 使用資訊。 請按一下**檢視詳細資料**在可排序的資料欄中查看 XMPP 使用者端和第三方 API 清單。
報告說明	提供有關顯示報告的疑難排解和詳細資訊。 此報告會提供報告、每個資訊群組、每個資料項目提供說明，以及資料來源、相關問題的症狀和補救措施。

檢視報告說明

Cisco Unified 報告提供報告說明。「報告說明」連結會提供報告、每個資訊群組和每個資料項目的說明，以及資料來源、相關問題的症狀和補救措施。

附註　您可能仍需要聯絡 TAC，以取得有關報告問題的其他說明。

程序

步驟 1 選擇**系統報告**。

步驟 2 在報告清單中選擇**報告說明**連結。

附註　若在選擇 IM and Presence 服務報告時，系統提示您重新登入，請重新輸入您的 Cisco Unified Communications Manager 管理登入認證。

步驟 3 選擇**產生報告**圖示。

即會產生並顯示報告。

產生新報告

您可以產生和檢視新報告。

開始之前

確保 Cisco Tomcat 服務正在至少一個節點上執行，並且您正在使用支援的 Web 瀏覽器檢視報告。

若需要過多時間產生報告，或耗用過多的CPU時間，則應用程式會通知您。 產生報告時會顯示進度列。 顯示新報告，並更新日期和時間。

程序

步驟 1 從功能表列中選擇**系統報告**。

步驟 2 選擇報告。

附註　若在選擇 IM and Presence 服務報告時，系統提示您重新登入，請重新輸入您的 Cisco Unified Communications Manager 管理登入認證。

步驟 3 在**報告**視窗中，選擇**產生報告** (長條圖) 圖示。

步驟 4 選擇**檢視詳細資料**連結，以顯示不會自動出現之區段的詳細資料。

下一步

若報告顯示項目的資料檢查不成功，請選擇**報告說明**報告，並檢閱疑難排解資訊和可能的補救措施。由於報告說明報告是從資料庫動態產生的，因此您還可以產生新的報告說明報告。

檢視儲存的報告

您可以檢視現有報告的副本。

附註 在全新安裝或升級期間，Cisco Unified 報告應用程式不會儲存最新報告的本機副本。

開始之前

確保 Cisco Tomcat 服務正在至少一個節點上執行，並且您正在使用支援的 Web 瀏覽器檢視報告。

程序

步驟 1 從功能表列中選擇**系統報告**。

步驟 2 從報告清單中選擇您要檢視的報告。

步驟 3 選擇報告名稱的連結 (日期和時間戳記)。

步驟 4 選擇**檢視詳細資料**連結，以取得未自動顯示之區段的的詳細資料。

下一步

下載新的或儲存的報告。

若報告顯示項目的資料檢查不成功，請選擇**報告說明**報告，並檢閱疑難排解資訊，以取得可能的補救措施。

下載新報告

要下載新報告，請將其本機儲存在硬碟上。 下載報告會將原始 XML 資料檔案下載到您的硬碟上。

程序

步驟 1 產生新報告。

步驟 2 新報告顯示後，請選擇**報告**視窗中的**下載報告** (綠色箭頭) 圖示。

附註 您不需要在下載檔案之前按一下**檢視詳細資料**連結來取得報告詳細資料。 資料會擷取在下載的檔案中。

步驟 3 選擇**儲存**將檔案儲存到您指定的硬碟位置。

要變更檔案名稱或檔案儲存在硬碟中的位置，請輸入新位置或重新命名檔案 (選用)。 進度欄會顯示檔案正在下載。

檔案下載至您的硬碟。

步驟 4 下載完成後，選擇**開啟**以開啓 XML 報告。

附註 不要變更 XML 檔案中的內容，否則您的報告可能無法正確顯示在畫面上。

下一步

要在瀏覽器中檢視下載的報告檔案，請將檔案上傳到您的節點。

附註 爲了獲得技術協助，您可以將下載的檔案附加到電子郵件中，或將檔案上傳到另一個節點。

下載儲存的報告

要下載已儲存的報告，請下載報告並將其儲存於本機硬碟。 下載報告會將原始 XML 資料檔案下載至您的硬碟。

程序

步驟 1 開啓並檢視現有報告的詳細資料。

步驟 2 選擇**報告**視窗中的**下載報告** (綠色箭頭) 圖示。

步驟 3 選擇**儲存**將檔案儲存到您指定的硬碟位置。

要變更檔案名稱或檔案儲存在硬碟中的位置，請輸入新位置或重新命名檔案 (選用)。 進度欄會顯示檔案正在下載。

檔案下載至您的硬碟。

步驟 4 下載完成後，選擇**開啟**以開啓 XML 報告。

附註 不要變更 XML 檔案中的內容，否則報告可能無法正確顯示。

下一步

要在瀏覽器中檢視下載的報告檔案，請將檔案上傳到您的節點。

附註 爲了獲得技術協助，您可以將下載的檔案附加到電子郵件中，或將檔案上傳到另一個節點。

上傳報告

若要在瀏覽器視窗檢視下載的報告，您需將報告上傳至節點。

開始之前

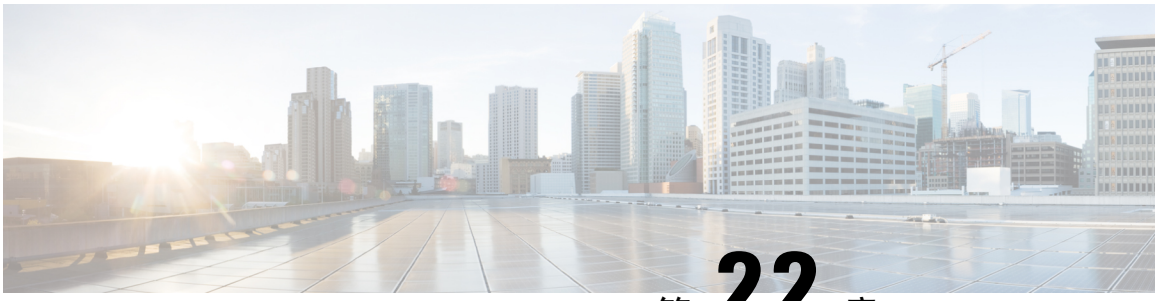
將報告下載到硬碟上。

程序

步驟 1 從功能表列中選擇**系統報告**。
步驟 2 存取任何報告，以將**上傳報告** (藍色箭頭) 圖示顯示在**報告**視窗中。
步驟 3 選擇**上傳報告**圖示。
步驟 4 若要尋找 .xml 檔案，請選擇**瀏覽**以導覽至其在硬碟上的位置。
步驟 5 選擇**上傳**。
步驟 6 選擇**繼續**以在瀏覽器視窗中顯示上傳的檔案。

下一步

您可以在升級期間並排比較上傳的報告和新產生的報告。



第 22 章

配置 Cisco IP 電話的通話診斷和品質回報

診斷與回報概覽

Cisco Unified Communications Manager 提供了兩個選項來確保 Cisco IP 電話上的通話品質：

- 通話診斷-通話診斷包括產生通話管理記錄（CMR）和語音品質指標。
- 品質回報工具 QRT)—QRT 爲一個適用於 Cisco IP 電話的語音品質及一般問題回報程式。 該工具讓使用者可輕鬆、準確地報告其 IP 電話的音訊和其他常見問題。

通話診斷概覽

您可以配置執行SCCP和SIP的Cisco IP電話來收集通話的診斷。 通話診斷包括通話管理記錄（CMR）（也稱爲診斷記錄）和語音品質指標。

語音品質指標預設情況下處於啓用狀態，且在大多數 Cisco IP 電話上均受支援。 Cisco IP 電話根據 MOS（平均意見平方）值計算語音品質指標。 音質指標不考慮雜訊或失真，僅考慮訊框遺失。

CMR 記錄是儲存有關通話中串流的音訊品質的資訊。 您可以配置 Unified Communications Manager 以產生 CMR。 此資訊對於後處理活動（例如產生帳單記錄和網路分析）很有用。

品質回報工具概覽

品質回報工具 (QRT) 爲一個適用於 Cisco IP 電話的語音品質及一般問題回報程式。 該工具讓使用者可輕鬆、準確地報告其 IP 電話的音訊和其他常見問題。

作爲系統管理員，您可以透過配置和指派軟鍵範本以在使用者 IP 電話上顯示 QRT 軟鍵來啓用 QRT 功能。 您可以從兩種不同的使用者模式中進行選擇，視您希望使用者使用 QRT 時與其互動的程度而定。 然後您可透過配置系統參數並設定 Cisco Unified Serviceability 工具來定義功能在系統中所運作方式。 您可以使用 QRT Viewer 應用程式建立、自訂和檢視電話問題報告。

當使用者在使用 IP 電話時遇到問題時，可以在掛下或已連線通話狀態期間按下Cisco IP 電話上的 QRT 功能鍵來回報問題的類型和其他相關統計資訊。 然後使用者即可選擇最能描述該 IP 電話所回報的問題的原因代碼。 自訂的電話問題報告將會提供特定的資訊。

使用者按下 QRT 功能鍵選擇問題類型後，QRT 將嘗試收集串流統計之資訊。 通話應至少進行 5 秒鐘，QRT 始能收集流統計資訊。

詳細通話回報和計費

Cisco CDR 分析和回報（CAR）工俱產生有關服務品質、流量、使用者通話量、計費和閘道的詳細報告。 CAR 使用來自通話詳細記錄（CDR），通話管理記錄（CMR）和 Unified Communications Manager 資料庫的資料來產生報告。 可在Cisco Unified Serviceability 的 **工具**功能表存取 CAR 介面。

CAR 不是意謂爲替代第三方公司所提供的通話計費和計費解決方案。 您可以透過搜尋Cisco開發者社區的主頁找到提供這些解決方案的公司，其皆爲 Cisco技術開發人員計劃的成員。

有關配置 CAR 回報的詳細資訊請參閱*Cisco Unified Communications Manager* 通話回報與計費管理指南。

Prerequisites

通話診斷必需條件

檢查您的 Cisco Unified IP 電話是否支援通話診斷。

使用此表來確定您的電話是否支援通話診斷。 “通話診斷支援”圖例如下：

- X-同時執行 SCCP 和 SIP 的電話支援
- 僅 S-SCCP 功能

表 *76:* 通話診斷的裝置支援

裝置	支援通話診斷
Cisco Unified IP 電話 7906	X
Cisco Unified IP 電話 7911	X
Cisco Unified IP 電話 7921	X
Cisco Unified IP 電話 7931	X
Cisco Unified IP 電話 7940	S
Cisco Unified IP 電話 7941	X
Cisco Unified IP 電話 7942-G	X
Cisco Unified IP 電話 7942-G/GE	X

裝置	支援通話診斷
Cisco Unified IP 電話 7945	X
Cisco Unified IP 電話 7960	S
Cisco Unified IP 電話 7961	X
Cisco Unified IP 電話 7962-G	X
Cisco Unified IP 電話 7962-G/GE	X
Cisco Unified IP 電話 7965	X
Cisco Unified IP 電話 7970	X
Cisco Unified IP 電話 7971	X
Cisco Unified IP 電話 7972-G/GE	X
Cisco Unified IP 電話 7975	X

品質回報工具必需條件

包括以下功能的任何 Cisco IP 電話：

- 支援軟鍵範本
- 支援 IP 電話服務
- 可透過 CTI 控制
- 包含一個內部 HTTP 伺服器

如需更多資訊請參閱您所使用電話機型的指南。

診斷及回報配置工作流程

程序

	命令或動作	目的
步驟 1	配置通話診斷 ，第 294 頁上的	執行此任務以配置 Cisco Unified Communications Manager 產生 CMR。 CMR 記錄是儲存有關通話中串流的音訊品質的資訊。 有關存取 CMR 的更多資訊，請參閱適用於 *Cisco Unified Communications Manager 12.5(1)SU1* 版的通話詳細記錄管理指南。

	命令或動作	目的
		語音品質指標在Cisco IP 電話上爲自動啓用。有關存取語音品質指標的更多資訊，請參閱適用於您的電話機型的《Cisco Unified IP 電話管理指南》。
步驟2	若要配置品質回報工具 ，第 295 頁上的，請完成下列子任務： • 使用 QRT 軟鍵配置軟鍵範本 ，第 295 頁上的 • 將 QRT 軟鍵範本與通用裝置組態建立關聯 ，第 296 頁上的 • 將 QRT 軟鍵範本新增至電話 ，第 298 頁上的 • 在 Cisco Unified Serviceability 中配置 QRT ，第 298 頁上的 • 配置品質回報工具的服務參數 ，第 301 頁上的	配置品質回報工具（QRT），以便遇到 IP 電話問題的使用者可透過按 QRT 軟鍵來回報問題的類型和其他相關統計資訊。

配置通話診斷

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**系統** > **服務參數**。

步驟 2 在**伺服器**下拉式清單中選擇執行 Cisco CallManager 服務的伺服器。

步驟 3 在**服務**下拉式清單中選擇 **Cisco CallManager**。
服務參數組態視窗隨即會顯示。

步驟 4 在**叢集範圍的參數（裝置-一般）**區中，配置**通話診斷已啟用**服務參數。 可使用的選項如下：

- **停用**-不產生 CMR。
- **僅當 CDR 啟用旗標為 True 時才啟用**-僅當“通話詳細記錄（CDR）啓用旗標”服務參數設定爲 True 時才會產生 CMR。
- **無論 CDR 啟用旗標如何都啟用**無論 CDR 啓用旗標服務參數的值爲 true 或 false 都會產生 CMR。

附註　在不啓用 CDR 啓用旗標服務參數的情況下產生 CMR 可能導致硬碟空間的消耗不受控制。Cisco建議您在啓用 CMR 時亦啓用 CDR。

步驟 5 點擊**儲存**。

配置品質回報工具

配置品質回報工具（QRT），以便遇到 IP 電話問題的使用者可透過按 QRT 軟鍵來回報問題的類型和其他相關統計資訊。

程序

	命令或動作	目的
步驟 1	使用 QRT 軟鍵配置軟鍵範本 ，第 295 頁上的	您需爲 QRT 軟鍵配置掛機和已連線通話狀態。 以下通話狀態亦可使用： • 連接的會議 • 連線的轉接
步驟 2	(可選) 若要將 QRT 軟鍵範本與通用裝置組態建立關聯 ，第 296 頁上的，請完成下列子任務： • 將 QRT 軟鍵範本新增至通用裝置組態 ，第 297 頁上的 • 將通用裝置組態與電話建立關聯 ，第 298 頁上的	要使軟鍵範本可用於電話，您需完成此步驟或後續步驟。 若您的系統使用**通用裝置組態**將配置選項應用於電話。 此爲使得軟鍵範本可用於電話的最常用的方法。
步驟 3	(可選) 將 QRT 軟鍵範本新增至電話 ，第 298 頁上的	可以使用此流程作爲將軟鍵範本與“通用裝置組態”相關聯的替代方法，或者與“通用裝置組態”結合使用。 若您需指定一個軟鍵範本來覆蓋“通用裝置組態”中的指定或任何其他預設軟鍵之指定，請將此流程與“通用裝置組態”結合使用。
步驟 4	若要在 Cisco Unified Serviceability 中配置 QRT ，第 298 頁上的，請完成下列子任務： • 啓動 Cisco Extended Functions 服務 ，第 299 頁上的 • 配置警報 ，第 299 頁上的 • 配置追蹤 ，第 300 頁上的	
步驟 5	(可選)配置品質回報工具的服務參數 ，第 301 頁上的	

使用 QRT 軟鍵配置軟鍵範本

您需爲 QRT 軟鍵配置掛機和已連線通話狀態。 以下通話狀態亦可使用：

- 連接的會議
- 連線的轉接

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **裝置設定** > **軟鍵範本**。

步驟 2 若要建立新電話按鈕範本，請執行此步驟；否則請進行下一個步驟。

a) 按一下**新增**。
b) 選擇預設的範本然後再點擊**複製**。
c) 在**軟鍵範本名稱**欄位中輸入此範本的新名稱。
d) 按一下**儲存**。

步驟 3 執行以下步驟將軟鍵新增至現有範本。

a) 輸入搜尋條件，然後按一下**尋找**。
b) 選擇所需的現有範本。

步驟 4 若要將此軟鍵範本指定爲標準軟鍵範本，請勾選**預設軟鍵範本**方塊。

附註 當您將軟鍵範本指定爲預設軟鍵範本時，除非先移除預設之指定，否則您將無法將其刪除。

步驟 5 在右上方的**相關連結**下拉式清單中選擇**配置軟鍵排列**然後點擊**執行**。

步驟 6 請在「**選擇要設定的通話狀態**」下拉式清單中選擇您要軟鍵顯示的通話狀態。

步驟 7 在**未選擇的軟鍵**清單中，選擇要新增的軟鍵，然後點擊向右箭頭將軟鍵移至**選定軟鍵**清單。 使用上下箭頭變更新軟鍵的位置。

步驟 8 重複上一步，以在其他通話狀態下顯示該軟鍵。

步驟 9 按一下**儲存**。

步驟 10 您可以執行下列一項作業：

- 若您修改已經與裝置關聯的範本，請按一下**套用組態**以重新啓動裝置。
- 若您建立新的軟鍵範本，請將範本與裝置相關聯，然後重新啓動裝置。 更多資訊請參閱將軟鍵範本新增至通用裝置組態和將軟鍵範本與電話關聯部分。

下一步

執行下列其中一個步驟:

- 將 QRT 軟鍵範本新增至通用裝置組態 ，第 297 頁上的
- 將 QRT 軟鍵範本新增至電話 ，第 298 頁上的

將 QRT 軟鍵範本與通用裝置組態建立關聯

選用。 有兩種方式可以將軟鍵範本與電話建立關聯:

- 將軟鍵範本新增至“電話組態”中。
- 將軟鍵範本新增至“通用裝置組態”中。

本節中的流程描述了如何將軟鍵範本與通用裝置組態建立關聯。 若系統使用“通用裝置組態”將組態選項套用於電話，請依步驟操作。 此爲使得軟鍵範本可用於電話的最常用的方法。

若要使用替代方式，請參閱將 QRT 軟鍵範本新增至電話 ，第 298 頁上的。

程序

	命令或動作	目的
步驟 1	將 QRT 軟鍵範本新增至通用裝置組態 ，第 297 頁上的	
步驟 2	將通用裝置組態與電話建立關聯 ，第 298 頁上的	

將 QRT 軟鍵範本新增至通用裝置組態

開始之前

使用 QRT 軟鍵配置軟鍵範本 ，第 295 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **裝置設定** > **通用裝置組態**。

步驟 2 執行以下步驟建立新的通用裝置組態，並將軟鍵範本與其建立關聯；否則，請繼續下一步。

a) 按一下**新增**。
b) 在“通用裝置組態”中的**名稱**欄位中輸入名稱。
c) 按一下**儲存**。

步驟 3 執行以下步驟，將軟鍵範本新增至現有的“通用裝置組態”中。

a) 輸入搜尋條件，然後按一下**尋找**。
b) 點擊現有的通用裝置組態

步驟 4 在**軟鍵範本**下拉清單中，選擇包含您要使其可用的軟鍵的軟鍵範本。

步驟 5 按一下**儲存**。

步驟 6 您可以執行下列一項作業：

- 若您修改已經與裝置關聯的範本，請按一下**套用組態**以重新啓動裝置。
- 若建立了新的“通用裝置組態”，請將該組態與裝置建立關聯然後將裝置重新啓動。

下一步

將通用裝置組態與電話建立關聯 ，第 298 頁上的

將通用裝置組態與電話建立關聯

開始之前

將 QRT 軟鍵範本新增至通用裝置組態 ，第 297 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **電話**。
步驟 2 點擊**尋找**並選擇電話裝置以新增軟鍵範本。
步驟 3 在**通用裝置組態**下拉式清單中選擇通用裝置組態的軟鍵範本。
步驟 4 點擊**儲存**。
步驟 5 點擊**重設**以更新電話設定。

將 QRT 軟鍵範本新增至電話

開始之前

使用 QRT 軟鍵配置軟鍵範本 ，第 295 頁上的

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**裝置** > **電話**。
步驟 2 按一下**尋找**以顯示所配置的電話的清單。
步驟 3 選擇您要新增電話按鈕範本的電話。
步驟 4 在**電話按鈕範本**下拉式清單中選擇包含新功能按鈕的電話按鈕範本。
步驟 5 按一下**儲存**。
含訊息的對話方塊會隨即顯示，按**重設**以更新電話設定。

在 Cisco Unified Serviceability 中配置 QRT

程序

	命令或動作	目的
步驟 1	啓動 Cisco Extended Functions 服務 ，第 299 頁上的	啓動 Cisco Extended Functions 服務以提供對語音品質功能的支援，如品質回報工具等。
步驟 2	配置警報 ，第 299 頁上的	配置 QRT 警報以在 SysLog Viewer 的應用程式記錄檔中記錄錯誤。 此功能記錄警報，提

	命令或動作	目的
		供警報描述和建議的操作。 您可以從 Cisco Unified 即時監控工具存取 SysLog Viewer。
步驟 3	配置追蹤 ，第 300 頁上的	爲 QRT 配置追蹤以記錄您的語音應用程式的追蹤資訊。 在您設定要納入各種服務之追蹤檔案中的資訊之後，您可以使用 Cisco Unified RTMT 中的「追蹤和記錄中心」選項來收集及檢視追蹤檔案。

啟動 Cisco Extended Functions 服務

啓動 Cisco Extended Functions 服務以提供對語音品質功能的支援，如品質回報工具等。

程序

步驟 1 在Cisco Unified Serviceability中，選擇**工具** > **服務啟用**。

步驟 2 在**伺服器**下拉式清單中選擇您要在其上啓動 Cisco Extended Functions 服務的節點。

步驟 3 勾選**Cisco Extended Functions**方塊。

步驟 4 點擊**儲存**。

下一步

配置警報 ，第 299 頁上的

配置警報

配置 QRT 警報以在 SysLog Viewer 的應用程式記錄檔中記錄錯誤。 此功能記錄警報，提供警報描述和建議的操作。 您可以從 Cisco Unified 即時監控工具存取 SysLog Viewer。

開始之前

啓動 Cisco Extended Functions 服務 ，第 299 頁上的

程序

步驟 1 在 Cisco Unified Serviceability中選擇**警報** > **組態**。

步驟 2 在下拉式清單選擇要配置警報的伺服器（節點），然後按一下**執行**。

步驟 3 在**服務群組**下拉式清單中選擇**CM 服務**。

步驟 4 在**服務**下拉式清單中選擇 **Cisco Extended Functions**。

步驟 5 勾選**啟用警報**方塊以啓用本地系統記錄檔和 SDI 追蹤。

步驟 6 在下拉式清單中，選擇下列的選項之一以配置本地系統記錄檔和 SDI 追蹤配置警報事件的級別：

- **緊急情況**-將系統指定爲不可用。
- **警示**—表示需立即採取行動。
- **嚴重**：系統偵測到嚴重狀況。
- **錯誤**—表示偵測到錯誤情況。
- **警告**-此層級表示偵測到警告情況。
- **注意**—表示偵測到正常但重要的狀況。
- **資訊性**—僅表示資訊訊息。
- **除錯**— 此層級指出 Cisco 技術支援中心工程師用於除錯的詳細事件資訊。

預設值爲**Error**。

步驟 7 點擊**儲存**。

下一步

配置追蹤 ，第 300 頁上的

配置追蹤

爲 QRT 配置追蹤以記錄您的語音應用程式的追蹤資訊。 在您設定要納入各種服務之追蹤檔案中的資訊之後，您可以使用 Cisco Unified RTMT 中的「追蹤和記錄中心」選項來收集及檢視追蹤檔案。

開始之前

配置警報 ，第 299 頁上的

程序

步驟 1 在 Cisco Unified Serviceability中選擇**追蹤** > **組態**。

步驟 2 在**伺服器**下拉式清單中選擇要設定警報的伺服器。

步驟 3 在**服務群組** 下拉式清單中選擇 **CM 服務**。

步驟 4 在**服務**下拉式清單中選擇 **Cisco Extended Functions**。

步驟 5 勾選**開啟追蹤**方塊。

步驟 6 在 **除錯追蹤等級** 下拉式清單中選擇下列的選項之一：

- **Error**—追蹤所有錯誤情況以及流程和裝置初始化訊息。
- **Special**—追蹤所有特殊狀況以及正常作業期間發生的子系統狀態轉換。 追蹤通話處理事件。
- **State Transition**—追蹤所有狀態轉換狀況以及正常作業期間發生的媒體層事件。
- **Significant**—追蹤所有顯著狀況以及例行步驟的進入和結束點。 並非所有服務都使用此追蹤層級。
- **Entry_exit**—追蹤所有進入和結束狀況以及低層級除錯資訊。
- **Arbitrary**—追蹤所有任意性狀況以及詳細的除錯資訊。
- **Detailed**— 追蹤警報狀況和事件。 用於異常路徑中產生的所有追蹤。 使用最少的 CPU 週期。

預設值爲**Error**。

提示 我們建議您勾選本節中講述的所有方塊以進行疑難排解。

步驟 7 點擊**儲存**。

下一步

（選用）配置品質回報工具的服務參數 ，第 301 頁上的

配置品質回報工具的服務參數

注意 除非 Cisco 技術支援中心（TAC）另有指示，否則我們建議您使用預設服務參數設定。

程序

步驟 1 在 Cisco Unified Communications Manager 管理中選擇 **系統** > **服務參數**。

步驟 2 選擇 QRT 應用程式所在的節點。

步驟 3 選擇 **Cisco Extended Functions** 服務。

步驟 4 配置服務參數。 如需有關這些服務參數及其組態選項的詳細資訊，請參閱「相關主題」一節。

步驟 5 點擊**儲存**。

相關主題

品質回報工具服務參數 ，第 301 頁上的

品質回報工具服務參數

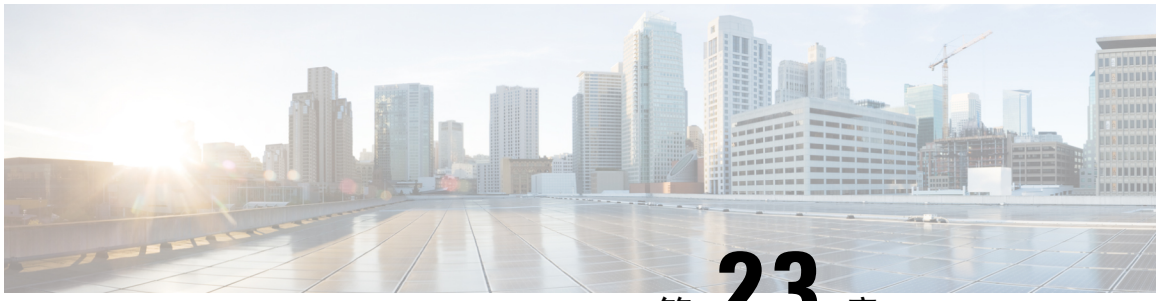
表 *77:* 品質回報工具服務參數

參數	描述
顯示擴展的 QRT 功能表選項	確定是否向使用者顯示擴展功能表選項。 您可選擇下列其中一個選項： • 將此欄位設定爲 true 可顯示擴展功能表選項（採訪模式）。 • 將此欄位設定爲 false 以不顯示擴展功能表選項（靜默模式）。 • 推薦的預設值爲 false（靜默模式）。

參數	描述
串流統計輪詢持續時間	確定用於輪詢串流統計資訊的持續時間。 您可選擇下列其中一個選項： • 將此欄位設定爲-1 以輪詢直到通話結束。 • 將此欄位設定爲 0 以根本不輪詢。 • 將其設定爲任何正值即可輪詢該秒數。 通話結束時輪詢停止。 • 推薦的預設值爲-1（輪詢直到通話結束）。
串流統計輪詢頻率（秒）	輸入兩次輪詢之間要等待的秒數。 值的範圍介於 30 到 3600。建議的預設值爲 30。
檔案數量上限	輸入在檔案計數重啓並覆寫舊檔案之前最大的檔案數。 有效值爲 1 到 10000 之間的值。建議的預設值爲 250。
每個檔案的最大行數	在開始下一個檔案之前，輸入每個檔案中的最大行數： • 值的範圍在 30～3600 之間。 • 建議的預設值顯示爲 2000。
用於安全連線至 CTIManager 的 CAPF 設定檔執行實例 ID	若啓用，則Cisco Extended Function 服務將使用爲應用程式使用者 CCMQRTSysUser 的實例 ID 配置的應用程式 CAPF 配置檔案開啓與 CTI Manager 的安全連線。 若啓用 CTI Manager 連線安全性旗標，請配置此參數。 附註 透過啓用 CTI Manager 連線安全性旗標服務參數來開啓安全性。 需重新啓動 Cisco XCP 路由器服務變更才會生效。
CTI Manager 連線安全性旗標	選擇啓用還是停用 Cisco Extended Function 服務 CTI Manager 連線的安全性。 若啓用，則Cisco Extended Function將使用爲應用程式使用者 CCMQRTSysUser 的實例 ID 所配置的應用程式 CAPF 配置檔案，開啓與 CTI Manager 的安全連線。 值的選項爲“true”和“false”。 您需選擇 True 才能啓用與 CTI 的安全連線。

第 VI 部分

管理安全性



第 23 章

管理 SAML 單一登錄

SAML 單一登錄概覽

使用 SAML 單一登錄 (SSO)，在登入其中一個應用程式後，存取定義的 Cisco 應用程式集。 SAML 描述信任的業務夥伴之間的安全性相關資訊交換。 其爲服務提供者（例如 Cisco Unified Communications Manager）用於驗證使用者的驗證通訊協定。 安全性驗證資訊透過 SAML 在身分識別提供者 (IdP) 和服務提供者之間交換。 此功能提供安全機制，以在不同應用程式使用一般憑證和相關資訊。

SAML SSO 會透過交換元資料和憑證來建立信任圈 (CoT)，以作爲 IdP 和服務提供者之間佈建流程的一部分。 服務提供者信任 IdP 的使用者資訊，以提供存取不同服務或應用程式。

用戶端會針對 IdP 進行驗證，IdP 會授予用戶端聲明。 用戶端會將聲明提供給服務提供者。 由於已建立 CoT，因此服務提供者會信任聲明，並授予用戶端存取權。

iOS 上 Cisco Jabber 憑證式 SSO 驗證的選擇加入控制

此版本的 Cisco Unified Communications Manager 引入選擇加入組態選項，以便使用身分識別提供者 (IdP) 在 iOS 上控制 Cisco Jabber 的 SSO 登入行爲。 使用此選項可讓 Cisco Jabber 使用 IdP 在控制的行動裝置管理 (MDM) 部署中執行憑證式的驗證。

您可以在 Cisco Unified Communications Manager 中透過 **iOS SSO 登入行為**企業參數來配置選擇加入控制。

附註 變更此參數的預設值前，請參閱位於 http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html 的 Cisco Jabber 功能支援和檔案，以確保 iOS 上的 Cisco Jabber 支援 SSO 登入行爲和憑證式驗證。

若要啓用此功能，請參閱在 iOS 上配置 Cisco Jabber 的 SSO 登入行爲 ，第 307 頁上的流程。

SAML SSO 必需條件

- 已爲 Cisco Unified Communications Manager 叢集設定 DNS
- 一個身分識別提供者 (IdP) 伺服器
- 受 IdP 伺服器信任且由系統支援的 LDAP 伺服器

下列使用 SAML 2.0 的 IdP 已針對 SAML SSO 功能進行測試：

- OpenAM 10.0.1
- Microsoft® Active Directory® 聯盟服務 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

第三方應用程式需滿足下列組態要求：

- 需在 IdP 設定必要屬性 “uid” 。 此屬性需符合 Cisco Unified Communications Manager LDAP 同步化使用者 ID 使用的屬性。
- 參與 SAML SSO 的所有實體皆需同步。 如需有關同步時鐘的相關資訊，請參閱 *Cisco Unified Communications Manager* 系統組態設定指南中的 “*NTP Settings*（*NTP* 設定）” ：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。

管理 SAML 單一登錄

啟用 SAML 單一登錄

附註 驗證同步代理測試成功前，您無法啓用 SAML SSO。

開始之前

- 請確保使用者資料與 Unified Communications Manager 資料庫同步。 如需詳細資訊，請參閱《*Cisco Unified Communications Manager* 系統組態指南》：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 確認 Cisco Unified CM IM and Presence Service Cisco 同步代理服務成功完成資料同步。 選擇 **Cisco Unified CM IM and Presence 管理** > **診斷** > **系統疑難排解程式**來檢查本測試的狀態。 若

成功完成資料同步，則測試“驗證同步代理已同步相關資料（例如裝置、使用者、授權資訊）”表示測試通過結果。

- 請確保至少將一位 LDAP 同步使用者新增至「標準 CCM 超級使用者」群組，以提供存取 Cisco Unified CM 管理。 如需詳細資訊，請參閱《*Cisco Unified Communications Manager* 系統組態指南》：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html。
- 若要設定 IdP 和伺服器之間的信任關係，您需從 IdP 取得信任元資料檔案，並將之匯入所有伺服器。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**系統** > **SAML 單一登錄**。
步驟 2 按一下**啟用 SAML SSO**。
步驟 3 看到將重新啟動所有伺服器連線的警告訊息後，按一下**繼續**。
步驟 4 按一下**瀏覽**尋找並上載 IdP 中繼資料檔案。
步驟 5 按一下**匯入 IdP 元資料**。
步驟 6 按**下一步**。
步驟 7 按一下**下載信任中繼資料檔**以便將伺服器中繼資料下載至您的系統。
步驟 8 在 IdP 伺服器上載伺服器元資料。
步驟 9 按**下一步**繼續。
步驟 10 從有效管理員 ID 的清單中選擇具有管理員權限的 LDAP 同步使用者。
步驟 11 按一下**執行測試**。
步驟 12 輸入有效使用者名稱和密碼。
步驟 13 看到成功訊息後，關閉瀏覽器視窗。
步驟 14 按一下**完成**，然後等待 1 到 2 分鐘，讓 Web 應用程式重新啟動。

在 iOS 上配置 Cisco Jabber 的 SSO 登入行為

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。
步驟 2 若要設定選擇加入控制，請在 SSO 組態區段中，針對 **SSO Login Behavior for iOS**（**iOS SSO 登入行為**）參數選擇 **Use Native Browser**（**使用本機瀏覽器**）選項：

附註　**SSO Login Behavior for iOS**（iOS SSO 登入行爲）參數包括下列選項：

- **Use Embedded Browser**（使用內嵌的瀏覽器）—若您啓用此選項，Cisco Jabber會使用內嵌的瀏覽器進行 SSO 驗證。 使用此選項能讓 9 版之前的 iOS 裝置使用 SSO，而無需另外從本機 Apple Safari 瀏覽器啓動。 預設會啓用此選項。
- **Use Native Browser**（使用本機的瀏覽器）—若啓用此選項，Cisco Jabber 會使用 iOS 裝置上的 Apple Safari 架構，透過 MDM 部署中的身份識別提供者 (IdP) 執行基於憑證的驗證。

  附註　除了在控制 MDM 部署中，我們不建議設定此選項，因爲使用本機瀏覽器的安全性不及使用內嵌的瀏覽器。

步驟 3 點擊**儲存**。

在升級後啟用 WebDialer 上的 SAML SSO

執行下列工作以在升級後重新啓用 Cisco WebDialer 上的 SAML 單一登錄。 Cisco WebDialer 得先啓用，才能啓用 SAML 單一登錄，SAML 單一登錄預設不會在 Cisco WebDialer 啓用。

程序

	命令或動作	目的
步驟 1	停用 Cisco WebDialer 服務 ，第 308 頁上的	若 Cisco WebDialer Web 服務已啓用，請將其停用。
步驟 2	停用 SAML 單一登錄 ，第 309 頁上的	若已啓用 SAML 單一登錄，請將其停用。
步驟 3	啓用 Cisco WebDialer 服務 ，第 309 頁上的	
步驟 4	啓用 SAML 單一登錄 ，第 306 頁上的	

停用 Cisco WebDialer 服務

若 Cisco WebDialer Web 服務已啓用，請將其停用。

程序

步驟 1 在Cisco Unified Serviceability中，選擇**工具** > **服務啟用**。
步驟 2 在**伺服器**下拉式清單中選擇所列出的 Cisco Unified Communications Manager 伺服器。
步驟 3 在 **CTI 服務**中，取消勾選**Cisco WebDialer Web 服務**（**Cisco WebDialer Web 服務**）方塊。
步驟 4 點擊**儲存**。

下一步

停用 SAML 單一登錄 ，第 309 頁上的

停用 SAML 單一登錄

若已啓用 SAML 單一登錄，請將其停用。

開始之前

停用 Cisco WebDialer 服務 ，第 308 頁上的

程序

從 CLI 執行命令 **utils sso disable**。

下一步

啓用 Cisco WebDialer 服務 ，第 309 頁上的

啟用 Cisco WebDialer 服務

開始之前

停用 SAML 單一登錄 ，第 309 頁上的

程序

步驟 1 在 Cisco Unified Serviceability 中，選擇**工具** > **服務啟動**。

步驟 2 在 **伺服器** 下拉式清單中，選擇所列出的 Unified Communications Manager伺服器。

步驟 3 在 **CTI 服務**中，選擇 **Cisco WebDialer Web Service**（Cisco WebDialer Web 服務）方塊。

步驟 4 按一下**儲存**。

步驟 5 在 Cisco Unified Serviceability 中，選擇**工具** > **Control Center - 功能服務**以確認 CTI 管理員服務啓用中且處於啓動模式。

爲了讓 WebDialer 正常運作，CTI 管理員服務需爲啓用中且處於啓動模式。

下一步

啓用 SAML 單一登錄 ，第 306 頁上的

存取復原 URL

請使用復原 URL 以略過 SAML SSO，並登入 Cisco Unified Communications Manager 管理和 Cisco Unified CM IM and Presence Service 的介面，以進行疑難排解。 例如，先啓用復原 URL，再變更網域或伺服器的主機名稱。 登入復原 URL 可更新伺服器元資料。

附註 恢復 URL 不適用於嘗試登入 Self Care 自助入口網站的一般使用者 (LDAP 或本機)。

開始之前

- 僅具有管理權限的應用程式使用者可以存取復原 URL。
- 若啓用 SAML SSO，復原 URL 會依預設啓用。 您可以從 CLI 啓用及停用復原 URL。 如需有關啓用及停用復原 URL 的 CLI 命令的詳細資訊，請參閱《*Cisco Unified Communications* 解決方案的指令行界面指南》。

程序

在瀏覽器中，輸入 `https://hostname:8443/ssosp/local/login`。

在變更網域或主機名稱後更新伺服器元資料

變更網域或主機名稱後，您需執行此流程，SAML 單一登錄才能使用。

附註 若執行此流程後仍無法登入 **SAML 單一登錄**視窗，請清除瀏覽器快取，然後再次嘗試登入。

開始之前

若停用復原 URL，便不會顯示以讓您略過單一登錄連結。 若要啓用復原 URL，請登入 CLI，然後執行下列命令：**utils sso recovery-url enable**。

程序

步驟 1 在網頁瀏覽器的網址列中，輸入下列 URL：

`https://<Unified CM-server-name>`

其中 `<Unified CM-server-name>` 爲伺服器的主機名稱或 IP 位址。

步驟 2 按一下 **Recovery URL to bypass Single Sign-On (SSO)**（**復原 URL 以略過單一登錄**）。

步驟 3 以系統管理員角色輸入應用程式使用者憑證，然後按一下**登入**。

步驟 4 在 Cisco Unified CM 管理中，選擇**系統** > **SAML 單一登錄**。

步驟 5 按一下 **Export Metadata**（**匯出中繼資料**）以下載伺服器中繼資料。

步驟 6 將伺服器元資料上傳至 IdP。

步驟 7 按一下**執行測試**。

步驟 8 輸入有效的使用者 ID 和密碼。

步驟 9 看到成功訊息後，請關閉瀏覽器視窗。

刪除伺服器後更新伺服器元資料

在叢集範圍 SSO 整合的叢集中刪除伺服器後，必須重新匯入中繼資料，以避免與 IdP 的索引不相符。

開始之前

附註 若停用復原 URL，便不會顯示以讓您略過單一登錄連結。若要啓用復原 URL，請登入 CLI，然後執行下列命令：**utils sso recovery-url enable**。

程序

步驟 1 在網頁瀏覽器的網址列中，輸入下列 URL：

`https://<Unified CM-server-name>`

其中 `<Unified CM-server-name>` 爲伺服器的主機名稱或 IP 位址。

步驟 2 按一下 **Recovery URL to bypass Single Sign-On (SSO)**（**復原 URL 以略過單一登錄**）。

步驟 3 以系統管理員角色輸入應用程式使用者憑證，然後按一下**登入**。

步驟 4 在 Cisco Unified CM 管理中選擇 **系統** > **SAML 單一登錄**。

步驟 5 按一下 **Export Metadata**（**匯出中繼資料**）以下載伺服器中繼資料。

步驟 6 將伺服器元資料上傳至 IdP。

步驟 7 按一下**執行測試**。

步驟 8 輸入有效的使用者 ID 和密碼。

步驟 9 看到成功訊息後，請關閉瀏覽器視窗。

手動提供伺服器元資料

若要爲多個 UC 應用程式配置 Identity Provider 的單一連線，則您需手動配置伺服器元資料，並在 Identity Provider 和服務提供者之間設定信任圈 (Circle of Trust)。 如需有關信任圈 (Circle of Trust) 的詳細資訊，請參閱 IdP 產品檔案。

一般 URL 語法如下所示：

```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

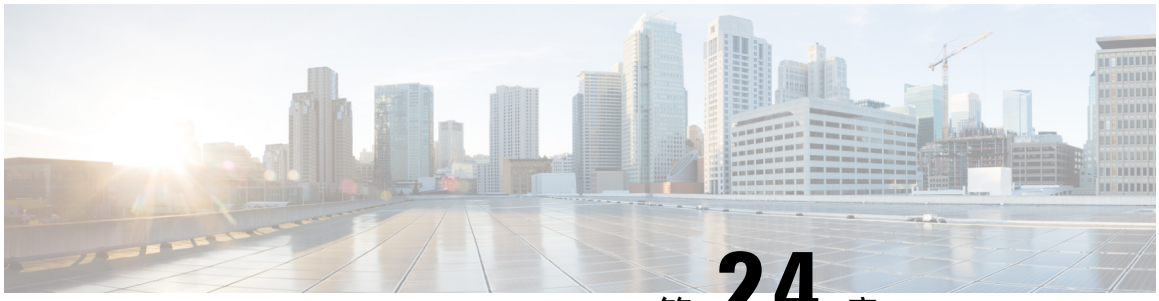
程序

若要手動佈建伺服器元資料，請使用 Assertion Customer Service (ACS) URL。

範例：

範例 ACS URL：

```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```



第 24 章

管理憑證

憑證概覽

您的系統使用自我簽署和第三方簽署的憑證。 憑證在系統中的裝置之間使用，以安全驗證裝置、加密資料及雜湊資料，以確保從來源到目的地的完整性。 憑證提供安全傳輸頻寬、通訊和作業。

憑證最重要的部分是您知道且定義資料加密及與實體（例如目標網站、電話或 FTP 伺服器）共用的方式。

當系統信任某憑證，這表示系統有預先安裝的憑證，也就是系統保證與正確的目的地共用資訊。 否則，這些點之間的通訊便會終止。

若要信任某憑證，需先以第三方憑證授權單位 (CA) 建立信任。

您的裝置需先知道可以信任 CA 和中間憑證，才可以信任稱爲安全通訊端層 (SSL) 交握的訊息交換提供的伺服器憑證。

附註 支援 Tomcat 適用的 EC 憑證。 這個新憑證稱爲 Tomcat-ECDSA。 如需詳細資訊，請參閱《*Cisco Unified Communications Manager IM and Presence Service* 的組態和管理》的「IM and Presence Service 的增強 TLS 加密」一節。

Tomcat 介面預設會停用 EC 加密。 您可在 Cisco Unified Communications Manager 或 IM and Presence Service 使用 **HTTPS 加密**企業參數來啓用。 若您變更此參數，則需重新啓動所有節點的 Cisco Tomcat 服務。

如需 EC 憑證的詳細資訊，請參閱 Cisco Unified Communications Manager 和 IM and Presence Service 版本資訊中的「ECDSA Support for Common Criteria for Certified Solutions」（認證的解決方案適用的 Common Criteria ECDSA 支援）。

第三方簽署的憑證或憑證鍊

上傳簽署應用程式憑證的憑證授權單位根憑證。 若下級憑證授權單位簽署應用程式憑證，您需上傳下級憑證授權單位的根憑證。 您也可以上傳所有憑證授權單位憑證的 PKCS #7 格式憑證鍊。

您可以使用相同**上傳憑證**對話方塊來上傳憑證授權單位根憑證和應用程式憑證。 當您上傳憑證授權單位根憑證，或僅包含憑證授權單位憑證的憑證鍊時，請選擇具有格式憑證類型信任的憑證名稱。 當您上傳應用程式憑證，或包含應用程式憑證和憑證授權單位憑證的憑證鍊時，請選擇僅包含憑證類型的憑證名稱。

例如，上傳 Tomcat 憑證授權單位憑證或憑證授權單位憑證鍊時，請選擇 **Tomcat 信任**；上傳 Tomcat 應用程式憑證，或包含應用程式憑證和憑證授權單位憑證的憑證鍊時，請選擇 **Tomcat** 或 **Tomcat-ECDSA**。

上傳 CAPF 憑證授權單位根憑證時，便會複製到 CallManager trust store，因此您不需要個別上傳 CallManager 的憑證授權單位根憑證。

附註 成功上傳第三方憑證授權單位簽署的憑證時，會刪除最近產生的 CSR，這是用於取得簽署的憑證及覆寫現有的憑證，包括第三方簽署的憑證（若已上傳）。

附註 系統會自動將 Tomcat-trust、CallManager-trust 和 Phone-SAST-trust 憑證複寫到叢集中的每個節點。

附註 您可以將目錄信任憑證上傳至 Tomcat 信任，以讓 DirSync 服務以安全模式運作。

第三方憑證授權單位憑證

若要使用第三方憑證授權單位核發的應用程式憑證，您需自憑證授權單位或 PKCS#7 憑證鍊（可辨別編碼規則 [DER]，其包含應用程式憑證和憑證授權單位憑證）取得簽署的應用程式憑證和憑證授

權單位根憑證。請向憑證授權單位取得擷取這些憑證的相關資訊。不同憑證授權單位可能有不同流程。 簽章演算法需使用 RSA 加密。

Cisco Unified Communications 作業系統會以隱私增強郵件 (PEM) 編碼格式產生 CSR。 系統可接受 DER 和 PEM 編碼格式的憑證，以及 PEM 格式的 PKCS#7 憑證鍊。 針對除了憑證授權單位代理功能 (CAPF) 以外的所有憑證類型，您皆需取得及上傳憑證授權單位根憑證和每個節點的應用程式憑證。

CAPF 方面請取得及上傳憑證授權單位根憑證和僅在第一個節點上的應用程式憑證。 CAPF 和Unified Communications Manager CSR 含有擴充，您需將之包括在憑證授權單位的應用程式憑證請求中。 若您的憑證授權單位不支援 ExtensionRequest 機制，您需啓用 X.509 擴充，如下所示：

- CAPF CSR 使用下列擴充：

```
X509v3 Extended Key Usage： TLS Web 伺服器驗證、IPSec 終端系統 X509v3 Key Usage：
 數位簽署、簽署憑證
```

- Tomcat 和 Tomcat-ECDSA 的 CSR 使用下列擴充：

附註 Tomcat 或 Tomcat-ECDSA 不需要金鑰合約或 IPsec 終端系統金鑰使用方式。

```
X509v3 Extended Key Usage： TLS Web 伺服器驗證、TLS Web 用戶端驗證、IPSec 終端系統
 X509v3 Key Usage： 數位簽章、金鑰編密、資料編密、金鑰合約
```

- IPsec 的 CSR 使用下列擴充：

```
 X509v3 Extended Key Usage： TLS Web 伺服器驗證、TLS Web 用戶端驗證、IPSec 終端系
統 X509v3 Key Usage： 數位簽章、金鑰編密、資料編密、金鑰合約
```

- Unified Communications Manager 的 CSR 使用下列擴充：

```
X509v3 Extended Key Usage： TLS Web 伺服器驗證、TLS Web 用戶端驗證 X509v3 Key
Usage： 數位簽章、金鑰編密、資料編密、金鑰合約
```

- IM and Presence Service cup 和 cup-xmpp 憑證的 CSR 使用以下擴充：

```
X509v3 Extended Key Usage： TLS Web 伺服器驗證、TLS Web 用戶端驗證、IPSec 終端系統
 X509v3 Key Usage： 數位簽章、金鑰編密、資料編密、金鑰合約
```

附註 您可以爲憑證產生 CSR，並讓第三方憑證授權單位以 SHA256 簽章進行簽署。 您便可將此簽署的憑證上傳回 Unified Communications Manager，以允許 Tomcat 和其他憑證支援 SHA256。

憑證簽署請求金鑰使用方式擴充

下表顯示適用於 Unified Communications Manager 和 IM and Presence 服務的 CA 憑證兩者的憑證簽署請求 (CSR) 的金鑰使用方式擴充。

表 *78: Cisco Unified Communications Manager CSR* 金鑰使用方式擴充

	多重伺服器	擴充金鑰使用方式			金鑰使用方式				
		伺服器驗證 **(1.3.6.1.5.5.7.3.1)**	用戶端驗證 **(1.3.6.1.5.5.7.3.2)**	**IP** 安全性終端系統 **(1.3.6.1.5.5.7.3.5)**	數位簽署	金鑰加密	資料加密	金鑰憑證簽署	金鑰同意書
CallManager CallManager-ECDSA	是	是	是		是	是	是		
CAPF (僅發佈者)	否	是			是	否		是	
IPSec	否	是	是	是	是	是	是		
Tomcat tomcat-ECDSA	是	是	是		是	是	是		
TVS	否	是	是		是	是	是		

表 *79: IM and Presence* 服務 *CSR* 金鑰使用方式擴充

	多重伺服器	擴充金鑰使用方式			金鑰使用方式				
		伺服器驗證 **(1.3.6.1.5.5.7.3.1)**	用戶端驗證 **(1.3.6.1.5.5.7.3.2)**	**IP** 安全性終端系統 **(1.3.6.1.5.5.7.3.5)**	數位簽署	金鑰加密	資料加密	金鑰憑證簽署	金鑰同意書
cup cup-ECDSA	否	是	是	是	是	是	是		
cup-xmpp cup-xmpp-ECDSA	是	是	是	是	是	是	是		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	是	是	是	是	是	是	是		
IPSec	否	是	是	是	是	是	是		
Tomcat tomcat-ECDSA	是	是	是		是	是	是		

附註 確保「資料加密」位元不會在 CA 簽署憑證過程中遭到變更或移除。

顯示憑證

使用「憑證清單」頁面上的過濾器選項，並根據憑證的一般名稱、有效期、按鍵類型和用法來排序和查看憑證清單。 因此，過濾器選項可讓您有效地對資料進行排序、查看和管理。

在整合通訊管理員版本 14 中，您可以選擇用法選項來排序和查看身份或信任憑證清單。

程序

步驟 1 在「Cisco Unified 作業系統管理」中，選擇安全性憑證管理。
憑證清單頁面隨即會出現。

步驟 2 從**在以下位置尋找憑證清單**下拉式清單中，選擇所需的過濾器選項，然後在**尋找**欄位中輸入搜尋字詞，然後按一下**尋找**按鈕。

例如，如只要查看身份憑證，請在**尋找憑證清單位置**下拉式清單中選擇**用法**，在**尋找**欄位中輸入身份，然後按一下**尋找**按鈕。

下載憑證

遞交 CSR 請求時，可使用下載憑證工作來獲取憑證的副本或上傳憑證。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**安全性** > **憑證管理**。

步驟 2 指定搜尋準則，然後按一下**尋找**。

步驟 3 選擇所需的檔案名稱，然後點按**下載**。

安裝中間憑證

若要安裝中間憑證，您需先安裝根憑證，然後上傳簽署的憑證。 僅當憑證授權單位提供憑證鍊中有多個憑證的簽署憑證時，才需要此步驟。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，按一下**安全性** > **憑證管理**。

步驟 2 按一下**上傳憑證/憑證鏈**。

步驟 3 在**憑證用途**下拉式清單中選擇恰當的trust store以安裝根憑證。

步驟 4 輸入所選擇的憑證用途的描述。

步驟 5 執行下列其中一個步驟以選擇要上傳的檔案：

- 在**上傳檔案**文字方塊中，輸入檔案路徑。
- 按一下**瀏覽**，導覽至該檔案，然後按一下**開啟**。

步驟 6 按一下**上傳**。

步驟 7 安裝客戶憑證後，請使用 FQDN 存取 Cisco Unified Intelligence Center URL。 若您使用 IP 位址存取 Cisco Unified Intelligence Center，便會看到訊息 “Click here to continue(按一下此處以繼續)” ，即使您已成功安裝自訂憑證。

附註
- 上傳 Tomcat 憑證時，應重新啓動 TFTP 服務。 否則 TFTP 仍會繼續提供舊的快取檔中的自我簽署 Tomcat 憑證。

刪除信任憑證

受信任的憑證是唯一可以刪除的憑證類型。 您無法刪除由系統產生的自我簽署憑證。

⚠

注意 刪除憑證可能會影響系統作業。 若此憑證是現有憑證鍊的一部分，刪除此憑證可能會中斷憑證鍊。 您可以**憑證清單**視窗中相關憑證的使用者名稱和主旨名稱確認有否此關係。 這個動作無法復原。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**安全性** > **憑證管理**。

步驟 2 使用**尋找**控制項過濾憑證清單。

步驟 3 選擇憑證的檔案名稱。

步驟 4 按一下**刪除**。

步驟 5 按一下**確定**。

附註
- 若您刪除的憑證是 “CAPF-trust” 、 “tomcat-trust” 、 “CallManager-trust” 、 “Phone-SAST-trust” 類型，便會在叢集中的所有伺服器刪除該憑證。
- 若將憑證匯入到 CAPF-trust 中，則僅在該特定節點上啓用該憑證，且不會跨叢集複製憑證。

重新產生憑證

我們建議您在憑證過期之前重新產生憑證。 憑證即將到期時，您將在 RTMT(Syslog Viewer)中收到警告並透過電子郵件收到通知，

但您也可以重新產生過期的憑證。 請在下班時間依照此程式操作，因爲您需重新啓動電話及服務。 您僅可重新產生一個在 Cisco Unified 作業系統管理中列爲[憑證]類型的憑證。

注意 重新產生憑證可能會影響系統作業。 重新產生憑證會覆寫現有的憑證，包括已上傳的第三方簽署憑證。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**安全性** > **憑證管理**。

輸入搜尋參數以尋找憑證並檢視其組態詳細資訊。 系統在**憑證清單**視窗中顯示符合所有條件的記錄。

在憑證詳細資訊頁面中按一下**重新產生**按鈕，具相同密鑰長度的自我簽署憑證將會重新產生。

附註 在重新產生憑證時，**憑證說明**檔位將不會更新，直到您關閉**重新產生**視窗並開啓新產生的憑證。

點按**產生自我簽署憑證**重新產生具有 3072 或 4096 的新密鑰長度的自我簽署憑證。

步驟 2 在 **Generate New Self-Signed Certificate**(產生新自我簽署憑證)視窗中設定欄位。 如需有關欄位及其組態選項的詳細資訊，請參閱線上說明。

步驟 3 按一下**產生**。

步驟 4 重新啓動受重新產生憑證影響的所有服務。 。

步驟 5 重新產生 CAPF、ITLRecovery 憑證或 CallManager 憑證後，請更新 CTL 檔案 (如有設定)。

附註 重新產生憑證後，您需執行系統備份，使最新的備份包含重新產生的憑證。 若備份不包含重新產生的憑證，且您執行系統還原工作，則您需手動解除鎖定系統中的每部電話，使電話可註冊。

重要須知 在重新產生/更新 CallManager、CAPF 和 TVS 憑證後，電話將會自動重設以接收已更新的 ITL 檔案。

憑證名稱和說明

下表描述可以重新產生的系統安全憑證，以及需重新啓動的相關服務。 如需關於重新產生 TFTP 憑證的詳細資訊，請參閱《*Cisco Unified Communications Manager* 安全性指南》：http://www.cisco.com/

c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

表 *80:* 憑證名稱和說明

名稱	描述	要重新啟動的服務
Tomcat tomcat-ECDSA	啓用 SIP Oauth 模式後，Cisco DRF 服務和 Cisco CallManager 服務將使用此憑證。	Cisco Tomcat 服務、Cisco CallManager 服務。
CallManager CallManager-ECDSA	這可用於 SIP、SIP trunk、SCCP、TFTP 等。	Cisco Call Manager 服務和其他相關服務，包括 Cisco CTI Manager — 如果伺服器處於安全模式，則請更新 CTL 檔案。 CallManager-ECDSA - Cisco CallManager 服務。
CAPF	由在整合通訊管理員發佈者上執行的 CAPF 服務使用。 該憑證用於向端點發出 LSC (在線和離線 CAPF 模式除外)	不適用
TVS	由信任驗證服務使用；該服務可充當電話的次要信任驗證機制，以防伺服器憑證發生變更。	不適用

重要須知 此附註僅適用於版本 14SU2。

對於版本 14SU2，Cisco DRF 服務需要在 tomcat-ECDSA 憑證重新產生或上傳後重新啓動。 不需要在 tomcat RSA 憑證操作後重新啓動。

為 OAuth 重新整理登入重新產生金鑰

使用此流程可透過「命令行介面」重新產生加密金鑰和簽署金鑰。 請僅在 Cisco Jabber 用於 Cisco Unified Communications Manager OAuth 驗證的加密金鑰或簽署金鑰遭到破解時完成此任務。 簽署金鑰爲非對稱且以 RSA 爲基礎，而加密金鑰爲對稱金鑰。

完成此工作後，使用這些金鑰的目前存取和重新整理記號環將會無效。

我們建議您在下班時間完成此工作，以最小化對一般使用者的影響。

加密金鑰僅可經由以下 CLI 重新產生，但您也可以使用 Cisco Unified 作業系統管理 GUI 重新產生簽署金鑰。 選擇**安全性** > **憑證管理**，選擇 **AUTHZ** 憑證，然後按一下**重新產生**。

程序

步驟 1 從Unified Communications Manager發布者節點登入**命令行**介面。

步驟 2 若要重新產生加密金鑰：

a) 執行 `set key regen authz encryption`命令。

b) 輸入 `yes`。

步驟 3 若要重新產生簽署金鑰：

a) 執行 `set key regen authz signing` 命令。

b) 輸入 `yes`。

Cisco Unified Communications Manager 發佈者節點便會重新產生金鑰，並將新的金鑰複製到所有 Cisco Unified Communications Manager 叢集節點上，包括任何本機 IM and Presence Service 節點。

您需重新產生及同步所有 UC 叢集的新金鑰：

- IM and Presence 中央叢集—若您有 IM and Presence 集中式部署，則您的 IM and Presence 節點會在與電話不同的叢集上執行。 在這種情況下，請在 IM and Presence Service 中央叢集的 Cisco Unified Communications Manager 發佈者節點重複此流程。
- Cisco Expressway 或Cisco Unity Connection—也會重新產生這些叢集上的金鑰。 如需詳細資訊，請參閱您的 Cisco Expressway 和 Cisco Unity Connection 檔案。

附註 重新分配密鑰後，在叢集中的所有節點上重新啓動 Cisco CallManager 服務。

上傳憑證或憑證鍊

上傳任何想要讓系統信任的新憑證或憑證鍊。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**安全性** > **憑證管理**。

步驟 2 按一下**上傳憑證/憑證鏈**。

步驟 3 **憑證用途**下拉式清單中選取憑證名稱。

步驟 4 執行下列其中一個步驟以選擇要上傳的檔案：

- 在**上傳檔案**文字方塊中，輸入檔案路徑。
- 按一下**瀏覽**，導覽至該檔案，然後按一下**開啟**。

步驟 5 若要將檔案上傳至伺服器，請按一下**上傳檔案**。

附註 在上傳憑證後重新啓動受影響的服務。 伺服器恢復正常運作時，您可以存取 CCMAdmin 或 CCMUser GUI 以驗證您所新增的使用中憑證。

管理第三方憑證授權單位憑證

此工作流程提供第三方憑證流程的概覽，並依序列出各步驟的參考內容。 您的系統支援第三方憑證授權單位使用 PKCS # 10 憑證簽署請求 (CSR) 發行的憑證。

程序

	命令或動作	目的
步驟 1	產生憑證簽署請求 ，第 322 頁上的	產生憑證簽署請求(CSR)，其爲一組包含憑證應用程式資訊(包括公開金鑰、組織名稱、一般名稱、位置和國家)的加密文字。 憑證授權單位會使用此 CSR 爲系統產生信任的憑證。
步驟 2	下載憑證簽署請求 ，第 323 頁上的	將 CSR 下載至電腦，如此便可隨時遞交至憑證授權單位。
步驟 3	請參閱憑證授權單位檔案。	向您的憑證授權單位取得應用程式憑證。
步驟 4	請參閱憑證授權單位檔案。	向您的憑證授權單位取得根憑證。
步驟 5	將憑證授權單位簽署的 CAPF 根憑證新增至 trust store ，第 323 頁上的	將根憑證新增至trust store。 使用憑證授權單位簽署的 CAPF 憑證時，請執行此步驟。
步驟 6	上傳憑證或憑證鍊 ，第 321 頁上的	將憑證授權單位根憑證上傳至節點。
步驟 7	若您更新 CAPF 或 Cisco Unified Communications Manager 的憑證，請產生新的 CTL 檔案。	請參閱《*Cisco Unified Communications Manager* 安全指南》：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。 上傳第三方簽署的 CAPF 或 CallManager 憑證後，請重新執行 CTL 用戶端(若有設定)。
步驟 8	重新啓動服務 ，第 323 頁上的	重新啓動受新憑證影響的服務。 針對所有憑證類型，重新啓動相應的服務(例如，若您更新 Tomcat 或 Tomcat-ECDSA 憑證，請重新啓動 Cisco Tomcat 服務)。

產生憑證簽署請求

產生憑證簽署請求 (CSR)，其爲一組包含憑證應用程式資訊(包括公開金鑰、組織名稱、一般名稱、位置和國家)的加密文字。 憑證授權單位會使用此 CSR 爲系統產生信任的憑證。

附註　若產生新的 CSR，便會覆寫任何現有 CSR。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**安全性** > **憑證管理**。

步驟 2 按一下**產生 CSR**。

步驟 3 在**產生憑證簽署請求**視窗中設定欄位。如需有關欄位及其組態選項的詳細資訊，請參閱線上說明。

步驟 4 按一下**產生**。

下載憑證簽署請求

將 CSR 下載至電腦，如此便可隨時遞交至憑證授權單位。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**安全性** > **憑證管理**。

步驟 2 按一下**下載 CSR**。

步驟 3 **憑證用途**下拉式清單中選擇憑證名稱。

步驟 4 按一下**下載 CSR**。

步驟 5 (可選) 系統提示時，請按一下**儲存**。

將憑證授權單位簽署的 CAPF 根憑證新增至trust store

使用憑證授權單位簽署的 CAPF 根憑證時，將根憑證新增至 CallManagerUnified Communications Manager trust store。

程序

步驟 1 從「Cisco Unified 作業系統管理」中，選擇**安全性** > **憑證管理**。

步驟 2 按一下**上傳憑證/憑證鏈**。

步驟 3 在**上傳憑證/憑證串鍊**快顯視窗中的**憑證用途**下拉式清單中，選擇 **CallManager-trust**，然後瀏覽至 CA 簽署的 CAPF 根憑證。

步驟 4 憑證顯示於**上傳檔案**欄位後，請按**上傳**。

重新啟動服務

若您的系統要求您重新啓動叢集中特定節點的任何功能或網路服務，請使用此流程。

程序

步驟 1 視您要重新啓動的服務類型而定，執行下列其中一個工作：

- 選擇**工具** > **控制中心 - 功能服務**。
- 選擇**工具** > **控制中心 - 網路服務**。

步驟 2 從**伺服器**下拉式清單中選擇您的系統節點，然後按一下**執行**。

步驟 3 按一下您要重新啓動的服務旁的單選按鈕，然後按一下**重新啟動**。

步驟 4 顯示指示重新啓動需要一些時間的訊息後，請按一下**確定**。

透過在線憑證狀態協定撤銷憑證

Unified Communications Manager 設定 OCSP 以監督憑證之撤銷。 系統會在排定的間隔檢查憑證狀態以確認其有效性，且每次皆會上載憑證。

在線憑證狀態協定（OCSP）可幫助管理員管理其系統的憑證要求。 配置 OCSP 後將會提供一種簡單、安全且自動化的方法來檢查憑證的有效性而亦可即時地撤銷過期的憑證。

啓用“通用標準”模式的 FIPS 部署方面，OCSP 還可促使您的系統符合“通用標準”之需求。

驗證檢查

Unified Communications Manager 檢查憑證狀態並確認有效性。

憑證按以下方式進行驗證：

- Unified Communications Manager 使用委託的信任模型（DTM）並檢查根 CA 或中間 CA 的 OCSP 簽署屬性。 根 CA 或中間 CA 需簽署 OCSP 憑證以檢查狀態。 若委派的信任模型失敗，則 Unified Communications Manager 會退回至信任回應者模型（TRP），並使用來自 OCSP 伺服器所指定之 OCSP 回應簽署憑證來驗證憑證。

附註 OCSP 回應程式需正在執行以檢查憑證的撤銷狀態。

- 在**憑證撤銷**視窗中啓用 OSCP 選項，以提供最安全的即時檢查憑證撤銷的方法。 從選項中選擇以使用來自憑證或已配置的 OCSP URI 的 OCSP URI。 有關手動 OCSP 配置的更多資訊，請參閱配置透過 OCSP 撤銷憑證。

附註 葉憑證方面，TLS 用戶端（如 syslog，FileBeat，SIP，ILS，LBM 等）會將 OCSP 請求傳送到 OCSP 回應程式，並從 OCSP 回應器即時接收憑證撤銷回應。

執行驗證並且“通用條件”模式爲“開啓”後，將爲憑證返回以下狀態之一。

- **良好 - 良好**狀態表示對狀態查詢的正面回應。 至少，這樣正面的回應表示該憑證未被撤銷，但不一定表示該憑證曾經頒發過或該回應所產生之時間是在憑證的有效時間間隔內。 回應擴充可以用於傳達有關回應者關於憑證狀態的斷言的附加資訊，例如有關發行，有效性等的肯定聲明。
- **撤銷-撤銷**狀態表示憑證已被撤銷（永久或暫時（保留））。
- **未知-未知**狀態表示 OCSP 回應者對所請求的憑證並不知曉。

附註 在“通用條件”模式下，連線在**撤銷**和**未知**的情況下均會失敗，而未啓用通用條件時的**未知**回應情況下連線將會成功。

憑證監視工作流程

完成這些工作以配置系統自動監督憑證狀態及到期日。

- 當憑證即將到期時傳送電子郵件給您。
- 撤銷到期的憑證。

程序

	命令或動作	目的
步驟 1	配置憑證監控通知 ，第 325 頁上的	設定自動憑證監控。 系統會定期檢查憑證狀態，並在接近憑證逾期日時，傳送電子郵件給您。
步驟 2	配置透過 OCSP 撤銷憑證 ，第 326 頁上的	配置線上憑證狀態通訊協定 (OCSP)，如此系統就會自動撤銷到期的憑證。

配置憑證監控通知

配置 Unified Communications Manager 或 IM and Presence Service的自動監控憑證。 系統會定期檢查憑證狀態，並在接近憑證到期日時，傳送電子郵件給您。

附註 **Cisco 憑證逾期監控**網路服務需爲執行中。 依預設啓用此服務，但您可確認服務正在 Cisco Unified Serviceability 中執行，做法是選擇**工具** > **Control Center - 網路服務**，並確認 **Cisco 憑證逾期監控服務**狀態正在**執行**。

程序

步驟 1 登入 Cisco Unified 作業系統管理 (適用於 Unified Communications Manager 憑證監控)或 Cisco Unified IM and Presence 管理 (適用於 IM and Presence Service憑證監控)。

步驟 2 選擇**安全性** > **憑證監控**。

步驟 3 在**通知開始時間**欄位中輸入數字值。 此值表示系統於憑證到期日前的幾天會開始通知您。

步驟 4 在**通知頻率**欄位輸入通知的頻率。

步驟 5 選用。 勾選**啟用電子郵件通知**方塊，讓系統傳送憑證即將逾期的電子郵件通知。

步驟 6 勾選**啟用 LSC 監控**方塊，將 LSC 憑證納入憑證狀態檢查。

步驟 7 在**電子郵件 ID**欄位中，輸入要系統傳送通知時所用的電子郵件地址。 您可以輸入多個電子郵件地址，各以分號分隔。

步驟 8 按一下**儲存**。

附註 憑證監控服務預設每 24 小時執行一次。 重新啓動憑證監控服務時，會先啓動服務，然後計算出 24 小時後下一次會執行的排程。 即使憑證接近七天的到期日，間隔也不會變更。 當憑證逾期或將於一天內到期時，便會每小時執行。

下一步

設定線上憑證狀態通訊協定 (OCSP)，如此系統就會自動撤銷已逾期的憑證。 如需詳細資訊，請參閱配置透過 OCSP 撤銷憑證 ，第 326 頁上的

配置透過 OCSP 撤銷憑證

啓用線上憑證狀態通訊協定 (OCSP) 以經常檢查憑證狀態，並自動撤銷過期的憑證。

開始之前

請確定系統具有 OCSP 檢查所需的憑證。 您可以使用 OCSP 回應屬性設定根或中繼 CA 憑證，或使用已上傳至 tomcat-trust 的已指定 OCSP 簽署憑證。

程序

步驟 1 登入 Cisco Unified 作業系統管理 (適用於 Unified Communications Manager 憑證撤銷)或 Cisco Unified IM and Presence 管理 (適用於 IM and Presence Service憑證撤銷)。

步驟 2 選擇**安全性** > **撤銷憑證**。

步驟 3 勾選 **啟用 OCSP**方塊，然後執行下列其中一項工作：

- 若要指定 OCSP 檢查的 OCSP 回應者，請選擇**使用設定的 OCSP URI** 按鈕，並在 **OCSP 設定 URI** 欄位輸入回應者的 URI。
- 若憑證有設定 OCSP 回應者 URI ，請選擇**使用來自憑證的 OCSP URI** 按鈕。

步驟 4 勾選**啟用撤銷檢查**方塊。

步驟 5 在**檢查間隔**欄位填寫撤銷檢查間隔時間。

步驟 6 按一下**儲存**。

步驟 7 選用。若有 CTI、IPsec 或 LDAP 連結，也需完成除上述步驟外的下列步驟，以啓用這些持久連線的 OCSP 撤銷支援：

a) 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。

b) 在**憑證撤銷和到期**下，配置憑證**有效性檢查**參數爲 **True**。

c) 配置**有效檢查頻率**參數的值。

附註　**啟用撤銷檢查**參數在**憑證撤銷**視窗中的間隔值，優先於**有效檢查頻率**企業參數的值。

d) 點擊**儲存**。

憑證錯誤疑難排解

開始之前

若您從 IM and Presence Service 節點或從 Cisco Unified Communications Manager 節點的 IM and Presence Service 功能嘗試存取 Cisco Unified Communications Manager 服務時發生錯誤，問題的來源爲 Tomcat 信任憑證。無法建立伺服器的連線 (無法連線至遠端節點) 錯誤訊息會顯示於下列的「Serviceability」介面視窗：

- **服務啟動**
- **控制中心 - 功能服務**
- **控制中心 - 網路服務**

使用此流程可協助您解決憑證錯誤。請從第一個步驟開始，然後視需要看是否得繼續。在某些情況下，只要完成第一個步驟即可解決錯誤；但有時您則需完成所有步驟。

程序

步驟 1 在 Cisco Unified 作業系統管理中，確認已具有需要的 Tomcat 信任憑證：**安全性** > **憑證管理**。

若需要的憑證不存在，請等待 30 分鐘，然後再檢查一次。

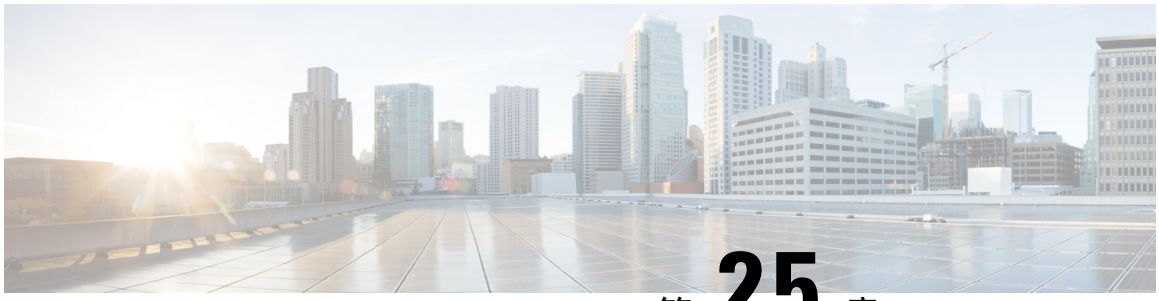
步驟 2 選擇要檢視其資訊的憑證。 確認內容符合遠端節點上的對應憑證。

步驟 3 從 CLI 重新啓動 Cisco 叢集間同步代理服務：**utils service restart Cisco Intercluster Sync Agent**。

步驟 4 Cisco 叢集間同步代理服務重新啓動後，重新啓動 Cisco Tomcat 服務：**utils service restart Cisco Tomcat**。

步驟 5 等待 30 分鐘。 若上述步驟未解決憑證錯誤，且 Tomcat 信任憑證存在，請刪除該憑證。 刪除憑證後，您需手動交換憑證，方法是爲每個節點下載 Tomcat 和 Tomcat-ECDSA 憑證，並上傳至其對等，作爲 Tomcat 信任憑證。

步驟 6 完成憑證交換後，請重新啓動每部受影響伺服器的 Cisco Tomcat：**utils service restart Cisco Tomcat**。



第 25 章

管理批量憑證

管理批量憑證

若要在叢集間共用一組憑證，請使用批量憑證管理。 需要在叢集間建立信任的系統功能需要執行此步驟，例如跨叢集的Extension Mobility。

程序

	命令或動作	目的
步驟 1	匯出憑證 ，第 329 頁上的	此程序可建立 PKCS12 檔案，其包含叢集中所有節點的憑證。
步驟 2	匯入憑證 ，第 330 頁上的	將憑證匯入回主叢集和遠端 (存取的) 叢集。

匯出憑證

此程序可建立 PKCS12 檔案，其包含叢集中所有節點的憑證。

程序

步驟 1 在 Cisco Unified 作業系統管理中，選擇**安全性** > **Bulk Certificate Management (批量憑證管理)**。

步驟 2 爲主叢集和遠端叢集皆可聯繫的 TFTP 伺服器進行設定。 如需有關欄位及其組態選項的資訊，請參閱線上說明。

步驟 3 按一下**儲存**。

步驟 4 按一下**匯出**。

步驟 5 在**批量憑證匯出**視窗中，在**憑證類型**欄位選擇**所有**。

步驟 6 按一下**匯出**。

步驟 7 按一下**關閉**。

附註　執行批量憑證匯出後，憑證將按以下方式上載至遠端叢集:

- CAPF 憑證以 CallManager-trust 形式上載
- Tomcat 憑證以 Tomcat 信任上載
- CallManager 憑證以 CallManager-trust 形式上載
- CallManager 憑證以 Phone-SAST-trust 形式上載
- ITLRecovery 憑證以 PhoneSast-trust 和 CallManager-trust 形式上載

當憑證爲自我簽署且在另一個叢集中無共同 trust 時，將執行上述步驟。若存在共同的信任或相同的簽署者則不需匯出所有的憑證。

匯入憑證

將憑證匯入回主叢集和遠端 (存取的) 叢集。

附註　使用批量憑證管理匯入憑證會導致電話重設。

開始之前

您需先完成下列活動，匯入按鈕才會顯示：

- 將憑證從至少兩個叢集匯出至 SFTP 伺服器。
- 整合匯出的憑證。

程序

步驟 1 在 在 Cisco Unified CM 管理中，選擇**安全性** > **批量憑證管理** > **匯入** > **批量憑證匯入**中。

步驟 2 在 **Certificate Type (憑證類型)** 下拉式清單中選擇 **All (所有)**。

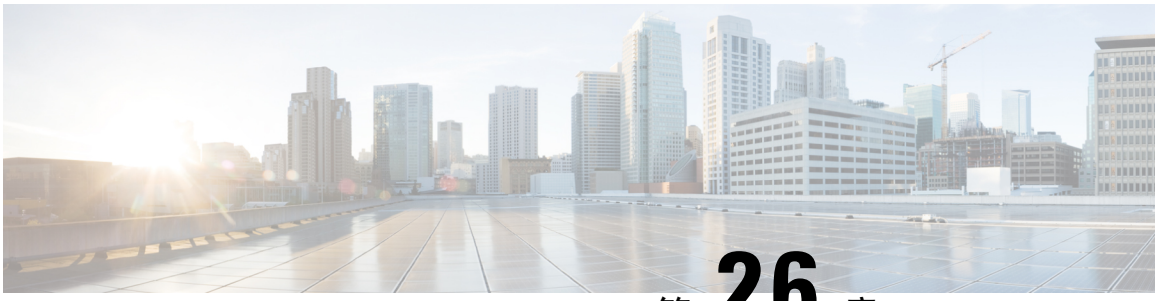
步驟 3 選擇 **Import (匯入)**。

附註　執行批量憑證匯入後，憑證將按以下方式上載到遠端叢集:

- CAPF 憑證以 CallManager-trust 形式上載
- Tomcat 憑證以 Tomcat 信任上載
- CallManager 憑證以 CallManager-trust 形式上載
- CallManager 憑證以 Phone-SAST-trust 形式上載
- ITLRecovery 憑證以 PhoneSast-trust 和 CallManager-trust 形式上載

附註　下列類型的憑證確定重新啓動的電話:

- Callmanager-僅在憑證所屬節點上啓動了 TFTP 伺服的情況下，僅適用於所有電話。
- TVS-基於 Callmanager 群組成員身份的 某些 電話。
- CAPF-僅在啓動了 CAPF 的情況下始可使用 所有 電話。



第 26 章

管理 IPSec 原則

IPSec 原則概覽

IPSec 是使用加密安全性服務透過 IP 網路來確保私人安全通訊的架構。 IPSec 原則是用於設定 IPSec 安全性服務。 該原則在您的網路中爲大多數流量類型提供不同層級的保護。 您可以設定 IPSec 原則，以滿足電腦、組織單位 (OU)、網域、網站或全球企業的安全性要求。

設定 IPSec 原則

附註

- 由於系統升級期間對 IPsec 原則進行的任何變更皆會遺失，因此請勿在升級期間修改或建立 IPsec 原則。
- IPSec 需要雙向配置，或每部主機（或閘道）一個對等。
- 當您在兩個 Unified Communications Manager 節點提供 IPsec 原則，且一個 IPsec 原則通訊協定設爲 “ANY” ，另一個 IPsec 原則通訊協定設爲 “UDP” 或 “TCP” 時，若從使用 “ANY” 通訊協定的節點執行，驗證可能會導致假陰性。
- IPSec（特別是具有加密）會影響系統效能。
- Unified CM 節點重新啓動後，如果 IPsec 無法連線，請確保使用指令 **utils ipsec restart** 重新啓動 IPsec 服務以成功建立 IPsec 連線。 此解決方法是在網路連線建立之前，緩解 IPsec 服務重新啓動的任何問題。

程序

步驟 1 在「Cisco Unified 作業系統管理」中，選擇 **Security**（安全性） > **IPSec Configuration**（**IPSec** 組態）。

步驟 2 按一下**新增**。

步驟 3 配置 **IPSEC Policy Configuration**（**IPSec 原則組態**）視窗中的欄位。 如需有關欄位及其組態選項的詳細資訊，請參閱線上說明。

步驟 4 按一下**儲存**。

步驟 5 (可選) 若要驗證 IPSec，請選擇 **服務** > **Ping**，勾選**驗證 IPSec**方塊然後再按**Ping**。

管理 IPSec 原則

由於系統升級期間對IPSec原則進行的任何變更皆會遺失，因此請勿在升級期間修改或建立IPSec原則。

⚠

注意 任何因主機名稱、網域或 IP 位址變更而對現有 IPSec 憑證進行的變更皆需要刪除並重新建立 IPSec 原則（若變更憑證名稱）。 若未變更憑證名稱，在匯入遠端節點重新產生的憑證後，需停用再啓用 IPSec 原則。

程序

步驟 1 在「Cisco Unified 作業系統管理」中，選擇 **Security**（安全性） > **IPSEC Configuration**（**IPSEC** 組態）。

步驟 2 若要顯示、啓用或停用原則，請執行下列步驟：

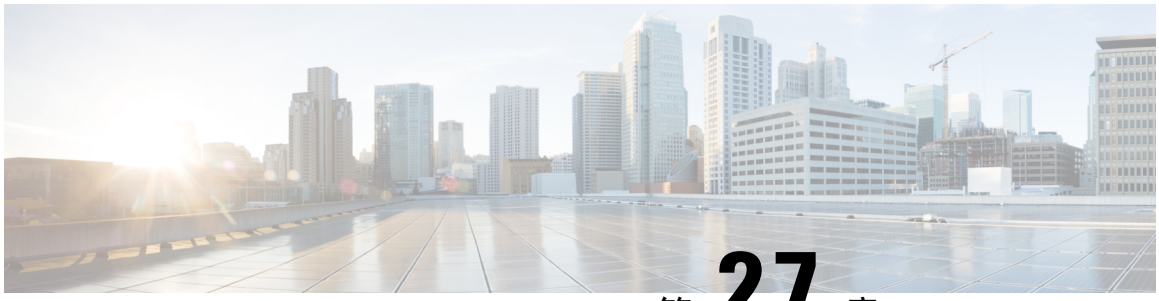
a) 按一下原則名稱。
b) 若要啓用或停用原則，請勾選或取消勾選 **啟用原則**方塊。
c) 按一下**儲存**。
d) 如果停用該原則，則必須執行 **utils ipsec restart** 指令，停用的變更才會生效。

步驟 3 若要刪除一或多個勾選，請執行下列步驟：

a) 勾選您要刪除的原則旁的方塊。

您可以按一下**全選**來選擇所有原則，或按一下**全部清除**來清除所有可勾選方塊。

b) 按一下**刪除選取的項目**。



第 27 章

管理憑證原則

憑證原則和驗證

驗證功能會驗證使用者、更新憑證資訊、追蹤及記錄使用者事件和錯誤、記錄憑證變更記錄，以及加密或解密資料儲存區的使用者憑證。

系統會一律針對 Unified Communications Manager 資料庫驗證應用程式使用者密碼和一般使用者 PIN 碼。 系統可以針對公司目錄或資料庫驗證一般使用者密碼。

若系統與公司目錄同步，則 Unified Communications Manager 或 Lightweight Directory Access Protocol (LDAP) 可以驗證密碼。

- 啓用 LDAP 驗證時，不適用使用者密碼和憑證原則。 這些預設適用於透過目錄同步（DirSync 服務）建立的使用者。
- 停用 LDAP 驗證時，系統會針對資料庫驗證使用者憑證。 您可以透過此選項指派憑證原則、管理驗證事件及管理密碼。 一般使用者可以透過電話UI 變更密碼和 PIN 碼。

憑證原則不適用於作業系統使用者或 CLI 使用者。 這些管理員使用作業系統支援的標準密碼驗證流程。

在資料庫中設定使用者後，系統會在資料庫中儲存使用者憑證的記錄，以防止使用者在收到變更憑證的提示時輸入先前的資訊。

憑證原則的 JTAPI 和 TAPI 支援

由於 Cisco Unified Communications Manager Java 電話應用程式設計介面 (JTAPI) 和電話應用程式設計介面 (TAPI) 支援指派至應用程式使用者的憑證原則，因此開發人員需建立回應至密碼到期、PIN 到期和鎖定傳回碼的應用程式，以實施憑證原則。

應用程式使用 API 驗證資料庫或公司目錄，無論應用程式使用的驗證機型。

如需有關開發人員適用的 JTAPI 和 TAPI 的詳細資訊，請參閱開發人員指南：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html。

配置憑證原則

憑證原則適用於應用程式使用者和一般使用者。 您可以將密碼原則指派至一般使用者和應用程式使用者，並將 PIN 碼原則指派至一般使用者。 憑證原則預設組態會列出這些群組的憑證指派。 將使用者新增至資料庫時，系統會指派預設的原則。 您可以變更指派的原則及管理使用者驗證事件。

附註 針對 CTI 應用程式使用者，確保將憑證原則設定下允許的非作用中天數參數設定爲 0（無限制）。否則，應用程式使用者將意外變爲非作用中的狀態，並且 CTI 應用程式在重新啓動後可能無法連線到 Unified CM。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者配置憑證** > **規則**。

步驟 2 執行下列其中一個步驟:

- 按一下**尋找**，然後選擇現有的憑證原則。
- 按一下**新增**以建立新的憑證原則。

步驟 3 完成**憑證原則組態**視窗中的欄位。 如需有關欄位及其組態設定的詳細資訊，請參閱線上說明。

步驟 4 點擊**儲存**。

配置憑證原則預設

在安裝時，Cisco Unified Communications Manager 會指派靜態預設憑證原則至使用者群組。 不提供預設憑證。 您的系統會提供選項來指派新的預設原則，及設定新的預設憑證和使用者的憑證要求。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**使用者管理** > **使用者配置憑證** > **規則預設值**。

步驟 2 在**憑證原則**下拉式清單方塊中選擇此群組的憑證原則。

步驟 3 在 **變更憑證**和 **確認認證**組態視窗中輸入密碼。

步驟 4 若您不想讓使用者變更此憑證，請勾選**使用者無法變更**方塊。

步驟 5 若您要將此憑證作爲暫時憑證，並要求一般使用者在下次登入時變更，請勾選 **使用者在下次登入時需變更** 方塊。

附註 請注意，若勾選此方塊，則使用者將無法使用“個人目錄”服務更改 PIN。

步驟 6 若您不想讓憑證到期，請勾選**不要到期**方塊。

步驟 7 按一下**儲存**。

監控驗證活動

系統會顯示最新的驗證結果，例如最後駭客嘗試時間和登入嘗試失敗計數。

系統會爲下列憑證原則事件產生記錄檔項目：

- 驗證成功
- 驗證失敗（錯誤的密碼或不明）
- 驗證因下列原因而失敗
  - 管理鎖定
  - 駭客鎖定（失敗登入鎖定）
  - 到期軟鎖（逾期憑證）
  - 不活躍鎖定（有一段時間未使用憑證）
  - 使用者需變更（需變更使用者憑證設定）
  - LDAP 非作用中（切換至 LDAP 驗證且 LDAP 非作用中）
- 成功的使用者憑證更新
- 失敗的使用者憑證更新

附註 若您針對一般使用者密碼使用 LDAP 驗證，則 LDAP 只會追蹤驗證成功和失敗。

所有包含字串 “ims-auth” 的事件訊息和嘗試驗證的使用者 ID。

程序

步驟 1 在 Cisco Unified CM 管理中，選取**使用者管理** > **一般使用者**。

步驟 2 輸入搜尋準則，按一下**尋找**，然後從結果清單中選擇使用者。

步驟 3 按一下**編輯憑證**檢視使用者的驗證活動。

下一步

您可以使用 Cisco Unified 即時監控工具 (Unified RTMT) 檢視記錄檔。 您也可以將擷取的事件收集爲報告。 如需如何使用 Unified RTMT 的詳細步驟，請參閱 *Cisco Unified Real-Time Monitoring Tool Administration Guide*（Cisco Unified 即時監控工具管理指南）：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

配置憑證快取

啓用憑證快取以提高系統效率。 系統不需要爲每一個單一登錄請求執行資料庫查詢或叫用預存流程。 關聯的憑證原則不會實施，除非快取持續時間結束。

此設定適用於所有叫用使用者驗證的 Java 應用程式。

程序

步驟 1 在 Cisco Unified CM 管理中選擇**系統** > **企業參數**。

步驟 2 視需要執行下列工作：

- 將 **Enable Caching**（**啟用快取**）企業參數設爲 **True**。 啓用此參數後，Cisco Unified Communications Manager 便會使用快取憑證最長 2 分鐘。
- 將 **Enable Caching**（**啟用快取**）企業參數設爲 **False** 便會停用快取，使系統不使用快取憑證進行驗證。 系統會針對 LDAP 驗證忽略此設定。 憑證快取每位使用者將需最低額外記憶體量。

步驟 3 點擊**儲存**。

管理作業期間終止

系統管理員可使用此流程終止各個特定的節點上使用者的活躍作業期間。

附註
- 權限等級 4 的管理員只能終止作業階段。
- 作業階段管理終止特定節點上的活動登錄作業階段。 若管理員想要終止所有相異節點上的所有使用者作業階段，需登入每個節點終止作業階段。

這個方法適用於以下介面：

- Cisco Unified CM 管理

- Cisco Unified Serviceability
- Cisco Unified 報告
- Cisco Unified Communications Self Care Portal
- Cisco Unified CM IM and Presence 管理
- Cisco Unified IM and Presence Service功能
- Cisco Unified IM and Presence 報告

程序

步驟 1 在 Cisco Unified OS 管理或 Cisco Unified IM and Presence OS 管理中，選擇**安全** > **作業期間管理**。顯示“作業期間管理”視窗。

步驟 2 輸入主動登入使用者的**使用者 ID**。

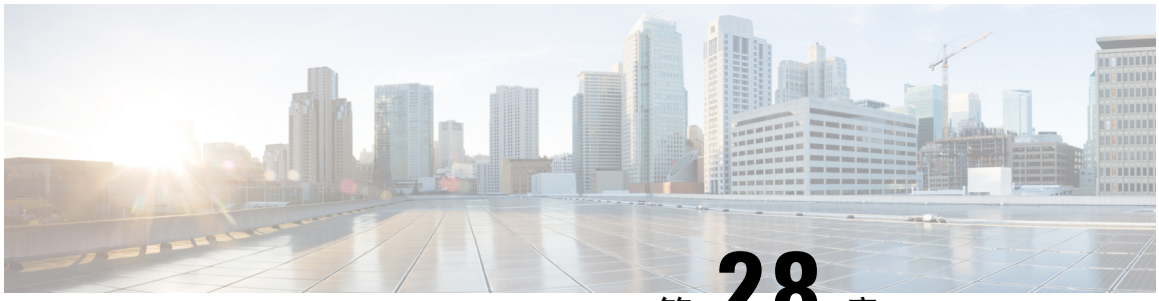
步驟 3 點擊**終止階段作業**。

步驟 4 按一下**確定**。

若被終止的使用者重新整理登錄介面頁面，則該使用者將被登出。 在審計記錄檔中輸入了一個項目，並顯示已被終止的使用者身份。

第 VII 部分

IP 位址、主機名稱和網域名稱更改



第 28 章

變更前任務和系統執行狀況檢查

變更前任務

IP 位址、主機名稱和其他網路標識符之變更

出於多種原因，您可以更改部署中節點的網路等級 IP 位址和主機名稱，包括將節點從一個叢集移至另一個叢集或解決重複的 IP 位址問題。 IP 位址是與節點關聯的網路等級 Internet 協定（IP），主機名稱是節點的網路等級主機名稱。

附註 所有 Unified Communications 產品（例如 Cisco Unified Communications Manager、Cisco Unity Connections、Cisco IM and Presence 等）皆僅有一個介面。 因此，每一項產品您僅能指派一個 IP 位址。

有關節點名稱和網域名稱等其他網路標識符的更改，請參閱以下資源：

- Cisco Unified Communications Manager 系統組態設定指南
- *IM and Presence Service* 配置及管理指南
- *Cisco Unified Communications Manager* 和 *IM and Presence Service*安裝指南

IM and Presence Service方面，變更節點名稱和該節點的網路等級 DNS 預設網域名稱的描述也包含在本檔案中。

IM and Presence Service 節點名稱和預設網域名稱的變更

節點名稱是使用 Cisco Unified CM 管理 GUI 配置的，並且需可從所有其他名稱中解析IM and Presence Service節點和所有用戶端電腦。 因此，推薦的節點名稱值爲節點的網路 FQDN。 但在某些部署中，還支援將 IP 位址和主機名稱作爲節點名的值。 有關節點名稱建議和支援的部署類型的更多資訊請參閱主機名稱組態 ，第 255 頁上的。

節點的網路等級 DNS 預設網域名稱與主機名稱在一起爲該節點的完全合格網域名稱（FQDN）。範例：具“imp-server”主機名稱和“example.com”網域的節點，FQDN 即爲“imp-server.example.com”。

勿將節點的網路等級 DNS 預設網域與 IM and Presence Service應用程式的企業等級網域混淆，

- 網路等級 DNS 預設網域僅作爲節點的網路標識符。
- 全企業範圍IM and Presence Service網域是一般使用者 IM 位址中使用的應用程式級網域。

您可以使用 Cisco Unified CM IM and Presence 管理 GUI 或Cisco Unified Communications Manager 管理。 有關企業範圍的網域和支援的部署類型的更多資訊請參閱*Cisco Unified Communications Manager* 上 *IM and Presence Service* 部署指南。

主機名稱組態

下表列出您可以爲 Unified Communications Manager 伺服器配置主機名稱的地方，允許主機名稱使用的字元數量以及建議主機名稱使用的第一個和最後一個字元。請注意，如果您沒有正確配置主機名稱，Unified Communications Manager 中的部分組件，例如作業系統、資料庫、安裝等元件可能無法按預期工作。

表 *81: Cisco Unified Communications Manager* 的主機名稱組態

主機名稱位置	允許的組態	允許的字元數	建議的主機名稱第一個字元	建議的主機名稱最後一個字元
主機名稱/IP 位址欄位 Cisco Unified Communications Manager 管理中的**系統** > **伺服器**。	您可以新增或變更叢集中的伺服器的主機名稱。	2-63	字母	英數字
主機名稱欄位 Cisco Unified Communications Manager 安裝精靈	您可以新增叢集中的伺服器的主機名稱。	1-63	字母	英數字
主機名稱欄位 Cisco Unified Communications 作業系統中的**設定** > **IP** > **乙太網路**	您可以變更 (非新增)叢集中的伺服器的主機名稱。	1-63	字母	英數字

主機名稱位置	允許的組態	允許的字元數	建議的主機名稱第一個字元	建議的主機名稱最後一個字元
設定網路主機名稱 主機名稱 命令行介面	您可以變更 (非新增)叢集中的伺服器的主機名稱。	1-63	字母	英數字

提示 主機名稱需遵循 ARPANET 主機名稱的規則。 您可以在主機名稱的第一個和最後一個字元之間輸入英數字元和連字符。

在任何位置設定主機名稱之前，請檢閱下列資訊：

- 「伺服器組態」視窗中的「主機名稱/IP 位址」欄位支援裝置對伺服器、應用程式對伺服器和伺服器對伺服器通訊，可讓您以小數點十進位的格式輸入 IPv4 位址或主機名稱。

  安裝 Unified Communications Manager 發佈者節點後，發佈者的主機名稱會自動顯示在此欄位。安裝 Unified Communications Manager 訂閱者節點前，請在 Unified Communications Manager 發佈者節點的此欄位中輸入訂閱者節點的 IP 位址或主機名稱。

  請僅在 Unified Communications Manager 可存取 DNS 伺服器以解析主機名稱爲 IP 位址時，在此欄位配置主機名稱；請確定您在 DNS 伺服器配置 Cisco Unified Communications Manager 的名稱和位址資訊。

提示 除了設定 DNS 伺服器的 Unified Communications Manager 資訊，您也會在 Cisco Unified Communications Manager 安裝期間輸入 DNS 資訊。

- Unified Communications Manager 發佈者節點安裝期間，您會輸入主機名稱，其爲必填欄位，以及發佈者節點的 IP 位址以設定網路資訊；也就是說，若您要使用靜態網路的話。

  Unified Communications Manager 訂閱者節點安裝期間，您會輸入 Unified Communications Manager 發佈者節點的主機名稱和 IP 位址，以讓 Unified Communications Manager 驗證網路連線和發佈者至訂閱者的驗證。 此外，您需輸入訂閱者節點的主機名稱和 IP 位址。 Unified Communications Manager 安裝提示您輸入使用者伺服器的主機名稱時，請輸入 Cisco Unified Communications Manager 管理「伺服器組態」視窗中顯示的值；亦即，若您已在「主機名稱/IP 位址」欄位設定使用者伺服器的主機名稱。

Procedure workflows

Cisco Unified Communications Manager 工作流程

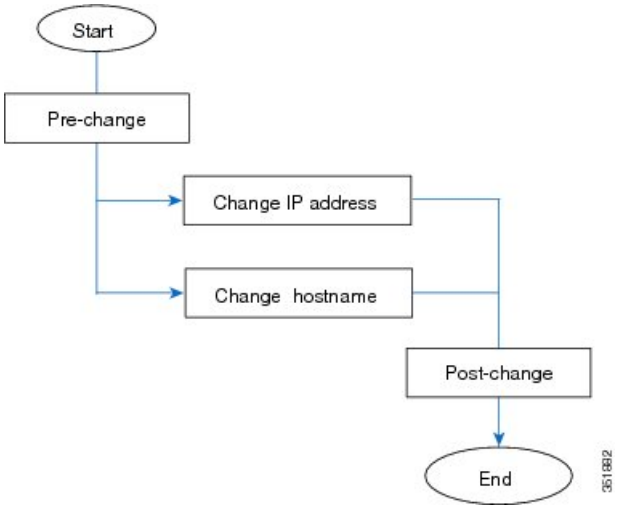
本檔案爲以下任務提供了詳細的步驟：Cisco Unified Communications Manager 節點：

- 更改節點的 IP 位址
- 更改節點的主機名稱

爲每個流程提供了任務清單，這些任務清單總結了要執行的步驟。

附註 在進行這些更改之前，您需完成所有的變更前任務和系統執行狀況檢查，並且需在進行任何這些變更之後完成變更後任務。

圖 *24: Cisco Unified Communications Manager* 工作流程



IM and Presence Service 工作流程

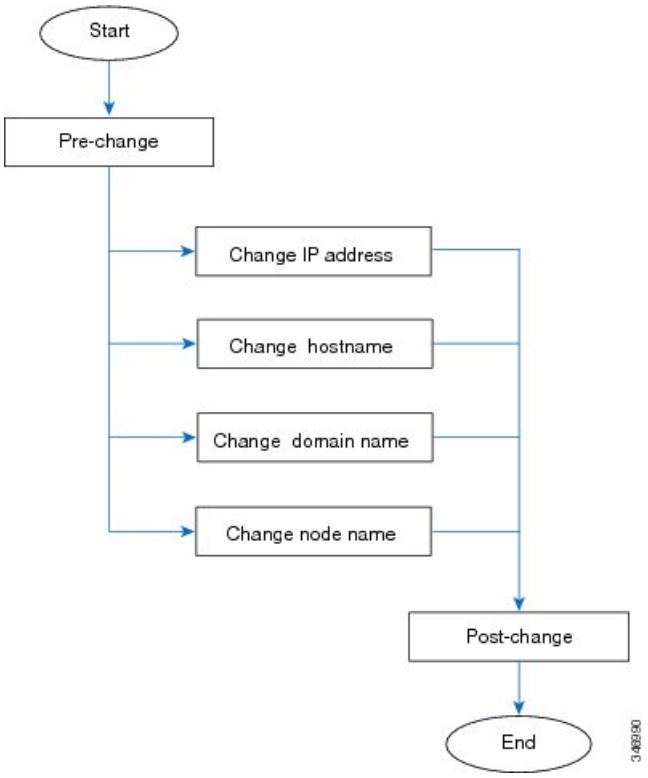
本說明文件爲 IM and Presence Service節點的任務提供了詳細的步驟：

- 更改節點的 IP 位址
- 更改節點的主機名稱
- 更改 DNS 預設網域名稱
- 更改節點的節點名稱

爲每個流程提供了任務清單，這些任務清單總結了要執行的步驟。

附註 在進行這些更改之前，您需完成所有的變更前任務和系統執行狀況檢查，並且需在進行任何這些變更之後完成變更後任務。

圖 *25: IM and Presence Service* 工作流程



Cisco Unified Communications Manager 節點的變更前任務

以下流程解釋Cisco Unified Communications Manager節點更改 IP 位址和主機名稱的任務該如何操作。您需在計劃的維護時段內執行這些步驟。

注意 若執行這些任務時未收到預期的結果，請勿在解決問題之前繼續操作。

程序

步驟 1 若您在 Cisco Unified Communications Manager 伺服器上的任何位置配置了 DNS，請確定有配置正向和反向記錄（例如，A 記錄和 PTR 記錄），且 DNS 可存取亦正常運作。

步驟 2 檢查是否有任何活動的 ServerDown 警示，以確保叢集中的所有伺服器均已啓動並可用。 在第一個節點上使用 Cisco Unified 即時監控工具（RTMT）或命令行介面（CLI）。

a) 若要使用 Unified RTMT 進行檢查，請存取 Alert Central 並檢查是否有 ServerDown 警示。

b) 若要在第一個節點上使用 CLI 進行檢查，請輸入以下 CLI 命令並檢查應用程式事件記錄檔：

```
file search activelog syslog/CiscoSyslog ServerDown
```

範例輸出：請參閱與範例資料庫複製輸出相關的主題。 詳細流程和疑難排解：請參閱與驗證資料庫複製和對資料庫複製進行疑難排解有關的主題。

步驟 3 檢查叢集中所有 Cisco Unified Communications Manager 節點的資料庫複製狀態，以確保所有伺服器都成功複製資料庫更改。 IM and Presence Service方面，若您的部署中有多個節點，請使用 CLI 在資料庫發布者節點上檢查資料庫複製狀態。 用 Unified RTMT 或 CLI。 所有節點的狀態應爲2。

1. 若要使用 RTMT 進行檢查，請存取“資料庫摘要”並檢查複製狀態。
2. 若要使用 CLI 進行檢查，請輸入**utils dbreplication runtimestate**。

步驟 4 如以下範例所示，輸入 utils diagnose CLI 命令以檢查網路連線和 DNS 伺服器組態是否正常。

範例:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
Starting diagnostic test(s)
===========================
test - validate_network : Passed
Diagnostics Completed
admin:
```

步驟 5 在 Cisco Unified Reporting中，產生 Unified CM 資料庫狀態報告。 在此報告中尋找任何錯誤或警告。

步驟 6 在 Cisco Unified Reporting中，產生 Unified CM 叢集概覽報告。 在此報告中尋找任何錯誤或警告。

步驟 7 在第一個節點上的“Cisco Unified Communications Manager 管理”中，選擇**系統**>**伺服器**然後點按**尋找**。 顯示叢集中所有伺服器的清單。 保留此伺服器清單以供將來參考。 確保您儲存了叢集中每個節點的主機名稱和 IP 位址的清單。

步驟 8 執行手動災難復原系統備份，並確保成功備份所有節點和活躍的服務。 更多資訊請參閱 *Cisco Unified Communications Manager* 管理指南。

步驟 9 若要更改主機名稱，請停用 SAML 單一登錄（SSO）。 如需更多有關 OpenAM SAMLSSO 的資訊，請參閱 *Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南。

步驟 10 已啓用安全性的叢集（叢集安全性模式 1 - 混合）而言，請更新憑證信任清單（CTL）檔案。 有關更新和管理 CTL 檔案的詳細描述，包括將新的 TFTP 伺服器新增至現有 CTL 檔案中，請參閱*Cisco Unified Communications Manager* 安全指南。

附註 爲避免不必要的延遲，需先使用 TFTP 伺服器的新 IP 位址更新 CTL 檔案，然後再更改 TFTP 伺服器的 IP 位址。 若不執行此步驟，則需手動更新所有安全 IP 電話。

附註 所有支援安全性的 IP 電話始終會下載 CTL 檔案，該檔案包括允許電話與之通訊的 TFTP 伺服器的 IP 位址。 若更改一個或多個 TFTP 伺服器的 IP 位址，則需首先將新 IP 位址新增至 CTL 檔案中，以便電話可以與其 TFTP 伺服器通訊。

IM and Presence Service 節點的變更前設定任務

執行適用的變更前設定任務，以確保您的系統爲成功進行 IP 位址，主機名稱，網域或節點名更改做好了準備。 您需在排定的維護時段內執行這些步驟。

注意 若執行這些任務時未收到預期的結果，請勿在解決問題之前繼續操作。

附註 除非您要變更網域名稱或節點名稱，否則無需執行步驟，以驗證 Cisco AXL Web 服務和 IM and Presence Cisco 同步代理服務均已啓動。如需要執行的完整任務清單，請參閱變更前的任務清單。

程序

步驟 1 檢查叢集中所有節點上的資料庫複製狀態，以確保所有伺服器皆成功複製了資料庫的變更。

IM and Presence Service方面，若您的部署中有多個節點，請使用 CLI 在資料庫發布者節點上檢查資料庫複製狀態。

用 Unified RTMT 或 CLI。 所有節點的狀態應爲**2**。

a) 若要使用 RTMT 進行檢查，請存取“資料庫摘要”並檢查複製狀態。
b) 要使用 CLI 進行檢查請輸入**utils dbreplication runtimestate**。

範例輸出：請參閱與範例資料庫複製輸出相關的主題。 詳細流程和疑難排解：請參閱與驗證資料庫複製和對資料庫複製進行疑難排解有關的主題。

步驟 2 如以下範例所示，輸入**utils diagnose** CLI 命令以檢查網路連線和 DNS 伺服器組態是否正常。

範例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
============================ test - validate_network : Passed Diagnostics Completed
 admin:
```

步驟 3 執行手動災難復原系統備份，並確保成功備份所有節點和活躍的服務。

更多資訊請參閱 *Cisco Unified Communications Manager* 管理指南。

步驟 4 停用在線狀態備援群組的高可用性 有關配置在線狀態備援群組的資訊，請參閱 *Cisco Unified Communications Manager* 的系統配置指南中“配置在線狀態備援群組”一文。

附註
- 在停用高可用性之前，請記錄每個節點和子叢集中的使用者數量。 您可以在Cisco Unified CM IM and Presence 管理的 (**系統** > **狀態拓撲**) 視窗中尋找此資訊。
- 停用高可用性後，請等待至少 2 分鐘使設定在整個叢集中同步，然後再進行任何進一步的更改。

步驟 5 若要更改主機名稱，請停用 SAML 單一登錄（SSO）。 如需更多有關 OpenAM SAMLSSO 的資訊，請參閱 *Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南。

步驟 6 若在部署中配置了叢集間對等項，請執行以下任務：

a) 要更改的 IM and Presence 資料庫發布者節點是爲叢集間對等項的每一個叢集中，請在叢集間對等項清單中刪除發布者的叢集。

範例：

ClusterA、ClusterB 和 ClusterC 皆爲叢集間對等項。 您要更改 ClusterA 的發布者節點上的主機名稱。 您需首先從 ClusterB 和 ClusterC 上的叢集間對等方清單中刪除 ClusterA 發布者節點。

b) 在每個叢集中的第一個狀態備援群組的發布者和訂閱者節點上重新啓動 Cisco Intercluster Sync Agent。

步驟 7 編譯當前已啓動的所有服務的清單。 保留這些清單以備將來參考。

a) 選擇**工具** > **控制中心 - 網路服務**以檢視已啓動的網路服務的清單。
b) 選擇**工具** > **控制中心 - 網路服務**以檢視已啓動的網路服務的清單。

步驟 8 停止所有使用 Cisco Unified Serviceability 功能服務，選擇**工具** > **控制中心 - 功能服務**。 停止功能服務的順序並不重要。

提示 若要更改IP位址、主機名稱或兩者皆要更改，則無需完成此步驟。這些名稱更改會自動停止功能服務。

步驟 9 於 Cisco Unified 服務能力中選取 **工具** > **控制中心 -網路服務**時，停止列於 IM and Presence 服務服務群組中的以下網路服務。

您需依下列的順序停止這些IM and Presence Service網路服務：

1. Cisco 組態代理
2. Cisco 叢集間同步代理
3. Cisco 用戶端設定檔代理
4. Cisco OAM 代理
5. Cisco XCP 組態管理員
6. Cisco XCP 路由器
7. Cisco Presence 資料庫
8. Cisco SIP 註冊資料庫
9. Cisco 登入資料庫
10. Cisco 路由資料庫
11. Cisco 伺服器復原管理員
12. Cisco IM and Presence 資料監控器

步驟 10 在 Cisco Unified 服務能力中的 **工具** > **控制中心-功能服務**確認 Cisco AXL Web 服務已在 Cisco Unified Communications Manager 發佈者節點上啓動。

附註 僅當您要更改網域名稱或節點名稱時，才執行此步驟。

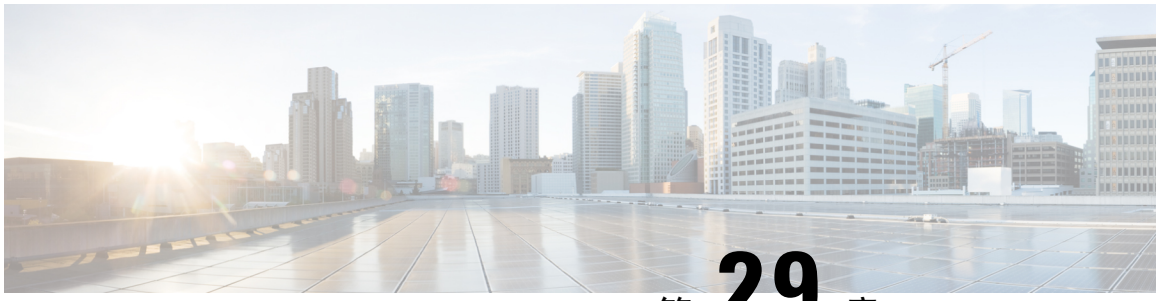
步驟 11 確認 Cisco Unified CM IM and Presence Cisco 同步代理服務已啓動並已成功完成資料同步。

附註 僅當您要更改網域名稱或節點名稱時，才執行此步驟。

a) 請執行以下的步驟以在 Cisco Unified Serviceability中確認：
   1. 選擇**工具** > **控制中心 - 網路服務**。
   2. 選擇 IM and Presence Service資料庫發佈者節點。
   3. 選擇 **IM and Presence Service 服務**。

4. 確定 Cisco 同步代理服務已經啓動。
5. 在 Cisco Unified CM IM and Presence 管理 GUI中選擇**診斷** > **系統儀表板** > **同步狀態**。
6. 確定同步已完成，且同步狀態區網域中沒有錯誤顯示。

b) 要在 IM and Presence 資料庫發布者節點上使用 Cisco Unified CM IM and Presence 管理 GUI 進行驗證，請選擇**診斷** > **系統儀表板**。



第 29 章

IP 位址和主機名稱之變更

更改 IP 位址和主機名稱任務清單

下表列出了更改Cisco Unified Communications Manager和IM and Presence Service節點的 IP 位址和主機名稱所要執行的任務。

表 *82:* 更改 *IP* 位址和主機名稱任務清單

物品	工作
1	執行變更前任務和系統執行狀況檢查。
2	使用命令行介面（CLI）或 Unified Operating System GUI 更改節點的 IP 位址或主機名稱。 請遵守以下有關IM and Presence Service節點的條件： • 在更改任何訂閱者節點之前，請更改資料庫發布者節點的 IP 位址和主機名稱。 • 您可以同時更改所有訂閱者節點的 IP 位址和主機名稱，亦可一個一個更改。 附註 變更 IP 位址或 IM and Presence 服務節點的主機名稱後，您必須變更 Cisco Unified Communications Manager 上 SIP 發佈 trunk 的目的地位址值。 請參閱變更後任務清單。
3	執行變更後任務。

透過作業系統管理 GUI 變更 IP 位址或主機名稱

您可以使用“Cisco Unified 作業系統管理”來更改由部署中的主機名稱定義的發布者和訂閱者節點的IP位址或主機名稱。除非另有說明，否則此流程中的每個步驟都適用於發布者節點和訂閱者節點上的Unified Communications Manager和IM and Presence 服務叢集。

透過 **set network hostname** 指令變更主機名稱會觸發自我簽署憑證的自動重新產生。 這將導致叢集中的所有裝置重設，以便它們可以下載更新的 ITL 檔案。 若叢集使用的是 CA 簽署的憑證，憑證將需重新簽署。

使用 **set network hostname** 指令僅變更 IP 位址將導致叢集中的所有裝置重設，以便能夠下載更新的 ITL 檔案。 憑證不會更新。

附註 變更主機名稱不會觸發 ITL 復原憑證的重新產生。

注意

- 透過 Cisco Unified 作業系統管理，我們建議您一次僅更改這些設定之一。 要同時更改 IP 位址和主機名稱，請使用 CLI 命令**設定網路主機名稱**。
- 若 Unified Communications Manager 叢集安全性在混合模式下執行，則在變更主機名稱或 IP 位址之後，直到執行 CTL 用戶端並更新 CTL 檔案或執行 **utils ctl update CTLFile**（若您使用無令牌 CTL 功能）前，連至此節點的安全連線將會失敗。

開始之前

在貴組織部署上執行變更前任務和系統執行狀況檢查。

附註 如果您必須從 vcenter 變更 vNIC，請使用 CLI 指令 **set network hostname**。

程序

步驟 1 在 Cisco Unified Operating System Administration 中選擇 **設定** > **IP** > **乙太網路**

步驟 2 更改主機名稱，IP 位址，並在必要時更改預設閘道。

步驟 3 按一下**儲存**。

節點伺服會隨著新更改自動重新啓動。 重新啓動服務可確保正確的更新和服務重新啓動順序，以使更改生效。

變更主機名稱將觸發自我簽署憑證的自動重新產生，並使叢集中的所有裝置重設，以便可以下載更新的 ITL 檔案。 變更主機名稱不會觸發 ITL 復原憑證的重新產生。

下一步

執行所有適用的變更後任務，以確保您的變更已在部署中正確納入。

附註 若新的主機名稱不能解析爲正確的 IP 位址，請勿繼續。

若叢集使用的是 CA 簽署的憑證，憑證將需重新簽署。

若您使用該流程將叢集設爲混合模式，請執行 CTL 用戶端以更新 CTL 檔案。 若您使用了無令牌 CTL 功能，請執行 CLI 命令：**utils ctl update CTLFile**

透過 Unified CM 管理 GUI 變更 IP 位址或主機名稱

您可以使用 Cisco Unified CM 管理變更在資料庫中定義的發佈者和訂閱者節點的 IP 位址或主機名稱。 這樣可確保主機名稱項目與系統定義的主機名稱或 IP 值一致。

變更IP位址或主機名稱會觸發自我簽署憑證的自動重新產生。這將導致叢集中的所有裝置重設，以便它們可以下載更新的 ITL 檔案。 若您的叢集使用的是 CA 簽署的憑證則需重新簽署。

注意

- 變更主機名稱或IP位址需要重新啓動系統服務。因此，應避免在正常工作時間內進行此變更。
- 透過 Cisco Unified CM 管理，我們建議您一次僅變更這些設定之一。 要同時更改 IP 位址和主機名稱，請使用 CLI 命令**設定網路主機名稱**。
- 若 Unified Communications Manager 叢集安全性在混合模式下執行，則在變更主機名稱或 IP 位址之後，直到執行 CTL 用戶端並更新 CTL 檔案或執行 **utils ctl update CTLFile**（若您使用無令牌 CTL 功能）前，連至此節點的安全連線將會失敗。
- 如果在 Cisco Unified 作業系統管理和 Cisco Unified CM 管理頁面上定義的主機名稱或 IP 位址不相符，則應用程式無法提取正確的電話狀態。 此外，由於憑證不符，TLS 交握會失敗。 因此，請確保 Cisco Unified 作業系統管理和 Cisco Unified CM 管理頁面中的 IP 位址和主機名稱項目是類似的。

開始之前

在部署上執行變更前任務和系統執行狀況檢查。

程序

步驟 1 在 Cisco Unified CM 管理中，選擇**系統** > **伺服器**。

尋找及列出伺服器視窗會隨即顯示。

步驟 2 若要取得所有伺服器的清單，請按一下**尋找**。

步驟 3 從清單中，按一下要修改其主機名稱的伺服器。

步驟 4 在 **Host name/IP Address***（主機名稱/IP 位址*）欄位中，輸入新主機名稱或 IP 位址，然後按一下儲存。

步驟 5 使用管理 CLI GUI、使用 **utils system restart** CLI 指令重新啓動節點。

透過 CLI 變更 IP 位址或主機名稱

您可以使用 CLI 更改由部署中的主機名稱所定義之發布者和訂閱者節點的 IP 位址或主機名稱。 除非另有說明，否則此過程中的每個步驟均適用於 Cisco Unified Communications Manager 和 IM and Presence Service 叢集上的發布者和訂閱者節點。

變更主機名稱會觸發自我簽署憑證的自動重新產生。 這將導致叢集中的所有裝置重設，以便它們可以下載更新的 ITL 檔案。 若您的叢集使用的是 CA 簽署的憑證則需重新簽署。 變更主機名稱不會觸發 ITL 復原憑證的重新產生。

⚠

注意 若 Cisco Unified Communications Manager 叢集安全性在混合模式下執行，則在變更主機名稱或 IP 位址之後，直到執行 CTL 用戶端並更新 CTL 檔案或執行 **utils ctl update CTLFile**（若您使用無令牌 CTL 功能）前，連至此節點的安全連線將會失敗。

開始之前

在貴組織部署上執行變更前任務和系統執行狀況檢查。

程序

步驟 1 登入要更改的節點的 CLI。

步驟 2 輸入 **`set network hostname`**。

步驟 3 依提示更改主機名稱、IP 位址或預設閘道。

a) 輸入新的主機名稱，然後按**Enter**。
b) 若您還想再更改 IP 位址就輸入**是**；否則，請執行步驟 4。
c) 輸入新的 IP 位址。
d) 輸入子網路遮罩。
e) 輸入閘道的位址。

步驟 4 驗證所有輸入正確無誤，然後輸入**是**以開始這個流程。

下一步

執行所有適用的變更後任務，以確保您的變更已在部署中正確納入。

附註 若新的主機名稱不能解析爲正確的 IP 位址，請勿繼續。

若您的叢集使用的是 CA 簽署的憑證則需重新簽署。

若您使用該流程將叢集設爲混合模式，請執行 CTL 用戶端以更新 CTL 檔案。 若您使用了無令牌 CTL 功能，請執行 CLI 命令：**utils ctl update CTLFile**

設定網路主機名稱的範例 CLI 輸出

附註 如果您需要從 vCenter 更改 vNIC，請在步驟之後更新 vNIC調用 4 of 5 組件通知指令：regenerate_all_certs.sh如以下輸出所示。

```
 admin:set network hostname ctrl-c: 退出輸入 ***警告***在未先取消命令之前，請勿關閉此視窗。 此命令將自動重新啓動系統服務。 該命令不應在正常運作時間內發出。
============================================== =====注意：請確認新主機名稱在整個叢集中是唯一的，並且若使用 DNS 服務，則在繼續操作之前，所有 DNS 的配置都已完成。
============================================== =====安全警告：此操作將重新產生所有 CUCM 憑證，包括已上載的任何第三方簽署的憑證。 輸入主機名稱 ::newHostname 是否要此時更改網路 ip 位址[是]::警告：在命令完成之前，請不要關閉此視窗。ctrl-c：退出輸入。 ***警告***
============================================ ============注意：請驗證新 IP 位址在整個叢集中是否唯一。 ================================================ =====輸入 IP 位址:: 10.10.10.28 輸入 IP 子遮罩碼:：#pii_ajhfhhhzz 輸入閘道的 IP 位址:: 255.255.255.0：new 主機名稱 IP 位址：255.255.255.0 IP 子網路遮罩：#pii_ 10.10.10.1 是否要繼續[是/否]？是，調用 5 個組件通知指令中的 1 個：ahostname_callback.sh 資訊（0）：Processnode 查詢返回 = 名稱========== bldr-vcm18 將伺服器表從：“oldHostname”更新爲：“newHostname”行數：1 正在更新資料庫，請等待 90 秒更新資料庫，請等待 60 秒更新資料庫，請等待 30 秒 將要觸發/ usr / local / cm / bin / dbl updatefiles --remote = newHostname，oldHostname 調用 5 中的 2 個組件通知指令：clm_notify_hostname.sh 通知 正在驗證跨叢集節點的更新... platformConfig.xml 已爲最新的版本：bldr-vcm21 叢集更新成功調用了 5 個組件通知指令中的 3 個：drf_notify_hostname_change.py 調用了 5 個組件通知指令中的 4 個：regenerate_all_certs .sh 調用 5 個組件通知指令中的 5 個：update_idsenv.sh 調用 2 個組件通知指令中的 1 個：ahostname_callback.sh 資訊（0）：返回的 Processnode 查詢=名稱====要觸發/ usr / local / cm / bin / dbl updatefiles --remote = pii902 8587121 調用 2 個組件通知指令中的 2 個：clm_notify_hostname.sh 驗證跨叢集節點的更新... 關閉介面 eth0 中：
```

僅變更 IP 位址

您可使用 CLI 更改節點的 IP 位址。

若節點是以主機名稱或 FQDN 定義，若使用 DNS，則在進行更改之前需僅更新 DNS。

附註 IM and Presence Service方面:

- 首先更改並驗證 IM and Presence 資料庫發布者節點。
- 您可同時更改IM and Presence Service訂閱者節點或一次僅更改一個。

開始之前

在貴組織部署上執行變更前任務和系統執行狀況檢查。

程序

步驟 1 登入要更改的節點的 CLI。

步驟 2 輸入**set network ip eth0** ***new-ip_address new_netmask new_gateway***更改節點的 IP 位址。

附註 僅以 **set network ip eth0** 命令更改 IP 位址，並不會觸發憑證重新產生。

*new_ip_address*指定新的伺服器 IP 位址時， *new_netmask*指定新的伺服器網路遮罩而*new_gateway*則指定閘道位址。

將顯示以下輸出：

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1 警告：更改此設定將使該伺服器上的軟體授權無效。 該授權將需重新承載。 是否繼續？(y/n)
```

步驟 3 確保 CLI 命令有輸出。 輸入**是**然後按**輸入**開始此流程。

下一步

執行所有適用的變更後任務，以確保您的變更已在部署中正確納入。

設定網路 IP 位址的輸出範例

附註 如果您需要從 vCenter 更改 vNIC，請在步驟之後更新 vNIC調用 6 個組件通知指令中的 3 個：aetc_hosts_verify.sh如以下輸出所示。

```
admin:set network ip eth0 10.77.30.34 255.255.255.0 10.77.30.1 *** 警告 *** 該指令將重啓系統服務 ====================== ================================ 注意：請驗證新的 IP 位址在整個叢集群中是唯一的，如果使用 DNS 服務，在繼續之前請先完成所有 DNS 配置。 ================================================ ====== 繼續 (y/n)？y 調用 1 of 6 組件通知指令：acluster_healthcheck.sh 調用 2 of 6 組件通知指令：adns_verify.sh 未定義主 DNS 伺服器未定義輔助 DNS 伺服器調用 3 of 6 組件 通知指令：aetc_hosts_verify.sh 調用 4
```

```
 of 6 組件通知指令：afupdateip.sh 調用 5 of 6 組件通知指令：ahostname_callback.sh 訊息（0）：使用 10.77.30.33 返回的進程節點查詢：名稱 ==== 調用 6 of 6 組件通知指令：clm_notify_hostname.sh
```

使用 CLI 更改 DNS IP 位址

您可以使用 CLI 更改部署中發布者和訂閱者節點的 DNS IP 位址。 此流程中的每個步驟皆適用於CiscoUnified Communications Manager和IM and Presence Service叢集上發布者節點和訂閱者節點，除非另有說明

開始之前

在貴組織部署上執行變更前任務和系統執行狀況檢查。

程序

步驟 1 登入要更改的節點的 CLI。

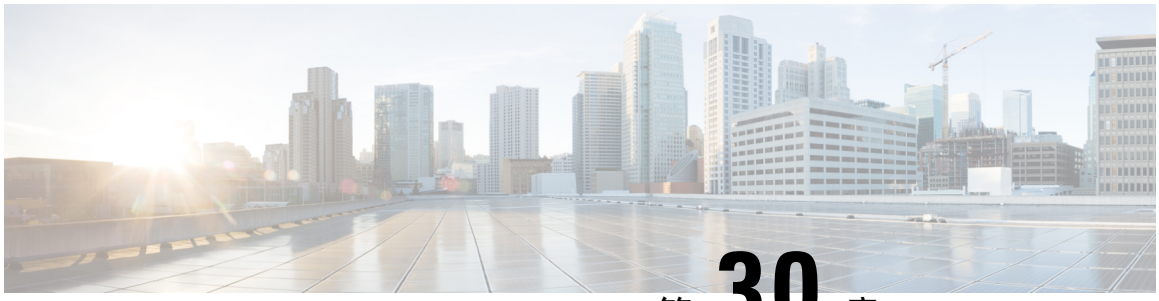
步驟 2 輸入 `set network dns primary/secondary <new IP address of the DNS>`

附註 如果變更 DNS 伺服器的 IP 位址，則必須透過 **utils system restart** CLI 指令重新啓動伺服器。

顯示以下輸出：

```
admin:set network dns primary/secondary <new IP address of DNS> *** 警告 *** 這將導致系統暫時失去網路連線
```

步驟 3 確保 CLI 命令有輸出。 輸入是然後按**輸入**開始這個流程。



第 30 章

網域名稱和節點名稱之變更

網域名稱更改

管理員可以修改與IM and Presence Service節點或節點組。

全企業範圍IM and Presence Service網域不需要與任何IM and Presence Service節點的 DNS 預設網域對齊。 若要爲部署修改企業範圍的網域，請參閱 *Cisco Unified Communications Manager* 上 *IM and Presence* 服務部署指南*IM and Presence Service* 組態和管理指南。

注意 更改網路中任何IM and Presence Service叢集節點上的預設網域將導致節點重新啓動以及狀態伺服和其他系統功能的中斷。 由於這會對系統造成影響，因此您需在計劃的維護時段內執行此網域更改流程。

更改節點的預設網域名稱時，所有第三方簽署的安全憑證都將自動被新的自我簽署憑證覆蓋。 若要讓第三方 CA 對這些憑證重新簽署，則需手動請求並上載新憑證。 可能需要重新啓動服務才能獲取這些新憑證。 根據請求新憑證所需的時間，可能需要一個單獨的維護視窗來安排服務重新啓動。

附註 變更節點的預設網域名稱之前無法請求新的憑證。 僅在節點上更改了網域並重新啓動節點後，才能產生憑證簽署請求（CSR）。

IM and Presence Service預設網域名稱變更任務

下表包含用於修改與 IM and Presence Service 節點或節點組關聯的網路等級 DNS 預設網域名稱的詳細步驟的指示。 此流程的詳細描述指定了在叢集中的多個節點上執行變更的確切步驟順序。

若要在多個叢集上執行此流程，則需一次在一個叢集上依序完成變更。

附註 您需按照此工作流程中顯示的確切順序完成此流程中的每個任務。

程序

步驟 1 在叢集中所有適用的節點上完成變更前任務。 某些變更前任務可能僅適用於 IM and Presence 資料庫發布者節點，若您正在修改訂閱者節點則可跳過這些任務。

步驟 2 在叢集中所有適用的節點上更新 IM and Presence Service 節點的 DNS 記錄。 您亦應適當地更新 SRV、正向（A）和反向（PTR）記錄以合併新的節點網域。

步驟 3 使用 Cisco Unified Communications Manager 管理更新叢集中所有適用節點上的 IM and Presence Service 節點名稱。

附註 對於 FQDN 節點名稱格式而言此步驟是必需的。 若節點名稱是 IP 位址或主機名稱，則不適用。

- 如果節點名稱是FQDN，則其將參照舊節點網域名稱。因此，您必須更新節點名稱，以使FQDN值反映新的網域名稱。
- 若節點名稱爲一 IP 位址或主機名稱，則不會引用該網域，因此不需要進行任何更改。

步驟 4 使用命令行介面（CLI）在所有適用的節點上更新 DNS 網域。 CLI 命令在節點作業系統上將進行所需的網域更改，並觸發每個節點的自動重新開機。

步驟 5 網域名稱更新後，您需在叢集中重啓所有節點的「A Cisco DB」服務，以確保所有節點上的作業系統配置檔皆有取得與已修改之節點關聯的 DNS 網域名稱變更。

附註 驗證系統是否正常運作。 如果您發現任何重複出現的問題，請確保重新啓動叢集中的所有節點。

步驟 6 使用 CLI 確認資料庫複製 詳細的資訊，請參閱與執行系統執行狀況檢查和資料庫複製疑難排解有關的主題。 在叢集中同步所有系統檔案後需驗證資料庫複製。

步驟 7 在節點上重新產生安全憑證。

- 所有 IM and Presence Service 安全憑證上的“對象通用名稱”皆設定爲節點 FQDN。 所以爲了合併新的節點網域，更改 DNS 網域後將會自動重新產生所有憑證。
- 先前由其他憑證簽署的任何憑證。

步驟 8 完成叢集中所有適用節點的變更後任務，以確保叢集可完全運作。

更新 DNS 記錄

因爲您要更改該節點的 DNS 網域，所以還需更新與該節點關聯的所有現有 DNS 記錄。 這包括以下類型的記錄：

- A 記錄
- PTR 記錄
- SRV 記錄

若要修改叢集中的多個節點，則需爲每個這些節點完成以下流程。

若要修改 IM and Presence 資料庫發布者節點，則需先在 IM and Presence 資料庫發布者節點上完成此流程，然後再在任何適用的IM and Presence Service訂閱者節點上重複流程。

附註
- 這些 DNS 記錄需在相同的維護視窗中更新，因爲 DNS 網域在節點上會自行更改。
- 在計劃的維護時段之前更新 DNS 記錄可能會產生不利影響IM and Presence Service功能。

開始之前

在部署上執行所有變更前任務和適用的系統執行狀況檢查。

程序

步驟 1 從舊網域中刪除該節點的舊 DNS 轉發（A）記錄。

步驟 2 爲新網域內的節點創建一個新的 DNS 轉發（A）記錄。

步驟 3 更新該節點的 DNS 反向（PTR）記錄，以指向該節點的更新的完全合格網域名稱（FQDN）。

步驟 4 更新任何指向該節點的 DNS SRV 記錄。

步驟 5 更新指向該節點的所有其他 DNS 記錄。

步驟 6 在每個節點上執行以下命令行介面（CLI）命令，以驗證上述所有 DNS 更改是否已傳播至叢集中的所有其他節點：

a) 要驗證新的 A 記錄請輸入**utils network host new-fqdn**；new-fqdn爲節點上更新的 FQDN。

範例：

```
admin:utils network host server1.new-domain.com 本地解析：server1.new-domain.com
 在本地解析爲 10.53.50.219 外部解析：server1.new-domain.com 的位址爲 10.53.50.219
```

b) 要驗證更新的 PTR 記錄請輸入**utils network host ip-addr**；ip-addr爲節點的 IP 位址。

```
admin:utils network host 10.53.50.219 本地解析：10.53.50.219 在本地解析爲
server1.new-domain.com 外部解析：server1.new-domain.com 有 10.53.50.219
219.50.53.10.in-addr.arpa 位址 網域名稱指針 server1.new-domain.com。
```

附註 在流程中的這裡，**本地解析**IP 位址的結果將繼續指向舊的 FQDN 值，直到在節點上更改 DNS 網域爲止。

c) 若要驗證任何更新的 SRV 記錄，請輸入**utils network host srv-name srv**；srv 名稱爲 SRV 記錄。

範例：

_xmpp-server SRV 記錄尋找範例。

```
admin:utils network host_xmpp-server._tcp。□galway-imp.com srv 本地解析：找不到任何內容 外部解析：_xmpp-server._tcp.sample.com 有 10.53.50.219 server1.new-domain.com 的 SRV 記錄。
```

下一步

更新IM and Presence Service節點名稱。

在 FQDN 值中更新節點名稱

若在 Cisco Unified CM IM 和狀態管理 GUI 上的狀態拓撲視窗中爲該節點定義的節點名稱設定爲該節點的完整網域名稱（FQDN），則其將參考舊網域名稱。因此，您必須更新節點名稱，以參照新的網域名稱。

附註 僅當此節點的節點名稱值設定爲 FQDN 時才需要此流程。 若節點名稱與節點的 IP 位址或主機名稱相符，則不需此流程。

若要修改叢集中的多個節點，則需爲每個這些節點依序完成以下流程。

若要修改 IM and Presence 資料庫發布者節點，則需先在IM and Presence Service 訂閱者節點上完成此流程，然後才能在發布者節點上完成該流程。

開始之前

更新該節點的 DNS 記錄。

程序

步驟 1 修改IM and Presence Service節點的名稱。

a) 登入 Cisco Unified Communications Manager 管理。
b) 選取 **系統** > **伺服器**。
c) 搜尋並選擇節點。
d) 更新**完全合格的網域名稱/ IP 位址**欄位，以便 FQDN 引用新的網域值， 例如將**完全合格的網域名稱/ IP 位址**的值從server1.old-domain.com更新爲server1.new-domain.com。
e) 選取**儲存**。

步驟 2 在**Cisco Unified CM IM and Presence 管理 GUI 的**在線狀態拓撲視窗中驗證此節點的應用程式伺服器項目是否已更新，以在伺服器上反映新的節點名稱。

a) 登入 Cisco Unified Communications Manager 管理後選擇**系統** > **應用程式伺服器**。
b) 視需要在**尋找並列出應用程式伺服器**視窗中按一下**尋找**。
c) 確定用於更新的節點名稱的項目存在於應用程式伺服器清單中。

附註 若沒有該節點的項目或項目存在但卻反映了該節點的舊節點名稱，則請勿繼續。

下一步

在所有適用的節點上更新 DNS 網域。

更新 DNS 網域

您可以使用命令行介面（CLI）更改IM and Presence Service節點的 DNS 網域。

全企業範圍的IM and Presence Service網域毋需與任何IM and Presence Service節點的網路等級 DNS 預設網域一致。 若要在部署中修改全企業範圍的網域，請參閱 *Cisco Unified Communications Manager* 上的 *IM and Presence* 服務部署指南。

若要修改叢集中的多個節點，則需爲每個節點依序完成以下流程。

若要修改 IM and Presence 資料庫發布者節點，則需先在資料庫發布者節點上完成此流程，然後再修改任何訂閱者節點。

開始之前

更新IM and Presence Service節點名稱。

程序

步驟 1 登錄至節點上的 CLI 並輸入**set network domain new-domain**；new-domain爲新網域的值。

範例：

```
admin:set network domain new-domain.com ***警告***在此伺服器上新增/刪除或更改網域名稱將破壞資料庫複製。 在要修改的所有系統上完成網域之修改後，請將叢集中的所有伺服器重新開機， 這樣將確保複製會繼續正常運作。 伺服器重新開機後，請確認資料庫複製所產生的 Cisco Unified Reporting 報告中未回報任何問題。 現在伺服器將重新啓動， 您是否要繼續？ 安全警告：此操作將重新產生所有 CUP 憑證，包括已上載的任何第三方簽署的憑證。 是否繼續？(y/n)
```

步驟 2 輸入**y**然後按**Return**以確認已更改網域並重新啓動節點，或輸入**n**以取消。

提示 節點名稱更改完成後將在該節點上重新產生所有憑證。若這些憑證中有任何憑證爲第三方CA所簽署，那您需在此流程稍後的步驟中重新請求這些憑證。

步驟 3 節點重新啓動後，輸入shownetwork eth0確認網域名稱的更改已生效。

範例：

在以下的範例中，新的網域爲 new-domain.com。

```
admin:show network eth0 乙太網路 □ DHCP：停用 狀態：啓用 IP 位址：10.53.50.219 IP 遮罩：255.255.255.000 是否偵測到連結：是 模式：自動停用、完整、1000 Mbit / s 重複 IP：否 DNS 主伺服器：10.53.51.234 輔助伺服器：未配置之選項：逾時：5 次嘗試：2  網域：new-domain.com 閘道：乙太網路 □上 10.53.50.1
```

步驟 4 在叢集中所有適用的節點上重複上述步驟。

下一步

將叢集中的所有節點重新啓動。

叢集節點注意事項

您可以使用命令行介面（CLI）重新啓動叢集節點中的「A Cisco DB」。

更改網域名然後節點重新啓動後，您必須重新啓動叢集中所有節點的「A Cisco DB」服務，包括那些自動重新啓動的節點，從 Unified CM Publisher 開始，然後隨著系統顯示已發佈的資料庫，便爲所有訂閱者重啓相關服務。 這樣可確保所有節點上的作業系統組態檔與新的網域值對齊。

驗證系統是否正常運作。 如果您發現任何重複出現的問題，請確保重新啓動叢集中的所有節點。

首先在 IM and Presence 資料庫發布者節點上啓動重新啓動流程。 資料庫發布者節點重新啓動後，以任何順序繼續重新啓動其餘的IM and Presence 服務訂閱者節點。

開始之前

確保該節點的 DNS 網域名稱已更改。

程序

步驟 1 使用 CLI 重新啓動 IM and Presence 資料庫發布者節點。 輸入**utils system restart**。

範例：

```
admin:utils system restart 您是否真的要重啓？ 輸入（是/否）？
```

步驟 2 輸入是然後按**返回**將其重新啓動。

步驟 3 等候直到看到顯示 IM and Presence 資料庫發布者節點已重新啓動的訊息。

範例：

```
根目錄的廣播訊息（星期三，十月 24 16:14:55 2012）：系統正在關閉，現在重新啓動！ 等候中 操作成功重新啓動。
```

步驟 4 登錄到IM and Presence 服務訂閱者節點並輸入**utils system restart**以重新啓動每個訂閱者節點。

附註 嘗試停止服務幾分鐘後，CLI 可能會要求您強制重新啓動。 若發生這種情況，請輸入是。

下一步

確認資料庫複製 請參閱與系統執行狀況檢查相關的主題以取得更多資訊。

重新產生安全憑證

節點的完全合格網域名稱（FQDN）在所有IM and Presence Service安全憑證中均用作主旨共同名稱。因此，在節點上更新 DNS 網域時，將自動重新產生所有安全憑證。

若任何憑證是由第三方 CA 所簽署的，則您需手動產生新的 CA 所簽署的憑證。

若要修改叢集中的多個節點，則需爲每個節點完成以下流程。

附註 變更節點的預設網域名稱之前無法請求新的憑證。 僅在節點上更改了網域並重新啓動節點後，才能產生憑證簽署請求（CSR）。

開始之前

驗證資料庫複製以確保在所有節點上成功建立資料庫複製。

程序

步驟 1 若憑證需由第三方憑證頒發機構簽署，請登錄到 Cisco Unified Operating System 管理 GUI 並爲每個相關憑證執行所需的步驟。

步驟 2 上載簽署憑證後，您可能需要在IM and Presence Service節點上重新啓動服務。

所需的服務重新啓動如下：

- Tomcat 憑證：執行以下命令行介面（CLI）命令來重新啓動 tomcat 服務：

  ```
  utils service restart Cisco Tomcat
  ```

- Cup-xmpp 憑證：從 Cisco Unified IM and Presence Serviceability GUI 重新啓動 Cisco XCP 路由器服務。
- Cup-xmpp-s2s 憑證: 從 Cisco Unified IM and Presence Serviceability GUI 重新啓動 Cisco XCP 路由器服務。

附註
- 這些操作將重新啓動受影響的服務。 因此，視獲取簽署憑證 lag 的時間而定，您可能需要安排重新啓動以供以後的維護時段使用。 同時，自我簽署憑證將繼續顯示在相關介面上，直到重新啓動伺服爲止。
- 若在前面的清單中未指定憑證，則不需重新啓動該憑證的服務。

下一步

在叢集內所有適用的節點上執行變更後任務清單。

節點名稱更改

您可以修改與IM and Presence Service關聯的節點或節點組。 更新會顯示在 Cisco Unified Communications Manager 管理中的**伺服器組態**視窗。

將這些流程用於以下的節點名稱變更之情形：

- IP 位址至主機名稱
- IP 位址至完整網域名稱 (FQDN)
- 主機名稱至 IP 位址
- 主機名稱至 FQDN
- FQDN 至主機名稱
- FQDN 至 IP 位址

如需更多有關節點名稱建議的資訊，請參閱 *Cisco Unified Communications Manager* 上 *IM and Presence* 服務的部署指南。

⚠

注意 使用此流程以只更改一個不需要網路等級更改的 IM and Presence Service節點的名稱。 在該情況下您需執行特定於更改網路IP位址、主機名稱或網域名稱的流程。您需在排定的維護時段內執行此節點名稱更改流程。 更改IM and Presence Service叢集中任何節點的節點名稱將導致節點重新啓動以及在線狀態服務和其他系統功能的中斷。

IM and Presence Service 節點名稱變更任務清單

下表爲更改與 IM and Presence Service節點或節點群組關聯的節點名稱的詳細步驟操作的描述。 此流程的詳細描述指定了執行變更的確切步驟順序。

若要在多個叢集上執行此流程，請依序完成所有步驟以一次更改一個叢集上的節點名稱。

表 *83:* 更改 *IM and Presence Service* 節點名稱任務清單

物品	工作
1	在叢集中所有適用的節點上完成變更前任務。 某些變更前任務可能僅適用於 IM and Presence 資料庫發布者節點，若您正在修改訂閱者節點則可跳過這些任務。
2	使用Cisco Unified Communications Manager 管理更新 IM and Presence Service節點名稱。
3	驗證節點名稱更新，並確定節點名稱的更改有與IM and Presence Service同步。
4	節點名稱更新完成後，使用命令行介面（CLI）驗證資料庫複製。 確保新的節點名稱已在整個叢集中複製，並且資料庫複製在所有節點上都可操作。
5	完成更新後的節點上的變更後任務清單，並驗證該節點是否正常運作。

更新節點名稱

若要修改叢集中的多個節點，則需爲每個節點依次完成以下流程。

若要修改 IM and Presence 資料庫發布者節點，則需先在 IM and Presence Service 訂閱者節點上完成此流程，然後才能在發布者節點上完成該流程。

附註　對於 IM and Presence 節點，建議使用完整網域名稱。但是，也支援 IP 位址和主機名稱。

開始之前

爲您的部署執行所有變更前任務和適用的系統執行狀況檢查。

程序

步驟 1 登錄 Cisco Unified CM IM and Presence 管理。

步驟 2 選取 **系統** > **伺服器**。

步驟 3 選擇您想要修改的節點。

步驟 4 在**主機名稱/ IP 位址**的欄位中更新節點名稱。

附註　確保將新產生的 SP 元資料上載到 IDP 伺服器。

步驟 5 若要修改叢集中的多個節點，請對每個節點重複此流程。

附註　若您更新 IM and Presence 服務節點名稱且也設定了第三方合規，則必須更新合規伺服器以使用基於節點名稱的新領域。此組態更新會在第三方合規伺服器上進行。 新領域將顯示在**Cisco Unified CM IM and Presence管理** > **訊息傳遞** > **合規** > **合規設定**視窗中。

下一步

驗證節點名稱的更改。

使用 CLI 驗證節點名稱之變更

您可以使用命令行介面（CLI）來驗證新節點名稱是否已在整個叢集中複製。

程序

步驟 1 輸入**run sql name select from processnode**以驗證新節點名稱已在叢集中的每個節點上正確複製。

範例：

```
admin:run SQL select name from processode name ======================
EnterpriseWideData server1.example.com server2.example.com server3.example.com
server4.example.com
```

步驟 2 驗證指定新節點名稱的叢集中每個節點都有一個項目。輸出中不應出現舊節點名稱。

a) 若輸出符合預期，則驗證已透過，您無需驗證節點的資料庫複製。
b) 若缺少任何新的節點名稱，或有偏好舊的節點名稱的設定，請繼續執行步驟 3。

步驟 3 要對在節點上所出現舊的節點名稱或缺少節點名稱進行疑難排解，請執行以下操作：

a) IM and Presence 資料庫發布者節點而言，請使用 Cisco Unified CM IM and Presence 管理 GUI 上的儀表板檢查同步Proxy是否執行正常，並驗證同步Proxy狀態中是否沒有錯誤。
b) 訂閱者節點而言，請執行驗證資料庫複製流程。

使用 Cisco Unified CM IM and Presence 管理驗證節點名稱變更

僅 IM and Presence Service 節點方面，請驗證此節點的應用程式伺服器項目已更新以反映 Cisco Unified CM IM and Presence 管理 GUI 上的新節點名稱。

開始之前

更新IM and Presence Service節點名稱。

程序

步驟 1 登錄 Cisco Unified CM IM and Presence 管理 GUI。

步驟 2 選擇**系統** > **在線狀態拓撲**。

步驟 3 驗證新節點名稱是否出現在**在線狀態拓撲**窗格中。

下一步

確認資料庫複製

更新 Cisco Unified Communications Manager 的網域名稱

您可以使用命令行介面（CLI）更改Cisco Unified Communications Manager網域名稱。 使用 CLI 在所有適用的節點上更新 DNS 網域名稱。 CLI 命令在節點上更改所需的網域名稱，並觸發每個節點的自動重新開機。

如果 Unified CM 叢集安全性模式並非安全，且您正在更新或變更網域，則會作爲網域變更的一部分，而所有憑證亦會重新產生。若要確保在電話上更新ITL，請在更新網域名稱之前執行以下步驟：

1. 確保所有電話均已在線且已註冊，以便可以處理更新的ITL。 執行此流程時不在線的電話，需手動刪除 ITL。
2. 將**準備將叢集返回舊版本 8.0 之前的企業參數**設定爲 **True**。 所有電話皆會自動重設並下載一個 ITL 檔案，其中包含空的 Trust Verification Services（TVS）和 TFTP 憑證部分。
3. 在電話上選取**設定 > 安全性 > 信任清單 > ITL 檔案**，以驗證 ITL 檔案的 TVS 和 TFTP 憑證部分爲空白。
4. 變更伺服器的網域，並讓設定爲返回舊版本的電話註冊到叢集。
5. 在所有電話都成功註冊到叢集後，將**準備叢集以返回至 8.0 之前的版本**企業參數設爲 **False**。

開始之前

- 更改網域名稱之前，請確定已有啓用 DNS。
- 登入 Cisco Unified Communications Manager 管理，然後導覽至**系統 > 伺服器欄位**頁面。 如果此伺服器組態設定頁面已有主機名稱項目，請先變更網域名稱的主機名稱項目。
- 執行所有變更前任務和適用的系統執行狀況檢查。 請參閱「相關主題」一節以取得更多資訊。

程序

步驟 1 登入命令行介面。

步驟 2 輸入**執行設定網路網域<new_domain_name>**。
該命令提示系統重新開機。

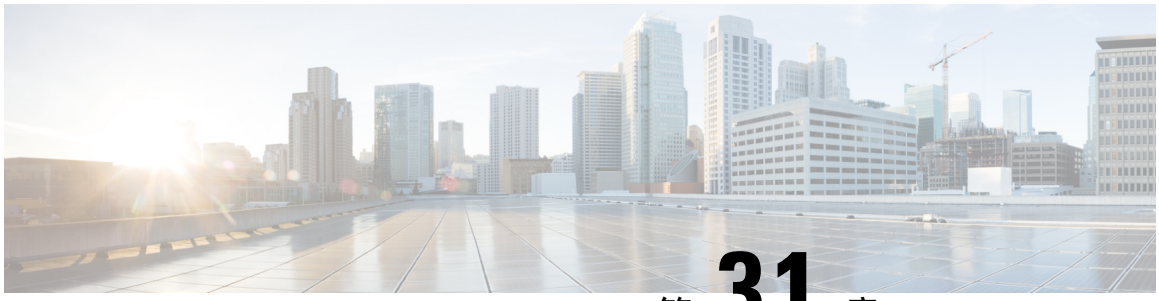
步驟 3 點按**是**以重新啓動系統。
重新啓動系統後，新網域名稱將會更新。

步驟 4 輸入**show network eth0**命令重新啓動後檢查新網域名稱是否已更新。

步驟 5 對於所有叢集節點重複此流程。

下一步

執行所有適用的變更後任務，以確保您的變更已在部署中正確納入。



第 31 章

變更後任務及驗證

Cisco Unified Communications Manager 節點的變更後任務

執行所有變更後任務，以確保您的變更在部署中正確納入。

⚠

注意 若執行這些任務時未收到預期的結果，請勿在解決問題之前繼續操作。

程序

步驟 1 若您在Cisco Unified Communications Manager伺服器上的任何位置配置了 DNS，請確定有配置正向和反向尋找區域且 DNS 可存取並正常運作。

步驟 2 檢查是否有任何活動的 ServerDown 警示，以確保叢集中的所有伺服器均已啓動並可用。 在第一個節點上使用 Cisco Unified 即時監控工具（RTMT）或命令行介面（CLI）。

a) 若要使用 Unified RTMT 進行檢查，請存取 Alert Central 並檢查是否有 ServerDown 警示。

b) 若要在第一個節點上使用 CLI 進行檢查，請輸入以下 CLI 命令並檢查應用程式事件記錄檔：

```
file search activelog syslog/CiscoSyslog ServerDown
```

步驟 3 檢查叢集中所有節點上的資料庫複製狀態，以確保所有伺服器皆成功複製了資料庫的變更。

IM and Presence Service方面，若您的部署中有多個節點，請使用 CLI 在資料庫發布者節點上檢查資料庫複製狀態。

用 Unified RTMT 或 CLI。 所有節點的狀態應爲**2**。

a) 若要使用 RTMT 進行檢查，請存取“資料庫摘要”並檢查複製狀態。

b) 要使用 CLI 進行檢查請輸入**`utils dbreplication runtimestate`**。

範例輸出：請參閱與範例資料庫複製輸出相關的主題。 詳細流程和疑難排解：請參閱與驗證資料庫複製和對資料庫複製進行疑難排解有關的主題。

步驟 4 如以下範例所示，輸入**utils diagnose** CLI 命令以檢查網路連線和 DNS 伺服器組態是否正常。

範例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
========================== test - validate_network : Passed Diagnostics Completed
 admin:
```

若您正在執行變更前的系統執行狀況檢查，則描述您已經完成；否則，請繼續執行變更後驗證步驟。

步驟 5 驗證新的主機名稱或 IP 位址是否出現在Cisco Unified Communications Manager伺服器清單。 在 Cisco Unified Communications Manager 管理中選擇**系統** > **伺服器**。

附註 執行此步驟作爲變更後任務的一部分。

步驟 6 驗證是否已在網路中完全納入對 IP 位址、主機名稱或兩者的更改。 在叢集中的每個節點上輸入 CLI 命令：**show network cluster**。

附註 執行此步驟作爲變更後任務的一部分。

輸出應包含節點的新 IP 位址或主機名稱。

範例：

```
admin:show network cluster 10.63.70.125 hippo2.burren.pst hippo2 訂閱者 cups DBPub
 已認證 10.63.70.48 aligator.burren.pst aligator 發布者 callmanager DBPub 已認證 自
星期三 2013 年 5 月 29 日 17:44:48 起使用 TCP
```

步驟 7 驗證對主機名稱的更改已在網路中完全納入。 在叢集中的每個節點上輸入CLI 指令 **utils network host**<***new_hostname***>。

附註 執行此步驟作爲變更後任務的一部分。

輸出應確認新的主機名稱在本地和外部解析爲 IP 位址。

範例：

```
admin:utils network host hippo2 Local Resolution: hippo2.burren.pst resolves
locally to 10.63.70.125 External Resolution: hippo2.burren.pst has address
10.63.70.125
```

工作。

步驟 8 啓用了安全性的叢集（叢集安全模式 1-混合）：在執行系統執行狀況檢查和其他變更後任務之前，請先更新 CTL 檔案，然後重新啓動叢集中的所有節點。

如需更多資訊，請參閱多伺服器叢集電話的憑證和 ITL 重新產生 ，第 377 頁上的一節。

步驟 9 若使用憑證信任清單（CTL）檔案和 USB eToken 啓用了叢集安全性，則若您更改了 8.0 版或更高版本節點的 IP 位址或主機名稱，需重新產生初始信任清單（ITL）檔案和 ITL 中的憑證。 若尚未使用憑證信任清單（CTL）檔案和 USB eToken 啓用叢集安全性，請跳過此步驟。

步驟 10 執行手動 DRS 備份，並確保所有節點和活躍的服務皆成功備份。

更多資訊請參閱 *Cisco Unified Communications Manager* 管理指南。

附註 更改節點的 IP 位址後，需執行手動 DRS 備份，因爲無法使用包含其他 IP 位址或主機名稱的 DRS 檔案還原節點。 更改後的 DRS 檔案將含新的 IP 位址或主機名稱。

步驟 11 更新所有相關的 IP 電話 URL 參數。

步驟 12 使用 Cisco Unified Communications Manager 管理來更新所有相關的 IP 電話服務。 選擇**系統** > **企業參數**。

步驟 13 更新 Unified RTMT 自訂警示和儲存的配置檔。

- 性能計數器所衍生出的 Unified RTMT 自訂警示包括硬編碼的伺服器 IP 位址。 您需刪除並重新配置這些自訂警示。
- 具有性能計數器的 Unified RTMT 儲存的配置檔包括硬編碼的伺服器 IP 位址。 您需刪除並重新新增這些計數器，然後儲存配置檔以將其更新爲新的 IP 位址。

步驟 14 若您使用的是在Cisco Unified Communications Manager上執行的整合 DHCP 伺服器，請將 DHCP 伺服器更新。

步驟 15 檢查並對其他關聯的 Cisco Unified Communications 組件進行任何必需的組態變更。

以下是要檢查的某些組件的部分清單：

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP / H.323 trunk
- IOS 閘道管理員
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 電話的 DHCP 作用網域範圍
- 用於 Cisco Unified Communications Manager Trace Collection以進行 CDR 匯出或作爲 DRS 備份目標的 SFTP 伺服器
- 註冊於 Cisco Unified Communications Manager 的 IOS 硬體資源（會議橋接、媒體終止點、代碼轉換器、RSVP Proxy）
- 註冊或與 Cisco Unified Communications Manager 整合的 IPVC 視訊 MCU
- Cisco Emergency Responder
- Cisco Unified Application Environment

- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 關聯的路由器和閘道

附註 請查閱您產品的說明文件，以確定如何對組態進行任何必需的更改。

Cisco Unified Communications Manager 節點的已啟用安全性的叢集任務

初始信任清單和憑證重新產生

若更改 Cisco Unified Communications Manager 8.0 或更高版本叢集中伺服器的 IP 位址或主機名稱，則會重新產生初始信任清單（ITL）檔案和 ITL 中的憑證。 重新產生的檔案與電話上儲存的檔案不相符。

附註 若使用憑證信任清單（CTL）檔案和USB eToken啓用叢集安全性，則無需執行以下流程中的步驟，因爲信任由 eToken 維護且 eToken 不會有所更改。

若未啓用叢集安全性，請執行單伺服器叢集或多伺服器叢集流程中的步驟以重設電話。

為單伺服器叢集電話重新產生憑證和 ITL

若您在 Cisco Unified Communications Manager 8.0 版或更高版本的單伺服器叢集中更改伺服器的 IP 位址或主機名稱，並且您正在使用 ITL 檔案，請執行以下步驟來重設電話。

在更改伺服器的 IP 位址或主機名稱之前，請啓用返回舊版本。

程序

步驟 1 確保所有電話均已在線且已註冊，以便可以處理更新的 ITL。 執行此流程時不在線的電話，需手動刪除 ITL。

步驟 2 將“準備將叢集返回舊版本 8.0 之前的企業參數”設定爲 True。 所有電話皆會自動重設並下載一個 ITL 檔案，其中包含空的 Trust Verification Services（TVS）和 TFTP 憑證部分。

步驟 3 在電話上選取**設定** > **安全性** > **信任清單** > **ITL 檔案**，以驗證 ITL 檔案的 TVS 和 TFTP 憑證部分爲空白。

步驟 4 更改伺服器的 IP 位址或主機名稱，並讓配置爲返回舊版本的電話註冊到叢集。

步驟 5 在所有電話都成功註冊到叢集後，將“準備叢集以返回至 8.0 之前的版本企業參數設爲**false**。

下一步

若使用 CTL 檔案或令牌，請在更改伺服器的 IP 位址或主機名稱後或在更改 DNS 網域名稱後重新執行 CTL 用戶端。

多伺服器叢集電話的憑證和 ITL 重新產生

在多伺服器叢集中，電話應具有主 TVS 伺服器和輔助 TVS 伺服器，以驗證重新產生的 ITL 檔案和憑證。 若電話無法聯繫主 TVS 伺服器（由於最近的組態變更），將退回至輔助伺服器。 TVS 伺服器由指派給電話的 CM 群組辨識。

在多伺服器叢集中，請確保一次僅更改一台伺服器上的 IP 位址或主機名稱。 若使用 CTL 檔案或令牌，請重新執行 CTL 用戶端或 CLI 命令集**utils ctl**在更改伺服器的 IP 位址或主機名稱之後，或者在更改 DNS 網域名稱之後。

IM and Presence Service 節點的變更後任務

執行所有變更後任務，以確保您的變更在部署中正確納入。

⚠

注意 若執行這些任務時未收到預期的結果，請勿在解決問題之前繼續操作。

程序

步驟 1 驗證對主機名稱或 IP 位址的更改是否已在 Cisco Unified Communications Manager 伺服器上更新。

步驟 2 在更改的節點上檢查網路連線和 DNS 伺服器組態。

附註 若您將 IP 位址更改爲其他子網路，請確保您的網路適配器現在已連線到正確的 VLAN。 此外，若 IP 位址更改後 IM and Presence Service節點屬於不同的子網路，請確保將 Cisco XCP Router 服務參數的“路由通訊類型”欄位設定爲“路由器到路由器”。 否則，“路由通訊類型”欄位應設定爲“多播 DNS”。

步驟 3 確認已在網路中完全納入對 IP 位址、主機名稱的變更。

步驟 4 若變更了主機名稱，請驗證主機名稱的變更已在網路中完全納入。

步驟 5 驗證資料庫複製已成功建立。 所有節點的狀態應顯示爲 2 並已連線。 若未設定複製，請參閱與資料庫複製疑難排解相關的主題。

步驟 6 若您停用了SAML單一登錄（SSO），您現在可將其啓用。 如需更多有關 SAMLSSO 的資訊，請參閱 *Cisco Unified Communications Manager* 上 *IM and Presence Service* 的部署指南。

步驟 7 若更改了主機名稱，則需確定 cup、cup-xmpp、Tomcat 憑證有包含新的主機名稱。

a) 在 Cisco Unified 作業系統管理 GUI 中，選擇**安全性** > **憑證管理**。

b) 確保信任憑證的名稱包含新的主機名稱；
c) 若憑證不包含新的主機名稱，請重新產生憑證。

更多資訊請參閱 *Cisco Unified Communications Manager* 管理指南。

步驟 8 若節點的 IP 位址已更改，請更新 Cisco Unified Real-Time Monitoring Tool（RTMT）自訂警示和已儲存的配置檔：

- 性能計數器所衍生出的 RTMT 自訂警示含有硬編碼的伺服器位址。 您需刪除並重新配置這些自訂警示。
- 具有性能計數器的 RTMT 儲存配置檔含有硬編碼的伺服器位址。 您需刪除並重新加入這些計數器，然後儲存配置檔以更新至新的位址。

步驟 9 檢查並對其他關聯的 Cisco Unified Communications 組件進行必要的組態變更，例如Cisco Unified Communications Manager上的 SIP trunk。

步驟 10 使用 Cisco Unified Serviceability 啓動在 CUP Services群組下列出的所有網路服務，選擇**工具** > **控制中心-網路服務**。

提示 若要更改IP位址、主機名稱或兩者皆要更改，則無需完成此步驟。這些名稱更改將自動啓動網路服務。 但是，若更改後某些伺服沒有自動啓動，請完成此步驟以確保啓動所有網路服務。

您需依下列的順序啓動 CUP Services 網路服務：

1. Cisco IM and Presence 資料監控器
2. Cisco 伺服器復原管理員
3. Cisco 路由資料庫
4. Cisco 登入資料庫
5. Cisco SIP 註冊資料庫
6. Cisco Presence 資料庫
7. Cisco XCP 組態管理員
8. Cisco XCP 路由器
9. Cisco OAM 代理
10. Cisco 用戶端設定檔代理
11. Cisco 叢集間同步代理
12. Cisco 組態代理

步驟 11 使用 Cisco Unified Serviceability 啓動所有功能服務，選擇**工具** > **控制中心 - 功能服務**。 啓動功能服務的順序並不重要。

提示 若要更改IP位址、主機名稱或兩者皆要更改，則無需完成此步驟。這些名稱更改將自動啓動功能服務。 倘若更改後某些服務沒有自動啓動，請完成此步驟以確保啓動所有功能服務。

步驟 12 請在啓用高可用性之前確認您的Cisco Jabber作業期間已重新建立， 否則爲其建立作業期間的 Jabber 用戶端將無法連線。

在所有叢集節點上執行 `show perf query counter Cisco Presence Engine Active JsmSessions` CLI 命令。活躍的作業期間數應符合停用高可用性時所記錄的使用者數。若開始作業期間所花費的時間超過 30 分鐘則可能爲較大的系統問題。

步驟 13 若在變更前設定期間停用了 HA，則在所有狀態備援群組上啓用高可用性（HA）。

步驟 14 驗證IM and Presence Service變更後可正常運作。

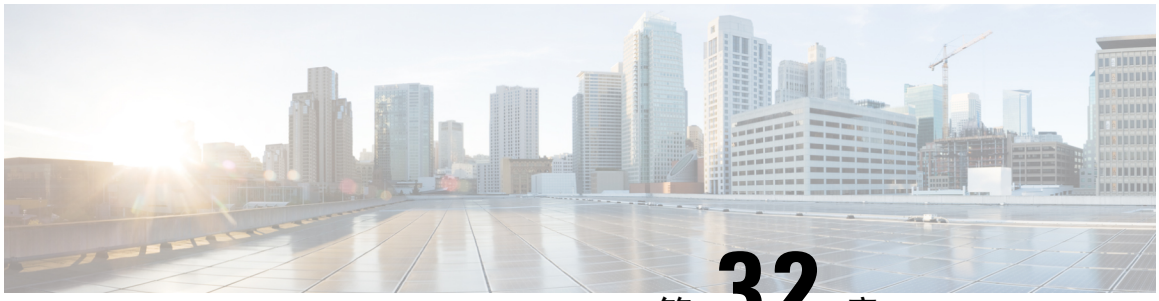
a) 在 Cisco Unified Serviceability GUI 中選擇**系統** > **在線狀態拓撲**。

- 若啓用了 HA，請確認所有 HA 節點都處於“正常”狀態。
- 確認所有服務皆已啓動。

b) 在 Cisco Unified CM IM and Presence 管理 GUI 中執行系統疑難排解工具，確保沒有失敗的測試。選擇**診斷程式** > **系統疑難排解工具**。

步驟 15 更改節點的 IP 位址或主機名稱後，需將手動災難復原系統備份，因您無法使用包含不同 IP 位址或主機名稱的 DRS 檔案來還原節點。 更改後的 DRS 檔案將含新的 IP 位址或主機名稱。

更多資訊請參閱 *Cisco Unified Communications Manager* 管理指南。



第 32 章

解決位址更改問題

對叢集身份驗證進行疑難排解

您可以使用命令行介面（CLI）對訂閱者節點上的叢集身份驗證問題進行疑難排解。

程序

步驟 1 輸入**show network eth0 [詳細資料]**以驗證網路組態。

步驟 2 輸入**顯示網路叢集**驗證網路叢集資訊。

- 若輸出顯示不正確的發布者資訊，請輸入**設定網路叢集發布者[主機名稱/ IP 位址]**訂閱者節點上的 CLI 命令以更正該資訊。
- 若您位於發布者節點上然後`show network cluster`CLI 命令顯示錯誤的訂閱者資訊，請登入至 Cisco Unified Communications Manager 管理再選擇**系統** > **伺服器**以檢查輸出。
- 若您在訂閱者節點上然後`show network cluster`輸出顯示不正確的發布者資訊，請使用`set network cluster publisher [主機名稱| IP 位址]` CLI 命令來變更發布者主機名稱或 IP 位址。

對資料庫複製進行疑難排解

您可以使用命令行介面（CLI）對叢集中的節點上的資料庫複製進行疑難排解。

- 驗證資料庫複製在叢集中處於正確狀態。
- 修復並重新建立節點的資料庫複製。

- 將資料庫複製重設。

如需有關使用 CLI 的詳細資訊，請參閱 *Cisco Unified Communications* 解決方案的命令行介面指南。

確認資料庫複製

使用命令行介面（CLI）檢查叢集中所有節點的資料庫複製狀態。 驗證複製設定（RTMT）和詳細資訊顯示的值爲**2**。 除 2 以外的任何其他值均表示存在資料庫複製的問題且您需重設該節點的複製。 請參閱與資料庫複製範例相關的主題以獲取範例輸出。

程序

步驟 1 在第一個節點上輸入**utils dbreplication runtimestate**以檢查叢集中所有節點上的資料庫複製。

IM and Presence Service方面，若您的部署中有多個節點，請在資料庫發布者節點上輸入命令。

提示 若未爲叢集中的節點設定複製，則可以使用 CLI 重設節點的資料庫複製。 更多資訊請參閱與使用 CLI 重設資料庫複製有關的主題。

範例：

```
admin:utils dbreplication runtimestimate DDB 和複製服務：ALL RUNNING DB CLI 狀態：沒有其他 dbreplication CLI 正在執行... 叢集複製狀態：BROADCAST SYNC 在 1 個伺服器上完成：2013-09-26-15-18 最後同步結果：SYNC COMPLETED 257 個表中的 257 個已同步 同步錯誤：NO ERRORS 資料庫版本：ccm9_0_1_10000_9000 複製表數：257 Repltimeout 設定爲：300s 在 PUB（2 台伺服器）中的叢集詳細資料檢視：PING REPLICATION REPL。 DBver& REPL。 REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? （RTMT）和詳細資訊----------- ------------ ----------------------- ---- ------ ----- ----------------- server1 100.10.10.17 0.052 是 已連線 0相符 是（2）PUB 設定已完成 server2 100.10.10.14 0.166 是 已連線 0相符 是（2）設定完成
```

步驟 2 驗證輸出。

輸出應顯示複製狀態爲**已連線**而應顯示每個節點的複製設定值爲（**2**）**設定完成**。 這代表著叢集中的複製網路執行正常。 若輸出結果不同，請繼續進行疑難排解和修復資料庫複製。

範例資料庫複製 CLI 輸出

以下清單顯示了您在叢集中第一個節點上的執行 `utils dbreplication runtimestate`命令行介面（CLI）命令時，Replicate_State 可能的值。

IM and Presence Service方面，若您的部署中有多個節點，請在資料庫發布者節點上輸入命令。

- 0-複製尚未開始。 不是沒有訂閱者存在，就是自安裝訂閱者以來資料庫層監控服務尚未執行。
- 1-已建立副本，但副本之計數不正確。
- 2-複製良好。
- 3-複製在叢集中不佳。

- 4-複寫設定未成功。

附註 驗證“複製設定（RTMT）和詳細資訊”顯示的值爲 2 非常重要。 除 2 以外的任何值均表示資料庫複製存在問題，您即需重設複製。 有關解決資料庫複製問題的資訊，請參閱與對資料庫複製進行疑難排解有關的主題。

Cisco Unified Communications Manager 節點範例 CLI 輸出

在此範例中，“複製設定（RTMT）和詳細資訊”顯示的值爲2。 複製良好。

```
admin: utils dbreplication runtimestate 伺服器時間：星期一 Jun 1 12:00:00 EDT 2013 叢集複製狀態：BROADCAST SYNC已在 1 個伺服器上完成：2013-06-01-12-00 上次同步結果：SYNC COMPLETE 在 672 個表中已完成 672 個 同步狀態：NO ERRORS 使用 CLI 檢視詳細資訊：'檔案檢視 activelog cm /trace/dbl/2013_06_01_12_00_00_dbl_repl_output_Broadcast.log'資料庫版本：ccm10_0_1_10000_1 Repltimeout 設定爲：300s PROCESS 選項設定爲：1 uc10-pub 的叢集詳細檢視（2 個伺服器）：PING 複製 REPLICATION SETUP SERVER-NAME IP ADDRESS（毫秒）RPC？ 群組 ID（RTMT）和詳細資訊----------- ---------- ---------------------- ------------------ uc10-pub 192.0.2.95 0.040 是（g_2）（2）安裝已完成 uc10-sub1 192.0.2.96 0.282 是（g_3）（2）安裝已完成
```

IM and Presence Service 節點的 CLI 輸出範例

在此範例中，“複製設定（RTMT）和詳細資訊”顯示的值爲2。 複製良好。

```
admin： utils dbreplication runtimestate 伺服器時間：星期一 Jun 1 12:00:00 EDT 2013 資料庫和複製服務：ALL RUNNING 叢集複製狀態：複製狀態命令始於：2012-02-26-09-40 複製狀態命令 COMPLETED 269 表中已完成檢查 269 個 沒有發現錯誤或不相符。 使用“file view activelog cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out”檢視詳細資訊資料庫版本：ccm8_6_3_10000_23 已複製表的數目：269 在 PUB 中的叢集詳細檢視（2 個伺服器）：PING REPLICATION REPL。 DBver& REPL。 REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? （RTMT）和詳細資訊----------- ------------ ---------------------- ---- ---------- ----- ----------------- gwydla020218 10.53.46.130 0.038 是已連線 0 相符是（2）PUB 設定已完成 gwydla020220 10.53.46.133 0.248 是已連線 128 相符是（2）設定完成
```

修補資料庫複製

使用命令行介面（CLI）修復資料庫複製。

程序

步驟 1 在第一個節點上輸入**utils dbreplication repair all**以嘗試修復資料庫複製。

IM and Presence Service方面，若您的部署中有多個節點，請在資料庫發布者節點中修復資料庫複製狀態。

根據資料庫的大小，修復資料庫複製可能需要幾分鐘。 繼續進行下一步，以監視資料庫複製修復的進度。

範例：

```
admin：utils dbreplication repair all-------------------- utils dbreplication repair--------------------複製修復程式現在已在背景執行。 使用“utils dbreplication runtimestate”命令檢查其進度輸出將在 cm / trace / dbl / sdi / ReplicationRepair.2013_05_11_12_33_57.out 檔案中。請使用“檔案檢視 activelog cm / trace / dbl / sdi / ReplicationRepair.2013_05_11_12_33_57.out”命令看輸出
```

步驟 2 在第一個節點上輸入**utils dbreplication runtimestate**檢查複製修復的進度。

IM and Presence Service方面，若您的部署中有多個節點，請在資料庫發布者節點上輸入命令。

範例複製輸出中的粗體文字強調了複製修復的最終狀態。

範例：

```
admin：utils dbreplication runtimestate DB and Replication Services：所有正在執行的叢集複製狀態：複製修復命令始於：2013-05-11-12-33複製修復命令已完成 已處理 269 個表（共 269 個）未找到錯誤或不相符。 使用“file view activelog cm / trace / dbl / sdi / ReplicationRepair.2013_05_11_12_33_57.out”檢視詳細資訊資料庫版本：ccm8_6_4_98000_192 複製表之數目：269 PUB 中的叢集詳細檢視（2 個伺服器）：PING REPLICATION REPL。 DBver& REPL。 REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? （RTMT）和詳細資訊----------- ------------ ---------------------- ---- ------ ----- ----------------- server1 100.10.10.17 0.052 是 已連線 0相符 是（2）PUB 設定已完成 server2 100.10.10.14 0.166 是 已連線 0相符 是（2）設定完成
```

a) 若複製修復執行完成而沒有任何錯誤或不相符，請執行該流程以再次驗證節點名稱是否更改，以驗證新節點名稱現在是否已正確複製。
b) 若發現錯誤或不相符，則節點之間可能存在短暫的不相符。 執行該流程以再次修復資料庫複製。

附註 若經過多次嘗試修復複製後，若回報有不相符或錯誤，請與您的 Cisco 支援代表聯繫以解決此問題。

步驟 3 在第一個節點上輸入**utils dbreplication reset all**以嘗試重新建立複製。

IM and Presence Service方面，若部署中有多個節點，請在資料庫發布者節點上輸入命令。

根據資料庫的大小，完全重新建立複製可能需要幾分鐘到一個小時以上。 繼續進行下一步，以監視資料庫複製重建的進度。

範例：

```
admin：utils dbreplication reset all 此命令將嘗試啓動複製重設，並在 1-2 分鐘內返回。 複製之後將繼續進行背景修復 1 小時。 請注意 RTMT 複製狀態， 此值應爲 0 到 2。當所有子項的 RTMT 複寫狀態爲 2 時，複寫便已完成。 若“子複製”狀態變爲 4 或 1，則複製設定中有錯誤。 監視所有子項上的 RTMT 計數器，以確定複製何時完成。 若找到錯誤詳細資訊，將在下面列出。OK [10.53.56.14]
```

步驟 4 在第一個節點上輸入**utils dbreplication 執行時狀態**，以監視嘗試重建資料庫複製的進度。

IM and Presence Service方面，若您的部署中有多個節點，請在資料庫發布者節點上輸入命令。

當所有節點的複製狀態爲**連線**時，複製已視爲重新建立。複製設定值爲（**2**）**設定完成**。

範例：

```
admin:utils dbreplication runtimestimate DDB 和複製服務：ALL RUNNING DB CLI 狀態：沒有其他 dbreplication CLI 正在執行... 叢集複製狀態：BROADCAST SYNC 在 1 個伺服器上完成：2013-09-26-15-18 最後同步結果：SYNC COMPLETED 257 個表中的 257 個已同步 同步錯誤：NO ERRORS 資料庫版本：ccm9_0_1_10000_9000 複製表數：257 Repltimeout 設定爲：300s 在 newserver100（2 台伺服器）中的叢集詳細資料檢視：PING REPLICATION REPL。 DBver& REPL。 REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? （RTMT）和詳細資料----------- -------------- -------------------- ------ ------ ----- ----------------- server1 100.10.10.201 0.038 是 已連線 0 相符是（2）PUB 設定已完成 server2 100.10.10.202 0.248 是已連線 0 相符是（2）設定已完成 server3 100.10.10.203 0.248 是已連線 0 相符是（2）設定已完成 server4 100.10.10.204 0.248 是已連線 0
```

a) 若重新建立複製，請執行該流程以再次驗證節點名稱是否變更，以驗證新節點名稱現在是否已正確複製。

b) 若複製無法恢復，請與您的 Cisco 支援代表聯繫以解決此問題。

注意 若資料庫複製已損壞，請不要繼續進行此操作。

將資料庫複製重設

若未爲叢集中的節點設定複製，請重設資料庫複製。 您可以使用命令行介面（CLI）重設資料庫複製。

開始之前

檢查叢集中所有節點的資料庫複製狀態。 確定複製設定（RTMT）和詳細資訊所顯示的值爲2。 除 2 以外的任何其他值均表示存在資料庫複製的問題且您需重設該節點的複製。

程序

步驟 1 在叢集中的節點上重設複製。 請執行下列其中一個步驟:

a) Unified Communications Manager：請輸入**utils db Replication reset all**。

在任何Cisco Unified Communications Manager 節點上執行此 CLI 命令之前，先在所有重設的訂閱伺服器節點上和在發布伺服器上執行**utils dbreplication stop**命令。 如需詳細資訊，請參閱 *Cisco Unified Communications* 解決方案的命令行介面指南。

b) IM and Presence Service：請在資料庫發布者節點上輸入**utils db Replication reset all**以在叢集中重設所有IM and Presence Service的節點。

提示 您可以輸入一個特定的主機名稱而非**所有**的主機名稱以僅在該節點上重設資料庫複製。 如需詳細資訊，請參閱 *Cisco Unified Communications* 解決方案的命令行介面指南。

步驟 2 輸入**utils dbreplication runtimestate**以檢查資料庫複製狀態。

IM and Presence Service：在 IM and Presence 資料庫發布者節點上執行 CLI 命令

網路疑難排解

您可以使用命令行介面（CLI）對節點上的網路問題進行疑難排解。

程序

步驟 1 輸入**show network eth0 [詳細資料]**以驗證網路組態。

步驟 2 若缺少任何欄位，則需重設網路介面。

a) 輸入**set nework status eth0 down**。

b) 輸入**set network status eth0 up**。

步驟 3 確認 IP 位址、遮罩和閘道。

確定這些值在整個網路中皆爲唯一。

Network Time Protocol troubleshooting

對訂閱者節點上的 NTP 進行疑難排解

您可以使用命令行介面（CLI）對訂閱者節點上的網路時間協定（NTP）問題進行疑難排解。

程序

步驟 1 輸入**show network eth0 [detail]**以驗證網路組態。

步驟 2 輸入**utils ntp status**以驗證 NTP 狀態。

步驟 3 輸入**utils ntp restart**以重新啓動 NTP。

步驟 4 輸入**show network cluster**驗證網路叢集。

若輸出顯示不正確的發布者資訊，請使用**設定網路叢集發布者[主機名稱/ IP 位址]** CLI 命令以重設發布者。

對發布者節點上的 NTP 進行疑難排解

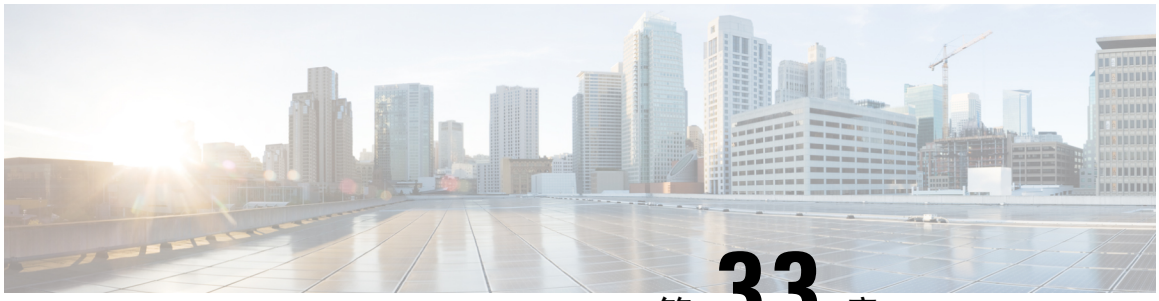
您可以使用命令行介面（CLI）解決發布者節點上的網路時間協定（NTP）問題。

程序

	命令或動作	目的
步驟 1	輸入**show network eth0 [detail]**以驗證網路組態。	
步驟 2	輸入**utils ntp status**以驗證NTP狀態。	
步驟 3	輸入**utils ntp restart**以重新啓動NTP。	
步驟 4	輸入**utils ntp server list**以驗證NTP伺服器。	若要新增或刪除 NTP 伺服器，請使用**utils ntp server[新增/刪除]** CLI 命令。

第 VIII 部分

災害復原



第 33 章

備份系統

備份概覽

Cisco 建議您定期執行備份。 您可以使用災害復原系統 (DRS) 爲叢集中的所有伺服器執行完整的資料備份。 您可以設定自動備份或隨時叫用備份。

災害復原系統會執行叢集層級備份，這表示它會將 Cisco Unified Communications Manager 叢集中所有伺服器的備份收集到一個中心位置，然後將備份資料封存到實體存放裝置。 備份檔案已加密，且僅可由系統軟體開啓。

DRS 會將其設定 (備份裝置設定和排程設定)還原爲平台備份/還原的一部分。 DRS 會備份及還原 drfDevice.xml 和 drfSchedule.xml 檔案。 伺服器還原這些檔案時，您不需要重新設定 DRS 備份裝置和排程。

執行系統資料還原時，您可以選擇您要還原的叢集中節點。

災害復原系統包含下列功能：

- 用於執行備份和還原工作的UI 。
- 用於執行備份功能的分散式系統架構。
- 排程備份或手動 (使用者叫用)備份。
- 備份會封存至遠端 SFTP 伺服器。

該表格會顯示災害復原系統可以備份和還原的功能和元件。 對於您選擇的每個功能，系統會自動備份其所有元件。

表 *84: Cisco Unified CM* 功能和元件

功能	組件
CCM - Unified Communications Manager	Unified Communications Manager 資料庫
	平台
	Serviceability
	待話期間背景音樂 (MOH)
	Cisco Emergency Responder
	批量工具 (BAT)
	偏好設定
	電話裝置檔案 (TFTP)
	syslogagt (SNMP 系統日誌代理)
	cdpagent (SNMP cdp 代理)
	tct (追蹤收集工具)
	通話詳細記錄 (CDR)
	CDR 報告和分析 (CAR)

表 *85: IM and Presence* 功能和組件

功能	組件
IM and Presence Service	IM and Presence 資料庫
	syslogagt (SNMP 系統日誌代理)
	cdpagent (SNMP cdp 代理)
	平台
	報告工具 (Serviceability 回報工具)
	CUP SIP 代理
	XCP
	CLM
	批量工具 (BAT)
	偏好設定
	tct (追蹤收集工具)

備份之先決條件

- 請確定您符合版本之需求：
  - 所有 Cisco Unified Communications Manager 的叢集節點皆需執行相同版本的 Cisco Unified Communications Manager 應用程式。
  - 所有 IM and Presence Service 叢集節點皆需執行相同版本的 IM and Presence Service 應用程式。
  - 備份檔案中儲存的軟體版本需符合叢集節點上執行的版本。

  整個版本字串需相符。 例如，若 IM and Presence 資料庫發佈者節點的版本是 11.5.1.10000-1，則所有 IM and Presence 訂閱者節點都需是 11.5.1.10000-1，且備份檔案也需是 11.5.1.10000-1。若您嘗試在與目前版本不符的備份檔案還原系統，還原將會失敗。 每當您升級軟體版本時，請務必備份系統，以讓儲存於備份檔案中的版本符合叢集節點執行的版本。
- 請注意，DRS加密取決於叢集安全性密碼。執行備份時，DRS會產生隨機密碼以進行加密，然後使用叢集安全性密碼加密隨機密碼。 若曾經在備份和本次還原之間變更叢集安全性密碼，您需記得備份時的密碼才能使用該備份檔案還原系統，或在變更/重設安全性密碼後立即備份。
- 若要備份至遠端裝置，請確定您已設定 SFTP 伺服器。 如需可用的 SFTP 伺服器的詳細資訊，請參閱 遠端備份的 SFTP 伺服器 ，第 399 頁上的

備份工作流程

完成這些工作以設定及執行備份。請勿在執行備份時執行任何作業系統管理工作。這是因爲災害復原系統鎖定平台 API 以封鎖所有作業系統管理請求。 然而，災害復原系統不會封鎖大多數 CLI 命令，因爲僅 CLI 式升級命令會使用平台 API 鎖定套件。

程序

	命令或動作	目的
步驟 1	配置備份裝置 ，第 394 頁上的	指定要備份資料的裝置。
步驟 2	備份檔案的估計大小 ，第 395 頁上的	估計建立於 SFTP 裝置上的備份檔案大小。
步驟 3	選擇下列其中一個選項： • 配置排程的備份 ，第 396 頁上的 • 開始手動備份 ，第 397 頁上的	建立備份排程以於排程期間備份資料。 您也可以執行手動備份。
步驟 4	檢視目前備份狀態 ，第 398 頁上的	選用。 檢查備份狀態。 執行備份時，您可以檢查目前備份工作的狀態。
步驟 5	檢視備份記錄 ，第 398 頁上的	選用。 檢視備份記錄

配置備份裝置

您可以設定最多 10 部備份裝置。 執行下列步驟以設定您要儲存備份檔案的位置。

開始之前

- 確保您具有 SFTP 伺服器的目錄路徑寫入存取權，以儲存備份檔案。
- 當 DRS Master Agent驗證備份裝置的組態時，請確保使用者名稱、密碼、伺服器名稱和目錄路徑有效。

附註　請在網路傳輸流量較少的時候排程備份。

程序

步驟 1 在災害復原系統中選擇 **Backup (備份)** > **Backup Device (備份裝置)**。

步驟 2 在 **備份裝置清單**視窗中，執行下列其中一項作業：

- 若要設定新裝置，請按一下 **新增**。
- 若要編輯現有的備份裝置，請輸入搜尋準則，按一下「尋找」，然後按一下 **編輯所選擇項目**。

- 若要刪除備份裝置，請在 **備份裝置**清單中選擇裝置，然後按一下 **刪除所選擇項目**。

您無法刪除在備份排程中設爲備份裝置的備份裝置。

步驟 3 在 **Backup Device Name (備份裝置名稱)**欄位中輸入備份名稱。

備份裝置名稱僅包含英數字元、空格 ()、破折號 (-) 和底線 (_)。 請勿使用任何其他字元。

步驟 4 在 **Select Destination (選擇目標)**區域中，於 **Network Directory (網路目錄)**底下執行下列工作：

- 在 **Host name/IP Address (主機名稱/IP 位址)**欄位中，輸入網路伺服器的主機名稱或 IP 位址。
- 在 **Path name (路徑名稱)**欄位中，輸入要儲存備份檔案的目錄路徑。
- 在 **(User name)使用者名稱**欄位中，輸入有效的使用者名稱。
- 在 **Password (密碼)**欄位中，輸入有效的密碼。
- 在 **Number of backups to store on Network Directory**（**於網路目錄儲存的備份數目**）下拉式清單中，選擇所需的備份數目。

步驟 5 點擊**儲存**。

下一步

備份檔案的估計大小 ，第 395 頁上的

備份檔案的估計大小

Cisco Unified Communications Manager 會估計備份 .tar 檔案的大小，但只在一或多個所選功能具有備份記錄的情況下估計。

計算的大小並非實際值而是備份壓縮檔案的估計大小。 大小是根據先前的成功備份實際備份大小來計算；若上次備份後已變更組態，則大小可能不同。

僅在先前的備份存在時，您才可以使用此流程；首次備份系統時無法使用此流程。

遵循此程序以估計儲存至 SFTP 裝置的備份壓縮檔案大小。

程序

步驟 1 在災害復原系統選擇**備份** > **手動備份**。

步驟 2 在**選擇功能**區域中，選擇要備份的功能。

步驟 3 按一下**估計**檢視所選功能的備份估計大小。

下一步

執行下列其中一個流程以備份系統：

- 配置排程的備份 ，第 396 頁上的

- 開始手動備份 ，第 397 頁上的

配置排程的備份

您可以建立最多 10 個備份排程。 每個備份排程皆有自己的屬性組合，包括自動備份的排程、要備份的功能組合和儲存位置。

請注意，您的備份 .tar 檔案會以隨機產生的密碼加密。 此密碼便會使用叢集安全性密碼加密，並與 .tar 備份檔案一同儲存。 變更或重設安全性密碼後，您需記住此安全性密碼或立即備份。

⚠

注意 請在非尖峰時段排程備份，以避免通話處理中斷或影響服務。

開始之前

配置備份裝置 ，第 394 頁上的

程序

步驟 1 在災害復原系統，選擇**備份排程工具**。

步驟 2 在 **Schedule List** (排程清單)視窗中執行下列其中一個步驟，以新增新排程或編輯現有的排程。

- 若要建立新排程，請按一下**新增**。
- 若要設定現有的排程，請按一下「Schedule List」 (排程清單)欄中的名稱。

步驟 3 在**排程工具**視窗中的**排程名稱**欄位輸入排程名稱。

附註 您無法變更預設排程的名稱。

步驟 4 在 **Select Backup Device** (選擇備份裝置)區域中，選擇備份裝置。

步驟 5 在 **Select Features** (選擇功能)區域中，選擇要備份的功能。 您至少須選取一個功能。

步驟 6 在 **Start Backup at** (開始備份時間)區域中，選擇您要開始備份的時間和日期。

步驟 7 在 **Frequency** (頻率)區域中，選擇您要進行備份的頻率。 頻率可設爲「Once Daily」 (每天)、「Weekly」 (每週)和「Monthly」 (每月)。 若您選擇 **Weekly** (每週)，您也可以選擇要在星期幾進行備份。

提示 若要將備份頻率設爲 **Weekly** (每週)，並在星期二至星期六進行，請按一下 **Set Default** (設定預設)。

步驟 8 若要更新這些設定，請按一下 **Save** (儲存)。

步驟 9 選擇下列其中一個選項：

- 若要啓用所選的排程，請按一下**啟用所選排程**。
- 若要停用所選的排程，請按一下 **Disable Selected Schedules** (停用所選排程)。
- 若要刪除所選的排程，請按一下**Delete Selected (刪除所選擇項目)**。

步驟 10 若要啓用排程，請按一下 **Enable Schedule** (啓用排程)。

下次備份會自動在您設定的時間進行。

附註 請確定叢集中的所有伺服器皆執行相同版本的 Cisco Unified Communications Manager 或Cisco IM and Presence Service 且可透過網路連線。 排程備份期間無法連線的伺服器將不會備份。

下一步

請執行下列流程：

- 備份檔案的估計大小 ，第 395 頁上的
- （選用） 檢視目前備份狀態 ，第 398 頁上的

開始手動備份

開始之前

- 請確定您使用的網路裝置與備份檔案的存放位置相同。 Unified Communications Manager 的虛擬部署不支援使用磁帶機儲存備份檔案。
- 請確定所有叢集節點皆已安裝相同的 Cisco Unified Communications Manager 或 IM and Presence Service 版本。
- 備份流程可能因爲遠端伺服器的可用空間不足或網路連線中斷而失敗。 面對導致備份失敗的問題後，您需開始新的備份。
- 請避免網路中斷。
- 配置備份裝置 ，第 394 頁上的
- 備份檔案的估計大小 ，第 395 頁上的
- 請確定您擁有叢集安全性密碼的記錄。 若叢集安全性密碼在完成此備份後變更，您需要知道密碼，否則將無法使用備份檔案還原系統。

附註 執行備份時，您無法在 Cisco Unified 作業系統管理或 Cisco Unified IM and Presence 作業系統管理中執行任何工作，因爲災害復原系統會鎖定平台 API 以封鎖所有請求。 然而，災害復原系統不會封鎖大多數 CLI 命令，因爲只有 CLI 式升級命令會使用平台 API 鎖定套件。

程序

步驟 1 在災害復原系統選擇**備份** > **手動備份**。

步驟 2 在**手動備份**視窗中，在 **Backup Device Name (備份裝置名稱)**區域選擇備份裝置。

步驟 3 在 **Select Features**（選擇功能）區域選擇功能。

步驟 4 按一下 **Start Backup**（開始備份）。

下一步

（選用）檢視目前備份狀態 ，第 398 頁上的

檢視目前備份狀態

執行下列步驟以檢查目前備份工作的狀態。

注意 請注意，若遠端伺服器的備份未在20個小時內完成，則備份階段作業會逾時，您需開始新的備份。

程序

步驟 1 在災害復原系統選擇**備份** > **目前狀態**。

步驟 2 若要檢視備份記錄檔，請按一下記錄檔檔案名稱的連結。

步驟 3 若要取消目前的備份，請按一下**取消備份**。

附註 目前的元件完成其備份作業後，便會取消備份。

下一步

檢視備份記錄 ，第 398 頁上的

檢視備份記錄

執行下列步驟可檢視備份記錄。

程序

步驟 1 在災害復原系統中選擇**備份** > **記錄**。

步驟 2 在 **備份記錄**視窗中，您可以檢視已執行的備份，包括檔案名稱、備份裝置、完成日期、結果、版本、已備份的功能和故障的功能。

附註 **備份記錄**視窗僅顯示最近 20 個備份工作。

備份互動和限制

備份限制

下列限制適用於備份：

表 *86:* 備份限制

限制	描述
叢集安全性密碼	我們建議您在變更叢集安全性密碼時執行備份。 備份加密使用叢集安全性密碼來加密備份檔案的資料。 若您在建立備份檔案後編輯叢集安全性密碼，將無法使用該備份檔案還原資料，除非您記得舊密碼。
Certificate Management	災害復原系統 (DRS) 在 Master Agent 和 Local Agent 之間使用 SSL 式通訊，以便在 Cisco Unified Communications Manager 的叢集節點之間進行資料驗證和加密。 DRS 針對公開/私密金鑰加密使用 IPSec 憑證。 請注意，若您在 Certificate Management 頁面刪除 IPSEC 信任存放區 (hostname.pem) 檔案，則 DRS 不會如預期運作。 若您手動刪除 IPSEC 信任檔案，則需確保將 IPSEC 憑證上傳至 IPSEC 信任。 如需詳細資訊，請參閱《*Cisco Unified Communications Manager* 安全指南》中的“憑證管理”一節：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html。

遠端備份的 SFTP 伺服器

若要將資料備份至網路上的遠端裝置，您需先配置 SFTP 伺服器。 對於內部測試，Cisco 在 Cisco Prime Collaboration 部署 (PCD) 上使用 SFTP 伺服器 (這些由 Cisco 提供)，支援則由 Cisco TAC 提供。請參考下表，瞭解有關 SFTP 伺服器選項的摘要：

使用下表中的資訊來判斷要在系統中使用的 SFTP 伺服器解決方案。

表 *87: SFTP* 伺服器資訊

SFTP 伺服器	資訊
Cisco Prime Collaboration 部署上的 SFTP 伺服器	此伺服器是由 Cisco 提供及測試的 SFTP 伺服器，並完全由 Cisco TAC 支援。 版本相容性視您的 Unified Communications Manager 版本和 Cisco Prime Collaboration 部署而定。 請先參閱 Cisco Prime Collaboration 部署管理指南，再升級其版本 (SFTP) 或 Unified Communications Manager，以確保版本相容。

SFTP 伺服器	資訊
Technology Partner 的 SFTP 伺服器	這些伺服器是由第三方提供和測試。 版本相容性視第三方測試而定。 若升級其 SFTP 產品和/或升級 Unified Communications Manager，請參閱 Technology Partner 頁面以瞭解相容的版本： https://marketplace.cisco.com
其他第三方 SFTP 伺服器	這些伺服器由第三方提供，且不受 Cisco TAC 正式支援。 版本相容性爲以能力所及的最佳方式建立相容的 SFTP 版本和 Unified Communications Manager 版本。 附註 這些產品未經過 Cisco 的測試，我們不保證功能性， Cisco TAC 不支援這些產品。 若需要完整測試及支援的 SFTP 解決方案，請使用 Cisco Prime Collaboration 部署或 Technology Partner。

加密支援

Unified Communications Manager 11.5 會通告下列 CBC 密碼以連線 SFTP：

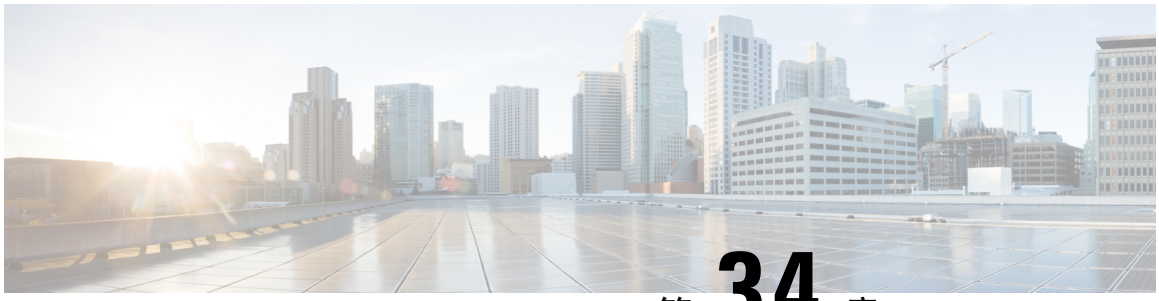
- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

附註 確保備份 SFTP 伺服器支援下列其中一個 CBC 加密與 Unified Communications Manager 通訊。

從 Unified Communications Manager 12.0 版開始，不支援 CBC 加密。 Unified Communications Manager 支援並僅通告下列 CTR 加密：

- aes256-ctr
- aes128-ctr
- aes192-ctr

附註 確保備份 SFTP 伺服器支援下列其中一個 CTR 加密與 Unified Communications Manager 通訊。



第 34 章

將系統還原

還原 概覽

災害復原系統 (DRS) 提供精靈，可引導您進行還原系統的流程。

備份檔案已加密，僅 DRS 系統可以開啓檔案以還原資料。 災害復原系統包含下列功能：

- 用於執行還原工作的UI 。
- 用於執行還原功能的分散式系統架構。

Master Agent

系統會自動啓動叢集各節點的 Master Agent 服務，但 Master Agent 只能在發佈者節點上運作。 訂閱者節點上的 Master Agent 不會執行任何功能。

Local Agent

伺服器具有 Local Agent，以執行備份和還原功能。

Cisco Unified Communications Manager 叢集中的每個節點 (包括含 Master Agent 的節點)皆需具有自己的 Local Agent，才能執行備份及還原功能。

附註 預設狀態爲，Local Agent 會自動在叢集的每個節點啓動，包括 IM and Presence節點。

還原的先決條件

- 請確定您符合版本之需求：
  - 所有 Cisco Unified Communications Manager 的叢集節點皆需執行相同版本的 Cisco Unified Communications Manager 應用程式。
  - 所有 IM and Presence Service 叢集節點皆需執行相同版本的 IM and Presence Service 應用程式。
  - 備份檔案中儲存的版本需符合叢集節點上執行的版本。

  整個版本字串需相符。 例如，若 IM and Presence 資料庫發佈者節點的版本是 11.5.1.10000-1，則所有 IM and Presence 訂閱者節點都需是 11.5.1.10000-1，且備份檔案也需是 11.5.1.10000-1。若您嘗試在與目前版本不符的備份檔案還原系統，還原將會失敗。
- 請確定伺服器的 IP 位址、主機名稱、DNS 組態和部署類型與儲存於備份檔案的 IP 位址、主機名稱、DNS 組態和部署類型相符。
- 若您在開始執行備份後變更叢集安全性密碼，請確保您擁有舊密碼的記錄，否則還原會故障。

恢復後重新啟用 SAML SSO

重要須知 此部分僅適用於版本 12.5(1)SU7。

使用 DRS 恢復系統後，可以在叢集中的任何節點間歇性停用 SAML SSO。 如要在受影響的節點上重新啓用 SAML SSO，您必須執行以下操作：

1. 在 Cisco Unified CM 管理中，選擇**系統** > **SAML 單一登入**。
2. 點擊**執行 SSO 測試**。
3. 在您看到 **SSO 測試成功！** 訊息之後，請關閉瀏覽器視窗；點擊**完成**。

附註 在 SAML SSO 重新啓用過程中，Cisco Tomcat 會重新啓動。 它對已啓用 SAML SSO 的節點不會有任何影響。

還原工作流程

在還原期間，請勿使用 Cisco Unified Communications Manager 作業系統管理或 Cisco Unified IM and Presence 作業系統管理執行任何工作。

程序

	命令或動作	目的
步驟 1	僅還原第一個節點 ，第 403 頁上的	(可任選)只使用此流程還原叢集中的第一個發佈者節點。
步驟 2	還原後續的叢集節點 ，第 405 頁上的	(可任選)使用此流程還原叢集中的訂閱者節點。
步驟 3	在重新建立發佈者後一個步驟即還原叢集 ，第 406 頁上的	(可任選)若已重新建立發佈者，遵循此流程以一個步驟還原整個叢集。
步驟 4	還原整個叢集 ，第 408 頁上的	(可任選)使用此流程還原叢集中的所有節點，包括發佈者節點。 若發生重大硬碟故障或升級，或進行硬碟移轉時，您可能需要重新建立叢集中所有節點。
步驟 5	將節點或叢集還原爲上次已知之正確組態 ，第 409 頁上的	(可任選)僅在您要將節點還原爲上次正確組態時使用此流程。 請勿在硬碟故障或其他硬體故障後使用此程式。
步驟 6	重新啓動節點 ，第 410 頁上的	使用此流程重新啓動節點。
步驟 7	檢查還原工作狀態 ，第 410 頁上的	(可任選)使用此流程檢查還原工作之狀態。
步驟 8	檢視還原記錄 ，第 411 頁上的	（可任選）使用此流程檢視還原歷史。

僅還原第一個節點

若您在重新建立後還原第一個節點，則需配置備份裝置。

此流程適用於 Cisco Unified Communications Manager 第一個節點，亦稱爲發佈者節點。 其他 Cisco Unified Communications Manager 節點和所有 IM and Presence Service 節點將會被視爲次要節點或訂閱者。

開始之前

若叢集中有 IM and Presence Service 節點，請確保您還原第一個節點時，該節點執行中且可存取。需如此，才能在流程期間找到有效備份檔案。

程序

步驟 1 在災害復原系統中選擇**Restore (還原)** > **Restore Wizard (還原精靈)**。

步驟 2 在 **Restore Wizard Step 1 (還原精靈步驟 1)**視窗中，於 **Select Backup Device (選擇備份裝置)**區域中，選擇要還原的適當備份裝置。

步驟 3 按**下一步**。

步驟 4 在 **Restore Wizard Step 2 (還原精靈步驟 2)**視窗中選擇您要還原的備份檔案。

附註 備份檔案名稱指示系統建立備份檔案的日期和時間。

步驟 5 按**下一步**。

步驟 6 在 **Restore Wizard Step 3 (還原精靈步驟 3)**視窗中按一下**下一步**。

步驟 7 選擇您想要還原的功能。

附註 選擇進行備份的功能會隨即顯示。

步驟 8 按**下一步**。「還原精靈步驟 4」視窗隨即顯示。

步驟 9 如果想要執行檔案完整性檢查，請選擇「使用 SHA1 訊息摘要執行檔案完整性檢查」核取方塊。

附註 檔案完整性檢查是可任選項目，僅在 SFTP 備份時才需要。

請注意，檔案完整性檢查程式會耗用大量 CPU 和網路頻寬，這會大幅地減慢還原程式。

我們也可以在 FIPS 模式下使用 SHA-1 進行訊息摘要驗證。 SHA-1 允許用於散列函數應用程式(如HMAC和隨機位產生)中的所有非數字簽名用途，這些應用程式不會用於數字簽名。 例如，SHA-1 仍可用於計算校驗和。 僅用於簽名產生和驗證，我們不能使用 SHA-1。

步驟 10 選擇要還原的節點。

步驟 11 按一下**還原**以還原資料。

步驟 12 按**下一步**。

步驟 13 提示您選擇要還原的節點時，請只選擇第一個節點 (發佈者)。

注意 請勿在此時選擇後續 (訂閱者) 節點，因爲這會造成還原失敗。

步驟 14 (選用)在 **Select Server Name (選擇伺服器名稱)**下拉式清單中，選擇您要還原發佈者資料庫的訂閱者節點。 請確保您選擇的訂閱者節點運作中且連線至叢集。
災害復原系統會在備份檔案還原所有非資料庫資訊，並在選擇的訂閱者節點提取最新的資料庫。

附註 僅當您選取的備份檔案包含 CCMDB 資料庫元件時，才會顯示此選項。 最初只會完全還原發佈者節點，但當您執行步驟 14 並重新啓動後續叢集節點時，災害復原系統會執行資料庫複製，並完整同步所有叢集節點資料庫。 這可確保所有叢集節點皆使用目前的資料。

步驟 15 按一下**還原**。

步驟 16 您的資料便會還原至發佈者節點。 視您的資料庫大小和選擇還原的元件而定，系統可能需要幾小時還原。

附註 還原第一個節點會將整個 Cisco Unified Communications Manager 資料庫還原至叢集。 視還原的資料庫節點數目和大小而定，這可能需要數個小時。 視您的資料庫大小和選擇還原的元件而定，系統可能需要幾小時還原。

步驟 17 當**恢復狀態**視窗上的**完成百分比**欄位顯示 100% 時，重新啓動伺服器。 若僅還原至第一個節點，則需重新啓動叢集中的所有節點。 請務必重新啓動第一個節點，再重新啓動後續節點。 如需關於如何重新啓動伺服器的相關資訊，請參閱「後續步驟」一節。

附註 若您只還原 Cisco Unified Communications Manager 節點，Cisco Unified Communications Manager 和 IM and Presence Service 叢集皆需重新啓動。

若您只還原 IM and Presence Service 發佈者節點，則需重新啓動 IM and Presence Service 叢集。

下一步

- （選用）若要檢視還原狀態，請參閱 檢查還原工作狀態 ，第 410 頁上的
- 若要重新啓動節點，請參閱 重新啓動節點 ，第 410 頁上的

還原後續的叢集節點

此流程僅適用於 Cisco Unified Communications Manager 訂閱者 (後續) 節點。 安裝的第一個 Cisco Unified Communications Manager 節點爲發佈者節點。 所有其他 Cisco Unified Communications Manager 節點，以及所有 IM and Presence Service 節點皆爲訂閱者節點。

遵循此流程以還原叢集中一或多個 Cisco Unified Communications Manager 訂閱者節點。

開始之前

執行還原作業前，請確保還原的主機名稱、IP 位址、DNS 組態和部署類型符合您要還原的備份檔案的主機名稱、IP 位址、DNS 組態和部署類型。 災害復原系統無法在不同主機名稱、IP 位址、DNS 組態和部署類型之間還原。

請確定安裝在伺服器的軟體版本符合您要還原的備份檔案的版本。 災害復原系統僅支援在符合的軟體版本進行還原作業。 若您在重新建立後還原後續節點，則必須設定備份裝置。

程序

步驟 1 在災害復原系統中，選擇 **Restore (還原)** > **Restore Wizard (還原精靈)**。

步驟 2 在 **Restore Wizard Step 1 (還原精靈步驟 1)**視窗中，於 **Select Backup Device (選擇備份裝置)**區域中，選擇要還原的備份裝置。

步驟 3 按**下一步**。

步驟 4 在 **Restore Wizard Step 2 (還原精靈步驟 2)**視窗中，選擇您要還原的備份檔案。

步驟 5 按**下一步**。

步驟 6 在 **Restore Wizard Step 3 (還原精靈步驟 3)**視窗中，選擇您要還原的功能。

附註　視窗中僅顯示您所選擇的已備份至檔案的功能。

步驟 7　按**下一步**。「還原精靈步驟 4」視窗隨即顯示。

步驟 8　在 **Restore Wizard Step 4 (還原精靈步驟 4)**視窗中，提示您選擇要還原的節點時，請僅選擇後續節點。

步驟 9　按一下**還原**。

步驟 10　您的資料便會還原至後續節點。 如需有關如何檢視還原狀態的詳細資訊，請參閱「後續步驟」一節。

附註　在還原期間，請勿使用「Cisco Unified Communications Manager 管理」或「使用者選項」執行任何工作。

步驟 11　當 **Restore Status (還原狀態)** 視窗中的 **Percentage Complete (完成百分比)** 欄位顯示 100% 時，請重新啟動您剛剛還原的次要伺服器。若僅還原至第一個節點，則需重新啟動叢集中的所有節點。請務必重新啟動第一個節點，再重新啟動後續節點。 如需關於如何重新啟動伺服器的相關資訊，請參閱「後續步驟」一節。

附註　若還原 IM and Presence Service 的第一個節點， 請務必重新啟動 IM and Presence Service 的第一個節點，再重新啟動 IM and Presence Service 的後續節點。

下一步

- （選用）若要檢視還原狀態，請參閱 檢查還原工作狀態 ，第 410 頁上的
- 若要重新啟動節點，請參閱 重新啟動節點 ，第 410 頁上的

在重新建立發佈者後一個步驟即還原叢集

視您的資料庫大小和選擇還原的元件而定，系統可能需要幾小時還原。 若已重新建立發佈者或新安裝發佈者，請遵循此流程以一個步驟還原整個叢集。

程序

步驟 1　在災害復原系統中，選擇 **Restore (還原)** > **Restore Wizard (還原精靈)**。

步驟 2　在 **Restore Wizard Step 1 (還原精靈步驟 1)**視窗中，於 **Select Backup Device (選擇備份裝置)**區域中，選擇要還原的備份裝置。

步驟 3　按**下一步**。

步驟 4　在 **Restore Wizard Step 2 (還原精靈步驟 2)**視窗中，選擇您要還原的備份檔案。

備份檔案名稱指示系統建立備份檔案的日期和時間。

請僅選擇您要還原整個叢集的叢集備份檔案。

步驟 5　按**下一步**。

步驟 6 在 **Restore Wizard Step 3 (還原精靈步驟 3)**視窗中，選擇您要還原的功能。

螢幕只會顯示已儲存至備份檔案的功能。

步驟 7 按**下一步**。

步驟 8 在 **Restore Wizard Step 4 (還原精靈步驟 4)**視窗中，按一下 **One-Step Restore (單步驟還原)**。

選擇還原的備份檔案是叢集中的備份檔案，且選擇還原的功能包含註冊發佈者和發佈者節點的功能時，此選項才會出現在 **Restore Wizard Step 4 (還原精靈步驟 4)**視窗中。 如需更多資訊，請參閱僅還原第一個節點 ，第 403 頁上的及還原後續的叢集節點 ，第 405 頁上的。

附註 如果狀態訊息指出發佈者無法成爲叢集感知。 無法開始單步驟還原” ，則您需要恢復發佈者節點，然後再恢復訂閱者節點。 請參閱相關主題以取得更多資訊。

此選項可讓發佈者成爲叢集感知，且需要 5 分鐘。 當您按一下此選項，狀態訊息就會顯示爲 “Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period” (請等待 5 分鐘，直到發佈者成爲叢集感知，請勿在這段期間啓動任何備份或還原活動)。

延遲過後，若發佈者會成爲叢集感知，狀態訊息會顯示爲 “Publisher has become cluster aware. (發佈者已成爲叢集感知。) Please select the servers and click on Restore to start the restore of entire cluster (請選擇伺服器，然後按一下「還原」開始還原整個叢集)。”

延遲過後，若發佈者仍未成爲叢集感知，狀態訊息會顯示爲「Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore.」(發佈者未成爲叢集感知。無法開始一步即還原，請繼續執行一般的兩步還原。)若要以兩個步驟還原整個叢集 (先還原發佈者，然後還原訂閱者)，請執行僅還原第一個節點 ，第 403 頁上的和還原後續的叢集節點 ，第 405 頁上的中的步驟。

步驟 9 提示您選擇要還原的節點時，請選擇叢集中所有節點。

還原第一個節點時，災害復原系統會自動還原後續節點上的 Cisco Unified Communications Manager 資料庫 (CCMDB)。 視還原的資料庫節點數目和大小而定，這可能需要數個小時。

步驟 10 按一下**還原**。
您的資料便會在叢集中的所有節點上還原。

步驟 11 當**恢復狀態視窗**上的**完成百分比**欄位顯示 100% 時，重新啓動伺服器。 若僅還原至第一個節點，則需重新啓動叢集中的所有節點。請務必重新啓動第一個節點，再重新啓動後續節點。如需關於如何重新啓動伺服器的相關資訊，請參閱「後續步驟」一節。

下一步

- （選用）若要檢視還原狀態，請參閱 檢查還原工作狀態 ，第 410 頁上的
- 若要重新啓動節點，請參閱 重新啓動節點 ，第 410 頁上的

相關主題

僅還原第一個節點 ，第 403 頁上的
還原後續的叢集節點 ，第 405 頁上的

還原整個叢集

若發生重大硬碟故障或升級，或進行硬碟移轉時，您需重新建立叢集中所有節點。 請遵循下列步驟還原整個叢集。

若您正在進行其他大多數類型的硬體升級，例如更換網路卡或新增記憶體，您無需再執行此程式。

程序

步驟 1 在災害復原系統中，選擇 **Restore (還原)** > **Restore Wizard (還原精靈)**。

步驟 2 在**選擇備份裝置**一區中選擇要還原的適當備份裝置。

步驟 3 按**下一步**。

步驟 4 在 **Restore Wizard Step 2 (還原精靈步驟 2)**視窗中選擇您要還原的備份檔案。

附註 備份檔案名稱指示系統建立備份檔案的日期和時間。

步驟 5 按**下一步**。

步驟 6 在 **Restore Wizard Step 3 (還原精靈步驟 3)**視窗中按一下**下一步**。

步驟 7 收到提示選擇還原節點時，請在 **Restore Wizard Step 4 (還原精靈步驟 4)**視窗中選擇所有節點。

步驟 8 按一下**還原**以還原資料。

還原第一個節點時，災害復原系統會自動還原後續節點上的 Cisco Unified Communications Manager 資料庫 (CCMDB)。 視資料庫節點數目和大小而定，這可能需要數個小時。

資料便會還原至所有節點。

附註 在還原期間，請勿使用「Cisco Unified Communications Manager 管理」或「使用者選項」執行任何工作。

視您的資料庫大小和選擇還原的元件而定，系統可能需要幾小時還原。

步驟 9 還原流程完成後，請重新啓動伺服器。 如需關於如何重新啓動伺服器的相關資訊，請參閱「接下來該做的」一節。

附註 請務必重新啓動第一個節點，再重新啓動後續節點。

第一個節點重新啓動且執行還原版本的 Cisco Unified Communications Manager 後，請重新啓動後續節點。

步驟 10 複寫會在重新啓動叢集後自動設定。 請使用 “utils dbreplication runtimestate” CLI 命令來檢查所有節點的「複製狀態」值，如 *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* (Cisco Unified Communications 解決方案的命令行介面參考指南)所述。 每個節點的值應等於 2。

附註 重新啓動後續節點後，視叢集大小而定，可能需要足夠的時間來完成後續節點的資料庫複製。

提示 若複製未正確設定，請使用「utils dbreplication rebuild」CLI 命令，如 *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* (Cisco Unified Communications 解決方案的命令行介面參考指南)所述。

下一步

- （選用）若要檢視還原狀態，請參閱 檢查還原工作狀態 ，第 410 頁上的
- 若要重新啓動節點，請參閱 重新啓動節點 ，第 410 頁上的

將節點或叢集還原為上次已知之正確組態

請遵循此流程以將節點或叢集還原至上次的正確組態。

開始之前

- 請確保還原檔案包含主機名稱、IP 位址、DNS 組態，以及在備份檔案中設定的部署類型。
- 請確定安裝在伺服器的 Cisco Unified Communications Manager 版本符合您要還原的備份檔案的版本。
- 請確定此流程僅用於還原上次正確組態的節點。

程序

步驟 1 在災害復原系統中選擇**還原** > **還原精靈**。

步驟 2 在**選擇備份裝置**一區中選擇要還原的適當備份裝置。

步驟 3 按**下一步**。

步驟 4 在 **Restore Wizard Step 2 (還原精靈步驟 2)**視窗中選擇您要還原的備份檔案。

附註 備份檔案名稱指示系統建立備份檔案的日期和時間。

步驟 5 按**下一步**。

步驟 6 在 **Restore Wizard Step 3 (還原精靈步驟 3)**視窗中按一下**下一步**。

步驟 7 收到提示選擇還原節點時，請選擇適當的節點。
資料便會還原至選擇的節點。

步驟 8 重新啓動叢集中所有節點。 重新啓動第一個 Cisco Unified Communications Manager 節點，然後再重新啓動後續 Cisco Unified Communications Manager 節點。 若叢集也有 Cisco IM and Presence 節點，請重新啓動第一個 Cisco IM and Presence 節點，然後再重新啓動後續 IM and Presence 節點。 如需詳細資訊，請參閱「接下來該做的」一節。

重新啟動節點

還原資料後，您需重新啓動節點。

若要還原發佈者節點 (第一個節點)，您需先重新啓動發佈者節點。 請在重新啓動發佈者節點且成功執行還原的軟體版本後，再重新啓動訂閱者節點。

附註 若 CUCM 發布者節點爲離線，請勿重新啓動 IM and Presence 訂閱者節點。 在這種情況下，訂閱節點將無法啓動，因爲訂閱者節點無法連線至 CUCM 發布者。

注意 此程式會導致系統重新啓動及暫時暫停服務。

請在您需要重新啓動的每個叢集節點執行此流程。

程序

步驟 1 在 Cisco Unified 作業系統管理選擇**設定** > **版本**。

步驟 2 若要重新啓動節點，請按一下**重新啟動**。

步驟 3 複寫會在重新啓動叢集後自動設定。 請使用 **utils dbreplication runtimestate** CLI 命令檢查所有節點的「複製狀態」值。 每個節點上的值應等於 2。請參閱下方的「相關主題」部分，查找有關 CLI 指令的資訊。

若複製未正確設定，請使用 **utils dbreplication reset** CLI 命令，如 *Command Line Reference Guide for Cisco Unified Communications Solutions* (Cisco Unified Communications 解決方案的命令行參考指南)所述。 請參閱下方的「相關主題」部分，查找有關 CLI 指令的資訊。

附註 重新啓動後續節點後，視叢集大小而定，可能需要數小時來完成後續節點的資料庫複製。

下一步

(選用)若要檢視還原狀態，請參閱檢查還原工作狀態 ，第 410 頁上的。

相關主題

Cisco Unified Communications Manager (CallManager) 命令參考

檢查還原工作狀態

請遵循此流程以檢查還原工作狀態。

程序

步驟 1 在災害復原系統選擇**還原** > **目前狀態**。

步驟 2 在**還原狀態**視窗中，按一下記錄檔名稱連結以檢視還原狀態。

檢視還原記錄

執行下列步驟可檢視還原記錄。

程序

步驟 1 在災害復原系統選擇**還原** > **記錄**。

步驟 2 在**還原記錄**視窗中，您可以檢視已執行的還原，包括檔案名稱、備份裝置、完成日期、結果、版本、還原的功能和故障的功能。

還原記錄視窗只會顯示最近 20 個還原工作。

資料驗證

追蹤檔案

疑難排解期間或收集記錄時，會使用下列追蹤檔案位置。

Master Agent、GUI、各 Local Agent 和 JSch 程式庫的追蹤檔案會寫入下列位置：

- Master Agent 的追蹤檔案位於：platform/drf/trace/drfMA0*
- 各 Local Agent 的追蹤檔案位於：platform/drf/trace/drfLA0*
- GUI 的追蹤檔案位於：platform/drf/trace/drfConfLib0*
- JSch 的追蹤檔案位於：platform/drf/trace/drfJSch*

如需詳細資訊，請參閱 *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*（Cisco Unified Communications 解決方案的命令行介面參考指南）：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html。

命令行介面

災害復原系統還提供備份和還原功能子集的命令行存取，如下表所示。 如需這些命令和使用命令行介面的詳細資訊，請參閱 *Cisco Unified Communications* 解決方案命令行介面參考指南：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html。

表 *88:* 災害復原系統命令行介面

命令	描述
utils disaster_recovery estimate_tar_size	顯示 SFTP/本機裝置備份壓縮檔案的估計大小，並針對功能清單需求參數
utils disaster_recovery backup	使用災害復原系統介面中設定的功能開始手動備份
utils disaster_recovery jschLogs	啓用或停用 JSch 程式庫記錄
utils disaster_recovery restore	針對備份位置、檔案名稱、功能和要還原的節點開始還原及需求參數
utils disaster_recovery status	顯示正在進行的備份或還原工作的狀態
utils disaster_recovery show_backupfiles	顯示現有的備份檔案
utils disaster_recovery cancel_backup	取消正在進行的備份工作
utils disaster_recovery show_registration	顯示目前設定的註冊
utils disaster_recovery device add	新增網路裝置
utils disaster_recovery device delete	刪除裝置
utils disaster_recovery device list	列出所有裝置
utils disaster_recovery schedule add	新增排程
utils disaster_recovery schedule delete	刪除排程
utils disaster_recovery schedule disable	停用排程
utils disaster_recovery schedule enable	啓用排程
utils disaster_recovery schedule list	列出所有排程

命令	描述
utils disaster_recovery backup	使用災害復原系統介面中設定的功能開始手動備份。
utils disaster_recovery restore	針對備份位置、檔案名稱、功能和要還原的節點開始還原及需求參數。
utils disaster_recovery status	顯示正在進行的備份或還原工作的狀態。
utils disaster_recovery show_backupfiles	顯示現有的備份檔案。
utils disaster_recovery cancel_backup	取消正在進行的備份工作。
utils disaster_recovery show_registration	顯示目前設定的註冊。

警示和訊息

警示和訊息

災害復原系統會針對備份或還原程式期間可能發生的各種問題提供警示。 下表提供 Cisco 災害復原系統警示的清單。

表 *89:* 災害復原系統警示和訊息

警示名稱	描述	說明
DRFBackupDeviceError	DRF 備份程式在存取裝置時發生問題。	DRS 備份程式在存取裝置時
DRFBackupFailure	Cisco DRF 備份處理故障。	DRS 備份程式發生錯誤。
DRFBackupInProgress	其他備份仍在執行時，無法開始新的備份	其他備份仍在執行時，DRS 的備份。
DRFInternalProcessFailure	DRF 內部程式發生錯誤。	DRS 內部程式發生錯誤。
DRFLA2MAFailure	DRF Local Agent 無法連線至 Master Agent。	DRS Local Agent 無法連線 Agent。
DRFLocalAgentStartFailure	DRF Local Agent 未啟動。	DRS Local Agent 可能未啟
DRFMA2LAFailure	DRF Master Agent 未連線至 Local Agent。	DRS Master Agent 無法連線 Agent。
DRFMABackupComponentFailure	DRF 無法備份至少一個元件。	DRS 需求元件備份其資料 期間發生錯誤，而且未備份

警示名稱	描述	說明
DRFMABackupNodeDisconnect	備份中的節點在完全備份前就在Master Agent 中斷。	DRS Master Agent 在 Cisco Un Communications Manager 節點作業時，節點在備份作業完成
DRFMARestoreComponentFailure	DRF 無法還原至少一個元件。	DRS需求元件還原其資料；但期間發生錯誤，而且未還原元
DRFMARestoreNodeDisconnect	還原中的節點在完全還原前就在Master Agent 中斷。	DRS Master Agent 在 Cisco Un Communications Manager 節點作業時，節點在還原作業完成
DRFMasterAgentStartFailure	DRF Master Agent 未啓動。	DRS Master Agent 可能未啓動
DRFNoRegisteredComponent	沒有可用的已註冊元件，因此備份故障。	因爲沒有可用的已註冊元件，備份故障。
DRFNoRegisteredFeature	未針對備份選取功能。	未針對備份選取功能。
DRFRestoreDeviceError	DRF 還原程式在存取裝置時發生問題。	無法在裝置讀取 DRS 還原程式
DRFRestoreFailure	DRF 還原程式故障。	DRS 還原程式發生錯誤。
DRFSftpFailure	DRF SFTP 作業發生錯誤。	DRS SFTP 作業中有錯誤。
DRFSecurityViolation	DRF 系統偵測至可能導致安全性危害的惡意型樣。	DRF 網路訊息包含可能導致安的惡意型樣，例如程式碼注入越。 DRF 網路訊息遭到封鎖。
DRFTruststoreMissing	節點缺少 IPSec 信任存放區。	節點缺少 IPSec 信任存放區。 I Agent 無法連線至 Master Ager
DRFUnknownClient	Pub 上的 DRF Master Agent 在叢集外的不明伺服器收到使用者端連線需求。 需求遭拒。	Pub 上的 DRF Master Agent 在不明伺服器收到使用者端連線求遭拒。
DRFBackupCompleted	DRF 備份成功完成。	DRF 備份成功完成。
DRFRestoreCompleted	DRF 還原成功完成。	DRF 還原成功完成。
DRFNoBackupTaken	DRF 在目前的系統上找不到有效備份。	DRF 在升級/移轉或新安裝後的系統上找不到有效備份。
DRFComponentRegistered	DRF 成功註冊需求的元件。	DRF 成功註冊需求的元件。
DRFRegistrationFailure	DRF 註冊作業故障。	因爲某些內部錯誤，元件的 D 作業故障。
DRFComponentDeRegistered	DRF 成功取消註冊需求的元件。	DRF 成功取消註冊需求的元件
DRFDeRegistrationFailure	元件的 DRF 取消註冊需求故障。	元件的 DRF 取消註冊需求故障

警示名稱	描述	說明
DRFFailure	DRF 備份或還原程式故障。	DRF 備份或還原程式發生錯
DRFRestoreInternalError	DRF 還原作業發生錯誤。 已內部取消還原。	DRF 還原作業發生錯誤。 還原。
DRFLogDirAccessFailure	DRF 無法存取記錄檔目錄。	DRF 無法存取記錄檔目錄
DRFDeRegisteredServer	DRF 已爲伺服器自動取消註冊所有元件。	伺服器可能已與Unified Co Manager 叢集斷開連線。
DRFSchedulerDisabled	DRF 排程工具停用，因爲沒有可用於備份的已設定功能。	DRF 排程工具停用，因爲沒 份的已設定功能
DRFSchedulerUpdated	DRF 排程備份組態已因爲功能取消註冊而自動更新。	DRF 排程備份組態已因爲功 而自動更新

授權預訂

授權預訂

重要須知 在 Unified CM 14SU1 版本之前支援以下授權功能表格。

在該份已啓用指定授權預訂或的 Unified Communications Manager 上執行還原操作之後，請執行以下步驟。

表 *90:* 災難復原系統，用於授權預訂

還原後之狀態	**CSSM** 上之產品	解決方法
未註冊	是	聯繫 Cisco 以從 CSSM 移除產品並在產品中註冊
	否	無需採取任何行動

還原後之狀態	CSSM 上之產品	解決方法
進行中的預訂	是	執行以下任一程序： 流程-1: 1. 從 CSSM 獲取產品的授權代碼。 2. 輸入授權代碼 **license smart reservation return-authorization "<authorization-code>"** 以執行下列的 CLI。 流程-2: 1. 聯繫 Cisco 以從 CSSM 移除產品
	否	從產品執行 **license smart reservation cancel** CLI
已註冊	是	1. 在產品中執行以下 **license smart reservation return**CLI。 預訂返回碼將印在主控台上。 2. 在 CSSM 上輸入預訂返回碼以移除產品。
	否	從產品執行 **license smart reservation return** CLI

還原互動和限制

還原限制

下列限制適用於使用災害復原系統還原 Cisco Unified Communications Manager 或 IM and Presence Service

表 *91:* 還原限制

限制	描述
匯出限制	您僅可從限制版本將 DRS 備份還原至限制版本，不受限制的版本備份僅可還原至不受限制的版本。 請注意，若您升級爲美國出口限制版本的Cisco Unified Communications Manager，您便無法在之後升級或執行此軟體的美國出口限制版本全新安裝。

限制	描述
平台移轉	您無法使用災害復原系統在平台之間移轉資料 (例如，在 Windows 移轉至 Linux，或在 Linux 移轉至 Windows)。 還原必須以備份執行相同產品版本。 如需有關在 Windows 平台至 Linux 平台的資料移轉的資訊，請參閱 *Data Migration Assistant User Guide* (資料移轉助理使用者指南)。
HW 取代和移轉	執行 DRS 還原以將資料移轉至新伺服器時，您需將舊伺服器使用的相同 IP 位址和主機名稱指派至新伺服器。 此外，若執行備份時設定 DNS，則需在執行還原前具有相同 DNS 組態。 如需取代伺服器的詳細資訊，請參閱 *Replacing a Single Server or Cluster for Cisco Unified Communications Manager guide* (取代 Cisco Unified Communications Manager 的單一伺服器或叢集指南)。 此外，硬體更換後，您需執行憑證信任清單 (CTL) 用戶端。 若未還原後續節點(訂閱者)伺服器，則您需執行CTL使用者端。在其他情況下，DRS會備份您需要的憑證。 如需更多資訊，請參閱《*Cisco Unified Communications Manager* 安全指南》中的“安安裝 CTL 用戶端”和“設定 CTL 用戶端”流程。
跨叢集 Extension Mobility	在備份時登入至遠端叢集的跨叢集的Extension Mobility使用者應在還原後持續登入。

附註 DRS 備份/還原爲高度基於 CPU 的流程。 Smart License Manager 是備份和還原的組件之一。 在此流程中，將重新啓動 Smart License Manger 服務， 您可期望較高的資源利用率，因此建議您在維護期間安排該流程。

成功還原 Cisco Unified Communications 伺服器元件後，請使用 Cisco Smart Software Manager 或 Cisco Smart Software Manager 衛星註冊 Cisco Unified Communications Manager 。 若產品在執行備份前已註冊，請註冊該產品以更新授權資訊。

如需有關如何以 Cisco Smart Software Manager 或 Cisco Smart Software Manager satellite 註冊產品，請參閱適用您版本的 *Cisco Unified Communications Manager* 系統組態指南。

疑難排解

DRS 還原至較小的虛擬機器失敗

問題

若將 IM and Presence Service 節點還原至具有較小硬碟的 VM，資料庫還原可能會故障。

原因

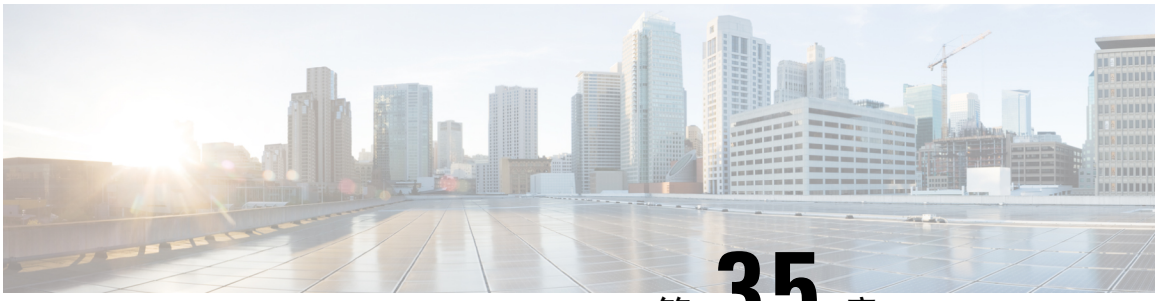
在較大硬碟移轉至較小硬碟時，會發生此故障狀況。

解決方法

在具有 2 部虛擬硬碟的 OVA 範本針對還原部署 VM。

第 IX 部分

疑難排解



第 35 章

疑難排解概覽

本節提供了必要的背景資訊和可用資源來對Unified Communications Manager進行疑難排解。

Cisco Unified Serviceability

Cisco Unified Serviceability爲 Web 型的疑難排解工具，用於Unified Communications Manager，提供下述的功能協助管理員解決系統問題：

- 儲存用於疑難排解的Unified Communications Manager服務警報及事件，提供警報訊息定義；
- 儲存Unified Communications Manager服務追蹤資訊到不同的記錄檔，以用於疑難排解； 系統管理員可以配置、收集和檢視追蹤資訊；
- 透過 Unified 即時監控工具 (RTMT) 監控Unified Communications Manager叢集中元件的即時行爲；
- 透過 Cisco Unified Communications Manager CDR 分析和回報產生服務品質、流量和計費資訊的報告；
- 提供您可以透過「啓動服務」視窗啓動、停止及檢視的功能服務。
- 提供用於啓動及停止功能與網路服務的介面。
- 存檔與以下內容相關的報告Cisco Unified Serviceability工具；
- 讓 Unified Communications Manager 可作爲簡單網路管理通訊協定 (SNMP) 遠端管理和疑難排解的管理裝置使用；
- 監控節點（或叢集中的所有節點）上記錄檔分區的硬碟使用量。

在導航下拉式清單方塊中選擇Cisco Unified Serviceability以在Cisco Unified Communications Manager管理視窗中存取Cisco Unified Serviceability。 安裝Unified Communications Manager軟體時亦會自動安裝Cisco Unified Serviceability，兩者將皆可使用。

請參閱*Cisco Unified Serviceability*管理指南有關 Serviceability 工具的詳細資料和配置流程。

Cisco Unified Communications 作業系統管理

您可使用*Cisco Unified Communications* 作業系統管理執行下列的任務配置及管理您的*Cisco Unified Communications* 作業系統：

- 檢查軟體和硬體狀態。
- 檢查及更新 IP 位址。
- 對其他網路裝置進行 ping。
- 管理網路時間通訊協定 (NTP) 伺服器。
- 升級系統軟體和選項。
- 重新啓動系統。

有關Serviceability工具的詳細資訊和配置流程請參閱Cisco Unified Communications Manager 管理指南。

解決問題的通用模型

對電話或 IP 網路環境進行疑難排解時，請定義特定的症狀，識別可能導致該症狀的所有潛在問題，然後有系統地消除每個潛在問題（從最可能到最不可能），直到症狀消失。

以下步驟提供了在問題解決流程中使用的準則。

流程

1. 分析網路問題並創建明確的問題描述。 定義症狀和潛在起因。
2. 收集需要幫助釐清可能原因的證據。
3. 根據您所收集到的證據考慮可能的起因。
4. 根據這些起因創建一個行動計劃。 從最可能出現的問題開始，並設計一個僅操作一個變數的計劃。
5. 實施行動計劃；測試時請仔細執行每個步驟，以檢視症狀是否消失。
6. 分析結果以確定問題是否已解決。 若問題已解決，該流程應視爲已完成。
7. 若問題仍未解決，請根據清單上的第二個最可能的起因創建一個行動計劃。 返回4 ，第 422 頁上的並重複該流程，直到問題解決。

確保有撤消在實施行動計劃時所做的任何更改。 請記得您一次僅想更改一個變數。

附註 若您用盡了所有常見的原因和措施（本說明文件中概述的原因和環境中發現的其他原因和措施），請與 Cisco TAC 聯繫。

網路故障準備

若您提前做好準備則始終可以更輕鬆地從網路故障中恢復。 要確定您是否爲網路故障做好了準備，請回答以下問題：

- 您是否有貴組織互連網路精確的實際邏輯位置圖？位置圖概括顯示了網路上所有裝置的實際位置及其所連線的方式。是否也有網路位址、網路號碼和子網路的邏輯位置圖？
- 您是否有實施於貴組織網路中的每一種通訊協定的清單？是否有與之關聯的網路號碼、子網路，區域的清單？
- 您是否知道要路由哪些協定以及各個協定的最新正確組態資訊？
- 您知道哪些協定正在被橋接嗎？ 這些橋接中是否配置了任何過濾器，您是否有這些配置的副本？ 可套用於Unified Communications Manager嗎？
- 您是否知道與外部網路的所有聯繫點，包括與 Internet 的任何連線？ 您知道各個外部網路連線是使用何種路由協定嗎？
- 貴組織是否已記錄了正常的網路表現和性能，因此可以將當前問題與基準進行比較？

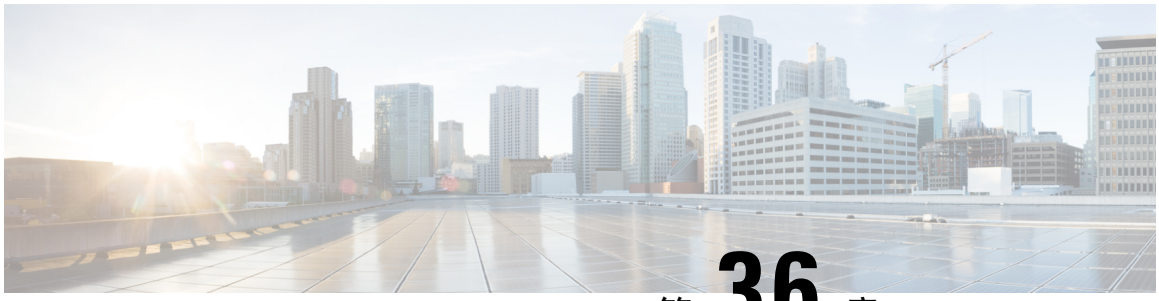
若您對這些問題的回答爲“是”，則可以更快地自故障中恢復。

何處有更多的資訊

使用以下的連結可獲取有關各種 IP 電話主題的資訊：

- 更多有關 Cisco IP 電話應用程式和產品的資訊請參閱《*Cisco Unified Communications Manager* 說明文件指南》。 以下 URL 顯示了說明文件指南路徑的範例：

  https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html
- 有關與 Cisco Unity 相關的說明文件，請參閱以下 URL：
  https://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html
- 有關Cisco Emergency Responder的檔案請參閱以下網址：
  https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html
- 有關Cisco Unified IP 電話的檔案請參閱以下網址：
  https://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html
- 有關設計和排除 IP 電話網路故障的資訊，請參閱《Cisco IP 電話解決方案參考網路設計指南》：
  https://www.cisco.com/go/srnd



第 36 章

疑難排解工具

本節介紹用於配置、監控和疑難排解Unified Communications Manager的工具和公用程式並提供了收集資訊的一般準則，以避免重複測試和重新收集相同的資料。

附註 要存取本檔案中所列出的某些 URL 站點，您需爲註冊使用者並登錄。

Cisco Unified Serviceability 疑難排解工具

有關Cisco Unified Serviceability所提供以監控和分析各種Unified Communications Manager系統的不同類型工具的詳細資訊請參閱*Cisco Unified Serviceability* 管理指南。

表 *92: Serviceability* 工具

條件	定義
Cisco Unified 即時監控工具 (RTMT)	此工具提供有關Unified Communications Manager裝置和性能計數器的即時資訊，並使您能夠收集追蹤資訊。 性能計數器可爲專屬於系統的，也可爲專屬於Unified Communications Manager的。 對象包含針對特定裝置或功能（例如Cisco Unified IP 電話或Unified Communications Manager系統性能）的類似計數器的邏輯分區。 計數器測量系統性能的各個方面。 計數器測量統計資訊，例如已註冊電話的數目、嘗試的通話和正在進行的通話。
警報	管理員使用警報來取得運作狀態和 Unified Communications Manager 系統狀態。 警報包含有關系統問題的資訊，例如解釋和建議的操作。 系統管理員會在警報定義視窗中搜尋警報資訊。 警報定義包含警報的描述和建議的操作。
追蹤	系統管理員和Cisco工程師使用追蹤檔案取得有關Unified Communications Manager服務方面的問題的特定資訊。Cisco Unified Serviceability將配置的追蹤資訊傳送至追蹤記錄檔。 存在兩種類型的追蹤記錄檔案：SDI 和 SDL。 每個服務皆包含一個預設的追蹤記錄檔案。 系統追蹤來自服務的系統診斷介面（SDI）資訊、記錄 runtime 事件並追蹤到記錄檔案。 SDL 追蹤記錄檔案包含來自伺服的通話處理資訊，例如Cisco CallManager和Cisco CTIManager。 系統追蹤通話的信號分佈層（SDL），並將狀態轉換記錄到記錄檔案中。 **附註** 在大多數情況下，僅在 Cisco 技術支援中心（TAC）要求您收集 SDL 追蹤時您才收集。
品質回報工具	此術語是表示Cisco Unified Serviceability中的語音品質和一般問題報告公用程式。
Serviceability Connector	Cisco Webex Serviceability 服務加快了 Cisco 技術支援人員診斷基礎架構問題的速度， 系統會自動執行查找、擷取診斷記錄和資訊，並將其儲存到 SR 個案。 該服務亦會觸發診斷簽署的分析，以便 TAC 可以更有效地識別和解決本地裝置的問題。

命令行介面

使用命令行介面（CLI）存取Unified Communications Manager系統進行基本維護和故障恢復。 透過硬接線終端（系統監視器和鍵盤）或執行 SSH 作業期間來存取系統。

帳號名稱和密碼在安裝時創建。 您可以在安裝後更改密碼，但您永遠無法更改帳號名稱。

命令代表會導致系統執行某些功能的文字命令。 命令可以爲獨立的，也可以具有必需或可選的參數或選項。

一個級別爲命令的集合的概括；例如，show 指定一個級別，而 show status 指定一個命令。 每個級別和命令還包括一個關聯的特權級別。 僅當您具有足夠的特權級別時，才可以執行命令。

如需Unified Communications Manager CLI 檔案命令組的更多資訊請參閱 *Cisco Unified Solutions* 命令行介面參考指南。

Kerneldump 公用程式

Kerneldump 公用程式使您可以在受影響的電腦上本地收集故障轉儲記錄檔，而無需輔助伺服器。

在一個Unified Communications Manager叢集，您僅需要確保在伺服器上啓用了 kerneldump 公用程式，即可收集故障轉儲資訊。

附註 Cisco建議您在安裝後驗證 kerneldump 公用程式是否已啓用Unified Communications Manager以便進行更有效的疑難排解。 若您尚未這樣做，請先啓用 kerneldump 公用程式，然後再從受支援的裝置版本升級Unified Communications Manager。

重要須知 啓用或停用 kerneldump 公用程式需將節點重新啓動。 除非您位於可將結點重新啓動的視窗中，否則請不要執行 enable 命令。

Cisco Unified Communications 作業系統的指令行介面（CLI）可用於啓用、停用或檢查 kerneldump 公用程式的狀態。

使用以下流程來啓用核心轉儲公用程式：

使用公用程式收集的檔案

要檢視 kerneldump 公用程式崩潰資訊請使用*Cisco Unified RTMT*或命令行介面（CLI）。 要使用*Cisco Unified RTMT*收集 kerneldump 記錄檔，請在“追蹤和記錄中心”中選擇“收集檔案”選項。 在“選擇系統服務/應用程式”索引標籤中，選擇“Kerneldump 記錄檔”方塊。 如需如何在*Cisco Unified RTMT* 存取所收集記錄檔的相關資料，請參閱 *Cisco Unified* 即時監控工具管理指南。

要使用 CLI 收集 kerneldump 記錄檔，請使用“檔案”崩潰目錄中檔案上的 CLI 命令， 位於“activelog”分區中。 記錄檔檔案名稱開頭爲 kerneldump 用戶端的 IP 位址然後以檔案創建的日期爲結尾。 如需 CLI 檔案命令的更多資訊請參閱 *Cisco Unified Solutions* 命令行介面參考指南。

啟用 Kerneldump 公用程式

使用此流程啓用 kerneldump 公用程式。 萬一發生核心崩潰，該公用程式提供了一種收集和轉儲崩潰的機制。 您可以將公用程式配置爲將記錄檔轉儲到本地伺服器或外部伺服器。

程序

步驟 1 登入命令行介面。

步驟 2 完成以下的任一操作：

- 如要在本地伺服器上轉儲核心崩潰，請執行 `utils os kerneldump enable` CLI 指令。
- 要將核心崩潰傾印到外部伺服器，請執行 `utils os kerneldump ssh enable <ip_address>` CLI 指令再加上外部伺服器的 IP 位址。

步驟 3 重新啓動伺服器。

範例

附註 若您需要停用 kerneldump 公用程式，則可以執行 `utils os kernelcrash disable` CLI 指令以停用本地伺服器進行核心傾印，以及 `utils os kerneldump ssh disable <ip_address>` CLI 指令以在外部伺服器上停用該公用程式。

下一步

在 RTMT 中配置電子郵件警報以通知核心轉儲發生時機。 如需詳細資訊，請參閱 啓用核心轉儲的電子郵件警示 ，第 258 頁上的

有關 kerneldump 公用程式和疑難排解的更多資訊請參閱*Cisco Unified Communications Manager* 疑難排解指南。

啟用核心轉儲的電子郵件警示

使用此流程可配置 RTMT 以在發生核心轉儲時傳送電子郵件給管理員。

程序

步驟 1 選擇**系統** > **工具** > **警示** > **警示中心**。

步驟 2 在 **CoreDumpFileFound** 警示上按一下滑鼠右鍵，然後選擇**設定警示內容**。

步驟 3 按照精靈提示設定您的偏好準則：

a) 在**警示內容：電子郵件通知**快顯視窗中，確定已勾選**啟用電子郵件**，然後按一下**設定** 以設定預設警示動作，動作即爲寄送電子郵件給管理員。

b) 按照提示進行，然後**新增**收件人電子郵件地址。 觸發此警示時，預設動作是透過電子郵件寄送到此地址。

c) 按一下**儲存**。

步驟 4 設定預設電子郵件伺服器：

a) 選擇**系統** > **工具** > **警示** > **設定電子郵件伺服器**。
b) 輸入電子郵件伺服器和連接埠資訊，以傳送電子郵件警示。
c) 輸入**傳送使用者 ID**。
d) 點擊**確定**。

網路管理

使用網路管理工具來實現 Unified Communications Manager 的遠端 Serviceability。

- 系統記錄檔管理
- Cisco Discovery Protocol 支援
- 簡易網路管理通訊協定支援

更多資訊請參閱各網路管理工具的各節中所提供的 URL 上的說明文件。

系統記錄檔管理

儘管它可以調整以於其他網路管理系統使用，但與資源管理器必備軟體（RME）綑在一起的 Cisco Syslog Analysis 提供了管理 Cisco 裝置的 Syslog 訊息的最佳方法。

Cisco Syslog Analyzer 充當 Cisco Syslog Analysis 可爲多個應用程式提供通用的儲存和系統記錄檔分析的組件。 另一個主要組件 Syslog Analyzer Collector 則自Unified Communications Manager伺服器收集記錄檔訊息。

這兩個Cisco應用程式一起運作以爲Cisco Unified Communications Solutions 提供集中式系統記錄檔記錄服務。

請至此 URL 參閱 RME 說明檔案：
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Cisco Discovery Protocol 支援

Cisco Discovery Protocol 支援可發現 Unified Communications Manager的伺服器及管理這些伺服器。

請至此 URL 參閱 RME 說明檔案：
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

簡易網路管理通訊協定支援

網路管理系統（NMS）使用 SNMP（產業標準的介面）在網路裝置之間交換管理資訊。 SNMP 爲 TCP/IP 通訊協定的其中一部分，可讓管理員遠端管理網路效能、尋找及解決網路問題，及計畫未來的網路成長。

SNMP 管理的網路包括三個關鍵元件：受管理裝置、代理和網路管理系統。

- 受管理裝置：指定含有 SNMP 代理並位於受管理網路上的網路節點。 受管理裝置會收集並儲存管理資訊，並透過使用 SNMP 使其可用。
- 代理：位於受管理裝置的網路管理軟體。代理包含管理資訊的本機知識，並將其轉換爲與SNMP相容的形式。
- 網路管理系統（NMS）包括 SNMP 管理應用程式及執行該應用程式的電腦。 NMS 執行監控和控制受管理裝置的應用程式。 NMS 提供了網路管理所需的大量處理和內存資源。 以下網管與以下網管共用相容性Unified Communications Manager：
  - CiscoWorks 共同服務軟體
  - HP OpenView
  - 支援 SNMP 和 Unified Communications ManagerSNMP 介面的第三方應用程式

Sniffer追蹤

通常您可以透過在配置爲跨越包含故障資訊的一個或多個VLAN（CatOS，Cat6K-IOS，XL-IOS）的Catalyst連接埠上連線便攜式電腦或其他配備Sniffer的裝置來收集Sniffer追蹤。 若沒有可用的連接埠，請在交換機和裝置之間插入的集線器上將配備Sniffer的裝置連線。

提示 爲了幫助 TAC 工程師讀取和解釋追蹤，Cisco建議使用 Sniffer Pro 軟體，因爲該軟體在 TAC 中被廣泛使用。

有可用的所有相關裝置的 IP / MAC 位址，例如 IP 電話，閘道，Unified Communications Manager s，依此類推。

除錯

來自**除錯**的輸出具權限 EXEC 命令可提供有關各種與協定狀態和網路活動相關的互通網路事件的診斷資訊。

設定終端模擬器軟體（例如 HyperTerminal），以便它可以將除錯輸出擷取至檔案中。 在超級終端中，點按**轉移**，然後再點按**擷取文字**並選擇適當的選項。

在執行任何 IOS 語音閘道除錯之前，請確認在閘道上已全局配置 **servicetimestampsdebugdatetimemsec**。

附註 避免在工作時間內在現場環境中收集除錯資訊。

最好在非工作時間收集除錯資訊。 若需在即時環境中收集除錯，請輸入**no logging console**和**loggingbuffered**。 請輸入**show log**收集除錯。

由於某些除錯可能會較長，故請直接在主控台通訊埠上收集（預設的**記錄主控台**）或緩衝區（**記錄緩衝區**）。 透過 Telnet 作業期間收集除錯可能會影響裝置性能，結果可能是除錯不完整，您將需再重新收集。

要停止除錯，請輸入**no debug all**或**undebug all**命令。 使用**show debug**命令確定除錯已關閉。

Cisco Secure Telnet

*Cisco Secure Telnet*允許Cisco 服務工程師（CSE）可直接穿過防火牆存取您網站上的Unified Communications Manager節點。 *Cisco Secure Telnet*使用增強的加密使得 Cisco Systems 的特殊 Telnet 用戶端可連線至防火牆後的 Telnet 守護程式， 安全的連線可以對您的Unified Communications Manager節點進行遠端監控和疑難排解，無需修改防火牆。

附註 Cisco僅在您授權的情況下提供此服務。 您需確保您站點上的網路管理員可用，以幫助啓動該流程。

封包擷取

本節包含有關封包截獲的資訊。

相關主題

封包截獲概覽 ，第 431 頁上的
封包截獲的配置清單 ，第 432 頁上的
將一般使用者新增至標準封包Sniffer存取控制群組 ，第 432 頁上的
配置封包截獲服務參數 ，第 433 頁上的
在“電話組態”視窗中配置封包截獲 ，第 433 頁上的
在閘道和trunk組態視窗中配置封包截獲 ，第 434 頁上的
封包截獲組態設定 ，第 436 頁上的
分析截獲的封包 ，第 436 頁上的

封包截獲概覽

由於啓用加密後，偵測媒體和 TCP 封包的第三方疑難排解工具無法正常工作，因此需使用Unified Communications Manager發生問題時執行以下任務：

- 分析封包中的訊息之間的交換Unified Communications Manager和裝置[Cisco Unified IP 電話（SIP 和 SCCP），Cisco IOS MGCP 閘道，H.323 閘道，H.323 / H.245 / H.225 trunk或 SIP trunk]。
- 在裝置之間擷取安全即時協定（SRTP）封包。
- 從訊息中擷取媒體加密密鑰內容，並在裝置之間解密媒體。

提示 同時對多個裝置執行此任務可能會導致較高的 CPU 使用率和通話處理中斷。 Cisco 強烈建議您在盡量減少通話處理中斷的情況下執行此任務。

如需更多資訊，請參閱Cisco Unified Communications Manager 安全性指南。

封包截獲的配置清單

擷取和分析相關的資料包括執行下列的任務。

流程

1. 將一般使用者新增至“標準封包Sniffer使用者”群組。
2. 在“服務參數組態”視窗中配置封包截獲服務參數Cisco Unified Communications Manager 管理；例如，配置“封包截獲啓用”服務參數。
3. 在“電話”或“閘道或trunk組態”視窗中，依各個裝置配置封包截獲設定。

附註 Cisco 強烈建議您不要同時爲多個裝置啓用封包截獲，因爲此任務可能會導致網路中的 CPU 使用率過高。

4. 在您聯絡 TAC 之前，需在受影響的裝置之間使用Sniffer追蹤來擷取 SRTP 封包。 請參閱支援Sniffer追蹤工具的說明文件。
5. 截獲封包後，將“封包截獲啓用”服務參數設定爲 False。
6. 收集分析封包所需的檔案。
7. Cisco技術支援中心（TAC）將會分析封包。 直接聯繫 TAC 以執行此任務。

相關主題

將一般使用者新增至標準封包Sniffer存取控制群組 ，第 432 頁上的
分析截獲的封包 ，第 436 頁上的
在閘道和trunk組態視窗中配置封包截獲 ，第 434 頁上的
在“電話組態”視窗中配置封包截獲 ，第 433 頁上的
配置封包截獲服務參數 ，第 433 頁上的
封包截獲組態設定 ，第 436 頁上的

將一般使用者新增至標準封包Sniffer存取控制群組

屬於標準封包Sniffer存取控制群組的一般使用者可以爲支援封包截獲的裝置配置“封包截獲模式”和“封包截獲持續時間”設定。 若使用者不存在於標準封包Sniffer存取控制群組中，則該使用者無法啓動封包截獲。

以下流程描述了如何將一般使用者新增至標準封包Sniffer存取控制群組，並假定您已在Cisco Unified Communications Manager 管理中配置了一般使用者，如Cisco Unified Communications Manager 管理指南中所述。

流程

1. 如Cisco Unified Communications Manager 管理指南中所述，先找到存取控制群組。
2. “尋找/列出”視窗顯示後，點按**標準封包Sniffer使用者**連結。
3. 按一下**將使用者新增至群組**按鈕。
4. 新增一般使用者，如Cisco Unified Communications Manager 管理指南中所述。
5. 新增使用者後，點按**儲存**。

配置封包截獲服務參數

若要配置封包截獲的參數請執行以下流程：

流程

1. 在 Unified Communications Manager中，選擇 **系統** > **企業參數**。
2. 在伺服器下拉式清單方塊中，選擇您之前啓動 Cisco CallManager 服務的在線伺服器。
3. 在服務下拉式清單方塊中選擇 **Cisco Call Manager**（活躍）服務。
4. 捲動至“TLS 封包截獲配置”窗格，然後配置封包截獲設定。

提示 有關服務參數的資訊，請點按參數名稱或顯示在視窗中的問號。

附註 若要封包截獲有進行，需將“封包截獲啓用”服務參數設定爲“True”。

5. 按一下**儲存**使變更生效。
6. 您可以繼續配置封包截獲。

相關主題

在閘道和trunk組態視窗中配置封包截獲 ，第 434 頁上的
在“電話組態”視窗中配置封包截獲 ，第 433 頁上的

在“電話組態”視窗中配置封包截獲

在“服務參數”視窗中啓用封包截獲後，可在 Cisco Unified Communications Manager 管理視窗中爲每一個裝置“電話配置”配置封包截獲。

您可以按電話啓用或停用封包截獲。 封包截獲的預設設定爲“無”。

注意 Cisco 強烈建議您不要同時啓用多個電話的封包截獲，因爲此任務可能會導致網路中的 CPU 使用率過高。

若您不想截獲封包或完成任務，請將“封包截獲啓用”服務參數設定爲 False。

要配置電話的封包截獲請執行以下流程：

流程

1. 在配置封包截獲設定之前，請參閱與封包截獲配置相關的主題。
2. 如Cisco Unified Communications Manager 系統組態設定指南中所述找到 SIP 或 SCCP 電話。
3. “電話組態”視窗顯示時，參考封包截獲配置設定以配置疑難排解設定。
4. 完成配置後點擊**儲存**。
5. 在重設對話方塊中，按一下**確定**。

提示 雖然Cisco Unified Communications Manager 管理會提示您重設裝置，您無需重設裝置以截獲封包。

附加步驟

在您聯絡 TAC 之前，需在受影響的裝置之間使用Sniffer追蹤來擷取 SRTP 封包。

截獲封包後，將“封包截獲啓用”服務參數設定爲 False。

相關主題

分析截獲的封包 ，第 436 頁上的
封包截獲的配置清單 ，第 432 頁上的

在閘道和trunk組態視窗中配置封包截獲

以下閘道和 trunk 支援Unified Communications Manager中的封包截獲。

- Cisco IOS MGCP 閘道
- H.323 閘道
- H.323 / H.245 / H.225 trunk
- SIP 中繼線

提示 Cisco 強烈建議您不要同時爲多個裝置啓用封包截獲，因爲此任務可能會導致網路中的 CPU 使用率過高。

若您不想截獲封包或完成任務，請將“封包截獲啓用”服務參數設定爲 False。

要在“閘道或trunk組態”視窗中配置封包截獲設定，請執行以下流程：

流程

1. 在配置封包截獲設定之前，請參閱與封包截獲配置相關的主題。
2. 您可以執行下列一項作業：
   - 如Cisco Unified Communications Manager 系統組態設定指南中所述，找到 Cisco IOS MGCP 閘道。
   - 如Cisco Unified Communications Manager 系統組態設定指南中所述，找到 H.323 閘道。
   - 如Cisco Unified Communications Manager 系統組態設定指南中所述，找到 H.323 / H.245 / H.225 trunk。
   - 如Cisco Unified Communications Manager 系統組態設定指南中所述，找到 SIP trunk。
3. 組態視窗顯示時找到“封包截獲模式”和“封包截獲持續時間”設定。

提示 若您找到了 Cisco IOS MGCP 閘道，請確保已爲 Cisco IOS MGCP 閘道配置了通訊埠，如Cisco Unified Communications Manager 管理指南中所述。 Cisco IOS MGCP 閘道的封包截獲設定是顯示於端點標識符的“閘道組態”視窗中。 要存取此視窗，請點按語音介面卡的端點標識符。

4. 配置疑難解答設定，如中所述封包截獲配置設定。
5. 配置封包截獲設定後，點按**儲存**。
6. 在重設對話方塊中，按一下**確定**。

提示 雖然Cisco Unified Communications Manager 管理會提示您重設裝置，您無需重設裝置以截獲封包。

附加步驟

在您聯絡 TAC 之前，需在受影響的裝置之間使用Sniffer追蹤來擷取 SRTP 封包。

截獲封包後，將“封包截獲啓用”服務參數設定爲 False。

相關主題

分析截獲的封包 ，第 436 頁上的
封包截獲的配置清單 ，第 432 頁上的

封包截獲組態設定

下表描述了爲閘道、trunk和電話配置封包截獲時的“封包截獲模式”和“封包截獲持續期間”設定。

設定	描述
封包擷取模式	此設定是專爲加密的疑難排解而存在；封包擷取可能會導致 CPU 使用量過高或通話處理中斷。 請從此下拉式清單方塊中，選擇下列其中一個選項： • **無**—這個選項爲預設設定，表示不會進行任何封包截獲。 完成封包截獲後，Unified Communications Manager將“封包截獲模式”設定爲“無”。 • **批次處理模式**—Unified Communications Manager會將已解密或未加密的訊息寫入檔案中，然後系統會加密每個檔案。 系統每天都會以新的加密金鑰建立新的檔案。 Unified Communications Manager，可將檔案儲存七天，也會將加密檔案的金鑰儲存在安全的位置。Unified Communications Manager 將檔案儲存在 PktCap 虛擬目錄中。 單一檔案包含時間戳記、來源 IP 位址、來源 IP 通訊埠、目的地 IP 位址、封包通訊協定、訊息長度和訊息。 TAC 除錯工具會使用 HTTPS、管理員使用者名稱與密碼和指定的日期來要求包含擷取封包的單一加密檔案。 同樣地，此工具也會要求金鑰資訊來爲加密檔案解密。 **提示** 在您聯絡 TAC 之前，需在受影響的裝置之間使用 Sniffer 追蹤來擷取 SRTP 封包。
封包擷取持續時間	此設定是專爲加密的疑難排解而存在；封包擷取可能會導致 CPU 使用量過高或通話處理中斷。 此欄位會指定分配給一個封包擷取作業階段的分鐘數上限。 預設設定等於 0，但是範圍是從 0 到 300 分鐘。 若要起始封包擷取，請在此欄位中輸入 0 以外的值。 在封包擷取完成後，將會出現 0 的值。

相關主題

在閘道和trunk組態視窗中配置封包截獲 ，第 434 頁上的
在“電話組態”視窗中配置封包截獲 ，第 433 頁上的

分析截獲的封包

*Cisco*技術支援中心（TAC）使用除錯工具分析封包。 在您聯絡 TAC 之前，需在受影響的裝置之間使用Sniffer追蹤來擷取 SRTP 封包。 收集以下資訊後，請直接與 TAC 聯繫：

- 封包擷取檔— **https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**，您可以在其中瀏覽伺服器並按月份、日期和年份（mm-dd-yyyy）找到封包擷取檔

- 檔案金鑰— **https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**，您可以在其中瀏覽伺服器並按月份、日期和年份（mm-dd-yyyy）找到金鑰
- “標準封包Sniffer使用者群組“中一般使用者的使用者名稱和密碼

如需更多資訊，請參閱Cisco Unified Communications Manager 安全性指南。

常見的疑難排解任務、工具和命令

本節提供了有關命令和公用程式的快速參考以協助您對Unified Communications Manager停用 root 存取權限的伺服器進行疑難排解。 下表提供了 CLI 命令和 GUI 選擇的摘要，可用於收集資訊以解決各種系統問題。

表 *93: CLI* 命令和 *GUI* 選擇的摘要

資訊	Linux 命令	Serviceability GUI 工具	CLI 命令
CPU 用量	上	RTMT 移至檢視標籤然後選擇**伺服器** > **CPU 和記憶體**	處理器 CPU 使用率： 顯示效能查詢級別處理器 所有流程的流程 CPU 使用率： 顯示效能查詢計數器進程“% CPU 時間” 各個流程計數器的詳細資訊（包括 CPU 使用率） 顯示性能查詢實例<Process task_name>
流程狀態	ps	RTMT 移至檢視標籤，然後選擇**伺服器** > **流程**	show perf query counter Process “Process Status”
硬碟使用量	Df / du	RTMT 移至檢視標籤，然後選擇**伺服器** > **硬碟使用量**	顯示效能查詢計數器分區“已用的 %” 或顯示性能查詢類分區
記憶體	可用	RTMT 移至檢視標籤然後選擇**伺服器** > **CPU 和記憶體**	show perf query class Memory
網路狀態	netstats		show network status
重新啓動伺服器	重新啓動	登入伺服器上的平台網頁 移至**伺服器** > **當前版本**	utils system restart
收集追蹤/記錄檔	Sftp, ftp	RTMT 移至工具標籤，然後選擇**追蹤** > **追蹤和記錄中心**	列出檔案：file list 下載檔案：file get 檢視檔案：file view

下表列出了常見的問題和用於解決這些問題的工具。

表 *94:* 對 *CLI* 命令和 *GUI* 選擇的常見問題進行疑難排解

工作	**GUI** 工具	**CLI** 命令
存取資料庫	none	以管理員身份登入並使用以下任何一項**show**的命令： • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* 要執行 SQL 命令，請使用**run**命令： • 執行 sql<sql command>
空出可用硬碟空間 **附註** 您僅能從記錄檔分區中刪除檔案。	在 RTMT 使用者端應用程式中移至**工具**標籤並選擇**追蹤和記錄中心**>**收集檔案**。 選擇條件以選擇要收集的檔案，然後勾選**刪除檔案**選項， 檔案下載到 PC 後將刪除Unified Communications Manager伺服器上的該份檔案。	file delete
檢視核心檔案	您無法檢視核心檔案，但您可使用 RTMT 應用程式然後選擇**追蹤和記錄中心** > **收集故障轉儲**。	utils core[options.]

工作	**GUI** 工具	**CLI** 命令
重新啓動 Unified Communications Manager 伺服器	登入至伺服器上的平台並一致**重新開始** > **當前版本**。	utils system restart
更改追蹤的除錯級別	在 `https://<server_ipaddress>:8443/ccmservice/` 登入至 *Cisco Unity Connection* 服務能力管理，然後選擇**追蹤** > **組態**。	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
查看 netstats	none	show network status

疑難排解秘訣

當您對Unified Communications Manager進行疑難排解時，下裂的提示可能會對您有所幫助。

提示 檢視Unified Communications Manager的版本資訊以查看已知的問題。 版本資訊提供了已知問題的描述和解決方法。

提示 了解您的裝置在哪裡註冊。

每個Unified Communications Manager記錄在本地記錄追蹤檔案。 若電話或閘道已註冊到特定位址Unified Communications Manager，若在該位址起始了通話，通話即於該Unified Communications Manager處理。 您將需於Unified Communications Manager擷取有關的追蹤以除錯。

一個常見的錯誤涉及使裝置在訂閱者伺服器上註冊但在發布伺服器上擷取追蹤。 這些追蹤檔案將幾乎爲空白，且絕對不會含有該通話。

另一個常見問題所涉及的爲將裝置 1 註冊至 CM1 及將裝置 2 註冊至 CM2。 若裝置 1 撥話給裝置 2，則通話追蹤發生在 CM1 中，若裝置 2 撥話給裝置 1，則追蹤發生在 CM2 中。 若要解決雙向通話的問題，則兩個追蹤Unified Communications Manager皆需同時獲取以取得疑難排解所需的所有資訊。

提示 請記得問題大概發生的時間。

可能發生了多個通話，故約略記得通話的時間可以幫助 TAC 快速找出問題所在。

您可在通話流程中在 Cisco Unified IP 電話 79xx 上按下**i**或**?**按鈕兩次取得電話統計資料。

在執行測試以重現問題並產生資訊時，請意識到下列的資料將對問題之理解攸關緊要：

- 撥話的號碼/被撥話的號碼

- 該情形中所涉及的任何其他號碼
- 通話的時間

附註 請記得全部設備上時間的同步對疑難排解都很重要。

若要重現問題，請確定先查看修改日期和檔案中的時間戳記以選擇該時間範圍的檔案。 收集正確追蹤資訊最佳的 方式意謂您可以重現問題然後再快速找到最新的檔案並從Unified Communications Manager伺服器複製。

提示 儲存記錄檔檔案以防止其被覆寫。

一段時間後，檔案將被覆寫； 知道要記錄到哪個檔案的唯一方法就是在功能表欄上選擇**檢視** > **重新整理**，檢視檔案上的日期和時間。

系統歷史記錄檔

此系統歷史記錄檔提供了初始系統安裝、系統升級、Cisco 選件安裝、DRS 備份和 DRS 還原以及交換機版本和重新開機歷史記錄的概覽一個中心位置。

相關主題

系統歷史記錄檔概覽 ，第 440 頁上的
系統歷史記錄檔欄位 ，第 441 頁上的
存取系統歷史記錄檔 ，第 442 頁上的

系統歷史記錄檔概覽

系統歷史記錄檔以簡單的 ASCII 檔案形式存在（ **system-history.log**），且資料不會保留在資料庫中，因此檔案不會變得太大，所以系統歷史記錄檔案不會巡迴。

系統歷史記錄檔提供以下的功能：

- 在伺服器上記錄初始的軟體安裝。
- 記錄每個軟體升級（Cisco 選項檔和修補程式）的成功、失敗或取消。
- 記錄每個所執行的 DRS 備份和還原。
- 記錄透過 CLI 或 GUI 所發出的每次切換版本之調用。
- 記錄透過 CLI 或 GUI 所發出的每次重新啓動和關機之調用。
- 記錄系統每次的啓動。 若不與重新啓動或關閉項目建立關聯，則開機是手動重新開機，關機後再開機或核心崩潰的結果。
- 從初始安裝或功能可用性開始，維護一個包含系統歷史記錄的檔案。

- 存在於安裝資料夾中。 您可在 CLI 中使用**file**命令或您可自即時監控工具（RTMT）存取記錄檔。

系統歷史記錄檔欄位

該記錄檔顯示一個共同頁首，其中包含有關產品名稱、產品版本和核心映像的資訊，如：

==========

產品名稱 - Unified Communications Manager

產品版本-7.1.0.39000-9023

核心映像-＃2.6.9-67.EL

==========

每個系統歷史記錄檔項目均包含以下欄位：

timestamp userid action description start/result

系統歷史記錄檔欄位可以包含以下的值：

- *timestamp*—使用 *mm/dd/yyyy hh:mm:ss*格式顯示伺服器上的本機時間和日期
- *userid*-顯示調用操作的使用者的使用者名稱。
- *action*—顯示下列其中一項動作：
  - 安裝
  - Windows 升級
  - 安裝期間升級
  - 升級
  - Cisco 選件安裝
  - 切換版本
  - 系統重啓
  - 關機
  - 開機
  - DRS 備份
  - DRS 還原
- *description*-顯示以下訊息之一：
  - *version*：顯示“基本安裝”、“Windows 升級”、“安裝期間升級”和“升級”的操作。
  - *Cisco*選項檔名稱：顯示 Cisco 選件安裝操作。
  - *timestamp*：顯示“DRS 備份”和“DRS 還原”操作。

- 活躍版本至非活躍版本：顯示“切換版本”操作。
- 活躍版本：顯示系統重新啓動、關機和開機的操作。

- *result*—顯示以下的結果：
  - 開始
  - 成功或失敗
  - 取消

下面顯示了系統歷史記錄檔的範例。

```
admin:file dump install system-history.log=====================================
 Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
===================================== 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 | root:
 Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade 6.1.2.9901-126
 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117 to
6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version 6.1.2.9901-117
to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart 6.1.2.9901-126 Start
 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start 08/01/2008 16:29:31 | root:
 Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31 | root: Boot 6.1.2.9901-126
Start
```

存取系統歷史記錄檔

您可以使用 CLI 或 RTMT 來存取系統歷史記錄檔。

使用 CLI

您可以使用 CLI 存取系統歷史記錄檔**案**命令，如：

- **file view install system-history.log**
- **file get install system-history.log**

如需 CLI **檔案**命令的更多資訊請參閱 *Cisco Unified Solutions* 命令行介面參考指南。

使用 RTMT

您亦可使用 RTMT 存取系統歷史記錄檔。 在“追蹤和記錄中心”標籤中選擇**收集安裝記錄檔**。

如需使用 RTMT 的詳細資訊，請參閱 *Cisco Unified Real-Time Monitoring Tool* 管理指南。

審計記錄

集中式的記錄審計確保Unified Communications Manager系統的組態變更會記錄於個別的記錄檔中。審計事件代表任何需要記錄的事件。 以下Unified Communications Manager組件產生審計事件：

- Cisco Unified Communications Manager 管理
- Cisco Unified Serviceability
- *Unified Communications Manager CDR* 分析與回報
- *Cisco Unified* 即時監控工具
- *Cisco Unified Communications* 作業系統
- 災害復原系統
- 資料庫
- 命令行介面
- 啓用了遠端支援帳號（技術支援團隊發布的 CLI 命令）

在*Cisco Business Edition 5000*中，以下Cisco Unity Connection組件亦會產生審計事件：

- Cisco Unity Connection 管理
- *Cisco Personal Communications Assistant*（Cisco PCA）
- Cisco Unity Connection Serviceability
- Cisco Unity Connection 使用代表性狀態傳輸（REST）API 的使用者端

以下顯示審計事件的範例：

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:Successful
 Description: Call Manager Service status is stopped App ID:Cisco Tomcat Cluster
 ID:StandAloneCluster Node ID:sa-cm1-3
```

包含有關審計事件資訊的審計記錄檔將寫入公共分割區中。記錄檔分區監視器（LPM）與追蹤檔案類似，依需要管理這些審計記錄檔的清除。預設情況下，LPM將清除審計記錄檔，但審計使用者可以在Cisco Unified Serviceability的“審計使用者配置”視窗中更改此設定。每當公共分割區硬碟使用率超過臨界值時，LPM皆會傳送警報。但因有審計記錄檔或追蹤檔案，警報中沒有有關硬碟是否已滿的資訊。

提示 Cisco 審計事件服務 是一種支援審計記錄檔記錄的網路服務，將顯示在Cisco Unified Serviceability的“控制中心-網路服務”中。 若未寫入審計記錄檔，請在Cisco Unified Serviceability中的**工具** > **Control Hub** —**網路服務**選擇停止並啓動此服務。

在*Cisco Unified* 即時監控工具中，所有審計記錄檔都可以從「追蹤和記錄檔中心」收集、檢視及刪除。 在追蹤和記錄中心的 RTMT 中存取審計記錄檔。 移至**系統** > **即時追蹤** > **審計記錄檔** > **節點**。選擇節點後將有另一個視窗顯示**系統** > **Cisco審計記錄檔**。

RTMT 中顯示以下類型的審計記錄檔：

- 應用程式記錄檔
- 資料庫記錄檔
- 作業系統記錄檔
- 遠端 SupportAccEnabled 記錄檔

應用程式記錄檔

顯示在 RTMT 的 AuditApp 資料夾中的應用程式審計記錄檔提供了Cisco Unified Communications Manager 管理、Cisco Unified Serviceability、命令行介面、*Cisco Unified Real-Time Monitoring Tool*（RTMT）、災難復原系統及 Cisco Unified CDR 分析和回報（CAR）的組態變更：。 *Cisco Business Edition 5000*方面，應用程式審計記錄檔亦會記錄Cisco Unity Connection行政、*Cisco* 個人通訊助理（Cisco PCA）、Cisco Unity ConnectionServiceability 及使用代表性狀態傳輸（REST）API 的用戶端內容的更改。

儘管預設情況下“應用程式記錄檔”保持啓用狀態，但是您可選擇**工具** > **審計記錄檔組態**以進行配置Cisco Unified Serviceability 。 有關可以爲審計記錄檔組態配置的設定的描述，請參閱《*Cisco Unified Serviceability* 管理指南》。

若審計記錄檔在Cisco Unified Serviceability被停用則不會創建新的審計記錄檔案。

提示 請注意，僅具有審計角色的使用者才能變更審計記錄檔設定。 預設情況下，在全新的安裝和升級後，CCMAdministrator 擁有審計角色。 CCMAdministrator 可指定“標準審計使用者”群組至 CCMAdministrator 專門爲審計目的而創建的新使用者， 然後即可自審計使用者群組中刪除 CCMAdministrator。 “「標準審計記錄檔組態」”角色用於提供刪除審計記錄檔功能、讀取/更新以下各項目的存取權限：*Cisco Unified* 即時監控工具（*RTMT*）、Trace Collection工具、RTMT 警示組態、控制中心 - 網路服務 視窗、RTMT 設定檔儲存、審計組態視窗及名爲審計追蹤的新資源。 *Cisco Business Edition 5000*中的 Cisco Unity Connection：在安裝流程中所建立的應用程式管理帳號具有「審計管理員」角色，而且可以將其他管理使用者指派給該角色。

Unified Communications Manager建立一個應用程式審計記錄檔案直到達到配置的最大檔案大小爲止；然後檔案將關閉並再建立一個新的應用程式審計記錄檔案。 若系統指定將記錄檔案巡迴，Unified Communications Manager會儲存所配置的檔案數目。 可使用 RTMT SyslogViewer 檢視某些記錄事件。

Cisco Unified Communications Manager 管理方面將會記錄以下事件：

- 使用者登入和登出
- 使用者角色成員資格更新（新增使用者、刪除使用者、更新使用者角色）。
- 角色更新（新增、刪除或更新新角色）。
- 裝置更新 （電話與閘道）。

- 伺服器組態更新（變更警報或追蹤組態、服務參數、企業參數、IP 位址、主機名稱、乙太網路設定及 Unified Communications Manager伺服器新增或刪除）。

Cisco Unified Serviceability方面將會記錄以下事件：

- 自任何 Serviceability 視窗啓動、停用、啓動或停止服務。
- 追蹤組態和警報組態變更。
- SNMP 組態變更。
- CDR 管理中的變更。
- 檢視Serviceability報告封存中的任何報告。 此記錄檔可在回報程式節點上檢視。

RTMT 以審計事件警報記錄以下事件：

- 警示組態。
- 警示暫停。
- 電子郵件組態。
- 設定節點警示狀態。
- 警示新增。
- 新增警示動作。
- 清除警示。
- 啓用警示。
- 移除警示動作。
- 移除警示。

記錄*Unified Communications Manager CDR* 分析和回報的以下事件：

- 正在重新排程載入程式。
- 安排每日、每周和每月使用者報告、系統報告和裝置報告。
- 郵件參數組態。
- 撥號計劃組態。
- 閘道組態。
- 系統偏好設定組態。
- 自動清除組態。
- 評估引擎組態在某段期間、一日中某時、語音品質等方面的分數。
- 服務品質組態。
- 自動產生/警告預先產生的報告組態。

- 通知限制組態。

記錄災難復原系統的以下事件：

- 備份啓動成功/失敗
- 還原成功啓動/失敗
- 備份已成功取消
- 備份成功完成/失敗
- 還原成功完成/失敗
- 儲存/更新/刪除/啓用/停用備份排成
- 儲存/更新/刪除目標裝置以進行備份

Cisco Unity Connection管理記錄*Cisco Business Edition 5000*的以下事件：

- 使用者登入和登出
- 所有組態變更，包括但不限於使用者、聯絡人、通話管理物件、網路、系統設定和電話。
- 任務管理（啓用或停用任務）。
- 批量管理工具（批量建立、批量刪除）。
- 自訂鍵台對應（對應更新）

Cisco PCA 記錄*Cisco Business Edition 5000*的以下事件：

- 使用者登入和登出
- 透過 Messaging Assistant 變更的所有組態。

Cisco Unity ConnectionServiceability 記錄*Cisco Business Edition 5000*的以下事件：

- 使用者登入和登出
- 所有組態變更。
- 啓用、停用、啓動或停止服務。

使用 REST API 的使用者端記錄*Cisco Business Edition 5000*的以下事件：

- 使用者登入和登出（使用者 API 驗證）。
- 使用Cisco Unity Connection佈建介面的 API 通話。

資料庫記錄檔

顯示在 RTMT 的 notifyix 資料夾中的資料庫審計記錄檔報告資料庫更改。 選擇**工具** > **審計記錄檔配置**即於Cisco Unified Serviceability中配置此記錄檔（預設情況下未啓用）。 有關可以爲審計記錄檔配置而配置的設定的說明，請參閱Cisco Unified Serviceability。

此審計與應用程式審計不同，因爲它記錄資料庫之更改，而應用程式審計則記錄應用程式組態之更改， 除非在以下位置啓用了資料庫審計，否則 notifyix 資料夾不會顯示在 RTMT 中：Cisco Unified Serviceability。

作業系統記錄檔

顯示在 RTMT 的 vos 資料夾中的作業系統審計記錄檔回報由作業系統觸發的事件。 預設不會啓用。**utils auditd**CLI 命令啓用、停用或提供事件狀態。

除非在 CLI 中啓用了審計，否則 vos 資料夾不會顯示在 RTMT 中。

如需 CLI 方面的資訊，請參閱 *Cisco Unified Solutions* 的命令行介面參考指南。

啟用遠端支援 Acct 的記錄檔

顯示在 RTMT 的 vos 資料夾中的“啓用了 Remote Support Acct 的審計記錄檔”回報由技術支援團隊發出的 CLI 命令。 您無法對其進行配置，且僅在技術支援團隊啓用了“遠端支援帳號”的情況下才會創建記錄檔。

確認 Cisco Unified Communications Manager 上的服務已在執行

使用以下步驟驗證哪些 Cisco CallManager 服務在伺服器上爲活躍狀態。

流程

1. 在 Cisco Unified Communications Manager 管理中選擇 **導覽** > **Cisco Unified Serviceability**。
2. 選擇**工具** > **服務啟用**。
3. 在“伺服器”一欄中選擇所需的伺服器。

   您選擇的伺服器會顯示在“當前伺服器”標題旁，並顯示一系列已配置妥服務的方塊。

   “啓動狀態”欄的 Cisco CallManager 行中顯示“已啓動”或“已停用”。

   若顯示**活躍**狀態，指定的 Cisco CallManager 伺服在所選的伺服器上保持活躍狀態。

   若顯示**已停用**狀態，請繼續下裂的步驟。
4. 勾選所需要的 Cisco CallManager 服務的方塊。
5. 按一下 **更新**按鈕。

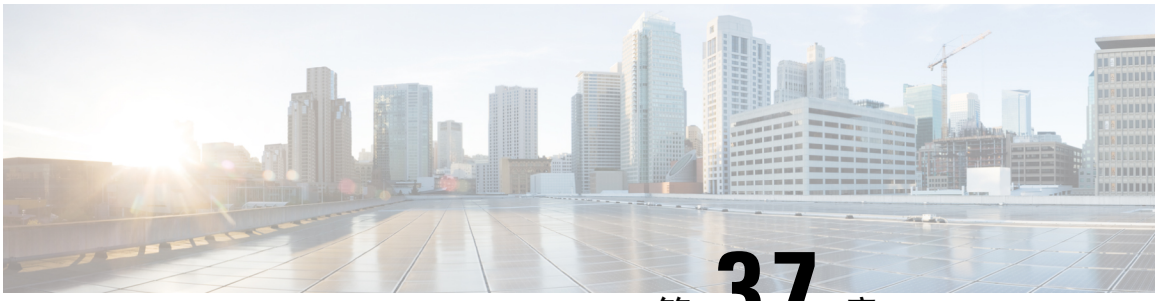
   啓動狀態列將在所指定的 Cisco CallManager 服務一行中顯示**活躍**。

   所選的伺服器上指定的服務即會顯示爲活躍狀態。

若 Cisco CallManager 服務已被啓動，且您要驗證該務當前是否正在執行，請執行下列的步驟。

流程

1. 在 Cisco Unified Communications Manager 管理中選擇 **導覽** > **Cisco Unified Serviceability**。
   將顯示“Cisco Unified Serviceability”視窗。
2. 選擇 **工具** > **控制中心 － 功能服務**。
3. 在“伺服器”列中，選擇伺服器。
   您選擇的伺服器會顯示在“當前伺服器”標題旁，並顯示已配置妥服務的方塊。
   “狀態”列顯示所選伺服器正在執行的服務。



第 37 章

在 TAC 建立個案

本節包含有關與TAC聯繫時所需的資訊類型的詳細資訊，以及與TAC人員共用資訊的方法的資訊。

所有持有有效 Cisco 服務合約的客戶、夥伴、代理商和分銷商，Cisco 技術支援皆提供每天 24 小時優秀的技術協助。 Cisco支援網站可提供疑難排解與解決使用 Cisco 產品及技術時之技術性問題時所需的線上說明檔案及工具。 全年 365 天，全日 24 小時均可尋求支援： *http://www.cisco.com/techsupport*

使用線上 TAC 服務申請工具是提出 S3 及 S4 服務申請的最快方式。（S3 與 S4 服務請求是指在網路效能些微降低，或您需要產品資訊的情況下所提出的服務申請。）在描述您所遇到的情況後，TAC服務請求工具即會自動提供建議的解決方案。若建議的因應措施無法解決您的問題您的服務請求將會指派給 Cisco 工程師。 TAC 伺服請求工具位於此 URL：
http://www.cisco.com/techsupport/servicerequest

若要提出 S1 或 S2 服務申請，或您無法存取網際網路，請以電話連絡 Cisco TAC。（S1 或 S2 服務請求是指在實際執行網路無法運作，或效能嚴重衰退的情況下所提出的服務申請。) Cisco TAC 工程師將會立即接到 S1 及 S2 服務請求以協助您保持業務執行順暢。

若要以電話提出服務申請，請撥打下列一組電話號碼：

亞太地區：+61 2 8446 7411 (澳大利亞：1 800 805 227)

歐洲、中東、非洲地區：+32 2 704 55 55

美國：1 800 553 2447

如需 Cisco TAC 聯絡人的完整清單，請移至下列 URL：*http://www.cisco.com/techsupport/contacts*

您將會需要的資訊

當您使用 Cisco TAC 建立個案時，您需提供初步資訊，以更好地識別和確定問題。 您可能需要提供其他資訊，具體取決於問題的性質。 建立個案後，等待收集以下資訊直到您有工程師的請求將不可避免地導致解決的延遲。

相關主題

Cisco Live! ，第 453 頁上的
Cisco Secure Telnet ，第 454 頁上的
一般資訊 ，第 451 頁上的
網路佈局 ，第 450 頁上的
線上個案 ，第 452 頁上的
問題說明 ，第 451 頁上的
Remote Access ，第 453 頁上的
所需的初步資訊 ，第 450 頁上的

所需的初步資訊

所有的問題請始終向 TAC 提供以下資訊。 收集並儲存此資訊以在開啓 TAC 個案時使用，並定期進行更新。

相關主題

一般資訊 ，第 451 頁上的
網路佈局 ，第 450 頁上的
問題說明 ，第 451 頁上的

網路佈局

提供有關實際和邏輯布局，及語音網路（若適用）中所涉及的所有以下網路元件的詳細描述：

- 一個或多個實例的 Unified Communications Manager
  - 版本 (在 Unified Communications Manager 管理中選擇 **詳細資訊**)
  - Unified Communications Manager的數目
  - 設定（獨立，叢集）
    - Unity
  - 版本 (在 Unified Communications Manager 管理中)
  - 整合類型
    - 應用程式

- 已安裝的應用程式清單
- 每個應用程式的版本號碼
  - IP /語音閘道
- 作業系統版本
- 顯示技術（IOS 閘道）
- Unified Communications Manager 載檔（精簡閘道）
  - 切換
- 作業系統版本
- VLAN 組態
  - 撥號方案-編號方案，通話路由

理想情況下，遞交 Visio 或其他詳細圖表，如 JPG 等。 使用白板，您還可在 Cisco Live! 會議期間時提供圖表。

問題說明

提供發生問題時使用者執行的操作的分步詳細資訊。 確保詳細資訊有包括

- 預期的表現
- 詳細觀察到的表現

一般資訊

確保可以隨時取得以下資訊：

- 這是新安裝嗎？
- 若此爲Unified Communications Manager安裝的舊版本，自開始以來是否發生過此問題？（若沒有，最近對系統進行了哪些更改？）
- 問題是否可以重現？
  - 若能重現，是在正常情況下還是在特殊情況下？
  - 若能重現，發生的時間點是有什麼特別之處？
  - 發生的頻率是？
- 受影響的裝置有哪些？
  - 若特定裝置受到影響（不是隨機的），它們有什麼共同點？
  - 包括問題中涉及的所有裝置的 DN 或 IP 位址（若爲閘道）。

- 通話路徑上有哪些裝置（若適用）？

線上個案

透過 Cisco.com 在線上建立個案比所有其他個案建立的方式初始優先等級都更高， 高優先等級個案（P1 和 P2）爲此慣例的例外。

建立個案時，請提供較精細的問題描述。 該問題的描述將返回 URL 連結，這些連結可能會爲您提供立即的解決方案。

若找不到解決方案，請將繼續傳送個案給 TAC 工程師。

Serviceability Connector

Serviceability Connector概覽

您可以使用 Webex Serviceability 服務簡化記錄檔的收集。 該服務可自動執行尋找、擷取和儲存診斷記錄和資料的任務。

此功能使用部署於您公司處所中的*Serviceability Connector*。 Serviceability Connector是在網路專用主機（連接器主機）上執行的軟體， 您可以在以下任何一個組件上安裝連接器：

- 企業計算平台（ECP）- 推薦

  ECP 使用 Docker 容器隔離、保護和管理其服務。 主機和 Serviceability Connector應用程式是自雲端安裝的。 您無需手動將其升級即可保持其更新狀態和安全狀態。

重要須知 我們建議使用 ECP。 我們未來的發展將集中在這個平台上。 如果您在 Expressway 上安裝 Serviceability Connector，某些新功能將無法使用。

- Cisco Expressway

您可以將可 Serviceability Connector 用於以下目的：

- 服務請求的自動記錄和系統資訊擷取
- Cloud-Connected UC 部署中 Unified CM 叢集的記錄檔收集

您可在這兩個用例使用相同的 Serviceability Connector。

使用 Serviceability 服務的好處

該服務具有下列的優點：

- 加快記錄檔收集速度。 TAC 工程師在執行問題診斷時可以擷取相關記錄檔。 他們可以避免請求額外記錄檔和等待手動收集和交付的延遲。 這種自動化可能會使您的問題解決時間減少個幾天。
- 與 TAC 的協作解決方案分析器及其診斷簽署資料庫一起使用。 系統會自動分析記錄檔，識別已知問題，並推薦已知的修復或解決方法。

Serviceability Connector的 TAC 支援

有關Serviceability連接器的更多詳細資訊，請參閱https://www.cisco.com/go/serviceability或聯繫您的 TAC 代表。

Cisco Live!

Cisco Live！是一種安全的加密 Java 小程式，可讓您和您的 Cisco TAC 工程師透過使用協作 Web 瀏覽/ URL 共用、白板、Telnet 和剪貼板工具來更有效地協作。

在以下的 URL 存取 Cisco Live！：

`http://c3.cisco.com/`

Remote Access

Remote Access使您能夠建立到所有必要裝置的終端服務（遠端通訊埠 3389），HTTP（遠端通訊埠 80）和 Telnet（遠端通訊埠 23）作業期間。

注意 設定撥入時，請勿使用**login:cisco**或**password:cisco**因爲這樣做便成了系統漏洞。

允許 TAC 工程師使用以下其中之一的方式Remote Access裝置即可非常快速地解決許多問題：

- 具有公共 IP 位址的設備。
- 撥入存取-按照優先等級降序排列：模擬資料機、整合服務數位網路（ISDN）資料機，虛擬專用網（VPN）。
- 網路位址轉換（NAT）-IOS 和專用 Internet 交換（PIX），允許存取具有專用 IP 位址的裝置。

確保防火牆在工程師干預期間不會阻塞 IOS 流量和 PIX 流量，並確保所有必需的服務（例如終端服務）都在伺服器上啓動。

附註 TAC 會全權決定處理所有存取資訊，未經客戶同意，不會對系統進行任何更改。

Cisco Secure Telnet

Cisco Secure Telnet 允許 Cisco 服務工程師（CSE）可直接穿過防火牆存取您網站上的Unified Communications Manager伺服器。

Cisco Secure Telnet 運作的方式是使 Cisco Systems 防火牆內的 Telnet 用戶端連線至防火牆後面的 Telnet 守護程式。 這種安全的連線允許您遠端監控和維護您的Unified Communications Manager伺服器而無需修改防火牆。

附註 Cisco 僅在您允許的情況下存取您的網路。 您需在您的站點上提供網路管理員以幫助啓動該流程。

防火牆防護

幾乎所有內部網路都使用防火牆應用程式來限制外部對內部主機系統的存取， 會透過限制網路與公共 Internet 之間的 IP 連線來保護您的網路。

防火牆是透過自動阻止從外部啓動的 TCP / IP 連線而運作，除非將其重新配置爲允許某些類型的存取。

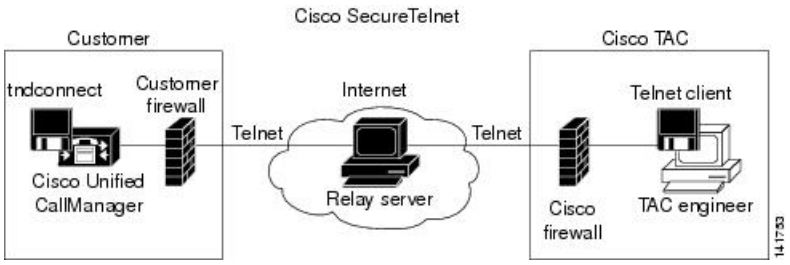
企業網路通常允許與公共網際網路的通訊，但前提是指向外部主機的連線是來自防火牆內部。

Cisco Secure Telnet 設計

Cisco Secure Telnet 充分利用了可以很輕易地在防火牆後啓動 Telnet 連線的優點。 系統使用外部 proxy 電腦將 TCP / IP 的通訊轉傳到位於在*Cisco* 技術支援中心（TAC）中另一道防火牆後的主機。

使用此轉傳伺服器可維護兩個防火牆的完整性，同時亦可支援受屏蔽的遠端系統之間的安全通訊。

圖 ***26: Cisco Secure Telnet*** 系統



Cisco Secure Telnet 結構

外部轉傳伺服器透過構建 Telnet 隧道在網路和 Cisco Systems 之間建立連線。 這使您可以傳輸自己的 IP 位址和密碼標識符Unified Communications Manager伺服器到您的自訂搜尋引擎。

附註 密碼包含您的管理員和 CSE 皆認同的一個文字字串，

您的管理員透過啓動 Telnet 隧道來開始該流程，該隧道建立了從防火牆內部到公用 Internet 上的轉傳伺服器的 TCP 連線。 然後，Telnet 隧道將建立與本地 Telnet 伺服器的另一個連線，從而在實體之間創建雙向連結。

附註 Cisco TAC 上的 Telnet 用戶端與 Windows NT 和 Windows 2000 或 UNIX 作業系統上執行的系統相容。

在您站點的 Cisco Communications Manager 接受密碼後，在 Cisco TAC 上執行的 Telnet 用戶端將連線到在防火牆後面執行的 Telnet 守護程式。 由此產生的透明連線允許進行與本地使用機器相同的存取。

Telnet 連線穩定後，CSE 可以實施所有遠端Serviceability功能，以在您的電腦上執行維護，診斷和疑難排解任務Unified Communications Manager伺服器。

您可以檢視 CSE 傳送的命令以及您的Unified Communications Manager伺服器的回應，但命令和回應可能並不總是完全格式化。

設定遠端帳戶

在 Unified Communications Manager 中配置遠端帳戶，讓 Cisco 支援可以暫時存取系統以進行疑難排解。

程序

步驟 1 在「Cisco Unified 作業系統管理」中選擇 **服務** > **遠端支援**。

步驟 2 在**帳戶名稱**欄位中，輸入遠端帳戶的名稱。

步驟 3 在 **Account Duration**（帳戶期間）欄位中，輸入帳戶期間天數。

步驟 4 按一下**儲存**。
系統產生一個加密的密碼短語。

步驟 5 請聯絡 Cisco 支援，以提供遠端支援帳戶名稱和複雜密碼。