## When you're ready to take control.™

# CommandCenter<sup>®</sup> NOC





Copyright © 2007 Raritan Computer, Inc. CCDNOC-0F-CHT 2007 年 2 月 255-80-5315-00 本頁刻意保持空白。



## 版權及商標資訊

本文件包含的專屬資訊受到版權保護。版權所有。未經 Raritan Computer, Inc. 明確書面許可,不得影印、複製本文件任何部份,或將本文件任何部份或翻譯成其他語言。

© Copyright 2007 Raritan、CommandCenter、RaritanConsole、Dominion 及 Raritan 公司標 誌均為 Raritan Computer, Inc. 的商標或註冊商標。版權所有。Java 是 Sun Microsystems, Inc. 的註冊商標。Internet Explorer 是 Microsoft Corporation 的註冊商標。Netscape 及 Netscape Navigator 是 Netscape Communication Corporation 的註冊商標。所有其他商標均為其擁有者 所有。

## FCC 資訊

本設備已經過測試,符合 A 類別數位裝置的限制(按照「FCC 規定」第15部份)。這些限制的設計目的,是針對商業安裝作業中的有害干擾,提供合理的防護。此設備會產生、使用和散發無線電能量,如果未遵照指示來安裝並使用此設備,就會對無線電通訊造成有害的干擾。在住宅環境中操作此設備可能會造成有害的干擾。

## 日本安規認證

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準 に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波 妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ず るよう要求されることがあります。

由於意外、天災、誤用、濫用、未由 Raritan 人員修改產品、在 Raritan 合理控制範圍外的 事件、或是在非標準操作狀況下對本產品所導致的損害, Raritan 均不負責任。



*美洲地區用戶若需協助,請聯繫力登技術服務中心,* 電話:(732)764-8886;傳真:(732)764-8887;電子郵件:<u>tech@raritan.com</u> 技術支援提供時間-週一至週五8:00am 到8:00pm(美國東部時間)。

全球各地用戶若需協助,請參閱本指南最後一頁的力登各地辦事處聯繫資訊。



## 安全準則

若要避免可能發生的致命電擊事件以及對於力登設備的損害:

- 請勿在任何產品組態設定中,使用雙纜電源線。
- 測試電腦及監視器的 AC 電源接口是否有適當的電極及接地。
- 電腦及監視器都只能使用已接地的電源接口。使用備份 UPS 時,請先關閉電腦、監視器及裝置的電源,再接上電源供應裝置。

## 預設登入使用者 ID/密碼

CC-NOC 的預設使用者名稱是 admin,而密碼是 raritan。建議您立即變更。

## 機架裝載安全準則

需要「機架裝載」的力登產品都必須遵循下列預防措施:

- 在密閉式機架環境中,作業溫度可能會高於室溫。請勿讓裝置超過周遭環境溫度上限 (請參閱《CommandCenter NOC 管理指南》的〈附錄A:規格〉)。
- 確保機架環境中有足夠的空氣流通。
- 小心地將設備裝入機架,避免造成機械負載不平衡。
- 小心地將設備連接到電源供應裝置,避免電路超載。
- 適當地將所有設備 尤其是例如電源延長線等電源供應連線(非直接連線) 接地至 分支電路。



<u>烟</u> 工 式 後 直	
分散式 2500 系列裝置	
變更顯示的語言	
CommandCenter Secure Gateway	
使田考 PC 准備動作	
[次/17日・● 平屈勁/[	
本機驗證	
第 2 章:	
規劃與準備	
基礎設備規劃	
用戶端 PC 規劃	
主要資訊	
次要資訊	
Windows 代理伺服器	
網路考量	
人侵俱測、流重分竹及朔覓監視	
第3章:實體及網路安裝	
獨立式安裝 (CC-NOC 100/250)	
會體宏裝	
5 m ろな 腔距或鏡像連接追	
7.大網路 TAP	
網路組態設定	
分散式安裝(CC-NOC 2500 系列)	
CC-NOC 2500M	
CC-NOC 2500S	
第4章:建立初始組態設定及遷移現有的組態設定	
<b>第4章:建立初始組態設定及遷移現有的組態設定</b> 使用第一次組態設定精靈	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈 第一次組態設定精靈的概略說明 載入授權 安裝授權 開始必要的組態設定	
<b>第4章:建立初始組態設定及遷移現有的組態設定</b> 使用第一次組態設定精靈	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈 第一次組態設定精靈的概略說明 載入授權 安裝授權 開始必要的組態設定 日期、時間、時區 自動更新	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈 第一次組態設定精靈的概略說明 載入授權 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈 第一次組態設定精靈的概略說明 載入授權 安裝授權 開始必要的組態設定 日期、時間、時區 自動更新 探査範圍 SNMP 社群	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈 第一次組態設定精靈的概略說明	
第4章:建立初始組態設定及遷移現有的組態設定 使用第一次組態設定精靈	
<ul> <li>第4章:建立初始組態設定及遷移現有的組態設定</li> <li>使用第一次組態設定精靈</li></ul>	
<ul> <li>第4章:建立初始組態設定及遷移現有的組態設定</li> <li>使用第一次組態設定精靈</li></ul>	
<ul> <li>第4章:建立初始組態設定及遷移現有的組態設定</li> <li>使用第一次組態設定精靈</li> <li>第一次組態設定精靈的概略說明</li></ul>	
<ul> <li>第4章:建立初始組態設定及遷移現有的組態設定</li> <li>使用第一次組態設定精靈的概略說明</li></ul>	
<ul> <li>第4章:建立初始組態設定及遷移現有的組態設定</li></ul>	
<ul> <li>第4章:建立初始組態設定及遷移現有的組態設定</li> <li>使用第一次組態設定精靈</li></ul>	
第4章:建立初始組態設定及遷移現有的組態設定	
第4章:建立初始組態設定及遷移現有的組態設定	
第4章:建立初始組態設定及遷移現有的組態設定	

目錄



i

第6章: Windows 管理、入侵偵測及效能監視	45
Windows 管理的概略說明	
設定外部 Windows 代理伺服器的組態	45
指定 Windows 管理範圍	
指定代理伺服器識別及身分	50
入侵偵測的槪略說明	52
相態設定裝置的沂端網路	
相態設定連接埠掃描偵測	
設定入侵偵測簽名效能評測器的組態	
設定效能監視的組態	61
	<b>~</b>
第1章:開始使用	
啓用通知	63
通知狀態	63
格用網路弱點掃描	64
設定網路中斷報告的組態	65
下載備份檔案	65

圕	1 0	C-NOC 250 獨立式組態設定	9
圕	2 0	C-NOC 250 後方面板	10
圕	з с	C-NOC 250 前方面板	10
圕	4 2	乙太網路 TAP 部署	11
圕	5 C	C-NOC 100/250 的「組態設定」畫面	12
圕	6 C	C-NOC 100/250 的「Setup Network Port」畫面	13
圕	7 C	C-NOC 2500 系列分散式組態設定	14
昌	8 C	CC-NOC 2500N 後方面版	15
圕	9 C	C-NOC 2500N 的「組態設定」畫面	16
圕	10	CC-NOC 2500N 的「Setup Network Port」畫面	16
圕	11	CC-NOC 2500M 後方面版	17
圕	12	CC-NOC 2500M 的「裝置組態設定」畫面	18
圕	13		19
圕	14	授權 CC-NOC 2500M 裝置	19
昌	15	CC-NOC 2500N 登入書面	20
晑	16	按一下 [管理] 索引標籤	20
_ 圕	17	上載裝置授權	20
_ 圕	18	—————————————————————————————————————	20
_ 圕	19	載入裝置授權以加入清單	21
	20	在 CC-NOC 2500N 輸入啓動碼	21
 	21	CC-NOC 2500S 後方面版	22
圖	22	CC-NOC 2500S 的「裝置組態設定」書面	23
圖	23	授權合約	25
圖	24	上載授權	26
 圕	25	安裝授權	27
圖	26	二个个人。 開始必要的組態設定	28
圖	27	設定日期、時間、時區的組態	29
副	28	設定自動更新的組能	30
副	29	設定探查範圍的組能	31
圖	30	設定 SNMP 計理連線密碼的組能	33
副	31	設定 ISP 間道的組能	34
副	32	設定 ONS 伺服器的組態	35
圖	33	設定	36
副	34	在田和能設完和重新啟動	37
国	35	会小社念政之相重和任勤。	37
国	.36		39
国	37		40
国	38	又衣袖///	40
圖	30	N頁科逐水到木体衣直····································	41
四	۵3 ۸۸	CC-NOC 立了重山	71 /1
国	70 /1	設定从並代理伺服哭的組能鬥進行 Windows 签理	18
圖	42		0 2₽
副	42	JRALIVELLINRRU 指定 Windows 管理範圍	40
副	4 <u>4</u>		50
国	45	11~1~1~1~1~1~1~1~1~1~1~1~1~1~1~1~1~1~1	51
国	46 46	JHCMP场响应习力 Windows 答理代理伺服哭的清單	51
围	-+0	WINDOWS 日在17年1月1日中	51

圖 47 入侵偵測組態設定
圖 48 組態設定裝置的近端網路
圖 49 指定近端網路裝置的 IP 位址54
圖 50 設定連接埠掃描偵測的組態
圖 51 指定連接埠偵測的 IP 位址
圖 52 選擇簽名效能評測器的入侵偵測裝置
圖 53 「選擇簽名類型」表格
圖 54 選擇要監視的作業系統和服務 59
圖 55 選擇要監視的應用程式60
圖 56 流量分析61
圖 57 依照通訊協定來排序流量62
圖 58 網路報告62
圖 59 啓用通知狀態
圖 60 設定層級 1 和層級 2 的網路弱點掃描64
圖 61 設定網路中斷報告的組態
圖 62 下載備份檔案

## 第1章: 簡介

CommandCenter NOC (CC-NOC)的主要功能就是管理您網路中的節點。如果節點的 IP 位 址介於受管理的位址範圍之間,就會自動探查節點。除了網路探查之外,CC-NOC 也會提 供服務管理、網路資訊的資料庫、規則引擎、通知引擎,以及 Web 伺服器。您也可以指 示 CC-NOC 收集您 Windows 系統中的統計資料、監視網路流量以得知是否有入侵嘗試、 監視網路流量中的頻寬效能,以及掃描系統中的弱點。

在本文件中,CC-NOC 這個辭彙是指下列機型:

- CommandCenter NOC 100
- CommandCenter NOC 250
- CommandCenter NOC 2500N
- CommandCenter NOC 2500M
- CommandCenter NOC 2500S

注意:如果資訊與特定機型相關,就會明確標示出來。

## 獨立式裝置

CC-NOC 可以在獨立式環境中操作;在這個環境中,裝置本身會提供完整的功能,例如網路探查、輪詢、Windows 管理、流量分析、網路弱點掃描,以及入侵偵測。

以下這些 CC-NOC 裝置可以在獨立式環境中操作:

- CC-NOC 100
- CC-NOC 250

若需部署和組態設定 CC-NOC 100 或 CC-NOC 250 的指示,若需額外資訊,請參閱 (第3章:實體及網路安裝)的 (獨立式安裝 (CC-NOC 100/250)) 一節。

## 分散式 2500 系列裝置

CC-NOC 也可以在獨立式環境中操作;在這個環境中,像是網路探查、輪詢、Windows 管理、流量分析、網路弱點掃描以及入侵偵測等功能,都會分散到不同的裝置中。以下這些CC-NOC 裝置可以在分散式環境中操作:

- CC-NOC 2500N:用於其他裝置、網路探查、輪詢、網路弱點掃描及網路中斷的組態 設定。
- CC-NOC 2500M:用於 Windows 管理。
- CC-NOC 2500S:用於入侵偵測及流量分析。

若需在分散式環境中部署和組態設定 CC-NOC 的指示,若需額外資訊,請參閱 (第3) 章:實體及網路安裝)的 (分散式安裝 (CC-NOC 2500 系列)) 一節。

注意:如果不需要 CC-NOC 2500M 或 CC 2500S 所提供的功能,则也可以獨立部署 CC-NOC 2500N。

## 變更顯示的語言

CC-NOC 使用者介面可以 6 種語言顯示 — 英文、法文、德文、簡體中文、繁體中文及日 文—視用戶端 PC 的瀏覽器設定而定。若要變更顯示的語言,請在瀏覽器的語言設定下選 擇其中一種語言當作喜好的語言,或將您要的語言移到喜好語言清單的頂端:

- 英文 [en-us]
- 法文 [fr-fr]
- 德文 [de-de]
- 簡體中文 [zh-cn]
- 繁體中交 [zh-tw]
- 日文 [ja]

使用者介面會在下次顯示 CC-NOC 頁面時,以新的語言顯示,即使您使用不同的語言設定登入也一樣。

注意:您必須擁有適當的語言 fonts installed on your client system for the selected language to display properly.

## CommandCenter Secure Gateway

CC-SG 針對受管理的力登裝置、目標伺服器及基礎設備裝置,提供單一點存取及控制。 CC-NOC 可以與 CC-SG 結合部署。若需如何設定 CC-SG 組態來登錄 CC-NOC 事件以及在 裝置之間交換通知的初步指示,請參閱力登的《CommandCenter Secure Gateway 管理 指南》。

## 使用者 PC 準備動作

若要存取 CC-SG 及任何由 CC-SG 管理的目標,瀏覽器就必須有正確的 Sun JRE 版本,例 如 rev 1.4.2.05。若需詳細資料,請至 <u>www.raritan.com/support</u>參閱 CC-SG 的「**韌體升級**」 (Firmware Upgrades)下的「相容性矩陣」(Compatibility Matrix)。

如果使用 CC-SG,則必須停用快顯視窗封鎖程式,以及預設啓用的任何防火牆軟體,例如 XP SP2。

#### 遠端驗證

CC-SG 可以遠端驗證 CC-NOC 使用者,來提供作業的增強完整模式和針對 CC-SG 目標的「單一登入 (SSO)」存取方式。利用按一下存取 CC-SG 的方式和針對目標的 SSO 存取方式,CC-NOC 使用者就可以輕鬆地在系統之間移動。

#### 對映使用者群組

利用遠端驗證,就可以安全地路由所有 CC-NOC 登入,並由 CC-SG 解析以進行補救措施。CC-NOC 會接收 CC-NOC 使用者所屬的 CC-SG 使用者群組,並將這些群組對映到它的任一個本機群組(也就是 Admin、User、Executive)。如果使用者隸屬於多個群組,就會使用權限最高的群組。當 CC-NOC 使用者存取 CC-SG 目標時,存取權利、使用權限以及原則就會根據他們的使用者群組成員資格而定。

**注意**:在 CC-NOC 上對映群組時,必須先在 CC-SG 建立使用者群組,或是從外部驗證伺服器(例如Active Directory) 匯入使用者群組。



## 本機驗證

如果沒有設定遠端驗證的組態,就會依照預設在本機驗證 CC-NOC 使用者。如果設定遠端驗證的組態,但是無法使用 CC-SG 或是密碼不正確,則也會使用本機驗證。

如果使用「遠端驗證」,CC-NOC 使用者就必須登入 CC-SG 才能存取目標。系統會提示使用者提供 CC-SG 登入及密碼,並比對本機 CC-SG 使用者資料。

注意:無論其他使用者在哪裡驗證, CC-NOC 的 admin 帳戶一律在本機驗證。

本頁刻意保持空白。



## 第2章:部署前的規劃

本文件的焦點是部署 CC-NOC。安裝 CC-NOC 之前,必須對於環境有明確的瞭解。這可以只是知道要管理哪些節點這麼簡單,也可以像是參照完整網路拓撲那麼複雜。有了這樣的知識,您就可以規劃部署並確保順利進行。在環境中部署一部 CC-NOC 裝置(獨立式)或多部 CC-NOC 裝置(分散式)時,這是最重要的一環。

## 規劃與準備

要考量的關鍵事項包括:

- 基礎設備規劃 對於設備和先決條件的計畫,例如適當的 HVAC、電源、實際存取和 裝載、配線等。
- 使用者 PC 規劃 確定符合存取 CC-NOC 的 PC 需求。
- 主要資訊 CC-NOC 需要此資訊才能能夠有效管理環境。
- Windows 代理伺服器組態設定 收集系統資訊。只有已啓用自動更新的 Windows XP Professional Service Pack 2(或更新版本)才能作為外部代理伺服器使用。您不一定要 為 CC-NOC 2500M 設定外部代理伺服器的組態,因為它有自己的內部代理伺服器。
- 網路考量 了解您要使用的環境。
- 入侵偵測 了解要在環境中的哪個位置部署 CC-NOC、CC-NOC 會監測哪些流量,以 及流量如何到達 CC-NOC。
- 收集效能資料 了解要在環境中的哪個位置部署 CC-NOC、CC-NOC 會監測哪些流量,以及流量如何到達 CC-NOC。

注意:正確規劃是成功部署 CC-NOC 的關鍵。

#### 基礎設備規劃

HVAC、電源、實際存取和裝載、網路、配線以及遠端存取,都應該事先規劃。

- 必須有適當的加熱和冷卻設備,在設定的溫度和溼度範圍中運作。
- 序列裝置連線使用內含的虛擬數據機電纜線。

#### 用戶端 PC 規劃

您可以在具有終端機模擬程式(例如 Hyper Terminal、Tera Term 或 Minicom)的 PC 上, 透過序列埠存取 CC-NOC 以進行初始安裝;或是從使用者 PC 利用 Web 瀏覽器來進行初 始安裝。瀏覽器必須啓用 Javascript 才能正確運作力登產品。

用戶端 PC 支援這些瀏覽器及作業系統:

用戶端瀏覽器	用戶端作業系統
IE 6.0	Win 2K   Win XP
Mozilla 1.7	Win 2K 、 Win XP 、 Solaris 10
Mozilla 1.7	RedHat9
Mozilla Firefox 2.0	Win 2K 、 Win XP 、 Solaris 10
Mozilla FireFox 2.0	RedHat9
Netscape 7.2	Win 2K  Vin XP  Solaris 10
Netscape 7.2	RedHat9



### CC-SG 的 JRE

若要存取 CC-SG 及任何由 CC-SG 管理的目標,瀏覽器就必須安裝正確的 Java 版本,例如 rev 1.4.2.05。若需詳細資料,請至 <u>www.raritan.com/support</u> 參閱 CC-SG 的「**韌體升級**」 (Firmware Upgrades)下的「相容性矩陣」(Compatibility Matrix)。

PC 必須停用所有快顯視窗封鎖程式,以及預設啓用的任何防火牆軟體,例如 XP SP2。

## 主要資訊

安裝之前請收集下列資訊:

- CC-NOC的IP位址: CC-NOC 必須有靜態 IP。您也需要子網路遮罩和閘道位址。
- 發現的裝置 IP 位址:事先得知您要探查且由 CC-NOC 管理的 IP 位址(無論是單一 IP 或 IP 範圍)。同時,知道 DCHP 範圍之後,就可以從管理範圍中加以排除;這樣做可 以使 CC-NOC 的效能最佳化。
- DNS 位址: CC-NOC 必須得知用於主機解析的 DNS 伺服器。
- 時區:指定正確的時區,才能在發生網路中斷及事件時精確報告。
- 電子郵件通訊需求: CC-NOC 必須能夠傳送 SMTP 流量,才能接收事件通知。CC-NOC 通常就是它本身的遞送代理程式;不過,如果您的防火牆會限制傳出 SMTP 流量,您就必須提供 SMTP 轉送。如果是這樣,請找出 SMTP 轉送的 IP 位址,並從 CC-NOC 選擇電子郵件使用者名稱。

注意:使用附錄中的〈現場調查〉可協助您循序設定組態。

## 次要資訊

要考量的其他資訊包括:

- ISP 閘道:為了監視 ISP 連線,您必須提供 ISP 閘道位址,讓 CC-NOC 檢查開機/停機 狀態。
- SNMP 社群連線密碼及 SNMP 組態設定:如果要接收設限、收到基準值違規通知,以 及從已啓用 SNMP 的節點收集歷史效能資訊,就必須確定已設定裝置的組態以將設限 傳送到 CC-NOC,且您已經知道要收集其效能資料之系統的適當社群連線密碼。
- NTP 伺服器:若要透過使用 NTP 通訊協定的網路同步化時間,請考慮安裝 NTP 伺服器。

## Windows 代理伺服器

必須有代理伺服器,您收集的 WMI (Windows Management Instrumentation) 代理程式資料 才能監視和管理 Windows 系統。

如果您是在分散式環境中使用 CommandCenter 2500M,請使用它本身的內部代理伺服器,或是設定外部代理伺服器的組態。

注意: CC-NOC 100 及 CC-NOC 250 都必須使用外部代理伺服器。



## 網路考量

開始部署之前,請確認下列限制因素:

- 路由:請確定 CC-NOC 能夠看到您想管理的所有裝置。確認 CC-NOC 所在的子網路能夠與其他子網路通訊。
- 防火牆:請確定防火牆允許從 CC-NOC 進行 SSH 傳入及傳出 這樣才能下載 CC-NOC 更新程式。檢查 SMTP 限制(如果有的話)。

## 入侵偵測、流量分析及頻寬監視

有數種組態設定選項可讓 CC-NOC 提供入侵偵測、流量分析及頻寬監視。這些功能都仰賴相同的混雜流量探查連接埠。

如果能以最佳方式在網路中設置 CC-NOC,它就能監視安全性、識別入侵嘗試、分析流量,以及判斷網路速度緩慢或未獲授權之流量的根本原因。

您可以把 CC-NOC 當成轉換點,將它設置於受信任的網路區段(也就是防火牆之內)與 不受信任的網路區段(也就是防火牆之外)之間,或是將 CC-NOC 設置於無線路由器與 內部網路區段之間。如果有任何問題,請聯繫力登技術服務中心。 本頁刻意保持空白。



## 第3章:實體及網路安裝

本章說明如何在獨立式或分散式環境中實際安裝 CC-NOC 和設定 CC-NOC 網路設定的 組態。

## 獨立式安裝 (CC-NOC 100/250)

在獨立式環境中, CC-NOC 100 及 CC-NOC 250 都具備所有功能,例如網路探查、輪詢、 Windows 管理、流量分析、網路弱點掃描及入侵偵測 – 這些都在同一個裝置中進行組態設 定。這些裝置能夠監視的裝置數量如下:

	<b>CC-NOC 100</b>	<b>CC-NOC 250</b>
基礎設備裝置數量	10	25
Windows 伺服器數量	10	25
Windows 工作站數量	100	250

\***注意:**因效能問題,監視大量的 Windows 工作站 (超過 250) 僅於跨多個子網路使用多個 外部代理伺服器才受到支援。此外,多個代理伺服器組態設定一次應安裝於一台代理伺服 器上,安裝於每台代理伺服器之間的時間應有數小時的間隔。。

下圖說明 CC-NOC 250 的網路拓撲。



圖 1 CC-NOC 250 獨立式組態設定

## 實體安裝

第一個步驟就是在網路中安裝 CC-NOC 100/250。您應該擁有下列各項:

- (1) CC-NOC 100 或 CC-NOC 250
- (1) 電源線
- (1) 虛擬數據機電纜線



圖 2 CC-NOC 250 後方面板

若要安裝 CC-NOC 100 或 CC-NOC 250:

- 1. 將 CC-NOC 裝入機架組,或是放在桌面或架子上。確定機殼後方通風良好。
- 2. 將網路線一端插入 CC-NOC 擴充槽的「管理」(Management) 連接埠 (LAN 1)。
- 3. 將網路線另一端插入網路的 10Mbps 或 100Mbps 乙太網路連接埠。這個連接埠應該連接到您要指派 CC-NOC 的網路。
- 4. 將網路線一端插入 CC-NOC 的「監視」(Monitor) 連接埠 (LAN 2)。
- 5. 將纜線另一端插入交換器上的跨距或鏡像連接埠或是乙太網路 TAP。若需設定跨距連接埠的詳細資訊,請參閱下一節〈**跨距或鏡像連接埠**〉或本章的〈乙太網路 TAP〉。
- 6. 將電源線一端插入 CC-NOC 後方的接口。
- 7. 將電源線另一端插入標準 110V 插座。
- 按下電源按鈕, 啓動 CC-NOC(電源按鈕是系統前方面板內兩個按鈕的右邊按鈕)。
   系統會開機且電源燈亮起。系統大約需要五分鐘來完成初始啓動工作。



## 跨距或鏡像連接埠

裝置必須能夠看到在網路上傳遞的封包,入侵偵測及網路效能才能正確運作。若要達到這個目標,請在網路上組態設定「鏡像」或「跨距」連接埠。建議您可以利用下列資源來設 定連接埠的組態:

- 若為 Cisco Catalyst 交換器: http://www.cisco.com/warp/public/473/41.html
- 若為 HP Procurve 交換器,請下載交換器的「管理與組態設定指南」: http://www.hp.com/rnd/support/manuals/index.htm
- 若為 3Com 交換器,請參閱適當的組態設定手冊中,有關於「Roving Analysis Port」的部份。



## 乙太網路 TAP

除了使用跨距或鏡像連接埠以外,使用乙太網路 TAP 來接聽網路流量,會比跨距連接埠 更爲安全。

乙太網路 TAP 會在兩個網路連接埠之間傳遞資料。此外,它還會將資料從兩個網路連接 埠輸出到兩個半雙工監視連接埠,或是輸出到單一彙總全雙工監視連接埠。CC-NOC 監視 連接埠會連接到全雙工乙太網路 TAP 監視連接埠。

## 優點

乙太網路 TAP 是在電力層級而非網路層級運作,所以它會精確鏡射網路流量,不會有所 更動。再者,TAP 監視連接埠是單向的。因此,在集線器或跨距連接埠上使用乙太網路 TAP 有數個好處:

- 流量一定會精確鏡射,不會有所更動。
- 流量只會單向流出乙太網路 TAP,所以入侵者(或網路的任何使用者)都不會偵測到 CC-NOC 正在監視流量。
- 因為沒有輸出網路,這樣 CC-NOC 的監視連接埠無法連接到網路,所以 CC-NOC 不會 意外將流量傳出連接埠。

### 部署

請使用乙太網路 TAP 與乙太網路纜線來取代使用乙太網路集線器。乙太網路 TAP 與集線器的功能完全相同,只不過其中一個連接埠是單向的,而且會將透過網路傳遞的資料輸出。這就是連接到 CC-NOC 監視介面的連接埠。



圖 4 乙太網路 TAP 部署

#### 網路組態設定

若要指定 CC-NOC 的網路組態設定(也就是 IP 位址、網路遮罩、預設閘道、DNS 伺服器):

1. 將鍵盤和監視器連接到 CC-NOC 後方的鍵盤和監視器連接埠

注意:以虛擬數據機電纜線連接 CC-NOC 的序列埠與 PC,並使用終端機程式且設定如下,也可以進行初始組態設定:模式:VT100,速度:9600bps,資料位元:8,同位: 無,停止位元:1,流量控制:無。

- 2. 按二或三次 Enter 鍵即可顯示登入提示。
- 3. 輸入 config (有區分大小寫)即可登入。不需要密碼。這樣會出現「組態設定」 畫面。

tun Naturnic Dant	License Hddress	00304858874D
etup Network Routes	Configuration	Current Value
est Network Connectivity tart Support Connection ange Password est to Factory Defaults estart Server nutdown Server kit Configuration	MAC Address IP Address Network Mask Gateway Address DNS Address	00304858874C 192.168.45.222 255.255.255.0 192.168.45.1 192.168.45.4

圖 5 CC-NOC 100/250 的「組態設定」畫面

4. 在主選單中,選擇選單中的 [Setup Network Port]。這樣會出現「Setup Network Port」 畫面。

Network Management S Please enter a valid TP address format is	erver: Setup Networ IP address in each	-k n f	Port
NAME	IP ADDRESS		DESCRIPTION
IP Address Network Mask Gateway Address DNS Address	[192.168.45.222 [255.255.255.0 [192.168.45.1 [192.168.45.4	] ] ]	this server's IP address defines network address range router's address domain name server's address
< OK > < Cancel	>		
CTRL+Q: quit j:	down k: up -		TAB: next field

圖 6 CC-NOC 100/250 的「Setup Network Port」畫面

- 5. 輸入網路設定 TCP/IP 位址、網路遮罩、閘道位址及 DNS 伺服器位址。如果您需要 此資訊,請聯繫系統管理員。
- 6. 選擇 [OK] 即可儲存變更並退出「Setup Network Port」畫面。
- 7. 在主選單上選擇 [Exit Configuration] 即可退出「Configuration」畫面。

注意: 稍後透過 Web 使用者介面存取 CC-NOC 時,可以變更 IP 位址。依序按一下 [管理] 索引標籤、[**裝置網路設定**] 及 [設定網路連線組態],即可執行此動作。

在圖 5中,主選單上的其他選擇可提供額外選項,讓您設定 CC-NOC 的組態。

- [Setup Network Routes] 可提供公用程式,用來建立靜態路由以設定 CC-NOC 的路由表。
- [Test Network Connectivity] 可提供簡易工具,用來測試裝置與網路中其他裝置(例如 另一部 CC-NOC 或您已經設定的靜態路由)的連通性。
- [Start Support Connection] 可在您需要診斷及疑難排解時,連線到 CC-NOC 裝置的技術服務中心。
- [變更密碼] 會永久變更密碼, 直到您下次重設它為止。
- [Reset to Factory Defaults] 會將裝置重設為「出貨時」的狀況,並還原成沒有預存組態設定的原始軟體建置版本(還原成出廠預設值也會將密碼重設為出貨時的預設值)。
- [Restart Server] 會重新啓動 CC-NOC。
- [Shutdown Server] 會關閉 CC-NOC。

注意:此時強烈建議您變更預設的 admin 密碼。

現在您已經完成獨立式 CC-NOC 的實際安裝及網路組態設定,可以利用「組態設定精 靈」繼續建立初始組態設定 – 若需額外資訊,請參閱〈第4章:建立初始組態設定及遷移 現有的組態設定 > 。

## 分散式安裝(CC-NOC 2500 系列)

本節說明分散式組態設定(也就是 CC-NOC 2500N、CC-NOC 2500M 及 CC-NOC 2500S) 的實際安裝和設定網路設定的組態。在這個分散式環境中,功能會分散到各個裝置(如下 所示),而受監視裝置的數量會大於獨立式組態設定的受監視裝置數量:

	CC-NOC 2500N	CC-NOC 2500M <sup>1</sup>	<b>CC-NOC</b> 25005 <sup>2</sup>
		2500IVI	23003
功能	網路探查、輪詢、用於組態	Windows 管理	流量分析、
	設定的 Web 使用者介面、 網路弱點掃描、網路中斷		入侵偵測
基礎設備裝置數量	250		
Windows 伺服器數量		50	
Windows 工作站數量		500	

**注意**:如果不需要 CC-NOC 2500M 或 CommandCenter 2500S 所提供的功能,则也可以獨 立部署 CC-NOC 2500N。

下圖說明分散式 2500 系列組態設定的網路拓撲。



圖 7 CC-NOC 2500 系列分散式組態設定

在分散式環境中設定組態是非常靈活的。舉例來說,如果您著重於管理大量的 Windows 伺服器及工作站(也就是超過 50 部伺服器和 500 部工作站),就可以在分散式環境中部 署多達五部 CC-NOC 2500M 裝置。部署五部 CC-NOC 2500M 裝置即可支援監視多達 250 部伺服器及 2500 部工作站。或者,如果您著重於安全性,則可以在分散式環境中部署多 達五部 CC-NOC 2500S 裝置。



<sup>&</sup>lt;sup>1</sup>分散式環境可支援0到5部CC-NOC 2500M 裝置。

<sup>&</sup>lt;sup>2</sup>分散式環境可支援0到5部CC-NOC 2500S裝置(每部裝置使用的頻寬最多20MB/秒)。

#### **CC-NOC 2500N**

在分散式環境中,CC-NOC 2500N 可視為中央伺服器。如果您在環境中部署 CC-NOC 2500M 或 2500S,就必須在這些裝置上組態設定 CC-NOC 2500N 的 IP 位址。您必須在遠端裝置(也就是 CC-NOC 2500M 或 2500S)上產生啓動碼,然後設定 CC-NOC 2500N 的 組態以建立連線。

#### 實體安裝

第一個步驟就是在網路中安裝 CC-NOC 2500N。

注意:在分散式環境中安裝 CC-NOC 2500M 或 CC-NOC 2500S 之前,必須先安裝 CC-NOC 2500N 並建立初始組態設定。若需額外資訊,請參閱(第4章:建立初始組態設定及遷移 現有的組態設定)。

您應該擁有下列各項:

- (1) CC-NOC 2500N
- (1) 電源線
- (1) 虛擬數據機電纜線



圖 8 CC-NOC 2500N 後方面版

若要安裝 CC-NOC 2500N, 請遵循下列步驟:

- 1. 將 CC-NOC 裝入機架組,或是放在桌面或架子上。確定機殼後方通風良好。
- 2. 將網路線一端插入 CC-NOC 擴充槽的「管理」(Management) 連接埠 (LAN 1)。
- 3. 將網路線另一端插入網路的 10Mbps 或 100Mbps 乙太網路連接埠。這個連接埠應該連接到您要指派 CC-NOC 的網路。
- 4. 將電源線一端插入 CC-NOC 後方的接口。
- 5. 將電源線另一端插入標準 110V 插座。
- 6. 按下電源按鈕, 啓動 CC-NOC (電源按鈕是系統前方面板內兩個按鈕的右邊按鈕)。 系統會開機且電源燈亮起。系統大約需要五分鐘來完成初始啓動工作。

#### 網路組態設定

若要指定 CC-NOC 的網路組態設定(也就是 IP 位址、網路遮罩、預設閘道、DNS 伺服器):

1. 將鍵盤和監視器連接到 CC-NOC 後方的鍵盤和監視器連接埠。

注意:以虛擬數據機電纜線連接 CC-NOC 的序列埠與 PC,並使用終端機程式且設定如下,也可以進行初始組態設定:模式:VT100,速度:9600bps,資料位元:8,同位: 無,停止位元:1,流量控制:無。

- 2. 按二或三次 Enter 鍵即可顯示登入提示。
- 3. 輸入 config (有區分大小寫)即可登入。不需要密碼。這樣會出現「組態設定」 畫面。

Network Management Server: Mair	n Menu		
This server's network connectiv	vity is fully config	ured.	
<ul> <li>Select operation</li> <li>Setup Network Port</li> <li>Setup Network Routes</li> </ul>	Serial Number License Address Configuration	ACF6400013 00304858874D Current Value	
Test Network Connectivity Start Support Connection Change Password Reset to Factory Defaults Restart Server Shutdown Server Exit Configuration	MAC Address IP Address Network Mask Gateway Address DNS Address	00304858874C 192.168.45.222 255.255.255.0 192.168.45.1 192.168.45.4	
5.3.0.5. Copyright 2006 Rari	tan Inc. All rights	reserved.	
	<del></del> THD: nex		

圖 9 CC-NOC 2500N 的「組態設定」畫面

4. 在主選單中,選擇選單中的 [Setup Network Port]。這樣會出現「Setup Network Port」 書面。

Network Management S	erver: Setup Network	Port
Please enter a valid IP address format is	IP address in each xxx.xxx.xxx.xxx whe	field. re each x is a digit.
NAME	IP ADDRESS	DESCRIPTION
IP Address Network Mask Gateway Address DNS Address	[192.168.45.222 ] [255.255.255.0 ] [192.168.45.1 ] [192.168.45.4 ]	this server's IP address defines network address range router's address domain name server's address
< OK > < Cancel	>	
CTRL+Q: quit j:	down k: up	TAB: next field

圖 10 CC-NOC 2500N 的「Setup Network Port」畫面

- 輸入網路設定 TCP/IP 位址、網路遮罩、閘道位址及 DNS 伺服器位址。如果您需要 此資訊,請聯繫系統管理員。
- 6. 選擇 [OK] 即可儲存變更並退出「Setup Network Port」畫面。
- 7. 在主選單上選擇 [Exit Configuration] 即可退出「Configuration」畫面。

注意: 稍後透過 Web 使用者介面存取 CC-NOC 時,可以變更 IP 位址。依序按一下[管理] 索引標籤、[**裝置網路設定]** 及[設定網路連線組態],即可執行此動作。

在圖 9 CC-NOC 2500N 的「組態設定」畫面中,主選單上的其他選擇可提供額外選項,讓您設定 CC-NOC 的組態。

- [Setup Network Routes] 可提供公用程式,用來建立靜態路由以設定 CC-NOC 的路由表。
- [Test Network Connectivity] 可提供簡易工具,用來測試裝置與網路中其他裝置(例如 另一部 CC-NOC 或您已經設定的靜態路由)的連通性。



- [Start Support Connection] 可在您需要診斷及疑難排解時,連線到 CC-NOC 裝置的技術服務中心。
- [變更密碼] 會永久變更密碼,直到您下次重設它為止。
- [Reset to Factory Defaults] 會將裝置重設為「出貨時」的狀況,並還原成沒有預存組 態設定的原始軟體建置版本(還原成出廠預設值也會將密碼重設為出貨時的預 設值)。
- [Restart Server] 會重新啓動 CC-NOC。
- [Shutdown Server] 會關閉 CC-NOC。

注意:此時強烈建議您變更預設的admin 密碼。

現在您已經完成獨立式 CC-NOC 的實際安裝及網路組態設定,必須利用「組態設定精靈」建立初始組態設定,之後才能安裝和設定 CC-NOC 2500M 或 CC-NOC 2500S 裝置。 若需額外資訊,請參閱〈第4章:建立初始組態設定及遷移現有的組態設定〉。

## **CC-NOC 2500M**

在分散式環境中, CC-NOC 2500M 負責從指定的 Windows 伺服器及工作站(在 WMI 伺服器及範圍中識別)收集 WMI 資訊,以及將這些統計資料報告回 CC-NOC 2500N。

## 實體安裝

安裝 CC-NOC 2500N 並建立初始組態設定之後,就可以在網路中安裝和設定 CC-NOC 2500M。您應該擁有下列各項:

- (1) CC-NOC 2500M
- (1) 電源線
- (1) 虛擬數據機電纜線



## 若要安裝 CC-NOC 2500M:

- 1. 將 CC-NOC 裝入機架組,或是放在桌面或架子上。確定機殼後方通風良好。
- 2. 按二或三次 Enter 鍵即可顯示登入提示。
- 3. 將網路線一端插入 CC-NOC 擴充槽的「管理」(Management) 連接埠 (LAN 1)。
- 4. 將網路線另一端插入網路的 10Mbps 或 100Mbps 乙太網路連接埠。這個連接埠應該連接到您要指派 CC-NOC 的網路。



- 5. 將電源線一端插入 CC-NOC 後方的接口。
- 6. 將電源線另一端插入標準 110V 插座。
- 7. 按下電源按鈕, 啓動 CC-NOC (電源按鈕是系統前方面板內兩個按鈕的右邊按鈕)。 系統會開機且電源燈亮起。系統大約需要五分鐘來完成初始啓動工作。

#### 裝置的組態設定

第二個步驟分為兩個部份 – 設定網路設定的組態,以及在 2500M 與 CC-NOC 2500N 之間 建立管理連線。

重要事項:如果要設定 CC-NOC 2500M(或 CC-NOC 2500S)裝置的組態,您必須先向力登支援中心請求授權,其網址是 <u>http://www.raritan.com/support</u>。

若要為 CC-NOC 2500M 裝置指定網路組態設定:

1. 將鍵盤和監視器連接到 CC-NOC 後方的鍵盤和監視器連接埠。

注意:以虛擬數據機電纜線連接 CC-NOC 的序列埠與 PC,並使用終端機程式且設定如下,也可以進行初始組態設定:模式:VT100,速度:9600bps,資料位元:8,同位: 無,停止位元:1,流量控制:無。

- 2. 輸入 config (有區分大小寫)即可登入。不需要密碼。
- 3. 這樣會出現「裝置組態設定」畫面。

Select operation	Serial Number A License Address Ø	CH6400010 030485891E7
Test Network Connectivity License & Update Software	Configuration Management Address	Current Value
Restart Appliance	MAC Address	0030485891E6
Exit Configuration	Network Mask	255.255.255.0
 +	Gateway Hddress DNS Address	192.168.43.1 192.168.43.1
.3.0.6. Copyright 2006 Rari	tan Inc. All rights r	eserved.

圖 12 CC-NOC 2500M 的「裝置組態設定」畫面



4. 在選單中選擇 [Setup IP Addresses]。

Appliance Configuration: Setup IP Addresses Please enter a valid IP address in each field. IP address format is xxx.xxx.xxx where each x is digit.				
NAME	IP ADDRESS	DESCRIPTION		
Management Address Appliance Address Network Mask Gateway Address DNS Address < Setup IP Addr	[192.168.45.223 ] [192.168.45.224 ] [255.255.255.0 ] [192.168.45.1 ] [192.168.45.4 ] esses > < Cancel >	management computer's address this appliance's address defines network address range router's address domain name server's address		
CTRL+Q: quit j:	down k: up	TAB: next field		

圖 13 設定 IP 位址並連接到 CC-NOC 2500N

- 5. 在 [管理位址] 旁, 輸入相關聯的 CC-NOC 2500N 的 IP 位址。
- 6. 在適當欄位中,輸入 CC-NOC 2500M 裝置的 IP 位址、網路遮罩、閘道位址及 DNS 位址。
- 7. 選擇 [Setup IP Addresses],即可儲存組態設定變更,並建立 CC-NOC 2500M 與 CC-NOC 2500N 之間的連線。

再來,您必須建立可連到 CC-NOC 2500N 網路管理伺服器的連線。

8. 在主選單中,選擇 [License & Update Software] 以授權此裝置。

Appliance Configuration: Licence This Appliance	+
Please follow these steps to license this appliance.	
<ol> <li>On another computer, open management computer's WEB page.         <ul> <li>a) Click the 'Admin' tab at top of page.</li> <li>b) Under 'Licensing', click 'Upload Appliance Licenses'.</li> <li>c) Locate appliance-&gt; 0030485890D1</li></ul></li></ol>	
2) On this computer, highlight 'License this Appliance', press Enter.	
NOTE: To obtain appliance license contact customer support. You will be asked to supply this information: Serial Number ACI6400002 License Address 0030485890D1	
< License this Appliance > < Cancel >	
CTRL+V: quit j: down k: up IHB: next field	

圖 14 授權 CC-NOC 2500M 裝置

- 9. 遵循畫面上的提示,並記下裝置編號及啓動碼。
- 從用來儲存授權檔案的 PC 中,開啓 Web 瀏覽器並指向 http://<CommandCenter\_NOC2500N\_IP\_Address>(CC-NOC 2500N 的 IP 位 址)。這樣會出現 CC-NOC 2500N 的登入畫面。

CommandCenter <sup>®</sup> NOC 250
使用者名稱:
密碼:
登入
圖 15 CC-NOC 2500N 登入畫面

11. 輸入使用者名稱及密碼,然後按一下[登入]。

管理索引標籤

利路中斷 事件 通知 設備 報告 利路弱點 系统 安全性 流量 工具 管理 說明 登出

圖 16 按一下[管理] 索引標籤

12. 在首頁中,按一下[管理]索引標籤。

授權 安裝 CommandCenter NOC 2500N 授權 安裝的裝置清單 上載裝置授權

圖 17 上載裝置授權

- 13. 在「授權」下,按一下[上載裝置授權]。
- 14. 按一下 [載入新的裝置授權] 即可載入 CC-NOC 2500M 的授權。

#### 裝置授權上載

下列是載入 CommandCenter NOC 2500N 的所有裝置授權清單。如果要上載新的授權,請按一下 [*載入新的裝置授權*] 按鈕。每一個將要連線到 CommandCenter NOC 2500N 的新裝置都必須擁有一個**啟動碼**,才能與 CommandCenter NOC 2500N 溝通。按一下 [*新增做動碼*] 按鈕,以輸入一個新的授 權啟動碼。

載入新的装置授權

圖 18 按一下[載入新的裝置授權]



15. 按一下 [瀏覽],並選擇力登客戶支援部門傳送給您的授權檔案。然後按一下 [載入此 授權]。

Browse	載入此項授権
Browse	载人此項授

取消

圖 19 ]	载入装置授權以加入清單
--------	-------------

16. 在 [目前的裝置授權] 清單中找出新增的 CC-NOC 2500M 裝置,然後按一下 [新增啓動碼]。

#### 裝置授權上載

下列是載入 CommandCenter NOC 2500N 的所有装置授權清單。如果要上載新的授權,請按一下「*載入新的裝置接機* 按鈕。每一個將要連線到 CommandCenter NOC 2500N 的新裝置都必須擁有一個**腺動碼**,才能與 CommandCenter NOC 2500N 溝通。按一下 [新增啟動碼,按鈕,以輸入一個新的授 權啟動碼。

技置	類型	有效到	啟動碼狀態	行動
0030485890D1	CommandCenter NOC 2500S	31-May-2006 to 31-May-2016	appliance synched	新的啟動碼
J030485891D5	CommandCenter	1-Jun-2006 to 1-Jun-2016	appliance synched	新的啟動碼
	NOC 2500M			
	NOC 2500M	Fundament Horn Deserved		
	NOC 2500M	Explorer User Prompt		
	NOC 2500M	Explorer User Prompt Script Prompt:		

圖 20 在 CC-NOC 2500N 輸入啓動碼

- 17. 輸入 CC-NOC 2500M 所產生的啓動碼,然後按一下 [確定]。
- 18. 返回 CC-NOC 2500M 並選擇 [License This Appliance]。
- 19. 在系統提示時重新啓動 CC-NOC 2500M, 然後等候大約五分鐘讓 CC-NOC 2500M 重新 啓動和初始化。

在「裝置組態設定」畫面中,主選單上的另一個選擇,可以提供額外選項,用來設定 CC-NOC 裝置的組態。

- [Test Network Connectivity] 可提供簡易工具,用來測試裝置與網路中其他裝置(例如 另一部 CC-NOC 或您已經設定的靜態路由)的連通性。
- [授權和更新軟體] 可讓您管理裝置的授權及更新程式。
- [Update Appliance Software] 可讓您更新 CC-NOC 裝置。
- [重新啓動裝置] 會重新啓動 CC-NOC。
- [Shutdown Appliance] 會關閉 CC-NOC。





### **CC-NOC 2500S**

在分散式環境中,CC-NOC 2500S 負責入侵偵測及流量分析。這些功能仰賴的是混雜流量 探查連接埠,而後者最適合與跨距或鏡像連接埠搭配使用 – 若需額外資訊,請參閱本章稍 早的〈**跨距或鏡像連接埠**〉一節。

#### 實體安裝

安裝 CC-NOC 2500N 並建立初始組態設定之後,就可以在網路中安裝和設定 CC-NOC 2500S。您應該擁有下列各項:

- (1) CC-NOC 2500S
- (1) 電源線
- (1) 虛擬數據機電纜線



圖 21 CC-NOC 2500S 後方面版

若要安裝 CC-NOC 2500S:

- 1. 將 CC-NOC 裝入機架組,或是放在桌面或架子上。確定機殼後方通風良好。
- 2. 將網路線一端插入 CC-NOC 擴充槽的「管理」(Management) 連接埠 (LAN 1)。
- 3. 將網路線另一端插入網路的 10Mbps 或 100Mbps 乙太網路連接埠。這個連接埠應該連接到您要指派 CC-NOC 的網路。
- 將網路線一端插入 CC-NOC 的「監視」(Monitor) 連接埠 (LAN 2)。將纜線另一端插入 交換器上的跨距或鏡像連接埠 – 若需設定跨距連接埠的詳細資訊,請參閱本章稍早的 〈**跨距或鏡像連接埠**〉一節。
- 6. 將電源線一端插入 CC-NOC 後方的接口。
- 7. 將電源線另一端插入標準 110V 插座。
- 8. 開啓 CC-NOC 電源。系統前方有兩個按鈕 電源按鈕是右邊的那個按鈕。系統會開機 且電源燈亮起。系統大約需要五分鐘來完成初始啓動工作。

#### 裝置的組態設定

設定裝置本身以及在 CC-NOC 2500S 與 CC-NOC 2500N 之間建立連線的步驟,與 CC-NOC 2500M 的步驟相同。請參閱 CC-NOC 2500M 的網路組態設定指示,但是請以 CC-NOC 2500S 取代 CC-NOC 2500M。

• Select operation	Serial Number ACI6400002 License Address 0030485890D1	
Setup Network Routes	Configuration	Current Value
Test Network Connectivity License Software Restart Appliance Shutdown Appliance Exit Configuration	Management Address LAN 1 Setup MAC Address IP Address Network Mask Gateway Address DNS Address	192.168.45.223 static 0030485890D0 192.168.45.224 255.255.255.0 192.168.45.1 192.168.45.4
+		

圖 22 CC-NOC 2500S 的「裝置組態設定」畫面

本頁刻意保持空白。



## 第4章:建立初始組態設定及遷移現有的組態設定

您將在本章使用「第一次組態設定精靈」,針對您要進行組態設定的 CC-NOC 100、CC-NOC 250 或 CC-NOC 2500N 建立初始組態設定:

- 要探查和輪詢的 IP 範圍及位址。
- 可解析主機名稱的 DNS 伺服器。
- CC-NOC 通訊對象的電子郵件位址。

注意: CC-NOC 2500S 與 CC-NOC 2500M 都不會使用「第一次組態設定精靈」。

本章也在<**還原來自其他 CC-NOC 系統的組態設定>**一節中說明從較舊的 CC-NOC 系統 遷移到較新的 CC-NOC 系統。

注意:將備份的組態設定還原到新裝置之前,新裝置必須先取得授權,而且執行過「第一 次組態設定精靈」。

## 使用第一次組態設定精靈

您將在本節使用「組態設定精靈」,針對 CC-NOC 建立初始組態設定。「組態設定精靈」,提供逐步工具,用來建立裝置的初始組態設定,或是重新設定基礎組態。

**注意**:首次設定 CC-NOC 的組態時,會依照預設執行「組態設定精靈」。只有在必須重新 設定裝置的組態時,才需要重新執行「組態設定精靈」。

1. 開啓瀏覽器並指向 CC-NOC 的 IP 位址

ttp://<CommandCenter\_NOC\_IP\_Address>。這是在〈**第3章:實體及網路安裝**〉中 設定網路設定時,所指定的 CC-NOC 的 IP 位址。例如,<u>http://192.168.53.5</u>。



圖 23 授權合約



2. 閱讀授權合約,然後按一下[我同意]。

#### 第一次組態設定精靈的概略說明

以下幾個步驟將指導您完成組態設定:

- 授權 此頁面可讓您上載由力登零售商或力登技術服務中心所提供的授權檔案。如果 您沒有授權檔案,請造訪力登支援中心(網址是<u>http://www.raritan.com/support</u>),並按一 下「CC-NOC 授權請求」(CC-NOC License Request)連結,以請求授權。
- 日期、時間、時區 此頁面可讓您設定裝置的日期、時間及本地時區。這將影響出現 在事件、網路中斷和通知上的時間戳記。
- 自動更新設定 此頁面可讓您啓用或停用 CC-NOC 更新程式的自動檢查、下載和安裝 等動作。您必須有服務合約才能使用此功能。
- 管理的位址 此頁面可讓您判斷要探查和輪詢哪些 IP 範圍和位址,以及要忽略哪些位址。需要此資訊才能探查和管理網路。
- SNMP 社群管理 此頁面可識別支援 SNMP 通訊協定的 IP 範圍和位址,以及與這些機器溝通時所需的適當社群連線密碼。
- ISP **閘道設定** 此頁面可讓您輸入「網際網路服務提供者」(ISP)的 TCP/IP 位址,這 樣裝置就能夠偵測出可能對您的網際網路連線造成影響的任何網路中斷。
- 名稱伺服器設定 此頁面可讓您設定 DNS 伺服器的組態,系統就可使用這個伺服器來 解析主機名稱。最少需要一個名稱伺服器。
- 電子郵件通訊 此頁面會告訴 CC-NOC 如何透過電子郵件通訊。需要此資訊才能管理 網路。

**注意**:您可以使用此附錄中的〈現場調查〉協助您循序設定組態。聯絡技術服務中心時, 此資訊也很有幫助。

## 載入授權

每部 CC-NOC 都需要裝置特定的授權才能運作。您的力登零售商或力登區域通路經理應 該已經提供授權檔案,讓您在這個頁面進行上載。如果您沒有授權檔案,請造訪力登支援 中心 (網址是<u>http://www.raritan.com/support</u>),並按一下「CC-NOC 授權請求」(CC-NOC License Request)連結,以請求授權。

🗱 Raritan.	2006/8/1 下午 04:35:32
請求&安裝您的授權	
您現在必須上載裝置的授權到 CommandCen	ter NOC 250。如果您尚未收到装置的接權,請聲給 Raritan 服務中心。您的 CommandCenter NOC 250 装置認證 審是 00304856EB27。
一旦您收到授權,請按一下[ <i>瀏覽</i> 按鈕以邊 <i>權</i> 按鈕,將它上載到 CommandCenter NOC	標授變 <sup>國</sup> 案。然後按一下[ <i>載1.光洗鐘<sup>城</sup>興</i> 稅過、後視後遭資源。如果接種 <sup>個</sup> 案就是 <sup>122</sup> 視要上載的 <sup>個</sup> 案。請按一下在[新 <b>增授觀</b> ] 方塊下方的[ <i>安裝此項接</i> ] 250。如果 <sup>123</sup> 已經安裝一項授權,而且感到繼續使用它,請按一下在[目 <b>前的授觀</b> ] 方塊下方的[ <i>保持於透我戲</i> ] 按鈕。
上载授禮檔案: Browse	上就此有我提福案

圖 24 上載授權



若要上載授權檔案,請按一下[瀏覽],然後選擇您擁有的授權檔案。

連接檔案之後,請按一下 [載入此授權檔案]。如果目前的授權不正確或過期,您就必須輸入新檔案。

## 安裝授權

如果這個授權檔案就是您想要上載到 CC-NOC 的檔案,請按一下 [新的授權] 方塊下的 [安 裝此項授權]。如果您已經安裝授權而且想要繼續使用,請按一下 [目前的授權] 方塊下的 [保持此項授權]。

🕘 上载授權   Admin   Rarita	n CommandCenter NOC 250 - Microso	ft Internet Explorer
檔案(F) 編輯(E) 檢視(V)	我的最愛(A) 工具(T) 說明(H)	
🌀 上一頁 🔹 🐑 🔹 본	🛛 🔁 🎧 🔎 搜尋 🏑 我的最多	t 🕑 🖾 - 🍥
地址(D) • 🎒 https://192.168	3 4 3 2 51/admin/configuration/license/licenseFo	
= Darite	~~	
	2006/7/31 下午 10:35:	:43
請求 & 安裝您的授權		
您現在必須上載裝置的授權約 署認證碼是 003048565827。	癿CommandCenter NOC 250。如果您尚未収	剑装置的授權,請聯絡 Raritan 服務中心。您的 CommandCenter NOC 250 装
一旦忍収到授催,請按一下[ 案,請按一下在「 <b>新贈授業</b> 」。	[ <i>例覽</i> ]按鈕以選擇授權倫荼。然依按一下[. 方塊下方的」 <i>完備的項標構</i> 扶紐,將它上。	<i>氧人助授彊彊黨</i> 對按鈕,懷視授權資訊。如果授權檔案就是忽想要上載的檔 封到 Command Center NOC 250。如果您已經安裝一項授權,而且想要繼續使
用它,請按一下在[目前的接	夏霍]方塊下方的[ <i>保持此項授權</i> ]按鈕。	WAS COMMONICONNER NOC 200 SHACESESS SHEEK IN SHEEK IN SHEEK IN
上載授權檔案:		
	瀏覽上載此項授權檔案	
您目前的授權是有效的。如果	果您想要繼續使用這項授權,請按一下以	
1.0.1 [W-1000-9578-788] 19380 -		
目前的授權		
產品:	CommandCenter NOC 250	
装置序號:	SRNUM00304856EB27	
MAC 位址:	00:30:48:56:EB:27	Fat+A マニート、シャスト - 200 A
有效期至:	17-Apr-2006 到 17-Apr-2016	請按一下上述时[例第]按雄,进择一间和时发帷。备必进择打過备时 授權權案後,請按─下「 <i>載入計得遵備案</i> 」以上載和檢選授權答訊。
<b>允許的基礎設備裝置:</b>	25	
<b>允許的伺服器:</b>	25	
<b>允許的工作站:</b>	250	
无計的升級工作站:	5	
	保持体质透露	
	INTER STRATE	
Copyright © 1999-2006 Raritan,	Inc.	
		15
🗿 完成		🔒 🖨 Internet
C C C C C C C C C C C C C C C C C C C		

圖 25 安裝授權

#### 開始必要的組態設定

這個精靈將指導您完成 CC-NOC 的必要組態設定。建議您下載調查工作表,協助您在啓動此精靈之前,先收集必要資訊。完成精靈之後,您可以在 CC-NOC 的 Web 使用者介面中,存取 [管理] 索引標籤,即可重新進入您在此精靈中進行的設定。按一下 [開始組態 設定]。



圖 26 開始必要的組態設定
### 日期、時間、時區

在探查任何節點和收集任何 SNMP 資料之前,都必須先設定正確的日期和時間戳記。選擇 [使用本地日期和時間並且保持目前時間],即可保持本地時間不變。如果您想在 CC-NOC 設定本地時間,請選擇 [使用本地日期和時間並且設定時間]。當您繼續進行下一個步驟 時,就會立即重設時間。

🜁 設定日期 & 時間   Admin   Raritan CommandCenter NOC 250 - Microsoft Internet Explorer	
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)	At 1997
③ 上一頁 · 〇 · 🛃 🛃 🏠 🔎 搜尋 📩 我的最爱 🧐 🔗 - 🍃	
地址(D) • @ https://192.168.43.251/admin/configuration/time/timeForm.jsp	🗲 输入中文,直接搜索 🔽 🋃 移至
	~
- N= Dawitan	
設定日期 & 時間	
Current Data & Time: 7/21/06 10:27:10 D	M
	IVI
在体型江河即翻载有权来江河SNMP首种之前,必须放足正確的石材如时间数据。 你可以發展 <b>(使用太助口期和時間前日發完時間</b> )發行。設定 Carmanad Cartar Mich 250 装器的太阳時間。太阳	1洋注何细百迭,時期就會立刻而
設。如果您想要保持本地時間不變,諸選擇 <b>使用本地日期和時間並且保持目前時間</b> 」選項。	
諸從下列的選擇方塊中,選取您的時區。這份清單首先按照國家(二個字元碼)排序,然後逐一在每個國家內 多的區域的在最前面,這並不會與按照地理狀況排列有所衝突。該選擇最接近您位置的區域。	按照某些地理情况匾分,將人口最
選擇 [使用 NTP 伺服器] 選項,以開啓 CommandCenter NOC 250 的 NTP 客戶端。NTP 是一種網路服務,用來同:	步化網路上各個電腦的時間。您將會
被要求提供最少一個 NTP 伺服器。如果目前已經選取 [使用 NTP 伺服器],您很想要停止使用 NTP 客戶端,諸 重設時間,決定選用上述兩種選項之一。	按照您是否想要保持目前時間或者
○使用本地日期和時間並且保持目前時間	
○使用本地日期和時間並且設定時間:	
日期(月、日、年):	
七月 😪 31 , 2006	
時間(時、分):	
時 篇 : United States - Eastern Time	
●使用 NTP 伺服器:	
伺服器 1 - 192 168 43 1	
1"360, 189 £ "	
continue >>>>	
Convright @ 1000-2006 Baritan Inc	
avpyright a root base righterit, me	0
🙆 完成 🕠	🔒 💣 Internet

圖27 設定日期、時間、時區的組態

選擇您的 [時區]。這份清單首先按照國家(二個字元碼)排序,然後逐一在每個國家內按 照某些地理情況區分,將人口最多的區域放在最前面,但這並不會與按照地理狀況排列有 所衝突。請選擇最接近您位置的區域。

選擇 [使用 NTP 伺服器] 以開啓「網路時間通訊協定」(NTP) 用戶端。NTP 是一種網路服務,用來同步化網路上各個電腦的時間。如果您選擇此選項,則必須至少提供一個 NTP 伺服器。如果目前已經選擇 [使用 NTP 伺服器],但您想要停止使用 NTP 用戶端,則可根據您想要保持目前時間或重設時間,來決定選擇上述兩種選項之一。

### 自動更新

您可以讓系統定期檢查是否有更新程式,並在可以使用更新程式時下載至 CC-NOC。然後 就可以依照指示自動安裝這些更新程式。每項指示(也就是檢查、下載、安裝)都可以啓 用或停用。這些更新程式也包含目前的入侵偵測簽名。

注意:需要服務合約才能使用此功能。

如果您針對 HTTP 要求使用代理伺服器,請按一下 [是],然後輸入代理伺服器設定,也就 是伺服器、使用者名稱及密碼。否則請按一下 [否]。



#### 圖28設定自動更新的組態

### 探查範圍

**CC-NOC** 的主要功能是管理您網路上的節點。如果節點的 **IP** 位址是在受管理的位址範圍 之內,就會自動探查節點。此步驟可判斷要探查哪些位址或位址範圍,或是「不」探查哪 些位址或位址範圍。

注意:您必須至少指定一個「包含」範圍或者位址,才能完成這部分的組態設定。

(D) • 🕘 https://192.168.43	251/edmin/configuration/mages/magesForm.jsp			🗲 输入中交,直接按束 💌 🔂
<b>₩</b> Rarita	<b>n.</b> 2006/7/31 下午 10:38:13			
新探查的範疇				
nmwndCenter NOC 250 的主要	功能是管理您的網路上的能點。如果能點的ド(	立址是在某個位址範圍之內,就會自動探查訪認點。		
能定您想要探查的範圍和拉娃	<ul> <li>         ·</li></ul>	,以完成這部分的組織設定。如果有任何範圍或者位址地想	要排除,您也可以在此或指定它們。請參考下	列夏递一步指示。
p前點可以放變它們的網路的 所以它們可以放變 p 位往堂	並並,當它們說變時,就被 ConstandCenter NOC 还不會這派失敗的網路中斷。如果要有用這項功	:250 認為是 <i>失敗的網路牛衛</i> 。因此 <b>我們來讓任何定義的</b> ) 能,請核取下列的[ <i>自用 DHCP IP 位並。</i> ]核取汚現。	NICP 範圍要講解在授權和管理之外。支援 S	MB 通訊協定的 DHCP 節點可按照主張名稱道
要使用下列[ <i>探查位他</i> ] 表格 以下是有關上述的一些經常	。先顧入▶位址或電範圍,然没後下! <i>感增者は</i> 用法的範問:	會演劇。與者(影響放映演劇,以漂亮已們新增到相關產業中	<ul> <li>您只能一次新增一個,如果您夠後想從活業</li> </ul>	移祥一個·您可以按一下這單右側的(長納)技
<ul> <li>如果要採查某個範圍</li> <li>若要採查某個特定的</li> </ul>	• 完购入第一個位址和最次位址,然決該下18 申位址,在「開稿」欄位內輸入位址,然決議	曾告念探考 这些,聪密可以跨速数量考验。如果有任何的 「未端」微位保持空白。按下(新曾在古伊男 按鈕,将它制	戰戰成者位址不可以成者不應該採查,要確定# 增到活單中。一般來說,這些是指在範圍之外	時它們新聞到1時增加於波環(譯着下列方法)。 約節點。例如公司要託編件主順代管的任何伺服
64			in this way to be the line of the second sec	IN REPORT .
<ul> <li>若要請件某個範圍。</li> <li>若要請件某個特定的。</li> </ul>	先輸入第一個位並和最次位址,然決按下1 <i>個個</i> 19 位址,在「開稿」欄位內輸入位址,然決讀	动脉体制 按鈕。範圍可以跨過映個網路。在大部分情况下 「未編」欄位保持空白。按下(新增动脉发制按鈕,將它新	,怎只需要在怎已经已经的40個內,指定未做# 看到香葉中。	et Billeto - 1 -
<ul> <li>         ・         :         表明時末個範囲         ・         主要請時末個純面         ・         主要請時末個特定的         ・         ま         ・         ま</li></ul>	先職入第一個位地和最後位址,然就接下1新增 19位址,在「開端」欄位內職入位址,然就讓 16.1000年1月20日時時時的花樓。	动脉弹机 按照。範圍可以應過軟個網絡。在大部分情况下 「來碼」欄位保持空白。该下11秒傳动熱炉機 16组,將它斬	,怎只需要在怎己经已经的範圍內,指毛末面# 著到酒業中。	N 88 AN 17
<ul> <li>若要排件末個範疇;</li> <li>若要排件末個範疇;</li> <li>若要排件末個特定的;</li> <li>對於在下列的陶器和位址;</li> <li>自動管理經由被管理疑蹤;</li> </ul>	无赖入第一做位世和教政位士,然改拔下1.例想 9.位址,在「開端」欄位內備入位壮,然設護 新厚查到的新裝整白動誘難和答理。 的 SHMP 新課查到的介面。請注意這也可能	动被波網 经道·範圍可以跨速检信網絡。在大时分描沒下  末端目標位得時空白。接下(前傳动脉波機 接迫)病它新 答理到在薛查範圍之外的介面。	,您问题新任你们将回知的时候都以,现在完成吗。 我们就是你。	Million of a
<ul> <li>主要將你某個範圍。</li> <li>主要將你某個物理的</li> <li>對於在下列的範圍和位址/</li> <li>自動管理鍵由被管理装置。</li> <li>費用 DesiCP IP 位址變更。</li> </ul>	先能入第一份位址和最优位址,然但按于1余例 27位址,在「開稿」相位内能入位址,然此道 新厚查到他听我是自動质靴和答理。 的 SIMP 所译查到的介面。請註意提也可能 史都那些史著 SIM 编课编定的的数。	动粉浆斑 珍担。如即可以即通想做制料。在大时分和次下 「本頭」做位原料空白。按下「肉炒奶粉发烟 炒田,南已新 答理列在探查離翻之外的介面。	,这小局要在怎已经已经回到的。我们无关面。 著刻活着中。	d Bites 43 −
<ul> <li>北京抗特美國範圍:</li> <li>北京抗特美國範圍:</li> <li>北京抗特美國特定的:</li> <li>對於在了列的範圍和位位;</li> <li>自動管理經由被管理榮務(</li> <li>費用 DescP IP 位建變更:</li> </ul>	先用入第一個位才和時度位才,然於於下(#約 P 位並,在「開展」權位內備入位才,然於算 將厚查到的新裝置自動內積。當該在當在可書。 客都是主要當 Santi 孫讓協定的角點。	动物规模 按照。和即可以即进制的标志。在大时分成次下 [本稿] 模位用并空白。按下( <i>的电动物规</i> 模 接迫,所它则 答考列在探查案据之外的介面。 更一	1.20月间到来已发出这些结约和我们,"我吃来面看 建筑这里中。	d Blan of a
<ul> <li>若要這時末個歌聞:</li> <li>若要這時末個時末個時 普要這時末個時末個時 的也下列的機關和位址」 自動管理器員 費用 corce in 位址變更,3      </li> </ul>	先用入第一個位は和助作位は,然前於下(#約 ▶ 位並,在「開展」權位內備入位止,然於算 然序查到他的研究還口的內機一個非常。 影 Same 所來意的的機構。就是當是做可能。 史都那些支援 Sam 编訳编定的角點。	3時が規模(転換)- 転回可以時機機能解除。 金工制分成次丁 (本項)機(原外空白- 修丁( <i>前等3時地規</i> 模) 接迫。 南石朝 著種列在課意電観之外的介面。 夏一 伊 或者範疇的間隔::	120时间接在这已经把55的两部门。"加卡从面单 经记录某中。	e Maria
<ul> <li>若要這時末個範疇:</li> <li>若要這時末個時末的</li> <li>若要這時末個時末的</li> <li>對於在下列的範疇的位址/</li> <li>自動管理器由著管理展示</li> <li>會用 cacc p 位址變更,3</li> </ul>	先用入具一部位定和制度位之,然然并了(参加 中 位立,在 前位关闭制度位之,然然并 中 位立,在 定期从 建位为载入位上,然就是 亦完全的场化表定了自由使是中位。 的 sander 所属意则的介面, 請註意語自可能 笔都是在 老 sant 被调励定的相数。	30秒波測時24-100可以時機機能構成。在二前分成次下 (末頃)構造用分型白。後下(約%約約波測時26)第它初 管理列在原意識創之外的介面。 夏一 P 或者識範的問題: 意能的末稿((可測用)):	- 2014日第七2014日14日14日14日14日14日14日14日14日 1925日第七・ - 2014日第七2014日14日15日14日15日14日14日14日14日14日14日14日14日14日14日14日14日14日	e Maria
<ul> <li>王要則得不當說說:</li> <li>王要則得不當說說</li> <li>王要則得不當時定的!</li> <li>對於血子對防衛運動自動管理</li> <li>自動管理</li> <li>由管理</li> <li>自動管理</li> <li>正</li> <li>正</li></ul>	地區入減一部位並不能的定定上,然此於了(將使 中位上。在「開設」的社会。 將於並到的所裝式自動的使用。 前5 mane 所能意列的介面。而能意識。可當 者都將此主著 sam 補限指定的相點。	30秒が変更的2-転回可以時後後的時期。金工10分前後下   本頃  値(同分空白-16下10分型がが変更)時3-南三切 著者列在算法電観25分的介面- 夏ーレ 広名電影的間隔: 範囲的末稿(110月1):	- 150-4619年1日2日2日2日2日2日2日2日2日2日2日3日19日9日9日9日9日3日2日2日2日2日2日2日2日2日2日2日2日2日2日2日	e Maria
• 花费共同未高级起了。 • 花费共同本定的体现的位在上 与时代电路内的位在上 日期等者理由著等理关系统 物用 DatcP IP 位注量更 • 3	地域入場一部位並不能的定定は、部成時下(参加 中区:本。在第201 (総合)地入込ま、部成後 所存在到的所保護口論的保護中容量。 約 maner 所在意到的介面。最後意識的考慮。 世 都那些天著 Sang 場談起次的資源」。	30秒が須 約22- 和副可以防張供給條約6-企工則分成次下 (末頃) 備位用分空白-近下(か学が約22東) 著理列在耳然電観之外的介面- 夏一 伊 或者美能的個稱: 集胎的末稿(19週用):	1254日第七2014日14日20日3日15日5月1日 第516月1日 - 141日日 - 1516月1日 - 141日日 - 1516月1日 - 141日日 - 1516月1日 - 141日日 - 1516月1日 - 1516月1日 - 1516月1日 - 1516月1日 - 1516 - 15	e Maria
<ul> <li>電影和体系電報部:</li> <li>電影和体系電報</li> <li>電影和体系電報</li> <li>動作電量和体報</li> <li>動作電量和</li> <li>動作電量和</li> <li>動作</li> <li>助作</li> <li>助作</li> <li>助作</li> <li>助用</li> <li>助作</li> <li>助作</li> <li>助用</li> <li></li></ul>	●規入3→前位2年7時代定法、部位於下(参援 中区4、6(第2),目標2),構成2(第2), 所定2(14),在(第2),目標2), 所定2(14),在(第2),目標2), 所以2(14),在(第2),目標2), 所以2(14),在(第2), 所以2(14),在(第2),在(第2),在(第2),在(第2), 所以2(14),在(第2),在(第2),在(第2),在(第2),在(第2), 所以2(14),在(第2), a,	30分が成果10回-和回可以改进供給給料料。企工10分初次T (末頃)構造料分型合。後T10分型が加速機械。適定第20例 若導列在課意電動起外的介面。 夏一 中 或者電動的間隔: 重一 中 或者電動的間隔:	120-400 ¥ €-20-52 £4365,40803 - 48-6,408 \$535 ¥ 4	e Maria
<ul> <li>         ・         三要則将承認解認         ・         三要則將承認將注         ・         三要則將承認將注         ・         引         か         二         予         目前         ・         言         書         二         第         二         第</li></ul>	4.电入调一的过去时和你定法。"你放开了。伊姆 PP 亿法,在「预风」报念为载入这法,然后就 你完全的你你我怎么问题的是你的是。" 第.世界是如何你不是一些,我们就是你的你就。 你们就是你们的你就。" 我们那些大都"conn 就到我们的你就。"	动物发展的运车和回口以即进展的组织。中企工时分现及下 [末頃] 欄位用外空白。除了( <i>的)等动物发</i> 展 ) 第三前 一前 著理列在译意集剧之外的介面。 第一 中 或者集剧的图码: 集剧的末端(可谓用): 斯曼社会法策 ————————————————————————————————————	125481#E20202E8863408015 * AFCA.m# #558#4 + -	Alline d
<ul> <li>王要共称天团和赵司、</li> <li>王要共称天团称王的、</li> <li>王要共称天团称王的、</li> <li>科技会学习的传统部門位址/</li> <li>自動完考型出出著名理秘書名理秘書</li> <li>(第四 DAICP IP 位注量更 * 3)</li> </ul>	48人3年前位2年7月8日定年、初度時で1月8日 中区本・6月7日、「彼安市私人3年」、新設設 所存立時的に発展(1)時時時でで・ 作うmane 所有充分的介有。当該意識(日)書 作家那些大部 som 補満協定の指数・ 管部単生素部 som 補満協定の指数・	30秒波測 於照-和副可以時後後個條約-企工前分核次下 (本項) 個位得分空白-除下 (かゆぶか波束 除道・南石朝 著考列在算意筆觀之外的介面- 夏一 P 或者集觀的目稿: 夏一 P 或者集觀的目稿: 數個的末稿(可選用): 」	125481#E2602E886548819 * AFEA.me #558.¥ + -	Alline d
● 医素纳尿 法勤劳法的 ● 医索纳尿 法勤劳法的 科外 & 下列的电缆时位 社/ 品册名 理想角 被在 琴系起 即間 cace p 你 是要是 • 3	地震入調一部位支化局熱度定法、部度時下(通停 中区)、金 (開発)、総合(執入法と、部度) 部(除空)(執入法、部度)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(執定)(動)(和)(動)(加)(和)(動)(加)(和)(m)(和)(m)(m)(m)(m)(m)(m)(m)(m)(m)(m)(m)(m)(m)	3時が成果(1962-100可以時後後前時時。金工前分成次下   本頃) 欄位得分空白-16下16分部が成果(時道・高石前 著得列在耳察衛期起外的介面- 第一 伊 式者策範的間隔: 	(1)354(1)が日本日には2日35(5)(3)(1))・AIでAI(1) 2015年4 -	All front a
<ul> <li>医胃炎系统管理的</li> <li>医胃炎系统管理的</li> <li>使用的电量的位置</li> <li>自由管理组合管理系列</li> <li>使用 enco p 位置量度 · 3</li> </ul>	地路入場一部位並不能的定定と、部位計下(後の) のだよ。を(788)、(彼の)の私人はと、部位語 所存在気的の所有度(気の)の前者、当該意識(前り)客 比較原始支援(500)(前者、当該意識(前り客) と変形的不可能気気(加)の前期)、           102(2)利用         102(2)10(42:50)           102(3)0(43)、102(10(42:50)	3時が成項(1)組2・和前可以時後機能解除。金工制分成次下 (本項)構造得分空白・近下(1)分支が成果(時道・南空朝 著考列在算意範觀之外的介面。 夏一 伊 求者範範的開稿:	「 した 取 した した した した した した した した した した	
<ul> <li>医胃炎系统管理的</li> <li>医胃炎系统管理的</li> <li>生素和成素的管理的</li> <li>動於点下列的陶器中位</li> <li>自動管理師會業等者</li> <li>使用 enco # 位著學派 • 引</li> </ul>	<ul> <li>現在入場一部位立体の設定など、が成功下では、またまた</li> <li>構成の主体、方法を(第二)(第二)(第二)(第二)(第二)(第二)(第二)(第二)(第二)(第二)</li></ul>	3かが成果(1962-100可以用供供給給料料。企工10分用以下 (本項) 構造用料空白-16下1か学ぶか成果(時道・南三朝 著考別在算成業観之外的介面- 夏ーレ 式名集節的目稿: 夏一レ 式名集節的目稿: 前部名含活業 前部は解読業 約	(URE)	

圖 29 設定探查範圍的組態

輸入 IP 位址或範圍,然後按一下 [新增包含清單] 或 [新增排除清單] – 這樣 IP 位址或範圍 就會新增到適當的清單。 您一次只能新增一個 IP 或範圍。如果您稍後想從清單移除其中一個,則可按一下清單右 側的 [移除]。完成時請按一下 [繼續]。

- 若要管理範圍,請在[單一 IP 或者範圍的開端]欄位中輸入第一個位址,然後在[範圍的末端]欄位中輸入最後一個位址,再按[新增包含清單]。範圍可以跨過幾個網路。如果有任何的範圍或者位址不可以或者不應該探查,請按一下[新增排除清單],在排除範圍中新增項目(如下所示)。
- 若要管理特定 IP 位址,請在 [單一 IP 或者範圍的開端] 欄位中輸入位址,然後保留
   [範圍的末端] 欄位空白。按一下 [新增包含清單] 將它新增到清單中。一般來說,這些 是指在範圍之外的節點,例如公司委託網外主機代管的任何伺服器。
- 若要排除某個範圍,請先輸入第一個位址和最後一個位址,然後按一下[新增排除 清單]。
- 若要排除單一 IP 位址,請在 [單一 IP 或者範圍的開端] 輸入位址,然後保留 [範圍的 末端] 欄位空白。例如,您想要排除印表機。
- 範圍可以跨過幾個網路。在大部分情況下,您只需要在已經包含的範圍內,指定某個 範圍即可。
- 若要排除特定 IP 位址,請在 [單一 IP 或者範圍的開端] 欄位中輸入位址,然後保留
   [範圍的末端] 欄位空白。按一下 [新增排除清單] 將它新增到清單中。

注意:「排除清單」的優先順序高於「包含清單」。因此,如果「包含」範圍落在「排除」範圍之內,該「包含」範圍就不會被視為包含(因為您已經排除它了)。為了避免此問題,請限制「排除」範圍 – 範例:您有一部 Server 的 IP 位址位於不是由您所管理的子網路中。除了排除整個範圍並包含那一個 IP 位址之外,您還可以建立兩個「排除」清單 – 其中一個清單排除到該位址之前的位址為止,另一個清單則從下一個位址開始,一直排除 到該範圍的末端

#### 範例

不過,您可以從包含範圍中排除特定 IP 位址 - 例如您不想管理的特定伺服器。舉例來說,您包含了這個範圍的 IP 位址: 192.168.0.1 到 192.168.0.255。在這個範圍內,您可以指定不想要管理的一個 IP 位址 (192.168.0.210)。

您也包含了在指定要管理的範圍之外的特定 IP 位址 (192.168.5.100)。這是良好的設定方式。不過,因為 CC-NOC 會先排除該範圍再包含您要管理的特定位址,所以如果您排除的 IP 範圍涵蓋了特定 IP (例如排除 192.168.5.10 到 192.168.5.150),就有可能發生問題。

### SNMP 社群

CC-NOC 使用 SNMP 通訊協定,從支援此通訊協定的裝置中收集效能資訊,並提供簡單的方法,用來檢視網路上特定裝置的效能圖表。

SNMP 實施的安全機制稱為「*社群連線密碼*」,與密碼類似。CC-NOC 需要「*取得社群連 線密碼*」(通常稱為「*唯讀社群*」),才能存取 SNMP 效能測量值。因為社群連線密碼是 按照裝置進行組態設定,因此您需要輸入的社群連線密碼數量會隨環境的狀況而定。有許 多企業是整個企業都使用同一個社群連線密碼,也有其他公司是每部裝置或每一類裝置就 設定一個社群連線密碼。



若要編輯 SNMP 社群連線密碼,請按一下 [新增新的社群]。

上一頁 • 🕑 · 💌 📓 🎧 🎾 按尋 🏫 邦的局景 (	0 Ø· 🖗		
0 • 🕘 https://192.160.43.251/admin/configuration/mmp/mmpForm.jsp			🗲 输入中义,直接搜索 💌 🔁
<b>ERaritan.</b> 2006/7:31 下午 10:38:37			
19 資別			
windCenter NOC 250 使用 Share 通訊编定收集支援這個通訊编定裝置的	效能資訊,而且提供這一個容易的方法植成網路上特定萎縮	的效能圖 -	
· 資源的安全線制編集「 <i>計算集解度碼</i> 」(Connunty Strings) · 復請似定 動入の計算連絡安認の計算器度描述は予約素。 時本 企業具務価企業は	调的方式。CommandCenter NOC 250要求 ( <i>取得台群環境)</i> 第一一個計算環境安認,可算你公司目是統論新國際環境完	明(時常編爲建備任成)以存取 Share 的效能测量 一個計劃連絡安護。	值。因爲社群連線密碼是按照装置於定。因此也
8.人的社會理由中心的意思是我们的外心的心态。11步至黑星星星星星星星星星星星星星星星星星星星星星星星星星星星星星星星星星星星	· 相對下列您的社群定義, 按照當要新聞、編輯或者移動社	- 回时167元490.000 ·	
潮動的社群			
and a first of the second			
1收牙線密碼 1有新計戶信 (sage 計劃定錄	SIMP @#	包含的位址。範圍	87980
CONTRACTO OVER TAXITOON			
	[unit: 333]		
	continue >>>>		
spit & 1999-2008 Raitan, Ins.	continue >>>>		
sant & 1999 2008 Rantan, fins.	continue 🔊		
1944 0 1999 2000 Martan, Inc.	continue >>>>		
1010-1009-2009 Raitan, Inc.	continue 🔊		
1918 1000 2008 Raitan, 164.	continue >>>>		
Lett & 1999-2008 Nattan, No.	confinue >>>>		
Lan o 1000-2008 Hartan, Ins.	confinue 🔊		
rgnt & 1000-2000 Rattan, Inc.	continue 🔊		
1944 0 1999 2000 Raitan, No.	continue >>>>		
ren o 1999-2008 Nartan, INS.	confinue >>>>		
Lan o 1999 2008 Kartan, Ins.	confinue >>>>		
rgato 1999-2008 Kartan, Ins.	confinue >>>>		
1994 0 1999 2000 Battan, Inc.	continue 🔊		
1491 0 1999-2008 Nattan, No.	confinue >>>>		
1910 - 1999 2008 Bartan, Inc.	confinue ≫		

圖 30 設定 SNMP 社群連線密碼的組態

將範圍或者位址新增到社群,一次一個。若要輸入範圍,請在 [**單一 IP 或者範圍的開端**] 及 [**範圍的末端**] 欄位填入,然後按一下 [**新增位址/範圍**]。若要輸入單一位址,只需保留 [ **範圍的末端**] 位址空白即可。請注意,您必須為每個連線密碼提供一個 IP 位址或者範圍; 如果您想對 CC-NOC 管理的所有裝置提供一個 SNMP 連線密碼,只需將範圍指定為 0.0.0.0 - 255.255.255.255。按一下 [**繼續**]。

注意:您想要收集其 SNMP 效能及目錄資訊的任何裝置,都需要「社群連線密碼」。

### ISP 閘道

CC-NOC 會以特殊方式來處理 ISP 閘道。如果在此處設定組態,則可監視 ISP 閘道是否可用,並且單獨提出報告。如果狀況允許,請指定您閘道的 TCP/IP 位址。如果您沒有這項資訊,您的 ISP 就應該能夠提供,或者您可以從受管理網路上的電腦追蹤連線到網際網路的路徑,以取得這項資料。

		A 13	
<form></form>	)上一頁 • 🙄 · 💌 📓 🎧 🎾 投母 쑰 热的感觉 🥝	12·4	
	20) • 🕘 https://192.168.43.251/w/min/configmation/inp/inp/form.jsp		← 始入中文,直接就非 💌 🄁
PAGE TOTAL CONTRACT ON TOTAL CONTRACT ON THE CONTRACT ON THE SECTION OF ME * 211 実現出版 * 211 実現出版 * 211 実現主法 * 211 実用 * 211 生用 * 2	2006.7/31 F4 10:44:37		
mend new for som State Som State Som State Som State Source Sou	P 解謝		
<ul> <li>・ Microsoft Wendows考慮者: 私行 tracet way, yubao, com 指令: * 2000 (北京立会社 2000 大阪市内市会社 2000 大阪市会社 2000 大阪市内市会社 2000 大阪市内市会社 2000 大阪市内市会社 2000 大阪市会社 2000 大阪市内市会社 2000 大阪市内市会社 2000 大阪市内市会社 2000 大阪市会社 2000 大阪市会社 2000 大阪市会社 2000 大阪市会社 2000 大阪市内市会社 2000 大阪市内市会社</li></ul>	ntmandCenter NOC 250 肠结的 ISP 開產當做時別就说處理。如果在此處說定, 您可以從管理的網路上的電腦泡販達練到網際網路的船徑。以取還這項資料	可針對有用性監疫您的 ISP 開連,並且單環現出報告。如果就況尤許,指定如	B的開車的 TCPAP 位址。如果想並沒有這項波訊,您的 ISP 應該能夠提供,成
2度・道鉛端位是不分表的。 如果那不错提供 ev 位址,調刷入 & AAAA 的位址。 sp 期間: ① ① ① ① ① ① drvvs 是 Morouff Ceparator 在美丽印度性态变化性质的变化的原始。 pright # 1989 2008 Rates, has	● UNEX 電腦:執行 traceroute vew.yahoo.com指令,並且導送さ ● Microsoft Windows0 電腦:執行 tracert vew.yahoo.com指令	您的体地網路之外,但是屬於您的 ISP 的第一個 TCPIP 位址或者 DNIS 名稱。 ,並且尊其在您的本地網路之外,但是屬於您的 ISP 的第一個 TCPIP 位址或有	考慮在這個造影歸線上出現 WAAN 介面的可能性。 費DNS 名稱。
ser Min : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	注意,這個階位是不必要的。如果想不想提供 ISP 位址,請輸入 0.8.8.0 的位	t.	
un		ISP 開選:	
aron 着 Morouff Capacaton 在美丽的环代放花花的描述中的描述		0 0 0	
pript N 8-1989 2000 Renter, Inc.	dows 是 Microsoft Coporation 在美丽和其他語家,地區的过用面標。		
yrigh 8 1000 2005 Karlan, Ina		continuae >>>>	
	pright & 1999-2009 Raitlan, Inc.		

圖 31 設定 ISP 閘道的組態

輸入 ISP 間道的 IP 位址。您可以使用下列秘訣:

- UNIX 電腦:執行 traceroute www.yahoo.com 指令,並尋找位於本地網路之外且屬 於您 ISP 的第一個 TCP/IP 位址或者 DNS 名稱。考慮在這個追蹤路線上出現 WAN 介 面的可能性。
- Microsoft Windows® 電腦:執行 tracert www.yahoo.com 指令,並尋找位於本地網路之外且屬於您 ISP 的第一個 IP 位址或者 DNS 名稱。

注意:這個欄位不是必要的。如果您不想提供 ISP 位址, 請輸入 0.0.0.0 的位址。

按一下[繼續]。



### DNS 伺服器

DNS 伺服器讓系統能夠把 IP 位址轉譯成有意義的名稱。您必須至少輸入一個 CC-NOC 能夠確實到達的 DNS 伺服器。

- 輸入名賽伺服器的位址   Admin   Raritan CommandCenter NOC 250 - Microsoft Ia	ternet Explo	ner						
(葉の) 編輯(E) 被視(V) 我的最愛(A) 工具(T) 説明(E)								
🕽 上一耳 ・ 🙄 💿 🔝 😭 🌈 説母 👷 物的教業 🚱 🔗・	-							
姓の) ・ 🕘 https://152.168.43.251/ed.min/configmation/temeservers/temeservers/form.jsp							← 输入中文,直接按非	2 🔁 8
2008/7/31 F# 10:44:54								
输入名稍伺服器的位址								
NE 你服務讓系統影響記 P 位址群律成有意義的名稱。請輸入最少一個 CommandCenter NO 取述。	C 250 能夠確	赛到建的	DNS 伺服器	·病您最快	的本地间服器放在希望	的最頂端・如果忠宗有名	4續從服器好輸入,可以使用位址 127.0.0.1 作	a.
NNS 间服器是在 NetBIOS 和 Windows 網路環境中使用,可跨過子網路邊界解析 NetBIOS 名 NNS 间服器的空址。	<b>新</b> •如果您爸	同理的映画	子網路・其	中有经重超	随用 NetBIOS 名質・司	使用的是 Wes 间腺廢弃	管理這些電腦的名稱,請在提供的欄位內戰。	κ.
	主要 pers							
	192	168	43	1	-			
	大要 DHS							
	1	1	1	. 1				
	第三套日	HRS :		-				
	2	2	1.12	2				
	WINS FILM	(器):	1	10-	-			
	-				- 05			
		cont	inue 3333					
		-	141					
opyright @ 1999-2000 Kartan, Inc.								
194.48							0.000	

圖 32 設定 DNS 伺服器的組態

請儘可能將最快的本地伺服器放在清單最頂端。WINS 伺服器是在 NetBIOS 和 Windows 網路環境中使用,可跨過子網路邊界解析 NetBIOS 名稱。如果您管理的幾個子網路所包含的電腦使用 NetBIOS 名稱,但使用 WINS 伺服器來管理這些電腦的名稱,請在提供的欄 位內輸入 WINS 伺服器的位址。輸入 DNS 伺服器之後,請按一下 [繼續]。

### 電子郵件通訊

這些設定會影響 CC-NOC 與您溝通的方式。此頁面可讓您設定 [通知] 的「寄件者:」電子郵件位址以及 SMTP 轉送設定。此畫面也會提供如何遠端支援 CC-NOC 的相關資訊。

**注意:**重要的是,要隨時更新此資訊並確定指定正確的電子郵件位址,因為 CC-NOC 會使 用這些電子郵件位址來傳送重要裝置的狀態資訊。

電子郵件通訊組動設定   Admin   Raritan CommandCenter NOC 250 - Microsoft Internet Explorer	
(電行) 編輯(四) 檢戒(7) 裁約與愛(A) 工具(7) 説明(页)	
3 L-A · 🔘 · 🖹 🖉 🚯 🔎 194 👷 1608% 🥝 🍰	
建②) + 🕘 https://192.168.43.251.hdminkconfigurationkomministionkomministionForm.jp	← 始入中文,直接放案 💌 🛃 😣
<b>王王Raritan.</b> 2008/7/31 下午 10:45:20	
電子郵件通訊紙物設定	
這些設定影響 CommandCatter NOC 250 如何與您清後。 扁時保持這道會料最新,以及種形指定的電子關係位並是有效的,這是非常重要,因素這些電子關係在並是而來構造重要得重的於	创业的总管理具。
系了傳送電子郵行通知:ConnewCenter NOC 200 需要知道如何得送電子郵行。如果软泥尤指,ConnewCenter NOC 200 用但用记的半地 SMIP 服務傳送電子郵件。然而,某些網絡並不接 例子94的 SMIP 网路播的 P 位址。	受不明束得的電子都件。如果状況如此,講提
SMTP 位服器	
③使用Ps提的 SMTP(提出 DHS MX 記録)	
○使用在下列 IP 位址的地端 SMTP 何厭器	
<b>非正电子都</b> 件	
输入供基础通知期则使用的電子都件位址。所有從 CommandCenter NOC 250 活出的電子都件 (例如,電子解件通知) 將形與不由於這個位址。如果您並未在此處提供一個數值,將會使用預	12道 -
ronf@nerve2K1 raleigh raiitan com	
密理局徵字#科拉址	
职入您公司負責管理 ContrandCenter NOC 250 人員的電子都件拉挂。這個電子都件拉挂指用來傳送 CommandCenter NOC 250 裝置本身的試驗提訊。	
larry.karnowski@rantan.com +	
使用下列的 ( <b>测试 samp 設立</b> ) 按钮,指备利用指定的 samp 伺服器像进一份测试電子模件,容到在 ( <i>管理具 每子 模件 位给</i> 模位内指定的電子都件位址。读项测试证明 CommandCetter NOC	250 能夠經由過當的網路連線準泛電子郵件訊
Muk shirp are:	
Public and a 1000 YOM Russian Tax	
organise instances in the second s	
	0 0 total

圖 33 設定電子郵件位址設定的組態

為了傳送電子郵件通知,CC-NOC 必須知道如何傳送電子郵件。如果狀況允許,CC-NOC 將使用它的本地 SMTP 服務來傳送電子郵件。然而,某些網路並不接受不明來源的電子郵件。如果是這樣,請按一下 [使用在下列 IP 位址的遠端 SMTP 伺服器],並提供 SMTP 伺服器的 IP 位址。

在 [**傳送電子郵件**] 所指定的電子郵件位址,會詳述基礎通知機制將使用的電子郵件位址。 所有從 CC-NOC 送出的郵件(例如電子郵件通知)將形同來自於這個位址。如果您並未 在此處提供值,則會使用預設值 (root@localhost.com)。

在 [管理員電子郵件位址] 所指定的電子郵件位址,應該是組織中負責管理 CC-NOC 的人員的位址。這個電子郵件位址是必要欄位,且會用來傳送 CC-NOC 本身的狀態資訊。

按一下 [**測試 SMTP 設定**],即可使用指定的 SMTP 伺服器,將測試電子郵件傳送到 [**管理 員電子郵件位址**] 欄位所指定的電子郵件位址。這項測試可證明 CC-NOC 能夠經由適當的 網路連線傳送電子郵件。

按一下 [繼續]。

### 套用組態設定和重新啓動

您已經利用「第一次組態設定精靈」完成初始組態設定。您可以按一下連結,重新進入組態設定,如下所示。您也可以存取這項組態設定資訊,方法是在完成這個精靈之後,按一下 CC-NOC Web 使用者介面的 [管理] 索引標籤。

教心組織院定務書 I Admin I Rarritan CommandCenter NOC 250 - Microsoft Internet Explorer	
(案(F)编辑(E)	
) 1-17 • 🕤 · 📓 🕼 🔎 1980 👷 1908 🛪 🥹	
性の) ・ 👜 ImpuH 192 160 43 251 hdminkonfigunskonfinntineFraink.jsp?gotsOnSuknin-firstinekvined&batten Type-0	🗲 输入中变,直接频率 😁 🎦
<b>E Raritan.</b> 2006/7/01 15/4 10:45:38	
那一次相想設定時間	
已經完成必要的組織設定網頁。如果想想繼續設定 ConnandCerter NOC 250 的組織,可以進入這個網頁應能所總額的組織設定網頁。這邊 ConnandCerter NOC 250 的 [ 世際	朝貢,您可以重新進入所有必要的和建議的組修說定朝貢。
會認定成所有要求的組織認定相互,按一下這個相互相思想的( <i>律用這些最后因素所含約</i> ,按鈕,這樣會重新留動 ConnandCenter NOC 250,開始觀話認的網絡。	
必要的細想設定網頁	
<b>业一下下列任何一個课結,就可重新導入該組織設定網頁。</b>	
<ul> <li>課題の紙幣数定。構算</li> <li>編励2年 Webuer 客理</li> <li>細胞2年 Webuer 客理</li> <li>細胞2年 展開2年展開25 長期36</li> <li>○ 最短2年 展開26 長期36</li> <li>○ 人類公開26 会別21 長期46</li> </ul>	
<b>在用如果得定和事好物面</b>	
Secretaria (1990) NOVA Busines Iso	
ojsnjim o tese-uko nastan, mc	

圖 34 套用組態設定和重新啓動

您已經完成組態設定精靈,但是尚未確認變更。如有需要,您也可以組態設定 Windows 管理及入侵偵測 – 若需額外資訊,請參閱〈第6章:Windows 管理、入侵偵測 及效能監視〉。

若要儲存所有變更,請按一下[**套用組態設定和重新啓動**],這樣就會顯示此畫面。

🗿 Applying First-Time Configuration   Admin   Raritan Network Management Appliance - Microsoft Internet Explorer	I I I I I I I I I I I I I I I I I
File Edit View Favorites Tools Help	1
🔇 Back 👻 😥 🔹 🕼 🔎 Search 🤺 Favorites 🜒 Media 🤣 🎧 😓 💷 💷 💷	
Address 🕘 http://192.168.53.76/admin/configuration/firsttimeApply.jsp	Go Links »
NAdobe - 🍸 - 🖉 - 💌 Search Web - 🚍 - 👾 🖂 Mail - 🐼 My Yahool 💽 Games - 😕 🥱 Snagit 🖃	
<b>Raritan.</b> 7/28:05 4:55:58 PM	
Please Wait for the Network Management Appliance to restart	
All Web Console links will be unevaliable until the system has completed its reinitialization in just a few minutes. You can revisit any of the configuration pages you just completed by visiting web console.	g the Admin section of the

圖 35 CC-NOC 重新啓動

CC-NOC 將重新啓動,並開始探查網路裝置以進行監視。



### 還原來自其他 CC-NOC 系統的組態設定

使用 CC-NOC 的「下載備份」及「上載備份」功能,就可以將來自一個 CC-NOC 系統的 資料遷移到另一個 CC-NOC 系統。這對於取代毀損的裝置,或升級 CC-NOC 系統 (例如從 CC-NOC 250 升級到 CC-NOC 2500 分散式系統)尤其有用。

遷移資料有一些基本需求:

- 必須從來源 CC-NOC 系統下載備份資料。
- 目標裝置必須經過授權(遷移時不會傳輸授權)。如果您需要目標裝置的授權,請造訪 力登支援中心(網址是 <u>http://www.raritan.com/support/</u>),並按一下「CC-NOC 授權請 求」(CC-NOC License Request)連結。
- 如果目標是分散式 CC-NOC 系統,則所有衛星裝置也必須經過授權和啓動。
- 如果目標系統是新的機器,則必須先完成初始組態設定精靈。
- 必須已從與目標裝置相同的韌體版本,或前一版的韌體建立備份。您無法還原早於前 一版的 CC-NOC 資料到目標裝置。

此外,請注意,您只能將資料遷移到相同類型或更新的 CC-NOC 系統,您無法「降級」 您的系統 (例如,將資料從 CC-NOC 250 遷移至 CC-NOC 100)。下表描述有效的遷移可 能性:

來源 CC-NOC 系統	Target CC-NOC Systems					
	CC-NOC 100	CC-NOC 250	CC-NOC 2500N, M, S			
CC-NOC 100	有效	有效	有效*			
CC-NOC 250		有效	有效*			
CC-NOC 2500N, M, S			有效			

注意:如果您正在從使用外部 Proxy 來收集 Windows 管理資料的 CC-NOC 100 或 250 遷移 到 CC-NOC 2500 設定,則目標 CC-NOC 2500 系統會使用該外部 Proxy,而非使用 2500M 裝置作為內部 Proxy。如果您在遷移之後有任何與 Proxy 相關的問題,則請聯絡力登技術 支援中心。

依循下列一般程序,將資料從一個 CC-NOC 遷移到另一個 CC-NOC:

- 1. 登入到來源 CC-NOC 系統。
- 2. 從來源 CC-NOC「下載備份檔案」,並將備份檔案存入您的用戶端 PC。
- 3. 登入到目標 CC-NOC 系統。
- 4. 從用戶端 PC「**手動上載備份檔案**」到目標 CC-NOC 系統。這個檔案現在應該會出 現在目標系統的備份清單中。
- 5. 在目標系統上「**安裝備份檔案**」。

注意:為了充分使用分散式 CC-NOC 系統的備份,目標系統至少應具備與來源系統一樣多的裝置。例如,如果來源系統有兩個 CC-NOC 2500M 裝置,則目標系統也應該有兩個 2500M 裝置如果目標系統只有一個 2500M 裝置,則您仍可以執行遷移,但是在還原期間 只能對映一組 Windows 管理資料。另一組必須被捨棄。

同樣地,從 CC-NOC 100 或 250 遷移到分散式系統時,因爲獨立式系統 (CC-NOC 100 及 250 機型) 會收集所有資料類型,所以目標系統應該包含至少一個經過授權且已啓用的 2500N、2500M 及 2500S 裝置。如果目標系統沒有包含其中任一項,則您將無法在還原程 序執行期間對映所有資料。



### 下載備份檔案

注意:This 此步驟發生在舊的 CC-NOC 系統上,其中含有您想儲存的組態設定。

建議以週期性或定期性的方式下載備份檔案。

- 1. 在最頂端的瀏覽列中,按一下「管理」標籤。
- 2. 按一下「進階管理」。
- 3. 按一下「資料備份和還原」。
- 4. 按一下「下載備份檔案」。

#### 下載備份歸檔

按一下下列任何一個備份歸檔,以下載到您的電腦。

備份歸檔	日期	大小	版本
backup-5.5.2-20061212010516.dat Daily backup	2006/12/12	20.173 MB	5.5.2
backup-5.5.2-20061211010517.dat Daily backup	2006/12/11	19.867 MB	5.5.2

圖 36 下載備份檔案

5. 按一下某個檔案開始下載。

#### 手動上載備份檔案

注意:此步驟及所有後續的步驟會發生在新的 CC-NOC 系統上,即組態設定要遷往的系統。

若要上載組態設定檔案,必須先從某個 CC-NOC 系統下載它。已建立「上載檔案:」對話方塊來方便上載。注意,只有力登有效的備份檔案可以上載到這個裝置。上載其他的檔案可能會造成裝置出問題,也可能讓您的保固失效。

- 1. 在最頂端的瀏覽列中,按一下「管理」標籤。
- 2. 按一下「進階管理」。
- 3. 按一下「資料備份和還原」。
- 4. 按一下「**瀏覽:**」
- 5. 選擇要上載的備份檔案,然後按一下「開啓」。
- 6. 按一下「**上載**」。

順利上載檔案之後,它會出現爲新 CC-NOC 系統上的可用備份。

### 安裝備份檔案

CC-NOC 上會保留一份可用備份檔案的清單。針對其中一個備份檔案按一下「安裝」,就 會將存在該檔案中的組態設定還原到 CC-NOC 系統。來自其他 CC-NOC 系統的組態設定 檔案,在手動上載它們之後,也可從這份清單取得。

- 1. 在最頂端的瀏覽列中,按一下「管理」標籤。
- 2. 按一下「**進階管理**」。
- 3. 按一下「資料備份和還原」。
- 4. 按一下「**安裝備份檔**」。

#### 安裝備份橋 按一下 [安朝]按鈕,就可安裝下列任何的備份檔。如果某個備份檔顯示為 下數中,當全部下載完成後,就可供安裝。 諸注意,只有 5.0 或更高版本的備份檔才可供安裝。 進備安装 版本 有刑 登行的 已下載完成 backup-5.5.2-20061212010516.dat 552 Backup 2006/12/12 2006/12/12 安装 ... 2006/12/11 2006/12/11 安装... backup-5.5.2-20061211010517.dat 552 Backup

#### 圖 37 安裝備份檔

5. 按一下緊鄰備份檔案的「**安裝**」,以安裝檔案。只有來自裝置目前版本或前一版的備 份才能用來安裝。

注意:如果您需要安裝較舊的備份,請聯絡力登技術支援中心。

- 6. 您可以按一下備份檔案名稱,檢視檔案的詳細資料。
- 7. 會出現「備份檔案組態設定」(Backup File Configuration)畫面。這裡會顯示儲存在備 份中各式各樣的資料類型。收集資料之裝置的序號會顯示在「來源裝置」欄位中。用 來復原資料的裝置清單會顯示在「目標裝置」欄位中的下拉式清單中。

來週裝置	装置類型	包含的範圍/位址	排除的範圍/位址	目標装置	狀態
ACF6600034	Network Management	192.168.32.56 - 192.168.32.63	192.168.32.57	ACF6600034 💌	
ACF6600034	Network Performance			ACF6600034 💌	
ACF6600034	Intrusion Detection			ACF6600034 💌	
ACF6600034	Vulnerability Scanning			ACF6600034 💌	
ACF6600034	Windows Management			ACF6600034 💌	

#### 圖 38 將資料還原到來源裝置

8. 將每一組收集的資料對映到適當的裝置,方法是在「來源裝置」欄位中選擇序號。例如:如果將兩組 Windows Management 資料還原到含有兩個 CC-NOC 2500M 裝置的分散式環境,則請替第一組資料選擇一個 2500M 的序號,再替第二組選擇另一個 2500M 的序號。或者,如果您不想還原一組資料,或無法將它對映到適當的裝置,則可以選擇「捨棄」。

注意:如果您捨棄資料,以後就不能再還原它。這個資料會永久流失。

9. 按一下「**安裝**」可按照表格中的對映方式將資料還原到裝置。CC-NOC 系統會自行重 新啓動,而且需要等幾分鐘,它才會重新初始設定。



## 第5章:確認和微調安裝

CC-NOC 已經組態設定完成,且已經執行它的探查程序,也已經將服務指派給類別...現在要做什麼呢?每個環境各有不同,形成的挑戰也各異。知道要尋找什麼以及如何解決問題,是判斷您是否會使用並精通 CC-NOC 的重要因素。

因爲您在安裝之前已經花費時間來收集資訊和設定適當的期待結果,所以下列幾個項目應該很容易完成。

## 登入 CC NOC

開啓瀏覽器並指向 CC NOC 的 IP 位址 http://<CommandCenter\_NOC\_IP\_Address>。這 是稍早指派的 IP 位址 – 若需額外資訊,請參閱〈第3章:實體及網路安裝〉。您會看到 登入畫面。

CommandCenter® NOC 250
使用者名稱:
密碼:
登入

圖 39 CC-NOC 登入畫面

預設使用者名稱是 admin,而密碼是 raritan。如果您尚未將它變更爲較安全的密碼,請 立即這樣做。然後就會顯示首頁:

🕮 Raritan.		NX+5 *# #X 2# 167 N	1881 AR 379		A (2011)
CommandCenter® NOC 250	ant to the second second		A sitter and a second	the strategy of the second second	
006/7/24 上午 03:22:09 U形像: edmin	#285.中156	8106 N 82	服用	可用作	入校績器
	目前沒有網路中斷可以釐示。	網路介面	18	100.000%	0全部提訊
<b>花技母:</b>		新草和品子绿	0	100.000%	
15 THE R	silou	影曲器	1	100.000%	Windows 管理
aferra	重要的通知: admin 第 22 例语的	何服器	服務	可用物	1 Windows (和語語
管理联盟: 重要的通知:20	全部 23 個通知	#105(10)积 88	23	100.000%	14 Windows 工作站
	I書檢查地的通知 醫檢查至然的公開通知	電子郵件伺服器	5	100.000%	A 1718-0117
前的網絡中斷 0 要約事件: 3,617		DHIS TO DHCP (TOUR ME	4	100.000%	0 SOL (TURIS)
	5125 SV2A	W #4 mk (mbR ab	1	100.000%	Active Directory (ILE)     Active Directory (ILE)
enmandCenter Secure	上次完成的歸饋:		<b>E</b> a	可用性	1 KING DE N
2.168.0.3	間数: 2006/7/19上午 09:00:00 数束: 2006/7/19下午 05:52:06	整體服務可用性	54	100.000%	應用程式目錄
理員軟態: 自開約	が加え 50 朝鮮ないない。 (1947年) 44530 (1947年) 44630	Ť.	過去24小時的四分比 檢視所有類別		
NEWEW:MM	·····································				由未收集到任何流量分析的资
	Canvright @ 1999-2006 Raritan Inc.				

*圖* 40 CC-NOC 首頁

進入之後,您就會看到各種不同的網路中斷欄位顯示「0於0」;這表示探查程序尚未 開始。

一旦您看到數字開始變更,就表示探查程序已經開始。探查所花費的時間長度,是根據 CC NOC 必須探查和測試的個別 IP 位址數量而定 – 這可能是數個小時,但如果是較大的 環境 (5+ class-C),也可能會花上整天。

執行探查程序之後,請確認結果。



## 第1天

### 抽樣探查

**CC-NOC** 完成「探查」程序之後,請確定它已經探查您參與的節點。另外也請確定您需要的服務與這些節點相關聯。如果遺失節點,或是受管理節點中有您不需要的節點,請參閱本章稍後的〈**微調**〉一節來清理安裝。

### SNMP 收集資料

讓 CC-NOC 收集資料一天之後,請按一下 CC-NOC 介面頂端瀏覽工具列上的 [**報告**] 索引 標籤。然後按一下 [SNMP 效能報告]。

請記下哪些節點正在收集 SNMP 資料,並抽樣檢查資料是否出現。如果您看到的節點與您 需要的節點有差異,請確認您想收集其 SNMP 資料的節點都已啓用 SNMP,且 CC-NOC 已有適當的「唯讀社群連線密碼」(如果有的話)。

### 第2天

執行探查程序之後,請確認已經正確設定下列各項的組態:

#### SSH

只要力登能夠以 SSH 方式存取 CC-NOC,力登就能協助您進行部署、驗證及微調。請先 確認此連線,再繼續進行下列步驟。若要確認 CC-NOC 能夠正確通訊,請進行下列任一 動作:

- 1. 聯繫力登技術服務中心來進行快速連線測試,或是
- 2. 按一下[說明] 選單下的 [建立支援連線]。

CC-NOC 會建立與力登伺服器之間用於遠端存取的連線。建立連線之後,力登技術支援人員就能夠直接連接到 CC-NOC,來診斷裝置或修正裝置的問題。連線完全隱密且安全,並使用業界標準的加密方案,在連線期間為出入裝置的所有流量進行加密。

**注意**:建立連線不一定會使支援人員收到警示,所以如果發生需要特別注意的問題,您仍 有需要致電或以電子郵件通知技術服務中心。

#### SMTP

最重要的一點就是 CC-NOC 能夠將電子郵件傳送給適當的人員以取得通知。有兩種方法可以確認 SMTP 是否正確通訊:

- 1. 從 CC-NOC 聯繫力登技術服務中心,並要求對方產生電子郵件訊息。
- 各用通知,然後引起或模擬會傳送通知的事件。若需額外資訊,請參閱(第7章:開始使用)。

### 微調

完成確認安裝及組態設定之後,下一個步驟就是微調設定。微調是由下列步驟所組成:

- 改變用來管理節點及服務的設定。
- 新增「自訂輪詢器」(如有需要)。

### 清理安裝

探查完成之後,便會將每個系統分類成伺服器、基礎設備裝置或工作站,並指派適當的授權(如果有的話)。您應該查看 CC-NOC 已經探查過的節點及服務,以及它產生的初始 事件。這樣會提供詳細資料,讓您知道哪些區域需要進一步調整。請特別注意下列事項:

- 應該受到管理卻未出現在清單中的節點或服務。
- 您不想管理的節點或服務(請參閱下列附註)。
- 您不想管理的非嚴重服務的事件,或是包含在可用性計算中的非嚴重服務的事件

**注意:**如果您在一天結束時看到大量的網路中斷,有可能是因為在管理組態設定中,將使 用者工作站電腦以輪詢方式視為基礎設備裝置。較爲適當的作法是將這些系統的管理授權 變更爲「工作站」授權。

若要清理安裝,請依序按一下 CC-NOC Web 使用者介面頂端的 [管理] 索引標籤、[網路管 理組態設定] 及 [編輯探查的範圍]。這時您就可以輸入要包含或排除的新範圍。

此外,您也可以按一下[管理]索引標籤,再按[網路管理組態設定]下的[管理、未管理、 重新掃描或者刪除裝置],為發現的所有裝置調整管理設定。如果有授權(根據您使用的 CC-NOC裝置機型而定),您就可以在這裡為每個裝置變更授權類型。

#### 新增/移除輪詢器

即使您比較可能會使用已經設定組態的輪詢器,也可以視需要新增任何額外的輪詢器或停 用預設的輪詢器。例如,您的主從式帳戶處理應用程式使用 TCP 透過連接埠 5252 進行通 訊。您可以設定輪詢器的組態來監控連接埠 5252 上的 TCP 服務。

注意:您監控的不是應用程式本身,而是它提供的網路服務。

- 1. 在頂端的導覽索引標籤列中,按一下[管理]索引標籤。
- 2. 按一下 [網路管理組態設定]。
- 3. 按一下[設定輪詢器的組態]。
- 4. 捲動到頁面底端,然後按一下[新增自訂輪詢器]。
- 5. 輸入新輪詢器的名稱。
- 6. 選擇用於輪詢服務的通訊協定,例如 TCP。
- 7. 輸入它藉以通訊的連接埠。
- 8. 按一下[設定作用中]核取方塊。
- 9. 按一下 [新增]。

如果您不要輪詢特定服務,請按一下[設定輪詢器的組態],取消選擇[作用中]清單中的輪 詢器,然後按一下[套用變更]。

若需輪詢器的詳細資料,請參閱力登的《CommandCenter NOC 管理指南》。

本頁刻意保持空白。



# 第6章:Windows管理、入侵偵測及效能監視

實際安裝和設定 CC-NOC 裝置的組態之後,您就可以選擇設定 CC-NOC 的組態來進行下列各項動作:

- 開始透過 WMI (Windows Management Instrumentation) 從 CC-NOC 管理的節點收集視 窗資訊。
- 探查網路上的封包並尋找入侵跡象。
- 監視網路的頻寬使用量,並提供窗口讓您了解網路利用率。

在力登的《CommandCenter NOC 管理指南》中,可以找到詳細資料。

注意:如果您使用的是 CC-NOC 100 或 250,則上述所有功能都會在該裝置上執行。如果 您在分散式環境中部署,則「Windows 管理」會移交給 CC-NOC 2500M,並在 CC-NOC 2500S 設定入侵偵測的組態。本節會列出在這兩個環境中,Web 使用者介面的不同之處。

## Windows 管理的概略說明

若要設定 CC-NOC 的組態,使它從受管理的 Windows 伺服器及工作站中,收集和報告 WMI 統計資料,您就必須:

設定代理伺服器的組態-促進 CC-NOC 2500N 與受管理系統之間的通訊。在獨立式環境中,會強制設定外部代理伺服器;但是如果使用已有內部代理伺服器的 CC-NOC 2500M,則可以選擇不設定外部代理伺服器的組態。

注意:如果您使用外部代理伺服器,則建議使用已啓用自動更新的 Windows XP Professional Service Pack 2 (或更新版本),來促進 CC-NOC 與受管理系統之間的通訊。 這個系統造成的資源負荷通常不多,不會在尖峰時刻造成系統的嚴重負荷。

- *指定 Windows 管理範圍* 您必須確認在 CC-NOC 和定義的*代理主機*之間能夠溝通的 TCP/IP 位址範圍。系統會使用 Microsoft 的 Windows Management Instrumentation (WMI) 來管理和掃描這個範圍。
- 指定網域及主機-一旦您確認代理伺服器及範圍,CC-NOC就會開始進行探查程序, 透過WMI來搜尋要管理的目標裝置。對於與您希望管理的主機相關聯的每一個網 域、工作群組或是受信任的網域,您都必須提供認證資訊(例如使用者名稱和密 碼),而此資訊可用來登入系統以及取得效能、事件記錄及/或系統目錄資訊。如果您 願意的話,一旦探查到裝置,您也可以提供有關該裝置的這份資料。請注意,這樣做 是否更爲安全,仍有爭論;但是在管理方面就要更注意。

### 設定外部 Windows 代理伺服器的組態

若要從受管理的 Windows 系統收集 WMI 資料,則需要代理伺服器將 WMI 要求從 CC-NOC 轉寄到受管理的 Windows 系統。您不一定要為 CC-NOC 2500M 設定外部代理伺服器的組態,因為它有自己的內部代理伺服器。

若要設定 CC-NOC 的組態,讓它從外部代理伺服器收集 WMI 資料,則必須:

- 找出要用作代理伺服器的系統。只有已啓用自動更新的 Windows XP Professional Service Pack 2 (或更新版本)才能作為代理伺服器使用。
- 除非您使用的是 CC-NOC 2500M 的內部代理伺服器,否則請下載組態設定工具並加以 執行,這樣才能在環境內設定外部系統的組態,作為代理伺服器來收集 WMI 資料。
- 以適當的使用權限來設定 CC-NOC 的組態,才能與代理伺服器和目標系統(網域或個別的系統使用權限)進行互動。

注意:同時,除非您已經在環境中設定 WINS 伺服器的組態,否則建議您為每個子網路都設定代理伺服器的組態。您也可以在 CC-NOC 2500M 指定 LMHOST 檔案項目以進行名稱解析。

以下幾節說明如何設定外部代理伺服器的組態。

### 外部代理主機需求

為了獲得最佳的結果,建議您使用已啓用自動更新的 Windows XP Professional Service Pack 2(或更新版本),來促進 CC-NOC 與受管理系統之間的通訊。

外部代理伺服器必須符合這些需求:

- 1000 MHz CPU 或更高頻率
- 512 MB 的 RAM 或更高容量
- Windows XP Professional 加上 Service Pack 2 或更高版本
- 網路上的非關鍵性角色

#### 下載和執行 ProxyInstaller

只需兩個步驟就可以設定系統的組態,作為代理伺服器使用。第一個步驟是移除外部系統 上的舊有代理伺服器設定(若您具有一個 5.4 版或更舊版本設定的代理伺服器)。第二個 步驟是安裝新的外部代理伺服器 5.5 版。這些功能皆可藉由執行 ProxyInstaller 來完 成。ProxyInstaller 將會編輯所需的登錄設定,並安裝看門狗服務。。

注意:如果 CC-NOC 5.4 或更舊的版本無法順利使用目前的外部代理伺服器,則建議您升級成 CC-NOC 5.5 代理伺服器。

您必須針對作為 CC-NOC 100、250 或 2500M 之外部代理伺服器的所有 Windows 電腦,重 複這些步驟。CC-NOC 2500M 可作為它本身的 Windows 管理代理伺服器;不需要任何動 作就可以將它遷移至新的組態設定,而且 CC-NOC 2500 的所有更新程式都會自動完成。 若要設定外部代理伺服器的組態:

- 1. 確定您有外部代理伺服器的「管理員」權限。
- 從這個位置下載最新的代理伺服器組態設定程式 ProxyInstaller: http://<address\_of\_noc>/public/ProxyInstaller.zip。
- 將 Windows 電腦上的 ProxyInstaller 歸檔解壓縮,並將目錄移至您想放置程式的 位置。例如,一個良好的位址可以是:
   C:\Program Files\Raritan\ProxyInstaller。
- 4. 連按兩下 ProxyInstaller.exe 即可執行程式。
- 5. 若此 Windows 電腦作為 CC-NOC 5.4 或較舊版本的代理伺服器,您必須先解除安裝舊版的代理伺服器組態設定。按一下「**解除安裝**」,移除舊版的代理伺服器
- 6. 若此代理伺服器將提供 CC-NOC 2500 組態設定,請鍵入將管理此代理伺服器之 2500M 遠端裝置的 IP 位址。若此代理伺服器將提供 CC-NOC 100 或 250 組態設定,請 於可用的欄位中鍵入該「遠端裝置」的 IP 位址。
- 7. 按 [**安裝**] 按鈕,即可利用最新的代理伺服器設定來重新設定外部 Windows 電腦的 組態。

### 開啓目標裝置和防火牆上的連接埠

為了讓 CC-NOC 裝置能夠查詢網路上裝置的 Windows 效能資料,任何目標 Windows 裝置上的軟體防火牆都可能需要修改。任何目標 Windows 裝置上的下列連接埠,都必須接受來自 CC-NOC 2500M 的 IP 位址的流量,或是已經組態設定成外部 Window 代理伺服器之任何系統的 IP 位址的流量:

• 137 udp



- 139 tcp
- 445 tcp

此外,應對任何介於目標裝置、代理伺服器與 NOC 間的硬體防火牆進行設定,以允許這些相同連接埠上的流量。

若要在執行 Windows 防火牆的任何 Windows XP (SP2) 電腦上開啓這些連接埠,請使用下 列程序:

 開啓 cmd 提示並輸入下列指令: netsh firewall set service type = fileandprint mode = enable scope = custom address = <address of external proxy or 2500M>

舉例來說,如果外部代理伺服器或 CC-NOC 2500M 的 IP 位址是 192.168.1.45,您就應該 輸入:

netsh firewall set service type = fileandprint mode = enable scope = custom address = 192.168.1.45

2. 輸入下列指令:

netsh firewall set service type = remoteadmin mode = enable scope =
custom address = <address of external proxy or 2500M>

舉例來說,如果外部代理伺服器或 CC-NOC 2500M 的 IP 位址是 192.168.1.45,您就應該 輸入:

netsh firewall set service type = remoteadmin mode = enable scope =
custom address = 192.168.1.45

依照預設, Windows XP (SP2) 會啓用登錄中的 "Force Guest" 選項。CC-NOC 裝置無法認 證已經啓用 "Force Guest" 選項的 Windows 系統。若要停用 "Force Guest" 選項,您必須使 用下列程序修改登錄:

- 1. 備份登錄。
- 在 Run 提示中,輸入下列指令: Regedit
- 瀏覽找出這個登錄機碼:
   Hkey\_Local\_Machine\System\CurrentControlSet\Control\LSA\Forceguest
- 將 "Forceguest" 機碼的值從 1 (已啓用) 變更為 0 (已停用)。

#### 設定 CC-NOC 組態以與外部代理伺服器通訊

若要設定 CC-NOC 的組態以與網路上的外部代理伺服器通訊,請使用「Windows 管理組態設定精靈」來完成。

「Windows 管理組態設定精靈」是一種用來指定和設定代理主機組態的介面,可促進 CC-NOC 和您管理的 Windows 伺服器和桌上型電腦之間的連通性。這個組態設定精靈能夠帶領您逐步找出代理伺服器、建立認證資訊與特定網域之間的關聯,以及認證資訊與特定主機之間的關聯。

- 1. 在頂端的導覽索引標籤列中,按一下[管理]索引標籤。
- 2. 按一下 [Windows 管理組態設定]。
- 3. 按一下 [Windows 管理組態設定精靈]。
- 4. 按一下 [**開始組態設定**] 即可啓動精靈。



新增新的外部代理伺	殿器			
代理伺服器	網域	使用者名稱	行動	
192.168.43.181	OCULAN	Administrator	測試編報■除	
儲存變更取消				

圖 41 設定外部代理伺服器的組態以進行 Windows 管理

5. 按一下[新增新的外部代理伺服器]。

注意:若要在分散式環境中存取「Windows 管理組態設定精靈」(也就是從 CommandCenter 2500N 存取),請在頂端的瀏覽索引標籤列中,按一下[管理] 索引標 籤,再按[CC-NOC 2500M 組態設定]。選擇[CommandCenter NOC 2500M 組態設定精 靈],或是按一下您目前設定組態之裝置旁的[設定組態]。

#### 找出本地代理伺服器

這裡指定的本地代理主機主要是用來和您管理的一些或所有 Windows 平台進行溝通,讓 CC-NOC 向特定的伺服器或工作站要求資訊,而這個代理伺服器就能夠將它轉換成 Microsoft 專用的通訊協定,並將它傳送給終端系統。

注意:只有在使用外部代理伺服器時才需要此步驟。如果您使用的是 CC-NOC 2500M,就 可以使用它本身的內部代理伺服器。

代理伺服器的 IP 位址:		
*		
网城:		
^		
友用者名稱:		
*		
2语:		
•		
薛認密碼:		
f		
	cancel	continue >>>>



- 6. 輸入代理主機的「**IP 位址**」。這應該就是執行組態工具的主機。若需額外資訊,請參 閱本章稍早的外部代理主機需求
- 7. 為了獲得最佳的結果,建議您使用已啓用自動更新的 Windows XP Professional Service Pack 2(或更新版本),來促進 CC-NOC 與受管理系統之間的通訊。

外部代理伺服器必須符合這些需求:

- 1000 MHz CPU 或更高頻率
- 512 MB 的 RAM 或更高容量
- Windows XP Professional 加上 Service Pack 2 或更高版本
- 網路上的非關鍵性角色
- 8. 下載和執行一節。

注意:此欄位中的主機名稱值必須能夠透過DNS 解析,或者必須是數字 IP 位址。



- 9. 爲 [網域]、[使用者名稱]、[密碼] 輸入值,然後確認密碼。請注意,使用者名稱必須是 該系統上的本地使用者,也就是「本地管理員」群組的成員。
- 10. 按一下 [繼續] 即可繼續進行。

### 指定 Windows 管理範圍

在這個步驟中,您將找出能夠與 CC-NOC 和定義的*代理主機*進行通訊的 TCP/IP 位址範圍。

注意:如果您使用的是 CC-NOC 2500M 的預設內部代理伺服器,請按一下[預設代理伺服器]下的[編輯]來指定位址範圍。

系統會使用 Microsoft 的 Windows Management Instrumentation (WMI) 來管理和掃描這個範 圍。探查完成之後,便會將每個系統分類成伺服器、基礎設備裝置或工作站,並指派適當 的授權(如果有的話)。

注意:建議您不要在探查範圍中包含 DHCP 裝置。不過,受管理的裝置(也就是指派成 「基礎設備裝置或伺服器的裝置)仍有受限制的 DHCP 支援。若為工作站,則必須手動移 除由於 DHCP 位址變更所造成的重複現象。

業間的末端(可選用): 新營食活車 新營沸除済車 和合物開始は 192.168.43.1-192.168.43.254 務件		軍— IP 或者範圍的	開端:	1	
新増包含活車 新増芽酵装車 和合範別がJ# 192168.43.1 - 192.188.43.254 務院 教授/範囲/位生		範圍的末端(可選用	∄):	1	
和合範圍的J# 192.168.43.1 - 192.168.43.254		新赠包含清算	製湯詳解発面	-	
192.168.43.1 - 192.168.43.254 審批 排除範密/应址	包含範圍前非				
排除範圍应生	192:168.43.1 - 192:168.43.254			私胜	
	排除範圍应社				
諸使用上述表格,新增排除的範圍。這是一個可選用的操作。	諸使用上述表格,新屬排除的	カ離園。這是一個可選用	的操作。		

*圖* 43 指定 Windows 管理範圍

11. 輸入 [IP 位址] 或 [範圍],然後按一下 [新增包含清單] 或 [新增排除清單],將 IP 位址 或範圍新增到適當的清單。您一次只能新增一個。您輸入的 TCP/IP 位址範圍及/或特 定位址,就是您想管理的 TCP/IP 位址範圍及/或特定位址。您必須至少指定一個「包 含」範圍或者位址,才能完成這部分的組態設定。如果您有任何想要排除的範圍或位 址,也可以在「全域排除範圍/位址」面板上加以指定。「排除」面板可以避免探查某 些裝置,而「包含」面板則指出必須探查和管理哪些位址。如果您稍後想從清單移除 其中一個,則可按一下清單右側的 [移除]。

注意:如果這個範圍的 IP 位址所包含的服務已經在「探查範圍」中指定,您就必須變更 某些裝置的授權 – 例如,您可能必須將「工作站」授權變更爲「伺服器」授權 – 若需額外 資訊,請參閱〈第5 章:確認和微調安裝〉的〈清理安裝〉一節。

### 指定代理伺服器識別及身分

確認*代理伺服器及範圍*之後,CC-NOC 就會開始進行探查程序,透過 WMI 來搜尋要管理 的目標裝置。現在您必須組態設定目標伺服器和工作站(例如桌上型電腦、筆記型電腦 等)的認證資訊。

			1 200
WORKGROLP Y	forkgroup A	dmininsfrator	新報 國除
оси в	omain A	dmininstrator	<b>編輯</b> 開除

圖 44 指定代理伺服器身分

對於與您希望管理的主機相關聯的每一個網域、工作群組或是受信任的網域,您都必須提供認證資訊(例如使用者名稱和密碼),而此資訊可用來登入系統以及取得效能、事件記錄及/或系統目錄資訊。如果您願意的話,一旦探查到裝置,您也可以提供有關該裝置的這份資料。請注意,這樣做是否更爲安全,仍有爭論;但是在管理方面就要更注意。

CC-NOC 支援透過下列三個常用認證機制其中之一來進行認證:

- 網域認證
- 工作群組認證
- 信任網域認證

網域認證是 Windows 環境中最常用的認證形式,所以在此加以說明。力登的

《CommandCenter NOC 管理指南》中,涵蓋了另外兩種認證形式。

對於與您希望管理的主機相關聯的每一個網域,您都必須提供認證資訊(例如使用者名稱 和密碼),而此資訊可用來登入系統以及取得效能、事件記錄及/或系統目錄資訊。「使 用者名稱」和「密碼」將會傳送給網域內的伺服器,以供認證之用。目標伺服器必須是這 個網域的成員,而且使用者名稱必須組態設定成該網域內的使用者。

注意:需要管理權限才能新增這三種認證類型的身分。



12. 按一下 [新增網域身分] 即可為網域認證新增身分。

新的網域身分	
請輸入做為認證之用的網域名稱。	
注意:以下輸入的使用者名稱必須是目標系統[ <i>本地管理員</i> ]群組的成員。在大部分的情況	,網域管理員應該是這個群組的成員。
請注意,CommandCenter NOC 250 只可以接受擁有唯一網域名稱的身分。	
<b>劉</b> 域:	
使用者名稱:	
密碼:	
確認密碼:	
新聞自分」「取済」	

圖 45 指定網域認證身分

13. 輸入網域、使用者名稱、密碼,然後確認密碼。

注意:基於安全理由,Windows Vista 系統中內建的系統管理員帳戶「Administrator」依預 設將不會進行資料收集。不論使用哪個 Windows 版本,力登建議對所有的伺服器使用非 「Administrator」的系統管理員帳戶。

請參閱《CC-NOC 管理指南》中的〈附錄 D:在目標電腦上設定 WMI〉,以取得更多對 Windows Vista 目標電腦設定代理伺服器驗證的相關資料。

14. 按一下 [新增身分]。

15. 若要完成精靈,請按一下[繼續]。

利城/工作群組/信任網城	類型	使用者名群	行動
WORKGROUP	Workgraup	Admininstrator	<b>編編 國除</b>
TEST	Domain	admin	<b>新設 調味</b>
оси	Domein	Administrator	新聞開除

圖 46 Windows 管理代理伺服器的清單

16. 如果您對於代理伺服器清單感到滿意,請按一下[儲存變更]。

### 入侵偵測的概略說明

在 CC-NOC 安裝期間,您可以選擇將 CC-NOC 連接到環境內的跨距或鏡像連接埠 – 若需額外資訊,請參閱〈第3章:實體及網路安裝〉。使用這個連線可以監視網路流量的入侵企圖和頻寬效能。

注意: CC-NOC 100、CC-NOC 250 或 CC-NOC 2500S 都支援入侵偵測。

若要設定 CC-NOC 的組態,讓它監視網路流量是否有入侵企圖,您必須:

- 設定「近端網路」的組態-因為 CC-NOC 偵測某些簽名的方式,是根據簽名進入近端網路或是從近端網路送出而定,所以您應該為裝置設定近端網路,以確保入侵偵測儘可能正確,且讓假警訊的數目降到最低。
- 設定連接埠掃描的組態-CC-NOC 裝置會執行封包的狀態檢測,以偵測網路上的連接 埠掃描活動。然而,某些合法的服務會開啓與主機之間的多重連線,例如 DNS、NFS 和 SMB,都可能產生假的連接埠掃描事件。您應該從連接埠掃描偵測作業中排除這些 伺服器。
- 設定簽名效能評測器的組態-使用「簽名效能評測器」,就可以啓用和停用每個 CC-NOC 裝置上的數種入侵偵測。CC-NOC 裝置會偵測有害網路流量中的一些「簽名」特徵,以找出潛在的威脅。調整 CC-NOC 裝置能夠偵測的簽名組,就可以設定入侵偵測功能的組態,以偵測出會影響網路上特定裝置和服務的攻擊。

#### 組態設定裝置的近端網路

**CC-NOC** 會以不同方式偵測某些簽名,這要看它們是「*進入*」近端網路或是從近端網路「*外送*」而定。因爲這個原因,設定裝置的近端網路就很重要,可以確定入侵偵測儘可能準確,而假警訊的數目就會降到最低。

若要為 CC-NOC 設定「近端網路」的組態:

- 1. 在主視窗中,按一下[管理]索引標籤。
- 2. 按一下[入侵偵測組態設定]。

**注意**:若要在分散式環境中存取「入侵偵測組態設定」(也就是從 CommandCenter 2500N 存取),請在頂端的瀏覽索引標籤列中,按一下 [ **管理**] 索引標籤,再按 [CC-NOC 2500S 組態設定] 。 入侵值測組態設定

組態設定裝置的近端網路

組態設定連接埠掃描偵測

入侵值測簽名效能評測器

入侵值测的推護

刪除效能資訊

### 進階管理

進階安全管理

相關的連結

入侵偵測網頁

網路錫點掃描網頁

網路弱點掃瞄管理

圖 47 入侵偵測組態設定

3. 按一下[組態設定裝置的近端網路]。

入侵值测近端铜路的组態設定



圖 48 組態設定裝置的近端網路

4. 按一下您想設定組態的裝置旁的[設定組態]。

入侵值測近端網路的組態設定
下列設定是目前近端網路的設定。
目前的装置
SRNUM00304856EB27
新增位址
網路位址:
子翻路連章 = 255.255.255.0 (CIDR /24, Class C) V
新贈
單一 IP 或者範圍的開端:
範圍的末端:
(可 選用)
新贈

圖 49 指定近端網路裝置的 IP 位址

- 5. 如果要將整個子網路包括在您的近端網路內,請使用[新增位址]方塊。輸入網路位址,然後從提供的清單中選取子網路遮罩。如果要包括單一主機或主機 IP 位址的範圍,請使用面板下半部的輸入方塊。
- 6. 按一下 [新增]。

注意:您最多可以新增50個不屬於已包含之子網路的特定IP位址。

### 組態設定連接埠掃描偵測

CC-NOC 可以執行封包檢測,以值測網路上的連接埠掃描活動。然而,某些合法的服務會開啓與主機之間的多重連線,例如 DNS 和 NFS,都可能產生假的連接埠掃描事件。

若要從連接埠掃描偵測作業中排除這些伺服器:

1. 在「入侵偵測組態設定」主視窗中,按一下[組態設定連接埠掃描偵測]。

現在設定組集
組態設定

圖 50 設定連接埠掃描偵測的組態

判斷目標電腦上有那些連接埠是開放的,通常就是對網路系統進行成功攻擊的第一個步驟。攻擊者通常會使用連接埠掃描公用程式來刺探目標系統,然後列出裝置上所有開放連接埠的清單。有了這份名單之後,他們就會對這些開放的連接埠進行特定攻擊,期望能夠找出目標電腦的網路弱點。監控進入目標電腦的流量,通常就可以偵測出連接埠掃描的程序。然而,某些服務(像是 DNS、NFS 和 SMB)的正常活動,通常也很類似針對目標系統進行連接埠掃描的攻擊者活動。

2. 按一下您想設定組態的裝置旁的[設定組態]。

連接埠掃嘯偵測
下列設定是目前連接埠掃描值測的設定。
目前的装置
SRNUM00304856EB27
新增位址
網路位址:
子網路這罩:
255.255.255.0 (CIDR /24, Class C) 💌
新增
軍一 IP 或者範圍的開端:
範圍的末端:
(可
) 送用 /
新増

圖 51 指定連接埠偵測的 IP 位址

這個組態設定頁面可讓您從 CC-NOC 所執行的連接埠掃描偵測程序中,排除特定主機。

- 若要排除整個子網路不進行連接埠掃描,請使用[新增位址]方塊。輸入網路位址,然 後從提供的清單中選取子網路遮罩。若要排除單一主機或者主機 IP 位址的範圍,請使 用面板下半部的輸入方塊。
- 4. 按一下 [新增]。

建議您將所有 DNS 和 NFS 伺服器新增到這份清單中。

**注意**:使用這個視窗最多只能排除 50 個位址。如果您需要排除更多位址,請聯繫力登技 術服務中心。

### 設定入侵偵測簽名效能評測器的組態

使用「入侵值測簽名效能評測器」(Intrusion Detection Signature Profiler),就可以啓用和 停用在 CC-NOC 上的多種類型入侵值測。正確設定組態的 CC-NOC 會值測網路流量中的 特別模式,以找出潛在的威脅。調整 CC-NOC 裝置能夠值測的簽名組,就可以設定入侵值 測功能的組態,以值測出會影響網路上特定裝置和服務的攻擊。

以4個基本步驟設定簽名效能評測器:



- 2. 在「選擇裝置」(Choose Appliances)頁面上,選擇要設定的裝置。
- 3. 在「**選擇類型**」(Select Types)頁面上,選擇一組您想偵測的簽名類型,以及用來進行 偵測的規則集。
- 4. 在「**選擇作業系統系統和服務**」(Select Operating Systems and Services) 頁面上,選擇 在您的網路上,您想監視有無這些簽名的作業系統和服務。
- 5. 在「**選擇應用程式**」(Select Applications) 頁面上,選擇一組特定的應用程式,以監視 在您網路上的入侵。

建立簽名規則之後,CC-NOC 就會使用這些規則來動態選擇要將哪些簽名套用到環境中, 讓您省下不停管理簽名的麻煩。若要開始設定這些簽名規則:

- 1. 在最頂端的瀏覽列中,按一下「管理」(Admin)標籤。
- 2. 按一下「入侵偵測組態設定」。
- 3. 按一下「入侵偵測簽名效能評測器」(Intrusion Detection Signature Profiler)。

#### 選擇裝置

可與主控此中央裝置之系統溝通的所有「入侵偵測」裝置,都會列在「選擇裝置」 (Choose Appliances)頁面中。每個裝置都附隨著該裝置的 IP 位址以及上次變更該裝置之 「入侵偵測方案」的時間(無論是由軟體更新或由管理員變更)。

如果入侵偵測裝置列為「**尙未組態設定」(Not Configured**),您必須使用「簽名效能評測 器」來設定它的簽名,讓它可以開始轉送事件。

#### 遷擇裝置

所有能夠與 CommandCenter NOC 250 溝通的入侵值測裝置如下所列。表格中的欄位指出裝置的值測方案上次改變的時間,或者上次使用安全性修正 程式更新裝置入侵值測签名的時間。

如果入侵值測裝置的一些欄位被註明爲[*尚未組態設定*],您必須使用管理網頁來設定它的簽名,讓它可以開始轉送事件。

若要設定一個或者多個入侵偵測裝置爲相同的組態,諸核取位於 [選擇]標題下方的方塊。當您完成選擇後,按一下 [了一步]按鈕。

入侵值测装置						
序號	IP 位址	上次近端網路的更新	上次連接埠掃描設定的更新	上次签名的更新	選擇	
ACF6600034	192.168.32.57	2006/12/11 上午 07:29:44	2006/12/11 上午 07:29:44	2006/12/9 下午 01:47:52		1
		下 <b>□?</b> □	>>			

圖 52 選擇簽名效能評測器的入侵偵測裝置

1. 若要設定具有相同組態設定的一或多個入侵偵測裝置,請核取位於「**選擇**」欄位中的 方塊。

注意: CC-NOC 100 和 CC-NOC 250 只支援連接到流量偵聽連接埠的單一網路區段。如果 要監控其他網路區段,必須設定一個 CC-NOC 2500N 裝置配上個 CC-NOC 2500S 裝置。

2. 按「下一步」。您會被帶到「選擇類型」(Select Types)畫面。

#### 選擇監控的簽名類型

此頁面可讓您設定想在「入侵偵測系統」利用的簽名類型。各種簽名類型的完整清單顯示 在頁面底端的「選擇簽名類型」表格中,作為「規則類型」。對於其中每一種規則類型, 您可以包括來自三種來源的簽名偵測規則:Snort.org® Community 規則、Sourcefire® VRT 授權的規則及 Bleeding Edge Snort ™ 規則。請注意,「Bleeding Edge Snort 規則」 包含新建立的偵測規則,這些規則不像另外兩種規則經過嚴謹的驗證程序。

- 由 Snort 週遭的「開放原始碼」社群所開發的 Snort Community 規則。這些規則由社群 進行測試,以確保這些規則不會破壞現有的功能。
- Sourcefire VRT 規則由 Snort 目前的擁有者 Sourcefire 所開發,其具有為較大型組織所 支援的優點。這些規則需經過更完整的測試,其中包括效能測試。
- Bleeding Edge 規則是由另一個社群所開發,具有調整並滿足更多目前之社群要求的目的。這些規則接受相當多的測試,包括當有所變更時,在較舊/現存的規則上進行 測試。

選擇作業系統和服務									
目前的装置:192.168.32.57 若要載入一個先前已經設定為入侵偵測裝置的目前設定,諸在山 現有的組態設定: 載入預設值 ♥ <b>基入組態設定</b> 運擇預設值	北選擇它,然後按 <b>重設表格</b>	一下 [ <i>載</i> :	入組創書	短按	⊞∘				
< 上0?0 下0?0	3	>>							
作業系統	與服務無關	HTTP	SMTP	SQL	DNS	DHCP	Telnet	SNMP	SSH
Microsoft 的 Windows 9X/ME 版本									
與作業系統無關							<ul> <li>Image: A start of the start of</li></ul>		
Microsoft的 Windows XP Professional SP2 版本			<b>v</b>					~	
Microsoft的 Windows XP Professional SP1 版本									
Microsoft 的 Windows XP Professional 版本			<b>V</b>					<b>&gt;</b>	
Microsoft的 Windows XP Home SP2 版本									
Microsoft 的 Windows XP Home SP1 版本									
Microsoft 的 Windows XP Home 版本									
Microsoft的Windows Server 2003 SP1 版本							<b>V</b>	<b>&gt;</b>	
Microsoft 的 Windows Server 2003 版本									
Microsoft 的 Windows NT Workstation 4.0 SP6a 版本									

圖 53 「選擇簽名類型」表格

若要設定「入侵偵測系統」以監視特定類型的簽名:

 對於您想偵測的每一種偵測種類,核取您想用於偵測的規則集 (Community、VRT 或 Bleeding Edge)。取消核取、或留空您不想使用的任何規則集。
 例如,如果您想使用由 Sourcefire 及 Snort.org 定義的簽名設定檔啟用偵測「攻擊回

應」類型的簽名,但覺得 Bleeding Edge Snort 簽名尚未經過足夠的測試,則可以為 「**攻擊回應**」規則核取「**VRT**」及「**Community**」欄位,但不核取「**Bleeding Edge**」 欄位。

對於您不想偵測簽名的每一種偵測類別,請取消核取或留空所有三個規則集選項。
 在表格的頂端有三個額外的項目可以幫助您選擇「規則類型」組態設定:

6. 「載入組態設定」可讓您在系統上使用另一個裝置的「規則類型」組態設定。如果您 想複製該裝置的「規則類型」組態設定,則可以從「現有的組態設定」下的下拉式功 能表中選擇它的序號,然後按一下「載入組態設定」。如果您正在執行 CC-NOC 2500 分散式系統,也可以在此看見可供選擇的許多項目。



- 7. 「選擇預設值」(Select Defaults) 將選擇 CC-NOC 隨附的規則集組態設定。
- 8. 「**重設表格」(Reset Form)** 會還原自從到達此頁之後對規則集組態設定做過的所有變 更。按一下「**重設表格**」(**Reset Form**) 會使組態設定回到上次儲存的選擇。

注意:不知道要選擇什麼的時候,預設的偵測規則集是您最佳的選擇。

 按照您想要的方式設定偵測規則時,請按「下一步」進入「作業系統和服務」 (Operating Systems and Services)頁面。

### 選擇作業系統和服務

本頁可讓您設定要在數個作業系統上監視的服務。服務的明細與作業系統的清單會形成一份位於頁面底端上的「**選擇作業系統和服務**」(Select Operating System and Services)表格。對於列在左邊的每一個作業系統,您都可以選擇您想監視的服務,看看是否有您在上一頁選擇的入侵偵測簽名。

選擇作業系統和服務									
目前的裝置:192.168.32.57 并更新3.一個先前已經設定為3.得信測結果的日前設定,該在出	避摆它,就後续。		1 28 45 2	i ca tek	m.				
現有的組象設定: 載入預設值	重設表格	1 [#86	//# <u>11</u> .2949	(JC) 1943	£Ш -				
< 上070 下070	2	>>							
作業系統	與服務無關	HTTP	SMTP	SQL	DNS	DHCP	Telnet	SNMP	SSH
Microsoft 的 Windows 9X/ME 版本									
與作業系統無關									
Microsoft的Windows XP Professional SP2版本						~	<b>V</b>		
Microsoft的Windows XP Professional SP1 版本							<b>~</b>		
Microsoft 的 Windows XP Professional 版本			<b>&gt;</b>				<b>V</b>		
Microsoft 的 Windows XP Home SP2 版本									
Microsoft 的 Windows XP Home SP1 版本									
Microsoft的Windows XP Home版本									
Microsoft 的 Windows Server 2003 SP1 版本			~				~		
Microsoft 的 Windows Server 2003 版本							<b>V</b>		
Microsoft 的Windows NT Workstation 4.0 SP6a 版本									

圖 54 選擇要監視的作業系統和服務

- 1. 對於清單中的每一個作業系統,請選擇您要監視的服務。
- 如果在您網路上有個特定的作業系統沒有使用某些服務,您可以取消核取或留空該作業系統的服務欄位。
- 對於不在您網路上的作業系統,您可以取消核取或留空該列中的所有服務類型。
   在表格的頂端有三個額外的項目可以幫助您選擇一組要監視的服務:
- 「載入組態設定」可讓您在系統上使用另一個裝置的服務組態設定。如果您想複製該裝置的服務組態設定,則可以從「現有的組態設定」下的下拉式功能表中選擇它的序號, 然後按一下「載入組態設定」。如果您正在執行 CC-NOC 2500 分散式系統,也可以在 此看見可供選擇的許多項目。

「選擇預設值」(Select Defaults)將選擇預設要監視的作業系統與適當服務集。

「**重設表格」(Reset Form)** 會還原自從到達此頁之後對服務組態設定做過的所有變更。按 一下「**重設表格**」(Reset Form) 會使組態設定回到上次儲存的選擇。

注意:不知道要選擇什麼的時候,預設的作業系統與服務集是您最佳的選擇。



此外,如果您不確定要不要選擇作業系統或服務時,啓用偵測它們就對了。啓用額外的偵測並不會有任何不利的狀況,只是您會從入侵偵測裝置收到一些無關緊要的事件。您應該從不停用偵測「**非作業系統特定**」(Not OS Specific)類別中的簽名。不論網路上有哪些裝置和服務,這個類別都包含各種可能影響任何網路的攻擊。

4. 依您想要的方式選擇好作業系統和服務之後,請按「下一步」進入「選擇裝置」 (Select Applications)頁面。

### 選擇應用程式

在您網路中某些系統上執行的特定套裝軟體若存在弱點,就會提供入侵者一個進入點,對您的網路發動攻擊。本頁可讓您設定 CC-NOC 監視 (或不監視)針對「選擇應用程式」表格中列出之特定應用程式發動的攻擊。

海探库用把子								
建蓉是用程式 目前的装置:192.168.32.57 若要載入一個先前已經設定為入侵偵測装置的目前設定,請在此選擇它,然後按一下[載入租參設定]按鈕。 現有的組態設定: 載入預發值 ♥ 載入組態設定 選擇預設値 重設表格								
上070 下070	>>		dh dh					
<b>島田在</b> 式	版本/系列		状態					
1st Class Internet Solutions 1st Class Mail Server	4	●使用預設値	○已啓用	○已停用				
3Com 3CDaemon	2	⊙ 使用預設値	〇已啓用	〇已停用				
3Com 3CRADSL72 Wireless Router	none	●使用預設値	○已啓用	○已停用				
3Com Network Director	1	⊙ 使用預設値	○已啓用	〇已停用				
3Com Network Supervisor	5	◉ 使用預設値	○已啓用	〇己停用				
3Com OfficeConnect DSL Router	812	⊙ 使用預設值	〇己啓用	〇已停用				
3Com OfficeConnect DSL Router	840	◉ 使用預設值	○已啓用	○已停用				
4D WebSTAR	4	⊙ 使用預設値	〇己啓用	〇己停用				



- 1. 對於清單中已在您網路上執行的每一個應用程式,請選擇「**狀態**」下的「**使用預設** 值」(Use Default)。
- 2. 對於重要的應用程式或其他您要密切監視的應用程式,您可以選擇「**啓用**」該應用程 式的所有簽名(這樣會置換預設的作業系統和服務篩選,並可能增加假警示的數量)。
- 3. 如果您可以明確地判定應用程式未安裝在您的網路上,請選擇「**停用**」來減少假警示的數量。

在表格的頂端有三個額外的項目可以幫助您選擇應用程式組態設定:

- 「載入組態設定」可讓您在系統上使用另一個裝置的應用程式組態設定。如果您想複製那個裝置的應用程式組態設定,則可以從「現有的組態設定」下的下拉式功能表中選擇它的序號,然後按一下「載入組態設定」。如果您正在執行 CC-NOC 2500 分散式系統,也可以在此看見可供選擇的許多項目。
- 「選擇預設值」(Select Defaults) 將選擇 CC-NOC 隨附的應用程式組態設定。
- 「重設表格」(Reset Form) 會還原自從到達此頁之後對應用程式組態設定做過的所有 變更。Click 按一下「重設表格」(Reset Form) 會使組態設定回到上次儲存的選擇。

注意:不知道要選擇什麼的時候,預設的應用程式集是您最佳的選擇。

4. 依您想要的方式設定好應用程式清單後,請按「**下一步**」。 這會完成設定簽名效能評測器,並出現一頁,確認入侵偵測系統使用新的設定。



### 設定效能監視的組態

CC-NOC 提供流量分析的方式,就是成為網路上的混雜監聽程式。入侵偵測所使用的連接 埠也會用於效能監視。CC-NOC 會持續監視網路的頻寬使用量,且能夠提供入口讓您了解 網路利用率,為您顯示流量類型以及一些有用的統計資料。網路流量可以依照乙太網路通 訊協定、網際網路通訊協定 (IP) 和應用程式通訊協定來排序。這項資料讓您能夠快速和準 確地分析目前網路的使用情形。

注意:在分散式環境中,流量分析是在CC-NOC 2500S 上執行。

網路上最常被要求的網站及網域名稱也會受到監視。CC-NOC 會告訴您哪些節點使用的頻 寬最多(例如「*IP 節點發送資料最多者*」),以及哪些連線在節點之間產生的流量最大 (例如「*依據 IP 連線作業發送資料最多者*」)。

若要組態設定和檢視網路中的流量:

1. 在主視窗中,按一下[流量]索引標籤。

<u>流量</u> 分析
流量分析的檢視摘要:
時間週期: 最後一天 ▼ <b>檢視</b>
<b>檢視應用程式通訊協定摘要</b> :
時間週期: 最後一天 ✓ <b>檢視</b>
<b>检視低階通訊協定摘要</b> :
時間週期: 最後一天 💙
自訂流量分析報告
流量分析統計資料
最受歡迎的網站
最常被解析的 DNS 主機名稱
發送資料最多的節點和連線作業

圖 56 流量分析



2. 按一下[自訂流量分析報告]。

流量分析效能資料		
選擇要查詢的這量分析裝置:	選擇要執行的查詢:	開始時間 (Month, Day, Year, Hour):
SRNUM00304856EB27	app	七月 🖌 31 2006 10 РМ 💌
	ethernet	結束時間 (Month, Day, Year, Hour):
		八月 💟 1 2006 10 PM 💌
		Accession and a second s
送出 重設		

圖 57 依照通訊協定來排序流量

- 3. 選擇要查詢的電腦、一或多個通訊協定(也就是應用程式、IP 或乙太網路),以及時 間範圍。
- 4. 按一下 [送出]。以下顯示 IP 通訊協定網路使用量的範例。

#### 装置 {1} 的流量分析效能報告

2006年7月31日 星期一下午10時00分00秒 EDT
 3006年8月1日 星期二下午10時00分00秒 EDT

	Network	Usage	by IP	Pro	otocol	(bits/	second)	1	
40 M									
20 M									-levil
								1	
0	00:00		06:00	to the	÷+,	12:00		18:00	
EGP		Avg:	0.00		Min:	0.00	Max:	0.00	
EIGRP		Avg:	0.00		Min:	0.00	Max:	0.00	
Fibre_Chan	nel	Avg:	0.00		Min:	0.00	Max:	0.00	
GRE		Avg:	0.00		Min:	0.00	Max:	0.00	
ICMP		Avg:	3, 31	k	Min:	2.35 k	Max:	6,49	k
IGMP		Avg:	0.00		Min:	0,00	Max:	0.00	
IGP		Avg:	0.00		Min:	0.00	Max:	0.00	
IPSec		Avg:	4.06	Μ	Min:	2,69 1	1 Max:	8.04	М
IP_over_IP		Avg:	0.00		Min:	0.00	Max:	0.00	
🛯 IPv6_over_	IP	Avg:	0.00		Min:	0.00	Max:	0.00	
L2TP		Avg:	0.00		Min:	0.00	Max:	0.00	
OSPF		Avg:	0.00		Min:	0.00	Max:	0.00	
🛾 Other		Avg:	0,00		Min:	0.00	Max:	0.00	
ТСР		Avg:	18,20	М	Min:	14.38 1	1 Max:	34,75	М
UDP		Avg:	323, 36	k	Min:	224.20 k	( Max:	640.12	k
Total		Avg:	22.59	М	Min:	18.44 M	Max:	43.11	М

#### 圖 58 網路報告

**注意:**若要讓「效能監視」功能正確運作,CC-NOC 就必須能夠看到網路上傳遞的實際封 包。完成此動作的最佳方式,就是在網路上組態設定「鏡像」或「跨距」連接埠 – 若需額 外資訊,請參閱(**第3章:實體及網路安裝**)的**(跨距或鏡像連接埠**)一節。



## 第7章:開始使用

確認安裝、完成微調和執行一些建議進行的組態設定改變(例如「入侵偵測」)之後,您 就可以開始善加利用 CC-NOC 了。在這個階段,CC-NOC 應該會監視您想要監視的節 點,並收集效能和網路中斷資料。部署的最後一個步驟就是:

- 啓用通知
- 啓用層級1或層級2的網路弱點掃描
- 建立網路中斷報告
- 下載備份檔案

### 啓用通知

CC-NOC 有個非常強大的通知引擎。它很容易自訂,且可提供各種不同的選項 – 事實上, 它可讓您建立供 CC-NOC 遵循的程序,用以向技術服務人員警告環境內的問題,而不是 一定要遵守無法自訂的嚴格標準。您可以從超過 3000 種的不同事件類別來建立通知,而 且可以依照單一 IP、IP 範圍及服務來分類。您也可以建立通知來遵循詳盡的向上通報程 序,確保必須得知網路中斷/問題的人員一定會收到通知。

您可以利用每部 CC-NOC 原有的預設通知,或是建立自訂通知。無論您採取哪個方式, 都必須完成一些初步的步驟:

- 組態設定使用者
- 組態設定群組
- 組態設定報告
- 開啓通知

您可以在力登的《CommandCenter NOC 管理指南》中,找到如何組態設定使用者、群組 及通知的詳細資料。

### 通知狀態

「**通知**」頁面可提供視覺化提醒(例如是否傳呼/以電子郵件通知使用者、接收重要網路 事件的時間等),以及提供開啓或關閉通知系統的方法。這是整個系統的設定,會影響所 有通知和所有使用者。

若要啓用通知:

- 1. 在主視窗中,按一下[管理]索引標籤。
- 2. 按一下[通知組態設定]。
- 3. 將[報告狀態]從「關閉」切換成「開啓」。

#### 通知狀態

●開啓 ●開閉 更新狀態

圖 59 啓用通知狀態

### 4. 按一下 [**更新狀態**]。

### 啓用網路弱點掃描

在環境中善加利用 CC-NOC 的下一個步驟就是啓用「網路弱點掃描」。這是選擇性的步驟,但是建議您使用。「網路弱點掃描」可協助您判斷網路中的哪些節點正在執行含有已知安全性弱點的作業系統、網路服務或應用程式。

一開始只需開啓 [掃描層級 1] 或 [掃描層級 2]。這樣您就可以收集重要的網路弱點資料, 不需要使用較高的設定而承擔可能的損失風險。

警告:網路弱點掃描對於目標電腦會造成潛在性的傷害。因爲這個原因,預設會停用這項 功能。掃描動作又再逐級分成更多入侵「層級」的掃描。請詳閱掃描層級說明,然後再新 增要掃描的IP 位址並啓用掃描 – 尤其是「掃描層級3」和「掃描層級4」。

若要啓用掃描:

- 1. 在主視窗中,按一下[網路易點]索引標籤。
- 2. 按一下[設定網路易點掃描]。
- 3. 閱讀「網路弱點掃描警告」之後,請按一下[**我同意**]。
- 4. 按一下[編輯位址設定值]。

網路尋點掃描的組態設定		
従掃輻排除	軍一 IP 或者範圍的開端:	
使用右側的這些方塊,新增範圍和一些特定位址		
	範圍的末端 -	
	(可選用)	
	新贈	
掃描層級 1:連接埠掃描	單一 IP 或者範圍的開端:	
這個掃描層級的目標:		
使用右側的這些方塊,新增範圍和一些特定位址	範圍的末端: 	
	(可選用)	
	新贈	
掃描層級 2:設定檔研判	單一 IP 或者範圍的開端:	
這個掃描層級的目標:		
使用右側的這些方塊,新增範圍和一些特定位址	<b>範閣的末端:</b>	
	(可選用)	
	新碧	

圖 60 設定層級 1 和層級 2 的網路易點掃描

- 5. 輸入「層級1」的IP位址或範圍,然後按一下[新增]。
- 6. 輸入「層級 2」的 IP 位址或範圍,然後按一下 [新增]。
- 7. 按一下頁面底端的 [儲存設定值]。

「**掃描層級 1**」會使用幾種不同的連接埠掃描方法,來掃描目標系統是否有開放連接埠。 它不會對開放連接埠進行任何其他的檢查,對於在這些連接埠上正在進行監聽的服務功能 不會有所傷害。
「**掃描層級 2**」會掃描開放的連接埠,並嘗試找出在這些連接埠上執行的服務。這是藉由 讀取來自這些服務的回應來判斷;不會故意將有害封包傳送到這些伺服器以取得這些回 應。這個掃描層級也會嘗試研判作業系統的設定,並判斷可能有利於入侵者的主機網路活 動的相關資訊。因爲使用這個層級的掃描時,並不是直接測試網路弱點(這樣可能會危害 目標系統),所以可能會產生一些假警訊。

「**掃描層級 3**」和「**掃描層級 4**」處理的是針對目標電腦的實質入侵企圖,對於目標電腦 會造成負面影響,導致資料遺失和阻斷服務。進行這些層級的掃描要相當謹慎小心。

**警告:**所有掃描層級都是累加的。例如,「掃描層級 3」會執行層級 1 和 2 的所有掃描, 再加上一些其他的入侵掃描。

在力登的《CommandCenter NOC 管理指南》中,可以找到網路弱點掃描的詳細資料。

## 設定網路中斷報告的組態

網路中斷報告會產生兩個可用性百分比:一個是整週的總可用性,另一個是營業時間的可 用性。您可以變更下個頁面的資料,來編輯用於計算營業時間可用性的時間週期。 若要建立網路中斷報告:

- 1. 在主視窗中,按一下[管理]索引標籤。
- 2. 按一下[網路管理組態設定]。
- 3. 按一下[設定網路中斷報告的組態]。

網路中斷報告的組態設定
<b>営業時間:</b>
從:
09 : 00
直到:
19 : 00
工作天:
☑星期─
☑星期二
☑ 星期三
✔ 星期四
☑ 星期五
□星期六
□星期日
<b></b>

圖 61 設定網路中斷報告的組態

- 4. 以 24 小時制的格式輸入營業時間。
- 5. 使用核取方塊來選擇要包含在報告中的工作天。
- 6. 按一下 [**套用變更**]。
- 7. 若要產生報告,請按一下頁面右邊的[網路中斷報告]。

## 下載備份檔案

備份檔案會由 CC-NOC 自動產生。不過,建議您定期將備份檔案下載到 PC,必要時就可以在 CC-NOC 上加以還原。



- 1. 在頂端的導覽索引標籤列中,按一下[管理]索引標籤。
- 2. 按一下 [進階管理]。
- 3. 按一下[資料備份和還原]。
- 4. 按一下 [**下載備份檔案**]。

備份歸榆	日期	大小	版本
backup-5.4.0-20060724010516.dat Daily backup	2006/7/24	9.296 MB	5.4.0
backup-5.4.0-20060723010516.dat Daily backup	2006/7/23	9.157 MB	5.4.0

圖 62 下載備份檔案

5. 按一下檔案開始下載。





# 力登現場調査 CommandCenter® NOC 100/250

目標安裝日期:	-
位置	
地址1:	
地址 2:	
城市/州省/郵遞區號:	
電話:	

網路組態	SNMP 社群定義
IP 位址:	取得社群連線密碼:
子網路遮罩:	□ 單一 IP 或者範圍的開端:
預設 聞道:	節圍的末端:
時區: NTP 伺服器:	版本: v1 v2c(預設值)
自動更新設定	取得社群連線密碼:
自動檢查:  開啓 關閉	單一 IP 或者範圍的開端:
動下載:    開啓  關閉	範圍的末端:
自動安裝:  開啓 關閉	版本: v1 v2c
使用 HTTP 代理伺服器? 是 否	(預設値)
(如果「是」,請列出):	
伺服器:	網際網路閘道
使用者名稱:	ISP 開道位址:
密碼:	
	名稱伺服器和 WINS 位址
管理的位址	主要 DNS:
	次要 DNS:
單一 IP 或者範圍的開端:	第三套 DNS:
範圍的末端:	WINS 伺服器:
包含或排除:	電子郵件通訊
單一 IP 或者範圍的開端:	使用 SMTP 伺服器:
	是 否(如果「否」,請列出):
範圍的末端:	使用在下列 IP 位址的遠端 SMTP 伺服器:
包含或排除:	傳送通知電子郵件位址:
單一 IP 或者範圍的開端:	本地管理員電子郵件位址:
範圍的末端:	
	Windows 管理組態設定
包含或排除:	IP 位址:
單一 IP 或者範圍的開端:	網域:
範圍的末端:	使用者名稱:
	密碼:
包含或排除:	IP 範圍:
單一 IP 或者範圍的開端:	身分(選擇一個:網域/工作群組/受信任)
範圍的末端:	網域: 使用者名稱:
	密碼:
	1





# 力登現場調査 CommandCenter® NOC 2500N

目標安裝日期:	
位置	
地址 1:	
地址 2:	
城市/州省/郵遞區號:	
電話:	
網路組態	SNMP 社群定義
IP 位址:	取得社群連線密碼:
子網路遮罩:	單一 IP 或者範圍的開端:
預設閘道:	範圍的末端:
時區:NTP 伺服器:	版本: v1 v2c(預設值)
自動更新設定	取得社群連線密碼:
自動檢查: 開啓  關閉	單一 IP 或者範圍的開端:
自動下載: 開啓 關閉	範圍的末端:
自動安裝: 開啓  關閉	版本: v1 v2c
使用 HTTP 代理伺服器? 是 否	(預設値)
(如果「是」,請列出):	
伺服器:	網際網路閘道
使用者名稱:	ISP 閘道位址:
密碼:	
	名稱伺服器和 WINS 位址
管理的位址	主要 DNS:
包含或排除:	次要 DNS:
單一 IP 或者範圍的開端:	第三套 DNS:
範圍的末端:	WINS 伺服器:
句今武排除・	   電子郵化涌訊
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	电了异门通忆 体田 SMTP 伺服哭:
	是 否(如果「否」,請列出):
範圍的末端:	使用在下列 IP 位址的遠端 SMTP 伺服器:
	傳送通知電子郵件位址・
甲─ IP 或者軛圍的開端 ·	本地官埋貝電ナ郵件位址・
範圍的木端・	
句今戓排除:	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
→ → 次日乾酉町 Jm ···································	
包含或排除:	
單一 IP 或者範圍的開端:	
範圍的末端:	



255-80-5315-00



#### 美國總部

Raritan Computer, Inc. 400 Cottontail Lane Somerset, NJ 08873 USA Tel. (732) 764-8886 Fax (732) 764-8887 Email : <u>sales@raritan.com</u> www.raritan.com

#### 力登電腦 OEM 部門

Peppercon USA, Inc. 111 E. Wacker Dr, Suite 2626 Chicago, IL 60601 Tel. (847) 466-1392 Fax (312) 729-1375 Email : <u>info@peppercon.com</u> www.peppercon.com

#### 亞太區總部

力登電腦(台灣) 中華民國台灣省 台北縣新店市 寶橋路 235巷 121號 5樓 Tel. (886) 2 8919-1338 Fax (886) 2 8919-1338 Email:<u>sales.asia@raritan.com</u> http://www.rcit.com.tw

#### 力登電腦大陸辦事處

美國力登電腦股份有限公司上海代表處 中國上海徐匯區零陵路 899 號 飛洲國際廣場 17 樓 E 室 郵編: 200030 Tel. (86) 21 5425-2499 Fax (86) 21 5425-3992 Email: <u>sales.china@raritan.com</u> http://www.raritan.china.cn

Guangzhou Representative Office of Raritan Computer, Inc. 1205/F, Metro Plaza 183 Tian He Bei Road Guangzhou China 510075 Tel. (86-20)8755 5581 Fax (86-20)8755 5571 Email : sales.china@raritan.com http://www.raritan.com.cn

美國力登電腦股份有限公司北京代表處 中國北京市朝陽區霄雲路 36 號 國航大厦 1310 室 郵編: 100027 Tel. (86) 10 8447-5706 Fax (86) 10 8447-5700 Email: <u>sales.china@raritan.com</u> http://www.raritan.com.cn

### Raritan Korea

Raritan Computer Korea Inc. #3602, Trade Tower, World Trade Center Samsung-dong, Kangnam-gu Seoul, Korea Tel. (82) 2 557-8730 Fax (82) 2 557-8733 Email : <u>sales.korea@raritan.com</u> http://www.raritan.co.kr

#### Raritan Computer Japan, Inc.

4th Floor, Shinkawa NS Building 1-26-2 Shinkawa, Chuo-ku Tokyo, Japan 104-0033 Tel. (81) 03-3523-5991 Fax (81) 03-3523-5992 Email : <u>sales@raritan.co.jp</u>

http://www.raritan.co.jp

Raritan Computer Japan Osaka Office Honmachi Phoenix Bldg 8F 1-15-8 Nishihonmachi Nishi-ku Osaka, Japan 550-0005 Tel. (81) (6) 4391-7752 Fax (81) (6) 4391-7761 Email : <u>sales@raritan.co.jp</u>

http://www.raritan.co.jp

#### **Raritan Australia**

Level 2, 448 St Kilda Road Melbourne, VIC3004 Australia Tel. (61) 3 9866-6887 Fax (61) 3 9866-7706 Email : <u>sales.au@raritan.com</u> http://www.raritan.com

#### 美國力登電腦股份有限公司印度代表處

210 2nd Floor Orchid Square Sushant Lok 1, Block B, Mehrauli Gurgaon Rd, Gurgaon 122 002 Haryana India Tel. (91) 124 510 7881 Fax (91) 124 510 7880 Email : <u>sales.india@raritan.com</u> http://www.raritan.com

#### 歐洲總部

Raritan Computer Europe, B.V. Eglantierbaan 16 2908 LV Capelle aan den IJssel The Netherlands Tel. (31) 10-284-4040 Fax (31) 10-284-4049 Email : <u>sales.europe@raritan.com</u> http://www.raritan.com

#### **Raritan Computer France**

120 Rue Jean Jaurés 92300 Levallois-Perret France Tel. (33) 14-756-2039 Fax (33) 14-756-2061 Email : <u>sales.france@raritan.com</u> http://www.raritan.fr

#### **Raritan Computer Deutschland GmbH**

Lichtstraße 2 D-45127 Essen Germany Tel. (49) 201-747-98-0 Fax (49) 201-747-98-50 Email : <u>sales.germany@raritan.com</u> http://www.raritan.de

### Raritan Computer Italia

Via dei Piatti 4 20123 Milan Italy Tel. (39) 02-454-76813 Fax (39) 02-861-749 Email : <u>sales.italy@raritan.com</u> <u>http://www.raritan.com</u>

#### **Raritan Canada**

Raritan Computer Inc. 2085 Hurontario St., Suite 300 Mississauga, Ontario Canada L5A4G1 Tel. (905) 949-3650 Fax (905) 949-3651 Email : <u>sales.canada@raritan.com</u> <u>http://www.raritan.com</u>

#### Raritan Computer U.K. Limited

36 Great St. Helen's London EC3A 6AP United Kingdom Tel. (44) 20-7614-7700 Fax (44) 20-7614-7701 Email : <u>sales.uk@raritan.com</u> http://www.raritan.com