201509151

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201509151 A

(43)公開日： 中華民國 104 (2015) 年 03 月 01 日

(21)申請案號：102131465 (22)申請日： 中華民國 102 (2013) 年 08 月 30 日

(51)Int. Cl.： *H04L12/12 (2006.01)* *G06F21/50 (2013.01)*

(71)申請人：萬國商業機器公司 (美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)
美國

(72)發明人：劉智雄 LIU, JEFFREY CH (TW) ；曾煥逸 TSENG, JOEY HY (TW) ；李承達 LEE, CHENTA CT (TW) ；吳明峰 WU, RICK MF (TW)

(74)代理人：李宗德

申請實體審查：有 申請專利範圍項數：8 項 圖式數：4 共 27 頁

(54)名稱

具安全防護連結之遠端診斷的方法與電腦程式產品及實施該方法之資訊設備

A METHOD AND COMPUTER PROGRAM PRODUCT FOR PROVIDING A REMOTE DIAGNOSIS WITH A SECURE CONNECTION FOR AN APPLIANCE AND AN APPLIANCE PERFORMING THE METHOD

(57)摘要

本發明揭示一種提供一資訊設備具安全防護連結之遠端診斷的方法、裝置與電腦程式產品。該方法包括步驟如下：接收來自終端介面之命令；執行一認證/授權/稽核(AAA)模組以檢示該命令；若一遠端診斷模組已被啟用，判定是否已與一遠端資訊設備間建立一具安全防護之連結；及經由該具安全防護連結，傳送該命令至一遠端資訊設備。

A method and computer program product for providing a remote diagnosis with a secure connection for an appliance and an appliance performing the method. The method comprises the following steps: receiving a command from a console; performing an authentication/authorization/auditing (AAA) module to check the command; in response to the enabling of a remote diagnostic module determining if a secure connection with a remote appliance has been established; and passing the command via the secure connection to the remote appliance.

TW 201509151 A

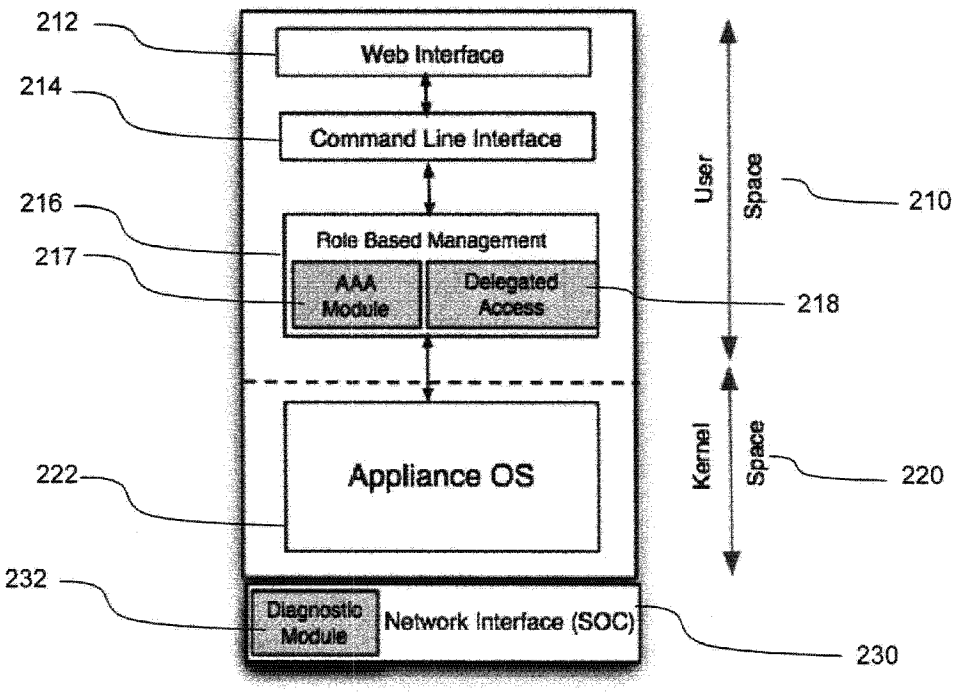

圖2

210・・・使用者空間

212・・・網路界面(web interface)

214・・・命令行界面CLI

216・・・角色式管理模組(RBM)

217・・・認證/授權/稽核(AAA)模組

218・・・指派存取模組

220・・・核心(kernel)空間

222・・・資訊設備作業系統

230・・・網路介面卡

232・・・診斷模組

201509151

發明摘要

※ 申請案號：102131465

※ 申請日：102年08月30日　　※IPC 分類：H04L 1/12 (2006.01)
G06F 21/50 (2013.01)

【發明名稱】(中文/英文)

具安全防護連結之遠端診斷的方法與電腦程式產品及實施該方法之資訊設備

A METHOD AND COMPUTER PROGRAM PRODUCT FOR PROVIDING A REMOTE DIAGNOSIS WITH A SECURE CONNECTION FOR AN APPLIANCE AND AN APPLIANCE PERFORMING THE METHOD

【中文】

本發明揭示一種提供一資訊設備具安全防護連結之遠端診斷的方法、裝置與電腦程式產品。該方法包括步驟如下：接收來自終端介面之命令；執行一認證/授權/稽核(AAA)模組以檢示該命令；若一遠端診斷模組已被啓用，判定是否已與一遠端資訊設備間建立一具安全防護之連結；及經由該具安全防護連結，傳送該命令至一遠端資訊設備。

【英文】

A method and computer program product for providing a remote diagnosis with a secure connection for an appliance and an appliance performing the method. The method comprises the following steps : receiving a command from a console; performing an authentication/authorization/auditing (AAA) module to check the command; in response to the enabling of a remote diagnostic module determining if a secure connection with a remote appliance has been established; and passing the command via the secure connection to the remote appliance.

【代表圖】

【本案指定代表圖】圖2。

【本代表圖之符號簡單說明】

210	使用者空間
212	網路界面(web interface)
214	命令行界面CLI
216	角色式管理模組(RBM)
217	認證/授權/稽核(AAA)模組
218	指派存取模組
220	核心(kernel)空間
222	資訊設備作業系統
230	網路介面卡
232	診斷模組

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】

無。

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

具安全防護連結之遠端診斷的方法與電腦程式產品及實施該方法之資訊設備

A METHOD AND COMPUTER PROGRAM PRODUCT FOR PROVIDING A REMOTE DIAGNOSIS WITH A SECURE CONNECTION FOR AN APPLIANCE AND AN APPLIANCE PERFORMING THE METHOD

【技術領域】

【0001】 本發明係關於提供一遠端診斷之技術；尤其是一種提供一資訊設備具安全防護連結之遠端診斷的方法、裝置與電腦程式產品。

【先前技術】

【0002】 通常一資訊設備，或稱之爲網際網路設備（Internet Appliance），爲內建有網路能力且具有某一特定功能的裝置，例如閘道器、路由器或附加式網路儲存裝置（Network Attached Storage）等，又如：無線網路橋接器(Access Point)、數位電視機上盒(set top box)、網路檔案分享(file sharing)伺服器等。實際之資訊設備可參考IBM® WebSphere® DataPower Series SOA Appliances 或 Tivoli® ISS Appliances ®)(「IBM」、「WebSphere」、「Tivoli」爲International Business Machine公司在美國及/或其他國家的註冊商標)。(http://www.redbooks.ibm.com/abstracts/redp4366.html)。

【0003】 相對於通用型(General Purpose)的電腦裝置，資訊設備一般係根據特定目的或特定服務而設計，以進行特定的交易(transaction)，因而具有較高的效能。相較於通用型電腦裝置，「資訊設備」顯得較爲「封閉」，也就是隨著其所設計的目的與服務，採用特定的作業系統與應用程式（或

驅動程式）。

【0004】 多個資訊設備形成之叢集(cluster)中，具「穩定性,可用性與可維護度（Reliability, Availability & Serviceability，RAS）」特徵之叢集係資訊設備之部署的重要面向，通常用來確保（ensure）多個伺服器或資訊設備(Appliance)可用來滿足業務需求（business needs）。尤其對那些作爲非管制區（Demilitarized Zone, DMZ）中企業之處理單元的資訊設備產品。關於「穩定性,可用性與可維護度（Reliability, Availability & Serviceability，RAS）」之詳細說明，可參考下列網頁：http://en.wikipedia.org/wiki/Reliability,_availability_and_serviceability_(computer_hardware) 的說明。

【0005】 一般資訊設備通常會在其網路介面卡(network interface card，NIC)上提供管理埠或串列埠（serial port）供網路系統管理員(administrators)診斷(diagnose)系統問題或失效。該網路介面卡一般是提供有TCP/IP堆疊以建立一TCP/IP連結(TCP/IP connection)之一系統單晶片(system on chip, SOC)或一 特殊應用積體電路 (application-specific integrated circuit, ASIC)。透過該TCP/IP堆疊，該資訊設備能建立一與該資訊設備之作業系統無關之TCP/IP連結。透過連結該管理埠或串列埠，該資訊設備之作業系統將啓動一終端介面(console)供網路系統管理員進行診斷與修復。

【0006】 這些管理埠或串列埠由於安全防護(security)的考量，通常不會開放給一般使用者存取或進行遠端存取。當一資訊設備當機(crashes)而失效(fail)或遭遇某些系統問題，即系統不再正常工作(functional)，管理員將須走進伺服機房，透過該管理埠或串列埠直接登入該資訊設備，以進行診斷與修復。因此，若能便利且具安全防護之方式，以允許管理員可遠端地進行之問題診斷，則是有利的。

【0007】 然遠端地診斷失效之資訊設備，並非是一件容易的工作(task)。尤其當該資訊設備位於非管制區DMZ而作爲一反向代理伺服器

（Reverse Proxy）以負責將用戶端的資料傳送給後面的網路伺服器上之一後端應用（backend）時，更是不易。因它可能將面對存在於非管制區DMZ中用於網路安全防護之設備（如防火牆、入侵偵測(intrusion detection system, IDS)或入侵預防系統（intrusion Prevention System, IPS）等），這使得遠端地診斷工作更形困難。缺少遠端診斷能力(facilities)，通常要求支援工程師實體地存取該失效之資訊設備，因而只能送支援工程師或服務團隊到客戶端的資料中心進行基本維護之例行程序(routines)。此外，失效系統之過長的停機時間(downtime)將導致業務上巨大衝擊。

【0008】 今日，存在一些解決方案供進行診斷，如利用(leverage)額外之提供於系統核心程序停機時存取該失效資訊設備的硬體模組，如IMM(Integrated Management Module)。IMM透過 IPMI 2.0提供系統管理功能。然此方法並不適用於安置於非管制區DMZ之資訊設備，或需求高安全防護之資訊設備。因於非管制區DMZ中種種網路攻擊，如字典式(dictionary)攻擊，可能輕易地波及(compromise)該硬體模組。

【發明內容】

【0009】 本發明揭示一透過利用一健康且可信賴(trusted)之同儕資訊設備，以進行具安全防護連結之遠端診斷機制。該健康之同儕資訊設備做爲一通訊橋樑，而在本地用戶應用與遠端之失效資訊設備(或稱目標裝置)間建立具安全防護之網路連結。失效目標裝置將主動建立連線到健康的同儕資訊設備以避免不必要的輪詢(polling)行爲，也進一步避免駭客(hacker)建立假的連線到健全的裝置以取得控制權。

【0010】 由於該橋接(bridging)用資訊設備及該目標裝置係位於相同網段或屬相同叢集，且本發明揭示的兩資訊設備間建立之具安全防護之網路連結係與作業系統無關，因此該遠端診斷機制爲可實施。此外，藉由利用橋接用資訊設備及該目標裝置中之角色式管理(Role-Based

Management ， RBM) 內 之 認 證 / 授 權 / 稽 核 (Authentication/Authorization/Auditing ，AAA)模組，該機制可提供診斷作業一更細密(fine-grained)之存取控制。其中稽核(auditing)一般有時也稱之計帳(accounting)，供追蹤使用者之行爲。

【0011】 所有存取控制(包含認證/授權控制)可在該健康之資訊設備上實施。若失效之目標裝置仍可啓用(initiate)其命令行界面（Command Line Interface，CLI），即該失效目標裝置仍可用(available)，則該健康之資訊設備對該失效目標裝置下達之修復命令，可直接傳送至該目標裝置之命令行界面。若失效目標裝置之命令行界面無法被啓用(即不可用)，則該失效目標裝置之網路介面卡所提供之用於網路系統管理員診斷系統問題的習知管理埠或串列埠，將被用來診斷該失效目標裝置之系統問題。

【0012】 總之，該遠端診斷機制至少包含下列優點：

1. 透過可信賴之橋接用資訊設備，使遠端診斷成爲可能。該橋接用資訊設備一般可經由網際網路(internet)存取；

2. 基於橋接用資訊設備及該目標裝置間之相似性，將能最小化兩者間同步與通訊之實施上困難。

【0013】 根據本發明一實施例，其揭示一種提供一資訊設備具安全

【0014】 防護連結之遠端診斷的方法。該方法包括步驟如下：接收來自終端介面之命令；執行一認證/授權/稽核(AAA)模組以檢示該命令；若一遠端診斷模組已被啓用，判定是否已與一遠端資訊設備間建立一具安全防護之連結；及經由該具安全防護連結，傳送該命令至一遠端資訊設備。

【0015】 根據本發明另一實施例，其揭示一種提供一資訊設備具安全防護連結之遠端診斷的方法。該方法包括步驟如下：偵測到一失效狀態；若一遠端診斷模組已被啓用，則擷取一預定之指派關係配置中可信賴資訊設備之IP位址及埠號，以建立訊息傳送路徑；建立與該可信賴資訊設備間安全防護之連結；及若本地命令行界面CLI程序可用，則橋接該具安全防護之

連結與該本地命令行界面CLI程序之輸入/輸出。

【0016】 根據本發明另一實施例，其揭示一種電腦程式產品包含一儲存有程式碼之電腦可讀媒體，供於一資訊設備上執行時，實施如前述之方法，以提供一資訊設備具安全防護連結之遠端診斷。

【0017】 根據本發明另一實施例，其揭示一種資訊設備，包含：

一匯流排；

一記憶體，連接到該匯流排，其中該記憶體包含一組指令；

一連接到該匯流排之處理單元，其中該處理單元執行該組指令，以執行如前述之方法，以提供一資訊設備具安全防護連結之遠端診斷。

【0018】 本說明書中所提及的特色、優點、或類似表達方式並不表示，可以本發明實現的所有特色及優點應在本發明之任何單一的具體實施例內。而是應明白，有關特色及優點的表達方式是指結合具體實施例所述的特定特色、優點、或特性係包含在本發明的至少一具體實施例內。因此，本說明書中對於特色及優點、及類似表達方式的論述與相同具體實施例有關，但亦非必要。

【0019】 此外，可以任何合適的方式，在一或多個具體實施例中結合本發明所述特色、優點、及特性。相關技術者應明白，在沒有特定具體實施例之一或多個特定特色或優點的情況下，亦可實施本發明。在其他例子中應明白，特定具體實施例中的其他特色及優點可能未在本發明的所有具體實施例中出現。

【0020】 參考以下說明及隨附申請專利範圍或利用如下文所提之本發明的實施方式，即可更加明瞭本發明的這些特色及優點。

【圖式簡單說明】

【0021】 爲了立即瞭解本發明的優點，請參考如附圖所示的特定具體實施例，詳細說明上文簡短敘述的本發明。在瞭解這些圖示僅描繪本發明

的典型具體實施例並因此不將其視爲限制本發明範疇的情況下，參考附圖以額外的明確性及細節來說明本發明，圖式中：

【0022】 圖1係顯示本發明一例示性實施例中包含複數個資訊設備之叢集的硬體環境方塊示意圖；

【0023】 圖2揭示根據本發明實施例之資訊設備之系統架構的示意圖；

【0024】 圖3A揭示根據本發明實施例之應用例之訊息流程的示意圖；

【0025】 圖3B揭示根據本發明實施例之網路系統管理員藉由可信賴系統(或資訊設備)之命令行界面（CLI）進行診斷或修復之終端介面之應用例圖示；

【0026】 圖4A揭示根據本發明實施例之診斷模組之方法流程圖；

【0027】 圖4B揭示根據本發明實施例之角色式管理模組(RBM)之方法流程圖。

【實施方式】

【0028】 本說明書中「一具體實施例」或類似表達方式的引用是指結合該具體實施例所述的特定特色、結構、或特性係包括在本發明的至少一具體實施例中。因此，在本說明書中，「在一具體實施例中」及類似表達方式之用語的出現未必指相同的具體實施例。

【0029】 熟此技藝者當知，本發明可實施爲資訊設備、方法或作爲電腦程式產品之電腦可讀媒體。因此，本發明可以實施爲各種形式，例如完全的硬體實施例、完全的軟體實施例（包含韌體、常駐軟體、微程式碼等），或者亦可實施爲軟體與硬體的實施形式，在以下會被稱爲「電路」、「模組」或「系統」。此外，本發明亦可以任何有形的媒體形式實施爲電腦程式產品，其具有電腦可使用程式碼儲存於其上。

【0030】 一個或更多個電腦可使用或可讀取媒體的組合都可以利用。舉例來說，電腦可使用或可讀取媒體可以是（但並不限於）電子的、磁的、光學的、電磁的、紅外線的或半導體的系統、裝置、設備或傳播媒體。更具體的電腦可讀取媒體實施例可以包括下列所示（非限定的例示）：由一個或多個連接線所組成的電氣連接、可攜式的電腦磁片、硬碟機、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除程式化唯讀記憶體(EPROM或快閃記憶體)、光纖、可攜式光碟片（CD-ROM）、光學儲存裝置、傳輸媒體（例如網際網路(Internet)或內部網路(intranet)之基礎連接）、或磁儲存裝置。需注意的是，電腦可使用或可讀取媒體更可以爲紙張或任何可用於將程式列印於其上而使得該程式可以再度被電子化之適當媒體，例如藉由光學掃描該紙張或其他媒體，然後再編譯、解譯或其他合適的必要處理方式，然後可再度被儲存於電腦記憶體中。在本文中，電腦可使用或可讀取媒體可以是任何用於保持、儲存、傳送、傳播或傳輸程式碼的媒體，以供與其相連接的指令執行系統、裝置或設備來處理。電腦可使用媒體可包括其中儲存有電腦可使用程式碼的傳播資料訊號，不論是以基頻(baseband)或是部分載波的型態。電腦可使用程式碼之傳輸可以使用任何適體的媒體，包括（但並不限於）無線、有線、光纖纜線、射頻(RF)等。

【0031】 用於執行本發明操作的電腦程式碼可以使用一種或多種程式語言的組合來撰寫，包括物件導向程式語言（例如Java、Smalltalk、C++或其他類似者）以及傳統程序程式語言（例如C程式語言或其他類似的程式語言）。程式碼可以獨立軟體套件的形式完整的於使用者的電腦上執行或部分於使用者的電腦上執行，或部分於使用者電腦而部分於遠端電腦。

【0032】 於以下本發明的相關敘述會參照依據本發明具體實施例之資訊設備、方法及電腦程式產品之流程圖及／或方塊圖來進行說明。當可理解每一個流程圖及／或方塊圖中的每一個方塊，以及流程圖及／或方塊圖中方塊的任何組合，可以使用電腦程式指令來實施。這些電腦程式指令

可供通用型電腦或特殊電腦的處理器或其他可程式化資料處理裝置所組成的機器來執行，而指令經由電腦或其他可程式化資料處理裝置處理以便實施流程圖及／或方塊圖中所說明之功能或操作。

【0033】 這些電腦程式指令亦可被儲存在電腦可讀取媒體上，以便指示電腦或其他可程式化資料處理裝置來進行特定的功能，而這些儲存在電腦可讀取媒體上的指令構成一製成品，其內包括之指令可實施流程圖及／或方塊圖中所說明之功能或操作。

【0034】 電腦程式指令亦可被載入到電腦上或其他可程式化資料處理裝置，以便於電腦或其他可程式化裝置上進行一系統操作步驟，而於該電腦或其他可程式化裝置上執行該指令時產生電腦實施程序以達成流程圖及／或方塊圖中所說明之功能或操作。

【0035】 其次，請參照圖1至圖7，在圖式中顯示依據本發明各種實施例的資訊設備、方法及電腦程式產品可實施的架構、功能及操作之流程圖及方塊圖。因此，流程圖或方塊圖中的每個方塊可表示一模組、區段、或部分的程式碼，其包含一個或多個可執行指令，以實施指定的邏輯功能。另當注意者，某些其他的實施例中，方塊所述的功能可以不依圖中所示之順序進行。舉例來說，兩個圖示相連接的方塊事實上亦可以同時執行，或依所牽涉到的功能在某些情況下亦可以依圖示相反的順序執行。此外亦需注意者，每個方塊圖及／或流程圖的方塊，以及方塊圖及／或流程圖中方塊之組合，可藉由基於特殊目的硬體的系統來實施，或者藉由特殊目的硬體與電腦指令的組合，來執行特定的功能或操作。

<硬體環境>

【0036】 圖1係顯示本發明一例示性實施例中包含複數個資訊設備之叢集的硬體環境方塊示意圖。在一實施例中，該叢集100包含3個資訊設備（100a, 100b, 100c）。 該資訊設備可以是IBM WebSphere DataPower Series

SOA Appliances 或Tivoli ISS Appliances的硬體架構。資訊設備（100a, 100b, 100c）具有處理器以執行專屬的應用程式；儲存裝置以儲存各種資訊及程式碼；通訊及輸出/入裝置做爲與使用者溝通之介面；以及週邊元件或其他特定用途元件。在其他實施例中，本發明亦可實施爲其他的形式，而具有更多或更少之其他裝置或元件。叢集100中之複數個資訊設備（100a, 100b, 100c）負責處理透過網路120接收到之外部企業夥伴系統(或用戶端電腦)的訊息，且傳送結果給後面的企業內部系統之網路伺服器上之一後端應用（backend）。該訊息可以是一封包、一TCP流或一交易。

【0037】 如圖1所示，資訊設備（100a, 100b, 100c）可具有處理器10、記憶體20與輸入/輸出(I/O)單元40。該輸入/輸出(I/O)匯流排可爲一高速串接匯流排，例如PCI-e匯流排，但其它的匯流排架構亦可以被使用。其它對輸入/輸出(I/O)匯流排的連接可以藉由直接元件互連，或是透過附加卡的方式。輸入/輸出(I/O)單元也可耦接至一硬碟機50、區域網路(LAN)配接器60。透過該區域網路配接器60，資訊設備（100a, 100b, 100c）能經由一網路120與一用戶端電腦通信。網路亦可實施爲任何型式之連線，包括固定連接之區域網路(LAN)或廣域網路(WAN)連線，或利用網際網路服務提供者來暫時撥接至網際網路，亦不限於有線無線等各種連接方式，例如透過GSM、或Wi-Fi等無線網路與用戶端電腦通信。然而應了解，雖未繪示但其他硬體及軟體組件(例如額外電腦系統、路由器、防火牆等)可包含於網路之中。記憶體20可爲隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除程式化唯讀記憶體(EPROM或快閃記憶體)。記憶體20用以存放作業系統、專屬的應用程式（application）與本發明主程式AP之程式碼及各種資訊。作業系統在處理器10上執行，用來協調並提供資訊設備（100a, 100b, 100c）中各種元件的控制，而處理器10可存取記憶體20，以執行主程式AP。該專屬的應用程式包含根據特定目的或特定服務而設計，以進行特定的交易之資訊設備的程式碼，以處理收到的訊息。

【0038】 主程式AP可包括一本發明之一診斷模組及一角色式管理模組。該角色式管理模組至少包含一習知之認證/授權/稽核(AAA)模組及本發明之一指派(delegated)存取模組。該診斷模組及該角色式管理模組包括程式模組及指令，供實施本發明之一種具安全防護連結之遠端診斷的方法。該診斷模組及該角色式管理模組可以是應用程式內之模組，或以常駐程式(Daemon)之方式實施。但在其他實施例中，亦可以用其他形式之程式型態來實施。該診斷模組及該角色式管理模組包括用於實施下文所說明之圖4A及4B內所說明之程序之代碼。

【0039】 熟此技藝者應可知，圖1中所述資訊設備（100a, 100b, 100c）的硬體可以依照不同的實施例而有各種變化。亦有其它的內部硬體或週邊裝置，例如快閃唯讀記憶體(Flash ROM)、等效的非揮發記憶體、或光碟機等等，可以附加或取代圖1所示的硬體。

【0040】 圖2揭示根據本發明實施例之資訊設備之系統架構的示意圖。該資訊設備之系統架構包含資訊設備之系統本身及一網路介面卡230。

【0041】 該系統本身包含一位於核心(kernel)空間220之資訊設備作業系統222，及位於一使用者空間210之網路界面(web interface)212、命令行界面214及一角色式管理模組(RBM) 216。該角色式管理模組(RBM) 216包含一習知之認證/授權/稽核(AAA)模組217及本發明之一指派存取模組218。關於「核心空間220」及「使用者空間210」之詳細說明，可分別參考下列網頁：

http://www.linfo.org/kernel_space.html

http://www.linfo.org/user_space.html

【0042】 認證/授權/稽核(AAA)模組217實施認證檢示(check)，以判定是否欲登入之使用者被允許使用該資訊設備，接著檢示是否該已認證之使用者被允許發出某種命令(即被授權)。例如，網路系統管理員可建立一稱爲"支援使用者(Backup user)"的使用者，其只能發出由資訊設備作業系統222提

供之系統支援相關命令。該認證/授權/稽核(AAA)模組217是一習知技術。關於「角色式管理模組(RBM)」及「認證/授權/稽核(AAA) 模組」之詳細說明，可分別參考下列網頁：

http://www.redbooks.ibm.com/abstracts/sg247901.html?Open 及

http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting 或

http://en.wikipedia.org/wiki/AAA_protocol

【0043】 資訊設備作業系統222將提供一組可用於網路界面212及命令行界面214之命令。網路界面212及命令行界面214由該資訊設備之用戶端存取程式使用以執行系統提供之命令。該用戶端存取程式可以是一網路瀏覽器、一安全防護殼層(secure shell，ssh) 終端程式或串列埠用之終端介面(console)。當該命令執行時，該角色式管理模組(RBM) 216將於傳送命令至該作業系統222前，執行安全防護檢示。關於安全防護殼層(ssh) 終端程式之詳細說明，可參考下列網頁：

http://www.ssh.com/manuals/server-admin/32/Introduction_to_SSH_Secure_Shell.html

【0044】 指派存取模組218係本發明之核心組件之一，其提供在一系統上之使用者可經由網路控制其他系統(或資訊設備)。一系統(或資訊設備)於執行時段系統配置(configure)存取之指派關係時，該資訊設備將建立一具安全防護之連結(如TCP/IP連結)至相同叢集(或網段)中一可信賴之系統(或資訊設備)。當該資訊設備落入失效狀態(如當機、核心錯誤(kernel panic)或不能重新啓動核心程序)時，一診斷模組232偵測到系統有問題且建立一具安全防護之連結至該可信賴系統(或資訊設備)。接著，網路系統管理員於該可信賴系統上執行命令(通常爲診斷相關之命令)。該指派存取模組218檢示之後，該命令將經由具安全防護之TCP/IP連結傳送至該失效之系統(或資訊設備)。

【0045】 該網路介面卡230包含一TCP/IP堆疊，因而能建立一與該資訊設備之作業系統無關之TCP/IP連結。該網路介面卡330通常實施爲一系統單晶片(SOC)或一特殊應用積體電路 (ASIC)。該網路介面卡230另包含一診斷模組232。該診斷模組232係本發明之另一核心組件。該診斷模組232被用來建立一具安全防護之連結至一可信賴系統(或資訊設備)。當網路系統管理員致能該指派存取功能時，該系統(或資訊設備)之IP位址及埠號（port）資訊被傳送至該診斷模組232，以建立訊息傳送路徑，因此該診斷模組232知道相同叢集(或網段)中哪一系統(或資訊設備)是可信賴的。當該系統(或資訊設備)落入失效狀態時，該診斷模組232將因此建立一具安全防護之連結至該可信賴系統。該失效系統(或資訊設備)由該可信賴系統收到診斷相關之命令，該診斷模組232將導向(direct)所有由網路收到/發出的輸入/輸出，即控制所有由網路收到/發出的輸入/輸出之傳送。該管理員因此能執行遠端診斷程序。

【0046】 當該系統(或資訊設備)落入失效狀態時，可依系統狀況之實際嚴重程度，以判定是否該失效系統(或資訊設備)之命令行界面214程序可被啓用(initiate)。

1）若失效系統(或資訊設備)仍可啓用其命令行界面（CLI），即該失效系統仍可用，則該可信賴系統(或資訊設備)對該失效目標裝置下達之修復命令，可直接導向該命令至該目標裝置之命令行界面CLI程序，即傳送至該目標裝置之命令行界面程序。

2）若失效系統之命令行界面無法被啓用(即不可用)，則該失效系統之網路介面卡將重新導向(redirect) 供網路系統管理員診斷系統問題之習知的資訊設備管理埠或串列埠至該可信賴系統。即所提供之用於網路系統管理員診斷系統問題的習知管理埠或串列埠，將被用來接收來自可信賴資訊設備之命令，供診斷及修復該失效目標裝置之系統問題，該管理員因此能執行遠端修復程序。關於「診斷模組232」及「指派存

取模組218」之進一步說明將參照圖4A及4B而詳述於後。

<較佳實施例之應用例>

【0047】 圖3A揭示根據本發明實施例之應用例之訊息流程的示意圖。如圖3A所示，其包含一健康且可信賴之資訊設備A及一失效之資訊設備B。其分別包含對應於圖2所示各組件，在此不再贅述。 當資訊設備B失效時，根據本發明實施例應用例之處理流程如下：

1）首先，當資訊設備B失效時，資訊設備B之診斷模組332b將與可信賴之資訊設備A間，建立一具安全防護之TCP/IP連結，以允許資訊設備A之指派存取模組318a能偵測資訊設備B之狀態。一般情形，兩資訊設備間可以RSA金鑰對(key pair)對該連結加密。

2）一網路系統管理員(或使用者)登入資訊設備A之命令行界面（CLI）314a之終端介面。該管理員可選擇一遠端診斷模式。

3）該管理員鍵入一命令(通常爲診斷相關之命令)。該命令先由資訊設備A之認證/授權/稽核(AAA)模組317a檢示。例如判定是否欲登入之管理員被允許使用該資訊設備，接著檢示是否該已認證之使用者被允許發出某種命令(即被授權)。一旦該命令通過該檢示，資訊設備A之指派存取模組318a將建立底層輸入/輸出連結供傳送該命令。

4）該命令經由該具安全防護之TCP/IP連結被傳送至資訊設備B之診斷模組332b。

5）若該資訊設備B之核心程序(包含命令行界面（CLI）314b) 仍可啓用，則該命令可直接傳送至該資訊設備B之指派存取模組318b而由該資訊設備B之作業系統322b執行。

若該資訊設備B之核心程序已不能啓用(如發生核心錯誤)，則該資訊設備B之網路介面卡330b所提供之用於網路系統管理員診斷系統問題的習知管理埠或串列埠，將被用來接收來自可信賴資訊設備之命令，供

診斷及修復該失效目標裝置之系統問題。

【0048】 圖3B揭示根據本發明實施例之網路系統管理員藉由可信賴系統(或資訊設備)之命令行界面（CLI）進行診斷或修復之終端介面之應用例圖示。首先，一網路系統管理員透過一安全防護殼層(ssh) 終端程式登入一可信賴之資訊設備(dpbox21)440。登入後該管理員於提示符(xb60#)後鍵入顯示相同叢集(或網段)中之失效資訊設備442。如例示，該可信賴資訊設備(dpbox21)收到兩個失效資訊設備(dpbox25、dpbox31)。接著，該管理員切換命令行界面（CLI）至失效資訊設備(dpbox25)444，即出現提示符(xb60<dpbox25-fail-safe>#)。最後，該管理員執行修復指令，而重新啓動載入舊版本韌體(5.0.0.0..)。

<診斷模組 232>

【0049】 圖4A揭示根據本發明實施例之診斷模組之方法流程圖。

- 步驟 410：資訊設備偵測到失效狀態。
- 步驟 412：判定遠端診斷模組是否已被啓用。
- 步驟 414：擷取一預定之指派關係配置中可信賴資訊設備之 IP 位址及埠號，以建立訊息傳送路徑。
- 步驟 416：建立與該可信賴資訊設備間安全防護之連結。
- 步驟 418：判定是否本地命令行界面 CLI 組件(程序)可用。
- 步驟 420：若本地命令行界面 CLI 組件(程序)可用，則橋接該具安全防護之連結(如 TCP/IP 連結)與該本地命令行界面 CLI 組件之輸入/輸出。即傳送命令至 CLI 組件。
- 步驟 422：若本地命令行界面 CLI 組件(程序)不可用，則橋接該具安全防護之連結與本地管理埠間之輸入/輸出。該失效資訊設備之網路介面卡將重新導向(redirect) 供網路系統管理員診斷系統問題之習知的資訊設備管理埠或串列埠至該可信

賴資訊設備。即該失效之資訊設備所提供之用於網路系統管理員診斷系統問題的習知管理埠或串列埠，將被用來接收來自可信賴資訊設備之命令，供診斷及修復該失效目標裝置之系統問題。

<角色式管理模組(RBM)>

【0050】 圖4B揭示根據本發明實施例之角色式管理模組(RBM)之方法流程圖。圖示中包含習知之認證/授權/稽核(AAA)模組。

- 步驟 430：接收來自終端介面(console)之命令。
- 步驟 432:由習知之認證/授權/稽核(AAA)模組執行檢示該命令。例如判定是否欲登入之管理員被允許使用該資訊設備，接著檢示是否該已認證之使用者被允許發出某種命令。
- 步驟 434：判定一遠端診斷模組是否已被啓用。
- 步驟 436：若無遠端診斷模組被啓用，代表該收到之命令並非用於遠端診斷，則作爲本地命令執行該命令。
- 步驟 438：若遠端診斷模組已被啓用，進一步判定是否已與遠端資訊設備間建立一具安全防護之連結(如 TCP/IP 連結)。
- 步驟 440：若具安全防護之連結已建立，經由該具安全防護連結傳送命令至遠端資訊設備。
- 步驟 442：由該具安全防護連結取得回應。

【0051】 需說明的是，如前述，本發明藉由利用橋接用資訊設備及該目標裝置中之角色式管理(RBM)內之認證/授權/稽核(AAA)模組，該機制可提供診斷作業一更細密之存取控制。如前述，當該系統(或資訊設備)落入失效狀態時，本發明可依系統狀況之實際嚴重程度，以判定是否該失效系統(或資訊設備)之命令行界面程序可被啓用。事實上，依系統狀況之實際嚴重程度，本發明也可有其他選替方式執行診斷與修復。

【0052】 因此，在不脫離本發明精神或必要特性的情況下，可以其他特定形式來體現本發明。應將所述具體實施例各方面僅視爲解說性而非限制性。因此，本發明的範疇如隨附申請專利範圍所示而非如前述說明所示。所有落在申請專利範圍之等效意義及範圍內的變更應視爲落在申請專利範圍的範疇內。

【符號說明】

100	叢集
100a、100b、100c	資訊設備
10	處理器
20	記憶體
40	輸入/輸出(I/O)單元
50	硬碟機
60	區域網路(LAN)配接器
120	網路
210	使用者空間
212、312a、312b	網路界面(web interface)
214、314a、314b	命令行界面CLI
216、316a、316b	角色式管理模組(RBM)
217、317a、317b	認證/授權/稽核(AAA)模組
218、318a、318b	指派存取模組
220	核心(kernel)空間
222、322a、322b	資訊設備作業系統
230、330a、330b	網路介面卡
232、332a、332b	診斷模組

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】無

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】無

【序列表】(請換頁單獨記載)無

申請專利範圍

1. 一種提供一資訊設備具安全防護連結之遠端診斷的方法，包含，

接收來自終端介面之命令；

執行一認證/授權/稽核(AAA)模組以檢示該命令；

若一遠端診斷模組已被啓用，判定是否已與一遠端資訊設備間建立一具安全防護之連結；及

經由該具安全防護連結，傳送該命令至一遠端資訊設備。

2. 如請求項 1 之方法，其中該連結係一 TCP/IP 連結。

3. 如請求項 1 之方法，其進一步包含，

由該具安全防護連結取得回應。

4. 一種提供一資訊設備具安全防護連結之遠端診斷的方法，包含，

偵測到一失效狀態；

若一遠端診斷模組已被啓用，則擷取一預定之指派關係配置中可信賴資訊設備之 IP 位址及埠號，以建立訊息傳送路徑；

建立與該可信賴資訊設備間安全防護之連結；及

若本地命令行界面 CLI 程序可用，則橋接該具安全防護之連結與該本地命令行界面 CLI 程序之輸入/輸出。

5. 如請求項 4 之方法，其進一步包含，

若本地命令行界面 CLI 程序不可用，則橋接該具安全防護之連結與一本地管理埠間之輸入/輸出。。

6. 如請求項 4 之方法，其中該連結係一 TCP/IP 連結。

7. 一種電腦程式產品包含一儲存有程式碼之電腦可讀媒體，供於一資訊設備上執行時，實施如請求項 1 至 6 中任一項之方法，以提供一具安全防護連結之遠端診斷。

8. 一種資訊設備，包含：

一匯流排；

一記憶體，連接到該匯流排，其中該記憶體包含一組指令；

一連接到該匯流排之處理單元，其中該處理單元執行該組指令，以執行如申請專利範圍第 1 至 6 項之任一項所述之方法，以提供一具安全防護連結之遠端診斷。

圖式

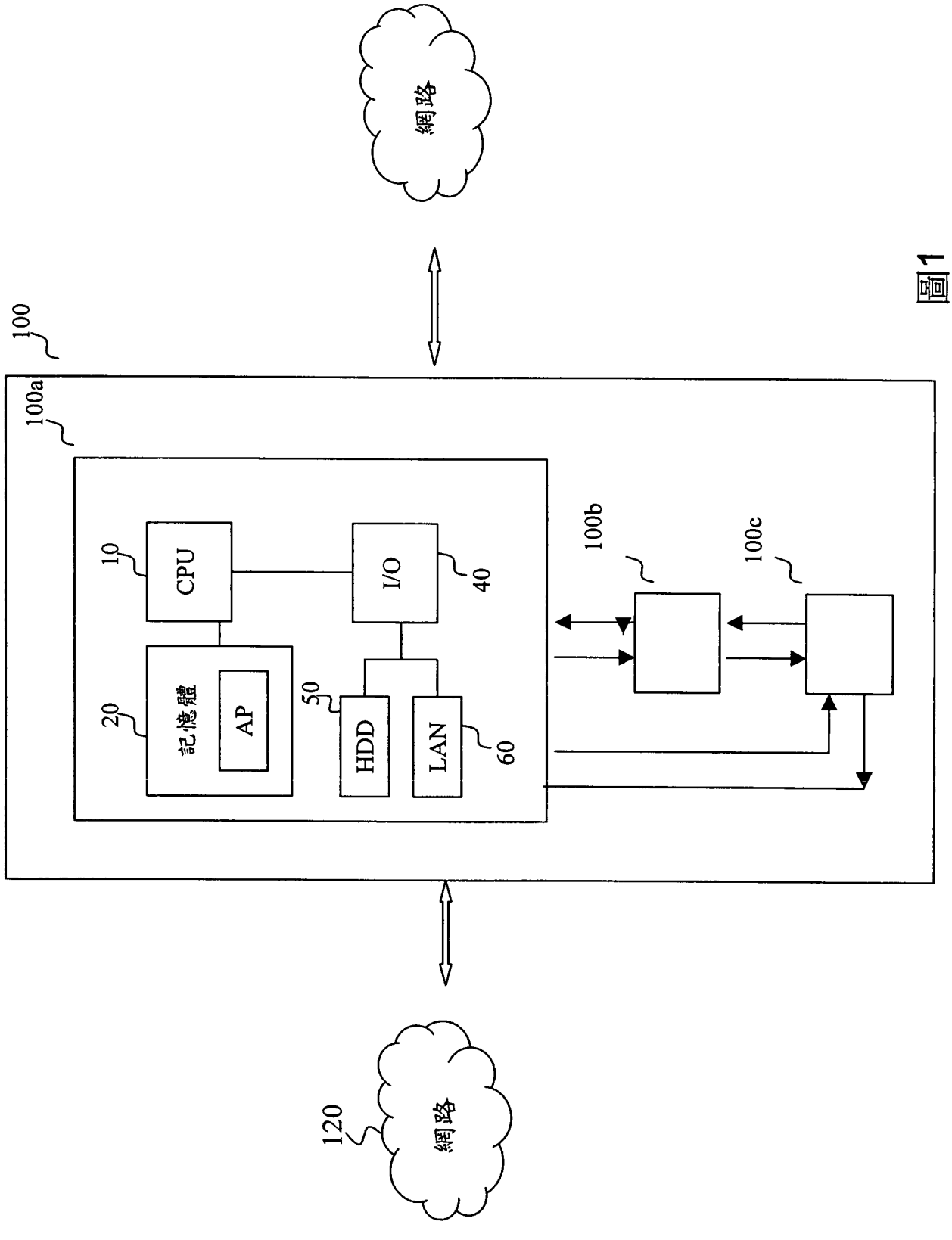

圖1

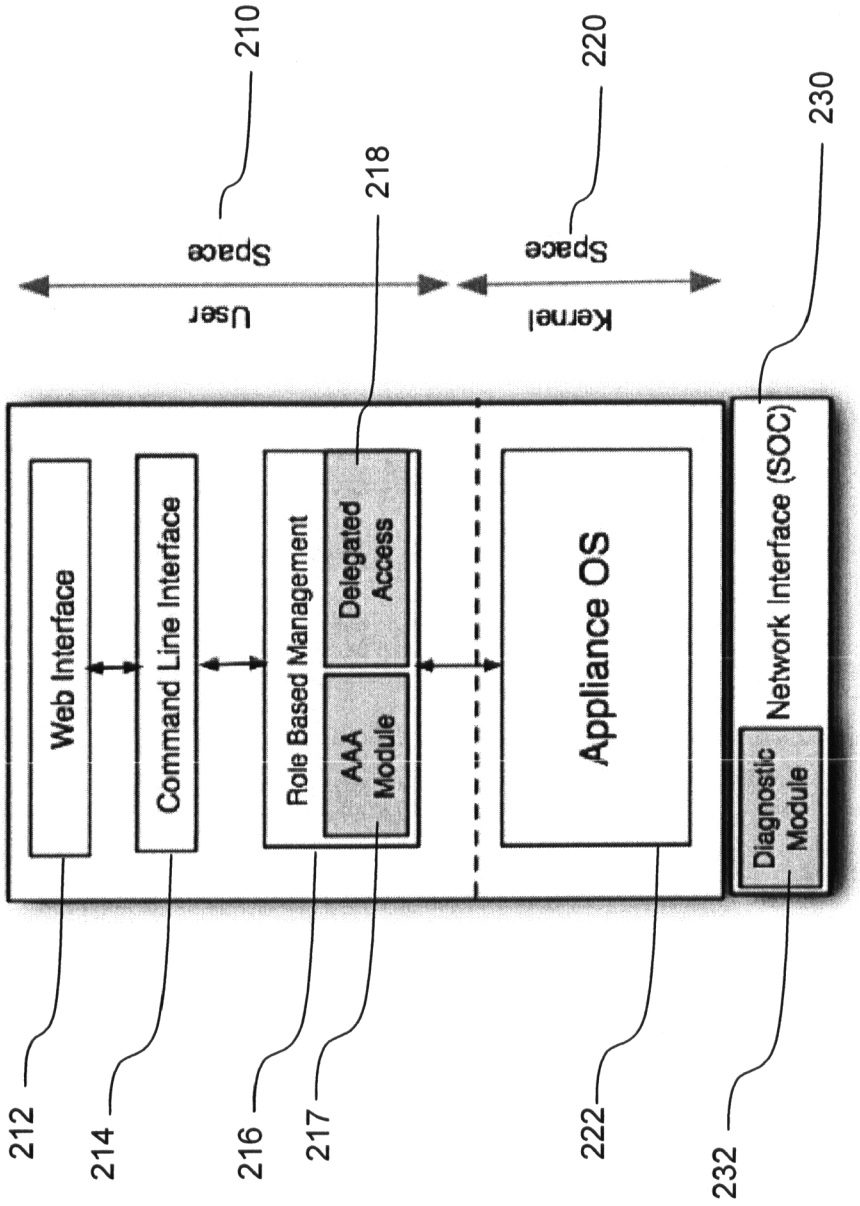
User Space
Kernel Space
210
220
218
230
Web Interface
Command Line Interface
Role Based Management
AAA Module
Delegated Access
Appliance OS
Network Interface (SOC)
Diagnostic Module
212
214
216
217
222
232

圖2

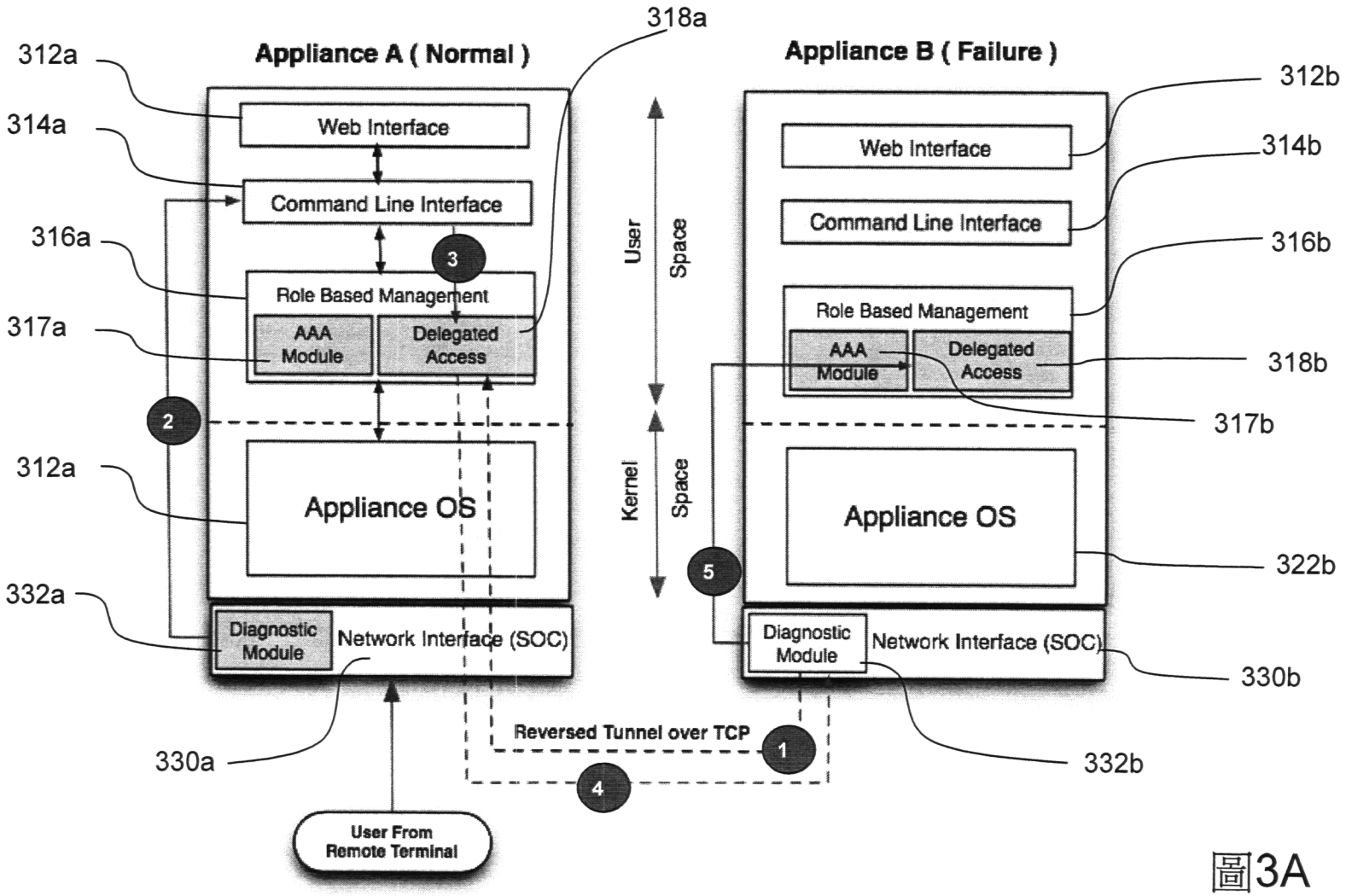
Appliance A (Normal)
Appliance B (Failure)
312a
314a
316a
317a
312a
332a
330a
318a
312b
314b
316b
318b
317b
322b
330b
332b
Web Interface
Command Line Interface
Role Based Management
AAA Module
Delegated Access
Appliance OS
Diagnostic Module
Network Interface (SOC)
User Space
Kernel Space
Reversed Tunnel over TCP
User From Remote Terminal
1
2
3
4
5

圖3A

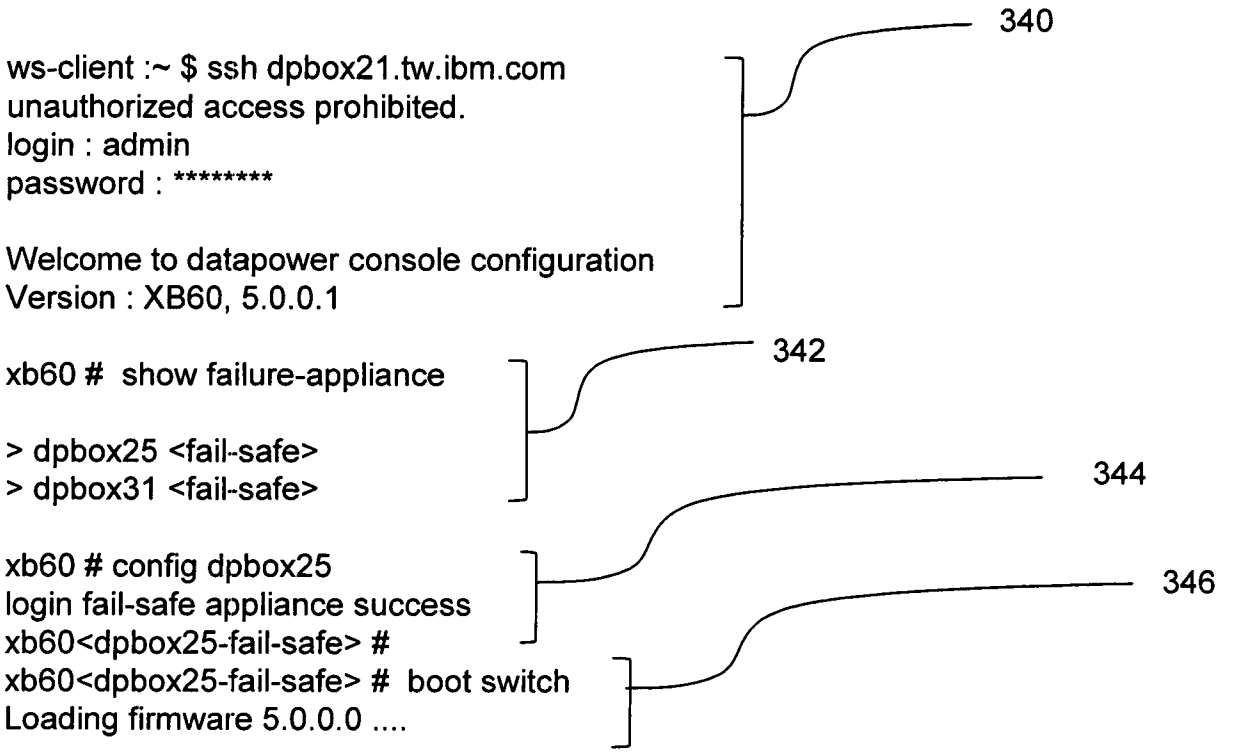
340
ws-client :~ $ ssh dpbox21.tw.ibm.com
unauthorized access prohibited.
login : admin
password : ********
Welcome to datapower console configuration
Version : XB60, 5.0.0.1
342
xb60 # show failure-appliance
> dpbox25 <fail-safe>
> dpbox31 <fail-safe>
344
xb60 # config dpbox25
login fail-safe appliance success
xb60<dpbox25-fail-safe> #
346
xb60<dpbox25-fail-safe> # boot switch
Loading firmware 5.0.0.0 ....

圖3B

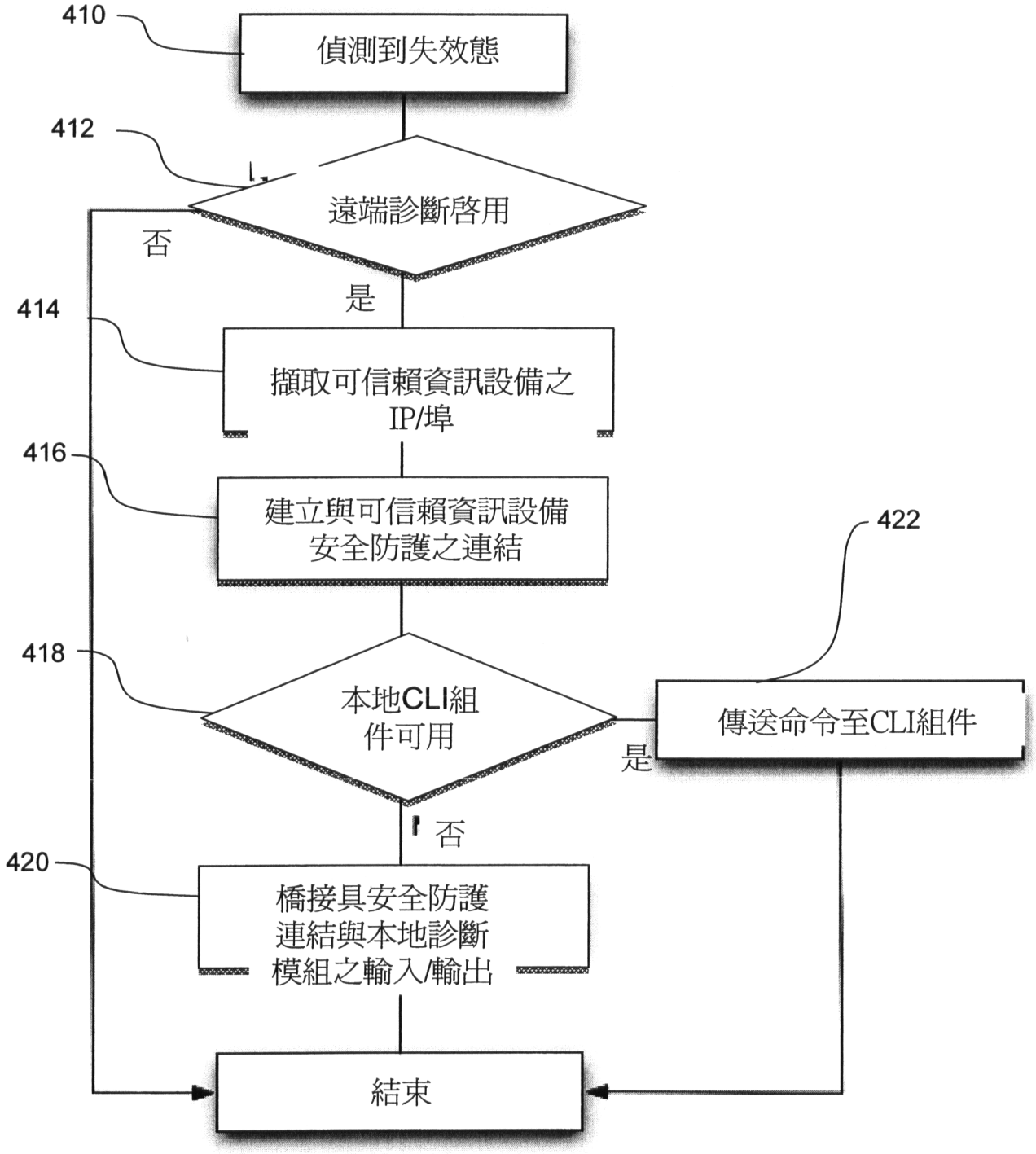
410
偵測到失效態
412
遠端診斷啓用
否
是
414
擷取可信賴資訊設備之
IP/埠
416
建立與可信賴資訊設備
安全防護之連結
418
本地CLI組
件可用
是
422
傳送命令至CLI組件
否
420
橋接具安全防護
連結與本地診斷
模組之輸入/輸出
結束

圖4A

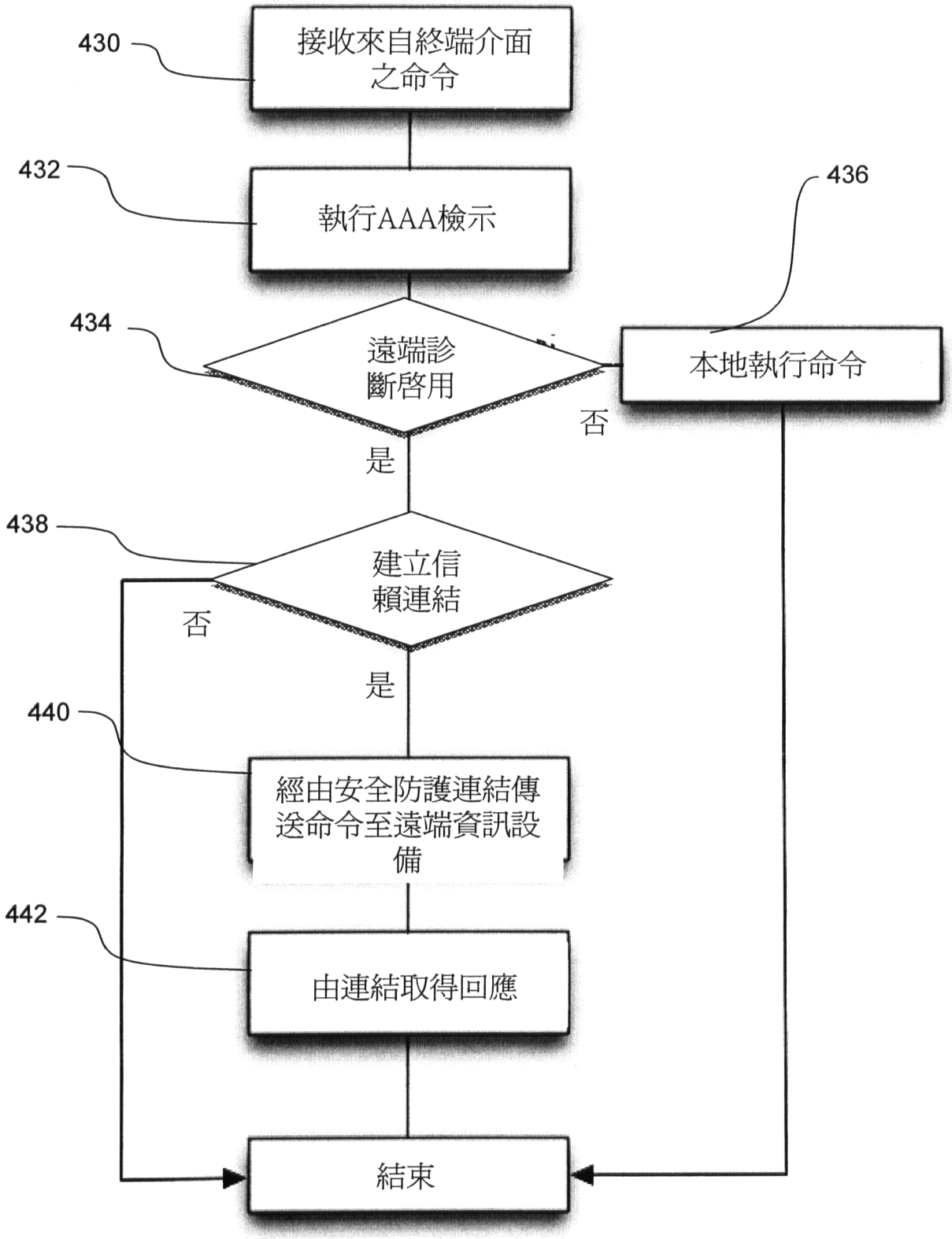
430
接收來自終端介面之命令
432
執行AAA檢示
436
434
遠端診斷啓用
本地執行命令
否
是
438
建立信賴連結
否
是
440
經由安全防護連結傳送命令至遠端資訊設備
442
由連結取得回應
結束

圖4B