1 Windows 2000 介紹

1.1 Windows 2000 簡介

Windows 2000 爲一整合主從式架構網路(Client /Server)及點對點(Peer To Peer)網路的作業系統，且提高了網路通訊服務及檔案資源的安全性並於 Windows 2000 Server 中加入了新的目錄服務(Active Directory)的管理技術，能讓管理者及使用者更有效率的管理及使用。

1.1.1 版本介紹

在 Windows 2000 又可分爲下列四種版本，說明如下。

Windows 2000 Professional

Windows 2000 技術平台，適用於個人工作站和企業平台，支援隨插即用、電源管理和檔案加密等整合性安全機制。

Windows 2000 Server

Windows 2000S Server 適用於中小型企業或多部門網路管理的作業系統，它以 Active Directory 目錄服務做爲一完整的服務模式，具有高度延展性的多用途目錄服務技術，它能有效的簡化網路資源管理。Windows 2000 Server 可爲檔案伺服器及網路管理的相關伺服器等功能，爲最佳，且穩定性高的作業系統。最多可支援 4 顆中央處理器和 4 GB 的記憶體。

Windows 2000 Advanced Server

除了提供Windows 2000 Server有的功能和特性之外，還提供更多的網際網路服務和網路負載平衡(Network Load Balancing)功能，並且支援2節點的叢集架構(Clustering Infrastructure)。

說明

叢集架構：當伺服器臨時發生故障時，另一台的伺服器可以隨時接手繼續正常動作。

Windows 2000 Datacenter Server

爲Windows 2000系列中最高階的伺服器，除了擁有上述伺服器的所有功能外還提供了資料倉儲(Data Warehousing)和線上交易處理(On-line Transaction Processing)等企業解決方案，適用於大型資料處理和多伺服器的整合，並且支援4節點的叢集架構(Clustering Infrastructure)，最多可支援32顆中央處理器和64GB的記憶體。

下表爲總結了Windows 2000系列間的差異，如果您目前使用Windows NT或是Windows 98/95，Windows 2000都將會是最佳選擇的網路作業系統。

Windows 2000版本	Windows 2000 Professional	Windows 2000 Server	Windows 2000 Advanced Server	Windows 2000 Datacenter
適用族群	個人工作站和企業平台	中小型企業或多部門網路管理	大型企業或多部門網路管理	大型資料處理和多伺服器的整合
支援CPU數量	2	4	8	32
記憶體	4 GB	4 GB	8 GB	64 GB
支援叢集架構	不支援	不支援	2節點叢集架構	4節點叢集架構

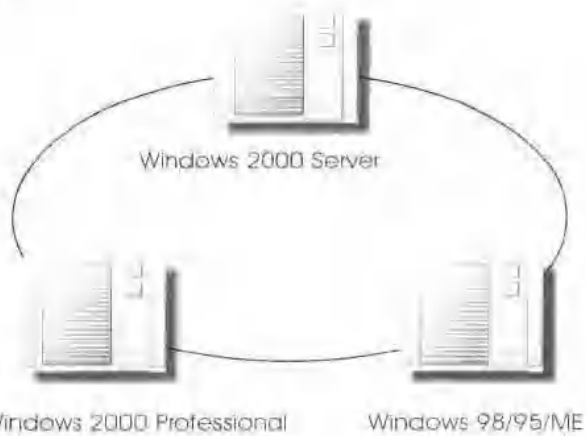
1.1.2 Windows 2000 網路架構

Windows 2000網路架構的建置上又可以分爲群組和網域兩種模式，來進行電腦間的溝通與資源的共享。

群組

群組(Workgroup)爲一點對點(Peer To Peer)的網路模式，此模式並不需要任何的伺服器來管理，在此群組中的電腦平等的的分享到資源，每一個資源的共享是由加入群組中的電腦來做分享的設定，如使用者欲儲存該項資源必須擁有存取資源的帳戶及密碼，此架構管理方式簡便，適合一般管理小於十台電腦以下的環境。

Windows 2000群組可包含任何的工作平台，如Windows 2000 Professional、Windows 2000 Server及Windows 98等，在群組中的Windows 2000 Server稱爲獨立伺服器，如下圖。



群組爲一點對點的網路模式，群組中可包含任何工作平台的主機。

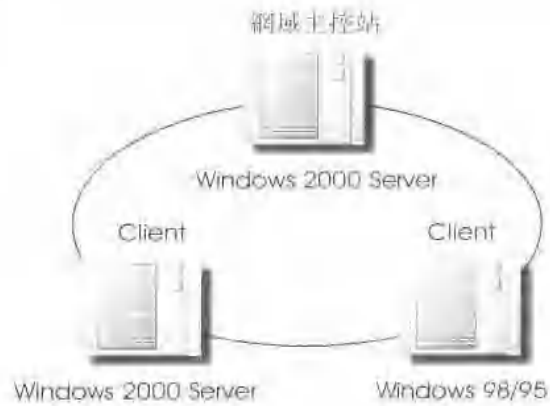
網域

網域(Domain)爲一集中式管理的網路架構，在Windows 2000 Server中加入了目錄服務(Active Directory)的新管理技術，此目錄服務中包含了使用者及網域內所有物件的資料，這些資料都存放於目錄服務資料庫(Active Directory Database)內，而此資料庫存放於網域控制站中將資源及使用者資料做集中管理，於此環境中只要所設定的使用者權限足夠就可存取網域中其他電腦中的所分享出來的資源。

網域控制站將使用用者的資料及原則存放於目錄服務資料庫內，也對使用者做網域登入的驗證工作，如網域中有一台以上的的網域控制站(Domain Controller)，則會複製彼此目錄資料庫內容，內定每五分鐘進行複製工作。

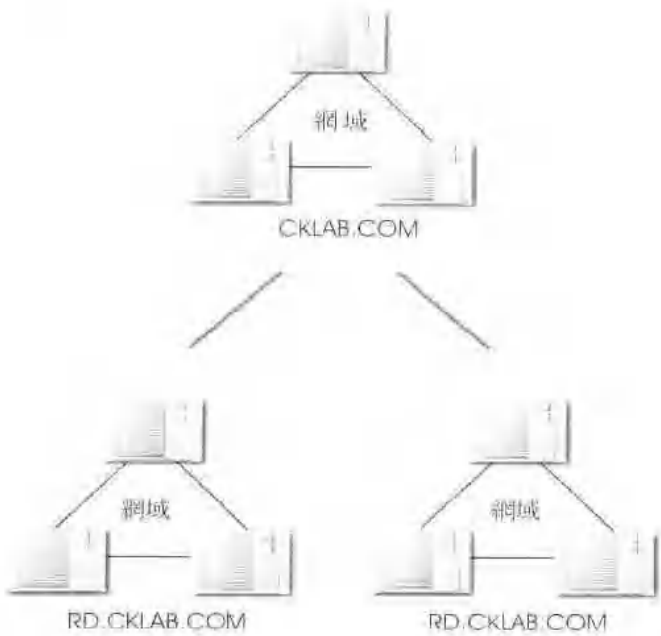
網域組織成員包含了執行Windows 2000 Server的網域控制站、執行Windows 2000 Server成員伺服器（Member Server）和執行Windows 2000 Professional的用戶端(Client)等，如下圖。

網域爲集中式管理的網路架構，其成員包含了網域控制站、成員伺服器和用戶端等。



樹狀網域

樹狀網域爲階層式的網域管理方式，在此階層中的網域可相互分享其資源，只要使用者有足夠權限即可登入其中任何一網域存取資源，所有階層的網域皆存放本身的資料於目錄資料庫中(Active Directory Database)，此網域架構採用連續命名方式(例：有一父網域名稱爲CKLAB.COM，則其子網域名稱爲RD.CKLAB.COM，也就是說其子網域命名必須包含父網域之名稱)，如下圖。



1.2 Active Directory

1.2.1 何謂 Active Directory

Active Directory 目錄服務在 Windows 2000 Server 中的階層網域架構中，提供了管理者將所有的網路共享資源和網路管理做集中式整合性的管理，而使用 Active Directory 目錄服務來管理網路，可簡化管理的工作、提高網路的安全性等。在沒有使用 Active Directory 目錄服務做管理時，往往由於可能公司中採用分散式資料的管理，會造成管理者的負擔以及公司在人事成本上的增加，如今採用Active Directory目錄服務將簡化管理，提高了管理正確性。

1.2.2 Active Directory 命名規則

Distinguished Name

每一個在 Active Directory 中的物件都擁有一個 Distinguished Name，而且 Distinguished Name 必須是唯一的。舉例來說，有一個在網域CKLAB.COM的Bill使用者，其標準的識別名稱表示法如下：

/DC=COM/DC=CKLAB/CN=USERS/CN=BILL

Relative Distinguished Name

爲Distinguished Name的一部份，Relative Distinguished Name在相同組織單位(OU)內是唯一性的。舉前例來說，使用者Bill的Relative Distinguished Name爲Bill，而在Bill所在的組織單位內不可能再產生相同的Relative Distinguished Name，但是在不同的組織單位中可建立相同的Relative Distinguished Name。

User Principle Name

爲使用者名稱和網域名稱所組成。舉例來說，在CKLAB.COM網域中的使用者Bill的User Principle Name的表示法爲：Bill@CKLAB.COM

Globally Unique Identifier

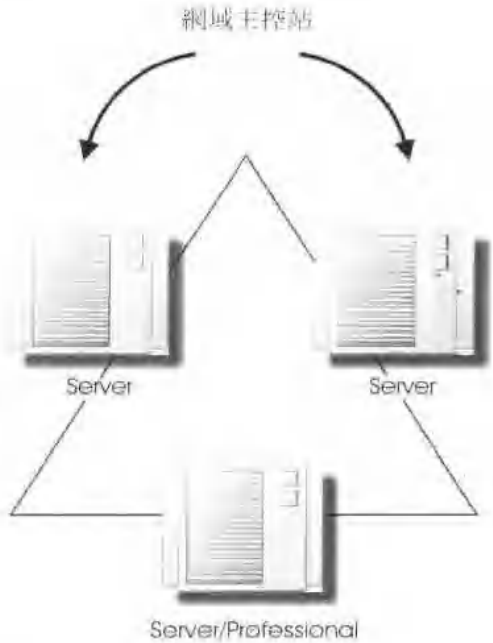
(GUID，Globally Unique Identifier)爲128Bit所組成的。在Active Directory每個物件都擁有一組唯一的GUID，假設您將一物件更改其名稱但是它的GUID還是不改變，而且相同名稱的物件其GUID也不同。

1.2.3 Active Directory的邏輯結構

在Active Directory的邏輯架構中包含了網域(Domain)、組織單位(Organizational Unit)、樹(Tree)和樹系(Forest)。

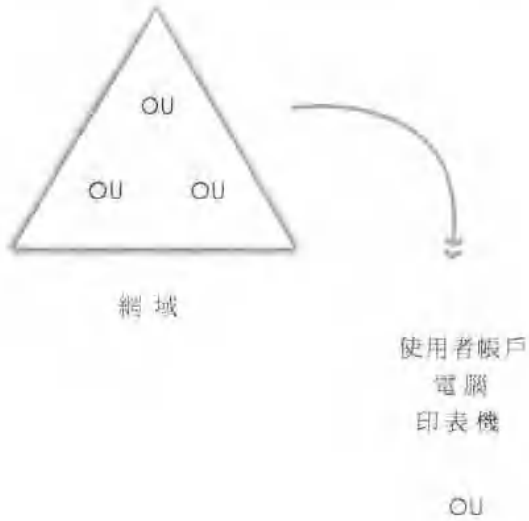
網域

網域(Domain)爲 Active Directory 架構中最核心的單位，在網域中所有的網域控制站，皆爲相互之關係，各網域中的網域控制站能接收到在 Active Directory 中資料的更新變化，並且複製這些更新的資料到其他的網域控制站中，如下圖。



組織單位

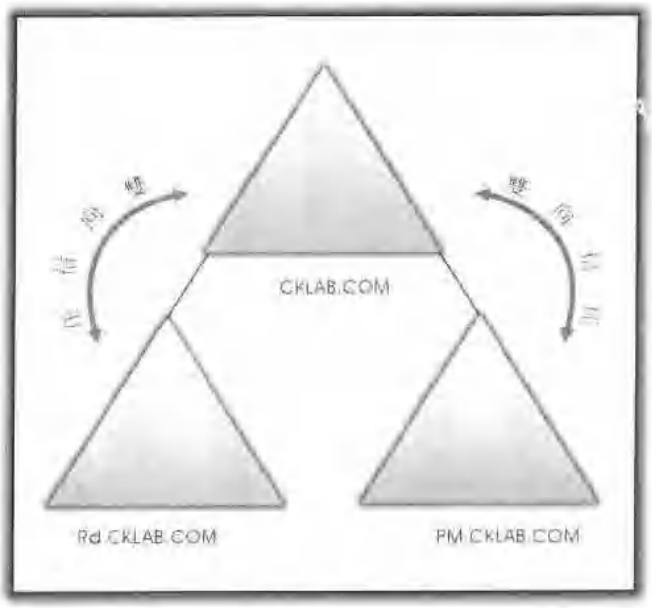
組織單位(OU，Organizational Unit)爲網域中存放物件的容器(Container)，所能存放的物件包含了使用者帳戶、群組、電腦和印表機等，如下圖。



樹

在Windows 2000的樹狀架構網域中，如爲連續命名空間的樹狀網域，則該樹狀架構網域可稱爲樹(Tree)。例如：一樹狀架構網域中的根網域(Root Domain)爲CKLAB.COM，子網域分別爲RD.CKLAB.COM和PM.CKLAB.COM，則這三個網域則爲一個樹。在樹中的網域皆爲雙向信任(Two-Way Transitive Trusts)方式，如下圖。

樹狀架構網域爲一連續命名空間的網域。

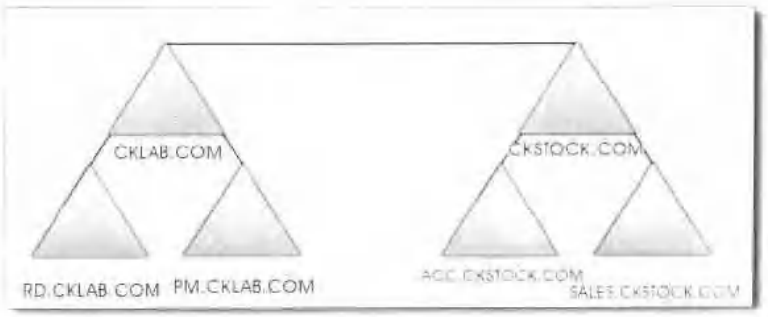


樹

樹系

樹系(Forest)爲兩個不連續的命名空間網域所組成，舉例來說：如有兩家公司進行合併，這兩家公司所屬的網域分別爲CKLAB.COM和CKSTOCK.COM，且這兩個網域皆爲不連續的命名空間網域，則這兩個樹可爲一個樹系。在樹系中的兩個網域的根網域爲雙向信任關係，但這兩個根網域所屬的子網域則爲單向信任關係(One-Way Transitive Trusts)，如下圖。

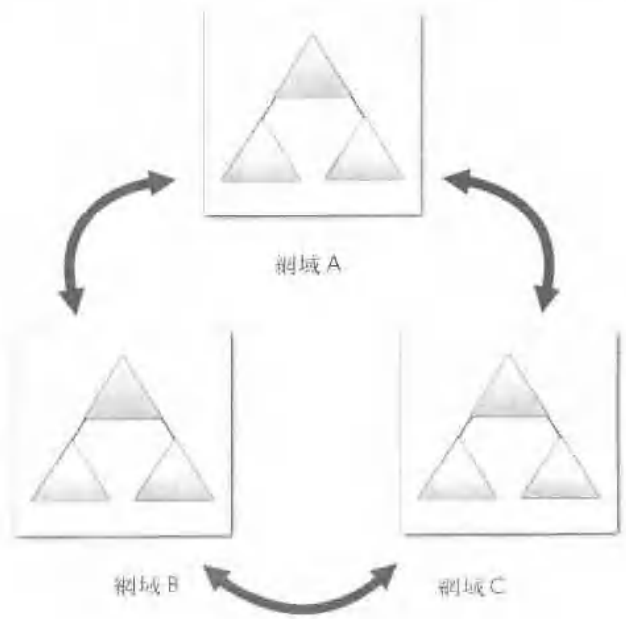
樹系爲兩個不連續命名空間所組成。



樹 系

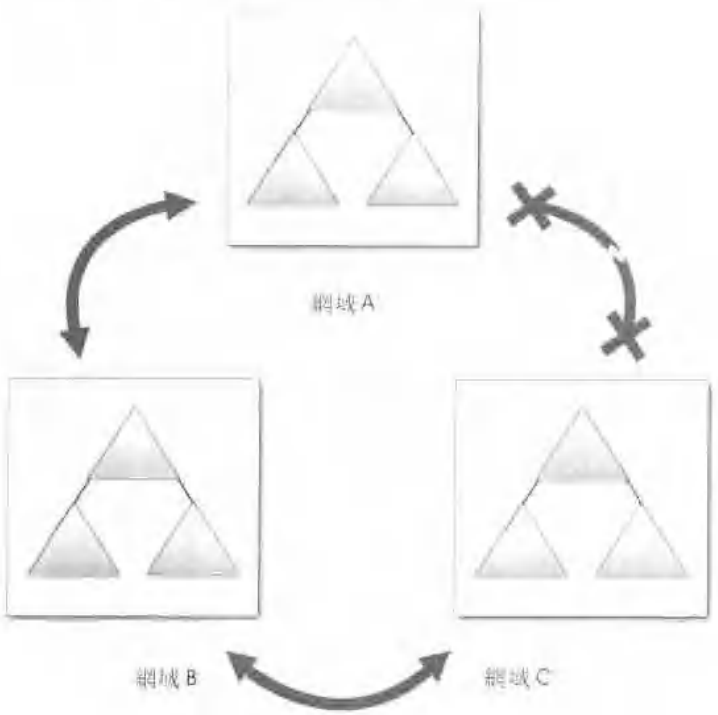
雙向信任關係

假設有三個網域分別爲網域 A 、網域 B 和網域 C ，如果網域 A 信任網域 B ，網域 B 信任網域 C ，則網域 A 自動信任網域 C ，如下圖。



單向信任關係

假設有三個網域分別爲網域 A 、網域 B 和網域 C ，如果網域 A 信任網域 B ，網域 B 信任網域 C ，則網域 A 並不自動信任網域 C ，如下圖。



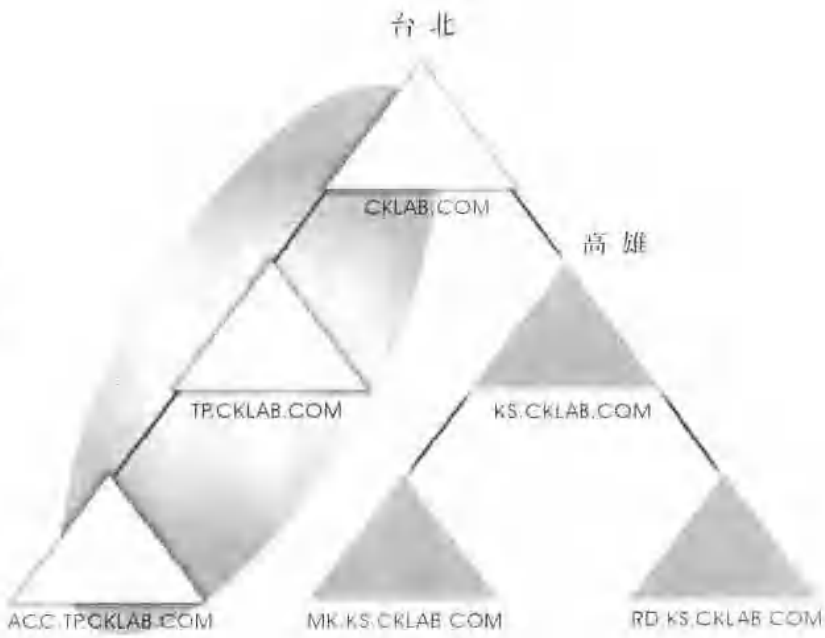
1.2.4 Active Directory的實體結構

在 Active Directory 的實體結構中，可將您的網路分爲不同的站台（Site）。

站台

站台(Site)爲一個以上的IP子網路(Internet Protocol Subnet)所組成，並且每個相互連接的IP子網路皆使用高速的專線互連。建立站台可以減少網路上的控制台複製所造成的大量網路流量負載。舉例來說：如有一個企業，分別在台北與高雄都有分公司，並且爲台北分公司爲該網域中的根網域，因爲網域控制站會每隔15分鐘到30分鐘進行各網路資料的複製，這樣下來會造成台北與高雄的網路流量因爲網域控制站的資料複製而效能降低，我們可以將其分割爲台北和高雄兩個站台，如下圖，等到離峰時間在進行站台的複製即可，此方式可提高網路的使用速度。

站台爲一個以上的IP子網域所組成，可減少於網路上複製所造成流量負載。



1.3 MMC Console

1.3.1 MMC簡介

MMC(Microsoft Management Console)爲Windows 2000系統管理的工具，他本身並不具管理功能，而是新增嵌入式單元到MMC中進行管理系統的工作，其能新增一個以上的嵌入式管理單元，您可以利用此工具集中管理特有的系統元件，如：Active Directory 使用者和電腦、Active Directory 站台及服務和磁碟管理等，可爲您省下不少時間。

說明

MMC 以副檔名.MSC 方式儲存於您的電腦上，爲了讓你更方便使用且更迅速的使用，建議可將其連結儲放於桌面上。

1.3.2 MMC 類型

在MMC的工作模式下又可分爲作者(Author)模式和使用者(User)模式，說明如下。

作者模式

在預設情況下，MMC 都會在作者模式(Author)下工作，在此模式下您可以使用MMC的完整功能包括了新增及移除嵌入式單元、建立新視窗等。

使用者模式

在使用者模式(User)下，使用者無法新增和移除任何嵌入式單元，及儲存，USER 模式包括三種不同類型的使用權限，您可參考下表。

使用者模式類型	說明
完整存取	對於使用者於 MMC 視窗中的嵌入式管理功能，擁有完整的存取權限，但無法新增或移除嵌入式管理單元。
限制存取，多重視窗	使用者僅能存取現存於 MMC 使窗中的嵌入式管理單元，使用者可建立新的視窗，但無法關閉現有視窗。
限制存取，單一視窗	使用者僅能存取現存於 MMC 使窗中的嵌入式管理單元，而且無法開啓新的視窗。

1.3.3 自訂 MMC

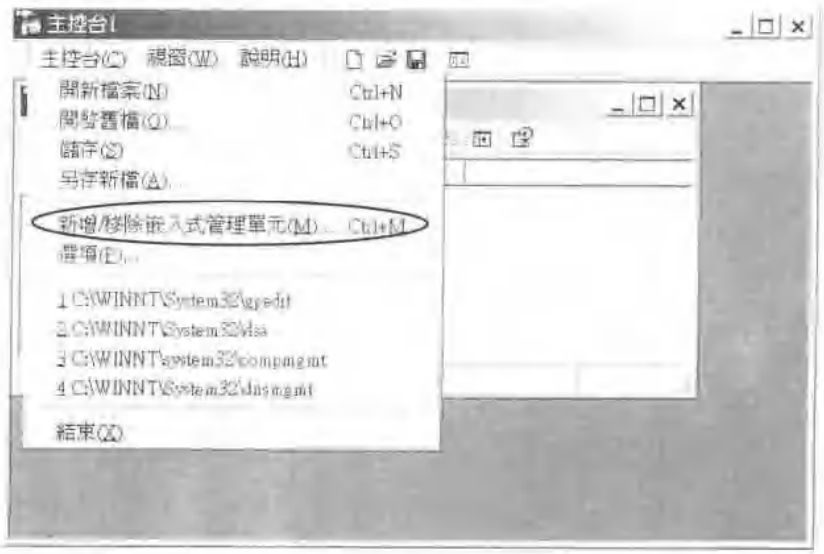
您可以自訂您常使用的系統管理元件於 MMC 中，您可參考下列步驟。

STEP 1

於[開始]/[執行]，輸入MMC後按**確定**執行。

STEP 2

進入「主控台」畫面，點選主控台，於下拉式選單點選新增/移除嵌入式管理單元。



STEP 3

進入「新增/移除嵌入式管理單元」畫面，點選新增後繼續。