

第 48 屆全國技能競賽

暨第 45 屆國際技能競賽國手選拔賽

資訊與網路技術

正式賽

競賽試題

選手姓名		崗位編號	
------	--	------	--

開始比賽前請勿翻閱試題。

請先在試題封面及評分表寫上姓名及崗位編號。

比賽後請將本試題及評分表留在崗位上，不得攜出賽場。

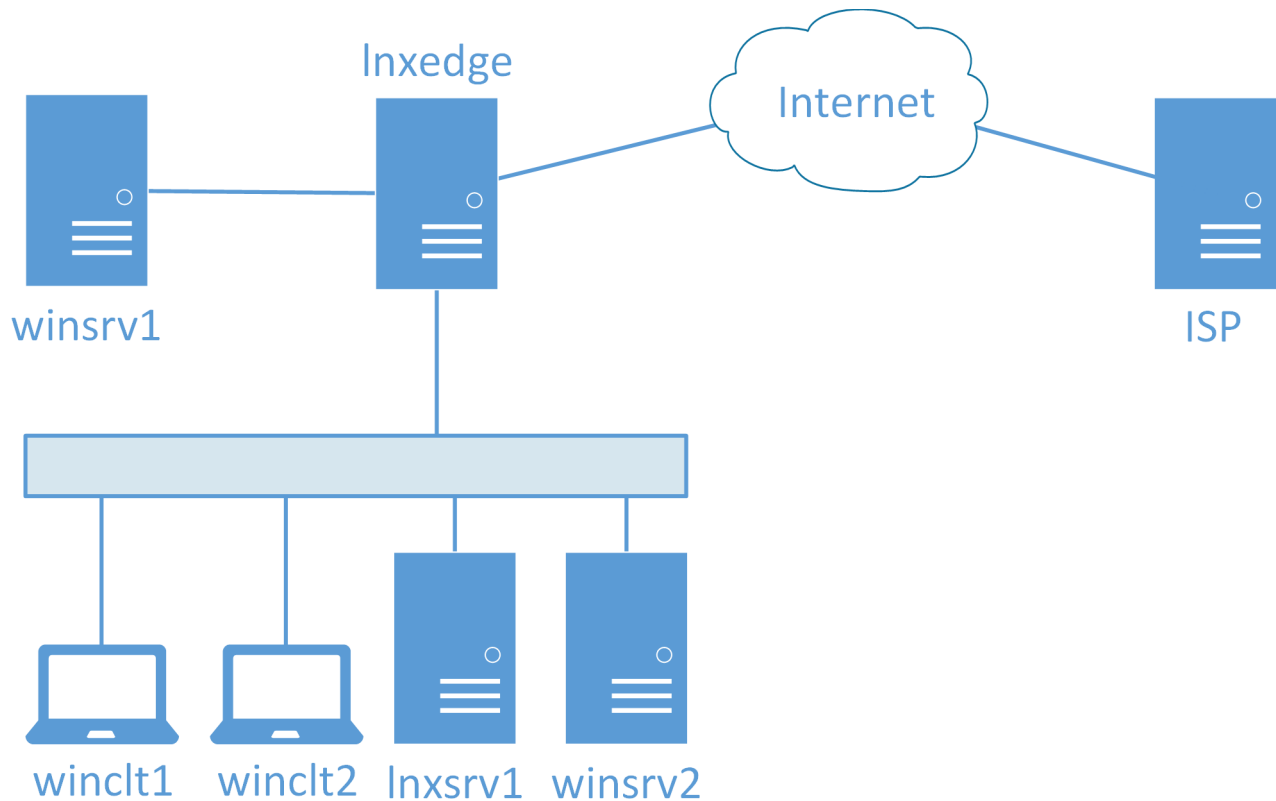






第 48 屆全國技能競賽暨第 45 屆國際技能競賽國手選拔賽

資訊與網路技術



Introduction & Description

- 本競賽為固定式起訖時間，請選手自行掌握工作流程，並依據試題敘述完成要求。
- 如在比賽過程中有任何疑問，或題意描述不清楚，請立即向裁判反應。
- 評分前將對所有虛擬系統進行重新啟動的動作，建議選手於競賽結束前預留些許時間，自行關閉虛擬系統。
- 評分時，將盡可能採用功能測試，項目之區隔以評分表所列為主，個別項目完全符合試題之敘述即得分，無部份給分。
- 工作項目中須設定密碼之處，若試題未明確指定，則一律使用 **Skills39**。
- 除了必須以檢視設定值的方式進行評分的項目外，所有面向用戶的服務一律由用戶端系統進行功能測試，否則該項目不予計分。



General Settings – 評分過程中，若發現不符合此設定時將於評分項扣分

- Host 主機不參與整個網路環境，請將其所有網卡 IPv4 及 IPv6 功能關閉
- 不指定 VM 安裝於哪台 HOST 主機，唯三台 PC 均須使用
- 在所有 VM 中安裝 VMware Tools
- 將所有 VM 名稱設定與 Hostname 相同
- 在所有 VM 中允許 ICMP 協定之流量
- 依照附錄 A 設定主機名稱、網卡名稱及相關 IP 位址
- 憑證請統一使用 CA 服務發放之憑證，評測時請勿出現憑證錯誤畫面

VMware Workstation Pro

- 所有 VM 須能支援超過 2TB 的開機磁區

ISP

- 於 PC 建立 Windows Server 2016 DataCenter 虛擬機 ISP
- 設定 DNS 服務，管理 org.tw 網域的資源紀錄 (Resource Records)
 - 將 wsc2019.org.tw 網域之查詢轉送給 winsrv1 (145.39.0.10)
※實際上查詢封包會經由 Inxedge 再流向 winsrv1
- 設定 DNS 服務，管理 isp.net 網域的資源紀錄 (Resource Records)
- 設定 Web 服務，提供 <https://www.isp.net> 瀏覽 ISP 網頁，請建立簡單的頁面內容以利測試
- 阻擋所有來源或目的為私有位址的流量 (根據 RFC1918)
- 扮演外部使用者進行相關測試



Inxedge

- 於 PC 建立 Debian 9 虛擬機 Inxedge
- 啟用 IP 封包轉送機制
- 為 DNS 相關查詢訊務設定封包轉譯功能，所有主機 (winsrv1 除外) 的 DNS 伺服器主機須設定為該網段的 Gateway (如：winclt1 的 DNS 伺服器主機為 192.168.10.1)
 - Inxedge 的 DNS 伺服器主機須設為 localhost
- 為來自內部網路及 DMZ 的流量設定 NAT，可經由 145.39.0.10 位址對外連線
- 安裝 Apache2，設定 Reverse Web Proxy 服務，以 <https://www.wsc2019.org.tw> 提供瀏覽網頁
 - 將 http 自動導向至 https
 - 將 Inxsrv1 及 winsrv2 的 https 站台設為後端主機，Inxsrv1 為主要主機，winsrv2 為備援主機，不進行負載平衡

winsrv1

- 於 PC 建立 Windows Server 2016 DataCenter 虛擬機 winsrv1
- 加入 wsc2019.org.tw 網域
- 設定 DNS 服務，作為 WSC2019 組織網路內唯一的 DNS 伺服器，管理 wsc2019.org.tw 網域的資源紀錄(Resource Records)
 - 依據題目需求建立相關正解與反解紀錄 (須包含主機紀錄)
 - 將其他請求轉送至 ISP
- 設定 VPN 服務，透過 vpn.wsc2019.org.tw (145.39.0.10) 連線，連入後僅能存取 Inxsrv1 主機
 - 使用 IKEv2 加密協定，並使用 Machine Certificate 驗證
 - 配發 10.1.1.150 ~ 10.1.1.180 範圍內的 IP 位址
 - 請避免造成非預期用戶也能存取 VPN 服務的重大安全疏失



winsrv2

- 於 PC 建立 Windows Server 2016 DataCenter 虛擬機 winsrv2
- 新增二個磁碟，將其設為 Raid 1 模式容量 10GB 提供於 F:\，且須支援自動完整性檢查及未來可擴增磁碟
- 設定 AD 網域服務，管理 wsc2019.org.tw 網域
- 將 AD 服務所需的 DNS 紀錄註冊於 winsrv1 下
- 建立 Root CA，根憑證命名為 WSC2019-ROOT，負責各項憑證簽發與管理
 - 對所有網域電腦自動發放憑證，憑證範本命名為 WSC2019-CMP
 - 各 Web 憑證須支援使用同金鑰展延，且個別核發包含相應 FQDN 資訊，憑證範本命名為 WSC2019-web
- 設定群組分享資料夾供網域使用者使用，依照附錄 C 進行分享設定
 - 各群組使用者僅能存取各自群組的分享資料夾
- 設定 Web 服務，以 https://winsrv2_web.wsc2019.org.tw 提供後端網頁
 - 為方便管理，請使用 Inxsrv1 之 web 分享資料夾同步網頁內容
 - 該站台僅供 Inxedge 之 Reverse Web Proxy 服務存取，其餘使用者禁止存取

Active Directory Tasks

- 依照附錄 B 建立 200 位使用者並進行相關設定
- 使用者開啟 Internet Explorer 後，可於分頁開啟 Edge 瀏覽器
- 為顧及 IT 人員方便性，IT 群組使用者於網域任意電腦登入後，檔案總管旁的瀏覽清單將完整跟隨使用者的瀏覽路徑
- 禁止 Sales 群組使用者於 winclt1 的檔案總管掛載磁碟機
- 使用者於登入後須自動掛載群組分享資料夾於 G:\
 - 掛載路徑為 \\wsc2019.org.tw\shares\
 - 不可於分享資料夾內出現其他群組的分享資料夾



Inxsrv1

- 於 PC 建立 Debian 9 虛擬機 Inxsrv1，並依照附錄 D 建立 60 位使用者
- 設定 DHCP 服務，配發 192.168.10.51 ~ 192.168.10.200 範圍內的 IP 位址
 - 使用系統預設日誌服務，將 DHCP 的日誌紀錄僅記錄於 /var/log/dhcp.log，並確保不會因主機斷電而使部分日誌遺失，且 mgts 群組使用者可以讀取
- 設定 SSH 服務，root 使用者須同時使用公開金鑰及密碼驗證後才能登入，其餘使用者使用密碼即可登入
 - 上述公開金鑰須使用 Edwards-Curve Digital Signature Algorithm，並將金鑰長度指定為 256bit
 - 預先於 winclt1 登入 it02 使用者產生金鑰供評分時連線使用
- 同一 IP 一分鐘內最多允許兩個 SSH 連線
- 設定 Samba 服務，分享以下資料夾
 - 分享名稱為 web，分享路徑為 /web，僅供 winsrv2 以 Administrator 存取，禁止副檔名為 EXE、DLL 及 TXT 相關檔案
 - 分享名稱為 public，分享路徑為 /public，匿名使用者可讀取該分享資料夾，一般使用者可存取該分享資料夾的任何檔案
 - 預先於 /public/readme.txt 建立一個檔案，內容為 " NSC48 "
- 設定 Web 服務，以 https://Inxsrv1_web.wsc2019.org.tw 提供後端網頁
 - 使用 Apache2 服務，並將 /web 設為網站根目錄
 - 請建立簡單的頁面內容以利測試
 - 該站台僅供 Inxedge 之 Reverse Web Proxy 服務存取，其餘使用者禁止存取



winclt1

- 於 PC 建立 Windows 10 Enterprise 虛擬機 winclt1
- 加入 wsc2019.org.tw 網域

winclt2

- 於 PC 建立 Windows 10 Enterprise 虛擬機 winclt2
- 請勿加入任何網域，此台主機將於評分時現場加入網域進行相關測試
- 如此台已加入或加過網域則 AD Task 將全部不進行評分



Appendix A - IP Address Assignment

VM Hostname	OS	Interface	IP Address	Default Gateway
ISP	WS 2016	Eth	145.39.0.1/24	N/A*
Inxedge	Debian 9	External	145.39.0.10/24	145.39.0.1
		DMZ	10.0.0.1/29	N/A*
		Internal	192.168.10.1/23	N/A*
winsrv1	WS 2016	Eth	10.0.0.2/29	10.0.0.1
winsrv2	WS 2016	Eth	192.168.10.10/23	192.168.10.1
lnxsrvt1	Debian 9	eth0	192.168.10.20/23	192.168.10.1
winclt1	Windows 10	Eth	Via DHCP	
winclt2	Windows 10	Eth	Via DHCP	

* 若預設閘道為 N/A，則請勿做任何設定

Appendix B - Domain Users

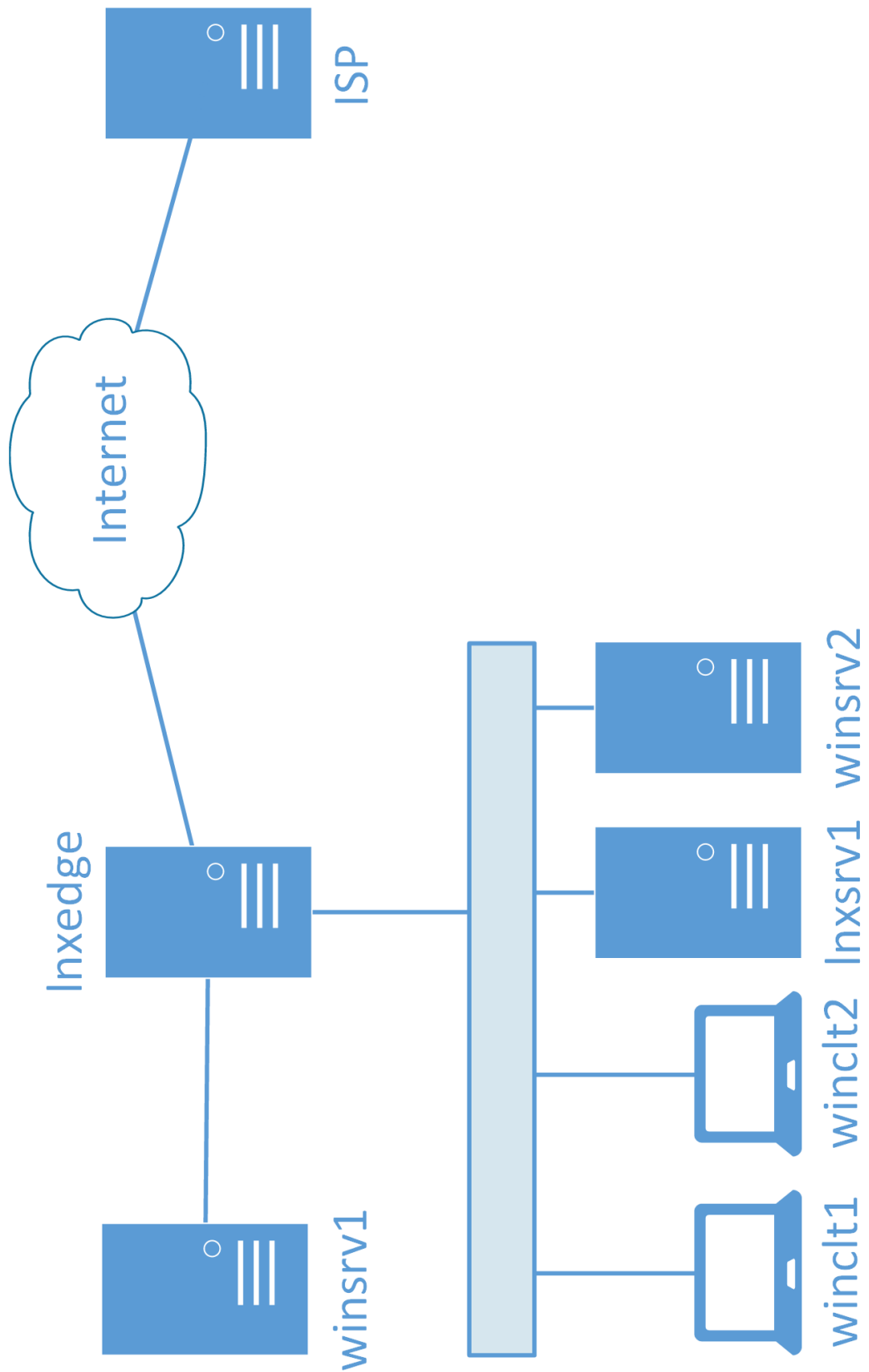
Username	Group	Password	Department
Administrator	Domain Admins	Skills39	Admins
IT01 ~ 50	Information Technology		IT
User001 ~ 020	KZUsers		HR
User021 ~ 080	Sales		Sales
User081 ~ 150	KZUsers		Marketing

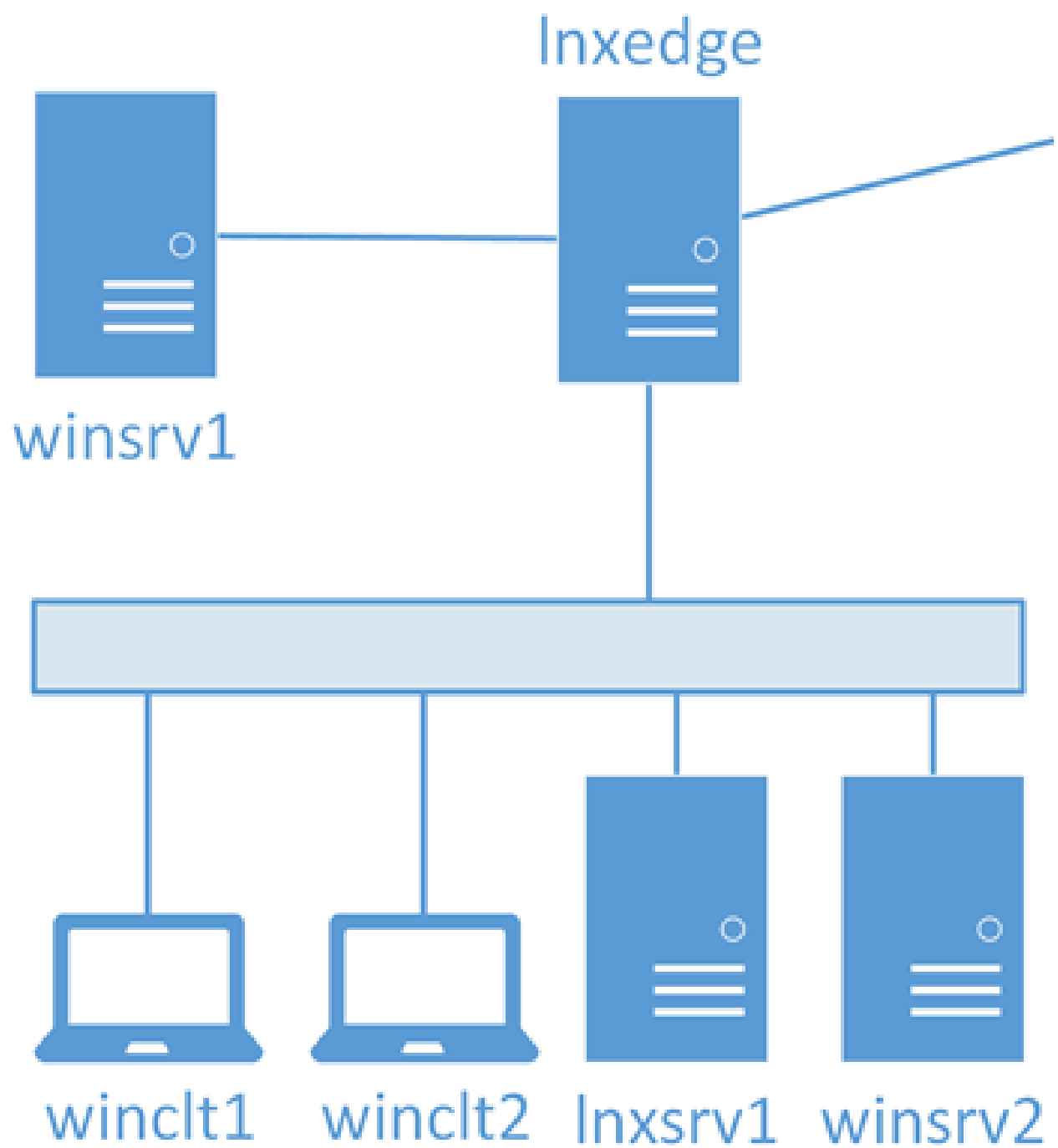
Appendix C – Share Folders

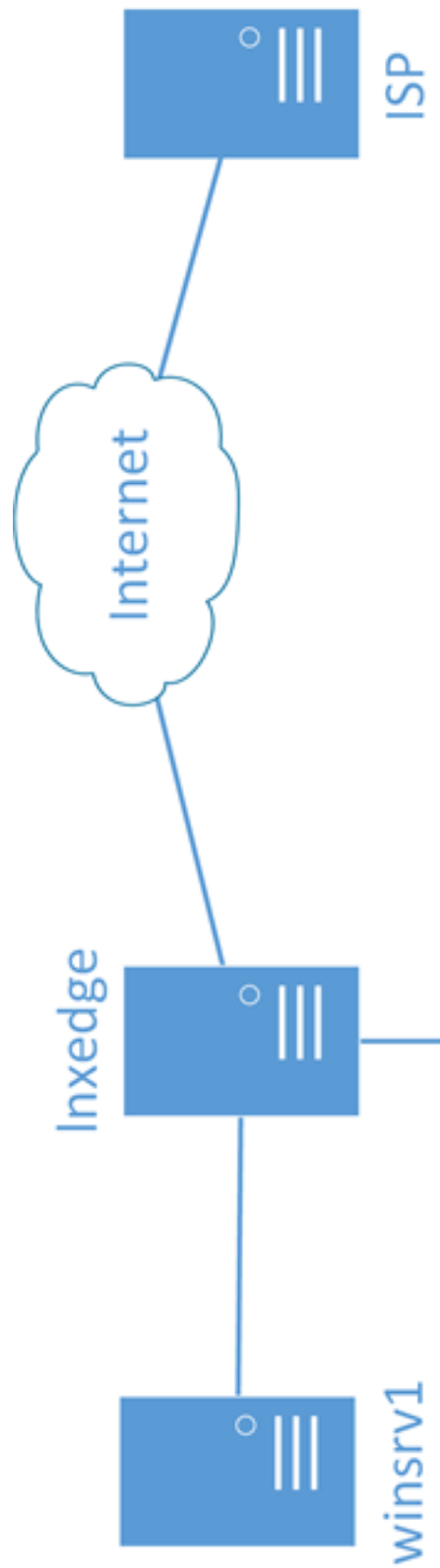
Share Name	Local Path	Group Permission
\\wsc2019.org.tw\shares\IT	F:\gpshares\InfoTech	Only IT Group
\\wsc2019.org.tw\shares\KZUsers	F:\gpshares\KZUsers	Only KZUsers Group
\\wsc2019.org.tw\shares\Sales	F:\gpshares\Sales	Only Sales Group

Appendix D – Linux Users

Username	Group	Password
root	root	Skills39
mgt01 ~ 60	mgts	



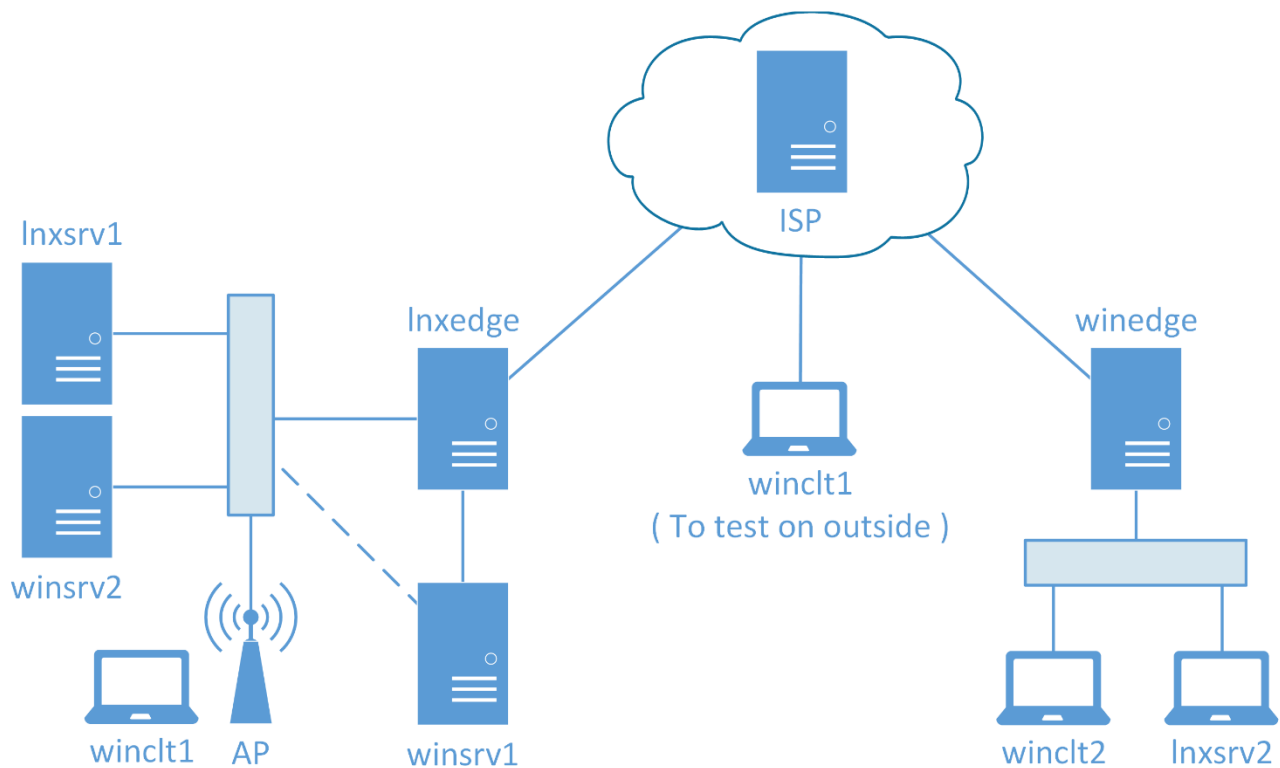






第 48 屆全國技能競賽暨第 45 屆國際技能競賽國手選拔賽

資訊與網路技術



Introduction & Description

- 工作項目中須設定密碼之處，若試題未明確指定，則一律使用 **Skills39**。
- 今日之工作項目將延續昨日之部分情境，部分資訊請選手自行參考昨日的試題
- 實際接線或網卡 IP 位址不符合題目要求，當天一律不進行評分

General Settings

- 依照附錄 A 設定主機名稱、網卡名稱(包含第二日的 VM)及相關 IP 位址

ISP

- 啟用 IP 封包轉送機制



Inxedge

- 與 winedge 建立 GRE 通道，使兩端點內部網路可互通
- 設定 Web 服務，提供 <http://wsc.wsc2019.org.tw> 瀏覽 wsc 網頁，請使用隨身碟中的網頁檔作為首頁
- 設定 iptables，外部網路不可在 DNS 查詢中得到 Private 網段的結果
- 組織計畫將 DMZ 與 Internal 兩個網段整併為一個網段，但 winsrv1 與 Inxedge 之間的接線尚不便更動，請思考並實作可達成此項要求的解決方案

winsrv1

- 新增 DNS 紀錄 (若前一日 DNS 設在 winsrv2 請將以下紀錄設在 winsrv2)
 - 將 remote.wsc2019.org.tw 對應至 145.39.0.11 位址
 - 將 wsc.wsc2019.org.tw 對應至 145.39.0.11 位址
- 設定 Direct Access 服務，讓使用者到 Internet 後仍能夠存取內部資源，客戶端將利用 remote.wsc2019.org.tw 來連接
 - 將 winclt1 客戶端加入 DA_Users 群組
 - 僅允許 DA_Users 群組連線
- 原本的 VPN 服務，仍應可正常運作，請於 winclt2 設定 VPN 連線設定

winsrv2

- 設定部門分享資料夾供網域使用者使用，依照附錄 B 進行分享設定
 - 使用者只能存取自己部門的部門分享資料夾。
※使用者更換部門後，應只能存取新部門的部門分享資料夾
 - 評分時，將新增一位新使用者進行相關測試
- 設定分享服務，作為 winclt1 的 BitLocker 修復金鑰儲存路徑
 - \\winsrv2\BitLocker -> C:\Backup\BitLocker



Inxsrv1

- 設定 Mail 服務，信箱地址為 <Username>@wsc2019.org.tw
 - 只提供 SMTPS 與 IMAPS 協定，憑證須使用 winsrv2 的 CA 簽署
 - 為 WSC2019 信件服務新增 MX 紀錄

AP

- 設定無線網路 SSID 為 WSC2019_XX，其中 XX 為選手崗位編號，並啟用 WPA2 with 802.1x，以 winsrv2 為 AAA 伺服器
 - 為考量無線網路安全性，請將 SSID 隱藏
 - 須使用憑證進行驗證，僅限 IT 群組連線
 - 網域內的電腦需自動取得無線網路設定檔，使用者不須手動進行任何設定及輸入驗證資訊，即可連上 WIFI

winclt1

- 使用內建 Mail Client 程式，登入 mgt02 使用者以供評分使用
 - 請預先由 mgt02 使用者寄一封測試信給 mgt01 使用者
 - 請勿刪除測試信
- 使用 BitLocker 為系統磁碟進行加密
 - 將修復金鑰存在 \\winsrv2\BitLocker\，檔名：BL_winclt1_key.txt
 - 請使用最適用於磁碟且最安全的加密演算法
- 安裝無線網卡並連線至 AP



winedge

- 於 PC 建立 Windows Server 2016 DataCenter 虛擬機 winedge
- 加入 wsc2019.org.tw 網域，並設為網域控制站
- 啟用 IP 封包轉送機制
- 為來自內部網路的流量設定 NAT，可經由 145.39.1.10 位址對外連線
- 設定 DHCP 服務，配發 192.168.20.51 ~ 192.168.20.200 範圍內的 IP 位址
 - 將 winclt2 配發到的 IP 固定為 192.168.20.100
- 與 Inxedge 建立 GRE 通道，使兩端點內部網路可互通

winclt2

- 將此台客戶端從左方拓譜移至右方拓譜

Inxsrv2

- 於 PC 建立 Debian 9 虛擬機 Inxsrv2
- 安裝 Gnome 圖形化系統
- 使用者 root 應可於圖形化系統登入
- 安裝圖形化 Mail Client 程式，並登入 mgt01 使用者以供評分使用
 - 請預先由 mgt01 使用者寄一封測試信給 mgt02 使用者
 - 請勿刪除測試信
- 為避免意外狀況發生，防止 root 使用者刪除系統重要資料(例如：rm -rf /)



Appendix A - IP Address Assignment

VM Hostname	OS	Interface	IP Address	Default Gateway
ISP	WS 2016	Eth1	145.39.0.1/24	N/A*
		Eth2	145.39.1.1/24	N/A*
Inxedge	Debian 9	External	145.39.0.10/24 145.39.0.11/24	145.39.0.1
		Internal	192.168.10.1/23	N/A*
winsrv1	WS 2016	Eth	192.168.10.40/23	192.168.10.1
winsrv2	WS 2016	Eth	192.168.10.10/23	192.168.10.1
Inxsrv1	Debian 9	eth0	192.168.10.20/23	192.168.10.1
AP	(AP)	Lan	192.168.10.30/23	192.168.10.1
winclt1	Windows 10	WIFI	Via DHCP	
winedge	WS 2016	Eth1	145.39.1.10/24	145.39.1.1
		Eth2	192.168.20.1/24	N/A*
Inxsrv2	Debian 9	eth0	192.168.20.10/24	192.168.20.1
winclt2	Windows 10	Eth	Via DHCP	

* 若預設閘道為 N/A，則請勿做任何設定

Appendix B – Share Folders

Share Name	Local Path	Department
\\wsc2019.org.tw\department\IT	C:\dept\IT	IT
\\wsc2019.org.tw\department\HR	C:\dept\HR	HR
\\wsc2019.org.tw\department\Sales	C:\dept\Sales	Sales
\\wsc2019.org.tw\department\Mkt	C:\dept\Marketing	Marketing

