N-Partner

如何設定 MS Exchange Server 郵件追蹤記錄

V014

2019/11/11



版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可,不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中, N-Partner Technologies Co. 保留不告知變動的權利。

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標,均屬其合法註冊公司所有。





| 前言2 |
|--|
| 1. NXLog |
| 1.1 NXLog 架構3 |
| 1.2 NXLog 安裝 4 |
| 1.3 NXLog 設定檔5 |
| 1.4 NXLog 啟動服務 8 |
| 2. Exchange 20079 |
| 2.1 使用 [Exchange 管理主控台] 設定 9 |
| 2.2 使用 [Exchange 管理命令介面] 設定 11 |
| 3. Exchange 201013 |
| 3.1 Exchange Message Tracking Log 13 |
| 3.1.1 Exchange Management Console 13 |
| 3.1.2 Exchange Management Shell 16 |
| 3.2 IIS log |
| 3.3 Event log |
| 3.3.1 組織單位(Organizational Unit) 33 |
| 3.3.2 群組原則(Group Policy Management) 36 |
| 4. Exchange 201341 |
| 4.1 Exchange Message Tracking Log 41 |
| 4.1.1 Exchange 系統管理中心(EAC) 41 |
| 4.1.2 Exchange Management Shell 44 |
| 4.2 IIS log |
| 4.3 Event log 52 |
| 4.3.1 組織單位(Organizational Unit) 52 |
| 4.3.2 群組原則(Group Policy Management) 55 |
| 5. Exchange 201662 |
| 5.1 Exchange Message Tracking Log 62 |
| 5.1.1 Exchange 系統管理中心(EAC)62 |
| 5.1.2 Exchange Management Shell 65 |
| 5.2 IIS log |
| 5.3 Event log 72 |
| 5.3.1 組織單位(Organizational Unit) 72 |
| 5.3.2 群組原則(Group Policy Management) 75 |
| 6. Exchange 201982 |
| 6.1 Exchange Message Tracking Log 82 |
| 6.1.1 Exchange 系統管理中心(EAC)82 |
| 🔊 N- Partner |

N-Partner Technologies Co

| 6.1.2 Exchange Management Shell 85 |
|--|
| 6.2 IIS log |
| 6.3 Event log 93 |
| 6.3.1 組織單位(Organizational Unit)93 |
| 6.3.2 群組原則(Group Policy Management)96 |
| |
| 7. N-Reporter |
| 7. N-Reporter1037. 1 Exchange Message Tracking log103 |
| 7. N-Reporter 103 7. 1 Exchange Message Tracking log 103 7. 2 Exchange Event log 105 |
| 7. N-Reporter 103 7. 1 Exchange Message Tracking log 103 7. 2 Exchange Event log 105 7. 3 Exchange IIS log 107 |



前言

本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLog 方式設定 MS Exchange Server 郵件追蹤記錄。NXLog 工具將 MS Exchange Server 郵件追蹤記錄轉成 Syslog,再轉發到 N-Reporter 做正規 化、稽核與分析。

此文件適用於 MS Exchange Server 2007 / 2010 / 2013 / 2016 / 2019 版本。

註: Microsoft Exchange Server 預設啟用郵件追蹤。

郵件追蹤記錄

<u>https://docs.microsoft.com/zh-tw/exchange/mail-flow/transport-logs/message-tracking?view=exchserver-2019</u> 信箱審核記錄

https://docs.microsoft.com/zh-tw/exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging?view=exchserver-2019

稽核原則建議

https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-best-practices/audit-policyrecommendations





1. NXLog

1.1 NXLog 架構

NXLog 的 plugin 架構允許任何類型的輸入讀取資料、解析和轉換訊息的格式,然後將其發送到任何類型的輸出。可以同時使用不同的輸入、處理和輸出模組來滿足事件記錄。

https://nxlog.co/documentation/nxlog-user-guide#modules-im







1.2 NXLog 安裝

(1) 下載 NXLog

前往網址 https://nxlog.co/products/nxlog-community-edition/download

下載網址最新版 nxlog-ce-x.x.xxxx.msi, 範例: nxlog-ce-2.10.2150.msi。



(2) 安裝 NXLog

點擊 [nxlog-ce-2.10.2150.msi] -> 按 [Install] 到 [Finish] 。

| MXLog-CE Setup — | | × |
|--|-----|------|
| Ready to install NXLog-CE | | |
| Click Install to begin the installation. Click Back to review or change any of you installation settings. Click Cancel to exit the wizard. | r | |
| | | |
| | | |
| Back Install | Car | ncel |

(3) 下載並覆蓋 NXLog 設定檔

下載連結 <u>https://www.npartnertech.com/download/tech/nxlog_Exchange.conf</u> ->

覆蓋 NXLog 設定檔 Copy-Item nxlog_Exchange.conf 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

| ≥ 系統管理員: Windows PowerShell | _ | | × |
|---|-------|----------|---|
| PS C:\Users\Administrator\Downloads> Copy-Item nxlog_Exchange.conf 'C:\Program Files (x86)\nxlog\con PS C:\Users\Administrator\Downloads> _ | \nx1c | og.conf' | 0 |





1.3 NXLog 設定檔

| ## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start. | | | | |
|---|--|--|--|--|
| define ROOT C:\Program Files (x86)\nxlog | | | | |
| define NCloud 192.168.3.51 | | | | |
| define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking | | | | |
| define IISLog C:\inetpub\logs\LogFiles | | | | |
| define CERTDIR %ROOT%\cert | | | | |
| define CONFDIR %ROOT%\conf | | | | |
| define LOGDIR %ROOT%\data | | | | |
| define LOGFILE %LOGDIR%\nxlog.log | | | | |
| LogFile %LOGFILE% | | | | |
| | | | | |
| Moduledir %ROOT%\modules | | | | |
| CacheDir %ROOT%\data | | | | |
| Pidfile %ROOT%\data\nxlog.pid | | | | |
| SpoolDir %ROOT%\data | | | | |
| | | | | |
| ## Load the modules needed by the outputs | | | | |
| <extension syslog=""></extension> | | | | |
| Module xm_syslog | | | | |
| | | | | |
| | | | | |
| ## For Exchange Message Tracking log file use the following: | | | | |
| <input in_mail=""/> | | | | |
| Module im_file | | | | |
| File '%MailLog%\MSGTRK*.LOG' | | | | |
| ReadFromLast TRUE | | | | |
| SavePos TRUE | | | | |
| | | | | |
| | | | | |
| <output out_mail=""></output> | | | | |
| Module om_udp | | | | |
| Host %NCloud% | | | | |
| Port 514 | | | | |
| Exec \$SyslogFacilityValue = 2; | | | | |



| Exec | \$SourceName = 'Exchange'; | | | | | |
|---|---|--|--|--|--|--|
| Exec | to_syslog_bsd(); | | | | | |
| | | | | | | |
| | | | | | | |
| <route ma<="" td=""><td>ail></td></route> | ail> | | | | | |
| Path | in_mail => out_mail | | | | | |
| | | | | | | |
| | | | | | | |
| ## For Wir | ndows Event log use the following: | | | | | |
| <input in_<="" td=""/> <td>eventlog></td> | eventlog> | | | | | |
| Module | im_msvistalog | | | | | |
| ReadFro | omLast TRUE | | | | | |
| SavePo | s TRUE | | | | | |
| Query | <querylist> \</querylist> | | | | | |
| | <query id="0"> \</query> | | | | | |
| | <select path="Security">*[System[(EventID=4624 or EventID=4625 or</select> | | | | | |
| EventID=4 | 1648)]] \ | | | | | |
| | <select path="Security">*[System[(EventID=4634 or EventID=4647)]]</select> \ | | | | | |
| | \ | | | | | |
| <td>ist></td> | ist> | | | | | |
| | | | | | | |
| | | | | | | |
| <output o<="" td=""><td>ut_eventlog></td></output> | ut_eventlog> | | | | | |
| N | lodule om_udp | | | | | |
| F | lost %NCloud% | | | | | |
| P | Port 514 | | | | | |
| E | xec \$SyslogFacilityValue = 20; | | | | | |
| E | Exec \$Message = string(\$SourceName) + ": " + string(\$EventID) + ": " + \$Message; | | | | | |
| E | Exec if (\$EventType == 'ERROR' or \$EventType == 'AUDIT_FAILURE') { \$SyslogSeverityValue = 3; } \ | | | | | |
| | else if (\$EventType == 'WARNING') { \$SyslogSeverityValue = 4; } \ | | | | | |
| | else if (\$EventType == 'INFO' or \$EventType == 'AUDIT_SUCCESS') { \$SyslogSeverityValue = 5; } | | | | | |
| E | xec to_syslog_bsd(); | | | | | |
| | | | | | | |
| | | | | | | |
| <route ev<="" td=""><td>/entlog></td></route> | /entlog> | | | | | |

Path in_eventlog => out_eventlog



| ## For Microsof | ft IIS(Internet Information Server) log file use the following: | | | | |
|--|---|--|--|--|--|
| <input in_iis=""/> | | | | | |
| Module | im_file | | | | |
| File | '%IISLog%\u_ex*.log' | | | | |
| ReadFromL | ast TRUE | | | | |
| Recursive | TRUE | | | | |
| SavePos | TRUE | | | | |
| | | | | | |
| | | | | | |
| <output out_iis<="" td=""><td>></td></output> | > | | | | |
| Module om | n_udp | | | | |
| Host | %NCloud% | | | | |
| Port | 514 | | | | |
| Exec | \$SyslogFacilityValue = 22; | | | | |
| Exec | <pre>\$raw_event = "IIS [info]: " + \$raw_event ;</pre> | | | | |
| Exec | ec to_syslog_bsd(); | | | | |
| | | | | | |
| | | | | | |
| <route iis=""></route> | | | | | |
| Path | in_iis => out_iis | | | | |
| | | | | | |
| | | | | | |

藍色文字部位請輸入 N-Reporter 系統 IP address:

define NCloud 192.168.3.51

藍色文字部位請輸入郵件追蹤記錄資料夾

define Mail_Log C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking

藍色文字部位請輸入 IIS log 資料夾

define IIS_Log C:\inetpub\logs\LogFiles



1.4 NXLog 啟動服務

開啟 [Windows PowerShell] -> 輸入 Start-Service nxlog 啟動 nxlog 服務和 Get-Service nxlog 查看 nxlog

服務狀態 -> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log' 確認沒有錯誤訊息。

| 🚬 Admi | nistrator: Wind | lows PowerShell - | × |
|----------------------------------|---|---|---|
| PS C:\Us PS C:\Us | ers\Administ ers\Administ | trator\Downloads> Start-Service nxlog trator\Downloads> <mark>Get-Service</mark> nxlog | ^ |
| Status | Name | DisplayName | |
| Running | nxlog | nxlog | |
| PS C:\Us 2019-02- PS C:\Us | ers\Adminis 12 17:09:34 ers\Adminis | trator\Downloads> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlo INFO nxlog-ce-2.10.2150 started trator\Downloads> _ | ~ |





2. Exchange 2007

可選擇 [Exchange 管理主控台] 或 [Exchange 管理命令介面] 設定郵件追蹤記錄。

2.1 使用 [Exchange 管理主控台] 設定

- (1) 以系統管理者 Administrator 登入 Exchange Server
- (2) 滑鼠左點[開始] -> [所有程式] -> [Microsoft Exchange Server 2007] -> [Exchange 管理主控台]

| Administrator | |
|--------------------------|---|
| 🧊 管理您的伺服器 | 受到 我的電腦 |
| □□□ 命令提示字元 | |
| 妏 Windows 檔案 🥶 | Windows Catalog Windows Update |
| 🚺 記事本 🛛 💽 | Microsoft Exchange Server 2007) 家 Exchange Server 説明 |
| 捷徑 - SyslogAgentCon 🛅 | R和管理工具 附屬應用 式 |
| 🔀 Exchange 管理: | 啓動 Internet Explorer (32-bit) |
| 🚰 Exchange 管理 á 🔗 | Outlook Express |
| Notepad++ | 遠端協助 WinRAR ▶ |
| Dintemer Explored | InterSect Alliance |
| 所有程式 🕑 🕨 🚠 | Notepad++ |
| | 💋 登出し) 🔟 闢機(11) |
| | 🥑 管理您的伺服器 |



server role]

| 器Exchange 管理主控台 | | | | | | <u>- 🗆 ×</u> |
|---|------------------------|-------------|--------------------------|--------------|-----------------------------------|--------------|
| 檔案(乎)執行(点)檢視(平) 説明(出) | | | | | | |
| Microsoft Exchange | E Lang ng og des | | | 1 1/10/4- | 動作 | |
| | ▶ 1回版番組18 ▼建立飾選器(R) | | | - 17/T干 - | 伺服器組態 | |
| 信相 | | 备色 | 版本號碼 | | 📔 修改組態網域控制站(C) | |
| □ □ □ 用戶端存取 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ | NPAR TNER-012A02 | 集線傳輸,用戶端存取, | Version 8.3 (Build 83.6) | | 📑 匯出清單(L) | |
| ■ 整合通訊 | | | | | 檢視 | • |
| 二 一 工具箱 | | | | | ◎ 重新整理 | |
| | | | | | 23 說明 | |
| | | | | | APAY THER-UIZAUZ | • |
| | | | | | ■ 管理 Client Access server role(C) | |
| | | | | | ≥ E Hub Transport server role(T) | |
| | | | | | 📔 管理診斷記錄內容(0) | |
| | | | | | □ 輸入產品金鑰(K): | |
| | | | | | ✓ 內容(R) | |
| | | | | | 😢 說明 | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | J | | | | | |
| | | | | | | |

(4) 滑鼠左點 [內容]。勾選 [啟用郵件追蹤記錄], 左點 [瀏覽], 設定郵件追蹤記錄檔路徑, 預設 C:\Program

Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking。左點 [確定],完成配置。

| ■ 集線傳輸 学建立篩選器 (R) 名額 ▲ ■ NPARTNER-0: ■ NPARTNER-0: ■ NPARTNER 接收連接器 名額 ▲ ■ Client NPART ■ Default NPAR | App (9 年) NPARTNER-012A02 内容 文術選器 (2) 一般 系統設定 外部 DNS 查閱 內部 DNS 查閱 限制 記錄檔設定 呼作追蹤記錄瘤 「「 啓用郵件追蹤記錄(2) 郵件追蹤記錄(2) 郵件追蹤記錄(2) 郵件追蹤記錄(2) 郵件追蹤記錄(2) 郵件追蹤記錄(2) 郵件追蹤記錄(2) 郵件追蹤記錄(2) 電線記錄 電線記錄 「 密用郵件追蹤記錄(2) 『 密用郵件追蹤記錄(2) 『 密用郵件追蹤記錄(2) 『 密用郵件追蹤記錄(2) 『 密用郵件追蹤記錄(2) 『 密見論(記録) 『 密見論(記述ののの(1) 日本の(2) 『 密見論(記録) 『 密見論(記述ののの(1) 日本の(2) 『 密見論(記述ののの(1) 日本の(2) 『 密見論(2) 『 密目』(2) 『 密見論(2) 『 密目』(2) 『 密目』(2) | | ✓ 勿件 | 動作 集線傳輸 通 距出清單(L) 校規 ② 重新整理 ③ 前新整理 ③ 前明 PARTNER-012A02 管理 Mailbox server role(M) 管理 Client Access server role(C) 管理 Client Access server role(C) 管理診斷記錄內容(0) ● 輸入產品金鑰(K): ●新增接收連接器(N) ● 內容(R) | × |
|---|---|--|------|--|---|
| ○ NPARTNER 接收連接器 名稱 ▲ ○ Client NPART ○ Default NPAR | C:Program FileslMioncooft/Exohapte Serverl/TransportRoles/Logs 通訊協定記錄檔 傳法連接器通訊協定記錄檔路描記D: C:Program FileslMioncooft/Exohagte Serverl/TransportRoles/Logs/Pro 接收連接器通訊協定記錄檔路是(D): C:Program FileslMioncooft/Exohagte Serverl/TransportRoles/Logs/Pro C:Program FileslMioncooft/Exohagte Serverl/TransportRoles/Logs/Pro 確定 取消 套用(<u>A</u>) | 瀏覽(W) 瀏覽(W) 瀏覽(S)]]]]]]]]] | | 管理 Client Access server role(C) 管理診斷記錄內容(0) 輸入產品金鑰(K): 新增接收連接器(N) (V) 內容(R) Client NPARTNER-012&02 (④ 停用(D) 移除(Y) (○ 內容(R) (※) 說明 | |
| | | | | | |





2.2 使用 [Exchange 管理命令介面] 設定

- (1) 以系統管理者 Administrator 登入 Exchange Server
- (2) 滑鼠左點 [開始] -> [所有程式] -> [Microsoft Exchange Server 2007] -> [Exchange 管理命令介面]







Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled \$True -MessageTrackingLogPath

<LocalFilePath>

或

Set-MailboxServer <ServerIdentity> -MessageTrackingLogEnabled \$True -MessageTrackingLogPath

<LocalFilePath>

<ServerIdentity> 為 Exchange Server 的電腦名稱, <LocalFilePath> 為郵件追蹤記錄的路徑,預設為

C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking

本例輸入:

Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled \$True -MessageTrackingLogPath

"C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"

🎇 Machine: npartner-012a02 | Scope: npexchange.local

_ 8 ×

_ 8 ×

[PS] C:\>Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled \$True -M▲ essageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\TransportRoles \Logs\MessageTracking"

[PS] C:∖>

(4) 檢查郵件追蹤記錄配置。命令列輸入:

Get-TransportServer npartner-012a02 | Select-Object *Track*

🎇 Machine: npartner-012a02 | Scope: npexchange.local

| [PS] C:\>Get-TransportServer npartner-Ø | 12a02 Select-Object *Track* 🔺 🔺 |
|---|--|
| | |
| MessageTrackingLogEnabled | : True |
| MessageTrackingLogMaxAge | : 30.00:00:00 |
| MessageTrackingLogMaxDirectorySize | : 250MB |
| MessageTrackingLogMaxFileSize | : 10MB |
| MessageTrackingLogPath | : C:\Program Files\Microsoft\Exchange S erver\TransportRoles\Logs\MessageTrac king |
| MessageTrackingLogSubjectLoggingEnabled | : True |



3. Exchange 2010

可選擇 [Exchange Management Console] 或 [Exchange Management Shell] 設定郵件追蹤記錄。

3.1 Exchange Message Tracking Log

修改 nxlog.conf

●¶_

註: 參考 1.3 NXLog 設定檔

藍色文字部位請輸入郵件追蹤記錄資料夾

define Mail_Log C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking

3.1.1 Exchange Management Console

- (1) 以系統管理者 Administrator 登入 Exchange Server
- (2) 滑鼠左點 [開始] -> [所有程式] -> [Microsoft Exchange Server 2010] -> [Exchange Management Console]



Copyright to All rights are reserved by N-Partner Technologies Co

(3) 滑鼠左點 [Microsoft Exchange 內部部屬] -> [伺服器組態] -> [集線傳輸] 滑鼠右點 Exchange Server · 本例為

MAIL,左點 [內容]。

| 😣 Exchange 管理主控台 | | | | |
|---|-----------------------|--------------------|--------------------|------------------|
| 檔案(F) 執行(A) 檢視(V) 說明(H) | | | | |
| 🗇 🄿 🗾 🖬 🔢 🗊 | | | | |
| 88 Microsoft Exchange | 🌬 集線傳輸 | | 1 個物件 | 動作 |
| □ Microsoft Exchange 內部部署 (mail.exchang | ☆建立篩選(R) | | | <u>集線傳輸</u> ▲ |
| | | 备色 | 版本 | 🔜 匯出清單 |
| 1、1、箱 | MAIL | 集線傳輸,用戶端存取, | Version 14.3 (Buil | 檢視 ▶ |
| 1 集線傳輸 | | | | □ □ 重新整理 |
| | | | | |
| | | | | |
| | | | | WATT |
| | | | | |
| | | | | |
| | | | | |
| | | | 2 個物件 | |
| | 接收建接器 | 1 015 215 | 1 | |
| | 名偶 へ 達 Client MAIL | <u> 秋態</u> 已啟用 | | |
| | Default MAIL | 已啟用 | | V 1345 |
| | | | I | Client MAIL |
| | | | I | ₩ 17/Π ₩ 40Re |
| | | | I | |
| | | | I | |
| | | | I | 👔 說明 |
| | | | I | |
| | | | I | |
| | | | I | |
| | | | I | |
| | | | I | |
| | | | | |
| | | | | |
| | <u>p</u> | | | 1 |





(4) 滑鼠左點 [記錄檔設定]。勾選 [啟用郵件追蹤記錄檔],輸入 [訊息追蹤記錄檔路徑],預設為 C:\Program

Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking。左點 [確定],完成配置。

| MAIL 種屬性 🛛 🛛 🗙 🗙 |
|---|
| 一般 糸統設定 外部 DNS 查閱 內部 DNS 查閱 限制 記錄檔設定 |
| 郵件追蹤記錄檔 |
| ☑ 歇用郵件追蹤記錄檔(E) |
| 訊息追蹤記錄檔路徑(M): |
| C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Me: |
| 連線記錄檔 ———————————————————————————————————— |
| ☑ 取用連線記錄(N) |
| 連線記錄檔路徑(C): |
| C:\Program Files\Microsoft\Exc <mark>1</mark> ange Server\V14\TransportRoles\Logs\Cor |
| 通訊協定記錄 ———————————————————————————————————— |
| 傳送通訊協定記錄檔路徑(D): |
| C:\Program Files\Microsoft\Exct <mark>l</mark> ange Server\V14\TransportRoles\Logs\Protoc |
| 接收通訊協定記錄路徑(V): |
| C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Protoci |
| |
| 確定 取消 套用(A) 說明 |



3.1.2 Exchange Management Shell

Ō

- (1) 以系統管理者 Administrator 登入 Exchange Server。
- (2) 滑鼠左點 [開始] -> [所有程式] -> [Microsoft Exchange Server 2010] -> [Exchange Management Shell]



(3) 啟用郵件追蹤。命令列輸入:

Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled \$True -MessageTrackingLogPath

<LocalFilePath>

或

Set-MailboxServer <ServerIdentity> -MessageTrackingLogEnabled \$True -MessageTrackingLogPath

<LocalFilePath>

<ServerIdentity>為 Exchange Server 的電腦名稱, <LocalFilePath>為郵件追蹤記錄的路徑,預設為 C:\Program

Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking

本例輸入:

Set-TransportServer MAIL -MessageTrackingLogEnabled \$True -MessageTrackingLogPath "C:\Program

Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"

👺 禮器:mail.exchange.npartnertech.com

198] C:\Windows\system32>Set-TransportServer MAIL -MessageTrackingLogEnabled \$True -MessageTrackingLogPath "C:\Program F iles\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"_



_ 🗆 🗵



(4) 檢查郵件追蹤記錄配置。命令列輸入:

Get-TransportServer MAIL | Select-Object *Track*

| 🚱 謾器:mail.exchange.npartnertech.com | | |
|--|--|---|
| [PS] C:\Windows\system32>get-transports | erver MAIL select-object *track* | |
| MessageTrackingLogEnabled MessageTrackingLogMaxAge MessageTrackingLogMaxDirectorySize MessageTrackingLogMaxFileSize MessageTrackingLogPath | : True : 30.00:00:00 : 1000 MB (1,048,576,000 bytes) : 10 MB (10,485,760 bytes) : C:\Program Files\Microsoft\Exchange Server\U14\TransportRoles\Logs\MessageTr | a |
| MessageTrackingLogSubjectLoggingEnabled | : True | |





3.2 IIS log

(1) 安裝 IIS Advanced Logging

IIS Advanced Logging 提供豐富、彈性的資料集合和即時的記錄功能。記錄任何 HTTP 要求/回應標頭、IIS 伺服器 變數和用戶端欄位,以追蹤使用者參與的情況。

https://www.microsoft.com/zh-tw/download/details.aspx?id=7211

點擊 [AdvancedLogging_amd64_zh-TW.msi] -> 勾選 [我接受這份授權合約] -> 按 [安裝] 到 [完成]



(2) 開啟 [Internet Information Services (IIS) 管理員]







(3) 選擇 [IIS Server] -> 點選 [Logging(記錄)]





(4) 點選 [停用]





(5) 確認記錄已停用







(6) 點選 [Advanced Logging]







(7) 按下 [編輯記錄欄位]







(8) 按下 [新增欄位]

| 编輯記錄欄位 | | | | ? × |
|-------------------|---------------------|-------|---------|-----------------|
| 群組依據(G): 沒有分組 | ¥ | | | |
| 識別碼 | 來源名稱 | 來源類型 | 類別 | 標頭名稱 ▲ |
| Win32Status | Win32Status | 內建 | Default | sc-win32-status |
| W3WP-PrivateBytes | \Process(w3wp)\Priv | 效能計數器 | Default | W3WP-PrivateE |
| UserName | UserName | 要求標頭 | Default | cs-username |
| User Agent | User-Agent | 要求標頭 | Default | cs(User-Agent) |
| URI-Stem | URI-Stem | 內建 | Default | cs-uri-stem |
| URI-Querystring | URI-Querystring | 內建 | Default | cs-uri-query |
| Time-UTC | Time-UTC | 內建 | Default | time |
| Time-Local | Time-Local | 內建 | Default | time-local |
| Time Taken | Time-Taken | 內建 | Default | Time TakenMS |
| Substatus | Substatus | 內建 | Default | sc-substatus |
| Status | Status | 內建 | Default | sc-status |
| Site Name | SiteName | 內建 | Default | s-sitename |
| Server-IP | Server-IP | 內建 | Default | s-ip |
| Server Port | ServerPort | 內建 | Default | s-port 🗾 |
| | | | | • |
| 新增欄位(A) | 移除(R) | 1 | 編輯欄位(E) | |
| | | | 確定 | 取消 |

(9) 輸入欄位識別碼: X-Forwarded-For -> 選擇類別: [Default] -> 來源類型: [Request Header(要求標頭)] -> 輸入來源

名稱: X-Forwarded-For -> 按下 [確定]

| 新増記錄欄位 | ? × |
|-----------------|-------|
| 欄位識別碼(F): | |
| X-Forwarded-For | |
| 類別(C): | |
| Default | |
| | |
| 來源類型(T): | |
| 要求標頭 | |
| 來源名稱(N): | |
| X-Forwarded-For | |
| 效能計數器類型(7). | |
| 速度 | |
| | |
| | |
| 周示准限内容 | |
| | |
| | 確定 取消 |





(10) 點選 [啟用 Advanced Logging] 和 [啟用用戶端記錄]

| 🐂 Internet Information Services (IIS) 管理員 | | | | |
|---|---|--|--|--|
| | 🖸 🖬 🖬 🖉 🕶 | | | |
| 檔案(F) 檢視(V) 說明(H) | | | | |
| 建設給網頁 WIN2008 (WIN2008) 應用程式集區 使用這個功能可以建立並管理記錄定錄 (用以指定要記錄哪些伺服器端和印用戶端記錄描位), 以及設定其他記錄設定。 詳細依據: 沒有分組 名稱 已数用 SCOMPUTERNAME%S 已数用 WOME WIN2008 ● 查 ● WIN2018 ● ● 站台 ● 站台 ● 公 ● 公 ● 公 ● 公 ● ● | ● Advanced Logging 功能已停用。 動作 新增記錄定義 放用 Advanced Logging 助能已修用。 放用用戶端記錄 編輯記錄欄位 編輯記錄欄位 續輯記錄檔 ② 說明 線上說明 | | | |
| 設定: localhost'applicationHost.config | S.: | | | |





(11) 選擇 [%COMPUTERNAME%-Server] -> 點選 [停用記錄定義]

| Ng Internet Information Services (IIS) 管理員 | | | | |
|---|--|---|--|--|
| G S № WIN2008 | > | 🗾 🖬 🛛 🟠 I 🖉 🔹 | | |
| 檔案(F) 檢視(∀) 說明(H) | | | | |
| 建築 ● ● ● <t< td=""><td>Advanced Logging 使用這個功能可以建立並管理記錄定義(用以指定要記錄哪些伺服器端和用戶端記錄欄位),以及設定其他記錄設定。 詳組依據: 沒有分組 名稱 ▲ ● 日啟用 冬稻 ▲ ● 日啟用 冬〇の杯PUTERNAME%-Server ● 日啟用 ● 小路魚 ● 小路魚</td><td> 勤作 新増記錄定義 編輯記錄定義 移除記錄定義 停用記錄定義 複製記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 編輯記錄欄位 檢視記錄檔 說明 線上說明 </td></t<> | Advanced Logging 使用這個功能可以建立並管理記錄定義(用以指定要記錄哪些伺服器端和用戶端記錄欄位),以及設定其他記錄設定。 詳組依據: 沒有分組 名稱 ▲ ● 日啟用 冬稻 ▲ ● 日啟用 冬〇の杯PUTERNAME%-Server ● 日啟用 ● 小路魚 ● 小路魚 | 勤作 新増記錄定義 編輯記錄定義 移除記錄定義 停用記錄定義 複製記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 編輯記錄欄位 檢視記錄檔 說明 線上說明 | | |
| 設定: 'localhost' applicationHost.con | fig | S.: | | |

(11) 點選 [新增記錄定義]

| Nation Services (IIS) 管理員 | | | | |
|---|---|--|--|--|
| | 🖸 🖬 🖬 🖉 🕶 | | | |
| 檔案(F) 檢視(V) 說明(H) | | | | |
| 建始網頁 ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●● | 新增記錄定義 編輯記錄定義 ※ 移除記錄定義 啟用記錄定義 複製記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 編輯記錄欄位 續輯記錄目錄 檢視記錄檔 | | | |
| 設定: localhost' applicationHost.config | Sec. 1 | | | |





(12) 輸入基底檔案名稱: u_ex -> 勾選 [已啟用] -> 選擇排程 [每小時] -> 按下 [選取欄位]

| National Information Services (IIS) 管理員 | |
|---|--|
| | 🖸 🗠 🔄 I 🕑 🗝 |
| 檔案(F) 檢視(♡) 說明(H) | |
| Image: Control of the second sec | 動作 承用 取消 検視記録檔 返回 Advanced Logging 說明 涂上說明 |
| 就緒 | Sec. 1 |





(13) 勾選 [X-Forwarded-For]、[Win32Status(sc-win32-status)]、[UserName(cs-username)]、[User Agent(cs(User-Agent))]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Time-Local(time-local)]、[Time Taken(TimeTakenMS)]、[Substatus(sc-substatus)]、[Status(sc-status)]、[Site Name(s-sitename)]、[Server-IP(s-ip)]、[Server Port(s-port)]、[Server Name(s-computername)]、[Referer(cs(Referer))]、[Protocol Version(cs-version)]、[Method(cs-method)]、[Host(cs(Host))]、[Date-Local(date-local)]、[Cookie(cs(Cookie))]、[Client-IP (c-ip)]、[Byte Sent(sc-bytes)]、[Bytes Received(cs-bytes)] -> 按下 [確定]

| | 來源名稱 | 來源類型 | 類別 | 標頭名稱▲ |
|-------------------|----------------------|-----------|---------|-----------------|
| Default | 1 2000 H 101 | 1 ABBROAL | 10003 | DRAW H IN |
| X-Forwarded-For | X-Forwarded-For | 要求標頭 | Default | |
| ✓ Win32Status | Win32Status | 内建 | Default | sc-win32-status |
| W3WP-PrivateBytes | Process(w3wp)Priv | 效能計數器 | Default | W3WP-PrivateE |
| ✓ UserName | UserName | 要求標頭 | Default | cs-usemame |
| 🗸 User Agent | User-Agent | 要求標頭 | Default | cs(User-Agent) |
| ✓ URI-Stem | URI-Stem | 內建 | Default | cs-uri-stem |
| ✓ URI-Querystring | URI-Querystring | 內建 | Default | cs-uri-query |
| Time-UTC | Time-UTC | 內建 | Default | time |
| Time-Local | Time-Local | 內建 | Default | time-local |
| 🖌 Time Taken | Time-Taken | 內建 | Default | Time TakenMS |
| 🗸 Substatus | Substatus | 內建 | Default | sc-substatus |
| 🗸 Status | Status | 內建 | Default | sc-status |
| 🗸 Site Name | SiteName | 內建 | Default | s-sitename |
| ✓ Server-IP | Server-IP | 內建 | Default | s-ip |
| Server Port | ServerPort | 內建 | Default | s-port |
| 🗸 Server Name | ServerName | 內建 | Default | s-computername |
| RequestsPerSecond | \W3SVC_W3WP(_T | 效能計數器 | Default | RequestsPerSecc |
| Referer | Referer | 要求標頭 | Default | cs(Referer) |
| Proxy | Via | 要求標頭 | Default | s-proxy |
| Protocol Version | ProtocolVersion | 內建 | Default | cs-version |
| Protocol | Protocol | 內建 | Default | c-protocol |
| 🗸 Method | Method | 內建 | Default | cs-method |
| ✔ Host | Host | 要求標頭 | Default | cs(Host) |
| EndRequest-UTC | EndRequest-UTC | 棋組 | Default | EndRequest-UT |
| Date-UTC | Date-UTC | 內建 | Default | date |
| 🗸 Date-Local | Date-Local | 內建 | Default | date-local |
| CPU-Utilization | \Processor(_Total)\% | 效能計數器 | Default | CPU-Utilization |
| 🖌 Cookie | Cookie | 要求標頭 | Default | cs(Cookie) |
| ContentPath | ContentPath | 內建 | Default | s-contentpath |
| Client-IP | Client-IP | 內建 | Default | c-ip |
| 🖌 Bytes Sent | BytesSent | 棋組 | Default | sc-bytes |
| Bytes Received | BytesReceived | 棋組 | Default | cs-bytes |
| BeginRequest-UTC | BeginRequest-UTC | 棋組 | Default | BeginRequest-U |
| | | | | |





(14) 調整選取的欄位: [Data-Local(date-local)]、[Time-Local(time-local)]、[Site Name(s-sitename)]、[Server Name(s-computername)]、[Server-IP(s-ip)]、[Method(cs-method)]、[URI-Stem(cs-uri-stem)]、[URI-Querystring(cs-uri-query)]、[Server Port(s-port)]、[UserName(cs-username)]、[Client-IP(c-ip)]、[Protocol Version(cs-version)]、[User Agent(cs(User-Agent))]、[Cookie(cs(Cookie))]、[Referer(cs(Referer))]、[Host(cs(Host))]、[Status(sc-status)]、[Substatus(sc-substatus)]、[Win32Status(sc-win32-status)]、[Bytes Send(sc-bytes)]、[Bytes Received(cs-bytes)]、[Time Taken(TimeTakenMS)]、[X-Forwarded-For] -> 按 [上移] 或 [下移] -> 按下 [套用]

| °崖Internet Information Services (IIS) 管理員 | |
|--|---|
| (3) ○ ♥ WIN2008 > | 🔛 🖂 🚹 I 🕑 🗝 |
| 檔案(F) 檢視(V) 說明(H) | |
| 田本(下) 接現(下) 説明(日) 日本(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日本)(日 | DIYHE ▼ 変用 ★ 取消 検視記録欄 ● 返回 Advanced Logging ② 説明 線上說明 |
| 設定: localhost' applicationHost.config | € <u>1</u> .: |





(15) 點選 [編輯記錄目錄]

| 译Internet Information Services (IIS) 管理員 | |
|--|---|
| | 🖸 🛛 🖓 🛛 |
| 檔案(F) 檢視(V) 說明(H) | |
| 建築 ● ● ● <td< td=""><td> 勤作 新增記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 檢視記錄檔 값明 線上說明 </td></td<> | 勤作 新增記錄定義 停用 Advanced Logging 停用用戶端記錄 編輯記錄欄位 編輯記錄欄位 檢視記錄檔 값明 線上說明 |
| 設定: localhost' applicationHost.config | € 1.: |

(16) 確認伺服器記錄目錄和預設站台記錄目錄 -> 按下 [確定]



- (17) 修改 nxlog.conf
- 註: 參考 1.3 NXLog 設定檔

藍色文字部位請輸入 Microsoft IIS 記錄檔資料夾路徑

define BASEDIR C:\inetpub\logs\AdvancedLogs





(18) 重啟 nxlog 服務

開啟 [Windows PowerShell] -> 輸入 Restart-Service nxlog 重新啟動 nxlog 服務和 Get-Service nxlog 查看 nxlog

服務狀態 -> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log' 確認沒有錯誤訊息



(19) 點選 [重新啟動] IIS 服務





(20) 確認 [C:\inetpub\logs\AdvancedLogs] 資料夾 IIS log 檔案: u_ex*.log

| 🕌 AdvancedLogs | | | | _ | |
|---------------------------------------|--------------------------------|-------------------|-----------|----------|-----|
| 00 💵 | \inetpub\logs\AdvancedLogs | - (| 🧑 搜尋 Adva | ncedLogs | 2 |
| 組合管理 👻 加 | 1入至媒體櫃▼ 共用對象 ▼ 新增] | 資料夾 | | = - | (?) |
| 🚖 我的最愛 | 名稱 ▲ | 修改日期 | 類型 | 大小 | |
| ;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;; | 🖺 u_ex_H20190806-091441942.log | 2019/8/6 下午 05:19 | 文字文件 | 51 KB | |
| 🜉 電腦 | | | | | |
| 👊 網路 | | | | | |





3.3 Event log

3.3.1 組織單位(Organizational Unit)

(1) 開啟 [Active Directory 使用者和電腦]



(2) 在 [Doman Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]

| 😑 Active Directory 使用者和電腦 📃 🗆 🗙 | | | | | | | |
|-------------------------------------|--------------|----------------|-------------------|--|--|--|--|
| 檔案(F) 執行(A) 檢視(V) 說明(H) | | | | | | | |
| (+ -> 2 💼 📋 🖻 🗟 🕞 🛛 🖬 🧏 🗽 🛅 🍸 🗾 🗞 | | | | | | | |
| 📃 Active Directory 🖗 | 使用者和電腦 [W 名稱 | 類型 | 描述 | | | | |
| 田 🧰 儲存查詢 | 📔 Builtin | builtinDomain | | | | | |
| 🖃 🏥 npartner.local | Computer 📔 | s 容區 | Default containe: | | | | |
| 🛨 🚞 Builtin | 委派控制(E) | mtr 組織單位 | Default containe: | | | | |
| 🕂 📒 Computer | 尋找(I) | uri 容區 | Default containe: | | | | |
| | 變更網域(D) | erv 容區 | Default containe: | | | | |
| | 變更網域控制站(C) | 谷區 | Default containe: | | | | |
| 🕀 🧰 Users | 提高網域功能等級(A)… | | | | | | |
| | 操作主機(M) | | | | | | |
| | 新增(N) ▶ | 電腦 | | | | | |
| | 所有工作(K) ▶ | 連絡人 | | | | | |
| | ▶ | 群組 | | | | | |
| | 104126(17 | InetOrgPerson | | | | | |
| | 重新整理(F) | msImaging-PSPs | | | | | |
| | 匯出清單(L) | MSMO 佇列別名 | | | | | |
| | 内容(R) | 組織單位 | | | | | |
| | | 印表機 | | | | | |
| | 說明(H) | 使用者 | | | | | |
| | | 共用資料夾 | | | | | |
| • | | | | | | | |
| 建立一個新物件… | | | | | | | |





| 新培物件 - 組織單位 | × |
|------------------------|---|
| 🧾 建立在: npartner.local/ | |
| _名稱(A): | |
| Servers | |
| ✓ 保護容器以防止被意外刪除(P) | |
| | |
| | |
| | |
| | |
| | |
| | _ |
| 工程定 取消 | |

(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Win2008)] 上按滑鼠右鍵 -> 點選 [移動]

| 🔚 Active Directory 使用者和電話 📃 🗆 🗙 | | | | | | | | |
|--|------------------|-----------------------------|----|--|--|--|--|--|
| 檔案(F) 執行(A) 檢視(V) 說明(H) | | | | | | | | |
| 🗢 🔿 📶 🤾 🗎 🗙 🖬 🖬 🛃 🖬 % 🗞 😭 🝸 💆 🎘 | | | | | | | | |
| ☐ Active Directory 使用者和電腦 [₩ 田 ^{○●} 儲存查詢 | 名稱 1. WIN2008 | 類型 電腦 | 描述 | | | | | |
| mpartner.local Builtin | | 加入群組中(G) 電路帳戶(A) | | | | | | |
| Computers | | ^{単設限戸(A)} 移動(V) | | | | | | |
| 🕀 🧮 ForeignSecurityPrincipals | | 管理(M) | | | | | | |
| ⊕ | | 所有工作(K) ▶ | | | | | | |
| Servers | | 剪下(T) 刪除(D) | | | | | | |
| | | 内容(R) | | | | | | |
| | | 說明(H) | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | • | | | | | | | |
| 將目前的選取項目移動到另一個組織單位。 | | | | | | | | |




(5) 點選 [Servers] 組織單位 -> 按下 [OK]



(6) 點選 [Servers] 組織單位,確認 Exchange Server(Win2008) 伺服器已移動





3.3.2 群組原則(Group Policy Management)

(1) 開啟 [群組原則管理]



(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到]







(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]

| 新増 GPO | | × |
|------------------|---------------|---|
| _名稱(N): | | |
| N-Partner Policy | | |
| 來源入門 GPO(\$): | | |
| (無) | | - |
| | 正確定 取消 | |

(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]





(5) 選擇 [Computer Configuration(電腦設定)] -> [Policies(原則)] -> [Windows Settings(Windows 設定)] -> [Security Settings(安全性設定)] -> [Local Policies(本機原則)] -> [Audit Policy(稽核原則)] -> 點選 [Audit account logon events(稽核帳戶登入事件)], [Audit account management(稽核帳戶管理)], [Audit logon events(稽核登入事件)] 項目 -







- (6) 在 Exchange Server 伺服器更新群組原則
- PS C:\> gpupdate /force



(7) 在 AD 網域伺服器,產生 Exchange Server 伺服器群組原則報表。參數: -Computer 為產生報告的電腦名稱,-

Path 指定報告文件的路徑和檔名。

PS C:\> Get-GPResultantSetofPolicy -Computer WIN2008 -Path C:\tmp\Win2008.html -ReportType html







| ØNPAR (| TNER\WIN2008 - W | indows Internet Expl | oiei | |
|-----------------|------------------------|----------------------|----------|-------------------|
| $\Theta \Theta$ | 🗢 🙋 C:\tmp\Win200 | 8.html 💌 🐓 | 🕨 🔀 Bing | P - |
| 🔶 我的最 | 💱 🔎 NPARTNER | 21WIN2008 | | 1 |
| ~ | | 我相反制结 | 里 | |
| NDADT | NED/WIN2008 | THER AN TERMAN | <i>ж</i> | |
| 資料收集 | : 2019/9/17下午 01:43:42 | | | <u> </u> |
| 摘要 | | | | 翻示 |
| 電腦設定 | ! | | | 隠藏 |
| 原則 | | | | 隠藏 |
| Wind | ows 設定 | | | 隠蔽 |
| 安全 | 全性表定 | | | 隠藏 |
| | 帳戶原則/密碼規則 | | | 顯示 |
| | 振戶原則/帳戶鎖定原則 | 1 | | 顯示 |
| | 版戶原則/Kerberos 原則 | 9 | | 顯示 |
| | 本禮原則/楷核原則 | | | 隠藏 |
| | 原則 | 設定 | 優勢(| \$PO |
| | 稽核帳戶登入事件 | 成功,失敗 | N-Partn | er Policy |
| | 稽核帳戶管理 | 成功,失敗 | N-Partn | er Policy |
| | 稽核登入事件 | 成功,失敗 | N-Partn | er Policy |
| | 本禮原則/安全性選項 | | | 顯示 |
| 3 | 公開金鑰原則/進證服務 | 第用戶端 - 自動註冊設》 | 定 | 翻示 |
| 3 | 公開金貨原則/加密檔案 | 《永統 | | 題示 |
| 3 | 公開金鑰原則/被信任的 | 的根準證授權單位 | | 翻示 |
| 使用者義 | 定 | | | 隠滅 |
| | 沒有可用的資料。 | | | |
| | | | | |
| | | 🗣 電腦 受保護模式: | 關閉 | 🐴 🔻 💐 100% 👻 // |





4. Exchange 2013

可選擇 [Exchange 系統管理中心] 或 [Exchange 管理命令介面] 確認啟用郵件追蹤記錄。

4.1 Exchange Message Tracking Log

4.1.1 Exchange 系統管理中心(EAC)

(1) 開啟 [瀏覽器] -> URL 輸入 <u>https://ExchangelP/ecp</u> -> 輸入網域名稱\帳號和密碼 -> 按下 [登入]





| 🔶 🔿 🍇 https://192.168.1.1 | 83/ecp/default.aspx?exsvurl=1&p=Servers ♀ ▼ | S 憑證錯誤 C III IIII IIIIIIIIIIIIIIIIIIIIIIIIII | |
|-----------------------------------|---|--|---|
| ① 企業版 Office 365 | | | Administrator 👻 📍 👻 |
| Exchange 系統管理 | 皇中心 | | |
| 收件者 | 伺服器 資料庫 資料庫可用性 | 群組 虛擬目錄 憑證 | |
| 權限 | | | |
| 法務遵循管理 | | | |
| 組織 | 名稱 ▲ 伺服器角色 | 版本 | |
| 保護 | WIN2012 信箱,用戶端存取 | Version 15.0 (Build 1473.3) | WIN2012 |
| 郵件流程 | | | 信相,用户骑存取 Version 15.0 (Build 1473.3) |
| 行動 | | | 信率30.HM 試用 輸入產品金銷 |
| 公用資料夾 | | | |
| 整合通訊 | | | |
| 伺服器 | | | |
| 混合 | | | |
| 工具 | | | |
| | | | |
| | | 已遇取1項,共1項 | |
| https://192.168.1.183/ecp/Servers | s/Servers.slab?showhelp=talse# | | |

(2) 點選 [伺服器] -> [伺服器] -> 選擇 [Mailbox 伺服器] -> 點選 [編輯]



(3) 點選 [傳輸記錄檔] -> 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange

х Exchange 伺服器 - Internet Explorer 🔹 https://**192.168.1.183**/ecp/Servers/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=454958ba-d6f1-431a-k 💈 憑證錯誤 說明 WIN2012 一般 郵件追蹤記錄檔 資料庫和資料庫可用性 ✔ 啟用郵件追蹤記錄檔 群組 郵件追蹤記錄檔路徑: POP3 C:\Program Files\Microsoft\Exchange Server\V15\TransportF IMAP4 整合通訊 連線記錄檔 ✓ 啟用連線記錄檔 DNS 查閱 連線記錄檔路徑: 傳輸限制 C:\Program Files\Microsoft\Exchange Server\V15\TransportF ▶傳輸記錄檔 Outlook Anywhere 通訊協定記錄檔 傳送通訊協定記錄檔路徑: C:\Program Files\Microsoft\Exchange Server\V15\TransportRole 接收通訊協定記錄檔路徑: C:\Program Files\Microsoft\Exchange Server\V15\TransportRole 儲存 取消 https://192.168.1.183/ecp/Servers/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=454958ba-d6f1-431a-l 🔍 100% +

Server\V15\TransportRoles\Logs\MessageTracking] -> 按下 [儲存]

¢¢





(1) 開啟 [Exchange Management Shell]



(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange

Server\V15\TransportRoles\Logs\MessageTracking]

[PS] C:\> Get-TransportService win2012 | Select-Object *Track*







4.2 IIS log

(1) 開啟 [Internet Information Services (IIS) 管理員]



(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]





(3) 選擇依下列項目為單位建立一個記錄檔: [Site(站台)] -> 記錄檔格式: [W3C] -> 目錄:

[%SystemDrive%\inetpub\logs\LogFiles] -> 編碼: [UTF-8] -> 記錄事件目的地: [Log file only(僅限記錄檔)] -> 排程: [Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select Fields(選取檔位)]

| Internet Information Services (IIS) 管理員 | _ D X |
|--|---|
| | 🔁 🛛 🟠 🔞 - |
| 檔案(F) 檢視(V) 說明(H) | |
| 田田山() (100(1) (100(1)) E | ● 要用 ● 取消 停用 強視記錄檔 ● 説明 |
| 設定: 'localhost' applicationHost.config | €L: |





(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、 [伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(csuri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(scwin32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(csversion)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [Add Field(新增欄位)]

| | W | 3C 記錄欄位 | | ? X |
|--|-------|---------|----|---------|
| 捂進躍(h/c). | | | | |
| [標準儞1辺(S): [夏日期(dete) | | | | |
| ▼ L 知 (date) | | | | |
| ▼ 時間(unie) | | | | |
| ☑ 使用者名稱(cs-username) | | | | |
| ☑ 服務名種(s-sitename) | | | | |
| ✓ 加切口時(Concentration) ✓ 伺服器名種(s-computernam) | ne) | | | |
| ✓ 伺服器 IP 位址 (s-ip) | , | | | |
| ✓ 伺服器連接埠(s-port) | | | | |
| ✔ 方法 (cs-method) | | | | |
| ✔ URI主體 (Stem) (cs-uri-stem | 1) | | | |
| ✔ URI 查詢 (cs-uri-query) | | | | |
| ✓ 通訊協定狀態 (sc-status) | | | | |
| | s) | | | |
| ✔ Win32 狀態 (sc-win32-status | 5) | | | |
| ☑ 已傳送位元組(sc-bytes) | | | | |
| ☑ 已接收位元組(cs-bytes) | | | | |
| ✔ 花費時間 (time-taken) | | | | |
| ✔ 通訊協定版本 (cs-version) | | | | |
| ✔ 主機 (cs-host) | | | | |
| ✔ 使用者代理程式(cs(User-Age | ent)) | | | |
| Cookie (cs(Cookie)) | | | | |
| ✔ 推薦者 (cs(Referer)) | | | | |
| 自訂欄位(C): | | | | |
| 包約四位 | 本酒箱刑 | | 本酒 | |
| 育し、季味・作業コムと | 不尽現至 | | 水尽 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| [| | | | |
| 新増欄位(A) 移除欄位 | (R) | | | 編輯檔案(E) |
| | | | | |
| | | | 確定 | 取消 |





- (5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [Request Header(要求標頭)] -> 輸入來源: X-Forwarded-For -
- > 按下 [確定]

| 新增自訂欄位 | ? | x |
|-----------------------------|----|---|
| 欄位名稱(N): X-Forwarded-For | | |
| ∝源蘋型(T): 要求種頭 | | |
| 來源(S): X-Forwarded-For | ~ | |
| | | |
| 確定 | 取消 | |



(6) 按下 [確定]

| | W3C 記錄欄位 | | ? X |
|------------------------------|----------|----|-----|
| / 種進欄位(S)· | | | |
| 展型用期(dete) | | | |
| ▼ I用 (time) | | | |
| ▼ 時間(unie) | | | |
| ▼ 用戶端IF 並且(C+p) | | | |
| ♥ 使用自有傳(Cs-username) | | | |
| ▼ 服務有機 (s-sitename) | | | |
| ✓ 向服器 TD 位地(sin) | ie) | | |
| ▼ 10版森 IP 12址(s-ip) | | | |
| ✓ 何服發建按焊(s-port) | | | |
| ✓ 方法 (cs-method) | | | |
| ✔ UKI 主證 (Stem) (cs-uri-stem |) | | |
| ✔ UKI 笪詞 (cs-uri-query) | | | |
| ✓ 通訊協定訊應 (sc-status) | | | |
| ✔ 週訊協定子款態 (sc-substatu | s) | | |
| ✔ Win32 狀態 (sc-win32-status | ;) | | |
| ✓ L傳送位元組 (sc-bytes) | | | |
| ✓ 已接收位元組(cs-bytes) | | | |
| ✓ 花費時間 (time-taken) | | | |
| ✓ 通訊協定版本 (cs-version) | | | |
| ✔ 主機 (cs-host) | | | |
| ✔ 使用者代理程式(cs(User-Age | ent)) | | |
| Cookie (cs(Cookie)) | | | |
| ✔ 推薦者 (cs(Referer)) | | | |
| 自訂欄位(C): | | | |
| 記錄欄位 | 來源類型 | 來源 | |
| | | | |

| 記録欄12 | 米源類型 | 米源 | |
|-----------------|-----------------------|-----------------|---------|
| X-Forwarded-For | 要求櫄頭 | X-Forwarded-For | |
| 新増欄位(A) 移除欄位 | <i>ζ</i> (R) | [| 編輯檔案(E) |
| | | 確定 | 取消 |





| V | Internet Information Services (IIS) 管理員 | _ |
|---|---|---------------|
| 🕞 💽 📲 🕨 WIN201 | 2 • | 🖬 🛛 🖓 🕡 - |
| 檔案(F) 檢視(V) 說明(H |) | |
| 檔案(F) 檢視(V) 說明(H 連線 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● | 副子子 副子 副子 如此市田不設定 IS 在銀頁伺服器上記錄要求的方式。 你下列項目為單位建立一個記錄欄(0): 「「」 記錄幅 相式(M): 「「「」 「「記錄幅 相式(M): 「「「」 「「」 「「」 「「」 「「」 「「」 「「」 「「」 「」 「「」 「「」 「「」 「」 「「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「 「 「 「」 「」 「」 「 「 | 数作 ▶ |
| 設定: 'localhost' applicationH | ost.config | € <u>1</u> .: |
| | | ul.:: |





(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log

| 34 | W3SVC | :1 | | _ 🗆 X |
|---------|---------------------------|-------------------|------|--------|
| € 🕘 🔹 ↑ | C:\inetpub\logs\LogFiles\ | W3SVC1 V | | VC1 ,9 |
| ☆ 我的最愛 | 名稱 | 修改日期 | 類型 | 大小 |
| | u_ex19080611_x.log | 2019/8/6 上午 11:45 | 文字文件 | 13 KB |
| 』 ● 本機 | | | | |
| 🗣 網路 | | | | |
| 1 個項目 | | | | = |





4.3 Event log

4.3.1 組織單位(Organizational Unit)

(1) 開啟 [Active Directory 使用者和電腦]



x Active Directory 使用者和電腦 檔案(F) 動作(A) 檢視(V) 說明(H) 🗢 🔿 🙍 🖬 📋 📑 🧔 🕪 🚺 <u>P</u> & 🔧 🗽 🛅 💎 Active Directory 使用者和電腦 名稱 類型 描述 ▶ 📔 儲存查詢 🚞 Builtin builtinDomain 🗯 🛱 npartner.local Computers 審區 Default container for u... 委派控制(E)... Default container for d... 組織單位 Default container for s... 尋找(1)... ipals 審區 Default container for ... cou... 容區 變更網域(D)... Sec... 組織單位 變更網域控制站(C)... 審區 Default container for u... 提高網域功能等級(A)... 操作主機(M)... 新增(N) 電腦 ۲ 所有工作(K) 連絡人 ۲ 群組 檢視(V) ۲ InetOrgPerson 重新整理(F) msExchDynamicDistributionList 匯出清單(L)... msImaging-PSPs 內容(R) MSMQ 佇列別名 說明(H) 組織單位 印表機 使用者 共用資料夾 > < ш 建立一個新物件...

(2) 在 [Doman Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





(3) 輸入組織單位名稱: Servers -> 按下 [確定]

| 新增物件 - 組織單位 | x |
|------------------------|---|
| 🥩 建立在: npartner.local/ | |
| 名稱(A): | |
| Servers | |
| ✔ 保護容器以防止被意外刪除(P) | |
| | |
| | |
| | |
| | |
| | |
| | — |
| 確定 取消 說明 | |



(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Win2012)] 上按滑鼠右鍵 -> 點選 [移動]

| ☐ Active Directory 使用者和電腦 | | | |
|--|---|--|--|
| 檔案(F) 動作(A) 檢視(V) 說明(H) ← → 2 〒 よ 目 × □ Q → 2 〒 * 2 & | | | |
| Active Directory 使用者和電腦 ● 儲存查詢 ▲ 鋼 npartner.local ▶ Builtin ○ Computers ▶ ○ Domain Controllers ▶ ○ Domain Controllers ▶ ○ ForeignSecurityPrincip ▶ ○ Managed Service Accc ▶ ○ Microsoft Exchange Se ▶ ○ Users ○ Servers | 稱 WIN2012 電腦 加入群組中(G) 停用帳戶(S) 重設帳戶(A) 移動(V) 管理(M) 所有工作(K) 前下(T) 刪除(D) 內容(R) 說明(H) | | |
| < Ⅲ > < ⅠⅡ ※ <li< td=""></li<> | | | |

(5) 點選 [Servers] 組織單位 -> 按下 [OK]





4.3.2 群組原則(Group Policy Management)

(1) 開啟 [群組原則管理]



•

(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到]

| <u> </u> | 群組原則 | 」管理 | _ D X |
|--|--|---------------------------|--------------|
| 🔜 檔案(F) 動作(A) 檢視(V |) 視窗(W) 說明(H) | | _ 8 × |
| 🗢 🔿 🖄 🔂 🚺 🗙 🛙 | i 🛛 🗊 | | |
| I 群組原則管理 ⊿ A 樹糸: npartner.local | | Servers 已連結的群組原則物件 | 群組原則繼承 委派 |
| ▲ 編 網域 ▲ 論 npartner.local 局 Default Dom ▷ î Domain Con ▷ î Microsoft Ex ▷ î Servers ▷ î 評組原則 ▷ î 秋田 師 ▷ î 秋田 原 戶 î 和組原則 從 群組原則 結果 | ain Policy trollers change Security Groups 在這個網域中建立 GPO 1 連結到現有的 GPO(L) 禁止繼承(B) 更新群組原則(U) 群組原則模型精靈(G) 新増組織單位(N) 檢視(V) 從這裡開啟新視窗(W) 刪除(D) 重新 命名(M) 重新 整理(F) 內容(R) 說明(H) | i 連結順序 並連結到(C) ト | GPO |
| | | < 111 | > |
| 在這個網域中建立 GPO 並將它調 | 車結到這個容器 | | |





(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]

| | 新増 GPO | × |
|-------------------------------------|--------|----|
| 名稱(<u>N</u>): N-Partner Policy | | |
| 來源入門 GPO(<u>S</u>): (無) | | ~ |
| | 確定 | 取消 |

(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]

| <u>II</u> | | 群組原則 | 管理 - ロ X |
|---|-------------|--|---|
| 🔜 檔案(F) 動作(A) 檢視(V) 視窗 | i(W) | 說明(H) | _ <i>8</i> × |
| 🧢 🔿 🙍 🖬 🗊 🖄 | ? | ÞE | |
| ■ 群組原則管理 ▲ 樹 樹糸: npartner.local ▲ 鋼 網域 ▲ 鋼 npartner.local ■ Default Domain Pol ▶ 窗 Domain Controllers ▶ 窗 Microsoft Exchange ▲ 窗 Servers | icy Secu | rity Groups | Servers 已連結的群組原則物件 群組原則繼承 委派 連結順序 GPO 会 1 副 N-Partner Policy |
| ▶ → 詳細原則物件 ▶ → → WMI 篩選器 ▶ → → 入門 GPO ▶ → → 和 ▶ → → 和 ▶ → → 和 ▶ → → → → → → → → → → → → → → → → → → → | | 編輯(E) 強制(N) 愈用連結(L) 儲存報告(S) 從這裡開啟新 刪除(D) 重新命名(M) 重新整理(F) 說明(H) | · 視窗(VV) |
| | | | |
| 開啟 GPO 編輯器 | | | |





(5) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶登入] -

> 點選 [稽核認證驗證] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]







> 點選 [稽核其他帳戶管理事件], [稽核使用者帳戶管理] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]

(6) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶管理] -

≜©





- > 點選 [稽核帳戶鎖定], [稽核登出], [稽核登入] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]
- (7) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [登入/登出] -

ner Technologies Co

♠¶__



PS C:\> gpupdate /force



(9) 在 AD 網域伺服器,產生 Exchange Server 伺服器群組原則報表。參數: -Computer 為產生報告的電腦名稱,-

Path 指定報告文件的路徑和檔名。

PS C:\> Get-GPResultantSetofPolicy -Path C:\tmp\Win2012.html -ReportType html -Computer WIN2012







(10) 開啟 [C:\tmp\Win2012.html] 確認啟用 [N-Partner Policy]

| ~ | | | | | | × |
|----------|---------------------------------|---------------------|---------------|----------------------|--|---|
| () | ∋ 🗿 C:\tmp\Win2012.html | 🔎 - ¢ 🏉 NPAF | RTNER\WIN2012 | × | 🕀 🛣 | ¢ |
| | | 群組原則結界 | 2 | | | |
| NPA | RTNER\WIN2012 | | | | | |
| 資料收 | 集: 16/8/2019 10:04:28 | | | | 顯示全部 | |
| 摘要 | | | | | 顯示 | |
| 電腦詳 | 細資料 | | | | <u> </u> | |
| 一般 | | | | | 顯示 | |
| 元件制 | 進) | | | | 顧示 | |
| 設定 | | | | | <u> </u> | |
| 原則 | | | | | <u> </u> | |
| Wi | ndows 設定 | | | | <u> </u> | |
| 3 | | | | | <u> </u> | |
| | | | | | <u>趙</u> 不 | |
| | 帳尸原則/帳尸類定原則 古機医則/向合始潮速 | | | | <u>顧不</u> | |
| | ▲ 微原則/安主性選貝 | | | | <u>顧不</u> | |
| | 公開金備原則/感證服務用尸婦-1 | 目動註冊設定 | | | <u>顧不</u> | |
| | 公開玉備原則/加密倫染系統 | | | | <u> 組不</u> | |
| | 進階相仮設定 | | | | 陸戦 | |
| | | | / | | 11111111111111111111111111111111111111 | |
| | | | 授努 N-P | GPO artner Policy | | - |
| | 作日答理 | 19973 · 2000 | | arener r oney | 四蘭 | |
| | · 10/2 · 12/2 | | 店墊 | CRO. | <u>Hartes</u> | |
| | 原則 | 成化 成功 , 失敗 | 1985 N-P | artner Policy | | - |
| | 稽核使用者帳戶管理 | 成功,失敗 | N-P | artner Policy | | |
| | 登入/登出 | | | | <u> </u> | |
| | 原則 | 設定 | 優勢 | GPO | | |
| | 稽核帳戶鎖定 | 成功,失敗 | N-P | artner Policy | | |
| | 稽核登出 | 成功,失敗 成功,失敗 | N-P | artner Policy | | |
| 문북 성당 [2 | | 19493 - 2016 | | arener roney | 座蔵 | - |
| 計組内 | 用的 GPO | | | | <u>吃</u> 跑 哩 蒂 | |
| | efault Domain Policy ((3182534) | 0-0160-1102-9455-00 | C04EB984E911 | | 開売 | |
| | -Partner Policy [/C8C6D0D6-97 | 1-42AD-BE1E-BC6A11 | 10BE20531 | | 顯示 | |
| 神拓 | 揮的 GPO | LAND DETERBOOK | | | 頭示 | |
| WMI | 篩選器 | | | | 顯示 | |
| 体田孝 | ¥如客料 | | | | | |
| 10,7131 | | | | | 粗小 | ~ |

Copyright © All rights are reserved by N-Partner Technologies Co



5. Exchange 2016

可選擇 [Exchange 管理主控台] 或 [Exchange 管理命令介面] 設定郵件追蹤記錄。

5.1 Exchange Message Tracking Log

5.1.1 Exchange 系統管理中心(EAC)

(1) 開啟 [瀏覽器] -> URL 輸入 <u>https://ExchangelP/ecp</u> -> 輸入網域名稱\帳號和密碼 -> 按下 [登入]







(2) 點選 [伺服器] -> [伺服器] -> 選擇 [Mailbox 伺服器] -> 點選 [編輯]

| (=) | 🔎 👻 憑證 🕈 🏉 伺服器 | - Microsoft Exchan × | | - □ × 企会感 ⁹ |
|------------------------------------|----------------|----------------------|---------------------|--|
| 企業版 Office 365 | | | | Administrator 🝷 📍 🝷 |
| Exchange 系統管理 | 瞿中心 | | | |
| 收件者 | 伺服器 資料庫 | ▣ 資料庫可用性群組 虛 | a擬目錄 憑證 | |
| 權限 | | | | |
| 合規性管理 | P 2 | | | |
| 組織 | 名稱 ▲ | 伺服器角色 | 版本 | |
| 保護 | EXCH2016 | 信箱 | Version 15.1 (Build | EXCH2016 |
| 郵件流程 | | | | 信箱 Version 15.1 (Build 1713.5) 標準試用版 |
| 行動 | | | | 試用 輸入產品金鑰 |
| 公用資料夾 | | | | |
| 整合通訊 | | | | |
| 伺服器 |] | | | |
| 混合 | | 已選取1個,共1個 | | |



(3) 點選 [傳輸記錄檔] -> 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange

| <i>@</i> Exchange 伺服器 - Internet Ex | xplorer — | | × |
|--|--|-------|-------|
| @ https:// 192.168.1.183 /ecp/Se | rvers/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=2297e724-7aad-425b | 8 | 慿證錯誤 |
| ➢ https://192.168.1.183/ecp/Se EXCH2016 一般 資料庫和資料庫可用性 群組 POP3 IMAP4 整合通訊 DNS 查閱 傳輸記錄檔 Outlook Anywhere | ■ 保建設記錄欄 ● 飲用郵件追蹤記錄欄 ● 飲用郵件追蹤記錄欄 ● 飲用郵件追蹤記錄欄 ● C\Program Files\Microsoft\Exchange Server\V15\TransportF ● 飲用連線記錄欄 ● 「 ● (小Pogram Files\Microsoft\Exchange Server\V15\TransportF) ● 「 ● (小Pogram Files\Microsoft\Exchange Server\V15\TransportF) ● (小Pogram Files\Microsoft\Exchange Server\V15\TransportF) ● (小Dagram Files\Microsoft\Exchange Server\V15\TransportRole) ● (小Pogram Files\Microsoft\Exchange Server\V15\TransportRole) ● (小Dagram Files\Microsoft\Exchange Server\V15\TransportRole) | | 憑證錯誤 |
| - | | | |
| https://192.168.1.183/ecp/Servers | :/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=2297e724-7aad-425b- 🔮 | ,1009 | 6 🔻 🔐 |

Server\V15\TransportRoles\Logs\MessageTracking] -> 按下 [儲存]





5.1.2 Exchange Management Shell

(1) 開啟 [Exchange Management Shell]



(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange

Server\V15\TransportRoles\Logs\MessageTracking]

[PS] C:\> Get-TransportService EXCH2016 | Select-Object *Track*







5.2 IIS log

(1) 開啟 [Internet Information Services (IIS) 管理員]



(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]







(3) 選擇依下列項目為單位建立一個記錄檔: [Site(站台)] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [Log file only(僅限記錄檔)] -> 排程:

[Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select

Fields(選取檔位)]

| ● WIN2016 ◆ ● WIN2016 ◆ 電気 ● WIN2016 ◆ ● WIN2016 ◆ 電気 ● WIN2016 ◆ ● WIN2016 ◆ ■ WIN2016 ◆ ● WIN2016 ◆ ● WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ● WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ ■ WIN2016 ◆ </th <th>♥iii Internet Information Services (IIS) 管理員</th> <th>– 🗆 X</th> | ♥iii Internet Information Services (IIS) 管理員 | – 🗆 X |
|---|--|--|
| ● (本人の) 設得(+) ● (本) (本人の) 設得(+) ● (本) (本人の) (************************************ | (← → ♥] ► WIN2016 ► | 🔯 🖂 🟠 🔞 🗸 |
| ● | 檔案(F) 檢視(V) 說明(H) | |
| ✓ 使用本地時間為檔案命名(U) ✓ 可用本地時間為檔案命名(U) ✓ 可用本地時間為檔案命名(U) | | 動作 ● 奈用 ● 夜視記錄檔 ● 説明 |
| | 設定: 'localhost' applicationHost.config | Sec. : |





(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、 [伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(csuri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(scwin32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(csversion)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [Add Field(新增欄位)]

| W3C 記錄欄位 | | | ? | × |
|--|-----------------------|----|--------|---|
| 櫄準欄位(S): | | | | |
| 標準欄位(S): ○ 日期(date) ○ 時間(time) ○ 用戶端IP位址(c-ip) ○ 使用者名稱(cs-username) ○ 使用者名稱(s-computername) ○ 伺服器名稱(s-computername) ○ 伺服器名稱(s-computername) ○ 伺服器連接埠(s-port) ○ 方法(cs-method) ○ URI 主體(Stem)(cs-uri-steme) ○ URI 查詢(cs-uri-query) ○ 通訊協定狀態(sc-status) ○ 通訊協定子狀態(sc-substatua) ○ 通訊協定子狀態(sc-substatua) ○ 已接收位元組(sc-bytes) ○ 花費時間(time-taken) ○ 連訊協定版本(cs-version) ○ 主機(cs-host) ○ 使用者代理程式(cs(User-Age ○ Cookie (cs(Cookie)) ○ 推薦者(cs(Referer)) | ne))) s) ;) | | | |
| 自訂欄位(C): | | | | |
| 記錄欄位 | 來源類型 | 來源 | | |
| | | | | |
| 新増欄位(A) 移除欄位 | (R) | | 編輯檔案(E |) |
| | | 確定 | 取消 | |





- (5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [Request Header(要求標頭)] -> 輸入來源: X-Forwarded-For -
- > 按下 [確定]

| 所増自訂欄位 | | ? | \times |
|-----------------|----|----|----------|
| 欄位名稱(N): | | | |
| X-Forwarded-For | | | |
| 來源類型(T): | | | |
| 要求櫄頭 | | ~ | |
| 來源(S): | | | |
| X-Forwarded-For | | ~ | |
| | | | |
| | | | |
| | 確定 | 取消 | |



(6) 按下 [確定]

| W3C 記錄欄位 | | | ? | \times |
|---|--------|-----------------|-------|----------|
| 標進欄位(S): | | | | |
| 日期(date) | | | | |
| 区時間(time) | | | | |
| | | | | |
| ☑ 佈田考之稱(cs-username) | | | | |
| ☑ 股份有有得(Cs-username) | | | | |
| ☑ / / / / / / / / / / / / / / / / / / / | me) | | | |
| ○ 同成報告報 (secomputernal) | ne) | | | |
| ☑ 伺服器連接控(shp) | | | | |
| ✓ 向成發建技程(s-port) | | | | |
| ☑ JPL 主聘 (Stem) (stem) (stem) | ~) | | | |
| ☑ UPI 查詢 (seturi, query) | ") | | | |
| ☑ 通知協定狀能 (sc-status) | | | | |
| ☑ 通訊協定訊號(sc-substat |) | | | |
| ☑ Win32 狀態 (sc-win32-state | us) | | | |
| 図 已傳送位元组 (sc-bytes) | , | | | |
| 図 已接收位元组 (cs-bytes) | | | | |
| ☑ 花费時間(time-taken) | | | | |
| ☑ 補訊協定版本 (cs-version) | | | | |
| ☑ 主機 (cs-host) | | | | |
| ☑ 使用者代理程式 (cs(User-Ac | aent)) | | | |
| Cookie (cs(Cookie)) | ,=,,, | | | |
| ☑ 推薦者 (cs(Referer)) | | | | |
| | | | | |
| 目訂欄位(C): | | | | |
| 記錄欄位 | 來源類型 | 來源 | | |
| X-Forwarded-For | 要求櫄頭 | X-Forwarded-For | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| 新増欄位(A) 移除欄(| 立(R) | | 編輯檔案(| E) |
| | | | | |
| | | 確定 | 取消 | |
| | | | | |
| | | | | |




(7) 按下 [Apply(套用)]



(8) 確認 [C:\inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log

| W3SVC1 | | | | - 0 | × |
|---|---------------------------|-------------------|------|--------|------------|
| $\leftarrow \rightarrow \cdot \uparrow$ | C:\inetpub\logs\LogFiles\ | W3SVC1 | ~ Ō | 搜尋 W39 | م V |
| 3. 他语方取 | | 修改日期 | 類型 | 大小 | |
| | u_ex19080614_x.log | 2019/8/6 下午 02:45 | 文字文件 | | 3 KB |
| ── 本機 | | | | | |
| 💣 網路 | | | | | |
| | | | | | |
| 1 個項目 | | | | | |

Copyright © All rights are reserved by N-Partner Technologies Co



5.3 Event log

5.3.1 組織單位(Organizational Unit)

(1) 開啟 [Active Directory 使用者和電腦]



| | 」,又府部百姓 · 赵]丰 [师相] | | | | |
|-------------------------|------------------------|---------------------|-------------------------|------|----------|
| Active Directory | 吏用者和電腦 | | _ | | \times |
| 檔案(F) 動作(A) 相 | 僉視(Ⅴ) 說明(H) | | | | |
| 🗢 🔿 🔁 📰 🗎 | 🖾 🗟 🗟 🚺 🖏 | 8 🛅 🔻 🖻 ' | L | | |
| Active Directory 億 > | 使用者和電腦 名稱 ■ Builtin | 類型 builtinDomain | 描述 | | |
| ✓ jii npartner.local | | क्रान का | Default container for u | I | |
| > Builtin | 委派控制(E) | 單位 | Default container for c | ł | |
| Domain Co | 尋找(I) | | Default container for s | | |
| > 🧮 ForeignSec | 變更網域(D) | | Default container for | - | |
| > 📔 Managed : | 變更網域控制站(C) | | Default container for u | l | |
| > 📔 Users | 提高網域功能等級(A) | | | | |
| | 操作主機(M) | | | | |
| | 新增(N) | > 電腦 | | | |
| | 所有工作(K) | > 連絡 | ٨. | | |
| | 檢視(∨) | →群組 | | | |
| | 手が教理の | InetC | DrgPerson | | |
| | 里利亞煋(F) 陳山注留(1) | msD | S-ShadowPrincipalConta | iner | |
| | 進山周半(L) | mslm | naging-PSPs | | |
| | 內容(R) | MSN | /IQ 佇列別名 | | |
| | 說明(H) | 組織 | 單位 | | |
| | | 印表 | 機 | | |
| | | 使用: | 者 | | |
| < | > | 共用: | 資料夾 | | |
| 建立一個新物件 | | | | | |

(2) 在 [Doman Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





(3) 輸入組織單位名稱: Servers -> 按下 [確定]

| 亲 | 「増物件 - 組 | 織單位 | | | × |
|---|----------|--------|-----------------|----|----|
| | 1 | 建立在: | npartner.local/ | | |
| | 名稱(A): | | | | _ |
| | Servers | | | | |
| | ☑保護容 | 器以防止被怠 | ፻外刪除(P) | | • |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| - | | | 確定 | 取消 | 說明 |





(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Exch2016)] 上按滑鼠右鍵 -> 點選 [移動]

(5) 點選 [Servers] 組織單位 -> 按下 [OK]

Ó





5.3.2 群組原則(Group Policy Management)

(1) 開啟 [群組原則管理]



≜[®]_

_ 群組原則管理 × 🔜 檔案(F) 動作(A) 檢視(V) _ 8 × 視窗(W) 說明(H) 🔜 群組原則管理 群組原則管理 ✓ ▲ 樹条: npartner.local 內容 🗸 📑 網域 名稱 ✓ i npartner.local 🛒 Default Domai \Lambda 樹条: npartner.local 道 Domain Contro Servers > 📑 群組原則 在這個網域中建立 GPO 並連結到(C)... → 📑 WMI 篩 連結到現有的 GPO(L)... > 🛅 入門 GF 禁止繼承(B) > 📫 網站 更新群組原則(U)... 矡 群組原則模型 📑 群組原則結果 群組原則模型精靈(G)... 新增組織單位(N) 從這裡開啟新視窗(W) 刪除(D) 重新命名(M) 重新整理(F) 內容(R) 說明(H) > > 1 < 在這個網域中建立 GPO 並將它連結到這個容器

(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到這裡]





(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]

| 新増 GPO | × |
|------------------|-------|
| 名稱(N): | |
| N-Partner Policy | |
| 來源入門 GPO(S): | |
| (無) | ~ |
| | 確定 取消 |

(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]

| 🗾 群組原則管理 | - 🗆 × |
|--|--|
| <u>属</u> 檔案(F) 動作(A) 檢視(V) 視窗 | (W) 說明(H) _ & × |
| 🖛 🔿 📊 🖸 🖬 | · · · · · · · · · · · · · · · · · · · |
| ¥組原則管理 ▲ 樹系: npartner.local ● 鍋 網域 ● 鋼 npartner.local ● 圖 Default Domain Poli > 圖 Domain Controllers > 圖 Servers ● N-Partner Policy | 群組原則管理 內容 CY 名稱 ▲樹系: npartner.local |
| ○□ 群組原則物件 >□○ WMI 篩選器 >□○ 入門 GPO >□○ 網站 20 群組原則模型 10 群組原則結果 | 編輯(E) 強制(N) 愈用連結(L) 儲存報告(S) 從這裡開啟新視窗(VV) 刪除(D) 重新命名(M) 重新整理(F) 說明(H) |
| < | > < > > |
| 開啟 GPO 編輯器 | |





(5) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶登入] -

> 點選 [稽核認證驗證] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]







> 點選 [稽核其他帳戶管理事件], [稽核使用者帳戶管理] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]

(6) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶管理] -

≜°≏





- > 點選 [稽核帳戶鎖定], [稽核登出], [稽核登入] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]
- (7) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [登入/登出] -

🔊 N- Partner

er Technologies Co



- (8) 在 Exchange Server 伺服器更新群組原則
- PS C:\> gpupdate /force



(9) 在 AD 網域伺服器,產生 Exchange Server 伺服器群組原則報表。參數: -Computer 為產生報告的電腦名稱, -

Path 指定報告文件的路徑和檔名。

PS C:\> Get-GPResultantSetofPolicy -Path C:\tmp\Exch2016.html -ReportType html -Computer EXCH2016







| C:\tmp\Exch2016.html | P → C @ NPARTNER\EXCH | 12016 × | - □ × |
|----------------------|-----------------------|------------------|---------------------|
| 設定 | | | 四边 |
| 原則 | | | (元, (2)) (元, 元年) |
| Windows 設定 | | | (京和) |
| 安全性設定 | | | 時職 |
| 帳戶原則/密碼規則 | | | |
| 低いための中国が低いの | | | 顧示 |
| 帳尸原則/帳尸類定原則 | | | 顯示 |
| 本機原則/安全性選項 | | | 顧示 |
| 公開金鑰原則/憑證服務用戶端 - 自動語 | 注冊設定 | | 顯示 |
| 公開金鑰原則/加密檔案系統 | | | RT |
| 進階稽核設定 | | | ##/\ |
| 帳戶登入 | | | 清瓶 |
| E BI | -1 | 原動でゆう | 陪藏 |
| 原见 箱核認證論語 | | N-Partner Policy | |
| | - XXX | in tartier ency | |
| 10/18/H | | | 傿藏 |
| 原則 | 設定 | 優勢 GPO | |
| 稽核其他帳戶管理事件 | 成功,失敗 | N-Partner Policy | |
| 稽核使用者帳戶管理 | 成功,失敗 | N-Partner Policy | |
| 登入/登出 | | | 医藏 |
| 原則 | 設定 | 優勢 GPO | |
| 稽核帳戶鎖定 | 成功,失敗 | N-Partner Policy | |
| 稽核登出 | 成功,失敗 | N-Partner Policy | |
| 稽核登入 | 成功,失敗 | N-Partner Policy | |

(10) 開啟 [C:\tmp\EXCH2016.html] 確認啟用 [N-Partner Policy]





6. Exchange 2019

可選擇 [Exchange 系統管理中心] 或 [Exchange 管理命令介面] 確認啟用郵件追蹤記錄。

6.1 Exchange Message Tracking Log

6.1.1 Exchange 系統管理中心(EAC)

(1) 開啟 [瀏覽器] -> URL 輸入 <u>https://ExchangelP/ecp</u> -> 輸入網域名稱\帳號和密碼 -> 按下 [登入]

| () Ittps://192.168.1.183/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a | - □ × a962f962f192.168.1.183' ▼ 2 憑證錯誤 C 搜尋 |
|--|--|
| P Exchange 系統管理中心 × | <section-header><form><form><form><form><form></form></form></form></form></form></section-header> |





(2) 點選 [伺服器]-> [伺服器]-> 選擇 [Mailbox 伺服器]-> 點選 [編輯]

| 会 会 Mttps://192.168.1.1 | 183/ecp/default.aspx | → 😒 憑證錯誤 ひ | 搜尋 | - ロ × 9 読 会 優 <mark>- Q</mark> |
|--|----------------------|------------|---------------------|-----------------------------------|
| ① 企業版 Office 365 | | | | Administrator 👻 📍 👻 |
| Exchange 系統管理 | 里中心 | | | |
| 收件者 | 伺服器 資料庫 | 資料庫可用性群組 虛 | 擬目錄 憑證 | |
| 權限 | | | | |
| 合規性管理 | <u>,</u> P B | | | |
| 組織 | 名稱▲ | 伺服器角色 | 版本 | |
| 保護 | EXCH2019 | 信箱 | Version 15.2 (Build | EXCH2019 |
| 郵件流程 | | | | 信箱 Version 15.2 (Build 330.5) |
| 行動 | | | | 標準試用版 試用 輸入產品金鑰 |
| 公用資料夾 | | | | |
| 伺服器 | | | | |
| 混合 | | 已選取1個,共1個 | | |



(3) 點選 [傳輸記錄檔] -> 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange

🥝 Exchange 伺服器 - Internet Explorer × 😼 https://**192.168.1.183**/ecp/Servers/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=95fc12aa-c374-49ca-b 💈 憑證錯誤 EXCH2019 一般 郵件追蹤記錄檔 資料庫和資料庫可用性 ✔ 啟用郵件追蹤記錄檔 群組 郵件追蹤記錄檔路徑: POP3 C:\Program Files\Microsoft\Exchange Server\V15\TransportF IMAP4 整合通訊 連線記錄檔 ☑ 啟用連線記錄檔 DNS 查閱 連線記錄檔路徑: 傳輸限制 C:\Program Files\Microsoft\Exchange Server\V15\TransportF ▶傳輸記錄檔 Outlook Anywhere 通訊協定記錄檔 傳送通訊協定記錄檔路徑: C:\Program Files\Microsoft\Exchange Server\V15\TransportRole 接收通訊協定記錄檔路徑: C:\Program Files\Microsoft\Exchange Server\V15\TransportRole 儲存 取消 https://192.168.1.183/ecp/Servers/EditServer.aspx?pwmcid=3&ReturnObjectType=1&id=95fc12aa-c374-49ca-b 🍕 100% Ŧ

Server\V15\TransportRoles\Logs\MessageTracking] -> 按下 [儲存]





6.1.2 Exchange Management Shell

(1) 開啟 [Exchange Management Shell]



(2) 確認 [啟用郵件追蹤記錄檔] 和郵件追蹤記錄檔路徑: [C:\Program Files\Microsoft\Exchange

Server\V15\TransportRoles\Logs\MessageTracking]

[PS] C:\> Get-TransportService EXCH2019 | Select-Object *Track*







6.2 IIS log

(1) 開啟 [Internet Information Services (IIS) 管理員]



(2) 選擇 [IIS Server] -> 點選 [Logging(記錄)]







(3) 選擇依下列項目為單位建立一個記錄檔: [Site(站台)] -> 記錄檔格式: [W3C] -> 目錄:

%SystemDrive%\inetpub\logs\LogFiles -> 編碼: [UTF-8] -> 記錄事件目的地: [Log file only(僅限記錄檔)] -> 排程:

[Hourly(每小時)] -> 勾選 [Use local time for file naming and rollover(使用本地時間為檔案命名)] -> 按下 [Select

Fields(選取檔位)]





(4) 勾選 [日期(date)]、[時間(time)]、[用戶端 IP 位址(c-ip)]、[使用者名稱(cs-username)]、[服務名稱(s-sitename)]、 [伺服器名稱(s-computername)]、[伺服器 IP 位址(s-ip)]、[伺服器連接埠(s-port)]、[方法(cs-method)]、[URI 主體(csuri-stem)]、[URI 查詢(cs-uri-query)]、[通訊協定狀態(sc-status)]、[通訊協定子狀態(sc-substatus)]、[Win32 狀態(scwin32-status)]、[傳送位元組(sc-bytes)]、[接收位元組(cs-bytes)]、[花費時間(time-taken)]、[通訊協定版本(csversion)]、[主機(cs-host)]、[使用者代理(cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者(cs(Referer))] -> 按下 [Add Field(新增欄位)]

| W3C 記錄欄位 | | ? | × |
|---|----|---------------|---|
| 標準欄位(S): ● 日期(date) ● 時間(time) ● 月戶端IP位址(c-ip) ● 使用者名稱(cs-username) ● 使用者名稱(s-sitename) ● 伺服器名稱(s-computername) ● 小孩(cs-method) ● URI 查閱(cs-uri-query) ● 通訊協定大態(sc-substatus) ● ご接收位元組(sc-bytes) ● 活費時間(time-taken) ● 連開協定版本(cs-version) ● 主機(cs-host) ● 使用者代理程式(cs(User-Agent)) ● Cookie(cs(Cookie)) ● 推薦者(cs(Referer)) | | | |
| 記錄欄位 來源類型 | 來源 | | |
| 新増欄位(A) 移除欄位(R) | 確定 | 編輯檔案(E) 取消 |) |





- (5) 輸入欄位名稱: X-Forwarded-For -> 選擇來源類型: [Request Header(要求標頭)] -> 輸入來源: X-Forwarded-For -
- > 按下 [確定]

| 所増自訂欄位 | | ? | \times |
|-----------------|----|----|----------|
| 欄位名稱(N): | | | |
| X-Forwarded-For | | | |
| 來源類型(T): | | | |
| 要求櫄頭 | | ~ | |
| 來源(S): | | | |
| X-Forwarded-For | | ~ | |
| | | | |
| | | | |
| | 確定 | 取消 | |



(6) 按下 [確定]

| W3C 記錄欄位 | | | ? | \times |
|---|--------|-----------------|-------|----------|
| / 種 準 擱 位 (€)・ | | | | |
| 1票4年間位(3). | | | | |
| ☑ 山朔 (date) | | | | |
| | | | | |
| ☑ 用戶端 IF 並址 (C-IP) ☑ 使田考名稱(cs-username) | | | | |
| ☑ 使用有有偿 (Cs-username) | | | | |
| ☑ 加扬石博 (s-sitename) ☑ 伺昭器名稱 (s-computernar) | me) | | | |
| ☑ 伺服器 IP 位址 (s-in) | iic y | | | |
| ☑ 伺服器連接塢 (s-port) | | | | |
| 区 方法 (cs-method) | | | | |
| ☑ URI主體 (Stem) (cs-uri-sten | n) | | | |
| ☑ URI 查詢 (cs-uri-query) | , | | | |
| ☑ 通訊協定狀態 (sc-status) | | | | |
| ☑ 通訊協定子狀態 (sc-substatu) | us) | | | |
| ☑ Win32 狀態 (sc-win32-statu | is) | | | |
| □ □ 已傳送位元組 (sc-bytes) | | | | |
| ☐ 已接收位元組(cs-bytes) | | | | |
| ☑ 花費時間 (time-taken) | | | | |
| ☑ 通訊協定版本 (cs-version) | | | | |
| ✓ 主機 (cs-host) | | | | |
| ☑ 使用者代理程式 (cs(User-Ag | jent)) | | | |
| Cookie (cs(Cookie)) | | | | |
| ✓ 推薦者 (cs(Referer)) | | | | |
| | | | | |
| 自訂欄位(C): | | | | |
| 記錄欄位 | 來源類型 | 來源 | | |
| X-Forwarded-For | 要求櫄頭 | X-Forwarded-For | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| 新増欄位(A) 移除欄位 | 立(R) | 43 | 冒輯檔案(| E) |
| | | | | |
| | | 確定 | 取消 | |
| | | l | | |
| | | | | |





(7) 按下 [Apply(套用)]

| ♥ Internet Information Services (IIS) 管理員 | - 🗆 × |
|---|--|
| (← → ♥] → WIN2019 → | 🖆 🖂 🙆 • |
| 檔案(F) 檢視(V) 說明(H) | |
| 職員 記録 夏安福岡 ● 日本地陸電海電査会(1) 記録 記録 ● 日本地陸電海電会(1) 記録 記録 記録 ● 日本地陸電空 記録 記録 記録 記録 ● 「「「 記録 記録 『 記録 『 記録 『 記録 記録 記録 記録 記録 記録 記録 記録 記録 記録 | 動作 ● 取当 儲存目前的變更。 停用 檢視記錄欄 ② 說明 |
| 設定: 'localhost' applicationHost.config | • <u></u> .: |
| | |





(8) 確認 [C:\ inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: u_ex*.log

| W3SVC1 | 5 | | | - | | × |
|-----------------|--|-------------------|-----------------|----|------|----------|
| ← → ~ ↑ 📙 C:\ir | netpub\logs\LogFiles\W3SVC1 | ٽ ~ | 搜尋 W3SVC | 1 | | <i>م</i> |
| 人 快速方面 | 名稱 | 修改日期 | _{類型} ^ | 大小 | | |
| A 下述1+4X | u_ex19080614_x.log | 2019/8/6 下午 02:58 | 文字文件 | | 5 KB | |
| 🔜 本機 | | | | | | |
| 🥣 網路 | <mark>etpub\logs\LogFiles\W3SVC</mark> 名稱 | | | | | |
| 1 個項目 | | | | | | :== |





6.3 Event log

6.3.1 組織單位(Organizational Unit)

(1) 開啟 [Active Directory 使用者和電腦]



📃 Active Directory 使用者和電腦 Х 檔案(F) 動作(A) 檢視(V) 說明(H) 🗢 🔿 🙋 📅 📋 🗐 🧟 🗟 🛛 🖬 🖄 🍇 🛅 🍸 💆 🍇 Active Directory 使用者和電腦 [Win2019/ 名稱 類型 描述 📔 儲存查詢 5 🚞 Builtin builtinDomain npartner.local Computers 審區 Default container for u... > 📔 Builtin 委派控制(E)... Default container for d... o... 組織單位 > Computers 尋找(l)... c... 容區 Default container for s... > 💼 Domain Co S... 容區 Default container for ... 變更網域(D)... > ForeignSec 審區 Default container for u... 變更網域控制站(C)... > 📔 Managed > 📔 Users 提高網域功能等級(A)... 操作主機(M)... 新增(N) Σ 電腦 連絡人 所有工作(K) > 群組 > 檢視(V) InetOrgPerson 重新整理(F) msDS-ShadowPrincipalContainer 匯出清單(L)... msImaging-PSPs 內容(R) MSMQ 佇列別名 組織單位 說明(H) 印表機 使用者 共用資料夾 > < | 建立一個新物件...

(2) 在 [Doman Name] 按滑鼠右鍵 -> 選擇 [新增] -> 點選 [組織單位]





(3) 輸入組織單位名稱: Servers -> 按下 [確定]

| 新増物件 - 組織單位 | | | × |
|-----------------|----------------|----|----|
| 建立在: ng | partner.local/ | | |
| 名稱(<u>A</u>): | | | |
| Servers | | | |
| ☑ 保護容器以防止被意外冊 | NI除(P) | | _ |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | 確定 | 取消 | 說明 |







(4) 點選 [Computers] 組織單位 -> 在 [Exchange Server(Exch2019)] 上按滑鼠右鍵 -> 點選 [移動]

(5) 點選 [Servers] 組織單位 -> 按下 [OK]





6.3.2 群組原則(Group Policy Management)

(1) 開啟 [群組原則管理]



(2) 在 [Servers] 上按滑鼠右鍵 -> 點選 [在這個網域中建立 GPO 並連結到這裡]

| 🔜 群組原則管理 | | | | — C |) × |
|------------------------------|---------------|-----------------------|--------|-----------|-------|
| <u>属</u> 檔案(F) 動作(A) 檢視(V) | 視窗(W) | 說明(H) | | | - 8 × |
| 🗢 🔿 🗖 📰 🗎 🗙 🗐 (| 0 | ÞE | | | |
| 🔜 群組原則管理 | | Servers | | | |
| ✓ ▲ 樹糸: npartner.local | | 已連結的君 | ¥組原則物件 | 群組原則繼承 | 委派 |
| ✓ 論 約以 ✓ 論 npartner.local | | | 連結順序 | GPO | |
| 🗐 Default Domain | Policy | | | | |
| > 📴 Domain Controll | llers | | | | |
| > ■ Servers | 這個網想 | ¢由建文GPO | 前救它浦结药 | ∭這裡(()) | |
| > 🔓 WMI 篩 連 | 這個調算 結到現有 | (中建立 GPO 1的 GPO(L) | | -JJE1±(C) | |
| → 1 (m) 入門 GP (注) | 止繼承(B | 3) | | | |
| > | , 新群組原 | 〔 [則(U) | | | |
| ■ 群組原則結果 群組 | 組原則構 | 型結囊(G) | | | |
| 新知 | 増組織單 | (山) | | | |
| 合 | 這つつ | | | | > |
| (2) | 這裡開創 | x新視窗(W) | | | ŕ |
| mula | | | | | _ |
| | 际(D) 新命之(N | JD. | | | |
| | 新幣石(1) | -) -) | | | |
| | (中) (中) | , | | | |
| Mi | 풉(K) | | | | |
| 說印 | 明(H) | | | | |
| | | < | | | > |
| └── 在這個網域中建立 GPO 並將它連結到 | 到這個容 | 器 | | | |





(3) 輸入群組原則物件名稱: N-Partner Policy -> 按下 [確定]

| 新増 GPO | × |
|------------------|-------|
| _名稱(N): | |
| N-Partner Policy | |
| 來源入門 GPO(S): | |
| (無) | ~ |
| | 確定 取消 |

(4) 在 [N-Partner Policy] 上按滑鼠右鍵 -> 點選 [編輯]

| 📓 群組原則管理 | – 🗆 × |
|--|---|
| ▲ 檔案(F) 動作(A) 檢視(V) 視窗(V) | V) 說明(H) |
| 🗢 🔿 🗖 📆 📋 🗙 🗒 🝳 | ? |
| ¥組原則管理 ★ 樹系: npartner.local ★ 副 網域 ★ 副 npartner.local ● Default Domain Policy > 圖 Domain Controllers ★ 圖 Servers ● 副 和組原則物件 > 圖 秋川 篩選器 > 圖 入門 GPO > 圖 網站 ● 群組原則模型 ● 群組原則結果 | Servers 已連結的群組原則物件 群組原則繼承 委派 連結順序 GPO ① 1 通 1 編輯(E) 運 強制(N) 酸用連結(L) 儲存報告(S) 從這裡開啟新視窗(W) 刪除(D) 重新 命名(M) 重新整理(F) 說明(H) |
| | < |
| 開啟 GPO 編輯器 | |



(5) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶登入] -

> 點選 [稽核認證驗證] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]







(6) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [帳戶管理] -

🔊 N- Partner

iner Technologies Co



> 點選 [稽核帳戶鎖定], [稽核登出], [稽核登入] -> 勾選 [設定下列稽核事件:] [成功] 和 [失敗] -> 按下 [確定]

≜°≏

(7) 選擇 [電腦設定] -> [原則] -> [Windows 設定] -> [安全性設定] -> [進階稽核原則設定] -> [稽核原則] -> [登入/登出] -





(8) 在 Exchange Server 伺服器更新群組原則

PS C:\> gpupdate /force



(9) 在 AD 網域伺服器,產生 Exchange Server 伺服器群組原則報表。參數:-Computer 為產生報告的電腦名稱,-

Path 指定報告文件的路徑和檔名。

PS C:\> Get-GPResultantSetofPolicy -Path C:\tmp\Exch2019.html -ReportType html -Computer EXCH2019







(10) 開啟 [C:\tmp\EXCH2019.html] 確認啟用 [N-Partner Policy]

| | | | 00 273 000 |
|---|--|--|--|
| | | | |
| | 群組原則結果 | | |
| NPARTNER\EXCH2019 | | | |
| 資料収集: 2019/9/4 上午 11:59:15 | | | 全部顯示 |
| 1 安 | | | <u>顧示</u> |
| 匿腦詳細資料 | | | مين 100 |
| - \$ | | | par res. |
| 元件狀態 | | | 顧示 |
| 11.c> | _ | | 顧示 |
| | | | 隱藏 |
| 原則 | | | 晤藏 |
| Windows 設定 | | | |
| 安全性設定 | | | 時間 |
| 能后面削/索研组制 | | | |
| | | | 顧示 |
| 帳戶原則/帳戶鋇定原則 | | | 顧示 |
| 本機原則/安全性選項 | | | 顯示 |
| 公開金鑰原則/憑證服務用戶端 - 自動語 | 注冊設定 | | |
| 公開金鑰原則/加密檔案系統 | | | 翻示 |
| · · · · · · · · · · · · · · · · · · · | | | 顧示 |
| 建帕帕尔波龙 | | | 陪藏 |
| 帳戶登入 | | | 馮藏 |
| 原則 | 設定 | 優勢 GPO | |
| 稽核認證驗證 | 成功,失敗 | N-Partner Policy | |
| 帳戶管理 | | | |
| | ÷1. ÷ | (月前) 000 | 四方 四 |
| E Bul | | 優恐 GPO | |
| 原則 | ====================================== | N Pertra P II | |
| 原則 稽核其他帳戶管理事件 緒核伸田者框戶管理 | 成功,失敗 成功,失敗 成功,失敗 | N-Partner Policy | |
| 原則 稽核其他帳戶管理事件 稽核使用者帳戶管理 | 成功,失敗 成功,失敗 | N-Partner Policy N-Partner Policy | |
| 原則 稽核其他帳戶管理事件 稽核使用者帳戶管理 登入/登出 | 成功,失敗 成功,失敗 成功,失敗 | N-Partner Policy N-Partner Policy | 匯藏 |
| 原則 稽核其他帳戶管理事件 稽核使用者帳戶管理 登入/登出 原則 | | @BS GPO | 陪藏 |
| 原則 稽核其他帳戶管理事件 稽核使用者帳戶管理 登入/登出 原則 稽核帳戶鎖定 | | 使势 GPO N-Partner Policy 何势 GPO N-Partner Policy | 医藏 |





7. N-Reporter

7.1 Exchange Message Tracking log

(1) 新增 Exchange Server 設備

選擇 [設備管理] -> [設備樹狀圖] -> 按下 [新增]







(2) 設定 Exchange message tracking 設備的資料格式和 Facility

輸入設備 名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Exchange] 和 Facility: [(2) mail system] -> 選擇 設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]

| L 新增設備 | |
|---|-----|
| 設備基本設定 | ^ |
| 名稱 | |
| Exchange_Mail-192.168.1.183 | |
| IP | |
| 192.168.1.183 | |
| 設備種類 | · |
| Syslog Flow SNMP | |
| Syslog 相關設定 | |
| 資料格式 | |
| Exchange 2013 🗸 | |
| Facility | |
| (2) mail system 🗸 🗸 | |
| 編碼方式 | |
| UTF-8 | |
| | |
| 設備進階設定 | |
| 設備 Icon | |
| icon-host 🗸 | |
| Login Account | |
| | |
| Login Password | |
| | |
| 接收狀態 | |
| ● 啟用 | |
| 暫無資料告警 | |
| ▶ 上 ● L ■ L ■ L ■ L ■ L ■ L ■ L ■ L ■ L ■ L | |
| | ✓ |
| | .01 |





7.2 Exchange Event log

(1) 新增 Exchange Event 設備

選擇 [設備管理] -> [設備樹狀圖] -> 按下 [新增]







(2) 設定 Exchange event 設備的資料格式和 Facility

輸入設備 名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Windows] 和 Facility: [(20) local use 4 (local4)] -

> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]

| 新增設備 | | | |
|---------------------------------------|-----|---------|---|
| 設備基本設定 | | | 1 |
| 名稱 | | | |
| Exchange_Event-192.168.1.183 | | | |
| D | | | |
| 192.168.1.183 | | | |
| | | | |
| ☆備連類 ✓ Svslog □ Flow □ SNIMP | | | |
| | | | |
| Syslog 相關設定 | | | |
| | | | |
| 資料格式 | | | |
| Windows | ~ | | |
| Facility | | | |
| (20) local use 4 (local4) | ~ | - | |
| 編碼方式 | | - | |
| UTF-8 | ~ | - | |
| | | | |
| 時佛谁限設定 | | | |
| | | | |
| 設備 Icon | | _ | |
| icon-host | ~ | | |
| Login Account | | | |
| | | | |
| Login Password | | | |
| | | | |
| 按收罪能 | | | |
| ■ | | | |
| ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● | | | |
| 自無見行百言 | | | |
| | | | |
| | | Birtick | |
| | Т.E | 収泊 | |




7.3 Exchange IIS log

(1) 新增 Exchange IIS 設備

選擇 [設備管理] -> [設備樹狀圖] -> 按下 [新增]







(2) 設定 Exchange IIS 設備的資料格式和 Facility

輸入設備 名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [IIS] 和 Facility: [(22) local use 6 (local6)] -> 選 擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]

| 新增設備 | |
|----------------------------|---|
| 設備基本設定 | ^ |
| | |
| 名稱 | |
| Exchange_IIS-192.168.1.183 | |
| IP | |
| 192.168.1.183 | |
| 設備種類 | |
| Syslog Flow SNMP | |
| | |
| Syslog 相關設定 | |
| 資料格式 | |
| IIS v | |
| Facility | |
| (22) local use 6 (local6) | |
| | |
| 編碼方式 | |
| UTF-8 | |
| | |
| 設備進階設定 | |
| | |
| 設備 Icon | |
| icon-host 🗸 | |
| Login Account | |
| | |
| Login Password | |
| | |
| | |
| | |
| | |
| | |
| ▶ 展用 Sysiog/Flow 智無資料告誓 | |
| | × |
| 確定 取 | 肖 |



連絡資訊

....

TEL: +886-4-23752865 FAX: +886-4-23757458 技術問題請洽:

Email: support@npartnertech.com

Skype: support@npartnertech.com

業務相關請洽:

Email: sales@npartnertech.com

