使用 PortQry 命令行工具

發行項 • 2024/03/21

PortQry 是一種命令行工具，可用來協助針對 TCP/IP 連線問題進行疑難解答。 此工具會報告本機電腦或遠端電腦上目標 TCP 和用戶數據報協定 (UDP) 埠的狀態。 它也會提供本機計算機埠使用量的詳細資訊。

由於 PortQry 是用來作為疑難解答工具，因此使用它來針對特定問題進行疑難解答的用戶應該有足夠的運算環境知識。

您可以在數種模式的其中一種模式中，從命令提示字元使用 PortQry：

- 命令行模式。 您可以使用此模式對本機或遠端電腦進行疑難解答。
- 本機模式。 在此模式中，您可以使用數個參數來針對本機計算機進行疑難解答。
- 互動式模式。 類似於命令行模式，但您可以使用快捷方式命令和參數。

> **注意**
>
> 您可以下載稱為 PortQryUI 的個別工具，其中包含適用於 PortQry 的圖形化 UI。 PortQryUI 有數項功能，可讓您更輕鬆地使用 PortQry。 若要取得 PortQryUI 工具，請參閱 PortQryUI - PortQry 命令行埠掃描器的使用者介面。

適用於： 支援的 Windows 版本

PortQry 測試和結果

一般埠掃描工具會報告，如果目標 UDP 埠未傳回因特網控制訊息通訊協定 (ICMP) 「目的地無法連線」訊息，則埠會有「接 **聽** 」狀態。 此結果可能因為下列其中一個或兩個原因而不正確：

- 如果沒有對有向數據報的回應，則目標埠可能是 **FILTERED**。
- 大部分的服務不會回應傳送給它們的未格式化用戶數據報。 一般而言，接聽埠的服務或程式只會回應使用特定會話層或應用層通訊協定的訊息。

為了產生更精確且實用的結果，PortQry 會使用雙步驟測試程式。

步驟 1：埠狀態測試

PortQry 會將埠的狀態報告為三個值的其中一個：

- **接聽**：此回應表示進程正在目標埠上接聽。 PortQry 收到來自目標埠的回應。

- **不接聽**：此回應表示目標埠上沒有進程正在接聽。 PortQry 從目標埠收到下列其中一個 ICMP 訊息：

  > 無法連線到目的地埠

- **FILTERED**：此回應表示正在篩選目標埠。 PortQry 未收到來自目標埠的回應。 進程不一定正在目標埠上接聽。 根據預設，PortQry 會先查詢 TCP 連接埠三次，再傳回 **FILTERED** 的回應，然後在傳回 **FILTERED** 的回應之前查詢 UDP 埠一次。

步驟 2：特製化測試

如果沒有來自目標 UDP 埠的回應，PortQry 會報告埠為 LISTENING **或 FILTERED**。 不過，當您針對連線問題進行疑難解答時，瞭解埠是否正在篩選或正在接聽很有用。 這在包含一或多個防火牆的環境中尤其如此。

PortQry 會使用第二組測試來精簡其埠狀態報告，以與接聽目標埠的服務或程序互動。 針對這項測試，PortQry 會執行下列動作：

- PortQry 會使用位於 *%SYSTEMROOT%\System32\Drivers\Etc* 資料夾中的 Services 檔案，來判斷每個埠上接聽的服務。
- PortQry 會建立特別針對預期的服務或程式建構的訊息，然後將該訊息傳送至目標埠。 根據服務或程式，訊息可能會要求適用於疑難解答的資訊，如下所示：
  - LDAP 查詢 (網域和域控制器資訊)
  - 已註冊的用戶端服務和埠 (RPC 查詢)
  - FTP 查詢 (是否允許匿名存取)
  - NETBIOS 查詢 (MAC 位址)
  - Mspclnt.ini ISA Server 查詢 (檔案資訊)
- PortQry 會剖析、格式化，然後從服務或程式傳回回應，作為其測試報告的一部分。

針對本機計算機進行疑難解答的其他測試

當您必須在安裝 PortQry 的電腦上針對埠進行疑難解答時，請在本機模式中使用 PortQry。 當您在命令列使用本機模式參數時，可以在本機電腦上執行下列工作：

- 列舉埠對應
- 監視特定埠的變更
- 監視特定程序的變更

如需詳細資訊，請 參閱在本機 (命令行) 模式中使用 PortQry。

在命令行模式中使用 PortQry

您可以使用與任何其他命令行工具相同的方式，在命令提示字元中執行 PortQry。 本文中的大部分範例都會顯示命令行 PortQry 命令。 在命令行模式中，您可以將多個選項新增至命令字串，以指定要執行的查詢以及執行方式。 若要在命令行模式中執行 PortQry，請執行使用下列語法的命令：

主控台

```
portqry.exe -n <name_to_query> [options]
```

> **注意**
>
> 在此命令中， *<name_to_query>* 是要查詢的IP位址、計算機名稱或網域。 這是必要參數。 [*options*] 是選擇性參數。

命令行模式的 PortQry 參數

下列參數可在一般命令行模式中使用：

展開資料表

參數	描述	Comments
`-n <name>`	查詢特定目的地	• 這是命令行模式的唯一必要參數。 • *名稱*><值代表要查詢之計算機的名稱或IP位址。 這個值不能包含空格。
`-p <protocol>`	使用指定的通訊協定	• 通訊 <*協定*> 值代表要查詢的埠類型， (可能的值為 `tcp`、 `udp` 或 `both`)。 • 預設值為 `tcp`。
`-e <port_number>`	指定目標埠 (也稱為「端點」)	• port_number值代表要在目的地計算機上查詢的埠。 >> • 預設值為 `80`。
`-o <port_number>,<port_number>`	依序指定多個目標埠	*port_number*，*port_number*>><<值代表以逗號分隔的埠號碼清單，以順序查詢。 請勿在逗號周圍使用空格。
`-r <port_number>:<port_number>`	指定目標埠的範圍	• > <port_number：<*port_number*> 值代表起始和結束埠號碼，並以冒號分隔。 請勿在冒號周圍使用空格。

參數	描述	Comments
		• 起始埠號碼必須小於結束埠號碼。
`-l <filename.txt>`	產生記錄檔	• filename.txt值代表記錄檔的名稱和擴展名。>< 這個值不能包含空格。 • 當命令執行時，PortQry 會在安裝它的目錄中建立記錄檔。 • 如果檔案已經存在，除非您也使用 `-y` 參數) ，否則 PortQry 會要求您確認您想要將它覆寫 (。
`-y`	覆寫先前的記錄檔	• 當您搭配 `-l`使用 `-y` 時，PortQry 會覆寫現有的記錄檔，而不會提示您確認動作。 • 如果 PortQry 命令字串不包含 `-l`，PortQry 會 `-y`忽略 。
`-sl`	等候額外的回應時間 (也稱為慢速連結延遲)	使用此參數可讓 PortQry 等候 UDP 埠回應的時間加倍，然後 PortQry 會判斷埠未接聽或已篩選。 當您查詢速度緩慢或不可靠的網路連結時，一般等候時間可能太短而無法接收回應。
`-nr`	略過反向名稱查閱	• 根據預設，當您使用 `-n` 指定目標計算機的IP位址時，PortQry 會執行反向名稱查閱，將IP位址解析為名稱。 此程式可能很耗時，特別是當 PortQry 無法解析 IP 位址時。 使用 `-nr` 略過查詢的這個步驟。 • 如果您使用 `-n` 指定電腦或網域名稱，PortQry 會 `-nr`忽略 。

參數	描述	Comments
`-sp <port_number>`	從特定來源埠查詢	• port_number值代表 PortQry 用來傳送查詢的埠。>< • PortQry 無法使用另一個進程已使用的埠。 如果您指定的埠已在使用中，PortQry 會傳回下列錯誤訊息： 無法使用指定的來源埠。 埠已在使用中。 指定未使用的埠，然後再次執行命令。 • 在下列情況下，PortQry 會使用指定的埠進行查詢的第一個測試，但不會使用第二個測試： ○ RPC (TCP 和 UDP 連接埠 135) ○ LDAP (UDP 連接埠 389) ○ UDP 連接埠 137 (NetBIOS 配接器狀態查詢) 在這些情況下，PortQry 會使用暫時埠進行第二次測試。 發生這種情況時，PortQry 會在其輸出中記錄「使用暫時來源埠」。 • 如果安裝 PortQry 的計算機也執行 IPSec 原則代理程式，UDP 連接埠 500 可能無法作為來源埠使用。 若要暫時關閉 IPSec 原則代理程式，讓您可以使用埠 500，請執行 `net stop PolicyAgent`。 當您完成測試時，請執行 `net start PolicyAgent`。
`-cn ! <community_name>!`	查詢SNMP社群	• community_name值代表要查詢的SNMP社群名稱。>< 您必須使用驚嘆號來分隔此值，如左欄所示。 • 如果 SNMP 服務未接聽目標埠，PortQry 會 `-cn`忽略。 • 預設社群名稱為 `public`。
`-q`	在無訊息模式中執行 PortQry	• 當您使用 `-q`時，PortQry 會隱藏所有屏幕輸出，但錯誤訊息除外。 • 若要查看錯誤訊息以外的輸出，請搭配 使用 `-q` 。`-l` PortQry 會在記錄檔中記錄一般輸出。 • 如果記錄檔已經存在，而且您搭配 `-l`使用 `-q` ，PortQry 會覆寫現有的記錄檔，而不會提示您。 • 您無法與`-o`、 `-r`或`-p both`一起使用`-q`。 • 當您使用批處理文件來執行 PortQry 命令字串時，這個參數特別有用。

命令行模式中參數的備註

- 任何埠號碼值都必須是介於 1 到 65535 之間的有效埠號碼，包含在內。
- 、 `-e` `-o`和 `-r` 參數互斥。 單一 PortQry 命令只能使用其中一個參數。
- 對 UDP 連接埠 389 (LDAP) 的查詢可能無法針對執行 Windows Server 2008 的域控制器運作。 若要檢查在 UDP 連接埠 389 上執行之服務的可用性，您可以使用 Nltest 而非 PortQry。 如需詳細資訊，請參閱 Nltest。

- 當您使用 `-e` 或 `-o`查詢埠 135 (RPC) 時，PortQry 會傳回目前向 RPC 端點對應程式註冊的所有端點。

  > **ⓘ 重要**
  >
  > 當您使用 時 `-r`，PortQry 不會查詢 RPC 端點對應程式。

- 當您查詢埠 53 (DNS) 時，PortQry 會使用 TCP 和 UDP 來傳送 的 `portqry.microsoft.com` DNS 查詢。 如果伺服器傳回回應，PortQry 會判斷埠為 LISTENING。

  > **ⓘ 注意**
  >
  > DNS 伺服器傳回正回應或負回應並不重要。 任何回應都表示埠正在接聽。

在本機 (命令行) 模式中使用 PortQry

您可以在本機模式中使用 PortQry 來取得有關執行 PortQry 之本機電腦上 TCP 連接埠和 UDP 連接埠的詳細資訊，而不是查詢遠端目標電腦上的埠。 使用下列語法在本機模式中執行 PortQry：

主控台

```
portqry -local | -wpid <pid> | -wport <port_number> [-wt <seconds>] [-l
<filename.txt>] [-v]
```

下表的本機模式參數說明此語法中的佔位元：

展開資料表

參數	描述	Comments
`-local`	擷取本機資訊	• 列舉本機計算機上目前作用中的所有 TCP 和 UDP 埠對應。 此輸出類似於命令產生的輸出 `netstat.exe -an` 。 • 在支援 PID 對埠對應的電腦上，輸出會包含在本機電腦上使用埠之進程的 PID。 如果您使用詳細資訊選項 () `-v` ，輸出也會包含 PID 所屬服務的名稱，並列出進程已載入的所有模組。 您可以使用此資訊來判斷哪些埠與電腦上執行的特定程式或服務相關聯。
`-wport <port_number>`	監看式埠	• 監視特定埠的變更。 port_number值代表要監視的埠。> • 如果是 TCP 連接埠，PortQry 會報告下列狀態之間的變更：

參數	描述	Comments
		○ **CLOSE_WAIT** ○ **關閉** ○ **建立** ○ **FIN_WAIT_1** ○ **LAST_ACK** ○ **聽** ○ **SYN_RECEIVED** ○ **SYN_SEND** ○ **TIMED_WAIT** • 針對UDP埠，PortQry 會報告程式是否系結至埠，但不會報告UDP埠是否收到數據報。 • 若要停止監視，請按 Esc。
`-wpid <pid>`	監看程式標識碼 (PID)	• 監視特定 PID，以取得連線數目和狀態的變更。process_number值代表要監視的 PID。>< • 若要停止監視，請按 Esc。
`-wt <seconds>`	依特定間隔檢查	• 在 */<seconds>* 值所代表的間隔內，檢查 或 `"-wpid` `-wport` 所識別目標的狀態。 • *秒*><數值必須介於 1 到 1,200 (內含) 。 • 預設值為 `60` 。 • 您無法單獨或搭配 `-local`使用 `-wt` 。
`-l <filename.txt>`	產生記錄檔	• filename.txt值代表記錄檔的名稱和擴展名。>< 這個值不能包含空格。 • 當命令執行時，PortQry 會在安裝它的目錄中建立記錄檔。 • 如果檔案已經存在，除非您也使用 `-y` 參數) ，否則 PortQry 會要求您確認您想要將它覆寫 (。
`-y`	覆寫先前的記錄檔	• 當您搭配 `-l`使用 `-y` 時，PortQry 會覆寫現有的記錄檔，而不會提示您確認動作。 • 如果 PortQry 命令字串不包含 `-l` ，PortQry 會 `-y`忽略 。
`-v`	產生詳細信息輸出	如果使用) ，PortQry 會將其他詳細數據提供給螢幕輸出 (和記錄檔。

本機模式中參數的備註

- 、 `-local` `-wport`和 `-wpid` 參數互斥。 您只能在單一 PortQry 命令字串中使用其中一個參數。
- 參數 `-q` 無法在本機模式中運作。

- 在某些情況下，PortQry 可能會報告系統閒置程式 (PID 0) 使用某些 TCP 連接埠。 如果本機程式連線到 TCP 連接埠，然後停止，可能會發生此行為。 即使程式不再執行，程式與埠的 TCP 連線仍可能會保持「定時等候」狀態數分鐘。 在這種情況下，PortQry 可能會偵測到埠正在使用中，但無法識別使用埠的程式，因為 PID 已釋出。 根據預設，埠會保持「定時等候」狀態，長度是最大區段存留期的兩倍。
- 針對每個程式，PortQry 會報告可存取的信息數量。 某些資訊的存取受到限制。 例如，禁止存取Idle和 CSRSS進程的模組資訊，因為其存取限制會防止使用者層級程式代碼開啟它們。 為了獲得最佳結果，請在本機系統管理員或具有類似認證的帳戶內容中執行本機模式命令。
- 當您搭配 使用 `-wport` 或 `-wpid` 時 `-l`，請使用 Esc 鍵來中斷和結束 PortQry，而不是 CTRL+C。 您必須按下 Esc，以確保 PortQry 正確地關閉記錄檔並結束。 如果您按 CTRL+C 而不是 Esc 來停止 PortQry，記錄檔可能會變成空白或損毀。

在互動式模式中使用 PortQry

當您針對計算機之間的連線問題進行疑難解答時，可能必須輸入許多重複的命令。 在互動式模式中使用 PortQry，可以更輕鬆地完成這類動作。

互動式模式類似於 Nslookup DNS 公用程式或 Nblookup WINS 公用程式中的互動式功能。

若要在互動式模式中啟動 PortQry，請使用 `-i` 參數。 例如，執行下列命令：

主控台

```
portqry -i
```

此指令輸出類似下列摘錄：

輸出

```
Portqry Interactive Mode

Type 'help' for a list of commands

Default Node: 127.0.0.1

Current option values:
   end port= 80
   protocol= TCP
   source port= 0 (ephemeral)
>
```

互動式模式命令

您可以在互動式模式中使用下列命令：

展開資料表

命令	描述	Comments
`node <name>` 或 `n <name>`	設定要查詢的目的地	• *名稱*><值代表要查詢之計算機的名稱或IP位址。這個值不能包含空格。 • 預設值 (`127.0.0.1` 本機計算機) 。
`query` 或 `q`	傳送查詢	• 使用目前的設定查詢目前的目的地。 • 預設通訊協定為 `tcp`。 • 預設目的地埠是 TCP 連接埠 80。 • 默認來源埠是暫時埠) (埠 0。 • 您可以搭配 命令使用數個快捷方式 `query` 的其中一個，以便執行數個常見查詢中的任何一個。 如需可用快捷方式的清單，請參閱 互動式模式查詢快捷方式。
`set <option>=<value>`	設定查詢選項的值	• 在此命令中，*option*>< 代表要設定的選項名稱，*而*< value > 代表選項的新值。 • 若要檢視可用選項的目前值清單，請輸入 `set all`。 • 如需可用選項的清單，請參閱 互動式模式選項。
`exit`	保持互動模式	

互動式模式查詢快捷方式

您可以使用下列快捷方式搭配 `query` 命令來執行一般查詢，而不需要設定埠和通訊協議選項。 使用下列語法：

主控台

```
q <shortcut>
```

> **注意**
>
> 在此命令中， <*快捷方式*> 代表下表中的其中一個快捷方式。 如果您省略快捷方式，命令會 `q` 查詢 TCP 連接埠 80。

展開資料表

Shortcut	要查詢的埠
`dns`	TCP 連接埠 53，UDP 連接埠 53。
`ftp`	TCP 連接埠 21
`imap`	TCP 連接埠 143
`ipsec`	UDP 埠 500
`isa`	TCP 連接埠 1745，UDP 連接埠 1745
`ldap`	TCP 連接埠 389，UDP 連接埠 389
`l2tp`	UDP 埠 1701
`mail`	TCP 連接埠 25、110 和 143
`pop3`	TCP 連接埠 110
`rpc`	TCP 連接埠 135，UDP 連接埠 135
`smtp`	TCP 連接埠 25
`snmp`	UDP 埠 161
`sql`	TCP 連接埠 1433，UDP 連接埠 1434
`tftp`	UDP 埠 69

例如，在互動式模式中輸入 `q dns` 相當於 `portqry -n 127.0.0.1 -p both -e 135` 在一般命令行模式中執行。

互動式模式選項

您可以使用 `set` 命令來設定選項，例如來源埠或慢速連結延遲。 使用下列語法：

主控台

```
set <option>=<value>
```

> **注意**
>
> 在此命令中，*option*>< 代表要設定的選項名稱，而 <*value*> 則代表選項的新值。

展開資料表

選項	描述	Comments
`set all`	顯示選項的目前值	
`set port=<port_number>` `set e=<port_number>`	指定目標埠	port_number值代表要在目的地計算機上查詢的埠。>
`set sport=<port_number>` `set sp=<port_number>`	指定來源埠	• port_number值代表 PortQry 用來傳送查詢的埠。> • PortQry 無法使用另一個進程已使用的埠。 • 如果您指定的埠號碼為零，PortQry 會使用暫時埠。
`set protocol=<protocol>` `set p=<protocol>`	指定要使用的通訊協定	通訊<*協定*>值代表要 (、 `udp` 或 `both`) `tcp` 查詢的埠類型。
`set cn=<community_name>`	指定 SNMP 社群	• community_name值代表要查詢的SNMP社群名稱。> • 如果 SNMP 服務未接聽目標埠，PortQry 會 `-cn` 忽略 。 • 預設社群名稱為 `public` 。
`set nr`	關閉或開啟反向名稱查閱	• 根據預設，如果您已將IP位址設定為查詢目的地，PortQry 會將IP位址解析為名稱。 如果您變更此選項，PortQry 會略過名稱解析步驟。 • 若要再次開啟反向名稱查閱，請 `set nr` 執行第二次。
`set sl`	開啟或關閉慢速連結延遲	• 如果您變更此選項，PortQry 會在 PortQry 判斷埠未接聽或已篩選之前，等候 UDP 埠回應的時間長度加倍。 當您查詢速度緩慢或不可靠的網路連結時，一般等候時間可能太短而無法接收回應。 • 若要再次關閉慢速連結延遲，請 `set sl` 執行第二次。

假設您想要查詢IP位址為10.0.1.10的電腦。 在互動式模式命令提示字元中，輸入 `n 10.0.1.10`。 這個指令會產生類似下列摘錄的輸出：

輸出

```
Default Node: 10.0.1.10

>
```

若要傳送 DNS 查詢，請在互動式模式命令提示字元中輸入 `q dns` 。 這個指令會產生類似下列摘錄的輸出：

輸出

```
resolving service name using local services file...
UDP port resolved to the 'domain' service

IP address resolved to myserver.contoso.com

querying...

UDP port 53 (domain service): LISTENING

>
```

自定義埠與服務之間的關聯

根據預設，每部 Windows 計算機都有位於 *%SYSTEMROOT%\System32\Drivers\Etc* 資料夾中的 Services 檔案。 PortQry 會使用此檔案，將埠號碼解析為其對應的服務名稱。 PortQry 會使用此資訊來選取其查詢的格式。 您可以編輯此檔案，以指示 PortQry 將格式化的訊息傳送至替代埠。 例如，下列專案會出現在一般服務檔案中：

輸出

```
ldap              389/tcp                         #Lightweight Directory
Access Protocol
```

您可以編輯此連接埠專案或新增其他專案。 若要強制 PortQry 將 LDAP 查詢傳送至埠 1025，請修改專案，如下所示：

輸出

```
ldap              1025/tcp                         #Lightweight Directory
Access Protocol
```

範例

下列範例示範如何使用 PortQry 及其參數：

本機模式

- 查詢本機計算機
- 在存取可能受到限制時查詢本機計算機

- 使用特定間隔監視進程標識碼
- 查詢慢速連結

命令行模式

- 指定目標和通訊協定
- 指定一或多個目標埠
- 指定 PortQry 輸出的記錄檔
- 使用批處理檔以無訊息模式執行 PortQry
- 查詢埠 135 (RPC 服務)

查詢本機計算機

輸出 `portqry -local` 類似下列摘錄：

輸出

```
TCP/UDP Port Usage

96 active ports found

Port Local IPState Remote IP:Port
TCP 80 0.0.0.0 LISTENING 0.0.0.0:18510
TCP 80 169.254.149.9 TIME WAIT 169.254.74.55:3716
TCP 80 169.254.149.9 TIME WAIT 169.254.200.222:3885
TCP 135 0.0.0.0 LISTENING 0.0.0.0:10280
UDP 135 0.0.0.0 :
UDP 137 169.254.149.9 :
UDP 138 169.254.149.9 :
TCP 139 169.254.149.9 LISTENING 0.0.0.0:43065
TCP 139 169.254.149.9 ESTABLISHED 169.254.4.253:4310
TCP 139 169.254.149.9 ESTABLISHED 169.254.74.55:3714
```

在存取可能受到限制時查詢本機計算機

當您以本機模式執行 PortQry 時，如上一個範例所示，您可能會看到類似下列摘要的輸出。 這類輸出表示 PortQry 所使用的安全性內容沒有足夠的許可權可存取它要求的所有資訊。

輸出

```
Port and Module Information by Process

Note: restrictions applied to some processes may
prevent Portqry from accessing more information

For best results run Portqry in the context of
```

```
the local administrator

=====================================================
Process ID: 0 (System Idle Process)

PIDPortLocal IPState Remote IP:Port
0TCP 4442 169.254.113.96 TIME WAIT 169.254.5.136:80
0TCP 4456 169.254.113.96 TIME WAIT 169.254.5.44:445

Port Statistics

TCP mappings: 2
UDP mappings: 0

TCP ports in a TIME WAIT state: 2 = 100.00%

Could not access module information for this process

=====================================================
```

使用特定間隔監視進程標識碼

下列命令會監視特定行程：

主控台

```
portqry.exe -wpid 1276 -wt 2 -v -l pid.txt
```

因此，PortQry 會採取下列動作：

- 識別具有 1276 PID 的進程，並每隔兩秒檢查其使用的埠狀態，直到您按 Esc 為止。
- pid.txt建立*記錄檔*。 如果已經有該名稱的檔案存在，PortQry 會提示您確認要覆寫檔案。
- 記錄記錄檔中的任何輸出，包括額外的詳細信息輸出。

記錄檔的內容類似下列摘錄：

輸出

```
PortQry Version 2.0 Log File

System Date: <DateTime>

Command run:
portqry -wpid 1276 -wt 2 -v -l pid.txt

Local computer name:

host123
```

```
Watching PID: 1276

Checking for changes every 2 seconds

verbose output requested

Service Name: DNS
Display Name: DNS Server
Service Type: runs in its own process

============
System Date: <DateTime>

=======================================================

Process ID: 1276 (dns.exe)

Service Name: DNS
Display Name: DNS Server
Service Type: runs in its own process

PIDPortLocal IPState Remote IP:Port
1276TCP 53 0.0.0.0 LISTENING 0.0.0.0:2160
1276TCP 1087 0.0.0.0 LISTENING 0.0.0.0:37074
1276UDP 1086 0.0.0.0 :
1276UDP 2126 0.0.0.0 :
1276UDP 53 127.0.0.1 :
1276UDP 1085 127.0.0.1 :
1276UDP 53 169.254.11.96 :

Port Statistics

TCP mappings: 2
UDP mappings: 5

TCP ports in a LISTENING state: 2 = 100.00%

Loaded modules:
C:\WINDOWS\System32\dns.exe (0x01000000)
C:\WINDOWS\system32\ntdll.dll (0x77F40000)
C:\WINDOWS\system32\kernel32.dll (0x77E40000)
C:\WINDOWS\system32\msvcrt.dll (0x77BA0000)
C:\WINDOWS\system32\ADVAPI32.dll (0x77DA0000)
C:\WINDOWS\system32\RPCRT4.dll (0x77C50000)
C:\WINDOWS\System32\WS2_32.dll (0x71C00000)
C:\WINDOWS\System32\WS2HELP.dll (0x71BF0000)
C:\WINDOWS\system32\USER32.dll (0x77D00000)
C:\WINDOWS\system32\GDI32.dll (0x77C00000)
C:\WINDOWS\System32\NETAPI32.dll (0x71C40000)
```

指定目標和通訊協定

> **注意**
>
> 本節中的每個範例都會查詢埠 80，也就是預設埠。

下列命令會查詢電腦上的預設 TCP 連接埠，該電腦使用其完整功能變數名稱 (FQDN) ：

```
主控台

portqry -n myDomainController.example.com -p tcp
```

下列命令會查詢電腦上使用其電腦名稱指定的預設 UDP 連接埠：

```
主控台

portqry -n myServer -p udp
```

下列命令會查詢使用其 IP 位址指定之電腦的預設 TCP 和 UDP 連接埠：

```
主控台

portqry -n 192.168.1.20 -p both
```

下列命令會執行與上一個命令相同的查詢，但略過名稱解析步驟：

```
主控台

portqry -n 192.168.1.20 -p both -nr
```

下列命令會查詢網頁伺服器的預設 TCP 連接埠：

```
主控台

portqry -n www.widgets.microsoft.com
```

指定一或多個目標埠

下列命令會查詢 TCP 連接埠 25，以測試郵件伺服器的 SMTP 服務：

```
主控台

portqry -n mail.example.com -p tcp -e 25
```

下列命令會查詢 IP 位址為 192.168.1.20 之計算機的 TCP 連接埠 60897 和 UDP 連接埠 60897：

主控台

```
portqry -n 192.168.1.20 -p both -e 60897
```

下列命令會查詢該順序中的 UDP 連接埠 139、1025 和 135 (，) 計算機 “myServer” 上：

主控台

```
portqry -n myServer -p udp -o 139,1025,135
```

下列命令會查詢埠 135 到埠 139 的埠範圍， (計算機 “myServer” 上的內含) ：

主控台

```
portqry -n myServer -p udp -r 135:139
```

指定 PortQry 輸出的記錄檔

下列命令會查詢 mail.widgets.microsoft.com 上的 TCP 連接埠 143，並將輸出記錄在 *portqry.txt* 檔中。 如果檔案已經存在，PortQry 會覆寫該檔案，而不會提示您確認。

主控台

```
portqry -n mail.widgets.microsoft.com -p tcp -e 143 -l portqry.txt -y
```

查詢慢速連結

下列命令會在 mail.widgets.microsoft.com 上查詢 TCP 連接埠 143、110 和 25。 針對每個目標埠，PortQry 會比平常等候兩倍的回應。

主控台

```
  portqry -n mail.widgets.microsoft.com -p tcp -o 143,110,25 -sl
```

指定來源埠

如果本機計算機上的) 可將查詢傳送至 192.168.1.20 上的 UDP 連接埠 53，則下列命令會使用 UDP 連接埠 3001 (。 如果服務正在該埠上接聽並回應查詢，它會將回應傳送至本機

計算機上的 UDP 連接埠 3001。

主控台

```
portqry -p udp -e 53 -sp 3001 -n 192.168.1.20
```

如果可在本機計算機上) 將查詢傳送至 myDomainController.contoso.com 上的 UDP 連接埠 389，則下列命令會使用 UDP 連接埠 3000 (。 根據預設，LDAP 服務應該接聽此埠。 如果LDAP服務回應第一個查詢，PortQry 會使用暫時來源埠來傳送格式化的查詢並接收任何回應。

主控台

```
portqry -n myDomainController.contoso.com -e 389 -sp 3000
```

使用批處理檔以無訊息模式執行 PortQry

下列文字是以無訊息模式執行 PortQry 的批次處理檔範例：

主控台

```
:Top
portqry -n 169.254.18.22 -e 443 -nr -l pqlog.txt -q
:end
```

當此批處理文件執行時，PortQry 會產生名為 *pqlog.txt*的記錄檔。 此檔案的內容如下所示：

輸出

```
PortQry Version 2.0 Log File

System Date: Thu Sep 16 10:35:03 2021

Command run:
 portqry -n 169.254.18.22 -e 443 -nr -l pqlog.txt -q

Local computer name:

 SOURCESERVER

Querying target system called:

 169.254.18.22

TCP port 443 (https service): LISTENING
```

```
========= end of log file =========
```

查詢埠 135 (RPC 服務)

下列命令會查詢 myServer 電腦上的 UDP 連接埠 135。 根據預設，RPC 服務應該接聽此埠。

主控台

```
portqry -n myServer -p udp -e 135
```

因此，PortQry 會採取下列動作：

- PortQry 會使用 *%SYSTEMROOT%\System32\Drivers\Etc* 資料夾中的 Services 檔案，將 UDP 連接埠 135 解析為服務。 使用預設組態，PortQry 會將埠解析為 RPC 端點對應程式服務，(Epmap)。
- PortQry 會將未格式化的用戶數據報傳送至目的地電腦上的 UDP 連接埠 135。 PortQry 不會收到來自目標埠的回應。 這是因為 RPC 端點對應程式服務只會回應格式正確的 RPC 查詢。 PortQry 報告埠為 LISTENING **或 FILTERED**。
- PortQry 會建立格式正確的 RPC 查詢，以要求目前向 RPC 端點對應程式註冊的所有端點。 PortQry 會將此查詢傳送至目的地電腦上的 UDP 連接埠 135。
- 根據回應，PortQry 會採取下列其中一個動作：
  - 如果 PortQry 收到此查詢的回應，PortQry 會將整個回應傳回給使用者，並報告埠正在 **接聽**。
  - 如果 PortQry 未收到此查詢的回應，則會報告埠已 **篩選**。

輸出

```
UDP port 135 (epmap service): LISTENING or FILTERED
Querying Endpoint Mapper Database...
Server's response:

UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076
ncacn_ip_tcp:169.254.12.191[4144]

UUID: ecec0d70-a603-11d0-96b1-00a0c91ece30 NTDS Backup Interface
ncacn_np:\\MYSERVER[\PIPE\lsass]

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2 MS NT Directory DRS Interface
ncacn_ip_tcp:169.254.12.191[1030]

UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2 MS NT Directory DRS Interface
ncadg_ip_udp:169.254.12.191[1032]

UUID: 12345678-1234-abcd-ef00-01234567cffb
```

```
ncacn_np:\\MYSERVER[\PIPE\lsass]

UUID: 12345678-1234-abcd-ef00-01234567cffb
ncacn_np:\\MYSERVER[\PIPE\POLICYAGENT]

Total endpoints found: 6

==== End of RPC Endpoint Mapper query response ====

UDP port 135 is LISTENING
```

從此輸出中，您不僅可以判斷服務是否正在埠上接聽，還可以判斷哪些服務或程式已向目的地計算機上的 RPC 端點對應程式資料庫註冊。 輸出包括每個程式的通用唯一標識碼 (UUID) 、標註名稱 (如果有) 、每個程式使用的通訊協定、程式所系結的網路位址，以及以方括弧括住程式的端點。

> **注意**
>
> 當您在 PortQry 命令中指定 `-r` 選項來掃描埠範圍時，PortQry 不會查詢 RPC 端點對應程式以取得端點資訊。 此參數可加速掃描埠範圍。

意見反應

此頁面對您有幫助嗎？ Yes No

提供產品意見反應