

Utilisation de l'outil en ligne de commande PortQry

Article • 10/06/2022 • 26 minutes de lecture

S'applique à : Windows 10 : toutes les éditions, Windows 8.1, Windows 8, Windows 7, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003

Résumé

PortQry est un outil en ligne de commande que vous pouvez utiliser pour résoudre les problèmes de connectivité TCP/IP. Cet outil signale l'état des ports TCP et UDP (User Datagram Protocol) cibles sur un ordinateur local ou sur un ordinateur distant. Il fournit également des informations détaillées sur l'utilisation du port de l'ordinateur local.

Étant donné que PortQry est destiné à être utilisé comme outil de résolution des problèmes, les utilisateurs qui l'utilisent pour résoudre un problème particulier doivent avoir une connaissance suffisante de leur environnement informatique.

Vous pouvez utiliser PortQry à partir d'une invite de commandes dans l'un des modes suivants :

- [Mode ligne de commande](#). Vous pouvez utiliser ce mode pour résoudre les problèmes d'ordinateurs locaux ou distants.
- [Mode local](#). Dans ce mode, vous pouvez utiliser plusieurs paramètres destinés à résoudre les problèmes de l'ordinateur local.
- [Mode interactif](#). Similaire au mode de ligne de commande, mais vous pouvez utiliser des commandes et des paramètres de raccourci.

ⓘ Notes

Vous pouvez télécharger un outil distinct, appelé PortQryUI, qui inclut une interface utilisateur graphique pour PortQry. PortQryUI dispose de plusieurs fonctionnalités qui peuvent faciliter l'utilisation de PortQry. Pour obtenir l'outil PortQryUI, consultez [PortQryUI - User Interface for the PortQry Command Line Port Scanner](#) .

Tests et résultats PortQry

Les outils d'analyse de port classiques indiquent que le port a l'état **LISTENING** si le port UDP cible ne retourne pas de message « Destination inaccessible » du protocole ICMP (Internet Control Message Protocol). Ce résultat peut ne pas être exact pour l'une ou les deux raisons suivantes :

- S'il n'existe aucune réponse à un datagramme dirigé, le port cible peut être **FILTRÉ**.
- La plupart des services ne répondent pas à un datagramme utilisateur non mis en forme qui leur est envoyé. En règle générale, le service ou le programme qui écoute un port répond uniquement à un message qui utilise une couche de session ou un protocole de couche d'application spécifique.

Pour produire des résultats plus précis et utiles, PortQry utilise un processus de test en deux étapes.

Étape 1 : Test d'état du port

PortQry signale l'état d'un port comme l'une des trois valeurs suivantes :

- **ÉCOUTE** : cette réponse indique qu'un processus écoute sur le port cible. PortQry a reçu une réponse du port cible.
- **NOT LISTENING** : cette réponse indique qu'aucun processus n'écoute sur le port cible. PortQry a reçu l'un des messages ICMP suivants du port cible :

Port inaccessible de destination inaccessible

- **FILTRÉ** : cette réponse indique que le port cible est filtré. PortQry n'a pas reçu de réponse du port cible. Un processus peut ou non être à l'écoute sur le port cible. Par défaut, PortQry interroge un port TCP trois fois avant de retourner une réponse de **FILTERED** et interroge un port UDP une fois avant de retourner une réponse de **FILTERED**.

Étape 2 : Tests spécialisés

S'il n'y a aucune réponse d'un port UDP cible, PortQry signale que le port est **LISTENING** ou **FILTERED**. Toutefois, lorsque vous résolvez un problème de connectivité, il est utile de savoir si un port est filtré ou écoute. Cela est particulièrement vrai dans un environnement qui contient un ou plusieurs pare-feu.

PortQry affine son rapport d'état de port à l'aide d'un deuxième ensemble de tests qui peuvent interagir avec le service ou le programme qui écoute sur le port cible. Pour ce test, PortQry effectue les opérations suivantes :

- PortQry utilise le fichier Services qui se trouve dans le dossier `%SYSTEMROOT%\System32\Drivers\Etc` pour déterminer quel service écoute sur chaque port.
- PortQry crée un message spécifiquement construit pour le service ou le programme attendu, puis envoie ce message au port cible. Selon le service ou le programme, le message peut demander des informations utiles pour la résolution des problèmes, telles que les suivantes :
 - Informations sur le domaine et le contrôleur de domaine (requêtes LDAP)
 - Ports et services clients inscrits (requêtes RPC)
 - Indique si l'accès anonyme est autorisé (requêtes FTP)
 - Adresse MAC (requêtes NetBIOS)
 - MspcInt.ini informations sur le fichier (requêtes isa server)
- PortQry analyse, met en forme, puis retourne la réponse du service ou du programme dans le cadre de son rapport de test.

Tests supplémentaires pour résoudre les problèmes de l'ordinateur local

Lorsque vous devez résoudre les problèmes liés aux ports sur l'ordinateur sur lequel vous avez installé PortQry, utilisez PortQry en mode local. Lorsque vous utilisez les paramètres en mode local sur la ligne de commande, vous pouvez effectuer des tâches telles que les suivantes sur l'ordinateur local :

- Énumérer les mappages de ports
- Surveiller un port spécifique pour détecter les modifications
- Surveiller un processus spécifique pour les modifications

Pour plus d'informations, consultez [Utilisation de PortQry en mode local \(ligne de commande\)](#).

Utilisation de PortQry en mode ligne de commande

Vous pouvez exécuter PortQry à une invite de commandes de la même manière que n'importe quel autre outil en ligne de commande. La plupart des exemples de cet article montrent des commandes PortQry en ligne de commande. En mode ligne de commande, vous pouvez ajouter plusieurs options à la chaîne de commande pour spécifier la requête à exécuter et comment l'exécuter. Pour exécuter PortQry en mode ligne de commande, exécutez une commande qui utilise la syntaxe suivante :

Console

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

📌 Notes

Dans cette commande, *<name_to_query>* il s'agit de l'adresse IP, du nom de l'ordinateur ou du domaine à interroger. Ce paramètre est obligatoire. *[options]* sont les paramètres facultatifs.

Paramètres PortQry pour le mode de ligne de commande

Les paramètres suivants sont disponibles en mode de ligne de commande standard :

Paramètre	Description	Commentaires
-n <name>	Interroger la destination spécifique	- Il s'agit du seul paramètre requis pour le mode de ligne de commande. - La <i><name></i> valeur représente le nom ou l'adresse IP de l'ordinateur à interroger. Cette valeur ne peut pas inclure d'espaces.
-p <protocol>	Utiliser le protocole spécifié	- La <i><protocol></i> valeur représente le type de port à interroger (les valeurs possibles sont <code>tcp</code>, <code>udp</code> ou <code>both</code>). - La valeur par défaut est <code>tcp</code>.
-e <port_number>	Spécifier le port cible (également appelé « point de terminaison »)	- La <i><port_number></i> valeur représente le port à interroger sur l'ordinateur de destination. - La valeur par défaut est <code>80</code>.
-o <port_number>, <port_number>	Spécifier plusieurs ports cibles dans une séquence	Les <i><port_number></i> valeurs <i><port_number></i> représentent la liste délimitée par des virgules des numéros de port à interroger dans une séquence. N'utilisez pas d'espaces autour des virgules.

Paramètre	Description	Commentaires
-r <port_number>: <port_number>	Spécifier une plage de ports cibles	- Les <port_number> valeurs :<port_number> représentent les numéros de port de début et de fin, séparés par un signe deux-points. N'utilisez pas d'espaces autour du colon. - Le numéro de port de départ doit être inférieur au numéro de port de fin.
-l <filename.txt>	Générer un fichier journal	- La <filename.txt> valeur représente le nom et l'extension du fichier journal. Cette valeur ne peut pas inclure d'espaces. - Lorsque la commande s'exécute, PortQry crée le fichier journal dans le répertoire où il est installé. - Si le fichier existe déjà, PortQry vous demande de confirmer que vous souhaitez le remplacer (sauf si vous utilisez également le -y paramètre).
-y	Remplacer le fichier journal précédent	- Lorsque vous l'utilisez -y conjointement, -l PortQry remplace le fichier journal existant sans vous inviter à confirmer l'action. - Si la chaîne de commande PortQry n'inclut -l pas, PortQry ignore -y.
-sl	Attendre plus de temps pour la réponse (également appelé retard de liaison lente)	Utilisez ce paramètre pour doubler le temps pendant lequel PortQry attend une réponse à partir d'un port UDP avant que PortQry ne détermine que le port n'écoute pas ou qu'il est FILTRÉ. Lorsque vous interrogez des liens réseau lents ou non fiables, le temps d'attente normal peut être trop court pour recevoir une réponse.
-nr	Ignorer la recherche de nom inverse	- Par défaut, lorsque vous utilisez -n pour spécifier une adresse IP pour l'ordinateur cible, PortQry effectue une recherche de nom inverse pour résoudre l'adresse IP en nom. Ce processus peut prendre du temps, en particulier si PortQry ne peut pas résoudre l'adresse IP. Permet -nr d'ignorer cette étape de la requête. - Si vous utilisez -n pour spécifier un ordinateur ou un nom de domaine, PortQry ignore -nr.

Paramètre	Description	Commentaires
-sp <port_number>	Interroger à partir d'un port source spécifique	- La <port_number> valeur représente le port utilisé par PortQry pour envoyer la requête. - PortQry ne peut pas utiliser un port qu'un autre processus utilise déjà. Si le port que vous spécifiez est déjà utilisé, PortQry retourne le message d'erreur suivant : Impossible d'utiliser le port source spécifié. Le port est déjà utilisé. Spécifiez un port qui n'est pas utilisé et réexécutez la commande. - Dans les cas suivants, PortQry utilise le port spécifié pour le premier test de la requête, mais pas le deuxième test : - RPC (ports TCP et UDP 135) - LDAP (port UDP 389) - Requête d'état de l'adaptateur NetBIOS (port UDP 137) Dans ces cas, PortQry utilise un port éphémère pour le deuxième test. Lorsque cela se produit, PortQry enregistre « Utilisation du port source éphémère » dans sa sortie. - Si l'ordinateur sur lequel PortQry est installé exécute également l'agent de stratégie IPSec, le port UDP 500 peut ne pas être disponible pour être utilisé comme port source. Pour désactiver temporairement l'agent de stratégie IPSec afin de pouvoir utiliser le port 500, exécutez <code>net stop PolicyAgent</code>. Une fois le test terminé, exécutez <code>net start PolicyAgent</code>.
-cn ! <community_name>!	Interroger une communauté SMTP	- La <community_name> valeur représente le nom de la communauté SNMP à interroger. Vous devez délimiter cette valeur à l'aide de points d'exclamation, comme indiqué dans la colonne de gauche. - Si le service SNMP n'écoute pas sur le port cible, PortQry ignore -cn. - Le nom de la communauté par défaut est <code>public</code>.

Paramètre	Description	Commentaires
-q	Exécuter PortQry en mode silencieux	- Lorsque vous utilisez -q, PortQry supprime toutes les sorties d'écran, à l'exception des messages d'erreur. - Pour afficher la sortie autre que les messages d'erreur, utilisez -q avec -l. PortQry enregistre la sortie normale dans le fichier journal. - Si un fichier journal existe déjà et que vous l'utilisez -q conjointement -l, PortQry remplace le fichier journal existant sans vous y inviter. - Vous ne pouvez pas utiliser -q avec -o, -r ou -p both. - Ce paramètre est particulièrement utile lorsque vous utilisez un fichier batch pour exécuter une chaîne de commande PortQry.

Remarques relatives aux paramètres en mode de ligne de commande

- Toute valeur de numéro de port doit être un numéro de port valide compris entre 1 et 65535, inclus.
- Le -e, -o et -r les paramètres s'excluent mutuellement. Une seule commande PortQry ne peut utiliser qu'un seul de ces paramètres.
- Une requête vers le port UDP 389 (LDAP) peut ne pas fonctionner sur les contrôleurs de domaine qui exécutent Windows Server 2008. Pour vérifier la disponibilité du service qui s'exécute sur le port UDP 389, vous pouvez utiliser Nltest au lieu de PortQry. Pour plus d'informations, consultez [Nltest](#).
- Lorsque vous interrogez le port 135 (RPC) à l'aide -e ou -o, PortQry retourne tous les points de terminaison actuellement inscrits auprès du mappeur de point de terminaison RPC.

Important

Lorsque vous utilisez le -r, PortQry n'interroge pas le mappeur de point de terminaison RPC.

- Lorsque vous interrogez le port 53 (DNS), PortQry envoie une requête DNS à portqry.microsoft.com l'aide de TCP et UDP. Si le serveur retourne une réponse, PortQry détermine que le port est LISTENING.

Notes

Il n'est pas important que le serveur DNS retourne une réponse positive ou négative. Toute réponse indique que le port écoute.

Utilisation de PortQry en mode local (ligne de commande)

Au lieu d'interroger un port sur un ordinateur cible distant, vous pouvez utiliser PortQry en mode local pour obtenir des informations détaillées sur les ports TCP et les ports UDP sur l'ordinateur local sur lequel PortQry s'exécute. Utilisez la syntaxe suivante pour exécuter PortQry en mode local :

Console

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

Les espaces réservés de cette syntaxe sont expliqués dans le tableau suivant des paramètres de mode local :

Paramètre	Description	Commentaires
-local	Récupérer des informations locales	- Énumérez tous les mappages de ports TCP et UDP actuellement actifs sur l'ordinateur local. Cette sortie est similaire à la sortie générée par la <code>netstat.exe -an</code> commande. - Sur les ordinateurs qui prennent en charge les mappages piD-à-port, la sortie inclut le PID du processus qui utilise le port sur l'ordinateur local. Si vous utilisez l'option détaillée (-v), la sortie inclut également les noms des services auxquels le PID appartient et répertorie tous les modules chargés par le processus. Vous pouvez utiliser ces informations pour déterminer les ports associés à un programme ou un service particulier qui s'exécute sur l'ordinateur.

Paramètre	Description	Commentaires
-wport <port_number>	Port d'espion	- Surveillez les modifications apportées à un port spécifique. La <port_number> valeur représente le port à surveiller. - Dans le cas d'un port TCP, PortQry signale les modifications entre les états suivants : - CLOSE_WAIT - FERMÉ - ÉTABLI - FIN_WAIT_1 - LAST_ACK - ECOUTE - SYN_RECEIVED - SYN_SEND - TIMED_WAIT - Pour les ports UDP, PortQry indique si un programme est lié au port, mais il ne signale pas si le port UDP reçoit des datagrammes. - Pour arrêter la surveillance, appuyez sur Échap.
-wpid <pid>	ID de processus de surveillance (PID)	- Surveillez un PID spécifique pour détecter les modifications apportées au nombre et à l'état des connexions. La <process_number> valeur représente le PID à surveiller. - Pour arrêter la surveillance, appuyez sur Échap.
-wt <seconds>	Vérifier à un intervalle spécifique	- Vérifiez l'état de la cible identifiée par -wport ou "-wpid à l'intervalle représenté par la valeur /<secondes>. - La <seconds> valeur doit être comprise entre un et 1 200 (inclus). - La valeur par défaut est 60. - Vous ne pouvez pas utiliser -wt seul ou avec -local.
-l <filename.txt>	Générer un fichier journal	- La <filename.txt> valeur représente le nom et l'extension du fichier journal. Cette valeur ne peut pas inclure d'espaces. - Lorsque la commande s'exécute, PortQry crée le fichier journal dans le répertoire où il est installé. - Si le fichier existe déjà, PortQry vous demande de confirmer que vous souhaitez le remplacer (sauf si vous utilisez également le -y paramètre).

Paramètre	Description	Commentaires
-y	Remplacer le fichier journal précédent	- Lorsque vous l'utilisez -y conjointement, -l PortQry remplace le fichier journal existant sans vous inviter à confirmer l'action. - Si la chaîne de commande PortQry n'inclut -l pas, PortQry ignore -y.
-v	Produire une sortie détaillée	PortQry fournit des détails supplémentaires sur la sortie de l'écran (et sur le fichier journal, s'il est utilisé).

Remarques pour les paramètres en mode local

- Le -local, -wport et -wpid les paramètres s'excluent mutuellement. Vous ne pouvez utiliser qu'un seul de ces paramètres dans une seule chaîne de commande PortQry.
- Le -q paramètre ne fonctionne pas en mode local.
- Dans certains cas, PortQry peut signaler que le processus d'inactivité système (PID 0) utilise certains ports TCP. Ce comportement peut se produire si un programme local se connecte à un port TCP, puis s'arrête. Même si le programme n'est plus en cours d'exécution, la connexion TCP du programme au port peut rester dans un état « Attente chronométrée » pendant plusieurs minutes. Dans ce cas, PortQry peut détecter que le port est en service, mais il ne peut pas identifier le programme qui utilise le port, car le PID a été libéré. Par défaut, le port reste dans un état « Attente chronométrée » deux fois plus longtemps que la durée de vie maximale du segment.
- Pour chaque processus, PortQry fournit autant d'informations que possible. L'accès à certaines informations est restreint. Par exemple, l'accès aux informations de module pour les processus Inactif et CSRSS est interdit, car leurs restrictions d'accès empêchent le code au niveau de l'utilisateur de les ouvrir. Pour de meilleurs résultats, exécutez la commande en mode local dans le contexte de l'administrateur local ou d'un compte qui a des informations d'identification similaires.
- Lorsque vous utilisez l'une -wport ou l'autre -l de ces fonctionnalités, -wpid utilisez la touche Échap pour interrompre et quitter PortQry au lieu de Ctrl+C. Vous devez appuyer sur Échap pour vous assurer que PortQry ferme correctement le fichier journal et se ferme. Si vous appuyez sur Ctrl+C au lieu d'Échap pour arrêter PortQry, le fichier journal peut devenir vide ou endommagé.

Utilisation de PortQry en mode interactif

Lorsque vous résolvez des problèmes de connectivité entre les ordinateurs, vous devrez peut-être taper de nombreuses commandes répétitives. De telles actions peuvent être effectuées plus facilement à l'aide de PortQry en mode interactif.

Le mode interactif est similaire à la fonctionnalité interactive dans l'utilitaire DNS [Nslookup](#) ou dans l'utilitaire NBlookup WINS.

Pour démarrer PortQry en mode interactif, utilisez le `-i` paramètre. Par exemple, exécutez la commande suivante :

Console

```
portqry -i
```

La sortie de cette commande ressemble à l'extrait suivant :

Sortie

```
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)
>
```

Commandes en mode interactif

Vous pouvez utiliser les commandes suivantes en mode interactif :

Command	Description	Commentaires
node <name> ou n <name>	Définir la destination à interroger	- La <name> valeur représente le nom ou l'adresse IP de l'ordinateur à interroger. Cette valeur ne peut pas inclure d'espaces. - La valeur par défaut est 127.0.0.1 (l'ordinateur local).

Command	Description	Commentaires
query ou q	Envoyer une requête	- Interroge la destination actuelle à l'aide des paramètres actuels. - Le protocole par défaut est tcp. - Le port de destination par défaut est le port TCP 80. - Le port source par défaut est le port 0 (un port éphémère). - Vous pouvez utiliser l'un des raccourcis suivants avec la query commande pour exécuter l'une des requêtes courantes. Pour obtenir la liste des raccourcis disponibles, consultez les raccourcis de requête en mode interactif.
set <option>=<value>	Définir la valeur d'une option de requête	- Dans cette commande, <option> représente le nom de l'option à définir et <value> représente la nouvelle valeur de l'option. - Pour afficher la liste des valeurs actuelles des options disponibles, entrez set all. - Pour obtenir la liste des options disponibles, consultez Options de mode interactif.
exit	Quitter le mode interactif	

Raccourcis de requête en mode interactif

Vous pouvez utiliser les raccourcis suivants avec la query commande pour exécuter des requêtes courantes sans avoir à définir les options de port et de protocole. Utilisez la syntaxe suivante :

Console
q <shortcut>

ⓘ Notes

Dans cette commande, <shortcut> représente l'un des raccourcis du tableau suivant. Si vous omettez le raccourci, la commande interroge le q port TCP 80.

Raccourci	Ports à interroger
dns	Port TCP 53, port UDP 53.

Raccourci	Ports à interroger
ftp	Port TCP 21
imap	Port TCP 143
ipsec	Port UDP 500
isa	Port TCP 1745, port UDP 1745
ldap	Port TCP 389, port UDP 389
l2tp	Port UDP 1701
mail	Ports TCP 25, 110 et 143
pop3	Port TCP 110
rpc	Port TCP 135, port UDP 135
smtp	Port TCP 25
snmp	Port UDP 161
sql	Port TCP 1433, port UDP 1434
tftp	Port UDP 69

Par exemple, l'entrée `q dns` en mode interactif équivaut à l'exécution `portqry -n 127.0.0.1 -p both -e 135` en mode de ligne de commande standard.

Options de mode interactif

Vous pouvez utiliser la `set` commande pour définir des options telles que le port source ou le retard de liaison lente. Utilisez la syntaxe suivante :

Console

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

📌 Notes

Dans cette commande, *<option>* représente le nom de l'option à définir et *<value>* représente la nouvelle valeur de l'option.

Option	Description	Commentaires
<code>set all</code>	Afficher les valeurs actuelles des options	
<code>set port=<port_number></code> <code>set e=<port_number></code>	Spécifier le port cible	La <i><port_number></i> valeur représente le port à interroger sur l'ordinateur de destination.
<code>set sport=<port_number></code> <code>set sp=<port_number></code>	Spécifier le port source	- La <i><port_number></i> valeur représente le port utilisé par PortQry pour envoyer la requête. - PortQry ne peut pas utiliser un port qu'un autre processus utilise déjà. - Si vous spécifiez un numéro de port égal à zéro, PortQry utilise un port éphémère.
<code>set protocol=<protocol></code> <code>set p=<protocol></code>	Spécifier le protocole à utiliser	La <i><protocol></i> valeur représente le type de port à interroger (tcp, udp ou both).
<code>set cn=<community_name></code>	Spécifier une communauté SMTP	- La <i><community_name></i> valeur représente le nom de la communauté SNMP à interroger. - Si le service SNMP n'écoute pas sur le port cible, PortQry ignore -cn. - Le nom de la communauté par défaut est <code>public</code>.
<code>set nr</code>	Désactiver ou activer la recherche de noms inversés	- Par défaut, si vous avez défini une adresse IP comme destination de requête, PortQry résout l'adresse IP en nom. Si vous modifiez cette option, PortQry ignore l'étape de résolution de noms. - Pour réactiver la recherche de noms inversés, exécutez <code>set nr</code> une deuxième fois.
<code>set sl</code>	Activer ou désactiver le retard de liaison lente	- Si vous modifiez cette option, PortQry double la durée pendant laquelle il attend une réponse à partir d'un port UDP avant que PortQry détermine que le port n'écoute pas ou qu'il est FILTRÉ. Lorsque vous interrogez des liens réseau lents ou non fiables, le temps d'attente normal peut être trop court pour recevoir une réponse. - Pour désactiver à nouveau le délai de liaison lente, exécutez <code>set sl</code> une deuxième fois.

Supposons que vous souhaitez interroger un ordinateur qui a l'adresse IP 10.0.1.10. À l'invite de commandes en mode interactif, entrez `n 10.0.1.10`. Cette commande produit une sortie qui ressemble à l'extrait suivant :

Sortie
<pre>Default Node: 10.0.1.10 ></pre>

Pour envoyer une requête DNS, entrez `q dns` à l'invite de commandes en mode interactif. Cette commande produit une sortie qui ressemble à l'extrait suivant :

Sortie
<pre>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 ></pre>

Personnalisation de l'association entre les ports et les services

Par défaut, chaque ordinateur basé sur Windows a un fichier Services qui se trouve dans le dossier `%SYSTEMROOT%\System32\Drivers\Etc`. PortQry utilise ce fichier pour résoudre les numéros de port en leurs noms de service correspondants. PortQry utilise ces informations pour sélectionner le format de ses requêtes. Vous pouvez modifier ce fichier pour diriger PortQry afin d'envoyer des messages mis en forme à un autre port. Par exemple, l'entrée suivante s'affiche dans un fichier Services classique :

Sortie
<pre>ldap 389/tcp #Lightweight Directory Access Protocol</pre>

Vous pouvez modifier cette entrée de port ou ajouter une entrée supplémentaire. Pour forcer PortQry à envoyer des requêtes LDAP au port 1025, modifiez l'entrée comme suit :

Sortie		
ldap Access Protocol	1025/tcp	#Lightweight Directory

Exemples

Les exemples suivants montrent comment utiliser PortQry et ses paramètres :

Mode local

- [Interroger l'ordinateur local](#)
- [Interroger l'ordinateur local lorsque l'accès peut être restreint](#)
- [Surveiller un ID de processus à l'aide d'un intervalle spécifique](#)
- [Interroger sur un lien lent](#)

Mode ligne de commande

- [Spécifier une cible et un protocole](#)
- [Spécifier un ou plusieurs ports cibles](#)
- [Spécifier un fichier journal pour la sortie PortQry](#)
- [Utiliser un fichier batch pour exécuter PortQry en mode silencieux](#)
- [Port de requête 135 \(service RPC\)](#)

Interroger l'ordinateur local

La sortie ressemble `portqry -local` à l'extrait suivant :

Sortie	
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	

Interroger l'ordinateur local lorsque l'accès peut être restreint

Lorsque vous exécutez PortQry en mode local, comme dans l'exemple précédent, vous pouvez voir une sortie qui ressemble à l'extrait suivant. Cette sortie indique que le contexte de sécurité utilisé par PortQry ne dispose pas des autorisations suffisantes pour accéder à toutes les informations demandées.

Sortie

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

=====

Surveiller un ID de processus à l'aide d'un intervalle spécifique

La commande suivante surveille un processus spécifique :

Console

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

Par conséquent, PortQry effectue les actions suivantes :

- Identifie le processus qui a le PID 1276 et vérifie l'état des ports qu'il utilise toutes les deux secondes jusqu'à ce que vous appuyiez sur Échap.
- Crée le fichier journal *pid.txt*. Si un fichier ayant ce nom existe déjà, PortQry vous invite à confirmer que vous souhaitez remplacer le fichier.
- Enregistre toute sortie dans le fichier journal, y compris la sortie détaillée supplémentaire.

Le contenu du fichier journal ressemble à l'extrait suivant :

Sortie

```
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)
```

Spécifier une cible et un protocole

① Notes

Chacun des exemples de cette section interroge le port 80, le port par défaut.

La commande suivante interroge le port TCP par défaut sur un ordinateur spécifié à l'aide de son nom de domaine complet (FQDN) :

Console

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

La commande suivante interroge le port UDP par défaut sur un ordinateur spécifié à l'aide de son nom d'ordinateur :

Console

```
portqry -n myServer -p udp
```

La commande suivante interroge les ports TCP et UDP par défaut d'un ordinateur spécifié à l'aide de son adresse IP :

Console

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

La commande suivante exécute la même requête que la commande précédente, mais ignore l'étape de résolution de noms :

Console

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

La commande suivante interroge le port TCP par défaut d'un serveur web :

Console

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

Spécifier un ou plusieurs ports cibles

La commande suivante teste le service SMTP d'un serveur de messagerie en interrogeant le port TCP 25 :

Console

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

La commande suivante interroge le port TCP 60897 et le port UDP 60897 d'un ordinateur qui a l'adresse IP 192.168.1.20 :

Console

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

La commande suivante interroge les ports UDP 139, 1025 et 135 (dans cette séquence) sur l'ordinateur « myServer » :

Console

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

La commande suivante interroge la plage de ports du port 135 au port 139 (inclus) sur l'ordinateur « myServer » :

Console

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

Spécifier un fichier journal pour la sortie PortQry

La commande suivante interroge le port TCP 143 sur mail.widgets.microsoft.com et enregistre la sortie dans le fichier *portqry.txt* . Si le fichier existe déjà, PortQry le remplace sans demander de confirmation.

Console

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

Interroger sur un lien lent

La commande suivante interroge les ports TCP 143, 110 et 25 sur mail.widgets.microsoft.com. Pour chaque port cible, PortQry attend deux fois plus longtemps que d'habitude pour une réponse.

Console

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

Spécifier un port source

La commande suivante utilise le port UDP 3001 (s'il est disponible) sur l'ordinateur local pour envoyer une requête au port UDP 53 sur la version 192.168.1.20. Si un service écoute ce port et répond à la requête, il envoie la réponse au port UDP 3001 sur l'ordinateur local.

Console

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

La commande suivante utilise le port UDP 3000 (s'il est disponible) sur l'ordinateur local pour envoyer une requête au port UDP 389 sur myDomainController.contoso.com. Par défaut, le service LDAP doit être à l'écoute sur ce port. Si le service LDAP répond à la première requête, PortQry utilise un port source éphémère pour envoyer la requête mise en forme et recevoir des réponses.

Console

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

Utiliser un fichier batch pour exécuter PortQry en mode silencieux

Le texte suivant est un exemple de fichier batch qui exécute PortQry en mode silencieux :

Console

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

Lorsque ce fichier de commandes s'exécute, PortQry produit un fichier journal nommé *pqlog.txt*. Le contenu de ce fichier ressemble à ce qui suit :

Sortie

```
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 =====
```

Port de requête 135 (service RPC)

La commande suivante interroge le port UDP 135 sur l'ordinateur myServer. Par défaut, le service RPC doit écouter sur ce port.

Console

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

Par conséquent, PortQry effectue les actions suivantes :

- PortQry utilise le fichier Services dans le dossier `%SYSTEMROOT%\System32\Drivers\Etc` pour résoudre le port UDP 135 en service. À l'aide de la configuration par défaut, PortQry résout le port en service de mappeur de point de terminaison RPC (Epmap).
- PortQry envoie un datagramme utilisateur non mis en forme au port UDP 135 sur l'ordinateur de destination. PortQry ne reçoit pas de réponse du port cible. Cela est dû au fait que le service de mappeur de point de terminaison RPC répond uniquement à une requête RPC correctement mise en forme. PortQry signale que le port est **LISTENING** ou **FILTERED**.
- PortQry crée une requête RPC correctement mise en forme qui demande tous les points de terminaison actuellement inscrits auprès du mappeur de point de terminaison RPC. PortQry envoie cette requête au port UDP 135 sur l'ordinateur de destination.
- En fonction de la réponse, PortQry effectue l'une des actions suivantes :
 - Si PortQry reçoit une réponse à cette requête, PortQry retourne la réponse entière à l'utilisateur et signale que le port est **LISTENING**.
 - Si PortQry ne reçoit pas de réponse à cette requête, il signale que le port est **FILTRÉ**.

Sortie

```
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
```

À partir de cette sortie, vous pouvez déterminer non seulement si le service écoute sur le port, mais également quels services ou programmes sont inscrits auprès de la base de données du mappeur de point de terminaison RPC sur l'ordinateur de destination. La sortie inclut l'identificateur unique universel (UUID) pour chaque programme, le nom annoté (le cas échéant), le protocole utilisé par chaque programme, l'adresse réseau à laquelle le programme est lié et le point de terminaison du programme entre crochets.

📌 Notes

Lorsque vous spécifiez l'option `-r` dans la commande PortQry pour analyser une plage de ports, PortQry n'interroge pas le mappeur de point de terminaison RPC pour obtenir des informations sur le point de terminaison. Ce paramètre accélère l'analyse d'une plage de ports.