Comment utiliser PortQry pour résoudre les problèmes de connectivité Active Directory

Article • 09/11/2021 • 7 minutes de lecture

Cet article explique comment exécuter PortQry pour tester la connectivité réseau pour n'importe quel Windows ou scénario sur n'importe quelle version de Windows.

S'applique à : Windows Server 2012 R2
Numéro de la ko d'origine : 816103

Introduction

PortQry est un utilitaire de ligne de commande que vous pouvez utiliser pour résoudre les problèmes de connectivité TCP/IP utilisés par Windows composants et fonctionnalités. L'utilitaire signale l'état des ports TCP (Transition Control Protocol) et UDP (User Datagram Protocol) sur un ordinateur distant. Vous pouvez exécuter PortQry pour tester la connectivité réseau pour n'importe quel Windows ou scénario sur n'importe quelle version de Windows.

Cet article explique comment utiliser portqry pour vérifier la connectivité TCP/IP de base pour les composants liés à Active Directory et Active Directory, notamment :

- Services de domaine Active Directory (ADDS)
- Active Directory for Lightweight Directory Access Protocol (LDAP)
- Appel de procédure distante (RPC)
- Domain Name Service (DNS)
- Autres composants liés à ADDS
- Autres composants dépendants d'ADDS

La vérification de la connectivité réseau sur les ports et protocoles requis est particulièrement utile lorsque des contrôleurs de domaine sont déployés sur des périphériques intermédiaires, y compris des pare-feu.

Installer PortQry

Télécharger Portqry.exe

PortQry .exe est disponible en téléchargement à partir du Centre de téléchargement Microsoft. Pour télécharger le .exe PortQry, visitez le site Web Microsoft suivant :

Télécharger PortQry Command Line Port Scanner Version 2.0

Pour plus d'informations sur le téléchargement des fichiers du support Microsoft, voir la Base de connaissances Microsoft :

119591 obtenir des fichiers de support Microsoft à partir de Online Services

Microsoft a analysé ce fichier à la recherche de virus. Microsoft a utilisé le logiciel de détection de virus le plus actuel disponible à la date de la date de la mise en ligne du fichier. Le fichier est stocké sur des serveurs à sécurité améliorée qui permettent d'empêcher toute modification non autorisée du fichier.

Une version graphique de l'outil PortQry, appelée PortQueryUI, contient des fonctionnalités supplémentaires qui facilitent l'utilisation de PortQry. Pour télécharger l'outil PortQueryUI, visitez le site Web Microsoft suivant :

Télécharger PortQryUI - Interface utilisateur pour l'analyseur de port de ligne de commande PortQry

Plus d'informations

PortQry signale l'état d'un port de trois manières :

- Écoute : un processus est à l'écoute sur le port cible sur le système cible. PortQry a reçu une réponse du port.
- Non à l'écoute : aucun processus n'est à l'écoute sur le port cible sur le système cible. PortQry a reçu un message ICMP (Internet Control Message Protocol) « Destination Unreachable - Port Unreachable » du port UDP cible. Ou, si le port cible est un port TCP, Portqry a reçu un paquet d'accusé de réception TCP avec l'indicateur Réinitialiser.
- Filtré : le port cible sur le système cible est en cours de filtrage. PortQry n'a pas reçu de réponse du port cible. Un processus peut être à l'écoute ou non sur le port. Par défaut, les ports TCP sont interrogés trois fois et les ports UDP sont interrogés une fois avant de signaler que le port cible est filtré.

Avec PortQry, vous pouvez également interroger un service LDAP. Il envoie une requête LDAP, à l'aide de LDP ou TCP, et interprète la réponse du serveur LDAP à la requête. La réponse du serveur LDAP est l'une des réponses, mise en forme et renvoyée à l'utilisateur.

Les interfaces RPC proposées par Active Directory peuvent utiliser des ports de serveur dynamiques (la plupart sont configurables).) Les clients utilisent le mappeur de point de terminaison RPC pour rechercher le port serveur de l'interface RPC d'un service Active Directory spécifique.

La base de données de mapper de point de fin RPC écoute le port 135. Cela signifie que le port TCP 135 est un port requis pour la plupart des déploiements qui vont au-delà des requêtes LDAP de base. Elle est également requise pour tous les clients membres d'un domaine.

Pour plus d'informations sur PortQry, voir :

310099 description de l'utilitaire Portqry.exe ligne de commande

Vous trouverez une liste des ports et protocoles qu'Windows utilise, notamment Active Directory, DFS, DFSR, les services de certificats et tous les autres services dans l'article suivant de la base de connaissances :

vue d'832017 service et conditions requises pour les ports réseau pour Windows

> **Notes**
>
> Active Directory et d'autres services qui utilisent des ports éphémères doivent avoir une connectivité entre le port 135 et toutes les conditions répertoriées dans la vue d'ensemble du service et les exigences relatives aux ports réseau pour Windows article.

Vous pouvez également trouver des ports et des protocoles spécifiques à AD dans l'article :

179442 configurer un pare-feu pour les domaines et les trusts

PortQry sait comment envoyer une requête au mappeur de point de fin RPC (à l'aide d'UDP et de TCP) et interpréter la réponse. Cette requête affiche tous les points de fin enregistrés avec le mappeur de point de fin RPC. La réponse du point de fin du mappeur est l'une des réponses, mise en forme et renvoyée à l'utilisateur.

Si PortQry n'est pas disponible, vous pouvez utiliser LDP.EXE pour vous connecter au contrôleur de domaine sur le port 389 avec la case à cocher **Connectionless** activée.

Une autre alternative à PortQry est NLTEST, mais elle ne fonctionne pas pour les serveurs arbitraires. Le serveur doit être un contrôleur de domaine dans le même domaine que l'ordinateur sur qui vous exécutez l'outil. Si tel est le cas, vous pouvez utiliser Nltest /sc_reset pour forcer un canal de sécurité **<domain name>** \ **<computer**

name> sur un contrôleur de domaine spécifique. Pour plus d'informations, voir Connectivité réseau.

Utilisation de portqry

Exemple 1 : utilisation de Portqry pour tester la connectivité sur un port et un protocole spécifiques à l'aide du port UDP 389 comme exemple

Cet exemple montre comment utiliser PortQry pour déterminer si le service LDAP répond. En examinant la réponse, vous pouvez déterminer le service LDAP à l'écoute sur le port et obtenir des détails sur sa configuration. Ces informations peuvent être utiles pour résoudre divers problèmes.

Par défaut, LDAP est configuré pour écouter le port 389. L'exemple d'appel spécifie le serveur à interroger à l'aide du protocole UDP :

```
PortQry -n <fqdn> -p udp -e 389
```

PortQry résout automatiquement le port UDP 389 à l'aide du fichier %SystemRoot%\System32\Drivers ...\Services inclus dans Windows Server 2003 et les ordinateurs \ ultérieurs. Dans l'exemple de sortie ci-dessous, le port est résolu en un service LDAP actif et PortQry signale que le port est à l'écoute ou FILtré.

PortQry envoie ensuite une requête LDAP mise en forme à laquelle il reçoit une réponse. Elle renvoie la réponse entière à l'utilisateur et signale que le port est LISTENING. Si PortQry ne reçoit pas de réponse à la requête, il signale que le port est FILTRÉ.

Sortie d'exemple

> C : \>portqry -n <*fqdn*> -e 389 -p udp
>
> Système cible d'interrogation appelé :
>
> <*fqdn*>
>
> Tentative de résolution du nom en adresse IP...
>
> Nom résolu en 169.254.0.14
>
> Port UDP 389 (service inconnu) : ÉCOUTE ou FILTRAGE

Envoi d'une requête LDAP au port UDP 389...

Réponse de requête LDAP :

currentdate: <*DateTime*> (GMT non ajustée)
subschemaSubentry :
CN=Aggregate,CN=Schema,CN=Configuration,DC=reskit,DC=com
dsServiceName: CN=NTDS
Paramètres,CN=mydc,CN=Servers,CN=eu,CN=Sites,CN
=Configuration,DC=reskit,DC=com
namingContexts: DC=reskit,DC=com
defaultNamingContext: DC=reskit,DC=com
schemaNamingContext :
CN=Schema,CN=Configuration,DC=reskit,DC=com
configurationNamingContext :
CN=Configuration,DC=reskit,DC=com
rootDomainNamingContext: DC=reskit,DC=com
supportedControl : 1.2.840.113556.1.4.319
supportedLDAPVersion: 3
supportedLDAPPolicies : MaxPoolThreads
highestCommittedUSN: 815431405
supportedSASLMechanisms : GSSAPI
dnsHostName : <*HostName*>
ldapServiceName : <*ServiceName*>
serverName :
CN=MYDC,CN=Servers,CN=EU,CN=Sites,CN=Configuration,DC=reskit,DC=com
supportedCapabilities: 1.2.840.113556.1.4.800
isSynchronized: TRUE
isGlobalCatalogReady: TRUE

======== Fin de la réponse de requête LDAP ========
Le port UDP 389 est À L'ÉCOUTE

Notes

Le test LDAP sur UDP peut ne pas fonctionner avec les contrôleurs de domaine qui exécutent Windows Server 2008 et ultérieures. Cela peut être dû au fait que vous avez désactivé IPv6 sur le contrôleur de domaine. Pour activer IPv6, définissez la valeur abordée dans l'article ci-dessous sur la valeur par défaut **de 0**:
929852 recommandations pour la configuration d'IPv6 dans Windows pour les utilisateurs avancés

Exemple 2 : identification des services inscrits auprès du mappeur de point de terminaison RPC

Cet exemple montre comment utiliser PortQry pour déterminer quels services ou applications sont enregistrés avec la base de données de point de fin RPC du serveur cible. Le résultat inclut l'ID UUID (Universally Unique Identifier) de chaque application, le nom annoté (le cas présent), le protocole utilisé par l'application, l'adresse réseau à qui l'application est liée et le point de fin de l'application (numéro de port, canal nommé entre crochets). Ces informations peuvent être utiles pour résoudre divers problèmes.

Par défaut, la base de données de mapper de point de fin RPC est configurée pour écouter le port 135. L'exemple d'appel spécifie le serveur à interroger à l'aide du protocole UDP :

```
portqry -n <fqdn> -p udp -e 135
```

Sortie d'exemple

> Système cible d'interrogation appelé :
>
> *<fqdn>*
>
> Tentative de résolution du nom en adresse IP...
>
> Nom résolu en 169.254.0.18
>
> Port UDP 135 (service epmap) : ÉCOUTE ou FILTRAGE
> Interrogation de la base de données Depper du point de terminaison...
> Réponse du serveur :
>
> UUID : ecec0d70-a603-11d0-96b1-00a0c91ece30 NTDS Backup Interface
> ncacn_np : \ \ \ \MYDC[\ PIPE \ lsass]
>
> UUID : 16e0cf3a-a604-11d0-96b1-00a0c91ece30 NTDS Restore Interface
> ncacn_np : \ \ \ \MYDC[\ PIPE \ lsass]
>
> UUID : e3514235-4b06-11d1-ab04-00c04fc2dcd2 Interface DRS du répertoire MS NT
> ncacn_ip_tcp:169.254.0.18[1027]
>
> UUID : f5cc59b4-4264-101a-8c59-08002b2f8426 NtFrs Service
> ncacn_ip_tcp:169.254.0.18[1130]

> UUID : d049b186-814f-11d1-9a3c-00c04fc9b232 API NtFrs
> ncacn_ip_tcp:169.254.0.18[1130]
>
> UUID : d049b186-814f-11d1-9a3c-00c04fc9b232 API NtFrs
> ncacn_np : \ \ \ \MYDC[\ pipe \ 00000580.000]
>
> Nombre total de points de terminaison trouvés : 6
>
> ==== Fin de la réponse de requête Depper de point de terminaison RPC ====
>
> Le port UDP 135 est À L'ÉCOUTE

PortQry peut envoyer une requête DNS correctement formatée (à l'aide d'UDP ou de TCP). L'utilitaire envoie une requête DNS pour « `portqry.microsoft.com .` » PortQry attend ensuite une réponse du serveur DNS cible. Le fait que la réponse DNS à la requête soit négative ou positive n'est pas pertinent, car toute réponse indique que le port est à l'écoute.