Microsoft Ignite

Nov 19–22, 2024

Register now ›

Discover ⌄   Product documentation ⌄   Development languages ⌄   Topics ⌄   Sign in

ⓘ We're no longer updating this content regularly. Check the **Microsoft Product Lifecycle** for information about how this product, service, technology, or API is supported.

Recommended Version

Filter by title

Rpcping

Article • 08/31/2016

In this article

Syntax

Parameters

Examples

Additional references

Applies To: Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows 8

Confirms the RPC connectivity between the computer running Microsoft Exchange Server and any of the supported Microsoft Exchange Client workstations on the network. This utility can be used to check if the Microsoft Exchange Server services are responding to RPC requests from the client workstations via the network. For examples of how this command can be used, see Examples ⌗ .

Syntax

☐ Copy

```
rpcping [/t <protseq>] [/s <server_addr>] [/e <endpoint>
        |/f <interface UUID>[,MajorVer]] [/O <Interface Object UUID]
        [/i <#_iterations>] [/u <security_package_id>] [/a <authn_level>]
        [/N <server_princ_name>] [/I <auth_identity>] [/C <capabilities>]
        [/T <identity_tracking>] [/M <impersonation_type>]
        [/S <server_sid>] [/P <proxy_auth_identity>] [/F <RPCHTTP_flags>]
        [/H <RPC/HTTP_authn_schemes>] [/o <binding_options>]
        [/B <server_certificate_subject>] [/b] [/E] [/q] [/c]
        [/A <http_proxy_auth_identity>] [/U <HTTP_proxy_authn_schemes>]
        [/r <report_results_interval>] [/v <verbose_level>] [/d]
```

Parameters

⛶ Expand table

Parameter	Description

'

Time

Timeout

Title

Option	Description
/t <protseq>	Specifies the protocol sequence to use. Can be one of the standard RPC protocol sequences, for example: ncacn_ip_tcp, ncacn_np, or ncacn_http. If not specified, default is ncacn_ip_tcp.
/s <server_addr>	Specifies the server address. If not specified, the local machine will be pinged.
/e <endpoint>	Specifies the endpoint to ping. If none is specified, the endpoint mapper on the target machine will be pinged. This option is mutually exclusive with the interface (/f) option.
/o <binding_options>	Specifies the binding options for the RPC ping.
/f <interface UUID> [,MajorVer]	Specifies the interface to ping. This option is mutually exclusive with the endpoint option. The interface is specified as a UUID. If the *MajorVer* is not specified, version 1 of the interface will be sought. When interface is specified, **rpcping** will query the endpoint mapper on the target machine to retrieve the endpoint for the specified interface. The endpoint mapper will be queried using the options specified in the command line.
/O <Object UUID>	Specifies the object UUID if the interface registered one.
/i <#_iterations>	Specifies the number of calls to make. The default is 1. This option is useful for measuring connection latency if multiple iterations are specified.
/u <security_package_id>	Specifies the security package (security provider) RPC will use to make the call. The security package is identified as a number or a name. If a number is used it is the same number as in the RpcBindingSetAuthInfoEx API. The list below shows the names and numbers. Names are not case sensitive: • Negotiate / 9 or one of nego, snego or negotiate • NTLM / 10 or NTLM • SChannel / 14 or SChannel • Kerberos / 16 or Kerberos • Kernel / 20 or Kernel If you specify this option, you must specify authentication level other than none. There is no default for this option. If it is not specified, RPC will not use security for the ping.
/a <authn_level>	Specifies the authentication level to use. Possible values are: • connect • call • pkt • integrity • privacy If this option is specified, the security package ID (/u) must also be specified. There is no default for this option. If this option is not specified, RPC will not use security for the ping.
/N <server_princ_name>	Specifies a server principal name. This field can be used only when authentication level and security package are selected.
/I <auth_identity>	Allows you to specify alternative identity to connect to the server. The identity is in the form user,domain,password. If the user name, domain, or password have special characters that can be interpreted by the shell, enclose the identity in double quotes. You can specify * instead of the password and RPC will prompt you to enter the password without echoing it on the screen. If this field is not specified, the identity of the logged on user will be used.

	This field can be used only when authentication level and security package are selected.
/C <capabilities>	Specifies a hexadecimal bitmask of flags. This field can be used only when authentication level and security package are selected.
/T <identity_tracking>	Specifies static or dynamic. If not specified, dynamic is the default. This field can be used only when authentication level and security package are selected.
/M <impersonation_type>	Specifies anonymous, identify, impersonate or delegate. Default is impersonate. This field can be used only when authentication level and security package are selected.
/S <server_sid>	Specifies the expected SID of the server. This field can be used only when authentication level and security package are selected.
/P <proxy_auth_identity>	Specifies the identity to authenticate with to the RPC/HTTP proxy. Has the same format as for the /I option. You must specify security package (/u), authentication level (/a), and authentication schemes (/H) in order to use this option.
/F <RPCHTTP_flags>	Specifies the flags to pass for RPC/HTTP front end authentication. The flags may be specified as numbers or names The currently recognized flags are: • Use SSL / 1 or ssl or use_ssl • Use first auth scheme / 2 or first or use_first You must specify security package (/u) and authentication level (/a) in order to use this option.
/H <RPC/HTTP_authn_schemes>	Specifies the authentication schemes to use for RPC/HTTP front end authentication. This option is a list of numerical values or names separated by comma. Example: Basic,NTLM. Recognized values are (names are not case sensitive): • Basic / 1 or Basic • NTLM / 2 or NTLM • Certificate / 65536 or Cert You must specify security package (/u) and authentication level (/a) in order to use this option.
/B <server_certificate_subject>	Specifies the server certificate subject. You must use SSL for this option to work. You must specify security package (/u) and authentication level (/a) in order to use this option.
/b	Retrieves the server certificate subject from the certificate sent by the server and prints it to a screen or a log file. Valid only when the Proxy Echo only option (/E) and the use SSL options are specified. You must specify security package (/u) and authentication level (/a) in order to use this option.
/R	Specifies the HTTP proxy. If *none*, the RPC proxy is used. The value *default* means to use the IE settings in your client machine. Any other value will be treated as the explicit HTTP proxy. If you do not specify this flag, the default value is assumed, that is, the IE settings are checked. This flag is valid only when the **/E** (Echo Only) flag is enabled.
/E	Restricts the ping to the RPC/HTTP proxy only. The ping does not reach the server. Useful when trying to establish whether the RPC/HTTP proxy is reachable. To specify an HTTP proxy, use the /R flag. If an HTTP proxy is specified in the /o flag, this option will be ignored. You must specify security package (/u) and authentication level (/a) in order to use this option.

/q	Specifies quiet mode. Does not issue any prompts except for passwords. Assumes *Y* response to all queries. Use this option with care.
/c	Use smart card certificate. RPCPing will prompt user to choose smart card.
/A	Specifies the identity with which to authenticate to the HTTP proxy. Has the same format as for the /I option. You must specify authentication schemes (/U), security package (/u) and authentication level (/a) in order to use this option.
/U	Specifies the authentication schemes to use for HTTP proxy authentication. This option is a list of numerical values or names separated by comma. Example: Basic,NTLM. Recognized values are (names are not case sensitive): • Basic / 1 or Basic • NTLM / 2 or NTLM You must specify security package (/u) and authentication level (/a) in order to use this option.
/r	If multiple iterations are specified, this option will make **rpcping** display current execution statistics periodically instead after the last call. The report interval is given in seconds. Default is 15.
/v	Tells **rpcping** how verbose to make the output. Default value is 1. 2 and 3 provide more output from **rpcping**.
/d	Launches RPC network diagnostic UI.
/p	Specifies to prompt for credentials if authentication fails.
/?	Displays Help at the command prompt.

Examples

To find out if your Exchange server that you connect through RPC/HTTP is accessible, type:

```
rpcping /t ncacn_http /s exchange_server /o RpcProxy=front_end_proxy /P "usernam
```

<Here is where you put a detailed description of another example.>

```
This /is /a:"different" /example
```

Additional references

- Command-Line Syntax Key