Microsoft

RAP as a Service for SQL Server

Prerequisites

Download the latest prerequisites from:
http://www.microsoft.com/en-us/download/details.aspx?id=34698

Last modified: Oct 25, 2016

How to prepare for your RAP as a Service for SQL Server

The Tools machine is used to connect to each of the servers in your environment and retrieve configuration and health information from them. The Tools machine retrieves information from the environment communicating over Remote Procedure Call (RPC), Server Message Block (SMB), and Distributed Component Object Model (DCOM). Once data is collected, the Tools machine is used to upload the data to the Microsoft Premier Services portal for automated analysis, followed up by manual analysis by one of our expert engineers. This upload requires internet HTTPS connectivity to specific sites. Alternatively, you can also export the collected data from the Tools machine and use a different machine to submit it. You need to ensure the machine used to upload the data also has the RAP as a Service client tool installed and has internet connection.

Internet connectivity is needed to:

- *Access the RAP as a Service portal*
- *Activate your account*
- *Download the toolset*
- *Submit data*

At a high level, your steps to success are:

1. **Install prerequisites** on your Tools machine and configure your environment
2. **Collect data** from your environment
3. **Submit the data** to Microsoft Premier Services for assessment

Data submission to Microsoft online servers and displaying your results on the online portal uses encryption to help protect your data. Your data is analyzed using our RAP expert system.

A checklist of prerequisite actions follows. Each item links to any additional software required for the Tools machine, and detailed steps included later in this document.

Checklist

Please ensure the following items have been completed before accessing the RAP as a Service Portal for the first time and starting your engagement.

1. General Use

□ A Microsoft Account is required to activate and sign in to the RAP as a Service portal. If you don't have one, you can create one at http://login.live.com. Learn more about [Microsoft Account](#).

□ Ensure access to https://services.premier.microsoft.com

□ Ensure the internet browser on the data collection machine has JavaScript enabled.
Follow the steps on How to enable scripting in your browser. Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11 are the supported browsers for this offering. Most other modern HTML5 based browsers will also work.

□ Access to https://ppas.uservoice.com for access to the Support Forum and Knowledge Base Articles for RAP as a Service.

2. Activation

□ Ensure access to http://corp.sts.microsoft.com

□ Ensure access to http://live.com

3. Data Collection

a. Tools machine hardware and Operating System:

□ Server-class or high-end workstation machine running Windows 7, Windows 8, Windows 10, or Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

Note: *Windows Server 2003 is not supported as a tools machine. To successfully gather Performance data, please ensure the data collection machine's OS matches, or is a higher version of the highest versioned OS target machine used within the environment.*

□ Minimum: 4GB RAM, 2Ghz dual-core processor, 5 GB of free disk space.

□ Joined to the same or trusted domain as the target servers. When target instance is a standalone instance in a server with different domain or without a domain you can use the workaround mentioned in page 5, section 2.

□ If this is an Azure IaaS environment review azure notes in this document and Appendix A. Special Requirement for Availability Group Cluster in Azure

b. Software:

□ Microsoft® .NET Framework 4.6 installed

□ PowerShell 2.0 or higher installed

c. Account Rights:

□ Administrator permissions to all SQL server instances

□ Administrative access to the SQL Server hosts

d. Additional Requirements for Windows Server 2008 Servers or later:

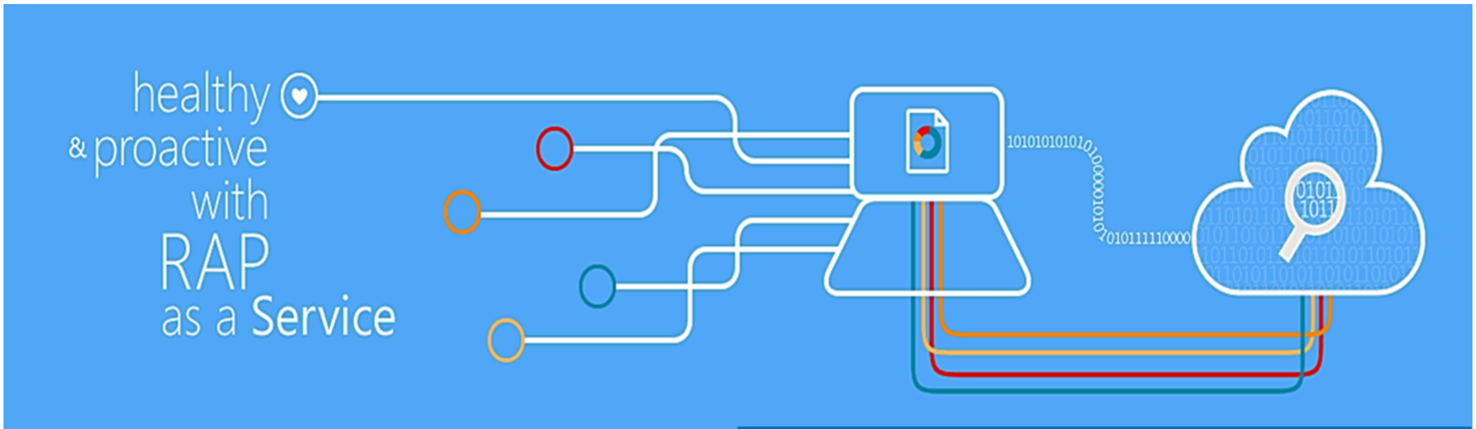
□ Configure the servers' firewall for "Remote Event Log Management"

The Appendix B Data Collection Methods details the methods used to collect data.

4. Submission

□ Internet connectivity is required to submit the collected data to Microsoft.

□ Ensure access to *.accesscontrol.windows.net
this URL is used to authenticate the data submission before accepting it.



Machine Requirements and Account Rights

1. Hardware and Software

Server-class or high-end workstation computer equipped with the following:

- ♦ Minimum single 2Ghz processor — Recommended dual/multi-core 2Ghz or higher processors.
- ♦ Minimum 4 GB RAM—Recommended 8 GB RAM.
- ♦ Minimum 5 GB of free space.
- ♦ Windows 10, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 or Windows Server 2008. Windows Server 2003 is not supported.

  Supported Scenario for Azure: Azure Client and Azure target server on the same virtual network. Non Azure clients are not currently supported.

  Note*: To successfully gather Performance data, please ensure the data collection machine's OS matches, or is a higher version of the highest versioned OS target machine used within the environment. Typically, this means that Windows 8 or Windows Server 2012 is OK to use.*
- ♦ Can be 32-bit or 64-bit operating system.
- ♦ At least a 1024x768 screen resolution (higher preferred).
- ♦ A member of the same domain as the SQL Server hosts or a member of a trusted domain.
- ♦ Microsoft® .NET Framework 4.6.— https://www.microsoft.com/en-gb/download/details.aspx?id=48130
- ♦ PowerShell 2.0 or higher.
  - ∗ PowerShell 2.0 is part of the Windows Management Framework — http://support.microsoft.com/kb/968929
- ♦ Networked "Documents" or redirected "Documents" folders are not supported. Local "Documents" folder on the data collection machine is required.

2. Accounts Rights

- ♦ If the client and target server are on the same domain then:
  - A domain account with the following:
    - Local administrator permissions to all SQL server hosts to be assessed.
    - Administrative access to the SQL server instances (member of SysAdmin Role)
- ♦ If the client and Azure VM target server are NOT the same domain but on the same subnet or virtual network then:
  - Configure Pass through authentication between the client and the target server. Basically the local user name and password used should be the same on the client and the target server.
  - The Pass through authentication account should have the following:
    - Local administrator permissions to all SQL server hosts to be assessed.
    - Administrative access to the SQL server instances (member of SysAdmin Role)

WARNING: Do not use the "Run As" feature to start the client toolset as the discovery process and collectors might fail. The account starting the client toolset must logon to the local machine.

Internet connectivity is needed for the delivery of your engagement

Ensure access to the following URLs:

For General Use:

https://services.premier.microsoft.com.

For the Token Activation and Authentication:

http://corp.sts.microsoft.com.

http://live.com

For Data Collection:

http://go.microsoft.com

For Data Submission

https://services.premier.microsoft.com
https://.windows.net*

https://ajax.aspnetcdn.com

Review the article below for complete information regarding these URLs

https://ppas.uservoice.com/knowledgebase/articles/120616-what-do-i-need-to-open-in-my-firewall-proxy-to-use

- ♦ A Windows Live ID for each user account to logon to the Premier Proactive Assessment Services portal (https://services.premier.microsoft.com). This is the RAP as a Service portal where you will activate your access token, download the toolset and fill out the operational survey, and the URL that hosts the web service that coordinates the data submission
  - ∗ If you don't have one, you can create one at http://login.live.com.
  - ∗ Please contact your TAM if the token in your Welcome Email has expired or can no longer be activated. Tokens expire after 10 days. Your TAM can provide new activation tokens for additional people.

3. Network and Remote Access

- ♦ Ensure that the browser on the tools machine or the machine from where you activate, download and submit data has JavaScript enabled. Follow the steps on How to enable scripting in your browser.

- ♦ Internet Explorer is the supported browser for a better experience with the portal. Ensure Internet Explorer Enhanced Security Configuration (ESC) is not blocking Java-Script on sites. A workaround would be to temporary disable Internet Explorer Enhanced Security Configuration when accessing the https://services.premier.microsoft.com portal. Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11 are the supported browsers for this offering. Most other modern HTML5 based browsers will also work.

- ♦ The following services must be started on the target SQL Server hosts:
  - ∗ Windows Management Instrumentation
  - ∗ Remote Registry
  - ∗ Server
  - ∗ Workstation
  - ∗ Performance Logs & Alerts
  - ∗ Task Scheduler

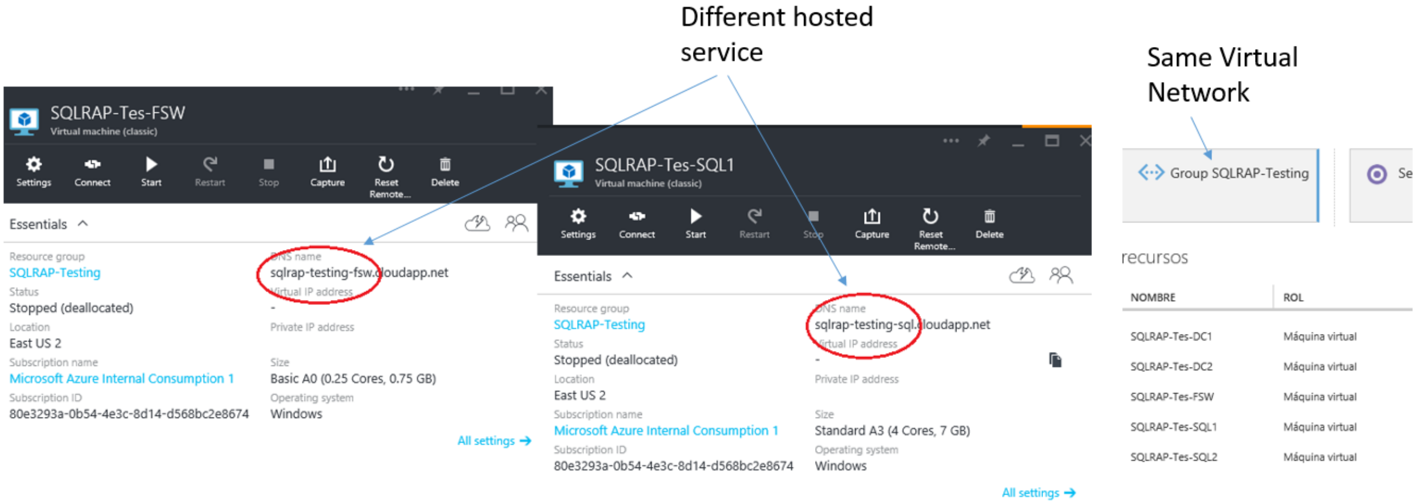
  □ For Availability Groups in Azure follow the requirements in Appendix A. Special Requirement for Availability Group Cluster in Azure.

- ♦ If a Firewall exist (Windows or Hardware) between the tools machine and the target server follow steps and recommendations on Appendix C: Firewall Requirements.

Appendix A: Special Requirements for Availability Group Cluster in Azure

Virtual networks in Azure put some connectivity restrictions to clusters and availability groups that affect the toolset. In summary:

1. You cannot use the listener name for discovery. You can use the cluster name or a node name.
2. If you are using cloud services (discontinued in Azure Resource Manager for IaaS) and you are using an External load balancer (internal load balancer does not have this limitation), then you need to have the tools machine in a different cloud service as shown in this image.



SQLRAP-Tes-FSW
Virtual machine (classic)

Resource group SQLRAP-Testing	DNS name sqlrap-testing-fsw.cloudapp.net
Status Stopped (deallocated)	Virtual IP address -
Location East US 2	Private IP address
Subscription name Microsoft Azure Internal Consumption 1	Size Basic A0 (0.25 Cores, 0.75 GB)
Subscription ID 80e3293a-0b54-4e3c-8d14-d568bc2e8674	Operating system Windows

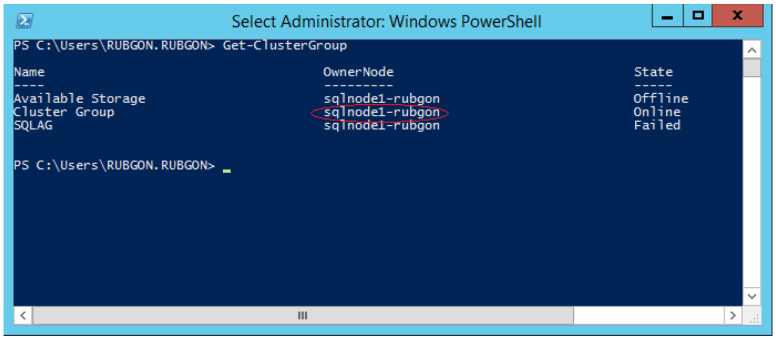
SQLRAP-Tes-SQL1
Virtual machine (classic)

Resource group SQLRAP-Testing	DNS name sqlrap-testing-sql.cloudapp.net
Status Stopped (deallocated)	Virtual IP address -
Location East US 2	Private IP address
Subscription name Microsoft Azure Internal Consumption 1	Size Standard A3 (4 Cores, 7 GB)
Subscription ID 80e3293a-0b54-4e3c-8d14-d568bc2e8674	Operating system Windows

recursos

NOMBRE	ROL
SQLRAP-Tes-DC1	Máquina virtual
SQLRAP-Tes-DC2	Máquina virtual
SQLRAP-Tes-FSW	Máquina virtual
SQLRAP-Tes-SQL1	Máquina virtual
SQLRAP-Tes-SQL2	Máquina virtual

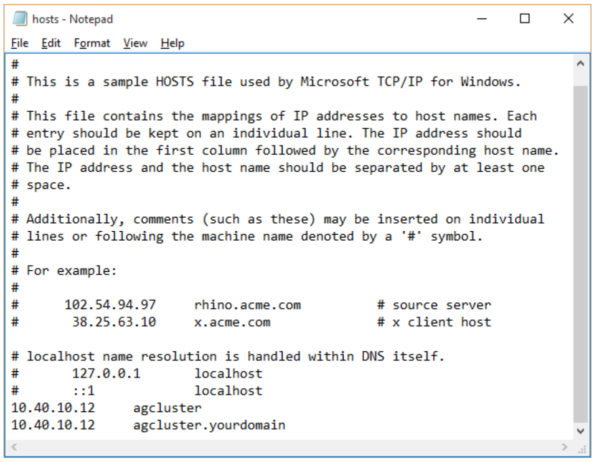
3. You need to modify the hosts file to make the Cluster Collectors work. You need to identify the IP of the active node and modify the hosts files as shown below. The hosts file is located at “C:\Windows\System32\drivers\etc”.



```
PS C:\Users\RUBGON.RUBGON> Get-ClusterGroup

Name                                    OwnerNode                                State
----                                    ---------                                -----
Available Storage                       sqlnode1-rubgon                          Offline
Cluster Group                           sqlnode1-rubgon                          Online
SQLAG                                   sqlnode1-rubgon                          Failed

PS C:\Users\RUBGON.RUBGON> _
```



```
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#	127.0.0.1       localhost
#	::1             localhost
10.40.10.12	agcluster
10.40.10.12	agcluster.yourdomain
```

Note: The hosts configuration change needs to be reviewed every time you run the toolset in case a failover has happened since the last time the toolset was executed.

Appendix B: Data Collection Methods

RAP as a Service for SQL Server uses multiple data collection methods to collect information. This section describes the methods used to collect data from an SQL Server environment. No VB scripts are used to collect data. Data collection uses workflows and collectors. The collectors are:

1. Registry Collectors
2. FileDataCollector
3. WMI
4. TSQL Data collector
5. EventLogCollector
6. Windows PowerShell
7. SQL Error Log collection
8. Local Security Policy
9. Performance Monitor Counters data

1. Registry Collectors

Registry keys and values are read from the data collection machine and all SQL Servers. They include items such as:

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.

  This allows to determine where the SQL Server instances installed on given server or failover cluster and get detailed information on each service relevant to the proper function of SQL Server. We do not collect all services, only the ones relevant to SQL.
- Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

  This allows to determine Operation System information such as Windows Server 2008 or Windows Server 2012.

2. FileDataCollector

Enumerates files in a folder on a remote machine, and optionally retrieves those files.

3. Windows Management Instrumentation (WMI)

WMI is used to collect various information such as:

- WIN32_Volume

  Collects information on Volume Settings for each SQL Server. The information is used for instance to determine the system volume and drive letter which allows the tool to collect information on database files located on the system drive and other drives.
- Win32_LogicalDisk

  Used to collect information on the logical disks. We use the information to determine the amount of free space on the disk where the database or log files are located.

4. TSQL Data Collector

- Queries against system tables

  RAP as a Service for SQL Server collects information from SQL Server system tables using the T-SQL data collector. The information includes but not limited to database backups, Log shipping information, databases participated in replication, etc..

- Queries against system DMVs

  Dynamic management views and functions return server state information that can be used to monitor the health of a server instance, diagnose problems, and tune performance.

5. EventLogCollector

Collects event logs from SQL Server hosts. We collect the last 7 days of Warnings and Errors from the Application,
and System event logs.

6. Windows PowerShell

Collects various information, such as:

- Failover Cluster resource dependencies.

7. SQL Error Log collection

Collects SQL Server error log data for the last 15 days or for 6MB of size.

8. Local Security Policy

Local Policies, which is part of the Local Security Settings console, determine the security options for a user or service account

9. Performance Monitor Counters data

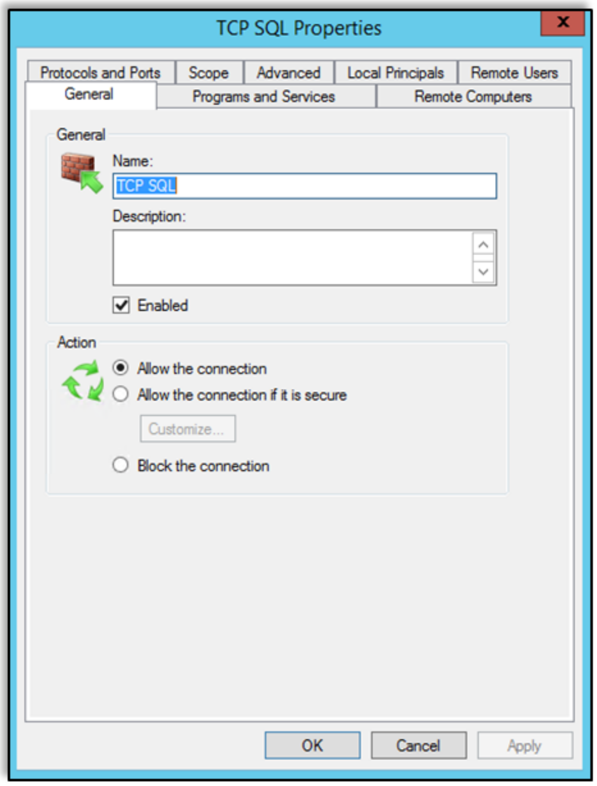
System and SQL Server instance related performance counters.

Appendix C: Firewall Requirements

If you have a firewall between the tools machine and target servers and/or you are using Windows Firewall you need to open several ports and range of ports to allow the data collection to succeed. The following steps apply to Windows Firewall but the same ports and protocols need to be open on any other firewall you are using.

1. Open SQL Server port in the Windows firewall for TCP access.

- If SQL Server instance is running on a static TCP/IP port, open the static port in the Windows firewall for TCP access.
    - Under inbound rules, create a new custom rule for the SQL port. (port 1433 is used in the example below)



General

Name: TCP SQL

Description:

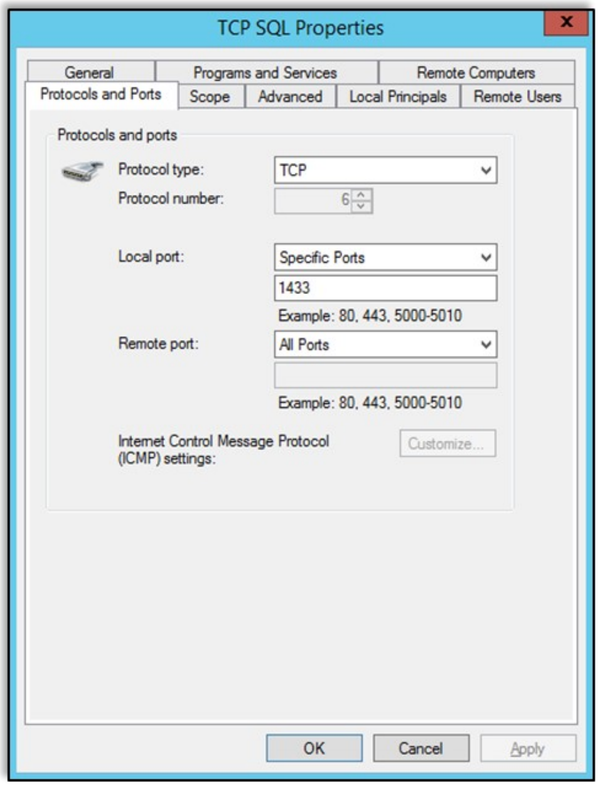
☑ Enabled

Action

● Allow the connection

○ Allow the connection if it is secure

○ Block the connection



Protocols and ports

Protocol type: TCP

Protocol number: 6

Local port: Specific Ports

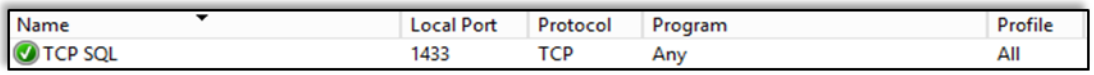
1433

Example: 80, 443, 5000-5010

Remote port: All Ports

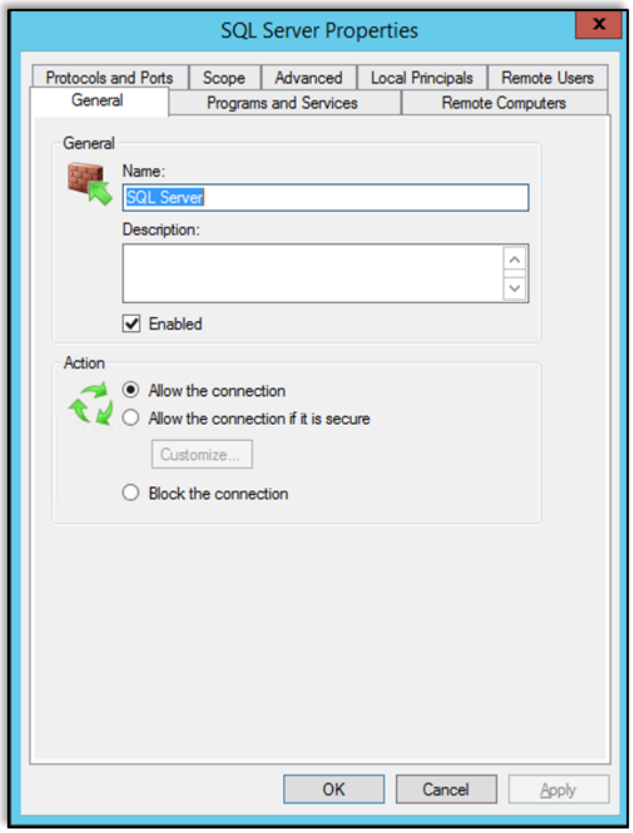
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:



Name	Local Port	Protocol	Program	Profile
✓ TCP SQL	1433	TCP	Any	All

- If using dynamic port for SQL Server, create custom rule to allow connections to the SQL program.



General

Name: SQL Server

Description:

☑ Enabled

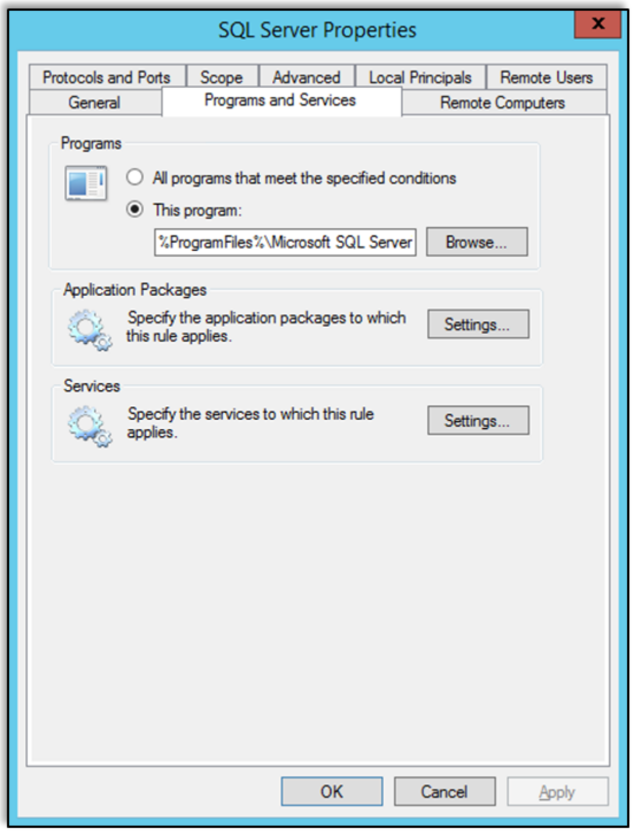
Action

● Allow the connection

○ Allow the connection if it is secure

Customize...

○ Block the connection



Programs

○ All programs that meet the specified conditions

● This program:

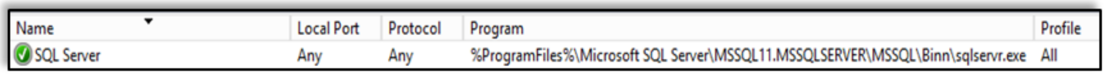
%ProgramFiles%\Microsoft SQL Server

Application Packages

Specify the application packages to which this rule applies.

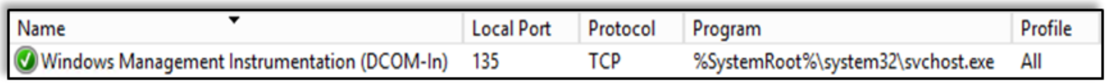
Services

Specify the services to which this rule applies.



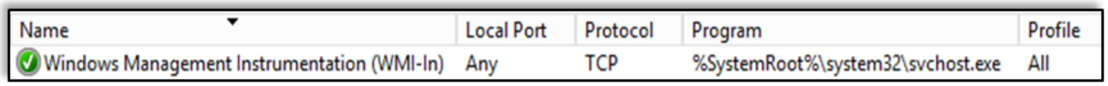
Name	Local Port	Protocol	Program	Profile
✓ SQL Server	Any	Any	%ProgramFiles%\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Binn\sqlservr.exe	All

2. Open port 135 or just enable DCOM-In inbound rule in firewall



Name	Local Port	Protocol	Program	Profile
✓ Windows Management Instrumentation (DCOM-In)	135	TCP	%SystemRoot%\system32\svchost.exe	All

3. Enable WMI-In firewall rule



Name	Local Port	Protocol	Program	Profile
✓ Windows Management Instrumentation (WMI-In)	Any	TCP	%SystemRoot%\system32\svchost.exe	All

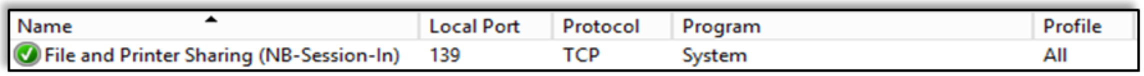
WMI uses dynamic ports for RPC connectivity. RPC dynamic port allocation will instruct the RPC program to use a particular random port in the range configured for TCP and UDP.

If you want to control which ports RPC is using then follow the instructions provided in these kb articles and only open those ports in the firewall.

How to configure RPC dynamic port allocation to work with firewalls
TCP/IP has changed in Windows Vista and in Windows Server 2008

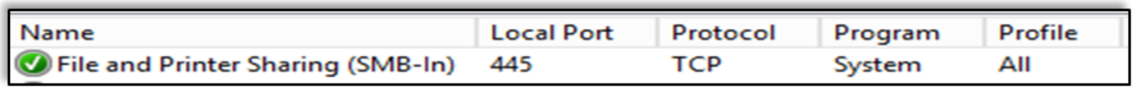
Azure Note: Remember that the tools machine needs to be on the same Virtual Network as the target server.

4. Open port 139 or just enable File and Print Sharing (NB-Session-In)



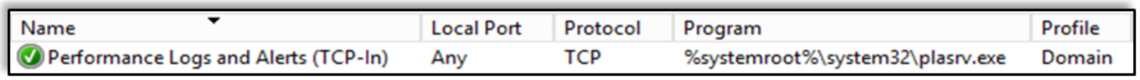
Name	Local Port	Protocol	Program	Profile
✓ File and Printer Sharing (NB-Session-In)	139	TCP	System	All

5. Open port 445 or just enable File and print sharing (SMB-In) in firewall



Name	Local Port	Protocol	Program	Profile
✓ File and Printer Sharing (SMB-In)	445	TCP	System	All

6. Enable Performance logs and alerts (TCP-in) rule in firewall



Name	Local Port	Protocol	Program	Profile
✓ Performance Logs and Alerts (TCP-In)	Any	TCP	%systemroot%\system32\plasrv.exe	Domain

Performance logs and alerts uses dynamic ports for RPC connectivity. RPC dynamic port allocation will instruct the RPC program to use a particular random port in the range configured for TCP and UDP.

If you want to control which ports RPC is using then follow the instructions provided in these kb articles and only open those ports in the firewall.

How to configure RPC dynamic port allocation to work with firewalls
TCP/IP has changed in Windows Vista and in Windows Server 2008