RAP as a Service for SharePoint Server

Prerequisites

Last modified: February 13, 2018

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

Internet connectivity is needed to:

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

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.

How to prepare for your RAP as a Service for SharePoint 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.

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

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 already, you can create one at http://login.live.com

- To learn more about Microsoft Accounts, see: http://windows.microsoft.com/en-US/windows-live/sign-in-what-is-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 listed at How to enable scripting in your browser. Internet Explorer 11 and Microsoft Edge are the supported and recommended browsers for this offering. Most other modern HTML5 based browsers will also work.

☐ The site https://ppas.uservoice.com provides 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.

☐ Minimum: 4GB RAM **12GB Recommended**, 2Ghz dual-core processor, 5 GB of free disk space.

☐ Joined to the same domain as the SharePoint farm being assessed.

b. Software for Tools machine:

☐ Microsoft .NET Framework 4.6.1

* NOTE: If the SharePoint Server has a higher version of .NET installed than 4.6.1 than the version installed on the Tools machine must be equal to or higher than installed on the Target SharePoint Server.

☐ Windows PowerShell 2.0 or later installed

☐ PowerShell Execution policy set to RemoteSigned

c. Account Rights:

☐ Member of the local Administrators group on all servers in the SharePoint environment

☐ Member of SharePoint Farm Administrators group

☐ Full Control to all Service Applications.

☐ Member of the "SysAdmin" group on SQL instances hosting SharePoint databases

☐ Unrestricted network access from the Tools machine to all servers

d. Additional Requirements for Windows Server 2008 (and later) servers:

☐ Configure all server firewalls for "Remote Event Log Management"

NOTE: The data collection is done from a machine (a.k.a. **Tools Machine** or **Data Collection Machine**) which is not part of the

SharePoint farm that is analyzed but is joined to the same domain as of the SharePoint farm. The details regarding the requirements for the Tools Machine are provided in the subsequent pages of this document. ***Tools machine should not have SharePoint bits installed on it.***

Data is collected by the Tools Machine by connecting to one of the SharePoint Servers in the farm, which is called "**Target Server**". More information about the Target Server requirements is provided later in this document.

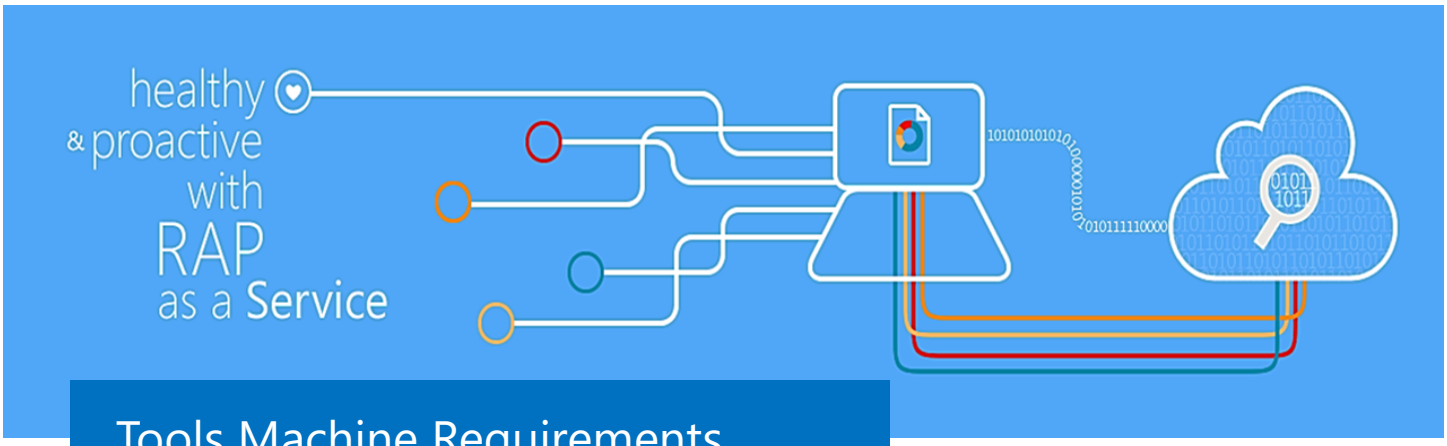
A domain user account is needed for data collection (recommended to use a dedicated account). The details regarding the account rights are provided later in this document.

The Appendix 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 — *URL is used to authenticate the data submission before accepting it.*



Tools Machine Requirements

1. Hardware and Software

- Minimum single 2Ghz processor — Recommended dual-core/multi-core 2Ghz or higher processors.
- Minimum 4 GB RAM—**Recommended 12 GB RAM.**
- Minimum 5GB of free disk space.
- High End Workstation: Windows 10/Windows 8.1/Windows 8/Windows 7
  Server: Windows Server 2016/Windows Server 2012 R2/Windows Server 2012/Windows Server 2008 R2/Windows Server 2008.
- Can be 32-bit or 64-bit operating system.
- At least a 1024x768 screen resolution (higher preferred).
- Must be a member of the same domain as the SharePoint farm that is being assessed.
- Microsoft® .NET Framework 4.6.1— https://www.microsoft.com/en-us/download/details.aspx?id=49982
  - NOTE: If the SharePoint Server has a higher version of .NET installed than 4.6.1 than the version installed on the SP Server must match or be greater.
- Windows PowerShell 2.0 or higher
  - Windows PowerShell 2.0 is part of the Windows Management Framework: http://support.microsoft.com/kb/968929
  - PowerShell 3.0 is part of the Windows Management Framework 3.0: http://support.microsoft.com/kb/2506143
  - The execution policy for PowerShell should be set to remotesigned on both the tools machine and the servers
  - The execution policy settings can be verified using “get-executionpolicy –list” in a PowerShell command window
- Networked “Documents” or redirected “Documents” folders are not supported. Local “Documents” folder on the data collection machine is required.
- IIS 7 Administration components
- Firewall exception for Remote Administration(RPC) – Dynamic Port Range

Important for SharePoint 2010 Farms:

- PowerShell 2.0 is required for SharePoint 2010 farm assessments only. If PowerShell 3.0 or later and .NET framework 4.0 o greater are installed on the target server of the SharePoint 2010 farm, register the following session on the target server to make sure the PowerShell 2.0 instance is used for data collection.

```
Register-PSSessionConfiguration -Name "Microsoft.RAP.PowerShellv2Config" -
PowerShellVersion 2.0 -Confirm:$false
```

- If PowerShell 2.0 and .NET framework 4.0 or greater are installed on the target server of the SharePoint 2010 farm, register the following session on the target server to make sure the PowerShell 2.0 instance is used for data collection.

```
Register-PSSessionConfiguration –Name "Microsoft.RAP.PowerShellv2Config" -
Confirm:$false
```

2. Scanning Security Updates with Microsoft Security Baseline Analyzer (MBSA)

MBSA is used to scan the servers for security patches using the Windows Update Agent. For more information, review the MBSA Frequently Asked Questions—http://technet.microsoft.com/en-us/security/cc184922.aspx

MBSA 2.3 is needed for scanning missing and installed patches. If the Tools machine is a 32-bit machine the x86 version of MBSA must be installed, if the Tools machine is a 64-bit machine the x64 version must be installed. All versions are posted on the MBSA download site — http://www.microsoft.com/en-us/download/details.aspx?id=7558

Windows Update Agent Service must be running on all servers.

3. Accounts Rights

A domain account with the following:

- Member of the local Administrators group on all servers in the SharePoint environment
- Full Control to all Service Applications.
- Member of the "SysAdmin" group on SQL instances hosting SharePoint databases
- Unrestricted network access from the Tools machine to all servers
- Member of SharePoint Farm Administrators group
- Unrestricted network access from the Tools machine to all servers

Ability to run PowerShell scripts on the machine running the RAP as a Service Client. The Windows PowerShell execution policy must be set to RemoteSigned or a policy that provides an equivalent ability to run local scripts http://technet.microsoft.com/library/hh847748.aspx

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.

- A Microsoft Account is required to activate and sign in 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.

    - If you don't have one, you can create one at http://login.live.com.
    - Contact your TAM if the token in your Welcome Email has expired or can no longer be activated. Tokens expire after ten days. Your TAM can provide new activation tokens for additional people.

4. 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 listed at How to enable scripting in your browser.

Internet Explorer is the recommended browser for a better experience with the portal. Ensure Internet Explorer Enhanced Security Configuration (ESC) is not blocking JavaScript on sites. A workaround would be to temporary disable Internet Explorer ESC when accessing the https://services.premier.microsoft.com portal.

Unrestricted network access from the Tools machine to all servers. This means access through any firewalls and router ACLs that might be limiting traffic to any of the servers. This includes remote access to:

- DCOM
- Remote Registry service
- Windows Management Instrumentation (WMI) services
- default administrative shares (C$, D$, IPC$).

Ensure that the machine you use to collect data has complete TCP/UDP access, including RPC access to all servers. Access over ports 135, and 139 or 445 is also required.

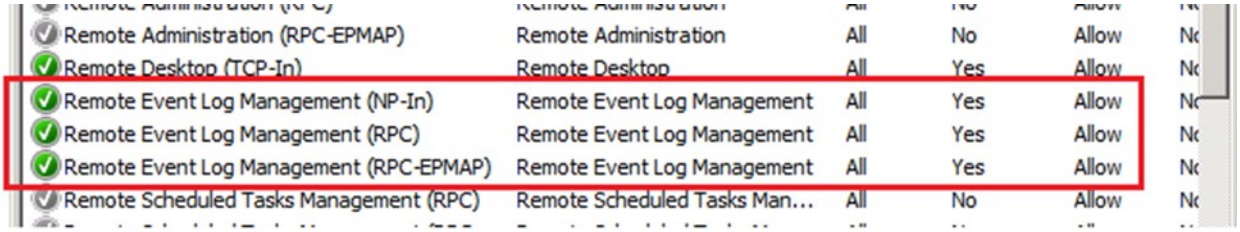
Windows Remote Management (WinRM) uses Ports 5985 for HTTP. Communication between the Tools machine and the SharePoint server that is targeted for the data collection on port 5985 has to be enabled as PowerShell commands will be executed remotely via this port.

> **Note:** When you execute the Remote PowerShell and CredSSP configuration steps in section 6 of this document you will be prompted to allow port 5985 to be opened as part of the configuration, please select yes to allow the port to be opened when prompted.

Configure the servers firewall to ensure all servers running Windows Server 2008/Windows Server 2008 R2 and later have Remote Event Log Management enabled: Offline client might be unable to collect event log information from a Windows Server 2008/Windows Server 2008 R2 or later if **Remote Event Log Management** has not been allowed. When **Remote Management** is enabled, the following services must be started on the target servers:

- WMI
- Remote Registry service
- Server service
- Workstation service
- File and Printer Sharing service
- Automatic Updates service

Configure the server firewall to ensure all servers running Windows Server 2008/R2 and higher have "Remote Event Log Management" enabled: RAP as a Service for SharePoint Server Client might be unable to collect event log information from a Windows Server 2008/R2 if "Remote Event Log Management" has not been allowed. When "Remote Management" is enabled, the rules that allow Remote Event Log Management are also enabled.



To test if the tool will be able to collect event log data from a Windows Server 2008/R2 host you can try to connect to the Windows Server 2008/R2 server using eventvwr.msc. If you are able to connect, collecting event log data is possible. If the remote connection is unsuccessful you may need to enable the Windows built-in firewall to allow "Remote Event Log Management".

Connectivity Testing

- **Event Log:** To test if the tool will be able to collect event log data from a Windows Server 2008 R2 server, you can try to connect to the Windows Server 2008/R2 server using eventvwr.msc. If you are able to connect, collecting event log data is possible. If the remote connection is unsuccessful you may need to enable the Windows built-in firewall to allow "Remote Event Log Management".
- **Registry:** Use regedit.exe to test remote registry connectivity to the target servers (File > Connect Network Registry).
- **File:** Connect to the C$ and Admin$ shares on the target servers to verify file access.

5. Additional requirements for Windows Server 2008 or later:

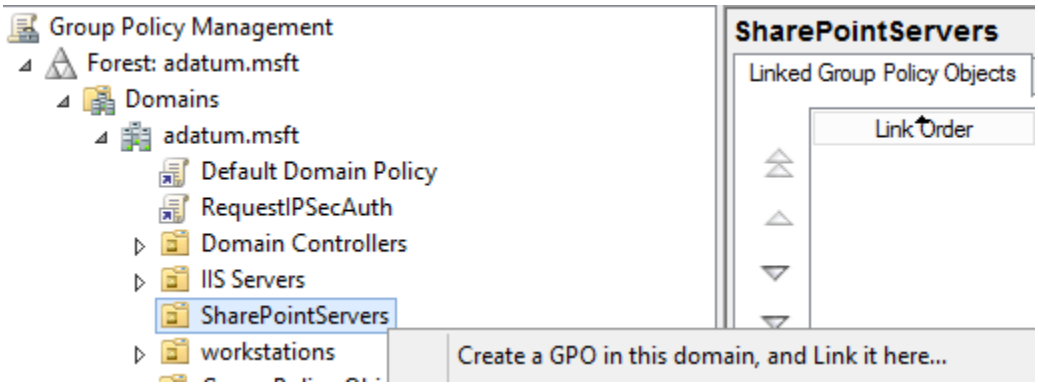
5a. Log into the chosen data collection machine to identify its current IP address using IPConfig.exe from the command prompt.

An example output is as follows:
C:\Program Files\Microsoft Baseline Security Analyzer 2>ipconfig

Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::X:X:X:X%13
IPv4 Address. . . . . : **X.X.X.X**
Subnet Mask . . . . . : X.X.X.X
Default Gateway . . . . . : X.X.X.X

Make a note of the IPv4 address of your machine. The final step in the configuration will use this address to ensure only the data collection machine can communicate with the Windows Update Agent on the SharePoint server farm.

5b. Create, configure, and link a group policy object to the SharePoint Servers OU in the domain of the servers.

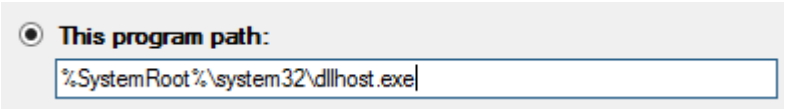


Create a new GPO.

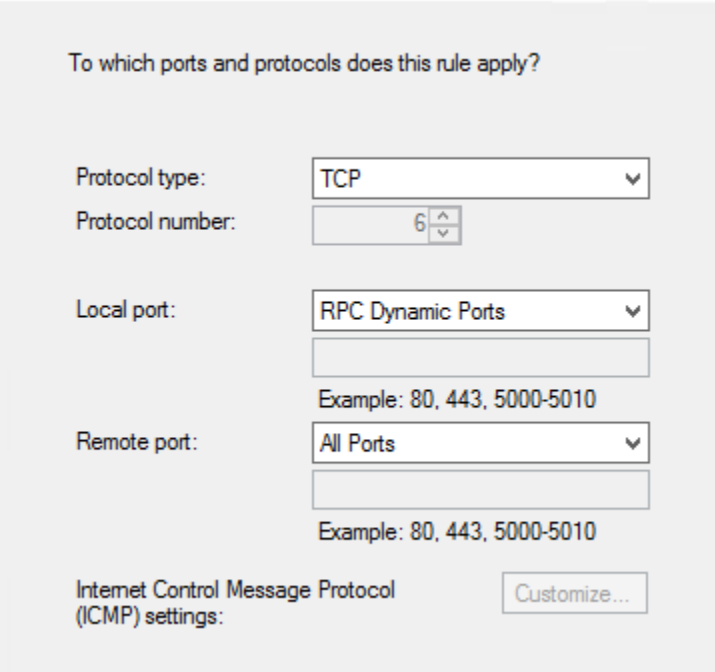
- Make sure the GPO applies to the SharePoint Servers organizational unit.

  Note: If other servers outside the scope are present in the OU, then security group filtering can be used to restrict the application of group policy to only the SharePoint Servers.

- Within the GPO open: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\ Windows Firewall with Advanced Security\.
- Right-click Inbound Rules and then click New Rule.
- The rule you create will be merged with the rules that already enabled on the SharePoint Servers' through local policy and/or other group policy objects that have inbound rules defined.
- On the New Inbound Rule Wizard, on the Rule Type page click Custom, and then click Next.
- On the Program tab, choose This Program Path and insert the following path without the quotes:
- "%SystemRoot%\system32\dllhost.exe" as shown in the below graphic and choose next.



- On the Protocol and Ports Page Select "TCP" for the Protocol Type and "RPC Dynamic Ports" for Local Ports and select next as shown in the following graphic.



- On the scope page, select These IP Addresses under “which remote IP addresses does this rule apply to”, then click Add. Insert the IP address of the data collection machine identified in the first step. Click OK, then Next on the scope page.
- Choose Allow the Connection on the Action page and select Next.
- Leave the default profiles checked on the Profile page, then on the Name page, give the rule a name that describes what it allows, similar to “Allow Inbound to WUA from x.x.x.x” and finish the rule creation wizard to commit the rule to the firewall policy.
- Once the rule applies, it can be confirmed as active through Windows Firewall with Advanced Security MMC (WF.MSC) monitoring navigation node or by interrogating the output of the following PowerShell command “Get-NetFirewallRule -Enabled true -policystore ActiveStore” and confirming the created rule shows up.

6. Remote PowerShell and CredSSP Configuration (Tools Machine)

On the Tools Machine, launch PowerShell Prompt with the option "Run as Administrator". And run the following commands (see important note below before running the below commands)

```
Enable-WSManCredSSP -Role client -DelegateComputer <SharePointServer FQDN>
```

Note :

- The "**SharePointServer FQDN**" in the above command **is the** "**Target Server**" to which the "Tools Machine" connects to when collecting data. You must use the FQDN for the SharePoint server and not just the host name.
- The WinRM service needs to be running for this command to succeed.

7. Remote PowerShell and CredSSP Configuration (Target Server)

On the Target Server (see the first page and the fourth page of this document to learn about Target Server), launch PowerShell Prompt with the option "Run as Administrator". And run the following commands (see important note below before running the below commands)

```
winrm quickconfig
Enable-WSManCredSSP -Role server
```

(Run the following two commands for Windows Server 2008/R2 only)

```
winrm set winrm/config/winrs '@{MaxShellsPerUser="25"}'
winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="600"}'
```

(Watch the quotes in the last 2 commands above)

Note :

- SharePoint 2010, SharePoint 2013 and SharePoint 2016 farms supported only at this time. RAP as a Service for Share-Point Server does not support Office SharePoint Server 2007/Windows SharePoint Services 3 or earlier.
- RAP as a Service for SharePoint Server supports SharePoint farms backed by SQL servers running SQL Server 2016, SQL Server 2014, SQL Server 2012, SQL Server 2008 R2, SQL Server 2008, and SQL Server 2005. Earlier versions of SQL Server are not supported.

8. Remote PowerShell and CredSSP Configuration

As part of the assessment, most of the SharePoint information is gathered by executing PowerShell scripts remotely from the Tools Machine. It is very important for the CredSSP delegation to be configured correctly so that the PowerShell scripts can be executed remotely on the Target Server. The below script helps in knowing if the CredSSP is configured correctly by connecting and executing the script on the Target Server. Run the below script from the Tools Machine.

Executing the below snippet should output the list of all SharePoint Content databases of your SharePoint farm.

```
$farm = Get-Credential
$s = New-PSSession -ComputerName [FQDN of Target Server] -Authentication CredSSP -Credential $farm
Invoke-Command -Session $s -ScriptBlock { add-pssnapin Microsoft.SharePoint.PowerShell -ea 0 }
Invoke-Command -Session $s -ScriptBlock { get-spfarm }
Invoke-Command -Session $s -ScriptBlock { get-spcontentdatabase }
Get-PSSession | Remove-PSSession
```

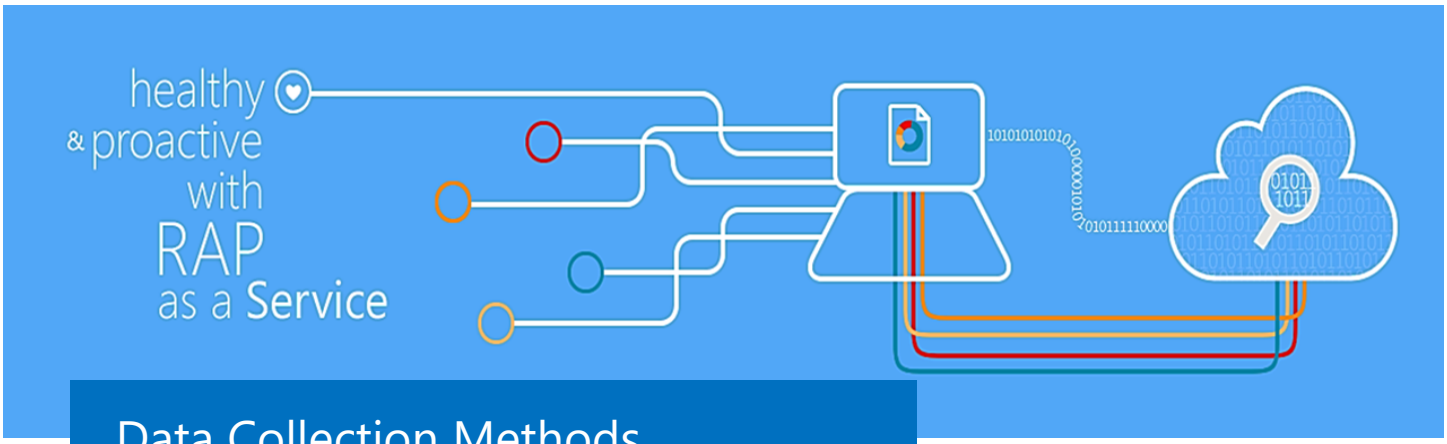
If the following components are installed on the SharePoint 2010 farm, use the below snippet instead

- NET framework 4.0 and/or PowerShell 3.0
- NET framework 4.0 and PowerShell 2.0

```
$farm = Get-Credential
$s = New-PSSession -ComputerName [FQDN of Target Server] -Authentication CredSSP -Credential $farm –ConfigurationName "Microsoft.RAP.PowerShellv2Config"
Invoke-Command -Session $s -ScriptBlock { add-pssnapin Microsoft.SharePoint.PowerShell -ea 0 }
Invoke-Command -Session $s -ScriptBlock { get-spfarm }
Invoke-Command -Session $s -ScriptBlock { get-spcontentdatabase }
Get-PSSession | Remove-PSSession
```

Note :

- The “FQDN of Target Server” is the SharePoint server on which the CredSSP is enabled (see the first page and the fourth page of this document to learn about Target Server).
- If the above test fails, DO NOT proceed with the assessment and reach out the TAM for further assistance.



Data Collection Methods

Appendix A: Data Collection Methods

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

- Registry Collectors
- SharePoint PowerShell Scripts
- Event Log Collector
- SQL Queries
- IIS information
- File Data Collector
- WMI
- Microsoft Baseline Analyzer

Registry Collectors

Registry keys and values are read from the RAP as a Service data collection machine (a.k.a Tools Machine) and all SharePoint Servers including SQL servers. They include items such as:

- SQL Alias information from **HKLM\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo**
  - This allows to determine if the SharePoint servers are using SQL alias to connect to the SQL server that is hosting the SharePoint databases.
- Operating System information from **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion**
  - This allows to determine Operation System information such as Windows Server 2003, Windows Server 2008 or Windows Server 2012.

SharePoint PowerShell Scripts

Majority of the SharePoint data is gathered via running the SharePoint PowerShell scripts. For example, the information pertaining to Large list views, Alternate Access mappings, SharePoint services, ULS information, SharePoint Lists information, SharePoint Search, Timer Jobs etc., are all gathered using SharePoint PowerShell scripts.

These scripts are executed remotely from the Tools Machine by connecting to the Target Machine. For more information about Tools Machine and Target Machines, see 1st page and 4th page of this document.

Event Log Collector:

Collects event logs from all the SharePoint Servers including SQL servers. RAP as a Service for SharePoint Server collects the last 7 days of Warnings and Errors from the Application and System logs.

SQL Queries:

Some of the information pertaining to the SQL databases that are hosted by the SharePoint SQL instance are gathered via SQL scripts. For example, the information related to the SQL data and log files (for example, the size and next growth size), SQL instance properties (for example, if using Integrated Security, if the instance is clustered), Index Fragmentation, Statistics information etc., are all gathered via SQL Scripts.

IIS Information:

The details of the IIS web sites and App Pool configurations are gathered using .NET code and workflows.

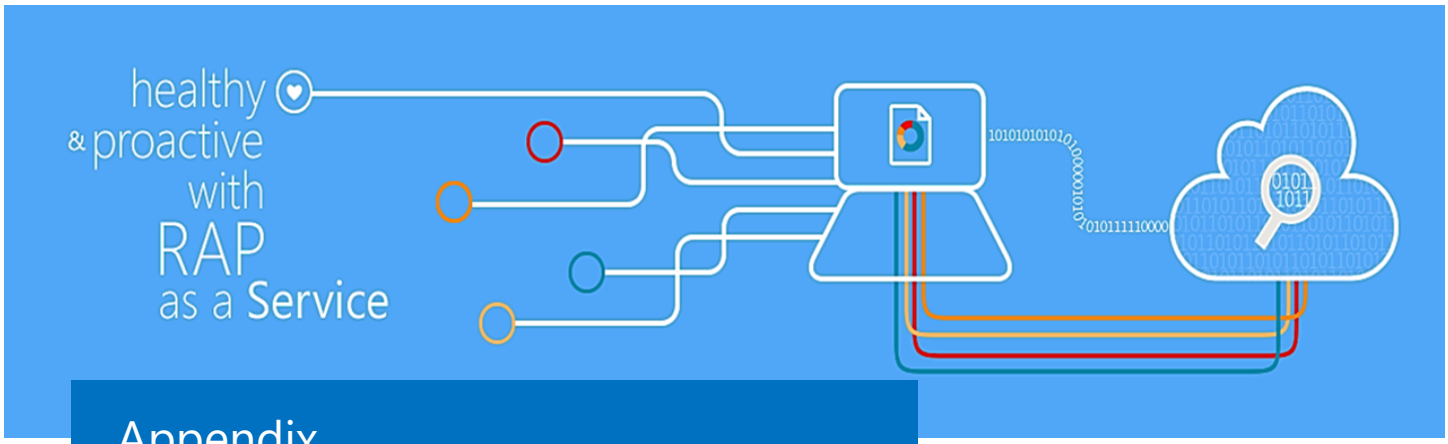
File Data Collector:

Enumerates files in a folder on a remote machine, and optionally retrieves those files. For example, web.config files, IIS Log files, App Host config files etc.

Windows Management Instrumentation (WMI):

WMI is used to collect various information such as:

- **WIN32_Volume:** Collects information on Volume Settings for each server in the SharePoint environment. The information is used for instance to determine the system volume and drive letter which allows RAP as a Service for SharePoint Server to collect information on files located on the system drive.
- **Win32_Process:** Collect information on the processes running on each server in the SharePoint environment. The information provides insight in processes that consume a large amount of threads, memory or have a large page file usage.
- **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.

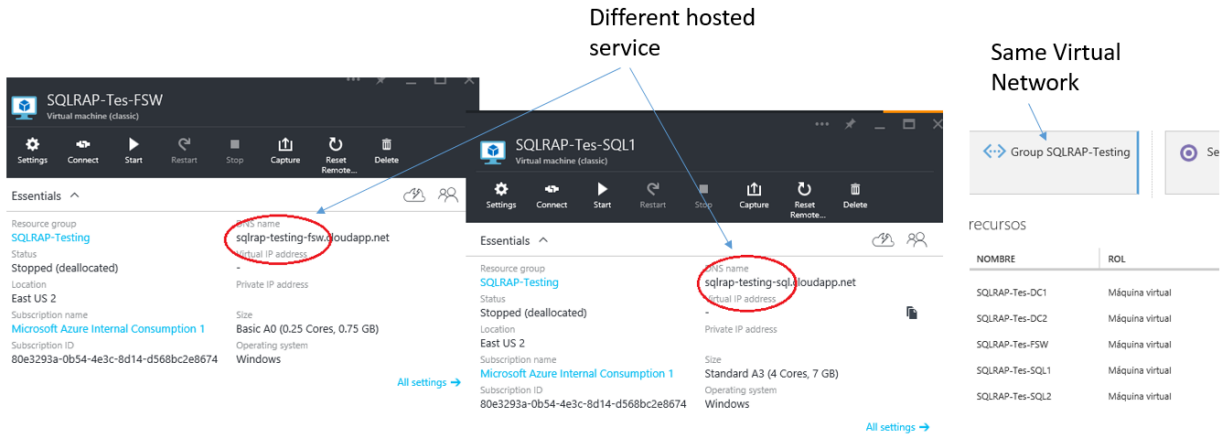


Appendix

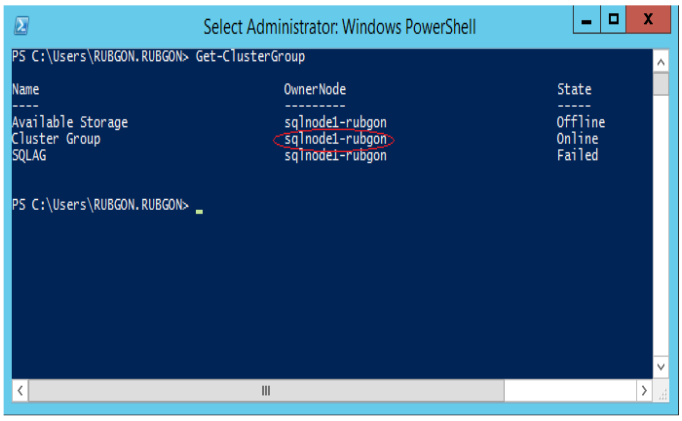
Appendix B: Special Requirements for SharePoint farms using SQL Availability Group Cluster in Azure

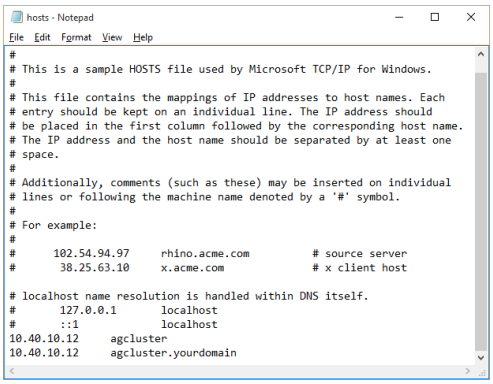
Virtual networks in Azure put some connectivity restrictions to clusters and availability groups that affect the toolset. In summary:

1. 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.



2. You need to modify the hosts file on the tools machine 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”.





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.