RAP as a Service for Failover Cluster

Last modified: March 15th, 2017

Prerequisites

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*

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 Failover Cluster.
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 9, Internet Explorer 10 and Internet Explorer 11 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 machine running Windows Windows 7/Windows 8/windows 10, or Windows Server 2008/Windows Server 2008 R2/Windows Server 2012/Windows Server 2012 R2/2016

  Note: *Windows Server 2003 is not supported as Tools machines.*

  Note: *The Operating System of the Tools machine should be equal or higher than the cluster being reviewed.*
- ☐ Minimum: 8GB RAM, 2Ghz dual-core processor, 5 GB of free disk space.
- ☐ Joined to the same domain as the environment servers or a trusted domain.
- ☐ Windows PowerShell 2.0 engine should be installed on Server 2012 or Server 2012 R2/2016.
- ☐ DO NOT USE a cluster node as the machine to install the data collection toolset on. This will cause additional items to be identified as the cluster nodes will not have matching software installed. This tool also will use system resources that can negatively affect the performance of the machine that it is running on.
- ☐ Disjoined domain names are not supported.
- ☐ Only a single tools machine is supported, collecting from multiple machines will exclude each others data collection.

b. Software for Tools machine:

- ☐ Microsoft .NET Framework 4.0 installed
- ☐ Windows PowerShell 2.0 or later installed
- ☐ PowerShell Execution policy set to RemoteSigned

c. Account Rights:

- ☐ Member of the local Administrators group on all cluster nodes in the environment being reviewed.
- ☐ Unrestricted network access from the Tools machine to all cluster nodes in the environment being reviewed. Active Directory access is required as well to check cluster related computer accounts.

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

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

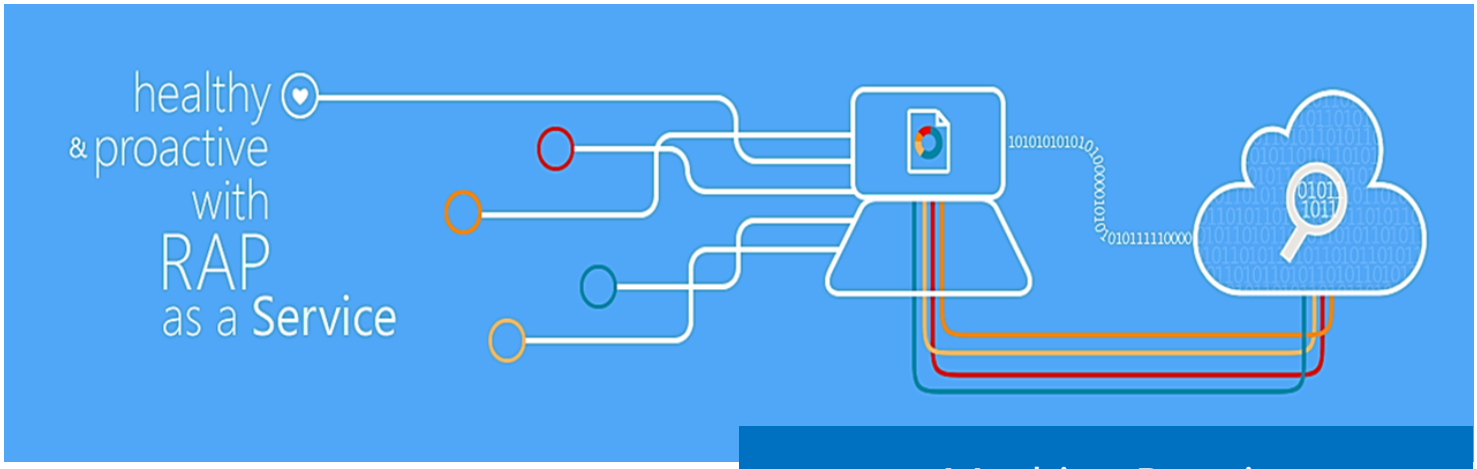
The Appendix Data Collection Methods details the methods used to collect data.

4. Submission

- ☐ Internet connectivity is required to submit the collected data to Microsoft.
  - ☐ Ensure access to *.accesscontrol.windows.net
    this URL is used to authenticate the data submission before accepting it.

The rest of this document contains detailed information on the steps discussed above.

Once you have completed these prerequisites, you are ready to use the RAP as a Service Portal to begin your assessment.



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-core/multi-core 2Ghz or higher processors.
- Minimum 8 GB RAM.
- Minimum 3 GB of free disk space.
- Windows 10 (preferred), Windows 8.1, Windows 7, Windows Server 2012/Windows Server 2012 R2, Windows Server 2016, or Windows Server 2008/Windows Server 2008 R2. .

  ***Note**:* Server 2003 is **not supported** as a data collection machine.
  To successfully gather Performance data, ensure the data collection machine's Operating System (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 2012/2016 is acceptable to use.

  ***Note**:* Windows Storage Server Clusters are not supported for Failover Cluster RAP as a Service.
- 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 servers being reviewed or a member of a domain in the same forest.
- Microsoft® .NET Framework 4.0 — http://www.microsoft.com/en-us/download/details.aspx?id=17851
- Windows PowerShell 2.0 or higher
  - Windows PowerShell 2.0 is part of the Windows Management Framework — http://support.microsoft.com/kb/968929
  - 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.

2. Accounts Rights

- A domain account with the following:
  - Local Administrator permissions on the tools machine and on all cluster nodes in the environment being reviewed.
  - Unrestricted network access from the Tools machine to all cluster nodes in the environment being reviewed. Active Directory access is required as well to check cluster related computer accounts.
  - 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 RAP as a Service client. Some collectors might fail. The account starting the RAP as a Service client must logon to the local machine.

- A Microsoft Account 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. This is also 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.
  - 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.

Internet connectivity is needed in order to complete this RAP as a Service offering

You will require access to the following sites and URLs:

For general use:
https://services.premier.microsoft.com

For 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
***Note:** Some of these URLs cannot be opened using a web browser.*

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

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 listed at How to enable scripting in your browser.

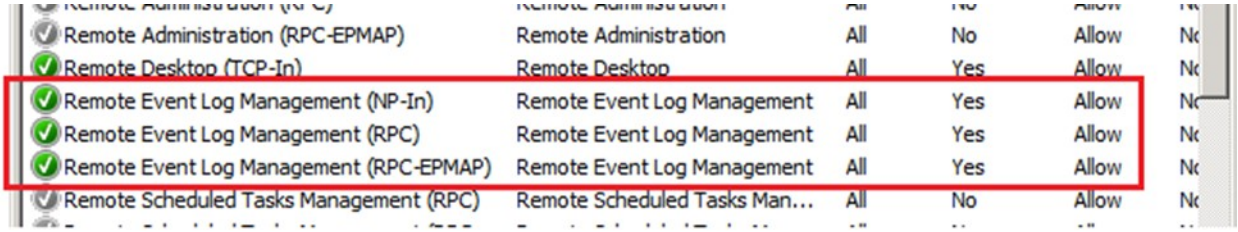
- Internet Explorer is the recommended browser for a better experience with the portal. Ensure Internet Explorer Enhanced Security Configuration (ESC) is not blocking JavaScript on sites. A workaround would be to temporary disable Internet Explorer ESC when accessing the https://services.premier.microsoft.com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

- Unrestricted network access from the Tools machine to all cluster nodes in the environment being reviewed. Active Directory access is required as well to check cluster related computer accounts.
  - 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, and default administrative shares (C$, D$, IPC$). File and printer sharing must be enabled.
  - Ensure that the machine you use to collect data has complete TCP/UDP access, including RPC access to all servers.

- The following services must be started on the target servers:
  - Windows Management Instrumentation
  - Remote Registry
  - Server
  - Workstation
  - Performance Logs & Alerts

- **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 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/R2/2016 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.

Appendix: Data Collection Methods

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

1. Registry Collectors
2. LDAP Collectors
3. EventLogCollector
4. Windows PowerShell
5. FileDataCollector
6. WMI
7. Custom C# Code
8. System Performance Data

1. Registry Collectors

Registry keys and values are read from the RAP as a Service data collection machine for all the Failover Cluster nodes. They include items such as:

- Detailed information from HKEY_LOCAL_MACHINE\Cluster.
- This allows to determine where the Failover Cluster database and log files are located on each node and get detailed information on each of the resources relevant to the proper functions that are highly available. We do not collect all services, only the ones relevant to Failover Cluster.
- Operating System information from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
- This allows to determine Operation System information such as Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 or Windows Server 2016.

2. LDAP Collectors

LDAP queries are used to collect data for the Domain, DCs, nTDSSiteSettings objects, Partitions and other components from Failover Cluster itself. For a complete list of ports required by Failover Cluster, see: http://support.microsoft.com/kb/179442.

3. EventLogCollector

Collects event logs from Failover Cluster nodes. We collect the last 7 days of Warnings and Errors from the Application and System event logs.

4. Windows PowerShell

Collects various information, such as:

- SYSVOL details which is looking for the content of the SYSVOL folder.

5. FileDataCollector

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

6. Windows Management Instrumentation (WMI)

WMI is used to collect various information such as:

- WIN32_Volume

  Collects information on Volume Settings for each node in the cluster. The information is used for instance to determine the system volume and drive letter which allows RAP as a Service for Failover Cluster to collect information on files located on the shared drives.

- Win32_Process

  Collect information on the processes running on each node in the cluster. 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.

8. Custom C# Code

Collects information not captured using other collectors.