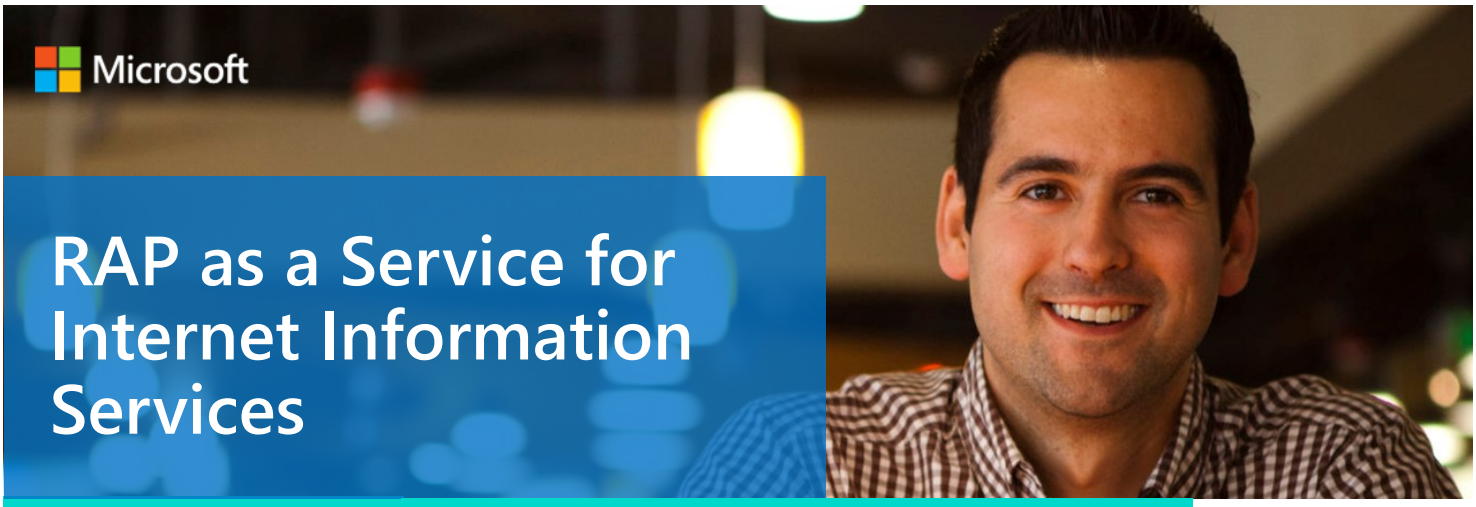


RAP as a Service for Internet Information Services

Prerequisites

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

Last modified:
March 16th, 2017

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 Internet Information Services

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. 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://signup.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 is 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

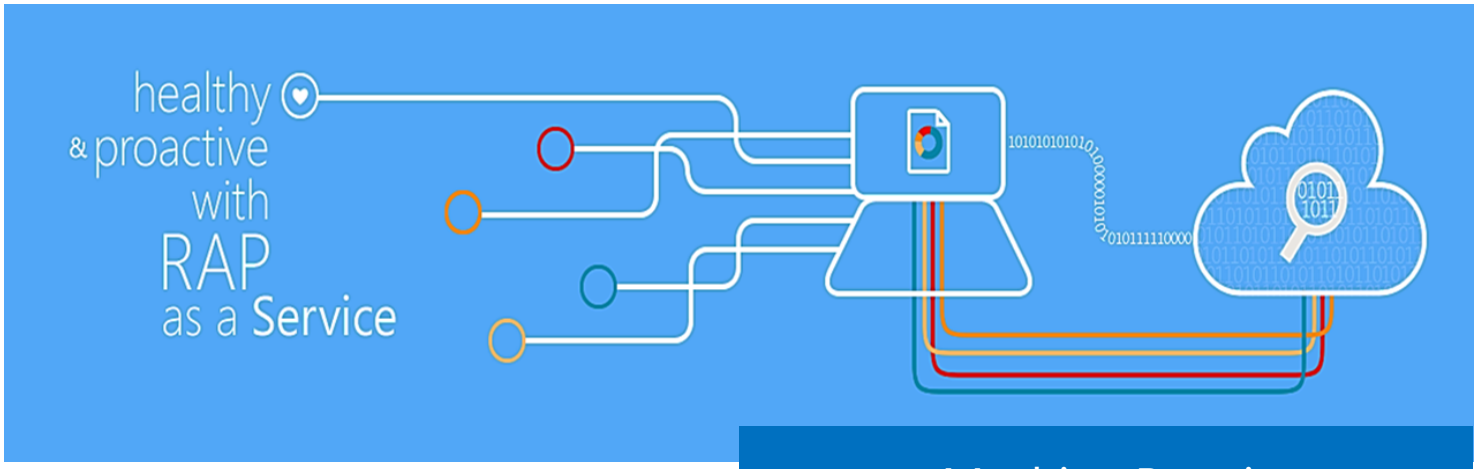
- Tools Machine — Hardware
  - ☐ Server-class or high-end workstation machine running Windows 7, Windows 8, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 or Windows Server 2016.
    ***Note**: Windows Server 2003 and Windows Server 2008 are not supported as Tools machines.*
  - ☐ Minimum: 8GB RAM, 2Ghz dual-core processor
  - ☐ Minimum 5 GB of free disk space, plus up to 6 GB for every target server in the assessed environment during data collection.
- Tools Machine — Software
  - ☐ Microsoft .NET Framework 4.5 installed
  - ☐ Windows PowerShell 3.0 or later installed
  - ☐ Log Parser 2.2 installed
  - ☐ PowerShell Execution policy set to RemoteSigned
- Account Rights:
  - ☐ Member of the local Administrators group on all IIS servers in the environment
  - ☐ Member of the local Administrators group of the tools machine
  - ☐ Unrestricted network access from the Tools machine to all servers
- Additional Requirements
  - ☐ Tools machine joined to the same domain as the environment servers or a trusted domain.
  - ☐ Ensure the machine you use to collect data has IIS 7.5 or greater installed

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/multi-core 2Ghz or higher processors.
- Minimum 8 GB RAM.
- Minimum 5 GB of free space.
- Windows 7, Windows 8, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 or Windows Server 2016.

  Note: Windows Vista, Windows Server 2003 and Windows Server 2008 are not supported as a data collection machine. These exclusions are due to IIS supportability on the data collection machine against the targets.
- 64-bit operating system version.
- At least a 1024x768 screen resolution (higher preferred).
- A member of the same domain as the IIS servers or another domain in the same forest.
- Microsoft® .NET Framework 4.5
- Windows PowerShell 3.0 or later installed
- Log Parser 2.2 installed
- 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 to all target machines to be assessed.
- 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, 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://signup.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.
- Unrestricted network access from the Tools machine to all servers.
- Ensure SMB admin share is accessible (access via \\server\<drive>$). Refer to http://support.microsoft.com/kb/2696547,

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

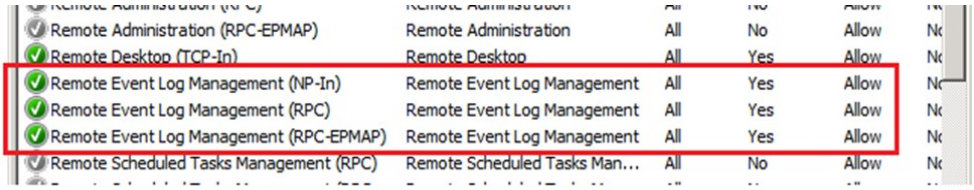
Review the article below for complete information regarding these URLs

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

http://support.microsoft.com/kb/842715, http://support.microsoft.com/kb/954422, http://msdn.microsoft.com/en-us/library/ms143455(v=sql.105).aspx on how to verify this.

- Ensure that the machine you use to collect data has complete TCP/UDP access, including RPC access to all servers and target IIS Servers:
  - TCP Ports 135, 139, 445, 5985, 5986, 1024-65535 (DCOM)
  - UDP Ports 137, 138
- DCOM must be enabled
- The following services must be started on the target servers:
  1. WMI
  2. Remote Registry Service
  3. Windows Remote Management (WinRM) service and PowerShell remoting must be enabled on tools machine and target sever
  4. Server service
  5. Workstation service
  7. Windows Update service
  8. Performance Logs and Alerts service
- The File and Printer Sharing client must be enabled on the network adapter

- **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.

- 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. Unsupported configuration

- IIS Server running with Shared Configuration (http://www.iis.net/learn/web-hosting/configuring-servers-in-the-windows-web-platform/shared-configuration_211)
- IIS Server running in workgroup (not domain joined). This scenario can be accomplished by running the collection process directly on each target server separately.

Appendix: Data Collection Methods

RAP as a Service for Internet Information Services 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. EventLogCollector
3. Windows PowerShell
4. FileDataCollector
5. WMI
6. Discovery Fields

1. Registry Collectors

Registry keys and values are read from all the Internet Information Services servers. They include items such as:

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.
- Operating System information from HKLM\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. EventLogCollector

Collects event logs from Internet Information Services. We collect the last 7 days of Warnings and Errors from the Application and System event logs.

3. Windows PowerShell

Collects various information, such as:

- IIS configuration using Microsoft.Web.Administration API

4. FileDataCollector

Enumerates files in a folder on a remote machine, and optionally retrieves files like IIS logs and HTTP Error logs.

5. Windows Management Instrumentation (WMI)

WMI is used to collect various information such as:

- IIS configuration using Microsoft.Web.Administration API

  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.

6. Discovery Fields

Display Name	Description	Example
Web Server Name(s)	The names of the web servers you wish to include in this analysis. Multiple web servers are separated by semi-colons.	ContosoWeb1;ContosoWeb2

Appendix: Glossary

Term	Description
Web farm	Multiple servers behind a single VIP servicing a website is the definition of a web farm. Each server is independent of each other but usually serving the same application/workload.

Appendix: Enabling Firewall Rules

The most common cause of failure during collection is a firewall blocking the necessary traffic between the tools machine and the target IIS server. This is usually evidenced by errors similar to the following one:

```
Creating an instance of the COM component with CLSID {2B72133B-3F5B-4602-8952-803546CE3344} from the
IClassFactory failed due to the following error: 800706ba The RPC server is unavailable. (Exception from
HRESULT: 0x800706BA)..
```

If the traffic is being blocked by the Windows Firewall on the target server, the following commands can be used to enable RPC traffic on the target IIS server:

```
netsh AdvFirewall Firewall Add Rule Name="_RaaS Remote Web Server Management (RPC)" Dir=In Action=Allow
Program="%SystemRoot%\SYSTEM32\dllhost.exe" Protocol=TCP LocalPort=RPC

netsh AdvFirewall Firewall Add Rule Name="_RaaS Remote Web Server Management (RPC-EPMap)" Dir=In Ac-
tion=Allow Program="%SystemRoot%\system32\svchost.exe" Service=RPCSS Protocol=TCP LocalPort=RPC-EPMap
```

The following commands can be used to remove the firewall rules once collection is complete:

```
netsh AdvFirewall Firewall Del Rule Name="_RaaS Remote Web Server Management (RPC)"
netsh AdvFirewall Firewall Del Rule Name="_RaaS Remote Web Server Management (RPC-EPMap)"
```