RAP as a Service for Windows Server Hyper-V

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 Windows Server Hyper-V

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 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

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

2. Activation

- ☐ Ensure access to http://corp.sts.microsoft.com
- ☐ Ensure access to http://live.com

3. Data Collection

- ☐ The data collection is done from a machine (a.k.a. Tools Machine or Data Collection Machine) which is not part of the Hyper-V environment that is analyzed but is joined to the same domain. The details regarding the requirements for the Tools Machine are provided in the subsequent pages of this document.
- ☐ Data is collected by the Tools Machine by connecting to each of the Hyper-V servers to be assessed, 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.
- ☐ Specific firewall requirements are listed later in this document
- ☐ If System Center Virtual Machine Manager (SCVMM) is used to manage the Hyper-V environment, then the SCVMM Console is installed on the data collection machine, and is updated to the same version and rollup used on the SCVMM server.
- ☐ Only a single tools machine is supported, collecting from multiple machines will exclude each others data collection.

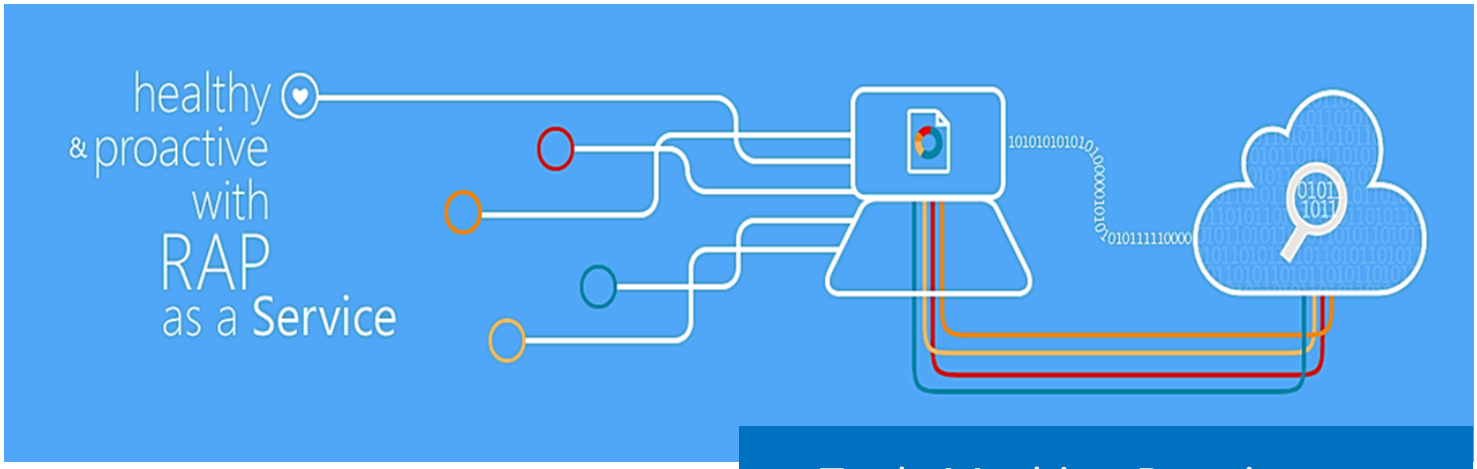
The Appendix Data Collection Methods details the methods used to collect data.

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.



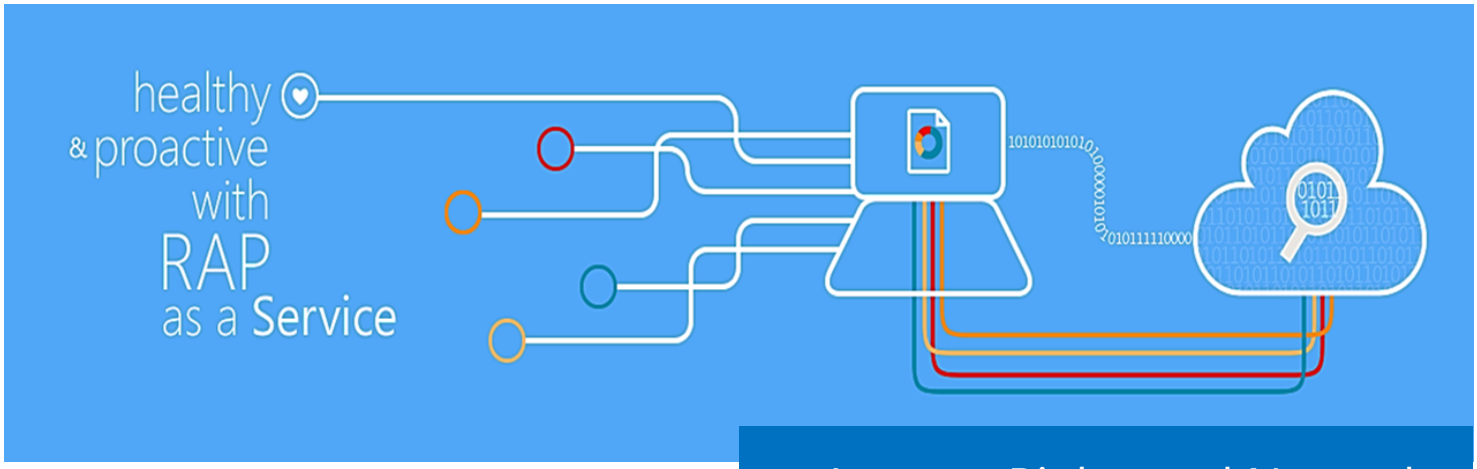
Tools Machine Requirements and Account Rights

1. Hardware and Software

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

- Minimum dual-core 2Ghz processor — Recommended 4-core or higher processors.
- Minimum 8 GB RAM
- Minimum 20 GB of free disk space.
- Windows 7 SP1 / Windows 8 / Windows 8.1, or Windows Server 2008 R2 SP1 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016. Windows Server 2008 SP2, Window Server 2008 R2 RTM are not supported as Tools machines.

  ***Note**: To successfully collect all 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 8.1 / Windows 10 or Windows Server 2012 R2 / 2016 is acceptable to use.*
- Must be 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 trusted domain.
- Microsoft® .NET Framework 4.5 — https://www.microsoft.com/en-us/download/details.aspx?id=30653
- PowerShell 3.0 or 4.0
  - PowerShell 3.0 is part of the Windows Management Framework 3.0: http://support.microsoft.com/kb/2506143
  - PowerShell 4.0 is part of the Windows Management Framework 4.0: http://go.microsoft.com/fwlink/?LinkId=293881
  - On Windows Server 2012 and Windows Server 2012 R2 / 2016, the Windows PowerShell 2.0 engine feature must be enabled
- If System Center Virtual machine Manager (SCVMM) is used to manage the Hyper-V environment, then the SCVMM console must be installed on the data collection machine, and updated to the same version and Update Rollup as is installed on the SCVMM servers.
- Networked "Documents" or redirected "Documents" folders are not supported. Local "Documents" folder on the data collection machine is required.



Account Rights and Network Requirements

2. Account Rights

- A domain account with the following:
  - Local Administrator permissions on the tools machine and on all Hyper-V servers in the environment.
  - Unrestricted network access from the Tools machine to all Hyper-V servers

  If SCVMM is in use in the environment, then the following is also needed:
  - Local Administrator permissions on the SCVMM servers
  - The account must be in the "Administrator" user role within SCVMM.
  - Read access to the targeted SCVMM Database

  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

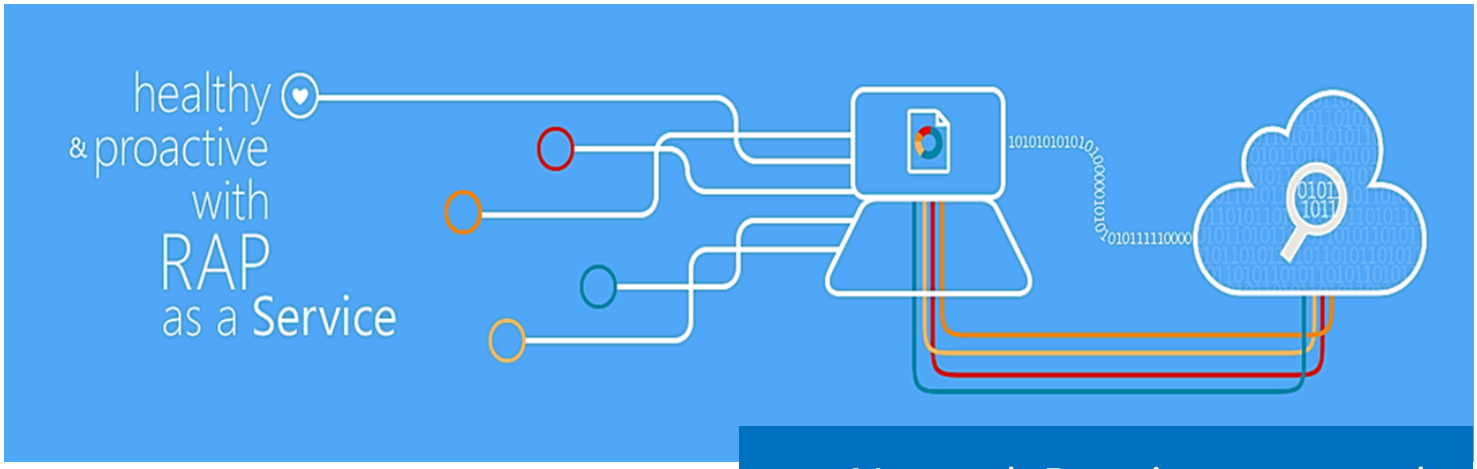
- A Windows Live ID for each user account to logon to the Premier Proactive Assessment Services portal (https://services.premier.microsoft.com). This is the RAP as a Service portal where you will activate your access token, download the toolset and fill out the operational survey. This is also the URL 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.

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 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, and default administrative shares (C$, D$, IPC$).

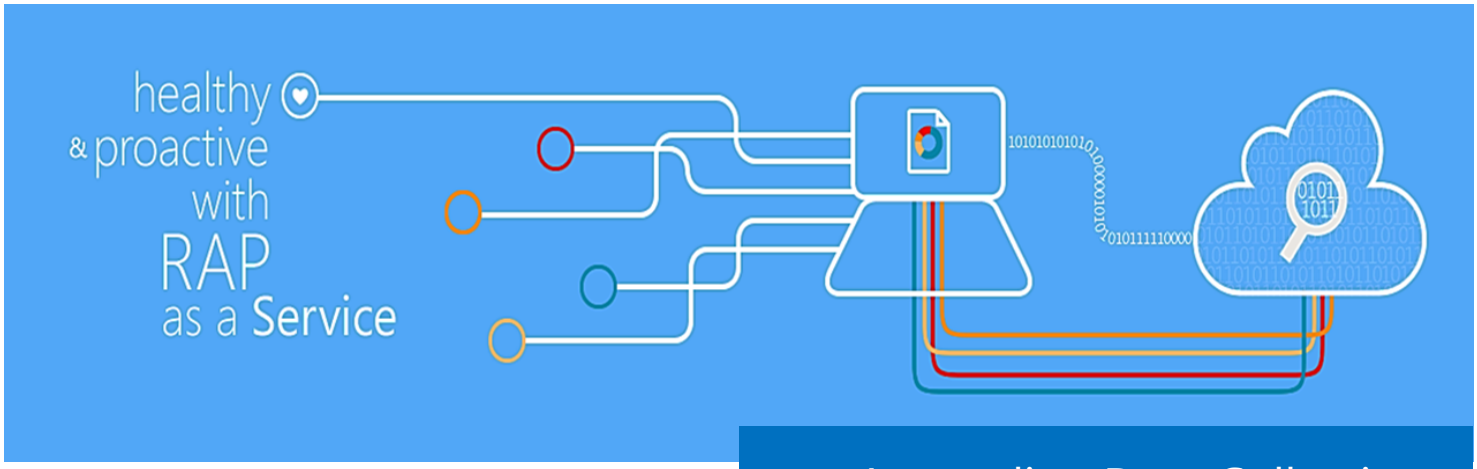


Network Requirements and Connectivity Testing

- Firewall Rules: The following firewall rules need to configured on the tools machine and on all target machines.
  - Inbound Firewall rule: Performance Logs and Alerts (DCOM-In)
  - Inbound Firewall rule: Performance Logs and Alerts (TCP-In)
  - Inbound Firewall rule: Remote Event Log Management (RPC)
  - Inbound Firewall rule: Remote Management (RPC)
  - Inbound Firewall rule: Windows Management Instrumentation (DCOM-In)
  - Inbound Firewall rule: Windows Management Instrumentation (WMI-In)
  - Inbound Firewall rule: Remote Scheduled Tasks Management (RPC)
  - Inbound Firewall rule: Windows Remote Management (WinRM)

- Ensure that the machine you use to collect data has complete TCP/UDP access, including RPC access to all servers.
  - TCP 135: RPC Endpoint Mapper
  - UDP 137: NetBIOS name service
  - UDP 138: NetBIOS mailslot
  - TCP 139: NetBIOS session service /SMB
  - TCP 445: SMB over sockets/TCP
  - TCP 5386/5387: Windows Remote Management (WinRM)
  - TCP 49152-65535: Dynamic Ports used by RPC/DCOM/WMI
  - TCP 8100: VMM management port

- The following services must be started on the target servers:
  - WMI
  - Remote Registry service - on Windows Server 2012: Automatic (Trigger Start)
  - Server service
  - Workstation service
  - File and Printer Sharing service
  - Performance Logs and Alerts service
  - Windows Remote Management (WS-Management)



Appendix - Data Collection Methods

- 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.

Data Collection Methods

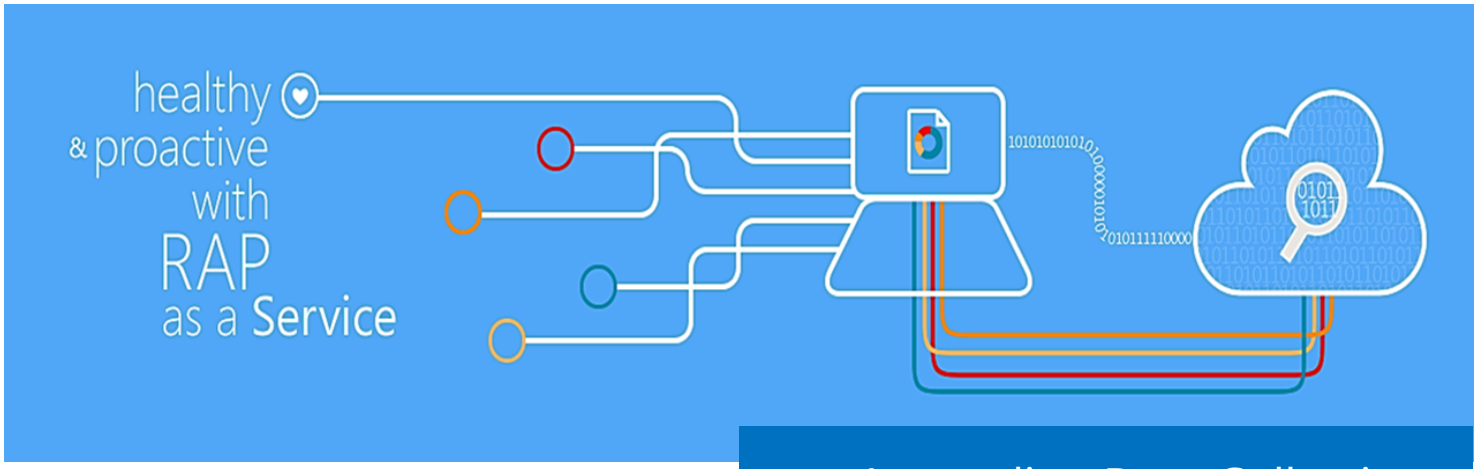
RAP as a Service for Windows Server Hyper-V uses multiple data collection methods to collect information. This section describes the methods used to collect data from your environment. No VB scripts are used to collect data. Data collection uses workflows and collectors. The collectors are:

1. Registry Collectors
2. LDAP Collectors
3. EventLogCollector
4. Windows PowerShell
5. FileDataCollector
6. WMI
7. System Performance Data

1. Registry Collectors

Registry keys and values are read from all the Hyper-V Servers. They include items such as:

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.
- This allows to determine the detailed informationon each service relevant to the proper function of Hyper-V. We do not collect all services, only the ones relevant to Hyper-V.
- Virtualization Configuration from HLKM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization
- This allows to determine the server wide Hyper-V configuration Settings



Appendix - Data Collection Methods

2. LDAP Collectors

LDAP queries are used to collect data for the Computer objects from AD. For a complete list of ports required by AD, see: http://support.microsoft.com/kb/179442.

3. EventLogCollector

Collects event logs from Hyper-V servers. We collect the last 7 days of Warnings and Errors from the System, Application event logs as well as the "Microsoft-Windows-Hyper-V-*", "Microsoft-Windows-FailoverClustering-Operational" and "Microsoft-Windows-VHDMP-Operational" event logs.

4. Windows PowerShell

Collects various information, such as:

- Details and configuration of virtual hard disk files.
- For more complicated WMI collection and parsing of some WMI output.

5. FileDataCollector

Enumerates files in a folder on a remote machine, and collects information on those files.

- This is used to check file versions of key Windows and Hyper-V drivers, DLLs and EXE files

6. Windows Management Instrumentation (WMI)

WMI is used to collect various information such as:

- WIN32_Volume

  Collects information on Volume Settings for each server. The information is used for instance to determine the system volume and drive letter which allows RAP as a Service for Hyper-V to collect information on files located on the system drive.

- MSVM_ComputerSystem

  Collect general information on the virtual machines.

- Win32_LogicalDisk

  Used to collect information on the logical disks. We use the information to determine the amount of free space on the disks where the virtual machine data files are located.