RAP as a Service for Windows Desktop

Prerequisites

How to prepare for your RAP as a Service for Windows Desktop

The tools machine is used to connect to each of the Devices in your environment and retrieves information from them by communicating over Remote Procedure Call (RPC), Server Message Block (SMB), Lightweight Directory Access Protocol (LDAP) and Distributed Component Object Model (DCOM). Once the data is collected and submitted to the RAP as a Service infrastructure and the operational interview is completed the data will be analyzed and can be viewed at the RAP as a Service portal.

Internet connectivity is needed to access the RAP as a Service portal, activate your account, download the toolset, and submit data.

A checklist of prerequisite actions follows. Detailed steps and test scripts are included later in this document.

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 devices
3. Submit the collected data to the RAP as a Service portal
3. Complete the operational survey

Data collected and submitted via secure transfer to the RAP as a Service infrastructure is analyzed using our RAP as a Service expert system.

This document was last updated September 15th, 2016. To ensure you have the latest version of this document , check here: http://www.microsoft.com/en-us/download/details.aspx?id=34698

Checklist

Please ensure the following items have been completed before 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 https://signup.live.com.
- ☐ Ensure access to https://services.premier.microsoft.com.
- ☐ Ensure the internet browser on the tools machine has JavaScript enabled. If you need more information follow the steps on How to enable scripting in your browser. Internet Explorer is the supported and recommended browser to access the portal.
- ☐ Ensure access to https://ppas.uservoice.com for access to the Support Forum and Knowledge Base Articles.

2. Activation

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

3. Data Collection

- ♦ Hardware — Tools machine
  - ☐ High-end class machine with at least 8 GB RAM, dual 2 GHz processor and 5 GB of free disk space, joined to the same domain as the target machines or a trusted domain.

Tools Machine	Target Machine (all Service Pack levels supported)
Windows 7 SP1 and higher or Server 2008 R2 SP1 and higher	Windows Vista and higher

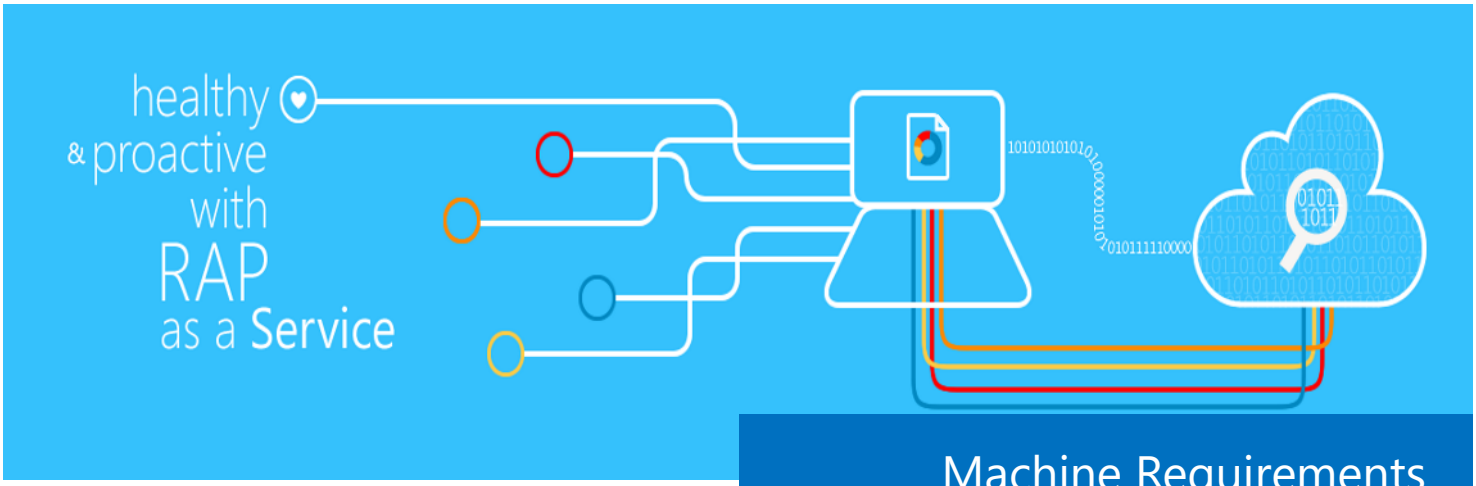
- ♦ Software — Tools machine
  - ☐ Microsoft .NET Framework 4.5 installed
  - ☐ Windows PowerShell 3.0 or later installed
- ♦ Account Rights
  - ☐ Domain user with Administrator permissions on all destination targets.
- ♦ Additional Requirements
  - ☐ Please check the firewall rules and configure necessary services.
  - ☐ Please check that the default Admin shares are not disabled.
- ♦ Additional requirements for Windows Server 2012 Servers, Windows 8 or higher — Tools machine
  - ☐ Windows 8/2012 Feature .Net Framework 3.5 (includes .NET 2.0 and 3.0) enabled.

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

Once you have completed these prerequisites you are ready to start the RAP as a Service.



Machine Requirements and Account Rights

1. Hardware and Software

A tools machine equipped with the following:

- Minimum single 2 GHz processor — Recommended dual/multi-core 2 GHz or higher processors.
- Minimum 8 GB RAM.
- Minimum 5 GB of free disk space.
- Windows 7, Windows Server 2008 or higher.
- Can be 32-bit or 64-bit operating system.
- At least a 1024x768 screen resolution (higher preferred).
- A member of the same domain as target hosts or a member of a trusted domain.
- Microsoft® .NET Framework 4.5.
- Windows PowerShell 3.0 or higher.
  http://support.microsoft.com/kb/968929
  - Windows PowerShell 3.0 is part of the Windows Management Framework 3.0.
- A networked or redirected “Documents” folder on the tools machine is not supported.

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 to log on to the Premier Proactive Assessment Services portal. https://services.premier.microsoft.com.
  - Here you can:
    - Download the toolset to be installed on the data collection machine.
    - Activate your access token.
    - Complete the operational survey.
  - If you don’t have a Microsoft account, you can create one at https://signup.live.com.
  - Please contact your TAM or SDM if the token in your Welcome email has expired or can no longer be activated. Tokens expire after 10 days. Your TAM or SDM can provide new activation tokens for additional people.

WARNING: Do not use the Run As feature to start the RAP as a Service toolset. Some collectors might fail. The account starting the RAP as a Service client must logon to the local machine.

3. Network and Remote Access

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

- Ensure that the Internet browser on the data collection 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.
- Short name resolution must work from the tools machine. This typically means making sure DNS suffixes for all
  domains in the forest are added on the tools machine.
- The following services must be started on the target hosts:
  - Server service
  - Windows Update
    - Windows 8 and higher: Manual (Trigger Start)
  - WMI Management Instrumentation
  - Workstation
- Remove network access restriction to the target clients or configure the firewall rules to meet the following conditions:

Port or Protocol	Notes
ICMP	
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 1024—65535	Dynamic Ports used by RPC/DCOM/WMI

  - This includes access through any firewalls and router ACLs that might be limiting traffic to any host. This also
    includes remote access to Remote Registry service, WMI services and default administrative shares (C$, D$, IPC$).

4. Additional Requirements

- **Firewall Rules:**
  The following firewall rules need to configured on the tools machine and on all target machines:
  - 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)
- **Scan for missing Windows Updates:**
  One of the following needs to be configured on the tools machine:
  - Access to the Windows Update service in the Internet without the need for additional authentication.

  or
  - Place an up to date wsusscn2.cab file at %LOCALAPPDATA%\RAPaaSWD
    http://go.microsoft.com/fwlink/?LinkId=76054

5. Additional requirements for Windows 8, Windows Server 2012 or higher

- **Features:**

  The following features needs to be enabled:

  * .Net Framework 3.5 (includes .NET 2.0 and 3.0)

6. Windows PowerShell commands to validate the environment is ready

- Check if the Documents folder is redirected on the tools machine

```
(Get-ItemProperty -path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" -name "Personal").Personal.toString()

Expected  Result: C:\Users\<UserName>\Documents
```

- Check computer DNS name resolution against every target machine

```
[System.Net.Dns]::GetHostByName("<ComputerName>").HostName

Expected  Result: <ComputerName>.dns.name
```

- Check computer Registry FQDN name and WMI against every target machine

```
get-wmiobject Win32_ComputerSystem -computer localhost | fl Name,Domain

Expected  Result:

                    Name   : <ComputerName>
                   Domain : dns.name
```

- Check if administrative shares are available against every target machine

```
get-wmiobject WIN32_Share -computer "<ComputerName>" | ?{$_.Name -eq "C$"} | FL Name

                    Expected  Result: Name : C$
```

- Check Scheduled Tasks access against every target machine

```
$([xml](schtasks /query /XML ONE /S "<ComputerName>")).Tasks.Task.Count

                    Expected  Result: > 0
```

Appendix A: Data Collection Methods

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

1. Registry Collectors
2. Xperf
3. EventLogCollector
4. Windows PowerShell
5. FileDataCollector
6. WMI
7. Nltest

1. Registry Collectors

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

- Service information from HKLM\SYSTEM\CurrentControlSet\Services
- Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

2. Xperf

Xperf is a tool that is part of the Windows Performance Toolkit that can create boot time statistics. With Xperf the boot time is evaluated and the top 10 processes that utilize disk and/or cpu most.

3. EventLogCollector

Collects event logs from target machines. We mostly collect the last 7 days of different event logs.

4. Windows PowerShell

Collects various information, such as:

- BCD store boot configuration Data
- Defragmentation rate

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
- Win32_Process
- Win32_LogicalDisk

7. Nltest

Nltest is a build-in tool that can discover the Domain controller for each client computer. This is information is used to check Domain Controller connectivity.

Appendix B: Frequently asked questions

1. Am I able to review the data that has been collected before it gets submitted?

Yes, it is possible to review the collected data before submission. The data is stored in clear text xml format in the following location: %UserProfile%\Documents\RaaS\RaaSWD_*\DataModel.
This folder contains subfolders that represent the targets and in these folders the collected information is stored. Once the data has been collected it can be reviewed before the submit process was initiated.

2. Is it possible to remove data that has been collected so that it will not be submitted?

No, it is not possible and not supported to remove data manually. Please open a support case at https://ppas.uservoice.com to get assistance.
To avoid submission of data from specific targets it is possible to close the toolset, delete everything inside %UserProfile%\Documents\RaaS\RaaSWD_* and recollect excluding the specific targets.