How to prepare for your Offline Assessment for Windows Server

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 the operational interview is completed the Offline Assessment tool will analyze the data locally.

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. Complete the operational survey

All data collection and analysis is done locally on the tools machine.

No data is transported outside your Windows Server environment to help protect your data. Your data is analyzed using our RAP expert system that is part of the Offline Assessment client.

Internet connectivity is needed to:
* Activate your account
* Download the toolset

This document was last updated February 7th, 2017. To ensure you have the latest version of this document, check here: http://download.microsoft.com/download/1/C/1/1C15BA51-840E-498D-86C6-48D35D33C79E/Prerequisites_Offline_WS.pdf
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 portal to download the toolset.
     - 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

2. 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.

<table>
<thead>
<tr>
<th>Tools Machine</th>
<th>Target Machine (all Service Pack levels supported)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 and higher</td>
<td>Windows Server 2008 and higher</td>
</tr>
</tbody>
</table>

   - 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 and above Servers — Tools machine

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 Offline Assessment.
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 Server 2008 or higher.
- 64-bit operating system version.
- Office 2013 or higher
- 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](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.

  **WARNING:** Do not use the Run As feature to start the RAP as a Service toolset. Some collectors might fail.

  The account starting the Offline Assessment client 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](https://services.premier.microsoft.com)). This is where you where you will activate your access token and download the toolset.

  If you don’t have one already, you can create one at [http://login.live.com](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

- 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: Manual (Trigger Start)
  * WMI Management Instrumentation
- Remove network access restriction to the target clients or configure the firewall rules to meet the following conditions:

<table>
<thead>
<tr>
<th>Port or Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td>TCP 135</td>
<td>NetBIOS name service</td>
</tr>
<tr>
<td>UDP 137</td>
<td>NetBIOS mailslot</td>
</tr>
<tr>
<td>TCP 139</td>
<td>NetBIOS session service /SMB</td>
</tr>
<tr>
<td>TCP 445</td>
<td>SMB over sockets/TCP</td>
</tr>
<tr>
<td>TCP 1024—65535</td>
<td>Dynamic Ports used by RPC/DCOM/WMI</td>
</tr>
</tbody>
</table>

* 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 be 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:
  The following needs to be configured on the tools machine:
  * Place an up to date wsusscn2.cab file at %LOCALAPPDATA%\RapaaSServer
    http://go.microsoft.com/fwlink/?Linkid=76054

5. Additional requirements for 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]::GetHostName("<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: Data Collection Methods

Offline Assessment for Windows Server 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
   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. EventLogCollector
   Collects event logs from target machines. We mostly collect the last 7 days of different event logs.

3. Windows PowerShell
   Collects various information, such as:
   ♦ BCD store boot configuration Data
   ♦ Defragmentation rate

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

5. Windows Management Instrumentation (WMI)
   WMI is used to collect various information such as:
   ♦ Win32_Volume
   ♦ Win32_Process
   ♦ Win32_LogicalDisk