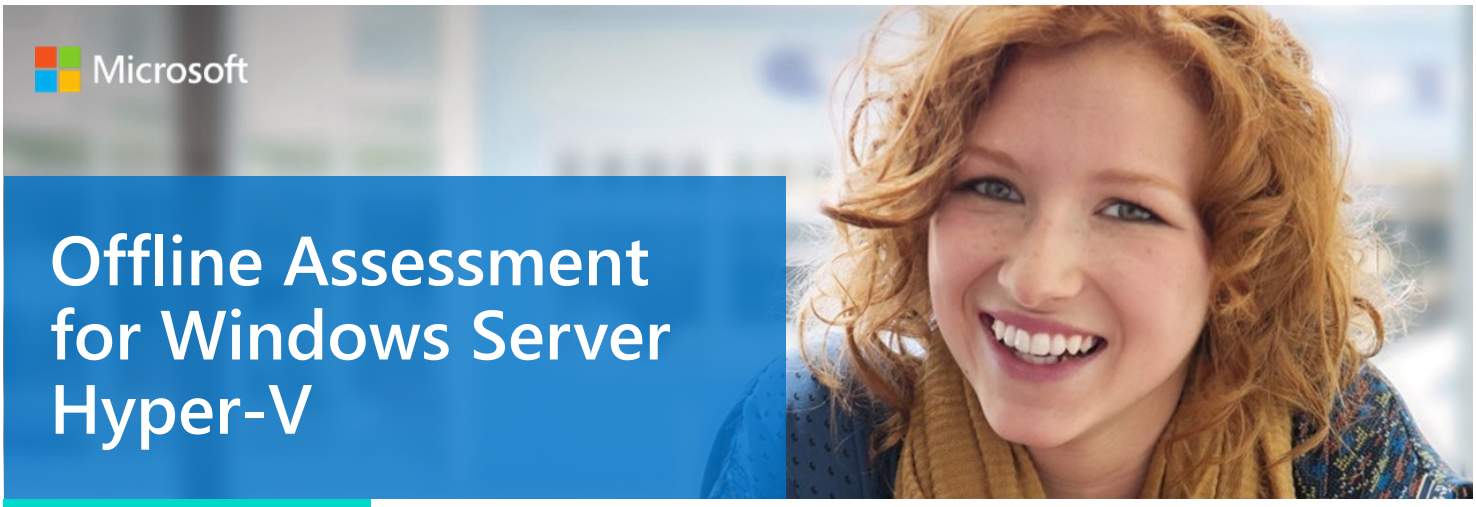


Offline Assessment for Windows Server Hyper-V

Prerequisites

How to prepare for your Offline Assessment for Windows Server Hyper-V

The tools machine is used to connect to each of the servers in your environment and retrieves information from them, communicating over Remote Procedure Call (RPC), Server Message Block (SMB), Lightweight Directory Access Protocol (LDAP), Kerberos, Windows Management Instrumentation (WMI) 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.

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

A checklist of the prerequisite actions follows this section. Each item links to any additional software required
for the tools machine, and detailed steps are included later in this document.

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

Checklist

Ensure that 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

Internet connectivity is needed to:

- *Activate your account*
- *Download the toolset*

2. Data Collection

a. Tools machine hardware and Operating System:

- ☐ Server-class or high-end workstation machine running Windows Server 2012 R2 / 2016 Windows Server 2012 / Windows Server 2008 R2 / Windows Server 2008 or Windows 10 / Windows 8.1 / Windows 8 / Windows 7.

  Note: Computers running Windows XP and Windows Server 2003 are not supported as Tools machines.

- ☐ Minimum: 8GB RAM, 2GHz dual-core processor, 50 GB of free disk space plus up to 7 GB for every 100,000 objects in the assessed environment during data collection.
- ☐ Joined to the same forest of the Hyper-V host/cluster to be assessed.
- ☐ 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 4.5 installed
- ☐ Windows PowerShell 3.0 or later installed
- ☐ Microsoft Office
- ☐ 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.

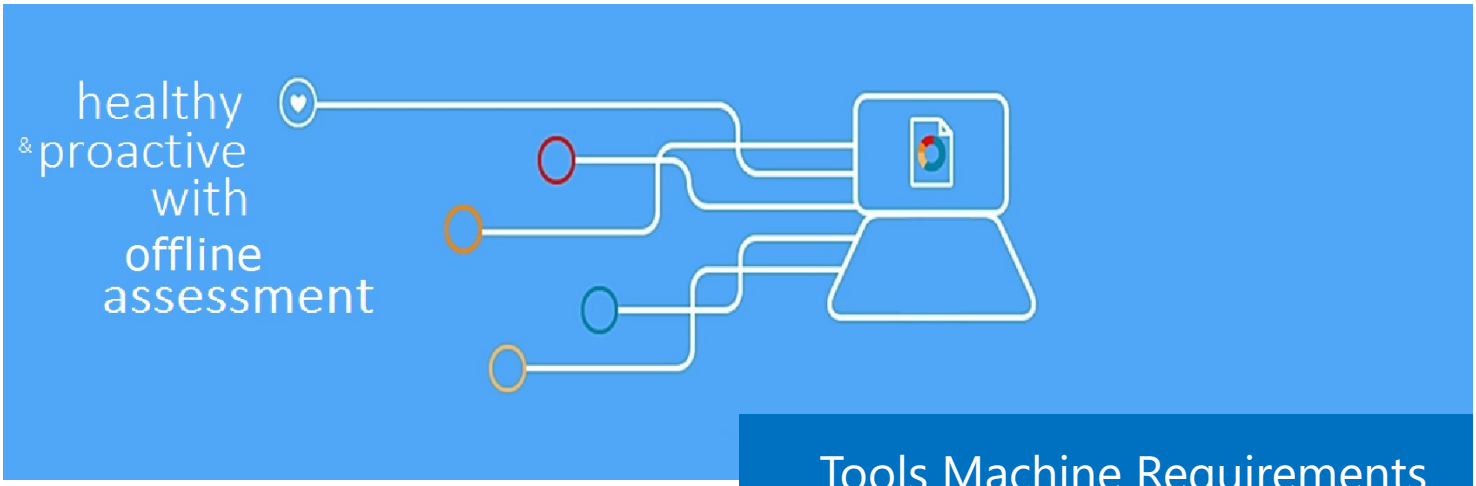
c. Account Rights:
- ☐ Administrator account with Local Admin access to every server in the environment that is being assessed
- ☐ Unrestricted network access to every assessed server in the environment

d. Firewall Changes:
- ☐ Configure the Hyper-V servers' firewalls for Remote Event Log Management
- ☐ 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 (WS-MAN/WinRM)

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

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

Once you have completed these prerequisites, you are ready to start the Offline Assessment.



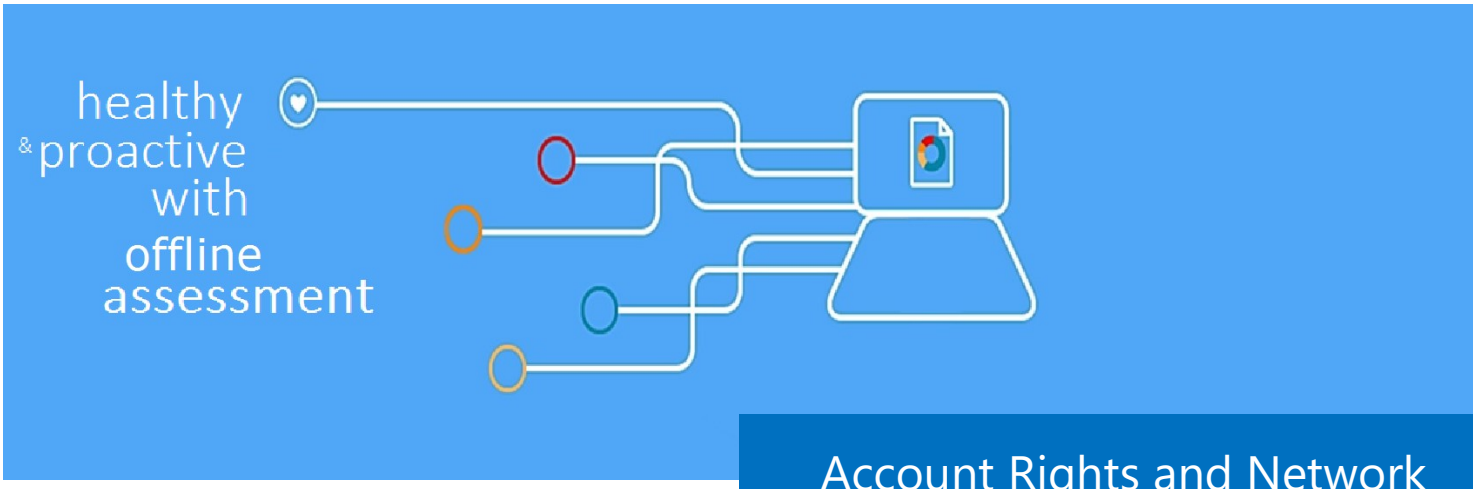
Tools Machine Requirements and Account Rights

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 4 GB RAM—Recommended 8 GB RAM.
- Minimum 5 GB of free disk space.
- Windows 7 SP1/ Windows 8 / Windows 8.1 / Windows 10, or Windows Server 2016 / Windows Server 2008 R2 SP1 / Windows Server 2012 / Windows Server 2012 R2. Windows Server 2003, 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 or Windows Server 2012 R2 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
- 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

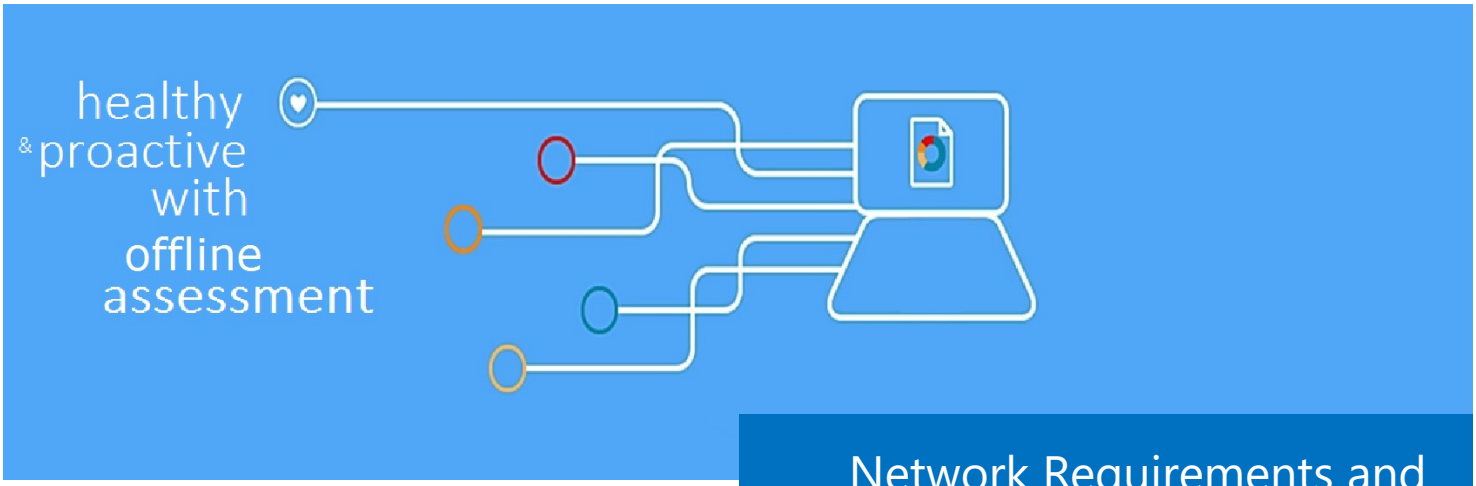
- A domain account with the following:
  - Local Administrator permissions on the tools machine and on all Hyper-V servers in the environment.
  - Unrestricted network access from the Tools machine to all Hyper-V servers

  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

  - 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
  - Ensure that the machine you use to collect data has complete TCP/UDP access, including RPC access to all assessed servers, for the following protocols: RPC, WMI, DCOM, LDAP, SMB, WinRM, Remote Registry, Remote Event Log Management.

  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

- A Microsoft Account is required to activate and sign in to the Premier Proactive Assessment Services portal (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
- 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.

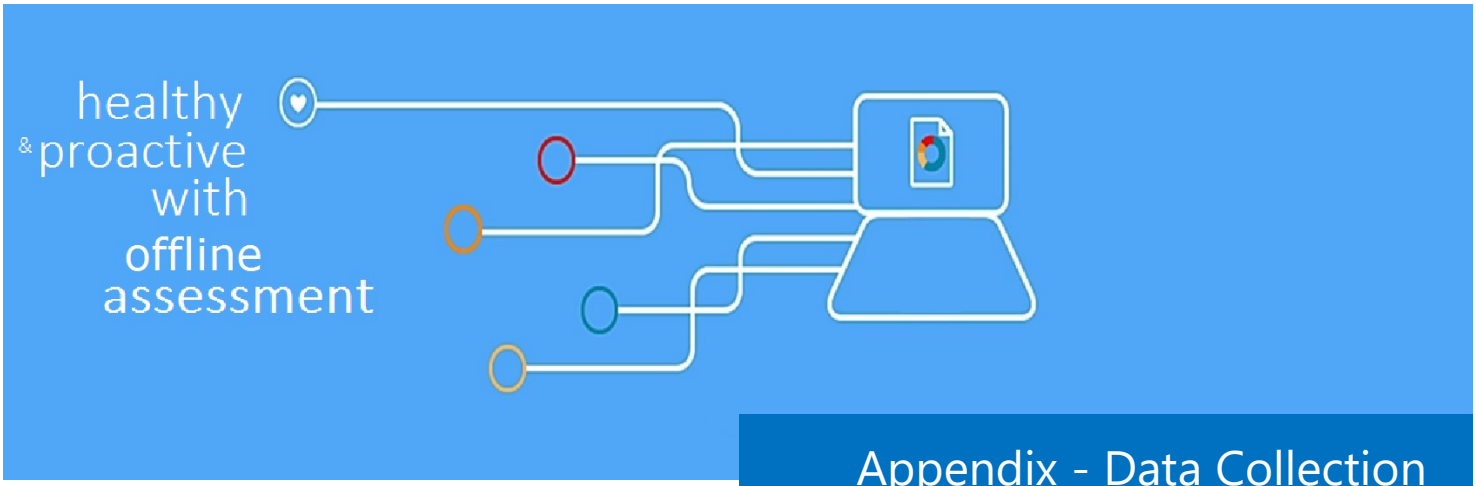


Network Requirements and Connectivity Testing

- 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)

- 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.



Appendix - Data Collection Methods

Offline Assessment for Hyper-V uses multiple data collection methods to collect information. This section describes the methods used to collect data from a Hyper-V environment. No Visual Basic scripts are used to collect data. Data collection uses workflows and collectors. The collector types are:

1. Registry Collectors
2. LDAP Collectors
3. Event Log Collector
4. Windows PowerShell
5. File Data Collector
6. WMI
7. SQL Data Collector
8. System Performance Collector

1. Registry Collectors

Registry keys and values are read from the data collection machine and all assessed servers. They include but are not limited to items such as:

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.
- Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
  This allows to determine Operating System information such as Windows Server 2012, Windows Server 2008.

2. LDAP Collectors

LDAP queries are used to collect data for the cluster objects and other components from Active Directory Domain Services (AD DS) itself. For a complete list of ports required by AD DS, see: http://support.microsoft.com/kb/179442.

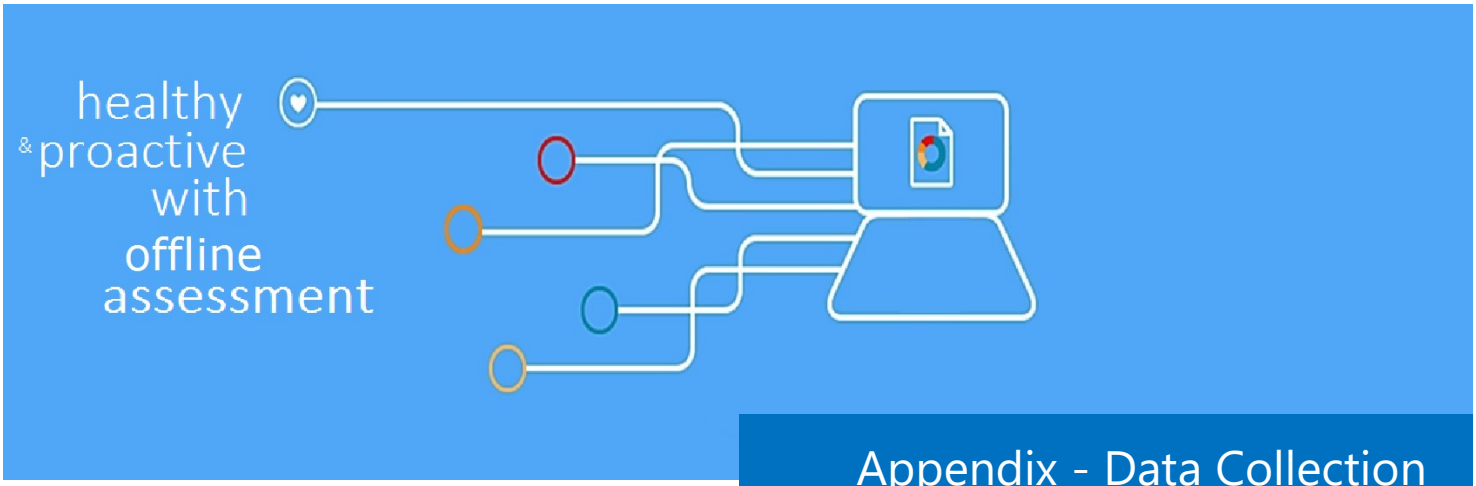
3. Event Log Collector

Collects event logs from Hyper-V Servers. We collect the last seven days of Warnings and Errors from the application, Hyper-V-*, VHDMP and System event logs.

4. Windows PowerShell

Collects different information such as:

- Virtual machine's virtual disk information
- For more complicated WMI collection and parsing of some WMI output.
- Querying the SCVMM server for configuration and settings



Appendix - Data Collection Methods

5. File Data Collector

Enumerates files in a folder on a remote machine, collecting file metadata (File version and size information), 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 server to be assessed. The information is used for instance to determine the system volume and drive letter which allows the client to collect information on files on the system drive.
- Win32_Process
  Collect information on the processes running on each assessed server. 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.

7. SQL Data Collector

- Queries the VMM Database on the SQL server used by VMM

8. System Performance Data

- Queries detailed performance information from all Hyper-V servers, and basic performance information from VMM servers, VMM Library servers, and VMM SQL servers.