Offline Assessment for Exchange

Prerequisites

How to prepare for your Offline Assessment for Exchange

You will hear many references to your *Tools* machine. The *Tools* machine is used to connect to each of your Exchange Servers and retrieve configuration and health related information from them.

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 Exchange Organization
3. **Analyze and review findings from the collected data**

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

Verifying Environment Qualification for Rap as a Service for Exchange Server

The RAP as a Service for Exchange Server is currently optimized for analyzing environments containing Exchange Server 2013, Exchange Server 2016, and Exchange Server 2019.

Not Supported:

Servers with Exchange Server 2007 or prior versions of Exchange Server.

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.

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

This document was last updated August 24, 2021. To ensure you have the latest version of this document , check here:
https://go.microsoft.com/fwlink/?LinkId=619033

Checklist

Please ensure the following items have been completed before starting your engagement.

1. Data Collection

a. Tools machine hardware and Operating System:

- □ Server-class or high-end workstation machine running Windows 8/Windows 10 (all Exchange Servers must be Exchange 2016 or above) or Windows Server 2012/Windows Server 2012 R2/Windows Server 2016 (all Exchange Servers must be Exchange 2016 or above)

  Minimum: 8GB RAM, 2Ghz dual-core processor, 10 GB of free disk space
- □ Joined to a domain in the forest where Exchange Server is installed

b. Software for Tools machine:

- □ Microsoft .NET Framework 4.8 or newer installed.
- □ Windows PowerShell 2.0, 3.0, or 4.0 installed. **NOTE:** Windows PowerShell 5.0 is not currently supported unless all Exchange servers are Exchange Server 2016 or above.
- □ PowerShell Execution policy set to RemoteSigned

c. Account Rights:

- □ At least Exchange View Only Administrator permissions to the Exchange organization
- □ Local Administrator permissions on the Tools machine and on all Exchange servers in the organization
- □ Unrestricted network access to every server in the environment
- □ The account being used and the tools machine must not be part of an auto logoff policy. If logoff is forced automatically data collection will be interrupted.

d. Exchange Server requirements:

All Exchange Servers must have the following services running and accessible from the Tools machine:

- □ Windows Management Interface (WMI) service
- □ Remote Registry service
- □ Server service
- □ Workstation service
- □ File and Printer Sharing service
- □ Performance Logs and Alerts service
- □ Enable Message Tracking on Exchange Servers

2019 - https://technet.microsoft.com/en-us/library/aa997984(v=exchg.160).aspx

2016 - https://technet.microsoft.com/en-us/library/aa997984(v=exchg.160).aspx

2013 - http://technet.microsoft.com/en-us/library/aa997984(v=exchg.150).aspx

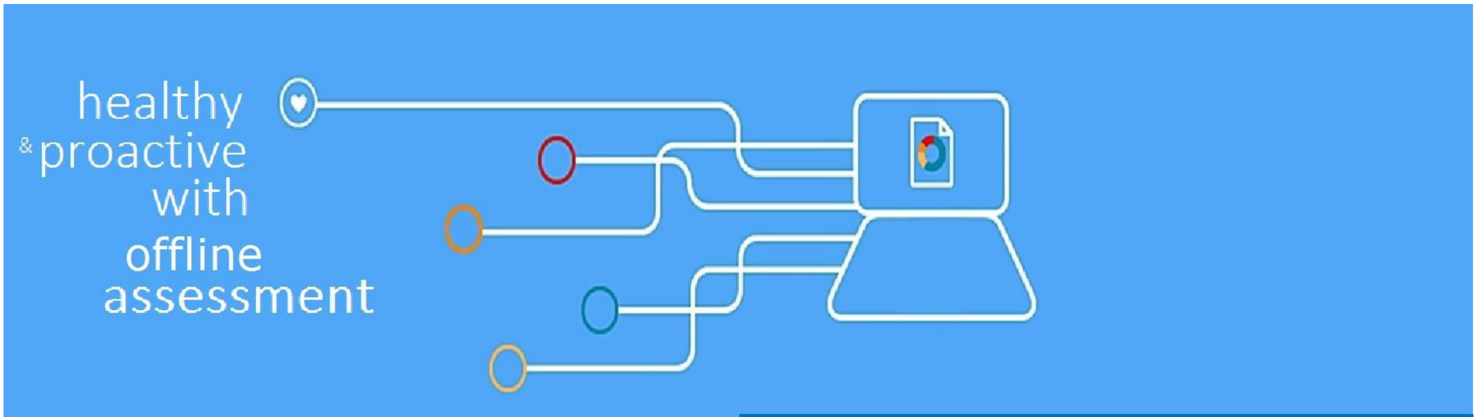
e. Additional Requirements for Windows Server 2008 (and later) servers:

- □ Configure the servers’ firewalls for Remote Event Log Management

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.



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-core/multi-core 2Ghz or higher processors
- Minimum 8 GB RAM
- Minimum 10 GB of free disk space

***Note**: Use the chart below to reference the Exchange/OS version combinations in your environment with acceptable operating systems for the tools machine. You should select a tools machine OS that has YES for all Exchange/OS version combinations found in your environment.*

Exchange/ OS Combination Toolset OS	Exchange 2013 on Server 2008 R2/ 2012 /2012 R2	Exchange 2016 on Server 2012 / 2012 R2	Exchange 2016 on Server 2016	Exchange 2019 on Server 2019
Windows 8	YES	YES	YES	YES
Server 2012	YES	YES	YES	YES
Server 2012 R2	YES	YES	YES	YES
Server 2016	NO	YES	YES	YES
Windows 10	NO	YES	YES	YES

- Can be 32-bit or 64-bit operating system (64-bit recommended)
- At least a 1024x768 screen resolution (higher preferred)
- Joined to a domain in the forest where Exchange Server is installed
- Microsoft® .NET Framework 4.8

- ♦ Windows PowerShell 2.0 or higher
  - ∗ Windows PowerShell 2.0 is part of the Windows Management Framework — http://support.microsoft.com/kb/968929
  - ∗ The execution policy for PowerShell should be set to remotesigned on both the tools machine and the Exchange Servers.
  - ∗ The execution policy settings can be verified using "*get-executionpolicy –list*" in a PowerShell command window.
- ♦ Networked "Documents" or redirected "Documents" folders are not supported. Local "Documents" folder on the data collection machine is required.
- ♦ Office 2013 or higher

2. Accounts Rights

- ♦ A domain account with the following:
  - ∗ Local Administrator permissions on the Tools machine and on all Exchange servers in the organization
  - ∗ At least Exchange View Only Administrator permissions to the Exchange organization
  - ∗ Public Folder Admin permissions

  Note: Only required when domain account in use is not Exchange Full Administrator or Domain Administrator

WARNING: Do not use the Run As feature to start OfflineAssessmentClient.exe. Some collectors might fail. The account starting the offline client must logon to the local machine.

3. Scanning Security Updates

PowerShell V5 on the tools machine is used to scan the servers for installed and missing security patches as well as collecting audit policy configuration.

- ♦ Scanning for security updates: Download the Windows Update offline scan file (Wsusscn2.cab). The latest cab file can be downloaded from the following link: http://go.microsoft.com/fwlink/?LinkId=76054. The file should be transferred to the collection machine and placed in the root of the OS drive, **C:\wsusscn2.cab,** folder.
- ♦ Windows Update Agent must be running on all Exchange servers.

4. Network and Remote Access

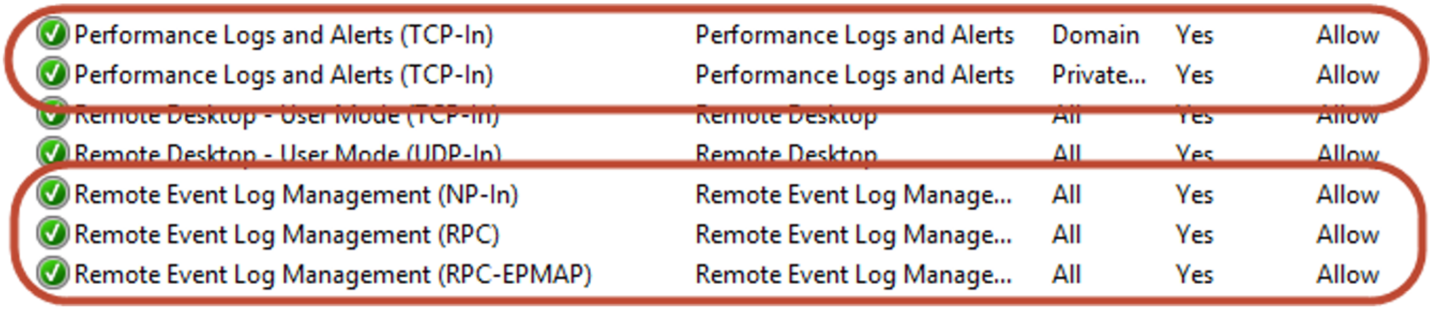
- ♦ Ensure that the browser on the tools machine or the machine from where you activate, download and submit data has JavaScript enabled. Follow the steps on How to enable scripting in your browser.

  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://serviceshub.microsoft.com portal. Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11 are the supported browsers for this offering. Most other modern HTML5 based browsers will also work.

- ♦ 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.

- Unrestricted network access to every server in the environment
    - This means access through any firewalls, and router ACLs that might be limiting traffic to any server. This includes



Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Domain	Yes	Allow
Performance Logs and Alerts (TCP-In)	Performance Logs and Alerts	Private...	Yes	Allow
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Allow
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Allow
Remote Event Log Management (NP-In)	Remote Event Log Manage...	All	Yes	Allow
Remote Event Log Management (RPC)	Remote Event Log Manage...	All	Yes	Allow
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Manage...	All	Yes	Allow

To test if the tool will be able to collect event log data from a Windows Server 2008/Windows Server 2008 R2 or later Exchange Server, you can try to connect to the Windows Server 2008/Windows Server 2008 R2 or later Exchange Server using **eventvwr.msc** from the tools machine. 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 the **Remote Event Log Management** rules noted above.

To test if the tool will be able to collect performance data from a Windows Server 2008/Windows Server 2008 R2 or later Exchange Server, you can try to query the performance log information using the following command from a command prompt or PowerShell prompt on the Tools machine: ***'logman /query /s SERVERNAME'*** If the command returns "The command completed successfully" then performance data collection is possible. If the command returns "The network path was not found" then you may need to enable the Windows built-in firewall to allow **Performance Logs and Alerts** rules noted above.

Appendix

Data Collection Methods

The **Exchange Server Assessment in the log analytics workspace and Microsoft Unified Support Solution Pack** uses multiple data collection methods to collect information from your environment. This section describes the methods used to collect data from your environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

1. Registry Collectors
2. EventLogCollector
3. Windows PowerShell
4. FileDataCollector
5. WMI
6. Custom C# Code
7. System Performance Data

1. **Registry Collectors**

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

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.

  This allows to analyze the status of Exchange Server related services

- Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

  This allows the assessment to determine Operation System information such as Windows Server 2012, Windows Server 2016 or Windows Server 2019.

2. EventLogCollector

Collects event logs from Exchange Server. We collect the last 7 days of Warnings and Errors from the Application and System event logs.

3. Windows PowerShell

PowerShell is used extensively in the Exchange Server Assessment to gather configuration data.

4. FileDataCollector

Enumerates files in a folder on a remote machine, and optionally retrieves those files. For example, the EdgeTransport.exe.config file for each Hub server is gathered so that the settings may be validated.

5. Windows Management Instrumentation (WMI)

WMI is used to collect various information such as:

- ♦ WIN32_Volume

  Collects information on Volume Settings for each server in the environment. The information is used for instance to determine the system volume and drive letter which allows Exchange Server Assessment to collect information on files located on the system drive.

♦ Win32_Process

Collect information on the processes running on each server in the environment. 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.

6. Custom C# Code

Collects information not captured using other collectors.

7. System Performance Data

Utilizes the Performance Logs and Alerts service to create a data collector on each target server. By default the performance data will be written to the c:\perflogs directory on each server. Before the collection is started the required disk space is verified by the collector. Once the collection is completed the data collection configuration as well as the collected data are removed from each target server.