Offline Assessment for System Center Configuration Manager

Prerequisites

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

No data is transported outside your 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*

How to prepare for your Offline Assessment for System Center Configuration Manager

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), SQL Database, 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. 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 starting your engagement.

1. Data Collection

a. Tools machine hardware and Operating System:

- ☐ Server-class or high-end workstation machine running Windows7/Windows8/ Windows8.1/Windows 10, or Windows Server 2008/Windows Server 2008 R2/ Windows Server 2012/Windows Server 2012 R2/Windows Server 2016.
- ☐ English (United States) locale setting is required
- ☐ Minimum: 8GB RAM, 2Ghz dual-core processor, 10 GB of free disk space plus at least 7 GB for every 100,000 objects in the assessed environment during data collection.
- ☐ Joined to one of the same domain where the Configuration Manager Central server is or another domain in the same forest which has trust relationship with all domains.

b. Software for Tools machine:

- ☐ Microsoft .NET Framework 4.7 installed
- ☐ Windows PowerShell 2.0 or later installed
- ☐ Configuration Manager Console (Please make sure you can connect from this console to all CAS/Primary Sites)

This document was last updated August 12, 2017. To ensure you have the latest version of this document , check here: http://download.microsoft.com/download/1/C/1/1C15BA51-840E-498D-86C6-4BD35D33C79E/Prerequisites_Offline_CM.pdf

c. Account Rights:
   - ☐ Enterprise User account with Admin access to every server (Site System) in the Configuration Manager hierarchy. Single user account if Site Systems are in Multi-domain Environment.
   - ☐ Unrestricted network access to every server (Site System) in the Configuration Manager hierarchy.
   - ☐ Administrator permissions to all SQL servers used by the Configuration Manager Sites or Software Update Points
   - ☐ Full access rights to all the Configuration Man ager Site objects in all Primary Sites
   - ☐ SysAdmin permission to all SQL Instances used by Configuration Manager Sites or Software Update Points

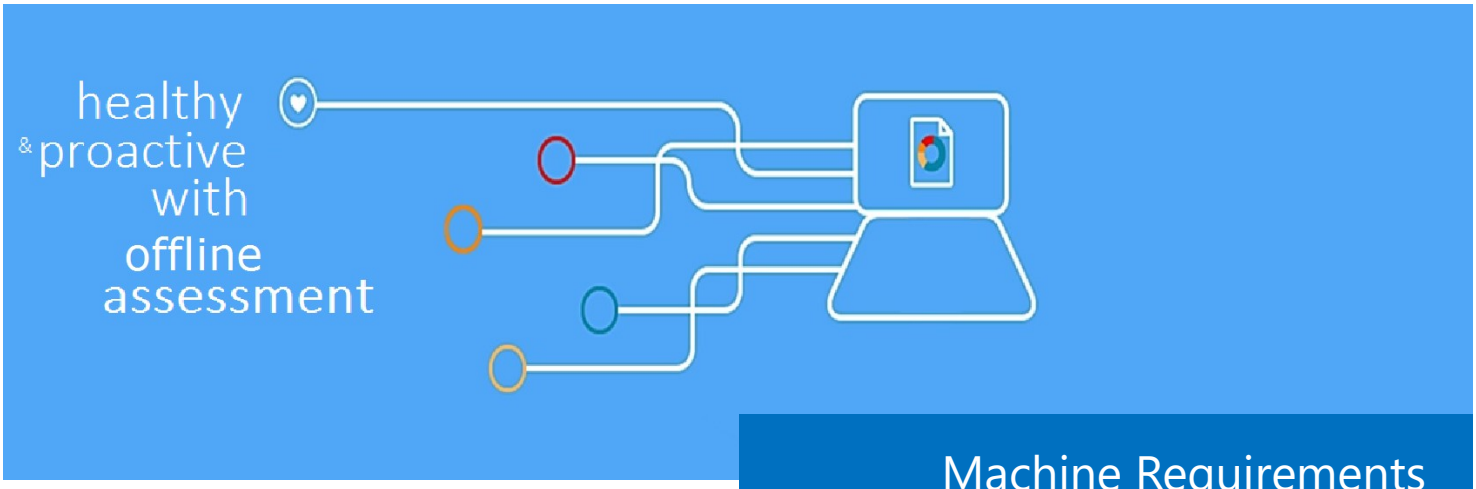
   WARNING: Do not use the Run As feature to start OfflineAssessmentClient.exe. Some collectors might fail. The account starting the offline client must logon to the local machine. Due to UAC restrictions, the discovery might fail. In such cases, please login with appropriate user account and then start Offline Client using "Run the Administrator"

d. Additional Requirements for Windows Server 2008 (and later) servers:
   - ☐ Please check the firewall rules and configure necessary services
   - ☐ Please check that the default Admin shares are not disabled
   - ☐ On Windows 8.1/2012/2012R2/2016 Feature .NetFramework 3.5 (includes .NET 2.0 and 3.0) must be enabled

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—Recommended 12 GB RAM.
- Minimum 10 GB of free disk space, plus at least 7 GB for every 100,000 objects in the assessed environment during data collection.
- Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012/2012R2 or Windows Server 2008/Windows Server 2008 R2.
- English (United States) locale setting is required
- Can be 32-bit or 64-bit operating system.
- At least a 1024x768 screen resolution (higher preferred).
- Must be a member of the assessed AD Forest (member of the Forest Root Domain is preferred not but required)
- Microsoft® .NET Framework 4.7 — http://www.microsoft.com/en-us/download/details.aspx?id=55170
- Windows PowerShell 2.0 or higher
  - Windows PowerShell 2.0 is part of the Windows Management Framework — http://support.microsoft.com/kb/968929
- Networked "Documents" or redirected "Documents" folders are not supported. Local "Documents" folder on the data collection machine is required.
- Configuration Manager Console (Please make sure you can connect from this console to all CAS/Primary Sites)

2. Accounts Rights

- A domain account with the following:
  - Local Administrator permissions on all Configuration Manager Server (Site Systems). Single user account if Site Systems are in Multi-domain Environment.
  - Local Administrator permissions on all SQL Servers used by the Configuration Manager Sites or Software Update Points.
  - Administrative access to the SQL Server that is used by the Configuration Manager Sites or Software Update Points (member of SysAdmin role).
  - Full access rights to all the Configuration Manager Site objects in all Primary Sites.

  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. Due to UAC restrictions, the discovery might fail. In such cases, please login with appropriate user account and then start Offline Client using "Run the Administrator"

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.

- Unrestricted network access to every Configuration Manager server in the environment

  * This means access through any firewalls, and router ACLs that might be limiting traffic to any SQL Server and Configuration Manager Site server. This includes remote access to DCOM, Remote Registry service, Windows Management Instrumentation (WMI) services, and default administrative shares (C$, D$, IPC$).
  * Ensure that the machine you use to collect data has complete TCP/UDP access, including RPC access to all servers. For a complete list of protocols, services and ports required by System Center Configuration Manager.
  * Remote data collections are performed by using TCP ports 135, 139, 445 and 1433. UDP ports 137 and 138 are required. RPC communications and DCOM must be enabled.

4. Run the CMRAP Scoping Tool to validate the environment is ready

Please note the tool must be run with an account that has full access rights to all the Configuration Manager Site servers in all sites. The tool does NOT make any changes to the environment. It simply uses standard operations such as WMI queries, LDAP queries, port queries and so on. It is completely read-only.

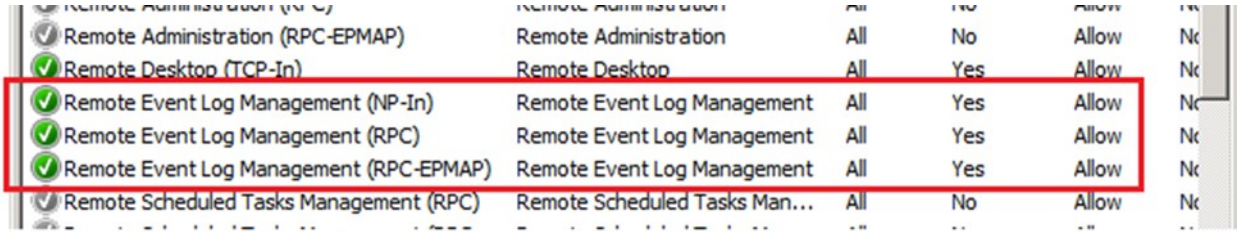
The tool is serial in nature and only attempts to perform a single check against a single server at a time. This means there should be relatively minimal network or target system overhead while the tool is running. This also means it may take it several minutes or even hours to complete depending upon the size of the environment.

1. Download the CMRAP Scoping tool from http://www.microsoft.com/en-us/download/details.aspx?id=2536
2. Extract the CMRAPScoping.zip file and open the Scoping directory.
3. Launch the tool by running Microsoft.CmRap.Scoping.exe. A wizard will walk you through running the tool. The checks that it performs may take several minutes depending upon the size of the environment. Refer to the file, Instructions.txt,
4. within the Scoping folder for detailed instructions.

Please note that this tool is also used for legacy CM RAPS. Ignore the failures relating to Log Parser 2.2, ConfigMgr Console Installed, and SQL Server Compact Edition.

5. Additional requirements for Windows Server 2008 or later: Windows Firewall configurations

- **Configure the servers firewall to ensure all servers running Windows Server 2008/Windows Server 2008 R2 and later have Remote Event Log Management enabled**: Offline client might be unable to collect event log information from a Windows Server 2008/Windows Server 2008 R2 or later if **Remote Event Log Management** has not been allowed. When **Remote Management** is enabled, the rules that allow **Remote Event Log Management** are also enabled.



To test if the tool will be able to collect event log data from a Windows Server 2008/Windows Server 2008 R2 or later, you can try to connect to the Windows Server 2008/Windows Server 2008 R2 or later 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**.

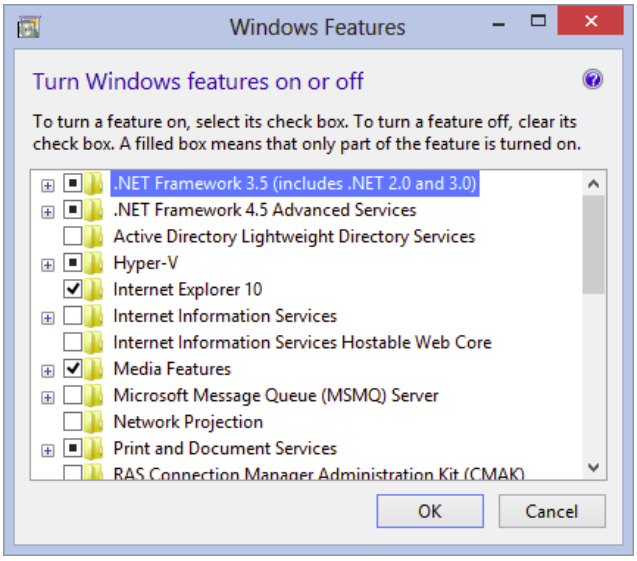
Before you can create firewall rules remotely on the server, the option **remote firewall management** must have been enabled on all Windows Server 2008/Windows Server 2008 R2 or later with the Advanced Firewall enabled. To allow Remote **Event Log Management,** create a new GPO:

Configure a GPO

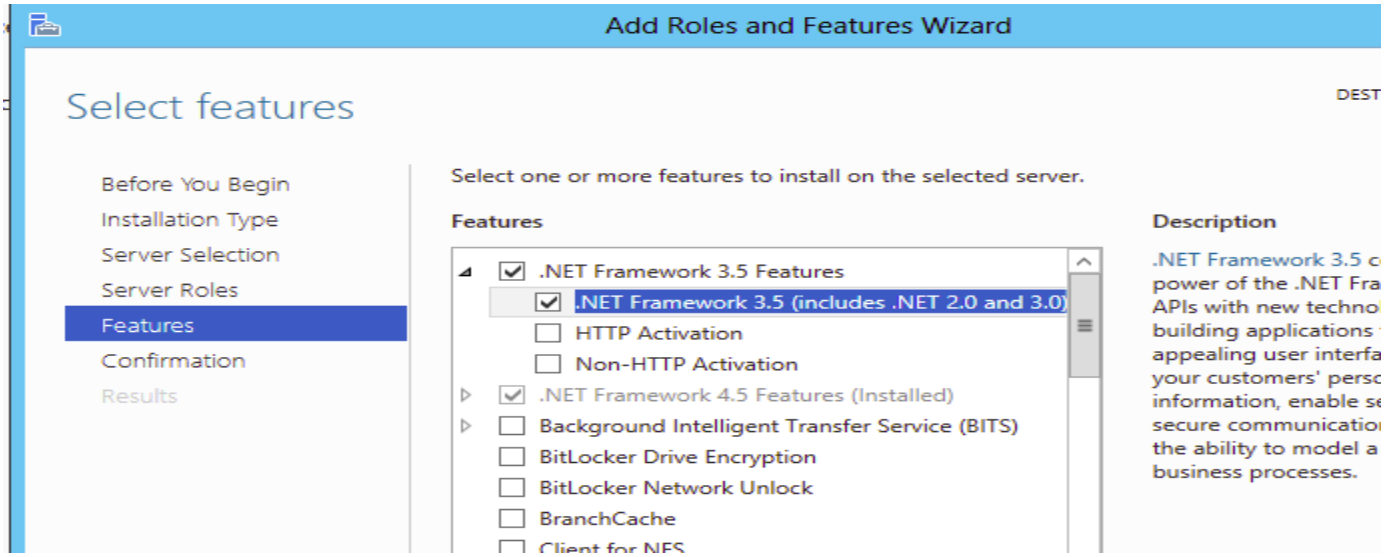
1. Create a new GPO and link it to the corresponding OU for your servers.
   Within the GPO open **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\ Windows Firewall with Advanced Security**, right-click **Inbound Rules** and then click **New Rule**.
2. In the **New Inbound Rule Wizard**, on the **Rule Type** page, select **Predefined**. In the **rule** list, click **Remote Event Log Management,** and then click **Next**.
3. On the **Predefined Rules** page, select the **Remote Event Log Management (RPC)** rule check box, and click **Next**.
   Note: the other two Remote Event Log Management rules are not required for the assessment but might be needed for Remote Event Log Management
4. On the **Action** page, select **Allow the connection** and then click **Finish**.

***NOTE**: Allow for this GPO to replicate and apply to all servers that are being assessed before starting data collection.*

6. Additional requirements for Windows Server 2012 Servers, Windows 8 or later:



In Windows Server 2012 and Windows 8 the following feature needs to be enabled: **.NetFramework 3.5 (includes .NET 2.0 and 3.0)**



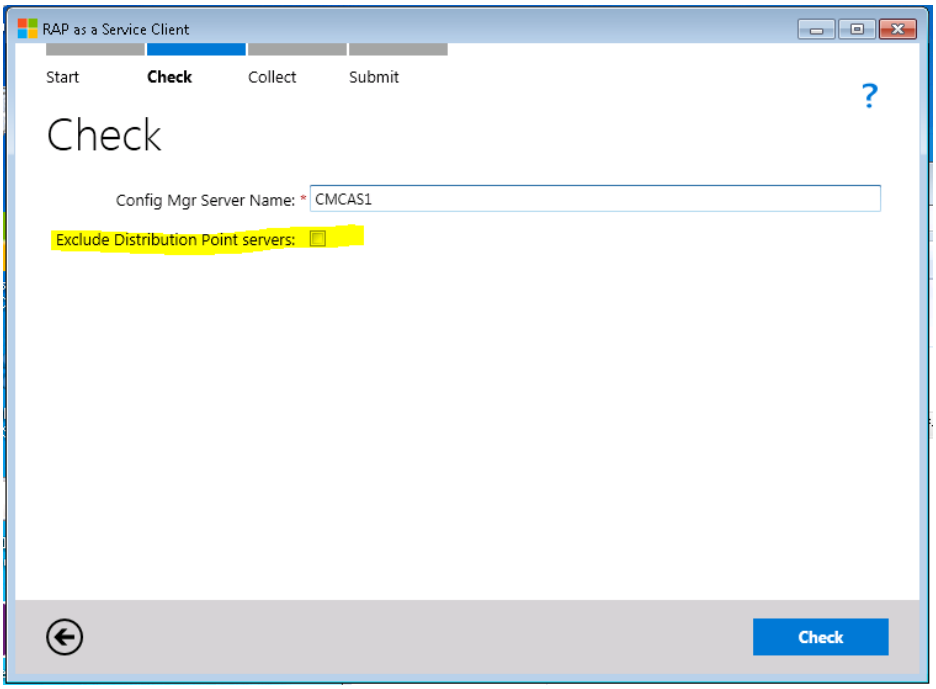
Appendix: Data Collection Methods

Offline Assessment for Configuration Manager uses multiple data collection methods to collect information. This section describes the methods used to collect data from an Configuration Manager environment. No VB scripts are used to collect data. Data collection uses workflows and collectors. The collectors are:

1. Registry Collectors: Registry keys and values are read from the Configuration Manager Site Servers in the hierarchy.
2. LDAP Collectors: LDAP queries are used to collect data for the Domain, DCs, nTDSSiteSettings objects, Partitions and other components from AD itself.
3. Windows PowerShell: For some basic Configuration Manager Site properties.
4. FileDataCollector: Enumerates files in a folder on a remote Configuration Manager Site Servers.
5. WMI: WMI queries are used to collect information from CIMV2 and SMS_Site namespaces.
6. SQL: SQL queries are used to collect information from Site Servers
7. Custom C# Code: Collects information not captured using other collectors.

Appendix: New discovery Feature

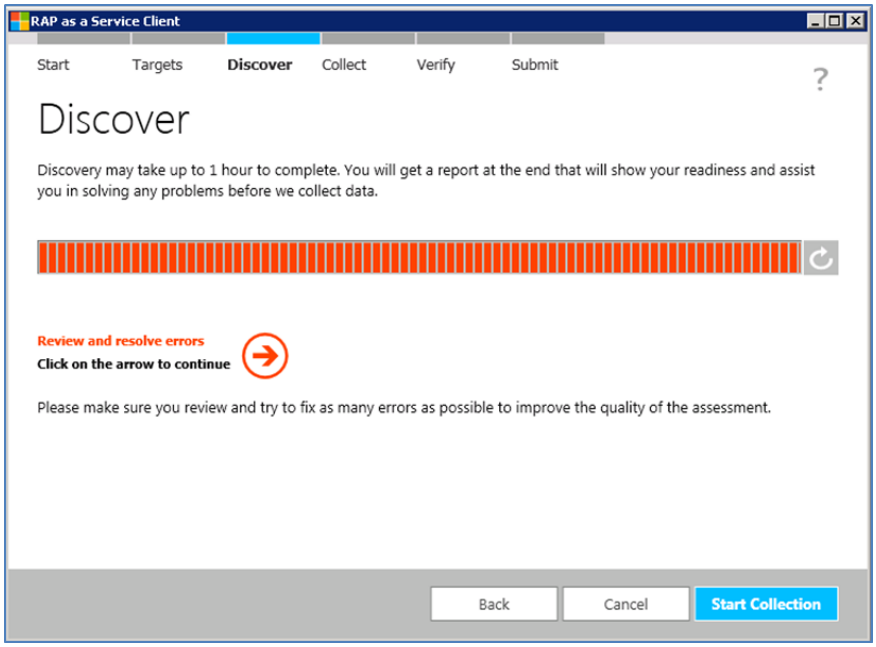
With the June 2016 release of Offline Assessment for Configuration Manager, a new discovery feature which enables very large customers to exclude server which are **only** covering the "Distribution Point" role from being discovered, was added. These servers are not critical to the environment and are normally located across slow/unreliable WAN links or behind firewalls, making the discovery taking longer than expected and not able to find them. On account of this, we want to give customers the ability to exclude them in advance, making the discovery process smoother and faster. In order to use this new feature, which is disabled by default, customers have to check the checkbox for the option "Exclude Distribution Point server"



Appendix: Troubleshooting

- Discovery related errors

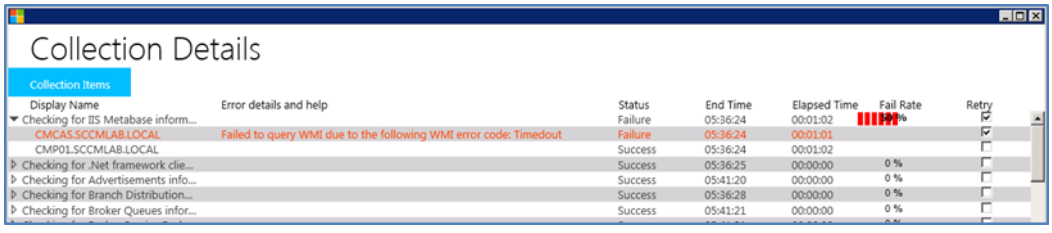
  If there is an issue in the discovery process an error screen will appear.



  If the error screen appears, click on the arrow to see the details and resolve the issues and then go back to the **Find Targets** screen and click on **Find Targets.** You can also review this information in DiscoveryTrace_*.log file. This file can be found in the folder ..\Documents\RaaS\RaaSxx_*\Logs. The trace file holds information on the discovery process and lists all the error messages.

- Collection related errors

  If there are errors on collecting data then they will be displayed in collection details with information relating to error details and possible help. If possible resolve the errors and select the items where the errors have been resolved and choose to gather the data on these items again by clicking on Retry Checked.



  You can also review this information in SironaTrace_*.log file. This file can be found in the folder ..\Documents\RaaS\RaaSxx_*\Logs. The trace file holds information on the data collection process and lists all the error messages.