Windows Client Assessment: Prerequisites and Configuration

This document explains the required steps to configure the Windows Client Assessment prerequisites.

There are configuration and setup tasks to be completed prior to executing the assessment setup tasks in this document. For all pre-work, follow the Getting Started with On-Demand Assessments in the Services Hub Resource Center.

Table of Contents

Prerequisites

According to the scenario you want to use, review the following details to ensure that you meet the necessary requirements.

Supported Versions

- This service is available for clients running Windows 10 or later which are
    - Active Directory domain joined
    - Azure Active Directory domain joined
    - Workgroup member

Accounts and Permissions

Common to all Scenarios

- You will need a **Log Analytics** workspace with at least Contributor rights

Common to Active Directory

- User account rights:
    - A domain account with the following rights on all **test clients**:
        - Member of the local Administrators group
        - *Log on locally*
        - *Access to this computer from the network*
    - A domain account with the following rights on the **data collection machine**:
        - Member of the local Administrators group
        - *Log on locally*
        - *Log on as batch job*
- Networking requirements:
    - Unrestricted network access from the data collection machine to all clients.
    - On all **test clients** the following Windows Defender Firewall build-in inbound rules need to be enabled:
        - Remote Event Log Management (RPC)
        - Remote Scheduled Task Management (RPC)
        - Windows Management Instrumentation (DCOM-In)
        - Windows Management Instrumentation (WMI-In)
        - Windows Remote Management (HTTP-In)

Common to Azure Active Directory / Workgroup

- User account rights:
    - A local account with the following rights:
        - Member of the local Administrators group
        - *Log on locally*
        - *Log on as batch job*

Data Collection Machine

- Supported Windows Server full GUI or Windows Client operating system.

- Minimum 8 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 5 GB of free disk space, plus up to 2 GB for every target client in the assessed environment during data collection.
- The CLR version on the data collection machine should be using .NET 4.8 or greater. This can be verified by running *`dotnet --list-runtimes`* in the PowerShell prompt.
- Microsoft Monitoring Agent installed and configured for one of the deployment scenarios at the beginning of this document.

Common to Active Directory

- On all **test clients**:
    - The following services need to be running:
        - Remote Registry
        - Windows Management Instrumentation
        - Windows Remote Management (WS-Management)
    - Execute *`Enable-PSRemoting`* Powershell in the PowerShell prompt. This one command will configure PS-Remoting, WinRM service and listener, and enable required Inbound FW rules. A detailed description of everything Enable-PSRemoting does is documented here.
- On the **data collection machine**:
    - The following services need to be running:
        - Task Scheduler
        - Windows Management Instrumentation
    - To scan for missing Microsoft updates an up to date wsusscn2.cab file needs to be located at C: root.

Common to Azure Active Directory / Workgroup

- The following services need to be running:
    - Task Scheduler
    - Windows Management Instrumentation

Configuration

Detailed instructions on assessment configuration can be found on Getting Started with the Windows Client On-Demand Assessment.

Appendix

Data Collection Methods

The **Windows Client Assessment** uses the following data collection methods to collect information from your environment:

- Event Log
- Filesystem
- Registry
- PowerShell
- WMI

The collection consists of machine configuration data only which will be stored on the data collection machine. If an issue is found the corresponding configuration and the name of the affected machine will be send to the Log Analytics workspace.