
# On-Premises Collector System Requirements & Installation Guide

## Get Started Now

Version: 05.31.21

Formerly TSO Logic

# On-Premises Collector System Requirements and Installation Guide

## Table of Contents

## Pre-Install Checklist

The following preconditions should be completed before proceeding to step 1.

- Has an account been created on https://console.tsologic.com?
    - Please contact your Migration Evaluator specialist if you have not received an invitation request
- Has the server for the Migration Evaluator Collector been created and provisioned according to this guideline?
    - See **Appendix A – Server Hardware Requirements**
    - If your environment exceeds the sizing specifications, please contact your Migration Evaluator specialist
- Does your Windows account have local administrator rights on the new server for the Migration Evaluator Collector?
    - See **Appendix B – Server Account Requirements**
- If you have VMware infrastructure being monitored, have you verified account credentials and network connectivity?
    - See **Appendix C – Connectivity to VMware vCenter**
- If you have bare metal infrastructure being monitored, have you verified account credentials, network connectivity and completed the CSV template?
    - If connecting via SNMP, see **Appendix D – Connectivity via SNMP**
    - If connecting via WMI, see **Appendix E – Connectivity via WMI**
    - Have the servers to be monitored been listed in a CSV file? See **Appendix H – CSV Example for Monitoring Bare Metal Servers**
- If you have Hyper-V infrastructure being monitored, have you verified account credentials, network connectivity, and completed the optional CSV template?
    - See **Appendix F – Connectivity to Hyper-V Hosts**
    - If discovering Hyper-V hosts via Active Directory scanning, see **Appendix K – Connectivity via Active Directory**
    - If manually providing the Hyper-V hosts to be included, have the hosts been listed in a CSV file? See **Appendix I – CSV Example for Monitoring Hyper-V Servers**
- If you have SQL Server infrastructure to be discovered, have you verified account credentials and network connectivity?
    - See **Appendix J – Connectivity via T-SQL**
- Have you verified network connectivity from the server for the Migration Evaluator Collector to the analytics engine hosted in the US East region?
    - See **Appendix G – Connectivity to Analytics Engine**

## Data Synchronization with AWS

The Migration Evaluator Collector by default will not synchronize logs or any data about the discovered on-premises environment with AWS.

To permit the Migration Evaluator service to monitor the health of the collector, it is recommended that automatic synchronization is configured. To enable, please complete section **9 – Configure Synchronization with the Migration Evaluator Analytics Engine** of this guide once the collector has been deployed.

Alternatively, to manually provide records of the inventory discovered, the Inventory and Utilization export will need to be generated and uploaded to the Migration Evaluator Management console. This will need to be done at least twice during the assessment (after the initial collector deployment and at the end of the collection window). See section **10 - Annotating Discovered Inventory with Business Data** for details.

# 1 – Install the Migration Evaluator Bootstrapper

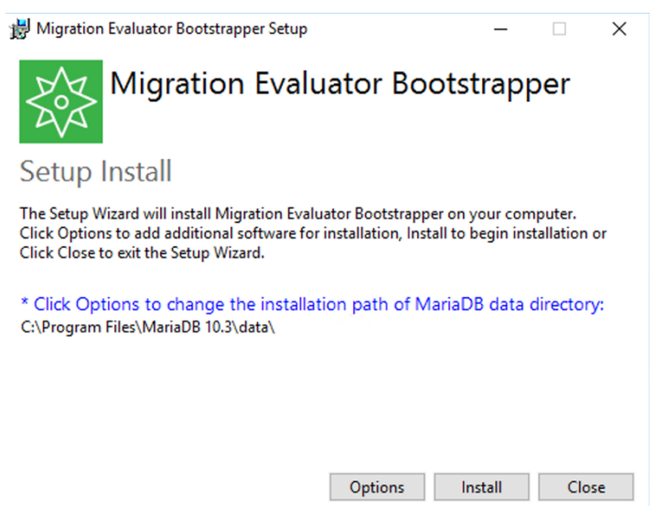
## Preconditions

- Has the server for the Migration Evaluator Collector been created and provisioned according to this guideline?
    - See **Appendix A – Server Hardware Requirements**
- Can the server for the Migration Evaluator Collector easily be recreated?
    - Reverting the server to a snapshot or re-creating the server may be required if your company's security policies interfere with the software installation. To plan for unlikely event, you may want to create a snapshot prior to proceeding
- Does your Windows account have administrator rights on the new server for the Migration Evaluator Collector?
    - See **Appendix B – Server Account Requirements**
- Have you logged into the Migration Evaluator Management Console at https://console.tsologic.com?
    - Please contact your Migration Evaluator specialist if you have not received an invitation request

## Steps

The TSOBootstrapper.exe automatically scans the server you provisioned to run the Migration Evaluator Collector and installs any missing software packages. You may be prompted to restart Windows during this process. Depending on the speed of your server and Windows version, this may take up to 20 minutes.

1. Download and save the **TSOBootstapper.exe** from https://console.tsologic.com/discover/tools onto the new designated server.
    a. You may have to rename the file extension to .exe after the download. This is normal and is due to Windows internal security settings.
2. Ensure you are logged in as a local Administrator.
3. If a non-C: drive was allocated to meet the collector storage requirement (see **Appendix A – Server Hardware Requirements**), click **Options** and select the correct drive.




4. Select **Install** and wait while the packages are installed. Once done, select the **Close** button to complete the process.
    a. If there is an error, see **Appendix N – Troubleshooting Bootstrapper Installation**.

## 2 – Install the Migration Evaluator Collector

### Preconditions

- Has the Bootstrapper been installed?
    - See **1 – Install the Migration Evaluator Bootstrapper**
- Have you logged into the Migration Evaluator Management Console at https://console.tsologic.com?
    - Please contact your Migration Evaluator specialist if you have not received an invitation request

### Steps

The Migration Evaluator Collector software is a Windows Service and IIS application used to monitor your on-premises infrastructure.

1. Download and save the Migration Evaluator Collector software MSI from https://console.tsologic.com/discover/tools onto the new designated server.
2. Download and save the collector specific encryption certificate from https://console.tsologic.com/discover/collectors onto the new designated server. If you have multiple collectors, each instance must have a *unique* certificate.
3. Ensure you are logged in as a local Administrator.
4. Run the TSOCollector_.msi
    a. Select the certificate file (<assessment>-<number>.crt) previously downloaded.
    b. Select to run the collector under a local system account or the service account created prior to install. The account selected cannot be changed after install. See **Appendix B – Server Account Requirements** for more details on service accounts.
        i. If the service account does not have the needed permissions, a dialog requesting to grant the permissions will be presented.
        ii. Select the **Grant rights automatically** checkbox and click **OK** to proceed. Click **Test Credentials.**
    c. Select **HTTPS** for communication with the IIS application. If you wish to replace the auto-generated self-signed certificate, see **Appendix L – Replace Self-Signed Certificate**.
    d. Select **Yes** to automatically start the collection service once the install sequence finishes.
    e. If there is an error, see **Appendix O – Troubleshooting Collector Installation**
5. Once installation has completed, your next step will be to create your local account for managing the collector. This is not the account used on https://console.tsologic.com.
    a. Access the Migration Evaluator Collector software by clicking on the newly-created desktop shortcut, or by opening your browser at: *https://localhost*.
    b. Enter your desired credentials, and click Create Account
    c. If you cannot create an account, see **Appendix P – Troubleshooting Collector Configuration**
6. Take note of your recovery key. This will allow you access to the Migration Evaluator Collector if you forget your password.

## 3 – Configure Collection from VMware

*Skip this section if you do not have VMware infrastructure to monitor.*

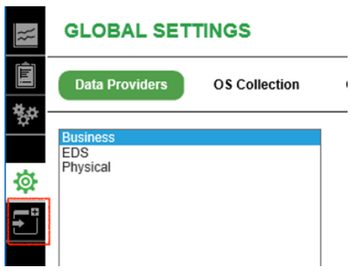
### Preconditions

- Have you verified vCenter account credentials and network connectivity?
    - See **Appendix C – Connectivity to VMware vCenter**
- Have you logged into the Migration Evaluator Collector software?
    - Select the newly-created desktop shortcut, or by opening your browser at: https://localhost and using the local account created in step 2-5.

### Steps

If you have VMware infrastructure being monitored, the following section outlines the steps needed to configure the Migration Evaluator Collector. This process will need to be repeated for each vCenter in scope.

1. Select **Add Data Provider** from the navigation bar




2. Select **VMware vSphere**, and click the **Next** button.
3. Populate the following details of your vCenter where:
    a. **Name** is descriptive label for the vCenter instance, the **Address** is either the IP or FQDN of the vCenter, and the **User Name** includes the domain if applicable.
    b. The **Advanced Settings** is our default polling cycle, you don't need to edit this unless suggested by your Migration Evaluator specialist.
4. Select **Save** and then **Done**.
5. Check the **Status**. Most vCenter instances are deployed with a self-signed certificate, you may need to either disable SSL certificate validation by sliding the **VMware Certification Validation** option to **OFF**, or fix the certificate installed on the vCenter instance being monitored.


6. After a configuration change, you may force the software to try connecting again by selecting **Advanced Status**, then **Force**.

## 4 – Configure Operating System Credentials

*Skip this section if you do not have servers to be monitored directly (bare metal or virtual machine) or Hyper-V infrastructure to monitor.*

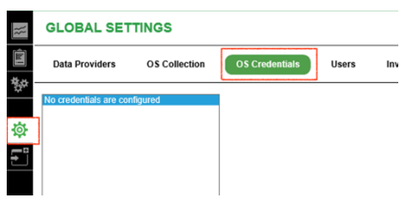
### Preconditions

- If you have servers (bare metal or virtual machines) being monitored directly, have you verified account credentials and network connectivity?
    - If connecting via SNMP, see **Appendix D – Connectivity via SNMP**
    - If connection via WMI, see **Appendix E – Connectivity via WMI**
- If you have Hyper-V infrastructure being monitored, have you verified account credentials and network connectivity?
    - See **Appendix F – Connectivity to Hyper-V Hosts**
- Have you logged into the Migration Evaluator Collector software?
    - Select the newly-created desktop shortcut, or by opening your browser at: https://localhost and using the local account created in step 2-5.

### Steps

If you have bare metal or Hyper-V infrastructure being monitored, you will need to configure credentials for SNMP and/or WMI. You may also optionally configure credentials for collecting utilization directly from each virtual machine. See section **8 – Configure Virtual Machine OS Metrics Collection** for more details.

1. Select **Global Settings** from the Navigation bar, then the **OS Credentials** tab




2. For each SNMP credential to be used, select **New**, then **SNMP v2c or v3** from the protocol dropdown.
    a. Configure as many SNMP credentials as needed. See **Appendix D – Connectivity via SNMP**.
3. For each WMI credential to be used, select **New**, then **WMI** from the protocol dropdown
    a. Configure as many WMI credentials as needed. See **Appendix E – Connectivity via WMI**, and **Appendix F – Connectivity to Hyper-V Hosts**

## 5 – Configure Collection from Bare Metal Servers

*Skip this section if you do not have bare metal infrastructure to monitor.*

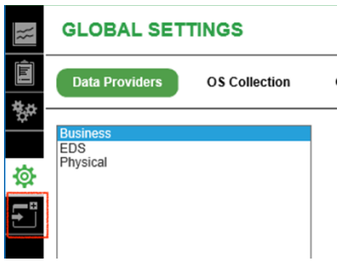
### Preconditions

- Have you verified account credentials and network connectivity?
    - See **4 – Configure Operating System Credentials**
- Have you logged into the Migration Evaluator Collector software?
    - Select the newly-created desktop shortcut, or by opening your browser at: https://localhost and using the local account created in step 2-5.

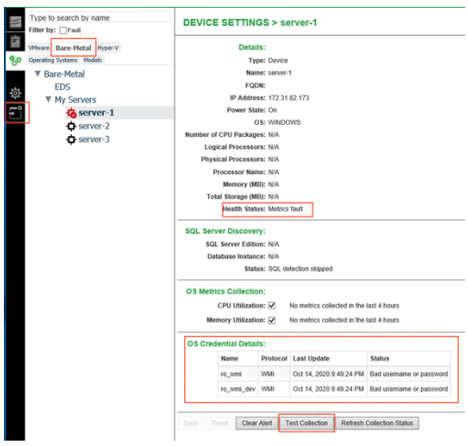
### Steps

If you have bare metal infrastructure being monitored, the following section outlines the steps needed to configure the Migration Evaluator Collector. This process will need to be repeated for each list of bare metal servers in scope.

1. Create a CSV file containing the list of servers to be monitored (see **Appendix H – CSV Example for Monitoring Bare Metal Servers**).
    a. Note that the file must have a .CSV file extension.
2. Select **Add Data Provider** from the navigation bar:




3. Select **Migration Evaluator CSV**, and click the **Next** button.
4. Populate the details of your CSV file including a descriptive label for this list of servers.
5. Select **Save** and then **Done**. The system will now start to asynchronously add the servers. This initial cycle can take more than 10 minutes to complete.
6. Verify that at least one server you feel should work can be monitored. To do this, select the **Device Settings** from the navigation bar and select the **Bare Metals** view. Navigate to a server you would like to test and select **Test Connection**.




    a. If the server is tagged as unhealthy, please review the **OS Credential Details** section for each configured OS credential's status, as well as **Appendix Q – Troubleshooting Operating System Collection.**

## 6 – Configure Collection from Hyper-V Servers

*Skip this section if you do not have Hyper-V infrastructure to monitor.*

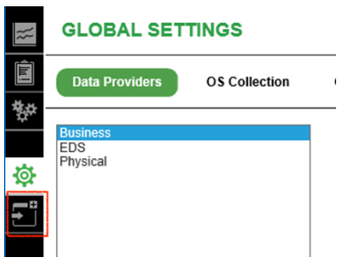
### Preconditions

- Have you verified account credentials and network connectivity?
    - See **4 – Configure Operating System Credentials**
- Have you logged into the Migration Evaluator Collector software?
    - Select the newly-created desktop shortcut, or by opening your browser at: https://localhost and using the local account created in step 2-5.

### Steps

If you have Hyper-V infrastructure being monitored, the following section outlines the steps needed to configure the Migration Evaluator Collector. This process will need to be repeated for each Active Directory server or list of Hyper-V hosts in scope.

1. Select **Add Data Provider** from the navigation bar




2. Select **Microsoft Hyper-V**, and click the **Next** button.
3. If using Active Directory to discover the Hyper-V hosts on your network, select **Active Directory Scan**. See **Appendix K – Connectivity via Active Directory.**
    a. **Name** is a descriptive label for the Active Directory instance + base distinguished name (DN)
    b. **Address** is either the IP or FQDN of the Active Directory server
    c. **User Name** includes the domain if applicable.
    d. **Base DN** specifies the root for searches in the Active Directory. By default this is ou=users,dc=domain,dc=com. Modify this to reduce the scope of Hyper-V hosts to be included.
4. If using a known list of Hyper-V hosts, select **CSV File Containing the Hyper-V Hosts**
    a. Create a CSV file containing the list of Hyper-V hosts to be monitored (see **Appendix I – CSV Example for Monitoring Hyper-V Servers**)
    b. **Name** is a descriptive label for the Hyper-V hosts in the file
    c. Select your CSV file
5. Select **Save** and then **Done**. The system will now start to asynchronously add the servers. This initial cycle can take more than 10 minutes to complete.
6. Verify that the Hyper-V hosts and their virtual machines were discovered. To do this, select the **Device Settings** from the navigation bar and select the **Hyper-V** view.

# 7 - Configure SQL Server Discovery

*Skip this section if you do not have Microsoft SQL Server instances to discover.*

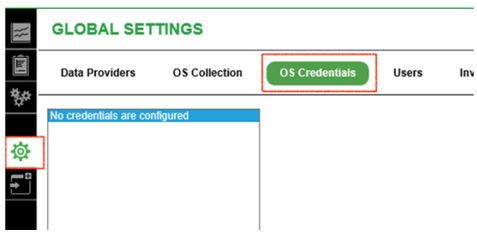
## Preconditions

- Has the Migration Evaluator Collector software been installed and configured?
    - See **3 – Configure Collection from VMware**
    - See **5 – Configure Collection from Bare Metal Servers**
    - See **6 – Configure Collection from Hyper-V Servers**

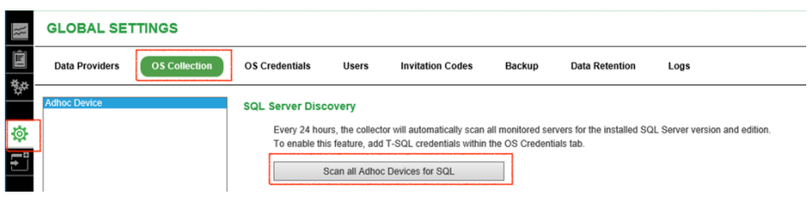
## Steps

If you have SQL Server infrastructure to be discovered, you will need to configure T-SQL credentials, then initiate the scan. Further scans will occur in the background every 24 hours.

1. Select **Global Settings** from the Navigation bar, then the **OS Credentials** tab




2. Select **New**, then **T-SQL** from the protocol dropdown.
    a. Domain accounts are not supported.
    b. Configure as many T-SQL credentials as needed. See **Appendix J – Connectivity via T-SQL**
3. Select **Global Settings** from the Navigation bar, then the **OS Collection** tab.




    a. For each data type configured (VMware, Adhoc, and Hyper-V), select **Scan all** to initiate the scan.
        i. Note: Every 24 hours the system will automatically look for new servers running SQL Server. Selecting Scan now is only needed to accelerate discovery during installation.

# 8 – Configure Virtual Machine OS Metrics Collection

*Skip this section if you do not have VMware or Hyper-V infrastructure to monitor.*

## Preconditions

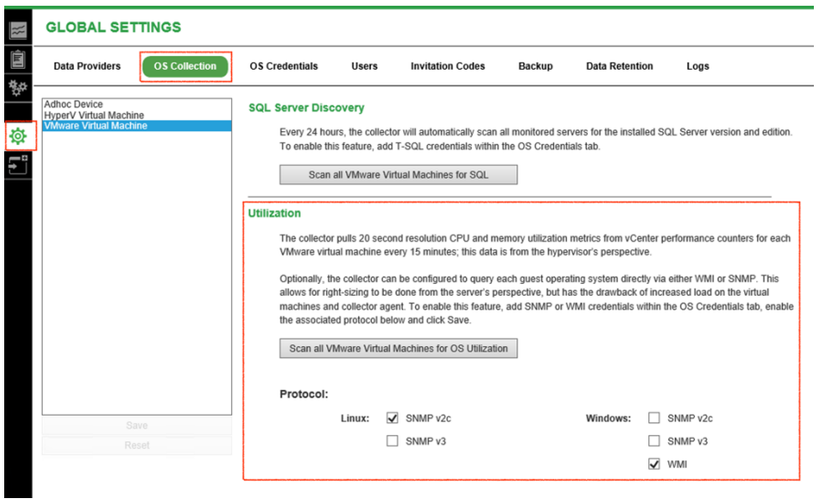
- Has the Migration Evaluator Collector software been installed and configured?
    - See **3 – Configure Collection from VMware**
    - See **6 – Configure Collection from Hyper-V Servers**
- Have you verified account credentials and network connectivity?
    - See **4 – Configure Operating System Credentials**

## Steps

To remove the dependency on network connectivity and server credentials (SNMP or WMI), the Migration Evaluator Collector by default pulls virtual machine resource utilization metrics from the hypervisors (via Hyper-V hosts and vSphere appliances). For Hyper-V, this means that no memory utilization is able to be captured. For VMware, the consumed host memory metric is used which is the total "amount of host memory that is allocated to the virtual machine".

If you would like the business case to factor in resource utilization from the operating system's point of view, WMI or SNMP monitoring may be optionally enabled. For any virtual server that WMI or SNMP fails to collect due to network connectivity, authentication or authorization, the collector will continue to use utilization from the hypervisor.

1. Select **Global Settings** from the Navigation bar, then the **OS Collection** tab.




2. For each data type configured (VMware and Hyper-V):
    a. Configure the desired protocols. For Windows virtual machines, WMI is preferred if both WMI and SNMP are available.
3. Select **Scan all** to initiate the scan.
    a. The collector will automatically attempt to collect utilization data every nine minutes and will back-off attempts if all credentials fail (see **Appendix M – Server Utilization Collection Back-off**). Selecting **Scan all** is only needed to accelerate discovery during installation or after providing a new / editing an existing OS credential.
    b. If the server is tagged as unhealthy, please review the "OS Credential Details" section for each configured OS credential's status, as well as **Appendix Q – Troubleshooting Operating System Collection.**

# 9 – Configure Synchronization with the Migration Evaluator Analytics Engine

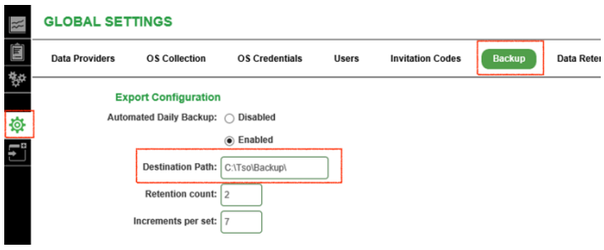
## Preconditions

- Have you verified network connectivity to Amazon S3 from the server for the Migration Evaluator Collector?
    - See **Appendix G – Connectivity to Analytics Engine**
- Have you logged into the Migration Evaluator Management Console at https://console.tsologic.com?
    - Please contact your Migration Evaluator specialist if you have not received an invitation request

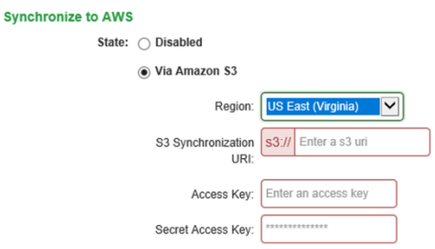
## Steps

Once the collector software is installed and monitoring your infrastructure, it is time to configure data synchronization to the Migration Evaluator Analytics Engine hosted in US East (Northern Virginia).

1. Verify the destination path for the nightly export is correct based on the server provisioning in **Appendix A**. To see, select **Global Settings**, then **Backup**.




1. Configure the Amazon S3 synchronization setting based on your collector details listed in the Migration Evaluator Management Console : https://console.tsologic.com/discover/collectors




    a. If required for your network to have connectivity to S3, enable the optional HTTP proxy.

2. Select **Initiate Backup Now** to verify both the backup and synchronization is working.
    a. If synchronization fails, see **Appendix P – Troubleshooting Collector Configuration**.

## 10 - Annotating Discovered Inventory with Business Data

### Preconditions

- Has the Migration Evaluator Collector software been installed and configured?
    - See **3 – Configure Collection from VMware**
    - See **5 – Configure Collection from Bare Metal Servers**
    - See **6 – Configure Collection from Hyper-V Servers**
- Have you logged into the Migration Evaluator Management Console?
    - Open a browser at https://console.tsologic.com. Please contact your Migration Evaluator specialist if you have not received an invitation request

### Steps

Once the collector software is installed and monitoring your infrastructure, it is time to annotate the discovered inventory with business data (logical environments) as well as any attributes not detected.

1. Generate an export of the collector's inventory by selecting **Global Settings**, then **Backup**, then **Download Inventory & Utilization Export**.
2. Open the Excel document.
    a. On the **Virtual Assets** sheet:
        i. Verify the inventory contains everything expected to be in-scope
        ii. For VMs running SQL Server, verify the Database Type column was populated. If not, manually add either: SQL Server Enterprise or SQL Server Standard
    b. On the **Physical Assets** sheet:
        i. Verify the inventory contains everything expected to be in-scope
        ii. For servers running SQL Server, verify the Database Type column was populated. If not, manually add either: SQL Server Enterprise or SQL Server Standard
    c. On the **Asset Ownership** sheet:
        i. Fill in as much as possible, including the server's logical environment. By providing production vs development tags, extra projected savings may be able to be modelled.
    d. On the **Utilization** sheet:
        i. No change is needed as values are populated automatically based on utilization patterns detected.
3. Upload the updated Excel workbook for your engagement in the Migration Evaluator Management Console: https://console.tsologic.com/discover/self-reported-files

## Appendix A – Server Hardware Requirements

The Migration Evaluator Collector requires one new server running the English version of Windows Server 2012 R2 or greater. Based on the mix of data sources, the following minimum specifications must be provisioned. When monitoring from multiple sources, select the largest server configuration tier.

*Example: a data center with 3000 virtual machines, 50 Hyper-V Host Systems and 200 Linux bare metal servers will require at least 6 CPU cores and 16GB of RAM.*

| Virtual Machines | Physical Servers | | | | | |
|---|---|---|---|---|---|---|
| | Hyper-V | Linux | Windows | CPU | RAM | Storage |
| 1-500 | | 1-500 | | 2 | 8 GB | 100 GB primary, SSD preferred |
| 500-2.5k | | 500-2.5k | | 4 | 12 GB | 200 GB primary, SSD required |
| 2.5k-5k | 1-100 | 2.5k-5k | 1-500 | 6 | 16 GB | 300 GB primary, SSD required |
| 5k-10k | 100-200 | 5k-10k | 500-1k | 8 | 32 GB | 500 GB primary, SSD required |
| 10k+ | 200+ | 10k+ | 1k+ | Please consult your Migration Evaluator specialist | | |

- Storage allocation will grow over time. The numbers above are for a typical three-month period and must be reviewed at term
- English version of Windows Server 2012 R2 or greater
- System Locale configured for en-US (English United States)

## Appendix B – Server Account Requirements

To install the software, you will need an account with local administrator rights on your new server for the Migration Evaluator Collector. This includes the permission to:

- Execute local unsigned PowerShell scripts
- Use non-FIPS compliant algorithms for encryption, hashing and signing

The Migration Evaluator Collector can optionally be configured to run under a local or domain user account. This configuration restricts decryption of collection credentials to only this user and cannot be changed post installation. The following rights are required for the service account:

- Logon as service
- Logon as batch job
- Logon locally
- Member of Builtin\Performance Monitor Users group
- Member of Administrators group

## Appendix C – Connectivity to VMware vCenter

The Migration Evaluator Collector requires the following to monitor VMware vCenter:

- Version 4.1 and greater of vSphere Web API provided from VMware
- Network connectivity via TCP port 443
- An account that:
    - Is a member of the 'Read-only' role
    - Is associated with the vCenter Server
    - Has inventory read on the Root folder

To test:

1. From a browser on your Server for the Migration Evaluator Collector, connect to the vCenter Managed Object Browser (MOB) interface
    a. https://<yourvcenter.yourcompany.com>/mob
2. Enter the vCenter user account and password to be used by the Migration Evaluator Collector

If the MOB authenticates and reveals objects, this should be sufficient to assume that read-only access is working as required. If not, please verify the expected permissions have been applied.

## Appendix D – Connectivity via SNMP

The Migration Evaluator Collector requires the following to monitor either Microsoft, Linux, RHEL or SUSE bare metal servers via SNMP:

- Network connectivity via ICMP
- Network connectivity via UDP port 161
- If using SNMP v2c:
    - a read-only community string
- If using SNMP v3:
    - a username/password and auth/privacy details for read-only permission

Access to the following OIDs:

| Description | Linux | Windows |
|---|---|---|
| CPU Utilization | 1.3.6.1.2.1.25.3.3.1.2 | 1.3.6.1.2.1.25.3.3.1.2 |
| Memory Utilization | 1.3.6.1.4.1.2021.4 | 1.3.6.1.2.1.25 |
| CPU Provisioning | 1.3.6.1.2.1.25.3.2 | N/A |
| Memory Provisioning | 1.3.6.1.2.1.25.2.3.* | N/A |
| Storage Provisioning | 1.3.6.1.2.1.25.2.3.* | N/A |

## Appendix E – Connectivity via WMI

The Migration Evaluator Collector requires the following to monitor Microsoft bare metal servers via WMI:

- Windows Server 2008 or greater
- Network connectivity via ICMP
- Network connectivity via TCP port 135 + ephemeral TCP port range (49152 - 65535)
    - WMI can be problematic through firewalls due to maintaining contracts in the ephemeral port range
- An account that is a member of the following groups:
    - Performance Monitor Users
- An account with the following permissions:
    - Execute Methods
    - Enable Account
    - Remote Enable
    - Remote Activation
- Access to the following namespaces (and their subfolders)
    - \root\cimv2
    - \root\default

## Appendix F – Connectivity to Hyper-V Hosts

The Migration Evaluator Collector requires the following to monitor Microsoft Hyper-V hosts:

- Windows Server 2008 R2 or greater
- Network connectivity via ICMP
- Network connectivity via TCP port 135 + ephemeral TCP port range (49152 - 65535)
    - WMI can be problematic through firewalls due to maintaining contracts in the ephemeral port range
- An account that is a member of the following groups:
    - Performance Monitor Users
    - Hyper-V Administrator (Windows Server 2012 R2 or greater)
- An account with the following permissions:
    - Execute Methods
    - Enable Account
    - Remote Enable
    - Remote Activation
- Access to the following namespaces (and their subfolders)
    - \root\cimv2
    - \root\default
    - \root\virtualization (Windows Server 2008 R2)
    - \root\virtualization\v2 (Windows Server 2012 or greater)

## Appendix G – Connectivity to Analytics Engine

Egress HTTPS traffic from the Migration Evaluator Collector to the AWS managed, Amazon S3 bucket in US East-1 (https://s3.amazonaws.com/tsologic-match-us-east/).

This URL will resolve to the following address ranges:

- 52.92.16.0/20
- 52.216.0.0/15
- 54.231.0.0/17

If direct egress traffic is not available, configuration of an HTTP proxy is supported. If a proxy is not available within your network, multiple manual exports out of the Server for the Migration Evaluator Collector will be required during the engagement.

## Appendix H – CSV Example for Monitoring Bare Metal Servers

The Migration Evaluator Collector requires a CSV (comma separated value) file containing the list of servers to be monitored via SNMP or WMI. The file is required to be in the following format where **NAME** is required along with either **IP** or **FQDN** in the first row.

```
NAME,IP,FQDN
server-1,192.168.0.1,
server-2,192.168.0.2,
server-3,,baz.example.com
```

## Appendix I – CSV Example for Monitoring Hyper-V Servers

The Migration Evaluator Collector requires a CSV (comma separated value) file containing the list of Hyper-V hosts to be monitored via WMI. The file is required to be in the following format where **HOSTNAMEORIP** is required in the first row.

```
HOSTNAMEORIP
Host-server-1
192.168.10.1
```

## Appendix J – Connectivity via T-SQL

The Migration Evaluator Collector requires the following to discover SQL Server version and edition via T-SQL:

- Network connectivity via TCP port 1433
- A local database account with:
    - PUBLIC role (this is the default permission given to all SQL Server accounts)

## Appendix K – Connectivity via Active Directory

The Migration Evaluator Collector requires the following to discover Hyper-V hosts via Active Directory:

- Active Directory server running schema 2012 or greater
- Network connectivity via TCP port 389
- An account that is a member of the domain

## Appendix L – Replace Self-Signed Certificate

Browsers connecting to the Migration Evaluator Collector's web application will generate a warning due to the default self-signed certificate provided. If you wish to remove the warning, replace the certificate with your own.

- Open Internet Information Services (IIS) Manager
    - Start > Run > inetmgr or search "IIS" from the start menu
- Import SSL Certificate (.pfx file)
    - Select the top-level node from menu on the left
    - Double click **Server Certificates** to open
    - Select **Import** from the menu on the right
    - Select your certificate file and enter the associated password. Click **Ok**.
- Assign your imported certificate to the HTTPS site binding
    - Click **TSO.OpCenter** from the menu on the left
    - Choose **Bindings** from the menu on the right
    - Edit the existing **https** binding
    - Replace the LocalHostCertificate certificate with your own certificate. Click **Ok**
- With **TSO.OpCenter** selected on the left, click **Restart** from the menu on the right

More details can be found:

- https://docs.microsoft.com/en-us/iis/manage/configuring-security/how-to-set-up-ssl-on-iis#iis-manager

## Appendix M – Server Utilization Collection Back-off

In the event that all configured WMI or SNMP credentials are failing on configured Bare Metal or Virtual Servers, the Migration Evaluator Collector will exponentially reduce the frequency of attempts. The following intervals will be used after consecutive failures: 7 minutes, 7 minutes, 30 minutes, 2 hours, 8 hours, 24 hours. After 6 failed attempts, the collector will continue to try once every day all configured credentials.

To force a collection attempt after adding new credential or resolving a client-side issue, go to **Select Global Settings** from the Navigation bar, then the **OS Collection** tab. For each data type configured (VMware, Hyper-V and Adhoc), select **Scan all**.

## Appendix N – Troubleshooting Bootstrapper Installation

In the event of an error while installing the Bootstrapper, logs are written to the user's temp folder and can be found by typing **%temp%** into Windows Explorer's address bar.

| Problem | Solution |
|---|---|
| Installation aborts prematurely | Ensure the user account utilized for installation has **local** administrator rights with permission to:<br><br>Execute local unsigned PowerShell Scripts<br><br>In PowerShell with "Run as Administrator" option.<br><br>`set-executionpolicy remotesigned`<br><br>If using a local:<br><br>Make sure the user logged in as a **local** administrator to the machine - this can be verified by making sure they prefixed their username with ".\" when logging in. |
| Log contains:<br><br>MSI (c) (50!7C) [10:41:23:062]: PROPERTY CHANGE: Adding CA_ERROR property. Its value is '0x80070542 - CheckTokenMembership failed: 0x80070542'.<br>Action ended 10:41:23: AsiUI_CheckMembership. Return value 3. | Ensure user used to install has **local** administrator rights on the server with the following rights:<br><br>Logon as service<br><br>Logon as batch job<br><br>Logon locally<br><br>Member of Builtin\Performance Monitor Users group<br><br>Member of Administrators group |
| Log contains:<br><br>RabbitMQ failed to install | When using a user not tied to a domain to install the bootstrapper.<br><br>Ensure the user logged in as a **local** administrator to the machine - this can be verified by making sure they prefixed their username with ".\" when logging in.<br><br>Ensure that the home directory for the user is local and not a network share<br><br>Once resolved, install the Bootstrapper again on the same server. |

Please contact your assigned Migration Evaluator specialist with supporting log files if additional support is required.

## Appendix O – Troubleshooting Collector Installation

In the event of an error while installing the Migration Evaluator Collector, the log file will be opened automatically. All logs are also written to the user's temp folder which can be found by typing **%temp%** into Windows Explorer's address bar.

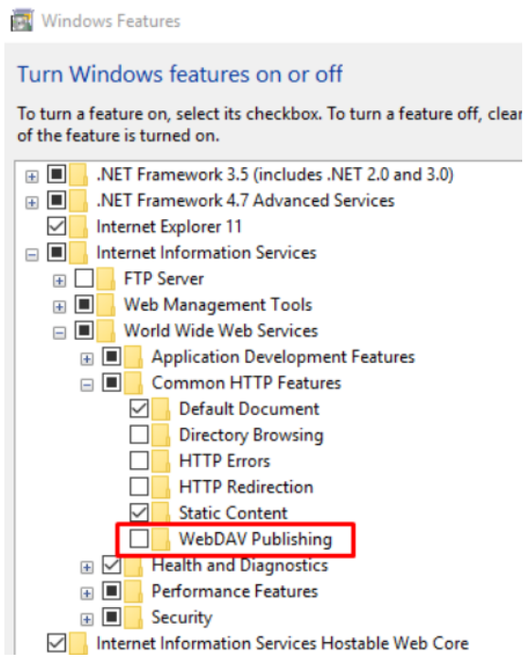
The specific error can be found by searching the log file for **value 3**.

| Problem | Solution |
|---|---|
| **Permissions / Policies** | |
| CheckTokenMembership failed: 0x80070542 | Related to permissions of the user running the installer.<br><br>To start installation: Right-click installer > Run as Administrator |
| An error occurred while setting up MariaDb encryption:<br>System.InvalidOperationException: This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms. | The server had a Group Policy setting that caused this: 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing: Enabled'<br><br>Use non-FIPS compliant algorithms for encryption, hashing and signing<br><br>Run gpedit.msc<br><br>Navigate to Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options<br><br>Right-click on "System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing<br><br>From Properties dialog select "Disabled"<br><br>If after updating the Group Policy, the error still persists, try having the system admin run the following command:<br>`gpupdate /force` |
| **Server Settings / Existing Software Conflicts** | |
| ERROR 2019 (00000): Can't initialize character set auto (path: compiled_in)<br><br>Retrying with old credential<br><br>Error provisioning database user accounts! Error trying to create database user "OpCenter": C:\Program Files\MariaDB 10.3\bin\mysql.exe exited with non-zero error code! Code: 1 | The software is being installed on a server with an unsupported localization. Currently only English version of Windows 2012 R2 or greater with a system locale configured to EN-US (English United States) is supported.<br><br>To fix this, vefify that an English version of Windows Server is used and change the system locale to English:<br><br>Go to "Control Panel" > "Region" > "Administrative" Tab<br><br>Ensure the "Current language for non-Unicode programs" is set to "English (United States)" |

| | |
|---|---|
| ERROR: Error executing script "C:\Program Files\TSOLogic_deployBase\Scripts\BaseLine_1.7\0000#DB.sql"<br><br>Line: 2733 Position: 0 Statement Type: Create<br><br>Message: Error on rename of '.\tso\assignmentvendorvirtualserver.TRG~' to '.\tso\assignmentvendorvirtualserver.TRG' (Errcode: 13 "Permission denied")<br><br>…<br><br>…<br><br>CustomAction UpdateDBElevated returned actual error code 1603 (note this may not be 100% accurate if translation happened inside sandbox)<br><br>Action ended 14:52:35: InstallFinalize. Return value 3. | Installation attempted on a server with anti-virus software blocking required installation steps.<br><br>Please remove or temporarily disable the anti-virus software and retry installation of the collector msi. |
| Start: Setup MariaDb encrypion<br>Warning: One or more file(s) needed for encryption already exist<br>MariaDb encrypion settings already exist<br>Finish: Setup MariaDb encrypion<br>.<br>.<br>.<br>Provisioning Database User Accounts Error provisioning database user accounts!<br>Error trying to create database user "OpCenter": C:\Program Files\MariaDB 10.3\bin\mysql.exe exited with non-zero error code! Code: 1<br>ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES) | Migration Evaluator Collector software is already installed on this server.<br><br>Installer failed initially and was run again on the same server<br><br>Figure out the cause of the first installation failure (typically permission error)<br><br>Provision a fresh server/virtual machine and retry installation after addressing the initial issue.<br><br>*Note: Alternately, refresh current server back to a new template VM state, and reattempt installation starting with bootstrapper installation.* |
| PIP was not installed with Bootstrapper | Customer will need to install pip manually and modify the python installation<br><br>1. Save this file to the collector VM<br><br>https://bootstrap.pypa.io/get-pip.py<br><br>2. Open cmd prompt to the saved location and run<br><br>`python get-pip.py`<br><br>3. Retry installation of collector msi |

Please contact your assigned Migration Evaluator specialist with supporting log files if additional support is required.

## Appendix P – Troubleshooting Collector Configuration

| Problem | Solution |
|---|---|
| **Access / Log-In** | |
| Collector Web UI will not load:<br><br>Web browser is stuck on our loading screen with the animating dots and just sits there<br><br>  <br><br>Web browser shows an error "No connection could be made because the target machine actively refused it 127.0.0.1:5672" | These issues are from RabbitMQ failing to deploy properly. To confirm please use Service Manager (services.msc) to review the following:<br><br>• RabbitMQ service isn't running, attempting to start succeeds, but it immediately stops<br><br>• RabbitMQ service is running, but the service description column is completely blank (it should say "Multi-protocol open-source messaging broker")<br><br>If either of these are the case, RabbitMQ needs to be reinstalled. This can be achieved by uninstalling it via Add/Remove programs and re-running the Migration Evaluator Bootstrapper as the local administrator. |
| Unable to log into the collector or bad username/password | A recovery code will allow you to create a new user/password to access the collector. The code is stored in:<br><br>C:\Users\TSOOpCenter\AppData\Local\TsoLogic\recovery.txt |
| **Configuration Updates** | |
| Receive "Save Failed" when trying to save configurations in the collector. | Error caused by WebDAV Publishing enabled on the server running the Migration Evaluator Collector. To disable, do the following:<br><br>Search for "Turn Windows Features On or Off"<br><br>Uncheck the box on WebDAV Publishing<br><br>  |
| Linux bare-metal servers being seen as Windows | The collector leverages ICMP fingerprinting to select Operating System Credential to use. Server with a Ping TTL greater or equal to 65 and less than or equal to 128 is assumed to be Windows; otherwise, the server is Linux. |

| | |
|---|---|
| | To force Operating Systems defined, please adjust your existing bare-metal CSV to the following format:<br><br>`NAME,IP,FQDN,Operating System`<br>`server-1,192.168.0.1,,Windows`<br>`server-2,192.168.0.2,,Linux`<br>`server-3,,baz.example.com,Linux`<br><br>Once complete, please follow solution steps identified for "Updating list of bare-metal servers configured". |
| Need existing list of bare-metal servers to be updated | To remove / add bare-metal servers to the collector:<br><br>1. Make adjustment to the original CSV file used for configuration followed by a save<br>2. In Global Settings > Data Providers, select the existing bare-metal configuration<br>3. Click on "Upload" and select the updated CSV file<br>4. Click "Save"<br><br>⚠ Important<br>The uploaded CSV file should contain all bare metal servers in scope of assessment. By creating a new Data Provider, potential duplicate servers may exist if multiple CSV files are used. |
| Synchronization with Analytics Engine (Amazon S3 Sync) | |
| Global Settings > Backup reports Amazon S3 Synchronization as Unsuccessful | Ensure the Migration Evaluator Collector is configured with the S3 credentials from: https://console.tsologic.com/discover/collectors<br><br>Ensure the server where Migration Evaluator Collector is installed has egress HTTPS access (**Appendix G – Connectivity to Analytics Engine**)<br><br>For further assistance, supply log files to your assigned Migration Evaluator specialist.<br><br>If the collector was installed under a Service Account:<br><br>C:\Users\<username>\AppData\Local\TsoLogic\logs<br><br>If the collector was installed under "Local System":<br><br>C:\Windows\System32\config\systemprofile\AppData\Local\tsologic\logs |
| Migration Evaluator team is unable to confirm successful sync | |
| Error found in Global Settings > Logs:<br><br>Amazon.S3.AmazonS3Exception: The difference between the request time and the current time is too large. | Ensure the local clock on the Migration Evaluator Collector is accurate within 15 minutes. |

| | |
|---|---|
| Migration Evaluator team confirms your data cannot be decrypted. | The Migration Evaluator Collector software was installed with an incorrect certificate and therefore the data synchronized cannot be decrypted. Replace the certificate, and re-sync the data.<br>1. Download the certificate for this Migration Evaluator engagement from: https://console.tsologic.com/discover/collectors<br>2. Delete all of the existing files from the local collector machine (path configured Global Settings > Backup)<br>3. Replace the certificate<br>• Open "certlm.msc" (Start -> Run)<br>• Navigate to Certificates (Local Computer) > TSO Logic Inc > Certificates<br>• Right-click on the existing certificate there and select Delete<br>• Click Yes to permanently delete the certificate<br>• Right-click in the right pane (where the certificate you just deleted was listed) and select All Tasks > Import<br>• This will start the Certificate Import Wizard, click Next until you see "File to import"<br>• Select the new certificate file and click Next<br>• On the Certificate Store dialog Place all certificates in the following store: TSO Logic Inc should be selected<br>• Click Next. Click Finish<br>4. Reset Registry Keys (local system user during installation)<br>• Open "regedit.exe" (Start > Run)<br>• Navigate to in regedit<br>• Local system user used during installation.<br>`HKEY_USERS\.DEFAULT\Software\TSO Logic\TSO logic`<br>• Service account user used during installation.<br>`HKEY_USERS\<<user SID>>\SOFTWARE\TSO Logic\TSOlogic`<br>• Edit key listed and erase the values for (double click the key, set Value data to blank) LastKnownFullBackupDir, LastBackupMetricTime, LastBackupAppDataTime, LastBackupWinEventLogTime, LastBackupWinEventLogID<br>5. Initiate backup from: Global Settings > Backup > Initiate Backup Now |

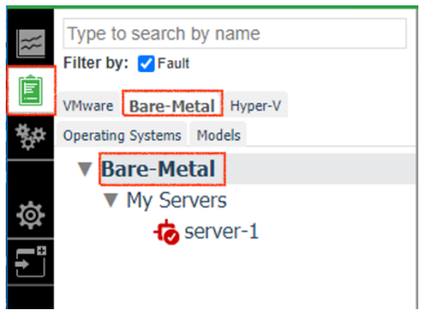
# Appendix Q – Troubleshooting Operating System Collection

The Migration Evaluator Collector has the ability to monitor Virtual Machines and Bare-Metal servers directly via SNMP or WMI (see sections 5 and 8 for details). This section outlines common solutions for resolving collection faults.

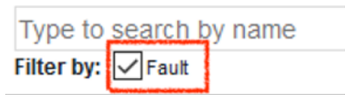
## Identifying Server Requiring Attention

To identify servers experiencing WMI or SNMP based collection faults:

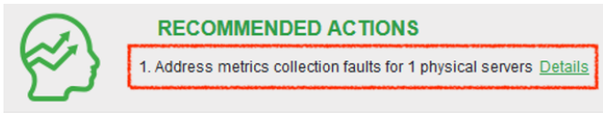
1. Select **Status Report** from the Navigation bar, select either the **VMware**, **Bare Metals**, or **Hyper-V** view and the top node in the tree.




2. Select the **Fault** checkbox to highlight the servers in question




3. If there are servers in collection fault, download the **Details** CSV file from the "Address metrics collection faults" recommended action.




## Troubleshooting WMI Based Collection

The follow table outlines the common solution for collection problems with WMI.

| Problem Code | Solution |
|---|---|
| Bad username or password | Please ensure username and/or password saved in collector is correct. Ensure adjustments made to existing credentials are retained by clicking "Save" |
| System.Management.ManagementException: Timed out | Network issues with WMI. Confirm connectivity from collector server to target server(s):<br>Network connectivity via ICMP<br>Network connectivity via TCP port 135 + ephemeral TCP port range (49152 - 65535) |
| The operation has timed out. | |
| Access Denied to namespace "Cimv2" | WMI credentials do not have access to required "Cimv2" namespace. Fix credential permissions on target server to have access to the namespaces (and their subfolders)<br>`\root\cimv2`<br>`\root\default` |

| | |
|---|---|
| The RPC server is unavailable. (Exception from HRESULT: 0x800706BA) | WMI is disabled or firewall is blocking it on target server. |
| An existing connection was forcibly closed by the remote host | Ensure the WMI protocol configured in the collector is deployed on the target server. |
| Already in progress | Collection is already in progress for this server, wait for it to complete |

### Testing WMI Based Collection

Amazon Web Services does not recommend any third-party products to help test WMI communication, but the Microsoft included tools nslookup.exe, ping.exe and wbemtest.exe are available.

Below are some steps that could be followed to debug WMI issues:

1. Run nslookup.exe for one of the host names that you want to investigate to get the associated IP address
2. Run ping.exe for the hostname and IP address. The Migration Evaluator Collector must be able to use ICMP to determine the operating system of the target server
3. From the WBEMtest.exe utility on your new server for the Migration Evaluator Collector, enter either an IP or FQDN of the server to be monitored and user account/password to be used by the Migration Evaluator Collector
4. Run the following queries against the root\cimv2 namespace. If the result set is empty, the calling account does not have the required permissions
    a. SELECT * FROM Win32_ComputerSystem
    b. SELECT Caption,OSArchitecture,Version FROM Win32_OperatingSystem
    c. SELECT UUID,Vendor,Name,IdentifyingNumber FROM Win32_ComputerSystemProduct
    d. SELECT MediaType,Size FROM Win32_LogicalDisk WHERE MediaType = 12
5. Run the following query against the root\virtualization namespace for Windows Server 2008 R2 or older. If the result set is empty, the calling account does not have the required permissions
    a. SELECT * FROM Msvm_ComputerSystem
6. Run the following query against the root\virtualization\v2 namespace for Windows Server 2012 or greater. If the result set is empty, the calling account does not have the required permissions
    a. SELECT * FROM Msvm_ComputerSystem
7. Once results are returned by WBEMtest.exe, return to the Migration Evaluator Collector
    a. Select **Device Settings** (the 3 gears icon) from the Navigation bar
    b. Navigate to the server reporting the fault
    c. Press **Clear Alert**, then **Test Collection.** If the problem has been resolved, Health Status will be updated as Healthy.

For ideas around troubleshooting WMI issues, please consult the following Microsoft guides:

- https://docs.microsoft.com/en-us/windows/win32/wmisdk/troubleshooting-a-remote-wmi-connection
- https://docs.microsoft.com/en-us/windows/desktop/WmiSdk/securing-a-remote-wmi-connection

### Troubleshooting SNMP Based Collection

The follow table outlines the common solution for collection problems with SNMP.

| Problem Code | Solution |
|---|---|
| The operation has timed out. | SNMPv2 configured – The community string is (likely) wrong.<br>SNMPv3 configured – The username and password are (likely) wrong.<br>Ensure the SNMP protocol configured in the collector is deployed on the target server. |
| Already in progress | Collection is already in progress for this server, wait for it to complete |
| An existing connection was forcibly closed by the remote host | Ensure the SNMP protocol configured in the collector is deployed on the target server. |

### Testing SNMP Based Collection

Amazon Web Services does not recommend any third-party products to help test SNMP communication, but the included Microsoft included tool, nslookup.exe, ping.exe and Migration Evaluator SNMP tool stored in C:\Program Files\TSOLogic\OpsUtil\TsoSnmpTool\TsoSnmpTool.exe are available.

Below are some steps that could be followed to debug SNMP issues:

1. Run nslookup.exe for one of the host names that you want to investigate to get the associated IP address
2. Run ping.exe for the hostname and IP address. The Migration Evaluator Collector must be able to use ICMP to determine the operating system of the target server
3. On the server where the Migration Evaluator Collector is installed, run the following command with the hostname from above and run it a second time with the IP from above. A healthy server will return successfully and put data into an output.xml file. An unhealthy server will return an error.

```
C:\Program Files\TSOLogic\OpsUtil\TsoSnmpTool\TsoSnmpTool.exe -
c=<Community String> -f=False -o=<OID (can be found in Appendix D)> -
t=<hostname or IP>
```

4. Once results are returned by TsoSnmpTool.exe, return to the Migration Evaluator Collector
    a. Select **Device Settings** (the 3 gears icon) from the Navigation bar
    b. Navigate to the server reporting the fault
    c. Press **Clear Alert**, then **Test Collection.** If the problem has been resolved, Health Status will be updated as Healthy.