On-Premises Collector System Requirements & Installation Guide

Get Started Now

Version: 2023-09-21

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 are planning to run an Optimized Licensing Assessment or have SQL Server infrastructure discovered, you will need to configure operating system credentials. Have you verified account credentials, and network connectivity?
    - If connecting via SNMP, see **Appendix D – Connectivity via SNMP**
    - If connecting via WMI, see **Appendix E – Connectivity via WMI**
    - See **Appendix J – Connectivity to SQL** Server
- 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**
- Have you verified network connectivity from the server for the Migration Evaluator Collector to the Amazon Web Services?
    - See **Appendix G – Connectivity to AWS**

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** 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.

Network Visualization in AWS Migration Hub requires the Migration Evaluator Collector to synchronize with your AWS Account. To enable, please complete section **12 – Configure Network Connection Collection for** of this guide once the collector has been deployed.

1 – Install the Migration Evaluator Bootstrapper

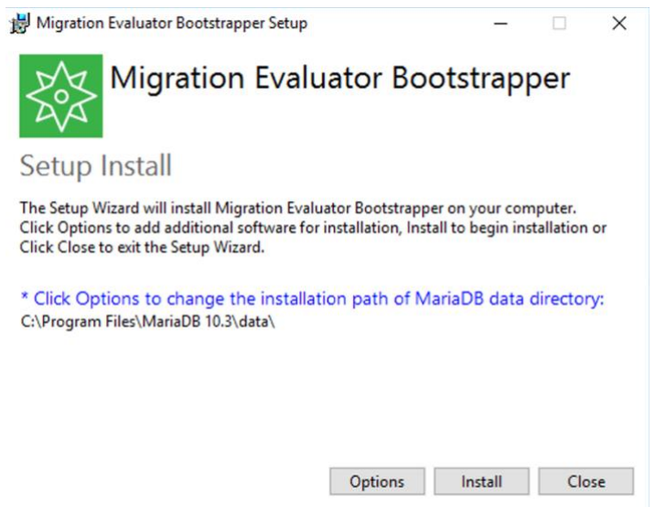
Preconditions

- 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 this 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 **TSOBootstrapper.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.
    a. 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.



3. 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, you *must* use the certificate that matches the assessment name.
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.

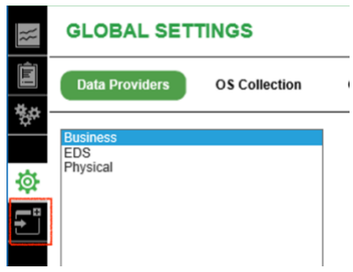
Preconditions

- 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

Operating System credentials are required if you are performing an Optimized License Assessment, want to include SQL Servers instances, have Hyper-V infrastructure, have bare-metal servers, or plan to visualize network dependencies.

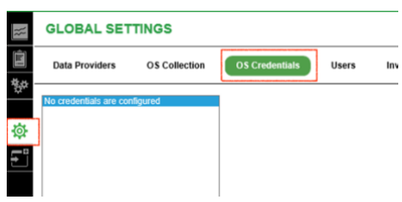
Preconditions

- 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 connecting 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**
- If you have Microsoft SQL Server databases being monitored, have you verified account credentials and network connectivity?
    - See **Appendix J – Connectivity to SQL Server**
- 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 or network connections directly from each server, or discovering SQL Server instances.

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**.
        i. Note. SNMP does not capture hyperthreading configuration from Linux, or provisioning details from Window Server. Linux workloads are assumed to have two threads per core. WMI credentials are recommended for Windows Server workloads.
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**, **Appendix F – Connectivity to Hyper-V Hosts, and Appendix J – Connectivity to SQL** Server
4. If WMI is being used for SQL Server Discovery, T-SQL is not required. Otherwise, for each SQL Server database credential to be used, select **New**, then **T-SQL** from the protocol dropdown.
    a. Configure as many T-SQL credentials as needed. See **Appendix J – Connectivity to SQL Server.** Domain accounts are not supported.

5 – Configure Collection from Bare Metal Servers

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

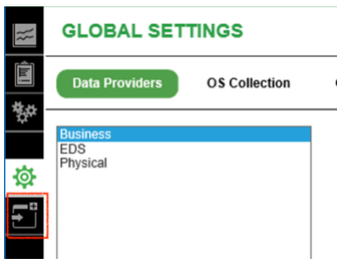
Preconditions

- 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.

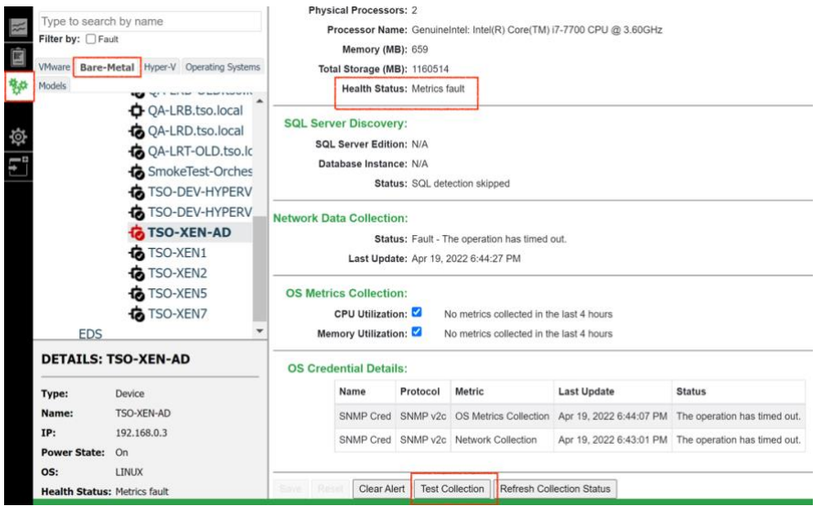
Steps

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 header and list of servers to be monitored.
    a. Note that the file must have a .CSV file extension and be formatted as shown in **Appendix H – CSV Example for Monitoring Bare Metal Servers.**
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 validate the format and content of the CSV file. This initial cycle can take more than 10 minutes to complete.
6. Verify that at least one server you expect should work can be monitored. To do this, select the **Device Settings** from the navigation bar and select the **Bare-Metal** view. Navigate to a server you would like to test and select **Test Collection**.



    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
    b. **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.

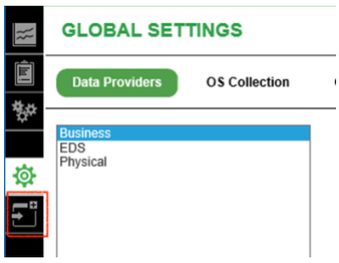
Preconditions

- 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 **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**
- Have you verified account credentials and network connectivity?
    - See **4 – Configure Operating System Credentials**

Steps

The Migration Evaluator Collector automatically scans all discovered virtual machines and bare-metal servers every 24 hours using the WMI and T-SQL credentials configured in step **4 – Configure Operating System Credentials**. To initiate the scan immediately:

1. 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 all 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

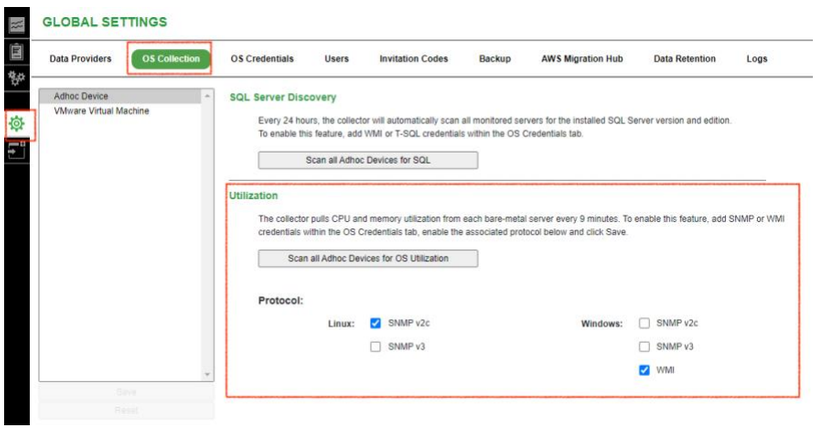
- Has the Migration Evaluator Collector software been installed and configured?
    - See **3 – Configure Collection from VMware**
    - See **6 – Configure Collection from Hyper-V Servers**
- Have you verified account credentials and network connectivity?
    - See **4 – Configure Operating System Credentials**

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

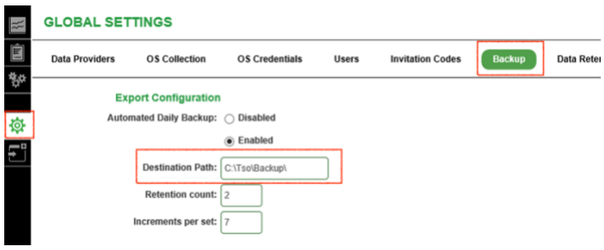
Preconditions

- Have you verified network connectivity from the server for the Migration Evaluator Collector to the Amazon S3 bucket hosted in the US East 1 region?
    - See **Appendix G – Connectivity to AWS**
- 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

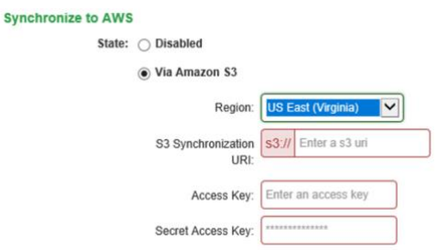
Steps

Once the collector software is installed and monitoring your infrastructure, it is time to configure data synchronization to Migration Evaluator 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 verify, select **Global Settings**, then **Backup**.

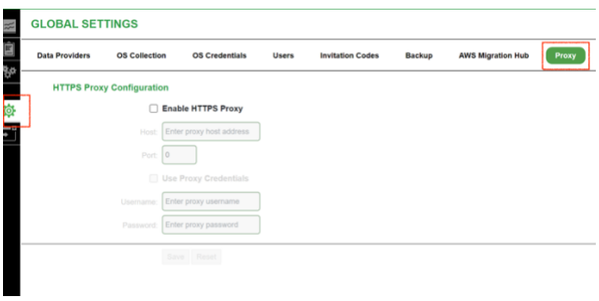


2. Configure the Amazon S3 synchronization setting based on your collector details listed in the Migration Evaluator Management Console: https://console.tsologic.com/discover/collectors



    a. Note: if you have multiple engagements with Migration Evaluator, each collector is given a unique Amazon S3 URI and access key which is linked to the certificate used during installation.

3. If direct egress traffic is not available, configuration of an HTTPS proxy is supported on the **Proxy** tab.



4. Select **Initiate Backup Now** to verify both the backup and synchronization is working.

    b. 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 Provisioning** 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 Provisioning** sheet:
        i. Verify the inventory contains everything expected to be in-scope
        ii. Verify the server provisioning was discovered. If not, manually add the core count, memory and storage.
        iii. 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.
        ii. For servers discovered, but not to be included in the analysis, fill in the In Scope attribute as False.
    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.
    a. Go to https://console.tsologic.com/discover/self-reported-files.
    b. If you have multiple engagements, select the engagement associated with this collector.
    c. Select **Upload** and the **Inventory and Utilization Export** file format.

11 – Export Discovered Inventory and Utilization into AWS Application Discovery Service

Skip this section if you do not want to leverage AWS Application Discovery Service to store discovered servers and their measured utilization.

Preconditions

- Have you created an AWS account?
    - https://docs.aws.amazon.com/application-discovery/latest/userguide/setting-up-signup.html

Steps

AWS Application Discovery Service (ADS) helps enterprise customers plan migration projects by gathering information about their on-premises data centers. Use the following steps to archive the information discovered by the Migration Evaluator Collector in an AWS account.

1. From the Migration Evaluator Collector software, select **Global Settings** from the Navigation bar, then the **AWS Migration Hub** tab
2. Download a pre-populated ADS import template by selecting **Download Export**.
3. Configure the AWS region where the discovered data is stored. *Note*: this may be different from the region used by Migration Evaluator.
    a. Log into the **AWS Management Console** via https://aws.amazon.com/console/
    b. Navigate to **AWS Migration Hub** from the list of available services.
    c. On your first log in, you will be prompted to configure your home Region on the **Migration Hub Settings** page. This region is where your data is stored and does not impact which destination region you use for your migration. Available regions can be found at https://docs.aws.amazon.com/general/latest/gr/migrationhubn.html
4. Upload the CSV file generated by the Migration Evaluator Collector into an **S3 bucket within your AWS account**. To learn about the permissions needed and creating an S3 bucket, please follow the AWS Application Discovery import guide:
    a. https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-import.html
5. Import the file uploaded to S3 into your AWS Migration Hub account by navigating to the **Tools** page within **Discover**, then selecting **Import**. To learn more, please follow the AWS Application Discovery import guide:
    a. https://docs.aws.amazon.com/application-discovery/latest/userguide/discovery-import.html

12 – Configure Network Connection Collection for Network Visualization

Skip this section if you do not want to leverage AWS Migration Hub to visualize the server-to-server dependencies.

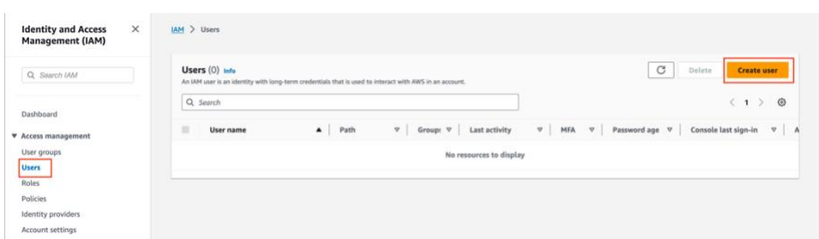
Preconditions

- Have you created an AWS account?
    - https://docs.aws.amazon.com/application-discovery/latest/userguide/setting-up-signup.html
- Have you verified network connectivity from the server for the Migration Evaluator Collector to AWS Application Discovery Service (ADS) in your AWS Migration Hub home region?
    - See **Appendix G – Connectivity to AWS**
- 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 verified account credentials and network connectivity?
    - See **4 – Configure Operating System Credentials**

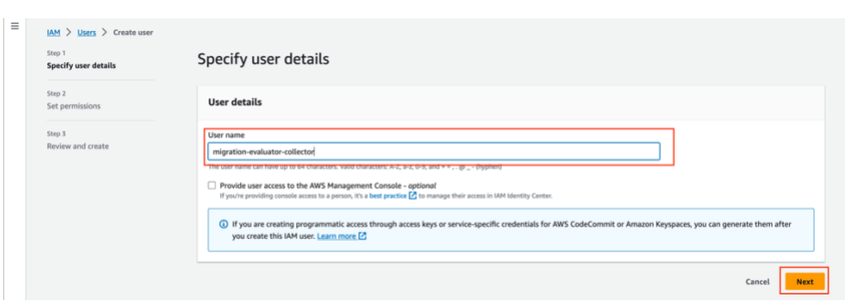
Steps

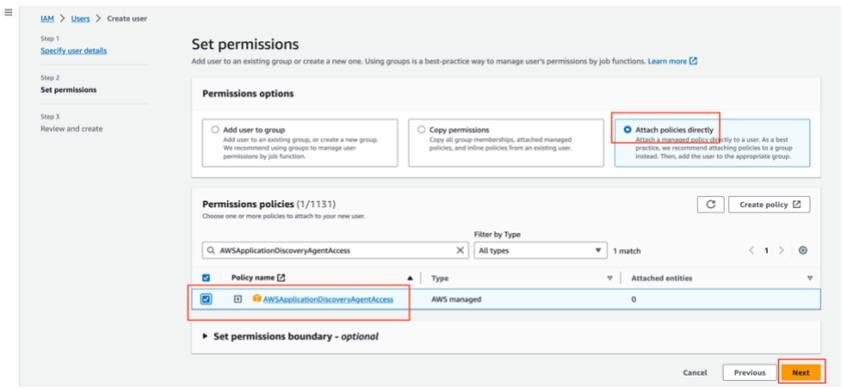
AWS Migration Hub network visualization accelerates migration planning by quickly identifying servers and their dependencies, identifying the role of a server, and grouping servers into applications. The Migration Evaluator Collector may be configured to monitor active TCP connections and store this data in AWS Application Discovery Service (ADS).

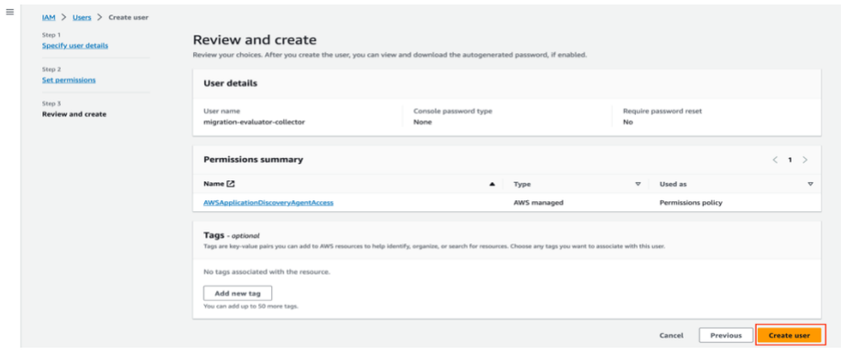
1. Configure the AWS region where the discovered network data is stored. *Note*: this may be different from the region used by Migration Evaluator.
    a. Log into the **AWS Management Console** via https://aws.amazon.com/console/
    b. Navigate to **AWS Migration Hub** from the list of available services.
    c. On your first log in, you will be prompted to configure your home Region on the **Migration Hub Settings** page. This region is where your data is stored and does not impact which destination region you use for your migration. Available regions can be found at https://docs.aws.amazon.com/general/latest/gr/migrationhubn.html
2. Create an AWS Identity and Access Management (IAM) user within your AWS account for the Migration Evaluator Collector. We strongly recommend that you not use the root user for everyday tasks, even the administrative ones. Instead, follow the security best practices (https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html) and create a unique user for this collector and grant the least privilege.
    a. Log into the **AWS Management Console** via https://aws.amazon.com/console/
    b. Navigate to **Users** within the **Identity and Access Management** service, and select **Create user.**



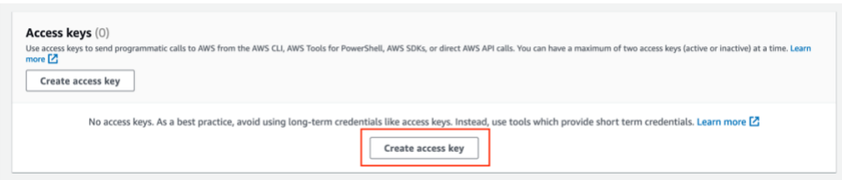
    c. Give the user a name, and apply the **AWSApplicationDiscoveryAgentAccess** managed policy.

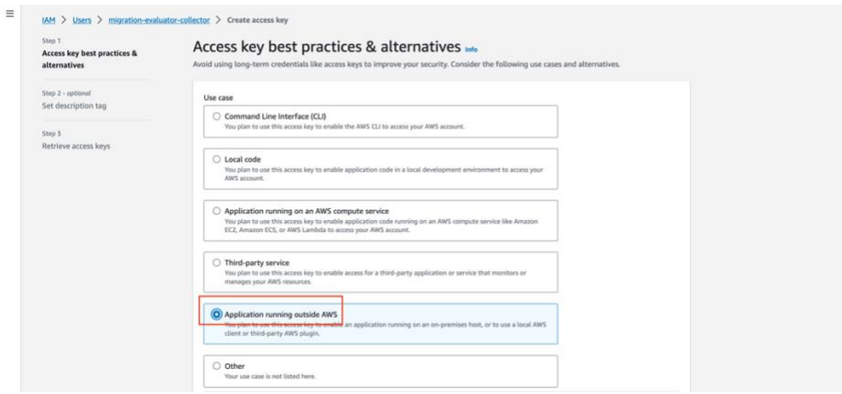


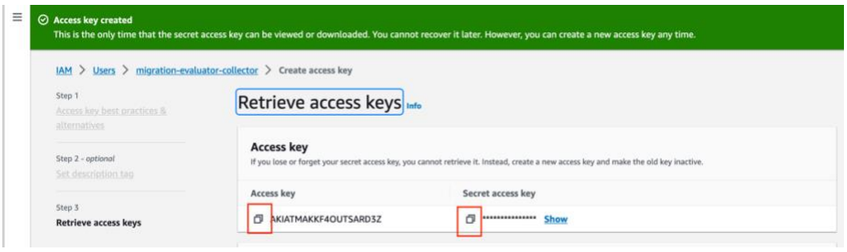




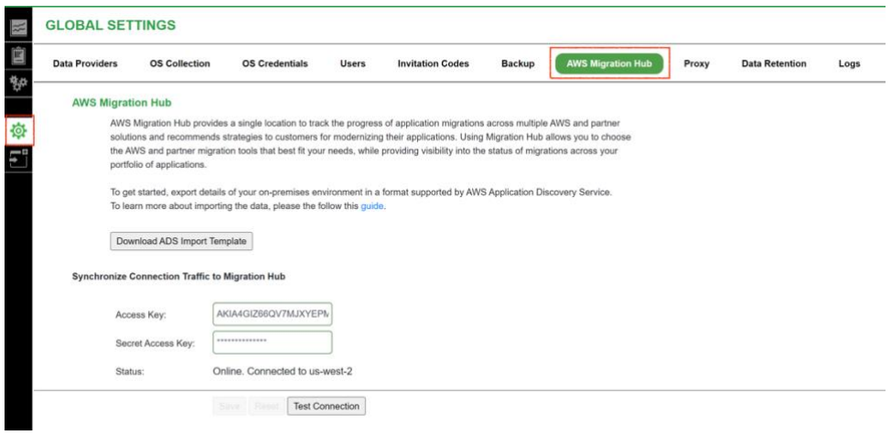
d. Generate an access key by selecting the user just created, navigating to the **Security credentials** tab, then selecting **Create access key**. Select the **Application running outside AWS use case**. Keep the browser window open to copy the keys into the next step.



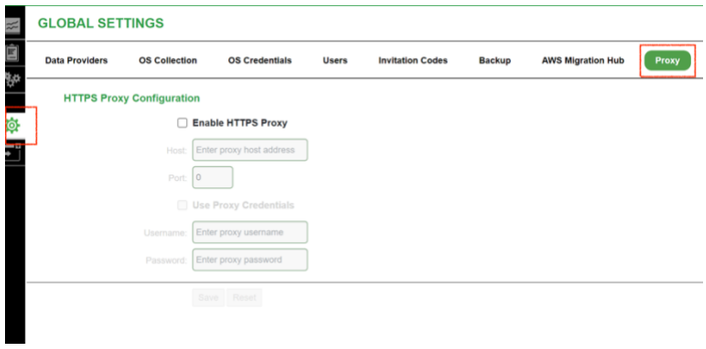




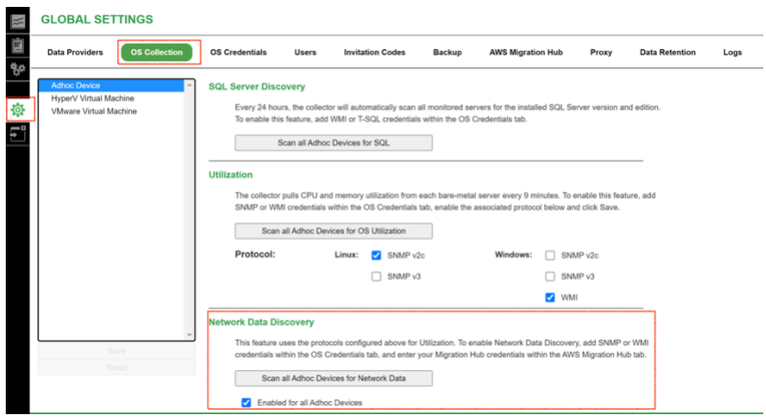
3. Within your Migration Evaluator Collector, navigate to the **AWS Migration Hub** tab within **Global Settings** and configure the **Access Key** and **Secret Access Key** created in the previous step. select **Save**.



a. If the Status reported is **Offline. Cannot Connect to AWS**, the optional configuration of an HTTPS proxy may be added on the **Proxy** tab. **See Appendix P – Troubleshooting Collector Configuration** for details.



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



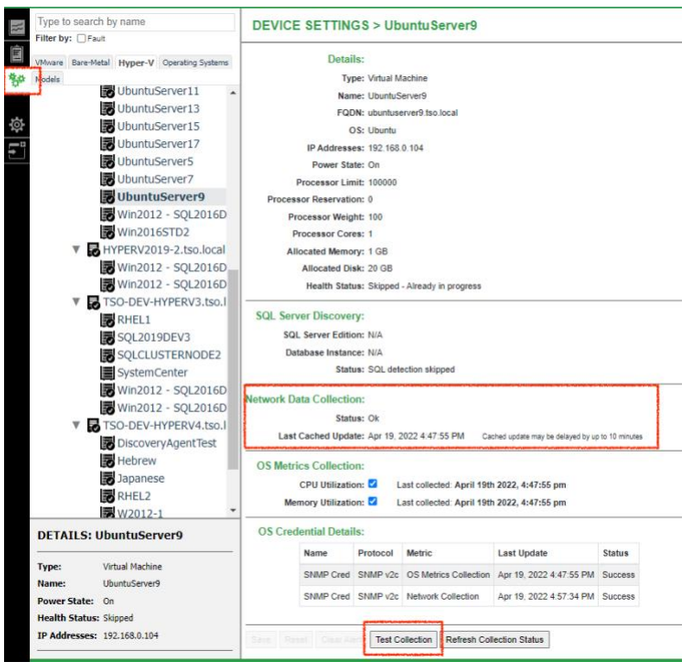
5. For each data type configured (Adhoc Device, VMware Virtual Machine and Hyper-V Virtual Machine):

    a. Enable network connection collection

6. Select **Scan all** to initiate the scan.

    a. The collector will automatically attempt to collect network connection data every 60 seconds 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.

7. Verify that at least one server you expect should work can be monitored. To do this, select the **Device Settings** from the navigation bar. Navigate to a server you would like to test and select **Test Collection**.



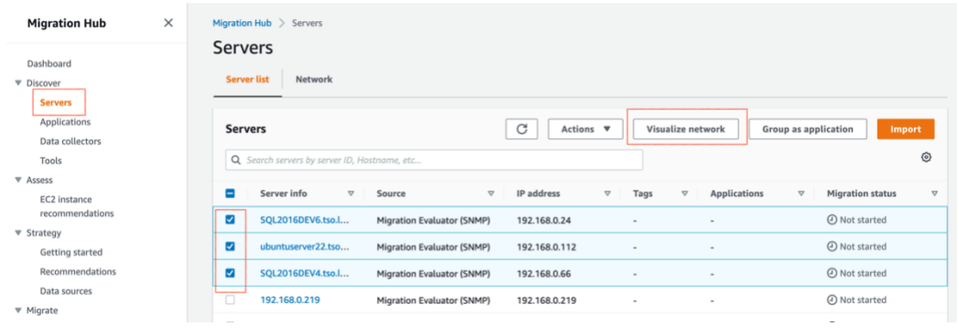
a. If no credentials are successful for Network Collection, please review the **OS Credential Details** section for each configured OS credential's status, as well as

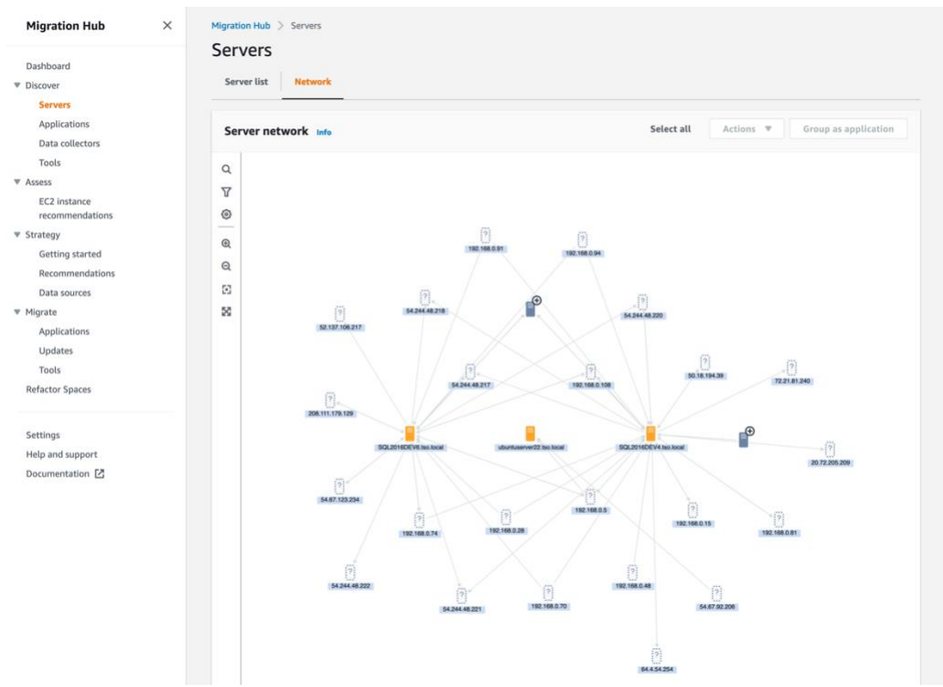
b. **Appendix Q – Troubleshooting Operating System** Collection**.**

8. Once configuration is complete, you may view the server-to-server dependency graph within AWS Migration Hub. *Note*: The Migration Evaluator Collector sends connected network data every 15 minutes.

   a. Log into the **AWS Migration Hub Console** at https://aws.amazon.com/console/

   b. Select **Servers** from the left-side navigation under **Discover**. Select the servers you wish to inspect, then press **Visualize network**. To learn more about using AWS Migration Hub, go to: https://docs.aws.amazon.com/migrationhub/latest/ug/network-diagram-how-to.html





Appendix A – Server Hardware Requirements

The Migration Evaluator Collector requires one new server running the English version of Windows Server 2016 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 are for a standard two-week engagement
- English version of Windows Server 2016 or greater
- Default system UI language and 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 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

SNMP does not capture hyperthreading configuration from Linux, or provisioning details from Window Server. Linux workloads are assumed to have two threads per core. WMI credentials are recommended for Windows Server workloads.

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
TCP Connections	1.3.6.1.2.1.6.13.*	1.3.6.1.2.1.6.13.*

Appendix E – Connectivity via WMI

The Migration Evaluator Collector requires the following to monitor Microsoft 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
    - \root\standardcimv2 (Windows Server 2012 or greater)

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 AWS

The Migration Evaluator Collector supports synchronizing collected data to both the Migration Evaluator managed Amazon S3 bucket in US East-1, and AWS Application Discovery Service (ADS) in the customer's AWS Migration Hub home region.

Egress HTTPS traffic to the AWS managed, Amazon S3 bucket goes to https://s3.amazonaws.com/tsologic-match-us-east/.

Egress HTTPS traffic to the customer managed AWS ADS account first connects securely with your home region, then registers with Application Discovery Service.

- For example, if eu-central-1 is your home region, the Migration Evaluator Collector registers arsenal-discovery.eu-central-1.amazonaws.com with Application Discovery Service.

If direct egress traffic is not available, configuration of an HTTPS proxy is supported.

Connectivity to AWS is optional for a Migration Evaluator assessment. If not configured, a manual export from the Migration Evaluator Collector will be required to be uploaded to the Migration Evaluator Console.

Connectivity to AWS is required for network visualization in AWS Migration Hub.

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.

Note, if enabling Network Connection Collection for Network Visualization, an IP address for each server must be provided.

```
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 to SQL Server

The Migration Evaluator Collector can discover SQL Server workloads via either WMI or T-SQL. If both are configured WMI, will be used as it supports discovering SQL workloads on non-standard ports.

If using WMI, the Migration Evaluator Collector requires:

- 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
- A local administrator or a domain account that is a member of the following group:
    - Local Windows Administrators
- Access to the following namespace (and subfolders)
    - \root\Microsoft\SqlServer

If using T-SQL, the Migration Evaluator Collector requires:

- 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

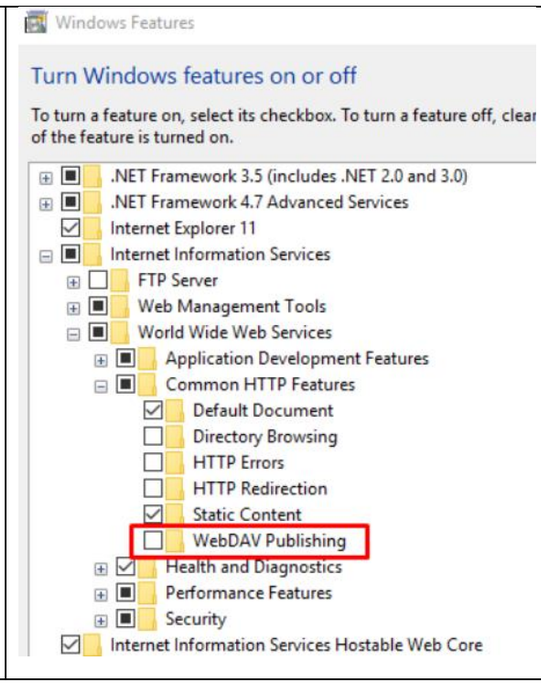
In the event that all configured WMI or SNMP credentials fail to authenticate with a server, the Migration Evaluator Collector will exponentially reduce the frequency of attempts. After 2 consecutive failures, attempts will happen after 30 minutes, 2 hours, 8 hours, then 24 hours. After 6 failed attempts, the collector will continue to try once every day all configured credentials.

To force a collection attempt after adding new credentials or resolving a client-side issue, 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: Execute local unsigned PowerShell Scripts In PowerShell with "Run as Administrator" option. `set-executionpolicy remotesigned` If using a local account: 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: PROPERTY CHANGE: Adding CA_ERROR property. Its value is '0x80070542 - CheckTokenMembership failed: 0x80070542'. Action ended	Ensure user used to install has **local** administrator rights on the server with the following rights: Logon as service Logon as batch job Logon locally Member of Builtin\Performance Monitor Users group Member of Administrators group
Log contains: RabbitMQ failed to install	When using a user not tied to a domain to install the bootstrapper. 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. Ensure that the home directory for the user is local and not a network share Once resolved, install the Bootstrapper again on the same server.
Installation aborts with the message: The installation has been aborted due to WebDAV being enabled.	Error caused by WebDAV Publishing enabled on the server running the Migration Evaluator Collector. To disable, do the following: Search for "Turn Windows Features On or Off" Uncheck the box on WebDAV Publishing

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, a dialog box containing the error will be displayed. On exit of the installer, the installation's log file will be opened automatically. The specific error can be found by searching the log file for **value 3**.

Note - All logs are also written to the user's temp folder which can be found by typing **%temp%** into Windows Explorer's address bar.

Problem	**Solution**
Permissions / Policies	
CheckTokenMembership failed: 0x80070542	Related to permissions of the user running the installer. To start installation: Right-click installer > Run as Administrator
An error occurred while setting up MariaDb encryption: 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' Use non-FIPS compliant algorithms for encryption, hashing and signing To resolve, run gpedit.msc Navigate to Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options Right-click on "System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing From Properties dialog select "Disabled" If after updating the Group Policy, the error still persists, try having the system admin run the following command: `gpupdate /force`
Server Settings / Existing Software Conflicts	
This application is only supported on US English language versions of Windows (en-US). Or ERROR 2019 (00000): Can't initialize character set auto (path: compiled_in) Retrying with old credential 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. Only Windows 2012 R2 or greater with the default system UI language and system locale configured to EN-US (English United States) is supported. To verify, run the following command: `dism /online /get-intl` To fix, change the system locale to English: Go to "Control Panel" > "Region" > "Administrative" Tab 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" Line: 2733 Position: 0 Statement Type: Create Message: Error on rename of '.\tso\assignmentvendorvirtualserver.TRG~' to	Installation attempted on a server with anti-virus software blocking required installation steps. Please remove or temporarily disable the anti-virus software and retry installation of the collector msi.

'.\tso\assignmentvendorvirtualserver.TRG' (Errcode: 13 "Permission denied") … … CustomAction UpdateDBElevated returned actual error code 1603 (note this may not be 100% accurate if translation happened inside sandbox) Action ended 14:52:35: InstallFinalize. Return value 3.	
Start: Setup MariaDb encrypion Warning: One or more file(s) needed for encryption already exist MariaDb encrypion settings already exist Finish: Setup MariaDb encrypion . . . Provisioning Database User Accounts 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 ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)	Migration Evaluator Collector software is already installed on this server. Installer failed initially and was run again on the same server Figure out the cause of the first installation failure (typically permission error) Provision a fresh server/virtual machine and retry installation after addressing the initial issue. *Note: Alternately, refresh current server back to a new template VM state, and reattempt installation starting with bootstrapper installation.*

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: Web browser is stuck on loading screen with the animating dots 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: • RabbitMQ service isn’t running, attempting to start succeeds, but it immediately stops • RabbitMQ service is running, but the service description column is completely blank (it should say “Multi-protocol open-source messaging broker”) 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: C:\Users\TSOOpCenter\AppData\Local\TsoLogic\recovery.txt
After logging into Collector Web UI, the navigation loads, but a number of pages are blank Windows Services shows TSO Power Service status as not running. Windows Event Viewer shows an Error for the ECczarPowerService that includes: Failed to decrypt using provider ‘MyUserDataProtectionConfiguration Provider’	The user configured in section 2, step 4 of the install guide to run the Migration Collector has either been changed or its password is no longer validate. To resolve: 1. Open Windows Services by running the ‘services.msc’ command 2. Select ‘TSO PowerService’ service 3. Confirm the configured user is the same account used during configuration. The configured user cannot be changed post installation Confirm the password entered is still valid for this user
Configuration Updates	

Linux bare-metal servers being detected as Windows	The collector leverages ICMP fingerprinting to detect which Operating System Credential to use. Servers with a ping TTL greater or equal to 65 and less than or equal to 128 are assumed to be running Windows; otherwise, the server assumed to be running Linux.
	
	To override the ICMP based detection, adjust your existing bare-metal CSV to the following format:
	
	`NAME,IP,FQDN,Operating System`
	`server-1,192.168.0.1,,Windows`
	`server-2,192.168.0.2,,Linux`
	`server-3,,baz.example.com,Linux`
	
	Once complete, follow solution steps identified when you “Need existing list of bare-metal server to be updated”.

Need existing list of bare-metal servers to be updated	To remove / add bare-metal servers to the collector: 1. Make adjustments to the original CSV file used for configuration 2. In Global Settings > Data Providers, select the existing bare-metal configuration

	3. Click “Upload” and select the updated CSV file 4. Click “Save” **⚠ Important** The uploaded CSV file should contain all bare metal servers in scope for the assessment. Do not create a new data provider as this will result in duplicate severs.
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 Ensure the server where Migration Evaluator Collector is installed has egress HTTPS access (**Appendix G – Connectivity to AWS**) If an HTTPS proxy was configured in **9 – Configure Synchronization with the Migration Evaluator**, verify the password and address is correct. Review with your proxy’s administrator that the required access was granted. For further assistance, supply log files to your assigned Migration Evaluator specialist. If the collector was installed under a Service Account: C:\Users\<username>\AppData\Local\TsoLogic\logs If the collector was installed under “Local System”: C:\Windows\System32\config\systemprofile\AppData\Local\tsologic\logs
Migration Evaluator team is unable to confirm successful sync	
Error found in Global Settings > Logs: [TSO.Common.AwsS3Sync.AwsS3SyncTool] Unknown error occured while uploading JSON to S3: Specified method is not supported.	
Error found in Global Settings > Logs: 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. 1. Download the certificate for this Migration Evaluator engagement from: https://console.tsologic.com/discover/collectors 2. Delete all of the existing files from the local collector machine (path configured Global Settings > Backup) 3. Replace the certificate • Open "certlm.msc" (Start -> Run) • Navigate to Certificates (Local Computer) > TSO Logic Inc > Certificates • Right-click on the existing certificate there and select Delete • Click Yes to permanently delete the certificate • Right-click in the right pane (where the certificate you just deleted was listed) and select All Tasks > Import • This will start the Certificate Import Wizard, click Next until you see "File to import" • Select the new certificate file and click Next

	• On the Certificate Store dialog Place all certificates in the following store: TSO Logic Inc should be selected
	• Click Next. Click Finish
	4. Reset Registry Keys (local system user during installation)
	• Open "regedit.exe" (Start > Run)
	• Navigate to in regedit
	  • Local system user used during installation.
	`HKEY_USERS\.DEFAULT\Software\TSO Logic\TSO logic`
	  • Service account user used during installation.
	`HKEY_USERS\<<user SID>>\SOFTWARE\TSO Logic\TSOlogic`
	• Edit key listed and erase the values for (double click the key, set Value data to blank) LastKnownFullBackupDir, LastBackupMetricTime, LastBackupAppDataTime, LastBackupWinEventLogTime, LastBackupWinEventLogID
	5. Initiate backup from: Global Settings > Backup > Initiate Backup Now

Synchronization with AWS Application Discovery Service and AWS Migration Hub	
Global Settings > AWS Migration Hub reports connection **Offline. Invalid IAM Credential**	Ensure the IAM access key and secret access key configured is for the AWS account to be used for storing network connection data. Ensure there is no Service control policy (SCP) in either the destination AWS account, organizational unit, or root AWS account that is restricting access to Migration Hub or Application Discovery Service. For details on setting up the IAM user please see: https://docs.aws.amazon.com/application-discovery/latest/userguide/setting-up-iam.html For details on the managed policy, please see: https://docs.aws.amazon.com/application-discovery/latest/userguide/security-iam-managed-policies.html For details on service control policies, please see: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps.html
Global Settings > AWS Migration Hub reports connection **Offline. Cannot Connect to AWS.**	Ensure the server where Migration Evaluator Collector is installed has egress HTTPS access **(Appendix G – Connectivity to AWS)** If an HTTPS proxy was configured, verify the password and address is correct. Review with your proxy's administrator that the required access was granted.
Global Settings > AWS Migration Hub reports connection **Offline. No AWS Migration Hub home region configured.**	Ensure the AWS Migration Hub home region was configured for the AWS account to be used. For details on configuring the home region, please see: https://docs.aws.amazon.com/migrationhub/latest/ug/home-region.html

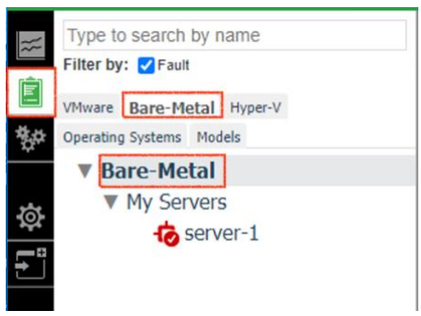
Appendix Q – Troubleshooting Operating System Collection

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.

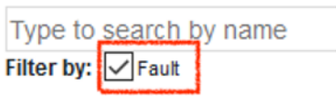
Identifying Servers Requiring Attention

To identify servers experiencing WMI or SNMP based collection faults:

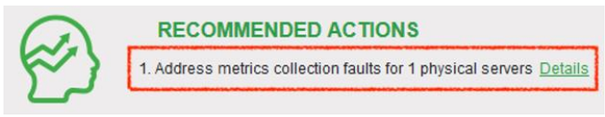
1. Select **Status Report** from the Navigation bar, select either the **VMware**, **Bare-Metal**, or **Hyper-V** view and the top node in the tree.



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**. Confirm that both the server running the Migration Evaluator Collector and all servers being monitored, have all Microsoft security updated applied relating to CVE-2021-26414 - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414
System.Management.ManagementException: Timed out	Network issues with WMI. Confirm connectivity from collector server to target server(s): Network connectivity via ICMP 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)
	
	`\root\cimv2`
	
	`\root\default`

Access Denied to namespace "standardcimv2"	WMI credentials do not have access to required "StandardCimv2" namespace. Fix credential permissions on target server to have access to the namespaces (and their subfolders) `\root\standardcimv2`
System.Management.ManagementException: Invalid namespace	MSFT_NetTCPConnection class used to collect network connection is available on Windows Server 2012 or greater. https://docs.microsoft.com/en-us/previous-versions/windows/desktop/nettcpipprov/msft-nettcpconnection
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
WMI credentials report no errors, but SQL Server instances are not found	WMI credentials do not have access to required namespace. Fix credential permissions on target server to have access to the namespaces (and their subfolders) WMI credentials are not a domain user which is a member of the Local Administrators group. Fix credential permissions on target server.

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 and verify a response without a timeout. 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 queries against the root\standardcimv2 namespace. If the result set is empty, the calling account does not have the required permissions
    a. SELECT LocalAddress, LocalPort, RemoteAddress, RemotePort, State FROM MSFT_NetTCPConnection
6. 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

7. 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
8. 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. SNMPv3 configured – The username and password are (likely) wrong. 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 tools, 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 and verify a response without a timeout. 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.