



VMware TAM Data Collector Installation and User Guide

Release 2.0

April 2016

For Use by VMware and VMware Customers

© 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book..... 5

 Intended Audience 5

 Support, Feedback, and Questions..... 5

1. Introducing TAM Data Collector 6

 1.1 Use Cases..... 6

 1.2 Security 6

2. Installing and Configuring TAM Data Collector 8

 2.1 System Requirements..... 8

 2.2 Installing and Configuring TAM Data Collector 8

3. Working with TAM Data Collector 17

 3.1 Setting Up Access to vCenter Server 17

 3.2 Setting Up Access to View Connection Server 18

 3.3 Using the Project Explorer 21

Appendix A: Examples of vCenter CSV Data 29

About This Book

This guide describes how to install, configure, and use the VMware TAM Data Collector.

The contents of this guide are also available by clicking **Help** and selecting **User Guide** in the TAM Data Collector user interface.

Intended Audience

The information provided in this guide is intended for use by VMware Technical Account Managers (TAMs) and VMware customers who have a current Services Software Solutions subscription.

Support, Feedback, and Questions

Contact services-software-support@vmware.com if you have questions, require support, or have suggestions for improving the TAM Data Collector documentation.

1. Introducing TAM Data Collector

The TAM Data Collector collects key statistics and usage information from VMware virtual infrastructure and VMware Horizon® View™ deployments to be sent to and analyzed by the VMware TAM team as well as the VMware Phone Home Customer Intelligence team..

1.1 Use Cases

TAM Data Collector is designed for the following use case.

1.1.1 Customer Completes Data Collection

Customers can install the TAM Data Collector to collect usage data. Customers collect data, export the project file, and provide it to VMware Technical Account Managers (TAMs) in person or by email. If the customer agrees to send data to VMware in the initial customer agreement, then data is sent to the VMware Phone Home network by the TAM at a later stage of the TDM process.

1.2 Security

To collect VMware vCenter® data, the TAM Data Collector connects to VMware vCenter Server® over port 443 using the VMware API. To collect data from View, TAM Data Collector uses a proprietary protocol over port 443.

During data collection, the communication between TAM Data Collector and the target servers is secured with HTTPS (HTTP over SSL, default port 443). For the TAM Data Manager virtual appliance, data is stored in a local database protected by VMDK file system security. For the TAM Data Collector application, the file is protected by default Windows or Mac OSX security. TAM Data Collector collects only general inventory, configuration, and some utilization information.

TAM Data Collector requires only minimal permissions (Read Only for vCenter and Read Only Administrator for the View Connection Server) for data collection, so consultants or administrators can use the inherent security and authorization features of vCenter Server to create an account without compromising the security of the customer's VMware vSphere® and View environments. TAM Data Collector does not store the password of the Read Only account or any customer account.

TAM Data Collector uses the following ports.

Table 1. TAM Data Collector Network Ports

Port	Protocol	Description
22	SSH	Inbound TCP port that is used by an administrator to log in to the TAM Data Collector virtual appliance to perform maintenance tasks. This port is not used by the TAM Data Manager application.
443	HTTPS	Outbound TCP port that is used by TAM Data Collector to retrieve data from the vCenter Server. This port is specified when configuring TAM Data Collector to retrieve data and might be different depending on the environment.
8080	HTTP	Inbound TCP port that is used by the TAM Data Collector user interface.
80 and 8080	HTTP	Both inbound TCP ports are used by the TAM Data Collector virtual appliance user interface.
41984		Port used for the TAM Data Collector database.
41985		Port used for TAM Data Collector database event service.
5480	HTTPS	Inbound TCP port used to access the TAM Data Collector virtual appliance management Web interface from a browser.

2. Installing and Configuring TAM Data Collector

The following sections describe how to install and configure TAM Data Collector.

2.1 System Requirements

TAM Data Collector is available as a Java application or as a virtual appliance. The TAM Data Manager user interface uses HTML and JavaScript, and is accessed through a Web browser. Before installing TAM Data Manager, confirm that the following system requirements are satisfied.

- Platform options:
 - TAM Data Collector Application – Microsoft Windows Server 2008 or later, Windows 7 or later, or Apple Mac (Lion, Mountain Lion, Mavericks, Yosemite, or El Capitan)
 - TAM Data Collector Virtual Appliance – Directly import and power on the OVF file containing the TAM Data Collector virtual appliance using the VMware vSphere Client™ (4.0 or later), VMware Workstation™ (9 or later), or VMware Fusion® (5 or later)
- At least 3 GB RAM
- JRE 1.8 (64-bit JRE is recommended for large environments). JDK 1.8 is recommended on Mac OSX

Note Do not run TAM Data Collector on the same machine that runs vCenter.

2.2 Installing and Configuring TAM Data Collector

Before installing TAM Data Collector, verify that you have satisfied all of the system requirements and review the *TAM Data Manager Release Notes* for information that might affect your installation.

Obtain the installation package (TAM Data Collector application or TAM Data Collector virtual appliance) from your VMware TAM.

2.2.1 Installing the TAM Data Collector Application

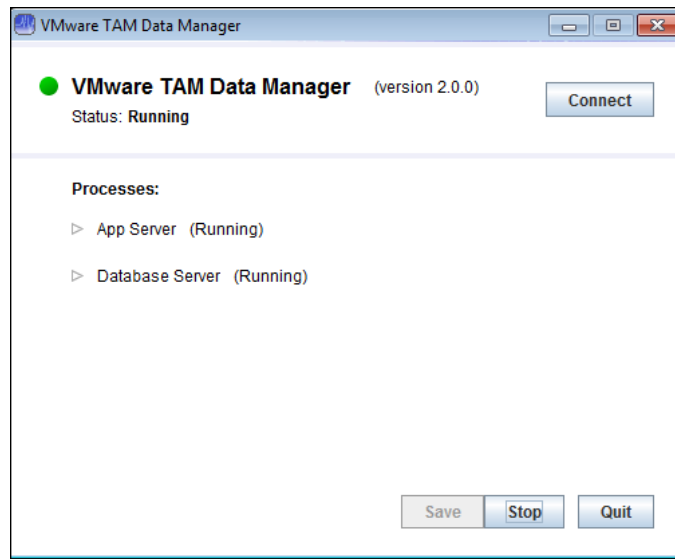
The following procedure shows how to install the TAM Data Collector application and display the user interface. If you have any issues completing this procedure:

- You might need to change browser proxy settings if proxies are used as part of the corporate firewall. See Section 2.2.4, Change Browser Proxy Settings.
- Examine the files in the `logs` folder within the installation folder.

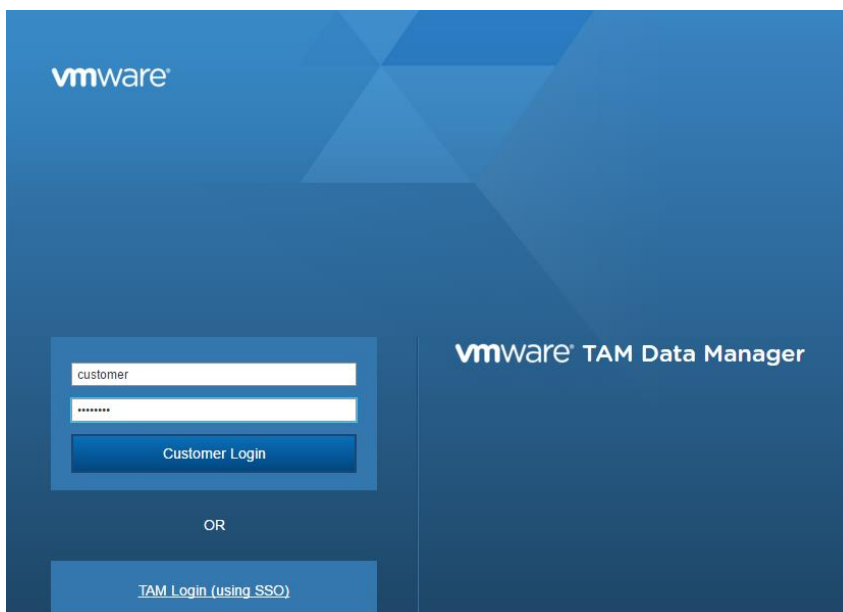
If you still have trouble, contact VMware Support.

To install and open the TAM Data Collector application

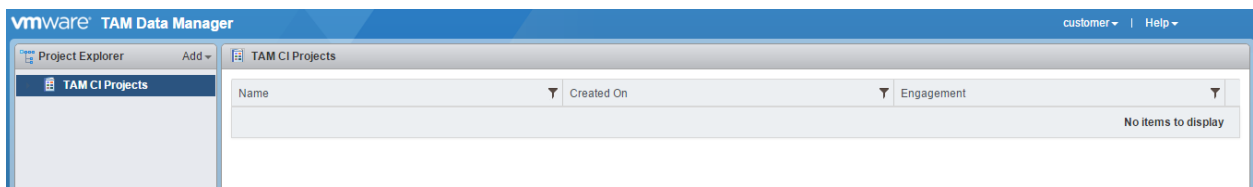
1. Download the TAM Data Collector application installation file.
2. Unzip the installation package and open the folder containing the unzipped files. Avoid placing the unzipped package in a folder with a long path name or a folder name containing special characters.
3. Double-click `TAM Data Manager.jar`.
4. The TAM Data Collector launcher application opens. Verify that the App Server and the Database Server are running, and click **Connect** to start the TAM Data Collector user interface in a Web browser. Review and accept the end user license agreement, if prompted to do so.



5. Log in to the TAM Data Collector user interface with the default username **customer** and password **customer**.



The interface opens to show the Project Explorer.



2.2.2 Installing the TAM Data Collector Virtual Appliance

The following steps are required to install the TAM Data Collector virtual appliance and display the user interface:

1. Download Installation Files and Power on the Virtual Appliance.
2. Log in to the Virtual Appliance.
3. Identify or Configure the Virtual Appliance IP Address.

4. Change Virtual Appliance Proxy Settings.
5. Change the Amount of Tomcat Process Memory, if needed.
6. Change Browser Proxy Settings.
7. Access the TAM Data Collector User Interface.

2.2.2.1. Download Installation Files and Power on the Virtual Appliance

To download installation files and power on the virtual appliance

1. Download the TAM Data Collector virtual appliance installation file.
2. Unzip the installation directory file.
3. Import the OVA file using vSphere Client (4.0 or later), Workstation (9 or later), or VMware Fusion (5 or later).
4. Power on the virtual appliance.

The virtual appliance must continue to run until you are finished using the TAM Data Collector user interface. You can minimize its window or run the process in the background.

2.2.2.2. Using the Virtual Appliance Web Console

The TAM Data Collector virtual appliance provides a Web console management user interface. This is the standard Web console for virtual appliances and VMware vSphere vApps™ generated using VMware Studio™. Instead of using the command line, you can use the Web console to perform tasks such as reboot, shutdown, setting the system time zone, finding or changing the appliance IP address, and changing network or proxy settings.

2.2.2.3. Log in to the Virtual Appliance

To log in to the virtual appliance Web console

1. Open your browser and go to `https://<virtual appliance IP address>:5480`.
2. **User name is root** and **Password is vmware**.

If you cannot access the appliance Web console, check proxy settings between the appliance and the browser. See Section 2.2.4, Change Browser Proxy Settings.

To log in to the virtual appliance command-line interface

1. At the login prompt, type **root** and press **Enter**.
2. For password, type **vmware** and press **Enter**.

To maintain security, change the password immediately after logging in for the first time.

2.2.2.4. Identify or Configure the Virtual Appliance IP Address

You need to know the virtual appliance IP address to display the TAM Data Collector user interface or the virtual appliance Web console. By default, the virtual appliance is configured to use DHCP, but you can configure it to use a static IP address.

To display the DHCP IP address from the vSphere Client

1. Power on the virtual appliance.
2. Open the vSphere Client.
3. Click the **Summary** or **Console** tab to display the IP address.

To display the DHCP IP address from Workstation

1. Power on the virtual appliance.
2. The IP address is displayed as the virtual appliance starts.

To display the DHCP IP address from the command-line

Type `ifconfig` at an appliance command-line prompt. Use the `eth0 inet` address.

To configure a static IP address from the Web console

1. Open the TAM Data Collector virtual appliance Web console.
2. Click the **Network** tab, and click **Address**.
3. Select **Use the following IP settings**.
4. Enter the IP address and other network parameters (**Netmask, Gateway, Preferred DNS Server, Alternate DNS Server, Hostname**) and click **Save Settings**.

To configure a static IP address if the Web console is not available

When there is no DHCP server available in the network, the virtual appliance will start with no IP address. In this case, you can log in to virtual appliance console and run the VAMI scripts to configure the static IP address.

1. Open the vSphere Client or Workstation or Fusion console.
2. Log in to virtual appliance using user 'root' and password 'vmware'.
3. Run the script `/opt/vmware/share/vami/vami_config_net`.
4. Choose the option for **IP Address Allocation for eth0** and provide the static IP details.
5. You can also set the DNS, host name, default gateway from this menu.
6. Restart the virtual appliance.

2.2.2.5. Change Virtual Appliance Proxy Settings

If there is a proxy server set up between the virtual appliance and the Internet or vCenter, configure the virtual appliance to use the proxy server.

To configure the proxy

1. Open the TAM Data Collector virtual appliance Web console.
2. Click the **Network** tab.
3. Click **Proxy**.
4. Select **Use a Proxy Server**.
5. Enter the information about the proxy server:
 - **Proxy Server** – Enter the IP address or fully qualified domain name of the proxy server.
 - **Proxy Port** – Enter the port used by the proxy server.
6. Click **Save Settings**.

2.2.3 Change the Amount of Tomcat Process Memory

You can change the amount of memory allocated to the Tomcat process for TAM Data Collector. You might need to increase the amount of memory allocated if you are using TAM Data Collector in a large environment. The procedure differs according to whether you are using the TAM Data Collector virtual appliance or the Java application.

To change the amount of Tomcat memory with a virtual appliance

1. Log in to the virtual appliance using the user **root** and password **vmware**.
2. Open the configuration file using `vi` or another text editor:


```
vi /usr/share/vha/tomcat/conf/vha-tomcat-memory
```
3. Locate the default value of 2048 and change it to your desired value. This is the amount of memory allocated to Tomcat in megabytes.
4. Restart the appliance with the following command:


```
shutdown -r now
```
5. You can confirm that the memory value changed by issuing the following command and reviewing the argument `-Xmx`.


```
ps -ef | grep catalina
```

To change the amount of Tomcat memory using the Java application

1. Quit the TAM Data Collector Java application.
2. Go to the directory where the TAM Data Collector Java application was unzipped.
3. Open the configuration file using a text or XML editor:


```
<unzipped location>/resources/applicationContext.xml
```
4. Locate the `util:map` XML section that contains memory settings by searching for `vha-start`.

Change the `-Xmx` value to the desired value. For example, to change the Tomcat memory to 1024 MB, change the XML entries as follows:

```
<util:map id="vha-start" map-class="java.util.LinkedHashMap">
  <entry key="java" value="" />
```

```
<entry key="-Xmx1024m" value="" />
```

5. Save the file, and start the TAM Data Manager Java application.

2.2.4 Change Browser Proxy Settings

You might use proxies as part of your corporate firewall. A proxy server acts as an intermediary between a client computer and the Internet by intercepting requests and contacting the target server to make the request on behalf of the client. Proxies offer fast access to cached content, filter content, and hide computers from the Internet to improve security.

However, a proxy server will also prevent the TAM Data Collector user interface from accessing the appliance because it does not recognize that the appliance is running locally. If you are running the TAM Data Collector on a LAN that runs behind a proxy server, you probably need to change the proxy settings before you can display the TAM Data Collector user interface. VMware recommends that you bypass the proxy by configuring your browser proxy settings to add the TAM Data Collector virtual appliance to the list of addresses that do not use a proxy.

If there is no proxy server, ignore these procedures.

To change proxy settings for Firefox

1. Start your Firefox browser.
2. Click **Tools > Options**.
3. Click the **Network** tab.
4. Click **Settings**.
5. Select **Manual proxy configuration** if it is not already selected.
6. In the **No proxy for** text box, type a comma delimiter after any existing entries, followed by the appliance IP address.
7. Click **OK** in each dialog box until you have exited.

To change proxy settings for Internet Explorer

1. Start your Internet Explorer browser.
2. Click **Tools > Internet Options**.
3. Click the **Connections** tab.
4. Click **LAN Settings**.
5. Click **Advanced**.
6. In the text box labeled **Do not use proxy server for addresses beginning with**, type a semicolon delimiter after any existing entries, followed by the appliance IP address.
7. Click **OK** in each dialog box until you have exited.

2.2.5 Access the TAM Data Collector User Interface

All project setup, data review, analysis, and reporting is performed using the TAM Data Collector user interface. The first time you display the user interface you might be asked to agree to the EULA.

To display the TAM Data Collector user interface using the TAM Data Collector application

1. Start your browser.
2. Enter the URL as `http://localhost:8443/web/index.html`.

If you cannot access the user interface, check the browser proxy settings and verify that there is no port conflict with another application. Verify that both the App Server and Database Server start. If you have

any trouble accessing the user interface, examine the files in the `logs` folder within the installation folder to see if there are any port conflicts with another application.

To display the TAM Data Collector user interface using the TAM Data Collector virtual appliance

1. Start your browser.
2. Enter the URL as `http://<virtual appliance IP address>`.

2.2.5.1. Port Settings

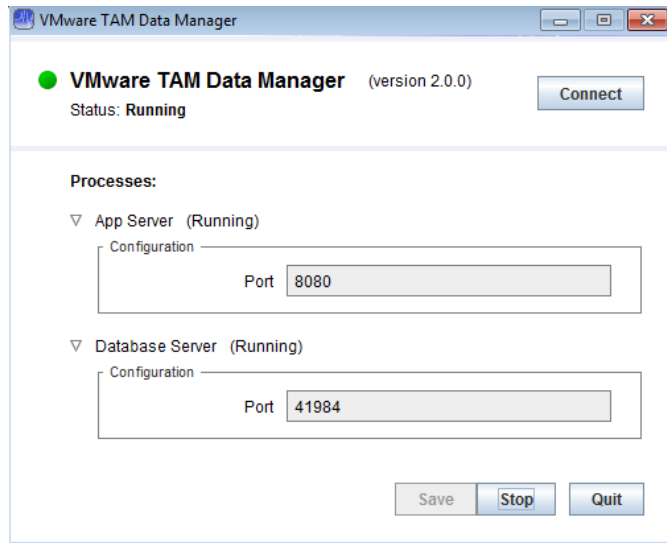
The TAM Data Collector virtual appliance and application use ports 80 and 8080. It is not necessary to specify the port number with the URL. Port conflicts are unlikely because all processes that run are known in advance, but if you do not want to use default ports 80 or 8080, change the port numbers using the one of the procedures given in the following sections.

For the user interface, it is also not necessary to specify the port number with the URL. Port conflicts are unlikely because all processes that run are known in advance. Follow this procedure if you need to change the port used by the TAM Data Collector application.

To change the ports used by the TAM Data Collector application

1. Start the TAM Data Collector application.

2. Click the disclosure triangle to the left of **App Server** or **Database Server** to reveal the port number.



3. Click **Stop**.
4. Enter the desired port values.
5. Click **Save**.
6. Click **Start**.

To change the port used by the TAM Data Collector virtual appliance

1. Log in to the virtual appliance.
2. From the virtual appliance command line interface, run the following command as root using your own password.

```
sudo -s
```

3. Edit `/usr/share/vha/tomcat/conf/Server.xml` and change

```
Connector port="8080"
```

to

```
Connector port="x"
```

where x is the new port number.

4. Save and close the file.
5. Reboot the virtual appliance.

2.2.6 Shutting Down TAM Data Collector

When you are finished working with TAM Data Collector, close the browser and perform a graceful shutdown. The procedure for shutting down depends on whether you are using the TAM Data Collector application or the virtual appliance.

2.2.6.1. Shutting Down the TAM Data Collector Application

To shut down TAM Data Collector, click **Stop** and click **Quit**.

2.2.6.2. Shutting Down the TAM Data Collector Virtual Appliance

To shut down the TAM Data Collector virtual appliance from the Web console

1. Open the TAM Data Collector virtual appliance Web console.
2. Click the **System** tab (the default).
3. Click **Information** (the default).
4. Click **Shutdown**.

To shut down the TAM Data Collector virtual appliance from the command line

1. Log in to the virtual appliance.
2. From the virtual appliance command-line interface, if you are not already running as the root user, run the following command as root using your own password:

```
sudo -s
```

3. Type `shutdown -h now` and press **Enter**.

2.2.7 Uninstalling TAM Data Collector

To uninstall TAM Data Collector, remove the installation folder and all associated files.

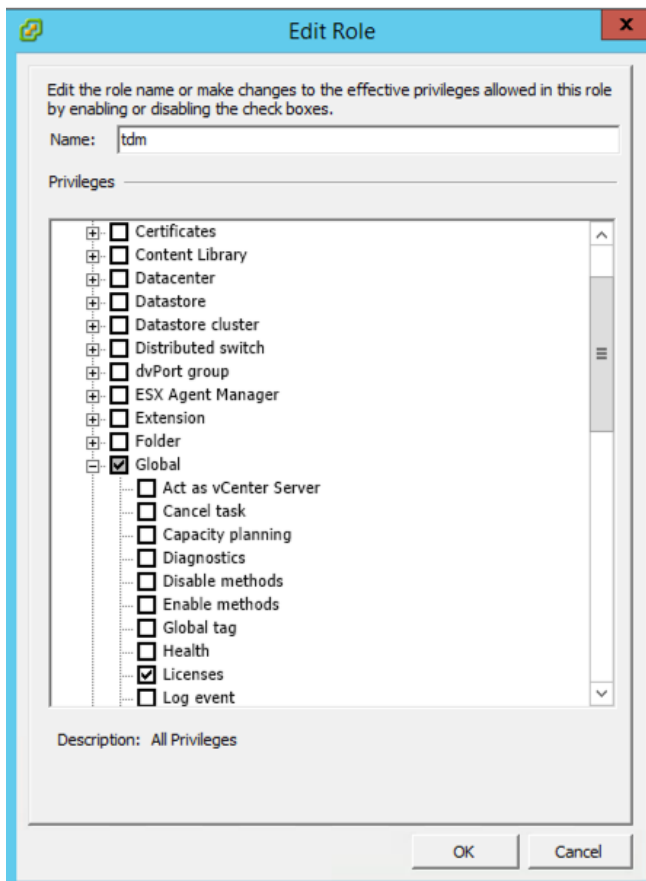
3. Working with TAM Data Collector

3.1 Setting Up Access to vCenter Server

You can use an administrator account to access the target systems and collect data, but it is a best practice to restrict use of the administrator account. The preferred approach is to set up user accounts on the target vCenter Server and View Connection Server with limited permissions sufficient to collect data.

Set up an account on vCenter Server

1. Set up an account with Read Only privileges for all objects.
2. To collect license data, add **Global > Licenses** privileges.

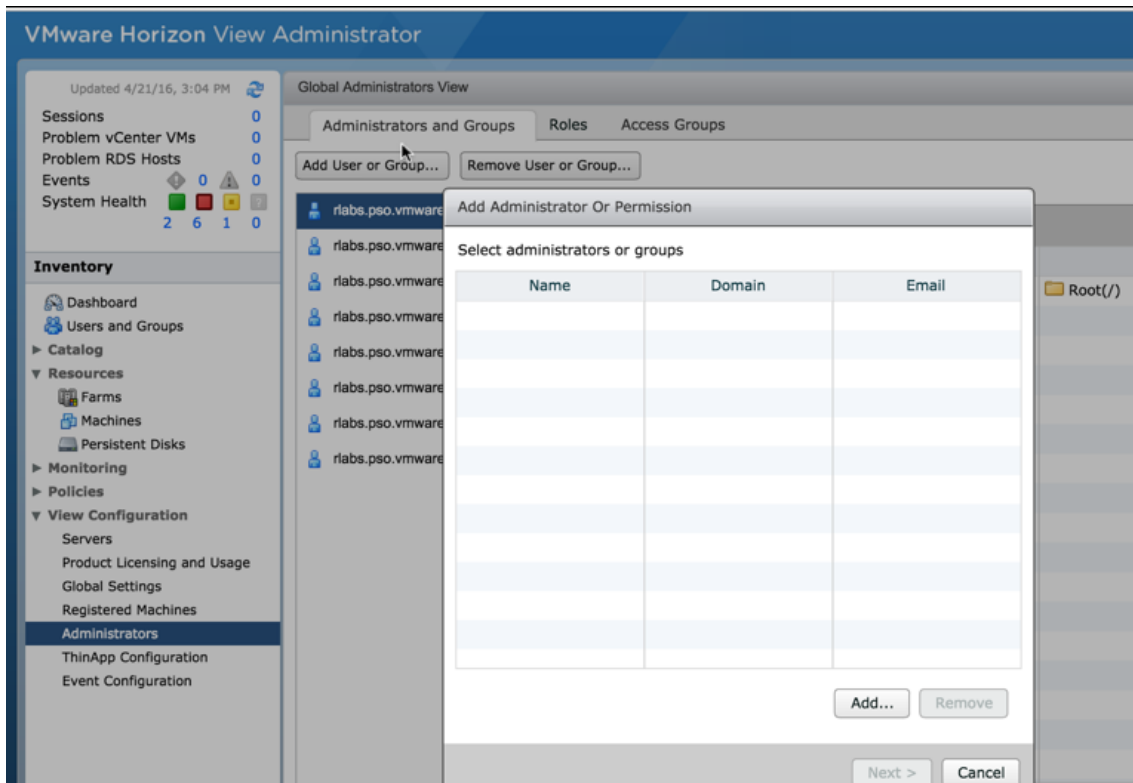


3.2 Setting Up Access to View Connection Server

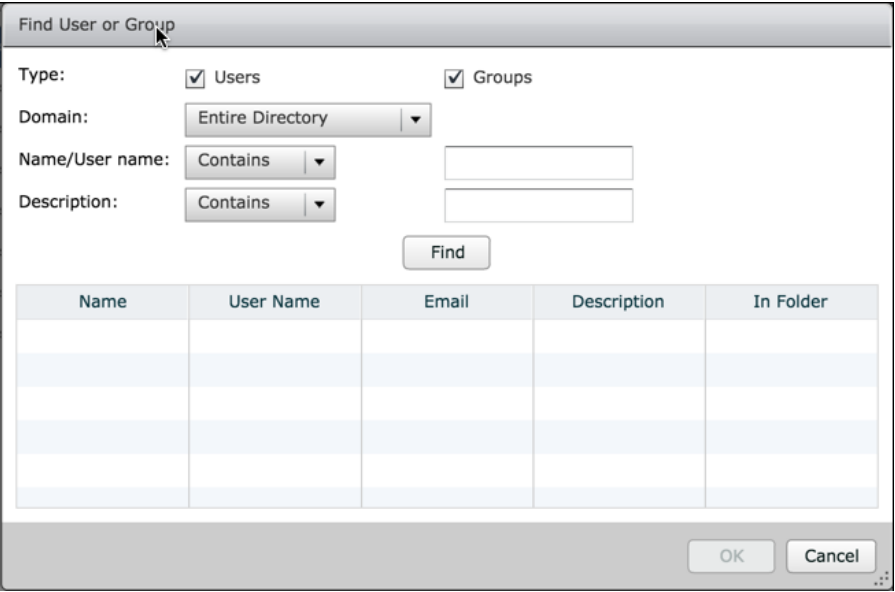
For the View Connection Server, the read only Administrator role permission is required. Create a new user account and add a role with appropriate permissions, or assign the role to an existing user account.

To set up an account on the target View Connection Server

1. Log in to the View Connection Server administration user interface.
2. Go to **View Configuration > Administrators > Add User or Group** to start the wizard.
3. Click **Add**.



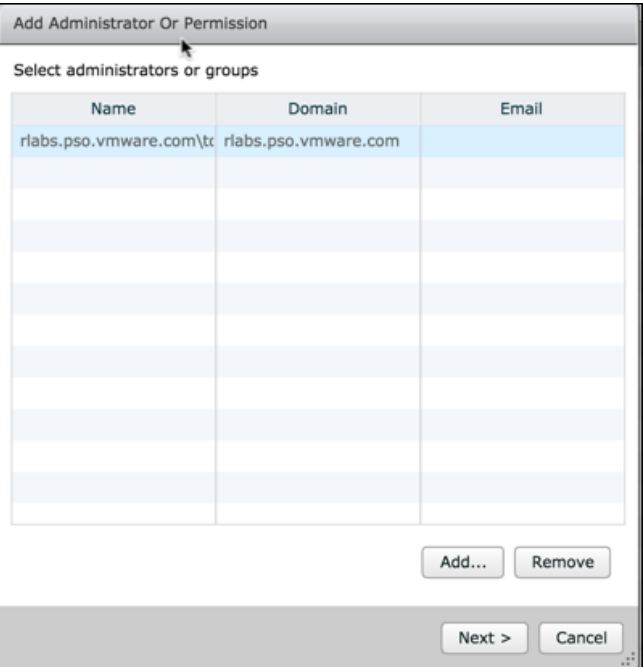
4. In the **Find User or Group** dialog box, select a user to change and click **OK**.



The 'Find User or Group' dialog box is shown. It has a title bar 'Find User or Group'. Below the title bar, there are two checked checkboxes: 'Users' and 'Groups'. Below these, there is a 'Domain:' label followed by a dropdown menu showing 'Entire Directory'. Below that, there are two labels: 'Name/User name:' and 'Description:'. Each label is followed by a 'Contains' dropdown menu and an empty text input field. Below these input fields is a 'Find' button. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. Below the 'Find' button is a table with five columns: 'Name', 'User Name', 'Email', 'Description', and 'In Folder'. The table is currently empty.

Name	User Name	Email	Description	In Folder
------	-----------	-------	-------------	-----------

5. In the **Add Administrator Or Permission** dialog box, select the administrator and click **Next**.



The 'Add Administrator Or Permission' dialog box is shown. It has a title bar 'Add Administrator Or Permission'. Below the title bar, there is a label 'Select administrators or groups'. Below this label is a table with three columns: 'Name', 'Domain', and 'Email'. The first row of the table is highlighted in blue and contains the text 'rlabs.pso.vmware.com\tr' in the 'Name' column and 'rlabs.pso.vmware.com' in the 'Domain' column. Below the table are 'Add...' and 'Remove' buttons. At the bottom of the dialog, there are 'Next >' and 'Cancel' buttons.

Name	Domain	Email
rlabs.pso.vmware.com\tr	rlabs.pso.vmware.com	

6. Make sure that the **Administrators (Read only)** role is marked **Yes** and click **Next**.

The dialog box titled "Add Administrator Or Permission" shows a table for selecting a role. The "Administrators (Read only)" role is selected and has "Yes" in the "Applies to an access group" column.

Role	Applies to an access group
Administrators	Yes
Administrators (Read only)	Yes
Agent Registration Administrators	
Global Configuration and Policy Adminis	
Global Configuration and Policy Adminis	
Inventory Administrators	Yes
Inventory Administrators (Read only)	Yes

Buttons at the bottom: < Back, Next >, Cancel.

7. Select **Root** and click **Finish**.

The dialog box titled "Add Administrator Or Permission" shows a table for selecting access groups. The "Root(/)" group is selected with a checkmark.

Access Group
<input checked="" type="checkbox"/> Root(/)

Buttons at the bottom: < Back, Finish, Cancel.

8. The selected user is shown with the **Administrators (Read only)** role.

The "Global Administrators View" window shows the "Administrators and Groups" tab. The user "riabs.pso.vmware.com/tdm" is listed. The "Roles" tab shows the "Administrators (Read only)" role assigned to the "Root(/)" access group.

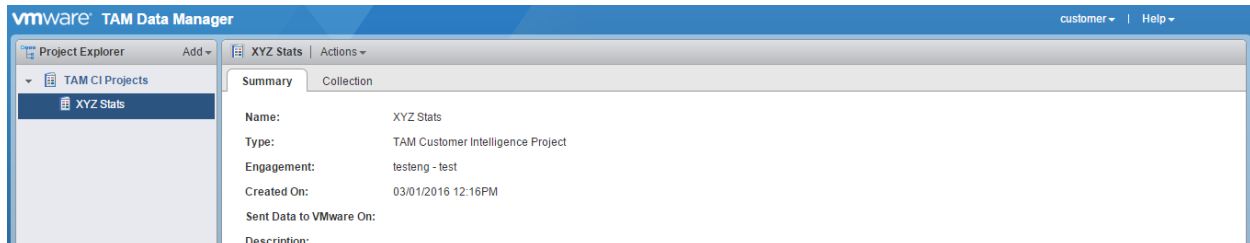
Role	Access Group
Administrators (Read only)	Root(/)

3.3 Using the Project Explorer

Use the Project Explorer to create and manage projects.

The Project Explorer opens when you start TAM Data Collector. Initially, the list of projects is empty. In the following figure, an existing project (XYZ Stats) is selected, and associated information is displayed in the right pane.

Figure 1. Project Explorer

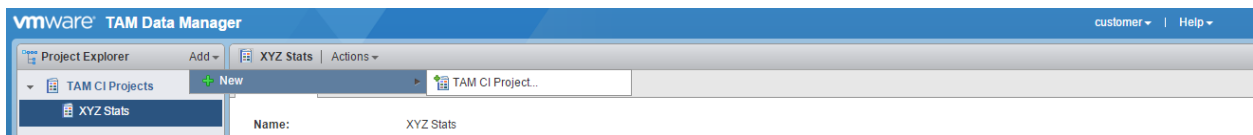


3.3.1 Creating a New Project

Customer data is organized into projects. You set up projects to collect usage data to be provided to VMware TAMs in person or by email..

To create a new project

1. Select **Add > New > TAM CI Project**.



2. Specify these general settings for the project and click **Next**.
 - **Name** – Give the project a name.
 - **Description** – Enter a description of the project.

- **Select the data sources to collect data from** – vCenter and View are the currently supported options.
 - Select the check boxes for **vCenter** and/or **Horizon View** if this project will include data collection. If you choose to include data collection, an **Anonymize data** check box will appear. Selecting this check box will anonymize the following during data collection:
 - Cluster names
 - Datastore names
 - Descriptions
 - IP addresses
 - License keys
 - Network names
 - Virtual machine names
 - VMware ESX® names

Note If you do not select **vCenter** or **Horizon View** check box, an empty project with no data collection will be created. Data exported from such a project cannot be used by the TAM team.

New TAM CI Project

1 Select Name
2 Ready to complete

Select Name

Name: XYZ Stats

Description:

Select the data sources to collect data from:

☐ vCenter

☐ Horizon View

Back Next Finish Cancel

3. If you selected the **vCenter** check box in the previous step, do the following and click **Next**.
 - a. Select the vCenter instances from which to collect data. The **Choose vCenters** page presents the following options for adding and removing vCenter instances:
 - Click **Add** and enter values for the server on the **Choose vCenters** page. Specify a name to identify the server, the vCenter IP address, the IP address of the SSO server used for server authentication, and user name and password.

New TAM CI Project

1 Select Name
2 **Choose vCenters**
3 Choose Horizon View Servers
4 Customer Agreement
5 Ready to complete

Choose vCenters
Choose existing vCenters to collect data from:

+ Add | - Delete | Choose From | Import | Apply Credentials | Validate All

Name	vCenter	User	Password	Status
10.129.132.40	10.129.132.40	rlabs\tdm	*****	
10.129.132.29	10.129.132.29	rlabs\tdm	*****	

2 items

Back Next Finish Cancel

- Click **Choose From** and select the servers to add.

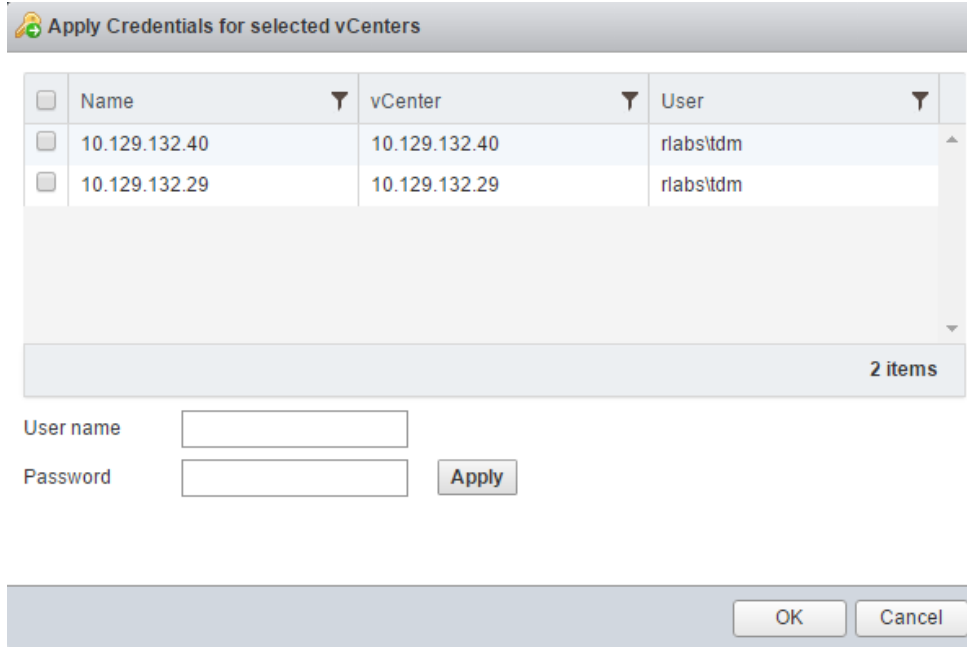
Choose From Existing vCenters

<input type="checkbox"/>	Name	vCenter	User
<input checked="" type="checkbox"/>	10.129.132.29	10.129.132.29	rlabs\wba

1 items

OK Cancel

- Click **Import** to import vCenter information from a file containing comma-separated values in the format <type>,<name>,<IP address>,<user>. For examples of the format, see Appendix A: Examples of vCenter CSV Data.
- Regardless of the method used to add servers, you can click **Apply Credentials** to provide a user name and password to multiple instances of vCenter at once.



<input type="checkbox"/>	Name	vCenter	User
<input type="checkbox"/>	10.129.132.40	10.129.132.40	rlabs\tdm
<input type="checkbox"/>	10.129.132.29	10.129.132.29	rlabs\tdm

User name

Password

- The **Validate All** option attempts a test connection to the vCenter instances using the supplied credentials.
- To remove a server, select it and click **Delete**.

- b. Upon clicking **Next**, TAM Data Collector attempts to connect to the servers, and the result is displayed in the **Status** column. If you see any errors, check to see whether the vCenter Server is available, and update or remove any entries as needed. To complete the setup, you need to be able to connect to all of the entered vCenter Server instances.

New TAM CI Project

✓ 1 Select Name
✓ 2 Choose vCenters
3 Choose Horizon View Servers
4 Customer Agreement
5 Ready to complete

Connection failed to some of the vCenters. Please enter valid details.

Choose existing vCenters to collect data from:

+ Add | ✖ Delete | 📁 Choose From | 📄 Import | 🛡️ Apply Credentials | 🔍 Validate All

Name	vCenter	User	Password	Status
10.129.132.40	10.129.132.40	rlabs\tdm	*****	✓
10.129.132.29	10.129.132.29	rlabs\tdm		Error

2 items

Back Next Finish Cancel

4. If you selected the **Horizon View** check box in step 2, do the following and click **Next**.
- a. Select the View servers from which to collect data. The **Choose Horizon View Servers** page presents the following options for adding and removing View servers:
- Click **Add** and enter values for the server on the **Choose Horizon View Servers** page. Specify a name to identify the server, the View IP address, and user name and password

New TAM CI Project

✓ 1 Select Name
✓ 2 Choose vCenters
3 Choose Horizon View Servers
4 Customer Agreement
5 Ready to complete

Choose Horizon View Servers

Choose existing Horizon View Servers to collect data from:

+ Add | ✖ Delete | 🔍 Validate All

Name	View Server	User	Password	Status
------	-------------	------	----------	--------

1 items

Back Next Finish Cancel

- The **Validate All** option attempts a test connection to the View servers using the supplied credentials.
 - To remove a server, select it and click **Delete**.
- b. Upon clicking **Next**, TAM Data Manager attempts to connect to the servers, and the result is displayed in the **Status** column. If you see any errors, check to see whether the View server is available, and update or remove any entries as needed. To complete the setup, you need to be able to connect to all of the entered View server instances.

New TAM CI Project

✓ 1 Select Name
✓ 2 Choose vCenters
✓ 3 Choose Horizon View Servers
4 Customer Agreement
5 Ready to complete

Connection failed to some of the Horizon View Servers. Please enter valid details.

Choose existing Horizon View Servers to collect data from:

+ Add | ✗ Delete | Validate All

Name	View Server	User	Password	Status
10.129.132.199	10.129.132.199	rlabs/tdm	*****	✓
10.129.132.98	10.129.132.98	rlabs/tdm	*****	Error

2 items

Back Next Finish Cancel

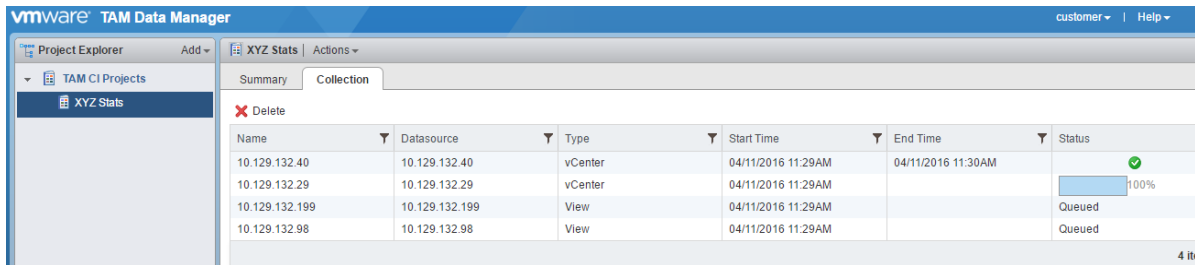
5. On the **Customer Agreement** page, the customer must read and choose whether to accept or decline the customer agreement and click **Next**.
 - If the agreement is declined, customers can still receive reports, but no data can be uploaded to VMware by the TAM using the project file created from this collection.

The screenshot shows the 'New TAM CI Project' window with the 'Customer Agreement' tab selected. On the left, a progress bar shows five steps: 1 Select Name, 2 Choose vCenters, 3 Choose Horizon View Servers, 4 Customer Agreement (highlighted), and 5 Ready to complete. The main content area displays the 'Customer Agreement' text, which explains that VMware TAM Data Manager Software collects data from VMware products for the purpose of providing high-quality customer-specific reports and industry standard benchmark reports (the 'VTCIP reports'). It also states that the collected data consists of technical information about VMware products and services deployed in the customer's environment, as well as the organization's VMware license key(s) and TAM engagement identifier(s). The agreement is for the VMware TAM Customer Intelligence Program ('VTCIP'). Below the text, there are radio buttons for 'Accept' and 'Decline'. At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

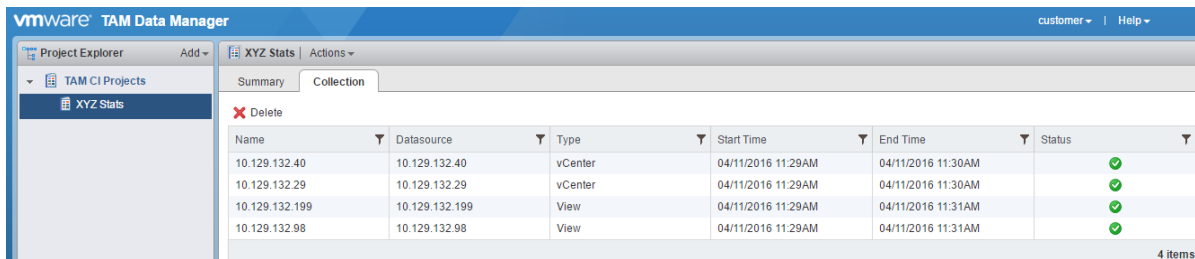
6. On the **Ready to Complete** page, review the settings and click **Finish** to add the project and begin data collection.

The screenshot shows the 'New TAM CI Project' window with the 'Ready to complete' tab selected. On the left, the progress bar shows the same five steps as before, with '5 Ready to complete' highlighted. The main content area displays the 'Ready to complete' settings. It includes fields for 'Name' (XYZ Stats), 'Engagement' (- Test), 'Description', 'Collection types' (vCenter, Horizon View), and 'Customer Agreement' (Accepted at 04/07/2016 12:51PM). Below these fields, a message states: 'This window will close and data collection will start in background. Data collection may take several minutes to complete.' At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

The project opens to the **Collection** tab, and collection proceeds automatically. The **Status** column displays the status as collection proceeds.



When collection is complete, a check box is displayed in the **Status** column.



The **Delete** button can be used to delete a vCenter or View instance from the project. This is useful if one of the data collections to a vCenter fails.

3.3.2 Exporting Project Data

Project data must be exported so that it can be sent to the TAM team. Project data can be provided to the TAM team by email or in person. TAM Data Collector does not automatically collect or send any data to VMware.

To export project data

1. Click the project in the Project Explorer and select **Actions > Export Project**.
2. Project data will be saved to the computer. Exported project is encrypted and can only be decrypted by an instance of TAM Data Manager. Exported project files are encrypted using the PBESWithHmacSHA256AndAES_128 algorithm, with an iteration count of 20.

3.3.3 Downloading Logs

A ZIP file containing logs of TAM Data Collector activity can be downloaded by clicking **Help** and selecting **Download Logs** from the TAM Data Collector UI.

If the TDM Web interface is not accessible, one can also download the logs from the TDM folder as follows:

- Java application:

```
<TDM instance folder>/logs
```
- OVF:

```
/usr/share/vha/tomcat/logs
```

```
/usr/share/vha/basex/data/.logs
```

Appendix A: Examples of vCenter CSV Data

This section provides several examples of the comma-separated value format that can be used when adding vCenter instances to a project.

The vCenter data is in the format `<type>,<name>,<IP address>,<user>`. Examples of data using this format are as follows:

```
VC,Dev vCenter 40,10.129.132.40,rlabs\user1
VC,Prod vCenter 29,prod1-vc.vmware.com,rlabs\user1
VC,Staging vCenter 29,stgl-vc,read-only-tdm-user
```