RIAT

Probe Deployment Guide

RIAT version : 8.2
Document updated : 11/10/2014

Table of Contents

1 Introduction 5
1.1 RIAT Components 5
1.1.1 RIAT Probe 5
1.1.2 RIAT Server 6
1.2 RIAT Probe deployment scenario 6
2 Prerequisites 7
3 RIAT Probe deployment 8
3.1 Deploying RIAT Probe appliance 9
3.1.1 Deploying RIAT Probe appliance using VMware vSphere Client 9
3.2 Configuring RIAT Probe appliance 10
3.2.1 Determining IP address of RIAT Probe 10
3.2.2 Connecting to RIAT Probe 10
3.2.3 Registering license for RIAT Probe 10
3.2.4 Creating an administrator account 10
3.2.5 Log into RIAT Probe appliance 11
3.2.6 Specifying customer details for RIAT Probe appliance 11
3.2.7 Setting time zone for RIAT Probe 11
3.2.8 Configuring FTP settings 11
3.2.9 Defining data collection duration for RIAT Probe 11
3.3 Adding Probes in RIAT Probe appliance 11
3.3.1 Adding VMware probe 12
3.3.2 Adding SMI-S probe 12
3.3.3 Adding NetApp probe 14
3.3.4 Adding XenServer probe 14
3.3.5 Adding AMS probe 15
3.3.6 Adding SQLServer Probe 16
3.3.7 Adding SVP probe 17
3.3.8 Adding HNAS Probe 21
3.3.9 Adding SAP HANA probe 21
3.3.10 Adding Linux probe 22

3.3.11 Adding IBM XIV Probe 23
3.3.12 Adding Network probe 23
3.3.13 Adding Unix probe 26
3.3.14 Adding UCP probe 27
3.3.15 Adding VMAX probe 28
3.4 Starting and stopping added probes 29
4 MARS Windows Probe for Windows and Hyper-V machines 30
4.1 MARS Windows Probe software deployment methods 30
4.1.1 Pre-requisites 31
4.1.2 Deploying MARS Windows Probe software 34
4.1.3 Configuring MARS Windows Probe software 34
4.1.4 Configuring FTP settings for cloud deployment model 38
4.1.5 Working with the SCOM Rules tab 39
5 Advanced Operations 41
5.1 Assigning a static IP address to RIAT Probe 41
5.1.1 Assigning static IP address to RIAT Probe in vSphere 41
5.1.2 Assigning static IP address to RIAT Probe in VMware Player 42
5.2 MARS Windows Probe 42
5.2.1 Importing Management Pack in SCOM 42
5.2.2 Viewing log files for MARS Windows Probe 42
5.3 Creating User in SQL Server 42
5.4 Manually uploading data on FTP target 44
5.5 Upgrading RIAT Probe without losing data 45
5.6 Reconfiguring RIAT Probe appliance 46
5.7 Identifying Microcode Version (for SVP Probe) 47
5.8 Adding Command Device in VMware Player (Only for USP V storage system) 47
5.9 Creating user for NetApp 7-mode 48
5.10 Creating user for NetApp C-mode 50
5.11 Managing VMAX probe 51
5.11.1 Adding VMAX probe for already added EMC Unisphere for VMAX 51
5.11.2 Edit details of EMC Unisphere for VMAX 52
5.12 CSV file format (for Network probe) 52
Appendix A: RIAT Probe deployment using Hyper-V Manager 53

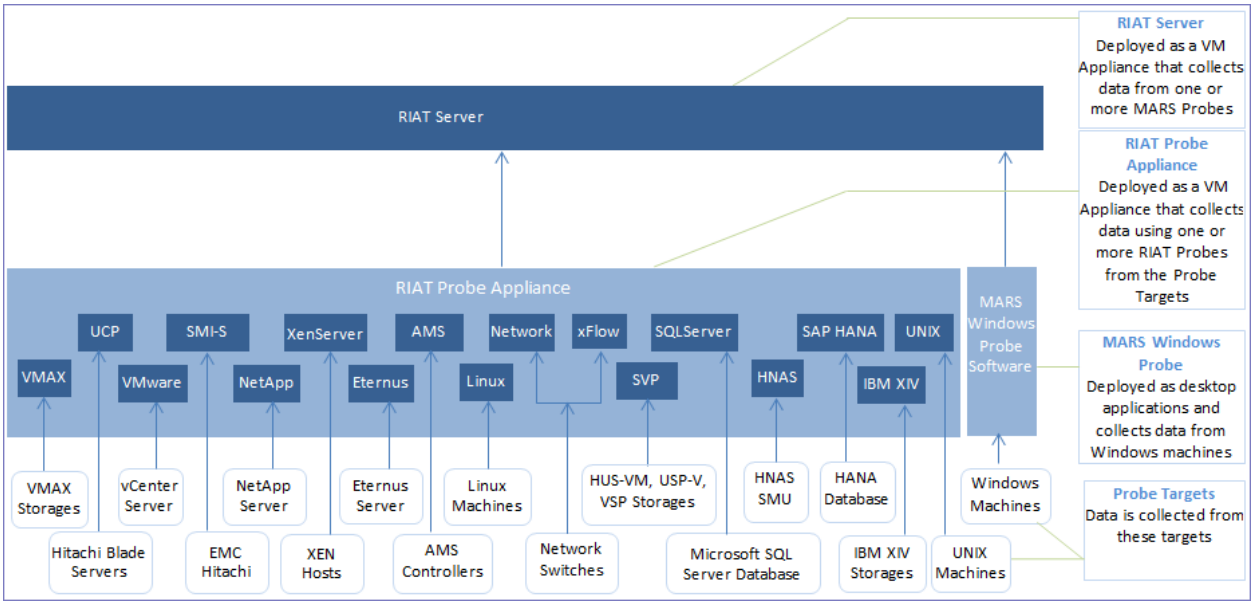
Appendix B: RIAT Probe deployment using Citrix XenCenter 53
RIAT Probe OVA package deployment 53
RIAT Probe XVA package deployment 55
Appendix C: RIAT Probe deployment using VMware Player 56

1 Introduction

RIAT is a Virtual Infrastructure Optimization (VIO) solution. It provides an assessment to measure, analyze, report, and solve optimization issues in data centers that have virtual infrastructures, storage systems, physical/virtual hosts running the Linux, Unix, and Windows operating systems, as well as network devices (switches). As virtual environments and the data associated with them continue to grow, this assessment allows organizations to understand what configuration changes are needed to enable the environment to run efficiently.

1.1 RIAT Components

RIAT consists of two components—RIAT Server and RIAT Probe



1.1.1 RIAT Probe

RIAT Probe collects performance and configuration data from different types of targets and sends it to RIAT Server. The target machines could be:

- Physical/virtual servers running Linux, Unix or Windows OS
- Virtualized infrastructures with VMware, Hyper-V , XenServer
- Storage systems, such as Hitachi, EMC, AMS, Eternus, etc.
- Network Devices - Switches

The performance metrics include — CPU utilization, swap rates, memory usage, response times, kernel and device read/write latency, packets received/transmitted/dropped, IOPS, throughput, storage capacity and utilization, read/write ratio, vMotion activity, KB /IO, etc.

RIAT Probe collects the performance data on a periodic, granular basis. This allows RIAT Server to analyze the data received over a period and identify trends, bottlenecks, etc. The data can be collected as frequently as 1 minute (even more frequently in some cases).

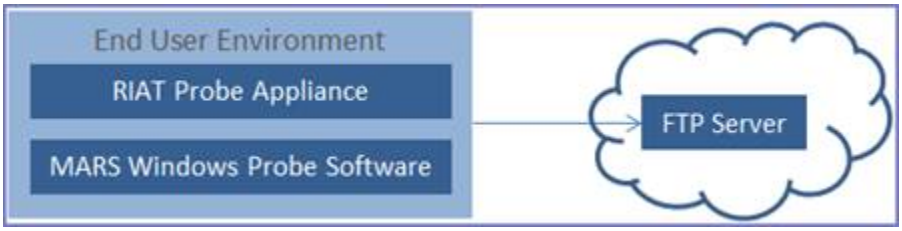
The configuration metrics include — the storage vendor, model, type and method of connectivity, availability method, number of CPUs, storage capacity, etc.

1.1.2 RIAT Server

RIAT Server consolidates the data reported by one or more RIAT Probes, analyzes the aggregated data in conjunction with industry best practices, and generates the reports.

1.2 RIAT Probe deployment scenario

RIAT Probe is deployed at the customer site and data is transferred to FTP Server (RIAT Server).



2 Prerequisites

RIAT Probe has the following prerequisites:

- vSphere client on ESX Server 3.5 or higher.
  Alternatively: VMware Player runing on Windows & Linux 64-bit/Citrix XENCenter client 5.5 and above/Hyper-V 2008 R2 and above
- RAM: Minimum 2 GB, Recommended 4 GB
- Storage: 50 GB minimum virtual disk space
- For platform support, refer **Support Platform** documentation

Note: RIAT supports IPv4 and does not support IPv6.

3 RIAT Probe deployment

RIAT Probe collects performance and configuration data from different types of targets:

- **Virtual infrastructure**: Data centers running these virtualization software
  - VMware
  - XenServer
- **Storage**
  - **NetApp**: Using NetApp ONTAP APIs
  - **AMS**: By connecting to AMS storage controllers
  - **SMI-S storage devices**: Other storage systems, such as EMC, Hitachi, etc. that comply with the open Storage Management Initiative Specification (SMI-S) standard
  - **SVP**: By connecting to VSP/HUS VM, USP V, and VSP G1000 storage systems separately.
  - **IBM XIV**: By connecting to IBM XIV storage systems
  - **VMAX**: By connecting to **Unisphere for VMAX** and **EMC Solutions Enabler Symmetrix CLI.**
- **Network switches and NetFlow/sFlow enabled network devices**
  - **Network**: By connecting to newtork switches
  - **xFlow**: By connecting to NetFlow/sFlow enabled network devices

  A user is provided separately for Network and xFlow probes.
- **Database:**
  - **SQLServer**: By connecting to Microsoft SQL Server database
- **Data centers with physical/virtual hosts running the Windows OS**
- **Data centers with physical/virtual hosts running the Linux OS**
- **Data centers with physical/virtual hosts running the Unix OS**

RIAT Probes for **Virtual infrastructure**, **Storage devices**, **Network switches and NetFlow/sFlow enabled network devices, Database**, and **Data centers with physical/virtual hosts running the Linux and Unix OS** are bundled as a virtual appliance called "**RIAT Probe Appliance**" that can itself run as a virtual machine in a virtual environment.

RIAT Probes for **data centers with Windows OS in Physical/Virtual/Hyper-V environment** is deployed differently. Refer to MARS Windows Probe for Windows and Hyper-V machines section.

3.1 Deploying RIAT Probe appliance

RIAT Probe virtual appliance is distributed as an OVA package. OVA is a single-file format of an OVF package that allows for an easy distribution. An OVF (Open Virtualization Format) is an open standard for packaging and distributing virtual appliance.

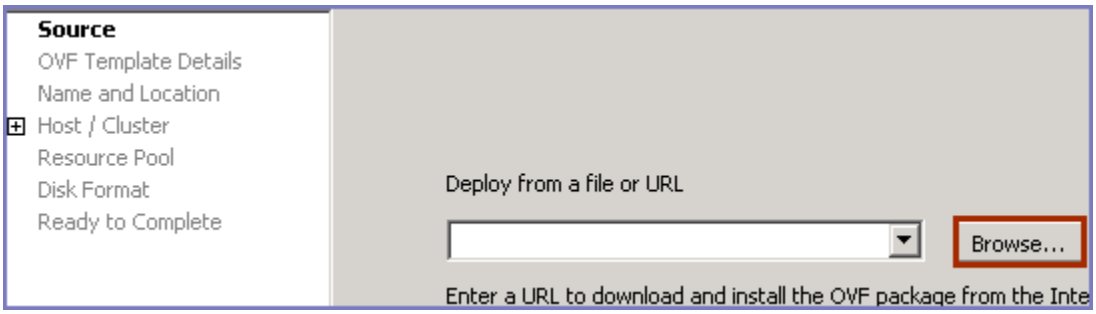
OVA file can be deployed using any virtual infrastructure management tool, such as VMware vSphere, Citrix XenCenter or VMware Player, or Hyper-V Manager.

Method to deploy RIAT Probe appliance using VMware vSphere Client is described in the following section.

Note: To deploy RIAT Probe using Citrix XenCenter or VMware Player or Hyper-V Manager see Appendix A, Appendix B and Appendix C sections.

3.1.1 Deploying RIAT Probe appliance using VMware vSphere Client

1. Open the vSphere Client application.
2. From the File menu, select **Deploy OVF Template**.
3. Click **Browse** and select RIAT Probe OVA file.



4. Click **Next**. In the OVF Template Details section, OVA file details are displayed.
5. Click **Next.** In the **Name and Location** section, enter the following details:
   - **Name:** RIAT Probe will be identified by this name in the vCenter.
   - **Inventory location**: RIAT Probe will be added under the selected inventory in the vSphere application.
6. Click **Next**. In the Host/Cluster section, select the appropriate cluster from the list of available clusters inside the inventory.
7. Click **Next**. The system displays the list of resource pools that are available in the cluster in the Resource Pool section. Either you can deploy RIAT Probe in resource pool or in cluster. Select an appropriate location based on your requirements.
8. Click **Next**. In the Datastore section, select the datastore for RIAT Probe. The system will save all the reports and log data in the selected datastore.
9. Click **Next**. In the Disk Format section, define the appropriate disk format:
   - **Thin Provisioned format**: System initially allocates 2.8 GB and it keeps allocating more space till maximum 8 GB.

- **Thick Provisioned format**: The system allocates entire virtual disk space (50 GB).

10. Click **Next**. The system displays the **Ready to complete** section for confirmation.
11. Click **Finish** to complete the deployment.
12. Power on RIAT Probe appliance.
13. Proceed to the Configuring RIAT Probe Appliance section.

3.2 Configuring RIAT Probe appliance

RIAT Probe configuration is a one-time operation that sets up RIAT Probe. The workflow guides the user through the following steps.

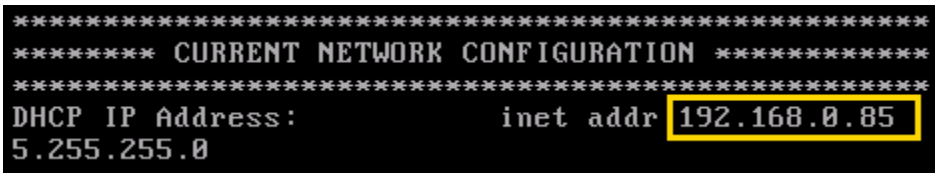
3.2.1 Determining IP address of RIAT Probe

Open RIAT Probe console. In the command prompt, enter the following login credentials:

Localhost login: `config`

Password: `megha!234`

IP address assigned to RIAT Probe is displayed next to the 'inet addr' field.



You can also assign the static IP address to RIAT Probe. For more information, see Assigning a static IP address to RIAT Probe.

3.2.2 Connecting to RIAT Probe

Open a browser and access RIAT Probe at the URL https://< RIAT Probe IP Address>:8443 where *RIAT Probe IP* is the IP address of RIAT Probe.

Read and accept the License Agreement. The Create New User window appears.

3.2.3 Registering license for RIAT Probe

1. On the Upload License window, click **Browse**.
2. Browse to the license file and click **Submit** to register the license. The Create Administrator account window appears.

3.2.4 Creating an administrator account

A user account with administrator privileges must be created to manage RIAT Probe.

1. On the Create Administrator account window, specify the following details:
   - **User ID and its password**

- **First name, last name, and email of the user**
- **Locale**: RIAT Probe is available in two languages – US English and Japanese.
- **Group**: Select **Admin** to create administrator account.

Note: Only one user can be created for a RIAT Probe appliance.

2. Click **Submit** to create the login account.

3.2.5 Log into RIAT Probe appliance

Enter defined user ID and password to log into RIAT Probe appliance.

3.2.6 Specifying customer details for RIAT Probe appliance

In the Basic Information window, specify the basic information of customer.

1. Enter the following details:
   - **Customer Name:** Name of the customer
   - **Administrator Contact Name** and the **Administrator Contact Email**: Administrator's name and email address
   - **Technical Contact Name** and **Technical Contact Email:** Resource (generally administrator) who needs to be notified in case of technical issues.
2. Click **Next**. The Select Timezone window appears.

3.2.7 Setting time zone for RIAT Probe

Select the time zone where RIAT Probe appliance is deployed and then click **Next**. The FTP Information window appears.

3.2.8 Configuring FTP settings

Refer to the document that is provided separately for FTP details.

After entering the FTP details, click **Next** to proceed to the next step.The Data Collection Duration window appears.

3.2.9 Defining data collection duration for RIAT Probe

Data collection duration is defined as per the imported license. It can be reduced.

Click **Next**. This completes the initial set up of RIAT Probe.

3.3 Adding Probes in RIAT Probe appliance

After initial setup of RIAT Probe appliance, you can add one or more types of RIAT Probes to collect data from different targets.

Types of available Probes are as follow:

- VMware
- SMI-S
- NetApp
- XenServer
- AMS
- SQLServer
- SVP
- HNAS
- SAP HANA
- Linux
- IBM XIV
- Network
- Unix
- UCP
- VMAX

For collecting data from Windows and Hyper-V targets, see MARS Windows Probe for Windows and Hyper-V machines.

3.3.1 Adding VMware probe

VMware Probe collects data of the Virtual Machines from the VMware vCenter Server and standalone ESX Server.

1. Click **Home** link and then click **Add Probe**.
2. Select **VMware** from the **Probes** list.
3. Enter the following values:
    - **vCenter Server**: Host name or IP address of the vCenter Server
    - **Username**: Any user having access to vCenter. Read-only privileges are also sufficient.
    - **Password**: Password of the vCenter user
4. Click **Next**. The system validates the entered details.
5. Click **Next** after successful validation.
6. Click **OK** and start the probe on the Status page to start collecting data.

3.3.2 Adding SMI-S probe

RIAT SMI-S Probe collects data from supported storage systems using Storage Management Initiative Specification (SMI-S).

1. Click **Home** link and then click **Add Probe**.
2. Select **SMI-S** from the **Probes** list.
3. Enter the following values:
   - **SMI-S Server**: Name or IP address of SMI-S Server
   - **URL**: URL of the SMI-S Server. Ensure to enter the correct namespace along with the IP address. Hence, the format of URL will be: http://<IP address of SMIS Server>/<Namespace>

     Note: If HTTPS protocol is used, you need to enter the port 5989 at the end of the IP address. For example, https://<IP address of SMIS Server>:5989/<Namespace>

     The following table describes model names and associated namespaces.

Manufacturer	Model	Namespace/s
EMC	Symmetrix , Clariion, VMAX,VNX	interop
		root/emc/ecom
		root/emc/vmware
		root/emc
Dell	Compellent	root/PG_Internal
		interop
		root/cimv2
		root
		root/compellent
IBM	DS6000/8000, SVC	interop
		root/ibm
HP	EVA, 3PAR	root/reflection
		Interop
		root/eva root/PG_InterOp

   - **Username**: Any user which has access to the SMIS-Provider. Read-only privileges are also sufficient.
   - **Password**: Password of the SMI-S User
4. Click **Next**. The system validates the entered details.

5. After successful validation of SMI-S Server details, click **Next**. The system displays the list of available SMI-S storage systems (arrays).
6. Choose the target SMI-S storage systems and click **Next**.
7. Click **OK** and start the probe on the Status page to start collecting data.

3.3.3 Adding NetApp probe

RIAT NetApp Probe allows you to collect configuration and performance data from NetApp storage systems using the ONTAP API.

Pre-requisites:

1. SSL must be enabled on the target NetApp storage system. NetApp probe uses Port 443 (Https connection) for connecting to NetApp Storage.
2. Ensure that you have a user (read-only privileges) available on NetApp storage system with appropriate role to collect configuration and performance data. RIAT Probe supports 7-mode and C-mode types of NetApp storage system. The procedure of creating user differs as per the target storage system type.

   To create user for 7-mode, see Creating user for NetApp 7-mode and to create user for C-mode, see Creating user for NetApp C-mode.

Add NetApp probe in RIAT Probe Appliance

1. Click **Home** link and then click **Add Probe**.
2. Select **NetApp** from the **Probes** list.
3. Enter the following values:
   - **NetApp Server**: IP address of NetApp server
   - **Username** and **Password**: Enter the username and password that you have created.
4. Click **Next**. The system validates the entered details.
5. Click **Next** after successful validation.
6. Click **Ok** and start the probe on Status page to start collecting data.

3.3.4 Adding XenServer probe

1. Click **Home** link and then click **Add Probe**.
2. Select XenServer from the **Probes** list.
3. Enter the follwing values:
   - **XenServer Probe Name**: A name given to XenServer Probe
   - **Master IP Address(es)**: IP address of one or more XenServer masters. Multiple XenServer masters should be separated by comma.

     Important:

- If you want to specify multiple XenServer masters, ensure that these masters are part of same group. You will need to define that group user name and its password in "**Group User Name & Group Password** fields.
- You cannot add individual slave nodes in XenServer probe.

- **Group Name:** Specify any desired group name.
- **Group User Name & Password**: Login username and password of the XenServer group.

  Note: The login credentials of the user with "read-only" privileges is sufficient to collect configuration and performance data for the XenServer environment.

  More details about the permissions available for the "read-only" role, refer to:

  http://docs.vmd.citrix.com/XenServer/6.0.0/1.0/en_gb/reference.html#RBAC-roles-def

- **Connection Protocol**: Connection protocol (HTTP or HTTPS) that will be used to collect data from XenServer hosts.
- **Communication Port**: Communication port as appropriate for the connection protocol. The default values are 80 (HTTP) and 443 (HTTPS).
- **KeyStore Password (https):** Default keystore password is **changeit**

  To establish secured SSL based communication, XenServer has its certificate. When the XenServer probe is started, RIAT Probe stores the certificate for any further communication in the trusted list and the trusted list has been assigned the default keystore password.

4. Click **Next**. The system validates the entered details.
5. Click **Next** after successful validation.
6. Click **Ok** and start the probe on the Status page to start collecting data.

3.3.5 Adding AMS probe

The AMS Probe collects data through the AMS storage controllers.

1. Click **Home** link and then click **Add Probe**.
2. Select AMS from the **Probes** list.
3. Enter the following values:

   - **AMS Storage Name**: Name of the AMS storage system. The name denotes the storage system for which this probe will be added. This need not be the same as storage name defined in your environment.

     Note: After you add the probe, it will be identified with this name in RIAT Probe appliance.

   - **Controller 0 IP address** and **Controller 1 IP address**: IP addresses of the Controller 0 and Controller 1.
   - **Username** and **Password**: User credential of a user who has "read only" permissions.

Note: If the user authentication for AMS storage is "Off", you need to enter a dummy Username and Password since these two fields are mandatory for adding AMS probe.

4. Click **Next.** The system validates the entered details.
5. Click **Next** after successful validation.
6. Click **Ok** and start the probe on the Status page to start collecting data.

3.3.6 Adding SQLServer Probe

SQLServer probe collects configuration and performance data from Microsoft SQL Server database.

Note: In the rest of the document, "SQL Server" refers to "Microsoft SQL Server".

Pre-requisites

- Ensure that SQL Server/Windows domain user with minimum 'View any database' and 'View server state' permissions is available. If you want to create a new user with these permissions, see Creating User in SQL Server.
- SQL Server Browser service must be running.
- SQL Server must be configured to accept TCP/IP requests.
- RIAT Probe appliance should have been deployed in your environment.

Adding SQLServer Probe in RIAT Probe Appliance

1. Click **Home** link and then click **Add Probe**.
2. Select **SQLServer** from the **Probes** list.
3. Enter the following details:
    - **Server Name**: **Host name** or **IP address** or **Host name\instance name** of the SQL Server
    - **Port Number**: Specify the port number. Default - 1433
    - **Authentication**: Specify the type of authentication needed to establish the connection between SQLServer probe and SQL Server instance.
        - **SQL Server**: If mixed authentication (Windows and SQL Server authentication) is enabled, select SQL Server.

          Note: You can create a user in SQL Server with minimum 'View any database' and 'View server state' permissions which will enable you to establish connection between SQLServer probe and SQL Server instance. For more information, see Creating User in SQL Server.
        - **Windows** - If Windows authentication mode is enabled for SQL Server database, select Windows.
    - **Username**: Enter username for the Windows or SQL Server authentication. In case of Windows authentication, domain is supported (DOMIN\username).
    - **Password:** Password of the entered user

4. Click **Next**. The system validates the entered details.
5. After successful validation, click **Next**.
6. Click **OK** and start the probe on the Status page to start collecting data.

3.3.7 Adding SVP probe

SVP probe collects configuration and performance data from HUS-VM, USP V, and VSP storage systems.

Pre-requisites

- **RAIDCOM**: RAIDCOM is used to collect the configuration and performance data. Hitachi provides the RAIDCOM in a CD named "Hitachi HUS VM/VSP/USP V/VM/USP/NSC/9900V/9900 Command Control Interface Software Distribution Library" under <Storage System Name >/<Microcode Version of target storage system >/program/RM/LINUX/x64/RMHORC.

  To find the target storage system's microcode version, see Identifying Microcode Version.

  For older Microcode versions, where 64-bit RMHORC file is not available, such as "R500-PP-50-09-98_14" and "R600-PP-60-08-24", then 32-bit RMHORC file is required. It is located under: <Storage System Name>/<Microcode Version>/program/RM/LINUX

- **Export Tool**: Export tool is used to collect the performance data. For each storage system, Hitachi provides the Export Tool in a CD named "<Storage System Name>Document and Programs DVD<Microcode Version>" under path Tools_Pack/ExportTool/UNIX/export.tar or under path Tools_Pack/ExportTool/HP-UX/export.tar.
  Microcode Version in the CD name should be similar with Microcode Version of target storage system. To find the target storage system's microcode version, see Identifying Microcode Version.
- Performance monitoring has to be enabled on target Control Units (CU) to collect performance data from LDEV, PG, LU, etc. To enable CUs, refer the documentation of target Hitachi storage system.
- A user with 'Read-Only' permission must be available on SVP to collect data from storage system.
  Note: Data cannot be collected with the user "Maintenance".

  Follow the steps to add an SVP Probe.
  Note: Follow step A only if you are adding SVP probe for USP V storage system.

  A. Adding command device (Only for USP V storage system)
  B. Uploading RAIDCOM
  C. Adding SVP probe in RIAT Probe appliance

A. Adding command device (Only for USP V storage system)

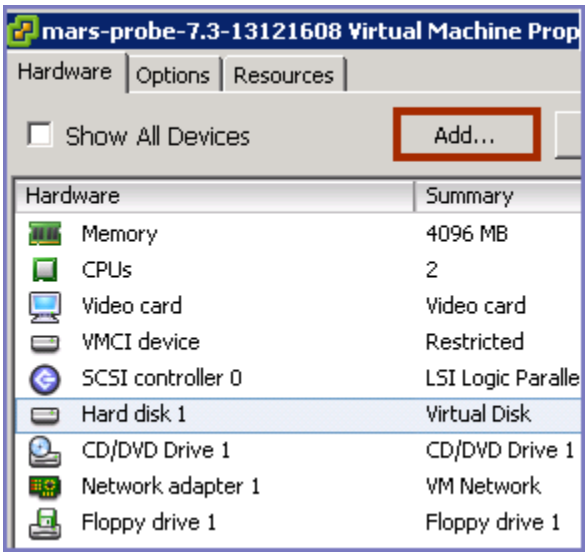
Command device enables SVP probe to collect configuration data from USP V storage system. The following procedures describe how to add command device in **VMware vSphere** client. If you want to add command device using VMware Player, Adding Command Device in VMware Player. To add command device using any other client, refer the documentation of respective client.

Pre-requisites:

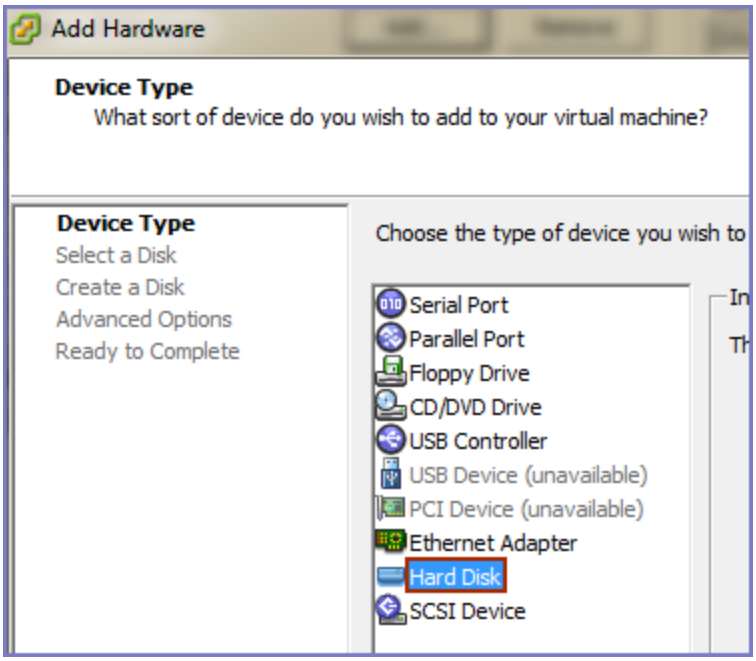
Before you add command device, ensure that target LUN is available for the desired USP V storage system to the ESX host on which RIAT Probe appliance is deployed. The LUN has to be enabled as command device and the following device attributes needs to be configured.

- **Command Device Security**: Disable the security of command device.
- **User Authentication**: Enable the user authentication.
- **Device Group Definition**: Enable the Device group definition.

1. Using vSphere Client, select the virtual machine on which RIAT probe appliance is deployed and click **Shut down the virtual machine**.
2. Click **Edit virtual machine settings**.
3. On the Virtual Machine properties window, click **Add**.



4. On the Add Hardware window, click **Hard Disk** and then click **Next**.

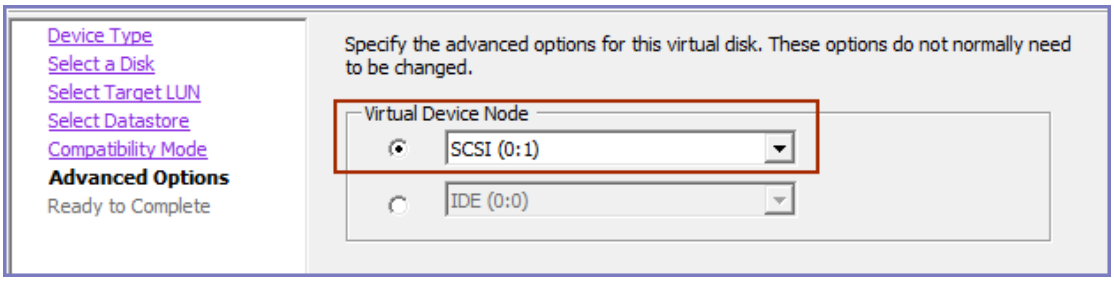


5. In the Select a Disk section, select the **Raw Device Mappings** button and then click **Next**.
6. In the Select Target LUN section, select the target LUN of USP V storage system for which command device should be added and then click **Next**.

   Note: If the target LUN is unavailable for the desired USP V storage system, map the target LUN to the ESX host on which RIAT Probe appliance is deployed. The mapped LUN has to be enabled as command device and the following device attributes needs to be configured.

   - **Command Device Security**: Disable the security of command device.
   - **User Authentication**: Enable the user authentication.
   - **Device Group Definition**:Enable the Device group definition.

   For more information, refer the USP V storage documentation.
7. In the Select Store section, select **Store with Virtual Machine** button and then click **Next**.
8. In the Compatibility Mode section, select **Physical** button and then click **Next**.
9. In the Advanced Options section, select the virtual device node as displayed in the following screen capture and then click **Next**.



10. Review the summary to ensure that the correct options have been chosen and then click **Finish**.

11. The system adds a new hard disk.
12. Click **OK**.
13. **Power-on** the virtual machine.
14. To ensure that command device is added for the USP V storage system, follow the steps as given below:
    a. Log on to RIAT Probe using console:

       Username: `root`

       Password: `app.jeos`

    b. Execute the `/usr/local/megha/lib/svp/list_devices` command to check if the command device is present for the desired USP V storage device.

    c. You can view the details as displayed in the following screen capture. The command device (OPEN-V-CM) has been added with storage device (serial number 53086).

```
login as: root
root@172.17.237.229's password:
Last login: Fri Aug 23 11:35:11 2013 from 10.1.136.14
[root@localhost ~]# /usr/local/megha/svp/list_devices

Device : /dev/sda       vendor id: VMware       product id:Virtual disk         Serial Number: 0
==========================================================================================
Device : /dev/sda1      vendor id: VMware       product id:Virtual disk         Serial Number: 0
==========================================================================================
Device : /dev/sda2      vendor id: VMware       product id:Virtual disk         Serial Number: 0
==========================================================================================
Device : /dev/sdb       vendor id: HITACHI      product id:OPEN-V-CM            Serial Number: 53086
==========================================================================================
[root@localhost ~]#
```

B. Uploading RAIDCOM

To add SVP probe for the first time, RAIDCOM needs to be uploaded. RAIDCOM is provided in a CD along with storage systems. On CD, RAIDCOM file is located at – `Linux/X64/RMHORC`.

1. In RIAT Probe appliance, click **Manage**.
2. On the Manage window, click the **Upload RAIDCOM** link.
3. On the Upload RAIDCOM window, click **Choose File** button in the Upload new version field.

   Note: Upload the latest version of RAIDCOM available with you.

4. Select the RAIDCOM file (.RMHORC file) and click **Submit**. Once RAIDCOM is uploaded, it need not be uploaded again. Later on, it can be upgraded if required.

C. Adding SVP probe in RIAT Probe appliance

1. In RIAT Probe appliance, click **Home** and then click **Add Probe** button.
2. On the Add Probe window, select SVP from the **Probes** list.
3. Provide the following details:
   - **Storage System type**: Select a storage system (VSP/HUS-VM/USP-V/VSP G1000).
   - **Serial Number:** Serial number of the storage system.

     Note: The Serial Number field is displayed only if USP V storage system is selected.

- **SVP IP address**: IP address of the SVP that is used to collect data from storage systems.
- **Username** and **Password:** Username and password of the above SVP

  Note: Do not use the user "Maintenance" to collect data.
- **Timezone:** Enter the time zone where the SVP is located.

4. Click **Next**. The system validates the entered details.
5. Click **Next** after successful validation. The Export Tool window appears where the Export file (.tar file) needs to be uploaded.

   Note: For each SVP probe, correct version of Export tool needs to be installed on the Probe appliance. If multiple storage systems have same microcode version, Export Tool is required only while adding probe for the first storage system. The same Export Tool will be used by other storage systems since they have the same microcode version.
6. In the **Upload New Export File** field, click **Browse** button.
7. Select the **Export Tool** file.
8. Click **Next**. The system validates the Export tool. After successful validation, click **Next.**
9. The Storage Name window appears where serial number of storage system is displayed. It can be edited. The probe will be identified with this name in RIAT Probe appliance.
10. Click **Next**.
11. Start the probe on the Status page to start collecting data.

3.3.8 Adding HNAS Probe

HNAS Probe collects data from HNAS systems.

1. Click **Home** link and then click **Add Probe**.
2. Select **HNAS** from the **Probes** list.
3. Enter the following values:
   - **HNAS SMU IP**: Enter the IP adderess of the HNAS System Management Unit (SMU).
   - **SMU Username and Password:** Enter the user credentials of the SMU.
4. Click **Next**. The system displays the list of available HNAS Servers.
5. Choose the HNAS server from which you want to collect data.
6. Click **Next**. The system validates the entered details.
7. Click **Next** after successful validation.
8. Click **Ok** and start the probe on the Status page to start collecting data.

3.3.9 Adding SAP HANA probe

SAP HANA probe collects data from HANA database. Before you add HANA probe, ensure that a user with Monitoring role should be available.

1. Click Home link and then click Add Probe.
2. Select SAP HANA from the **Probes** list.
3. Enter values for the following:
    - **Server Name/IP:** Enter HANA database server IP address/host name. Hostname should be a fully qualified domain name (FQDN).
    - **Port Number**: Port of the HANA database server. The default port is 30015 for JDBC connection.
    - **Username and Password**: User name and password of the HANA database server.
4. Click **Next**. The system validates the entered details.
5. Click **Next** after successful validation.
6. Click **Ok** and start the probe on the Status page to start collecting data.

3.3.10 Adding Linux probe

Linux probe collects **performance** and configuration data from individual machines running Linux operating systems.

Pre-requisites:

- All the target machine should have sysstat rpm installed.
- All target machines should have PERL installed with packages - IO::Select, IO::Handle, File::Path qw(mkpath), Getopt::Std, File::Path, Time::HiRes qw(gettimeofday) and Getopt::Std.
- 'scp' package must be installed on target machine.
- Directory with same name should be created manually on all target machines to copy all the data collection scripts.
- A user on target machine:
    - Permission: 'read , write and execute'.
    - If you are going to add probe for more than one target machines, a same user name and password should be available on each target machine.

1. Click Home link and then click Add Probe.
2. Select Linux from the **Probes** list.
3. Enter values for the following:
    - **Probe Name:** Probe name should be alpha numeric string with length – Min. 4 and Max. 64 characters.
    - **Username:** A user on each target Linux machine with 'read , write and execute' permissions.
    - **Password:** Password of the above user

- **Installation Directory:** Installation directory where all the data collection scripts will be copied.
- **Sample Interval (Seconds):** Defines at which interval data samples should be collected from Linux machines. You can either define sample interval to one second or sixty seconds.
- **Transfer Interval (Seconds):** Defines at which interval data will be trasferred from Linux machine to RIAT Probe appliance.

4. Click **Next.** The Add Host window appears. Enter host names of target Linux machines. Click **Add More** button if you want to add some more host names.
5. Click **Next.** RIAT Probe appliance will validate the entered details. Validation status will be displayed in the table. If validation of any target machine is failed, you can move ahead to add probe or you can go back to previous window to correct the host name details.
6. Click **Next.** The scripts to collect data from target machines will be deployed on each target machine you have added.
7. Click **Next** and then click **OK**.
8. Start the probe on the Status page to start collecting data.

3.3.11 Adding IBM XIV Probe

IBM XIV probe collects configuration and performance data from IBM XIV storage systems.

1. Click Home link and then click Add Probe.
2. Select IBM XIV from the **Probes** list.
3. Enter values for the following:
   - **Storage System IP Address:** IP address of the target IBM XIV storage system
   - **Username:** Username of the storage system. Ensure that user has minimum read only permissions to collect configuration and performance data.
   - **Password:** Password of the above user.
4. Click **Next.** RIAT Probe appliance will validate the entered details.
5. After successfully validating the details, click **Next** and then click **OK**.
6. Start the probe on the Status page to start collecting data.

3.3.12 Adding Network probe

Network probe is used to collect configuration and performance data from network switches. It collects data from the management port of the switch using SNMP.

Follow the steps to add a Network probe:

A. Add Devices (Switches)

B. Define Security Settings

C. Choose Interfaces

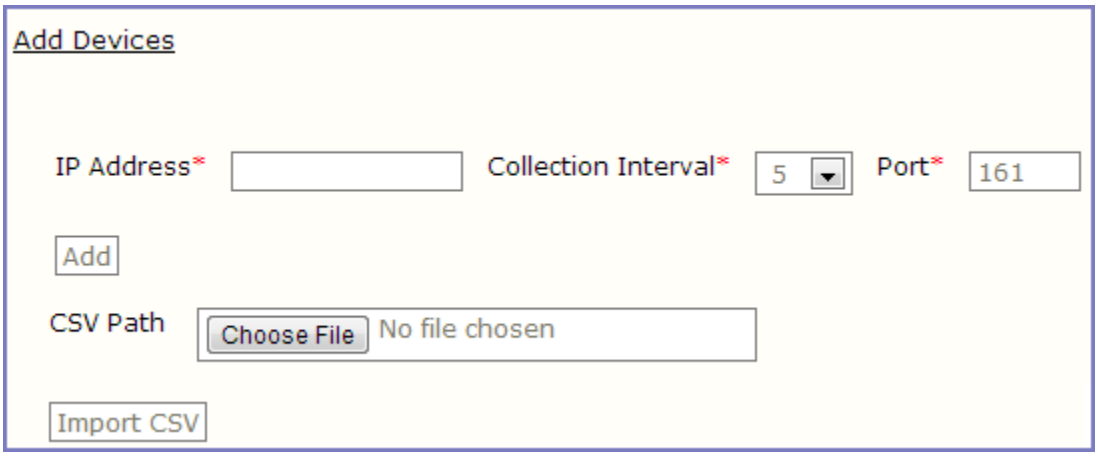
D. Configure probe: Change Interface Speed or Counter Type

E. Add Network probe

F. Start Network probe

A. Add Devices (Switches)

1. Click **Home** link and then click **Add Probe**.
2. Select **Network** from the Probes list. Add Probe window appears.



3. Enter the network switch details - **IP Address**, data **Collection Interval**, and **Port** using one of the following methods:
   - By entering IP address of each network switch and data collection interval, as well as port number for each switch.
   - By Importing a CSV file in which IP address of network switches, data collection interval, and port details. You need to create this CSV file manually before importing it, which contains one or more than one IP addresses. The format of each entry must be: <IP Address>:<Port>, <data collection interval>

     See CSV File Format to understand the CSV file format.

     Note: If port and data collection interval are not mentioned, the default values are considered. Default values are - Port – 161, Data Collection Interval – 5 Minutes.
4. Click **Add/Import CSV** based on your requirements. The details of the added devices will be dislayed in a tabel on same window.
5. Click **Next**. The Security Settings section appears.

B. Define Security Settings

1. Select IP address of the device for which you want to define the security. After selecting the IP address, the SNMP Security Version list is displayed. SNMP queries are run to collect configuration information for each device. For SNMP V1 and V2c, you need to enter only read

community string name for authentication. For SNMP V3, authentication information is required.

2. Select **SNMP Security Version** from the list and enter the authentication details as per the requirements.
   - If you select **v1** or **v2c** SNMP Security Version, the **Read Community String** field will be displayed. See the following table for details.
   - If you select **v3** option, the **SNMP Security Level** list is displayed where you must select the security levels. Based on SNMP Security Level, the required authentication must be provided. See the following table for details.

SNMP Security Version	SNMP Security Level	Required Authentication
v1 and v2c	-	Read Community String
v3	NOAUTH_NOPRIV	• Username • Security Name
	AUTH_NOPRIV	• Username • Security Name • Authentication • Authentication Password

	AUTH_PRIV	• Username
		• Security Name
		• Authentication
		  o MD5
		  o SHA
		• Authentication Password
		• Encryption
		  o AES
		  o DES
		• Encryption Password

3. Click **Apply Settings to All Devices** if you want to apply authentication settings to all the devices that are available in the "Select IP Address" list.
4. Click **Save**. The authentication details are saved.
5. After you finish defining authentication details for all the required devices, click **Next**.

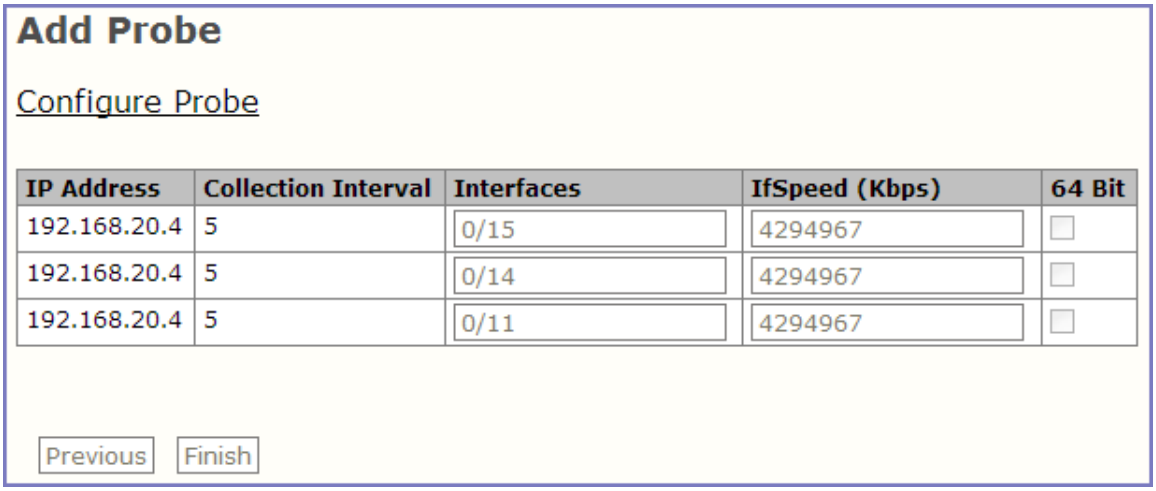
   The system attempts to connect to devices. If it is successfully connected to devices, the interface of each device is displayed, else "Connection request to this device timed out." message is displayed. Check if the authentication details of each device are correct.

C. Choose Interfaces

1. Choose the interfaces to enable data collection.

2. Click **Next**. The selected interfaces are displayed with its speed and counter type (32 bit or 64 bit). 32-bit counter type is by default configured to each interface. If the target interface supports 64-bit data collection, you can change it to 64-bit counter.

   D. Configure probe: Change Interface Speed or Counter Type



   The speed is by default displayed based on the interface configuration. Change it, if required in the **IfSpeed (Kbps)** column.

   By default, counter type is 32 bit. If you want to perform 64 bit data collection and the target interface also supports 64 bit data collection, click the checkbox in the **64 Bit** column.

   Note: For **v1** security level, the checkbox for 64 bit counter selection is disabled.

   E. Add Network probe

   Click **Finish** to add the probe. The Status window is displayed.

   F. Start Network probe

   Start the probe on the Status page to start collecting data.

3.3.13 Adding Unix probe

Unix probe collects configuration data from machines running the UNIX operating system. You can collect configuration data from following Unix flavors:

- AIX
- Linux
- Solaris
- HP-UX

Pre-requisites:

- Install perl package Net::OpenSSH on RIAT probe appliance
- Installation Directory:

    - Manually create a directory on target machines. RIAT Probe appliance will copy scripts in this directory to collect data from targets machines.
    - Installation directory should be empty.
    - Installation directory should have “0755” permission
- A user with “root” privileges should be available on each target machine

1. Click Home link and then click **Add Probe**.
2. Select Unix from the **Probes** list. The Probe Details window appears.
3. Enter the installation directory which you have created on target machine.
4. Click **Next**. On Add Host Details window, enter the following details:
    - **OS Type:** Select the operating system of the target machine.
    - **Host IP:** Target machine’s IP address
    - **Username and Password:** Credentials of the user having “root” privileges on target machine.

    Note: If you want to add more target machines, click **Add More** button. Ensure that the target machines that you are going to add should have the same directory that you have specified in Step 3.
5. Click **Next**. Entered details are validated. After successful validation, click **Next**.

    Note: If validation of any target machine fails, you can still move ahead to add probe or you can go back to previous window to correct the target system details.
6. Click **Next.** Scripts to collect data will be copied in Installation Directory.
7. Click **Next** and then click **OK**.
8. Start the probe on the Status page to start collecting data.

3.3.14 Adding UCP probe

UCP (Hitachi Unified Compute Platform) probe collects following information from the Hitachi Blade Servers.

- Chassis details
- Hitachi blade hardware details

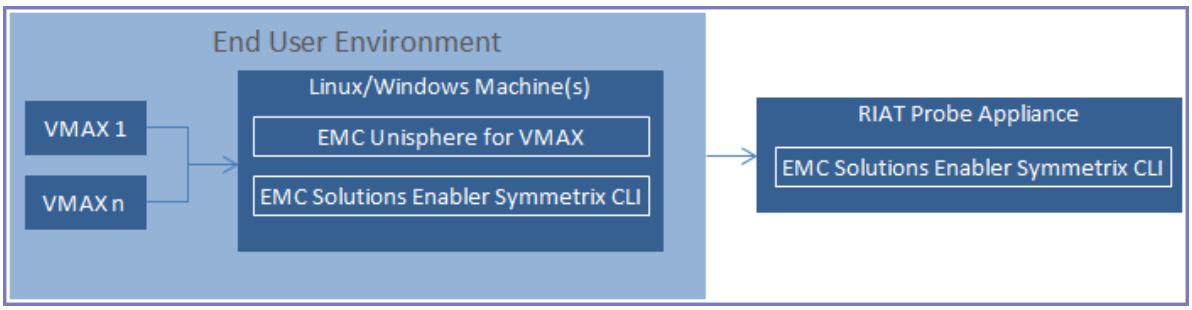
1. Click **Home** link and then click **Add Probe**.
2. Select **UCP** from the Probes list.
3. Enter the following values:
    - **IP Address:** IP address of the UCP**.** Supported IP address version is IPv4.
    - **Port Number:** Port number of SNMP to which UCP probe should listen to. By default, UCP probe listens on port - 161

- **Chassis Model:** Select the chassis model that you want to monitor. CB500 and CB 2000 chassis models are supported.
- **SNMP Version:** Select one of the SNMP versions. v1 and v2c versions are supported.
- **Community String:** Enter community string.

4. Click **Next**. The details are validated.
5. After successful validation, click **Next** and then click **OK** and start the probe on the Status page to start collecting data.

3.3.15 Adding VMAX probe

VMAX probe collects data from EMC VMAX storage systems.



Pre-requisites:

Configuration in Target environment

- **EMC Unisphere for VMAX:** A machine with EMC Unisphere for VMAX (v1.6.2.4 or above) installed, monitoring target storage systems.
- **EMC Solutions Enabler Symmetrix CLI**: A machine (could be the same as above for EMC Unisphere for VMAX or different) with EMC Solutions Enabler Symmetrix CLI (v7.6.2.26 or above) installed, monitoring all the target storage systems for which probe needs to be added.

Configuration on RIAT Probe appliance

- Install **EMC Solutions Enabler Symmetrix CLI** on RIAT Probe appliance.
    1. Log into RIAT Probe appliance. (**Username**: root **Password**: app.jeos)
    2. Copy EMC Solutions Enabler Symmetrix CLI tar.

       Note: It is recommended to install same version of EMC Solutions Enabler Symmetrix CLI, as installed in the target environment.
    3. Untar it: `tar zxf se<version>-Linux-i386-SMI.tar.gz`
    4. Install it: `./se<version>_install.sh  -install -all`
- **Configure environment variable entry in netcnfg file:** To collect data from target storage systems using EMC Solutions Enabler Symmetrix CLI , edit netcnfg file.
    1. Log into RIAT Probe appliance. (**Username**: root **Password**: app.jeos)

2. Edit **netcnfg** file: `vi /var/symapi/config/netcnfg`
3. At the end of the file, add entry as follow:

   SYMAPI_SERVER - TCPIP <*IP Address> <*IP Address> <Port> NONSECURE

   <*IP Address> = IP address of the machine where EMC Solutions Enabler Symmetrix CLI is installed.

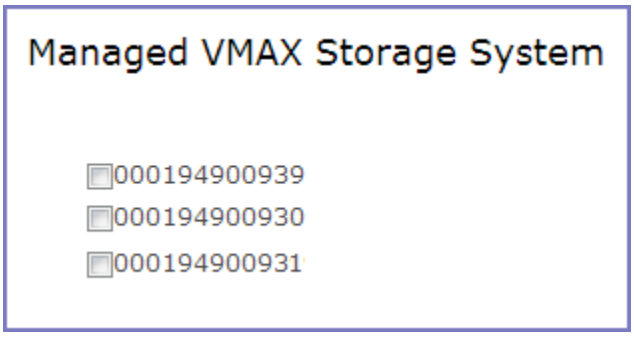
   Default port number: 2707

   Example:

   SYMAPI_SERVER - TCPIP 172.17.40.19 172.17.40.19 2707 NONSECURE
4. Save the file.

Add VMAX probe as follow:

1. Click **Home** link and then click **Add Probe**.
2. Select **VMAX** from the Probes list.
3. On the VMAX Unisphere Details window, click **Add Unisphere**.
4. On the Add VMAX Unisphere window, enter **IP Address** of the machine where EMC Unisphere for VMAX is installed, Unisphere's **Username** and **Password**.
5. Click **Next**. After successful validation, click **Next** again.
6. On the Managed VMAX Storage System window, select the VMAX storage systems for which you want to add VMAX probe.



   For each VMAX storage a separate probe will be added. If you do not want to add probe for all the listed storage systems, you can add those later on. To add probe for remaining storage systems later on, see Managing VMAX probe.

7. Click **Finish** and then click **OK**. Proceed to start added probe(s).

3.4 Starting and stopping added probes

To start a probe, go to the Status window and click **Start** corresponding to the Probe.

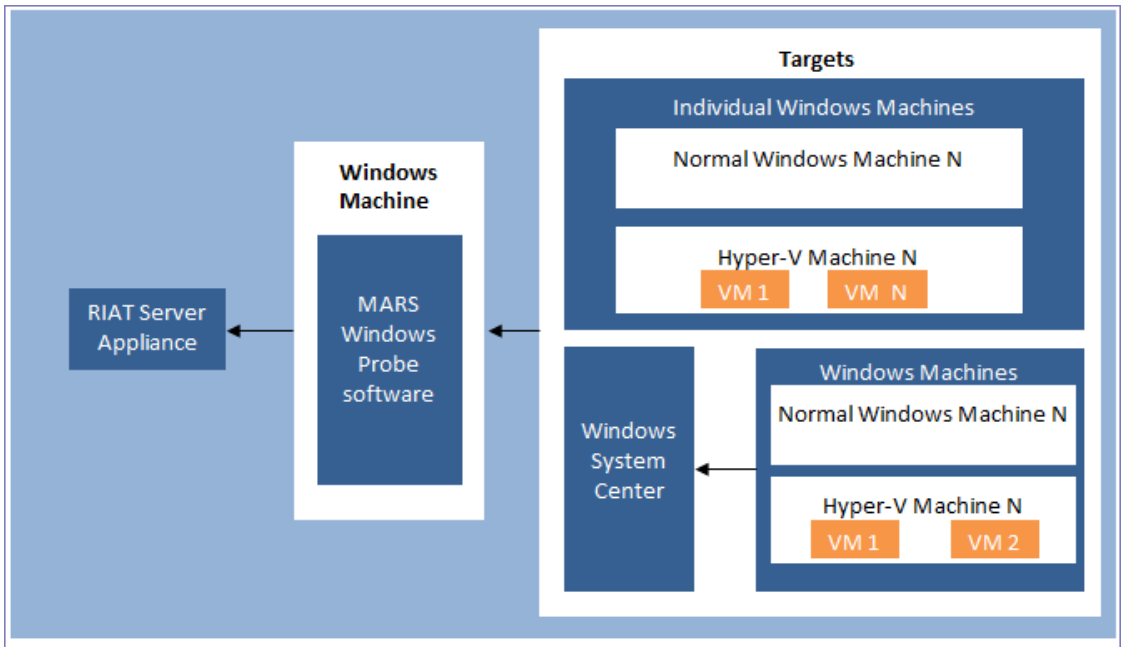
The 'Status' of the Probe will change to green and it will start collecting data. It could be anywhere between 15 minutes to 1 hour for the collected data to appear on the FTP Server.

4 MARS Windows Probe for Windows and Hyper-V machines

MARS Windows Probe is desktop-based software that collects performance and configuration data from Microsoft System Center, individual Windows machines (using WMI and PerfMon) and Hyper-V machines. A Hyper-V machine is any target standard Windows machine on which multiple VMs are running.

MARS Windows probe uploads the collected data to RIAT Server over cloud, which generates separate reports for Hyper-V machines and standard Windows machines.

See the following diagram to understand the MARS Windows Probe deployment scenario:

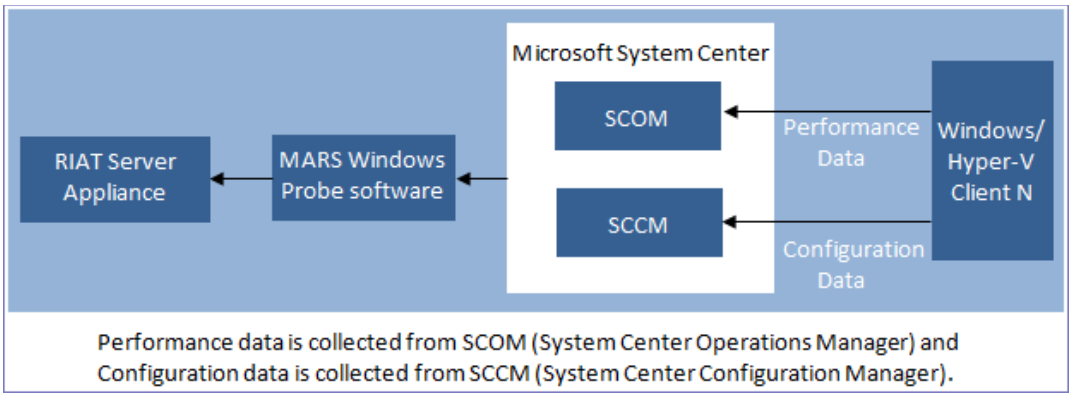


MARS Windows Probe software is installed on a Windows machine to collect data from Individual Windows Machines/Microsoft System Center / Windows machines (Hyper-V) on which one or more VMs are running.

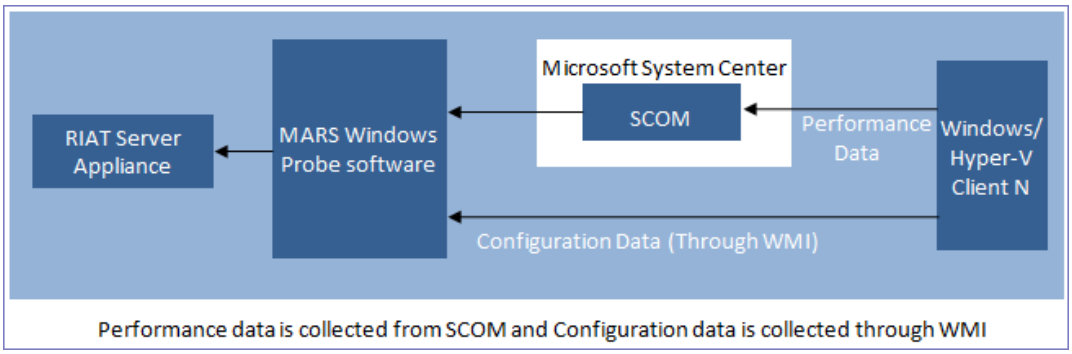
4.1 MARS Windows Probe software deployment methods

Using this software, you can collect the configuration and performance data from Windows machines using any one of the following three methods.

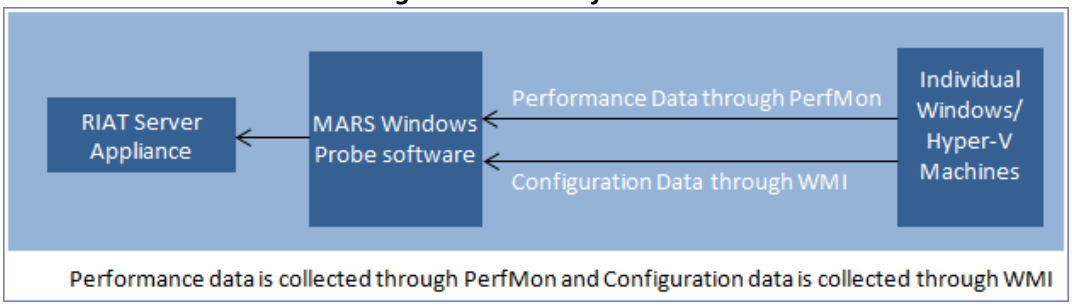
Method 1: Data collection from SCOM and SCCM



Method 2: Data Collection from SCOM and WMI



Method 3: Data Collection through WMI and PerfMon



4.1.1 Pre-requisites

For Method 1

SCOM:

- Target Windows machines should be configured in SCOM
- For discovering SCOM, user should have “Advanced Operator” or “Administrator” role in SCOM and it should have remote logon permissions to SCOM Server.
- Remote registry service must be running on all the machines configured in SCOM.
- For importing Cumulus management pack in SCOM (which configures performance rules), access to SCOM console is required.

SCCM:

- Target Windows machines should be configured in SCCM
- Hardware Inventory Client Agent (of SCCM) must be running on target machines. This agent collects required configuration data and dumps into the SCCM database.
- For discovering SCCM, it is required to connect database which is configured for SCCM. The discovery user should be part of db_datareader group in SQL Server.

For Method 2

SCOM:

- Target Windows machines should be configured in SCOM
- For discovering SCOM, user should have "Advanced Operator" or "Administrator" role in SCOM and it should have remote logon permissions to SCOM Server.
- Remote registry service must be running on all the machines configured in SCOM.
- For importing Cumulus management pack in SCOM (which configures performance rules), access to SCOM console is required.

WMI:

- User should be a domain administrator and ensure that the user has permissions to access ROOT and ROOT/CIMV2 WMI namespaces on each target machine. Permissions required for these namespaces are: **Execute Methods** and **Remote Enable**
- Firewall exceptions must be added for WMI on all the target machines. Add the exceptions using the following commands:
  - `netsh firewall set service RemoteAdmin`
  - `netsh firewall set service type=fileandprint mode=enable profile=all scope=all`
- For workgroup computers: UAC must be disabled or DWORD value **LocalAccountTokenFilterPolicy** has to be added in **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system** registery of every target machine with value 1**.** For more information, refer to http://support2.microsoft.com/kb/942817/en-us

For Method 3

- Probe machine and target machines should be part of either Workgroup or Domain.
- If the firewall is enabled on target machine, open the ports for WMI and Perfmon to respond to remote connections. To add WMI and PerfMon firewall exceptions, execute the following commands on every target system:
  - `netsh firewall set service RemoteAdmin`
  - `netsh firewall set service type=fileandprint mode=enable profile=all scope=all`
- To connect to Windows machines remotely:

- On every target system, “Local Service” should have ‘read’ permissions on the following registery key:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
- Remote Registry service must be running on all target machines

- For domain computers, discovery user must be member of “Domain Admin” group.
- For workgroup computers: Following settings are required only in case of Workgroup computers and if you are not using built-in administrator for connections.
  - A user (Administrator) with same username and password should be present on probe and target machines and ensure that the user has permissions to access ROOT and ROOT/CIMV2 WMI namespaces on each target machine. Permissions required for these namespaces are: **Execute Methods** and **Remote Enable**
  - UAC must be disabled or DWORD value LocalAccountTokenFilterPolicy has to be added in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system registery of every target machine with value 1. For more information, refer to http://support2.microsoft.com/kb/942817/en-us
  - Computer Browser service must be running on target machines

Pre-requisites for Windows machine where you will deploy MARS Windows Probe software:

- **Operating System**: Any one of the following operating systems:
  - Windows 7
  - Windows 8
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- **RAM**: Minimum 8 GB
- **Disk Space**: Minimum 50 GB
- Microsoft .Net Framework 3.5 SP1 or later must be installed
- A user on this computer should have the “Logon as a service” permission.
- One MARS Windows Probe can collect data from maximum 100 individual machines. To collect data from more than 100 Windows machines, you need to deply another Windows probe.

Supported Windows operating systems as targets:

- Windows 7
- Windows 8
- Windows Server 2003
- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

4.1.2 Deploying MARS Windows Probe software

1. Execute the MARS Windows Probe installer.
2. Click **Next** and enter the Domain Administrator's or Local user's credentials for the Windows machine in the format specified on the window.

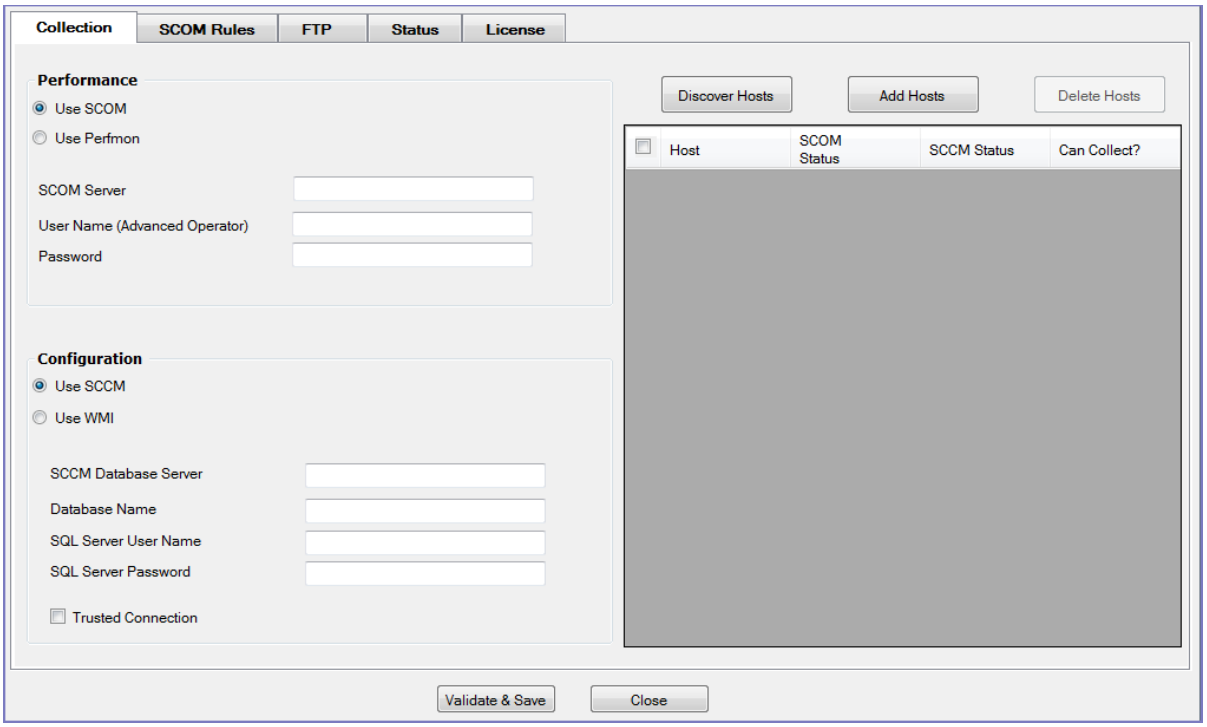
   Important: The entered user should have the "Logon as a service" permission.
3. Click **Next** and then select the installation folder.
4. Click **Install** to start the installation.
5. Click **Finish**.

4.1.3 Configuring MARS Windows Probe software

1. Double-click the **MARS Windows Probe** icon on the desktop.

   Note: If you do not see MARS icon on desktop, execute this command on command prompt which will referesh Windows icon database.

   ```
   ie4uinit.exe -ClearIconCache
   ```
2. In the **License** tab, click **Browse** and select the License file to register it.
3. Click **Submit**.
4. Click **Collection** tab. Configure the settings based on your requirements:


Collection
SCOM Rules
FTP
Status
License
Performance
Use SCOM
Use Perfmon
SCOM Server
User Name (Advanced Operator)
Password
Configuration
Use SCCM
Use WMI
SCCM Database Server
Database Name
SQL Server User Name
SQL Server Password
Trusted Connection
Discover Hosts
Add Hosts
Delete Hosts
Host
SCOM Status
SCCM Status
Can Collect?
Validate & Save
Close

For method 1 and method 2:

Method	Configuration Required for the Selected Method
Method 1: Data collection from SCOM and SCCM	1. Select **Use SCOM** button and enter the following details: • **SCOM Server:** SCOM Server IP address • **User Name (Advanced Operator):** SCOM Server user name • **Password:** Password of SCOM Server 2. Select **Use SCCM** button and enter the following details: • **SCCM Database Server:** IP address of SCCM Server. <IP or name of the server>\<username> • **Database Name:** Database name • **SQL Server User Name:** Database user name • **SQL Server Password:** Password of the database **Note:** If you click the **Trusted Connection** checkbox, SQL Server User Name and SQL Server Password fields will be disabled.
Method 2: Data collection from SCOM and WMI	1. Select **Use SCOM** and enter the details mentioned in the previous row. 2. Select **Use WMI** and enter the following details: • **User Name (Administrator):** <Domain Name>\<User> • **Password:** Password of the entered user

For method 3:

Method	Configuration Required for the Selected Method
Data collection through WMI and PerfMon	1. Select **Use Perfmon**. The system enables the **Use WMI** option automatically. 2. Enter the following details for **Use Perfmon** and **Use WMI** options: • **User Name (Administrator)**: o In Workgroup environment: <Computer Name>\<User> ▪ Computer Name: Computer name where MARS Windows Probe software is installed ▪ User: A user with administrative privilege. This user must exist on all computers that you have specified. o In Active Directory environment: <Domain Name>\<User> ▪ Domain Name: Name of the domain ▪ User: A user with Domain Admin privilege • **Password**: Password of the entered user 3. To know the performance of processes, select the **Collect Process Data** check box.

5. Click one of the following:
   - **Discover Hosts:** Click this button to discover all hosts present in current domain i.e. domain of this machine. Out of the listed target machines, you can choose target machines that should be probed by selecting/clearing checkbox corresponding to the host.
   - **Add Hosts:** Click this button if you want to enter host names manually. A new window will appear, where you should enter comma-separated list of Windows machines' host names/IP addresses, which will be monitored by this probe. After entering target machines, save the changes.
6. After you successfully discovered/entered hosts, click the **Validate & Save** button to establish connection.

   After connecting successfully, the list of the Windows hosts' is displayed in the table.

	Host	SCOM Status	SCCM Status	Can Collect?
☑	PDC	True	True	True
☐	TESTXP1			
☑	ALPHA	True	True	True
☐	MIMOSA			
☑	adstest	True	True	True
☐	NETAPP-PUNE1			

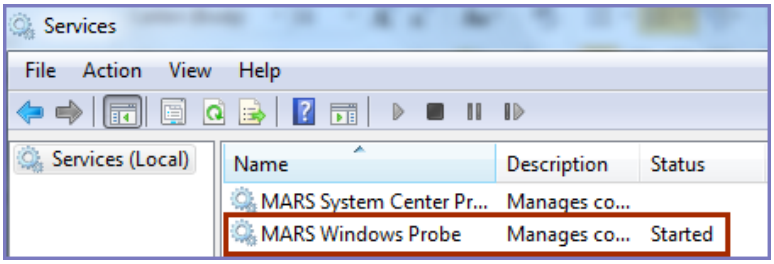
Table Details:

Column Name	Description
Host	Name of the host
SCOM Status	Displays if the host is available from SCOM **Note:** If data is being collected through Perfmon, the "Perfmon Status" column will be displayed.
SCCM Status	Displays if host is accessible from SCCM **Note:** If data is being collected through WMI, the "WMI Status" column will be displayed.
Can Collect?	Displays if MARS Windows Probe software can collect data from host **Note:** If MARS Windows Probe is unable to collect data from target systems, refer to logs, which are created in log directory in the installation folder. The Console.log file contains the probe console logs.

4.1.4 Configuring FTP settings for cloud deployment model

MARS Windows Probe software should be configured to send the collected data to cloud FTP server.

1. Click the **FTP** tab.
2. Click the **Not Configured** link.
3. Enter the FTP Details. FTP details are provided in a separate document.
4. Click **OK**.
5. Click **Status** tab.
6. On the Status tab, click the **Start** button to start the MARS Windows Probe service.
7. Check if the **MARS Windows Probe** service is installed and started on this machine.



4.1.5 Working with the SCOM Rules tab

Viewing SCOM Rules tab details

On MARS Windows Probe software, Rules tab contains the Performance rules in SCOM. The SCOM Rules tab displays the table along with the details about the existing performance rules configured on SCOM server.

SCOM Performance Rules

Object	Counter	Rule Exists	Rule Name	Enabled	Frequency in sec	Instances
Processor	% Idle Time	Exists	Prasad2	True	60	All
Processor	% Processor Ti...	Exists	Performance Collection Processor % Proc...	True	60	All
Processor	C1 Transaction...	Exists	Performance Collection Processor C1 Tran...	True	60	All
Processor	C2 Transaction...	Exists	Performance Collection Processor C2 Tran...	True	60	All
Processor	C3 Transaction...	Exists	Performance Collection Processor C3 Tran...	True	60	All
Processor	Interrupts/sec	Exists	Performance Collection Processor Interrup...	True	60	All
Physical...	% Disk Read T...	Exists	Performance Collection PhysicalDisk % Di...	True	60	All
Physical...	% Disk Write Ti...	Exists	Performance Collection PhysicalDisk % Di...	True	60	All
Physical...	% Idle Time	Exists	% Physical Disk Idle Time Windows Server...	False	300	$Target/Prope
Physical...	Avg. Disk Bytes...	Exists	Performance Collection PhysicalDisk Avg. ...	True	60	All
Physical...	Avg. Disk Bytes...	Exists	Performance Collection PhysicalDisk Avg. ...	True	60	All

The details of the column headers are as follow:

Column Name	Description
Object	Name of the object to be monitored
Counter	Name of the performance metric
Rule Exists	Displays whether the performance rules for given object and counter exists in the current SCOM server. If rule for the given object and counter is absent in the current SCOM server, either rules need to be created manually or imported from the Management Pack, which is available along with the MARS Windows Probe installer. To import the management pack, see Importing Management Pack in SCOM.
Rule Name	Name of the rule
Enabled	Displays if the rule is enabled
Frequency in sec	Rule execution frequency in seconds
Instances	Displays the name of instances for which the rule is configured. **All** stands for all the instances.

Understanding Rules list

The listed rules are either in one of the following colors:

- **Row in the Green** color indicates that the rule for given object and counter is present in the SCOM Server and no action is required.

- **Row in the Gray** color indicates that the rule is present in the SCOM server for the given object and counter but it is disabled. You need to enable these rules in SCOM.
- **Row in the Red** color indicates that the performance rule for the given object and counter is not present in the current SCOM server.

Refreshing MARS Windows Probe software

If you create the missing rules or enable the disabled rules in SCOM server, click the **Refresh** button to get the changes reflected in MARS Windows Probe software.

5 Advanced Operations

This chapter describes steps that are not common but required only in specific situations.

5.1 Assigning a static IP address to RIAT Probe

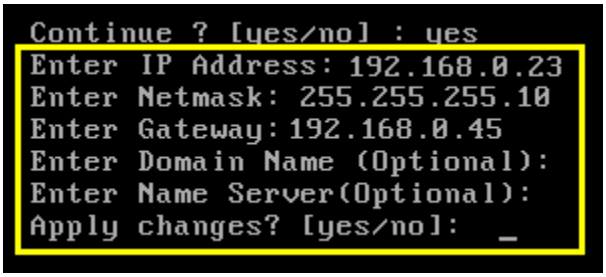
An IP address is dynamically assigned to RIAT Probe using DHCP at the time of deployment. If you need to assign a static IP address to RIAT Probe, follow the steps in this section.

5.1.1 Assigning static IP address to RIAT Probe in vSphere

1. In the vSphere application, select RIAT Probe that you have deployed and then click the **Console** tab in the right navigation pane.
2. Log on to the console
   - **localhost login**: `config`
   - **Password**: `megha!234`

   The system displays a notification to assign a static IP address.

3. Type **yes** and then press **Enter**.
4. Enter the following details and type **yes** to apply the changes.
   - IP address
   - NetMask
   - Gateway
   - Domain Name
   - Server Name



The system assigns the desired static IP address to RIAT Probe if there are no conflicts.

5.1.2 Assigning static IP address to RIAT Probe in VMware Player

The process for assigning a static IP address to RIAT Probe using VMware Player is similar to that using vSphere.

First, log on to the console in VMware Player

- **localhost login**: `config`
- **Password**: `megha!234`

The rest of the steps are identical to that of "Assigning static IP address to RIAT Probe in vSphere"

5.2 MARS Windows Probe

This section describes more details of MARS Windows Probe.

5.2.1 Importing Management Pack in SCOM

1. Log on to SCOM server and click **Administration**.
2. Right-click the **Management Packs** and then click **Import Management Packs**.
3. Click **Add** and then select **Add from Disk**.
4. Browse to the management pack and then click **Open**. Ensure that the management pack copy is the latest one.
5. Click **Install** and then click **Close**. The Management Pack is successfully imported.
6. Open MARS Windows Probe and click the **Settings** tab.
7. Click **Validate and Save**.
8. Click **SCOM Rules** tab and then click **Refresh**.
9. Click **Close**.

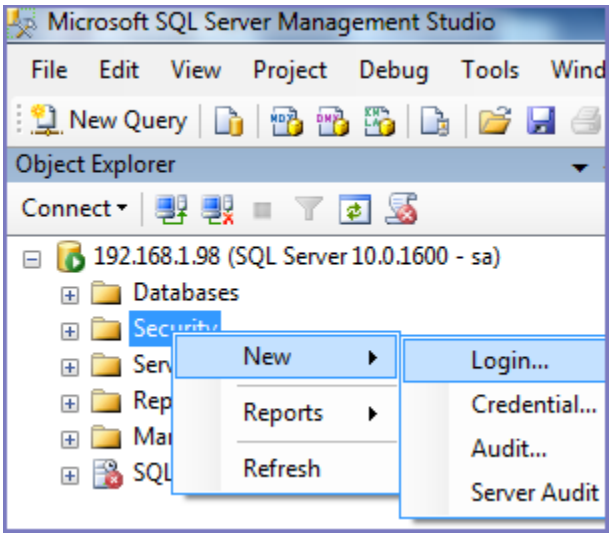
5.2.2 Viewing log files for MARS Windows Probe

The log files help to view the details of the application and errors for diagnostic purposes.

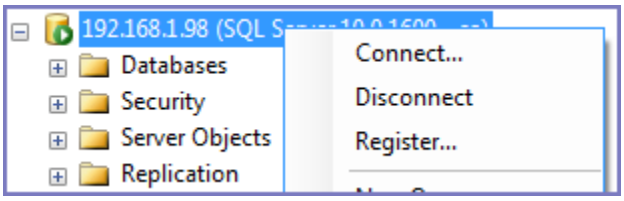
The logs are created in **log** directory in the installation folder. The **Console.log** file contains the probe console logs and the **MARSWindowsProbe.log** file contains the Probe service logs.

5.3 Creating User in SQL Server

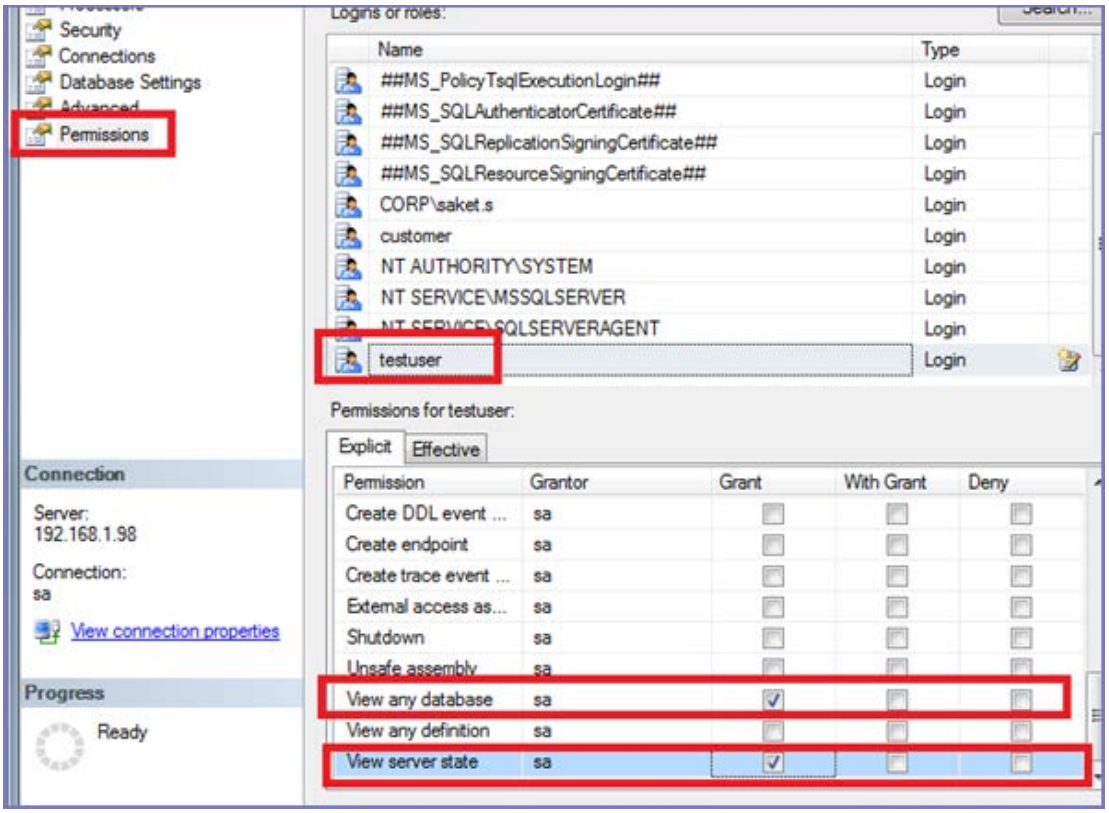
1. Log on to SQL Server Management Studio with a user belonging to the group that has the Administrative rights.
2. In **Object Explorer**, expand the SQL Server.
3. Right-click **Security** and point to **New** and select **Login**.



4. On the **Login – New** dialog box, enter the following details:
    a. In the **Login name** field, enter the user name that you are going to create.
    b. To create a login in a SQL Server database, select **SQL Server authentication** button.
    c. In the **Password** field, enter a password for the new user. Enter the password again into the **Confirm Password** field.
    d. Click **OK**.
5. Right click **Database Server** and click **Properties**.



6. Click **Permission** and select the created user.
7. Grant the **View any database** and **View server state** permissions for the created user. See the following screen capture for more details.

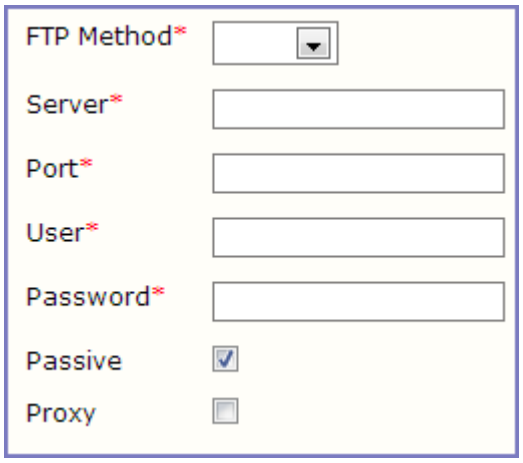


8. Click **OK**.

5.4 Manually uploading data on FTP target

RIAT Probe can also be used as the SFTP Server; it has capability to store data to itself.

To configure RIAT Probe as the FTP target, specify the RIAT Probe details in the FTP section during the time of deployment.



- **FTP Method:** SFTP
- **Server:** IP address of RIAT Probe
- **Port**: 22

- **User**: `root`
- **Password**: `app.jeos`
- **Passive**: Select the check-box.
- **Proxy:** Do not select this check-box.

To copy the data collected by RIAT Probe to a FTP location do the steps as follow:

1. Log on to the RIAT Probe console:

   Localhost login: `root`

   Password: `app.jeos`

2. To display the contents of the directory execute **ls** command.

   The Probe data is stored in the directory with a long name. For example - 7fe18389-7a45-4b1e-89eb-3b37459c7f27. This name is the unique appliance id assigned to RIAT Probe appliance.

3. Navigate to appliance ID folder.

   ```
   cd <Appliance ID folder name>
   ```

4. Create zip folder:

   ```
   zip  -r  <ApplianceIDFoldername>.zip *
   ```

5. Login to the RIAT Probe appliance using Filezilla (Third party tool) and enter the following details:

   Note: If you do not have Filezilla, download it.

   - Host: <IP address of RIAT Probe Appliance>
   - Username: root
   - Password: app.jeos
   - Port: 22

6. Copy the zipped folder from RIAT Probe appliance to your local machine.
7. Extract the folder on the local machine and upload this folder on:

   - Host : datamartftp.hds.com
   - Username : riatdata
   - Password : riatdata123
   - Port : 22

5.5 Upgrading RIAT Probe without losing data

RIAT Probe can be upgraded either remotely or locally without losing the previous data and configuration.

It is recommended that the upgrade should be done locally which takes less time (approximately 10 minutes) rather than doing it remotely, which takes more time (approximately 1 Hour).

Pre-requisites:

You must have two 'upgrade files' for RIAT Probe, as appropriate. It consists of a .zip file and a .hash file that has the same filename as the target version number.

For example, if you are upgrading RIAT Probe to a new version "RIAT-probe-8.1-12072010" then you will need the following files:

a. Build file: riat-probe-8.1-12072010.zip

b. Hash file: riat-probe-8.1-12072010.zip.hash

To upgrade RIAT Probe without losing the data, do the following:

1. On RIAT Probe UI, click the **Manage** link and then select **Upgrade Probe**.
2. Select **Upgrade** option.
3. Browse to the **Build** and **Hash** file, and then click **OK**.
4. Restart RIAT Probe.

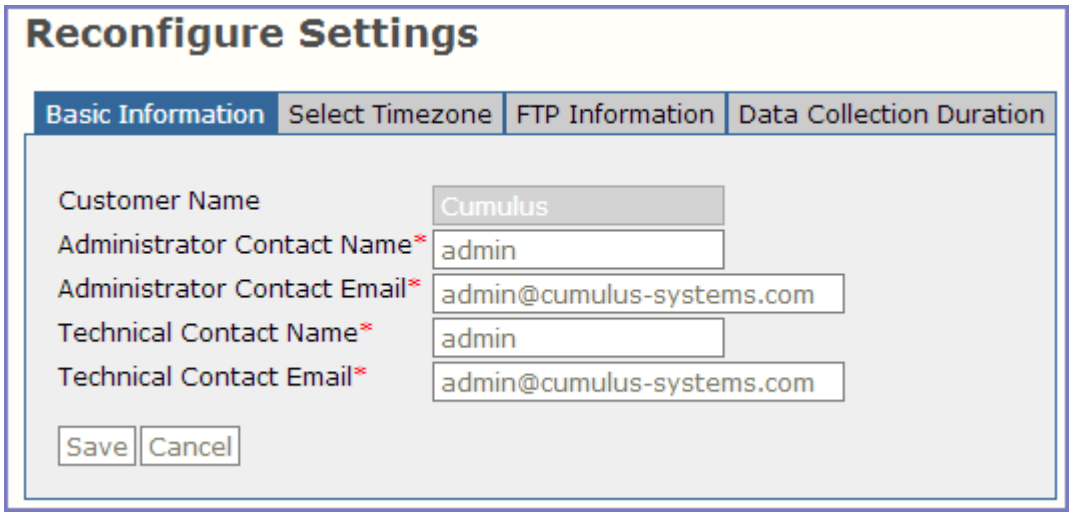
   Verify the new version number at the bottom of the RIAT Probe/Server Login window.

5.6 Reconfiguring RIAT Probe appliance

You can reconfigure the following details for RIAT Probe Appliance:

- User's basic information
- Timezone settings
- FTP information
- Data Collection Duration

To reconfigure these details, click **Reconfigure** located at the bottom of the RIAT Probe's Home page and reconfigure the details on Reconfigure Settings window.



Updating user's basic information

1. Click the **Reconfigure** tab.
2. Enter the follwing details:

- **Customer Name:** Name of the customer
- **Administrator Contact Name** and **Administrator Contact Email:** Name and email address of the administrator.
- **Technical Contact Name** and **Technical Contact Email**: Name and email address of the technical contact.

3. Click **Save**.

Setting time zone

Select the time zone where RIAT Probe appliance is deployed.

1. Click the **Select Timezone** tab.
2. Select the timezone in the **Timezone** field and then click **Save**.

Updating the FTP Information

See Configuring FTP settings for updating FTP Information.

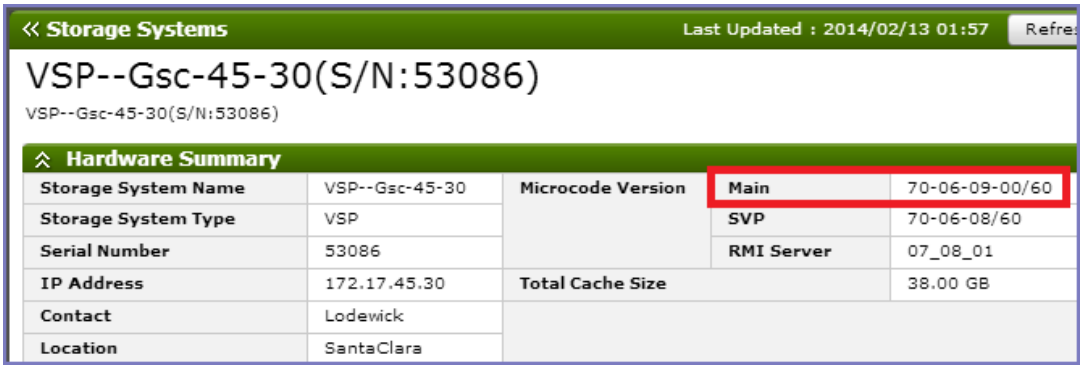
Configuring the data collection duration

Maximum data collection duration is set as per the license expiry date but it can be reduced.

1. On the Data Collection Duration window, select the collection date and time.
2. Click **Save**.

5.7 Identifying Microcode Version (for SVP Probe)

1. Log on to the Storage Navigator.
2. Select the storage system in the left pane to see the microcode version.
3. The microcode version is displayed as follow:



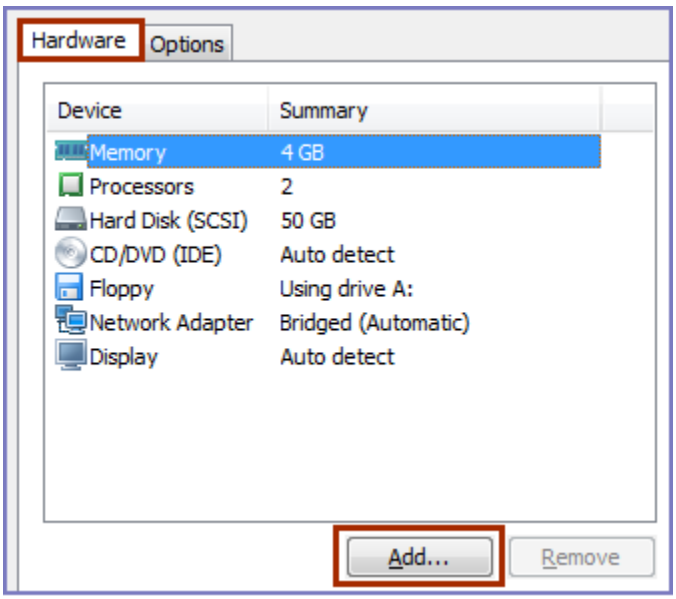
5.8 Adding Command Device in VMware Player (Only for USP V storage system)

Command device enables SVP probe to collect configuration data from USP V storage system.

Pre-requisite:

Ensure that RIAT Probe appliance is powered-off. Ignore this, if it is already powered-off.

1. Select the virtual machine where you have deployed RIAT Probe appliance and then click **Edit virtual machine settings.**
2. On the VMware Machine Settings page, select Hardware tab, and click **Add.**



3. On the Add Hardware Wizard, select **Generic SCSI Device**, and click **Next.**
4. Select the appropriate SCSI device, select the checkbox for **Connect at power on** and click **Finish**.
5. Ensure that that command device is added for the USP V storage system:
   a. Log on to RIAT Probe using console. (Username: `root`, Password: `app.jeos`)
   b. Execute the `/usr/local/megha/svp/list_devices` command to check if the command device is added for the desired USP V storage device.
   c. In the following screen capture, the command device is highlighted:

```
login as: root
root@172.17.237.229's password:
Last login: Fri Aug 23 11:35:11 2013 from 10.1.136.14
[root@localhost ~]# /usr/local/megha/svp/list_devices

Device : /dev/sda       vendor id: VMware       product id:Virtual disk         Serial Number: 0
==========================================================================================
Device : /dev/sda1      vendor id: VMware       product id:Virtual disk         Serial Number: 0
==========================================================================================
Device : /dev/sda2      vendor id: VMware       product id:Virtual disk         Serial Number: 0
==========================================================================================
Device : /dev/sdb       vendor id: HITACHI      product id:OPEN-V-CM            Serial Number: 53086
==========================================================================================
[root@localhost ~]#
```

5.9 Creating user for NetApp 7-mode

1. Log on to the NetApp command line.
2. Add a role:

Run the following command for NetApp storage system version 7.3.6:

```
useradmin role add <Role Name> -a login-http-admin,api-system-get-info,api-license-list-info,api-aggr-list-info,api-volume-list-info,api-nfs-exportfs-list-rules,api-disk-list-info,api-quota-report,api-lun-list-info,api-lun-map-list-info,api-qtree-list,api-perf-object-instance-list-info,api-perf-object-counter-list-info,api-perf-object-get-instances,api-system-get-version,api-snapmirror-get-status,api-useradmin-user-list,api-volume-get-root-name,api-volume-options-list-info,api-useradmin-group-list,api-snapshot-list-info,api-useradmin-role-list,security-api-vfiler
```

For example:

```
netapp73-1(takeover)> useradmin role add marsrole -a login-http-admin,api-system
-get-info,api-license-list-info,api-aggr-list-info,api-volume-list-info,api-nfs-
exportfs-list-rules,api-disk-list-info,api-quota-report,api-lun-list-info,api-lu
n-map-list-info,api-qtree-list,api-perf-object-instance-list-info,api-perf-objec
t-counter-list-info,api-perf-object-get-instances,api-system-get-version,api-sna
pmirror-get-status,api-useradmin-user-list,api-volume-get-root-name,api-volume-o
ptions-list-info,api-useradmin-group-list,api-snapshot-list-info,api-useradmin-r
ole-list,security-api-vfiler
Wed Jul  9 07:17:15 GMT [netapp73-1 (takeover): useradmin.added.deleted:info]: T
he role 'marsrole' has been added.
Role <marsrole> added.
```

Run the following command for NetApp storage system version 8.0.1:

```
useradmin role add <Role Name> -a login-http-admin,api-system-get-info,api-license-list-info,api-aggr-list-info,api-volume-list-info,api-nfs-exportfs-list-rules,api-disk-list-info,api-quota-report,api-lun-list-info,api-lun-map-list-info,api-qtree-list,api-perf-object-instance-list-info,api-perf-object-counter-list-info,api-perf-object-get-instances,api-system-get-version,api-snapmirror-get-status,api-useradmin-user-list,api-volume-get-root-name,api-volume-options-list-info,api-useradmin-group-list,api-snapshot-list-info,api-useradmin-role-list,api-net-ifconfig-get,security-api-vfiler
```

For example:

```
dataontap> useradmin role add marsrole  -a login-http-admin,api-system-get-i
nfo,api-license-list-info,api-aggr-list-info,api-volume-list-info,api-nfs-ex
portfs-list-rules,api-disk-list-info,api-quota-report,api-lun-list-info,api-
lun-map-list-info,api-qtree-list,api-perf-object-instance-list-info,api-perf
-object-counter-list-info,api-perf-object-get-instances,api-system-get-versi
on,api-snapmirror-get-status,api-useradmin-user-list,api-volume-get-root-nam
e,api-volume-options-list-info,api-useradmin-group-list,api-snapshot-list-in
fo,api-useradmin-role-list,api-net-ifconfig-get,security-api-vfiler
Role <mars.role> added.
dataontap> Wed Jul  9 13:03:09 IST [dataontap: useradmin.added.deleted:info]
: The role 'mars.role' has been added.
```

3. Add a group:

```
useradmin group add <Group Name> -r marsrole
```

For example:

```
dataontap> useradmin group add mars_group -r marsrole
Group <mars_group> added.
```

4. Add a user:

```
useradmin user add <User Name> -g mars_group
```

For example:

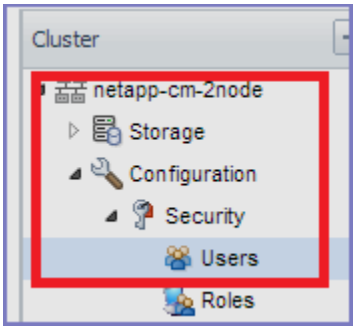
```
dataontap> useradmin user add mars_user -g mars_group
New password:
Retype new password:
Thu Feb 20 18:23:57 IST [dataontap: useradmin.added.deleted:info]: The user 'mars_us
er' has been added.
User <mars_user> added.
```

5. Enter the password.

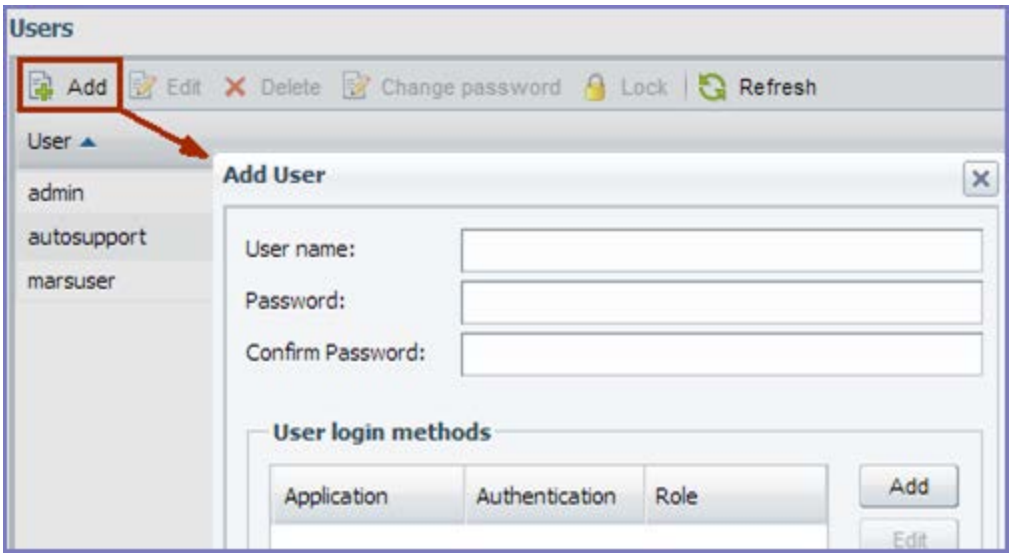
Proceed to Add NetApp probe in RIAT Probe Appliance.

5.10 Creating user for NetApp C-mode

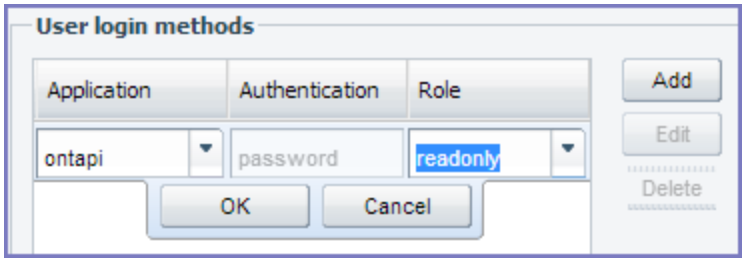
1. Log on to target NetApp storage system using NetApp OnCommand System Manager.
2. Navigate to <NetApp Storage system name> → Configuration → Security → Users.



3. In the Users pane, click **Add** and enter details in Add User window:



- **UserName:** Enter any valid username.
- **Password & Confirm Password:** Enter password for above user and confirm it.
- Under User login methods section, click **Add** and do the following:



  - Select **ontapi** in the Application column.
  - In the Role column, select **readonly**.

    Note: By default, **password** is selected in Authentication column.
  - Click **OK.**

4. Click **Add**. The new user will be added. You can use this user to collect configuration and performance data.
   Next: Proced to Add NetApp probe in RIAT Probe Appliance

5.11 Managing VMAX probe

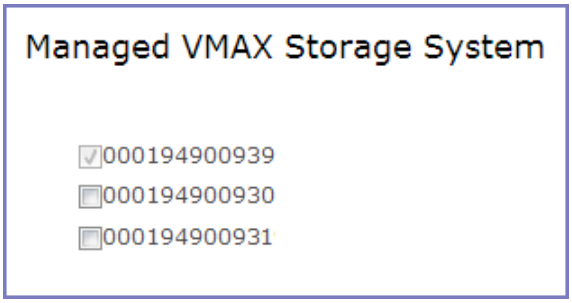
After you add VMAX probe, you can:

- Add VMAX probe for the remaining VMAX storage systems
- Edit details of EMC Unisphere for VMAX

5.11.1 Adding VMAX probe for already added EMC Unisphere for VMAX

1. Click **Home** link and then click **Add Probe**.

2. Select VMAX from the **Probes** list. The VMAX Unisphere Details window appears.
3. Click **Add Storage** link corresponding to the Unisphere for which you want to add Probe. The Managed VMAX Storage System window appears.
4. Select the checkbox for which you have not added probe(s):



5. Click **Finish** and then click **OK**. Proceed to start added probe(s).

5.11.2 Edit details of EMC Unisphere for VMAX

Due to security reasons, EMC Unisphere for VMAX's administrator may change password or user name in future. To continue data collection, you need to change password or username in RIAT Probe appliance as well.

1. On the Status page, if VMAX probe corresponding to EMC Unisphere for VMAX is (which you want to edit) is running, stop it.
2. Click **Edit** link corresponding to the EMC Unisphere for VMAX that you want to edit. The Edit VMAX Unisphere Details window appears.
3. Edit the username or password of the EMC Unisphere for VMAX.
4. Click **Next**. The system validates entered details.
5. After successful validation, click **Next.**
6. Click **OK**.

5.12 CSV file format (for Network probe)

Each row must consist of a single IP address followed by an optional comma and a data collection interval value.

<ip_address>,[<collection_interval>]

Valid values for the collection interval are 1, 3, 5, 10, or 15. If the field is not provided, the default value of five is assumed. If an invalid or empty value is found, the default value of five will be used.

Examples:

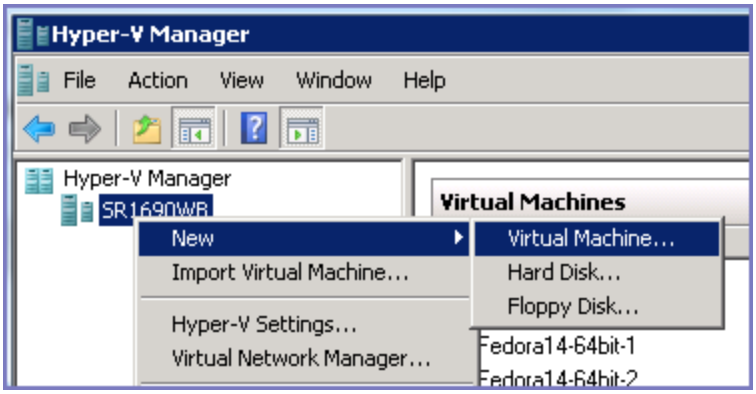
192.168.2.100,10 -- indicates 10 minute collection for this IP address
192.168.1.20,5 -- indicates default 5 minute collection for this IP address
192.168.10.10,5 -- indicates default 5 minute collection for this IP address
192.168.1.24,9 -- incorrect, defaulted to 5 minute collection for this IP address

RIAT Probe setup will inform you when invalid values are found and will set it to default five minutes.

Appendix A: RIAT Probe deployment using Hyper-V Manager

To deploy RIAT Probe in Hyper-V, you must deploy Virtual Hard Disk (VHD) of probe.

1. Right-click Hyper-V machine, point to **New** and then click **Virtual Machine**.



2. Click **Next**.
3. In the Spcify Name and Location section, specify name of the virtual machine in **Name** field and then click **Next**.
4. In the Assign Memory section, specify the required memory. Minimum: 4 GB Recommended: 8 GB

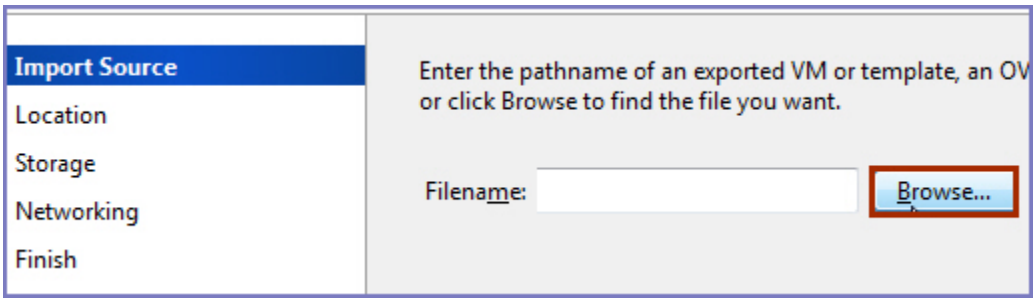
   Click **Next**.The Configure Networking section appears.
5. Configure network for the VM and then click **Next**.
6. In the Connect Virtual Hard Disk section, click **Use an existing virtual hard disk** button.
7. Browse to the location to select RIAT Probe VHD.
8. Click **Finish.**
9. Right-click VM and start it.
10. Proceed to the Configuring RIAT Probe Appliance section.

Appendix B: RIAT Probe deployment using Citrix XenCenter

RIAT Probe OVA package deployment

1. Open the Citrix XenCenter application.
2. From the File menu, select **Import**.

3. Click **Browse** and select RIAT Probe OVA file.

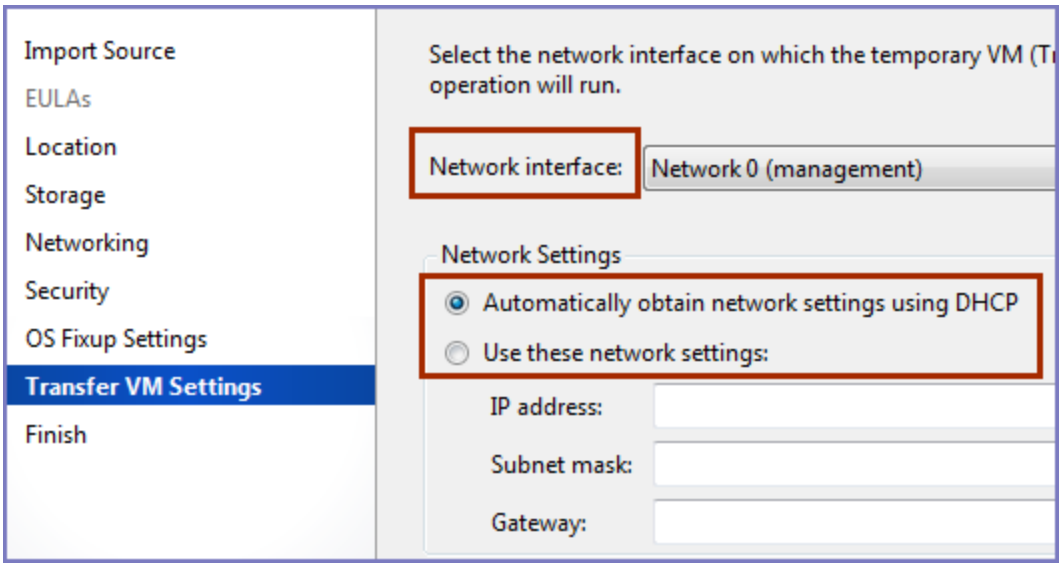


4. Click **Next.** The system skips the EULA section, as it is not applicable to RIAT Probe OVA file and displays Location section to specify the location of RIAT Probe and home server.
5. In the Loction section, select a pool to deploy RIAT probe appliance from the **Import VM(s) to** list. Based on the selection, the Home Server will be selected. A Home Server provides the resources for RIAT Probe.
6. Click **Next**. In the Storage section, select the Storage Repositories (SRs) for keeping RIAT Probe.
   - To keep all the imported disk images for RIAT Probe on the same SR, click **Place all imported virtual disks on this target SR** and select a SR from the list.
   - To keep the disk images for RIAT Probe on different SRs, click **Place imported virtual disks onto specified target SRs**. Then, for each virtual disk, select the target SR from the list in the **SR** column.
7. Click **Next.**

   In the Networking section, specify the virtual network interface.
8. Click **Next.** In the Security section, select the **Verify Manifest Content** check box to specify the security settings.
9. Click **Next.** The OS Fixup Settings section appears. When RIAT Probe OVA file is built on a hypervisor other than XenServer, sometimes there could be compatibility issues when trying to deploy it on XenCenter.

   By selecting the **Use Operating System Fixup** check box, XenCenter ensures a basic level of interoperability for RIAT Probe OVA file that is being imported.
10. Click **Next.**

    In the Transfer VM Settings section, the network settings for RIAT Probe can be configured.
    - From the **Network Interface** list, select a network interface.
    - To configure the network settings (IP address, subnet mask, and gateway) for RIAT Probe, do one of the following:
      - To assign network settings automatically, select the **Automatically obtain network settings using DHCP** radio button.
      - To configure networking settings manually, click the **Use these network settings** button and enter the IP address, subnet mask and gateway.



11. Click **Next**. The configuration summary is displayed.

    Note: Keep the **Start VM(s) after import** check box selected to start RIAT Probe immediately after successful deployment.

12. Click **Finish**. RIAT Probe is deployed.
13. Proceed to the Configuring RIAT Probe Appliance section.

RIAT Probe XVA package deployment

1. Open the XenCenter application.
2. From the File menu, select **Import**.
3. Click **Browse** and select RIAT Probe XVA file.
4. Click **Next.** In the Home Server section, specify the server to nominate it as the home server for RIAT Probe.
5. Click **Next**. In the Storage section, select the Storage Repository (SR) for placing RIAT Probe.
6. Click **Import.** The XVA package gets imported and Networking section is displayed. In the Networking section, specify the Virtual Network Interface.
7. Click **Next**. The configuration summary is displayed.

   Note: Keep the **Start VM(s) after import** check box selected to start RIAT Probe immediately after successful deployment.

8. Click **Finish**. RIAT Probe is deployed.
9. Proceed to the Configuring RIAT Probe Appliance section.

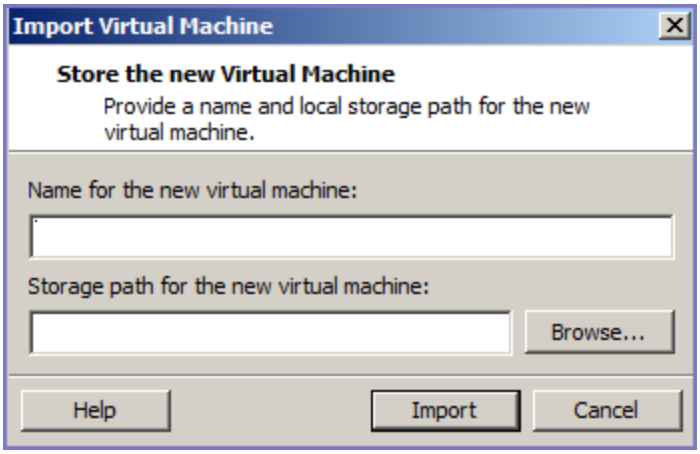
Appendix C: RIAT Probe deployment using VMware Player

The recommended RIAT Probe appliance file formats to deploy it using VMware Player are:

- VMware Player on Linux machine – RIAT Probe VMware Configuration (VMX) file.
- VMware Player on Windows machine – RIAT Probe Open Virtual Appliance (OVA) file.

The deployment process is similar for both RIAT Probe appliance file formats.

1. Open the VMware Player application.
2. From the File menu, select **Open a Virtual Machine**. The Open Virtual Machine window appears.
3. Navigate to RIAT Probe VMX/OVA file, select it and then click **Open**.
4. On Import Virtual Machine window, click **Import**.



5. Click **Play Virtual Machine** to start RIAT Probe.
6. Proceed to the Configuring RIAT Probe Appliance section.