Netsurion®
Powering Secure and Agile Networks

Quick Start Guide

EventTracker Security Center: Hyper-V VHD

Version: 9.3.8

Publication Date:

June 30, 2021

© Copyright Netsurion. All Rights Reserved.

Abstract

This document describes the steps to deploy EventTracker Virtual Hard Disk (VHD) on Hyper-V.

Audience

EventTracker administrators who want to deploy EventTracker VHD on Microsoft Hyper-V Manager.

This guide is intended for use by all EventTracker users responsible for investigating and managing network security. This guide assumes that you have EventTracker access and understanding of networking technologies.

© Copyright Netsurion. All Rights Reserved.

Table of Contents

© Copyright Netsurion. All Rights Reserved.

1. EventTracker Virtual Appliance in MS Hyper V Environment

1.1 Minimum Hardware Requirements

The minimum VM requirement to import EventTracker virtual appliance on VMware ESX/Esxi.

- **CPU** – 8 Core @2.5 GHz minimum
- **Memory** – 16 GB
- **VM Controller** – LSI Logic RAID
- **VM Hard Drive** – SCSI/SSD type
- **Disk** – 300 GB
- **Network Adapter** – 1

1.2 EventTracker VHD Details

- **EventTracker VHD file size** – 15.7 GB
- **Hostname** – ETConsole
- **WorkGroup** – EventTracker
- **Disk Space**: 300 GB (33 GB initial)
- **CPU** – 8 Core @2.5 GHz minimum
- **Memory** – 16 GB
- **IP Address** – Assign Static IP address
- **Operating System** – Windows server 2019 Standard Edition
- **Web Server** – IIS 11
- **Database Server** – Microsoft SQL Server 2017 Express Edition
- **EventTracker Version** – 9.3 Build 5 ETSC Collection Point
- **EventTracker Updates Applied** – ET93U20-2005, ET93U20-008, ET93U20-8009, ET93U21-043, ET93U21-044, ET93U21-046, ET93U21-047, ET93U21-048, ET93U21-049, ET93U21-050, ET93U21-051, ET93U21-052, ET93U21-053

1.3 Prerequisites

- EventTracker customer must have a license key for Microsoft Windows 2019 Standard edition.
- The 30-days grace period is not available In Microsoft Windows Server 2019. If the operating system is not activated, watermark appears showing the Windows edition (although it does not show to

© Copyright Netsurion. All Rights Reserved.

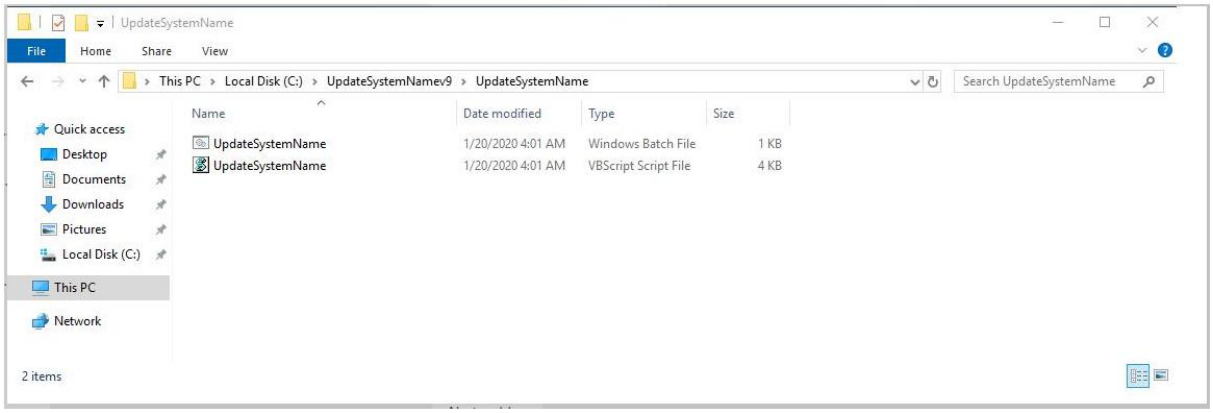
activate) On the desktop, personalization features in PC Settings like changing the lock screen is disabled. Entire screen notification appears periodically. However, the operating system continues to function normally.

- User must provide a product key and activate.

1.3.1 Summary

1. Download the VHD file from the link provided by the EventTracker technical support.
2. Get the EventTracker license from the EventTracker technical support.
3. Create VM using the downloaded VHD.
4. Login as ETAdmin,

- Change the Computer name, connect it to the domain if the active directory authentication is required, else leave it as it is for local account authentication and restart the Virtual Machine.
- Run the downloaded batch file UpdateSystemName.bat in the command prompt available in the C:\UpdateSystemName\directory.



5. Update the credentials in the EventTracker.
6. Change **startup** to **Automatic** for following EventTracker Services and start the following services.

- EventTracker Agent
- EventTracker Alerter
- EventTracker EventVault
- EventTracker Indexer
- EventTracker Receiver
- EventTracker Remoting
- EventTracker Reporter

© Copyright Netsurion. All Rights Reserved.

- EventTracker Scheduler
- Elasticsearch 7.2.1 (elasticsearch-service-x64)
- EventTracker Elasticsearch Indexer
- EventTracker Monitoring Daemon
- WCW Service
- Traptracker Receiver

7. Install EventTracker license using **EventTracker License Manager**.
8. Run Microsoft Windows updates to install the latest windows updates and security patches.
9. Install the latest EventTracker updates.
10. Start **EventTracker Evaluation**.

NOTE:

- Microsoft Windows OS will continue to run the 30 days trial without activation. To continue using you need to activate Microsoft Windows using a valid license key.
- No antivirus software is installed by default. It is recommended to install antivirus software.

2. EventTracker Virtual Appliance in Hyper-V Manager Environment

Deploying and configuring EventTracker Virtual Hard Disk (VHD) on Hyper-V.

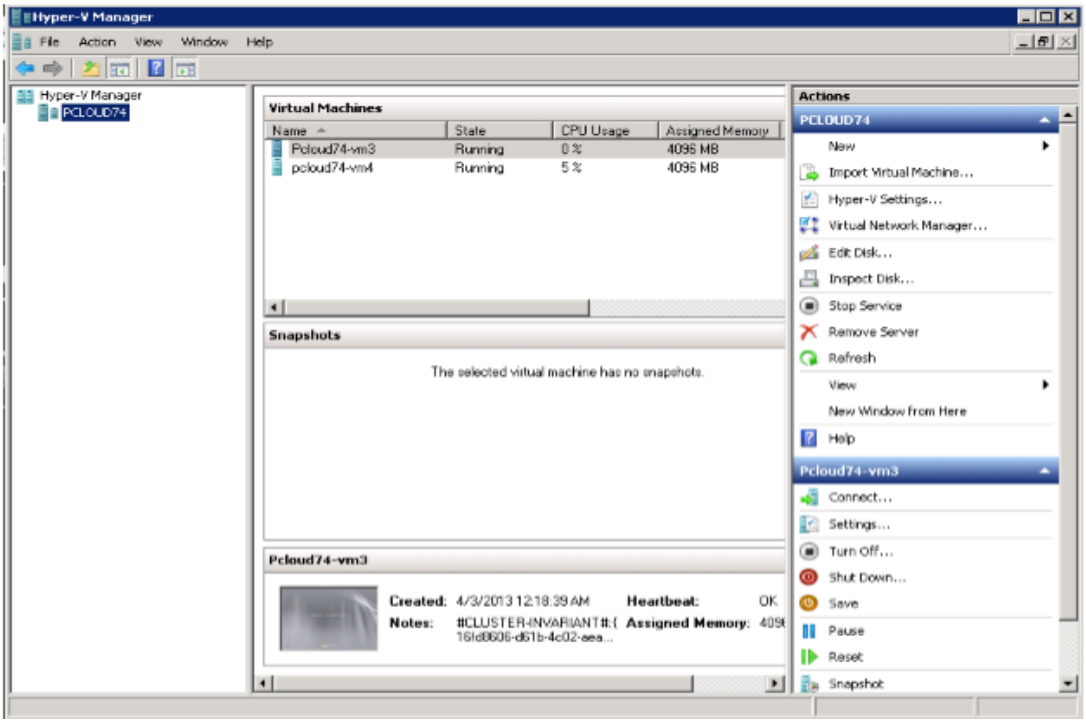
2.1 Deploying Event Tracker on Hyper-V Manager

To login to Hyper-V manager

1. Click **Start** and select **All Programs**.
2. Select **Administrative Tools** and select **Hyper-V Manager**.

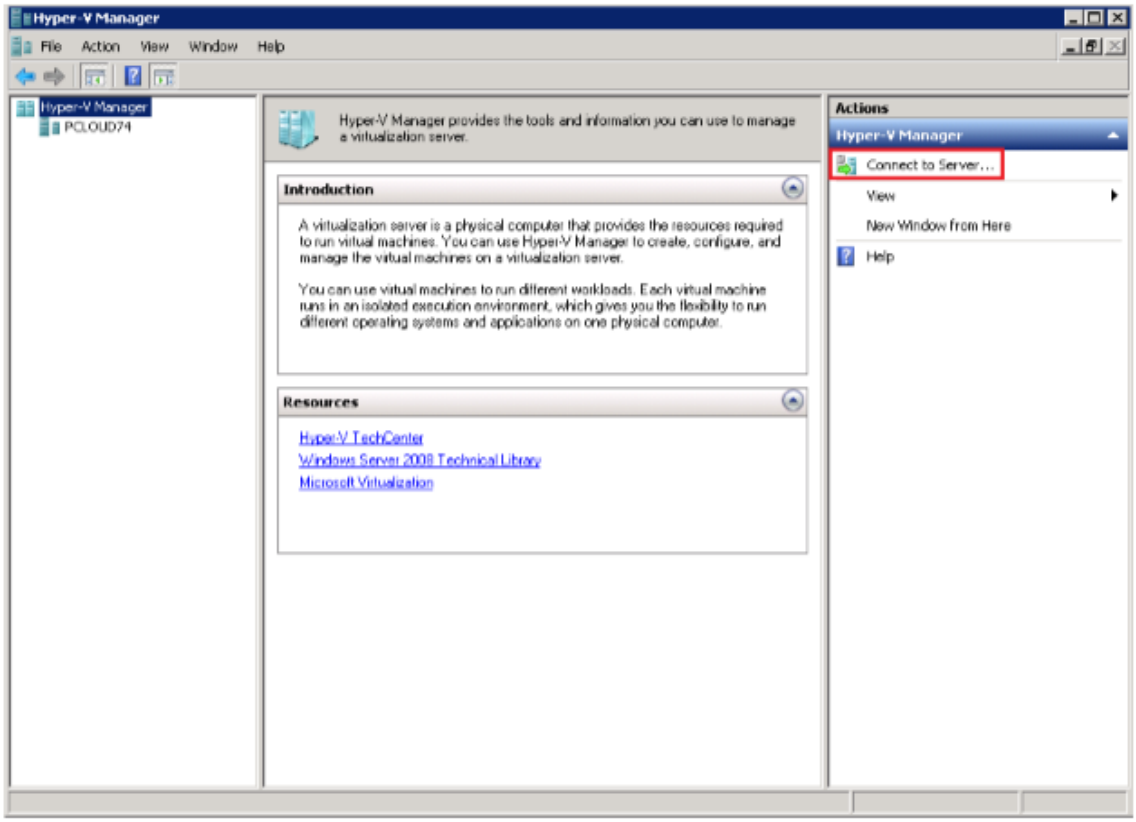
Hyper-V Manager Console opens.

© Copyright Netsurion. All Rights Reserved.



3. Select **Hyper-V Manager** node.

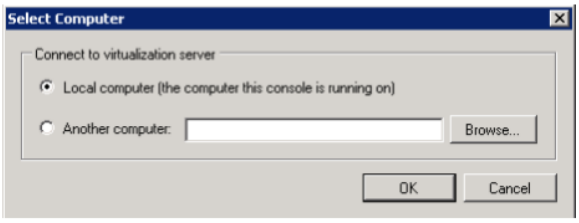
4. In **Actions** pane, select **Connect to Server**.



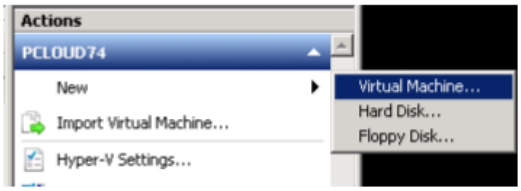
© Copyright Netsurion. All Rights Reserved.

Select Computer window opens.

5. Choose the option **Local Computer (the computer this console is running on)** or **Another computer** as required and Click **OK**.

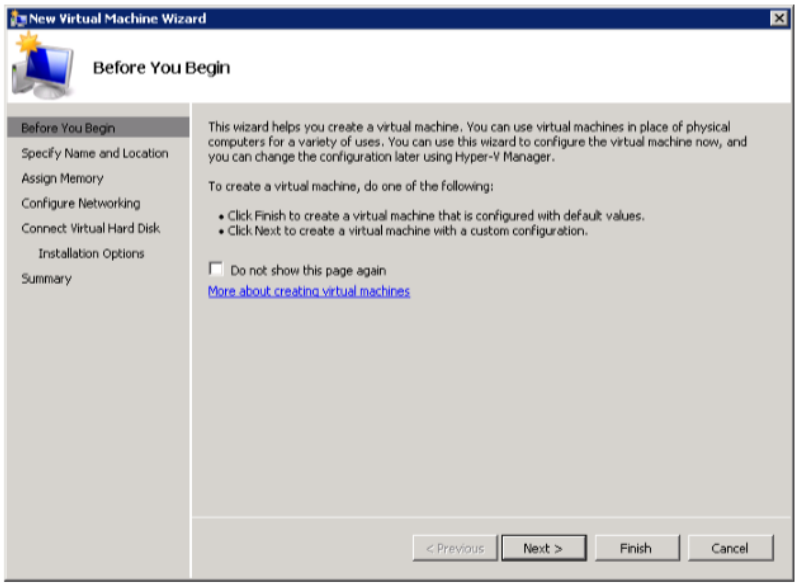


6. In **Actions** pane, point to **New** and select **Virtual Machine.**



New Virtual Machine Wizard opens.

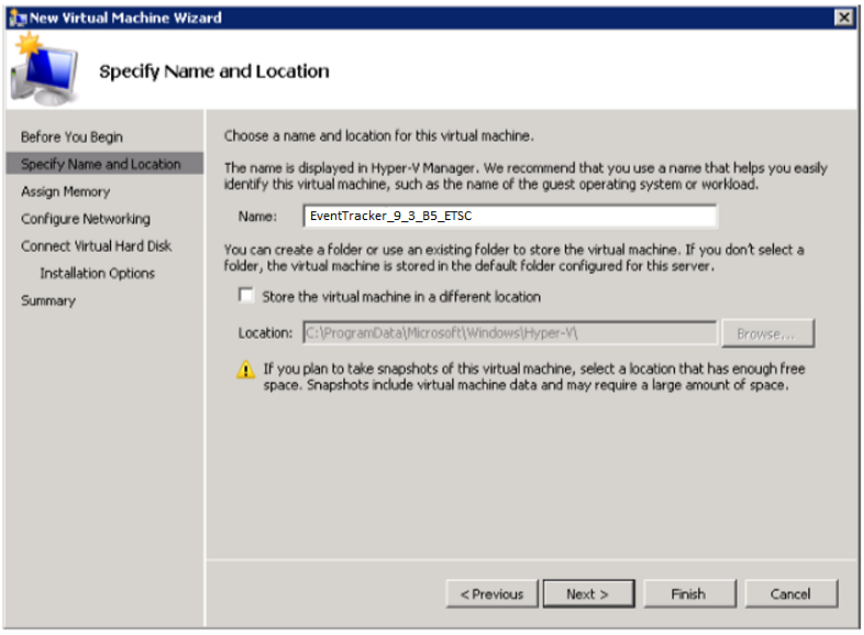
7. Click **Next >**.



Specify Name and Location page displays.

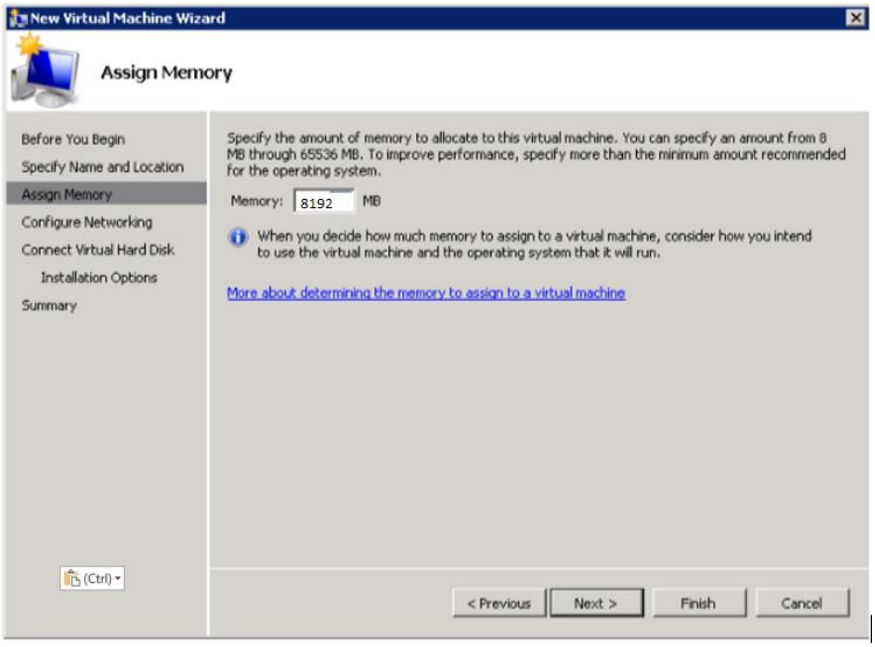
8. Enter a name for the virtual machine in the **Name** field. Click **Next** >.

© Copyright Netsurion. All Rights Reserved.



Assign Memory page displays.

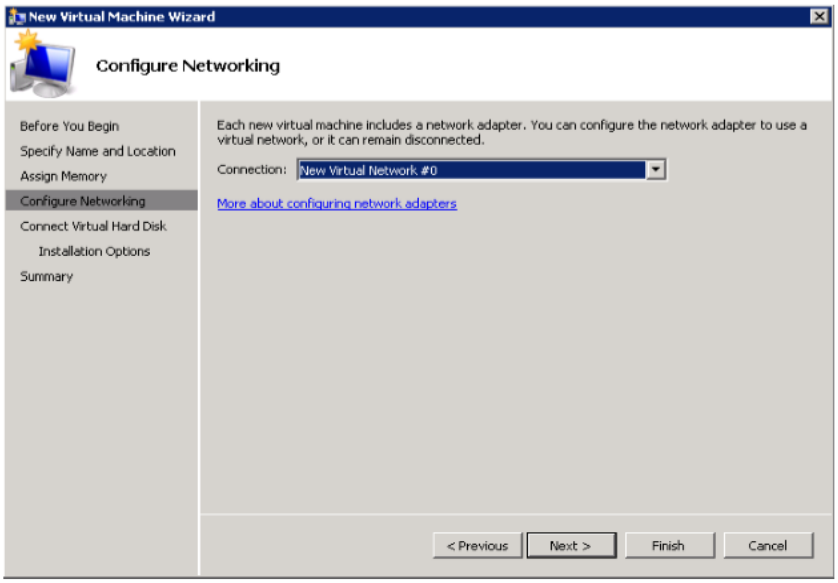
9. Specify the Memory size. Click **Next >**.



Configure Networking page displays.

10. Configure the network adapter, click **Connection** drop-down and select the LAN Card for this virtual machine. Click **Next** >.

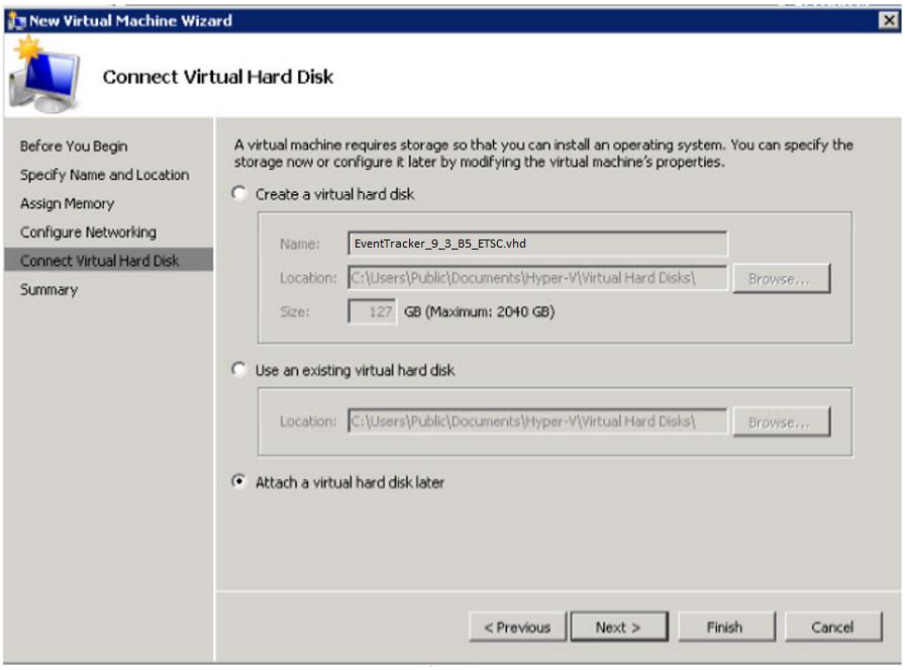
© Copyright Netsurion. All Rights Reserved.



Connect Virtual Hard Disk (VHD) page displays.

You can create / select an existing / attach a VHD later as required.
In our example, we are enabling the option **Attach a VHD later**.

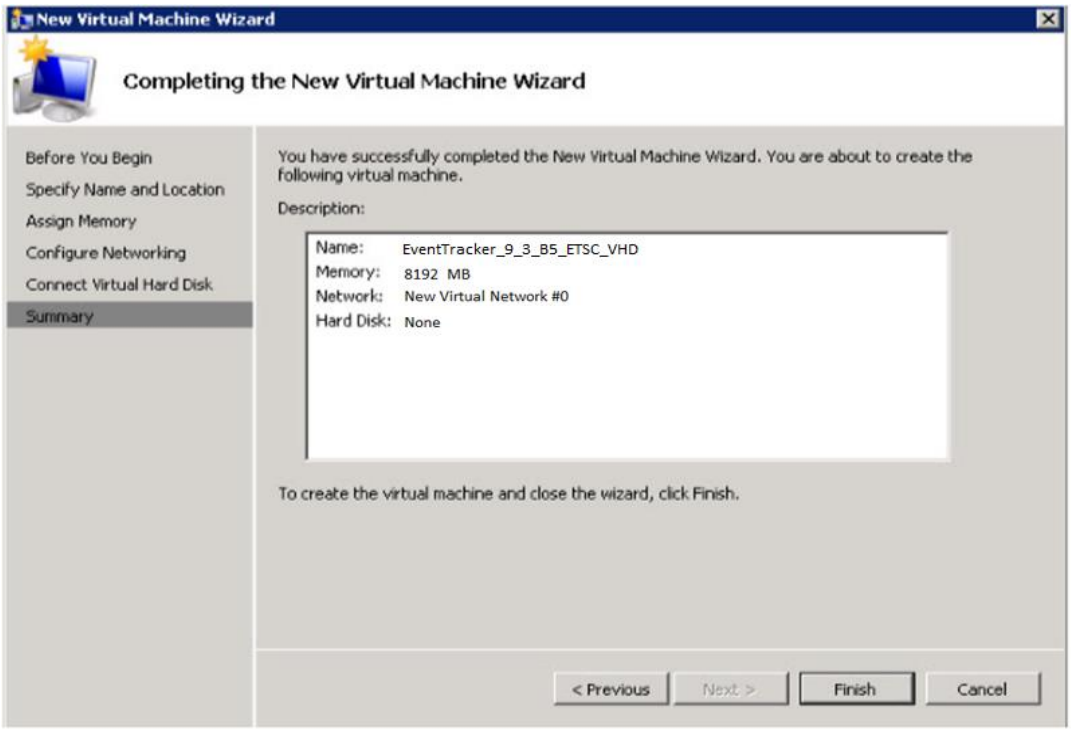
11. Select **Attach a virtual hard disk (VHD) later** option and click **Next >**.



Completing the New Virtual Machine Wizard opens.

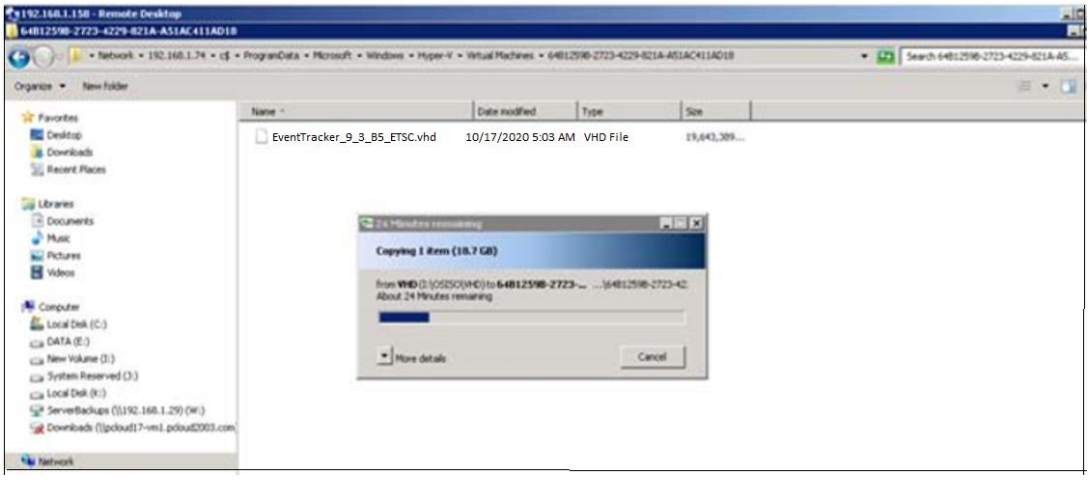
12. Click **Finish**.

© Copyright Netsurion. All Rights Reserved.



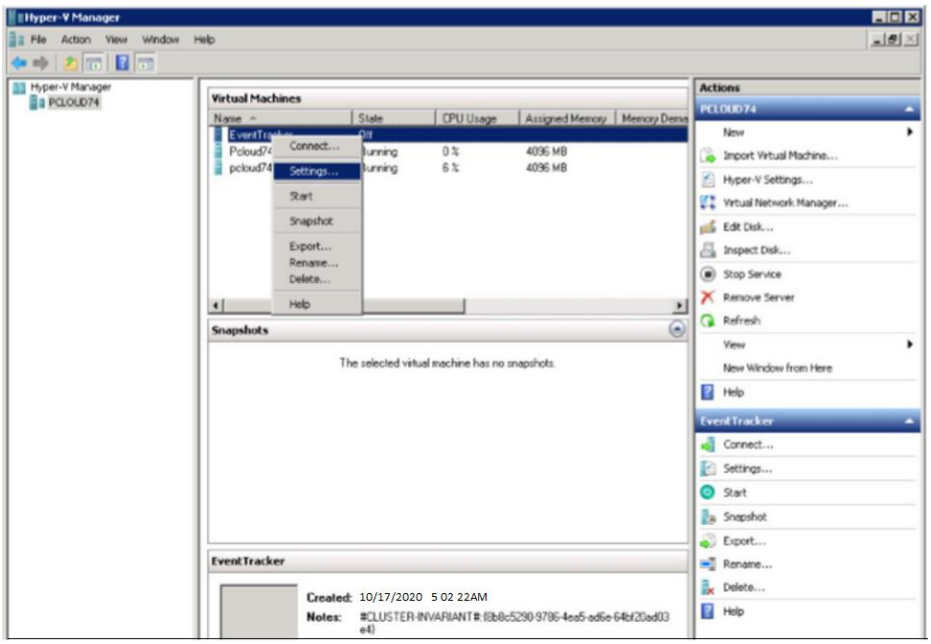
13. Download and extract the .**vhd** file.

NOTE: Please contact the Support team to retrieve the VHD file. Place this file in the location where Hyper-V is installed.

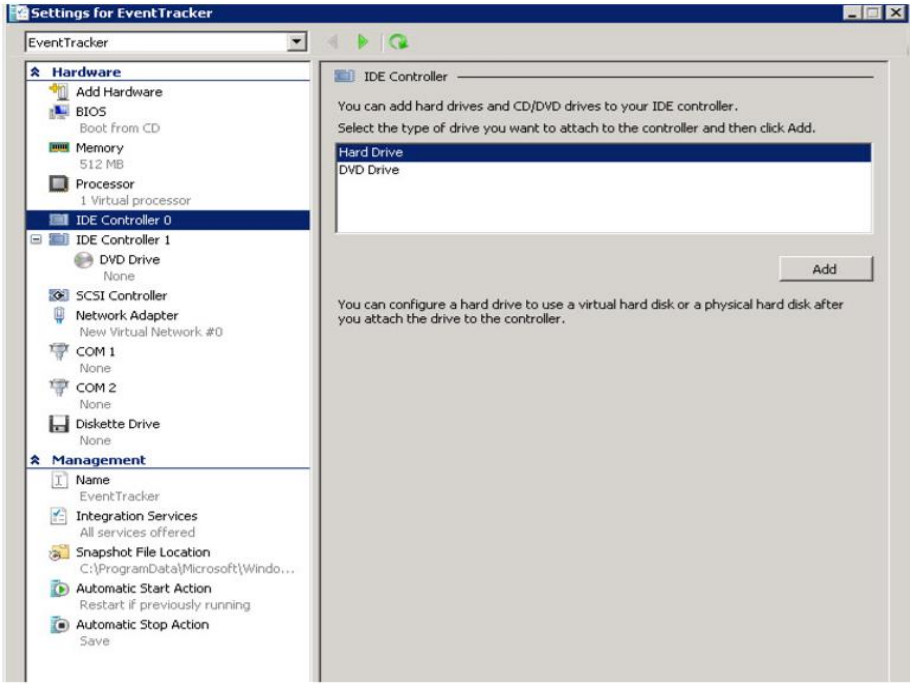


14. In Virtual Machines pane, select and right-click the required Virtual Machine and click **Settings**.

© Copyright Netsurion. All Rights Reserved.

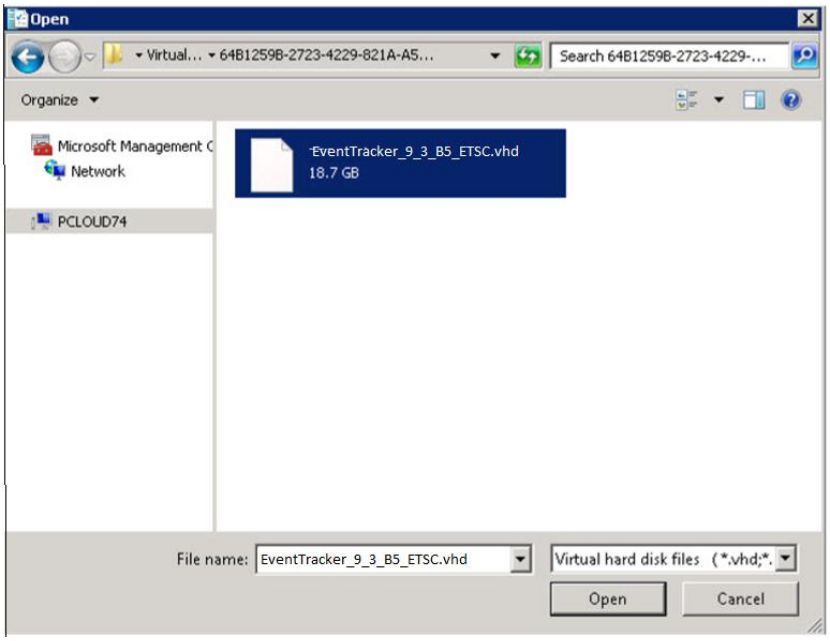


Settings for EventTracker window opens.

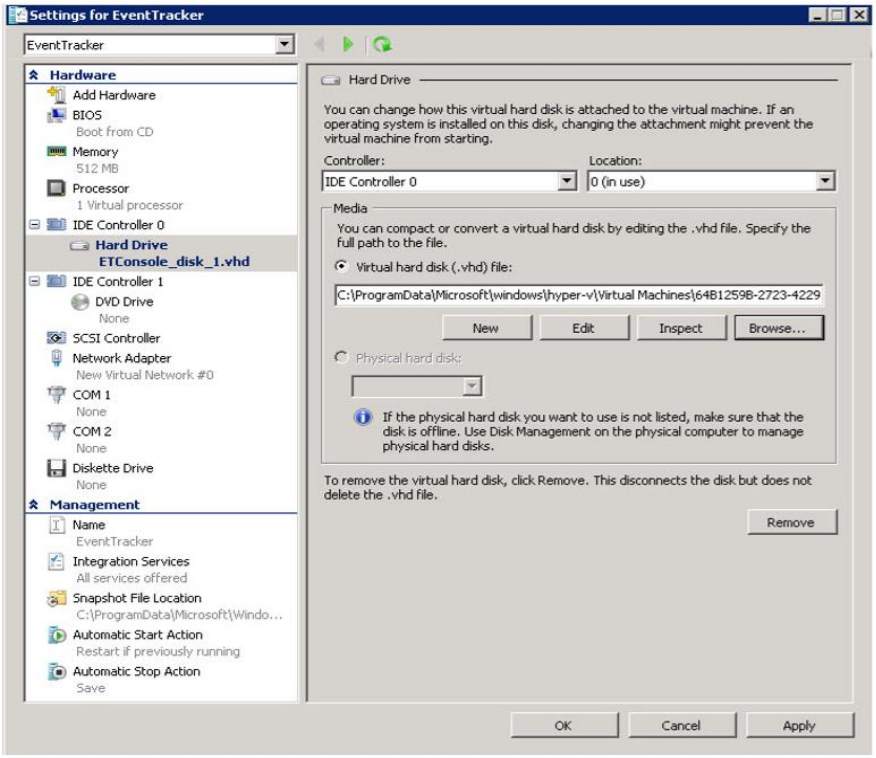


15. Click **Add** and browse the location of the VHD file.

© Copyright Netsurion. All Rights Reserved.

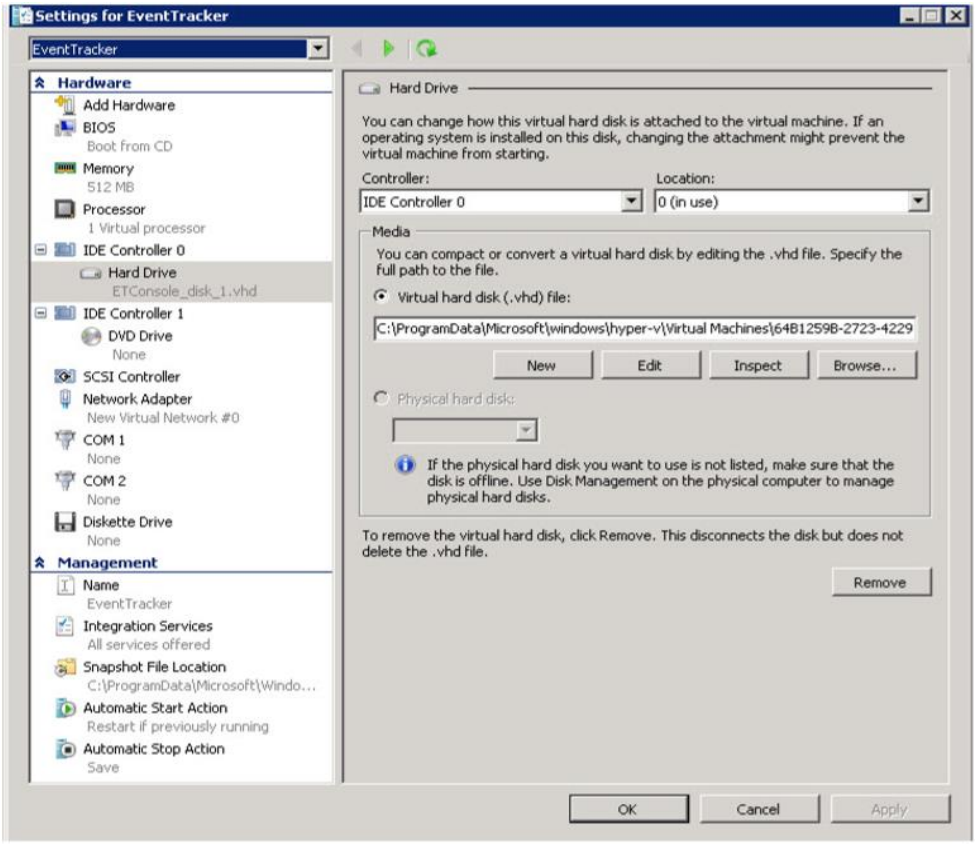


16. Select the Virtual Hard Disk file and click **Apply** and **OK**.

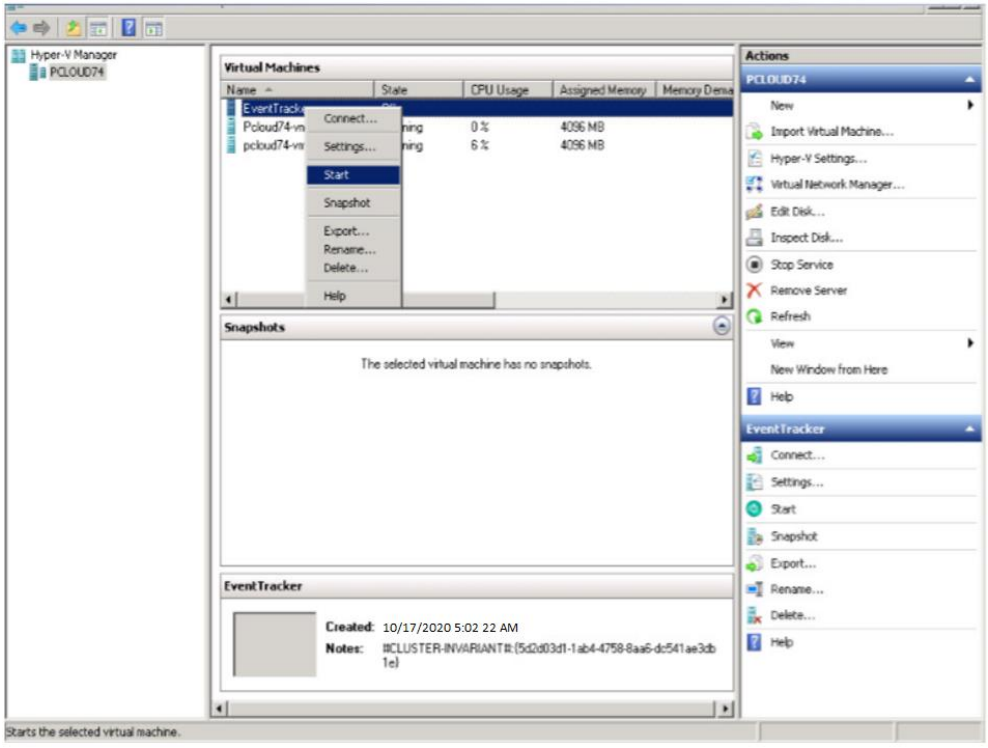


Settings for EventTracker window opens.

© Copyright Netsurion. All Rights Reserved.



17. In Virtual Machines pane, right-click the required Virtual Machine and Click **Start**.



© Copyright Netsurion. All Rights Reserved.

2.2 Configuring EventTracker Virtual Appliance on Hyper-V Manager

After EventTracker Virtual appliance is deployed successfully, make few configuration changes as below:

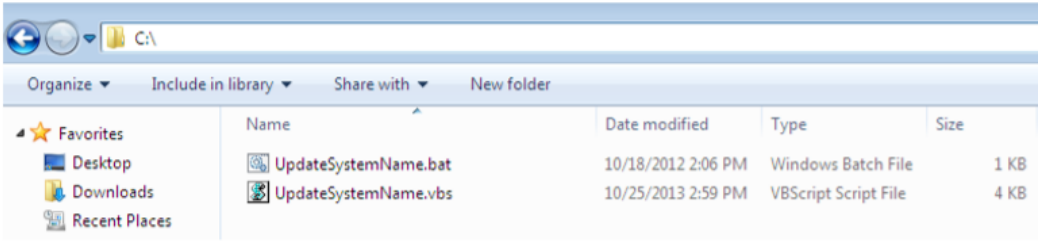
1. Power on the EventTracker Virtual machine.
2. Log in to 'EventTracker Virtual' system as EventTracker administrator using below credential.

   • Username: ETConsole\ETAdmin

   • Password: Welc0me$129#

NOTE: On first successful logon you will be prompted to change the ETAdmin user password. Change it to a secure password.

3. Change the Computer name, join it to Domain if active directory authentication is required or leave it for local account authentication and restart the Virtual machine.
4. Download the Update System Name zip file and extract this file in the C:\ drive.

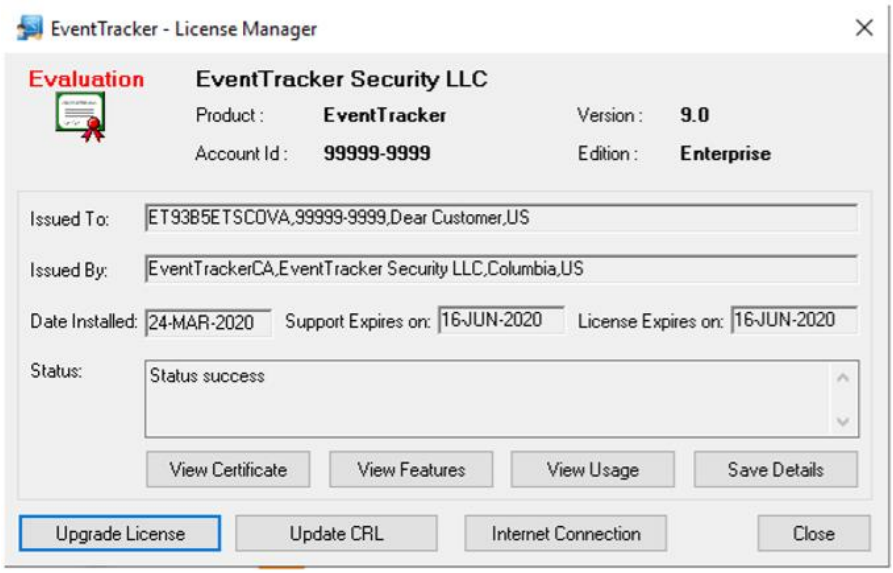


5. Right click on **UpdateSystemName.bat available** in C:\ and click **Run as Administrator**.
6. To update ETAdmin user credentials in EventTracker, click **Start**, select **Programs**, and select **Prism Microsystems**.
7. Select **EventTracker** and select **EventTracker Configuration**.
   Update the user credential ETAdmin user or select active directory and enter domain user credential.

© Copyright Netsurion. All Rights Reserved.

8. After **EventTracker Configuration** validates the credential and runs successfully, install **VMware Tools** on the newly imported Virtual machine.
9. Change **Start up type to Automatic** for following **EventTracker Services** and **start** the following services.
   - EventTracker Agent
   - EventTracker Alerter
   - EventTracker Elasticsearch Indexer
   - EventTracker EventVault
   - EventTracker Indexer
   - EventTracker Monitoring Daemon
   - EventTracker Receiver
   - EventTracker Remoting
   - EventTracker Reporter
   - EventTracker Scheduler
   - Elasticsearch 7.2.1 (elasticsearch-service-x64)
   - EventTracker Elasticsearch Indexer
   - EventTracker Monitoring Daemon
   - WCW Service
   - Traptracker Receiver
10. Open **License Manager** from **EventTracker Control Panel** and click the **Upgrade License** button to upgrade the License.

© Copyright Netsurion. All Rights Reserved.



11. After successful license installation, login to **EventTracker Web** using ETConsole\ETAdmin user credentials in the web browser.

© Copyright Netsurion. All Rights Reserved.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.
Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

713-929-0200

https://www.netsurion.com/company/contact-us

© Copyright Netsurion. All Rights Reserved.