

**Quick Start Guide** 

## **EventTracker Security Center: Hyper-V VHD**

Version: 9.3.8

**Publication Date:** 

June 30, 2021



## 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.

## Table of Contents

Table of Contents	3
1. EventTracker Virtual Appliance in MS Hyper V Environment	4
1.1 Minimum Hardware Requirements	4
1.2 EventTracker VHD Details	4
1.3 Prerequisites	4
1.3.1 Summary	5
2. EventTracker Virtual Appliance in Hyper-V Manager Environment	6
2.1 Deploying Event Tracker on Hyper-V Manager	6
2.2 Configuring EventTracker Virtual Appliance on Hyper-V Manager	15
About Netsurion	18
Contact Us	18



## 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



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.

-> · ↑ 📙 :	> Th	is PC → Local Disk (C:) → UpdateSyste	mNamev9 > UpdateSystemNan	ne			5 V	Search UpdateSystemName	P
Quick access Desktop Documents Downloads Pictures Local Disk (C:)	* * * * *	Name	Date modified 1/20/2020 4:01 AM 1/20/2020 4:01 AM	Type Windows Batch File VBScript Script File	Size	1 KB 4 KB			
This PC									

- 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



- 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.

≣EHyper-¥ Manager					
E File Action View Window	Help				X
🗢 🔿 🖄 🗰 📓 💷					
Hyper-V Manager	Wintered Marshimma				Actions
PCLOUD74	Name e	State	CRILLIaana	Assigned Memory	PCLOUD74
	Poloud74-vm3	Bunning	0%	4095 MB	New
	pcloud74-vm4	Bunning	5%	4096 MB	强 Import Virtual Machine
					Phyper-V Settings
					👯 Virtual Network Manager
					🔬 Edit Disk
					E Inspect Disk
	•				Stop Service
	Spapshots				X Ramove Server
					G Refresh
	. · · ·	The selected virtue	al machine has no s	napehote.	View
					New Window from Here
					12 Halo
					Pcloud74-vm3
					Connect
					Settings
	Pcloud74-ym3				Turn Off
					Ø Shut Down
	Create	d: 4/3/2013 12:1	18:39 AM He	artbeat: OK	( Save
	Notes:	#CLUSTER-IN 16Hd8606-d61	WARIANT#:{ Ass b-4c02-aca	signed Memory: 4096	Pause
					I▶ Reset
	•				🛃 Snapshot

- 3. Select Hyper-V Manager node.
- 4. In Actions pane, select Connect to Server.



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.

Select Computer		×
Connect to virtualization s	erver computer this console is running on)	
Another computer:	DK Cancel	

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

Actions	
PCLOUD74	▲ ▲
New	Virtual Machine
🕞 Import Virtual Machine	Hard Disk Floppy Disk
Hyper-V Settings	

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 >.



#### Assign Memory page displays.

9. Specify the Memory size. Click Next >.

New Virtual Machine Wiz     Assign Mem	ard 🛛
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 65556 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Memory: 8192 MB When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run. More about determining the memory to assign to a virtual machine
(Ctrl) •	< <previous next=""> Finish Cancel</previous>

#### Configure Networking page displays.

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



🎦 New Virtual Machine Wiza	rd 🛛
Configure N	etworking
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual network, or it can remain disconnected. Connection: Vew Virtual Network #0  More about configuring network adapters
	< Previous Next > Finish Cancel

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 >.

Before You Begin Specify Name and Location Assign Memory	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.
Configure Networking Connect Virtual Hard Disk Summary	Name:         EventTracker_9_3_B5_ETSC.vhd           Location:         C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\         Browse           Size:         127         GB (Maximum: 2040 GB)
	Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Browse  Attach a virtual hard disk later

Completing the New Virtual Machine Wizard opens.

12. Click Finish.



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.

192.168.1.158 - Remote Desktop 64012598-2723-4229-821A-ASIAC411AD18					
🚱 🕞 📕 + Network + 192.160.1.74 + c\$ +	ProgramCata • Microsoft • Windows • Hyper	-V + Virtual Machines. + 64	11.25/10-2723-4229-82	14-451AC411A018	• 💭 Search 64812596-2723-4229-8218-45
Organize • New folder					# • 🖬
	Name - EventTracker_9_3_B5_ETSC.vhd Copying 1 Rec from VHD (B)(0) About 24 More data	Date modified 10/17/2020 5:03 - 10/17/2020 5:03 - 10/17/200 5:03 - 10/17/200 5:05 - 10/17/200 5:05 - 10/17/200 5:05 - 10	AM VHD File	500 19,443,309 5722-42 coli	
Network					

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

Hyper-V Manager							
File Action View Window H	Help						_ <b>8</b> ×
Hyper-V Manager	Victual Markines				_	Actions	
PCLOUD74	Virtual Hachines					PCLOUD74	-
	Com     Poloug7/     Ren     Ren     Delet     t     Poloug7     Ren     Poloug7     Poloug7/     Snapshots	1 5000 000000000000000000000000000000000	0% 6%	4096 MB 4096 MB		Nov Import Vrtual Machine Hyper-V Settings Vrtual Network Manager Mit Ed Disk Stop Service X Remove Server Refresh	•
		The selected vit	View New Window from Here Help	,			
			EventTracker	-			
			Settings				
						3 Start	
						a Snapshot	
			Export				
	EventTracker					Rename	
		lotes: #CLUSTER e4}	0 5 02 22AM	:5290-9786- <b>4</b> ea5-ad6e	64bf20ad03	Br Delete	

Settings for EventTracker window opens.

EventTracker	4 1 9
Hardware     Add Hardware     Boot from CD     Memory     S12 MB     Processor     1 Virbual processor	IDE Controller           You can add hard drives and CD/DVD drives to your IDE controller.           Select the type of drive you want to attach to the controller and then click Add.           Hard Drive           DVD Drive
	Add You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.
Name     EventTracker     EventTracker     Integration Services     All services offered     Snapshot File Location     C:\ProgramData\Microsoft\Windo     Automatic Start Action     Restart if previously running     Automatic Stop Action     Save	

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

🚰 Open				×
	- 😰	Search 64B1259B-272	3-4229	-
Organize 🔻			•	0
Microsoft Management C Wetwork  EventTracker_9_3_B5_E  18.7 GB	TSC.vhd			
PCLOUD74				
File name: EventTracker_9_3_B5_ETSC.vhd	•	Virtual hard disk files	(*.vhd;*.	•
		Open	Cancel	

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

ventTracker				
t Hardware Add Hardware BtOS Boot from CD Memory 512 MB	You can change how this virt operating system is installed virtual machine from starting Controller:	ual hard disk is a on this disk, cha	attached to the virtual r anging the attachment r Location:	nachine. If an night prevent the
Processor I Virtual processor I Virtual processor IDE Controller 0 Hard Drive ETConsole disk 1.vhd	Media You can compact or conver full path to the file.	t a virtual hard	disk by editing the .vhc	file. Specify the
DVD Drive None     None     SCSI Controller     Network Adapter     New Virtual Network #0     COM 1     None     COM 2     None     Diskette Drive     None     Diskette Drive     None	ProgramData/Microsoft      Ne     Physical hard disk      To remove the virtual hard disk      To remove the virtual hard disk	windows\hyper	vivirtual Machines(64E     dit Inspect     to use is not listed, maint on the physical comp e. This disconnects the	Browse Browse Re sure that the uter to manage disk but does not
				Remove

#### Settings for EventTracker window opens.

_						
	ardware Add Hardware BOS Boot from CD Memory 512 MB	You can change how this vi operating system is installed virtual machine from startin Controller:	tual hard o I on this di g.	disk is a sk, cha	attached to the virtual m nging the attachment mi Location:	achine. If an ght prevent the
	Processor	IDE Controller 0		-	0 (in use)	-
-	1 Virtual processor	Media				
31	IDE Controller 0	You can compact or conv	ert a virtua	al hard	disk by editing the .vhd I	file. Specify the
	ETConsole_disk_1.vhd	full path to the file.				
301	IDE Controller 1	• virtual hard disk (.vhd	) nie:			
	DVD Drive	C:\ProgramData\Microsof	t'(windows'	\hyper	-v\Virtual Machines\64B1	259B-2723-4229
	None	N		E	det Tospect	Browse
٠	SCSI Controller				and inspect	
Q	Network Adapter	C Physical hard disk:				
-	New Virtual Network #0	v				
11	COM 1					
100	COM 2	If the physical had disk is offline. Use	nd disk you Disk Many	want	to use is not listed, make at on the physical compu	e sure that the
14	None	physical hard disk	s.	Jone	it off the privated compo	cor co manago
-	Diskette Drive					
-	None	To remove the virtual hard	disk, click R	temove	<ol> <li>This disconnects the di</li> </ol>	isk but does not
M	anagement	delete the tyrid filet				
I	Name EventTracker					Remove
	Integration Services					
2	All services offered					
1	All services offered Snapshot File Location C:\ProgramData\Microsoft\Windo					
	All services offered Snapshot File Location C:\ProgramData\Microsoft\Windo Automatic Start Action Restart if previously running					

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

Virtual	Machines					Actions
Name -	-	State	CPU Usage	Assigned Memory	Memory Dema	PCLOUD74
E ver Polo polo	ttrask ud74-vn Connect ud74-vn Settings. Start Snapsho Export Decome	ning ning t	0% 6%	4096 MB 4096 MB		New  Import Virtual Machine  Hyper-V Settings  Kitual Network Manage Kitual Network
4 Snapsh	Help				-	Stop Service     Remove Server     Refresh     View
						Heb EventTracker
						Gonnect
						Settings
						Start
						🛃 Snapshot
EventTr	acker					<ul> <li>Export</li> <li>Rename</li> </ul>
	Creater	# 10/17/202	0 5:02 22 AM	03d1-1ab4-4758-8aa6	dc541ae3db	Ex Delete



### 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 <u>Update System Name</u> zip file and extract this file in the C:\ drive.



- 5. Right click on UpdateSystemName.bat available in C:\ and click Run as Administrator.
- 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.

Vetsurion	EventTracker*	
ACTORIO III	LVCITTIGORCI	
User Credentials		User Authentication
User Name	ETAdmin	O Local Account
Password	*********	O Antina Directory
T dooword		Active Directory
		Database Authentication
EventTracker Group	EventTracker	Enable
		OK Cancel
Vote:		



- 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.

Evaluation	eventTra	cker Security LLC		
	Product : Account Id :	EventTracker 99999-9999	Version : Edition :	9.0 Enterprise
Issued To:	ET93B5ETSCOVA,	99999-9999,Dear Customer,L	JS	
Issued By:	EventTrackerCA,Ev	ventTracker Security LLC,Col	umbia,US	
Issued By: Date Installed:	EventTrackerCA,Ev	ventTracker Security LLC,Col upport Expires on: 16JUN-2	umbia,US 020 License Ex	pires on: 16JUN-2020
issued By: Date Installed: Status:	EventTrackerCA,Ev  24-MAR-2020 S  Status success	ventTracker Security LLC,Col upport Expires on: 16JUN-2	umbia,US 020 License Ex	pires on: 16JUN-2020
Issued By: Date Installed Status:	EventTrackerCA,Ev  24-MAR-2020 S  Status success  View Certificate	ventTracker Security LLC,Col upport Expires on: 16JUN-2 View Features	umbia,US 020 License Ex View Usage	pires on: 16JUN-202 Save Details

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



### **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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

### **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