EventTracker

Actionable Security Intelligence

Integrate Rapid7 InsightVM

EventTracker v8.x and above

Publication Date: September 5, 2018

Abstract

This guide provides instructions to integrate Rapid7 InsightVM with EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and Rapid7 InsightVM.

Audience

IT Admins, Rapid7 InsightVM administrators and EventTracker users who wish to integrate Rapid7 InsightVM with EventTracker.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Table of Contents

Overview

The Rapid7 Insight platform brings together Rapid7's library of vulnerability research, exploit knowledge, global attacker behavior, Internet-wide scanning data, exposure analytics, and real-time reporting to provide a fully available, scalable, and efficient way to collect your vulnerability data and turn it into answers. InsightVM leverages this platform for live vulnerability and endpoint analytics.

EventTracker consumes the Qualys formatted XML reports and provides vulnerability scores based on the scans performed. EventTracker will also download the reports configured in InsightVM and display them in report dashboard.

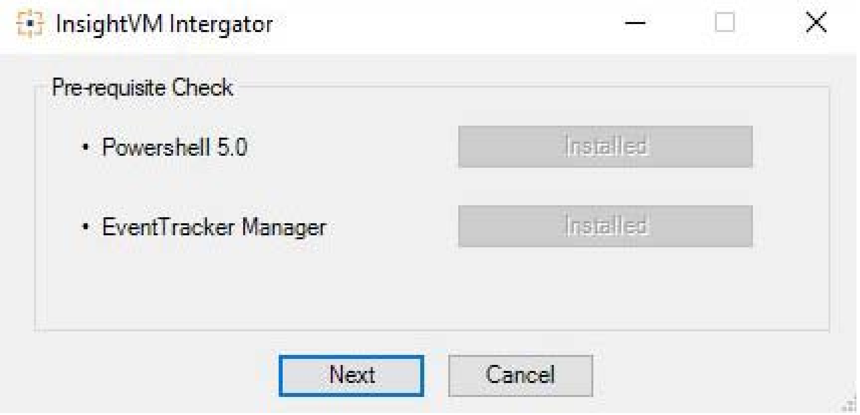
Prerequisites

- EventTracker v8.x or above should be installed.
- PowerShell v5 should be installed.
- Rapid7 InsightVM must be installed.
- Local account with administrative privilege.

Integrate Rapid7 InsightVM with EventTracker

NOTE: If you haven't configured any pdf reports, please following the instructions in the link and create the reports based on your preferences. Select **PDF format** and under frequency select **Run a recurring report** after every scan.

- Go to this link , download and install the latest Knowledge Pack updates.
- Go to the following path **<EventTracker Install Path>\Prism Microsystems\EventTracker\Knowledge Packs\Rapid7 InsightVM.**
- Run the **Integrator InsightVM.bat** file as **Admin**.
- A pre-requisite check for EventTracker Manger and PowerShell version is performed.

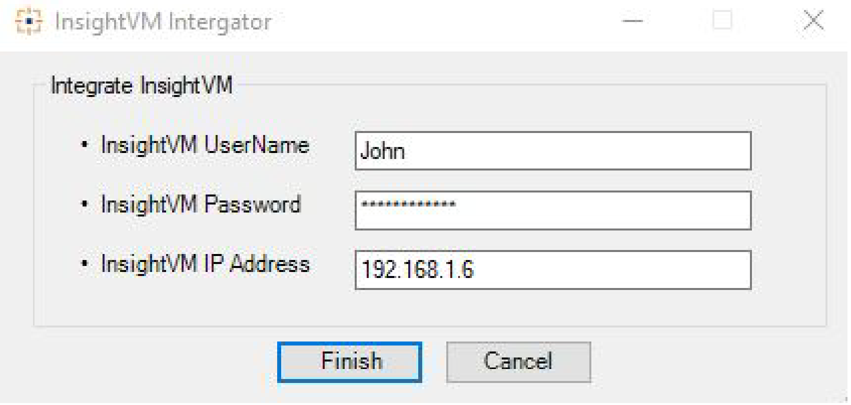


Pre-requisite Check

- Powershell 5.0 — Installed
- EventTracker Manager — Installed

Figure 1

- If all the pre-requisites are met, click **Next**.

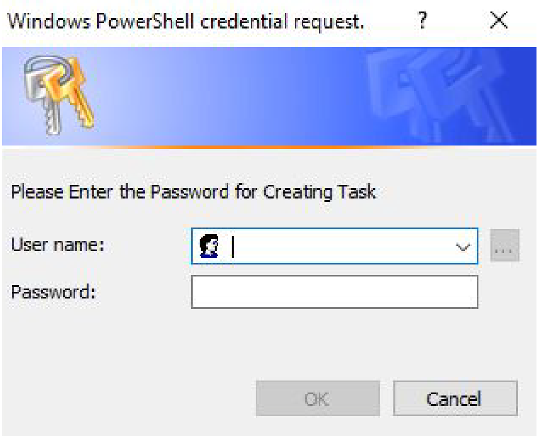


Integrate InsightVM

- InsightVM UserName: John
- InsightVM Password: *************
- InsightVM IP Address: 192.168.1.6

Figure 2

- Enter the Rapid7 InsightVM **Username, Password and the IP address** of the host on which the Rapid7 InsightVM is installed and click **Finish**.
- Enter the local admin credentials to create and schedule a task.



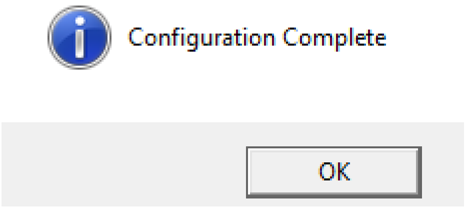
Please Enter the Password for Creating Task

User name:

Password:

Figure 3

- You will get a successful configuration message once the integration is successful.



Configuration Complete

Figure 4

Verifying the Integration

Verifying the Direct Log Archiver

- Logon to EventTracker Manager.
- Under the **Admin** drop-down, select **Manager**.

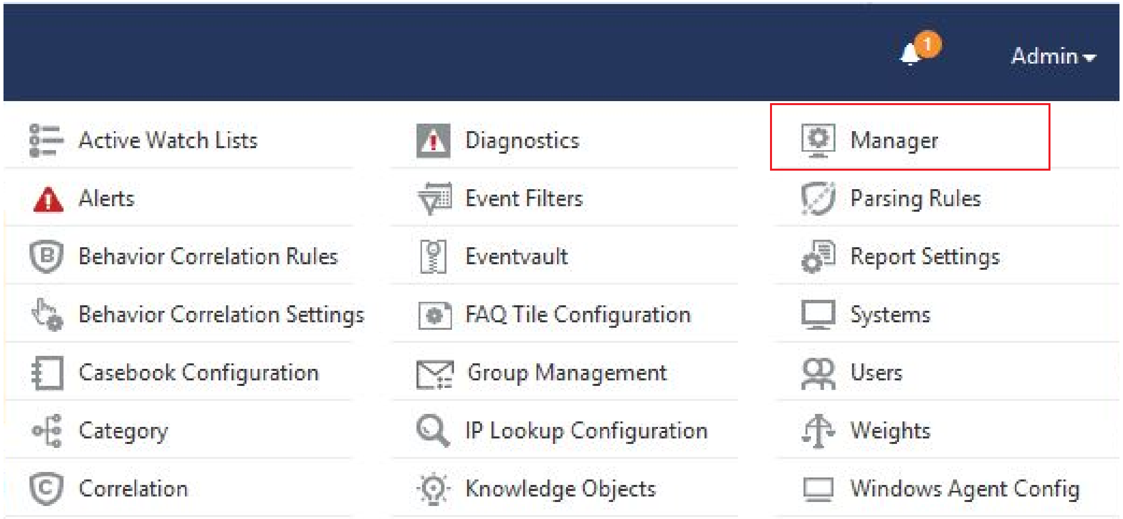
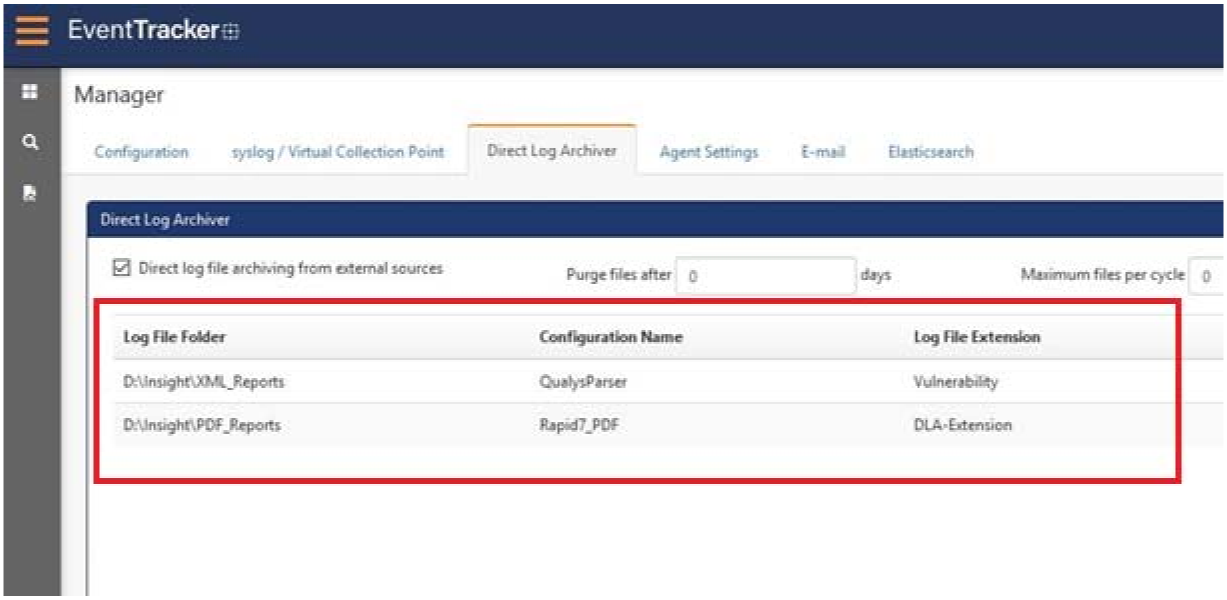


Figure 5

- Select the **Direct Log Archiver** tab and verify for the below shown configurations.



Direct Log Archiver

☑ Direct log file archiving from external sources

Purge files after 0 days

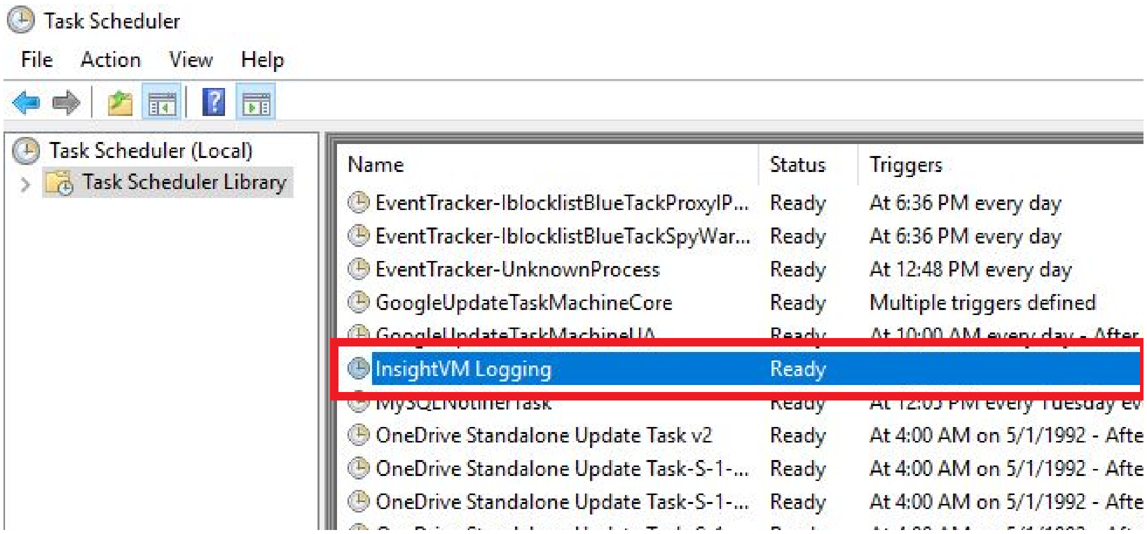
Maximum files per cycle 0

Log File Folder	Configuration Name	Log File Extension
D:\Insight\XML_Reports	QualysParser	Vulnerability
D:\Insight\PDF_Reports	Rapid7_PDF	DLA-Extension

Figure 6

Verify Task Scheduler

- Open the **Task Scheduler** on the **EventTracker Manager workstation**.
- Select the **Task Scheduler Library** in the left-hand side and verify for a task named **InsightVM logging**.



Name	Status	Triggers
EventTracker-IblocklistBlueTackProxyIP...	Ready	At 6:36 PM every day
EventTracker-IblocklistBlueTackSpyWar...	Ready	At 6:36 PM every day
EventTracker-UnknownProcess	Ready	At 12:48 PM every day
GoogleUpdateTaskMachineCore	Ready	Multiple triggers defined
GoogleUpdateTaskMachineUA	Ready	At 10:00 AM every day - After
InsightVM Logging	Ready	
MySQLNotifierTask	Ready	At 12:05 PM every Tuesday ev
OneDrive Standalone Update Task v2	Ready	At 4:00 AM on 5/1/1992 - Afte
OneDrive Standalone Update Task-S-1-...	Ready	At 4:00 AM on 5/1/1992 - Afte
OneDrive Standalone Update Task-S-1-...	Ready	At 4:00 AM on 5/1/1992 - Afte

Figure 7