Configuration Guide

Snare E3 QRadar

Document History

Version	Date	Author	Description
1.0	28 Apr 2021	Rhys Thornton	1st issue
2.0	03/09/2021	Rhys Thornton	Updated release for E3 Version 2.0

Table of Contents

1. Executive Summary

The purpose of this document is to outline the required steps to install and configure the custom DSM for Snare File and Registry integrity events. It also details the process for adding preconfigured Pulse dashboards for visuallisng the data.

2. Pre-requisites

The folllowing table detials the requirements to be able to install the DSM and Pulse dashboards:

Requirement
Snare agents deployed and forwarding events. **Note: Some features may also require a Snare Central to be deployed.**
Web access to the QRadar server.
Download the SnareE3ContentPackV2.0.zip file for installing into QRadar. It can be found at the link below: https://www.snaresolutions.com/e3-ibm-qradar/
Download and install the QRadar Pulse application from the IBM AppExchange.

3. Pack Contents

The tables below detail the contents of the Snare E3 Content Pack:

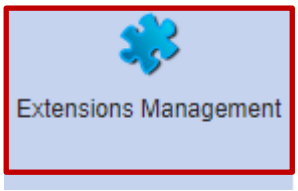
DSM's (with event mapping and custom fields)
Snare Integrity Monitoring
Snare Linux Agents

Pulse Dashboards
Data Enrichment
DNS Analytics
FAM
FIM
RAM
RIM
Time Series
USB

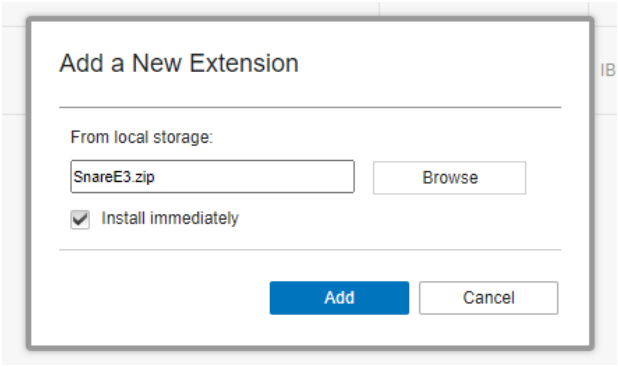
Note: Details regarding each dashboard can be found under Section 7. Dashboards

4. Install the Snare E3 Content Pack

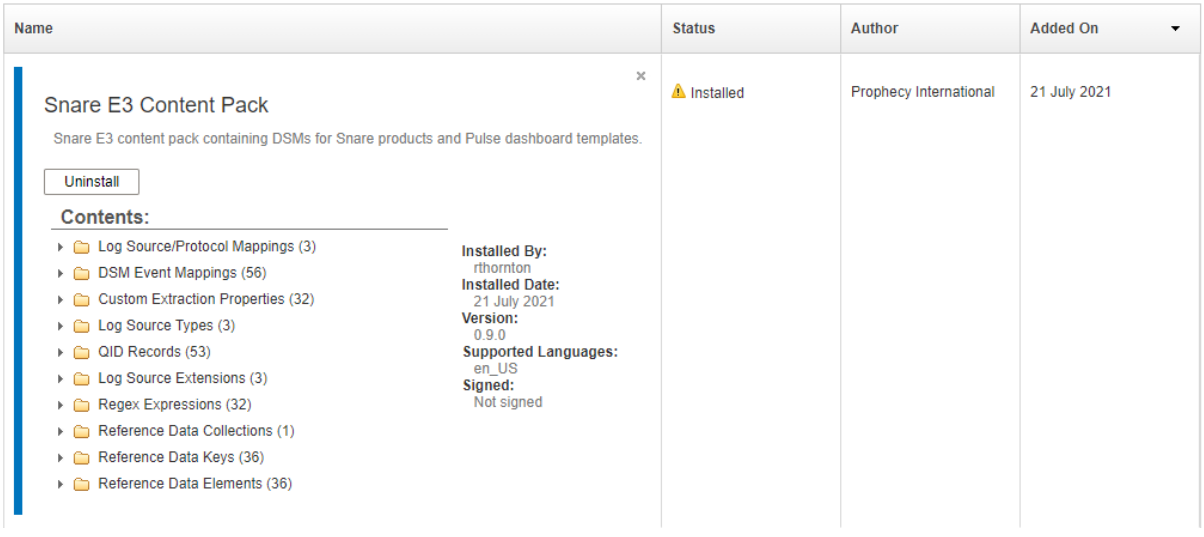
1. Login to QRadar as an administrator and select “Admin” on the navigation menu.
2. Under system configuration section, select “Extension Management”



3. Within the Extension management window, select add in the top right corner and browse to the location of the Snare E3 content pack. Tick “Install Immediately” and then select “Add”.



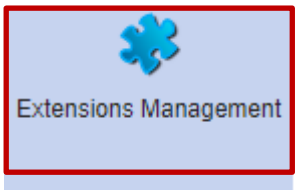
4. Follow the onscreen prompts to finalise installation. Once completed, click the “Snare E3 Content Pack” then select “More Details”. You will see the content pack items listed as below:



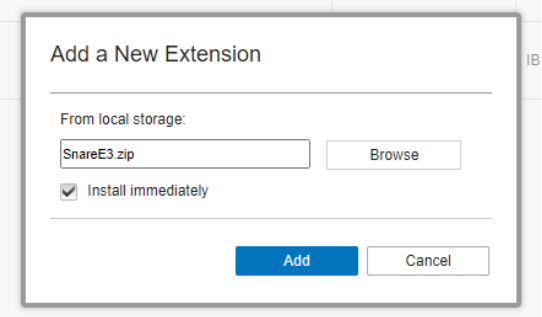
Note: Now the extension has been installed, please ensure you follow the rest of the documentation to create log sources utilising the supplied DSMs and import the Pulse dashboards.

5. Updating the Snare E3 Content Pack

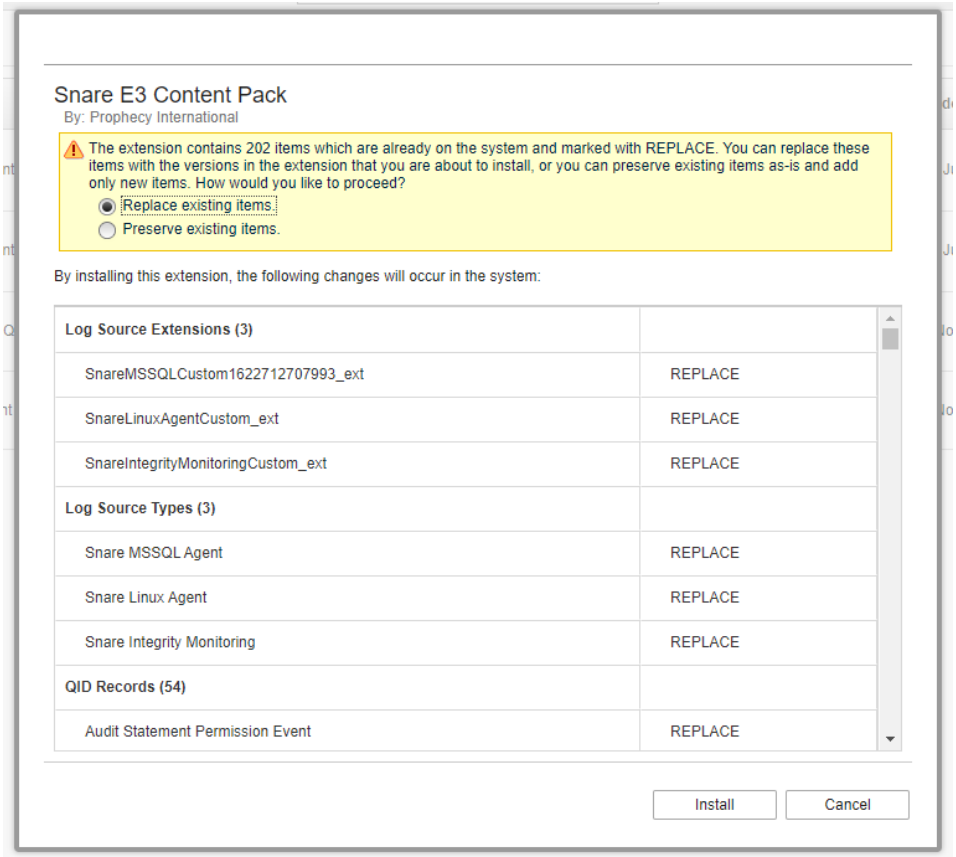
1. Login to QRadar as an administrator and select “Admin” on the navigation menu.
2. Under system configuration section, select “Extension Management”



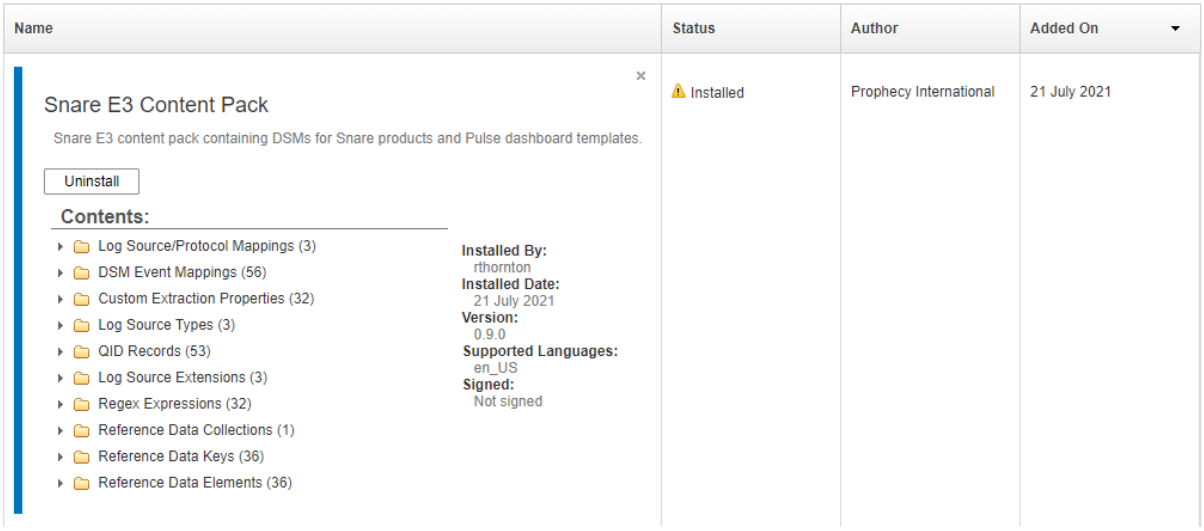
3. Within the Extension management window, select add in the top right corner and browse to the location of the Snare E3 content pack. Tick “Install Immediately” and then select “Add”.



4. A window will popup stating already exisiting components, to perform a full upgrade, leave the option “Replace exisiting items” and click install:



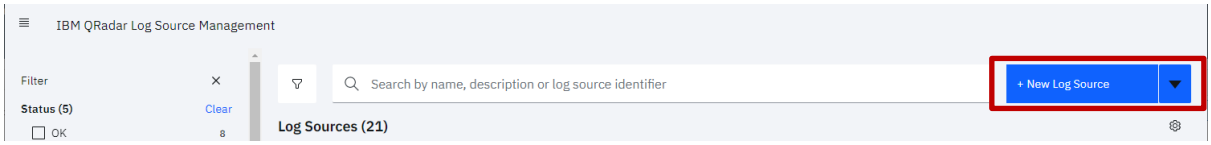
5. Follow the onscreen prompts to finalise installation. Once completed, click the “Snare E3 Content Pack” then select “More Details”. You will see the content pack items listed as below:



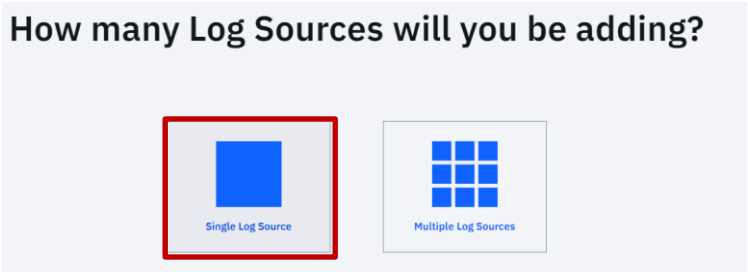
5. Create a log source to utilize the new DSMs

To enable the included Pulse dashboards to correctly detect FIM and RIM events, log sources will need to be created for any devices that send these events to QRadar. The below steps detail how to setup the required log sources.

1. Login to QRadar and select the “Admin” tab on the navigation bar.
2. Once loaded, select “QRadar Log Source Management” under the “Apps” header.
3. The log source management window will popup. Select “+New Log Source”.

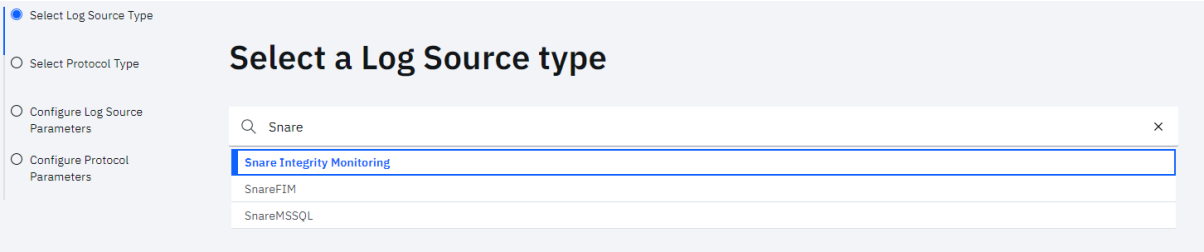


4. Select “Single Log Source”.



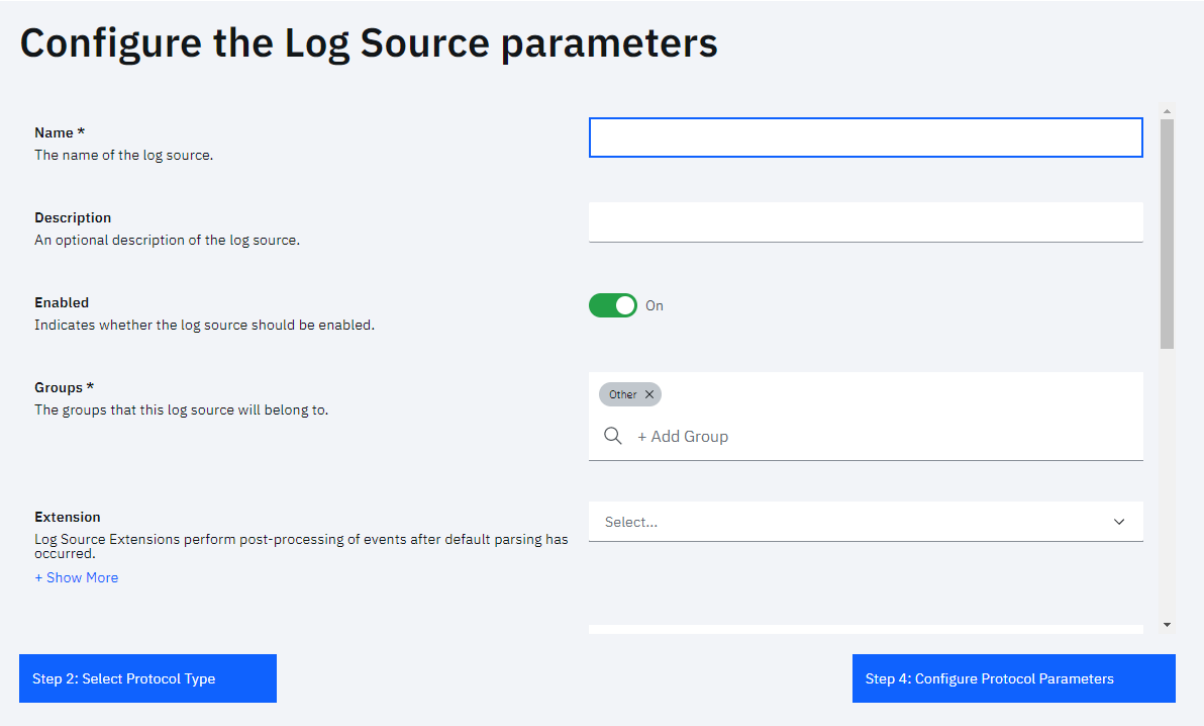
Note: In this guide we only create 1 log source for a known device running Snare Integrity monitoring. You can use the “Multiple Log Sources” option to create a large number of new log source definitions.

5. At the “Select a Log Source Type” prompt, type “Snare” and select the corresponging Logs source for your Snare agent. Then press the “Step 2: Select Protocol Type” button.



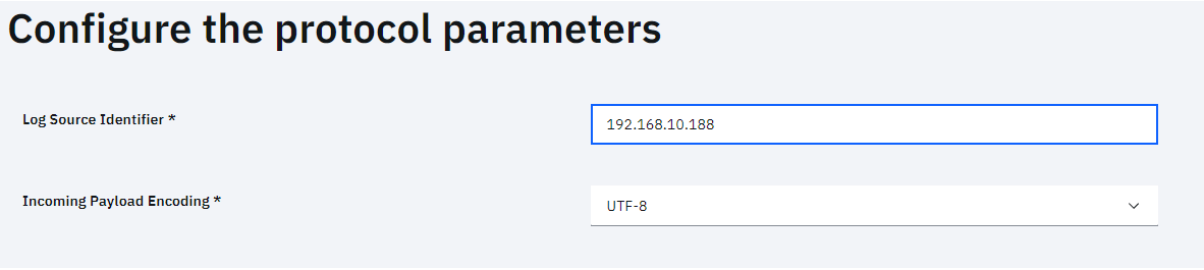
6. At the “Select a protocol type” window, select “Syslog” then press the “Step 3: Configure Log Source Parameters” button.

7. At the “Configure the log source parmeters” window, configure the parameters according to the table below

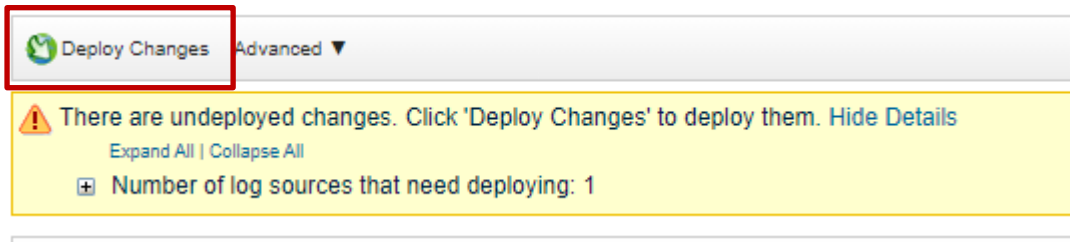


Field	Value
Name	Set a name for the log source, this would usually be the name of the log source type followed by the “@” symbol and the log soure identifier.
Description	Set as per your requirements
Enabled	**Set to Enabled**
Groups	Set as per your requirements
Extension	**Set to “SnareIntegrityMonitoringCustom_ext”, “SnareLinuxAgentCustom” or “Snare MSSQLAgentCustom” depending on the log source type selected.**
Language	Set as per your requirements
Target Event Collector	Set as per your requirements
Credibility	Set as per your requirements
Coalescing Events	**Set to “Off”**
Store Event Payloads	**Set to “On”**

8. Once completed, press the “Step 4: Configure Protocol Parameters” button.
9. At the “Configure the protocol parameters” window, enter the Log source Identifier (the IP address of the system running Snare software) and select “Finish”.



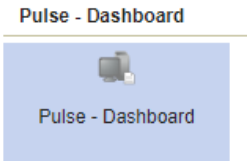
10. Finally, the log source will need deploying. In the “Admin” page of QRadar (found on the navigation bar) you will see a new warning regarding “undeployed changes”. Click the “Deploy Changes” button and follow the pormpts.



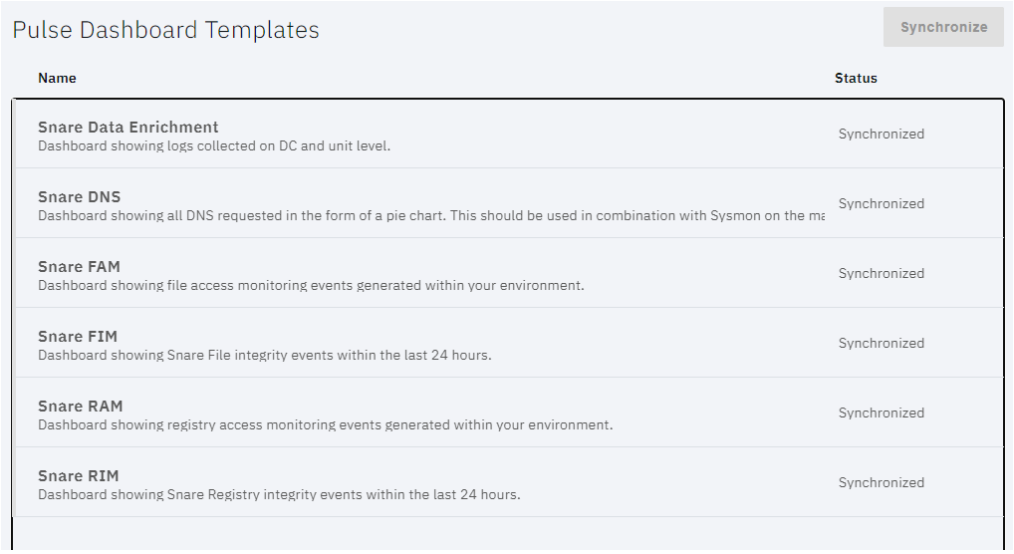
11. The new log source has been successfully deployed.

6. Import the Pulse Dashboards to visualize the data.

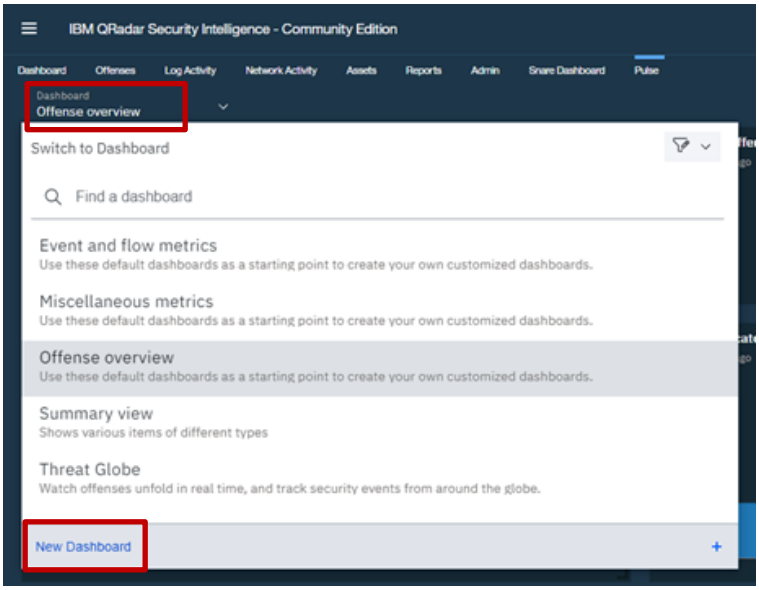
1. Select the Admin app on the navigation bar.
2. Select the “Pulse – Dashboard” optioon under Apps.



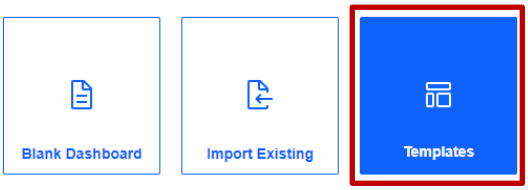
3. You will be presented with available Pulse dashbaord templates. There should be 6 Snare dashboards listed in this view. Press the “Synchronize” button to sync these dashboards to the Pulse app and make them available for users to deploy



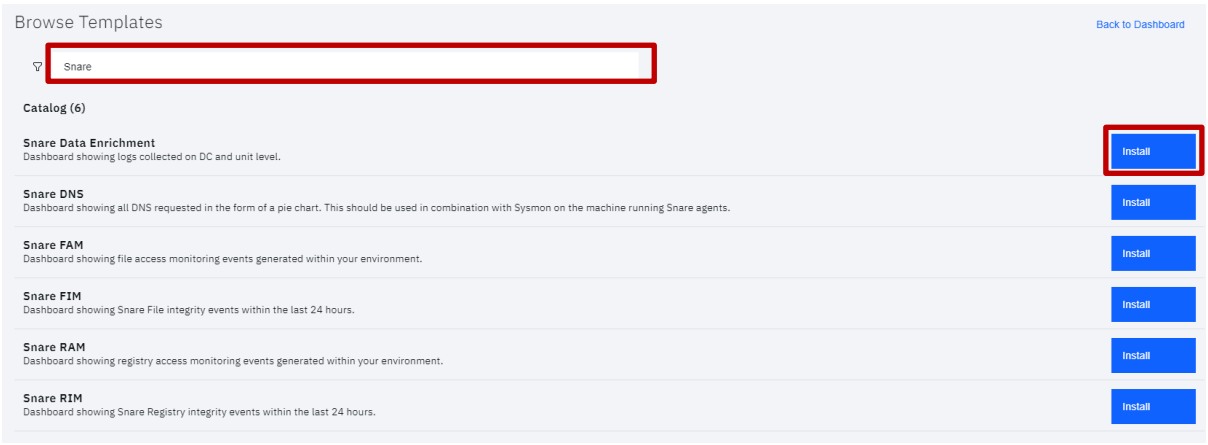
4. Login as a user who requires one of the dashboards. Then select the “Pulse” option on the naviation bar.
5. Select the Dashboard drop down in the Pulse app and then select “New Dashboard”.



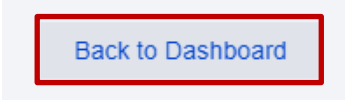
6. The new dashboard window will popup. Select “Templates”:



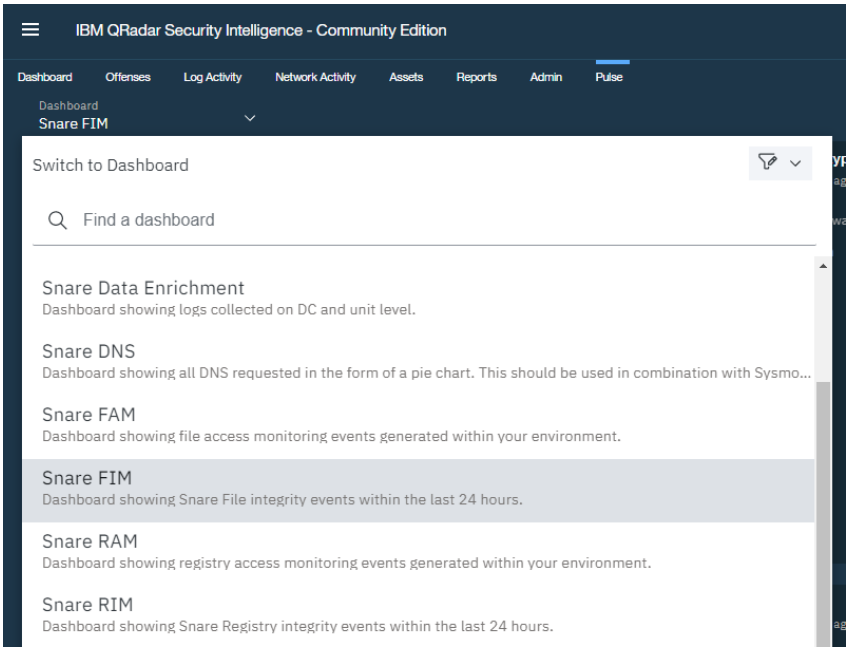
7. Enter “Snare” in the search box at the top of the browse templates page. Then select “install” on the dashboards you would like to add.



8. Once compelete, select “Back to Dashbaord” in the top right corner.



9. If you select the Dashboard drop down again, you will now see the Dashboards have been added.



7. Dashboards

This section will review each dashboard and the various requirements to ensure the correct data is collected.

i. DNS Dashboard

The DNS dashboard utlises the combination of Sysmon and Snare Agents for Windows to collect enchanced DNS logs. To ensure that these events are collected. Sysmon needs to be installed on Windows machines seperately. Sysmon will also need to be configured to collect DNS logs. More information can found at the below links:

Symon Download: Sysmon - Windows Sysinternals | Microsoft Docs

Pre-existing Sysmon configuration: sysmon-config/sysmonconfig-export.xml at master · SwiftOnSecurity/sysmon-config · GitHub

Once installed and configured, Sysmon logs will be captured and forwarded by Snare.

ii. FAM Dashboard

The FAM dashboard surfaces File activity monitoring events that have been captured by Snare agents. This dashboard requires File activity monitoring events to be configured at the agent level. The video at the below link details how to configure this:

FAM Monitoring - YouTube

iii. FIM Dashboard

The FIM dashboard surfaces File activity monitoring events that have been captured by Snare agents.The FIM dashboard requires File integrity monitoring events to be configured at the agent level. The video at the below link details how to configure this:

FIM Monitoring - YouTube

iv. RAM Dashboard

The RAM dashboard surfaces File activity monitoring events that have been captured by Snare agents.The RAM dashboard requires File integrity monitoring events to be configured at the agent level. The video at the below link details how to configure this for RAM, to apply this to Regisrty set the “General Search Term” to the location of your registry key.

FAM Monitoring - YouTube

v. RIM Dashboard

The RM dashboard surfaces File activity monitoring events that have been captured by Snare agents. The RIM dashboard requires Registry access monitoring events to be configured at the agent level. The video at the below link details how to configure this:

RIM Monitoring - YouTube

vi. Enrichment Dashboard

The enrichment dashboard requires data tagging to be configured on both an agent and Central level. This allows logs to be tagged with enriched data providing greater insight into logging systems.

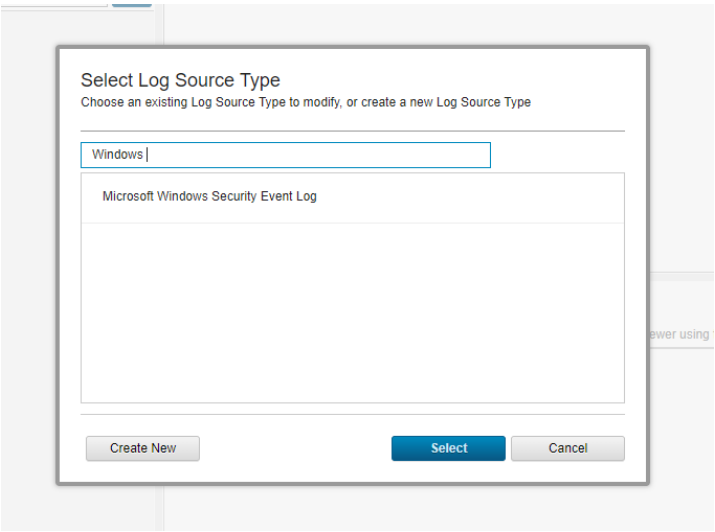
To configure agent level logging, the EventSourceID field needs to be set with a text value. This can be found in the “Destinations” page within Snare agents, set within .ini files or pushed to agents using Snare AMC and Micrsoft GPO. For Linux and MSSQL agents, this data will be automatically parsed as part of the DSM.

Note: When using the Event source ID feature within Snare agents space characters are not supported. Using spaces will affect the data parsing configured within the DSM.

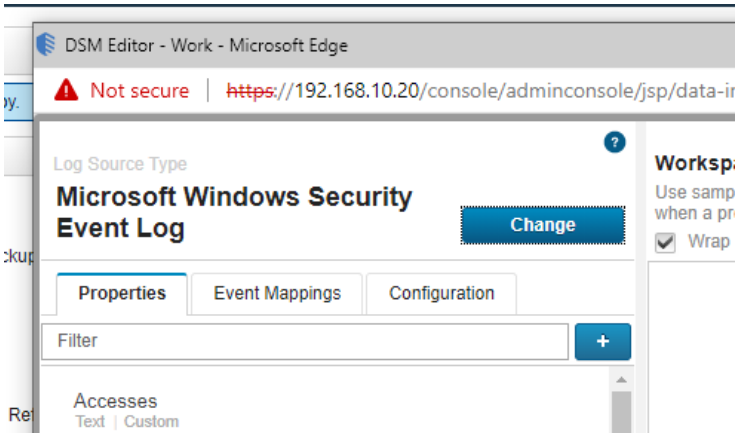
With the Windows Agents, a couple specific fields need to be mapped to the existing DSM that exists in QRadar. To do this follow the below steps.

Note: When modifying the builtin “Microsoft Windows Security Event Log” to parse enrichment data, updates to QRadar may remove the configuration. This will need to be reapplied if removed.

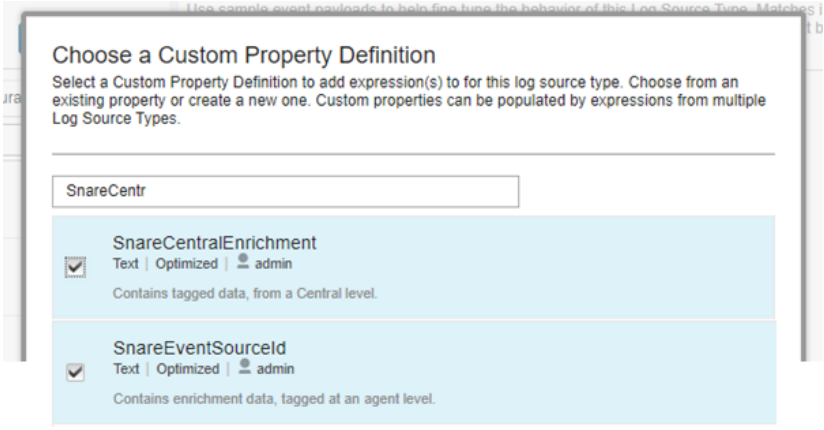
1. Login to QRadar and select “Admin” on the navigation menu.
2. Once the DSM editor window opens, Select “Microsoft Windows Security Event Log”.



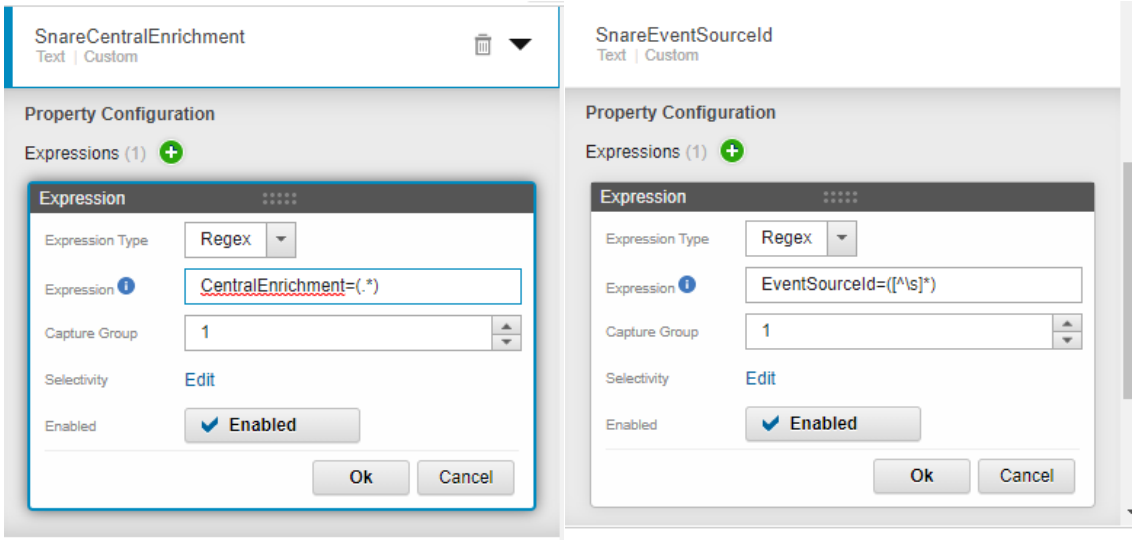
3. Select the “+” option in the properties section of the DSM editior.



4. In the “Choose a custom property definition” window, seach for and tick both “SnareCentralEnrichment” and “SnareEventSourceId”, then press “Select”.



5. These 2 fields will now be added to the properties list. Located them in the list and expand them by clicking them, then apply the settings as per the images below and click ok.

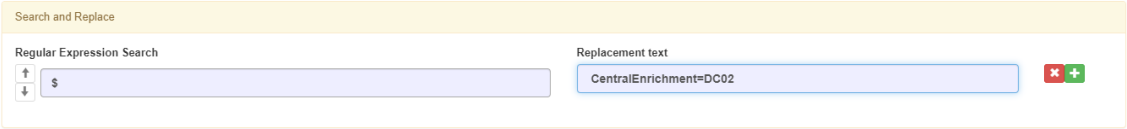


SnareCentralEnrichment: CentralEnrichment=(.*)
SnareEventSourceId: EventSourceId=([^\s]*)

6. With the fields confgiured and added, select the “Save” option in the bottom right corner of the DSM editor to save these new settings.

To configure Central level data enrichment follow the below steps. The tag set here will be applied to all logs being sent to that destination:

1. Login to Snare Central and from the left hand menu select “System” -> “Administrative Tools” -> “Configure Collector/Reflector”.
2. Once the page loads select the “Configure” option at the top of the page.
3. Locate the destination you would like to tag logs on and create a new “Search and Replace” rule.
4. Set the “Regular Expression Search” value to “$”.
5. Then set the “Replacement Text” value to “ CentralEnrichment=” plus any tag you would to add to the logs after the “=”.



Note: It is important to start the “Replacement Text” field with a space character. This ensures seperation of the tag with other log content.

6. Now scroll to the bottom of the window and select “Set”. Then when prompted select “Restart” to restart the reflector services so that the changes take affect.

Note: When restarting the reflector services, log delivery to destinations will be temporarily inturupted.