

Open Mic: Maintaining QRadar 101

A discussion with administrators about maintaining QRadar and what data to review on a reoccurring basis.


<https://ibm.biz/JoinQRadarOpenMic>

Disclaimer

Please Note:

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Announcements & information

- QRadar 7.3.2 Patch 1 is released.
Release notes: <https://ibm.biz/qradarsoftware>
- QRadar M5 v3.3.0 Firmware is released.
Release notes: <https://ibm.biz/qradarfirmware>
- Support recently released a WinCollect page to put resources & links in one area.
<https://ibm.biz/wincollect101>

WinCollect 101
Capturing Windows-based events for Qradar SIEM administrators. Find information, ask us questions, important notices, and resources for WinCollect administrators.

Download the latest WinCollect software from IBM Fix Central 7.2.2 Patch 2 (Build 155). All files for managed or standalone installations included in this link.

What's new in WinCollect 7.2.2?
New features are announced in WinCollect software for the release of WinCollect 7.2.2. Log on and visit the single WinCollect page for more information. A new reporting tool is available for the administrators, providing enhanced and improved reports. To support the latest WinCollect 7.2.2 for log collection, administrators can add support for various log file formats. A new WinCollect plugin is available for WinCollect 7.2.2 to collect Windows events, including the Windows Event Log. The new reporting tool is available for WinCollect 7.2.2. The new reporting tool is available for WinCollect 7.2.2. The new reporting tool is available for WinCollect 7.2.2.

Supported versions
WinCollect 7.2.2 Patch 2
WinCollect 7.2.2 Patch 1
WinCollect 7.2.2
WinCollect 7.2.1
WinCollect 7.2.0

Useful articles
How to install WinCollect on a Windows Server
How to install WinCollect on a Windows Server
How to install WinCollect on a Windows Server

Configuration help
How to install WinCollect on a Windows Server
How to install WinCollect on a Windows Server
How to install WinCollect on a Windows Server

WinCollect Error Messages
WinCollect Error Messages
WinCollect Error Messages
WinCollect Error Messages

Resources
WinCollect Error Messages
WinCollect Error Messages
WinCollect Error Messages

Watch the Latest WinCollect Open Mic
Using this session we ask WinCollect users, techs, notifications, and developers to ask questions, share their experiences, and get answers for the audience. The questions for this session include: The WinCollect 7.2.2 Patch 2 and Support Center, or a list of previous open mic sessions, use the link open mic for more.

QRadar Open Mic Replay: WinCollect Troubleshooting
IBM Qradar Support
21 September 2018

Expert blogs
Risk Rating in WinCollect & Log Source Management
Install WinCollect to Include WinX System
Install WinCollect to Include WinX System
Install WinCollect to Include WinX System

Agenda

- Daily review items for admins
- Weekly review items admins
- Monthly review items for admins
- Future considerations
- Recommended apps

Daily review items for administrators

- System notifications
- Disk space reviews
- Service reviews
- Incoming data review
- Offense generation review
- WinCollect agent status
- UI app check

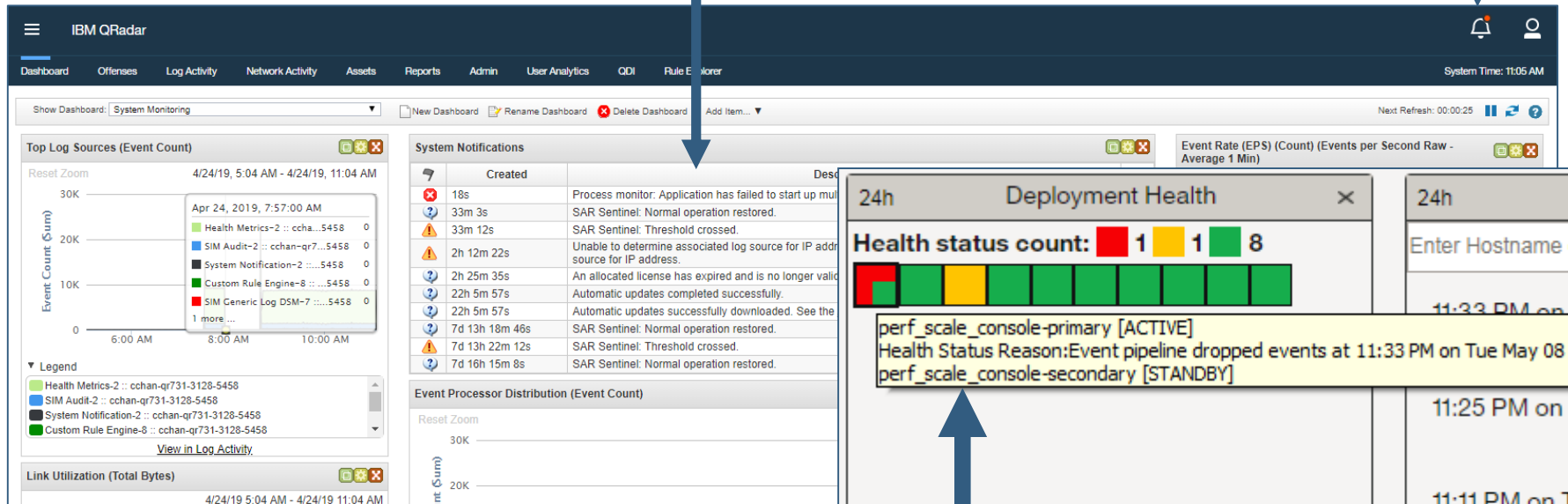


1. System Notifications – Daily Reviews

- ❑ Review System Notifications daily for QRadar!

System Notifications are the primary method for QRadar to alert users to problems. Administrators should consider System notifications your first line of defense in to understanding a problem exists.

Basic notification Dashboard






Deployment overview in QRadar
Deployment Intelligence App (QDI)

Daily Review for System Notifications (Continued)

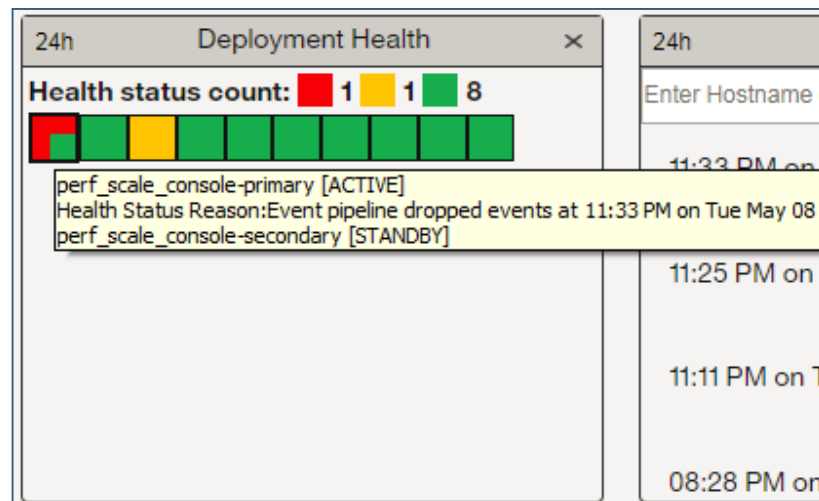
How many system notifications are in QRadar?

There are 85 system notifications in QRadar that cover everything from disk space, rules, offenses, memory, log source issues, and more.

-  **Errors** – Advises administrators of high severity issues (Severity 7 - 10). Error notifications are issues that should be examined as soon as possible.
-  **Warning** – Advises administrators of medium severity issues (Severity 3 - 6).
-  **Info** - Advises administrators of low severity issues (Severity 1 - 2).

Does QDI and the standard interface show the same information?

QRadar Deployment Intelligence will list notifications by host. Someone should be reviewing System Notifications daily for QRadar. Where the standard UI shows you a list of notifications by most recent based on timestamp.



The screenshot displays the '24h Deployment Health' window. At the top, it shows the 'Health status count' with three colored squares: a red square for '1', a yellow square for '1', and a green square for '8'. Below this is a horizontal bar chart with 10 segments: the first is red, the second is yellow, and the remaining eight are green. A tooltip is visible over the bar chart, showing the following details:

- perf_scale_console-primary [ACTIVE]
- Health Status Reason: Event pipeline dropped events at 11:33 PM on Tue May 08
- perf_scale_console-secondary [STANDBY]

The right side of the screenshot shows a list of notifications with timestamps: 11:33 PM on T, 11:25 PM on T, 11:11 PM on T, and 08:28 PM on.

2. Check Disk Space – Daily Review

❑ Do you review disk space daily for QRadar?

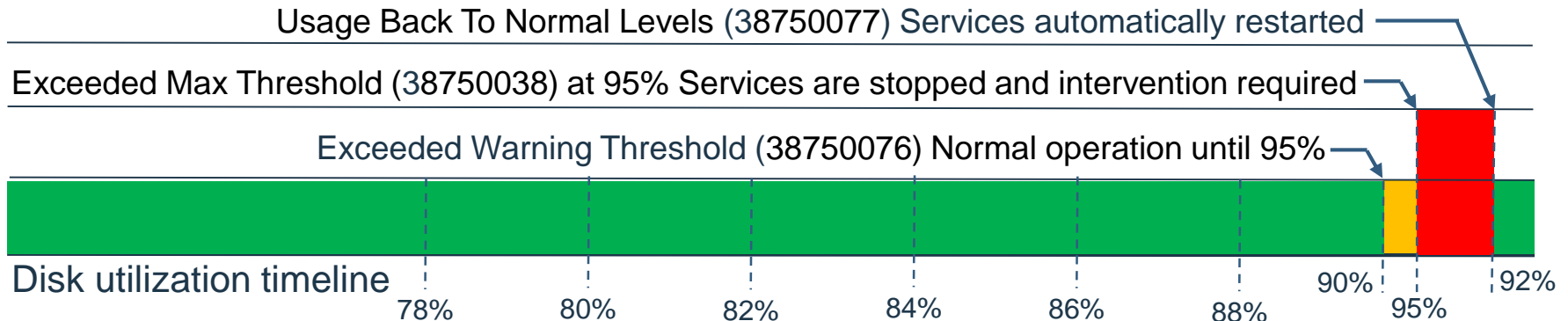
QRadar currently monitors the following partitions and will issue a notification when utilization of any of these partitions are over 90% →

System Notifications checks are completed every 60 seconds on all appliances.

- /
- **/store**
- **/transient**
- **/storetmp**
- **/opt**
- /var
- /var/log
- /var/log/audit
- /tmp
- /home

NOTE: Bold indicates directories that stop services when full versus directories that will generate a system notification only.

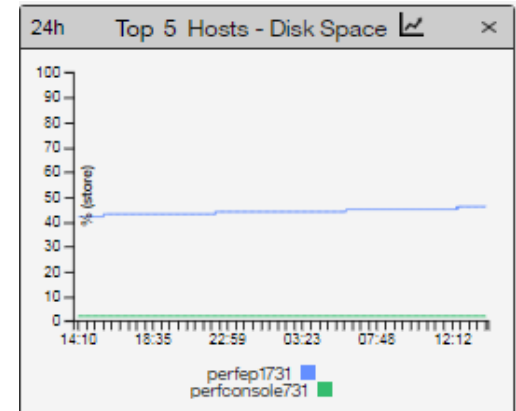
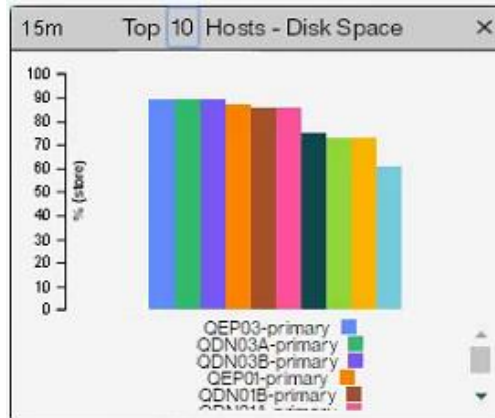
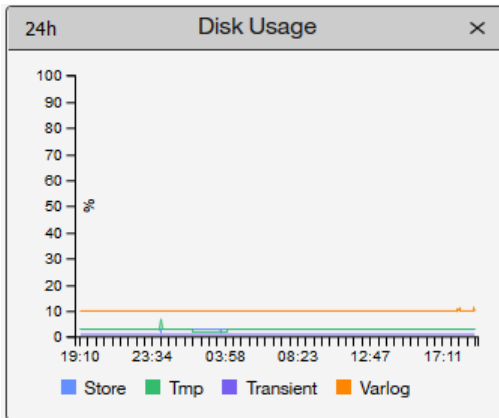
- ⚠️ 90%: Warning - Disk Sentry: Disk Usage Exceeded Warning Threshold (38750076)
- ❌ 95%: Error - Disk Sentry: Disk Usage Exceeded Max Threshold (38750038)
- 🔍 92%: Information - Disk Sentry: System Disk Usage Back To Normal Levels (38750077)



Check Disk Space – Daily Review (Continued)

Since the system notification gives you disk space alerts on partitions that can stop services administrators might consider being proactive with disk checking:

- To see utilization for the entire deployment:
`/opt/qradar/support/all_servers.sh "df -Th"`
- To see usage of a partition:
`df -k | grep sda8`
- To do a quick check in the logs for disk messages:
`/var/log/qradar.error | grep -i "disk usage"`
- What directories are using the most space in a specified path:
`du -Phx /opt --max-depth=1`
- QDI can help here too, see metrics on individual hosts or top hosts in the deployment



3. Service issues – Daily Review

- Review for service issues in your QRadar deployment.

The easiest way to locate service issues in QRadar for your deployment or for specific appliances is to use QRadar Deployment Intelligence. Status and outage durations are both reported in a searchable view.

The screenshot displays four overlapping windows from the QRadar Deployment Intelligence interface:

- Process Monitor - Last 7 days:** A table showing the status of various components. All listed components are currently available with no known outages.
- Component Status Feed - Last 7 days:** A log of status changes for various components, all showing a transition to 'Available' at 09:54 AM on 23-Apr-2019.
- 24h Top 5 Hosts - Process Outage (Bar Chart):** A bar chart showing outage durations for two components: perf_scale_ec1 (50.42 minutes) and perf_scale_console (0.98 minutes).
- 24h Top 5 Hosts - Process Outage (Bar Chart):** A bar chart showing the count of outages over time for the same two components.

Component	Total Outage (min) ↓	Current Status	Last Outage Starttime	Last Outage Duration (min)
reporting_execu	0.00	Available	No Known Outages	0
historical_corr	0.00	Available	No Known Outages	0
arc_builder	0.00	Available	No Known Outages	0
hostcontext	0.00	Available	No Known Outages	0

Component Status Feed - Last 7 days

Enter Component or Hostname or Status or Date/Time to Filter Status Feed

- setprofiler on [redacted] went Available at 23-Apr-2019 09:54 AM
- nprocessor on [redacted] went Available at 23-Apr-2019 09:54 AM
- orting_executor on [redacted] went Available at 23-Apr-2019 09:54 AM
- s-ec-ingress on [redacted] went Available at 23-Apr-2019 09:54 AM
- on [redacted] went Available at 23-Apr-2019 09:54 AM
- torical_correlation_server on [redacted] went Available at 23-Apr-2019 09:54 AM
- s-ep on [redacted] went Available at 23-Apr-2019 09:54 AM
- ss on [redacted] went Available at 23-Apr-2019 09:54 AM

24h Top 5 Hosts - Process Outage

Component	Outage (minutes)
perf_scale_ec1	50.42
perf_scale_console	0.98

24h Top 5 Hosts - Process Outage

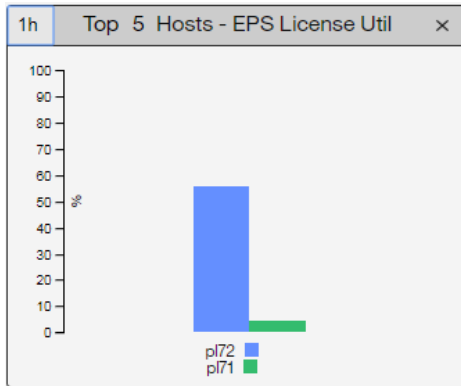
Count

perf_scale_ec1

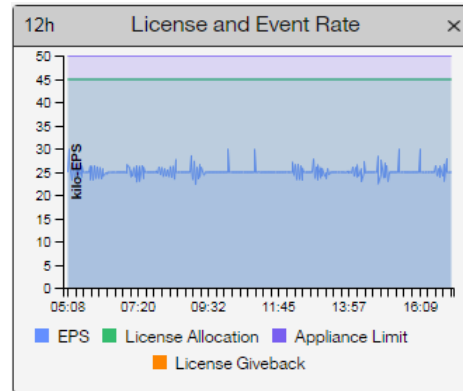
perf_scale_console

4. Incoming Data – Daily Review

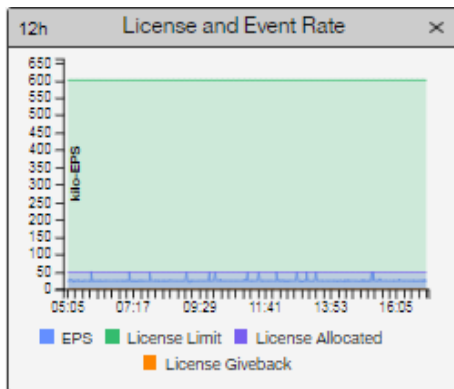
What is happening for event rate or flow rate in the deployment or on specific appliances?



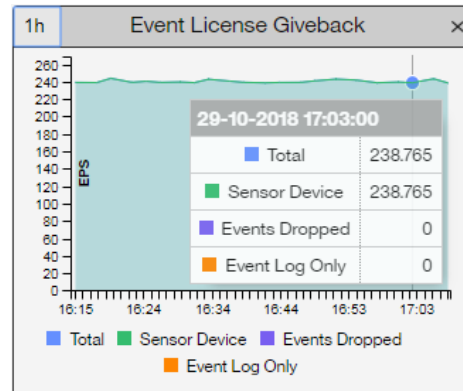
License utilization - Allocations



Appliance Event Rate - Status



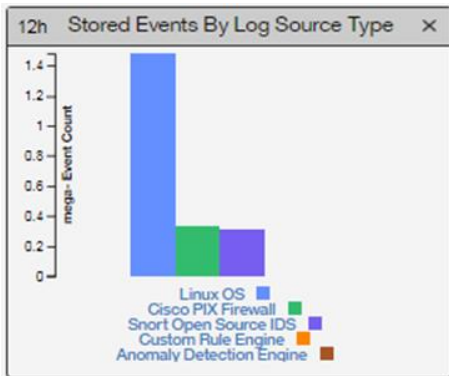
EPS Deployment - Capacity



EPS Giveback – Non-security data

Incoming Data – Daily Review (Continued)

What log sources are contributing the most data, what in error, being stored, unparsed?



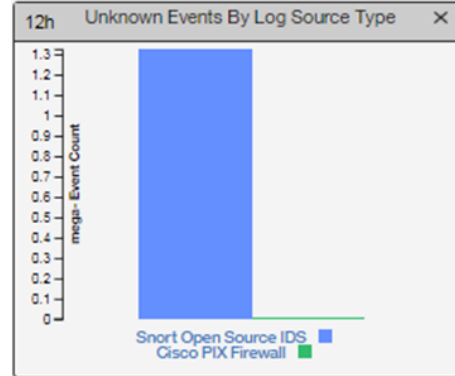
Top 5 Recently Errored Log Sources

Enter LogSource to Filter

Log Source	Last Event Time
Search Results-2	5-May-2018 4:42 AM
SIM Generic Log	4-May-2018 4:51 AM

15m Expensive Log Sources

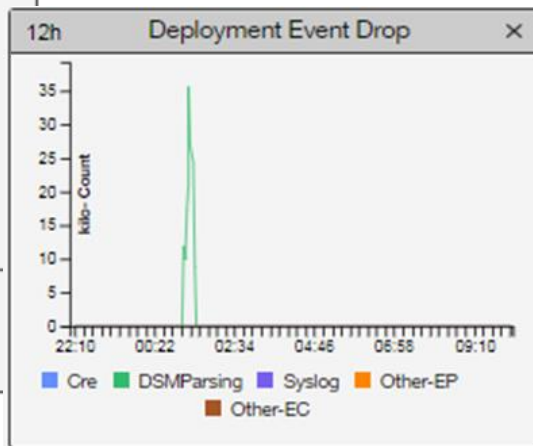
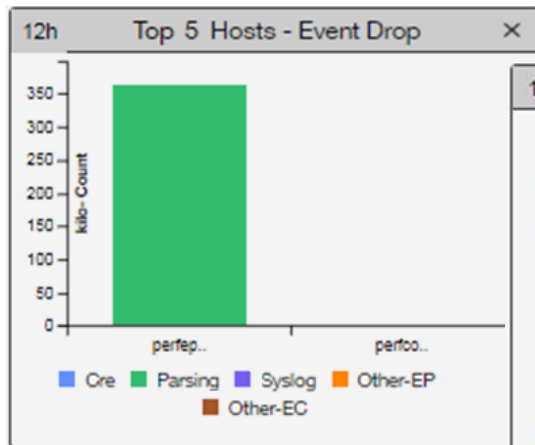
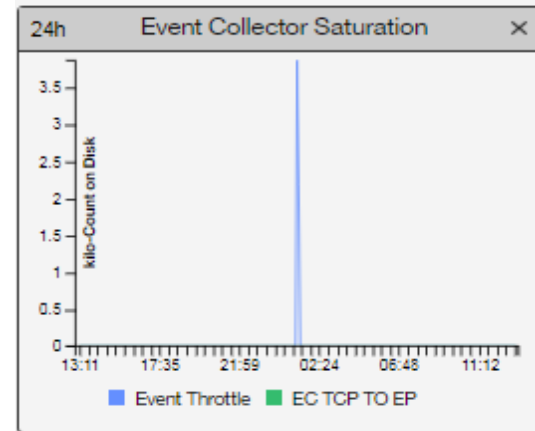
Hostname	Log Sources	EPS
pl72	SIMNotification	9889
pl72	Pix	8431
pl72	LinuxServer	5518
pl72	VmWare	3127
pl72	GenericLogDSM	815



- **Stored** - The DSM associated with the Log Source is unable to parse the payload of the event. If this is an official IBM Device Support Module, verify the version is supported and that you are not experiencing performance issues (Routed to storage) to relieve backpressure on the event pipeline.
- **Unknown** - QRadar extracts event information (parses) and associates the data to a log source. For example, “Cisco Meraki Unknown”. However, the eventID was not able to be mapped to an existing QID.
- **Error/stopped sending** – What stopped sending? You can create a Log Source report for new/stopped sending log sources or view the data in QDI.
- **SIM Generic** – If traffic analysis fails to auto discover a new log source, it is added to the SIM Generic log source to catch the events as they are received.

Incoming Data – Daily Review (Continued)

- ❑ Is data in the spillover buffer (5GB)? Does the queue impact important rules that need to be evaluated in real-time? →
- ❑ Throughput of log sources can indicate performance of expensive log source types (more of a weekly issue). Lower number = lower performance.
- ❑ Is any data being dropped and what pipeline specific components are having issues (protocol queue, parsing, custom rules)?



15m Expensive Log Sources

Hostname	Log Sources	EPS
p172	SIMNotification	9889
p172	Pix	8431
p172	LinuxServer	5518
p172	VmWare	3127
p172	GenericLogDSM	815

5. Rules and Offense Generation

- Run a search to determine how many offenses were generated in the last 24 hours or see what rules are alerting the most.

The QRadar Tuning App (Early Access at the time of this presentation) includes an offense trend line at the top of the application.

IBM QRadar Tuning
Last updated: 01/25/2019, 13:36:20

Open offenses: **48**
Active offenses: **46**

Offense creation trend

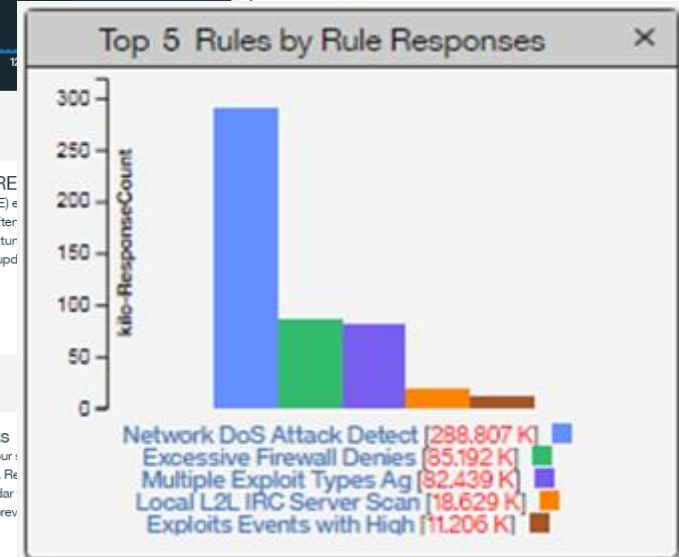
Tune your QRadar offenses by analyzing rules that cause the biggest number of offenses

- Tune most active rules: QRadar Tuning can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.
- Tune based on the CRE: The Custom Rules Engine (CRE) events were generated most often about the rule activity. You can tune information from the report to update.

Tune your QRadar offenses by going through the most common configuration steps

- Review network hierarchy: Network Hierarchy is used to define which IP addresses and subnets are part of your network. Defining your network hierarchy and keeping it up-to-date is an important step in helping prevent false offenses.
- Review building blocks: Rules use information about your building blocks to generate the rule responses. Rebuilding blocks to enable QRadar servers on your network, and prevent.

QDI



6. WinCollect Agent Status

- ❑ Review Admin > WinCollect > Agents.

The agent list provides status information for all WinCollect agents deployed in managed mode and their status information. Agents that are in the STOPPED or OFFLINE states should be reviewed.

7. Application Status

- ❑ Review User interface > App tabs

Administrators can spot check apps to ensure that the tab are visible (not blank) in the user interface and that no errors are displayed. If any tabs are blank, run one of the following utilities to confirm service status:

QRadar 7.3.2: `/opt/qradar/support/recon`

QRadar 7.3.1: `/opt/qradar/support/qapp_utils730.py`

QRadar 7.2.8: `/opt/qradar/support/qapp_utils.py`

Example Recon Output – PS

```
$ recon ps
```

App:	Workload:	Service:	Container:	Port:						
ID	Name	ID	Name	AB	Name	Image	CDEFGH	Container IP:Port	Host IP:Port	IJKL
1051	User Analytics	apps	qapp-1051	++	container-1	consul.local/qapp-1051:1.2.3	+++++	169.254.3.3:5000	9.21.123.12:35929	+++
1051	User Analytics	apps	qapp-1051	++	container-1	consul.local/qapp-1051:1.2.3	+++++	169.254.3.3:5001	9.21.123.12:35930	+++
1052	Threat Intelligence	apps	qapp-1052	+-	container-1	consul.local/qapp-1052:1.2.3	-----	N/A	N/A	----
1053	QRadar Assistant	apps	qapp-1053	++	container-1	consul.local/qapp-1053:1.2.3	+++++	169.254.3.5:5000	9.21.123.12:35932	+++
1053	QRadar Assistant	apps	qapp-1053	++	container-2	consul.local/qapp-1053:1.2.3	+++--	N/A	N/A	----

LEGEND [+ is success, - is fail, n is not applicable]

Service:

- A - Service is in ConMan workload file
- B - Service is set to started

Container:

- C - Container is in ConMan workload file
- D - Container environment file exists and is not corrupt
- E - Container image is in si-registry
- F - Container Systemd Unit file exists
- G - Container Systemd Units are started
- H - Container exists and is running in Docker

Port:

- I - Container port is in iptables NAT rules
- J - Container port are in firewall rules
- K - Container port has routes through Traefik
- L - Container port is responsive on debug path

Weekly review items for administrators

- Auto updates
- Log Source Groups
- Domains/tenants
- Vulnerability Scans
- Asset review
- Threat Feeds and IOCs
- Backup and Restore
- Reports



1. Auto Updates – Weekly Review

- ❑ QRadar auto updates are available weekly starting on Tuesday evening (Eastern Time Zone). Administrators can run a manual update or schedule an update closer to the posting of the server files if they prefer in the auto update configuration settings.
- Did the update complete? Check system notifications to confirm.
- First troubleshooting step you want to take for new installations and proxy confirmation steps for auto update issues are outlined here: [500 SSL Negotiation Failed Errors](#)
- If you think a firewall change might be blocking your updates and you have events from your firewall in QRadar, a quick test is to put the IP addresses of the QRadar auto update server in the Quick Filter search. The results returned will allow you to identify if your firewall is returning Accept or Deny events to QRadar.

Log Activity > Add Filter > Destination IP > 69.20.113.167 and 212.64.156.13

qmmunity.q1labs.com's IP address is 69.20.113.167

qmmunity-eu.q1labs.com's IP address is 212.64.156.13

2. Log Source Groups – Weekly Review

- ❑ Review the ‘Other’ log source group list.

Administrators who have a lot of auto discovered log sources should put a check in their admin process to review log source groups. By default, log sources not categorized are added to the ‘Other’ log source group.

- Use the Log Source Management App to filter Other.
OR
- Admin tab > Log Source Groups > Other

Why is this important?

Administrators should complete a weekly review to categorize these properly so that rules and searches will capture all intended log sources in QRadar. Log source groups are leveraged across QRadar in searches, rules, and reports. For example:

The screenshot shows the 'IBM QRadar Log Source Management' interface. It features a 'Filter' section on the left with three categories: 'Status (5)', 'Enabled (2)', and 'Log Source Type (351)'. Each category has a list of options with checkboxes and counts. The 'Status' options are OK (5), Warning (0), Error (1), Not Available (8), and Disabled (4). The 'Enabled' options are True (14) and False (4). The 'Log Source Type' options include Cisco ACE Firewall (2), Custom Rule Engine (2), APC UPS (2), SIM Generic Log DSM (2), Health Metrics (1), System Notification (1), Anomaly Detection Engine (1), Amazon AWS CloudTrail (1), Apache HTTP Server (1), and Linux DHCP Server (1). A '+341 More' link is at the bottom of this list. On the right, there is a search bar 'Search by name or description' and a table of log sources with columns for 'ID' and 'Name'. The table lists several log sources, including 'Anomaly Detection Engine-2 :: ip-127-203', 'APC @ host123', 'APC @ host456', 'Asset Profiler-2 :: ip-127-203', 'AWS Trial', 'Custom Rule Engine-105 :: ip-127-58', 'Custom Rule Engine-8 :: ip-127-203', 'DHCP Server (Linux)', 'Firewall #12', 'Firewall #9', and 'Health Metrics-2 :: ip-127-203'.

Apply on events which are detected by the system
and when the event(s) have not been detected by one or more of these log sources for this many seconds
and when the event(s) have not been detected by one or more of these log source groups for this many seconds
and when the event(s) have not been detected by one or more of these log source types for this many seconds

3. Domains & Tenants – Weekly Review

- ❑ Review domain and tenant information.
- Administrators should run some searches for Assets, log sources, or some general IP searches in known overlapping ranges to see if any data only belongs to the ‘Default’ domain. Data that is not assigned to a domain ends up in the default domain, which might not be viewable by users, searches, or rules unless explicitly defined.
- Administrators should complete a review to categorize new data for domains and tenants:
 - Log sources
 - Flows
 - Scanners
 - Event Collectors
 - User Profiles
 - Reference Sets
 - Subnets in Network Hierarchy
 - Custom property definition (Tenant)
 - Retention buckets (Tenant)

4. Vulnerability scans – Weekly Review

- ❑ Review to ensure that vulnerability scans completed.
- QRadar Vulnerability Manager users should confirm that the daily vulnerability update completed. QVM is issued daily updates with vulnerability catalog updates, scan tool changes, and more.
- Update scans with new CIDR ranges or consider splitting CIDRs in to smaller groups so they can complete faster. Never scan a 0.0.0.0/0 network. [Understand scan times](#) and account for that in your reporting.
- Assign owners to your assets.
- Consider tuning server discovery by enabling or disabling options:
 - Send ICMP pings (default)
 - Send TCP SYN packets to ports (default)
 - Send UDP packets to ports
 - Enable traceroute detection
 - Enable ICMP detection
 - OS and service fingerprinting

5. Assets – Weekly Review

- ❑ Review the number of assets created recently in QRadar using searches.
- Review asset system notifications if any were triggered.
 - 38750106 - Asset Changes Aborted.
 - 38750137 - The system detected asset profiles that exceed the normal size threshold.
 - 38750136 - The Asset Reconciliation Exclusion rules added new asset data to the asset blacklists.
 - 38750126 - An external scan execution tried to scan an unauthorized IP address or address range.
- Run the search **Deviating Asset Growth: Asset Report** to identify if any assets have an unusually high number of IP addresses, DSN names, or NetBIOS names associated to a single asset.
- Review Asset Exclusions in QRadar to prevent assets from being updated by the Asset profiler.
- To determine what caused asset updates, users can search against the Asset Profiler-2 log source.

6. Threat Feeds & IOCs – Weekly Review

- ❑ Verify that the Threat Intel app and associated thread feeds are updated in QRadar.
 - Click **Poll Now** to test feed collection.
 - Ensure that the X-Force API key hasn't been regenerated for the account linked to the application (X-Force Exchange login > Profile > Settings > API Access).
 - Confirm application framework services are running.
 - Connect to the app container: `recon connect <app id>`
 - Verify that Reference Sets are updated in QRadar.

Configured Threat Intelligence Feeds			
https://api.xforce.ibmcloud.com/taxii Client Certificate: None Client Key: None Collection: xte.ipr.botnet.command.and.control.server Reference Set: Botnet C&C IPs	↓ 1 Signatures received last poll	3,105 Total signatures received	Edit - Delete Polling End Date: Mar 25, 2019, 9:53 AM (Poll Now) Polling Interval: 60 minutes
https://api.xforce.ibmcloud.com/taxii Client Certificate: None Client Key: None Collection: xfe.default Reference Set: IP Reputation	↓ 1,662 Signatures received last poll	188,094 Total signatures received	Edit - Delete Polling End Date: Mar 25, 2019, 9:24 AM (Poll Now) Polling Interval: 60 minutes

7. Backup and Recovery – Weekly Review

- ❑ Verify that both configuration and data backups are enabled.
 - Are backups available on the remote sites?
Configuration backups occur on the Console. Data Backups are created on each appliance that stores event & flow data. Data backups for long term storage need to be moved to a separate location or you need to set up off-board storage on each appliance.
 - New users should realize that QRadar's default setting is to do Configuration backups, but not Data Backups as well and the default file retention is 7 days.

Backup Archives On Demand Backup Restore Delete Configure

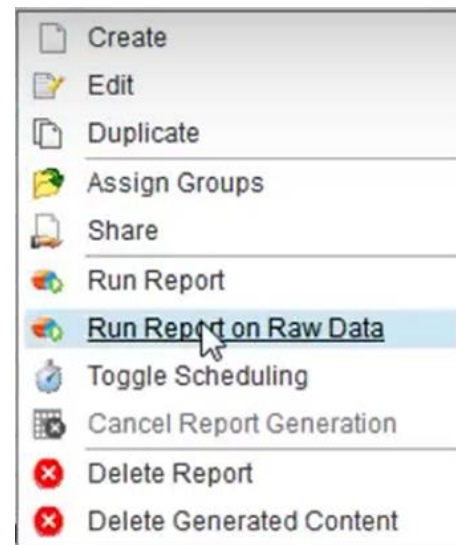
Existing Backups

!	Host	Name	Type	Size	Time Initiated	Duration	Initialized By
⚠	SUPPORT	nightly	config	2.4GB	Jan 22, 2019, 12:00:14...	4m 34s	scheduled_initiator
			config	2.4GB	Jan 21, 2019, 12:00:10...	4m 37s	scheduled_initiator
			config	2.4GB	Jan 20, 2019, 12:00:10...	4m 38s	scheduled_initiator
	SUPPORT	nightly	config	2.4GB	Jan 19, 2019, 12:00:12...	4m 36s	scheduled_initiator

Upload Archive: No file selected.

8. Reports – Weekly Review

- ❑ Verify that reports are complete and include expected data.
 - Run the search associated to the report to ensure it returns the expected data. Use the Network, Activity, or Log Activity tab to run the search again. You can compare the results with the generated report.
 - Review the notification message on the Reports tab. The Reports tab displays a notification message when your data is incomplete. Look at QID processes and see if accumulator (responsible for graph data) had a service interruption.
 - Did you know you can view a list of search and report titles associated with it?
`/opt/qradar/support/collectGVStats.sh -M | less`
 - Run your report against raw data from the initial time period.



Monthly review items for administrators

- Incoming Data
- Defect Inspector
- Software and Firmware Updates
- Apps and Content Pack Updates
- General Tuning
- Retention buckets
- Custom properties
- Search duration by user
- Review for coalesced log sources

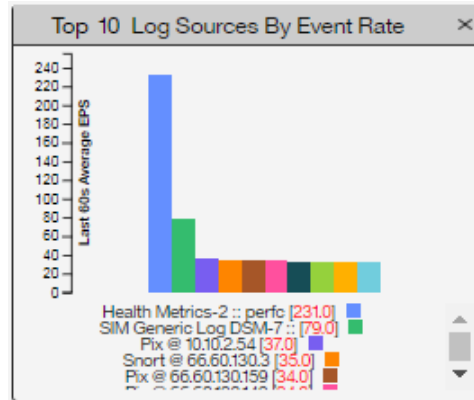


1. Incoming Data - Monthly checks

Questions that admins might ask themselves during an incoming data review:

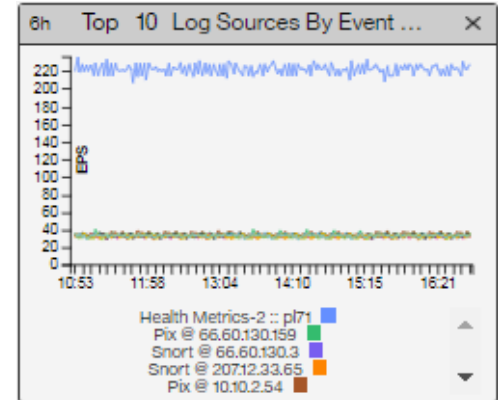
What is contributing a lot of data?

QDI shows this data readily for both Top 10 and trending event rates. Do you need to consider adjusting your retention settings? Compare to disk space on hosts.



How big are these payloads?

Deployment_info.sh can be used to determine the average payload size. This is a support tool in /opt/qradar/support that should at minimum show the average payload size for each Event Processor that receives data directly or from attached Event Collectors.



How is QRadar's default TCP Maximum Syslog Payload Size configured to?

QRadar will truncate payloads past the maximum length setting configured in Admin > System Settings. Evaluate if larger payloads are coming in from Windows hosts, firewalls, or apps that provide JSON or large URL strings.

2. Defect Inspector - Monthly check

- ❑ Run a monthly check of the defect inspector utility.

Defect inspector is a support tool that compares known stack traces for important issues from your QRadar appliance logs on the Console and creates an output file with known APARs or defect numbers. This file can be provided for support to review at: <https://ibm.com/mysupport>.

```
/opt/qradar/support/defect-inspector
```

3. Software & Firmware updates - Monthly check

- ❑ Run a monthly check of the defect inspector utility.

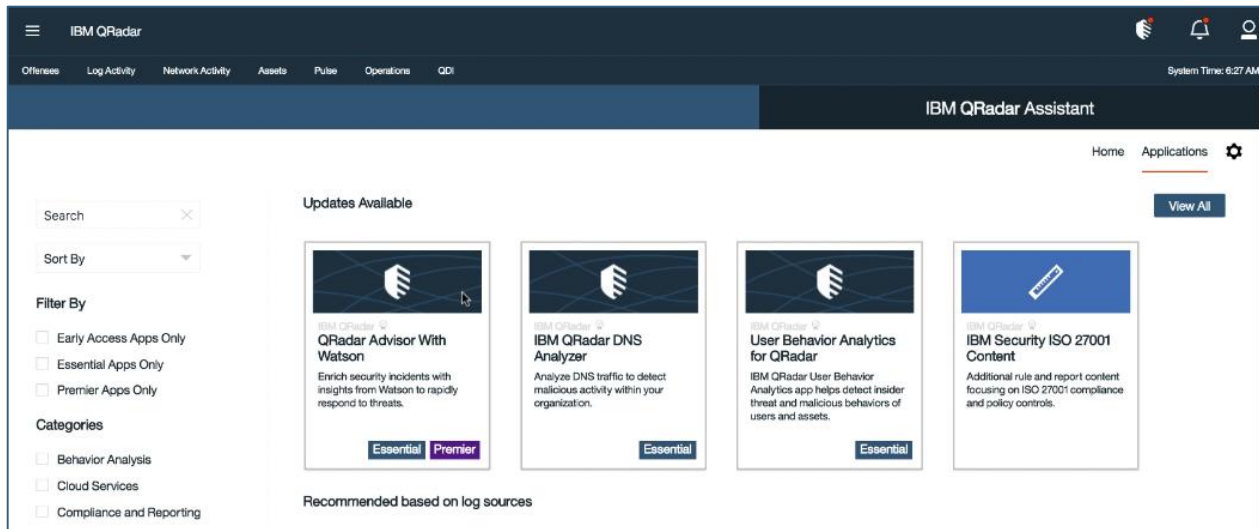
Administrators can review for the latest software and firmware here:

- Software = <https://ibm.biz/qradarsoftware>
- Firmware = <https://ibm.biz/qradarfirmware>

4. Apps and Content Pack Updates - Monthly

- ❑ Verify that you have the latest apps and content extensions installed.

The easiest way to stay informed of new app releases is to ensure you have the latest version of QRadar Assistant installed. The QRadar Assistant App has a API that integrates with the X-Force App Exchange to show updates or recommend new apps.



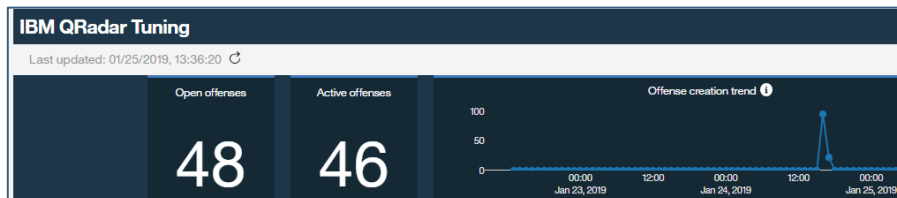
The screenshot displays the IBM QRadar Assistant interface. At the top, there's a navigation bar with 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Pulse', 'Operations', and 'QDI'. The main header reads 'IBM QRadar Assistant' with 'Home' and 'Applications' tabs, and a 'View All' button. On the left, there's a search bar and a 'Filter By' section with checkboxes for 'Early Access Apps Only', 'Essential Apps Only', and 'Premier Apps Only'. Below that are 'Categories' with checkboxes for 'Behavior Analysis', 'Cloud Services', and 'Compliance and Reporting'. The main content area is titled 'Updates Available' and shows four update cards. Each card features the QRadar logo, the app name, a brief description, and a tier label (Essential or Premier). The cards are: 1. 'QRadar Advisor With Watson' (Premier), 2. 'IBM QRadar DNS Analyzer' (Essential), 3. 'User Behavior Analytics for QRadar' (Essential), and 4. 'IBM Security ISO 27001 Content' (Essential). A note at the bottom states 'Recommended based on log sources'.

IMPORTANT: Make sure you have the [QRadar Baseline Maintenance content pack installed](#). This app includes updates for core QRadar rules, searches, custom properties, building blocks, and more that we tune on regular basis.

5. General Tuning - Monthly check

What to evaluate for rules and offenses in QRadar?

- ❑ How many open and active offenses are there in QRadar?
- ❑ Have you used the QRadar Tuning App to identify what is firing most often?
- ❑ Network Hierarchy review completed?
- ❑ Building block review completed?



Tune your QRadar offenses by analyzing rules that cause the biggest number of offenses



Tune most active rules
QRadar Tuning can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.



Tune based on the
The Custom Rules Engine events were generated most about the rule activity. You information from the report

Tune your QRadar offenses by going through the most common configuration steps



Review network hierarchy
Network Hierarchy is used to define which IP addresses and subnets are part of your network. Defining your network hierarchy and keeping it up-to-date is an important step in helping prevent false offenses.



Review building blocks
Rules use information about your servers to detect and generate the rule responses. Review and update building blocks to enable QRadar to discover anomalies on your network, and prevent false positive

Active rules that generate offenses

Filter rules
Time Period: Last 24 Hours
01/03/2019, 16:00 - 01/03/2019, 23:00

Exclude: Closed, Hidden, Inactive, Protected, Follow Up

Percentage of offenses per rule

Rule Category	Percentage
General Audit Events	63.2%
Access Denied	21.1%
Read Activity Attempted	8.28%
Create Activity Attempted	~2.5%
Update Activity Attempted	~2.5%

Total offenses by category/rule

Category	Offenses
General Audit Events	~12
Access Denied	~8
Read Activity Attempted	~3
Create Activity Attempted	~2
Update Activity Attempted	~2

Investigate rules

- 1 Introduction
- 2 AWS Cloud: User Profile ...
- 3 QRadar Tuning demo rule 3

Multiple Login Failures for Single Username

Flowchart showing dependencies: Login Failures Followed By Success to the same Username, Multiple Failed Logins to a Compliance Asset, USA: User Access Login Anomaly, QRadar Tuning demo rule, QRadar Tuning demo rule 2, QRadar Tuning demo rule 3, BB CategoryDefinition: Authentication Failures.

6. Retention Buckets - Monthly

- ❑ Based on disk space requirements and storage, review retention buckets
 - Retention allows users to define the most important data sources to keep when disk space is low. Use retention buckets to optimize your existing storage. Log Source Groups and other filters help you organize what is retained.
 - Retention buckets are pointers to data in /store/ariel when you move buckets existing data at rest will stay in its current bucket, we do not reclassify data that has been processed.

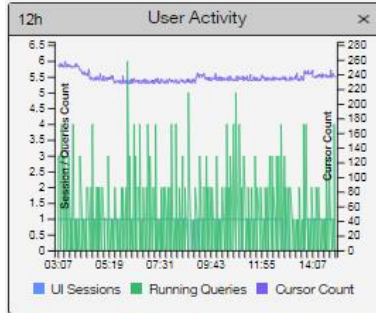
The screenshot shows the 'Retention Properties' dialog box. The 'Name' field is 'SIEM Audit retention'. The 'Keep data placed in this bucket for' is set to '1 year(s)'. The 'Delete data in this bucket' is set to 'Immediately after the retention period has expired'. The 'Description' field is empty. Under 'Current Filters', there is a filter for 'Log Source' with the operator 'Equals'. The 'Log Source Filter' is 'Type to Filter'. A list of log sources is shown: Anomaly Detection Engine-2, Asset Profiler-2, Custom Rule Engine-8, Health Metrics-2, and SIM Audit-2. The selected filter is 'Log Source is SIM Audit-2'. There are 'Remove Selected Filters', 'Save', and 'Cancel' buttons.

7. Custom Properties - Monthly

- Look for expensive custom properties and determine who is creating them and how they can be optimized.

8. Search durations by user - Monthly

- Look for expensive custom properties and determine who is creating them and how they can be optimized.



24h		Top User Roles By Search Activity				
Enter Username to Filter						
Usergroup	Count	Running	Error	Cancelled	Max Duration(s)	Avg Duration(s) ↓
(-) Admin	122430	0	0	0	296.168	0.739
admin	253	0	0	0	296.168	16.668
QDI	122177	0	0	0	77.731	0.116
Total	122430	0	0	0	296.168	0.151

24h		Expensive Custom Properties	
Hostname	Custom Properties	EPS	
pl71	SIM Audit	1000	
pl71	System Notification	1000	

9. Review for coalesced log sources - Monthly

- Coalescing preserves storage by looking at payloads with the same core characteristics and combining them down to a single event payload (34), where 34 is the number of coalesced payloads associated to the event. Audit and compliance events should likely have coalescing disabled. There is a system setting to globally disable coalescing for auto discovered event sources.

Planning for the future



1. Rule Performances – Planning for the future

❑ Do you have QRadar 7.3.2 to use the rule performance visualization feature?

Performance	Rule Name	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	Creation Date	Modification Date
	Destination Asset Weight is High	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:33...	Dec 5, 2018, 6:03...
	Local Mass Mailing Host Detec...	Post-Intrusion Acti...	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jan 12, 2006, 7:03...	Dec 5, 2018, 6:03...
	Login Failures Followed By Su...	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	1,312,281	1	System	Jun 29, 2010, 6:38...	Dec 5, 2018, 6:03...
	Source Address is a Known Q...	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:41...	Dec 5, 2018, 6:03...
	Source Address is a Bogon IP	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:44...	Dec 5, 2018, 6:03...
	AssetExclusion: Exclude NetBI...	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 6, 2014, 4:02...	Dec 5, 2018, 6:03...
	Login Failures Followed By Su...	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jul 13, 2010, 2:42...	Dec 5, 2018, 6:03...
	AssetExclusion: Exclude DNS ...	Asset Reconciliati...	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 6, 2014, 3:58...	Dec 5, 2018, 6:03...
	Source Asset Exists	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:25...	Dec 5, 2018, 6:03...
	Chained Exploit Followed by S...	Intrusion Detection	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jul 14, 2010, 5:10...	Dec 5, 2018, 6:03...
	Excessive Firewall Denies fro...	Recon	Custom Rule	Event	True	Dispatch New Event	0	0	System	Nov 29, 2005, 8:1...	Dec 5, 2018, 6:03...
	Multiple Exploit Types Against ...	Intrusion Detection	Custom Rule	Event	True	Dispatch New Event	0	0	System	Jun 22, 2006, 9:50...	Dec 5, 2018, 6:03...
	Source Asset Weight is Medium	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:30...	Dec 5, 2018, 6:03...
	Destination Asset Exists	Magnitude Adjust...	Custom Rule	Common	True		0	0	System	Mar 10, 2010, 3:26...	Dec 5, 2018, 6:03...
	__genyrule		Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:46...	Dec 6, 2018, 4:46...
	__genyrule2		Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:57...	Dec 6, 2018, 4:59...
	__genyrule3		Custom Rule	Event	True		0	0	User	Dec 6, 2018, 4:57...	Dec 6, 2018, 4:59...

Rule
 Apply Local Mass Mailing Host Detected on events which are detected by the Local system
 and NOT when an event matches any of the following BB:HostDefinition: Mail Servers, BB:HostReference: Mail Servers
 and when the event(s) were detected by one or more of Flow Classification Engine
 and when any of these BB:CategoryDefinition: Mail Policy Violation with the same source IP more than 20 times, across more than 1 destination IP within 1 minutes
 and when the event context is Local to Remote

Notes
 Reports a local host sending more than 20 SMTP flows in 1 minute. This may indicate a host being used as a spam relay or infected with a form of mass mailing worm.

Performance Analysis 4 minutes ago

Capacity
 Lowest: 1,099,840 EPS
 Average: 1,099,840 EPS

Lowest Capacity Host Details
 Hostname: ip-125-89 (172.18.125.89)
 Appliance Type: 3199
 License EPS Capacity: 5,000 EPS
 Appliance Capacity: 30,000 EPS

2. Considerations further in to the year

- Do you have season event/flow traffic coming up in the future?

QRadar has add-on, flexible licensing that can help account for future traffic volume. Have you completed a review for non-security payloads that can be dropped to save license capacity?

- When do your certs expire?

It is helpful to keep a list of certificates that expire for your organization. This help prevents outages and data collection gaps in QRadar.

- When do your event sources change passwords / expire passwords?

It is always a good idea to understand the cycle of user passwords, especially if you are not the administrator responsible for the changes.

Questions and Answers

- Use the Q&A panel to ask questions of the panelists!
- If you have questions after the session has ended, you can talk to us in the QRadar forums: <https://ibm.biz/qradarforums>.





Resources

- ❑ [QRadar Troubleshooting and System Notifications Guide](#)
- ❑ [QRadar Deployment Intelligence v2](#)
- ❑ [QRadar Tuning App](#)
- ❑ [QRadar Assistant App](#)
- ❑ [QRadar Support 101](#)
- ❑ [WinCollect 101](#)
- ❑ [QRadar Forums](#)



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.