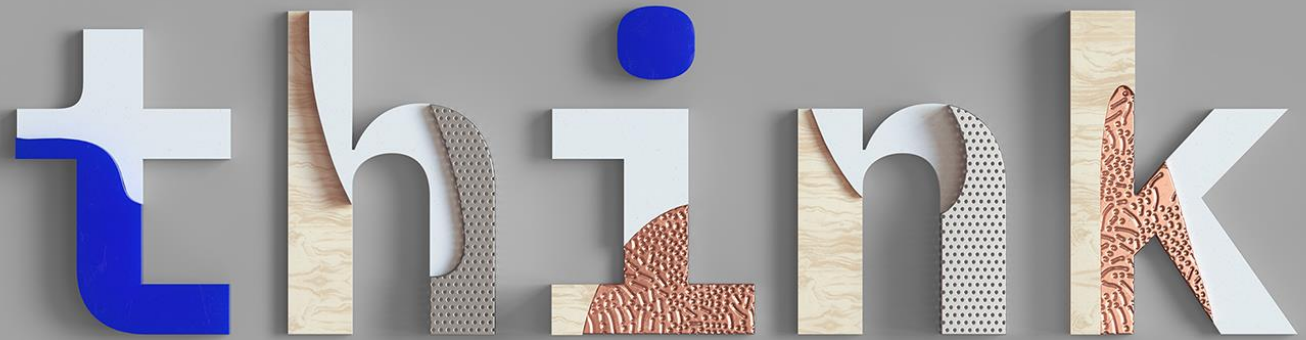
QRadar 7.3.2 Feature Discussion

think 2019

-

Matthew Carle
QRadar Offering Management
&
Jonathan Pechta
QRadar Support Content Lead



Please note

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

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.** The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.
.

Contents

Part 1
Platform Updates in QRadar 7.3.2

App Hosts (formerly QRadar App Nodes)

What is the same?

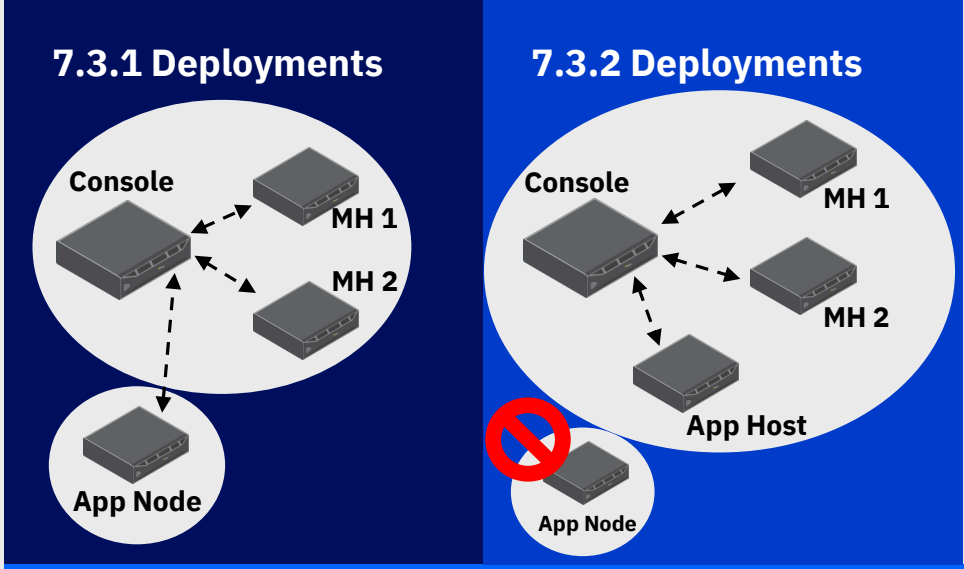
From an architecture perspective, the App Host is identical to the functionalist of an App Node.

- App Hosts be physical, virtual, or software. Installs are completed with the QRadar 7.3.2 ISO file.
- Purpose built to hosts all apps in the deployment and remove processing load from the Console. (appliance ID = 4000).

What is different?

App Host has been rebuilt from the ground up to stabilize the whole process of running apps in QRadar.

- Fully managed and patched as part of QRadar software update process.
- Admins are no longer required to manage the OS.
- Supports standard deployment capabilities, such as backup & restore and High Availability.



- App Nodes are no longer supported from 7.3.2 and forward. If an App Node is present during the 7.3.2 upgrade, users will be instructed to replace it with an App Host. Apps can be migrated after the App Host is installed.
- A new 80% memory limitation is in place when you migrate to an App Host. Available memory utilization was previously 100% for App Nodes.
- Entitlement for App Nodes comes from Q1PD.

Introducing App Host (formerly QRadar App Node)

Where are app migrations managed?

Admin > System and License Management

System and License Management - Mozilla Firefox

Allocate License to System | Upload License | Actions ▼ | Deployment Actions ▼ | Search....

Display Syst

▼ **Deployment Details**

Event Limit	30000/15000	Users	2
Flow Limit	600000/300000		

▼ **Apps are running on the App Host**

There are currently no migrations so migration status cannot be retrieved
Click to change where apps are run

▼ **License Information Messages**

▼ **System Support Activities Messages**

Transferring Apps

Transfer Apps and Data to the Console this may take some time.
Apps will be unavailable during the transfer.

Please do not perform the following actions while a migration is underway:

Installing / Uninstalling other apps,
A full deploy,
A restore,
Deletion of app host or
Re-IP of Console.

The Apps are running on **Console**.
Do you want to transfer to **App Host**?

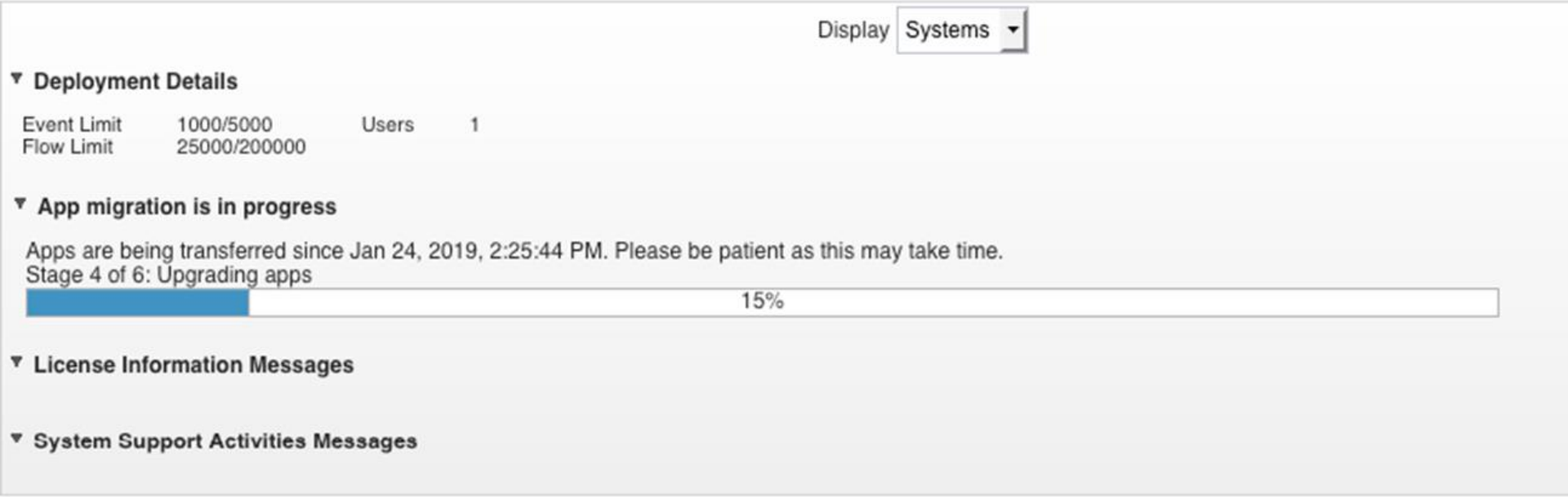
Console | **Cancel**

Host Name	Host IP	Appliance Type	Version	Serial Number	Host Status	License Expiration Date	License Status	Event Rate Limit	F

Introducing App Host (continued)

Apps that are migrated to the app host are moved and updated without impact to customer data. Apps that are being migrated to the App Host appliance cannot be used until the migration is complete. A progress bar indicates the current status of the app migration.

NOTE: App Hosts have the same minimum system requirements as App Nodes.



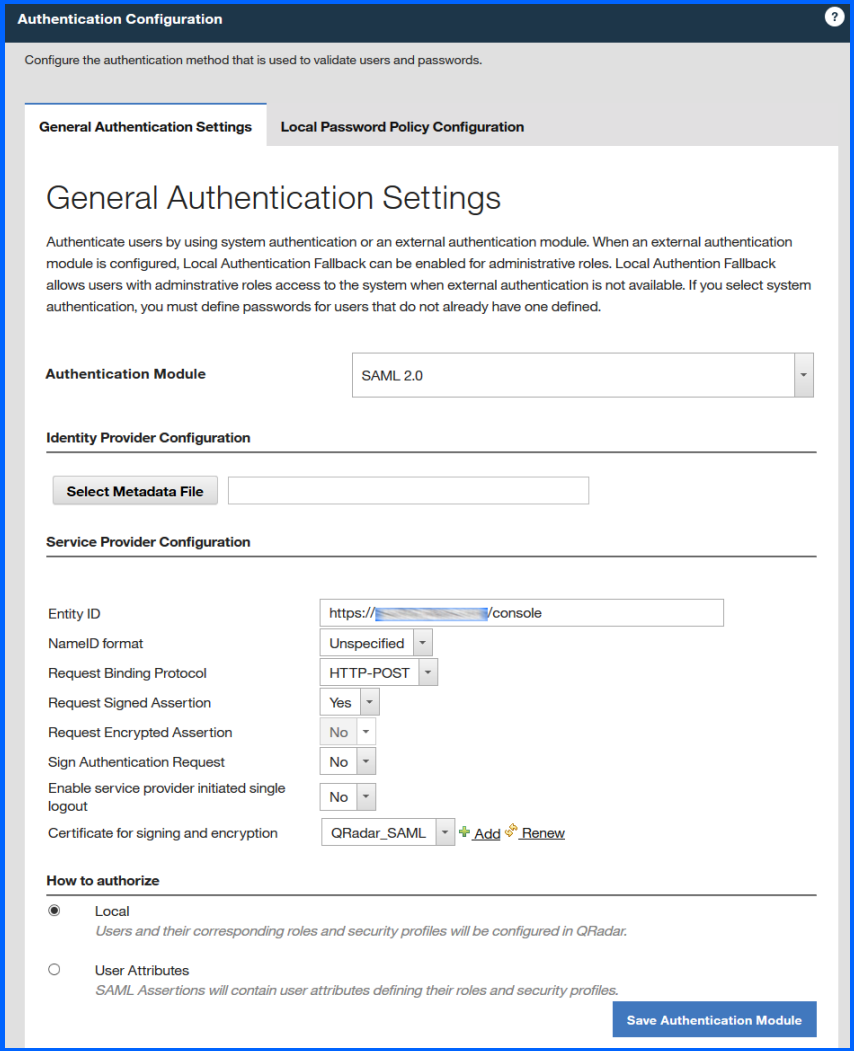
Security Assertion Markup Language (SAML) 2.0

What's new?

- QRadar starts supporting SAML 2.0 single sign on authentication (WEB SSO profile) from 7.3.2.
- Easy to integrate with organization-wise single sign on solution in a standard way.
- SAML 2.0 SSO web profile requires no direct server to server connection.
- Fully support QRadar initiated or identity provider initiated single sign on/sign off.

Why?

Enterprise Single Sign-On, two/multi-factor authentication, CAC Cards. These are all solutions administrators look to in order to secure and manage authentication to enterprise infrastructure. QRadar 7.3.2 introduces support for SAML 2.0 to allow administrators to choose the best of breed technology for identity management and apply those same technologies to govern authentication and authorization within the QRadar platform.



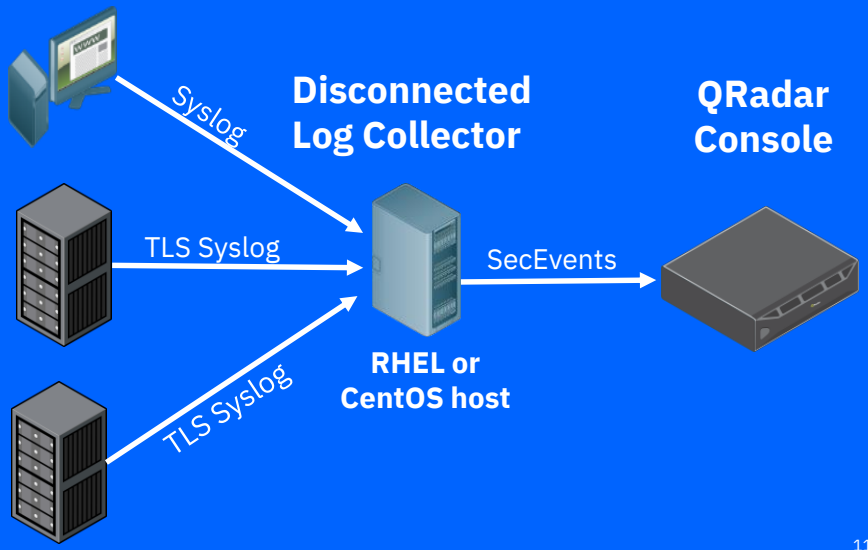
New - Disconnected Log Collector (DLC)

In the 7.3.2 timeframe we introduce the QRadar DLC, which mirrors a number of powerful capabilities of our 15XX Event Collector and removes deployment restrictions. No longer does an administrator need full virtual infrastructure or even stand alone, purpose build appliance. A simple RPM install on existing RHEL or CentOS infrastructure can provide almost all of QRadar's event collection capabilities. Uses a Universal DSM and the 'IBM QRadar DLC Protocol' when you configure log sources.

- Entitled to all QRadar customers
- RPM can install on any CentOS or RHEL host
- No EPS license – simply collects and forwards data
- Supports all Syslog sources
- Compressed backhaul of traffic over:
  - TCP/TLS
  - UDP

What is in store for 2019?

- Continuous delivery of protocols
- Configuration entirely from within QRadar
- Disconnected Log Collector (DLC) Chaining



Data Obfuscation – Multi-tenant Environments

QRadar's data obfuscation capabilities allow administrators to strategically "hide" and restrict visibility to PII data within shared environments.

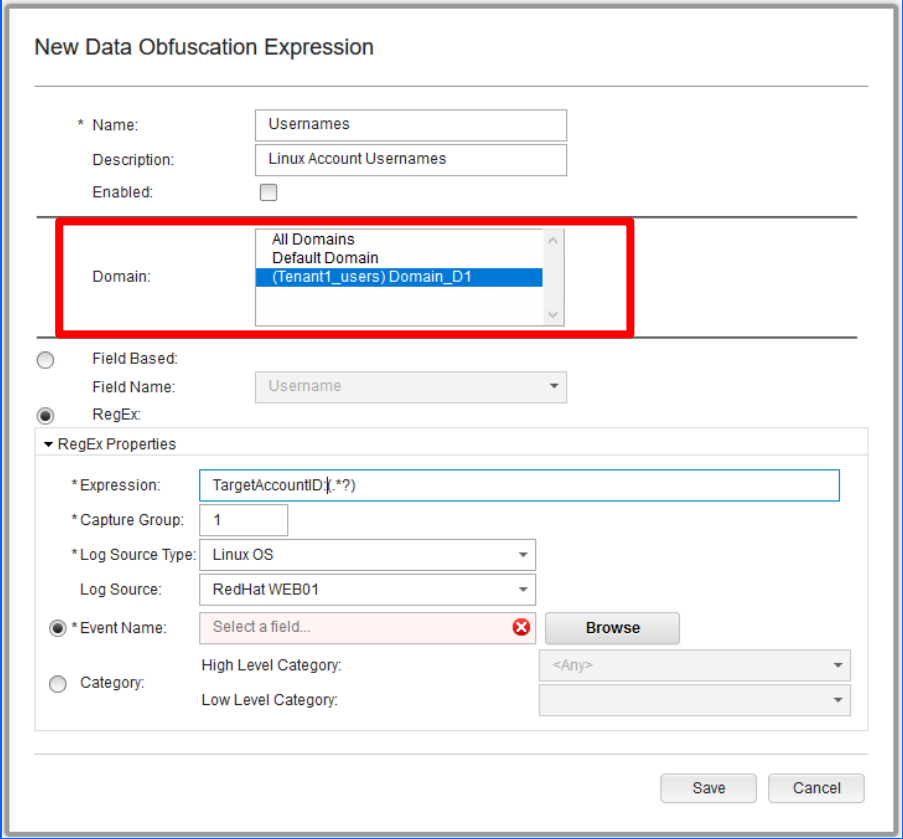
What's new in 7.3.2?

Data obfuscation can now be configured on a per-tenant or domain basis as **(Tenant)Domain**.

Why?

There is a need to balance security with the privacy of individuals. Ensuring this privacy is arguably even more important in the world of MSSPs where the analyst is not even from the same company as the people he/she may be investigating.

There is no doubt that in security, visibility into the who, what, when, where and why is critically important for analysts to fully understand the situation that they are dealing with.



VLAN Segmentation for Multi Tenant Environments

What's New?

QRadar 7.3.2 provides QRadar administrators the ability to mirror VLAN segmentation of traffic directly into the QRadar domain and tenant framework.

Administrators can now map Enterprise and Customer VLAN IDs directly to a domain/tenant level within QRadar. After the VLANs are defined, QRadar will separate the flow data being collected (NetFlow, QFlow and QNI) and enforce QRadar's data access controls (Security Profiles)

Why?

Shared network infrastructure is commonplace in data centers world wide. Numerous tenants leveraging the same wires to communicate with each other as well as with the open internet.

Low Level Category	Unknown Flow
VLAN ID	100
Post VLAN ID	101
Dot1q VLAN ID	100
Dot1q Priority	0
Dot1q Customer VLAN ID	0
Dot1q Customer Priority	0
Post Dot1q VLAN ID	102
Post Dot1q Customer VLAN ID	1
Dot1q DEI	true
Dot1q Customer DEI	false
Flow Direction Algorithm	Arrival time (3)
Application Determination Algorithm	Unknown (1)
Enterprise VLAN ID	100
Customer VLAN ID	0
Domain	Default Domain

VLAN segmentation provides network administrators the ability to isolate these tenants from each other and provide secure logical networks on which they can operate.

Enhanced clarity into MPLS flows from IPFIX data

What's new?

- We now have the ability to filter and search for IPFIX flows in QRadar that contain MPLS fields and write rules based on the values of these MPLS fields.
- These MPLS fields are now available for searching and filtering.
- The MPLS stack can contain up to 10 layers where each layer shows information about the flow routing.

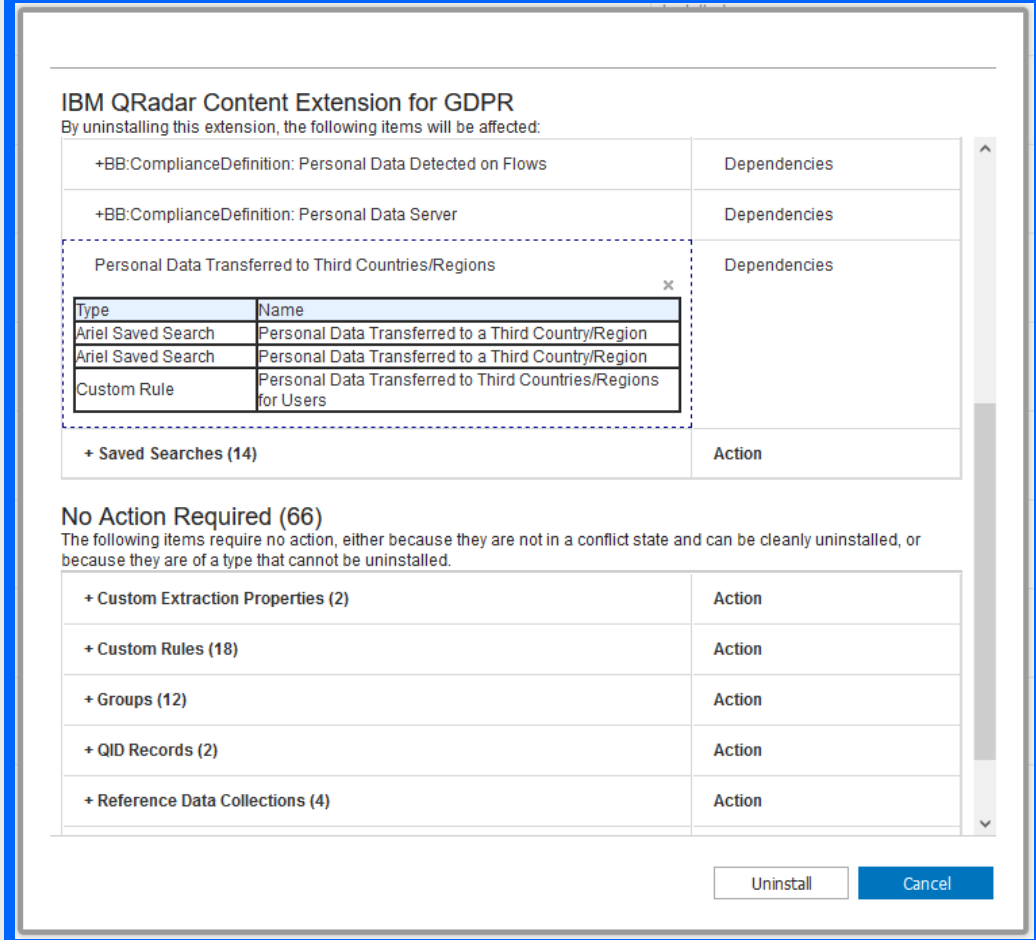
An IPFIX flow is exported from a switch on a network that uses MPLS (Multiprotocol Label Switching) and this export contains information about the MPLS stack, which is now categorized and stored as part of the flow in QRadar.

MPLS Top Label IPv4 Address	10.0.0.3
MPLS Label 1 (Top Label)	Label Value: 1; Experimental Use: 001; Bottom of Stack: 0 (0x000012)
MPLS Label 2	Label Value: 2; Experimental Use: 001; Bottom of Stack: 0 (0x000022)
MPLS Label 3	Label Value: 3; Experimental Use: 001; Bottom of Stack: 0 (0x000032)
MPLS Label 4	Label Value: 4; Experimental Use: 001; Bottom of Stack: 0 (0x000042)
MPLS Label 5	Label Value: 5; Experimental Use: 001; Bottom of Stack: 0 (0x000052)
MPLS Label 6	Label Value: 6; Experimental Use: 001; Bottom of Stack: 0 (0x000062)
MPLS Label 7	Label Value: 7; Experimental Use: 001; Bottom of Stack: 0 (0x000072)
MPLS Label 8	Label Value: 8; Experimental Use: 001; Bottom of Stack: 0 (0x000082)
MPLS Label 9	Label Value: 9; Experimental Use: 001; Bottom of Stack: 0 (0x000092)
MPLS Label 10	Label Value: 10; Experimental Use: 001; Bottom of Stack: 1 (0x0000a3)
MPLS VPN Route Distinguisher	0101010101010101
MPLS Top Label Prefix Length	4
MPLS Top Label IPv6 Address	102:304:506:708:90a:b0c:d0e:f10
MPLS Payload Length	255
MPLS Top Label TTL	7
MPLS Label Stack Length	30
MPLS Label Stack Depth	10
MPLS Top Label Exp	1
Post MPLS Top Label Exp	1

Enhanced Content Management

What's New?

- Uninstalling apps will remove all associated content (or note required dependencies) to prevent orphaned rules, searches, reports, custom properties, groups, QIDs, dashboards, etc.
- Content relationships are more strongly managed to prevent deletions from content accidentally.
- A preview window now shows what is to be uninstalled or skipped and what interim changes will be lost.
- The uninstallation dialog shows a retrospective of what happened to the content owned by the application when the uninstall has finished.



Incremental EPS/FPM Licensing

What's new?

- With incremental licensing, you can now acquire stackable EPS and FPM increments instead of replacing the overall QRadar Console license.
- These stackable licenses can be temporarily or permanent EPS/FPM expansions that get auto allocated to the QRadar Console.
- Multiple stackable licenses can be applied.
- License allocation can be added temporarily and will notify users 35 days in advance (not new).
- Administrators can reallocate the event or flow capacity by using the existing License Pool Management tool to allocate EPS to Event or Flow Processor appliances (not new).

Until I finish {X} project, I need…

- 2,500 EPS
- 5,000 FPM

Where {X} is a special project, tuning, network merge, seasonal requirement, new firewalls, etc….

Why?

Increasing EPS or Flow rates meant that an existing license needed to be replaced and the operation group (Q1PD) had to get the customer's license request to understand the request.

EPS/Flow increases can be added to the new license to streamline requests or get you through short windows of high EPS. For example, retail environments during Black Friday or Singles' day.

Installation, DrQ Health check framework, & Security

What is DrQ?

An extensible health check framework which will check the QRadar system against a knowledgebase of globally known defects.

When to run DrQ?

- Before major events, such as upgrades, to determine whether there are any issues that need to be addressed first.
- Routinely to monitor the health of your system!

What runs now?

With the release of QRadar 7.3.2, DrQ runs 9 tests that were created to check for common update issues.

For example:

- File permissions
- Disk space
- User and group permissions
- Contents of config files
- Presence of files
- systemd unit properties

What's the future?

The capability to create and run your own DrQ check in the deployment.

A scripting language will be available in the 7.3.2 timeframe for administrators to leverage to customize your own deployment checks.

Running DrQ

Output of the test conditions include the pass fail conditions of the tests completed.

Optionally, individual tests can be run that include success conditions, failure conditions, and a basic remediation procedure for administrators or support representatives.

QRadar weekly auto updates can deploy new tests to expand on the capabilities of the health checks.

```
[root@csd~]# drq
DrQ version 1.0.1 (mode: checkup, tag(s): <none>, verbosity: summary)

[SUMMARY] 9 successful checkups
[SUMMARY] 0 failed checkups
[SUMMARY] 0 invalid files
[SUMMARY] 0 skipped files

[root@csd~]#
```

```
[root@csd~]# drq -f /opt/ibm/si/diagnostiq/deploymentXmlInGlobalConfigCheck.lua -v
DrQ version 1.0.1 (mode: checkup, tag(s): <none>, verbosity: verbose)

DeploymentXml In Global Config Check
  Ensures that deployment.xml does not exist in ConfigServices globalconfig
  directories
     [SUCCESS]
         The file /store/configservices/deployed/globalconfig/deployment.xml
         does not exist.
     [FAILURE]
         The file /store/configservices/staging/globalconfig/deployment.xml
         exists.
        [REMEDIATION]
           The proper location for deployment.xml is
           /store/configservices/staging/deployment.xml.  The invalid file in
           /store/configservices/staging/globalconfig/deployment.xml should be
           merged with the correct one if needed then removed.

[SUMMARY] 0 successful checkups
[SUMMARY] 1 failed checkup
[SUMMARY] 0 invalid files
[SUMMARY] 0 skipped files

[root@csd~]#
```

Installation and Virtual Machine Updates

Kernel-based Virtual Machine (KVM)

- Must be a software install. The administrator provides RedHat OS, then installs QRadar on top of the OS.
- Appliance installs (booting from QRadar ISO) are not supported due to differences in disk drivers.
- Only supported on CentOS/RedHat 7.5 with QEMU KVM 1.5.3-141.

Microsoft Hyper-V

- Must be a software install. The administrator provides RedHat OS, then installs QRadar on top of the OS.
- Appliance installs (booting from QRadar ISO) are not supported due to differences in disk drivers.
- Only supported on Windows Server 2016 (Hyper-V plugin) with all Windows updates applied.

Red Hat 7.5 is the default operation system version in QRadar 7.3.2

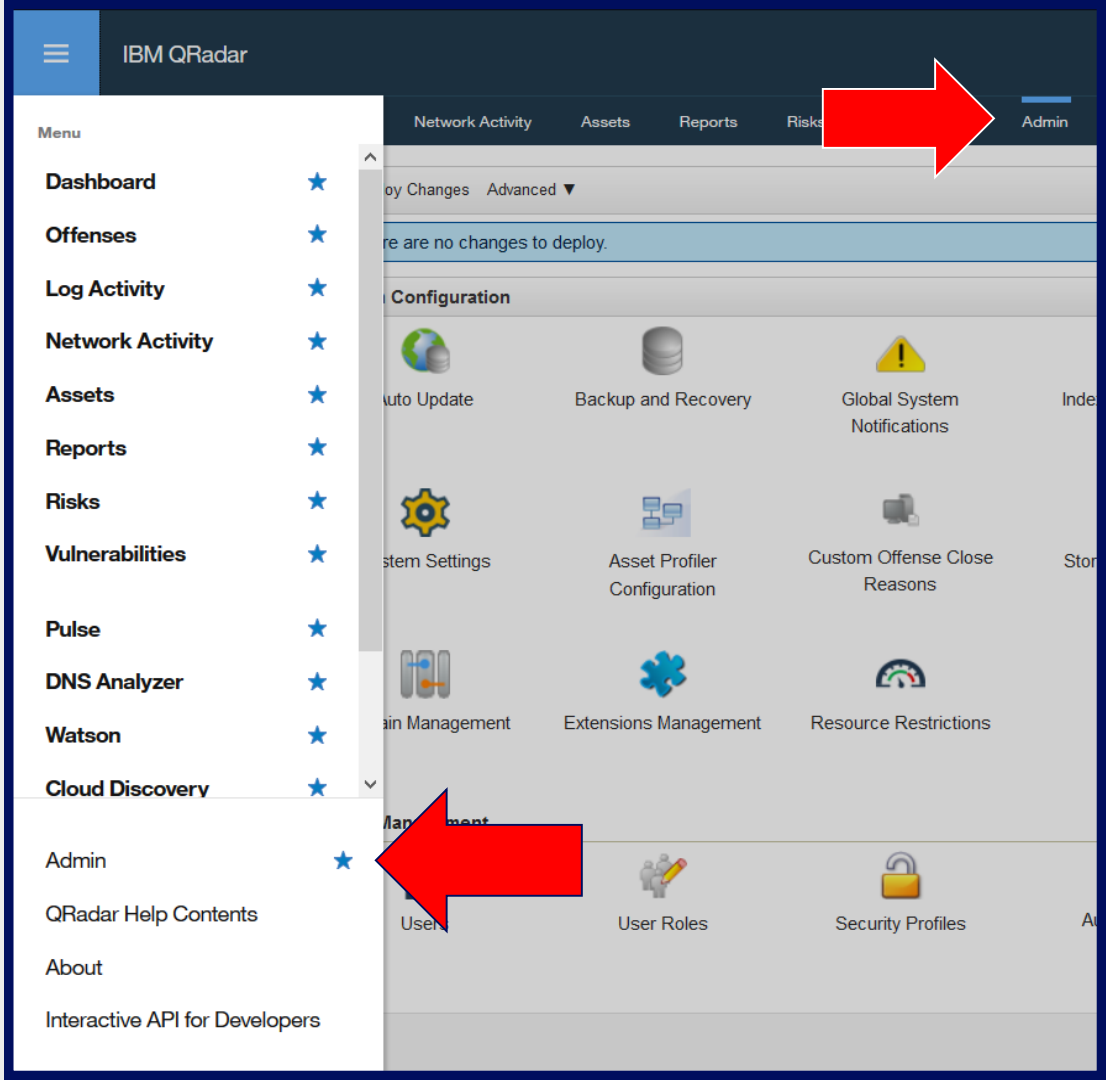
- Required as base OS for software installs of 7.3.2
- Updated for several reasons:
  - Security Updates
  - Support new Dell hardware
  - Fixes an issue with Lenovo hardware introduced in Red Hat 7.4

Part 2
User Interface and Usability in QRadar 7.3.2

The Admin tab can be assigned as a favorite

What's New?

The Admin tab can now be marked as a favorite and can be conveniently accessed from QRadar as a menu tab.



Rule Performance Visualization

Display: Rules | Group: Select a group... | Groups | Actions ▼ | Revert Rule | Search Rules... | View the IBM App Exchange for more...

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**

Rule Performance Visualization (continued)

What's New?

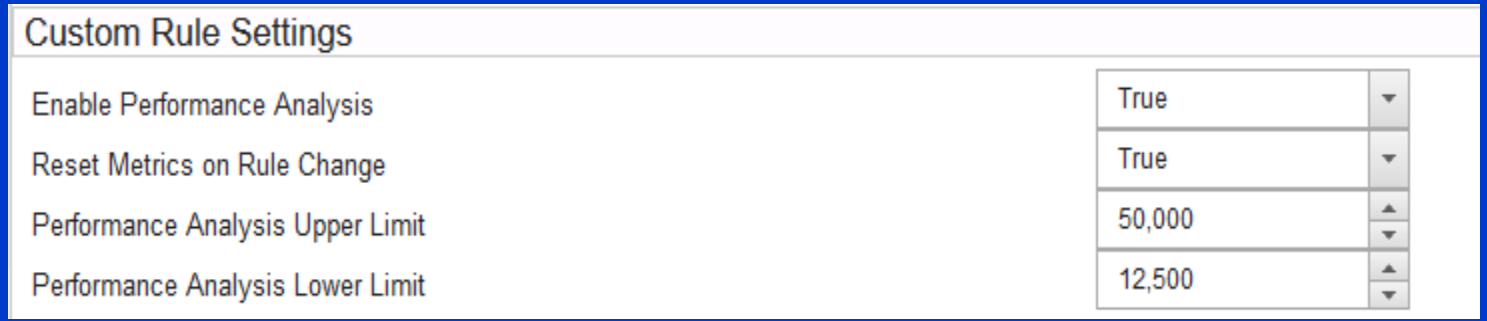
- Administrators can define a global performance upper/lower limit and rules are evaluated by their throughput in the QRadar pipeline.
- Users can sort rules by their performance in the user interface and identify expensive rules.
- Hover text in the user interface shows the performance metrics for the evaluated rule.

Why?

- Users had no easy way in the interface to view or understand the relative performance of their rules.
- Users could not easily identify rules that have performance issues.

How do I enable this feature?

Admin > System Settings > Advanced > Custom Rule Settings



Rule Performance Visualization (continued)

When does analysis run?

Analysis runs when performance degradation has been noticed in the processing pipeline if it has been enabled as a System Setting.

If a rule is edited, the analysis can be reset based on the System Setting defined by the administrator.

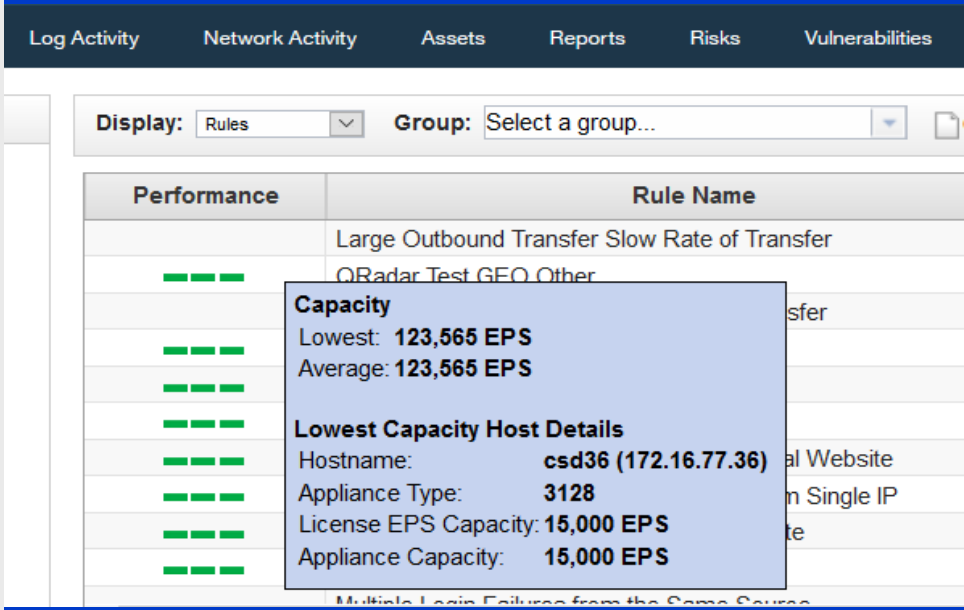
Throughput visualization

Performing above the upper EPS limits

Performing within the existing limits

Underperforming and throughput is below the lower defined limit.

User Interface Hover Details



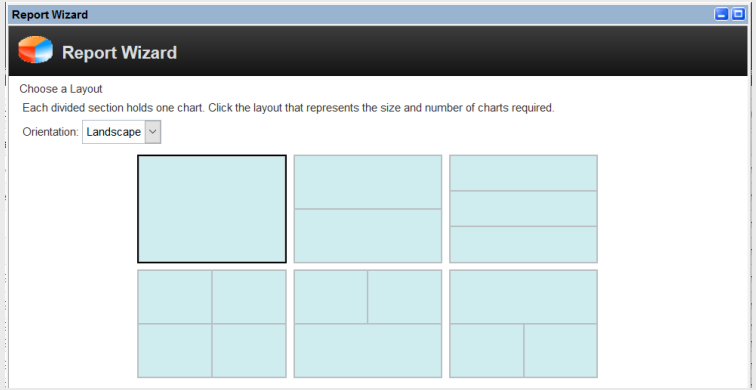
Can a rule performance be toggled manually?
Yes, support has a command-line string that can be entered to force a rule performance analysis.

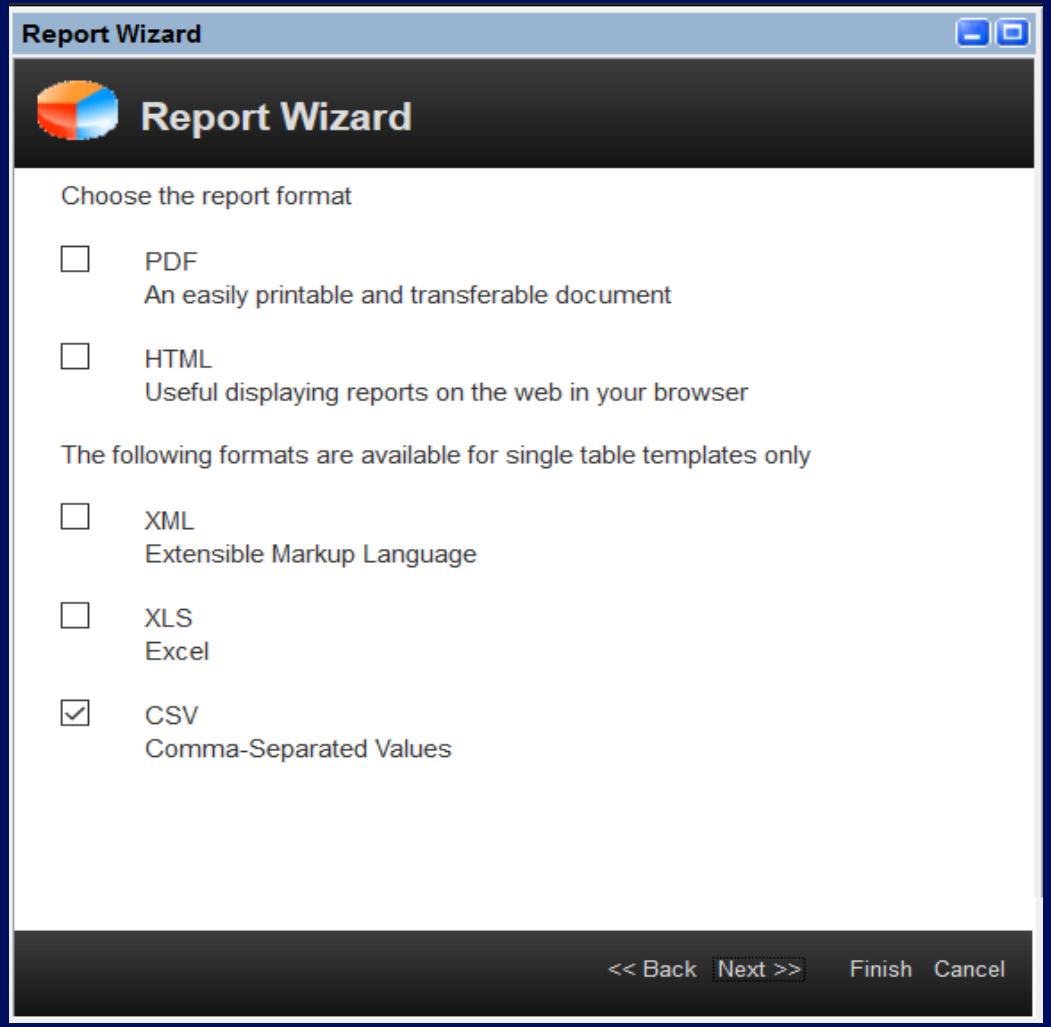
Reporting - CSV File Format Option

What's New?

You can now export reports by selecting a CSV file format for reports that use single table templates.

In previous version of QRadar, reports could have only been exported in XML and XLS format for single table templates.





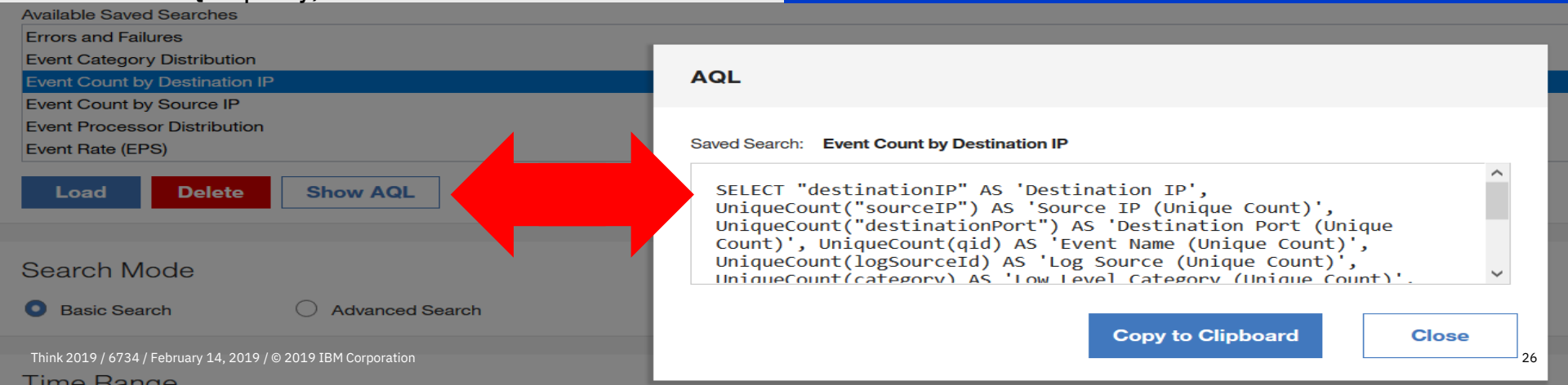
Saved Searches – Show AQL Option

What's New?

- View the associated for any Log/Network Activity saved search.
- Create searches faster than by typing the search criteria.
- Use this AQL string to create your own searches, as QRadar converts the saved search to an AQL string.
- Run a saved search by using the API ID of the search (Previously, you ran a saved search only with an AQL query)

Why?

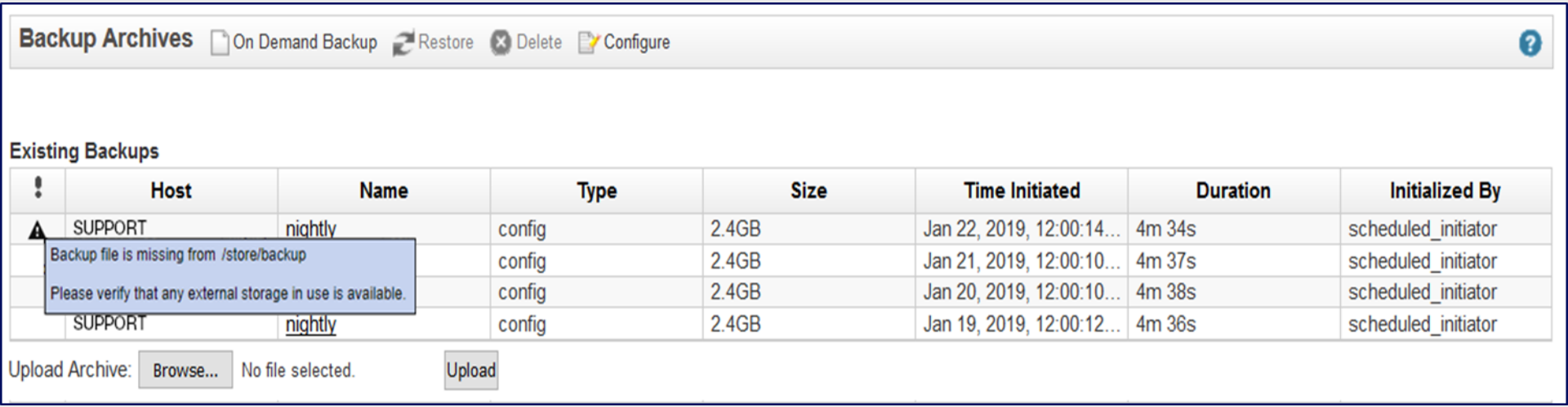
- This will allow users who are learning AQL to gain a better grasp of AQL functions and fields.
- Provide seasoned users the ability to quickly convert basic searches to AQL and leverage more advanced features without rewriting the search from scratch.



Improved Management for Backup Files

Missing backup files are now detected and flagged in the QRadar user interface for the Console and managed hosts in the deployment. If your external storage becomes unavailable for a period, the risk of inadvertently deleting backup files is reduced.

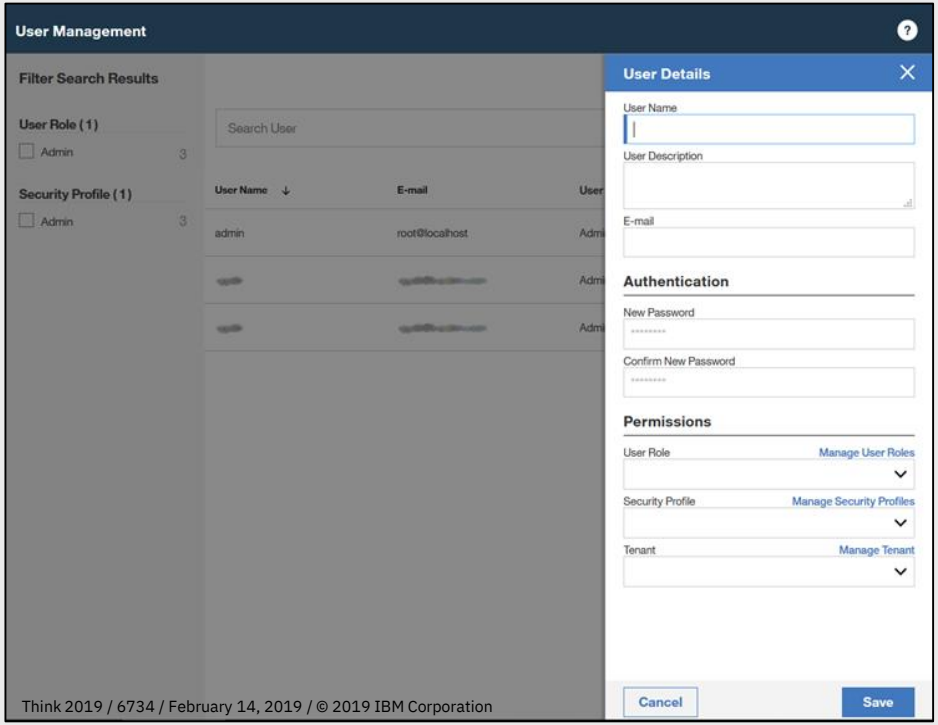
Now, the backups that are listed on the Backup and Recovery page are flagged as missing if they are not found. If files were intentionally deleted by a QRadar administrator from the command line, the administrator can remove backups that are listed on the Backup and Recovery page with the Delete option.



!	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

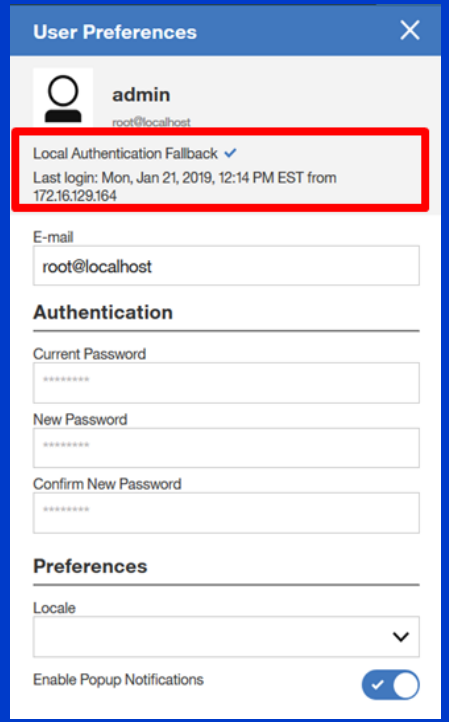
User Management Facelift

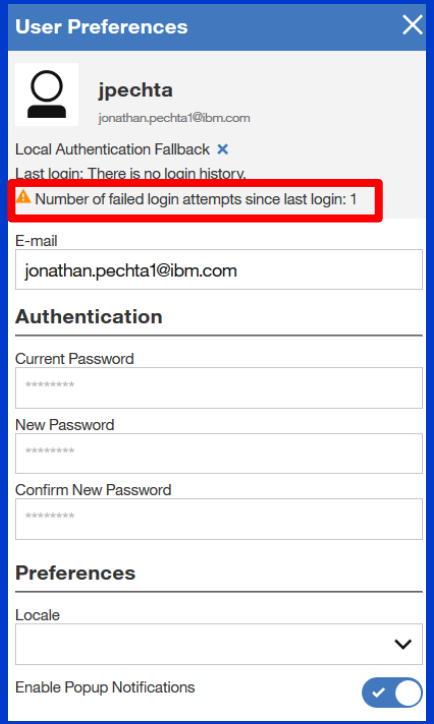
A streamlined User Management interface from the Admin tab allows for better management of QRadar users, such as creating and updating user accounts.



What's new?

- Enhanced User Preferences
- Login History and Failed Accesses





User Management Facelift (continued)

Password policy rules set in QRadar are displayed in the user password area for Local Authentication users.

Authentication Configuration

Configure the authentication method that is used to validate users and passwords.

General Authentication Settings | Local Password Policy Configuration

Local Password Policy Configuration

Password policy settings apply only to local (not external) passwords. When the policy is updated, users are prompted to change their password if they log in with a password that does not meet the new requirements.

Password Complexity

Minimum Password Length	5
Use Complexity Rules	✓
Number of rules required	2
Contain an uppercase character	✗
Contain a lowercase character	✓
Contain a digit	✓
Contain a special character (e.g. &, -, ,)	✗
Not contain repeating characters	✗
Password History	✓
Unique password count	8
Days before password will expire	90

Login History and Failed Accesses

Local password rules are listed in the user preference area.

User Details

User Name
jpechta

User Description
Jonathan (Support)

E-mail
jonathan.pechta1@ibm.com

Authentication

New Password
****

Your Password must include

At least 5 characters
At least one lowercase character
At least one digit character

Strength Tip

Don't reuse passwords between sites.
Don't use your name, email, address, etc.

Reference Data Expiration Messages

What's new?

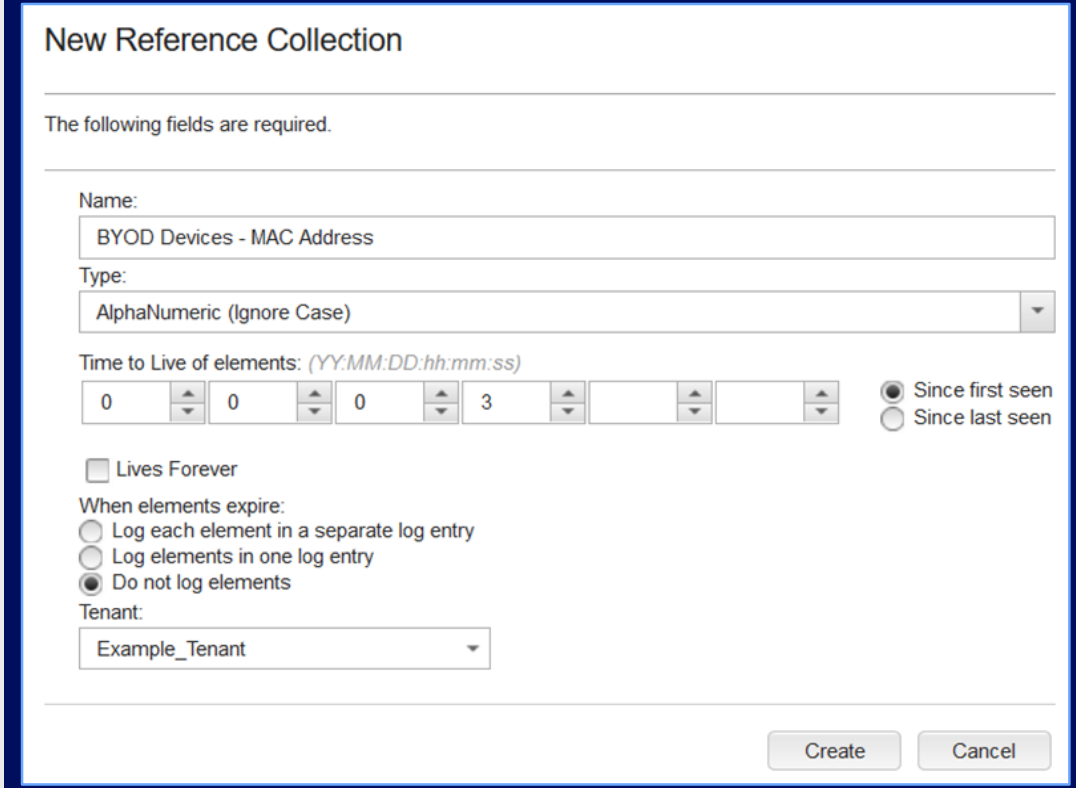
Administrators are now allowed to define what reference sets log expiration of data in the logs. This feature allows users to reduce log clutter, reduce log rotation, and less I/O usage.

Why?

To provide more flexibility to administrators to either audit these changes in more detail or to allow admins to ignore certain expiring reference data.

New options available in the user interface and `/opt/qradar/bin/ReferenceDataUtil.sh`

Note: This feature was backported to QRadar 7.3.1 versions.



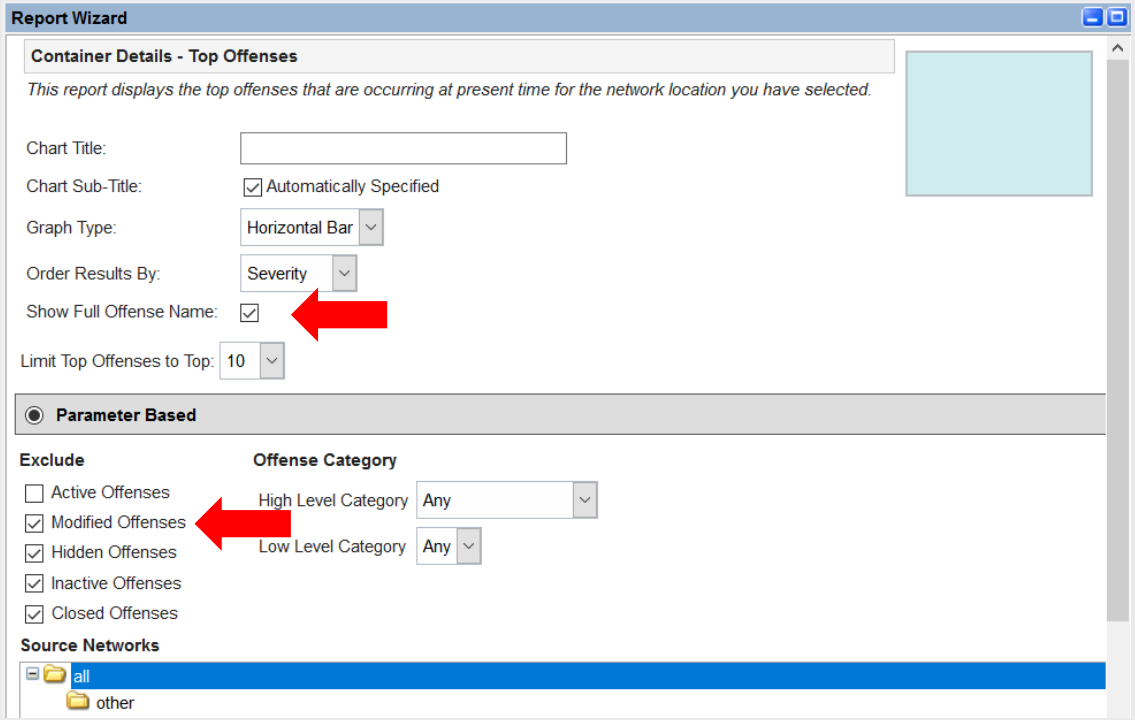
Additional Platform Updates

New Audit Record Creation

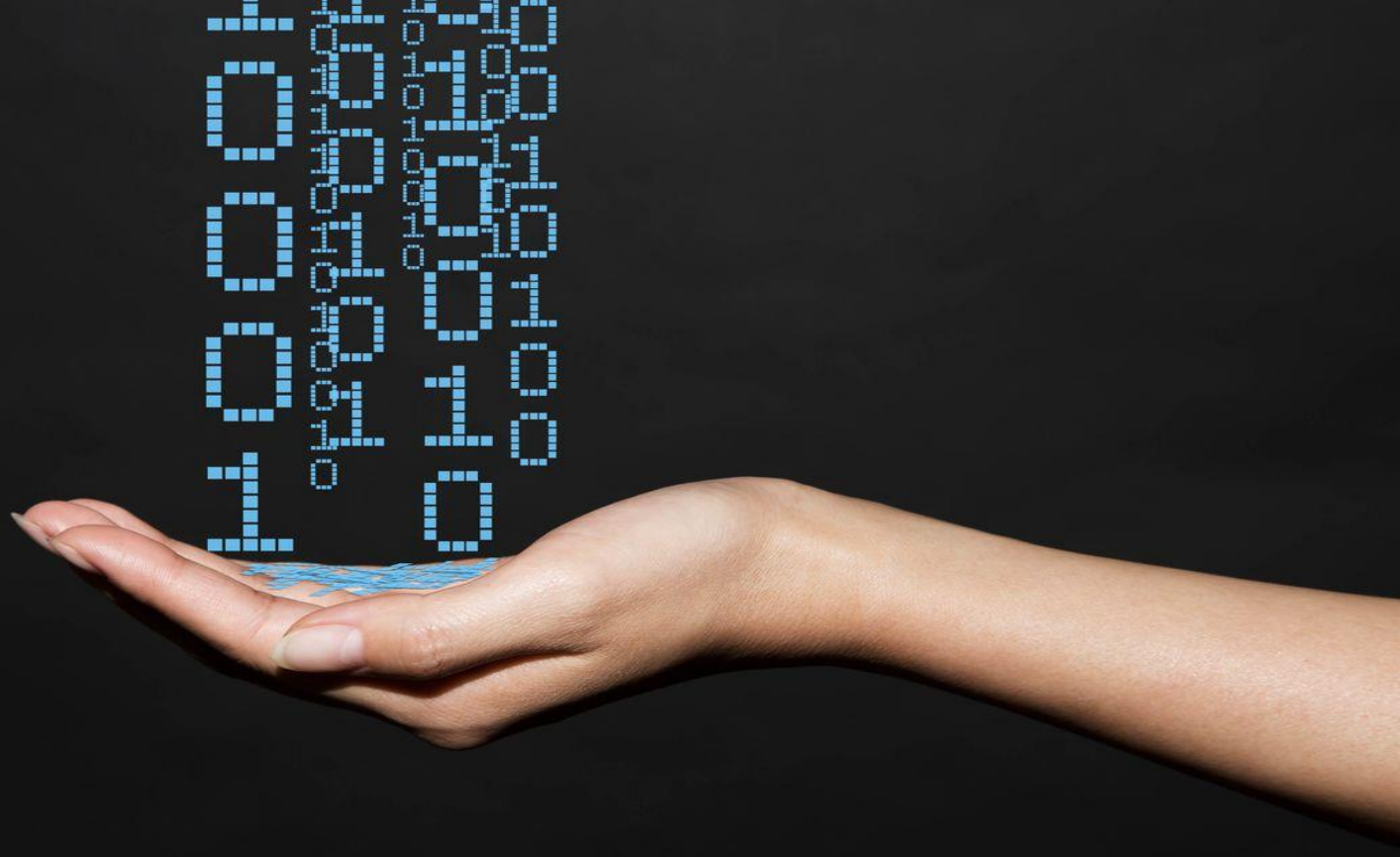
When an offense is created, it triggers an audit event with QRadar Identifier (QID) 28250369, which can be used by QRadar searches, filters, and rule test conditions.

Enhanced Offense Reporting Templates

Ability to choose extra options, such as ability to display full offense names in offense reports and include modified offenses when creating offense reports. These new options give you more visibility into the offenses that are in the report depending on your update version.



Part 3
Data Ingestion



Traffic Analysis & Custom Log Sources

What's New?

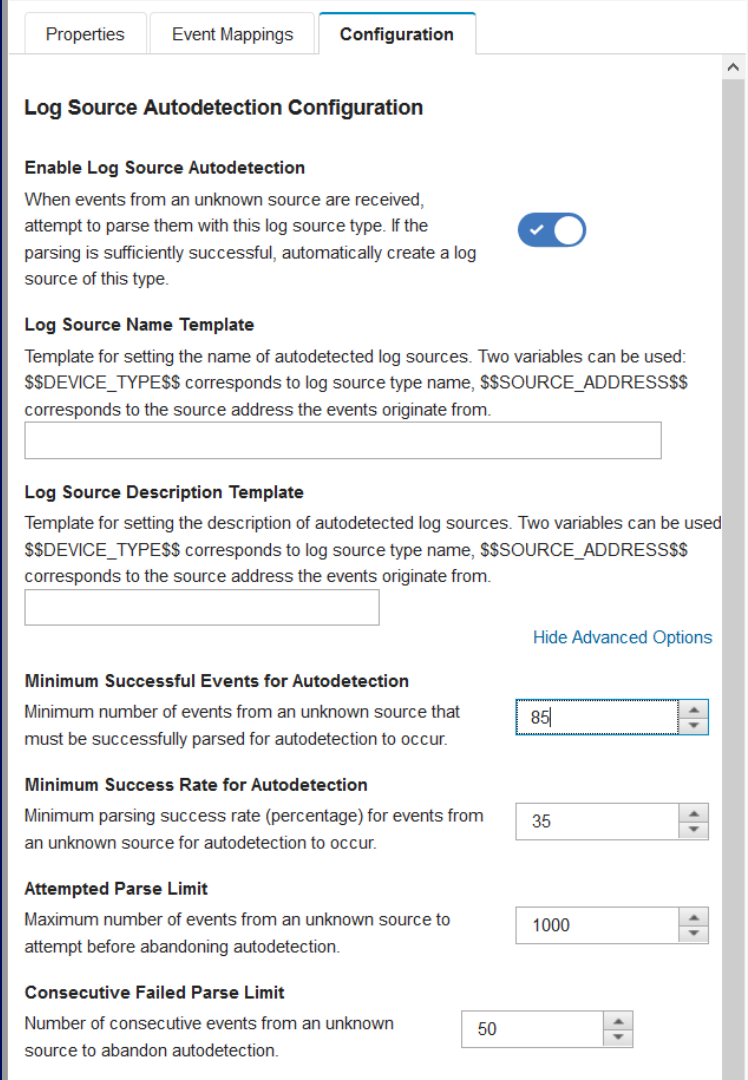
- The DSM Editor supports the creation of custom Log Source Types.
- Customizations of standard Log Source Types will also contribute to Traffic Analysis (TA).
- This feature is coupled with the ability to turn auto-discovery of log-source on/off for any Log Source Type in the DSM Editor user interface.

Why?

Auto-discovery of log sources was unavailable for Custom Log Source Types.

Where?

Admin tab > DSM Editor > Configuration



New LEEF and CEF autodetection available

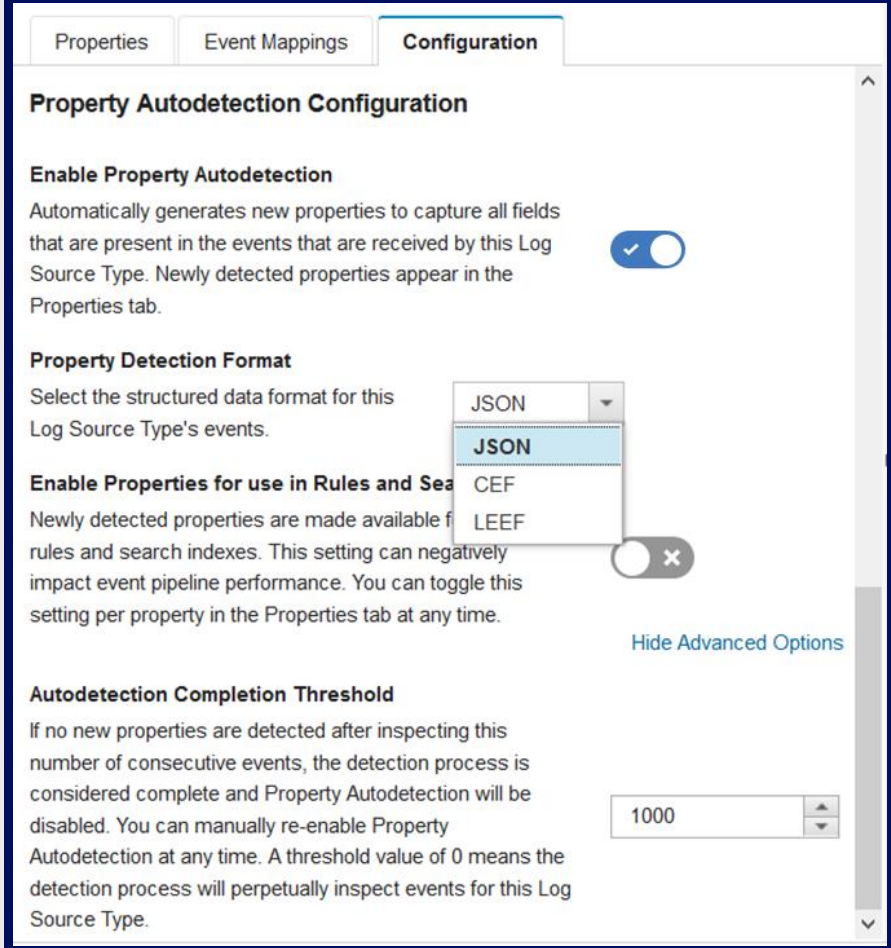
Continuing our push to simplify data ingestion, our development teams have updated the process of getting LEEF and CEF data into QRadar and make this functionality fully searchable. In fact, we have pretty much trimmed the whole process down to two steps:

1. Tell QRadar that you would like to auto-discover the properties for this feed.
2. Get the data in to QRadar: Syslog, flat files, you name it… just get the data into QRadar.

Step 1 is as easy as changing an existing DSM that supports CEF or LEEF, via the DSM Editor.

Step 2, you configure a log source within QRadar and get the data flowing. Within seconds, QRadar will evaluate the incoming data feed and produce custom properties for each field within the event data.

With one extra step, users can quickly update the DSM parsing as well by simply copying the auto discovered property definition. No need to write REGEX patterns or worry about ingestion of LEEF or CEF formatted data.



LEEF and CEF Field Extraction for Custom Properties

IBM QRadar

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | DNS A

Tuning

Return to Event List | Offense | Map Event | False Positive | Extract Property

Payload Information

utf | hex | base64

☑ Wrap Text

```
Feb  5 09:24:41 127.0.0.1  [Thread-50]
[172.16.77.21/- -] [-/- -]LEEF:1.0|QRad
DeploymentID=477ef476-f52b-11e8-ada8-ec
ComponentName=hostcontext        devTime
Element=sda     Value=4.4
```

Additional Information

Protocol	255
Log Source	Health Metrics-2 :: csd36
Custom Rules	Source Asset Weight is Low BB:CategoryDefinition: Source IP is a Third Country/Region Source Asset Exists Destination Asset Weight is Low Context is Local to Local

Custom Event Property Definition - Mozilla Firefox

Property Expression Definition

Enabled: ☑

Selection

Log Source Type: Healt

Log Source Filter: Search

Log Source: Healt

◉ Event Name: Health Metric Browse

○ Category: High Level Category System

Low Level Category Information

Extraction using LEEF Key

LEEF Key ComponentName ✓

Test

Save

Text matching your expression has been highlighted in the payload:
hostcontext

OK

Part 4
APIs

QRadar v10 (7.3.2) API Endpoints

QRadar introduces the v10 API with new endpoints and user interface updates, such as a version filter.

API Documentation

Home

API Version: 10.0

- access
- analytics
- ariel
  - databases
  - event_saved_search_groups
  - flow_saved_search_groups
  - flow_vlans
  - functions
  - lookups
  - parser_keywords
  - processors
  - saved_search_delete_tasks
  - saved_search_dependent_tas
  - saved_searches
  - searches
  - taggedfields
  - validators
- asset_model
- auth
- config
- data_classification
- forensics

GET

10.0 - GET - /ariel/saved_searches

Last modified in API version: 10.0

Description

Retrieves a list of Ariel saved searches.

Response Description

An array of Ariel Saved Search objects. An Ariel Saved Search object contains the following fields:

- **id** - Long - The ID of the Ariel saved search.
- **uuid** - String - The uuid of the Ariel saved search.
- **name** - String - The name of the Ariel saved search.
- **database** - String - The database of the Ariel saved search, events or flows.
- **isShared** - Boolean - True if the Ariel saved search is shared with other users.
- **owner** - String - The owner of the Ariel saved search.
- **aql** - String - The AQL query.
- **description** - String - The description of the Ariel saved search.
- **isAggregate** - Boolean - True if the Ariel saved search is an aggregate search.
- **isDashboard** - Boolean - True if the Ariel saved search is in the dashboard.
- **isDefault** - Boolean - True if the Ariel saved search is default search.
- **isQuickSearch** - Boolean - True if the Ariel saved search is default search.

QRadar v10 (7.3.2) API Endpoints

Application Framework Health Monitoring API

- /api/config/platform/metrics

Ariel Saved Searches API

- /api/ariel/saved_searches/
- /api/ariel/searches/

EULA Acceptance API

- /api/system/eulas
- /api/system/eula_acceptances

Auto-detection Configuration API

- /api/config/event_sources/log_source_management/autodetection/config_records

Event Ariel Property CEF Expression API

- /api/config/event_sources/custom_properties/property_cef_expressions

Event Ariel Property LEEF Expression API

- /api/config/event_sources/custom_properties/property_leef_expressions

QRadar 7.3.2 API Endpoints (continued)

Flow VLAN API

- /api/ariel/flow_vlans

Hosts API

- /api/config/deployment/

Locale API

- /api/system/information

Login Attempts API

- /api/access/login_attempts

Name Service Registration

- /api/gui_app_framework/named_services/registration

QNI Stacking Configuration

- /api/qni/stacking

QRadar 7.3.2 API Endpoints (continued)

Risk Management API

- /api/qrm/

Users API

- /api/config/access/users
- /api/config/access/users/{id}/dependents
- /api/config/access/user_dependent_tasks
- /api/config/access/user_dependent_tasks/{task_id}/results
- /api/staged_config/access/users
- /api/staged_config/access/user_delete_tasks
- /api/system/authorization/password_validators

User Roles API

- /api/config/access
- /api/staged_config/access

Thank you

Matthew Carle
Program Director QRadar Offering Management and Strategy
—
mcarle@ca.ibm.com
+1-506-449-5555

Jonathan Pechta
QRadar Support Content Lead
—
jonathan.pechta1@ibm.com
+1-470-554-4666

Your Feedback is Important!

Access the Think 2019 Conference Attendee Portal to complete your session surveys from your smartphone, laptop or conference kiosk.