

QRadar braindump

15. März. 2017

Karl Jaeger



Pro4bizz GmbH

<https://www.pro4bizz.de>

karl.jaeger@pro4bizz.de

0721-909 81 720

Agenda

- SIEM Markt und Einführung QRadar
- IBM Training und Zertifizierung
- QRadar Dokumentation
- IBM Fix Central und Installationsschritte
- Demo VM
- Betrieb QRadar
- Einbindung in IT Infrastruktur
- Einbindung in Workflow
- QRadar Architektur und Plattformen
- SIEM Sizing
- QRadar Finetuning
- Logs & Flow (Datenquellen, Netzwerkinfrastruktur)
- Alarme & Regeln
- System Monitoring (Beispielalarme)
- Trouble Shooting
- IBM Service Request
- High Availability

SIEM Markt

- Gartner MQ August 2016
 - Leaders: IBM, HPE, EMC, Splunk, Intel Security, LogRhythm
 - Challengers: EMC
 - Visionaries: AlienVault
- Hype/Top
 - APT / Cyberdefense
 - RM / VM
 - Forensik
 - HP TAP
 - Know How
 - NG SIEM
 - Fireeye HX/NX

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (August 2016)

Einführung QRadar & Marktüberblick

2017-p4b-IT-Sicherheit

ITSiG: Ziel, Inhalt und Herausforderung

P4B SIEM und Q1Labs 2017

Q1 Training

- **IBM Security QRadar SIEM 7.2 Foundations**

https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=course_description&cc=&courseCode=BQ102G

- **IBM Security QRadar SIEM 7.2 Administration and Configuration (Advanced)**

https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=course_description&cc=&courseCode=BQ150G

Q1 Zertifizierung



Industries & solutions Services Products Support & downloads My IBM

Search



IBM Professional Certification Program

Certify your skills. Accelerate your career.

Overview

Products

Certifications

Tests

Mastery Tests

About the Program

Process

By Number

By Unit

Pricing

Updates & Revisions

Test Info

Test Series Changes

Test C2150-612: IBM Security QRadar SIEM V7.2.6 Associate Analyst

Overview

Objectives

Test preparation

Sample / Assessment Test

Sample Test

[Sample Test for Test C2150-612](#)

Assessment Test

To assess your current skill level and readiness for **Test C2150-612 - IBM Security QRadar SIEM V7.2.6 Associate Analyst**, you can take a Web-based assessment test.

Passing this assessment test does not result in achieving a credential. It is designed to provide diagnostic feedback on the Examination Score Report, correlating back to the test objectives, showing how you scored on each section of the test.

- Number of questions: 54
- Time allowed in minutes: 90
- Passing score: 66%
- Language: English

Promotions



Testing Policies

Take a minute to review our testing policies and guidelines, and registration process.



Register for a Test

Register for an IBM Certification test at Pearson VUE and take a step into your future. Take a minute to review how to [Create Pearson VUE account](#) associated with IBM and [Selecting Tests on](#)

Q1 Dokumentation

IBM QRadar Security Intelligence Platform Version 7.2.6



Quick Start Guide

This guide gets you started with a typical installation.

National Language Version: To obtain the Quick Start Guide in other languages, print the language-specific PDF from the installation media.

Product overview

IBM® QRadar® Security Intelligence Platform products provide a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics, and configuration and vulnerability management. This Quick Start Guide provides information about installing IBM Security QRadar appliances.

1 Step 1: Access the software and documentation



Review the [release notes](#) for the QRadar component you want to install.

Download the ISO for your QRadar component from the [IBM FIX Central](#) website.

Q1 Dokumentation

References:

- *IBM Security QRadar SIEM Users Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar SIEM Administration Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar Log Sources User Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar WinCollect User Guide* <http://ibm.co/1wvpSEE>
- *IBM Security QRadar Adaptive Log Exporter Users Guide* <http://ibm.co/1wvpSEE>
- Microsoft Windows Management Instrumentation
<http://technet.microsoft.com/en-us/library/ee692942.aspx>
- *IBM Security QRadar Vulnerability Assessment Configuration Guide* <http://ibm.co/1wvpSEE>

DSM Configuration Guide (b_dsm_guide.pdf)

IBM Fix Central



IBM Support > Fix Central >

Fix Central

[http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/
com.ibm.qradar.doc/t_siem_vrt_ap_inst_iso.html](http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/t_siem_vrt_ap_inst_iso.html)

Fix Central stellt Fixes und Updates für Software, Hardware und Betriebssystem Ihrer Umgebung bereit. Sie suchen nicht nach Fixes oder Updates? Besuchen Sie [Passport Advantage](#), um beliebte Softwareprodukte herunterzuladen oder [Unterstützung für meine berechtigten Systeme](#), um Systemsoftware herunterzuladen.

Klicken Sie für weitere Informationen auf den folgenden Link.

[Einführung zu Fix Central](#)

Produkt finden

Produkt auswählen

Wählen Sie unten das Produkt aus.

Wenn Sie mithilfe der Tastatur auf der Seite navigieren, verwenden Sie die Taste **Alt** und die **Abwärtspfeiltaste**, um zu den Auswahllisten zu gelangen.

Produktgruppe*

IBM Security

Auswählen aus IBM Security*

IBM Security QRadar SIEM

Installierte Version*

7.2.0

Plattform*

Linux

Fix Central
durchsuchen [Tipps](#)



Mein Produktprotokoll

- IBM Security QRadar SIEM (7.2.0, Linux)
- IBM Domino (9.0.17, Windows)
- IBM Domino (9.0.15, Windows)
- IBM Domino (Alle, Alle)
- Lotus Notes Traveler (9.0.1, Linux)

Kontakt und Feedback

Q1 installation steps

- download des iso image von
- <https://www-945.ibm.com/support/fixcentral/>
- dort QRadar als Produkt auswählen
- dann wählen Sie das entsprechende ISO Image, zB QR 7.2.8 als Basis aus und installieren darauf den entsprechenden fixpack, also 7.2.8 patch1
- zum installieren wird der activation key der VM benötigt
- Lizenz wird automatisch für 30 Tage generiert


Demo VM

- Prerequisites Demo VM
- Recommended hardware and software requirements for each demo VM
- VMware Workstation 9 or above, or equivalent ESXi/vSphere
- min. 2 core CPU
- min. 24 GB available RAM (32GB empfohlen)
- Solid state drive (SSD) with 100GB available space


here we go...



IBM Knowledge Center

 IBM QRadar Security Intelligence Platform > IBM QRadar Security Intelligence Platform 7.2.7 > Installing > QRadar installations > Installing the QRadar software on a virtual machine

Installing the QRadar software on a virtual machine

Version 7.2.7 



After you create your virtual machine, you must install the IBM® Security QRadar® software on the virtual machine.

Before you begin

Ensure that the activation key is readily available.

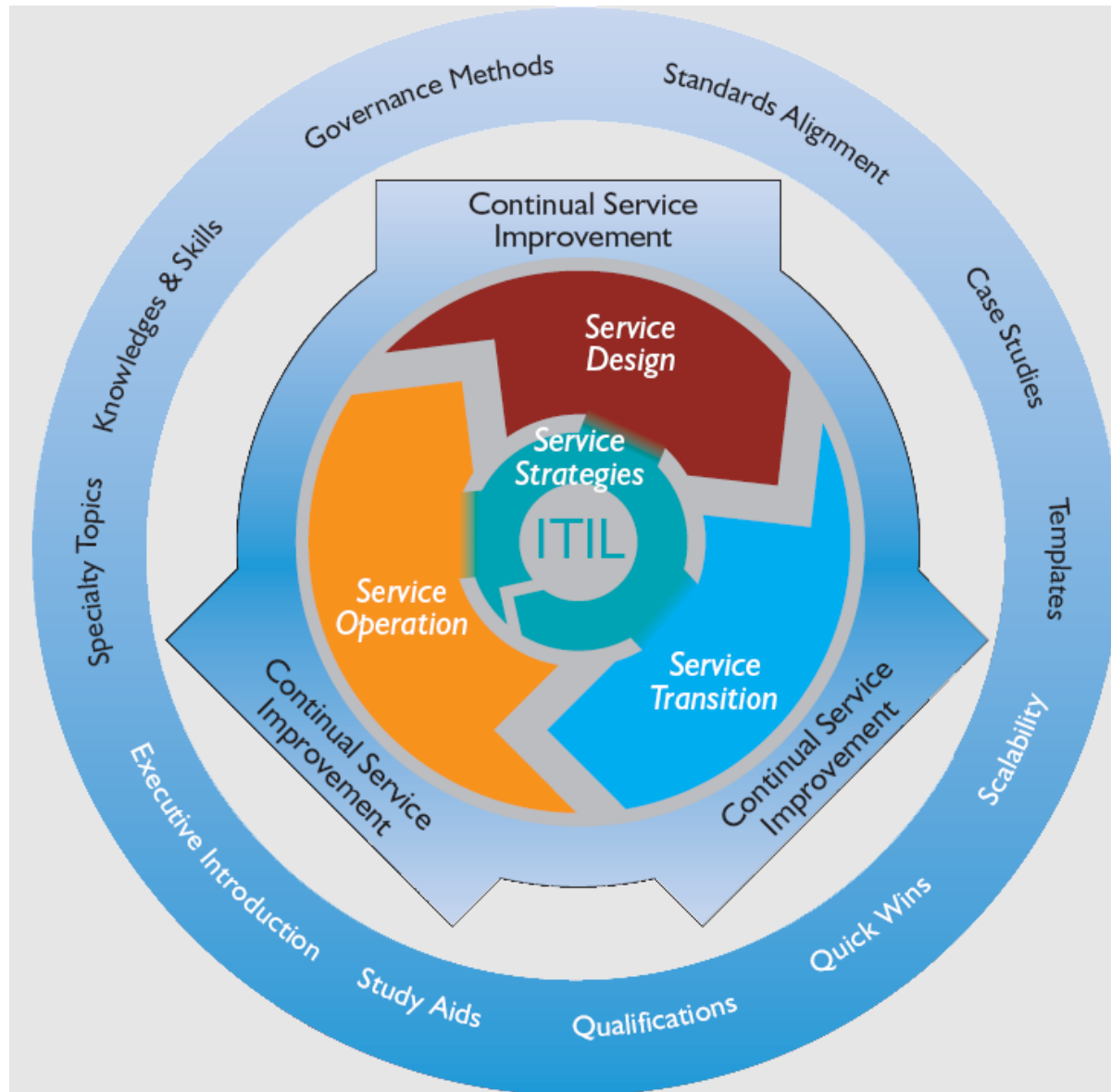
Procedure

1. In the left navigation pane of your VMware vSphere Client, select your virtual machine.
2. In the right pane, click the **Summary** tab.
3. In the **Commands** pane, click **Edit Settings**.
4. In the left pane of the **Virtual Machine Properties** window, click **CD/DVD Drive 1**.
5. In the **Device Type** pane, select **DataStore ISO File**.
6. In the **Device Status** pane, select the **Connect at power on** check box.
7. In the **Device Type** pane, click **Browse**.
8. In the Browse Datastores window, locate and select the QRadar product ISO file, click **Open** and then click **OK**.
9. After the QRadar product ISO image is installed, right-click your virtual machine and click **Power > Power On**.
10. Log in to the virtual machine by typing `root` for the user name.

Betrieb Qradar

- **Infrastrukturmgmt**
 - DNS intern
 - CMDB
 - Namenskonzept
 - Netzwerkkonzept
- **Best Practice**
 - Change Mgmt
 - Patch Mgmt
 - Security Mgmt (Incident Handling, CERT, NOC)
 - Risk Mgmt
- **ITIL Prozesse**
 - Service Operation
 - Continuous Service Improvement

ITIL v3



Einbindung in IT Infrastruktur

- Rekursives DNS
- CMDB import oder autodiscovery via Flow
- Netzwerkhierarchie (notfalls aus Regelwerk)
- Syslog forwarder (may need IP spoofing)
- DMZ
- BBs

Einbindung in SI Workflow

Offense Workflow

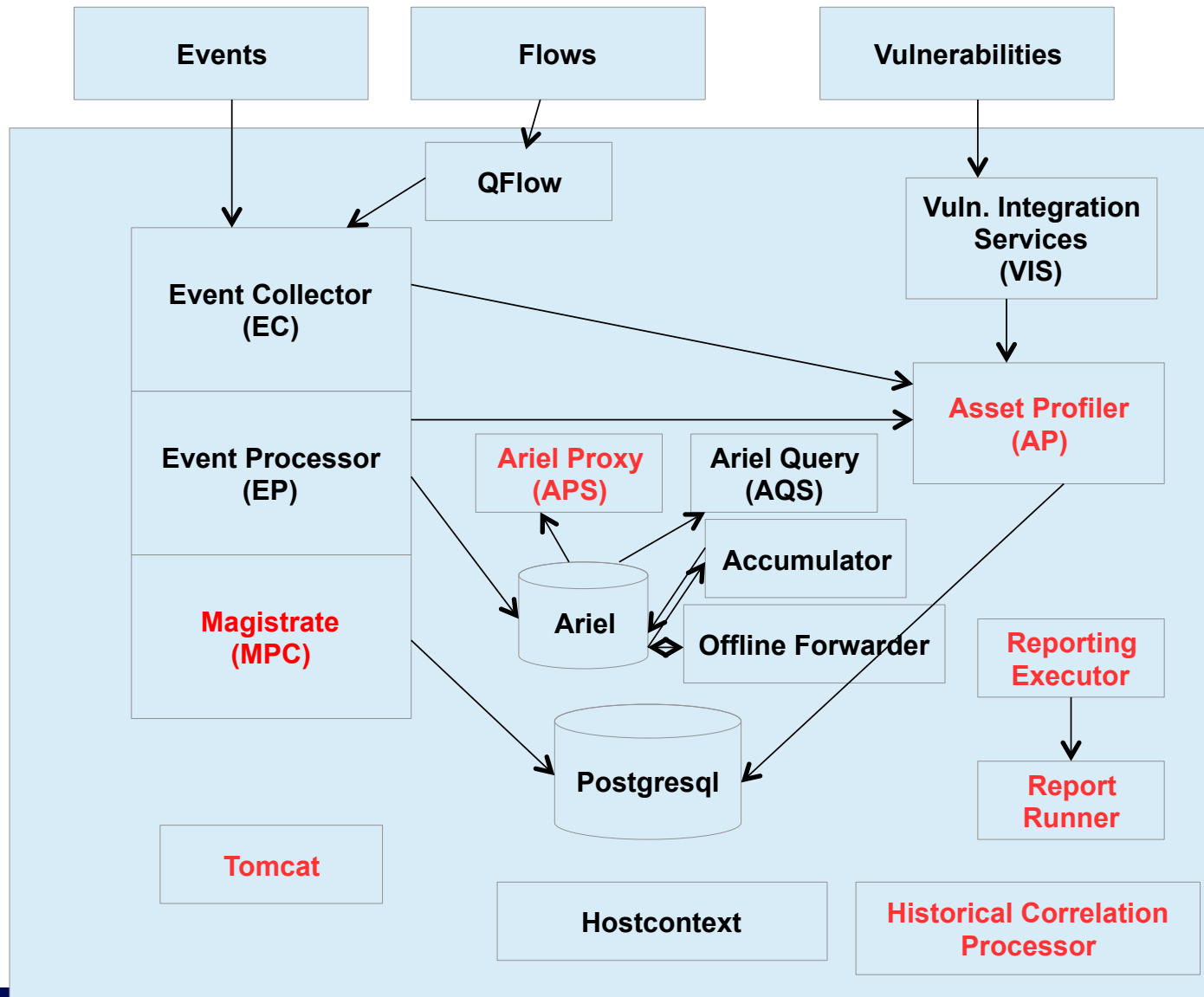
Protokolle

- SMTP
- SNMP
- syslog
- API (REST)

Products

- OTRS
- Service Now
- Remedy
- ...

QRadar Architektur



Plattformen

1. Appliance incl. HA-Option
 2. Software (Server Platform)
 3. VM (ESX)
- QRadar_Hardware_Guide.pdf



QRadar_hardware_guide.pdf - Verknüpfung.lnk

Sizing

- Design
AiO vs. Distributed
- Tools
EPS and Flow Calculator V2
- Lab
Boot Camp
SAO
VM

Finetuning

1. Network Hierarchy
2. Asset Discovery / BBs / VA
3. False Pos
4. Offense disable
5. User defined rules
6. LSX

Logs & Flow (Datenquellen, Netzwerkinfrastruktur)

- Logsources
- 80% autodiscovered
- Rest nach DSM Guide und Log Source Guide
- Unknown Logsource
- Advanced: BQ121_Unit06_CollLogs



b_dsm_guide.pdf - Verknüpfung.lnk



b_logsource.pdf - Verknüpfung.lnk

Flow Sources

- Flow Typen
- IPFIX
- Foundations: **Unit 7 Investigating an offense triggered by flowsQRadar**
- Admin Guide.pdf: **Chapter 12. Flow sources management**
- ESX Switch
- Offene Fragen

Netzwerkhierarchie

- Advanced: IBM Security QRadar SIEM 7.2 Administration and Configuration - **Unit 02**
- QRadar Admin Guide: **Chapter 6. Set up Qradar: Network hierarchy**
- CLI
- Demo

Alarme = Offenses

- Unit 4 Foundations (BQ101): BQ101_04_OffenseEvents_slides - Investigating an offense triggered by events
- Unit 9/10 Advanced (BQ121):
 - BQ121_Unit09_RulesOverview
 - BQ121_Unit10_RulesDesign
- Admin Guide: Chapter 6 Setup QRadar - Configuring custom email notifications
- Unit 12 Advanced (BQ121): Creating Reference Maps (BQ121_Unit12_RefMaps)
- User Guide: Chapter 4 Offense Management
- Rules.pdf
- Health Monitoring Rules

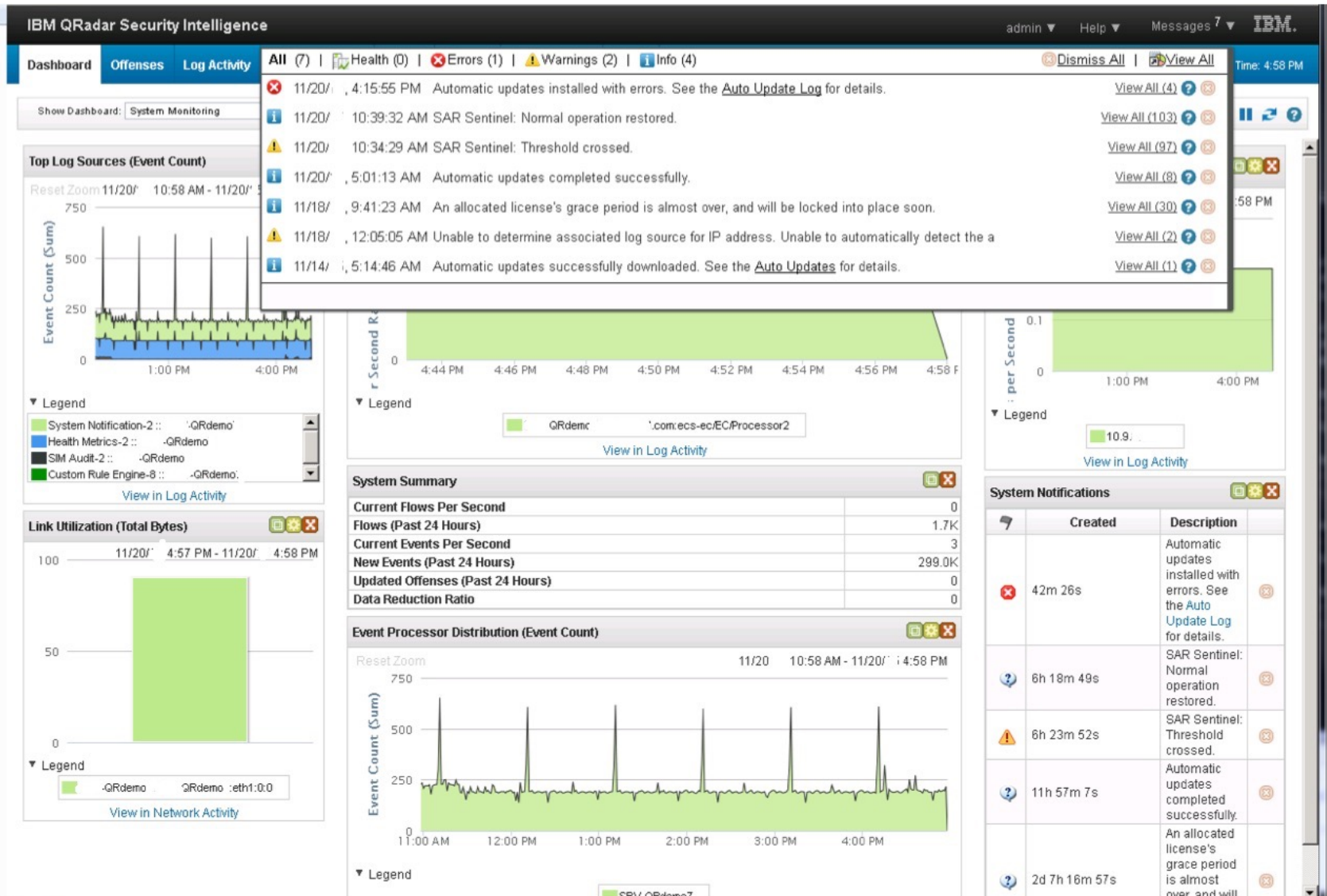
Offenses – alle Links

- **P4B QRadar hacks: false alarm (pro4bizz)**
- Unit 4/5 Foundations (BQ101)
- Unit 9/10 Advanced (BQ121):
- Admin Guide: Chapter 6 - Configuring custom email notifications
- Unit 12 Advanced (BQ121)
- User Guide: Chapter 4 Offense Management
- Rules.pdf
- Security Monitoring Rules (health check)



Rules.pdf - Verknüpfung.lnk

QR System Monitoring Labsystem 1



QR System Monitoring Labsystem 2

- View All
- Select Leistungseinbußen

Suchen... ▼ Schnellsuchvorgänge ▼ Filter hinzufügen Kriterien speichern Ergebnisse speichern Abbrechen Falscher Alarm Regeln ▼ Aktionen ▼

Erweiterte Suche Suchen

Ereignisse von 10.11.2015 01:01:20 bis 17.11.2015 09:42:23 werden angezeigt Ansicht: Wählen Sie eine Option aus: ▼ Anzeigen: Benutzerdefiniert ▼ Grenzwert für die Ergebnisse

Gruppierung nach:
Quellen-IP, Untergeordnete Kategorie, Ereignisname

Verwendung der Suche: Systemprotokolle

Aktuelle Filter:
Ereignisname ist eines von [License Near Lock oder SAR Sentinel: recov... (Filter abwählen)]









▼ Aktuelle Statistik

Gesamtergebnisse	228 (396 B gesamt)	Durchsuchte komprimierte Datendateien	16 (88,4 KB gesamt)	Dauer	1m 14s 468ms
Durchsuchte Datendateien	382 (53,2 MB gesamt)	Anzahl indizierter Dateien	10.599 (10,1 MB gesamt)	Weitere Details	


(Diagramme anzeigen)

Quellen-IP	Untergeordnete Kategorie	Ereignisname	Ziel-IP (Eindeutiger Zahler)	Zielport (Eindeutiger Zahler)	Protokollquelle (Eindeutiger Zahler)	Protokoll (Eindeutiger Zahler)	Benutzername (Eindeutiger Zahler)	Ereignisanzahl (Summe)	Zähler ▼
10.9.8	Leistungsstatus	SAR Sentinel: recovered	127.0.0.1	0	System Notification-2...	Sonstige	Keine	93	93
10.9.8	Leistungseinbußen	SAR Sentinel: threshold crossed	127.0.0.1	0	System Notification-2...	Sonstige	Keine	84	84
10.9.8	Lizenzstatus	License Near Lock	127.0.0.1	0	System Notification-2...	Sonstige	Keine	40	40
127.0	Information	Auto-Update successful	127.0.0.1	0	System Notification-2...	Sonstige	Keine	7	7
127.0	Hinweis	Auto-Update successful download	127.0.0.1	0	System Notification-2...	Sonstige	Keine	2	2
10.9.8	Serviceunterbrechung	Unable to Determine Associated Log Source For IP Address	127.0.0.1	0	System Notification-2...	Sonstige	Keine	2	2

QR System Monitoring Labsystem 3

 Zur Ereignisliste zurückkehren
  Angriff
  Ereignis zuordnen
  Falscher Alarm
  Eigenschaft extrahieren
  Zurück
  Weiter
  Drucken

Ereignisdaten

Ereignisname	SAR Sentinel: threshold crossed						
Untergeordnete Kategorie	Leistungseinbußen						
Ereignisbeschreibung	SAR Sentinel: threshold crossed.						
Ausmaß	 (8)			Relevanz	10	Schweregrad	4
Benutzername	nicht zutreffend						
Startzeit	17.11.201 05:11:56		Uhrzeit der Speicherung	17.11.201 05:11:56		Protokollquellenzeit	17.11.201 05:11:56

Quell- und Zielangaben

Quellen-IP	10.9.	Ziel-IP	127.0.0.1
Quellenassetname	nicht zutreffend	Zielfassetname	nicht zutreffend
Quellenport	0	Zielport	0
Prä-NAT Quellen-IP		Prä-NAT Ziel-IP	
Prä-NAT Quellenport	0	Prä-NAT Zielport	0
Post-NAT Quellen-IP		Post-NAT Ziel-IP	
Post-NAT Quellenport	0	Post-NAT Zielport	0
IPv6-Quelle	0:0:0:0:0:0:0:0	IPv6-Ziel	0:0:0:0:0:0:0:0
Quellen-MAC	00:00:00:00:00:00	Ziel-MAC	00:00:00:00:00:00

Angaben zu den Nutzdaten

☒ utf
 ☐ hex
 ☐ base64

☒ Zeilenumbruch

```
Nov 17 05:11:56 127.0.0.1 [Thread-102] com.qllabs.hostcontext.sar.SarSentinel: [WARN] [NOT:0150124100][10.9. . -] [-/- -]System load over 15 minutes has an average of 3.6 over the past 5 intervals, and still exceeds the configured threshold of 2.6. To resolve: If your system continues to exhibit this behavior, please contact Customer Support.
```

Weitere Informationen

Protokoll	255	QID	38750073
Protokollquelle	System Notification-2 :: SRV-QRdemo7	Ereignisanzahl	1
Angepasste Regeln	BB Network Definition: Honeypot like Addresses System Notification		

QR Beispielalarm - Summary

IBM QRadar Security Intelligence

dv690a3 Help Messages 10 IBM


System Time: 11:47 AM

Dashboard Offenses Log Activity Network Activity Assets Reports Admin

Offenses

All Offenses

Offense 17228

Magnitude  Status Relevance 5 Severity 5

Description RuV-QR-SysMon Max events reached

Source IP(s) Multiple (2)

Destination IP(s) 127.0.0.1

Network(s) other

Offense Source Summary

Rule Name	Max events reached	Response	Dispatch New Event, Email, Notify
Group(s)	QR	Rule Type	Event
Offenses	2	Events/Flows	227
Notes	QRadar System Notification: Max. events reached - A Managed Host (MH) has reached its license limit		
Rule Description	Apply RuV-QR-SysMon Max. events reached on events which are detected by the Local system and when the event GID is one of the following (38750008) Max events reached		



Last 5 Notes

Notes	Username	Creation Date
No results were returned.		

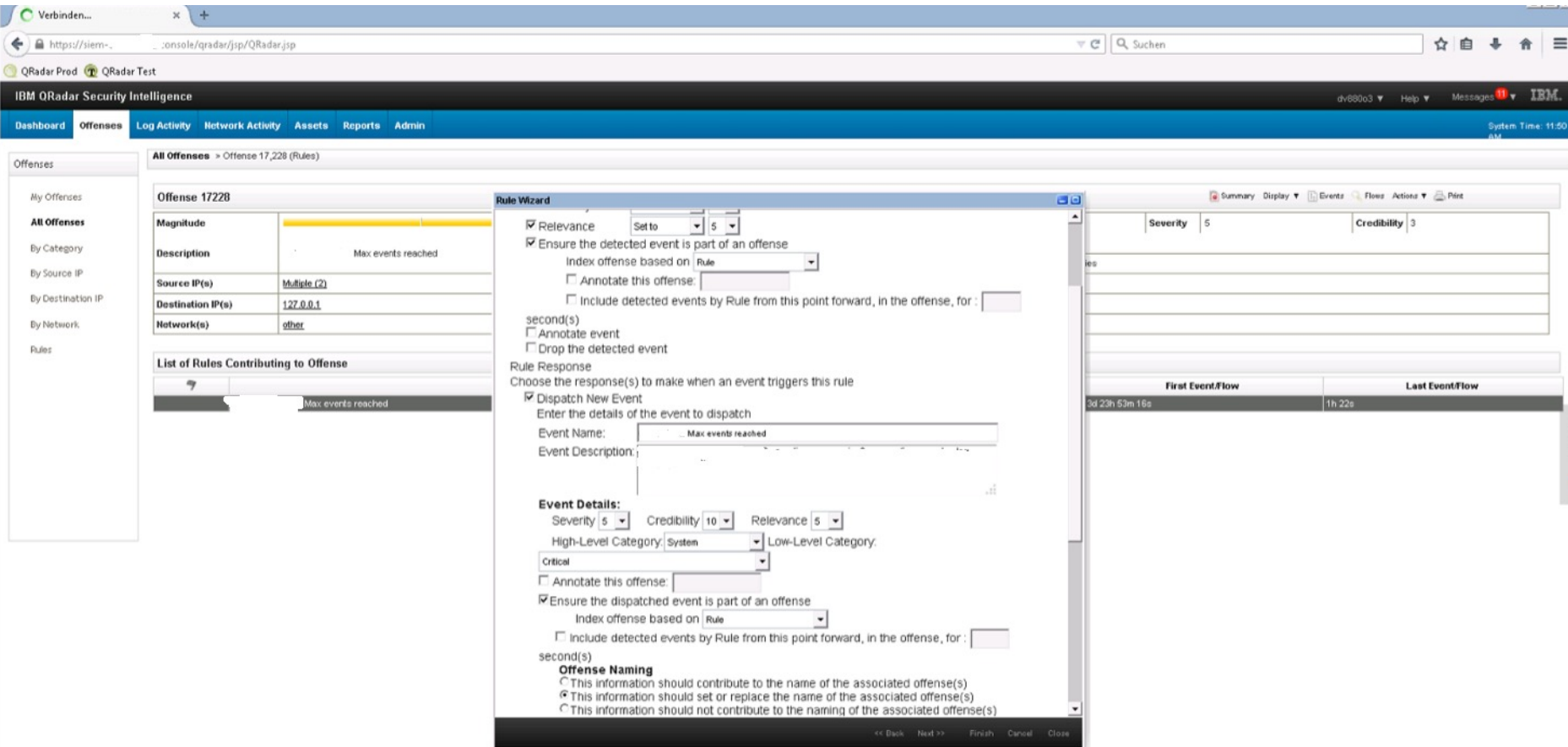
Last 5 Search Results

Magnitude	Started On	Ended On	Duration	Events/Flows
No results were returned.				

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
10.192.1.1		SEM_DMZ	No	Unknown	Unknown NIC	0	2	0	59m 36s	23
10.199.1.1			Yes	Unknown	Unknown NIC	0	1	0	3d 22h 51m 24s	1

QR Beispiellalarm - Regel



The screenshot displays the IBM QRadar Security Intelligence web interface. The main navigation bar includes links for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, and Admin. The current view is 'Offenses', specifically 'All Offenses > Offense 17,228 (Rules)'. On the left, a sidebar shows filters for 'All Offenses', 'By Category', 'By Source IP', 'By Destination IP', 'By Network', and 'Rules'. The main content area shows details for 'Offense 17228', including its 'Magnitude' (Max events reached), 'Description', 'Source IP(s)' (Multiple (2)), 'Destination IP(s)' (127.0.0.1), and 'Network(s)' (other). Below this is a 'List of Rules Contributing to Offense' table. A 'Rule Wizard' dialog box is open, showing configuration for a rule. It includes sections for 'Relevance' (Set to 5), 'Ensure the detected event is part of an offense' (checked), 'Index offense based on' (Rule), 'Annotate this offense' (unchecked), 'Include detected events by Rule from this point forward, in the offense, for:' (second(s)), 'Rule Response' (Dispatch New Event), 'Event Name' (Max events reached), 'Event Description', 'Event Details' (Severity 5, Credibility 10, Relevance 5, High-Level Category System, Low-Level Category Critical), 'Annotate this offense' (unchecked), 'Ensure the dispatched event is part of an offense' (checked), 'Index offense based on' (Rule), 'Include detected events by Rule from this point forward, in the offense, for:' (second(s)), and 'Offense Naming' (This information should set or replace the name of the associated offense(s)). The wizard has navigation buttons: << Back, Next >>, Finish, Cancel, and Close. On the right, a table shows 'Severity' 5 and 'Credibility' 3. Below this, a table displays 'First Event/Flow' and 'Last Event/Flow' with timestamps.

First Event/Flow	Last Event/Flow
3d 23h 53m 16s	1h 22s

QR Beispielalarm - Alarmsearch

IBM QRadar Security Intelligence

admin ▾ Hilfe ▾ Nachrichten 10 ▾ IBM.

Dashboard Angriffe Protokollaktivität Netzaktivität Assets Berichte Verwaltung Systemzeit: 13:48

Angriffe

Suchen... ▾ Bedingungen speichern Aktionen ▾ Drucken Letzte Aktualisierung: 00:00:35

Alle Angriffe Angriffe anzeigen: Option auswählen: ▾

Using Search:
Aktuelle Suchparameter:
Beschreibung enthält (Filter abwählen), Ausschließen Ausgeblendete Angriffe (Filter abwählen), Ausschließen Geschlossene Angriffe (Filter abwählen)

	ID	Beschreibung	Angriffstyp	Angriffsquelle	Ausmaß	Quel
	18475	Event pipeline dropped events or connections	Regel	Event pipeline error		10
	18095	Event pipeline error	Regel	Event pipeline error		10

offense details

IBM QRadar Security Intelligence admin ▼ Hilfe ▼ Nachrichten ¹² ▼ IBM.

Dashboard Angriffe Protokollaktivität Netzaktivität Assets Berichte Verwaltung Systemzeit: 17:15

Angriffe

Eigene Angriffe

Alle Angriffe

Nach Kategorie

Nach Quellen-IP


Nach Ziel-IP

Nach Netz

Regeln

Alle Angriffe > Angriff 18.475 (Zusammenfassung)

Angriff 18475 Zusammenfassung Anzeige ▼ Ereignisse Flüsse Aktionen ▼ Drucken ?

Ausmaß		Status		Relevanz	1	Wertigkeit	10	Zuverlässigkeit	3
Beschreibung	Event pipeline dropped events or connections		Angriffstyp	Regel					
Quellen-IP(s)	10.19 2		Anzahl Ereignisse/Flüsse	2 Ereignisse und 0 Flüsse in 2 Kategorien					
Ziel-IP(s)	127.0.0.1		Start	17.01.201 12:47:24					
Netz(e)	Sonstige		Dauer	2s					
			Zugeordnet zu	Nicht zugeordnet					

Zusammenfassung der Angriffsquelle

Regelname	Event pipeline error	Antworten	Neues Ereignis senden, E-Mail, Benachrichtigen
Gruppe(n)		Regeltyp	Ereignis
Angriffe	2	Ereignisse/Flüsse	2.399
Notizen	QRadar System Alert: Event pipeline dropped events or connections		
Regelbeschreibung	Apply Event pipeline error on events which are detected by the Local system and when the event QID is one of the following (38750060) Event pipeline dropped events, (38750061) Event pipeline dropped connections		

event details

Dashboard
Angriff

Angriffe

Eigene Angriffe

Alle Angriffe

Nach Kategorie

Nach Quellen-IP

Nach Ziel-IP

Nach Netz

Regeln

Zur Ereignisliste zurückkehren
Angriff
Ereignis zuordnen
Falscher Alarm
Eigenschaft extrahieren
Zurück
Weiter
Drucken

Ereignisdaten

Ereignisname	Event pipeline dropped connections							
Untergeordnete Kategorie	Fehler							
Ereignisbeschreibung	Connections were dropped by the event pipeline.							
Ausmaß	<div></div> (9)		Relevanz	10	Schweregrad	7	Zuverlässigkeit	10
Benutzername	nicht zutreffend							
Startzeit	1.01.201 12:47:24	Uhrzeit der Speicherung	1.01.201 12:47:24	Protokollquellenzeit	1.01.201 12:47:24			
Domäne	Standarddomäne							

Quell- und Zielangaben

Quellen-IP	10.199.	Ziel-IP	127.0.0.1
Quellenassetname	siem-	Zielassetname	.
Quellenport	0	Zielport	0
Prä-NAT Quellen-IP		Prä-NAT Ziel-IP	
Prä-NAT Quellenport	0	Prä-NAT Zielport	0
Post-NAT Quellen-IP		Post-NAT Ziel-IP	
Post-NAT Quellenport	0	Post-NAT Zielport	0
IPv6-Quelle	0:0:0:0:0:0:0:0	IPv6-Ziel	0:0:0:0:0:0:0:0
Quellen-MAC	00:00:00:00:00:00	Ziel-MAC	00:00:00:00:00:00

Angaben zu den Nutzdaten

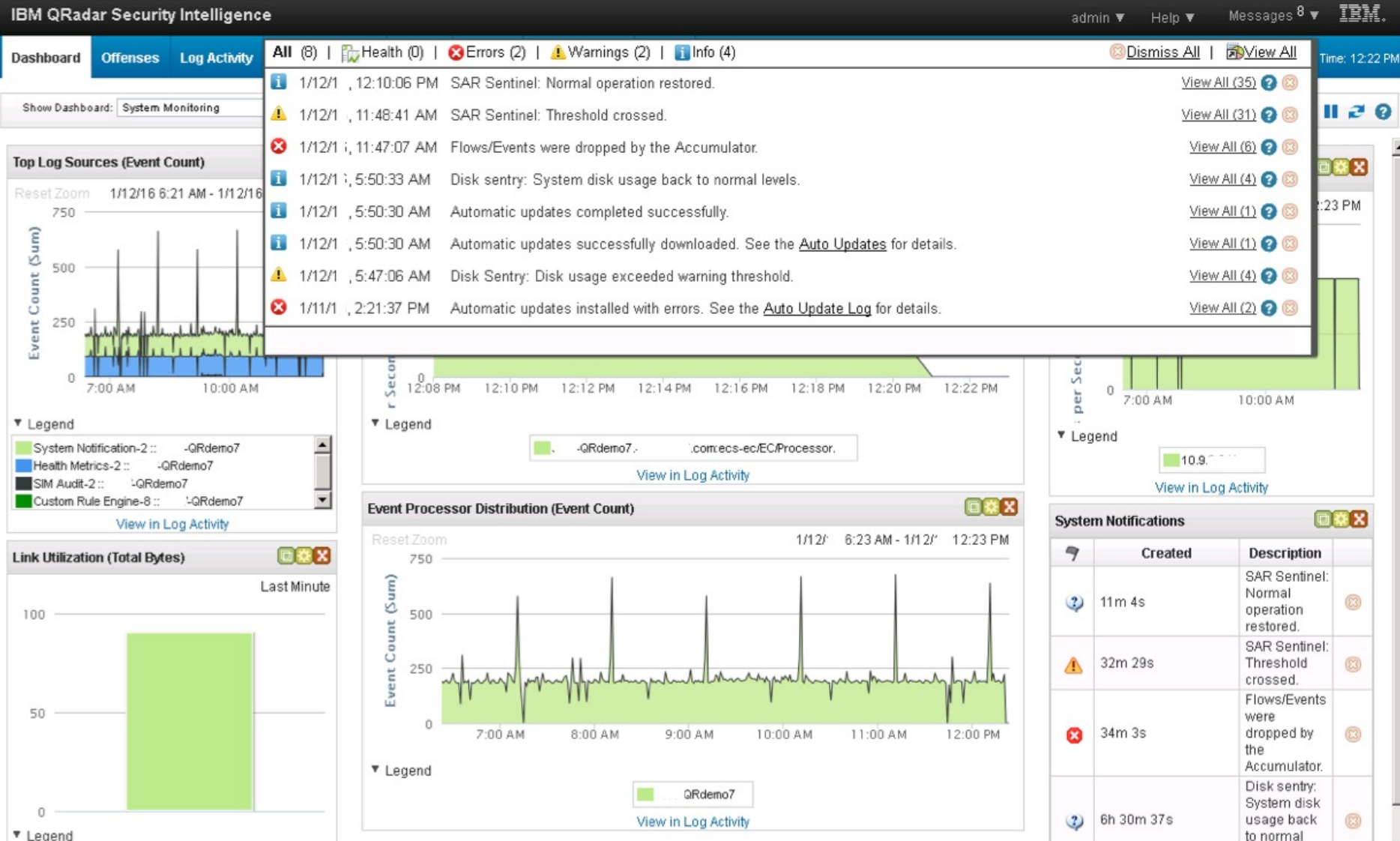
utf
hex
base64

☒ Zeilenumbruch

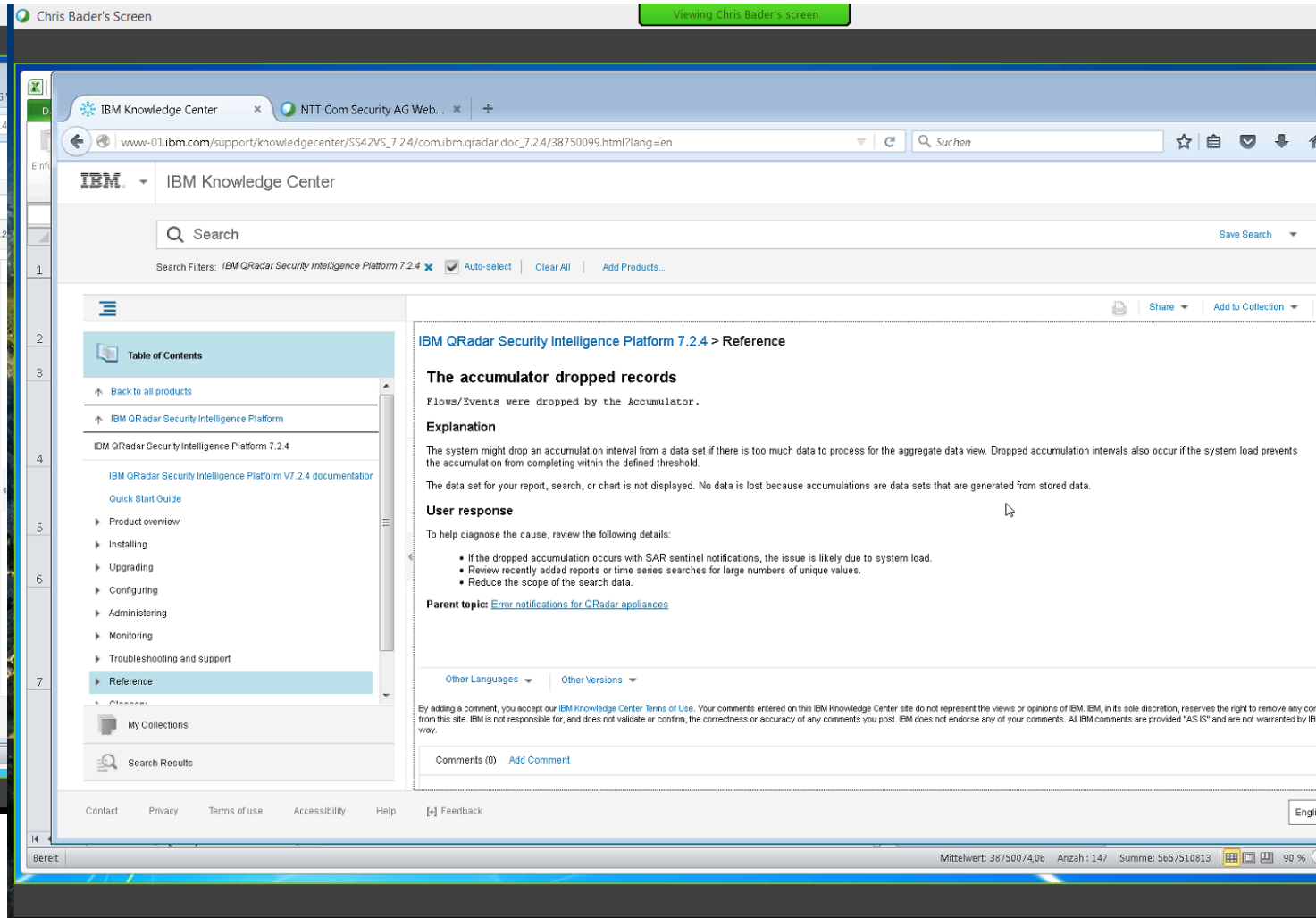
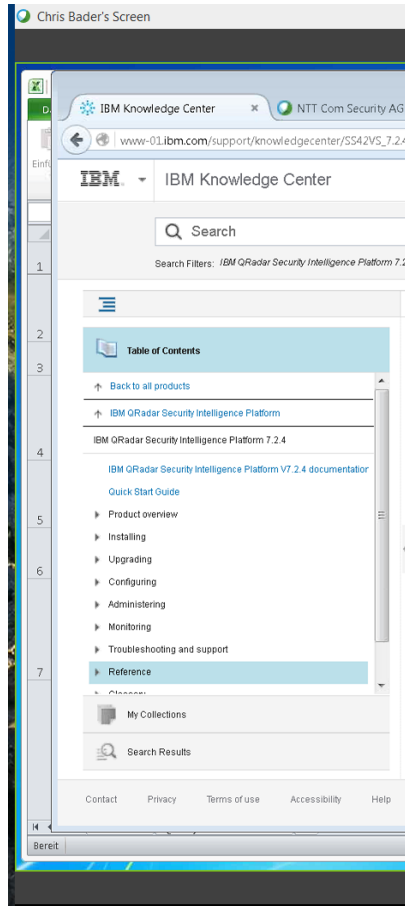
Jan 12, 12:47:24 127.0.0.1 [TosSecLog/0.0.0.0/514] Protocol: Proxify Thread: 0x00000000

© pro4bizz GmbH 2017

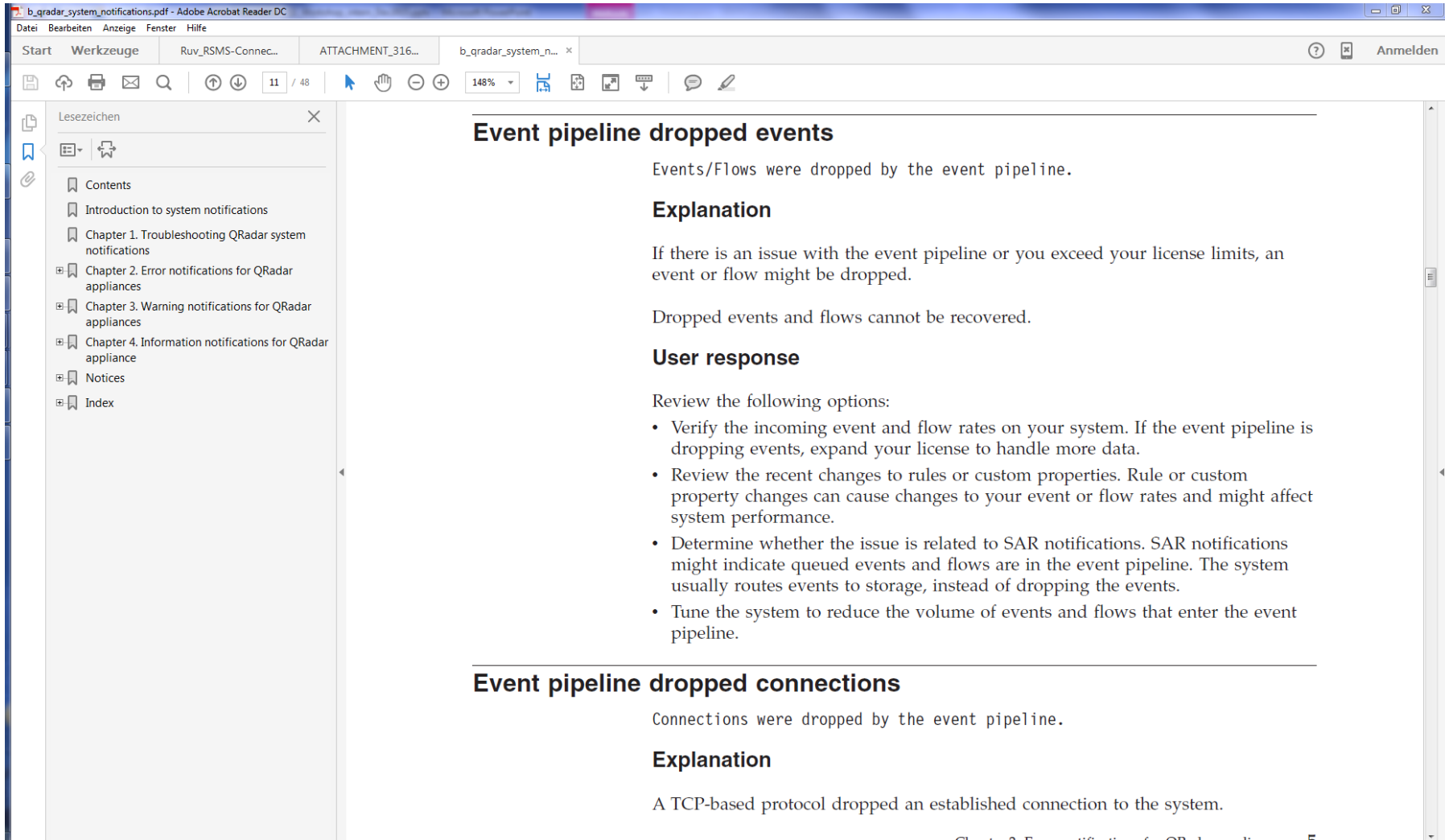
QR Beispiel Systemerror Labsystem



IBM Knowledgebase via Help



IBM System notifications



Event pipeline dropped events

Events/Flows were dropped by the event pipeline.

Explanation

If there is an issue with the event pipeline or you exceed your license limits, an event or flow might be dropped.

Dropped events and flows cannot be recovered.

User response

Review the following options:

- Verify the incoming event and flow rates on your system. If the event pipeline is dropping events, expand your license to handle more data.
- Review the recent changes to rules or custom properties. Rule or custom property changes can cause changes to your event or flow rates and might affect system performance.
- Determine whether the issue is related to SAR notifications. SAR notifications might indicate queued events and flows are in the event pipeline. The system usually routes events to storage, instead of dropping the events.
- Tune the system to reduce the volume of events and flows that enter the event pipeline.

Event pipeline dropped connections

Connections were dropped by the event pipeline.

Explanation

A TCP-based protocol dropped an established connection to the system.

Drilldown auto update error from dashboard 1

Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾

Advanced Search ▾ Search

Viewing events from Jan 11, 201 , 2:19:37 PM to Jan 11, 201 , 2:22:37 PM View: Select An Option: ▾

Display: Src IP / Low Level Cat. ▾ Results Limit

Grouping By:
 Source IP,Low Level Category

Using Search: System Logs

Current Filters:
 Event Name is Auto-Update installed with errors (Clear Filter)







▾ Current Statistics


Total Results	2 (90B Total)	Compressed Data Files Searched	0 (0B Total)	Duration	512ms
Data Files Searched	2 (133.3KB Total)	Index File Count	4 (4.4KB Total)	More Details	

(Show Charts)

Source IP	Low Level Category	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Event Count (Sum)	Count ▾
10.9.	Error	127.0.0.1	0	Auto-Update i...	System Notific...	Other	None	2	2

Drilldown auto update error from dashboard 2

Search... ▾ Quick Searches ▾  Add Filter  Save Criteria  Save Results  Cancel  False Positive Rules ▾ Actions ▾ 

Advanced Search ▾ 

Search


Viewing events from Jan 11, 201 , 2:19:37 PM to Jan 11, 201 2:22:37 PM View:

Select An Option: ▾

Display:

Default (Normalized) ▾

 Results Limit


Completed

Current Filters:

Source IP is 10.9. (Clear Filter) Event Name is Auto-Update installed with errors (Clear Filter)

Low Level Category is Error (Clear Filter)

▼ Current Statistics

Total Results2 (1.1KB Total)

Compressed Data Files Searched0 (0B Total)

Duration493ms

Data Files Searched4 (270.7KB Total)

Index File Count4 (4.3KB Total)

[More Details](#)

(Show Charts)

	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source
	Auto-Update installed with errors	System Notification-2 :: SRV-...	1	Jan 11, 201 , 2:21:3...	Error	10.9. ...
	Auto-Update installed with errors	System Notification-2 :: SRV-...	1	Jan 11, 201 , 2:21:3...	Error	10.9. ...

Drilldown auto update error from dashboard 3

[Return to Event List](#)
[Offense](#)
[Map Event](#)
[False Positive](#)
[Extract Property](#)
[Previous](#)
[Next](#)
[Print](#)

Event Information

Event Name	Auto-Update installed with errors							
Low Level Category	Error							
Event Description	Automatic updates installed with errors. See the Auto Update Log for details.							
Magnitude	<div><div></div></div> (9)		Relevance	10	Severity	7	Credibility	10
Username	N/A							
Start Time	Jan 11, 2015 , 2:21:36 PM		Storage Time	Jan 11, 2015 , 2:21:36 PM		Log Source Time	Jan 11, 2015 , 2:21:36 PM	

Source and Destination Information

Source IP	10.9	Destination IP	127.0.0.1
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
IPv6 Source	0:0:0:0:0:0:0:0	IPv6 Destination	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf
hex
base64

☒ Wrap Text

```

Jan 11 14:21:36 127.0.0.1 [Thread-2610] com.qrlabs.hostcontext.action.AutoUpdateQVMRPMAction: [WARN]
[NOT:0260004100][10.9. -] [-/- -]A request was made to install autoupdate rpm /opt/qradar/conf/QVM-
Autoupdate-SQL-724-2015.12.31.x86_64.rpm but the rpm file is missing - check error logs
    
```

Autoupdate log

Admin

Check for Updates

View Update History

Change Settings

Restore Hidden Updates

View Log

Autoupdate Log

?

Last update status: **All updates completed successfully.**

DAU 1452514175 successfully applied auto update package from 01/11/2016 at 13:09.
Deploying autoupdate configuration changes. NOTE: If global files have not been modified, we will ignore this request.
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-WinCollectMicrosoftSQL-7.2-851082.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-WinCollectNetAppDataONTAP-7.2-818094.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-WinCollectJuniperSBR-7.2-880311.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/MIS-eEyeRem-7.2-1090448.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-WinCollectConfigServer-7.2-1096879.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-SNMP-7.2-1081013.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-WinCollectFileForwarder-7.2-20150930100700.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-TLSSyslog-7.2-20151028074735.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-WindowsEventLog-7.2-20151112140622.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-WindowsEventRPC-7.2-20150813144046.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-Estreamer-7.2-20150915224844.noarch.rpm
A new DSM has been downloaded and placed in /store/configservices/staging/updates/DSM-BlueCoatWebSecurityService-7.2-20151206122707.noarch.rpm
An updated DSM has been downloaded and placed in /store/configservices/staging/updates/DSM-CiscoFirewallDevices-7.2-20151214130911.noarch.rpm
An updated DSM has been downloaded and placed in /store/configservices/staging/updates/DSM-F5NetworksBigIP-7.2-20151201203059.noarch.rpm
A new DSM has been downloaded and placed in /store/configservices/staging/updates/DSM-SeculertSeculert-7.2-20151117123141.noarch.rpm
An updated DSM has been downloaded and placed in /store/configservices/staging/updates/DSM-SolarWindsOrion-7.2-20151216131449.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-BlueCoatWSSRESTAPI-7.2-20151117173052.noarch.rpm
A DSM has been downloaded and placed in /store/configservices/staging/updates/PROTOCOL-SeculertProtectionRESTAPI-

Trouble shooting auto update

```
root@ QRdemo /var/log
[root@ -QRdemo ~]# cd /var/log
[root@ -QRdemo log]#
[root@ -QRdemo log]#
[root@ -QRdemo log]# ls *update*
autoupdate-deploy.log  qvm-assetupdates.log

autoupdates:
AU-1450061283.tgz  AU-1450752482.tgz  AU-1451443682.tgz  AU-1452221283.tgz
AU-1450147682.tgz  AU-1450838885.tgz  AU-1451530082.tgz  AU-1452307683.tgz
AU-1450234082.tgz  AU-1450925282.tgz  AU-1451616482.tgz  AU-1452394083.tgz
AU-1450320482.tgz  AU-1451011682.tgz  AU-1451702882.tgz  AU-1452480482.tgz
AU-1450406883.tgz  AU-1451029203.tgz  AU-1451789282.tgz  AU-1452566882.tgz
AU-1450493283.tgz  AU-1451098082.tgz  AU-1451875683.tgz  AU-1452574209.tgz
AU-1450579683.tgz  AU-1451184483.tgz  AU-1451962082.tgz  insertscript.log
AU-1450599603.tgz  AU-1451270883.tgz  AU-1452048482.tgz  qradar.properties
AU-1450666083.tgz  AU-1451357282.tgz  AU-1452134883.tgz
[root@ -QRdemo log]# tail autoupdate-deploy.log

Jan 12 05:58:56 - 0;;Ran=1;;RestartVIS=0
Jan 12 05:58:56 - Script /opt/qradar/conf//autoupdate-deploy-9000000000-01 executed.
Jan 12 05:58:56 - Finished executing autoupdate scripts.
Jan 12 05:58:56 - Restarting ECS.
Jan 12 05:58:57 - ecs is running... restarting it ...
Jan 12 05:59:59 - ~~~~~
Jan 12 05:59:59 - Autoupdate deploy complete.
Jan 12 05:59:59 - ~~~~~

[root@ -QRdemo log]#
```

auto update 2

The screenshot shows the IBM Knowledge Center search interface. The search term 'autoupdate' is entered in the search bar. The search filters are set to 'IBM QRadar Security Intelligence Platform 7.2.4' and 'Auto-select'. The search results are displayed in a list format, showing the first 5 items. The results include links to 'Auto update installed with errors', 'Configuring automatic update settings', 'Set up QRadar SIEM', 'Found an unmanaged process that is causing long transaction', and 'Remote networks and services configuration'.

IBM Knowledge Center

Search: autoupdate

Search Filters: IBM QRadar Security Intelligence Platform 7.2.4 x ☒ Auto-select | Clear All | Add Products...

Did you mean: [auto update](#)

1 - 5 items

Auto update installed with errors

Automatic updates installed with errors. See the **Auto Update Log** for details.
Date: October 30, 2015 | Found in: [IBM QRadar Security Intelligence Platform 7.2.4](#)

Configuring automatic update settings

Click the Admin tab. In the navigation pane, click System Configuration. Click the **Auto Update** icon. In the navigation pane, click Change Settings. In the **Auto** ...
Date: October 30, 2015 | Found in: [IBM QRadar Security Intelligence Platform 7.2.4](#)

Set up QRadar SIEM

Use the features on the Admin tab to set up IBM Security QRadar SIEM.
Date: October 30, 2015 | Found in: [IBM QRadar Security Intelligence Platform 7.2.4](#)

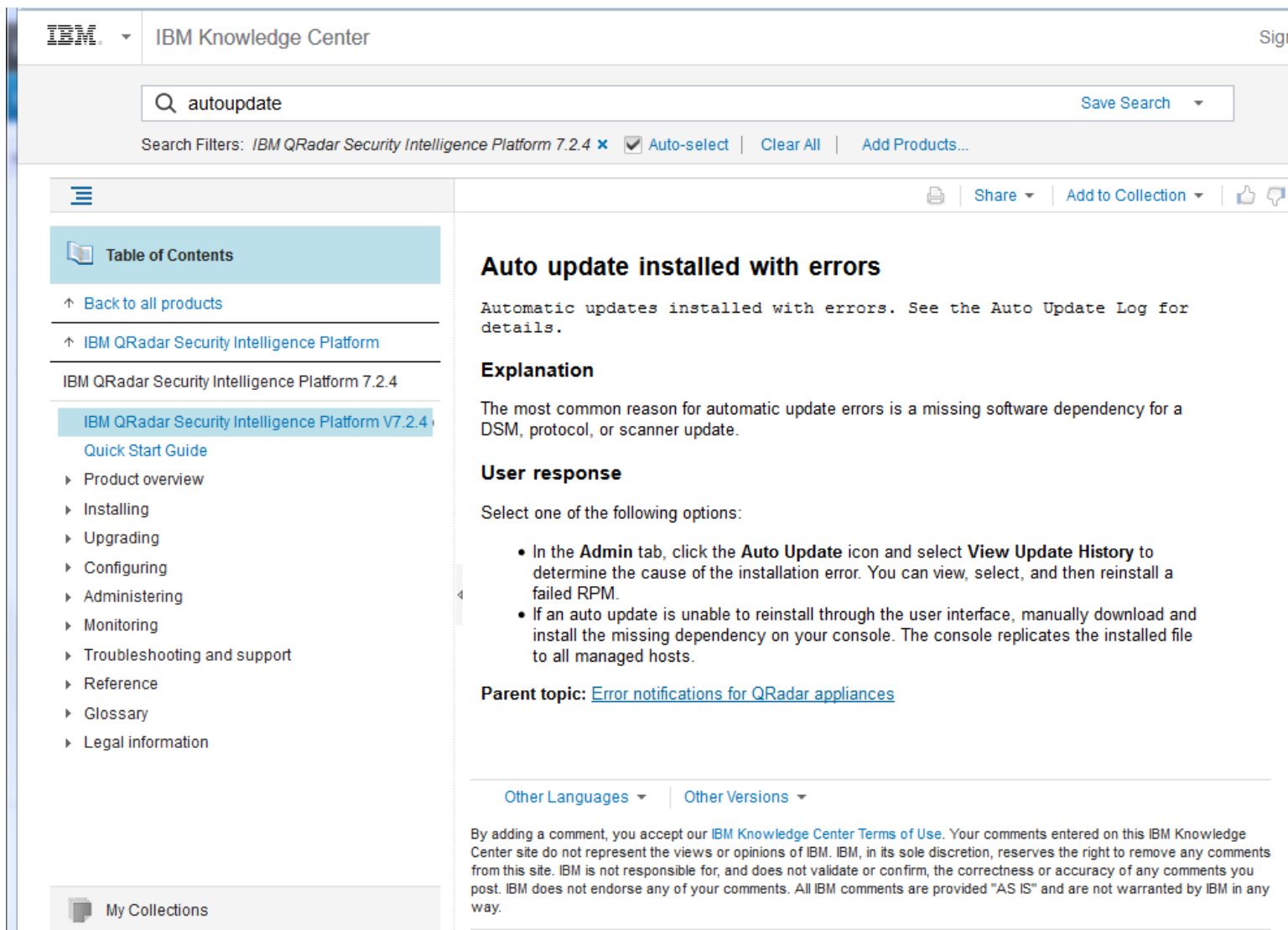
Found an unmanaged process that is causing long transaction

Explanation. The transaction sentry determines that an outside process, such as a database replication issue, maintenance script, **auto update**, or command line ...
Date: October 30, 2015 | Found in: [IBM QRadar Security Intelligence Platform 7.2.4](#)

Remote networks and services configuration

Use remote network and service groups to represent traffic activity on your network for a specific profile. Remote networks groups display user traffic that ...
Date: October 30, 2015 | Found in: [IBM QRadar Security Intelligence Platform 7.2.4](#)

auto update 3



The screenshot shows the IBM Knowledge Center interface. At the top, the IBM logo and 'IBM Knowledge Center' are visible. A search bar contains the text 'autoupdate' with a 'Save Search' button. Below the search bar, search filters are listed: 'IBM QRadar Security Intelligence Platform 7.2.4' (with a close icon), 'Auto-select' (checked), 'Clear All', and 'Add Products...'. The left sidebar contains a 'Table of Contents' section with links to 'Back to all products', 'IBM QRadar Security Intelligence Platform', and 'IBM QRadar Security Intelligence Platform 7.2.4'. Under the 7.2.4 section, there is a 'Quick Start Guide' and a list of topics: 'Product overview', 'Installing', 'Upgrading', 'Configuring', 'Administering', 'Monitoring', 'Troubleshooting and support', 'Reference', 'Glossary', and 'Legal information'. The main content area is titled 'Auto update installed with errors'. It includes a paragraph stating that automatic updates were installed with errors and to check the Auto Update Log. An 'Explanation' section follows, stating that the most common reason for errors is a missing software dependency. A 'User response' section lists two options: clicking the 'Auto Update' icon and selecting 'View Update History' in the Admin tab, or manually downloading and installing the missing dependency. A 'Parent topic' link points to 'Error notifications for QRadar appliances'. At the bottom of the main content area, there are links for 'Other Languages' and 'Other Versions'. A disclaimer at the very bottom states that comments are provided 'AS IS' and are not warranted by IBM.

IBM Knowledge Center

Search: autoupdate Save Search

Search Filters: IBM QRadar Security Intelligence Platform 7.2.4 ☒ Auto-select | Clear All | Add Products...

Table of Contents

- ↑ Back to all products
- ↑ IBM QRadar Security Intelligence Platform
- IBM QRadar Security Intelligence Platform 7.2.4
 - IBM QRadar Security Intelligence Platform V7.2.4
 - Quick Start Guide
 - Product overview
 - Installing
 - Upgrading
 - Configuring
 - Administering
 - Monitoring
 - Troubleshooting and support
 - Reference
 - Glossary
 - Legal information

My Collections

Auto update installed with errors

Automatic updates installed with errors. See the Auto Update Log for details.

Explanation

The most common reason for automatic update errors is a missing software dependency for a DSM, protocol, or scanner update.

User response

Select one of the following options:

- In the **Admin** tab, click the **Auto Update** icon and select **View Update History** to determine the cause of the installation error. You can view, select, and then reinstall a failed RPM.
- If an auto update is unable to reinstall through the user interface, manually download and install the missing dependency on your console. The console replicates the installed file to all managed hosts.

Parent topic: [Error notifications for QRadar appliances](#)

Other Languages | Other Versions

By adding a comment, you accept our [IBM Knowledge Center Terms of Use](#). Your comments entered on this IBM Knowledge Center site do not represent the views or opinions of IBM. IBM, in its sole discretion, reserves the right to remove any comments from this site. IBM is not responsible for, and does not validate or confirm, the correctness or accuracy of any comments you post. IBM does not endorse any of your comments. All IBM comments are provided "AS IS" and are not warranted by IBM in any way.

Trouble Shooting

- IBM QRadar Dokumentation
- QRadar Help
- Log Activity
System (lokale IP)
SIM Audit
- QRadar_Troubleshooting_System_Notifications_Guide.pdf
- CLI
/var/log/qradar.log
/var/log/qradar.error
/opt/qradar/support/get_logs.sh -s



b_qradar_system_notifications.pdf - Verknüpfung.lnk

IBM SR (PMR)

- Support ICN
- Customer Contract
- SR Access right

The screenshot shows the IBM Service Request (PMR) creation interface. At the top, there is a navigation bar with the IBM logo and links for 'Industries & solutions', 'Services', 'Products', 'Support & downloads', and 'My IBM'. Below this, the page title 'Serviceanforderungen > Neue Serviceanforderung' is displayed. A blue button labeled 'Neue Serviceanforderung' is prominently featured. To the right of the button is a 'Hilfe' (Help) link with a question mark icon. Below the button, a section titled 'Welche Art von Problem liegt vor?' (Which type of problem is it?) contains a list of four options, each preceded by a right-pointing arrow: 'Ich habe ein Problem mit der Software', 'Ich habe ein Problem mit der Hardware', 'Ich habe ein Problem mit einem Gerät', and 'Als Partnerworld Business Partner hat mein Kunde ein Problem mit der Software'.

IBM Industries & solutions Services Products Support & downloads My IBM

Serviceanforderungen >

Neue Serviceanforderung


Neue Serviceanforderung

Hilfe

Welche Art von Problem liegt vor?

- Ich habe ein Problem mit der Software
- Ich habe ein Problem mit der Hardware
- Ich habe ein Problem mit einem Gerät
- Als Partnerworld Business Partner hat mein Kunde ein Problem mit der Software

IBM SR (PMR)

 Industries & solutions Services Products Support & downloads My IBM

[← Zurück zu Service Request](#)
Unterstützungsregistrierungen
[Kundenverwaltung](#)
[Hilfe](#)

Unterstützungsregistrierungen

Wenn Sie auf IBM Software Support-Services (z. B. IBM Support Portal, Fix Central und IBM Service Request) zugreifen möchten, müssen Sie sich registrieren. Sie können sich mit Ihrer IBM Kundennummer oder einem Systemtyp und einer Seriennummer registrieren. Wählen Sie unten eine Option aus, um die Registrierung zu beginnen.

☒ Nach Kunde ☐ Nach Systemtyp und Seriennummer


Geben Sie Ihre Kundeninformationen unten ein. Wenn Sie diese Informationen nicht kennen, kann Ihnen die Vertrags- oder Einkaufsniederlassung Ihres Unternehmens möglicherweise weiterhelfen.

IBM Kundennummer*

Land/Region*
Ist Ihr Land/Ihre Region in der Liste nicht enthalten, wenden Sie sich bitte an [Länder-/regionsspezifische IBM Unterstützung](#), um festzustellen, welches Land/welche Region Sie auswählen müssen.
[Get Adobe Reader](#)

Begründung

Vorhandener Zugriff (0) Anstehende Zugriffsanforderungen (1)

IBM Kundennummer	Angebote	Zugriffsebene	Status
008 [Deutschland]		 Basic User	Anstehende Genehmigung für Aktualisierung

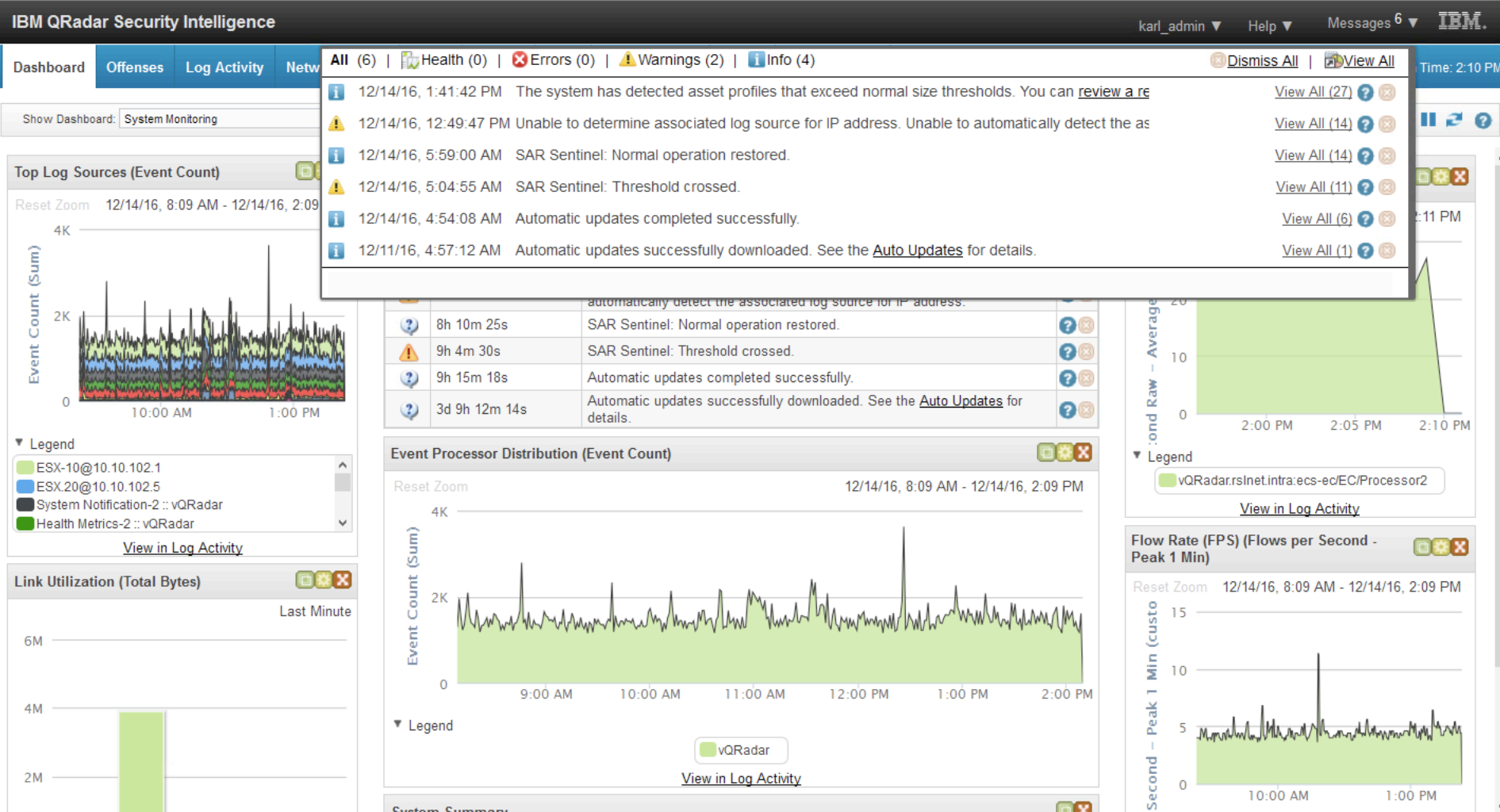
Business Partner-Standorte (1)

(Germany)

Business Partner
[Klicken Sie hier, um den Geschäftspartnerstatus zu überprüfen](#)

Andere Unterstützungsregistrierung

health check messages



Prüfe Logaktivität

List of Events - Mozilla Firefox

https://vqradar.rslnet.intra/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FarielSearchId%3DSYSTEM-LOGS%26pageId%3DEventList%26appName%3DEventViewer%26dispatch%3DloadSavedSearch%26strings(qid)%3DEQany+38750137

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Advanced Search Search

Start Time 12/7/2016 4:44 AM End Time 12/14/2016 1:42 PM Update

View: Select An Option Display: Custom Results Limit

Completed

Grouping By:
Source IP, Low Level Category, Event Name

Using Search: System Logs

Current Filters:
Event Name is any of [Deviant Asset Activity Detected or Unable to Det... (Clear Filter)]

Current Statistics

Total Results	74 (396B Total)	Compressed Data Files Searched	0 (0B Total)	Duration	308ms
Data Files Searched	128 (2.8MB Total)	Index File Count	220 (19.3MB Total)	More Details	

(Show Charts)

Source IP	Low Level Category	Event Name	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Event Count (Sum)	Count
10.10.100.40	Information	Deviant Asset Activity Detected	127.0.0.1	0	System Notifica...	Other	None	27	27
10.10.100.40	Service Disruption	Unable to Determine Associated Log...	127.0.0.1	0	System Notifica...	Other	None	15	15
10.10.100.40	Performance Status	SAR Sentinel: recovered	127.0.0.1	0	System Notifica...	Other	None	14	14
10.10.100.40	Performance Degradation	SAR Sentinel: threshold crossed	127.0.0.1	0	System Notifica...	Other	None	11	11
127.0.0.1	Information	Auto-Update successful	127.0.0.1	0	System Notifica...	Other	None	6	6
127.0.0.1	Notice	Auto-Update successful download	127.0.0.1	0	System Notifica...	Other	None	1	1

System Management

QRadar - Admin Console - Mozilla Firefox

https://vqradar.rslnet.intra/console/qradar/jsp/QRadar.jsp

IBM QRadar Security Intelligence

karl_admin ▾ Help ▾ Messages 6 ▾ IBM.

Dashboard Offenses Log Activity Network Act... Assets Reports Risks Vulnerabilities Admin User Analytics System Time: 2:23 PM

Admin

- System Configuration
- Data Sources
- Remote Networks and Services Configuration
- Try it out

Deployment Editor Deploy Changes Advanced ▾

Checking for undeployed changes...

System Configuration

Auto Update Backup and Recovery Global System Index Management Aggregated Data Network Hierarchy System and License

System and License Management

Allocate License to System Upload License Actions ▾ Deployment Actions ▾

Deployment Details

Log Source Count	21/750	Users	4
Event Limit	1000/1000	Flow Limit	25000/50000

License Information Messages

System Support Activities Messages

System Information

Host Name	vQRadar (console)	Host IP	10.10.100.40
Version	7.2.7	Appliance Type	2100
Host Status	Active	Log Source Limit	21/750
Event Rate Limit	1000/1000	Flow Rate Limit	25000/50000
License Status	Deployed	License Expiration Date	Sep 15, 2017

Security Data Distribution

License Firewall Network Interfaces Email Server

% of Disk Used

vQRadar : /store (/dev/sda8)

0% 20% 40% 60% 80% 100%

Used To Grow To Shrink

Backup

IBM QRadar Security Intelligence

karl_admin ▼ Help ▼ Messages 6 ▼ IBM.

Dashboard Offenses Log Activity Network A... Assets Reports Risks Vulnerabil... Admin User Anal... System Time: 2:27 PM

Admin

Deployment Editor Deploy Changes Advanced ?

There are no changes to deploy.

System Configuration

Auto Update Backup and Recovery Global System Notifications Index Management Aggregated Data Management Network Hierarchy

Backup Archives - Mozilla Firefox

https://vqradar.rslnet.intra/console/do/qradar/maintainBackupSummary?dispatch=init

Backup Archives On Demand Backup Restore Delete Configure ?

Existing Backups

Host	Name	Type	Size	Time Initiated	Duration	Initialized By ▲
vQRadar_53	nightly	config	813.3MB	Dec 13, 2016, 12:00:08...	11m 40s	scheduled_initiator
vQRadar_53	nightly	config	813.2MB	Dec 14, 2016, 12:00:09...	12m 4s	scheduled_initiator

Upload Archive: Durchsuchen... Keine Datei ausgewählt. Upload

HA Status

```
cd /opt/qradar/support  
./ha_diagnosis.sh
```

```
root@siem-con /opt/qradar/support  
[root@siem-con ~]# ./ha_diagnosis.sh  
> HA manager is running  
> Parsing current HA status from cstate  
Currently, You are on HA primary.  
> Check the HA State  
Currently, local HA state reaches ACTIVE state  
Currently, remote HA state reaches STANDBY state  
> Check the HA heartbeat  
Local HA heartbeat is up. Network connection has been established properly on local host [OK]  
Local Network Connection check is PASSED [OK]  
Remote HA heartbeat is up. Network connection has been established properly on remote host [OK]  
Remote Network Connection check is PASSED [OK]  
> Checking HA Virtual IP  
HA Virtual Interface is UP  
Local HA virtual IP test PASSED [OK]  
> Checking HA Mount  
HA Mount service is running  
/store has been mounted properly  
/store/transient has been mounted properly  
/store/tmp has been mounted properly  
Local HA Mount test PASSED [OK]  
> Checking HA DRBD  
Local DRBD Role is primary  
HA DRBD Connection Status is Connected  
Local HA DRBD Check PASSED [OK]  
> Check the hidden token  
No hidden token was found on local HA host  
No patch token was found on local HA host [OK]  
  
> Diagnosis Summary:  
All the HA check is PASSED [OK]  
[root@siem-con1-primary support]#
```


HA Status

Lizenz dem System zuordnen
Lizenz hochladen
Aktionen ▼
Implementierungsaktionen ▼

Hochverfügbarkeit ▼
Letzte Aktualisierung: 00:03:20





Anzeige Systeme ▼

▼ **Implementierungsdetails**

Protokollquellenanzahl	22	Benutzer	28
Ereignisgrenzwert	85	Datenflussbegrenzung	520

► **Nachrichten zu Lizenzinformationen**

▼ **Nachrichten zu Systemunterstützungsaktivitäten**

Hostname	Host-IP	Gerätetyp	Version	Seriennummer	Hoststatus	Ablaufdatum der Lizenz	Lizenzstatus
 siem-fp- (Hochverfügbarkeit)	10.19.1.16	1701	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-fp- (primär)	10.19.1.17	1701	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-fp- (sekundär)	10.19.1.18	1701	7.2.5	KQ3	Standby	Zeitlich unbeg...	Implementiert
 siem-ep- (Hochverfügbarkeit)	10.19.1.20	1605	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-ep- (primär)	10.19.1.21	1605	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-ep- (sekundär)	10.19.1.22	1605	7.2.5	KQ2	Standby	Zeitlich unbeg...	Implementiert
 siem-ep- (Hochverfügbarkeit)	10.19.1.36	1605	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-ep- (primär)	10.19.1.37	1605	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-ep- (sekundär)	10.19.1.38	1605	7.2.5	KQ2	Standby	Zeitlich unbeg...	Implementiert
 siem-con1 (Konsole) (Hochverfügbarkeit)	10.19.1.12	3105	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-con (Konsole) (primär)	10.19.1.13	3105	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-con (Konsole) (sekundär)	10.19.1.14	3105	7.2.5	KQ2	Standby	Zeitlich unbeg...	Implementiert