IBM Security

Open Mic: Domains and Tenants

A discussion about domains and tenants, how it works, when to contact support, tips and other helpful information for QRadar administrators.

https://ibm.biz/JoinQRadarOpenMic

October 26th, 2018

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

- QRadar 7.3.1 Patch 6 Interim Fix 02 was just released. This update resolved four issues reported by administrators.
- The QRadar Risk Manager team released a new adapter bundle.
  - F5 BIG-IP version support increased to version 13.1.
  - Palo Alto PAN-OS version support increased to version 8.1.
  - Check Point HTTPS adapter now supports discovery and backup via Domain Management Server.
- A new script was posted to IBM Fix Central for an error related to a manifest issue that some users are hitting.
  - Error message: “`Manifest requires version 8.9 but the scripts only contains 8.8. Cannot continue`.

    If customers continue to experience this issue error message, they should try to run a manual auto updates after October 25 and if you continue to have issues, then post in the forums (https://ibm.biz/qradarforums) or open a case so we can review (https://ibm.com/mysupport).
- The November Open Mic topic is User Behavior Analytics v3.0.

Let’s talk about domains and tenants

- About domains
- Where are domains used in QRadar?
- Where does domain tagging occur?

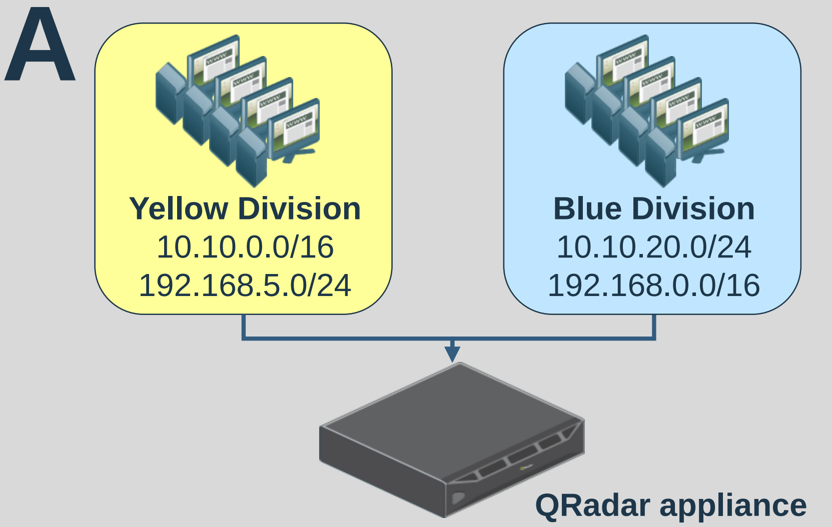
About domains in QRadar

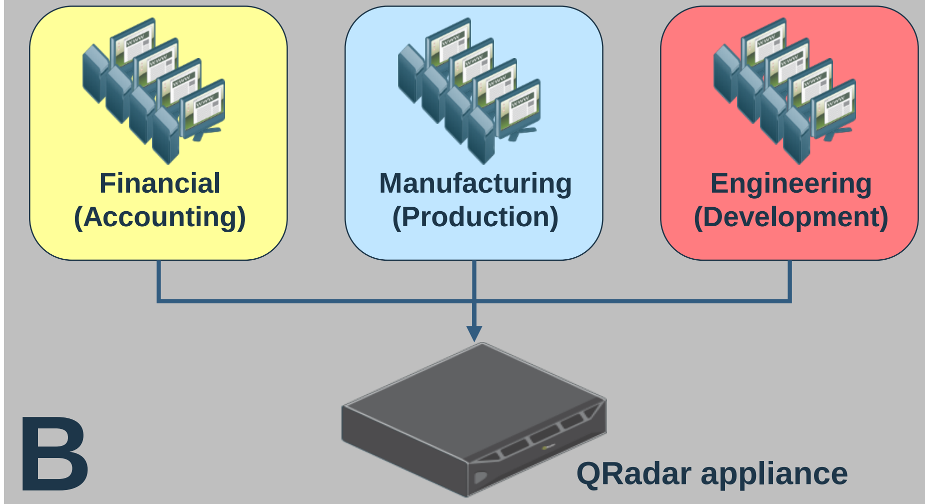
Domain tags in QRadar are added to events as they come through the event pipeline. The tags themselves are meta data added to the original event as the data is processed in the event pipeline.

Domains create individual correlation entities to segment and separate important information.

Why is this useful for administrators?

- **A. Handling overlapping IP addresses**
  - Companies that merge networks or obtain networks/assets through acquisition
  - Managed security services hosting organizations within a single QRadar deployment
- **B. Segmenting data in your organization**
  - Separate networks within the enterprise to individual domains
  - Accomplish individual correlation and dedicated offense creation





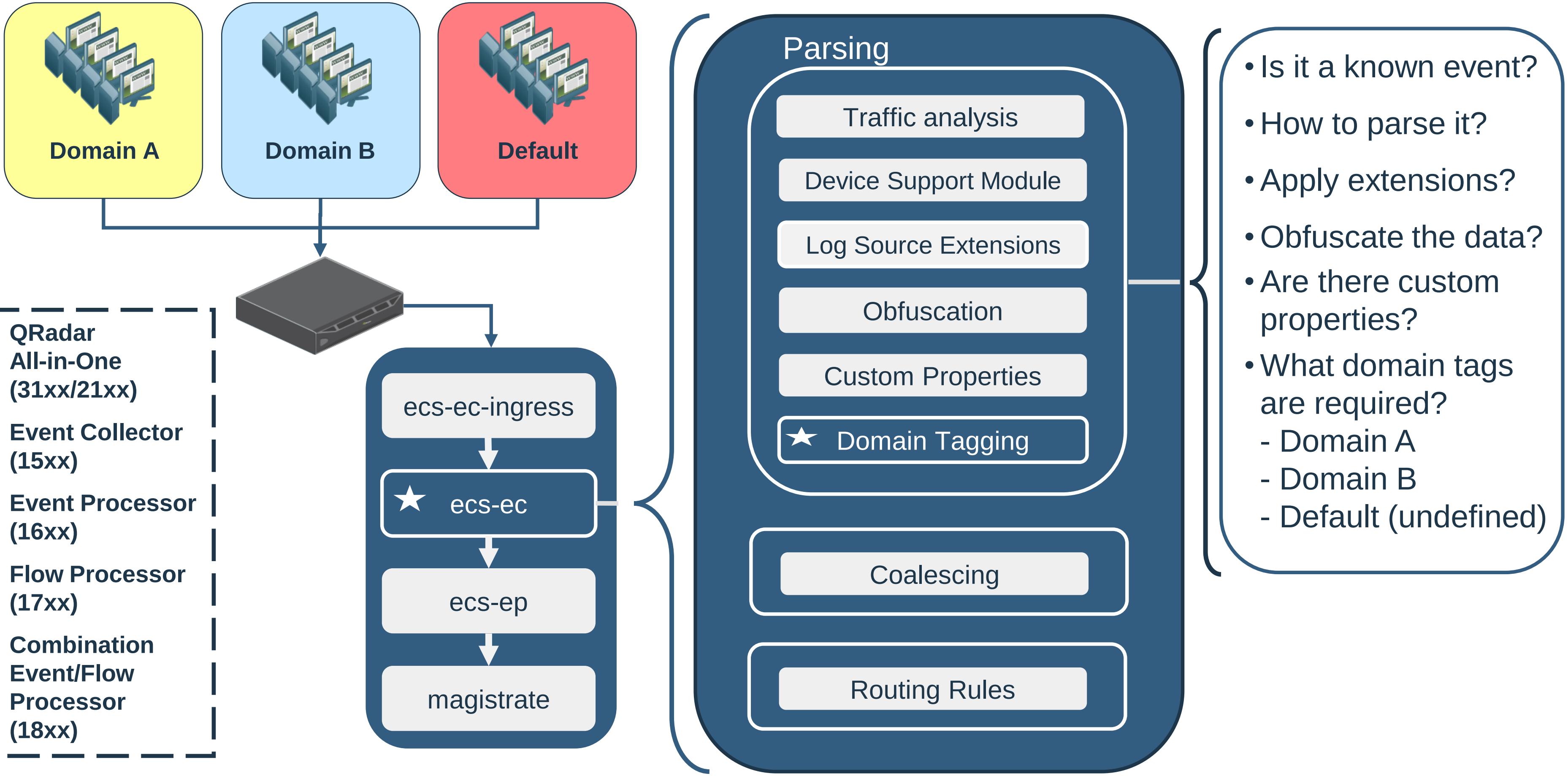
Where are domains used in QRadar?

- Events
- Flows
- Assets
- Vulnerabilities
- Network Hierarchy
- Rules
- Offenses
- Searches
- Reference Sets
- Retention (➔ Tenants)
- Centralized Credentials
- Custom Property definition (➔ Tenants)
- Security Profiles

Where are domains not available currently?

- Obfuscation (planned)
- VLAN (planned)
- Index Management
- QRadar Apps
- Reference Data
- Forensics
- Risk Management
- Backup and Recovery

Where does domain tagging occurs in the event pipeline?

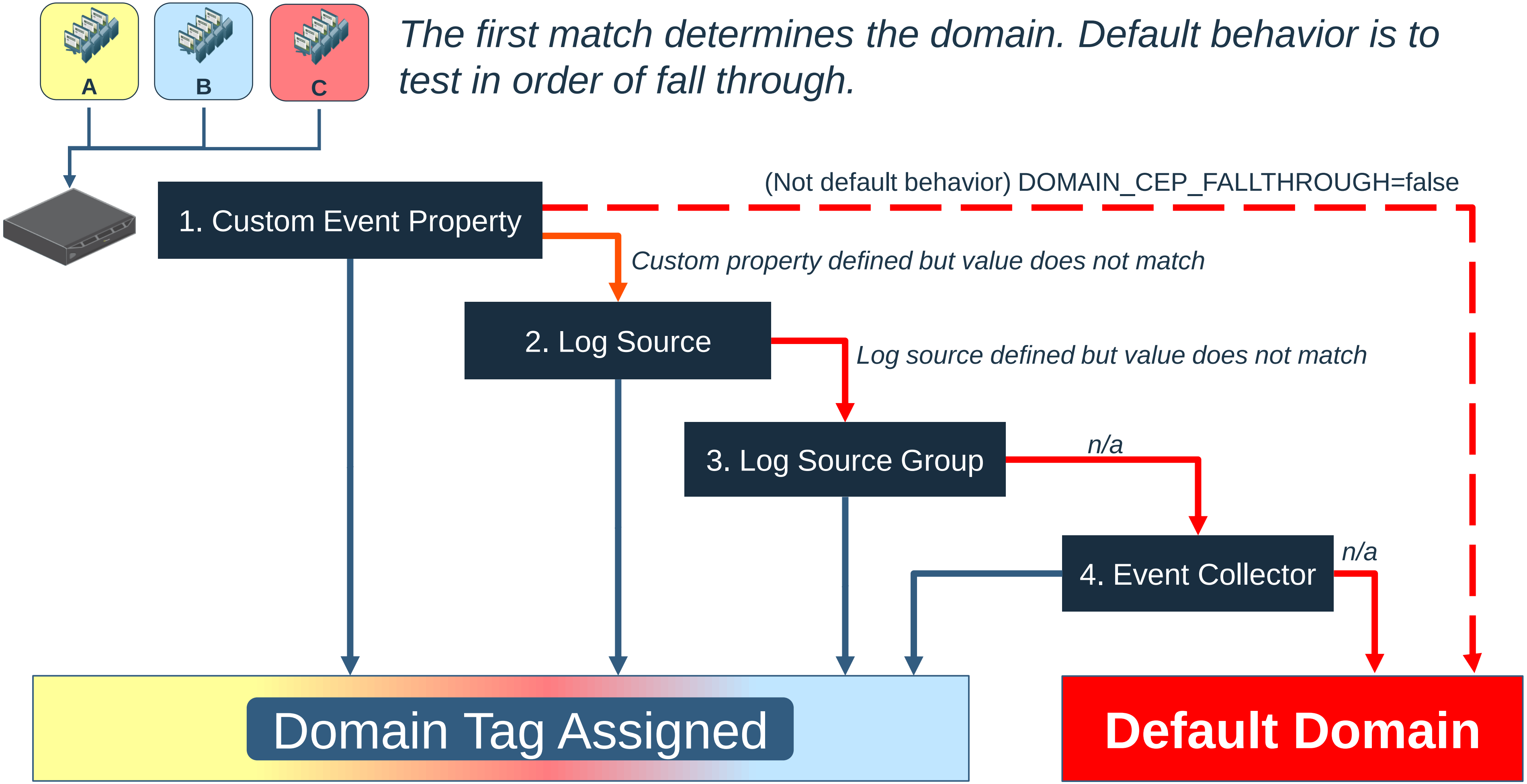


- Is it a known event?
- How to parse it?
- Apply extensions?
- Obfuscate the data?
- Are there custom properties?
- What domain tags are required?
  - Domain A
  - Domain B
  - Default (undefined)

- QRadar All-in-One (31xx/21xx)
- Event Collector (15xx)
- Event Processor (16xx)
- Flow Processor (17xx)
- Combination Event/Flow Processor (18xx)

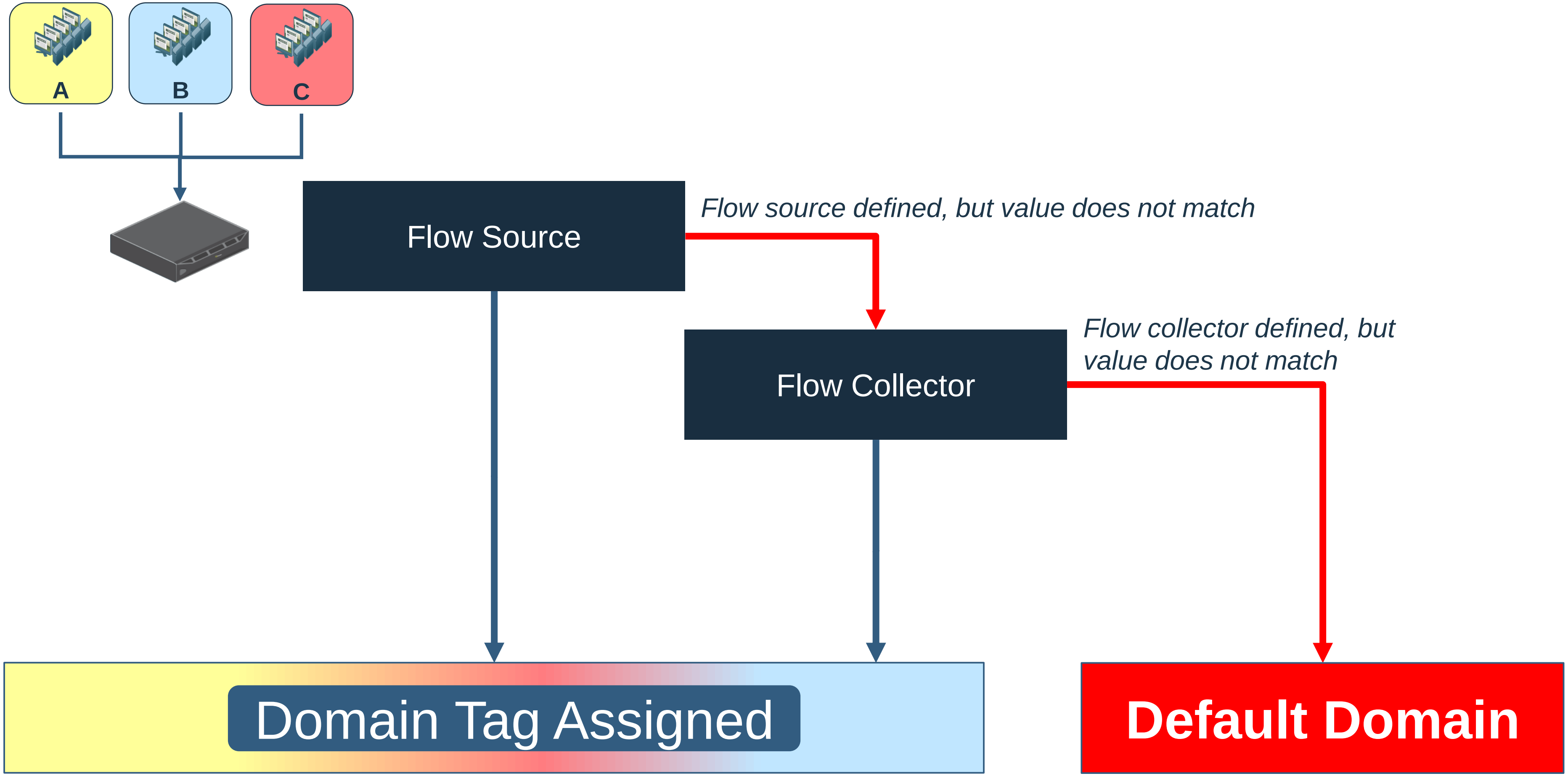
Precedence Order for Evaluating Domain Criteria (Events)

The first match determines the domain. Default behavior is to test in order of fall through.


A
B
C
(Not default behavior) DOMAIN_CEP_FALLTHROUGH=false
1. Custom Event Property
Custom property defined but value does not match
2. Log Source
Log source defined but value does not match
3. Log Source Group
n/a
4. Event Collector
n/a
Domain Tag Assigned
Default Domain

Precedence Order for Evaluating Domain Criteria (Flows)

The first match determines the domain assignment.



A

B

C

Flow Source

Flow source defined, but value does not match

Flow Collector

Flow collector defined, but value does not match

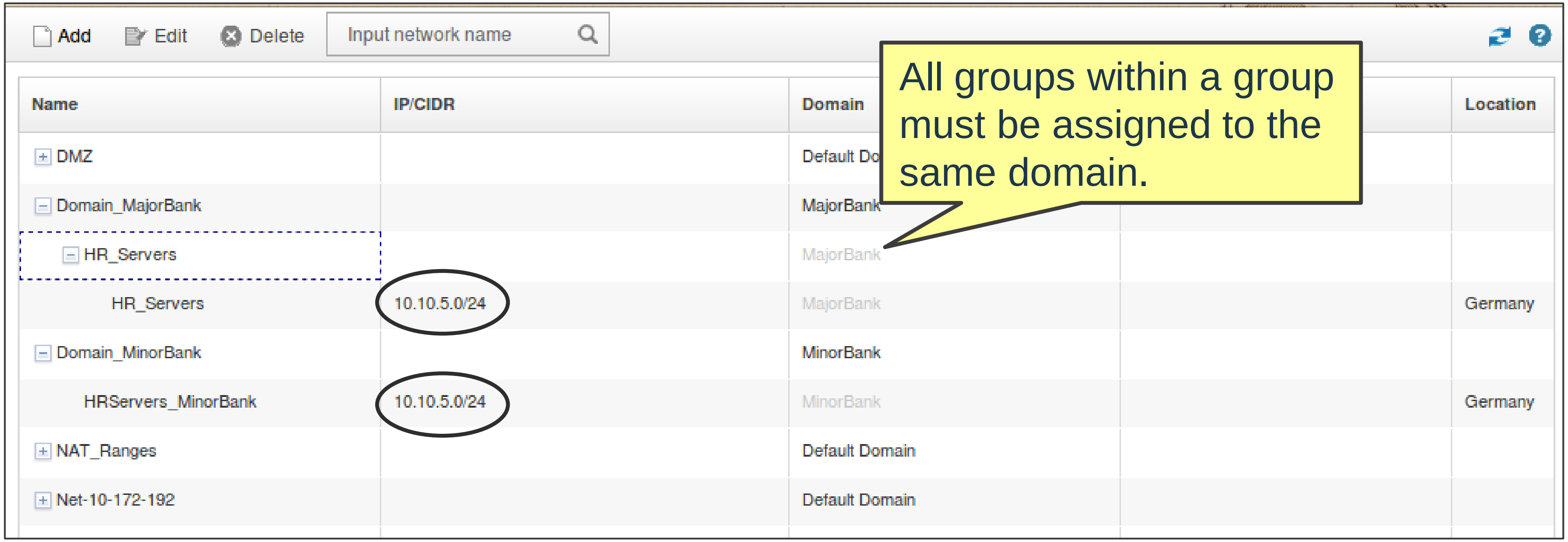
Domain Tag Assigned

Default Domain

Domain Support - Network Hierarchy

Domains are now present throughout QRadar SIEM and can be utilized in the following areas

1. **Network Hierarchy**



Name	IP/CIDR	Domain		Location
+ DMZ		Default Do		
− Domain_MajorBank		MajorBank		
− HR_Servers		MajorBank		
HR_Servers	10.10.5.0/24	MajorBank		Germany
− Domain_MinorBank		MinorBank		
HRServers_MinorBank	10.10.5.0/24	MinorBank		Germany
+ NAT_Ranges		Default Domain		
+ Net-10-172-192		Default Domain		

All groups within a group must be assigned to the same domain.

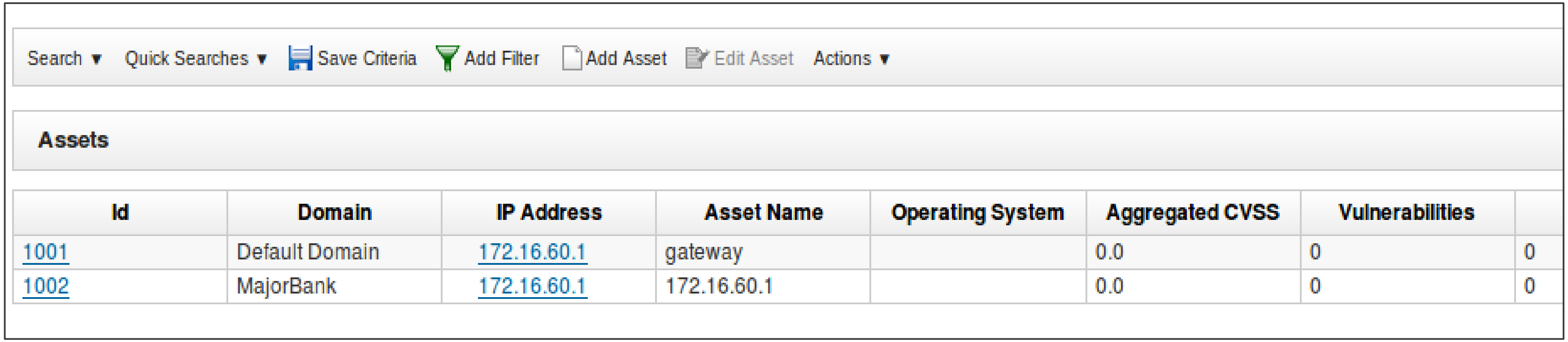
Domain Support - Assets

Domains are now present throughout QRadar SIEM and can be utilized in the following areas

1. Network Hierarch
2. **Assets**

Assets are created based on domain values derived from

- Events
- Flows, or
- Scan data

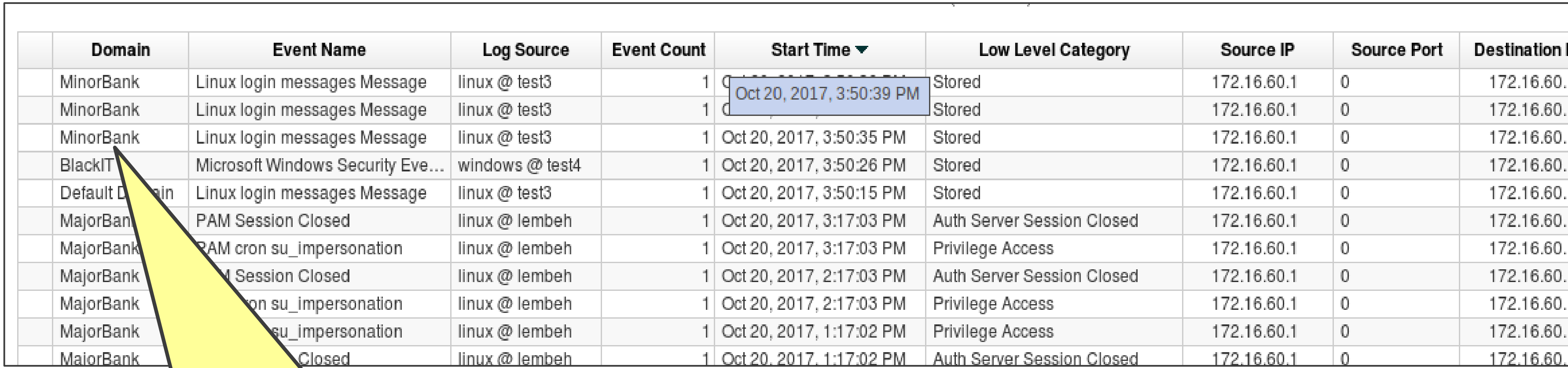


Id	Domain	IP Address	Asset Name	Operating System	Aggregated CVSS	Vulnerabilities	
1001	Default Domain	172.16.60.1	gateway		0.0	0	0
1002	MajorBank	172.16.60.1	172.16.60.1		0.0	0	0

Domain Support - Searches

Domains are now present throughout QRadar SIEM and can be utilized in the following areas

1. Network Hierarchy
2. Assets
3. **Searches**



	Domain	Event Name	Log Source	Event Count	Start Time ▼	Low Level Category	Source IP	Source Port	Destination I
	MinorBank	Linux login messages Message	linux @ test3	1	Oct 20, 2017, 3:50:39 PM	Stored	172.16.60.1	0	172.16.60.
	MinorBank	Linux login messages Message	linux @ test3	1	[illegible]	Stored	172.16.60.1	0	172.16.60.
	MinorBank	Linux login messages Message	linux @ test3	1	Oct 20, 2017, 3:50:35 PM	Stored	172.16.60.1	0	172.16.60.
	BlackIT	Microsoft Windows Security Eve...	windows @ test4	1	Oct 20, 2017, 3:50:26 PM	Stored	172.16.60.1	0	172.16.60.
	Default Domain	Linux login messages Message	linux @ test3	1	Oct 20, 2017, 3:50:15 PM	Stored	172.16.60.1	0	172.16.60.
	MajorBank	PAM Session Closed	linux @ lembeh	1	Oct 20, 2017, 3:17:03 PM	Auth Server Session Closed	172.16.60.1	0	172.16.60.
	MajorBank	PAM cron su_impersonation	linux @ lembeh	1	Oct 20, 2017, 3:17:03 PM	Privilege Access	172.16.60.1	0	172.16.60.
	MajorBank	PAM Session Closed	linux @ lembeh	1	Oct 20, 2017, 2:17:03 PM	Auth Server Session Closed	172.16.60.1	0	172.16.60.
	MajorBank	PAM cron su_impersonation	linux @ lembeh	1	Oct 20, 2017, 2:17:03 PM	Privilege Access	172.16.60.1	0	172.16.60.
	MajorBank	PAM cron su_impersonation	linux @ lembeh	1	Oct 20, 2017, 1:17:02 PM	Privilege Access	172.16.60.1	0	172.16.60.
	MajorBank	PAM Session Closed	linux @ lembeh	1	Oct 20, 2017, 1:17:02 PM	Auth Server Session Closed	172.16.60.1	0	172.16.60.

Domain is an additional event or flow attribute and can be used in search filters.

Input Sources for domain classification

- Events
  - Custom Event Properties
  - Log Sources
  - Log Source Groups
  - Event Collectors
- Flows
- Scanners

Domain Definition – Events – Based on Custom Event Property

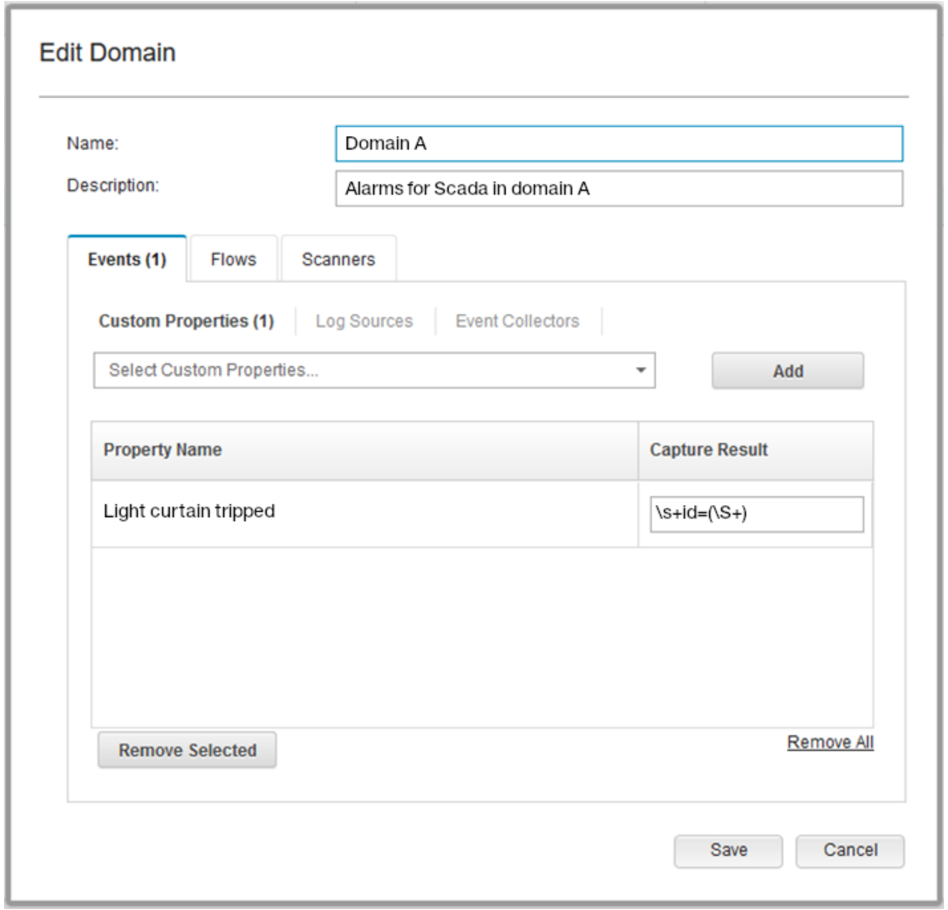
An event is tagged with **Domain A** when:

- Event has custom event property ‘Light curtain tripped’ containing the ID of the device. This property could be received from any of the following input sources:
  - A log source
  - A Log source group
  - An Event Collector

- You can assign a custom property as the only event source type for a domain. However, you can map the same custom property to two different domains, but the capture result must be different for each one.

An event is tagged with domain “Default Domain“ when:

- An event has custom event property AccountDomain containing any other value not assigned to a domain and regardless of any other definition for log sources or collectors.



Edit Domain

Name: Domain A

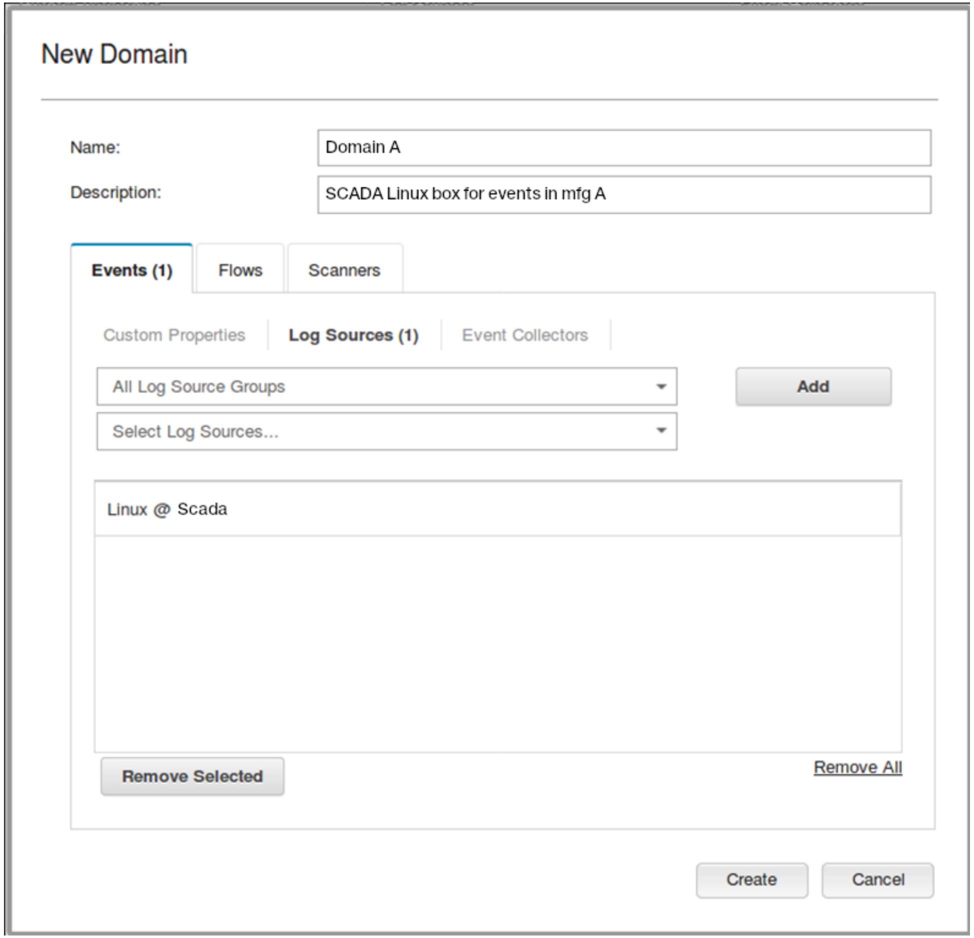
Description: Alarms for Scada in domain A

Property Name	Capture Result
Light curtain tripped	\s+id=(\S+)

Domain Definition – Events – Based on Log Source

An event is tagged with **Domain A** when:

- Event was received by log source "Linux @ Scada"
- None of the domain criteria based on custom event property can be applied to this event.



New Domain

Name: Domain A

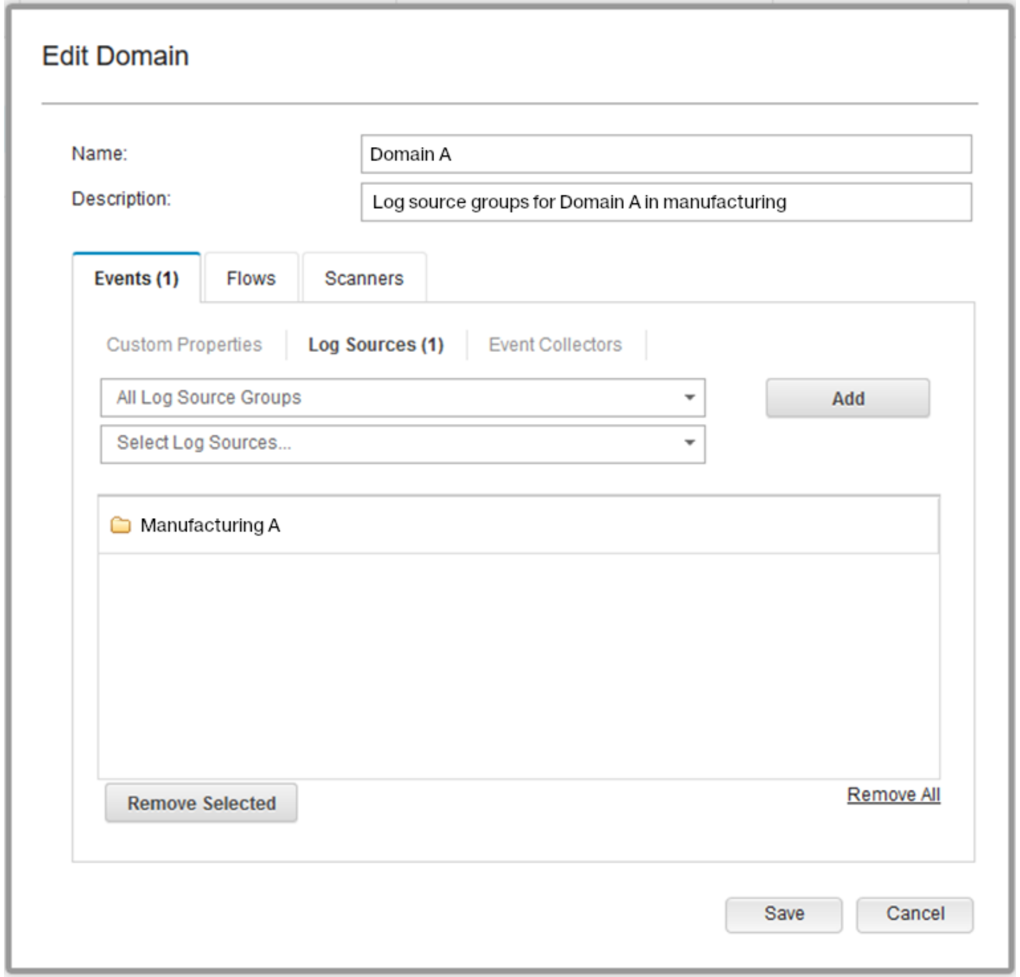
Description: SCADA Linux box for events in mfg A

Linux @ Scada

Domain Definition – Events – Based on Log Source Group

An event is tagged with **Domain A** when:

- Event was received by a log source which is a direct or indirect member of log source group “Manufacturing A“.
- None of the domain criteria based on custom event property or an individual log source matched this event.



Edit Domain

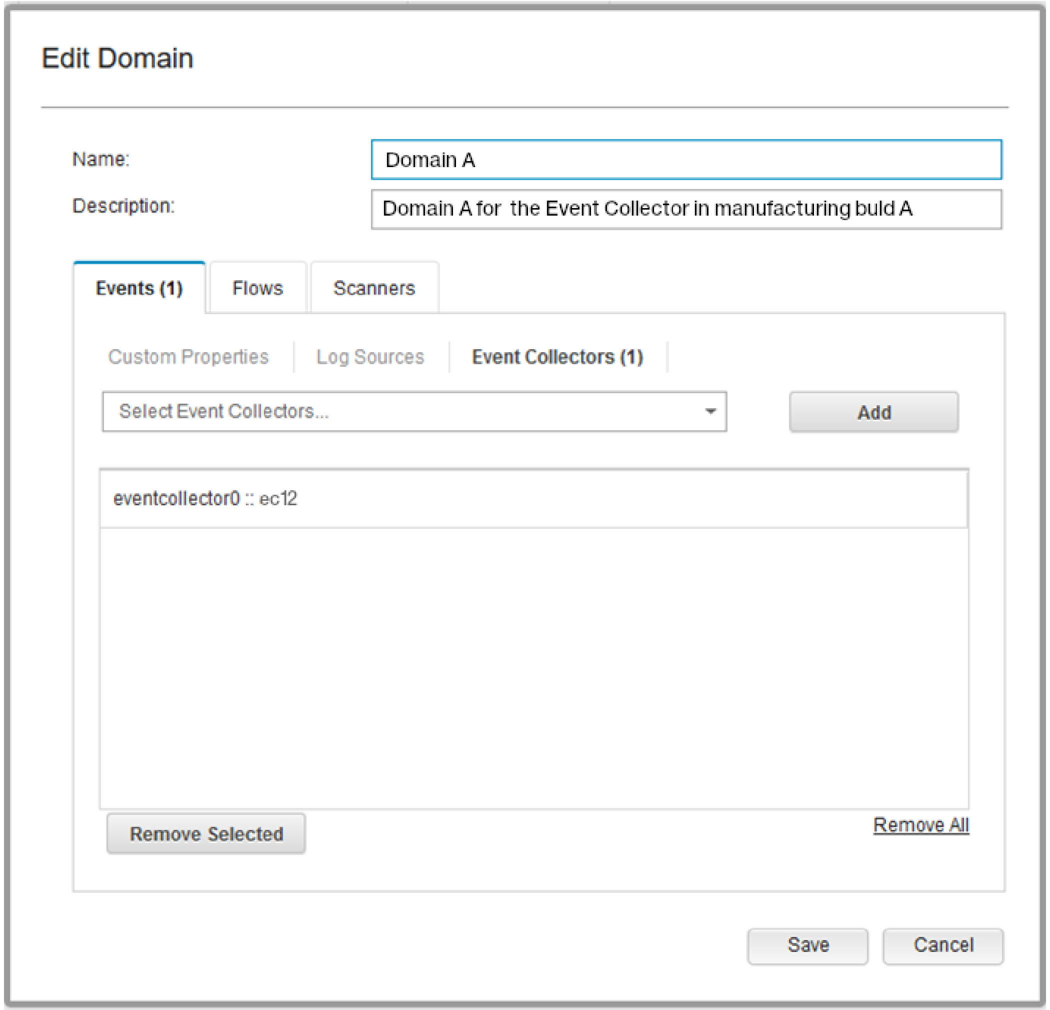
Name: Domain A

Description: Log source groups for Domain A in manufacturing

Domain Definition – Events – Based on Event Collector

An event is tagged with **Domain A** when:

- Event was received by this event collector
- None of the other domain criteria matched this event, such as a custom property, log source, or log source group.



Edit Domain

Name: Domain A

Description: Domain A for the Event Collector in manufacturing buld A

eventcollector0 :: ec12

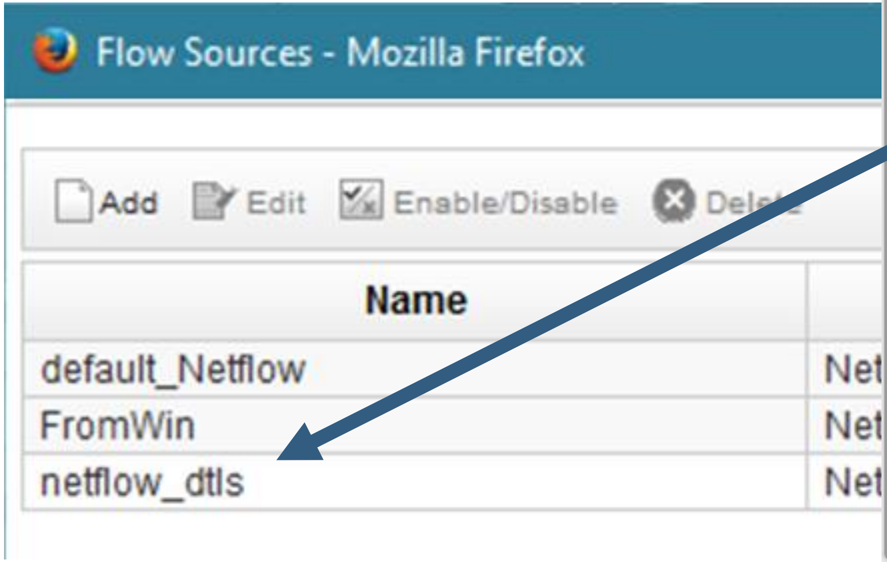
Input Sources for domain classification

- Events
  - Custom Event Properties
  - Log Sources
  - Log Source Groups
  - Event Collectors
- Flows
- Scanners

Domain Definition – Flows – Based on Flow Source

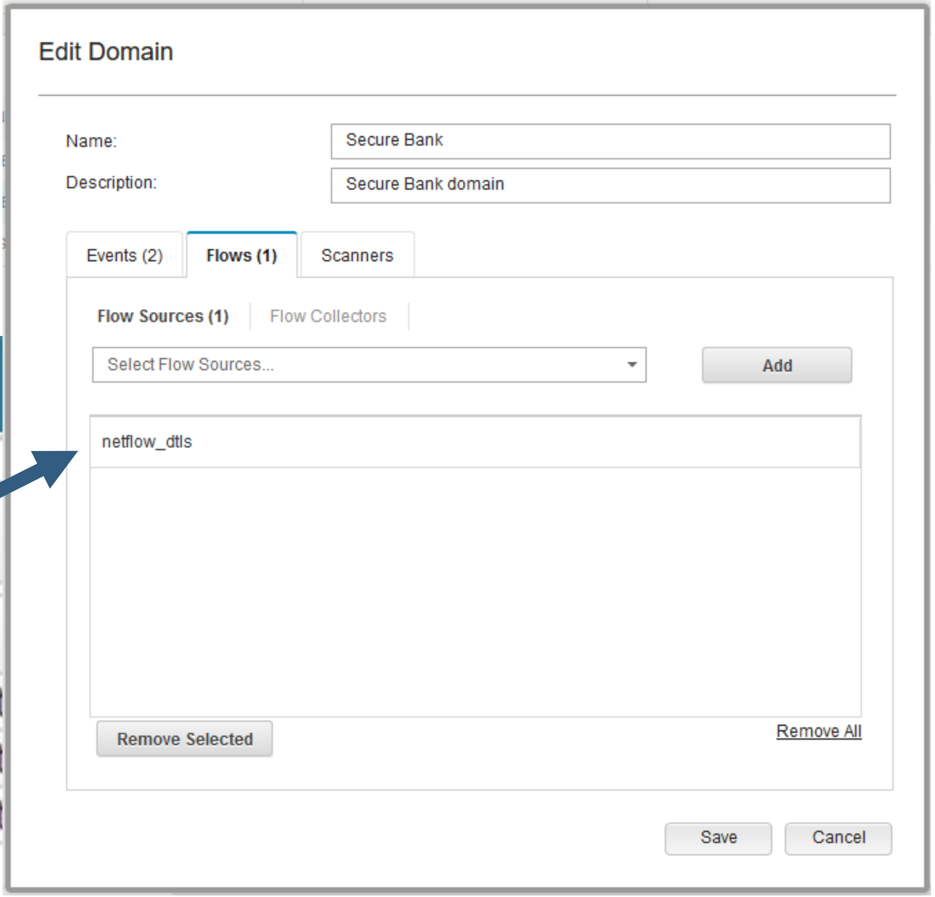
A flow session is tagged with domain “Secure Bank“ in case:

- Flow records were received through the flow source’s interface as defined in Flow Sources:



Flow Sources - Mozilla Firefox

Name	
default_Netflow	Net
FromWin	Net
netflow_dtls	Net



Edit Domain

Name: Secure Bank

Description: Secure Bank domain

netflow_dtls

Input Sources for domain classification

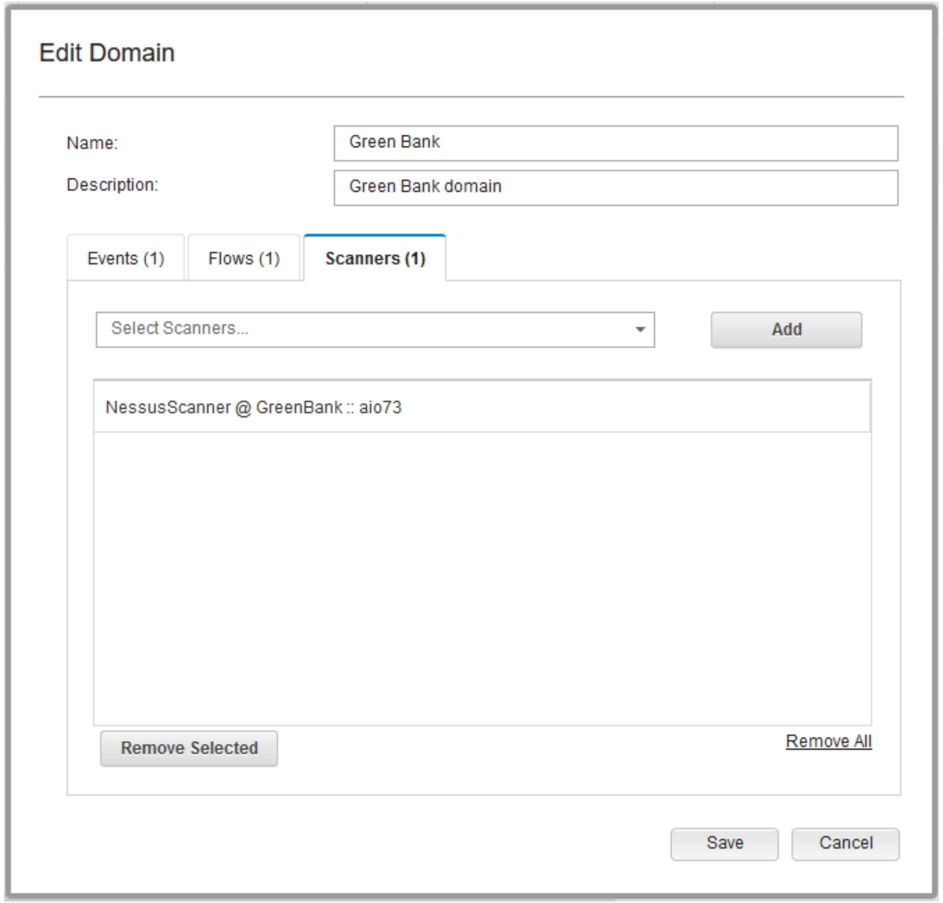
- Events
  - Custom Event Properties
  - Log Sources
  - Log Source Groups
  - Event Collectors
- Flows
- Scanners

Domain Definition – Vulnerabilities – Based on Scanner

A vulnerability scanner is selected to be part of the domain

- The vulnerability was imported by scanner “ScannerName @ Domain”

If the asset in the domain does not exist, QRadar creates a corresponding assets from the scan data and adds a domain tag.



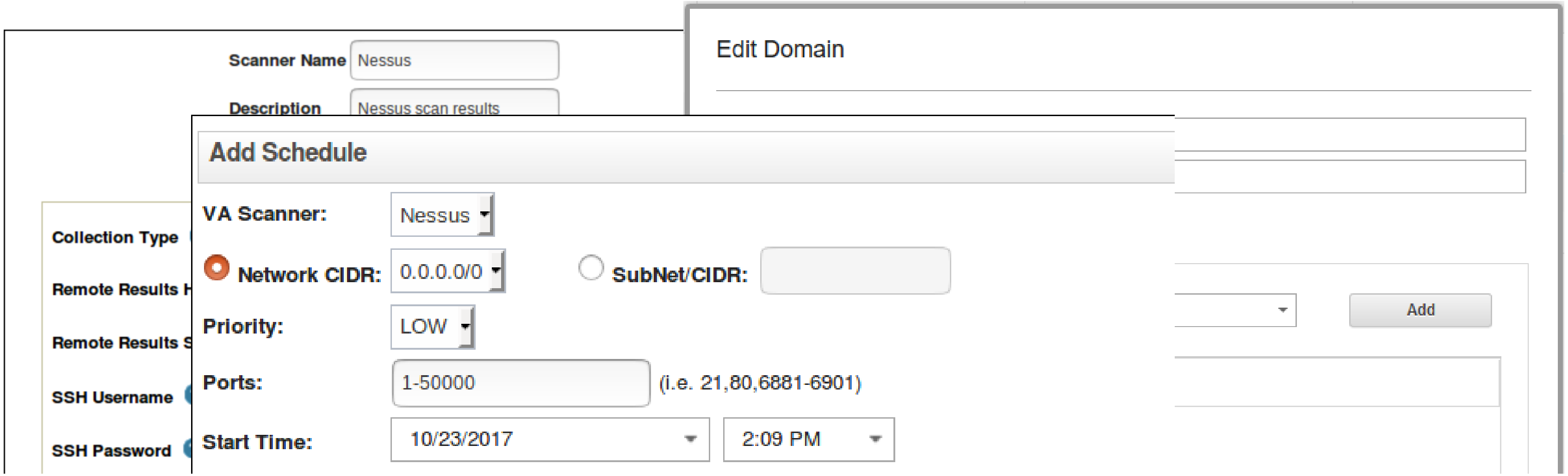
Edit Domain

Name: Green Bank

Description: Green Bank domain

NessusScanner @ GreenBank :: aio73

Example: Import Scan Results from Nessus



Scanner Name: Nessus

Description: Nessus scan results

Collection Type

Remote Results H

Remote Results S

SSH Username

SSH Password

Edit Domain

Add Schedule

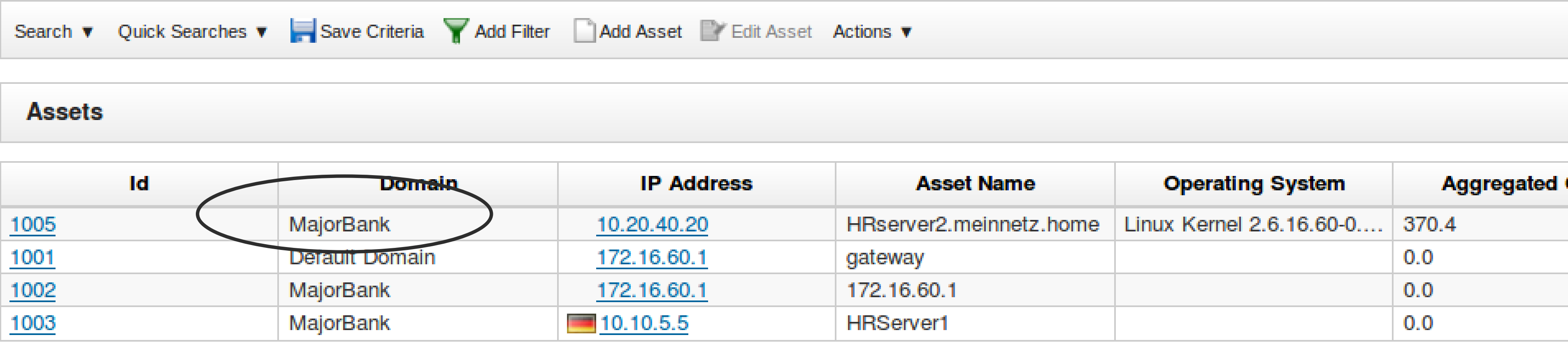
VA Scanner: Nessus

● Network CIDR: 0.0.0.0/0 ○ SubNet/CIDR:

Priority: LOW

Ports: 1-50000 (i.e. 21,80,6881-6901)

Start Time: 10/23/2017 2:09 PM



Assets

Id	Domain	IP Address	Asset Name	Operating System	Aggregated
1005	MajorBank	10.20.40.20	HRserver2.meinnetz.home	Linux Kernel 2.6.16.60-0....	370.4
1001	Default Domain	172.16.60.1	gateway		0.0
1002	MajorBank	172.16.60.1	172.16.60.1		0.0
1003	MajorBank	10.10.5.5	HRServer1		0.0

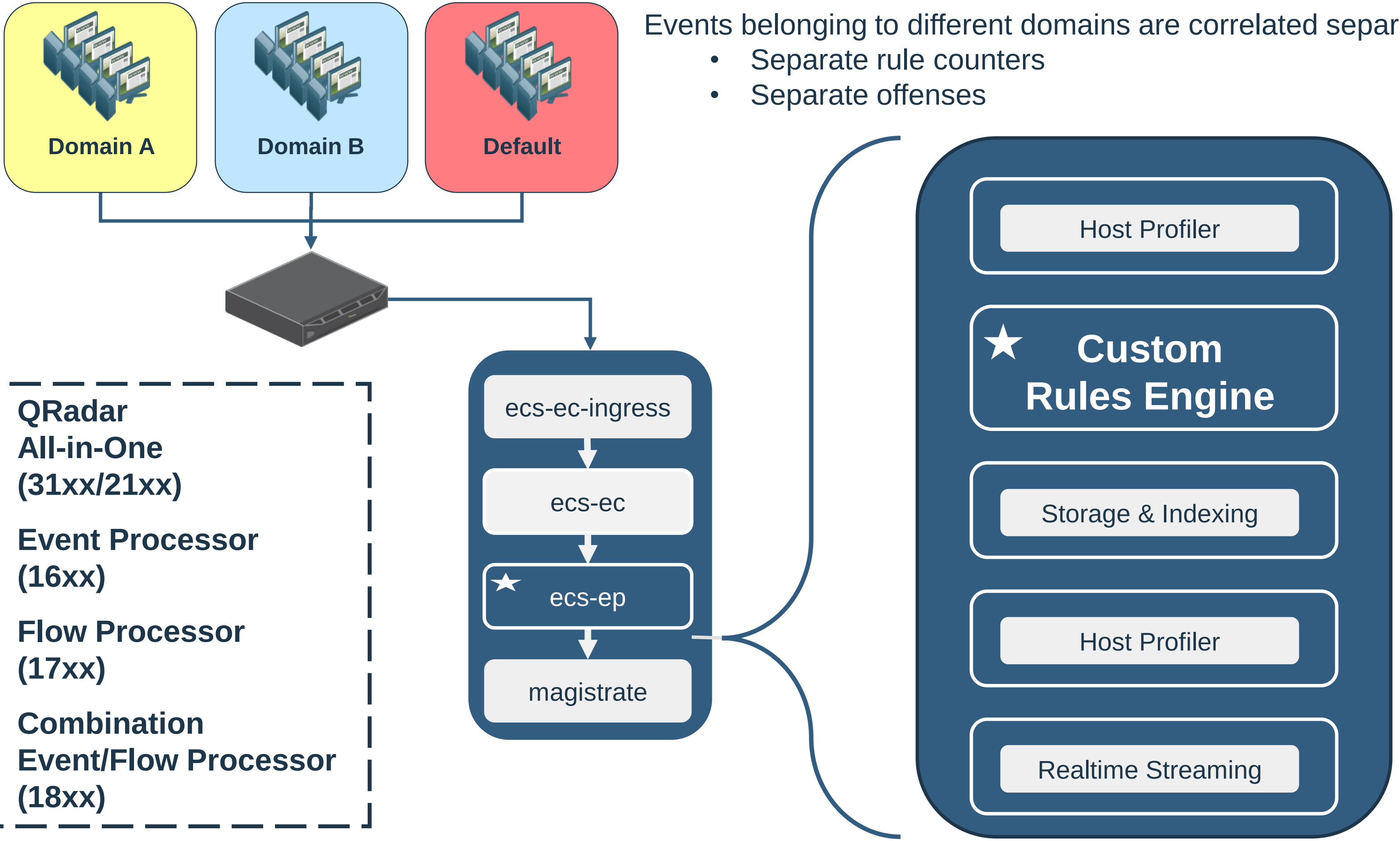
Domain rules

- How does it work?
- Domain unaware rules
- Single domain rules
- Multi-domain rules
- Shared data rules

Where does rule evaluation take place in the event pipeline?

Events belonging to different domains are correlated separately

- Separate rule counters
- Separate offenses



Domain A

Domain B

Default

ecs-ec-ingress

ecs-ec

★ ecs-ep

magistrate

Host Profiler

★ Custom Rules Engine

Storage & Indexing

Host Profiler

Realtime Streaming

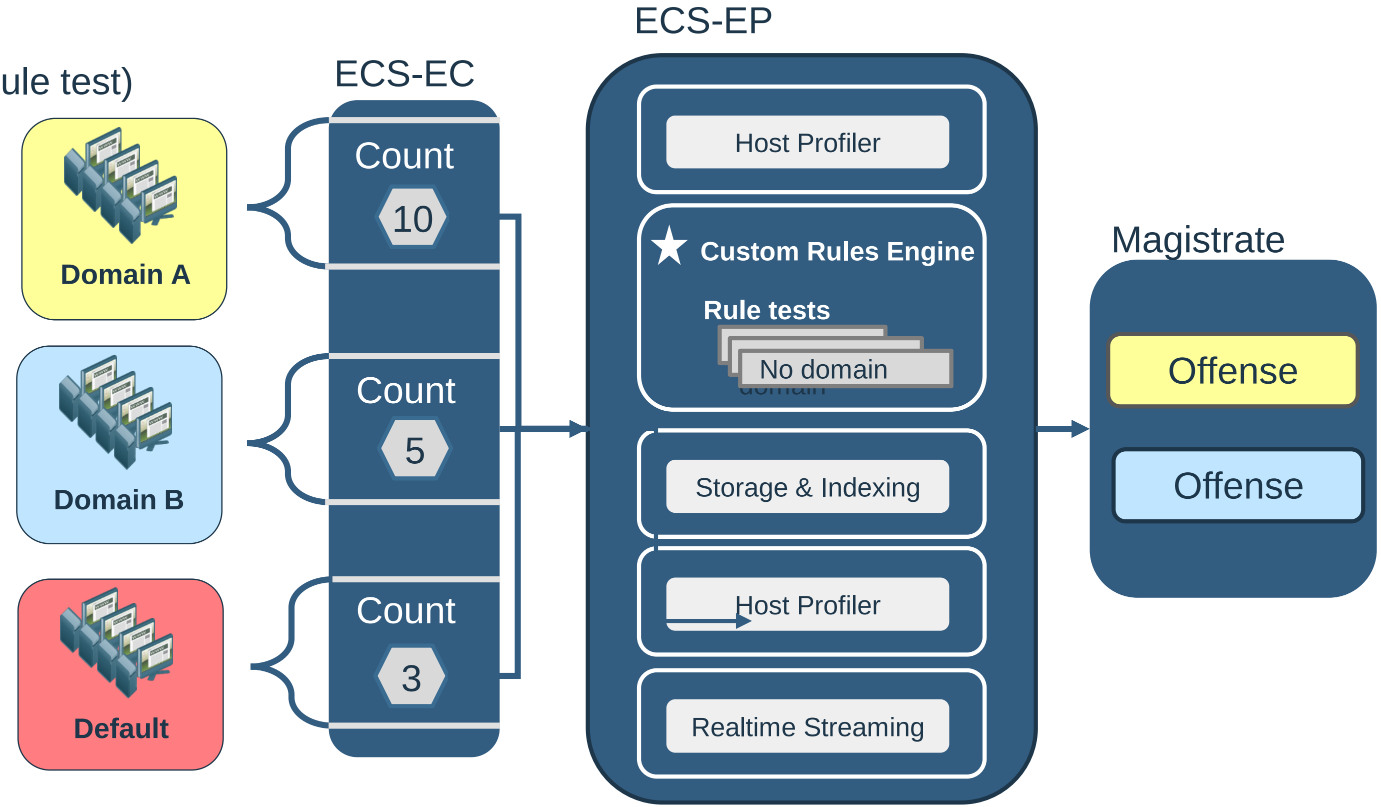
- **QRadar All-in-One (31xx/21xx)**
- **Event Processor (16xx)**
- **Flow Processor (17xx)**
- **Combination Event/Flow Processor (18xx)**

Rules - Domain Unaware Rules

Apply (Rule name) on events which are detected by the Local system
and when BB:GenericAuthentication match at least __5__ times in 5 minutes

If a rule is not domain aware
(does not contain a domain rule test)

- Rule counters are maintained separately for each domain
- The rule is triggered separately for each domain
- Offenses are created separately for each domain that is involved
- The offenses are tagged with those domains.

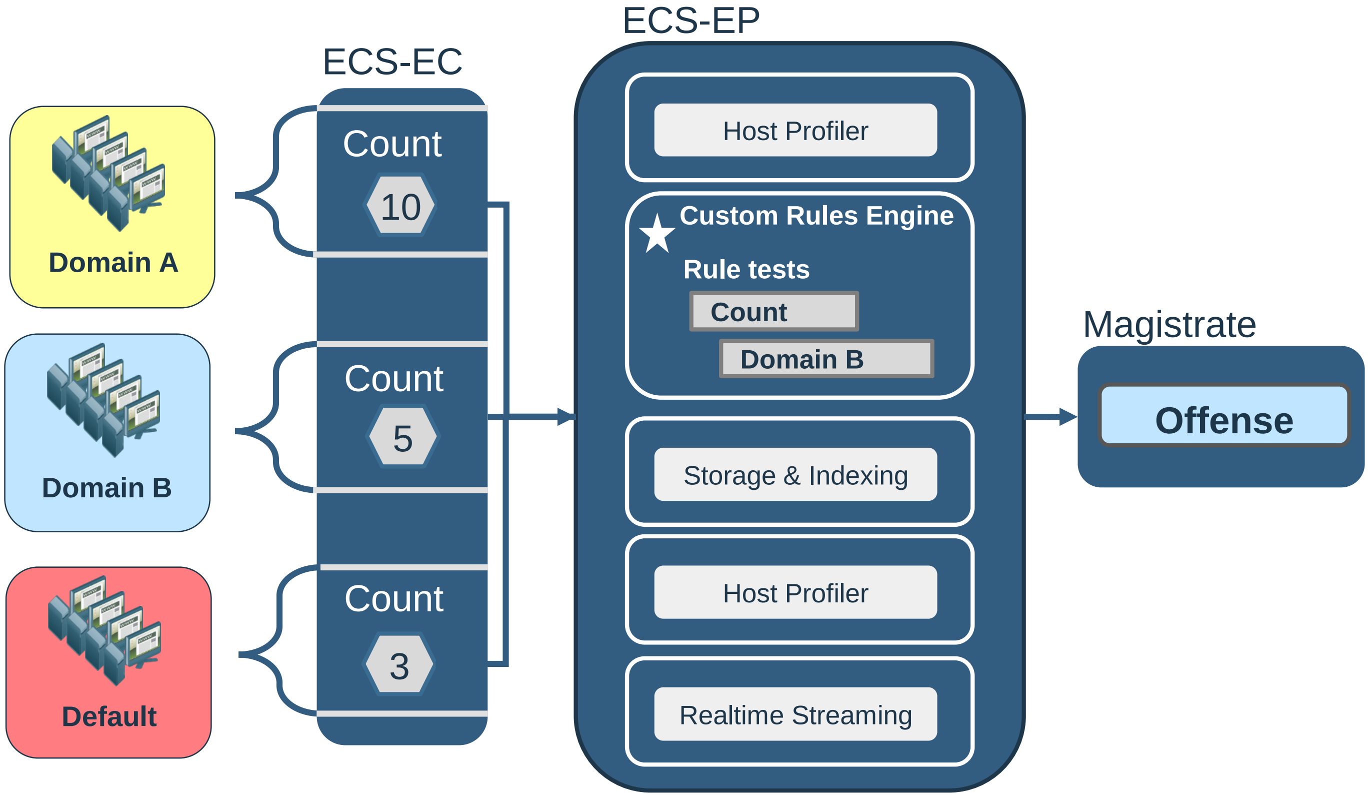


Rules - Single Domain Rules

Apply (Rule name) on events which are detected by the Local system
*and when BB:GenericAuthentication match at least **5** times in 5 minutes*
*and when the domain is one of the following **Domain B***

Single Domain Rule

- Rule counters are maintained separately for each domain
- The offenses are tagged with the domains
- Only events that are tagged with **Domain B** can match against this rule

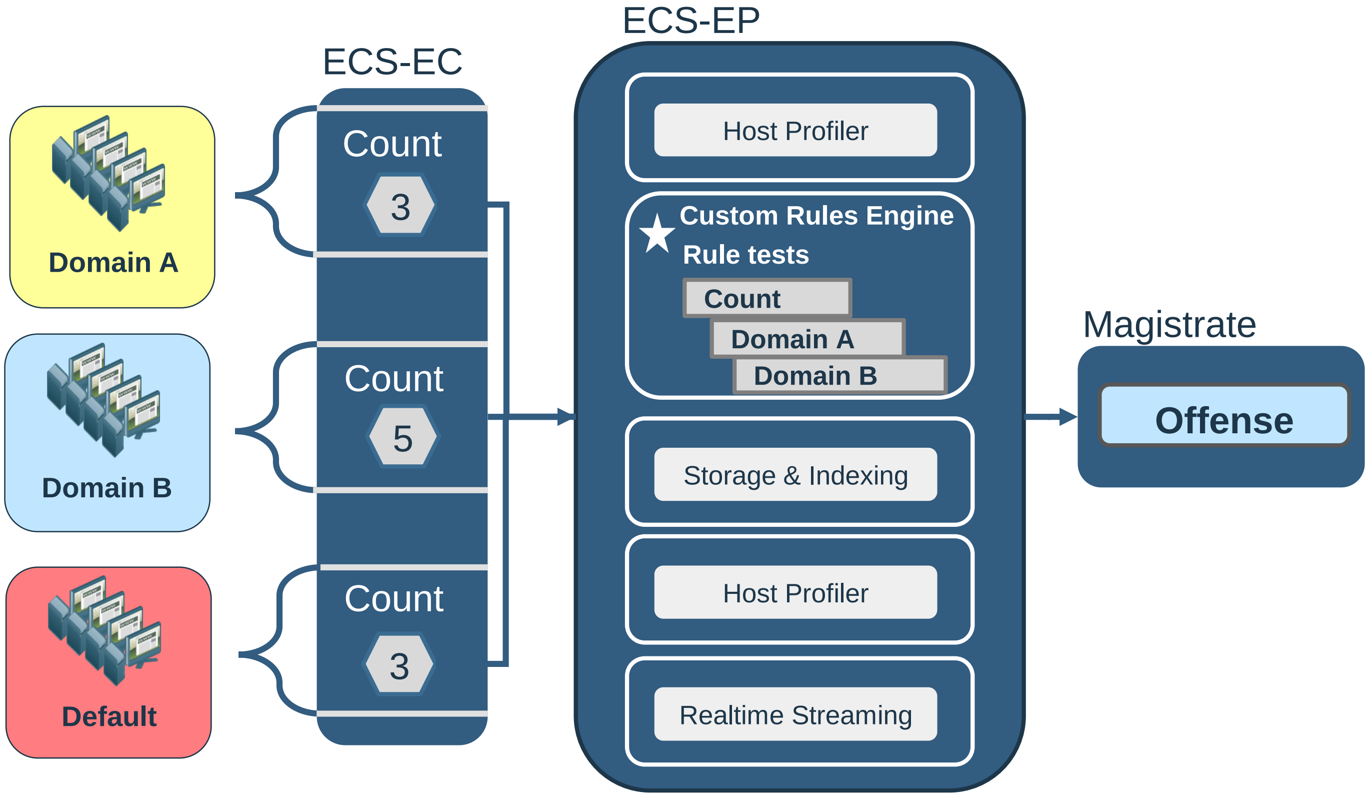


Rules - Multiple Domain Rules

Apply (Rule name) on events which are detected by the Local system
*and when BB:GenericAuthentication match at least **5** times in 5 minutes*
*and when the domain is one of the following **Domain A**, **Domain B***

Multiple Domain Rule

- Rule counters are maintained separately for each domain
- The rule is triggered separately for each domain
- Offenses are created separately for each domain that is involved
- The offenses are tagged with those domains
- Only events that are tagged with these domains can match against this rule

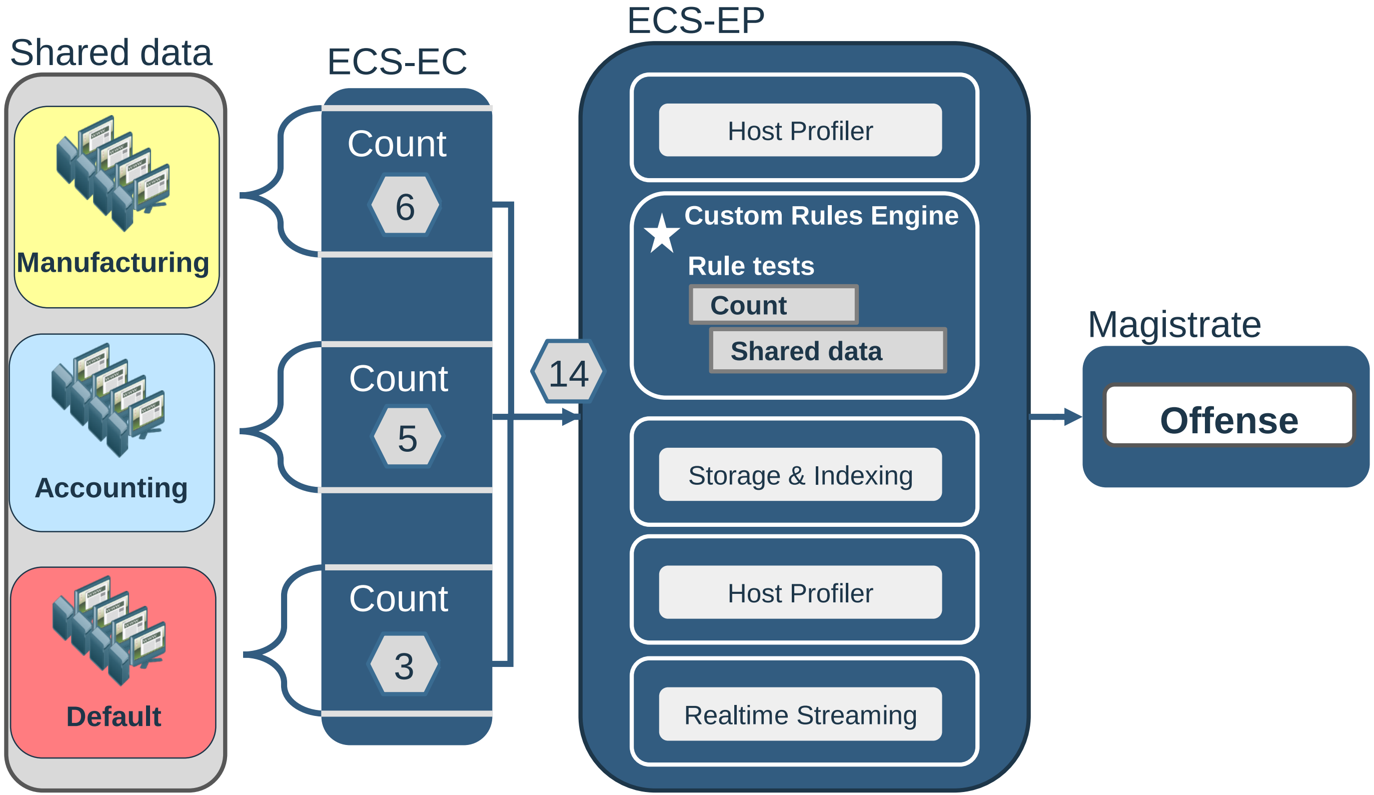


Rules - Shared Data Rules

Apply (Rule name) on events which are detected by the Local system
and when B BB:GenericAuthentication match at least ***5*** *times in 5 minutes*
and when the domain is one of the following ***Shared data***

Share Data Rule

- The counters are maintained across all domains
- The rule is triggered once and contains events from all domains
- the offense is tagged with domain "All Domains"
- all events can match against this rule regardless of their domain



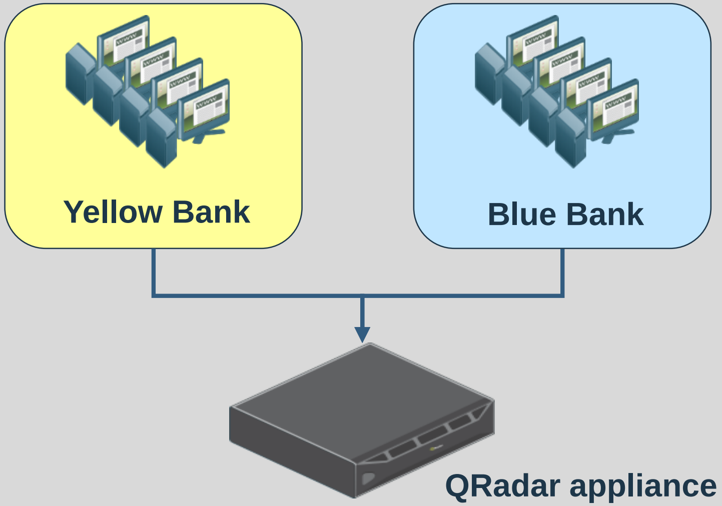
Tenants

- About tenants
- Creating tenants
- Assigning tenants
- Retention buckets for tenants

About Multi Tenancy in QRadar

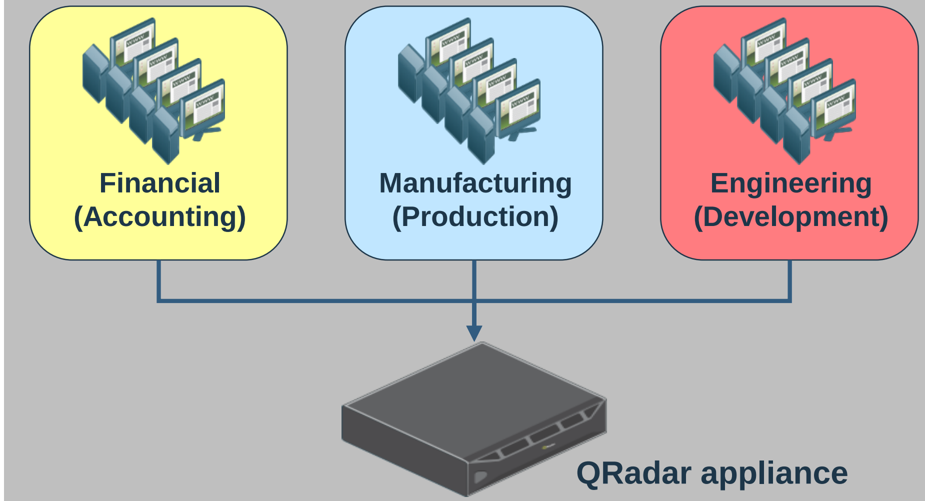
Tenant are subsets of a domain in QRadar and allow specific controls for the tenants within the assigned domain.

- Manage network hierarchy for a tenant
- Apply license restrictions
- Create retention areas for specific tenant data



Multi Tenancy – what is it good for?

- Managed Security Service Providers (MSSP)
- Customers see only their data by creating domains that are based on their QRadar input sources
- Provide security services to multiple client organizations from a single, shared IBM Security QRadar deployment
- Multi-divisional organizations



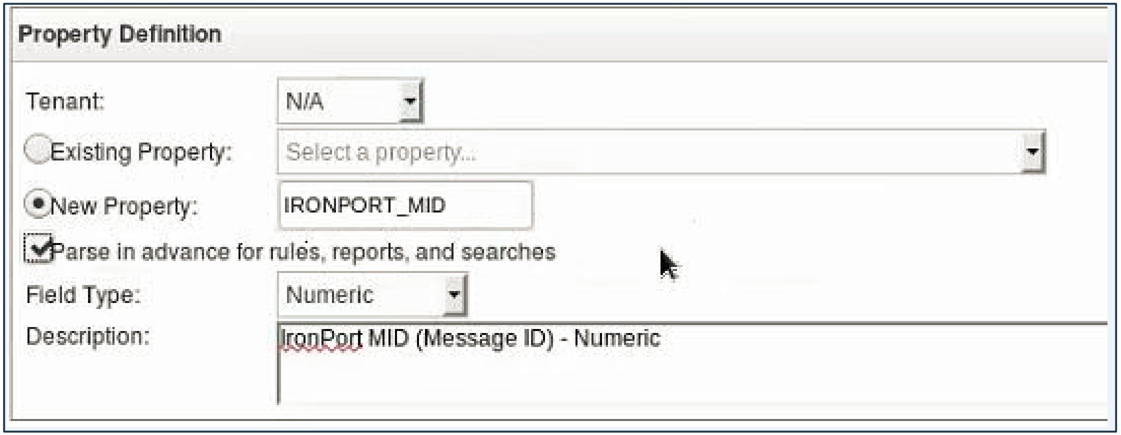
Tenant Management: About custom properties

Can tenants create custom properties, should they?

A Delegated administrators can create custom properties; however they cannot select **Parse in advance for rules, reports, and searches**’.

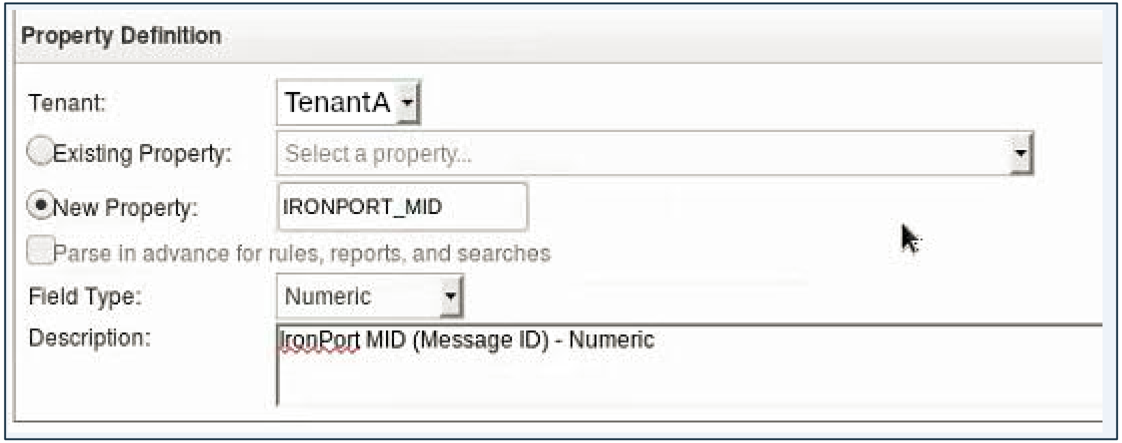
Why?
This is intentional as improperly written or very complex custom properties can impact the overall pipeline for all users. Tenants should not create issues for other tenants that happen to share an appliance.

What is the best option?
It is best to have the overall admin own the custom property without any tenant assignment for all users. CEPs are generally pretty safe to share between tenants as it is just a name / property.



Property Definition

Tenant: N/A
○ Existing Property: Select a property...
● New Property: IRONPORT_MID
☑ Parse in advance for rules, reports, and searches
Field Type: Numeric
Description: IronPort MID (Message ID) - Numeric



Property Definition

Tenant: TenantA
○ Existing Property: Select a property...
● New Property: IRONPORT_MID
□ Parse in advance for rules, reports, and searches
Field Type: Numeric
Description: IronPort MID (Message ID) - Numeric

Tenant Management: Create new tenants

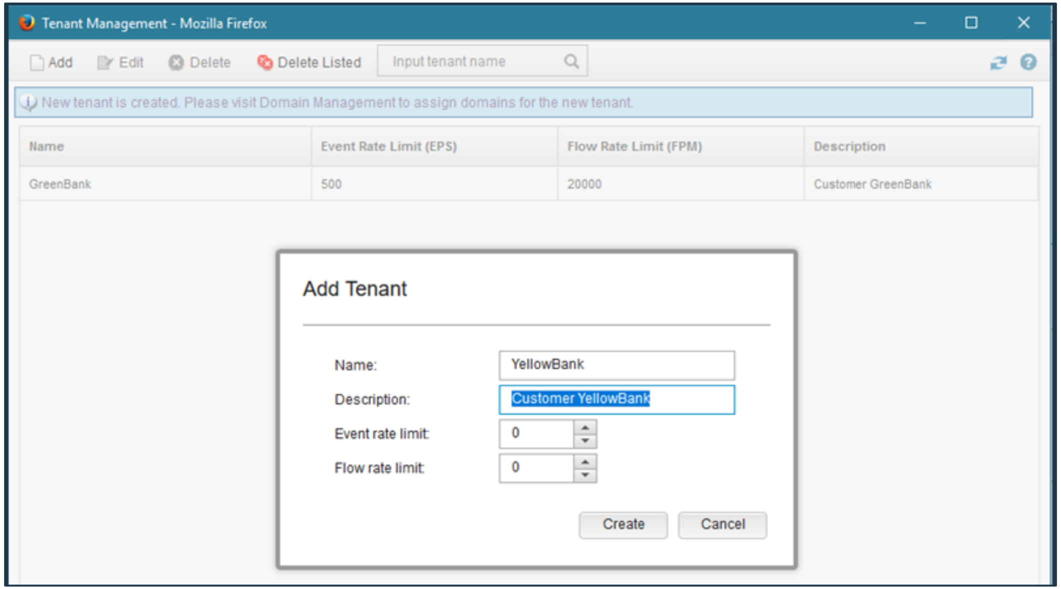
Creating a tenant does not require a deploy in QRadar.

A delegated administrator can adjust the following properties for each tenant:

- Event Per Second
- Flows Per Minute

About tenant rate limits
When you assign a rate limit to the data incoming for a tenant, there is a throttle that takes place when tenants exceed their set event or flow rate.

Default value is 1.5 meaning 150% of EPS limit value before events are dropped.



New tenant is created. Please visit Domain Management to assign domains for the new tenant.

Name	Event Rate Limit (EPS)	Flow Rate Limit (FPM)	Description
GreenBank	500	20000	Customer GreenBank

Add Tenant

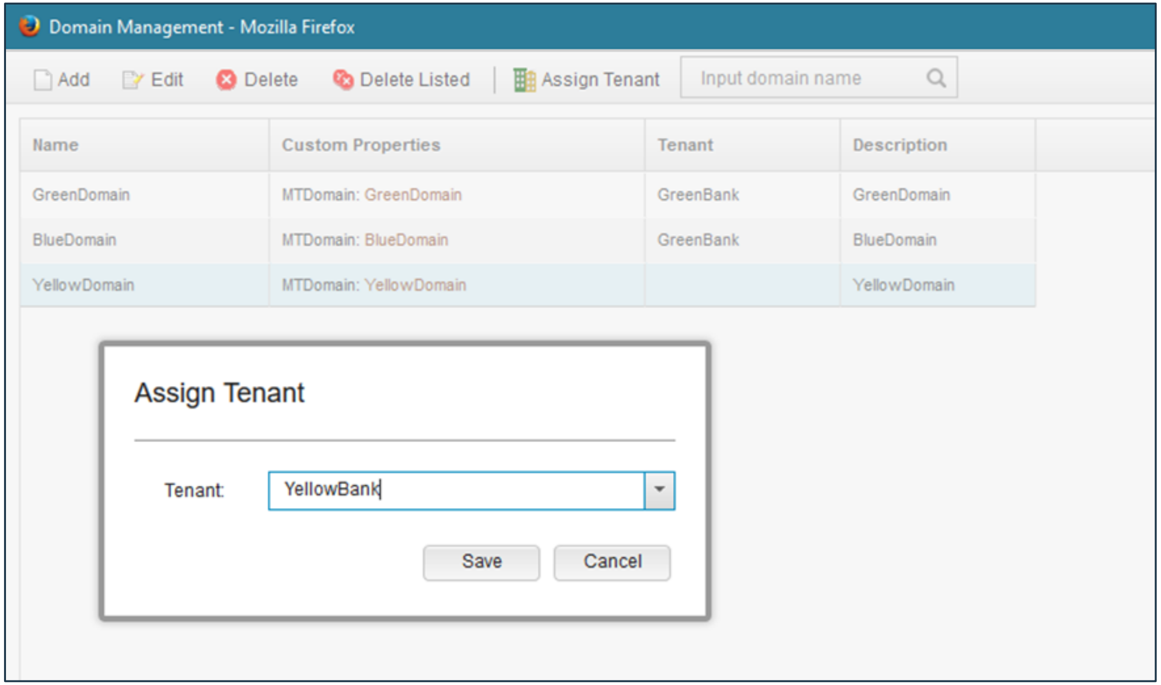
Name: YellowBank
Description: Customer YellowBank
Event rate limit: 0
Flow rate limit: 0

If a tenant goes too far above license or the queue is full due to processing overload the event can be dropped. This information is logged:

```
[Tenant:<tenantID>:<tenantName>] Event dropped while attempting to add to Tenant
Event Throttle queue. The Tenant Event Throttle queue is full.
```

Tenant Management: Assign domains to tenants

- Domains are the building blocks for multitenant environments
- A tenant can have one more domains
- If no domains are configured, the events and flows are assigned to the default domain
- All internal events go to the default domain, except the event collector is assigned to a domain



Name	Custom Properties	Tenant	Description
GreenDomain	MTDomain: GreenDomain	GreenBank	GreenDomain
BlueDomain	MTDomain: BlueDomain	GreenBank	BlueDomain
YellowDomain	MTDomain: YellowDomain		YellowDomain

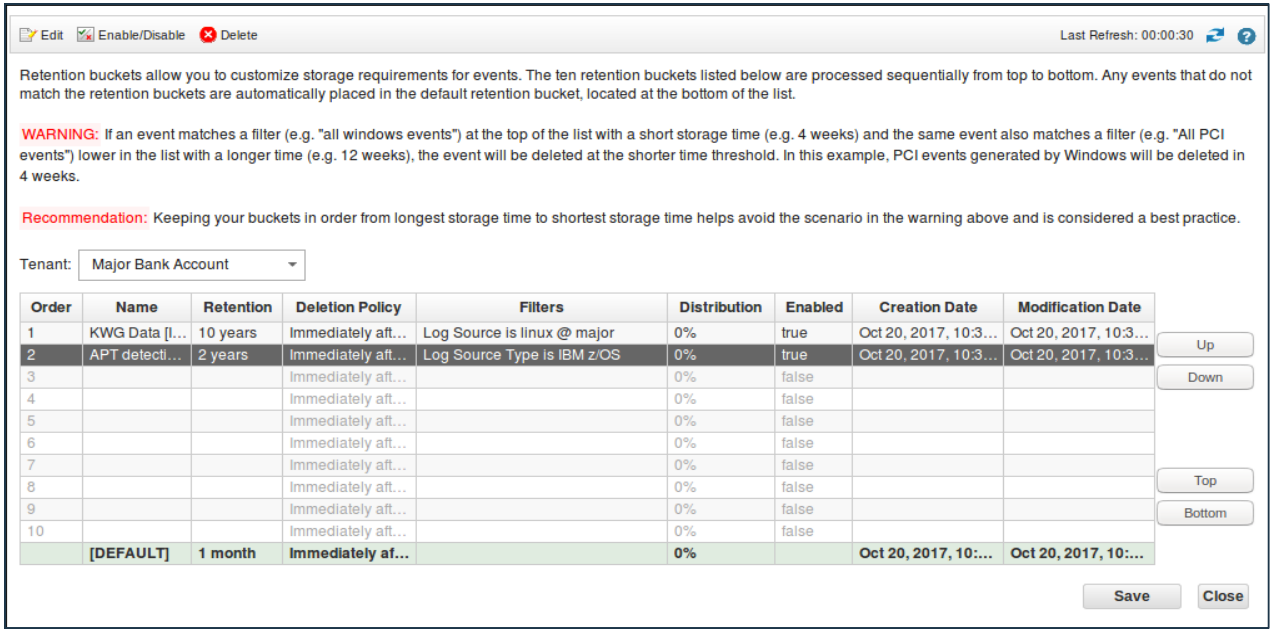
Assign Tenant

Tenant: YellowBank

Tenant Management: Define Retention Periods

Each tenant can have separate retention buckets

- Retention buckets for tenants are stored in /store/ariel/events/payloads/aux/<tenantID>/ /store/ariel/events/records/aux/<tenantID>/
- There can be up to 10 separate buckets for each tenant



Retention buckets allow you to customize storage requirements for events. The ten retention buckets listed below are processed sequentially from top to bottom. Any events that do not match the retention buckets are automatically placed in the default retention bucket, located at the bottom of the list.

WARNING: If an event matches a filter (e.g. "all windows events") at the top of the list with a short storage time (e.g. 4 weeks) and the same event also matches a filter (e.g. "All PCI events") lower in the list with a longer time (e.g. 12 weeks), the event will be deleted at the shorter time threshold. In this example, PCI events generated by Windows will be deleted in 4 weeks.

Recommendation: Keeping your buckets in order from longest storage time to shortest storage time helps avoid the scenario in the warning above and is considered a best practice.

Tenant: Major Bank Account

Order	Name	Retention	Deletion Policy	Filters	Distribution	Enabled	Creation Date	Modification Date
1	KWG Data [I...	10 years	Immediately aft...	Log Source is linux @ major	0%	true	Oct 20, 2017, 10:3...	Oct 20, 2017, 10:3...
2	APT detecti...	2 years	Immediately aft...	Log Source Type is IBM z/OS	0%	true	Oct 20, 2017, 10:3...	Oct 20, 2017, 10:3...
3			Immediately aft...		0%	false		
4			Immediately aft...		0%	false		
5			Immediately aft...		0%	false		
6			Immediately aft...		0%	false		
7			Immediately aft...		0%	false		
8			Immediately aft...		0%	false		
9			Immediately aft...		0%	false		
10			Immediately aft...		0%	false		
	[DEFAULT]	**1 month**	**Immediately af...**		**0%**		**Oct 20, 2017, 10:...**	**Oct 20, 2017, 10:...**

Further reading (support article): http://www.ibm.com/support/docview.wss?uid=swg22010279

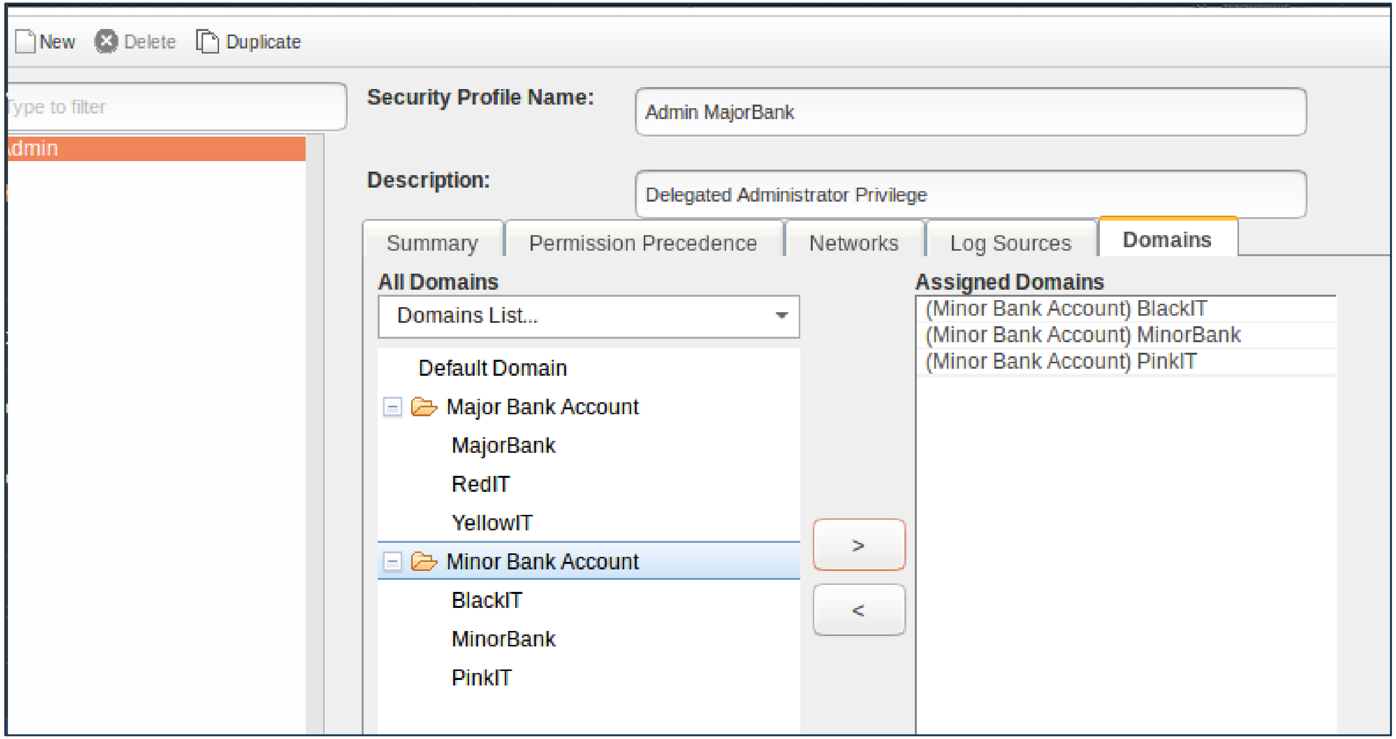
Security profiles and users

- About security profiles and tenants
- Creating tenants
- Assigning tenants
- Retention buckets for tenants

Security Profiles determine what data a domains user has access to

- A list of tenants appear in the Assigned Domains section as:
  (Domain) Tenant name

- You can assign tenants or individual domains



Security Profile Name: Admin MajorBank

Description: Delegated Administrator Privilege

Assigned Domains

(Minor Bank Account) BlackIT
(Minor Bank Account) MinorBank
(Minor Bank Account) PinkIT

Domains and Security Profiles

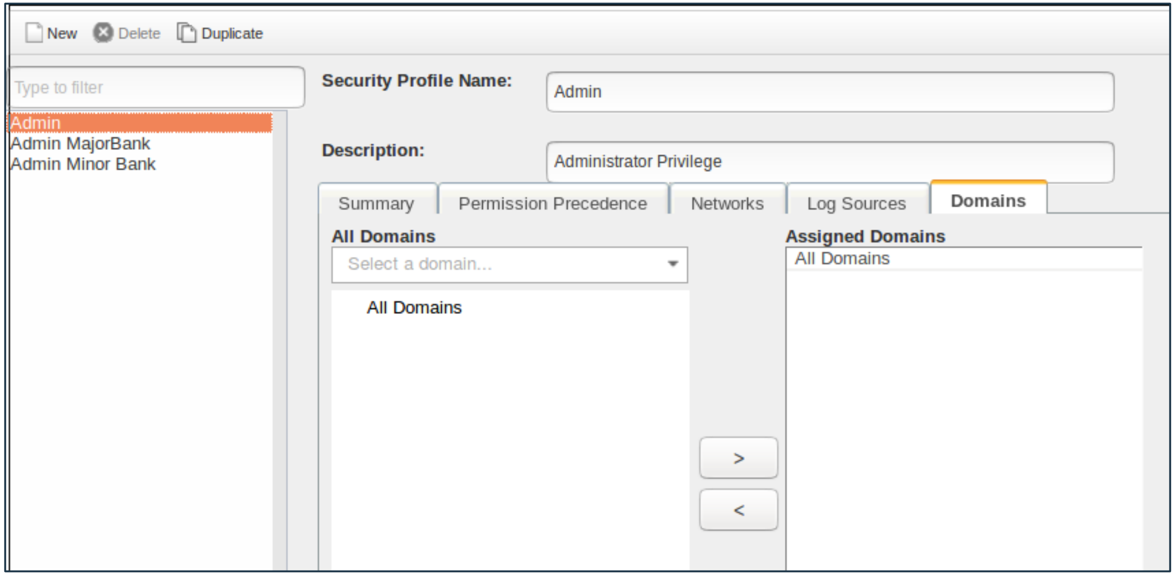
Users are assigned to domains through Security Profiles

Assigned Domains

- Add a list of domains
  A user of this profile will have access to these domains.

All Domains

- Can see all active domains within the system, as well as the default domain and any domains that were previously deleted across the entire system
- They will also be able to see all domains that will be created in the future



Admin
Admin MajorBank
Admin Minor Bank

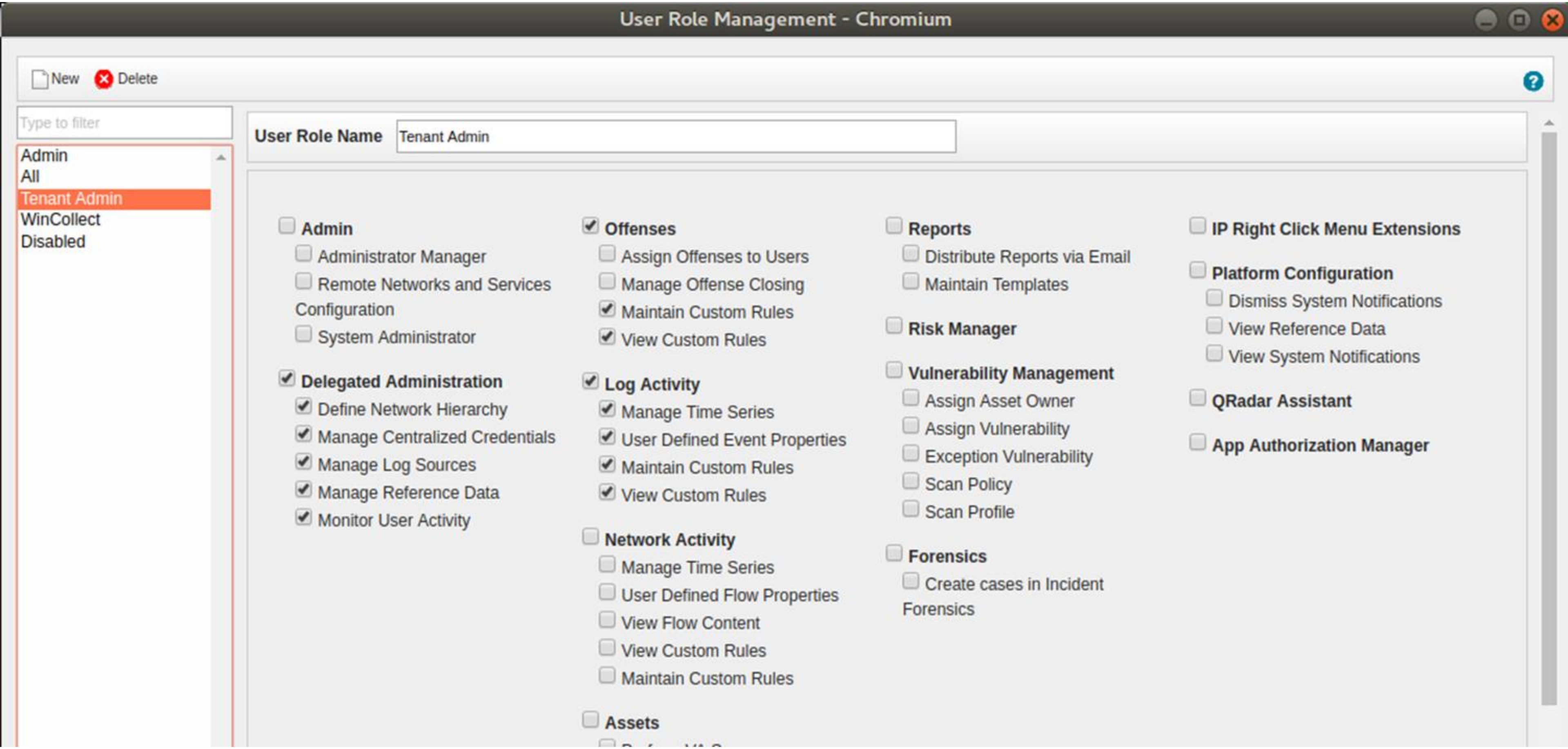
Security Profile Name: Admin

Description: Administrator Privilege

All Domains: All Domains

Assigned Domains: All Domains

The user role for tenants is delegated administration



Admin
All
Tenant Admin
WinCollect
Disabled

User Role Name: Tenant Admin

□ **Admin**
- □ Administrator Manager
- □ Remote Networks and Services Configuration
- □ System Administrator

☑ **Delegated Administration**
- ☑ Define Network Hierarchy
- ☑ Manage Centralized Credentials
- ☑ Manage Log Sources
- ☑ Manage Reference Data
- ☑ Monitor User Activity

☑ **Offenses**
- □ Assign Offenses to Users
- □ Manage Offense Closing
- ☑ Maintain Custom Rules
- ☑ View Custom Rules

☑ **Log Activity**
- ☑ Manage Time Series
- ☑ User Defined Event Properties
- ☑ Maintain Custom Rules
- ☑ View Custom Rules

□ **Network Activity**
- □ Manage Time Series
- □ User Defined Flow Properties
- □ View Flow Content
- □ View Custom Rules
- □ Maintain Custom Rules

□ **Assets**

□ **Reports**
- □ Distribute Reports via Email
- □ Maintain Templates

□ **Risk Manager**

□ **Vulnerability Management**
- □ Assign Asset Owner
- □ Assign Vulnerability
- □ Exception Vulnerability
- □ Scan Policy
- □ Scan Profile

□ **Forensics**
- □ Create cases in Incident Forensics

□ **IP Right Click Menu Extensions**

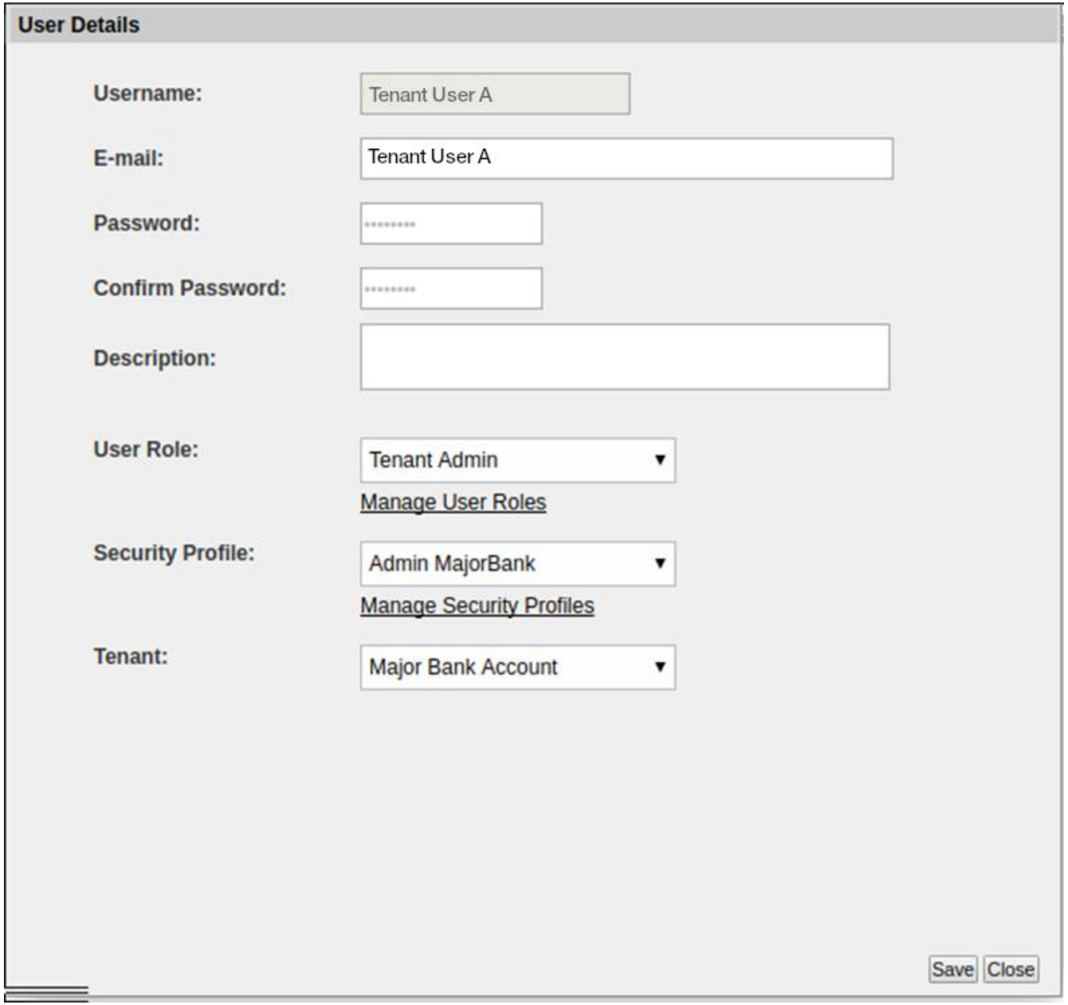
□ **Platform Configuration**
- □ Dismiss System Notifications
- □ View Reference Data
- □ View System Notifications

□ **QRadar Assistant**

□ **App Authorization Manager**

User Details screen

- When defining the user you assign a tenant to the user
- QRadar checks if all definitions in the security profile comply with the tenant assignment.

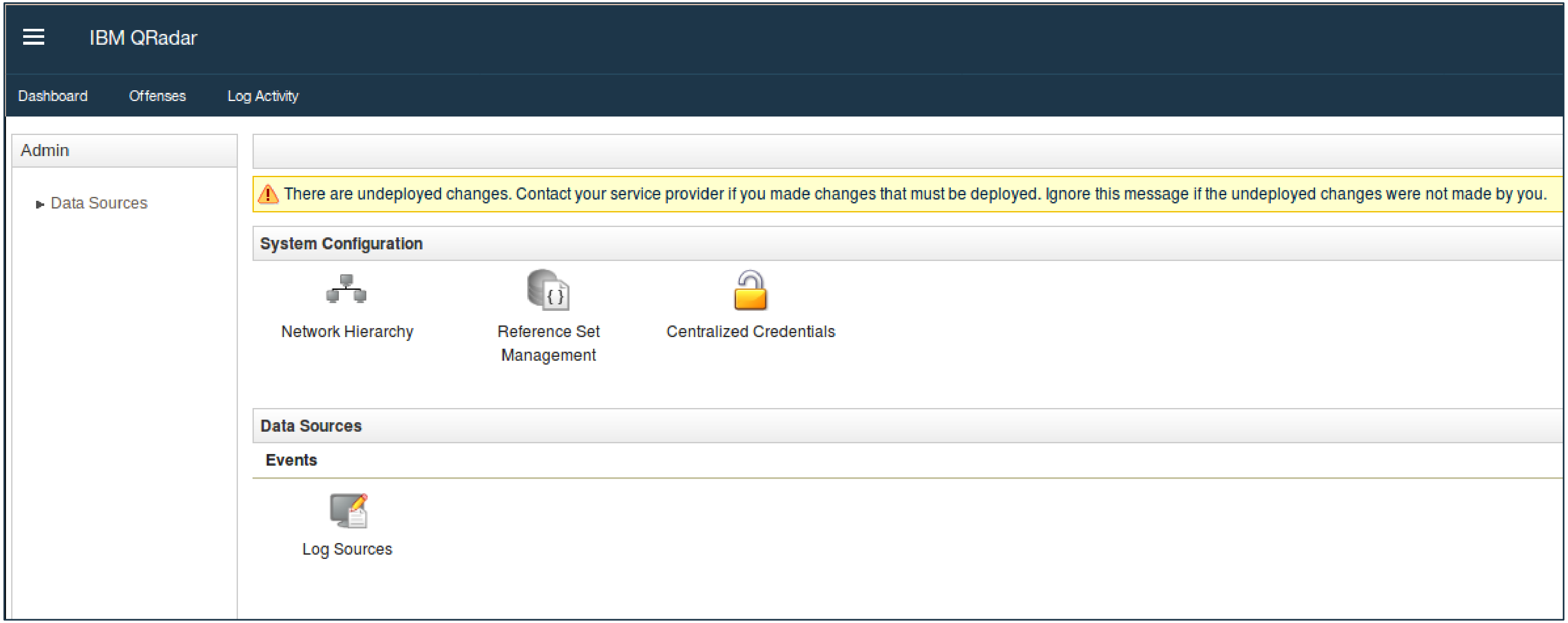


User Details

Username:	Tenant User A
E-mail:	Tenant User A
Password:	•••••••••
Confirm Password:	•••••••••
Description:	
User Role:	Tenant Admin ▾ Manage User Roles
Security Profile:	Admin MajorBank ▾ Manage Security Profiles
Tenant:	Major Bank Account ▾

Delegated administrators see a reduced set of admin applications

Tenant administrator icon list

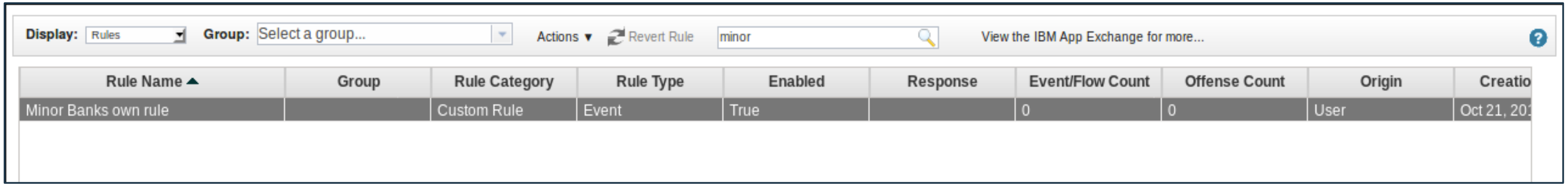


There are undeployed changes. Contact your service provider if you made changes that must be deployed. Ignore this message if the undeployed changes were not made by you.

NOTE: Visibility of tab is dictated by the permissions provided in the Security Profile. In this example, the user does not have the Reports, Vulnerabilities tabs enabled.

Defining access rights in a multi domain environment

TIP: Rules can be viewed, modified, or disabled by any user who has both the Maintain Custom Rules and View Custom Rules permissions, regardless of which domain that user belongs to.



Display: Rules **Group:** Select a group... minor

Rule Name ▲	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	Creatio
Minor Banks own rule		Custom Rule	Event	True		0	0	User	Oct 21, 201

When sending events or flows to another QRadar environment, all domain information is removed as the domain tags are meta data in QRadar and not part of the initial payload. If you forward events events and flows belong to the default domain in the receiving system.

Questions?

Domain & Tenant Questions

Question 1
I have Domain A, which has Windows Server 192.168.100.100
I have Domain B, which has Linux Server 192.168.100.100.
My building block BB:HostDefinition: Windows Servers is configured with 192.168.100.100

If that Linux server in Domain B uses BB:PortDefinition: Windows Ports, BB:ProtocolDefinition: Windows Protocols, it passes BB:HostDefinition: Windows Servers rule test, will it fire a false positive?

Answer: Yes, until Server Discovery in QRadar is domain aware, you probably need a custom property to define when this data belongs to either the Windows Server or the Linux server. This is something on our road map at the moment to all Server Discovery to support domains.

Question 2
What is the maximum number of tenants for a QRadar deployment?

Answer: There is no hard limit, but how much will work depends on the environment specifics (and possibly the license capacity you have at hand if you are assigning event or flow rates to each tenant). We test up to 150 tenants when we validate QRadar builds before release.

Domain & Tenant Questions (Continued)

Question 3
We want to a domain in the reference set, for example: https://www.microsoft.com. Can we add the wild card entries like `* .microsoft.com` or `https://www.microsoft.*` to refer the entire domain and it's sub domains?

Answer: No, wildcard entries are not supported. Data contained within the extended URL can fill references sets with unique values due to the variability and volume of URL data. Typically, it is best to create a property that matches the root or header domains and expand on those requirements as needed.

Question 4
Does QRadar has the ability to export and import configurations based on the per domains segregations? In an MSSP deployment, I want to only restore a configurations backup only for a single client to another QRadar instance is that possible?

Answer: No, not at this time.

Question 5
Does the User Behavior Analytics app support multi tenancy?

Answer: No, multi tenancy is not supported currently is any QRadar application. This functionality is being looked at to be added in a future release.

Domain & Tenant Questions (Continued)

Question 6
Can I have log sources with same log source identifier and log source type?

Answer: The only way to have two log sources of the same type and same Log Source Identifier is if they are using different protocol types.

In an overlapping IP scenario, the system does not end up with two log sources. What really happens is that one log source with (for example) Log Source Identifier=10.10.10.10 ends up actually collecting logs from two different physical machines, each with IP address 10.10.10.10. Each individual event can be tagged with a domain, and in the case of a shared log source situation like this, the separation is done using custom properties.

If there is some field in the events that can be used to differentiate between events for domain A versus events for domain B, then you could create a custom property to capture this field's value for the log source type in question, then assign particular values of that property to each domain. So all events get linked to a single log source which is domain-agnostic, but each event received by that log source is tagged for either domain A or domain B based on the value of the custom property

Domain & Tenant Questions (Continued)

Question 7
Is there a way to create an advanced search (AQL) to get the EPS rate for each specific tenant?

Answer: We do not keep track of EPS rates on a per-tenant basis by default at this time. If you wanted to create a query to track EPS data, it would be a big query where you are counting domains over time, but it should be possible to do. We are looking in to this question to provide an answer and an example query. We'll likely take this follow-up to the forums to answer.

Question 8
If I want to use an advanced query to find a domain, is there a way to do so without using the domain ID?

Answer: Yes, you need to use DOMAINNAME(domainid) instead of just domainid in your advanced search. The DOMAINNAME function will look up the name for you and can be used with matches, imatches, like, ilike, etc.

Question 9
Is there a way to query the lack of a domain in an advanced search parameter?

Yes, if you wanted to audit for data that is not assigned to a domain, you could use use **`'NULL' AS Domain`** in your advanced search query to help locate this data.

IBM Security

THANK YOU

FOLLOW US ON:

- 🌐 ibm.com/security
- 🌐 securityintelligence.com
- 🌐 xforce.ibmcloud.com
- 🐦 @ibmsecurity
- ▶ youtube/user/ibmsecuritysolutions

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.