

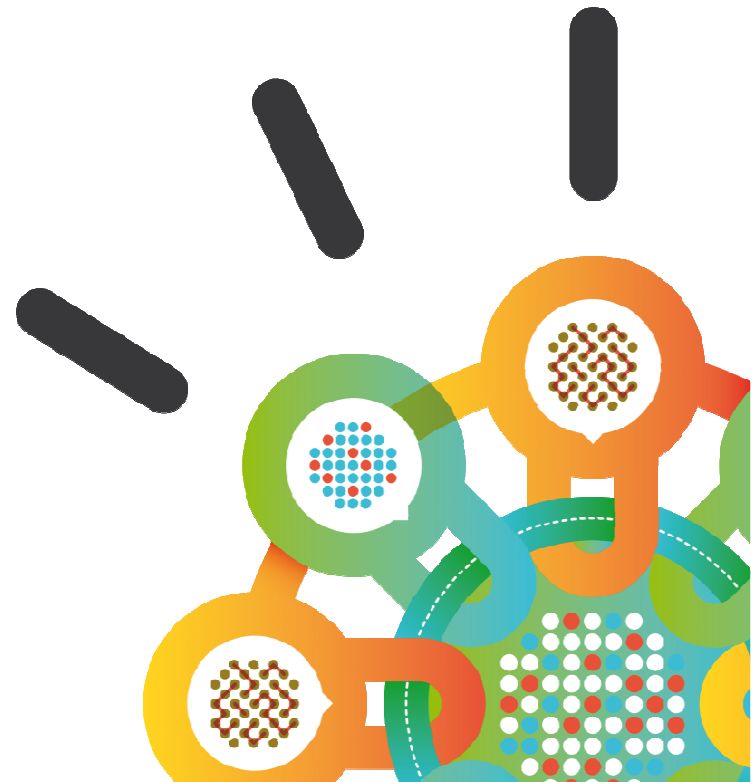
---

Security Intelligence.  
Think Integrated.

## IBM Security QRadar SIEM v7.2.2

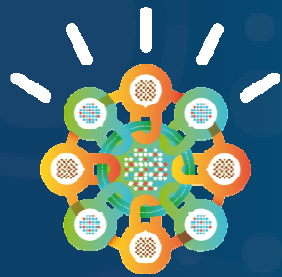
### New Feature Overview

April, 2014



## BIG and exiting QRadar Release

- § New appliances, capabilities and features to handle even more data more quickly !
  - Higher EPS, more disk, additional powerful and cost effective expansion options
  - Customers NEED this now and it is unique
- § New APIs !
  - Now have open APIs to QRadar flow and event data
  - SOC integration, improved visualization enablement, value add enablement for business partners, and much more ....
- § Faster !
  - More tuning, optimizations and options to make QRadar searches faster
- § Translated
  - Fantastic new translation and globalization capabilities
  - Users can now pick their language !
- § Exciting new approach to user documentation



# Opening up QRadar data and analytics

## New APIs - Events and Flows

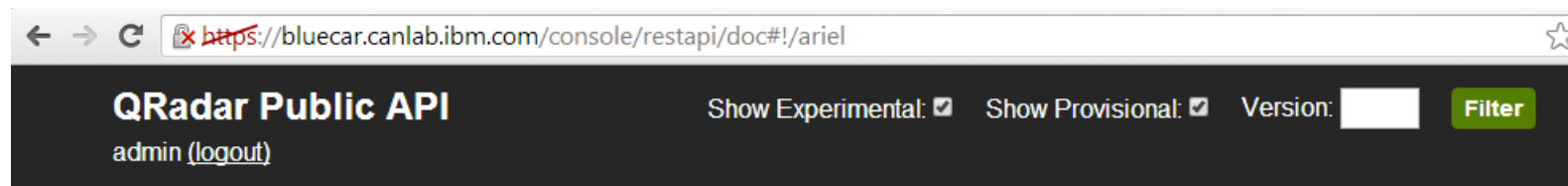


## Open APIs – Events and Flows

- § Customers and Partners can now easily do the following in a supported manner:
- Integrate third-party reporting solutions using our API to report on Events / Flows
  - Create custom dashboards / visualizations on Events and Flows
  - Allows for operations on QRadar's data, that is not currently supported in the UI  
e.g. Historical Correlation (think scripting)
  - Selective data backup – Query and preserve only the data you want to keep
  - Advanced Use cases – Easily implement use cases that are not currently feasible in the UI. E.g.: Custom application that Maps Nat IP to Internal IP and presents a view on its relationships.
  - Query and feed valuable data to other Big Data solutions for long term machine data analysis or data warehouse.

## Open APIs – Events and Flows

- The Ariel API documentation page can be viewed from URL:
- [https://QRadar\\_IP/console/restapi/doc](https://QRadar_IP/console/restapi/doc)



/ariel		Show/Hide APIs	List APIs
GET	/databases	Show/Hide Versions	List Versions
GET	/databases/{databaseName}	Show/Hide Versions	List Versions
GET	/searches	Show/Hide Versions	List Versions
POST	/searches	Show/Hide Versions	List Versions
GET	/searches/{searchID}	Show/Hide Versions	List Versions
POST	/searches/{searchID}	Show/Hide Versions	List Versions
DELETE	/searches/{searchID}	Show/Hide Versions	List Versions
GET	/searches/{searchID}/results	Show/Hide Versions	List Versions

# Open APIs – Events and Flows

- Along with definition, try your queries!

**Error Responses**

HTTP Response	Unique Code	Description
409	1004	The search could not be created, the searchID provided is already in use. Please use a unique searchID.
422	2000	The queryExpression contains invalid AQL syntax.
422	1005	A request parameter is not valid.
500	1020	An error occurred while attempting to create a new search.

**Response Type**

MIME Type	Sample
<input checked="" type="checkbox"/> application/json	<a href="#">Show/Hide</a>

**Parameters**

Parameter	Type	Value	Data Type	MIME Type	Sample	Details
queryExpression	query	<input type="text" value="select * from event"/>	String	text/plain	<a href="#">View</a>	Required - The AQL query to execute.
queryLanguageVersion	query	<input type="text"/>	Integer	text/plain	<a href="#">View</a>	Optional - The version of the AQL expression. Acceptable values are "1" and "2". The default value is "2".
searchID	query	<input type="text"/>	String	text/plain	<a href="#">View</a>	Optional - A searchID value to be used for the new search instead of a system generated searchID. The searchID must be
startTime	query	<input type="text"/>	Long	text/plain	<a href="#">View</a>	Optional - The beginning of the query time interval, in milliseconds since 0:00:00 1/1/1970. The queryExpression time interval
endTime	query	<input type="text"/>	Long	text/plain	<a href="#">View</a>	Optional - The end of the query time interval, in milliseconds since 0:00:00 1/1/1970. The queryExpression time interval

[Try it out!](#)

## Give your search result a nice name – and re-query it

Parameters

Parameter	Type	Value	Data Type	MIME Type	Schema	Details
queryExpression	query	<code>select * from events w</code>	String	text/plain ▼	<a href="#">View</a>	Required - The AQL query to execute.
queryLanguageVersion	query		Integer	text/plain ▼	<a href="#">View</a>	Optional - The version of the AQL expression. Acceptable values are "1" and "2". The default value is "2".
searchID	query	<code>mybadguys</code>	String	text/plain ▼	<a href="#">View</a>	Optional - A searchID value to be used for the new search instead of a system generated searchID. The searchID must be unique and is only used for SELECT
startTime	query		Long	text/plain ▼	<a href="#">View</a>	Optional - The start time for the search.

Parameters

Parameter	Type	Value	Data Type	MIME Type	Schema	Details
queryExpression	query	<code>select * from mybadguys where username='adam'</code>	String	text/plain ▼	<a href="#">View</a>	Required - The AQL query to execute.
queryLanguageVersion	query		Integer	text/plain ▼	<a href="#">View</a>	Optional - The version of the AQL expression. Acceptable



# Open APIs – Events and Flows

- Utilize full power for AQL

## Ariel Query Language (AQL)

---

The Ariel Query Language, or AQL, is a structured query language for Ariel databases. It uses a familiar SQL-like syntax to express queries that retrieve data and perform other operations.

The use of an SQL-like language makes it easy to begin creating AQL queries if you are already familiar with SQL. The structure of an Ariel database, however, is internally very different from a relational database, so there are areas in which AQL deviates from familiar SQL forms in order to provide more precise control over the Ariel server's capabilities. The important differences in database structure are discussed in the [concepts](#) section below.

This document briefly introduces Ariel databases and some of the concepts that are unique to them, and then provides a detailed reference describing the elements of AQL and how to compose them.

### Contents

- [Changes from previous AQL versions](#)
- [Ariel database concepts](#)
  - [Databases](#)
  - [Interval data](#)
  - [Searches](#)
  - [Properties](#)
  - [Aggregation](#)
  - [Views](#)
- [AQL reference](#)
  - [Lexical conventions](#)
  - [DESCRIBE](#)
  - [SELECT](#)
  - [MATERIALIZERUN](#)
  - [DROP](#)

---

## Changes from previous AQL versions

The AQL language was originally designed for the Ariel command line client tool. The tool provides many powerful capabilities, but it has not previously been formally supported and so the expression language has remained incomplete or unrefined in some areas. This document describes a revised expression language that adds a number of important capabilities and changes a number of existing expression elements to make them more complete or consistent. The new language has all of the same capabilities as the older version, and most simple queries are identical. However, the new language does not yet provide complete backwards compatibility.

If you are familiar with the older AQL syntax, you may be interested just in a description of the changes introduced by the newer version. Differences are described in context with the rest of the documentation, but are highlighted in this way:

**NEW** -- This is a new feature introduced with this version.



# Open APIs – Events and Flows

- Need to run a saved search defined in the UI?

Saved Searches Group:  [Manage Groups](#)

Type Saved Search or Select from List

Available Saved Searches

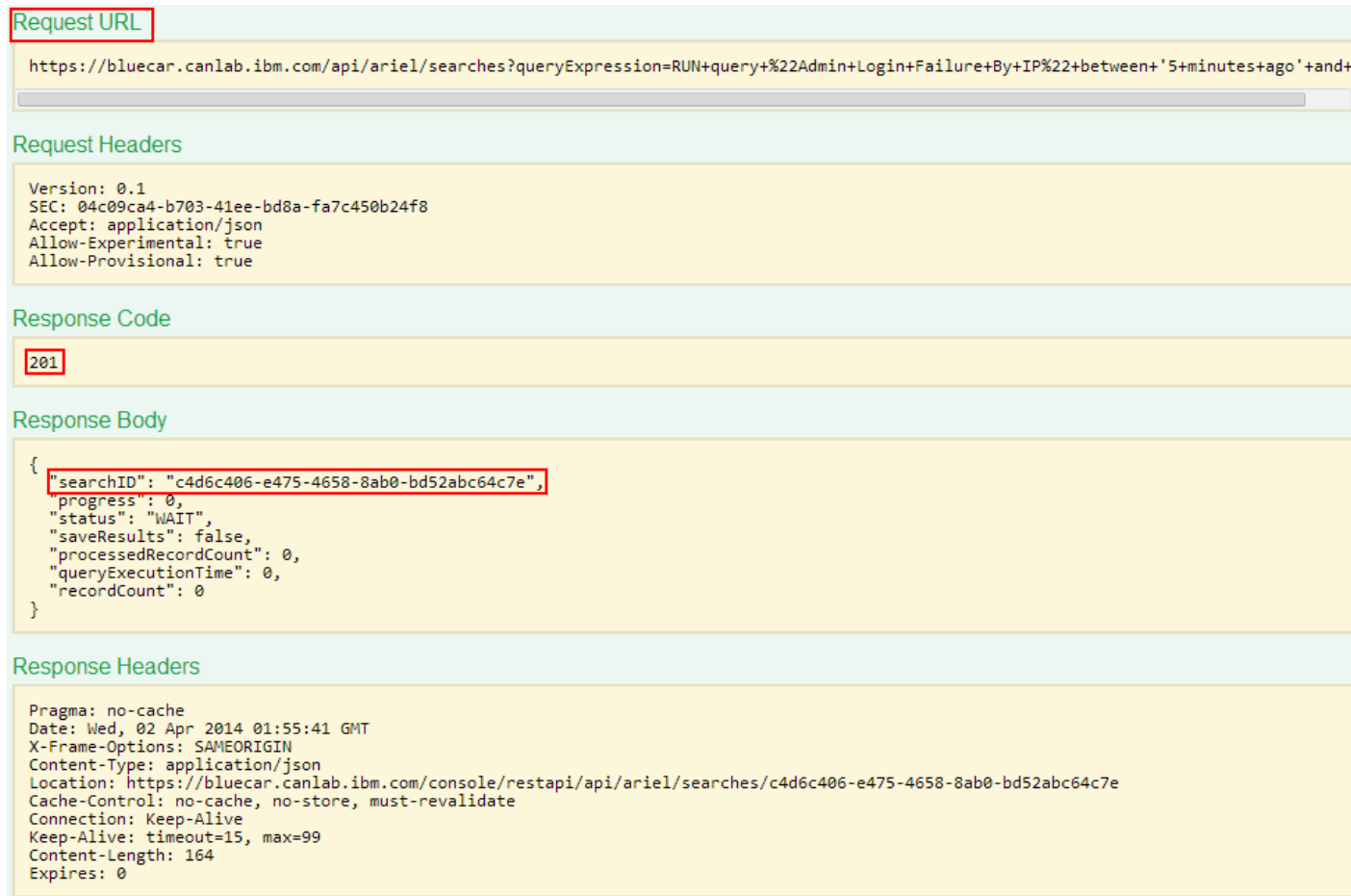
- Accessed Resources
- Admin Login Failure
- Admin Login Failure By IP**
- Admin Login Failure By User
- Admin Login Failures by Network
- Admin Login Success By IP

Execute it from the API

Parameters						
Parameter	Type	Value	Data Type	MIME Type	Sample	Details
queryExpression	query	<code>RUN query "Admin Login Failure By IP" between '5 minutes ago' and now</code>	String	text/plain	<a href="#">View</a>	Required - The AQL query to execute.

## Open APIs – Events and Flows

- Can handle very large queries



**Request URL**

```
https://bluecar.canlab.ibm.com/api/ariel/searches?queryExpression=RUN+query+%22Admin+Login+Failure+By+IP%22+between+'5+minutes+ago'+and+
```

**Request Headers**

```
Version: 0.1  
SEC: 04c09ca4-b703-41ee-bd8a-fa7c450b24f8  
Accept: application/json  
Allow-Experimental: true  
Allow-Provisional: true
```

**Response Code**

**201**

**Response Body**

```
{  
  "searchID": "c4d6c406-e475-4658-8ab0-bd52abc64c7e",  
  "progress": 0,  
  "status": "WAIT",  
  "saveResults": false,  
  "processedRecordCount": 0,  
  "queryExecutionTime": 0,  
  "recordCount": 0  
}
```

**Response Headers**

```
Pragma: no-cache  
Date: Wed, 02 Apr 2014 01:55:41 GMT  
X-Frame-Options: SAMEORIGIN  
Content-Type: application/json  
Location: https://bluecar.canlab.ibm.com/console/restapi/api/ariel/searches/c4d6c406-e475-4658-8ab0-bd52abc64c7e  
Cache-Control: no-cache, no-store, must-revalidate  
Connection: Keep-Alive  
Keep-Alive: timeout=15, max=99  
Content-Length: 164  
Expires: 0
```

# Open APIs – Events and Flows

- How to get results of the query? Use the following API endpoint

**GET** /searches/{searchID}/results Show/Hide Versions | List Versions

0.1 | EXPERIMENTAL Retrieves search results in the format requested

**Description**

Retrieve the results of the Ariel search that is identified by the searchID. The results are returned in the format indicated by the 'Accepts' request header. The format can be JSON, CSV, XML, or tabular text.

Select the format of results desired

**Response Type**

MIME Type

- application/json ← Great for web visualization packages
- application/csv ← Great for quick an easy reporting
- text/table
- application/xml ← Great for custom data processing applications

Pass the search ID as the parameter to get results

**Parameters**

Parameter	Type	Value
searchID	path	c4d6c406-e475-4658-8ab0-bd52abc64c7e

## Open APIs – Events and Flows

- Search results returned, in JSON example

```
Response Code
200

Response Body
{
  "events": [
    {
      "Source IP": "51.100.100.2",
      "Destination IP (Unique Count)": "{127.0.0.1}",
      "Destination Port (Unique Count)": "{0}",
      "Event Name (Unique Count)": "{44251970}",
      "Log Source (Unique Count)": "{71}",
      "Low Level Category (Unique Count)": "{3015}",
      "Protocol (Unique Count)": "{255}",
      "Username (Unique Count)": "{java.lang.String|root}",
      "Magnitude (Maximum)": "3.0",
      "Event Count (Sum)": "210.0",
      "Count": "19.0"
    },
    {
      "Source IP": "51.100.100.3",
      "Destination IP (Unique Count)": "{127.0.0.1}",
      "Destination Port (Unique Count)": "{0}",
      "Event Name (Unique Count)": "{44251970}",
      "Log Source (Unique Count)": "{71}",
      "Low Level Category (Unique Count)": "{3015}",
      "Protocol (Unique Count)": "{255}",
      "Username (Unique Count)": "{java.lang.String|root}",
      "Magnitude (Maximum)": "3.0",
      "Event Count (Sum)": "245.0",
      "Count": "19.0"
    },
    {
      "Source IP": "55.100.100.24",
      "Destination IP (Unique Count)": "{127.0.0.1}",
      "Destination Port (Unique Count)": "{0}"
    }
  ]
}
```



# Open APIs – Events and Flows

- Search results returned, in table/text example

## Request Headers

```
Version: 0.1
SEC: 04c09ca4-b703-41ee-bd8a-fa7c450b24f8
Accept: text/table
Allow-Experimental: true
Allow-Provisional: true
```

## Response Code

200

## Response Body

Source IP	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)
51.100.100.2	{127.0.0.1}	{0}	{44251970}	{71}
51.100.100.3	{127.0.0.1}	{0}	{44251970}	{71}
55.100.100.24	{127.0.0.1}	{0}	{44251970}	{71}
47.100.50.13	{127.0.0.1}	{0}	{44251970}	{71}
131.203.4.120	{127.0.0.1}	{0}	{44251970}	{71}
156.35.130.230	{127.0.0.1}	{0}	{44251970}	{71}
47.11.11.17	{127.0.0.1}	{0}	{44251970}	{71}
10.100.50.42	{127.0.0.1}	{0}	{44251970}	{71}
47.11.11.7	{127.0.0.1}	{0}	{44251970}	{71}
55.100.100.21	{127.0.0.1}	{0}	{44251970}	{71}
47.11.11.2	{127.0.0.1}	{0}	{44251970}	{71}
55.100.100.25	{127.0.0.1}	{0}	{44251970}	{71}
156.35.130.226	{127.0.0.1}	{0}	{44251970}	{71}
55.100.100.15	{127.0.0.1}	{0}	{44251970}	{71}
10.106.3.25	{127.0.0.1}	{0}	{44251970}	{71}
10.106.3.12	{127.0.0.1}	{0}	{44251970}	{71}
156.35.130.232	{127.0.0.1}	{0}	{44251970}	{71}
55.100.100.29	{127.0.0.1}	{0}	{44251970}	{71}
47.11.11.13	{127.0.0.1}	{0}	{44251970}	{71}

Returned results 1 to 19 of 19

# Open APIs – Events and Flows

Build your own visualization on top!  
A Step towards driving community developed content.

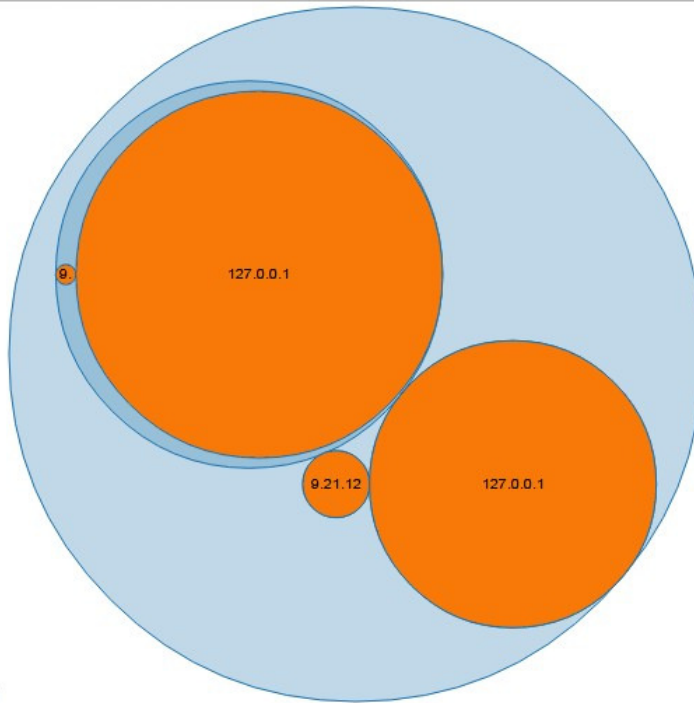




## Example visualization

AQL: `select sourceIP, destinationIP, count(*) from events group by sourceIP, destinationIP limit 100`

Token: `e1de4b87-947d-48f1-b794-7bf3e9b6e516`



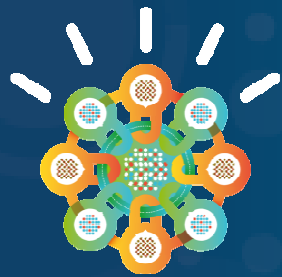
- § Simple example of a visualization
- § < 100 lines of java script
- § Huge range of visualization options



## API Summary

- § Opens up endless possibilities extracting the value out of QRadar
  - § Visualization and reporting options
  - § 3rd party and business partner value add applications
  - § And much more...
- 
- § Only the start !





**Limitless data and searching**

**The QRadar Data Node**

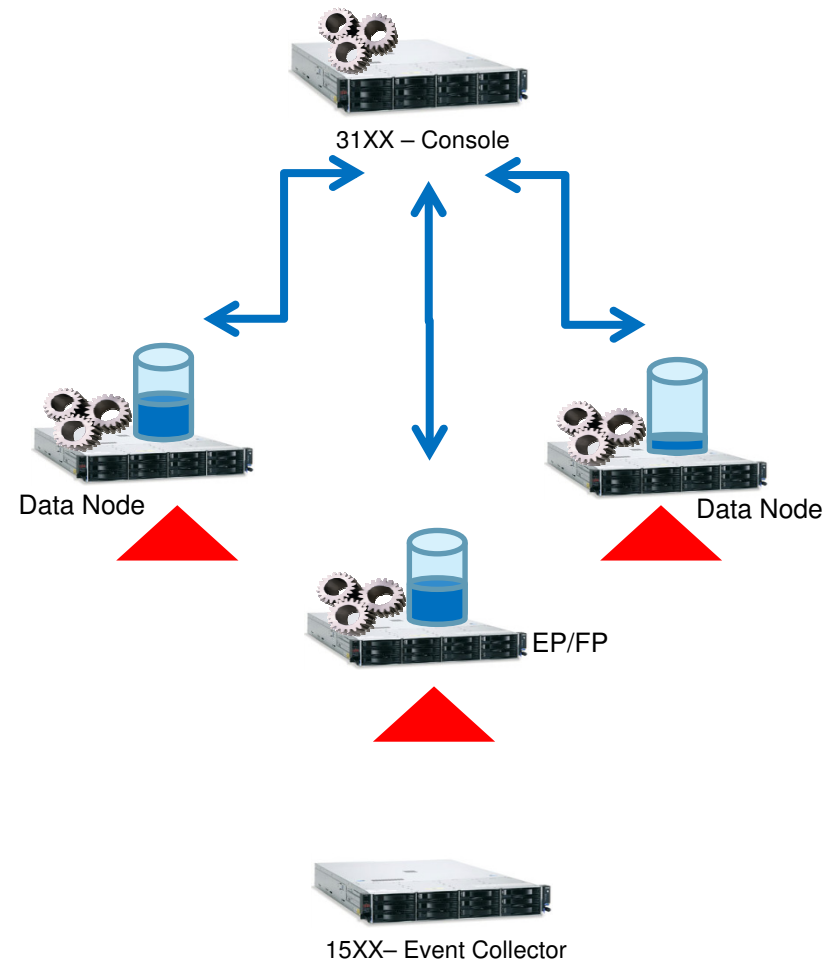
# The Problem

- Customer need to collect, store and analyse more and more data
  - Long term trend analysis
  - Incident diagnosis
- They want to be able to analyse this data quickly !
- Activities such as correlation, searching and storage must compete for available system resource, limiting possible performance improvements
- Limited scaling capabilities, requiring additional EP/FP instances in order to scale storage and search performance
- Off board storage solutions such as SANs can help but only address one aspect of the actual problem, scaling storage without concern for query performance



## The Solution – The Data Node

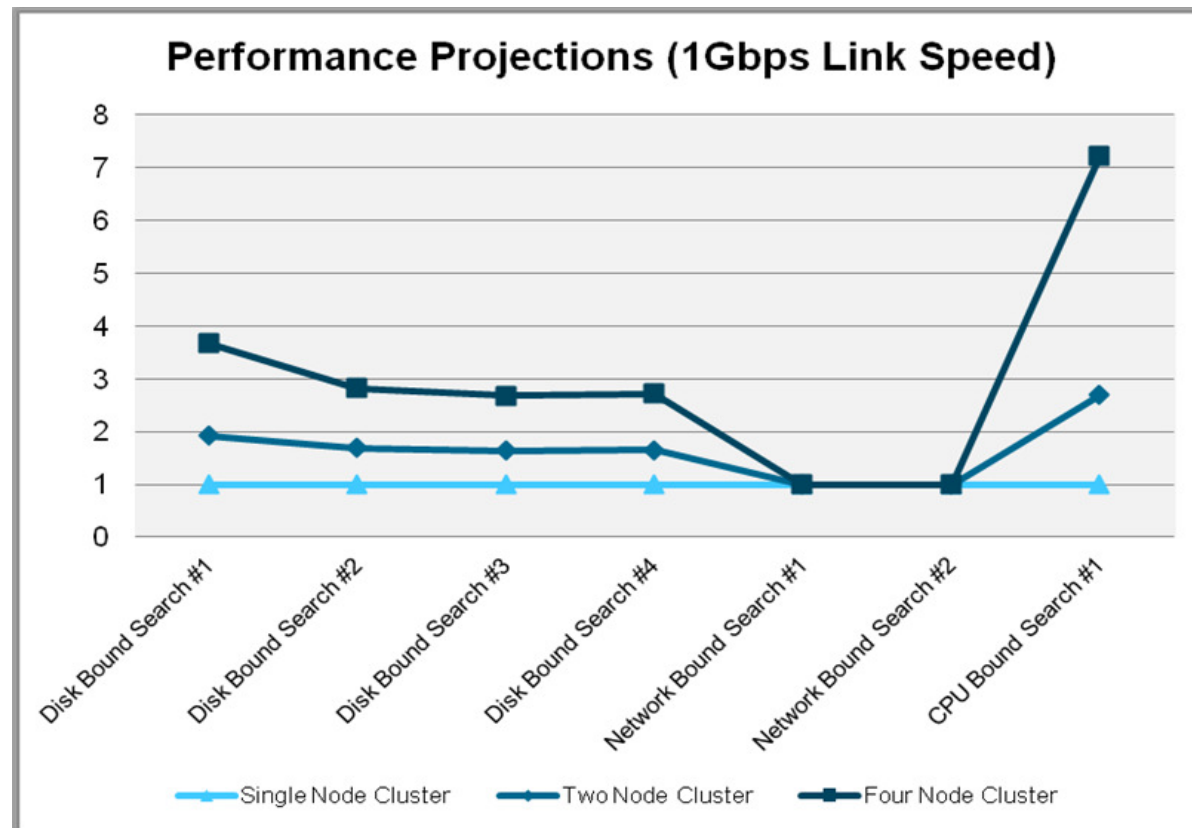
- Data node address the entire problem, scaling data storage out while simultaneously adding the processing capabilities to handle queries on data.
- Each Data Node instance that is added to a deployment bring the full processing power of an appliance that can be utilized during data storage and retrieval operations.
- The Data Nodes do not participate in activities such as correlation so they can focus their efforts on the retrieval of data and the work associated with queries such as aggregation.
- Scale any new or existing deployment to meet even the most demanding client needs; years of data, hundreds of users, all searchable in seconds



# Performance Projections

The addition of Data Node can have a dramatic impact on search performance in a number of situations.

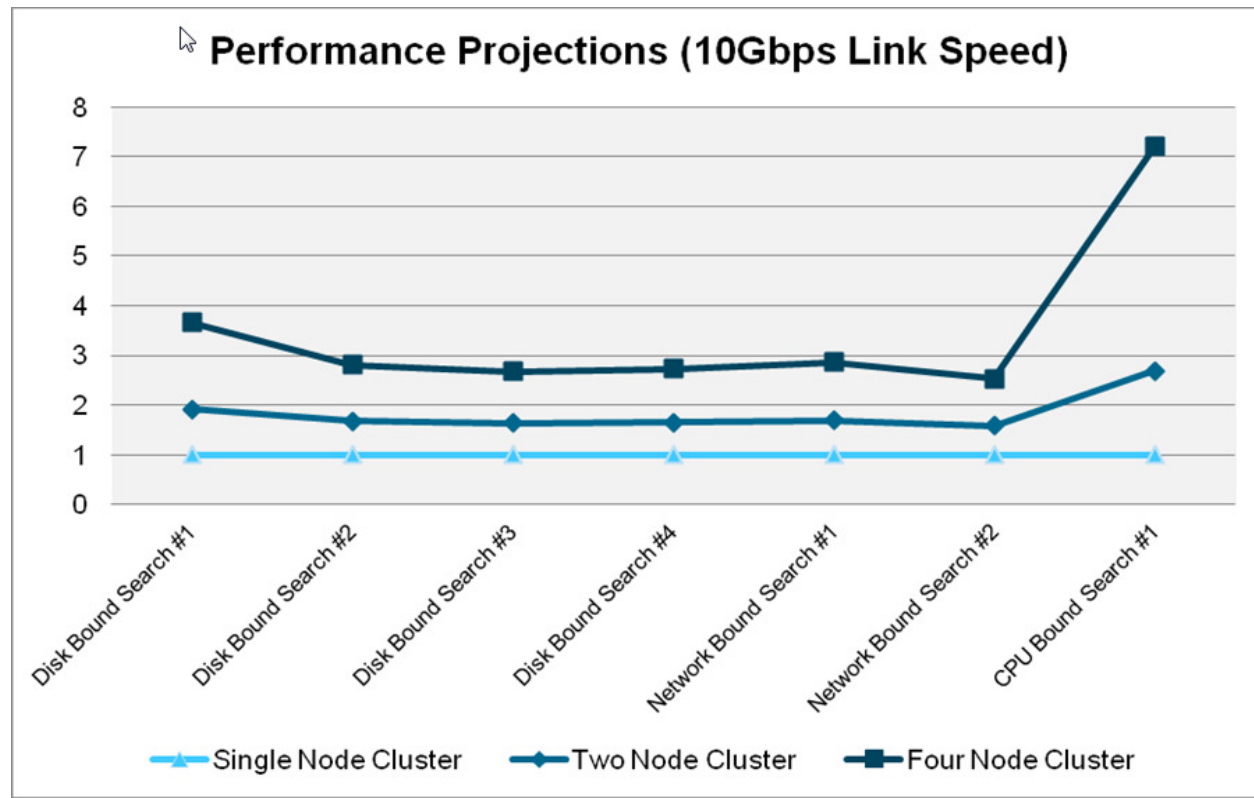
- **Disk bound searches**
  - All data with a source IP of 192.168.0.1 over the last 7 days
- **Network bound searches**
  - All data from the last 7 days
- **CPU bound searches**
  - All data from the last 4 hours, aggregated by SourceIP



# Performance Projections

The addition of Data Node can have a dramatic impact on search performance in a number of situations.

- **Disk bound searches**
  - All data with a source IP of 192.168.0.1 over the last 7 days
- **Network bound searches**
  - All data from the last 7 days
- **CPU bound searches**
  - All data from the last 4 hours, aggregated by SourceIP



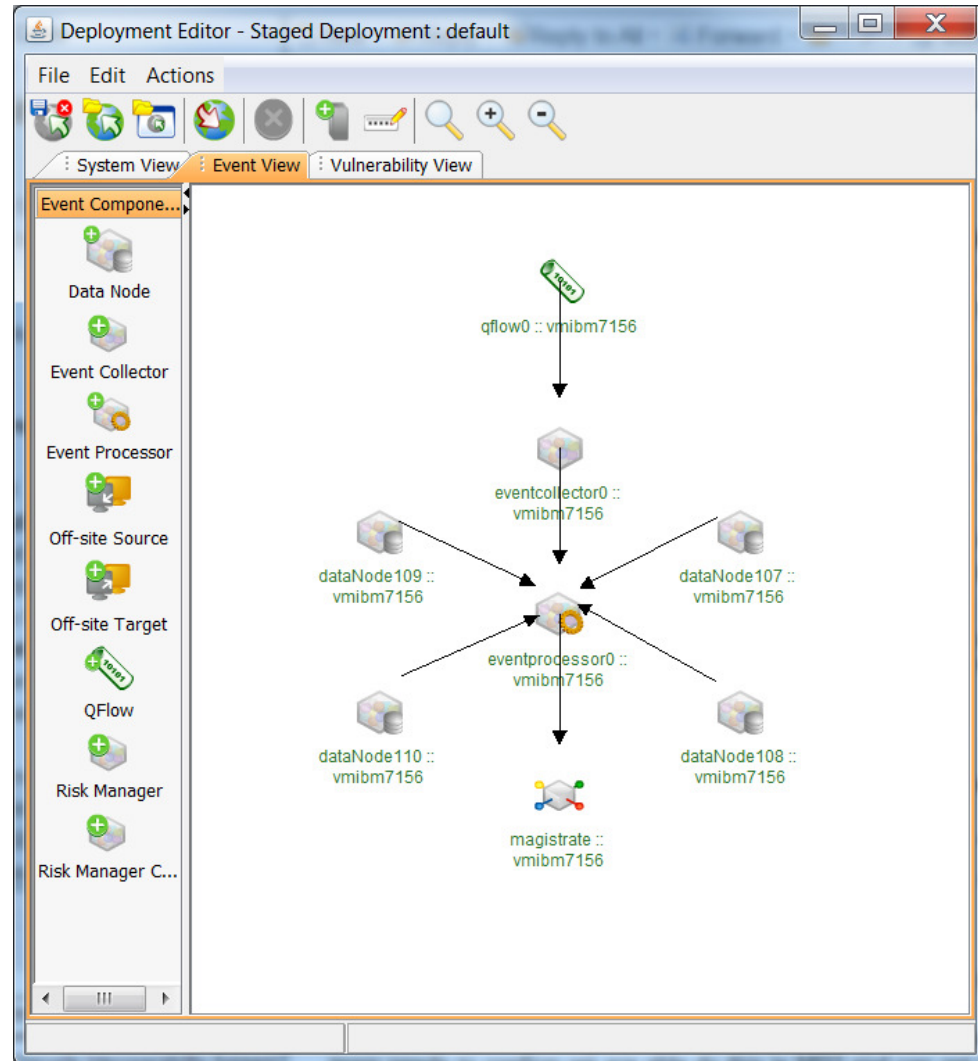


## Data Node – A Brief Introduction

- Offered in all three standard QRadar form factors; Software, Virtual or Software Pack bundled with either xx05 or xx28 Core Appliance
- Can mix and match software, virtual and hardware in a deployment
- Requires **NO** additional EPS or FPM licensing
- Can be used as companion to the following QRadar components:
  - 16XX – Event Processor
  - 17XX – Flow Processor
  - 18XX – Event/Flow Processor
  - 31XX – Console/All-In-One
  - 2100 – All-In-One

# Data Node – Configuration and Deployment

- Activate Data Node using standard QRadar activation key process
- Simple point-and-click configuration in Deployment Editor to attach Data Node instances to the appropriate host
- “Deploy” operation sends all new Data Node instances into service





# SIEM Data Node 1400 Appliance

## § Positioning

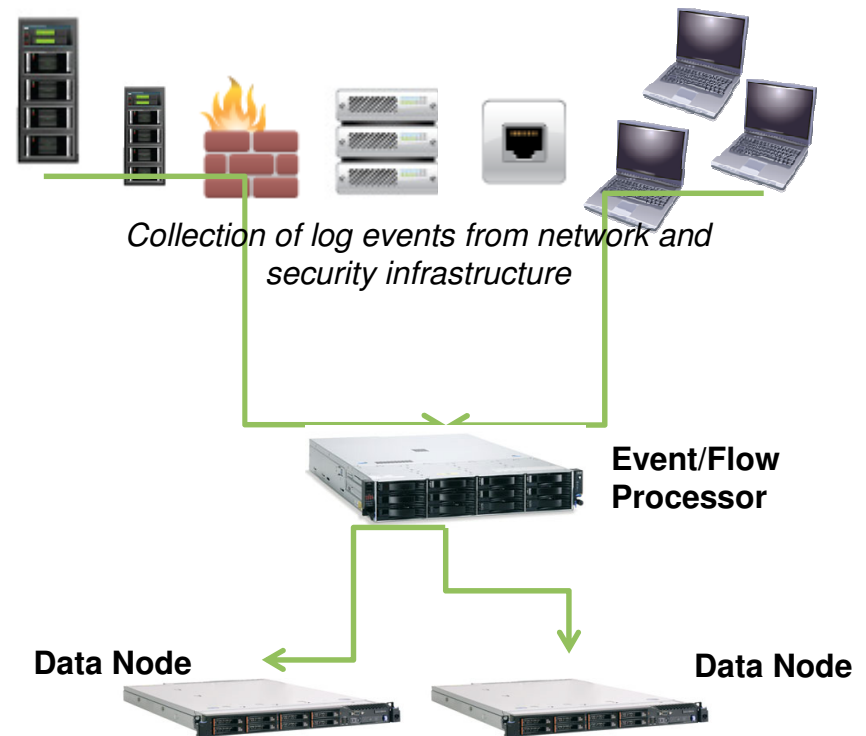
- Plug and play storage that can be used to meet the most demanding data retention requirements.

## § Characteristics and Capacity

- Receives events and flows from associated QRadar components for storage
- Actively participates in query operations, providing additional processing power and thus increased query performance
- Requires no additional EPS/FPM licensing
- Requires associated QRadar component such as 31XX, 2100, 16XX, 17XX or 8XX
- Storage
  - 40TB with xx28
  - 6 TB with xx05
  - Up to 100TB user supplied

## § Upgradability

- Additional Data Nodes can be added as needed

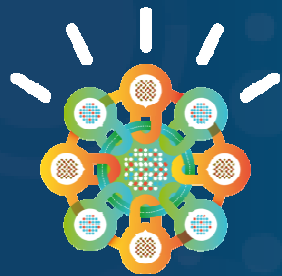






## Summary

- § A fantastically powerful and unique offering
- § Enables almost limitless data storage
- § Simple addition of incremental storage
  - Avoids complexity, cost, and potential performance issues of SAN
  - Does not require any complex disk or file reconfiguration
  - No changes required log source collection configuration
- § Ability to add process power cost effectively to improve performance
- § Addresses the performance and data storage requirements and concerns of many customers



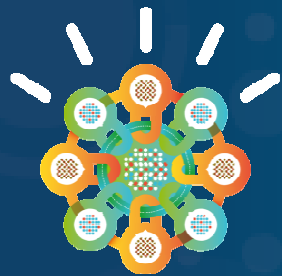
**Making QRadar even faster**

**Search Performance Improvements**



## Search Performance Enhancements

- § Search performance tuning (Ariel, Linux kernel), significantly increasing search performance and concurrency
  - Up to 3 times faster searches using indexed criteria (including Quick Filter)
    - Web proxy searching e.g. 'www.cnn.\*'
    - Specific IP activity e.g. 'sourceip = 10.33.41.5'
  - Up to 40% faster non index searches compared to 7.2.1
- § Improvement in **addition** to those introduced in **7.2.1 and the Data Node**



**Bigger and Faster !**

**New M4 Appliances**



## Why do we migrate QRadar Appliance hardware to xSeries M4?

### § **M3 approaching end of sales**

- QRadar currently uses two xSeries M3 platforms: x3550 (for 2100 and QFlow) and x3630 (for xx05 and xx24). Both platforms have their extended End of Sales planned for June 30, 2014.
- All SWG xSeries based appliances have been moving to M4.

### § **Meeting customer demands and addressing competition**

The current appliances are approaching their hardware capacity limits to handle the increasing workload, especially for large enterprise deployment.

We are under pressure from competition to increase capacity that can be delivered from one single appliance (e.g., more than 5000 EPS from AIO), instead of just scaling out (buying more event/flow processors).

### § **Supporting future software capabilities**

- Future software features planned in QRadar's roadmap such as Big Data, extended delivery mechanisms (multi-tenancy, SaaS, MSSP), forensics, and incorporating more SI data by integration with other IBM solutions all demand more hardware resources.

### § **Improving the configuration**

- The M3 platforms currently used have limited network interfaces, making QRadar lack the ability to support 10G fiber network and fiber channel storage out of the box.
- Event Collector 1501 needs to be rebased on a cheaper platform to be more cost effective.



## Overview of Appliance model and hardware changes

### § **Model number changes**

- Current QRadar model numbers remain the same, except that xx24 is replaced with xx28 due to significant hardware upgrade.
- To distinguish from M3 based appliances, all M4 based appliances are named with “G2”.

### § **Two xSeries M4 hardware platforms**

- [x3550 M4](#) is used for 2100, QFlow Collector 1201/1202/1301/1310, and Event Collector 1501.
- [x3650 M4 BD](#) is used for xx05 and xx28.

### § **Enhanced hardware resources**

Faster processors and more cache

More memory (32GB for 2100, 64GB for xx05, 128GB for xx28, 16GB for QFlow)

More disk storage for QRadar data (40TB for xx28)

Improved network interfaces

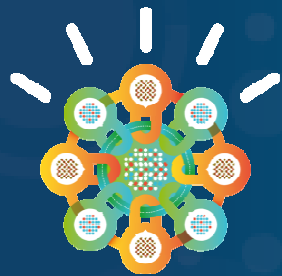
3 or 4 1Gbps network interfaces

1 [two port 10Gbps network adaptor](#) (for 10Gbps fiber networks) included in all models

1 two port Emulex FC HBA card (for Remote SAN support) included in xx28

1 [4 x 1Gbps Napatech capture adaptor](#) included in QFlow Collector 1202 and 1301.

1 [2 x10Gbps Napatech capture card](#) (Gen 2) included in QFlow Collector 1310.



**Taking QRadar GLOBAL !**

**Translation**



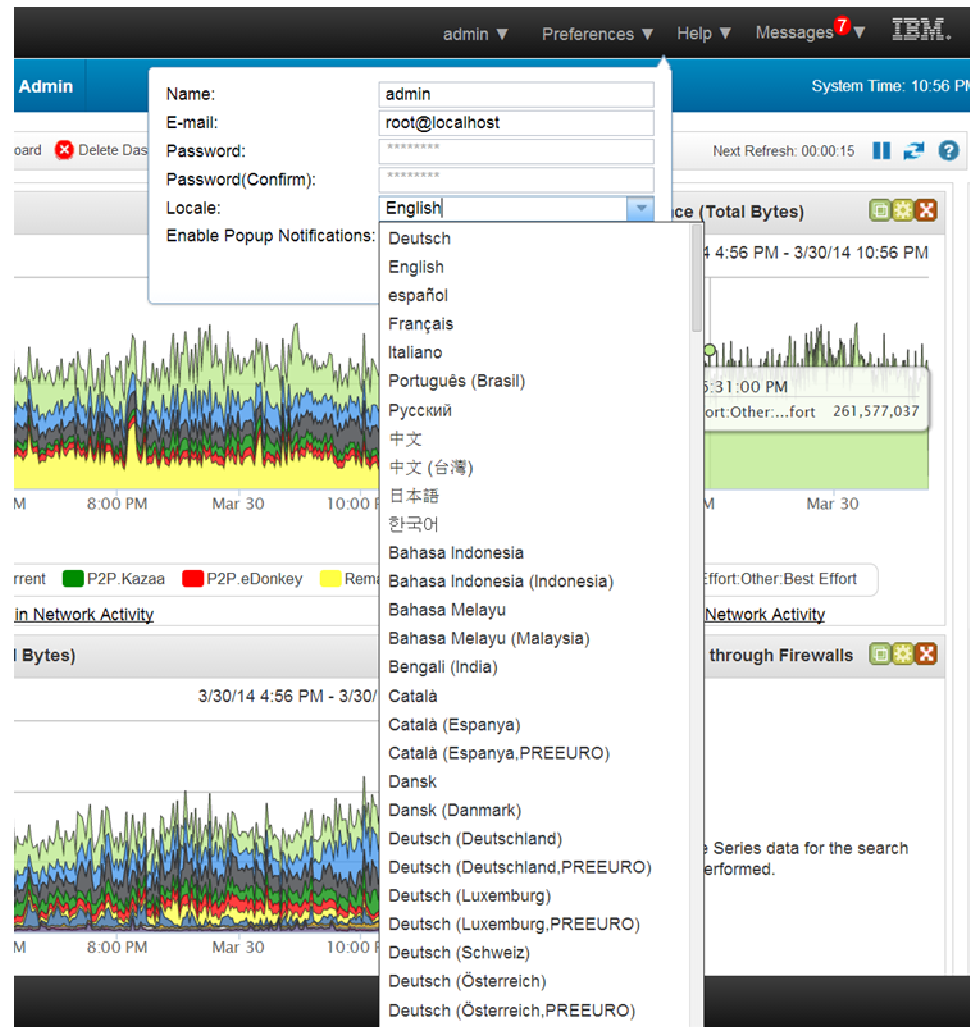
## Globalization - Overview

- QRadar will be available in the following languages
  - French, German, Italian, Spanish, Brazilian (Portuguese), Russian, Traditional Chinese, Simplified Chinese, Korean and Japanese
  
- This translation effort has been a significant investment involving translators and QA resources in 10 different countries and has resulted in over 160,000 words being translated covering most aspects of the QRadar SIEM Platform including:
  - Dashboards
  - Log and Flow Activity Panels
  - Search Screens Throughout
  - Reporting
  - Administration
  - Documentation



# Globalization – Language/Locale Selection

- Users simply pick their language and refresh !





# Globalization - Dashboards

The image displays two screenshots of the IBM Security QRadar SIEM interface. The top screenshot shows a dashboard with a navigation bar and several widgets:

- Входящий трафик по странам/регионам (Всего байт):** A pie chart showing traffic distribution by country/region: USA (46%), Canada (36%), China (9%), and Belgium (4%).
- Первые приложения (Всего байт):** A line chart showing the top applications by volume.
- DSCP - Приоритет (Всего байт):** A line chart showing DSCP priority levels.
- Исходящий трафик по странам/регионам (Всего байт):** A line chart showing outgoing traffic volume.

The bottom screenshot shows a more detailed dashboard with multiple widgets:

- ICMP 類型/代碼 (封包總數):** A line chart showing ICMP packet counts over time.
- 依 DST 埠列出的防火牆拒絕 (事件計數):** A stacked area chart showing firewall rejection events by destination port.
- 前幾個應用程式 (位元組總計):** A line chart showing top applications by total bytes.
- 依交通流量列出的前幾個網路 (位元組總計):** A line chart showing top networks by traffic volume.
- 依 DST IP 列出的防火牆拒絕 (事件計數):** A line chart showing firewall rejection events by destination IP.
- DSCP - 優先順序 (位元組總計):** A line chart showing DSCP priority levels by total bytes.

Both screenshots include a navigation bar with options like 'Нарушения', 'Ведение журналов', and 'Интенсивность работы сети'. The interface is in Russian and includes various interactive elements like zoom controls and refresh buttons.





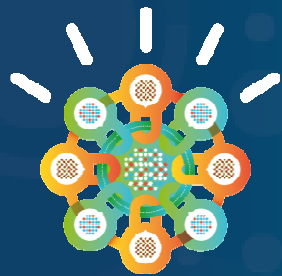
## Globalization – Exceptions

- Although the majority of QRadar has been translated there are a few exceptions that should be mentioned. A few of the more visible exceptions are as follows:
  - Custom Rules Engine
  - QID Map
  - QRadar Vulnerability Manager
  - QRadar Risk Manager
  - QRadar Incident Forensics
  - Asset Details (e.g. Vulnerability Names, Product Names etc.)
  - REST API Interfaces
  - Numerous Administration Screens



## Globalization – Exceptions

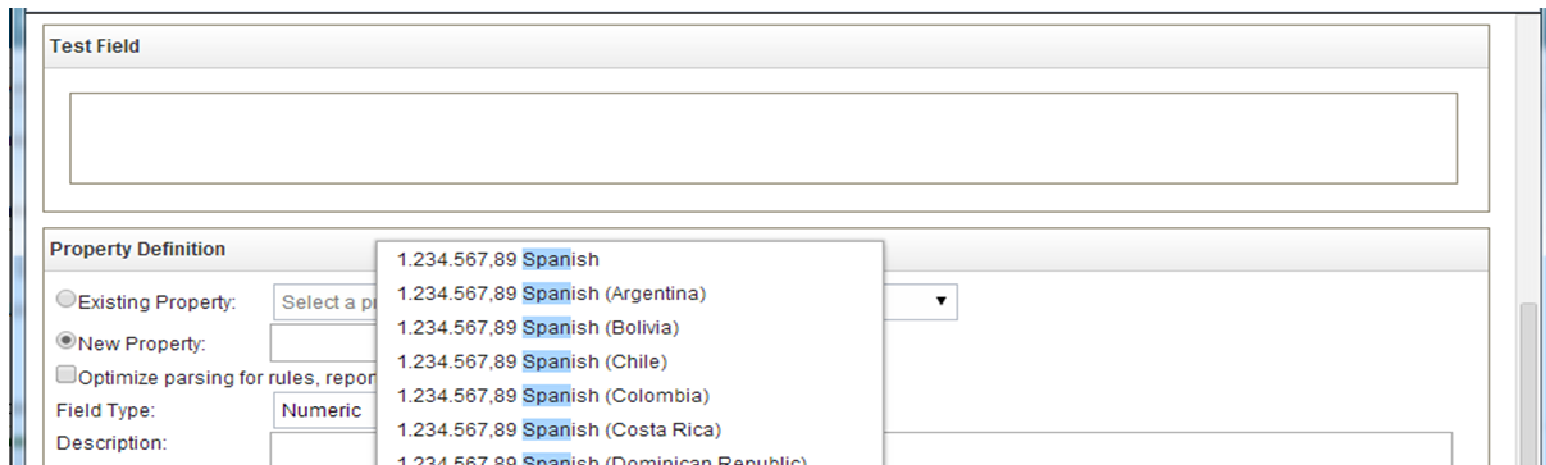
- Although the majority of QRadar has been translated there are a few exceptions that should be mentioned. A few of the more visible exceptions are as follows:
  - Custom Rules Engine
  - QID Map
  - QRadar Vulnerability Manager
  - QRadar Risk Manager
  - QRadar Incident Forensics
  - Asset Details (e.g. Vulnerability Names, Product Names etc.)
  - REST API Interfaces
  - Numerous Administration Screens

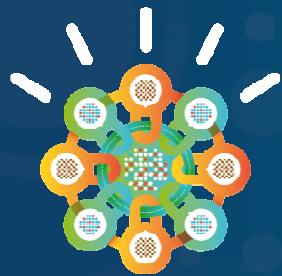


# Universal Number Parsing Support

# Universal Number Parsing Support

- Customers with globally distributed deployments, or deployments in countries with different number formatting standards has to process payloads with numbers formatted for that specific locale.
  - Example: 1234567.89 is valid in the following formats:
    - US: 1,234,567.89
    - Spain: 1.234.567,89
    - Switzerland: 1'234'567.89





## **Completing our appliance portfolio**

**1828 – Combined Event and Flow Processor Appliance**





# SIEM Combined Event/Flow Processor 1828 Appliance

## § Positioning

- High capacity and scalable log and flow collection for distributed deployment in a large enterprise

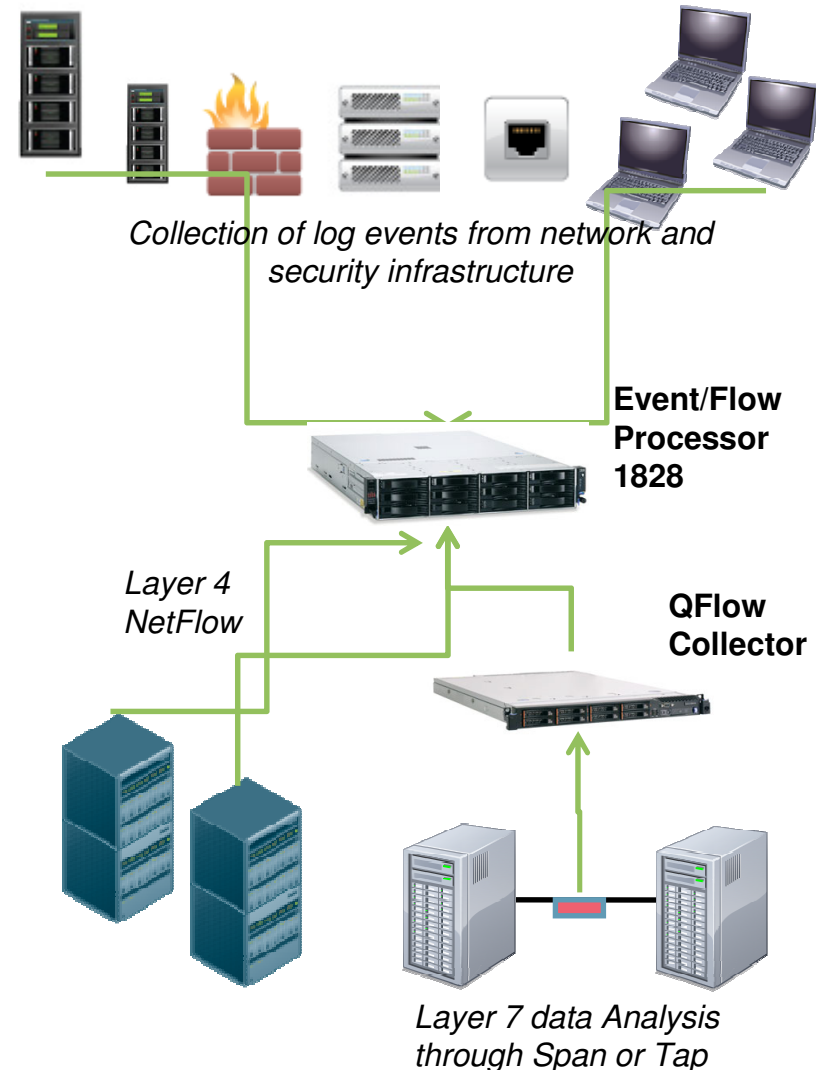
## § Characteristics and Capacity

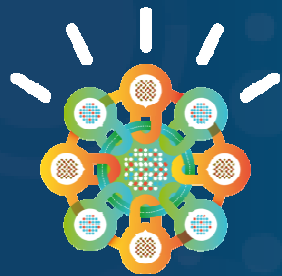
- Collect logs from network devices, security devices, operating systems and applications
- Receives flows from external flow sources (e.g. NetFlow) or QFlow Collectors for layer 7 network activity monitoring
- 1000 EPS, 25K Flows/minute
- Requires Console 31XX
- 40 TB of storage

## § Upgradability

- EPS upgradable to 15K
- Flows upgradable to 300K

## § HA / DR available



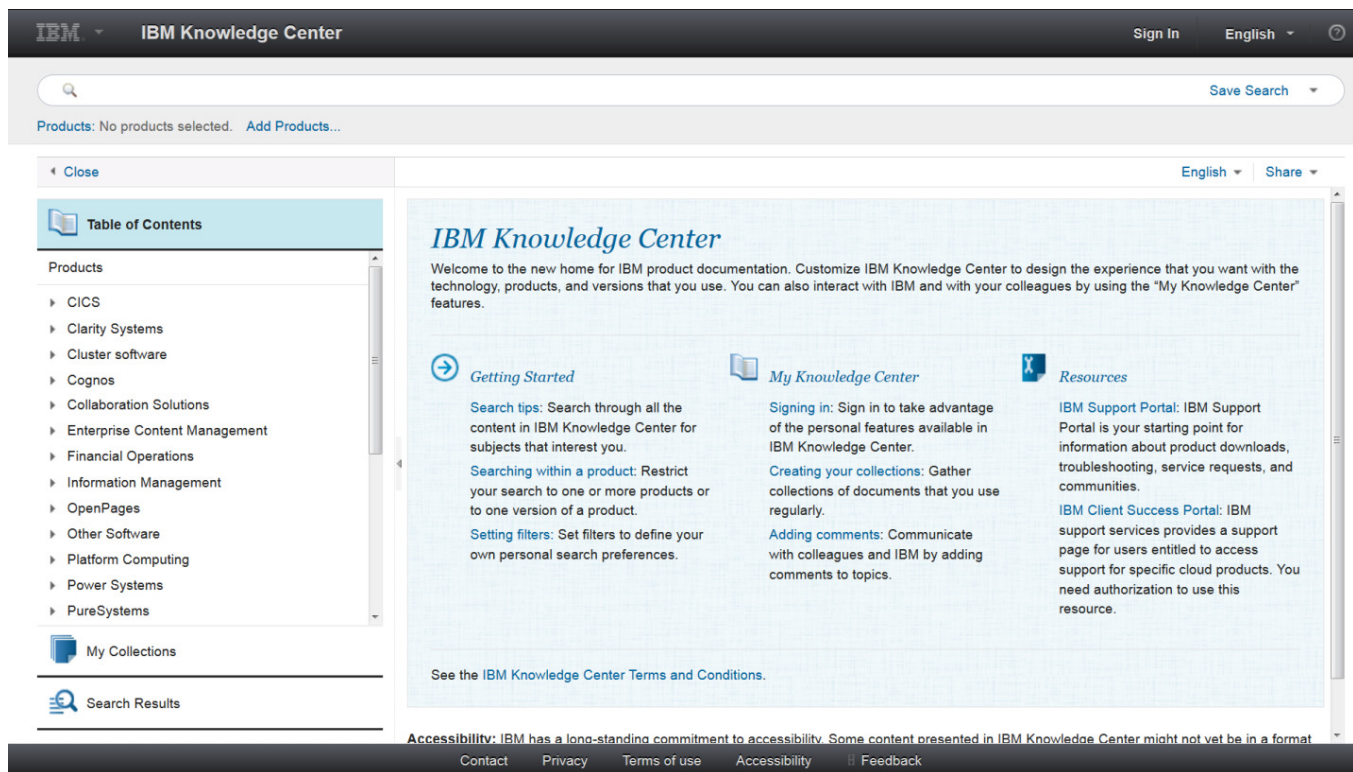


**The next generation of product  
documentation**

**IBM Knowledge Center**

## IBM Knowledge Center – Overview

- ❑ Huge amount of information and documentation available on QRadar
- ❑ New knowledge centre gives the streamlined and powerful access
- ❑ An IBM-wide view of technical information for multiple offerings in a single location on the web (<http://www-01.ibm.com/support/knowledgecenter/>).



The screenshot displays the IBM Knowledge Center homepage. At the top, there is a navigation bar with the IBM logo, the text "IBM Knowledge Center", and options for "Sign In" and "English". Below this is a search bar with a magnifying glass icon and a "Save Search" button. A secondary bar indicates "Products: No products selected. Add Products...".

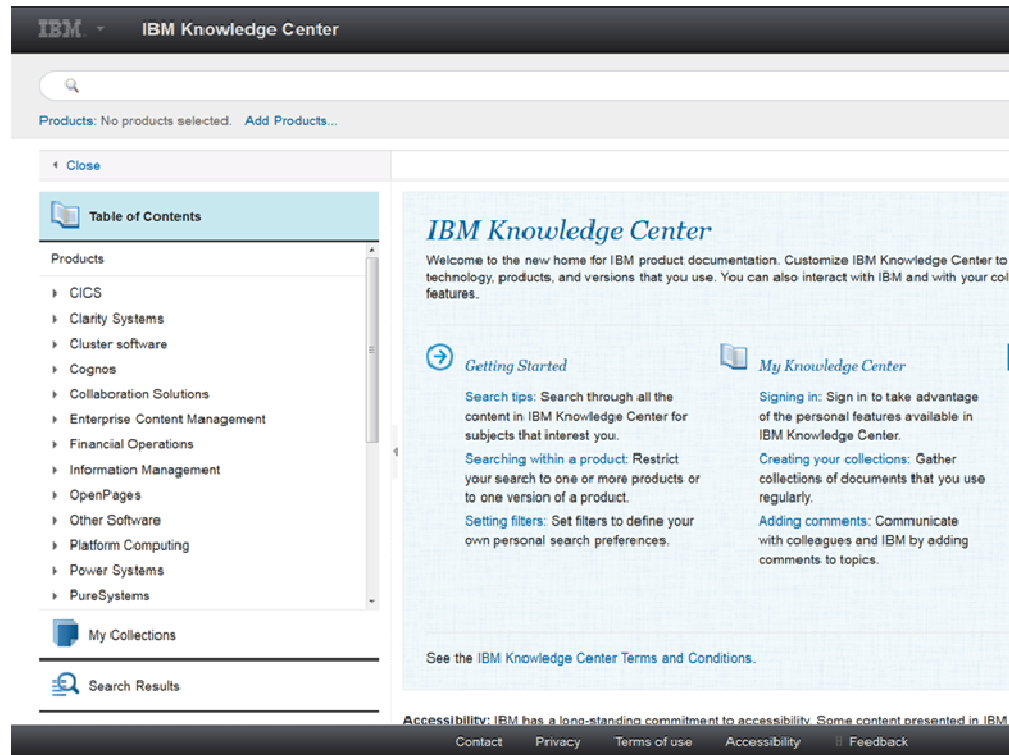
The main content area is divided into a left sidebar and a main panel. The sidebar includes a "Close" button, a "Table of Contents" section, a "Products" list with various categories like CICS, Clarity Systems, and Cluster software, and sections for "My Collections" and "Search Results".

The main panel features the heading "IBM Knowledge Center" and a welcome message: "Welcome to the new home for IBM product documentation. Customize IBM Knowledge Center to design the experience that you want with the technology, products, and versions that you use. You can also interact with IBM and with your colleagues by using the 'My Knowledge Center' features." Below this are three columns of featured content: "Getting Started" (with sub-points on search tips, searching within a product, and setting filters), "My Knowledge Center" (with sub-points on signing in, creating collections, and adding comments), and "Resources" (with sub-points on the IBM Support Portal and the IBM Client Success Portal). A link to "See the IBM Knowledge Center Terms and Conditions." is also present.

At the bottom of the page, there is an accessibility notice: "Accessibility: IBM has a long-standing commitment to accessibility. Some content presented in IBM Knowledge Center might not yet be in a format..." followed by a footer with links for "Contact", "Privacy", "Terms of use", "Accessibility", and "Feedback".

## IBM Knowledge Center – Easy to find topics

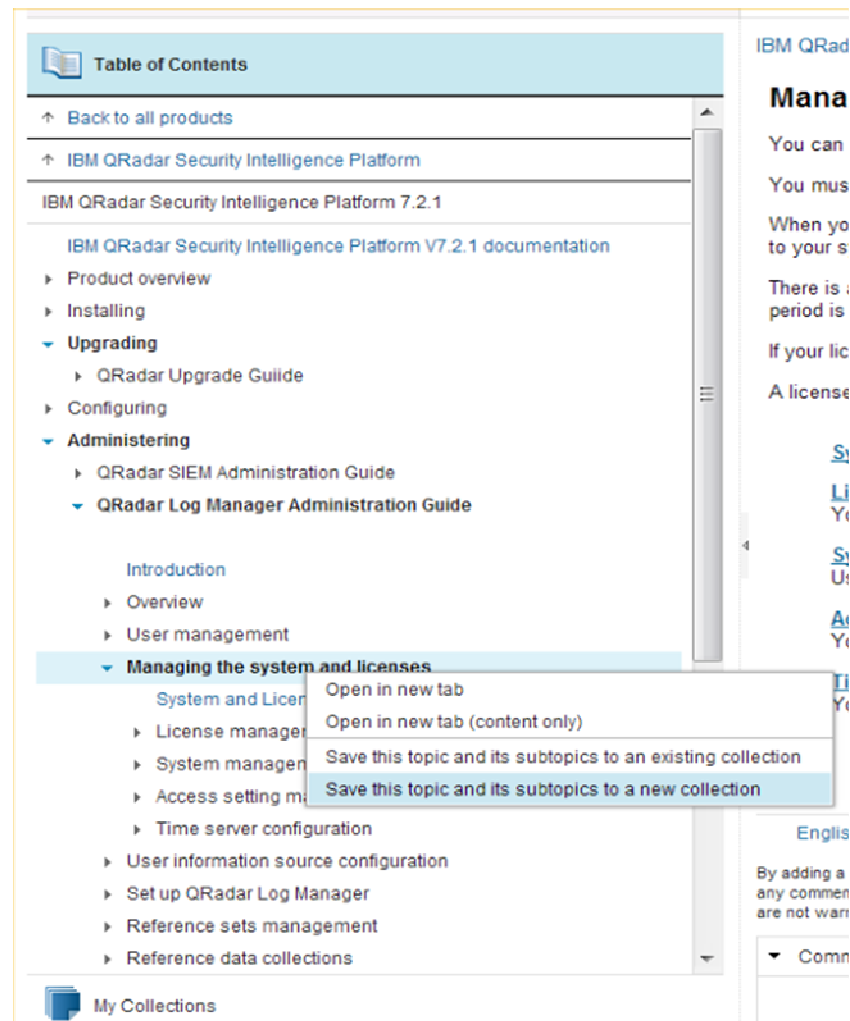
- Search across all technical information to get information quickly from a single, simple search.
- Search the content from a subset of products, or even a single product
- Remembers where you are and if you open a topic, the table of contents automatically changes to show you the context.



The screenshot displays the IBM Knowledge Center interface. At the top, there is a search bar and a navigation menu. Below the search bar, a section titled "Products" shows a list of product categories with expandable arrows. The main content area features a "Getting Started" section with sub-sections like "Search tips", "Searching within a product", and "Setting filters". There is also a "My Knowledge Center" section with sub-sections like "Signing in", "Creating your collections", and "Adding comments". The footer contains links for "Contact", "Privacy", "Terms of use", "Accessibility", and "Feedback".

## IBM Knowledge Center – Customize the documentation

- ❑ Customers want direct involvement in customizing the documentation so that they see only the information that they need.
- ❑ Can create collections of selected information.
- ❑ Publish collections in PDF format and share with others.
- ❑ Future updates to product information in your collection are automatically reflected in your existing collections.
- ❑ Less information to read/scan



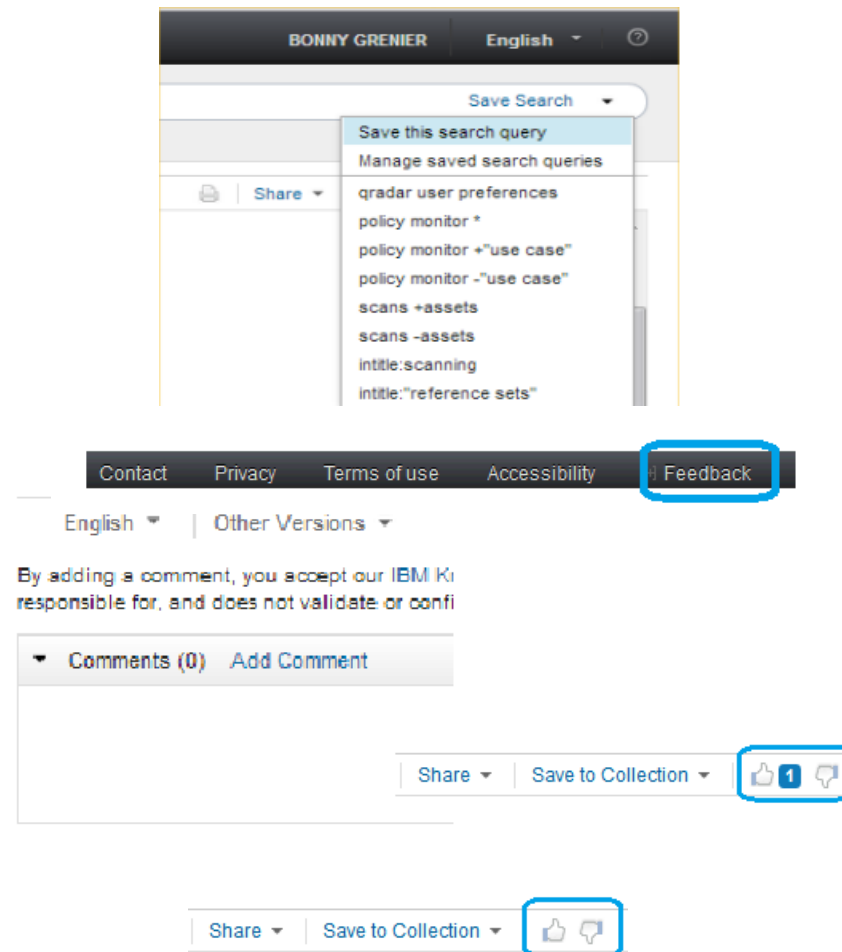
The screenshot displays the IBM Knowledge Center interface. On the left, a 'Table of Contents' pane shows a hierarchical list of topics for 'IBM QRadar Security Intelligence Platform 7.2.1'. The 'Managing the system and licenses' section is expanded, and a context menu is visible over it. The menu options are:

- Open in new tab
- Open in new tab (content only)
- Save this topic and its subtopics to an existing collection
- Save this topic and its subtopics to a new collection

On the right side of the interface, there is a sidebar with the text 'IBM QRadar' and 'Mana'. Below this, there is a section titled 'You can' and 'You mus', followed by 'When yo to your s'. There is also a section for 'There is : period is' and 'If your lic A license'. At the bottom right, there is a language selector set to 'Englis' and a comment section with the text 'By adding a any commen are not warr' and a 'Comn' button.

## IBM Knowledge Center – Share information with others

- Save search results to share with others or to save for future use.
- Provide topic-level feedback by providing public comments or submitting private feedback.
- Rate a topic by clicking the thumbs-up or thumbs-down icons on the top right of the IBM Knowledge Center window.





## Summary

- A really big important release
- Demonstrates IBM's commitment to our strategy, product and our customers
- The Data Node
  - How big and fast do you want to go ?
- APIs
  - What do you want to do with our data and analytics ?
- Globalisation
  - Your own language
- New M4s
  - HUGE disk, more CPU, more speed, more network options
- Knowledge centre
  - Easier to find information
- Not only a fantastic feature set but....
  
- .... provides the basis for even more ground breaking capabilities later this year..



[ibm.com/security](http://ibm.com/security)

© **Copyright IBM Corporation 2014. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.