IBM Security QRadar
Version 7.2.8

Ariel Query Language Guide

Note
Before you use this information and the product that it supports, read the information in "Notices" on page 53.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.8 and subsequent releases unless superseded by an updated version of this document.

Contents

About this guide v

Chapter 1. What's new for users in AQL 1

Chapter 2. Ariel Query Language 3

Ariel Query Language deprecated versions 3
AQL fields changed in AQL V3 3
Overview of Ariel Query Language. 5
Best practices for using quotation marks in AQL queries. 7
SELECT statement 9
WHERE clause 10
GROUP BY clause 11
HAVING clause 12
ORDER BY clause 13
LIKE clause 14
COUNT function 15
AQL logical and comparison operators 15
AQL data calculation and formatting functions 18
AQL data aggregation functions 22
AQL data retrieval functions. 25
Time criteria in AQL queries. 34
AQL date and time formats 36
AQL subquery 38
Conditional logic in AQL queries 39
CIDR IP addresses in AQL queries 40
Custom properties in AQL queries. 41
System performance query examples 41
Events and flows query examples 42
Reference data query examples 44
User and network monitoring query examples. 46
Event, flow, and simarc fields for AQL queries 48

Notices 53

Trademarks 54
Terms and conditions for product documentation. 55
IBM Online Privacy Statement 56

Index 57

About this guide

The Ariel Query Language (AQL) Guide provides you with information for using the AQL advanced searching and API.

Intended audience

System administrators who view event or flow data that is stored in the Ariel database.

Technical documentation

To find IBM® Security QRadar® product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

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.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. What's new for users in AQL

IBM Security QRadar introduces new Ariel Query Language (AQL) functions and enhancements.

New AQL subquery

Use a subquery as a data source or reference for the main query. Use the FROM or IN clause to refine your AQL query by referring to the data that is retrieved by the subquery.

 Learn more about using AQL subqueries to refine your search.

AQL guide enhancements

The AQL guide features new content with relevant examples.

Chapter 2. Ariel Query Language

The Ariel Query Language (AQL) is a structured query language that you use to communicate with the Ariel databases. Use AQL to query and manipulate event and flow data from the Ariel database.

Ariel Query Language deprecated versions

Ariel Query Language (AQL) V1 and V2 are deprecated.

The command-line script, **/opt/qradar/bin/arielClient** is deprecated. The following warning message is displayed both before and after the results are returned:

```
WARNING: AQL V1 and V2 will be deprecated in the future.
 For information about using AQL V3, see the product documentation.
```

During your migration to AQL V3, you can suppress the warning message by typing: `/opt/qradar/bin/arielClient | grep -v WARNING`

The Python client and the Advanced search option use AQL V3.

AQL fields changed in AQL V3

Ariel Query Language (AQL) V2 is deprecated in QRadar V7.2.4 and later. Some Ariel database fields were changed or removed in AQL V3. If you have queries that use these fields, you must replace them.

Table 1 shows the new Ariel database fields.

Table 1. Fields that were replaced in AQL V3

Field name (AQL V2)	Replacement function name (AQL V3)
destinationAssetName	AssetHostname
deviceGroup	LogSourceGroupName
sourceAssetName	AssetHostname
eventDescription	QidName
destinationNetwork	NetworkName
endDate	DateFormat
endDateFormatted	DateFormat
eventProcessor	Processorname
identityUsername	AssetUser
identityMAC	AssetProperty
identityHostName	AssetHostname
identityNetBiosName	AssetHostname
identityGroupName	AssetProperty
identityExtendedField	AssetProperty
deviceDate	DateFormat
payloadHex	UTF8
protocol	ProtocolName
sourceNetwork	NetworkName
startDate	DateFormat
startDateFormatted	DateFormat
destinationAssetName	AssetHostname

Table 1. Fields that were replaced in AQL V3 (continued)

Field name (AQL V2)	Replacement function name (AQL V3)
sourceAssetName	AssetHostname
destinationNetwork	NetworkName
sourceNetwork	NetworkName
application	ApplicationName
destinationPayloadHex	UTF8
firstPacketDate	DateFormat
eventProcessorId	ProcessorName

This following Ariel database fields were removed.

- partialorMatchList
- qidNumber
- token
- destinationHost
- destinationIPSearch
- destinationPortNA
- sourceHost
- sourceIPSearch
- sourcePortNA
- destinationDscpOnly
- anyDestinationFlag
- smallDestinationPayload
- smallDestinationPayloadHex
- destinationPrecedanceOnly
- lastPacketDate
- localHost
- remoteHost
- sourceDscpOnly
- anySourceFlag
- sourcePayloadHex
- smallSourcePayload
- smallSourcePayloadHex
- sourcePrecedanceOnly
- sourceHostString
- destinationHostString
- destinationNetwork
- application
- sourceNetwork
- smallPayload
- smallPayloadHex
- quickSearchMatches
- bitsPerSecond
- srcBitsPerSecond
- dstBitsPerSecond
- bytesPerSecond

- bytesPerPacket
- srcBytesPerPacket
- dstBytesPerPacket
- destinationByteRatio
- destinationPacketRatio
- packetsPerSecond
- sourceByteRatio
- sourcePacketRatio
- totalBytes
- totalPackets
- retentionBucket
- properLastPacketTime
- properLastPacketDate

Overview of Ariel Query Language

Use AQL to extract, filter, and perform actions on event and flow data that you extract from the Ariel database in IBM Security QRadar. You can use AQL to get data that might not be easily accessible from the user interface.

The following diagram shows the flow of an AQL query.

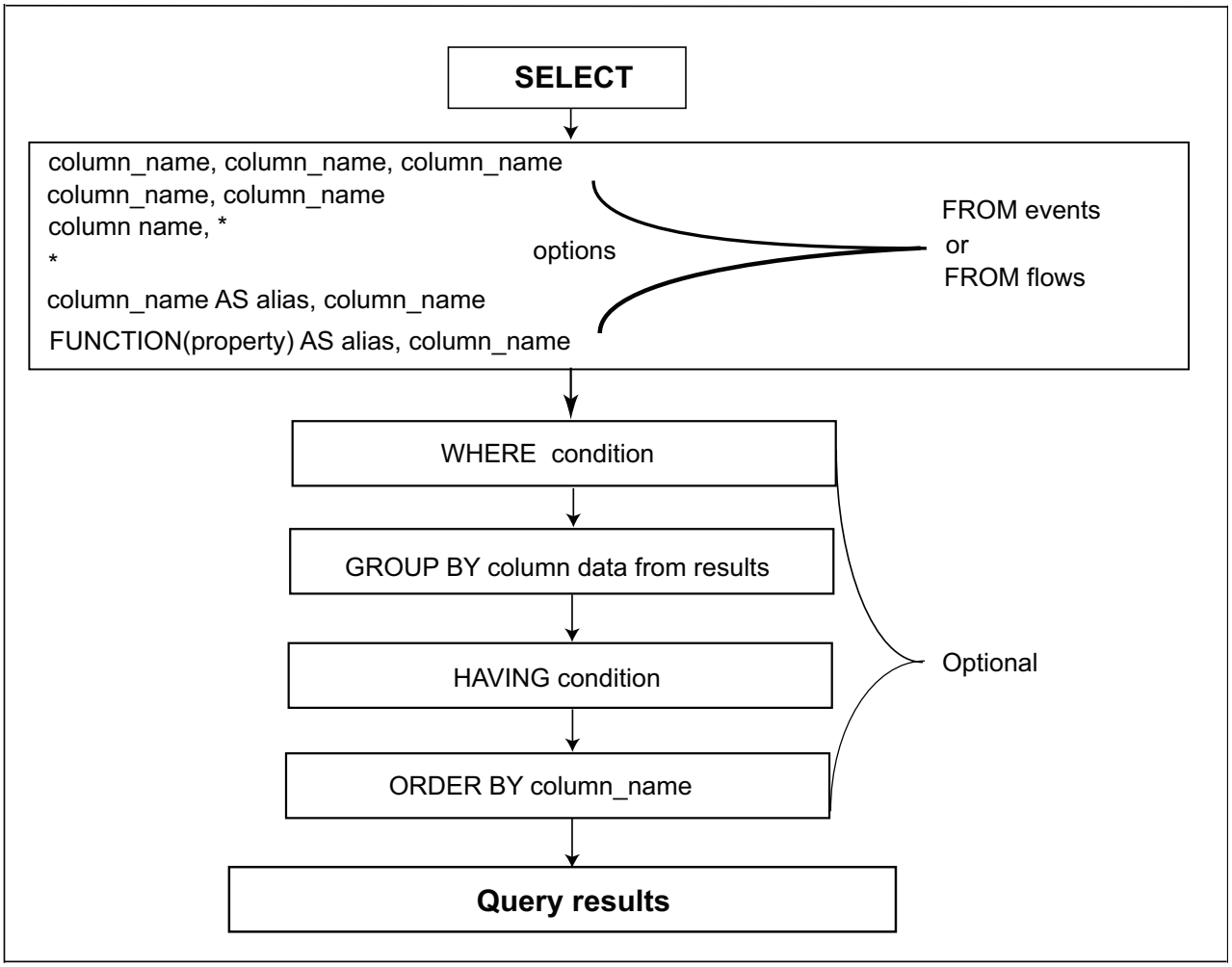

Figure 1. AQL query flow

Structure of an AQL statement

Use the `SELECT` statement to select fields from events or flows in the Ariel database, which are displayed as columns. For example, the following query returns the results that are shown in the following table:

```
SELECT sourceip, destinationip, username, protocolid, eventcount FROM
events
```

Table 2. AQL query results

sourceip	destinationip	Username	Protocolid	eventcount
193.2.45.21	195.23.44.21	Joe Ariel	233	1
193.2.45.22	195.23.44.24	Jim Ariel	233	1

AQL queries begin with a SELECT statement to select event or flow data from the Ariel database. You can refine the data output of the SELECT statement by using the WHERE, GROUP BY, HAVING, ORDER BY, LIMIT, and LAST clauses.

SELECT

Use the SELECT statement to select fields from events or flows. For example, select all fields from events or flows by typing:

`SELECT * FROM events`, or `SELECT * FROM flows`

Use the following clauses to filter and manipulate the data that is returned by the SELECT statement:

WHERE

Use the `WHERE` clause to insert a condition that filters the output, for example, `WHERE logsourceid='65'`.

GROUP BY

Use the `GROUP BY` clause to group the results by one or more columns that you specify in the query, for example, `GROUP BY logsourceid`.

HAVING

Use the `HAVING` clause to specify a condition after the `GROUP BY` clause, for example, `HAVING MAG > 3`.

ORDER BY

Use the `ORDER BY` clause to order the results for a column in the AQL query in an ascending or descending order, for example, `ORDER BY username DESC`.

LIMIT

Use a `LIMIT` clause to limit the number of results that are returned to a specific number, for example `LIMIT 50` to limit the output to 50 results.

LAST Use a LAST clause to specify a time frame for the query, for example `LAST 1 HOURS`.

The following example incorporates all of the clauses that are described in the list:

```
SELECT sourceip, destinationip, username
FROM events
WHERE username = 'test name'
GROUP by sourceip, destinationip
ORDER BY sourceip DESC
LIMIT 10
LAST 2 DAYS
```

Best practices for using quotation marks in AQL queries

In an AQL query, query terms and queried columns sometimes require single or double quotation marks so that QRadar can parse the query.

The following table defines when to use single or double quotation marks.

Table 3. Type of quotation marks to use in a query

Type of quotation marks	When to use

Single	To specify any American National Standards Institute (ANSI) VARCHAR string to SQL such as parameters for a LIKE or equals (=) operator, or any operator that expects a VARCHAR string.
	Examples:
	`SELECT * from events WHERE sourceip = '173.16.152.214'`
	`SELECT * from events WHERE userName LIKE '%james%'`
	`SELECT * from events WHERE userName = 'james'`
	`SELECT * FROM events`
	`WHERE INCIDR('10.45.225.14', sourceip)`
	`SELECT * from events WHERE TEXT SEARCH 'my search term'`

Double	Use double quotation marks for the following query items to specify table and column names that contain spaces or non-ASCII characters, and to specify custom property names that contain spaces or non-ASCII characters.
	Examples:
	`SELECT "username column" AS 'User name' FROM events`
	`SELECT "My custom property name"`
	`AS 'My new alias' FROM events`
	
	Use double quotation marks to define the name of a system object such as field, function, database, or an existing alias.
	Example:
	`SELECT "Application Category", sourceIP,`
	`EventCount AS 'Count of Events'`
	`FROM events GROUP BY "Count of Events"`
	
	Use double quotation marks to specify an existing alias that has a space when you use a WHERE, GROUP BY, or ORDER BY clause
	Examples:
	`SELECT sourceIP, destinationIP, sourcePort,`
	`EventCount AS 'Event Count',`
	`category, hasidentity, username, payload, UtF8(payLoad),`
	`QiD, QiDnAmE(qid) FROM events`
	`WHERE (NOT (sourcePort <= 3003 OR hasidentity = 'True'))`
	`AND (qid = 5000023 OR qid = 5000193)`
	`AND (INCIDR('1.1.1.0/4', sourceIP)`
	`OR NOT INCIDR('1.1.1.0/4', sourceIP)) ORDER BY "Event Count"`
	`DESC LAST 60 MINUTES`
	`SELECT sourceIP, destinationIP, sourcePort, EventCount`
	`AS 'Event Count',`
	`category, hasidentity, username, payload, UtF8(payLoad),`
	`QiD, QiDnAmE(qid)`
	`FROM events ORDER BY "Event Count"`
	`DESC LAST 60 MINUTES`

Table 3. Type of quotation marks to use in a query (continued)

Type of quotation marks	When to use

Single or double	Use single quotation marks to specify an alias for a column definition in a query.
	Example:
	`SELECT username AS 'Name of User', sourceip AS 'IP Source' FROM events`
	
	Use double quotation marks to specify an existing alias with a space when you use a WHERE, GROUP BY, or ORDER BY clause.
	Example:
	`SELECT sourceIP AS 'Source IP Address', EventCount AS 'Event Count', QiD, QiDnAmE(qid) FROM events GROUP BY "Source IP Address" LAST 60 MINUTES`

Copying query examples from the AQL guide

If you copy and paste a query example that contains single or double quotation marks from the AQL Guide, you must retype the quotation marks to be sure that the query parses.

SELECT statement

Use the SELECT statement to define the criteria that you use to retrieve event or flow data.

Use the `SELECT` statement to define the columns (fields) that you want to output from your query. You can use the SELECT statement to output data from an AQL function by using a column alias. Typically, you refer to events or flows in your SELECT statement but you can also use the `SELECT` statement with the `GLOBALVIEW` database, or any other database that you might have access to.

Use the `SELECT` statement to select the columns that you want to display in the query output.

A `SELECT` statement can include the following elements:

- Fields from the events or flows databases
- Custom properties from the events or flows databases
- Functions that you use with fields to represent specific data that you want to return.

  For example, the function `ASSETHOSTNAME(sourceip)` searches for the host name of an asset by source IP address at a specific time.

Use an asterisk (*) to denote all columns.

Field names and `SELECT` and `FROM` statements are not case-sensitive. For example, the following query uses different cases and it parses.

```
select Sourceip, DATEFORMAT(starTTime,'YYYY-MM-dd HH:mm') as startTime from
events WHERE username is noT Null GROUP BY sourceip ordER BY starttime lAsT
3 houRS
```

The following examples are queries that use SELECT statements:

- `SELECT * FROM flows`

  Returns all columns from the flows database.
- `SELECT sourceip, destinationip FROM events`

  Returns only the `sourceip` and `destinationip` columns from the events database.
- `SELECT sourceip, * FROM flows`

  Returns the `sourceip` column first, which is followed by all columns from the flows database.
- `SELECT sourceip AS 'MY Source IPs', FROM events`

  Returns the `sourceip` column as the alias or renamed column `'MY Source IPs'`.
- `SELECT ASSETHOSTNAME(sourceip) AS 'Host Name', sourceip FROM events`

  Returns the output of the function `ASSETHOSTNAME` as the column name `Host Name`, and the `sourceip` column from the events database.

WHERE clause

Filter your AQL queries by using `WHERE` clauses. The `WHERE` clause describes the filter criteria that you apply to the query and filters the resulting view to accept only those events or flows that meet the specified condition.

You can apply the `WHERE` clause to add a condition to search criteria in AQL queries, which filters the search results.

A search condition is a combination of logical and comparison operators that together make a test. Only those input rows that pass the test are included in the result.

You can apply the following filters when you use `WHERE` clause in a query:

- Equal sign (`=`)
- Not equal to symbol (`<>`)
- Less than symbol (`<`)
- Greater than symbol (`>`)
- Less that or equal to symbol (`<=`)
- Greater than or equal to symbol (`>=`)
- `BETWEEN` between two values, for example (64 AND 512)
- `LIKE` case sensitive match
- `ILIKE` case insensitive match
- `IS NULL` is empty
- `AND / OR` combine conditions or either condition
- `TEXT SEARCH` text string match

Examples of WHERE clauses

The following query example shows events that have a severity level of greater than nine and are from a specific category.

```
SELECT sourceIP, category, credibility
FROM events
WHERE
severity > 9
AND
category = 5013
```

Change the order of evaluation by using parentheses. The search conditions that are enclosed in parentheses are evaluated first.

```
SELECT sourceIP, category, credibility
FROM events
WHERE
(severity > 9 AND category = 5013)
OR
(severity < 5 AND credibility > 8)
```

Return events from the events database where the text 'typot' is found.

```
SELECT QIDNAME(qid)
AS EventName,
* FROM events
WHERE
TEXT SEARCH 'typot'
```

The following query outputs events from the events database where health is included in the log source name.

```
SELECT logsourceid, LOGSOURCEGROUPNAME(logsourceid), LOGSOURCENAME(logsourceid)
FROM events
WHERE LOGSOURCENAME(logsourceid)
ILIKE '%%health%%'
```

The following query outputs events where the device type ID is equal to 11 (Linux Server DSM), and where the QID is equal to 44250002, which is the identifier for Cron Status.

```
SELECT * FROM events
WHERE deviceType= '11'
AND qid= '44250002'
```

GROUP BY clause

Use the GROUP BY clause to aggregate your data by one or more columns. To provide meaningful results of the aggregation, usually, data aggregation is combined with arithmetic functions on remaining columns.

When you use the GROUP BY clause with a column name or AQL function, only the first value is returned for the GROUP BY column, by default, even though other values might exist.

Examples of GROUP BY clauses

The following query example shows IP addresses that sent more than 1 million bytes within all flows in a specific time.

```
SELECT sourceIP, SUM(sourceBytes)
FROM flows where sourceBytes > 1000000
GROUP BY sourceIP
```

The results might look similar to the following output.

```
---------------------------------
| sourceIP | SUM_sourceBytes |
---------------------------------
| 64.124.201.151 | 4282590.0 |
| 10.105.2.10 | 4902509.0 |
| 10.103.70.243 | 2802715.0 |
| 10.103.77.143 | 3313370.0 |
| 10.105.32.29 | 2467183.0 |
| 10.105.96.148 | 8325356.0 |
| 10.103.73.206 | 1629768.0 |
---------------------------------
```

However, if you compare this information to a non-aggregated query, the output displays all the IP addresses that are unique, as shown in the following output:

```
-----------------------------
| sourceIP | sourceBytes |
-----------------------------
| 64.124.201.151 | 1448629 |
| 10.105.2.10 | 2412426 |
| 10.103.70.243 | 1793095 |
| 10.103.77.143 | 1449148 |
| 10.105.32.29 | 1097523 |
| 10.105.96.148 | 4096834 |
| 64.124.201.151 | 2833961 |
| 10.105.2.10 | 2490083 |
| 10.103.73.206 | 1629768 |
| 10.103.70.243 | 1009620 |
| 10.105.32.29 | 1369660 |
| 10.103.77.143 | 1864222 |
| 10.105.96.148 | 4228522 |
-----------------------------
```

To view the maximum number of events, use the following syntax:

```
SELECT MAX(eventCount) FROM events
```

To view the number of average events from a source IP, use the following syntax:

```
SELECT AVG(eventCount), PROTOCOLNAME(protocolid)
FROM events
GROUP BY sourceIP
```

The output displays the following results:

```
--------------------------------
| sourceIP | protocol |
--------------------------------
| 64.124.201.151 | TCP.tcp.ip |
| 10.105.2.10 | UDP.udp.ip |
| 10.103.70.243 | UDP.udp.ip |
| 10.103.77.143 | UDP.udp.ip |
| 10.105.32.29 | TCP.tcp.ip |
| 10.105.96.148 | TCP.tcp.ip |
| 64.124.201.151 | TCP.tcp.ip |
| 10.105.2.10 | ICMP.icmp.ip |
--------------------------------
```

HAVING clause

Use the HAVING clause in a query to apply more filters to specific data by applying filters to the results after the GROUP BY clause.

The HAVING clause follows the GROUP BY clause.

You can apply the following filters when you use a `HAVING` clause in a query:

- Equal sign (=)
- Not equal to symbol (<>)
- Less than symbol (<)
- Greater than symbol (>)
- Less that or equal to symbol (<=)
- Greater than or equal to symbol (>=)
- `BETWEEN` between two values, for example (64 AND 512)
- `LIKE` case-sensitive match

- ILIKE case insensitive match
- SUM/AVG total or average values
- MAX/MIN maximum or minimum values

Examples of HAVING clauses

The following query example shows results for users who triggered VPN events from more than four IP addresses (HAVING 'Count of Source IPs' > 4) in the last 24 hours.

```
SELECT username, UNIQUECOUNT(sourceip) AS 'Count of Source IPs'
FROM events
WHERE LOGSOURCENAME(logsourceid) ILIKE '%vpn%'
AND username IS NOT NULL
GROUP BY username
HAVING "Count of Source IPs" > 4
LAST 24 HOURS
```

Note: When you type an AQL query, use single quotation marks for a string comparison, and use double quotation marks for a property value comparison.

The following query example shows results for events where the credibility (HAVING credibility > 5) is greater than five.

```
SELECT username, sourceip, credibility
FROM events
GROUP BY sourceip
HAVING credibility > 5
LAST 1 HOURS
```

The following query groups results by source IP but displays only results where the magnitude (HAVING magnitude > 5) is greater than five.

```
SELECT sourceIP, magnitude
FROM events
GROUP BY sourceIP
HAVING magnitude > 5
```

ORDER BY clause

Use the ORDER BY clause to sort the resulting view that is based on expression results. The result is sorted by ascending or descending order.

Note: When you type an AQL query, use single quotation marks for a string comparison, and use double quotation marks for a property value comparison.

You can use the ORDER BY clause on one or more columns.

Use the GROUP BY and ORDER BY clauses in a single query.

Sort in ascending or descending order by appending the ASC or DESC keyword to the ORDER BY clause.

Examples of ORDER BY clauses

To query AQL to return results in descending order, use the following syntax:

```
SELECT sourceBytes, sourceIP
FROM flows
WHERE sourceBytes > 1000000
ORDER BY sourceBytes DESC
```

To display results in ascending order, use the following syntax:

```
SELECT sourceBytes, sourceIP
FROM flows
WHERE sourceBytes > 1000000
ORDER BY sourceBytes ASC
```

To determine the top abnormal events or the most bandwidth-intensive IP addresses, you can combine GROUP BY and ORDER BY clauses in a single query. For example, the following query displays the most traffic intensive IP address in descending order:

```
SELECT sourceIP, SUM(sourceBytes)
FROM flows
GROUP BY sourceIP
ORDER BY SUM(sourceBytes) DESC
```

Note:

When you use the GROUP BY clause with a column name or AQL function, only the first value is returned for the GROUP BY column, by default, even though other values might exist.

LIKE clause

Use the LIKE clause to retrieve partial string matches in the Ariel database.

You can search fields by using the LIKE clause.

The following table shows the wildcard options are supported by the Ariel Query Language (AQL).

Table 4. Supported wildcard options for LIKE clauses

Wildcard character	Description
%	Matches a string of zero or more characters
_	Matches any single character

Examples of LIKE clauses

To match names such as Joe, Joanne, Joseph, or any other name that begins with Jo, type the following query:

```
SELECT * FROM events WHERE userName LIKE 'Jo%'
```

To match names that begin with Jo that are 3 characters long, such as, Joe or Jon, type the following query:

```
SELECT * FROM events WHERE userName LIKE 'Jo_'
```

You can enter the wildcard option at any point in the command, as shown in the following examples.

```
SELECT * FROM flows WHERE sourcePayload LIKE '%xyz'
SELECT * FROM events WHERE payload LIKE '%xyz%'
SELECT * FROM events WHERE payload LIKE '_yz'
```

Examples of string matching keywords

The keywords, ILIKE and IMATCHES are case-insensitive versions of LIKE and MATCHES.

```
SELECT qidname(qid) as test FROM events WHERE test LIKE 'Information%'
SELECT qidname(qid) as test FROM events WHERE test ILIKE 'inForMatiOn%'

SELECT qidname(qid) as test FROM events WHERE test MATCHES '.*Information.*'
SELECT qidname(qid) as test FROM events WHERE test IMATCHES '.*Information.*'
```

COUNT function

The COUNT function returns the number of rows that satisfy the WHERE clause of a SELECT statement.

If the SELECT statement does not have a WHERE clause, the COUNT function returns the total number of rows in the table.

Examples of the Count function

The following query returns the count of all events with credibility that is greater than or equal to 9.

```
SELECT COUNT(*) FROM events WHERE credibility >= 9
```

The following query returns the count of assets by location and source IP address.

```
SELECT ASSETPROPERTY('Location',sourceip)
AS location, COUNT(*)
FROM events
GROUP BY location
LAST 1 days
```

The following query returns the user names, source IP addresses, and count of events.

```
SELECT username, sourceip,
COUNT(*) FROM events
GROUP BY username
LAST 600 minutes
```

The `sourceip` column is returned as `FIRST_sourceip`.

One `sourceip` is returned only per `username`, even if another `sourceip` exists.

Note:

When you use the `GROUP BY` clause with a column name or AQL function, only the first value is returned for the `GROUP BY` column, by default, even though other values might exist.

AQL logical and comparison operators

Operators are used in AQL statements to determine any equality or difference between values. By using operators in the **WHERE** clause of an AQL statement, the results are filtered by those results that match the conditions in the **WHERE** clause.

The following table lists the supported logical and comparison operators.

Table 5. Logical and comparison operators

Operator	Description	Example

*	Multiplies two values and returns the result.	`SELECT *`
		`FROM flows`
		`WHERE sourceBytes * 1024 < 1`

Table 5. Logical and comparison operators (continued)

Operator	Description	Example
=	The equal to operator compares two values and returns true if they are equal.	SELECT * FROM EVENTS WHERE sourceIP = destinationIP
!=	Compares two values and returns true if they are unequal.	SELECT * FROM events WHERE sourceIP != destinationip
< AND <=	Compares two values and returns true if the value on the left side is less than or equal to, the value on the right side.	SELECT * FROM flows WHERE sourceBytes < 64 AND destinationBytes <= 64
> AND >=	Compares two values and returns true if the value on the left side is greater than or equal to the value on the right side.	SELECT * FROM flows WHERE sourceBytes > 64 AND destinationBytes >= 64
/	Divides two values and returns the result.	SELECT * FROM flows WHERE sourceBytes / 8 > 64
+	Adds two values and returns the result.	SELECT * FROM flows WHERE sourceBytes + destinationBytes < 64
-	Subtracts one value from another and returns the result.	SELECT * FROM flows WHERE sourceBytes - destinationBytes > 0
^	Takes a value and raises it to the specified power and returns the result.	SELECT * FROM flows WHERE sourceBytes ^ 2 < 256
%	Takes the modulo of a value and returns the result.	SELECT * FROM flows WHERE sourceBytes % 8 == 7
AND	Takes the left side and right side of a statement and returns true if both are true.	SELECT * FROM events WHERE (sourceIP = destinationIP) AND (sourcePort = destinationPort)
BETWEEN (X,Y)	Takes in a left side and two values and returns true if the left side is between the two values.	SELECT * FROM events WHERE magnitude BETWEEN 1 AND 5
COLLATE	Parameter to order by that allows a BCP47 language tag to collate.	SELECT * FROM EVENTS ORDER BY sourceIP DESC COLLATE 'de-CH'
INTO	Creates a named cursor that contains results that can be queried at a different time.	SELECT * FROM EVENTS INTO 'MyCursor' WHERE....

Table 5. Logical and comparison operators (continued)

Operator	Description	Example
NOT	Takes in a statement and returns true if the statement evaluates as false.	`SELECT * FROM EVENTS WHERE NOT (sourceIP = destinationIP)`
ILIKE	Matches if the string passed is LIKE the passed value and is not case sensitive. Use % as a wildcard.	`SELECT * FROM events WHERE userName ILIKE '%bob%'`
IMATCHES	Matches if the string matches the provided regular expression and is not case sensitive.	`SELECT * FROM events WHERE userName IMATCHES '^.bob.$'`
LIMIT	Limits the number of results to the provided number.	`SELECT * FROM events LIMIT 100 START '2015-10-28 10:00' STOP '2015-10-28 11:00'` **Note:** Place the LIMIT clause in front of a START and STOP clause.
LIKE	Matches if the string passed is LIKE the passed value but is case sensitive. Use % as a wildcard.	`SELECT * FROM events WHERE userName LIKE '%bob%'`
MATCHES	Matches if the string matches the provided regular expression.	`SELECT * FROM events WHERE userName MATCHES '^.bob.$'`
NOT NULL	Takes in a value and returns true if the value is not null.	`SELECT * FROM events WHERE userName IS NOT NULL`
OR	Takes the left side of a statement and the right side of a statement and returns true if either side is true.	`SELECT * FROM events WHERE (sourceIP = destinationIP) OR (sourcePort = destinationPort)`

Table 5. Logical and comparison operators (continued)

Operator	Description	Example

TEXT SEARCH	Full-text search for the passed value.
	
	TEXT SEARCH is valid with AND operators. You can't use TEXT SEARCH with OR or other operators; otherwise, you get a syntax error.
	
	Place TEXT SEARCH in the first position of the WHERE clause.
	
	You can also do full-text searches by using the Quick filter in the QRadar user interface. For information about Quick filter functions, see the *IBM Security QRadar User Guide*.
		`SELECT *`
		`FROM events`
		`WHERE TEXT SEARCH 'firewall'`
		`AND sourceip='192.168.1.1'`
		
		`SELECT sourceip,url`
		`FROM events`
		`WHERE TEXT SEARCH`
		`'download.cdn.mozilla.net'`
		`AND sourceip='192.168.1.1'`
		`START '2015-01-30 16:10:12'`
		`STOP '2015-02-22 17:10:22'`

Examples of logical and comparative operators

- To find events that are not parsed, type the following query:

```
SELECT * FROM events
WHERE payload = 'false'
```

- To find events that return an offense and have a specific source IP address, type the following query:

```
SELECT * FROM events
WHERE sourceIP = '231.12.37.17'
AND
hasOffense = 'true'
```

- To find events that include the text "firewall", type the following query:

```
SELECT QIDNAME(qid)
AS EventName,
* FROM events
WHERE TEXT SEARCH 'firewall'
```

AQL data calculation and formatting functions

Use Ariel Query Language (AQL) calculation or formatting functions to do calculations or data formatting on search results that are retrieved from the Ariel databases.

Data calculation and formatting functions

Use the following AQL functions to do calculations or data formatting on search results that are retrieved from the Ariel databases:

- "CONCAT" on page 19
- "DATEFORMAT" on page 19
- "DOUBLE" on page 19
- "LONG" on page 19

- "LOWER" on page 20
- "NOW" on page 20
- "PARSEDATETIME" on page 20
- "REPLACEALL" on page 20
- "REPLACEFIRST" on page 21
- "STRLEN" on page 21
- "SUBSTRING" on page 21
- "UPPER" on page 21

CONCAT

Purpose

Concatenates all passed strings into 1 string.

Example

```
SELECT CONCAT(username, ':', sourceip,  ':', destinationip)
FROM events LIMIT 5
```

Concatenates user name, source IP address, and destination IP address and places a colon between the concatenated results. For example, `userJoe:10.2.2.1:127.0.0.1`

DATEFORMAT

Purpose

Formats a time, which is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on January 1, 1970 to a user-readable form.

Examples

```
SELECT
DATEFORMAT(startTime, 'yyyy-MM-dd hh:mm:ss')
AS StartTime
FROM events
```

```
SELECT DATEFORMAT(starttime,'yyyy-MM-dd hh:mm')
AS 'Start Time',
DATEFORMAT(endtime, 'yyyy-MM-dd hh:mm')
AS End_time,
QIDDESCRIPTION(qid)
AS 'Event Name'
FROM events
```

See more examples

DOUBLE

Purpose

Converts a value that represents a number into a double.

Example

```
DOUBLE('1234')
```

LONG

Purpose

Converts a value that represents a number into a long integer.

Examples

```
SELECT destinationip,
LONG(SUM(sourcebytes+destinationbytes))
AS TotalBytes
FROM flows
GROUP BY sourceip
```

The example returns the destination IP address, and the sum of the source and destination bytes in the **TotalBytes** column.

PARSEDATETIME

Purpose

Pass a time value to the parser, for example, `PARSEDATETIME('time reference')`. This is the parse time for the query.

Example

```
SELECT * FROM events
START PARSEDATETIME('1 hour ago')
```

Parse events from hour ago.

See more examples of time functions

NOW

Purpose

Returns the current time that is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on January 1, 1970.

Example

```
SELECT ASSETUSER(sourceip, NOW())
AS 'Asset user' FROM events
```

Find the user of the asset at this moment in time (NOW).

LOWER

Purpose

Returns an all lowercase representation of a string.

Example

```
SELECT
LOWER(username),
LOWER(LOGSOURCENAME(logsourceid))
FROM events
```

Returns user names and log source names in lowercase.

REPLACEALL

Purpose

Match a regex and replace all matches with text.

Replaces every subsequence (*arg2*) of the input sequence that matches the pattern (*arg1*) with the replacement string (*arg3*).

Example

```
REPLACEALL('\d{16}',
username, 'censored')
```

REPLACEFIRST

Purpose

Match a regex and replace the first match with text.

Replaces the first subsequence (*arg2*) of the input sequence that matches the pattern (*arg1*) with the replacement string (*arg3*).

Example

```
REPLACEFIRST('\d{16}',
 username, 'censored')
```

STR

Purpose

Converts any parameter to a string.

Example

```
STR(sourceIP)
```

STRLEN

Purpose

Returns the length of this string.

Example

```
SELECT STRLEN(sourceIP),
STRLEN(username) from events
```

Returns the string length for `sourceip` and `username`.

STRPOS

Purpose

Returns the position (index - starts at zero) of a string in another string. Searches in string for the index of the specified substring. You can optionally specify an extra parameter to indicate at what position (index) to start looking for the specified pattern.

The search for the string starts at the specified offset and moves towards the end of string.
`STRPOS(string, substring, index)`
Returns `-1` if the substring isn't found

Examples

```
SELECT STRPOS(username, 'name') FROM events
SELECT STRPOS(sourceip, '180', 2) FROM events)
```

SUBSTRING

Purpose

Copies a range of characters into a new string.

Examples

```
SELECT SUBSTRING(userName, 0, 3) FROM events
SELECT SUBSTRING(sourceip, 3, 5) FROM events
```

UPPER

Purpose

Returns an all uppercase representation of a string.

Example

```
SELECT
UPPER(username),
UPPER(LOGSOURCENAME(logsourceid))
FROM events
```

Returns user names and log source names in uppercase.

UTF8

Purpose

Returns the UTF8 string of a byte array.

Example

```
SELECT UTF8(payload)
FROM events
WHERE sourceip='20.189.234.55'
```

Returns the UTF8 payload for events where the source IP address is 20.189.234.55

AQL data aggregation functions

Ariel Query Language (AQL) aggregate functions help you to aggregate and manipulate the data that you extract from the Ariel database.

Data aggregation functions

Use the following AQL functions to aggregate data, and to do calculations on the aggregated data that you extract from the AQL databases:

- "AVG"
- "COUNT" on page 23
- "FIRST" on page 23
- "GROUP BY" on page 23
- "HAVING" on page 23
- "LAST" on page 24
- "MIN" on page 24
- "MAX" on page 24
- "STDEV" on page 24
- "STDEVP" on page 24
- "SUM" on page 25
- "UNIQUECOUNT" on page 25

AVG

Purpose

Returns the average value of the rows in the aggregate.

Example

```
SELECT sourceip,
AVG(magnitude)
FROM events
GROUP BY sourceip
```

COUNT

Purpose

Returns the count of the rows in the aggregate.

Example

```
SELECT sourceip,
COUNT(*)
FROM events
GROUP BY sourceip
```

See more examples

FIRST

Purpose

Returns the first entry of the rows in the aggregate.

Example

```
SELECT sourceip,
FIRST(magnitude)
FROM events
GROUP BY sourceip
```

GROUP BY

Purpose

Creates an aggregate on one or more columns.

When you use the GROUP BY clause with a column name or AQL function, only the first value is returned for the GROUP BY column, by default, even though other values might exist.

To return values other than the default first value, use functions such as COUNT, MAX, AVG.

Examples

```
SELECT sourceip,
COUNT(*)
FROM  events
GROUP BY sourceip, destinationip
```

```
SELECT username, sourceip,
COUNT(*) FROM events
GROUP BY username
LAST 5 minutes
```

The `sourceip` column is returned as `FIRST_sourceip`. Only one `sourceip` is returned per `username`, even if another `sourceip` exists.

```
SELECT username,
COUNT(sourceip),
COUNT(*) FROM events
GROUP BY username
LAST 5 minutes
```

The `sourceip` column is returned as `COUNT_sourceip`. The count for `sourceip` results is returned per `username`.
See more examples

HAVING

Purpose

Uses operators on the result of a grouped by column.

Example

```
SELECT sourceip,
MAX(magnitude)
AS MAG
FROM events
GROUP BY  sourceip
HAVING MAG > 5
```

See more examples
Saved searches that include the having clause and that are used for scheduled reports or time-series graphs are not supported.

LAST

Purpose

Returns the last entry of the rows in the aggregate.

Example

```
SELECT sourceip,
LAST(magnitude)
FROM events
GROUP BY sourceip
```

MIN

Purpose

Returns the minimum value of the rows in the aggregate.

Example

```
SELECT sourceip,
MIN(magnitude)
FROM events
GROUP BY sourceip
```

MAX

Purpose

Returns the maximum value of the rows in the aggregate.

Example

```
SELECT sourceip,
MAX(magnitude)
FROM events
GROUP BY sourceip
```

STDEV

Purpose

Returns the Sample Standard Deviation value of the rows in the aggregate.

Example

```
SELECT sourceip,
STDEV(magnitude)
FROM events
GROUP BY sourceip
```

STDEVP

Purpose

Returns the Population Standard Deviation value of the rows in the aggregate.

Example

```
SELECT sourceip,
STDEVP(magnitude)
FROM events
GROUP BY sourceip
```

SUM

Purpose

Returns the sum of the rows in the aggregate.

Example

```
SELECT sourceip,
SUM(sourceBytes)
FROM flows
GROUP BY sourceip
```

UNIQUECOUNT

Purpose

Returns the unique count of the value in the aggregate.

Example

```
SELECT username,
UNIQUECOUNT(sourceip)
AS CountSrcIP
FROM events
GROUP BY sourceip
```

AQL data retrieval functions

Use the Ariel Query Language (AQL) built-in functions to retrieve data by using data query functions, and field ID properties from the Ariel database.

Use the following AQL functions to extract data from the AQL databases:

Data retrieval functions

- "APPLICATIONNAME" on page 26
- "ASSETHOSTNAME" on page 26
- "ASSETPROPERTY" on page 26
- "ASSETUSER" on page 27
- "CATEGORYNAME" on page 27
- "DOMAINNAME" on page 27
- "GLOBALVIEW" on page 28
- "HOSTNAME" on page 28
- "INCIDR " on page 28
- "INOFFENSE" on page 29
- "LOGSOURCENAME" on page 29
- "LOGSOURCEGROUPNAME" on page 29
- "LOGSOURCETYPENAME" on page 30
- "MATCHESASSETSEARCH" on page 30
- "NETWORKNAME" on page 30
- "PROCESSORNAME" on page 31
- "PROTOCOLNAME" on page 32

- "QIDNAME" on page 32
- "QIDESCRIPTION" on page 32
- "REFERENCEMAP" on page 32
- "REFERENCETABLE" on page 33
- "REFERENCESETCONTAINS" on page 33
- "RULENAME" on page 34

APPLICATIONNAME

Purpose

Returns flow application names by application ID

Parameters

Application ID

Example

```
SELECT APPLICATIONNAME(applicationid)
AS 'Name of App'
FROM flows
```

Returns the names of applications from the flows database. These application names are listed in the **Name of App** column, which is an alias.

ASSETHOSTNAME

Purpose

Searches for the host name of an asset at a point in time.

The domain can optionally be specified to target an asset on a particular domain.

```
ASSETHOSTNAME(sourceip)
ASSETHOSTNAME(sourceip, NOW())
ASSETHOSTNAME(sourceip, dommainid)
```

Parameters

IP address, (timestamp and domain ID are optional)

If the time stamp is not specified, the current time is used.

Examples

```
SELECT ASSETHOSTNAME(destinationip, NOW())
AS 'Host Name'
FROM events
```

```
SELECT ASSETHOSTNAME(sourceip, NOW())
AS 'Host Name'
FROM events
```

Returns the host name of the asset at the time of the query.

ASSETPROPERTY

Purpose

Looks up a property for an asset.

The domain can optionally be specified to target an asset on a particular domain.

```
ASSETPROPERTY
('Unified Name', sourceIP, domainId)
```

Parameters

Property name, IP address

Domain ID is optional

Example

```
SELECT
ASSETPROPERTY('Location',sourceip)
AS Asset_location,
COUNT(*)
AS 'event count'
FROM events
GROUP BY Asset_location
LAST 1 days
```

Returns the asset location that is affiliated with the source IP address.

ASSETUSER

Purpose

Searches for the user of an asset at a point in time.

Domain can optionally be specified to target an asset in a specific domain.

```
ASSETUSER(sourceIP,NOW(), domainId)
```

Parameters

IP address, (timestamp and domain ID are optional)

If the time stamp is not specified, the current time is used.

Example

```
SELECT
ASSETUSER(sourceip, now())
AS 'Username of Asset'
FROM events
```

Returns the user name that is affiliated with the source IP address.

CATEGORYNAME

Purpose

Searches for the name of a category by the category ID.

```
CATEGORYNAME(Category)
```

Parameters

Category

Example

```
SELECT sourceip, category,
CATEGORYNAME(category)
AS 'Category name'
FROM events
```

Returns the source IP, category ID, and category name

DOMAINNAME

Purpose

Searches for the domain name by the domain ID.

```
DOMAINNAME(domainID)
```

Parameters

Domain ID

Example

```
SELECT sourceip, username,
DOMAINNAME(domainid)
AS 'Domain name'
FROM events
```

Returns source IP, user name, and domain names from events database

GLOBALVIEW

Purpose

Returns the GLOBALVIEW database results for a given saved search name based on the time range that is input.

This query can be run only by using API.

For more information about accessing a GLOBALVIEW database, see the *IBM Security QRadar Administration Guide*.

Parameters

Saved search, time range (DAILY, NORMAL, HOURLY)

Example

```
SELECT *
FROM GLOBALVIEW
('Top Log Sources','DAILY')
LAST 2 days
```

HOSTNAME

Purpose

Searches for the host name by the log source ID or the flow source ID.

```
HOSTNAME(logsourceid)
```

```
HOSTNAME(flowinterfaceid)
```

Parameters

Log source ID or the flow source ID

Examples

```
SELECT HOSTNAME(logsourceid)
AS 'Host Name' from events
```

Returns the host name that is linked to the log source ID

```
SELECT HOSTNAME(flowinterfaceid)
AS 'Host Name'
FROM flows
```

Returns the host name that is linked to the flow source interface ID

INCIDR

Purpose

Filters the output of the SELECT statement by referencing the source/destination CIDR IP address that is specified by INCIDR.

Parameters

IP/CIDR, IP address

Example

```
SELECT sourceip, username
FROM events
WHERE INCIDR('172.16.0.0/16', sourceip)
```

Returns the source IP and user name columns from the flows database where the source CIDR IP address is from the 172.16.0.0/16 subnet. See more examples

INOFFENSE

Purpose

If an event or flow belongs to the specified offense, it returns `true`.

Parameters

Offense ID

Example

```
SELECT * FROM events
 WHERE InOffense(123)
```

```
SELECT * FROM flows
 WHERE InOffense(123)
```

LOGSOURCENAME

Purpose

Looks up the name of a log source by its log source ID.

```
LOGSOURCENAME(logsourceid)
```

Parameters

Log source ID

Example

```
SELECT * FROM events
WHERE LOGSOURCENAME(logsourceid)
ILIKE '%mylogsourcename%'
```

Returns only results that include `mylogsourcename` in their log source name.

```
SELECT LOGSOURCENAME(logsourceid)
AS Log_Source
FROM events
```

Returns the column alias **Log_source**, which shows log source names from the events database.

LOGSOURCEGROUPNAME

Purpose

Searches for the name of a log source group by its log source group ID.

```
LOGSOURCEGROUPNAME(deviceGroupList)
```

Parameters

Device group list

Example

```
SELECT sourceip, logsourceid
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist)
ILIKE '%other%'
```

Returns the source IP address and log source IDs for log source groups that have 'other' in their name.

LOGSOURCETYPENAME

Purpose

Searches for the name of a log source type by its device type.

`LOGSOURCETYPENAME(deviceType)`

Parameters

Device type

Example

```
SELECT LOGSOURCETYPENAME(deviceType)
AS 'Device names', COUNT(*)
FROM events
GROUP BY "Device names"
LAST 1 DAYS
```

Returns device names and the event count.

All log sources functions example:

```
SELECT logsourceid,
LOGSOURCENAME(logsourceid)
AS 'Name of log source',
LOGSOURCEGROUPNAME(devicegrouplist)
AS 'Group Names',
LOGSOURCETYPENAME(deviceType)
AS 'Devices'
FROM events
GROUP BY logsourceid
```

Returns log source names, log source group names, and log source device names.
When you use the `GROUP BY` function, the first item only in the `GROUP BY` list is shown in the results.

MATCHESASSETSEARCH

Purpose

If the asset is returned in the results of the saved search, it returns true.

```
MATCHESASSETSEARCH
('My Saved Search', sourceIP)
```

Parameters

Saved Search Name, IP address

Example

```
MATCHESASSETSEARCH
('My Saved Search', sourceIP)
```

NETWORKNAME

Purpose

Searches for the network name from the network hierarchy for the host that is passed in.

```
NetworkName(sourceip)
```

The domain can optionally be specified to target a network in a particular domain.

```
NETWORKNAME(sourceip, domainId)
```

Parameters

Host property (domain is optional)

Examples

```
SELECT NETWORKNAME(sourceip)
ILIKE 'servers'
AS 'My Networks'
FROM flows
```

Returns any networks that have the name servers.

```
SELECT NETWORKNAME(sourceip, domainID)
ILIKE 'servers'
AS 'My Networks'
FROM flows
```

Returns any networks that have the name servers in a specific domain.

```
SELECT NETWORKNAME(sourceip)
AS 'Src Net',
NETWORKNAME(destinationip)
AS Dest_net
FROM events
```

Returns the network name that is associated with the source and destination IP addresses.

PROCESSORNAME

Purpose

Returns the name of a processor by the processor ID.

```
PROCESSORNAME(processorid)
```

Parameters

Processor ID number

Example

```
SELECT sourceip, PROCESSORNAME(processorid)
AS 'Processor Name'
FROM events
```

Returns the source IP address and processor name from the events database.

Example

```
SELECT * FROM EVENTS
PARAMETERS REMOTESERVERS='122.16.104.83:32006'
```

Returns results from the specified Ariel query server. By using the REMOTESERVERS parameter, you can narrow your search to specific servers, which speeds up your search by not searching all hosts. The Ariel server port 32006 and IP address 122.16.104.83 are used in the example.

Example

```
SELECT processorid, PROCESSORNAME(processorid)
FROM events WHERE processorid=104
GROUP BY processorid LAST 5 MINUTES
```

Returns results from the Event Processor that has a processor ID equal to 104.

PROTOCOLNAME

Purpose

Returns the name of a protocol by the protocol ID

Parameters

Protocol ID number

Example

```
SELECT sourceip, PROTOCOLNAME(protocolid)
AS 'Name of protocol'
FROM events
```

Returns the source IP address and protocol name from the events database.

QIDNAME

Purpose

Searches for the name of a QID by its QID.

```
QIDNAME(qid)
```

Parameters

QID

Example

```
SELECT QIDNAME(qid)
AS 'My Event Names', qid
FROM events
```

Returns QID name and QID number.

QIDESCRIPTION

Purpose

Searches for the QID description by its QID.

```
QIDDESCRIPTION(qid)
```

Parameters

QID

Example

```
SELECT QIDDESCRIPTION(qid)
AS 'My_Event_Names', QIDNAME(qid)
AS 'QID Name'
FROM events
```

Returns QID description and QID name.

REFERENCEMAP

Purpose

Searches for the value for a key in a reference map.

```
ReferenceMap('Value',Key)
```

Parameters

String, String

Example

```
SELECT
REFERENCEMAP('Full_name_lookup', username)
AS Name_of_User
FROM events
```

Searches for the `userName` (key) in the `Full_name_lookup` reference map, and returns the full name (value) for the user name (key).

REFERENCETABLE

Purpose

Searches for the value of a column key in a table that is identified by a table key in a specific reference table collection.

```
REFERENCETABLE
('testTable','value','key')
or
REFERENCETABLE
('testTable','value','key')
```

Parameters

String, String, String (or IP address)

Example

```
SELECT
REFERENCETABLE('user_data','FullName',username)
AS 'Full Name',
REFERENCETABLE('user_data','Location',username)
AS Location,
REFERENCETABLE('user_data','Manager',username)
AS Manager
FROM events
```

Returns the full name (value), location (value), and manager (value) for the `username` (key) from `user_data`.
See more Reference data examples

REFERENCESETCONTAINS

Purpose

If a value is contained in a specific reference set, it returns `true`.

```
REFERENCESETCONTAINS
('Ref_Set', 'value')
```

Parameters

String, String

Example

```
SELECT
ASSETUSER(sourceip, NOW())
AS 'Source Asset User'
FROM flows
WHERE
REFERENCESETCONTAINS('Watchusers', username)
GROUP BY "Source Asset User"
LAST 24 HOURS
```

Returns the asset user when the `username` (value) is included in the `Watchusers` reference set.

RULENAME

Purpose

Returns one or more rule names that are based on the rule ID or IDs that are passed in.

```
RULENAME(creeventlist)
RULENAME(3453)
```

Parameters

A single rule ID, or a list of rule IDs.

Example

```
SELECT * FROM events
WHERE RULENAME(creEventList)
ILIKE '%my rule name%'
```

Returns events that trigger a specific rule name.

```
SELECT RULENAME(123)
FROM events
```

Returns rule name by the rule ID.

Time criteria in AQL queries

Define time intervals in your AQL queries by using START and STOP clauses, or use the LAST clause for relative time references.

Define the time settings that are passed to the AQL query

The SELECT statement supports an `arieltime` option, which overrides the time settings.

You can limit the time period for which an AQL query is evaluated by using the following clauses and functions:

- "START"
- "STOP " on page 35
- "LAST" on page 36
- "NOW" on page 36
- "PARSEDATETIME" on page 36

START

You can pass a time interval to `START` selecting data (from time), in the following formats:

```
yyyy-MM-dd HH:mm
yyyy-MM-dd HH:mm:ss
yyyy/MM/dd HH:mm:ss
yyyy/MM/dd-HH:mm:ss
yyyy:MM:dd-HH:mm:ss
```

The *timezone* is represented by `'z` or `Z'` in the following formats:

```
yyyy-MM-dd HH:mm'Z'
yyyy-MM-dd HH:mm'z'
```

Use `START` in combination with `STOP`.

Examples

```
SELECT *
FROM events WHERE userName IS NULL
START '2014-04-25 15:51'
STOP '2014-04-25 17:00'
```

Returns results from: 2014-04-25 15:51:00 to 2014-04-25 16:59:59

```
SELECT *
FROM events WHERE userName IS NULL
START '2014-04-25 15:51:20'
STOP '2014-04-25 17:00:20'
```

Returns results from: 2014-04-25 15:51:00 to 2014-04-25 17:00:59

```
SELECT * from events
START PARSEDATETIME('1 hour ago')
STOP PARSEDATETIME('now')
```

STOP is optional. If you don't include it in the query, the STOP time is = now

STOP

You can pass a time interval to STOP selecting data (end time), in the following formats:

```
yyyy-MM-dd HH:mm
yyyy-MM-dd HH:mm:ss
yyyy/MM/dd HH:mm:ss
yyyy/MM/dd-HH:mm:ss
yyyy:MM:dd-HH:mm:ss
```

The *timezone* is represented by 'z or Z' in the following formats:

```
yyyy-MM-dd HH:mm'Z'
```

```
yyyy-MM-dd HH:mm'z'
```

Use STOP in combination with START.

Examples

```
SELECT * FROM events
WHERE username IS NULL
START  '2016-04-25 14:00'
STOP '2016-04-25 16:00'
```

```
SELECT * FROM events
WHERE username IS NULL
START '2016-04-25 15:00:30'
STOP '2016-04-25 15:02:30'
```

Use any format with the PARSEDATETIME function, for example,

```
SELECT *
FROM events
START PARSEDATETIME('1 day ago')
```

Even though STOP is not included in this query, the STOP time is = now.

```
Select * FROM events
START PARSEDATETIME('1 hour ago')
STOP PARSEDATETIME('now')
```

```
SELECT * FROM events
START PARSEDATETIME('1 day ago')
```

```
Select *
FROM events
WHERE logsourceid = '69'
START '2016-06-21 15:51:00'
STOP '2016-06-22 15:56:00'
```

LAST

You can pass a time interval to the LAST clause to specify a specific time to select data from.

The valid intervals are MINUTES, HOURS, and DAYS

Examples

```
SELECT * FROM events
LAST 15 MINUTES
```

```
SELECT * FROM events
LAST 2 DAYS
```

```
SELECT * from events
WHERE userName ILIKE '%dm%'
LIMIT 10
LAST 1 HOURS
```

Note: If you use a LIMIT clause in your query, you must place it before START and STOP clauses, for example,

```
SELECT *
FROM events
LIMIT 100
START '2016-06-28 10:00'
STOP '2016-06-28 11:00'
```

Time functions

Use the following time functions to specify the parse time for the query.

NOW

Purpose

Returns the current time that is expressed as milliseconds since the time 00:00:00 Coordinated Universal Time (UTC) on January 1, 1970.

Example

```
SELECT ASSETUSER(sourceip, NOW())
AS 'Asset user' FROM events
```

Find the user of the asset at this moment in time (NOW).

PARSEDATETIME

Purpose

Pass a time value to the parser, for example, `PARSEDATETIME('time reference')`. This `'time reference'` is the parse time for the query.

Example

```
SELECT * FROM events
START PARSEDATETIME('1 hour ago')
```

AQL date and time formats

Use Ariel Query Language (AQL) date and time formats to represent times and dates in queries.

The following table lists the letters that represent date and time in AQL queries. This table is based on the *SimpleDateFormat*.

Table 6. Date and time formats

Letter	Date or time parameter	Presentation	Examples

y	Calendar year	Year
		
		Date example used is: 20-June-2016
			`DATEFORMAT(starttime,'yy-MM-dd')`
			
			Returns date format: 16-06-20
			
			`DATEFORMAT(starttime,'yyyy-MM-dd')`
			
			Returns date format: 2016-06-20
			
			`SELECT DATEFORMAT(devicetime,'yyyy-MM-dd') AS Log_Src_Date, QIDDESCRIPTION(qid) AS 'Event Name' FROM events`

Y	Week year	Year
		
		The first and last days of a week year can have different calendar year values.
		
		Date example used is: 20-June-2016
			`DATEFORMAT(starttime,'YY-MM-dd')`
			
			Returns date format: 16-06-20
			
			`DATEFORMAT(starttime,'YYYY-MM-dd')`
			
			Returns date format: 2016-06-20
			
			`SELECT DATEFORMAT(starttime,'YYYY-MM-dd hh:mm') AS 'Start Time', DATEFORMAT(endtime,'YYYY-MM-dd hh:mm') AS End_time, QIDDESCRIPTION(qid) AS 'Event Name' FROM events`
			
			Returns start time, end time, and event name columns

M	Month in year	Month
		
		3 or more letters are interpreted as text.
		
		2 letters are interpreted as a number.
		
		Date example used is: 20-June-2016
			`DATEFORMAT(starttime,'yyyy-MMMM-dd')`
			
			Returns date format: 2016-June-20
			
			`DATEFORMAT(starttime,'yyyy-MMM-dd')`
			
			Returns date format: 2016-Jun-20
			
			`DATEFORMAT(starttime,'yyyy-MM-dd')`
			
			Returns date format: 2016-06-20

w	Week in year	Number Date example used is: 20-June-2016	`DATEFORMAT(starttime,'yyyy-ww-dd')` Returns date format: 2016-26-20 **Note:** 26 is week 26 in year
W	Week in month	Number Date example used is: 20-June-2016	`DATEFORMAT(starttime,'yyyy-WW-dd')` Returns date format: 2016-04-20 **Note:** 04 is week 4 in month
D	Day in year	Number Day in year represented by number Date example used is: 20-June-2016	`DATEFORMAT(starttime,'yyyy-mm-DD')` Returns date format: 2016-06-172 **Note:** 172 is day number 172 in year
d	Day in month	Number Date example used is: 20-June-2016	`DATEFORMAT(starttime,'yyyy-mm-dd')` Returns date format: 2016-06-20
F	Day of week in month	Number Date example used is: 20-June-2016	`DATEFORMAT(starttime,'yyyy-MM-FF')` Returns date format: 2016-06-03 **Note:** 03 is day 3 of week in month

Table 6. Date and time formats (continued)

Letter	Date or time parameter	Presentation	Examples
E	Day name in week	Text	`DATEFORMAT(starttime,'yyyy-MM-EE')`
		Date example used is: 20-June-2016	Returns date format: 2016-06-Mon
a	AM or PM	Text	`DATEFORMAT(starttime,'yyyy-MM-dd h a')`
		Date example used is: 20-June-2016	2016-06-20 06 PM
H	Hour in day (0-23)	Number	`DATEFORMAT(starttime,'yyyy-MM-dd H')`
		Date example used is: 20-June-2016	Returns date format: 2016-06-20 18 **Note:** 18 is 18:00 hours
k	Hour in day (1-24)	Number	`DATEFORMAT(starttime,'yyyy-MM-dd k')`
		Date example used is: 20-June-2016	Returns date format: 2016-06-20 18 **Note:** 18 is 18:00 hours
K	Hour in AM/PM (0-11)	Number	`DATEFORMAT(starttime,'yyyy-MM-dd K a')`
		Date example used is: 20-June-2016, 6 PM	Returns date format: 2016-06-20 6 PM **Note:** K = 6 and a = PM
h	Hour in AM/PM (1-12)	Number	`DATEFORMAT (starttime,'yyyy-MM-dd h a')`
		Date example used is: 20-June-2016 6 PM	Returns date format: 2016-06-20 6 PM **Note:** h = 6 and a = PM
m	Minute in hour	Number	`DATEFORMAT(starttime,'yyyy-MM-dd h:m a')`
		Date example used is: 20-June-2016, 6:10 PM	Returns date format: 2016-06-20 6:10 PM **Note:** colon added in query to format time
s	Second in minute	Number	`DATEFORMAT(starttime,'yyyy-MM-dd h:m:s a')`
		Date example used is: 20-June-2016, 6:10:56 PM	Returns date format: 2016-06-20 6:10:56 PM **Note:** colons added in query to format time
S	Millisecond	Number	`DATEFORMAT(starttime,'yyyy-MM-dd h:m:ss:SSS a')`
		Date example used is: 20-June-2016, 6:10 PM	Returns date format: 2016-06-20 6:10:00:322 PM **Note:** colons added in query to format time
z	Time zone	General Time zone	`DATEFORMAT(starttime,'yyyy-MM-dd h:m a z')`
		Date example used is: 20-June-2016, 6:10 PM GMT +1	Returns date format: 2016-06-20 6:10 PM GMT + 1 **Note:** colon added in query to format time
Z	Time zone	RFC 822 time zone	`DATEFORMAT(starttime,'yyyy-MM-dd h:m a Z')`
		Date example used is: 20-June-2016, 6:10 PM GMT +1	Returns date format: 2016-06-20 6:10 PM + 0100 **Note:** colon added in query to format time
X	Time zone	ISO 8601 time zone	`DATEFORMAT(starttime,'yyyy-MM-dd h:m a X')`
		Date example used is: 20-June-2016, 6:10 PM GMT +1	Returns date format: 2016-06-20 6:10 PM + 01 **Note:** colon added in query to format time

AQL subquery

Use an AQL subquery as a data source that is referred to, or searched by the main query. Use the FROM or IN clause to refine your AQL query by referring to the data that is retrieved by the subquery.

A *subquery* is a nested or inner query that is referenced by the main query. A subquery is accessible only by using API and is not yet available for use in searches from the **Log Activity** or **Network Activity** tabs. The subquery is available in the following formats:

- SELECT *<field/s>* FROM (*<AQL query expression>*)

  This query uses the FROM clause to search the output (cursor) of the subquery.
- SELECT *<field/s>* FROM events WHERE *<field>* IN (*<AQL query expression>*)

  This query uses the IN clause to specify the subquery results that match values from the subquery search. This subquery returns only one column. You can specify the results limit but the maximum is 10,000 results.

Subquery examples

The nested SELECT statement in parentheses is the subquery. The subquery is run first and it provides the data that is used by the main query. The main query SELECT statement retrieves the user names from the output (cursor) of the subquery.

Note: Works with API only

```
SELECT username FROM
(SELECT * FROM events
WHERE username IS NOT NULL
LAST 60 MINUTES)
```

The following query returns records where the user name from the Ariel database matches values in the subquery.

```
SELECT * FROM events
WHERE username IN
(SELECT username FROM events
LIMIT 10 LAST 5 MINUTES) LAST 24 HOURS
```

The following query returns records where the source IP address from the Ariel database matches the destination IP address in the subquery.

```
SELECT * FROM EVENTS
WHERE sourceip IN
(SELECT destinationip FROM events)
```

The following query returns records where the source IP address from the Ariel database matches the source IP addresses that are returned in the subquery. The subquery filters the data for the main select statement by locating internal hosts that interacted with high-risk entities. The query returns hosts that communicated with any hosts that interacted with high-risk entities.

```
SELECT sourceip AS 'Risky Hosts' FROM events
WHERE destinationip IN (SELECT sourceip FROM events
WHERE eventdirection = 'L2R'
AND REFERENCESETCONTAINS('CriticalWatchList', destinationip)
GROUP BY sourceip)
GROUP BY sourceip last 24 hours
```

Conditional logic in AQL queries

Use conditional logic in AQL queries by using IF and CASE expressions.

Use conditional logic in your AQL queries to provide alternative options, depending on whether the clause condition evaluates to true or false.

CASE Statements

CASE expressions return a Boolean true or false result. When an expression is returned as true, the value of that CASE expression is returned and processing is stopped. If the Boolean result is false, then the value of the ELSE clause is returned.

In the following example, when the user name is root, the value of the CASE expression that is returned is `Admin root`. When the user name is admin, the value of the CASE expression that is returned is `Admin user`. If the CASE expressions return a Boolean false, the value of the ELSE clause is returned.

```
SELECT CASE username
WHEN 'root'
THEN 'Admin root'
WHEN 'admin'
THEN 'Admin user'
ELSE 'other' END FROM events
```

When the WHEN statement is true, the THEN statement is processed, otherwise processing finishes.

IF, THEN, ELSE statements

Statements between THEN and ELSE are processed when the IF statement is true.

In this example, when the IF condition is true, `'ADMIN'` is returned when the user name is `'root'`, otherwise the user name is returned from the events log.

```
SELECT sourceip,
IF username = 'root'
THEN 'ADMIN'
ELSE username AS user FROM events
```

In the following example, if the log has no user name, then get it from the asset model. Otherwise, the user name is returned from the events log.

```
SELECT sourceip,
IF username IS NULL
THEN ASSETUSER(sourceip)
ELSE username AS username FROM events
GROUP BY username
LAST 2 DAYS
```

CIDR IP addresses in AQL queries

You can insert CIDR IP addresses in your AQL statements to query by IP address range, source IP, destination IP, or you can exclude specific CIDR IP addresses.

Examples of CIDR IP addresses in AQL queries

Query by source CIDR IP address, or by destination CIDR IP address.

```
SELECT * FROM flows
WHERE INCIDR('10.100.100.0/24',sourceip)
```

```
SELECT * FROM flows
WHERE INCIDR('10.100.100.0/24',destinationip)
```

Query for flows that have a source or destination CIDR IP address of 10.100.100.0/24

```
SELECT * FROM flows
WHERE INCIDR('10.100.100.0/24',sourceip)
OR INCIDR('10.100.100.0/24',destinationip)
```

Query for events where 192.168.222.0/24 is not the source CIDR IP address.

```
SELECT *
FROM events
WHERE NOT INCIDR('192.168.222.0/24',sourceip)
```

Query for flows where 192.168.222.0/24 is not the destination CIDR IP address.

```
SELECT *
FROM flows
WHERE NOT INCIDR('192.168.222.0/24',destinationip)
```

Custom properties in AQL queries

You can call a custom property directly in your AQL statements. If the custom property contains spaces you must use double quotation marks to encapsulate the custom property.

You must enable a custom property before you can use it in an AQL statement.

If the custom property is not enabled, you will be able to run your AQL query but you will not get results.

Custom property example

```
SELECT Bluecoat-cs-host, sourceip, Bluecoat-cs-uri
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist)
ILIKE '%Proxies%'
AND Bluecoat-cs-host ILIKE '%facebook.com%'
GROUP BY sourceip
```

`Bluecoat-cs-host` is the host name from the client's URL that is requested.

`Bluecoat-cs-uri` is the original URL that is requested.

System performance query examples

You can use or edit examples of system performance AQL queries to run in your network.

Use the following query examples to get information about system performance in your network or edit these examples to build your own custom queries.

Disk Utilization and CPU usage

```
SELECT Hostname, "Metric ID", AVG(Value)
AS Avg_Value, Element
FROM events
WHERE LOGSOURCENAME(logsourceid)
ILIKE '%%health%%'
AND
"Metric ID"='SystemCPU'
OR
"Metric ID"='DiskUtilizationDevice'
GROUP BY Hostname, "Metric ID", Element
ORDER BY Hostname last 20 minutes
```

This query outputs the **Hostname**, **MetricID**, **Avg_Value**, and **Element** columns.

The **Avg_Value** column returns an average value for CPU usage and disk utilization.

Disk Utilization by partition

```
SELECT Hostname, AVG(Value) AS Disk_Usage, Element
FROM events
where LOGSOURCENAME(logsourceid)
ILIKE '%%health%%'
and "Metric ID"='DiskUsage'
GROUP BY Hostname, Element
ORDER BY Hostname
LAST 2 HOURS
```

This query outputs the **Hostname**, **Disk_Usage**, and **Element** columns

The **Disk_Usage** column returns a value for disk usage for the directories that are listed in the **Element** column.

Disk usage in gigabytes (GB) per partition

```
SELECT element
AS Partiton_Name,
MAX(value/(1024*1024*1024))
AS 'Gigabytes_Used'
FROM events
WHERE "Metric ID"='DiskSpaceUsed'
GROUP BY element
ORDER BY Gigabytes_Used DESC
LAST 2 DAYS
```

This query outputs the **Partition_Name** and the **Gigabytes_Used** columns from the events database.

The **Gigabytes_Used** column returns a value for the gigabytes that are used by each partition that is listed in the **Gigabytes_Used** column for the last two days.

Copying query examples from the AQL guide

If you copy and paste a query example that contains single or double quotation marks from the AQL Guide, you must retype the quotation marks to be sure that the query parses.

Events and flows query examples

Use or edit query examples to create events and flows queries that you can use for your AQL searches.

Use the following query examples to get information about events and flows in your network or edit these examples to build your own custom queries.

Event rates and flow rates for specific hosts

```
SELECT AVG(Value), "Metric ID", Hostname
FROM events
WHERE LOGSOURCENAME(logsourceid)
ILIKE '%%health%%'
AND ("Metric ID"='FlowRate' OR "Metric ID"='EventRate')
GROUP BY "Metric ID", Hostname
LAST 15 minutes
```

This query outputs the **AVG_Value**, **Metric ID**, and **Hostname** columns from the events or flows database for the last 15 minutes.

The **AVG_Value** column returns a value for the average flow or event rate over the last 15 minutes for the host that is named in the **Hostname** column.

EPS rates by log source

```
SELECT logsourcename(logsourceid)
AS 'MY Log Sources',
SUM(eventcount) / (( MAX(endTime) -MIN(startTime)) / 1000 )
AS EPS_Rates
FROM events
GROUP BY logsourceid
ORDER BY EPS_Rates DESC
LAST 2 HOURS
```

This query outputs **My Log Sources**, and **EPS_Rates** columns from events.

The **My Log Sources** column returns log source names and the **EPS_Rates** column returns the EPS rates for each log source in the last two hours.

Event counts and event types per day

```
SELECT
DATEFORMAT( devicetime, 'dd-MM-yyyy')
AS 'Date of log source',
QIDDESCRIPTION(qid)
AS 'Description of event', COUNT(*)
FROM events
WHERE devicetime >( now() -(7*24*3600*1000) )
GROUP BY "Date of log source", qid
LAST 4 DAYS
```

This query outputs the **Date of log source**, **Description of event**, and **count** of event columns from events.

The date of the event, description of event, and count of events are returned for the last four days.

Monitoring local to remote flow traffic by network

```
SELECT sourceip,
LONG(SUM(sourcebytes+destinationbytes))
AS TotalBytes
FROM flows
WHERE flowdirection= 'L2R'
AND NETWORKNAME(sourceip)
ILIKE 'servers'
GROUP BY sourceip
ORDER BY TotalBytes
```

This query outputs the **sourceip** and **TotalBytes** columns.

The **TotalBytes** column returns the sum of the source and destination bytes that crosses from local to remote.

Monitoring remote to local flow traffic by network

```
SELECT sourceip,
LONG(SUM(sourcebytes+destinationbytes))
AS TotalBytes
FROM flows
WHERE flowdirection= 'R2L'
```

```
AND NETWORKNAME(sourceip)
ILIKE 'servers'
GROUP BY sourceip
ORDER BY TotalBytes
```

This query outputs the **sourceip** and **TotalBytes** columns.

The **TotalBytes** column returns the sum of the source and destination bytes from remote to local.

Copying query examples from the AQL guide

If you copy and paste a query example that contains single or double quotation marks from the AQL Guide, you must retype the quotation marks to be sure that the query parses.

Reference data query examples

Use AQL queries to get data from reference sets, reference maps, or reference tables. You can create and populate reference data by using rules to populate reference sets, by using external threat feeds, for example, LDAP Threat Intelligence App, or by using imported data files for your reference set.

Use the following examples to help you create queries to extract data from your reference data.

Use reference tables to get external metadata for user names that show up in events

```
SELECT
REFERENCETABLE('user_data','FullName',username) AS 'Full Name',
REFERENCETABLE('user_data','Location',username) AS 'Location',
REFERENCETABLE('user_data','Manager',username) AS 'Manager',
UNIQUECOUNT(username) AS 'Userid Count',
UNIQUECOUNT(sourceip) AS 'Source IP Count',
COUNT(*) AS 'Event Count'
FROM events
WHERE qidname(qid)ILIKE '%logon%'
GROUP BY "Full Name", "Location", "Manager"
LAST 1 days
```

Use the reference table to get external data such as the full name, location, and manager name for users who logged in to the network in the last 24 hours.

Get the global user IDs for users in events who are flagged for suspicious activity

```
SELECT
REFERENCEMAP('GlobalID_Mapping',username) AS 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') AS 'Full Name',
UNIQUECOUNT(username),
COUNT(*) AS 'Event count'
FROM events
WHERE RULENAME(creEventlist)
ILIKE '%suspicious%'
GROUP BY "Global ID"
LAST 2 days
```

In this example, individual users have multiple accounts across the network. The organization requires a single view of a user's activity. Use reference data to map local user IDs to a global ID. The query returns the user accounts that are used by

a global ID for events that are flagged as suspicious.

Use a reference map lookup to extract global user names for user names that are returned in events

```
SELECT
QIDNAME(qid) as 'Event name',
starttime AS Time,
sourceip AS 'Source IP',
destinationip AS 'Destination IP',
username AS 'Event Username',
REFERENCEMAP('GlobalID_Mapping', username) AS 'Global User'
FROM events
WHERE "Global User" = 'John Ariel'
LAST 1 days
```

Use the reference map to look up the global user names for user names that are returned in events. Use the WHERE clause to return only events for the global user John Ariel. John Ariel might have a few different user names but these user names are mapped to a global user, for example, in an external identity mapping system, you can map a global user to several user names used by the same global user.

Monitoring high network utilization by users

```
SELECT
LONG(REFERENCETABLE('PeerGroupStats', 'average',
REFERENCEMAP('PeerGroup',username)))
AS PGave,
LONG(REFERENCETABLE('PeerGroupStats', 'stdev',
REFERENCEMAP('PeerGroup',username)))
AS PGstd,
SUM(sourcebytes+destinationbytes) AS UserTotal
FROM flows
WHERE flowtype = 'L2R'
GROUP BY UserTotal
HAVING UserTotal > (PGAve+ 3*PGStd)
```

Returns user names where the flow utilization is three times greater than the average user.

You need a reference set to store network utilization of peers by user name and total bytes.

Threat ratings and categories

```
SELECT
REFERENCETABLE('ip_threat_data','Category',destinationip)
AS 'Threat Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip)
AS 'Threat Rating',
UNIQUECOUNT(sourceip)
AS 'Source IP Count',
UNIQUECOUNT(destinationip)
AS 'Destination IP Count'
FROM events
GROUP BY "Threat Category", "Threat Rating" LAST 24 HOURS
```

Returns the threat category and the threat rating.

You can look up reference table threat data and include it in your searches.

Copying query examples from the AQL guide

If you copy and paste a query example that contains single or double quotation marks from the AQL Guide, you must retype the quotation marks to be sure that the query parses.

User and network monitoring query examples

Use query examples to help you create your user and network monitoring query AQL queries.

Use the following examples to monitor your users and network, or you can edit the queries to suit your requirements.

Find users who used the VPN to access the network from three or more IP addresses in a 24-hour period

```
SELECT username,
UNIQUECOUNT(sourceip)
AS 'Source IP count'
FROM events
WHERE LOGSOURCENAME(logsourceid)
ILIKE '%VPN%'
AND username IS NOT NULL
GROUP BY username
HAVING "Source IP count" >= 3
ORDER BY "Source IP count"
DESC
LAST 24 HOURS
```

This query outputs the **username** and **Source IP count** columns.

The **username** column returns the names of users who used the VPN to access the network from three or more IP addresses in the last 24 hours.

Find users who used the VPN from more that one geographic location in 24 hours

```
SELECT username, UNIQUECOUNT(geographiclocation)
AS 'Count of locations'
FROM events
WHERE LOGSOURCENAME(logsourceid)
ILIKE '%VPN%'
AND geographiclocation <> 'other location'
AND username
IS NOT NULL
GROUP BY username
HAVING "Count of locations" > 1
ORDER BY "Count of locations"
DESC
LAST 3 DAYS
```

This query outputs the **username** and **Count of locations** columns.

The **username** column returns the names of users who used the VPN from more than one location that is not called 'other location' in the last 24 hours.

Monitoring local to remote flow traffic by network

```
SELECT sourceip,
LONG(SUM(sourcebytes+destinationbytes))
AS TotalBytes
FROM flows
```

```
WHERE flowdirection= 'L2R'
AND NETWORKNAME(sourceip)
ILIKE 'servers'
GROUP BY sourceip
ORDER BY TotalBytes
```

This query outputs the **sourceip** and **TotalBytes** columns.

The **TotalBytes** column returns the sum of the source and destination bytes that crosses from local to remote.

Monitoring remote to local flow traffic by network

```
SELECT sourceip,
LONG(SUM(sourcebytes+destinationbytes))
AS TotalBytes
FROM flows
WHERE flowdirection= 'R2L'
AND NETWORKNAME(sourceip)
ILIKE 'servers'
GROUP BY sourceip
ORDER BY TotalBytes
```

This query outputs the **sourceip** and **TotalBytes** columns.

The **TotalBytes** column returns the sum of the source and destination bytes from remote to local.

Application usage by application name, users, and flows traffic

```
SELECT sourceip
AS Source_IP,
FIRST(destinationip)
AS Destination_IP,
APPLICATIONNAME(applicationid)
AS Application,
DATEFORMAT(lastpackettime, 'dd-MM-yyyy hh:m:ss')
AS 'Start Time',
FIRST(sourcebytes)
AS Source_Bytes,
ASSETUSER(sourceip, NOW()) AS Src_Asset_User
FROM flows
GROUP BY Source_IP
ORDER BY Source_Bytes DESC
```

This query outputs data about your asset users, application names, and flow data. Use this query to report specific user activity or application usage, or to build a variation of this query to achieve your desired results.

Location of assets

```
SELECT ASSETPROPERTY('Location',sourceip)
AS asset_location,
COUNT(*)
FROM events
GROUP BY asset_location
LAST 1 days
```

This query outputs the **asset_location** and **count** columns.

The **asset location** column returns the location of the assets.

Copying query examples from the AQL guide

If you copy and paste a query example that contains single or double quotation marks from the AQL Guide, you must retype the quotation marks to be sure that the query parses.

Event, flow, and simarc fields for AQL queries

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Supported event fields for AQL queries

The event fields that you can query are listed in the following table.

Table 7. Supported event fields for AQL queries

Field name	Description
adekey	Ade key
adevalue	Ade value
category	Low-level category
creEventList	Matched custom rule
credibility	Credibility
destinationMAC	Destination MAC
destinationPort	Destination port
destinationv6	IPv6 destination
destinationaddress	Destination address
destinationip	Destination IP
sourceaddress	Source address
deviceTime	Log source time
deviceType	Log source type
devicegrouplist	Device group list
domainID	Domain ID
duration	Duration
endTime	End time
eventCount	Event count
eventDirection	Event direction: **local-to-Local (L2L)** **local-to-remote (L2R)** **remote-to-local (R2L)** **remote-to-remote (R2R)**
geographiclocation	geographic location
sourcegeographiclocation	Source geographic location
destinationgeographiclocation	Destination geographic location
hasIdentity	Has identity
hasOffense	Associated with offense

Table 7. Supported event fields for AQL queries (continued)

Field name	Description
highLevelCategory	High-level category
identityhostname	Identity host name
identityip	Identity IP address
isduplicate	Is duplicate
isCREEvent	Is custom rule event
logsourceid	Log source ID
magnitude	Magnitude
pcappacket	PCAP packet
partialMatchList	Partial match list
payload	Payload
postNatDestinationIP	Destination IP after NAT
postNatDestinationPort	Destination port after NAT
postNatSourceIP	Source IP after NAT
postNatSourcePort	Source port after NAT
preNatDestinationIP	Destination IP before NAT
preNatDestinationPort	Destination port before NAT
preNatSourceIP	Source IP before NAT
preNatSourcePort	Source port before NAT
protocolid	Protocol
processorId	Event Processor ID
qid	Event name ID
relevance	Relevance
severity	Severity
sourceIP	Source IP
sourceMAC	Source MAC
sourcePort	Source port
sourcev6	IPv6 source
startTime	Start time
isunparsed	Event is unparsed
userName	User name

Supported flow fields for AQL queries

The flow fields that you can query are listed in the following table.

Table 8. Supported flow fields for AQL queries

Field name	Description
applicationId	Application ID
category	Category
credibility	Credibility
destinationASN	Destination ASN

Table 8. Supported flow fields for AQL queries (continued)

Field name	Description
destinationBytes	Destination bytes
destinationDSCP	Destination DSCP
destinationFlags	Destination flags
destinationIP	Destination IP
destinationIfIndex	Destination if index
destinationPackets	Destination packets
destinationPayload	Destination payload
destinationPort	Destination port
destinationPrecedence	Destination precedence
destinationv6	IPv6 destination
domainID	Domain ID
fullMatchList	Full match list
firstPacketTime	First packet time
flowBias	Flow bias
flowDirection	Flow direction **local-to-local (L2L)** **local-to-remote (L2R)** **remote-to-local (R2L)** **remote-to-remote (R2R)**
flowInterfaceID	Flow interface ID
flowSource	Flow Source
flowType	Flow type
geographic	Matches geographic location
hasDestinationPayload	Has destination payload
hasOffense	Has offense payload
hasSourcePayload	Has source payload
icmpCode	Icmp code
icmpType	ICMP type or code
flowInterface	Flow interface
intervalId	Interval ID
isDuplicate	Duplicate event
lastPacketTime	Last packet time
partialMatchList	Partial match list
protocolId	Protocol ID
qid	Qid
processorID	Event processor ID
relevance	Relevance
retentionBucket	Retention bucket dummy
severity	Severity

Table 8. Supported flow fields for AQL queries (continued)

Field name	Description
sourceASN	Source ASN
sourceBytes	Source bytes
sourceDSCP	Source DSCP
sourceFlags	Source flags
sourceIP	Source IP
sourceIfIndex	Source if index
sourcePackets	Source packets
sourcePayload	Source payload
sourcePort	Source port
sourcePrecedence	Source precedence
sourcev6	IPv6 source
startTime	Start time
viewObjectPair	View object pair

Supported simarc fields for AQL queries

The simarc fields that you can query are listed in the following table.

Table 9. Supported simarc fields for AQL queries

Field name	Description
destinationPort	Destination port key creator
destinationType	Destination type key creator
deviceId	Device key creator
direction	Direction key creator
eventCount	Event count key creator
eventFlag	Flag key creator
applicationId	Application ID key creator
flowCount	Flow count key creator
destinationBytes	Destination bytes key creator
flowSource	Flow source key creator
sourceBytes	Source bytes key creator
lastPacketTime	Time key creator
protocolId	Protocol key creator
source	Source key creator
sourceType	Source type key creator
sourceRemoteNetwork	Source remote network key creator
destinationRemoteNetwork	Destination remote network key creator
sourceCountry	Source geographic key creator
destinationCountry	Destination geographic key creator
destination	Destination key creator

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

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

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Index

A
AQL 3
Ariel Query Language 3

C
contact information v
COUNT function 15
customer support v

D
description v
documentation v

E
events and flows 48

F
field list 48
functions
  Date and time format 37
  fields 3

G
GROUP BY 11

H
HAVING 12

L
LIKE clause 14

N
network administrator v
new features
  version 7.2.8 users 1

O
ORDER BY clause 13

S
SELECT clause 9
Start and Stop clauses 34

T
technical library v

W
what's new
  version 7.2.8 users 1
WHERE clause 10

Printed in USA