ES|QL Cheat Sheet

elastic

Binary Operators				Logical Operators	Basic Functions	
Equality	==	Add	+	AND	DROP	LIMIT
Inequality	!=	Subtract	-	OR	IN	RENAME
Less than	<	Multiply	*	NOT	CIDR_MATCH	RLIKE
Less than or equal to	<=	Divide	/		KEEP	SORT
Greater than	>	Modulus	%	**NULL Handling**	LIKE	WHERE
Greater than or equal to	>=			IS NULL		
				IS NOT NULL		

Processing Commands	
Function	**Syntax**
EVAL	`EVAL [column1 =] value1[, ..., [columnN =] valueN]`
STATS...BY	`STATS [column1 =] expression1[,... [columnN =] expression] [BY grouping_expression1[,..., grouping_expresionN]`

STATS...BY GROUPING Functions		
Function	**Syntax**	
BUCKET	`BUCKET(expression, buckets, from, to)`	

STATS...BY Aggregate Functions			
Function	**Syntax**	**Function**	**Syntax**
AVG	AVG(expression)	MIN	MIN(expression)
COUNT	COUNT([expression])	PERCENTILE	PERCENTILE(expression, percentile)
COUNT_DISTINCT	COUNT_DISTINCT(expression[, precision_threshold])	SUM	SUM(expression)
MAX	MAX(expression)	TOP	TOP(field, limit, order)
MEDIAN	MEDIAN(expression)	WEIGHTED_AVG	WEIGHTED_AVG(expression_weight)
MEDIAN_ABSOLUTE_DEVIATION	MEDIAN_ABSOLUTE_DEVIATION(expression)		

String Functions			
Function	**Syntax**	**Function**	**Syntax**
CONCAT	CONCAT(string1, string2[, …, stringN])	RIGHT	RIGHT(string, length)
ENDS_WITH	ENDS_WITH (string_field, prefix)	RTRIM	RTRIM(string)
FROM_BASE64	FROM_BASE64(string)	SPLIT	SPLIT(string, delim)
LEFT	LEFT(str, length)	STARTS_WITH	STARTS_WITH (string_field, prefix)
LENGTH	LENGTH(str)	SUBSTRING	SUBSTRING(string, start, length)
LTRIM	LTRIM(string)	TO_BASE64	TO_BASE64(string)
LOCATE	LOCATE(string, substring, start)	TO_LOWER	TO_LOWER(string)
REPEAT	REPEAT(string, number)	TO_UPPER	TO_UPPER(string)
REPLACE	REPLACE(str, regex, newStr)	TRIM	TRIM(string)

Date-Time Functions			
Function	**Syntax**	**Function**	**Syntax**
DATE_DIFF	DATE_DIFF(unit, startTimestamp, endTimestamp)	DATE_PARSE	datePattern, dateString)
DATE_EXTRACT	DATE_EXTRACT(datePart, date)	DATE_TRUNC	DATE_TRUNC(interval, date)
DATE_FORMAT	DATE_FORMAT(dateFormat, date)	NOW	NOW()

IP Functions			
Function	**Syntax**	**Function**	**Syntax**
CIDR_MATCH	CIDR_MATCH(ip, blockX)	IP_PREFIX	IP_PREFIX(ip, prefixLengthV4, prefixLengthV6)

Type Conversion Functions					
Function	**Syntax**	**Function**	**Syntax**	**Function**	**Syntax**
TO_BOOLEAN	TO_BOOLEAN(field)	TO_DOUBLE	TO_DOUBLE(field)	TO_LONG	TO_LONG(field)
TO_CARTESIANPOINT	TO_CARTESIANPOINT(field)	TO_GEOPOINT	TO_GEOPOINT(field)	TO_RADIANS	TO_RADIANS(number)
TO_CARTESIANSHAPE	TO_CARTESIANSHAPE(field)	TO_GEOSHAPE	TO_GEOSHAPE(field)	TO_STRING	TO_STRING(field)
TO_DATETIME	TO_DATETIME(field)	TO_INTEGER	TO_INTEGER(field)	TO_UNSIGNED_LONG	TO_UNSIGNED_LONG(field)
TO_DEGREES	TO_DEGREES(number)	TO_IP	TO_IP(field)	TO_VERSION	TO_VERSION(field)

Multi Value Functions					
Function	**Syntax**	**Function**	**Syntax**	**Function**	**Syntax**
MV_APPEND	MV_APPEND(field1, field2)	MV_FIRST	MV_FIRST(field)	MV_SLICE	MV_SLICE(field, start,end)
MV_AVG	MV_AVG(number)	MV_LAST	MV_LAST(field)	MV_SORT	MV_SORT(field, order)
MV_CONCAT	MV_CONCAT(string, delim)	MV_MAX	MV_MAX(field)	MV_SUM	MV_SUM(number)
MV_COUNT	MV_COUNT(field)	MV_MEDIAN	MV_MEDIAN(field)	MV_ZIP	MV_ZIP(string1, string2, delim)
MV_DEDUPE	MV_DEDUPE(field)	MV_MIN	MV_MIN(field)		

Mathematical Functions							
Function	**Syntax**	**Function**	**Syntax**	**Function**	**Syntax**	**Function**	**Syntax**
ABS	ABS(N)	CEIL	CEIL(N)	LOG10	LOG10(N)	SINH	SINH(N)
ACOS	ACOS(N)	COS	COS(N)	PI	PI()	SQRT	SQRT(N)
ASIN	ASIN(N)	COSH	COSH(N)	POW	POW(BASE, EXPONENT)	TAN	TAN(N)
ATAN	ATAN(N)	E	E()	ROUND	ROUND(VALUE, DECIMALS)	TANH	TANH(N)
ATAN2	ATAN2(Y,X)	FLOOR	FLOOR(N)	SIGNUM	SIGNUM(N)	TAU	TAU()
CBRT	CBRT(N)	LOG	LOG([BASE], VALUE)	SIN	SIN(N)		

Conditional Functions			
Function	**Syntax**	**Function**	**Syntax**
CASE	`CASE(condition, true_value, else_value)`	GREATEST	`GREATEST(first, rest)`
COALESCE	`COALESCE(first, rest)`	LEAST	`LEAST(first, rest)`

Enrich Function	
Function	**Syntax**
ENRICH	`ENRICH enrich_policy`
	`ENRICH enrich_policy on field_name`
	`ENRICH enrich_policy on field_name WITH field1, field2`