Infoblox
NEXT LEVEL NETWORKING

Quick Start Guide

ATC DNS Response Logs File Conversation Tool

TABLE OF CONTENTS

Introduction

This tool converts one or many parquet files to different supported formats(json or csv or cef). It is currently executed as a Java application from a jar file. This document explains how to get started.

Prerequisites

- Java JDK 8 or later

Converted Output Formats

- JSON
- CSV
- CEF

Using the Tool

Operations available

-f	Output format type to convert files into. Supported options: json, csv or cef.
-i	Input file path/director
-o	Output file path/directory

Options

- Convert single parquet file to another supported format file.
- Convert a directory of files to another supported format file.

Examples

1. Converting a directory of parquet files to JSON format:

```
Java -jar parquet_tool-1.0-uber.jar -f json -i /Users/demo/Parquet -o /Users/demo/JSON
```

2. Converting a single parquet file to JSON format:

```
Java -jar parquet_tool-1.0-uber.jar -f json -i /Users/demo/Parquet/file.parquet -o /Users/demo/JSON/file.json
```

3. Converting a directory of parquet files to CEF format:

```
Java -jar parquet_tool-1.0-uber.jar -f cef -i /Users/demo/Parquet -o /Users/demo/CEF
```

4. Converting a single parquet file to CEF format:

```
Java -jar parquet_tool-1.0-uber.jar -f cef -i /Users/demo/Parquet/file.parquet -o /Users/demo/CEF/file.cef
```

5. Converting a directory of parquet files to CSV format:

```
Java -jar parquet_tool-1.0-uber.jar -f csv -i /Users/demo/Parquet -o /Users/demo/CSV
```

6. Converting a single parquet file to CSV format:

```
Java -jar parquet_tool-1.0-uber.jar -f csv -i /Users/demo/Parquet/file.parquet -o /Users/demo/CSV/file.csv
```

JSON Output Example

```
[
    {
        "opcode": 0,
        "timestamp": 1542993678,
        "qname": "www.google.com.",
        "qtype": 1,
        "qclass": 1,
        "source": "fe84a5e4facaee2a9c360ac48d597e15",
        "qip": "223.38.30.241",
        "qport": 38187,
        "rip": "",
        "rport": -1,
        "protocol": 6,
        "delay": -1,
        "rcode": 0,
        "type": 4,
        "qqr": false,
        "qaa": false,
        "qtc": false,
        "qrd": false,
        "qra": false,
        "qad": false,
        "qcd": false,
        "qdo": false,
        "rqr": true,
        "raa": false,
        "rtc": false,
        "rrd": true,
        "rra": true,
        "rad": false,
        "rcd": false,
        "rdo": false,
        "qrr1": null,
        "qrr2": null,
        "qrr3": null,
        "rrr1": [
            {
                "name": "www.google.com.",
                "ttl": 29,
                "type": 1,
                "clas": 1,
                "data": "172.217.22.4"
            }
        ],
        "rrr2": [],
        "rrr3": [
            {
                "name": ".",
                "ttl": 0,
                "type": 41,
                "clas": 4096,
                "data": ""
            }
        ],
        "view": "6",
        "anonymized": false,
        "nanosec": 498619001,
        "pid": "67129",
        "cid": "df8e87fc2995232cf106a3a9867e1ca8:ff52ffcc9a820d69b5bc05a62b5b8963",
        "tid": ""
    }
```

Refer to Fields Map Table to know what each field represents.

CEF Output Example

CEF is a message format. If you specify to receive your data output in CEF, every event is encoded as a line of CEF.

```
CEF:0|Infoblox|ATC|2.0||DnsEvent|10|InfobloxAtcOpcode=0 InfobloxAtcTimestamp=1486170973
InfobloxAtcQname=tjtekyrkytryhrjtrjdkigasdj.xyz. InfobloxAtcQtype=1 InfobloxAtcQclass=1
InfobloxAtcSource= InfobloxAtcQip=172.23.18.138 InfobloxAtcQport=39295 InfobloxAtcRip=
InfobloxAtcRport=-1 InfobloxAtcProtocol=17 InfobloxAtcDelay=-1.0 InfobloxAtcRcode=3
InfobloxAtcType=1 InfobloxAtcQqr=false InfobloxAtcQaa=false
```

The CEF data output includes the following header:

CEF:<Version>|<Device Vendor>|<Device Product>|<Device Version>|<Signature ID>|<Name>|<Severity>|<Extension>

The following table describes the header fields:

CEF Prefix Field	Description	Value
Version	Integer defining the CEF version. used to determine what the following fields.	“0”
Device Vendor	Strings uniquely identifying the type of device sending the information.	“Infoblox”
Device Product		“ATC”
Device Version		“2.0”
Signature ID	Unique identifier per event-type	SHA2 digest of CEF log line (with an empty Signature ID field)
Name	Human readable description of the event.	“DnsEvent” or “RpzEvent” or “IPMetaEvent”
Severity	Importance of the event. From 10 – 0 where 10 is most important.	Uses severity value from the ATC database. Default value is 10.
Extension	A collection of key-value pairs. An event can contain any number of key value pairs in any order, separated by spaces.	See the Fields Map Table below for more details.

CSV Output example

Example:

```
0,1486170973,tjtekyrkytryhrjtrjdkigasdj.xyz.,1,1,,172.23.18.138,39295,,-1,17,-
1.0,3,1,false,false,false,false,false,false,false,false,true,true,false,true,true,false,false,false,,,,
[],[],[{"name": "."| "ttl": 32768| "type": 41| "clas": 4096| "data":
""}],,false,151112000,33686018,c34c5029ee336d4ba7cec6cf44f9056a:d3eaf394bf43fa644f0b96e6b50fe
3f6,
```

The format is in the following order:

```
opcode, timestamp, qname, qtype, qclass, source, qip, qport,  rip, rport,  protocol, delay, rcode, type, qqr,
qaa, qtc, qrd, qra, qad, qcd, qdo, rqr, raa, rtc, rrd, rra, rad, rcd, rdo, qrr1, qrr2, qrr3, rrr1, rrr2, rrr3, view,
anonymized, nanosec, pid, cid, tid
```

Refer to Fields Map Table to know what each field represents.

Fields Map Table

The following tables describes the data fields (if they exist) that can appear in the output file:

DNS Output Fields

Field Name	CEF Field Name	Notes
opcode	InfobloxAtcOpcode	opcode for NOTIFY, STATUS, QUERY, UPDATE
timestamp	InfobloxAtcTimestamp	Timestamp in Unix format
qname	InfobloxAtcQname	DNS query name in FQDN
qtype	InfobloxAtcQtype	DNS query type
qclass	InfobloxAtcQclass	DNS query class
source	InfobloxAtcSource	data source or DNS server ID
qip	InfobloxAtcQip	requester IP
qport	InfobloxAtcQport	requester port
rip	InfobloxAtcRip	responder IP
rport	InfobloxAtcRport	responder port
protocol	InfobloxAtcProtocol	DNS protocol for TCP or UDP
delay	InfobloxAtcDelay	delay in response

rcode	InfobloxAtcRcode	return code
type	InfobloxAtcType	message type by ISC 0: UDP_INVALID 1: UDP_QUERY_RESPONSE 2: UDP_UNANSWERED_QUERY 3: UDP_UNSOLICITED_RESPONSE 4: TCP 5: ICMP 6: UDP_QUERY_ONLY 7: UDP_RESPONSE_ONLY
qqr qaa qtc qrd qra qad qcd qdo	InfobloxAtcQqr InfobloxAtcQqa InfobloxAtcQtc InfobloxAtcQrd InfobloxAtcQra InfobloxAtcQad InfobloxAtcQcd InfobloxAtcQdo	Query flags from DNS packet header:
rqr raa rtc rrd rra rad rcd rdo	InfobloxAtcRqr InfobloxAtcRaa InfobloxAtcRtc InfobloxAtcRrd InfobloxAtcRra InfobloxAtcRad InfobloxAtcRcd InfobloxAtcRdo	Response flags from DNS packet header:
qrr1 qrr2 qrr3	InfobloxAtcQrr1 InfobloxAtcQrr2 InfobloxAtcQrr3	Query resource record list qrr1 : Array of [FQDN, TTL, RRType, RRclass, RRdata] qrr2 : Array of ResourceRecords qrr3 : Array of ResourceRecords
rrr1 rrr2 rrr3	InfobloxAtcRrr1 InfobloxAtcRrr2 InfobloxAtcRrr3	Response resource record list will be in the form of Array of ResourceRecords
view	InfobloxAtcView	DNS view
anonymized	InfobloxAtcAnonymized	Anonymized flag
nanosec	InfobloxAtcNanosec	timestamp in nano second part
pid	InfobloxAtcPid	Policy Identifier
cid	InfobloxAtcCid	Client Identifier
tid	InfobloxAtcTid	Transaction Identifier

RPZ Output Fields

Field Name	CEF Field Name	Notes
opcode	InfobloxAtcOpcode	opcode for NOTIFY, STATUS, QUERY, UPDATE
timestamp	InfobloxAtcTimestamp	Seconds part of timestamp
nanosec	InfobloxAtcNanosec	Nanoseconds part of timestamp
tcode	InfobloxAtcTcode	RPZ Trigger code 0: QNAME Trigger on query name 1: CLIENT-IP Trigger on DNS client IP 2: IP Trigger on query response IP 3: NSDNAME Trigger on NS name during delegation 4: NS-IP Trigger on NS IP during delegation
tname	InfobloxAtcTname	FQDN for RPZ trigger (feedname.rpz_entry)
acode	InfobloxAtcAcode	RPZ Action code (adapted from ZyTrax) 0: Local-Data Response data defined by RR and target name 1: NODATA Return name exists but with no answer data 2: PASSTHRU Do nothing - normally defines an exception in a range 3: NXDOMAIN Return name does not exist 4: TCP-Only Force use of TCP (REDIRECT for policy engine) 5: REFUSED Support for JANUS 6: DROP Causes client timeout
arrtype	InfobloxAtcArrtype	RPZ Action RR type
arrdata	InfobloxAtcArrdata	RPZ Action RR data
qname	InfobloxAtcQname	DNS query name in FQDN
qtype	InfobloxAtcQtype	DNS query name in FQDN
qclass	InfobloxAtcQclass	DNS query class
source	InfobloxAtcSource	data source or DNS server ID
qip	InfobloxAtcQip	requester IP
qport	InfobloxAtcQport	requester port
rip	InfobloxAtcRip	responder IP

rport	InfobloxAtcRport	responder port
view	InfobloxAtcView	DNS view (Infoblox feed or others. Optionally prefix with network view qualifier)
pvendor	InfobloxAtcPvendor	Product vendor
pname	InfobloxAtcPname	Product name
pversion	InfobloxAtcPversion	Product version
loglevel	InfobloxAtcLoglevel	Syslog severity level indicator
disabled	InfobloxAtcDisabled	Is RPZ rule disabled
tid	InfobloxAtcTid	Transaction Identifier of DNS response
pid	InfobloxAtcPid	Policy Identifier (optional)
cid	InfobloxAtcCid	Client Identifier (optional)
anonymized	InfobloxAtcAnonymized	Anonymized flag
cmac	InfobloxAtcCmac	Client MAC address (optional)
csite	InfobloxAtcCsite	Client Site ID (optional)
qcat	InfobloxAtcQcat	Content category (optional)
tinfo	InfobloxAtcTinfo	Trigger information: threat property, threat level, threat confidence (optional)

IPMeta Output Fields

Field Name	CEF Field Name	Notes
opcode	InfobloxAtcOpcode	opcode for INSERT=0, DELETE=1, UPDATE=2 (Required)
source	InfobloxAtcSource	Data source (identical to DNS schema attribute with same name)
timestamp	InfobloxAtcTimestamp	Seconds part of timestamp
nanosec	InfobloxAtcNanosec	Nanoseconds part of timestamp
cip	InfobloxAtcCip	Client IPv4 or IPv6 address
hostnames	InfobloxAtcHostnames	Client machine names or hostnames

usernames	InfobloxAtcUsernames	Client usernames associated with IP (from AD)
mac	InfobloxAtcMac	Client MAC address or hardware ID
view	InfobloxAtcView	Network view name containing DHCP lease
fingerprint	InfobloxAtcFingerprint	Description of Fingerprint from DHCP lease
os	InfobloxAtcOs	OS discovered
firstts	InfobloxAtcFirstts	Timestamp of first discovery
lastts	InfobloxAtcLastts	Timestamp of last discovery
extattrs	InfobloxAtcExtattrs	IPAM Extensible Attributes
anonymized	InfobloxAtcAnonymized	Anonymized flag

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com