

# CDNI Logging

## draft-ietf-cdni-logging-05

### (Update from -02)

François Le Faucheur – cisco

Gilles Bertrand - Orange

Iuniana Oprescu - Orange

Roy Peterkofsky – Skytide

IETF 87 Berlin 2013

# Changes between -02 and -05

- Significant work done on cdni-logging since Orlando
- Held three “informal” meetings to gather input and feedback
- Published -03, -04 and -05 (with incremental diffs)
- Many items discussed on the list along the way

# Changes between -02 and -05

- Introduced full ABNF notation and rules for specification of all Fields, Directives, File Format
- Restructured section 3 specifying the CDNI Logging File format, syntax and semantic
- Cleaned-up definition of all base format/rules (e.g. QSTRING, NHTABSTRING)
- Added directives:
  - Claimed-Origin
  - Verified-Origin

# Changes between -02 and -05

- Introduced new prefixes in the logging fields (u: uCDN, d: dCDN)
- Changed separator inside the “Fields” directive from “Space” to “Tab”
- Time is UTC (like in metadata-02)
- Changed Date & Time to be on processing completion instead of processing start
- Removed Non-Repudiation-Hash (TBD w/ a mechanism relying on Atom)
- Added anonymization mechanism on IP addresses inside logging records: (c-ip-anonimizing)
- Added text on anonymization in Privacy subsection of Security Considerations

# Changes between -02 and -05

- Introduced text for the “CDNI Logging Feed”
  - dCDN to advertise to uCDN the availability of CDNI Logging Files
  - Based on IETF Atom protocol [RFC4287], using the Archived format [RFC5005] (which allows to publish “new” info and keep archives of “old” info)
  - Discusses:
    - formatting
    - updates to logging files and to the Logging Feed
    - redundant feeds
- For memory, the CDNI Logging File pull mechanism is based on HTTP/HTTPS

# Changes between -02 and -05

- Populated the IANA section
  - Created three Registries
    - Directive Names
    - Record-Types
    - Field Names
  - Defined initial allocation with all values defined in cdni-logging
  - Defined policy for future allocation
    - Within the registry, names are to be allocated by IANA according to the "Specification Required" policy specified in [RFC5226]
    - In line with RFC 6648 (xdash-considered-harmful)
    - Allows easy extensibility
  - Requested allocation of a new MIME Type
    - "application/cdni.LoggingFile" used in CDNI Logging Feed

## Changes between -02 and -05

- Non-Repudiation mechanism expected to be moved into the CDNI Logging Feed – TBD
- Tweaking some figures and text

# CDNI Logging File Directives

- Version
- UUID
- Claimed-Origin
- Verified-Origin
- Record-Type
- Fields
- Integrity-Hash

```
+-----+
|CDNI Logging File
|
| #Directive 1
| #Directive 2
| ...
| #Directive P
|
+-----+
|CDNI Logging Record 1
| +-----+ +-----+ +-----+
| |CDNI Logging |CDNI Logging | ... |CDNI Logging |
| | Field 1 | | Field 2 | | Field N |
| +-----+ +-----+ +-----+
|
+-----+
|CDNI Logging Record 2
| +-----+ +-----+ +-----+
| |CDNI Logging |CDNI Logging | ... |CDNI Logging |
| | Field 1 | | Field 2 | | Field N |
| +-----+ +-----+ +-----+
|
+-----+
| ...
|
| #Directive P+1
|
| ...
|
+-----+
|CDNI Logging Record M
| +-----+ +-----+ +-----+
| |CDNI Logging |CDNI Logging | ... |CDNI Logging |
| | Field 1 | | Field 2 | | Field N |
| +-----+ +-----+ +-----+
|
+-----+
|
| #Directive P+Q
|
+-----+
```



# Old CDNI Logging Fields

- Start-time
- End-time
- Duration
- Client-IP
- Client-port
- Destination-IP
- Destination-hostname
- Destination-port
- Operation
- URI\_full
- URI\_part
- Protocol
- Request-method
- Status
- Bytes-Sent
- Headers-Sent
- Bytes-received
- Referrer
- User-Agent
- Cookie
- Byte-Range
- Cache-control
- Record-digest
- CCID
- SID
- uCDN-ID
- Delivering-CDN-ID
- Cache-Bytes
- Action
- MIME-type
- dCDN-ID
- Caching-Date
- Validity-headers
- Lookup-duration
- Delay-to-first-bit
- Delay-to-last-bit

# Current HTTP Logging Fields

- Date
- Time
- Time-taken
- C-IP
- C-IP-anonimizing
- C-port
- S-IP
- S-hostname
- S-port
- CS-method
- CS-URI
- U-URI
- Protocol
- SC-status
- SC-total-bytes
- SC-entity-bytes
- CS(<HTTP-header-name>)
- SC(<HTTP-header-name>)
- S-CCID
- S-SID
- S-cached
- S-URI-signing

where C: client (User Agent), S: server (dCDN surrogate), U: uCDN, D: dCDN

# Open issues

- Non-repudiation on top of CDNI Logging Feed
- Compliance w/ cdni-requirements: reshape text
- One question on compression of logs (gzip & deflate)
- Precise definitions of implementation requirements versus deployment requirements

# Open issues

- Handling of event logs and notifications
  - eg notification by dCDN to uCDN that dCDN request routing is down
  - Non real-time exchange of event logs for audit purposes
    - “It is proposed that this be handled as a [MED] requirement. e.g. try first to specify what events and what information needs to be exchanged; and depending on progress, decide to include in initial logging spec or not”
    - Currently no progress on that. Can we agree to make explicit decision to not address in initial version?
  - Real-time exchange from dCDN to uCDN for immediate operational action
    - “It is proposed that this be kept out of the scope of the current cdni-logging spec “
    - Can we agree to that?

# Next Steps

- New rev covering
  - remaining Open Items (previous slides)
  - Potential comments on -05