CDNI Logging
draft-ietf-cdni-logging-18

François Le Faucheur – Cisco
Gilles Bertrand - Orange
Iuniana Oprescu - Orange
Roy Peterkofsky – Skytide

IETF 92 Dallas

Changes from 14 to 15

- Addressed XML Expert Review (performed by Daryl Malas)
  - removes the redundant line in Fig 7
  - removes the 3 occurrences of the Editor's Note, and replaced the incorrect hash value by a textual description , so it reads:

    #Integrity-Hash:<HTAB>...32-hexadecimal-digit hash value...<CRLF>

Changes from 15 to 16

- Clarified handling of CDNI Logging File version

> *The entity transmitting a CDNI Logging File as per the present document MUST set the value to "CDNI/1.0". In the future, other versions of CDNI Logging File might be specified; those would use a value different to "CDNI/1.0" allowing the entity receiving the CDNI Logging File to identify the corresponding version.*
>
> *An entity receiving a CDNI Logging File with a value set to "CDNI/1.0" MUST process the CDNI Logging File as per the present document. An entity receiving a CDNI Logging File with a value set to a different value MUST process the CDNI Logging File as per the specification referenced in the CDNI Logging File Version registry (see Section 6.1) if the implementation supports this specification and MUST reject the CDNI Logging File otherwise.*

Changes from 15 to 16

- Clarified handling of CDNI Logging File version

6.2. CDNI Logging File Version Registry

The IANA is requested to create a new registry, CDNI Logging File Version.

The initial contents of the CDNI Logging Logging File Version registry comprise the value "CDNI/1.0" specified in Section 3.3 of the present document, and are as follows:

Version	Reference	Description
CDNI/1.0	RFC xxxx	CDNI Logging File version 1.0 as specified in RFC xxxx

Figure 9

. . .

Changes from 15 to 16

- Clarified handling of invalid CDNI Logging File

> *An uCDN-side implementation of the CDNI Logging interface MUST reject a CDNI Logging File that does not comply with the occurences specified above for each and every directive. For example, an uCDN-side implementation of the CDNI Logging interface receiving a CDNI Logging file with zero occurence of the Version directive, or with two occurences of the Integrity-hash, MUST reject this CDNI Logging File.*
>
> *. . .*
>
> *In case, an uCDN-side implementation of the CDNI Logging interface receives a CDNI Logging File with HTTP Request Logging Records that do not contain field values for exactly the set of field names actually listed in the preceding "Fields" directive, the implementation MUST reject those HTTP Request Logging Records, and MUST accept the other HTTP Request Logging Records .*

Changes from 15 to 16

- Clarified handling of invalid HTTP-header-name

> *The entity transmitting the CDNI Logging File MUST ensure that the <HTTP-header-name> of the cs(<HTTP-header-name) listed in the Fields directive comply with HTTP specifications and, in particular, does not include any HTAB, since this would prevent proper parsing of the Fields directive by the entity receiving the CDNI Logging File.*

Changes from 15 to 16

- MAY → may

> *We note that, in addition to the CDNI Logging File exchange protocol specified in Section 4, implementations of the CDNI Logging interface specified in Section 4, implementations of the CDNI Logging interface may also support other mechanisms to exchange CDNI Logging Files.*

Changes from 15 to 16

- Improved Security Section

7.1. Authentication, Authorization, Confidentiality, Integrity, Protection

An implementation of the CDNI Logging interface MUST support TLS transport of the CDNI Logging feed (Section 4.1) and of the CDNI Logging File pull (Section 4.2) as per [RFC2818] and [RFC7230].

The use of TLS for transport of the CDNI Logging feed and CDNI Logging File pull allows:

o the dCDN and uCDN to authenticate each other

and, once they have mutually authenticated each other, it allows:

o the dCDN and uCDN to authorize each other (to ensure they are transmitting/receiving CDNI Logging File to/from an authorized CDN)

o the CDNI Logging information to be transmitted with confidentiality

o the integrity of the CDNI Logging information to be protected during the exchange.

Changes from 15 to 16

- Improved Security Section

> *In an environment where any such protection is required, the use of a mutually authenticated encrypted transport MUST be used to ensure confidentiality of the logging information. TLS SHOULD be used (including authentication of the remote end) by the server- side and the client-side of the CDNI Logging feed, as well as the server- side and the client-side of the CDNI Logging File pull mechanism, unless alternate methods are used. Alternate methods could include establishing an IPsec tunnel between the two CDNs or using a physically secured internal network between two CDNs that are owned by the same corporate entity).*
>
> *The general TLS usage guidance in [I-D.ietf-uta-tls-bcp] SHOULD be followed.*

Changes from 15 to 16

- DOS: TLS does not help !

> *However, the CDNI Logging feed and CDNI Logging pull endpoints are typically to be accessed only by a very small number of valid remote endpoints and therefore can be easily protected against DoS attacks through the usual conventional DOS protection mechanisms such as firewalling or use of Virtual Private Networks (VPNs).*

Changes from 15 to 16

- Enhanced Privacy text

> *The use of mutually authenticated TLS to establish a secure session for the transport of the CDNI Logging feed and CDNI Logging pull as discussed in Section 7.1 access to the logging information. This provides confidentiality while the logging information is in transit and prevents any other party than the authorised uCDN to gain access to the logging information.*

Changes from 15 to 16

- Clarified W3C ELF format was reused whenever possible
- Editorials

Changes from 16 to 17

- Discuss example usage for non-anonymized logs

> *Some of these maintenance and debugging applications only require aggregate logging information highly compatible with anonymization of IP addresses (as supported by the present document and specified in Section 3.4.1). However, in some situations, it may be useful, where compatible with privacy protection, to access some CDNI Logging Records containing full non-anonymized IP addresses. For example, this may be useful for detailed fault tracking of a particular end user content delivery issue.*

Changes from 16 to 17

- Defined DATE and TIME by reference to RFC3339 (instead of re-defining them inside document)

```
DATE = 4DIGIT "-" 2DIGIT "-" 2DIGIT
 Dates are encoded as "full-date" specified in [RFC3339].

TIME = 2DIGIT ":" 2DIGIT ":" 2DIGIT [ "." *DIGIT]
 Times are encoded as "partial-time" specified in [RFC3339].
```

Changes from 16 to 17

- ABNF Clean up

```
The CDNI Logging File ("CDNILOGFILE") structure is defined
by the following rules:
      DIRLINE = "#" directive CRLF
      DIRGROUP = 1*DIRLINE
      RECLINE = CDNILOGREC CRLF
      RECGROUP = *RECLINE
      CDNILOGFILE = 1*(DIRGROUP RECGROUP)
See Section 3.4 for the definition of CDNILOGREC.
. . .
DIRNAME = NAMEFORMAT
. . .
 o  Version:
     *  format: NHTABSTRING
```

Changes from 16 to 17

- ABNF Clean up

```
CDNILOGREC = FIEVAL *(HTAB FIEVAL)
FIEVAL = <CDNI Logging field value corresponding to the CDNI
Logging field names (FIENAME) listed is the last Fields
directive preceding the present CDNI Logging Record.>
```

Changes from 16 to 17

- Corrected UUID definition

directive value: this a Uniform Resource Name (URN) from the Universally Unique IDentifier (UUID) URN namespace specified in [RFC4122]). The UUID contained in the URN uniquely identifies the CDNI Logging File.

Changes from 16 to 17

- Integrity-Hash → SHA256-Hash

> *directive value: this a Uniform Resource Name (URN) from the Universally Unique IDentifier (UUID) URN namespace specified in [RFC4122]). The UUID contained in the URN uniquely identifies the CDNI Logging File.*

Changes from 16 to 17

- Enhanced Privacy support

```
IPv4 addresses SHOULD be anonymized to /24 boundary (i.e.,
with c-ip-anonymizing set to 8), and IPv6 addresses SHOULD
be anonymized to a /48 boundary (i.e., with c-ip-anonymizing
set to 80).

. . .

 o  c-port-anonymizing:

. . .

Note that cs-uri can be privacy sensitive.  In that case,
and where appropriate, u-uri could be used instead of cs-
uri.
```

- c-ip-anonymizing and c-port-anonymizing made Mandatory to Implement
- All Logging Files examples extended to include anonymization

Changes from 16 to 17

- Renamed “2.2.5.4. Security” into “2.2.5.4. Content Protection”
- Removed “2.2.5.5. Legal Logging Duties” (controversial and not related to interoperability)
- Removed IANA recommendations for naming to include “cdni” prefixes for standardized names
- Editorials

Changes from 17 to 18

- Added *#Remark* directive (as discussed on the list)

```
o  Remark:
  *  format: NHTABSTRING
  *  directive value: this contains comment information. Data
contained in this field is to be ignored by analysis tools.
  *  occurrence: there MAY be zero, one or any number of instance
of this directive per CDNI Logging File.

. . .

6.1.  CDNI Logging Directive Names Registry
. . .
| Remark                         | RFC xxxx  |
```

Next Steps

- Fix editos
  - SHA256-Hash: format: 32HEXDIG →64
  - occurences →occurrences
  - rightmost bits of the IPv4 address → … address
- Work with ADs to resolve the few remaining open items (incl ABNF)
- Discuss resulting changes on WG list
- Move cdni-logging to publication