CDNI Logging
draft-ietf-cdni-logging-19

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

IETF 93 Prague 2015

Changes between -18 and -19

- Clarified use of TLS (TLS MUST be used when protection is needed) and turned the reference to the usage guidance in RFC 7525 into a "MUST" (when TLS is used).
- Updated some references, including RFC 7540.
- Specified that Directive Names and Field Names are case-insensitive, as in the basic ABNF in RFC 2234.
- Added VCHAR to the list in section 3.1.
- Added PCT-ENCODED to the list in section 3.1.

"PCT-ENCODED = "%" HEXDIG HEXDIG ; percent encoding is used for escaping octets that might be possible in HTTP headers such as bare CR, bare LF, CR LF, HTAB, SP or null. These octets are rendered with percent encoding in ABNF as specified by [RFC3986] in order to avoid considering them as separators for the logging records.

Changes between -18 and -19

- Modified “QSTRING = DQUOTE *(NDQUOTE / PCT-ENCODED) DQUOTE.”
- Modified “NDQUOTE = %x21 / %x23-24 / %x26-7E / (DQUOTE DQUOTE) ; whereby a DQUOTE is conveyed inside a QSTRING unambiguously by escaping it with PCT-ENCODED.”
- Added “USER-COMMENT = * (SP / VCHAR / UTF8-2 / UTF8-3 / UTF8-4).”

Changes between -18 and -19

- Specified that the text must be sanitized before being logged: "To ensure that the logging file is correct, the text MUST be sanitized before being logged. Null, bare CR, bare LF and HTAB have to be removed by escaping them through percent encoding to avoid confusion with the logging record separators."
- Added something about the order and dependency of the fields: "A CDNI Logging Record contains the corresponding values for the fields that are enumerated in the last fields directive before the current log line. Note that the order in which the field values appear is dictated by the order of the fields names in the fields directive. There SHOULD be no dependency between the various fields values."
- Added an example for each directive:

  example: "version: HTAB cdni/1.0".

  example: "UUID: HTAB NHTABSTRING" etc.

Changes between -18 and -19

- Added prose about the structure of the logging file:

A CDNI Logging File MUST contain a sequence of lines containing US-ASCII characters [CHAR_SET] terminated by CRLF. Each line of a CDNI Logging File MUST contain either a directive or a CDNI Logging Record.

Directives record information about the CDNI Logging process itself. Lines containing directives MUST begin with the "#" character. Directives are specified in Section 3.3. Logging Records provide actual details of the logged event. Logging Records are specified in Section 3.4.

The CDNI Logging File has a specific structure. It always starts with a directive line and the first directive it contains MUST be the version.

The directive lines form together a group that contains at least one directive line. Each directives group is followed by a group of logging records. The records group contains zero or more actual logging record lines about the event being logged. A record line consists of the values corresponding to all or a subset of the possible Logging fields defined within the scope of the record-type directive. These values MUST appear in the order defined by the fields directive.

Changes between -18 and -19

Note that future extensions MUST be compliant with the previous description. The following examples depict the structure of a CDNILOGFILE as defined currently by the record-type "cdni_http_request_v1." The record line in this example enumerates strictly what is presently defined in the fields directive of the record-type "cdni_http_request_v1.“

DIRLINE = "#" directive CRLF

DIRGROUP = 1*DIRLINE

RECLINE = 1* ([date HTAB] [time HTAB] [time-taken HTAB] [c-ip HTAB] [c-ip-anonymizing HTAB] [c-port HTAB] [s-ip HTAB] [s-hostname HTAB] [s-port HTAB] [cs-method HTAB] [cs-uri HTAB] [u-uri HTAB] [protocol HTAB] [sc-status HTAB] [sc-total-bytes HTAB] [sc-entity-bytes HTAB] [cs(insert_HTTP_header_name_here) HTAB] [sc(insert_HTTP_header_name_here) HTAB] [s-ccid HTAB] [s-sid HATB] [s-cached HTAB]) CRLF

RECGROUP = *RECLINE

CDNILOGFILE = 1*(DIRGROUP RECGROUP)

Changes between -18 and -19

- Added text about the Logging Directives:

A CDNI Logging directive line contains the directive name followed by ":" HTAB and the directive value.

Directive names MUST be of the format NAMEFORMAT. All directive names MUST be registered in the CDNI Logging Directives Names registry. Unknown directives MUST be ignored. Directive values can have various formats. All possible directive values for the record-type "cdni_http_request_v1" are further detailed in this section.

The following example shows the structure of a directive and enumerates strictly the directive values presently defined in the record-type "cdni_http_request_v1."

directive = DIRNAME ":" HTAB DIRVAL

DIRNAME = NAMEFORMAT

DIRVAL = NHTABSTRING / QSTRING / host / USER-COMMENT / FIENAME * (HTAB FIENAME) / 64HEXDIG

Remaining issues

- Tweaks on the ABNF – talked over with Martin Thomson and Pete Resnick.
- Stephen Farrell's DISCUSS about the anonymization part, sharing of granular information and more comments related to privacy.