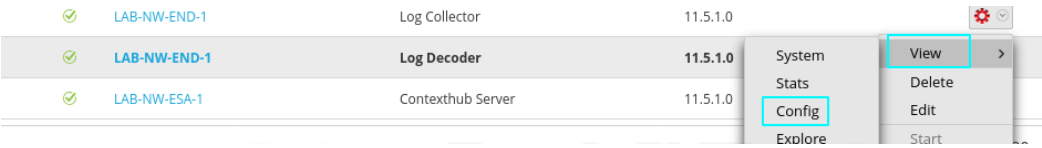
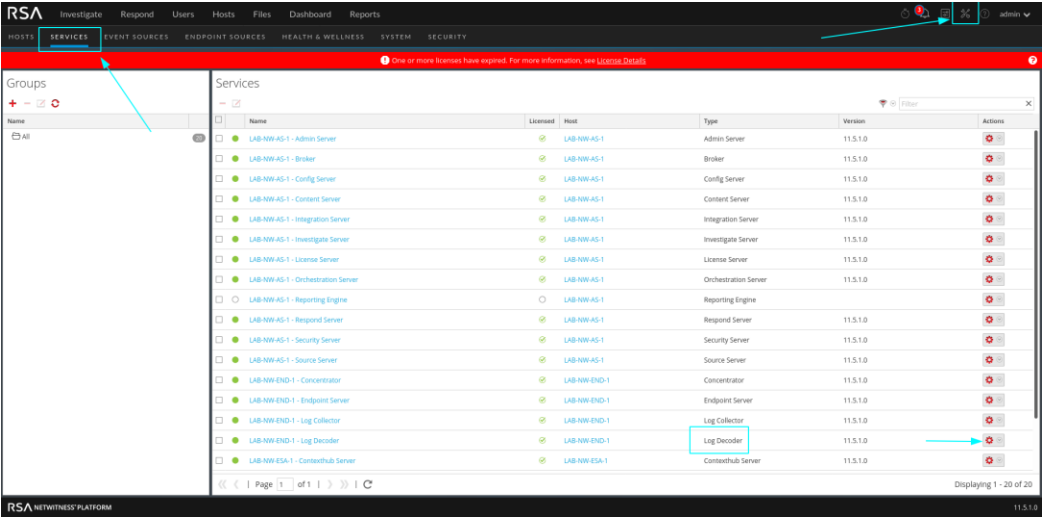


Utilize Web Page Meta for Logs

The "webpage" meta is disabled by default. The process to enabling it is quick and simple. The method reviewed here can be used to turn on any meta key of interest that is already present in the log decoders table-map.xml file.

- 1. go to the log decoder's configuration page.



2. Open the "table-map.xml" file in the files tab.

RSANetWitness PLATFORM

Investigate Respond Users Hosts Files Dashboard Reports

HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

One or more licenses have expired. For more information, see License Details

Change Service LAB-NW-END-1 - Log Decoder Config

General Files Data Retention Scheduler App Rules Correlation Rules Feeds Parsers Parser Mappings Data Privacy Appliance Service Configuration

table-map.xml Log Decoder Get Backup Push

```
<mapping evisionName='duration' nwName='duration.time' flags='None' format='Float64' failureKey='duration.str' failureMapping='duration_string'/>
<mapping evisionName='effective_time' nwName='effective.time' flags='Transient' format='TimeT'/>
<mapping evisionName='endtime' nwName='endtime' flags='Transient' format='TimeT'/>
<mapping evisionName='event_queue_time' nwName='event.queue.time' flags='Transient' format='TimeT'/>
<mapping evisionName='expiration_time' nwName='expire.time' flags='Transient' format='TimeT' failureKey='expire.time.str' failureMapping='expiration_time_string'/>
<mapping evisionName='expiration_time_string' nwName='expire.time.str' flags='Transient' format='Text'/>
<mapping evisionName='recorded_time' nwName='recorded.time' flags='Transient' format='TimeT'/>
<mapping evisionName='starttime' nwName='starttime' flags='None' format='TimeT'/>
<mapping evisionName='timezone' nwName='timezone' flags='None' format='Text'/>
<mapping evisionName='cctld' nwName='cctld' flags='Transient' format='Text'/>
<mapping evisionName='dns.resptext' nwName='dns.resptext' flags='Transient' format='Text'/>
<mapping evisionName='dns.responstype' nwName='dns.responstype' flags='Transient' format='Text'/>
<mapping evisionName='fqdn' nwName='fqdn' flags='None' format='Text'/>
<mapping evisionName='web_referer' nwName='referer' flags='None' format='Text' nullTokens='None' deprecated='1'/>
<mapping evisionName='referer' nwName='referer' flags='None' format='Text'/>
<mapping evisionName='reputation_num' nwName='reputation.num' flags='Transient' format='Float64' nullTokens='None' |ns|n/a|Risk unknown|Well known|err'/>
<mapping evisionName='web_root' nwName='web.root' flags='Transient' format='Text'/>
<mapping evisionName='sld' nwName='sld' flags='Transient' format='Text'/>
<mapping evisionName='tld' nwName='tld' flags='Transient' format='Text'/>
<mapping evisionName='url' nwName='url' flags='Transient' format='Text'/>
<mapping evisionName='query' nwName='query' flags='None' format='Text' deprecated='1'/>
<mapping evisionName='web_query' nwName='query' flags='None' format='Text'/>
<mapping evisionName='web_cookie' nwName='web.cookie' flags='Transient' format='Text'/>
<mapping evisionName='webpage' nwName='web.page' flags='Transient' format='Text'/>
<mapping evisionName='web_ref_domain' nwName='web.ref.domain' flags='Transient' format='Text'/>
<mapping evisionName='web_ref_query' nwName='web.ref.query' flags='Transient' format='Text'/>
<mapping evisionName='web_ref_root' nwName='web.ref.root' flags='Transient' format='Text'/>
<mapping evisionName='web_ref_page' nwName='web.ref.page' flags='Transient' format='Text'/>
<mapping evisionName='web_domain' nwName='web.domain' flags='Transient' format='Text'/>
<mapping evisionName='access_point' nwName='access.point' flags='None' format='Text'/>
<mapping evisionName='ssid' nwName='wlan.ssid' flags='Transient' format='Text'/>
<mapping evisionName='bssid' nwName='wlan.bssid' flags='Transient' format='Text'/>
<mapping evisionName='wifi_channel' nwName='wlan.channel' flags='Transient' format='UInt16'/>
```

Apply

RSANetWitness PLATFORM

web.page Highlight All Match Case Match Diacritics Whole Words 1 of 1 match

3. Find the "webpage" (web.page) key. It will have a flag value of "Transient". Copy the entire line to clipboard.

4. In the files drop-down, open the "table-map-custom.xml". Paste the line in the section marked for custom content.

5. Change the "Transient" value to "None" and apply when done.

RSANetWitness PLATFORM

Investigate Respond Users Hosts Files Dashboard Reports

HOSTS SERVICES EVENT SOURCES ENDPOINT SOURCES HEALTH & WELLNESS SYSTEM SECURITY

One or more licenses have expired. For more information, see License Details

Change Service LAB-NW-END-1 - Log Decoder Config

General Files Data Retention Scheduler App Rules Correlation Rules Feeds Parsers Parser Mappings Data Privacy Appliance Service Configuration

table-map-custom.xml Log Decoder Get Backup Push

Optional, push to any other log decoders

```
<mapping evisionName='duration' nwName='duration.time' flags='None' format='Float64' failureKey='duration.str' failureMapping='duration_string'/>
<mapping evisionName='effective_time' nwName='effective.time' flags='None' format='TimeT'/>
<mapping evisionName='endtime' nwName='endtime' flags='None' format='TimeT'/>
<mapping evisionName='event_queue_time' nwName='event.queue.time' flags='None' format='TimeT'/>
<mapping evisionName='expiration_time' nwName='expire.time' flags='None' format='TimeT' failureKey='expire.time.str' failureMapping='expiration_time_string'/>
<mapping evisionName='expiration_time_string' nwName='expire.time.str' flags='None' format='Text'/>
<mapping evisionName='recorded_time' nwName='recorded.time' flags='None' format='TimeT'/>
<mapping evisionName='starttime' nwName='starttime' flags='None' format='TimeT'/>
<mapping evisionName='timezone' nwName='timezone' flags='None' format='Text'/>
<mapping evisionName='cctld' nwName='cctld' flags='None' format='Text'/>
<mapping evisionName='dns.resptext' nwName='dns.resptext' flags='None' format='Text'/>
<mapping evisionName='dns.responstype' nwName='dns.responstype' flags='None' format='Text'/>
<mapping evisionName='fqdn' nwName='fqdn' flags='None' format='Text'/>
<mapping evisionName='web_referer' nwName='referer' flags='None' format='Text' nullTokens='None' deprecated='1'/>
<mapping evisionName='referer' nwName='referer' flags='None' format='Text'/>
<mapping evisionName='reputation_num' nwName='reputation.num' flags='None' format='Float64' nullTokens='None' |ns|n/a|Risk unknown|Well known|err'/>
<mapping evisionName='web_root' nwName='web.root' flags='None' format='Text'/>
<mapping evisionName='sld' nwName='sld' flags='None' format='Text'/>
<mapping evisionName='tld' nwName='tld' flags='None' format='Text'/>
<mapping evisionName='url' nwName='url' flags='None' format='Text'/>
<mapping evisionName='query' nwName='query' flags='None' format='Text' deprecated='1'/>
<mapping evisionName='web_query' nwName='query' flags='None' format='Text'/>
<mapping evisionName='web_cookie' nwName='web.cookie' flags='None' format='Text'/>
<mapping evisionName='webpage' nwName='web.page' flags='None' format='Text'/>
<mapping evisionName='web_ref_domain' nwName='web.ref.domain' flags='None' format='Text'/>
<mapping evisionName='web_ref_query' nwName='web.ref.query' flags='None' format='Text'/>
<mapping evisionName='web_ref_root' nwName='web.ref.root' flags='None' format='Text'/>
<mapping evisionName='web_ref_page' nwName='web.ref.page' flags='None' format='Text'/>
<mapping evisionName='web_domain' nwName='web.domain' flags='None' format='Text'/>
<mapping evisionName='access_point' nwName='access.point' flags='None' format='Text'/>
<mapping evisionName='ssid' nwName='wlan.ssid' flags='None' format='Text'/>
<mapping evisionName='bssid' nwName='wlan.bssid' flags='None' format='Text'/>
<mapping evisionName='wifi_channel' nwName='wlan.channel' flags='None' format='UInt16'/>
```

Apply

RSANetWitness PLATFORM

web.page Highlight All Match Case Match Diacritics Whole Words 1 of 1 match

6. Open the configuration page for the concentrator associated with the log decoder that was just adjusted

<input checked="" type="checkbox"/>	LAB-NW-END-1 - Concentrator	LAB-NW-END-1	Concentrator	11.5.1.0	
<input type="checkbox"/>	LAB-NW-END-1 - Endpoint Server	LAB-NW-END-1	Endpoint Server	11.5.1.0	
<input type="checkbox"/>	LAB-NW-END-1 - Log Collector	LAB-NW-END-1	Log Collector	11.5.1.0	
<input type="checkbox"/>	LAB-NW-END-1 - Log Decoder	LAB-NW-END-1	Log Decoder	11.5.1.0	
<input type="checkbox"/>	LAB-NW-ESA-1 - Contexthub Server	LAB-NW-ESA-1	Contexthub Server	11.5.1.0	

7. Open the "index-concentrator-custom.xml" file in the files tab. Add an entry for the "webpage" meta key as shown below. This will allow the "webpage" meta to be seen in the Navigate and Events views.

RSA Investigate Respond Users Hosts Files Dashboard Reports

HOSTS
SERVICES
EVENT SOURCES
ENDPOINT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY

One or more licenses have expired. For more information

Change Service
LAB-NW-END-1 - Concentrator
Config

General
Files
Data Retention Scheduler
Correlation Rules
Appliance Service Configuration

index-concentrator-custom.xml
Concentrator
 Get Backup
 Push

destination = specifies the key name or the transformed meta value to create

Decoder examples - Normally you do not need to edit index files on the Decoder, unless you want to add aliases or have data privacy requirements. Parsers and feeds declare their meta keys internally and those keys are automatically added to the language. Also, you should *never* set the index level to `IndexKeys` or `IndexValues` on a Decoder if you have a `Concentrator/Archiver` aggregating from it. The index partition size is too small to support any indexing beyond the default "time" meta.

Data privacy
`<key description="existing meta key" format="Text" level="IndexNone" name="existing" protected="true">`
`<transform destination="existing.hash"/>`
`</key>`

`Concentrator/Archiver` examples - Any new meta keys that should be indexed must be added to this file.

Adding new meta key for custom parser at the index key level
`<key description="my new parser meta key" format="Text" level="IndexKeys" name="mynewparserkey"/>`

Data privacy
`<key description="existing meta key" format="Text" level="IndexValues" name="existing" protected="true">`
`<transform destination="existing.hash"/>`
`</key>`
`<key description="existing meta key hash" format="Text" level="IndexValues" name="existing.hash" token="true"/>`

Broker derives its language from all the devices it aggregates from. There is simply no need to edit a broker's custom language file.
 -->

<!-- *** Please insert your custom keys or modifications below this line *** -->

`<key description="Stream Info" name="streams" format="UInt8" singleton="true" level="IndexValues" valueMax="6"/>`

`<key description="webpage" name="web.page" format="Text" level="IndexValues" valueMax="1000000"/>`

</language>

Apply

RSA NETWITNESS PLATFORM