Logstash conf file example

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

```
input { file { path => "C:/Users/shzada/Desktop/c.log" start_position => "beginning" sincedb_path => "NUL" } }

filter { json{ source => "message" } date { match => [ "timestamp" , "UNIX_MS" ] target => "iso8610timestamp" } }

output { azure_loganalytics { customer_id => "802d39e1-9d70-404d-832c-2de5e2478eda" shared_key => "**********" log_type => "CrowdStrike" key_names => ['AuthenticationId','CommandLine','ConfigBuild','ConfigStateHash','EffectiveTransmissionClass','Entitlements','ImageFileName','ImageSubsystem','IntegrityLevel','MD5HashData','ParentAuthenticationId','ParentProcessId','ProcessCreateFlags','ProcessEndTime','ProcessParameterFlags','ProcessStartTime','ProcessSxsFlags','RawProcessId','SHA1HashData','SHA256HashData','SessionId','ShowWindowFlags','SourceProcessId','SourceThreadId','Tags','TargetProcessId','TokenType','UserSid','WindowFlags','aid','aip','cid','event_platform','event_simpleName','id','name','timestamp','iso8610timestamp'] flush_items => 10 flush_interval_time => 5 time_generated_field => "iso8610timestamp" } stdout { codec => "rubydebug" } }
```