Tessera Logging

Tessera uses the Logback logging framework. See the Logback documentation for detailed information on configuring Logback.

You can monitor Tessera logs using Splunk or Elastic Stack (ELK).

Log level

Messages are written to the Tessera logs according to the following log levels:

- ERROR
  - System failures or situations that require some action to ensure correct operation of the system
- WARN
  - Notifications that don't require immediate action or that are indications that a transaction failed
- INFO
  - Information message to allow investigation of issues or to provide reassurance that the system is operating correctly
- DEBUG
  - More verbose logging to assist with investigation of issues

The log level is written out in uppercase as part of the log message. You can use this for alert monitoring.

The log level is specified by the Logback configuration file. See the default configuration file packaged with Tessera. To specify a different log level or logging configuration, pass a customized Logback configuration file on the command line:

JAVA_OPTS="-Dlogback.configurationFile=/path/to/logback.xml" tessera --configfile config.json

Errors

The following is a non-exhaustive list of error messages and suggested actions. Braces '' indicate where further detail of the root cause is logged as part of the message.

Message Cause Error decoding message: {error details} Invalid base64 in privateFrom/privateFor from the privacy-enabled Ethereum client, or in transaction hash for resend. Action :Sender needs to provide valid base64 Error occurred: {error details} Root cause: {root cause} Generated for a variety of reasons:

- Invalid content in message, example:curl -X POST "http://localhost:9001/push" -H "accept: application/json" -H "Content-Type: application/octet-stream" -d ["a garbage string"]
- Could not send message to peer, example: Root cause: Unable to push payload to recipient urlhttp://localhost:9001/" Action :depends on the root cause in the log message Enclave unavailable: {error details} Action :user needs to check why enclave is unavailable (look in log file for enclave) Entity not found: {error details} API request received againstq2tserver/transaction/{key} where key is not a transaction hash in the DB Entity not found:{error details} Thrown if endpoint doesn't exist on that API, example: curl -shttp://localhost:9001/invalidendpoint Security exception {followed by exception message, example "java.lang.SecurityException: No key found for url 127.1.1.1"} Thrown if enableRemoteKeyValidation: true and partyinfo request received from a URL of a node for which we don't hold a public key (for example potentially a malicious party).Note: if key validation enabled then this exception will be thrown during startup whilst the nodes exchange key information. ERROR c.q.t.a.e.DefaultExceptionMapper - HTTP 400 Bad Request Logged if received message is corrupt/incorrectly formatted, example:curl -X POST "http://localhost:9001/resend" -H "accept: text/plain" -H "Content-Type: application/json" -d "{ "some rubbish" }" Error while reading secret from file Unable to read the secret key (password) from file specified by TESSERACONFIG_SECRET Action : _ensure the secret key file configuration is correct, and file can be read unable to initialize encryption façade {error details} Unable to initialize elliptical curve encryption. Logged error message will give further details Action :check configuration properties unable to generate shared secret {error details} Unable to generate shared secret for elliptical curve encryption. Logged error message will give further details. Action :check configuration properties unable to perform symmetric encryption {error details} Unable to encrypt data. Logged error message will give further details. Action :check configuration properties unable to perform symmetric decryption {error details} Unable to decrypt data. Logged error message will give further details. Action :check configuration properties Error when executing action {action type}, exception details: {error details} Unable to start Influx DB. Logged error message will give further details Action :check configuration properties Error creating bean with name 'entityManagerFactory' Unable to create connection to database due to failure to decrypt the DB password using the supplied secret key Action :ensure that the correct value is supplied for the secret key Config validation issue: {property name} {error details} Invalid configuration detected Action :correct the configuration of the named property.

Invalid json, cause is {error details} Invalid JSON in the configuration file Action :check the configuration file for mistakes. Configuration exception, cause is {error details} Invalid data in the configuration file Action :check the configuration file for mistakes. CLI exception, cause is {error details} Invalid command line Action :The error details will give further information regarding the action to be taken.

Warnings

The following is a list of warning messages and possible causes. Braces '' indicate where further detail of the root cause is logged as part of the message.

Message Cause Public key {publicKey} not found when searching for private key The key in a transaction is not recognized, example: it is not the public key of a known participant node Recipient not found for key: {public key} An unrecognized participant is specified in a transaction.No action needed. Unable to unmarshal payload A received message is corrupt, or incorrectly formatted Remote host {remote host name} with IP {remote host IP} failed whitelist validation Logged if whitelist validation is enabled and the remote host is not in the whitelist. Action :either this is a malicious connection attempt, or mis-configuration Ignoring unknown/unmatched json element: {element tag name} An unrecognized element has been found in the configuration file. Action :remove or correct the configuration file entry Not able to find or read any secret for decrypting sensitive values in config Secret key (password) could not be read from console or password file (see TESSERACONFIG_SECRET in docs). Action : *correction needed for the secret key or the file access permission Some sensitive values are being given as unencrypted plain text in config. Please note this is NOT recommended for production environment. Self explanatory Not able to parse configured property. Will use default value instead Error in configuration file IOException while attempting to close remote session {error details} Only occurs on shutdown, no action needed Could not compute the shared key for pub {public key} and priv REDACTED Possible cause is that a public key does not match the configured cryptography algorithm. Action :ensure provided key is correct Could not create sealed payload using shared key {shared key} Possible cause is that a public key does not match the configured cryptography algorithm. Action : _ __ensure provided key is correct* Could not open sealed payload using shared key {shared key} Possible cause that wrong password was given for key file decryption or making a change to the values in the keyfile so that the password no longer works. Action :ensure that password is correct for the keyfile Unable to generate a new keypair! Internal error - potentially an issue with jnacl dependency Exception thrown : {exception message} While starting service {service name} Internal error - failed to start a service Invalid key found {remote host url} recipient will be ignored Remote key validation check failed.No action needed, however it is a possible indication of a malicious node_ Push returned status code for peer {remote peer url} was {status code} The peer rejected a transaction 'push' request. Action :check logs on peer to see why it failed PartyInfo returned status code for peer{remote peer url} was {status code} The peer rejected a partyInfo request. Action :check logs on peer to see why it failed Unable to resend payload to recipient with public key {public key}, due to {error details} The peer rejected a transaction push request during a resend operation. Action :check reason message, or logs on peer to see why it failed Attempt is being made to update existing key with new url. Please switch on remote key validation to avoid a security breach Self explanatory Failed to connect to node {remote node url}, due to {error details} A remote node refused partyinfo request. Can occur if: - remote node is not running - remote node doesn't recognize this node's public key - remote node doesn't have this node's IP registered against a key - etc

Can also be expected to occur when nodes are shutdown/restarted, so not necessarily an error. Failed to connect to node {remote node url} for partyInfo, due to {error details} A node failed partyInfo request during resend to peer. Action :check reason message, or logs on peer to see why it failed Failed to make resend request to node {remote node url} for key {public key}, due to {error details} Peer communication failed during '/resend' request. Action :check reason message, or logs on peer to see why it failed Connection error while communicating with {uri} Peer communication failed during '/push' request. Action :check logs on peer to see why it failed - it may be a failed node requiring restart or removal from peer list An error occurred during batch resend sync stage. {exception error details} During the Data Recovery process (sync stage), transaction data from a peer either failed the enhanced privacy checks, or could not be stored in the database Action :check error details to see why it failed and determine action to be taken note Some messages will be rearranged to correct logging levels in our next release. Edit this page Last updatedonNov 29, 2023 byJoshua FernandesPrevious Monitoring Next Mandatory recipients