**FACTOM**

**COMMUNITY**

**Draft**

**Incident Reporting**

**&**

**Management**

**DOC 108**

|  |  |  |  |
| --- | --- | --- | --- |
| VERSION | DATE | CHANGED BY | CHANGES |
| 0.1 | 2018-07-17  :  2018-08-06 | Centis BV  (Niels Klomp)  The 42ND Factoid AS  (Tor Hogne Paulsen) | First draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

* 1. This document describes the process for incident reporting for issues related to the Factom network as well as individual nodes. All chapters of this document are important, but mainly chapters 2 and 3 are of vital importance for the reporter of the incident, as it describes required actions on his/her part.
  2. The types of incidents we experience most of the time falls into two categories;
     1. **Individual authority node stalls/crashes;** Most of the time these only influence the failed node. There are many failure modes that can lead up to a node crash; examples are: Bug(s) in the factomd-code, network issues, running out of disk space, botched brain-transfer/swap etc..
     2. **Network stalls**. These incidents have an impact on everyone utilizing the Factom blockchain as it is unavailable until the network is rebooted. These happen most of the time because of failsafe conditions in the Factom code to prevent forks of the Factom blockchain, as well as due to failed authority elections when one or multiple node stalls.

# Incident Reporting

* 1. An ANO experiencing an authority node failing (crash, stall, network outage etc.) or identifies a network stall, is required to create an incident report in the discord channel **#incident-management** channel, tagging the role **@Incidents** as the first line. This ensures people handling incidents are notified.
  2. When a **network stall** is detected only one ANO incident report is required, and subsequent ANOs joining the #incident-management channel is not required to file duplicate reports.
  3. The incident-management channel is available for everyone to use. All who can aid with the incident is welcome to help and participate, as incident management is a collaborative effort.
  4. **Filing the report:**

* + 1. Please provide the following information in your incident report:
       1. The tag @Incidents.
       2. Date and time when the issue occured;

(format: YYYY-MM-DD, HH:MM UTC)

* + - 1. Categorization (next chapter) & node type;

(node stall/crash/instability (type),network stall? Other? Federated, Audit or follower node? Election triggered?

* + - 1. Initial Impact & Urgency (next chapter)

Impact can be high or low. Urgency can be high or low. Please see the next chapter for more explanation about this.

* + - 1. Create a Google document (text) file [here](https://drive.google.com/open?id=1O0RKBUOlMFNvbHQKfvyaE-degRoQqZjt) in the folder corresponding to the current year and adhering to the following naming standard:

<YYYY-MM-DD\_HH-MM>\_<Operator-name>\_<version>

(examples: 2018-07-17\_00-40\_TFA\_01 or 2018-08-01\_12-15\_BIF\_05 ).

* + - 1. Paste/Place your factomd/docker logs in the above. document. *Please only paste the relevant sections, but do not limit it too much. If unsure paste everything.*

(use the following command: docker logs -t factomd).

* + - 1. Post a link in Discord to the log-file above if relevant.

(Tip: Embed the link in <LINK> to avoid previewing the file).

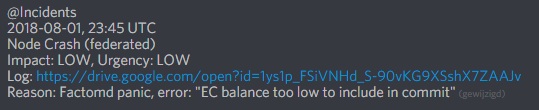
* + - 1. Reason for incident.

(format: Reason: Unknown / Reason: factomd panic / Reason: user error).

* + - 1. Any additional information you may have.

(did the incident happen when working on the node, connectivity issues, related incidents?).

Example:



# Categorization and prioritization

* 1. After the incident is reported somebody from the core- and code deployment committee will pick up the incident.
  2. Incidents are preliminary categorized by the reporter itself and later finalized by someone of the committee. The most prominent categories are:
     + 1. Network stall
       2. Node crash
  3. The incident will get a unique consecutive number assigned to it (format: FIN-YY-00x for network incidents and NODE-YY-00x for node incidents) and it will be entered into the respective category tab in the Factom Network Incident Log [here](https://docs.google.com/spreadsheets/d/1xPfEjTETUulqO35aMjvEKMkGxroYwfatv6JYnCcuBMY/edit#gid=0).
  4. The incident gets prioritized using a combination of Impact and Urgency to determine a Priority. A preliminary Impact and Urgency determination is done by the reporter. The final values will be made by committee members. For our use-case we will probably see the impact and urgency categories having the same values most of the time, given the impact and urgency are highly correlated in our case.
  5. The Factom Network stalls whenever something of importance happens in the network which shouldn’t have happened and cannot be resolved automatically. This is a deliberate security measure to prevent forks of the blockchain.
  6. **Impact**

Impact is primarily determined by the scope of the effect of the incident.

* + 1. **High Impact events:**
       1. Factom network is down/stalled.
       2. Multiple nodes are affected.
       3. The incident affects multiple users of the protocol.
    2. **Low Impact events:**
       1. Only one node is affected.
       2. The incident affects only a small number of users of the protocol.
  1. **Urgency**

Urgency is mainly determined by how quickly an incident has an effect on the whole network.

* + 1. High Urgency:
       1. The effects of the incident are expanding or quick action is necessary.
       2. Important or time sensitive work/customers are affected.
       3. The Incident affects one or multiple FCT exchanges.
    2. Low Urgency:
       1. The effects of the incident appear stable.
       2. Important or time sensitive work/customers are not affected.
  1. **Priority**

The priority is a direct result of the Impact and the Urgency and is used to determine the pickup time, escalation level and speed at which the incident needs to be resolved.

|  |  |  |  |
| --- | --- | --- | --- |
|  | | **Impact** | |
| **High** | Low |
| **Urgency** | **High** | 1 | 3 |
| Low | 3 | 5 |

Note: Normally you would see a medium impact and urgency as well. Given it is highly unlikely in a distributed network that needs to work together we will be seeing medium impacts and urgencies we left them out. In order to make sure they could be taken into account in the future the priority matrix does account for future inclusion of medium values, hence priority 2 and 4 are left out.

|  |  |  |
| --- | --- | --- |
| **Priority** |  |  |
| 1 | Critical | Urgent action required, escalation almost immediately |
| 3 | Medium | Quick action required, however escalation might not be necessary. |
| 5 | Low | No direct action required. No escalation. |

# Initial diagnosis and escalation

* 1. Initial diagnosis is done in the **#incident-management** channel on Discord and is open to everybody that can contribute. Basically this is the process of asking the initial questions to better determine the problem at hand. ANO-representatives should follow the direction of members of the core-committee, and
  2. Whenever an incident has priority 1 and needs to be handled by somebody from the core- and networking committee or by Factom Inc, the incident will be escalated when nobody appropriate to handle the incident is available at the time.
  3. Incidents with a priority of 3 or higher will be escalated as well when they cannot be handled by current users in the above channel, but at an appropriate time. Please note that escalation in this context means getting a person involved with more appropriate knowledge to solve the incident at hand. This can be done by anybody in the committee.

# Status updates

* 1. Whenever warranted by the priority status updates to external parties will be given. Parties are for instance users of the protocol, exchanges, ANO etc.
  2. Status updates will given at appropriate times when there is something to report, or whenever a priority 1 incident is ongoing; at least every 3 hours, so parties know it is still being investigated or worked on.
  3. Updates will be posted in the **#incident-management** channel on Discord.
  4. For network wide incidents Factom Inc will update the <https://status.factom.com> status page with updates about the incident. External parties can subscribe to updates via an e-mail service hosted at this site.
  5. Exchanges will be informed based on existing communication channels with the respective exchanges.

# Investigation and diagnosis

* 1. Whenever an incident cannot be resolved during initial diagnosis, incident investigation and diagnosis will be initiated by the core committee. In most situations this will involve Factom Inc, where they try to reproduce the incident under controlled conditions or work directly with the incident reporter. Whenever dialogue with the initial incident reporter is warranted, communications will be effected using the **#incident-management** channel, unless information of a sensitive nature is being discussed.
  2. Whenever a bug is resolved that was seen in one or more incident reports, the release notes of Factomd shall mention the affected incident numbers.

# Resolution, Reporting & Closure

* 1. Solving the incident sometimes can be an integral part of the investigation & diagnosis, but often software development is needed to fix a bug and add (regression) tests to the software. Unless the incident is a priority 1 bug and it is determined by the core- and code deployment committee and urgent fix is required, bug-fixes will be rolled out during normal release procedure and cadence. Sometimes a temporary workaround can be necessary in the meantime.
  2. After an incident of at least priority 3 the core- and code committee will create and after-action report about the incident and whenever it is an incident that affects multiple parties that after-action report will be shared with the operators and other parties in the #incident-management channel.