target services | TIPS

TIPS Incidents

19 May and follow up on 27 March and 4 April

TIPS CG – 24 June 2021

BANCA D'ITALIA
EUROSISTEMA

Incident on March 27, 2021

- On **27th March** the scheduled TIPS site recovery test was carried out. This test envisaged the simulation of a disaster on TIPS primary site and the execution of the failover activities to restore the service on TIPS secondary site.

- The failover activities were completed in 5 minutes(9:03 – 09:08) but the service was not completely resumed as expected and Instant Payments were not processed correctly

- The Internal Network Service Provider identified a misconfiguration of the firewalls on the secondary site. The correspondent fix was applied resuming the service at 10:36 .

- After the installation of the fix, although the most of IPs were settled, some payments got expired due to a network instability.

Incident on March 27th, 2021

- The network instability was caused by an incorrect behavior of network switches leading to lack of full connectivity between TIPS core components and MQ Servers in charge of communication with Network Service Provider

- The malfunctioning switches were disabled at 10:57 and from that point onwards all the IPs were correctly settled

- The failback activities were completed at 17:40

Incident on March 27th, 2021 – Action Plan

- The misconfiguration of the firewalls was caused by a software bug that was fixed on 5th June
- The network instability was caused by an incorrect behavior of some network switches. The software of the switches was updated on 5th June during the TIPS planned downtime.

Incident on April 4, 2021

- On the 04th April the TIPS Service desk was contacted by an Instructing Party reporting issues in sending and receiving transactions with TIPS. In parallel an NCB informed about missing reply to their End to End checks towards TIPS.

- The support team was involved to perform all checks on the functionalities of the platform with the conclusion that everything was working normally as both the settlement and the expired payments rate seemed to be in line with the average - also the internal E2E returned positive results.

- As the reports from two different customers require thorough investigation, the support team also opened a case with their NSP, SWIFT, to perform check on their end as well. The initial checks on the NSP came back with no evidence of any malfunction on their side either.

target services | TIPS

Incident on April 4, 2021

- On 6th April the TIPS Service Desk received the information from the IP's responsible NCB that the issues were still ongoing for their customer, along with reports from another NCB experiencing similar issues where most of the payments were being settled and a small percentage expired. A Settlement Managers' call was held to inform about the unusual behaviour when interacting with TIPS.

- In a coordinated way with SWIFT, a controlled restart of some TIPS infrastructural boundary components was performed at around 13:20, and once this action was carried out the expiration rate seemed to drop. Checks with the impacted NCB's/IPs confirmed the success of the action.

BANCA D'ITALIA
EUROSISTEMA

Incident on April 4, 2021 – Action Plan

- The SWIFT-BDI joined investigation revealed that SWIFT was not compliant to TIPS requirements. SWIFT sent persistence messages to non-persistent TIPS queues and it caused the issue described. The usage of persistent messages lead to reach the size limit of the log files causing messages to be uncommitted and blocking the entire queue.

- SWIFT delivered the fix according to the following schedule:
  - **Between 5th - 9th July in CERT environment**
  - **Between 12th – 16th July in PROD environment**

- On TIPS side some improvements were implemented to manage the presence of persistent messages
  - **Monitoring**
    - checks for persistent messages in TIPS queues checks of uncommitted messages in TIPS queues
  - **Infrastucture**
    - operational log's tolerance raised in case of usage of persistence messages
  - **Automation**
    - Implementation of a new self-healing mechanism to process uncommitted persistence messages
  - **Escalation**
    - Adding automatic call-out in case of issues on the inbound and outbound queues which interface with the NSP

Incident on May 19, 2021 - description

- On 19/05/2021 in the afternoon the Service Desk received an email from an NCB for not having received the Delta 3 reports scheduled at 11:00 and 14:00.
- The analysis was started involving the support team as no alarms had been raised in the technical monitor. The support team, confirmed the issue with the database responsible for the reports generation at 11:00, which actually prevented all the expected reports to be delivered, whereas the subsequent run of the Delta 3 reports scheduled at 14:00 was successful, which was also confirmed by the relevant NCB eventually.
- All the next reporting sequences were fine until the generation of the Full reports scheduled at 18:00, when the issue reoccurred. Again no error was triggered on the Technical Monitor, the support teams were already monitoring the situation though and after a second manual intervention the issue was solved and the full reports were finally sent out at 20:38.

Incident on May 19, 2021 – root cause and action plan

- The root cause of the issue was found in the configuration of the component responsible for the report generation. The configuration had been modified to allow an infrastructural change the previous weekend. The updated configuration did not allow the component to access the Database with write-privileges, hence causing the failure of the reporting process.
- The correct configuration was then restored.

- Action plan:

  ✓ Enhancement of the technical monitor to detect issues to access Database for report generation
  ✓ Improvement of the operational procedure to shorten the time required to recover the missing reports

Thank you for your attention