FUJ00171946

Document Title:	Post Incident Report: IRE19 Galleon Time Server Issue 27 03 2023
Document Reference:	SVM/SDM/INR/4831
Release:	Release Independent
Abstract:	On the evening of 27.03.2023, the IRE19 Galleon time server, time/date had reset to 11th August 2003, following a failure with the GPS Antenna. This caused domain authentication issues, server failures and resulted in a degradation of live counter service.
Document Status:	DRAFT
Author & Dept.:	Piotr Nagajek & James Yates
External Distribution:	None
Information Classification	POST INCIDENT REPORTS ARE TO BE INTERNAL FUJITSU DOCUMENTS, NOT TO BE SENT TO POL. See section 0.8.

Approval Authorities:

Name	Role	
Steve Bansal	POA Senior Service Delivery Manager	See Dimensions for record
Sonia Hussain	POA Head of Online Services	

FUJ00171946

0 Document Control

0.1 Table of Contents

0 DOCUMENT CONTROL 2

0.1 Table of Contents 2
0.2 Document History 2
0.3 Review Details 2
0.4 Associated Documents (Internal & External) 2
0.5 Abbreviations 2
0.6 Glossary 2
0.7 Accuracy 2
0.8 Information Classification 2

1 PIR MEETING 2

1.1 Purpose 2
1.2 Date 2
1.3 Attendees 2

2 INCIDENT SUMMARY/OVERVIEW 2

2.1 Description 2
2.2 Date, Time and Duration 2
2.3 Root Cause 2
2.4 Summary of the Impact to POL and their Customers and or Suppliers 2

3 POST INCIDENT REVIEW NOTES 2

4 RECOMMENDED ACTIONS 2

FUJ00171946

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change CP/CCN/PEAK Reference
NOTE: This document is based on template **SVM/SDM/TEM/2531.** See file SVMSDMTEM2531.DOCX for history of template.			
0.1	30/03/2023	Draft by Incident Management	
0.2	04/04/2023	Following CHG0362095 activities, IRE19 Galleon server has been fixed. Updated sections 3. and 4.	CHG0362095
0.3	05/04/2023	Updated sections 3. and 4.	CHG0362793
0.4	19/04/2023	Updated section 4.	CHG0365831 PC0305349

0.3 Review Details

Review Comments by:	
Review Comments to:	Piotr.Nagajek: GRO + POA Document Management

Mandatory Review	
Role	**Name**
POA Senior Service Delivery Manager	Steve Bansal
Principal Consultant (SMG)	Shaun Wood

Optional Review	
Role	**Name**
POA Head of Online Services	Sonia Hussain

(*) = Reviewers that returned comments

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**

0.4 Associated Documents (Internal & External)

References should normally refer to the latest approved version in Dimensions; only refer to a specific version if necessary.

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 *(DO NOT REMOVE)*	See note above	See note above	POA Generic Document Template	Dimensions
SVM/SDM/TEM/2531			Post Incident Report Template	Dimensions
SVM/SDM/WKI/2399			Problem and Major Incident Management Team Work Instructions	Dimensions
SVM/SDM/PRO/0018			POA Operations Incident Management	Dimensions

FUJ00171946

			Procedure	
SVM/SDM/PRO/0001			POA Operations Major Incident Procedure	Dimensions
SVM/SDM/PRO/0025			POA Problem Management Procedure	Dimensions
SVM/SDM/MAN/2738			Post Incident Report: Subject	Dimensions
SVM/SDM/INR/4833			Major Incident Report 4833	Dimensions

0.5 Abbreviations

Abbreviation	Definition
BCP	Business Continuity Plan or Planning
DM	Duty Manager
DVLA	Department of Vehicle Licensing
GWS	Generic Web Service
HORIce	Horizon Information Centre
MI	Major Incident
OOH	Out of Hours
PIR	Post Incident Review
POA	Post Office Account
PODG	Post Office Data Gateway
POL	Post Office Limited
POL IT DSD	Post Office Limited IT Digital Service Desk
SSC	System Support Centre
TfS	TRIOLE for Service
VWB	Virtual White Board

0.6 Glossary

Term	Definition

0.7 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.8 Information Classification

POST INCIDENT REPORTS ARE TO BE INTERNAL FUJITSU DOCUMENTS NOT TO BE SENT TO POL.

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED

FUJ00171946

PIR Meeting

0.9 Purpose

Purpose of this Post Incident Review is to complete the root cause analysis and lessons learnt processes.

0.10 Date

1st PIR Meeting – 29.03.2023, 15:00

Recording: IRRELEVANT

IRRELEVANT

RE_ _PIR_ IRE11_19 Galleon Time Server I

Minutes:

2nd PIR Meeting – 0504.2023, 13:00

Recording: IRRELEVANT

IRRELEVANT

PIR Meeting Galleon PIR Technical

Minutes:

0.11 Attendees

1st PIR Meeting – Stuart Johnston, Matthew Hatch, Andrew Hemingway, Steve Bansal, Joseph Diffin, Robert Gelder, Shaun Wood, Piotr Nagajek, Michael Greene, Farzin Denbali

2nd PIR Meeting – Andrew Hemingway, Ankit B.Agarwal, James Yates, Mahesh Gandhi, Piotr Nagajek, Jason Kidd, Pravin Gotur, Shaun Wood, Shashank Kulkarni, James Horsfall, Nikhil Bhagade, Vishal Pathak, Amar Dafal

1 Incident Summary/Overview

1.1 Description

On 27.03.2023, at approx. 18:56 the IRE19 Galleon NTS-6002 time server time/date had reset to 11th August 2003. This affected all platforms running time off these servers, including live Network Reverse Proxy servers. This caused NRP005, NRP006 and NRP007 to believe that client certificates were expired and only NRP008 servicing the traffic. As a result, counter service impact was observed starting from 18:58:15 when first Counter Super Event – 0440 was observed until approx. 04:00, when all impacts were resolved.

Example branch traffic during the impact - about 1 transaction per minute was observed between 19:47 and 22:12.

The batch schedule delays were observed, but all files were delivered within the agreed time window. Example: previous week Santander GIRO files were sent to NBIT at 20:50, on 27.03.2023 they were delayed to 22:20.

Also, EPAY service was impacted by this issue from 19:47 until 22:12.

FUJ00171946

Multiple Windows servers were impacted and had to be recovered. SSNv2 (Windows 2012) access was affected as well causing partial impact to monitoring tools (No issues with SSNv1). Windows NRPs were affected, however, on Linux platforms the NTP service was stopped, but it did not refer to the default date due to the safety mechanism that did work ("tinker panic" setting).

During the tech bridge call, once issues with the IRE19 Galleon server were identified, the faulty IRE19 Galleon Server was removed from the service via GUI ("soft shut down") and the working IRE11 Galleon Server configuration was updated to remove the peer of the IRE19 Galleon Server. A decision was then taken by Fujitsu Service to manually point NRP005, NRP006 and NRP007 to the working IRE11 Galleon Time Sync server. Following this and reboot of the NRPs, the services started to gradually recover.

The IRE19 Galleon NTS-6002 Time Sync Server time/date reset to 11th August 2003 was due the GPS Antenna counter resetting itself. Due to a faulty GPS Antenna, this counter was steadily increasing to a point when it reset itself which could be to a GPS antenna default date/time.

Please detailed OOH DM timeline attached in the email below:

OOH DM Handover .msg

1.2 Date, Time and Duration

	Date	Time
Time of Service Impact	27.03.2023	18:56
Time Service Restored	28.03.2023	04:00

1.3 Root Cause

The IRE19 Galleon NTS-6002 Time Sync Server time/date reset to 11th August 2003 was due the GPS Antenna counter resetting itself. Due to a faulty GPS Antenna, this counter was steadily increasing to a point when it reset itself to the GPS antenna default date/time.

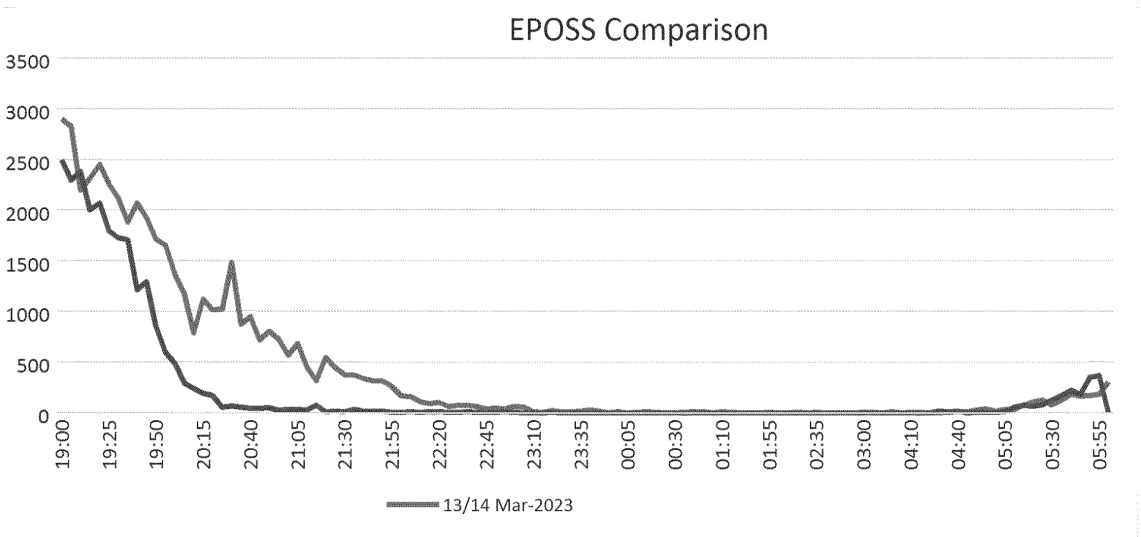
1.4 Summary of the Impact to POL and their Customers and or Suppliers

Live branch traffic was significantly degraded between 18:58 and approx. 04:00, when only one NRP IRRELEVANT was servicing traffic.

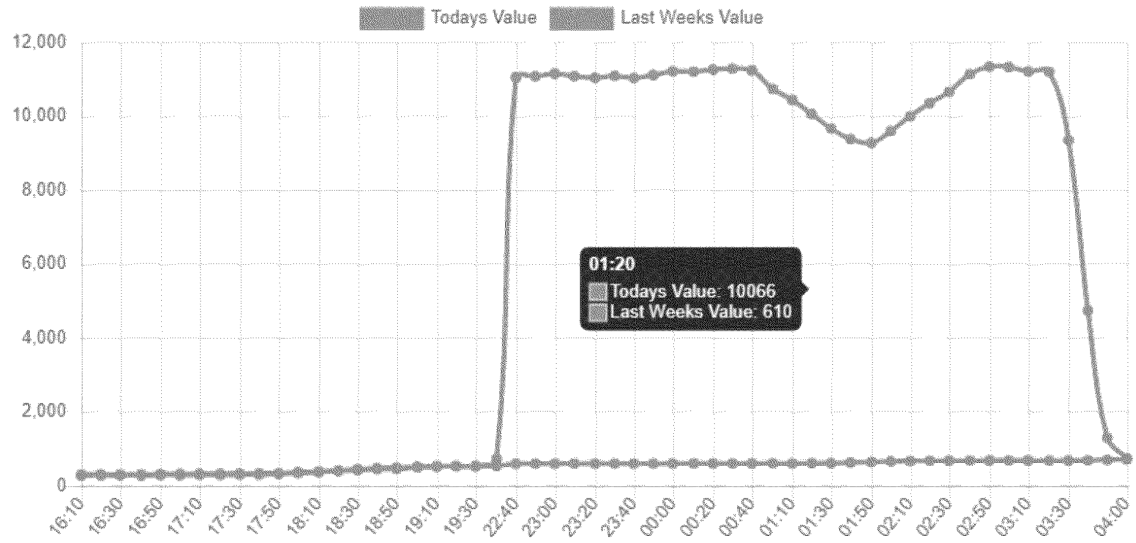
Example branch traffic during the impact - about 1 transaction per minute was observed between 19:47 and 22:12.

Below is a EPOSS transaction comparison graph 13/14 March vs 27/28 March 2023:

FUJ00171946



Non-polling counters comparison graph:



The batch schedule delays were observed, but all files delivered within agreed time. Example: previous week Santander GIRO files were sent to NBIT at 20:50, on 27.03.2023 they were delayed to 22:20.

EPAY service was impacted by this issue from 19:47 until 22:12.

SSN access was affected as well causing impact to monitoring tools such as HORIce, PODG Reporter.

2 Post Incident Review Notes

OBSV1: Underlying cause of the issue – investigation with the vendor.

See action 1.

OBSV2: The IRE11 Galleon server could face the same GPS Antenna issue anytime and cause further live service impact.

FUJ00171946

See action 2, 3 and 4.

OBSV3: Need to establish how the time service is provided to the POL Counters.

See action 5.

OBSV4: Issue with 2012 Windows NTP setting time when difference is greater than 5 mins.

See action 6.

OBSV5: We need to make our time solution more robust. We should also have MSF (Radio) signal received and GPS in NTPs in IRE11 and IRE19. Relying only on GPS signal could be risky, given it could face aerial issue or be turned off unilaterally by the GPS solution provider (United States Air Force).

See action 7.

OBSV6: Need to update Galleon firmware. The update will prevent time reset to default

See action 8.

OBSV7: When investigating the incident on the tech bridge, it was spotted that there are different configurations on the NRP servers. Some of them had multiple entries of time servers and some of them only had one entry.

See action 9.

OBSV8: The IRE11 and IRE19 Galleon servers - are they load balancing, or do we have a primary and secondary?

See action 10.

OBSV9: It appears that SMC junior staff was covering the nightshift when the issue occurred. POA OOH DM had an impression of SMC engineers being unsupportive on the tech bridge call, not responding to requests, there was no Minimum Data Set ready on time and there was no mention of the Counter Super Event incident for at least 2 hours since the impact started.

See action 11.

OBSV10: Check with SecOps how often SOC 24/7 log into their accounts. Not enough support from other engineers until James Horsfall joined the investigation.

See action 12.

OBSV11: Review possibility of improving the NTP solution – cloud source etc.

See action 13.

OBSV12: In POL Major Incident Review meeting, a potential impact to audit was discussed and POL requested Fujitsu to check Audit logs to ensure no transactions have been dated 2003.

See action 14.

3 Recommended Actions

Act	Action	Actionee	Target/Status
1	Investigate the underlying cause with vendor Galleon.	Shaun Wood	Closed completed 28.03.2023
Closure/Comments: 28.03.2023: Shaun Wood: I have raised this with Galleon who have advised the following **"*The 2003 date issue you're experiencing is due to the GPS antenna rolling over, to resolve it a new antenna is required. Re 'rolling over', all GPS antennas have a counter inside them that when exceeded will reset itself.*"**			

FUJ00171946

Owing to the above, the Root Cause Statement was produced, please refer to section 2.3 of this report. **Action closed as completed.**			
2	Remove the IRE19 Galleon Time Sync server IRRELEVANT from LAN to prevent further issues.	Shaun Wood	Closed completed 28.03.2023
Closure/Comments: 28.03.2023: This has been completed under internal change CHG0361340. HES engineer removed the LAN cable from the IRE19 Galleon Time Server - IRRELEVANT IRRELEVANT **to ensure that it does not provide a time service to clients due to GPS Antenna issues.**			
3	Restore the IRE19 Galleon NTS-6002 server and fix the GPS Antenna issue in both servers.	Shaun Wood	Closed completed 03.04.2023
Closure/Comments: 28.03.2023: Update from Shaun Wood from Galleon regarding debug, public time source and possible diagnosis for IRE11 Galleon server: Not much value in debugging the time server. The debug shows the time information coming from the antenna, in case of an issue with the antenna, we will get an event and some warning, but we cannot tell when it will go wrong. It was confirmed that if the running IRE11 Galleon Time Sync server was not able to get a time source due to potential GPS Antenna issue, then the client devices should ignore it and the client should then pull back to their own internal clocks i.e. network devices would then start using their clocks. This situation creates a risk to live service as stability of the service can be guaranteed only if all the devices within the service infrastructure refer to the unified time source – therefore the NTP solution is in place. As a preventative measure to limit this risk, Galleon vendor suggested the antenna cable should be removed from IRE11 Galleon server to prevent the GPS reset-to-default time issue. Galleon engineer's visit to IRE11 and IRE19 has been arranged for Monday, 03.04.2023, 10:00. The aim of the visit is to replace the faulty antennas, test the existing cabling, connect to the new antennas, test the MSF aerials. **31.03.2023:** CHG0362095 (POL change ref. CHG0053803) raised to cover the Galleon engineer visit in IRE11 and IRE19 on 03.04.2023 to install replacement antenna and recommission time server. Time server is currently isolated from the network, and engineer will require site access (including live comms rack access) to connect new antenna located on outside of the building. Once new antenna are connected, device time sync will be tested and verified. Pending verification of time sync – time server will then be re connected to the network and peering with IRE11 to be re-established. **03.04.2023: Following CHG0362095 activities, IRE19 Galleon server is now all fixed, the Galleon engineer has jointed the new cables and made good all connections including the connection into the back of the IRE19 Galleon Time Server. We have a good GPS / MSF signal are IRE19 and this is now offering out a time service and chatting to the IRE11 Galleon Time Server.** **The "peer" setting on the IRE11 Galleon Server has been re-added and this is now chatting to the IRE19 Galleon Time Server.** **Action closed as completed.**			
4	Raise a service risk.	Piotr Nagajek	Closed completed 28.03.2023
Closure/Comments: 28.03.2023: Extreme service Risk 601 Risk Plan - Time Sync Service Risk (sharepoint.com) **raised for the running IRE11 server can face the same issue at any point.** **As a preventative measure to limit this risk, Galleon vendor suggested the antenna cable**			

FUJ00171946

should be removed from IRE11 Galleon server to prevent the GPS reset-to-default time issue.			
5	Need to confirm how the time service is provided to the counters. What responsibilities we have documented? POL to confirm with DXC and Verizon.	Matthew Hatch, POA Service	Closed completed 06.04.2023

Closure/Comments: 29.03.2023: As part of the tech bridge call that Matthew Hatch was holding with Post Office and DXC, the question about the time service at the counters was asked, however DXC were not able to answer.

Ravi (Saini) confirmed to Andrew Hemingway that as a part of the migration to Verizon, we made a network time source available via our router handoffs.

There is a document called EUC responsibilities – what responsibilities have we documented?

To be reviewed within the POA Service team first.

03.04.2023: An extract from *End User Compute Towers Responsibilities and Requirements for Horizon Anywhere* document (REQ/SIR/SRS/2605):

3.8.1 Time Synchronisation

The EUC tower will provide time sync service to the HNG-A counter. The system clock will not "drift" from real time by an amount agreed between Fujitsu and Post Office. Note that the provision of the NTP time service was the subject of GAP analysis change request HNG-A CP1563, it will still be the requirement that EUC will configure the O/S to set the time correctly.

The HNG-X time servers will be part of the same time service as the Verizon (network providers) time servers. The Verizon routers in Fujitsu data centre will obtain their time from the HNG-X time servers. The HNG-A counters will indirectly (via EUC and AD) take their time from the Verizon servers. Hence they will all be part of same time service system allowing correct time synchronisation.

Reviewed the statement on the POA Service Team Weekly Round-up.

06.04.2023: POL provided a statement on this action from Verizon and DXC:

DXC:

"We *don't use Fujitsu to synchronize the time in Azure.*

The time on PDC is synchronized with AZURE Stratum 2 internal NTP provider.

All the servers in the AD synchronize with PDC."

Verizon:

"*For the POL core network, branch network, branch test network and the admin network, Verizon use Fujitsu's NTP servers located in IRE11 and IRE19. Having said that, I've been assured our network would not fail with the loss of NTP time sync from these NTP servers.*

There have been discussions recently about the strategy for NTP once the FJ data centres close, as NTP cannot be hosted in the AWS cloud."

6	INC12598983 / PC0305349 raised to investigate the issue with 2012 Windows NTP setting time when difference is greater than 5 mins.	Shaun Wood, Mike Conneely	Target date: 31.05.2023

Closure/Comments: 28.03.2023: Shaun Wood: *This incident has been raised to investigate why the NTP service on Windows 2012 R2 platforms did a date / time leap from 2023 back to 2003 as this was the date provided by the IRE19 Galleon Time Server, such a large gap should not normally be acted upon by a time service as is far exceeds a certain tolerance range.*

On the Linux Platforms the NTP daemon didn't change to the 2003 date and the NTPD daemon stopped, and the time/date remained unchanged on the server.

Mike Conneely*: Looking at the Windows NTP config, it doesn't have the following option set which is present on Linux servers: "tinker panic 300".*

FUJ00171946

The current value used for Linux, 300, should cause NTP to abort if the time server is more than 300 seconds difference from the client. That said, it's supposed to have a default of 1,000 seconds so, if Windows supports it, it doesn't explain why any of the Windows 2012 servers would change the time back to 2003.

What might explain it is a message seen in the Windows event logs, at the time of the issues on the 27th, where the NTP service states 'using Windows clock directly'. That implies it's falling back to the time value in the CMOS clock, virtual in this case, and it's something that could be checked in case it's got, or might have had, a value of 2003.

If falling back to the CMOS clock is potentially an issue, it can be excluded as an option in the NTP config on Windows.

The revised config would therefore be to include 'tinker panic 300' and to exclude the hardware clock as fallback.

Shaun Wood: *I have checked the changelog for Meinberg NTP and since our current version these are 1828 Bug/Sec/Other changes*

I have checked on the Windows NTP software provider site :-

https://www.meinbergglobal.com/english/sw/ntp.htm#ntp_stable

Their change log shows the following release fate on 2011 for the version we have running on all Windows Platforms making this 12 year old.

(4.2.6p5) 2011/12/24 Released by Harlan Stenn GRO

The latest version is 4.2.8p15.v3 from 24th February 2021.

PC0305349 to go through the BIF/PTF route for approval to proceed with testing and if successful, live implementation.

30.03.2023: Michael Conneely: *Having checked in source code for the version of NTP we're using on Windows, it does look like it'll be using the default of 1000 for 'tinker panic' so changing it to 300 will make little difference.*

What seems to have been the issue is the Windows NTP service being restarted, by ntpmon, when it wasn't at stratum 2.

It looks like it's applied the iburst setting, at startup, to quickly stabilise NTP and that the 'tinker panic' value only applies to steady running. The restart was initially introduced on BPL servers at the time when they were acting as time sources for the counter estate and were losing their stratum level even when the higher level time sources were working. It's probably unnecessary across all Windows servers that run the NTP service and could operate like Linux where it's an alert only.

On Linux, where it only alerts when the stratum is incorrect, rather than restarting the NTP daemon, there were no issues other than correctly reporting, in ntp.log, that the time source difference was too great.

It's definitely worth updating the Windows NTP to a newer version given that the version deployed is based on an ntp.org release that's 12 years old. It's likely that any newer version would minimise the instances of stratum being incorrect as long as the higher level time sources are available.

04.04.2023: PC0305349 reviewed in the BIF/PTF meeting. Proposed for next Sysman Maintenance Release 44.09. 8th of May is Integration date for the Release.

13.04.2023: PEAK PC0305349 is progressed in test. 31st of May 2023 is the live date for Release 44.09.

7	Test new MSF aerials for IRE11 and IRE19 Galleon servers. If successful, this gives a resilience to the GPS signal.	Shaun Wood	Target date: 24.04.2023

FUJ00171946

Closure/Comments: 29.03.2023: Shaun Wood: We have bought new MSF aerials for IRE11 and IRE19 Galleon servers. Testing the MSF signal to be performed during the Galleon engineer visit in Belfast. If this is proven to be working, this gives a resilience to the GPS signal.

31.03.2023: CHG0362095 raised to cover the Galleon engineer visit in IRE11 and IRE19

03.04.2023: Following CHG0362095 activities, IRE19 Galleon server is now all fixed. Awaiting outcomes of the IRE11 site survey.

Shaun Wood: Richard Hawkesford (Galleon Engineer) has visited the IRE11 site and completed a site survey which included checking the existing GPS/MSF antenna. A second site visit is now being arranged to replace the IRE11 GPS / MSF antenna.

IRRELEVANT - IRE11 - Galleon - NTS-6002 - GPS & MSF (Old Antenna MSF not working) -

IRRELEVANT - IRE19 - Galleon - NTS-6002 - GPS & MSF (New Antenna both working) -

14.04.2023: The second visit of the Galleon Engineer has been arranged for Monday 24th April when he will attend IRE11. Fujitsu change reference: CHG0365831. He will install the new GPS/MSF antenna and then connect these to the Galleon NTS-6002 Timer Server and perform health checks of the GPS/MSF signals.

8	Once Antenna issue is fixed on both Galleon servers, update of the Galleon firmware to be scheduled. High level plan: fix IRE19 Galleon antenna -> Update IRE11 -> Update IRE19 -> Get the antenna issues fixed in IRE11.	Shaun Wood	Closed completed 14.04.2023

Closure/Comments: 29.03.2023: Shaun Wood to monitor this and raise change for the upgrade.

04.04.2023: Shaun Wood: Change request CHG0362793 has been raised to upgrade the firmware on the IRE11 Galleon Time Server from V12#9 to V12#11 which is the latest version which doesn't set the clock back due to a faulty GPS antenna. This is planned for implementation this Thursday 6th April at 18:00. A further change request will be raised to upgrade the IRE19 Galleon Time Server from V12#9 to V12#11 on Thursday 13th April at 18:00.

06.04.2023: The IRE11 Galleon NTS-6002 was successfully upgraded to the latest firmware this evening.

14.04.2023: Completed. The IRE19 Galleon NTS-6002 Timer Server was successfully upgraded to the latest firmware last night under change request CHG0364035 (POL change: CHG0053971). This now completes this upgrade as both of the Galleon NTS-6002 Timer Servers are now on the latest version of firmware.

Shaun Wood additionally checked with Galleon on the Warranty of our two Galleon NTS-6002 devices. We have 3 years of warranty left on them which is good news and will take us to 2026.

9	Infrastructure review exercise to ensure that unified, correct configuration is applied on all devices.	POA Infrastructure management, Networks	Target date: 28.04.2023

Closure/Comments: 29.03.2023: Shaun Wood: all devices within the system should always have both time servers configured and it came to the light that this is not the case.

Suggestion: Configure DNS naming rather than IP address on the devices.

Andrew Hemingway: Networks to use Cisco Prime to get that info. This action needs to have multiple owners, depending on the platform.

Need to understand why NRP008 stayed all despite all the event that led to the incident. Need to check version of the NTP software on the devices, not only NRPs. To be a part of the Infrastructure Review Action.

FUJ00171946

NTP pings and debug firewalls for any rejections etc. - part of the exercise.

Need to understand what devices were impacted by the issue, but the impact did not manifest.

04.04.2023: Meeting scheduled for 05.04.2023. Updated Action details following feedback from Andrew Hemingway:

- Agree Networks should be able to run a report on Cisco Prime to understand the NTP config on all managed Cisco network devices.
- Configure DNS – potential service improvement.
- Need to understand why NRP008 stayed – SOC ECS to check all NRP config.
- Need to understand what devices were impacted by the issue, but the impact did not manifest - all system administrators / solutions owners to review NTP settings.

Shaun Wood: We currently have two Galleon NTS-6002 Time Servers which provide the time service to all datacentre platforms including servers, network devices, appliances, blade frames, storage etc. The Symmetricom Time Servers were decommissioned in 2021 and their DNS entries (lprnt001/lprnt004) were updated to point to the IP addresses of the Galleon Time Servers, this was done so that the NTP config on all servers didn't require an update.

All network devices, appliances, blade frames, storage etc should be configured with the following time server entries and should ideally use the hostname if they are able to resolve DNS, if this is not possible then the IP address. As part of the PIR for the Time Service issue this was one of the follow-on actions as during the issue it was noted that the BlueCoat Reverse Proxy systems didn't all a common set pf NTP server entries so these do need to be updated to have both of these hostnames / IPs configured.

This is covered by PIR Action 9 which is with Andy Hemmingway.

Hostname (DNS resolvable)	IP Address
IRRELEVANT	IRRELEVANT

IRRELEVANT - IRE11 - Symmetricom - Atomic & GPS - IRRELEVANT
(Decommissioned in 2021 – The DNS entry points to lprnt002)

IRRELEVANT - IRE11 - Galleon - NTS-6002 - GPS & MSF (Old Antenna MSF not working) -

IRRELEVANT IRE19 - Galleon - NTS-6002 - GPS & MSF (New Antenna both working) -

IRRELEVANT - IRE19 - Symmetricom - Atomic & GPS - IRRELEVANT
(Decommissioned in 2021 – The DNS entry points to: IRRELEVANT

05.04.2023: Attendees: Andrew Hemingway, Ankit B.Agarwal, James Yates, Mahesh Gandhi, Piotr Nagajek, Jason Kidd, Pravin Gotur, Shaun Wood, Shashank Kulkarni, James Horsfall, Nikhil Bhagade, Vishal Pathak, Amar Dafal

Please see summary of the meeting and the agreed actions below:

- **Agree Networks should be able to run a report on Cisco Prime to understand the NTP config on all managed Cisco network devices.**
  - Chris Harrison already requested Networks to check the NTP configuration on various devices whether it is being synced with IRE11 Galleon or IRE19 Galleon. Networks have pulled the details manually and via Cisco Prime. Networks to produce an Excel spreadsheet with the details of each reviewed device and provide for further review if config changes are required. **Target date: 11.04.2023**
  - **11.04.2023:** Networks (Shashank V Kulkarni): As discussed over the meeting invite

FUJ00171946

last week, we gathered the data for devices with NTP server sync issues. Kindly do refer the attached template showing the same.

We've highlighted the devices which are already in sync & which are not in sync with NTP server hosted at IRE11 & IRE19.

NTP-Statistics-Updated.xlsx

18.04.2023: Chris Harrison confirmed this was analysed and the below workaround was planned for the required devices.

NTP status-cisco prime.xlsx

NTP workaround.docx

Omkar Rangam to arrange relevant changes.

- **Configure DNS – potential service improvement.**
  - AH: This is an individual service improvement. Need to be on the CSI item list. This needs Solution Architect's view.
  - Data provided by Shaun could be useful there. General recommendation is to config items to use the hostname rather than IP Address of the time sync server. It's more beneficial to have the host name configured - that way the device uses DNS to resolve the IP address. It is possible that if we decide to move the time server to different IP address, then DNS would be updated with its new IP address. That would then mean all the end systems would not need to have any conflict changes done on them.
  - Future service improvement, Refresh 3 will be probably looking into it.
  - Piotr to add a new item to the Internal CSI Spreadsheet and track the action there. Internal CSI item INTCSI008 raised. **CLOSED**
- **Need to understand why NRP008 stayed – SOC ECS to check all NRP config.**
  - NRP008 was configured to take the time from IRE11 Galleon server, while other live NRPs were configured to take the time from IRE19 Galleon which failed. I.e. NRPs 005, 006 and 007 had the IRE19 Galleon server set as primary.
  - NRP config work required - IRRELEVANT to be pointed to the IRE19 Galleon server first, and IRE11 Galleon second. IRRELEVANT to be pointed to the IRE11 Galleon server first and IRE19 Galleon server second. This is recommended, most logical way of setting up the live NRPs.
  - AH: Is there a time service design? Shaun: Service should work in the way that it speaks with all time servers within configuration and it should be able to determine which one provides good time.
  - Recommendation for the NRP config change described above to be sent to Network Design Architects Ravi Sani and Dave Haywood for review. **Action on Piotr to type an email to Ravi and Dave. Email sent – see attached.**

    19.04.2023: Chaser sent by PN to Ravi and Dave.
- **Need to understand what devices were impacted by the issue, but the impact did not manifest - all system administrators / solutions owners to review NTP settings.**
  - Need to reach out to non-Cisco devices owners.
  - Shaun Wood: All the servers are configured correctly; they don't need to be checked.

FUJ00171946

	We know that because they have been configured by the same baseline. It's rather Network device appliances, blade frames, non-server type devices need to be checked. ○ Action assigned to Andrew Hemingway. Need more time to plan this. Review on Thursday next week (13.04.2023). ○ **19.04.2023: Chaser sent by PN to Andrew Hemingway.**		
10	Understand the relationship between the two Galleon servers.	Shaun Wood	Closed complete 29.03.2023
Closure/Comments: 29.03.2023: Shaun Wood: We do not have a primary and secondary. The two Galleon servers run as a unit, and we have them peered. What they do is they are able to see their time sources from the GPS or MSF (Radio) and they are also able to see the other time server in the other data centre. So they communicate between themselves and they are able to identify any delays in the time, because obviously it takes X amount of milliseconds to send a packet from one data centre to the other. So the Galleon servers then offer out to all their clients a time service and a client will call in and it will work out, which is the most reliable and closest time service.			
11	SMC Service Improvement Plan to be established and progressed.	POA Service Management, Jerry Acton	Target date: 28.04.2023

Closure/Comments: 29.03.2023: SMC shifts:

- Early Shift (09:30 to 17:30 BST) or (8:30 to 16:30 BST Day light saving)
- Late Shift (17:30 to 2:30 BST) or (16:30 to 1:30 BST Day light saving)
- Night Shift (2:30 to 9:30 BST) or (1:30 to 8:30 BST Day light saving)

Need to review how many SMC engineers are on the shift? When is the shift handover?

31.03.2023: Incident Management team produced a list of observations for the SMC Improvement Plan and sent to Jerry Acton (SMC SDM) for review with SMC Management. The list contains observations from this incident:

- Observation from the “Galleon” incident: It appears that SMC junior staff was covering the nightshift when the issue occurred. POA OOH DM had an impression of SMC engineers being unsupportive on the tech bridge call, not responding to requests, there was no Minimum Data Set ready on time and there was no mention of the Counter Super Event incident for at least 2 hours since the impact started.
- Initial SMC shift appeared to be in experienced and lacked the knowledge to deal with the issue.
- SMC having issues with raising the MDS to log an incident with POL
- Not responding to asks on the technical bridge. Quiet and non-responsive.
- Unsure if the SMC escalated to Ramana or not.
- Better traction from the SMC once additional staff joined the technical bridge.
- Asked for impact details but could not be provided
- The SMC could have compiled a spreadsheet of all the incidents raised so they could be assessed on the technical bridge.

See full list attached:

FUJ00171946

SMC Issues March 2023.docx

05.04.2023: The plan is under review between Jerry Acton and SMC Management. Meeting to review the progress set up by POA Service Team for 18/04.

SMC MDS Mock Drill meeting re-instated starting from Wednesday 19/04.

19.04.2023: MDS Mock Drill exercise completed. Outcomes attached.

RE_ MDS Mock Drill - Scenario 25.msg

Matthew Hatch and Jason Kidd are working on the SMC tracker of issues. Updates to follow.

12	Review with SecOps how often SOC 24/7 log into their accounts. Review the support quality.	POA Service Management, James Yates	Target date: 21.04.2023

Closure/Comments: 04.04.2023: POA SecOps to be engaged as the owner of relationship with SOC.

James Yates sent the below email to SecOps:

IRE19 Galleon PIR .msg

12.04.2023: Response from SecOps:

Who in the SOC 24/7 team has an MSAD account?

- Various team members within ATC have access via MSAD and are managed using the AD templates to ensure minimal access.
- The 24/7 team have 2 login's one for MSAD and one for the NSM box which is managed by the ATC infrastructure team this team only manage the IDS box at this time. Are we sure this is the team from the Major Incident?

Are there records or a way to determine how often people log into their accounts? If so, can this information be shared with the Service team?

- All MSAD accounts are reviewed by the SecOps team weekly and any accounts over 90 days are disabled.
- The 24/7 team has high focus with there MSAD accounts and we do regularly review with the team leads for this team as well as 2nd line to ensure logins are regular to cover shifts and on call, if this is the right team we would need to understand who had the issues to identify with the leads as to why this failed.

How long do the logins last before they require a reset or become inactive due to no usage?

- It is unclear the exact time but believed to be between 30 and 45 days although ikeys are more frequent

Is there something in writing instructing holders of the accounts to log in on a regular basis to ensure that the accounts are kept active?

- There are frequent reminders to login to ikey (means you have to access MSAD as well) sent out at the start of every month by POA User Management to all MSAD account holders this is sent at the same time as the team verification.

19.04.2023: PN emailed James and Andrew Hemingway to confirm if the actions can be closed.

FUJ00171946

13	Improve the NTP solution. E.g. research cloud-based time sync solution	POA Infrastructure Management	Closed completed 05.04.2023

Closure/Comments: 05.04.2023: During the 2nd PIR Meeting it has been agreed that a designed NTP solution is enough when fully fixed. For details of the fixes please refer to Actions 7 and 8 of this PIR.

Closing this Action against PIR Action 7 and 8.

14	Fujitsu to check Audit logs to ensure no transactions have been dated 2003.	Gerald Barnes, SecOps	Target date: 20.04.2023

Closure/Comments: 06.04.2023: Piotr reached out to Gerald Barnes to assist. Response from Gerald Barnes:

For LST the audit logs will definitely have dates from 2003 in. I do not even need to ask to get them back to say that. I have already received some with the incorrect dates in to investigate some knock on incidents. See the first attachment.

RE TWS job SSC_GATH_JOURNAL.

Are you, in general, asking about LST or live?

The second attachment says there was no problem with live but I wonder where the IRE19 live audit server gets its time from.

RE TWS job SSC_GATH_JOURNAL.

18.04.2023: Following further conversations, Gerald Barnes requested SecOps to perfom the following:

Please try and do the following to check to see whether there are any transactions with the wrong date.

Run a query for audit point BRDB and sub point AUD and also (at the same time) audit point AUDIT and sub point HxLog1 for the date 27th March 2023 to 28th March 2023.

Delete the files with sql in displayed.

Retrieve all the files. This may take a while.

Now do a free text abstract search for <Date>2003

See what the size of the QUERY_AT/FINAL/Filteredhx.xml file is on the audit server. If it is bigger then 0 try and get it back to the audit workstation for further analysis. It might be very big.

Hassan Shakeel is performing this task, ETA is 20.04.2023.