Troubleshooting Procedure

**Playbook for Troubleshooting**

**Version 0.1**

**IT4A Ref. IT4A-PR-159**

Publish Date

**08/11/2022**

Author: Adrian Clive Prasad

Approved By:

## Table of Revisions

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Description | Author | Date |
| 0.1 | Draft | Adrian Prasad | 08.11.2022 |
|  |  |  |  |

Table of Contents

[Introduction 3](#_Toc121322542)

[Background 3](#_Toc121322543)

[Purpose 3](#_Toc121322544)

[Scope 3](#_Toc121322545)

[Types of faults 3](#_Toc121322546)

[Communications: 3](#_Toc121322547)

[Power 3](#_Toc121322548)

[Hardware: 3](#_Toc121322549)

[Human error: 3](#_Toc121322550)

[Configuration 3](#_Toc121322551)

[Compromise 3](#_Toc121322552)

[Service Desk Process 4](#_Toc121322553)

[General Steps to be taken (Service desk) 4](#_Toc121322554)

[Check N Central: 4](#_Toc121322555)

[Try and ping the Site as well as the sim address: 4](#_Toc121322556)

[Contact the site engineer or the relevant professional 4](#_Toc121322557)

[Reboot the device if the SIM address is reachable. 5](#_Toc121322558)

[Access syslog data and determine cause 5](#_Toc121322559)

[Steps to be taken 5](#_Toc121322560)

[Sutton East and Surry Water 6](#_Toc121322561)

[Communications (SESW): 6](#_Toc121322562)

[Power (SESW): 9](#_Toc121322563)

[Hardware (SESW): 9](#_Toc121322564)

[Human error (SESW): 9](#_Toc121322565)

[Configuration (SESW): 9](#_Toc121322566)

[Compromise (SESW): 9](#_Toc121322567)

# Introduction

The troubleshooting Playbook has been written for the IT4A engineer tasked to remedy issues arriving on the NOC and SOC service desk in a timely manner.

# Background

IT4A have developed many procedures over the years but have failed to create a consistent and sustainable library of proven troubleshooting, investigation, and remedial methods to aid an individual tasked to remediate issues.

# Purpose

To provide the service desk engineer with a library of proven methods to remedy the most common faults detected by the service desk

# Scope

* Managed Service Customers
* Internal Systems
* External Systems (Telecoms, service portals, DNS, SSL, Web site, etc)
* Standard products

# Types of faults

Experience tells us network issue result from one or more of the following:

# Communications:

Comms issue, ADSL line down, SIM unreachable.

# Power

UPS down, Power line down etc

# Hardware:

Hardware/ physical damage, temperature etc

# Human error:

Issue caused due to human mistakes (Mis-patch, depower, etc)

# Configuration

Issues caused due to misconfigurations of the device/appliance.

# Compromise

Issues caused due to wrong configurations of the device/appliance

# Service Desk Process

The IT4A service desk process is as follows:

* Monitor and Capture
* Detect
* Assess
* Prioritise
* Resource
* Remedy
* Return to Service

## Monitor and Capture

Device status and condition are polled using SNMP to pull device specific information into a Remote Monitoring and Management (RMM) software. Exceeding a threshold will trigger wither a warning or a failure event to be generated and passed to IT4A’s Professional Service Automation (PSA) tool in the form of a trouble ticket. SLA timers are started when the trigger is activated and stopped once remediation is complete. Tickets are put on hold when third party intervention is requested and released from hold once a response is received.

*To be continued with a section for each topic explaining method*

# General Steps to be taken (Service desk)

# Check N Central:

The first course of action to be taken must be check the status of the device on the n central monitoring platform as well as check the report on the particular device that is down.

# Try and ping the Site as well as the sim address:

If N central check is not helpful, then the personnel must manually ping the address of the device or use a tool such as multi ping. If the L2TP addresses are not reachable then the SIM addresses (if the device has it) must be tried to be pinged. If both the sim addresses as well as the L2TP addresses are not reachable then we suspect that the issue might be Loss of power (speculative at this point in time).

# Contact the site engineer or the relevant professional

If there is a suspected power issue or any disconnection from the device, email or ring up the relevant engineer and provide them with the details about the device. The details for the device would be : Name of device, Location of the device, ID of the device, Photos (if available) of the device.

# Reboot the device if the SIM address is reachable.

If the device is reachable from its SIM address,(commonly for the robustel router for SESW sites) then login to the respective device and then navigate to check the status of the L2TP lines of the device. If the device states that the L2TP connection is disconnected or unavailable then navigate to the power setting of the device. Make sure that rebooting the device does not affect any live client networks or systems that maybe working or dependent on that device. Once it is safe, reboot the device and wait for the device to restart. After the device restarts, monitor both the L2Tp as well as the SIM addresses of the device. This must solve (in most cases) the L2TP issue that the respective device was having. If the problem persists go back to step 3. After step 3 is completed go to step 5

# Access syslog data and determine cause

If the device is accessible and yet the line or the device is not working as intended, then login to the device and navigate to the logging section of the device. Examine the syslog that the device has sent before and after the disconnection. This will help to troubleshoot the problem as well as help in the case of an incident to create an RCA report for the incident.

# Steps to be taken

When an issue is considered in order to troubleshoot it the following steps must be taken:

## Identify site and customer:

The site at which the fault has occurred must be determined as well as the issues with the site in question must also be considered for the troubleshooting of the issue.

## Determine type of fault:

Check what services are still up and running and check what services are down, By looking at these as well as the previous ticket we can narrow down the type of fault that has occurred at the device/site to raise this issue.

## Evaluate with preliminary checks:

Using tools like Multiping and manually pinging from the relevant server we must determine the path of the connection and where in this path the device resides. This also can be done using traceroute or other commands.

## Identify type of device:

The device or the line that is having an issue must first be classified and identified. This is done due to the fact that different devices have different issues and their respective different solutions.

## Determine point of failure:

Determine which device/ port or process has failed. Determine the way to navigate to it and then attempt to isolate the single point of failure and its reason.

## Fix the issue or raise a ticket for third party to resolve:

After the identifying the problem reboot, fix or raise a ticket to the third party regarding the issue in order to solve the problem.

# Sutton East and Surry Water

Experience tells us network issue result from one or more of the following:

# Communications (SESW):

Most of the SESW site devices have 3 IP addresses that can be used to ping and await a response from the router.

First check N Central

**If the L2TP address is unreachable and 4G interface is reachable**, then we can follow the following steps to login to the router and reboot the router:

Rebooting the router may be necessary for a maintenance procedure or to troubleshooting any issues with the router.

1. Log in to the DMZ PC using VMWARE and ping the SIM IP address for respective site.

Graphical user interface, application, table

Description automatically generated

Figure 12

2) In the web browser, navigate to the SIM IP address (found in the SESW ORI ASSETS) of the router using HTTPS, for example https://100.70.16.44 as shown in below figure.

Graphical user interface

Description automatically generated

Figure 1

3) Once logged into the router as mentioned earlier in the document, navigate to “status/Reboot” as shown in figure 2Graphical user interface, website

Description automatically generated

**Figure 2**

4) The router in this example will take approximately 60 seconds to reboot and get the VPN connected

**If there is ADSL Line failure or unstable ADSL:** then we can follow the following steps to check if the connection from Hightide is good or not:

1) Login into Hightide portal and enter the username and password and click “Sign in” as shown in Figure . The login credentials are kept with the Pass portal.

Graphical user interface, text, application

Description automatically generated

**Figure 3**

2. Under Customers, click List

3. Choose the site ITAUTO-SESW (P-IT4AUTO-SESW - 45)

4. Check the Connection status

Table

Description automatically generated with medium confidence

**Figure 4**

If the connection is not online, please raising a ticket with IT4A datacentre by sending email to High Tide Support <support@hightidegroup.net>

Andrew will run line test and confirm whether this is CPE issue or BT line issue.

# Power (SESW):

**If the ADSL, L2TP and 4G interfaces are unreachable,** then check the dataflow (from the DMZ system and the respective site). It is probably a power issue at the site. In this case contact the engineer (Luis Lazarte) so that a on-site inspection will help us to troubleshoot the problem. If possible request the engineer to check the power supply and reboot the device.

# Hardware (SESW):

Hardware/ physical damage.

**When a Temperature** **warning is display on N Central regarding a device:** Contact the site engineer regarding the temperature of the device and request them to fix the issue in order to avoid hardware issues etc

# Human error (SESW):

**When there are login failures:** Follow up with the relevant customer contact and enquire if the login attempts were genuine failed login attempts rather than an external cause.

# Configuration (SESW):

Issues caused due to misconfigurations of the device/appliance.

# Compromise (SESW):

**Use the daily Graylog monitoring system to detect intrusions** and if intrusions are detected **:**

Investigate the logs captured by graylog

Determine the Source Device, Source IP, Source port, destination device, destination IP, destination port.

Investigate and determine a cause for this intrusion and create and Root cause analysis for the issue. Record the incidents and save it in the “LFE” folder in the customer/SESW/troubleshooting procedure.

**Features**

**Generalised troubleshooting**

Since the playbook generalises the methods it is applicable to a very wide type of devices.

**Quick troubleshooting**

Allows us to quickly identify and solve any issues that may come up.

End of Document