*Make the Cloud Yours!®*

# Post Incident Report - 2020-03-30

**Descriptive Name:** SSO outage

**Incident Reference Number**: 20200330

**Date of Incident:** 30/03/2020, Monday

**Time & Duration of Incident:** 16:50 to 18:45AEST, 1hr 55min

**Severity**:
☒ Service Effecting ☐ Access Effecting
☐ Performance Effecting ☐ Network Effecting

**Location Effect**:
☐ Isolated school ☐ Host + all VMs
☐ Sub-Net ☒ Muiltiple schools

**Services Affected:** - SSO login from any location inoperative.

**Incident Cause**: - Cloudwork SSO service experienced a DOS like surge of sign in activity on Monday morning

- Adjustments to resource allocation and configuration were made late in the afternoon to optimise configuration of resources

- These adjustments unexpectedly triggered a resource overload requiring the container swarm to be restarted.

- Subsequent analysis on Tuesday 31/3/2020 determined that authentication volume was not legitimate activity. Volume was generated by a misbehaving app continuously completing successful sign on requests hundreds of times a minute.

**Incident Resolved**: ☒ Yes ☐ No ☐ Open

**Time of Resolution:** 17:15, 30/03/2020, Monday

**Restoration Timeframe**: 1hr 30mins 00secs

**Issued By:** Technical Support, support@studentnet.net & support@coherentcloud.com

**PIR Issue Date**: 01/04/2020

**Strictly Confidential**

***Make the Cloud Yours!***®

**Contact Information:** Please report any continued service disruption ***immediately*** to :

Studentnet NOC Support: +61 2 9281 3905
Support Email: support@studentnet.net support@coherentcloud.com

**Incident Description**

**30/03/2020**

- 08:30-09:30 Extraordinarily high sign in authentication activity observed
- Expectation was that this reflected legitimate extra traffic caused by schools moving en mass to remote learning work models as a result of COVID-19 pandemic
- Planning commenced to audit resources allocated to critical processes and heavily utilised schools
- 16:50 Re-allocation of resources commenced including creation of new containers
- New containers created exceeded a pragmatic limit overloading an instance in the swarm
- Overload rapidly spread through whole swarm disabling operation of the swarm
- 17:10 – the situation was recognised and work commenced on re-establishing communication to the swarm in order to regain control
- 17:30 – homepage and support page of Studentnet website(studentnet.net) were updated advising of SSO outage and requesting schools to contact office(02 9281 1626) to leave a mobile phone number to which status notification SMS texts could be sent
- 17:52 – first status notification texted out to all reporting schools:
  - "*Studentnet SSO service outage for some schools. Our tech team is currently working on resolving. Update will be advised via SMS to follow.*"
- 18:27 – second status notification texted out to all reporting schools:
  - "*SSO outage update: Our tech team is regaining control of our swarm. We expect to be restarting schools within 30minutes.*"
- 19:08 – third status notification texted out to all reporting schools:
  - "*All Cloudwork SSO services successfully restored. Please report any further issues to our NOC on 02 9281 3905. PIR to follow tomorrow.*"
- 19:15 – Outage notice removed from Studentnet website home and support pages

**31/03/2020**

- Continued investigation of surge authentication loads identified a single school responsible for vast majority of load
- Investigation of that school's activity identified a single app responsible for generating the huge volume(hundreds a minute) of successful authentications
- Further testing and investigation successfully reproduced the inappropriate authentication behaviour of the app.
- Determined that the app caches the username and password of the user in javascript and continuously issues successful authentications to the school's on premises LMS for an extended period of time(many minutes). This behaviour is observed even if the user does not interact with the app in any manner.

**01/04/2020**

- Studentnet has documented the app authentication behaviour and provided logs and evidence to the developer for their examination.

**Root Cause**

- Inappropriate authentication behaviour by an app not required for remote learning

**Recommendations/Preventative Measures**

- Audit app behaviours and rectify to conform to standard protocols where needed
- Monitor resource usage re-allocating and optimising where needed
- Prepare for further orders of magnitude growth in authentication volumes as remote learning is established as the new normal mode of operation

*oOo*