

Silverstripe Incident Report

INC-212761 | Outage affecting www.bnz.co.nz

Priority	P1
Impact Start Date/Time	17/07/2025 9.17 am
Impact End Date/Time	17/07/2025 9.40 am
Impact Duration	23 mins
Report Date/Version	18 July 2025 - Draft
Report Prepared By	Delivery Lead - Julio Kalolo
Report Audience	Bank of New Zealand



Impact Statement

The websites experienced website degradation that occurred from 9.17 am to 9.40 am, 17 July 2025. The impact lasted for a period of 23 mins. This impacted the following website below.

- www.bnz.co.nz

Chronology of Events

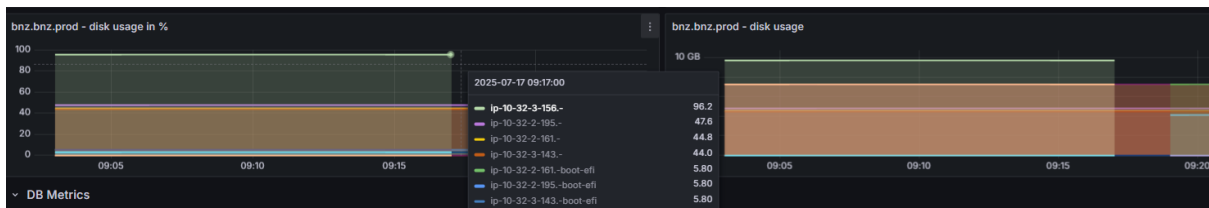
Date	Time	Event
17/07/2025	9.17 am	Outage occurred.
	9.19 am	Alert fired and acknowledged by Platform support for investigation.
	9.40 pm	Platform support observed symptoms of instance recycling behavior in the load balancer group and observed logs to identify faults. One of the instances had a 96.7% disk usage.
	9.46 pm	Initial ticket raised to inform client of the outage detected earlier. Alert closed.
	10.42 am	Escalation received by Silverstripe Account Manager from BNZ.
	11.00 am	MIM war room stood up. Incident raised as a High Priority but treated with urgency. Investigation prioritized with Senior Platform support engineer and Platform support engineer.
	11.30 am	Initial MIM comms sent to BNZ
	11.42 am	MIM comms sent to BNZ confirming progress and next scheduled update for 1.30pm
	12.51 pm	Root cause discovered. Risk identified for a separate assessment under RISK-33 as part of operations continual improvement.
	3.30 pm	Relayed initial findings to BNZ on summary of Incident, root cause shared and an agreement of post action items with recommendations to be shared.

Workaround

No suitable workaround was discovered during this incident.

Root Cause and Resolution

During our root cause analysis, we observed an instance associated with 10.32.3.156 had 96.2% disk usage while instances in the load balancer were within acceptable disk usage operations. At 9.17 am, the instance had terminated (observed in the below graph) and fetched the new wild card certificate for *.sites.silverstripe.com . As this rolled over to the remaining instances, there were invalid SSH handshakes between web instances and certificates stored on the Akamai WAF.



The incident was instantly resolved from BNZ when certificate for the wild card certificate had to be uploaded to Akamai which restored the dependency as *.sites.silverstripe.com is part of the certificate chain of authority.

Follow-up Actions

1.	Silverstripe to share root cause analysis	Silverstripe	Completed
Root cause details have been amended.			
2.	Silverstripe to share recommendations	Silverstripe	Reviewed
1. As an enhanced support approach, Silverstripe can tailor the certificate renewal process and engage an agreed interval on when to refresh the wild card certificate and coordinate with BNZ on safely uploading the custom certificate to the WAF. This may require both parties to proactively engage and having BNZ to raise service desk ticket strictly focus on Production to ensure wild card certificates are renewed safely and securely on an agreed date.			
3.	Silverstripe to investigate all alert notifications received	Silverstripe	Completed

All expected notifications were received.

Our pingdom uptime checks detected downtime which was alerted at 9.19 am and acknowledged by our Platform support.


Opsgenie APP 9:19 AM

charitha.punchinilame acknowledged alert #77314 "Pingdom Uptime Alert: akopanuk-prod.sites.silverstripe.com [SC] akopanuk has an alert"

Pingdom added note "OK" to alert #77314 "Pingdom Uptime Alert: akopanuk-prod.sites.silverstripe.com [SC] akopanuk has an alert"

Pingdom closed alert #77314 "Pingdom Uptime Alert: akopanuk-prod.sites.silverstripe.com [SC] akopanuk has an alert"

#77317: Pingdom Uptime Alert: www.bnz.co.nz [SC] BNZ has an alert
 HTTP Server Error 503 Service Unavailable
 Check Name : [SC] BNZ
 Check Type : HTTP
 Check Params : {basic_auth=false, encryption=true, full_url=https://www.bnz.co.nz/, header=User-Agent:Pingdom.com_bot_version_1.4_(http://www.pingdom.com/), hostname=www.bnz.co.nz, ipv6=false, port=443, responsetime_threshold=30000, url=/, verify_certificate=true}
 Time (UTC) : 2025-07-16T21:17:38

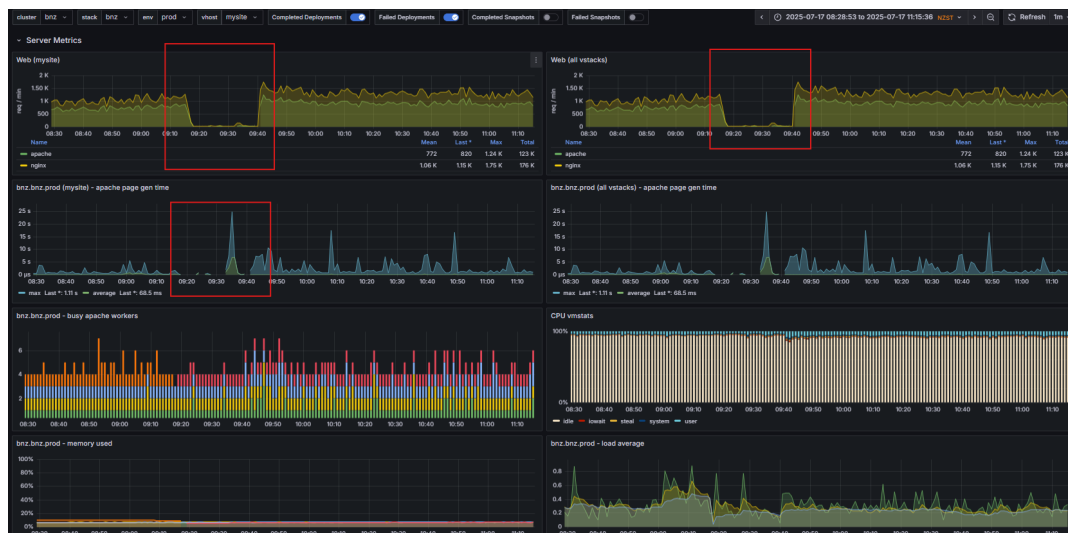
Priority
P1

Routed Teams
Platform Support

Monitoring also picked up with the instance behavior during the investigation into the load balancer.



More inspections were done on the server level.



4.	Silverstripe to share learnings	Silverstripe	Completed
----	---------------------------------	--------------	-----------

1. Silverstripe identified a risk as part of the annual routine process for specific BYO WAF clients under RISK-33 which will be assessed as part of the operations continual improvement progress. This risk relates to unintentional instance recycling (i.e., high disk or compute consumption) which will fetch updated secrets, key and certificates from the AWS SSM parameter store.
2. Silverstripe acknowledges changes to recommended communication and specifically with edge cases for BYO WAF.
3. Silverstripe to also review the change management practices as this learning had identified one client impact and may need a maintenance review on accommodating to the requirement. Internal continual improvement item captured to track the internal improvements under PO-438 scheduled for October 2025 completion.

5.	Silverstripe to provide updates during the monitoring phase of the incident being controlled.	Silverstripe	Completed
----	---	--------------	-----------

No further trends of downtime detected from the symptoms observed leading towards the outage.

6.	Silverstripe to identify preventative measures	Silverstripe	Review
----	--	--------------	--------

As a separate review of the platform maintenance, we can look into opting out BNZ from the annual routine while rolling out the certificate to other environments.