DSB Production Incident Root Cause Analysis

For the Production Incident on 9th August 2022

Prepared by: technical.support@anna-dsb.com
RCA Owner: David Lane
Date: 16th August 2022

Revision History

Version	Date	Reason
1.0	16th August 2022	Initial Revision
1.1	14th October 2022	Amendment of Status to Completed of Items 4 & 5 in the Corrective Actions and Taken and Planned

Table of Contents

IMPACT ASSESSMENT & CATEGORIZATION

Major Impact (Severity One - S1)

Start: 6:46 AM UTC - 9th August 2022
Resolved: 10:55 AM UTC - 9th August 2022
Impact: The Production OTC ISIN Service was unavailable
Total: 4 hours and 09 minutes

For details of classification of Incidents please see **Appendix 1** on page 7.

INTRODUCTION

The DSB suffered a Production Incident on 9th August 2022 between the hours of 6:46 AM UTC and 10:55 AM UTC. During this time, the Production OTC ISIN Service was unavailable for all users regardless of access method. This RCA has determined what happened in the lead-up to, during, and after the event.

EXECUTIVE SUMMARY - FINDINGS AND ROOT CAUSE

The root cause has been determined as a failure in the DSB Change Management Process, whereby a change was categorized incorrectly. The change that resulted in the incident was related to a broader ongoing DSB cost management initiative. The cost management initiative is focused on deleting redundant copies of data, primarily older copies of server backups within AWS, whereas the change that caused the incident was related to the deletion of a perceived unused AWS Directory Service.

The data being deleted under the cost management initiative are redundant or older copies of server backups where the risk is deemed low and changes are permitted mid-week in both the Production and Disaster Recovery (DR) environments. This follows the standard production change process associated with low-risk repeatable activities. The change that resulted in the incident was the deletion of an AWS Directory Service. AWS Directory Service deletions are unrecoverable and impact entire regions.

The AWS Directory Service deletion should not have been categorized as low risk. This incorrect categorization is the root cause of the incident.

On incident closure, the DSB immediately suspended all change in client facing environments and initiated a recovery plan to assess:
- Any performance impacts relating to the changes implemented to recover the OTC ISIN Service
- The Change Management Process within the DSB and its technology providers
- The notifications platform and contact information
- The incident and incident management with industry via the DSB Technology Advisory Committee

DETAILED EVENT DESCRIPTION

As background information, the AWS service that was deleted was the AWS Directory Service. This was introduced in 2017 as part of a trial with the DSB's Service Provision Partner (SPP) related to server access authentication. The trial was unsuccessful, however, the AWS Directory Service was never decommissioned.

The DSB is running a cost management initiative which has been focused on deleting redundant copies of data, primarily older copies of server backups within AWS. This is part of the DSB's continued focus on lowering infrastructure costs.

The DSB team working on the cost management initiative identified that the AWS Directory Service appeared redundant as the AWS Directory Service had only default AWS configuration settings and was a legacy service from testing in 2017. Based on this history and supported by a lack of any DSB specific configuration within the AWS Directory Service, the DSB team assumed the AWS Directory Service was unused. The team proceeded to raise a change to remove the AWS Directory Service under the umbrella of the cost saving initiative.

The data removal tasks under the cost management initiative were deemed a low risk because they were only deleting redundant copies of server backups and no production or business data of any type. The DSB team followed the DSB Change Management Process for low-risk changes. This process permits changes in Production and DR locations without review by the DSB change board. As the removal of the AWS Directory Service was technically different, it should have been classified differently and should not have followed the low-risk process associated with data deletions.

On 9th August 2022 at 6:55 AM UTC, DSB Technical Support received an alert that the instances could not be accessed. At 7:15 AM UTC, the DSB initiated an incident bridge with both AWS and the SPP.

The first step was to consider what, if anything, had been changed. One change had been made that morning and coincided with the timing of the alert. This change was to remove a legacy AWS Service – AWS Directory Services from both the Production and Production-DR regions. This change followed the standard procedure of raising a ticket with the SPP, which was then assessed by the SPP prior to being approved by DSB support before being actioned by the SPP.

An investigation into this change identified that the directory name associated with the AWS Directory Service was still being referenced by all customer facing servers. The AWS Directory Service was used by all customer facing servers for name resolution. The removal of the AWS Directory Service from both regions broke the name resolution for Production *and* Production-DR. This impacted network connectivity between all production customer facing servers in both regions. It also ruled out the option of failing over the OTC ISIN Service to the disaster recovery region.

Having investigated further, AWS advised that AWS does not provide the ability to restore a deleted AWS Directory Service. AWS suggested that the DSB amended the server configurations to use AWS DNS Service (Route53) for name resolution. The change involved AWS configuration and then a refresh of network settings on all customer facing servers. This was tested successfully on an individual server prior to a wider rollout.

The lack of name resolution on DSB client facing servers meant every server needed to be accessed individually and remediation activities carried out. Once this was completed, the DSB performed application restarts and operational checks. The Production OTC ISIN Service was restored by 10:55 AM UTC. All OTC ISIN Services across all other environments were available by 12:15 PM UTC.

On incident closure, the DSB immediately suspended all change in client facing environments and initiated recovery plan to assess:

- Any performance impacts relating to the changes implemented to recover the OTC ISIN Service
- The Change Management Process within the DSB and its technology providers
- The notifications platform and contact information
- The incident and incident management with industry via the DSB Technology Advisory Committee

TIMELINE OF EVENTS

9th August 2022 Time (UTC)	Description
02:59 AM UTC	MSP raised a ticket with SPP to decommission AWS Directory Services deployed within the DSB's production AWS account as part of cost management processes.
04:27 AM UTC	SPP provided a statement of work for the decommission of the AWS Directory Services, this included a default AWS statement relating to the deletion of AWS Directory Services not being recoverable.
06:46 AM UTC	A change in AWS was executed by the SPP with the go signal from DSB Technical Support team to delete the AWS Directory Services in Ireland and North Virginia Region.
06:55 AM UTC	DSB received a monitoring alert that all DSB instances could not be accessed across all environments (PROD, UAT, UAT2, PROD-DR, UAT-DR).
06:56 AM UTC	DSB Technical Support performed operational readiness checks across all environments which had failed results.
07:10 AM UTC	DSB Technical Support raised a SPP incident ticket and called their hotline to check on the issue experienced by all instances.
07:15 AM UTC	An incident bridge was initiated to discuss the issue with the SPP team as well as AWS Support (what possible causes for the issue and any resolution options).
07:30 AM UTC	Failover to DR site ruled out due to inaccessibility of the DR servers.
07:45 AM UTC	UAT2 GUI was placed in maintenance.
08:00 AM UTC	DSB sent an **Informational Notification** to all DSB audience stating the DSB environments were inaccessible. (https://www.anna-dsb.com/download/2022-0809-informational-notice-dsb-prod-uat-uat2-services-inaccessible/).

08:29 AM UTC	PROD GUI was placed in maintenance mode. (Due to an issue DSB Technical Support had to perform this task manually.)

9th August 2022 Time (UTC)	Description
08:49 AM UTC	UAT GUI was placed in maintenance mode. (Due to an issue DSB Technical Support had to perform this task manually).
09:00 AM UTC	DSB sent an **Update Notification** to clients (https://www.annadsb.com/download/2022-08-09-informational-notice-dsb-prod-uat-uat2-servicesinaccessible-9-00am-utc-update/).
10:00 AM UTC	DSB sent an **Update Notification** to clients (https://www.annadsb.com/download/2022-08-09-informational-notice-dsb-prod-uat-uat2-servicesinaccessible-10-00am-utc-update/).
10:05 AM UTC	AWS updated the DHCP configuration.
10:10 AM UTC	DSB renewed the DHCP lease on a specific instance.
10:10 AM UTC	DSB confirmed the refreshed instance was now available via SSM.
10:15 AM UTC	DSB Technical Support began to take down the OTC ISIN Services in UAT2.
10:16 AM UTC	Some Ireland instances were now online in SSM even without the manual DHCP renew. The assumption was they had automatically expired their lease and renewed.
10:19 AM UTC	DSB Technical Support began to take down the OTC ISIN Services in PROD-DR.
10:23 AM UTC	DSB Technical Support noted that they were having to perform multiple DHCP renewals as the changes were not reflecting on some instances.
10:29 AM UTC	DSB Technical Support began to take down OTC ISIN Services in UAT.
10:35 AM UTC	DSB Technical Support started the OTC ISIN Services in PROD-DR.
10:38 AM UTC	DSB Technical Support began to take down the OTC ISIN Services in UAT-DR.
10:42 AM UTC	DSB Technical Support removed the maintenance page in GUI for Production.
10:46 AM UTC	DSB Technical Support successfully undertook operational readiness checks for Production REST.
10:50 AM UTC	DSB Technical Support successfully undertook operational readiness checks for Production FIX.
10:55 AM UTC	DSB Technical Support successfully undertook operational readiness checks for Production GUI.
11:00 AM UTC	DSB sent an **Update Notification** to clients advising that a fix had been implemented and recovery was underway (https://www.anna-dsb.com/download/2022-08-09informational-notice-dsb-prod-uat-uat2-services-inaccessible-11-00am-utc-update/)
11:11 AM UTC	DSB Technical Support started the OTC ISIN Services in UAT2.

11:30 AM UTC	DSB Technical Support successfully completed UAT2 REST/FIX/GUI operational readiness checks.
11:35 AM UTC	DSB Technical Support started the OTC ISIN Services in PROD-DR.
12:00 PM UTC	DSB Technical Support started the OTC ISIN Services in UAT.
12:02 PM UTC	DSB sent an **Update Notification** to clients (https://www.annadsb.com/download/2022-08-09-informational-notice-dsb-prod-uat-uat2-servicesinaccessible-12-00pm-utc-update/).
12:15 PM UTC	DSB Technical Support successfully completed UAT REST/FIX/GUI operational readiness checks.
12:16 PM UTC	Technical Support started the OTC ISIN Services in UAT-DR.

9th August 2022 Time (UTC)	Description
12:17 PM UTC	DSB sent an **Update notification** to clients informing them that the issue had been resolved across all environments (https://www.anna-dsb.com/download/issueresolved-2022-08-09-informational-notice-dsb-prod-uat-uat2-services-inaccessible/)
12:57 PM UTC	One client reported they had not received any notifications.

CORRECTIVE ACTIONS TAKEN & PLANNED

#	Action	Status	Completion Date
1	Immediate suspension of ANY change in the Production environment. This will remain in place until the completion of Action item "5".	Completed	09/08/22
2	Post Incident KPI review	Completed	10/08/22
3	Publication of the RCA	Completed	16/08/22
4	Review the email notification distribution system	Completed	26/08/22
5	Review of the existing Change Management Processes within both the MSP and SPP, to address not only the findings of the RCA, but a review of all aspects of the Change Management Process in both organizations. This will include the interaction points between the MSP and SPP processes.	Completed	02/09/22
6	TAC review of the RCA	Not-Started	26/10/22

APPENDIX 1

Classification of Incidents

Severity	Definition
Critical (S1)	**Critical production issue that severely impacts the DSB Service for all Users. The situation halts business operations and no procedural workaround exists.** **DSB Service is down or unavailable. Major data elements are corrupted or lost and must be restored from backup. A critical documented feature / function is not available.**
Major (S2)	Major functionality is impacted or significant performance degradation is experienced and is not a Critical Incident. The situation is causing a high impact to some Users' business operations and no reasonable workaround exists. DSB Service is operational but highly degraded performance to the point of major impact on usage. Important features of the system offering are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion.
Minor (S3)	There is a partial, loss of use of the DSB Service with a medium-to-low impact on your business, but your business continues to function that is not a Critical Incident or a Major Incident. Short-term workaround is available, but not scalable.
Cosmetic (S4)	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Acceptable workaround available.

Reference: DSB Service Level Policy 2022