Incident Root Cause Analysis Report Summary:

Application / Infrastructure / Customer Service impacted:	
Severity: Critical Incident	
Incident analysis held on by: IT Service Monitoring and Control Center, Online Banking System Management, Application Management (Core and Aux), Server and Storage Admin, Database Admin, Data Analytics and Information Management Division & Payment Systems Management Teams	
Date Analysis: September 23, 2025	
Incident site: • Core Banking (Essence) Database Servers with IP addresses 10.10.10.118 and 10.10.10.119; • CBS Application servers; • AwashBIRR Pro and ATM Servers; • Report API Endpoint Servers with IP addresses 10.10.12.118, 10.10.12.219, 10.10.12.222.	
Start Date of incident: 22/09/2025, 4:06 PM **Cascaded Effect Recurrence Date and Time:** 23/09/2025, 12:20 PM	**End Date of incident:** 22/09/2025, 7:03 PM 23/09/2025, 1:04 PM
Correlated incidents and customer impact: AwashBIRR Pro, USSD and ATM Services	

I. Summary analysis of the incident

- Delay in synchronization between the CBS Primary database server (10.10.10.119) and its HA standby (10.10.10.118) caused widespread disruption across CBS-dependent services. As a result, key services such as **AwashBirr Pro, USSD, and ATM transactions** experienced slow processing and intermittent failures.
- The delay in synchronization caused resource strain that further degraded the CBS-dependent operations. To mitigate the issue, the HA server had been isolated, and **manual log forwarding** applied between **05:10**

PM and 05:30 PM, after which normal replication resumed. Once synchronization was restored, **CBS and all dependent services had been returned to normal operation**.

II. Classification of the incident

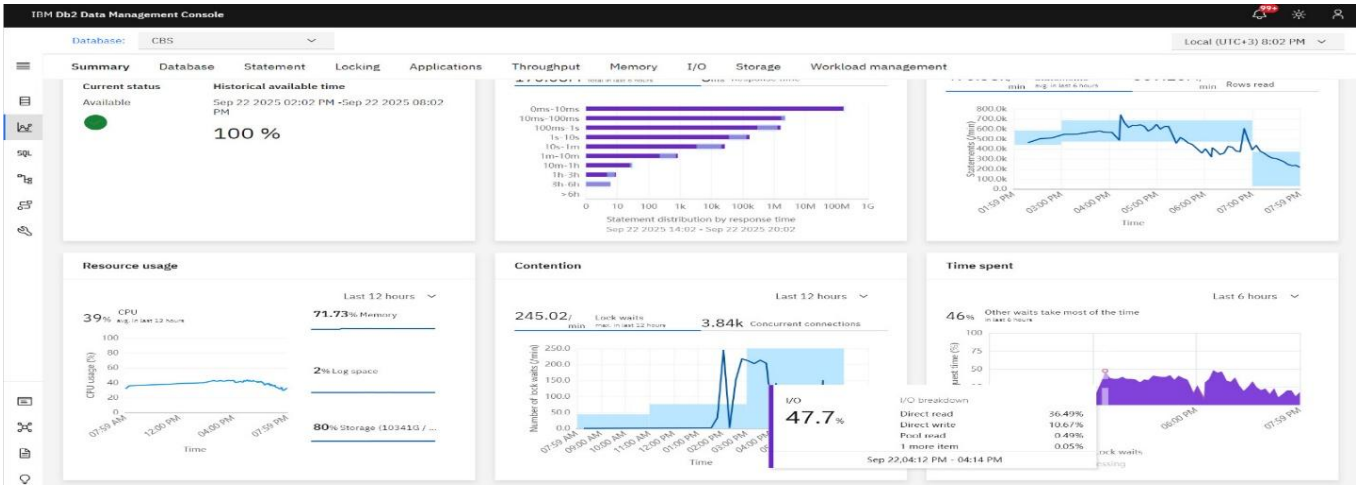
- Critical

III. Cause of the incident

The root cause of the incident was a **synchronization gap** between the CBS Primary database server (10.10.10.119) and the HA standby server (10.10.10.118) operating in near-sync mode.

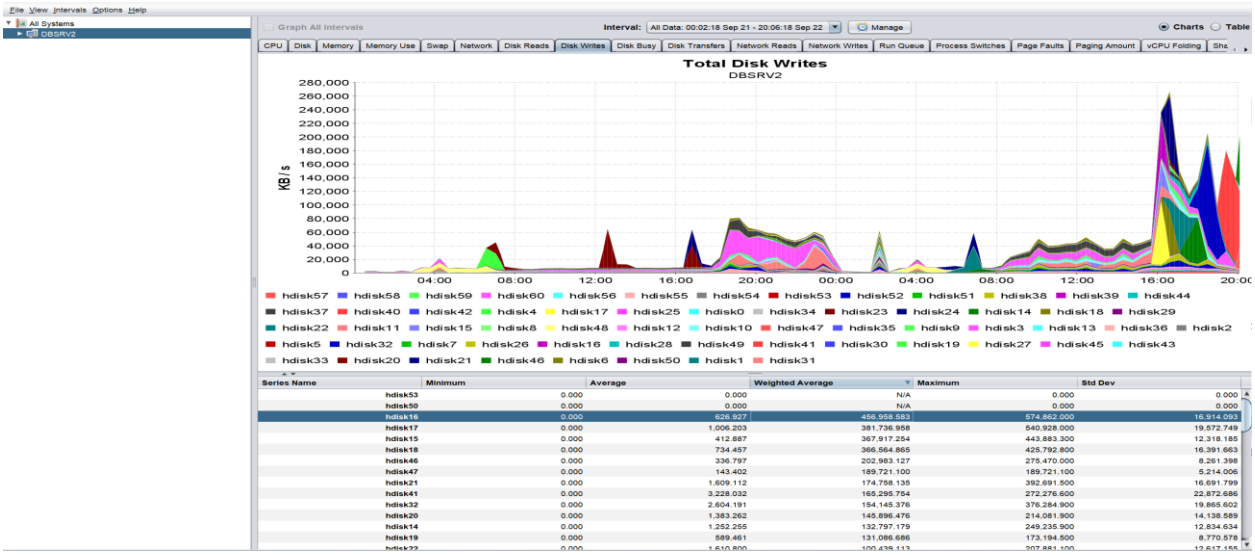
This gap was triggered by **heavy reporting queries executed against the HA server (.118)**, which caused:

- **I/O spikes:** The 'Data Management Console' showing a significant I/O spike on the DB 119 database during the incident. A large portion of database time was spent on I/O operations, with increased direct reads and writes. This I/O congestion led to longer transaction response times, higher lock durations, and overall slower application performance.

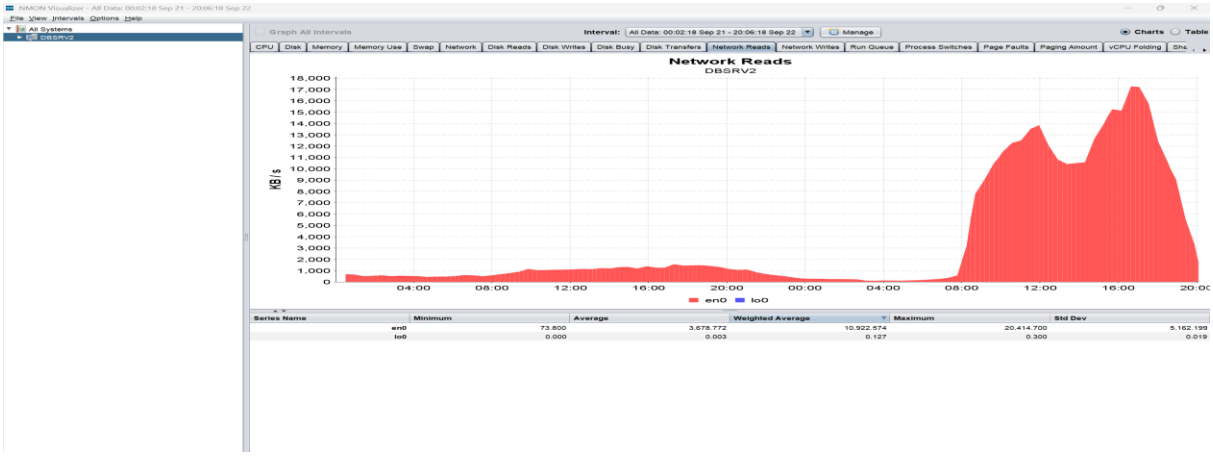


- **High disk write activity:** The 'Total Disk Writes' graph follows the same pattern as the Disk Percent Busy graph, confirming that the I/O spike was primarily driven by increased write

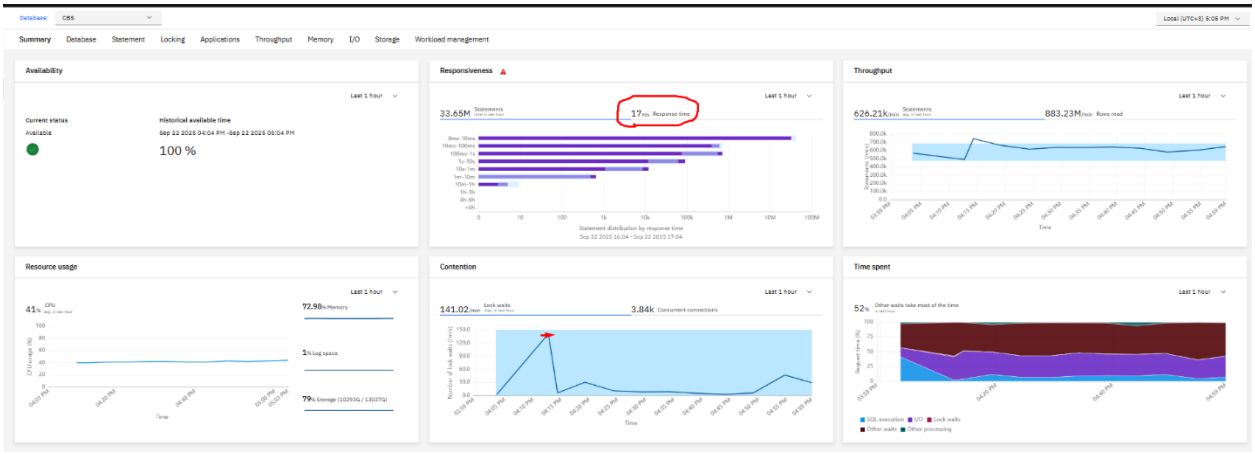
activity.



- **Increased network usage:** The ‘Network Reads’ graph was showing a corresponding spike, indicating high network traffic on the database. This network congestion likely degraded the HADR replication and increased log transmission times, contributing to the synchronization delay.



- **Increased response time on the DB:** A significant increase in database response time was observed, indicating that operations on the CBS Primary and HA standby servers were experiencing delays. This degradation affected the processing speed of transactions and queries, contributing to slower performance across CBS-dependent services.



CBS stopped responding, causing requests to pile up and halt. Logs show the USSD failure was mainly due to an upstream connection issue where the backend API ‘MoonlightMBanking/Rest/AndroidRS/SecureAppServer’ connection closed before processing.

upstream prematurely closed connection while reading response header from upstream, client: 10.10.84.252, server: awashpay.awashbank.com, request: "POST /awashbirrpro/securemmservice HTTP/1.1", upstream: "http://10.10.134.158:12021/MoonlightMBanking/Rest/AndroidRS/SecureAppServer", host: "awashpay.awashbank.com:8225" Root Cause Analysis Report 09-23-2025 Backend application API end point MoonlightMBanking/Rest/AndroidRS/SecureAppServer not responding and results connectionclosed before processing request

Additionally, a database connection in the Reporting-PG-Pool failed due to an I/O error while sending data to the backend. This caused the connection to be marked as broken ‘SQLSTATE 08006’, preventing the application from completing its transaction. The web service returned a **500 Internal Server Error** from Nginx, indicating the server encountered an unhandled error while processing the request instead of sending a proper SOAP response.

2025-09-22 17:08:46 [qtp485041780-886458] WARN ProxyConnection:157 - Reporting-PG-Pool - Connection org.postgresql.jdbc.PgConnection@3522bf98 marked as broken because of SQLSTATE(08006), ErrorCode(0)
org.postgresql.util.PSQLException: An I/O error occurred while sending to the backend. at org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:383) ~[postgresql-42.5.1.jar:42.5.1] at org.postgresql.jdbc.PgStatement.executeInternal(PgStatement.java:496) ~[postgresql-42.5.1.jar:42.5.1] at org.postgresql.jdbc.PgStatement.execute(PgStatement.java:413) ~[postgresql-42.5.1.jar:42.5.1]
at org.postgresql.jdbc.PgPreparedStatement.executeWithFlags(PgPreparedStatement.java:190) ~[postgresql-42.5.1.jar:42.5.1]
at org.postgresql.jdbc.PgPreparedStatement.executeQuery(PgPreparedStatement.java:134) ~[postgresql-42.5.1.jar:42.5.1]
at org.postgresql.core.PGStream.receiveChar(PGStream.java:455) ~[postgresql-42.5.1.jar:42.5.1]
at org.postgresql.core.v3.QueryExecutorImpl.processResults(QueryExecutorImpl.java:2120) ~[postgresql-42.5.1.jar:42.5.1]
at org.postgresql.core.v3.QueryExecutorImpl.execute(QueryExecutorImpl.java:356) ~[postgresql-42.5.1.jar:42.5.1]

Following the restart of the CBS endpoint, new tokens were generated, which led to errors. These errors caused account validation failures due to data format and parsing issues when processing responses from CBS.

```
at java.util.concurrent.FutureTask.report(FutureTask.java:122)
at java.util.concurrent.FutureTask.get(FutureTask.java:206)
at com.jmsoft.mobilebanking.financials.PostPostingUtils.querySourceAccountEndBalance(SourceFile:95)
at com.jmsoft.mobilebanking.financials.PostPostingUtils.postPostingRoutines(SourceFile:33)
at com.jmsoft.mobilebanking.financials.FinancialProcessor.processFinancial(SourceFile:119
```

Multiple issues were observed during the incident. USSD requests failed due to upstream connection problems where the backend API closed connections prematurely. At the same time, database connections in the Reporting-PG-Pool were marked as broken because of I/O errors, preventing transactions from completing. Additionally, the web service returned a 500 Internal Server Error from Nginx, indicating the server encountered an unhandled error instead of sending a proper SOAP response.

Further complications arose when the CBS endpoint was restarted, generating a new token and leading to account validation failures and parsing errors in CBS responses. Taken together, these errors indicate a diverse failure involving CBS unavailability, database instability, and web service errors, which likely caused authentication issues due to piled-up connections rather than a single point of failure.

The slowness is further confirmed by a log gap in the DB2 HADR (High Availability Disaster Recovery) setup.

HADR_SYNCMODE	HADR_CONNECT_STATUS	HADR_STATE	PRIMARY_MEMBER_HOST	STANDBY_MEMBER_HOST	HADR_LOG_GAP	STANDBY_LOG_TIME
NEARSYNC	CONNECTED	PEER	DBSRV2	DBSRV1	154450709	2025-09-22 17:51:16
SUPERASYNC	CONNECTED	REMOTE_CATCHUP	DBSRV2	DBSRV9	86660051	2025-09-22 17:51:16
SUPERASYNC	CONNECTED	REMOTE_CATCHUP	DBSRV2	DRDBSRV1	97363363	2025-09-22 17:51:16

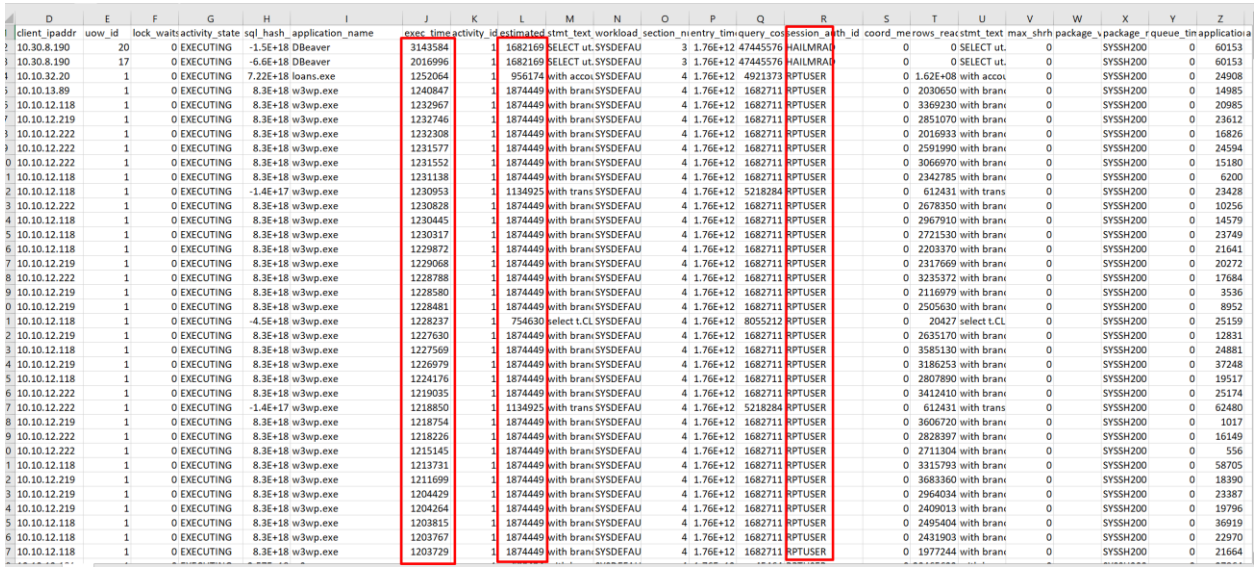
These resource bottlenecks slowed down the log apply and synchronization process, preventing timely replication from the Primary to the HADR server.

The image log below illustrates incoming traffic from the reporting user (RPTUSER) during the incident period. This user executed resource-intensive queries on the HADR server, generating high

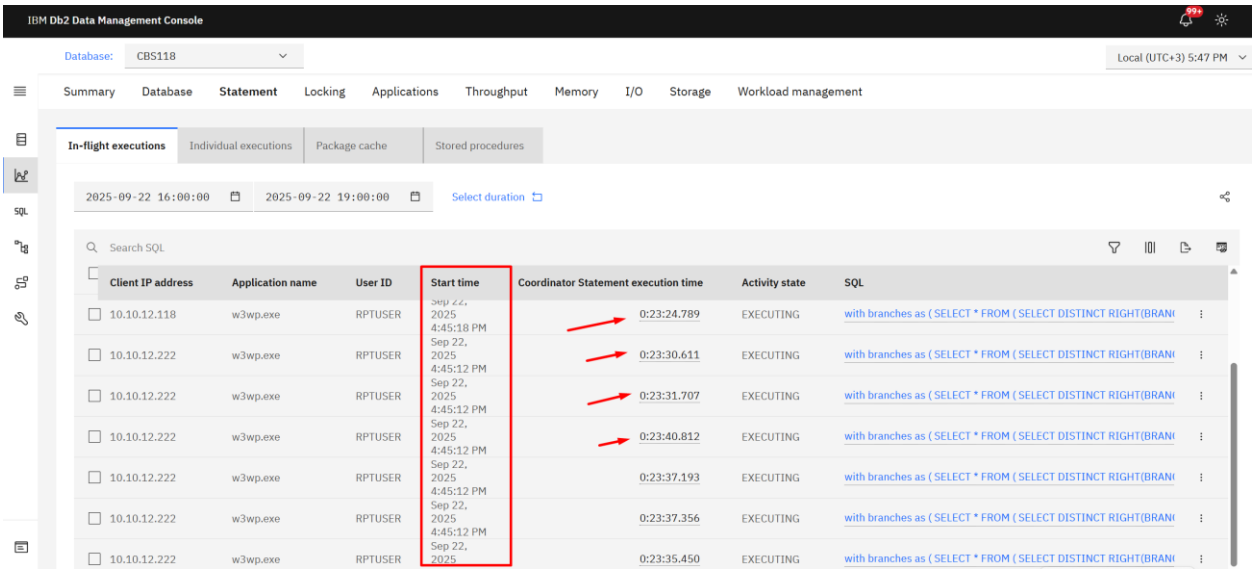
I/O and network load. As the database operates in near-sync mode, each transaction requires acknowledgment from the standby server before it can be fully committed. The heavy reporting queries created a backlog, preventing normal transactions from completing efficiently and slowing down the overall synchronization process, contributing to service disruption.

Auth Id	Application Name	Appl. Handle	Application Id	DB Name	# of Agents
RPTUSER	w3wp.exe	19796	10.10.12.219.10445.250922134044	FEPRODDB	1
RPTUSER	w3wp.exe	17684	10.10.12.222.10464.250922134022	FEPRODDB	1
RPTUSER	w3wp.exe	22776	10.10.12.222.10492.250922134113	FEPRODDB	1
RPTUSER	w3wp.exe	13901	10.10.12.222.10513.250922134143	FEPRODDB	1
RPTUSER	w3wp.exe	25947	10.10.13.89.65198.250922134121	FEPRODDB	1
RPTUSER	w3wp.exe	21993	10.10.12.118.10602.250922134424	FEPRODDB	1
RPTUSER	w3wp.exe	20493	10.10.12.118.10576.250922134102	FEPRODDB	1
RPTUSER	w3wp.exe	13585	10.10.13.181.59778.250922135116	FEPRODDB	1
RPTUSER	w3wp.exe	10256	10.10.12.222.10461.250922134017	FEPRODDB	1
RPTUSER	w3wp.exe	24881	10.10.12.118.10552.250922134021	FEPRODDB	1
RPTUSER	w3wp.exe	21381	10.10.12.219.10516.250922134742	FEPRODDB	1
RPTUSER	w3wp.exe	2381	10.10.12.118.10587.250922134148	FEPRODDB	1
RPTUSER	w3wp.exe	20098	10.10.12.118.10574.250922134058	FEPRODDB	1
MELKAMU	httpd.exe	26065	10.10.12.165.8326.250922140751	FEPRODDB	1
RPTUSER	w3wp.exe	25690	10.10.12.222.10503.250922134119	FEPRODDB	1
RPTUSER	w3wp.exe	21940	10.10.12.118.10671.250922134745	FEPRODDB	1
RPTUSER	w3wp.exe	13486	10.10.12.118.10581.250922134127	FEPRODDB	1
RPTUSER	w3wp.exe	24486	10.10.12.219.10464.250922134115	FEPRODDB	1
RPTUSER	w3wp.exe	6157	10.10.12.222.10537.250922134432	FEPRODDB	1
RPTUSER	w3wp.exe	23782	10.10.12.222.10625.250922135214	FEPRODDB	1
RPTUSER	w3wp.exe	23203	10.10.12.118.10702.250922135032	FEPRODDB	1
RPTUSER	w3wp.exe	23749	10.10.12.118.10541.250922134017	FEPRODDB	1
RPTUSER	w3wp.exe	22374	10.10.12.118.10686.250922134835	FEPRODDB	1
RPTUSER	w3wp.exe	36920	10.10.12.222.10551.250922134511	FEPRODDB	1
MELKAMU	httpd.exe	11216	10.10.12.165.8067.250922140626	FEPRODDB	1
RPTUSER	w3wp.exe	22841	10.10.13.89.49167.250922140030	FEPRODDB	1
RPTUSER	w3wp.exe	17466	10.10.12.222.10529.250922134428	FEPRODDB	1
RPTUSER	w3wp.exe	20591	10.10.12.118.10613.250922134444	FEPRODDB	1
RPTUSER	w3wp.exe	5512	10.10.12.118.10704.250922135057	FEPRODDB	1
RPTUSER	w3wp.exe	11012	10.10.13.89.65205.250922134138	FEPRODDB	1
CLPRTUSR	db2jcc_applica	7887	10.10.12.172.17258.251020105635	FEPRODDB	1
RPTUSER	w3wp.exe	30808	10.10.13.89.49313.250922140614	FEPRODDB	1
RPTUSER	w3wp.exe	14558	10.10.12.222.10508.250922134133	FEPRODDB	1
RPTUSER	w3wp.exe	24729	10.10.12.118.10722.250922135337	FEPRODDB	1
RPTUSER	w3wp.exe	5979	10.10.12.118.10582.250922134128	FEPRODDB	1
RPTUSER	w3wp.exe	1900	10.10.12.219.10608.250922135445	FEPRODDB	1
WABIAPI>	db2jcc_applica	7571	10.10.32.22.57870.251020105747	FEPRODDB	1
RPTUSER	w3wp.exe	17821	10.10.12.219.10568.250922135102	FEPRODDB	1
RPTUSER	w3wp.exe	17617	10.10.12.118.10586.250922134143	FEPRODDB	1
RPTUSER	w3wp.exe	24242	10.10.12.222.10506.250922134129	FEPRODDB	1
RPTUSER	w3wp.exe	24867	10.10.12.222.10601.250922134904	FEPRODDB	1
RPTUSER	w3wp.exe	14492	10.10.12.222.10633.250922135237	FEPRODDB	1
RPTUSER	w3wp.exe	24663	10.10.12.222.10589.250922134832	FEPRODDB	1
REPRINT	httpd.exe	22880	10.10.12.165.6516.250922135906	FEPRODDB	1
RPTUSER	w3wp.exe	26505	10.10.12.118.10672.250922134744	FEPRODDB	1
RPTUSER	w3wp.exe	14255	10.10.13.181.60050.250922135733	FEPRODDB	1
RPTUSER	w3wp.exe	24426	10.10.12.222.10557.250922134530	FEPRODDB	1
RPTUSER	w3wp.exe	26301	10.10.12.219.10523.250922134818	FEPRODDB	1
RPTUSER	w3wp.exe	23472	10.10.12.118.10693.250922134851	FEPRODDB	1
RPTUSER	w3wp.exe	56768	10.10.12.219.10470.250922134140	FEPRODDB	1

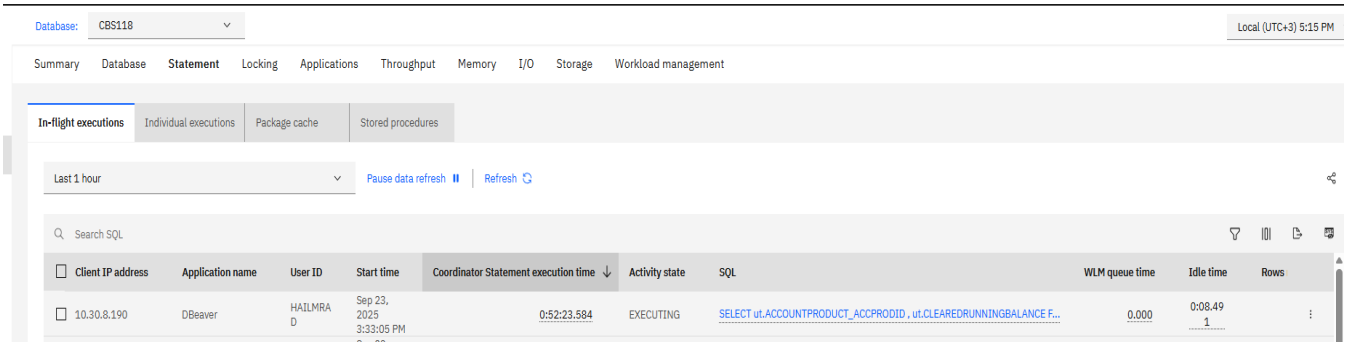
The images below indicate that the queries executed by the RPTUSER were resource-intensive, consuming significant CPU time. These expensive queries contributed to high I/O, slowed database responses, and blocked normal transaction processing during the incident.



	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	client_ipaddr	uow_id	lock_waits	activity_state	sql_hash_application_name		exec_time	activity_id	estimated	stmt_text	workload_section_n		entry_time	query_cos	session_auth_id	coord_me	rows_reac	stmt_text	max_shrh	package_v	package_r	queue_tin	applicatioia
2	10.30.8.190	20	0	EXECUTING	-1.5E+18 DBeaver		3143584	1	1682169	SELECT ut.	SYSDEFAU	3	1.76E+12	47445576	HAILMRAD	0	0	SELECT ut.	0		SYSSH200	0	60153
3	10.30.8.190	17	0	EXECUTING	-6.6E+18 DBeaver		2016996	1	1682169	SELECT ut.	SYSDEFAU	3	1.76E+12	47445576	HAILMRAD	0	0	SELECT ut.	0		SYSSH200	0	60153
4	10.10.32.20	1	0	EXECUTING	7.22E+18 loans.exe		1252064	1	956174	with acco	SYSDEFAU	4	1.76E+12	4921373	RPTUSER	0	1.62E+08	with acco	0		SYSSH200	0	24908
5	10.10.13.89	1	0	EXECUTING	8.3E+18 w3wp.exe		1240847	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2030650	with bran	0		SYSSH200	0	14985
6	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1232967	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3369230	with bran	0		SYSSH200	0	20985
7	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1232746	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2851070	with bran	0		SYSSH200	0	23612
8	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1232308	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2016933	with bran	0		SYSSH200	0	16826
9	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1231577	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2591990	with bran	0		SYSSH200	0	24594
10	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1231552	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3066970	with bran	0		SYSSH200	0	15180
11	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1231138	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2342785	with bran	0		SYSSH200	0	6200
12	10.10.12.118	1	0	EXECUTING	-1.4E+17 w3wp.exe		1230953	1	1134925	with trans	SYSDEFAU	4	1.76E+12	5218284	RPTUSER	0	612431	with trans	0		SYSSH200	0	23428
13	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1230828	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2678350	with bran	0		SYSSH200	0	10256
14	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1230445	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2967910	with bran	0		SYSSH200	0	14579
15	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1230317	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2721530	with bran	0		SYSSH200	0	23749
16	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1229872	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2203370	with bran	0		SYSSH200	0	21641
17	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1229068	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2317669	with bran	0		SYSSH200	0	20272
18	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1228788	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3235372	with bran	0		SYSSH200	0	17684
19	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1228580	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2116979	with bran	0		SYSSH200	0	3536
20	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1228481	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2505630	with bran	0		SYSSH200	0	8952
21	10.10.12.118	1	0	EXECUTING	-4.5E+18 w3wp.exe		1228237	1	754630	select t.CL	SYSDEFAU	4	1.76E+12	8055212	RPTUSER	0	20427	select t.CL	0		SYSSH200	0	25159
22	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1227630	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2635170	with bran	0		SYSSH200	0	12831
23	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1227569	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3585130	with bran	0		SYSSH200	0	24881
24	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1226979	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3186253	with bran	0		SYSSH200	0	37248
25	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1224176	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2807890	with bran	0		SYSSH200	0	19517
26	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1219035	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3412410	with bran	0		SYSSH200	0	25174
27	10.10.12.222	1	0	EXECUTING	-1.4E+17 w3wp.exe		1218850	1	1134925	with trans	SYSDEFAU	4	1.76E+12	5218284	RPTUSER	0	612431	with trans	0		SYSSH200	0	62480
28	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1218754	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3606720	with bran	0		SYSSH200	0	1017
29	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1218226	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2828397	with bran	0		SYSSH200	0	16149
30	10.10.12.222	1	0	EXECUTING	8.3E+18 w3wp.exe		1215145	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2711304	with bran	0		SYSSH200	0	556
31	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1213731	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3315793	with bran	0		SYSSH200	0	58705
32	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1211699	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	3683360	with bran	0		SYSSH200	0	18390
33	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1204429	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2964034	with bran	0		SYSSH200	0	23387
34	10.10.12.219	1	0	EXECUTING	8.3E+18 w3wp.exe		1204264	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2409013	with bran	0		SYSSH200	0	19796
35	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1203815	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2495404	with bran	0		SYSSH200	0	36919
36	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1203767	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	2431903	with bran	0		SYSSH200	0	22970
37	10.10.12.118	1	0	EXECUTING	8.3E+18 w3wp.exe		1203729	1	1874449	with bran	SYSDEFAU	4	1.76E+12	1682711	RPTUSER	0	1977244	with bran	0		SYSSH200	0	21664



Additionally, a similar behavior was observed the following day (on September 23, 2025 around 3:33 PM). Long-running queries initiated by a personal user named ‘HAILMRAD’, rather than a service account, caused high resource consumption on the HA server running for about ~52 minutes, however restored through killing the long-running queries before affecting service. The below image illustrates the impact of these queries on database performance.



In summary, the CBS system experienced a cascading performance degradation when heavy reporting queries executed by the ‘RPTUSER’ user on the HA server (118) triggered DB2 full table scans and lock waits. This led to elevated I/O activity and longer wait times on the HA server, slowing down database responsiveness. Consequently, application threads—including AWP and other CBS-dependent services—became blocked, resulting in overall service slowness and temporary disruptions during the incident.

IV. Impact of the incident

- **CBS Replication Delay:** Service degradation occurred due to replication lag between the Primary DB (10.10.10.119) and HA (10.10.10.118) servers.
- **AWP and ATM Services:** Transactions dependent on CBS experienced delays and failures.
- **Customer-Facing Services:** Temporary interruptions affected online and ATM banking, reducing overall service availability.
- **Transaction Failures:** Increased transaction processing time and failed operations led to customer dissatisfaction.
- **Operational Strain:** Manual intervention (isolating HA server, log forwarding) was required to restore normal operations, increasing operational workload.
- **System Performance:** High I/O, network congestion, and lock wait on HA caused application thread blocking and degraded overall system responsiveness.
- **Business Impact:** financial impact and reputational risk due to the disruption of critical banking services.

V. Aggravating factors:

- The incident occurred during working hours when transaction volume was high, which amplified the replication lag and overall system load.
- The resource-heavy queries consumed significant database resources, which blocked normal transaction processing, application threads including user logins for troubleshooting.
- High Traffic Load: Increased volume of transactions and reporting activities during the incident window worsened the log gap and slowed synchronization recovery.

VI. Context before / during / after the incident

Context before the incident

- CBS database servers (119 – Primary, 118 – HA) were running in a near-sync replication mode.
- Reporting users had access to the HA server for read-heavy queries.
- No major sync gap was present between Primary and HA.

Context During the incident

- A reporting user executed heavy queries on the HA server (118), causing high I/O, disk writes, and network usage which led to a log synchronization gap between the Primary (119) and HA (118).

- CBS-dependent services such as **AwashBIRR Pro and ATM transactions** experienced service degradation due to the HADR synchronization issue behind CBS.
- The HA server (118) was isolated from traffic.
- Manual log forwarding was initiated, reducing the synchronization gap.
- Once the gap decreased to an acceptable level, 10.10.10.118 rejoined replication mode with 10.10.10.119.

Context After the incident

- CBS and dependent services resumed normal operation, and service availability was restored.
- The 'RPTUSER' user account was disabled to prevent further load on the HA server.
- Since the 'RPTUSER' user account was also utilized by the ETSwitch service, disabling the account caused an interruption to ETSwitch connectivity which led to transaction failures on the next day (September 23, 2025, from 12:20 PM to 1:05 PM).

VII. Troubleshoot and diagnose

- Troubleshooting on CBS Application nodes;
- Checking resource usage: observed **high I/O, disk write activity, and network utilization** on CBS Database Servers (Primary and HADR Servers).
- Verified database logs and discovered a **log synchronization gap** between Primary (119) and HA (118).
- Identified the cause as heavy reporting queries from the 'RPTUSER' user, directly impacting HA performance.
- Confirmed that CBS Primary DB (119) was functioning normally, and the issue was isolated to HA server (118).
- HA server (118) was temporarily isolated, and manual log forwarding was performed to reduce the gap.
- Services (CBS, AwashBIRR Pro, ATM transactions) were tested and confirmed operational.
- Checking log on All Awash birr pro, sunlyte servers, CBS Application and Database Servers, & Reporting API endpoint Servers for possible error logs.
- Opening case with Vendors for further troubleshooting and analysis.
- Analyzed the workload and performance impact of queries from the 'RPTUSER' user.

VIII. Recommendation

- **Enforcing utilization of Dedicated Reporting Server:** Direct all heavy reporting queries to a dedicated reporting server (10.10.10.136) instead of the HA server (118) to prevent resource spikes and replication lag.
- **Monitoring and Alerts:** Implement real-time monitoring of HA server metrics: log sync lag, I/O, disk writes, and network usage and configure proactive alerts for abnormal sync gaps or resource spikes.
- **Controlled Access for Reporting Users:** Disable direct access to HA servers for high-load reporting users. Route all reporting workloads through the dedicated reporting server (136).
- **Automated Safeguards and Failover Planning:** implementing automated failover or log gap monitoring mechanism in place to detect and mitigate the large sync gap in real time while testing HA failover and recovery mechanisms periodically.
- **Periodic Review and Testing:** Conduct regular drills and reviews of CBS and all other systems HA performance and replication health. Validate that preventive measures effectively mitigate potential sync delays and service impact.