What is Happening Overall?

REVISED: Feb 2024

Key:

	Correla Identified	Customer Identified
Correla Controllable	Correla Identified the incident and the incident could have been avoided had Correla taken earlier action	Customer Identified the incident and the incident could have been avoided had Correla taken earlier action
Correla Uncontrollable	Correla Identified the incident but the incident could not have been avoided had Correla taken earlier action	Customer Identified the incident but the incident could not have been avoided had Correla taken earlier action

Existing Year to Date

	Correla Identified	Customer Identified
Correla Controllable	20	3
Correla Uncontrollable	1	0

Proposed Year to Date

	Correla Identified	Customer Identified
Correla Controllable	8	0
Correla Uncontrollable	13	3

Reclassified incidents

Ref.	What happened?	Why did it happen?	Impact	Reason for reclassification	Incident Date
INC0358137	Customer contacts did not process as expected within the legacy CMS application.	Due to the slow running job, a small number of customer contacts were prevented from being processed.	A controlled restart of CMS application was performed to allow customers contacts to be processed successfully.	Monitoring and alerting detected the issue quickly and Correla initiated the restoration of service promptly. This incident has been reclassified as the cause was due to a third party supplier.	4th April ‘23
INC0372725	Whilst undertaking manual checks, it was highlighted that the data transfer between UK Link and Discovery had failed.	A maintenance activity was being carried out by SAP which resulted in a requirement for a change to configure new IP addresses within our firewall.	Any requests made via the Discovery APIs would incorrectly show data for the 20th May (D-2)	This was because of a change being made by SAP and there were no clear instructions that a firewall change was required. This incident has been reclassified as the cause was due to a third party supplier.	21st May ‘23
INC0388208	Customers were unable to access the Gemini system	A network issue within our partner's shared data centre caused congestion when accessing the database servers. The congestion was identified on day two as an unexpected volume of traffic from another customer utilising the shared datacentre infrastructure. This caused the network to become saturated, resulting in performance issues for multiple customers within the datacentre.	Customers were unable to access the Gemini service, resulting in some customers to have to renominate where initial nominations were impacted	A hardware failure of a shared networking component was put under excessive load due to another customer of that data centre sending high levels of data, chocking the network. This incident has been reclassified as the cause was due to a third party supplier.	5th & 6th July ’23
INC0390335	Our monitoring and alerting detected that the primary Gemini node had become unavailable	The primary node experienced an unplanned sudden shutdown.	During the circa 8 min period between the unexpected shutdown and the secondary server taking over, customers would not have been able to access Gemini.	This was an unexpected system shutdown of the operating system. The support team logged a call promptly with the vendor. Despite logs being shared with the vendor, no route cause could be determined. This incident has been reclassified as the cause was due to a third party supplier.	7th July ‘23
INC0401334	During the planned UK Link Disaster Recovery test, SAP PO became unresponsive following failover to the secondary servers.	Root cause could not be established as replication of the scenario did not result in the similar failures	During the planned Disaster Recovery Test, Customers could not access legacy CMS for 60 minutes	With support from SAP the root cause could not be determined despite attempts made to replicate the scenario. This incident has been reclassified as we monitored and checked performance as part of the process and we could not have acted sooner.	19th Aug ‘23

Reclassified incidents

Ref.	What happened?	Why did it happen?	Impact	Reason for reclassification	Incident Date
INC0409188	Our monitoring detected file processing slowness with Gemini files.	An intermittent performance issue with the Network Interface Card (NIC) caused communication interruption to the service.	Customers would have seen delayed response times when using Gemini APIs. Some customers would also have experienced issues logging into Gemini	This was a rare hardware failure of a component in the Gemini infrastructure. The fault was difficult to determine due to the intermittent nature of the fault. Our support team acted quickly to restore service This incident has been reclassified as the cause was due to a third party supplier.	18th Sept ‘23
INC0413414	The support teams identified connectivity issues affecting SAP Process Orchestration (SAP PO).	The SAP PO database space was utilised to full capacity. This was exacerbated by the annual IDL activity and an unexpected bulk load of files.	The weather data loaded into Gemini was delayed causing incorrect day ahead values to be published. Customers were unable to access the UK Link Portal and legacy CMS services during the outage period.	Our monitoring and alerting detected the cause of the issue promptly and action was taken. This incident has been reclassified as we monitored and checked performance as part of the process and we could not have acted sooner.	3rd October ‘23
INC0434910	When customers were attempting to log into the Xoserve Services Portal and legacy CMS, the Microsoft Multi-Factor Authentication (MFA) emails were not being sent by Microsoft.	Microsoft confirmed there was a multi-customer incident occurred due a faulty node impacting customers utilising the Azure Active Directory MFA Service.	Customers were unable to access the Xoserve Services portal and legacy CMS as Microsoft MFA emails were not being sent. Customers logged in before the incident would have retained systems access.	This was a Microsoft, multi customer impacting incident. Following internal checks, a high priority ticket was raised with Microsoft, who acknowledged the issue was within their environment. This incident has been reclassified as the cause was due to a third party supplier.	3rd Jan ‘24
INC0436707	Monitoring & alerting identified that there was slowness in job performance within SAP ISU	An ongoing index rebuild activity caused DB locks which caused performance issues.	Customers would have been unsuccessful when attempting to log a contact in legacy CMS or, when attempting a transaction on the UK Link Portal	In reacting to the system alerting promptly, the team took remedial actions in a timely manner restoring service quickly. This incident has been reclassified as the cause was due to a third party supplier.	11th Jan ‘24
INC0437828	Monitoring and alerting detected that the SAP ISU database went offline causing the system to become unavailable.	The disk on ISU DB server became unavailable whilst adding a new node to the existing database.	Customers would have been unsuccessful when attempting to log a contact in legacy CMS or, when attempting a transaction on the UK Link Portal	In reacting to the system alerting promptly, the team took remedial actions in a timely manner restoring service quickly. This incident has been reclassified as the cause was due to a third party supplier.	17th Jan ‘24
INC0441344 & INC0442730	Our support teams and monitoring/alerting identified connectivity issues affecting SAP Process Orchestration (SAP PO).	Following detailed analysis, Microsoft recommended that a default Azure setting should be disabled as this was creating a slow memory leak, which led to the system consuming high levels of memory over time. Since this was disabled, no further issues have been experienced.	During the restart activity customers were unable to access the UK Link Portal and legacy CMS services.	Our alerting identified that there was a connectivity issue and quickly initiated a restart of the services after the initial triage. A case was raised promptly with Microsoft to aid investigations This incident has been reclassified as the cause was due to a third party supplier.	1st Feb ’24 & 6th Feb ‘24