cloud bridge

Managed Backup Powered by Commvault

Service Description

August 2025

aws PARTNER Advanced Tier Services

Document Control

Author:	Philip Reeve
Date created:	01/05/2024
Classification:	Public
Document type:	Service Description

Version	Modified Date	Description	Modified By
V0.1	15/01/2024	Initial draft	Philip Reeve
V1.0	28/08/2025	Major updates to several sections	Philip Reeve

Table of Contents

1 Overview

The Managed Backup Powered by Commvault Metallic service provides fully managed, cloud-based data protection for your AWS workloads. Built on Commvault Metallic, an industry-leading Data Management as a Service (DMaaS) platform, it combines proven enterprise backup technology with the simplicity and efficiency of SaaS delivery.

This service delivers enterprise-grade backup and recovery capabilities in a cost-effective, turnkey package. By leveraging a standardised, multi-tenant platform and economies of scale, we make robust data protection accessible to organisations of all sizes.

All critical AWS data — including EC2 instances, databases, and storage — can be protected to the Metallic cloud with air-gapped, immutable copies for ransomware resilience. The service is available globally, supporting multiple AWS regions and data residency requirements.

Delivered as a fully managed service, we handle the entire lifecycle of backup and recovery: from initial setup to daily monitoring, ongoing optimisation, and restore operations. Customers can also access the Metallic web console for optional self-service monitoring or recoveries. To provide assurance, we include comprehensive reporting and you can opt for regular restore testing, giving you confidence that backups are reliable and your data is always recoverable.

2 Scope of Management

The Managed Backup Powered by Commvault Metallic service provides end-to-end protection of AWS workloads through backup, retention, air-gapped storage, restore services, and continuous monitoring. Below is a summary of the key areas of scope.

2.1 AWS Workloads Coverage

We provide backup and restore for supported AWS workloads, including:

- **EC2 Instances** – File-system and image-level backups of Windows and Linux instances. This includes application-consistent backups (via agents or scripts for supported applications and databases) and EBS volume snapshots for rapid recovery.
- **AWS Databases** – Protection for Amazon RDS (including Aurora). Backups use native APIs and snapshots to ensure consistent recovery points.
- **AWS Storage Services** – Optional protection for Amazon S3 buckets to safeguard against accidental deletion or corruption, including metadata and object versions if required.
- **Other AWS Services** – On request, additional workloads such as Amazon Redshift, EFS and Amazon EKS (cluster configuration, persistent volumes) can also be protected using Metallic's cloud-native capabilities.

2.2 Backup Policy Management

We will design and implement backup policies and schedules using the Metallic platform to meet your operational and compliance needs.

- **Standard Policies** – Unless otherwise agreed, the following default backup schedules are applied:
    - **Option 1 (Balanced Policy)** – 7 daily backups, 4 weekly, 12 monthly, 3 yearly.

    - **Option 2 (Extended Daily Retention)** – 30 daily backups, 12 monthly, 3 yearly.

- **Frequency** – Standard backup frequency is once per day for most workloads, giving a Recovery Point Objective (RPO) of 24 hours.

- **Backup Windows** – Backups are scheduled during agreed maintenance windows to minimise production impact.

Any policies outside these defaults (e.g. hourly backups, extended long-term archival) must be formally agreed during onboarding and may carry additional subscription cost.

2.3 Retention Management

We manage retention of backup copies in line with the agreed policies.

- **Policy Enforcement** – Retention is configured and enforced in the Metallic SaaS platform. Expired backups are automatically pruned unless specifically flagged for extended retention.

- **Long-Term Retention** – Annual, compliance-driven, or legal hold requirements (beyond standard policy) can be supported but must be explicitly requested and agreed in scope.

- **Customer Responsibility** – Customers are responsible for confirming that retention settings meet their internal, legal, and regulatory requirements. We will advise on best practice but do not own compliance obligations.

- **Exclusions** – Retention does not include open-ended, indefinite, or "forever" backups. These must be scoped separately with appropriate storage and cost implications.

2.4 Commvault Metallic SaaS Platform (Licensed & Maintained)

Full use of the Metallic cloud backup platform is included. This covers the necessary licensing, deployment of any required components, and maintenance of the SaaS platform:

- **Backup Infrastructure:** Metallic's cloud backup infrastructure is provided as part of the service. If backup gateway virtual appliances are needed in your AWS environment (for example, to facilitate data movement for certain workloads), we will deploy and manage those as part of the service.

- **Software Updates:** All updates, patches, and upgrades to the Commvault/Metallic software are handled automatically by the SaaS platform. You always benefit from the latest features and security patches without any effort or downtime on your side.

- **Scalability:** The service will scale to protect your growing environment. As you add more AWS instances or data, the backup infrastructure will elastically scale in capacity and performance (with prior notice if a significant increase is expected, so we can adjust any subscription tier accordingly). No need to provision your own backup servers or storage – we handle the growth seamlessly.

2.5 Air-Gapped Backup Storage

As part of the service, backup data can be stored securely in Commvault Metallic's managed cloud storage, with air-gapped copies created for ransomware resilience.

- **Primary Backup Copies (Hot/Frequent Tier)** – By default, backups are written directly to Hot/Frequent Access tier storage for fast restore performance. Daily backups are typically retained in the Hot tier to support common restore scenarios.

- **Secondary Tiering (Cool/Infrequent Tier)** – For longer-term retention, older backups are tiered to Cool/Infrequent Access storage to optimise cost while preserving recovery capability. Weekly, monthly, and yearly backups are commonly stored in the Cool tier.

- **Air-Gapped Secondary Copies** – Metallic creates isolated copies in a separate, Commvault-managed tenancy inaccessible from the customer's AWS environment. These air-gapped copies are immutable and cannot be modified or deleted until retention expiry.

- **Immutability** – Both Hot and Cool tier copies are protected with write-once immutability controls. Even administrative users cannot alter or delete backup data before its retention period expires.

- **Recovery from Air-Gapped Copies** – In a worst-case scenario, such as a ransomware incident that compromises primary backups, we can recover data from the isolated vault.

2.6 Recovery Services

The service covers end-to-end restore assistance and execution for supported AWS workloads. Restore options vary by resource type:

- **Amazon EC2 Instances**
    - **Instance-Level Restore** – Recover an entire EC2 instance from backup, either in-place or to a new instance.
    - **Volume-Level Restore** – Restore individual EBS volumes and reattach to an instance.
    - **File-Level Restore** – Recover individual files or folders from backups.
    - **Application-Aware Restore** – For workloads such as SQL or Active Directory running inside EC2, application-consistent restores may be supported using agents.
- **Amazon RDS**
    - **Instance-Level Restore Only** – RDS backups can be restored to a new database instance or overwrite an existing one.
    - **Granular Restore Not Supported** – Item-level restore (e.g., individual tables/rows) is not supported natively for RDS. Customers needing finer recovery granularity should consider running the database on EC2, where file- or record-level restore is possible.
- **Amazon S3**
    - **Bucket/Object Restore** – Recover objects that were deleted or corrupted.
    - **Version Restore** – Restore previous object versions if retained.
    - **Limitations** – Restores are at the object level.
- **Amazon EFS**
    - **File-System-Level Restore** – Restore an entire file system snapshot.
    - **File/Folder-Level Restore** – Recover individual files or directories from backup.

- **Alternate Location Restore** – Option to restore to a new file system for testing or recovery.

- **Other AWS Services**
    - Workloads such as Amazon Redshift or EKS can be restored if in scope, but restore granularity depends on the specific service and Metallic's native support. These will be confirmed during onboarding.

2.6.1 Restore Testing (Optional Add-on)

Restore testing is available as a paid add-on to validate recoverability and ensure confidence in your backup strategy. Customers can select the number of test restores to be performed on a monthly or quarterly basis, with tests conducted to a non-production environment. These exercises confirm that RPO/RTO targets are achievable and highlight any issues before a live incident, reducing the risk of failed restores when they matter most.

2.7 Security and Compliance Measures

The service includes robust security practices:

- **Encryption:** All backup data is encrypted using strong encryption (AES-256) at rest and in transit. If needed, integration with AWS KMS for customer-managed keys can be arranged, ensuring you have full control over encryption keys.

- **Access Control:** The managed service team uses role-based access within the Metallic platform to perform operations. Optional customer access accounts can be set with limited privileges (e.g. to allow view/restore of their own data). Multi-factor authentication (MFA) is enabled for all console access. Additionally, the connection between your AWS environment and Metallic is governed by secure IAM roles (via AWS STS) – no long-term credentials are stored, and least privilege access is configured.

- **Compliance Support:** The backup solution can help meet data retention requirements for regulations (HIPAA, GDPR, etc.) by ensuring data copies are kept for the required duration and are securely stored. Metallic is FedRAMP High ready and follows stringent security controls, which benefits regulated customers. We can provide reporting needed for audits (such as evidence of successful backup jobs, restore test logs, etc.).

2.8 Ongoing Management & Support

Continuous management is part of the service:

- **Proactive Backup Monitoring:** We continuously monitor backup job statuses, as detailed in the Monitoring section. Any failures or warnings are investigated and addressed by our team.

- **Issue Remediation:** If a backup job fails, our team will retry and/or troubleshoot the issue. We escalate to your team only if input is needed (for example, credentials update or if a source server is unreachable). Our goal is to resolve issues before they become problems (e.g. ensuring a successful backup runs after a failed one so that protection is up-to-date).

- **Restore Assistance:** When you need to perform a restore, you can simply contact our service desk with the request (unless you do it yourself via portal). We will then coordinate and execute the restore promptly, including any validation steps.

- **Configuration Changes:** If you need to add a new server to backup, adjust retention, or modify a schedule, just let us know – we will update the configuration as part of the service. Similarly, if you deploy a new AWS resource, we can include it in the backup scope if supported.

- **Periodic Reviews:** We will conduct periodic service reviews to discuss your backup environment – ensuring it continues to meet your needs, reviewing any capacity or performance trends, and planning for future needs. This is an opportunity for you to provide feedback and for us to suggest optimisations or upgrades.

2.9 Monitoring

Our team provides continuous monitoring of the backup environment to quickly identify and address any issues:

- We utilise Metallic's centralised monitoring dashboard and alerts to keep watch on all backup activities. Backup jobs are monitored 24/7. If a backup fails, completes with errors, or runs longer than expected, the system generates an alert that our engineers receive.

- **Daily Checks:** Every day, our team reviews the last 24 hours of backup jobs to verify success and identify any anomalies. This includes checking that all scheduled backups ran and reviewing any warnings (like skipped files). Any incidents and remediation steps taken are recorded in tickets or change requests.

- **Security Monitoring:** We also monitor for any unusual access or security events in the backup system. Metallic includes features like anomaly detection (spotting unusual data change rates that might indicate ransomware) – such events would alert us to potentially suspicious activity.

- **Capacity Monitoring:** The storage usage of your backups is tracked. We watch the consumption against quotas or thresholds. If you are nearing your subscribed storage limit, we will alert you well in advance (and discuss options like pruning data or adjusting the plan). The goal is no surprises in terms of running out of space or incurring overages.

3 Service Exclusions

3.1 Non-AWS Environments

By default, this service is focused on AWS cloud workloads. Data or systems outside of AWS (e.g. on-premises servers or other public cloud platforms) are not covered under this service. Backup of on-premise environments or other clouds can be provided via a separate service or an extended agreement, but are not included in the base scope here.

3.2 Advanced Cyber Recovery Features

Some of Commvault's cutting-edge disaster recovery and cyber resiliency features are **not included** in this version of the service. Specifically:

- **Cleanroom Recovery:** The ability to automatically create an isolated sandbox environment and restore systems (like Active Directory, critical servers, etc.) into it for malware scanning or forensic analysis is not part of the standard service. (Cleanroom Recovery is a new feature that deploys a separate AWS environment for recovery to test and ensure data is clean. This is on our roadmap but not offered yet in the base service.)

- **Cloud Rewind:** The capability to perform an automated, point-in-time "rewind" of an entire cloud environment (using technology like Appranix) is not included. Cloud Rewind acts as an AWS time machine – restoring not just data but also the cloud infrastructure and configuration to a previous clean state. This goes beyond traditional backups.

- **Instant Mass Restore for S3 (via specialised technology):** While we back up S3 data, ultra-fast restoration of massive S3 buckets (e.g. with billions of objects) via specialised snapshotting technology is not in scope until

that capability becomes generally available in the Metallic platform (this relates to forthcoming technology via Commvault's Clumio integration for instant S3 recovery, currently not standard).

3.3 Customer On-Premises Copy or BYO Storage (unless arranged)

The standard service stores backups in cloud (Metallic managed storage). Maintaining an additional copy of backups on customer-provided storage or physical media (like writing to tape, or replicating to a customer's own data center) is not included by default. If you require a local copy of backups or bring-your-own-storage approach for compliance, that would be outside this service's scope and can be discussed as a custom add-on.

3.4 Data Archival Beyond Retention Policy

Long-term archival storage (such as moving backups to deep archive for many years) beyond the defined retention is not included in base scope. The service keeps data as per the agreed retention (e.g. 30 days or 1 year). If you have needs for *indefinite or very long-term retention* (such as maintaining certain backups for 7+ years for compliance), this may fall outside the standard scope and require an archival add-on service or a tailored retention plan (which could incur additional cost).

3.5 Disaster Recovery Orchestration

While we facilitate data recovery, the broader process of full disaster recovery orchestration (automatically failing over entire applications, network reconfiguration, etc.) is not part of this backup service. For instance, we do not include runbooks to bring up complex multi-tier applications in DR, or tools to switch DNS, etc. The focus is on data restoration. (That said, the backup service provides the *foundation* for DR – data availability. Customers needing full DR planning can engage our consulting services separately.)

3.6 Live Database Cloning for Dev/Test

Using backups to spin up clones of databases or systems for dev/test on a frequent basis is not in the standard scope. We will of course do restores when requested (including to non-prod environments), but if you need *regular* automated clones (say nightly refresh of a dev database from production backup), that might be treated as a special requirement outside the basic backup/restore service.

3.7 Anything Not Explicitly Mentioned in Inclusions

General catch-all – if a service element is not listed in the inclusions above, it is not provided as part of this managed service. For example, end-user file backup from desktops, data encryption key management by the provider, or customised application-specific backup scripting – unless explicitly agreed, these are out of scope.

4 Customer Responsibilities

While we handle the heavy lifting for backup and recovery, there are some customer responsibilities and prerequisites to ensure the service operates smoothly. These define what we need from your side:

- **AWS Account and Access:** You will need to provide our team with appropriate access to your AWS environment for backup operations. We will supply a CloudFormation template or policy document to help set this up. It's your responsibility to deploy that in your AWS account with sufficient permissions (e.g. the ability to snapshot volumes, read instances, etc.).
- **Networking Connectivity:** Ensure that your AWS resources can communicate with the Metallic backup service endpoints. If your instances are in private subnets, you may need to allow egress to the internet or to specific Metallic IP ranges, or deploy a VPC endpoint if Metallic supports that. If a Backup Gateway appliance is used in

your environment, it will need outbound internet access to connect to Metallic. Typically, Metallic operates over secure HTTPS; you might need to adjust firewall rules or proxy settings to allow this. We will guide you on the exact requirements. Your responsibility is to work with us to configure any network or firewall settings on your side so that backups can flow.

- **Resource Identification:** Inform us which systems and data need to be protected. During onboarding and whenever you add new resources, it's important that you identify what should be backed up.
- **Application Consistency Coordination:** If certain applications require special steps to back up consistently (for example, quiescing a database, or pausing writes to a file system), you may need to coordinate with us on those. In many cases, Metallic can leverage AWS's native snapshot which is crash-consistent, or use application agents for consistency (for instance, VSS for Windows).
- **Data Accuracy and Completeness:** Ensure that the data sources we are backing up are the authoritative and complete sources that need protection.
- **Timely Communication:** Communicate any relevant changes or incidents in your environment that might affect backups. For example:
    - If you plan maintenance that might shut down an EC2 instance or make a database unavailable during the normal backup window, let us know so we can reschedule or be aware.
    - If you discover an issue in your data (like some files got corrupted by an application error), let us know – we might want to perform an extra backup or ensure that we have a clean restore point prior to the corruption.
    - If you add a large amount of data (say you bulk load 2 TB of new data into a system), giving us a heads-up is helpful so we anticipate a longer backup.
- **Access to Restored Data:** When we perform a restore, especially to production, we will coordinate with you for the timing and target. It's your responsibility to validate the data once restored (to confirm everything is as expected, no data missing). If we restore to an alternate location (say a different instance or a file share), you might need to move that data into your application or give users access.
- **Compliance and Policy Guidance:** If your organisation has specific policies (for example, data must not leave a certain country, or backups must be held for X years), you need to communicate those requirements to us clearly. We rely on you to provide the compliance criteria so we can configure the service appropriately.
- **Software Agents on Instances:** In scenarios where a Metallic agent might be needed on an EC2 instance (for specialised backup of that instance's content), you may need to allow installation of that agent. Our team will handle the install and config, but we need your permission and possibly assistance in accessing the instance (admin credentials or opening firewall on the instance for our agent communication).

5 Onboarding

To ensure a consistent and scalable onboarding experience for customers transitioning into our Managed Services offering, we have implemented a standardised onboarding package that is aligned to the customer's monthly AWS spend. This approach allows us to provide predictable effort, clearly defined deliverables, and consistent onboarding quality.

5.1 Onboarding Overview

Initial setup of the service is included:

- We work with your team to identify all workloads that need protection and gather requirements (RPO, retention, any special considerations).
- We assist in configuring an AWS IAM Role or roles that allow the Metallic service to access your AWS resources securely (often via a CloudFormation template provided by Metallic for cross-account access). This includes necessary permissions to perform snapshots, read data, etc., without overly broad access.
- Deployment or configuration of any required Backup Gateways (lightweight VM agents) in your AWS account, if needed for certain backup types (for instance, to stream backup data for file-level backups of EC2).
- Configuration of backup policies in Metallic: setting up schedules, retention, and backup content definitions for each workload.
- A full initial backup seeding of all in-scope data to establish baseline recovery points.
- Verification of backup jobs and a handover where we review how to request restores, interpret reports, and (if opted) how to use the self-service portal.

5.2 Onboarding Exclusions

To maintain clarity and ensure the onboarding scope remains focused and deliverable, the following items are not included in the standard onboarding fee:

- Configuration of **custom monitoring solutions** beyond the defined standard alarm set
- Refactoring of **IAM roles**, permission boundaries, or trust policy realignments
- **Landing zone redesign** or remediation for multi-account structures
- Integration of **third-party tooling** (e.g., SIEMs, CMDBs, enterprise ticketing systems)
- Establishment of **compliance-specific baselines** (e.g., PCI, CIS, GxP)
- **Workload-level onboarding**, including deep dives into CI/CD pipelines, application infrastructure, or deployment pipelines
- **Onboarding of additional service lines** (e.g. Sentinel One and Commvault/Druva)

Where any of the above are required, they will be scoped separately through the Professional Services team and delivered under a separate Statement of Work (SOW).

6 Service Management

Our service management approach ensures a seamless, efficient, and effective operation of the Platform Management Core service. We provide a dedicated service manager who acts as your primary point of contact. This manager is responsible for overseeing the delivery of services, managing the service relationship, and ensuring that the service aligns with your strategic business objectives. Regular service reviews are conducted ton a monthly basis to discuss service performance, Cost optimisation, Security, Green Ops, upcoming changes, and continual improvement opportunities.

Through our Customer Success program, we aim to align our deliverables to provide a service which helps you achieve you business goals.

6.1 Reporting and Reviews

We are committed to maintaining transparent communication and ensuring customers have full visibility of their backup solution.

6.1.1 Reporting Deliverables

We believe in transparency and keeping you informed about your data protection. We provide comprehensive regular reports as well as on-demand updates:

- **Monthly Backup Health Report:** Delivered monthly, this report summarises the overall health of your backups. It includes:
    - **Backup Job Summary:** number of successful backups vs. failures in the past month, broken down by week or day. We highlight any recurring issues and their resolution. Ideally, you will see a near-100% success rate, but if there were failures, we explain why and how they were fixed.
    - **Restore Activities:** a log of any restore requests fulfilled during the month (what was restored, when, and confirmation of success).
    - **Issues and Resolutions:** a section describing any notable incidents (e.g., a backup that kept failing due to a permission issue until we applied a fix) so you're aware of what happened and that it's resolved.
    - **Upcoming Actions:** if any action is needed or planned (e.g., "Upgrade to new version next month" or "Add new server X to backup as requested"), we note it.
- **Restore Test Report:** If you have opted for restore testing this report will include details of the restore test(s) we performed:
    - We specify which backup was tested – e.g. "February 15: Restored Server1 from the Jan 31 backup to a test instance".
    - The procedure and environment of the test (e.g. restored to an isolated VPC or to a sandbox folder).
    - The outcome of the test: success metrics (was the data fully readable and intact? Did the application start up correctly from the restore? How long did it take?).
    - Any issues discovered and corrections made.
    - By providing this, you have documented evidence for compliance/regulations that restore viability is regularly verified – a key component of many data protection standards.
- **Capacity and Usage Report:** We include a section (or a separate report) on storage utilisation:
    - Current total backup storage used vs. allocated.
    - Growth trend (how it changed month over month).
    - Breakdown by data type or server (e.g. how much each server or workload is contributing to the stored data).
    - If you are nearing a threshold of capacity, we'll make recommendations (such as increasing capacity or adjusting retention). Metallic also often provides deduplication stats; we can include stats like

deduplication ratios achieved, which show how much we optimized your data (for instance, “100 GB of source data was reduced to 40 GB in backup storage due to deduplication and compression”).

- **Report Delivery:** Reports are delivered in a convenient format (PDF or PPT summary). We can also review them with you on a call to answer any questions. Additionally, you have the option to access the Metallic dashboard which provides real-time information and some built-in reporting if you prefer direct visibility.

- **Ad-hoc Reporting:** You can request on-demand reports or status updates at any time. For instance, if you want to know “what was the last backup date of Server X” or “how many restores have we done this year,” our team can pull that information quickly.

6.1.2 Review Cadence

Customers will receive regular reviews on the below cadence, unless requested otherwise:

- **Monthly Service Review Meeting** – Led by your Service Delivery Manager (SDM) or Customer Success Manager (CSM), focusing on the monthly report findings, actions, and upcoming changes.
- **Quarterly Strategic Review** – For larger engagements or upon request, we can conduct a QBR that includes a roll-up of the last quarter’s backup reports, key trends, and discuss any changes needed in the service. This is more of a meeting than a report, but it’s part of our service culture to ensure the backup service continues to meet your business objectives.

Reports are typically delivered in advance of scheduled review meetings and distributed to named customer contacts via email.

7 Incident, Change and Problem Management

Tickets are raised through the following methods:

- Email: support@aws-bytes.co.uk
- OOH case logging phone number: 01628 965190
- Bytes Web Portal: https://cloudservices-support.zendesk.com/hc/en-gb
- Chat via Bytes Web Portal: https://cloudservices-support.zendesk.com/hc/en-gb
- Automated email alerts: support@aws-bytes.co.uk

7.1 Incident Management

Cloud Bridge operates a structured incident management process designed to minimise disruption and restore normal service operation as quickly as possible. All incidents are managed under a single framework, with categorisation aligned to SLA priority levels (P1–P4).

7.1.1 Scope of Incidents

Incidents cover a wide range of events that may impact your AWS environment. These include, but are not limited to:

- Alerts generated by monitoring tools (e.g., CloudWatch, third-party observability tools).
- Customer-reported issues (via the service desk, phone, or email).
- Proactively identified issues by Cloud Bridge engineers.

Incidents are categorised at logging in line with agreed SLA priorities (see Service SLAs).

7.1.2 Our Responsibilities

As part of incident management, Cloud Bridge is responsible for ensuring incidents are recorded, investigated, and resolved as efficiently as possible. This includes:

- **Logging** – Every incident is logged in our service desk (Zendesk) to ensure full auditability. Alerts from monitoring systems may be logged automatically.
- **Triage** – Engineers begin triage immediately upon picking up the incident, gathering context and isolating the issue.
- **Escalation Path** – Incidents follow a structured escalation chain:
    1. First/Second Line Engineer
    2. Team Lead
    3. Specialist Engineer
    4. Service Management
    5. Director-level escalation (if required)
- **AWS Escalation** – If the customer has Partner-Led Support or an active AWS support plan, Cloud Bridge will escalate to AWS on the customer's behalf and manage the case lifecycle.
- **Communication** – Customers receive regular updates in line with SLA priority (e.g., P1 hourly, P2 every 2 hours, etc.). Updates are logged in the ticket for traceability.
- **Resolution & Closure** – Once resolved, incident details, actions, and root cause are documented in the ticket.

7.1.3 Customer Responsibilities

To ensure incidents are prioritised and resolved effectively, customers are responsible for providing context and validation where needed. This includes:

- **Impact Identification** – Customers must identify the business impact of an incident when logging it to ensure correct prioritisation.
- **Validation** – Customers are requested to validate fixes, particularly where application testing is required. If no response is received, tickets will be closed after a pre-agreed timeframe, but can be reopened if further issues occur.
- **Transparency** – Customers should inform Cloud Bridge of planned changes or events that may trigger alerts, to avoid confusion with genuine incidents.

7.1.4 Scope Boundaries

Incident management focuses on AWS platform services under Platform Management Core. To ensure clarity of scope:

- Incident management covers **AWS services in scope of Platform Management Core only** (see Appendix – In-Scope Services). Customer applications and data are outside this scope.
- Recurrent or underlying issues identified during incident management may be raised as **Problem Management** items for root cause analysis. Where the resolution requires architectural redesign or significant project work, this will be delivered under a separate Professional Services Statement of Work (SOW).

7.2 Change Management

Cloud Bridge follows structured change management protocols to ensure that all changes to your AWS environment are controlled, approved, and documented. This protects service availability and ensures accountability for every modification.

7.2.1 What Constitutes a Change

A "Change" is defined as **any modification to your AWS environment**, including but not limited to:

- Configuration of an existing resource (e.g., updating a security group, resizing an instance, modifying IAM permissions).
- Addition of a new resource (e.g., deploying a new EC2 instance, adding a new S3 bucket).
- Deletion of an existing resource (e.g., decommissioning instances, removing a VPC component).

7.2.2 Our Approach to Change

- **Change Logging** – Every change is logged in our service desk (Zendesk), regardless of whether it is raised by Cloud Bridge or by the customer. This ensures a complete audit trail.
- **Approval Model** –
    - No change is applied without explicit customer approval **if it could have a detrimental impact on service availability, security, or costs**.
    - For minor, low-risk activities, customers may agree to a set of **standard pre-approved changes** that do not require approval each time. Even in these cases, a change will always be logged.
- **Execution & Scheduling** – Approved changes are scheduled at appropriate times to minimise disruption. Stakeholders are notified in advance of significant changes.
- **Transparency** – Change records include details of the request, approvals, impact assessment, rollback plan, and validation steps.

7.2.3 Customer Involvement

- Customers are responsible for providing business impact context for requested changes, as they will always have the best understanding of their applications.
- Customers must validate changes where business-level testing is required (e.g., application testing after a database change).
- If required, Cloud Bridge can attend **Customer Change Advisory Board (CAB) meetings** to discuss and present changes. Attendance must be requested and booked in advance.

7.2.4 Scope Boundaries

- Day-to-day operational changes (e.g., adding a single instance, adjusting monitoring alarms) are included in Platform Management Core.
- Larger-scale initiatives (e.g., workload migrations, VPC redesigns, or deployment of full new applications) are outside this scope and will be delivered under a separate Professional Services Statement of Work (SOW).

7.3 Problem Management

Problem Management is an integral part of Platform Management Core. It focuses on identifying and eliminating the underlying causes of incidents to prevent recurrence, improving overall service quality and stability of your AWS environment.

7.3.1 Our Responsibilities

Cloud Bridge takes a proactive role in analysing incidents and implementing long-term fixes where possible. This includes:

- **Root Cause Analysis (RCA)** – Conducting thorough investigations into significant or recurring incidents to determine their underlying causes.
- **Problem Logging** – Ensuring all problems are formally logged in our service desk for traceability, whether identified by Cloud Bridge or raised by the customer.
- **Resolution & Workarounds** – Developing and implementing permanent fixes where possible, or documenting workarounds if resolution requires wider architectural changes.
- **Continuous Improvement** – Identifying trends across multiple incidents and recommending improvements to reduce the likelihood of future problems.

7.3.2 Customer Responsibilities

Effective problem management requires input from customers to provide context on the business impact and application behaviour. Customers are responsible for:

- **Providing Context** – Supplying relevant details about application dependencies and business processes that may influence problem resolution.
- **Validation** – Testing and confirming that implemented fixes or workarounds resolve the problem in their business context.
- **Collaboration** – Working with Cloud Bridge to approve and schedule any changes arising from problem investigations.

7.3.3 Scope Boundaries

Problem management within Platform Management Core is limited to AWS services in scope of this service. To ensure clarity of responsibility:

- Problems identified at the **application or data layer** remain the responsibility of the customer.
- Problems that require **major architectural redesign or project work** will be flagged for Professional Services delivery under a separate Statement of Work (SOW).

8 Service Level Agreement (SLA)

The priority levels which drive the SLAs are based on the impact to the business and its users.

8.1 Response SLA

Cloud Bridge provides **response SLAs** (time to acknowledge and begin working on an incident) but not **fix SLAs**. Due to the varied and complex nature of AWS environments, resolution times cannot be guaranteed. Our commitment is to engage promptly, apply appropriate resources, and provide regular updates until resolution.

	Incident	Change/Request	Problem
Ticket Logged	15 mins	15 mins	
P1 – Urgent(*)(**)	15 mins	30 mins	1 hour updates

P2 - High(**)	1 hour	1 hour	2 hour updates
P3 - Medium(**)	4 hour	4 hour	4 hour updates
P4 - Low(**)	12 hour	12 hour	12 hour updates

**To ensure the fastest possible response, any P1 incident should be logged by telephone or immediately followed up with a telephone call. This guarantees that our engineers are engaged without delay.*

***P1 (Urgent) and P2 (High) incidents are measured against SLA targets on a 24/7 basis. P3 (Medium) and P4 (Low) incidents are measured against SLA targets only during Business Hours (Monday–Friday, 09:00–17:00 local time).*

8.1.1 SLA Category Description

Priority	Description
Urgent	A service / system which is critical for day-to-day operations is unavailable. A significant number of staff members are not able to perform their functions. The incident affects a large number of customers. The incident has the potential for major financial loss or damage to the organisation's reputation.
High	One or more departments is affected. A service / system which is significant for day-to-day operations is unavailable. The incident's sphere of impact is expanding rapidly, or quick action may make it possible to limit its scope. Financial loss and damage to the organisation's reputation are possible. Time-sensitive work or customer actions are affected. The incident affects high-status individuals or organisations (i.e., upper management or major clients).
Medium	Only a small number of users are affected. None of the services lost are critical. Financial loss and damage to the organisation's reputation are limited in scope.
Low	The effects of the incident appear to be stable. Affected services are optional and used infrequently. Important or time-sensitive work is not affected. No critical services are involved, and there is little or no potential for financial loss or loss of reputation.

8.2 Backup Success & Recovery Objectives

Area	Commitment / Target	Notes
Backup Success Rate	Target of 100% completion of scheduled backup jobs within their window	Monitoring detects failures/misses; corrective backup initiated within 24 hours.
First-Attempt Success	>99% of backups to succeed on first attempt	Internal processes aim to resolve failures (retry/fix) same day.
Critical Restore Request (Urgent)	Restore operations initiated within 1 hour (24×7 availability)	Example: production system outage. Small restores may complete in minutes; larger VM restores may take hours depending on size.

Normal Restore Request (Non-Urgent)	Restore operations initiated within 4 hours (business hours) or next business morning if low-priority overnight	Example: user file recovery. In practice, often faster than SLA. Completion depends on data size.
Disaster Recovery Scenario	Prioritisation of critical systems first, restores run in parallel across regions/accounts	No fixed RTO guaranteed (not a full DR contract), but significant resources applied to recover as quickly as possible.

8.3 Service Availability

The Metallic SaaS platform has a very high uptime (underlying infrastructure is fault-tolerant across availability zones). While a formal SLA from Commvault for Metallic is around 99.9% availability, for our managed service we ensure monitoring 24/7 such that if the platform had any disruption, we would know and communicate with you. Practically, you can expect the backup service to be continuously available. Any maintenance windows (rare, since updates are seamless) will be communicated. There is no daily operational dependence on on-prem hardware that could fail – everything is in the resilient cloud service.

8.4 Escalation

For all technical related matters, the support team have clear escalation routes to their higher-level technical colleagues and also to our 3rd party suppliers with whom we have underpinning support contracts in place with.

Escalation routes and contact numbers for any issues the customer feels are not being progressed in line with their expectations will be provided to all customers and this will give them access to the Cloud Bridge management team within and outside of normal working hours.