cloud bridge

# System Operations Suite

## Service Description

August 2025

aws PARTNER Advanced Tier Services

# Document Control

| | |
|---|---|
| **Author:** | Philip Reeve |
| **Date created:** | 07/07/2025 |
| **Classification:** | Public |
| **Document type:** | Service Description |

| Version | Modified Date | Description | Modified By |
|---|---|---|---|
| V0.1 | 07/07/2025 | Initial draft | Philip Reeve |
| V1.0 | 26/08/2025 | Major updates to several sections | Philip Reeve |

# Table of Contents



# 1 Overview

The **System Operations Suite** extends Platform Management Core to provide managed services inside your AWS EC2 instances. While AWS is responsible for the underlying cloud infrastructure, customers remain responsible for what happens at the operating system (OS) level.

System Operations is designed to remove this burden, offering discrete services such as in-guest troubleshooting and managed patching. Each service is **priced, scoped, and contracted individually**, allowing customers to adopt only the capabilities they need.

# 2 System Operations Suite

The System Operations Suite currently includes two core services, each designed to address common operational gaps inside customer-managed EC2 instances:

- **In-Guest Support & Troubleshooting** – Hands-on OS-level support for Linux and Windows instances, covering troubleshooting, configuration, log analysis, performance tuning, and security hardening.
- **EC2 Patch Management** – Fully managed, predictable patching cycles for EC2 instances, including patch assessment, scheduled deployments, rollback capability, and compliance reporting.

# 3 In-Guest Support & Troubleshooting

## 3.1 Scope of Services

AWS is responsible for the resilience of the underlying infrastructure, but the management of your EC2 instances at the operating system (OS) level remains your responsibility. **In-Guest Support & Troubleshooting** is designed to bridge that gap by providing Cloud Bridge engineers to act as an extension of your team, managing and resolving OS-level issues inside your instances.

This service ensures that your Linux and Windows workloads are configured, secured, and running efficiently — without the need to escalate across multiple providers or rely solely on in-house expertise.

### 3.1.1 What It Includes

The service provides hands-on OS-level support to diagnose and resolve issues, optimise performance, and improve security. Key capabilities include:

- **Troubleshooting & Remediation** – Rapid investigation and resolution of OS-level problems such as failed services, driver issues, or system instability.
- **Configuration Advice** – Best-practice guidance for OS settings, kernel parameters, services, and integrations with AWS-native tools.
- **User & Access Management** – Assistance with user account creation, permissions, and security policies at the OS level.
- **Log & Event Analysis** – Detailed review of system logs and events to trace root causes and implement corrective actions.
- **Performance Tuning** – Recommendations and configuration changes to optimise memory, CPU, and storage utilisation.
- **Security Hardening** – Applying OS-level security best practices (e.g., disabling unused services, enforcing password policies, enabling OS-native firewalls).

Access to instances is performed through secure, least-privilege methods. Where possible, Cloud Bridge will use **AWS Systems Manager (SSM)** to perform remote troubleshooting and remediation. Direct user account access will only be used where required and must be provided by the customer.

Together, these capabilities give customers peace of mind that their instances are stable, secure, and compliant with best practice.

### 3.1.2 Supported Operating Systems

In-Guest Support & Troubleshooting currently covers the following operating systems:

**Linux Distributions**

- Amazon Linux 2
- Ubuntu LTS (18.04, 20.04, 22.04)
- Red Hat Enterprise Linux (RHEL 7, 8, 9)
- CentOS (7 & 8, supported until EOL)
- SUSE Linux Enterprise Server (SLES 12, 15)

**Windows Server**

- Windows Server 2012 & 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Support for other distributions or versions may be considered on request but may require a separate scope of work.

## 3.2 Exclusions

The following are not included in In-Guest Support & Troubleshooting:

- Support for customer-developed or third-party applications.
- Database administration (schema management, tuning, query optimisation).
- Middleware or application stack management (e.g., Java, .NET, Tomcat, IIS).
- Major OS upgrades or replatforming activities.
- Development of compliance frameworks (e.g., PCI, HIPAA) — though Cloud Bridge will align to security best practices.

## 3.3 Customer Responsibilities

To enable effective support, customers must:

- **Provide Access** – Create and maintain user accounts for Cloud Bridge engineers to access managed instances. This is normally achieved through named users or temporary credentials in line with customer security policies.
- **Permit Remote Operations** – Allow Cloud Bridge to perform remote actions via AWS Systems Manager (SSM) where supported, reducing the need for direct log-in access and ensuring secure, auditable operations.
- **Knowledge Transfer** – Provide initial knowledge transfer during onboarding of existing OS configurations, critical workloads, and business impact priorities.
- **Context & Impact** – Supply application context for incidents and requested changes, as customers retain the best knowledge of how OS-level changes may affect workloads.
- **Validation** – Validate application-level functionality after OS-level changes or fixes have been applied.
- **Transparency** – Notify Cloud Bridge of customer-initiated configuration changes to avoid duplication of effort or misinterpretation of monitoring alerts.

## 3.4 Service Level Agreement

### 3.4.1 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).*

### 3.4.2 SLA Category Description

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

## 3.5 Onboarding – In-Guest Support & Troubleshooting

### 3.5.1 Onboarding Overview

Each engagement includes a dedicated onboarding SME and project management oversight to guide the customer through setup and readiness.

The following activities are included by default:

- **Pre-onboarding validation** – Confirming IAM roles, SSM agent status, and required user account setup for Cloud Bridge engineers.
- **Kick-off session** – Customer and service team alignment on scope, roles, responsibilities, and access requirements.
- **Access enablement** – Configuration of required IAM roles and/or named user accounts to allow Cloud Bridge secure in-guest access, supported by Systems Manager where possible.
- **Knowledge transfer** – Customer walkthrough of current OS configurations, workloads, and business priorities.
- **BAU alignment** – Establish relevant contacts for incident, request, and change management processes at the OS level.
- **Service readiness** – Test connectivity and access, validate monitoring integration, and confirm service activation.

### 3.5.2 Onboarding Exclusions

The following are not included in the standard onboarding fee:

- Redesign or remediation of operating system builds.
- Migration of workloads between operating systems or versions.
- Development of custom automation or OS-level tooling.
- Compliance baseline establishment (e.g., CIS hardening) unless separately scoped.
- Onboarding of application or database workloads above the OS.

Where these are required, they will be scoped and delivered via Professional Services.

# 4 EC2 Instance Patching

## 4.1 Scope of Services

Keeping EC2 instances patched is critical to maintaining **security, compliance, and performance**. Unpatched vulnerabilities are among the most common attack vectors, and even a single missed update can create significant risk.

Cloud Bridge's **EC2 Patch Management** service provides **controlled, predictable, and automated patching cycles**. We orchestrate patching through automated tooling (AWS Systems Manager or third-party platforms), ensuring instances are updated consistently while minimising disruption. Cloud Bridge does not log directly into instances to perform patching; all operations are delivered via secure, automated methods.

### 4.1.1 What It Includes

This service provides the orchestration of patching for managed instances:

- **Patch Assessment** – Continuous monitoring of OS-level patch availability across managed instances.
- **Scheduled Deployment** – Patches applied during agreed maintenance windows via automated tooling.
- **Rollback Capability** – Instances can be restored to pre-patch state if issues occur, where rollback functionality is enabled.
- **Compliance Alignment** – Baselines aligned to customer-defined policies and regulatory requirements.
- **Reporting & Verification** – Post-patch reporting using monitoring tools, instance screenshots, or automation outputs to confirm patch execution status.

**Important Notes:**

- **Patch Testing** – Cloud Bridge does not test or validate patches for application compatibility. Customers are responsible for testing in their **own development or staging environments** prior to production rollout. Cloud Bridge can support orchestration of patching in those environments if requested.
- **Validation** – Cloud Bridge validates patch execution at the OS level via automation outputs (e.g., compliance reports, screenshots, monitoring status). We do not log into servers to manually verify patch success.
- **Baseline Management** – Customers are required to define patch baselines and provide input on exclusions (e.g., specific patches not to install, instances not to patch). Cloud Bridge orchestrates patching according to these baselines.

### 4.1.2 Supported Operating Systems

EC2 Patch Management currently supports the following operating systems:

**Linux Distributions**

- Amazon Linux 2
- Ubuntu LTS (18.04, 20.04, 22.04)
- Red Hat Enterprise Linux (RHEL 7, 8, 9)
- CentOS (7 & 8, supported until EOL)
- SUSE Linux Enterprise Server (SLES 12, 15)

**Windows Server**

- Windows Server 2012 & 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Support for other distributions or versions may be considered on request but may require a separate scope of work.

## 4.2 Exclusions

The following are not included in EC2 Patch Management:

- Application-level patching (databases, middleware, or customer software).
- Major OS version upgrades or replatforming (e.g., RHEL 7 → 8 migrations).
- Testing patches against bespoke customer applications (customers are responsible for validating business impact).
- Development or management of custom patch pipelines outside Cloud Bridge's standard framework.
- End-user device patching (desktops, laptops, or non-EC2 workloads).
- Manual server logins to perform or validate patching.

## 4.3 Customer Responsibilities

To enable Cloud Bridge to deliver patch management effectively, customers must:

- **Approve Schedules** – Agree and maintain patching windows to minimise disruption to business operations.
- **Baseline Definition** – Provide input into required patch baselines, including excluded patches or instances.
- **Testing** – Perform application-level testing in development or staging environments prior to production patching.
- **Access Enablement** – Permit Cloud Bridge to execute patching via AWS Systems Manager or agreed third-party platforms.
- **Validation** – Validate that business applications continue to function correctly after OS patches are applied.
- **Transparency** – Notify Cloud Bridge of changes or exceptions that may affect patch cycles.

## 4.4 Service Level Agreement

### 4.4.1 Change SLA for Patching

To ensure patching runs are scheduled effectively and with minimal disruption, Cloud Bridge applies the following SLAs to patch-related change requests. These define the expected notice periods for standard, short-notice, and emergency patching scenarios.

| Request Type | Description |
|---|---|
| Standard Patching Requests | Customers must submit a change request to schedule a patching run with a minimum of 5 business days' notice. This ensures sufficient time for scheduling, baseline validation, and maintenance window alignment. |
| Short-Notice Requests | Requests submitted with less than 5 business days' notice will be assessed on a best-effort basis and may require rescheduling if capacity is not available. |
| Emergency Patching (Security Threats) | In the event of a major incident or security vulnerability (e.g., a critical CVE or zero-day exploit), Cloud Bridge will prioritise emergency patching requests. These must be raised as a P1 change and followed up by phone to ensure immediate engagement. Emergency patching will be executed as quickly as possible, subject to customer approval and maintenance window agreement. |

### 4.4.2 Response SLA for Patch Related Incidents

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).*

### 4.4.3 SLA Category Description

| Priority Level | Description |
|---|---|

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

## 4.5 Onboarding – EC2 Patch Management

### 4.5.1 Onboarding Overview

Each patch management onboarding engagement includes a dedicated SME and project oversight to ensure patch orchestration is implemented securely and consistently.

The following activities are included by default:

- **Pre-onboarding validation** – Confirm Systems Manager agent status, IAM permissions, and connectivity for patch orchestration.
- **Kick-off session** – Customer and service team alignment on patching scope, roles, responsibilities, and change management process.
- **Baseline definition** – Work with customer to define patching baselines, including exclusions (instances or patches not to be applied).
- **Schedule agreement** – Define and agree patching windows, emergency patching escalation paths, and approval workflows.
- **Test cycle** – Run an initial patch test on a limited set of instances to validate orchestration and reporting.
- **Reporting setup** – Configure reporting outputs to confirm patching results via monitoring tools and automation.
- **Service readiness** – Validate baseline, schedule, and access before transitioning into BAU patching operations.

### 4.5.2 Onboarding Exclusions

The following are not included in the standard onboarding fee:

- Application-level testing of patches for compatibility.
- Development of bespoke patching pipelines outside AWS Systems Manager or approved third-party platforms.
- Migration of workloads to supported OS versions.
- Remediation or patching of legacy OS instances not supported by Systems Manager.
- Compliance framework certification or audit preparation.

Where these are required, they will be scoped separately and delivered under Professional Services.