AWS MANAGED SERVICE BY INTERVISION - SERVICE GUIDE

Last Modification Date: 01/29/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1 OVERVIEW

The AWS Managed Service (AMS) by InterVision is a managed service for operations of your AWS environments. This Service combines InterVision Managed Services with AWS Managed Service (provided by AWS) to provide a broad suite of infrastructure operations, IT management and ongoing improvements. This Service includes InterVision services personnel comprising of a Cloud Service Deliver Manager, a Cloud Architect and managed services team to assist, when required, with service requests in to the AMS service offerings.

AMS by InterVision provides the tools, processes and personnel for the ongoing operations management such as patch, continuity management, security management and IT processes such as incident, change and service requests. The Service is available in two service levels - Plus and Premium - which defines the level of responsiveness for service requests, change requests and incidences. These service levels can selectively applied based upon application requirements.

This service can be combined with additional InterVision services including Migration, DevOps, Network and Security management and other services. See associated service guide and service description for details regarding these additional services. This Service Guide covers the AWS Managed Service by InterVision.

2 SERVICE DESCRIPTION AND DETAILS

AWS Managed Services offers the following features for supported AWS services[1]:

1. **Logging, Monitoring, Guardrails, and Event Management**[2] – AWS Managed Services configures and monitors the customer's Managed Environment for logging activity and defines Alerts based on a variety of health checks. Alerts are investigated by AWS Managed Services for applicable AWS services, and those that negatively impact the customer's usage of those services result in the creation of Incidents. AWS Managed Services aggregates and stores all logs generated as a result of all operations in CloudWatch, CloudTrail, and system logs in S3. Upon request, customers can ask for additional alerts to be put in place. In addition to AWS Managed Services' Preventative Controls, AWS Managed Services deploys configuration guardrails and Detective Controls to provide ongoing protection for customers from misconfigurations that could reduce the operational and security integrity of the managed accounts, and to enforce customer controls such as tagging and compliance. When a monitored control is detected an alarm is generated that results in notification, modification, or termination of resources based on pre-defined AWS Managed Services defaults that can be modified by the customer.
2. **Continuity Management** – AWS Managed Services provides backups of resources using standard, existing AWS Backup functionality on a scheduled interval determined by the customer. Restore actions from specific snapshots can be performed by AWS Managed Services per customer RFC. Data changes that occur between snapshot intervals are the responsibility of the customer to backup. Customers may submit an RFC for backup/snapshot requests outside of scheduled intervals. In the case of Availability Zone (AZ) unavailability in a Region, with the customer's permission, AWS Managed Services will restore the Managed Environment by recreating new Stack(s) based on templates and available EBS snapshots of impacted Stacks.
3. **Security and Access Management** – AWS Managed Services provides Security Management services such as configuring anti-malware protection, intrusion detection and intrusion prevention systems. AWS Managed Services also configures default AWS security capabilities that will be approved by the customer during onboarding, such as Identity Access Management (IAM) roles and EC2 security groups, and uses standard AWS tools (e.g. GuardDuty) to monitor and respond to security issues. Customers manage their users via an approved directory service provided by the customer. [3]
4. **Patch Management** – AWS Managed Services applies and installs updates to EC2 instances for Supported Operating Systems and software pre-installed with Supported Operating Systems.[4] AMS offers two models to execute patching:
   1) AMS Standard Patch for traditional account-based patching, and 2) AMS Patch Orchestrator, for tag-based patching. In AMS Standard Patch, a monthly maintenance window is chosen by the customer for AWS

Managed Services to perform most patching activities. AWS Managed Services applies Critical Security Updates outside of the selected maintenance window and Important Updates during the selected maintenance window. AWS Managed Services will notify the customer in advance with the details of the upcoming updates. Customers can exclude Stacks from Patch Management or reject updates. With AMS Patch Orchestrator, a default maintenance window per account is defined by the customer for AWS Managed Services to perform patching activities. Customers can schedule additional custom maintenance windows for AWS Managed Services to patch a specific set of instances defined by customers via Tags. AWS Managed Services will apply all available Updates, but customers can filter or reject updates by creating a custom patch baseline. For both models, if the customer approves or rejects an update provided under Patch Management but later changes their mind, the customer is responsible for initiating the update via RFC. AWS Managed Services will track the patch status of resources and highlight systems that aren't current in the monthly business review. Patch Management is limited to Stacks in the Managed Environment, including all AWS Managed Services Managed Applications and supported AWS services with patching capabilities (e.g. RDS). In order to support all types of infrastructure configurations when an update is released, AWS Managed Services a) updates the EC2 instance and b) provides an updated AWS Managed Services AMI for the customer to use. It is the customer's responsibility to install, configure, patch, and monitor any additional applications not specifically covered above.

5. **Change Management** – AWS Managed Services offers Change Management, which is the mechanism for customers to get access to or affect any changes in their Managed Environment. The customer creates a Request for Change (RFC) using the AWS Managed Services Interface. Most RFCs requested by the customer will be executed automatically. AWS Managed Services also creates RFCs to access customer resources or make changes. All RFCs follow a defined Change Management process. Access to customer resources within a Managed Production Environment is authorized through RFCs, while access to customer resources in a Managed Non-production Environment is authorized through RFC and, optionally, through a specialized Customer Developer IAM role ("Developer Mode") upon request. AWS Managed Services approves and executes RFCs that can be executed using the features or functionalities of AWS services. The customer may designate a start time for the requested change to be performed through the RFC process. Customers can also use Change Management to configure AWS Service Offerings in the Managed Environment.
6. **Automated and Self-Service Provisioning Management** – Customers can provision AWS resources on AWS Managed Services in several ways: 1) submit provisioning and configuration Change Types, 2) deploy AMS-provided securityhardened AMIs inclusive of the customer application, 3) deploy full Stacks using CloudFormation templates, 4) deploy via their integrated ITSM, and 5) configure AWS services directly using Self-service Provisioning for select AWS services (see "Supported AWS Services"). To provide Self-service Provisioning capabilities, AWS Managed Services has created elevated IAM roles with permission boundaries to limit unintended changes from direct AWS service access. Roles do not prevent all changes and the customer is responsible to adhere to their internal controls, compliance, and validate that all AWS services being used meet the required certifications[5]. For resources provisioned through Self-Service, AWS Managed Services provides Incident Management, Detective Controls and Guardrails, Reporting, Designated Resources (Cloud Service Delivery Manager and Cloud Architect), Security & Access, and technical support via Service Requests. Additionally, where applicable, the customer assumes responsibility for continuity management, patch management, infrastructure monitoring, and change management for resources provisioned and/or configured outside of AWS Managed Services Change Management system.
7. **Incident Management** – AWS Managed Services proactively notifies customers of Incidents detected by AWS Managed Services. AWS Managed Services responds to both customer-submitted and AMS-generated Incidents and resolves Incidents based on the Incident priority[6] . Unless otherwise instructed by the customer, Incidents that are determined by AWS Managed Services to be a risk to the security of the customer's Managed Environment and Incidents relating to the availability of AWS Managed Services and other AWS services will be proactively actioned. AWS Managed Services takes action on all other Incidents once customer authorization is received. Recurring Incidents are addressed by the Problem Management Process.

8. **Problem Management** - AWS Managed Services performs trend analysis to identify and investigate Problems and to identify the root cause. Problems are remediated either with a workaround or a permanent solution that prevents recurrence of similar future service impact. A Post Incident Report (PIR) may be requested for any Priority 1 Incident upon resolution. The PIR captures the root cause and preventative actions taken, including implementation of preventative measures.
9. **Reporting** – AWS Managed Services provides customers with a monthly service report which summarizes key performance metrics of AWS Managed Services, including an executive summary and insights, operational metrics, managed resources, AMS SLA adherence, and financial metrics around spend, savings and cost optimization. Reports are delivered by an AMS Cloud Service Delivery Manager (CSDM) assigned to the customer.
10. **Service Request Management** – Customers can request information on their Managed Environment, AWS Managed Services, or AWS Service Offerings by submitting Service Requests using the AWS Managed Services Interface. Service Request types also include "How to" questions about AWS services and features, troubleshooting API issues, customer service requests and technical support cases.
11. **Service Desk** – AWS Managed Services staffs engineering operations with full-time Amazon employees to fulfill nonautomated requests including Incident Management, Service Request Management, and Change Management. The Service Desk operates 24 x 7 365 days a year.
12. **Designated Resources** – Each Customer is assigned a Cloud Service Delivery Manager (CSDM) and a Cloud Architect (CA). 1) CSDMs can be contacted directly, perform service reviews, and delivery reporting and insights through all phases of the implementation, migration and operational life cycle. CSDMs conduct monthly business reviews and detail items such as financial spend, cost-saving recommendations, service utilization, and risk reporting. They dive deep into operational performance statistics and provide recommendations of areas of improvements. 2) CAs can be contacted directly and provide technical expertise to help customers optimize their use of AWS Cloud. Example activities include, workload selection for migration, assisting with the on-boarding additional accounts and workloads, acting as the technical lead in operational activities such as game days, disaster recovery testing, problem management, and technical advice to get the most out of AWS Managed Services and AWS. CAs drive technical discussions at all levels of the customer's organization and will assist with incident management, making trade-offs, establishing best practices, and technical risk mitigation.
13. **Developer Mode** – This feature enables developers and migration teams to iterate their designs quickly within AWS Managed Services-configured Plus accounts7 by allowing direct access to AWS service APIs and the AWS Console. Once architectural designs and configurations have been finalized, customers can test their integration within the same account by creating and submitting an AWS CloudFormation template via an automated Request for Change. Finalized templates also follow the same automated Request for Change provisioning process in staging and production accounts. Any workloads provisioned via Change Management in Developer Mode enabled accounts will be supported like any other workload on AWS Managed Services, and can be used for long-running test workloads that mirror production environment. Resources provisioned and/or configured outside of the Change Management process are the responsibility of customers to manage (See "6. Automated and Self-Service Provisioning Management).
14. **Enterprise Support** – Accounts enrolled in AWS Managed Services will receive Enterprise-level Premium Support at no additional cost, subject to the following limitations:
    a. All support services may be provided directly by AWS Managed Services personnel.
    b. AWS Managed Services customers will not receive training discounts or credits unless they are entitled to such credits under a separate agreement.
    c. If AWS Managed Services is enabled on an evaluation basis, AWS Managed Services Evaluation Accounts will not receive Enterprise-level Premium Support during the evaluation period.

    Additional information concerning Enterprise Support can be found at https://aws.amazon.com/premiumsupport/plans/enterprise/.

[1] See "Supported AWS Services" section below for a list of supported AWS services.
[2] Refer to the AWS Managed Services User Guide for details on which supported AWS services have logging and monitoring enabled.
[3] See "Supported Configuration" section below for a list of approved directory services.
[4] See "Supported Configuration" section below for a list of supported operating systems.
[5] See https://aws.amazon.com/compliance/ for details on AWS compliance requirements.
[6] See the AWS Managed Services Service Level Agreement[1] for more information.
[7] See the AWS Managed Services Service Level Agreement[2] for more information on Plus Accounts.

2.1 CLOUD SERVICE DELIVERY MANAGER

You will be assigned a Cloud Service Delivery Manager. This InterVision service manager will facilitate operational reviews, deliver insights and assist with services. This includes:

- Provide Service/Technical Reviews
- Share Cost Optimization recommendations
- Identify risks
- Deep dive into operational performance and utilization
- Enable technical assistance that includes runbooks, game day, DR test problem management, improvement recommendations
- Escalation management

2.2 CLOUD ARCHITECT

You will be provided an oparations Cloud Architect to be the technical resource to help navigate cloud computing. This adviser will offer AMS specific advice on the architecture to ensure you are getting the full value of the AMS feature set. The cloud architect will assist in solving difficult problems and engage with you regarding incidents, trade-offs, best practices, and risk management. In addition, the cloud architect can assist with game day scenarios, continuous improvements and helping you get the most out of AWS.

Supported Configuration

- **Supported Language -** Intervision and AWS Managed Services is available in English
- **Supported Operating Systems** – AWS EC2 created AMIs for RHEL 7.x, RHEL 6.5+, Microsoft Windows Server 2019, Microsoft Windows Server 2016, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2008 R2, Amazon Linux and Amazon Linux 2, Cent OS 6.5+, Cent OS 7.x, and SUSE Linux Enterprise Server 12 SP4
- **Supported AWS Regions** – US East (Virginia), US West (N. California), US West (Oregon), US East (Ohio), Canada (Central), South America (São Paulo), EU (Ireland), EU (Frankfurt), EU (London), Asia Pacific (Mumbai), Asia Pacific (Sydney), Asia Pacific (Singapore), Asia Pacific (Tokyo)
- **Supported Security Software** – Deep Security from Trend Micro
- **Approved Directory Services** – Microsoft Active Directory (AD)

1 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf
2 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf

2.3 SUPPORTED AWS SERVICES

AWS Managed Services provides operational management support services for the following AWS services. Each AWS service is distinct and as a result AMS' level of operational management support varies depending on the nature and characteristics of the underlying AWS service. Specific AWS services are grouped based on the complexity and scope of the operational management support service provided by AWS Managed Services. AWS Managed Services pricing reflects the level of operational management support and can be found in the InterVision AWS Managed Services Addendum - Rate Card.[3]

Note: In the below table, one star (*) represents services that are deployed within an AMS managed environment by a customer using the AWS Console and APIs. See 'Automated and self-service provisioning management' in AMS features[4] for additional details on customer responsibilities when provisioning and configuring services in this manner. Two stars (**) indicates that EC2 on AWS Outposts will be billed as a Group B service; all other resources hosted on AWS Outposts will be billed at their standard rate.

Group A	Group B*	Group C - Full Management
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon Simple Storage Service Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon ECS Fargate* Amazon Elastic Container Service for Kubernetes* Amazon EKS on AWS Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge / CloudWatch Events* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kinesis Analytics* Amazon Kinesis Firehose* Amazon Kinesis* Amazon Kinesis Video Streams* Amazon Lex* AWS Migration Hub Amazon MQ* Amazon QuickSight*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon Elasticsearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service

3 https://intranet.intervision.com/display/PT/InterVision+AWS+Managed+Service+Addendum+-+Rate+Card
4 https://docs.aws.amazon.com/managedservices/latest/userguide/ams-sd.html#features

Group A	Group B*	Group C - Full Management
	Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkDocs* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

3 ROLES AND RESPONSIBILITIES

The Services manages customer's AWS infrastructure. The table below provides an overview of the responsibilities of customer, AWS Managed Services and InterVision for activities in the lifecycle of an application running within the Managed Environment.

- "R" stands for responsible party that does the work to achieve the task.
- "C" stands for consulted; a party whose opinions are sought, typically as subject matter experts; and with whom there is bilateral communication.
- "I" stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.
- "Self-service Provisioning" refers to resources that are provisioned by the customer via self-service through the AWS API or Console.

General	Customer	AWS Managed Services by InterVision
AWS Account Information	R	I
Customer Escalation Information	R	I
Identify user roles (Admin., Change Approver,....)	R	I
Implementation and Configuration	**Customer**	**AWS Managed Services by InterVision**
AWS Account Creation and Handover to AWS Managed Service for account design and build	R	C, I
Establish access to the AWS console, AWS Managed Services interface and Customer active directory	R	C, I
Email Alias Creation	R	C, I
Allocate private address space for VPCs (e.g. /16)	R	C, I
Trend Micro subscription	R	C, I
VPN Tunnel turn-up	R	R
Active Directory federation turn-up	R	R
Active Directory trust configuration	R	R
During on-boarding, create cross-account IAM Admin roles within each managed account	R	C
Deploy AMS landing zone environment	C	R
Use RFC process to create application Accounts	R*	C, I
Application Migration	R*	I

Application Lifecycle	**Customer**	**AWS Managed Services by InterVision**
Application development	R	I
Application infrastructure requirements analysis and design	R*	C, I
Design and optimization for non-standard AMS stacks	R	C
Design and optimization of AMS standard stack	I	R
Application deployment	R*	C, I
AWS Infrastructure deployment	C	R
Application monitoring	R*	I
Application testing/optimization	R*	I
AWS infrastructure optimization guidance	I	R
AWS infrastructure monitoring	I	R
Troubleshoot and resolve application issues	R*	C
Troubleshoot and resolve AWS network issues	C	R
Troubleshoot and resolve operating system and infrastructure issues *Self-Service Provisioning*	C R	R C
Networking	**Customer**	**AWS Managed Services by InterVision**
Managed Environment VPC and VPC set-up and configuration	C	R
Allocate private address space for VPCs (e.g. /16)	R	C, I

Configure & Operate non-AWS Managed Services, Customer managed Firewalls/Proxy/Bastions/HOSTs	R*	C, I
Configure & Operate AWS Security Groups/NAT/ Customer Bastions/NACL inside the Managed Environment	I	R
Networking (e.g. DirectConnect) configuration and implementation within customer network	R*	C
Networking configuration and implementation within the Managed Environment	C	R
Managed Environment Configuration	**Customer**	**AWS Managed Services by InterVision**
Define default Auto Scaling settings for baseline Stack templates	I	R
Recommend RI optimization	C	R
Purchase RI and PIOP capacity	R	C, I
Remove capacity when capacity is over provisioned (when supported by customer application)	C	R
Create/update AWS customer specific account information for AWS Managed Services	C	R
Create/update AWS customer specific technical information for AWS Managed Services	C	R
S3 configuration *Self-Service Provisioning*	C R	R C, I
Glacier configuration	C	R
Define archival policy	R	C
Archival policy configuration	C	R

Selecting customer maintenance window	R	C, I
AWS RDS Management	**Customer**	**AWS Managed Services by InterVision**
Monitor master/slave/RO replication health	I	R
Identify RCA of master failover	I	R
Automated snapshot (backup) configuration *Self-Service Provisioning*	C R	R C, I
Coordinate and schedule DB engine patch management *Self-Service Provisioning*	C R	R C, I
Recommend DB storage and PIOP capacity *Self-Service Provisioning*	C R	R C, I
Recommend instance sizing for running databases *Self-Service Provisioning*	C R	R C, I
Recommend RI optimization for Managed Environment *Self-Service Provisioning*	C R	R C
RDS performance monitoring (CloudWatch) *Self-Service Provisioning*	I R	R C, I
RDS event subscription configuration (SNS) *Self-Service Provisioning*	C R	R C, I
RDS security group configuration *Self-Service Provisioning*	C R	R C, I
RDS engine parameter/option configuration	R	C, I
DB table design	R*	I
DB indexing	R*	I

DB log analysis	R*	I
Change Management	**Customer**	**AWS Managed Services by InterVision**
Creating Customer RFCs (E.g. access to resources, creating/updating/deleting managed Stacks, deploying/ updating applications, changes to configuration of AWS Service Offerings)	R	C, I
Approving Customer RFCs	I	R
Creating AWS Managed Services RFCs (E.g. access to resources, creating resources on customer's behalf, applying updates to OS as part of Patch Management)	I	R
Approving non-automated RFCs	R	I
Submitting request for new Change Types	R	C
Creating new Change Types	I	R
Maintenance of application change calendar	R	I
Notice of upcoming Maintenance Window	I	R
Provisioning	**Customer**	**AWS Managed Services by InterVision**
Customer specific additions to AWS Managed Services baseline AMI	R*	C
Configure additional approved Change Types used to provision Stack templates	C	R
Launch managed Stacks and associated AWS resources submitted through AMS change management process. *Self-Service Provisioning*	I R	R C, I

Install/Update custom and 3rd party applications on Instances provisioned through AMS change management process.	R*	I
Provisioning - Stack Architecture	**Customer**	**AWS Managed Services by InterVision**
Providing OS licenses (including usage fees for the applicable AWS services – e.g. EC2 and RDS) *Self-Service Provisioning*	I R	R I
Define baseline infrastructure templates (Stacks) for application deployment *Self-Service Provisioning*	I R	R C, I
Creating baseline approved AMIs	I	R
Evaluate customer application inventory and determine fit with available infrastructure templates (Stacks)	R	C, I
Define unique Stacks that are in addition to the baseline template offerings	R	C
Logging, Monitoring and Event Management	**Customer**	**AWS Managed Services by InterVision**
Recording AWS infrastructure change logs	I	R
Recording all application change logs	R	C
Installation and configuration of agents and scripts for patching, security, monitoring, etc. of AWS infrastructure provisioned through the AMS change management process. *Self-Service Provisioning*	I R	R C
Define customer specific monitoring and incident requirements	R	C
Configuring AWS alarms for Managed Environment	I	R

Monitoring all AWS alarms *Self-Service Provisioning*	I R	R C
Investigating infrastructure Alerts for Incident notification *Self-Service Provisioning*	I R	R C
Investigating application alarms	R*	C
Incident Management	**Customer**	**AWS Managed Services by InterVision**
Proactively notify Incidents on AWS infrastructure based on monitoring *Self-Service Provisioning*	I R	R C
Handle application performance issues and outages	R*	I
Categorize Incident priority	I	R
Provide Incident response	I	R
Provide Incident resolution / infrastructure restore	C	R
Problem Management	**Customer**	**AWS Managed Services by InterVision**
Identify Problems in Managed Environment	C	R
Perform RCA for Problems in Managed Environment	C	R
Remediation of Problems in Managed Environment	C	R
Identify and remediate application problems	R	I
Security Management	**Customer**	**AWS Managed Services by InterVision**

Customer infrastructure security and/or establishing baseline for security compliance process as determined and agreed to during customer onboarding. *Self-Service Provisioning*	C R	R C
Maintaining valid licenses for Managed Security Software	R	I
Configure Managed Security Software *Self-Service Provisioning*	I R*	R I
Update Managed Security Software *Self-Service Provisioning*	I R	R I
Monitoring malware on instances provisioned through the AMS CM process. *Self-Service Provisioning*	I R	R I
Maintaining and updating virus signatures *Self-Service Provisioning*	I R	R I
Remediating instances infected with malware *Self-Service Provisioning*	C R	R I
Security event management	C	R
Security - Access Management	**Customer**	**AWS Managed Services by InterVision**
Manage the lifecycle of users, and their permissions for local directory services, which are used to access AWS Managed Services	R	I
Operate federated authentication system(s) for customer access to AWS console/APIs	R	C
Accept and maintain Active Directory (AD) trust from AWS Managed Services AD to customer managed AD	R	C

During on-boarding, create cross-account IAM Admin roles within each managed account	R	C
Secure the AWS root credential for each account	I	R
Define IAM resources for Managed Environment	C	R
Manage privileged credentials for OS access for AMS engineers	I	R
Manage privileged credentials for OS access provided to customer by AMS	R	I
Patch Management	**Customer**	**AWS Managed Services by InterVision**
Monitor for applicable updates to supported OS and software preinstalled with supported OS for EC2 instances *Self-Service Provisioning*	I R	R C
iNotify customer of upcoming updates (*applies to AMS Standard Patch only*)	I	R
Exclude certain updates and/or certain Stacks from patching activities	R	I
Define default and custom maintenance windows schedules and other parameters (e.g. maintenance window duration) to apply patches (*applies to AMS Patch Orchestrator only*)	R	I
Define custom Patch Baselines to filter and exclude specific patches (*applies to AMS Patch Orchestrator only*)	R	I
Tag instances to associate them with custom maintenance windows and Patch Baselines (*applies to AMS Patch Orchestrator only*)	R	C, I
Track the patch status of resources and highlight systems that aren't current in the monthly business review.	C	R

Apply updates to EC2 instances per Customer instructions *Self-Service Provisioning*	I R	R C
Patch development software (.NET, PHP, Perl, Python)	R*	I
Patch, and monitor middleware applications (e.g. BizTalk, JBoss, WebSphere) *Self-Service Provisioning*	R*	C I
Patch, and monitor custom and 3rd party applications *Self-Service Provisioning*	R*	C I
Continuity Management	**Customer**	**AWS Managed Services by InterVision**
Specify backup schedules	R	I
Execute backups per schedule *Self-Service Provisioning*	I R	R C
Validate backups	R	I
Request backup restoration activities	R	I
Execute backup restoration activities *Self-Service Provisioning*	I R	R C
Restore affected Stacks and VPCs *Self-Service Provisioning*	I R	R C
Restore affected custom/3rd party application	R	C
Reporting	**Customer**	**AWS Managed Services by InterVision**
Prepare and deliver monthly service report	I	C

Configure and retrieve API audit history on demand (CloudTrail) *Self-Service Provisioning*	I R	R C, I
Provide access to incident history through AWS Managed Services Interface	I	R
Provide access to change history through AWS Managed Services Interface *Self-Service Provisioning*	I N/A	R N/A
Service Request Management	**Customer**	**AWS Managed Services by InterVision**
Request information using service requests	R	C, I
Reply to service requests	I	R

* Items marked with "*" are items that InterVision Professional Services can augment client responsibility.

4 MONITORING

AMS by InterVision provides monitoring, event management, and log management. This is described in the Service Description section 1 earlier in this document.

The following services are monitored:

- ALB instance, target
- Aurora
- EC2
- EC2 - Trend Micro Endpoint Protection (security alerts)
- Elastic Cache Node
- Elastic Search cluster, domain, instance
- ELB
- GuardDuty (security alerts)
- Managed Active Directory
- NLB instance
- RDS instance
- RedShift cluster
- Amazon Macie (security alerts). Note Macie is not configured for all accounts. Must be requested.

Detailed Monitoring documentation can be provided. NDA required.

5 REPORTING

The Services provides customers with a monthly service report which summarizes key performance metrics of AWS Managed Services, including an executive summary and insights, operational metrics, managed resources,

AMS SLA adherence, and financial metrics around spend, savings and cost Reports are delivered by an InterVision Cloud Service Delivery Manager (CSDM) assigned to the customer.

Service reviews will be scheduled and conducted by the InterVision Cloud Service Delivery Manager. Reviews will be scheduled at a minimum of a quarterly basis and may occur on a more frequent basis depending upon the overall account size.

6 SERVICE ACTIVATION

6.1 ON-BOARDING

The Services delivers a dedicated AWS landing zone within prescriptive architecture and operating environment. InterVision and AWS will work together with you to build out this environment and initiate managed services for you to initiate application migration and operations. The InterVision team will guide you through onboarding process and the creation of the following accounts: master account, network account, shared service account, logging account, security account and service region(s).

Onboarding will work with to establish the following:

- IAM Roles
- IAM Access to console
- Multi-factor Authentication (MFA)
- AWS Marketplace subscription for Trend Micro Endpoint Protection
- Set up networking
- Set up firewall
- Set up access management
- Set up Active Directory federated access
- Set up VPCs for applications

InterVision is responsible for providing project management for the AMS onboarding project. AWS is responsible for AWS Managed Services Account design and build. Specific client dependencies for the onboarding project is detailed in the Roles and Responsibility table above. Detailed onboarding documentation can be provided under NDA.

6.2 OFF-BOARDING ASSISTANCE

AWS Managed Services offers off-boarding assistance within 30 days prior to termination of AWS Managed Services. The customer must request off-boarding assistance at least 7 days before such assistance can be provided. Off-boarding assistance can be offered in two forms:

1. Control hand-over: AWS Managed Services will transfer account control back to the Customer along with access credentials for all AWS Managed Services Managed Applications, or
2. Resource termination and data transfer: AWS Managed Services backs-up all the data, deletes all the data in customer's Managed Environment, de-provisions any active resources in the account, and hands over the data backup to the Customer. At customer's request AWS Managed Services can transfer customer data in the existing format using Snowball or any other media with which AWS can interface. In addition to data backups, the following customer data can be provided as part of off-boarding assistance:
    a. Data stored in storage services including logs
    b. Customer-specific Change type schemas
    c. CloudFormation templates for Change type schemas.

If off-boarding activities are not completed upon the termination of AWS Managed Services, AWS Managed Services will hand over the controls of the account(s) to enable the customer to complete any pending activity.

7 SERVICE DELIVERY

7.1 GOVERNANCE

Customers are designated a Cloud Service Delivery Manager (CSDM) who provides advisory assistance across AWS Managed Services and has a detailed understanding of the customer's Managed Environment. CSDMs work with Account Managers, AWS Managed Services Cloud Architects, AWS Solution Architects, and support teams, as applicable, to help launch new projects and give best practices recommendations throughout the software development and operations processes. The CSDM is the primary point of contact for AWS Managed Services. Key responsibilities of CSDM are:

1. Organize and lead monthly service review meetings with
2. Provide details on security, software updates for environment and opportunities for
3. Champion customer's requirements including feature requests for AWS Managed
4. Respond to and resolve billing and service reporting
5. Provide insights for financial and capacity optimization

7.2 CONTACT AND ESCALATION

The InterVision AWS Managed Services will work on all customer requests during Hours as indicated below.

Service Organization	**Request Type**	**Business Hours**	
		Plus	**Premium**
AWS	Service Request	Monday to Friday from 8am- 6pm, local customer time	24 x 7
	Incident		24 x 7
	Automated RFCs	24 x 7	24 x 7
	Non-automated RFCs	Monday to Friday from 9am- 5pm, local customer time	24 x 7
InterVision	Cloud Service Delivery Manager		Monday to Friday from 9am- 5pm, local customer time
	Cloud Architect		
	InterVision Service Desk (RFC assistance)	Monday to Friday from 9am- 5pm, local customer time	24 x 7

7.3 ESCALATION PATH

Service requests and incidents notification primarially go through the AWS Managed Service portal.

1. For urgent incidences and requests, a ticket should be opened directly with AWS Managed Service (AMS) via the AMS portal.
2. For assistance Requests For Change (RFC), InterVision will assist. InterVision support is initated by opening a ticket online at http://service.hostedcafe.com.

Customer contacts with AWS Managed Services that require escalation will follow the escalation path below.

1. Cloud Service Delivery Manager: "CSDM Name"@hostedcafe.com
2. AWS Managed Services Operations Manager: ams-opsmanager@amazon.com[5]
3. AWS Managed Services Director: ams-director@amazon.com[6]
4. AWS VP: ams-vp@amazon.com[7]

7.4 SERVICE LEVEL OBJECTIVE AND AGREEMENTS

This service utilizes both the AWS Managed Service organization as well as the InterVision Managed Services to provide services. Both AWS and InterVision services have a unique SLA that stands on it own. When InterVision is engaged to provide service that overlay the AMS, portions of the InterVision Managed Services may be additive to the AMS SLA. This section outlines where this applies.

- AWS Managed Service SLA.[8]
- InterVision Managed Service SLA is provided in the InterVision Work Order sections 9, 10, 11

With respect to incident management, InterVision will use commercially reasonable efforts to meet the following Service Level Objectives. For AWS Managed Service by InterVision, the Service Level Objectives include SLAs from InterVision and/or AWS as detailed below. AWS Managed Service SLA pertaining to AWS responsibilities are subject to modification by AWS.

7.4.1 SLA FOR MACD REQUESTS SENT TO INTERVISION

SLA Metric	MACD Standard	MACD Urgent	MACD Scheduled
Respond within:	4 hours	30 min	4 hours
Assigned within:	24 hours	4 hours	N/A
Resolved within:	48 hours	24 hours	Scheduled

Change request resolution time objective may be impacted if an AWS security reviews is required and/or receiving enough information to execute the change.

The following Service Credits will apply and will be based on a full month of service unless otherwise specified in a Service Guide.

5 mailto:ams-opsmanager@amazon.com
6 mailto:ams-director@amazon.com
7 mailto:ams-vp@amazon.com
8 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf

SLA Metric	MACD Service Credit*
Respond within:	<95% = 10% <80% = 25%

* Service credit, if a percentage, is based on the monthly fees of the applicable Service. In no event shall the Service Credit be greater than the total monthly fees for the applicable Service.

Client may also make a request for change directly to AWS. In this case the InterVision MACD SLA does not apply.

7.4.2 SLA FOR INCIDENTS REQUESTS SENT TO INTERVISION

Incident requests and client notification of incident sent to InterVision, the InterVision response time and assignment time will apply prior to the AWS Managed Services Service Level Agreement[9] will apply.

SLA Metric	Priority 1	Priority 2	Priority 3	Priority 4
InterVision Respond within:	18 minutes	30 minutes	4 hours	4 hours
InterVision Assigned within:	30 minutes	4 hours	24 hours	36 hours
AWS Plus Level response time:	4 hours	8 hours	24 hours	
AWS Plus Level resolve time:	12 hours	24 hours	48 hours	
AWS Premium Level response time:	15 minutes	4 hours	12 hours	
AWS Premium Level resolve time:	4 hours	8 hours	24 hours	

For example, if the Priority 1 incident is reported to InterVision to address, the InterVision P1 response and assignment times will apply prior to AWS initiating the P1 incident response process and the AWS response time and resolution time is initiated. A priority 1 incident with an AWS Premium service level can take up to 30-minute for InterVision to process prior to AWS initiating their 15-minute response and 4-hour resolution SLA for a total of 4-1/2 hours for resolution.

9 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf

Due to the added time to engage InterVision in P1 urgent incident responses it is recommended that the client open tickets directly with AWS managed service. InterVision will be informed and engaged as necessary.

Service Credits: InterVision response time service credits in section 11.1 will apply to InterVision conformance. AWS service credits as outline the AWS Managed Service SLA[10] will be passed through to the client.

7.4.3 SLA FOR INCIDENTS REQUESTS AND NOTIFICATIONS SENT TO AWS

For incidents requests sent directly to AWS, the AWS Managed Services Service Level Agreement[11] will apply solely.

SLA Metric	Priority 1	Priority 2	Priority 3	Priority 4
InterVision Respond within:	n/a	n/a	n/a	n/a
InterVision Assigned within:	n/a	n/a	n/a	n/a
AWS Plus Level response time:	4 hours	8 hours	24 hours	
AWS Plus Level resolve time:	12 hours	24 hours	48 hours	
AWS Premium Level response time:	15 minutes	4 hours	12 hours	
AWS Premium Level resolve time:	4 hours	8 hours	24 hours	

For example, if the Priority 1 incident is reported to AWS to address, the AWS P1 incident response process and the AWS response time and resolution time is initiated.

AWS service credits as outline the AWS Managed Service SLA[12] will be passed through to the client.

11.4 Additional SLA items.

AWS provides additional SLAs for the following:

Patch Management – Patching time for critical security patches

- Plus level is within 10 business days of release by the vendor
- Premium level is within 8 calendar days of release by the vendor

Continuity Management - Environment Recovery Initiation Time

10 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf
11 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf
12 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf

- Plus level is <=12 hours
- Premium level is <=4 hours

AMS API and Console Availability is >=99.95%

AWS service credits as outline the AWS Managed Service SLA[13] will be passed through to the client upon request.

7.4.4 CLOUD SERVICE DELIVERY MANAGER (CSDM) AND CLOUD ARCHITECT SLA

Services interactions via Cloud Service Delivery Manager (CSDM) and Cloud Architect do not have an SLA. AWS Managed Service (AMS) provided by AWS are subject to modifications by AWS. Any changes will adhere to the AWS change notification.

8 TERMS & CONDITIONS

The following AWS documents apply to this service:

AWS Managed Service Description is https://docs.aws.amazon.com/managedservices/latest/userguide/ams-sd.html

AWS Managed Service SLA link is https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf

Additional AWS terms:

Changes to the AMS Service Level Agreements. AWS may change or add to the AWS Managed Services (AMS) Service Level Agreement from time to time, but will provide at least 12 months' prior Notice to Customer before materially reducing the benefits offered to Customer under the AWS Managed Services Service Level Agreement that are available as of the Addendum Effective

Unsupported AMS Configurations. If requested by Customer through a Request for Change or Service Request, AWS may (in its sole discretion) agree to provide AWS Managed Services for Unsupported Configurations within an AWS Managed Services Account. Any AWS Managed Services provided will be treated as a 'Beta Service' subject to Section 1.10 of the AWS Service Terms available at: https://aws.amazon.com/service-[14] terms/.[15]

9 SERVICE ITEMS

InterVision AWS Managed Service - inclusive of the AMS service, InterVision CSDM, CA and Service Desk.

Complimentary Services not detailed in this Service Guide:

- InterVision AWS Migration Services
- InterVision AWS Professional Services - Cloud Architect, Security Engineer, Data Scientist, Infrastructure Engineer, Project Manager, IT Consultant
- InterVision Infrastructure Managed Services - for non-AWS managed infrstructure items such as 3rd party Firewalls, Load Balancers, Security Services, etc.
- InterVision Security Managed Services - SIEM, Vulnerability Scanning, etc.
- InterVision Resiliency Managed Services

13 https://s3.amazonaws.com/ams.contract.docs/AWS+Managed+Services+Service+Level+Agreement.pdf
14 https://aws.amazon.com/service-terms/
15 https://aws.amazon.com/service-terms/

10 DEFINITIONS

An "**Alert**" is created whenever an Event from a supported AWS service exceeds a threshold and triggers an alarm.

"**AWS Managed Services Interface**" comprises of the AWS Managed Services Console, AWS Managed Services Command Line Interface (CLI) and the AWS Managed Services APIs.

"**AWS Managed Services Managed Applications**" include all applications required to deliver a feature or capability of AWS Managed Services. AWS Managed Services Managed Applications are managed for the customer as a part of the Managed Environment. Examples include: proxy services, bastion software, managed Active Directory, and security services.

A "**Critical Security Update**" means a security update rated as "Critical" by the vendor of a Supported Operating System.

An "**Event**" indicates a change of state in your Managed Environment.

An "**Important Update**" means an update rated as "Important" or a non-security update rated as "Critical" by the vendor of a Supported Operating System.

An "**Incident**" is an unplanned interruption or performance degradation of the Managed Environment or AWS Managed Services that results in a customer impact as reported by AWS Managed Services or the customer.

"**Managed Environment**" refers to one or more AWS accounts and the resources within those accounts owned by the customer but under the management of AWS Managed Services.

"**Managed Production Environment**" refers to a customer account where the customer's production applications reside.

"**Managed Non-production Environment**" refers to a customer account that only contains non-production applications, such as for Development and Testing.

A "**Problem**" is a shared underlying root cause of one or more Incidents.

A "**Request for Change**" or "RFC" is a request created by either the customer or AWS Managed Services through the AWS Managed Services Interface to make a change in the customer's Managed Environment.

"**Change Type**" is the method used when submitting an RFC to indicate the type and nature of a change request.

A "**Stack**" is a group of one or more AWS resources that are managed as a single unit.

"**Preventative Controls**" are configurations inherent to AWS Managed Services that improve the security and operating posture of our customers' environments, such as security-hardened Amazon Machine Images (AMI), AWS Identity and Access Management (IAM) roles with permission boundaries, networking configurations, and managed security software and services.

"**Detective Controls**" are a library of AWS Managed Services created monitors which provide ongoing oversight of customer environments and workloads for configurations that do not align with security, operational, or customer controls, and take action by notifying owners, modifying, or terminating resources.

Last Updated March 17th, 2020