MANAGED CLOUD SERVICE FOR AWS - SERVICE GUIDE

Last Modification Date: 12/06/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

1 OVERVIEW

The InterVision Managed Cloud Service (MCS) for AWS is a managed service for operations of your AWS environments. InterVision provides the tools, processes and personnel for the ongoing operations management of your AWS servers, containers, serverless environments such as patch, backup, continuity management, cost management, security management and IT processes such as incident, change and service requests. Customers have access to our certified AWS engineers 24/7. This Service offers a variety of modules for managing your AWS environment. These service modules include:

- **Managed Cloud Service for AWS Servers** - supporting EC2, RDS environments
- **Managed Cloud Service for AWS Containers** - supporting ECS, EKS & Fargate
- **Managed Cloud Service for AWS Serverless Environment** - supporting Lambda, Dynamo DB
- **Managed DevOps Automation Service** - supporting CI/CD pipeline, Infrastructure as Code (IaC) and configuration management tools and processes
- **Managed Compliance for Managed Cloud Services** - supporting CIS, PCI-DSS & HIPAA standards

For each service InterVision provides the following:

- 24/7 support team
- Customer portal and ticket system
- Set up and configuration of monitoring, logging and alerts
- Response time SLAs and resolution time objectives as specified in the managed service work order
- Customized escalation procedures for service events
- Support and management of your AWS environment as specified in the service descriptions below
- Incident response for support services as specified in the service descriptions below
- Service reporting including key service performance indicators that includes operational metrics, SLA adherence, financial metrics around AWS spend

This service can be combined with additional InterVision services including Migration, Cost Optimization, Network, Security and Service Management services. See associated service guide and service description for details regarding these additional services. This Service Guide covers the Managed Cloud Service for AWS and each of the service modules.

1.1 MINIMUM SECURITY REQUIREMENTS

For the successful operations of the Managed Cloud Services for AWS the following minimum-security requirements must be enabled. If these are not currently enabled, these can be enabled during onboarding.

- **Customer Bastion Hosts –** Bastion hosts will need to be deployed for access to compute resources. Bastion hosts are special-purpose servers that are hardened and host minimal applications with all other services removed to reduce the threat. They are typically located outside the firewall or inside a DMZ to provide access to untrusted networks.
- **CloudTrail** – Enable CloudTrail in order to log all access into resources in the customer environment. CloudTrail is an AWS service that enables governance, compliance, operational auditing and risk auditing of the customer's AWS environment. It provides logging and an event history which enables resource change tracking and assists troubleshooting.
- **Logging S3 Bucket** – A dedicated S3 bucket which will retain the CloudTrail logs. Access to this S3 bucket is limited to prevent unauthorized access and to ensure that the CloudTrail logs have not been tampered with.
- **Active Directory** – For Windows Environments, customers will need to provide Active Directory or equivalent solution to manage users and groups. This can either be dedicated Active Directory servers or the AWS Directory Service, a Managed Microsoft AD service provided by AWS. This is not required if the environment only consists of Linux servers.
- **Anti-Virus Software** – For Windows server environments, customer will need to deploy Anti-virus/Anti-malware software solution. InterVision recommends TrendMicro Cloud One but the specific software

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

vendor can be substituted for any enterprise grade endpoint protection solution. This is not required if the environment only consists of Linux servers.

1.2 RECOMMENDED SECURITY FEATURES

In addition to the above security requirements, we also recommend the following security features:

- **AWS Config -** AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines.
- **Amazon Guard Duty -** Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts, workloads, and data stored in Amazon S3.
- **Onboarding Security Checks -** During the Onboarding Phase, InterVision will run a security and configuration scanner that can detect potential vulnerabilities in the AWS accounts. We will work with the Customer to remediate these during the onboarding process. Any unresolved high-risk security issues would need signoff by a member of the customer's leadership team.

1.3 ONBOARDING AND ACCESS CONTROL

InterVision will provide a project manager to assist with onboarding the customer to the Managed Cloud Service for AWS. During this process InterVision will collect customer information, escalation data, runbook information, service set-up policy information and other critical data for the successful set up on managed services. During the workload onboarding process the following will be performed unless otherwise noted:

- Enabling Okta for Access Control and Multi-Factor Authentication to the AWS Console
- Addition of Bastion servers (if not already present)
- Implement account-wide environment controls for access control, security, and infrastructure best practices
- Configure monitoring and log collection
- Security assessment of each AWS account and remediation recommendations.
- Additional service specific onboarding activities are detailed under the description for each service

InterVision will perform a standard set of tasks as part of onboarding customer environments to Managed Cloud Services. If nonstandard or customer-requested tasks fall outside of the scope of the typical onboarding tasks, InterVision may require an additional Statement of Work to facilitate the completion of those tasks.

Service onboarding is not inclusive of workload migration or workload implementations; these are separate services. MCS is designed to be initiated once workloads have been initially built or migrated to AWS.

1.4 MANAGED CLOUD FOUNDATIONAL SERVICE

For each managed cloud environment, InterVision offers Managed Cloud Foundational Services that compliments and is tailored to the specific managed cloud service you are consuming. This service includes the following:

- Designated team of a Client Service Delivery Manager and Cloud Engineer which complements our 24/7 service desk of Level 2 and Level 3 cloud engineers
- Provides architectural and operational guidance
- Provides escalation management
- Coordinate FinOps and cost management reviews
- Liaison with InterVision technical teams and customer on high risk changes/projects

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

- Creation and maintenance of customer runbooks
- SLA reporting
- Facilitates game days sessions that include:
    - Accessing EC2 to view Instances
    - Launching an Instance
    - Connecting to Windows Instance
    - Connecting through Bastion Host
    - Defining Security Groups and Access settings
    - Connecting to Linux Instance
    - Monitoring walkthrough
    - Patching & backup walkthroughs
    - Vulnerability & compliance reporting walkthrough (Compliance service required for compliance)
- Facilitate business, service & technical reviews

2 MANAGED CLOUD SERVICE FOR AWS SERVERS

2.1 SERVICE DESCRIPTION AND DETAILS - MANAGED CLOUD SERVICE FOR AWS SERVERS

InterVision will provide the following Managed AWS server environment Services and Deliverable(s) as a part of our engagement, including but not limited to:

Event and Incident Management

- Supported AWS services: VPC, EC2, RDS, EBS, EFS, S3, CloudWatch, Backup Manager & CloudFront.
- VPN Tunnel Support - This service will monitor, alert, and provide response services for the VPN tunnel between Amazon Web Services (AWS)
- Provide 24/7 monitoring and management of the AWS infrastructure via CloudWatch.
- Set up and receive inbound platform alerts and respond to service reliability events, 24/7/365.
- Troubleshoot and assist with infrastructure issues.
- SLA based response to requests and incidences.
- Operate via Playbooks and Runbooks in providing 24/7 services.
- Respond to support requests from Client round the clock with no limitation on the number of tickets per month.
- Provide ad-hoc support to Client team members and stakeholders.
- Cloud Formation and/or Terraform support

Change Management

- Provide real-time guidance using Service Portal / ticketing system.

Configuration Management

- Configure Service Control Policies to protect from misconfigurations
- Configure AWS Config Rules as requested

Security Management

- Configure Anti-Malware protection
- Configure Access Control Lists and Security Groups (for newly created environments.)
- Audit and remediate Access Control Lists (for existing environments)
- Customer will manage their users via an approved directory service provided by customer.
- Set up AWS GuardDuty as requested – Response to GuardDuty alerts is CUSTOMER responsibility.

Patch Management

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

- Quarterly patching of all servers and guest OS services
- Coordinate with customer for service-specific patching within scheduled maintenance windows
- Perform patching to address service-impacting bugs (based on patch availability)

Continuity Management (Backup & Restore)

- Configuration of backup policies using AWS Backup service to meet business recovery objectives.
- 24/7 availability to restore data as requested to restore services
- Restore actions from specific snapshots can be performed by customer request
- Point-in-time RDS restore requests

Cost Optimization

- Right-size the infrastructure and reservation management as needed
- Audit S3 bucket usage and implement intelligent tiering or lifecycle management policies as appropriate
- Implement S3 lifecycle policies and recommend storage tiers for S3-based savings
- Recommend reservations and Savings Plans
- Implement cross-account VPC peering as appropriate to limit cross-account network traffic to the private networks (for customers not using Transit Gateway)
- Implement VPC peering between AWS account to minimize traffic leaving the AWS network
- Recommend new, cost saving solutions as appropriate to replace dated and expensive technologies
- Advise business stakeholders with cost control, budgeting and forecasting recommendations

2.2 ROLES AND RESPONSIBILITIES - MANAGED CLOUD SERVICE FOR AWS SERVERS

The Service 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.

* Items marked with "*" are items that InterVision Professional Services can augment client responsibility and may be specified in the Professional services Statement of work.

Onboarding	Customer	InterVision
AWS Account Information	R*	I
Customer Escalation Information	R*	I
Identify user roles (Admin., Change Approver,....)	R*	I
Anti-virus software subscription	R	C, I

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

VPN Tunnel turn-up (Customer firewall)	R*	I
VPN Tunnel turn-up (AWS Side)	I	R
Selecting customer maintenance window	R	C, I
Event and Incident Management	**Customer**	**InterVision**
Configuring AWS alarms for Managed Environment	I	R
Define customer-specific monitoring and incident requirements	R	C
Receive AWS infrastructure monitoring	I	R
Investigating EC2 and RDS alerts for Incident notification	I	R
Proactively notify Incidents on AWS infrastructure	I	R
Categorize Incident priority	I	R
Provide Incident response	I	R
Provide Incident resolution / infrastructure restore	C	R
Installation and configuration of agents and scripts for patching, security, monitoring, etc.	I	R
Ensuring that AWS infrastructure change logs are recorded in CloudTrail	I	R
Recording all application change logs	R	C
Handle application performance issues and outages	R*	I
Identify Problems in Managed Environment	C	R
Perform RCA for Problems in Managed Environment	C	R
Remediation of Problems in Managed Environment	C	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Identify and remediate application problems	R*	I
Monitor master/slave/RO replication health	I	R
Identify RCA of master failover	I	R
RDS health status monitoring (CloudWatch)	I	R
RDS connections monitoring (CloudWatch)	R	I
Additional RDS performance monitoring	R*	I
RDS event subscription configuration (SNS)	C	R
Change Management	**Customer**	**InterVision**
Make change requests to InterVision	R	C, I
Maintenance of application change calendar	R	I
Notice of upcoming Maintenance Window	I	R
Configure Cloud Front as requested	C	R
Configuration Management	**Customer**	**InterVision**
Configure Service Control Policies as requested	C	R
Configure AWS Config Rules as requested	C	R
Customer Cloud Formation / Terraform Support	C	R
Security Management	**Customer**	**InterVision**
Customer infrastructure security and/or establishing baseline for security compliance process as determined and agreed to during customer onboarding.	C	R
Maintaining valid licenses for Managed Security Software (Trend Micro is recommended)	R	I

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Monitoring malware on managed instances (if Trend Micro is deployed)	R	I
Maintaining and updating virus signatures	R	I
Manage the lifecycle of users, and their permissions for local directory services	R	I
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 InterVision engineers	I	R
Patch Management	**Customer**	**InterVision**
Monitor for applicable updates to supported OS and software preinstalled with supported OS for EC2 instances	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	R	I
Define custom Patch baselines to filter and exclude specific patches	R	I
Tag instances to associate them with custom maintenance windows and Patch Baselines	R*	C, I
Track the patch status of resources and highlight systems that aren't current in the business review.	C	R
Apply updates to EC2 instances per Customer instructions	I	R
Patch development software (.NET, PHP, Perl, Python)	I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Patch, and monitor middleware applications (e.g. BizTalk, JBoss, WebSphere)	I	R
Patch and monitor custom and 3rd party applications	R*	C
Coordinate and schedule DB engine patch management	C	R
Continuity Management	**Customer**	**InterVision**
Specify backup schedules	R	I
Execute backups per schedule	I	R
Validate backups	R	I
Request backup restoration activities	R	I
Execute backup restoration activities	I	R
Restore affected custom/3rd party application	R	C
Automated snapshot (backup) configuration	C	R
Cost Optimization	**Customer**	**InterVision**
Recommend RI optimization	C	R
Purchase RI and PIOP capacity (Customer has financial responsibility)	C	R
Remove capacity when capacity is over provisioned	C	R
S3 configuration	C	R
Glacier configuration	C	R
Define archival policy	R	C
Archival policy configuration	C	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Recommend DB storage and PIOP capacity	C	R
Recommend instance sizing for running databases	C	R
Reporting	**Customer**	**InterVision**
Configure and retrieve audit history on demand (CloudTrail)	I	R
Provide access to incident history	I	R
Provide access to change history	I	R
Application Lifecycle	**Customer**	**InterVision**
Application development	R	I
Application infrastructure requirements analysis and design	R*	C, I
Application deployment	R*	C, I
Application monitoring	R	I
Application testing/optimization	R	I
Troubleshoot and resolve application issues	R	I
Troubleshoot and resolve operating system and infrastructure issues	C	R
RDS security group configuration	C	R
RDS engine parameter/option configuration	R	C, I
DB table design	R*	I
DB indexing	R*	I
DB log analysis	R*	I

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Datadog/New Relic application performance monitoring	R	I

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

2.3 ONBOARDING AND PROVISIONING - MANAGED CLOUD SERVICE FOR AWS SERVERS

In addition to the general onboarding actions (see Onboarding & Access Control) the following will be performed as needed by InterVision:

- VPN tunnel turn-up
- Add to Monitoring and Log Collection
- Add to Backup
- Add to Patching
- Security assessment of each AWS account and remediation recommendations.
- Activate minimum security requirements (see Minimum Security Requirements)

3 MANAGED CLOUD SERVICE FOR AWS CONTAINERS

3.1 SERVICE DESCRIPTION AND DETAILS - MANAGED CLOUD SERVICE FOR AWS CONTAINERS

InterVision will provide 24/7 monitoring, incident response, support and management for AWS containers environments as a part of our engagement.

Supported for the following AWS services:

- Elastic Container Service (ECS)
- Elastic Kubernetes Service (EKS)
- Fargate

Managed Service include:

- Provide 24/7 monitoring and management of the AWS infrastructure.
- Monitoring and responding to incidences for Kubernetes Cluster using CloudWatch & Prometheus/Grafana
- Monitor AWS service quotas for Fargate on-demand resource usage
- Monitor POD health metrics after deployments and detailed metrics/monitoring –
- Enable Prometheus / Grafana to monitor health as necessary.
  Container Insights is not currently supported for EKS Fargate.
- Monitor application/API endpoints and publicly exposed services
- Provide Incident response / troubleshooting of notified issues
- Provide EKS cluster upgrade and maintenance that includes:
- Kubernetes version upgrades
- Upgrades to EKS supporting services: CoreDNS, VPC CNI Plugins, KubeProxy, Metrics Server, Ingress Controllers
- Perform Kubernetes security benchmarks using Kube-bench that includes:
- Check the worker nodes configurations for risks in these environments
- Scan Image / Programming Language for Vulnerabilities and provide support

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

- Provide Kubernetes applications package management tool Helm
- Provide Kubernetes deployment troubleshooting assistance

3.2 ROLES AND RESPONSIBILITIES - MANAGED CLOUD SERVICE FOR AWS CONTAINERS

The Service 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.

* Items marked with "*" are items that InterVision Professional Services can augment client responsibility and may be specified in the Professional services Statement of work.

ONBOARDING	**Customer**	**InterVision**
Perform manual review of existing environment, remediating any issues as necessary	C, I	R
Perform manual review of CI/CD pipelines	C, I	R
Perform manual review of logging, alerting and monitoring integrations	C, I	R
Perform manual review of deployment manifests	C, I	R
Perform manual review of SCM Repositories	C, I	R
INCIDENT AND EVENT MANAGEMENT	**Customer**	**InterVision**
Monitor and respond to incidences for Kubernetes Cluster using CloudWatch and Prometheus/Grafana	C, I	R
Monitor AWS service quotas for Fargate on-demand resource usage	C, I	R
Monitor POD health metrics after deployments	C, I	R
Enable Promethius/Grafana to monitor health as necessary	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Monitor application/API endpoints and publicly exposed services	C, I	R
Provide incident response/troubleshooting of notified issues	C, I	R
Approve remediation recommendations for the infrastructure	R	I
Implemented remediated recommendations post approval	C,I	R
APPLICATION PACKAGE MANAGEMENT	**Customer**	**InterVision**
Provide Kubernetes applications package management tool Helm	C, I	R
Assist in containerizing the application and tweaking container images	C, I	R
Perform Containerization of the Application	R,C	I
Set up Container Image Repositories	C, I	R
Set up Continuous Integration tools	C, I	R
Set up additional integrations (Code Quality, Vulnerability management, Container Image Scanning)	C, I	R
Set up monitoring and alerting for Continuous Deployment Pipelines	C, I	R
DEPLOYMENT ASSISTANCE	**Customer**	**InterVision**
Provide Kubernetes deployment troubleshooting assistance	C, I	R
Setup IaC Scripts for Infrastructure provisioning	C, I	R
Setup Cloud Network Infrastructure / IAM Resources	C, I	R
Setup EKS Cluster	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Initial Security benchmarking for EKS Cluster	C, I	R
Create Application deployment manifests (Kubernetes yaml/helm/kustomize)	C, I	R
Set up Continuous Deployment or GitOps Pipelines	C, I	R
Set up monitoring and alerting for Continuous Deployment Pipelines	C, I	R
Setup Infrastructure monitoring for EKS Cluster	C, I	R
Setup Backups for EKS Configurations (Velero)	C, I	R
Setup Log Aggregation for EKS Cluster (Datadog, Cloudwatch, Elasticsearch, Loki)	C, I	R
Setup monitoring for EKS cluster (Datadog, Cloudwatch, Prometheus)	C, I	R
Setup Kubernetes access for Development Team members	C, I	R
Guidance on Resource Optimization and cost optimization (Containers, Worker Nodes)	C, I	R
CHANGE MANAGEMENT	**Customer**	**InterVision**
Perform EKS cluster upgrade and maintenance activities	C, I	R
Perform EKS WorkerNode Upgrade	C, I	R
Perform Kubernetes version upgrade	C, I	R
Perform upgrade for Kubernetes Add-Ons/Plugins	C,I	R
Perform upgrade/tweakings for CI/CD Tools	C,I	R
Perform revisions and upgrades for supporting services tools (Ingress controller, Metrics Server, Cluster AutoScaler)	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

SECURITY MANAGEMENT	Customer	InterVision
Perform CIS Benchmarking for AWS Infrastructure	C, I	R
Perform CIS Benchmarking for EKS Cluster	C, I	R
Check worker node configurations for risks	C, I	R
Review Image Scanning / Code Scanning reports for vulnerabilities	C, I	R
REPORTING	**Customer**	**InterVision**
Configure and retrieve audit history on demand (CloudTrail)	I	R
Provide access to incident history	I	R
Provide access to change history	I	R

3.3 ONBOARDING AND PROVISIONING - MANAGED CLOUD SERVICE FOR AWS CONTAINERS

In addition to general onboarding tasks, an assigned onboarding project manager will provide a list of customer dependencies and InterVision set up tasks during a kick off meeting.

4 MANAGED CLOUD SERVICE FOR AWS SERVERLESS ENVIRONMENTS

4.1 SERVICE DESCRIPTION AND DETAILS - MANAGED CLOUD SERVICE FOR AWS SERVERLESS ENVIRONMENTS

InterVision will provide the following Managed Cloud Service for AWS Serverless Environment services as a part of our engagement:

Support (deployment incident response, incident remediation and change management) for the following AWS services:

- AWS Lambda
- DynamoDB
- API Gateway
- Step Functions

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Monitoring, incident response and support for the following:

AWS Lambda

- Invocations
- Duration
- Error count
- Throttles
- Async delivery failures
- Latency metrics
- Dead Letter Errors

DynamoDB

- CPU utilization
- Item cache hits
- Item cache misses
- Failed requests
- Client connections
- Provisioned Read Capacity
- Provisioned Write Capacity
- Consumed Read Capacity
- Consumed Write Capacity
- Read Threshold/Sec
- Write Threshold/Sec

API Gateway

- 4xx Error
- 5xx Error
- Integration Latency metrics
- Latency metrics
- Cache Hit Count
- Cache Miss Count metrics

Step Functions

- Metrics That Report a Time Interval
- Metrics That Report a Count
- Execution Metrics
- Activity Metrics
- Lambda Function Metrics
- Service Integration Metrics
- Service Metrics
- API Metrics

4.2 ROLES AND RESPONSIBILITIES - MANAGED CLOUD SERVICE FOR AWS SERVERLESS ENVIRONMENTS

The Service 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.

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

- “I” stands for informed; a party which is informed on progress, often only on completion of the task or deliverable.

* Items marked with "*" are items that InterVision Professional Services can augment client responsibility and may be specified in the Professional services Statement of work.

ONBOARDING	Customer	InterVision
Application detailing and overview, along with dependencies	R	I
Perform manual review of existing environment, remediating any issues as necessary	C, I	R
Review and evaluate existing CI/CD build and deployment (for takeovers)	C, I	R
CI/CD build and design for the deployed code	C,I	R
Evaluate the metrics and latencies if any if monitoring is enabled (for takeovers)	C, I	R
Provide guidance on resource allocation and stack along with best practices	C,I	R
Install Serverless Framework Plugins for external tool integrations	R	C,I
Ensure security best practices are implemented	C,I	R
CODE CREATION	**Customer**	**InterVision**
Write AWS Lambda functions	R	I
Test and review Lambda functions	R	I
INCIDENT AND EVENT MANAGEMENT	**Customer**	**InterVision**
Performance monitoring and ongoing support for AWS Lambda, DynamoDB, API Gateway and Step Functions	C,I	R
Use telemetry tools for monitoring and incident management (Latency monitoring, cold starts, invocation errors)	C,I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Set up CloudWatch alerts and alarms (for new environments)	C,I	R
Integration of APM tools with Serverless application for better monitoring and incident management (eg: Datadog)	C,I	R
Scope and Ownership of APM tools	R	C
Configure required CloudWatch alerts and CloudTrails (for existing environments)	C,I	R
Provide incident response/troubleshooting of notified issues	C, I	R
Approve remediation recommendations and code based implementations	R	I
OPTIMIZATION	**Customer**	**InterVision**
Analyze and improve startup time with necessary remediations	I	R
Evaluate application to optimize access patterns and apply caching as needed	I	R
Evaluate and implement optimum capacity units	C,I	R
Code level optimization and remediations	R,C	I
Review and optimize batch size, batch window and payload size for high throughput	I	R
SECURITY	**Customer**	**InterVision**
Review and enable minimal resource policies for Deployment Access Control	C,I	R
Recommend minimal access policies for serverless application	I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Persisting Secrets - lifecycle of secrets management in application	C,I	R
Configure AWS Systems Manager Parameter Store	C,I	R
Review and assist with API Authorization	C,I	R
REPORTING	**Customer**	**InterVision**
Configure and retrieve audit history on demand (CloudTrail)	I	R
Provide access to incident history	I	R
Provide access to change history	I	R

4.3 ONBOARDING AND PROVISIONING - MANAGED CLOUD SERVICE FOR AWS SERVERLESS ENVIRONMENT

In addition to general onboarding tasks, an assigned onboarding project manager will provide a list of customer dependencies and InterVision set up tasks during a kick off meeting.

5 MANAGED DEVOPS AUTOMATION SERVICE

5.1 SERVICE DESCRIPTION AND DETAILS - MANAGED DEVOPS AUTOMATION SERVICE

InterVision will：

- Supported CI/CD tools/services: AWS Developer Tools (AWS CodeBuild, AWS CodePipeline, CodeDeploy), Azure DevOps, Jenkins, Bitbucket Pipeline, GitHub Actions, Gitlab, CircleCI and other tools as approved by InterVision
- Supported Infrastructure as Code (IaC) tools: Terraform, AWS Cloud Formation
- Supported configuration management tools: Ansible, Puppet, Chef
- Build and configure CI/CD deployment pipelines for the infrastructure
- Implement pipelines using Infrastructure as Code (IaC)
- Provide management of the pipeline
- Monitoring and responding to incidents from CI/CD tools
- Provide incident response / troubleshooting of notified issues
- Provide deployment-based troubleshooting assistance

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

5.2 ROLES AND RESPONSIBILITIES - MANAGED CLOUD SERVICE FOR AWS DEVOPS AUTOMATION SERVICE

The Service 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.

* Items marked with "*" are items that InterVision Professional Services can augment client responsibility and may be specified in the Professional services Statement of work.

GENERAL	**Customer**	**InterVision**
Resource Stack Recommendation and Selection	R	C
Build and Configure Infrastructure	C, I	R
Develop and Maintain Pipeline Configurations	C, I	R
CODE CREATION	**Customer**	**InterVision**
Application Code Creation	R	I
Source Code Management	R	I
BUILD AND PACKAGE	**Customer**	**InterVision**
Implement CI/CD Pipelines using tools like Jenkins and AWS CodeBuild	C, I	R
Integration Testing	R	I
Integrate Source Code Repository with Build Tool	C, I	R
Package management - Configure the CI/CD pipeline to pull build files (pre-built package containers/docker images)	C, I	R
Use CodeDeploy to deliver packages	C, I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Automated deployment of code to non-production customer environments using Jenkins, AWS CodeDeploy, etc.	C, I	R
Deployment into Production environment	R	C, I
TESTING	**Customer**	**InterVision**
Test application code	R	
DEPLOYMENT	**Customer**	**InterVision**
Perform test deployments in the infrastructure	C,I	R
Making sure the deployment process works	C,I	R
Monitor deployments for success/failure	C,I	R
Troubleshoot failed deployments to production	C,I	R
INFRASTRUCTURE AS CODE (IaC)	**Customer**	**InterVision**
Provision AWS Resources using CloudFormation or Terraform	C,I	R
Managing Servers using Ansible Package Installations or Webserver Setup	C,I	R
Request/Approve package installations	R	C,I
Requests for user creation or IP additions	R	C,I
Create users or add new IP address to security group as per request	C,I	R
Requests and Approvals for change request or change management process	R	C,I
Impact review and solution recommendation for major change requests	C,I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Maintenance Review recommendation and scheduling	C,I	R
Version control for configuration files	C,I	R
Test and monitor configurations	C,I	R
Managing manifests of Kubernetes deployments	C,I	R
RELEASE MANAGEMENT	**Customer**	**InterVision**
Configure the Release Management process per client	C,I	R
Define Release Management Stages based on different environments	C,I	R
Own Release Management to Production Environment	R	C,I
DATABASE UPDATES	**Customer**	**InterVision**
Update the required database schema with the new code that requires it	R	I
OPERATIONS	**Customer**	**InterVision**
Configure Logging & Backups of the Infrastructure	I	R
Implement Monitoring tools for the AWS Infrastructure	I	R
Created Build Documentation and Architectural Diagrams	I	R
Analyze Application Performance	R	C
Review CloudWatch metrics - connection counts to load balancers, bottlenecks, connection buildup to DB servers - can involve an APM if the client has one	I	R
MANAGED SERVER SERVICE*	**Customer**	**InterVision**
Implement workflow for internal and external incident response teams	C,I	R

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

Patching of the infrastructure and guest OS services	C,I	R
Recommend and provision maintenance windows	C,I	R
Service-specific patching within scheduled maintenance windows	C,I	R
On-demand patching to address service-impacting bugs	C,I	R
Right-size the infrastructure and reservation management	C,I	R
Configure Backup policies using the AWS Backup service	I	R
Data restoration requests	R	I
Restore data as required	I	R

*The Managed Server Service list of tasks applies if the customer is using GitLab or Jenkins installed on an EC2 instances. These would then be managed by InterVision as part of the CI/CD pipeline.

5.3 ONBOARDING AND PROVISIONING - MANAGED CLOUD SERVICE FOR DEVOPS AUTOMATION SERVICE

In addition to general onboarding tasks, an assigned onboarding project manager will provide a list of customer dependencies and InterVision set up tasks during a kickoff meeting.

6 MANAGED COMPLIANCE FOR MANAGED CLOUD SERVICES

6.1 SERVICE DESCRIPTION AND DETAILS - MANAGED COMPLIANCE FOR MANAGED CLOUD SERVICES

This service can be added to the Managed Cloud Service for AWS EC2/RDS, Containers or Serverless.

The scope of services includes compliance scanning, benchmarking and support of the following:

- Supported compliance standards include CIS, PCI-DSS, and HIPAA
- Configure AWS config rules against standards and set-up alerting
- Run compliance scans and run reports quarterly, bi-annually, or annually per client requirements
- Validate configurations against compliance standards using automated tools
- Remediate out-of-compliance conditions and configuration errors
- Initiate security audit of the infrastructure using security compliance tools
- Provide a summarized report of findings of issues observed during the security assessment

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute

- Provide remediation plans to bring the environments up to compliance requirements
- Restructure or refactor the environment to fix the issues highlighted in the security assessment as described in the remediation summary
- Ensure benchmarking levels are met and the environment is compliant with required security standards on a scheduled basis

The roles and responsibility for this service are as follows: InterVision is responsible for the above tasks. InterVision will consult with customer on any item that will require changes, that may impact availability or performance of a service, and items that require customer input to configure. Items that are not listed above are customer's responsibility.

Copyright © 2020 InterVision Systems, LLC. All rights reserved | Confidential - Do Not Distribute