MANAGED CLOUD SERVICE FOR AZURE - SERVICE GUIDE

Last Modification Date: 11/28/2022
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1 MANAGED CLOUD SERVICE FOR AZURE - SERVICE GUIDE

1.1 OVERVIEW

The InterVision Managed Cloud Service (MCS) for Azure is a managed service for operations of your Microsoft Azure environments. InterVision provides the tools, processes and personnel for the ongoing operations management of your Azure servers, 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 Azure engineers 24/7.

As part of the 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 Azure environment as specified in the service description 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 Azure 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 Azure and each of the service modules.

1.2 ASSUMPTIONS

The managed service is designed for Day 2 operations of existing Azure environments. The initial build of the environment is completed. Minor changes to existing environments is included as part of the service as outlined below. Significant architectural changes or migration activities would require an additional Statement of Work.

1.3 MINIMUM SECURITY REQUIREMENTS

For the successful operations of the Managed Cloud Services for Azure 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.
- **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 Azure AD. 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 vendor can be substituted for any enterprise grade endpoint protection solution. This is not required if the environment only consists of Linux servers.

1.4 RECOMMENDED SECURITY FEATURES

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

- **Onboarding Security Checks -** During the Onboarding Phase, InterVision will run a security and configuration scanner that can detect potential vulnerabilities in the Azure environments. We will work with the Customer to remediate these during the onboarding process.
- **Ongoing Security Posture Management** – Customers may elect to adopt InterVision's Security Posture Management Service which will provide ongoing monitoring of best practices and compliance framework adherence.

2 MANAGED CLOUD SERVICES FOR AZURE DETAILS

Service Description and Details - Managed Cloud Service for Azure

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

2.1 CLOUD PLATFORM MANAGEMENT AND SUPPORT

InterVision will provide management and support activities related to the Azure cloud platform, including support for tenants, subscriptions, virtual networks, subnets, route tables, Azure load balancers, Azure firewall, network security groups, access control lists, Azure Traffic Manager and VPNs/VPN Gateway. Management and Support of the following services is included:

Cloud Platform Management and Support	InterVision	Customer
Tenant Creation, Onboarding, Management	R/A	C/I
Subscription Management	R/A	C/I
Azure Virtual Network Management	R/A	C/I
Subnet Management	R/A	C/I
Route Table Management	R/A	C/I
Azure Load Balancing Management	R/A	C/I
Azure Firewall Management	R/A	C/I
Azure Network Security Groups Management	R/A	C/I

Azure Network Access Control Lists Management	R/A	C/I
Azure Traffic Manager Management (DNS level traffic routing, load balancing, failover)	R/A	C/I
VPN/Private Connection/VPN Gateway Management	R/A	C/I
Access Control (IAM) - Create Users and Groups	R*	R*
Access Control (IAM) - Add/Remove Users/Groups from Resource Groups	R*	R*
Access Control (IAM) - Assign Roles to Users/Groups	R*	R*
Synchronize on-prem deployment of AD with Azure AD using Azure AD Connect	C/I	R/A
Modify AD Group Membership	C/I	R/A

*Both InterVision and Customer may modify Access Control (IAM) users and groups. Customer may request changes or perform those changes directly via the Azure console.

2.2 VIRTUAL MACHINE AND OPERATING SYSTEM SUPPORT

InterVision will provide management and support activities related to virtual machines and operating systems. Management and Support of the following services is included:

Virtual Machine and Operating System Support	InterVision	Customer
Virtual Machine Creation	R*	R*
Compute Instance Resizing/Family Changes	R/A	C/I
Reserved Instance Creation	R/A	C/I
Windows VM Monitoring	R/A	C/I
Windows VM Management	R/A	C/I
Windows OS Patching	R/A	C/I

Configure Anti-Malware Protection	R/A	C/I
Azure Backup Management	R/A	C/I
Virus removal and threat remediation	C/I	R/A
Database administration	C/I	R/A

*Both InterVision and Customer may create/deploy new virtual machines. Customer may request that InterVision create virtual machines via service request or Customer may create virtual machines directly via Azure console.

2.3 AZURE VIRTUAL DESKTOP SUPPORT

Azure Virtual Desktop Support	InterVision	Customer
Monitor/Receive Alerts	R/A	C/I
Monitor/Manage Storage	R/A	C/I
Disk Space Cleanup	R/A	C/I
Add/Remove Session Hosts from Host Pool	R/A	C/I
Clear out Hung Sessions	R/A	C/I
Backup Images and Session Hosts	R/A	C/I
Backup FSLogix User Profiles (hosted in Azure)	R/A	C/I
Backup FSLogix User Profiles (hosted On-Prem)	C/I	R/A
Image Management	C/I*	R/A*
Profile Management (using FSLogix)	C/I*	R/A*
Group Policy Administration	C/I*	R/A*
Update/Deploy New Desktop Applications	C/I*	R/A*

Create New Host Pools	C/I*	R/A*
End User Support	#	R/A

* These activities could be provided through InterVision Professional Services

End User Support is the customer responsibility unless managed Help Desk Service is also purchased.

2.4 OPERATIONAL PROCESSES

Support includes 24x7 monitoring, event and incident management, service, problem and change management, and also includes installation, move, add, change and delete requests.

The assumption here is that the customer's Azure environment is already built, and support activities exclude migration activities.

Operational Processes	InterVision	Customer
Incident, Service, Problem and Change Management	R/A	C/I
Installation, Move, Add, Change and Delete Requests	R/A	C/I

2.5 MANAGED CLOUD FOUNDATION SERVICES

As part of the managed service, InterVision will provide a designated team of a Cloud Service Delivery Manager and Cloud Engineer which complements our 24/7 service desk of level 2 and level 3 cloud engineers.

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
- Creation and maintenance of customer runbooks
- SLA reporting
- Facilitates game days sessions that include:
- Launching a virtual machine
- Connecting to Windows virtual machine
- Connecting through Bastion Host

- Defining Security Groups and Access settings
- Connecting to Linux Instance
- Monitoring walkthrough
- Patching & backup walkthroughs
- Facilitate business, service & technical reviews

Managed Cloud Foundation Services	InterVision	Customer
Provide architectural and operational guidance	R/A	C/I
Escalation management	R/A	C/I
Coordinate FinOps and cost management reviews	R/A	C/I
Liaison with InterVision technical teams and customer on high-risk changes/projects	R/A	C/I
Creation and maintenance of customer runbooks	R/A	C/I
SLA Reporting	R/A	C/I
Facilitate business, service & technical reviews	R/A	C/I

2.6 ENVIRONMENT MONITORING

InterVision will provide 24x7 monitoring of the following services related to the Customer Azure environment:

Environment Monitoring	InterVision	Customer
OS Level Monitoring	R	C
Virtual Machine Instance CPU/Memory/Disk Monitoring	R	C
Load Balancer Monitoring	R	C

Cache Service Monitoring	R	C
Serverless Code Execution Monitoring	R	C
DNS Monitoring	R	C
Content Delivery Network Monitoring	R	C
Notification System Monitoring	R	C
Queueing System Monitoring	R	C
URL Monitoring (up/down)	R	C
Alert Escalation	R	C
Website Monitoring: Availability	R	C
Database Monitoring (Performance/ system health / DB health / sizing / replication)	R	C
Data Warehouse Monitoring	R	C

2.7 AZURE VIRTUAL DESKTOP MONITORING

Azure Virtual Desktop Monitoring	InterVision	Customer
Connection Diagnostics	R/A	C/I
Connection Performance	R/A	C/I
Host Diagnostics	R/A	C/I
Host Performance	R/A	C/I
User Report	R/A	C/I
Utiliztion Report	R/A	C/I

Client Report	R/A	C/I

2.8 ONBOARDING

InterVision will provide a project manager to assist with onboarding the customer to the Managed Cloud Service for Azure. 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:

- Configure Okta Single Sign On (SSO) access for InterVision and Customer access
- 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 Azure account and remediation recommendations.
- Additional service specific onboarding activities are detailed below
- VPN tunnel turn-up
- Add to Monitoring and Log Collection
- Add to Backup
- Add to Patching

Typical onboarding tasks include:

Onboarding	InterVision	Customer
Create Role and Identity Provider in Azure Console to enable IV SSO Access	C/I	R
Azure Tenant Creation	I	R*
Customer Escalation Information	I	R*
Anti-Virus subscription (if not already present. Trend Micro recommended)	C, I	R
VPN Tunnel turn-up (Customer firewall)	I	R*
VPN Tunnel turn-up (Azure Side)	R	I
Synchronize on-prem AD with Azure AD by using Azure AD Connect	I	R*

*Asterisk means these tasks can also be performed by InterVision Professional Services.

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 Azure.

2.9 RECURRING ACCOUNT REVIEW

During regularly scheduled account reviews throughout the Order Term, the InterVision CSDM will address the operational activities to be performed by InterVision, as for instance the following, as needed:

- Strategic: Service trend reports, business planning initiatives, customer satisfaction, annual plans and evaluation, and focused recommendations in the space of the Services
- Tactical: InterVision support processes associated with the Services, disruptive incidents, planned and completed changes and key known issues/problems, operational improvement, approaching events, and any other input for the day-to-day tactical engagement with the Services

2.10 SUBSCRIPTION RENEWAL

The InterVision CSDM will work with InterVision Client Success Manager (CSM) to track, notify and facilitate software and services renewals.