ACTIVE DIRECTORY MANAGED SERVICE - SERVICE GUIDE

Last Modification Date: 09/29/2020
Exported and Shared on: 01/30/2023

For additional information, visit www.intervision.com

CONTENTS

1 Overview 1
2 Service Specification - Active Directory Service 1
3 Roles and Responsibilities Matrix 1
4 Monitoring 4
5 Reporting 6
6 Managed Infrastructure Services 6
6.1 Service Level Offers - Managed Infrastructure 7
6.2 Service Levels 8
6.3 Reporting 6
6.4 Service Activation 9
6.5 Steps to activate service 9
6.6 Service Delivery 9
6.7 Incident and Device Impact Classification 9
7 Definitions 10

1 OVERVIEW

The managed Microsoft Active service covers the application troubleshooting and availability monitoring of the associated Microsoft Active Directory infrastructure. This service covers the Microsoft Active Directory Application for all software versions currently under vendor support. This managed service is provided based upon one instance of the Active Directory application and for the domain controller (physical or virtual) delivering the application and its components.

2 SERVICE SPECIFICATION - ACTIVE DIRECTORY SERVICE

This service is designed to pick up day-to-day monitoring and management of the Microsoft Active Directory environment, after it has been designed, implemented and is running in production. Design and implementation services may be obtained via Professional services.

The service for the Active Directory Application support includes monitoring and support on the first two domain controllers. Additional domain controllers will need additional managed server support.

The service covers ongoing troubleshooting of Microsoft Active Directory environment including

- Replication Issues
- Authorization Issues
- Services (DNS, FRS etc…)
- Support Desk with 24/7/365 coverage

Mass (greater than 5) additions/deletions or changes are not covered as part of the managed service and will be considered project billable tasks.

This service by itself does not include support of critical dependencies such as networking, operating system, supporting applications, or device hardware. Support for critical dependencies must be purchased separately for certain features to be supported. Software licenses or maintenance are not included as part of this service. Certain features may require managed support on additional applications or hardware.

3 ROLES AND RESPONSIBILITIES MATRIX

General	**Client**	**Hosted Cafe'**	**Extended Services***
Microsoft Active Directory permissions, accounts	X		
Client escalation information	X		
Vendor support contracts	X		
Installation and Configuration	**Client**	**Hosted Cafe'**	**Extended Services***
Design of Microsoft Active Directory environment	X		ProServices
Physical or guest machine install	X		ProServices

Installation or configuration of Windows OS, Active Directory, Networking, or Clustering	X		ProServices
Installation, Integration or configuration of additional applications	X		ProServices
Monitoring	**Client**	**Hosted Cafe'**	**Extended Services***
Setup monitoring and logging		X	
Update monitoring thresholds per client requirements		X	
Manage notification profiles		X	
Active Directory application internal database size and growth		X	
Active Directory application servers CPU and RAM performance (for servers under management)		X	
DNS Services on Domain Controllers		X	
File Replication Service on Domain Controllers		X	
DHCP Service on Domain Controllers		X	
Certificate Service on Domain Controllers		X	
Incident and Problem Management	**Client**	**Hosted Cafe'**	**Extended Services***
Incident management		X	
Root cause analysis		X	
Troubleshoot down Microsoft Active Directory environment		X	
Identify and Resolve Cluster/DAG issues	X		Managed Server(s)
Patch Management	**Client**	**Hosted Cafe'**	**Extended Services***

Software updates	X		
Software version upgrade (Major release)	X		
Security patching (Critical Vulnerability Only for covered Domain Controllers only)		X	
Management	**Client**	**Hosted Cafe'**	**Extended Services***
Administration or Creation of Active Directory accounts		X	
User password changes/administration	X		Help Desk
Group Membership administration		X	
Group Policy creation/administration/installation	X		ProServices
DNS record creation/administration		X	
DHCP scope creation/administration		X	
Replication partner creation/administration	X		ProServices
Active Directory Design and Policy	X		ProServices
Active Directory and mailbox management	X		ProServices
Mail enable existing Active Directory account		X	
Anti-spam and anti-malware management	X		Managed Security
Administration and creation of Security Groups		X	
Administration and creation of Distribution Groups		X	
Administration and creation of Organizational Units		X	
Administration and Creation of additional Forests or Domains	X		ProServices

Administration and Creation of Federation Services	X		ProServices
Administration and Creation of Rights Management Services	X		ProServices
Permission and role management	X		ProServices
SSL certificate purchase, installation and renewal	X		ProServices
Administration and Creation of address book	X		ProServices
Content conversion	X		ProServices
Administration and Creation of Cluster/DAG	X		ProServices
Restore from backup	X		Backup as a Service
Reporting	**Client**	**Hosted Cafe'**	**Extended Services***
Standard Operations Reports		X	
Custom Reports	X		ProServices

*Extended services are optional services that can be provided with incremental fees.

4 MONITORING

Rule Name	Type	Frequency	Severity Ranking
Multiple Logon Failures High Qty: Domain (ND)	Event log	must fire 100 times within 30 minutes	Sev 4
Failed Login from Privileged Account (ND) (c) -	Event log	must fire 3 times within 10 minutes -	Sev 6
Multiple Logon Failures Low Qty: Domain (ND) -	Event log	must fire 5 times in 10 minutes	Sev 1

Rule Name	Type	Frequency	Severity Ranking
Account Locked: Domain (ND)	Event log	every occurrence	Sev 1
User deleted from Domain Admin Group (ND)	Event log	every occurrence	Sev 4
User added to Domain Admin Group (ND)	Event log	every occurrence	Sev 4
Concurrent Failed Authentications To Same Account From Multiple Countries (ND)	Event log	two failed logins from two different countries to the same account wihin an hour	Sev 1
Concurrent Failed Authentications To Same Account From Multiple Cities (ND)	Event log	two failed logins from two different cities to the same account wihin an hour	Sev 1
Concurrent Successful Authentications To Same Account From Multiple Countries (ND)	Event log	two successful logins from two different countries to the same account wihin an hour	Sev 1
Concurrent Successful Authentications To Same Account From Multiple Cities (ND)	Event log	two successful logins from two different cities to the same account wihin an hour	Sev 1
Sudden Increase in Successful Logons To A Host (ND)	Event log	Detects a sudden 50% increase of successful logons and 25% more distinct users or 100% more distinct source IP addresses to a particular server over a 30 minute window	Sev 3
Failed Account Activity On Disabled Account (ND)	Event log	Failed login attempt to a user disabled within the last 24 hours	Sev 6
Successful Account Activity On a Disabled Account (ND)	Event log	Successful login attempt to a user disabled within the last 24 hours	Sev 6

Rule Name	Type	Frequency	Severity Ranking
Transient Account Usage (ND)	Event log	Account created, successfully logged into, and deleted within 1 hour	Sev 6

5 REPORTING

Customized server availability and performance as requested by client.

This service is part of the Managed Infrastructure Services. Details listed below.

6 MANAGED INFRASTRUCTURE SERVICES

Managed Infrastructure and Monitoring Services provides organizations with the management and monitoring of their infrastructure, whether the infrastructure is on premises, a third party datacenter or the cloud. The service can support servers, file storage and specified applications. Managed Infrastructure and Monitoring Services allows businesses to extend their IT departments with experienced and expert resources. Managed Infrastructure and Monitoring Services can help drive down costs associated with infrastructure management, using a proven Information Technology Infrastructure Library (ITIL) framework for service delivery. ITIL consists of service desk, incident management, problem management, configuration management, change management and reporting.

Hosted Cafe's responsibilities for Managed Infrastructure and Monitoring Services include:

- Service and Support center with 24/7/365 coverage
- Hosted Cafe' offers management and monitoring of devices and software according to the agreement between customer and Hosted Cafe' to aid in resuming normal operations.
- Additional requests above and beyond will be based upon Time and Material expense to the customer, with no SLA.
- Detection, isolation, diagnosis of each fault and restoration to normal operating conditions, testing and documenting each fault within the Hosted Cafe' trouble ticket system
- Ownership of resolution of the problem on behalf of the Customer and act as an agent for the Customer under executed letters of agency
- Notify the Customer of the progress of all faults per Customer provided contact process.
- Critical software and firmware updates.
- Summary reports delivered via our Managed Services monitoring portal to help you understand performance, utilization and device details
- Assistance with warranty replacement and vendor escalations.
- Changes to individual devices. Mass additions/deletions or changes (greater than 5) are not covered via the Managed Network Services agreement and will be considered project billable tasks.
- Safeguard customer's proprietary information using commercially reasonable efforts to securely access client network and manage the infrastructure.
- Monthly Server OS Patching. For greater detail of InterVision server OS patching service see the Managed OS Patching Service Guide.

Out of Scope

- Hardware or Software installation, major upgrade or non-RMA replacement is not included with network support. Professional services may be purchased to assist with installation, upgrade or replacement.
- Software license and subscriptions are not included. Devices provided by InterVision to provide the service will be licensed.
- Mass additions/deletions or changes (greater than 5) are not covered via the Managed Network Services agreement and will be considered project billable tasks.
- Coverage for devices not under agreement are ineligible for support of any type.

Customer Requirements

To allow for successful monitoring and management of devices customer responsibilities include:

- Providing all network and device information for Hosted Cafe' to discover the contracted devices and enable monitoring. This information includes: network diagrams, site information, circuit information and Customer vendors, Letters of Agency, and current software levels.
- Providing resources to run Hosted Cafe's monitoring and collection tools, and the means for the Hosted Cafe' Collector to contact the Hosted Cafe' Data Center.
- Performing configuration of devices and network, as necessary, to facilitate monitoring and management of the contracted devices. In the event the customer is unable or does not have the personnel to enable monitoring and management of devices, Hosted Cafe's Professional Services can be engaged for assistance at an incremental cost.
- Provide devices access - Remote access to devices must be available for support. The client is responsible for out of band access, along with in-band access.
- Provide a distribution list of Customer contacts to receive alarm triggered emails and reports
- Supply InterVision with all the necessary security information including dial-in numbers, access ID's, passwords, SNMP community names necessary for InterVision to perform the Services
- Provide notification contact and escalation lists for use by InterVision during business and non-business hours.
- Provide InterVision with site contact to facilitate InterVision's access to Equipment and connection terminations, along with out-of-hours access procedures
- Notify InterVision within 72 hours of any changes to the contracted Devices.
- Execute letters of agency notifying vendors, such as carriers, that InterVision will represent the Customer by isolating and troubleshooting Customer's network problems
- All devices and applications must have vendor support contracts (example = Cisco SmartNet) and operate at currently supported vendor versions. Exceptions include Hosted Cafe'-hosted infrastructure, and devices with lifetime warranty support from the vendor for hardware replacement.
- All devices must be in a supportable state, including current versions of software supported by vendor, with all critical patches applied, in a production capable state with no known failures or functions in order to be covered. Remediation efforts to bring software to current version including patches to make a device production capable will be billable to the customer.

6.1 SERVICE LEVEL OFFERS - MANAGED INFRASTRUCTURE

Service	Monitor Only	Standard	Enhanced
Phone Support 24/7/365	Not Included	Unlimited	Unlimited

Service	Monitor Only	Standard	Enhanced
Onsite Support 24/7/365	Not Included	Not Included	Included [1, 2]

Figure 1 – Managed Infrastructure Service Levels

[1] *Applies to devices covered under Managed Infrastructure Services in the continental US. International onsite coverage may be added via a custom scope of work.*

[2] *Onsite support is at the discretion of Hosted Cafe'*

6.2 SERVICE LEVELS

Monitor Only levels of service are detailed below.

Service	Monitor Only	Standard	Enhanced
Phone Support 7AM-7PM, MON-FRI*	Not Included, No SLA	Included, with SLA	Included, with SLA
Phone Support Off-Hours	Not Included, No SLA	Included, with SLA	Included, with SLA
Onsite Support 7AM-7PM MON-FRI**	Not Included	Not Included, No SLA.	Included, with SLA
Onsite Support Off-Hours**	Not Included	Not Included, No SLA	Included, with SLA
Phone Support – Devices Not Covered by NetTend	Not Included	Not Included	Not Included
Onsite Support – Devices Not Covered by NetTend	Not Included	Not Included	Not Included

All coverage times are based on the local time zone of the supported device.

**Applies to devices covered under Managed Infrastructure Services in the continental US. International onsite coverage may be added via a custom scope of work.

- In the event that an outage or network problem occurs which is determined to be a site related issue Hosted Cafe' will document the Incident within its ticketing system. Examples of site related Incidents are: Loss of power to site, damage to premise cabling, accidental disconnection of site cabling or Equipment.
- In the event that an outage or network problem occurs which is determined to be a Broadband Carrier circuit failure, Hosted Cafe' will, via a Letter of Agency from Customer, contact the relevant Carrier or ISP and report the Incident for resolution. Hosted Cafe' will then continue to manage the problem and follow up with the Carrier or ISP to ensure service is restored as quickly as possible.

- In the event that an outage or network problem occurs which is determined to be a failure of CPE, Hosted Cafe' will diagnose and attempt to resolve the issue remotely. If the outage cannot be resolved remotely, Hosted Cafe' will escalate to the Customer and/or technician dispatch when needed. Determination of the necessity of on-site services is at the sole discretion of Hosted Cafe'. If dispatch is requested and cancelled within 48 hours of requested dispatch time, a $250 cancellation fee will be applied.

6.3 REPORTING

- Hardware availability
- Device performance and capacity
- Trouble tickets
- Change tickets
- Monthly overview reports
- SLA reports

6.4 SERVICE ACTIVATION

Hosted Cafe' employs a structured process to help ensure a smooth transition to Managed Infrastructure and Monitoring services. Our Project Management Office (PMO) owns the process with the Onboarding Engineer (OE), holding the ultimate responsibility and serving as the single point of contact (SPOC).

6.5 STEPS TO ACTIVATE SERVICE

1. Data gathering
    a. Customer service manual
    b. Order form
2. Collector/ Support workstation Deployment and Configuration
3. Onboard customer devices
4. Add data from step one into systems
5. Finalize customer onboarding
6. Send any found issues with onboarding for client to review
7. Go Live/ Customer training
8. Perform true up / Project Closeout

6.6 SERVICE DELIVERY

6.7 INCIDENT AND DEVICE IMPACT CLASSIFICATION

The Managed Infrastructure and Monitoring service employs a sophisticated algorithm called the Ticket Enrichment Engine that utilizes the severity of the incident, and the business criticality of the device to determine the appropriate priority levels. Devices such as routers and firewalls are defaulted to classification as critical devices, and are automatically prioritized higher than other devices. Customers are able to designate other devices as critical, to decrease/increase their prioritization based upon their business impact

Severity 1	No Ticket	
Severity 2	No Ticket	

Severity 3	No Ticket	
Severity 4	Notification Ticket Closed State	
Severity 5	Notification Ticket Closed State	Upgrade Eligible
Severity 6	P3 Ticket	
Severity 7	P3 Ticket	Upgrade Eligible
Severity 8	P2 Ticket	
Severity 9	P2 Ticket	Upgrade Eligible
Severity 10	P1 Ticket	

Emergency (P1 or P2) services require a phone call to create an incident.

7 DEFINITIONS

Monitor only- Hosted Cafe' will place the Customer premise equipment ("CPE"), Cloud Servers, and Software under support and monitoring only service. The Service covers the specific IT infrastructure devices as detailed in an applicable Service Order . There is no phone support or onsite support with this service.

Standard- Hosted Cafe' will place the Customer premise equipment ("CPE"), Cloud Servers, and Software under support and monitoring service. The Service covers the specific IT infrastructure devices as detailed in an applicable Service Order and includes unlimited phone support.

Enhanced- Hosted Cafe' will place the Customer premise equipment ("CPE"), Cloud Servers, and Software under support and monitoring service. With this version of the Service the customer receives both unlimited phone support and onsite support as detailed in an applicable Service Order.