ConRes
CONTINENTAL RESOURCES

ConRes IaaS Management Services for Microsoft Azure

Table of Contents

1. Introduction

Azure offers on-demand access to resources and services to solution providers. However, solution providers need tools and services to effectively manage applications and data residing in Azure to avoid application downtime and business losses. A solution provider, in combination with ConRes management tools and services, can help businesses to ensure that infrastructure on Azure is working optimally while collaborating with users.

With ConRes private labeled IaaS management services capabilities for Azure, solution providers can easily leverage resources on Azure alongside their traditional infrastructure (in LAN, WAN, or datacentre) via a "single-pane-of-glass" deployment model that provides 360 degree visibility, governance, and management.

This document covers the scope of ConRes services for Azure IaaS (compute, storage and network). Statement of service for applications are not covered in this document.

2. Pre-requisites

Customer will be responsible for performing the following activities as part of the preliminary work to begin onboarding customer's environment. All information is captured as part of the onboarding data collection documentSend onboarding form filled with the following information

- Provide remote access details to customer's infrastructure
- Provide network, and ISP information
- Provide Azure subscription and on-premise login information
- Provide point of contacts for notifications and escalations

3. Onboarding Infrastructure to ConRes IaaS Management Services for Azure

Onboarding a SMB's infrastructure for solution provider by ConRes IaaS management services for Azure is a three-stage process:

1. Stage-1: Process order
2. Stage-2: Onboard client's Azure instances and on-premise infrastructure to ConRes services
3. Stage-3: Start services for customer

The onboarding timelines are between 1 to 2 weeks if the customer has provided all of the onboarding information and access to client's infrastructure. (Note, ConRes will automatically initiate management services if customer has used ConRes services for migration of IaaS for Azure.)

Onboarding the infrastructure is tracked through a ConRes platform. First, confirmation to start onboarding is sent by ConRes to customer. Next, ConRes will start validation of the onboarding data, and provide real-time updates to the customer on any missing information. Customers can collaborate with ConRes real-time via the platform for any progress made, and also when additional information or approvals are required.

4. SOW Guidance

ConRes provides the following guidance to customers in terms of its assumptions and dependencies. These may be used by customers to customize scope and/or set expectations to their customers:

- ConRes IaaS management services for Azure defined in this document are scoped for SMB environments only (i.e. environments with less than 100 users)
- Customer has created and purchased Azure subscriptions for customer and provides login with administrator privileges to ConRes
- Customer is aware of Azure subscription costs for instances and storage

- ConRes provides private labeled IaaS management services for Azure to customer. Customer will manage the end-customer relationship, escalations to customer, and communication from customer to ConRes
- Supported OS: Windows Server 2008 & above
- Supported Applications: Active Directory, DNS, RDS, File server, Exchange, SQL, SharePoint, LOB Applications (Sage, QuickBooks, Time management, etc.,)
- Customer should subscribe to ConRes Backup and/or ASR management services for Azure on ASR protected instances for ConRes to monitor and manage disaster recovery (DR)
- ConRes will leverage its Azure specialists to remediate any issue encountered during the troubleshooting process. ConRes will escalate and coordinate with Microsoft Azure support for any events as required.

5. Scope of ConRes IaaS Management Services for Azure

Our goal is to increase margins to the customers with minimum or no effort from customers. Customers will benefit from saving resource time, avoiding need to hire and train new resources, and ensuring faster time to market their new technologies and services.

For IaaS management services for Azure, ConRes offers end-to-end management of customer's infrastructure for the alerts that are generated from existing configuration. ConRes ensures a time bound resolution of issues, and coordinates with 3rd party vendors or technology vendors such as Microsoft, for support to resolve issues.

This document specifies the scope and schedule of the services delivered within the ConRes IaaS management Services for Azure. As a requirement to start services, this document must be signed by the customer, as an agreement for the scope and deliverables.

Management for an Azure instance in IaaS includes the following components:

Compute	Storage (Disks attached to Azure instance)	Network

5.1. Entitlements for ConRes IaaS Management Services for Azure

ConRes Azure Premium: A complete suite of management services where ConRes covers all aspects of management and administrative activities. Scope includes monitoring, alerting, full problem troubleshooting, and remediation.

Entitlements for ConRes IaaS Management Services for Azure	ConRes AZURE PREMIUM
Customer Portal – monitoring, management, tickets, session recordings, remote console, reports, executive dashboard, private branded, on-demand, weekly & monthly reports, two-way integration with Autotask or ConnectWise	✓
24x7 monitoring, alert filtering & prioritization of Azure instances and applications from NOC (ISO27001 certified)	✓
On-Premise to cloud connectivity management Including ISP vendor escalations[1]	✓
Virtual Network, VPN Management[1]	✓
Troubleshooting and full remediation of IaaS including spinning up of new instances to resolve issues	✓
Root cause analysis of critical issues	✓
Microsoft Azure support escalation and coordination as required	✓
Patch Rating Service, Patch Failure Alerts [2]	✓
Patch Installations & Antivirus Definition Updates For Supported Antivirus Products [2]	✓
Advisory Services (quarterly once): ConRes Azure specialist, who understands client's Azure workloads, will run quarterly assessment of Azure environment and provide recommendations to optimize infrastructure	✓

---

[1] Available only for Azure VPN monitoring, On-Premise Network.

[2] Available only for Windows servers

Customer or Customer must have valid maintenance or technical contract from appropriate vendor for network devices, OS (Microsoft or non-Microsoft), 3rd party applications, and anti-virus products. Expiration of maintenance or technical support agreements places limits on management services. Software & hardware placed into 'End of Life' by vendor will be restricted to best effort basis only.

The various services and scope defined in this SOS document may be spread over and accounted in multiple SKUs (Stock Keeping Units), and not necessarily one SKU. Please refer to the price list to understand what services and scope is included in each SKU.

Any items not explicitly covered within this document are considered out of scope. ConRes will review new requests or questions received from customers and add clarifications or define the items explicitly in the SOS documents.

5.2. Supported Devices

IT INFRASTRUCTURE	SUPPORTED TECHNOLOGY
Azure Cloud	Virtual Machines, Active Directory, Websites, File Servers, Database, Storage, Virtual Networks, VPN
Server Operating Systems	Windows: Windows Server 2008 and above
	Linux: Centos/ Redhat 5.3 & above, and Ubuntu 10.0 & above
Infrastructure Applications	File & Print, DNS, DHCP, Domain Controller(Active Directory), Email (Microsoft Exchange), Terminal Services/Remote Desktop Services, Citrix
Line Of Business Apps (LOB)	Sage, QuickBooks, Time Management Apps, Project Management Apps
Backup Applications (if purchased separately)	Azure backup, Azure Site Recovery
Antivirus Products	Symantec, McAfee, Trend Micro, VIPRE Business Premium, Kaspersky, ESET NOD32, and Microsoft Security Essentials

5.3. Key Monitoring Parameters

ConRes monitors the IaaS infrastructure for Azure using standard Windows WMI, SNMP, API, and CLI data collection. All devices are monitored for hardware (if applicable), operating system, and application health. ConRes has a global list of monitoring templates that were built and enhanced over a period of over ten years. Monitors for IaaS management for Azure covers compute, storage, and network devices.

Customers can request for changes to the monitoring for a specific device. ConRes will review, and if changes are reasonable, it will authorize and apply the changes as requested.

5.4. Troubleshooting and Full Remediation

ConRes services team will remotely troubleshoot and fix issues for alerts that are generated from existing configuration of customer's infrastructure.

Multiple tasks and activities are performed remotely for the customer by ConRes. They include:

- **Azure virtual machine down**: ConRes will start virtual machine or restore Azure instance from backup
- **Server restart**: ConRes will perform sanity check to make sure all necessary automatic services are running and no critical events exist on server
- **Critical system services**: ConRes will troubleshoot dependencies and start services
- **Disk space issues**: ConRes will validate high disk space utilization, and if required increase disk size or add additional disks on Azure instance
- **CPU or memory utilization**: ConRes will validate processes that contribute to high utilization and kill rogue processes, if any, or if it is a system process, ConRes will reboot server to bring utilization to normal

- **Disk utilization (I/O)**: If disk queue length on server constantly grows, and disk I/O on server increases, ConRes will troubleshoot processes and applications that cause high disk I/O or queue length, and provide recommendations to resolve problem.
- **VPN connectivity**: ConRes will resolve any VPN connectivity issues
- **Name resolution issues**: ConRes will validate DNS and gateway settings to isolate problem and resolve

Application Management

Application management is included for supported applications that are in scope. Please refer to respective application statement of services (SOSs) and price list for applications that are included such as File & Print, DNS, DHCP, Domain Controller (Active Directory), Email (Microsoft Exchange), Websites (IaaS), Database, storage, Remote Desktop Services, Sage, QuickBooks, Time Management Apps, and Project Management Apps.

5.5. 3rd Party Vendor Escalations

For Microsoft vendor support, it is limited to Microsoft Azure support to resolve any issues with product or configuration for applications and operating systems.

For 3rd party vendors, if problem involves a 3rd party application (excluding LOB apps), then ConRes will contact vendor technical support to resolve issues with application configurations and operating systems.

- ConRes recommends that customer maintain valid support contracts for entire infrastructure management by ConRes
- ConRes requires that customer authorizes ConRes to act on their behalf when it interacts with vendor tech support organization

5.6. On-Premise to Azure Connectivity Management

ConRes will manage on-premise to Azure cloud connectivity for WAN links and VPN for following events: (a) link down (b) high latency (c) high interface errors.

Note, for ConRes to perform connectivity management, customer should subscribe to ConRes management services on network devices and firewall (VPN) device and authorize ConRes to act on their behalf for any escalation with ISP.

ConRes will monitor WAN connectivity, and if there is a problem, ConRes will contact ISP and/or create online ticket. All ISP related issues, such as internet or WAN links down will be escalated to ISP either by phone call and/or online ticket. ConRes will also escalate issue to customer. Summary of conversations with ISP will be updated in ticket.

5.7. Preventive Maintenance

The following preventive maintenance activities are done on a scheduled basis:

5.7.1. Windows Patch Management

ConRes patch management services for Azure includes: (a) scan of servers for missing patches every Wednesday, (b) publish results of patch scan, (c) publish actions to be taken, and (d) seek approval from customer via portal. Additionally, following policies are applied:

- If installation of patch fails, ConRes will take corrective action and failed patches will be re-installed during next scheduled patch maintenance schedule approved by customer
- The installation of security patches on servers will be scheduled for installation during maintenance window provided by customer
- Windows security patches and “Critical” patches are tested by ConRes using known best practices – ConRes then rates the patches as “Whitelisted” or “Blacklisted”.

Supported operating systems and applications

Operating Systems Windows	Windows Server 2008 and above

By default, ConRes will review and install all whitelisted patches at the defined patch installation schedule. Customer has option to manually approve patches via the ConRes customer portal.

Sanity Checks (Servers Only): After Windows Patch Installation and Server Reboot
ConRes conducts sanity checks on Windows servers only after a patch installation and server reboot. Sanity checks include the following:

- For Windows services: Check for services where "Start-up" type is "Automatic" and "Status" is "Started". ConRes will re-start the Windows service if "Start-up" type is "Automatic" and "Status" is "Stopped".
- For event logs: Application and system event logs that show "Severity Level" as "Error" will be checked

Additional Notes

- Default Windows patch management includes installation of security patches and critical patches.
- It is important to note that the server will be rebooted following any patch installation that requires rebooting. Therefore, customer's approval of the patching time window should take into consideration the possibility of reboot.
- Windows Patch Testing: Windows security patches are tested by ConRes using known best practices. Windows security patches released by Microsoft are first installed in a restricted test environment (that supports standard applications & tools). It is then tested for installation issues, standard application compatibility, and malfunction. ConRes personnel will also periodically review forums on patch testing to understand other known issues. ConRes testing procedures are best effort in a limited testing environment. After installation of whitelisted Windows security and critical patches, ConRes does not accept any liability resulting from crashes or malfunction of devices and applications, should they occur.

5.7.2. Linux Patch Management

ConRes patch management services for Azure includes: (a) scan of servers for missing patches the first week of each month, (b) publish results of patch scan, (c) publish actions to be taken, and (d) seek approval from customer via portal. Additionally, following policies are applied:

- If installation of the patch fails, a corrective action will be taken by ConRes, and the failed patches will be re-installed during the next scheduled patch maintenance schedule approved by the customer
- Linux patches on servers have to be approved by the customer
- The installation of security patches on servers will be scheduled for installation during the maintenance window provided by the customer

Sanity Checks (Servers Only): After Linux Patch Installation and Server Reboot
ConRes conducts sanity checks on Linux servers only after a patch installation and server reboot. Sanity check includes the following:

- Check for running Linux services -- ConRes will restart the Linux service if stopped
- Check for application & system logs

Additional Notes:

- Default Linux patch management services includes installation of security patches
- It is important to note that the server will be rebooted following any patch installation that requires rebooting. Therefore, customer's *approval of the patching time window should take into consideration the possibility of reboot.*

5.7.3. Antivirus Definition Updates

This activity includes checking the anti-virus definitions on the Windows server and updates to those definitions on a scheduled basis. Anti-virus definitions will be updated on a daily basis by default. If the anti-virus update event fails in its regular schedule, then ConRes will validate and run the definition updates once again. If the definition updates fail two consecutive times, or if the definition versions are older than two days, then ConRes will remedy the issues as per the SLA under effect.

The customer will be alerted for following issues with anti-virus application or its definition update: (a) corruption, or (b) license expiry. Additionally,

- All issues arising out of anti-virus definition updates are categorized at a "P3 Priority" (i.e. "Severity 4" in ITIL terminology)
- If the anti-virus or anti-malware update event causes system related issues, then the ConRes services team will engage as per the SLA under effect.

Supported Anti-Virus products
Symantec, McAfee, Trend Micro, Kaspersky, ESET NOD32, Microsoft Security Essentials, and VIPRE

Preventive maintenance schedules on servers

Maintenance Activity	Frequency	Schedule
Anti-virus definition updates	Daily or Weekly	2 PM if daily;
Patch Scan		Wednesday 1 PM
Patch Management (Install)	Monthly	One weekend in the month (Sat. or Sun.)

6. Customer Visibility and Auditability

6.1.1. Auditability

All remote activities performed through customer portal by ConRes Azure specialist are recorded and available for the customer to replay and review via the session recordings capability in the ConRes customer portal.

6.1.2. Infrastructure Visibility Portal

ConRes services provide visibility into customer's IT infrastructure via ConRes customer portal. This provides access to current status of the devices across different locations, while providing useful trending reports for advanced analysis.

All the incidents are logged into an ITIL based ticketing system and ticket is updated with its complete chronology as well as steps taken to remediate incident. All updates are synced to Customer's Connectwise or Autotask system via 2-way integration.

6.1.3. Reports

ConRes services for Azure also include reports that offer a comprehensive view of performance and availability of customer's infrastructure. Customer can generate on-demand and/or schedule reports from the ConRes customer portal that include the following:

- Inventory reports
- Problem & incident management reports
- Executive summary reports (monthly)

7. Service Level Agreements

All activities will be performed in an SLA based service delivery model. Customers should inform ConRes of any device addition or deletion, as well as any changes to customer's infrastructure.
The following table describes the various priority levels associated with incidents. The sources of alerts are either from monitoring system and/or user requests entered via the ticketing system, phone, and/or emails.

Priority Definitions

Priority	Resolution SLA	Mode of escalation
P0: Critical	This is an EMERGENCY condition that **significantly** restricts the use of an application, system, network or device to perform any critical business function. This could mean that several departments in the organization are impacted. Direct calls will be made by ConRes to the designated IT contact.	Phone, Email and Ticket
P1: High	The reported issue may **severely** restrict use of an application, system, or device in the network. This could mean that a single department is impacted but the overall network and servers are functioning.	Email and Ticket
P2: Medium	The reported issue may restrict the use of one or more features of the application, system, network or device, but the business or financial impact is not severe.	Email and Ticket
P3: Low	The reported anomaly in the system does not substantially restrict the use of one or more features of the application, system, network or device to perform necessary business functions.	Email and Ticket

Service Levels for ConRes Premium Services for Azure

Priority	Service Response Time	Customer Notification	Resolution SLA	Measured
P0: Critical	15 Min	Call within 15 Min	85% of the cases resolved in 12 Hours	Monthly
P1: High	2 Hours	Email sent and Ticket updated within 2 Hours	85% of the cases resolved in 24 Hours	Monthly
P2: Medium	4 Hours	Email sent and Ticket updated within 4 Hours	85% of the cases resolved in 60 Hours	Monthly
P3: Low	12Hours	Email sent and Ticket updated within 12 Hours	85% of the cases resolved in 120 Hours	Monthly

- Resolution SLAs are void for those cases that are escalated to vendor tech support, hardware vendor, ISP, or third party vendors
- Resolution SLA timer is paused during the following ticket statuses: (a) "Handed-over to customer" (b) "On-Hold" (c) "Under Observation" (d) "Resolved"

Appendix A. : Out of Scope Services

The following list of service activities are not within scope of **ConRes Management Services for Azure**. These activities can be delivered as custom services using the professional services option that may be purchased separately in conjunction with ConRes management services for Azure. Please contact ConRes for more details.

The following is the set of activities that are out of scope for **ConRes Management Services for Azure**

AREA	OUT OF SCOPE
Monitoring	▸ Customizations to monitoring templates are subject to review and acceptance
Azure Instance	▸ OS or root drive expansion on Azure instance is out of scope
Standard Operating Procedure (SOPs)	▸ Any SOP customized by customer is out of scope
3rd Party Vendor Escalations	▸ Line Of Business app vendors ▸ Full hardware vendor management
Patch Management	▸ Service pack updates, driver updates, and classification of patches are not included in default installation of patches. Customer can request installation of these updates by creating a request to ConRes
Antivirus Definition Updates	▸ Re-installation of AV software ▸ License management is the responsibility of the customer ▸ Anti-virus scans will not be scheduled by default on desktops & servers
Service Requests	See below

Service Requests

Service Requests (SRs) are out of scope. SRs are requests that originate outside of the scope of disruption of services. Examples of these SRs are:

- Architect, plan, install of server farms including install/upgrade/migrate of applications.
- Configure or setup VPN and/or network
- New instance, provisioning, configurations, & migrations
- New site architect/design/re-design/ migrations of network infrastructure, remote office, or branch office.
- New firewall rules & routing table modifications
- DNS changes & IP allocations, network topology changes
- Rule changes (NAT, rules, VLANs, routes, access)

(Some of the above requests can be handled as professional services projects by ConRes. Please contact ConRes for more details.)