Inframanage AWS Specsheet

ABOUT 'InfraManage AWS' SERVICE

'InfraManage AWS' offers management of AWS Cloud Services leveraging skills from shared NOC and 24 X 7 operations support. Shared infrastructure management service is built on a concept of standardization to bring in operational efficiency by means of monitoring, troubleshooting, remediation and capacity improvements. It is a SLA based service backed by defined escalation matrix and best practices processes. Netmagic, being a multi-cloud provider, offers this service to customers having AWS cloud billing through Netmagic and also to customers looking only for Managed Services.

The support includes AWS platform services configuration, Change & Configuration management, Fault management, and Performance management. The benefits with Netmagic AWS Managed Services are:

- AWS platform services management
- AWS certified engineers and architects
- Reduced downtime risks with Netmagic excellent operational delivery
- Coordination with AWS support team
- Infrastructure performance reports from AWS portal

AWS SUPPORTED SERVICES:

SR#	AWS Service	Service Category
1	Amazon Elastic Compute Cloud (EC2)	Compute
2	Auto Scaling	Compute
3	Amazon Relational Database Service (RDS)	Database
4	Amazon DynamoDB	Database
5	Amazon Simple Storage Service (S3)	Storage
6	Amazon Elastic Block Store (EBS)	Storage
7	Amazon Glacier	Storage

8	Amazon Virtual Private Cloud (VPC)	Network & Content Delivery
9	AWS Direct Connect	Network & Content Delivery
10	Elastic Load Balancing | NLB	Network & Content Delivery
11	Amazon Inspector	Security Identity & Compliance
12	AWS Shield Standard	Security Identity & Compliance
13	AWS Shield Advanced	Security Identity & Compliance
14	AWS WAF	Security Identity & Compliance
15	Amazon CloudWatch	Management Services
16	Amazon CloudWatch Events	Management Services
17	Amazon CloudWatch Logs	Management Services
18	AWS Snowball	Migration
19	AWS Support	
20	AWS Personal Health Dashboard	

SERVICE DETAILS

Service Scope of Work for AWS Services Configuration – (NSSIMSIMG-AWS)

Service Component	Description

AWS Platform Services Configuration	• AWS Portal Management
	• VM Provisioning with AWS OS Templates (Create / Modify / Delete)
	• Portal User Access (AWS – IAM)
	• VM Snapshot (Create / Delete)
	  ○ Create volume
	  ○ Create image
	  ○ Modify permissions
	  ○ Add / Edit tags
	• Virtual Firewall Rule Addition with AWS Security Groups
	  ○ Setup of Default / Custom security groups
	  ○ Add / Edit / Delete rules to security groups
	  ○ Add / Edit tags
	  ○ Add / Edit / Delete Inbound / Outbound rules

- Configure Monitoring with AWS Cloudwatch
  - Setup notifications with AWS Cloudwatch events
  - Creating log groups
- Instances management
  - Start / Stop / Reboot / Terminate instances
  - Add / Edit tags
  - Attach / Replace IAM role
  - Change instance type
  - Change termination protection
  - View / Change user data
  - Get instance screenshot
  - Modify instance placement
  - Attach / Detach network interface
  - Change Source /Destination check
  - Manage IP addresses
  - Enable / Disable detailed monitoring
  - Add / Edit alarms
- Virtual Network Provision with AWS – VPC
  - Create / Delete VPC
  - Edit CIDRs, DHCP options set, DNS resolution, DNS hostnames
  - Create / Delete Subnets
  - Create flow log
  - Modify auto-assign IP settings
  - Create / Delete route table
  - Internet gateway: Create / Delete and Attach / Detach to / from VPC
  - Create / Delete egress only internet gateway
  - Elastic IPs: Allocate new address, release addresses, associate / disassociate addresses
  - Endpoints: Create / Delete endpoints, choose route tables, edit policies
  - Create / Delete NAT gateways
  - Peering Connection: Create / Delete connections, accept / reject requests
  - Create / Delete Network ACL
  - Create / Delete customer gateway
  - Virtual private gateway: Create / Delete and Attach / Detach to / from VPC
  - VPN connection: Create / Delete VPN connection, download configurations
- VM Storage Provisioning [AWS EBS] – (Add / Delete)
  - Create / Modify / Delete volumes

	○ Attach / Detach volumes ○ Create snapshot ○ Change auto-enable IO setting ○ Add / Edit tags • AWS Simple Storage Service (S3) / Glacier ○ Create / Configure S3 bucket ○ Manage Object versioning ○ Create Lifecycle Policy ○ Set ACL / Bucket ACL • Virtual Load Balancer Rule with AWS ELB - (Add / Change / Modify) ○ Create / Delete Load Balancer ○ Edit health checks ○ Edit subnets ○ Edit IP address type ○ Edit instances ○ Edit listeners ○ Edit security groups ○ Create / Edit / Delete target groups ○ Register and de-register instances ○ Edit target group attributes • Auto-Scaling configuration ○ Create launch configurations i.e. provision instances based on a reusable template you define ○ Create auto scaling groups and assign a template created through launch configuration
Service Support	• Infrastructure as per AWS Service Limits / SLA AWS subscription Support • Managed Services • Portal Reports
Service Exclusions	• Any Scripting | API Programming and Integration

Service Scope of Work for AWS RDS – (NSSIMSIMG-AWSRDS)

Service Component	Description
AWS RDS for Oracle, MSSQL, MySQL, MariaDB, and PostgreSQL database engines	• Create a database • Set up a firewall rule • Create tables • Bulk load data • Query that data • Restore the database to a previous point in time using SQL Database point in time restore capabilities • Set up firewall rules for your sever and or database • Manage user access • Review, apply and revert performance improvement recommendations • Find queries with high resource utilization • Find long running queries

[1]*AWS RDS service needs to be subscribed separately and it will be based on number of database instances.*

Service Scope of Work for AWS WAF – (NSSIMSIMG-AWSWAF)

Service Component	Description
AWS WAF	• Web application firewall comes preconfigured with CRS 3.0 by default • SQL injection protection • Cross site scripting protection • Common Web Attacks Protection such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack • Protection against HTTP protocol violations • Protection against HTTP protocol anomalies such as missing host user-agent and accept headers • Prevention against bots, crawlers, and scanners • Detection of common application misconfigurations (i.e. Apache, IIS, etc.) • Custom Rule : Defined with help of Customer / Application Vendor • AWS CloudWatch to monitor the health of the WAF • Service Limits as per the AWS WAF service Limits • No Programming / Scripts will be written / configured

[1]*AWS WAF service needs to be subscribed separately.*

Service Scope of Work for Windows – (NSSIMSIMG-WINDOW)

Service Component	Description

Administration	• User Management:
	  ○ Create/modify/ delete local system users(with respect to application installed on the system)
	  ○ Manage local user groups
	  ○ Manage local user rights
	• Terminal Service installation and configuration
	• Automatic antivirus pattern/definition update[3]
	• Disk space administration - WINS administration

Change & Configuration Management	• Patch testing for system and supported application • Update security patches[1] • Terminal service configuration changes • WINS configuration changes • OS specific configuration changes required as part of change request • Memory dump configurations
Fault Management	• Response to alerts generated by systems or problems reported by customer • Troubleshooting and identification of problem area at OS level • Resolution of problems through configuration changes
Performance Management	• 24 X 7 monitoring of performance parameters (Parameters as per "Monitored Parameters & Threshold" document) through best in class Netmagic monitoring tool '**NGmon**' provided agent need to be deployed on the server • Auto alerts and notification to performance degradation / threshold violation • Identifying bottlenecks and suggesting de-bottlenecking solution
Operation Support[2]	• Work log update for trouble ticket and closure (using NM ITSM tool)
Version Support	• Windows 2008, 2008 R2, 2012, 2012 R2, & 2016 • Standard, Enterprise & Datacenter editions

[1] For patch updates, antivirus updates, server management, etc. Netmagic will use their standard management tools.

[2] Irrespective backup tool (native or third party) and backup type (configuration or data) backup supports need to be subscribed separately for backing up on tape / disk / on local server provided by customer.

[3] Only McAfee AV management is supported and customer has to procure the license. Also customer has to ensure that AV is licensed for usage in case if it is not procured through Netmagic. The supported AV client software is McAfee VSE 8.x (Latest being McAfee Virus Scan Enterprise 8.8, Patch 7 and above).

[4] Due to the dynamic nature of Elastic VMs, monitoring alerts, patches, updates etc. will be reactive/need based. Netmagic shall notify customer about the release of patches and once customer confirms to update the patch, backend team will coordinate with customer for the time to switch on the VM for scheduled maintenance.

Service Scope of Work for Linux – (NSSIMSIMG-LINUX)

Service Component	Description

Administration	• Local user and group management[1]:
	  ○ Create/modify/delete local system users(with respect to application installed on the system)
	  ○ Manage local user groups
	  ○ Manage local user rights
	• Automatic antivirus pattern/definition update[2]

Change & Configuration Management	• Hardening (tcp-wrappers, iptables, sshd_config) • NFS/ SFTP/FTP/SSH administration • File system management • RPM based application installation, perl, php module installation. • Update security patches[3] • OS specific configuration changes required as part of change request
Fault Management	• Response to alerts generated by systems or problems reported by customer • Troubleshooting and identification of problem area at OS level • Resolution of problems through configuration changes
Performance Management	• 24 X 7 monitoring of performance parameters (Parameters as per "Monitored Parameters & Threshold" document) through best in class Netmagic monitoring tool '**NGmon**' provided agent need to be deployed on the server • Auto alerts and notification to performance degradation / threshold violation • Identifying bottlenecks and suggesting de-bottlenecking solution • Kernel fine tuning in consultation with customer
Operation Support[4]	• Work log update for trouble ticket and closure (using NM ITSM tool) • Local System log retention (1 month retention policy) • Sudo access to customer

Version Support	• RHEL
	  • RHEL 5.7 & above
	  • RHEL 6.3 & above
	  • RHEL 7.x
	  • Standard & Enterprise editions
	• RHEL for SAP
	  • RHEL 6.3 for SAP & above
	  • RHEL 7.x for SAP

	• Standard & Enterprise editions
	• CENTOS
	  • CENTOS 6.3 & above
	  • CENTOS 7.x
	• Ubuntu 12.04 LTS, 14.04 LTS, 16.10 LTS, 16.10 LTS
	• OEL 6.x and 7.x
	• Debian 7.0, 7.0 LTS, 8.0, 8.0 LTS
	• SLES
	  • SLES SAP 11 SP3 / SP4
	  • SLES SAP 12, SP1/ SP2
	  • SLES 11 SP3 / SP4
	  • SLES 12 SP1/SP2

[1]*Compliance related task (password aging, individual logins, password policy) are not part of the same. It will require Centralized Authentication tool and to be implemented managed separately*

[2] *Only McAfee AV management is supported and customer has to procure the license. Also customer has to ensure that AV is licensed for usage in case if it is not procured through Netmagic. The supported AV client software is McAfee VSE 8.x (Latest being McAfee Virus Scan Enterprise 8.8, Patch 7 and above).*

[3] *For patch updates, antivirus updates, server management, etc. Netmagic will use their standard management tools.*

[4] *Irrespective backup tool (native or third party) and backup type (configuration or data) backup supports need to be subscribed separately for backing up on tape / disk / on local server provided by customer.*

[5] *Due to the dynamic nature of Elastic VMs - monitoring alerts, patches, updates etc. will be reactive/need based. Netmagic shall notify customer about the release of patches and once customer confirms to update the patch, backend team will coordinate with customer for the time to switch on the VM for scheduled maintenance.*

Service Pre-requisites:

In addition to the InfraMonitor prerequisites, following is required:

- For management of active directory, InfraManage Window is must. Along with OS management required upgrade is to be subscribed to consider of said feature under Netmagic management scope.
- Administrative Remote Access to various components under management with appropriate security measures as mutually discussed and agreed.
- Support for OS which is not part of OEMs Hardware Compatibility List will be on Best effort basis as there is no back to back commitment from the OEM for the concerned OS support.
- AWS Enterprise/Business support subscription is mandatory for technical support.
- AWS Cloudwatch service is mandatory for management of any AWS service.
- Storage space would be required on AWS for storing the hardened AMI's and variable charges would be applicable for the same.
- Ports for monitoring needs to be open for management of AWS services provided the IP addresses are static.

Design / Subscription Guidelines:

Service subscription will be governed by following guidelines:

- Irrespective of number of processor / cores, one InfraManage per server.
- Irrespective of number of vCPU, one InfraManage per instance (VM).

Service Level Agreement:

The SLA's for AWS services would be as per AWS service commitment in the subscription plan contracted by the customer. For InfraManage Windows & Linux OS, Netmagic provides 24 X 7 support.

Severity 1 (S1) -> System down significantly affecting customer

Severity 2 (S2) -> System performance severely degraded but still functioning

Severity 3 (S3) -> Error not significantly affecting the end customer

Severity	Time to log	Time to respond	Target time to update customer*
S1	10 minutes	15 minutes	Every 1 hour
S2	10 minutes	30 minutes	Every 4 hour
S3	10 minutes	30 Minutes	Every 8 hour
Change Request	30 minutes	4 Hours	4hrs or Up on completion of the CR

* Does not form part of SLA, detail definitions and credit calculation are mention in MSA.

DISCLAIMER

Netmagic offers this service based on a combination of third party Hardware, Network & Software. In case of non-availability of the customer infrastructure due to a problem with the Monitoring & Management Services, Netmagic will work with the customer to remedy incidents and restore services at the earliest.

Netmagic will follow best practices for system administration to ensure security of the monitored infrastructure. However customer needs to procure third party security software and services in order to ensure a comprehensive security posture of the monitored infrastructure.

As Internet is used as medium to connect Netmagic NOC to customer network, the monitoring data travels over the Internet; Netmagic will apply generally accepted security measures to ensure confidentiality of data in motion, but will not be responsible for maintaining the security of the data.