MAXPRO® Cloud

Architecture and Security

Version 2.0

May, 2020

Table of Contents

Summary

MAXPRO® Cloud represents one of the first innovations from Honeywell's connected buildings platform and is designed to provide an integrated security experience. MAXPRO® Cloud is powered by Microsoft Azure cloud.

MAXPRO® Cloud Services

Service Name	Description
Web Portal	Web Portal for users
API	ISOM API's for hardware panel and mobile app integration
Device Communication Services	Communications services that handle device to cloud and cloud to device communications for Access and Intrusion devices
Video Services	Live streaming, playback and clip storage Services for video devices
System Services	Core set of backend services which enable the front services and not exposed to internet
Database	Database for persisting data about customer and all hardware configuration and alarms/events

Compute

Following are compute (Virtual Machine) sizing requirements for MAXPRO® Cloud. The Azure VM type listed meets or exceeds the compute requirements identified.

Virtual Machine	Services	CPU/Cores	Memory	Azure VM Type
<ENV>-WEB	Web UI	4	14 GB	D3 v2
< ENV>-API	API service	4	14 GB	D3 v2
< ENV>-ANS	Alarm Notification services	4	14 GB	D3 v2
< ENV>-DCS	Communications services	8	28 GB	D4 v2
< ENV >-MS	Messaging Services	4	14 GB	D3 v2
< ENV >-NS	Notification service Email/Mobile	4	14 GB	D3 v2
< ENV >-CBS	Configuration Services Report Services	4	14 GB	D3 v2

< ENV>-HBS	Audit Service Hardware Services	4	14 GB	D3 v2
< ENV>-EBS	Event Service, Event Log Service	4	14 GB	D3 v2
< ENV>-RS	Rule service	8	28 GB	D4 v2
< ENV>-INFR	Infra services (Identity and cache)	4	14 GB	D3 v2
< ENV>-DB	Database server	8	56 GB	DS13_V2
<ENV>-ADS	Active Directory Service account	4	14 GB	D3 v2

<ENV> shall be specific to

Specific details on each Azure VM type can be accessed at

https://azure.microsoft.com/en-in/documentation/articles/virtual-machines-windows-sizes/

PaaS Services

Azure Redis Cache

Apart from the compute workload which leverage Azure IaaS, MAXPRO® Cloud cache server will leverage Azure Redis Cache PaaS. Azure Redis Cache is based on the popular open-source Redis cache. It gives access to a secure, dedicated Redis cache, managed by Microsoft and accessible from any application within Azure.

Azure Redis Cache is offered in three tier, MAXPRO® Cloud subscribes to the premium tier (P1) which offers high availability and enhanced security features.

Cache Security

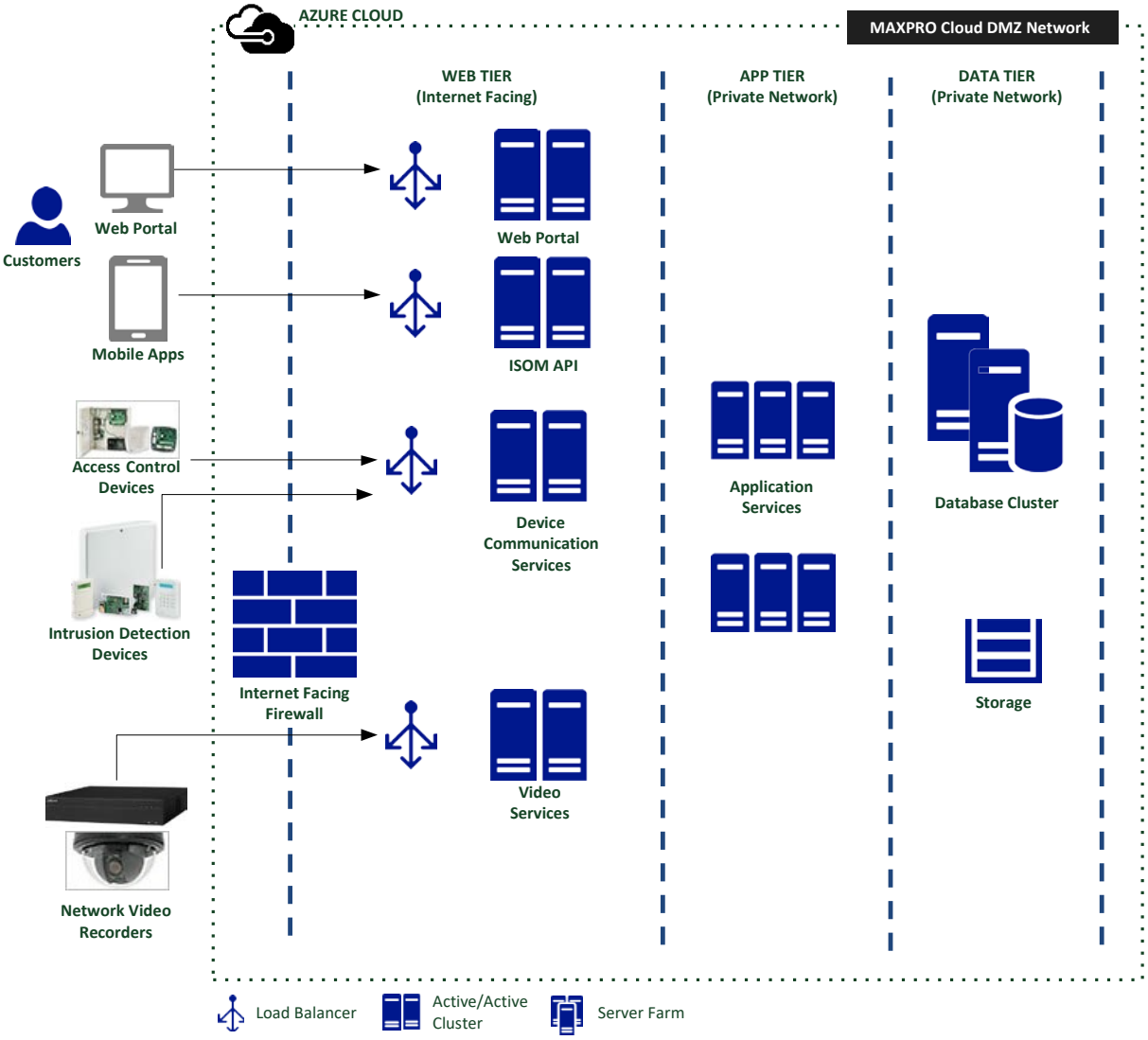
With the Premium tier, only clients within a specified network can access the Cache. **Redis Cache will be deployed in a separate subnet within a Virtual Network (VNet).**

This setup provides cache data isolation a fine-grained access control.

VNet deployment is further detailed under Section Azure Redis Cache Security

Architecture

Servers on Microsoft Azure cloud are deployed on a DMZ network with clear separation of internet services, backend services and database.



Honeywell intrusion and Azure is not shown in the above diagram

High Availability

To avoid a single point of failure, each service is deployed on two virtual machines assigned to an **Availability Set** and deployed across different **Fault Domains**. **Fault Domain** is a collection of servers that share common resources such as power and network connectivity.

Load Balancing

Internet Load Balancer

All internet facing traffic is routed through Internet Load Balancer. It provides network-level distribution of traffic across instances of application services deployed on multiple servers.

Live video streaming does not use load balancers because the devices directly correct to individual streaming server and routing is accomplished using a custom algorithm.

Internal Load Balancer

Backend system services and database are not exposed to internet traffic but are also load balanced using Internal Load Balancer (ILB).

Load Balancing Distribution Modes

All VMs are configured for Active/Active Load Balancing.

WEB tire Load Balancer and Device communication tire Load Balancer is configured for session affinity to keep user session on the same VM's.

Scalability

Azure environment is architected to address specific system performance commitments and growth projection with enough headroom. There is no requirement to support sudden burst in load.

Entire environment comprising of Windows Virtual Machines, SQL server database, storage accounts are monitored for resource utilization like CPU, memory and disk utilization. Alerts are configured which notifies when any resource is beyond a certain threshold.

In the event of resource performance degradation, either horizontal or vertical scaling approach will be adopted. **Performance degradation alerts are triggered by App Dynamics which monitors CPU and memory utilization.**

Horizontal Scaling

Add a similar size Virtual Machine to an availability set and distribute the load using active/active load balancing mode.

Vertical Scaling

Increase the CPU cores and memory on the VM, this is done simply by upgrading the Azure VM type to the next bigger configuration, for example upgrading from F8 which offers 8 CPU cores and 16 GB memory to F16 (16 CPU cores, 32 GB memory) or just increase memory by upgrading to D13_V2 (8 CPU cores, 56 GB memory)

Reserved Public IP Addresses

Following are the internet facing VMs which require public IP addressing and mapped to a domain name.

The public IP addresses are associated to Internet facing Load Balancers only.

Virtual Machine Name	Load Balancer Name	Public IP Resource Name	Domain Name E,g domain: maxprocloud.com
<ENV>-WEB	<ENV>-WEB-LB	<ENV>-WEB-PIP	<i>.maxprocloud.com
<ENV>-ISOM	<ENV>-API- LB	<ENV>-API-PIP	isom.<i>.maxprocloud.com api.<i>.maxprocloud.com
<ENV>-ANS	<ENV>-ANS- LB	<ENV>-ANS-PIP	ans.<i>.maxprocloud.com
< ENV >-DCS	< ENV >-DCS-LB	< ENV >-DCS-PIP	devicecomm.<i>.maxprocloud.com

Public Domain Names

Following are the internet facing domain names for different services.

Service Name	Domain Name (Examples)
Web Portal	https://maxprocloud.com
API Service – Mobile App	https://api.maxprocloud.com/isom
API Service – Device Registration	https://isom.maxprocloud.com/isom
Device Communication	https://devicecomm.maxprocloud.com
Alarm notification	https://ans.maxprocloud.com/isom

High Availability for SQL Server

Azure supports multiple options for SQL Server High Availability, the recommendation architecture is **Always On Availability Groups.** This offers both high availability and disaster recovery.

Always On Failover Cluster Instances leverages Windows Server Failover Clustering (WSFC) functionality to provide local high availability through redundancy at the server-instance level—a failover cluster instance (FCI).

An FCI is a single instance of SQL Server that is installed across Windows Server Failover Clustering (WSFC) nodes. On the network, an FCI appears to be an instance of SQL Server running on a single computer, but the FCI provides failover from one WSFC node to another if the current node becomes unavailable.

In case of a failure (hardware failures, operating system failures, application or service failures), or a planned upgrade, the resource group ownership is moved to another WSFC node. This process is transparent to the client or application connecting to SQL Server and this minimize the downtime the application or clients experience during a failure.

The Always On Availability Groups active secondary capabilities include support for read-only access to one or more secondary replicas (readable secondary replicas). A readable secondary replica allows read-only access to all its secondary databases.

However, readable secondary databases are not set to read-only. They are dynamic. A given secondary database changes as changes on the corresponding primary database are applied to the secondary database.

Always On Availability Groups also supports the re-routing of read-intent connection requests to a readable secondary replica (read-only routing).

Rabbit MQ Cluster

A RabbitMQ broker is a logical grouping of one or several Erlang nodes, each running the RabbitMQ application and sharing users, virtual hosts, queues, exchanges, bindings, and runtime parameters. A collection of nodes is called as a cluster.

Rabbit MQ cluster nodes are listed in a configuration file after the nodes are attached to an Azure Load Balancer. RabbitMQ brokers tolerate the failure of individual nodes. Queues are available on both master and slave nodes and also replicated for high availability. Both nodes are disk based which makes sure there is no loss of data in the event of a node failure. Rabbit MQ servers are running on Cent OS 7.2 Linux.

Azure Datacenters

MAXPRO® Cloud service is available in North America (NA), Latin America (LAR) and Europe (EU), to better serve these markets, two different instances are setup, one in **Azure West US** region to serve NA & LAR customers and another in **Azure West Europe** to serve EU customers.

Instance	Primary Datacenter	Backup Datacenter (Disaster Recovery)
North America, Latin America	West US – California	East US - Virginia

Europe	North Europe – Ireland	West Europe - Netherlands

More specific details on Azure data center locations and services availability can be accessed at:

https://azure.microsoft.com/en-in/regions/services/

Compliance

Azure datacenters comply with industry standards (such as ISO 27001) for physical security and availability

Certification	Azure
CSA STAR Certification	✓
ISO 27001:2013	✓
ISO 27017:2015	✓
ISO 27018:2014	✓
ISO 20000-1:2011	✓ **(new)**
ISO 22301:2012	✓
ISO 9001:2015	✓

Network

Each instance is configured on an Azure Virtual Network (**Vnet**). MAXPRO® Cloud adopts a three-tier deployment architecture – Web, App and Database.

VNet and Subnets

Virtual Network Name	Purpose
<ENV>-VNET	All resources of Staging and Production instances for a given region

Table 8.1 VNet Configurations

This three-tier architecture is achieved by creating separate **subnets** for web, app, database and associating the VMs to them. Communication between the subnets and from the internet is restricted using **Network Security Group (NSG)** configurations.

Below table defines the subnet configuration for North America and Europe production environments.

Subnet Name	VNet	Network Security Group
<ENV>-WEB-SUBNET	<ENV>-VNET	<ENV>-WEB-NSG
<ENV>-APP-SUBNET	<ENV>-VNET	<ENV>-APP-NSG
<ENV>-DB-SUBNET	<ENV>-PRD-VNET	<ENV>-DB-NSG
<ENV>-COMMON-SUBNET	<ENV>-PRD-VNET	<ENV>-COMMON-NSG

Table 8.2: Subnet

Global Traffic Management

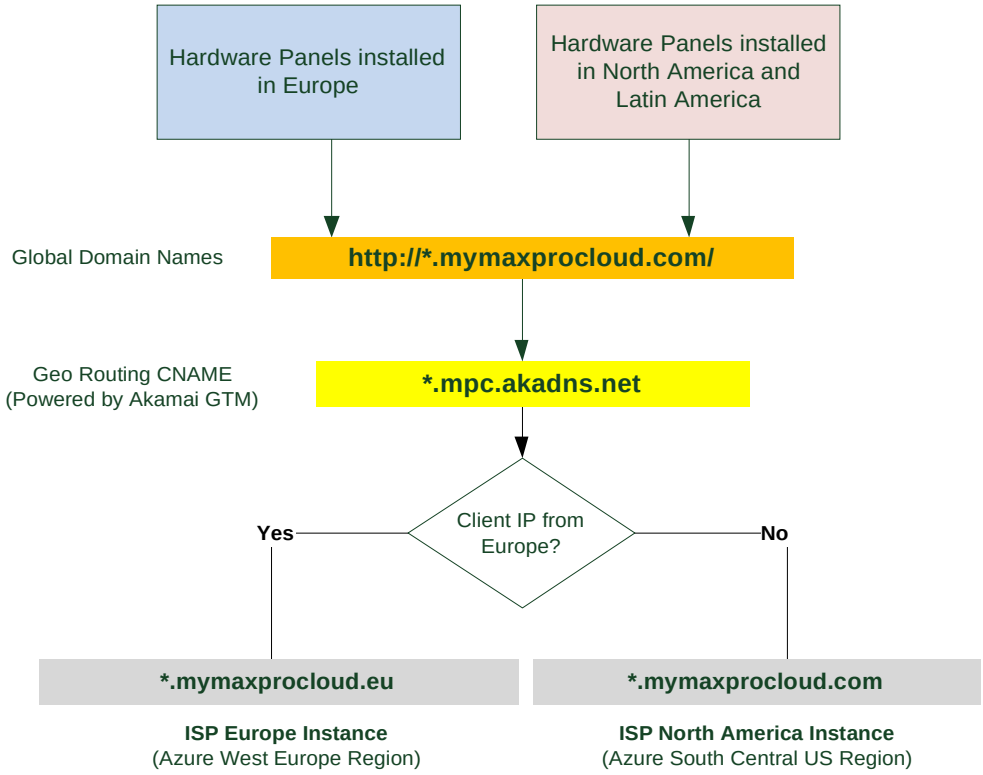
There are multiple product offerings based on MAXPRO® Cloud and the hardware devices are sold across different regions in the world – North America, Latin America, and Europe.

The hardware devices are shipped with pre-configured URLs to enable easy installation and establish device to cloud connectivity. Separate cloud instances are configured for European markets to satisfy legal and data privacy compliance requirements.

Changing the URLs on the panel to enable cloud connectivity to respective regional cloud instances requires introducing new SKUs with different firmware versions.

To avoid this scenario, a global traffic routing is implemented which can intelligently route traffic from hardware devices based on their installed location to respective regional cloud instances.

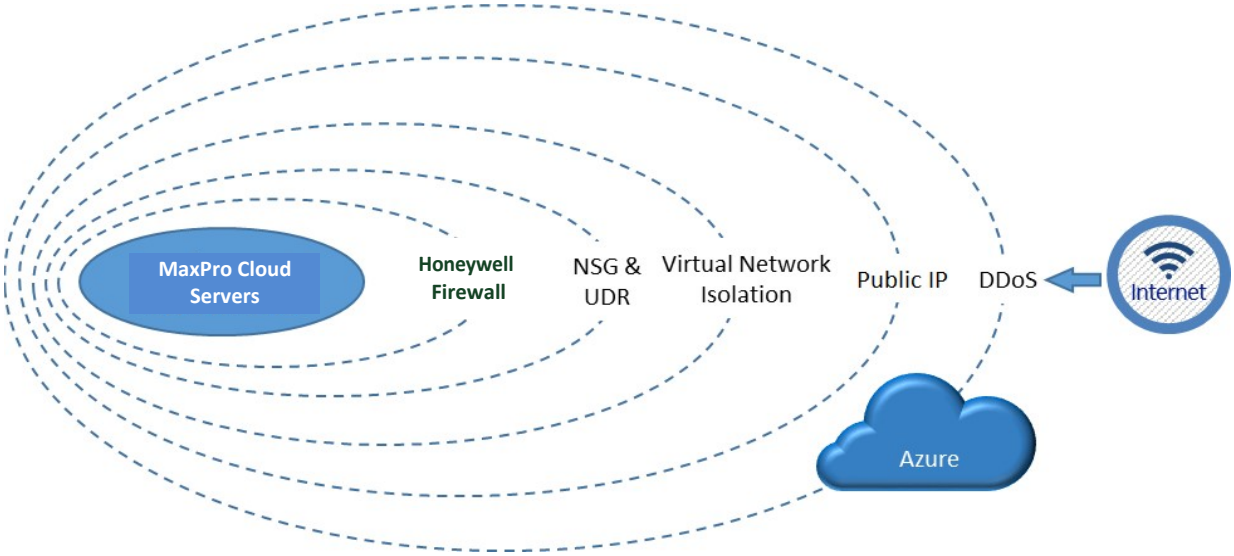
Akamai Global Traffic Management service is leveraged to accomplish this routing by using Geo specific IP intelligence.



Cyber Security

Firewall and IPS

Honeywell firewall deployed on Microsoft Azure extends security to the Azure cloud infrastructure and prevents network attacks and data breaches while enabling secure connectivity to Azure public cloud environments.



Honeywell Firewall also includes an Intrusion Prevention System (IPS) providing comprehensive network protection against malicious and unwanted network traffic including Malware attacks, Dos and DDoS attacks, Application and server vulnerabilities and Insider threats

Access Control to Servers

All the virtual machines are attached as member to a domain controller, local administrator accounts are disabled and not used for Remote Access.

Access to Azure Portal

All the subscriptions are configured with **Work Account** and integrated with Honeywell global Active Directory so that access can be granted only to users with valid Honeywell ID and password credentials.

Employees need to be on Honeywell Network or connect over VPN to authenticate to Azure Portal.

DMZ

Servers on Microsoft Azure cloud are deployed on a DMZ network protected against cyber-attacks using multiple levels of security.

WEB-SUBNET for Web tier servers that can only initiate connections to the app tier machines and can only accept connections from the Internet

APP-SUBNET for app tier servers that can only initiate connections with database tier and can only accept connections from the web tier

DB-SUBNET for database tier servers and cannot initiate connection with anything outside of their own subnet and can only accept connections from the app tier

Network Security Groups

Network Security Groups (NSGs) are simple stateful packet inspection devices that use the 5-tuple (the source IP, source port, destination IP, destination port, and layer 4 protocol) approach to create allow/deny rules for network traffic. You can allow or deny traffic to and from single IP address, to and from multiple IP addresses or even to and from entire subnets.

Using NSGs for network access control between subnets enables to put resources that belong to the same security zone or role in their own subnets. Four NSGs as described below are setup and assigned to the subnets to control traffic between them and the internet.

<ENV>-WEB-NSG

Inbound Security Rules

Priority	Name	Source	Destination	Protocol	Action
120	Allow-HTTPS	Internet	Any	HTTPS (TCP/443)	Allow

Outbound Security Rule

Priority	Name	Source	Destination	Protocol	Action
65501	AllowInternetOutBound	Any	Internet	Any	Allow

Azure Redis Cache Security

With the Premium tier, only clients within a specified network can access the Cache. Redis Cache will be deployed in a separate **CACHE-SUBNET** subnet in an Azure Virtual Network (VNet).

Server Security Hardening

Standard Honeywell cyber security policies are followed to harden the servers for maximum protection.

System Update Management

Update management is the process of controlling the deployment and maintenance of operating system and application server software and security updates into production environments. It helps to maintain operational efficiency, overcome security vulnerabilities, and maintain the stability of the production environment.

Updates to all servers are centrally managed by a dedicated update management service, all servers are ensured to be on the latest update and patch cycle.

Malware Protection

Microsoft Anti-malware security extension will be used to help identify and remove viruses, spyware or other malicious software. It provides real-time protection from the latest threats and also supports on-demand scheduled scanning.

More details at

https://azure.microsoft.com/en-in/documentation/articles/azure-security-antimalware/

SSL

All internet facing traffic from users and devices are over HTTPS protocol, SSL certificates are issued by a standard certificate issuing authority.

Multi Tenant Model

MAXPRO® Cloud system is designed to handle multi-tenancy, each tenant/customer's data is isolated and stored in the database/storage and remains invisible to other tenants, access to data is controlled by granular role based access control mechanisms.

Device to Cloud Security

All Intrusion devices uses Honeywell PKI infrastructure to manage certificates on the device and server, each device will be uniquely identified using the pre-installed certificate on the device during manufacturing time.

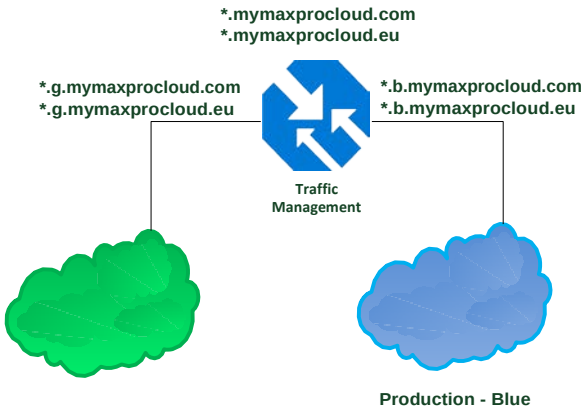
Azure Security Center

Azure Security Center helps to prevent, detect, and respond to threats, and provides increased visibility into, and control over, the security of Azure resources. It provides integrated security monitoring and policy management across Azure subscriptions, helps

detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

MAXPRO® Cloud Version Upgrade

- MAXPRO® Cloud follows Blue/Green Deployments to upgrade services
- **Two parallel production environments** referred as “blue” and “green”
- Only one of these environments is active and receiving production traffic at any one time
- When a new release is planned, it is deployed to the non-active environment
- Deployment of new build will be tested and certified without downtime to production
- After sanity testing of the new version, it can be released by routing the traffic
- **No down time** to route traffic to the new version
    - Always connected panels will disconnect and reconnect
- **Rollback to previous version is simple** with old environment still intact
- **Both environments** are considered production and will be **patched to latest Windows security updates**
- **Current active environment can be unambiguously identified** by referring the routing table



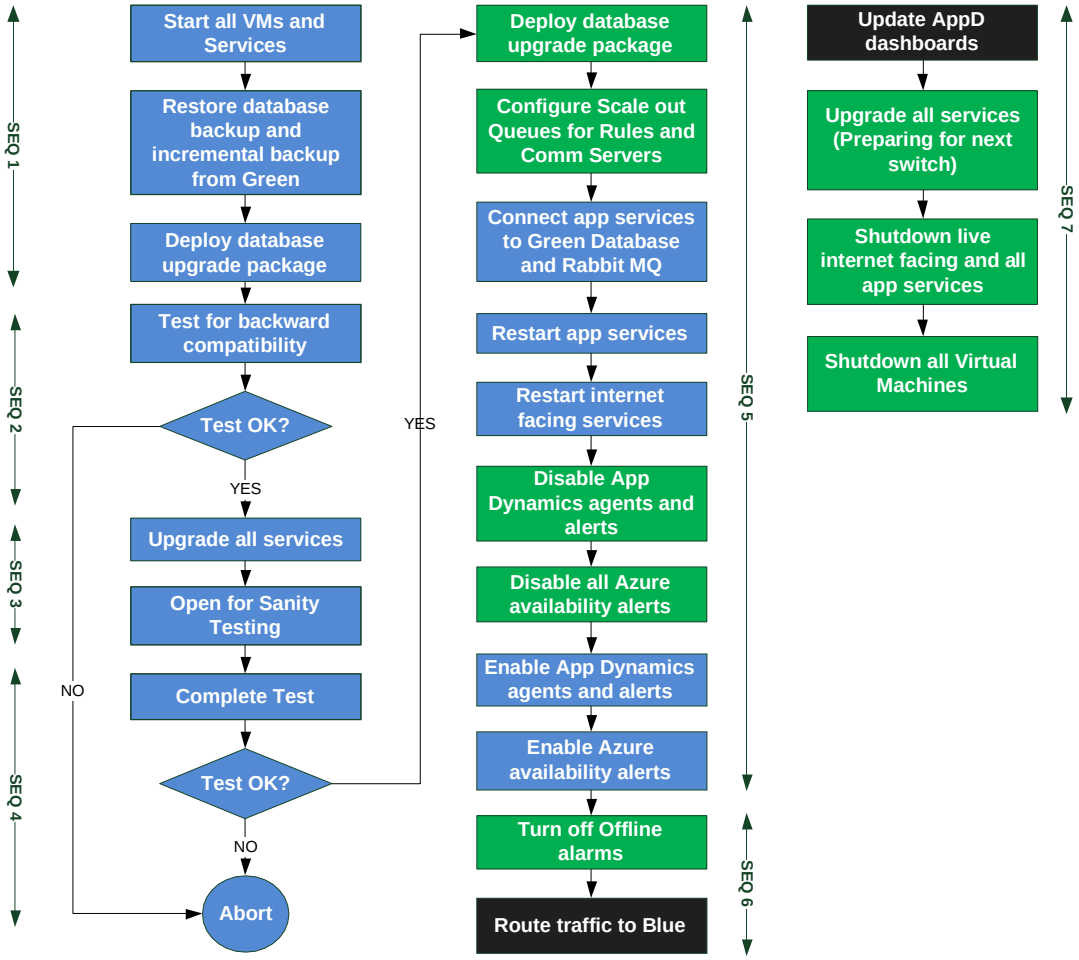
- **Two identical environments** under separate resource groups, all virtual machines will be tagged by their environment ID – “Blue” or Green” (Using Tags feature for a resource in Azure)
- Reference URLs
    - **Primary: maxprocloud.com**
    - **Blue: b.maxprocloud.com**

- **Green: g.maxprocloud.com**

- Both environments will be operational only during the upgrade window
- **Only one set** of SQL Database, Redis cache and Rabbit MQ
- **Separate instance of database**, Redis and Rabbit MQ will be available **to support backward compatibility and sanity testing**
- **Two separate** applications are created on App Dynamics
  - **G-Env** and **B-Env**
  - Agents from one environment will be active at any given time

Upgrade process

Following upgrade process shall be followed during a live upgrade, illustrated below is a scenario of switching traffic from Green to Blue instance.



- SEQ 6 is done during the upgrade window on the live system
- SEQ 1 to 4 are checkpoints to ensure the upgrade is stable

- Database upgrades will be done directly on live production database
- Dashboards and alerts configured on App Dynamics will be modified to reflect current active environment
- Entire workflow completed automated using **Octopus Deploy** tool

Traffic Routing and SSL Certificates

- **Fully Qualified Names** of blue or green environment are directly reachable and has proper SSL certificate binding
    - This enables a window to perform sanity testing of the new release

Multi-domain SAN certificates are created and servers are bound to both FQDNs using Server Name Identification capability on IIS 8.0 and on certificate stores for windows services

Backup & Disaster Recovery

Infrastructure Resiliency

All the above listed services remove single points of failure through redundancy and resilient design, two instances of these services are installed on separate virtual machines and traffic to them are routed through **Azure Load Balancers (web tier) and Internal Load Balancer (app and db tier)**.

Virtual Machines are also deployed in an **availability set**, this configuration ensures that during either a planned or unplanned maintenance event, at least one virtual machine will be available and meet the 99.95% Azure SLA.

Following are the Service Level Agreements (SLAs) for Azure services which MAXPRO® Cloud is primarily built on: Compute, Azure Storage

Azure Service	SLA	Potential minutes downtime/month
Compute	99.95%	21.6 minutes
Storage	99.90%	43.2 minutes

Recovery Point Objective (RPO)

Full backup of data is taken every 8 hours. Differential backup of data is taken ever xxx hours. There are two storage areas where critical data are stored in MAXPRO® Cloud platform.

Alarm, events, device, card and configuration data are stored in SQL Server. Video clip data is stored in Azure storage.

Backups will be stored on a different Azure region with **Read-access Globally Redundant Storage (RA-GRS) on a Cold access tier**

Instance	Primary Region	Backup Region	**Redundancy**
North America	West US	East US	RA-GRS
Europe	North Europe	West Europe	RA-GRS

Database Backup

Database backups are an essential part of business continuity and disaster recovery strategy because they protect your data from accidental corruption or deletion.

SQL Server Managed Backup to Microsoft Azure manages and automates SQL Server backups to Microsoft Azure Blob storage. The schedule for backups is designed keeping in mind production peak times and to ensure that customer experience is not impacted.

Following storage account will be used to store the backup, access to storage will be protected using SAS (Shared Access Signature).

Backup Storage Account	Region	**Retention Period**
mpcdbbkup **RA-GRS**	East US West Europe	30 days

More details on SQL Server Managed Backup to Microsoft Azure

https://msdn.microsoft.com/library/dn449496.aspx

Disaster Recovery

There are multiple disaster scenarios which need to be handled.

VM Data Corruption

In the event of a Virtual Machine failing or corruption, new VM will be provisioned using the Continuous Delivery toolsets.

1. Run Azure ARM template to provision the VM
2. Deploy MAXPRO® Cloud service using Octopus Deploy

Both these steps are completely automated and require just a manual trigger (push a button on a web page), the time taken to reinstall one VM and service is around 30 minutes.

Azure Outage within a Region

To provide redundancy two virtual machines are grouped in an availability set. This configuration ensures that during either a planned or unplanned maintenance event, at

least one virtual machine will be available. Each virtual machine in the availability set is assigned an update domain and a fault domain by the underlying Azure platform.

Fault domains define the group of virtual machines that share a common power source and network switch. By default, the virtual machines configured within an **availability set** are separated across up to three fault domains for resource manager deployments. While placing virtual machines into an availability set does not protect the application from operating system or application-specific failures, it does limit the impact of potential physical hardware failures, network outages, or power interruptions within an Azure datacenter.

Azure Region Outage

To avoid entire region outage a shadow instance of production will be setup on a different Azure DR region, this instance will not be active as all VMs will be in deallocated state. All future MAXPRO® Cloud service updates will be deployed to this DR region as well.

Purpose	Region	RTO
DR Site - Compute	East US, West Europe	Less than 2 hours
Data Backup Site	East US, West Europe	Less than 2 hours

East US is a paired region for the primary region (West US) used for MAXPRO® Cloud– North America and Latin America cloud instance.

West Europe is a paired region for the primary region (North Europe) used for MAXPRO® Cloud– Europe cloud instance.

Microsoft assures that in the event of a broad outage, recovery of one region is prioritized out of every pair.

More about Azure Paired Regions:

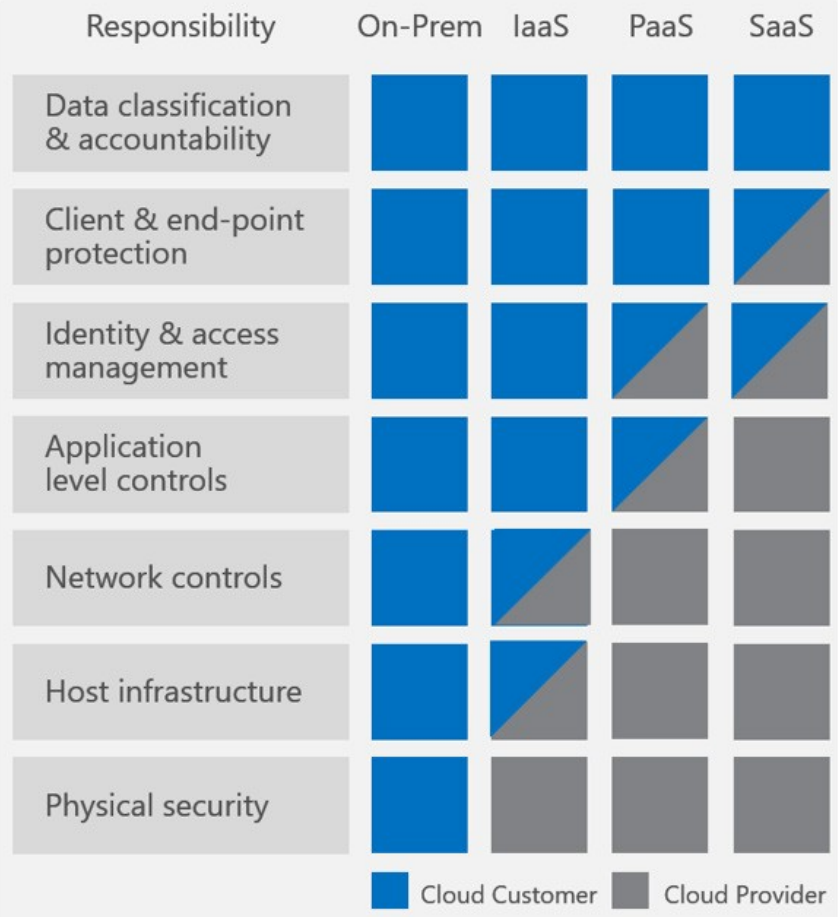
https://azure.microsoft.com/en-in/documentation/articles/best-practices-availability-paired-regions/

Below will be the series of steps required for bringing up a DR site.

1. Alert from Microsoft and CT team on Azure Region Outage
2. Start compute nodes on DR site
3. Restore database and video backup from Azure Storage account
4. Change routing on Akamai GTM to the DR site

Software Updates

The diagram below describes the responsibilities of Microsoft and Cloud Customer (Honeywell) for various deployment scenarios.



Below is the baseline configuration of MAXPRO® Cloud deployment on Azure:

Virtual Machine Names	Operating System	Other Software
Compute	Windows Server 2012 R2 Datacenter	.NET 4.6.1
Messaging	Cent OS 7.2	Rabbit MQ v3.6.5
Database	Windows Server 2012 R2 Datacenter	SQL Server Enterprise 2016 Enterprise
ADS	Windows Server 2012 R2 Datacenter	Active Directory Domain Services
CFSW	Windows Server 2012 R2 Datacenter	

WSUS	Windows Server 2012 R2 Datacenter	Windows Server Update Services

As explained in **Firewall and IPS**, all virtual machines are attached to a domain controller, with this, all the virtual machines can be configured simultaneously by including them in a Group Policy object (GPO), and then configuring that GPO with Windows Server Update Settings (WSUS). A new Group Policy object (GPO) is created that will contain only WSUS settings.

For maximum control over when servers are restarted as necessitated by an update installation, Group Policy has to be set to Download the updates automatically and notify when they are ready to be installed, and then manually accept and install the updates and then restart the VMs on demand.

Software Updates for MAXPRO® Cloud deployment on Azure can be broadly classified under these categories:

1. **Windows Server Critical Security Updates (includes IIS, .NET)**
2. **SQL Server Cumulative Updates**
3. **Service Packs**
    a. **Windows Server**
    b. **SQL Server**
4. **Third Party Software Updates**
    a. **Rabbit MQ**
    b. **Thinktecture Identity Server**

Windows Server Critical Security Updates

Microsoft releases security bulletins which contains critical security updates on second Tuesday of each month. Following shall be a process for managing critical security updates.

1. Connected Tech (CT) Team to monitor WSUS alerts on domain controller for critical security updates **(Second Tuesday of Every Month)**
2. Provide HSF engineering a consolidated set of critical updates
3. HSF engineering to validate security updates does not affect ISP functionality/performance on staging instance
4. CT team to update virtual machines (load balanced set) and ensure no down time

SQL Server Cumulative Updates

Update cycle for SQL Server follows a different schedule and which are announced on MSDN SQL Release Services blog.

Microsoft provides a RSS feed for these updates which can be subscribed at https://blogs.msdn.microsoft.com/sqlreleaseservices/

Following shall be a process for managing SQL Server updates.

1. CT Team to monitor SQL Server update announcement by subscribing to RSS feed **https://blogs.msdn.microsoft.com/sqlreleaseservices/feed/**
2. Provide HSF engineering a consolidated set of updates released for SQL Server
3. HSF engineering to validate updates does not affect ISP functionality/performance onstaging instance
4. CT team to update SQL Server and ensure no down time (Enabled by SQL Server Always On)

Service Packs

Service Packs for Windows Server and SQL Server are not released frequently and can be managed differently.

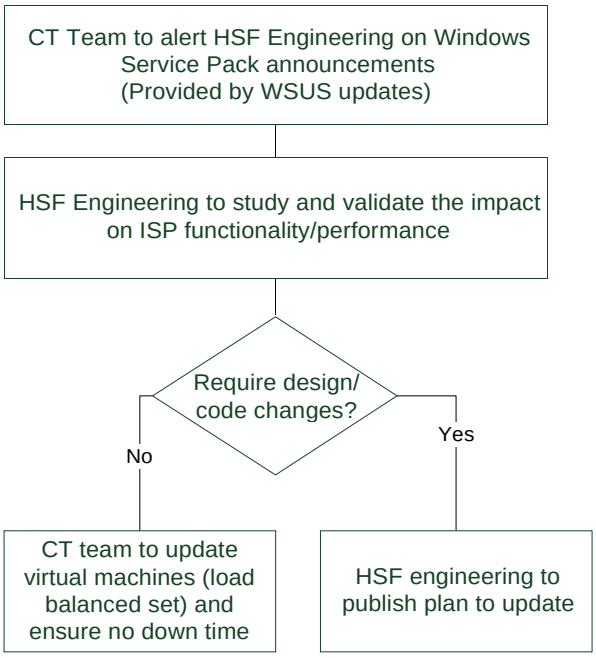
NOTE:

As a best practice it is advisable to be on the latest service pack levels.

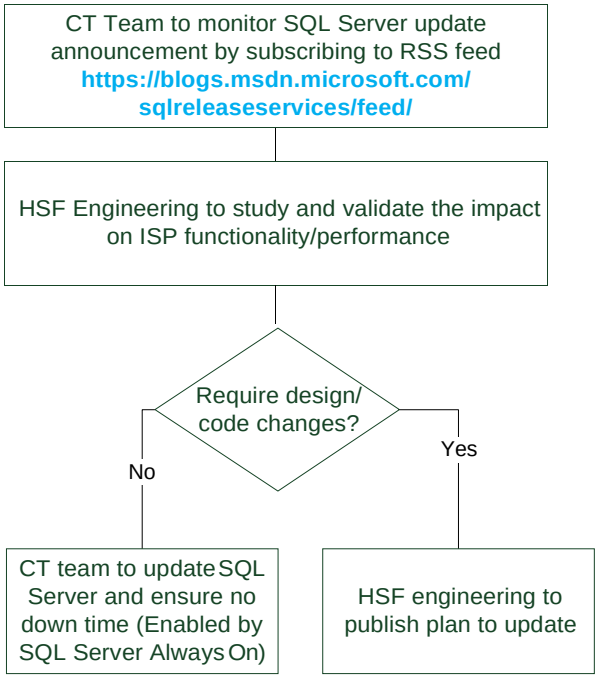
Support Lifecycle of each server product including service packs can be found at

https://support.microsoft.com/en-us/lifecycle/search?forceorigin=esmc

Windows Service Packs



SQL Server Service Packs



Third Party Software Updates

MAXPRO® Cloud leverages the following third party server software which will not be included in the Windows Server Update Services.

1. Thinktecture Identity Server - http://www.thinktecture.com/identityserver
2. Rabbit MQ - https://www.rabbitmq.com/

For both these software, Honeywell Engineering will plan for upgrades and share with Connected Tech team.

Infrastructure Monitoring

Server and Application Monitoring

App Dynamics is the standard monitoring solution deployed to monitor MAXPRO® Cloud application availability and performance.

Azure App Insights is leveraged to monitor Virtual Machine performance by deploying counters to monitor CPU, Memory and Disk performance.

Idera SQL Diagnostics Manager tool is used to monitor SQL Server database cluster availability, performance of queries and various other parameters.

Log Management

Azure OMS agent is installed on all VMs to aggregate windows, IIS and custom logs to central **Azure OMS dashboard** to search and create alerts.

Operations maintenance tasks

The CT team has a regular maintenance schedule that includes

- Monitoring schedule jobs in OLTP server and the data warehouse
- Regularly run smoke tests
- Regularly run reports on device connectivity

Backup & Disaster Recovery

Power Management

Multiple active power and cooling distribution paths, has redundant components, and is fault tolerant. Power availability is enabled by a facility wide uninterruptable power supply (UPS) and on-site generators. In the event of any local/regional blackouts or disaster, the datacenter would continue to provide uninterrupted power to systems for several days without refueling of the generators

Infrastructure Resiliency

All MAXPRO® Cloud services remove single points of failure through redundancy and resilient design, two instances of these services are installed on separate virtual machines and traffic to them are routed through **Azure Load Balancers (web tier) and Internal Load Balancer (app and db tier)**.

Virtual Machines are also deployed in an **availability set**, this configuration ensures that during either a planned or unplanned maintenance event, at least one virtual machine will be available and meet the 99.95% Azure SLA.

Following are the Service Level Agreements (SLAs) for Azure services which MAXPRO® Cloud is primarily built on: Compute, storage and cache

Azure Service	SLA
Compute	99.95%
Storage	99.99%
Cache	99.99%

Database Backup

Database backups are an essential part of business continuity and disaster recovery strategy because they protect data from accidental corruption or deletion.

Database backups are maintained at the backup datacenter with multiple replicas, this ensures data is never lost even if primary datacenter fails.

Video Backup

Video clips are stored on Azure storage and configured for Read Access Geo-redundant storage (RA-GRS), this enables to access backups anytime from secondary datacenter.

Disaster Recovery

Following disaster scenarios are handled in the architecture of the cloud.

Azure Datacenter Outage

To provide redundancy two or more virtual machines are grouped in an availability set. This configuration ensures that during either a planned or unplanned maintenance event, at least one virtual machine will be available. Each virtual machine in the availability set is assigned an update domain and a fault domain by the underlying Azure platform.

Fault domains define the group of virtual machines that share a common power source and network switch. By default, the virtual machines configured within an **availability set** are separated across up to three fault domains for resource manager deployments. While placing virtual machines into an availability set does not protect the application from operating system or application-specific failures, it does limit the impact of potential physical hardware failures, network outages, or power interruptions within an Azure datacenter.

Azure Region Outage

To avoid entire region outage a shadow instance of production will be setup on a different Azure DR region, this instance will not be active as all VMs will be in deallocated state.

Purpose	North America	Europe
DR Site - Compute	East US	West Europe
Data Backup Site	East US	West Europe

Microsoft assures that in the event of a broad outage, recovery of one region is prioritized out of every pair.

More about Azure Paired Regions:

https://azure.microsoft.com/en-in/documentation/articles/best-practices-availability-paired-regions/

Monitoring and Support

Monitoring Tools

Azure Diagnostics, App Dynamics and Idera are the standard monitoring solution deployed to monitor VM resources, application and database availability and monitor business transaction response times.

Application Support

In case of service degrade or infrastructure issue, monitoring tools trigger alerts to a dedicated support team for mitigation.

Application Support team are spread across United States and India to monitor and support the service 24x7 with well-established support models and escalation mechanisms.

Microsoft Azure Premier Support

MAXPRO® Cloud is under Azure Premier Support plan which ensures issues with any Azure cloud services are addressed on priority with initial response time of less than 15 minutes.

MAXPRO® Cloud support team raises tickets with Microsoft Azure support team with maximum severity (“A” – critical business impact) on issues which affects service availability.