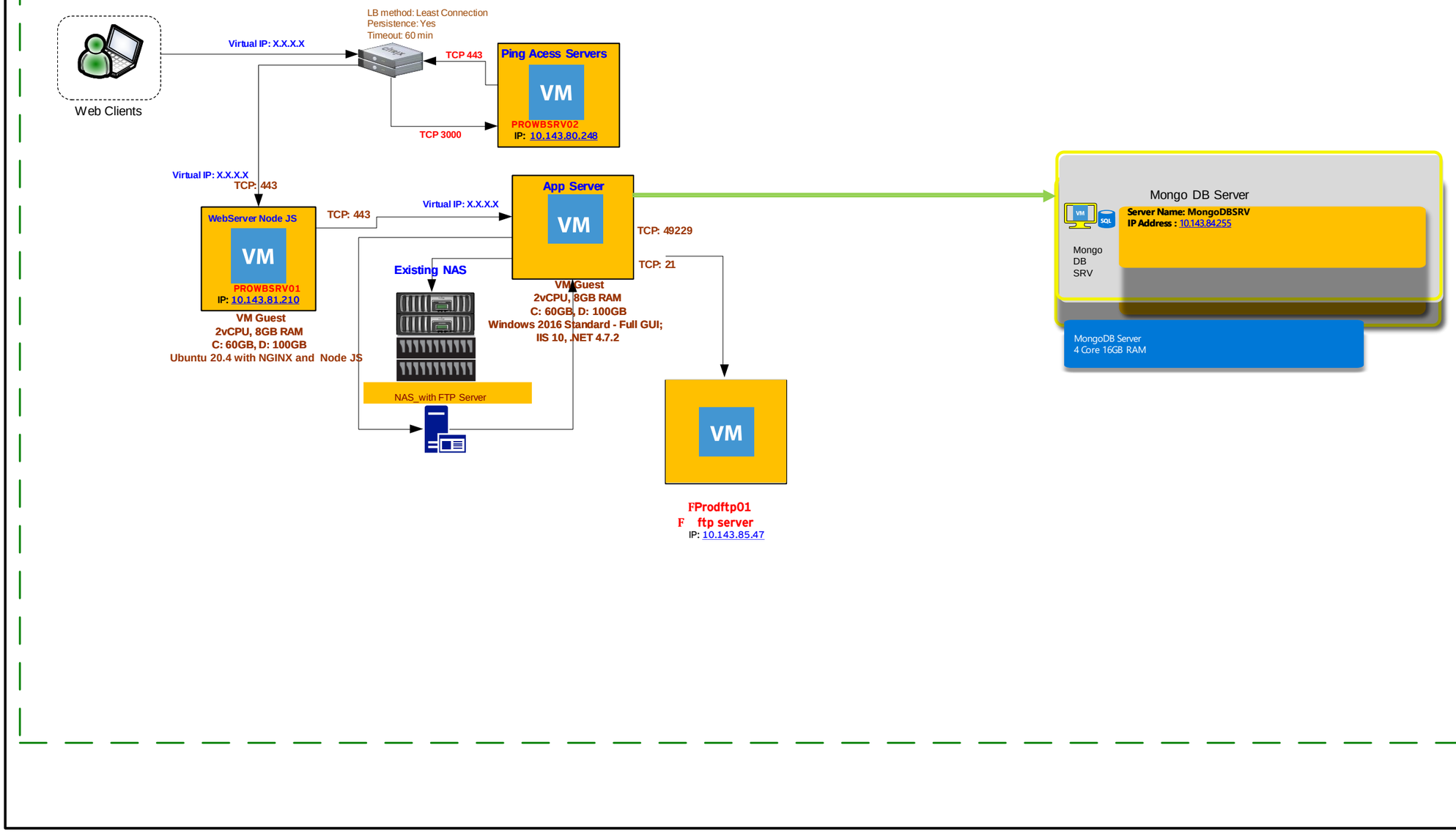
Production Environment



Title: US Production 1.0 Architecture

Azure

Internet

On-Premises

https://services.sentiademo.com
https://insights.sentiademo.com
Public Endpoint (Port 443)

PaaS: MongoDB Plan

MongoDB Server
Primary Server Name: sentiademomgdb0101.database.windows.net
Location: Central US
DB Names: Sentia_Audit_Logs , Sentia_Demo

Tier: Standard Elastic Pool, 400 eDTUs Size: 750 GB

Elastic Pool: sentiademomgdbpl01-pool(sentiademomgdbl01/sentiademomgdb01-pool)
Encryption: TDE Enabled

MongoDB Server - FailOver
Secondary Server Name: SENTIADEMO sentiademomgdb2.database.windows.net
Location: EAST US 2
DB Names: Sentia_AuditLog; SentiaDemo
Tier: Standard Elastic Pool, 400 eDTUs Size: 750 GB

Elastic Pool: sentiademo01-pool (sentiademomgdb01/sentiademomgdbl01-pool)
Encryption: TDE Enabled

Azure AD Federation

Azure MGDB Database

Recovery Services Vault
Vault Name: SENTIADEMORSV01
Location: Central US

Azure Key Vault
Key Vault Name: SENTIADEMOKV01
Location: Central US
Tier: Premium

Azure Key Vault
Key Vault Name: SENTIADEMOKV02
Location: EAST US 2
Tier: Standard

Vnet Location: Central US
Vnet Name: SENTIADEMOVNT01
Vnet Address Space: 10.48.18.0/24

Subnet Name: SENTIADEMOSBN02
Subnet Address Space: 10.48.18.32/28
NSG: SENTIADEMONSG01***

AGW - Web Application Firewall
Name: SENTIADEMOAG01
Tier: WAF V2 | Auto Scale 2-10 Instances
Dynamic IP mapped to DNS Label
sentiademoip01.centralus.cloudapp.azure.com
Multi-Site configuration enabled

Application Gateway

Traffic Manager
Primary
Secondary
Name: SENTIATRAFICMGR
Routing: Weighted
TTL: 60 mins
Probe Interval: 30
Failure Count: 3
Probe Timeout: 10

Internal Load Balancer
DR
ElasticSearch Cluster
Kibana

Users
External Users
Authentication

Ping Federate Servers
accessidp.sentiademo.com
10.143.176.87

DevOps
Authentication

App Service Plan

service certificate
Web App 01
Web App Name: DEMOSENTIAWAP01/3
Resource Group: SENTIADEMORSG01
Location: Central US
NODE Name: SENTIADEMO02
NODE Operating System: Linux
NODE Scale: 1 Instance | Manual
NODE Tier: S3 Standard | 50 GB
Application Insight: On

Web App 03
service certificate

Web App 02
service certificate
Web App Name: SENTIADEMOWAP02
Resource Group: SENTIADEMORSG01
Location: Central US
NODE Name: SENTIADEMO01
NODE Operating System: Linux
NODE Scale: 2 Instance | Auto
NODE Tier: S3 Standard | 50 GB
Application Insight: On
https://sentiademowap02.azurewebsites.net

PaaS Azure Monitor
Application Insight
Name: SENTIADEMOWAP01/2/3
Resource Group: SENTIADEMORSG01
Location: EAST US

Https 443

Storage Account
Purpose: Queue Storage
Name: sentiademo03
SKU: Standard_LRS
Replication: LRS
Endpoint:
Backup & Logs
Https 443

Storage Account
Purpose: Queue Storage
Name: sentiademostg02
SKU: Standard_GRS
Replication: GRS
Endpoint:
Queue Storage
Https 443

Storage Account
Purpose: Blob Storage
Name: sentiademostg01
SKU: Standard_GRS
Replication: GRS
Endpoint:
Blob Storage
Https 443

Integration Point

Virtual Network

EQUINIX COLOCATION

VNet Peer
ExpressRoute

Legend
New
Microsoft Azure
On-Premises

Title: US DEV 1.0 Architecture

Azure

Internet

On-Premises

https://services-dev.sentiademo.com
https://insights-dev.sentiademo.com
Public Endpoint (Port 443)

PaaS: MongoDB Plan

MongoDB Server
Primary Server Name: sentiademodevmgdb0101.database.windows.netdev
Location: Central US
DB Names: SentiaDev_Audit_Logs , Sentia_DemoDev

Tier: Standard Elastic Pool, 400 eDTUs Size: 750 GB

Elastic Pool: sentiademodevmgdbpl01-pool(sentiademomgdbl01/sentiademomgdb01-pool)
Encryption: TDE Enabled

MongoDB Server - FailOver
Secondary Server Name: SENTIADEMODEV sentiademodevmgdb2.database.windows.net
Location: EAST US 2
DB Names: SentiaDev_AuditLog; SentiaDemoDev
Tier: Standard Elastic Pool, 400 eDTUs Size: 750 GB

Elastic Pool: sentiademodevmgdb01-pool (sentiademodevmgdb01/sentiademodevmgdb01-pool)
Encryption: TDE Enabled

Azure AD Federation

Recovery Services Vault
Vault Name: SENTIADEMODEVRSV01
Location: Central US

Azure Key Vault
Key Vault Name: SENTIADEMODEVKV01
Location: Central US
Tier: Premium

Azure Key Vault
Key Vault Name: SENTIADEMODEVKV02
Location: EAST US 2
Tier: Standard

Vnet Location: Central US
Vnet Name: SENTIADEMODEVVNT01
Vnet Address Space: 10.48.18.0/24

Subnet Name: SENTIADEMODEVSBN02
Subnet Address Space: 10.48.18.32/28
NSG: SENTIADEMODEVNSG01***

AGW - Web Application Firewall
Name: SENTIADEMODEVAG01
Tier: WAF V2 | Auto Scale 2-10 Instances
Dynamic IP mapped to DNS Label
sentiademodevip01.centralus.cloudapp.azure.com
Multi-Site configuration enabled

Application Gateway

Traffic Manager
Primary
Secondary
Name: SENTIADEVTRAFICMGR
Routing: Weighted
TTL: 60 mins
Probe Interval: 30
Failure Count: 3
Probe Timeout: 10

Internal Load Balancer
DR
ElasticSearch Cluster
Kibana

Users
Authentication
External Users

Ping Federate Servers
accessidp.sentiademodev.com
10.143.176.87

DevOps
Authentication

Azure MGDB Database

App Service Plan

service certificate
Web App 01
Web App Name: DEMOSENTIADEVWAP01/3
Resource Group: SENTIADEMODEVRSG01
Location: Central US
NODE Name: SENTIADEMODEV02
NODE Operating System: Linux
NODE Scale: 1 Instance | Manual
NODE Tier: S3 Standard | 50 GB
Application Insight: On

Web App 03
service certificate

Web App 02
service certificate
Web App Name: SENTIADEMODEVWAP02
Resource Group: SENTIADEMODEVRSG01
Location: Central US
NODE Name: SENTIADEMODEV01
NODE Operating System: Linux
NODE Scale: 2 Instance | Auto
NODE Tier: S3 Standard | 50 GB
Application Insight: On
https://sentiademo-devdevwap02.azurewebsites.net

PaaS Azure Monitor
Application Insight
Name: SENTIADEMODEVWAP01/2/3
Resource Group: SENTIADEMORSG01
Location: EAST US

Https 443

Integration Point

Virtual Network

EQUINIX COLOCATION

VNet Peer
ExpressRoute

Storage Account
Purpose: Queue Storage
Name: sentiademodev03
SKU: Standard_LRS
Replication: LRS
Endpoint:
Backup & Logs
Https 443

Storage Account
Purpose: Queue Storage
Name: sentiademodevstg02
SKU: Standard_GRS
Replication: GRS
Endpoint:
Queue Storage
Https 443

Storage Account
Purpose: Blob Storage
Name: sentiademodevstg01
SKU: Standard_GRS
Replication: GRS
Endpoint:
Blob Storage
Https 443

Legend
New
Microsoft Azure
On-Premises

Title: US UAT 1.0 Architecture

Azure

Internet

On-Premises

https://services-uat.sentiademo.com
https://insights-uat.sentiademo.com
Public Endpoint (Port 443)

PaaS: MongoDB Plan

MongoDB Server
Primary Server Name: sentiademouatmgdb0101.database.windows.net
Location: Central US
DB Names: Sentiauat_Audit_Logs , Sentiauat_Demo

Tier: Standard Elastic Pool, 400 eDTUs Size: 750 GB

Elastic Pool: sentiademouatmgdbpl01-pool(sentiademouatmgdbl01/sentiademouatmgdb01-pool
Encryption: TDE Enabled

MongoDB Server - FailOver
Secondary Server Name: SENTIADEMOUAT sentiademouatmgdb2.database.windows.net
Location: EAST US 2
DB Names: Sentiauat_AuditLog; SentiaDemouat
Tier: Standard Elastic Pool, 400 eDTUs Size: 750 GB

Elastic Pool: sentiademouatmgdb01-pool (sentiademouatmgdb01/sentiademouatmgd01-pool

Azure AD Federation

Azure MGDB
Database

Recovery Services Vault
Vault Name: SENTIADEMOUATRSV01
Location: Central US

Azure Key Vault
Key Vault Name: SENTIADEMOUATKV01
Location: Central US
Tier: Premium

Azure Key Vault
Key Vault Name: SENTIADEMOUATKV0
Location: EAST US 2
Tier: Standard

Vnet Location: Central US
Vnet Name: SENTIADEMOUATVNT01
Vnet Address Space: 10.48.18.0/24

Subnet Name: SENTIADEMOUATSBN02
Subnet Address Space: 10.48.18.32/28
NSG: SENTIADEMOUATNSG01***

AGW - Web Application Firewall
Name: SENTIADEMOUATAG01
Tier: WAF V2 | Auto Scale 2-10 Instances
Dynamic IP mapped to DNS Label
sentiademouatip01.centralus.cloudapp.azure.com
Multi-Site configuration enabled

Application Gateway

Traffic Manager
Primary
Secondary
Name: SENTIATRAFICMGR
Routing: Weighted
TTL: 60 mins
Probe Interval: 30
Failure Count: 3
Probe Timeout: 10

Internal Load Balancer
DR
ElasticSearch Cluster
Kibana

Users
Authentication
External Users

Ping Federate Servers
accessidp.sentiademouat.com
10.143.176.87

DevOps
Authentication

App Service Plan

service certificate
Web App 01
Web App Name: DEMOSENTIAUATWAP01/3
Resource Group: SENTIADEMOUATRSG01
Location: Central US
NODE Name: SENTIADEMOUAT02
NODE Operating System: Linux
NODE Scale: 1 Instance | Manual
NODE Tier: S3 Standard | 50 GB
Application Insight: On

Web App 03
service certificate

Web App 02
service certificate
Web App Name: SENTIADEMOUATWAP02
Resource Group: SENTIADEMOUATRSG01
Location: Central US
NODE Name: SENTIADEMOUAT01
NODE Operating System: Linux
NODE Scale: 2 Instance | Auto
NODE Tier: S3 Standard | 50 GB
Application Insight: On
https://sentiademouatwap02.azurewebsites.net

PaaS Azure Monitor
Application Insight
Name: SENTIADEMOUATWAP01/2/3
Resource Group: SENTIADEMOUATRSG01
Location: EAST US

Https 443

Integration Point

Virtual Network

EQUINIX COLOCATION

VNet Peer
ExpressRoute

Storage Account
Purpose: Queue Storage
Name: sentiademouat03
SKU: Standard_LRS
Replication: LRS
Endpoint:
Backup & Logs
Https 443

Storage Account
Purpose: Queue Storage
Name: sentiademouatstg02
SKU: Standard_GRS
Replication: GRS
Endpoint:
Queue Storage
Https 443

Storage Account
Purpose: Blob Storage
Name: sentiademouatstg01
SKU: Standard_GRS
Replication: GRS
Endpoint:
Blob Storage
Https 443

Legend
New
Microsoft Azure
On-Premises

Architectural Desicions

From the architectural point of view this application count with the next design:

- Security:
- ✓ Integration with PING system for SSO and authentication login for users from different companies.
- ✓ Equinix Colocation with and Express route for integration between on prem and cloud infrastructure
- ✓ Implementation of and Azure Application Gateway WAF v2 for Intrusion detection and prevention and with Scale set for future grow.
- ✓ Deployment of a key vault to save in a secure way Passwords , Certificates SPNs and all the sensitive data.
- ✓ Azure AD federation to easy integrate the on-prem active directory with Azure AD.

-WebApps
- ✓ To solve the WebApp requests was deployed and Azure WebApp plan with and application gateway V2 to balance and scale up all the request that the app receive. The WEBAPPS nodes are based on NodeJs Version14 to afford all the webapps requests.
- ✓ 3 Webapps were created in this case 2 of the webapps will receive all the HTTPS request and the third WebApp will be for API request.
- ✓ All the webapps counts with its own Application Insight to control and troubleshooting all the problems that can appear in the operation of the webapps

- Log analytics and Alerts
- ✓ Was deployed and storage account to save all the logs and the analytics information for the deployment of all the system logs and the deployment of all the KPIs for reports.
- ✓ A SendGrid email system was deployed to email alerts for all the customers.
- ✓ Was deployed also and storage account to save all the blob storage and in this case that the information can be access over https in place of FTP.
- ✓ 3 storages accounts were created: One for save all the information from the application insights , another storage account for queue storage and the last one for logs and backups.

- MongoDB
- ✓ A MongoDB Paas was deployed to allocate all the no-schema data and noSQL , integrate all the large amounts of diverse data and JSON and BSON files.
- ✓ A MonDB Paas for failover was created to act as HA in case that the main database goes down or need maintenance or upgrades.

- Elastic search and Kibana
- ✓ And elastic search plan was deployed with and internal load balancer to balance the requests to the elastic search infrastructure and kibana dashboard for access to all the deployed dashboards.