TMA 02

Matt Mason: C6122243

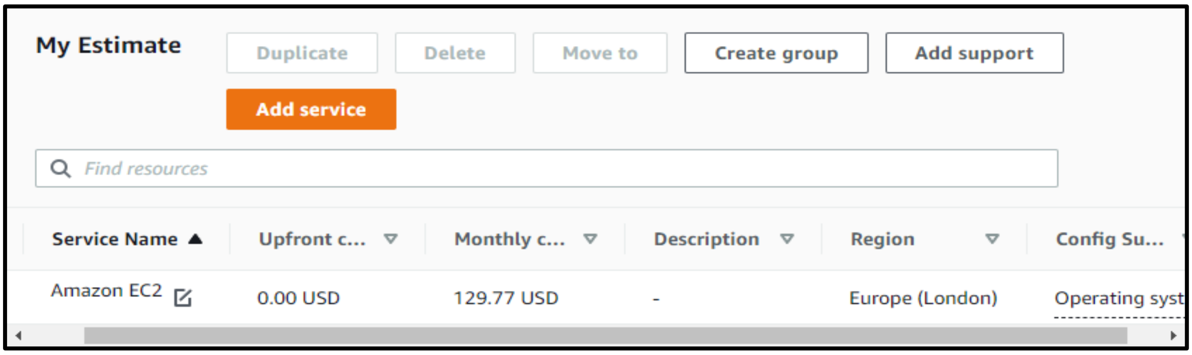
BSC (HONOURS) COMPUTING AND IT: TM-352

Table of Contents

Part 1: Benefits and risks

MegaMax can gain multiple benefits from using the cloud to host their sales team's application such as by converting capital expenditure into operational costs. Equipment, space and maintenance can be expensive, for example:

- Application Server (6 core CPU, 32GB RAM, 2x1TB HDD Raid1): £1877.54 (Dell, 2022)
- Database Server: £1896.03 (Dell, 2022)
- MySQL Enterprise Edition 1 year : £4273.04 (MySQL, 2022)
- Cisco FirePOWER 1010 ASA: £543.58 (Currys Business, 2022)
- Network Attached Storage (1.2TB): £3152.33 (Dell, 2022)



Service Name ▲	Upfront c... ▽	Monthly c... ▽	Description ▽	Region ▽	Config Su...
Amazon EC2	0.00 USD	129.77 USD	-	Europe (London)	Operating syst

Figure 1: Estimated cost of running AWS EC2

Other factors such as physical rack space, switches, internet access, power supply units, air conditioning, rent, employees, installation, configuration, redundancy, etc, all add to this cost. Cloud providers like Amazon Web Services (AWS), allow capital to be spent more efficiently through pay-per-use renting of resources. A single EC2 m5a.2xlarge instance consisting of 8 vCPUs and 32GB Memory is $129.77 per month on a 3-year reservation and the plethora of additional services available provide equivalency to their physical counterparts, which configured using AWS's well-architecture framework (AWS, 2022), can help with cost optimization.

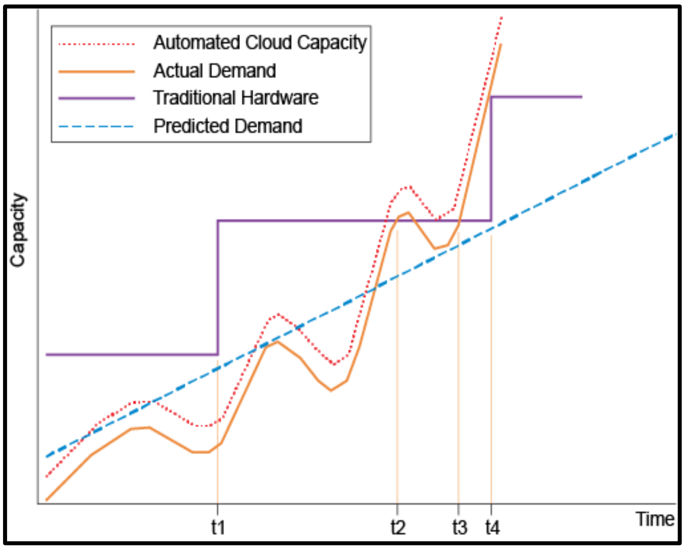


Figure 2: Comparison of demand and capacity for traditional and cloud deployments

Elasticity provides another benefit through the use of automatic horizontal scaling policies and resource health monitoring. These are used to meet increased demand by provisioning pre-configured instances and resources to start when server requests and traffic reach a specified threshold. Once the resources falls below a separate specified threshold, the instance is decommissioned. This provides optimal utilisation with no loss of requests and reduces costs by only paying for what resources are needed and used. Adding capacity in a traditional infrastructure can result in underutilisation and loss of service due to the time it takes to install and configure, whereas a new VM instance can be up and running within 5 minutes.

Cloud providers also deliver (Paradigm, 2023) benefits such as reliability and availability. AWS for example, can be classified as a tier 4 data centre (FS, 2022) with fault tolerance in the form of N+1 redundancy across multiple availability zones (AWS, 2022), and a 99.99% Service Level Agreements (SLAs) for resources such as their EC2 (AWS, 2022). This resilience along with the elasticity benefits will ensure that MegaMax staff and customers will always have access to the tools and services they require regardless of the amount of traffic imposed upon the system.

There are also risk factors that come with cloud adoption. One main concern for MegaMax is conducting financial transactions securely. Outsourcing the management of online transactions and other services is the first step to mitigating the risks. For example, Sage (Sage, 2022) will use Payment Card Industry (PCI), Data Security Standard (DSS) (PCI Security Standards Council, 2022) compliant, payment solutions providers such as PayPal, Stripe, and Visa Checkout (HostGator, 2022) to help keep transaction data secure and manage the whole process from merchant to the bank through payment gateway technology (emerchantpay, 2022). The only task MegaMax would need to manage is ensuring their website is secure by using HTTPS with proxy servers where necessary and TLS/SSL certification to be PCI DSS compliant. This means that all financial transactions would be secure and encrypted.

Another risk of the cloud is its multi-tenancy cloud infrastructure with the hypervisor being the only barrier between VMs, meaning there is no control where or who the host is shared with. One simple way to mitigate this is by using a dedicated reserved host. For example, AWS can provide a 48 Core/ 96 vCPU for £1851.85 per month on a 3 year reservation which can run up to 12 separate m5a.2xlarge instances. However, this may not be cost efficient for MegaMax's current purposes. Other more beneficial methods include creating VLANs for each tenant. This uses a unique ethernet packet header tag to direct traffic to each instance providing isolation and segregation of data of multiple tenants. Firewalls can also be used to screen packets and assure that VMs running on the same host can't gain privileged access to another.

MegaMax also needs to consider the risk of the privacy of its customers and staff's personal information being stored in the cloud and during transit. Cloud networks are accessible by anyone on the internet, therefor static data needs to be encrypted which can be done using symmetric keys. Using a single key for each tenant for decryption at scale is impractical so cloud provides offer a key management infrastructure that combines securely storing keys and authorising key usage. It means tenants don't have to write any additional code to manage these keys which requires considerable experience to ensure it would be fit for purpose. Before being used, storage media is sanitized to assure confidentially, and unauthorised disclosure of data isn't possible in accordance with the NIST publication 800-88. (NIST, 2014). Penetration testing consultants can also be employed to test the security of infrastructures to eliminate vulnerabilities and ensure legal and privacy compliance regulations are being met. These practices should enable MegaMax to be confident that data is secure in transit and at rest whilst also adhering to General Data Protection Regulations (GDRP) (EU, 2018) and Data Protection Act (DPA) principals (Parliament, 2018).

My recommendation for MegaMax would be to use a cloud infrastructure to launch and test its sales application. It provides cost savings, reliability, security, elasticity, automation and scaling based on demand. It also allows rapid delivery of new services and application updates without the need to download multiple software application versions to each device. Cloud provides can also guarantee continuous operations through SLAs, redundancy and assistance in a multitude of ways from documentation to solution consultancy. Maintenance of equipment is the responsibility of the provider which reduces operation costs and frees up IT resources, efficiency and developer hours.

The risks outlined above can be mitigated in a multitude of ways that allow each tenant a personalised level of security appropriate to their needs along with compliance, governance and services to ensure any specific requirements can be achieved together. I believe that the benefits far outweigh the risks and using the cloud would be the best course of action to take.

(1000 words)

Part 2: OpenStack and Autoscaling

a.

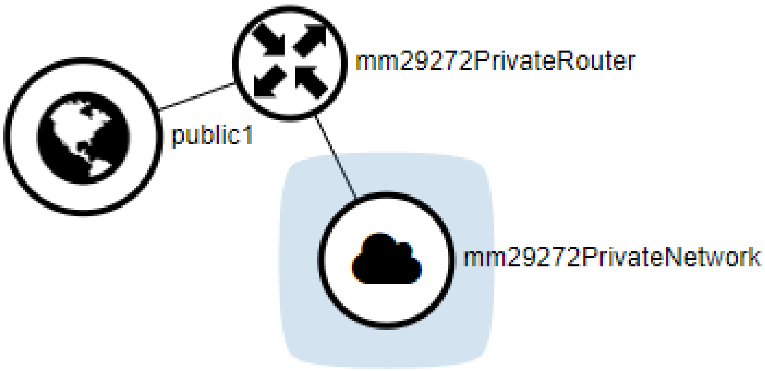
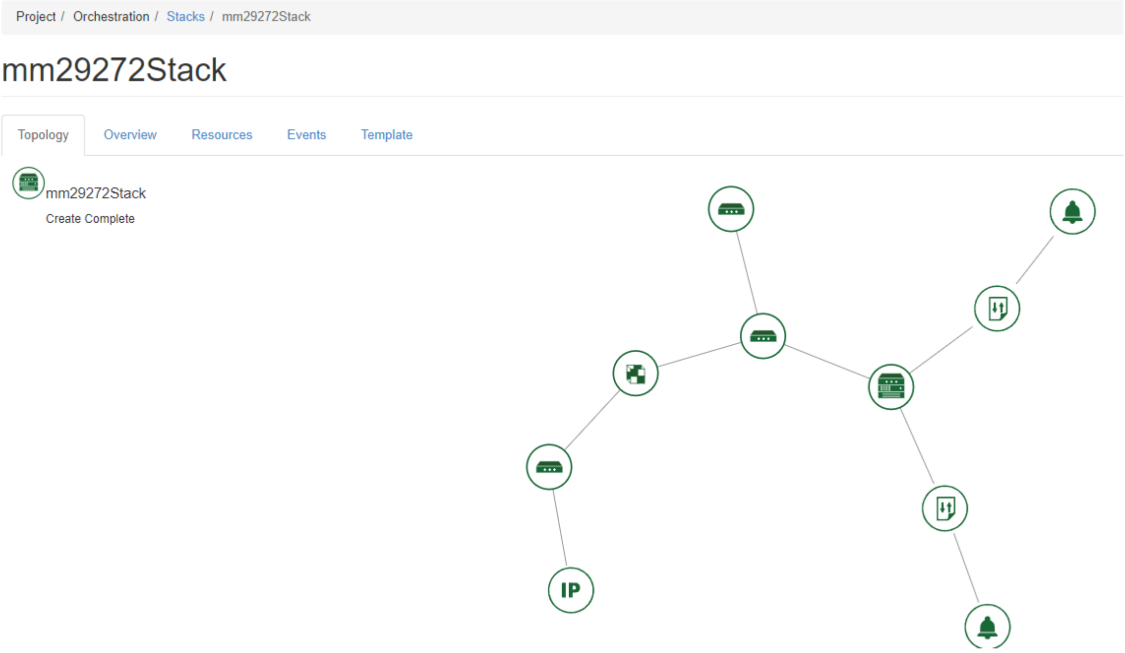


Figure 3:Basic Infrastructure Topology

b.



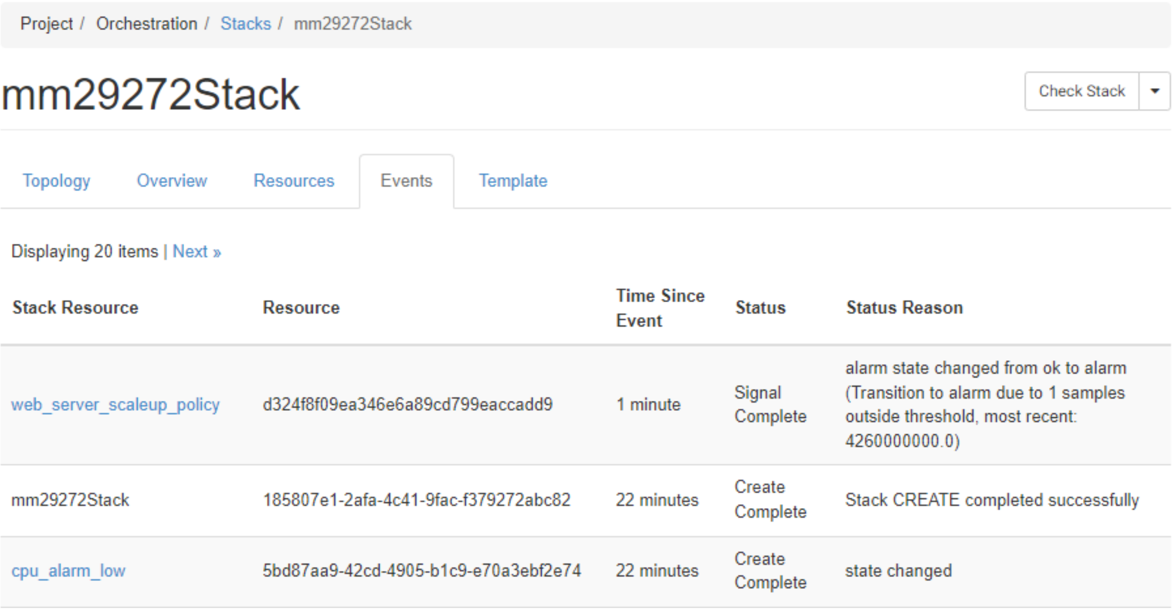
mm29272Stack

mm29272Stack

Create Complete

Figure 4: Stack Topology

c.



Project / Orchestration / Stacks / mm29272Stack

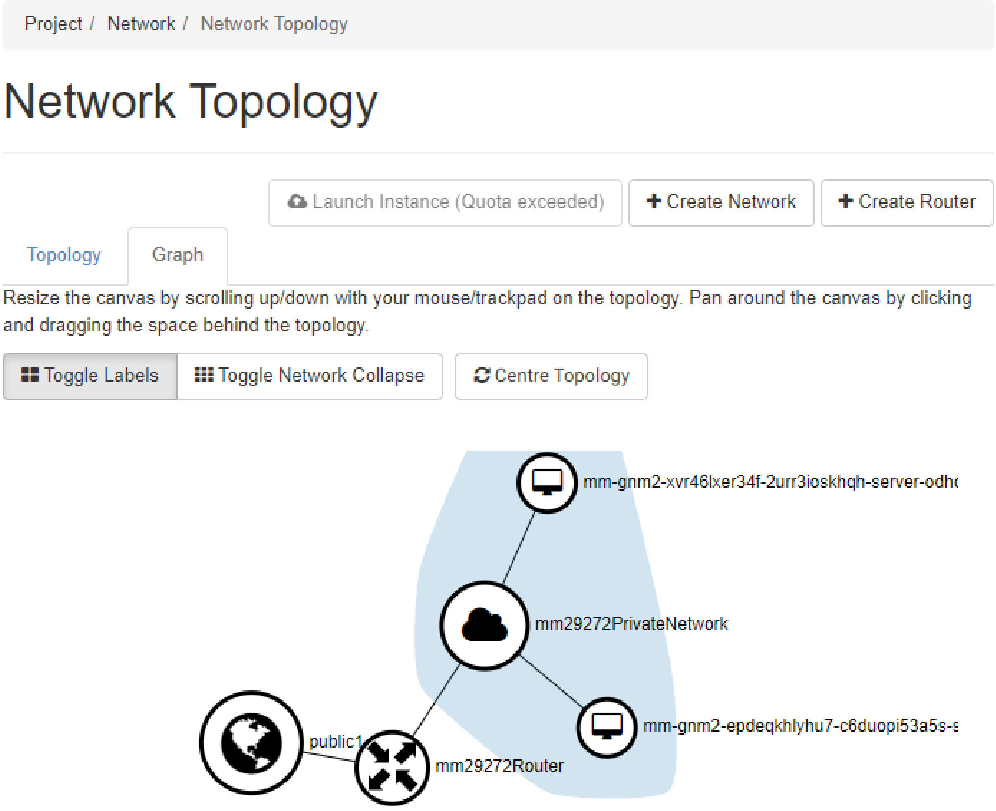
mm29272Stack

Displaying 20 items | Next »

Stack Resource	Resource	Time Since Event	Status	Status Reason
web_server_scaleup_policy	d324f8f09ea346e6a89cd799eaccadd9	1 minute	Signal Complete	alarm state changed from ok to alarm (Transition to alarm due to 1 samples outside threshold, most recent: 4260000000.0)
mm29272Stack	185807e1-2afa-4c41-9fac-f379272abc82	22 minutes	Create Complete	Stack CREATE completed successfully
cpu_alarm_low	5bd87aa9-42cd-4905-b1c9-e70a3ebf2e74	22 minutes	Create Complete	state changed

Figure 5:Stack Events List Scaling Up

d.

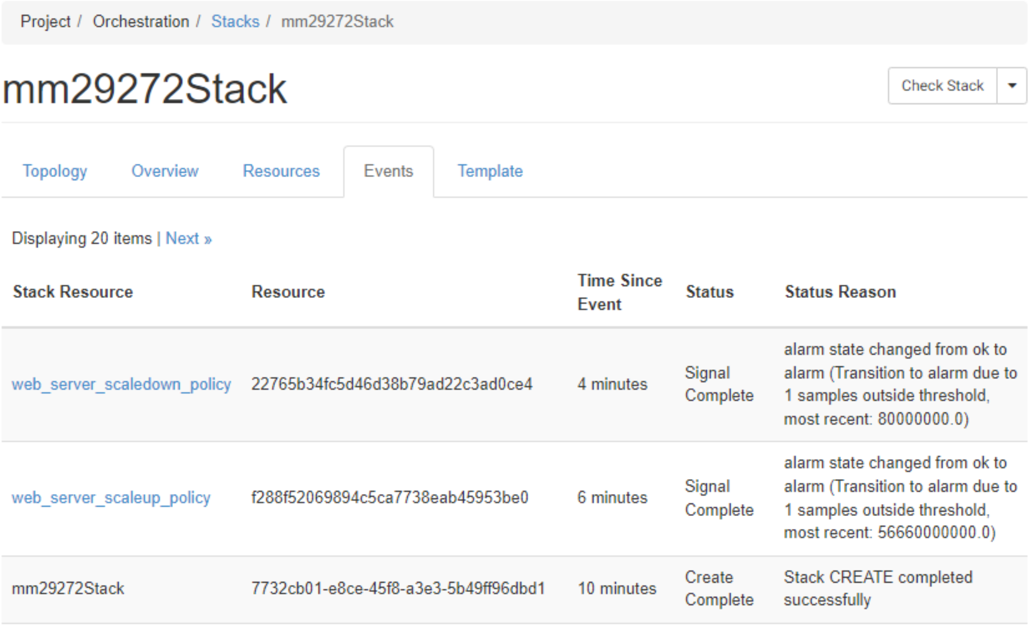


Project / Network / Network Topology

Network Topology

Resize the canvas by scrolling up/down with your mouse/trackpad on the topology. Pan around the canvas by clicking and dragging the space behind the topology.

e.



mm29272Stack

Displaying 20 items | Next »

Stack Resource	Resource	Time Since Event	Status	Status Reason
web_server_scaledown_policy	22765b34fc5d46d38b79ad22c3ad0ce4	4 minutes	Signal Complete	alarm state changed from ok to alarm (Transition to alarm due to 1 samples outside threshold, most recent: 80000000.0)
web_server_scaleup_policy	f288f52069894c5ca7738eab45953be0	6 minutes	Signal Complete	alarm state changed from ok to alarm (Transition to alarm due to 1 samples outside threshold, most recent: 56660000000.0)
mm29272Stack	7732cb01-e8ce-45f8-a3e3-5b49ff96dbd1	10 minutes	Create Complete	Stack CREATE completed successfully

Figure 6: Stack Events List Scaling Down

Part 3: AWS Cloud Solution

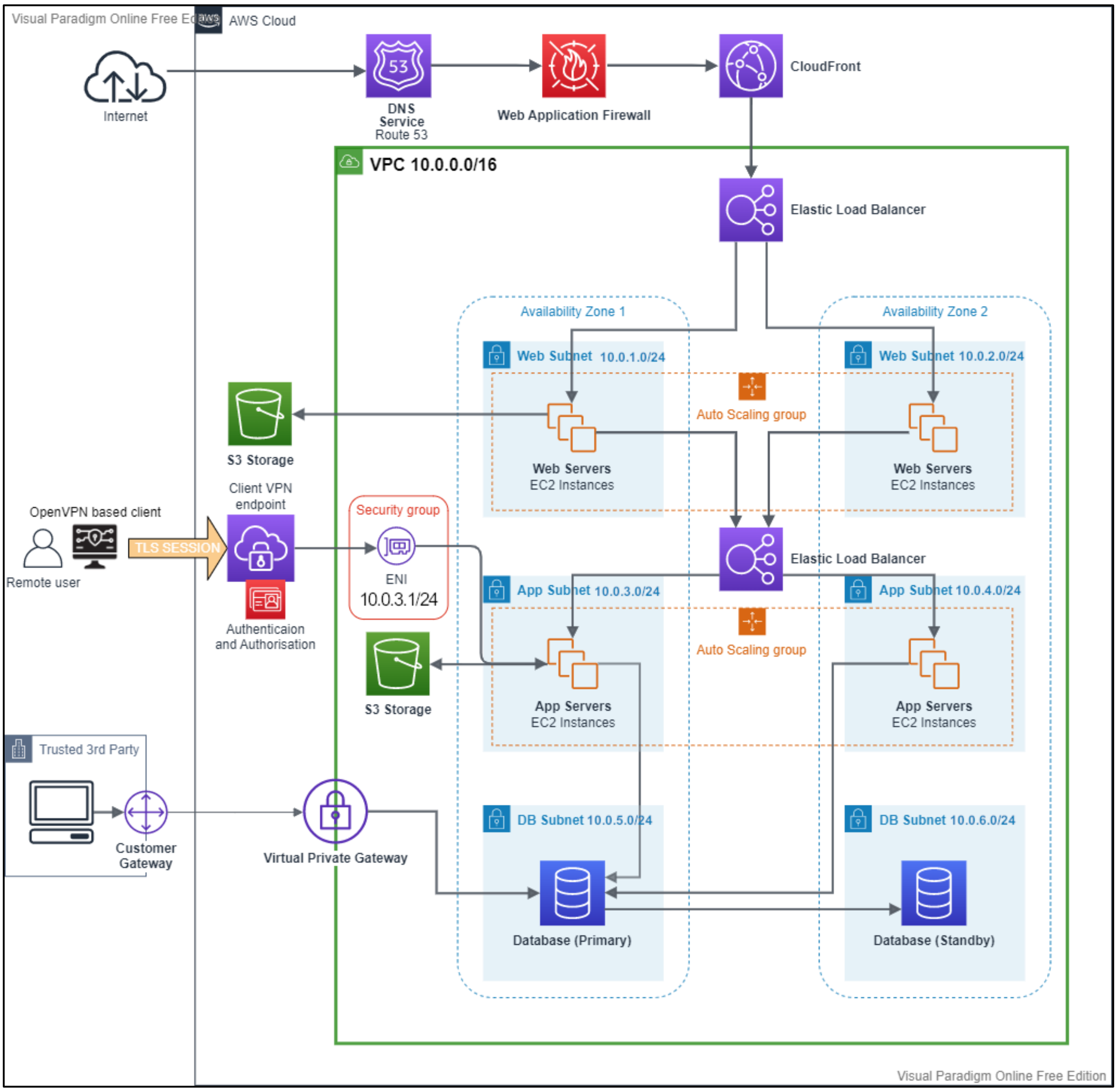


Figure 7: Cloud solution Architecture (AWS, 2022, p. Reference Architecture Examples and Best Practices), (Amazon, 2022, p. AWS Client VPN | Remote access VPN | Amazon Web Service (AWS)), (Amazon, 2010, p. Web Application Hosting in the AWS Cloud)

Figure 7 shows a potential cloud solution architecture for MegaMax's expanded and distributed infrastructure. A virtual private cloud splits the infrastructure into three separate subnets consisting of a website accessible to the public, the web app which has direct access for remote workers through the use of a secure encrypted client VPN, and the database subnet that trusted 3rd parties can use to access and process customs tax and commission. The infrastructure is distributed across multiple availability zones to provide redundancy in the case of any failings and to ensure the site and app remain accessible at all times. A copy of the database is also available in a separate availability zone to ensure transaction data remains current and correct.

The EC2 instances that form the the website and web application are part of their own auto scaling groups that span the various availability zones. This ensures that should traffic increase past a specific threshold, another instance can be initialised to prevent disruption to the service and meet demand, being terminated when no longer needed. This separation of website and web app, along with auto scaling policies should ensure that MegaMax's sales team have reliable access to the information they need and be able to place orders without any interference.

MegaMax remote sales staff can access the web app directly through the use of an open VPN based client to connect to an endpoint that uses a directory access protocol along with CA certificates to provide authorisation, authentication and encryption. The security group can be configured to ensure access is limited specific subnets or instances as required. A virtual private gateway is configured with a destination customer gateway and used to provide trusted 3rd parties with secure access to data that allows them to process tax and commission on sales for MegaMax's sales staff.

Elastic load balancers direct requests across each subnet of servers to ensure the most efficient use of the EC2 servers and distribution of traffic. Amazon Simple Storage Service (S3) is used by both the website and web app to store all data required by each to run and display correctly and can provide sales staff with contract templates and additional documents required for completing transactions with clients.

CloudFont is a content delivery service that can provide low-latency transfer of cached static and dynamic web content by leveraging AWS edge locations that reside closer to the geographical location of the request. This reduces traffic to servers and speeds us the responsiveness of the website. A Web Application Firewall provide protection against common web exploits and allows MegaMax to control what traffic is allowed to pass through to the network and Route 53 is a DNS service that provides translation and routing of human-readable websites into IP addresses connecting requests to the infrastructure running in AWS. (Amazon, 2022)

(468)

References

Amazon, 2010. *Web Application Hosting in the AWS Cloud.* [Online]
Available at: https://d0.awsstatic.com/whitepapers/aws-web-hosting-best-practices.pdf
[Accessed 06 01 2023].

Amazon, 2022. *AWS Client VPN | Remote access VPN | Amazon Web Service (AWS).* [Online]
Available at: https://aws.amazon.com/vpn/client-vpn/
[Accessed 06 01 2023].

Amazon, 2022. *AWS Documentation.* [Online]
Available at: https://docs.aws.amazon.com/index.html
[Accessed 06 01 2023].

Amazon, 2022. *Overview of Amazon Web Services - AWS Whitepaper.* [Online]
Available at: https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-overview/aws-overview.pdf#introduction
[Accessed 06 01 2023].

Amazon, 2022. *Traffic Encryption Options in AWS Direct Connect.* [Online]
Available at: https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/traffic-encryption-options-direct-connect-ra.pdf?did=wp_card&trk=wp_card
[Accessed 06 01 2023].

AWS, 2022. *Amazon Compute Service Level Agreement.* [Online]
Available at: https://aws.amazon.com/compute/sla/?did=sla_card&trk=sla_card
[Accessed 13 12 2022].

AWS, 2022. *Data Centers - Our Controls.* [Online]
Available at: https://aws.amazon.com/compliance/data-center/controls/
[Accessed 13 12 2022].

AWS, 2022. *Reference Architecture Examples and Best Practices.* [Online]
Available at: https://aws.amazon.com/architecture/?wasn_achp1&cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc&awsf.content-type=*all&awsf.methodology=*all&awsf.tech-category=*all&awsf.industries=*all
[Accessed 12 12 2022].

Currys Business, 2022. *Cisco FirePOWER 1010 ASA - firewall - Currys Business.* [Online]
Available at: https://business.currys.co.uk/catalogue/computing/servers-networking/networking/firewall-hardware/cisco-firepower-1010-asa-firewall/P292792P?cidp=Froogle&gclid=Cj0KCQiA1sucBhDgARIsAFoytUvTMepu5NS77smCdBxFOQy5gr35miAVANRK2g8OkPH8Y49eXjl1T08aAiDWEALw_wcB&gc
[Accessed 12 12 2022].

Dell, 2022. *Dell MD1420 DAS : DAS Enclosures & Storage | Dell UK.* [Online]
Available at: https://www.dell.com/en-uk/shop/cty/smart-selection-powervault-md1400/spd/storage-md1420/pvmd1400b
[Accessed 12 12 2022].

Dell, 2022. *PowerEdge R250 Rack Server | Dell UK.* [Online]
Available at: https://www.dell.com/en-uk/shop/dell-servers-storage-networking/smart-selection-

poweredge-r250-rack-server/spd/poweredge-r250/per2501a?configurationid=1267aa4b-b643-4564-a2c7-1784fca1cb91#features_section
[Accessed 12 12 2022].

Dell, 2022. *PowerEdge R350 Rack Server | Dell UK.* [Online]
Available at: https://www.dell.com/en-uk/shop/dell-servers-storage-networking/smart-selection-poweredge-r350-rack-server-easy-buy/spd/poweredge-r350/per35010s#features_section
[Accessed 12 12 2022].

emerchantpay, 2022. *What is a Payment Gateway and How Does it Work?.* [Online]
Available at: https://www.emerchantpay.com/insights/what-is-a-payment-gateway-and-how-does-it-work/
[Accessed 13 12 2022].

EU, 2018. *General Data Protection Regulation (GDPR) - Official Legal Text.* [Online]
Available at: https://gdpr-info.eu/
[Accessed 13 2022 2022].

FS, 2022. *What are Data Center Tiers | FS Community.* [Online]
Available at: https://community.fs.com/blog/what-are-data-center-tiers.html
[Accessed 13 12 2022].

HostGator, 2022. *Top 10 Online Payment Methods for eCommerce Sites | HostGator.* [Online]
Available at: https://www.hostgator.com/blog/online-payment-methods-ecommerce/
[Accessed 13 12 2022].

MySQL, 2022. *Product Details - MySQL Enterprise Edition Supscription.* [Online]
Available at:
https://shop.oracle.com/apex/f?p=DSTORE:PRODUCT::::RP,6:P6_LPI,P6_PROD_HIER_ID:60720318189220530576677,58095029061520477171389
[Accessed 12 12 2022].

NIST, 2014. *Guidelines for Media Sanitization.* [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
[Accessed 13 12 2020].

Paradigm, V., 2023. *Visual Paradigm.* [Online]
Available at: https://online.visual-paradigm.com/app/diagrams/#diagram:proj=0&type=AWSDiagram&width=11&height=8.5&unit=inch
[Accessed 06 01 2023].

Parliament, U., 2018. *Data Protection Act 2018.* [Online]
Available at: https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/crossheading/the-data-protection-principles/enacted
[Accessed 13 12 2022].

PCI Security Standards Council, 2022. *PCI_DSS-QRG-v4_0.pdf.* [Online]
Available at: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf
[Accessed 13 12 2022].

Sage, 2022. *Accept Card Payments | Take Payments Online | Sage UK.* [Online]
Available at: https://www.sage.com/en-gb/integrated-payment-solutions/accept-online-payments/
[Accessed 13 12 2022].