Session: 202130

Charles Sturt University

Cloud Computing

Assessment No.2

Business requirements report

Case study

Due date: 04/04/2021

Submitted by:

Johan Sebastian Ramirez Vallejo

11736865

TABLE OF CONTENTS

Table List

Figures List

1. Migration to the cloud

1.1 Issues DR Alarms

DR Alarms is a company that provides security services and products to home and commercial and recently develop monitoring devices related to IoT. The company tent to increase his presence internationally and they had large contracts with government and industry which is advisable to treat sensitive data appropriately.

To make the study we need to know deeply the DC to provide a cloud solution. therefore, this study resulted in a series of issues that are solved with the migration to cloud depending on the configuration that will be proposed. The issues found are related to **computing**, **storage and networking** which concern **High availability (redundancy)**, **security**, **operation** and **management** that are necessary for business continuity.

1.1.1 Computing

The issues related in the table below comprehend the mayor issues in computing. Cloud-based solutions can manage key manufacturing points, IT resources costs, application lifecycle management and version control, application monitoring and maintenance, and patch management. The solution can support faster adoption of new products and technologies(Attaran & Woods, 2018). For instance, DR Alarms is developing IoT monitor device that can be integrated as a part of cloud solution showing in the diagram cloud edge solution.

Actual Issues	Report issue	Implications	Solution if move Cloud
Application Servers	Constantly hacking - No updates - No maintenance - No customized - No monitoring - No server monitoring system	Constantly cyber attacks Crash any time Performance Mayor Cost Reliability	Application hosted online **(Cloud Service)** **Advantages -** Reliable, scalable, infrastructure on demand, Secure compute for your applications, Flexible options to optimize cost, Easy to migrate and build apps, Building Blocks. **Disadvantages -** No longer in control, No get all features, Risk data confidentially, Dependency of internet connection, Level security
Patching and update policy	no procedures acquiring, testing, and installing multiple patches of software or existing application	cost/security/reliability - resources can crash any time, and take certain time to replace or repair	Service automatically in the cloud **Advantages -** no maintenance for users **Disadvantage -** user should scan for vulnerabilities and missing patches, Hybrid environments required solution for partching
Security procedures	everyone know the passwords servers, personal accounts, and also all users have accounts on the email, database sql, and database servers./ No procedures after hack:	cost security reliability	In the process to move the serevices to the cloud, also required by part of the management increase secure procedures inside of organizationde due the governance of the services. The boundaries between client and provider have to clear during migration plan
Services offered by servers	Accesible from internet	cost security reliability	De best practice to is use proxy server, a firewall and if is required access remotely use a VPN, when the services are moving to the cloud the services will be accessible from internet. Control access management will be required to control employees access- **Advantages** - It can be controlled and reduce the risk. **Disadvantages** - security
Antivirus	It not updated recently/ basic	cost security reliability	Requirered Antivirus on-premises and a cloud-based antivirus **Advantages -** Agentless Scanning, Network Traffic Scanning, Lightweight Agents, Cloud-based Analysis. It is protection that proveedor include in their services
Email virus protection	No overal protection	cost security reliability	**Email security gatway:** all inbound and outbound email traffic to protect organizations from email-borne threats and data leaks.-**Advantages -** Encryptation. identity protectection, control sensitive data, andblock if required - **Disadvantages -** extra layer for data transport.
workstations	vanilla installs, no maintenance/ win7ent/ no back up home directory/Administrations privilages/ Environment relaxed (employes share passwords)/no hard and fast rules about passwords/No procedure for repairs and upgrades, or shops regarding to security	cost/security/reliability - resources can crash any time, and take certain time to replace or repair	Desktop-as-a-Service **(DaaS)** solution **Advantages -** Accessible any ware same environment, Data is protected, No need VPN, Centralized process. **Disadvantages -** Hight internet connection - device dependency, Single Point of Failure.
MacBook	unprotected, from virus	it can spread a virus into the organizations	
No contract maintenance	Resources with basics and 5 years old	cost/security/reliability - resources can crash any time, and take certain time to replace or repair	When the services are moving to the cloud, the control by users is reduced but the user have to take care his own resources.
System administrator	It is no constantly monitoring the systems/ Storage fill up regularly Active accounts from people who does not work anymore for the company (unused accounts) no Network monitoring systems/ Not server security system:	cost security reliability	The sysadmin will required traininng to support on-premises resourses and cloud services to optima operation. Advantages: improve skills, optimazin workflow - Disadvantages- learning curve.

Table 1. Computing issues and cloud solution

1.1.2 Network

Cloud computing assumes that each software application or system component becomes a service or part of a service (Attaran & Woods, 2018). Therefore, the architecture must be changed to be compatible with the cloud. The DR Alarms has a poor internal architecture that requires major structural adjustments. Security depends on the user and provider. Thus, the company has poor security policies and procedures that requires to increase the data protection philosophy(Diez & SIlva, 2013). It is predictable that people will resist change, bad behavior within companies requires a high level of control which need to be led by directors to face resistance within the DR Alarms.

Actual Issues	Report issue	Implications	Solution if move Cloud
Power supply	No redundancy	Shut down any time, the services will not available	**Public Model** - All the infrastructure is managed for provider . **Advantages -** No investing in infrastructure, no required maintenance for part of user due the provider supply this , highly redundancy, secure, fail over, running high-end redundant computer network, solid and data protection, network monitoring 24/7, Antivirus, Automatic back up. **Disadvantages -** out control of user, unexpected cost, security risk, limit customization, broadband dependency, availability, SLAs required deeply knowledge.
Network	No redundancy/	risk of failure along the critical data path.	
Procedures for network	No procedures/Servers are on the same networks as user workstations	Latency/lost data its no the best practice	
Public network	Employees can access outside	cost security reliability	
network security	no policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible	cost security reliability	
No firewall	Constantly hacking	Constantly cyber attacks	

Table 2. Network issues and cloud solution

1.1.3 Storage

Storage data is not just kept information. It is required a strategy to keep it safe and available. The redundancy and procedures for a regularly backed up to restore information in any case of lost, going through strategies to keep the data reliable it the best practice. Therefore, these strategies can be kept in a hybrid cloud environment.

Data protection tops the list of concerns of many manufacturers when they consider cloud-based solutions. Multi-tenant environments could share data from competitors for that reason is important the data integrity from source. Dr Alarms for being a company that manufactures security devices should be concerned about data security, since it also has contracts with state companies(Diez & SIlva, 2013).

Actual Issues	Report issue	Implications	Solution if move Cloud
Disk server configuration	no redundancy or fail over configuration	Constantly cyber attacks security crash any time Performance Cost Reliability can lost the information at any time	Application hosted online **(Cloud Service)** **Advantages -** Reliable, scalable, infrastructure on demand, Secure compute for your applications, Flexible options to optimize cost, Backup and Disaster Recovery, Building Blocks Syncing and Updating, Security. **Disadvantages -** No longer in control, No get all features, Risk data confidentially, Dependency of internet connection, Level security.
Backup and Disaster Recovery	Does not exist/ there is not any procedure/ the actual procedure it is not correct, and the company is in highly risk	Impossible to recovery data	
Data integrity	the data stored It is not, overall accuracy, completeness, and consistency data	Security of data it is no reliable when is transfer or reproduced	

Table 3. Storage issues and cloud solution

The cloud environment presents new challenges in securing data, mixed trust levels, and the potential weakening of the separation of duties and data governance (Diez & SIlva, 2013). Hence, with the hybrid cloud there are challenges of protecting data as it moves back and forth from the enterprise to a public cloud. The solution of a hybrid cloud is the most convenient to adopt, taking in account that we can use part of infrastructure already build and strengthen the availability, security operation and management to provide an integral solution.

Small business are tending to move to a cloud 78% of small businesses were fully adopt cloud computing by 2020(Flexera, 2020), according to security 82% of SMBs report reduced costs as a result of adopting cloud technology. 70% are reinvesting the saved money back into their business. 58% of cyber-attacks target small businesses. Cloud storage services offer a solution.(Verizon, 2020). And then there is a considerable growth of 21% by IoT(Flexera, 2020) which definitely indicates that the adoption of the cloud is a good path for the new development of the DR Alarms.

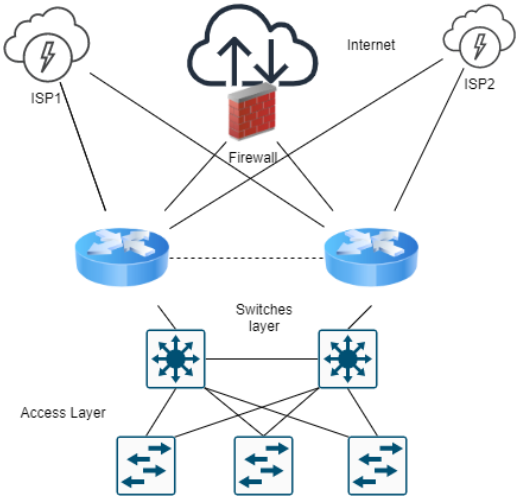
2. Possible cloud Architecture

The company currently has 42 employees, 25 of whom are in the manufacturing plant and 17 in the administrative offices. It is established that each employee requires a computer for different uses and applications. In order to reach a possible architecture, it is determined to develop a migration to cloud divided into two stages, considering the problems that the company faces with its IT infrastructure(NIST, 2013). The first stage is to develop the basic parameters in the client's infrastructure to ensure a continuous, reliable, and secure internet connection. In a second stage, the cloud architecture will be proposed considering the sensitivity of the data that the company manages.

2.1 Stage one on-premises DC

2.1.1 Network

According to the analysis of the issues that are facing the company we should solve network problems on - premises to ensure a connection secure and continual. First, it is suggested the connection should be connected through two ISPs to two routers connected in redundancy with a firewall to protect the data from the internet (Erl et al., 2013) .This is to make it to assure the constant connection to the internet and to the services that it would have in the cloud securely and constant.



2.1.2 Computation

Independently of the solution that the client chooses there is a certain responsibility by part of the client to maintenance their servers and desktops, although the solution reduces the maintenance and manage it is still required. It is highly recommended because the solution will focus on sensitive data storage on premises. Therefore, it is required that the client meeting certain parameters such as updating, patching, maintenance between others.

2.1.3 Security

The most important to DR Alarms is its sensitive data. So, it is recommended to isolate the data centre and apply security protocols and polices. Provide training to sysadmin and employees about the cloud and security because it has been evidenced that most cases of hacking are the fault of the users. In addition, it was also found that in the data centre there is no proxy server and no antivirus which it is recommended that it be installed and established.

2.2 Stage two Suggested cloud architecture

The architecture that considers the services provided by Amazon provides the solution of several problems in the company.

2.2.1 Architecture

The deployment model represented is a hybrid cloud and the delivery SaaS where services are migrated to the cloud and the sensitive data holds on-premises(NIST, 2013). The system architecture is structured to handle various disaster recovery scenarios, as a result, they can be recovery quickly in comparison to the actual structure.

The proposed solution covers critical segments in the business continuity in DR Alarms as the availability, security, operation, and management. Therefore, the architecture that considers the services provided by Amazon provides the solution of several problems in the company.

2.2.2 Features according to DR Alarms structure business aims.

It is considered to keep the most sensitive information in the client's infrastructure, regularly providing backups in the cloud, and making the information redundant. As a result, making them highly accessible and fail over with the ability of disaster recovery. So, regarding data security when travelling to AWS (Amazon Web Services, 2021b)is done with a security connection VPN gateway which encrypt the data that also can be used to access remotely with another figure called (client VPN) by an employee. To support the traffic, we use an IPsec VPN which use two tunnels to transfer data avoiding congestion, and a router on site CGW (client gateway) to control the data exit(Diez & SIlva, 2013).

It is suggested to be studied the option which is Aws direct connect (Amazon Web Services, 2020) that can vary in cost and geographical location. The company is located 3 hours from Sydney which can be considered a more secure connection. The tunnel that the VPN creates is still through the internet, so in terms of security there is still a risk.

The storage that is in VPC is in a private subnet which make a replica in on demand scalable instances to be ready to supply data when this zone become available. Finally, this data is sent through to VPC endpoint service to make secure the data exit and store them in Amazon Simple Storage Service (AWS S3)(Amazon Web Services, 2020).

VPC end point is important because If we do not have this service, we probably expose the data due to that we should send it through the NAT, which prevent the internet from initiating a connection with those instances, helping instances in private subnet be safe.

This architecture allows scaling resources controlled by a load balancer which support uses redundant deployments of cloud service implementation. The load balancer allows us to balance the load between both zones A, B. as a result, the architecture allow scale out and in, depending on the demand of the services(Amazon Web Services, 2020). Therefore, once the load balancer understands the level of workload, an automated provisioning program assembled and configured provides a rapid provisioning.

Considering the potential growth of the company towards international and local clients, and other products such as newer devices of monitoring, a cloud solution would provide considerable support for the expansion of the company. As the company is currently in this growth phase, a burst out cloud pattern established can be supplied to be triggered when it meets the established demand conditions with the advantage of cost reduction, operation, and administration.

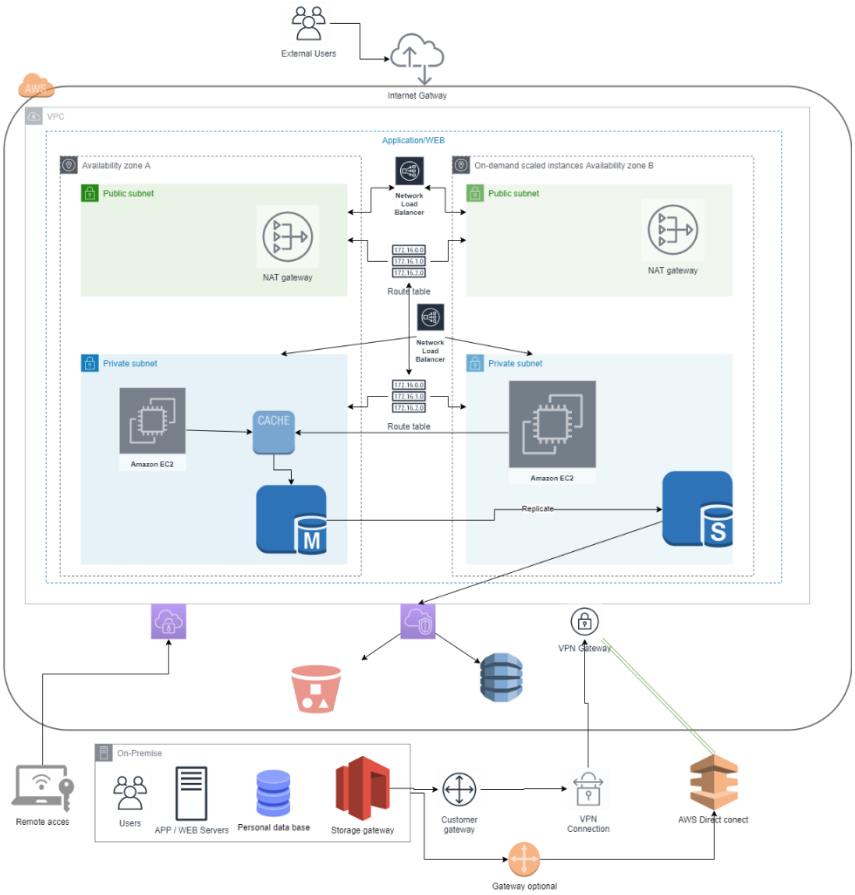


Figure 1. Suggested architecture Dr Alarms'

2.2.3 Advantages

- **Availability**: With elastic load balancing across different availability zones assure the continuity of the service where is hosted. It is highly available due the service is contained in different zones.
- **Management**: The management is low for DR Alarms because the services are in the cloud, which is responsibility of the provider to monitoring, licensing, updating and others.

- **Security**: The architecture allows DR and customize the backups through several VPN to stored it in a bucket (Aws S3).it is taken with priority, with the resource isolation that provide VPC the security group acts as controller inbound and outbound of VPC traffic.
- **Operativity**: It is low allowing to the client the client be focus on their business; it can be a set up source control to release management. Aggregate logs for centralized monitoring and alerts. Make sure alerts trigger automated responses, including notification and escalations.

2.2.4 Disadvantages

- **Risk data:** although measures were taken to reduce the risk, there will always be a risk when exist transport of our data through internet.
- **Internet connection:** the design is to operate in the cloud, so, it is very important take measures to provide a constant internet connection on- premises.
- **No control:** it can be an advantage, but depending on the side where are you looking, your services will depend on the provider.

2.3 Moving Servers to deployment model IaaS or PaaS

To move to the cloud, it is necessary to determine which servers should deploy in IaaS or PaaS we need to understand what my servers do and what is the architecture of each application which host each server.

2.3.1 Active Directory domain controller server

Basically, it is a database that with secure purposes combine in a security group User accounts, computers, Printers, File shares, Security(Microsoft, 2017). The server run authentication and approval for these resources to access. But this needs administration over the database to make sure who can access or not. Understanding the logical model, it is a distributed database that stores and manages information about network resources as well as application-specific data from directory-enabled applications. Understanding that the administrator is who control the databases the growing of resources such storage mostly is predictable which deploy it in IaaS model is better than PaaS because we do not need to make scalable. Public IaaS cloud connect it to your on-premises network, thus providing a hybrid environment where local resources can access cloud resources and vice versa. This configuration is to provide AD services for legacy application VMs that are also in the cloud. The IoT devices should support these devices in a public cloud to be admitted.

2.3.2 SQL Server

Firstly, define a SQL server is an interface between a database and end-user or program which it can modify, add, update, delete rows and retrieve subsets of information. As we can see in active directory there are several programs that use relational databases as based. This mean that is an essential part on-premises and cloud base application.

Considering that we can install SQL server in a VM or physical with both Linux and

windows(Shwerank, 2020), allow us more options. Therefore, the most important here is storage which can up of down depending on the workload, so a model IaaS could work, but the client is who going up or down VMs or Storage and install them which could result difficult if the demand increase. There is another option with PaaS which call me my attention with the provider Azure that virtualize the database, they call this DBaaS which offer different options of deployment between them elastic pools which is a good option for DR Alarms due to the local and international potential growth.

2.4 Exchange Email Server

This server is who handle our email and calendar even other option which helps a corporation's being more collaborative. According to the architecture application needs storage, active directory, databases, interfaces, domain, security and others which indicate that the best way to server is on-premises, or SaaS hosted in Microsoft 365 (Microsoft, 2021). For example, the Availability group in active directory must be available in the same location.

2.4.1 File and Printer server

This server is a convenient local solution for our client due to sensitive data that he use, and according to our solution we will storage the backups into the cloud make it the data highly available, a solution in IaaS or PaaS is not a best practice in this case(NIST, 2013).

2.4.2 Apache & Tomcat Linux server

Firstly, we should understand what is Apache which basically is a web server environment open-source where Java can run(Apache, 2021), Considering that the company is developing monitoring devices, and assumed that have internal and external web site between other

which the best platform for this es PaaS to team do not worried with hardware and its maintenance.

2.4.3 Proxy Server

Even this server is not on premise of Dr Alarms proposed this service on premise to increase the security(NIST, 2013). A proxy server provides a gateway between users and internet which is like an intermediary to protect the company from web site that the users visit, also protect the company from data breaches from hackers. Exit the option to move it to the cloud but is SaaS model.

3. Desktop approach

Amazon workspaces is a managed, secure Desktop solution(Amazon Web Services, 2021b), which the mostly features for the case is that no need licensing, it patches itself, pay just for the workspaces that the client lunch, use globally, and it can be connected to the VPC, as a result, the client can reduce cost for hardware management, and they can continue using their desktops. The disadvantage is it still need connection to internet. Amazon offers this service with the option to accept Microsoft Office licenses if the customer currently owns one, which reduces the cost.

Microsoft Office 365 is a Word process with different tools that allows collaboration experience to enhance productivity(Microsoft, 2021). This requires internet connection depending on the bundle that the enterprise acquire. The most important advantages are its uses in collaborative form and many forms of word processing, exchange can be used in this form of SaaS to reduce server maintenance, improve communication, and have automatic updating. However, this service required license and depending on this license the cost increase if the user wants to install in the PC.

It is suggested to use Microsoft 365 in combination with Amazon workspaces due to that Amazon workspace (WS) is a work environment like a VM it is not totally comparable with Microsoft 365. Although The solution comes with a word processor which the name is Amazon workdocs, it does not have the collaboration experience as Microsoft 365 does. However, it requires the workstation that needs maintenance, if the client decides to use this solution, it is not depending on hardware performance, but there is depending on the internet connection. Dr Alarms is struggle with maintenance contract, but the risk is low if a workstation goes down because the data is not store locally, which is other advantage for backups. This solution also supports remote access and the (WS) update itself. The company requires an IT resource restructuring.

4. Use the cloud each.

The approach to the Cloud Edge solution that is required by the engineering manager, is considered from the point of view in relation to the development of the product in the market.

It is considered that the manager requires that their IoT monitoring devices that are relatively new and still under development whose main function is to monitor a series of different activities outside the network of an organization, have interaction with the user according to their experience with the product, collecting this information so that results are later put into a forum and discussed, allowing other users to see and interact with real experiences of users who are currently using the product. Thus, it is improving the product experience according to these discussions developed in the forum, in turn delivering feedback on recommendation of use and reading of the data delivered by the devices. The solution is based on an interaction between marketing and engineering to promote the product in the market.

An Edge solution in the cloud is understood as the processing of data in a local way for decision making with low latency providing a fast solution(Amazon Web Services, 2021c). In other words, the monitoring device will process what it is obtaining in real time and interacting with the user. So, it later when the device has the availability to connect to the network, it will allow it to send the processed data to the DR Alarms datacenter to collect this information and, return a feedback, improving the customer experience.

The disadvantage of this solution is that the device requires an internet connection to process the information collected with the datacenter.

Amazon Simple Queue Service (SQS) is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications(Amazon Web Services, 2021a). SQS eliminates the complexity and overhead associated with managing and operating message-oriented middleware, keep sensitive data secure, Scale elastically and cost-effectively and empowers developers to focus on differentiating work.

Data analysis is provided through machine learning with Amazon Sagemaker combining this with Amazon Athena which is a serverless, which it is not require server to manage interactive query service that makes it easy to analyze data in Amazon S3 using a standard SQL(Amazon Web Services, 2021c).

The architecture of the solution used here is shown in the figure below where the mentioned service is highlighted, independent of the VPC, processing the information in Amazon EC2 and Amazon Lambda(Amazon Web Services, 2020). The information is moved and updated through the Amazon datasync service between on-premises, client and IoT monitoring device allowing a synchronized system.

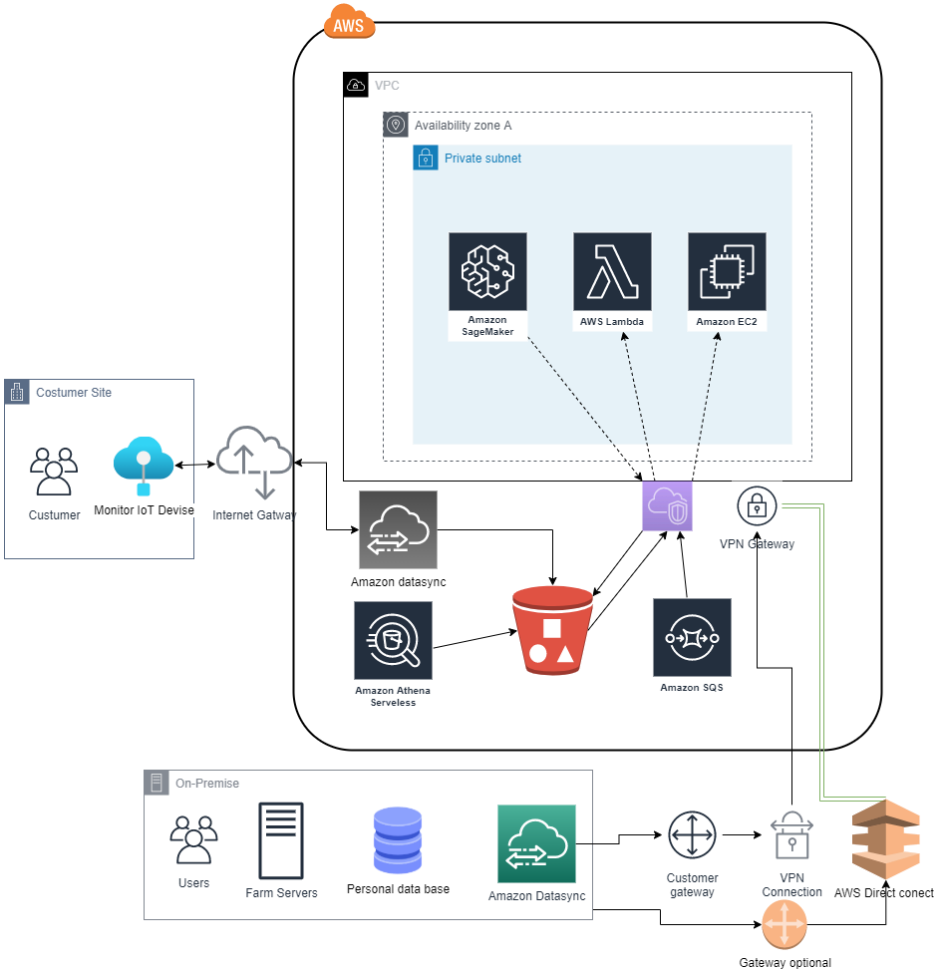


Figure 2. Architecture IoT monitoring device forum Cloud Edge solution

5. References

Amazon Web Services, I. o. i. a. (2021a). *Amazon Simple Queue Service*. https://aws.amazon.com/sqs/

Amazon Web Services, I. o. i. a. (2021b). *Amazon WorkSpaces*. https://aws.amazon.com/workspaces/?nc=sn&loc=0&workspaces-blogs.sort-by=item.additionalFields.createdDate&workspaces-blogs.sort-order=desc

Amazon Web Services, I. o. i. a. (2021c). *AWS for the Edge*. https://aws.amazon.com/edge/

Apache. (2021). *What is the Apache HTTP Server Project?* https://httpd.apache.org/

Attaran, M., & Woods, J. (2018). Cloud computing technology: improving small business performance using the Internet. *Journal of Small Business & Entrepreneurship, 13*, 94-106. https://doi.org/10.1080/08276331.2018.1466850

Diez, O., & SIlva, A. (2013). Govcloud: Using Cloud Computing in Public Organizations. *IEEE Technology and Society Magazine, 32*(1), 66-72. https://doi.org/10.1109/MTS.2013.2241473

Erl, T., Mahmood, Z., & Puttini, R. (2013). *Cloud computing : concepts, technology, & architecture* (1st edition ed.). Prentice Hall.

Flexera. (2020). State of the Cloud Report. https://doi.org/https://www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/

Microsoft. (2017). *Understanding the Active Directory Logical Model*. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-the-active-directory-logical-model

Microsoft. (2021). *Microsoft 365*. https://www.microsoft.com/en-au/microsoft-365

[Record #984 is using a reference type undefined in this output style.]

Shwerank, S. (2020). *Sql Server: IaaS Vs PaaS*. https://beingadba.com/2020/05/16/sql-server-iaas-vs-paas/

Verizon. (2020). Data Breach Investigation Report. https://doi.org/https://enterprise.verizon.com/resources/reports/dbir/