**CONL715 Assignment 3:  
Cloud Migration Report**

Word Count – 1,581

# Introduction

As the new IT Infrastructure Manager for Glyndwr Insurance Ltd, a decision has been made to migrate the current traditional server infrastructure - where all hardware, networks and other resources are bult and maintained by the company on site [1]; over to the cloud, where these assets are accessed over the internet as and when needed [2-3]. Therefore, this migration report aims to firstly, detail Glyndwr Insurance Ltd.’s current server infrastructure, elaborate on how it could adapt to the cloud, with justifications on why a migration is needed. Secondly, expound upon how the migration will be conducted, with any known potential issues declared. Finally, to propound contingencies including a disaster recovery plan. Since the IT infrastructure manager’s arrival, it has been made clear, that company is working remotely, with no view to move back into the office; moreover, looking to relinquish their office due to unnecessary overheads as part of the aftermath from the coronavirus pandemic.

# Current On-premises Network Infrastructure

At Glyndwr Insurance Ltd, the current infrastructure makes use of a Software Defined Network architecture, which has been useful thus far, as it has ensured ease of configuration from a single point of access across the entire network [4-5].

Additionally, the further elements in the network infrastructure will be documented as per below. Firstly, Glyndwr Insurance Ltd, implement web and application servers which hosts the company’s website, and allows information and interaction between the company database, site visitors to explore services available, including logging into their account to manage their policies [6,11]. Secondly, a series of database servers, used to store, query, backup, access and retrieve data about customers, policies taken out, premiums those policies, employees and so forth [7-8]. Thirdly, a mail server to capture and process all correspondence between employees and external sources contacting the insurance company [12]. Fourthly, Glyndwr Insurance Ltd have over two hundred devices – particularly, desktop PC’s, laptops, and mobile phones, which typically represents the number of employees working over the network in a medium sized business [9]; accessing internal systems via a virtual private network (VPN) which network traffic goes through the switch onto the local area network (LAN) [10]. It is understood the nature of employees accessing services via VPN is due to all workers working remotely, permanently going forward due to the aftermath of the coronavirus pandemic.

In addition to above, the current network infrastructure for Glyndwr Insurance Ltd. has been illustrated as seen in figure 1.

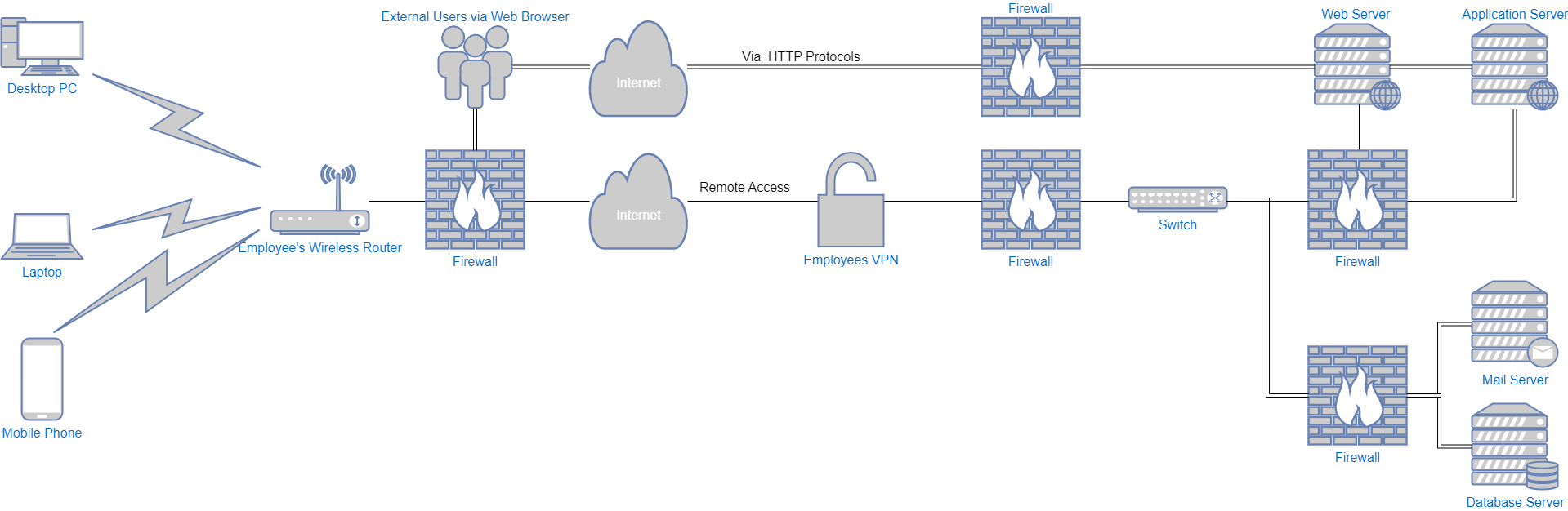


Figure 1 - Current Network Infrastructure for Glyndwr Insurance Ltd. Manually created using draw.io.

## How server infrastructure could be adapted to the cloud

Based on the current network infrastructure that has previously been shown above, there appears to areas that would benefit from adoption onto a cloud-based network infrastructure. One adoption refers to data storage. Firstly, it could prove to be more cost effective compared with current setup as data is hosted on virtual resources [13].Secondly, it provides enhanced security, as data is duplicated across multiple servers, in different areas to mitigate risk of hardware crashes or accidental deletion [13].Thirdly, due to service elasticity, storage can be increased or decreased as required [14], so databases held by the company will not become overloaded if data held is too much compared with the current physical servers – where expensive additions would need to be purchased, and a difficult justification required as to why more equipment has been purchased and then not used. Finally, the cloud infrastructure could help Glyndwr Insurance utilise the use of single sign on – where users either employee or customer have one set of credentials to enter to access the services they need [15-16]. Currently for example, employees are having to have different credentials for each service they are using, where using elements from the cloud could eliminate this issue.

## Justification as to why migrating to the cloud is necessary

It may be questioned as to why there is a need for Glyndwr Insurance Ltd to incorporate the use of a cloud-based network infrastructure, instead of sticking with what is currently implemented; there is one extraordinarily strong reason for this – innovation. One reason as to why this is needed, stems from the company wishing to use IoT – known as the Internet of Things, where devices can communicate with one another via the internet [17] -enabled black boxes as part of a new policy to advertise in the car insurance space. Without the cloud, this option would be exceedingly difficult to administer. Secondly, cost. Due to the per use practice, Glyndwr Insurance can harness more computing power as and when needed in term of analytics and removed need of investing into capital expenditure to do this and is replaced with operational expenses which can scale up or down as needed.[18].

# Proposed Cloud Infrastructure

Now the report so far has detailed the current network infrastructure, elements where it could be enhanced, and some reasons as to why Glyndwr Insurance Ltd needs to adopt some variation of cloud infrastructure, this section aims to uncover the best cloud service model for the company and would that mean. Additionally, will do the same for the type of cloud deployment to implement.

### Cloud service model

The cloud service model elected to be used for Glyndwr Insurance Ltd, would-be Infrastructure as a Service (IaaS) – where the company would be able to configure processing, storage, networks, computing, and applications, all without not having to worry about dealing with the underlying cloud infrastructure [19].This allows the company to reduce maintenance time and hardware costs, and the ability to scale resources up or down depending on demand [20].The reason for not choosing Software as a Service (SaaS) – where it allows application to be ran and used over the internet, without the need for individual installation of said applications [21]. Whilst this will not be useful for employees to have certain application delivered this way – such as email, Microsoft Office applications, this does not necessarily address the need of managing our infrastructure or building and further development our applications, or applications used in the business to interface with the customer or manage their data. Platform as a Service (PaaS) – where a computing platform is provided using cloud infrastructure [21], whilst a potential avenue to explore in future, once Glyndwr Insurance is more established in the cloud, it may be difficult to migrate all services over to this state – at least in first instance.

### Cloud Deployment Model

The cloud deployment model that the company could use would be via a hybrid cloud model – where it consists of both elements of private and public cloud deployment types. Some of the reasons as to why this would be the most beneficial deployment type, is that it allows the company to keep an emphasis on securing the data it holds, within a private cloud, whilst allows some of the cost benefits gained from the public cloud [22]. Additionally, this form of cloud deployment allows Glyndwr Insurance to tailor the cloud implementation it needs based on its requirements.

# Transition to cloud infrastructure

The next section of this report is to advise on how a migration from our current infrastructure to the proposed cloud infrastructure is feasible. The migration approach that Glyndwr Insurance Ltd could pursue would be via a rehost method – which institutes a ‘life and shift’ mentality- in that – the move of applications from on-premises, over to the cloud environment with minimal changes to the applications themselves, allowing for arguably the quickest method of migration [23]. Whilst the most straightforward method initially, it comes at a trade-off not optimising the use of the cloud applications that could further reduce complexity or cost. There are also additional complexities to be aware of with this method, such as the skill gap the company may from going to a new cloud infrastructure, and ensuring employees receive the relevant time needed before, during and after the migration to get up to speed with the relevant new practices to be adopted [24]. Another challenge involves ensuring the protection of customer data, which needs addressing, not only for reputational damage, but breaching compliance and data governance laws if not met. One method to mitigate this risk, would be to encrypt the transmission of data on transit and at rest from source to destination [25].

# Contingencies and Disaster Recovery

Finally, the last section of this report, is to establish what contingencies, as well as a disaster recovery plan to put in place, as part of the new cloud infrastructure, as used by Glyndwr Insurance Ltd. One method that is usable by way of some form of disaster recovery, involves the use of cloud configuration management tools. Examples of such tools are Terraform, created by Hashicorp [26], used to recover the cloud environment in its entirety, should such a natural or human related disaster fall upon it. Another approach to tackle the pre-empt the events of a disaster, would-be to apply a backup and restore policy in place – this would help to mitigate the risk of data loss or corruption. Furthermore, to replicate systems/ data in other cloud regions, so if one region is down, the cloud services can still be functional using other regions [27-28].

# Conclusion

Glyndwr Insurance in a good state to migrate over to the cloud, with many opportunities to exploit once migrated. Reviewing the current network infrastructure that is in use at present, this report identifies the type of cloud service and deployment models to take, with how to transition over to the new environment, as well any contingencies to consider going forward.

# References

[1] L. Ferreira et al., “Standardization Efforts for Traditional Data Center Infrastructure Management: The Big Picture,” IEEE Engineering Management Review, vol. 48, no. 1, pp. 92–103, Mar. 2020, doi: 10.1109/emr.2020.2969864.

[2] E. Knorr and G. Gruman, “What Cloud Computing Really Means,” Apr. 2008. Accessed: Nov. 26, 2022. [Online]. Available: http://skysolutions.co.zw/docs/What\_Cloud\_Computing\_Really\_Means.pdf

[3] T. Dillon, C. Wu, and E. Chang, “Cloud Computing: Issues and Challenges,” 2010 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, doi: 10.1109/aina.2010.187.

[4] S. H. Haji et al., “Comparison of Software Defined Networking with Traditional Networking,” Asian Journal of Research in Computer Science, vol. 9, no. 2, pp. 1–18, May 2021, doi: 10.9734/ajrcos/2021/v9i230216.

[5] geeksforgeeks, “Difference between Software Defined Network and Traditional Network,” GeeksforGeeks, Aug. 18, 2020. https://www.geeksforgeeks.org/difference-between-software-defined-network-and-traditional-network/ (accessed Nov. 15, 2022).

[6] M. C. Drott, “Using Web server logs to improve site design,” Proceedings of the 16th annual international conference on Computer documentation - SIGDOC ’98, 1998, doi: 10.1145/296336.296350.

[7] M. Grasdal, L. E. Hunter, M. Cross, L. Hunter, D. L. Shinder, and T. W. Shinder, “MCSE 70-293: Planning Server Roles and Server Security,” MCSE (Exam 70-293) Study Guide, pp. 53–146, 2003, doi: 10.1016/b978-193183693-7/50006-3.

[8] S. Zhang and M. Wang, “Server Classifications,” Encyclopedia of Information Systems, vol. 4, pp. 57–69, 2003, doi: 10.1016/b0-12-227240-4/00157-x.

[9] Gartner, “Small And Midsize Business (smb),” Gartner, 2019. https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses (accessed Dec. 03, 2022).

[10] geeksforgeeks, “Virtual Private Network (VPN) | An Introduction,” GeeksforGeeks, Oct. 05, 2017. https://www.geeksforgeeks.org/virtual-private-network-vpn-introduction/ (accessed Dec. 03, 2022).

[11] C. Mohan, “Tutorial,” Proceedings of the 2002 ACM SIGMOD international conference on Management of data - SIGMOD ’02, 2002, doi: 10.1145/564691.564796.

[12] Techopedia, “What is an Email Server (MTA)? - Definition from Techopedia,” Techopedia.com, Dec. 12, 2017. https://www.techopedia.com/definition/1660/email-server-email (accessed Dec. 03, 2022).

[13] J. Wu, L. Ping, X. Ge, Y. Wang, and J. Fu, “Cloud Storage as the Infrastructure of Cloud Computing,” 2010 International Conference on Intelligent Computing and Cognitive Informatics, Jun. 2010, doi: 10.1109/icicci.2010.119.

[14] I. Odun-Ayo, O. Ajayi, B. Akanle, and R. Ahuja, “An Overview of Data Storage in Cloud Computing,” IEEE Xplore, Dec. 01, 2017. https://ieeexplore.ieee.org/document/8520306 (accessed Oct. 03, 2020).

[15] P. Murukutla and K. C. Shet, “Single Sign on for Cloud,” 2012 International Conference on Computing Sciences, Sep. 2012, doi: 10.1109/iccs.2012.66.

[16]A. G. Revar and M. D. Bhavsar, “Securing user authentication using single sign-on in Cloud Computing,” 2011 Nirma University International Conference on Engineering, Dec. 2011, doi: 10.1109/nuicone.2011.6153227.

[17] K. Karimi and G. Atkinson, “What the Internet of Things (IoT) Needs to Become a Reality,” Jun. 2013. Accessed: Dec. 04, 2022. [Online]. Available: <http://files.iccmedia.com/pdf/freescale140527.pdf>

[18] M. G. Avram, “Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective,” Procedia Technology, vol. 12, no. 12, pp. 529–534, 2014, doi: 10.1016/j.protcy.2013.12.525.

[19] P. Mell and T. Grance, “The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology,” Sep. 2011. Accessed: Dec. 04, 2022. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

[20] Microsoft Azure, “What is IaaS? Infrastructure as a Service | Microsoft Azure,” azure.microsoft.com, 2022. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas/ (accessed Dec. 04, 2022).

[21] Y. Jadeja and K. Modi, “Cloud computing - concepts, architecture and challenges,” 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Mar. 2012, doi: 10.1109/icceet.2012.6203873.

[22] GeeksforGeeks, “Cloud Deployment Models,” GeeksforGeeks, Jul. 11, 2021. https://www.geeksforgeeks.org/cloud-deployment-models/ (accessed Dec. 04, 2022).

[23] S. Orban, “6 Strategies for Migrating Applications to the Cloud | Amazon Web Services,” Amazon Web Services, Nov. 2016. https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/ (accessed Dec. 04, 2022).

[24] M. Shuaib, A. Samad, S. Alam, and S. T. Siddiqui, “Why Adopting Cloud Is Still a Challenge?—A Review on Issues and Challenges for Cloud Migration in Organizations,” Advances in Intelligent Systems and Computing, pp. 387–399, 2019, doi: 10.1007/978-981-13-5934-7\_35.

[25] msmbaldwin, “Azure security baseline for Azure Migrate,” learn.microsoft.com, Oct. 12, 2022. https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-migrate-security-baseline (accessed Dec. 04, 2022).

[26] Hashicorp, “Terraform by HashiCorp,” Terraform by HashiCorp. https://www.terraform.io (accessed Dec. 04, 2022).

[27] aws, “Disaster recovery options in the cloud - Disaster Recovery of Workloads on AWS: Recovery in the Cloud,” docs.aws.amazon.com, 2022. https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html (accessed Dec. 04, 2022).

[28] S. Joshi, “Azure Site Recovery: Achieve Disaster Recovery with Azure,” Globant, Aug. 03, 2021. https://medium.com/globant/azure-site-recovery-achieve-disaster-recovery-with-azure-7ff762c3796e (accessed Dec. 04, 2022).