Heartland Escapes Network Design

Aidan Polivka

CS-635: Computer Networking

Colorado Technical University

December 3, 2023

Table of Contents

Project Outline

“Heartland Escapes” is a bookstore in Nebraska. They've been in Lincoln for years, opening their first store in 2010 and their second in 2019. Their recent popularity is thanks to a fresh marketing approach on social media platforms like Instagram and Tik Tok. Events like the 'school’s out reading program,' author meet-and-greets, and Halloween story readings have contributed to their success. They're planning to expand to Omaha and Grand Island.

Since their 2009 opening, 'Heartland Escapes' has made minor technology upgrades, like increasing disk space, RAM, and upgrading the processor. Their current system, hosted at their first store, includes a Windows 2008 server with an Intel Core i7-8700 processor. This processor has 6 cores and 12 threads, running at 3.2 GHz, with an L2 Cache of 256 KB per core and an L3 Cache of 12 MB. The server has 8 GB of RAM and 8 TB of Hard Disk space, with 3.5 TB in use. It hosts a point-of-sale system, an inventory system, and a public website, all written in .NET Framework 4.8 web forms. It also includes a Microsoft SQL Server for the inventory and accounting databases. A network of 8 machines between the two locations uses the Point-of-Sale web application and Inventory API. The website interacts with the inventory API so users can search for books in each store from their homes. With two new stores and a growing customer base, 'Heartland Escapes' plans to upgrade their system for scalability and ease of management by moving to the cloud.

Given their Microsoft-centric system and growth expectations, I recommend migrating their infrastructure to Azure while keeping an on-premises server as a backup. This shift to the cloud supports hardware scalability for increased traffic without requiring dedicated CPUs. Azure, a Microsoft product, aligns with their .NET applications and MS SQL Server database management system.

I suggest configuring Azure into two resource groups: one for data and infrastructure, and the other for applications. All resources should be in the us central region. In the application storage container, there will be three app services: one for the Point-of-Sale web application, one for the Inventory API, and one for

the public website. Azure App Services are like containers with a base operating system. In this case, I recommend running all services on a Windows system for simplicity. The app services would use the Premium v3 P1V3 hardware tier, which includes two vCPUs and 8 GB of RAM per instance, with the ability to scale up to 30 instances. In the data and infrastructure group, there would be an Azure SQL Server hosting both databases, and a virtual network (vNet) that manages firewall rules and security. A vNet Gateway would allow users to access the system via VPN. The public website would be the only part of the system outside of the vNet, accessible only through the gateway. The public website's IP address would also have access.

Distributed Network Requirements Analysis

Migrating to a distributed environment fulfils a lot of 'Heartland Escapes' business requirements in their expansion effort. In this section, we'll break down five distinct business requirements and outline the ways in which migrating to Azure Platform as a Service offers solutions to them.

The first and most important requirement of 'Heartland Escapes' is *scaling and flexibility*. With 'Heartland Escapes' business model being centered around events; they go through periods of incredibly high customer volume. This includes traffic through their public website, and their critical inventory system. Azure offers the ability to scale horizontally, adding service nodes when hardware resources reach a configurable threshold. With our current service plan, we can configure their app services to scale out to up to 30 instances across all three of 'Heartland Escapes' services. This is significantly more computational power than their current on-premises system allows for and should serve them well. An added benefit to Azure as a service is that we can easily upgrade their plan if 'Heartland Escapes' grows at an unexpected rate.

The next business requirement that moving to a distributed system fulfils is *redundancy and high availability*. Azure App Services allows for deployed services to have geographic redundancy. This redundancy serves multiple purposes: geographic redundancy allows for users to access services from servers geographically near them, offering higher network speeds. Redundancy also allows for fault tolerance from natural disasters, so if something were to happen to one of Microsoft's server facilities, another facility will pick up the load from your business's deployed services. Microsoft's app service plans boast an uptime percentage of 99.95% (Ekuan), making 'Heartland Escapes' availability potentially higher than their on-premises system depending on their maintenance schedule.

Another business requirement for 'Heartland Escapes' is *Security and Access Control*. Azure offers Azure Active Directory, which will allow for fine-tuned control of user access and authentication. This will benefit 'Heartland Escapes' greatly in controlling which individuals can have database read and/or write

access, access to the Point-of-Sale system, and granting accesses from services to connect to the Inventory API. Azure also allows lots of network security options like vNets and network gateways. This will allow 'Heartland Escapes' to control what service ports are open to be communicated with, and what IPs are able to communicate with resources within the virtual network. The virtual gateway will also allow employees using the Point-of-Sale system to connect to the virtual network via VPN and sign in securely.

The fourth business requirement needed when migrating to a distributed environment is *Resource Sharing and Centralized Data Management*. 'Heartland Escapes' shares a single SQL Server instance, and two distinct databases. This is central to their inventory management system and Point-Of-Sale system. This should not be a significant change to their architecture, however the SQL Server instance will no longer be hosted on the same machine as the services. Because these services are no longer hosted on the same machine, measure will need to be taken to ensure that only services within the virtual network can access the Azure hosted SQL Server.

The fifth and final business requirement for 'Heartland Escapes' migration effort is *Remote Access and Mobility*. Users of the Point-Of-Sale system will need to be able to access that service from within the Virtual Network, so a vNet Gateway will be required connect via VPN. 'Heartland Escapes' also hopes to be able to open mobile pop-up stores, so being able to connect from locations outside of the physical store will be a necessity. Their network structure will need consideration to make this functionality secure.

Security is of utmost importance for 'Heartland Escapes' since they are transferring financial data from their customers to third party payment processors. Measures will need to be taken to ensure that data in transit and at rest is encrypted per the Payment Card Industry Data Security Standard (PCI DSS). If compliance to this standard is not met, 'Heartland Escapes' risks large fines that are beyond the business's capability to pay. (Baykara, 2023)

Communication Protocols Analysis and Recommendations

We will want to make our choices of communication protocols with 'Heartland Escapes' business requirements in mind. Understanding that 'Heartland Escapes' transmits and stores customer financial information and potentially other personally identifiable information (PII), we'll want to ensure that the messaging protocols we subscribe to are highly secure. We also want to make sure that our protocol stack is robust and is not subject to change any time soon since this is a migration/modernization effort. Additionally, we'll need to consider what protocols Azure can communicate with. If we weren't migrating to a platform that's as established as Azure, we might have wanted to make this consideration prior to choosing Azure as a cloud host.

HTTPS and SSL/TLS Certificates

Because 'Heartland Escapes' system is primarily web based, we'll plan to use HTTPS for their web application protocols. HTTPS stands for "Hypertext Transfer Protocol Secure" and is an extension of its predecessor HTTP. HTTP was used for a long time but was considered insecure because it doesn't use any form of encryption of hypertext messages in transit. This security issue has been resolved by the HTTPS extension of HTTP, which encrypts the hypertext message to a cyphertext using SSL/TLS certificates. In fact, this security improvement to the original HTTP protocol has just about replaced HTTP entirely, and most modern web browsers will flag web pages as "not secure" if you try to access a domain that uses HTTP. (GeeksForGeeks, 2022)

So, what is SSL/TLS, and what does it add to the HTTP protocol to make it secure? SSL is an acronym for "Secure Socket Layer". This layer is an encryption-based internet protocol layer, used to secure messages across the web. The layer uses an authentication method called a "handshake" between the sending and receiving service before sending the message data. This handshake ensures that the two machines are who they say they are, rather than a bad actor claiming to be an authenticated machine in the network. As an

added layer of security, the SSL protocol digitally signs all messages to the receiving machine to ensure that the message wasn't tampered with in transit. (CloudFlare) As with any technology, the SSL protocol has undergone updates. The updated version of SSL is TLS, which stands for "Transport Layer Security". In the networking world those names have become synonymous, hence the name SSL/TLS. For example, the website DigiCert sells all their TLS certificates under the name SSL, although it is really a TLS certificate you're receiving. (digicert)

HTTPS and SSL/TLS will be used all over the new 'Heartland Escapes' system. It will be used in communication between app services, between app services and client web browsers, and between app services and the Azure hosted database. This is to ensure security of the message data sent, and to make sure that the services communicating amongst each other are who they say they are.

OpenVPN Protocol

Many VPN providers utilize a protocol called "OpenVPN". This protocol uses a custom protocol based on SSL/TLS to secure communication between machines. It also allows for two-factor authentication and a kill switch to ensure that individuals connecting are authenticated. OpenVPN is an open-source protocol, which means that its code base is available to be read by the public. This has its pros and cons, the benefit being that consumers can access the code and ensure that it's up to their standards, the cons being that bad actors can read the code and try to find ways to break it. OpenVPN allows for connection from most devices, including windows, linux, and mac computers, and android and apple phones. OpenVPN can access email, file servers, and databases. (GeeksForGeeks, 2023)

OpenVPN is one of the protocol options in Azure's Point-To-Site VPN, and it's clearly the best options for 'Heartland Escapes'. With it being one of the most secure VPN protocols available, and capable of accessing so many internal resources, it would be the perfect solution for 'Heartland Escapes' future

endeavors to allow pop up stores in temporary locations. It also helps ‘Heartland Escapes’ adhere to the requirements of the Payment Card Industry Data Security Standard.

Network Traffic Analysis and Recommendations

TBD

Network Design and Architecture

TBD

Future Needs Analysis and Recommendations

TBD

References

Baykara, S. (2023, October 9). PCI DSS control objectives. PCI DSS GUIDE. https://pcidssguide.com/pci-dss-control-objectives/

Ekuan, M. (n.d.). Azure App Service and reliability. Microsoft Azure Well-Architected Framework | Microsoft Learn. https://learn.microsoft.com/en-us/azure/well-architected/service-guides/azure-app-service/reliability

GeeksforGeeks. (2022, May 6). HTTPS full form. GeeksforGeeks. https://www.geeksforgeeks.org/https-full-form/

GeeksforGeeks. (2023, January 24). Types of virtual private network (VPN) and its protocols. GeeksforGeeks. https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/

How does SSL work? | SSL certificates and TLS | cloudflare. CloudFlare. (n.d.). https://www.cloudflare.com/learning/ssl/how-does-ssl-work/

What is an SSL certificate?. DigiCert. (n.d.). https://www.digicert.com/what-is-an-ssl-certificate