**Microsoft Cloud Workshops**

Whiteboard Design Sessions

Building a Resilient IaaS Architecture

Leader Guide

February 2017

© 2017 Microsoft Corporation. All rights reserved. This document is confidential and proprietary to Microsoft. Internal use only. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

Contents

[Proctor information 1](#_Toc474130982)

[Building a Resilient IaaS Architecture learner guide 4](#_Toc474130983)

[Building a Resilient IaaS Architecture leader guide 13](#_Toc474130984)

# Proctor information

Thank you for taking time to support the workshops as a proctor!

Role of the proctor

An amazing proctor:

* Creates a safe environment in which learning can take place.
* Stimulates the participant’s thinking.
* Involves the participant in the learning process.
* Manages the learning process (on time, on topic, and adjusting to benefit participants).
* Ensures individual participant accountability.
* Ties it all together for the participant.
* Provides insight and experience to the learning process.
* Effectively leads the workshop discussion.
* Monitors quality and appropriateness of participant deliverables.
* Effectively leads the feedback process.

Workshop flow

Each workshop uses the following flow:

Before the workshop: How to prepare

Before conducting your first workshop:

* Read the Attendee guide (including the case study) and Proctor guide
* Become familiar with all key points and activities.
* Plan the point you want to stress, which questions you want to drive, transitions, and be ready to answer questions.
* Prior to the workshop, discuss the case study to pick up more ideas.
* Make notes for later.

During the workshop: Tips for an effective workshop

**Refer to the Proctor guide** to stay on track and observe the timings.

**Do not expect to memorize every detail** of the workshop.

When participants are doing activities, you can **look ahead to refresh your memory**.

* **Adjust activity and workshop pace** as needed to allow time for presenting, feedback, and sharing.
* **Add examples, points, and stories** from your own experience. Think about stories you can share that help you make your points clearly and effectively.
* **Consider creating a “parking lot”** to record issues or questions raised that are outside the scope of the workshop or can be answered later. Decide how you will address these issues, so you can acknowledge them without being derailed by them.

***Have fun****! Encourage participants to have fun and share!*

**Involve your participants.** Talk and share your knowledge but always involve your participants, even while you are the one speaking.

**Ask questions** and get them to share to fully involve your group in the learning process.

**Ask first**, whenever possible. Before launching into a topic, learn your audience’s opinions about it and experiences with it. Asking first enables you to assess their level of knowledge and experience, and leaves them more open to what you are presenting.

**Wait for responses**. If you ask a question such as, “What’s your experience with (fill in the blank)?” then wait. Do not be afraid of a little silence. If you leap into the silence, your participants will feel you are not serious about involving them and will become passive. Give participants a chance to think, and if no one answers, patiently ask again. You will usually get a response.

# Building a Resilient IaaS Architecture learner guide

## Step 1: Review the customer case study

**Outcome**

Analyze your customer’s needs.

**Facilitator/SME presentation of customer case study**

Timeframe: 15 minutes

Directions: With all participants in the session, the facilitator/subject matter expert (SME) presents an overview of the customer case study along with technical tips.

1. Meet your table participants and proctor.
2. Read all of the directions for Steps 1–3 in this attendee guide.
3. As a table team, review the following customer case study.

### Customer background

LitWare Inc. manufactures, sells, distributes, and services parts for major appliances and Heating, Venting and Air-conditioning (HVAC) systems for large corporations and independent firms. The ordering system is currently housed in Azure on IaaS SQL server instances. Initially, the ordering process was done mainly via phone and expanded to email. Recently, the company has moved to an internet based ordering system with Internet Information Services (IIS) Web Servers in Azure housing the front-end application for the ordering, invoicing, and support options. In addition, they have a legacy application where the data is tightly coupled with the application and a re-write of the application is currently not planned. The application is currently being backed up using a disk to disk to tape application. The legacy application is currently supported on aging hardware and a decision must be made as to whether to purchase new hardware to run the application, re-write the application, which will take time or move the application.

They have grown into a viable, sustainable business and would like their technology to mirror the growth and sustainability. This would help cement their reputation in the industry and go a long way to assist their future growth. While business impact analysis (BIA) has not officially been performed, they have an overall plan of wanting to restore from an issue within 4 hours and recover to within the last 8 hours if at all possible.

There is no overall IT shop for LitWare Inc. as such. They are pretty much a classic IT company that doesn’t have deep experience in the interactivity of all the components. They have rolled out sections and departments successfully, but now as the technology matures, they are in need of guidance for their deployments.

Currently, there are 3 branch offices located throughout the United States. One is in the mid-West, another is on the East Coast and the third is located on the West Coast. Discussions are in progress to grow the business to Europe and a possibility of factories in Mexico and Asia.

Each branch office is small enough that there are no servers housed on-site. Each location has direct connectivity to corporate resources through a Virtual Private Network (VPN) connection to the Austin headquarters. Email is accessed via web as is the main ordering application.

At times, various branch offices have experienced connectivity issues due to the internet service provider having issues with the corporate office connection. While there is some understanding of these occurrences, there is a desire to provide a way to resolve this as growth continues. Employees work from home when this occurs.

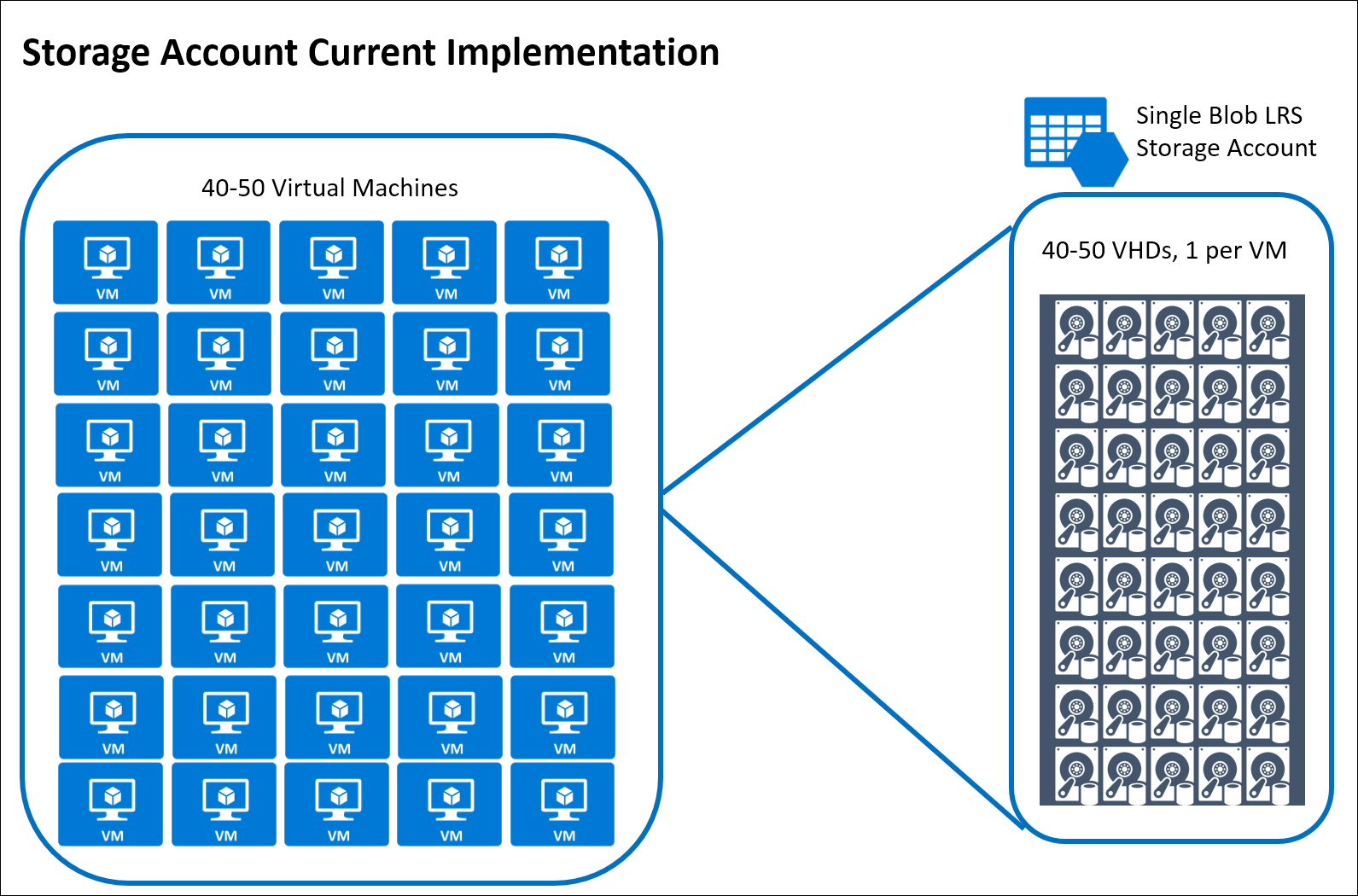
### Customer situation

Recently, under the overall guidance of Lewis Franklin (Head of Infrastructure and Operations), individual departments have been taking the servers from their scope of influence into Azure. The Active Directory Domain Services team has deployed a few IaaS Domain Controller Virtual Machines to a single region close to the Austin office in South Central U.S. There has been some effort to follow the guidance of Microsoft on the use of Active Directory in Azure, but there are some gaps in the configuration.

The web application team has also deployed Internet Information Services (IIS) Virtual Machines (VMs) within the same South Central U.S. region. While they do not have administrative rights for the database machines that provide database services for the web application, they do have database rights and can access the databases through normal SQL toolsets.

Taking their cue from the Active Directory (AD) and Web teams, the Database Administrators have also rolled out their SQL servers onto IaaS Virtual Machines, choosing to host them in the South Central U.S. region as well from a performance standpoint.

One of the newer departments that has recently been tasked with moving servers into Azure have started to build VMs while hosting them all in a single storage account. They have around 35-40 VMs already, but anticipate continued growth.

  
*Figure 2 – LitWare Inc.’s Storage Account Configuration*

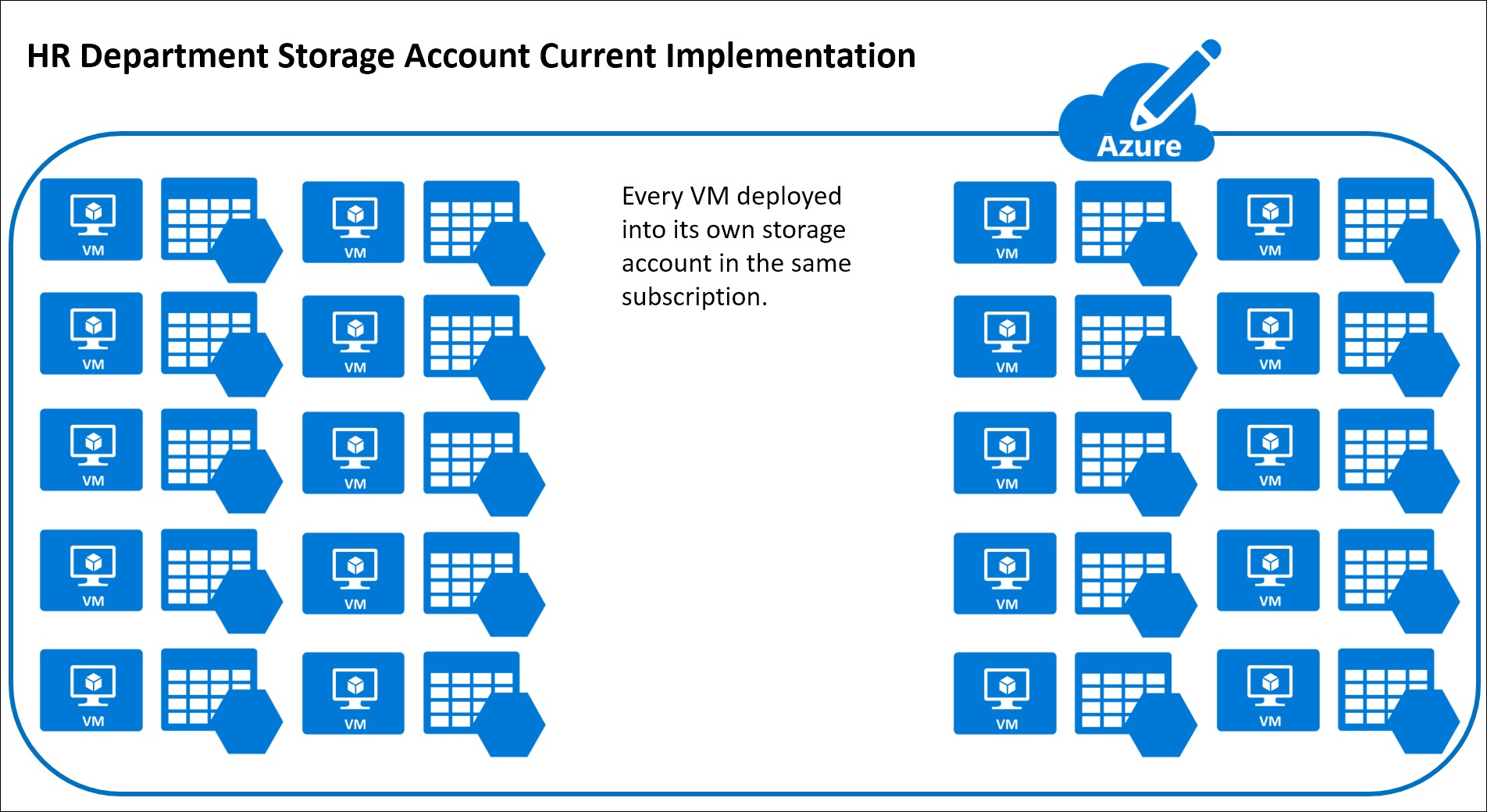
LitWare Inc. is currently connected via a Windows Server Routing and Remote Access Service (RRAS) VPN connection to Azure via a Site-to-Site Gateway in the South Central U.S. location. They are looking for options to provide redundancy for the hybrid connectivity to Azure due to some recent connectivity issues.

While this has served them well, there are some personnel who are beginning to be concerned that all of the servers are located in one region. While they know the Azure Datacenter is located in San Antonio, the recent floods in the Houston area have caused concern for key personnel. Many are questioning if this is such a good idea for LitWare Inc. Janet Lewis (Business Continuity Team Director) says that, “It appears that while services have moved to the cloud, the overall paradigm hasn’t moved from the single Datacenter model.”

Over a recent 3-day Holiday weekend, there was an incident with one of the Active Directory Domain Services (AD DS) Domain Controllers (DCs) where the disk drive housing the AD DS database file filled up and corrupted the copy of the AD DS Database (DB). This prompted a high-priority support call to Microsoft. While the damage was mitigated, the team was fortunate that the consequences were minimal.

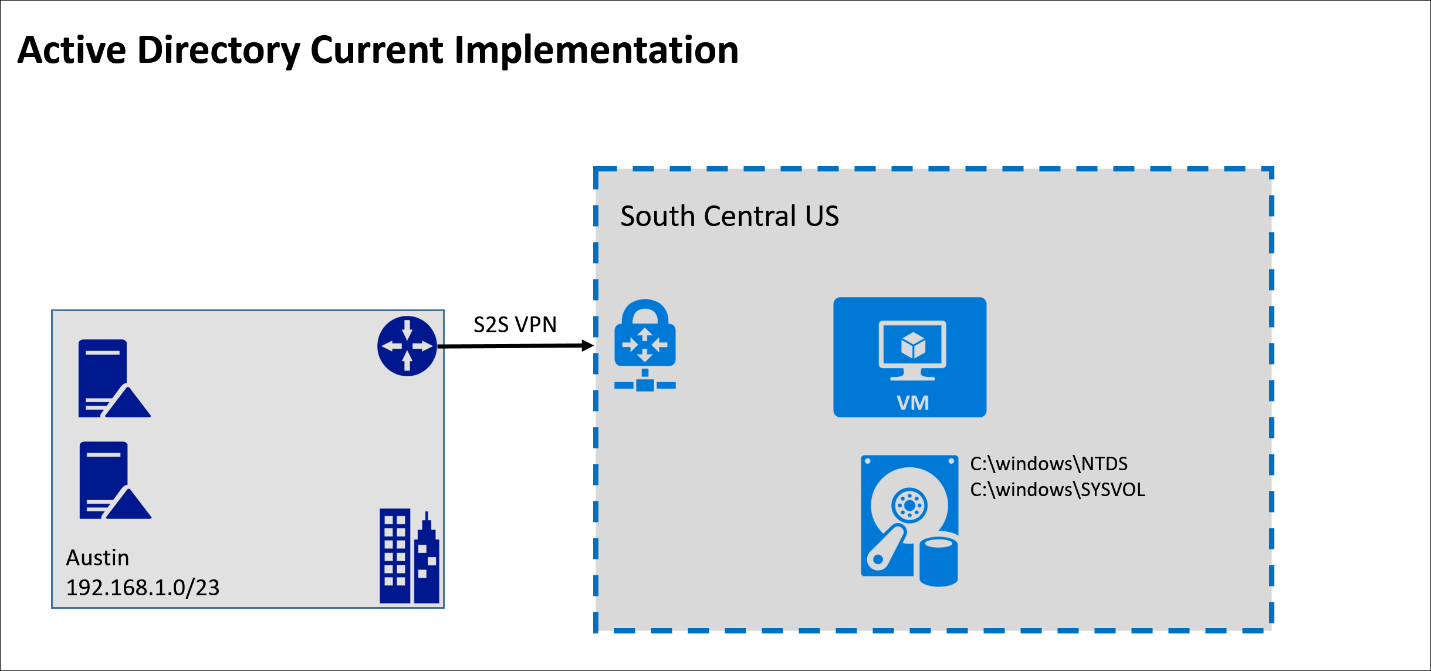
Retroactively, checks were made on some other IaaS disk drives and there were a number of them that were getting close to filling up due to teams not proactively monitoring their role servers. Key team members are now calling for a proactive approach to monitoring Operating System (OS) disk and data disk free space as well as other items.

The Human Resources (HR) team has requested that they move their server infrastructure into Azure and the process has begun. Their organization has a policy that they create a new storage account for each VM in the subscription. They have deployed about 40-50 VMs but anticipate growth that will more than double the size of their deployment numbers.

  
*Figure 3 – LitWare Inc.’s HR Department Storage Account Configuration*

Richard Wade (Infrastructure Lead), would really like to see a way for the overall Azure infrastructure to be made resilient so as to be able to recover from a region-wide service disruption. He also is highly interested in protecting against data corruption or even accidental deletion of data or virtual machines.

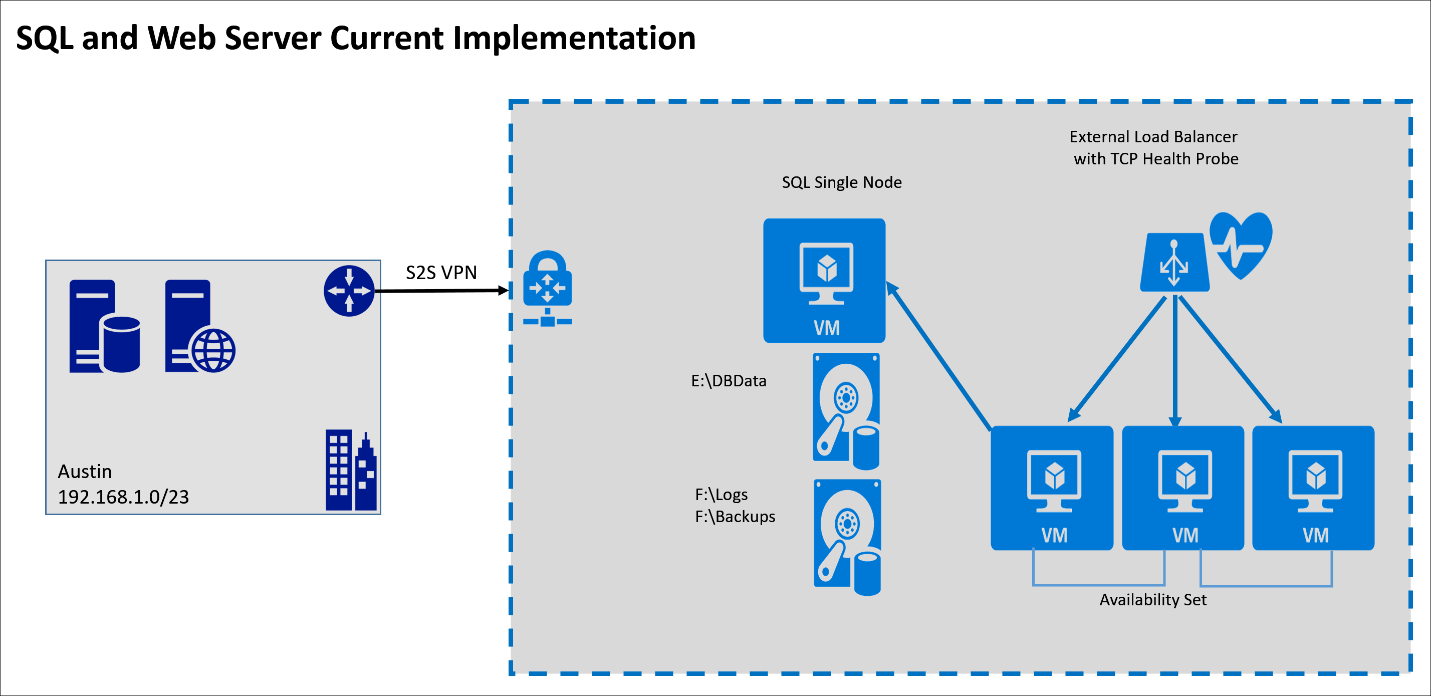
For the current Active Directory Azure implementation, the team has deployed a single AD DS DC in the South Central U.S. Region. It is running on a D1 Standard Instance with only the OS Disk. Both the NTDS folder containing the Active Directory DB and the System Volume (SYSVOL) folders are located on the OS disk, or drive C:\. No additional configuration changes were made to the IaaS VM for this DC.

  
*Figure 4 – LitWare Inc.’s Current Active Directory Configuration*

Additionally, the Azure SQL and Web site implementation were combined into the same South Central U.S. region as mentioned earlier. SQL has been deployed as a Single Node server with multiple disks. One disk is utilized for the data, the other disk is for backup and log file storage. The team configured SQL backups to be stored on geo-replicated storage in Azure on Standard storage.

They have deployed a load balancer for the web servers and configured a default health probe to monitor the servers in the load balanced pool. When they need scalability, they manually configure another web server and often leave it running even after the need for the scaling has long since passed.

LitWare Inc. has received multiple complaints from customers at times when they have intermittently received HTTP 500 errors on the website. Upon investigation, it was discovered that a recent deployment failed on one of the servers in the farm and resulted in files not being correctly copied to this server.

*  
Figure 5 – LitWare Inc.’s Current SQL and Web Server Configuration*

LitWare Inc.’s business critical applications include:

* Authentication and Authorization infrastructure for the organization.
* The web site for the employees and the customers to order parts, repairs, and provide support.
* This site allows for the tracking of the parts and support incidents.
* The database that supports the website for finances, ordering, accounts receivable, and customer information.
* The website and database also provide sales leads and a catalog of current inventory for ordering.
* 3rd party manufacturing plants and factories access their data via the interface of the website as well.

### Customer needs

1. Identify the infrastructure requirements that should to be configured to provide redundancy and resiliency to the web servers, the database servers, and the authentication and authorization servers.
2. Identify how LitWare Inc. could attain resiliency in their legacy application and require an SLA of 99.9% what pre-requisites are required to achieve this in Azure? What limitation does this solution introduce and how could you provide a work around for this?
3. Identify IaaS components, resources and instances in Azure that can provide the features of resiliency for the organization.
4. A plan of resiliency for recovery from a region-wide service disruption.
5. A plan for recovery from data corruption or accidental deletion.
6. Backup plans for all server roles and functions.
7. Have a good storage policy in place for the anticipation of growth in Azure.
8. Monitoring option for issues that may arise on the servers and also in Azure.

### Customer objections

1. “Cost is a huge concern for us. We have already deployed server instances into Azure. We want to avoid any unnecessary expenditures and duplication of effort.”
2. “The web application needs to have the ability to scale as we grow. What aspect of the cloud will allow this to be a reality?”
3. “Downtime is becoming more of an issue for us due to development and production environments not being separate. We need to separate these from one another to avoid outages.”
4. “Connectivity bandwidth is becoming an issue for our self-hosting of the applications, ordering system, support website, etc. We’re concerned that the cloud maybe constrained as well.”
5. “Our current backup/recovery system works just fine.”
6. “We already have a point of presence for our customers that we don’t want to change. How can we provide cross-region resiliency without impact to our customers?”
7. “We are very concerned about the disk space issue that occurred earlier with our ADDS DCs and nearly our Web Servers and Database Servers. Will this be addressed per the resiliency plan?”

## Step 2: Call to action: Design a proof of concept solution

**Outcome:**

Design and prepare to present a solution to the target customer audience in a 15-minute chalk-talk format.

Timeframe: 60 minutes

**Design**

The desired outcome is to have a complete resilient deployment for the authentication and authorization tier, the Web Server tier, the SQL Server tier and other components. Redundancy and protection in case of failure is the main goal for all components of the design. The design should include network resiliency, as well as backup and restore methods in case of failure of the physical or virtual machines. Plan your architecture accordingly. Address the customer concerns and objections in the architecture design.

Directions: Design the solution architecture by drawing it on the board, and separately provide insight into how you will address the following requirements. Identify the steps needed to implement a proof of concept for the proposed solution(s) as well as what would need to be demonstrated to stakeholders.

### Design for Resiliency in Azure

* Consider storage account resiliency. What would best suit the needs for LitWare Inc.? LRS, GRS, RA-GRS? Document why you chose the option you did.
* What changes, if any, will be needed to provide resiliency for the Active Directory servers? Diagram how many and where they need to be placed.
* How will you address the need for resilient Web and Data tier roles?
* How would you address the needs of the legacy application, what storage tier and limitations do you have to work around?
* What are you going to do for business continuity and making sure the company can continue to function with a server issue or a database corruption?
* Diagram how to provide for resilient web presence in multiple regions. What resource is needed? How will it be configured.
* Document how backups should be configured for SQL? For IIS? For AD?
* Provide LitWare Inc. with documentation needed surrounding service limitations, quotas, subscription limits.
* Inform LitWare Inc. with the options Azure provides for monitoring. Document what server roles could benefit from monitoring and what specifically could be addressed via this information.
* How can you help resolve the scalability and file consistency on the web farm VMs?
* Make sure your design takes into account the potential global growth and facilities of the organization.
* Make sure your design takes into account reasonable RTO and RPO values.
* How would you check in the Azure Portal for recommendations on the solution deployed and suggestions on changes to be looked at? What service, currently in preview, allows the user to view these recommendations?

### Virtual Network design in Azure

LitWare Inc. has agreed to provide route-based VPN gateway hardware or software devices for all locations.

* Document and diagram how you will build redundant Virtual Networks for LitWare Inc.
* How will you design the address space and subnets to support LitWare Inc.’s requirements?
* How will you configure regional or location redundancy within Azure?
* What Azure features would you utilize to protect traffic between on-premises network and the Azure VNET and subnets?
* Document what rules (ACLs) you would put in place for protection. What ports would you open and why?
* Diagram the options for providing highly available Virtual Network Gateways.
* How can you provide redundancy and resiliency in the Site-to-Site VPN connectivity from LitWare Inc.’s offices to Azure?

## Step 3: Call to action: Present the solution

**Outcome**

Present a solution to the target customer audience in a 10-minute chalk-talk format.

**Presentation**

Timeframe: 60 minutes

**Directions:**

1. Pair with another table.
2. One table is the Microsoft team and the other table is the customer.
3. The Microsoft team presents their proposed solution to the customer.
4. The customer makes one of the objections from the list of objections.
5. The Microsoft team responds to the objection.
6. The customer team gives feedback to the Microsoft team.
7. Tables switch roles and repeat Steps 2–6.

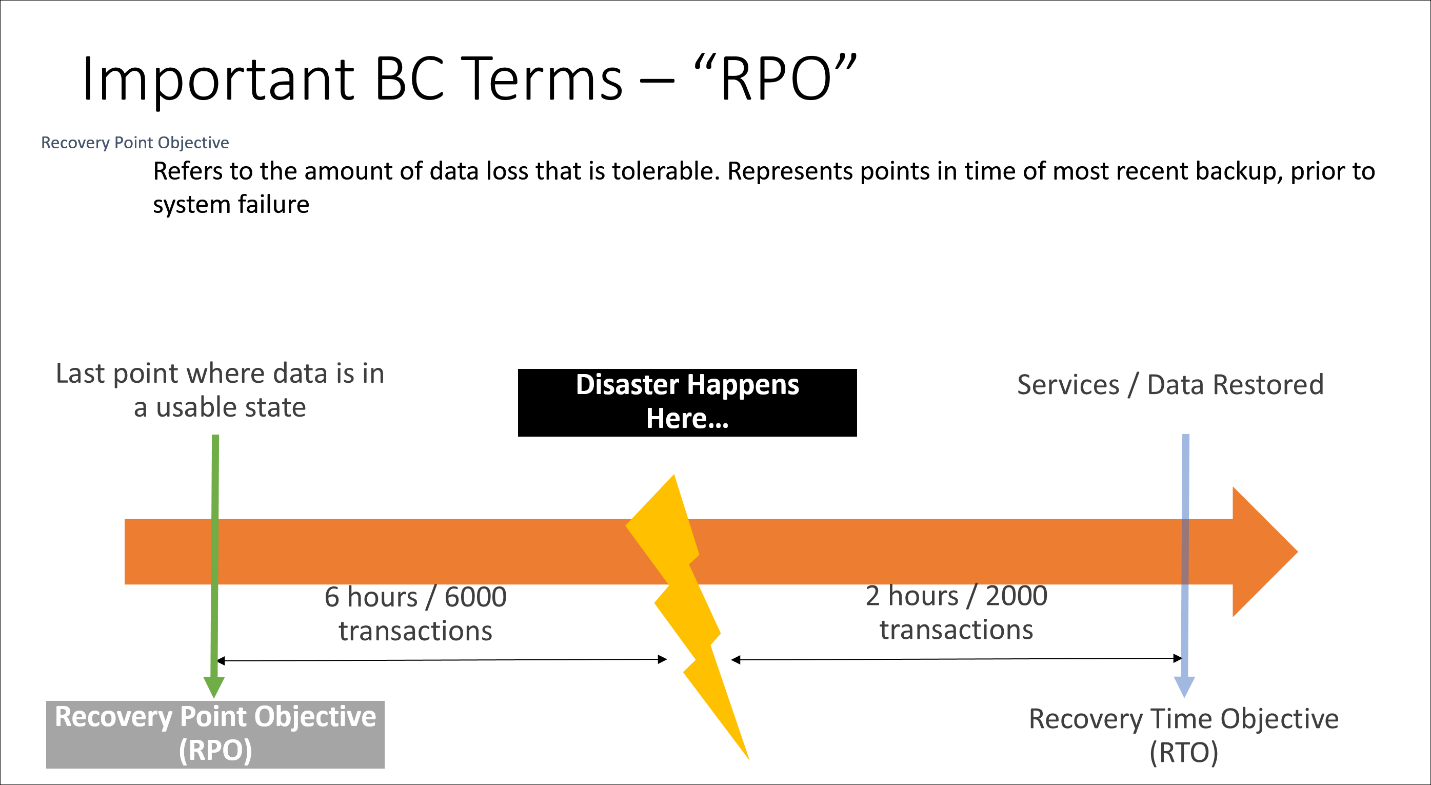
## Wrap up

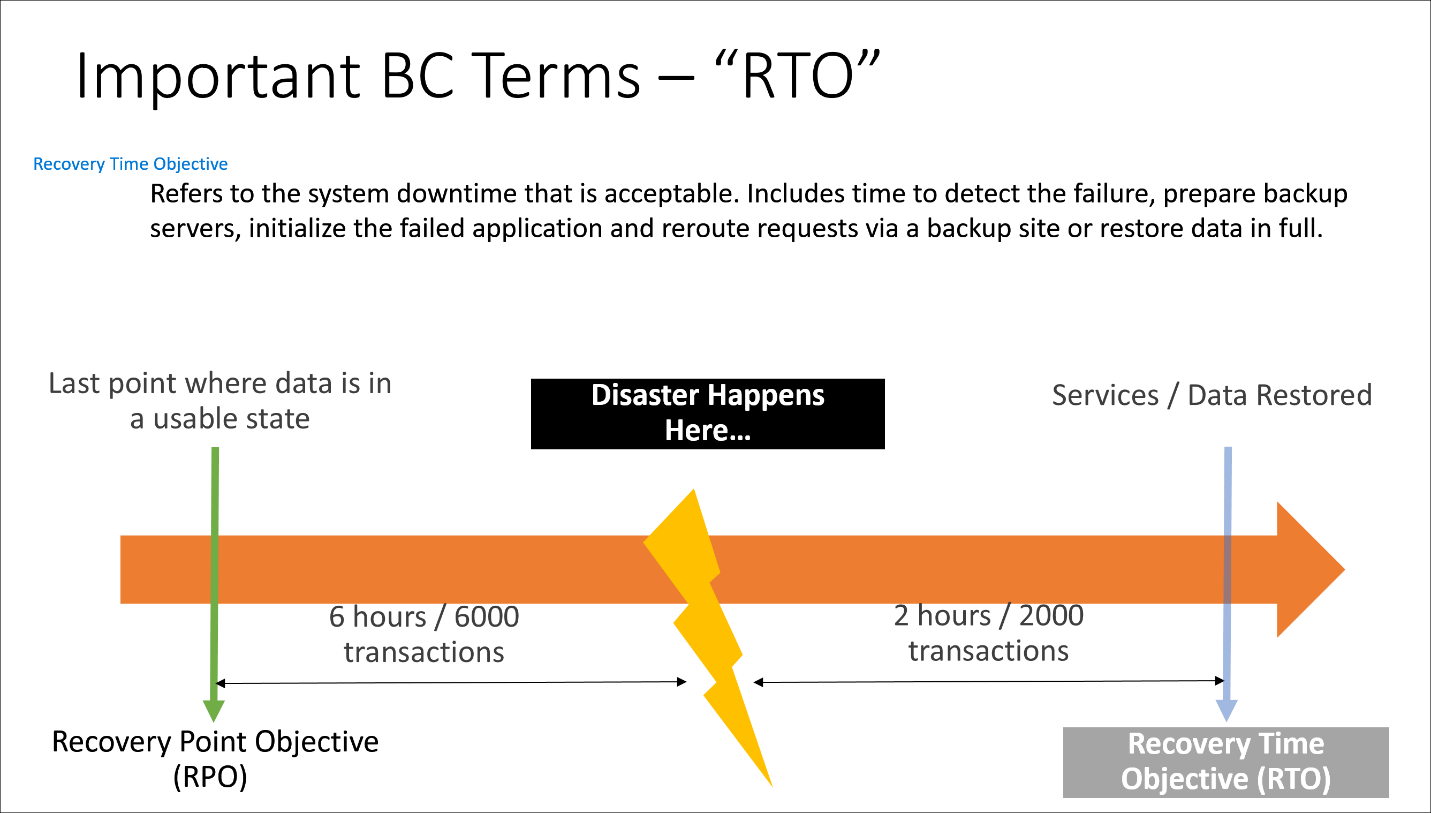
Timeframe: 15 minutes

* Tables reconvene with the larger group to hear a SME share the preferred solution for the case study.

### Additional references

| **Description** | **Links** |
| --- | --- |
| Microsoft Azure Reference Architectures | <https://docs.microsoft.com/en-us/azure/guidance/guidance-architecture> |
| High availability checklist | <https://docs.microsoft.com/en-us/azure/resiliency/resiliency-high-availability-checklist> |
| Design for scalability and high availability on Microsoft Azure | <https://myignite.microsoft.com/secondscreen/3179> |
| Azure resiliency technical guidance | <https://azure.microsoft.com/en-us/documentation/articles/resiliency-technical-guidance/> |
| Azure delivers the need for high resiliency to ensure the 24/7 availability of web services | <https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=25135> |
| United Airlines Boosts IT Efficiency, Business Resiliency with Private Cloud Solution | <https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=11155> |
| Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines | <https://msdn.microsoft.com/en-us/library/azure/jj156090.aspx> |
| Running your Active Directory in Windows Azure | <https://channel9.msdn.com/Events/TechDays/Techdays-2014-the-Netherlands/Running-your-Active-Directory-in-Windows-Azure> |
| Running VMs for an N-tier architecture on Azure | <https://docs.microsoft.com/en-us/azure/guidance/guidance-architecture> |
| Azure SQL Database DTU Calculator | <http://dtucalculator.azurewebsites.net/> |
| SQLIO Disk Subsystem Benchmark Tool replaced with DiskSpd.exe | <https://www.microsoft.com/en-ca/download/details.aspx?id=20163> |





# Building a Resilient IaaS Architecture leader guide

## Step 1: Review the customer case study

* Check in with your table attendees to introduce yourself as the proctor.
* Ask, “What questions do you have about the customer case study?”
* Briefly review the steps and timeframes of the workshop.
* Ready, set, go! Let the table participants begin.

## Step 2: Call to action: Design the solution

* Check in with your tables to ensure that they are transitioning from step to step on time.
* Provide some feedback on their responses for business needs and design.
  + Try asking questions first that will lead the attendees to discover the answers on their own.
* Provide feedback for their responses to the customer’s objections.
  + Try asking questions first that will lead the attendees to discover the answers on their own.

## Step 3: Call to action: Present the solution

1. Determine which table will be paired with your table before Step 3 begins.
2. For the first round, assign one table as the Microsoft team and the other table as the customer.
3. Have the Microsoft team present their solution to the customer team.
   * Have the customer team provide one objection for the Microsoft team to respond to.
   * The presentation and objection should be no longer than 10 minutes.
4. Have attendees on the customer team give feedback to the Microsoft team.
   * The feedback should be no longer than 5 minutes.
   * If needed, you may also provide feedback.
5. For the second round, have the tables switch roles and repeat Steps 3–5.

## Wrap up

Have the table attendees reconvene with the larger session group to hear a subject matter expert (SME) share the following preferred solution.

**Target Audience**

* Lewis Franklin, Head of Infrastructure and Operations
* Richard Wade, Infrastructure Lead
* Janet Lewis, Business Continuity Team Director

**Preferred solution**

The solution for LitWare Inc. involved several technologies, including:

* Site-to-Site VPN Gateway for connectivity from on-premises corporate home office and branch office locations.
* Site-to-Site VPN Gateway for connectivity between Azure Regions deployed for resiliency.
* Resiliency integrated into each aspect of the deployment and architecture to provide the opportunity for high SLA and performance. These include:
  + Multiple Storage accounts in each Azure region.
  + Legacy Application deployed to Azure in a VM with premium storage, necessary to achieve 99.9% SLA. Premium storage accounts currently only support LRS, so a snapshot of the blob by using Snapshot Blob REST API method then a Copy Blob of the snapshot to another storage account. <https://docs.microsoft.com/en-us/azure/storage/storage-premium-storage> and https://docs.microsoft.com/en-us/azure/storage/storage-premium-storage#snapshots-and-copy-blob
  + Virtual networks deployed in both Azure regions.
    - Subnets defined Apps, Data, Identity and VPN Gateway.
  + VPN connectivity between Azure and LitWare Inc.’s offices.
  + Backup Vaults in each of the Azure Regions to provide backups for the servers.
  + 4 domain controllers deployed in Azure, two in each region.
  + 2 Web VM Scale Sets deployed, one in each region.
  + 4 SQL virtual machines deployed in two Azure Regions, each with a witness.
  + SQL configured with always-On.
  + All machines deployed in availability sets for fault domain and upgrade domain protection.
  + Load balancers configured with health probes to remove servers that do not respond out of rotation.
  + Traffic Manager configured in priority mode for failover should the need arise.
  + Alerting configured to provide disk space alarms.
  + Backups configured for all IaaS VMs.
  + Check for Azure Advisor recommendations in the Azure Portal – the Azure Advisor, currently in preview, provides steps to take to optimally configure your Azure resources. These recommendations, which are made based on best practices, could in the long run, assist in reducing costs, increasing performance and security.

### Azure Virtual Network Configuration

In an Azure Region closest to Austin, e.g. South Central U.S., a VNET is deployed and configured with the address space 10.0.0.0/16 and with subnets for the following tiers:

* Apps: 10.0.0.0/24
* Data: 10.0.1.0/24
* Identity: 10.0.2.0/24

Also, create a GatewaySubnet for a VPN Gateway to allow for Site-to-Site VPN connectivity between Azure Regions with the following information:

* GatewaySubnet: 10.0.3.0/29

Secondarily, in North Central U.S., a VNET is deployed and configured with the address space of 172.16.0.0/16 and with subnets for the following tiers:

* Apps: 172.16.0.0/24
* Data: 172.16.1.0/24
* Identity: 172.16.2.0/24

Also, create a GatewaySubnet for a VPN Gateway to allow for Site-to-Site VPN connectivity between Azure Regions with the following information:

* GatewaySubnet: 172.16.3.0/29

Connections are then created between the gateways allowing region-to-region communication, replication, backup copies and redundancy of roles for the SQL servers, IIS servers, and AD DS DCs.

Also, after this is completed, the corporate network at LitWare Inc.’s location can also be connected via Site-to-Site VPN and allows for resilient IaaS infrastructure to be deployed into Azure.

**Resilient Benefits:**

* VNETs in the paired regions allow for a resiliency of network connectivity in the event of an Azure regional networking issue. Building redundancy allows for the DCs, the Web Servers and the Database to all be connected and usable even if there is one region affected.
* Subnets allow for the segmentation of the tiers and later on, hardening with Network Security Groups (NSGs) via subnet for the role servers. The Gateway Subnet allows for the use of VPN Gateways to provide a connection between regions for AD replication, SQL Replication and failover.

### Virtual Network Gateway Configuration Details

Within Azure, create a virtual network gateway that will allow for connectivity to LitWare Inc.’s Austin office site and also allow for connectivity for the three branch office sites via Site-to-Site connectivity. The gateway type is defined as VPN and the VPN type is defined as Route-based to allow for multiple Site-to-Site (S2S) connections.

Route-based VPN Gateway has to be a choice here for the option of multiple gateway Internet Protocol Security (IPSec) tunnels. The Gateway Stock Keeping Unit (SKU) needs to be the correct choice as well. Decisions on the SKU need to be based on bandwidth and the flow of data so be sure and work with the customer to monitor connectivity and bandwidth for the application for the appropriate choice.

In this scenario, a Standard SKU gateway would suffice for the number of connections and the bandwidth options but as they continue to grow, they should consider the High Performance SKU for bandwidth considerations.

It also is a mid-line price to assist in some cost savings as a High Performance SKU is not currently required. See: <https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpngateways/#gwsku> and <https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpngateways/#vpntype> for more information.

**Resilient Benefits:**

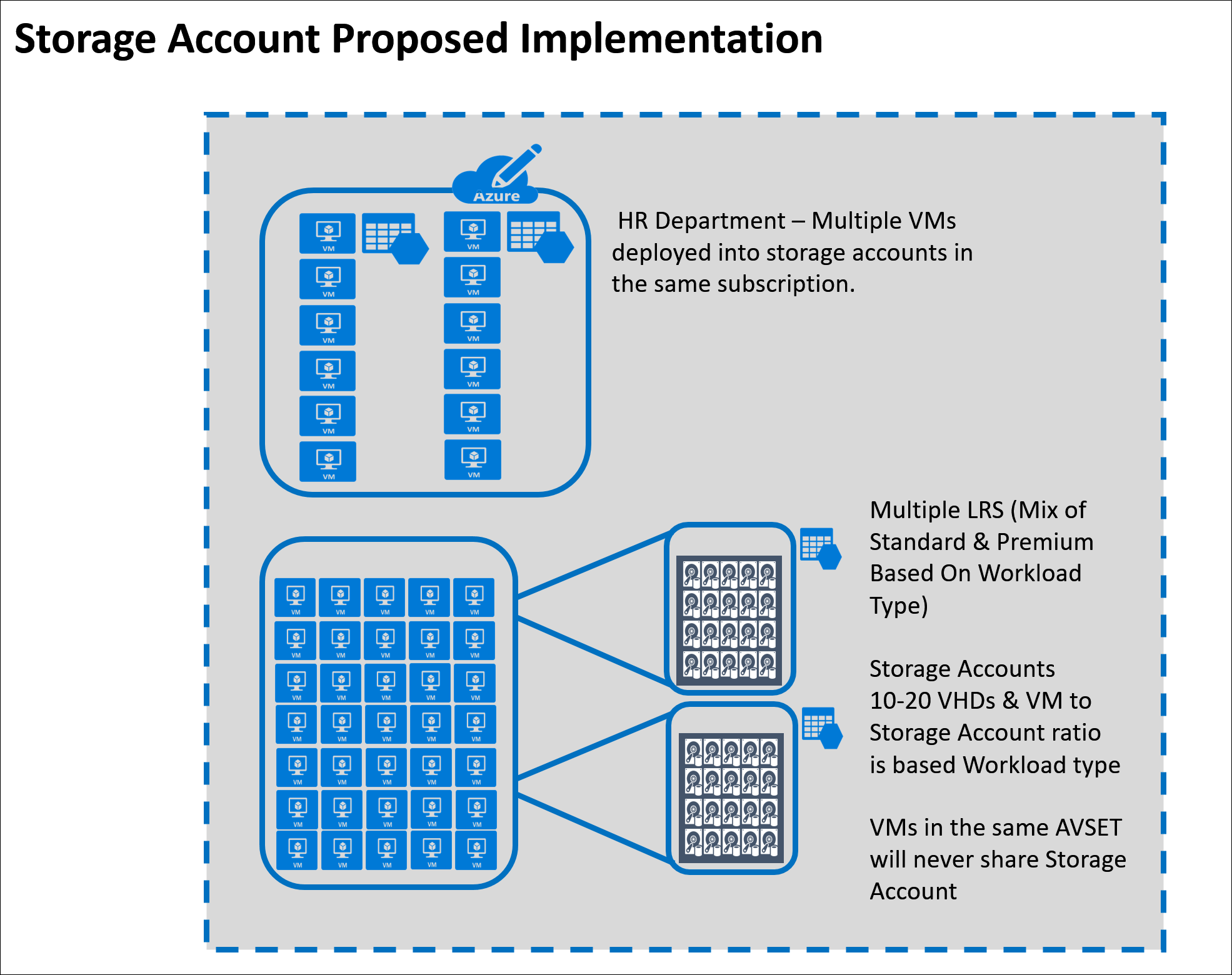
* Providing Route-based VPN gateways allows for the connection all three branch offices and the corporate office to connect via VPN. It also allows for the two regions to connect. There is even some room for growth and makes the connectivity resilient in case of some network event at the corporate office or a branch office.
* Configuring Highly Available (HA) VPN can be done using RRAS VPN and Azure VPN Gateways and clustering them for VPN redundancy. See the following: <https://azure.microsoft.com/en-us/blog/building-a-highly-available-on-premises-vpn-gateway/>

### Storage Account Configuration Details

Moving beyond using only one storage account is a must for Liteware. They will need to adjust this position moving forward. Also, using Premium Storage for applications that require Stateful and mission critical workloads is recommended. It is possible to use a mix of Standard and Premium Storage where is makes sense, but using Premium storage should be the default moving forward for them with no more than 40 disks.

For the department that was moving their servers to Azure and only using a single storage account, remember the default subscription and service limits, quotas, and constraints. They would quickly be beyond the default limits (> 40 disks standard or > 35 TB premium) should they continue down this path. They need to redesign their process quickly to address this.

The HR team also, as they created a new storage account for each VM will quickly get beyond the subscription limits for storage accounts per subscription. Their policy will need to be modified to correct this to help with their resiliency and storage needs. See the following for current limits: <https://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/>

  
*Figure 6 – Proposed HR Department Storage Account Configuration*

Make note of the Geo-Replication region mappings should your data require regional affinity with the storage. See the table for the primary and secondary location pairings in this article: <https://azure.microsoft.com/en-us/documentation/articles/resiliency-technical-guidance-recovery-loss-azure-region/>

**Resilient Benefits:**

Paired Regions allow for RA-GRS (Read-Access Geo-Redundant Storage) so there are 3 copies of the data in one region and three copies of the data that are readable in the paired region. LitWare Inc. would be able to read the copies of the data at any point were there a need.

* Creating multiple storage accounts allow for better allocation of storage and also replication for recovery purposes. This will also assist in making sure that they do not exceed the storage limits per subscription or per storage account.
* Site Recovery Vault replication across regions would also be a feature that would benefit from a multi-region storage policy.
* Writing data to the storage accounts and putting retention policies in place along with Role Based Access Control (RBAC) and Locks will also protect against deletion.
* Quick recovery time in case of accidental deletion or data corruption is also a benefit.

### Legacy Application

The existing legacy application could be moved into an Availability Set; however, it does not support the data being accessible across multiple VM’s. Azure introduced single instance SLA’s for VM’s, so moving this application across to Azure would now result in a 99.9% SLA. As the existing hardware on which it’s currently deployed on site is ageing, moving this application would benefit from reduced hardware expenditure through a refresh.

The application would eventually require a re-write to take advantage of the advanced features available in Azure. This could be doing once the application was in Azure.

To be able to achieve the SLA provided in Azure, the disks used for the VM must be premium storage disks. There is a limitation on Azure premium storage accounts such that they only support LRS. As such a mechanism to copy the blob across to another region needs to be setup. A backup of the VM will also be scheduled.

**Resilient Benefits:**

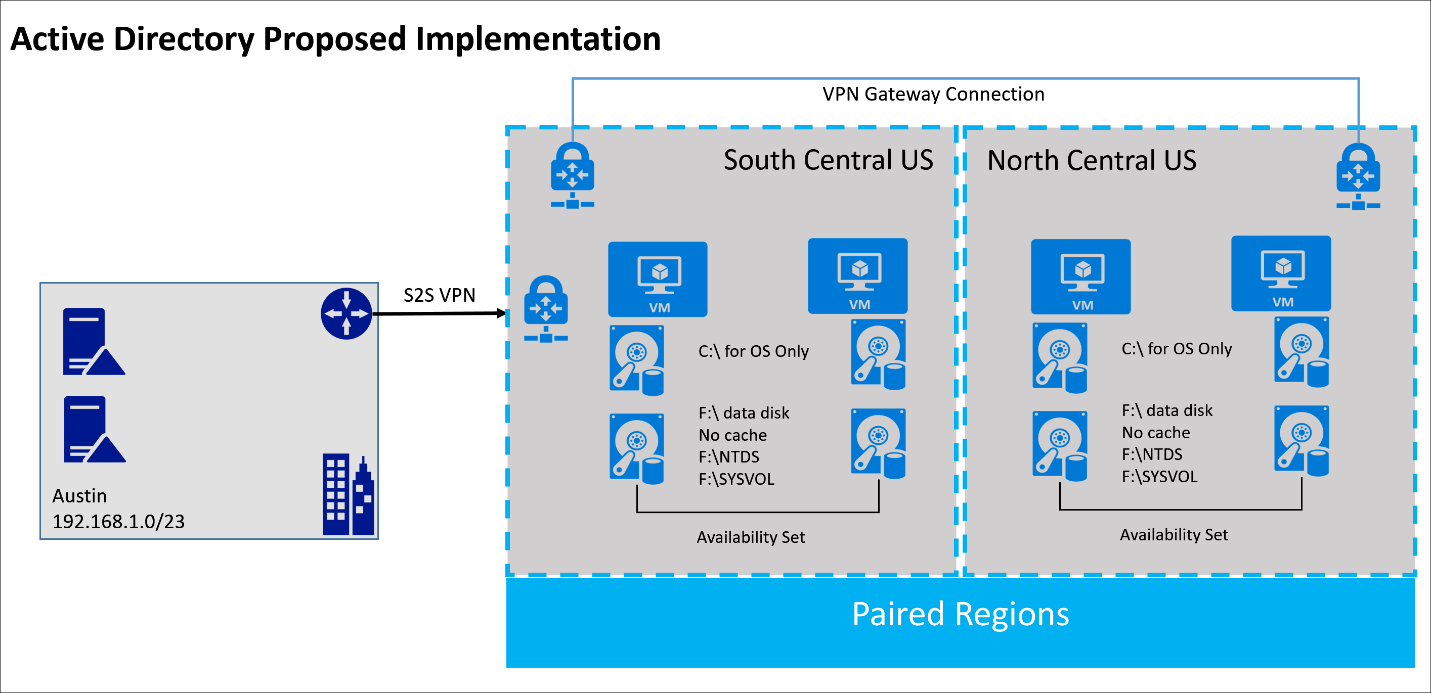
* Single instance VM now supported with a 99.9% SLA
* Premium storage account must be used and replicated across to another storage account

### Active Directory Configuration Details

Active Directory Domain Services Domain Controllers are deployed into Azure as IaaS Virtual Machines. These are extensions of the on-premises AD DS DCs and allow for resiliency for the authentication and authorization mechanism that LitWare Inc. employees today.

Configure multiple VMs as Domain Controllers in the South Central U.S. region and should the need arise for DCs to be located closer to the branch offices, this is easily configured by creating additional DCs in the West, East and Central regions. Remember to configure the Sites and Services option should this be the desire of LitWare Inc.’s team.

Each Domain Controller will be configured with a Data Disk for the AD DS database and will be configured to backup via Azure Backup for disaster recovery and business continuity. To avoid any issue with the AD DS DB, this data disk needs to be configured with having caching set to NONE.

  
*Figure 7 - Proposed Active Directory Resiliency Architecture*

Multiple AD DS DCs need to be deployed in multiple regions to provide for the correct redundancy options. To help protect the DCs from any planned or unplanned downtime in Azure, they will be deployed in an Availability Set to spread the VMs across Azure Racks.

Make sure that redundant DCs are also deployed in the North Central U.S. region to provide the authentication and authorization needs for the resources deployed in that region. Be sure to configure the ADDS Sites and Services to have the IPs and sites for the AD DS DCs housed in Azure.

For details on restoring ADDS DCs see the following: <https://azure.microsoft.com/en-us/documentation/articles/backup-azure-restore-vms/#restoring-domain-controller-vms> and <https://technet.microsoft.com/library/virtual_active_directory_domain_controller_virtualization_hyperv(v=ws.10).aspx#backup_and_restore_considerations_for_virtualized_domain_controllers>

**Resilient Benefits:**

* Storing the AD files on a data disk with caching set to None will keep the AD DS database and SYSVOL from any potential corruption due to caching.
* Adding DCs into an availability set will spread them across fault domains and update domains so that authentication and authorization servers are highly available.
* Azure Service Level Agreement (SLA) is not available at all without virtual machines in availability sets.
* Deploying multiple DCs in multiple regions allows for redundancy in each region in the event of a regional Azure issue.
* Replication across regions also allows for disaster recovery should the need arise and faster recovery of the AD DS database.
* Removing the DC that is not in an availability set helps avoid a single point of failure for that VM.
* Using Azure Backup, even with the caveats on restoring, allows for another layer of redundancy for recovery options.

### SQL Always-On Configuration Details

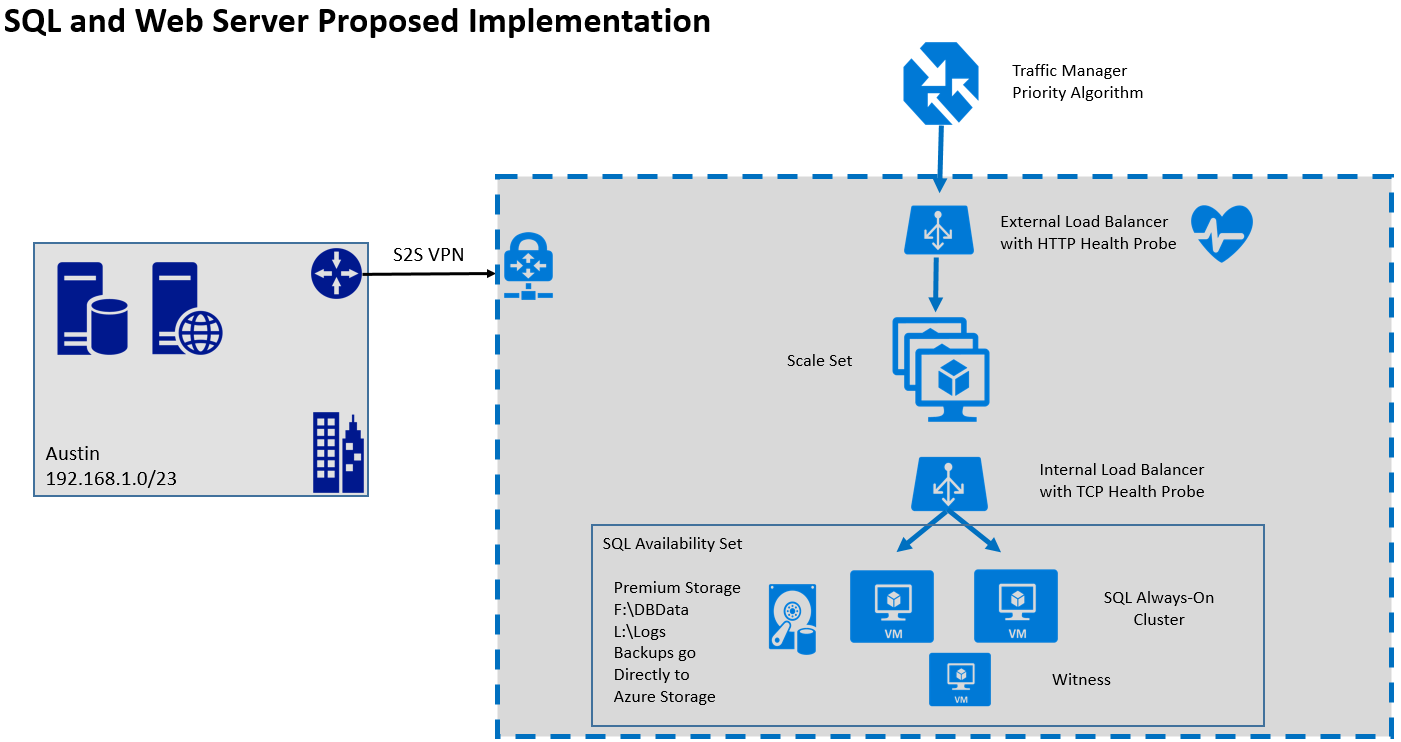
SQL will need to be backed up via SQL backup methods, but will need to be configured on a new VM Always-On cluster with the use of an internal load balancer. LitWare Inc.’s configuration of geo-replication for the storage will need to be addressed as geo-replication cannot be used to store a backup from SQL server.

Also, database and log files on separate disks cannot use geo-replicated storage unless they are on the same disk. Backing up the SQL database directly to Azure Blob storage is recommended here for speed and also for retention and restoration access.

Their choice of standard storage vs. premium storage should be reconsidered as well. Unless there is a change to premium storage, they may run into some performance issues in their database use as they continue to grow.

It is highly recommended that LitWare Inc.’s SQL IO be determined to then map the relevant IO to a premium based offering. Premium storage is the choice in this configuration or the users and customers will not be pleased with the responsiveness of the database in the web application.

Configuration of Always-On clusters across regions is also the recommended design which will allow for resiliency, failover, and even some performance benefit across regions. Were SQL servers deployed in multiple regions that then communicated to the database through a VPN tunnel to a single database, the performance would suffer greatly.

**

*Figure 8 – Proposed SQL and Web Server Architecture*

**Resilient Benefits:**

* Providing SQL Always-On will give access to the database in a highly available manner. Replacing the single node server with multiple disks in the first region with an Always-On cluster provides resiliency for the data in the first region.
* Setting the disk configuration to be correct allows for correct backups to be taken as the configuration in the original deployment did not provide the correct settings for successful backup.
  + Never use the E:\ drive on an Azure VM as some Azure Regions have Host machines that contain DVD Drives. Always use F:\ or higher. If a machine moves to a Host like it, your SQL Data would be at the wrong drive letter and it would not start.
  + Backing Up Directly to Azure Blob Storage is fast and supported by SQL Server. In addition, it does not use space on your Premium Storage drives.
  + Seperating the logs from data is a long known best practice for SQL Server.
* Creating a second region Always-On cluster provides redundancy and resiliency for the cluster and allowing that data to be synchronized across regions helps provide LitWare Inc. with the ability to failover the database between regions should that need ever arise.

### Web Server Configuration Details

The IIS Web Servers will be configured in the Apps Subnet and built on IaaS VMs. To help manage the load and provide performance options, the servers will be deployed into a Scale Set within Azure. This will allow LitWare the option to scale-up, scale-out, and even scale-down and scale-in based on the need. It will cease LitWare Inc.’s practice of scaling manually as it is rife with issues and lacks the automated scaling that can be provided otherwise for resiliency.

LitWare Inc.’s use of an Availability Set for the Web farm VMs should be applauded. This allowed them to utilize a Load balancer, but they configured the Load Balancer to have a Transmission Core Protocol (TCP) health probe which missed the Hypertext Transfer Protocol (HTTP) errors on the one server which failed to copy the files correctly. Availability Sets provide protection and resiliency against unplanned and even planned downtime. Spreading the VMs across fault domains and update domains for protection against failures and upgrades/updates to Azure.

Change the Health Probe on the Load Balancer to be focused on HTTP instead of TCP and it will monitor for 200s in IIS logs. If anything other than a 200 is detected, the 500 the customers complained about for example, then that server will be removed from the rotation until success is determined again.

**Resilient Benefits:**

* Moving the Health Probe from TCP to HTTP on the load balancer gives a deeper more application centric view into the web server health. It will help avoid any intermittent problems that customers experienced in the past.
* Providing Scale Sets for the Web farm deployment allows for configurable scaling (up and down) based on LitWare Inc.’s desires. It allows for this to occur automatically without manual intervention and will help with the issue of deploying manually and then typically not remembering to remove the extra servers when they are no longer needed.
* Scale Sets are automatically deployed into availability sets so the servers as they scale will be spread across update and fault domains via the Azure fabric.

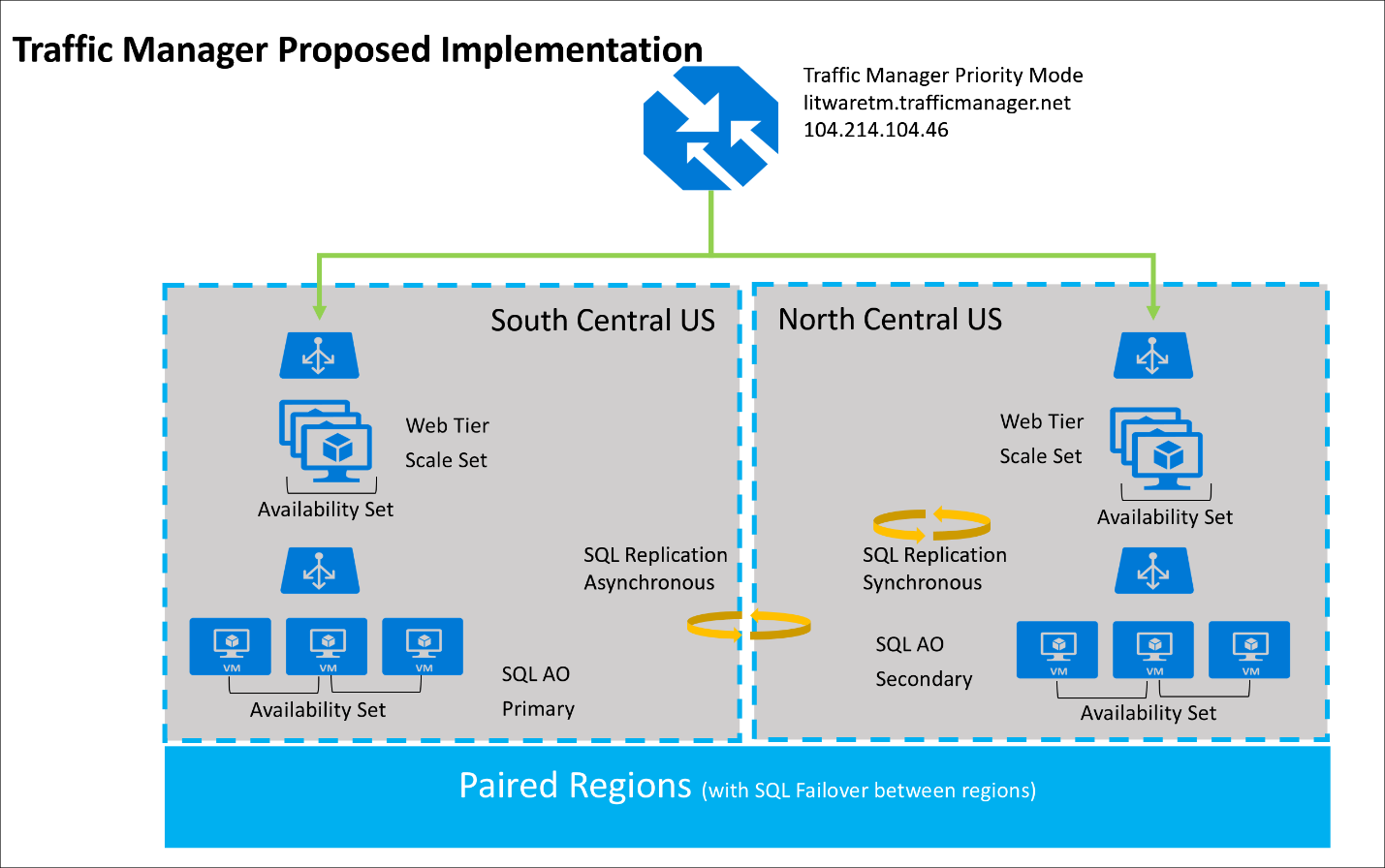
### Traffic Manager Configuration Details

LitWare Inc.’s desire to provide the web application to their employees and external customers from multiple regions in Azure, traffic manager can be employed to provide this solution. This will help provide the DNS based traffic distribution needed to meet the needs for LitWare Inc.

Deploying a Traffic Manager resource in Azure and configuring the distribution algorithm to be priority, this will allow LitWare Inc. to set the priority of the South Central U.S. region version via Canonical Name (CNAME) record redirection to the Traffic Manager. The URLs from both Azure region addresses are set in the Traffic Manager profile.

If the site which is configured as the highest priority has an issue and becomes degraded, the secondary priority site will take the traffic until the primary site is repaired and becomes available again. This will provide the resiliency needed for using the web application both regions in Azure.

Care should be taken in configuring the Domain Name System (DNS) settings for the Traffic Manager. Make sure to set the Time to Live (TTL) for DNS in the Traffic Manager profile at an appropriate level so that the time out will not affect the function of the use of the traffic manager deployment and its use in resilient web presence for LitWare Inc.’s application.

*  
Figure 9 – Proposed Traffic Manager Architecture*

**Resilient Benefits:**

* Traffic Manager in Priority Mode will allow LitWare Inc.’s web presence be seen regardless of which region it is running in. Priority will allow for one region to be the default and should something happen to that region, it will failover to the second region automatically.
* Traffic Manager used in conjunction with the load balancers allow for traffic to route around components of a given tier that are not functional.
* Traffic Manager could also be used to take one of the regions out of rotation for maintenance purposes without affecting customer and user connectivity.
* Pointing the endpoints to load balancers allow for an additional layer of resiliency since there are multiple servers on the web tier that will be able to provide the service.
* Traffic Manager could also be used to add non-Azure URLs should LitWare Inc. desire to do this in the future as well.

### Load Balancer Configuration Details

To assist with resiliency, load balancers will be configured so that there is no single point of failure for any of the tiers of the application.

An external load balancer is deployed and configured for the public facing website that will direct the traffic from the Internet through to the web servers providing the application for customers and external users. This load balancer will be setup with a HTTP health probe and will make sure that the servers providing the application are healthy and responding to IIS calls. Should a server not respond with a 200 to the probe, it will be removed from the rotation and continue to be probed until such a time that it responds successfully.

HTTP probes need to point to a specific page of the application that then calls out all dependencies so they can be the successful probe they are designed to be in a web farm environment. Failing to configure this page correctly may cause false positives and defeat the purpose of utilizing the probe. Make sure the application is configured correctly for HTTP probe use.

Internal load balancers will also be used between the VMs for the other tiers so they also cannot be a single point of failure. This builds resiliency for every tier of the application and health probes can be configured on TCP ports for each load balancer to allow for machines which fail to respond to probes to be removed until they respond to probes again and placed back into rotation.

**Resilient Benefits:**

* Load Balancers with properly configured health probes will remove an affected server from rotation until the health condition is resolved and then it will be placed back into rotation.
* This will help monitor the servers automatically and avoid any future issues from incorrect configuration.
* HTTP probes allow for investigation at the IIS level, not just a TCP port response. A server could still be responding on the port, but the file system still have an issue causing the affected server to remain in the rotation.

### Monitoring Configuration Details

While diagnostics and other options do exist in the portal, there are deeper and richer options available within Azure and these link with existing monitoring options from System Center Operations Manager to allow for hybrid monitoring. Operations Management Suite (OMS) is the tool of choice for ways to be up and monitoring quickly. It will help provide a single portal for all management tasks, can be on-boarded in a rapid fashion, integrate with any of LitWare Inc.’s current management tools, enhance System Center, and extend management and monitoring to Azure.

Monitoring of the virtual machines is recommended for LitWare Inc. as they are mainly concerned with the infrastructure and due to their culture of a classic IT shop. Based on their future growth and use of the web application, it is recommended that they also focus on monitoring application level events as well. At a minimum, monitor reads per second, successes, failures and response time. This will be expanded as the company grows and continues to monitor proactively.

OMS will help LitWare Inc. identify, assess and mitigate any missing patches on SQL, IIS, Windows Server, Active Directory, etc. There are options to monitor and apply recommended resolutions for many server types. See the following for details: <https://www.microsoft.com/en-us/cloud-platform/operations-management-suite>

**Resilient Benefits:**

* Operations Management Suite provides a way to get up and running quickly with monitoring of the Azure IaaS deployment for LitWare Inc.
* OMS is the tool of choice in the Azure platform for Virtual Machine monitoring.
* Various options are available to check the status of AD DS DC health, SQL Server health, every server for malware and also for updates that might be missing.
* Fixing issues discovered proactively will help from a resiliency perspective and taking action on alerts in a reactive manner will as well.
* System Center Operations Manager can be tied into OMS to extend existing monitoring solutions.
* Depending on the configuration, backups can also be monitored with OMS allowing for reporting of successful or otherwise results which will aid in resiliency.

### Network Security Group usage

Network security groups (NSGs) will be used to help secure the configuration by limiting traffic flow exactly as a firewall rule does. NSGs may be applied to either individual NICs or to subnets. In LitWare Inc.’s case there will be a single NSG applied to each subnet.

Be sure to reproduce the following charts for both regions VNETs adjusting the destination IP range as appropriate for the 172.16.0.0 address space in the North Central U.S.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Apps Tier NSGs** | | | | | | | |
| **Name** | **Priority** | **Source** | **Protocol** | **Source Port Range** | **Destination** | **Dest. Port Range** | **Action** |
| HTTP | 100 | Any | TCP | Any | 10.0.0.0/24 | 80 | Allow |
| HTTPS | 110 | Any | TCP | Any | 10.0.0.0/24 | 443 | Allow |
| RDP | 120 | 192.168.1.0/23 | ANY | Any | 10.0.0.0/24 | 3389 | Allow |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Tier NSGs** | | | | | | | |
| **Name** | **Priority** | **Source** | **Protocol** | **Source Port Range** | **Destination** | **Dest. Port Range** | **Action** |
| RDP | 100 | 192.168.1.0/23 | ANY | Any | 10.0.2.0/24 | 3389 | Allow |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Identity Tier NSGs** | | | | | | | |
| **Name** | **Priority** | **Source** | **Protocol** | **Source Port Range** | **Destination** | **Dest. Port Range** | **Action** |
| RDP | 100 | 192.168.1.0/23 | ANY | Any | 10.0.3.0/24 | 3389 | Allow |

**Resilient Benefits:**

* NSGs provide protection and only allow the traffic defined by the rules through. This protection is a form of resiliency as well.
* External and Internal protection is designed and provided for resiliency and hardening for the environment.

### Customer objections

1. “Cost is a huge concern for us. With looming infrastructure and server replacement costs, we want to avoid any unnecessary expenditures.”

**Potential Answer** – You can restructure the costs and save funds by rolling out the infrastructure into Azure as opposed to rolling out the infrastructure in the Austin office. The Azure datacenters are world class enterprise level datacenters providing a server environment that would cost LitWare Inc. a lot of expense to build. Also, deploying virtual machines in Azure provide resiliency at a fraction of the cost of physical hardware. Pay only for what you need and use. Also, bring up during the discussion that the cost of downtime might far outweigh the cost of the resiliency being built into the environment.

1. “The web application needs to have the ability to scale as we grow. What aspect of the cloud will allow this to be a reality?”

**Potential Answer** – Scale sets from an IaaS perspective would be a great choice to provide scaling of the web application. In the future, as the organization continues to grow, Azure Web Apps may also be an option from the PaaS perspective. This would allow for websites to be scaled-out, scaled-up or even scaled-down, and scaled-in based on use or other metric of your choice.

1. “Downtime is becoming more of an issue for us due to development and production environments not being separate. We need to separate these from one another to avoid outages.”

**Potential Answer** – Azure allows for a number of ways to mirror a production environment and use it for development and testing. Backing up the infrastructure and restoring it to Azure is one way. Another way would be Azure Site Recovery (ASR). ASR can replicate VMs and physical machines to Azure to mirror the production environment. Another option could be to create a DevTest Lab in Azure to provide a complete separate environment for developers and testers.

1. “Connectivity bandwidth is becoming an issue for our self-hosting of the applications, ordering system, support website, etc. We’re concerned that the cloud maybe constrained as well.”

**Potential Answer** – Azure is housed on one of the largest world-wide networks and Microsoft has invested billions of dollars for the infrastructure and connectivity to be world-class. Should there be performance issues, the applications can be scaled to address the needs of the business. There are resizing options and VM instances that address network performance options as well.

1. “Our current backup/recovery system works just fine.”

**Potential Answer** – Depending on which backup system you are using, you can extend your current backup system into Azure. There is no need to replace the current system, augment it. Azure backup works with Microsoft System Center Data Protection Manager (DPM) or you can use Microsoft Azure Backup Server to perform disk-to-disk-to-cloud VSS backups. For SQL Backup, use direct backup to Azure Blob Storage. Using Microsoft Azure Recovery Services Agent, you can backup Windows Server and Client Files and Folders directly to the cloud as well. IaaS instances are also able to be protected with Azure Backup and all can be monitored in one central location.

1. “We already have a point of presence for our customers that we don’t want to change. How can we provide cross-region resiliency without impact to our customers?”

**Potential Answer** – Azure has built in Traffic Manager that will allow multiple regions to be configured in a priority (or failover) algorithm. To the customer, the web URL is the same. You can map the URLs in the profile of the Traffic Manager and even use it in conjunction with load balancers to provide DNS traffic routing via the traffic manager to load balanced IaaS servers for the web application virtually eliminating the single point of failure. It will also allow one region or the other to be taken down for maintenance while the customers remain unaffected.

1. “We are very concerned about the disk space issue that occurred earlier with our ADDS DCs and nearly our Web Servers and Database Servers. Will this be addressed per the resiliency plan?”

**Potential Answer** – Azure has built in monitoring capabilities that will address the issue of an outage. Availability sets spread the IaaS VMs across multiple racks for fault protection. For ARM, 100 VMs can be spread across 3 fault domains and up to 20 upgrade/update domains in Azure allowing for your application to be protected from outages caused by faults or updates to the hosts. Alerting can provide you with emails and even scripts that can be automated when the alert occurs to take recovery actions. There is also monitoring that can be configured to monitor the health of the storage accounts and provide reporting on this. Operations Management Suite can also be utilized for monitoring workloads.

### Customer quote (to be read back to the attendees at the end)

“By using Azure, we can build out resiliency for all aspects of our environment. It allows for infrastructure, networking, web applications, Active Directory and other items to be redundant and highly available. With some planning and deployment of resilient resources, I envision our LOB apps and websites will no longer be impacted by full outages.”

—Lewis Franklin, Head of Infrastructure and Enterprise Operations, LitWare, Inc.