**Microsoft Cloud Workshops**

Whiteboard Design Sessions

Building a Resilient IaaS Architecture

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.

Workshop flow

Each workshop uses the following flow:



# 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.

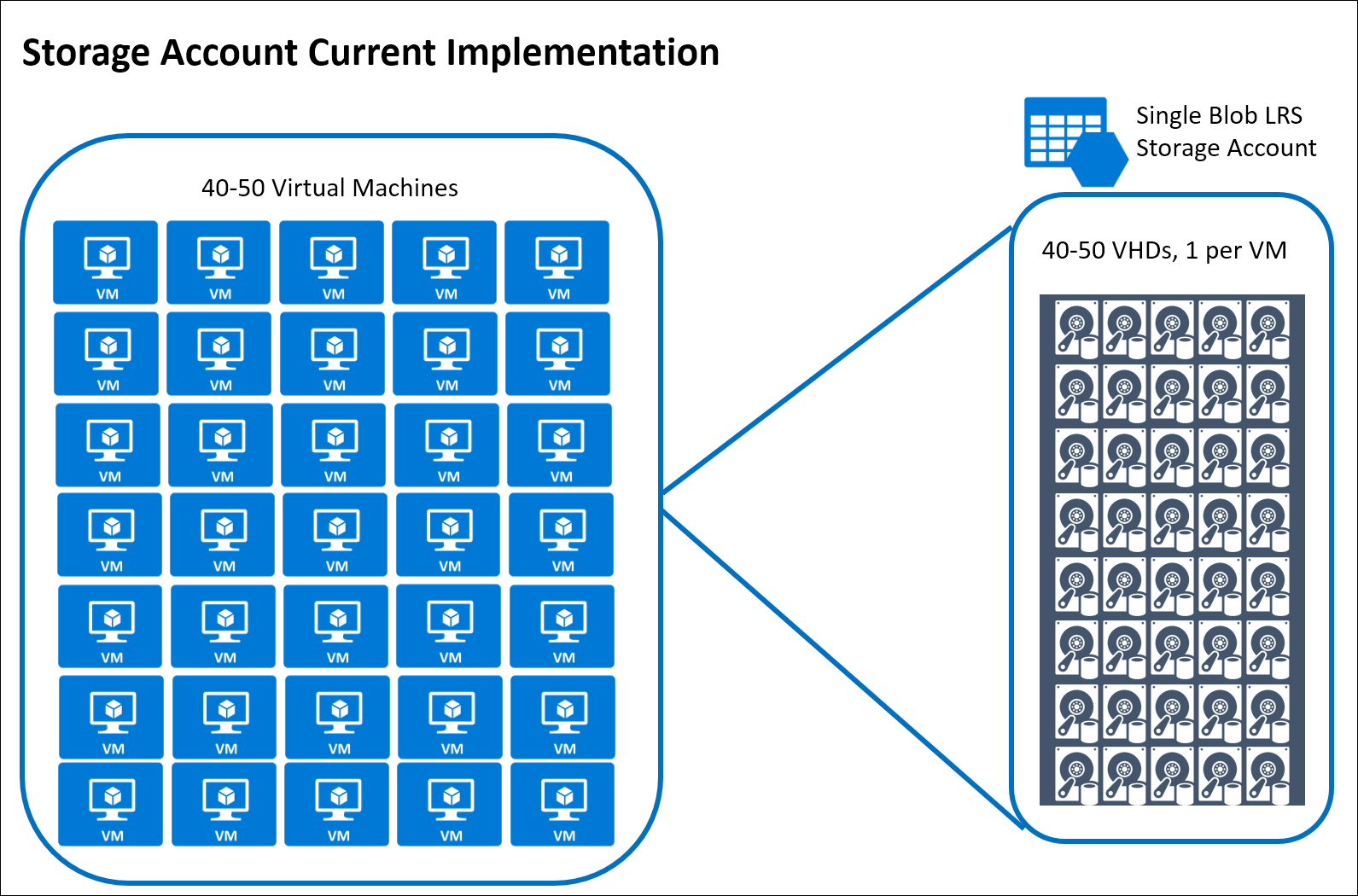
### Customer situation

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*

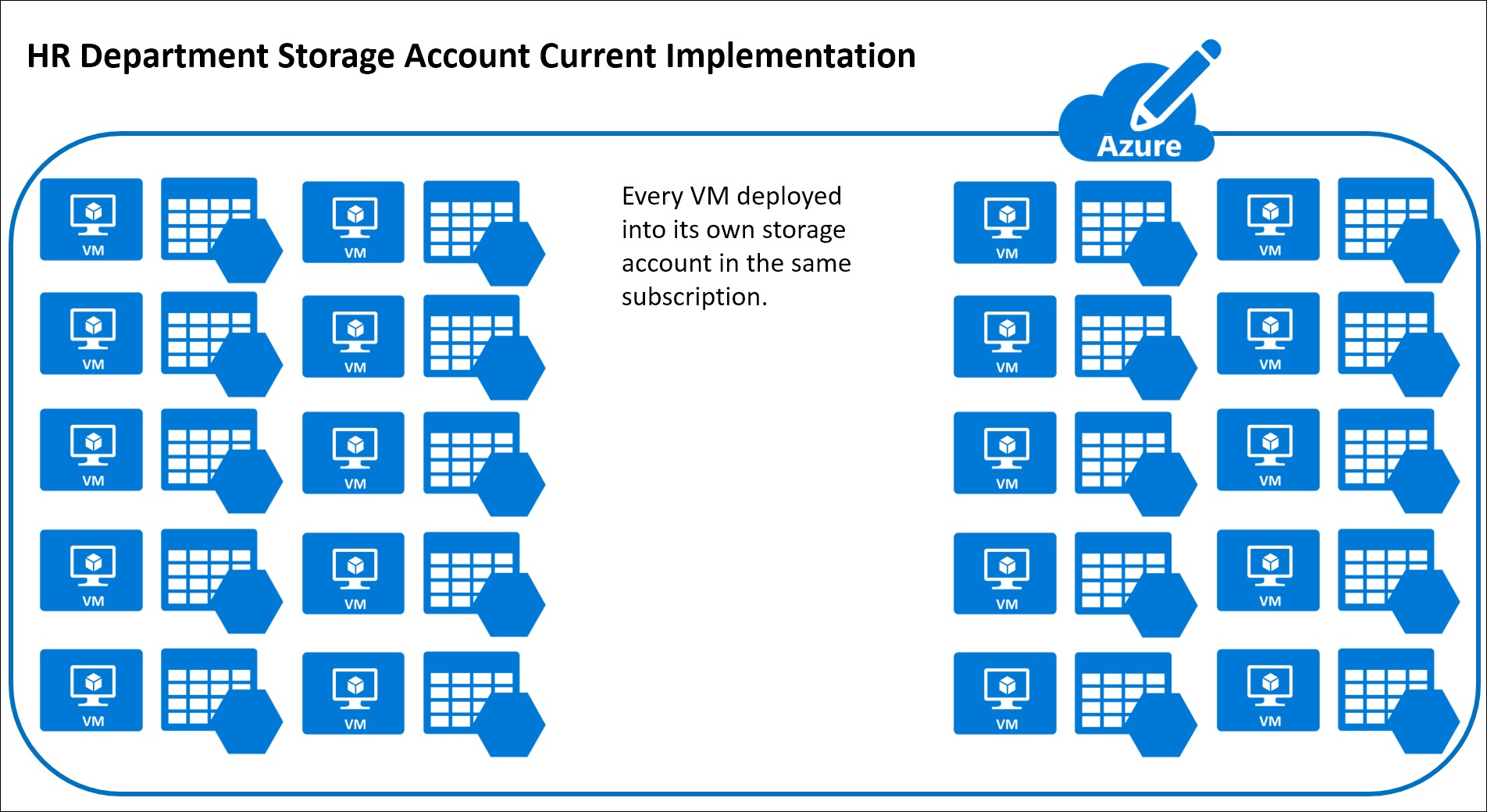
LitWare Inc. is currently connected via a Windows Server Routing and Remote Access Service (RRAS) VPN connection to Azure via a Site-to-Site Gateway in the South Central U.S. location. They are looking for options to provide redundancy for the hybrid connectivity to Azure due to some recent connectivity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

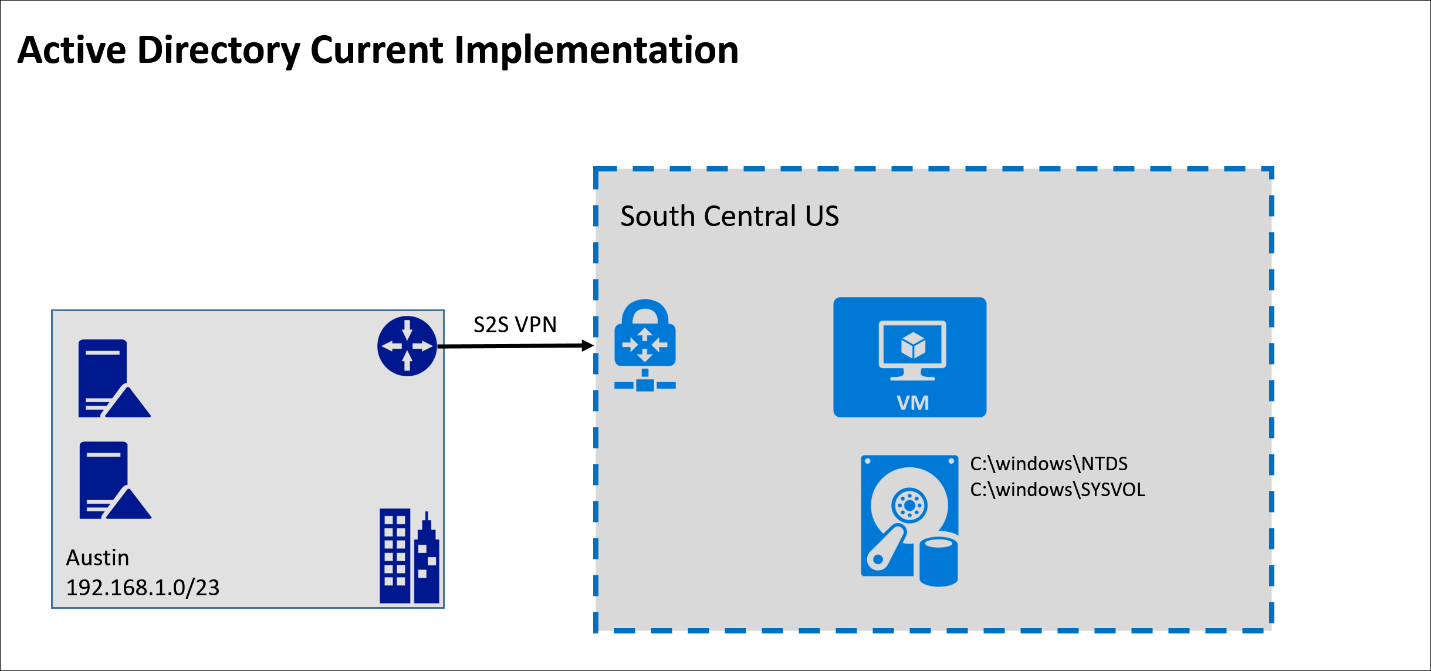
Retroactively, checks were made on some other IaaS disk drives and there were a number of them that were getting close to filling up due to teams not proactively monitoring their role servers. Key team members are now calling for a proactive approach to monitoring Operating System (OS) disk and data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

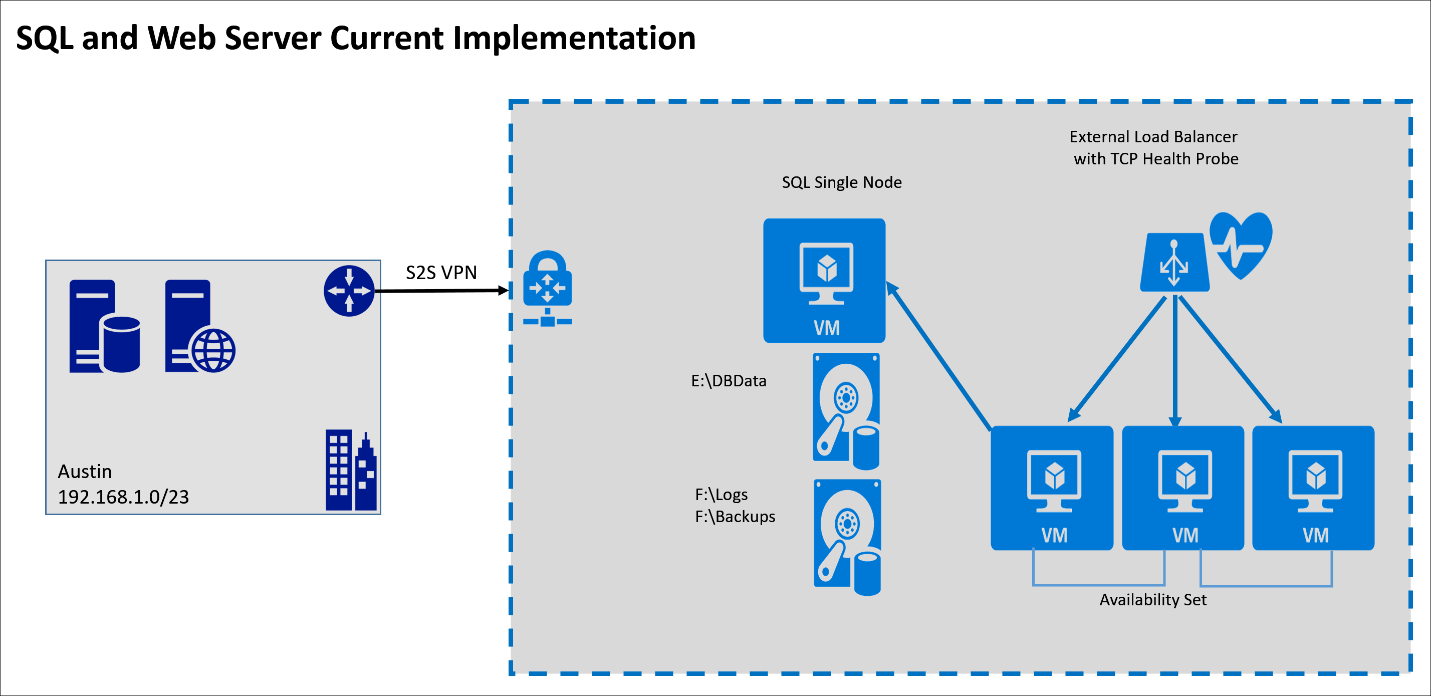
For the current Active Directory Azure implementation, the team has deployed a single AD DS DC in the South Central U.S. Region. It is running on a D1 Standard Instance with only the OS Disk. Both the NTDS folder containing the Active Directory DB and the System Volume (SYSVOL) folders are located on 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> |

