Sikich Customer

ERP on Azure Design

Produced by Sikich, LLP

Design Description: Four servers will be installed, a Domain Controller, a Remote Desktop Gateway Server, a Remote Desktop Session host and a SQL Server. Users will access the application through the Remote Desktop Gateway connection from their device, which will run the ERP Client and connect to the ERP Database on the SQL Server. The only inbound communication allowed is TCP 443 to the Remote Desktop Gateway Service which will be protected by a Web Application Filter. The entire virtual network will be connected to the corporate network with a Site to Site VPN to allow communications between the corporate network and the Azure subscription.

Client Communication : All Internet communication with the solution by the clients will occur over HTTPS, encrypted with a public trusted certificate. The remote desktop protocol will be encapsulated in SSL and will carry screen images, user inputs and printing and file transfers over this secure channel. A site to site VPN to the Corporate LAN is incorporated in this design, which could allow direct RDP when in the office. This will not be disabled, but Sikich recommends that clients access the application in a consistent manner, using RemoteApp in all cases. Operation of the ERP client from the corporate LAN across the VPN is not recommended.

User Sessions: Users of the solution will receive a Remote App running in a user session on the Remote Desktop Server. The user will only have access to the application in use, typically the ERP Application, and not the full desktop. If a file is produced by ERP appliocation with a valid file association on the server, the appropriate application will launch. The most likely example of this is a file with a .xlss extension launching Microsoft Excel.

User Authentication: The users will authenticate to RemoteApp sessions using their Windows Active Directory credentials. The corporate Domain will be extended to Azure with a Domain Controller to continue supporting logins in the event of a VPN issue.

Backup and Recovery:

Virtual Machine Backups - Each machine will be protected by a Recovery Service Vault. Machines will be protected nightly to Geo-Redundant Storage. Sikich recommends the following Retention schedule:

> Nightly – 14 Days
>
> Weekly – 12 Weeks
>
> Monthly – 12 Months
>
> Yearly – None

SQL Database Backups - Additional protection for the SQL Database will be configured using SQL Database Maintenance Plans. The SQL user databases will have a full nightly backup and a hourly log file backup to a Geo-Redundant disk attached to the SQL VM. Both will be retained for 3 days.

Azure Site Recovery -All the virtual machines are replicated to another Azure Region hourly. The recovery points will be retained for 24 hours.

Security and Management : This solution has Azure Security Center Standard applied to it for additional monitoring, recommendations and alerting based on Microsoft's adaptive threat prevention and Intelligent treat detection. Sikich recommends that all Azure Administrators utilize Azure Multi-Factor authentication when managing the subscription.

Expandability : This design has been created to scale both for high availability and increase user count in the following ways.

Domain Controllers : As the number of uses increases above 40, it is recommended that a second domain controller be added for redundancy.

Remote Desktop Gateway: As the number of users increases above 75, it is recommended that a second Remote Desktop Session Host be installed. This will also require a Network Load Balancer, either from Microsoft or a Third Party (Kemp).

Remote Desktop Session Hosts: The current design is suitable for 15-30 concurrent users. As the number of users increases, Sikich recommends adding additional Session Hosts.

SQL Server: The particular type of VM for the SQL server was chosen to allow for substantial performance expansion. The ES4 v3 can scale to 64 vCPU, 432 GB of RAM and up to 256 TB or storage. To add redundancy to the solution, a second SQL VM can be provisioned and SQL Always On configured.

Azure Availability Sets: Because each of the machine types is anticipated to expand in the future, it is recommended that an Availability Sets for each type of machine be created before any machine is created and the first machine of that type be created in the appropriate availability group.

Licensing Considerations: There are specific licensing considerations in Azure around Windows Server and SQL Server.

Windows Server Licensing : Machines created in Azure from the templates contain both their Windows Operating Systems Datacenter license and do not require Windows Server Client Access licenses. However, if the client has sufficient licensing to cover both the Operating Systems and Client Access license, it is recommended that the Hybrid Use right be utilized to reduce the hourly operating costs of the Azure Servers. Note that the licensing must have an active Software Assurance to qualify for Hybrid Use Rights. Windows Server SPLA licensing cannot be used on Azure.

SQL Server Licensing: SQL Machines created in Azure from the SQL Templates contain SQL server processor licensing for the chosen edition of SQL. Again, if existing licensing already exists for SQL, and has the License Mobility right, granted by Software Assurance, this can be used in substitution of the Azure SQL Licensing. SQL Server SPLA licensing is available to be used on Azure. Typically, SPLA licensing is less expensive if there are less than 27 users per 4 cores of SQL Standard deployed, and Azure SQL Core Licensing is less expensive above that deployment density.

Hosting Service Description

4 Virtual Machines

       2 Machines Stored on Geographically Redundant Storage

              1 Domain Controller

                     Size - A2v2- 2 Cores, 4 GB RAM

              1 Remote Desktop Gateway

                     Size - A2v2 – 2 Cores, 4 GB RAM

       2 Machines Stored on Locally Redundant Premium Storage

              1 Remote Desktop Session Host

                     Size D11v2 Promo -2 Core, 14 GB RAM

              1 SQL Server

                     Size D12v2 Promo – 4 Core, 28 GB RAM

260 GB Standard Geo-Graphically Redundant Storage

Premium Locally Redundant Storage

       3 P10 Disks – SQL and RDSH OS, SQL Logs

       1 P20 Disk – SQL Data

Standard Web Application Gateway

Virtual Network Gateway (Standard)

1 Site to Site VPN

4 Geographically Redundant Cloud Server Backups

5 Security Center Standard Nodes

4 Azure Site Recovery Instances (Azure to Azure)

Azure Standard Support

Sikich Customer ERP on Azure Design

Service type	Custom name	Region	Description	SKU
Data Transfers	Bandwidth	North Central US	250 GB/Month Zone 1: North America, Europe (North America, Europe)	Q5H-00003
IP Addresses	IP Addresses	North Central US	4 Static IP Addresses	T6Z-00010, AAA-69016, T6Z-00012
VPN Gateway	VPN Gateway	North Central US	standard tier, 744 gateway hour(s), 150 GB outbound vpn	N7H-03377, Q5H-00003
Application Gateway	Application Gateway	North Central US	1 instance(s) x 744 hours, 150 GB data processed, outbound transfers:: 150 GB	AAA-21764, T6Z-00092, Q5H-00003
Storage	Standard Storage - DC, RDGateway	North Central US	260 GB storage Unmanaged Disks & Page blobs type. Standard tier, GRS redundancy, 10000 x10,000 transactions	N9H-00092, N9H-00803
Storage	Premium Storage P10 - OS SQL and RDSH, SQL Logs	North Central US	3 disks P10 (128 GB, 500 IOPS, 100 MB/sec, $19.71/mo), Unmanaged Disks & Page blobs type, Premium (SSD) tier	N9H-00332, N9H-00803
Storage	P20 SQL Data	North Central US	1 disks P20 (512 GB, 2300 IOPS, 150 MB/sec, $73.22/mo), Unmanaged Disks & Page blobs type, Premium (SSD) tier	N9H-00360, N9H-00803
Backup	Backup	North Central US	4 instance(s), 200 GB, 800 GB GRS of storage	N9H-00430, N9H-00076
Virtual Machines	DC	North Central US	1 Standard virtual machine(s), A2 v2 (2 cores, 4 GB RAM, 20 GB disk) size: 744 hours	AAA-33510
Virtual Machines	RD Gateway	North Central US	1 Standard virtual machine(s), A2 v2 (2 cores, 4 GB RAM, 20 GB disk) size: 744 hours	AAA-33510
Virtual Machines	RDSH	North Central US	1 Standard virtual machine(s), D11 v2 Promo (2 cores, 14 GB RAM, 100 GB disk) size: 744 hours	

Virtual Machines	SQL Server	North Central US	1 Standard virtual machine(s), D12 v2 Promo (4 cores, 28 GB RAM, 200 GB disk) size: 744 hours	
Security Center	Security Center	North Central US		WW4-00002
Site Recovery	Site Recovery	North Central US	0 instance(s) of Recovery to customer-owned sites, 4 instance(s) of Recovery to Azure	7U9-00008, 7U9-00003
Support			Standard level	