NICHOLAS GULRAJANI

JULY 13, 2023

PRODUCTION '2' 'DR' DEPLOYMENT CONSIDERATIONS FOR FOLLETT – A FRAMEWORK

To deploy to a PRODUCTION2 Azure environment, it is recommended to follow a set of best practices and establish specific conditions for disaster recovery (DR).

The exact DR conditions will vary depending on FOLLETT's specific application and business requirements.

However, here are some general guidelines and considerations:

1. Define Recovery Point Objective (RPO):

   RPO determines the maximum acceptable data loss in case of a disaster.

   RPO represents the age of the last valid backup that needs to be restored.

   Would need to define an RPO that aligns with business needs and regulatory requirements.

2. Define Recovery Time Objective (RTO):

   RTO defines the maximum acceptable downtime for your application.

   It represents the time it takes to restore system to a fully operational state after a disaster.

   Define an RTO that meets business continuity goals.

3. Implement High Availability (HA): Implementing HA in the PRODUCTION2 environment will help minimize downtime by ensuring redundant and fault-tolerant infrastructure.

   Use features like load balancers, auto scaling, and redundant storage to distribute the workload and minimize the impact of failures.

4. Implement Data Replication:

   Use Azure services like Azure Storage Replication, Azure SQL Database Geo-Replication, or Azure Site Recovery to replicate data across multiple regions.

   This ensures that data remains available even if a disaster affects a single region.

5. Regular Backups:

   Perform regular backups of your data and configuration settings. Azure provides various options like Azure Backup and Azure SQL Database backups to securely store your backups.

6. Test and Validate DR Plan:

   Regularly test DR plan to ensure that it works as expected.

   Conduct simulations and drills to validate the recovery procedures and minimize potential risks.

7. Monitor and Alerting:

   Set up monitoring and alerting mechanisms to proactively detect and respond to any issues in PRODUCTION2 environment.

   Monitor performance, resource utilization, and health metrics to identify potential problems before they escalate.

8. Security and Compliance:

   Ensure that the DR plan adheres to security and compliance requirements.

   Implement proper access controls, encryption, and security measures to protect your data and infrastructure.

9. Document the DR Plan: Document DR plan with detailed steps and instructions. Include contact information, roles, and responsibilities of team members involved in the DR process.

   Keep the documentation up-to-date and easily accessible to relevant personnel.

Note: it's essential to consider the required applications and databases' infrastructure dependencies, such as networking, storage, and connectivity, to ensure a complete and functional environment.

---

1. Resource Group: Create a new resource group in the Azure portal or via Azure CLI. A resource group acts as a logical container for your Azure resources.
2. Virtual Network: Create a virtual network (VNet) within the resource group.

   A VNet provides an isolated network environment for your infrastructure components.
3. Subnets: Define one or more subnets within the virtual network. Subnets allow you to segment and organize your infrastructure resources.
4. Availability Zones: Choose the availability zones in which you want your infrastructure to be deployed. Availability zones provide high availability by distributing resources across multiple physical locations within an Azure region.
5. Virtual Machines (VMs): Deploy the required virtual machines within the subnets of your virtual network.

   Choose the appropriate VM sizes, operating systems, and configurations based on infrastructure needs.
6. Load Balancer: If there is a need to distribute incoming traffic across multiple VMs, configure a load balancer. It helps balance the load and ensure high availability.
7. Network Security Groups (NSGs): Create and configure NSGs to control inbound and outbound traffic to VMs. NSGs act as virtual firewalls, allowing one to define network security rules.
8. Storage Accounts: Provision one or more storage accounts to store any required data or configuration files for the infrastructure components.
9. Virtual Machine Scale Sets (optional): If needed to scale your infrastructure horizontally based on demand, consider using virtual machine scale sets.

They allow you to manage and automatically scale a group of VMs.

10. Connectivity: Establish connectivity between your PRODUCTION2 environment and other necessary resources, such as on-premises networks or other Azure environments, by setting up virtual network gateways, VPN connections, or Azure ExpressRoute.
11. Monitoring and Alerting: Enable monitoring and alerting for your infrastructure components.

    Use Azure Monitor or other monitoring tools to track the performance, availability, and health of your infrastructure resources.
12. Security and Compliance: Implement security best practices by configuring appropriate access controls, enabling encryption at rest and in transit, and adhering to compliance requirements relevant to your infrastructure.