VALUELINK DISASTER RECOVERY EXECUTION PLAN

Before proceeding with this document make sure that you have completed the (ValueLink Disaster Recovery Pre-Post Checklist) to identify the key area.

Policy Statement:

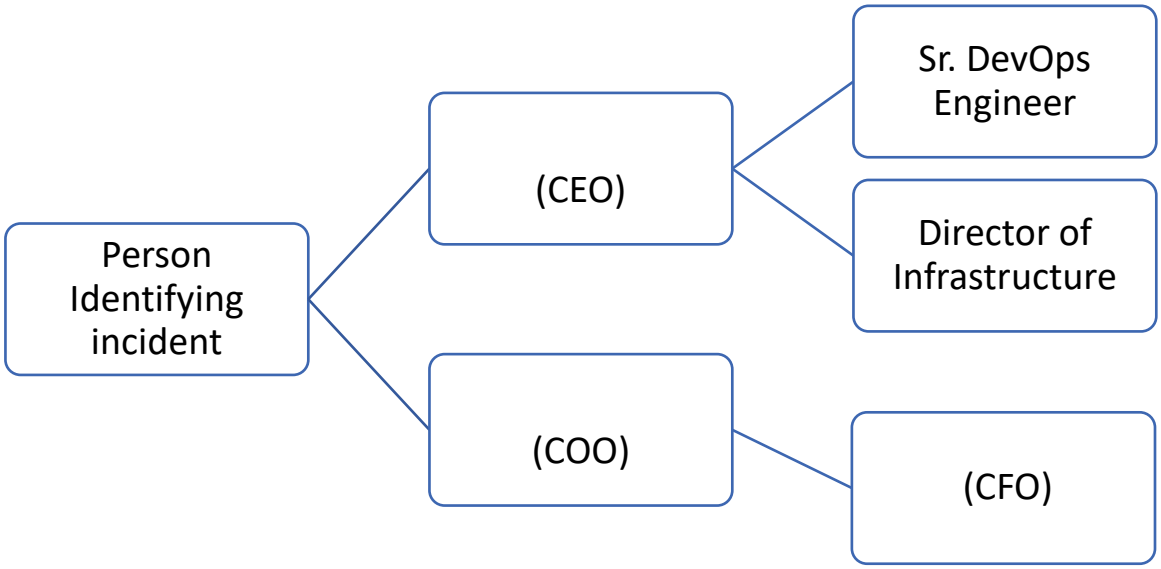
- Corporate management has approved the following policy statement:
- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

Notification Calling Tree:



Plan Triggering Scenarios:

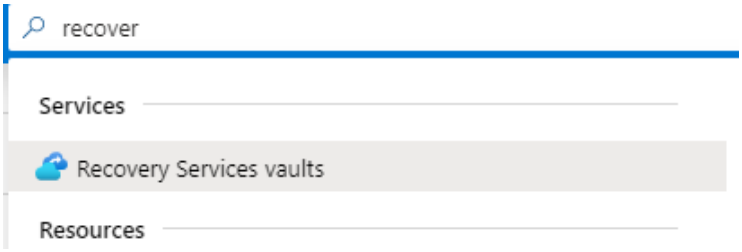
Key trigger Scenario at Azure EAST US Region that would lead to activation of the Disaster Recovery Plan are:

- All Azure Services Are Down.
- Azure SQL Server Service is Down.
- Azure Virtual Machine Services Are Down.
- Azure Storage is Down.
- Redis Cache for Azure is Down
- Azure Load Balancer Services are down.

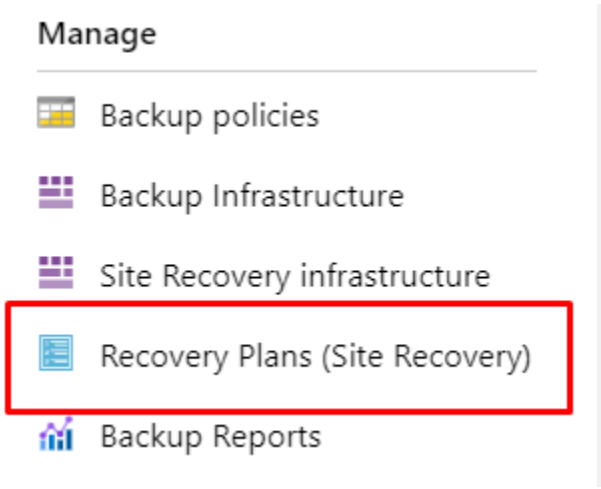
Scenario # 1: All Azure Services Are Down

If Status and Service Health is showing the All Azure services down then we need to execute the Complete Disaster recovery process, Follow the steps:

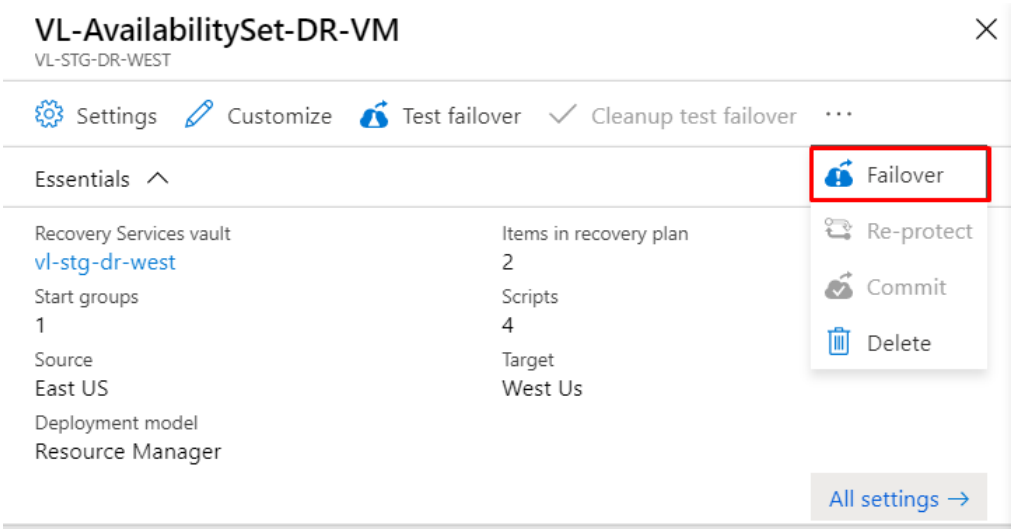
1. Search for the recovery service vault and select your recovery vault.



2. Under manage tab click on the recovery plan tab and select your recovery plan.



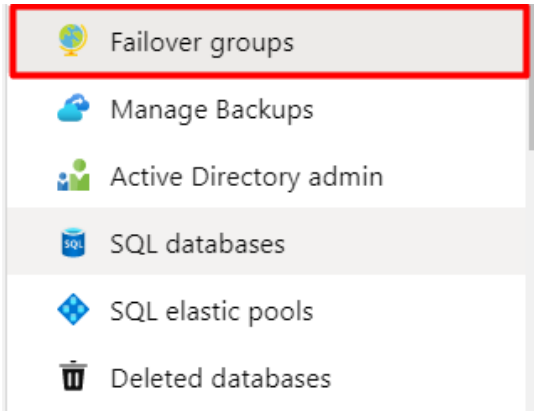
3. After selecting the recovery plan just click on the more button and execute the failover.



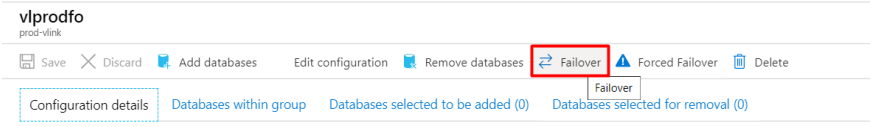
Scenario # 2: Azure SQL Server Service is Down.

If Azure SQL Service is down, we need to follow few steps for switching the secondary server to primary.

1. Open up the Primary SQL Server and click on failover group and Select the Failover Group **(VLPRODFO)**.

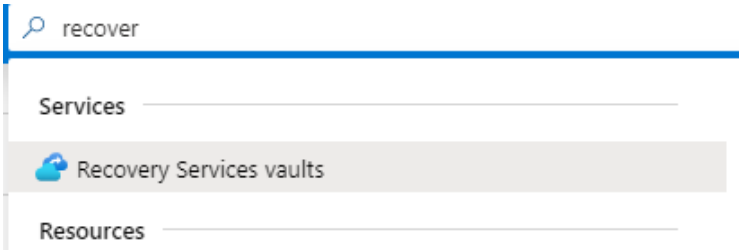


2. Click on the Failover button to initiate the failover, this will make the primary SQL Server to secondary in readable mode.

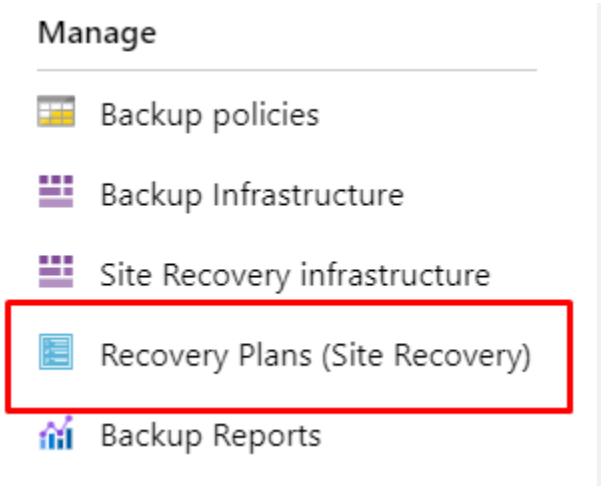


Scenario # 3: Azure Virtual Machines Services Are Down.
If health status is showing the virtual machine services as down then follow these steps:

1. Search for the recovery service vault and select your recovery vault.



2. Under manage tab click on the recovery plan tab and select your recovery plan.



3. After selecting the recovery plan just click on the more button and execute the failover.

Scenario # 4: Azure Storage is Down.

Azure Storage Failovers are managed by azure themselves, they will automatically initiate the failover when disaster occur.

Scenario # 5: Redis Cache for Azure is Down.

The Redis cache in the production environment is only accessible from a vent, which means it can only be accessed by virtual machines in the same vent.

To make Redis highly available in production, we must either make Redis geo redundant or build a new Redis server in the west US region.

Scenario # 6: Azure Load Balancer Service is Down.

In case the load balancer services are down in the source region (East us). We need to run the recovery plan from the recovery services vault. The plan will use the Azure automation account to build the load balancer service in the West US region

Key Findings:

During the DR drill, we discovered the following obstacles:

- The SQL server does not replicate the logins created in the master database
- Redis cache is not geo redundant

To resolve the SQL logins replication issue mentioned above, we need to ensure that the users are created separately for each database. Refer to the article below from Microsoft.

https://learn.microsoft.com/en-us/sql/relational-databases/security/contained-database-users-making-your-database-portable?view=sql-server-ver16

Redis cache is currently zone redundant. When it is zone redundant it does not allow the geo redundant feature. We can either create a new Redis cache in the West US region which will only be used in case of DR. The other way around is to create a new Redis cache in East US without making it zone redundant and then make it geo redundant.