Overview:
After securing the production instance and applying necessary monitoring capabilities, Contoso is now looking to protect the production instance from unintended data discrepancies, loss, and/or corruption. In addition, the company is also looking to have a secondary copy of data in a separate (DR) region in an event of a region-wide failure, or a failure that would trigger a disaster recovery response.

In order to meet the requirements, you need to ensure business continuity and the availability of the system's state by applying regular recovery points. Additionally, you will protect the system from a regional failure by setting up and validating an asynchronous replication-based disaster recovery mechanism.

Execution Guidelines:

1. Backup using a temporary solution (HANA native)
    a. For point-in-time recovery, you need to enable log backups. **Configure** HANA for log backups to the dedicated volume: /backup/log
    b. **Take** your first native HANA full file level backup
    c. This backup is a stop-gap solution until the permanent solution is stood up. Also, this will continue to serve as a fallback option.
2. Backup using a permanent solution (ANF snapshots) :
    a. Assess the backup requirements:
        i. Use ANF where possible
        ii. Cannot afford to lose more than 15 min worth of recent changes
        iii. Local availability of log backups for up to the last 24 hours
        iv. Point-in-Time recovery for up to the last 72 hours
        v. Additional protection of backup files by offloading to an intra region storage account
    b. **Update** the below backup schedule (frequency, retention, offloading, sizing)

Protect:	Size (customer provided)	Frequency	Retention	Offloading
HANA data	1 TiB (20% YoY Growth)	?	?	To a separate blob container, retain for 7 days.
HANA log backups	250 GiB	?	?	To a separate blob container, retain for 7 days.
Shared binaries and profiles	100 GiB	?	?	To a separate blob container, retain for 7 days.

(Please note that this OpenHack environment is a scaled down version of the above production-like scenario. Also, we will not protect Shared binaries for this challenge.)

c. **Adjust** log backup volume size for storing log backups, and **adjust** relevant HANA parameters to use this volume for log backups.
d. **Protect** ANF resources from accidental deletion
e. **Build** a backup (snapshots) orchestration by installing the tool on the Linux jump server, and by **automating** the snapshot scheduling using the Linux built-in tool - crontab
f. **Orchestrate** offloading of the required snapshot using azcopy in to respective containers in the provided storage account. The azcopy gets installed directly onto the HANA DB VM.
g. Ensure that you log into azcopy without supplying the authentication key or a SAS (use Managed Identity)
h. **Create** a security user "BACKUPTEST".
i. **Take** a backup (using azacsnap). Give a prefix "UseThisBackupTest" and note down the creation time stamp
j. **Delete** the security user BACKUPTEST "accidently" - Oops!
k. **Restore** the system so that the BACKUPTEST user is restored using the snapshot "UseThisBackupTest"

3. Disaster Recovery
    a. Assess the disaster recovery requirements:
        i. RPO < 30 min, RTO < 4 hrs.
        ii. Inter-region DR using storage replication capabilities
    b. **Set up** ANF storage replication (CRR) to meet the RPO
    c. **Create** a security user "DRTEST" on the Production instance in the primary region. (This is to validate the replication.)
    d. **Take** a backup (using azacsnap). Give a prefix "UseThisAtDR" and note down the creation time stamp
    e. Execute the DR by:
        i. Wait until the replication is Healthy, Mirrored and Idle
        ii. Shut down the Production HANA instance (**Stop** VM) at the primary region
        iii. **Stop** the QA HANA instance and leave the Production HANA instance at the DR region down
        iv. **Break** the replication and **swap** the necessary volume for the Production HANA instance at the DR region. Use snap revert to "UseThisAtDR" snapshot.
        v. **Start** HANA recovery (point in time) at the DR region for the Production HANA instance
        vi. **Validate** the existence of "DRTEST" user.

Success Criteria:

1. A successful setup of the temporary backup solution.
2. An automatic orchestration of ANF snapshots on the data and log backup volumes to achieve point-in-time recovery.
3. The availability of offloaded snapshots in storage account containers per the requirement. Be able to restore the BACKUPTEST user successfully.
4. Be able to successfully restore the dual-purpose environment with the recent production data (with DRTEST user)

Hints/Resources:

1. https://www.netapp.com/pdf.html?item=/media/17152-tr4746pdf.pdf
2. https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/hana-vm-operations-storage
3. Requirements and considerations for using Azure NetApp Files volume cross-region replication | Microsoft Docs
4. Blog: Search - Microsoft Tech Community