1. To safeguard virtual resources in a VCSA (vCenter Server Appliance) deployment, the employee should first ensure that vSphere HA and DRS are appropriately setup for high availability and resource optimization. This includes establishing HA and DRS on the cluster, implementing admission control rules, and configuring suitable failover capabilities. In addition, frequent backups of the VCSA should be planned using vCenter Server's built-in backup software. Configure and monitor storage and network redundancy, as well as establish security measures such as securing vCenter access, enabling role-based access control, and installing security updates on a regular basis.
2. To deploy the design, the employee must first activate vSphere HA and DRS on the relevant clusters inside the VCSA, as described in step 1. They should then set the HA admission control strategy to reserve enough resources for failover situations. Next, the employee would configure the VCSA backup schedule, selecting backup location and retention rules. Ensuring that storage and network pathways are redundant and robust is also crucial, which necessitates the configuration of multipathing for storage and NIC teaming or failover for network interfaces. Finally, the employee should examine and implement security settings, such as defining required user roles, safeguarding network connections, and verifying that the VCSA and related ESXi hosts have the most recent security patches and upgrades.