**Renew certificate sc-300**

1. You need to ensure that admin1 can manage the users from the marketing department – one administrative unit
2. AD DS, AD FS, Microsoft entra ID you need to monitor all three environment using AD connect health – Azure AD connect, AD DS, And AD FS
3. You plan to synchronize AD to Microsoft entra ID using AD connect cloud sync – a group managed service account
4. Microsoft entra ID connect health – Microsoft entra ID connect & AD DS only
5. You need to create Microsoft entra ID identity protection policy that required risky users to change their password – sign-in risk policy
6. Administrator will receive users at risk detection alerts from Entra ID identity protection – admin1 admin2 admin 3 only
7. Risky sign in report maximum number of day you can review the report – 90
8. Maximum number of user risk policies that you configure – 35
9. CAE – IP based name location
10. VM1 and VM2 same identity – a user assigned managed identity
11. VM can app1 acquire an access token – VM1 VM2 VM3 only
12. Which managed identity can assign to VM1 – one system assigned managed identity and one user assigned managed identity
13. Which two permission can be removed by admin1 – permission assigned to user3 and user4
14. Which resource can admin1 create in sub1 – bastion1 and container1 only
15. What resources can you assign role1 – MG1, sub1 only
16. You need to delegate the appropriate permission to admin1 to manage security on RG1 – user access administrator
17. What entity can add new apps to the cloud app catalog – cloud app administrator
18. You ned to implement shadow IT cloud discovery in Microsoft defender for cloud app – Microsoft graph
19. Two policy you have to create in Microsoft defender – asscess policy and session policy
20. You create a conditional access policy for app1 named policy1 – session
21. You need to to publish app1 to remote user by using tha entra ID application proxy – outbount connection over HTTP and HTTPS
22. You plan to provide remote users with access to app1 by using entra ID application proxy – install azure AD connect
23. KQL add additional column – extend
24. KQL graphical display – render
25. Which identity can you add to AU1 – user1 and group1 only
26. OU1 – Microsoft netra admin center
27. You need to required users to use MFA to sign in to Microsoft entra – MFA registration policy
28. Automatically created in Microsoft entra ID – a service identity
29. Which administrator can assign role on RG1 – admin2 only
30. Maximum number of log file that are retained in the backup directory – 20
31. Which portal should you use to create policy – Microsoft defender cloud app portal
32. Minimum number of connector that you must install – 2