To use serial console, need to enable boot diagnostics first.

To enable update management of vm, need to connect vm to log analytics workspace first.

To enable security audit logs for success and failure on VM1, need to:

Open Diagnostic settings blade for VM1, click enable guest-level monitoring, navigate to logs tab, enable audit success for security event logs

Just in Time need NSG

Just in Time need Azure Security Center Standard Tier

When installing azure ad connect, need both domain and global admin permissions.

Role Owner, Contributor, and ArcPush can push image.

All ACR roles except ArcDelete and ArcImageSigner can pull image.

Container network interface (CNI) is only for AKS

“Read-Only” lock does not allow creation.

Use Custom script extension to ensure key application services are started programmatically in VM.

Azure Sentinel are configured as logic app

Azure AD Connect is used to sync on-prem AD users with azure AD

Federation with ADFS allows authentication to occur on-prem and support smart card

Azure AD DS is a LDAP to allow on-prem app to use azure AD identity

Pass through allows user to use on-prem AD authentication but no support smart card

You can create one-time bypass as temporary solution for MFA issues. It is time-limited and allow 1 time bypass for user.

To configure JIT:

Open security center dashboard

Select jit VM access

Select not configured tab

Select each VM

Select enable JIT on Vm

You can bind an SSL certificate to web app using all service plan EXCEPTS free and shared plan