AZ-204 – Develop Azure Compute Solutions → Implement Azure App Service Web Apps → 1.2.4 Configure settings including TLS,API, ServiceConnections

- How do you enforce HTTPS (TLS) for an App Service?
- How do you configure minimum TLS version?
- How do you set custom domains and bind SSL certificates?
- How do you configure API settings such as CORS?
- How do you connect to backend services using managed identity?
- How do you restrict outbound traffic using VNET integration?

---

1. How do you enforce HTTPS (TLS) for an App Service?

az webapp update --name <app> --resource-group <rg> **--https-only true**

Redirects all HTTP traffic to HTTPS.

---

2. How do you configure minimum TLS version?

az webapp config set --name <app> --resource-group <rg> **--min-tls-version 1.2**

Options: 1.0, 1.1, 1.2. Use 1.2 for compliance.

---

3. How do you set custom domains and bind SSL certificates?

- Add domain:
  az webapp config hostname add --webapp-name <app> --resource-group <rg> --hostname <custom-domain>
- Upload and bind cert:

az webapp config ssl upload --certificate-file cert.pfx --certificate-password <pwd> --name <app> --resource-group <rg>
az webapp config ssl bind --name <app> --resource-group <rg> --ssl-type SNI --certificate-thumb

4. How do you configure API settings such as CORS?

az webapp cors add --name <app> --resource-group <rg> --allowed-origins https://example.com

Use cors remove or cors show to manage rules.

---

5. How do you connect to backend services using managed identity?

1. Enable identity:
   az webapp identity assign --name <app> --resource-group <rg>
2. Grant role to identity (e.g., Key Vault Reader):
   az role assignment create --assignee <principal-id> --role Reader --scope <resource-id>

---

6. How do you restrict outbound traffic using VNET integration?

- Integrate with VNET (Linux apps, Standard+):

az webapp vnet-integration add --name <app> --resource-group <rg> --vnet <vnet-name> --subnet <subnet-name>

Restricts outbound traffic and enables access to private services.