ETC

- AD NOTES
  - DHCP's house in AD
- Hybrid Exchange TLS
- ADFS

AD NOTES

AD NOTES

DHCP's house in AD

When you open the DHCP add-in for an MMC, you're presented with an option to manage authorized servers, but have you ever wondered just where authorized dhcp servers live in active directory? Pop open ADSIEDIT.msc and connect to your configuration. Drill down into Services and then NetServices.

Hybrid Exchange TLS

swapped a cert but messages still stuck in the queue? probably your send connector is being a bitch and holding onto the old cert.

```
$cert = Get-ExchangeCertificate -Thumbprint XXXXXX
```

```
$tlscertificatename = "<i>$($cert.Issuer)<s>$($cert.Subject)"
```

To Replace Send Connector –

```
Set-SendConnector "Outbound to Office 365" -TlsCertificateName $tlscertificatename
```

To Replace Receive Connector –

```
Set-ReceiveConnector "EXCH1\Default Frontend EXCH1" -TlsCertificateName $tlscertificatename
```

if you don’t update receive connector you can see hybrid mail flow stops with TLS error

Reason: [{LED=450 4.4.317 Cannot connect to remote server [Message=451 5.7.3 STARTTLS is required to send mail] [LastAttemptedServerName=83.0.59.81] [LastAttemptedIP=83.0.59.81:25] [DX2ARE01FT002.eop-are01.prod.protection.outlook.com]};{MSG=451 5.7.3 STARTTLS is required to send mail}

ADFS

Swapping certs is a bitch. dont forget to set the TLS cert for the server in addition to the service certificate. this isnt visible in the mmc.

Change the certificate for SSL and Service-Communications using the following commands:

Set-AdfsSslCertificate –Thumbprint XXX
Set-AdfsCertificate -CertificateType "Service-Communications" –Thumbprint XXX

Restart the adfs service.

If you havent given permissions to the new certificates private key to the service account, do that too.

If using a windows WAP, you likely broke the trust too. fix it by running Install-webapplicationproxy

```
$FScredential = Get-CredentialInstall-WebApplicationProxy -FederationServiceName
"FS01.Contoso.com" -FederationServiceTrustCredential $FScredential -CertificateThumbprint
"0a1b2c3d0a1b2c3d0a1b2c3d0a1b2c3d0a1b2c3d"
```

use a user account with admin on the ADFS box, and the certificate used should be the one you intend to present to clients. you can get the thumbprint with:

```
Get-ChildItem -Path cert: -Recurse | select Subject, FriendlyName, Thumbprint | Format-List
```

https://docs.microsoft.com/en-us/powershell/module/webapplicationproxy/install-webapplicationproxy?view=windowsserver2022-ps