ADFS Health Assessment Checklist (Detailed)

1. Inventory and Baseline Review

Identify all ADFS components: Federation Servers, WAP Proxies, SQL/WID backend.

Check ADFS version:

```
Get-AdfsProperties | Select-Object FarmVersion
```

List configured authentication types (Forms, Windows Integrated, etc.).

2. Service and Role Validation

Check if ADFS service is running:

```
Get-Service adfssrv
```

Check WAP (Web Application Proxy) service status:

```
Get-Service adfssrv
```

Review ADFS configuration properties:

```
Get-AdfsProperties | Format-List
```

Review ADFS logs in Event Viewer: Applications and Services Logs > AD FS/Admin

3. Endpoint and Metadata Validation

Test metadata endpoint in browser:

```
https://<adfs_FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
```

Test IdP-Initiated Sign-On page:

```
https://<adfs_FQDN>/adfs/ls/IdpInitiatedSignon.aspx
```

PowerShell check for metadata:

```
Invoke-WebRequest -Uri 'https://<hostname>/FederationMetadata/2007-06/FederationMetadata.xml' -UseBasicParsing
```

4. Network and DNS Checks

Ensure DNS resolution for ADFS and WAP FQDNs (internal/external).

Check port access: 443 (HTTPS), 49443 (WID replication).

Validate firewall and NSG rules if hosted in Azure.

5. SSL Certificate Validation

Retrieve ADFS SSL certificate details:

```
Get-AdfsSslCertificate
```

Verify SSL binding:

```
netsh http show sslcert
```

Check certificate expiration and thumbprint.

6. Performance Monitoring

Use Performance Monitor (PerfMon) to monitor ADFS:

```
AD FS\Requests/sec
AD FS\Token Requests
```

Check CPU, memory, and disk usage on ADFS servers.

Retrieve ADFS process resource usage:

```
Get-Process adfssrv
```

7. Replication & High Availability Check

For WID environments, check sync status:

```
Get-AdfsSyncProperties
```

Review LastSyncTime, LastSyncStatus, and PrimaryComputer.

If using SQL backend, validate SQL cluster health and performance.

8. Security Review

Verify MFA settings (Azure MFA, OTP, certificates).

Audit Relying Party Trusts and claim issuance rules.

Review login failures and anomalies via Event Viewer or logs.

9. Run Diagnostics Tools

Install diagnostics module (if not already installed):

```
Install-Module ADFSDiagnostics
```

Run the diagnostic tool:

```
Invoke-AdfsDiagnostics
```

Review output for warnings, misconfigurations, or missing elements.

10. Documentation & Reporting

Document all findings: system info, services, certs, endpoints, errors.

Include logs, screenshots, and remediation recommendations.

Share final report with infrastructure/security teams and leadership.