

Active Directory Domain Services

- Verzeichnisdienst, der Teil den wir in der Schule verwendet haben
- Netzwerkobjekte: Server, Benutzer, Computer, Drucker, ...
- Datenspeicher = relationale Datenbank

Ein Verzeichnisdienst wie AD DS speichert Verzeichnisdaten und stellt Daten für Netzwerkbenutzer und Administratoren bereit. Es werden beispielsweise Informationen über Benutzerkonten wie Namen, Kennwörter, Telefonnummern verwaltet, sodass sie von Administratoren und Benutzern leicht gefunden und verwendet werden können. Für AD wird ein strukturierter Datenspeicher als Basis für eine logische, hierarchische Organisation von Verzeichnisinformationen eingesetzt. Dieses Verzeichnis enthält Informationen zu AD-Objekten. Zu diesen Objekten gehören in der Regel freigegebene Ressourcen wie Server, Volumes, Drucker und die Netzwerkbenutzer- und Computerkonten.

- Rechte und hierarchische Vererbung ähnlich wie bei einem Dateisystem mit Möglichkeit der Unterbrechung
- Schutz vor ungewolltem Löschen von Objekten (zB. Organisationseinheiten)
- Viele Einstellmöglichkeiten und Löschen nur in der erweiterten Ansicht möglich

Die Sicherheit wird durch Anmeldeauthentifizierung und Zugriffssteuerung für Objekte im Verzeichnis in AD integriert. Mit einer einzigen Netzwerkanmeldung können Administratoren Verzeichnisdaten und die Organisation im gesamten Netzwerk verwalten, und autorisierte Netzwerkbenutzer können überall im Netzwerk auf Ressourcen zugreifen.

Quelle: <https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Active Directory Lightweight Directory Services

- Ähnlich zu LDAP
- Abgespecktes AD DS (Kein DNS, keine Computer, keine Group Policies, ...)
- Einsatzbereich?
- Als Verzeichnisdienst für bestimmte Anwendungen geeignet
- Kann man als Authentifizierungsinstanz verwenden

AD LDS arbeitet unabhängig von AD und unabhängig von AD-Domänen oder -Gesamtstrukturen. Er wird entweder als eigenständiger Datenspeicher oder in Kombination mit AD DS betrieben. Seine Unabhängigkeit ermöglicht die lokale Kontrolle und Autonomie von Verzeichnisdiensten für bestimmte Anwendungen. Es erleichtert auch unabhängige, flexible Schemas und Benennungskontexte.

Quelle: <https://docs.microsoft.com/en-us/previous-versions/windows/desktop/adam/what-is-active-directory-lightweight-directory-services>

Active Directory Federation Services

- Authentifizierung für Webanwendungen (Cloud-Anwendungen)
- SSO – Single Sign-ons

Der AD FS ermöglicht die Verbundidentitäts- und Zugriffsverwaltung durch die sichere Freigabe digitaler Identitäts- und Berechtigungsrechte über Sicherheits- und Unternehmensgrenzen hinweg. AD FS erweitert die Möglichkeit, Funktionen für einmaliges Anmelden, die innerhalb einer einzelnen Sicherheits- oder Unternehmensgrenze verfügbar sind, auf mit dem Internet verbundene Anwendungen zu verwenden, um Kunden, Partnern und Lieferanten eine optimierte Benutzererfahrung beim Zugriff auf die webbasierten Anwendungen einer Organisation zu ermöglichen.

Quelle: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview>

Active Directory Rights Management Services

- Schützen, verschlüsseln und signieren von Dokumenten, E-Mails

AD RMS kann verwendet werden, um die Sicherheitsstrategie für Organisationen zu erweitern, indem Dokumente mithilfe der Verwaltung von Informationsrechten (Information Rights Management, IRM) geschützt werden.

AD RMS ermöglicht es Einzelpersonen und Administratoren über IRM-Richtlinien, Zugriffsberechtigungen für Dokumente, Arbeitsmappen und Präsentationen anzugeben. Auf diese Weise wird verhindert, dass vertrauliche Informationen von unbefugten Personen gedruckt, weitergeleitet oder kopiert werden. Nachdem die Berechtigung für eine Datei mithilfe von IRM eingeschränkt wurde, werden die Zugriffs- und Nutzungsbeschränkungen unabhängig davon, wo sich die Informationen befinden, erzwungen, da die Berechtigung für eine Datei in der Dokumentdatei selbst gespeichert ist.

Quelle: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831364\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831364(v=ws.11))

Active Directory Certificate Services

- Vertraulichkeit durch Verschlüsselung
- Integrität durch digitale Signaturen
- Authentifizierung durch Zuordnen von Zertifikatschlüsseln zu Computer-, Benutzer- oder Gerätekonten in einem Computernetzwerk

AD CS bietet anpassbare Dienste zum Ausstellen und Verwalten digitaler Zertifikate, die in Softwaresicherheitssystemen verwendet werden. Die bereitgestellten digitalen Zertifikate können zum Verschlüsseln und digitalen Signieren elektronischer Dokumente und Nachrichten verwendet werden. Diese digitalen Zertifikate können für die Authentifizierung von Computer-, Benutzer- oder Gerätekonten in einem Netzwerk verwendet werden.

Quelle: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831740(v=ws.11))