2015

Planung einer zentralen Benutzerverwaltung

INFRA 4BHIT

PHILIPP ADLER, JAKUB KOPEC, ADIN KARIC

TGM | Wexstraße 19-23

Inhaltsverzeichnis

1. Aufgabenstellung

1.1. Ausgangssituation

Sie sind als Netzwerk- und Systemadministrator für bei einem Startup-Unternehmen angestellt worden. Dieses benötigt eine Vielzahl von Netzwerk-Services (Mail, Web, Filesharing, Drucken, Login am Desktop, ...) für die eine zentrale Benutzerverwaltung eingeführt werden soll.
Die Mitarbeiter des Unternehmens arbeiten mit heterogenen Systemen - manche unter Linux, machen unter Windows, manche unter Mac OS und einige mit FreeBSD. Die zentrale Authentifizierung soll bei all diesen Systemen funktionieren. Als nice-to-have Feature wünscht sich das Unternehmen eine Single-Sing-On-Lösung.

1.2. Aufgabenstellung

Vergleichen Sie für dieses Unternehmen die Kosten (Hardware-Anforderungen, Lizenzkosten, geschätzter Administrationsaufwand/Monat) für die Einführung einer zentralen Benutzerverwaltung (OpenLDAP oder Active Directory) sowie der dazugehörigen Server-Systeme (Webserver, Mailserver, Fileserver).
Überlegen Sie auch, ob für die gegebene Aufgabenstellung eine lokale Server-Infrastruktur benötigt wird, oder ob manche/alle Dienste in ein Cloud-Service ausgelagert werden können (z.B. AWS, Azure, Google Cloud, ...).

1.3. Abgabe

Geben Sie die fertige Kosten- und Aufwandsabschätzung als ordentlich formatiertes Dokument im PDF Format ab.
Das Dokument muss (zusätzlich zum "ordentlichen Aufbau", also Titelseite, Inhaltsverzeichnis, Kopf- und Fußzeilen, ...) die Evaluation der zur Auswahl stehenden Software-Lösungen sowie eine detaillierte Zeit- und Kostenaufstellung enthalten.
Die Arbeit in Gruppen (maximal 3 Personen, andere Gruppenzusammenstellung als bei der letzten Übung!) ist erlaubt.

1.4. Aufwand

Geschätzter Aufwand: 5h
Benötigter Aufwand(nach Verbesserung): 8h

2.Active Directory

Vorteile von Active Directory

- Informationssicherheit
- Richtlinienbasierte Verwaltung
- Erweiterungsfähigkeit
- Skalierbarkeit
- Replikation von Informationen
- DNS-Integration
- Zusammenarbeit mit anderen Verzeichnisdiensten

Benutzer- und Computerkonten im Active Directory sind einer physisch vorhandenen Person oder einem Computer zugeordnet. Diese Konten werden als Sicherheitsprincipals bezeichnet, denen eine Sicherheitskennung zugewiesen ist. Objekte mit Sicherheitskennung können sich am Netzwerk anmelden und auf Domänenressourcen zugreifen. Benutzer- und Computerkonten haben folgende Aufgaben:

- Authentifizierung des Benutzers oder des Computers
- Zugriffskontrolle auf Domänenressourcen
- Verwaltung anderer Sicherheitsprincipals
- Überwachungsaufgaben

http://www.elektronik-kompendium.de/sites/net/0905041.htm

2.1. Hardwarevoraussetzungen

Keine speziellen Harewareanforderungen, Speicheranzahl variiert mit den User-Accounts.

2.2. Kosten

Lizenzkosten:

Es gibt 3 Varianten von Azure Active Directory:

- Free → kostenlos
- Basic → ca. 1$ pro User pro Monat
- Premium → ca. 8$ pro User pro Monat

Features	Azure AD (Free)	Azure AD Basic	AAD Premium
Directory as a Service	Up to 500k Objects	No Object Limit	No Object Limit
User/Group Management	Yes	Yes	Yes
SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	10 apps per user	No Limit
Identity Synchronization Tool (WSAD Extension, Multi Forest, 3rd party)*	Yes	Yes	Yes
User-Based access management/provisioning	Yes	Yes	Yes
Self-Service Password Change for cloud users	Yes	Yes	Yes
Basic Security Reports	Yes	Yes	Yes
Cloud App Discovery (in public preview)	Yes	Yes	Yes
Group-based access management/provisioning		Yes	Yes
Self-Service Password Reset for cloud users		Yes	Yes
Company Branding (Logon Pages/Access Panel customization)		Yes	Yes
SLA		Yes	Yes
Identity Synchronization Tool advanced write-back capabilities (in preview)			Yes
Self-Service Group Management			Yes
Self-Service Password Reset/Change with on-premises write-back*			Yes
Advanced Security Reporting (machine learning-based)			Yes
Advanced Usage Reporting			Yes
MFA Cloud and On-premises (MFA Server)			Yes
FIM CAL + FIM Server			Yes

Hardwarekosten:

Da die Hardwarevorraussetzungen für Active Directory nicht besonders groß sein müssen, da dieser Verzeichnisdienst auf so gut wie jedem Rechner ordnungsgemäß funktionieren kann, halten sich somit die Hardwarekosten in Grenzen. Ein durchschnittlicher „Office-Rechner“ reicht für diesen Verzeichnisdienst mehr als vollkommen.

2.3. Administrationsaufwand/Monat:

Active Directory benötigt richtig eingerichtet keinen besonders hohen Administrationsaufwand. Aufgrund der höheren Komplexität des Systems, rechnen wir mit einem Administrationsaufwand von 20 Stunden im Monat. Pro Stunde werden 100€ verrechnet.

3. OpenLDAP

Vorteil von OpenLDAP:

- sehr weit verbreitet
- sehr viele andere LDAP System auf OpenLDAP basieren.
- OpenLDAP ist in den meisten Linux Distributionen, Unix, Mac und Windows verfügbar

3.1. Hardwarevoraussetzungen

Die Hardwareanforderungen von LDAP sind hinsichtlich erforderlichem Plattenplatz sehr gering. OpenLDAP braucht nur ca. 6 MB Platz auf der Festplatte für die Installation von Server und Hilfsdateien. Die Datenbank braucht, je nach Datenbestand, 50 KB bis ca. 20 MB (bei 20'000 Datensätzen) freien Festplattenspeicher.

Auch an Arbeitsspeicher und CPU werden keine besonderen Mindestanforderungen gestellt, da sie unter denen des Betriebssystems liegen, sollten aber in Hinblick auf eine performante Suche nicht allzu altertümlich sein.

3.2. Kosten

Lizenzkosten:

Da OpenLDAP „open-source" ist, Fallen die Lizenzkosten in diesem konkreten Fall, komplett weg.

Hardwarekosten:

Da die Hardwarevorraussetzungen für OpenLDAP nicht besonders groß sein müssen, da dieser Verzeichnisdienst auf so gut wie jedem Rechner ordnungsgemäß funktionieren kann, halten sich somit die Hardwarekosten in Grenzen. Ein durchschnittlicher „Office-Rechner" reicht für diesen Verzeichnisdienst mehr als vollkommen.

Gesamtkosten:

Da nur OpenSource Software verwendet wird, stellen sich die Gesamtkosten nur aus den Hardwarekosten und dem geschätzten Administrationsaufwand zusammen.

3.3. Administrationsaufwand/Monat:

OpenLDAP benötigt richtig eingerichtet keinen besonders hohen Administrationsaufwand. Daher rechnen wir mit ca 10 stunden Administrationsaufwand im Monat. Pro Stunde werden 100€ verrechnet.

4. Serversysteme

4.1. Webserver(Apache):

Apache ist eine Open-Source-Software für Webserver, die von der Apache Software Foundation entwickelt wurde. Auf einem solchen HTTP-Server werden Online-Informationen und Websites als http-Services bereitgestellt, die auf Anforderung von Web-Browsern abgerufen werden. Der Apache-Server ist der am häufigsten eingesetzte Webserver und arbeitet mit den Betriebssystemen Unix, Linux, Windows, Mac OS X, Netware, OpenBSD und einigen anderen.

Apache-Server sind als Kombination aus Linux, Apache-Software, der Datenbank MySQL und der Scriptsprache Hypertext Preprocessor (PHP) konfiguriert, die als LAMP abgekürzt wird.

4.2. Webserver(IIS 7.0)

Der Webserver Internet Information Server und die Webplattform ASP.NET gingen trotz vieler Gemeinsamkeiten bei der Konfiguration bisher eigene Wege. Nun vermählt Microsoft mit IIS 7.0 die beiden und stellt sie auf eine gemeinsame Basis. Gleichzeitig baut Microsoft den einst als reiner Webserver zur Welt gekommenen IIS zum Anwendungsserver aus. Microsoft nennt seinen Webserver Internet Information Server (IIS) 7.0 einen komponentenbasierten Server, weil er aus einzelnen unabhängigen Softwarekomponenten zusammengebaut ist. Das bietet den Vorteil, dass nur die wirklich benötigten Funktionen installiert werden müssen. Anders als der monolithische Vorgänger IIS 6.0, besteht IIS 7.0 aus einem kleinen Webserverkern (Web Core Server) und mehr als 40 IIS-Modulen für Netzwerkprotokolle, Protokollierung, Konfiguration, Authentifizierungsverfahren und Diagnose.

Der Aufbau aus Komponenten zeigt sich bereits beim Setup: Bei der Installation des IIS auf einem Longhorn-Server mithilfe des Add Roles Wizard fordert Windows als Grundlage die Installation des Windows Activation Service (WAS). WAS aber ist in der neuen Windows-Generation der Systembaustein, der für den IIS die Anwendungspools und Prozesse verwaltet.

In dem folgenden Installationsfenster kann der Administrator sehr viel genauer als in der Vergangenheit die einzurichtenden Funktionen auswählen. Neben Frameworks wie ASP, ASP.NET, CGI und ISAPI lassen sich in den Bereichen „HTTP-Features“, „Health and Diagnostics“, „Security“ und „Management Tools“ die gewünschten Module selektieren. Im Bereich Sicherheit sind verschiedene Authentifizierungsverfahren wie zum Beispiel Basic, Windows, Digest oder Zertifikate wählbar. Bei den Management-Diensten steht unter anderem zur Wahl, ob sich IIS 7.0 auch mit den Verfahren eines IIS, also mit Konsole, Skript oder per WMI verwalten lassen soll und ob eine Fernverwaltung des IIS über einen Management-Service erlaubt sein soll.

Die komponentenorientierte Architektur erlaubt auf jeder Ebene (Webserver, Website, Anwendung oder Verzeichnis) Modulsätze zu erstellen. So ist so beispielsweise möglich, einen Webserver zu betreiben, der ausschließlich Windows-NTLM-Authentifizierung, statische Webseiten, Kompression und Protokollierung beherrscht.

Im Hinblick auf Sicherheit reduziert dies die Angriffsfläche und erhöht die Sicherheit des Webservers gegenüber dem IIS 6.0, der nur für die Anwendungsentwicklungsframeworks eine Möglichkeit zum Deaktivieren von Merkmalen bot. Neben höherer Sicherheit ist von einem auf die notwendigen Module reduzierten Webserver auch eine bessere Leistung zu erwarten.

Installieren lässt sich IIS 7.0 auf Windows Longhorn Servern sowie den Home-Premium-, Business- und Ultimate-Varianten von Windows Vista. Auf keiner Plattform gehört IIS zur Standardinstallation, sondern ist immer eine Option, die nach dem Einrichten des

Betriebssystems zu aktivieren ist. Bei Windows Vista in der Systemsteuerung, beim Longhorn-Server mithilfe des Rollenassistent. Der IIS 7.0 wird nicht zu 100%-Kompatibel zu Vorgängerversionen sein (siehe Kasten "Kompatibilität zu vorherigen Versionen").

Der IIS war bisher ein Web-, Datei-, Mail- und Newsserver. Ab Version 7.0 wird der IIS auch TCP, MSMQ und Named Pipes verstehen und damit zum allgemeinen Host für die Windows Communication Foundation werden. Neben dem bereits aus der Vorgängerversion bekannten Kernel-Mode Listener HTTP.sys installiert der IIS 7.0 die Listener NET.TCP, NET.PIPE and NET.MSMQ. Beim Eintreffen einer Anfrage in einem der Listener prüft der Windows Activation Server (WAS), ob es bereits einen Arbeitsprozess gibt, der die Anfrage bearbeiten kann. Sofern noch keiner vorliegt, erzeugt WAS einen passenden Prozess. Der Aktivierungsdienst kann auf Wunsch verschiedene Protokolle in einem Arbeitsprozess bedienen. Die Anwendungspools dieses Dienstes besitzen ähnliche Eigenschaften wie die IIS 6.0-Anwendungspools, zum Beispiel Prozessidentität oder Recycling-Funktionen.

Im IIS 7.0 legt Microsoft Wert auf eine einfachere Konfiguration. Bisher ergaben sich die Einstellungen für eine Webanwendung aus dem Zusammenspiel der Einstellungen in der IIS-Metabase, die über den IIS-Manager festgelegt wurden, und den Einstellungen in den XML-basierten ASP.NET-Konfigurationsdateien, den web.config-Dateien.

Der neue Webserver übernimmt das .NET-basierte Konfigurationssystem, das heißt alle Einstellungen einer Webanwendung, sowohl die von ASP.NET als auch die des IIS, werden in .config-Dateien gespeichert. Microsoft spricht vom „Configuration Store“, der die bisherige Metabase ersetzt.

Web.Config-Dateien bieten gegenüber dem bisherigen Metabase-basierten Konfigurationsmodell vier wesentliche Vorteile:

- Die Konfigurationsdateien lassen sich mit einfachen Text- oder XML-Editoren bearbeiten.
- Die Konfigurationsdateien sind einfacher, nämlich per Dateikopie und auch per FTP übertragbar. Geänderte Konfigurationsdateien führen außerdem sofort zur Verhaltensänderung des Servers.
- Die Konfigurationsdateien liegen im Ordner des jeweiligen Webprojekts. Das macht die Delegation von administrativen Aufgaben einfacher, da der für diese Datei verantwortliche Mitarbeiter weder die Frontpage Server Extensions noch einen RPC-Zugang zu dem Webserver-Dienst benötigt.
- Die Konfigurationsdateien bilden eine Hierarchie. In jedem Unterverzeichnis können Konfigurationsdateien existieren, wobei untergeordnete Konfigurationsdateien übergeordnete Einstellung überschreiben.

Neben der Hochzeit auf Konfigurationsebene finden IIS und ASP.NET auch auf der Ebene der Verarbeitung eines Seitenabrufs über die Request Pipeline zueinander. Bisher kümmerte sich zunächst der IIS um die Anfrage und übergab sie dann an aspnet_isapi.dll; die von ASP.NET erzeugte Antwort ging wieder zurück an IIS, der sie an den Client gesendet hat. In dem neuen Integrated Application Pool Mode lassen sich die Modulen in beliebiger Reihenfolge nacheinander ausführen, egal ob es sich um Module in verwaltetem Code wie bei dem Modulen für ASP.NET HTTP Handler und HTTP oder in unverwaltetem wie beim Win32 HTTP Module handelt. Bisherige Doppelarbeiten, zum Beispiel im Bereich der Authentifizierung für den Webserver und für ASP.NET, entfallen dadurch. Die Administration wird einfacher, da sie nicht mehr zwischen IIS- und ASP.NET-Modulen unterschiedet. Der IIS verwaltet alle Module im Element <modules> in den Konfigurationsdateien. In dem neuen Modell sind die aus ASP.NET stammenden Konfigurationselemente <httpModules> und <httpHandlers> ohne Bedeutung. Daraus ergibt sich, was Microsoft „Unified Request Pipeline“ nennt: eine gemeinsame Aufrufkette für die beiden Modultypen. Um die Kompatibilität zu wahren, lässt sich IIS 7.0 auch

in den „ISAPI Application Pool Mode“ schalten. Dann funktioniert die Pipeline wieder wie im IIS 6.0.

http://www.it-visions.de/glossar/alle/109/Internet_Information_Server.aspx

4.3. Mailserver(Postfix):

Postfix ist ein Open-Source Mail Transfer Agent (MTA). Es implementiert den ersten Layer für Schutz gegen Spambots und Malware. Es ist schnell, sicher und einfach zu administrieren.

4.4. Mailserver(DOVECOT-mail)

Dovecot (englisch für Taubenschlag) ist eine Mailserver Software-Suite. Sie ist als Mail Delivery Agent (MDA) und für die Netzwerkprotokolle POP3 und IMAP gestaltet.

Die Software-Suite arbeitet unter UNIX, BSD und unixoiden Systemen wie Linux. Sie ist Open Source mit gemeinfreien Teilen und anderen unter LGPL oder MIT-Lizenz neben eigenständigen Lizenzen.

Der relativ junge IMAP-Server wird von Timo Sirainen seit 2002 als moderne Alternative zu Courier-IMAP mit besonderem Fokus auf Sicherheit entwickelt. Allerdings hat ihm erst der Code der inzwischen vollständig überarbeiteten Version 1.0 aus dem Jahr 2007 Dovecot seinen Ruf als derzeit bester und vor allem sicherster IMAP-Server verschafft.

https://thomas-leister.de/internet/mailserver-ubuntu-server-dovecot-postfix-mysql/

http://www.admin-magazin.de/Das-Heft/2012/02/Eigener-Mailserver-mit-Postfix-und-Dovecot

4.5. Fileserver(FTP Dienst):

ProFTPD ist ein weit verbreiteter FTP-Server für UNIX-Plattformen, der die Standards FTP, SFTP, und FTPS unterstützt. Im Vergleich mit anderen Programmen zeichnet er sich insbesondere durch vielfältige Konfigurationsmöglichkeiten aus. Speziell bei Ubuntu muss man berücksichtigen, dass die Version aus den offiziellen Paketquellen der Sektion universe zugeordnet ist und damit – im Gegensatz zum vsftpd – keine Sicherheitsupdates erhält.

4.6. Fileserver(Samba Server)

Samba ist eine freie Software für UNIX-Betriebssysteme, wie Linux/Debian/Raspbian, die das SMB (Server-Message-Block-Protokoll) bereitstellt, welches maßgeblich von Microsoft geprägt wurde. Praktisch bedeutet das, dass man mittels eines Samba Servers Datei- und Druckdienste von Microsoft Windows emulieren kann. Mit dem Samba Dateiserver ist es möglich, eine Netzwerkfreigabe im eigenen Netzwerk aufzubauen. Dies ist nützlich, wenn man z.B. Urlaubsvideos auf einem Linux Rechner abgelegt hat und diese allen berechtigten Rechnern im Netzwerk zugänglich machen möchte. Aufgrund des geringen Strombedarfs bietet sich für einen solchen zentralen Server der Raspberry Pi natürlich an. Wie man einen Samba Server auf dem Raspberry Pi installiert, Netzwerkfreigaben schaltet und Benutzer anlegt, erkläre ich im Folgenden. Da die Software unter der GPL-Lizenz kostenfrei verfügbar ist, wird sie als Alternative zu Microsoft-Windows-Server-Betriebssystemen eingesetzt.

http://jankarres.de/2013/11/raspberry-pi-samba-server-installieren/

4.7. Kosten:

Lizenzkosten:

Es wird nur OpenSource Software verwendet, deshalb fallen keine Softwarekosten an, Ausnahme MS IIS.

Hardwarekosten:

Je nach dem ob man die oben beschriebenen Dienste auf einzelnen oder verschiedenen Servern installiert variiert auch der Preis. Grundsätzlich kann man sagen, dass diese Dienste keine spezifischen Hardwareanforderungen benötigen und somit auf jedem beliebigen Server einwandfrei funktionieren werden. Somit halten sich die Kosten ziemlich gering. Wenn man von der Annahme ausgeht, dass man nur einen Server für all diese Dienste in Anspruch nimmt , kann man schon ab 5€ monatlich einen Server bei diversen Anbietern im Internet zwar nicht käuflich erwerben, aber mieten.

5.Cloud Service

5.1. Amazon EC2 Server

Die Auslagerung in ein Cloud Service bietet sich an. Das Unternehmen benötigt hierfür aber eine gute Internetanbindung um die Latenz- und Synchronisationszeit niedrig zu halten.

Es wird ein Amazon EC2 Server in der Klasse t2.medium vorgeschlagen. Dieser bietet 2 vCPU Cores und 4GB RAM. Der Speicher ist variabel und kann jederzeit reduziert und erweitert werden.

5.2. Azure Active

Azure Active Directory ist eine umfassende Cloudlösung mit hoher Verfügbarkeit für die Identitäts- und Zugriffsverwaltung. Sie kombiniert grundlegende Verwaltungsdienste mit Identitätsgovernance und Zugriffsverwaltung für Anwendungen. Azure Active Directory bietet auch eine umfassende auf Standards basierende Plattform, mit der Entwickler ihre Anwendungen mit einer Zugriffssteuerung ausstatten können, die auf zentralisierten Richtlinien und Regeln basiert.

Azure Active Directory wird in drei Stufen angeboten: Kostenlos, Basis und Premium. Eine detaillierte Liste der Features finden Sie in der Tabelle unten.

Azure Active Directory Kostenlos umfasst die Zugriffsverwaltung für Clodanwendungen und entspricht den Self-Service-Identitätsverwaltungsanforderungen von Aufgabenworkern und den wichtigsten Cloudanforderungen. Die Basisstufe von Azure Active Directory beinhaltet alle verfügbaren kostenlosen Azure AD-Funktionen und stellt zusätzlich gruppenbasierte Zugriffsverwaltung, Self-Service-Kennwortzurücksetzung für Cloudanwendungen, anpassbare Umgebung für den Start von Unternehmens- und Endbenutzeranwendungen bereit.

Azure Active Directory Premium ermöglicht IT-Abteilungen den effektiven Schutz von Unternehmensdaten und Ressourcen in jeder beliebigen Cloud mit Features wie Synchronisierung mit lokalen Verzeichnissen, gruppenbasierter Einzelanmeldung bei Tausenden von SaaS-Anwendungen, Sicherheits- und Nutzungsberichte, die auf der Funktion für maschinelles Lernen basieren, Warnungen und mehrstufige Authentifizierung. Azure Active Directory Premium ermöglicht Endbenutzern Self-Service-Kennwortzurücksetzung, delegierte Gruppenverwaltung

und anpassbare Umgebung für den Start von Unternehmens- und Endbenutzeranwendungen.

Die Azure AD Access Control ermöglicht die zentralisierte Authentifizierung und Autorisierung für Ihre Cloud-Anwendung durch die Zusammenarbeit mit standardbasierten Identitätsanbietern wie etwa Active Directory sowie mit Verbraucherwebidentitäten wie Microsoft-Konto, Google, Yahoo! und Facebook.

Azure Active Directory wird in drei Stufen angeboten: Kostenlos, Basisund Premium.

Azure Active Directory Basis und Premium sind separat von Azure-Diensten lizenziert und stehen zum Kauf über das Volumenlizenzierungsprogramm des Konzernvertrags von Microsoft zur Verfügung.

http://azure.microsoft.com/de-de/pricing/details/active-directory/