

Linux - Der bessere Nachfolger von Microsoft Windows 2000/2003?

Mit Open Source Software dem auslaufenden Support von Microsoft Windows 2000 Server begegnen

Inhaltsverzeichnis

Mit Open Source Software dem auslaufenden Support von Microsoft Windows 2000 Server begegnen...	1
1 Support für Microsoft Windows 2000 läuft aus.....	2
1.1 Handlungsbedarf.....	2
1.2 Migrationspfad.....	3
1.3 Kernfunktionen von Microsoft Windows 2000 Server.....	3
2 Grundlegende Gedanken zur Migration.....	5
2.1 Migrationsziel.....	5
2.2 Technologiewandel.....	5
3 Zugang zu neuen Technologien durch den Einsatz von Open Source Software.....	7
3.1 Open Source Software.....	7
3.2 Offene Standards.....	8
3.3 Open Source in der Unternehmensstrategie.....	8
4 Abdeckung von Microsoft Windows 2000 Server Funktionen mit Open Source Software.....	8
4.1 Domain Controller mit Samba.....	10
4.2 Verzeichnisdienst mit OpenLDAP.....	10
4.3 Single Sign-On.....	11
4.4 Public Key Infrastructure.....	11
4.5 Druckdienst mit CUPS.....	12
4.6 Migrationsschritte für typische Einsatzszenarien.....	12
4.7 Integration, Pflege und Support.....	12
5 Univention Corporate Server als fertige Open Source Plattform für die Unternehmens IT.....	13
5.1 Überblick Univention Corporate Server.....	13
5.2 Domänenkonzept.....	15
5.3 Datei- und Druckdienste.....	16
5.4 UCS Managementsystem.....	16
5.5 Univention Directory Manager.....	16
5.6 UCS Active Directory Connector.....	17
5.7 Virtualisierung.....	17
5.8 Thin Client und Remote Desktop Services.....	17
5.9 Groupware.....	18
5.10 Softwarepflege.....	18
5.11 Implementierung und Migrationsschritte mit UCS.....	18
6 Fazit.....	19
7 Erläuterungen der Funktionen.....	20
8 Literaturverzeichnis.....	21

Zehn Jahre nach der Veröffentlichung von Microsoft Windows 2000 läuft der Herstellersupport für dieses Betriebssystem am 13. Juli 2010 aus. Zwar verwendet kaum ein Unternehmen Microsoft Windows 2000 noch auf dem Desktop, doch im Serverbereich gibt es noch zahlreiche unternehmenskritische Installationen.

Dieses White Paper beschreibt die Folgen des auslaufenden Supports für Anwender und geht darauf ein, welche Optionen dem EDV-Verantwortlichen zur Verfügung stehen. Es zeigt den von Microsoft vorgesehenen Umstellungspfad und beschreibt, welche Alternativen dazu durch den Einsatz von Linux und anderer Open Source Software existieren. Es werden außerdem wichtige neue Technologien betrachtet, die im Zusammenhang mit der Erneuerung der IT-Infrastruktur berücksichtigt werden sollten. Ziel dieses White Papers ist es, IT-Verantwortlichen eine belastbare Grundlage für die Beurteilung der Weiterentwicklung ihrer bisher mit Microsoft Serverbetriebssystemen betriebenen IT-Infrastruktur zu geben.

1 Support für Microsoft Windows 2000 läuft aus

Microsoft beendet seinen "Extended Support" für Windows 2000 am 13. Juli 2010 und stellt dann nach eigenem Bekunden jegliche Updates für die gesamte Microsoft Windows 2000 Produktfamilie ein. Kostenlose Selbsthilfe steht bis auf weiteres noch über die Knowledge Base zur Verfügung (vgl. [MS_Support]). Laut Microsofts Support Lifecycle-Richtlinien werden Businessprodukte 10 Jahre lang unterstützt. Das beinhaltet fünf Jahre Mainstream Support mit Hotfixes und Sicherheitsupdates und fünf Jahre Extended Support nur noch mit Sicherheitsupdates (vgl. [MS_Product_Lifecycle]). Daraus folgt, dass auch Anwender von Microsoft Windows 2003 Server beginnen sollten, sich über die Ablösung der entsprechenden Systeme Gedanken zu machen.

1.1 Handlungsbedarf

Anwender müssen handeln: Denn fehlende Sicherheitsupdates und Aktualisierungen des Betriebssystems sind ein Sicherheitsrisiko für Systeme, Infrastruktur und Daten. Darüber hinaus lässt sich die alte Software zum Teil nicht mehr auf aktueller Hardware betreiben, so dass diese nach einem Ausfall nicht mehr ersetzt werden kann. Und schließlich lassen sich neuere Anforderungen wie bei der Kommunikation mit externen Partnern oder der Verwendung neuer Software mit den alten Betriebssystemen immer seltener realisieren.

Das Microsoft Lösungszentrum schlägt eine "*Migration von Windows 2000 nach Windows 7, Windows Server 2003, Windows Server 2008 oder Windows Server 2008 R2.*" (vgl. [Win2K_Update_Path]) vor und stellt dem Anwender Informationen für Bewertung und Planung einer Migrationsstrategie zur Verfügung. "*Eine direkte Aktualisierung von Windows 2000 auf Windows Server 2008 R2 wird nicht unterstützt.*" so die Webseite zum Lösungszentrum (vgl. [MS_Support]). Der Anwender muss also mehrere im folgenden skizzierte Schritte gehen, um seine Infrastruktur auf einen aktuellen Stand zu bringen.

1.2 Migrationspfad

Grundsätzlich kann zwischen zwei Arten der Migration unterschieden werden¹: Fortführende und ablösende Migration:

Fortführende Migration

Unter fortführender Migration wird die Fortführung eines bestehenden Produktes oder einer bestehenden Produktlinie verstanden. Sie bezieht sich auf die Umstellung auf die jeweils neuere Version eines Produktes oder einer Produktlinie, zum Beispiel die Migration von Microsoft Windows 2000 Server auf Microsoft Windows Server 2003.

Ablösende Migration

Eine ablösende Migration handelt dementsprechend von der Ablösung einer Produktlinie oder eines Produktes durch eine andere Produktlinie oder ein anderes Produkt. Ein Beispiel hierfür ist die Ablösung eines Microsoft Windows 2000 Domain Controllers durch Linux und den Serverdienst Samba.

Microsoft legt den Anwendern von Windows 2000 Server eine fortführende Migration und den Verbleib in der Microsoft Windows Produktlinie nahe. Das Ziel der Umstellung kann dabei jedoch nur über Zwischenschritte erreicht werden, so dass mit beträchtlichem Aufwand zu rechnen ist. Die älteste für eine Migration auf Microsoft Windows Server 2008 unterstützte Version des Windows Betriebssystems ist Windows Server 2003.

Das folgende Beispiel veranschaulicht den Aufwand anhand des Microsoft Clusterdienstes: Microsoft empfiehlt für die Migration des Clusterdienstes ein Upgrade von Microsoft Windows 2000 Server nach Microsoft Windows Server 2003. Nach der Migration auf Microsoft Windows Server 2003 hilft der Migrationsassistent des Failoverclusters von Windows Server 2008 bei der fortführenden Migration auf Microsoft Windows Server 2008. Microsoft weist allerdings darauf hin, unbedingt die Hardware-Anforderung mit der vorhanden Hardware vor der Migration des Clusters abzugleichen².

1.3 Kernfunktionen von Microsoft Windows 2000 Server

Windows 2000 erschien in verschiedenen Ausgaben für den Betrieb auf Notebooks, Desktop- und Serversystemen. Die wichtigsten Funktionen in Bezug auf den Serverbetrieb sind in Tabelle 1 aufgeführt.

Im Mittelpunkt der mit Microsoft Windows 2000 Server bereitstellbaren Dienste steht Microsoft Active Directory (AD). Dieser Dienst wurde mit Microsoft Windows 2000 Server eingeführt und zentralisiert die Verwaltung von Benutzern, Windows-Arbeitsplätzen und -servern in einer so genannten "Domain" (Domäne). Eine Domäne dient der zentralen Verwaltung von Computer- und Benutzerkonten über eine gemeinsame Datenbank und fasst diese Informationen in einem Vertrauenskontext zusammen. Andere Dienste greifen meist über LDAP und Microsoft-eigene Schnittstellen auf Microsoft Active Directory zu.

Eine der wichtigsten Funktionen von Microsoft Windows 2000 Server ist der Datei- und Druckdienst. Der Server stellt dabei im Netzwerk ganze Verzeichnisse in Form von Dateifreigaben zur Verfügung. Benutzer oder Projektgruppen erhalten somit einen zentralen Speicherort für ihre Dateien oder ein gemeinsames

¹ Siehe auch "Migrationsleitfaden des Bundesministeriums des Inneren, [BMI2000], Seite 8.

² Vergleiche die Quellen [MS_Cluster_Migration_Path], [MS_Migration_Cluster], [MS_Cluster_Hardware]

Verzeichnis. Eingebundene Dateifreigaben erscheinen dem Benutzer als Netzwerklaufwerke und erlauben einen transparenten Zugriff vergleichbar mit lokalen Dateien und Verzeichnissen. Der Druckdienst hingegen stellt dem Benutzer den Zugriff auf Drucker im Netzwerk zur Verfügung. Ohne ihn bestünde ausschließlich Zugriff auf lokal angeschlossene Drucker.

Microsoft Windows 2000 Server bietet darüber hinaus Funktionen für das Infrastrukturmanagement. Alle Computer sind im Active Directory erfasst und erhalten einen Namen, der über den Namensdienst (DNS) auch anderen Computern im Netzwerk bekannt ist. Die Adresszuweisung übernimmt der so genannte DHCP-Dienst. Windows 2000 Server mit Active Directory ist außerdem eine Voraussetzung für Microsoft Exchange Server und die damit bereit gestellten Groupware-Funktionen von Microsoft Outlook. Daneben gibt es einige weitere Microsoft-Produkte wie SharePoint (erst ab Microsoft Windows Server 2003) als auch Produkte von Drittherstellern, die Microsoft Active Directory voraussetzen.

Tabelle 1 zeigt eine Gegenüberstellung der wesentlichen Funktionen von Windows 2000 Server und Windows Server 2008. Ein *Ja* bedeutet, dass die Funktion von dem entsprechenden Serversystem abgedeckt wird, entweder durch das Betriebssystem selbst oder durch die Installation eines Softwarepakets. Die Unterschiede zwischen den Versionen sind auf den ersten Blick gering. Allerdings wird ein Großteil der Funktionen unter Microsoft Windows Server 2008 durch andere Dienste oder Programme bereit gestellt, wie an den Namen der einzelnen Komponenten in den Spalten sichtbar wird. Die Funktionen Virtualisierung und Firewall sind im Vergleich zu Microsoft Windows 2000 Server neu.

Funktion	Microsoft Windows 2000 Server	Microsoft Windows Server 2008
Identity Management	Ja - Active Directory (AD)	Ja - Active Directory (AD)
Infrastruktur Management	Ja	Ja
Domain Controller für Windows Clients	Ja	Ja
Public-Key-Infrastructure	Ja	Ja
Single-Point-of-Administration	Ja	Ja
Softwareverteilung	Ja - Remote Installation Service	Ja - Windows Deployment Services
Patch Management	Ja - Windows Update Service	Ja - Windows Server Update Services
Remote Desktop Services	Ja - Terminal Services	Ja - Remote Desktop Service
Remote Installation	Ja - Remote Installation Service	Ja - Windows Deployment Services
Unattended Installation	Ja - Antwortdatei	Ja
Druckdienste	Ja	Ja
Dateidienste	Ja	Ja
Replikation Verzeichnisdienste	Ja	Ja
Virtualisierung	Nein	Ja - Hyper-V
Desktop-Virtualisierung	Nein	Ja - Virtual Desktop Infrastructure
Failover Clustering	Ja - Microsoft Cluster Server	Ja - Failover Clustering
Datenbanken	Ja - MS SQL Server	Ja - MS SQL Server
Backup	Ja - NTBackup	Ja - Windows Server Sicherung
Maildienste	Ja - Exchange Server	Ja - Exchange Server
Firewall	Nein	Ja - Windows Firewall
Webproxy	Nein	Ja - Drittprodukt

Funktion	Microsoft Windows 2000 Server	Microsoft Windows Server 2008
Gruppenrichtlinien	Ja	Ja
Single Sign-On	Ja - NTLM, Kerberos	Ja - NTLM, Kerberos
Standortverwaltung	Ja - Active Directory (AD)	Ja - Active Directory (AD)
Remote Administration	Ja - AdminPack	Ja - AdminPack
Laufwerkverschlüsselung	Ja	Ja

Tabelle 1: Vergleich der Funktionen von Microsoft Windows 2000 Server und Microsoft Server 2008

Erläuterungen zu einigen Funktionen befinden sich im Abschnitt *Erläuterungen der Funktionen* am Ende des White Papers.

2 Grundlegende Gedanken zur Migration

Die Migration von IT-Lösungen ist ein komplexes Thema. Im Folgenden werde ein paar wichtige Aspekte der Migration vorgestellt, um eine Hilfestellung bei der Planung zu geben

2.1 Migrationsziel

Bevor die Migration von Windows 2000 Server durchgeführt wird, sind ein paar Vorüberlegungen sinnvoll. Sie helfen das Migrationsziel und die Gesamtstrategie zu definieren. Die Migrationsstrategie sollte sich nicht nur auf die Erneuerung eine bestimmten Funktion beziehen, also zum Beispiel auf die Erneuerung der Domänendienste, sondern auch neue Technologien, Verwendungsweisen und Nutzungsmuster berücksichtigen. Dadurch wird sichergestellt, dass die betreffende Organisation mit ihrer IT auch zukünftig optimal in einem veränderten Umfeld operieren kann. Der Migrationsleitfaden des BMI stellt dazu die Frage: *"Ist eine Migration innerhalb der Lösungsgattung überhaupt der richtige Schritt? Sind die fraglichen Lösungen und ihre Anwendung gemessen am Markt der Lösungen und an den Zielen des IT-Einsatzes überhaupt noch auf der Höhe der Zeit?"*³ Bezogen auf die Migration von Microsoft Windows 2000 Server ergeben sich folgende Einzelfragen:

1. Welche Funktionen werden von Microsoft Windows 2000 Server in der eigenen Infrastruktur bereitgestellt?
2. Welche Funktionen werden in dieser Form weiterhin benötigt?
3. Welche Funktionen können abgestellt und welche Dienste müssen ausgebaut werden?
4. Welche neuen Technologien in Form von zusätzlichen Funktionen sollen bereitgestellt werden?

2.2 Technologiewandel

In der letzten Dekade haben viele neue Technologien im Computersektor Einzug gehalten. Die Notwendigkeit zur Migration bietet eine gute Möglichkeit jene Technologien einzusetzen, die für die unternehmenseigene Computerinfrastruktur einen zusätzlichen Nutzen herbei führen.

³ [BMI2008] Seite 22.

Eine fortführende oder ablösende Migration von Microsoft Windows 2000 Server verfolgt vordergründig den Erhalt der bereitgestellten Funktionen. Microsoft Windows-Umgebungen sind meist über die Zeit gewachsen. Eine Konsolidierung durch Zusammenführen von Infrastrukturen und Daten und die Zentralisierung der Administration kann ein weiterführendes Ziel der Migration sein. Langfristig werden dadurch Administrationsaufwände und die Komplexität reduziert, wodurch Wirtschaftlichkeit und Benutzbarkeit verbessert werden.

Die folgende Auswahl wichtiger IT-Trends enthält Themen, die in den letzten drei Jahren in vielen Unternehmen bearbeitet worden sind oder auf der Agenda einzuführender Technologien stehen⁴:

- » Cloud Computing
- » Client Computing
- » Virtualisierung
- » Sicherheit und aktives Monitoring
- » Mobile Anwendungen
- » Green IT
- » Social Software
- » Web 2.0

Im Folgenden werden beispielhaft zwei Fragenkomplexe betrachtet, die sich mit den genannten Technologien auseinandersetzen und in den Migrationsprozess einfließen sollten:

1. Welche Möglichkeiten ergeben sich, um die Nutzung von Informationstechnik über den gesamten Lebenszyklus hinweg effektiv aber auch umwelt- und ressourcenschonend zu gestalten? Wie kann die Computerinfrastruktur in Richtung Green IT optimiert und damit Kosten gespart werden? Einsparpotential besteht hier vor allem in der Konsolidierung von Servern und Diensten auf einigen wenigen Systemen durch Virtualisierung.
2. Wie kann dann bei der Konsolidierung durch Virtualisierung Sicherheit, Datenschutz und aktives Monitoring gewährleistet werden? Eine Konsolidierung der Clients in einer Thin Client Infrastruktur mit Remote Desktop Services bringt Vorteile bei Stromverbrauch, Lärm- und Wärmeentwicklung der Geräte und bei der Administration durch die zentrale Verwaltung. Die einfach Austauschbarkeit der Systeme steigert die Unabhängigkeit von der Hardware. Darüber hinaus ermöglicht Virtualisierung eine sicherheitstechnische Trennung der virtuellen Maschinen durch Isolation. Auf einem Computer können mehrere virtuelle Maschinen zeitgleich parallel betrieben und der Auslastungsgrad optimiert werden.

Die vorgestellten Fragen sind natürlich nicht vollständig und zeigen nur Ausschnitt davon, in welchen Bereichen Überlegungen zur Migration angestellt werden sollten. Sie zeigen aber auch, dass eine Migration, egal ob fortführend oder ablösend, ein Konzept benötigt, in das derartige Fragen einfließen, die abhängig von der Umgebung beantwortet werden müssen.

4 Siehe [Gartner2009], [CIO2010], [CIO2009], [CP2009], [CIO2008]

3 Zugang zu neuen Technologien durch den Einsatz von Open Source Software

Bevor auf den Einsatz von Open Source Software selbst eingegangen wird, soll der Begriff Open Source zunächst kurz erläutert und dargestellt werden, welche Bedeutung diese Form von Software und eine darauf ausgerichtete Strategie für Organisationen hat.

3.1 Open Source Software

Der Begriff Open Source bezeichnet Software, die zusammen mit dem Quelltext unter einer Lizenz veröffentlicht wird, die dem Nutzer besondere Rechte einräumt. So ist der so genannte Quelltext der Schlüssel zum Verständnis der Software und vergleichbar mit einem elektronischen Schaltplan. Die Lizenz von Open Source Software stellt im Gegensatz zu klassischen Softwarelizenzen unter anderem sicher, dass der Quelltext der Software gelesen, verändert und verbessert und weitergegeben werden darf.

Open Source Software leistet einen wichtigen Beitrag zu Wahlfreiheit, Flexibilität, Qualität, niedrigeren Kosten, Transparenz und Herstellerunabhängigkeit, weil sie die Abhängigkeit des Anwenders vom Softwarehersteller drastisch reduziert. Der Anwender kann die Software selbst verändern oder von Dritten verändern lassen. Er ist dabei nicht mehr ausschließlich vom Hersteller abhängig. Die Entwicklung von Open Source Software ist oft in Projekten über das Internet organisiert. Eine Gruppe von Softwareentwicklern und Anwendern bildet hierbei die Community eines Open Source Projekts. Die Verfügbarkeit des Quelltextes erlaubt bei solchen Projekten Jedermann Einblick in den Aufbau der Software und ermöglicht ständige Verbesserungen, die durch eine stetige Weiterentwicklung eine hohe Qualität erzeugt. Beispiele für derartige Open Source Software Projekte sind das Betriebssystem Linux selbst, der Verzeichnisdienst OpenLDAP, die Software Samba und viele tausend weitere Projekte im Internet⁵.

Die Bedeutung von Open Source Software im Unternehmens- und Behördeneinsatz hat in den letzten Jahren stark zugenommen. Laut *Trendstudie Open Source* von Heise ist Open Source für 83 Prozent der Unternehmen von unternehmenskritischer oder wichtiger Bedeutung⁶. Anwender von Open Source Software sind beispielsweise die Oldenburgische Landesbank (OLB), die HUP AG oder das Auswärtige Amt der Bundesrepublik Deutschland. Die OLB ist eine Regionalbank in der Weser-Ems-Region und verfügt über 180 Geschäftsstellen und 2400 Mitarbeiter. Sie setzt Open Source Software für Datei-, Druck- und Authentifizierungsdienste, Applikationsserver und Kontoauszugsdrucker ein (vgl. [OLB]). Die HUP AG ist Hersteller für fachspezifische Softwarelösungen für Verlagshäuser mit mehreren Standorten. Mit Open Source Software werden das gesamte Firmennetzwerk administriert, Benutzer und Gruppen verwaltet und verschiedene Entwicklungs- und Datenbankserver betrieben (vgl. [HUP]).

5 Für weitere Details zur Definition von Open Source Software sei auf die Open Source Initiative unter <http://www.opensource.org/> und die Open Source DEfinition unter [OS_Definition] verwiesen. Für die deutsche Übersetzung der Open Source Definition der Open Source Initiative sei auf die Webseite [OS_Definition_DE] verwiesen.

6 Siehe heise "Trendstudie Open Source" [heise2009]

Das Auswärtige Amt der Bundesrepublik Deutschland betreibt seine Computerinfrastruktur weitgehend vollständig mit Open Source Software und stellt so für über 200 Auslandsvertretungen und über 11.000 Arbeitsplätzen den Betrieb sicher (vgl. [Werner2007]).

3.2 Offene Standards

Open Source Software unterstützt mit der Verfügbarkeit des Quelltextes die Etablierung Offener Standards. Ein Offener Standard ist ein Standard, der von einer gemeinnützigen Organisation beschlossen und gepflegt wird, der veröffentlicht ist und dessen Spezifikation ohne Hürden zugänglich und frei von gewerblichen Schutzrechten ist. Seine Wiederverwendung unterliegt keinen Einschränkungen. Die Verwendung Offener Standards und Softwarelösungen, die diese unterstützen, steigert Herstellerunabhängigkeit und Wahlmöglichkeit der Softwareprodukte. Gute Beispiele für offene Standards sind viele der im Internet verbreiteten Protokolle, wie zum Beispiel HTTP. Diese Protokolle können von jedem verwendet werden. Das hat dazu geführt, dass sie eine breite Herstellerunterstützung gefunden und sich sehr erfolgreich durchgesetzt haben. Eine wachsende Anzahl von Anbietern unterstützt zunehmend Offene Standards mit ihren Produkten.

3.3 Open Source in der Unternehmensstrategie

Open Source Software schafft Transparenz, Flexibilität und Offenheit in Computerinfrastrukturen. Eine Migration sollte darauf ausgerichtet sein, Herstellerabhängigkeiten zu reduzieren und die Flexibilität der betreffenden Organisation so hoch wie möglich zu halten. Open Source und Offene Standards leisten dazu einen wichtigen Beitrag und sollten deswegen in der allgemeinen IT-Strategie verankert werden. Der Migrationsleitfaden unterstreicht diese Ansicht und gibt folgende Empfehlung heraus:

*"Der Einsatz wirklich offener Standards muss ebenso wie die Herstellerunabhängigkeit und die Stärkung des Wettbewerbs ein strategisches Ziel der Behörden sein. Das bedeutet: Um langfristig eine Verbesserung der heutigen Situation hinsichtlich der Häufigkeit von Migrationen und der damit verbundenen hohen Kosten herbeizuführen, sollten die Behörden die [...] Ziele in ihre IT-Strategie aufnehmen und auch durchsetzen, insbesondere ist es wichtig die wirklich offenen Standards zu verwenden, da diese eine gewichtige Grundlage für die Umsetzung der anderen Ziele sind."*¹⁷

4 Abdeckung von Microsoft Windows 2000 Server Funktionen mit Open Source Software

Natürlich ist der Einsatz von Open Source Software nur dann möglich, wenn die benötigten Funktionen damit auch bereit gestellt werden können. Die folgenden Abschnitte zeigen eine Auswahl der Funktionen von Microsoft Windows 2000 Server und deren Abdeckung durch Open Source Software. Tabelle 2 stellt die Funktionen von Microsoft Windows Server 2008 und Open Source Software gegenüber. Ein *Ja* bei Open Source Software bedeutet, dass die Funktion durch Installation und Konfiguration einer bestimmten Open Source Software ohne größeren Aufwand erbracht werden kann. Ein *Nein* bedeutet, dass die Funktion nur

7 [BMI2008] Seite 21

durch einen zusätzlichen Integrationsaufwand verschiedener Open Source Software Produkte bereit gestellt werden kann. Wie allerdings die Gegenüberstellung in Tabelle 3 zeigen wird, können auch diese Funktionen mit Open Source Software erbracht werden.

Funktion	Microsoft Windows Server 2008	Open Source Software allgemein
Identity Management	Ja - Active Directory (AD)	Ja - OpenLDAP
Infrastruktur Management	Ja	Ja
Domain Controller für Windows Clients	Ja	Ja - Samba
Public-Key-Infrastructure	Ja	Ja - OpenSSL
Single-Point-of-Administration	Ja	Ja - Webmin, GOsa, UDM/UMC
Softwareverteilung	Ja - Windows Deployment Services	Ja - Distribution, OPSI
Patch Management	Ja - Windows Server Update Services	Ja - Distribution, OPSI
Remote Desktop Services	Ja - Remote Desktop Service	Ja - NX, x2go, X11, RDP
Remote Installation	Ja - Windows Deployment Services	Ja
Unattended Installation	Ja	Ja
Druckdienste	Ja	Ja - Samba, CUPS
Dateidienste	Ja	Ja - Samba, NFS
Replikation Verzeichnisdienste	Ja	Ja - OpenLDAP
Virtualisierung	Ja - Hyper-V	Ja - XEN, KVM
Desktop-Virtualisierung	Ja - Virtual Desktop Infrastructure	Ja - XEN, KVM, VirtualBox
Failover Clustering	Ja - Failover Clustering	Ja - Heartbeat
Datenbanken	Ja - MS SQL Server	Ja - PostgreSQL, MySQL, Ingres, u.a.
Backup	Ja - Windows Server Sicherung	Ja - Bacula, SEP, u.a.
Maildienste	Ja - Exchange Server	Ja
Firewall	Ja - Windows Firewall	Ja
Webproxy	Nein - Ja, über Drittprodukt	Ja - Squid
Gruppenrichtlinien	Ja	Nein
Single Sign-On	Ja - NTLM, Kerberos	Ja - Kerberos, NTLM über Samba
Standortverwaltung	Ja - Active Directory (AD)	Nein
Remote Administration	Ja - AdminPack	Ja - SSH, NX
Laufwerkverschlüsselung	Ja	Ja

Tabelle 2: Vergleich der Funktionen von Microsoft Windows Server 2008 und Open Source Software

Durch die Vielzahl der Open Source Software Produkte und die Flexibilität der möglichen Einstellungen gestaltet sich die Umsetzung mit Managementwerkzeugen, wie sie zum Beispiel für die Realisierung eines Single-Point-of-Administration oder für eine einfache Standortverwaltung benötigt werden, als recht komplex. Open Source Projekte wie Webmin⁸ bieten eine Webschnittstelle zur Verwaltung der Dienste auf einem einzelnen Linux-Server an. Die Art des Patch Managements und der Umfang der angebotenen Patches hängt von der Distribution ab. Kommerzielle Distributionen wie Red Hat Enterprise Linux oder Novell SUSE Linux Enterprise Server erfordern einen Wartungs- und Supportvertrag. Die Paketmanager der Distributionen bringen die nötige Funktionalität für das Patch Management mit.

⁸ <http://www.webmin.com/>

Eine vollständige Abdeckung der Funktionen von Microsoft Windows 2000 durch Open Source Software ist mit umfangreichen Integrationsarbeiten zwischen den einzelnen Komponenten möglich. Anhand eines durchdachten Konzepts können alle notwendigen Komponenten zu einer alternativen Lösung mit korrespondierenden Funktionen zusammengefügt und es kann der Weg einer ablösenden Migration beschränkt werden. Die folgenden Abschnitte gehen auf eine Auswahl einzelner Open Source Software Produkte und ihre Kernfunktionen näher ein.

4.1 Domain Controller mit Samba

Samba⁹ ist ein Open Source Softwarepaket, das gegenüber Microsoft Windows-basierten Clients (Windows 95, Windows 98, Windows ME, Windows 2000, Windows XP, Windows 7) die wesentlichen Funktionen eines Windows Serversystems zur Verfügung stellt. Dies sind insbesondere Datei-, Druck- und Anmeldedienste. Samba "spricht" dazu dasselbe Protokoll, welches ansonsten von Windows-basierten Serversystemen benutzt wird. Dadurch verhält sich ein Samba-Server aus der Sicht von mit Microsoft Windows betriebenen Clients so wie ein Windows-Server und die Clients können in gewohnter Weise ohne die Verwendung irgendwelcher Zusatzsoftware benutzt werden. Dies geht so weit, dass Samba sogar als so genannter "Domain Controller" fungieren kann, in dieser Konfiguration stellt die Software den Windows Clients alle zum Betrieb einer Windows-Domäne benötigten Dienste einschließlich der Authentifizierung von Benutzern gegen eine zentral gepflegte Benutzerdatenbank zur Verfügung. Das Samba-Projekt stellt installierbare Pakete für verschiedene Linux-Distributionen zur Verfügung. In der aktuell stabilen Reihe 3.x stellt Samba Domänendienste in einer zu Windows NT 4.0 kompatiblen Weise zur Verfügung. Diese Protokollversion wird von allen gängigen Windows-Versionen unterstützt¹⁰. Ein vollständiger zu Active Directory kompatibler Domain Controller befindet sich mit Samba4 in der Entwicklung.

4.2 Verzeichnisdienst mit OpenLDAP

Innerhalb einer zentral verwalteten IT-Infrastruktur wird eine Instanz benötigt, die alle Informationen über die in der Infrastruktur bekannten Benutzer, Gruppen, Berechtigungen, Systeme usw. vorhält und die als zentrale und vertrauenswürdige Instanz für die Überprüfung von Anmeldedaten und Berechtigungen von Benutzern verwendet wird. Ein so genannter Verzeichnisdienst setzt diesen weit verbreiteten Standard um, so wie Microsoft es mit Active Directory realisiert. Der Verzeichnisdienst dient dann nicht nur zur Authentifizierung und zur Prüfung von Berechtigungen, sondern er stellt für Programme aller Art auch eine Möglichkeit zur Verfügung, herauszufinden, welche Benutzer, Gruppen und sonstige Objekte es in der Infrastruktur gibt und welche Eigenschaften diese haben. Verzeichnisdienste müssen in der Regel redundant realisiert werden können. Das bedeutet, sie müssen auf mehreren Servern gleichzeitig ausgeführt werden, so dass ihre wichtige Funktion auch dann noch zur Verfügung steht, wenn ein System ausgefallen sein sollte. Außerdem ist die Redundanz Voraussetzung zur Lastverteilung oder für die Vorhaltung von Kopien des Verzeichnisses

⁹ <http://www.samba.org/>

¹⁰ Die Beschreibung einer Domänenmigration findet sich im Linux Technical Review (vgl. [Steuwer2009]). Für eine detaillierte Beschreibung von Samba, sei auf das Buch "Samba 3 für Unix/Linux-Administratoren" (vgl. [Samba2009]) und die Projektwebseite verwiesen.

an einzelnen Standorten, damit keine unnötige Abhängigkeit von der Netzanbindung zum Verzeichnisdienst entsteht.

Im Open Source Umfeld hat sich dazu der Verzeichnisdienst OpenLDAP¹¹ etabliert, der heute in zahlreichen Installationen mit vielen tausend Benutzern im Einsatz ist. In Kombination mit Samba stellt OpenLDAP einen zentralen Logonserver für Benutzer von Microsoft Windows dar. Linux-Systeme können OpenLDAP ebenfalls als Authentifizierungsdienst für die Anmeldung am System nutzen. Linux-Distributionen bringen OpenLDAP als installierbares Paket mit.

4.3 Single Sign-On

Single-Sign-On bezeichnet Techniken, die sicherstellen, dass Benutzer ihr Passwort oder andere Anmeldeinformationen nur einmal eingeben und dann für einen definierten Zeitraum ohne erneute Angabe von vertraulichen Informationen auf die ihnen erlaubten Dienste und Anwendungen zugreifen können. In mehrfacher Hinsicht wird mit Single Sign-On ein Sicherheitsgewinn erreicht. Das Passwort wird nur einmal übertragen und der Benutzer muss sich nur ein Passwort merken, so dass eine Vielzahl unsicherer Passwörter vermieden wird. Beim Entfernen oder Aktualisieren eines Benutzers muss nur ein Benutzerkonto bearbeitet werden.

Zur Realisierung von Single Sign-On stellt Microsoft einen Kerberos-Dienst als Bestandteil von Microsoft Active Directory zur Verfügung. Gleichzeitig wird das ältere NTLM / NTLMv2 Protokoll unterstützt. Single Sign-On kann damit für alle Anwendungen ermöglicht werden, die zur Authentisierung NTLM oder das Kerberos-Protokoll benutzen können. Als Basis für ein solches Single Sign-On können aber auch offene und herstellerunabhängige Dienste mit Open Source Software aufgesetzt werden. Dazu kann ein Open Source Kerberos Server an den Verzeichnisdienst OpenLDAP angebunden werden. Der NTLM-Dienst kann parallel dazu mit Samba realisiert werden.

4.4 Public Key Infrastructure

Public Key Infrastructure (PKI) ist ein kryptografisches System zum Ausstellen, Verteilen und Prüfen digitaler Zertifikate, die zur Absicherung der Kommunikation verwendet werden. Unterschieden wird hierbei zwischen Server-PKI und Benutzer-PKI. Server-PKI dient der abgesicherten Kommunikation zwischen Servern, beispielsweise Web oder E-Mail Server. Benutzer-PKI wird für die abgesicherte Kommunikation zwischen Benutzern verwendet. Ein bekannter Standard dafür ist S/MIME zum Verschlüsseln und Signieren von E-Mails. Microsoft Windows 2000 Server unterstützt keine Benutzer-PKI¹². Eine PKI besteht aus unterschiedlichen Bestandteilen, die ein Vertrauensnetz ergeben und kann mit den Open Source Software Paketen OpenSSL¹³, OpenLDAP und Apache¹⁴ aufgebaut werden.

11 <http://www.openldap.org/>

12 "An Introduction to the Windows 2000 Public-Key Infrastructure." <http://technet.microsoft.com/en-us/library/cc768063.aspx> (Accessed March 31, 2010).

13 <http://www.openssl.org/>

14 <http://www.apache.org/>

4.5 Druckdienst mit CUPS

Damit ein Linux-basierter Domain Controller mit Samba auch den Druckdienst für Mitglieder der Domäne übernehmen kann, ist die Installation und Konfiguration von CUPS (Common Unix Printing System)¹⁵ erforderlich. Wie Samba und OpenLDAP steht CUPS als installierbares Paket bereit.

4.6 Migrationsschritte für typische Einsatzszenarien

Wie im vorhergehenden Abschnitt gezeigt, gibt es viele Open Source Software Pakete, die in Kombination miteinander die wichtigen Funktionen zur Ablösung von Windows 2000 abbilden. Diese Pakete müssen nacheinander eingerichtet und für den gemeinsamen, reibungslosen Betrieb konfiguriert werden.

Das Grundprinzip besteht dabei immer im Aufsetzen des LDAP-Verzeichnisdienstes mit OpenLDAP, der darauf folgenden Kopplung der gewünschten Dienste an das LDAP-Verzeichnis und in der Migration der Nutzdaten.

Im Einzelnen müssen dazu zuerst die benötigten LDAP-Schemata zusammengetragen werden. Diese Schemata beschreiben Attribute und Typen von LDAP-Objekten und bilden die Grundlage der abgebildeten Informationen in einem Verzeichnisdienst. Als Nächstes werden OpenLDAP Server in den Rollen Master und Slave aufgesetzt. Für die Administration von OpenLDAP empfiehlt sich die Verwendung eines LDAP-Administrationswerkzeugs, das ebenfalls installiert, konfiguriert und an den Verzeichnisdienst angebunden werden muss. Dann werden weitere benötigte Dienste wie DNS, DHCP, Domain Controller, Datei- und Druckdienste installiert und konfiguriert. Die Kopplung dieser Dienste an das LDAP-Verzeichnis ist unbedingt zu empfehlen und geht der Migration der Dienste voraus. Nachdem alle benötigten Dienste installiert, konfiguriert, mit dem LDAP-Verzeichnis gekoppelt und ausgiebig getestet sind, können die Datenbestände von Microsoft Active Directory importiert werden. Des Weiteren folgen die Nutzdaten wie zum Beispiel von Datei- oder E-Mailservern.

4.7 Integration, Pflege und Support

Doch wie sieht es mit der Verfügbarkeit wirtschaftlicher und verlässlicher Unterstützung aus? Die Open Source Community ist ein Zusammenschluss von Freiwilligen, die keine festen Reaktionszeiten garantieren oder gar einen Anspruch auf Unterstützung gewähren kann. Umso wichtiger ist es, die implementierte Infrastruktur ausführlich zu dokumentieren und gleichzeitig das Know-how zur Pflege, zur Weiterentwicklung und zur Fehlerbehebung vorzuhalten. Dies kann innerhalb des Unternehmens oder über einen externen Dienstleister geschehen. Dadurch entstehen Kosten, die Bestandteil der Betrachtung der Migrationsalternativen sein müssen.

Im Open Source Umfeld haben sich Unternehmen etabliert, die mehr oder weniger vorgefertigte Softwarelösungen aus Open Source Software als Produkt anbieten. Die bekanntesten dieser Unternehmen sind die so genannten Linux-Distributoren. Eine Linux-Distribution ist eine Sammlung von Software, die ein Linux-Betriebssystem mit Applikationen umfasst. Die Aufgabe der Linux-Distributoren besteht darin, die

¹⁵ <http://www.cups.org/>

enthaltenen Softwarepakete miteinander zu integrieren, das Wissen darüber vorzuhalten, das Gesamtsystem zu pflegen und den Anwendern die Linux-Distribution und Dienste wie Support, Schulungen oder Projektunterstützung zur Verfügung zu stellen.

Transparenz und Herstellerunabhängigkeit von Open Source Software bleiben erhalten, wenn Linux-Distributoren, eigene Software als Teil ihrer Linux-Distribution erstellen und diese Eigenentwicklungen dann ebenfalls als Open Source Software zur Verfügung stellen und dokumentieren.

5 Univention Corporate Server als fertige Open Source Plattform für die Unternehmens IT

Wie können die Vorteile von Open Source Software im Hinblick auf Lizenzkosten, Unabhängigkeit und Flexibilität für Unternehmen und Behörden nutzbar gemacht werden, ohne dass diese das Know-how zum Aufbau und zur Pflege von Open Source Lösungen, die mit Microsoft Windows Serversystemen vergleichbar sind, selbst vorhalten oder individuell einkaufen müssen? Die Klärung dieser Frage ist neben der Verfügbarkeit von einfachen, integrierten Administrationswerkzeugen die Voraussetzung dafür, dass Open Source Software in professionellen Organisationen tatsächlich als zukunftsweisende und wirtschaftliche Alternative eingesetzt werden kann.

Die Lösung sind aber nicht nur geeignete Managementwerkzeuge, sondern vor allem die vorgefertigte Integration der beteiligten Open Source Produkte nach einem etablierten Konzept, das sowohl Administratoren als auch Anwendern bereits vertraut ist, damit es einfach und ohne große Lernaufwände angewandt werden kann. Schließlich sind die Verfügbarkeit von Know-how und Support für dieses Konzept nicht zu unterschätzen.

Das Domänenkonzept aus der Microsoft Windows-Welt ist eingeführt und hat sich bewährt, so dass seine Übertragung in die Linux-Welt ein guter Ansatzpunkt ist. Die Vorteile liegen auf der Hand: Die zentrale Administration von Benutzern, Gruppen, Richtlinien, Rechnern, Datei- und Druckdiensten in einem Vertrauenskontext in Kombination mit der Abdeckung der relevanten Funktionen von Microsoft Windows Serversystemen durch Open Source Software ermöglichen die Unterstützung Offener Standards und steigern Transparenz und Herstellerunabhängigkeit und damit die Wirtschaftlichkeit der Unternehmens-IT. Darüber hinaus können andere Dienste und Anwendungen in den Vertrauenskontext der Domäne integriert werden, auf die zentral gehaltenen Daten zugreifen und diese selbst nutzen.

5.1 Überblick Univention Corporate Server

Benötigt wird also eine Open Source Softwarelösung, die die oben aufgeführten Funktionen abdeckt, auf einer standardisierten Konzeption basiert, ein einheitliches und integriertes Managementsystem beinhaltet, wirtschaftlich betreibbar ist und für die Maintenance (Pflege) und Support zu ebenso wirtschaftlichen Konditionen verfügbar sind.

Univention hat sich der Schaffung einer solchen Softwarelösung angenommen und mit Univention Corporate Server (UCS) ein Open Source Produkt geschaffen, das Infrastruktur- und Identity-Management nach dem Domänenkonzept vereint und als Enterprise-Linux-Distribution eine ideale Plattform für den zuverlässigen Betrieb der Unternehmens-IT bietet. Es verwendet unter anderem die oben beschriebenen Open Source Produkte Samba, OpenLDAP, Kerberos und CUPS und bietet dem Anwender eine skalierbare Enterprise Identity- und Infrastruktur-Managementlösung. Die enthaltenen Open Source Produkte sind aufeinander abgestimmt und miteinander integriert. Es ist vergleichbar mit einem Microsoft Windows Domain Controller mit Active Directory.

Grundlage für die in UCS enthaltene Enterprise-Linux-Distribution, das UCS-Basissystem, ist die freie Linux-Distribution Debian GNU/Linux, die vom Debian Projekt erstellt und gepflegt wird. Dieses Projekt legt einen hohen Wert darauf, dass die enthaltene Software den Kriterien von Open Source Software entspricht. Hinter dem Projekt steht eine weltweite Community von über 1000 Personen, die seit der Projektgründung 1993 einen sehr guten Ruf für die Pflege einer stabilen Linux-Distribution genießt. Debian GNU/Linux ist im Serverbereich die am weitesten verbreitete freie Linux-Distribution überhaupt.

Ein einheitliches Managementwerkzeug wird dem Administrator durch das UCS Managementsystem zur Verfügung gestellt. Neben dem UCS-Basissystem und dem UCS-Managementsystem stehen darüber hinaus viele so genannte UCS-Komponenten zur Verfügung, die UCS um Funktionen wie Remote Desktop Services, Groupware, Anmelddienste, Dienste für Windows, Virtualisierung und vieles mehr ergänzen und die Verwaltung dieser Funktionen mit dem Managementsystem integrieren.

Alle Eigenentwicklungen von Univention stehen unter der Open Source Software Lizenz GPL und werden auf den Webseiten des Herstellers zum Download bereit gestellt. Anwender erhalten Maintenance und Support für UCS. Die Maintenance beinhaltet die Bereitstellung von Softwareupdates, so dass das System einfach und mit planbaren Kosten aktuell und gepflegt gehalten werden kann. Ein dreistufiges Supportmodell garantiert definierte Reaktionszeiten und die Möglichkeit zum Zugriff auf einen dem Einsatzzweck angemessenen Leistungsumfang.

Tabelle 3 zeigt eine vergleichbare Übersicht wie Tabelle 1 und konzentriert sich auf die Gegenüberstellung der Funktionen von Microsoft Windows 2008 Server mit Univention Corporate Server. Des Weiteren bietet UCS Funktionen, die im vorhergehenden Abschnitt über Open Source Software im Allgemeinen in Tabelle 2 fehlen: Desktop-Virtualisierung, Gruppenrichtlinien und Standortverwaltung.

Funktion	Microsoft Windows Server 2008	Open Source Software Univention Corporate Server
Identity Management	Ja - Active Directory (AD)	Ja - UCS-Managementsystem auf Basis von OpenLDAP
Infrastruktur Management	Ja	Ja - UCS-Managementsystem auf Basis von OpenLDAP
Domain Controller für Windows Clients	Ja	Ja - Samba
Public-Key-Infrastructure	Ja	Ja - OpenSSL / UCS-Management

Funktion	Microsoft Windows Server 2008	Open Source Software Univention Corporate Server
Single-Point-of-Administration	Ja	Ja - UDM/UMC
Softwareverteilung	Ja - Windows Deployment Services	Ja - APT, OPSI (über Managementsystem)
Patch Management	Ja - Windows Server Update Services	Ja - APT, OPSI (über Managementsystem)
Remote Desktop Services	Ja - Remote Desktop Service	Ja - NX, x2go, X11, RDP
Remote Installation	Ja - Windows Deployment Services	Ja - UCS-Managementsystem
Unattended Installation	Ja	Ja - UCS-Installer
Druckdienste	Ja	Ja - CUPS
Dateidienste	Ja	Ja - Samba, NFS
Replikation Verzeichnisdienste	Ja	Ja - OpenLDAP, UCS-Managementsystem
Virtualisierung	Ja - Hyper-V	Ja - XEN, KVM
Desktop-Virtualisierung	Ja - Virtual Desktop Infrastructure	Ja - XEN, KVM
Failover Clustering	Ja - Failover Clustering	Ja - Heartbeat
Datenbanken	Ja - MS SQL Server	Ja - PostgreSQL, MySQL
Backup	Ja - Windows Server Sicherung	Ja - Bacula, SEPsesam
Maildienste	Ja - Exchange Server	Ja
Firewall	Ja - Windows Firewall	Ja
Webproxy	Ja - Drittprodukt	Ja - Squid
Gruppenrichtlinien	Ja	Ja - für UCS, UCS-Managementsystem
Single Sign-On	Ja - NTLM, Kerberos	Ja - Kerberos, NTLM über Samba
Standortverwaltung	Ja - Active Directory (AD)	Ja
Remote Administration	Ja - AdminPack	Ja - Web, SSH, NX
Laufwerkverschlüsselung	Ja	Ja

Tabelle 3: Vergleich der Funktionen von Microsoft Windows Server 2008, Open Source Software und Univention Corporate Server

5.2 Domänenkonzept

UCS ermöglicht anhand des Domänenkonzepts Mehrserverumgebungen mit Domain Controllern in verschiedenen Setups (siehe Abbildung 1). Darüber hinaus können auch Microsoft Windows-Server Mitglieder der UCS-Domäne und UCS kann Mitglied einer Active Directory Domäne werden. Mit UCS werden alle Objekte einer UCS-Domäne organisationsweit zentral verwaltet. Das LDAP-Verzeichnis mit OpenLDAP nimmt mit seiner baumartigen Struktur eine tragende Rolle ein und hält alle verwaltungsrelevanten Daten vor. Die zentrale Datenhaltung im LDAP-Verzeichnis verringert die Wahrscheinlichkeit von

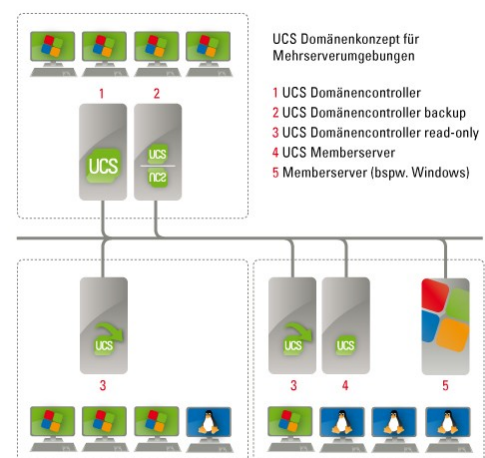


Abbildung 1: UCS Domänenkonzept

Inkonsistenzen und Fehlern bei der wiederholten Eingabe derselben Daten in verschiedenen Konfigurationsdateien. Die UCS-Domäne baut einen Sicherheits- und Vertrauenskontext für ihre Mitglieder auf.

5.3 Datei- und Druckdienste

UCS bietet die ideale Grundlage zur Ablösung der bestehenden Datei- und Druckdienste mit Linux und Samba, ohne großflächig Änderungen an den bestehenden Windows-Clients notwendig zu machen. Benutzer erhalten vorkonfigurierte Dateifreigaben auf zentralen UCS-Servern, die als Netzwerklaufwerke in Microsoft Windows-Clients eingebunden werden können. Benutzer bekommen so persönliche Laufwerke und auch Zugriff auf Gruppenlaufwerke. Über Samba und CUPS werden Drucker als Netzwerkdrucker für Microsoft Windows-Clients zur Verfügung gestellt und können standortabhängig angesprochen werden. UCS deckt damit die wichtigsten Funktionen von Microsoft Windows Server 2008 ab und bietet darüber hinaus noch ein Managementwerkzeug.

5.4 UCS Managementsystem

Das UCS Managementsystem ist die zentrale Anlaufstelle in UCS für Administratoren. Es ist mit seinen Managementwerkzeugen der Single-Point-of-Administration einer UCS-Domäne und bietet dem Administrator eine Web- und eine Kommandozeilenschnittstelle (siehe Abbildung 2). Das UCS Managementsystem ist modular aufgebaut, flexibel erweiterbar und somit einfach integrierbar und für zukünftige Erweiterungen gerüstet. Die

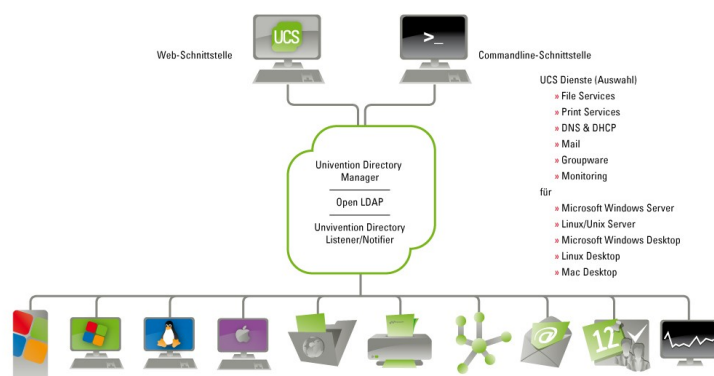


Abbildung 2: Übersicht UCS Managementsystem

Fernadministration ist mit der Webschnittstelle implizit in das UCS Managementsystem integriert.

5.5 Univention Directory Manager

Verwaltung und Administration des LDAP-Verzeichnisses erfolgen über Univention Directory Manager, einen Teil des UCS Managementsystems. Der Directory Manager erlaubt das Betrachten, Bearbeiten, Löschen und Suchen von Daten im LDAP-Verzeichnis. Die Webschnittstelle bietet Assistenten für verschiedene Verwaltungsaufgaben an. Abbildung 3 zeigt die Desktop Einstellungen für einen Benutzer. Richtlinien sind ein weiteres wichtiges Merkmal für eine UCS-Domäne. Sie enthalten Einstellungen, die an untergeordnete Objekte weitergegeben werden. Über Richtlinien sind Vererbungshierarchien von Eigenschaften für nachgeordnete Objekte möglich. Das UCS Handbuch [UCS2009] nennt als Beispiel die Grafikeinstellungen

von Computern mit dem gleichen Bildschirm. Über eine Richtlinie lassen sich die Einstellungen dafür zusammenfassen und für alle betroffenen Computer aktivieren.

5.6 UCS Active Directory Connector

UCS Active Directory Connector (AD Connector) ermöglicht die bidirektionale Synchronisation von Benutzerkonten inklusive verschlüsselter Passwörter, Gruppendefinitionen und anderen Verzeichnisdienstobjekten zwischen Microsoft Windows Server mit Microsoft Active Directory und dem OpenLDAP Verzeichnisdienst in UCS. Dadurch ist der Parallelbetrieb von Microsoft Windows- und Linux-Umgebungen reibungslos und ohne hohen Administrationsaufwand möglich, so dass Linux- und Microsoft Windows-basierte Umgebungen miteinander verbunden werden können. Der AD Connector vermeidet eine doppelte, anspruchsvolle, komplexe und

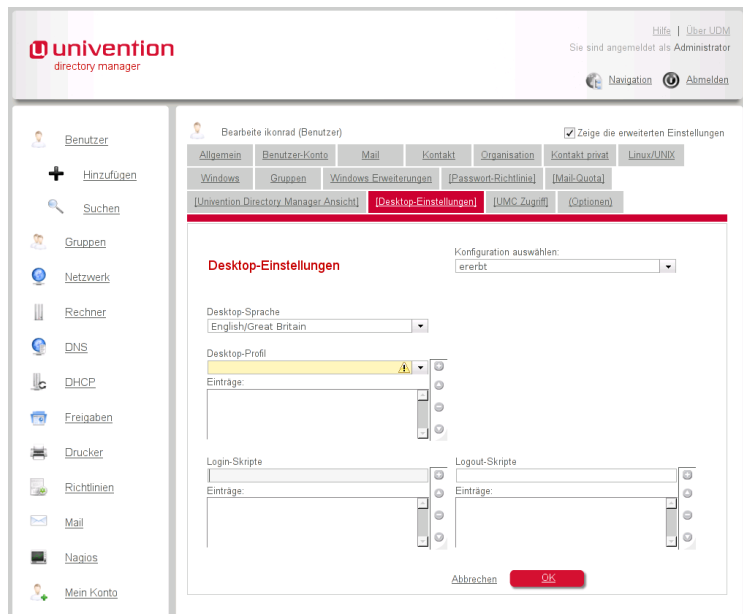


Abbildung 3: Desktop-Einstellungen eines Benutzers im Univention Directory Manager

fehleranfällige Administration bei einfachen Aufgaben wie das Anlegen eines Benutzers. Unterschiedliche Benutzernamen und mehrere Benutzerpasswörter werden ausgeschlossen. Sicherheitsrichtlinien können einfach durchgesetzt werden.

5.7 Virtualisierung

UCS ist die ideale Plattform für Server- und Desktop-Virtualisierung. Über das UCS Managementsystem werden die virtuellen Maschinen für Server oder Desktops und die jeweiligen Images zentral auf Virtualisierungsservern oder in Virtualisierungsclustern verwaltet. Vorhandene Microsoft Windows-Desktops lassen sich in eine virtuelle Umgebung umlagern, so dass eine Unabhängigkeit der Systeme von der vorhandenen Hardware erreicht wird. Univention Corporate Server verwendet etablierte Open Source Software wie XEN und KVM.

5.8 Thin Client und Remote Desktop Services

UCS integriert Remote Desktop Services in das UCS Managementsystem und ermöglicht darüber hinaus den Betrieb und das Management von Thin Clients. Für Letzteres bringt UCS eine eigene Komponente, die so genannten UCS Thin Client Services, mit. Mit ihnen lassen sich Thin Client Systeme in einer Thin Client Infrastruktur zentral ausrollen, betreiben und verwalten. Sie funktionieren mit einer breiten Palette

möglicherweise bereits vorhandener Thin Client- und PC-Systeme und eignen sich für den Betrieb mit Microsoft Windows Terminal Server, Citrix Presentation Server, Linux und Unix Server und VMware Desktop-Virtualisierung.

Die Integration der UCS Thin Client Services in das UCS Managementsystem sorgt für die Softwareverteilung und -Aktualisierung und integriert sich mit der Monitoringfunktionalität auf Basis von Nagios. Durch die Unterstützung beliebiger Thin Client Hardware und die Unabhängigkeit von den serverseitig eingesetzten Technologien zur Bereitstellung der Anwendungen ermöglicht UCS Thin Client Services eine doppelte Herstellerunabhängigkeit.

5.9 Groupware

Neben den klassischen Diensten einer Windows Domäne (Anmelde-, Datei- und Druckdienste) betreiben viele Organisationen darin auch Mail- und Groupwaredienste mit dem Produkt Microsoft Exchange. Microsoft Exchange integriert sich sehr weitgehend in die Benutzer- und Rechteverwaltung von Microsoft Active Directory und kann deswegen ohne Active Directory auch nicht betrieben werden. Exchange ist die Basis für Groupwarelösungen mit E-Mail, Kontaktmanagement, Kalenderfunktionen und Notizen einschließlich gemeinsamer Ordner und wird in der Regel mit Microsoft Outlook als Client-Software verwendet.

Analog dazu ist Univention Corporate Server (UCS) die Plattform für unterschiedliche Groupware-Lösungen. Für UCS zertifizierte Pakete werden beispielsweise von den Herstellern der Groupwaresysteme Kolab2, Open-Xchange, Scalix und Zarafa angeboten. Die Benutzerverwaltung der jeweiligen Groupware-Lösung ist dabei analog der Integration von Microsoft Exchange mit Active Directory in das UCS Managementsystem integriert. Der Leistungsumfang der genannten Systeme ist gut vergleichbar mit dem von Microsoft Exchange und geht teilweise deutlich darüber hinaus. Die Produkte unterstützen die Verwendung unterschiedlicher E-Mail- und Groupware-Clients, so zum Beispiel auch Microsoft Outlook.

5.10 Softwarepflege

Univention Corporate Server beinhaltet ein integriertes System zur Softwareverteilung und -pflege für die zentrale Verwaltung von Software, Release-Ständen und Paketversionen auf den UCS-Systemen in einer UCS-Domäne. Updates in Form von Release- oder Security-Updates und Hotfixes werden über Repository-Server bezogen. Univention bietet hierfür ein Online-Repository an, aus dem die Software direkt installiert werden kann. Sollte der Zugriff auf externe Repository-Server nicht möglich oder nicht gewünscht sein, können alternativ lokale Repository-Server verwendet werden. Eine Softwareverteilung für Microsoft Windows-Installationen ist über das Produkt *opsi4ucs* möglich, dessen Management mit dem UCS Managementsystem integriert ist.

5.11 Implementierung und Migrationsschritte mit UCS

Abschnitt 4.6 stellt die Migrationsschritte für eine ablösende Migration mit Open Source Software vor. Der prinzipielle Migrationsablauf gestaltet sich mit Univention Corporate Server ähnlich, er ist aber sehr viel

einfacher durchzuführen, weil die relevanten Dienste bereits miteinander integriert und die Konfigurationsdateien automatisch erzeugt werden. Technisch wird auch bei UCS zunächst der Verzeichnisdienst aufgesetzt und damit das zentrale Element der UCS-Domäne implementiert. Dann werden die verschiedenen Dienste an den Verzeichnisdienst gebunden, so dass sie innerhalb der Domäne verwaltbar werden. Dies geschieht während der Installation jedoch weitgehend automatisch und für den Anwender transparent. Nachdem das erste System einer UCS-Domäne aufgesetzt ist, können weitere Systeme durch einen einzigen Befehl in die Domäne aufgenommen werden, dadurch werden alle relevanten Dienste automatisch an den Verzeichnisdienst der Domäne gebunden. Diese Technik reduziert Fehler und die mit der Implementierung von Open Source Infrastrukturen verbundenen Aufwände erheblich, hilft Fehler zu vermeiden und stellt ein standardisiertes Verfahren dar, das einfach wiederholt werden kann. Nach Abschluss der Installation müssen die Nutzer- und Anwenderdaten migriert werden. Hierzu stellt UCS eine Reihe von Hilfen bereit, darunter ein Skript zur vollautomatischen Migration von Windows NT 4 Domänen und einen Konnektor zu Microsoft Active Directory mit dem sich und andere Benutzer- und Gruppensdefinitionen sowie die Passwörter vollautomatisch übernehmen lassen.

6 Fazit

Microsofts auslaufender Support zwingt Organisationen zum Handeln. Das gilt heute für Windows 2000 und wird in Kürze für Windows 2003 Server gelten. Die fortführende Migration über Microsoft Windows Server 2003 zu Microsoft Windows Server 2008 ist der empfohlene Weg von Microsoft. Die im Rahmen der Migration anzustrebende Weiterentwicklung der Umgebung ist bei diesem Migrationsweg nur in dem Rahmen möglich, wie sie durch die neuen Serverprodukte von Microsoft unterstützt wird.

Open Source Software deckt die von den meisten Organisationen benötigten Funktionen der Microsoft Betriebssysteme Windows 2000 Server und Windows Server 2008 ab. Eine ablösende Migration mit Open Source Software bietet darüber hinaus Herstellerunabhängigkeit, Offenheit, Transparenz und Flexibilität. Im Open Source Umfeld sind außerdem viele Programme, Techniken und Dienste verfügbar, mit denen IT-Infrastrukturen sehr kostengünstig und effektiv modernisiert und an aktuelle Anforderungen angepasst werden können. Dazu gehören Techniken zur Server- und Desktop-Virtualisierung, für Management und Betrieb von Thin Clients bis hin zu Groupware und Content-Management-Systemen. Auch die Ablösung von Office-Software und Desktop mit Open Source Software ist heute ein aktuelles Szenario, mit dem sich nicht zuletzt die Kosten erheblich optimieren lassen.

Univention Corporate Server als Open Source Enterprise Linux-Distribution vereinfacht Migration und Betrieb von Open Source IT Infrastrukturen durch die Integration der Komponenten, die zentrale Pflege und durch Werkzeuge wie Univention Directory Manager oder UCS AD Connector erheblich. UCS verfügt als Open Source Plattform über ein umfangreiches Managementsystem für den integrierten Betrieb von Datei-, Druck-, Infrastruktur- und Managementdiensten. Anwender erzielen somit einen Gewinn in Bezug auf Wirtschaftlichkeit, Effizienz, Herstellerunabhängigkeit und Skalierbarkeit.

7 Erläuterungen der Funktionen

Public Key Infrastructure (PKI)

PKI ist ein kryptografisches System zum Ausstellen, Verteilen und Prüfen digitaler Zertifikate, die zur Absicherung der Kommunikation verwendet werden. Die PKI ist Teil des Domänenkonzepts und trägt maßgeblich zum Aufbau des Sicherheits- und Vertrauenskontextes bei.

Single Sign-On (SSO)

Single Sign-On ist ein Verfahren zur einmaligen Authentisierung eines Benutzers in einem Netzwerk, so dass von einem Arbeitsplatz aus verschiedene Dienste ohne erneutes Anmelden benutzt werden können.

Replikation

Eine Replikation eines Verzeichnisdienstes ist eine Kopie des Verzeichnisdienstinhalts auf weitere Domain Controller. Die Replikation ist für die Aktualität der Daten verantwortlich.

Identity Management

Mit Identity Management werden Benutzer- und Gruppenidentitäten in der Domäne verwaltet und Attribute wie Benutzername, Passwort, E-Mailadresse und viele mehr erfasst.

Infrastruktur Management

Infrastruktur Management ist unter anderem verantwortlich für Verwaltung und Zuweisung von Netzwerkadressen in einem Computernetzwerk und für deren Namensauflösung.

Single-Point-of-Administration

Ein Single-Point-of-Administration ist eine zentrale Stelle, wo administrationsrelevante Einstellungen gespeichert und Aktionen vorgenommen werden. Er ist Interaktionspunkt für den Administrator und erfordert einen Mindestgrad an Benutzerfreundlichkeit.

Softwareverteilung

Softwareverteilung ist ein Administrationswerkzeug zum Ausrollen von nicht-installierter Software und Konfigurationen auf Computer einer Computerinfrastruktur.

Patch Management

Patch Management ist neben der Softwareverteilung ein essentielles Administrationswerkzeug zum Verteilen von Softwareupdates für bereits installierte Software.

Installation

Remote und unattended Installation sind zwei Arten, um ein Betriebssystem auf einem Computer zu installieren. Remote Installation ermöglicht die Installation auf einem entfernten Computer über das Netzwerk. Unattended Installation ermöglicht eine unbeaufsichtigte Betriebssysteminstallation über das Netzwerk, ohne dass sich Computer und Administrator an einem Ort befinden müssen.

Remote Desktop Services

Remote Desktop Services ist die gleichzeitige Bereitstellung einer zentralen Desktop-Umgebung für mehrere Benutzer für Thin Clients oder andere Geräte. In Thin Client Umgebungen wird die Desktop-Umgebung durch einen Terminalserver zur Verfügung gestellt.

Failover Clustering

Ein failover Cluster ist ein Zusammenschluss mehrerer Computersysteme in einem Computerverbund.

Failover Clustering steuert und verwaltet einen solchen Cluster.

8 Literaturverzeichnis

[BMI2008]

Bundesministerium des Innern, editor. Migrationsleitfaden [Internet]. 2008 Apr; Available from: http://www.cio.bund.de/cae/servlet/contentblob/294268/publicationFile/4678/migrationsleitfaden_download.pdf

[CIO2008]

Von Green IT bis Business Technologie: IT-Trends 2008 - CIO.de [Internet]. [cited 2010 Mar 2]; Available from: <http://www.cio.de/strategien/methoden/846817/>

[CIO2009]

Virtualisierung und Cloud Computing top, Green IT Flop: Die IT-Trends 2009 - CIO.de [Internet]. [cited 2010 Mar 2]; Available from: <http://www.cio.de/strategien/methoden/859923/>

[CIO2010]

Das Gartner-Orakel: Die 10 strategischen IT-Trends 2010 - CIO.de [Internet]. 2010 Jan 8 [cited 2010 Mar 2]; Available from: <http://www.cio.de/strategien/methoden/2212689/>

[CP2009]

Die fünf größten IT-Trends 2009 laut Bitkom - Home - Alle News - ChannelPartner [Internet]. 2009 Feb 2 [cited 2010 Mar 2]; Available from: <http://www.channelpartner.de/news/272274/index1.html>

[Gartner2009]

Gartner Identifies the Top 10 Strategic Technologies for 2010 [Internet]. 2009 Oct 20 [cited 2010 Mar 2]; Available from: <http://www.gartner.com/it/page.jsp?id=1210613>

[heise2009]

Dr. Oliver Diedrich. heise open - Trendstudie Open Source [Internet]. 2009 [cited 2010 Apr 12]. Available from: <http://www.heise.de/open/artikel/Trendstudie-Open-Source-221696.html>

[HUP]

Univention: Anwenderbericht HUP AG [Internet]. [cited 2010 Apr 8]; Available from: <http://www.univention.de/2392.html>

[MS_Cluster_Hardware]

Schrittweise Anleitung für Failovercluster: Prüfen der Hardware auf einen Failovercluster [Internet]. [cited 2010 Feb 24]; Available from: [http://technet.microsoft.com/de-de/library/cc732035\(W5.10\).aspx](http://technet.microsoft.com/de-de/library/cc732035(W5.10).aspx)

[MS_Cluster_Migration_Path]

Aktualisieren eines Clusters von Windows 2000 [Internet]. [cited 2010 Feb 24]; Available from: [http://technet.microsoft.com/de-de/library/cc739100\(W5.10\).aspx](http://technet.microsoft.com/de-de/library/cc739100(W5.10).aspx)

[MS_Migration_Cluster]

Grundlegendes zur Migration zu einem Cluster unter Windows Server 2008 R2 [Internet]. [cited 2010 Feb 24]; Available from: <http://technet.microsoft.com/de-de/library/cc731812.aspx>

[MS_Product_Lifecycle]

Übersicht Microsoft Support Lifecycle [Internet]. [cited 2010 Feb

25];Available from: <http://support.microsoft.com/gp/lifecycle/de>

[MS_Support]

Ablauf des Supports für Windows 2000 - Lösungszentrum [Internet]. [cited 2010 Feb 19];Available from: <http://support.microsoft.com/ph/1131>

[OLB]

Univention: Anwenderbericht OLB [Internet]. [cited 2010 Apr 8];Available from: http://www.univention.de/anwd_olb.html

[OS_Definition]

The Open Source Definition | Open Source Initiative [Internet]. [cited 2010 Mar 9];Available from: <http://www.opensource.org/docs/osd>

[OS_Definition_DE]

Open Source Initiative OSI - German:The Open Source Definition [Internet]. [cited 2010 Mar 9];Available from: <http://www.free-soft.org/mirrors/www.opensource.org/docs/osd-german.php>

[Samba2009]

Lendecke V, Seeger K, Adam M. Samba 3 für Unix/Linux-Administratoren. 3. ed. Heidelberg: dpunkt.verlag; 2009.

[Steuer2009]

Steuer I. Domänenmigration. In: Alles über: Migration. München: Linux New Media AG; 2009.

[UCS2009]

Univention GmbH, editor. Univention Corporate Server [Internet]. 2009 Dec;Available from: http://www.univention.de/fileadmin/download/dokumentation_2.3/handbuch_ucs23.pdf

[Werner2007]

Torsten Werner. World Domination: Die Erfolgsgeschichte der Linux- und Open-Source-Einführung im Auswärtigen Amt. In: Bernd Lutterbeck, Matthias Bärwolff, Robert A. Gehring, editors. Open Source Jahrbuch 2007. Berlin: Lehmanns Media; 2007.

[Win2K_Update_Path]

Aktualisierungspfade für Windows Server 2008 R2 [Internet]. [cited 2010 Apr 15];Available from: [http://technet.microsoft.com/de-de/library/dd979563\(WS.10\).aspx](http://technet.microsoft.com/de-de/library/dd979563(WS.10).aspx)