

Markus Wischnewski

Zentrale Benutzerverwaltung für heterogene Netzwerkkumgebungen mit LDAP und Samba

Diplomarbeit

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2004 Diplom.de
ISBN: 9783832481568

Markus Wischnewski

Zentrale Benutzerverwaltung für heterogene Netz- werkumgebungen mit LDAP und Samba

Markus Wischnewski

Zentrale Benutzerverwaltung für heterogene Netzwerkumgebungen mit LDAP und Samba

Diplomarbeit
Fachhochschule Fulda
Fachbereich angewandte Informatik
Abgabe Mai 2004



Diplomica GmbH _____
Hermannstal 119k _____
22119 Hamburg _____
Fon: 040 / 655 99 20 _____
Fax: 040 / 655 99 222 _____
agentur@diplom.de _____
www.diplom.de _____

ID 8156

Wischnewski, Markus: Zentrale Benutzerverwaltung für heterogene Netzwerkkumgebungen mit LDAP und Samba

Hamburg: Diplomica GmbH, 2004

Zugl.: Fachhochschule Fulda, Diplomarbeit, 2004

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomica GmbH

<http://www.diplom.de>, Hamburg 2004

Printed in Germany

Inhaltsverzeichnis

| | |
|---|-----------|
| 1. Einleitung | 5 |
| 1.1. Beschreibung der Thematik | 5 |
| 1.2. Zielsetzung der Arbeit | 5 |
| 1.3. Software | 6 |
| 1.4. Beschreibung der Testumgebung | 7 |
| 1.4.1. Testumgebung I - Labor | 7 |
| 1.4.2. Testumgebung II - VMWare | 8 |
| 2. Benutzerverwaltung | 9 |
| 2.1. Benutzerverwaltung unter Windows | 9 |
| 2.1.1. Workstation | 9 |
| 2.1.2. Primary Domain Controller | 10 |
| 2.1.3. Active Directory Server | 10 |
| 2.2. Benutzerverwaltung unter Unix | 11 |
| 2.2.1. shadow-System | 11 |
| 2.2.2. NIS | 12 |
| 2.2.3. NIS+ | 12 |
| 2.3. Benutzerverwaltung unter Novell | 14 |
| 2.3.1. NDS | 14 |
| 2.3.2. eDirectory | 14 |
| 2.4. Wichtige Anforderungen an die zentralisierte Benutzerverwaltung in heterogenen Netz- werkumgebungen | 15 |
| 2.4.1. Punkt 1 - keine redundant gespeicherte Benutzerdaten | 16 |
| 2.4.2. Punkt 2 - keine Inkonsistenzen | 16 |
| 2.4.3. Punkt 3 - ein einziges Heimatverzeichnis | 16 |
| 2.4.4. Punkt 4 - offene und verbreitete Technologien | 16 |
| 2.4.5. Punkt 5 - Verwendbarkeit | 16 |
| 2.4.6. LDAP und SAMBA | 16 |
| 3. SSL | 18 |
| 3.1. Zertifikate | 18 |
| 3.2. RSA - Verschlüsselung | 18 |
| 4. Verzeichnisdienste | 19 |
| 4.1. eDirectory und Active Directory | 19 |
| 4.2. X.500 und LDAP | 19 |
| 4.2.1. Aufbau | 19 |

| | | |
|-----------|--|-----------|
| 4.2.2. | Master-Slave Konzept | 21 |
| 4.2.3. | Replizierung | 21 |
| 4.2.4. | Die Partitionierung | 22 |
| 4.2.5. | Sicherheit | 22 |
| 4.2.6. | Administrator und Passwortkodierung | 23 |
| 5. | SAMBA | 25 |
| 5.1. | SMB-Protokoll | 25 |
| 5.1.1. | NetBIOS | 25 |
| 5.1.2. | WINS-Server | 27 |
| 5.2. | Benutzerverwaltung | 27 |
| 5.2.1. | Mögliche Einsatzszenarien für Benutzerverwaltung | 28 |
| 5.3. | Sicherheitsmodelle | 28 |
| 5.3.1. | share-Modus | 28 |
| 5.3.2. | user-Modus | 28 |
| 5.3.3. | server-Modus | 29 |
| 5.4. | LDAP-Unterstützung | 29 |
| 5.5. | SAMBA und Dateifreigaben | 29 |
| 5.6. | SAMBA und Druckerfreigaben | 29 |
| 5.6.1. | CUPS | 29 |
| 5.7. | ACLs | 30 |
| 5.7.1. | Kernel-Patch | 30 |
| 5.7.2. | Dateisysteme | 30 |
| 5.7.3. | Samba und ACLs | 30 |
| 5.8. | Samba 3.0 | 31 |
| 5.8.1. | Ausblick | 31 |
| 6. | Praxis | 32 |
| 6.1. | Arbeitsplan | 32 |
| 6.2. | SuSE 9.0 | 33 |
| 6.2.1. | Yast | 33 |
| 6.2.2. | apt-get | 33 |
| 6.2.3. | Checkconfig | 34 |
| 6.3. | Einrichtung des LDAP-Servers | 35 |
| 6.3.1. | LDAP-Server installieren | 35 |
| 6.3.2. | SSL-Verschlüsselung, das Erstellen von Zertifikaten | 35 |
| 6.3.3. | Konfiguration des LDAP-Servers | 37 |
| 6.4. | Hilfsprogramme und Tools | 39 |
| 6.4.1. | smbldap-tools | 39 |
| 6.4.2. | Perl-Bibliotheken | 41 |
| 6.5. | smbldap-tools benutzen | 43 |
| 6.6. | mkntpwd | 48 |
| 6.7. | Einrichtung des Samba-Servers | 48 |
| 6.7.1. | Samba kompilieren | 48 |
| 6.8. | Linux/Unix Clients | 50 |
| 6.8.1. | Automatische Einrichtung mit Yast unter SuSE Linux 9.0 | 50 |

| | |
|--|-----------|
| 6.8.2. nsswitch | 53 |
| 6.8.3. pam-Schnittstelle | 55 |
| 6.8.4. NFS-Server-Einrichtung | 55 |
| 6.9. Windows Clients | 56 |
| 6.9.1. Registry | 56 |
| 6.9.2. Automatisches Anmelden von Arbeitsstationen | 56 |
| 7. Diskussion | 60 |
| 7.1. Produktiver Einsatz | 60 |
| 7.1.1. Passwortänderung | 60 |
| 7.1.2. Profiles | 61 |
| 7.2. Zusammenfassung und Ausblick | 61 |
| 7.2.1. Samba als PDC-Killer | 61 |
| 7.3. Fazit | 62 |
| A. Quellen aus dem Internet | 65 |
| B. Softwareverzeichnis | 66 |
| C. Dateilistings | 67 |
| C.1. smbldap.conf | 67 |
| C.2. smbldapbind.conf | 71 |
| C.3. /etc/nsswitch.conf | 71 |
| C.4. /etc/ldap.conf | 72 |
| C.5. smb.conf | 73 |