# Empfehlungen für stabile und sichere Windows-Server im HU-Netz

Michael Sommerfeld
*michael.sommerfeld@cms.hu-berlin.de*

*Installation, Wartung, Windows-Server, Sicherheit, Benutzerverwaltung, Active Directory, Netzwerkressourcen*

*Dieser Beitrag richtet sich an Sie – falls Sie MS Windows-Systeme aufbauen oder betreuen – jedoch hauptsächlich an Administratoren, die Domänen in unserem Windows-Netz verwalten [werden]. Es werden Hinweise zum Aufbau von Windows 2000-Servern für das HU-Netz gegeben. Besonderes Augenmerk wird auf die stabile und sichere Funktion des Netzwerks gelegt. Es wird auf Anwendungen, Prozeduren, Konventionen, Empfehlungen und Dokumentationen verwiesen, die den effektiven Aufbau und die Funktionsfähigkeit des Windows-Netzes unterstützen.*

## Einleitung

Computernetzwerke werden mit dem Ziel aufgebaut und betrieben, den Benutzern möglichst gute Arbeitsbedingungen zu bieten. Dies schließt neben dem schnellen und stabilen Zugriff auf die benötigten Daten, Anwendungen und weiteren Netzwerkressourcen auch deren zuverlässigen Schutz vor unberechtigter Benutzung, Verfälschung, Zerstörung und Diebstahl ein.

Unter diesen Gesichtspunkten müssen administrative Arbeiten im Netzwerk auf Risiken untersucht und geeignete Empfehlungen abgeleitet werden. Man könnte die Aufgaben von Windows-Administratoren grob in folgende Gebiete gliedern:

- Installation sicherer Windows-Server,
- Sicherung der stabilen Funktion der bereitgestellten Netzwerkressourcen,
- Benutzerverwaltung,
- Anpassung der Netzwerkressourcen an neue Erfordernisse,
- Gewährleistung einer Vertretung (Urlaub, Krankheit, …).

## Installation sicherer Windows-Server

Bei der Auswahl der Hardware für Server sollte man bedenken, dass das Windows 2000-Netz der HU eine relativ große Anzahl solcher Server erfordert – je Domäne ist mit zwei Domänen-Controllern und zwei Fileservern zu rechnen. Um den Wartungsaufwand in Grenzen zu halten, sollten die Server aus möglichst einheitlichen Hardwarekomponenten aufgebaut werden. Bestimmte Hardwareunterschiede wird es wegen der unterschiedlichen Funktion der Server trotzdem geben (z. B. eine größere Anzahl von lokalen Platten für Domänen-Controller; Fibre Channel Adapter für die Anbindung an ein Storage Area Network (SAN)).

Außerdem ist es möglich, durch redundante Komponenten wie Netzteile, Platten (an einem RAID-Controller) oder Fibre Channel Adapter die Verfügbarkeit der Server zu erhöhen. Doch sollte das Streben nach Redundanz nicht übertrieben werden, da sich die Wahrscheinlichkeit des Ausfalls jeder einzelnen Komponente dadurch kaum ändert – also auch der Aufwand für die Instandhaltung aller Komponenten eines Servers steigt. Es ist angebracht, die Möglichkeiten, die der Aufbau von Server Clustern bietet, bei solchen Entscheidungen zu berücksichtigen. Zumal Cluster zusätzlich zur Lastverteilung und zur Reduzierung von Ausfallzeiten (z. B. bei Wartungsarbeiten an den Servern) genutzt werden können. Die Server eines Clusters müssen immer auf identischer Hardware aufgebaut werden.

Die Grundinstallation der Server muss offline (ohne Netzwerk Zugang) erfolgen, weil die von CD installierten Systeme noch zu viele Sicherheitslücken aufweisen. Bevor ein Windows-Rechner online gehen kann, sind das nötige Service Pack, alle Sicherheits-Updates und ein Virenscanner wirksam zu machen. Aus vielerlei Gründen (Sicherheit, Pflegeaufwand, Zusammenarbeit, …) sollen nur englischsprachige Serverversionen installiert werden. Für Terminal Server sind eventuell andere Sprachversionen erforderlich, um die auf ihnen geplanten Anwendungen in vollem Umfang zu ermöglichen. Es ist nicht angeraten, die Standardinstallation zu verwenden, da nur die unbedingt erforderlichen Dienste auf dem zukünftigen Server laufen sollten.

Der CMS stellt eine aktuelle Patch-Prozedur [1] für die Serversysteme bereit, die man sich z. B. auf einen Memory-Stick kopieren kann, um offline die aktuell behebbaren Sicherheitslücken zu schließen. Auch die Installation und Konfiguration des Virenscanners (von NAI) [2] muss offline erfolgen, um das Speichern infizierter Dateien von Anfang an zu verhindern. Eine Checkliste zur Serverinstallation [3] findet man im Wiki des CMS – fast alle Literaturangaben dieses Beitrags verweisen auf Dokumente dieses Wikis, die für

registrierte Administratoren online nutzbar sind und interessierten Lesern per Mail zur Verfügung gestellt werden können.

Plant man den Aufbau mehrerer Server mit identischer Hardware, bietet sich eine Musterinstallation an, in der alle Empfehlungen aus dem vorhergehenden Abschnitt schon berücksichtigt wurden (Service Pack, Sicherheits-Updates/-einstellungen, Virenscanner usw.). Auch der aktuell empfohlene Tivoli Storage Manager-Klient (TSM-Klient) sollte schon installiert und vorkonfiguriert werden (*www.hu-berlin.de/rz/filesv/clienten.html*). Bevor von dieser Installation ein Image erstellt wird, ist es sinnvoll, die Anwendung SYSPREP auszuführen (immer beim Klonen von Installationen aus einem Image). Spielt man ein derartig erzeugtes Image auf eine andere Serverhardware, so wird nach dem ersten Booten automatisch eine Individualisierung des Serversystems [4] gestartet. Unter anderem erhält das Serversystem dabei einen individuellen Sicherheits-Identifikator (SID), der das ordnungsgemäße Zusammenspiel des Servers mit dem Netzwerk erst ermöglicht.

Windows-Server sind entsprechend der gültigen Namenskonvention [5] zu benennen. Beispiele für gültige Namen sind HUCMS02, HUGEO01 für Domänen-Controller sowie HUPSY12, HUGEO11 für Fileserver.

Ein so vorbereiteter Server kann dann mit dem Netzwerk verbunden werden. Anschließend lässt er sich entweder zu einem Domänen-Controller, Terminal Server oder Fileserver konfigurieren. Auf allen Platten ist das Dateisystem NTFS einzusetzen, um eine ausreichende Sicherheit des Zugriffs auf Serverdaten zu gewährleisten.

## Sicherung der stabilen Funktion der bereitgestellten Netzwerkressourcen

Für die stabile Funktion von Servern sind regelmäßige Wartungsarbeiten erforderlich, die sich aus der Benutzung des Systems, aber auch aus der möglichen »Ausnutzung« neu entdeckter Schwachstellen der Server-Software ergeben.

Die Benutzung führt über kurz oder lang zu einer Fragmentierung von Dateien auf den Serverplatten, welche die Zugriffszeiten auf die Daten erhöht und die Platten mechanisch stärker beansprucht. Windows 2000 enthält ein eigenes Defragmentierungstool. Da die gegenwärtige Version nicht sehr leistungsfähig ist, muss das Tool von Anfang an regelmäßig angewendet werden. Außerdem muss noch mindestens 20 % der Speicherkapazität jeder logischen Platte frei sein, um mit ihm eine Defragmentierung erfolgreich durchführen zu können.

Eine Möglichkeit, hinreichend freien Platz auf den Serverplatten zu sichern, ist die konsequente Verwendung von Strategien zur Begrenzung des Speicherplatzes für Benutzer und Benutzergruppen (Quotas). Windows 2000 Server bietet nur eine minimale Unterstützung von Quotas. Ein Praxiseinsatz ist nur für Home-Verzeichnisse der Benutzer sinnvoll. Für gemeinsam genutzte Verzeichnisse bietet es keine Lösung. Wird diese Quota-Unterstützung benutzt, sollten außer Home-Verzeichnissen keine weiteren Datenbestände von Benutzern auf der Platte sein.

Durch den Einsatz von geeigneter Quota-Software (z. B. Space Guard SRM) können Sie die Probleme mit der Verwaltung des Speicherplatzes besser lösen und vor allem mit vernünftigem Zeitaufwand regeln.

Die Aufdeckung von Sicherheitslücken in der Windows-Software veranlasst Microsoft meist dazu, neue Sicherheitsupdates herauszugeben. Nach den letzten Ankündigungen soll dies einmal monatlich erfolgen. Automatic Update und Windows Update sind für Produktions-Server sehr riskant, da Sicherheitsupdates gelegentlich zu Fehlfunktionen führen. Vom CMS werden in einem Testnetz Erfahrungen mit den Sicherheitsupdates gesammelt, bevor sie in Patch-Prozeduren integriert werden. Diese vom CMS bereitgestellten Patch-Prozeduren können dazu genutzt werden, Ihre Server vor vielen neuen Angriffsvarianten zu schützen. Sie müssen sich jedoch bewusst sein, dass nicht alle Besonderheiten Ihrer Server vom CMS vorab getestet werden können.

Weitere Probleme im Serverbetrieb treten durch Stromausfälle, Ausfall von Netzteilen und »Durchbrennen« von Stromsicherungen auf. Neben dem Einsatz redundanter Netzteile ist es deshalb sinnvoll, eine Einschaltverzögerung für die an eine Sicherung gekoppelten Endverbraucher (Netzteile) zu realisieren, um die Gefahr der Überlastung dieser Sicherung zu reduzieren. Bei dem am CMS eingesetzten ePowerSwitch8 werden die acht geschalteten Stromanschlüsse im Abstand von 250 ms aktiviert. Unsere Tests haben gezeigt, dass die Überlastung der Stromkreise beim Einschalten dadurch verhindert wird.

Auch Plattenausfälle sind relativ häufig. Wird mit fehlertoleranten RAID-Systemen gearbeitet, ist es wichtig, dass die Verantwortlichen automatisch darüber informiert werden, welche Platten eines Servers vom Ausfall betroffen sind. Nur eine umgehende Warnung der RAID-Software kann verhindern, dass nicht durch weitere Plattenausfälle das RAID zerstört wird.

Über eine Vielzahl von Problemen werden die Serververantwortlichen von Windows-Systemen nicht automatisch informiert. Deshalb ist eine regelmäßige Kontrolle der Ereignisprotokolle erforderlich. Können dort aufgeführte Probleme nicht umgehend gelöst werden, so sollten die zugehörigen Log-Dateien unbedingt zwecks späterer Analyse gesichert werden. Um das lästige Einloggen auf alle Server zu umgehen, sollte ein zentrales Logging realisiert werden. Zur weiteren Vereinfachung bieten sich Skripts zur automatischen Logdatei-Analyse an.

Außerdem sind viele weitere Ereignisse (Brand, Diebstahl, Bedienfehler, …) denkbar, welche die Sicherung der wesentlichen Daten der Server auf einem räumlich getrennten Backupsystem erfordern. Die HU setzt zu diesem Zweck TSM mit einer einheitlichen Backupstrategie ein. Die TSM-Server aktivieren ihre Klienten (z. B. Windows-Server) täglich zu verabredeten Zeitpunkten zu inkrementellen Backups. Ist ein Backup total oder teilweise fehlgeschlagen, werden die Verantwortlichen des Klienten per Mail darüber informiert. TSM wird an der HU nicht zur Archivierung von Daten eingesetzt. So ist acht Wochen nach dem Löschen einer Datei, die mit dem TSM gesichert wurde, nichts mehr von ihr vorhanden. Daten, welche jahrelang von Interesse sind, sollten individuell auf geeigneten Medien (z. B. CD) gesichert und auch nach entsprechenden Zeiträumen auf eventuell modernere Medien kopiert werden.

Um den Überblick über durchgeführte Arbeiten an den zahlreichen Servern zu behalten, ist die Dokumentation dieser Arbeiten unumgänglich. Arbeiten, die alle Server betreffen (Updates, Defragmentierungen, Prüfen der Dateisysteme, der Event-Logs, der TSM-Logs, des Speicherverbrauchs auf den Festplatten, der Integrität der RAID-Systeme, der Funktion der Netzteile, der Aktualität des Virenscanners, …), sollten tabellarisch erfasst werden (siehe auch [6]). Arbeiten, die zur Dokumentation oder Behebung konkreter Probleme einzelner Server erfolgen, sollten in Form einer Änderungs-Log

(Changelog) für jeden Server getrennt dokumentiert werden. Die tabellarische Erfassung sichert, dass kein Server vergessen wird. Die Changelog eines Servers weist oft auf seine Besonderheiten hin – z. B. unzuverlässige Hard- oder Software, Lastprobleme, Änderungen an der Konfiguration.

Auch die Schaffung geeigneter Arbeitsbedingungen für die Administration unterstützt indirekt die Verfügbarkeit des Windows-Netzes. Die Verwendung von Monitor-, Tastatur- und Mouse-Umschaltern für PCs (z. B. KVM-Switches) bietet sich für die lokale Administration einer größeren Anzahl von Servern an. Analog sind die Terminal Services (im Remote Administration Mode) zur Fernwartung nutzbar. Die schon erwähnten Power-Switches lassen sich zusätzlich über den eingebauten Web-Server zum An- und Ausschalten von Servern (bei Havarien von entfernten Arbeitsplätzen aus) verwenden, was natürlich gut gegen Missbrauch abgesichert werden sollte. Für die Fernadministration ist es wichtig, dass nur über sichere Verbindungen gearbeitet wird.

## Benutzerverwaltung

An der HU besteht gegenwärtig das Ziel, einheitliche Benutzerkennzeichen in der UNIX- und in der Windows-Welt zu realisieren. So wird es einfacher, das im UNIX bewährte halbjährliche Passwort-Update auch zum Update des Windows-Passworts eines entsprechenden Active Directory (AD) Accounts zu benutzen. Auf diese Weise ist ein relativ hoher Schutz all jener AD-Accounts, die eine Entsprechung im UNIX haben, möglich. Die Vereinheitlichung der Benutzerkennzeichen zielt außerdem auf eine spätere Realisierung von Single Sign-On Mechanismen für Ressourcen der HU ab. Um in einer Windows-Domäne Übersichtlichkeit und Möglichkeiten der Delegierung von administrativen Aufgaben zu realisieren, ist der Aufbau einer geeigneten Organizational Unit-Struktur [7] erforderlich.

An der HU wird ein UNIX-Account, dessen Passwort über ein halbes Jahr nicht geändert wurde, als unsicher eingestuft und automatisch gesperrt. Diese Sicherheitsmaßnahme ist seit Jahren aktiv. Mit der Angleichung der Benutzerkennzeichen zwischen der UNIX- und der Windows-Welt sowie der Realisierung einer Passwort-Synchronisation zwischen diesen Welten ist auch die automatische Sperrung unsicherer AD-Accounts realisierbar. Der Active Directory User Manager (ADUM) [8] wurde am CMS entwickelt, um die Vereinheitlichung der Accounts zu unterstützen. Der ADUM benutzt Account-Informationen aus der Account-Datenbank des CMS [9] zur Erzeugung entsprechender Accounts im AD von Windows.

Die aufwendigste Aufgabe der Benutzerverwaltung und der Aufbauphase des Windows-Netzes der HU – die Einbindung der Arbeitsplatzrechner der Benutzer in das AD und die Wiederherstellung der gewohnten Arbeitsfähigkeit (Desktop, Browser, Netz-Platten, Netz-Pfade, Prozeduren, Anwendungen, Projektbeziehungen, Vertretungsfunktionen, …) – sei hier nur genannt. Als nachteilig erweist sich dabei die unter VINES verbreitete Praxis, Home- und Projektverzeichnisse auf einem Laufwerk zu verwalten. Für das Windows-Netz ist eine Trennung von Home- und Projektverzeichnissen vorgesehen, um z. B. eine Quotierung der Home-Verzeichnisse mit Windows-Mitteln realisieren zu können.

## Anpassung der Netzwerkressourcen an neue Erfordernisse

Heute ist ein Rechner, der vor drei Jahren Stand der Technik war, oft nur noch eingeschränkt nutzbar. Nicht ganz so schlimm ist es bei den Windows-Betriebssystemen, aber fünf Jahre scheint etwa das Limit zu sein. Man wird gezwungen, ständig neue Soft- und Hardware ins Netzwerk zu integrieren. Diese Arbeiten sind mit unabsehbaren Risiken bezüglich der Netzwerkfunktionen verbunden. Deshalb ist ein Test neuer Komponenten in einer geeigneten Testumgebung dringend angeraten. Trotz solcher Tests verbleibt beim produktiven Einsatz immer noch ein Restrisiko, mit dem man leben muss. Unser Test-Netz (rz2k.hu-berlin.de) wird deshalb das produktive Windows-Netz der HU ständig begleiten und sollte von allen Domänenverantwortlichen weiterhin genutzt werden.

## Literatur


[1] Naumann, W.: Patch-Prozedur post-sp3.bat, https://appel.rz.hu-berlin.de/twiki/bin/view/W2kadmin/PatchesW2kSrvProcPostSP3

[2] Rohde, D.: Installation und Konfiguration des Virenscanners (von NAI), https://appel.rz.hu-berlin.de/twiki/bin/view/W2kadmin/NAINetShieldInstallation

[3] Naumann, W.: Checkliste zur Serverinstallation, https://appel.rz.hu-berlin.de/twiki/bin/view/W2kadmin/InstW2SChecklist

[4] Naumann, W.: Individualisierung eines Serversystems, https://appel.rz.hu-berlin.de/twiki/bin/view/Windows2000/ServerIndividuum (eingeschränkter Zugriff)

[5] Naumann, W., Rohde, D.: Windows 2000 Namenskonvention der HU, https://appel.rz.hu-berlin.de/twiki/bin/view/W2kadmin/NamensKonventionen

[6] Rohde, D.: Zusammenarbeit organisieren durch TWiki. (in diesem Heft)

[7] Rohde, D.: Organisation Unit-Struktur im PC-Netz der HU, https://appel.rz.hu-berlin.de/twiki/bin/view/W2kadmin/PlanungOuStruktur

[8] Rohde, D.: Active Directory User Manager, https://appel.rz.hu-berlin.de/twiki/bin/view/W2kadmin/HandbuecherAdum

[9] Rohde, D.: Account-Datenbank des CMS, https://appel.rz.hu-berlin.de/twiki/bin/view/W2kadmin/HandbuecherAccMan