Re-Zentralisierung von DHCP und DNS als Ansatzpunkt neuer Dienste

Tarik Gasmi, Dirk von Suchodoletz

Lehrstuhl für Kommunikationssysteme
Rechenzentrum der Universität Freiburg
Herrmann-Herder-Straße 10
79104 Freiburg
tarik.gasmi@rz.uni-freiburg.de
dirk.von.suchodoletz@rz.uni-freiburg.de

Abstract: Eine geeignete Re-Zentralisierung der Basisdienste DHCP und DNS kann Rechenzentren in die Lage versetzen, ihre Netzwerke effektiver zu steuern, einen besseren Überblick zu behalten und sie gleichzeitig sicherer zu machen. Durch den Einsatz zentraler, redundanter Server mit Steuerung über ein Web-Interface können dezentrale Administratoren unter Nutzung bestehender Identity Management Infrastrukturen authentifiziert ihre Ressourcen verwalten. Zusätzlich kann das Rechenzentrum neue Dienste, wie VoIP-Telefonie, Diskless Remote Boot oder die Netzwerkinstallation verschiedener Betriebssysteme anbieten. Gleichzeitig erhält es die Möglichkeit lenkend einzugreifen und neue Herausforderungen, wie ein zentrales Energiemanagement, den flexiblen Aufbau neuer Dienste und langfristig die Einführung von IPv6 zu meistern. Dieser Artikel beschreibt, wie am Rechenzentrum der Universität Freiburg beispielhaft der Generationswechsel vorgenommen wird, welche Schritte schon erfolgt und welche weiteren geplant sind. Die berichteten Erfahrungen könnten durchaus für ähnliche Einrichtungen von Interesse sein.

1 Motivation

Rechenzentren sehen sich neuen Herausforderungen gegenüber: Trotz einer gewissen Sättigung bei der Zahl der festinallierten Arbeitsplatzrechner, kommt eine neue Dynamik in der Vergabe der IP-Adressen und Rechnernamen auf. Die Anzahl IP-basierter, dabei oft mobiler, Geräte nimmt mit drahtlosen und festinstallierten VoIP-Telefonen, Laptops, PDAs stark zu. Gleichzeitig steigt der Bedarf nach Compute-Leistung, die von einer größer werdenden Gruppe von Instituten nachgefragt und typischerweise als Rechen-Cluster oder GRID installiert wird. Die Menge dieser IP-Nachfrager ist nicht nur möglichst aufwandsarm zu bedienen, sondern gleichzeitig zu monitoren und sinnvoll zu steuern. Die Vergabe und Verteilung der Ressource IP erfolgte eine längere Zeit dezentral durch Delegation. Was in der Anfangszeit das RZ entlastete und einzelnen Einrichtungen die gewünschten Freiheiten brachte, schafft heutzutage Probleme. Die Netzwerksicherheit und das Site Monitoring stehen aktuell vor ganz anderen

Herausforderungen als vor zehn Jahren. Neue Angebote, wie Diskless Remote Boot oder -Installation, immer mehr IP-basierte Dienste oder die Forderung nach einem übergreifenden Energiemanagement, lassen eine Rezentralisierung von DHCP- und DNS-Management in einem neuen Licht erscheinen.

Dezentrale IP-Clients müssen geltenden Policies der Institution und individuellen Bedürfnissen der Nutzer entsprechend in unterschiedlichen Teilen der Netzinfrastruktur einsatzbereit gemacht werden, ohne dass dabei die Übersicht und Kontrolle über das wachsende Netz verloren geht. Hier erscheint es sinnvoll auf der einen Seite lokalen Administratoren weiterhin die Freiheiten zu lassen, weitgehende Einstellungen ihrer Clients vorzunehmen, ohne dass sie dafür einen eigenen Service pflegen und regelmäßig aktualisieren müssen. Auf der anderen Seite bietet eine zentrale Serverstruktur die beste Chance eine zentrale Datenbasis zu pflegen, die durch das Eigeninteresse der Beteiligten beständig aktualisiert wird. Den Zugriff auf diese gewährt sinnvollerweise eine Komponente des zentralen Identity Managements (IDM). So bleibt der Überblick erhalten und neue IP-basierte Dienstleistungen können schnell angeboten werden.

2 Projekt *Site Management* am RZ der Universität Freiburg

Wie bei den meisten anderen Rechenzentren auch, ist die Verwaltung der traditionellen IP-Dienste DHCP und DNS eine zentrale Aufgabe. Nach einer Anfangsphase der händischen IP- und Namensvergabe im RZ kam die Zeit einer dezentralen Administration und lokalen Zuweisung in den einzelnen Instituten. Diese Vorgehensweise war so lange sinnvoll leistbar, bis neue, campus-weite Dienste, wie Wireless LANs aufkamen und der Umstieg auf VoIP-Telefonie anvisiert wurde. Darüber hinaus erfolgt, oft verbunden mit dem Wechsel der Mitarbeiter der ersten Stunde, eine stärkere Fokussierung der Aufgaben der IT-Arbeiter an den Instituten auf die wissenschaftlichen Kernaufgaben. So sollen, wie schon die zentralen Dienste WWW-Server und Email, nun auch die Verwaltung der Infrastruktur von der zentralen Einrichtung Rechenzentrum übernommen werden.

2.1 Neue Herausforderungen – Umstellung auf IP-Telefonie

Maßgeblich für die Neustrukturierung der Administration der IP-Basisdienste war neben gestiegenen Anforderungen bei der Bedienung der WLAN-Infrastruktur und Rechner-Pools der Universität das anstehende Roll-Out einer großen Anzahl neuer VoIP-Geräte. Besonders in komplett neu aufzubauenden Strukturen, wie einiger im Zuge der Exzellenzinitiative neu geschaffener Einrichtungen, bietet sich der Umstieg auf IP-basierte Telefonie gerade zu an. Dies ist jedoch nicht die einzige Stelle, an der das Rechenzentrum einen zentral zu verwalteten Dienst – die Telefonie, die über ein eigenes drahtgebundenes Kabelnetz verfügt, mit dem IP-Netz zusammenzuführt. Jedes neuinstallierte VoIP-Telefon erfordert eine eigene Adresse im jeweiligen Teilnetz des Instituts. Ein zentralisierter DHCP-Dienst bietet erhebliche Vorteile, wenn einige Tausend IP-Geräte in die Infrastruktur integriert werden müssen. Darüber hinaus sollte

auch die Verwaltung der zunehmenden Zahl zentral gemanagter Rechner-Pools vereinfacht und für neue Arten der Steuerung und Nutzung geöffnet werden.

Genauso wie die klassische Telefonie ist auch IP-Telefonie wegen ihrer Komplexität in einer größeren Netzwerkinfrastruktur nur als zentraler Dienst wirklich sinnvoll betreibbar. Zwar wären in einzelnen Abteilungen lokale Services weiterhin denkbar. Jedoch ist ein hoher Beratungsaufwand und ein höheres Risiko des Ausfalls des kritischen Dienstes "Telefonie" zu erwarten. Das traditionelle Trivial FTP gewinnt mit der Zahl eingebetteter Geräte, wie Telefone und Infrastrukturkomponenten (Switches, WLAN Access-Points) wieder eine größere Bedeutung. Softwareinstallation und -verteilung nutzen diesen Service, der eng mit DHCP zusammenarbeitet. Hierzu möchte man sämtliche IP-Telefone zentral sehen und steuern können. Deshalb sind an der Universität Freiburg inzwischen Telefonzentrale und Rechenzentrum eng verzahnt.

Da eine komplette Netztrennung, aus Sicherheitsgründen und zur Einhaltung bestimmter Serviceparameter, zwar wünschenswert, aber aus Kosten- und Aufwandsgründen nicht realisierbar erscheint, bieten sich hier Virtual-LAN Konzepte an. Auch hier ist eine zentrale Steuerung und Koordination in größeren Umgebungen aus Gründen der Komplexität zwingend erforderlich. Die VLAN-Konfiguration lässt sich zudem gut mit DHCP integrieren[1], weiterhin bleiben dadurch relevante Netzwerkparameter, wie zu gewährleistendes QoS im Blick**.**

2.2 Vision: Re-Zentralisierte Strukturen und verteilte Administration

Dienst-spezifische Appliances können den Administrationsaufwand eines IP-Netzes durchaus senken, sind jedoch häufig zu eingeschränkt, um site-spezifische Anpassungen und Besonderheiten berücksichtigen zu können. Deshalb und angesichts des zu erwartenden Zuwachses an zu verwaltenden Ressourcen, ist das Rechenzentrum der Universität Freiburg bestrebt, die Administration dieser Dienste umzustrukturieren.

Schnell verfügbare Informationen zu Menschen und Maschinen sind in solchen Umgebungen unabdingbar: Das zentrale Netzwerkmanagement möchte zügig erfahren können, was für Maschinen welche Aufgaben versehen und wer die verantwortlichen Personen sind.

Die zentrale Speicherung dieser Daten, darunter auch Konfigurationsdaten von Diensten, bietet einige Vorteile. Zunächst sind sie einzelnen Administrationsprozessen in einem *Single Point of Administration* zugängig, so dass mittels netzbasierter Verwaltungswerkzeuge, Arbeiten von jedem beliebigen Rechner im Netzwerk zentral ausgeführt werden können. Außerdem lassen sich Daten und Zugriff auf diese Weise leichter kontrollieren, sowie Administrationsabläufe automatisieren und zentral steuern. Ferner besteht damit die Möglichkeit durch kontrollierte Delegation definierter administrativer Teilaufgaben, die Gesamtadministration auf mehrere Instanzen zu

[1] VLAN Discovery per DHCP: Das IP Device erhält beim ersten Booten anhand definierter Kriterien per DHCP Option ein bestimmtes VLAN mitgeteilt. Nach einem DHCP-Release bootet es erneut, allerdings mit VLAN-Tag in der DHCP Anfrage, und erhält so die dem VLAN entsprechende Konfiguration.

verteilen. Die zentrale Administration wird so entlastet, während lokale Site-Administratoren im Zuge der Re-Zentralisierung nicht entmündigt werden.

Leistungsfähigere Hardware und Netzwerkinfrastrukturen erlauben es Rechenzentren zunehmend, zentralisierte Dienste an ihre Kunden zu bringen. Diskless Remote Boot, Installation oder Hardwaretests via Netzwerk vereinfachen Arbeitsabläufe erheblich. Sind lokale Betriebssystem-Installationen nicht mehr notwendig, lassen sich Geräte leichter austauschen und durch unterschiedliche Betriebsarten flexibler einsetzen.

Weitere Vorteile zentralisierter Strukturen ergeben sich aus ihrer besseren Überschaubarkeit für die Organisation von Managementprozessen. In größeren Institutionen lassen sich Verwaltungsabläufe klarer strukturieren und definieren. Eine effiziente Abstimmung oder Kombination hilft bei der Senkung des Administrationsaufwands.[2]

2.3 Umsetzung und Ziele

Gegenstand des vorgestellten Projekts ist die Implementation und sukzessive Inbetriebnahme eines Verwaltungssystems, das bestimmte in Beziehung stehende Administrationsprozesse des Client, Dienste und Netzwerk Management in einem verteilten Framework gewinnbringend zusammenführt. Dabei sollen bereits vorhandene Strukturen, wie Monitoring-Dienste oder das zentrale Identity Management sinnvoll einbezogen werden.

Der grundlegende Entwurf entstand im Rahmen einer Diplomarbeit am angegliederten Lehrstuhl für Kommunikationssysteme [Ga06], und wird seit Anfang 2007 am Rechenzentrum als Projektarbeit zur praktischen Umsetztung weiterverfolgt. Die nachfolgend aufgeführten Ziele sollen dabei einen entscheidenden Beitrag zur effizienteren Verwaltung und besseren Kontrolle der Netzwerkinfrastruktur leisten und können in detaillierter Form den Artikeln in [SG07], [SSG07] entnommen werden.

Für die Umsetzung sollten eine Reihe von Punkten schrittweise Berücksichtigung finden und zudem die Grundlage für das Angebot neuer IP-basierter Dienste bieten:

- Ablösung der händischen Delegation von IP-Bereichen und Namensräumen zur Entlastung der dezentralen IT-Mitarbeiter vom DNS/DHCP-Serverbetrieb
- Automatisierung der Namens- und IP-Vergabe gerade für Massenressourcen, wie Pool-PC, WLAN-Laptops, Cluster-Maschinen oder VoIP-Telefone
- Delegation der Ressourcen von einer zentralen Stelle aus. Authentifizierung aller Administratoren, die Änderungen vornehmen zur Verknüpfung von Maschineninformationen mit zuständigen Ansprechpartnern

[2] So lassen sich Management Prozesse der Institution als global und klar definierte IT-Prozesse nach den standardisierten Vorgaben der IT Infrastructure Library (ITIL) leichter realisieren.

- Erstellung einer zentralen, aus Eigeninteresse gut gepflegten Datenbank, der IP-Clients

- Sichere Backups und Hochverfügbarkeit der Dienste, Realisierung von Rollbacks einzelner Schritte

Zentralisierte Standarddienste bei dezentraler Administration

Lokal, in einzelnen Abteilungen, vorliegende Konfigurationsdaten der zentralen IP-Dienste DNS und DHCP, wie beispielsweise Namen, MAC- und IP-Adressen der einzubindenden Clients, werden dezentral von den jeweiligen Administratoren bearbeitet. Das Verwaltungssystem sorgt dabei für die kontrollierte Aufnahme der Daten und die automatisierte, zeitnahe Aktualisierung der Dienstekonfiguration. Dies entlastet die zentrale Administration der Dienste entscheidend. Gleichzeitig beschränkt sich die Verwaltungsarbeit in den einzelnen Abteilungen auf die Administration Host-spezifischer Optionen der eigenen Clients.

Die Einführung von DHCP als organisationsweiter zentraler Dienst wird mittelfristig den eigenständigen Betrieb von DHCP-Servern auf Site-Ebene ablösen. Durch die Verwaltungshoheit über globale und Subnetz-spezifische DHCP-Optionen erhält das Rechenzentrum ein Stück zentraler Kontrolle über seine IP-Netze zurück.

Flexible Steuerung und Nutzung der Ressourcen

DHCP ist Bestandteil des von Remote Boot Diensten genutzten initialen Netz-Boot-Konzepts.[3] In dem Moment, wo sich jede Maschine beim Start zunächst einmal per DHCP in der Zentrale "meldet", kann diese bei Bedarf in den Startvorgang eingreifen und eine Reihe von Services, wie automatisierte Test der Maschine oder die Installation diverser Systeme und Software anbieten. Neben der immensen Erleichterung der Administration von Maschinen, ergeben sich daraus diverse Möglichkeiten, Ressourcen flexibel und gezielt einzusetzen.

Unterschiedliche Systemkonfigurationen für Clients lassen sich zentral einrichten und verwalten. Rechner können nach Bedarf zu definierten Zeiten, durch einen Reboot in einen anderen Betriebsmodus "umgeschaltet" werden (*Betriebsmodus on Demand*). So können Pool-Systeme oder Mitarbeiter-Desktops in Randzeiten in einem Compute Cluster verwendet werden. Zu diesem Zweck bietet das Framework in einer weiteren Ausbaustufe verschiedene Services und Systeminstallationen potenziellen lokalen Nutzern an.

Sie werden Form von Bausteinen für PXE-Bootkonfigurationen bereitgestellt, die alle Informationen zu den einzubindenden Ressourcen und ihren TFTP-Quellen enthalten.

[3] Dieses netzbasierte Bootkonzept wird durch Kombination der Dienste PXE, DHCP und TFTP realisiert, und versorgt den anfangs „nackten" Client mit einer Netzwerkkonfiguration und einer initialen Bootdatei. Darauf aufbauend können im weiteren Bootprozess remote verschiedenste Betriebsressourcen, wie Betriebssystem, Software, Dateisystem eingebunden werden.

Aus ihnen zusammengestellte Default-PXE-Bootmenüs werden via Netzwerk bootenden Rechnern standardmäßig präsentiert. Darüberhinaus können lokale Administratoren über das Verwaltungssystem eigenen Clients aus diesen Bausteinen individuell kombinierte PXE-Bootmenüs zuweisen. Zusätzlich soll eine integrierte Zeitsteuerung die Zuweisung unterschiedlicher Boot-Konfigurationen zu definierten Zeiten an einen Client ermöglichen. Aus den zentral im System gespeicherten PXE-Daten werden dann per Konfigurations-Tools auf entsprechenden TFTP-Servern die PXE-Konfigurationsdateien generiert.

Die Bereitschaft laufende, aber gerade nicht benötigte Geräte auszuschalten, ist vielfach zwar vorhanden. Jedoch geht durch fehlenden Überblick und das simple Vergessen viel Sparpotenzial verloren. In dem Augenblick, wo sich viele Maschinen zentral gesteuert durch Wake-on-Lan, Shutdown oder Reboot remote bedienen lassen, kann ein effizientes Energiemanagement greifen. Zudem lohnt sich mit einer steigenden Anzahl von Geräten auch über komplexere Mechanismen nachzudenken.

Mit der Aufnahme von IP-Clients in eine zentrale Datenbank sind die Grundlagen für verschiedene Arten der Remote-Administration geschaffen. Die Verknüpfung von Personen oder Administratoren mit ihren Maschinen erlaubt eine schnelle Benachrichtigung bei Problemstellungen. Überwachungs- und Service-Informationen können leicht an die richtige Stelle weitergeleitet werden. So können in Zukunft dezentrale Einrichtungen auch ohne einige Netzwerküberwachung und eigenes System-Monitoring ihre Komponenten im Blick behalten.

Self-Administration und Identity Management

Neben den Vorzügen für das zentrale Management entledigen zentrale Dienste lokale Administratoren der Aufgabe diese eigens betreiben zu müssen. Tätigkeiten, die die Betriebssicherheit und Überwachung umfassen, entfallen und treffen an zentraler Stelle auf bereits vorhandene Strukturen und spezialisierte Abnehmer. Erfahrungen zeigen, das zentralisierte IT-Strukturen nur Akzeptanz erfahren, wenn sie einerseits die tägliche Arbeit der Nutzer erleichtern, ihnen andererseits aber ein gewisses Maß an Eigenverantwortung und Gestaltungsmöglichkeiten lassen.

Das Management Framework erlaubt Self-Administration bzw. autonomes Management in einem definierten Rahmen. Lokalen Administratoren können das Netzwerk-Setup ihrer Maschinen in Eigenregie durchführen und ihren Betrieb durch die Auswahl verschiedener Remote Boot Dienste flexibel nach eigenen spezifischen Bedürfnissen gestalten. Die Kontrolle der delegierten Kompetenzen bzw. Zugriffsberechtigungen und die Sicherheit des verteilten Verwaltungssystems sind dabei durch entsprechende Authentifizierungs- und Autorisierungsmechanismen zu gewährleisten. Dabei wird auf vorhandene Strukturen des zentralen Identity Management der Universität zurückgegriffen.

Alle Mitglieder der Universität sind in einem zentralen LDAP Verzeichnis des Rechenzentrums registriert, das bereits von diversen Diensten, z.B. Email, WLAN-Zugriff, zur Authentifizierung und Autorisierung der Nutzer herangezogen wird.

Einzelne Accounts werden mittels Flags zur Nutzung bestimmter Dienste berechtigt, so dass Nutzer einen zentralen Login für eine Reihe von Diensten verwenden können. Analog wird über ein entsprechendes Flag in den Accounts berechtigter Site-Administratoren, der Zugang zum Site-Management-Dienst kontrolliert. Dies hat u.a. den Vorteil, dass bestimmte IDM Prozesse der Benutzerverwaltung, etwa die Sperrung eines Accounts oder eine einfache Passwortänderung, im Managementsystem sofort *aktiv* werden, ohne Notwendigkeit einer Synchronisation mit der systeminternen Benutzerdatenbank.

3 Aktueller Zwischenstand der Implementation

Der zentrale DHCP-Dienst ist inzwischen in Produktionsbetrieb übergegangen und die zu seiner verteilten Administration benötigten Komponenten des Verwaltungssystems implementiert. In der aktuellen Pilotphase bedient er bereits die Lehrpools, einen Großteil der Mitarbeiter-Desktops und die ersten angeschlossenen IP-Telefone des Rechenzentrums, sowie Netze und Maschinen einer Reihe von Instituten der Universität.

Das Herzstück des Frameworks bildet als Datenbasis ein LDAP-Verzeichnis, welches die Verwaltung des DHCP- und DNS-Diensts mittels entsprechendem Konfiguration-Tool erlaubt. Dieses ist aufgespalten in ein Web-basiertes Benutzer-Interface zur Durchführung der Administration und ein skriptgesteuertes Backend, das die Aktualisierungen der Dienste vornimmt. Hinzu kommen Komponenten für die Steuerung eines TFTP-Servers, welcher in Zukunft die per Web-Interface eingerichteten Boot-Menüs oder -Aktionen der Clients steuert. Alle Komponenten sind auf einem redundanten Serversystem implementiert.[4] Das System wird vom zentralen Netzwerkmanagement des Rechenzentrums betrieben und wurde in bestehende Sicherungsstrukturen, wie Monitoring- und Backup-Dienste integriert.

[4] Zwei redundante Server im Fallback-Mode mit *Gentoo* Linux (Hardened), *ISC DHCP* mit DHCP-Failover. Verwaltungssystem: *OpenLDAP* (Master-Slave-Modus), *Apache Webserver* mit PHP-Webinterface.

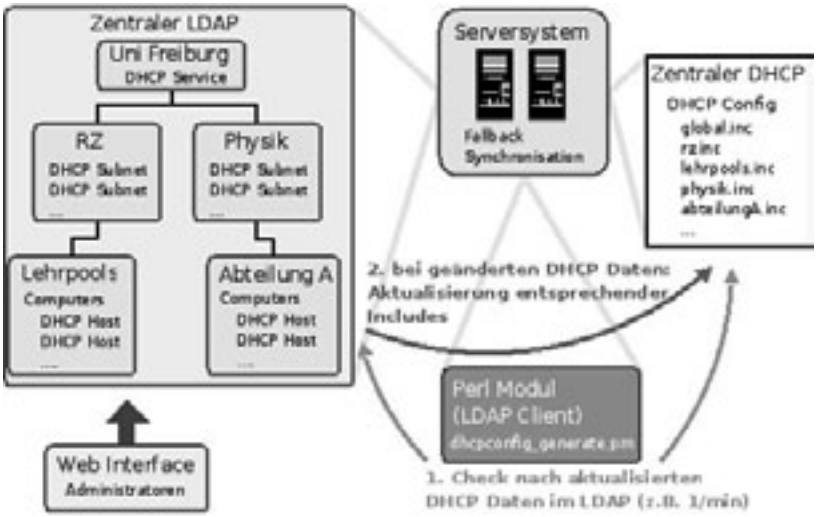

Abbildung 1: Site Management - DHCP Management und Konfiguration

Das System verfügt über Mechanismen zur Delegation von IP-Adressbereichen an untergeordnete Einheiten, und gewährleistet so, dass nur "korrekte" bzw. eindeutige Client-IP Zuweisungen in die Konfiguration der Dienste einfließen.

Die zentrale Instanz übernimmt Kontrolle und Administration der im System eingetragenen IP-Netze und ihrer DHCP-Optionen. Sie setzt auch die globalen Optionen des DHCP-Dienstes. Lokale Administratoren können über das Benutzerinterface Maschinen eintragen und diesen MAC und ihnen delegierte IP-Adressen zuweisen. Ferner steuern sie die Einbindung ihrer Clients in den DHCP-Dienst und legen deren DHCP Host Options fest. Lokale Sites, die im System über komplette Subnetze verfügen, können zudem spezifische DHCP Subnetzoptionen setzen und dynamische DHCP Pools mit entsprechenden Optionen anlegen. Die Aktualisierung der DHCP-Konfiguration erfolgt wiederum durch die zentrale Administration kontrolliert, asynchron und automatisiert über das eigens dafür implementierte Perl-Modul.[5] Die Gesamtkonfiguration ist dabei Zwecks besserer Übersicht und Handhabe, über einzelne Include-Dateien realisiert, die jeweils einer autonom administrierten Einheit entsprechen.

Das Interface unterstützt bereits die Nutzung der am Rechenzentrum betriebenen Remote Boot Services [OSLX], [NETP]. Deren Zugangsinformationen, Bootserver-IP und initiale Bootdatei, sind im System hinterlegt und werden für individuell auswählbare Clients, automatisch als DHCP-Optionen[6] in deren DHCP-Konfiguration übernommen. Die Implementierung der Verwaltung von spezifischen PXE-Konfigurationen, die dann einen noch flexibleren Einsatz von Maschinen ermöglicht, ist derzeit in der Entwicklung und Erprobung.

[5] Das Modul verwendet dazu das LDAP Client Perl-Modul *Net-LDAP*.
[6] DHCP Optionen *next-server* und *filename*

Ein zentraler DNS Dienst wird bereits betrieben. Hier soll die Verwaltung der DNS-Zonen soweit in das Framework integriert werden, dass die Administration der Namenseinträge in analoger Weise von lokal Administratoren dezentral erfolgen kann. Derzeit ist die eindeutige Zuordnung von DNS-Zonen zu einzelnen Einheiten und ihren Clients realisiert. Integrierte Mechanismen sorgen dabei für eindeutige DNS-Namen im LDAP Verzeichnis und Verwaltungssystem. Der konsistente Abgleich zwischen System, DHCP-/DNS-Konfiguration, sowie die automatisierte Generierung von DNS-Zonendateien, soll zukünftig über ein entsprechende Perl-Module erfolgen.

Nach erfolgreicher Anmeldung gegen das zentrale externe Benutzerverzeichnis, erfolgen alle weiteren Systemzugriffe über das dem Benutzer entsprechende intern gespeicherte Benutzerobjekt. Die Kontrolle der Zugriffsrechte zentraler und lokaler Administratoren auf definierte Daten ist dabei über ein Rollen-basiertes Rechte-Modell realisiert.[7] Definierte Rollenobjekte erhalten über LDAP Access-Control-Lists und entsprechende Mechanismen im Webinterface spezifische Rechte im System, die einem Benutzer durch die Zuordnung *Benutzerobjekt – administrative Rolle* übertragen werden. Neben der Rolle *Systemadministrator*, die vollen Zugriff auf alle Verzeichnisobjekte hat, verfügen *Hauptadministratoren* einer Verwaltungseinheit Zugriff auf alle ihre Objekte ihrer hierarchisch untergeordneten Einheiten. Innerhalb jeder Einheit kann per Rolle *Client-Administrator* Personen die Verwaltung von Rechnerobjekten übertragen werden. Dementsprechend kann das System für weitere spezifische Verwaltungstätigkeiten um zusätzliche Rollen erweitert werden.

4 Fazit und Ausblick

Die bisherigen Experimente und Erfahrungen, die neben dem eigenen Pool-Betrieb erste externe Institute außerhalb des Rechenzentrums umfassten, verliefen positiv. Das Angebot, IP-Dienste zentral zu verwalten, wurde begrüßt. Im Rechenzentrum gelang es, Aufgaben besser zu verteilen und zu delegieren. So konnte beispielsweise die Betriebsgruppe beim Austausch defekter Hardware selbstständig die MAC-Adresse des ersetzten Systems ändern, ohne hierfür den Pool-Betreiber beauftragen zu müssen. Zudem vereinfachte sich das Netzwerkmanagement, da nun in den Routern nur noch ein einheitliches DHCP-Relay eingetragen werden musste. Die Umstellung lief in Absprache mit den Beteiligten problemlos. Die Aufgabenverteilung wurde klarer. Der nächste Schritt besteht in der Integration der Boot-Menü-Zusammenstellung. Während diese bisher für Pool-Umgebungen noch fest vorgegeben ist, soll dieses in weiteren Schritten dezentral definiert werden können. Sobald dieses steht, sind in der nächsten Phase Experimente zum verteilten Cluster-Betrieb vorgesehen. Eine gewisse Herausforderung wird bei der Integration der verschiedenen PXE-Lösungen aus dem Windows-Umfeld erwartet, da es sich hier um proprietäre Software handelt, die sich eventuell nicht optimal einfügen lässt.

Generell scheint die Einrichtung eines generellen Netzwerk-Boots ein gut gangbarer Weg für Automatisierungen zu bieten. Einerseits kann ein Benutzer vor Ort jederzeit den

[7] *Role Based Access Control*, siehe dazu [NIST][SFK]

PXE-Boot vor dem Aufruf des Boot-Menüs abbrechen. Andererseits lässt sich ein Default-Boot von Festplatte einstellen, der aus Sicht der Nutzer fast keine Änderung des bisherigen Betriebsmodells bedeutet.

In Zukunft könnte man sich sogar vorstellen, dass große PC-Lieferanten, ihre Maschinen mit aktiviertem PXE als Default-Einstellung ausliefern. Für diese im Netzwerk zunächst noch unbekannten Maschinen könnte ein spezieller, zentraler Dienst angeboten werden. Dieser erlaubt dem jeweiligen Nutzer oder lokalen Administrator die Maschine im DHCP/DNS mit den gewünschten Daten zu registrieren, Einstellungen zum Betriebsmodus vorzunehmen und bei Bedarf und vorhandenen Lizenzen eine Installation des Betriebssystems anzustoßen. Auf diese Weise kann die oft sehr lange Zeit von der Anlieferung bis zur tatsächlichen Nutzung eines Gerätes deutlich reduziert werden. Zudem wäre die Maschine gleich von Anfang an im Netzwerk mit ihren Kontaktdaten eines Ansprechpartners bekannt.

Literaturverzeichnis

[DLC] Linux Diskless Clients Projekt. Lehrstuhl für Kommunikationssysteme, Rechenzentrum Universität Freiburg. http://www.ks.uni-freiburg.de/projekte/ldc.

[DRBL] DRBL - Diskless Remote Boot in Linux. National Center for High Performance Computing Taiwan.

[Ga06] Gasmi, T.: LDAP Site Management – ein LDAP/Web basiertes Framework zur Administration von IP Netzen und Rechnerpools. Lehrstuhl für Kommunikationssysteme, Universität Freiburg, 2006. http://www.ks.uni-freiburg.de/php_arbeitdet.php?id=6.

[LSM] LDAP Site Management Projekt. Lehrstuhl für Kommunikationssysteme, Rechenzentrum Universität Freiburg. http://www.ks.uni-freiburg.de/projekte/lsm.

[LTSP] LTSP - Linux Terminal Server Project. http://www.ltsp.org.

[OSLX] OpenSLX Linux Stateless Clients. http://www.openslx.org.

[NETP] Diskless Linux Surfstationen an der Universität Freiburg, http://portal.uni-freiburg.de/rz/dienste/net.point

[Su04] v. Suchodoletz, D: Linux Diskless Clients – eine Effizienzsteigerung im Kursbetrieb. Praxis der Informationsverarbeitung und Kommunikation (PIK). 4/2004; S. 246-250.

[SFK03] Sandhu, R.; Ferraiolo, D; Kuhn, R: The NIST Model for Role Based Access Control: Towards a Unified Standard. Proceedings, 5th ACM Workshop on Role Based Access Control, 2003.

[SG07] v. Suchodoletz, D.; Gasmi, T.: Rezentralisiertes Rechner Management. Praxis der Informationsverarbeitung und Kommunikation (PIK). 2/2007; S. 93-99.

[SSG07] Schneider, G.; v. Suchodoletz, D.; Gasmi, T.: LDAP Site Management – ein LDAP/Web basiertes Framework zur Administration von IP Netzen und Rechnerpools. Tagungsband des Workshops *Integriertes Informationsmanagement an Hochschulen*, Universität Karlsruhe 2007. Universitätsverlag Karlsruhe, 2007; S. 3-18.