

2 Verwalten einer Active Directory Infrastruktur

Lernziele

- Active Directory und DNS
- Besonderheiten beim Anmeldevorgang
- Vertrauensstellungen
- Sichern von Active Directory
- Wiederherstellen von Active Directory
- Verwalten der Datenbank

2.1 Einführung

Nach der Installation von Active Directory müssen einige Verwaltungsaufgaben regelmäßig erfüllt werden.

So ist es von großer Bedeutung, die Zusammenhänge von Active Directory und DNS zu kennen, damit im Fehlerfall eingegriffen werden kann.

Der komplette Anmeldevorgang ist ein sehr interessantes Thema, das ein Teil der Active Directory Verwaltung ist.

Auch verwaltungstechnische Aufgaben, die direkt mit der Datenbank zusammenhängen, müssen gekonnt durchgeführt werden. Hierzu gehören sowohl Sicherung und Wiederherstellung, als auch das Verschieben und Komprimieren der Datenbank.

2.2 Active Directory und DNS

Wie Sie bereits bei der Installation bemerkt haben, ist es unmöglich, Active Directory zu installieren, ohne einen DNS-Server zu haben.

An der reinen Namensauflösung kann das nicht liegen, wenn die ganze Domäne sich, wie in unserer Schulungsumgebung, in einem einzigen Subnetz befindet, ist eine Namensauflösung durch Broadcast möglich.

Der Umstand, dass DNS für Active Directory zwingend vorausgesetzt wird, hängt mit einigen Neuerungen zusammen, die mit Windows 2000 eingeführt worden sind.

2.2.1 Der Anmeldevorgang an einer Windows NT 4.0 Domäne

In einer NT 4.0 Domäne war der Anmeldevorgang sehr einfach.

- Der Client startet, und bemerkt, dass er Mitglied einer Domäne ist
- Der Client versucht per Broadcast einen Domänencontroller zu erreichen
- Alle Domänencontroller empfangen die Anfrage und antworten
- Der schnellste Domänencontroller erhält den Auftrag, den Client zu verifizieren
- Anmeldevorgang beginnt

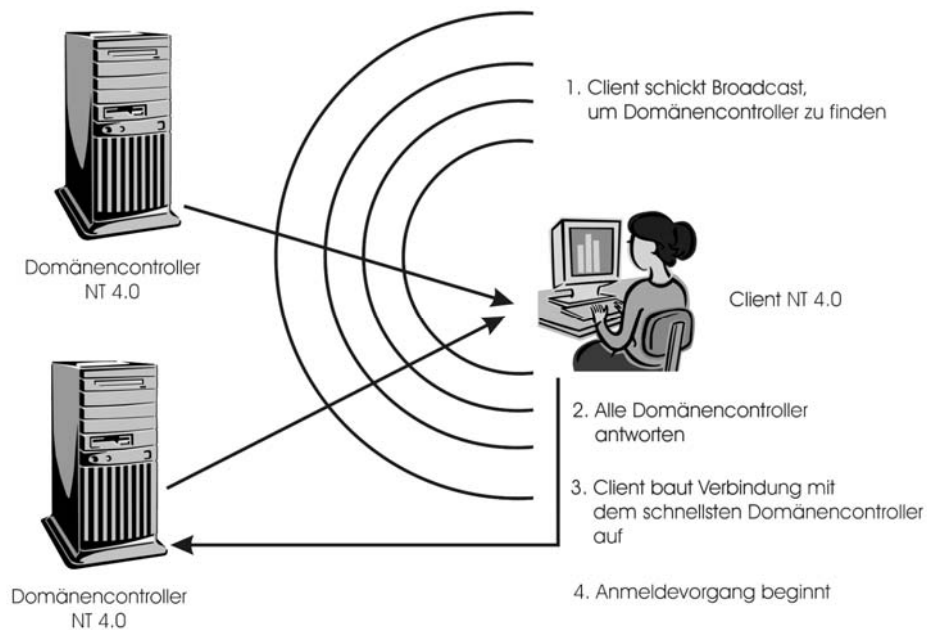


Abbildung 2.1: Anmeldevorgang in einer NT 4.0 Domäne

Dieser Vorgang ist zwar einfach, aber weder effizient, noch sicher.

Aus diesem Grund haben die Entwickler von Microsoft für den Anmeldevorgang ein völlig neues Konzept vorgestellt.

2.2.2 Der Anmeldevorgang an einer Windows 2000 oder Windows Server 2003 Domäne

Das größte Problem beim Anmeldevorgang unter Windows NT war, dass die Kommunikation mit einem Broadcast eingeleitet worden ist. Dies belastet das Netzwerk und bietet außerdem eine Angriffsfläche für „Sniffer“.

Es musste also eine Lösung gefunden werden, die ohne Broadcast arbeitet.

Hierfür gibt es einige Lösungsansätze

- Der Client muss eine Liste mit allen Domänencontrollern haben
- Der Client muss beim Systemstart Kontakt mit einer Stelle aufnehmen, die diese Informationen beinhaltet.

Die erste Lösung ist nicht praktikabel, es müsste eine Liste auf jedem Client und jedem Mitgliedserver geführt und gepflegt werden, was ein zu hoher Arbeitsaufwand wäre.

Aber die zweite Möglichkeit ist eine sehr gute Möglichkeit, um den Clients Informationen zukommen zu lassen.

Machen wir einmal ein Gedankenexperiment:

Welche Informationen über das Netzwerk stehen dem Client beim Systemstart bereits zur Verfügung?

Das ist einfach, der Client hat beim Systemstart bereits alle Informationen, die in seiner IP-Konfiguration eingetragen sind. Dies sind

- IP-Adresse
- Subnetzmaske
- Eventuell Standardgateway
- Server für die Namensauflösung

Jeder Client hat einen Namensserver eingetragen, die älteren NetBIOS Rechner haben einen WINS-Server, die neuen HOST-Rechner haben einen DNS-Server.

Also ist bei allen Clients ab Windows 2000 der DNS-Server in der IP-Konfiguration enthalten.

Das ist der Ansatzpunkt, den die Entwickler von Microsoft benutzt haben.

Es wäre doch optimal, wenn der Client beim Systemstart keinen Broadcast senden würde, sondern gezielt den DNS-Server fragen könnte, welche Domänencontroller für ihn zur Verfügung stehen, um dann eine direkte Verbindung per Unicast mit einem Domänencontroller aufzubauen.

Genau diese Funktion ist in alle Rechner ab Windows 2000 eingebaut.

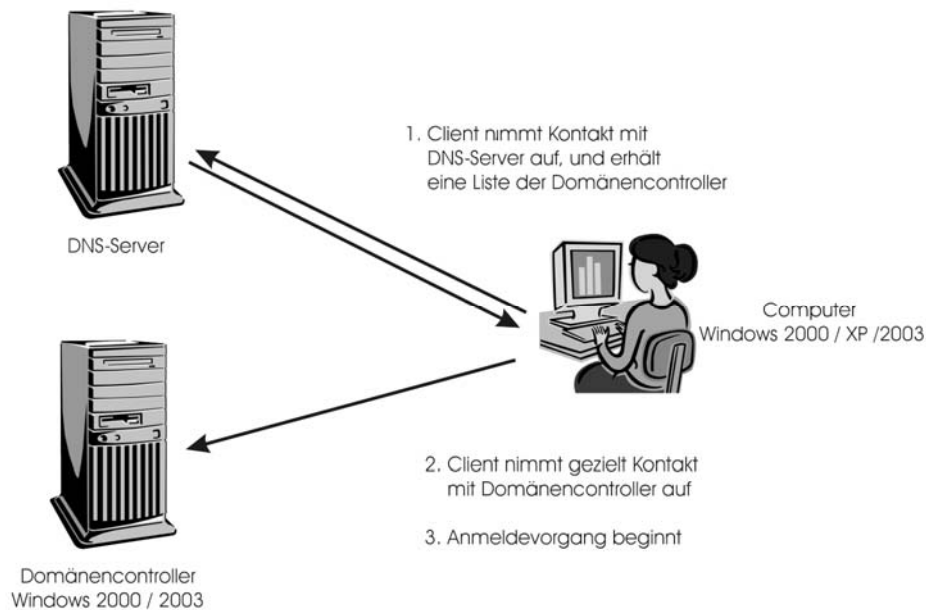


Abbildung 2.2: Anmeldevorgang in einer Windows 2000 / 2003 Domäne

Nun stellt sich nur eine Frage: Wie erhält der DNS-Server die Einträge?

2.2.3 Hinzufügen der Einträge in den DNS-Server

Dies ist eine weitere Funktion eines Domänencontrollers unter Windows 2000 / 2003.

Bei der Installation eines Domänencontrollers wird bereits der DNS-Server zwingend vorausgesetzt.

Dies hat den Grund, dass der Domänencontroller bereits bei der Installation bestimmte Einträge in den DNS-Server setzt.

Er erstellt so genannte „SRV-Einträge“. Dies sind Dienstidentifizierungen, mit denen bestimmte Dienste im DNS-Server eingetragen werden können.

ACHTUNG!

Solche Diensteeinträge gibt es schon lange, dies ist keine Erfindung für das Active Directory! Auch in anderen Umfeldern wird mit SRV-Einträgen gearbeitet.

Nun stellt sich die Frage, welche Dienste für die Identifikation eines Domänencontrollers relevant sind. Hier gibt es eigentlich nur zwei verschiedene Dienste zu nennen:

- Kerberos – Dienst für die Anmeldung
- LDAP – Dienst für die Abfrage des Verzeichnisdienstes

Wenn also ein Client einen Domänencontroller für die Anmeldung sucht, muss er eigentlich nur abfragen, auf welchem Computer der Dienst „Kerberos“ läuft.

Genauso ist es, wenn ein bereits angemeldeter Client eine weitere Abfrage des Verzeichnisdienstes vornehmen möchte. In diesem Fall muss er ebenfalls einen Domänencontroller finden, sucht aber diesmal nach einem anderen Dienst, nämlich LDAP.

Wenn Sie einen DNS-Server betrachten, der ein Active Directory verwaltet, werden Sie einige Einträge finden, die in einem „normalen“ DNS-Server nicht vorhanden sind:

_msdcs

_sites

_tcp

_udp

Dies sind die Einträge, die Active Directory bei der Installation hinzugefügt hat.

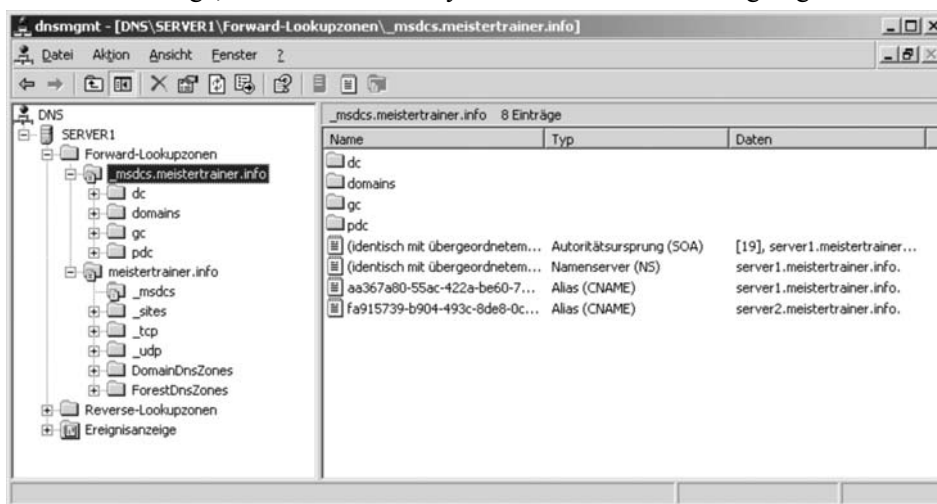


Abbildung 2.3: DNS-Server mit SRV-Einträgen

Der wichtigste neue Eintrag ist „_msdcs“.

Wenn Sie diesen Eintrag genauer betrachten, fällt Ihnen sicher auf, dass er in der Forward-Lookupzone delegiert ist.

Öffnen Sie _msdcs.

Hier sind alle relevanten Einträge vorhanden, nach denen ein Client suchen könnte.

- dc (Domänencontroller)
- domains (Domänen, die in der Gesamtstruktur vorhanden sind)
- gc (Globale Katalogserver)
- pdc (PDC-Emulator)

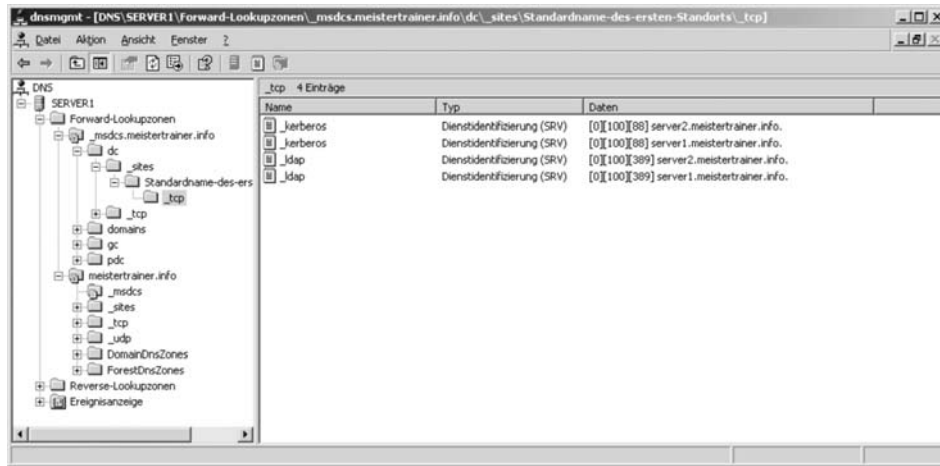


Abbildung 2.4: DNS-Server

Betrachten Sie die Einträge bei „dc“. Wenn Sie diesen Unterpunkt völlig öffnen, erkennen Sie die Einträge der Dienste.

_kerberos

_ldap

Die Computer, die diese Dienste verwalten, sind hier angegeben.

2.2.4 Troubleshooting

Leider kommen manchmal auch bei dieser Funktion Fehler vor. Sie sollten wissen, dass sich Clients nicht an der Domäne anmelden können, wenn die SRV-Einträge nicht vorhanden sind. In diesem Fall erwarten die Clients eine Liste mit Domänencontrollern, erhalten diese aber nicht.

Aus diesem Grund sollten Sie sofort die SRV-Einträge untersuchen, falls eine Verbindung mit der Domäne nicht möglich ist. Überprüfen Sie, ob die SRV-Einträge aller Domänencontroller vorhanden sind. Falls Einträge fehlen, müssen Sie dafür sorgen, dass dies schnell nachgeholt wird.

ACHTUNG!

Die Domänencontroller selber nehmen die Einträge im DNS-Server vor, um es genauer zu sagen, nimmt der „Anmeldedienst“ auf den Domänencontrollern den Eintrag vor.

Sollten also Einträge eines bestimmten Domänencontrollers im DNS-Server fehlen, starten Sie auf diesem Domänencontroller den Anmeldedienst neu, und kontrollieren Sie danach erneut die Einträge!

Leider gilt diese komfortable und sichere Kontaktaufnahme mit dem Domänencontroller nur für Clients, die mindestens Windows 2000 als Betriebssystem benutzen. Ältere Clients nehmen immer noch über Broadcast Kontakt mit einem Domänencontroller auf.

Aus diesem Grund ist es eine Überlegung wert, sich von den älteren Clients zu trennen, und auf die moderneren und sicheren Windows 2000 oder XP Clients zu wechseln.

2.3 Besonderheiten des Anmeldevorgangs

Der Anmeldevorgang in einer Active Directory Domäne wird normalerweise mit dem Protokoll Kerberos durchgeführt.

Microsoft kennt zwei Arten der Authentifizierung:

- NTLM und NTLMv2
- Kerberos

Die Authentifizierung mit Kerberos wird in Domänen seit Windows 2000 eingesetzt. Domänen unter NT 4.0 dagegen authentifizieren mit NTLMv2.

Domänen unter Windows Server 2003 können mit beiden Authentifizierungsprotokollen arbeiten, Computer, die Kerberos unterstützen, können mit Kerberos authentifiziert werden, die älteren Clients werden mit NTLM authentifiziert.

ACHTUNG!

Nur Clients mit Windows 2000, Windows XP und Server unter Windows 2000 und Windows Server 2003 unterstützen die Kerberos-Authentifizierung. Ältere Clients können sich nur mit NTLM oder NTLMv2 authentifizieren. Wenn Sie eine vollständige Kerberos-Authentifizierung wünschen, müssen Sie alle älteren Rechner ersetzen!

Damit eine Kerberos-Authentifizierung funktionieren kann, müssen folgende Voraussetzungen erfüllt sein:

- Das Benutzerkonto befindet sich in einer Windows 2000 oder Windows Server 2003 Domäne
- Der Client benutzt Windows 2000 oder Windows XP als Betriebssystem
- Das Computerkonto ist in der Domäne angelegt

- Computerkonto und Benutzerkonto sind in derselben Gesamtstruktur

Bei jeder anderen Kombination wird eine Authentifizierung über NTLM oder NTLMv2 ausgeführt!

Die Protokolle:

NTLM (NTLMv2)	Kerberos
Ein Authentifizierungsdienst auf einem Domänencontroller muss kontaktiert werden, dabei werden die Anmeldeinformationen über das Netzwerk gesendet	Bei einer Kerberos-Authentifizierung müssen die Anmeldeinformationen nicht über das Netzwerk gesendet werden. Der Client erhält ein „Ticket“, mit dem er sich authentifizieren kann

Tabelle 2.1: NTLM und Kerberos

Die Anmeldung an der Domäne mit Kerberos erfolgt in folgenden Schritten:

1. Wie bei der lokalen Anmeldung übergibt Winlogon die Informationen an die Local Security Authority (LSA).
2. Die LSA nimmt Kontakt zu einem Domänencontroller auf. Der KDC vergibt ein Sitzungsticket (*TGT – Ticket Granting Ticket*) für die Kommunikation. Dieses TGT wird für jede weitere Kommunikation mit dem KDC benötigt.
3. Nun wird der Domänencontroller um Verifizierung des Benutzers angefragt. Der DC schickt die eindeutige SID des Benutzers zurück, sowie alle SID aller Gruppen, in denen der Benutzer Mitglied ist.
4. Die LSA fordert vom Domänencontroller ein weiteres Ticket an, damit der Benutzer Zugriff auf den Arbeitsstationsdienst bekommt. Das Sitzungsticket authentifiziert hierbei den Benutzer.
5. Bei erfolgreicher Verifizierung des Sitzungstickets erstellt der KDC das gewünschte Arbeitsstationsticket und schickt es an den Client zurück.
6. Die LSA erstellt einen eigenen Schlüssel, das sogenannte Zugriffstoken. Mit diesem Token kann der Benutzer nun Zugriff auf alle Ressourcen bekommen, für die er Berechtigungen hat.
7. Der Desktop des Clients erscheint.

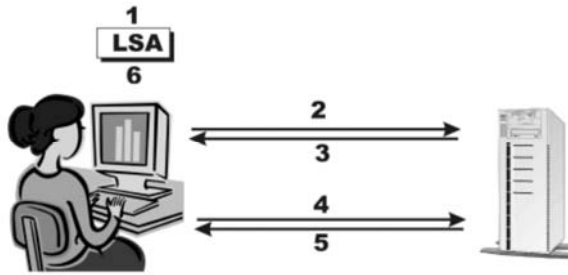


Abbildung 2.5: : Prinzip von Kerberos

2.3.1 Anmelden mit dem UPN (User Principal Name)

In einer Active Directory Gesamtstruktur ist es möglich, sich mit einem so genannten UPN anzumelden.

Der UPN wird beim Anlegen von Benutzerkonten generiert. Normalerweise ist er folgendermaßen aufgebaut:

Anmeldename@Domäne

Das Screenshot zeigt das Dialogfenster 'Neues Objekt - Benutzer' in Active Directory. Es enthält folgende Felder:

- Erstellen in: Meistertrainer.info/Users
- Distinguished Name
- Vorname: Hans, Initialen: (leer)
- Nachname: Test
- Vollständiger Name: Hans Test
- Benutzeranmeldename: HT | UPN | @Meistertrainer.info
- Benutzeranmeldename (Für Windows 2000): MEISTERTRAINER\ | HT | SAMID

Die Felder 'Distinguished Name', 'Benutzeranmeldename' und 'Benutzeranmeldename (Für Windows 2000)' sind mit roten Kreisen hervorgehoben.

Abbildung 2.6: UPN

Eine schöne Möglichkeit für eine sichere Anmeldung ist es, sich mit dem UPN anzumelden. Wenn Sie dies tun, wird in dem Moment, in dem Sie das „@“ tippen, die dritte Zeile des Anmeldebildschirms ausgeblendet. Damit können Sie also die Domäne nicht mehr wählen, die Domänenzugehörigkeit ist also mit Eingabe des UPN festgelegt.



Abbildung 2.7: Anmeldung mit dem UPN

Es ergibt sich hier natürlich eine besondere Sorgfaltspflicht. Wenn Sie eine Anmeldung mit dem UPN vornehmen möchten, müssen Sie natürlich darauf achten, dass der Benutzeranmeldename eindeutig sein muss. Sie können natürlich die e-Mailnamen benutzen, die im Unternehmen benutzt werden, denn auch diese müssen eindeutig sein.

ACHTUNG!

Ein großer Vorteil der Anmeldung mit dem UPN ist, dass eine Anmeldung mit dem e-Mailnamen möglich ist. Dadurch müssen sich die Benutzer nur einen Namen merken, und nicht e-Mailnamen und zusätzlich einen Benutzeranmeldenenamen.

Aus diesen Vorteilen ergibt sich aber auch eine Problematik.

Wenn Sie eine Gesamtstruktur mit mehreren Domänen haben, oder Sie haben mehrere Firmen fusioniert, existieren in Ihrem Unternehmen mehrere „UPN-Suffixe“, nämlich mehrere Namen nach dem „@“.

Windows Server 2003 bietet dafür eine Lösung. Sie können zusätzliche UPN-Suffixe definieren, die dann in der Gesamtstruktur zur Verfügung stehen. Dann können Sie in jeder Domäne die entsprechenden UPN-Suffixe frei wählen.

Erstellen können Sie zusätzliche UPN-Suffixe in der Konsole „Active Directory Domänen und Vertrauensstellungen“.

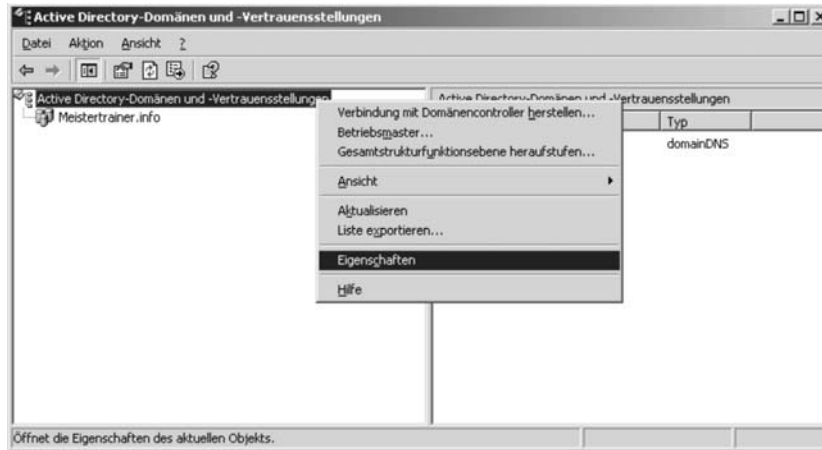


Abbildung 2.8: Zusätzliches UPN-Suffix erstellen

Wählen Sie die Eigenschaften von „Active Directory Domänen und Vertrauensstellungen“.



Abbildung 2.9: UPN-Suffix

ACHTUNG!

Ein zusätzliches UPN-Suffix können Sie nicht auf der Ebene einer Domäne erstellen, sondern nur auf Ebene der Gesamtstruktur, da dieses UPN-Suffix auch für alle Domänen in der Gesamtstruktur gelten soll. Aus diesem Grund müssen Sie die Eigenschaften von „Active Directory Domänen und Vertrauensstellungen“ wählen.

Sie gelangen nun direkt in das Fenster, in dem Sie zusätzliche UPN-Suffixe generieren können.

Erstellen Sie hier alle UPN-Suffixe, die Sie benötigen.

Wenn Sie nun einen neuen Benutzer anlegen möchten, können Sie beim Benutzeranmeldenamen ein UPN-Suffix anlegen.

The screenshot shows a Windows dialog box titled "Neues Objekt - Benutzer". At the top, it says "Erstellen in: Meistertrainer.info/Users". Below this are several input fields: "Vorname:" with "Hans", "Initialen:" (empty), "Nachname:" with "Dampf", and "Vollständiger Name:" with "Hans Dampf". There are two rows for "Benutzeranmeldename": the first row has "HD" and a dropdown menu showing "@Meistertrainer.info" (selected), "@superlearner.local", and "@Meistertrainer.info"; the second row has "MEISTERTRAINER\" and "HD". At the bottom are three buttons: "< Zurück", "Weiter >", and "Abbrechen".

Abbildung 2.10: UPN aussuchen

2.4 Vertrauensstellungen

Vertrauensstellungen sind Verbindungen, die einen Zugriff auf die Ressourcen einer anderen Domäne prinzipiell ermöglichen.

Es gibt mehrere Arten von Vertrauensstellungen, die je nach Anforderungen eingesetzt werden können.