LRP Landesbank Rheinland-Pfalz

Ein Unternehmen der LBBW-Gruppe

1A08

OpenVMS in einer Windows Active Directory Domäne

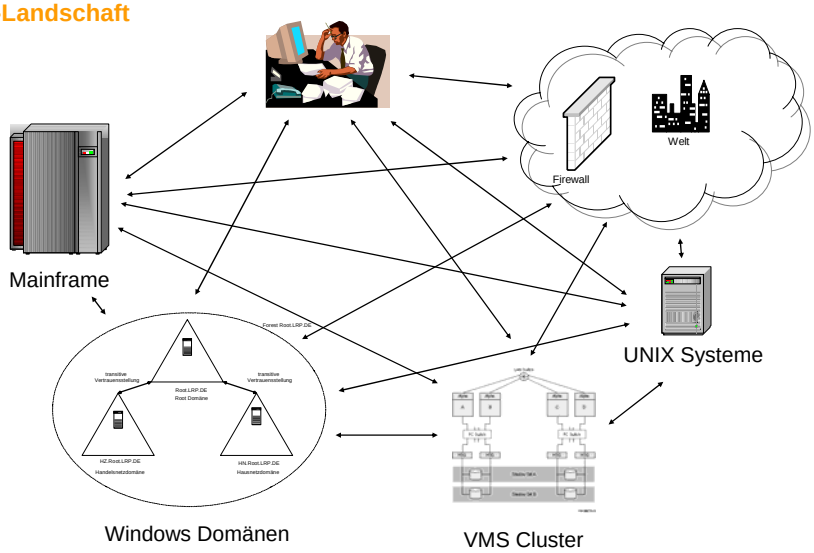
Detlef Buerdorff, Landesbank Rheinland-Pfalz

LRP Landesbank Rheinland-Pfalz

Ein Unternehmen der LBBW-Gruppe

Ausgangssituation

IT-Landschaft



Ausgangssituation

Anwendersicht

- verschiedene Terminals, GUIs und Workstations
- mehrere Logins

Ausgangssituation

Systemsicht

Aufgabenstellung:

- Datenaustausch
- Programm zu Programm Kommunikation

Nativ stehen für die Lösung dieser Aufgabe Netzwerkprotokolle zur Verfügung:

- NetBEUI / LAN-Manager
- IPX/SPX
- TCP/IP
- DNA
- SNA
- etc.

Frühere Lösungsansätze

Zum Beispiel

Anwender:

- **Bereitstellung nur eines Benutzerinterfaces z.B. X-Windows**

Systeme:

- **Nutzung von Gateways**

Weitere Entwicklung

Zum Beispiel

Anwender:

- **Nutzung von MS NT Workstations**

Systeme:

- **Allgemeine Bereitstellung eines TCP/IP Stacks**
- **Weltweit verteilte Systeme und Anwendungen (Distributed Computing Environment)**

Weitere Entwicklung

Neue Fragestellungen

- Wo finde ich was?
  - Lösung: Verzeichnisdienste, z.B. X.500
- Netzwerk-Security?
  Lösungsansätze z.B.:
  - Kerberos
  - SSL
  - IPSec

Begriffsklärung

Verzeichnisdienst (Directory Service)

- In einer verteilten Datenverarbeitung (DC „Distributed Computing“, auch „Distributed Processing“ – Eine Form der Datenverarbeitung, bei der die Rechenarbeit von mehreren Computer ausgeführt wird. -) stellt sich immer wieder die Frage, wo und wie finde ich was?
- Ein Verzeichnisdienst (so was wie ein Telefonbuch) soll hier Abhilfe verschaffen

Verzeichnisdienst

Eigenschaften

- Auf ein Verzeichnis wird oft lesend und eher selten schreibend zugegriffen.
- Ein Verzeichnis organisiert seine Daten in einer baumartigen Hierarchie, dem Verzeichnisbaum (DIT).
- Teilbereiche des Verzeichnisbaumes können auf verschiedene Hosts verteilt sein.
- Die Administration von Teilbereichen des Verzeichnisbaumes kann einfach delegiert werden.
- Der Verzeichnisbaum ermöglicht es, Suchoperationen von vornherein auf interessante Teilbäume zu beschränken.
- Viele Verzeichnisdienste basieren auf dem X.500-Modell und unterstützen damit von vornherein ein objektorientiertes Datenmodell.

Verzeichnisdienst

X.500 <-> LDAP

- Ab dem Jahre 1984 wurde das X.500 Verzeichnisdienst entwickelt.
- X.500 basiert auf dem OSI-Modell und das Protokoll DAP (Directory Access Protocol) benutzt intensiv die OSI Transportschicht.
- Mitte der 90‘er setzte sich flächendeckend immer mehr TCP/IP V4 durch, weil dieses Protokoll sehr viel einfacher ist als OSI.
- Aber auch TCP/IP Netze benötigen einen Verzeichnisdienst, aber wie soll man auf X.500 vernüftig zugreifen können?
- => Entwicklung vom LDAP „Lightweight Directory Access Protocol“. Zunächst mehr als Middleware gedacht, als ein echtes Verzeichnisdienst.

Verzeichnisdienst

X.500 <-> LDAP

- **Für den wachsenden Erfolg von LDAP ist aber auch ein Paradigmenwechsel mitverantwortlich, durch den sich die Einsatzgebiete dieses Protokolls verlagern, und zwar weg von einer Middleware, die zwischen TCP/IP und X.500 vermittelt, hin zu einer Serversoftware die LDAP-fähigen Clients den Zugriff auf eine fast beliebige Datenbasis vermittelt.**

Begriffsklärung

SSL und SSH

- **SSL S**ecure **S**ocket **L**ayer und **SSH S**ecure **Sh**ell stellen eine sichere Kommunikation über IP-Netzwerke von Host zu Host zur Verfügung.
- **SSH** wurde mit Blick auf Remote-Log-in, File-Transfer und Remote-Execution entwickelt.
- **SSL** wurde für eine Sicherung von Verbindungen auf HTTP-Basis im Web entwickelt.
- Die Protokolle gewährleisten **Vertraulichkeit, Authentizität** und **Integrität.**
- **Datenverschlüsselung** erfolgt mit dem **Public-Key-Verfahren**
- Keine Vererbung und Delegation möglich.

Begriffsklärung

Kerberos

- **Sichere Prüfung der Identität** eines Benutzers **(Authentifizierung)** in einem ungesicherten TCP/IP Netzwerk aus sicheren Hostrechnern.
- **Die Authentisierung übernimmt eine ,,vertrauenswürdige dritte Partei"**. Diese dritte Partei ist ein besonders geschützter Kerberos 5 Netzwerkdienst.
- Durch Kerberos werden insbesondere Angriffe durch passives ,,Sniffing" unterbunden, aber auch ,,Spoofing", ,,Dictionary Attacks", ,,Replay" und andere Angriffe werden erschwert.
- Das System überprüft weder die Berechtigungen der Benutzer (Autorisierung), noch verfolgt es die durchgeführten Aktionen (Audit).
- **Datenverschlüsselung** erfolgt mit dem **Shared-Key-Verfahren** (weniger sicher als das Public-Key-Verfahren)
  .
- Erlaubt **Vererbung** und **Delegation**

Begriffsklärung

IPSec

- Stellt eine **Sicherheitsarchitektur** für die Kommunikation über IP-Netzwerke zur Verfügung.
- Das Protokoll soll **Vertraulichkeit, Authentizität und Integrität** gewährleisten**.**
- Daneben soll es vor so genannten Replay-Angriffen schützen - das heißt, ein Angreifer kann nicht durch Abspielen eines vorher mitgeschnittenen Dialogs die Gegenstelle zu einer wiederholten Aktion verleiten.

Lösungsansatz bei OpenVMS

- Verzeichnisdienst
  - X.500
- Netzwerk-Security
  - SSL und SSH

Lösungsansatz vom Microsoft

- Verzeichnisdienst
  - Active Directory (LDAP basierend) mit MS Erweiterungen
- Netzwerk-Security
  - Kerberos mit MS Erweiterungen, wie z.B. die Benutzung von Public-Keys (smart cards)
  - IPSec

OpenVMS im AD

Was möchte ich erreichen?

- **Integration in ein bestehendes Windows 2003 AD**
- **Die Sicherheit, Zuverlässigkeit, Einfachheit und sehr gute Multi-Site-Cluster Funktionalität eines VMS Clusters als NT-Fileserver mit nutzen.**
- **Kritische Applikationen, bzw. Teile davon, auf dem OpenVMS Cluster laufen lassen.**
- **Die Kommunikation zwischen OpenVMS und den AD Memberservern sowie den Clients soll sicher sein.**
- **Die Sicherheit von OpenVMS nicht verringern.**

OpenVMS im AD

Wie möchte ich dies erreichen?

- **Die vorhandenen Funktionen und Anwendungen eines Windows 2003 AD und eines OpenVMS 8.2 Clusters nutzen.**

Welche Randbedingungen sind gegeben?

- **Die Merkmale Vererbung und Delegation sind in einer Windows Domäne sinnvoll. Das Betreiben einer solchen Domäne sollte möglichst einfach sein. => LDAP, Kerberos und IPSec mit MS Erweiterungen (offen gelegt?) kommen zum Einsatz.**
- **OpenVMS ist in der OSI-Welt Zuhause und hatte immer einen wesentlichen Blick auf Security => X.500, SSL und SSH sind zum Einsatz gekommen. KerberosV steht mit 8.2 zur Verfügung und IPSec wird kommen.**
- **Marketinggesichtspunkte von MS und HP**

OpenVMS im AD

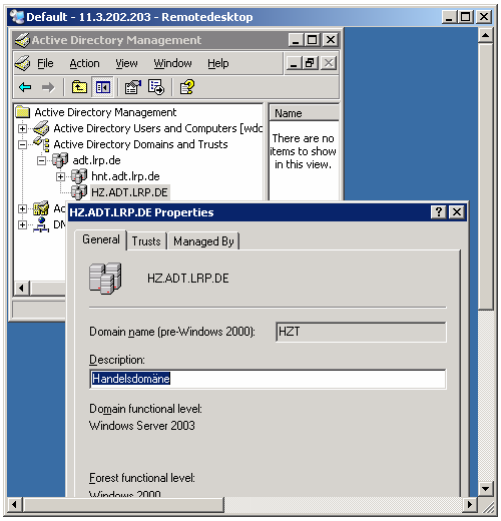
Was bedeutet dies?

- Nicht alles was man von Windows her kennt, wird unterstützt.
- Standards fliesen unterschiedlich schnell und gut in die Betriebssysteme ein.
- Plug and Play zwischen OpenVMS und Windows wird es wohl nicht (so schnell) geben.
- Am einfachsten wird es sein, wenn wir uns von OpenVMS aus dem AD annähern

OpenVMS im AD

File- und Print-Service mit dem Advanced Server

- Kann als Member Server in einer reinen Windows 2000 Domäne fungieren.
- Nutzt allerdings MSV1_0 mit dem Authentifizierungs-protokoll NTLMv2 (verhält sich wie ein Windows NT4 SP4 Member Server)
- Siehe Vortrag 1A07



OpenVMS im AD

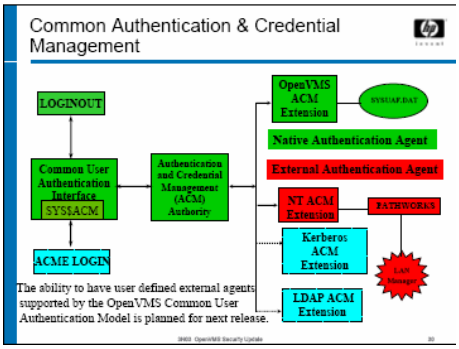
File- und Print-Service mit dem Advanced Server

- Per Default findet eine Zuordnung aller NT User Accounts zum OpenVMS Account PWRK$Default statt.
- Das Mappimg kann gesteuert werden, sprich einem NT Account kann genau einem OpenVMS Account zugeordnet werden.
- External Authentication ist möglich: Die Passwörter zwischen dem NT user und dem OpenVMS Account werden automatisch abgeglichen.
- Ermöglich wird obiges durch das Subsystem ACME (Authentication & Credential Management Extension)

OpenVMS im AD

ACME

- ACME (Authentication Credential Management Extension) is the new authentication subsystem
- The concept of ACME is very similar to PAM (Pluggable Authentication Module) on Unix platforms, ACME has a proprietary architecture and programming interfaces.



- Weitergehende Informationen sind den Vorträgen von Helmut Ammer, HP zu entnehmen (1G03).
- Ein guter Artikel hierzu wurde auch im OpenVMS Technical Journal V4 - June 2004 veröffentlicht.

OpenVMS im AD

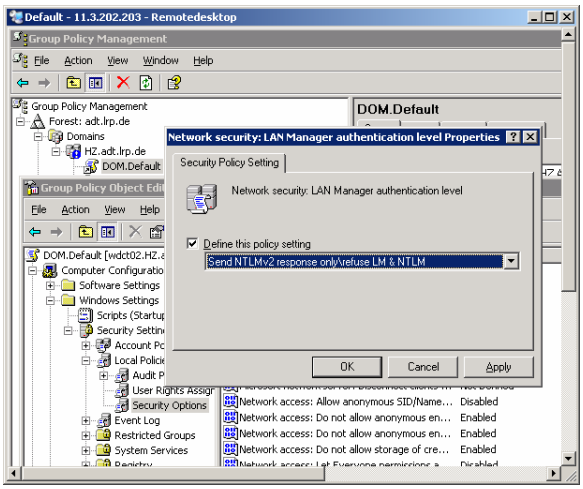
ACME Agents

- Der MSV1_0 ACME Agent ist Bestandteil vom Advanced Server und kann auch allein installiert werden.
- Weitere ACME Agenten können selbst entwickelt werden.
- Für Testzwecke gibt es einen LDAP ACME Agent, siehe SYS$HELP:ACME_DEV_README.TXT
- Mit dem LDAP ACME Agenten ist es nun möglich, das die Authentifizierung gegenüber einem LDAP Server, sprich dem AD, stattfinden kann.

OpenVMS im AD

File- und Print-Service mit dem Advanced Server

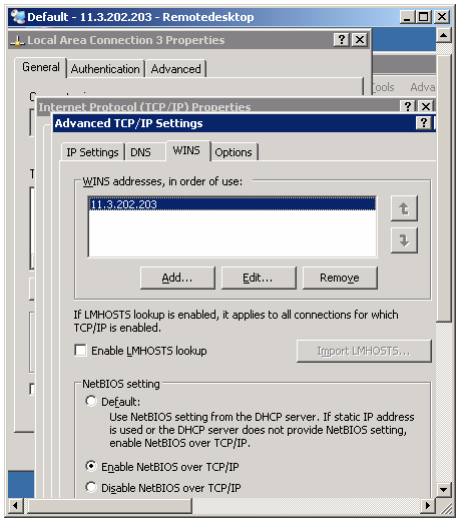
NTLMv2 Authentifizierung kann hoch gesetzt werden.



OpenVMS im AD

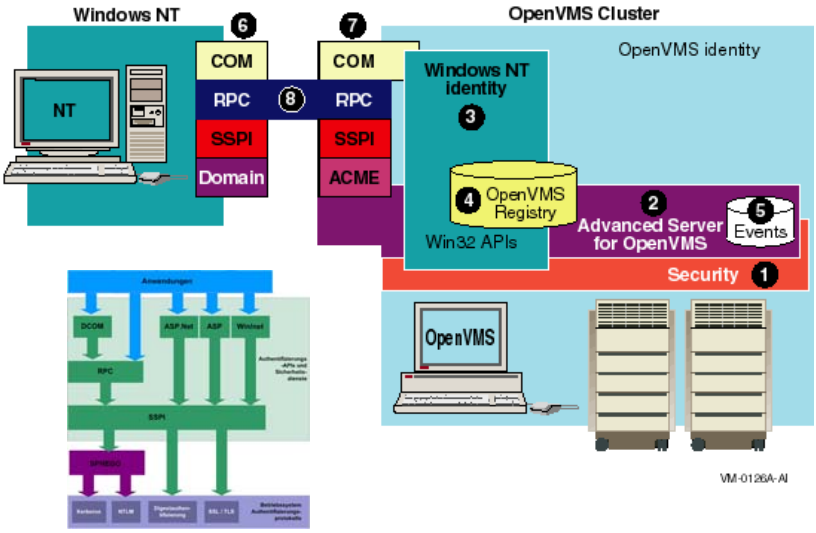
File- und Print-Service mit dem Advanced Server

NetBIOS Namen müssen erlaubt sein.

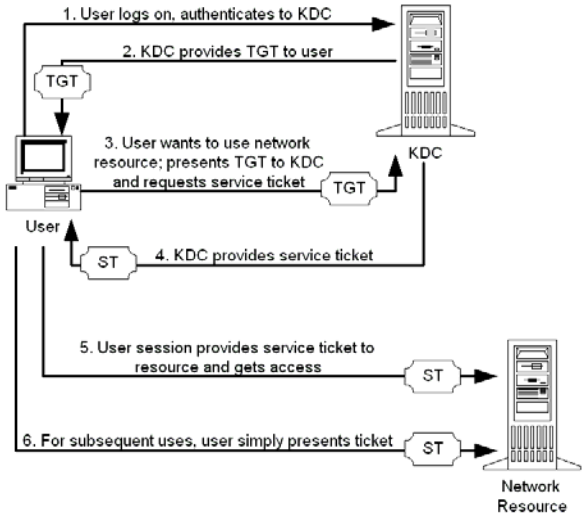


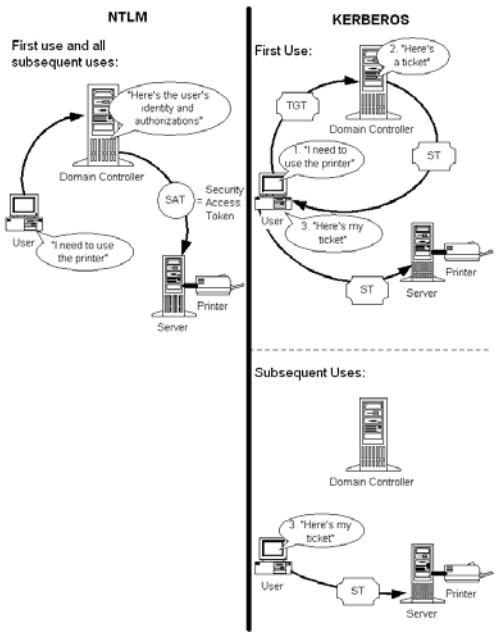
OpenVMS im AD

Verteilte Anwendungen mit COM



NTLM <-> Kerberos





Kerberos Begriffe

Principal:

Eindeutig bestimmter Nutzer, Client oder Server, der an einer Netzwerkkommunikation teilnimmt.

Session Key:

Ein Session Key ist ein temporärer Codierungsschlüssel der zwischen zwei Principals benutzt wird. Er ist nur diesen beiden bekannt und wird immer verschlüsselt versendet.

Secret Key :

Der Secret Key ist ein Codierungsschlüssel für die Kommunikation zwischen dem Kerberosdienst und einem Principal. Bei einem Benutzer besteht der Schlüssel aus dem Passwort, bei dem Server aus Zufallszahlen. Die Secret Keys müssen beim Kerberos-Dienst gespeichert sein, damit dieser chiffriert senden kann.

Kerberos Begriffe

Authentication Server

Der Authentication Server erteilt das TicketGranting Ticket (TGT). Mit diesem ist es dem Client möglich, sich am TicketGrantingService anzumelden.

TicketGrantingService (TGS)

Stellt dem Principal Tickets aus, die dem Client die Kommunikation mit dem Zielserver ermöglicht.

Key Distribution Center

Das Key Distribution Center (KDC) umfasst zwei Funktionen:

Den Authentication Server (AS) und den TicketGranting Service (TGS). Bevor ein Principal den TGS nutzen kann braucht es ein Ticket vom AS, nämlich das TGT.

Kerberos Begriffe

Realms

Kerberos benutzt einen Namensraum der in verschiedene Realms (Reiche) unterteilt ist.

Syntax

Es ist Konvention die Realms nach der Internet-Domäne in GROßBUCHSTABEN zu benennen.

Die Principal-Bezeichner setzen sich aus drei Namensteilen zusammen

primary/instance@REALM

z.B.

Benutzer **detlef@LRP.DE**

Dienst **ftp/pc.lrp.de@LRP.DE**

OpenVMS im AD

OpenVMS Kerberos

Kerberos ist integraler Bestandteil von OpenVMS 8.2.

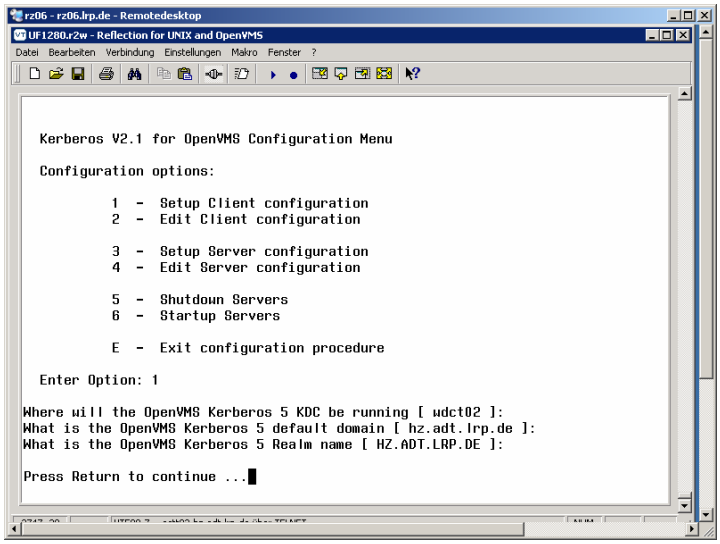
Somit können Client und Server Programme auf dem OpenVMS System ausgeführt werden, die sich im AD Realm authentifizieren bzw. den AD Tickets vertrauen.

Wie dies bewerkstelligt werden kann, siehe auch

Step-by-Step Guide to Kerberos 5 (krb5 1.0) Interoperability

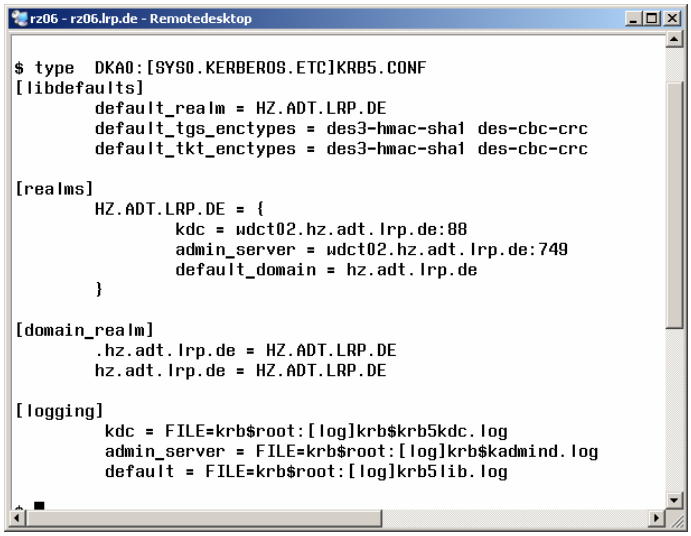
OpenVMS Kerberos

Client Konfiguration



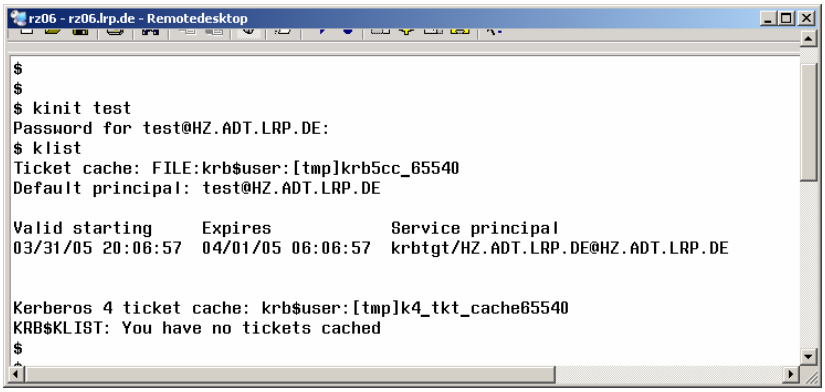
OpenVMS Kerberos

Client Konfiguration



OpenVMS Kerberos

Client Konfiguration



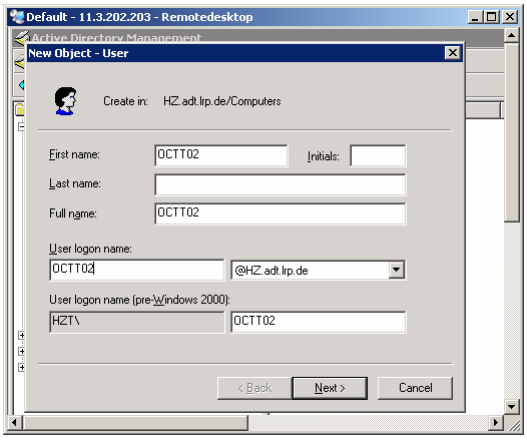
OpenVMS Kerberos

Host Konfiguration

Im AD einen User Account für den OpenVMS Host einrichten

Wohlgemerkt:
Einen User und keinen Computer!

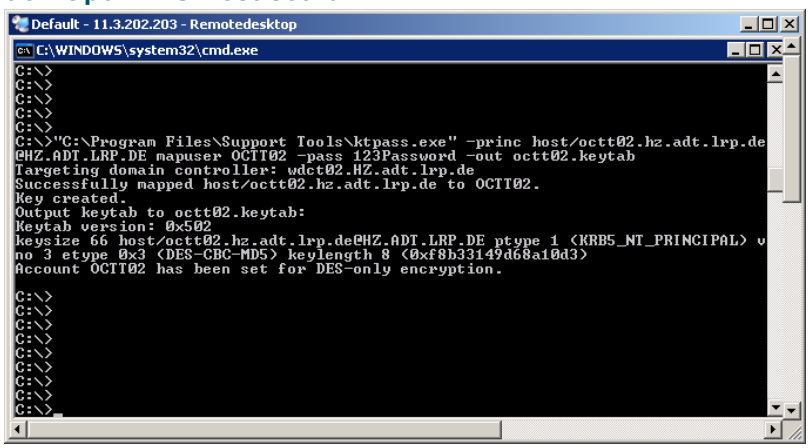
Den OpenVMS Host ebenfalls im DNS eintragen



OpenVMS Kerberos

Host Konfiguration

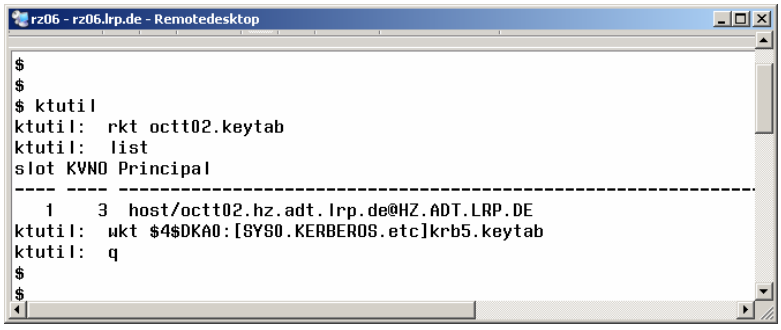
Mit Ktpass ein keytab file erzeugen und ein Passwort für den OpenVMS Host setzen.



OpenVMS Kerberos

Host Konfiguration

Keytab file auf den OpenVMS Host bringen und dem vorhanden krb5.keytab zusammenfügen.



OpenVMS in einem AD

Fragen ?