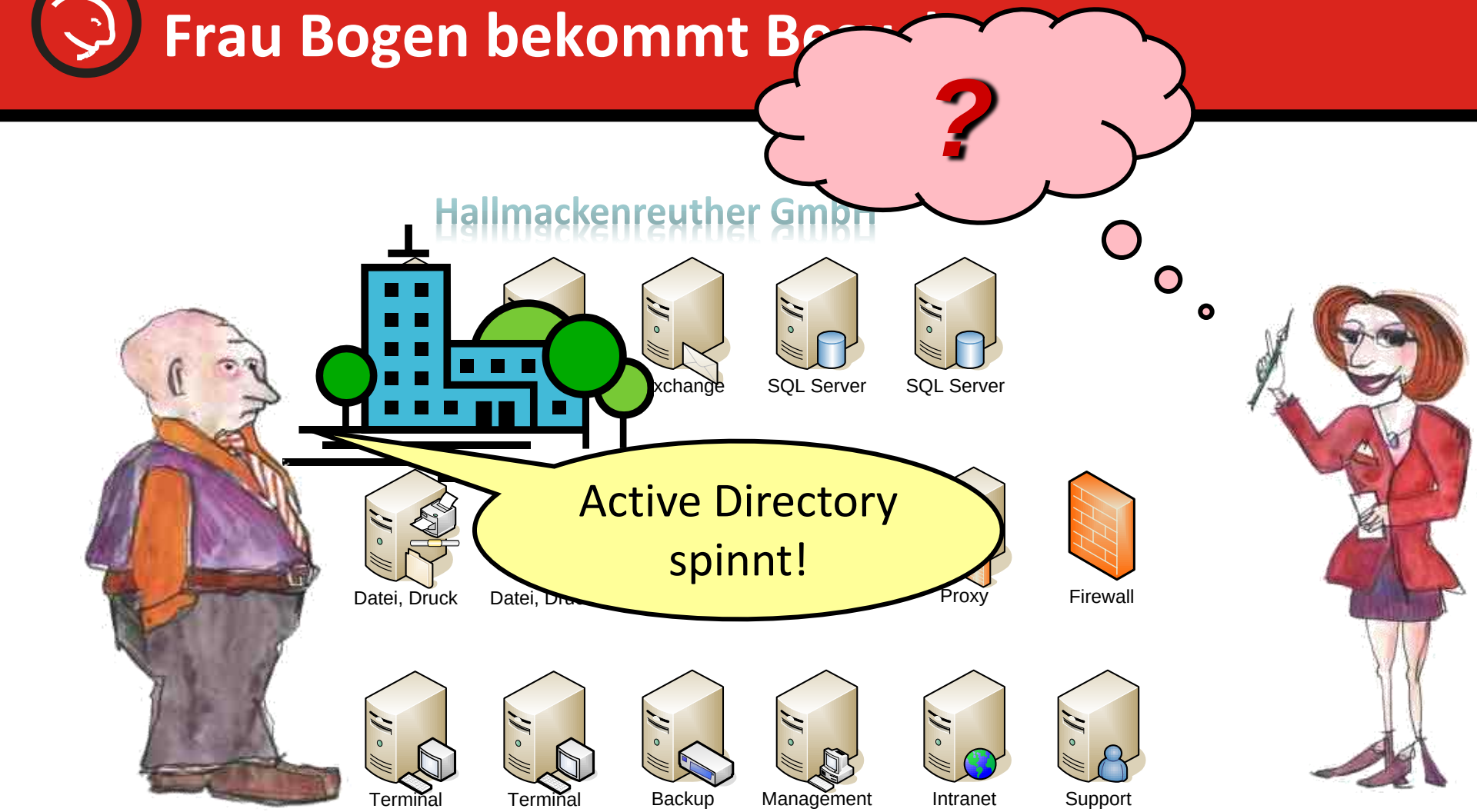
„Tu mir das nicht an“
sagte der Domänencontroller

Nils Kaczenski
MVP Directory Services
faq-o-matic.net

\\ice:lingen
intelligent communities for europe

Frau Bogen bekommt Be



FAQ-O-MATIC.NET

Wer zu Ihnen spricht

- Nils Kaczenski
- Leiter Consulting & Support WITstor Hannover
  - Windows, Exchange, Virtualisierung
  - Verfügbarkeit, Sicherheit
  - Strategische Beratung
  - Projektleitung
- Fachautor Windows
  - Microsoft Press
  - iX, c't, IT-Administrator
- Nils.Kaczenski@witstor.de

FAQ-O-MATIC.net

MVP Microsoft® Most Valuable Professional

Was euch erwartet

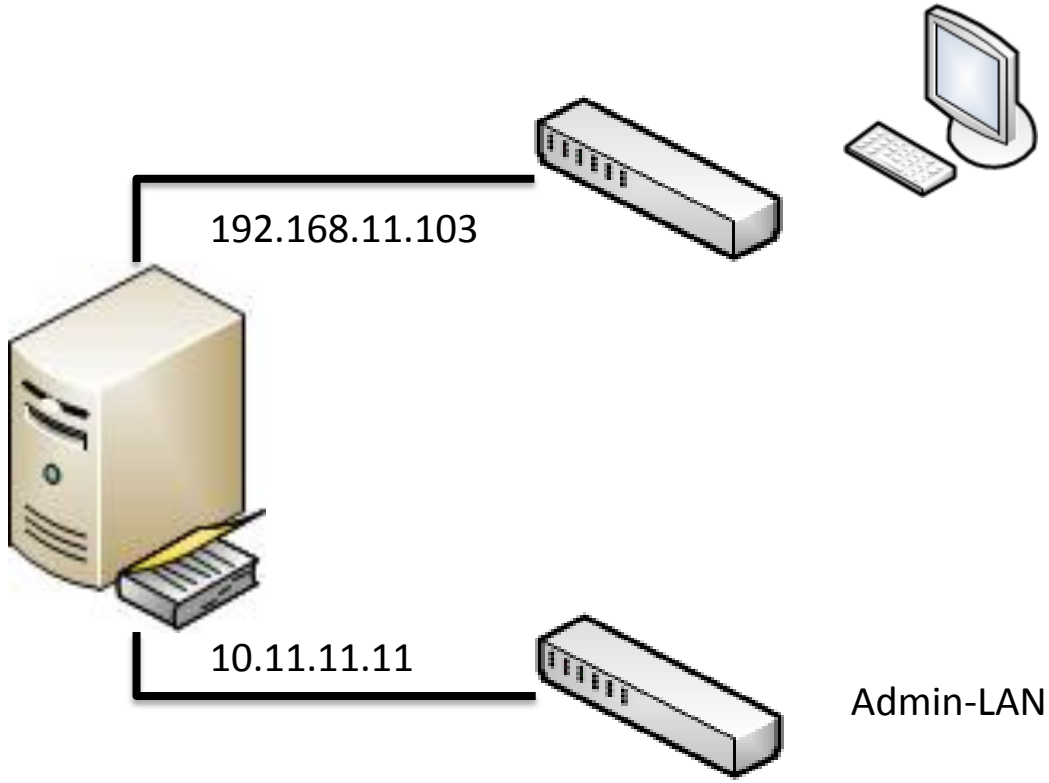
- Active Directory und DNS
- Replikation
- Virtuelle DCs
- Sicherheit
- Lieblingsfehler

Was euch erwartet

- Active Directory und DNS
- Replikation
- Virtuelle DCs
- Sicherheit
- Lieblingsfehler

DNS und AD: Der Multihomed DC

Name	Address
DC01	192.168.11.103
DC01	10.11.11.11



FAQ-O-MATIC.net

FaQ-o-maTiC.net

… anfassen!

DNS-Konfiguration

DNS-Fehler

- Falscher DNS-Server
- Keine DNS-Redundanz
- Multihomed DC
- DHCP-Client abschalten
- CNAME/Alias für den DC

Was euch erwartet

- Active Directory und DNS
- Replikation
- Virtuelle DCs
- Sicherheit
- Lieblingsfehler

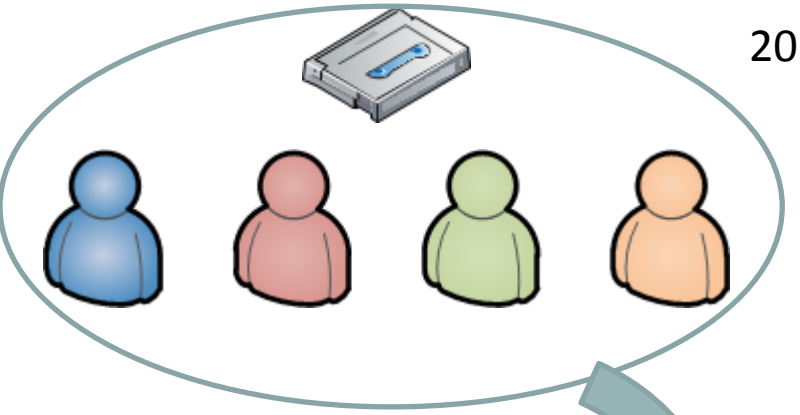
FAQ-O-MATIC.net

… anfassen!

Tombstone Lifetime

Lingering Objects

Herumlungernde Objekte



20. 06. 2011

User „Blau“
gelöscht am
21. Juni 2011

DC01

DC02

FAQ-O-MATIC.NET

Lingering Objects

- Gelöschte Objekte: Tombstone
- Nach Tombstone Lifetime:
  Jeder DC löscht das Objekt
- Restore eines zu alten Backup …
- … oder Replikationspause länger als
  Tombstone Lifetime …
- … führen zu Lingering Objects
- Abhilfe: repadmin /removelingeringobjects

FAQ-O-MATIC.net

Die Replikation höchstselbst

- Fehlendes oder falsches Standort-Konzept
  - Clients finden DCs nicht
  - Clients nutzen DC am anderen Ende der Welt
  - Replikation schlägt fehl
- Replikation abgeschaltet
  - Ursache oft: „Absicherung“ vor Schema-Update
  - Keine Replikation
  - Lingering Objects

FaQ-o-maTiC.net

… anfassen!

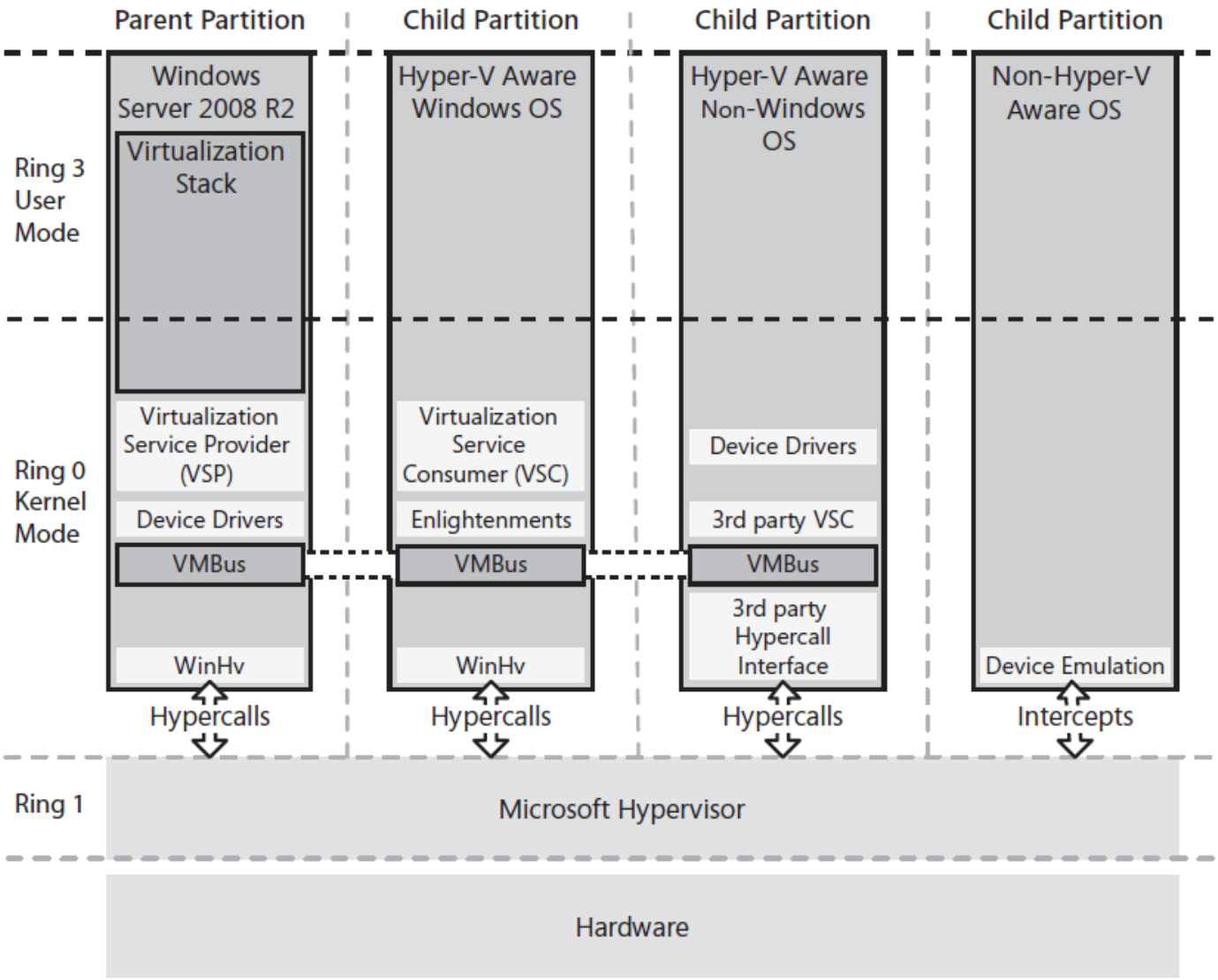
AD-Standorte

Replikation manipulieren

Was euch erwartet

- Active Directory und DNS
- Replikation
- Virtuelle DCs
- Sicherheit
- Lieblingsfehler

Lasst die Eltern in Ruhe!



VM-Snapshots

- Kann jeder Hypervisor
- Geht irre schnell
- Ist so ungemein praktisch
- … und zerstört Active Directory

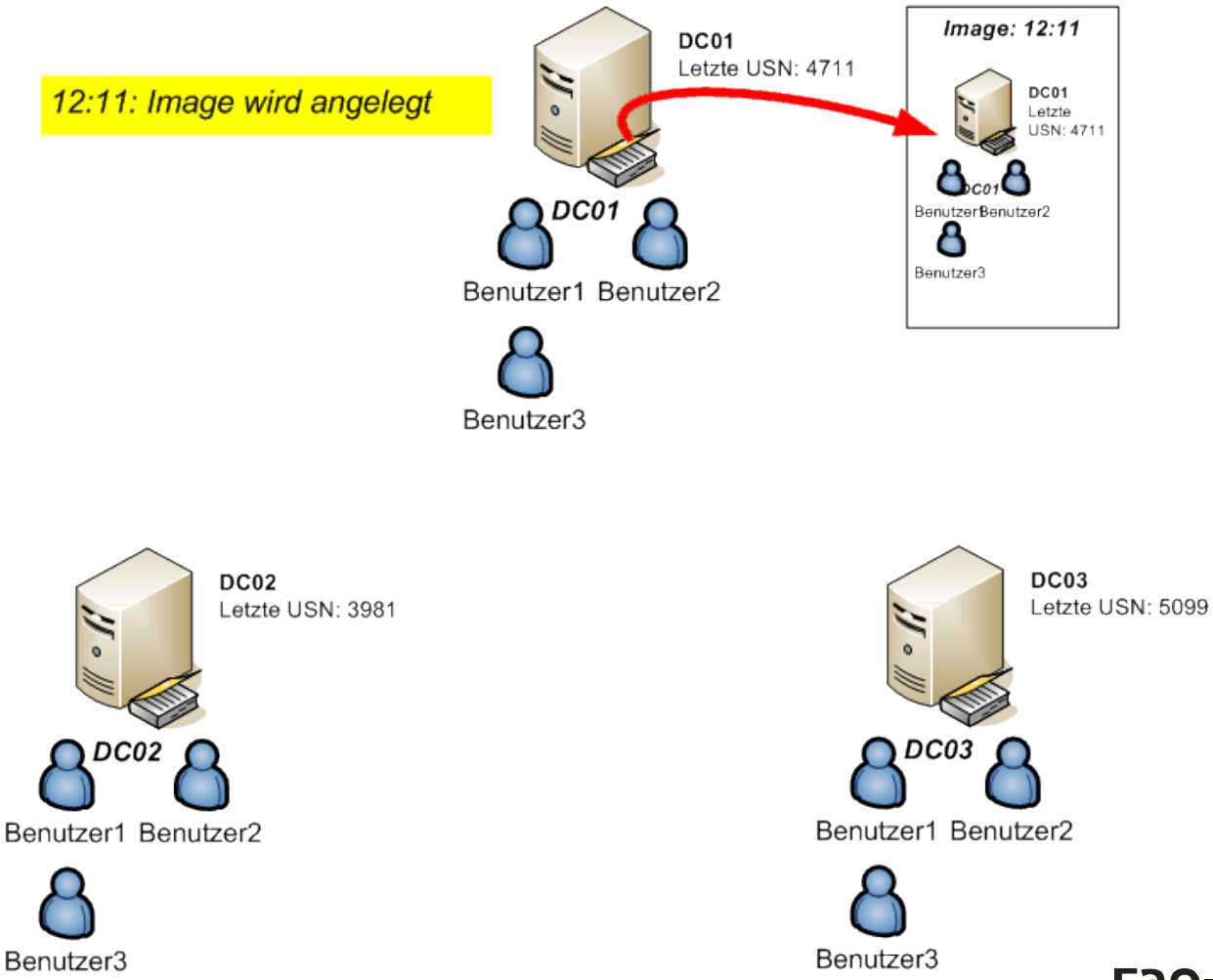
FAQ-O-MATIC.net

FaQ-o-maTiC.net

… anfassen!

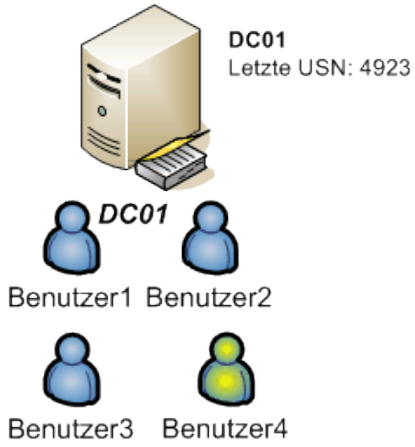
Snapshot-Rollback eines DC

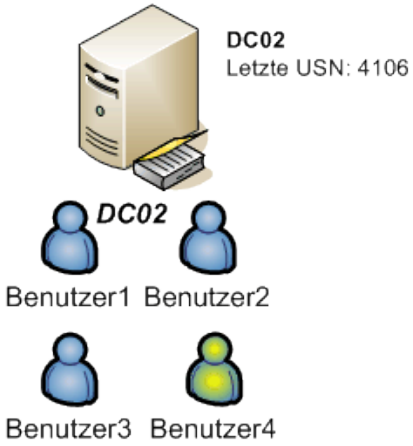
USN Rollback: Katastrophe statt Rettung

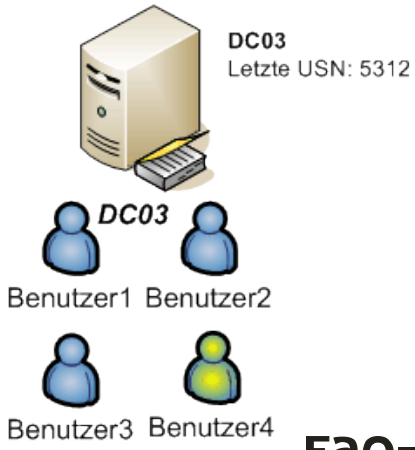


USN Rollback: Katastrophe statt Rettung

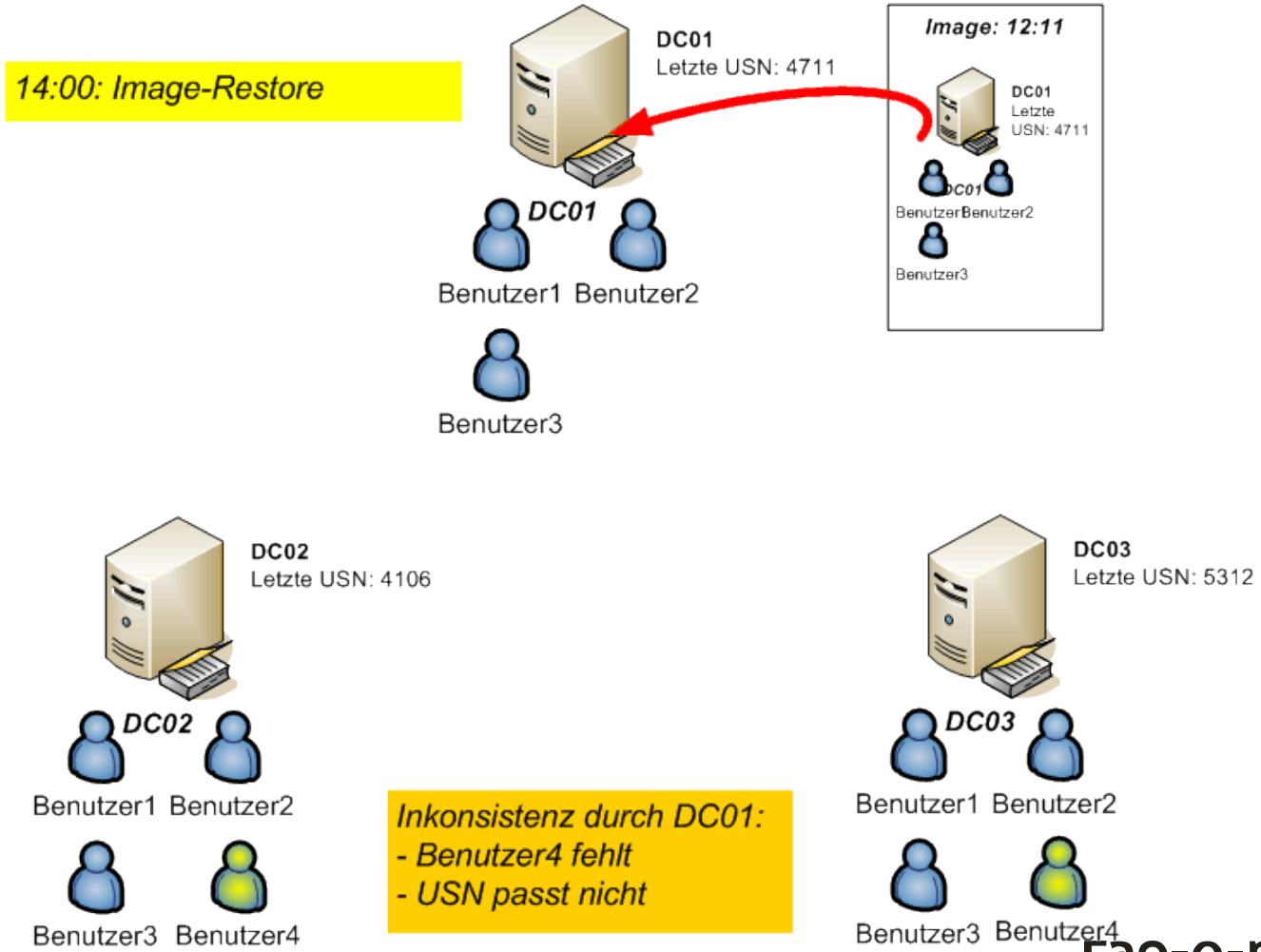
13:24: Neue Daten







USN Rollback: Katastrophe statt Rettung

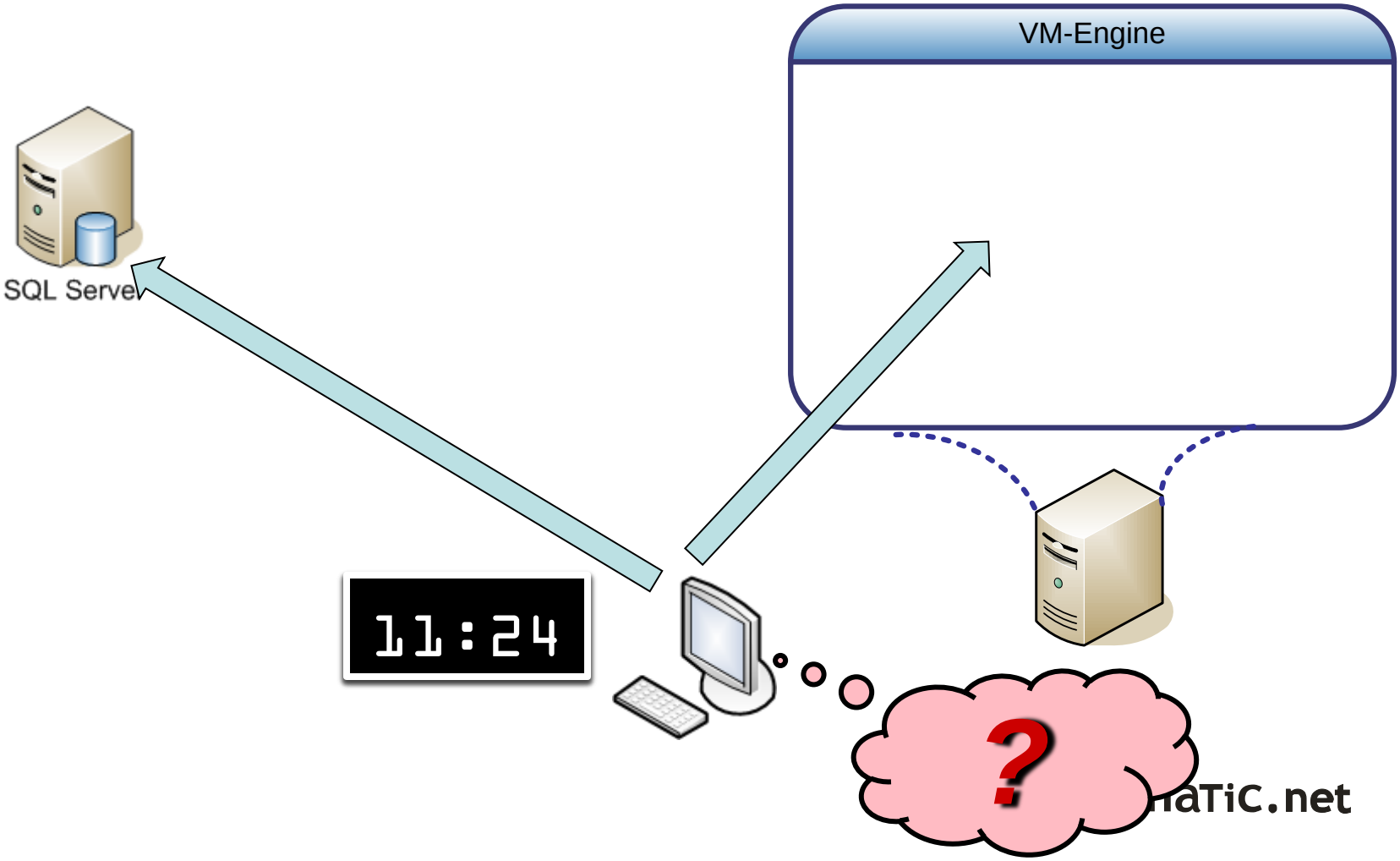


Der virtuelle Server: Neu oder gebraucht?

- Bestechend einfach: P2V-Migration
- Kein Neuaufsetzen, kein Migrationsaufwand
- Im laufenden Betrieb möglich
- … aber: Zerstört nicht nur Active Directory!

FAQ-O-MATIC.net

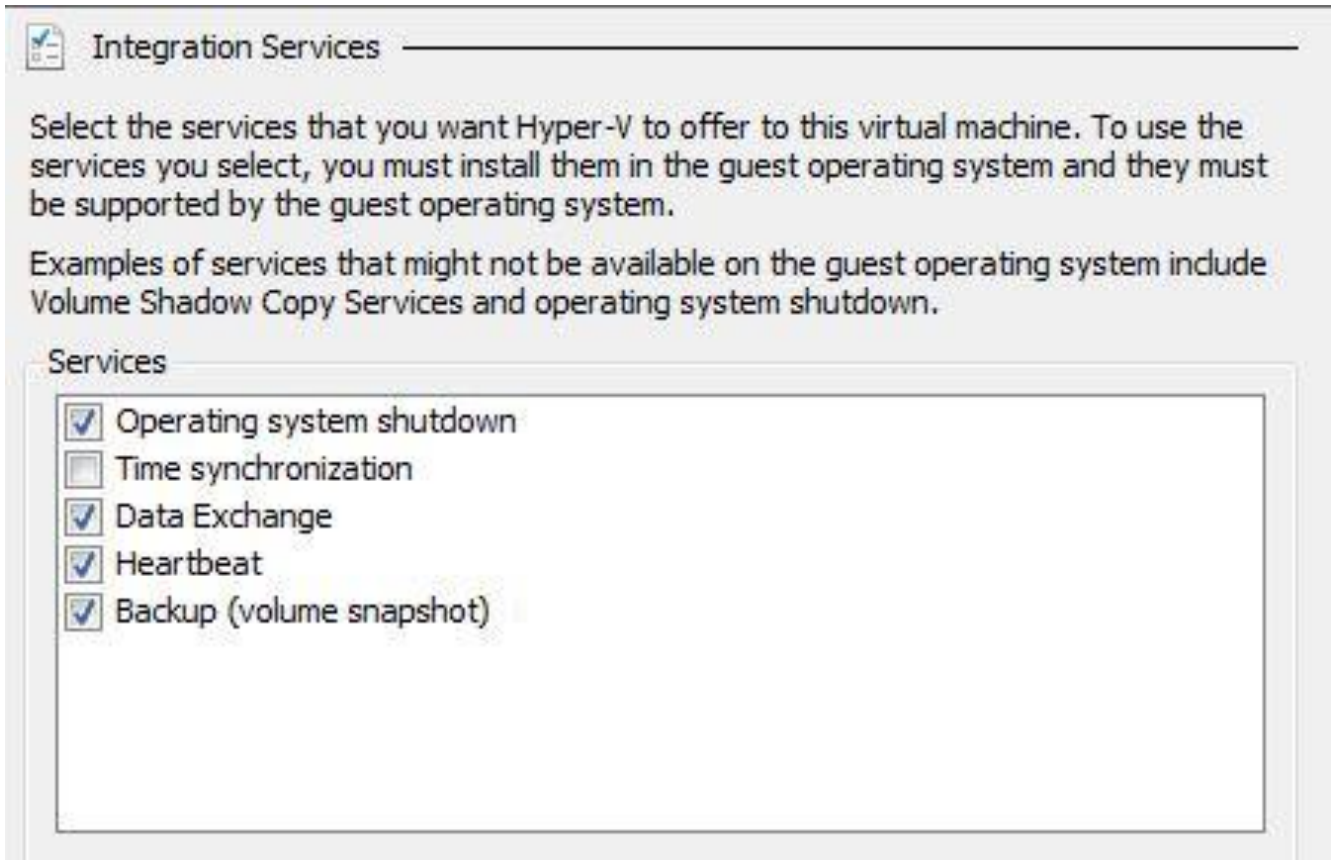
P2V: Alles andere als schmerzlos



Virtuelle DCs

- Kein P2V für Domänencontroller!
- Neue DCs einbinden ist so einfach:
  - Neuen Server installieren
  - Ins Netzwerk einbinden (DNS!)
  - dcpromo
  - … und fertig

Die Zeit und das Ticket



FAQ-O-MATIC.net

No-Go für virtuelle Domänencontroller

- DC in der Parent Partition
- Image-Backup und Snapshots
- P2V-Migration
- Cloning
- Live-Spiegelung
- Pause-Modus, Differencing Disks
- Zeitsynchronisation mit dem Host

Was euch erwartet

- Active Directory und DNS
- Replikation
- Virtuelle DCs
- Sicherheit
- Lieblingsfehler

Typische Sünden

- Der DC als Universalserver
- NETLOGON als universelle Freigabe
- Geplante Tasks, ungeschützte Skripts

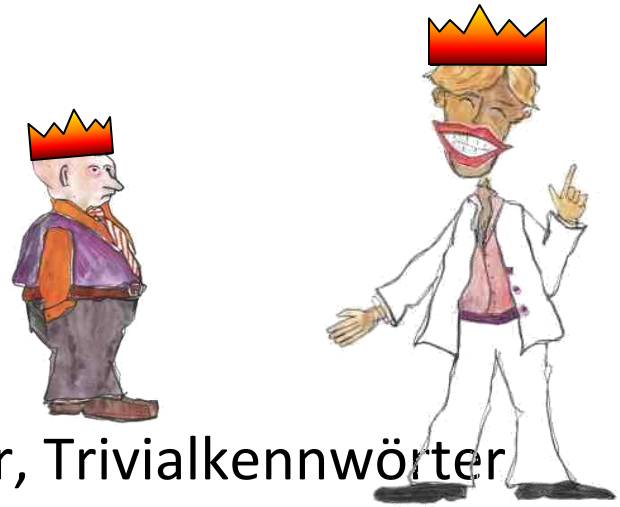
FaQ-o-maTiC.net

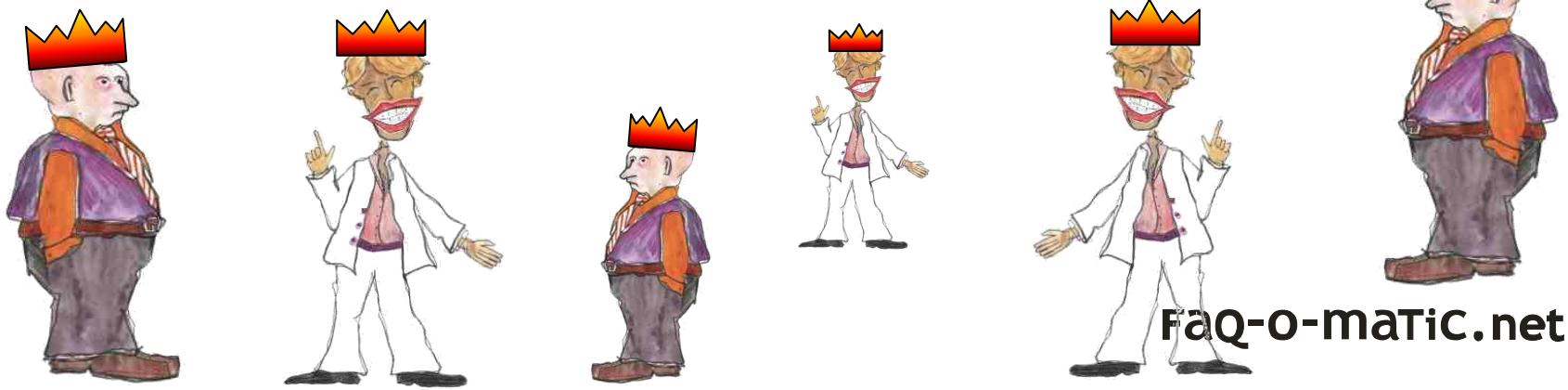
… anfassen!

Der Schnell-mal-eben-DC

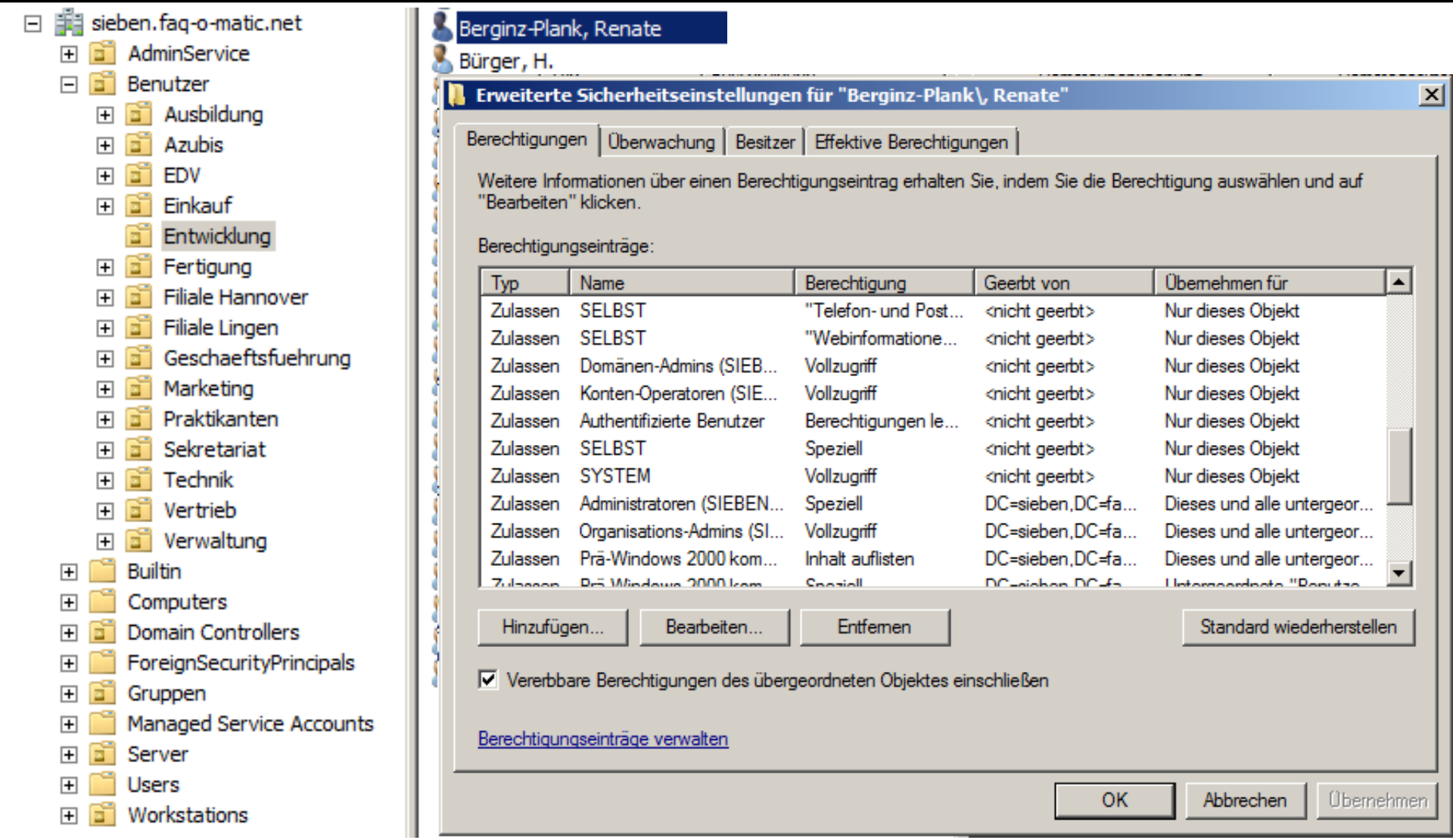
Der König ist tot – es leben die Könige!

- „Der“ Administrator
- Adminrechte fürs eigene Konto
- Mitglieder in Admin-Gruppen
- Dienstkonten auf mehreren Systemen
- Standardkennwörter, Startkennwörter, Trivialkennwörter
- Lokale Administratoren und Hauptbenutzer





Berechtigungen: Wer darf was?



Binsenweisheit oder Sicherheit?

- Automatische Kontensperrung
- Kennwortfilter
- Vertrauensstellung

FaQ-o-maTiC.net

… anfassen!

Kontensperrung – DoS leicht gemacht

AD gehackt per Silberscheibe

Was euch erwartet

- Active Directory und DNS
- Replikation
- Virtuelle DCs
- Sicherheit
- Lieblingsfehler

Noch ein paar Lieblingsfehler

- Global Catalog fehlt
- FSMO-Rolle läuft nicht
- Object Restore durch Neuerzeugung
- Restore-Versuch durch DB-Kopie

FAQ-O-MATIC.net

Was euch erwartet

- Active Directory
- Replikation
- Virtuelle DCs
- Sicherheit
- Lieblingsfehler

… mehr davon …

20./21. September 2011
Hyper-V Best Practice
Sicherheit in VM-Umgebungen
IT Admin Tech Talk

20./22. September 2011
AD Best Practice
AD-Sicherheit
n3k Roadshow

28. September 2011
Hyper-V sicher und sauber
iX-Workshop

FAQ-O-MATIC.net

Es gibt keine großen Entdeckungen und Fortschritte, solange es noch ein unglückliches Kind auf Erden gibt.

There’s no such thing as a discovery or progress as long as we have bitterly unhappy children on earth.

Er zijn geen grote ontdekkingen en geen vooruitgang, zolang er op deze wereld nog één kind ongelukkig is.

(Albert Einstein)