

# „Tu mir das nicht an“ sagte der Domänencontroller

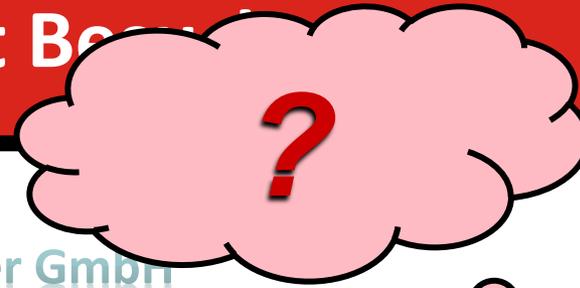
Nils Kaczenski  
*MVP Directory Services*  
*faq-o-matic.net*



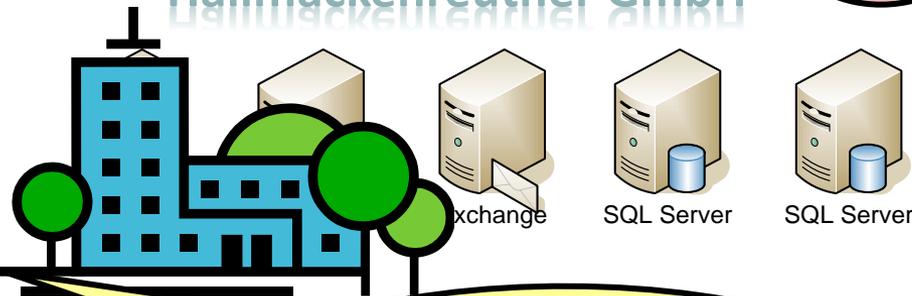
**\\vice:lingen**  
intelligent communities for europe



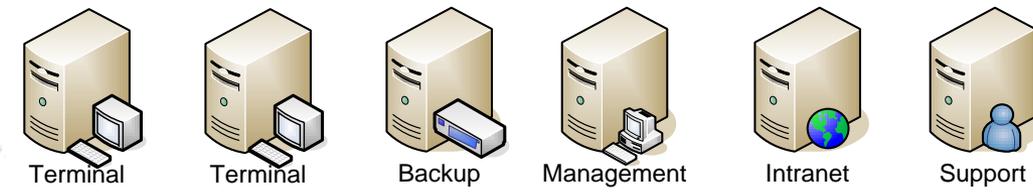
# Frau Bogen bekommt Besuch



Hallmackenreuther GmbH



Active Directory  
spinnt!



Karl Auer

Ellen Bogen



# 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**





# Was euch erwartet

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



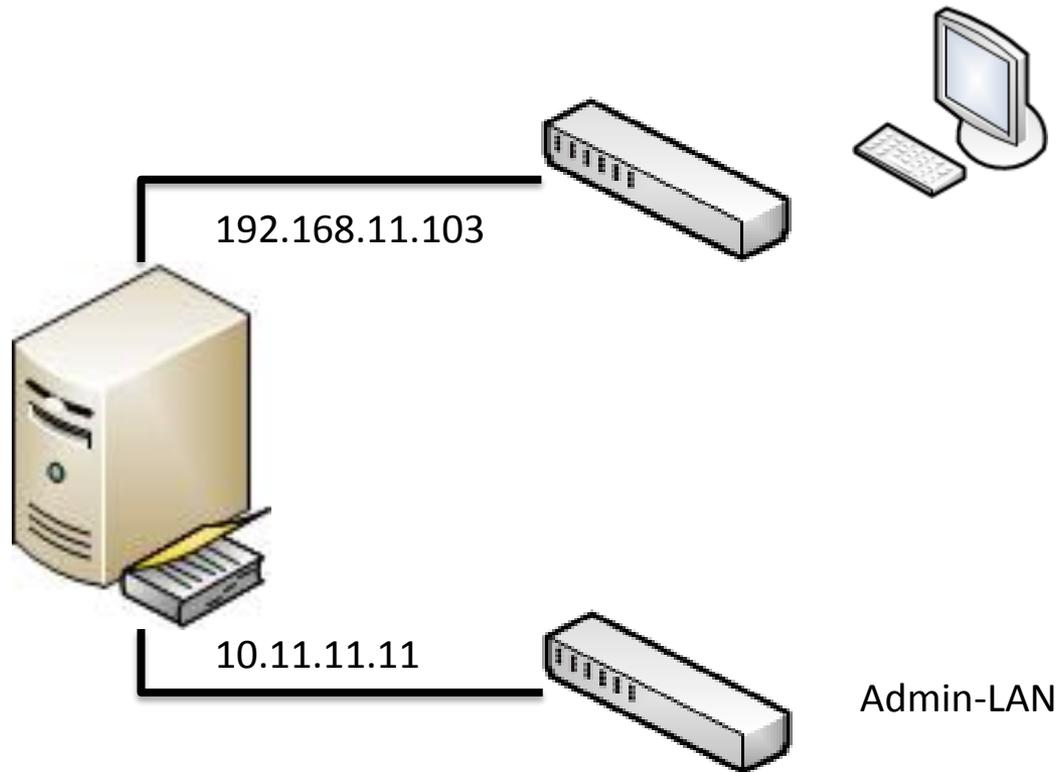
# Was euch erwartet

- 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

**... anfassend!**

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

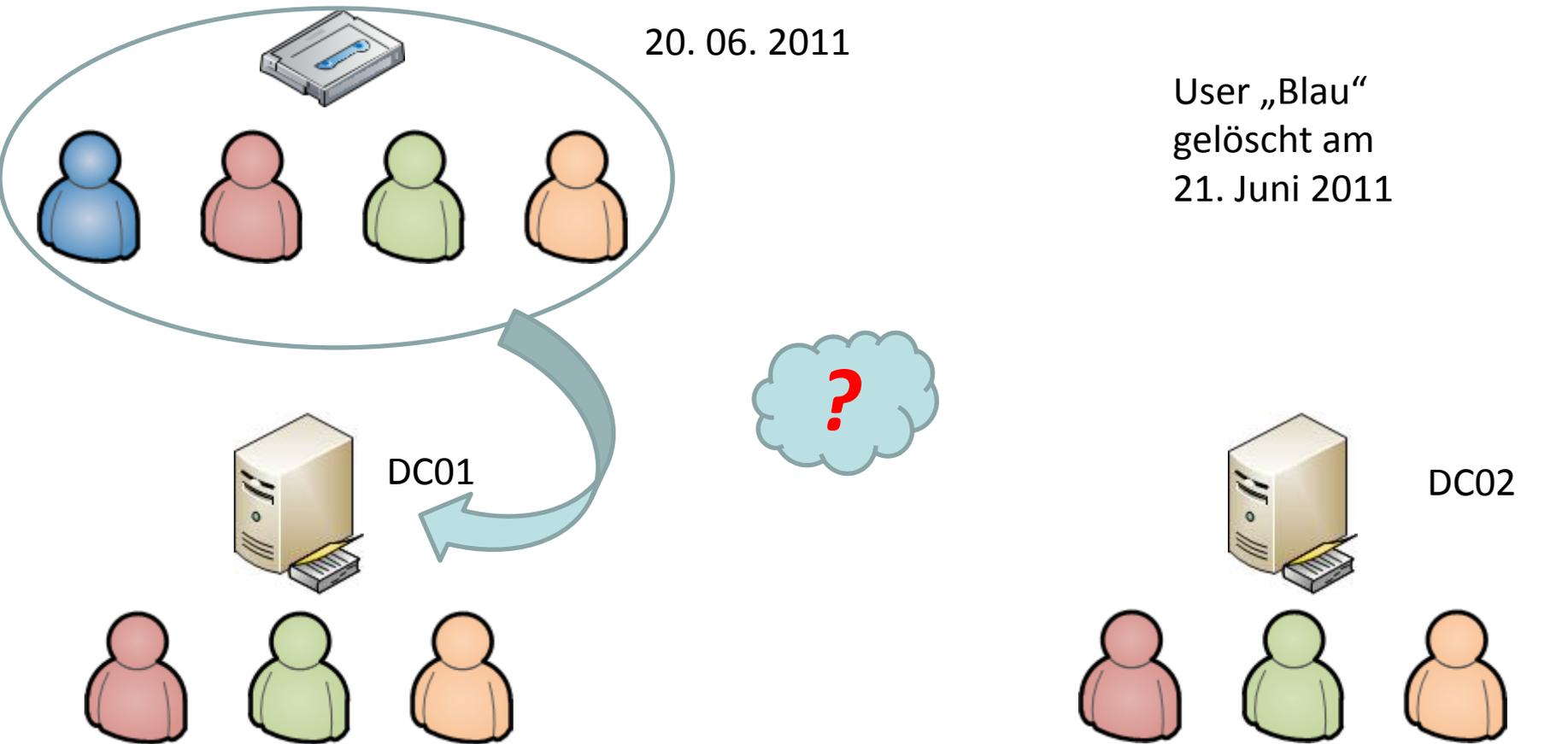
## **... anfassen!**

Tombstone Lifetime

Lingering Objects



# Herumlungernde Objekte





# 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 /removelingingobjects`



# 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

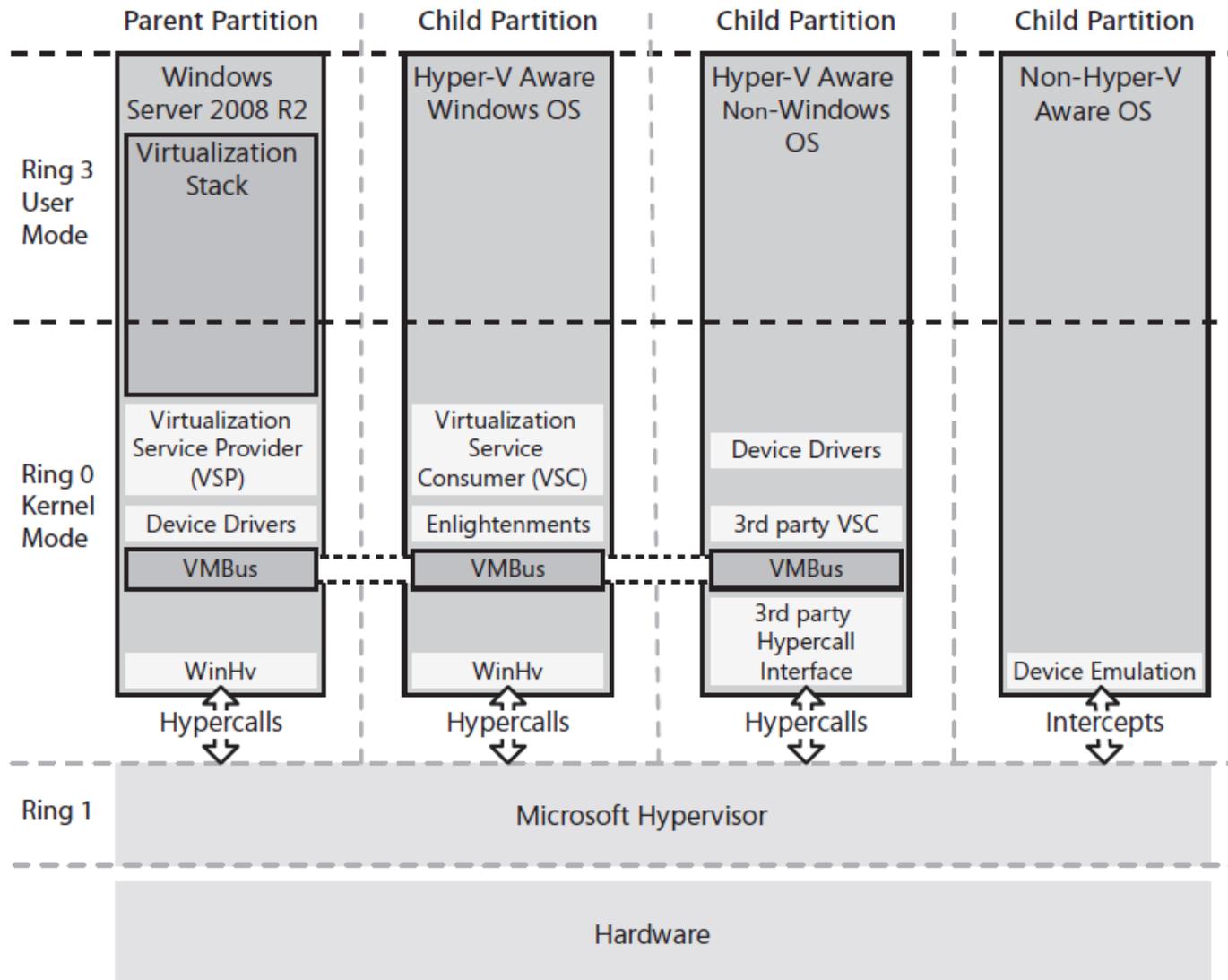


# Was euch erwartet

- ⦿ 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

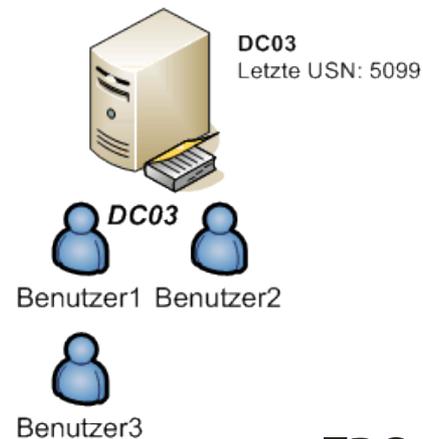
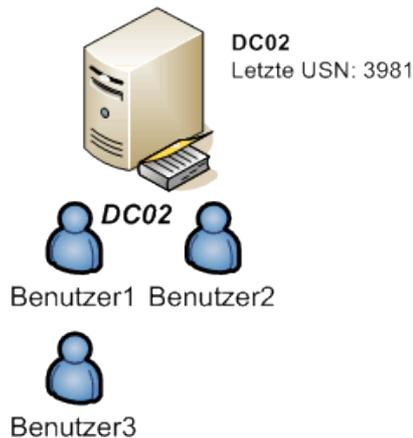
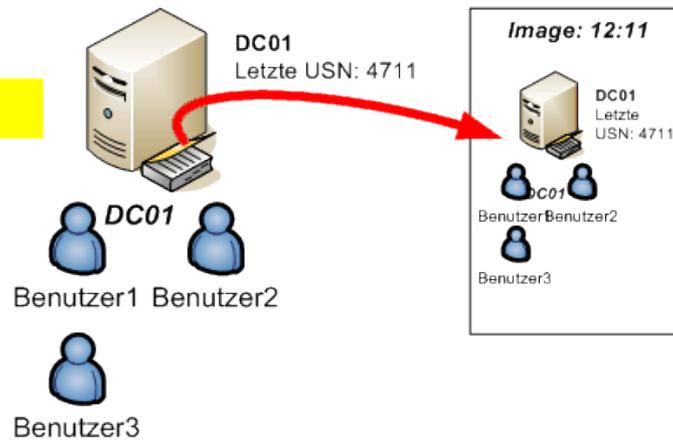
## **... anfassen!**

Snapshot-Rollback eines DC



# USN Rollback: Katastrophe statt Rettung

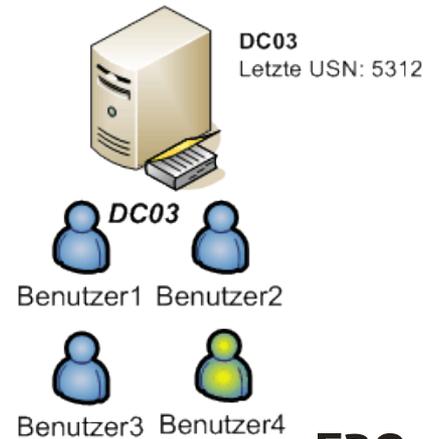
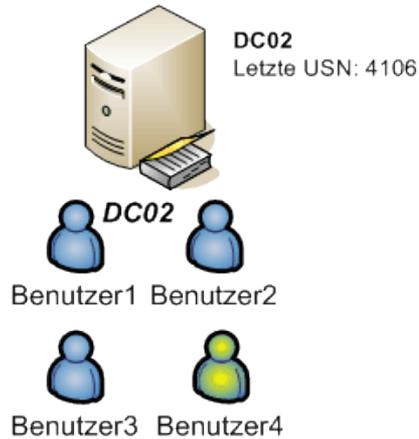
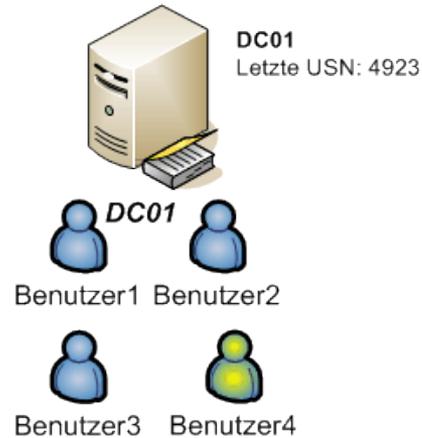
12:11: Image wird angelegt





# USN Rollback: Katastrophe statt Rettung

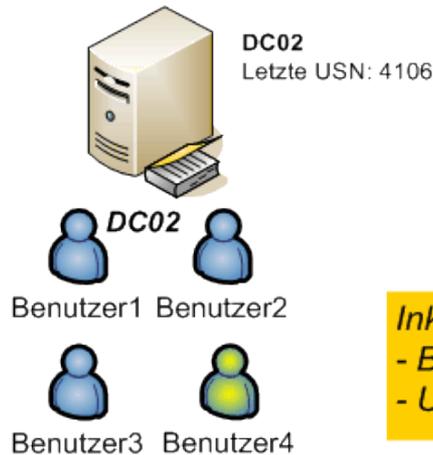
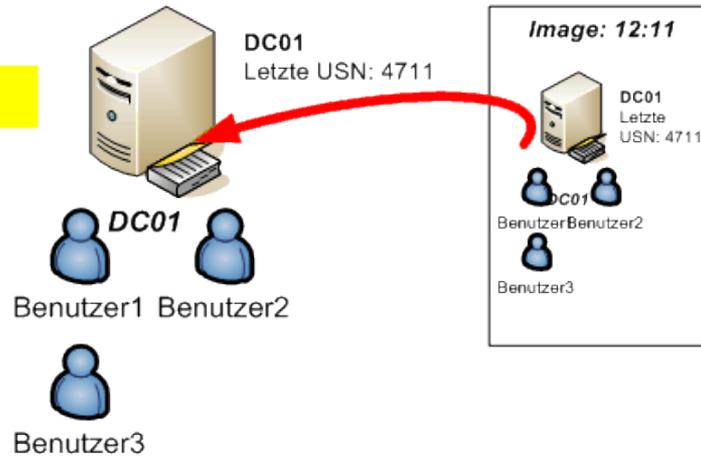
13:24: Neue Daten



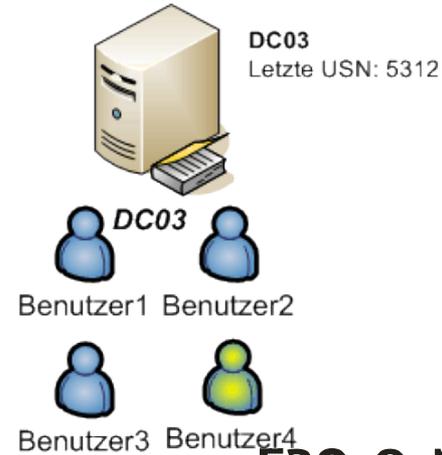


# USN Rollback: Katastrophe statt Rettung

14:00: Image-Restore



**Inkonsistenz durch DC01:**  
- Benutzer4 fehlt  
- USN passt nicht



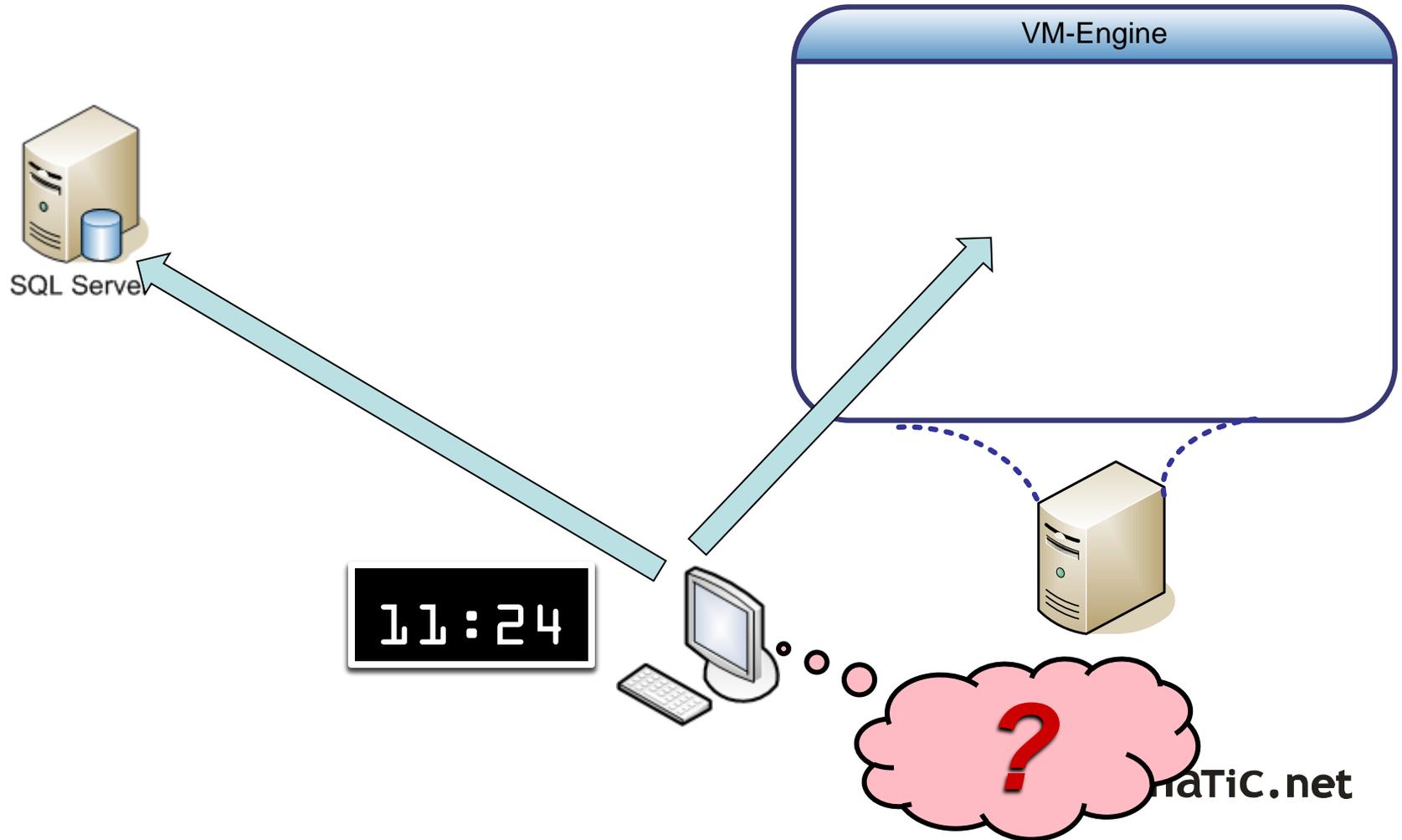


# Der virtuelle Server: Neu oder gebraucht?

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



# P2V: Alles andere als schmerzlos





- ⦿ 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

 Integration Services

Select the services that you want Hyper-V to offer to this virtual machine. To use the services you select, you must install them in the guest operating system and they must be supported by the guest operating system.

Examples of services that might not be available on the guest operating system include Volume Shadow Copy Services and operating system shutdown.

Services

- Operating system shutdown
- Time synchronization
- Data Exchange
- Heartbeat
- Backup (volume snapshot)



# 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

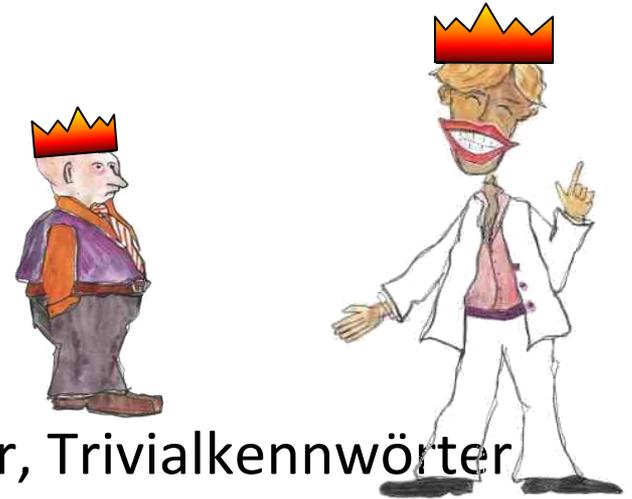
**... anfassen!**

Der Schnell-mal-eben-DC



# Der König ist tot – es leben die Könige!

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





# Berechtigungen: Wer darf was?

- [-] sieben.faq-o-matic.net
  - [+] AdminService
  - [-] Benutzer
    - [+] Ausbildung
    - [+] Azubis
    - [+] EDV
    - [+] Einkauf
    - [+] Entwicklung
    - [+] Fertigung
    - [+] Filiale Hannover
    - [+] Filiale Lingen
    - [+] Geschäftsfuehrung
    - [+] Marketing
    - [+] Praktikanten
    - [+] Sekretariat
    - [+] Technik
    - [+] Vertrieb
    - [+] Verwaltung
  - [+] BuiltIn
  - [+] Computers
  - [+] Domain Controllers
  - [+] ForeignSecurityPrincipals
  - [+] Gruppen
  - [+] Managed Service Accounts
  - [+] Server
  - [+] Users
  - [+] Workstations

Berginz-Plank, Renate

Bürger, H.

### Erweiterte Sicherheitseinstellungen für "Berginz-Plank\, Renate"

Berechtigungen | Überwachung | Besitzer | Effektive Berechtigungen

Weitere Informationen über einen Berechtigungseintrag erhalten Sie, indem Sie die Berechtigung auswählen und auf "Bearbeiten" klicken.

Berechtigungseinträge:

Typ	Name	Berechtigung	Geerbt von	Übernehmen für
Zulassen	SELBST	"Telefon- und Post...	<nicht geerbt>	Nur dieses Objekt
Zulassen	SELBST	"Webinformatio...	<nicht geerbt>	Nur dieses Objekt
Zulassen	Domänen-Admins (SIEB...	Vollzugriff	<nicht geerbt>	Nur dieses Objekt
Zulassen	Konten-Operatoren (SIE...	Vollzugriff	<nicht geerbt>	Nur dieses Objekt
Zulassen	Authentifizierte Benutzer	Berechtigungen le...	<nicht geerbt>	Nur dieses Objekt
Zulassen	SELBST	Speziell	<nicht geerbt>	Nur dieses Objekt
Zulassen	SYSTEM	Vollzugriff	<nicht geerbt>	Nur dieses Objekt
Zulassen	Administratoren (SIEBEN...	Speziell	DC=sieben,DC=fa...	Dieses und alle untergeor...
Zulassen	Organisations-Admins (SI...	Vollzugriff	DC=sieben,DC=fa...	Dieses und alle untergeor...
Zulassen	Prä-Windows 2000 kom...	Inhalt auflisten	DC=sieben,DC=fa...	Dieses und alle untergeor...
Zulassen	Prä-Windows 2000 kom...	Speziell	DC=sieben,DC=fa...	Untergeordnete "Benutz...

Hinzufügen...    Bearbeiten...    Entfernen    Standard wiederherstellen

Vererbare Berechtigungen des übergeordneten Objektes einschließen

[Berechtigungseinträge verwalten](#)

OK    Abbrechen    Übernehmen



# 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



# 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)

