WITSTOR
SYSTEMLÖSUNGEN . SERVICE

# » Go oder No-Go? Der VM-DC

## Virtualisierung von Domänencontrollern

» Nils Kaczenski
Leiter Consulting & Support, WITstor

WITSTOR
LÖSUNGEN . SERVICE

# Frau Bogen bekommt Besuch.

?

WITSTOR
SYSTEMLÖSUNGEN . SERVICE

# Wer vor Ihnen steht

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

FAQ-O-MATIC.net

MVP
Microsoft®
Most Valuable
Professional

WITSTOR
SYSTEMLÖSUNGEN . SERVICE

# WITstor: Systemlösungen. Service

## Network & Applications

Windows
Active Directory
Exchange
Security
Switching/Routing
Firewall
WAN-Optimierung

## Data Center

Storage
Server
Virtualisierung
Recovery
Verfügbarkeit

## IT Services

Rollout
Managed Services
Client Services
Helpdesk
Operating

NetApp Gold Partner
FUJITSU QUALIFIED PARTNER
vmware enterprise PARTNER
Cisco Systems
riverbed Think fast.
WatchGuard
CITRIX
Microsoft GOLD CERTIFIED Partner
BakBone
hp invent
H&S

# Was Sie erwartet

- Virtuelle DCs: Gute oder schlechte Idee?
- Was Sie Ihrem AD lieber nicht antun sollten
- Wie komme ich zum virtuellen DC?
- Best Practice für virtuelle DCs

# Was Sie erwartet

- **Virtuelle DCs: Gute oder schlechte Idee?**
- Was Sie Ihrem AD lieber nicht antun sollten
- Wie komme ich zum virtuellen DC?
- Best Practice für virtuelle DCs

# Was tut der DC eigentlich?

- **Anmeldedienste**
  - Kerberos
  - LDAP
  - Downlevel-Protokolle
- **Infrastrukturdienste**
  - DNS
  - WINS
  - AD-Replikation
- **Datenbank**
  - User, Computer, Gruppen
  - Konfiguration
  - Applikationsdaten

# Die AD-Datenbank

- **Eine Datenbank, mehrere Partitionen**
  - Domain Naming Context
  - Configuration Naming Context
  - Schema Naming Context
  - Application Naming Contexts
- **Intern: SQL-Datenbank (ESE) mit drei Tabellen**
  - Data Table
  - Link Table
  - Security Descriptor Table
- **Indizierung beschleunigt Such- und Lesezugriffe**
- **Moderne DCs: Datenbank im RAM**
  - 2-8 GB reicht für viele Unternehmen aus

# DC virtualisieren?

## Pro

- „Kein“ Hardware-Bedarf
- Leichtes Recovery durch Hardware-Abstraktion
- Host-Migration möglich
- Vorteile im systemnahen Operating

## Contra

- Mögliche Performance-Engpässe
- Erweiterte VM-Techniken nicht nutzbar
- Abhängigkeit von VM-Umgebung

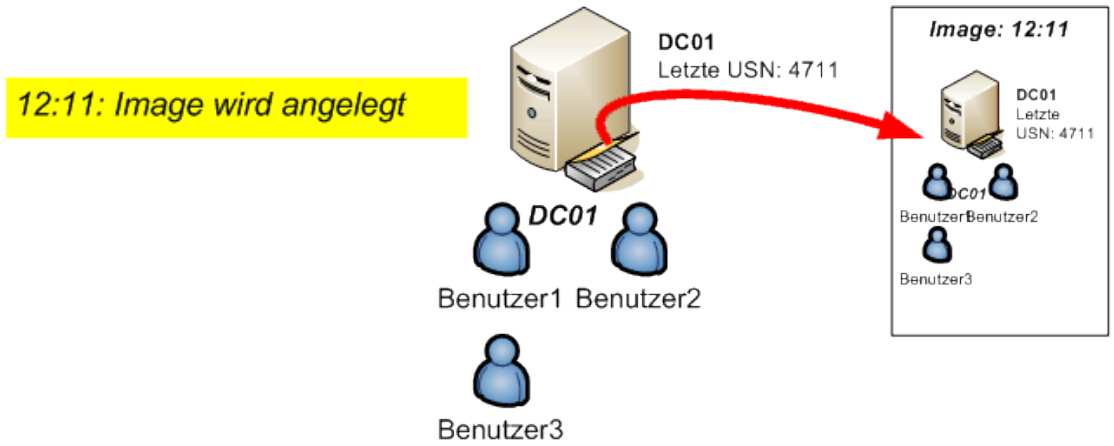
# Was Sie erwartet

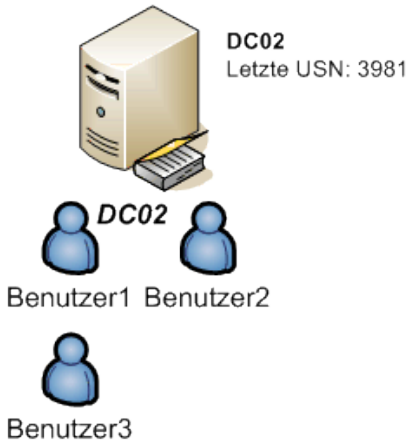
- Virtuelle DCs: Gute oder schlechte Idee?
- **Was Sie Ihrem AD lieber nicht antun sollten**
- Wie komme ich zum virtuellen DC?
- Best Practice für virtuelle DCs

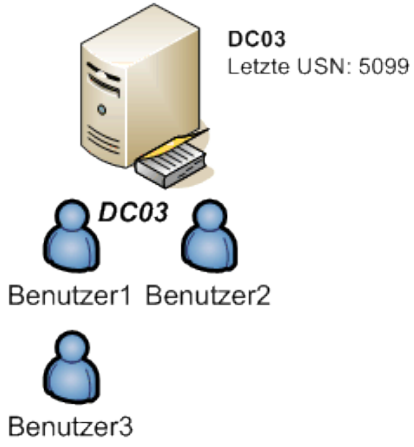
# No-Go für Domänencontroller

- **Image-Backup und Snapshots**
  - USN-Rollback
- **Cloning für Produktion**
  - SID und Individualisierung
  - Undefinierte Konfigurationen
- **Cloning fürs Testlabor**
  - Das Sicherheitsloch zum Selbermachen
- **DC in der Parent Partition**
- **Live-Spiegelung**
- **Zeitsynchronisation mit dem Host**
- **Host in mehreren Netzwerken**

# USN Rollback: Katastrophe statt Rettung

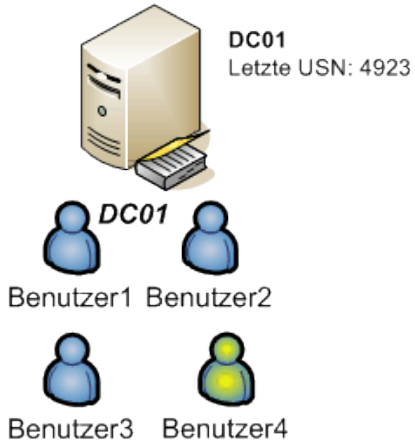


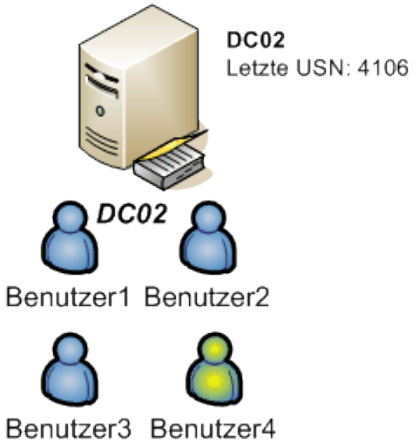



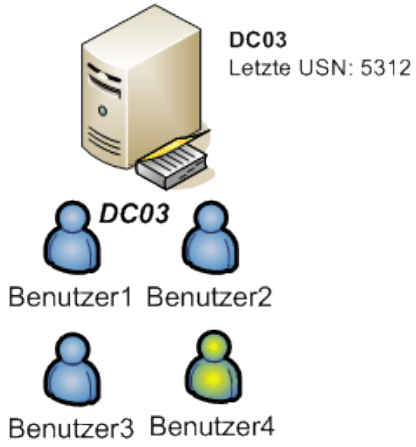



# USN Rollback: Katastrophe statt Rettung

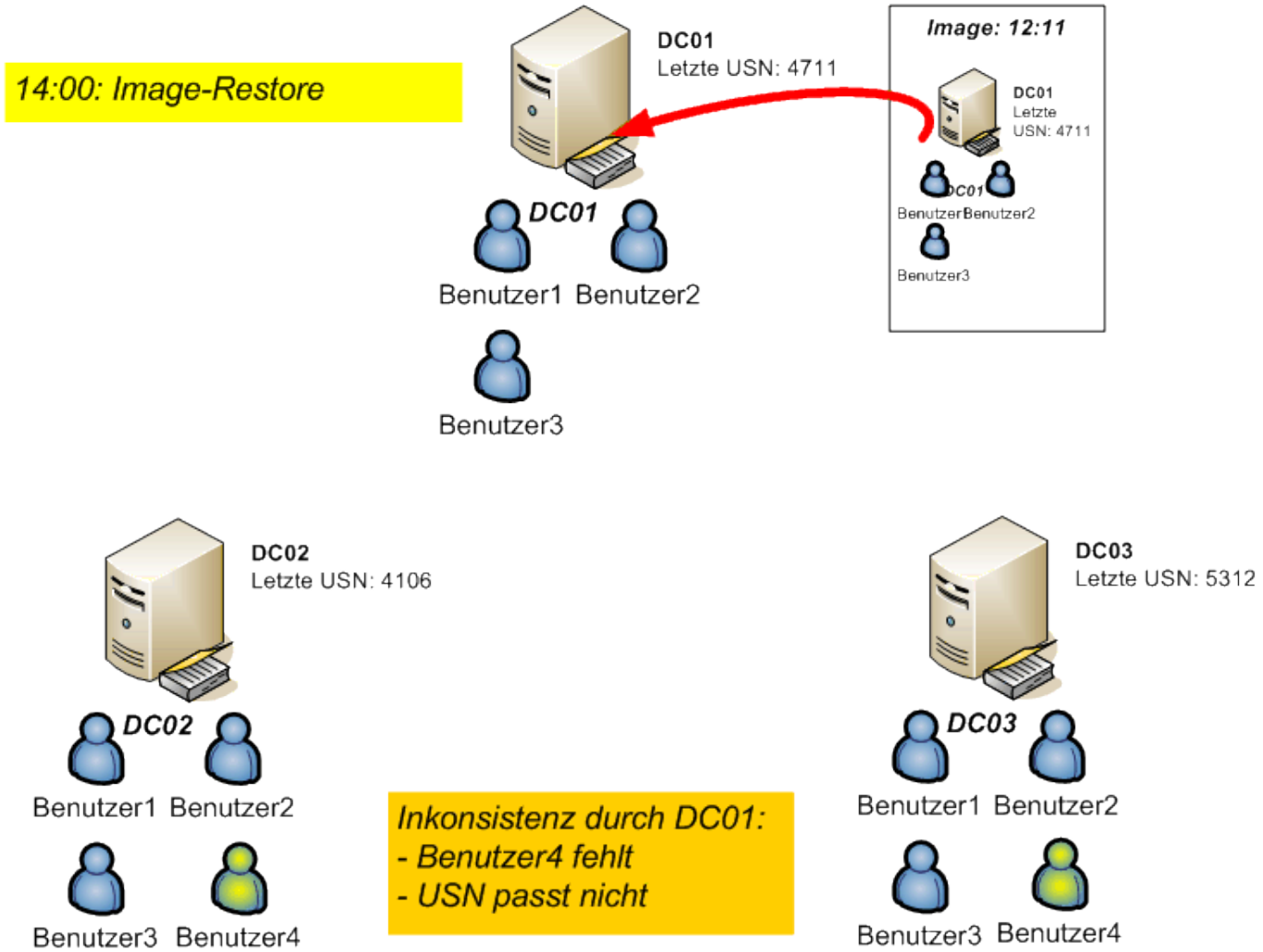
*13:24: Neue Daten*



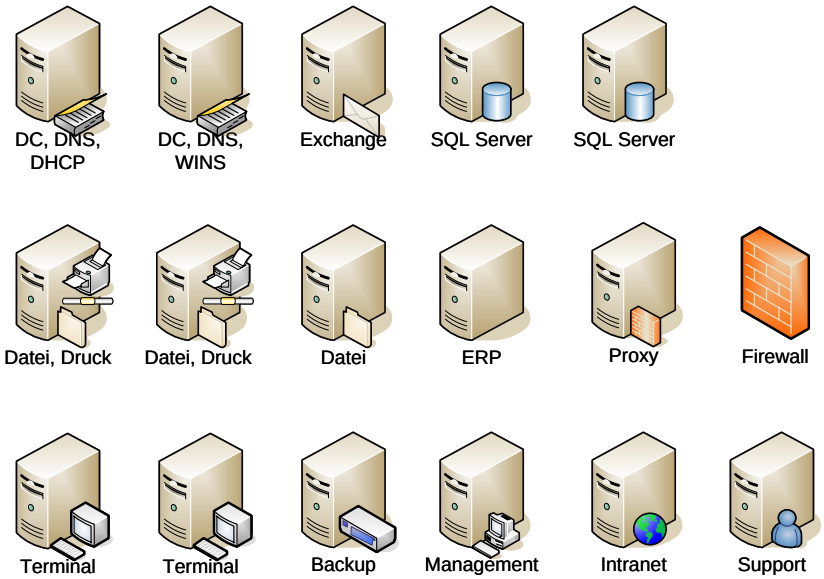



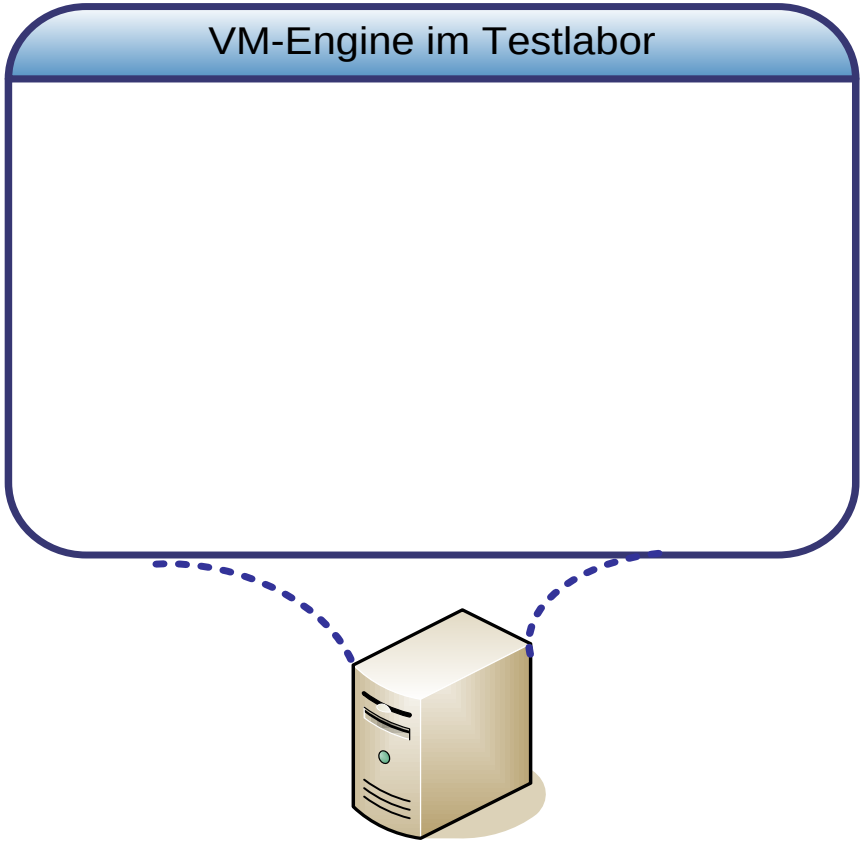
# USN Rollback: Katastrophe statt Rettung



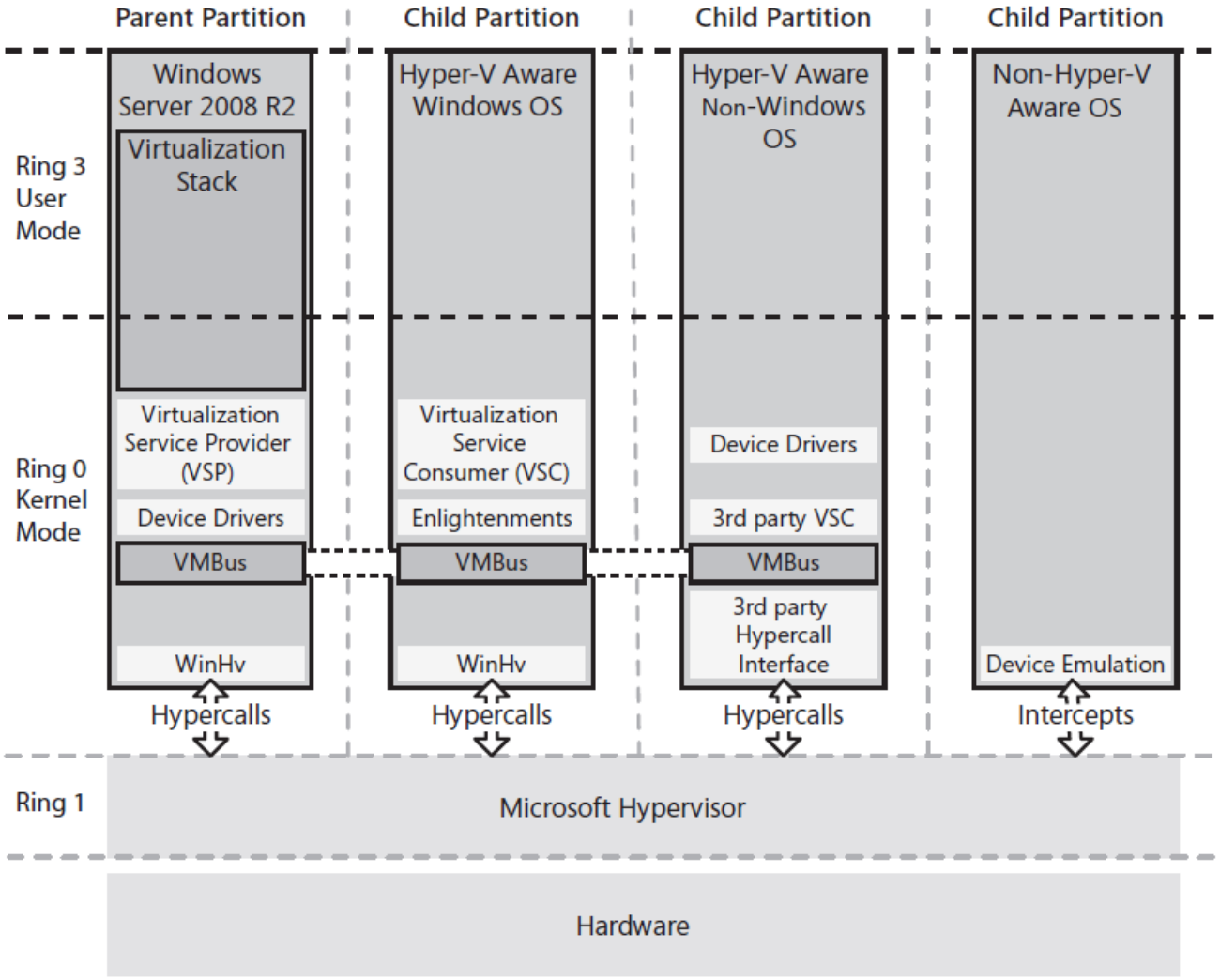
WITSTOR
SYSTEMLÖSUNGEN . SERVICE

# Sicherheitsloch auf Knopfdruck

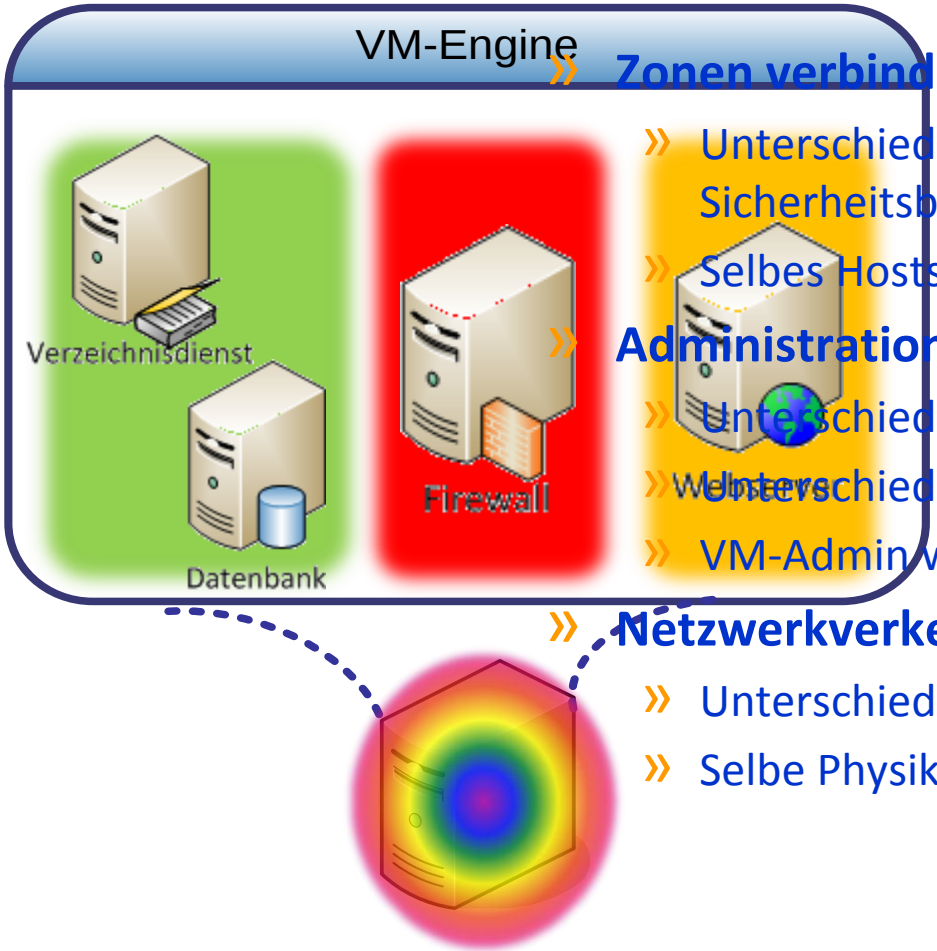


# Lasst die Eltern in Ruhe!



# Kuschlig beieinander

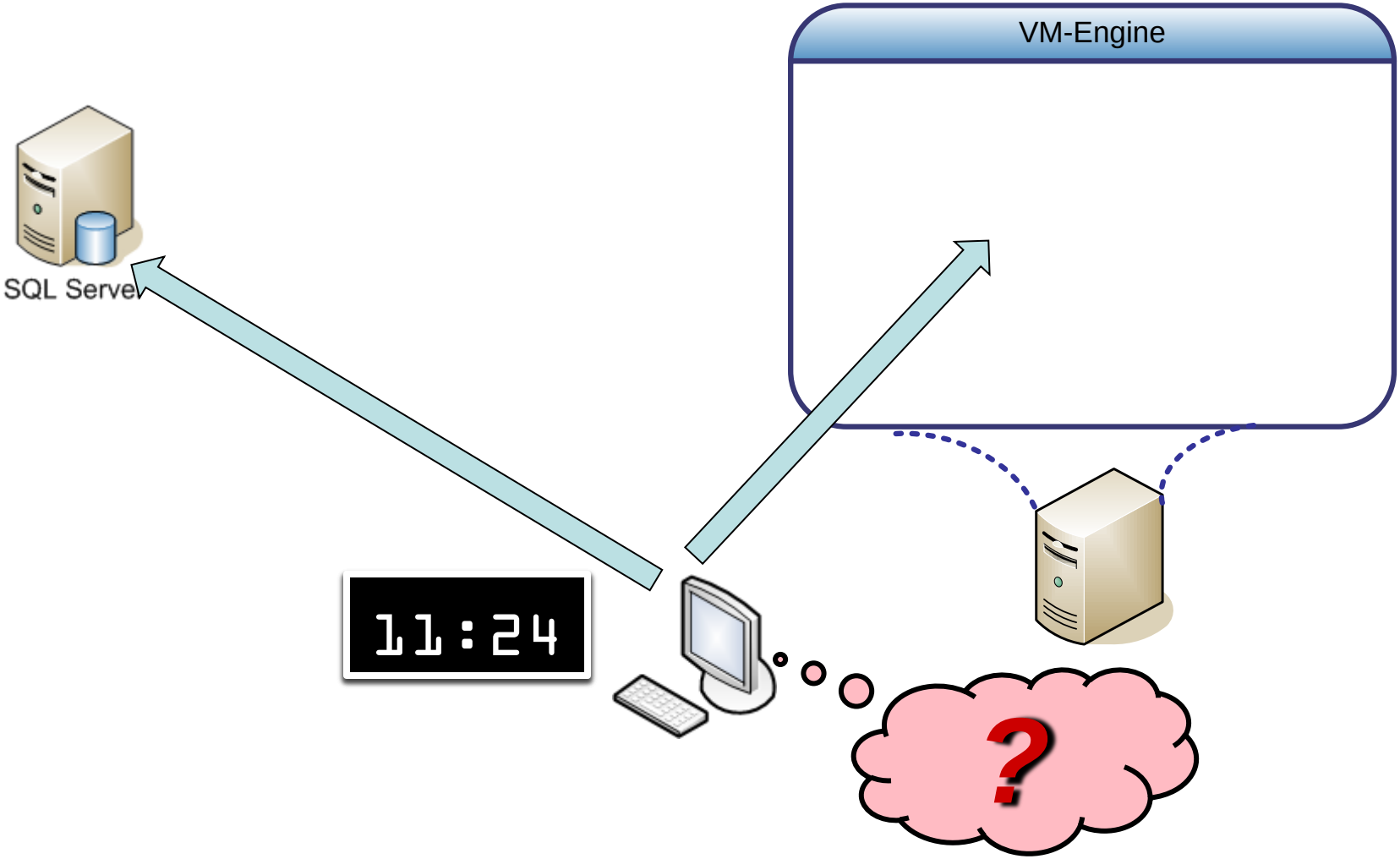



- **Zonen verbinden**
  - Unterschiedliche Sicherheitsbereiche
  - Selbes Hostsystem
- **Administration verbinden**
  - Unterschiedliche Admins
  - Unterschiedliche Richtlinien
  - VM-Admin wird Master-Admin
- **Netzwerkverkehr verbinden**
  - Unterschiedlicher Traffic
  - Selbe Physik

# Was Sie erwartet

- Virtuelle DCs: Gute oder schlechte Idee?
- Was Sie Ihrem AD lieber nicht antun sollten
- **Wie komme ich zum virtuellen DC?**
- Best Practice für virtuelle DCs

# 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

# Was Sie erwartet

- Virtuelle DCs: Gute oder schlechte Idee?
- Was Sie Ihrem AD lieber nicht antun sollten
- Wie komme ich zum virtuellen DC?
- **Best Practice für virtuelle DCs**

# So klappt’s mit der virtuellen Domäne

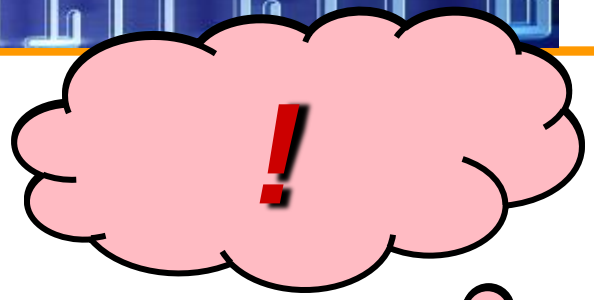
- **Ein DC als physischer Server**
  - Abhängigkeit vom VM-Umgebung vermeiden
  - PDC-Emulator zur Zeitsynchronisation
- **Zeitsynchronisation über AD-Mechanismen**
  - Keine Host-Zeitsynchronisation
- **VM als Backup-Quelle**
  - System State Backup
  - KEINE Snapshots, Images, VHD-Kopien …
- **Erweiterte VM-Funktionen meiden**
  - Pausieren
  - Snapshot-Restore, Cloning, Differencing Disks …
  - Spiegelung

# … und das sollte man sowieso immer beachten

- **Dedizierte DCs**
  - AD und Infrastrukturdienste (DNS, WINS)
  - Keine Applikationen
- **Kein Exchange auf einem DC!**
  - Ausnahme: SBS
- **DNS ins AD integrieren**
  - Forwarder statt externer Server
  - In heterogenen Netzen AD-Subzone an DCs delegieren
- **Planmäßiger Betrieb**
  - Sicherheitskonzept
  - Betriebs- und Notfallkonzept
  - Monitoring und laufende Wartung

WITSTOR
SYSTEMLÖSUNGEN . SERVICE

# Was Sie erwartet




- Virtuelle DCs: Gute oder schlechte Idee?
- Was Sie Ihrem AD lieber nicht antun sollten
- Wie komme ich zum virtuellen DC?
- Best Practice für virtuelle DCs

# Mehr …

» www.witstor.de

» Nils.Kaczenski@witstor.de

» twitter.com/WITstor