



WINone

1.-2.2.2012, MÜNCHEN



Windows Desktop und Server Konferenz

Active Directory reloaded in Windows Server „8“

Nils Kaczenski

faq-o-matic.net

WITstor GmbH



WINone



Windows Desktop Server Konferenz

1.-2.2.2012, MÜNCHEN

Frau Bogen bekommt



Hallmackenreuther GmbH



Lotte Macchiato



Datei, Druck



Datei, Druck



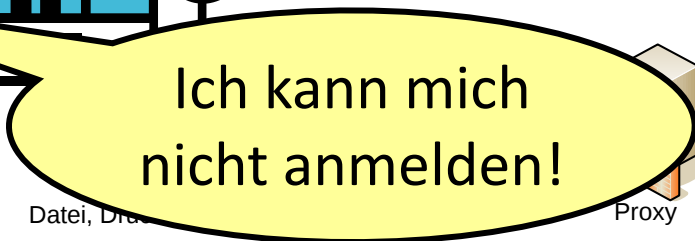
Exchange



SQL Server



SQL Server



Ich kann mich nicht anmelden!



Proxy



Firewall



Terminal



Terminal



Backup



Management



Intranet



Support



Ellen Bogen



WINone



Windows Developer Konferenz

1.-2.2.2012, MÜNCHEN

Frau Bogen fragt nach

?!



Ich hab nur
einen Snapshot
zurückgespielt!



Frans Iskaner

Ellen Bogen

Wer vor Ihnen steht

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



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



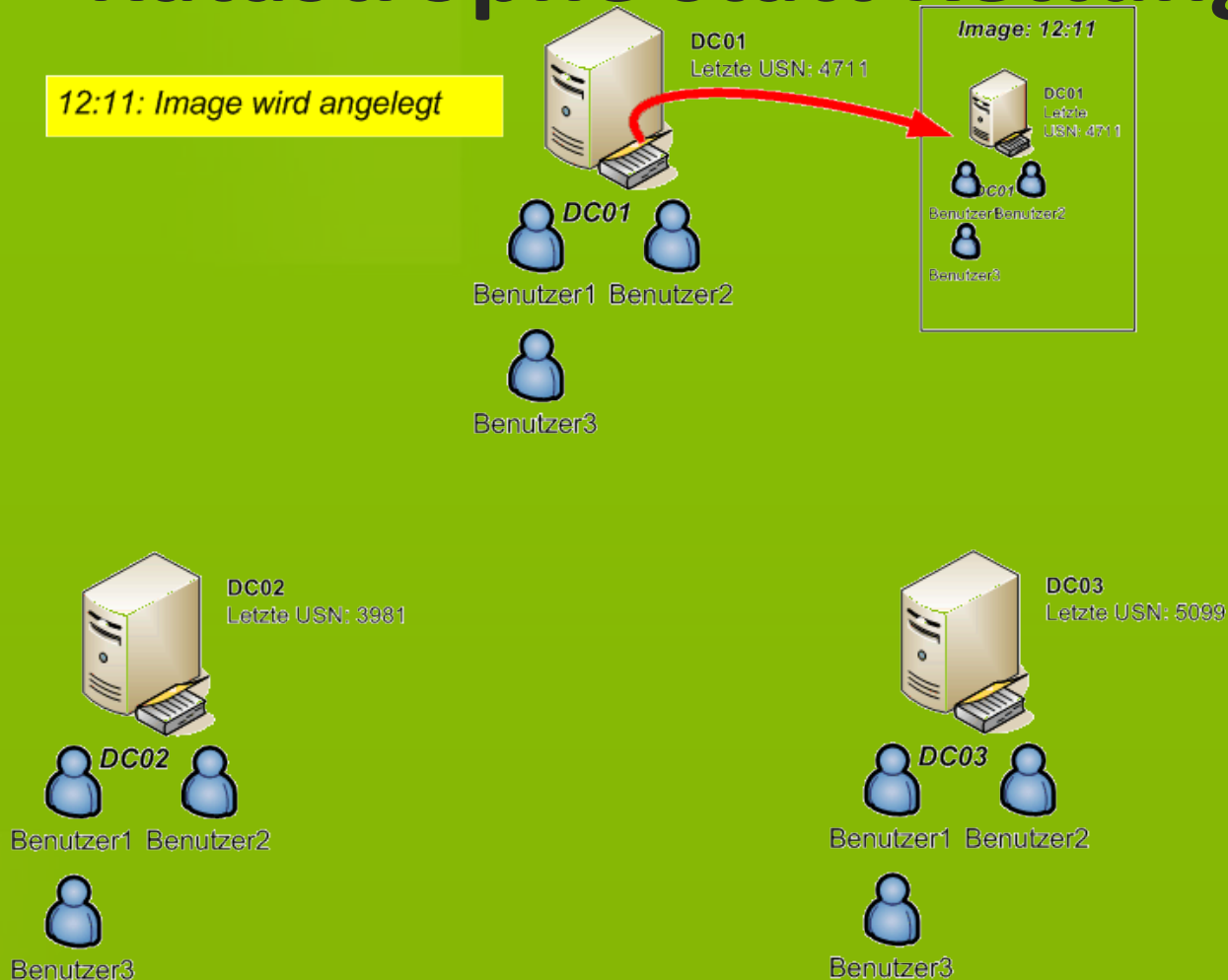
Heute: Der virtuelle DC

- Virtuelle DCs: Kein Problem ... eigentlich
- Ein DC pro Domäne auf Hardware
- Niemals:
 - DC in der Parent Partition
 - DC klonen
 - Zeitsynchronisation mit dem Host
 - Snapshot oder Image Restore

VM-Snapshots

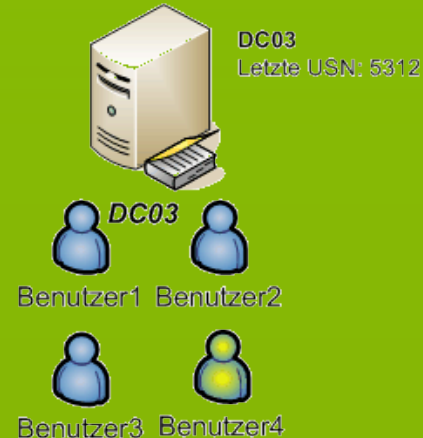
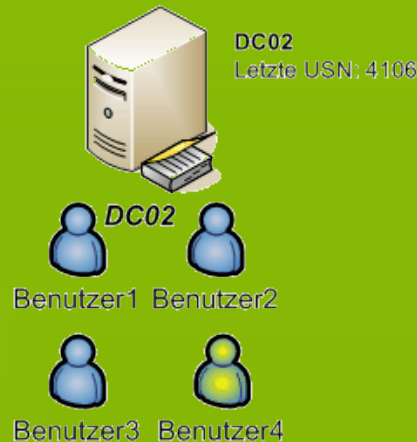
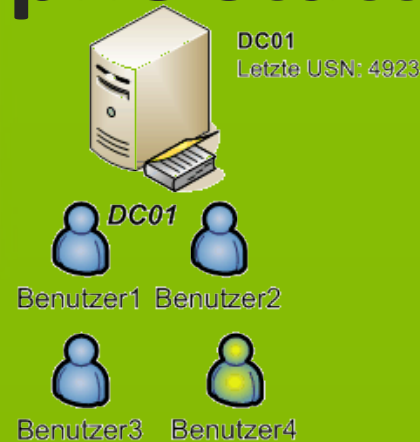
- Kann jeder Hypervisor
- Geht irre schnell
- Ist so ungemein praktisch
- ... und zerstört Active Directory

USN Rollback: Katastrophe statt Rettung



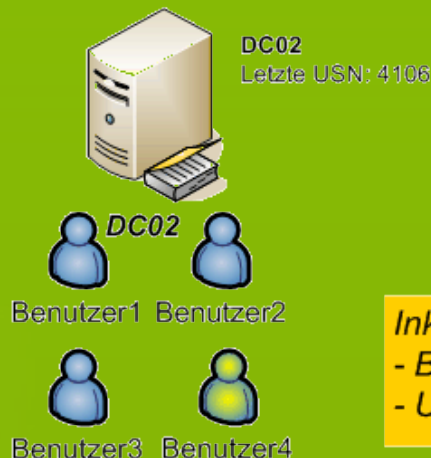
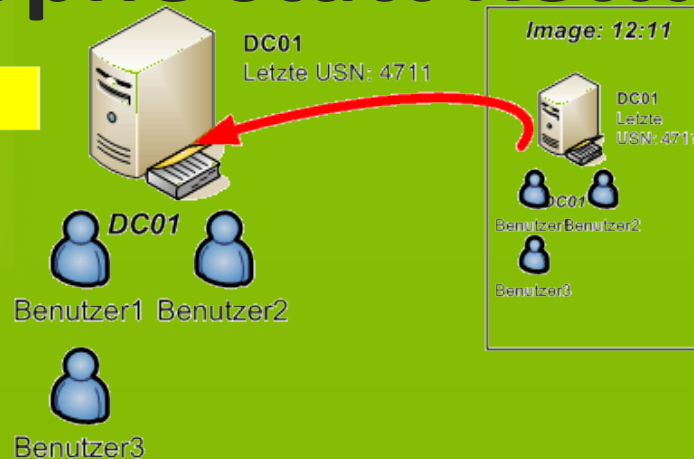
USN Rollback: Katastrophe statt Rettung

13:24: Neue Daten



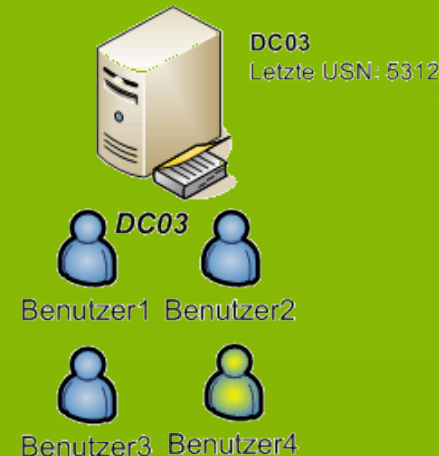
USN Rollback: Katastrophe statt Rettung

14:00: Image-Restore



Inkonsistenz durch DC01:

- Benutzer4 fehlt
- USN passt nicht

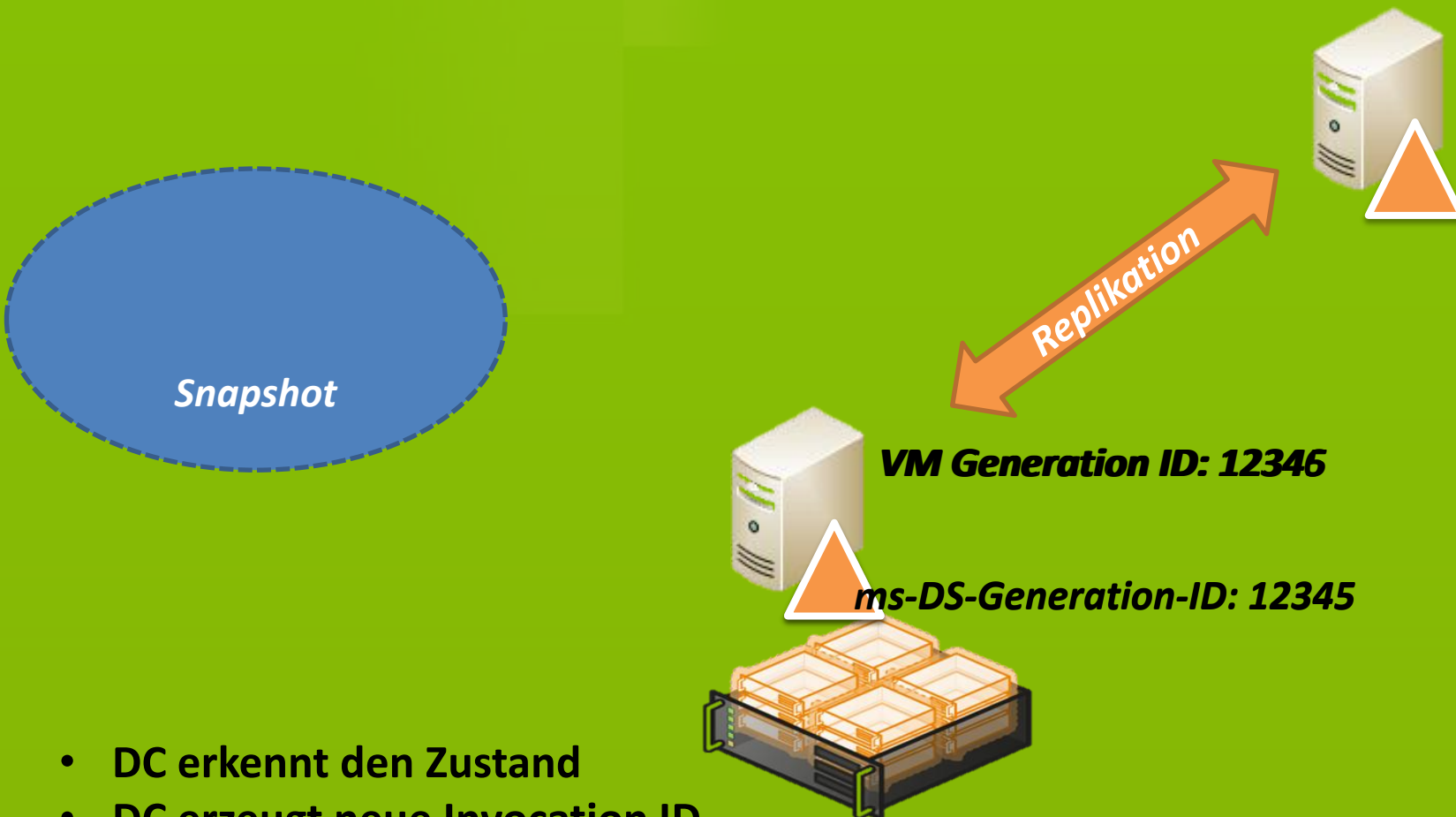


In Zukunft:

AD kennt VM-Snapshots

- Active Directory kann auf Snapshots reagieren
- ABER: Nur unter bestimmten Voraussetzungen
 - AD mit Windows Server „8“
 - VM unter Hyper-V 3.0
- VM Generation ID
 - Kennzeichnet den Zustand einer VM
 - Ändert sich bei Snapshot
 - AD prüft DC-ID gegen VM-ID

Nur mit ID



- DC erkennt den Zustand
- DC erzeugt neue Invocation ID
- Vollreplikation wie nach Restore



WINone

1.-2.2.2012, MÜNCHEN



Windows Desktop und Server Konferenz

... anfassen

- ms-DS-Generation-ID

VM Generation ID: Fragen und Grenzen

- Nur Hyper-V 3.0 beherrscht das Verfahren!
 - Andere Hersteller werden nachziehen
- Nur AD in Windows Server „8“ kann das!
- Wie liest die VM die ID aus?
- Was passiert bei Fehlern oder Angriffen?
 - Hypervisor erzeugt keine neue ID
 - Hypervisor teilt keine ID mit
 - Hypervisor erzeugt laufend neue IDs



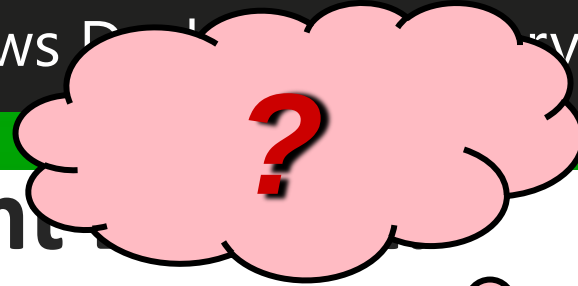
WINone



Windows Server Konferenz

1.-2.2.2012, MÜNCHEN

Frau Bogen bekommt



Karl Auer

Wir brauchen
viele neue DCs!



Ellen Bogen

Der Klon-DC

- Nur mit „8“-VMs unter Hyper-V 3.0
- Beruht auf VM Generation ID
- Vorbereitung nötig
 - Autorisierung zum Klonen
 - Flag-Dateien
- Schnelles Massen-Rollout für DCs
- In den meisten Umgebungen unnötig!



WINone

1.-2.2.2012, MÜNCHEN



Windows Desktop und Server Konferenz

... anfassen

- DC-Klonen
vorbereiten



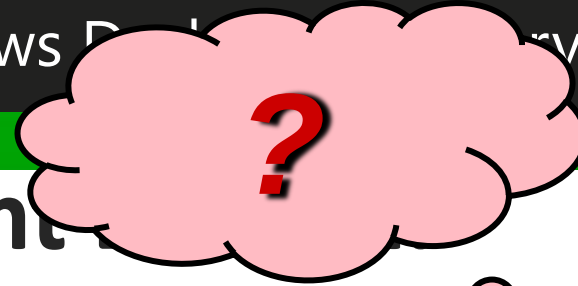
WINone



Windows Developer Konferenz

1.-2.2.2012, MÜNCHEN

Frau Bogen bekommt



Lotte Macchiato

Ich kann mich
schon wieder
nicht anmelden!



Ellen Bogen



WINone



Windows Developer Server Konferenz

1.-2.2.2012, MÜNCHEN

Frau Bogen fragt nach

?!



... äh ... das
Konto ist weg ...



Frans Iskaner

Ellen Bogen

Die gelben Engel vom ADAC

- Active Directory Administrative Center
 - Gab es schon in Windows Server 2008 R2
 - Renoviert und endlich nützlich
- AD-Papierkorb
- Fine-Grained Password Policies



WINone

1.-2.2.2012, MÜNCHEN



Windows Desktop und Server Konferenz

... anfassen

- AD-Papierkorb früher und heute
- PSOs früher und heute

Frau Bogen

AD ist so
kompliziert!

?

Windows?
Klickibunti!
(Hähö)



Karl Auer



Frans Iskaner



Ellen Bogen



WINone

1.-2.2.2012, MÜNCHEN

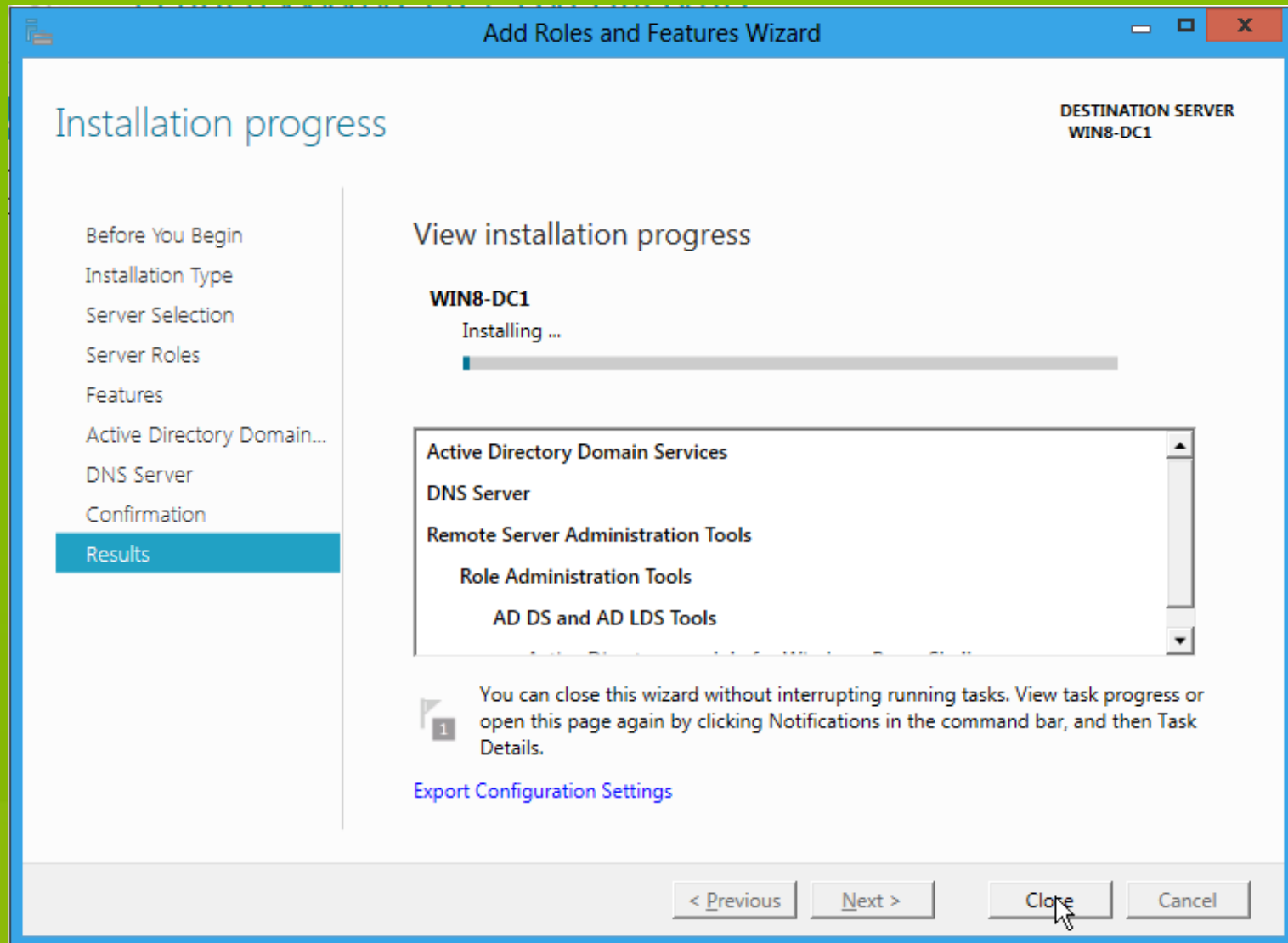


Windows Desktop und Server Konferenz

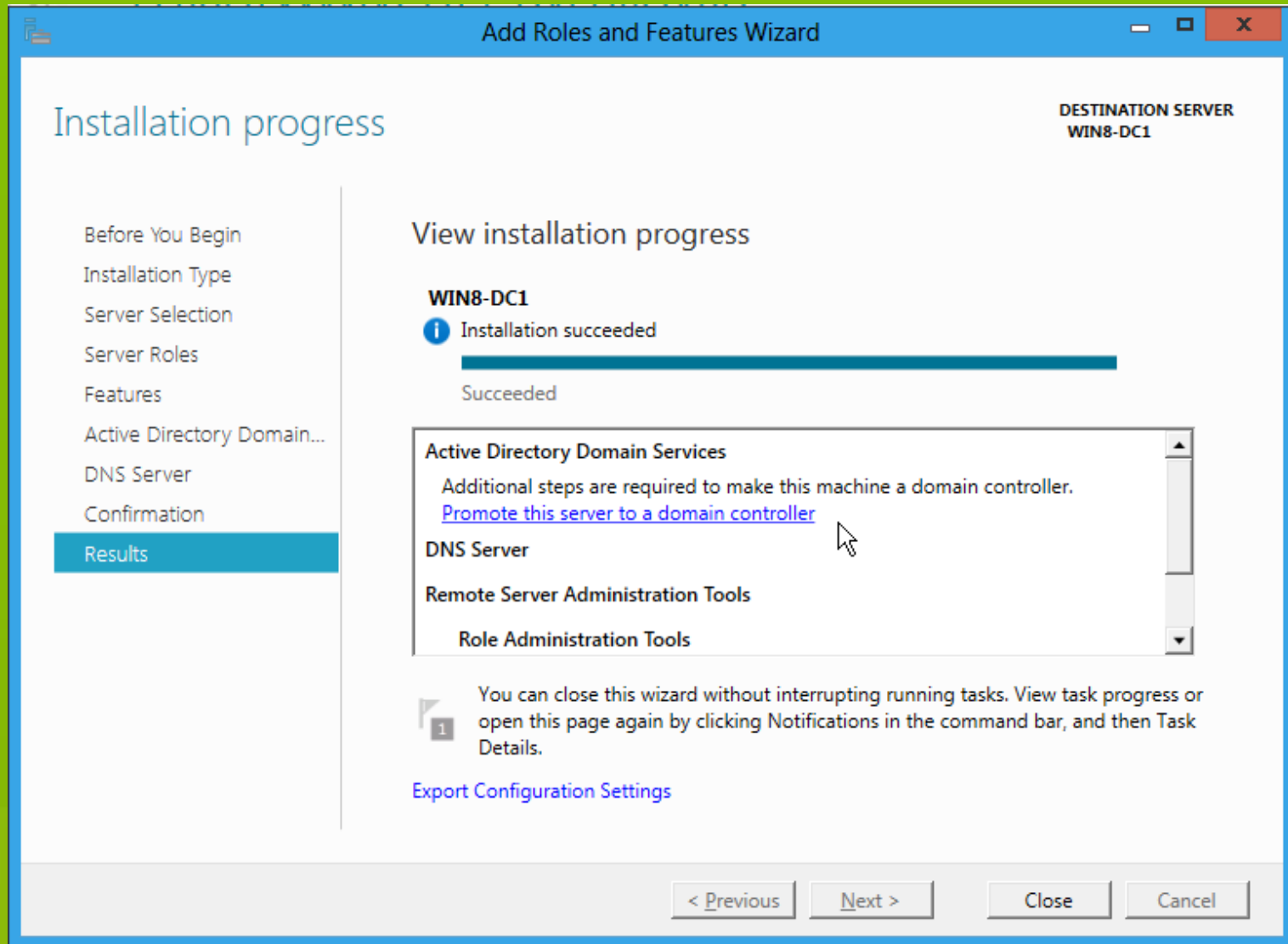
... anfassen

- dcpromo ist weg
- PowerShell für AD

dcpromo im Server-Manager



dcpromo im Server-Manager



Rechtlich flexibel

- Zugriff auf Daten nach Geschäfts-Merkmalen
 - Zugehörigkeit zu Abteilung, Projekt, Rolle ...
 - Art des Zugriffs (Firmen-/Privat-PC ...)
 - Für bestimmte Datentypen
- Flexibler in der Verwaltung
 - Ohne komplexe Gruppen
 - Automatisierung möglich
 - UND-Verknüpfung

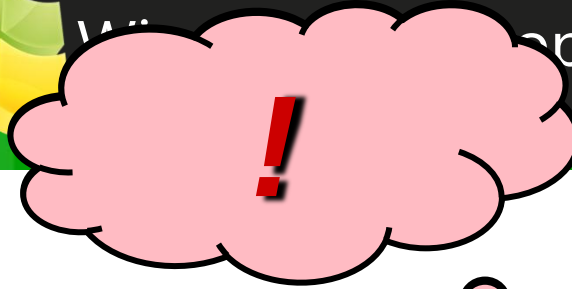


WINone

1.-2.2.2012, MÜNCHEN



Cloud und Server Konferenz



- DC-Snapshots
- DC-Cloning
- ADAC
- Management



Ellen Bogen



WINone

1.-2.2.2012, MÜNCHEN



Windows Desktop und Server Konferenz

FRAGEN?

Wir sehen uns wieder!



Advanced Developers Conference C++

3. – 4. Mai 2012, Zugspitzland

Development for C++ Professionals!

www.adcpp.de



SharePoint Konferenz in Wien

19. – 20. Juni 2012, Wien

ppedv-Konferenz in Kooperation mit

Microsoft Österreich

www.SharePointKonferenz.at

... wir auch:

- CeBIT Security-Konferenz
- heise CeBIT-Forum
- ITA-Training: Windows Server Best Practice
- iX-Workshop Hyper-V
- 5. März, Hannover
- 8. März, CeBIT
- 21. März, München
- 16. April, München
- 15. Mai, Hamburg
- 28. März, Köln
- 13. Juni, München



WINone

1.-2.2.2012, MÜNCHEN



Windows Desktop und Server Konferenz

Ich freue mich auf Ihr Feedback!

Vielen Dank!

Nils.Kaczenski@witstor.de

www.faq-o-matic.net

about.me/Nils.Kaczenski

@Kaczenski