Thomas Kurth
CONSULTANT/ MCSE
Netree AG
thomas.kurth@netree.ch
netECM.ch/blog

Netree AG
IT Consultants

@ThomasKurth_CH

Multimandantenfähige ConfigMgr Infrastruktur

Secunia
Stay Secure

BCD SINTRAG
Ein Unternehmen der ADN® Gruppe
value add distribution

Configuration Manager

Einführung

- Wieso habe ich dieses Thema gewählt?
- Wo ist der Geschäftsnutzen einer Multimandantenfähigen Infrastruktur?

Ziele

- **Wir lernen ConfigMgr Topologien kennen, welche für die Verwaltung von unterschiedlichen Sicherheitszonen optimiert sind.**

Ablauf

- **Infrastruktur Topologie**
- Netzwerkverbindungen / Firewalls
- Lizenzen und ConfigMgr Objekte
- ConfigMgr Konsolenberechtigungen
- Wie setzen wir dies bei der Netree um?

Infrastruktur Topologie

- Funktionen in ConfigMgr 2012
  - MP Zuweisung → R2 CU3
  - SUP Sync → R2
  - Mehrere Network Access Account →R2
  - Push DP
  - DP Bandwidth Controll
- Welche Rollen müssen beachtet werden?
  - SUP, MP, DP
- Workgroup-/Domain-/Forest-Anforderungen

Infrastruktur Topologie

- Single Primary Site für alle
  - Single Server
  - Multiple Server

→ Einfachste Form
Wenig Verwaltungsaufwand
Mehrfachverwendung von Content

- Single Primary Site per Mandant
  - Single Server
  - Multiple Server

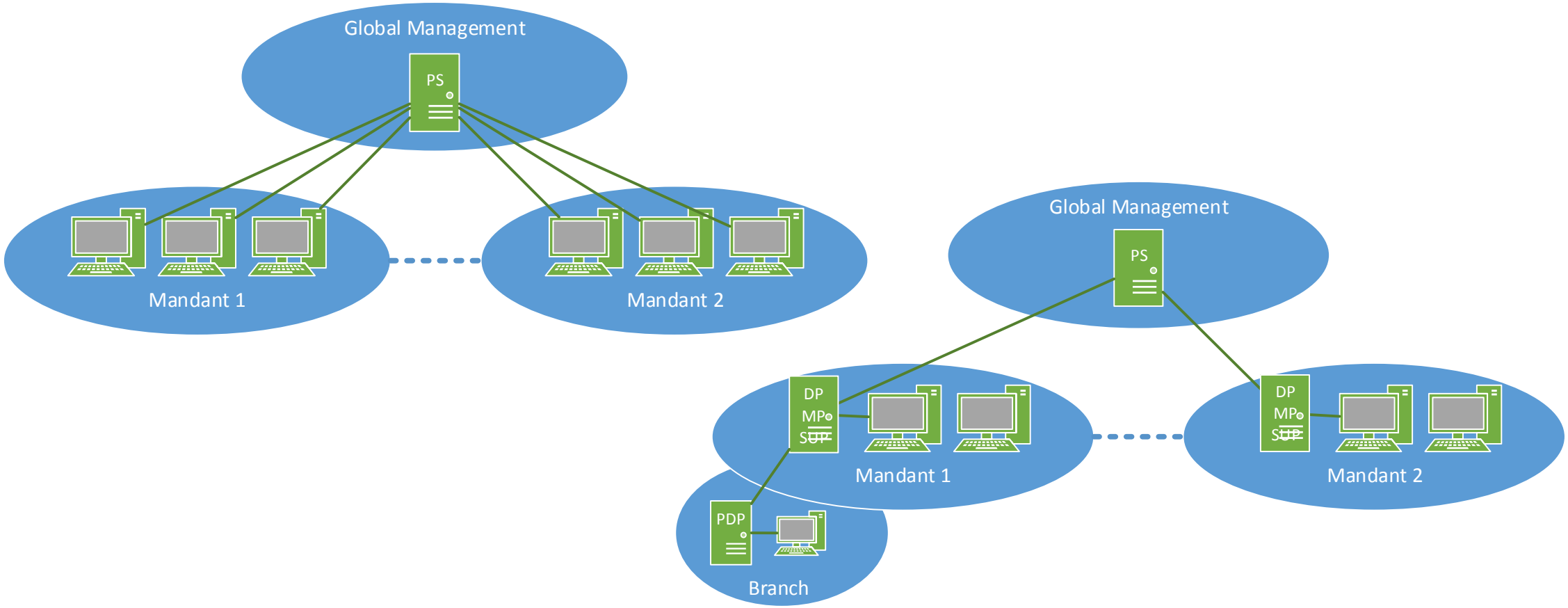
→ Strikte Applikations- und Datentrennung
Hoher Verwaltungsaufwand
Wird deshalb nicht weiter betrachtet!

- Multiple Sites mit Central Site
  - Single Server per Site
  - Multiple Server per Site

→ Mehrfachverwendung von Content
Hosts sind nur auf einer Site sichtbar
Mittlerer Verwaltungsaufwand

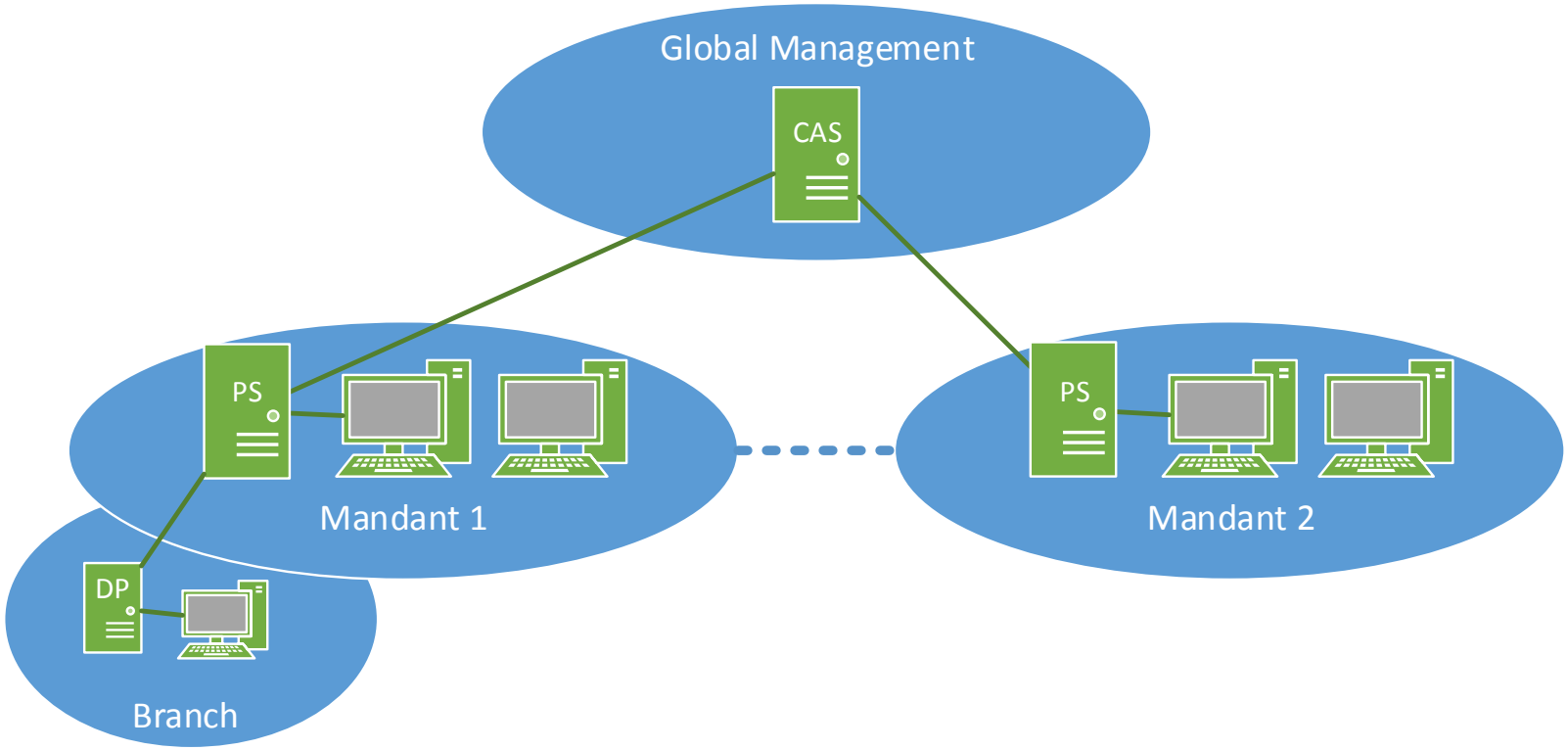
Infrastruktur Topologie

- Single Primary Site Varianten



Infrastruktur Topologie

- Multi Primary Site mit Central Site Variante



Infrastruktur Topologie

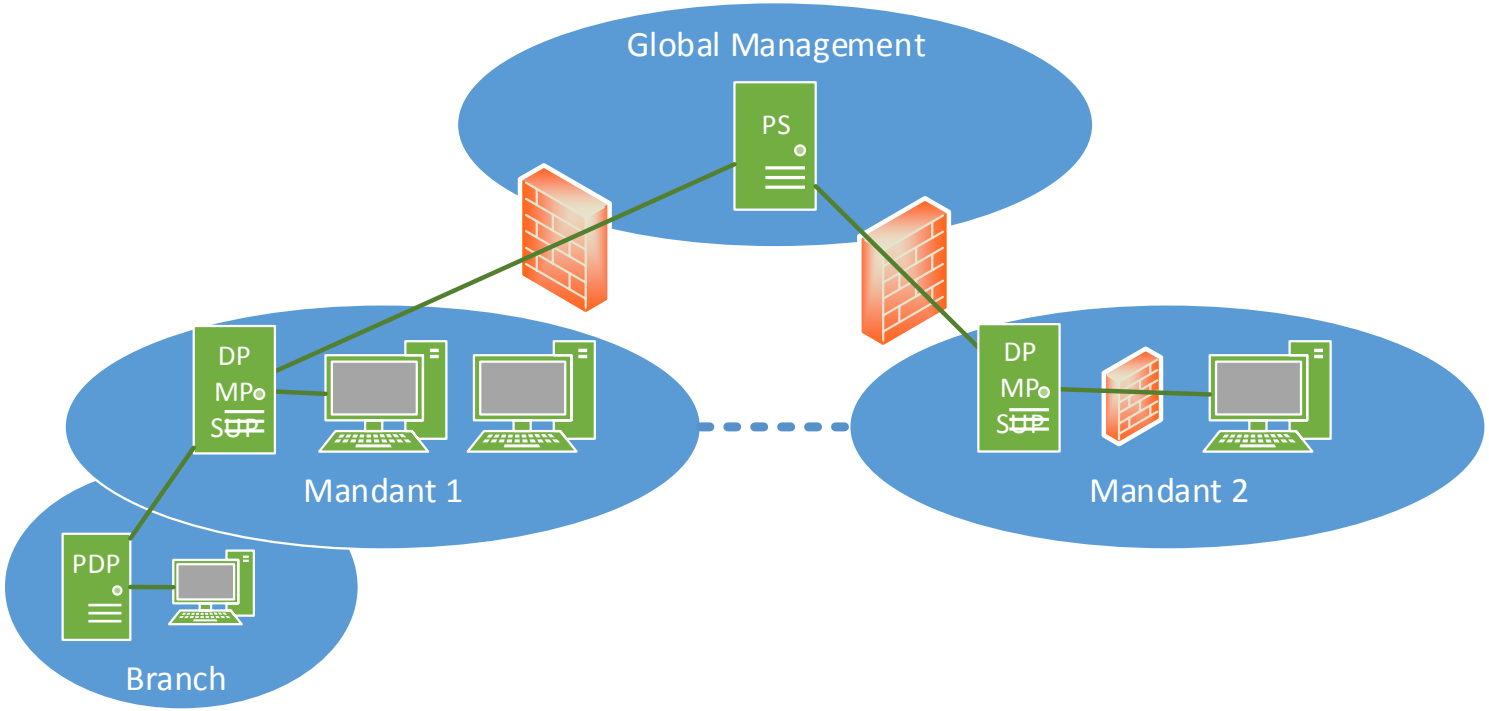
- Clients zu spezifischem Server zuweisen
  - MP → Registry / Compliance Item
    - Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM:AllowedMPs
    - Type: Reg_Multi_SZ
  - DP → Boundaries
  - SUP → Nicht steuerbar
    - http://blogs.technet.com/b/umairkhan/archive/2014/10/03/configmgr-2012-r2-multiple-sup-scenario-clients-not-failing-over-to-the-other-sup.aspx

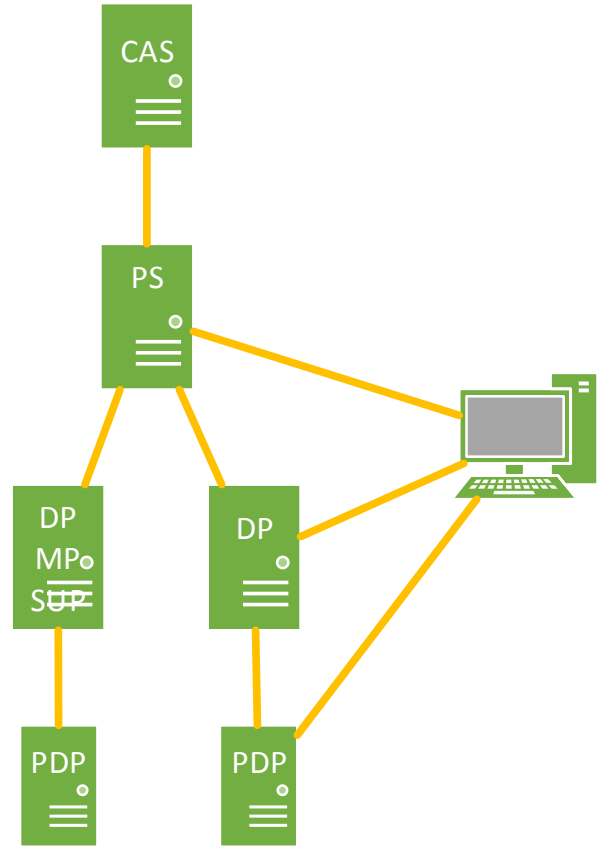
Ablauf

- Infrastruktur Topologie
- **Netzwerkverbindungen / Firewalls**
- Lizenzen und ConfigMgr Objekte
- ConfigMgr Konsolenberechtigungen
- Wie setzen wir dies bei der Netree um?

Netzwerkverbindungen / Firewalls

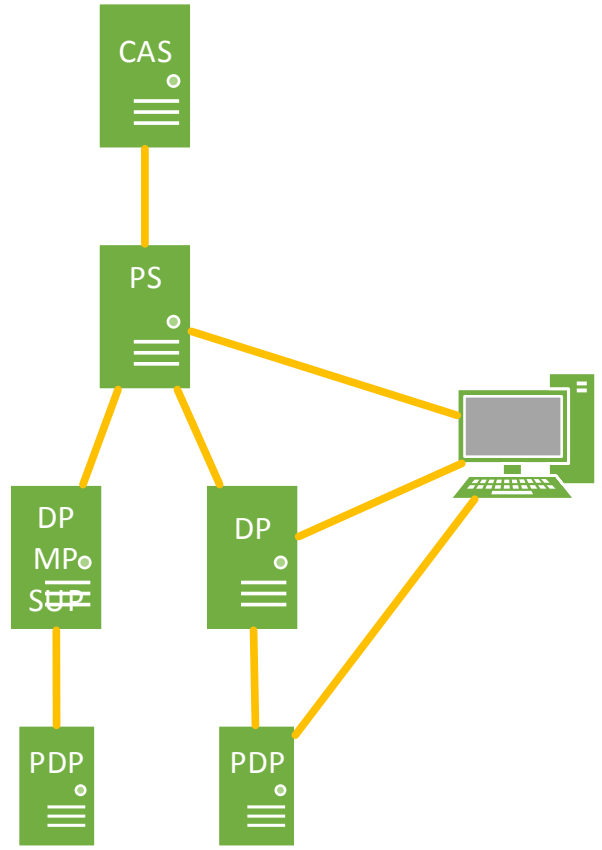
- Unser Ziel ist so wenig Ports wie möglich zu nutzen!





Netzwerkverbindungen / Firewalls

Von	Zu	Ports
PS / DP, MP, SUP	DP, MP, SUP / PS	80, 443 (HTTP/HTTPS) 135, 49152-65535 (RPC) 445 (SMB) 1433 (SQL)
PS	Client	UDP 9 (WoL)
Client	DP, MP, SUP	80, 443 PXE Boot UDP 67, 68, 69, 4011 State Migration 445 (SMB)



Ablauf

- Infrastruktur Topologie
- Netzwerkverbindungen / Firewalls
- **Lizenzen und ConfigMgr Objekte**
- ConfigMgr Konsolenberechtigungen
- Wie setzen wir dies bei der Netree um?

Lizenzen und ConfigMgr Objekte

- ConfigMgr
  - SPLA Lizenzen sobald Kunden(externe) verwaltet werden
  - Server bei Kunden sollten dem Lizenzbesitzer gehören

- Applikationslizenzierung
  - Korrekte Lizenzen pro Kunde verwenden
  - Achtung EULA bei Freeware Tools

- Prüft diese Fragen unbedingt mit eurem Lizenzmanager!!!

Lizenzen und ConfigMgr Objekte

- Lizenz Reports
  - Devices Tattooing
  - Siehe unterlagen des letzten Events https://netecm.netree.ch/blog/Lists/Posts/Post.aspx?ID=86#.VC51Kvl_uz5

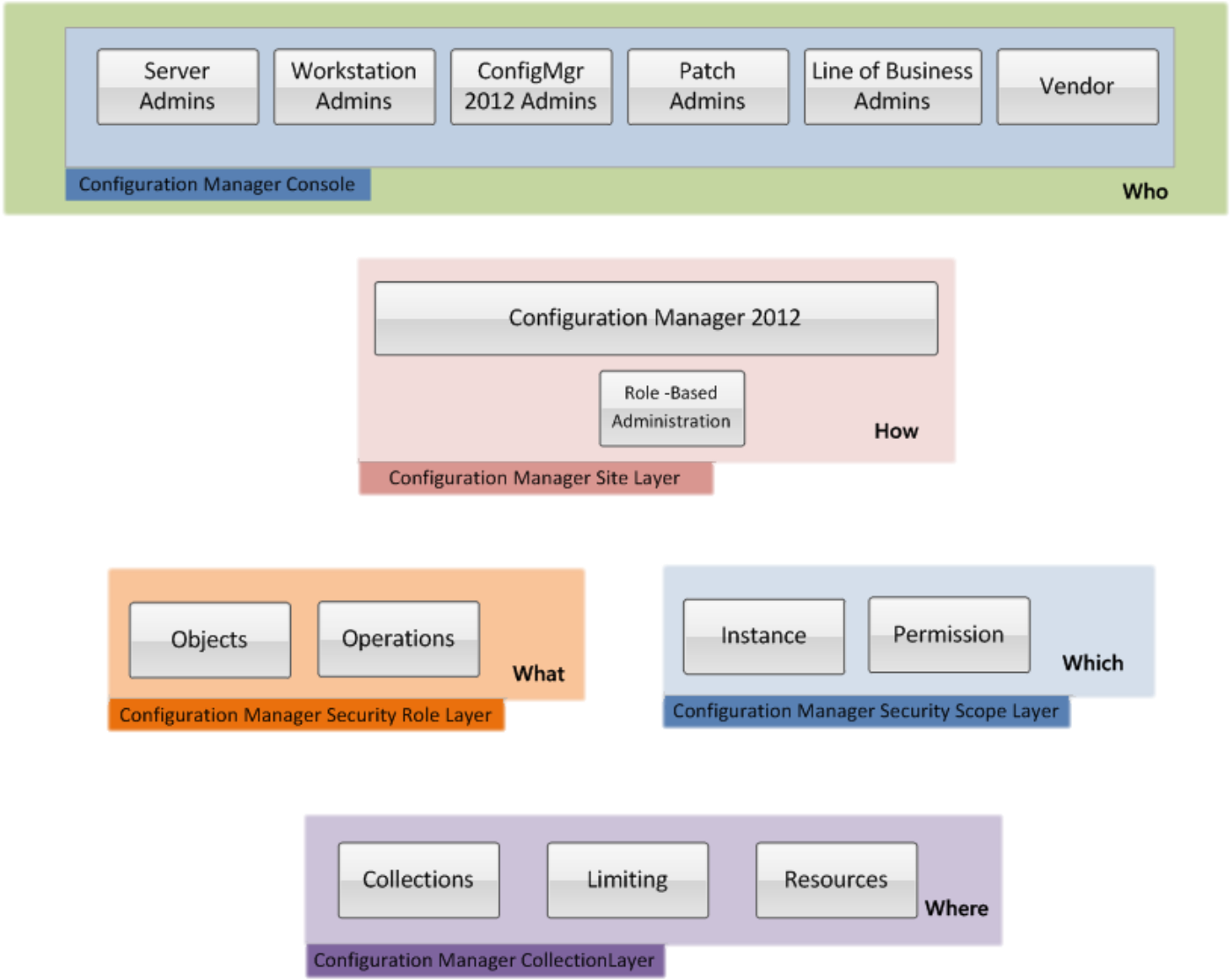
- ConfigMgr Objekte
  - Updates → Keine Lizenzauswirkungen
  - Devices → Keine Lizenzauswirkungen
  - OS → Eigene Images pro Mandant sinnvoll sofern stark abweichend und kein KMS
  - Apps → Aufteilung bei Lizenzierten Apps

Ablauf

- Infrastruktur Topologie
- Netzwerkverbindungen / Firewalls
- Lizenzen und ConfigMgr Objekte
- **ConfigMgr Konsolenberechtigungen**
- Wie setzen wir dies bei der Netree um?

ConfigMgr Konsolenberechtigung

- RBA!?!



ConfigMgr Konsolenberechtigung

- Wer muss überhaupt Zugriff haben?
  - Nur Betreiber → Namenskonzepte
  - Auch MA des Mandanten → Berechtigungen nötig oder Zugriff über eigene Schnittstellen

- Welche Rollen werden benötigt?

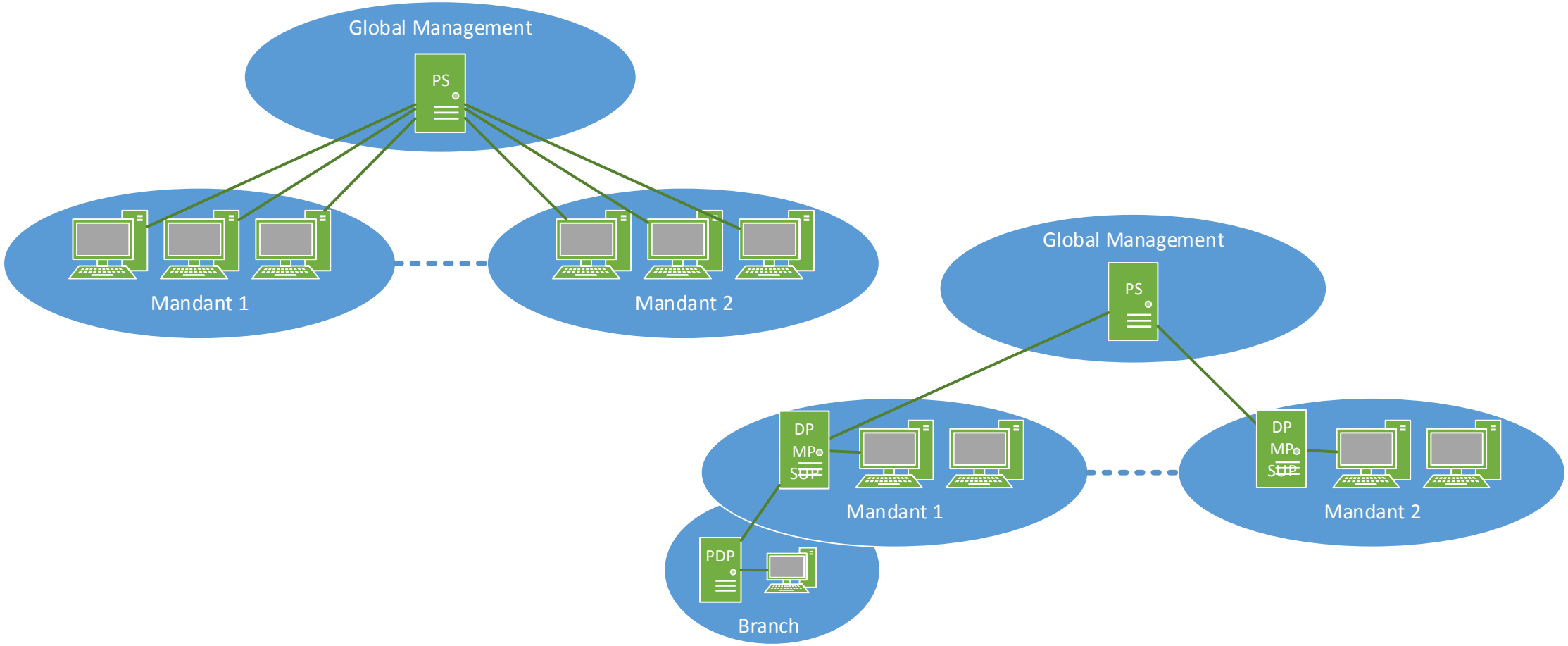
Ablauf

- Infrastruktur Topologie
- Netzwerkverbindungen / Firewalls
- Lizenzen und ConfigMgr Objekte
- ConfigMgr Konsolenberechtigungen
- **Wie setzen wir dies bei der Netree um?**

Wie setzen wir dies bei der Netree um?

- So wenig Server wie möglich → Weniger Verwaltungsaufwand
- So wenige Netzwerkverbindungen wie möglich → Reduzierte Gefahrenquelle
- So wenig Berechtigungen wie möglich → Reduzierte Gefahrenquelle
- So standardisiert wie nur möglich → Weniger Verwaltungsaufwand

So wenig Server wie möglich



So wenige Netzwerkverbindungen wie möglich

- Verbindungen von Clients nur über Port 80, 443 und für Staging TFTP/PXE Ports (67, 68, 69, 4011)
- SMB nur wenn unbedingt benötigt
- Zentraler Server + File Server für Pkg Source

Supplements

- Remote PowerShell Port 5985, 5986 --> Sofern nötig vom PS Server
- Wake on LAN UDP 9

So wenig Berechtigungen wie möglich

Rolle	Beschreibung	Zugriff über	Pro Mandant
SCCM Administrator	Zugriff auf die gesamte Infrastruktur.	Konsole, RDP, Shares, netECM	
Paketierer	Zugriff nur auf den Development Share	Development Share - Modify	X
Applikationsmanager	Überprüft und Kontrolliert Applikationspakete. Registriert diese im ConfigMgr. Testet die erste Zuweisung und mögliche Update Prozesse.	Shares -Modify netECM:APP Konsole -Create, Modify, Delete Apps -Create, Modify, Delete Collection -Create, Modify, Delete Deployments	

So wenig Berechtigungen wie möglich

Rolle	Beschreibung	Zugriff über	Pro Mandant
OSD/OSI Engineer	Stellt die OSD Task Sequencen bereit. Oft wird dies durch die SCCM Administratoren erledigt.	Konsole -Create, Modify, Delete TS, PKG -Create, Modify, Delete Collection -Create, Modify, Delete Deployments netECM:UserDevice -Stager Rolle	
Patch Manager	Managed Windows Updates. Komplette Automatisierung möglich! Oft wird dies durch die SCCM Administratoren erledigt.	Konsole -Create, Modify, Delete Update Groups und Update PKG -Create, Modify, Delete Deployments	
Supporter	Staged Devices und weisst Applikationen zu.	netECM:UserDevice -Supporter Rolle	X

So wenig Berechtigungen wie möglich

- Vereinfachte Schnittstellen für Supporter und Paketierer
  - Erlaubt Outsourcing oder dem Kunden selbst Arbeiten abzugeben
- Namenskonzepte für klare Mandantenauftrennung (Applikationen/OS/Collections)
  - Suffix bei Applikationsnamen
    http://netecm.netree.ch/blog/Lists/Posts/Post.aspx?ID=72
- Keine Scopes benötigt
  - Dynamische Berechtigungen anhand Namenskonzept

So standardisiert wie nur möglich

- Reduktion des Verwaltungsaufwand
  - First-Copy-Costs
  - Alle Mandanten gleich behandeln → Klare Angebotsdefinition
- Namenskonzept für alle Objekte
- Qualitätskontrolle
  - Applikationspakete
  - Deployments → Reports

Zusammenfassung

- Infrastruktur Topologie
- Netzwerkverbindungen / Firewalls
- Lizenzen und ConfigMgr Objekte
- ConfigMgr Konsolenberechtigungen
- Wie setzen wir dies bei der Netree um?

Danke

Herzlichen Dank
Thomas Kurth @ThomasKurth_CH
netECM.ch/blog

Bewertung der Session: Configmgr.ch

- Xing: https://www.xing.com/net/cmce
- Facebook: https://www.facebook.com/groups/411231535670608/
- Linkedin: http://www.linkedin.com
- Twitter: https://twitter.com/configmgr_ch

Nächster Event: Freitag 19. Juni Digicomp Bern
(begrenzte Anzahl Teilnehmer)