# Neuerungen in System Center Endpoint Protection (SCEP) 2012

- Marc Grote
  IT TRAINING GROTE – Consulting und Workshops

# Agenda

- Aus FEP 2012 wird SCEP 2012
- Neuerungen in SCEP 2012
- Neuerungen in SCCM 2012
- Installation und Upgrade

# Aus FEP 2012 wird SCEP 2012

- FCS (Forefront Client Security)
  - MOM als zentrales Management
  - SQL 2005 fuer Datawarehouse
  - Verteilung per Gruppenrichtlinien
- FEP 2010 (Forefront Endpoint Protection 2010)
  - SCCM 2007 R2/R3 als zentrales Management
  - SQL 2005/8 fuer Datawarehouse
- FEP 2012 (Forefront Endpoint Protection 2012)
  - SCCM 2012 als zentrales Management
  - Nie auf dem Markt erschienen, waehrend Beta Phase Produktgruppenwechsel ....
- SCEP 2012 (System Center 2012 Endpoint Protection)
  - SCCM 2012 als zentrales Management
  - Zum Zeitpunkt der Erstellung dieses Vortrags RC (26.12.2011)

# SCEP 2012 Schluesselfunktionen

- Zentrale Verwaltung mit der SCCM-Konsole
- Zentrale Erstellung von AV-Richtlinien
- Hohe Skalierbarkeit, angelehnt an das SCCM Infrastrukturmodell
- Neueste Antimalware- und Rootkit-Erkennung
- Behavioral Threat Erkennung
- Vulnerability Shielding
- Automatic Agent Replacement
- Windows Firewall Management

# Neue Funktionen in SCEP 2012

- Support fuer System Center 2012 Configuration Manager,
  - Integriertes Setup, Management und Reporting
- Role Based Access Control basierend auf SCCM
- SCEP Client ist Bestandteil des SCCM Client
- SCEP Policy Merging
- Client kann mehrere SCEP Policies zugeordnet haben
- Erweiterte Policy Einstellmoeglichkeiten
- Erweiterte Alarmierungs- und Protokollierungsfunktionen
- Verbesserte Signaturverteilung

# Demo

# Neue Funktionen in SCCM 2012

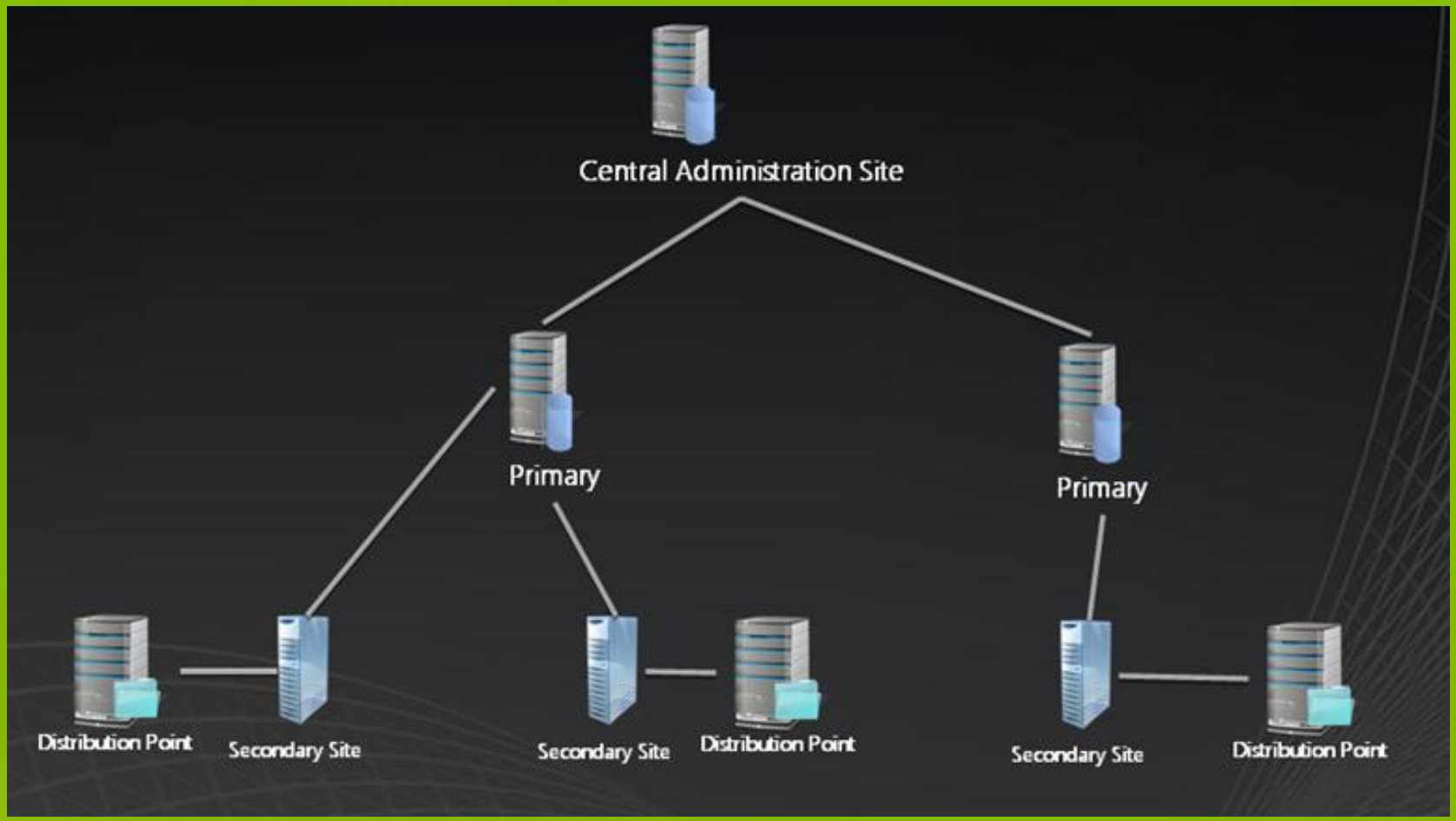
- Neues flaches Administrationsmodell
  - Ein zentraler CAS Server
  - Multiple Primary Flat Sites
- User Centric Management (UCM)
- Software Center
- Rollenbasierte Zugriffssteuerung
- Neue SCCM Konsole
- Unterstuetzung fuer Smartphones
- Und viele mehr ..... (was ich nicht kenne ☹) ... Aber diese Webseite: http://technet.microsoft.com/en-us/library/gg699359.aspx

# SCCM 2012 Anforderungen

- SCCM Server
  - Siehe naechste Folie ☺
- SQL Server
  - SQL 2008 64 Bit
  - SQL 2008 Express on Secondary Sites
- SCCM Client
  - Windows XP SP3, Vista, Windows 7
  - Windows Server 2003
  - Windows Server 2008 / R2

| Operating System ↓ / Roles → | Primary Site Server | Secondary Site Server | Management Point | Distribution Point | Server Locator Point | Site Database Server | Software Update Point | Fallback Status Point | Branch Distribution | State Migration Point | PXE Service Point | System Health Validator | Out -of-band Service Point | Asset Intelligence Synchronization | SMS Provider Computer | Reporting Services Point | Client Status Reporting Host Sys | Multi-cast Server | Central Administration Site | Mobile Device Management | Web Software Library |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Windows Server 2003 Standard Edition SP1 64-bit | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Enterprise Edition SP1 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Enterprise Edition SP1 64-bit | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Datacenter Edition SP1 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Datacenter Edition SP1 64-bit | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Storage Server Edition SP1 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Standard Edition R2 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Standard Edition R2 64-bit | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Enterprise Edition R2 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Enterprise Edition R2 64-bit | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Web Edition SP2 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Standard Edition SP2 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Standard Edition SP2 64-bit | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Enterprise Edition SP2 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Enterprise Edition SP2 64-bit | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Datacenter Edition SP2 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Datacenter Edition SP2 64-bit | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2003 Storage Server Edition SP2 | Ø | Ø | Ø | √[2] | Ø | Ø | Ø | Ø | √ | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø | Ø |
| Windows Server 2008 Standard Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 Enterprise Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 Datacenter Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows 2008 R2 (Windows 7 Server) | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 R2 Standard Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 R2 Enterprise Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 R2 Datacenter Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 R2 SP1 Standard Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 R2 SP1 Enterprise Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |
| Windows Server 2008 R2 SP1 Datacenter Edition 64 Bit[1] | √ | √ | √ | √[2] | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ |

# SCCM 2012 Hierarchie




Source: http://myitforum.com/cs2/blogs/jrobb259/simplify2_1FDE892B.png

# SCEP 2012 Anforderungen

- SCEP Server
  - Windows Server 2008 mit SP2 x64
  - Windows Server 2008 R2
  - System Center EP 2012 (CAS oder Standalone Primary)
  - SQL 2008 SP1 mit CU 10
- SCEP Console
  - Windows XP SP2 oder hoeher
  - Windows Server 2003
  - Windows Vista / 7 / 8 ☺
  - Windows Server 2008 / R2

# SCEP 2012 Anforderungen

- SCEP Reports
  - SCCM Reporting Point
- SCEP Client
  - Windows XP SP3, Vista, Windows 7
  - Windows Server 2003
  - Windows Server 2008 / R2

# SC / SCEP Lizenzierung

| Edition | Components Included |
| --- | --- |
| Microsoft System Center 2012 Datacenter | • Operations Manager<br>• Configuration Manager<br>• Data Protection Manager<br>• Service Manager<br>• Virtual Machine Manager<br>• Endpoint Protection*<br>• Orchestrator<br>• App Controller*<br>*New Component Introduced with System Center 2012 |
| Microsoft System Center 2012 Standard | |

Alle Details: http://download.microsoft.com/download/1/1/1/11128EC7-2BE7-480C-9D46-4ECECA9E481A/System%20Center%202012%20Licensing%20Datasheet.pdf

# SC / SCEP Lizenzierung

| | Datacenter | Standard |
|---|---|---|
| # of physical processors per license | 2 | 2 |
| # of Managed Operating System Environments (OSEs) per license | Unlimited | 2 |
| Includes all System Center server management components | ✓ | ✓ |
| Right to run management server software and supporting SQL Server Runtime | ✓ | ✓ |
| Manage any type of supported workload | ✓ | ✓ |
| Open No Level (NL) License and Software Assurance (L&SA) 2-year price | $3,607 | $1,323 |

# SCEP Deployment

- SCCM 2012 Installation
- AD Vorbereitungen
- SCCM Discovery Methoden konfigurieren
- SCCM Site Boundaries / Boundary Group konfigurieren
- Neue SCCM Device Collection erstellen
- SCCM Endpoint Protection Point hinzufuegen
- Endpoint Protection Policy erstellen und den Device Collections zuweisen
- SCCM Client deployen
- SCEP Deployment abwarten / Monitoring / Troubleshooting

# Demo

# Wenn es mal Probleme gibt ...

- SCCM Server Logs
  - CCM.LOG → Client Configuration Manager Tasks
  - SMSEXEC.LOG → All Site Server Components
  - Und Dutzende andere mehr ....
- SCCM Console
  - Site Status
  - Component Status
- Client Logs
  - C:\Windows\CCM\Logs
  - CCMEXEC.LOG → Client Aktivitaeten/ SMS Agent Host
  - Und Dutzende andere mehr ....
  - C:\ProgramData\Microsoft\Microsoft Security Client\Support
    - EPPSetup.log → SCEP Master Logfile
    - MSSecurity*.* → Antimalwareservice Logfiles

# Demo

# Migration von FEP 2010 zu SCEP 2012

- SCCM 2012 kann in die bestehende SCCM 2007 Implementierung integriert werden (Site by Site) → Migrationtasks
- FEP-Policy Migration durch Ex- und Import ☺
- Policy SCEP Default wird automatisch zu allen SCCM Sammlungen zugewiesen
- Ausrollen des SCCM Client(Updates)
  - Existierender Client muss nicht erneut ausgerollt werden
- FEP 2010 zu SCEP 2012 Reporting Migration
  - FEP 2010 Security Reports werden nicht migriert
- Nach der Migration werden alle SCEP Clients als „Deployed“ angezeigt

# 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

# Hat Ihnen mein Vortrag gefallen?
# Ich freue mich auf Ihr Feedback!

# Vielen Dank!

Marc Grote

# Kontakt

- **Marc Grote**
- E-Mail: grotem@it-training-grote.de (7*16*365)
- Web: http://www.it-training-grote.de
- Blog: http://blog.it-training-grote.de
- XING: https://www.xing.com/profile/Marc_Grote2
- Mobile: 0176/23380279 (manchmal)
- MSN: Was ist das? ☺
- Twitter: Nicht mit mir
- Facebook: Face was?