midpoints
purify it

DNUG 05.2011

Extending Lotus Traveler

Detlev Pöttgen
midpoints GmbH

midpoints
purify it

Detlev Pöttgen

Solutions Architect & Consultant
Gesellschafter |Geschäftsführer

midpoints GmbH
http://www.midpoints.de

IBM Advanced Business Partner
IBM Design Partner for Domino Next
IBM Mobile Design Partner
Apple Enterprise Developer Program

Schwerpunkte:
- Notes / Domino Consulting
- E-Mail Management
- Notes / Domino & mobile App Entwicklung

- We mobilize Notes
  (Lotus Traveler Planung & Implementierung
  App Entwicklung & Apple iOS Device Management)

Blog: http://www.netzgoetter.net

midpoints purify it

Agenda

- Fragen und Herausforderungen von Traveler Projekten
- In den letzten 6 Monaten 20 zum Teil mehrtägige Workshops mit Kunden zu Traveler & Apple iOS im Unternehmen
- Zwei große Traveler Projekte im 1.H 2011 die jetzt im Rollout sind mit einmal 3.000 bzw. 1.200 Endgeräten
- Seit 3 Jahren verantworten wir den Traveler Rollout bei Miele mit aktuell 750 Endgeräten

midpoints purify it

Agenda

Extending Lotus Traveler

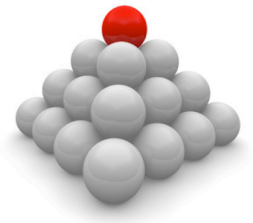
- Ausfallsicherheit, Failover, Backup

- Verteilte Umgebung | Zentraler Betrieb

- Wer darf welche Endgeräte benutzen?

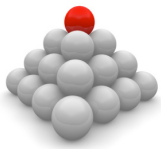
- Verwaltung der Endgeräte

Ausfallsicherheit, Failover, Backup

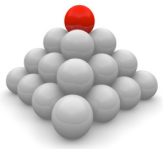


Ausfallsicherheit, Failover, Backup

- Lotus Traveler 8.5.2.2 ist nicht Clusterfähig
- Der Domino Server unterhalb von Traveler natürlich schon, aber Traveler selbst nicht.
- Daher kein natives Failover oder Lastverteilung möglich
- Häufige Kundenanforderung, da Push-Mail wichtig und zuverlässig funktionieren muß.

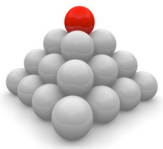


- Um im Worst Case Ausfallzeiten zu minimieren, bleiben nur zwei Möglichkeiten übrig:
  - Wenn ich Traveler in einer virtuellen Umgebung betreibe, die Möglichkeiten bzgl. Failover-Funktionen der Virtualisierungsplattform benutzen.
  - Ein zweites Hot-Stand-By Gerät fertig konfiguriert als schnell verfügbare zweite Instanz einsetzbar zu haben.

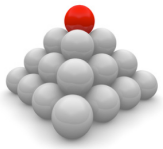


midpoints purify it
Ausfallsicherheit, Failover, Backup

- Kann ich die zweite Instanz zur Lastverteilung verwenden?
- Also User zum Beispiel per DNS Round Robin oder vorgeschaltetem Load Balancer auf beide Maschinen verteilen?
- N-E-I-N !!! Und versuchen Sie es erst gar nicht.

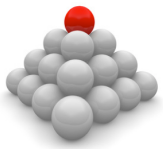


- Warum geht das nicht?
- Traveler speichert das Synchronisationsprotokoll und die Geräte & Security-Einstellungen nicht in einer Lotus Datenbank (die ich replizieren könnte) sondern in einer lokalen File-basierten Java Derby SQL-Datenbank
- Diese State-DB ist an die installierte Traveler Instanz gebunden.

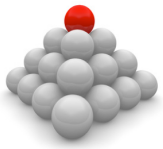


midpoints purify it
Ausfallsicherheit, Failover, Backup

- Wechselt das Endgeräte von Trav01 auf Trav02, werden auf dem Trav02 in der State-Datenbank keine aktuellen Informationen für das Endgerät gefunden.
- Traveler veranlasst dann einen erneuten ersten Prime-Sync.
- Damit werden alle Daten auf dem Endgerät verworfen und neu synchronisiert.
- Der Benutzer merkt dies, da ein Prime-Sync einige Zeit dauert.



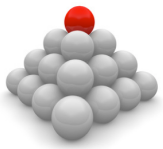
- Eine dynamische Lastverteilung ist somit nicht möglich.
- Wichtig auch für Backup & Restore
- Sichern Sie den Traveler-Ordner im Data-Verzeichnis, aber sorgen Sie dafür, das Sie die Derby-State-Datenbank vom Restore ausnehmen.
- Wenn Sie eine veraltete State-Datenbank zurücksichern, werden eh auf allen Endgeräten Prime-Syncs ausgeführt.
- Beim Restore sichern Sie keine State-Datenbank zurück, sondern lassen Traveler eine neue aufbauen. Die Endgeräte haben Ihre Konfiguration lokal gespeichert und führen automatischen einen Prime Sync aus.

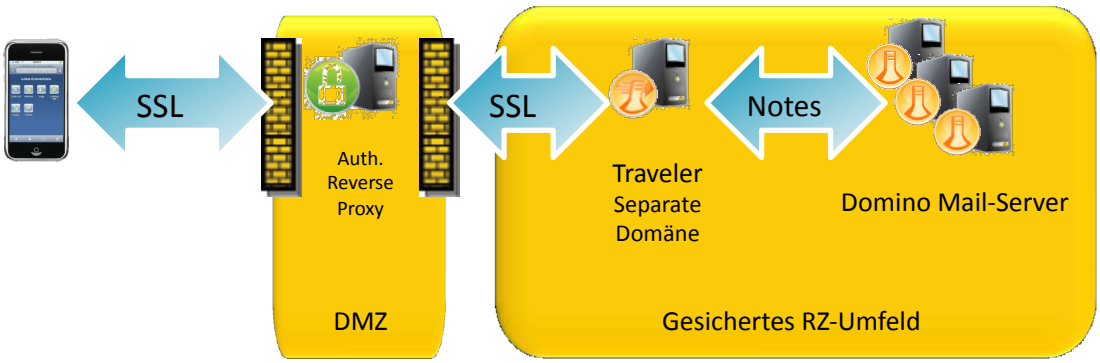


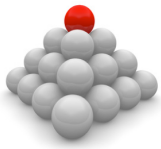
midpoints purify it

Ausfallsicherheit, Failover, Backup

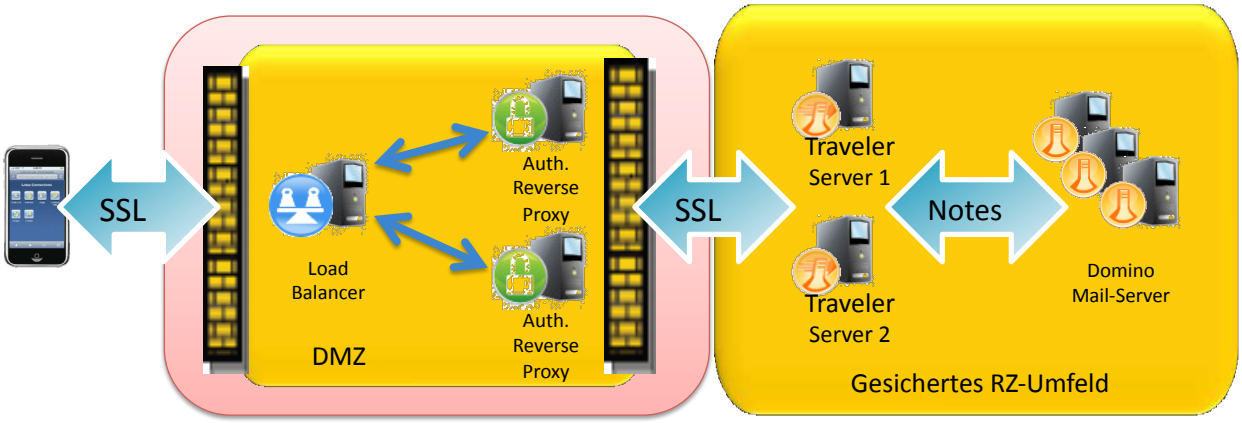
- Beispiel aus der Praxis:
- Rahmenbedingung: 3.500 User bis Ende 2011
- Traveler Server nicht virtualisiert sondern Hardware
- Ausfallzeit bzw. Wechsel auf ein neues System innerhalb von max. 5 Minuten.
- Wichtig der Wechsel muß einfach ohne Eingriffe in die Domino Infrastruktur möglich sein.



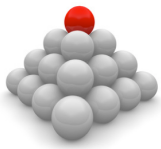


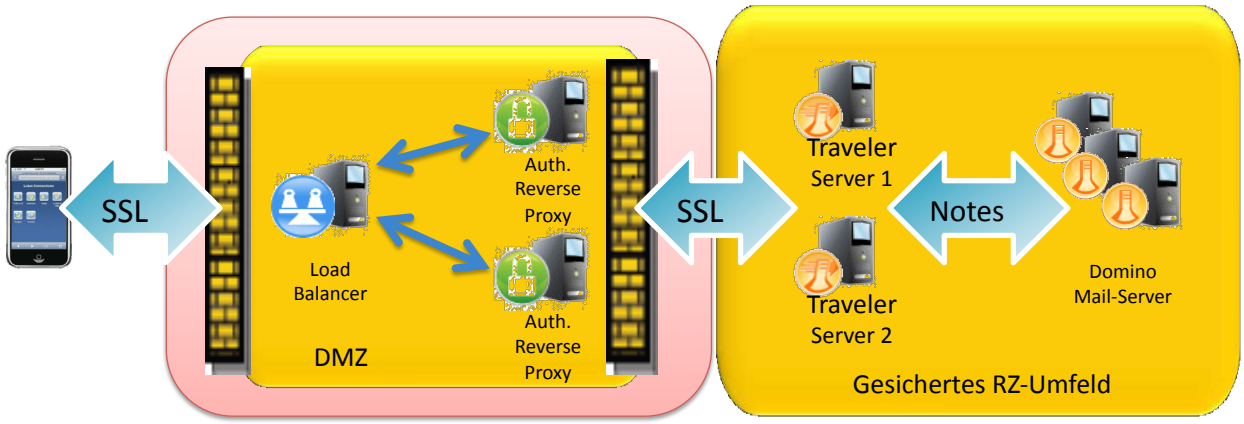


midpoints purify it
Ausfallsicherheit, Failover, Backup

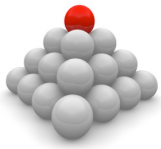


- Die Reverse Proxys leiten Anfragen immer an den gleichen Traveler Server weiter.
- Beide Traveler Server sind gleich & fertig konfiguriert

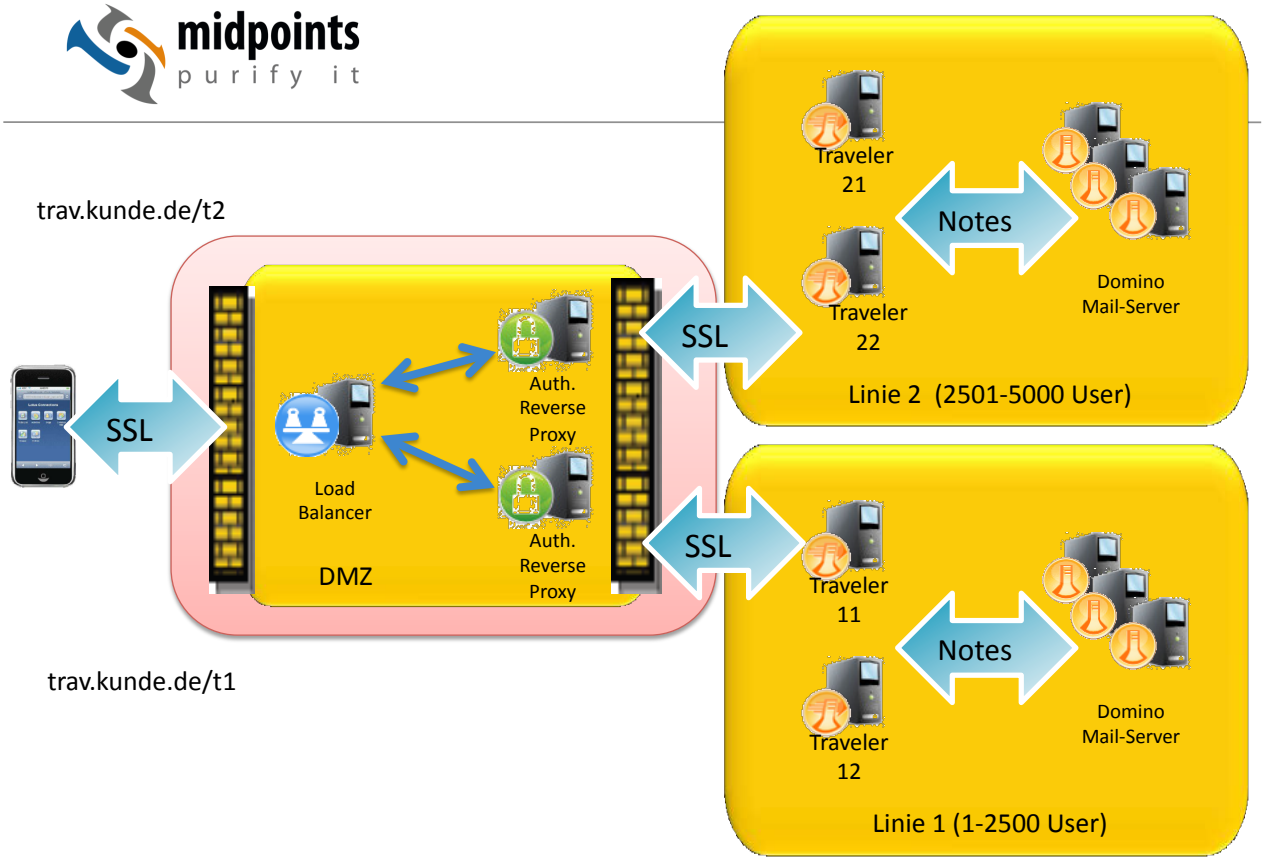




Die Traveler Server Hardware ist für 2.500 Endgeräte pro Instanz ausgelegt. Für 2.500 Endgeräte ist somit obige Umgebung ausreichend



midpoints purify it



midpoints
purify it

Verteilte Umgebungen | Zentraler Betrieb

midpoints
purify it

Verteilte Umgebungen | Zentraler Betrieb

- Ich habe eine verteilte Domino Umgebungen mit:
  - Mehreren Standorten
  - Lokale Administratoren
  - Unterschiedliche Administrationsrollen (Helpdesk)
- Kann ich eine zentrale Traveler Umgebung betreiben oder benötige ich pro Standort einen eigenen Server?

- Kann ich eine zentrale Traveler Umgebung betreiben oder benötige ich pro Standort einen eigenen Server?
  - Abhängig von der Netzinfrastruktur und Verbindungsqualität zwischen Zentrale und Lokation
  - Generell es ist ausreichend eine zentrale Traveler Umgebung zu betrieben.
  - Sichern Sie diesen ab und setzen Ihre Sicherheitstandards durch.

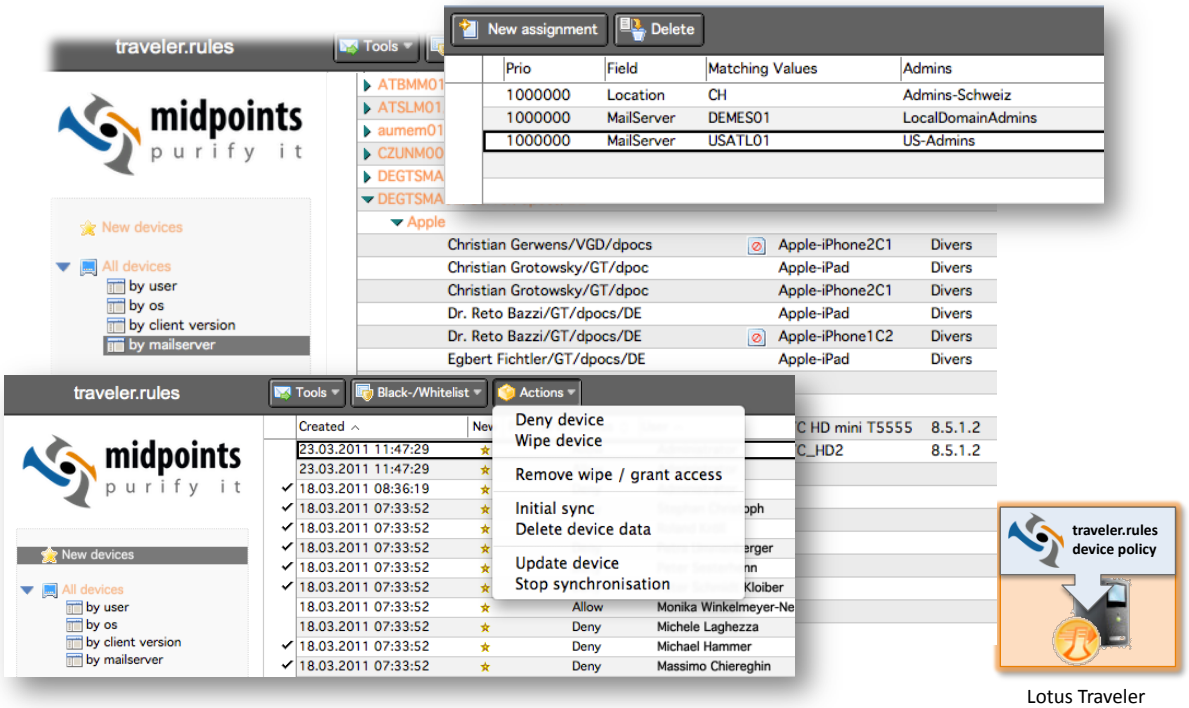
midpoints purify it
Verteilte Umgebungen | Zentraler Betrieb

- Traveler bietet keine „Mandanten“-fähige oder Rollen basierte Administration.
  - Jeder sieht alles in der LotusTraveler.nsf
  - Soll jemand Traveler spezifische Aktionen ausführen (Device sperren, wipen oder eine Sperre zurücknehmen) werden Konsolenberechtigungen benötigt.
  - Ein Wipe sollte schnellst möglich ausgeführt werden können. Am besten direkt vom Helpdesk. Somit braucht jeder Helpdesk-Mitarbeiter Konsolenberechtigungen.
  - Will ich das?

- Dies Thema wurde in fast jedem unserer Traveler Projekte angesprochen und es wurde ein Lösung benötigt.

- Wir nutzen in unseren Projekten eine einfach einzurichtende Notes Anwendung, die die Traveler Administration erweitert und eine zentrale Traveler Installation „Mandanten“-fähig macht und eine Rollen basierte Administration ermöglicht

Verteilte Umgebungen | Zentraler Betrieb



Lotus Traveler

Wer darf welche Endgeräte benutzen?

- Die Traveler Zugriffssteuerung ist User-basiert.
- Über eine Gruppe, die im Domino Server Dokument des Traveler Servers hinterlegt ist, wird gesteuert wer Traveler benutzen kann.
- Dies ist in vielen Kundensituationen nicht ausreichend.
- Es gibt keine praktikable Möglichkeit gezielt nur bestimmte Devices für die Verwendung von Traveler freizugeben.

Wer darf welche Endgeräte benutzen?

- Wie bei Blackberry möchte ich eigentlich für genau dies Device diesem Notes User Zugriff auf seine Mail ermöglichen.
- Wenn der User die Traveler Zugangsdaten kennt, kann er sich auch auf einem zweiten (privaten) Endgerät Traveler einrichten.
- Drei Lösungen die mit Traveler nativ funktionieren würden, aber nicht praktikabel sind.

Wer darf welche Endgeräte benutzen?

- Lösung 1:
  Sie verwenden SSL-Client Zertifikate

- Vorteil:
  Neben den Zugangsdaten benötigen Sie noch auf dem Endgerät das zugehörige Zertifikat

- Nachteil:
  Aufwendige Administration (Zertifikatsmanagement)
  Wie bringe ich die Zertifikate auf das Endgerät?

Wer darf welche Endgeräte benutzen?

- Lösung 2:
  Sie lassen nur den Zugriff per VPN zu

- Vorteil:
  Wenn VPN auf den Endgeräten eingerichtet ist, ist es sicher.

- Nachteil:
  Aufwendige Administration (VPN-Umgebung & in der Regel damit verbundenes Zertifikatsmanagement)
  Gibt es für die Devices VPN Clients?
  Wie integriert ist die VPN-Lösung (Stichwort: Anmeldung)?
  Wie bringe ich die Zertifikate auf das Endgerät?

Wer darf welche Endgeräte benutzen?

- Lösung 3:
  Sie schauen täglich in die LotusTraveler.nsf und sperren fremde Geräte

- Vorteil:
  Das geht bei 10 Geräten und Sie können Ihre regelmäßigen Kaffeepausen gut nutzen.

- Nachteil:
  Nicht praktikabel bei vielen Endgeräten
  Wenn Sie dort ein Gerät sehen, sind die Daten bereits auf dem Gerät

Wer darf welche Endgeräte benutzen?

- Diese Kontrolle und die Zugriffssteuerung ist sehr sehr wichtig

- Wenn Sie festlegen können, das nur dieses Endgerät von genau diesem Notes User verwendet werden kann UND natürlich SSL verwendet wird, dann:

  - Ist Ihre Traveler Umgebung, ähnlich sicher wie Blackberry.
  - Sie brauchen sich nicht um SSL-Client-Zertifikate kümmern.
  - VPN ist für Traveler allein nicht notwendig.

Wer darf welche Endgeräte benutzen?

- Wir haben lange mit der IBM persönlich diskutiert und einige Travelerprojekte drohten daran zu scheitern.
- Unsere Motivation hier eine sichere Lösung zu schaffen, die inzwischen Erfolgreich bei unseren Traveler Projekten eingesetzt wird.
- Wir ermöglichen ein Realtime White- bzw. Blacklisting von Devices

Lotus Traveler

Wer darf welche Endgeräte benutzen?

- Generell verbieten wir alle Devices und erlauben anhand von White-List-Regeln den Traveler-Zugriff.
- Berechtigungsebenen

  Notes User | Device | Devicetyp

- So ist es möglich:
  - Frank Mustermann mit seinem Dienst-iPad freizugeben
  - Frank Mustermann mit seinem privat iPhone zu sperren

Lotus Traveler

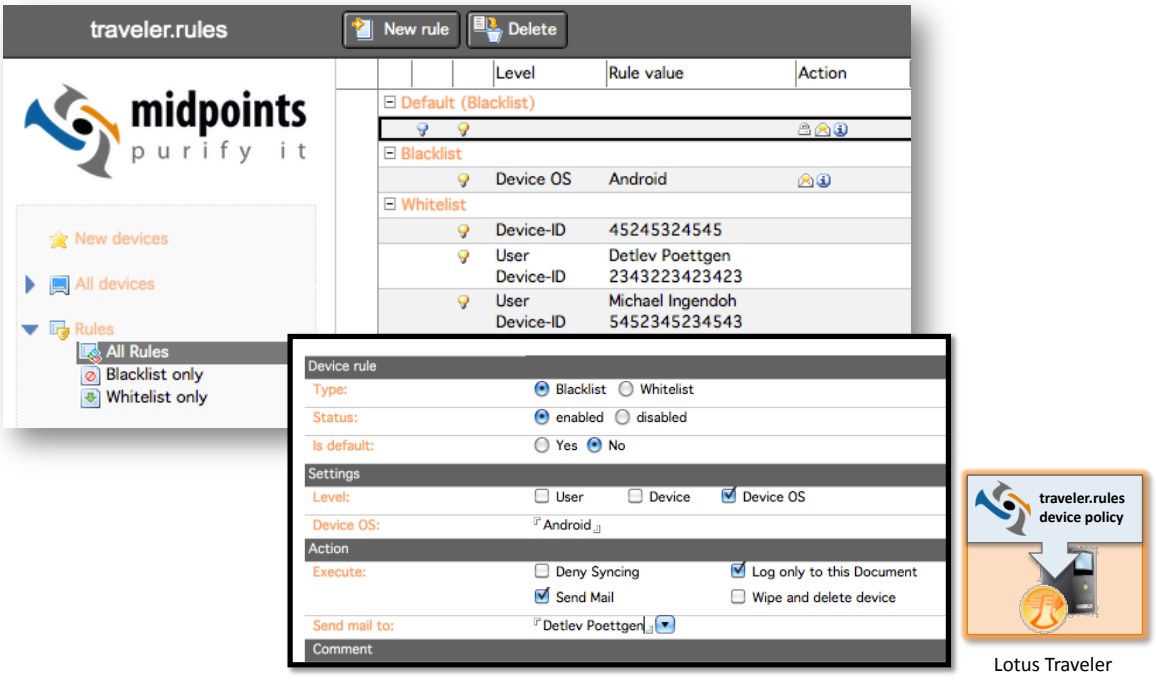
Wer darf welche Endgeräte benutzen?

- Registriert sich ein neues Gerät und verstößt gegen eine Regel, kann automatisch
  - das Gerät gesperrt
  - eine Mail an einen definierten Administrator geschickt
  - das Gerät direkt ge-wiped

  werden. Dies geschieht in Realtime.

Lotus Traveler

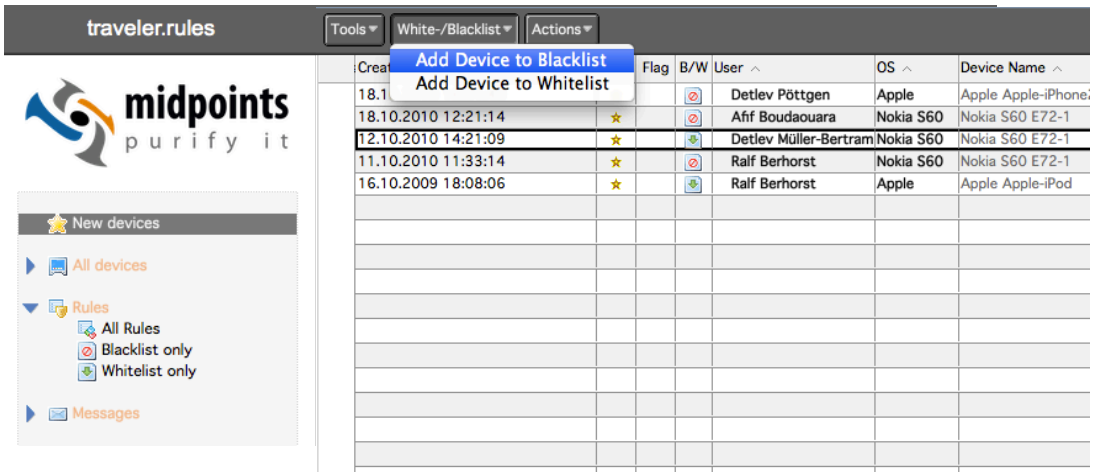
Wer darf welche Endgeräte benutzen?



Lotus Traveler

midpoints
purify it

Wer darf welche Endgeräte benutzen?



Lotus Traveler

midpoints
purify it

Verwaltung der Endgeräte

- Traveler ermöglicht mir mit den Traveler Policy Security Settings eine Grundsicherheit, wie
  - Passcode Erzwingung & Komplexität
  - Storage-Card Verschlüsselung
- Wipe eines Endgerätes

midpoints purify it
Verwaltung der Endgeräte

- Darüber hinausgehende Dinge (insbesondere für Apple Devices) müssen von Hand auf dem Endgerät eingerichtet werden. Um hier einige zu nennen:
  - Restriktionen (YouTube, iTunes-Store, App-Installation)
  - WLAN
  - VPN
  - Sicherheitseinstellungen
  - Mail
  - Inhouse App-Verteilung

- Wie dies mit Apple Devices geht, habe ich auf der Herbstkonferenz gezeigt. Dort bin ich im Detail auf die Möglichkeiten und das **Wie** eingegangen.
  Als Stichwort hier zusammengefasst:

  – Eine Erstkonfiguration für kleine Umgebungen kann ich mit Apple Bordmitteln automatisieren (iPhone Configuration Utility)
  – Bei großen Rollouts kommt man um eine Device Management von Drittanbietern nicht drum herum.

midpoints purify it
Verwaltung der Endgeräte

- Vor der Auswahl einer Device Management Lösung ist es wichtig die Anforderungen zu definieren:

  – Was will & muß ich auf dem Device einschränken?
  – Was darf ich auf dem Device einschränken?

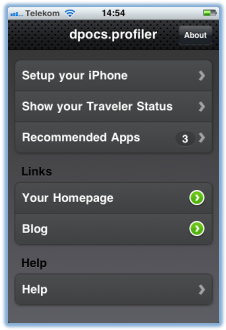
  – Welche Einstellungen & Apps müssen eingerichtet werden?
  – Benötige ich Over-the-Air Funktionen?
  (Inventarisierung, Compliance, unintended Profile Update)

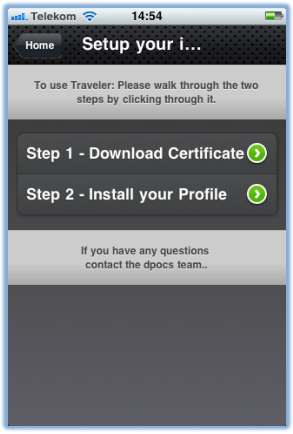
- In unseren Projekten benutzen wir für die Erstkonfiguration von iPhone & iPads eine eigene Lösung, die das Apple iPhone Configuration Utility (iCU) ersetzt.
  - Reine Domino Lösung, die als Beispiel mit auf dem Traveler-Server betrieben werden.
  - Es werden User spezifische dynamische Konfigurationen erzeugt, die gezielt Usern zugewiesen werden.
  - Beinhaltet alle Funktionen & Parameter die über das iCU verfügbar sind.

midpoints purify it

Verwaltung der Endgeräte

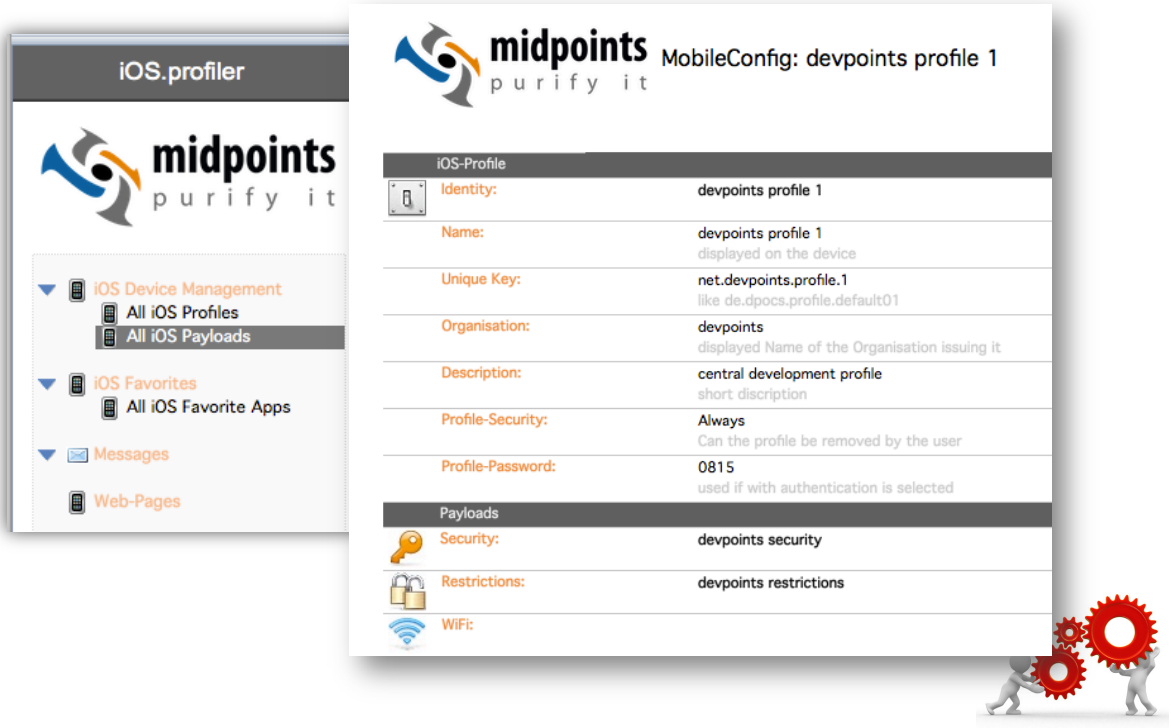
- Zur Erstkonfiguration wird dem User idealerweise per SMS eine URL geschickt. Diese wird geöffnet geöffnet und der User meldet sich mit seinem Noteszugangsdaten an.





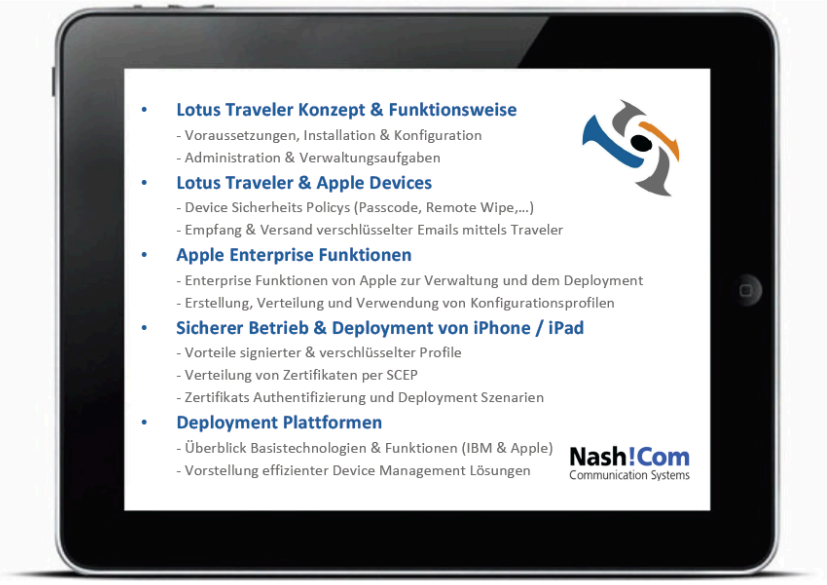
midpoints purify it

Verwaltung der Endgeräte



midpoints purify it

Workshop:
Lotus Notes Traveler & iPhone | iPad im Unternehmen



08.06.11 – Hagen	28.06.11 - München
22.06.11 – Hamburg	29.06.11 - Stuttgart
23.06.11 – Berlin	14.09.11 – Fulda

midpoints
purify it

Vielen Dank!

Mein Blog
(Präsentation + Links):

http://www.netzgoetter.net