8MAN for vSphere

# SICHERHEIT IN DER PRIVATE CLOUD

Dank der private Cloud ist IT-Infrastruktur ein Service, auf den jederzeit problemlos zugriffen werden kann – und diese Verfügbarkeit birgt Risiken. Benötigte man früher immerhin den Schlüssel zum Serverschrank, um beliebige Manipulationen vorzunehmen, reicht bei virtuellen Maschinen ein Passwort oder eine Überberechtigung, um einen kompletten Server zu entwenden.

Gut 300 Rechte werden auf virtuellen Maschinen verwaltet. Hier den Überblick über Gruppen und Gruppenmitgliedschaften zu behalten ist schwierig, redundante Berechtigungen aufzudecken, selbst bei sorgfältigster Arbeit, beinahe unmöglich.

## VORTEILE

| SEHEN UND AUFDECKEN | BEST PRACTICES |
|---|---|
| Wer darf wo was und welche Rechte sind delegiert? Schnell erkennbar ist dies dank der klaren Benutzer-oberfläche. | Standardarbeitsdarbeitsabläufe ermöglichen einen Soll-Ist -Vergleich mit der Nutzerrolle. |
| Auf welchem Weg hat jemand ein Recht erlangt? | Nutzerrollen können dadurch schneller verglichen werden. |
| Wer gehört zu einer Gruppe, anzeigen der Gruppenzugehörigkeiten? | Die Einarbeitungszeit in ein bestehendes Rechtekonzept wird vermindert. |
| Gibt es unnötige Berechtigungs-pfade bzw. Redundanzen und Überberechtigungen? | Die klare Darstellung beugt dem Entstehen von Fehl- und Überberechtigungen vor. |

8MAN
FOR VSPHERE

# BERECHTIGUNGSMANAGEMENT für VMware vSphere™

Viele Fragen können mit dem vSphere Client nur umständlich geklärt werden, zum Beispiel: Wer darf wo was? Welche Rechte sind an wen delegiert? Inwieweit verursacht die Mitgliedschaft in mehreren Gruppen redundante Berechtigungen?

## ALLES AUF EINEN BLICK

Alle Rechte eines Nutzers werden übersichtlich dargestellt.

## BEST PRACTICES

Für Standardarbeitsabläufe, d.h. für bestimmte Funktionen, werden genau die Rechte vorgeschlagen, die ein Nutzer üblicherweise braucht. Best practices sparen nicht nur Zeit, sie ermöglichen auch beim Qualitätsmanagement einen schnellen Überblick.

Auch benötigte Rechte für Drittherstellertools wie von Symantec und Quest werden im best practices check abgebildet!

## PERSPEKTIVEN WECHSELN

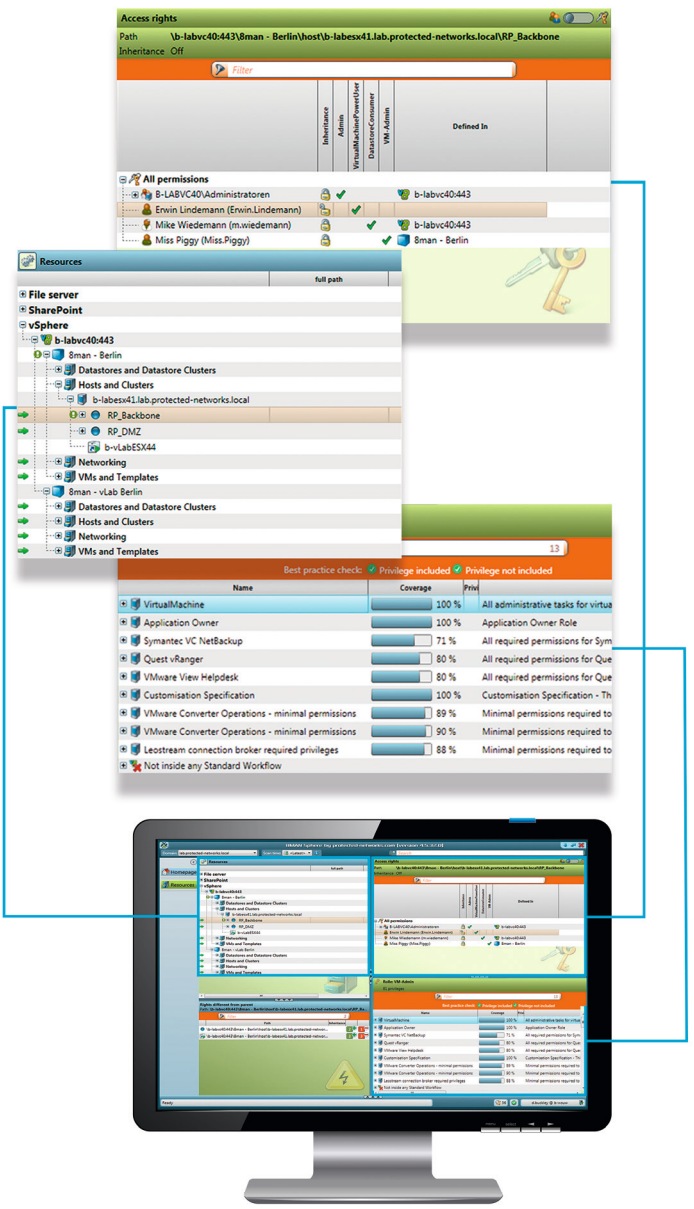
Mit ein paar Mausklicks kann sich der Admin in die Rolle des Nutzers versetzen, d.h. er sieht, wie die Oberfläche für den Nutzer aussieht, ohne dessen Daten zu sehen. Dadurch hat er eine Übersicht über dessen Rechtesituation und kann Auswirkungen von Rechtveränderungen antizipieren.

## SICHERHEIT FÜR KUNDEN UND PARTNER

Kunden, Partnern und Auditoren kann gezeigt werden, wer auf ein Kundensystem zugreifen kann und auch, auf welchem Weg, bzw. aufgrund welcher Gruppenzugehörigkeiten.

## EFFIZIENZ SERIENMÄSSIG

Ein neuer Admin braucht keine Schulungen oder lange Einarbeitungszeiten, um das Rechtekonzept zu verstehen. Best practices bündeln das Wissen von 8MAN wie vSphere -Spezialisten und machen das Berechtigungsgeschäft signifikant schneller.




## Über uns:

**protected-networks.com wurde in Berlin im Jahr 2009 gegründet und entwickelt 8MAN, eine integrierte Softwarelösung für die Verwaltung von Zugriffsrechten in Windows Umgebungen.**

**www.8man.com**


## Deutschland (Hauptsitz)

protected-networks.com GmbH

Alt-Moabit 73
10555 Berlin

Tel. +49 (0) 30 390 63 45 - 0
Fax +49 (0) 30 390 63 45 - 51

info@protected-networks.com
www.protected-networks.com

## UK

protected-networks.com
1 Stanhope Gate
Camberley, Surrey , GU15 3DW

+44 (0) 1276 919 989
uk@8man.com