michael wessel
it performance

Woher kennt mich die Cloud?

Authentifizierung in Web-Umgebungen

Nils Kaczenski

Ellen Bogen und die Wolken am

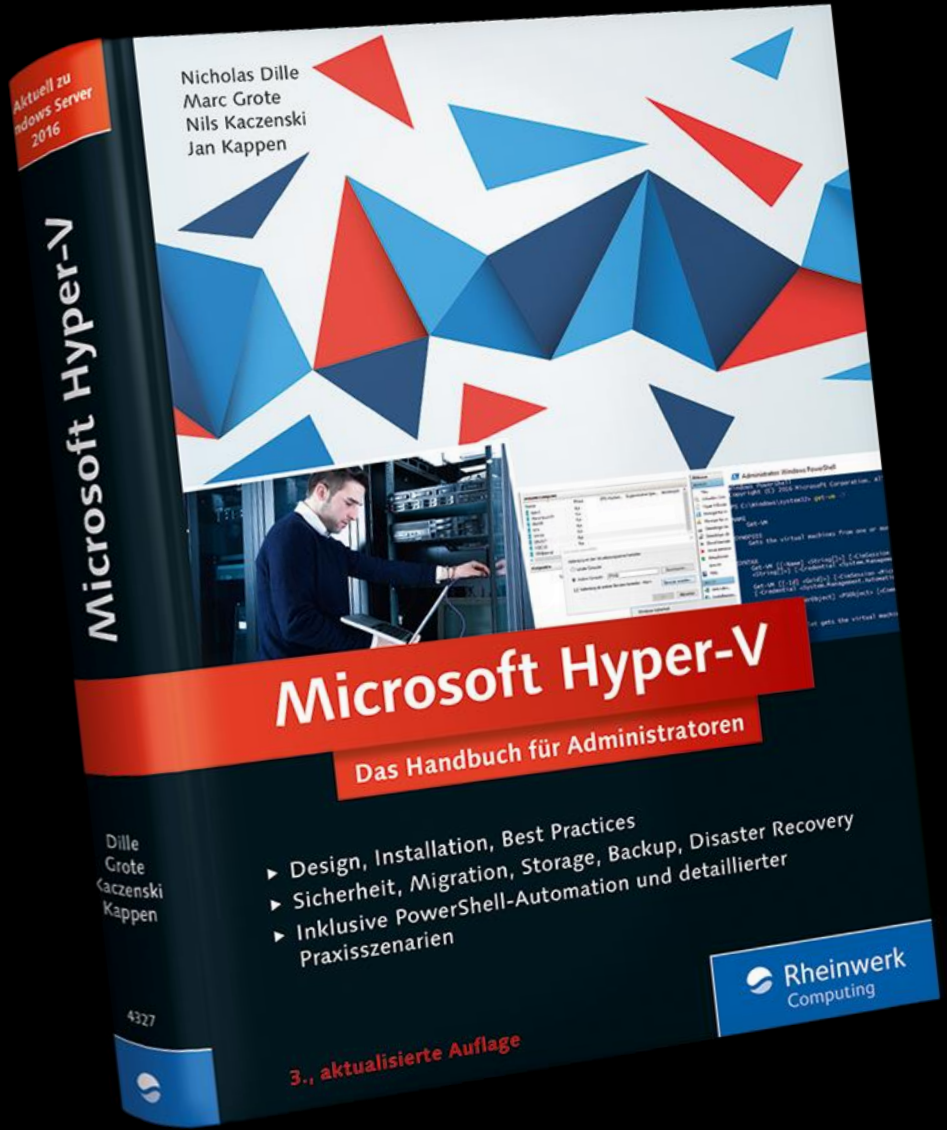
michael wessel
it performance

Johannes Beere

Ellen Bogen


FAQ-O-MATIC.net
michael wessel
it performance
MVP
Microsoft®
Most Valuable
Professional

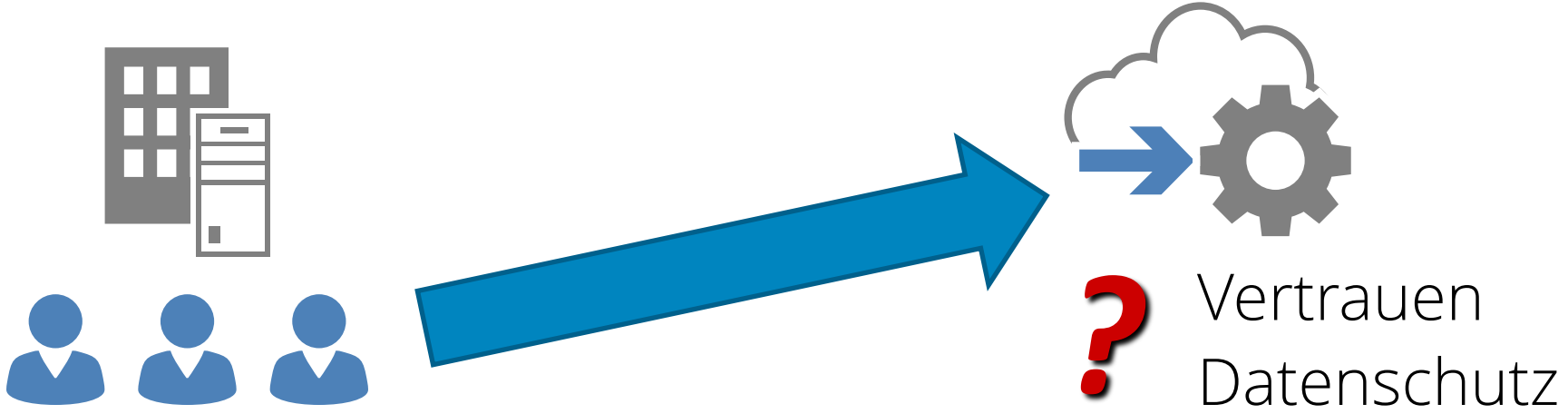
michael wessel
it performance


Aktuell zu Windows Server 2016
Microsoft Hyper-V
Dille
Grote
Kaczenski
Kappen
4327
Nicholas Dille
Marc Grote
Nils Kaczenski
Jan Kappen
Microsoft Hyper-V
Das Handbuch für Administratoren
Design, Installation, Best Practices
Sicherheit, Migration, Storage, Backup, Disaster Recovery
Inklusive PowerShell-Automation und detaillierter Praxisszenarien
Rheinwerk Computing
3., aktualisierte Auflage

Los geht’s!

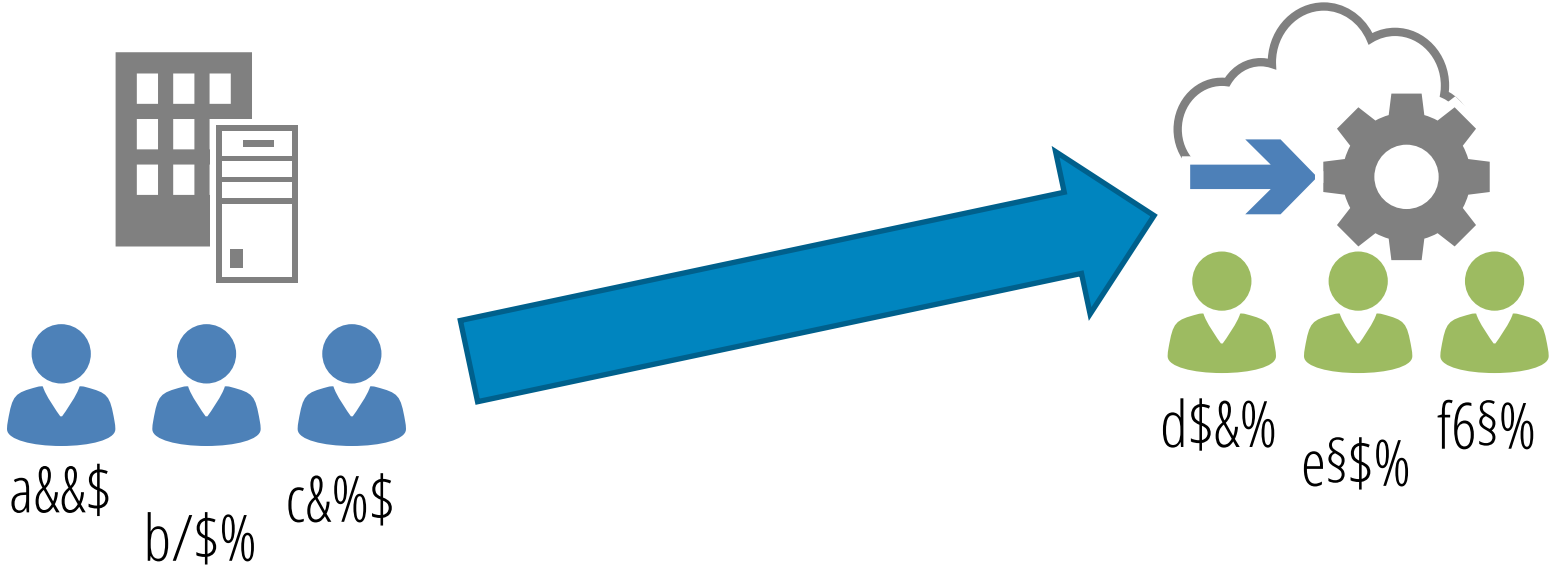
Das Wolken-Dilemma

michael wessel
it performance

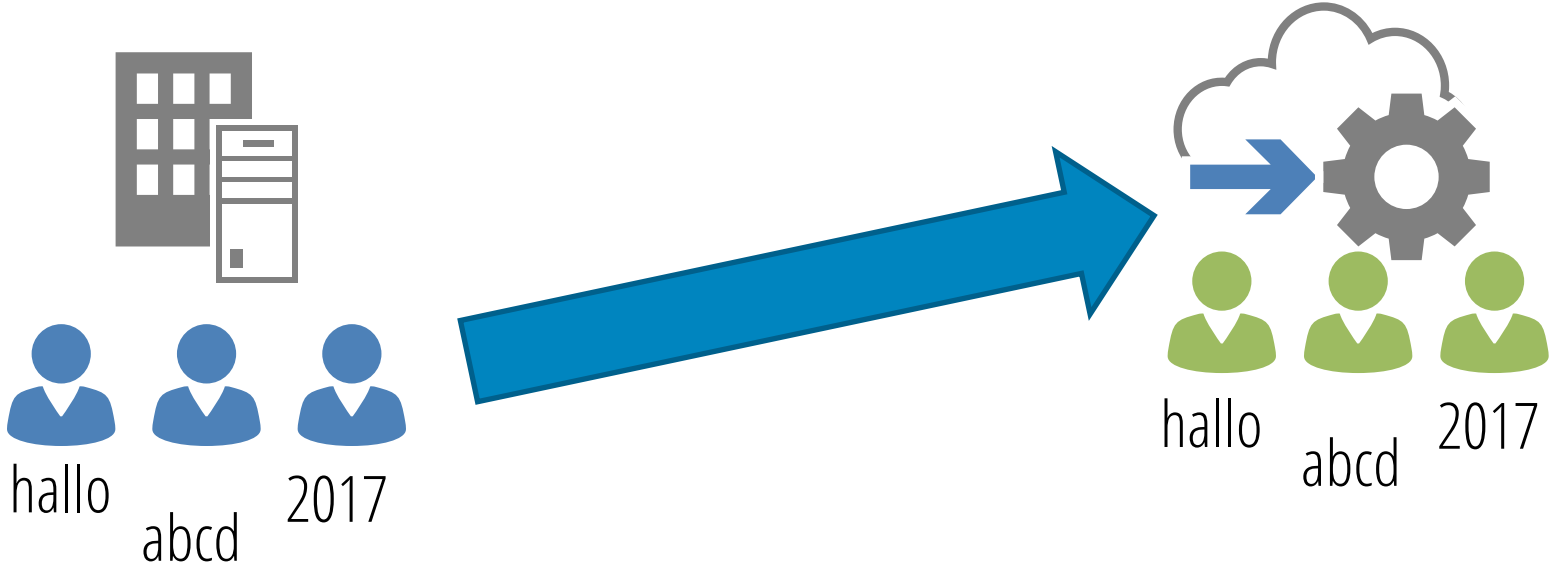


Das Wolken-Dilemma

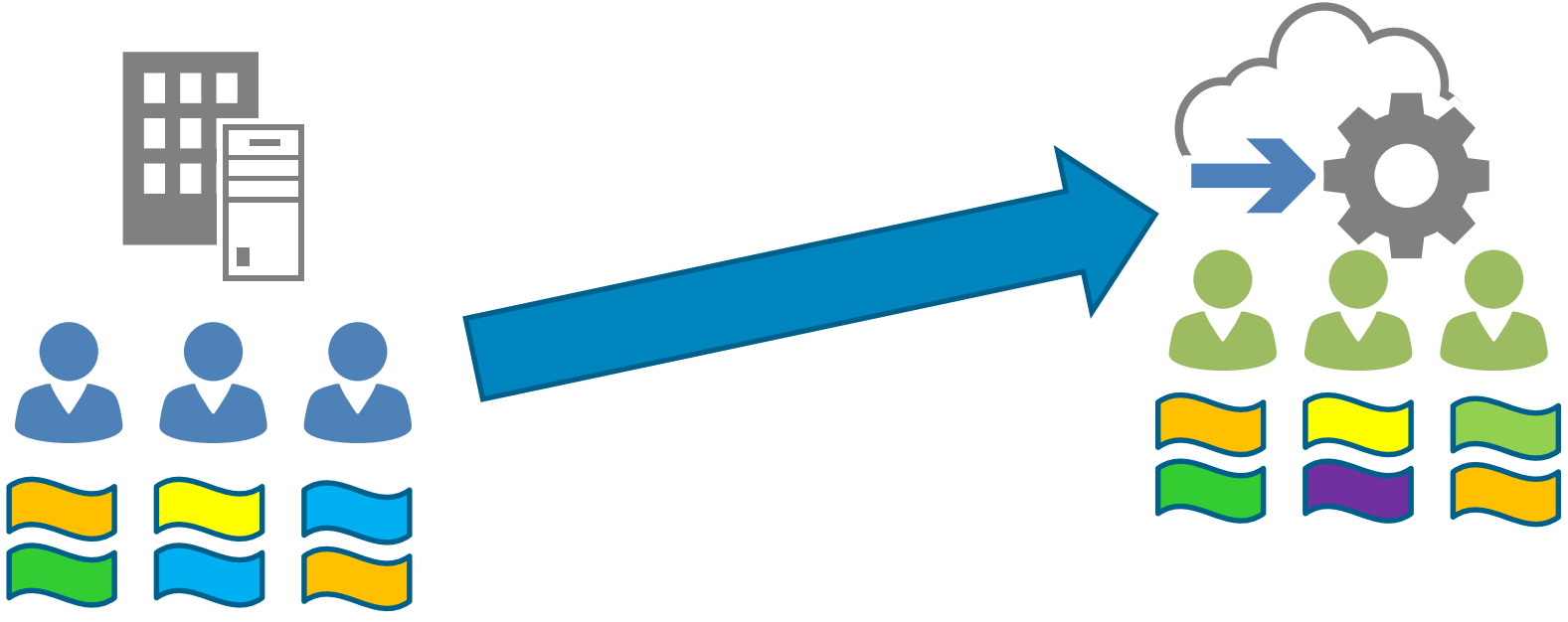
michael wessel
it performance



Das Wolken-Dilemma

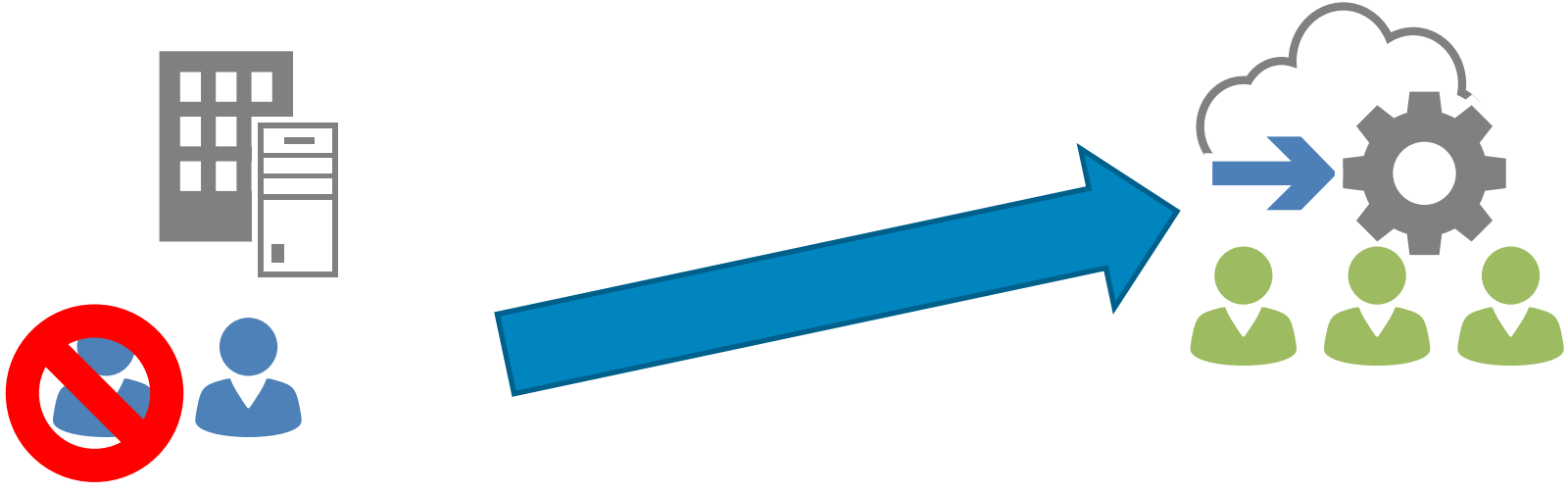


Das Wolken-Dilemma



Das Wolken-Dilemma

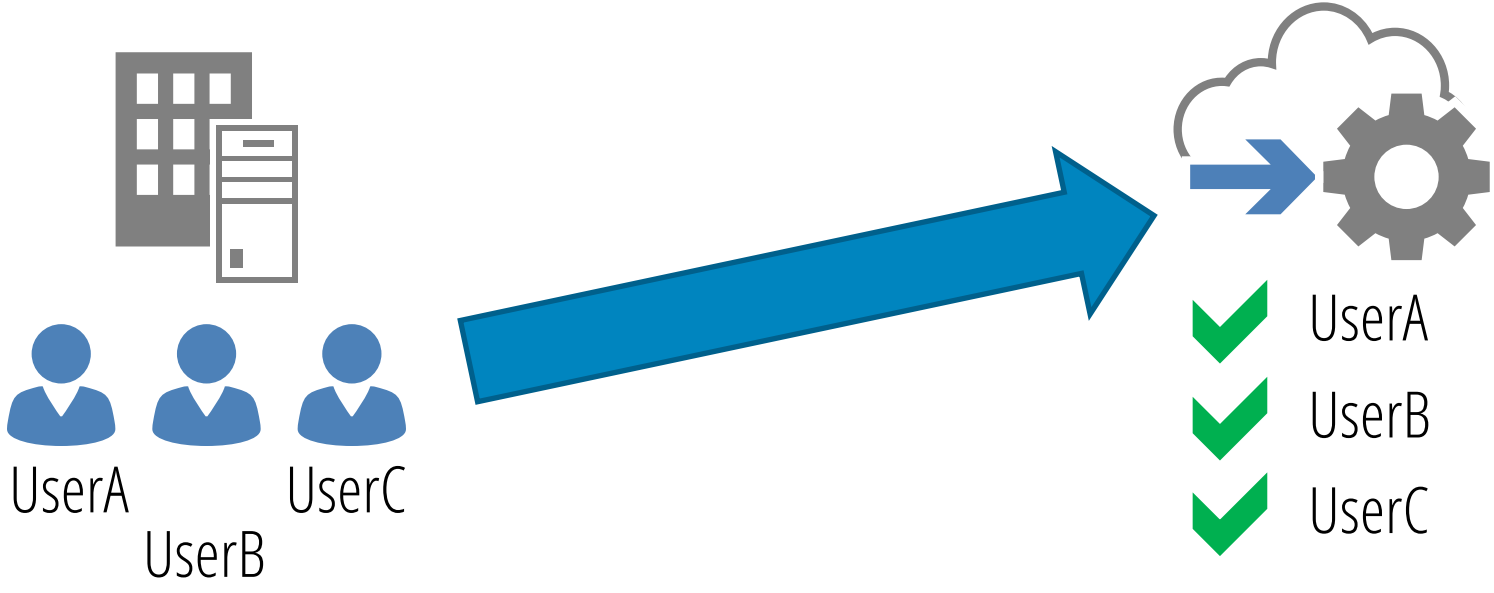
michael wessel
it performance



Kontrolle zurück ins Unternehmen

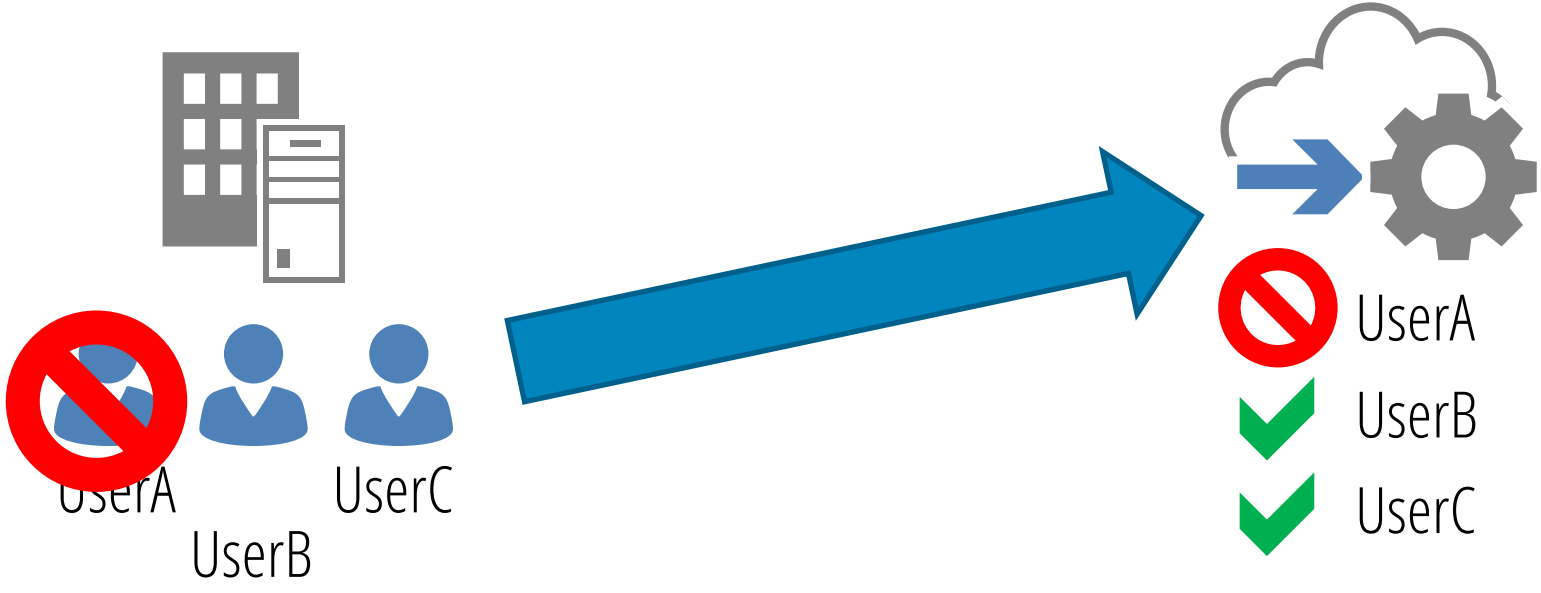
Wir steuern das selbst

michael wessel
it performance



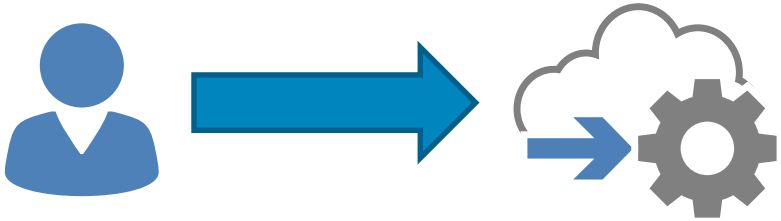
Wir steuern das selbst

michael wessel
it performance



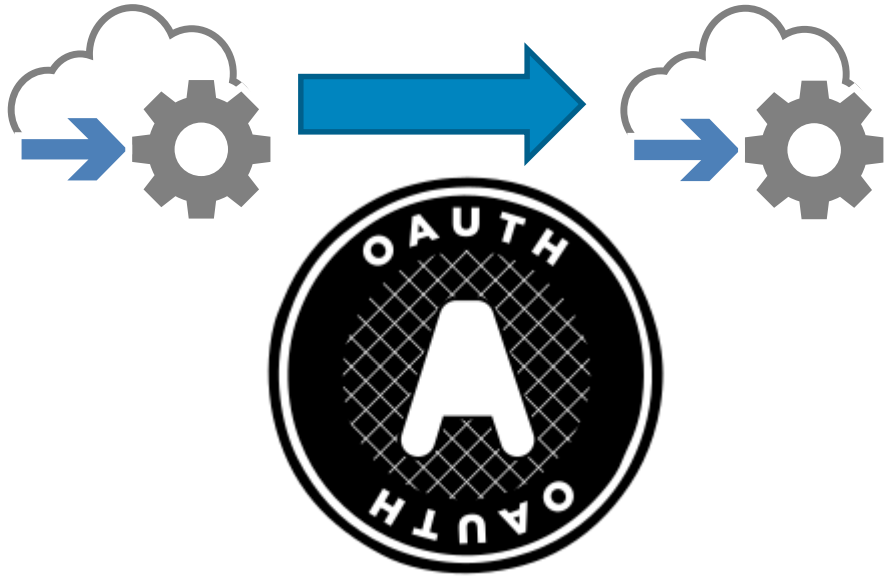
Federation: Zwei Beispiele

michael wessel
it performance



SAML

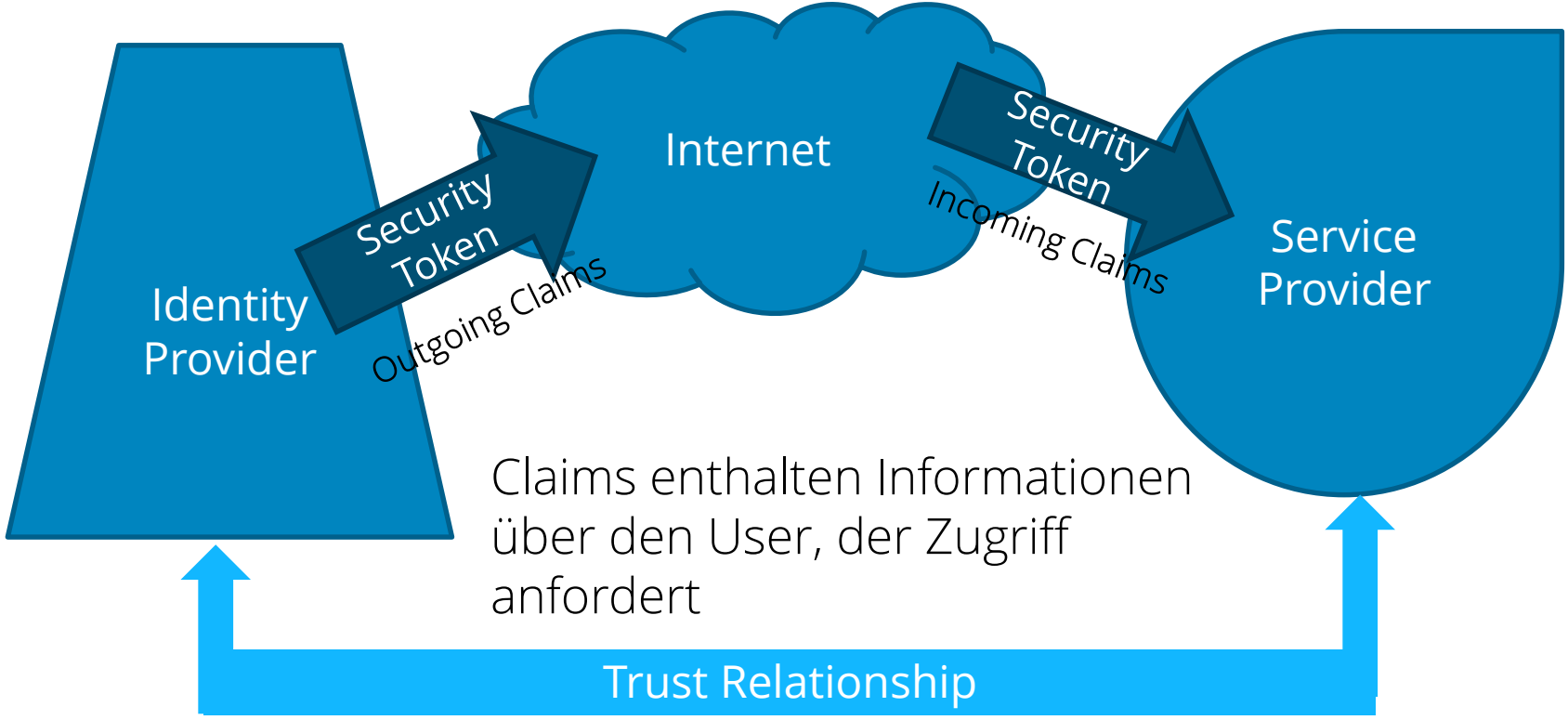
Security Assertion Markup Language



Open Authorization

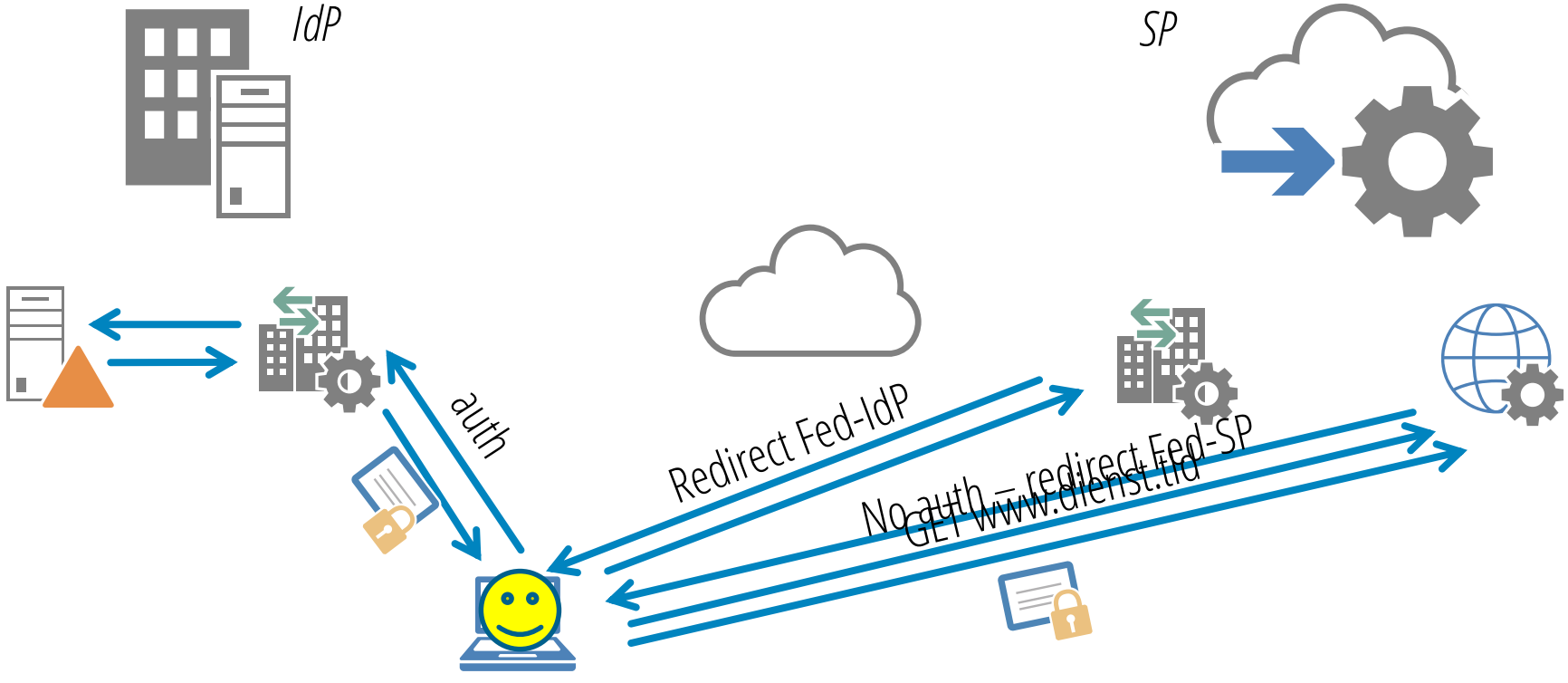
SAML

Federation schematisch



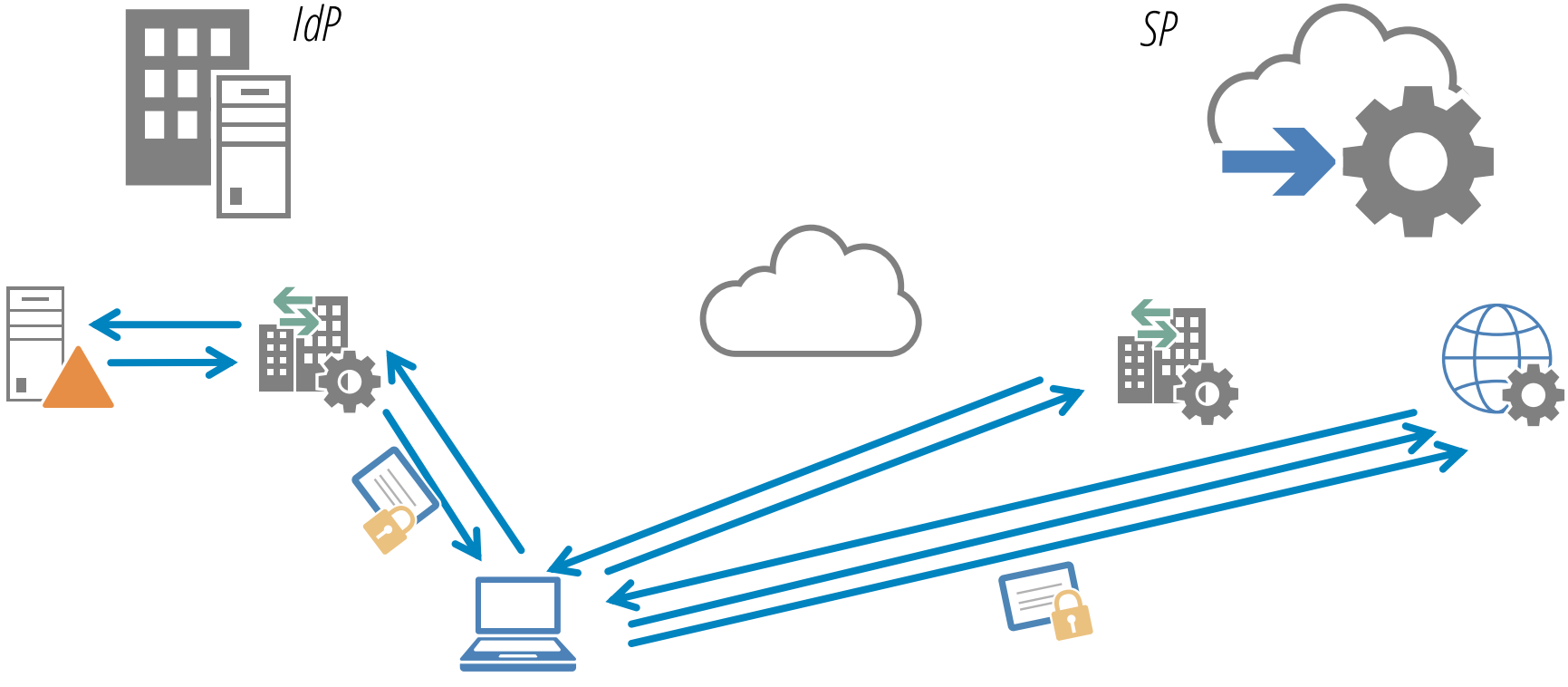
SAML zur Cloud-Anbindung

michael wessel
it performance



SAML zur Cloud-Anbindung

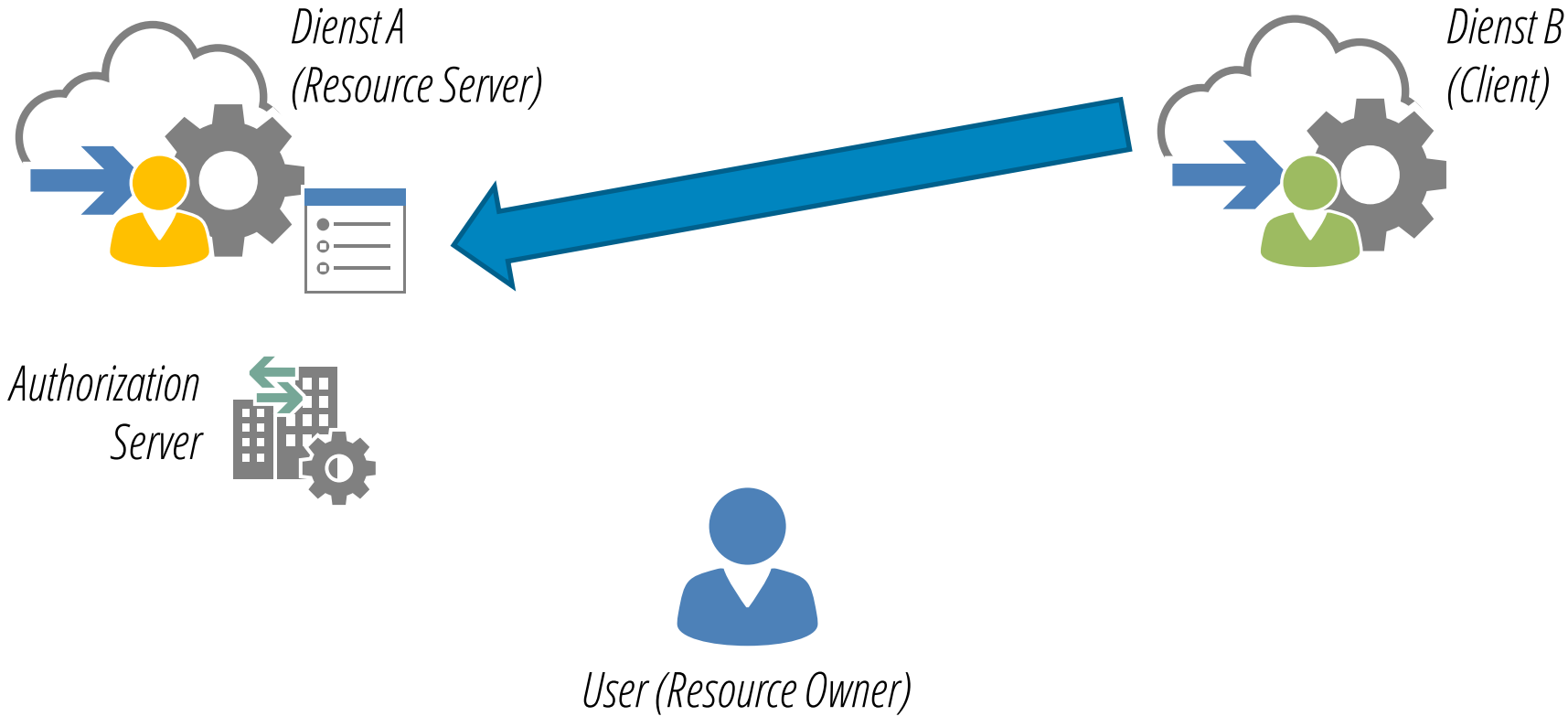
michael wessel
it performance



OAuth

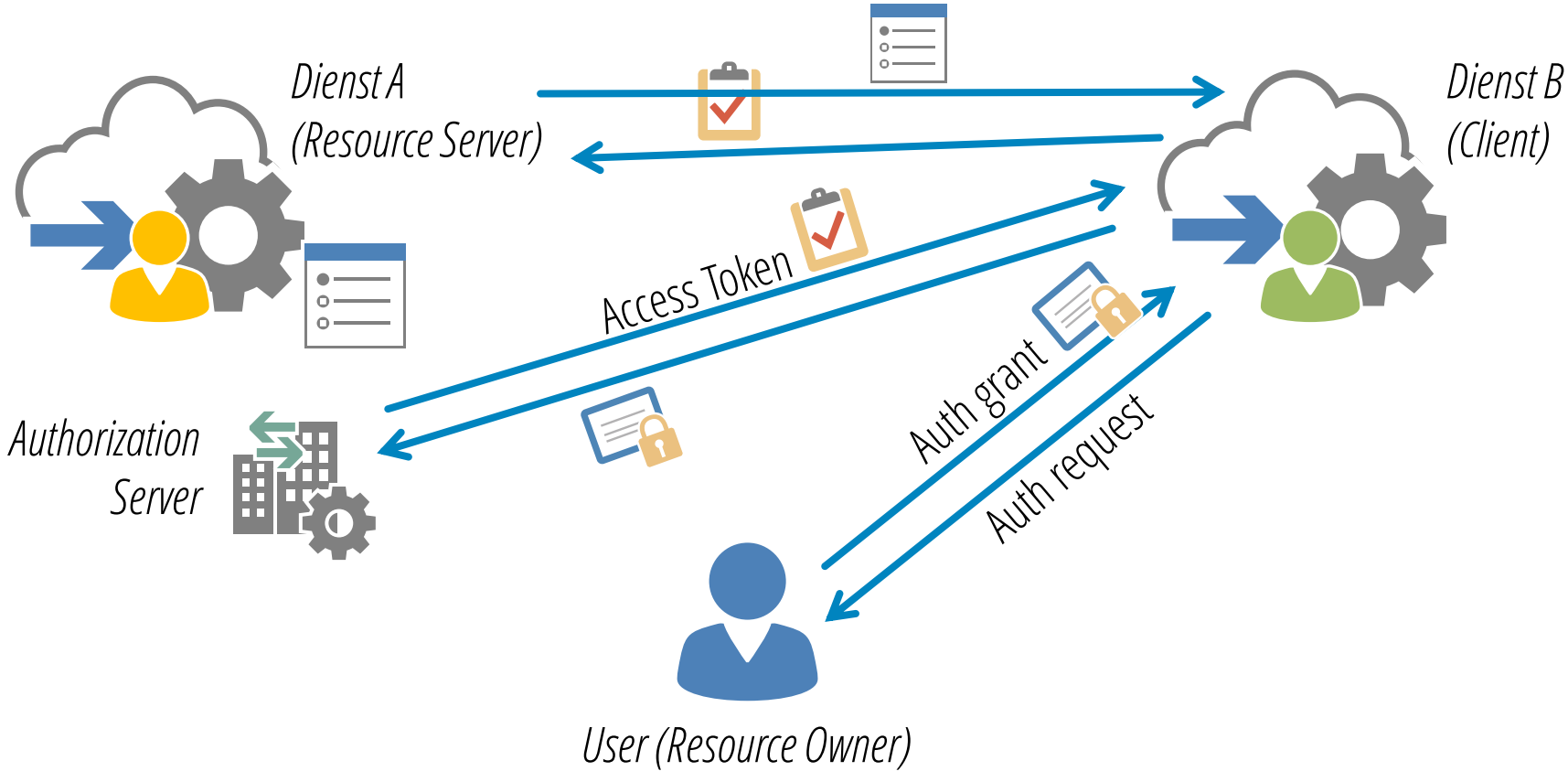
OAuth verbindet Dienste

michael wessel
it performance



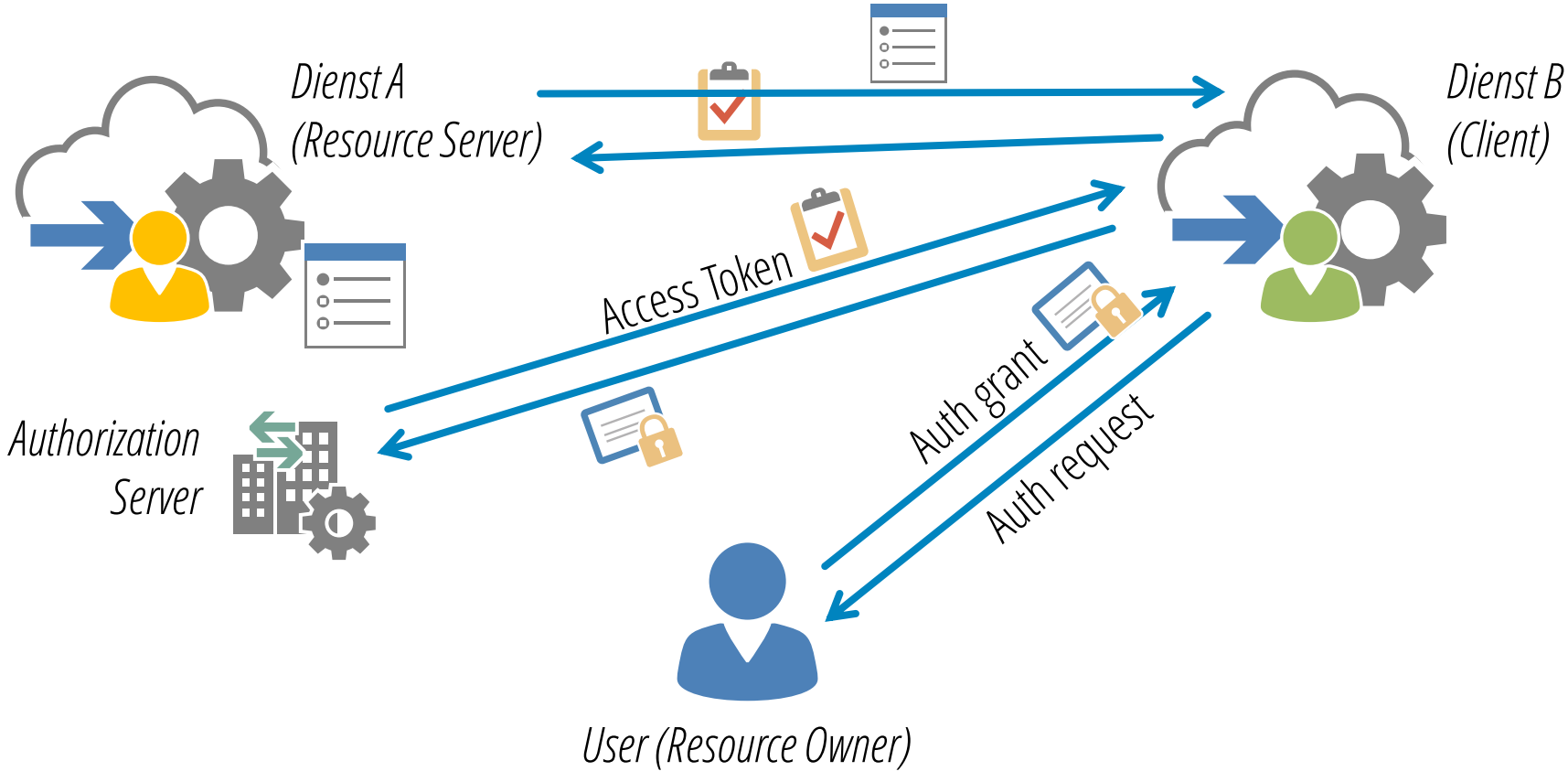
OAuth verbindet Dienste

michael wessel
it performance



OAuth verbindet Dienste

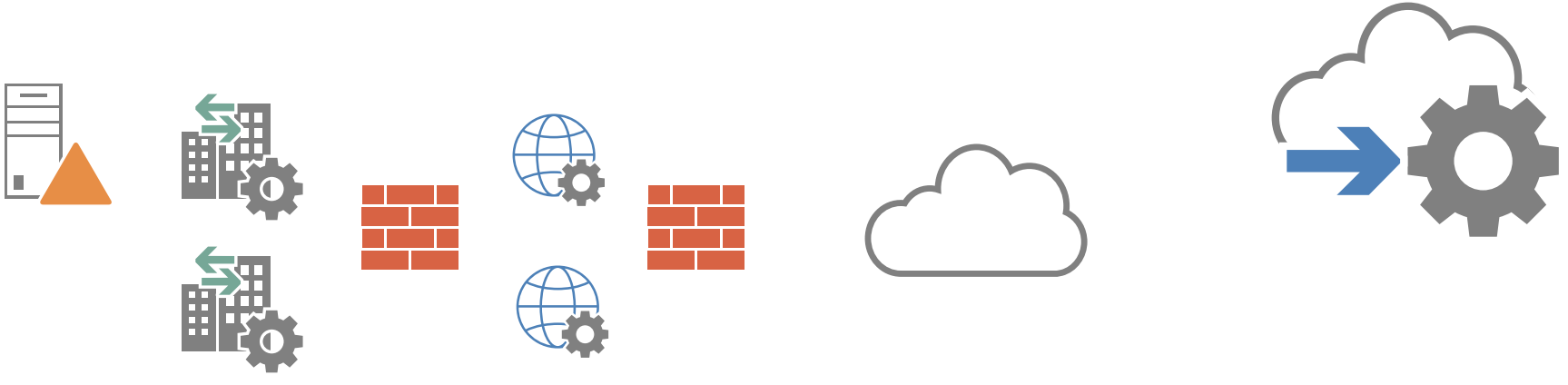
michael wessel
it performance



ADFS: Federation mit Windows

ADFS-Systemarchitektur

michael wessel
it performance



DC

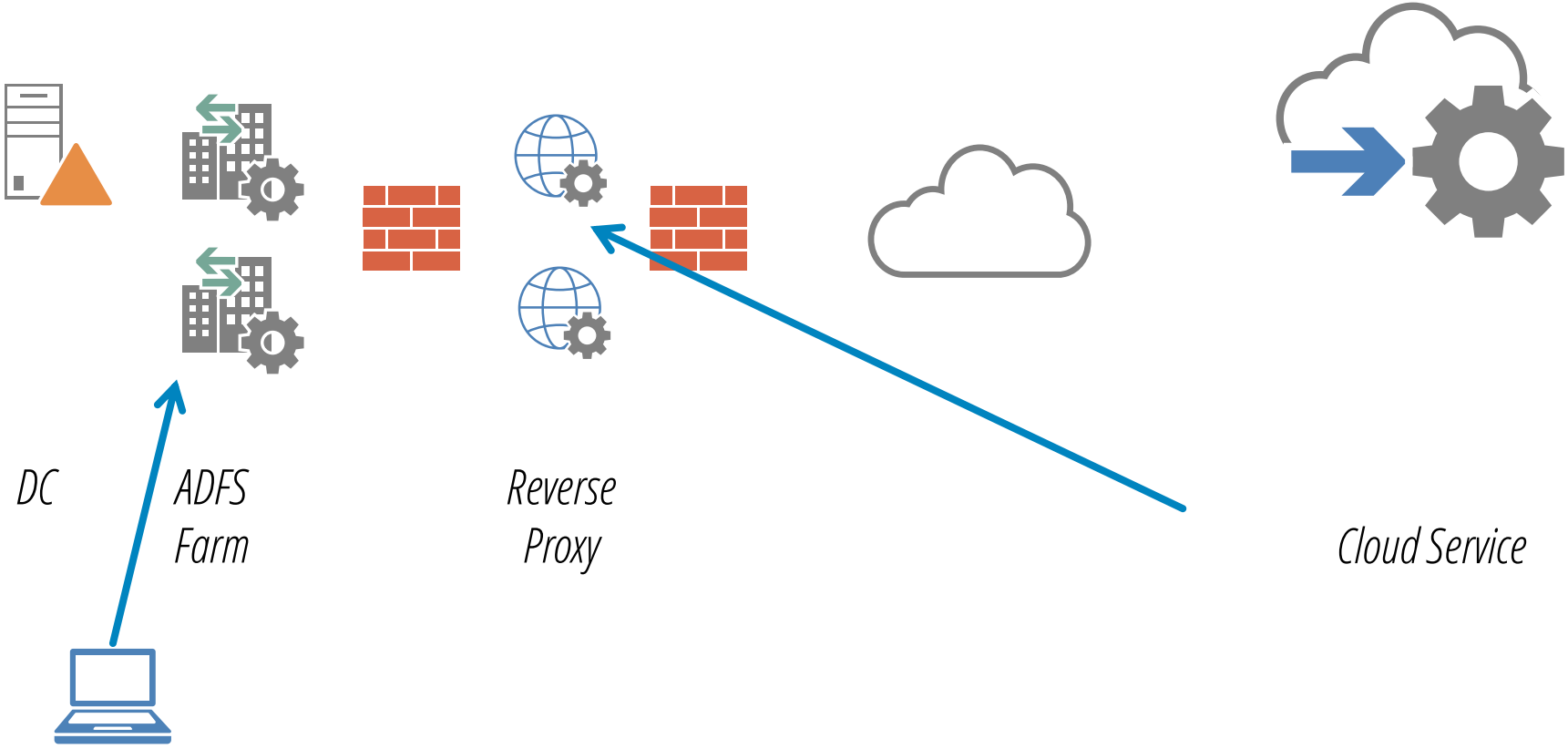
ADFS Farm

Reverse Proxy

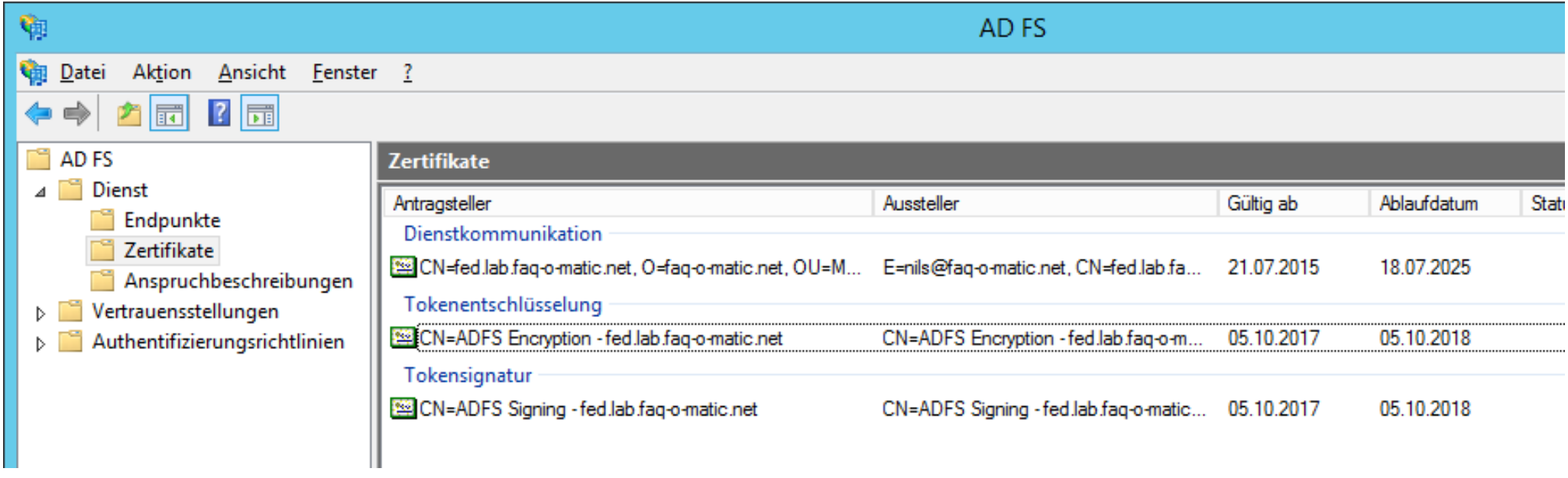
Cloud Service

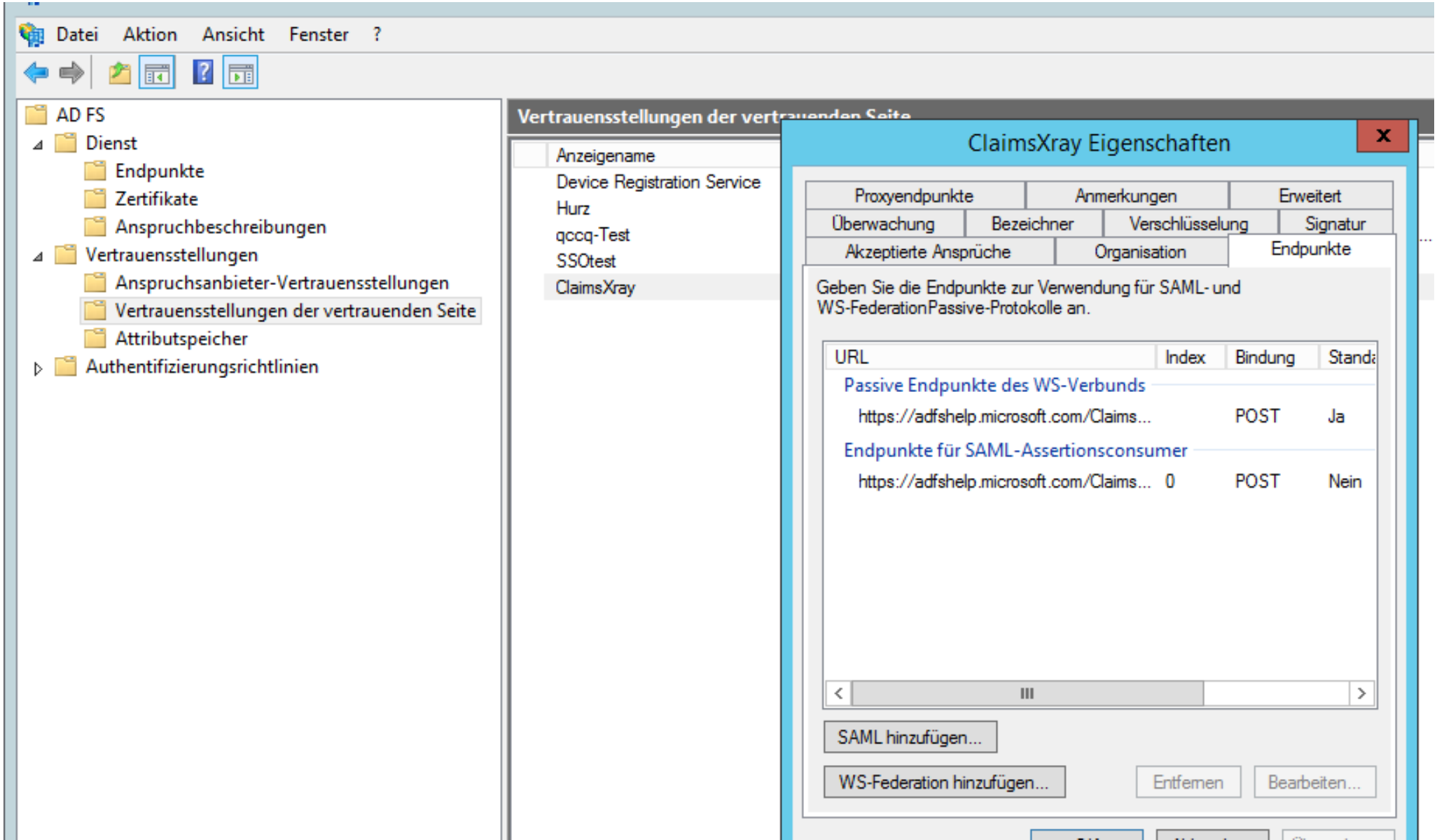
ADFS-Systemarchitektur

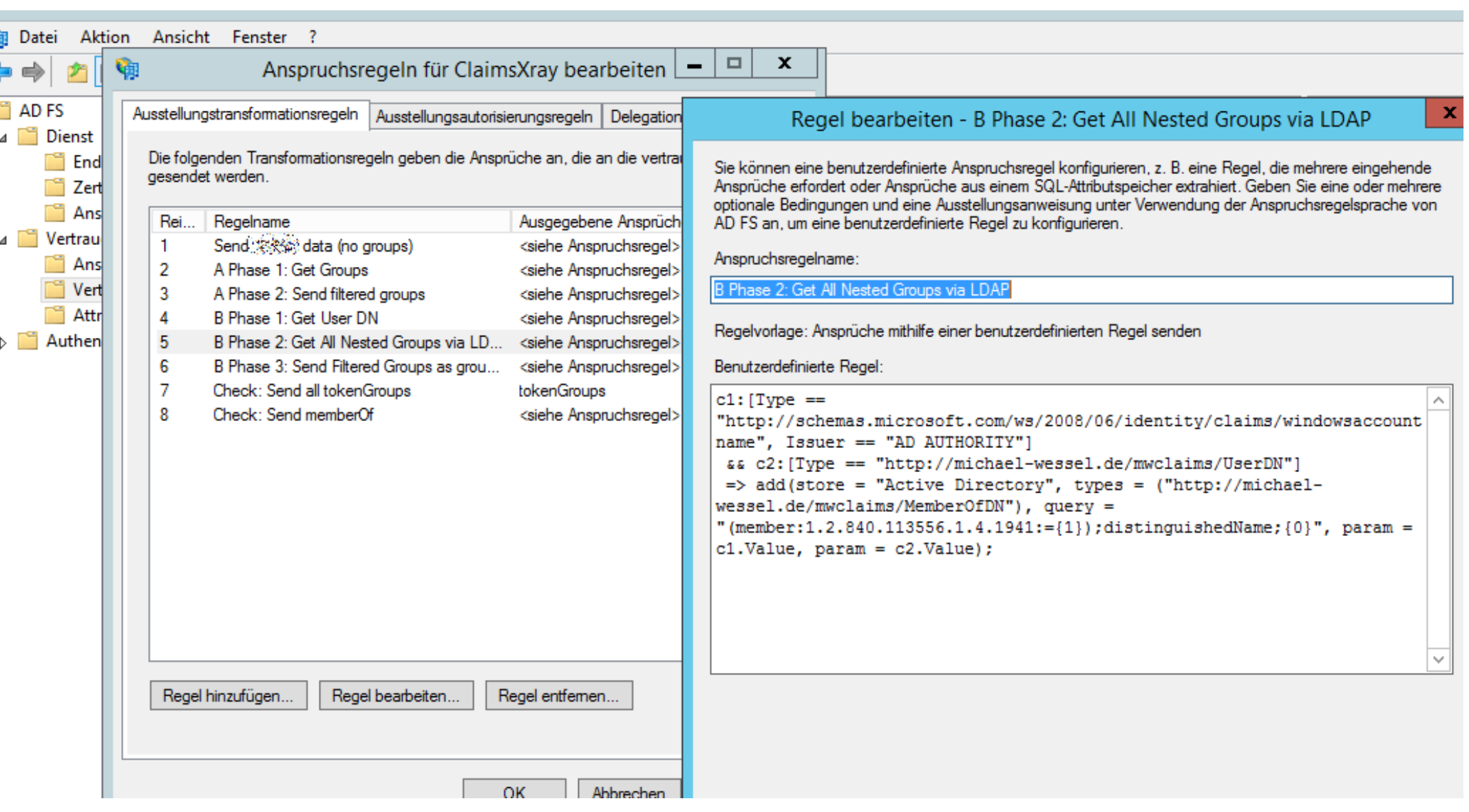
michael wessel
it performance



Wie das aussieht

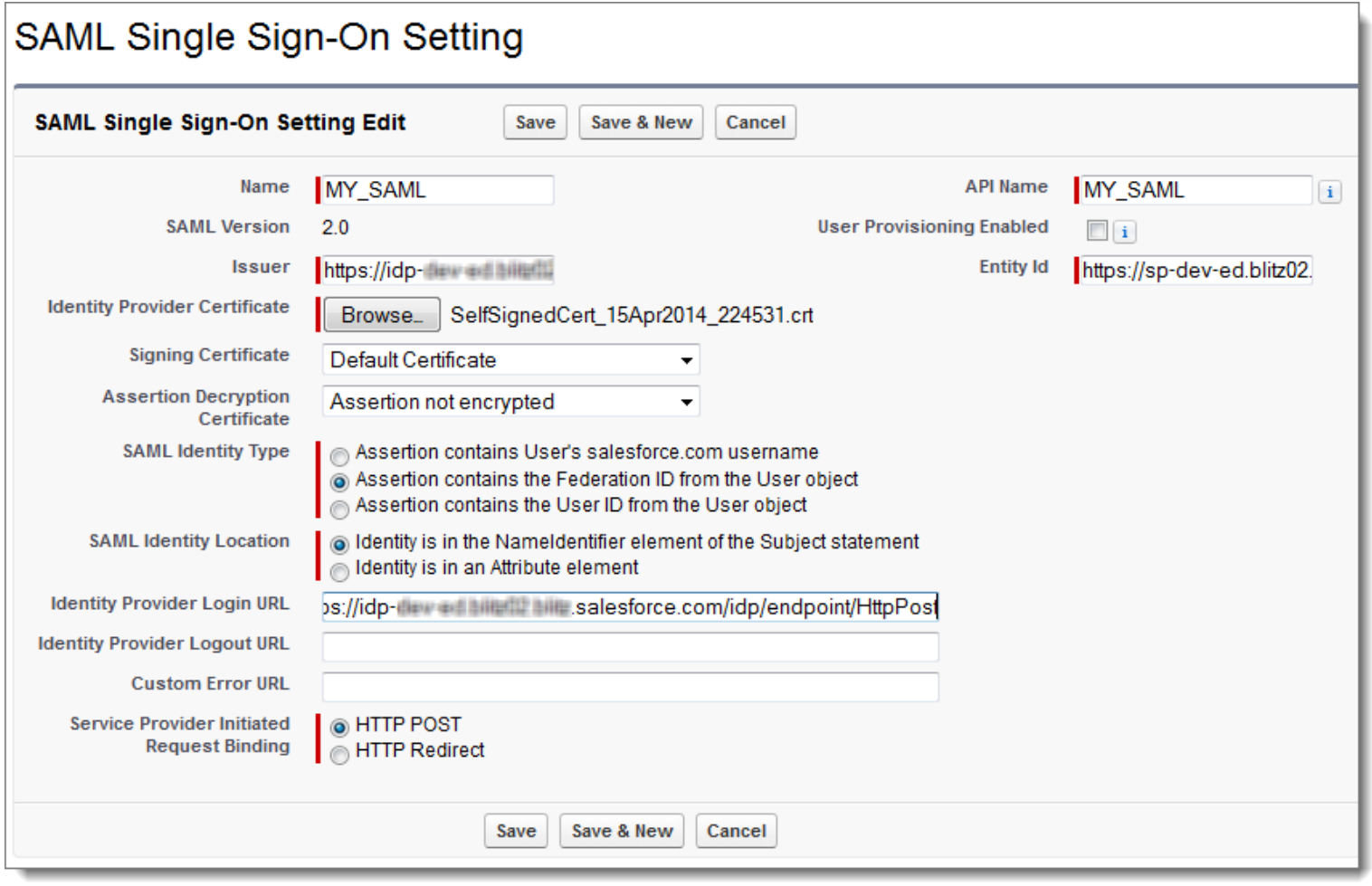

AD FS
Datei
Aktion
Ansicht
Fenster
?
AD FS
Dienst
Endpunkte
Zertifikate
Anspruchbeschreibungen
Vertrauensstellungen
Authentifizierungsrichtlinien
Zertifikate
Antragsteller
Aussteller
Gültig ab
Ablaufdatum
Dienstkommunikation
CN=fed.lab.faq-o-matic.net, O=faq-o-matic.net, OU=M...
E=nils@faq-o-matic.net, CN=fed.lab.fa...
21.07.2015
18.07.2025
Tokenentschlüsselung
CN=ADFS Encryption - fed.lab.faq-o-matic.net
CN=ADFS Encryption - fed.lab.faq-o-m...
05.10.2017
05.10.2018
Tokensignatur
CN=ADFS Signing - fed.lab.faq-o-matic.net
CN=ADFS Signing - fed.lab.faq-o-matic...
05.10.2017
05.10.2018


Datei Aktion Ansicht Fenster ?
AD FS
Dienst
Endpunkte
Zertifikate
Anspruchbeschreibungen
Vertrauensstellungen
Anspruchsanbieter-Vertrauensstellungen
Vertrauensstellungen der vertrauenden Seite
Attributspeicher
Authentifizierungsrichtlinien
Vertrauensstellungen der vertrauenden Seite
Anzeigename
Device Registration Service
Hurz
qccq-Test
SSOtest
ClaimsXray
ClaimsXray Eigenschaften
Proxyendpunkte
Anmerkungen
Erweitert
Überwachung
Bezeichner
Verschlüsselung
Signatur
Akzeptierte Ansprüche
Organisation
Endpunkte
Geben Sie die Endpunkte zur Verwendung für SAML- und WS-FederationPassive-Protokolle an.
URL
Index
Bindung
Standa
Passive Endpunkte des WS-Verbunds
https://adfshelp.microsoft.com/Claims...
POST
Ja
Endpunkte für SAML-Assertionsconsumer
https://adfshelp.microsoft.com/Claims...
0
POST
Nein
SAML hinzufügen...
WS-Federation hinzufügen...
Entfernen
Bearbeiten...


Datei Aktion Ansicht Fenster ?
AD FS
Dienst
End
Zert
Ans
Vertrau
Ans
Vert
Attr
Authen
Anspruchsregeln für ClaimsXray bearbeiten
Ausstellungstransformationsregeln
Ausstellungsautorisierungsregeln
Delegation
Die folgenden Transformationsregeln geben die Ansprüche an, die an die vertra
gesendet werden.
Rei...
Regelname
Ausgegebene Anspruch
1 Send data (no groups) <siehe Anspruchsregel>
2 A Phase 1: Get Groups <siehe Anspruchsregel>
3 A Phase 2: Send filtered groups <siehe Anspruchsregel>
4 B Phase 1: Get User DN <siehe Anspruchsregel>
5 B Phase 2: Get All Nested Groups via LD... <siehe Anspruchsregel>
6 B Phase 3: Send Filtered Groups as grou... <siehe Anspruchsregel>
7 Check: Send all tokenGroups tokenGroups
8 Check: Send memberOf <siehe Anspruchsregel>
Regel hinzufügen...
Regel bearbeiten...
Regel entfernen...
OK
Abbrechen
Regel bearbeiten - B Phase 2: Get All Nested Groups via LDAP
Sie können eine benutzerdefinierte Anspruchsregel konfigurieren, z. B. eine Regel, die mehrere eingehende Ansprüche erfordert oder Ansprüche aus einem SQL-Attributspeicher extrahiert. Geben Sie eine oder mehrere optionale Bedingungen und eine Ausstellungsanweisung unter Verwendung der Anspruchsregelsprache von AD FS an, um eine benutzerdefinierte Regel zu konfigurieren.
Anspruchsregelname:
B Phase 2: Get All Nested Groups via LDAP
Regelvorlage: Ansprüche mithilfe einer benutzerdefinierten Regel senden
Benutzerdefinierte Regel:
c1:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
&& c2:[Type == "http://michael-wessel.de/mwclaims/UserDN"]
=> add(store = "Active Directory", types = ("http://michael-wessel.de/mwclaims/MemberOfDN"), query = "(member:1.2.840.113556.1.4.1941:={1});distinguishedName;{0}", param = c1.Value, param = c2.Value);

Die andere Seite …

michael wessel
it performance



Claims X-Ray

Claims X-Ray is an online service that can be used to debug and troubleshoot problems with claims issuance. It will interact with *your* AD FS deployment and help *you* issue the claims that you need for your applications.

Choose between different authentication methods and request types, and we will show you all of the claims returned by your federation service. You can use this to fully customize your policies to get the claims you need.

1 Federation Services Configuration

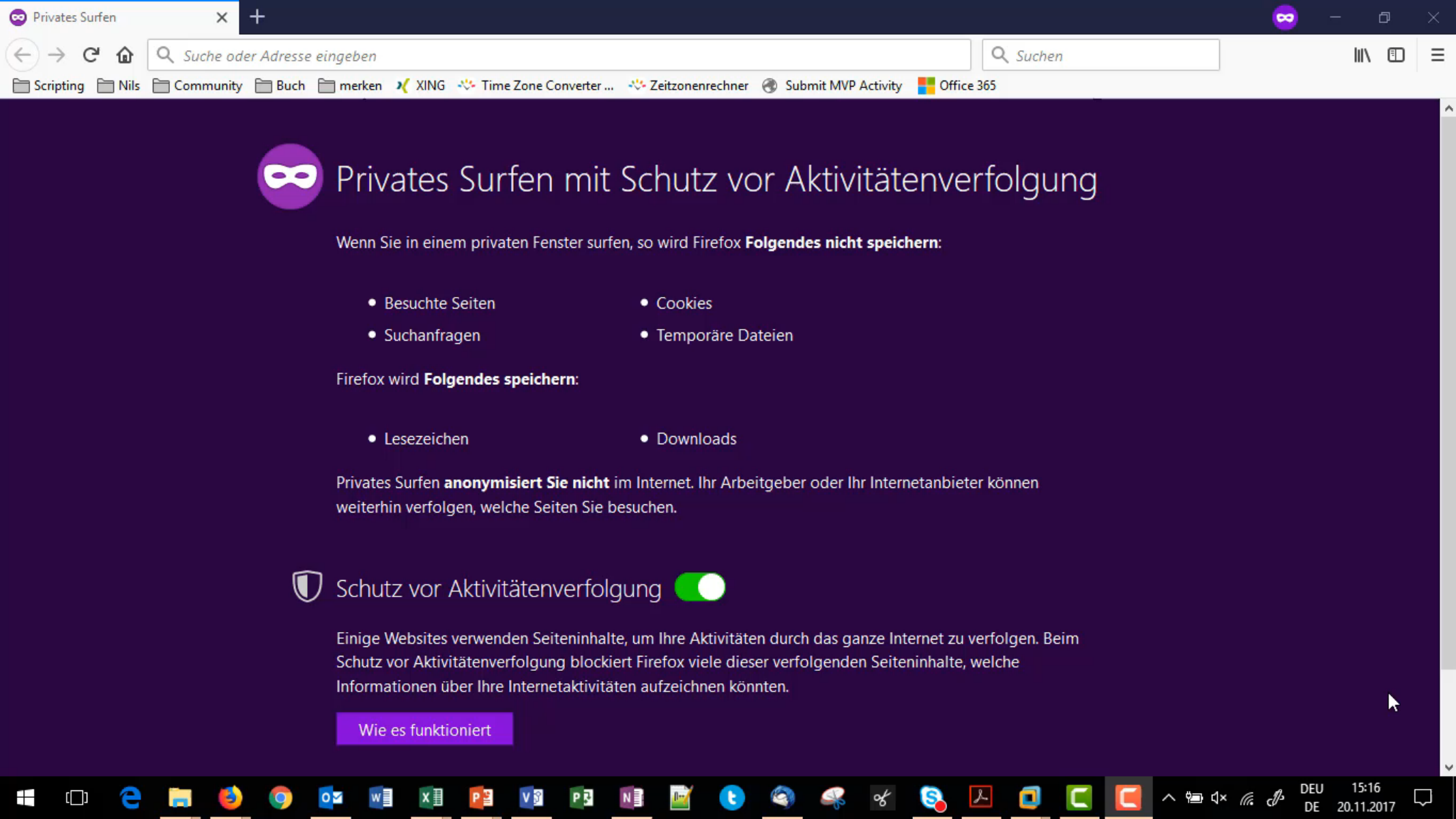
In order to use Claims X-Ray, you must create a relying party trust for the service in your federation deployment. You can customize the claim rules to whatever you want to test. We've provided an example below that will display all claims.

1. Log into the primary node of your federation service
2. Launch an elevated PowerShell session
3. Create the Claims X-Ray relying party trust

```
$authzRules = "=>issue(Type = `"http://schemas.microsoft.com/authorization/claims/permit`", Value =
`"true`"); "
$issuanceRules = "x:[]=>issue(claim = x); "
$redirectUrl = "https://adfshelp.microsoft.com/ClaimsXray/TokenResponse"
$samlEndpoint = New-AdfsSamlEndpoint -Binding POST -Protocol SAMLAssertionConsumer -Uri $redirectUrl

Add-ADFSRelyingPartyTrust -Name "ClaimsXray" -Identifier "urn:microsoft:adfs:claimsxray"
```

In order to use oAuth with Claims X-Ray, you must create an oAuth client for the service in your federation deployment.

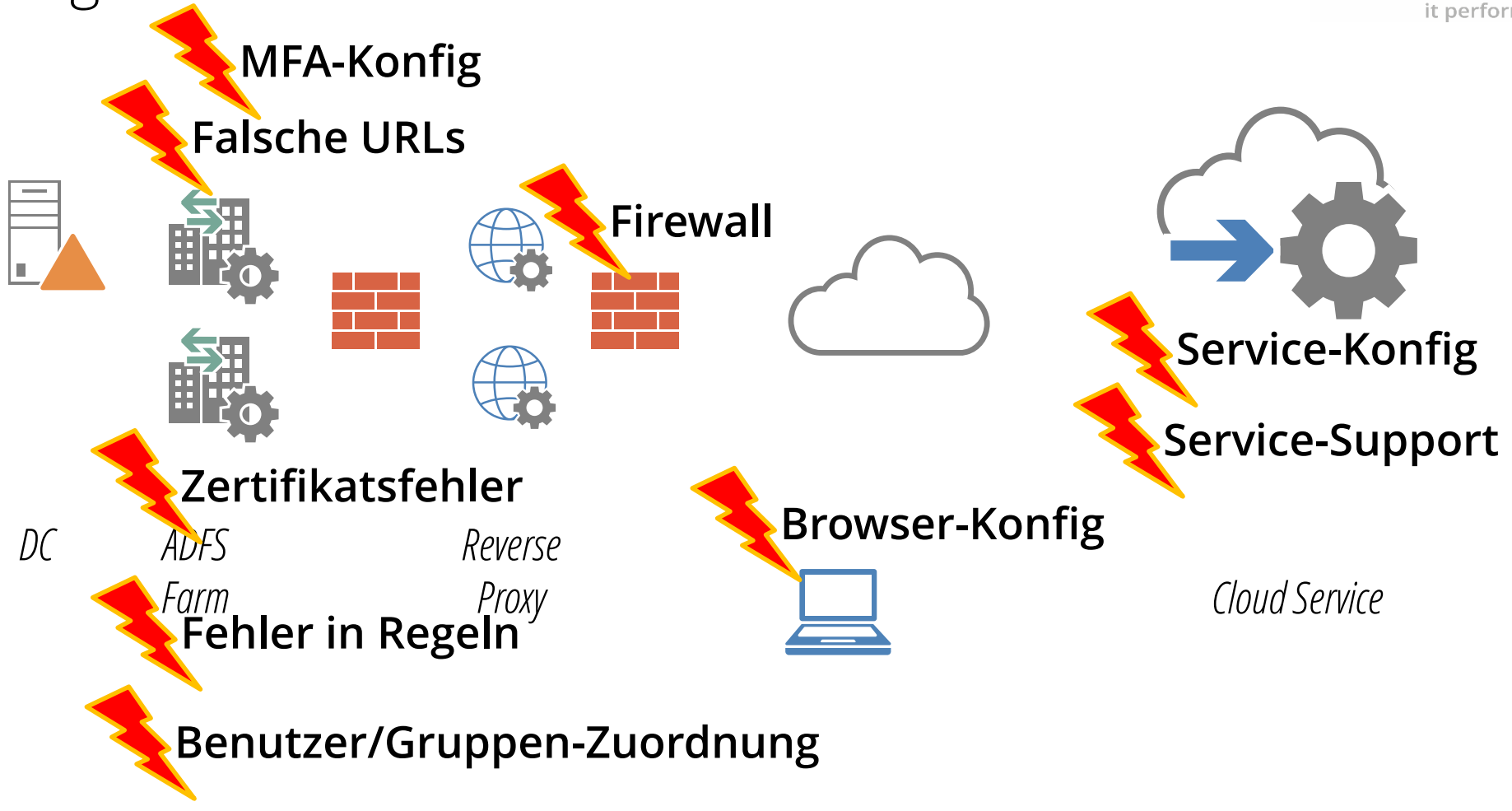

Privates Surfen
Suche oder Adresse eingeben
Suchen
Scripting
Nils
Community
Buch
merken
XING
Time Zone Converter ...
Zeitzonenrechner
Submit MVP Activity
Office 365
Privates Surfen mit Schutz vor Aktivitätenverfolgung
Wenn Sie in einem privaten Fenster surfen, so wird Firefox **Folgendes nicht speichern**:
Besuchte Seiten
Suchanfragen
Cookies
Temporäre Dateien
Firefox wird **Folgendes speichern**:
Lesezeichen
Downloads
Privates Surfen **anonymisiert Sie nicht** im Internet. Ihr Arbeitgeber oder Ihr Internetanbieter können weiterhin verfolgen, welche Seiten Sie besuchen.
Schutz vor Aktivitätenverfolgung
Einige Websites verwenden Seiteninhalte, um Ihre Aktivitäten durch das ganze Internet zu verfolgen. Beim Schutz vor Aktivitätenverfolgung blockiert Firefox viele dieser verfolgenden Seiteninhalte, welche Informationen über Ihre Internetaktivitäten aufzeichnen könnten.
Wie es funktioniert
DEU
DE
15:16
20.11.2017

Was dabei schiefgehen kann

(das sind nur ca. 10.000 Stellen)

Sorgenschießen

michael wessel
it performance



Federation planen

Ellen Bogen plant die Föderation

michael wessel
it performance

- Welche Applikationen?
- Welches Protokoll?
- Welche Anwender?
- Zugriff von wo?
- Berechtigungen in den Apps?
- Welche AD-Informationen?
- Namen und Zertifikate?
- Ausfallsicherheit?
- Betrieb und Wartung?

Ellen Bogen

nka@michael-wessel.de

@Kaczenski