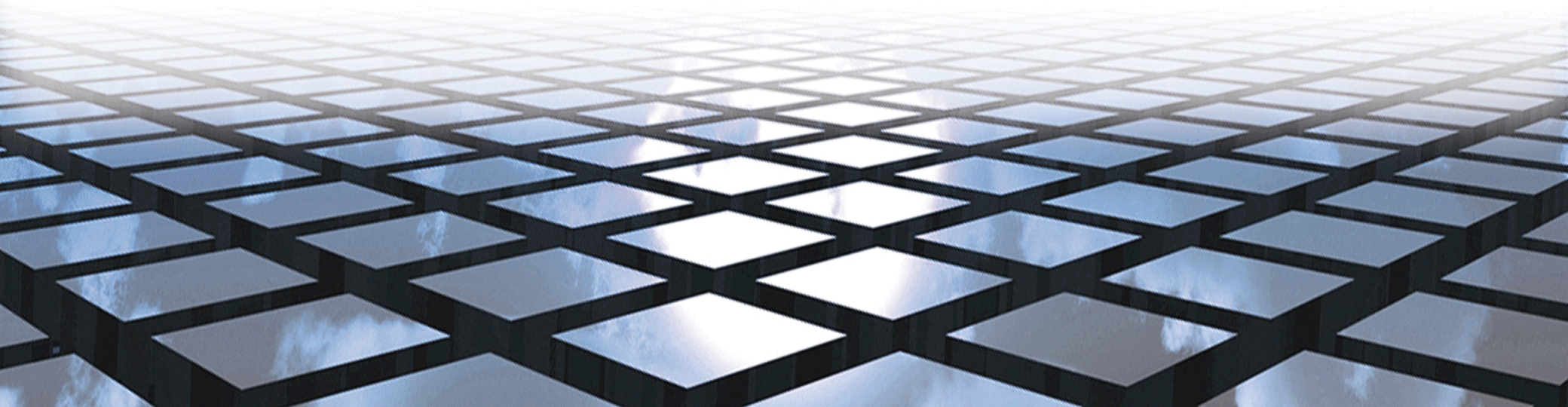
NETCLOUD

ICT PROFESSIONALS



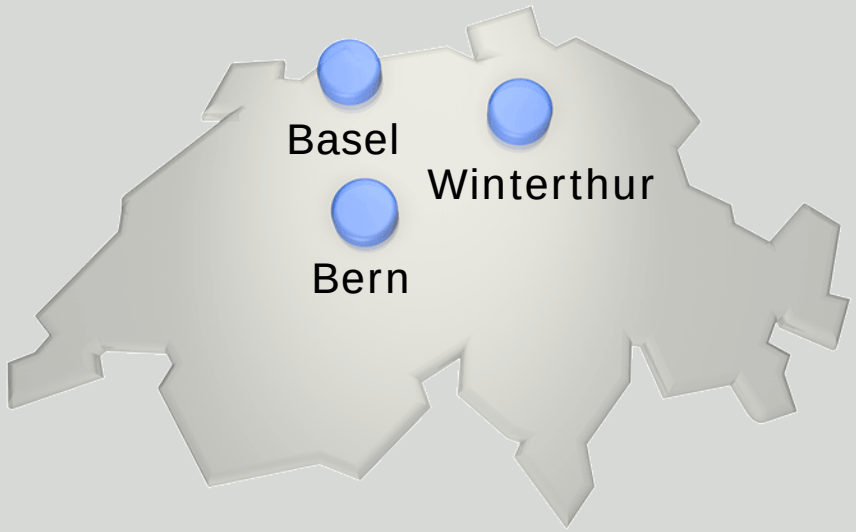
NETCLOUD

ICT PROFESSIONALS

Jarle Steffensen

steffensen@netcloud.ch

Auf einen Blick



Gründungsjahr
1998

Anzahl Mitarbeiter
121

Umsatz 2015
98.9 Mio. CHF

Cisco Partner Level
Gold

Besitzverhältnisse
Zu 100% in Besitz des Managements, eigenfinanziert

Rechtsform
Aktiengesellschaft

Der beste Beweis für unsere Leistung und Kompetenz

Unsere Zertifizierungen

- Cisco Gold Partner
- Cisco Master Collaboration Partner
- Cisco Master Cloud Builder
- Cisco Intercloud Service Provider
- Cisco Advanced Data Center Architecture
- Cisco Enterprise Networks Architecture
- Cisco Advanced Borderless Network Architecture
- Cisco Advanced Collaboration Architecture
- Cisco Advanced IP NGN Architecture
- Cisco ATP Telepresence Video Master
- Cisco ATP Identity Services Engine
- Cisco Advanced Routing & Switching
- Cisco Advanced Wireless LAN
- Cisco Advanced Security
- Cisco Advanced Content Security
- Cisco Application Centric Infrastructure (ACI) Partner

- NetApp Gold Partner
- Flexpod Premium Partner
- Microsoft Gold Partner Datacenter
- VMware Enterprise Solution Provider
- f5 Silber Partner
- WhatsUp Gold Gold Partner
- RSA Partner
- ARC Certified Partner
- Andtek Partner

Unsere Kompetenz hat viele Namen

Netcloud ist führend in der Breite und Tiefe des Cisco ICT Knowhows:

Auf Level Expert

20 CCIE, Cisco Certified Internet Expert **Routing / Switching**
1 CCIE, Cisco Certified Internet Expert **Security**
2 CCIE, Cisco Certified Internet Expert **Service Provider**
4 CCIE, Cisco Certified Internet Expert **Data Center**
1 CCIE, Cisco **ISP Dial Technology**
2 CCIE, Cisco Certified Internet Expert **Collaboration**
1 CCIE, Cisco Internet Certified Expert **Storage**

Auf Level Professional

14 CCDP, Cisco Certified **Design Professional**
6 CCNP, Cisco Certified Network Professional **Data Center**
6 CCNP, Cisco Certified Network Professional **Security**
2 CCNP, Cisco Certified Network Professional **Service Provider**
3 CCNP, Cisco Certified Network Professional **Collaboration**
4 CCSP, Cisco Certified Network Professional **Wireless**
38 CCNP, Cisco Certified Network Professional **R&S**

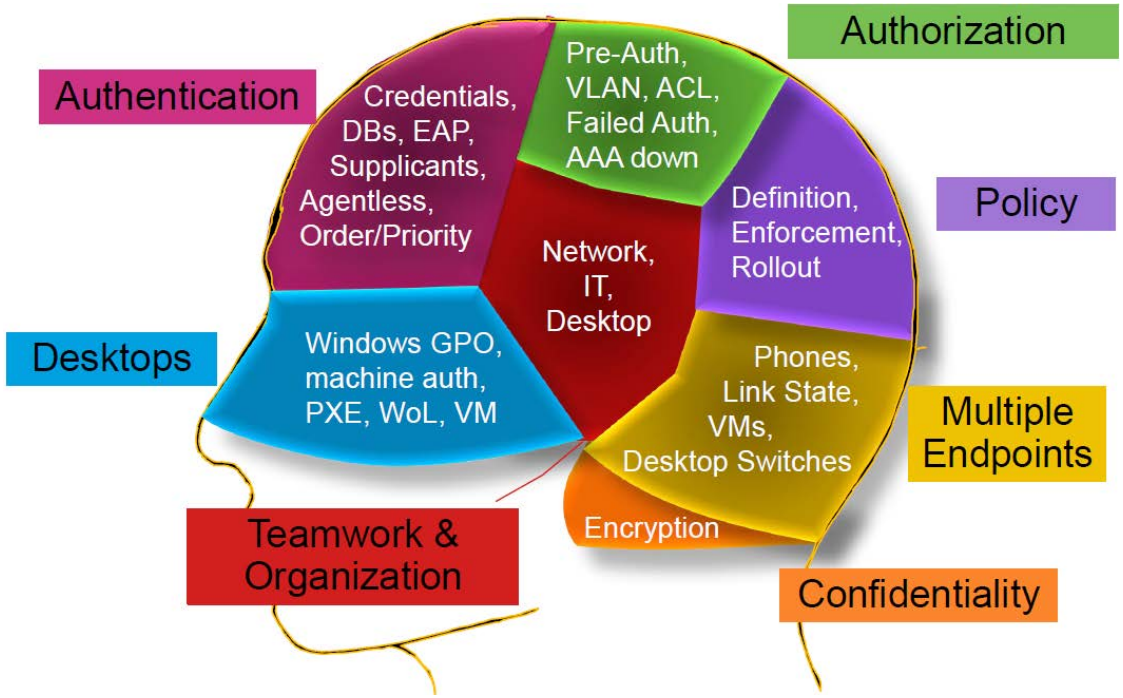
Unsere Aufgabe ist Ihr Erfolg

Netcloud AG bietet zukunftsorientierte und sichere ICT Lösungen, welche einfacher und zuverlässiger sind und dadurch unsere Kunden erfolgreicher machen.

NETCLOUD
ICT PROFESSIONALS

Agenda – 802.1x Projekterfahrungen

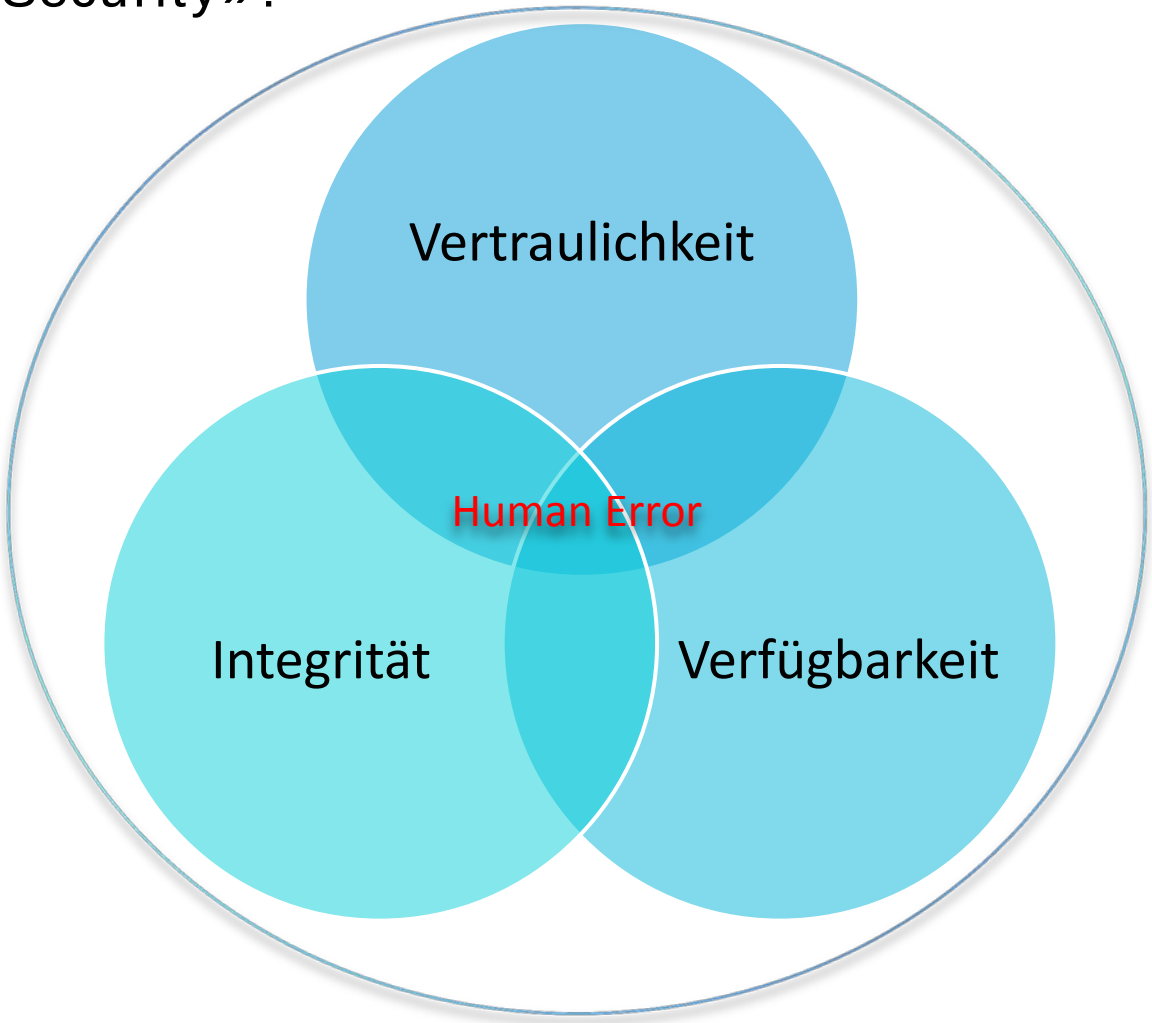
- Introduktion 802.1x
- Erwartungshaltung zur Komplexität
- Authentisierungsmethoden
- Fallback
- Projektablaufe
  - Testing
  - Rollout
- Betriebsprozesse
  - Logging



NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – 802.1x Intro

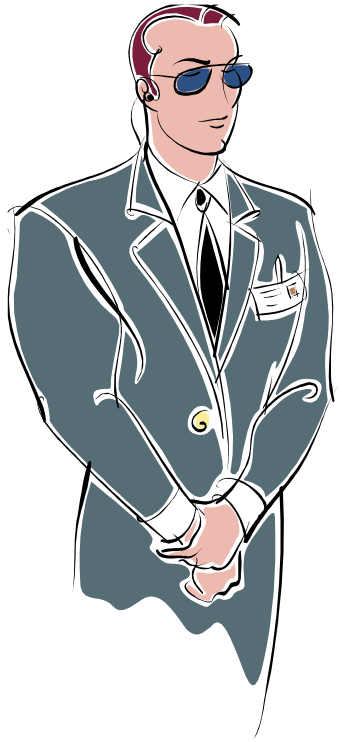
- Was ist «Security»?



NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – 802.1x Intro

- Was ist das Ziel von 802.1x?
  - Sicherheit erhöhen,
  - Nur bekannte Geräte an Netzwerk erlauben



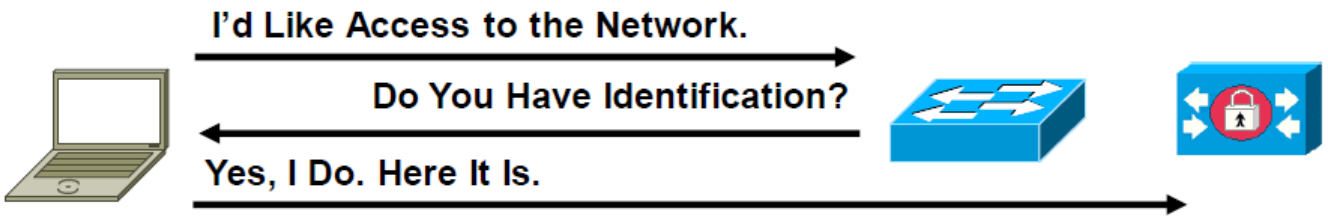
802.1x Erfahrungen – 802.1x Intro

- Was ist 802.1x / Was meinen wir mit 802.1x
  - Framework für Authentisierung und Autorisierung
  - Standardizierte Protokoll durch IEEE 802.1x
  - NAC Network Admission Control?

Primary Components			
Supplicant	**Authenticator**	**Authentication Server**	**Backend Database**
802.1X Client	Switch / WLAN	RADIUS Server	AD, LDAP, etc
			

802.1x Erfahrungen – 802.1x Intro

- Wie funktioniert 802.1x?
  - Identifikation
  - Zugriffsberechtigung

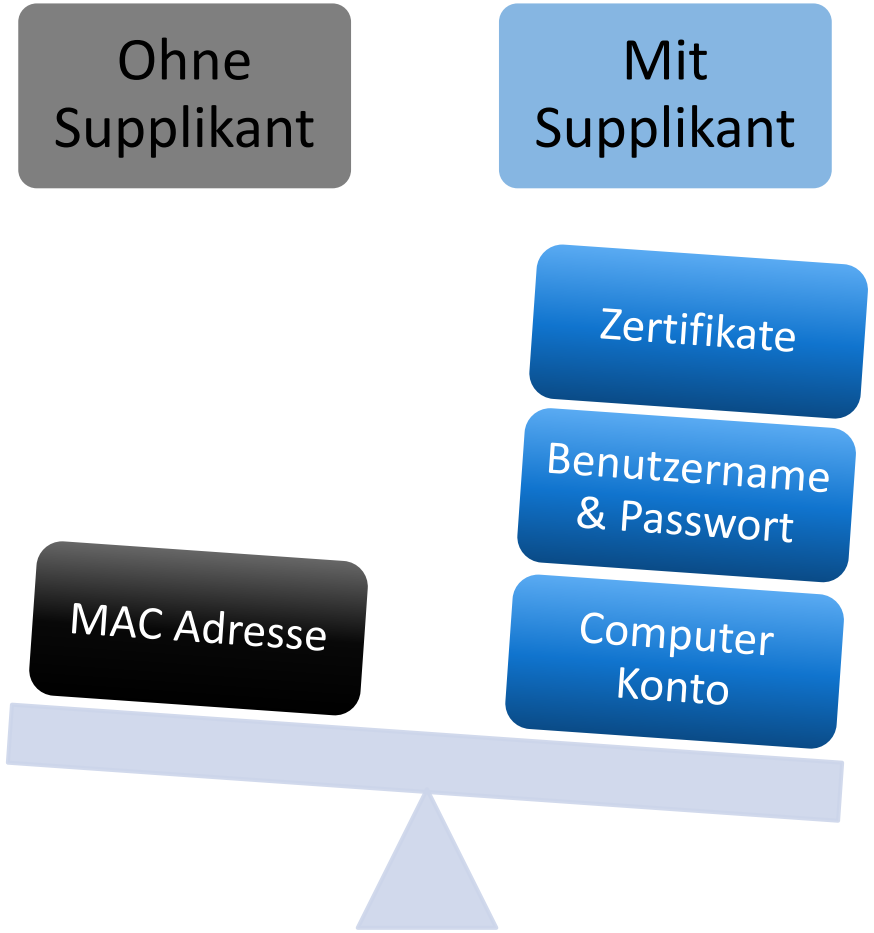


  - Schlüsselelement:

Die Identifikation ist nur so stark/sicher wie die verwendete Methode um die Identität zu verifizieren.

802.1x Erfahrungen – 802.1x Intro

- Welche Identifikations-Methoden können dazu verwendet?

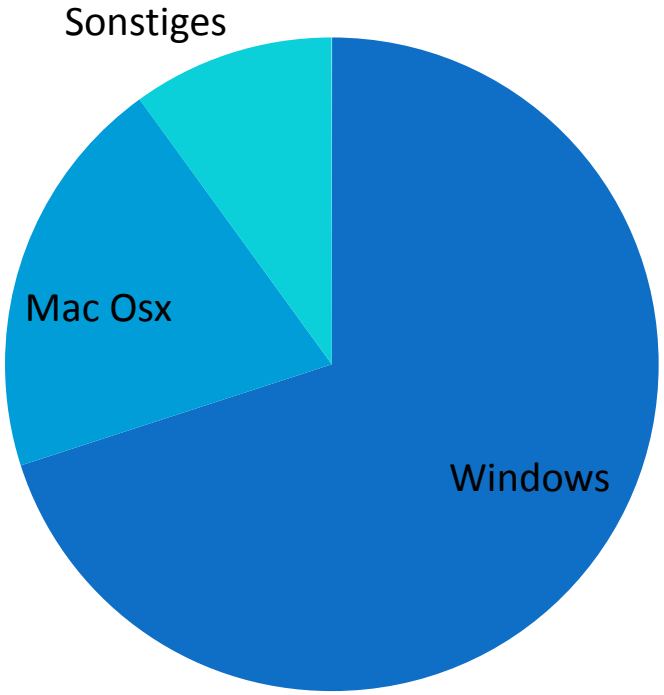


802.1x Erfahrungen – 802.1x Intro

- Fragen?

802.1x Erfahrungen – Erwartete Komplexität

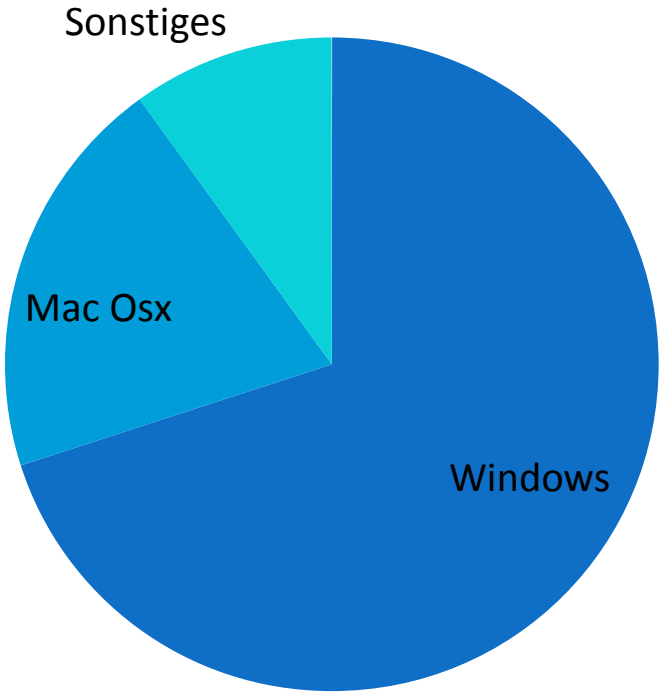
Erwartet:
Aufwand/Komplexität



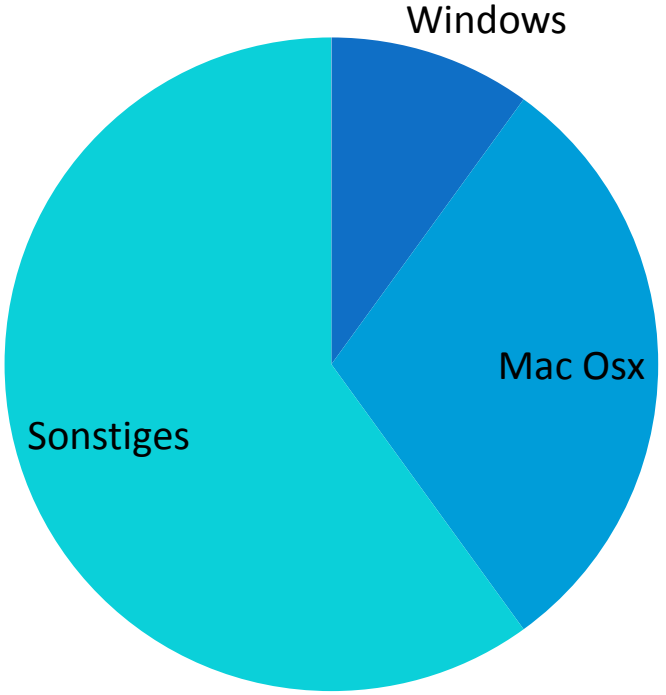
NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – Erwartete Komplexität

Erwartet:
Aufwand/Komplexität



Effektiv:
Aufwand/Komplexität



802.1x Erfahrungen – Effektive Komplexität

- Microsoft Windows
  - Windows kann einfach und zentral via GPOs gesteuert werden.
  - Windows 802.1x Supplikant ist bewährt.
    (seit WinXP vorhanden)

- Mac OSX
  - MacOSX 802.1x Supplikant ist bewährt
  - Wie MacOSx zentral verwalten?

802.1x Erfahrungen – Effektive Komplexität

- «Sonstiges»
  - Was können die «Sonstiges»?
  - Was sind das für Geräte? Wie verhalten sie sich?
  - Wie können sie möglichst zentral verwaltet werden?


Printers


IP Cameras


Alarm Systems


Fax Machines


Wireless APs


Turnstiles


Video Conferencing Stations


Managed UPS


HVAC Systems


IP Phones


Cash Registers


RMON Probes


Hubs


Medical Imaging Machines


Vending Machines

802.1x Erfahrungen – Effektive Komplexität

- Was können die Netzwerkkomponenten?
  - Unterstützen sie MAB?
  - FailOpen?
- Wie verhalten sie sich?

NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – Effektive Komplexität

- Ein 802.1x Projekt startet mit einem Endgeräte- und Infrastrukturinventar!
- Spätestens beim Rollout werden alle Endgerätetypen gefunden, an welche noch niemand gedacht hat.
- Am Ende eines 802.1x Projektes hat man definitiv ein vollständiges Endgeräte- und Infrastrukturinventar!

802.1x Erfahrungen – Effektive Komplexität

- Individuelle Umgebung benötigt:
  - Individuelle Regeln
  - Individuelle Software auf Switches
  - Individuelle Software auf Endgeräte
  - Tests um alle Szenarien zu prüfen
  - Individuelle Betriebsprozesse

Bisher noch in jedem Projekt gehörter Satz:

Ist es das erste 802.1x Projekt, das Sie machen?

Antwort:

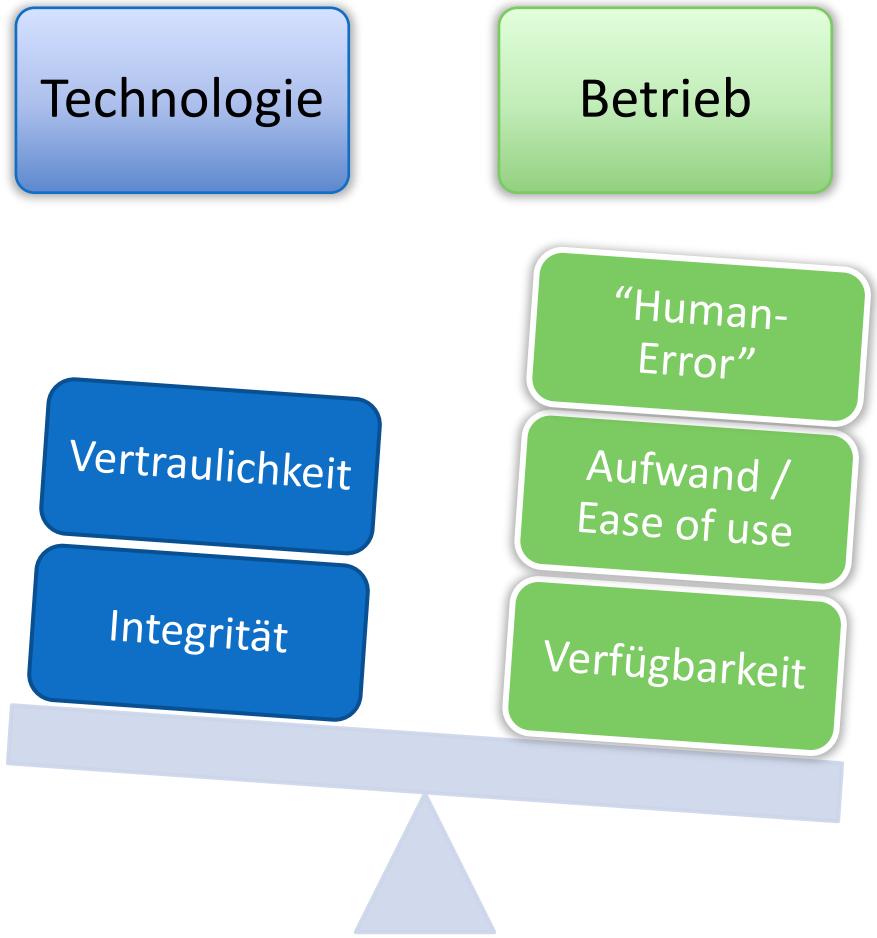
Definitiv nicht! Aber mit den Endgeräten, auf den Netzwerkkomponenten, mit diesen Software Versionen, mit diesen Geschäfts- und Regelwerkanforderungen? **JA!**

802.1x Erfahrungen – Projektstart „Key–Takeaway‘s“

- Umgebung und eingesetzte Geräte sind Unterschiedlich!
  - Wir starten deshalb mit Infrastrukturinventar
- Seit 5-6 Jahren realisieren wir erfolgreich 802.1x Projekte
  - Bis jetzt gab es immer Lösungen für alle «Herausforderungen».
- Projekt Dauer von Realisations-Entscheidung bis abgeschlossene Rollout
  - ist ab 6 Monate
  - ist in Normalfall 9-24 Monate
- Anforderungen sind unterschiedlich
  - Sicherheit
  - Betrieb
  - Flexibilitiät

802.1x Erfahrungen – Projektstart „Key–Takeaway‘s“

- Anforderungen sind unterschiedlich



NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – Authentisierungsmethoden

- Wie stark ist die Sicherheit?
  - «Wie stark darf denn die Sicherheit sein?»
- Welche Varianten stehen zur Auswahl?

802.1x Erfahrungen – Authentisierungsmethoden

- LEAP (Lightweight Extensible Authentication Protocol)
- EAP-TLS (Transport Layer Security)
- EAP-MSChapv2 (MS-ChapV2)
- EAP-MD5 (MD5 Hashes)
- EAP-POTP (Protected One-Time Password)
- EAP-PSK (Presahred-Key)
- EAP-PWD (Shared Password)
- EAP-TTLS (Tunneled Transport Layer Security)
- EAP-IKEv2 (Internet Key Exchange v2)
- EAP-FAST (Flexible Authentication via Secure Tunneling)
- EAP-SIM (Subscriber Identity Module)
- EAP-AKA (UMTS Authentication and Key Agreement)
- EAP-AKA‘ (Authentication and Key Agreement für 3GPP)
- EAP-GTC (Generic Token Card)
- EAP-EKE (Encrypted key exchange)

802.1x Erfahrungen – Authentisierungsmethoden

- LEAP (Lightweight Extensible Authentication Protocol)
- **EAP-TLS (Transport Layer Security)**
- **EAP-MSChapv2 (MS-ChapV2)**
- **EAP-MD5 (MD5 Hashes)**
- EAP-POTP (Protected One-Time Password)
- EAP-PSK (Presahred-Key)
- EAP-PWD (Shared Password)
- EAP-TTLS (Tunneled Transport Layer Security)
- EAP-IKEv2 (Internet Key Exchange v2)
- **EAP-FAST (Flexible Authentication via Secure Tunneling)**
- EAP-SIM (Subscriber Identity Module)
- EAP-AKA (UMTS Authentication and Key Agreement)
- EAP-AKA‘ (Authentication and Key Agreement für 3GPP)
- EAP-GTC (Generic Token Card)
- EAP-EKE (Encrypted key exchange)

802.1x Erfahrungen – Authentisierungsmethoden

- EAP-TLS (Transport Layer Security)
  - Unterstützt Zertifikate
  - Wie kommen die Zertifikate aufs Gerät?
  - Wie werden die Zertifikate erneuert?
  - Wie können Zertifikate gesperrt werden?
  - Authentisierung braucht Zeit! ⇨ Roaming bei Voice-WLAN beachten!
- EAP-MSChapV2 (MS Chap v2)
  - Passwort basierend
    IMMER nur innerhalb von Protected EAP! (PEAP/MS-ChapV2)
  - Wie kommt das Passwort aufs Gerät?

802.1x Erfahrungen – Authentisierungsmethoden

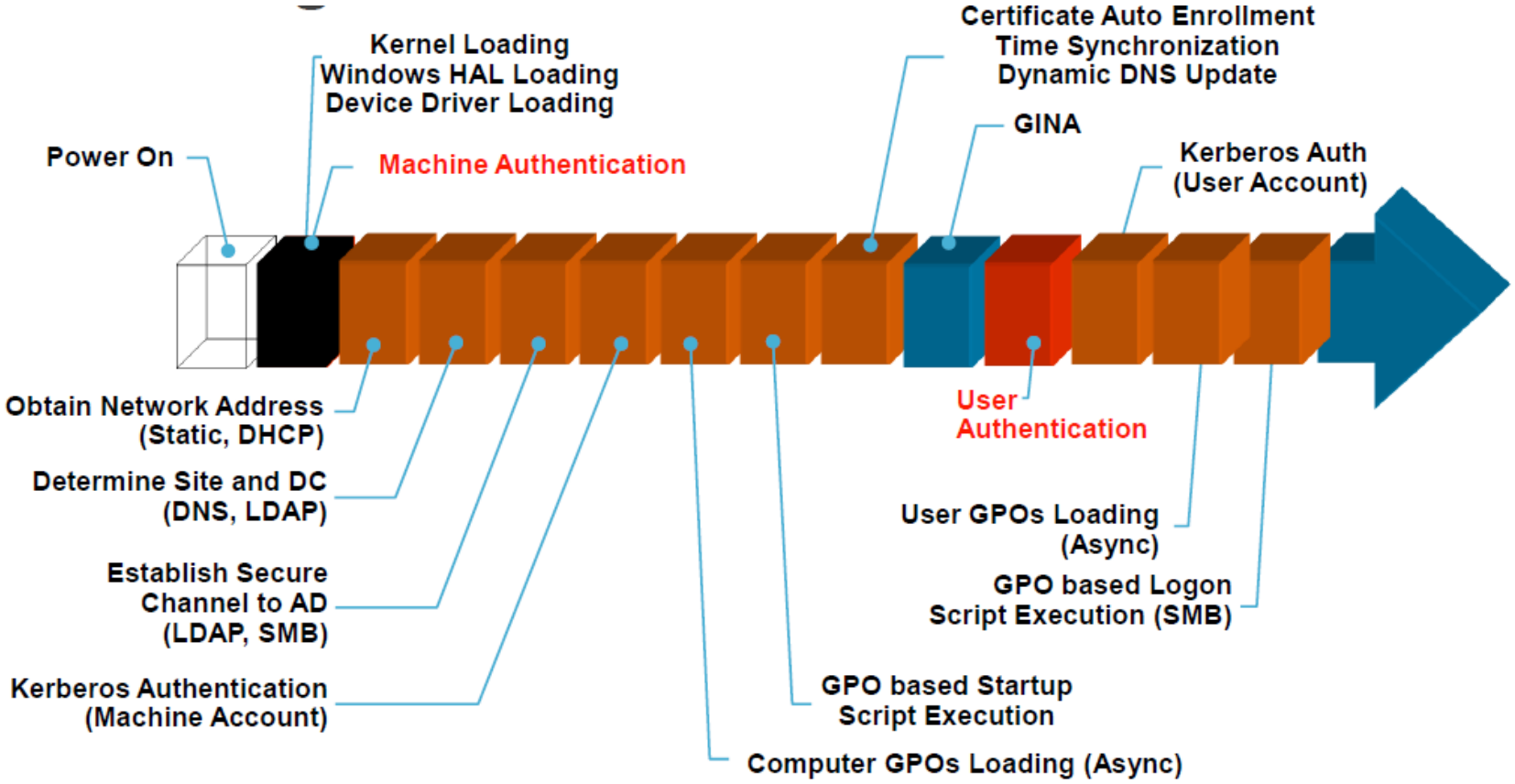
- EAP-MD5
  - Passwort basierend
    Kein «Mutual Authentication».
  - Passwort wird durch MD5 Hash übertragen.
  - Wie kommt das Passwort aufs Gerät?

- MAC Authentication Bypass (MAB)
  - Identifikation via MAC-Adresse für Geräte ohne 802.1x
  - Für Geräte ohne sinnvolle Verwaltungsmöglichkeit.

802.1x Erfahrungen – Authentisierungsmethoden

- EAP-FAST / EAP-CHAINING
  - Verknüpfung von verschiedene Authentisierungsmethden und Identitäten.
  - Häufig Angefragt für Schule und «Shared desktops» Umgebungen.

802.1x Erfahrungen – Windows



NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – Authentisierungsmethoden „Key–Takeaway‘s“

- Verwende möglichst starke Authentisierungsmethoden

- Verwende Existierende Authentisierungsmethoden
  - Ist AD-Domain vorhanden:
    - Verwende EAP-PEAP und Computer Domain Credentials
  - Ist ein CA vorhanden
    - Verwende EAP-TLS mit Zertifikate

- Gibt es für das Gerät es kein Supplikant
  - Verwende MAB

- Ist es eine «stille Gerät» ohne Supplikant
    - Ersetze es mit eine neue Gerät mit Supplikant
    - Schalte 802.1x ab auf diesen port!

802.1x Erfahrungen – Betrieb & Authentisierungsmethoden

- Authentisierungs-Reihenfolge
  - MAB ⇨ 802.1x?
    - «Authentisierungsfehler» für reine 802.1x Geräte da unbekannte MAC.
    - Prophylaktisch alle MACs erfassen?
  - 802.1x ⇨ MAB
    - Timeouts beachten!
    - Wie schnell gibt ein Nicht-802.1x Gerät DHCP auf?

- Wieviele MAC-Adressen pro Endgerät?
  - Wird auf PCs VMWare im Bridge-Mode verwendet?

802.1x Erfahrungen – Betrieb und Authentisierung „Key–Takeaway‘s“

- Verwende möglichst MAB ⇨ 802.1x?
  - Dann gibt es weniger Timer-Tuning zu machen
- Periodische Re-Authentisierung?
  - Versuche es zu vermeiden!
- Erfassen von Mac Adressen:
  - Wie wird neue Hardware installiert?
    - Dedizierte Staging-Ports?
    - MAB Authentisierung?
    - Intel vPro mit Zertifikat für Pre-OS Authentication?
- Guest Access
  - WLAN oder auch Wired?

802.1x Erfahrungen – Betrieb und Authentisierung „Key–Takeaway‘s“

- Kunden Anforderungen

Bank/Industrie

- Identifikation
- 9-17 Betrieb
- Onboarding
- GBL-Systeme
- GästeAccess

Spital

- “PublicSpace”
- 24 Std Betrieb
- Onboarding
- Medizin-Geräte
- GästeAccess

Schule

- Hetrogene Clients
- Massen-Mutationen
- GBL
- GästeAccess

802.1x Erfahrungen – Fallback-Szenarien

- Betriebssicherheit / Verfügbarkeit!
- Was passiert wenn der Authentisierungsserver nicht erreichbar ist?
  - Zweiter Server vor Ort?
  - Fail-Open / Critical VLAN (Aufmachen und alles reinlassen)
  - VLAN-Zuweisungen funktionieren dann nicht.
  - Group-Tags werden nicht zugewiesen.

802.1x Erfahrungen – Fallback „Key–Takeaway‘s“

- Verwende Fail-Open / Critical VLAN
  (Aufmachen und alles reinlassen)
  - NB! VLAN Zuweisung funktioniert dann nicht.

- Wenn die Authentication Servers wieder aktiv werden, werden alle unbekannte Devices ausgesperrt.

802.1x Erfahrungen – Testing

- Tests für alle Szenarien definieren.
  - Wie reagiert der jeweilige Endgerät auf Authentication requests?
  - Was passiert bei einem Switchreboot?
  - Was passiert wenn Authentisierungsserver nicht erreichbar ist?
  - Was passiert bei einem Switchreboot wenn Authentisierungsserver nicht erreichbar ist?
  - Was passiert wenn der Authentisierungsserver wieder erreichbar ist?
  - ...

802.1x Erfahrungen – Testing

- Wenn neuer Gerätetyp gefunden wird:
  - Testszenarien überarbeiten.
- Wenn Szenarien ergänzt oder Konfiguration angepasst werden:
  - Alle Tests wiederholen!
- Testen, testen, testen, testen, testen, testen, …
- Wir nennen dies PoC – Proof of Concept.

802.1x Erfahrungen – Testing „Key–Takeaway‘s“

- Testen, testen, testen, testen, testen, testen, …
- Proof of Concept macht den grössten Teil des Zeitaufwandes des gesamten Projektes aus!

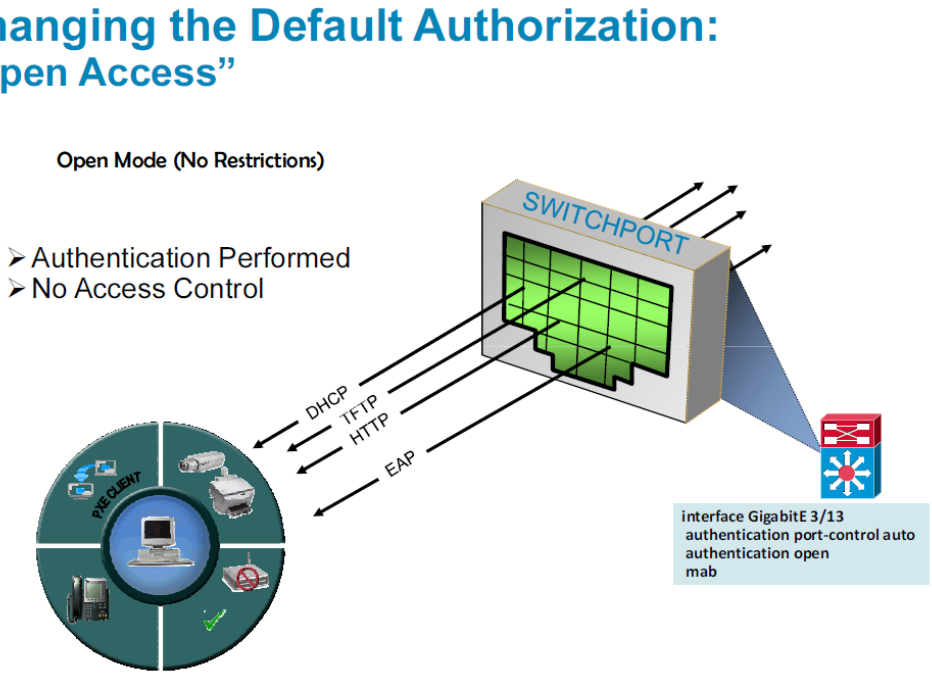
Geschätzt >50%

- Wenn PoC richtig gemacht ist, ist der Rollout «nur» Fleissarbeit

802.1x Erfahrungen – Rollout

Authentication Mode Open

- 802.1x ohne Filterung.
- Erlaubt das Testen der Clients ohne den Betrieb zu stören.
- Aufräumen der Problemfälle vor Scharfschaltung.

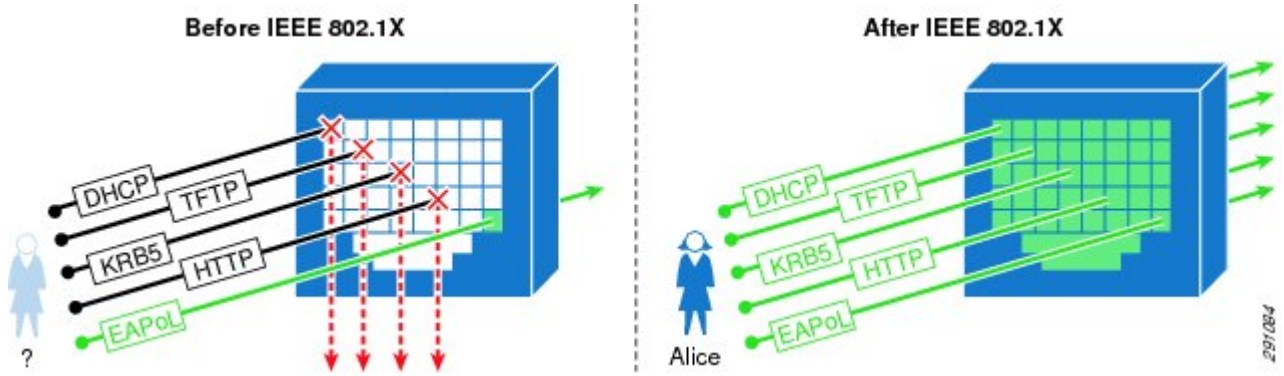


NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – Rollout

Scharfstellung: High Security Mode

- 802.1x mit
  - Default No Access
  - VLAN Zuweisung
- Scharfschaltung pro Port, pro Switch.

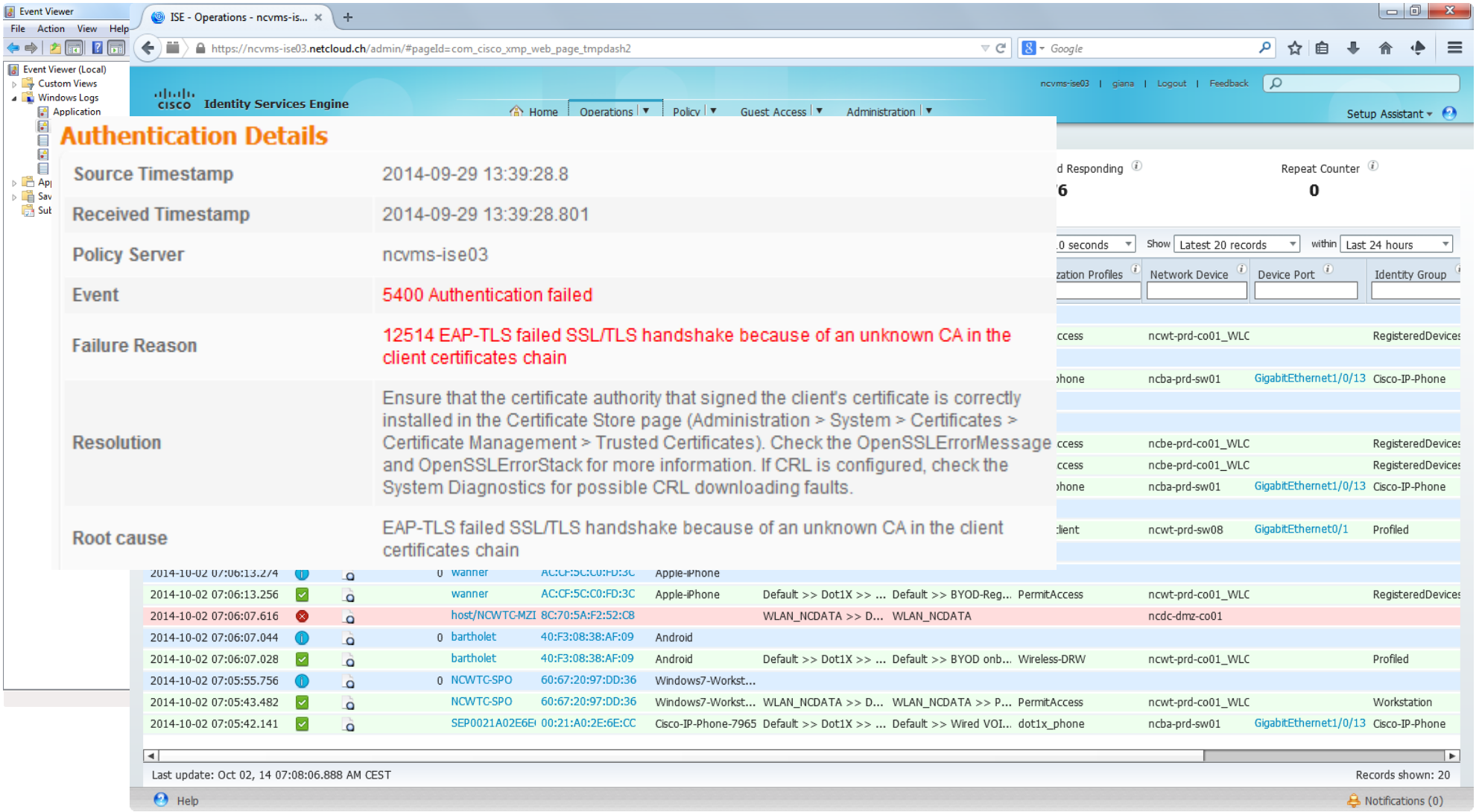


NETCLOUD
ICT PROFESSIONALS

802.1x Erfahrungen – Betrieb & Logs

- Ein gutes Log ist pures Gold wert!
- Betrieb wird fast nur mit dem Log arbeiten.
- Betrieb muss Probleme schnell eingrenzen können.

802.1x Erfahrungen – Betrieb & Logs



NETCLOUD ICT PROFESSIONALS

802.1x Erfahrungen – Zusammenfassung

- Klassisches 80/20 Projekt
  - 80% Vorbereitung
  - 20% «Doing» / «Rollout»

- Erstellen eines Highlevel Design / Grobkonzept – Was ist das Ziel?
  - Sicherheit erhöhen?
  - Betrieb vereinfachen?
  - Konfiguration-Vereinfachung?

- Involviere die
  - Netzwerk Abteilung
  - Client-Verantwortliche
  - Server-Verantwortliche
  - Security-Officers

- Projekt startet mit dem Inventar

- Führe auf jeden fall ein PoC durch

802.1x Erfahrungen – Zusammenfassung

- Windows-Clients sind das kleinste Problem
- Verwaltungsmöglichkeiten der Clients beachten
- Applikationen und Einsatzgebiet können Authentisierungsmethode bestimmen.
- MAB für Geräte ohne 802.1x Support.
- Lösung muss gute Logs bieten.

802.1x Erfahrungen – Dot1x ist der anfang…

- Wo geht’s weiter?
  - Profiling
  - Posture Checks
  - Trustsec
  - MAC Sec
  - PxGrid

- Integration mit
  - NextGen Firewall
  - Proxy
  - IPS
  - Antivirussoftware

Konnten wir Ihre Fragen beantworten?
Herzlichen Dank!

NETCLOUD
ICT PROFESSIONALS