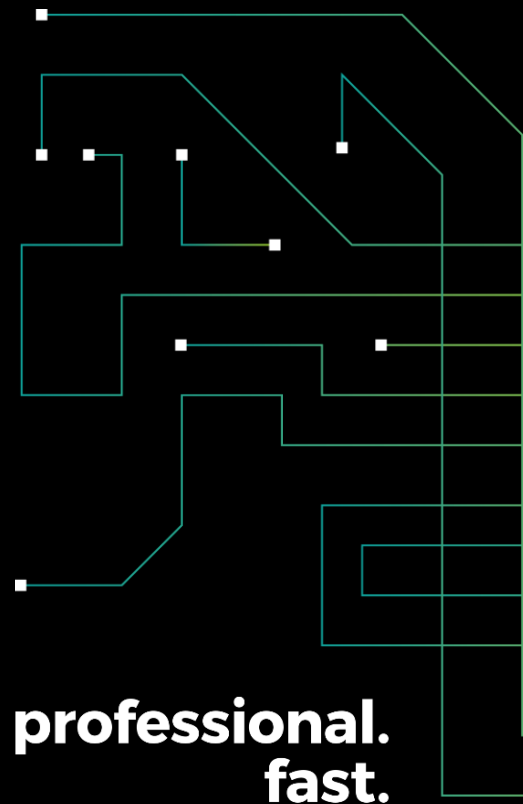
VEEAM BACKUP-INFRASTRUKTUR

Hardening & Security
base-IT Security Audit



professional.
fast.
secure.

Christian Tomas

Clemens Landl

BASE-IT EXPERTEN

Christian Tomas

- VEEAM Certified Engineer

- Christian.tomas@baseit.at
- +43 676 / 897 424 298

Clemens Landl

- Teamleitung Hybrid Cloud Team

- Clemens.landl@baseit.at
- +43 676 / 897 424 125

AGENDA

- VEEAM v12.3 – News & Features
- Why VEEAM? Security like no other
- Hardening beneath backup
- base-IT Backup Audit

VEEAM V12.3 – NEWS & FEATURES

- Microsoft Entra ID support
- Microsoft Server 2025 official supported
- Indicators of Compromise (IoC) Detection
- Veeam Thread Hunter

WHY VEEAM?

- Hardware agnostisch
- Eine Plattform für das Backup sämtlicher Workloads
- Simpel & Flexibel
- Hohe Skalierbarkeit (5 Workloads – Unlimitiert)
- Sehr hoher Sicherheitsstandard out of the Box

base it

SECURITY

VEEAM SECURITY FEATURES

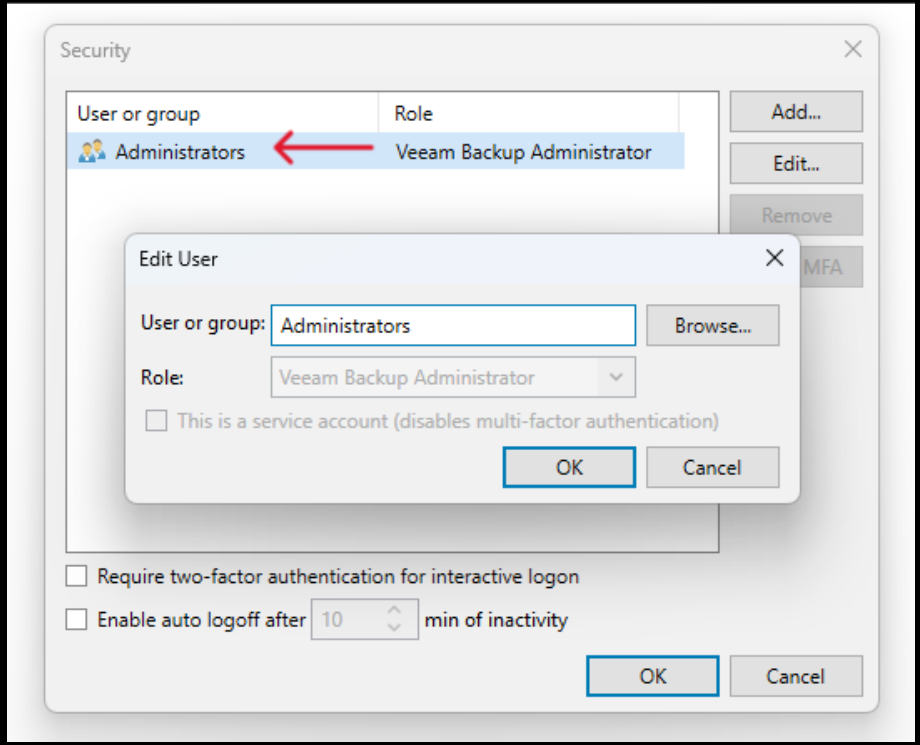
TEIL 1

- RBAC
  - Bsp. Backup Admin, Backup Operator, Restore Operator, View only
- MFA für Veeam Konsole
- 4 Augen Prinzip
- Configuration Backup & PW Loss Protection

RBAC
WELCHE ROLLEN GIBT ES?

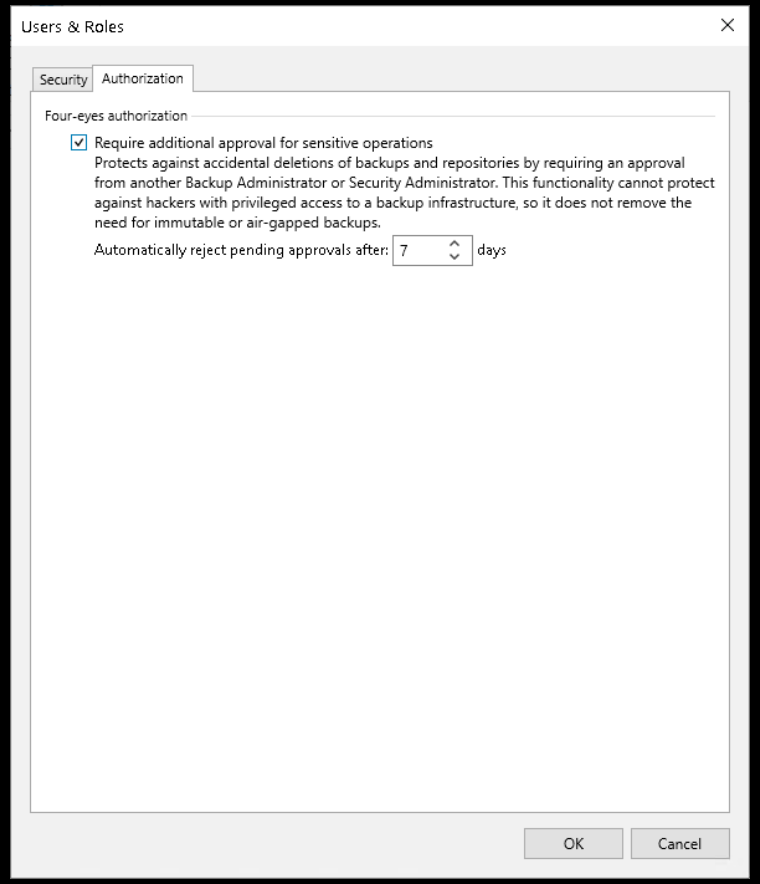
- Veeam Backup Administrator
  - Vollzugriff auf sämtliche Komponenten der Veeam Konsole
- Veeam Security Administrator
  - Kann Credentials hinzufügen, ändern oder löschen (z.b. Serviceuser)
  - Kann 4 Augen Authorizierungen bestätigen
- Veeam Restore Operator
  - Kann Restore Operationen ausführen
- Veeam Backup Operator
  - Kann existierende Jobs starten/stoppen
  - Kann Backups exportieren
- Veeam Backup Viewer
  - Lesender Zugriff auf die meisten Veeam Funktionen

MFA FÜR VEEAM KONSOLE



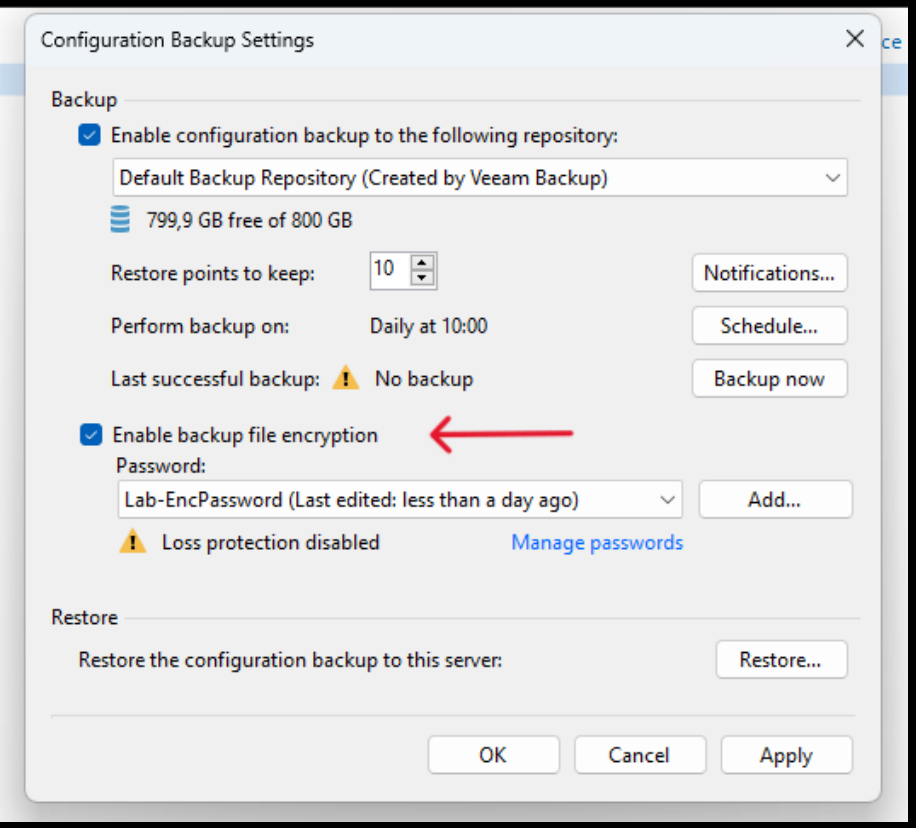
- Kann nur auf einzelne User aktiviert werden, Gruppen sind nicht möglich.
- Auto logoff sollte ebenfalls gleich mitaktiviert werden
- Sämtliche bekannten Authenticator Apps werden unterstützt

VIER AUGEN AUTHENTIFIZIERUNG



- Setzt mindestens zwei User mit Backup Administrator oder Security Administrator Rolle voraus
- Aktionen die eine four-eyes authorization verlangen:
  - Löschen von Backups
  - Entfernen von Repositories
  - Änderungen RBAC inkl. MFA
- Limitierungen:
  - Setzt Veeam VUL oder Enterprise Plus voraus
  - Löschoperationen über PS, API oder Veeam BEM nicht mehr möglich

CONFIGURATION BACKUP
UND PW LOSS PROTECTION



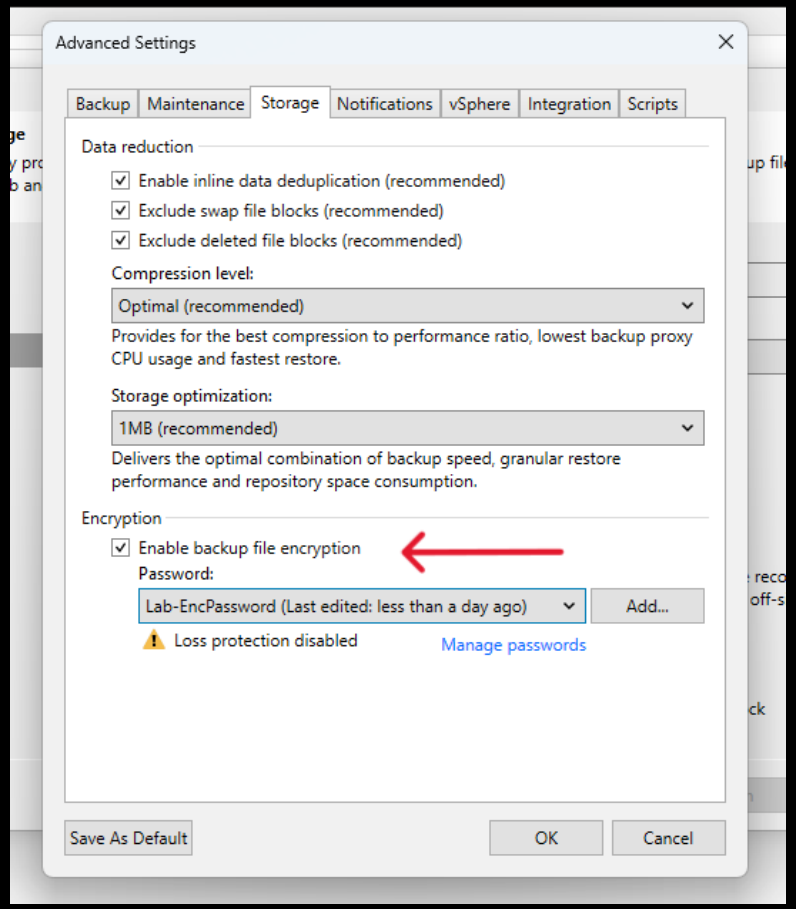
- Fungiert als Backup des Backupservers
- Schneller Wiederanlauf bei irreparablen Schäden am Backupserver oder Fehlkonfigurationen
- Target für Config Backup unbedingt ausserhalb des Backupserver/ Backup Infrastruktur
- Loss Protection über Backup Enterprise Manager (BEM)
  - Sichert sämtliche verwendeten Encryption Passwörter in eine eigene verschlüsselte Datenbank, merkt sich aktuelle und historische Passwörter
  - BEM ebenfalls unabhängig vom Backupserver betreiben!

VEEAM SECURITY FEATURES

TEIL 2

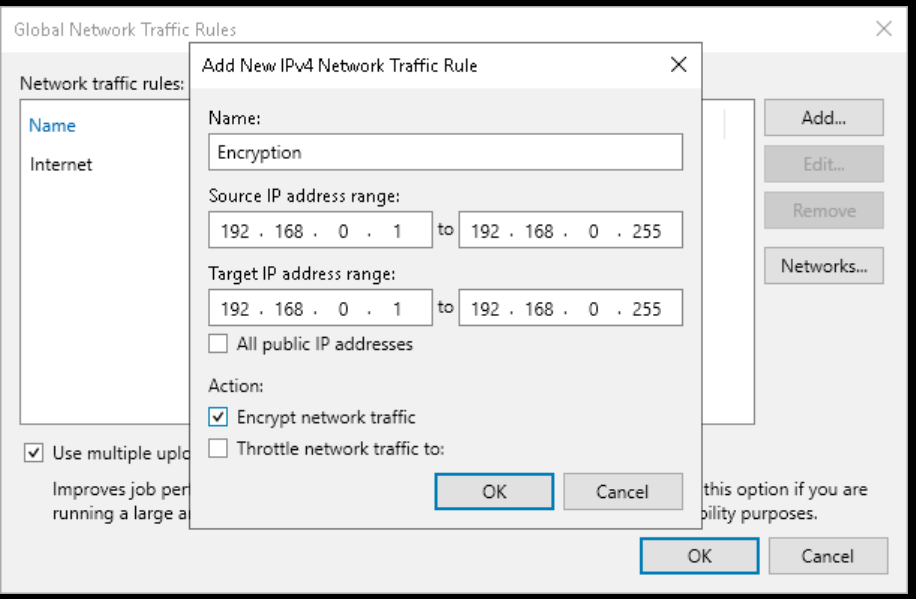
- Backup Encryption
- Traffic Encryption
- Security & Compliance Analyzer
- Malware Detection / Veeam Threat Hunter

BACKUP ENCRYPTION



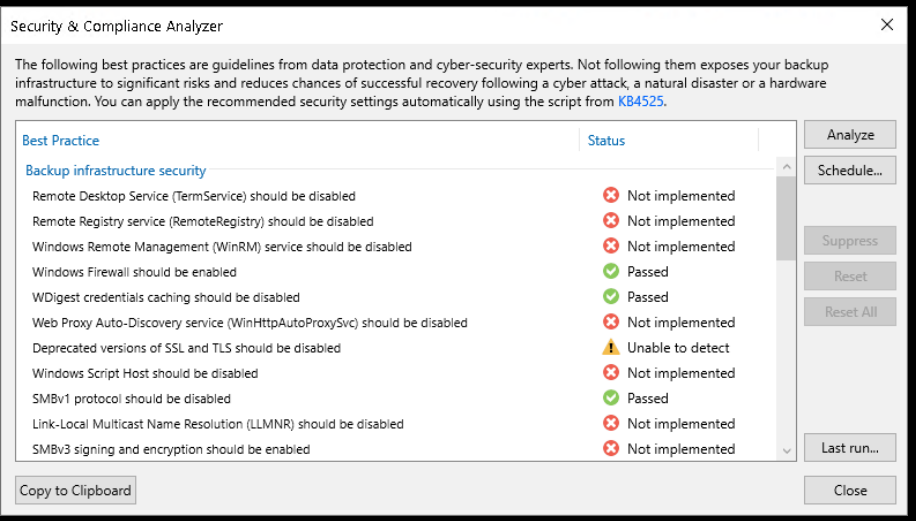
- Verschlüsselt Backup auf
  - Disk
  - Tape
  - Object Repository (Cloud und Onprem)
- Schutz vor unberechtigtem Zugriff auf Backup Daten
- Besonders zu empfehlen bei Offsite- und Tapebackup

TRAFFIC ENCRYPTION



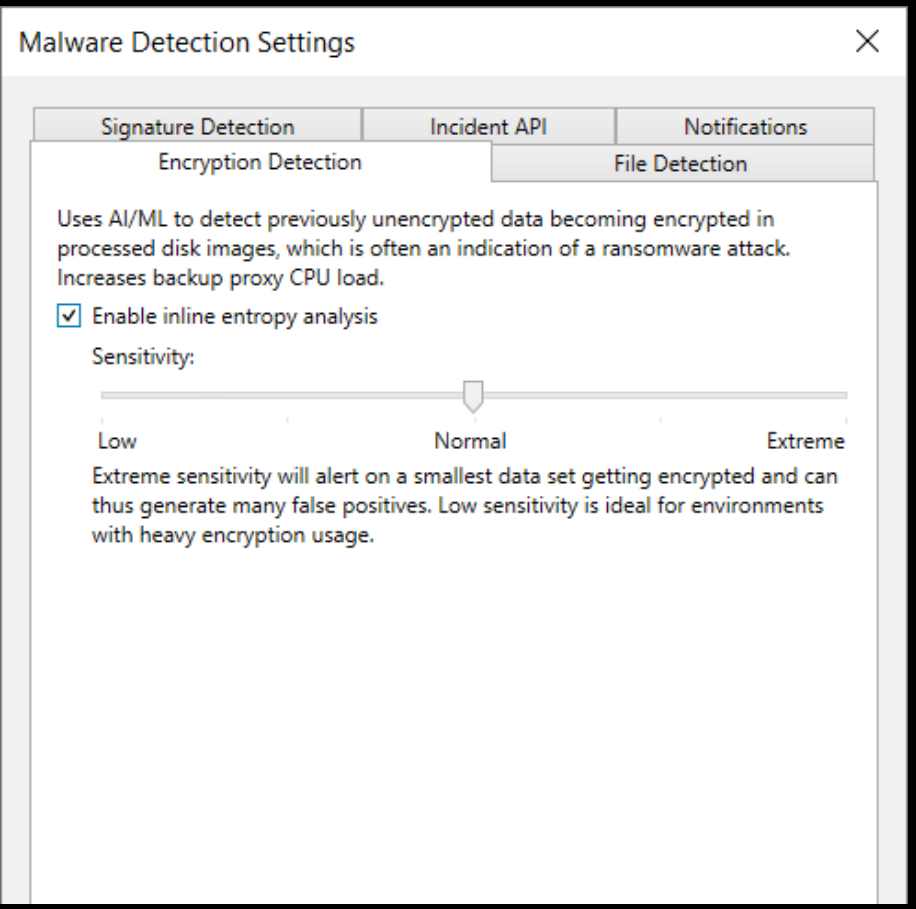
- TLS Zertifikate für Management zwischen den Veeam Komponenten
- TLS encrypted Traffic für Transfer der Backup Daten
- Standardmäßig ist nur der Traffic zwischen öffentlichen Netzen verschlüsselt

SECURITY & COMPLIANCE ANALYZER



- Seit V12 (Veeam BPA)
- Führt eine Selbstdiagnose von Veeam- und Serversettings durch
- Wird mit jedem größeren Release um neue Testpunkte erweitert

MALWARE DETECTION / VEEAM THREAT HUNTER



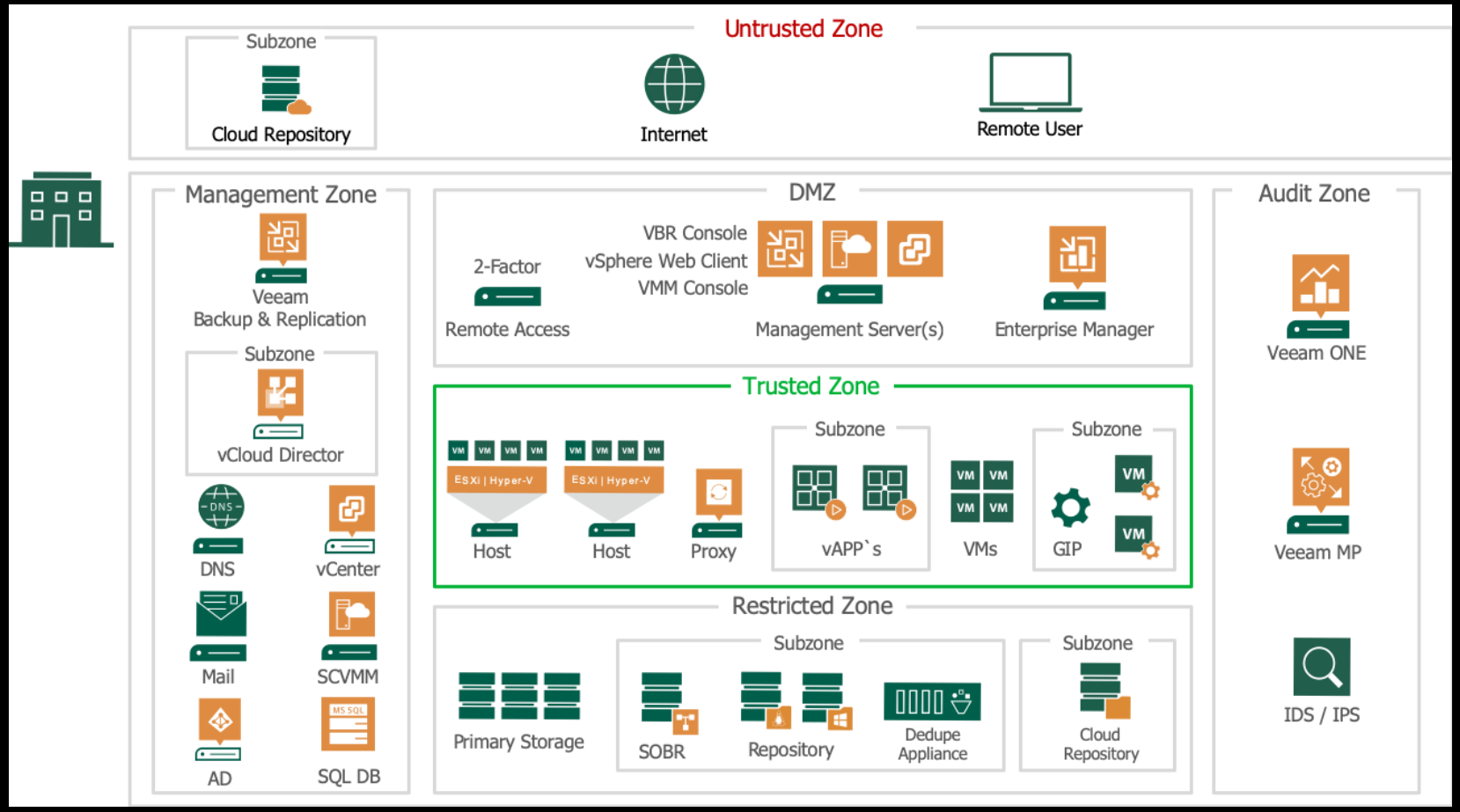
- Untersucht während des Backups auf Malware, veschlüsselte Files, Onione Links, …
- Seit V12.3 bietet Veeam mit dem Thread Hunter eine eigene signature-based scan engine an
- YARA Scans – Rule-based detection
  - Backups auf z.B. spezifische Schlagwörter durchsuchen
- Scan Backup & Secure Restore
  - Letzten sauberen Backup Stand finden

base it

HARDENING BENEATH BACKUP

SECURE BY DESIGN

IDEALER AUFBAU DER BACKUP UMGEBUNG



NETZWERKSEGMENTIERUNG
BACKUP INFRASTRUKTUR

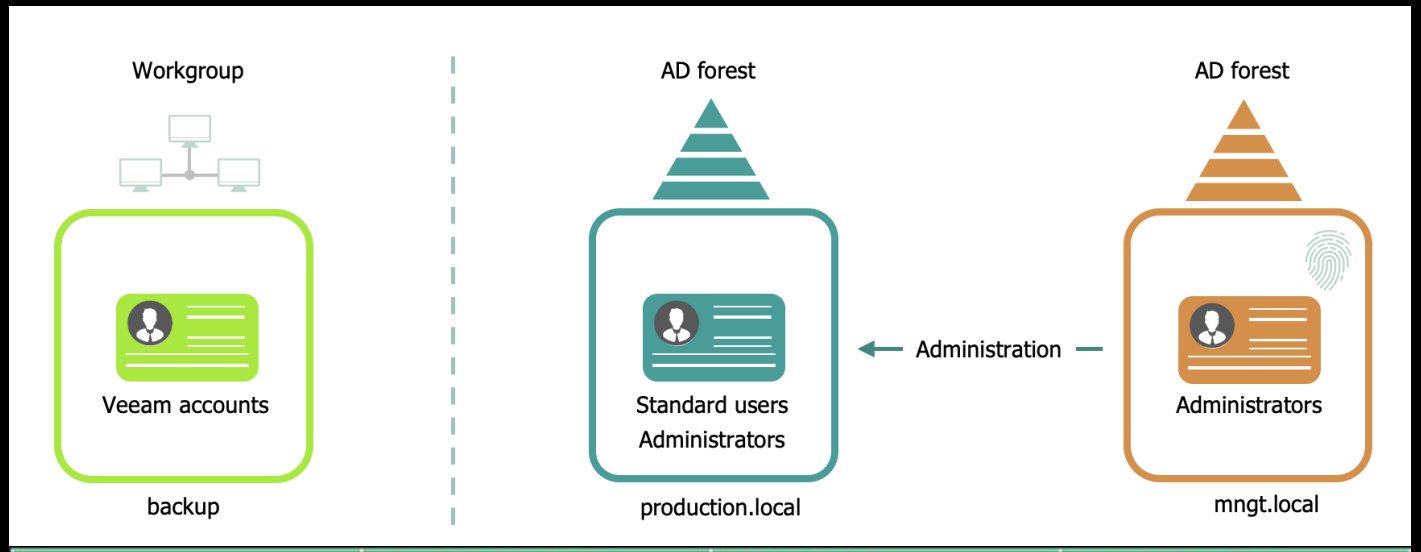
- Für den Betrieb einer sicheren Backup Infrastruktur sind 4 getrennte Netze notwendig:
  - Backup Traffic
  - Backup OS MGMT
  - Backup HW MGMT
  - Backup Admin

SERVER HARDENING

BACKUPSERVER, REPOS, DR HOSTS, ETC.

- Hardening auf OS Ebene
  - Berechtingskonzept
  - Auditing
  - PW und Lockout Policies
- Monitoring & Alerting
- Patchmanagement OS, Backupsoftware und Firmware

AD JOIN ODER LOCAL WORKGROUP?



	Worst practice	Quick win	Best Practice
What	Single Domain	Workgroup	One-way Trusted Management Domain
Pros	Deployment Management Usage	Isolation Deployment	Isolation Management Usage
Cons	First target Pivot for lateral moves	Management Usage	Deployment

HARDENED REPOSITORY
IMMUTABILITY

- Schützt Backups für einen definierten Zeitraum vor Löschung und Veränderung
- Erreichbar durch:
  - Linux Hardened Repository (XFS Filesystem)
  - Deduplication Appliances (z.B. Dell Datadomain)
  - S3 Objectstorage mit Object Lock (z.b. Azure Blob Storage)
- Können auch gemischt werden, z.b. Linux Hardened Repository als First Tier und Dedup Appliance oder Objectstorage als Langzeitspeicher

MONITORING

- Backup Komponenten laufen unabhängig von der Produktiven Umgebung und müssen daher um einen „Tieringbruch“ zu vermeiden auch unabhängig überwacht werden
- Sichtbarkeit von Seiten der Produktivumgebung soll auf einem Minimum gehalten werden

LEAST-PRIVILEGE-PRINZIP

- Backupkomponenten die in die Produktivumgebung greifen werden mit der geringstmöglichen Berechtigung versehen (z.b. Serviceuser)
- Eigener Serviceuser pro Tätigkeit:
  - Hosts/Cluster
  - AD Backup
  - Application Aware Backup (pro Tier)
- Veeam braucht für keine Tätigkeit DomainAdmin Berechtigungen!

base it

BASE-IT BACKUP SECURITY AUDIT

BASE-IT
BACKUP SECURITY AUDIT

- Audit auf Workshop Basis
- Fragenkatalog ausgearbeitet aus Veeam Security Guidelines und langjähriger Backup und Desaster Recovery Erfahrung
- Wird ständig erweitert und sollte periodisch durchgeführt werden
- Fokus auf Security Settings
- Vollständiger Maßnahmenkatalog als Ergebnis

WAS WIRD IM AUDIT BETRACHTET?

- Backupserver, OS und Veeam Settings
- Repositories
- Berechtigungen
- Encryption
- Hardware / Infrastruktur
- Desaster Recovery

base it

Q&A

base it

Haider Straße 23 | 4052 Ansfelden | AT

+43 7229 87800 - 0 | office@baseit.at |

www.baseit.at

Base-IT GmbH (unserebroschuere.at)

Management System ISO/IEC 27001:2013

TÜVRheinland ZERTIFIZIERT

www.tuv.com ID 9000002884

Microsoft Solutions Partner