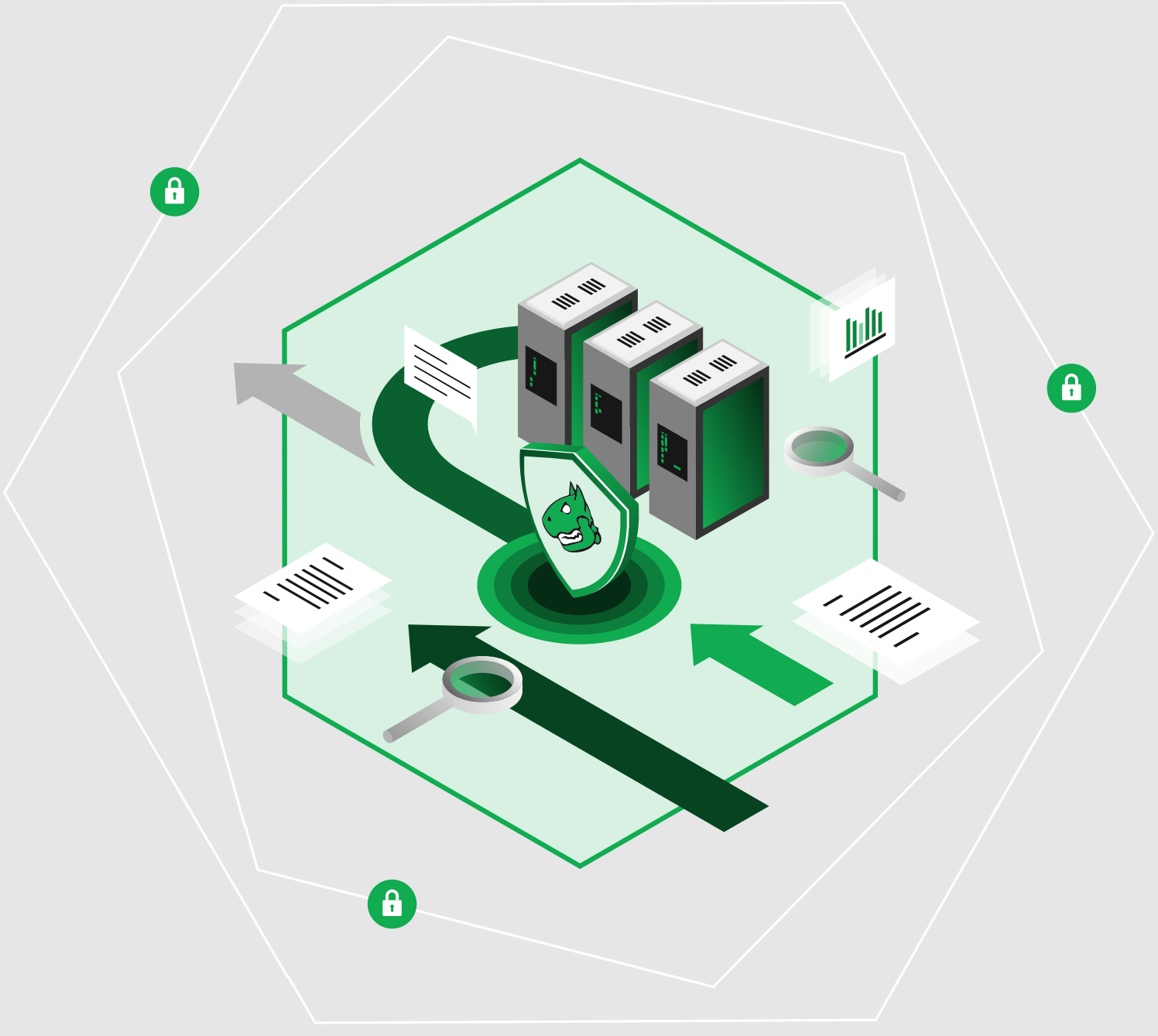
Greenbone

Handbuch

Greenbone Enterprise Appliance mit Greenbone OS 22.04



Greenbone

Greenbone AG
Neumarkt 12
49074 Osnabrück
Deutschland
https://www.greenbone.net

GOS-Version: GOS 22.04.18, 20. Februar 2024

Dies ist das Handbuch für die Greenbone Enterprise Appliance mit Greenbone OS (GOS) Version 22.04. Aufgrund der zahlreichen funktionalen Unterschiede zwischen GOS 22.04 und den vorherigen Versionen ist dieses Handbuch nicht für die Verwendung mit älteren GOS-Versionen vorgesehen. Die Greenbone Enterprise Appliance wird fortlaufend weiterentwickelt. Dieses Handbuch bemüht sich, immer den aktuellsten Softwarestand zu dokumentieren. Dennoch kann es sein, dass neueste Funktionen noch nicht in dem Handbuch berücksichtigt sind. Sollten Sie Anmerkungen oder Fehlerkorrekturen zu diesem Handbuch haben, kontaktieren Sie bitte den Greenbone Enterprise Support (https://www.greenbone.net/technischer-support/).

Inhaltsverzeichnis

KAPITEL 1

Einführung

1.1 Schwachstellenmanagement

In der IT-Sicherheit beeinflusst die Kombination von drei Elementen die Angriffsfläche einer IT-Infrastruktur:

- Cyber-Kriminelle mit ausreichend Erfahrung, Ausrüstung und Geld, um den Angriff auszuführen.
- Zugriff auf die IT-Infrastruktur.
- Schwachstellen in IT-Systemen, verursacht durch Fehler in den Anwendungen und Betriebssystemen oder inkorrekte Konfigurationen.

Falls diese drei Elemente zusammentreffen, ist ein erfolgreicher Angriff auf die IT-Infrastruktur wahrscheinlich.

Da die meisten Schwachstellen bekannt sind und behoben werden können, kann die Angriffsfläche durch Schwachstellenmanagement aktiv beeinflusst werden. Beim Schwachstellenmanagement wird die IT-Infrastruktur von außen betrachtet – genauso wie es potenzielle Cyber-Kriminelle tun würden. Das Ziel ist es, jede Schwachstelle zu finden, die in der IT-Infrastruktur vorhanden sein könnte.

Schwachstellenmanagement identifiziert Schwachstellen in der IT-Infrastruktur, bewertet deren Risikopotenzial und empfiehlt konkrete Maßnahmen zur Behebung. Auf diese Weise können Angriffe durch gezielte Vorsorgemaßnahmen verhindert werden. Dieser Prozess – vom Erkennen über die Behebung bis hin zur Überwachung – wird kontinuierlich durchgeführt.

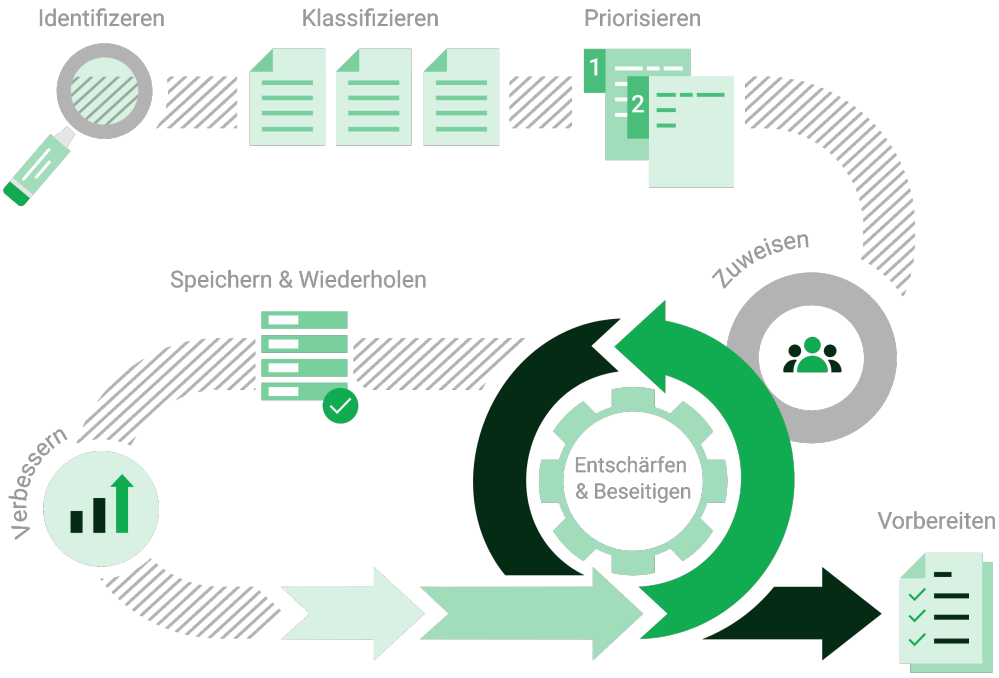


Abb. 1.1: Prozess des Schwachstellenmanagements

1.2 Greenbone Enterprise Appliance

Die Greenbone Enterprise Appliance ist eine Appliance für das Schwachstellenmanagement, die als Hardware- und virtuelle Modelle erhältlich ist. Sie unterstützt Unternehmen und Behörden beim automatisierten und integrierten Bewerten und Managen von Schwachstellen.

1.2.1 Komponenten und Anwendungsbereich

Die Appliance besteht aus dem Greenbone Operating System (GOS), auf dem der Greenbone Enterprise Feed installiert ist, einem Scandienst, der Web-Oberfläche und, im Falle einer physischen Appliance, einer speziellen Hardware. Der Feed liefert die Schwachstellentests (VTs), die der Scandienst verwendet, um vorhandene Schwachstellen im untersuchten Netzwerk zu erkennen.

Da jeden Tag neue Schwachstellen entdeckt werden, müssen ständig neue Schwachstellentests hinzugefügt werden. Greenbone analysiert CVE-Meldungen[1] und Sicherheitsempfehlungen von Anbietern und entwickelt neue Schwachstellentests. Der Feed wird täglich aktualisiert und bietet somit immer die neuesten Schwachstellentests, um die aktuellsten Schwachstellen zuverlässig zu erkennen.

Die Appliance ist flexibel einsetzbar und kann sowohl für Großunternehmen, für mittlere und kleine Unternehmen als auch für spezielle Anwendungsfälle wie Audits und Schulungen genutzt werden. Durch die Master-Sensor-Technologie kann die Appliance auch in Hochsicherheitsbereichen eingesetzt werden.

[1] Das Common Vulnerability and Exposures (CVE) Projekt ist ein herstellerunabhängiges Forum für die Identifikation und Veröffentlichung neuer Schwachstellen.

1.2.2 Arten von Scans

Die Appliance deckt Schwachstellen durch verschiedene Perspektiven von Cyber-Kriminellen auf:

Extern Die Appliance kann einen externen Angriff simulieren, um veraltete oder falsch konfigurierte Firewalls zu entdecken.

Demilitarisierte Zone (DMZ) Die Appliance identifiziert tatsächliche Schwachstellen, welche von Cyber-Kriminellen, die die Firewall überwunden haben, ausgenutzt werden können.

Intern Die Appliance ist zusätzlich in der Lage, Schwachstellen, die ausgenutzt werden können (z. B. durch Social Engineering oder Computerwürmer), zu entdecken. Aufgrund der möglichen Auswirkungen solcher Attacken ist diese Perspektive für die Sicherheit von IT-Infrastrukturen besonders wichtig.

DMZ- und interne Scans können sowohl unauthentifiziert als auch authentifiziert sein. Bei einem authentifizierten Scan verwendet die Appliance Anmeldedaten und kann Schwachstellen in Anwendungen entdecken, die nicht als Dienst ausgeführt werden, aber ein hohes Risikopotenzial aufweisen (z. B. Webbrowser, Office-Anwendungen oder PDF-Viewer).

1.2.3 Klassifikation und Beseitigung von Schwachstellen

Die entdeckten Schwachstellen werden mit Hilfe des Common Vulnerability Scoring System (CVSS) nach ihrem Schweregrad eingestuft. Anhand des Schweregrads kann bestimmt werden, welche Schwachstellen bei der Durchführung von Abhilfemaßnahmen vorrangig zu behandeln sind. Die wichtigsten Maßnahmen sind die, die das System vor kritischen Risiken schützen und die entsprechenden Schwachstellen beseitigen.

Grundsätzlich gibt es zwei Möglichkeiten zum Behandeln von Schwachstellen:

- Beseitigen der Schwachstelle durch Aktualisieren der Software, Entfernen der anfälligen Komponente oder Ändern der Konfiguration.
- Implementieren einer Regel in einer Firewall oder in einem Intrusion Prevention System (virtuelles Patching).

  Virtual Patching ist die scheinbare Eliminierung einer Schwachstelle durch eine ausgleichende Maßnahme. Die wirkliche Schwachstelle existiert weiterhin und Cyber-Kriminelle können die Schwachstelle ausnutzen, falls die Maßnahme versagt oder ein alternativer Ansatz genutzt wird.

Eine tatsächliche Korrektur oder ein Update der betroffenen Software ist dem Virtual Patching immer vorzuziehen.

KAPITEL 2

Vor der ersten Verwendung lesen

2.1 Nutzung einer unterstützten GOS-Version

Die Greenbone Enterprise Appliance sollte immer in einer von Greenbone unterstützten Version (inklusive Patchlevel)[2] betrieben werden. Andernfalls können die folgenden Probleme/Auswirkungen auftreten:

- Kompatibilitätsprobleme im Feed
- Nicht behobene Bugs
- Fehlende Funktionalitäten (z. B. solche, die erforderlich sind, damit VTs zuverlässig oder überhaupt funktionieren)
- Verringerte Scanabdeckung oder fehlende Schwachstellenerkennung aufgrund der oben genannten Probleme
- Nicht behobene Sicherheitslücken in den verwendeten Komponenten (z. B. GOS)

2.2 Auswirkungen auf die gescannte Netzwerkumgebung

Die Greenbone Enterprise Appliance beinhaltet einen vollständigen Schwachstellenscanner. Obwohl der Schwachstellenscanner so konzipiert wurde, dass alle negativen Auswirkungen auf die Netzwerkumgebung minimal sind, muss er während des Scans mit dem untersuchten Zielsystem interagieren und kommunizieren.

Bemerkung: Es ist die grundlegende Aufgabe der Greenbone Enterprise Appliance, ansonsten unentdeckte Schwachstellen zu finden und zu identifizieren. Der Scanner muss sich bis zu einem gewissen Grad so verhalten, wie es echte Cyber-Kriminelle tun würden.

Obwohl die standardmäßigen und empfohlenen Einstellungen die Auswirkungen des Schwachstellenscanners auf die Netzwerkumgebung auf ein Minimum beschränken, sind unerwünschte Nebeneffekte möglich. Durch die Einstellungen des Scanners können diese Nebeneffekte kontrolliert und verbessert werden.

[2] https://www.greenbone.net/roadmap-lifecycle/

Bemerkung: Die folgenden Nebeneffekte sollten zur Kenntnis genommen werden:

- Auf dem Zielsystem können Protokoll- und Warnmeldungen angezeigt werden.
- Auf Netzwerkgeräten, Überwachungslösungen, Firewalls und Intrusion-Detection-/Intrusion-Prevention-Systemen können Protokoll- und Warnmeldungen angezeigt werden.
- Firewall-Regeln und andere Intrusion-Prevention-Maßnahmen können ausgelöst werden.
- Scans können die Latenzzeit auf dem Ziel und/oder dem gescannten Netzwerk erhöhen. In extremen Fällen kann dies zu Situationen führen, die einem Denial-of-Service-Angriff (DoS-Angriff) ähneln.
- In anfälligen oder unsicheren Anwendungen können durch den Scan Fehler ausgelöst werden. Diese können weitere Fehler oder Abstürze verusachen.
- Eingebettete Systeme und Elemente der operativen Technologien mit schwachen Netzwerk-Stacks sind besonders anfällig für mögliche Abstürze oder sogar beschädigte Geräte.
- Logins (z. B. über SSH oder FTP) werden zu Banner-Grabbing-Zwecken gegen die Zielsysteme durchgeführt.
- Alle exponierten Dienste werden über verschiedene Protokolle (z. B. HTTP, FTP) zur Diensterkennung getestet.
- Scans können dazu führen, dass Benutzerkonten durch das Testen standardmäßiger Benutzername-Passwort-Kombinationen gesperrt werden.

Da das oben beschriebene Verhalten beim Schwachstellenscanning erwartet, gewünscht oder sogar erforderlich ist, sollte(n) die IP-Adresse(n) des Scanners in die Ausnahmeliste des betroffenen Systems/Diensts aufgenommen werden. Informationen zur Erstellung einer solchen Ausnahmeliste finden sich in der Dokumentation oder beim Support des jeweiligen Systems/Diensts.

Das Auslösen von Fehlern, Abstürzen oder Sperrungen mit den Standardeinstellungen bedeutet, dass Cyber-Kriminelle dasselbe zu einer ungewissen Zeit und zu einem ungewissen Ausmaß tun können. Das Finden von Schwachstellen, bevor sie von Cyber-Kriminellen gefunden werden, ist der Schlüssel zur Widerstandsfähigkeit.

Obwohl die Nebeneffekte sehr selten auftreten, wenn standardmäßige und empfohlene Einstellungen genutzt werden, erlaubt der Schwachstellenscanner die Konfiguration von invasivem Verhalten, welches die Wahrscheinlichkeit der genannten Effekte erhöht.

Bemerkung: Die oben genannten Gegebenheiten sollten berücksichtigt und die benötigte Autorisierung sollte verifiziert werden, bevor die Greenbone Enterprise Appliance zum Scannen des Zielsystems genutzt wird.

2.3 Scannen durch Netzwerkgeräte

2.3.1 Allgemeine Informationen

Das Scannen durch Netzwerkgeräte wie ein IDS (Intrusion Detection System)/IPS (Intrusion Prevention System), eine WAF (Web Application Firewall), einen Proxy oder eine Firewall sollte vermieden werden, da solche Geräte den Scan stören können, was zu folgendem unvorhersehbarem Scan-Verhalten oder Auswirkungen auf die Umgebung führen kann:

- Falsch-positive und falsch-negative Ergebnisse
- Geringe Scangeschwindigkeit
- Zu viele als offen gemeldete Ports auf dem Scanziel

- Verlorene Pakete aufgrund von TCP-Verbindungsgrenzen oder Erreichen des maximalen Sitzungslimits
- Je nach Einstellung können die Logs sehr umfangreich werden, was zu einer Überlastung des Logservers oder – falls sie komplett deaktiviert wereden – zu einem blinden Fleck führen kann.

Bemerkung: Ein solches Verhalten kann auch auftreten, wenn die maximale Anzahl von Prüfungen pro Host begrenzt ist.

2.3.2 Firewall-spezifische Informationen

Je nach Modell kann eine Firewall über verschiedene Zusatzmodule wie Deep Packet Inspection und Denial-of-Service-Schutz (DoS-Schutz) verfügen.

- Diese Module sind möglicherweise nur begrenzt konfigurierbar, z. B. allgemeines Ein- und Ausschalten pro Schnittstelle und nicht pro Quell-/Ziel-IP-Adresse.
- Einige der Module können sogar versteckt oder überhaupt nicht konfigurierbar sein, sodass die oben erwähnten Auswirkungen auftreten können, ohne dass bekannt ist, warum und wo sie auftreten.
- Die Belastung der Firewall steigt deutlich an. Im schlimmsten Fall werden nicht nur die Verbindungen für den Scanner unterbrochen, sondern die gesamte Firewall-Funktionalität kann beeinträchtigt werden, was zu einem Denial of Service führen kann.

KAPITEL 3

Greenbone Enterprise Appliance – Überblick

Die Greenbone Enterprise Appliance ist eine Appliance für das Schwachstellenscanning und -management. Sie wird in unterschiedlichen Leistungsstufen angeboten.

3.1 Hardware-Appliances

3.1.1 Große Organisationen – Greenbone Enterprise 5400/6500

Die Greenbone Enterprise 6500 und Greenbone Enterprise 5400 sind für den Einsatz in großen Organisationen ausgelegt.

Abb. 3.1: Greenbone Enterprise Appliance für große Organisationen

Sie können andere Appliances als Sensoren steuern und auch selbst als Remote-Scanner von anderen Appliances gesteuert werden.

Die Appliances werden zur einfachen Integration in das Rechenzentrum in einem 2U-19“-Gehäuse geliefert. Zur leichten Installation und Überwachung sind sie mit einem zweizeiligen LC-Display mit 16 Zeichen pro Zeile ausgestattet. Für den unterbrechungsfreien Betrieb haben sie redundante Netzteile, 4 Festplatten (HDDs) und Lüfter, die während des Betriebs gewechselt werden können.

Die Appliances verwenden RAID (Redundant Array of Independent Disks) 6 als Software-RAID. RAID ist eine Technologie zur Datenspeichervirtualisierung, bei der mehrere Festplattenkomponenten zum Zwecke der Datenredundanz zu einer oder mehreren logischen Einheiten zusammengefasst werden.

Um die Appliance zu verwalten, ist zusätzlich zu zwei Out-of-Band-Ethernet-Ports ein serieller Port vorhanden. Der serielle Port ist als ein mit Cisco kompatibler Konsolenport eingerichtet.

Für die Verbindung zu anderen Systemen können die Appliances mit bis zu vier Modulen ausgestattet werden. Die folgenden Module können in beliebiger Reihenfolge genutzt werden:

- Modul(e) mit 8 Ports GbE-Base-TX (Kupfer)
- Modul(e) mit 8 Ports 1 GbE SFP (Small Form-factor Pluggable)
- Modul(e) mit 2 Ports 10 GbE SFP+ (Enhanced Small Form-factor Pluggable)

3.1.2 Mittelgroße Organisationen und Zweigstellen – Greenbone Enterprise 400/450/600/650

Die Greenbone Enterprise 400, Greenbone Enterprise 450, Greenbone Enterprise 600 und Greenbone Enterprise 650 sind für den Einsatz in mittelgroßen Organisationen sowie in größeren Zweigstellen ausgelegt.

Abb. 3.2: Greenbone Enterprise Appliance für mittelgroße Organisationen

Sie können andere Appliances als Sensoren steuern und auch selbst als Remote-Scanner von anderen Appliances gesteuert werden.

Die Appliances werden zur einfachen Integration in das Rechenzentrum in einem 1U-19“-Gehäuse geliefert. Zur leichten Installation und Überwachung sind sie mit einem zweizeiligen LC-Display mit 16 Zeichen pro Zeile ausgestattet. Für den unterbrechungsfreien Betrieb haben sie redundante Lüfter, die während des Betriebs gewechselt werden können.

Um die Appliances zu verwalten, ist zusätzlich zu einem Ethernet-Port ein serieller Port vorhanden. Der serielle Port ist als ein mit Cisco kompatibler Konsolenport eingerichtet.

Für die Verbindung zu anderen Systemen sind die Appliances mit insgesamt zehn vorkonfigurierten und -eingestellten Ports ausgestattet:

- 8 Ports GbE-Base-TX (Kupfer)
- 2 Ports 10 GbE SFP+ (Enhanced Small Form-factor Pluggable)

Eine modulare Konfiguration der Ports ist nicht möglich. Einer der Ports wird ebenfalls als Management-Port genutzt.

3.1.3 Kleine Organisationen und Zweigstellen – Greenbone Enterprise 150

Die Greenbone Enterprise 150 ist für kleine Unternehmen sowie für kleine bis mittelgroße Zweigstellen ausgelegt.

Das Steuern von Sensoren in anderen Sicherheitszonen wird nicht unterstützt. Allerdings kann die Greenbone Enterprise 150 selbst als Remote-Scanner von anderen Appliances gesteuert werden.

Die Appliance wird in einem 1U-Stahlgehäuse geliefert. Zur einfachen Integration in das Rechenzentrum kann ein zusätzliches Rackmount-Kit genutzt werden. Die Appliance besitzt kein Display.

Um die Appliances zu verwalten, ist zusätzlich zu einem Ethernet-Port ein serieller Port vorhanden. Der serielle Port ist als ein mit Cisco kompatibler Konsolenport eingerichtet.

Abb. 3.3: Greenbone Enterprise Appliance für kleine Organisationen

Für die Verbindung zu anderen Systemen ist die Appliance mit vier GbE-Base-TX-Ports (Kupfer) ausgestattet. Einer der Ports wird ebenfalls als Management-Port genutzt.

3.1.4 Sensor – Greenbone Enterprise 35

Die Greenbone Enterprise 35 ist als Sensor für verteilte Scansysteme konzipiert.

Abb. 3.4: Hardware-Sensor

Die Appliance kann nur im Sensormodus genutzt werden und muss durch eine Master-Appliance verwaltet werden. Aus diesem Grund hat sie keine eigene Web-Oberfläche. Appliances ab Greenbone Enterprise 400/DECA können als Master für die Greenbone Enterprise 35 verwendet werden.

Die Appliance wird in einem 1U-Stahlgehäuse geliefert. Zur einfachen Integration in das Rechenzentrum kann ein zusätzliches Rackmount-Kit genutzt werden. Die Appliance besitzt kein Display.

Um die Appliances zu verwalten, ist zusätzlich zu einem Ethernet-Port ein serieller Port vorhanden. Der serielle Port ist als ein mit Cisco kompatibler Konsolenport eingerichtet.

Für die Verbindung zu anderen Systemen ist die Appliance mit vier GbE-Base-TX-Ports (Kupfer) ausgestattet. Einer der Ports wird ebenfalls als Management-Port genutzt.

	Appliance							Sensor
	Greenbone Enterprise 6500	Greenbone Enterprise 5400	Greenbone Enterprise 650 Rev. 2	Greenbone Enterprise 600 Rev. 2	Greenbone Enterprise 450 Rev. 2	Greenbone Enterprise 400 Rev. 2	Greenbone Enterprise 150	Greenbone Enterprise 35
Klasse/Anwendungsbereich	Große Unternehmen/ Dienstleister	Große Unternehmen/ Dienstleister	Mittelgroße Unternehmen/ Zweigstellen	Mittelgroße Unternehmen/ Zweigstellen	Mittelgroße Unternehmen/ Zweigstellen	Mittelgroße Unternehmen/ Zweigstellen	Kleine und mittlere Unternehmen/kleine Zweigstellen	Sensor für Managed Services/ Zweigstellenscans
Geschätzte Scankapazität* (IP-Adressen pro 24 h)	Bis zu 15.000	Bis zu 8.000	Bis zu 4.000	Bis zu 2.000	Bis zu 1.000	Bis zu 300	Bis zu 100	Bis zu 100
Gewicht (kg)	22 kg	22 kg	7 kg	7 kg	7 kg	7 kg	4 kg	4 kg
Abmessungen (BxTxH)	480x550x88 mm	480x550x88 mm	480x300x44 mm	480x300x44 mm	480x300x44 mm	480x300x44 mm	480x200x45 mm	480x200x45 mm
Netzwerke								
Management/Feed	2 Out-of-Band-Management	2 Out-of-Band-Management	1	1	1	1	1	1
Scan GbE-Base-TX	0 – 32 Ports	0 – 32 Ports	8 Ports	8 Ports	8 Ports	8 Ports	4 Ports	4 Ports
Scan 1 GbE SFP	0 – 32 Ports	0 – 32 Ports	✓	✓	✓	✓	×	×
Scan 10 GbE SFP+	0 – 8 Ports	0 – 8 Ports	2 Ports	2 Ports	2 Ports	2 Ports	×	×
Portrollen	2 Management, andere dynamisch	2 Management, andere dynamisch	10 Ports dynamisch	10 Ports dynamisch	10 Ports dynamisch	10 Ports dynamisch	4 Ports dynamisch	4 Ports dynamisch
VLAN-Support	128 pro Ethernet-Port	64 pro Ethernet-Port	64 pro Ethernet-Port	64 pro Ethernet-Port	16 pro Ethernet-Port	16 pro Ethernet-Port	8 pro Ethernet-Port	8 pro Ethernet-Port
Max. Routen pro Netzwerkschnittstelle	20	20	20	20	16	16	8	8
Hardware								
Lüfter-Drehzahlregelung	×	×	✓	✓	✓	✓	✓	✓
Redundanter Lüfter	✓	✓	✓	✓	✓	✓	×	×
Redundante Stromversorgung	✓	✓	×	×	×	×	×	×
Redundante Festplatte	✓	✓	×	×	×	×	×	×
Hot-Swap Stromversorgung	✓	✓	×	×	×	×	×	×
Hot-Swap Festplatte	✓	✓	×	×	×	×	×	×
Hot-Swap Lüfter	✓	✓	×	×	×	×	×	×
LCD	✓	✓	✓	✓	✓	✓	×	×
Stromversorgungen/ Ausgänge	2	2	1	1	1	1	1	1
Max. Leistungsaufnahme pro Versorgung	500 W	500 W	300 W	300 W	300 W	300 W	40 W	40 W
Fernbetrieb								
Master-Modus (Scan & Management)	Bis zu 80 Sensoren	Bis zu 40 Sensoren	Bis zu 20 Sensoren	Bis zu 12 Sensoren	Bis zu 6 Sensoren	Bis zu 2 Sensoren	×	×
Sensor-Modus (verwaltet via Master)	✓	✓	✓	✓	✓	✓	✓	✓
Airgap-Master	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	×	×
Airgap-Sensor	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	FTP	×
Features								
SSH v2	✓	✓	✓	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓	✓	✓	✓
GMP (API)	✓	✓	✓	✓	✓	✓	✓	×
Web-Oberfläche (G), Bericht-Plugins (P), Benachrichtigungen (A), Zeitpläne (S)	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	×
LDAP/RADIUS	✓	✓	✓	✓	✓	✓	✓	×
SNMP v2	✓	✓	✓	✓	✓	✓	✓	✓
Syslog (UDP/TCP/TLS)	✓	✓	✓	✓	✓	✓	✓	✓
IPv6-Support	✓	✓	✓	✓	✓	✓	✓	✓
RAID6	✓	✓	×	×	×	×	×	×
Zertifikat-Management	✓	✓	✓	✓	✓	✓	✓	×
Netzwerk-Namensräume	✓	✓	✓	✓	✓	✓	×	×
Remediation-Workflow	✓	✓	✓	✓	✓	✓	×	×
Backup/Wiederherstellung	Remote/USB, periodisch	Remote/USB, periodisch	Remote/USB, periodisch	Remote/USB, periodisch	Remote/USB, periodisch	Remote/USB, periodisch	USB	×

* Die tatsächlich erreichbare Zahl hängt vom Scanmuster, den Scanzielen, der Netzwerk-Infrastruktur und der Häufigkeit der Scans ab. Die angegebenen Werte für die geschätzte Scankapazität können nur als Richtwerte verstanden und nicht garantiert werden. Weitere Informationen finden sich in Kapitel *20.2* (Seite 427).

3.2 Virtuelle Appliances

3.2.1 Mittelgroße Organisationen und Zweigstellen – Greenbone Enterprise DECA/TERA/PETA/EXA

Die Greenbone Enterprise DECA, Greenbone Enterprise TERA, Greenbone Enterprise PETA und Greenbone Enterprise EXA sind für den Einsatz in mittelgroßen Organisationen sowie in größeren Zweigstellen ausgelegt.

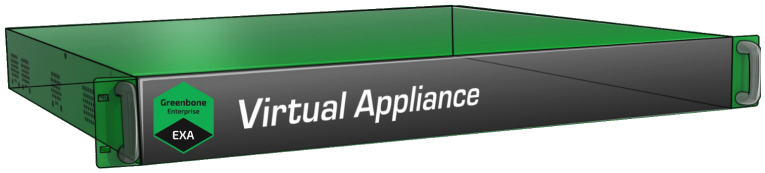


Abb. 3.5: Greenbone Enterprise Appliance für mittelgroße Organisationen

Sie können andere Appliances als Sensoren steuern und auch selbst als Remote-Scanner von anderen Appliances gesteuert werden.

Die Appliances können mithilfe von VMware ESXi auf Microsoft Windows, MacOS und Linux-Systemen eingesetzt werden.

Für die Verbindung zu anderen Systemen sind die Greenbone Enterprise TERA/PETA/EXA mit insgesamt acht dynamischen, virtuellen Ports und die Greenbone Enterprise DECA mit insgesamt vier dynamischen, virtuellen Ports ausgestattet.

Einer der Ports wird ebenfalls als Management-Port genutzt.

3.2.2 Kleine Organisationen – Greenbone Enterprise CENO

Die Greenbone Enterprise CENO ist für kleine Unternehmen sowie für kleine bis mittelgroße Zweigstellen ausgelegt.

Das Steuern von Sensoren in anderen Sicherheitszonen wird nicht unterstützt. Allerdings kann die Greenbone Enterprise 150 selbst als Remote-Scanner von anderen Appliances gesteuert werden.

Die Appliance kann mithilfe von VMware ESXi auf Microsoft Windows, MacOS und Linux-Systemen eingesetzt werden.

Für die Verbindung zu anderen Systemen ist die Appliance mit insgesamt vier dynamischen, virtuellen Ports ausgestattet.

Einer der Ports wird ebenfalls als Management-Port genutzt.

3.2.3 Sensor – Greenbone Enterprise 25V

Die Greenbone Enterprise 25V ist als Sensor für verteilte Scansysteme konzipiert.

Die Appliance kann nur im Sensormodus genutzt werden und muss durch eine Master-Appliance verwaltet werden. Aus diesem Grund hat sie keine eigene Web-Oberfläche. Appliances ab Greenbone Enterprise 400/DECA können als Master für die Greenbone Enterprise 25V verwendet werden.

Die Appliance kann mithilfe von VMware ESXi auf Microsoft Windows, MacOS und Linux-Systemen eingesetzt werden.

Für die Verbindung zu anderen Systemen ist die Appliance mit insgesamt vier dynamischen, virtuellen Ports ausgestattet.

Einer der Ports wird ebenfalls als Management-Port genutzt.

3.2.4 Schulungen und Audit-via-Laptop

Die Greenbone Enterprise ONE ist für spezielle Anforderungen wie Audits mit einem Laptop oder Schulungen ausgelegt. Sie kann weder andere Appliances als Sensoren steuern noch selbst als Sensor von einer anderen Appliance gesteuert werden.

Die Appliance kann mithilfe vieler Virtualisierungsumgebungen eingerichtet werden. Die empfohlene und unterstützte Umgebung ist Oracle VirtualBox.

Die Appliance ist mit einem virtuellen Port für Management, Scans und Updates ausgestattet.

Die Appliance besitzt alle Funktionen wie die Appliances für mittelgroße und große Unternehmen, abgesehen von den folgenden:

- Master-Modus: Die Greenbone Enterprise ONE kann andere Appliances nicht als Sensoren steuern.
- Sensor-Modus: Die Greenbone Enterprise ONE kann nicht als Remote-Scanner von einer anderen Appliance gesteuert werden.
- VLANs: Die Greenbone Enterprise ONE unterstützt keine VLANs auf virtuellen Ports.

Bemerkung: Die Greenbone Enterprise ONE ist für die Verwendung auf mobilen Computern optimiert. Features wie Remote-Scanner, die für das Schwachstellenmanagement von Unternehmen benötigt werden, sind nur auf voll ausgestatteten Appliances verfügbar.

	Appliance						Sensor
	Greenbone Enterprise EXA	Greenbone Enterprise PETA	Greenbone Enterprise TERA	Greenbone Enterprise DECA	Greenbone Enterprise CENO	Greenbone Enterprise ONE	Greenbone Enterprise 25V
Klasse/Anwendungsbereich	Mittelgroße Unternehmen/ Zweigstellen	Mittelgroße Unternehmen/ Zweigstellen	Mittelgroße Unternehmen/ Zweigstellen	Mittelgroße Unternehmen/ Zweigstellen	Kleine und mittlere Unternehmen/kleine Zweigstellen	Spezielle Anwendungen/ Schulung/Audit-via-Laptop	Sensor für Managed Services/ Zweigstellenscans
Geschätzte Scankapazität* (IP-Adressen pro 24 h)	Bis zu 5.000	Bis zu 2.000	Bis zu 1.000	Bis zu 300	Bis zu 100	Bis zu 100	Bis zu 100
Benötigter Arbeitsspeicher auf Hypervisor (GB)	24	16	8	8	8	6	6
vCPUs	12	8	6	4	2	2	2
Netzwerke							
Virtuelle Ports	8	8	8	4	4	1	4
Portrollen	8 Ports dynamisch	8 Ports dynamisch	8 Ports dynamisch	4 Ports dynamisch	4 Ports dynamisch	1 Port Management/ Scan/Update	4 Ports dynamisch
Max. Routen pro Netzwerkschnittstelle	8	8	8	8	8	0	0
Fernbetrieb							
Master-Modus (Scan & Management)	Bis zu 24 Sensoren	Bis zu 12 Sensoren	Bis zu 6 Sensoren	Bis zu 2 Sensoren	✕	✕	✕
Sensor-Modus (verwaltet via Master)	✓	✓	✓	✓	✓	✕	✓
Airgap-Master	✕	✕	✕	✕	✕	✕	✕
Airgap-Sensor	FTP	FTP	FTP	FTP	FTP	✕	✕
Open-VM-Tools	✓	✓	✓	✓	✓	✕	✓
Unterstützte Hypervisoren	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi)	Oracle VirtualBox, VMware Workstation Pro, VMware Workstation Player	Microsoft Hyper-V, VMware vSphere Hypervisor (ESXi), Huawei FusionCompute
Features							
SSH v2	✓	✓	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓	✕	✓
GMP (API)	✓	✓	✓	✓	✓	✓	✕
Web-Oberfläche (G), Bericht-Plugins (P), Benachrichtigungen (A), Zeitpläne (S)	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	G, P, A, S	✕
LDAP/RADIUS	✓	✓	✓	✓	✓	✕	✕
SNMP v2	✓	✓	✓	✓	✓	✕	✓
Remediation-Workflow	✓	✓	✓	✓	✕	✕	✕
Syslog (UDP/TCP/TLS)	✓	✓	✓	✓	✓	✕	✕
IPv6-Support	✓	✓	✓	✓	✓	✓	✓
Zertifikat-Management	✓	✓	✓	✓	✓	✓	✕
Backup/Wiederherstellung	Remote, periodisch, VM-Snapshot	Remote, periodisch, VM-Snapshot	Remote, periodisch, VM-Snapshot	Remote, periodisch, VM-Snapshot	Remote, periodisch, VM-Snapshot	VM-Snapshot	VM-Snapshot

* Die tatsächlich erreichbare Zahl hängt vom Scanmuster, den Scanzielen, der Netzwerk-Infrastruktur und der Häufigkeit der Scans ab. Die angegebenen Werte für die geschätzte Scankapazität können nur als Richtwerte verstanden und nicht garantiert werden. Weitere Informationen finden sich in Kapitel *20.2* (Seite 427).

KAPITEL 4

Leitfaden zum Benutzen der Greenbone Enterprise Appliance

Die folgenden Schritte sind wesentlich in der Benutzung der Greenbone Enterprise Appliance:

- Die Appliance einrichten → Kapitel *5* (Seite 28)
- Das Greenbone Operating System auf die neueste Version upgraden → Kapitel *6* (Seite 58) und *7.3.4* (Seite 150)
- Den Feed updaten → Kapitel *7.3.6* (Seite 151)
- Einen Scan durchführen → Kapitel *10* (Seite 210)
- Einen Bericht lesen und nutzen → Kapitel *11.2.1* (Seite 293)

Die folgenden Schritte sind fortgeschrittener:

- Einen authentifizierten Scan durchführen → Kapitel *10.3* (Seite 220)
- Zeitpläne und Benachrichtigungen verwenden, um den Scanvorgang zu automatisieren → Kapitel *10.10* (Seite 272) und *10.12* (Seite 277)
- Übersteuerungen nutzen, um Falsch-Positiv-Meldungen zu verwalten → Kapitel *11.8* (Seite 315)
- Ein Master-Sensor-Setup für verteiltes Scannen verwenden → Kapitel *16* (Seite 380)

KAPITEL 5

Die Greenbone Enterprise Appliance einrichten

5.1 Voraussetzungen für das Setup

5.1.1 Greenbone Enterprise 6500/5400

Die Greenbone Enterprise 5400 und Greenbone Enterprise 6500 sind 19-Zoll-montierbar und benötigen zwei Rackeinheiten. Rackhalter für die Installation in einem 19-Zoll-Rack sind im Lieferumfang enthalten.

Für die Verkabelung besitzen die Greenbone Enterprise 5400 und Greenbone Enterprise 6500 entsprechende Anschlüsse an der Front und der Rückseite:

- **Front**
  - 1 RS-232 serieller Port, Cisco-kompatibel, entsprechendes Kabel liegt bei
  - 2 USB-2.0-Ports
  - 2 RJ45 Ethernet-Ports als Management-Ports, gekennzeichnet mit „MGMT“
  - Bis zu 4 optionale Module mit zusätzlichen Ethernet-Ports (RJ45, SFP, SFP+ oder XFP)
- **Rückseite**
  - 1 VGA-Port
  - 2 USB-3.0-Ports
  - 2 USB-2.0-Ports
  - 1 Netzteil

Die Installation erfordert entweder einen Monitor und eine Tastatur oder eine serielle Konsole und eine Terminalanwendung.

5.1.2 Greenbone Enterprise 650/600/450/400

Die Greenbone Enterprise 400, Greenbone Enterprise 450, Greenbone Enterprise 600 und Greenbone Enterprise 650 sind 19-Zoll-montierbar und benötigen eine Rackeinheit. Rackhalter für die Installation in einem 19-Zoll-Rack sind im Lieferumfang enthalten.

Für die Verkabelung besitzen die Greenbone Enterprise 400, Greenbone Enterprise 450, Greenbone Enterprise 600 und Greenbone Enterprise 650 entsprechende Anschlüsse an der Front und der Rückseite:

- **Front**
  - 1 RS-232 serieller Port, Cisco-kompatibel, entsprechendes Kabel liegt bei
  - 2 USB-3.0-Ports
  - 6 RJ45 Ethernet-Ports
  - 2 SFP Ethernet-Ports
- **Rückseite**
  - 1 VGA-Port
  - 1 Stromanschluss

Die Installation erfordert entweder einen Monitor und eine Tastatur oder eine serielle Konsole und eine Terminalanwendung.

5.1.3 Greenbone Enterprise 150

Die Greenbone Enterprise 150 ist 19-Zoll-montierbar und benötigt eine Rackeinheit. Das optionale RACKMOUNT150-Kit stellt die Rackhalter für die Installation in einem 19-Zoll-Rack zur Verfügung.

Für eigenständige Appliances müssen vier selbstklebende Gummifüße an den entsprechenden Prägungen an der Unterseite befestigt werden.

Für die Verkabelung besitzt die Greenbone Enterprise 150 entsprechende Anschlüsse an der Front und der Rückseite:

- **Front**
  - 1 RS-232 serieller Port, Cisco-kompatibel, entsprechendes Kabel liegt bei
  - 2 USB-3.0-Ports
  - 1 HDMI-Port
  - 4 RJ45 Ethernet-Ports
- **Rückseite**
  - 1 Stromanschluss

Die Installation erfordert entweder einen Monitor und eine Tastatur oder eine serielle Konsole und eine Terminalanwendung.

5.1.4 Greenbone Enterprise 35

Die Greenbone Enterprise 35 ist 19-Zoll-montierbar und benötigt eine Rackeinheit. Das optionale RACKMOUNT35-Kit stellt die Rackhalter für die Installation in einem 19-Zoll-Rack zur Verfügung.

Für eigenständige Appliances müssen vier selbstklebende Gummifüße an den entsprechenden Prägungen an der Unterseite befestigt werden.

Für die Verkabelung besitzt die Greenbone Enterprise 35 entsprechende Anschlüsse an der Front und der Rückseite:

- **Front**
  - 1 RS-232 serieller Port, Cisco-kompatibel, entsprechendes Kabel liegt bei
  - 2 USB-3.0-Ports
  - 1 HDMI-Port
  - 4 RJ45 Ethernet-Ports
- **Rückseite**
  - 1 Stromanschluss

Die Installation erfordert entweder einen Monitor und eine Tastatur oder eine serielle Konsole und eine Terminalanwendung.

5.1.5 Greenbone Enterprise DECA/TERA/PETA/EXA

Dieser Abschnitt listet die Voraussetzungen auf, die nötig sind, um eine Greenbone Enterprise DECA, Greenbone Enterprise TERA, Greenbone Enterprise PETA oder Greenbone Enterprise EXA bereitzustellen. Alle Voraussetzungen müssen erfüllt werden.

Die virtuellen Appliances benötigen und beschränken sich auf die folgenden Ressourcen:

- Greenbone Enterprise DECA
  - 4 virtuelle CPUs
  - 8 GB RAM
  - 220 GB virtuelle Festplatte
- Greenbone Enterprise TERA
  - 6 virtuelle CPUs
  - 8 GB RAM
  - 220 GB virtuelle Festplatte
- Greenbone Enterprise PETA
  - 8 virtuelle CPUs
  - 16 GB RAM
  - 220 GB virtuelle Festplatte
- Greenbone Enterprise EXA
  - 12 virtuelle CPUs
  - 24 GB RAM
  - 225 GB virtuelle Festplatte

Die folgenden Hypervisoren werden offiziell für den Einsatz einer Greenbone Enterprise DECA/TERA/PETA/EXA unterstützt:

- Microsoft Hyper-V, Version 5.0 oder höher
- VMware vSphere Hypervisor (ESXi), Version 6.0 oder höher
- Huawei FusionCompute, Version 8.0

Für Microsoft Hyper-V wird jede Greenbone Enterprise CENO/DECA/TERA/PETA/EXA als virtuelle Maschine der 2. Generation 2 ausgeliefert.

Der erforderliche Bootmodus ist der EFI/UEFI-Boot-Modus.

5.1.6 Greenbone Enterprise CENO

Dieser Abschnitt listet die Voraussetzungen auf, die nötig sind, um eine Greenbone Enterprise CENO bereitzustellen. Alle Voraussetzungen müssen erfüllt werden.

Die virtuelle Appliance benötigt und beschränkt sich auf die folgenden Ressourcen:

- 2 virtuelle CPUs
- 8 GB RAM
- 135 GB virtuelle Festplatte

Die folgenden Hypervisoren werden offiziell für den Einsatz einer Greenbone Enterprise CENO unterstützt:

- Microsoft Hyper-V, Version 5.0 oder höher
- VMware vSphere Hypervisor (ESXi), Version 6.0 oder höher

Für Microsoft Hyper-V wird jede Greenbone Enterprise CENO/DECA/TERA/PETA/EXA als virtuelle Maschine der 2. Generation 2 ausgeliefert.

Der erforderliche Bootmodus ist der EFI/UEFI-Boot-Modus.

5.1.7 Greenbone Enterprise 25V

Dieser Abschnitt listet die Voraussetzungen auf, die nötig sind, um eine Greenbone Enterprise 25V bereitzustellen. Alle Voraussetzungen müssen erfüllt werden.

Die virtuelle Appliance benötigt und beschränkt sich auf die folgenden Ressourcen:

- 2 virtuelle CPUs
- 6 GB RAM
- 70 GB virtuelle Festplatte

Die folgenden Hypervisoren werden offiziell für den Einsatz einer Greenbone Enterprise 25V unterstützt:

- Microsoft Hyper-V, Version 5.0 oder höher
- VMware vSphere Hypervisor (ESXi), Version 6.0 oder höher
- Huawei FusionCompute, Version 8.0

Für Microsoft Hyper-V wird jede Greenbone Enterprise 25V als virtuelle Maschine der Generation 2 ausgeliefert.

Der erforderliche Bootmodus ist der EFI/UEFI-Boot-Modus.

5.1.8 Greenbone Enterprise ONE

Dieser Abschnitt listet die Voraussetzungen auf, die nötig sind, um eine Greenbone Enterprise ONE bereitzustellen. Alle Voraussetzungen müssen erfüllt werden.

Die virtuelle Appliance benötigt und beschränkt sich auf die folgenden Ressourcen:

- 2 virtuelle CPUs
- 6 GB RAM
- 130 GB virtuelle Festplatte

Die folgenden Hypervisoren werden offiziell für den Einsatz einer Greenbone Enterprise ONE unterstützt:

- Oracle VirtualBox, Version 6.1 oder höher
- VMware Workstation Player, Version 16.0 oder höher
- VMware Workstation Pro, Version 16.0 oder höher

Der erforderliche Bootmodus ist der EFI/UEFI-Boot-Modus.

5.2 Eine Hardware-Appliance einrichten

Bemerkung: Die Voraussetzungen für die Installation der Appliance finden sich in Kapitel *5.1* (Seite 28).

5.2.1 Den seriellen Port nutzen

Das beigelegte Konsolenkabel wird für die Nutzung des seriellen Ports verwendet. Alternativ kann ein blaues Cisco-Konsolenkabel (Rollover-Kabel) genutzt werden.

Für den Zugriff auf den seriellen Port ist eine Terminalanwendung erforderlich. Die Anwendung muss auf eine Geschwindigkeit von 9600 Bits/s (Baud) konfiguriert sein.

Unter Linux kann der Befehl `screen` in der Kommandozeile verwendet werden, um auf die serielle Schnittstelle zuzugreifen. Das Gerät, das die serielle Schnittstelle bereitstellt, muss als Parameter übergeben werden:

```
screen /dev/ttyS0  #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Tipp: Nach dem Starten von screen kann es nötig sein, mehrmals `Enter` zu drücken, um eine Eingabeaufforderung zu sehen.

Um die serielle Verbindung zu trennen, kann `Strg` + `a` und sofort danach `\` gedrückt werden.

Unter Microsoft Windows kann die Anwendung PuTTY[3] verwendet werden. Nach dem Start müssen die Optionen wie in Abb. 5.1 und der entsprechende serielle Port ausgewählt werden.

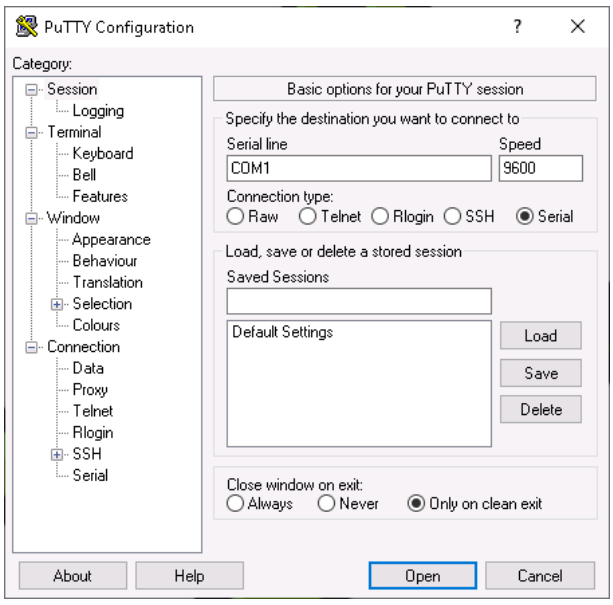


Abb. 5.1: Den seriellen Port in PuTTY einrichten

[3] https://www.chiark.greenend.org.uk/~sgtatham/putty/

5.2.2 Die Appliance starten

Wenn die Appliance vollständig verkabelt, eine Verbindung zur Appliance über das Konsolenkabel hergestellt und die Terminalanwendung (PuTTY, screen oder ähnliche) eingerichtet wurde, kann die Appliance gestartet werden.

Die Appliance fährt hoch und nach kurzer Zeit – abhängig vom Modell – wird die Eingabeaufforderung angezeigt. Die Standarddaten für den Login sind:

- Benutzer: `admin`
- Passwort: `admin`

Bemerkung: Während des ersten Setups sollte dieses Passwort geändert werden (siehe Kapitel *7.2.1.1* (Seite 70)).

5.2.3 Ein grundlegendes System-Setup durchführen

Alle Appliances haben die gleiche Art der Grundkonfiguration und Bereitschaftsprüfung.

Nach dem Ausliefern der Appliance durch Greenbone oder nach einem Factory-Reset zeigt das GOS-Administrationsmenü nach dem Einloggen den First Setup Wizard, um bei der Basis-Konfiguration von GOS behilflich zu sein (siehe Abb. 5.2).

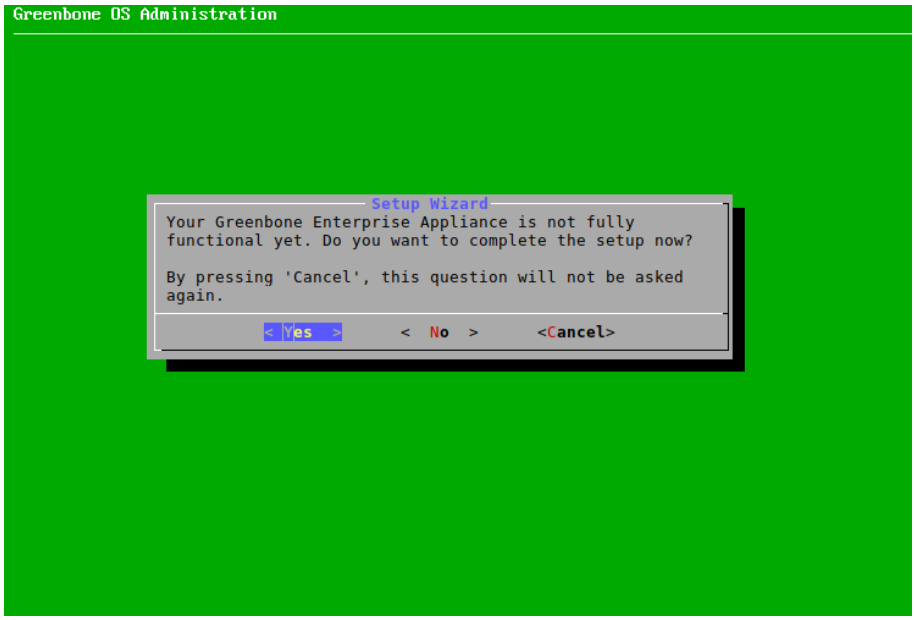


Abb. 5.2: Benutzen des First Setup Wizards

Durch Wählen von *Yes* und Drücken von `Enter` wird der Wizard geöffnet.

Bemerkung: Durch Wählen von *No* und Drücken von `Enter` kann der Wizard geschlossen werden. Unvollständige Schritte werden beim erneuten Einloggen angezeigt.

Durch Wählen von *Cancel* und Drücken von `Enter` kann der Wizard ebenfalls geschlossen werden. In diesem Fall werden unvollständige Schritte allerdings nicht erneut angezeigt.

Der First Setup Wizard ist dynamisch und zeigt nur die für das genutzte Appliance-Modell nötigen Schritte. Im Folgenden werden alle möglichen Schritte aufgeführt, auch wenn sie nicht in jedem Fall erscheinen.

Im Falle eines Factory-Resets müssen alle Schritte durchgeführt werden (siehe *20.9* (Seite 431)).

Jeder Schritt kann durch Wählen von *Skip* oder *No* und Drücken von `Enter` übersprungen werden. Übersprungene Schritte werden beim nächsten Einloggen erneut angezeigt.

5.2.3.1 Das Netzwerk konfigurieren

Das Netzwerk muss eingerichtet sein, damit die Appliance vollständig funktionsfähig ist. Falls keine IP-Adresse konfiguriert ist, wird gefragt, ob die Netzwerkeinstellungen angepasst werden sollen (siehe Abb. 5.3).

Bemerkung: Bei der Verwendung von DHCP überträgt die Appliance nicht die MAC-Adresse, sondern eine DHCP Unique ID (DUID). Während dies bei modernen DHCP-Servern nicht zu Schwierigkeiten führen sollte, sind einige ältere DHCP-Server (z. B. Windows Server 2012) möglicherweise nicht in der Lage, diese zu verarbeiten.

Eine mögliche Lösung ist die Angabe der DUID anstelle der MAC-Adresse auf dem DHCP-Server. Alternativ kann auch eine statische IP-Adresse auf der Appliance verwendet werden.

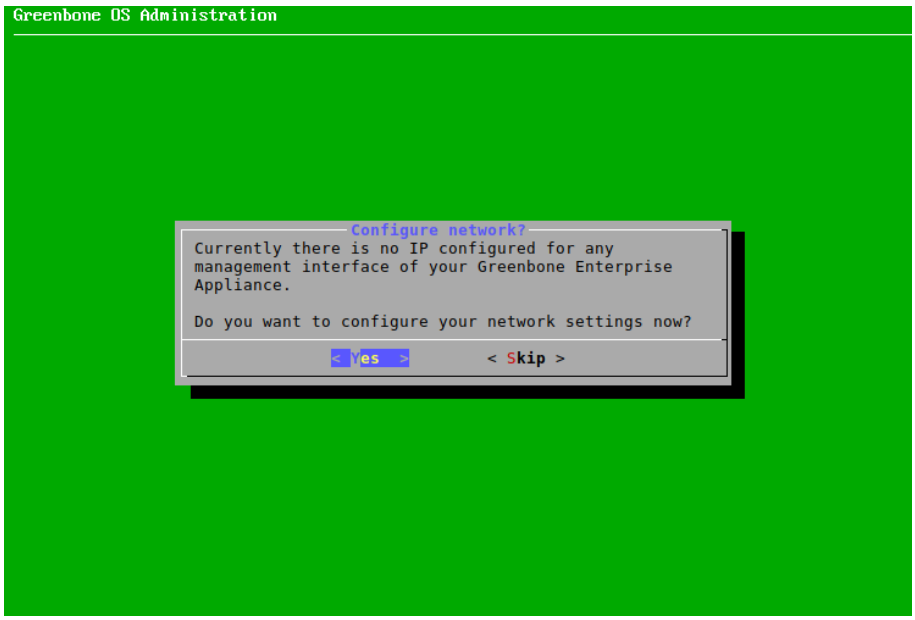


Abb. 5.3: Konfigurieren der Netzwerkeinstellungen

1. *Yes* wählen und `Enter` drücken.
2. *Interfaces* wählen und `Enter` drücken.

3. Gewünschte Schnittstelle wählen und `Enter` drücken.

   → Die Schnittstelle kann konfiguriert werden.

4. Falls DHCP genutzt werden soll, *DHCP* (für IPV4 oder IPv6) wählen und `Enter` drücken (siehe Abb. 5.4).

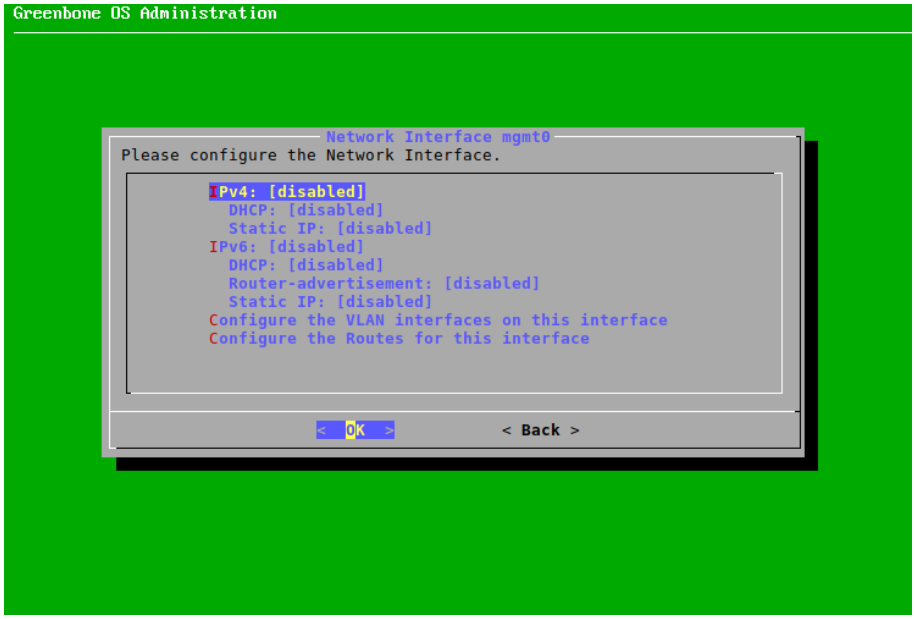


Abb. 5.4: Konfigurieren der Netzwerkschnittstelle

5. *Save* wählen und `Enter` drücken.
6. *Back* wählen und `Enter` drücken.
7. *Back* wählen und `Enter` drücken.
8. *Ready* wählen und `Enter` drücken.

   oder

4. Falls eine statische IP-Adresse genutzt werden soll, *Static IP* (für IPv4 oder IPv6) wählen und `Enter` drücken.
5. IP-Adresse, einschließlich Präfixlänge, in das Eingabefeld eingeben (siehe Abb. 5.5).
6. `Enter` drücken.

   → Eine Nachricht informiert den Benutzer darüber, dass die Änderungen gespeichert werden müssen.

7. `Enter` drücken, um die Nachricht zu schließen.
8. *Save* wählen und `Enter` drücken.
9. *Back* wählen und `Enter` drücken.
10. *Back* wählen und `Enter` drücken.
11. *Ready* wählen und `Enter` drücken.

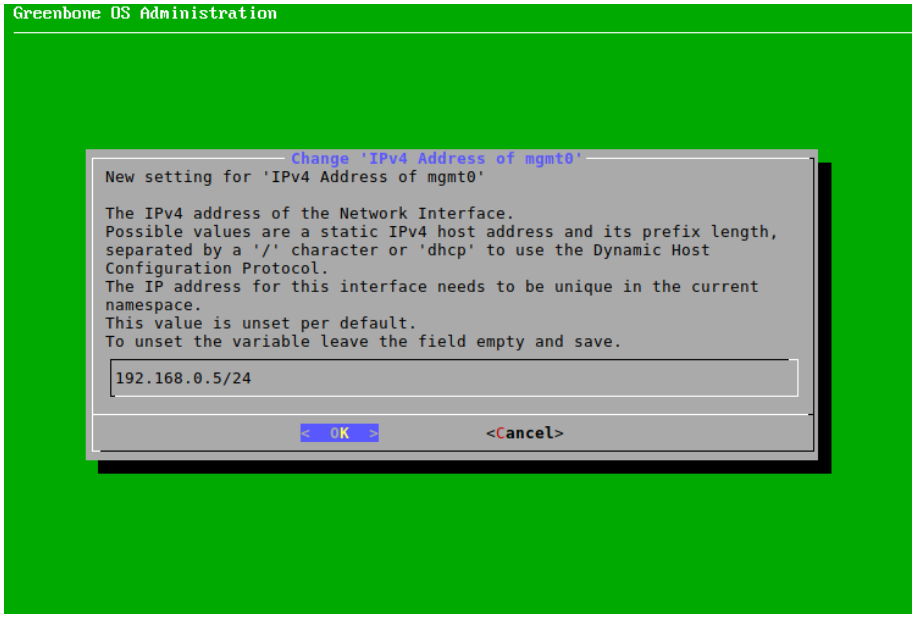


Abb. 5.5: Eingeben einer statischen IP-Adresse

5.2.3.2 Ein HTTPS-Zertifikat importieren oder generieren

Um die Web-Oberfläche sicher nutzen zu können, muss ein HTTPS-Zertifikat auf der Appliance vorhanden sein. Das Zertifikat kann wie folgt importiert oder generiert werden:

1. *Import* wählen und `Enter` drücken (siehe Abb. 5.6).

   → Eine Nachricht informiert den Benutzer darüber, dass eine PKCS#12-Datei importiert werden kann.

2. *Continue* wählen und `Enter` drücken.
3. Webbrowser öffnen und angezeigte URL eingeben.
4. Auf *Browse...* klicken, die PKCS#12-Datei wählen und auf *Upload* klicken.

   → Wenn das Zertifikat von der Appliance erhalten wurde, zeigt das GOS-Administrationsmenü den Fingerprint des Zertifikats zur Verifizierung an.

5. Fingerprint prüfen und `Enter` drücken, um das Zertifikat zu bestätigen.

   oder

1. *Generate* wählen und `Enter` drücken.

   → Eine Nachricht informiert den Benutzer darüber, dass für die Erstellung des Zertifikats Parameter eingegeben werden müssen.

2. *Continue* wählen und `Enter` drücken.

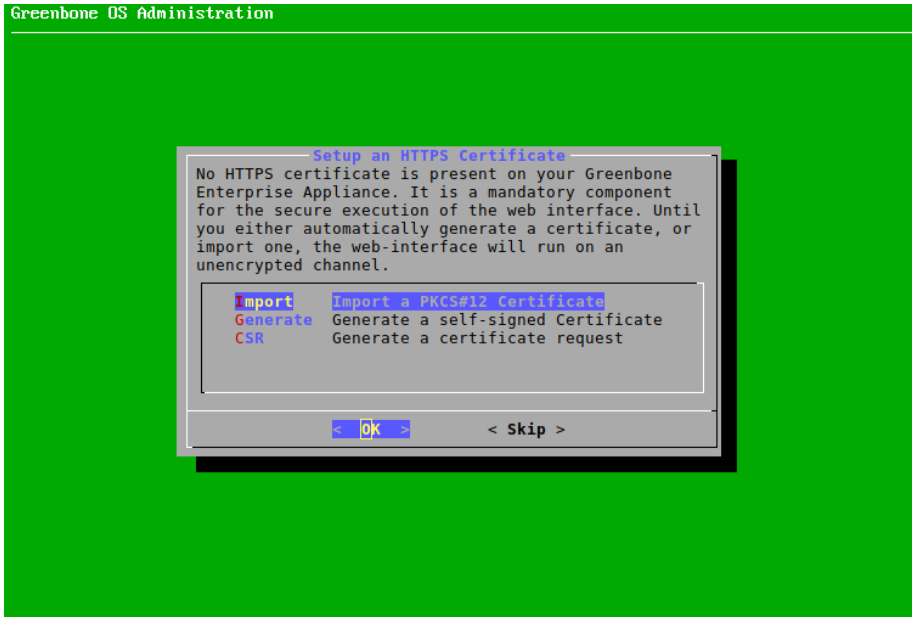


Abb. 5.6: Importieren oder Generieren eines HTTPS-Zertifikats

3. Einstellungen für das Zertifikat eingeben (siehe Abb. 5.7).

Bemerkung: Es ist zulässig, ein Zertifikat ohne einen Common Name zu erstellen. Allerdings sollte ein Zertifikat nicht ohne (einen) Subject Alternative Name(s) erstellt werden.

Falls ein Common Name verwendet wird, sollte dieser mit einem der SANs identisch sein.

---

4. *OK* wählen und `Enter` drücken.

   → Eine Nachricht informiert darüber, dass das Zertifikat erstellt wurde und heruntergeladen werden kann (siehe Abb. 5.8).

Bemerkung: Das Herunterladen wird nicht im First Setup Wizard, sondern im späteren GOS-Administrationsmenü durchgeführt, siehe Kapitel *7.2.4.1.7.1* (Seite 101), Schritte 1–4 und 9–13.

---

oder

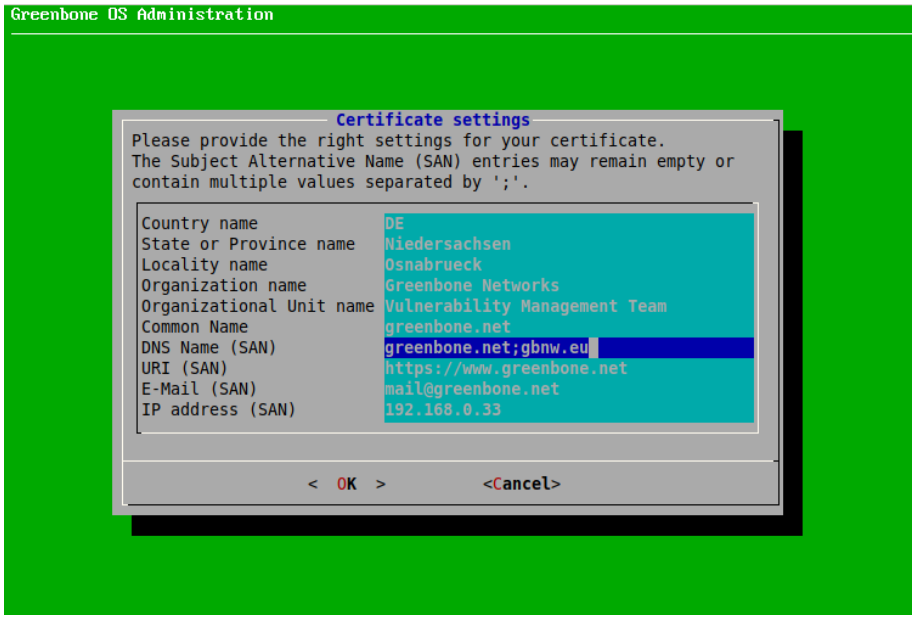


Abb. 5.7: Eingabe der Informationen für das Zertifikat

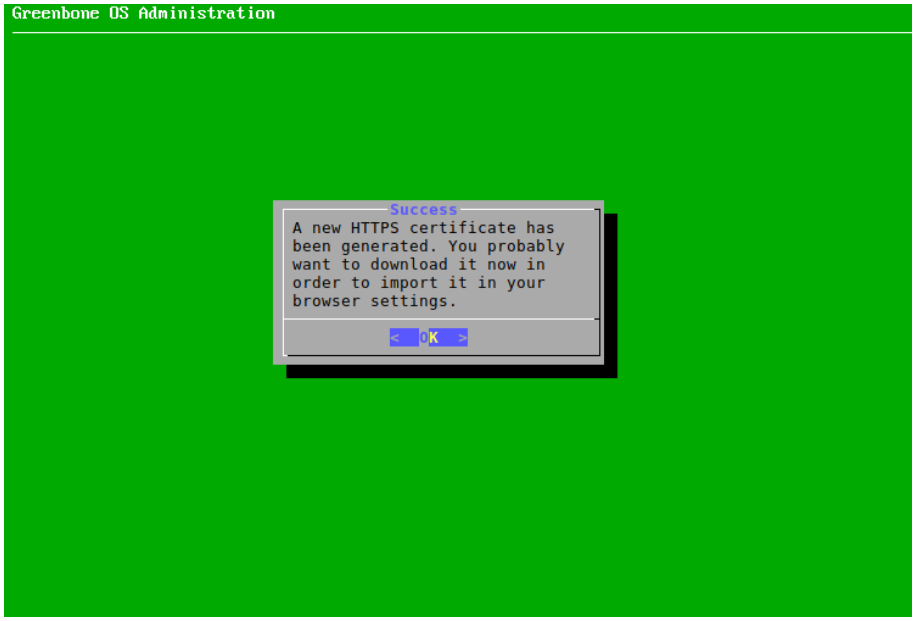


Abb. 5.8: Fertigstellen des HTTPS-Zertifikats

1. *CSR* wählen und `Enter` drücken.

   → Eine Nachricht informiert den Benutzer darüber, dass ein Schlüsselpaar und eine Zertifikatsanforderung erstellt wurden.

2. *Continue* wählen und `Enter` drücken.
3. Einstellungen für das Zertifikat eingeben.

   Bemerkung: Es ist zulässig, ein Zertifikat ohne einen Common Name zu erstellen. Allerdings sollte ein Zertifikat nicht ohne (einen) Subject Alternative Name(s) erstellt werden.

   Falls ein Common Name verwendet wird, sollte dieser mit einem der SANs identisch sein.

4. *OK* wählen und `Enter` drücken.
5. Webbrowser öffnen und angezeigte URL eingeben.
6. PEM-Datei herunterladen.

   → Das GOS-Administrationsmenü zeigt eine Nachricht, um zu verifizieren, dass die Zertifikatsanforderung nicht gefälscht wurde.

7. `Enter` drücken, um die Information zu verifizieren.

   Bemerkung: Wenn das Zertifikat signiert wurde, muss es auf die Appliance hochgeladen werden. Das Hochladen wird nicht im First Setup Wizard, sondern im späteren GOS-Administrationsmenü durchgeführt, siehe Kapitel *7.2.4.1.7.2* (Seite 103), Schritte 1–4 und 11–14.

5.2.3.3 Einen Web-Administrator erstellen

Falls kein Web-Administrator vorhanden ist, wird gefragt, ob ein solcher Account erstellt werden soll (siehe Abb. 5.9).

Bemerkung: Um die Web-Oberfläche der Appliance nutzen zu können, wird ein Web-Administrator benötigt.

Der erste erstellte Web-Administrator (Web-Benutzer) ist automatisch der Feed Import Owner (siehe Kapitel *7.2.1.10* (Seite 78)).

1. *Yes* wählen und `Enter` drücken.
2. Benutzernamen des Web-Administrators eingeben.

   Bemerkung: Für den Benutzernamen sind nur die folgenden Zeichen zulässig:

   - Alle alphanumerischen Zeichen
   - - (Bindestrich)
   - _ (Unterstrich)
   - . (Punkt)

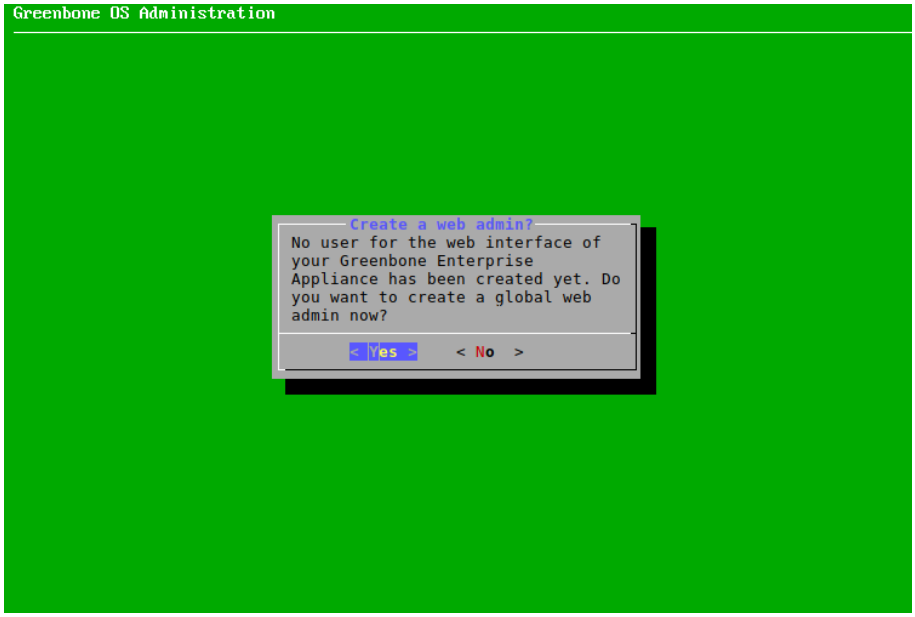


Abb. 5.9: Erstellen eines Web-Administrators

3. Passwort für den Web-Administrator zweimal eingeben.

Bemerkung: Das Passwort kann jede Art von Zeichen enthalten und darf maximal 30 Zeichen lang sein.

Bei der Verwendung von Sonderzeichen ist zu beachten, dass diese auf allen verwendeten Tastaturen vorhanden sein müssen und von jeder Client-Software und allen Betriebssystemen korrekt unterstützt werden. Das Kopieren und Einfügen von Sonderzeichen für Passwörter kann je nach diesen externen Faktoren zu ungültigen Passwörtern führen.

---

4. *OK* wählen und `Enter` drücken.

   → Eine Nachricht informiert den Benutzer darüber, das der Web-Administrator erstellt wurde.

5. `Enter` drücken, um die Nachricht zu schließen.

5.2.3.4 Einen Greenbone-Enterprise-Feed-Subskription-Schlüssel eingeben oder hochladen

Falls kein gültiger Subskription-Schlüssel auf der Appliance gespeichert ist, nutzt die Appliance nur den öffentlichen Greenbone Community Feed und nicht den Greenbone Enterprise Feed.

Bemerkung: Es ist nicht notwendig, einen Greenbone-Enterprise-Feed-Subskription-Schlüssel auf einer neu gelieferten Appliance hinzuzufügen, da bereits ein Schlüssel vorinstalliert ist.

Ein Subskription-Schlüssel kann wie folgt eingegeben oder hochgeladen werden:

1. *Editor* wählen und `Enter` drücken (siehe Abb. 5.10).

   → Der Editor wird geöffnet.

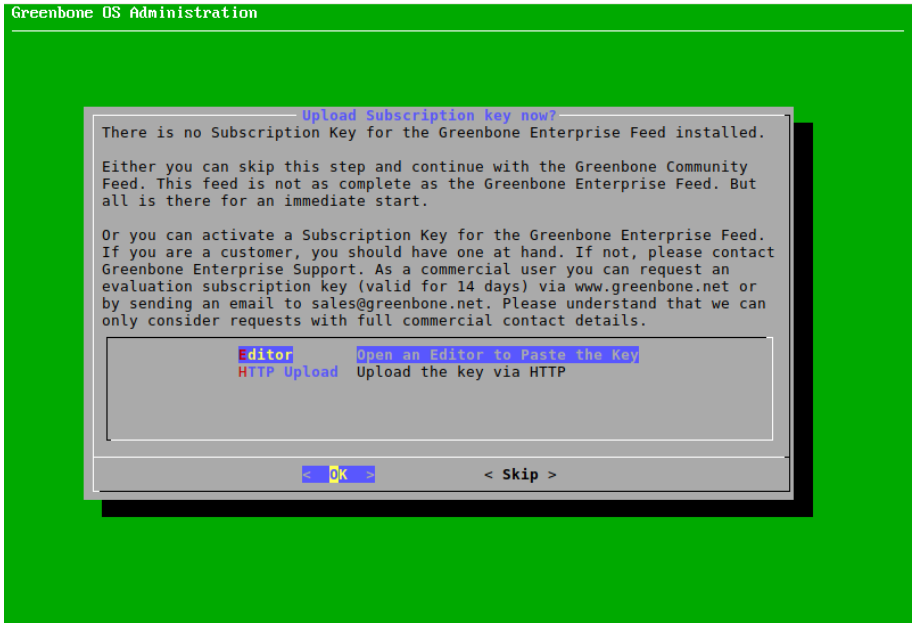


Abb. 5.10: Eingabe oder Hochladen eines Subskription-Schlüssels

2. Den GSF-Subscription-Schlüssel eingeben.
3. `Strg` + `S` drücken, um die Änderungen zu speichern.
4. `Strg` + `X` drücken, um den Editor zu schließen.

   oder

1. *HTTP Upload* wählen und `Enter` drücken.
2. Webbrowser öffnen und angezeigte URL eingeben.
3. Auf *Browse...* klicken, den Subscription-Schlüssel wählen und auf *Upload* klicken.

5.2.3.5 Den Feed herunterladen

Falls kein Feed auf der Appliance vorhanden ist, kann der Feed wie folgt heruntergeladen werden:

1. *Yes* wählen und `Enter` drücken (siehe Abb. 5.11).

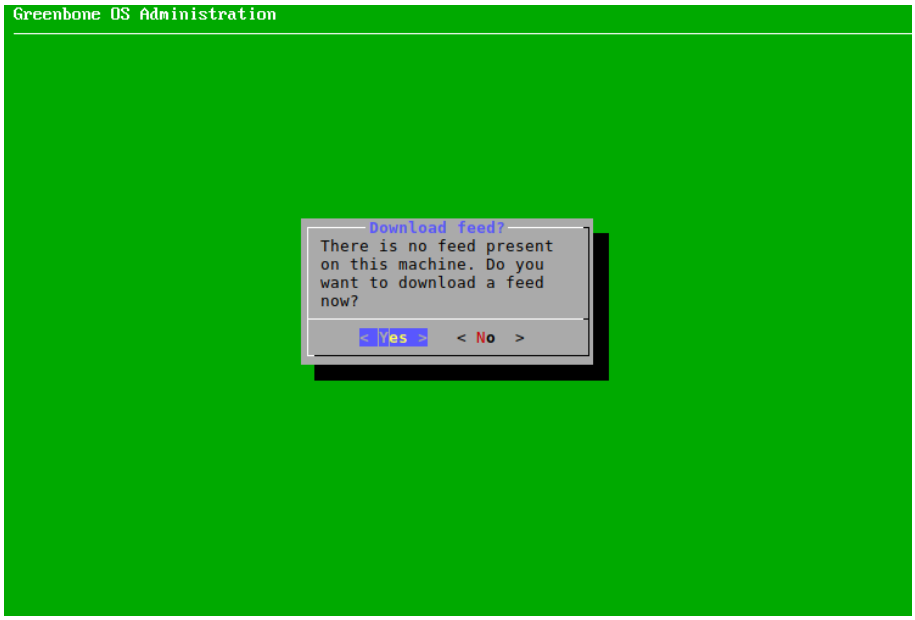


Abb. 5.11: Herunterladen des Feeds

→ Eine Meldung informiert darüber, dass das Feed-Update im Hintergrund gestartet wurde (siehe Abb. 5.12).

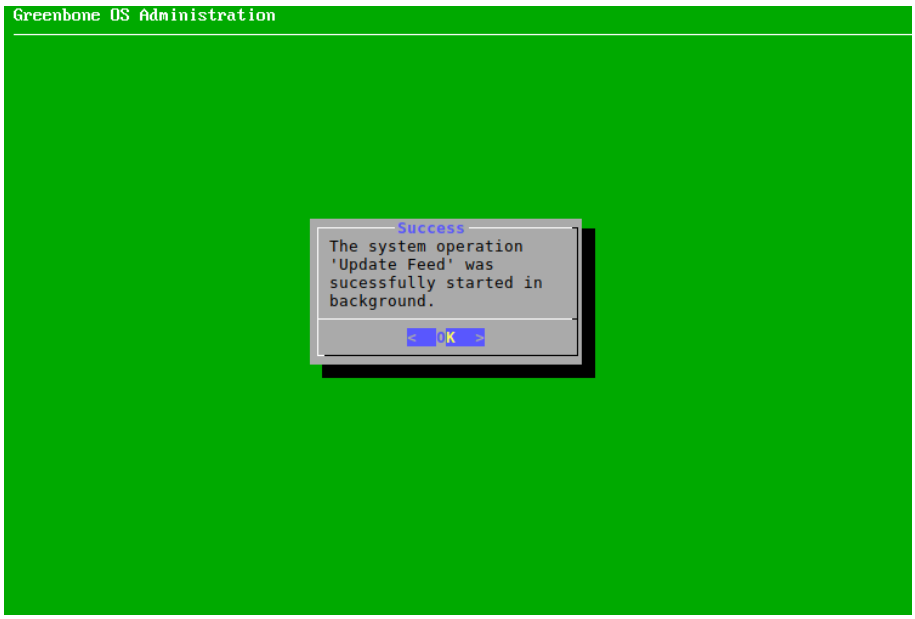


Abb. 5.12: Herunterladen des Feeds

2. `Enter` drücken, um die Nachricht zu schließen.

5.2.3.6 Den First Setup Wizard abschließen

Bemerkung: Nach dem letzten Schritt wird ein Statuscheck durchgeführt.

1. `Enter` drücken, wenn der Check beendet ist.

   → Die Ergebnisse des Checks werden angezeigt (siehe Abb. 5.13).

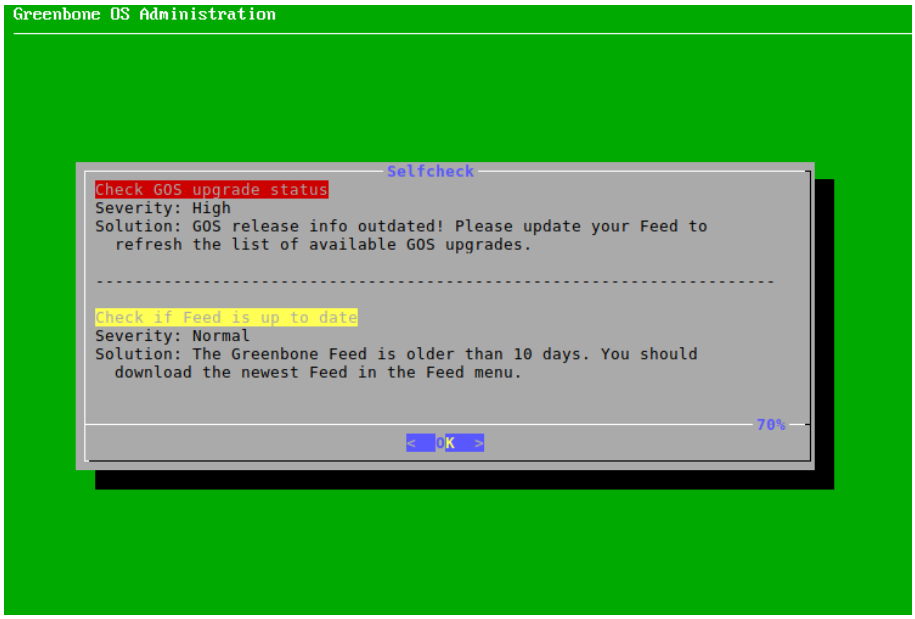


Abb. 5.13: Ergebnis der Statusprüfung

2. `Enter` drücken.

   → Das GOS-Administrationsmenü kann wie in Kapitel *7* (Seite 65) beschrieben genutzt werden.

   Falls es unvollständige oder übersprungene Schritte gibt, wird der First Setup Wizard beim nächsten Einloggen erneut angezeigt.

5.2.4 In die Web-Oberfläche einloggen

Bemerkung: Dieser Schritt entfällt für die Greenbone Enterprise 35.

Die wichtigste Schnittstelle der Appliance ist die Web-Oberfläche, auch Greenbone Security Assistant (GSA) genannt. Auf die Web-Oberfläche kann wie in Kapitel *8.1* (Seite 164) beschrieben zugegriffen werden.

5.3 Eine virtuelle Appliance einrichten

Bemerkung: Die Voraussetzungen für die Installation der Appliance finden sich in Kapitel *5.1* (Seite 28).

5.3.1 Verifikation der Integrität

Bemerkung: Die Integrität der virtuelle Appliance kann verifiziert werden. Auf Anfrage stellt der Greenbone Enterprise Support dafür eine Prüfsumme zur Verfügung.

Um eine Prüfsumme anzufordern, kann der Greenbone Enterprise Support[4] unter Angabe der Subskription-Nummer kontaktiert werden.

Die Prüfsumme kann entweder per Telefon oder über das Support-Portal[5] bereitgestellt werden.

Die lokale Verifikation der Prüfsumme ist abhängig vom genutzten Betriebssystem.

Unter Linux kann der folgende Befehl zum Berechnen der Prüfsumme genutzt werden:

```
sha256sum <file>
```

Bemerkung: `<file>` durch den Namen der OVA-Datei der Appliance ersetzen.

Unter Microsoft Windows kann der folgende Befehl zum Berechnen der Prüfsumme in der Windows PowerShell genutzt werden:

```
Get-Filehash 'C:\<path>\<file>' -Algorithm SHA256
```

Bemerkung: `<path>` und `<file>` durch den Pfad und den Namen der OVA-Datei der Appliance ersetzen.

Falls die Prüfsumme nicht mit der vom Greenbone Enterprise Support bereitgestellten Prüfsumme übereinstimmt, wurde die virtuelle Appliance verändert und sollte nicht verwendet werden.

5.3.2 Die Appliance bereitstellen

5.3.2.1 VMware vSphere/ESXi

Die virtuelle Appliance wird von Greenbone im Format Open Virtualization Appliance (OVA) bereitgestellt.

Jede Appliance wird durch die Nutzung eines eindeutigen Subskription-Schlüssels aktiviert.

Bemerkung: Das Klonen der Appliance und parallele Nutzen mehrerer Instanzen ist nicht erlaubt und kann zu Inkonsistenzen und unerwünschten Nebeneffekten führen.

[4] https://www.greenbone.net/technischer-support/
[5] https://jira.greenbone.net/servicedesk/customer/user/login?destination=portals

Um eine Appliance bereitzustellen, muss sie wie folgt in den Hypervisor importiert werden:

Bemerkung: Dieses Beispiel nutzt VMware ESXi, kann aber auch auf VMware vCenter angewendet werden.

Die Abbildungen zeigen die Installation einer Greenbone Enterprise TERA. Die Installation eines anderen Appliance-Modells wird äquivalent durchgeführt. Dateinamen, die in diesem Beispiel genutzt werden, unterscheiden sich basierend auf dem Appliance-Modell und dem Subskription-Schlüssel.

1. Web-Oberfläche der VMware-ESXi-Instanz öffnen und einloggen.
2. In der Spalte *Navigator* links auf *Virtuelle Maschinen* klicken.
3. Auf *VM erstellen/registrieren* klicken.
4. *Eine virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen* wählen und auf *Weiter* klicken (siehe Abb. 5.14).

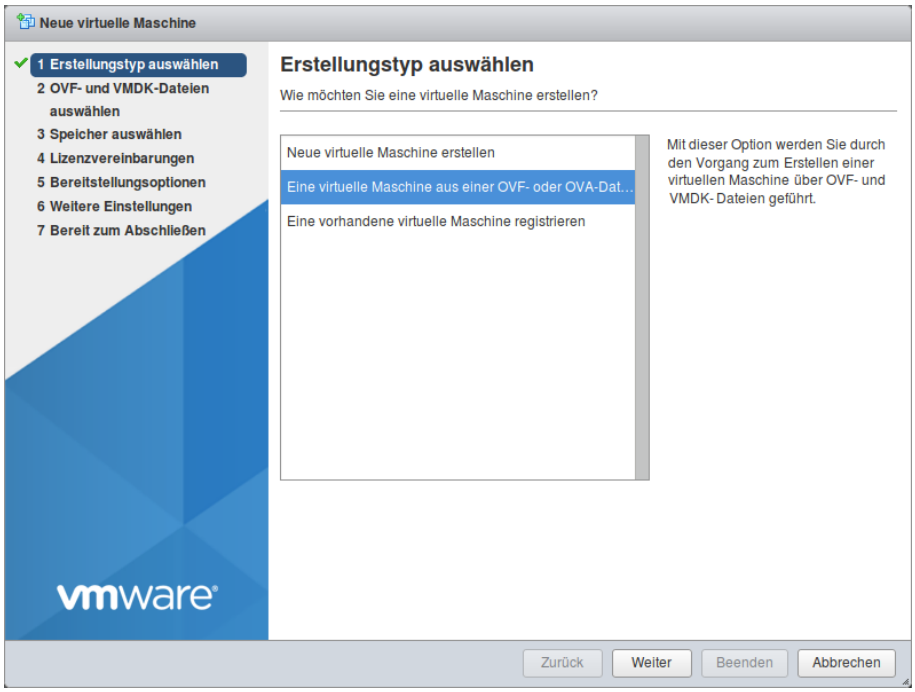


Abb. 5.14: Auswählen des Erstellungstypen

5. Namen für die virtuelle Maschine in das Eingabefeld eingeben.
6. Auf *Zum Auswählen der Dateien klicken oder ziehen/ablegen* klicken, OVA-Datei der Appliance wählen und auf *Weiter* klicken.
7. Speicherort, in dem die Dateien der virtuellen Maschine gespeichert werden soll, wählen und auf *Weiter* klicken.
8. Bereitsstellungsoptionen wie benötigt anpassen und auf *Weiter* klicken.

Bemerkung: Die Standardeinstellungen können verwendet werden.

9. Konfiguration der virtuellen Maschine kontrollieren (siehe Abb. 5.15).

Tipp: Einstellungen können geändert werden, indem auf *Zurück* geklickt wird und die Einstellungen im entsprechenden Fenster angepasst werden.

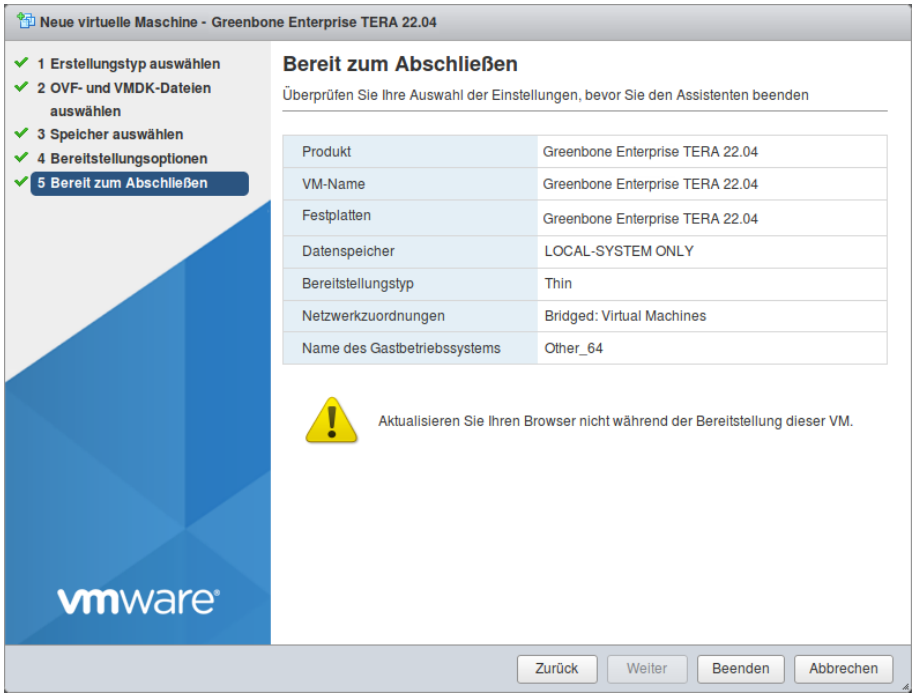


Abb. 5.15: Kontrollieren der Konfiguration der virtuellen Maschine

10. Auf *Beenden* klicken.

    → Die Appliance wird importiert. Dieser Vorgang kann bis zu 10 Minuten dauern.

Wichtig: Der Webbrowser darf nicht aktualisiert werden, während die virtuelle Maschine bereitgestellt wird.

11. Wenn die Appliance importiert wurde, in der Spalte *Navigator* links auf *Virtuelle Maschinen* klicken.
12. Appliance in der Liste wählen und auf *Einschalten* klicken (siehe Abb. 5.16).

    → Die Appliance fährt hoch und nach kurzer Zeit – abhängig vom Modell – wird die Eingabeaufforderung angezeigt.
13. Mit den Standarddaten für den Login einloggen:
    - Benutzer: `admin`
    - Passwort: `admin`

Bemerkung: Während des ersten Setups sollte dieses Passwort geändert werden (siehe Kapitel *7.2.1.1* (Seite 70)).

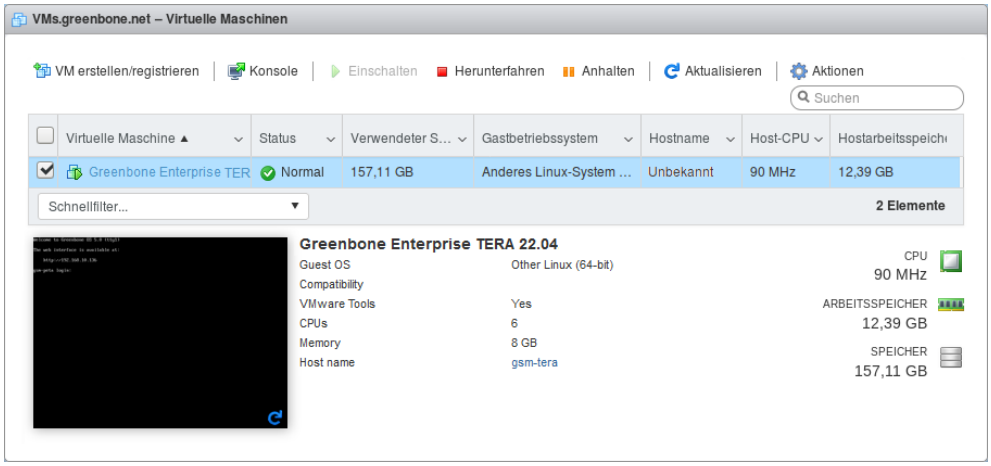


Abb. 5.16: Importierte virtuelle Maschine

5.3.2.2 Oracle VirtualBox

Die virtuelle Appliance wird von Greenbone im Format Open Virtualization Appliance (OVA) bereitgestellt.

Jede Appliance wird durch die Nutzung eines eindeutigen Subskription-Schlüssels aktiviert.

Bemerkung: Das Klonen der Appliance und parallele Nutzen mehrerer Instanzen ist nicht erlaubt und kann zu Inkonsistenzen und unerwünschten Nebeneffekten führen.

Um eine Appliance bereitzustellen, muss sie wie folgt in den Hypervisor importiert werden:

Bemerkung: Dateinamen, die in diesem Beispiel genutzt werden, unterscheiden sich basierend auf dem Subskription-Schlüssel.

---

1. Oracle VirtualBox für das aktuelle Betriebssystem installieren.

   Bemerkung: VirtualBox ist oft in Linux-Distributionen enthalten.

   Sollte dies nicht der Fall sein oder Microsoft Windows genutzt werden, ist VirtualBox unter https://www.virtualbox.org/wiki/Downloads verfügbar.

   ---

2. VirtualBox starten.
3. *Datei > Appliance importieren . . .* in der Menüleiste wählen.
4. Auf klicken und OVA-Datei der Appliance wählen (siehe Abb. 5.17).
5. Konfiguration der virtuellen Maschine im Fenster *Appliance-Einstellungen* kontrollieren (siehe Abb. 5.17).

   Werte können durch Doppelklicken in das Eingabefeld des entsprechenden Werts geändert werden.
6. *Importieren* klicken.

   → Die Appliance wird importiert. Dieser Vorgang kann bis zu 10 Minuten dauern.

   Wenn die Appliance importiert wurde, wird sie in der linken Spalte in VirtualBox angezeigt.

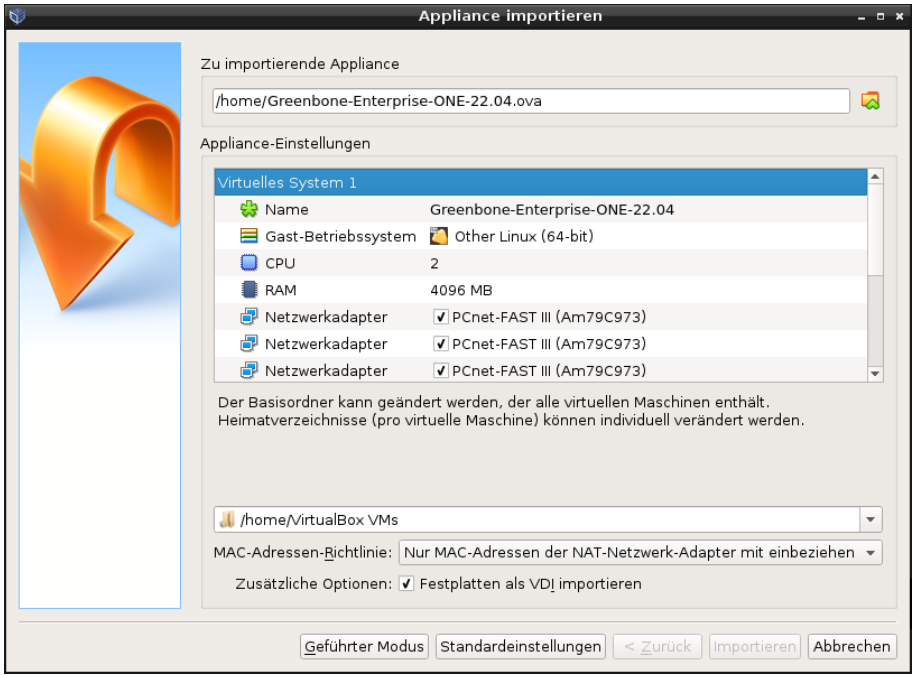


Abb. 5.17: Importieren der OVA-Datei der Appliance

7. Appliance in der Liste auswählen und auf *Start* klicken.

   → Die Appliance fährt hoch und nach kurzer Zeit – abhängig vom Modell – wird die Eingabeaufforderung angezeigt.

8. Mit den Standarddaten für den Login einloggen:

   - Benutzer: `admin`
   - Passwort: `admin`

Bemerkung: Während des ersten Setups sollte dieses Passwort geändert werden (siehe Kapitel *7.2.1.1* (Seite 70)).

5.3.3 Ein grundlegendes System-Setup durchführen

Alle Appliances haben die gleiche Art der Grundkonfiguration und Bereitschaftsprüfung.

Nach dem Ausliefern der Appliance durch Greenbone oder nach einem Factory-Reset zeigt das GOS-Administrationsmenü nach dem Einloggen den First Setup Wizard, um bei der Basis-Konfiguration von GOS behilflich zu sein (siehe Abb. 5.18).

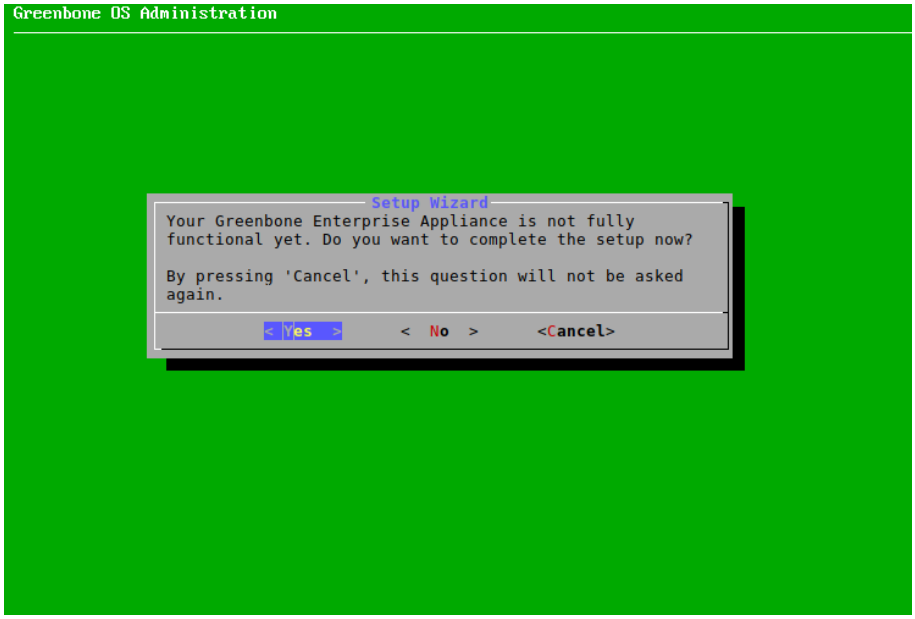


Abb. 5.18: Benutzen des First Setup Wizards

Durch Wählen von *Yes* und Drücken von `Enter` wird der Wizard geöffnet.

Bemerkung: Durch Wählen von *No* und Drücken von `Enter` kann der Wizard geschlossen werden. Unvollständige Schritte werden beim erneuten Einloggen angezeigt.

Durch Wählen von *Cancel* und Drücken von `Enter` kann der Wizard ebenfalls geschlossen werden. In diesem Fall werden unvollständige Schritte allerdings nicht erneut angezeigt.

Der First Setup Wizard ist dynamisch und zeigt nur die für das genutzte Appliance-Modell nötigen Schritte. Im Folgenden werden alle möglichen Schritte aufgeführt, auch wenn sie nicht in jedem Fall erscheinen.

Im Falle eines Factory-Resets müssen alle Schritte durchgeführt werden (siehe *20.9* (Seite 431)).

Jeder Schritt kann durch Wählen von *Skip* oder *No* und Drücken von `Enter` übersprungen werden. Übersprungene Schritte werden beim nächsten Einloggen erneut angezeigt.

5.3.3.1 Das Netzwerk konfigurieren

Bemerkung: Anders als bei Hardware-Appliances ist bei virtuellen Appliances in den Werkseinstellungen DHCP für die eth0-Schnittstelle aktiviert. Daher entfällt hier der Schritt zur Konfiguration des Netzwerks.

5.3.3.2 Ein HTTPS-Zertifikat importieren oder generieren

Um die Web-Oberfläche sicher nutzen zu können, muss ein HTTPS-Zertifikat auf der Appliance vorhanden sein. Das Zertifikat kann wie folgt importiert oder generiert werden:

1. *Import* wählen und `Enter` drücken (siehe Abb. 5.19).

   → Eine Nachricht informiert den Benutzer darüber, dass eine PKCS#12-Datei importiert werden kann.

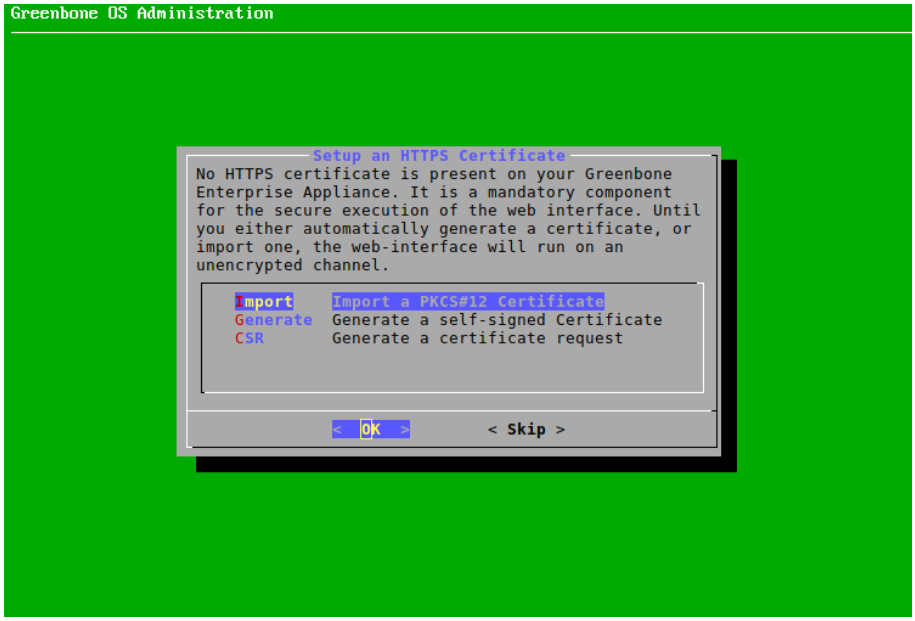


Abb. 5.19: Importieren oder Generieren eines HTTPS-Zertifikats

2. *Continue* wählen und `Enter` drücken.
3. Webbrowser öffnen und angezeigte URL eingeben.
4. Auf *Browse...* klicken, die PKCS#12-Datei wählen und auf *Upload* klicken.

   → Wenn das Zertifikat von der Appliance erhalten wurde, zeigt das GOS-Administrationsmenü den Fingerprint des Zertifikats zur Verifizierung an.
5. Fingerprint prüfen und `Enter` drücken, um das Zertifikat zu bestätigen.

   oder

1. *Generate* wählen und `Enter` drücken.

   → Eine Nachricht informiert den Benutzer darüber, dass für die Erstellung des Zertifikats Parameter eingegeben werden müssen.
2. *Continue* wählen und `Enter` drücken.
3. Einstellungen für das Zertifikat eingeben (siehe Abb. 5.20).

Bemerkung: Es ist zulässig, ein Zertifikat ohne einen Common Name zu erstellen. Allerdings sollte ein Zertifikat nicht ohne (einen) Subject Alternative Name(s) erstellt werden.

Falls ein Common Name verwendet wird, sollte dieser mit einem der SANs identisch sein.

---

4. *OK* wählen und `Enter` drücken.

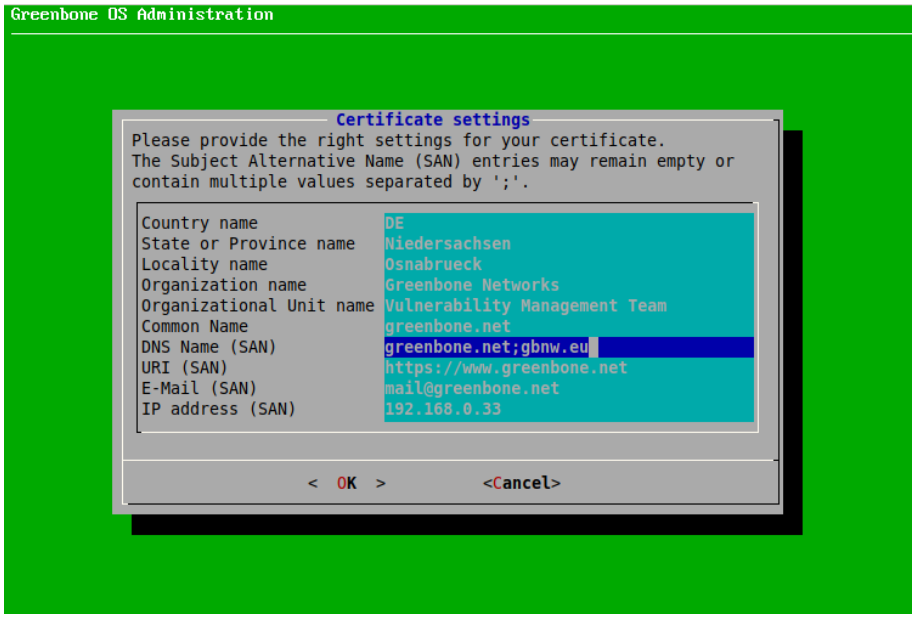


Abb. 5.20: Eingabe der Informationen für das Zertifikat

→ Eine Nachricht informiert den Benutzer darüber, dass das Zertifikat erstellt wurde und heruntergeladen werden kann (siehe Abb. 5.21).

Bemerkung: Das Herunterladen wird nicht im First Setup Wizard, sondern im späteren GOS-Administrationsmenü durchgeführt, siehe Kapitel *7.2.4.1.7.1* (Seite 101), Schritte 1–4 und 9–13.

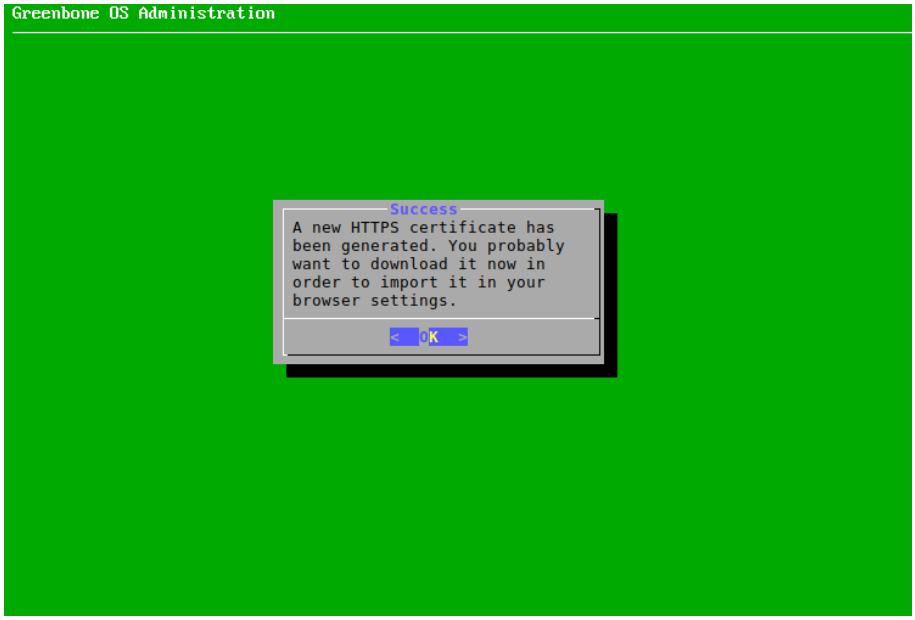


Abb. 5.21: Fertigstellen des HTTPS-Zertifikats

oder

1. *CSR* wählen und `Enter` drücken.

   → Eine Nachricht informiert den Benutzer darüber, dass ein Schlüsselpaar und eine Zertifikatsanforderung erstellt wurden.

2. *Continue* wählen und `Enter` drücken.
3. Einstellungen für das Zertifikat eingeben.

   Bemerkung: Es ist zulässig, ein Zertifikat ohne einen Common Name zu erstellen. Allerdings sollte ein Zertifikat nicht ohne (einen) Subject Alternative Name(s) erstellt werden.

   Falls ein Common Name verwendet wird, sollte dieser mit einem der SANs identisch sein.

   ---

4. *OK* wählen und `Enter` drücken.
5. Webbrowser öffnen und angezeigte URL eingeben.
6. PEM-Datei herunterladen.

   → Das GOS-Administrationsmenü zeigt eine Nachricht, um zu verifizieren, dass die Zertifikatsanforderung nicht gefälscht wurde.

7. `Enter` drücken, um die Information zu verifizieren.

   Bemerkung: Wenn das Zertifikat signiert wurde, muss es auf die Appliance hochgeladen werden. Das Hochladen wird nicht im First Setup Wizard, sondern im späteren GOS-Administrationsmenü durchgeführt, siehe Kapitel *7.2.4.1.7.2* (Seite 103), Schritte 1–4 und 11–14.

5.3.3.3 Einen Web-Administrator erstellen

Falls kein Web-Administrator vorhanden ist, wird gefragt, ob ein solcher Account erstellt werden soll (siehe Abb. 5.22).

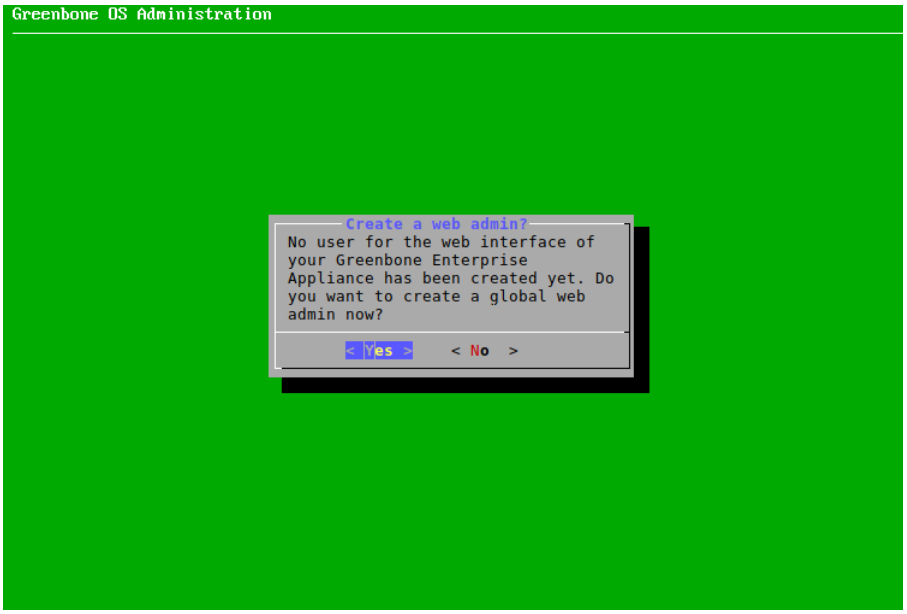


Abb. 5.22: Erstellen eines Web-Administrators

Bemerkung: Um die Web-Oberfläche der Appliance nutzen zu können, wird ein Web-Administrator benötigt.

Der erste erstellte Web-Administrator (Web-Benutzer) ist automatisch der Feed Import Owner (siehe Kapitel *7.2.1.10* (Seite 78)).

---

1. *Yes* wählen und `Enter` drücken.
2. Benutzernamen des Web-Administrators eingeben.

   Bemerkung: Für den Benutzernamen sind nur die folgenden Zeichen zulässig:

   - Alle alphanumerischen Zeichen
   - - (Bindestrich)
   - _ (Unterstrich)
   - . (Punkt)

   ---

3. Passwort für den Web-Administrator zweimal eingeben.

   Bemerkung: Das Passwort kann jede Art von Zeichen enthalten und darf maximal 30 Zeichen lang sein.

   Bei der Verwendung von Sonderzeichen ist zu beachten, dass diese auf allen verwendeten Tastaturen vorhanden sein müssen und von jeder Client-Software und allen Betriebssystemen korrekt unterstützt werden. Das Kopieren und Einfügen von Sonderzeichen für Passwörter kann je nach diesen externen Faktoren zu ungültigen Passwörtern führen.

   ---

4. *OK* wählen und `Enter` drücken.

→ Eine Nachricht informiert den Benutzer darüber, das der Web-Administrator erstellt wurde.

5. `Enter` drücken, um die Nachricht zu schließen.

5.3.3.4 Einen Greenbone-Enterprise-Feed-Subskription-Schlüssel eingeben oder hochladen

Falls kein gültiger Subskription-Schlüssel auf der Appliance gespeichert ist, nutzt die Appliance nur den öffentlichen Greenbone Community Feed und nicht den Greenbone Enterprise Feed.

Bemerkung: Es ist nicht notwendig, einen Greenbone-Enterprise-Feed-Subskription-Schlüssel auf einer neu gelieferten Appliance hinzuzufügen, da bereits ein Schlüssel vorinstalliert ist.

Ein Subskription-Schlüssel kann wie folgt eingegeben oder hochgeladen werden:

1. *Editor* wählen und `Enter` drücken (siehe Abb. 5.23).

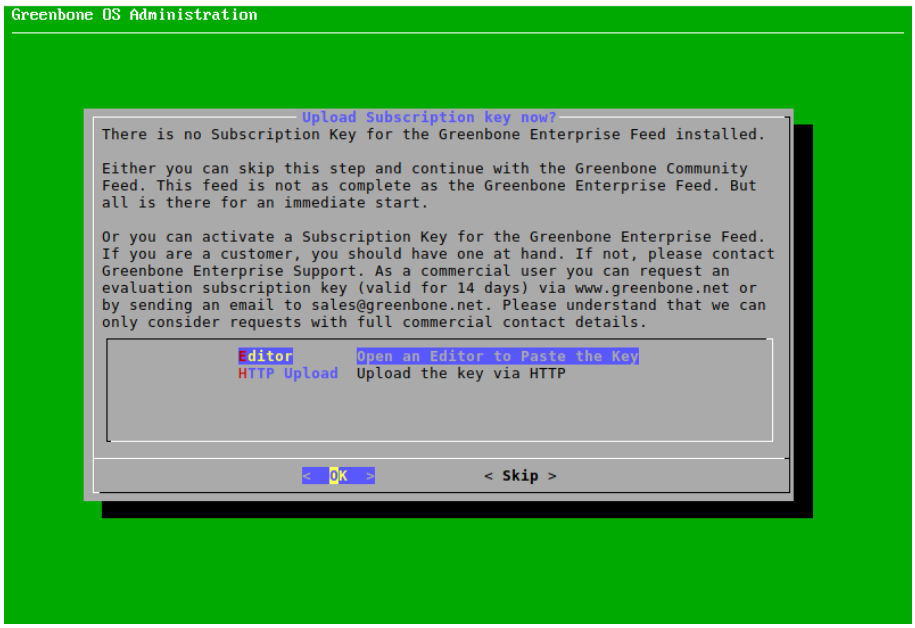


Abb. 5.23: Eingabe oder Hochladen eines Subskription-Schlüssels

→ Der Editor wird geöffnet.

2. Den GSF-Subscription-Schlüssel eingeben.
3. `Strg` + `S` drücken, um die Änderungen zu speichern.
4. `Strg` + `X` drücken, um den Editor zu schließen.

   oder

1. *HTTP Upload* wählen und `Enter` drücken.
2. Webbrowser öffnen und angezeigte URL eingeben.
3. Auf *Browse. . .* klicken, den Subscription-Schlüssel wählen und auf *Upload* klicken.

5.3.3.5 Den Feed herunterladen

Falls kein Feed auf der Appliance vorhanden ist, kann der Feed wie folgt heruntergeladen werden:

1. *Yes* wählen und `Enter` drücken (siehe Abb. 5.24).

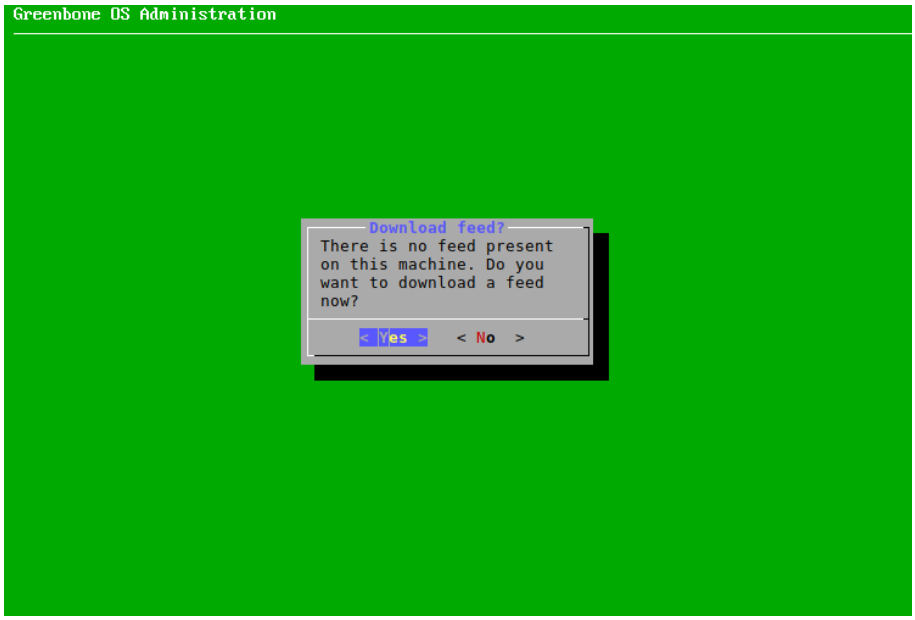


Abb. 5.24: Herunterladen des Feeds

→ Eine Meldung informiert den Nutzer darüber, dass das Feed-Update im Hintergrund gestartet wurde (siehe Abb. 5.25).

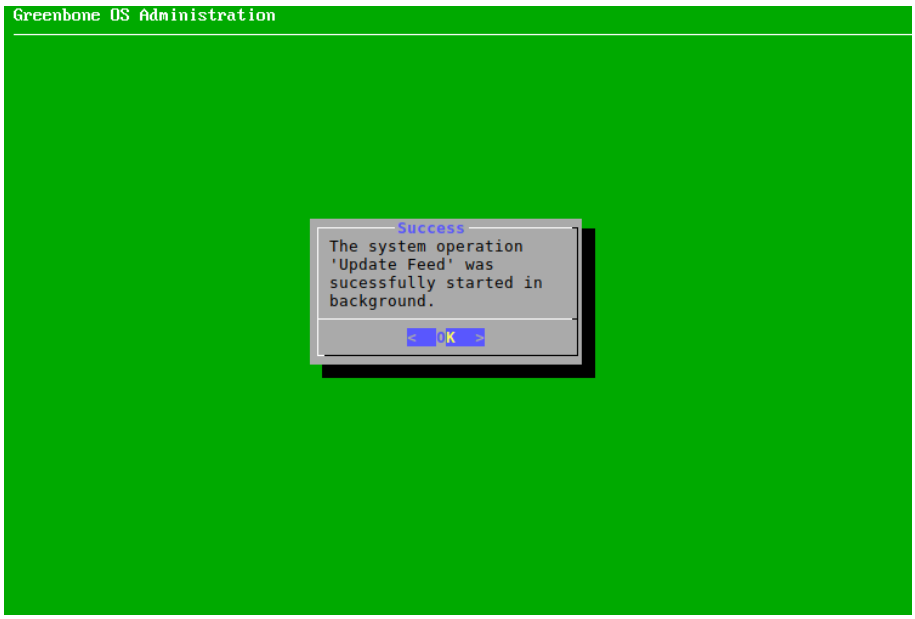


Abb. 5.25: Herunterladen des Feeds

2. `Enter` drücken, um die Nachricht zu schließen.

5.3.3.6 Den First Setup Wizard abschließen

Bemerkung: Nach dem letzten Schritt wird ein Statuscheck durchgeführt.

1. `Enter` drücken, wenn der Check beendet ist.

   → Die Ergebnisse des Checks werden angezeigt (siehe Abb. 5.26).

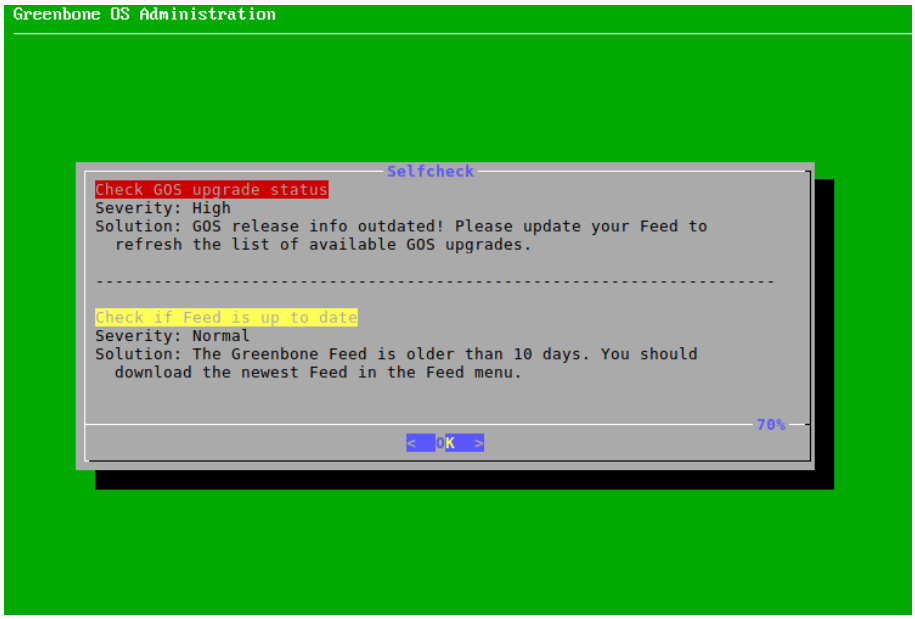


Abb. 5.26: Ergebnis der Statusprüfung

2. `Enter` drücken.

   → Das GOS-Administrationsmenü kann wie in Kapitel *7* (Seite 65) beschrieben genutzt werden.

   Falls es unvollständige oder übersprungene Schritte gibt, wird der First Setup Wizard beim nächsten Einloggen erneut angezeigt.

5.3.4 In die Web-Oberfläche einloggen

Bemerkung: Dieser Schritt entfällt für die Greenbone Enterprise 25V.

Die wichtigste Schnittstelle der Appliance ist die Web-Oberfläche, auch Greenbone Security Assistant (GSA) genannt. Auf die Web-Oberfläche kann wie in Kapitel *8.1* (Seite 164) beschrieben zugegriffen werden.

KAPITEL 6

Die Greenbone Enterprise Appliance auf die neueste Hauptversion upgraden

GOS 21.04 unterstützt nahtlose Upgrades auf die neue Hauptversion GOS 22.04.

Alle Systemeinstellungen und Benutzerdaten werden beibehalten und automatisch in die neue Version migriert, es sei denn, eine Änderung des Standardverhaltens betrifft eine bestimmte Einstellung oder Daten. Eine Liste der Änderungen am Standardverhalten befindet sich in Kapitel *6.5* (Seite 61).

6.1 Das Greenbone Operating System upgraden

Bemerkung: Vor dem Upgrade auf GOS 22.04 müssen einige Voraussetzungen in GOS 21.04 erfüllt sein:

- Die neueste Version von GOS 21.04 muss auf der Appliance installiert sein.
- Ein Feed Import Owner muss wie hier[6] beschrieben festgelegt werden.
- Die Datenobjekte müssen installiert werden. Dazu ist ein Feed-Update nach dem Festlegen des Feed Import Owners erforderlich.

Es wird empfohlen, vor dem Upgrade auf GOS 22.04 zum Netzwerkmodus *gnm* zu wechseln (siehe Kapitel *7.2.2.1* (Seite 81)).

Das Upgrade auf GOS 22.04 kann wie folgt durchgeführt werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Upgrade* wählen und `Enter` drücken.

   → Eine Nachricht informiert darüber, dass ein neues GOS-Release verfügbar ist.
3. `Enter` drücken, um die Nachricht zu schließen.

[6] https://docs.greenbone.net/GSM-Manual/gos-21.04/de/managing-gos.html#changing-the-feed-import-owner

4. *Switch Release* wählen und `Enter` drücken.

   → Eine Warnung informiert darüber, dass die Appliance auf eine grundlegende neue Version aktualisiert wird (siehe Abb. 6.1).

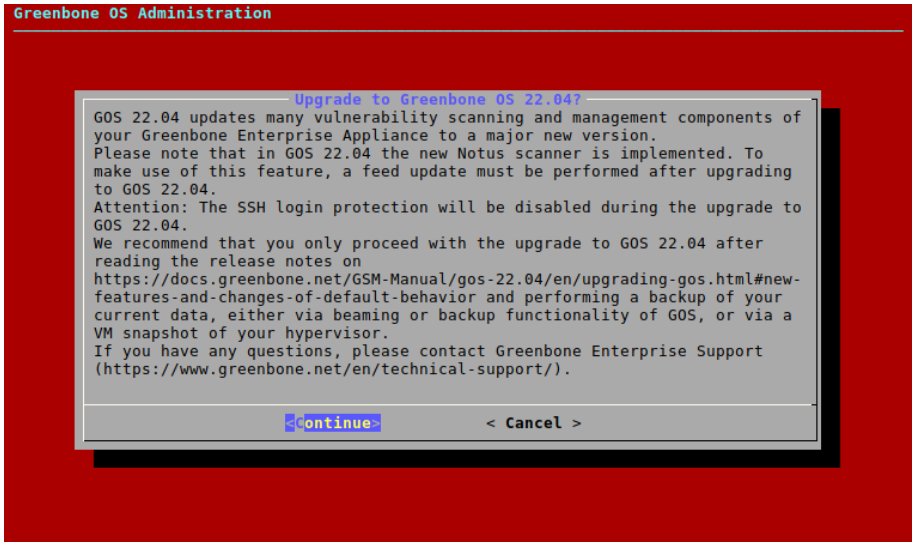


Abb. 6.1: Warnung beim Upgrade auf GOS 22.04

5. *Continue* wählen und `Enter` drücken.

   → Eine Warnung informiert darüber, dass die Appliance während des Upgrades auf GOS 22.04 gesperrt ist (siehe Abb. 6.2).

Bemerkung: Während des Upgrades können keine Systemoperationen durchgeführt werden. Alle laufenden Systemoperationen müssen vor dem Upgrade abgeschlossen werden.

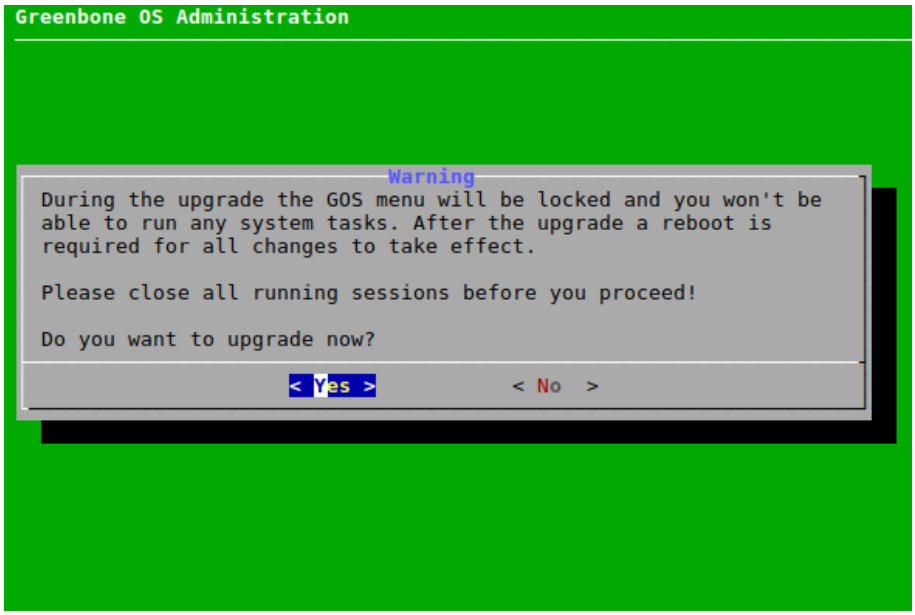


Abb. 6.2: Warnung, dass das System während des Upgrades gesperrt ist

6. *Yes* wählen und `Enter` drücken.

→ Eine Nachricht informiert darüber, dass das Upgrade gestartet wurde.

Bemerkung: Wenn das Upgrade beendet ist, informiert eine Nachricht darüber, dass ein Reboot nötig ist, um alle Änderungen anzuwenden (siehe Abb. 6.3).

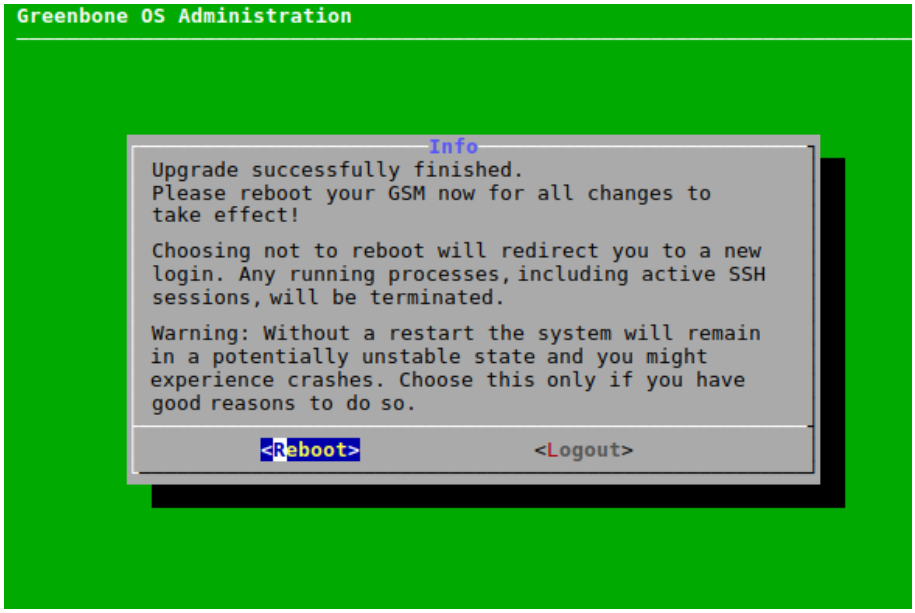


Abb. 6.3: Meldung nach dem erfolgreichen Upgrade

7. *Reboot* wählen und `Enter` drücken.

   → Nachdem der Reboot abgeschlossen ist, wird geprüft, ob es offene Einrichtungsschritte gibt. Falls es offene Schritte gibt, wird gefragt, ob diese nun abgeschlossen werden sollen.

Bemerkung: Wenn beim Upgrade von GOS 21.04 auf GOS 22.04 noch der alte Legacy-Netzwerkmodus verwendet wurde, bietet eine Meldung an, auf den neuen Netzwerkmodus *GOS Network Manager (gnm)* umzuschalten. Wenn der Netzwerkmodus nicht direkt nach dem Upgrade umgestellt wird, kann dies auch zu einem späteren Zeitpunkt erfolgen (siehe Kapitel *7.2.2.1* (Seite 81)).

Nach dem Upgrade auf GOS 22.04 muss ein Feed-Update durchgeführt werden, um neue Funktionen wie den Notus-Scanner nutzen zu können (siehe Kapitel *6.5* (Seite 61)).

6.2 Die Flash-Partition auf die neueste GOS-Version upgraden

Die interne Flash-Partition der Appliance enthält ein Backup von GOS und wird im Falle eines Factory-Resets verwendet.

Es wird empfohlen, die GOS-Version auf der Flash-Partition zu aktualisieren (siehe Kapitel *7.3.8* (Seite 153)).

6.3 Nach einem Upgrade neu im GOS-Administationsmenü anmelden

Es ist möglich, dass ein GOS-Upgrade die über das GOS-Administrationsmenü verfügbaren Funktionen verändert. Diese geänderten Funktionen sind erst nach einem erneuten Laden des GOS-Administrationsmenüs verfügbar. Es wird daher empfohlen, sich nach dem GOS-Upgrade vom GOS-Administrationsmenü abzumelden und wieder neu anzumelden.

6.4 Web-Oberfläche nach einem Upgrade neu laden

Nach einem Upgrade von einer grundlegenden Version auf eine andere muss der Cache des Browsers, der für die Web-Oberfläche genutzt wird, geleert werden. Das Leeren des Browsercaches kann in den Einstellungen des genutzten Browsers vorgenommen werden.

Alternativ kann der Seitencache jeder Seite der Web-Oberfläche geleert werden, indem `Strg` und `F5` gedrückt wird.

Bemerkung: Das Leeren des Seitencaches muss für jede einzelne Seite durchgeführt werden.

Das Leeren des Browsercaches ist global und für alle Seiten gültig.

6.5 Neue Features und Änderungen des Standardverhaltens

Die folgende Liste zeigt die wichtigsten Erweiterungen und Änderungen des Standardverhaltens von GOS 21.04 zu GOS 22.04.

Abhängig von den aktuell verwendeten Funktionen können sich diese Änderungen auf das aktuell eingesetzte Setup auswirken. Eine vollständige Liste der Änderungen befindet sich auf der Seite Roadmap & Lifecycle[7].

6.5.1 Notus-Scanner

Mit GOS 22.04 wird der neue Notus-Scanner eingeführt. Er scannt nach jedem regulären Scan, so dass keine Benutzerinteraktion erforderlich ist.

Der Notus-Scanner bietet eine bessere Leistung, da er weniger Systemressourcen verbraucht und somit schneller scannt.

Wenn eine Scan-Konfiguration manuell erstellt wird und der Notus-Scanner funktionieren soll, muss der VT *Determine OS and list of installed packages via SSH login* (OID: 1.3.6.1.4.1.25623.1.0.50282) aktiviert sein.

Der Notus-Scanner ersetzt die Logik potenziell aller NASL-basierten lokalen Sicherheitskontrollen (engl. local security checks, LSCs). Statt für jeden LSC ein VT-Skript auszuführen, wird ein Vergleich der auf einem Host installierten Software mit einer Liste bekannter anfälliger Software durchgeführt.

Der reguläre OpenVAS-Scanner lädt jeden NASL-LSC einzeln und führt ihn nacheinander für jeden Host aus. Eine einzelne bekannte Schwachstelle wird dann mit der installierten Software verglichen. Dies wird für alle LSCs wiederholt.

Mit dem Notus-Scanner wird die bei einem Scan ermittelte Liste der installierten Software direkt mit allen bekannten Schwachstellen verglichen. Dadurch entfällt die Notwendigkeit, die LSCs auszuführen, da die Informationen über die bekannte anfällige Software in einer einzigen Liste gesammelt und nicht in einzelnen NASL-Skripten verteilt werden.

[7] https://www.greenbone.net/roadmap-lifecycle/#gos-22-04

Derzeit gibt es Notus-Daten für die folgenden LSC-VT-Familien:

- AlmaLinux Local Security Checks
- Amazon Linux Local Security Checks
- Debian Local Security Checks
- EulerOS Local Security Checks
- Mageia Linux Local Security Checks
- Oracle Linux Local Security Checks
- Rocky Linux Local Security Checks
- Slackware Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

Die Einstellung *Report vulnerabilities of inactive Linux kernel(s) separately* im VT *Options for Local Security Checks* ist nicht mehr gültig. Die Einstellung ist zwar noch sichtbar, aber nicht mehr funktionsfähig.

6.5.2 Funktionsumfang der Appliance

Mit GOS 22.04 wird der Funktionsumfang für einige Appliances erweitert:

- Der SNMP-Dienst (GOS-Menü *Setup > Services > SNMP*) wird für die Appliance-Modelle Greenbone Enterprise 150, Greenbone Enterprise 35, Greenbone Enterprise CENO und Greenbone Enterprise 25V verfügbar gemacht.
- Die automatische Zeitsynchronisation über NTP (GOS-Menü *Setup > Timesync*) wird für die Appliance-Modelle Greenbone Enterprise CENO und Greenbone Enterprise 25V verfügbar gemacht.
- Die Remote- und lokale Backup-Funktionalität (GOS-Menüs *Setup > Backup*, *Maintenance > Backup > Incremental Backup* und *Maintenance > Backup > List*) wird für das Appliance-Modell Greenbone Enterprise CENO verfügbar gemacht.

6.5.3 Virtuelle Appliances

Mit GOS 22.04 wurden die Größen der virtuellen Festplatten für virtuelle Appliances geändert.

Die neuen Größen sind:

- Greenbone Enterprise EXA: 225 GB
- Greenbone Enterprise DECA/PETA/EXA: 220 GB
- Greenbone Enterprise CENO: 135 GB
- Greenbone Enterprise ONE: 130 GB
- Greenbone Enterprise 25V: 70 GB

Die neuen Größen sind nur für neu installierte virtuelle Appliances relevant. Upgegradete Appliances behalten ihr Partitionslayout und damit ihre erforderliche Festplattengröße bei.

6.5.4 HTTP-Zugriff auf die Web-Oberfläche

Mit GOS 22.04 wird der unverschlüsselte HTTP-Zugriff auf die Web-Oberfläche nicht mehr unterstützt. Stattdessen muss HTTPS verwendet werden.

Ein gültiges HTTPS-Zertifikat (entweder selbst signiert oder von einer Zertifizierungsstelle signiert) muss nun auf der Appliance konfiguriert werden, um die Web-Oberfläche zu nutzen (siehe Kapitel *7.2.4.1.7* (Seite 101)).

6.5.5 Backups

6.5.5.1 Passwort für Remote-Backup-Repository

Mit GOS 22.04 ist es möglich, das Passwort für das Remote-Backup-Repository zu ändern. Dazu wurde im GOS-Administrationsmenü der Menüpunkt *Setup > Backup > Backup Password* hinzugefügt. Der Menüpunkt ist nur sichtbar, wenn der Ort des Backups als *remote* konfiguriert ist.

Es wird empfohlen, das Backup-Passwort zu ändern.

Wenn mehrere Appliances dasselbe Remote-Backup-Repository verwenden, wird empfohlen, dass jede Appliance ihr eigenes, eindeutiges Backup-Passwort verwendet.

6.5.5.2 *obnam*

Mit GOS 20.08 wurde das Backend für die Verwaltung von Backups in GOS von *obnam* auf *restic* umgestellt. Allerdings war *obnam* in GOS 20.08 und 21.04 weiterhin verfügbar, ebenso wie die mit *obnam* in GOS 6 oder früher erstellten Backups.

Mit GOS 22.04 werden *obnam* und alle mit *obnam* erstellten Backups entfernt. Inkrementelle Backups, die mit GOS 6 und früher erstellt wurden, werden aufgrund von Inkompatibilität und zur Rückgewinnung von Speicherplatz entfernt.

Wenn diese alten Backups beibehalten werden sollen, muss vor dem Upgrade auf GOS 22.04 eine Kopie der Dateien erstellt werden. Falls Fragen auftreten, kann der Greenbone Enterprise Support[8] kontaktiert werden.

6.5.6 Mailhub

Mit GOS 22.04 wird eine neue Option hinzugefügt, um die Verwendung von SMTPS für die von einer Greenbone Enterprise Appliance versendeten E-Mails zu erzwingen.

Dazu gibt es im GOS-Administrationsmenü das neue Menü *Setup > Mail > SMTP Enforce TLS*.

6.5.7 Web-Oberfläche

6.5.7.1 Geschäftsprozessanalyse

Mit GOS 22.04 wird die Geschäftsprozessanalyse-Funktionalität von der Web-Oberfläche entfernt. Vorhandene Geschäftsprozessanalysen werden gelöscht und können nicht wiederhergestellt werden. Wenn die in einer Geschäftsprozessanalyse enthaltenen Informationen gespeichert werden sollen, muss dies in GOS 21.04 erfolgen.

[8] https://www.greenbone.net/technischer-support/

6.5.7.2 Aufgaben-/Auditeinstellung *Netzwerk-Quell-Interface*

Mit GOS 22.04 wird die Aufgaben-/Auditeinstellung *Netzwerk-Quell-Interface* entfernt. Wenn diese Einstellung zuvor für eine Aufgabe oder ein Audit konfiguriert war, wird sie ignoriert.

6.5.7.3 Benutzereinstellung *Interface-Zugriff*

Da die Aufgaben-/Auditeinstellung *Netzwerk-Quell-Interface* mit GOS 22.04 entfernt wird, wird auch die Benutzereinstellung *Interface-Zugriff* entfernt. Wenn diese Einstellung zuvor für einen Benutzer konfiguriert war, wird sie ignoriert.

6.5.7.4 OVAL-Definitionen

Mit GOS 22.04 werden die OVAL-Definitionen aus dem Sicherheitsinfo-Management auf der Web-Oberfläche entfernt. Die bisherigen OVAL-Definitionen waren veraltet und erfüllten keinen Zweck mehr.

6.5.7.5 OSP-Scanner

Mit GOS 22.04 wird der Scannertyp *OSP-Scanner* entfernt. Es ist nicht mehr möglich, OSP-Scanner zu erstellen und sie für die Ausführung von Scans auszuwählen.

Dies betrifft nur den Scannertyp *OSP-Scanner*, nicht das Protokoll OSP im Allgemeinen. Der Scannertyp *Greenbone Sensor* wird weiterhin OSP verwenden.

Der Anmeldedatentyp *Benutzerzertifikat*, der für (benutzerdefinierte) OSP-Scanner verwendet wurde, wurde ebenfalls entfernt. Bestehende Anmeldedaten dieses Typs sind davon nicht betroffen und werden nicht entfernt. Es kann weiterhin auf sie zugegriffen werden, aber sie sind nicht mehr von Nutzen und können manuell gelöscht werden.

6.5.8 Qualität der Erkennung (QdE)

Mit GOS 22.04 wird die neue Stufe für die Qualität der Erkennung (QdE) *package_unreliable* mit einer QdE von 30 % eingeführt. Sie wird für authentifizierte paketbasierte Prüfungen, die nicht immer vollständig zuverlässig sind, für z. B. Linux(oide) Systeme.

6.5.9 Schwachstellen-Referenzen

Mit GOS 22.04 wird der Tag *script_bugtraq_id();*, der auf eine BID von Bugtraq verweist, nicht mehr unterstützt. Für VTs mit einem solchen Tag wurde die BID unter *Verweise* auf der Web-Oberfläche angezeigt. Da bugtraq.securityfocus.com nicht mehr gepflegt wird, hatte der Verweis zu Verwirrungen geführt.

Alle bestehenden BID-Referenzen wurden in *Andere* Referenzen migriert und erscheinen dort als URLs auf der Web-Oberfläche. Um auf den Inhalt der URLs zuzugreifen, können gängige Dienste wie archive.org genutzt werden.

6.5.10 Greenbone Management Protocol (GMP)

Das Greenbone Management Protocol (GMP) wurde auf Version 22.04 aktualisiert und die Programmierschnittstelle wurde leicht angepasst. Die Nutzung mancher Befehle wurde verändert und einige Befehle, Elemente und Attribute wurden überholt. Das gesamte Referenzhandbuch und die Liste aller Veränderungen ist hier[9] verfügbar.

[9] https://docs.greenbone.net/API/GMP/gmp-22.04.html

KAPITEL 7

Das Greenbone Operating System verwalten

Bemerkung: Dieses Kapitel dokumentiert alle möglichen Menüoptionen.

Allerdings unterstützen nicht alle Appliance-Modelle alle Menüoptionen. Um festzustellen, ob ein bestimmtes Feature für das genutzte Appliance-Modell verfügbar ist, können die Tabellen in Kapitel *3* (Seite 20) genutzt werden.

7.1 Allgemeine Informationen

7.1.1 Greenbone-Enterprise-Feed-Subskription-Schlüssel

Beim Kauf einer Greenbone Enterprise Appliance wird ein eindeutiger Subskription-Schlüssel für den Greenbone Enterprise Feed vorinstalliert, um der Appliance Zugang zum Greenbone Feed Service zu gewähren. Der Subskription-Schlüssel wird nur für Autorisierungszwecke genutzt, nicht für Abrechnungen oder Verschlüsselungen.

Der Subskription-Schlüssel ist für jede Appliance individuell und kann nicht auf mehr als einer Appliance installiert sein.

Falls der Subskription-Schlüssel gefährdet wird (z. B. indem er in die Hände Dritter gerät), entsteht dem rechtmäßigen Besitzer des Subskription-Schlüssels kein Schaden. Greenbone wird den kompromittierten Schlüssel deaktivieren, um eine weitere unbefugte Nutzung zu verhindern. Ein Ersatzschlüssel kann kostenlos ausgestellt werden.

Bei einem Factory-Reset wird der Subskription-Schlüssel von der Appliance gelöscht und muss neu installiert werden. Falls ein Factory-Reset geplant ist, sollte der Greenbone Enterprise Support[10] kontaktiert werden, um eine Kopie des Subskription-Schlüssels zu erhalten.

[10] https://www.greenbone.net/technischer-support/

7.1.2 Autorisierungskonzept

Die Appliance bietet zwei unterschiedliche Level für den Zugriff:

- **Anwendungsebene – über Web-Oberfläche oder GMP** Die Anwendungsebene ist über die Web-Oberfläche oder die API des Greenbone Management Protocol (GMP) erreichbar.
- **Systemebene – über das GOS-Administrationsmenü** Die Systemebene ist nur über die Konsole oder das Secure Shell Protocol (SSH) erreichbar.

7.1.2.1 Zugriff auf die Anwendungsebene

Die Anwendungsebene ermöglicht den Zugriff auf Schwachstellenscanning und -verwaltung und unterstützt die Administration von Benutzern, Gruppen und Berechtigungen.

Der Zugriff auf die Anwendungsebene ist entweder über die Web-Oberfläche (siehe Kapitel *8* (Seite 164) und *9* (Seite 184)) oder über die API des Greenbone Management Protocol (GMP) (siehe Kapitel *15* (Seite 370)) möglich.

Bemerkung: Bei der Auslieferung der Appliance durch Greenbone oder nach einem Factory-Reset ist standardmäßig kein Account für die Anwendungsebene konfiguriert. Es ist notwendig, mindestens einen solchen Account, einen sogenannten „Web-Administrator“, über das GOS-Administrationsmenü zu erstellen (siehe Kapitel *7.2.1.3* (Seite 72)).

Neben dem initialen Web-Administrator gibt es zwei Möglichkeiten, Web-Benutzer anzulegen:

Über die Web-Oberfläche Über die Web-Oberfläche können Web-Benutzer mit unterschiedlichen Rollen und Berechtigungen angelegt werden. Diese Benutzer haben einen Besitzer, welcher der Benutzer ist, der sie angelegt hat. Sie können sowohl über die Web-Oberfläche als auch über das GOS-Administrationsmenü verwaltet werden.

Über das GOS-Administrationsmenü Benutzer, die über das GOS-Administrationsmenü angelegt werden, haben immer die Rolle *Admin*. Diese Benutzer haben keinen Besitzer und sind sogenannte „globale Objekte“. Manchmal werden sie auch als „global web users“ bezeichnet. Sie können nur über das GOS-Administrationsmenü oder von einem Super-Administrator verwaltet werden.

Bemerkung: Für die Appliance-Modelle Greenbone Enterprise 35 und Greenbone Enterprise 25V ist kein Zugriff auf die Anwendungsebene möglich. Diese Appliances müssen über eine Master-Appliance verwaltet werden.

7.1.2.2 Zugriff auf die Systemebene

Die Systemebene ermöglicht den Zugriff auf die Administration des Greenbone Operating Systems (GOS). Nur ein einziger Systemadministrator wird unterstützt. Der Systemadministrator kann Systemdateien nicht direkt verändern, aber das System anweisen, Konfigurationen zu ändern.

GOS wird über eine menübasierte grafische Oberfläche (GOS-Administrationsmenü) verwaltet. Die Befehlszeile (Shell) muss nicht für Konfigurations- oder Wartungsaufgaben verwendet werden. Der Shell-Zugang ist nur für Support- und Fehlerbehebungszwecke vorgesehen.

Für den Zugriff auf die Systemebene wird entweder ein Konsolenzugriff (seriell, Hypervisor oder Monitor/Tastatur) oder eine SSH-Verbindung benötigt. Um SSH zu nutzen, ist eine Netzwerkverbindung notwendig und der SSH-Dienst muss aktiviert sein (siehe Kapitel *7.2.4.4* (Seite 107)).

Nach dem Ausliefern der Appliance durch Greenbone oder nach einem Factory-Reset ist ein Standardaccount und -passwort für den Systemadministrator vorkonfiguriert. Während des ersten Setups sollte das Passwort des Systemadministrators geändert werden (siehe Kapitel *7.2.1.1* (Seite 70)).

Mithilfe der Konsole auf das GOS-Administrationsmenü zugreifen

Nachdem die Appliance eingeschaltet wurde, bootet sie. Dieser Prozess kann in der Konsole überwacht werden.

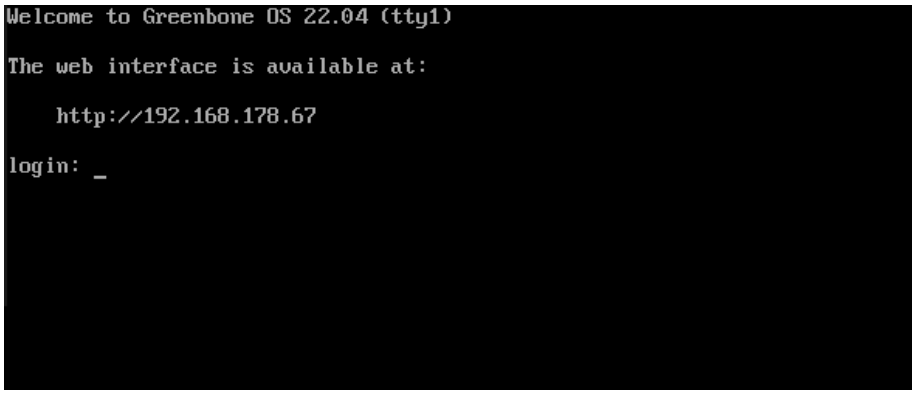


Abb. 7.1: Eingabeaufforderung der Appliance

Nachdem der Boot-Vorgang abgeschlossen ist, wird eine Eingabeaufforderung angezeigt (siehe Abb. 7.1). Die Standarddaten für den Login sind:

- Benutzer: `admin`
- Passwort: `admin`

> **Bemerkung:** Während des ersten Setups sollte dieses Passwort geändert werden (siehe Kapitel *7.2.1.1* (Seite 70)).

Nach dem Ausliefern der Appliance durch Greenbone oder nach einem Factory-Reset wird ein Setup-Wizard angezeigt, der bei der grundlegenden Konfiguration von GOS behilflich ist.

- Durch Wählen von *Yes* und Drücken von `Enter` können alle notwendigen Einstellungen konfiguriert werden.
- Durch Wählen von *No* und Drücken von `Enter` wird der Setup-Wizard geschlossen. Unvollständige Schritte werden beim nächsten Einloggen wieder angezeigt.
- Durch Wählen von *No* und Drücken von `Enter` wird der Setup-Wizard geschlossen. Unvollständige Schritte werden beim nächsten Einloggen **nicht** wieder angezeigt.

Mithilfe von SSH auf das GOS-Administrationsmenü zugreifen

Bemerkung: Nach dem Ausliefern der Appliance durch Greenbone oder nach einem Factory-Reset ist der SSH-Zugriff möglicherweise deaktiviert und muss zuerst über die Konsole aktiviert werden (siehe Kapitel *7.2.4.4* (Seite 107)). Für SSH wird eine Netzwerkverbindung benötigt (siehe Kapitel *7.2.2.4* (Seite 83)).

Linux-, macOS- oder Unix-ähnliche Systeme

Um eine SSH-Verbindung auf Linux-, macOS- oder Unix-ähnlichen Systemen herzustellen, kann die Befehlszeile wie folgt genutzt werden:

```
$ ssh admin@<appliance>
```

`<appliance>` durch die IP-Adresse oder den Domainnamen der Appliance ersetzen.

Durch Anzeigen des Fingerprints kann der Host-Schlüssel wie folgt verifiziert werden:

1. In das GOS-Administrationsmenü einloggen.
2. *Setup* wählen und `Enter` drücken.
3. *Services* wählen und `Enter` drücken.
4. *SSH* wählen und `Enter` drücken.
5. *Fingerprint* wählen und `Enter` drücken.

   → Der Fingerprint wird angezeigt.

Microsoft Windows

Um eine SSH-Verbindung auf Microsoft-Windows-Systemen herzustellen, können die Tools PuTTY oder smarTTY genutzt werden. Auf Microsoft Windows Server 2019, Microsoft Windows 10 Build 1809 oder neuer kann die OpenSSH-Client-Komponente installiert werden, um über die Befehlszeile auf SSH zuzugreifen.

7.1.3 Das GOS-Administrationsmenü nutzen

Das GOS-Administrationsmenü kann mithilfe einer Tastatur gesteuert werden.

- Die Pfeiltasten der Tastatur werden für die Menüauswahl verwendet.
- Durch Drücken von `Enter` wird die aktuelle Menüauswahl bestätigt und fortgefahren.
- Durch Drücken von `Space` wird zwischen Auswahlmöglichkeiten gewechselt.
- Das aktuelle Menü kann durch Drücken von `Esc` verlassen werden.
- In den meisten Fällen werden Änderungen, die im GOS-Administrationsmenü vorgenommen werden, nicht sofort aktiviert. Stattdessen wird der Menüpunkt *Save* unterhalb der anderen Optionen eingefügt (siehe Abb. 7.2). *Save* wählen und `Enter` drücken, um die Änderungen zu speichern.

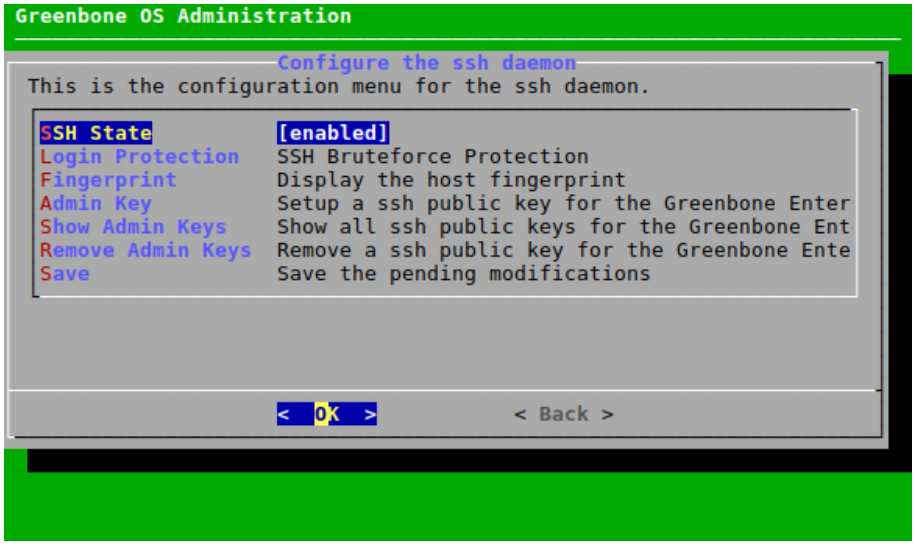


Abb. 7.2: Neue Menüoption zum Speichern ausstehender Änderungen

Falls ein Menü verlassen wird, ohne die ausstehenden Änderungen zu speichern, wird eine Warnung angezeigt (siehe Abb. 7.3).

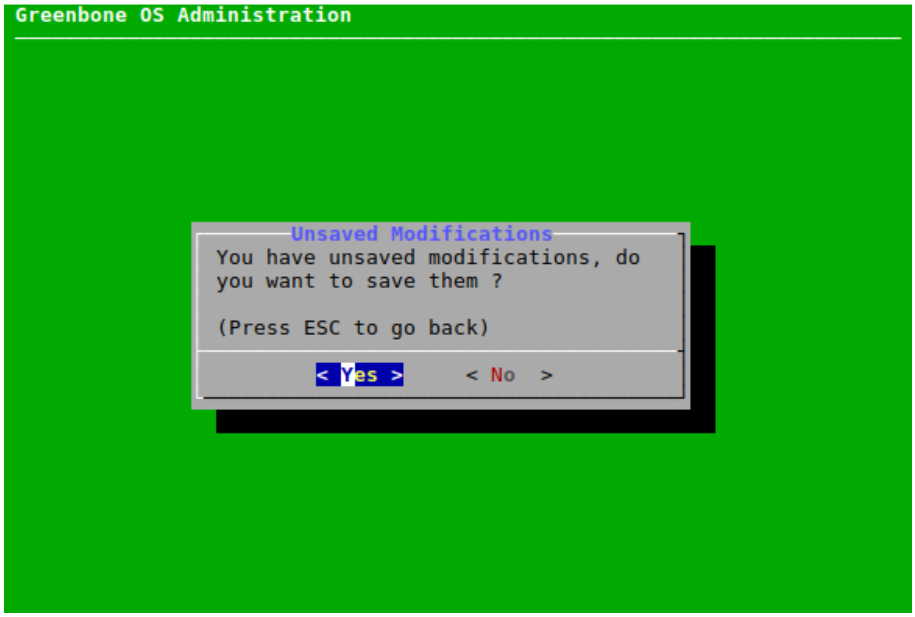


Abb. 7.3: Speichern ausstehender Änderungen

7.2 Setup-Menü

7.2.1 Benutzer verwalten

7.2.1.1 Das Passwort des Systemadministrators ändern

Das Passwort des Systemadministrators kann geändert werden. Dies ist besonders bei der ersten grundlegenden Konfiguration wichtig. Die Standardeinstellung ist für eine Produktionsumgebung nicht geeignet.

Das Passwort kann wie folgt geändert werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Password* wählen und `Enter` drücken (siehe Abb. 7.4).

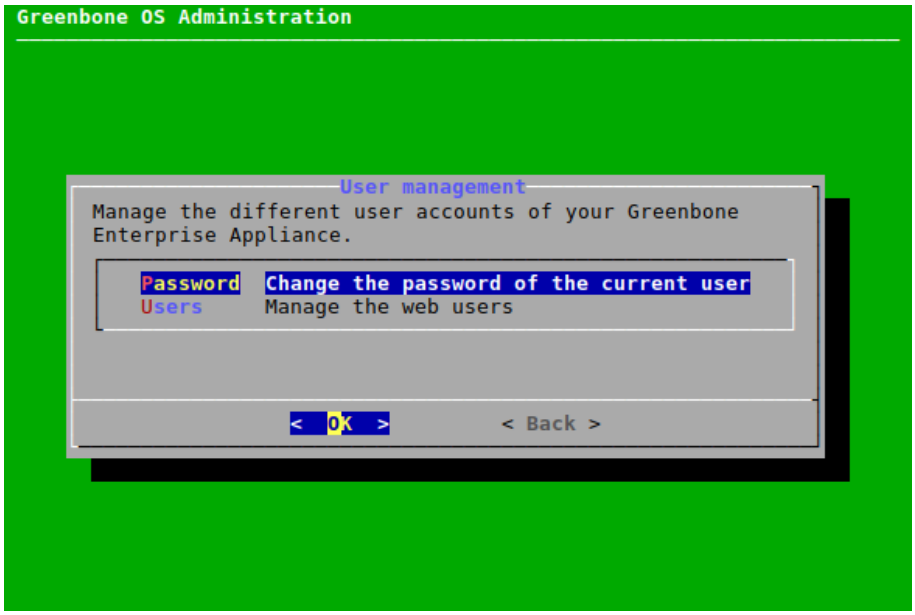


Abb. 7.4: Öffnen der Benutzerverwaltung

4. Aktuelles Passwort eingeben und `Enter` drücken (siehe Abb. 7.5).

Abb. 7.5: Das Passwort des Systemadministrators ändern

5. Neues Passwort eingeben und `Enter` drücken.

Bemerkung: Triviale Passwörter einschließlich des Standardpassworts `admin` werden abgelehnt.

6. Neues Passwort wiederholen und `Enter` drücken.

Bemerkung: Die Änderung tritt sofort in Kraft und eine Bestätigung ist nicht notwendig. Es ist nicht möglich, die Änderung rückgängig zu machen.

7.2.1.2 Web-Benutzer verwalten

Das GOS-Administrationsmenü bietet die Möglichkeit, Web-Benutzer (= Benutzerkonten für die Web-Oberfläche der Appliance und die GMP-API) zu verwalten.

Bemerkung: Für die Appliance-Modelle Greenbone Enterprise 35 und Greenbone Enterprise 25V gibt es keine Web-Oberfläche.

Für diese Appliance-Modelle sind dieses Kapitel und seine Unterkapitel nicht relevant.

Bemerkung: Um die Web-Oberfläche der Appliance nutzen zu können, muss mindestens ein Web-Administrator (= Web-Benutzer mit der Rolle *Admin*) erstellt werden (siehe Kapitel *7.2.1.3* (Seite 72)).

Web-Administratoren, die über das GOS-Administrationsmenü erstellt wurden, haben keinen Besitzer und sind sogenannte „globale Objekte“. Manchmal werden sie auch als „global web users“ bezeichnet. Sie können nur über das GOS-Administrationsmenü oder von einem Superadministrator verwaltet werden.

Alle Web-Benutzer können wie folgt angezeigt werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *List Users* wählen und `Enter` drücken, um eine Liste aller konfigurierten Web-Benutzer anzeigen zu lassen (siehe Abb. 7.6).

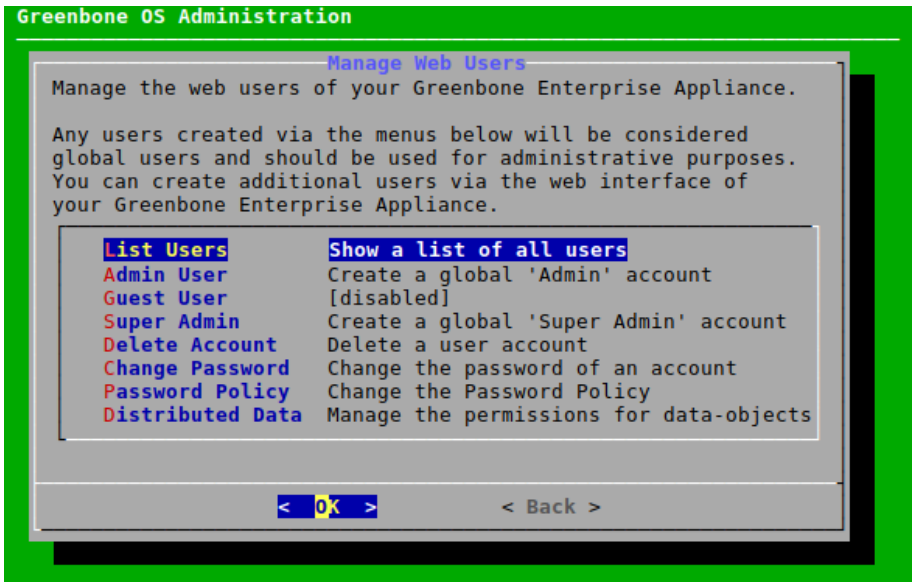


Abb. 7.6: Verwalten der Web-Benutzer

7.2.1.3 Einen Web-Administrator erstellen

Um die Web-Oberfläche der Appliance nutzen zu können, muss mindestens ein Web-Administrator (= Web-Benutzer mit der Rolle *Admin*) erstellt werden.

Bemerkung: Das Anlegen des ersten Web-Administrators ist nur über das GOS-Administrationsmenüs möglich.

Ein neuer Web-Administrator kann wie folgt erstellt werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *Admin User* wählen und `Enter` drücken.
5. Benutzernamen für den Web-Administrator festlegen (siehe Abb. 7.7).

Bemerkung: Für den Benutzernamen sind nur die folgenden Zeichen zulässig:

- Alle alphanumerischen Zeichen
- - (Bindestrich)
- _ (Unterstrich)
- . (Punkt)

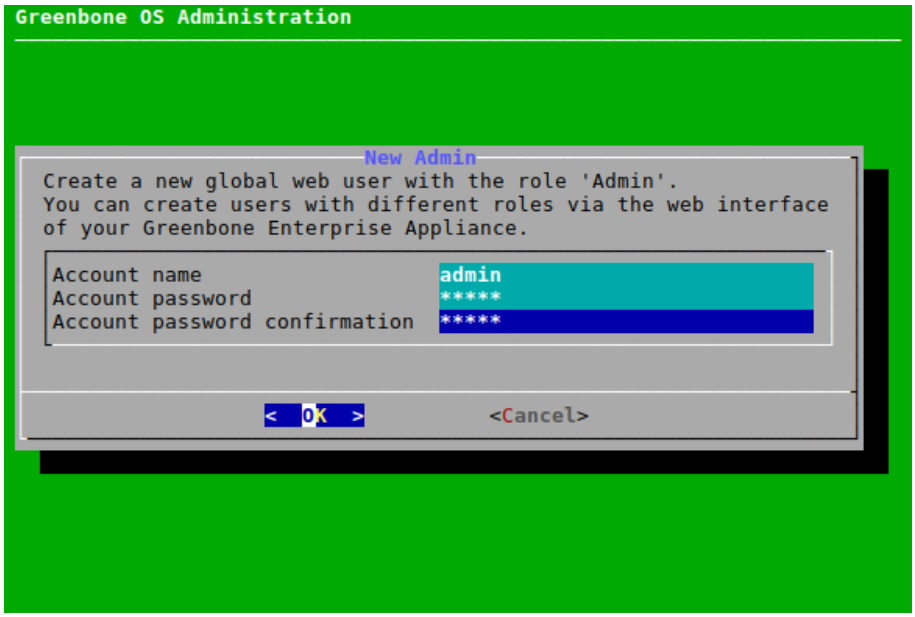


Abb. 7.7: Erstellen eines neuen Web-Administrators

6. Passwort für den Web-Administrator zweimal eingeben.

   Bemerkung: Das Passwort kann jede Art von Zeichen enthalten und darf maximal 30 Zeichen lang sein.

   Bei der Verwendung von Sonderzeichen ist zu beachten, dass diese auf allen verwendeten Tastaturen vorhanden sein müssen und von jeder Client-Software und allen Betriebssystemen korrekt unterstützt werden. Das Kopieren und Einfügen von Sonderzeichen für Passwörter kann je nach diesen externen Faktoren zu ungültigen Passwörtern führen.

7. *OK* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass der Web-Administrator erstellt wurde.

8. `Enter` drücken, um die Meldung zu schließen.

7.2.1.4 Einen Gastbenutzer aktivieren

Damit sich ein Gast ohne Passwort anmelden kann, muss der Gastzugang wie folgt aktiviert werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *Guest User* wählen und `Enter` drücken.
5. Benutzernamen und Passwort eines vorhandenen Web-Benutzers eingeben und `Tab` drücken.
6. `Enter` drücken.

   → Der Web-Benutzer kann sich nun auch ohne Passwort auf der Web-Oberfläche anmelden (siehe Abb. 7.8).

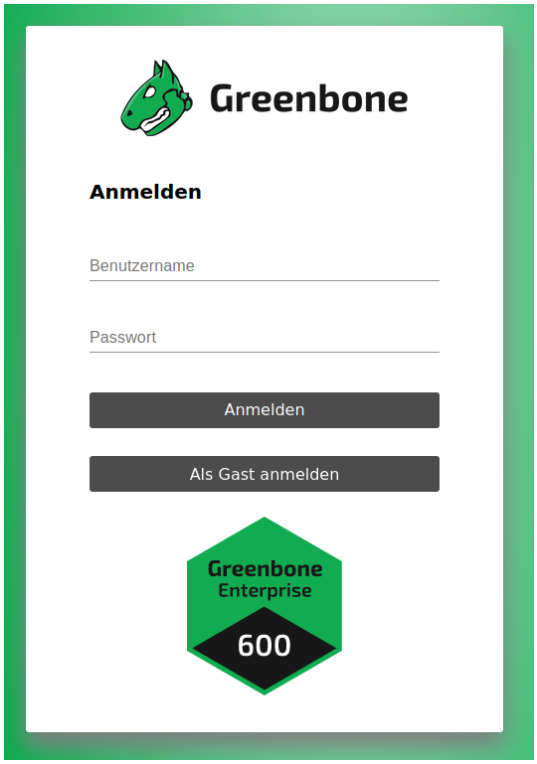


Abb. 7.8: Einloggen als Gast ohne Nutzung eines Passworts

7.2.1.5 Einen Super-Administrator erstellen

Die Rolle *Super Admin* stellt die höchste Zugriffsstufe dar. Ein Benutzer mit dieser Rolle kann wie folgt erstellt werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *Super Admin* wählen und `Enter` drücken.

   → Eine Warnung fordert den Benutzer auf, den Vorgang zu bestätigen (siehe Abb. 7.9).
5. *Yes* wählen und `Enter` drücken.
6. Benutzernamen für den Super-Administrator festlegen.

Bemerkung: Für den Benutzernamen sind nur die folgenden Zeichen zulässig:

- Alle alphanumerischen Zeichen
- - (Bindestrich)
- _ (Unterstrich)
- . (Punkt)

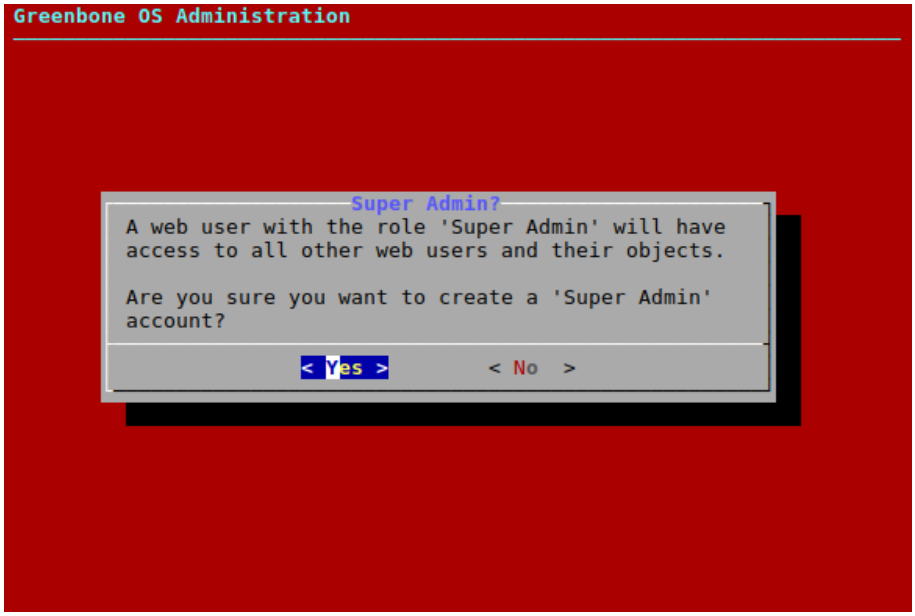


Abb. 7.9: Warnung beim Erstellen eines neuen Super-Administrators

7. Passwort für den Super-Administrator zweimal eingeben.

Bemerkung: Das Passwort kann jede Art von Zeichen enthalten und darf maximal 30 Zeichen lang sein.

Bei der Verwendung von Sonderzeichen ist zu beachten, dass diese auf allen verwendeten Tastaturen vorhanden sein müssen und von jeder Client-Software und allen Betriebssystemen korrekt unterstützt werden. Das Kopieren und Einfügen von Sonderzeichen für Passwörter kann je nach diesen externen Faktoren zu ungültigen Passwörtern führen.

---

8. *OK* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass der Super-Administrator erstellt wurde.

9. `Enter` drücken, um die Meldung zu schließen.

Bemerkung: Der Super-Administrator kann nur vom Super-Administrator selbst bearbeitet werden.

7.2.1.6 Einen Benutzeraccount löschen

Bemerkung: Super-Administratoren können nur wie hier beschrieben gelöscht werden. Das Löschen eines Super-Administrators über die Web-Oberfläche ist nicht möglich.

Der Benutzer, der Feed Import Owner ist, kann nicht gelöscht werden. Zuerst muss ein anderer Feed Import Owner festgelegt oder die Einstellung auf *(Unset)* geändert werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Ein Web-Benutzer kann wie folgt gelöscht werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.

4. *Delete Account* wählen und `Enter` drücken.
5. Web-Benutzer, der gelöscht werden soll, wählen und `Enter` drücken.

   → Eine Meldung fragt, ob ein Nachfolger gewählt werden soll.
6. Falls ein Nachfolger festgelegt werden soll, *Yes* wählen und `Enter` drücken.
7. Web-Benutzer, der der Nachfolger sein soll, wählen und `Enter` drücken.

   → Der Web-Benutzer wird sofort gelöscht.

   oder
6. Falls kein Nachfolger festgelegt werden soll, *No* wählen und `Enter` drücken.

   → Der Web-Benutzer wird sofort gelöscht.

7.2.1.7 Die Anzahl der gleichzeitigen Websitzungen begrenzen

Derselbe Web-Benutzer kann sich in mehreren Websitzungen auf der Web-Oberfläche anmelden. Es ist möglich, die Anzahl der gleichzeitigen Websitzungen zu begrenzen.

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *User sessions* wählen und `Enter` drücken.
5. Maximale Anzahl der gleichzeitigen Websitzungen in das Eingabefeld eingeben (siehe Abb. 7.10).

Bemerkung: Der Wert kann zwischen `0` und `25` liegen. Der Standardwert ist `0`, was bedeutet, dass die Anzahl der Websitzungen unbegrenzt ist.

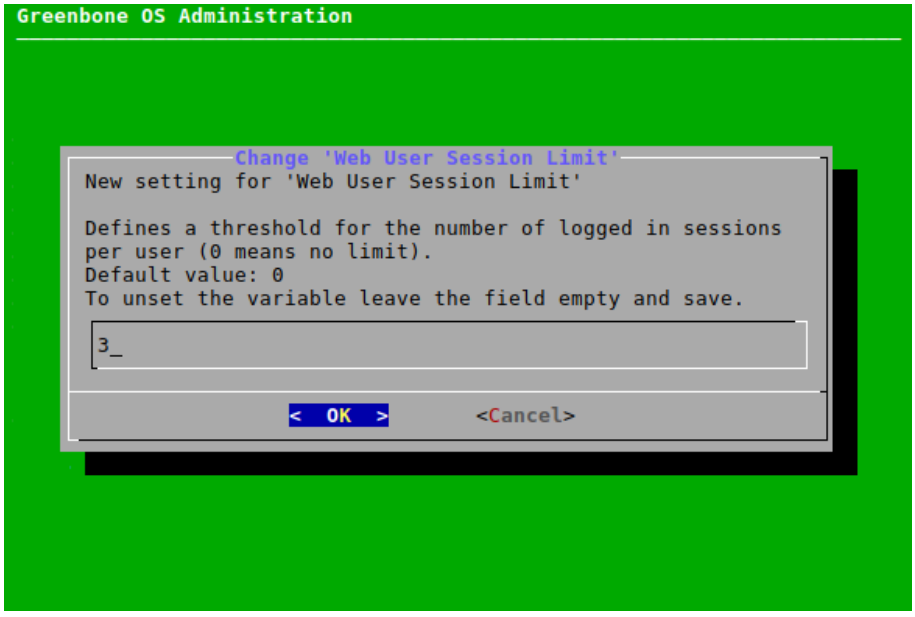


Abb. 7.10: Begrenzen der Anzahl von Websitzungen

6. `Enter` drücken.

7.2.1.8 Das Benutzerpasswort ändern

Das Passwort eines Web-Benutzers kann wie folgt geändert werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *Change Password* wählen und `Enter` drücken.
5. Web-Benutzer, dessen Passwort geändert werden soll, wählen und `Enter` drücken.
6. Neues Passwort zweimal eingeben und `Tab` drücken (siehe Abb. 7.11).

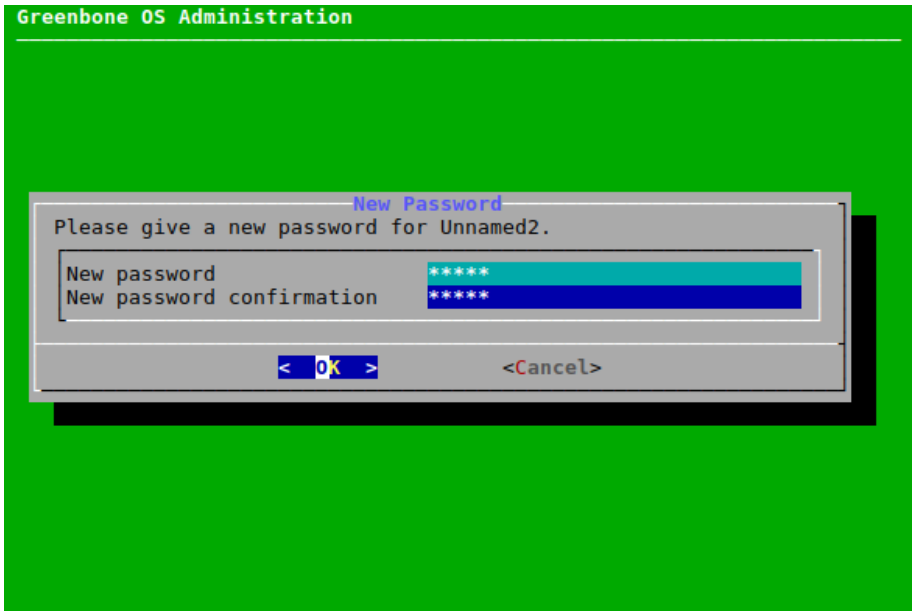


Abb. 7.11: Ändern des Benutzerpassworts

7. `Enter` drücken.

7.2.1.9 Die Passwortrichtlinie ändern

Die Anforderungen an Passwörter können wie folgt geändert werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *Password Policy* wählen und `Enter` drücken.

5. *Length* wählen und `Enter` drücken, um die Mindestlänge eines Passworts festzulegen.

   Bemerkung: Die Mindestlänge muss mindestens 10 Zeichen betragen.

   Username wählen und `Enter` drücken, um festzulegen, ob Benutzername und Passwort gleich sein dürfen.

   Complex wählen und `Enter` drücken, um festzulegen, ob ein Passwort mindestens einen Buchstaben, eine Zahl und ein Symbol enthalten muss.

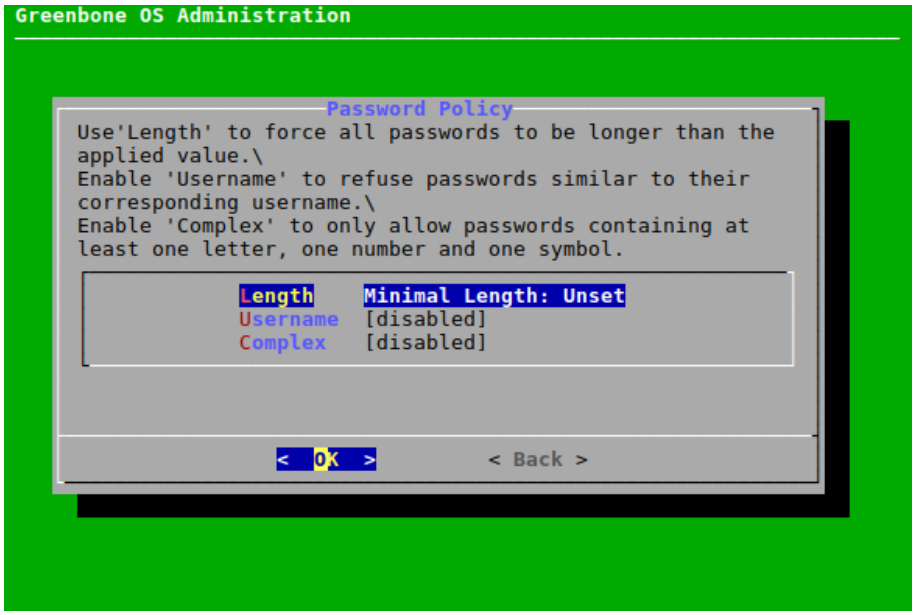


Abb. 7.12: Ändern der Passwortrichtlinie

7.2.1.10 Die Einstellungen für Datenobjekte konfigurieren

Scan-Konfigurationen, Compliance-Richtlinien, Berichtformate und Portlisten von Greenbone (im Folgenden als „Objekte“ bezeichnet) werden über den Feed verteilt. Diese Objekte müssen im Besitz eines Benutzers, des Feed Import Owners, sein.

Die Objekte werden während eines Feed-Updates heruntergeladen und aktualisiert, falls ein Feed Import Owner festgelegt wurde.

Nur der Feed Import Owner, ein Super-Administrator oder Nutzer, die entsprechende Berechtigungen erhalten haben, können Objekte löschen. Wenn die Objekte gelöscht werden, werden sie während des nächsten Feed-Updates erneut heruntergeladen.

Bemerkung: Falls die Objekte im Papierkorb verbleiben, gelten sie noch nicht als gelöscht und werden beim nächsten Feed-Update nicht erneut heruntergeladen.

Falls keine Objekte heruntergeladen werden sollen, darf kein Feed Import Owner festgelegt sein.

Der Feed Import Owner, ein Super-Administrator (Standardrolle) und ein Administrator (Standardrolle), welcher aktuell Berechtigungen für die Objekte hat, können anderen Nutzern auch zusätzliche Berechtigungen für die Objekte erteilen (siehe Kapitel *9.4.1.1* (Seite 195) oder *9.4.1.2* (Seite 196)). Normalerweise gilt dies nur für die Standardrollen. Benutzerdefinierte Rollen müssen zunächst manuell mit Berechtigungen ausgestattet werden.

Den Feed Import Owner ändern

Der Feed Import Owner wird bei der ersten Einrichtung der Appliance festgelegt (siehe Kapitel *6* (Seite 58) und *5* (Seite 28)). Der Feed Import Owner kann jedoch zu einem späteren Zeitpunkt geändert werden.

Bemerkung: Falls der Feed Import Owner geändert wird, werden die Objekte beim nächsten Import aus dem Feed in den Besitz des neuen Feed Import Owners übergehen. Der vorherige Feed Import Owner ist bis dahin weiterhin Eigentümer der Objekte.

Falls der vorherige Feed Import Owner die Objekte entfernt, werden sie während des Feed-Updates importiert und gehen in den Besitz des neuen Feed Import Owners über.

Der Feed Import Owner kann wie folgt geändert werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *Distributed Data* wählen und `Enter` drücken (siehe Abb. 7.13).

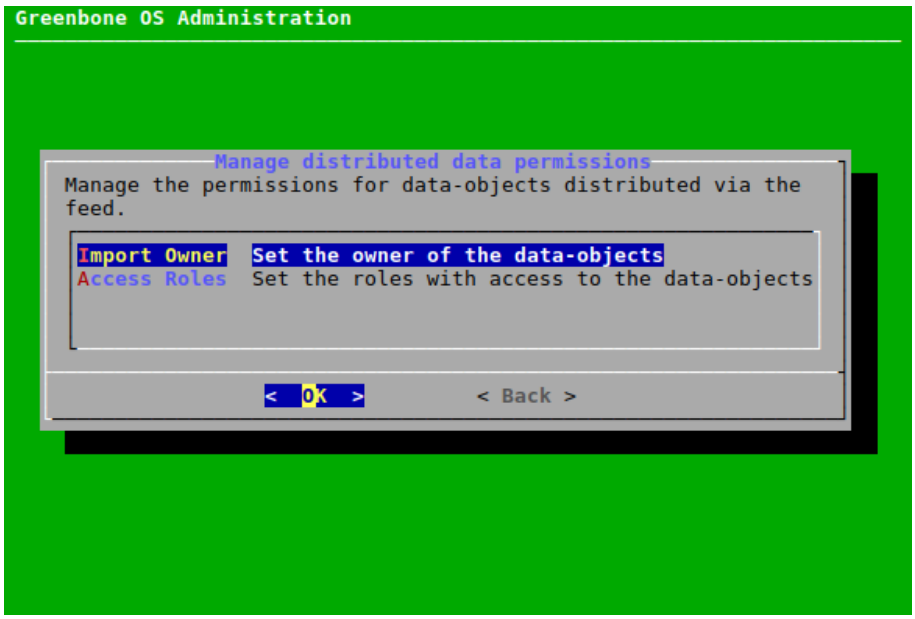


Abb. 7.13: Konfigurieren der Einstellungen für die Datenobjekte

5. *Import Owner* wählen und `Enter` drücken.
6. Nutzer, der Feed Import Owner sein soll, wählen und `Leertaste` drücken.
7. `Enter` drücken.

Bemerkung: Der Benutzer, der Feed Import Owner ist, kann nicht gelöscht werden (siehe Kapitel *7.2.1.6* (Seite 75)). Es muss ein anderer Feed Import Owner oder die Einstellung *(Unset)* ausgewählt werden.

Die Zugriffsrollen festlegen

Standardmäßig haben die Rollen *User*, *Admin* und *Super Admin* Lesezugriff auf die Objekte, d. h. sie können sie auf der Web-Oberfläche sehen und nutzen.

Jedoch können die Rollen, die Lesezugriff auf die Objekte haben sollen, wie folgt ausgewählt werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Users* wählen und `Enter` drücken.
4. *Distributed Data* wählen und `Enter` drücken.
5. *Access Roles* wählen und `Enter` drücken.
6. Rollen, die die Objekte sehen und benutzen können sollen, wählen und `Leertaste` drücken (siehe Abb. 7.14).

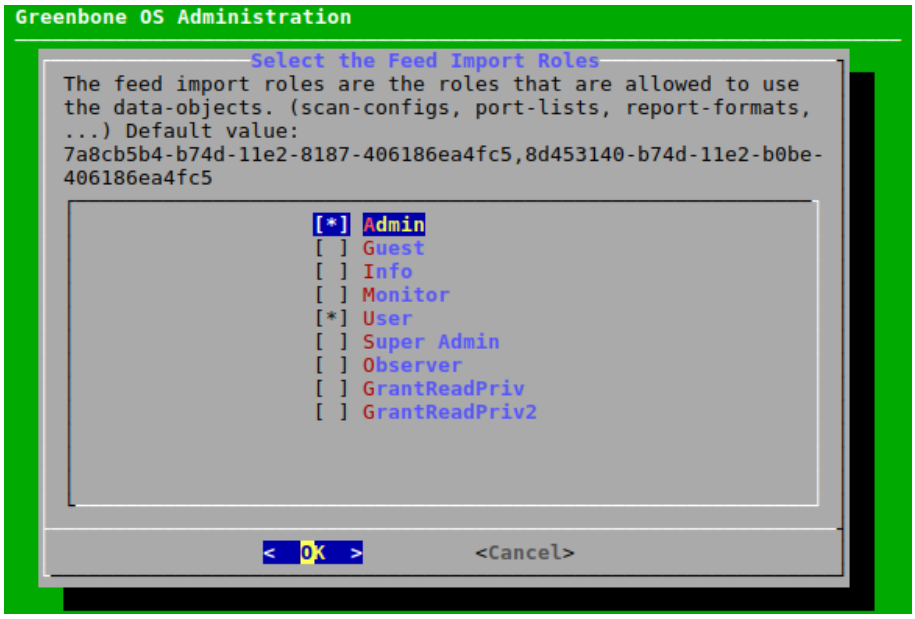


Abb. 7.14: Wählen der Rollen mit Lesezugriff auf die Objekte

7. `Enter` drücken.

7.2.2 Die Netzwerkeinstellungen konfigurieren

7.2.2.1 Den Netzwerkmodus auf *gnm* aktualisieren

Wenn der alte Netzwerkmodus noch aktiv ist, steht eine Menüoption zum Umschalten auf den neuen Netzwerkmodus *GOS Network Manager (gnm)* zur Verfügung. Wenn der Netzwerkmodus *gnm* bereits verwendet wird, wird die Option nicht angezeigt. Ein Zurückschalten in den alten Netzwerkmodus ist nicht möglich.

Der Netzwerkmodus kann wie folgt umgeschaltet werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.
3. *Switch Networking Mode* wählen und `Enter` drücken.

   → Eine Warnung empfiehlt, vor dem Umschalten des Netzwerkmodus eine Konsolenverbindung zur Appliance herzustellen (siehe Abb. 7.15).

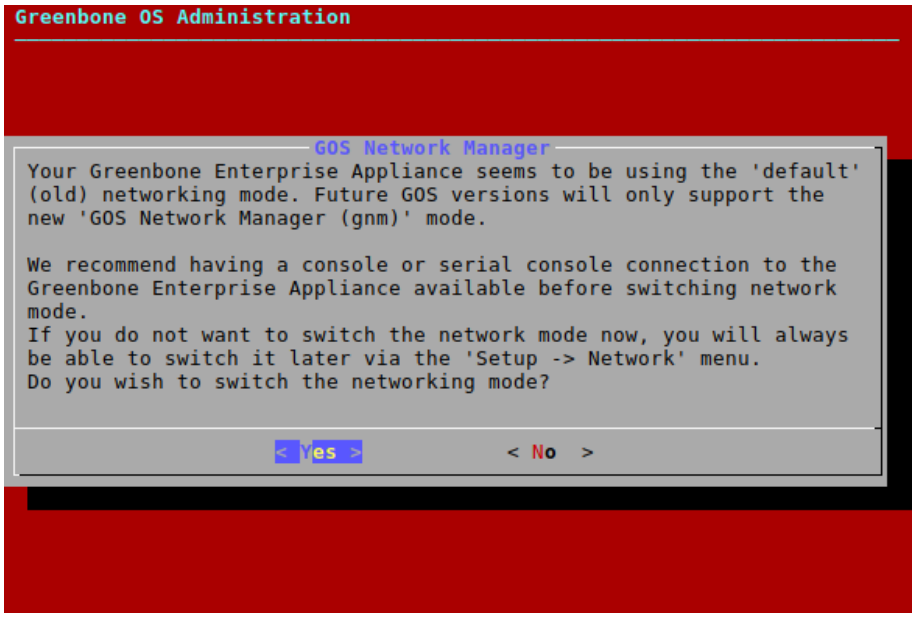


Abb. 7.15: Umschalten des Netzwerkmodus

4. *Yes* wählen und `Enter` drücken.

   → Wenn der Vorgang abgeschlossen ist, weist eine Meldung darauf hin, dass der Netzwerkmodus erfolgreich auf *gnm* aktualisiert wurde.

7.2.2.2 Allgemeine Informationen über Namensräume

Bei einigen Appliance-Modellen (Greenbone Enterprise 5400/6500 und Greenbone Enterprise 400/450/600/650) sind die Netzwerkschnittstellen in unterschiedlichen Namensräumen organisiert:

Management-Namensraum

- Dieser Namensraum enthält alle Schnittstellen, die für Managementtätigkeiten benötigt werden.
- Nur Schnittstellen im Management-Namensraum können Managementverkehr verarbeiten. Dies beinhaltet den Zugriff auf das GOS-Administrationsmenü, die Web-Oberfläche und den Greenbone Feed Server sowie die Konfiguration und den Betrieb von Master-Sensor-Setups.

Scan-Namensraum

- Dieser Namensraum enthält alle Schnittstellen, die für Schwachstellenscans benötigt werden.
- Schnittstellen im Scan-Namensraum verarbeiten nur Scanverkehr.

Standardmäßig befinden sich alle Schnittstellen im Management-Namensraum. Dies ermöglicht sowohl Management- als auch Scanverkehr über alle Schnittstellen. Sobald mindestens eine Schnittstelle im Scan-Namensraum ist, tritt die Namensraumtrennung in Kraft.

Die Namensräume werden getrennt, um nur die Schnittstellen im Scan-Namensraum mit vom Internet aus zugänglichen Netzwerken zu verbinden. Auf diese Weise können Angriffe aus dem Internet die Management-Schnittstellen der Appliance nicht erreichen.

Tipp: Die Trennung der Namensräume wird empfohlen.

7.2.2.3 Eine Schnittstelle in einen anderen Namensraum verschieben

Schnittstellen können wie folgt in einen anderen Namensraum verschoben werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.
3. *Configure Namespaces* wählen und `Enter` drücken.
4. `Enter` drücken.

Bemerkung: Schnittstellen, die sich derzeit im Scan-Namensraum befinden, sind mit * gekennzeichnet (siehe Abb. 7.16).

Schnittstellen, die sich derzeit im Management-Namensraum befinden, sind entsprechend gekennzeichnet.

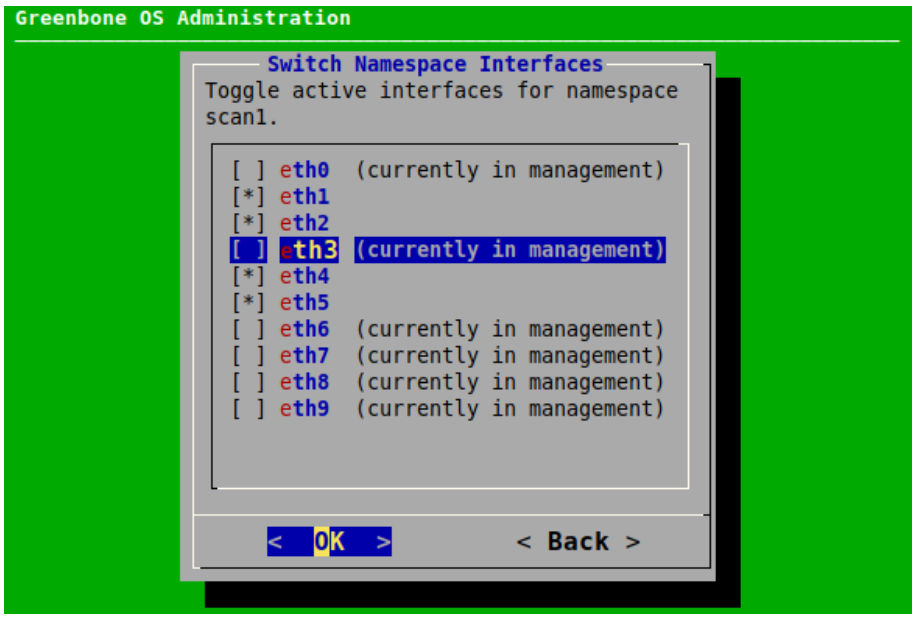


Abb. 7.16: Verschieben von Schnittstellen in einen anderen Namensraum

5. Schnittstelle, die verschoben werden soll, wählen und `Leertaste` drücken.

   Bemerkung: Es dürfen nicht alle Schnittstellen in den Scan-Namensraum verschoben werden, da sonst die Appliance nicht mehr erreichbar ist.

6. `Enter` drücken.

7.2.2.4 Netzwerkschnittstellen konfigurieren

Bemerkung: Mindestens eine Netzwerkschnittstelle muss für den Zugriff auf die Appliance über das Netzwerk konfiguriert sein. Normalerweise wird die erste Netzwerkschnittstelle *eth0* dafür genutzt. Der Administrator muss diese Netzwerkschnittstelle konfigurieren und die Appliance mit dem Netzwerk verbinden.

Auf allen virtuellen Appliances ist die erste Netzwerkschnittstelle über DHCP mit IPv4 vorkonfiguriert.

Netzwerkschnittstellen können wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.
3. Namensraum, in dem sich die gewünschte Schnittstelle befindet, wählen und `Enter` drücken.
4. *Interfaces* wählen und `Enter` drücken.
5. Gewünschte Schnittstelle wählen und `Enter` drücken.

   Bemerkung: Falls es in diesem Namensraum nur eine Schnittstelle gibt, wird die Konfiguration dieser Schnittstelle direkt geöffnet.

   → Die Schnittstelle kann konfiguriert werden (siehe Abb. 7.17).

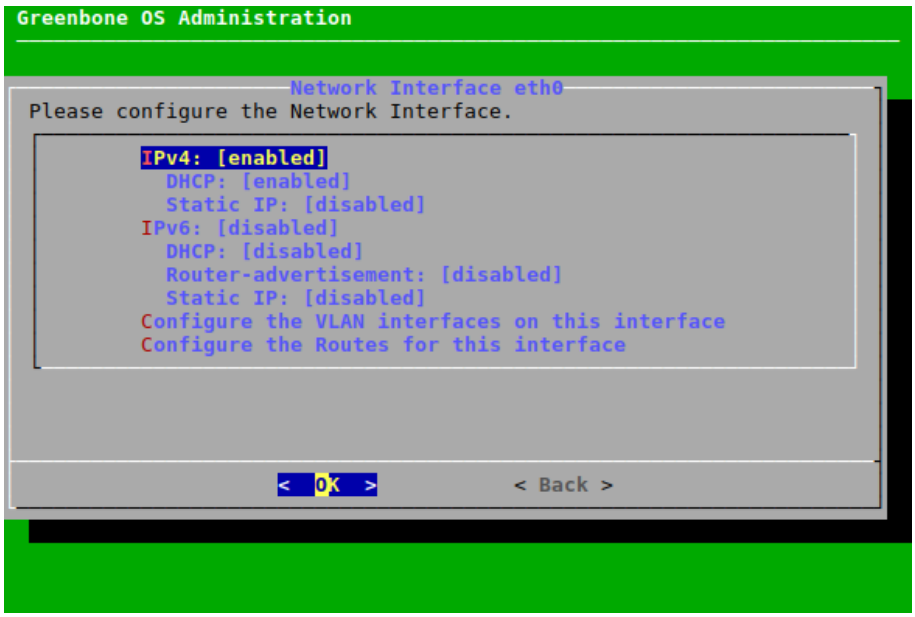


Abb. 7.17: Konfigurieren der Netzwerkschnittstelle

Eine statische IP-Adresse festlegen

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *Static IP* (für IPv4 oder IPv6) wählen und `Enter` drücken.
3. `dhcp` aus dem Eingabefeld löschen und mit korrekter IP-Adresse, einschließlich Präfixlänge, ersetzen (siehe Abb. 7.18).

Bemerkung: Die statische IP-Adresse kann deaktiviert werden, indem das Eingabefeld leer gelassen wird.

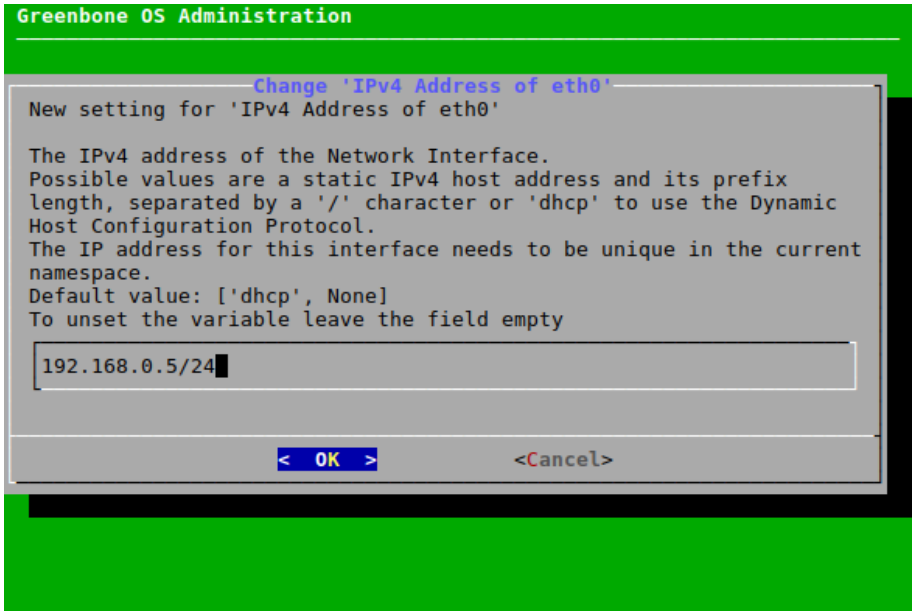


Abb. 7.18: Eingeben einer statischen IP-Adresse

4. `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
5. `Enter` drücken, um die Meldung zu schließen.

Eine Netzwerkschnittstelle so konfigurieren, dass DHCP genutzt wird

---

Bemerkung: Bei der Verwendung von DHCP überträgt die Appliance nicht die MAC-Adresse, sondern eine DHCP Unique ID (DUID). Während dies bei modernen DHCP-Servern nicht zu Schwierigkeiten führen sollte, sind einige ältere DHCP-Server (z. B. Windows Server 2012) möglicherweise nicht in der Lage, diese zu verarbeiten.

Eine mögliche Lösung ist die Angabe der DUID anstelle der MAC-Adresse auf dem DHCP-Server. Alternativ kann auch eine statische IP-Adresse auf der Appliance verwendet werden.

Eine Netzwerkschnittstelle kann wie folgt konfiguriert werden, sodass DHCP genutzt wird:

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *DHCP* (für IPv4 oder IPv6) wählen und `Enter` drücken.

Die Maximum Transmission Unit (MTU) konfigurieren

Bemerkung: Die Konfiguration der MTU ist nur möglich, falls eine statische IP-Adresse konfiguriert ist.

Die MTU kann wie folgt festgelegt werden:

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *MTU* (für IPv4 oder IPv6) wählen und `Enter` drücken.
3. MTU in das Eingabefeld eingeben.

   Bemerkung: Falls das Eingabefeld leer gelassen wird, wird der Standardwert eingestellt.

4. `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
5. `Enter` drücken, um die Meldung zu schließen.

Das Router-Advertisement für IPv6 nutzen

Falls die Konfiguration von IP-Adressen und eines globalen Gateways für IPv6 automatisch via SLAAC (Stateless Address Autoconfiguration) ablaufen sollen, kann das Router-Advertisement wie folgt aktiviert werden:

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *Router-advertisement* wählen und `Enter` drücken.

VLANs konfigurieren

Bemerkung: VLAN-Schnittstellen werden derzeit auf virtuellen Appliances nicht unterstützt. Wenn der Hypervisor virtuelle Switches unterstützt, können diese verwendet werden, um die Funktionalität zu realisieren.

Ein neues VLAN erstellen

Eine neue VLAN-Subschnittstellen kann wie folgt erstellt werden:

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *Configure the VLAN interfaces on this interface* wählen und `Enter` drücken.
3. *Configure a new VLAN interface* wählen und `Enter` drücken.
4. VLAN ID in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.19).

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
5. `Enter` drücken, um die Meldung zu schließen.

   → Die neue Schnittstellen kann mithilfe von IPv4 und IPv6 konfiguriert werden (siehe Abb. 7.20).

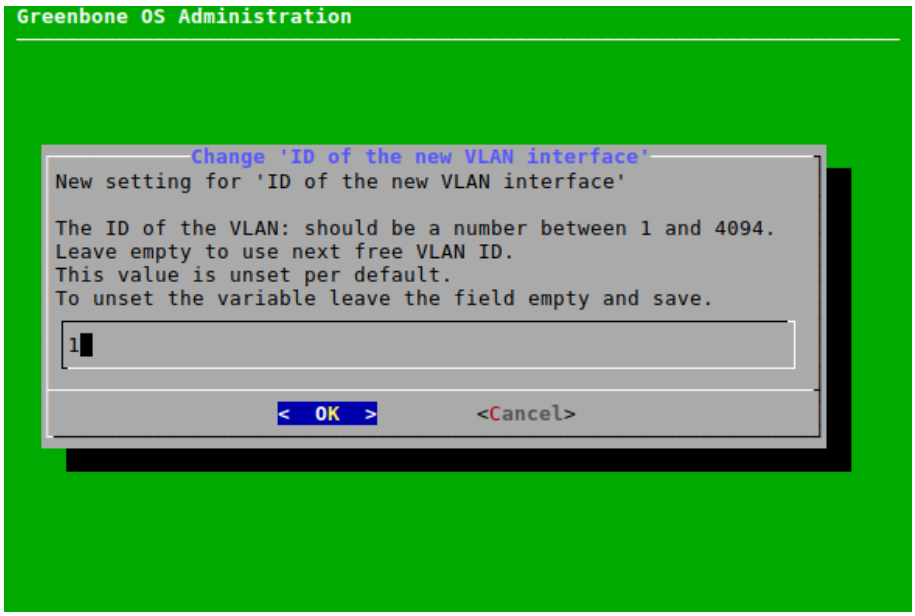


Abb. 7.19: Erstellen einer neuen VLAN-Subschnittstelle

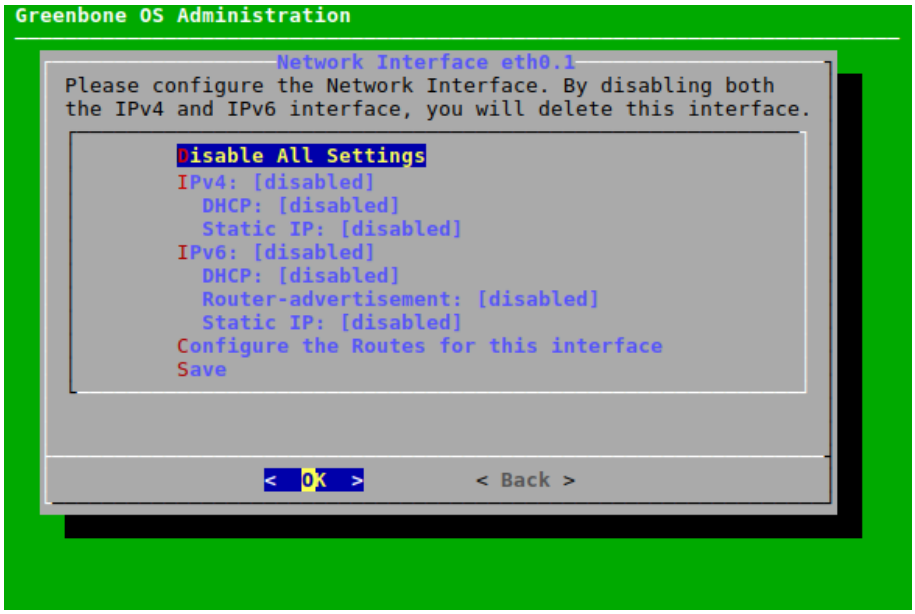


Abb. 7.20: Konfigurieren der VLAN-Subschnittstelle

Ein VLAN konfigurieren

Eine erstellte Subschnittstelle kann wie folgt konfiguriert werden:

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *Configure the VLAN interfaces on this interface* wählen und `Enter` drücken.
3. *Configure the VLAN interface . . .* für die gewünschte Subschnittstelle wählen.
4. Subschnittstelle wie in den Unterkapiteln von Kapitel *7.2.2.4* (Seite 83) beschrieben konfigurieren.

Bemerkung: Das VLAN kann durch Wählen von *Disable All Settings* und Drücken von `Enter` gelöscht werden.

Die Routen für eine Schnittstelle konfigurieren

Eine neue Route hinzufügen

Eine neue Route für eine Schnittstelle kann wie folgt konfiguriert werden:

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *Configure the Routes for this interface* wählen und `Enter` drücken.
3. *Configure IPv4 Routes* oder *Configure IPv6 Routes* wählen und `Enter` drücken (siehe Abb. 7.21).

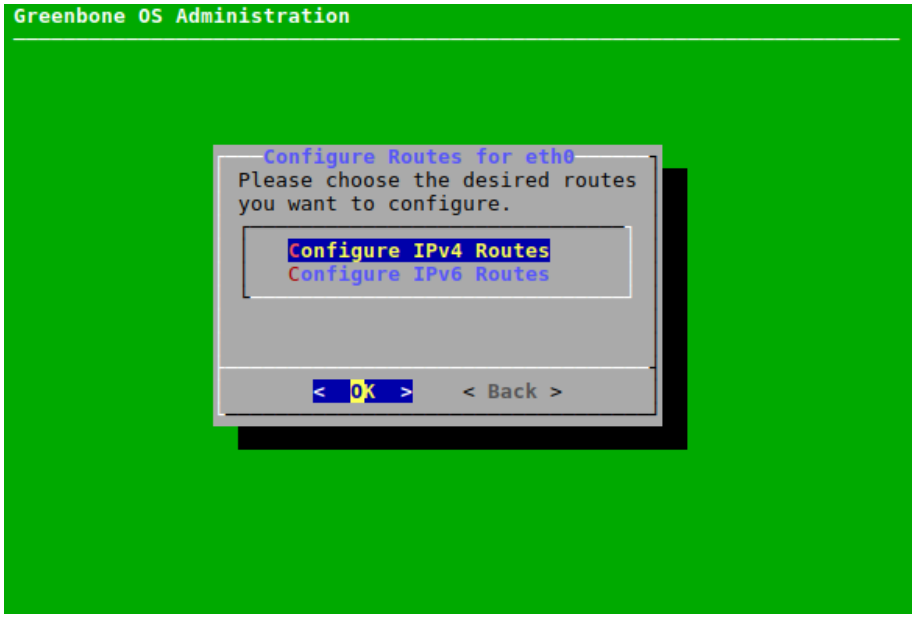


Abb. 7.21: Konfigurieren der Routen für eine Schnittstelle

4. *Add a new route* wählen und `Enter` drücken.
5. Zielnetzwerk und next hop in die Eingabefelder eingeben, *OK* wählen und `Enter` drücken.

Eine Route konfigurieren

Alle erstellten Routen können wie folgt konfiguriert werden:

1. Gewünschte Schnittstelle wählen (siehe Kapitel *7.2.2.4* (Seite 83)).
2. *Configure the Routes for this interface* wählen und `Enter` drücken.
3. *Configure IPv4 Routes* oder *Configure IPv6 Routes* wählen und `Enter` drücken.
4. Gewünschte Route wählen und `Enter` drücken.
5. Route bearbeiten, *OK* wählen und `Enter` drücken.

7.2.2.5 Den DNS-Server konfigurieren

Um den Feed und Updates zu erhalten, benötigt die Appliance einen erreichbaren und funktionierenden DNS-Server (Domain Name System) für die Namensauflösung. Diese Einstellung wird nicht benötigt, falls die Appliance einen Proxy zum Herunterladen des Feeds und der Updates verwendet.

Falls DHCP für die Konfiguration der Netzwerkschnittstellen genutzt wird, werden die vom DHCP-Protokoll bereitgestellten DNS-Server genutzt.

Die Appliance unterstützt bis zu drei DNS-Server. Mindestens ein DNS-Server wird benötigt. Zusätzliche Server werden nur bei einem Ausfall des ersten Servers genutzt.

Der DNS-Server kann wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.
3. *Namespace: Management* wählen und `Enter` drücken.
4. *DNS* wählen und `Enter` drücken.
5. Gewünschten DNS-Server wählen und `Enter` drücken.
6. IP-Adresse, die als DNS-Server genutzt wird, in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.22).

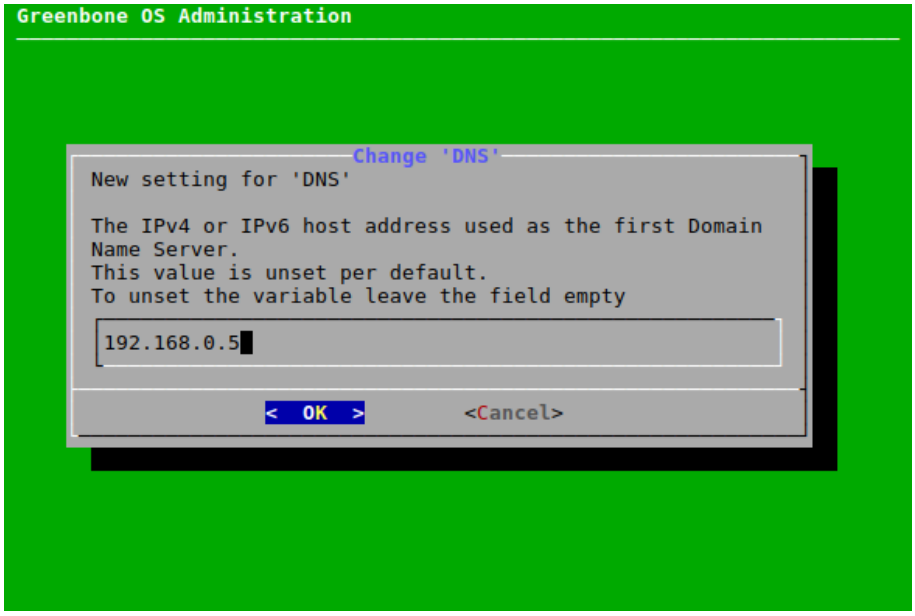


Abb. 7.22: Konfiguration des DNS-Servers

→ Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

7. `Enter` drücken, um die Meldung zu schließen.

Bemerkung: Ob der DNS-Server erreicht wird und funktioniert, kann ermittelt werden, indem ein Self-Check durchgeführt wird (siehe Kapitel *7.3.1* (Seite 138)).

7.2.2.6 Das globale Gateway konfigurieren

Das globale Gateway wird oft das Standard-Gateway genannt.

Es kann automatisch über DHCP oder Router-Advertisement bezogen werden.

- Falls DHCP für das Zuweisen von IP-Adressen genutzt wird, wird das globale Gateway über DHCP bestimmt, sofern es nicht explizit festgelegt wurde.
- Falls SLAAC (Stateless Address Autoconfiguration) bei IPv6 verwendet werden soll, muss das Router-Advertisement aktiviert werden (siehe Kapitel *7.2.2.4.4* (Seite 85)).

Wenn die Appliance jedoch so konfiguriert ist, dass sie ausschließlich statische IP-Adressen verwendet und der Zugriff auf andere Netzwerke gewünscht wird, muss das Gateway manuell konfiguriert werden. Für IPv4 und IPv6 sind getrennte Optionen verfügbar.

Das globale Gateway kann wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.

   Bemerkung: Wenn die Appliance über Namensräume verfügt (siehe Kapitel *7.2.2.2* (Seite 81)), muss zuerst der gewünschte Namensraum gewählt werden.

   Wenn die Appliance keine Namensräume hat, mit Schritt 4 fortfahren.

   ---

3. Namensraum, für den das globale Gateway konfiguriert werden soll, wählen und `Enter` drücken.
4. *Global Gateway* für IPv4 oder *Global Gateway (IPv6)* für IPv6 wählen und `Enter` drücken.
5. Gewünschte Schnittstellen wählen und `Enter` drücken (siehe Abb. 7.23).
6. IP-Adresse, die als globales Gateway genutzt wird, in das Eingabefeld eingeben und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

7. `Enter` drücken, um die Meldung zu schließen.

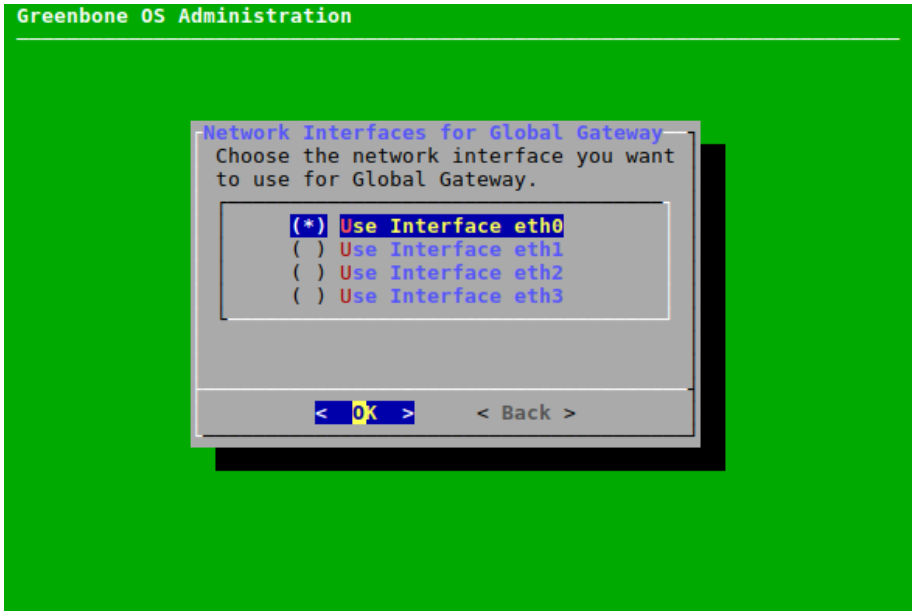


Abb. 7.23: Konfigurieren des globalen Gateways

7.2.2.7 Den Hostnamen und den Domainnamen festlegen

Nach dem Ausliefern der Appliance durch Greenbone oder nach einem Factory-Reset sind ein Standard-Hostname und ein Standard-Domainname konfiguriert. Die Konfiguration eines korrekten Fully Qualified Domain Name (FQDN) kann je nach der Umgebung, in der die Appliance eingesetzt wird, erforderlich sein und wird generell empfohlen.

Mit der Hostname-Option wird der kurze Hostname konfiguriert, mit der Domainname-Option der Domainname einschließlich seines Suffixes. Die beiden Werte zusammen bilden den FQDN. Die Standardwerte sind:

- Hostname: gsm
- Domainname: gbuser.net

Der aktuell konfigurierte Domainname wird immer als Suchdomain verwendet. DHCP-Server können Suchdomains hinzufügen, wenn DHCP für mindestens eine Netzwerkschnittstelle der Appliance konfiguriert ist und wenn der DHCP-Server entsprechend konfiguriert ist. GOS bietet keine zusätzlichen Konfigurationsoptionen, um weitere benutzerdefinierte Suchdomains hinzuzufügen.

Der Hostname und der Domainname können wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.
3. *Namespace: Management* wählen und `Enter` drücken.
4. *Hostname* oder *Domainname* wählen und `Enter` drücken.
5. Hostnamen oder Domainnamen in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.24).

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
6. `Enter` drücken, um die Meldung zu schließen.

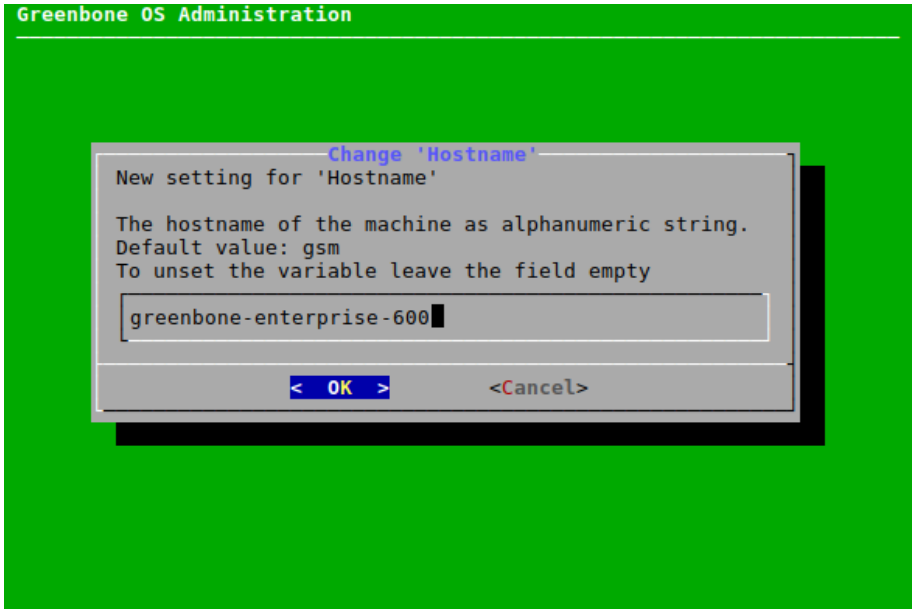


Abb. 7.24: Festlegen des Hostnamens/Domainnamens

7.2.2.8 Den Managementzugriff beschränken

Die IP-Adresse, unter der die Managementschnittstelle verfügbar ist, kann festgelegt werden.

Jeder administrative Zugriff (SSH, HTTPS, GMP) wird auf die entsprechende Schnittstelle beschränkt und ist nicht auf anderen Schnittstellen verfügbar.

Bemerkung: Diese Funktionalität überschneidet sich mit der Namensraumtrennung (siehe Kapitel *7.2.2* (Seite 81)). Die Namensraumtrennung wird empfohlen.

Falls keine IP-Adresse festgelegt wird, ist die Managementschnittstelle auf allen IP-Adressen im Management-Namensraum verfügbar.

Die IP-Adresse für die Managementschnittstelle kann wie folgt festgelegt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.
3. *Namespace: Management* wählen und `Enter` drücken.
4. *Management IP (v4)* oder *Management IP (v6)* wählen und `Enter` drücken.

5. IP-Adresse für die Managementschnittstelle in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.25).

Bemerkung: Die IP-Adresse muss die IP-Adresse einer der Schnittstellen im Management-Namensraum sein. Falls eine andere IP-Adresse festgelegt wird, ist die Managementschnittstelle nicht verfügbar.

Es kann entweder die IP-Adresse oder der Name der Schnittstelle (z. B. `eth0`) eingegeben werden.

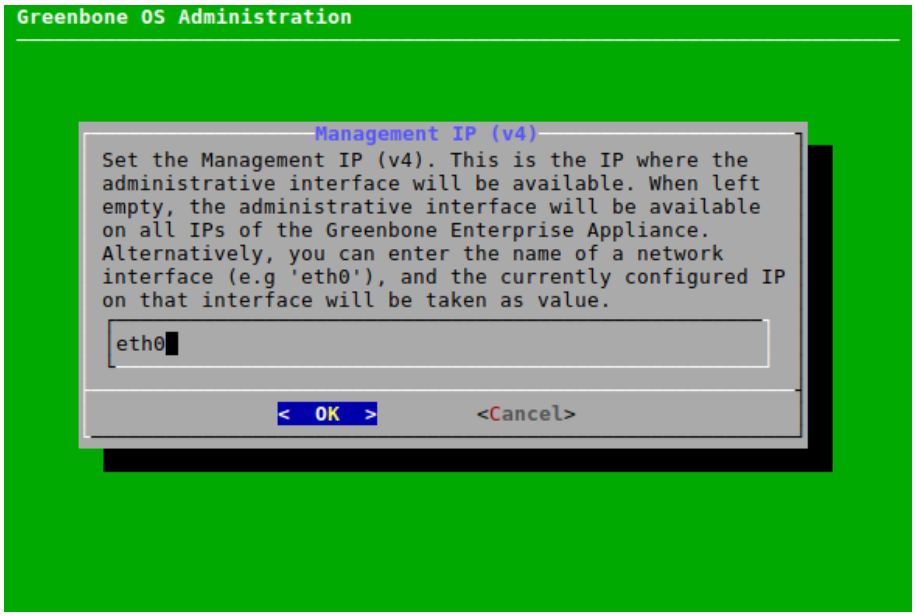


Abb. 7.25: Beschränken des Managementzugriffs

7.2.2.9 Die MAC- und die IP-Adressen und die Netzwerkrouten anzeigen

In einer einfachen Übersicht können die verwendeten MAC-Adressen, die aktuell konfigurierten IP-Adressen und die Netzwerkrouten der Appliance angezeigt werden.

Bemerkung: Dies unterstützt nicht die Konfiguration von MAC-Adressen.

Die MAC-Adressen, IP-Adressen oder Netzwerkrouten können wie folgt angezeigt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Network* wählen und `Enter` drücken.
3. Namensraum, für den die IP-Adressen, MAC-Adressen oder Netzwerkrouten angezeigt werden sollen, wählen und `Enter` drücken.

4. *MAC*, *IP* oder *Routes* wählen und `Enter` drücken.

   → Die MAC-/IP-Adressen oder Netzwerkrouten des gewählten Namensraums werden angezeigt (siehe Abb. 7.26).

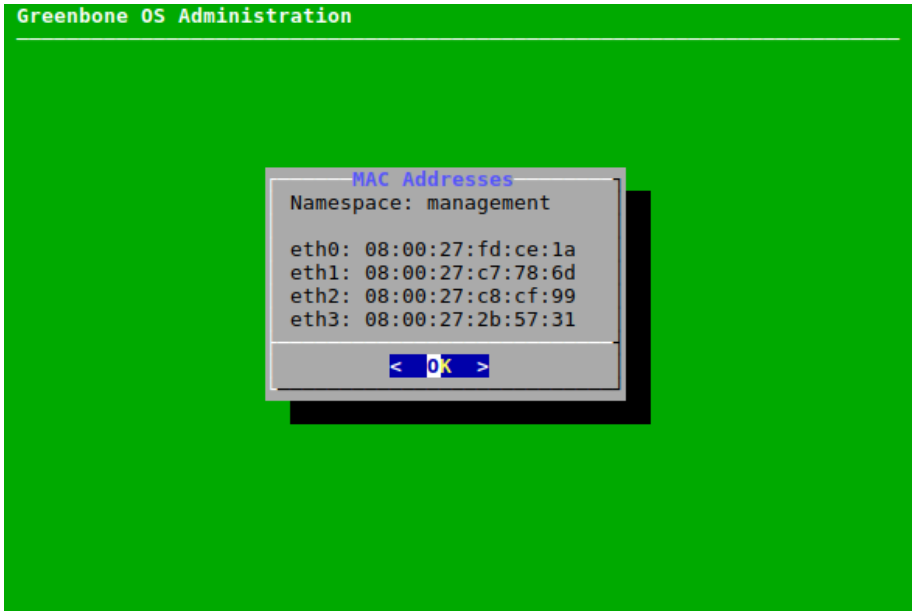


Abb. 7.26: Anzeigen der MAC-/IP-Adressen oder Netzwerkrouten

7.2.3 Eine Virtual-Private-Network-Verbindung (VPN-Verbindung) konfigurieren

OpenVPN ist in GOS integriert. Die VPN-Funktion ermöglicht das Scannen von Zielen, die über den VPN-Tunnel erreichbar sind, hat aber keine Auswirkungen auf andere Ziele, Netzwerkeinstellungen oder Master-Sensor-Verbindungen.

Bemerkung: Das Scannen durch einen VPN-Tunnel ist nur für die Appliance-Modelle Greenbone Enterprise DECA/TERA/PETA/EXA verfügbar (siehe Kapitel *3* (Seite 20)).

Um Scans durch einen VPN-Tunnel durchzuführen, muss eine VPN-Verbindung aufgebaut werden. Der VPN-Tunnel wird immer applianceseitig initiiert.

Zur Authentifizierung der Appliance im VPN wird eine PKCS#12-Datei mit den folgenden Anforderungen benötigt:

- Die PKCS#12-Datei muss die erforderlichen Dateien für das Zertifikat und den privaten Schlüssel enthalten.
- Die PKCS#12-Datei kann eine Datei für die Zertifizierungsstelle (CA) enthalten. Falls sie keine enthält, muss die CA-Datei separat importiert werden.
- Die PKCS#12-Datei kann passwortgeschützt sein oder nicht.
- Passwortgeschützte private Schlüsseldateien innerhalb der PKCS#12-Datei werden nicht unterstützt.

7.2.3.1 Eine VPN-Verbindung einrichten

Bemerkung: Es kann immer nur eine VPN-Verbindung zur gleichen Zeit eingerichtet werden.

Eine neue VPN-Verbindung kann wie folgt eingerichtet werden:

1. *Setup* wählen und `Enter` drücken.
2. *VPN* wählen und `Enter` drücken.
3. *Add a new VPN* wählen und `Enter` drücken (siehe Abb. 7.27).

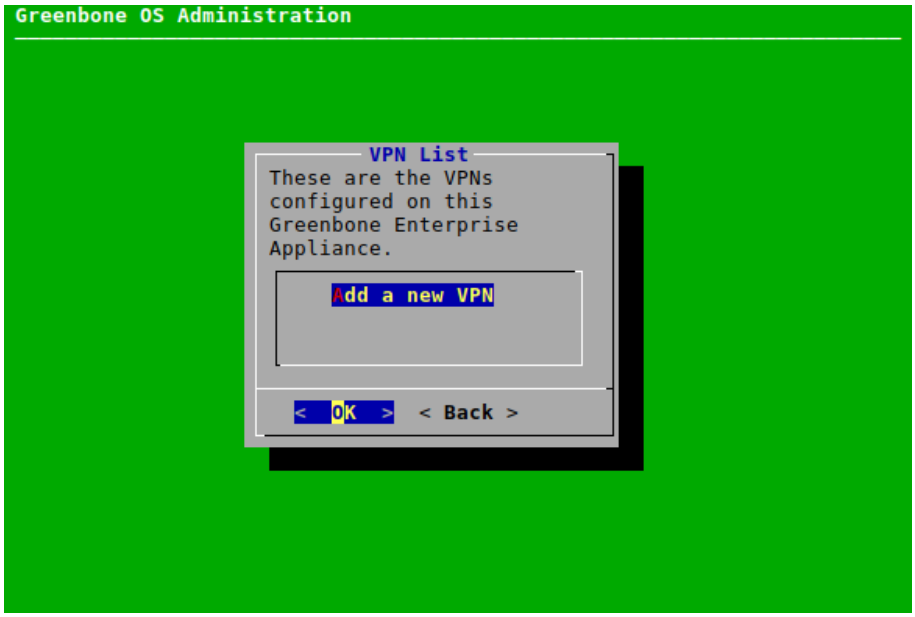


Abb. 7.27: Eine VPN-Verbindung hinzufügen

4. IP-Adresse des VPNs in das Eingabefeld eingeben und `Enter` drücken.
5. Webbrowser öffnen und angezeigte URL eingeben.
6. Auf *Browse...* klicken, die PKCS#12-Datei wählen und auf *Upload* klicken.
7. Falls ein Exportpasswort zum Schutz des PKCS#12-Containers verwendet wurde, Passwort eingeben und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die PKCS#12-Datei erfolgreich extrahiert wurde.
8. `Enter` drücken.

   Bemerkung: Falls die PKCS#12-Datei keine CA-Datei enthält, muss die CA-Datei separat importiert werden.

   Falls die PKCS#12-Datei bereits eine CA-Datei enthält, kann zwar auch eine CA-Datei separat importiert werden, dies überschreibt jedoch die CA-Datei aus der PKCS#12-Datei.
9. *Certificate Authority* wählen und `Enter` drücken.
10. Webbrowser öffnen und angezeigte URL eingeben.
11. Auf *Browse...* klicken, die CA-Datei wählen und auf *Upload* klicken.

    → Eine Meldung weist darauf hin, dass die CA-Datei erfolgreich importiert wurde.

12. `Enter` drücken.

    → Die VPN-Verbindung wird aufgebaut und die über das VPN erreichbaren Ziele können gescannt werden (siehe Kapitel *10.2* (Seite 213)).

7.2.3.2 Eine VPN-Verbindung bearbeiten oder löschen

Die VPN-Verbindung kann wie folgt bearbeitet werden:

1. *Setup* wählen und `Enter` drücken.
2. *VPN* wählen und `Enter` drücken.

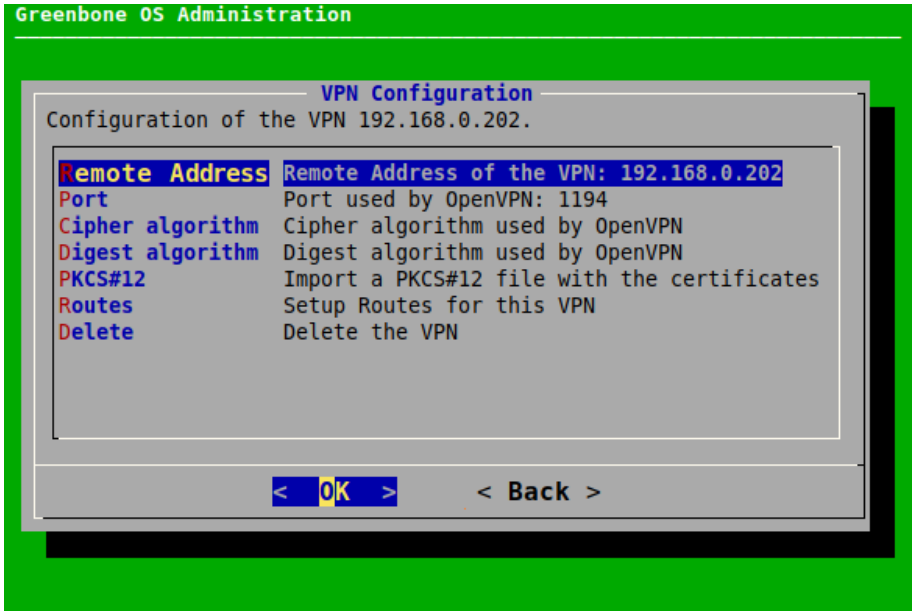


Abb. 7.28: Bearbeiten oder Löschen einer VPN-Verbindung

Die folgenden Aktionen sind verfügbar:

Remote Address Die IP-Adresse des VPN festlegen.

Port Den Port festlegen, der von OpenVPN verwendet wird. Standardmäßig ist der Port 1194.

Cipher algorithm Den Cipher-Algorithmus wählen. Standardmäßig wird die Voreinstellung von OpenVPN verwendet.

Digest algorithm Den Digest-Algorithmus wählen. Standardmäßig wird die Voreinstellung von OpenVPN verwendet.

PKCS#12 Die PKCS#12-Datei ersetzen.

Routes Eine Route für die VPN-Verbindung hinzufügen. Ziel-IP-Adresse, Netzmaske und Ziel-Gateway müssen definiert werden.

Bemerkung: Es kann nur eine Route für die VPN-Verbindung eingerichtet werden.

Delete Die VPN-Verbindung löschen.

7.2.4 Dienste konfigurieren

Um remote auf die Appliance zuzugreifen, sind viele Schnittstellen verfügbar:

- HTTPS, siehe Kapitel *7.2.4.1* (Seite 96)
- Greenbone Management Protocol (GMP), siehe Kapitel *15* (Seite 370)
- Open Scanner Protocol (OSP), siehe Kapitel *7.2.4.3* (Seite 106)
- SSH, siehe Kapitel *7.2.4.4* (Seite 107)
- SNMP, siehe Kapitel *7.2.4.5* (Seite 110)

7.2.4.1 HTTPS konfigurieren

Die Web-Oberfläche ist die übliche Option zum Erstellen, Ausführen und Analysieren von Schwachstellenscans. Sie ist standardmäßig aktiviert und kann nicht deaktiviert werden.

Für die Nutzung der Web-Oberfläche ist ein HTTPS-Zertifikat erforderlich.

Die Web-Oberfläche ist mit den von Greenbone bereitgestellten Werkseinstellungen sicher konfiguriert, aber die Sicherheit kann mit den in diesem Kapitel beschriebenen Konfigurationsoptionen weiter erhöht werden.

Das Timeout der Web-Oberfläche konfigurieren

Falls für eine bestimmte Zeit keine Aktion auf der Web-Oberfläche durchgeführt wird, wird der Benutzer automatisch ausgeloggt. Der Timeout-Wert kann wie folgt eingestellt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Timeout* wählen und `Enter` drücken.
5. Gewünschten Timeout-Wert in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.29).

   Bemerkung: Der Wert kann zwischen 1 und 1440 Minuten (1 Tag) liegen. Der Standardwert ist 15 Minuten.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
6. `Enter` drücken, um die Meldung zu schließen.

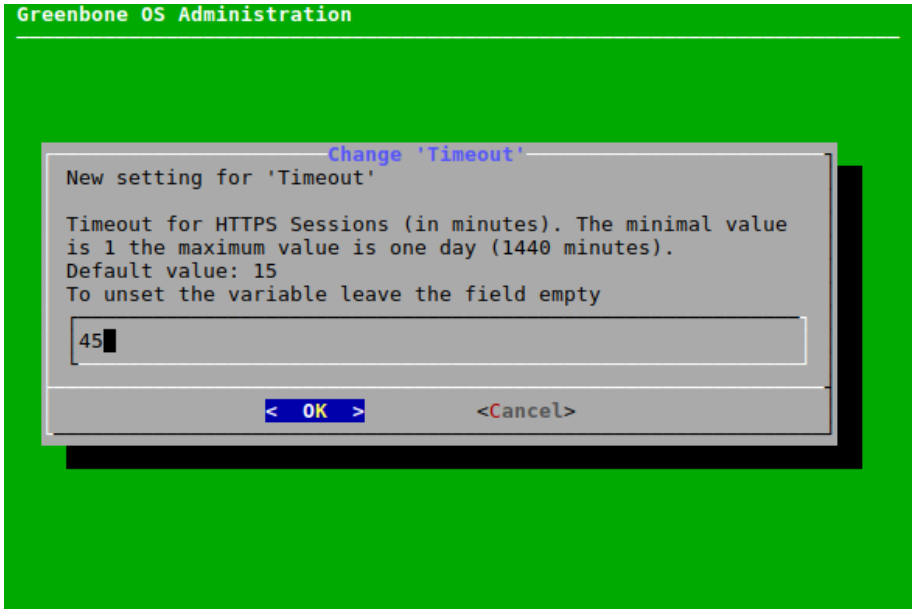


Abb. 7.29: Festlegen des Timeout-Werts

Die TLS-Protokolle konfigurieren

Die TLS-Protokolle für die HTTPS-Verbindung der Web-Oberfläche können wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Protocols* wählen und `Enter` drücken.
5. Gewünschte Protokollversion wählen und `Leertaste` drücken (siehe Abb. 7.30).

   Bemerkung: Standardmäßig sind beide Versionen ausgewählt.

   Falls *TLSv1.2* ausgewählt ist (entweder allein oder in Kombination mit Version 1.3), können die Ciphers für die HTTPS-Verbindung konfiguriert werden (siehe Kapitel *7.2.4.1.3* (Seite 98)).

   Falls nur *TLSv1.3* ausgewählt ist, wird der Standardwert für `-ciphersuites val` von OpenSSL[11] für die Cipher-Suiten verwendet. In diesem Fall ist der Menüpunkt zur Konfiguration der Ciphers nicht verfügbar.

6. *OK* wählen und `Enter` drücken.

[11] https://www.openssl.org/docs/man1.1.1/man1/ciphers.html

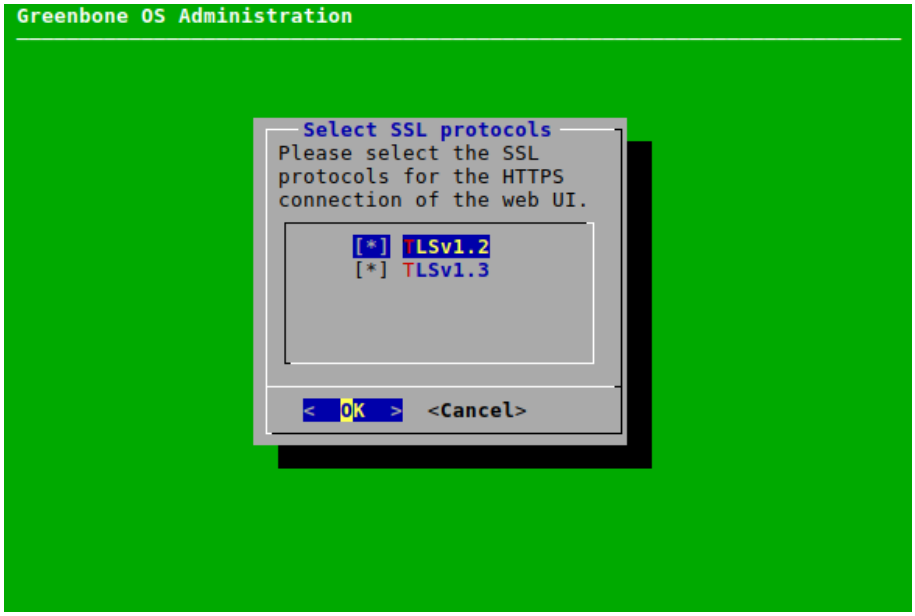


Abb. 7.30: Konfigurieren der Protokolle für die HTTPS-Verbindung

Die Ciphers konfigurieren

Falls TLS-Version 1.2 für die HTTPS-Verbindung der Web-Oberfläche verwendet wird (entweder allein oder in Kombination mit Version 1.3, siehe Kapitel *7.2.4.1.2* (Seite 97)), können die HTTPS-Ciphers konfiguriert werden, um die Sicherheit der Web-Oberfläche weiter zu erhöhen.

Bemerkung: Die derzeitige Einstellung lässt nur sichere Ciphers mit einer Schlüssellänge von mindestens 128 Bit zu, wobei die von SSLv3 und TLSv1.0 verwendeten Cipher-Suiten ausdrücklich nicht zugelassen werden.

Für TLSv1.1 gibt es keine Ciphers.

Der HTTPS-Ciphers können wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Ciphers* wählen und `Enter` drücken.
5. Gewünschten Wert in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.31).

   Bemerkung: Die Zeichenkette, die zur Definition der Ciphers verwendet wird, wird von OpenSSL validiert und muss der Syntax einer OpenSSL-Cipherliste entsprechen.

   Weitere Informationen zur Syntax sind hier[12] zu finden.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
6. `Enter` drücken, um die Meldung zu schließen.

[12] https://www.openssl.org/docs/man1.1.1/man1/ciphers.html

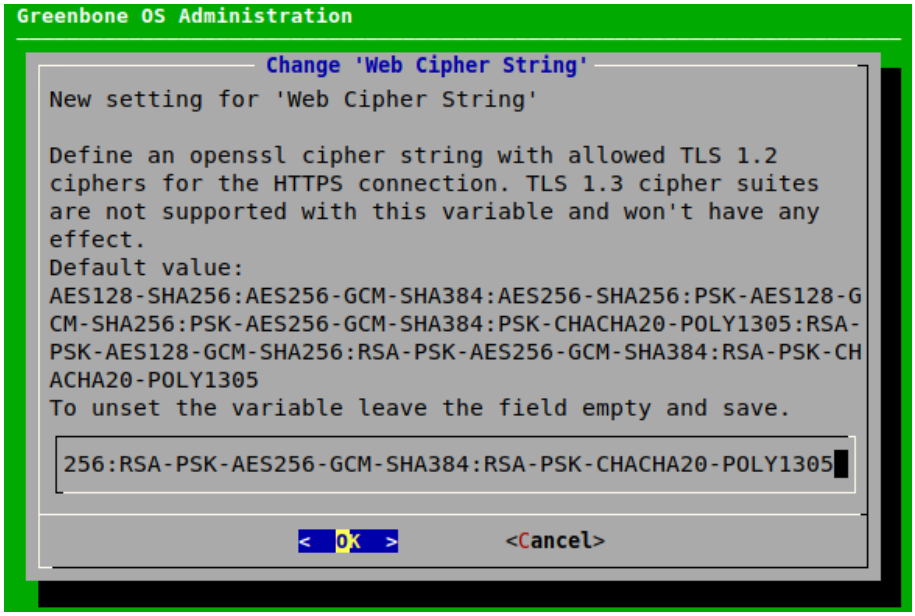


Abb. 7.31: Konfigurieren der Ciphers

Die Diffie-Hellman-Parameter (DH-Parameter) konfigurieren

DH-Parameter werden vom Webserver für den Aufbau von TLS-Verbindungen genutzt. Um die Sicherheit der Web-Oberfläche weiter zu erhöhen, können wie folgt neue DH-Parameter generiert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *DH Parameters* wählen und `Enter` drücken.
5. Gewünschte Schlüsselgröße wählen und `Leertaste` drücken.
6. `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Generierung im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

HTTP STS konfigurieren

Um die Sicherheit der Web-Oberfläche weiter zu erhöhen, kann HTTP Strict Transport Security (HSTS) aktiviert werden. Damit HSTS funktioniert, ist ein von einer Zertifizierungsstelle signiertes HTTPS-Zertifikat erforderlich (siehe Kapitel *7.2.4.1.7.2* (Seite 103)).

HSTS aktivieren

HSTS kann wie folgt aktiviert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.

3. *HTTPS* wählen und `Enter` drücken.
4. *HTTP STS* wählen und `Enter` drücken, um HSTS zu aktivieren oder zu deaktivieren.

Das maximal zulässige Alter des HSTS-Headers festlegen

Wenn HTTP STS aktiviert ist, kann das maximal zulässige Alter für den HSTS-Header wie folgt festgelegt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *HTTP STS max age* wählen und `Enter` drücken.
5. Maximales Alter in Sekunden in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.32).

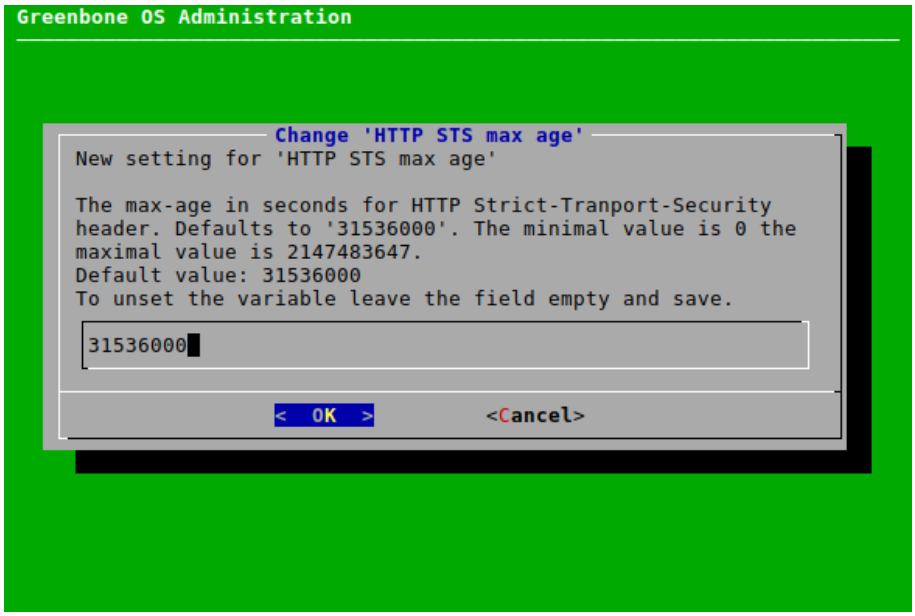


Abb. 7.32: Festlegen des maximal zulässigen Alters für den HTTP-STS-Header

→ Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

6. `Enter` drücken, um die Meldung zu schließen.

OCSP stapling konfigurieren

OCSP (Online Certificate Status Protocol) stapling wird zur Überprüfung des Gültigkeitsstatus von digitalen X.509-Zertifikaten verwendet. Es ermöglicht der zertifizierten Partei, die Zertifikatsvalidierung durchzuführen, indem sie eine von der Zertifizierungsstelle signierte OCSP-Antwort mit Zeitstempel an den ursprünglichen TLS-Handshake anhängt („stapling“).

OCSP stapling kann wie folgt aktiviert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *OCSP Stapling* wählen und `Enter` drücken, um OCSP stapling zu aktivieren oder zu deaktivieren.

Zertifikate verwalten

Die Appliance nutzt grundsätzlich zwei Arten von Zertifikaten:

- Selbstsignierte Zertifikate
- Zertifikat einer externen Zertifizierungsstelle

Alle modernen Betriebssysteme unterstützen das Erstellen und Verwalten eigener Zertifizierungsstellen.

- Unter Microsoft Windows Server unterstützen die Active Directory Certificate Services den Administrator bei der Erstellung einer Root-CA[13].
- Für Linux-Systeme sind verschiedene Optionen verfügbar. Eine Option ist im IPSec-Howto[14] beschrieben.

Bemerkung: Vor der Erstellung des Zertifikats muss überprüft werden, wie später auf die Systeme zugegriffen wird.

Die IP-Adresse oder der DNS-Name wird bei der Erstellung des Zertifikats gespeichert.

Das aktuelle Zertifikat anzeigen

Das aktuelle Zertifikat kann wie folgt angezeigt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Certificate* wählen und `Enter` drücken.
5. *Show* wählen und `Enter` drücken.

   → Das Zertifikat wird angezeigt.

Selbstsignierte Zertifikate

Die Nutzung selbstsignierter Zertifikate ist der einfachste Weg. Es stellt trotzdem die niedrigste Sicherheit und mehr Arbeit für den Benutzer dar:

- Die Vertrauenswürdigkeit eines selbstsignierten Zertifikats kann nur manuell durch den Benutzer geprüft werden, indem das Zertifikat importiert und sein Fingerprint untersucht wird.
- Selbstsignierte Zertifikate können nicht widerrufen werden. Sobald sie durch den Benutzer akzeptiert wurden, werden sie dauerhaft im Browser gespeichert. Wenn ein Angreifer Zugang zum entsprechenden privaten Schlüssel erhält, kann ein Man-in-the-Middle-Angriff auf die durch das Zertifikat geschützte Verbindung gestartet werden.

Um eine schnelle Einrichtung zu ermöglichen, unterstützt die Appliance selbstsignierte Zertifikate.

- Bei den meisten Appliance-Modellen ist ein solches Zertifikat nicht standardmäßig installiert und muss erstellt werden.
- Nur die Greenbone Enterprise ONE ist bereits mit einem vorinstallierten Zertifikat ausgestattet.

[13] https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority
[14] https://www.ipsec-howto.org/x600.html

Ein selbstsigniertes Zertifikat erstellen

Selbstsignierte Zertifikate können wie folgt erstellt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Certificate* wählen und `Enter` drücken.
5. *Generate* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass das aktuelle Zertifikat und der aktuelle private Schlüssel überschrieben werden.
6. *Yes* wählen und `Enter` drücken, um die Meldung zu bestätigen.
7. Einstellungen für das Zertifikat eingeben (siehe Abb. 7.33), *OK* wählen und `Enter` drücken.

Bemerkung: Es ist zulässig, ein Zertifikat ohne einen Common Name zu erstellen. Allerdings sollte ein Zertifikat nicht ohne (einen) Subject Alternative Name(s) (SAN) erstellt werden.

Falls ein Common Name verwendet wird, sollte dieser mit einem der SANs identisch sein.

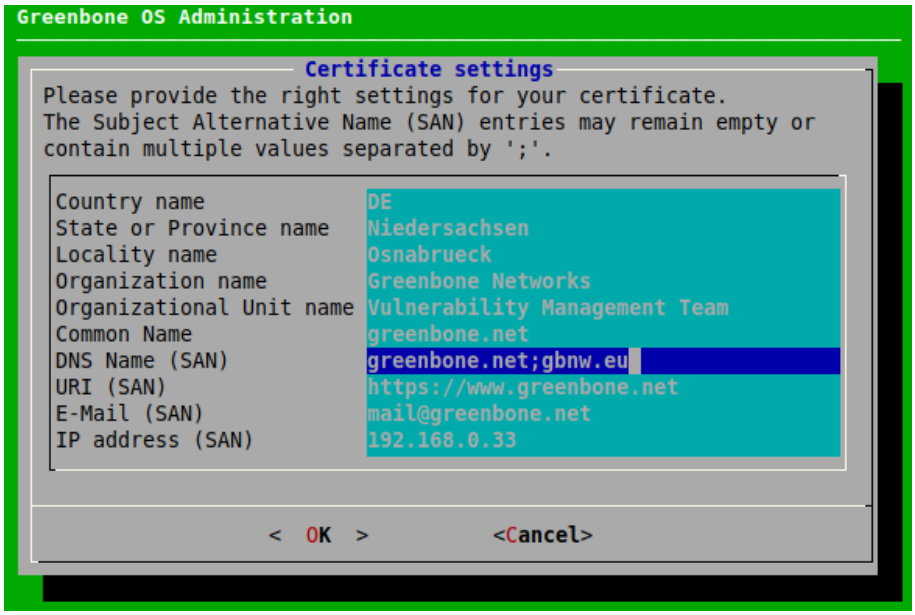


Abb. 7.33: Bereitstellen der Einstellungen für das Zertifikat

   → Wenn der Vorgang abgeschlossen ist, weist Meldung darauf hin, dass das Zertifikat heruntergeladen werden kann.
8. `Enter` drücken, um die Meldung zu schließen.
9. *Download* wählen und `Enter` drücken.
10. Webbrowser öffnen und angezeigte URL eingeben.
11. PEM-Datei herunterladen.
12. Im GOS-Administrationsmenü `Enter` drücken.

    → Wenn das Zertifikat von der Appliance erhalten wurde, zeigt das GOS-Administrationsmenü den Fingerprint des Zertifikats zur Verifizierung an.

13. Fingerprint prüfen und `Enter` drücken, um das Zertifikat zu bestätigen.

Zertifikat einer externen Zertifizierungsstelle

Das Nutzen eines Zertifikats, das von einer Zertifizierungsstelle ausgegeben wurde, hat mehrere Vorteile:

- Alle Clients, die der Zertifizierungsstelle vertrauen, können das Zertifikat direkt verifizieren und eine sichere Verbindung herstellen. Im Browser wird keine Warnung angezeigt.
- Das Zertifikat kann problemlos von der Zertifizierungsstelle widerrufen werden. Wenn die Clients die Möglichkeit haben, den Zertifikatsstatus zu überprüfen, können sie ein Zertifikat ablehnen, das zwar noch gültig ist, aber bereits widerrufen wurde. Als Mechanismen können die Certificate Revocation Lists (CRLs) oder das Online Certificate Status Protocol (OCSP) verwendet werden.
- Insbesondere wenn mehrere Systeme innerhalb einer Organisation SSL/TLS-geschützte Informationen bereitstellen, vereinfacht die Verwendung einer organisatorischen Zertifizierungsstelle die Verwaltung erheblich. Alle Clients müssen lediglich der organisatorischen Zertifizierungsstelle vertrauen, um alle von der Zertifizierungsstelle ausgestellten Zertifikate akzeptieren.

Um ein Zertifikat von einer externen Zertifizierungsstelle zu importieren, gibt es zwei Möglichkeiten:

- Eine Zertifikatsignierungsanforderung (engl. Certificate Signing Request, CSR) auf der Appliance generieren, diese über eine externe Zertifizierungsstelle signieren und das Zertifikat importieren.
- Die Zertifikatsignierungsanforderung und das Zertifikat extern generieren und beides mithilfe einer PKCS#12-Datei importieren.

Eine Zertifikatsanforderung erzeugen und ein Zertifikat importieren

---

Bemerkung: Die Web-Oberfläche der Appliance kann nicht verwendet werden, solange auf die Bearbeitung der CSR durch die CA gewartet wird. Erst nachdem das signierte Zertifikat importiert wurde, ist die Web-Oberfläche wieder zugänglich.

Das Erstellen einer neuen Zertifikatsanforderung und das Importieren des Zertifikats kann wie folgt durchgeführt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Certificate* wählen und `Enter` drücken.
5. *CSR* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass das aktuelle Zertifikat und der aktuelle private Schlüssel überschrieben werden.
6. *Yes* wählen und `Enter` drücken, um die Meldung zu bestätigen.
7. Einstellungen für das Zertifikat eingeben (siehe Abb. 7.34), *OK* wählen und `Enter` drücken.

   Bemerkung: Es ist zulässig, ein Zertifikat ohne einen Common Name zu erstellen. Allerdings sollte ein Zertifikat nicht ohne (einen) Subject Alternative Name(s) erstellt werden.

   Falls ein Common Name verwendet wird, sollte dieser mit einem der SANs identisch sein.

   ---
8. Webbrowser öffnen und angezeigte URL eingeben.

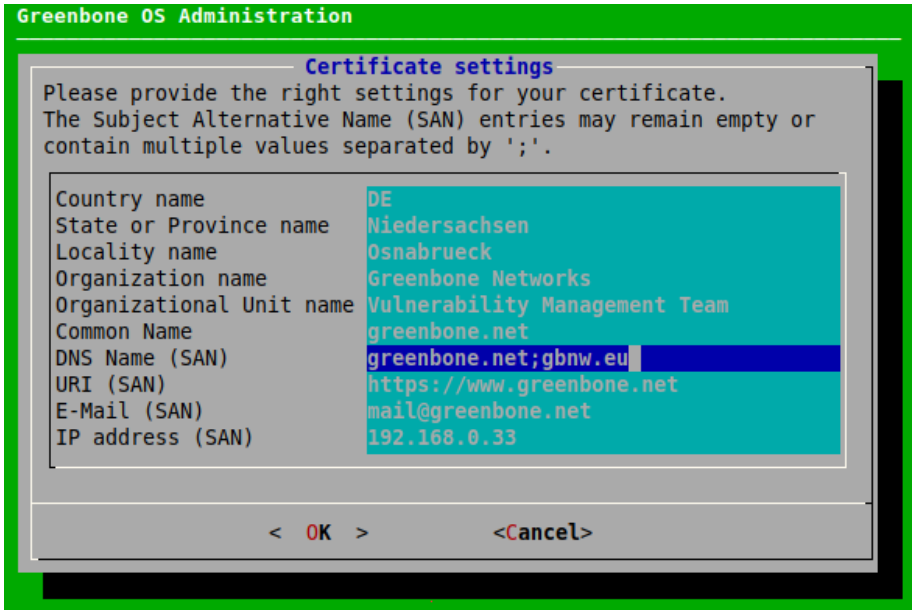


Abb. 7.34: Bereitstellen der Einstellungen für das Zertifikat

9. PEM-Datei herunterladen.

   → Das GOS-Administrationsmenü zeigt eine Meldung, um zu verifizieren, dass die Zertifikatsanforderung nicht gefälscht wurde.

10. `Enter` drücken, um die Information zu verifizieren.
11. Wenn das Zertifikat von der Zertifizierungsstelle signiert wurde, *Certificate* wählen und `Enter` drücken.
12. Webbrowser öffnen und angezeigte URL eingeben.
13. Auf *Browse...* klicken, das signierte Zertifikat wählen und auf *Upload* klicken.

    → Wenn das Zertifikat von der Appliance erhalten wurde, zeigt das GOS-Administrationsmenü den Fingerprint des Zertifikats zur Verifizierung an.

14. Fingerprint prüfen und `Enter` drücken, um das Zertifikat zu bestätigen.

Ein bereits vorhandenes Zertifikat importieren

Falls bereits ein privater Schlüssel und ein signiertes Zertifikat vorhanden sind, können diese importiert werden. Der private Schlüssel und das Zertifikat müssen als PKCS#12-Datei formatiert sein. Die Datei kann mit einem Exportpasswort geschützt werden.

Die PKCS#12-Datei kann wie folgt importiert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Certificate* wählen und `Enter` drücken.
5. *PKCS#12* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass das aktuelle Zertifikat und der aktuelle private Schlüssel überschrieben werden.

6. *Yes* wählen und `Enter` drücken, um die Meldung zu bestätigen.
7. Webbrowser öffnen und angezeigte URL eingeben.

8. Auf *Browse...* klicken, die PKCS#12-Datei wählen und auf *Upload* klicken.

   Bemerkung: Wenn der PKCS#12-Container durch ein Exportpasswort geschützt ist, muss das Passwort eingegeben werden.

   → Wenn das Zertifikat von der Appliance erhalten wurde, zeigt das GOS-Administrationsmenü den Fingerprint des Zertifikats zur Verifizierung an.

9. Fingerprint prüfen und `Enter` drücken, um das Zertifikat zu bestätigen.

Fingerprints anzeigen

Die Fingerprints des verwendeten Zertifikats können wie folgt angezeigt und überprüft werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *HTTPS* wählen und `Enter` drücken.
4. *Fingerprints* wählen und `Enter` drücken.

   → Die folgenden Fingerprints des aktuell aktiven Zertifikats werden angezeigt:

   - SHA1
   - SHA256
   - BB

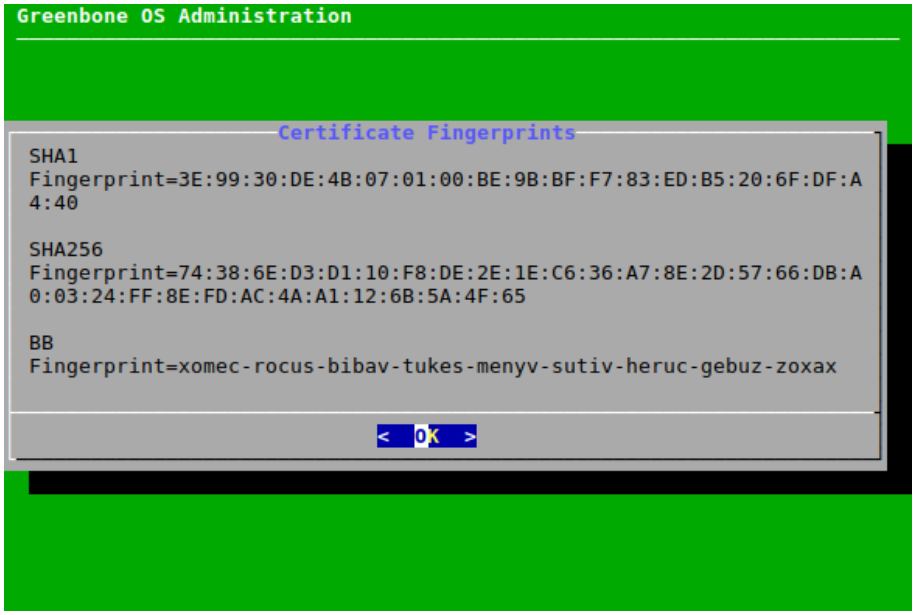


Abb. 7.35: Anzeigen der Fingerprints

7.2.4.2 Das Greenbone Management Protocol (GMP) konfigurieren

Das Greenbone Management Protocol (GMP) kann für die Kommunikation interner Software mit der Appliance genutzt werden.

GMP kann wie folgt mithilfe des GOS-Administrationsmenüs aktiviert werden:

Bemerkung: Der SSH-Dienst muss aktiviert werden, bevor GMP aktiviert werden kann (siehe Kapitel *7.2.4.4* (Seite 107)).

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *GMP* wählen und `Enter` drücken.
4. `Enter` drücken, um GMP zu aktivieren oder zu deaktivieren (siehe Abb. 7.36).

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
5. `Enter` drücken, um die Meldung zu schließen.

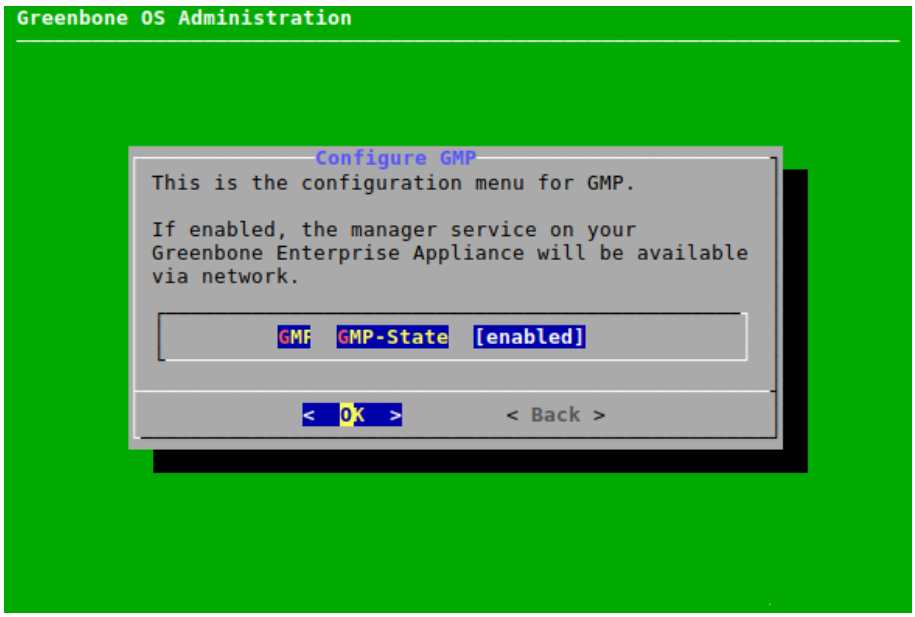


Abb. 7.36: Aktivieren von GMP

7.2.4.3 Das Open Scanner Protocol (OSP) konfigurieren

Das Open Scanner Protocol (OSP) wird für die Master-Sensor-Kommunikation benötigt (siehe Kapitel *16* (Seite 380)).

OSP kann wie folgt mithilfe des GOS-Administrationsmenüs aktiviert werden:

Bemerkung: Der SSH-Dienst muss aktiviert werden, bevor OSP aktiviert werden kann (siehe Kapitel *7.2.4.4* (Seite 107)).

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.

3. *OSP* wählen und `Enter` drücken.
4. `Enter` drücken, um OSP zu aktivieren oder zu deaktivieren.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
5. `Enter` drücken, um die Meldung zu schließen.

7.2.4.4 SSH konfigurieren

SSH ermöglicht den sicheren Fernzugriff auf das GOS-Administrationsmenü und die Kommandozeile der Appliance über ein ungesichertes Netzwerk. Außerdem ist es für die Master-Sensor-Kommunikation erforderlich (siehe Kapitel *16* (Seite 380)).

SSH ist auf der Appliance standardmäßig deaktiviert und muss erst aktiviert werden, z. B. über die serielle Konsole. Außerdem ist ein SSH-Client erforderlich, um eine Verbindung zur Appliance herzustellen.

- Bei der Verbindung *zur* Appliance mit einem SSH-Client werden die folgenden Schlüsselaustauschmethoden unterstützt:
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - curve25519-sha256
  - curve25519-sha256@libssh.org
- Bei der Verbindung *von* der Appliance zu einem anderen System hängen die unterstützten Methoden sowohl vom anderen System als auch von der Appliance ab. Es gibt viele mögliche Kombinationen, die jedoch den Rahmen dieser Dokumentation übersteigen würden.

Den SSH-Zustand aktivieren

Der in die Appliance integrierte SSH-Server kann wie folgt aktiviert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *SSH* wählen und `Enter` drücken.
4. *SSH State* wählen und `Enter` drücken, um SSH zu aktivieren.

Einen Loginschutz aktivieren und verwalten

Es kann ein Loginschutz aktiviert werden, d.h. wenn eine Anzahl von aufeinanderfolgenden Loginversuchen fehlschlägt, wird der Benutzer gesperrt.

Bemerkung: Ein Selbst-Scan, d. h. ein Scan, bei dem die Appliance Teil des Scan-Ziels ist, kann den Loginschutz auslösen.

Das Einloggen mithilfe eines SSH-Administratorschlüssels wird nicht vom Loginschutz gesperrt, falls solch ein Schlüssel eingerichtet ist (siehe Kapitel *7.2.4.4.3* (Seite 109)).

Den Loginschutz einrichten

Der Loginschutz kann wie folgt aktiviert und verwaltet werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *SSH* wählen und `Enter` drücken.
4. *Login Protection* wählen und `Enter` drücken.
5. *Login Protection* wählen und `Enter` drücken (siehe Abb. 7.37).

Abb. 7.37: Einrichten eines Loginschutzes

   → Eine Meldung weist darauf hin, dass der Loginschutz zu einem gesperrten SSH-Zugang führen kann.
6. *Continue* wählen und `Enter` drücken, um den Loginschutz zu aktivieren.
7. *Login Attempts* wählen und `Enter` drücken.
8. Gewünschten Wert eingeben und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
9. `Enter` drücken, um die Meldung zu schließen.

Ein gesperrtes System entsperren

Wenn das System nach zu vielen fehlgeschlagenen Loginversuchen gesperrt ist, muss es über den Konsolenzugriff (seriell, Hypervisor oder Monitor/Tastatur) wie folgt entsperrt werden:

1. *Setup* wählen und `Enter` drücken.
2. *User* wählen und `Enter` drücken.
3. *Unlock SSH* wählen und `Enter` drücken.

   → Die Loginversuche werden zurückgesetzt.
4. `Enter` drücken, um die Meldung zu schließen.

Einen SSH-Administratorschlüssel hinzufügen

Öffentliche SSH-Schlüssel können hochgeladen werden, um eine schlüsselbasierte Authentifizierung der Administratoren zu ermöglichen.

Bemerkung:

- SSH-Schlüssel können mit OpenSSH mit dem Befehl `ssh-keygen` unter Linux oder `puttygen.exe` bei Verwendung von PuTTY unter Microsoft Windows erzeugt werden.
- Die folgenden Formate werden unterstützt:
  - Ed25519, z. B. `ssh-ed25519 AAAAB3NzaC1y...P3pCquVb admin@greenbone`
  - RSA, z. B. `ssh-rsa AAAAB3NzaC1y...P3pCquVb admin@greenbone`

Ein SSH-Administratorschlüssel kann wie folgt hochgeladen werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *SSH* wählen und `Enter` drücken.
4. *Admin Key* wählen und `Enter` drücken.
5. Webbrowser öffnen und angezeigte URL eingeben (siehe Abb. 7.38).

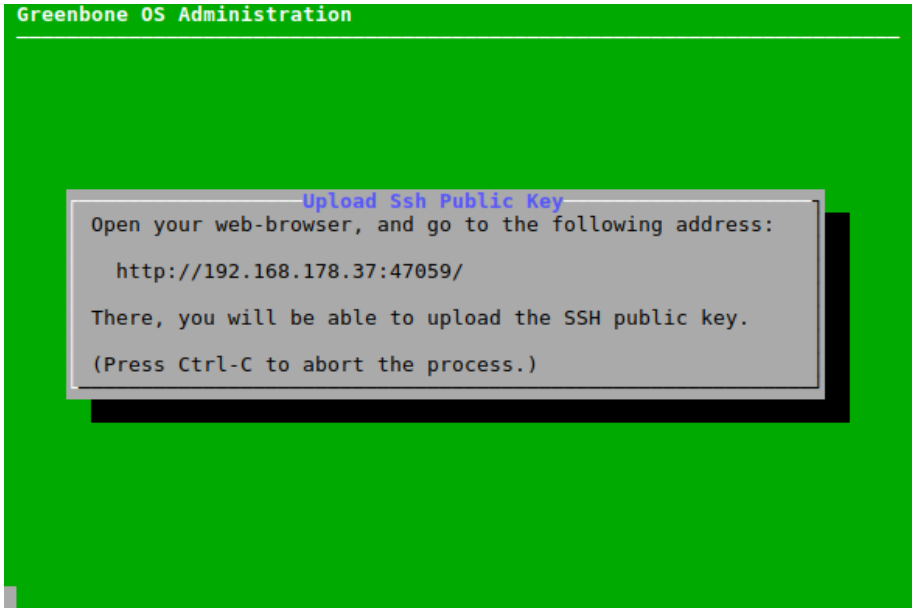


Abb. 7.38: Hochladen eines öffentlichen SSH-Schlüssels

6. Auf *Browse...* klicken, den öffentlichen SSH-Schlüssel wählen und auf *Upload* klicken.

   → Wenn das Hochladen abgeschlossen ist, weist Meldung darauf hin, dass der Login über SSH möglich ist.

Fingerprints anzeigen

Die Appliance stellt verschiedene Host-Schlüssel für ihre eigene Authentifizierung bereit. Der Client entscheidet, welchen öffentlichen Schlüssel er verwenden möchte.

Die Fingerprints der vom SSH-Server der Appliance verwendeten öffentlichen Schlüssel können wie folgt angezeigt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *SSH* wählen und `Enter` drücken.
4. *Fingerprint* wählen und `Enter` drücken.

   → Die SHA256-Fingerprints der folgenden Schlüssel werden angezeigt:

   - Ed25519
   - RSA

7.2.4.5 SNMP konfigurieren

Die Appliance unterstützt SNMPv3 für den Lesezugriff und SNMPv1 für das Versenden von Traps über Benachrichtigungen und das Überwachen wichtiger Parameter der Appliance.

Die unterstützten Parameter sind in einer MIB-Datei (Management Information Base) festgelegt. Die aktuelle MIB ist im Greenbone TechDoc-Portal[15] verfügbar.

SNMPv3 kann wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.
3. *SNMP* wählen und `Enter` drücken.
4. *SNMP* wählen und `Enter` drücken, um SNMP zu aktivieren.

   → Mehrere neue Optionen werden angezeigt (siehe Abb. 7.39).
5. *Location* wählen und `Enter` drücken.
6. Ort des SNMP-Diensts in das Eingabefeld eingeben und `Enter` drücken.
7. *Contact* wählen und `Enter` drücken.
8. Kontakt des SNMP-Diensts in das Eingabefeld eingeben und `Enter` drücken.
9. *Username* wählen und `Enter` drücken.
10. SNMP-Benutzername in das Eingabefeld eingeben und `Enter` drücken.

    Bemerkung: Bei der Konfiguration der Authentifizierungs- und Datenschutzpassphrase ist zu beachten, dass die Appliance SHA-1 bzw. AES128 verwendet.

    ---

11. *Authentication* wählen und `Enter` drücken.
12. SNMP-Authentifizierungspassphrase in das Eingabefeld eingeben und `Enter` drücken.
13. *Privacy* wählen und `Enter` drücken.

[15] https://docs.greenbone.net/API/SNMP/snmp-gos-22.04.de.html

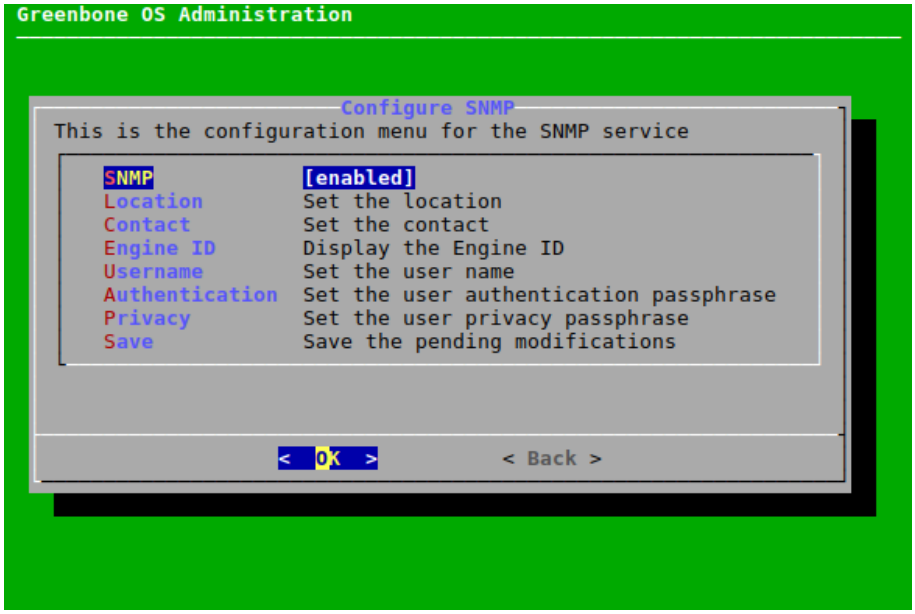


Abb. 7.39: Konfigurieren von SNMPv3

14. Passphrase für die Verschlüsselung des SNMP-Benutzers eingeben und `Enter` drücken.

Bemerkung: Nachdem ein Benutzer konfiguriert wurde, kann die Engine-ID der Appliance durch Wählen von *Engine ID* und Drücken von `Enter` angezeigt werden.

---

15. Den Lesezugriff des SNMP-Diensts unter Linux/Unix mit `snmpwalk` prüfen:

```
$ snmpwalk -v 3 -l authPriv -u user -a sha -A password -x aes -X key 192.168.222.115
iso.3.6.1.2.1.1.1.0 = STRING: "Greenbone Enterprise Appliance"
iso.3.6.1.2.1.1.3.0 = Timeticks: (347275248) 40 days, 4:39:12.48
iso.3.6.1.2.1.1.4.0 = STRING: "Greenbone AG <info@greenbone.net>"
...
```

Die folgenden Informationen können gesammelt werden:

- Betriebszeit
- Netzwerkschnittstellen
- Speicher
- Festplatte
- Last
- CPU

7.2.4.6 Einen Port für den temporären HTTP-Server konfigurieren

Standardmäßig wird der Port für HTTP-Uploads und -Downloads zufällig gewählt.

Ein permanenter Port kann wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Services* wählen und `Enter` drücken.

3. *Temporary HTTP* wählen und `Enter` drücken.
4. *Port* wählen und `Enter` drücken.
5. Port in das Eingabefeld eingeben und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
6. `Enter` drücken, um die Meldung zu schließen.

7.2.5 Regelmäßige Backups konfigurieren

Die Appliance unterstützt automatische tägliche Backups. Die folgenden Backups werden lokal oder remote gespeichert:

- Tägliche Backups der letzten 7 Tage
- Wöchentliche Backups der letzten 5 Wochen
- Monatliche Backups des letzten Jahrs

Backups, die älter als ein Jahr sind, werden automatisch gelöscht.

7.2.5.1 Periodische Backups aktivieren

Periodische Backups können wie folgt aktiviert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Backup* wählen und `Enter` drücken.
3. *Periodic Backup* wählen und `Enter` drücken (siehe Abb. 7.40).

   → Periodische Backups sind aktiviert.

Abb. 7.40: Konfigurieren periodischer Backups

7.2.5.2 Einen Remote-Backupserver einrichten

Standardmäßig werden Backups lokal gespeichert. Um sie auf einem Remote-Server zu speichern, muss der Server entsprechend eingerichtet werden. Die Appliance verwendet das SSH File Transfer Protocol (SFTP), um die Backups sicher zu übertragen.

Der Remote-Server kann wie folgt eingerichtet werden:

1. *Setup* wählen und `Enter` drücken.
2. *Backup* wählen und `Enter` drücken.
3. *Backup Location* wählen und `Enter` drücken.

   → Mehrere neue Optionen für den Ort des Backups werden angezeigt (siehe Abb. 7.41).

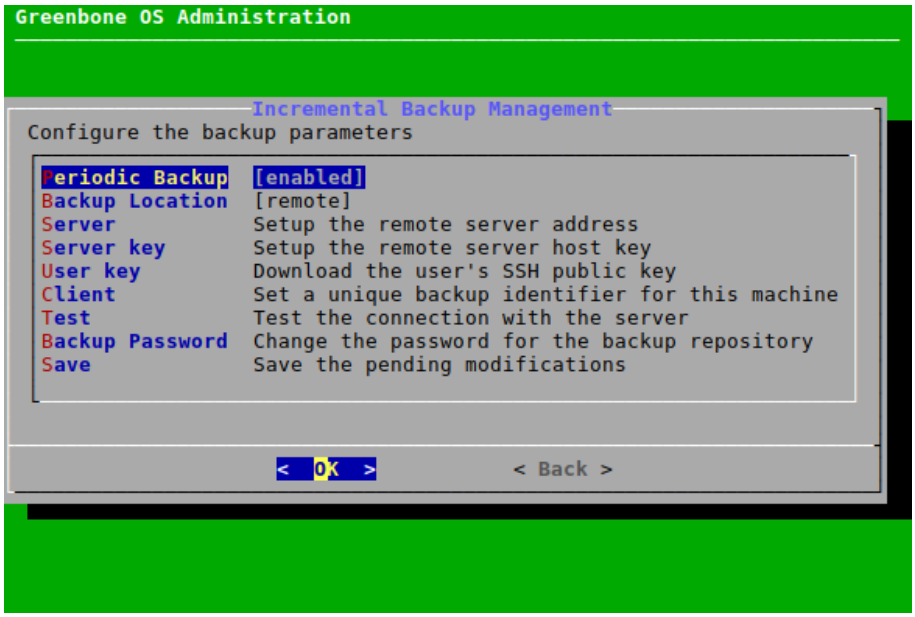


Abb. 7.41: Einrichten des Remote-Servers

4. *Server* wählen und `Enter` drücken.
5. Adresse des Remote-Servers im folgenden Format eingeben:

   ```
   username@hostname[:port]/directory
   ```

   Bemerkung: Der optionale Port kann weggelassen werden, falls der Server Port 22 nutzt.

6. *OK* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

7. `Enter` drücken, um die Meldung zu schließen.

Bemerkung: Die Appliance nutzt einen öffentlichen SSH-Hostschlüssel, um den Remote-Server vor dem Einloggen zu identifizieren.

- Der Schlüssel ist auf dem Remote-Backupserver zu finden. Unter Linux und den meisten Unix-ähnlichen Systemen befindet er sich unter `/etc/ssh/ssh_host_*_key.pub`.
- Der Schlüssel muss im OpenSSH Public Key Format vorliegen.
- Die erwartete Struktur ist `<algorithm> <key> <comment>`.
  - Der Abschnitt `<key>` muss Base64-kodiert sein.
  - Der Abschnitt `<comment>` ist optional.
  - Beispiel: `ssh-rsa AAAAB3NzaC1y...P3pCquVb`

8. *Server key* wählen und `Enter` drücken.
9. Webbrowser öffnen und angezeigte URL eingeben (siehe Abb. 7.42).

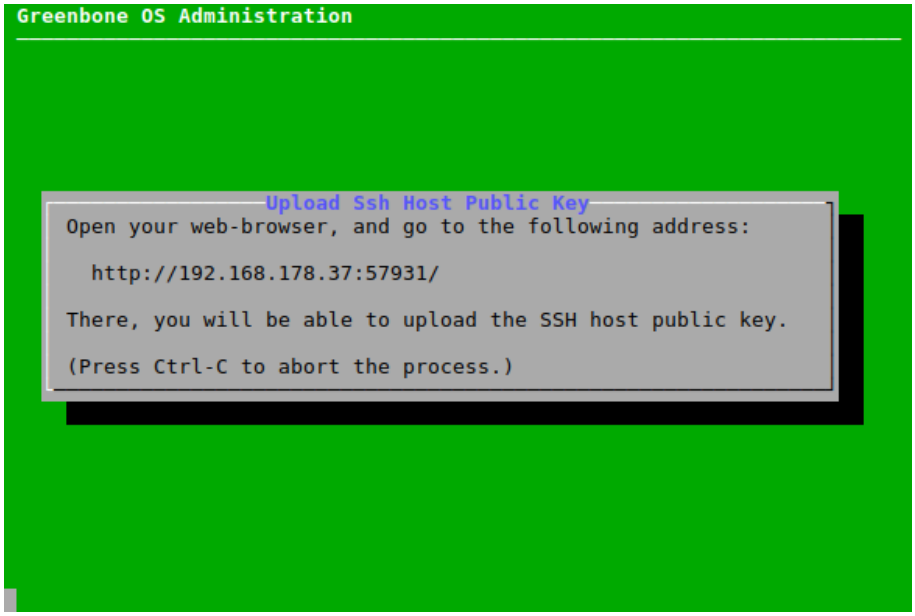


Abb. 7.42: Einrichten des Serverschlüssels

10. Auf *Browse...* klicken, den öffentlichen SSH-Schlüssel wählen und auf *Upload* klicken.

Bemerkung: Die Appliance nutzt einen öffentlichen SSH-Schlüssel, um sich in den Remote-Server einzuloggen. Um den Loginvorgang zu ermöglichen, muss die Appliance mit der `authorized_keys`-Datei auf dem Remoteserver aktiviert sein.

11. *User key* wählen und `Enter` drücken, um den öffentlichen Schlüssel herunterzuladen.
12. Webbrowser öffnen und angezeigte URL eingeben.

13. PUB-Datei herunterladen.

Bemerkung: Wenn mehrere Appliances ihre Backups auf denselben Remote-Server hochladen, müssen die Dateien unterscheidbar sein. Dazu muss ein eindeutiger Identifikator für das Backup festgelegt werden. Wird dieser Identifikator nicht festgelegt, wird der Hostname verwendet.

14. *Client* wählen und `Enter` drücken.
15. Bezeichnung eingeben und `Enter` drücken.

Bemerkung: Da das Setup des Remotebackups mit den Schlüsseln fehleranfällig ist, ist eine Prüfroutine verfügbar. Diese testet das erfolgreiche Einloggen in das Remotesystem.

16. *Test* wählen und `Enter` drücken.

    → Der Login in das Remotesystem wird getestet.

Bemerkung: Optional kann das Passwort für das Backup-Repository geändert werden, was zu empfehlen ist.

Wenn mehrere Appliances dasselbe Remote-Backup-Repository verwenden, wird empfohlen, dass jede Appliance ihr eigenes, eindeutiges Backup-Passwort verwendet.

17. *Backup Password* wählen und `Enter` drücken.
18. Passwort in das Eingabefeld eingeben und `Enter` drücken.

7.2.6 Besondere Upgrade-Einstellungen konfigurieren

7.2.6.1 Einen Upgrade-Schlüssel hinzufügen

Diese Option ist für mögliche Wiederherstellungszwecke gedacht. Das Hochladen eines Upgrade-Schlüssels ist für den normalen Betrieb der Appliance nicht erforderlich und sollte nur auf Anweisung von Greenbone durchgeführt werden. Greenbone stellt den Upgrade-Schlüssel in einem solchen Fall zur Verfügung.

Bemerkung: Der Schlüssel wird automatisch entfernt, wenn GOS erfolgreich aktualisiert wurde.

Einen Upgrade-Schlüssel mit dem Editor hinzufügen

Der Schlüssel kann über den Editor wie folgt hinzugefügt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Upgrade* wählen und `Enter` drücken.
3. *New Upgrade Key (Editor)* wählen und `Enter` drücken (siehe Abb. 7.43).

   → Der Editor wird geöffnet.

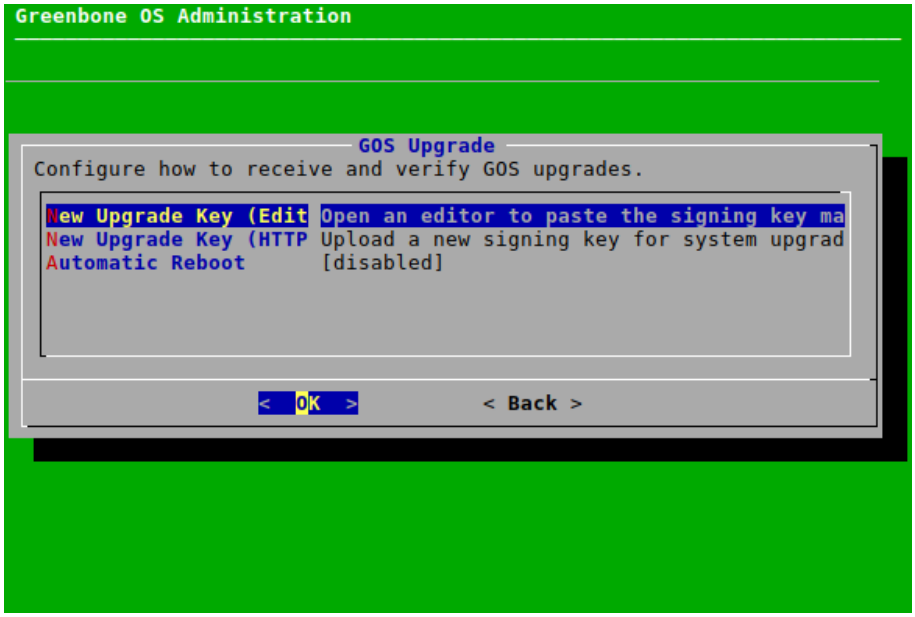


Abb. 7.43: Hochladen eines Upgrade-Schlüssels

4. Inhalt des Upgrade-Schlüssels eingeben.

   Bemerkung: Es ist wichtig, den Inhalt des Schlüssels und nicht den Namen des Schlüssels (z. B. `GBFeedSigningKeyUntil2024.gpg.asc`) einzugeben.

   Der Inhalt des Schlüssels kann mit einem beliebigen Texteditor oder unter Linux mit dem Programm `less` angezeigt werden. Wenn der Inhalt mit einem Texteditor geöffnet wird, muss darauf geachtet werden, dass nichts verändert wird.

   ---

5. `Strg` + `S` drücken, um die Änderungen zu speichern.
6. `Strg` + `X` drücken, um den Editor zu schließen.

   → Eine Meldung weist darauf hin, dass der Upgrade-Schlüssel erfolgreich hochgeladen wurde.
7. `Enter` drücken, um die Meldung zu schließen.

   Beide Menüpunkte zum Hochladen eines Schlüssels werden vorübergehend ausgeblendet. Stattdessen wird der Menüpunkt *Delete Upgrade Key* angezeigt (siehe Kapitel *7.2.6.2* (Seite 117)).

Einen Upgrade-Schlüssel über HTTP hinzufügen

Der Schlüssel kann über HTTP wie folgt hinzugefügt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Upgrade* wählen und `Enter` drücken.
3. *New Upgrade Key (HTTP)* wählen und `Enter` drücken (siehe Abb. 7.43).
4. Webbrowser öffnen und angezeigte URL eingeben.
5. Auf *Browse...* klicken, den Upgrade-Schlüssel wählen und auf *Upload* klicken.

   → Eine Meldung weist darauf hin, dass der Upgrade-Schlüssel erfolgreich hochgeladen wurde.

6. `Enter` drücken, um die Meldung zu schließen.

   Beide Menüpunkte zum Hochladen eines Schlüssels werden vorübergehend ausgeblendet. Stattdessen wird der Menüpunkt *Delete Upgrade Key* angezeigt (siehe Kapitel *7.2.6.2* (Seite 117)).

7.2.6.2 Einen Upgrade-Schlüssel löschen

Ein Upgrade-Schlüssel kann wie folgt gelöscht werden:

1. *Setup* wählen und `Enter` drücken.
2. *Upgrade* wählen und `Enter` drücken.
3. *Delete Upgrade Key* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass der Upgrade-Schlüssel entfernt wurde.
4. `Enter` drücken, um die Meldung zu schließen.

7.2.6.3 Den automatischen Neustart konfigurieren

Die Appliance kann nach einem erfolgreichen GOS-Upgrade automatisch neu starten. Ein Neustart wird jedoch nur bei Bedarf durchgeführt, z. B. wenn der GOS-Linux-Kernel aktualisiert wird.

Der automatische Neustart ist standardmäßig deaktiviert. In diesem Fall wird nach einem GOS-Upgrade, das einen Neustart erfordert, eine Self-Check-Warnung angezeigt, die zum manuellen Neustart auffordert.

Bemerkung: Diese Einstellung gilt nur für die Appliance, auf dem sie konfiguriert ist. Sie gilt nicht für alle Sensoren, die mit der Appliance verbunden sind. Wenn Sensoren automatisch neu starten sollen, muss jeder Sensor für sich konfiguriert werden.

---

1. *Setup* wählen und `Enter` drücken.
2. *Upgrade* wählen und `Enter` drücken.
3. *Automatic Reboot* wählen und `Enter` drücken.

   → Eine Warnung informiert darüber, dass die Appliance nach einem GOS-Upgrade sofort neu gestartet wird (siehe Abb. 7.44).

   Bemerkung: Alle Scans, die zu diesem Zeitpunkt laufen, werden beendet. Dies kann zum Verlust von ungesicherten Daten führen.

   ---

4. *Continue* wählen und `Enter` drücken.

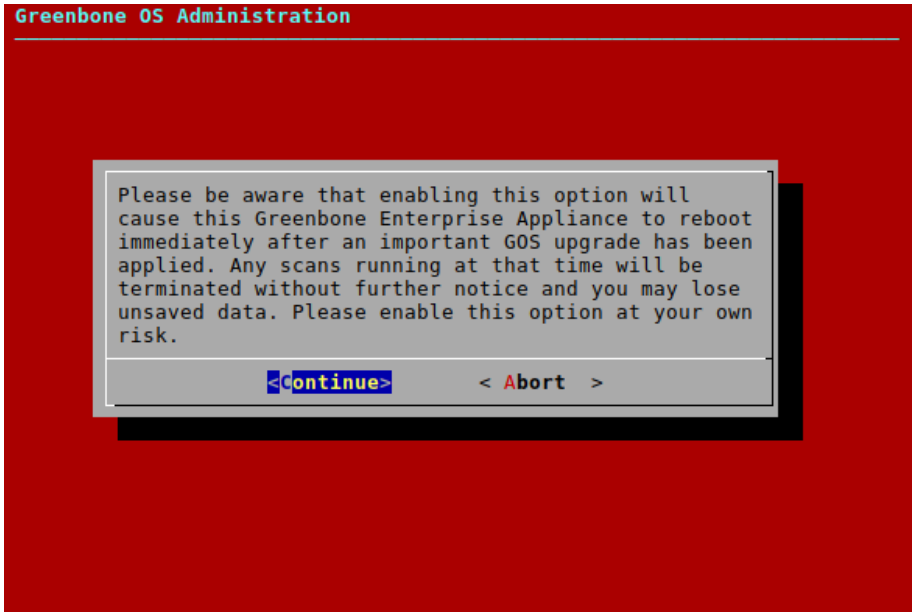


Abb. 7.44: Aktivieren des automatischen Neustarts

7.2.7 Die Feedsynchronisation konfigurieren

Der Greenbone Enterprise Feed[16] stellt Updates für Schwachstellentests (VTs), SCAP-Daten (CVE und CPE) und CERT-Bund- sowie DFN-CERT-Advisories bereit. Außerdem stellt der Feed Upgrades für GOS sowie Updates für Scan-Konfigurationen, Compliance-Richtlinien, Portlisten und Berichtformate bereit.

Für das Herunterladen und die Nutzung des Greenbone Enterprise Feeds ist ein Subskription-Schlüssel erforderlich (siehe Kapitel *7.1.1* (Seite 65)). Wenn kein gültiger Schlüssel auf der Appliance gespeichert ist, wird der öffentliche Greenbone Community Feed anstelle des Greenbone Enterprise Feeds verwendet.

7.2.7.1 Einen Greenbone-Enterprise-Feed-Subskription-Schlüssel hinzufügen

---

Bemerkung: Es ist nicht notwendig, einen Greenbone-Enterprise-Feed-Subskription-Schlüssel auf einer neu gelieferten Appliance hinzuzufügen, da bereits ein Schlüssel vorinstalliert ist.

Ob bereits ein Subskription-Schlüssel auf der Appliance vorhanden ist, kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

Ein neuer Subskription-Schlüssel kann auf der Appliance gespeichert werden, indem er entweder über HTTP hochgeladen oder mit einem Editor kopiert und eingefügt wird.

Für mehr Informationen über den Subskription-Schlüssel siehe Kapitel *7.1.1* (Seite 65).

Bemerkung: Ein neuer Schlüssel überschreibt jeden Schlüssel, der bereits auf der Appliance gespeichert ist.

Wenn der Subskription-Schlüssel überschrieben wird, wird der Status des Feeds auf der Appliance auf „No feed present“ zurückgesetzt. Nach dem Hinzufügen des neuen Subskription-Schlüssels muss ein Feed-Update durchgeführt werden.

---

[16] https://www.greenbone.net/feedvergleich/

Einen Subskription-Schlüssel über HTTP hinzufügen

Der Schlüssel kann über HTTP wie folgt hinzugefügt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Key(HTTP)* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass der aktuelle Subskription-Schlüssel überschrieben wird (siehe Abb. 7.45).

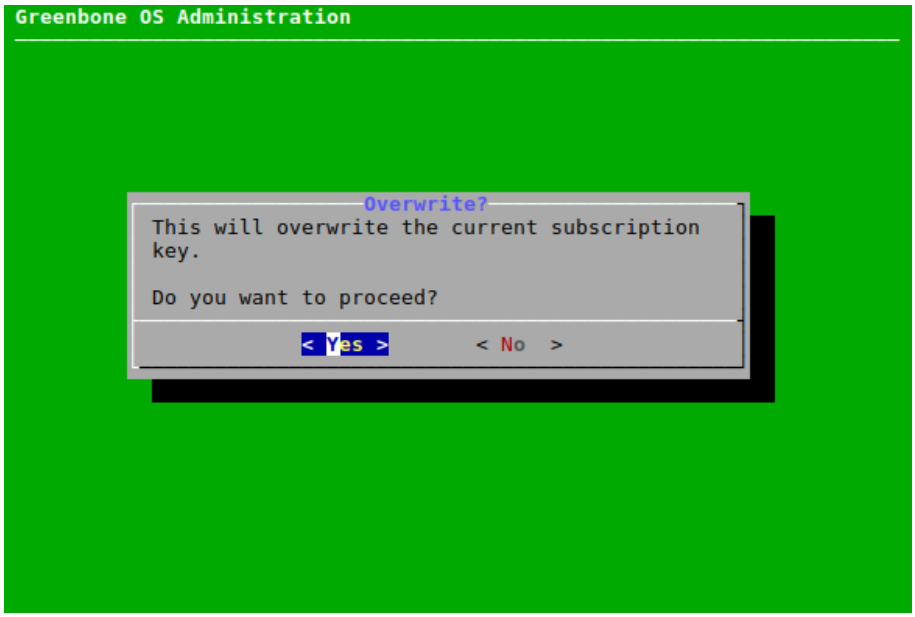


Abb. 7.45: Überschreiben des aktuellen Subskription-Schlüssels

4. *Yes* wählen und `Enter` drücken.
5. Webbrowser öffnen und angezeigte URL eingeben.
6. Auf *Browse...* klicken, den Subskription-Schlüssel wählen und auf *Upload* klicken.

   → Eine Meldung weist darauf hin, dass der Subskription-Schlüssel erfolgreich hochgeladen wurde.
7. `Enter` drücken, um die Meldung zu schließen.
8. Feed-Update wie in Kapitel *7.3.6* (Seite 151) beschrieben durchführen.

Einen Subskription-Schlüssel mit dem Editor hinzufügen

Der Schlüssel kann über den Editor wie folgt hinzugefügt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Key(Editor)* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass der aktuelle Subskription-Schlüssel überschrieben wird (siehe Abb. 7.45).
4. *Yes* wählen und `Enter` drücken.

   → Der Editor wird geöffnet.

5. Inhalt des Subskription-Schlüssels eingeben.

   Bemerkung: Es ist wichtig, den Inhalt des Schlüssels und nicht den Namen des Schlüssels (z. B. `gsf2022122017`) einzugeben.

   Der Inhalt des Schlüssels kann mit einem beliebigen Texteditor oder unter Linux mit dem Programm `less` angezeigt werden. Wenn der Inhalt mit einem Texteditor geöffnet wird, muss darauf geachtet werden, dass nichts verändert wird.

6. `Strg` + `S` drücken, um die Änderungen zu speichern.
7. `Strg` + `X` drücken, um den Editor zu schließen.

   → Eine Meldung weist darauf hin, dass der Subskription-Schlüssel erfolgreich hochgeladen wurde.

8. `Enter` drücken, um die Meldung zu schließen.
9. Feed-Update wie in Kapitel *7.3.6* (Seite 151) beschrieben durchführen.

7.2.7.2 Die Synchronisation aktivieren oder deaktivieren

Die automatische Synchronisation des Greenbone Enterprise Feeds kann deaktiviert werden, falls die Appliance keinen Internetzugang hat und nicht versuchen soll, auf die Greenbone-Dienste im Internet zuzugreifen. Die Synchronisation kann wieder aktiviert werden.

Die Synchronisation kann wie folgt aktiviert oder deaktiviert weden:

1. *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Synchronisation* wählen und `Enter` drücken.

   → Die Synchronisation ist aktiviert.

4. Die Synchronisation kann deaktiviert werden, indem erneut *Synchronisation* gewählt und `Enter` gedrückt wird.

Bemerkung: Die Zeit der automatischen Feedsynchronisation kann eingestellt werden, indem die Wartungszeit geändert wird (siehe Kapitel *7.2.13* (Seite 137)).

7.2.7.3 Den Synchronisationsport konfigurieren

Der Greenbone Enterprise Feed wird von Greenbone auf zwei verschiedenen Ports bereitgestellt:

- 24/tcp
- 443/tcp

Während Port 24/tcp der Standardport ist, lassen viele Firewall-Setups den Verkehr zu diesem Port im Internet nicht zu. Daher ist es möglich, den Port auf 443/tcp zu ändern, da dieser Port am meistens zugelassen wird.

Bemerkung: Port 443/tcp wird normalerweise für HTTPS-Verkehr verwendet. Obwohl die Appliance diesen Port verwendet, handelt es sich beim eigentlichen Datenverkehr nicht um HTTPS, sondern um SSH, da die Appliance das in SSH eingebettete `rsync` verwendet, um den Feed abzurufen. Firewalls, die Deep Inspection und Application Awareness einsetzen, können den Datenverkehr dennoch zurückweisen.

Der Port kann wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Greenbone Server* wählen und `Enter` drücken.
4. *Sync port* wählen und `Enter` drücken.
5. Gewünschten Port wählen und `Enter` drücken (siehe Abb. 7.46).

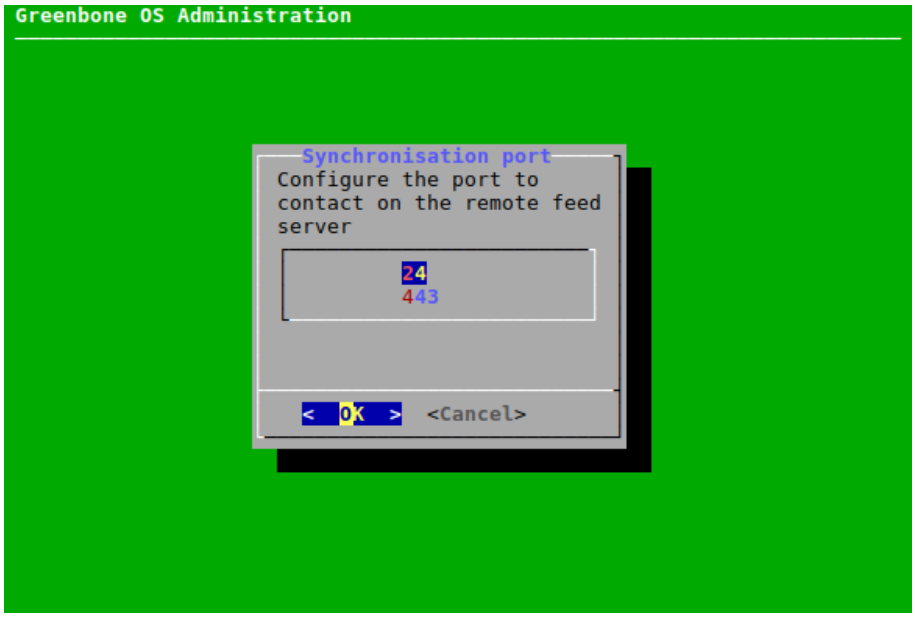


Abb. 7.46: Konfigurieren des Synchronisationsports

7.2.7.4 Den Synchronisationsproxy einstellen

Wenn eine Sicherheitsrichtlinie den direkten Internetzugang nicht zulässt, kann die Appliance einen HTTPS-Proxydienst verwenden. Dieser Proxy darf den SSL/TLS-Verkehr nicht untersuchen, muss aber die CONNECT-Methode unterstützen. Der Verkehr, der durch den Proxy läuft, ist nicht HTTPS, sondern SSH, das in http-proxy gekapselt ist.

Der Proxy kann wie folgt eingerichtet werden:

1. *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Greenbone Server* wählen und `Enter` drücken.
4. *Sync proxy* wählen und `Enter` drücken.
5. URL des Proxys in das Eingabefeld eingeben (siehe Abb. 7.47).

Bemerkung: Die URL muss die Form `http://proxy:port` haben.

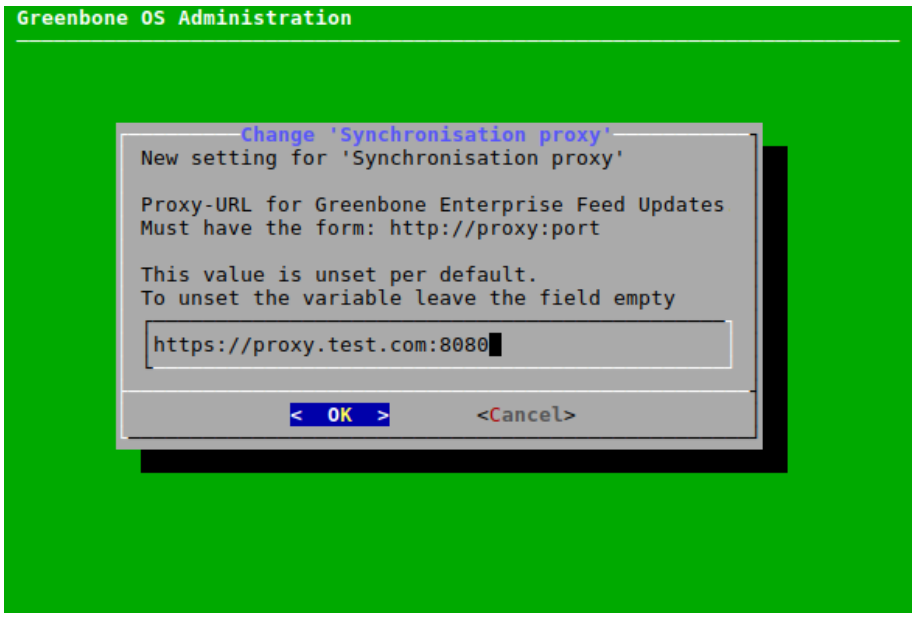


Abb. 7.47: Einstellen des Synchronisationsproxys

7.2.7.5 Den Greenbone-Enterprise-Feed-Subskription-Schlüssel löschen

Der Subskription-Schlüssel kann entfernt werden. Dies ist nützlich, wenn eine Appliance das Ende ihrer Lebensdauer erreicht hat und nicht mehr verwendet wird. Das Entfernen stellt sicher, dass keine Lizenzen mehr auf der Appliance vorhanden sind. Ohne den Subskription-Schlüssel wird die Appliance nur den Greenbone Community Feed abrufen.

Das Entfernen kann wie folgt durchgeführt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Cleanup* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Synchronisation mit dem Greenbone Enterprise Feed nach dem Entfernen nicht länger möglich ist (siehe Abb. 7.48).

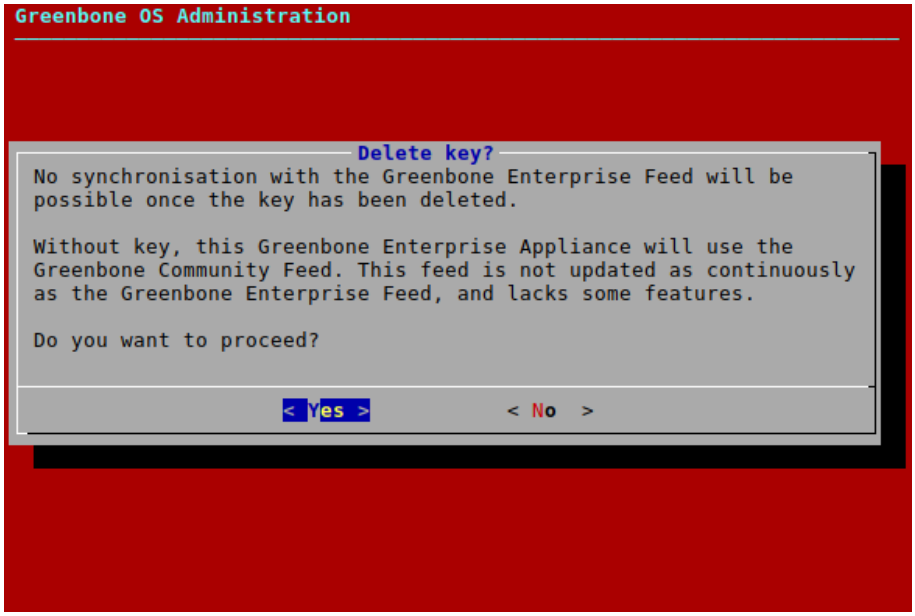


Abb. 7.48: Entfernen des Subskription-Schlüssels

4. *Yes* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass der Subskription-Schlüssel entfernt wurde.

5. `Enter` drücken, um die Meldung zu schließen.

7.2.8 Die Appliance als Airgap-Master/-Sensor konfigurieren

Die Airgap-Funktion ermöglicht es einer Appliance, die nicht direkt mit dem Internet verbunden ist, Feed-Updates und GOS-Upgrades zu erhalten.

Mindestens zwei Appliances werden benötigt:

- Airgap-Sensor: befindet sich in einem gesicherten Bereich und ist nicht mit dem Internet verbunden
- Airgap-Master: mit dem Internet verbunden

Bemerkung: Airgap-Appliances können auch verkettet werden, d. h. ein Airgap-Sensor wird zum Airgap-Master für einen anderen Airgap-Sensor.

Zwei Optionen sind für die Airgap-Funktion verfügbar:

- Airgap-USB-Stick von Greenbone
- Airgap-FTP-Server

Die folgenden Appliance-Modelle können für USB-Airgap konfiguriert werden:

- Greenbone Enterprise 400 und höher als Airgap-USB-Master
- Greenbone Enterprise 400 und höher als Airgap-USB-Sensor

Die folgenden Appliance-Modelle können für FTP-Airgap konfiguriert werden:

- Greenbone Enterprise 400 und höher als Airgap-FTP-Master
- Greenbone Enterprise 150 und höher als Airgap-FTP-Sensor
- Greenbone Enterprise CENO und höher als Airgap-FTP-Sensor

7.2.8.1 Den Airgap-USB-Stick nutzen

Die Updates und Upgrades werden von einer mit dem Internet verbundenen Appliance geladen und auf einen USB-Stick kopiert. Der USB-Stick kann dann zur Aktualisierung einer anderen Appliance verwendet werden.

Bemerkung: Der USB-Stick muss ein spezieller Airgap-USB-Stick sein, der von Greenbone bereitgestellt wird. Ein entsprechender Airgap-USB-Stick kann vom Greenbone Enterprise Support[17] unter Angabe der Kundennummer angefordert werden.

Tipp: Der USB-Stick kann vorher durch ein Sicherheitsgateway auf Schadsoftware geprüft werden.

Die Datenübertragung mithilfe des Airgap-USB-Sticks wird wie folgt durchgeführt:

1. Im GOS-Administrationsmenü des Airgap-Masters *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Airgap Master* wählen und `Enter` drücken.
4. *USB Master* wählen und `Enter` drücken (siehe Abb. 7.49).
5. *Save* wählen und `Enter` drücken.

[17] https://www.greenbone.net/technischer-support/

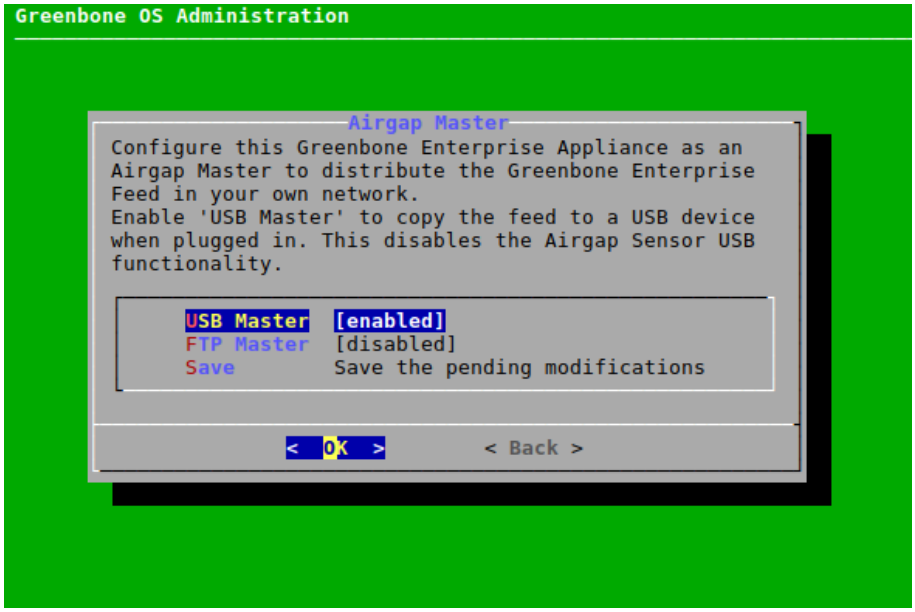


Abb. 7.49: Konfigurieren des Airgap-USB-Masters

Bemerkung: Das Konfigurieren einer Appliance als einen Airgap-USB-Master deaktiviert die Möglichkeit, die Appliance als einen Airgap-USB-Sensor zu konfigurieren.

6. Airgap-USB-Stick mit dem Airgap-Master verbinden.

   → Die Datenübertragung startet automatisch.

7. Wenn die Datenübertragung abgeschlossen ist, Airgap-USB-Stick mit dem Airgap-Sensor verbinden.

   → Die Datenübertragung startet automatisch.

7.2.8.2 Den Airgap-FTP-Server nutzen

Die Updates und Upgrades können über einen FTP-Server, der als Datendiode wirkt, bereitgestellt werden. Eine Datendiode ist ein einseitiges Sicherheitsgateway, das den Datenfluss nur in eine Richtung erlaubt.

Das FTP-Airgap-Update wird durchgeführt, wenn ein manuelles (siehe Kapitel *7.3.6* (Seite 151)) oder ein automatisches Feed-Update zur Wartungszeit durchgeführt wird.

Bemerkung: Der Airgap-Master muss genügend Zeit haben, um den Airgap-FTP-Feed auf den FTP-Server hochzuladen. Bei langsameren Verbindungen kann es ratsam sein, die Wartungszeit des Airgap-Sensors mindestens drei Stunden hinter die des Airgap-Masters zu legen (siehe Kapitel *7.2.9* (Seite 128)).

Die Konfiguration eines Airgap-FTP-Setups wird wie folgt durchgeführt:

1. Im GOS-Administrationsmenü des Airgap-Masters *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Airgap Master* wählen und `Enter` drücken.

4. *FTP Master* wählen und `Enter` drücken.

   → Mehrere neue Menüoptionen für die Konfiguration des FTP-Servers werden angezeigt (siehe Abb. 7.50).

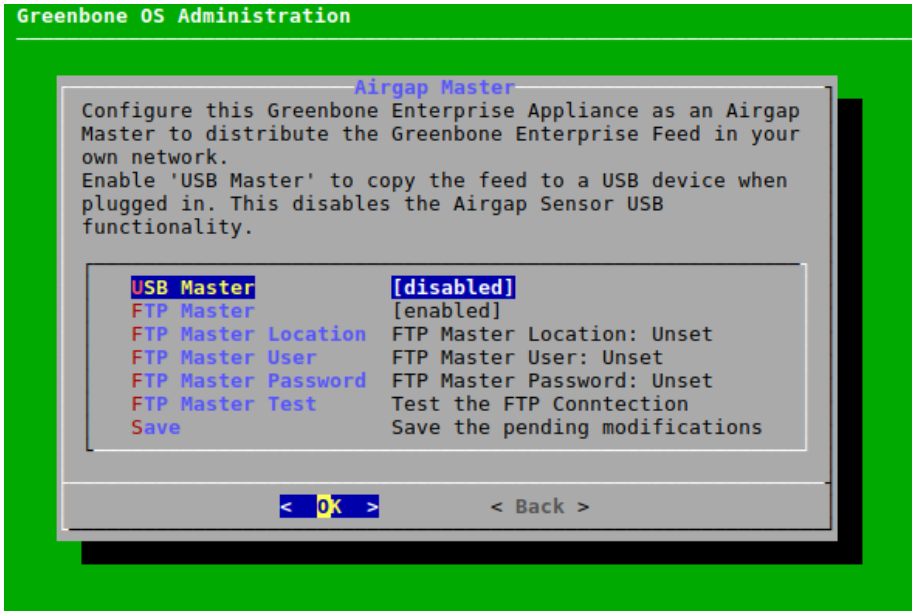


Abb. 7.50: Konfigurieren des FTP-Servers für den Airgap-Master

5. *FTP Master Location* wählen und `Enter` drücken.
6. Pfad des FTP-Servers in das Eingabefeld eingeben und `Enter` drücken.
   - Das erforderliche Importformat ist `ftp://1.2.3.4` oder `ftp://path.to.ftpserver`.
   - Optional kann ein Port konfiguriert werden, z.B. `ftp://1.2.3.4:21`.
   - Wenn kein Port konfiguriert ist, wird der Standard-FTP-Port 21 verwendet. Wenn ein anderer Port als 21 verwendet werden soll, muss dieser explizit konfiguriert werden.
7. *FTP Master User* wählen und `Enter` drücken.
8. Benutzer, der für das Einloggen in den FTP-Server genutzt wird, in das Eingabefeld eingeben und `Enter` drücken.
9. *FTP Master Password* wählen und `Enter` drücken.
10. Passwort, das für das Einloggen in den FTP-Server genutzt wird, in das Eingabefeld eingeben und `Enter` drücken.
11. *FTP Master Test* wählen und `Enter` drücken.

    → Es wird getestet, ob ein Login mit den eingegebenen Informationen funktioniert.
12. *Save* wählen und `Enter` drücken.
13. Im GOS-Administrationsmenü des Airgap-Sensors *Setup* wählen und `Enter` drücken.
14. *Feed* wählen und `Enter` drücken.
15. *Airgap Sensor* wählen und `Enter` drücken.

16. Schritte 5 bis 23 im GOS-Administrationsmenü des Airgap-Sensors mit den gleichen Eingaben wie für den Airgap-Master durchführen.

Bemerkung: Die Menüpunkte haben etwas andere Namen als im GOS-Administrationsmenü des Airgap-Master (siehe Abb. 7.51).

→ Die Datenübertragung startet beim nächsten Feed-Update.

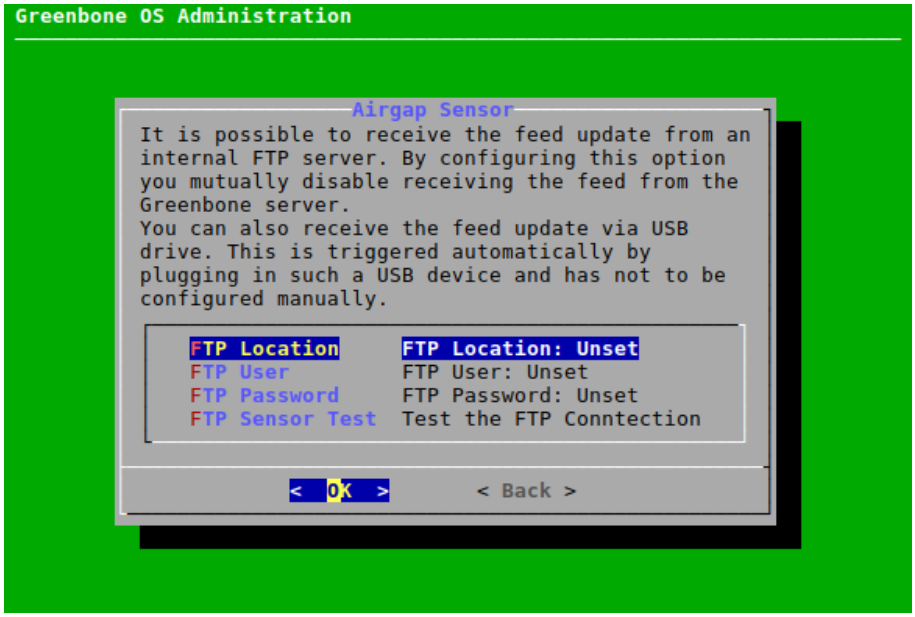


Abb. 7.51: Konfigurieren des FTP-Servers für den Airgap-Sensor

7.2.9 Die Zeitsynchronisation konfigurieren

Um die Appliance mit zentralen Zeitservern zu synchronisieren, unterstützt die Appliance das Network Time Protocol (NTP). Es können bis zu vier verschiedene NTP-Server konfiguriert werden. Die Appliance wählt den passendsten Server aus. Fällt ein Server aus, wird automatisch ein anderer Server verwendet.

Sowohl IP-Adressen als auch DNS-Namen werden unterstützt.

Bemerkung: Zeitzonen- und Sommerzeitsynchronisierung werden von NTP nicht unterstützt. Die Zeitzone der Appliance ist immer UTC±00:00.

Die NTP-Einstellungen können wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Timesync* wählen und `Enter` drücken.
3. *Time synchronisation* wählen und `Enter` drücken.

   → Die Zeitsynchronisation ist aktiviert.
4. Gewünschten Zeitserver wählen und `Enter` drücken (siehe Abb. 7.52).

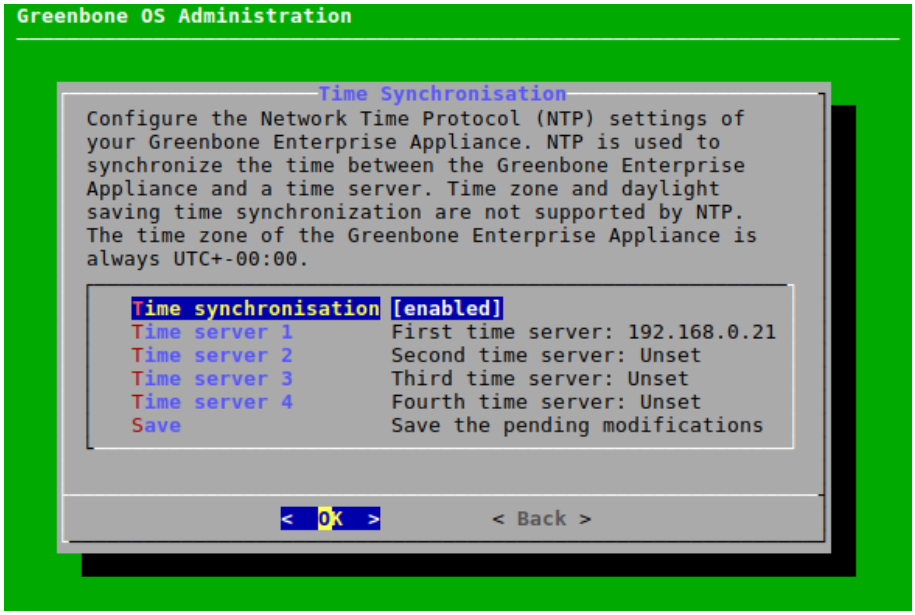


Abb. 7.52: Konfigurieren der NTP-Einstellungen

5. Zeitserver in das Eingabefeld eingeben und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
6. `Enter` drücken, um die Meldung zu schließen.

7.2.10 Das Tastaturlayout wählen

Das Tastaturlayout der Appliance kann wie folgt verändert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Keyboard* wählen und `Enter` drücken.

   → Alle verfügbaren Tastaturlayouts werden angezeigt. Das aktuelle Layout hat die Anmerkung *(selected)* (siehe Abb. 7.53).

Abb. 7.53: Wählen des Tastaturlayouts

3. Gewünschtes Tastaturlayout wählen und `Enter` drücken.

   → Eine Meldung fordert den Benutzer auf, die Änderung zu bestätigen.

4. *Yes* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass das Layout geändert wurde.

7.2.11 Die E-Mail-Einstellungen konfigurieren

Wenn Berichte über Schwachstellenscans oder Compliance-Audits per E-Mail zugestellt werden sollen, muss die Appliance zunächst mit einem Server verbunden werden, der als Mailhub fungiert. Ein solcher Server wird auch als „Mail-Relay“, „Relay-Host“ oder „Smarthost“ bezeichnet. Standardmäßig stellt die Appliance E-Mails nicht direkt ins Internet zu, sondern nur indirekt über den Mailhub, über den sie dann an die E-Mail-Server der Empfänger weitergeleitet werden müssen. Der Mailhub muss das Simple Mail Transfer Protocol (SMTP) unterstützen.

Die Appliance speichert keine E-Mails, wenn die Zustellung fehlschlägt, und es wird kein zweiter Zustellversuch unternommen.

Bemerkung: Die Appliance implementiert den Mail Transfer Agent Postfix. Der Mailhub muss möglicherweise korrekt eingerichtet werden, um mit der Appliance zusammenzuarbeiten. Informationen über spezielle Konfigurationen für diesen Fall finden sich in der Mailhub-Dokumentation.

Jeglicher Spamschutz auf dem Mailhub, wie z. B. graue Listen, muss für die Appliance deaktiviert werden.

7.2.11.1 Den Mailhub konfigurieren

Der Mailhub kann wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Mail* wählen und `Enter` drücken.
3. *Mail* wählen und `Enter` drücken.
4. URL des Mailhubs in das Eingabefeld eingeben (siehe Abb. 7.54).

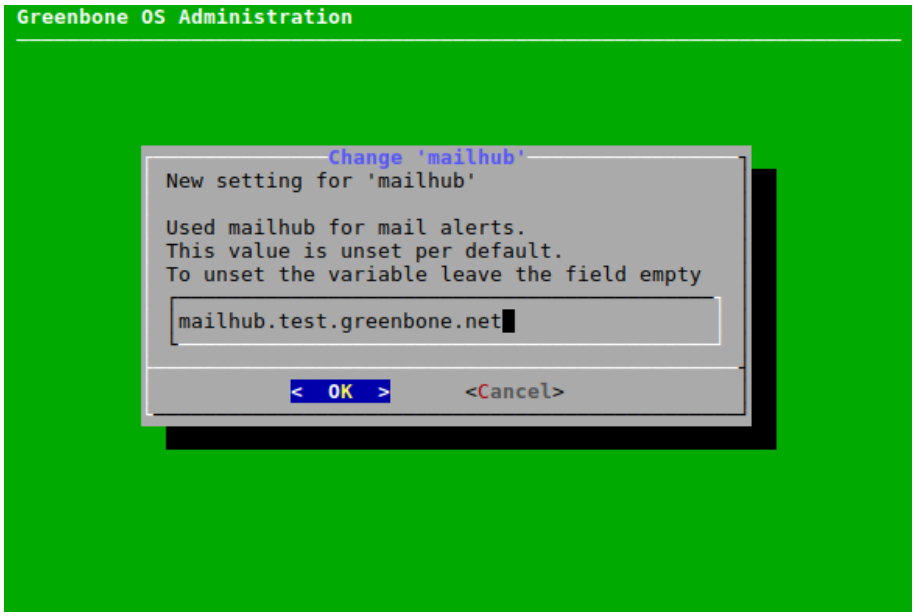


Abb. 7.54: Konfigurieren des Mailhubs

5. *OK* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
6. `Enter` drücken, um die Meldung zu schließen.

Bemerkung: Ein Port, der für den Mailhub verwendet wird, kann bei Bedarf konfiguriert werden. Eine manuelle Konfiguration ist jedoch nicht erforderlich.

Wenn kein Port konfiguriert ist, werden automatisch die Standard-Ports für SMTP(S) verwendet.

---

7. *Mailhub Port* wählen und `Enter` drücken.
8. Port in das Eingabefeld eingeben und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
9. `Enter` drücken, um die Meldung zu schließen.

7.2.11.2 SMTP-Authentifizierung für den Mailhub konfigurieren

Bemerkung: Die Appliance unterstützt nur die Authentifizierung über die SMTP-Auth-Erweiterung.

SMTP einrichten

Optional kann die SMTP-Authentifizierung für den verwendeten Mailhub wie folgt konfiguriert werden:

1. *Setup* wählen und `Enter` drücken.
2. *Mail* wählen und `Enter` drücken.
3. *SMTP Authentication Requirements* wählen und `Enter` drücken, um die SMTP-Authentifizierung zu aktivieren (siehe Abb. 7.55).

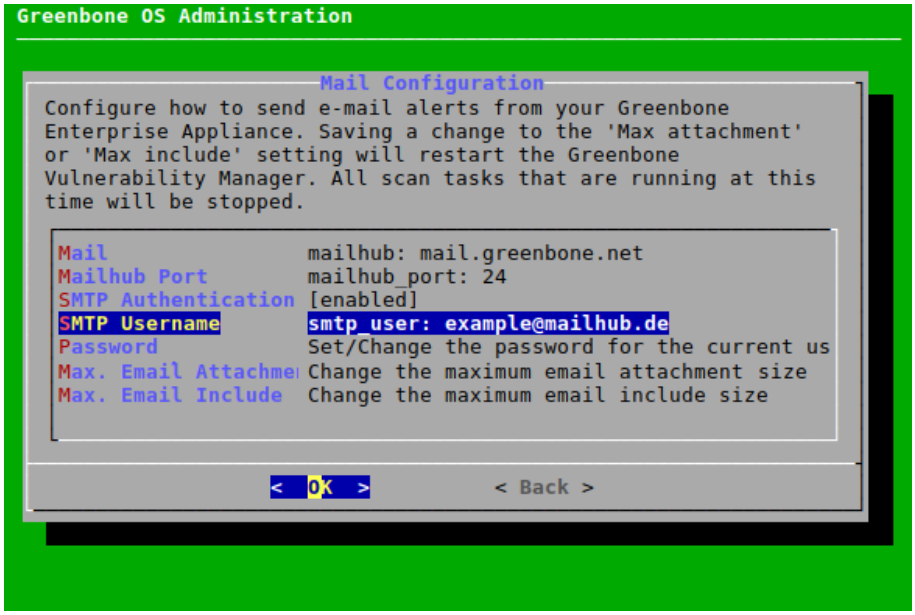


Abb. 7.55: Konfigurieren der SMTP-Authentifizierung

4. *SMTP Username* wählen und `Enter` drücken.
5. Benutzernamen des Accounts, der für die Authentifizierung genutzt wird, in das Eingabefeld eingeben und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.
6. `Enter` drücken, um die Meldung zu schließen.
7. *Password* wählen und `Enter` drücken.
8. Passwort des Accounts, der für die Authentifizierung genutzt wird, zweimal eingeben und `Tab` drücken.

   Bemerkung: Passwörter dürfen höchstens 128 Zeichen lang sein.
9. `Enter` drücken.

Die Verwendung von SMTPS erzwingen

SMTPS kann aktiviert werden, um den E-Mail-Verkehr immer mit TLS zu sichern.

Bemerkung: Wenn es aktiviert ist, muss der Mailhub auch SMTPS unterstützen, sonst schlägt der E-Mail-Versand fehl.

Auch wenn SMTPS nicht erzwungen wird, versucht GOS automatisch, die Verschlüsselung über STARTTLS zu verwenden. Nur wenn der Mailhub STARTTLS nicht unterstützt, ist der E-Mail-Verkehr unverschlüsselt.

SMTPS kann wie folgt erzwungen werden:

1. *Setup* wählen und `Enter` drücken.
2. *Mail* wählen und `Enter` drücken.
3. *SMTP Enforce TLS* wählen und `Enter` drücken.

7.2.11.3 Die maximale Größe enthaltener oder angehängter Berichte festlegen

Die maximale Größe (in Bytes) von enthaltenen oder angehängten Berichten (siehe Kapitel *10.12* (Seite 277)) kann wie folgt begrenzt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Mail* wählen und `Enter` drücken.
3. *Max. Email Attachment Size* oder *Max. Email Include Size* wählen und `Enter` drücken.

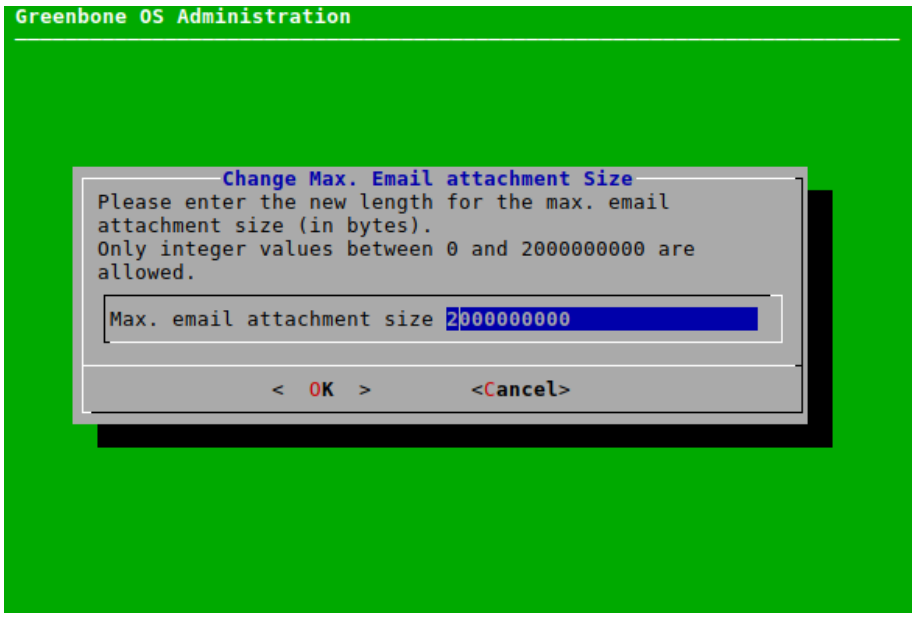


Abb. 7.56: Festlegen der maximalen Größe enthaltener oder angehängter Berichte

→ Eine Warnung weist darauf hin, dass eine Änderung der Größe einen Neustart des Greenbone Vulnerability Managers erfordert, was dazu führt, dass alle derzeit laufenden Scans gestoppt werden.

4. Maximale Größe (in Bytes) in das Eingabefeld eingeben (siehe Abb. 7.56).
5. *OK* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

6. `Enter` drücken, um die Meldung zu schließen.

7.2.12 Die Sammlung von Logs konfigurieren

Die Appliance unterstützt die Konfiguration eines zentralen Loggingservers für die Sammlung von Logs. Es können entweder nur die sicherheitsrelevanten Logs oder alle Systemlogs an einen Remote-Loggingserver gesendet werden.

Die sicherheitsrelevanten Logs enthalten nur Meldungen von den Facilities zur Sicherheits- und Authentifizierungsprotokollierung:

- *auth*
- *authpriv*
- *security*

Zusätzlich enthalten die vollständigen Logs die folgenden Facilities:

- *cron*
- *daemon*
- *ftp*
- *kern*
- *lp*
- *lpr*
- *ntp*
- *mail*
- *news*
- *syslog*
- *user*
- *uucp*
- *console*
- *solaris-cron*
- *local0 – local7*

Die Appliance nutzt das Syslog-Protokoll. Die zentrale Sammlung von Logs ermöglicht eine zentrale Analyse, Verwaltung und Überwachung der Logs. Zusätzlich werden die Logs immer auch lokal gespeichert.

Für jede Art von Logs (sicherheitsrelevante Logs oder alle Systemlogs) kann ein eigener Loggingserver konfiguriert werden.

Für die Übertragung können UDP (Standard), TLS und TCP verwendet werden.

- TCP gewährleistet die Zustellung der Logs auch bei Paketverlusten.
- Wenn bei einer Übertragung über UDP ein Paketverlust auftritt, gehen die Logs verloren.
- TLS ermöglicht eine optionale Authentifizierung des Absenders über TLS. Es werden nur TLS 1.2 und TLS 1.3 unterstützt. Dieses Verfahren ist nicht mit RFC 5425 konform.

Bemerkung: Die Zeitzone der Appliance (UTC±00:00) wird für die Zeitstempel der Logs verwendet, sofern dies nicht auf dem Syslog-Server angepasst wurde.

7.2.12.1 Den Loggingserver konfigurieren

Der Loggingserver kann wie folgt eingerichtet werden:

1. *Setup* wählen und `Enter` drücken.
2. *Remote Syslog* wählen und `Enter` drücken.
3. *Security Syslog* wählen und `Enter` drücken, um sicherheitsrelevante Logs zu aktivieren (siehe Abb. 7.57).

   oder

3. *Full Syslog* wählen und `Enter` drücken, um alle Systemlogs zu aktivieren (siehe Abb. 7.57).

Bemerkung: Beide Logs können aktiviert sein.

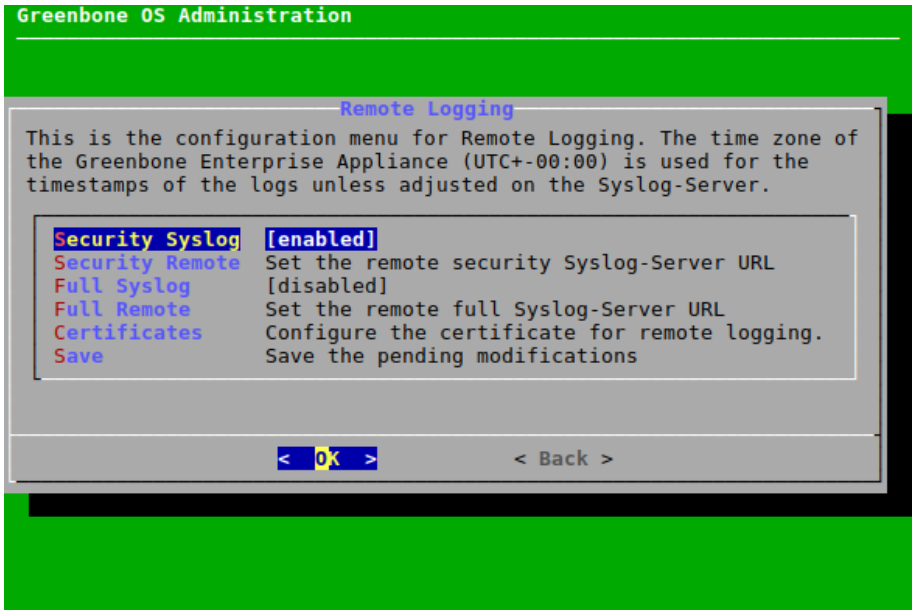


Abb. 7.57: Konfiguration der Logs

4. *Security Remote* wählen und `Enter` drücken, um die URL des Loggingservers für sicherheitsrelevante Logs einzustellen.

   oder

4. *Full Remote* wählen und `Enter` drücken, um die URL des Loggingservers für alle Systemlogs einzustellen.
5. URL des Loggingservers einschließlich des gewünschten Protokolls in das Eingabefeld eingeben (siehe Abb. 7.58).

Bemerkung: Falls kein Port festgelegt wird, wird der Standardport 514 genutzt.

Falls das Protokoll nicht angegeben wird, wird UDP genutzt.

Falls TLS verwendet wird, muss ein HTTPS-Zertifikat vorhanden sein (siehe Kapitel *7.2.12.2* (Seite 135)).

→ Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

6. `Enter` drücken, um die Meldung zu schließen.

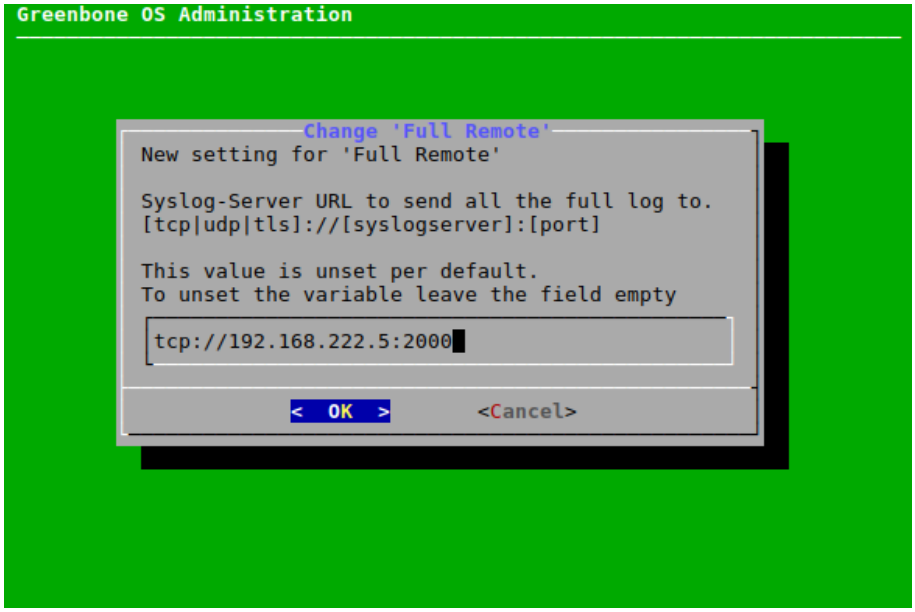


Abb. 7.58: Konfigurieren des Loggingservers

7.2.12.2 HTTPS-Zertifikate für das Logging verwalten

Ein Zertifikat erstellen

Die HTTPS-Zertifikate für das Logging können wie folgt verwaltet werden:

1. *Setup* wählen und `Enter` drücken.
2. *Remote Syslog* wählen und `Enter` drücken.
3. *Certificates* wählen und `Enter` drücken.
4. *Generate* wählen und `Enter` drücken, um ein Zertifikat zu generieren.

   → Eine Meldung weist darauf hin, dass das aktuelle Zertifikat und der aktuelle private Schlüssel überschrieben werden.
5. *Yes* wählen und `Enter` drücken, um die Meldung zu bestätigen.
6. Einstellungen für das Zertifikat eingeben (siehe Abb. 7.59), *OK* wählen und `Enter` drücken.

   Bemerkung: Es ist zulässig, ein Zertifikat ohne einen Common Name zu erstellen. Allerdings sollte ein Zertifikat nicht ohne (einen) Subject Alternative Name(s) (SAN) erstellt werden.

   Falls ein Common Name verwendet wird, sollte dieser mit einem der SANs identisch sein.

   → Wenn der Vorgang abgeschlossen ist, weist Meldung darauf hin, dass das Zertifikat heruntergeladen werden kann.
7. `Enter` drücken, um die Meldung zu schließen.
8. *Certificates* wählen und `Enter` drücken.
9. *Download* wählen und `Enter` drücken.
10. Webbrowser öffnen und angezeigte URL eingeben.
11. Datei herunterladen.

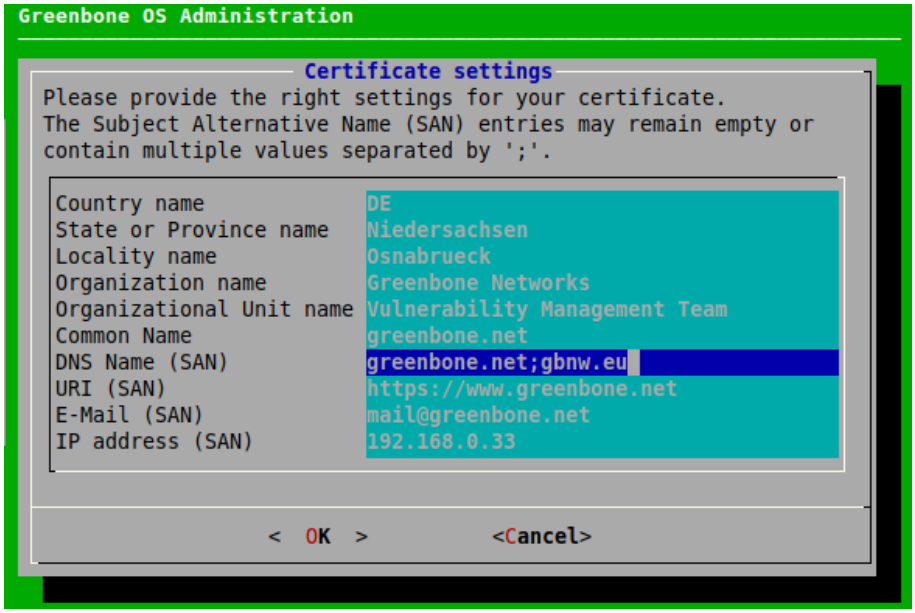


Abb. 7.59: Bereitstellen der Einstellungen für das Zertifikat

12. Im GOS-Administrationsmenü `Enter` drücken.

    → Wenn das Zertifikat von der Appliance erhalten wurde, zeigt das GOS-Administrationsmenü den Fingerprint des Zertifikats zur Verifizierung an.

13. Fingerprint prüfen und `Enter` drücken, um das Zertifikat zu bestätigen.

Das aktuelle Zertifikat und die Fingerprints anzeigen

Das Zertifikat und die zugehörigen Fingerprints können wie folgt angezeigt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Remote Syslog* wählen und `Enter` drücken.
3. *Certificates* wählen und `Enter` drücken.
4. *Show* wählen und `Enter` drücken, um das Zertifikat anzuzeigen.

   Fingerprint wählen und `Enter` drücken, um die Fingerprints anzuzeigen.

   → Die folgenden Fingerprints des aktuell aktiven Zertifikats werden angezeigt:

   - SHA1
   - SHA256

7.2.13 Die Wartungszeit festlegen

Während der Wartung findet die tägliche Synchronisierung des Feeds statt. Es kann ein beliebiger Zeitpunkt während des Tags gewählt werden, mit Ausnahme von 10:00 bis 13:00 UTC. Während dieser Zeit aktualisiert Greenbone den Feed und deaktiviert die Synchronisationsdienste.

Die standardmäßige Wartungszeit ist eine zufällige Zeit zwischen 3:00 und 5:00 UTC±00:00.

Die Wartungszeit kann wie folgt festgelegt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Time* wählen und `Enter` drücken.
3. Gewünschte Wartungszeit in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.60).

Bemerkung: Die Zeit muss vor der Eingabe in UTC umgerechnet werden.

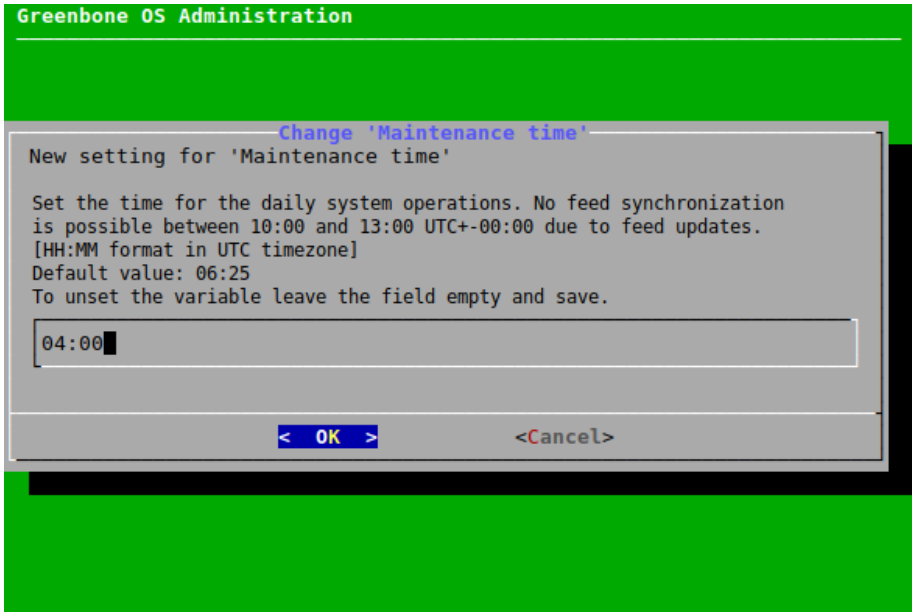


Abb. 7.60: Konfigurieren der Wartungszeit

→ Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

4. `Enter` drücken, um die Meldung zu schließen.

7.3 Maintenance-Menü

7.3.1 Einen Self-Check durchführen

Mit der Self-Check-Option wird die Einrichtung der Appliance überprüft. Sie zeigt falsche oder fehlende Konfigurationsdetails an, die eine korrekte Funktion der Appliance verhindern könnten. Die folgenden Punkte werden überprüft:

- Netzwerkverbindung
- DNS-Auflösung
- Erreichbarkeit des Feeds
- Verfügbare Updates
- Benutzerkonfiguration

Der Self-Check wird wie folgt durchgeführt:

1. *Maintenance* wählen und `Enter` drücken.
2. *Selfcheck* wählen und `Enter` drücken.

   → Der Self-Check wird durchgeführt. Anschließend wird das Ergebnis angezeigt.
3. `Enter` drücken (siehe Abb. 7.61).

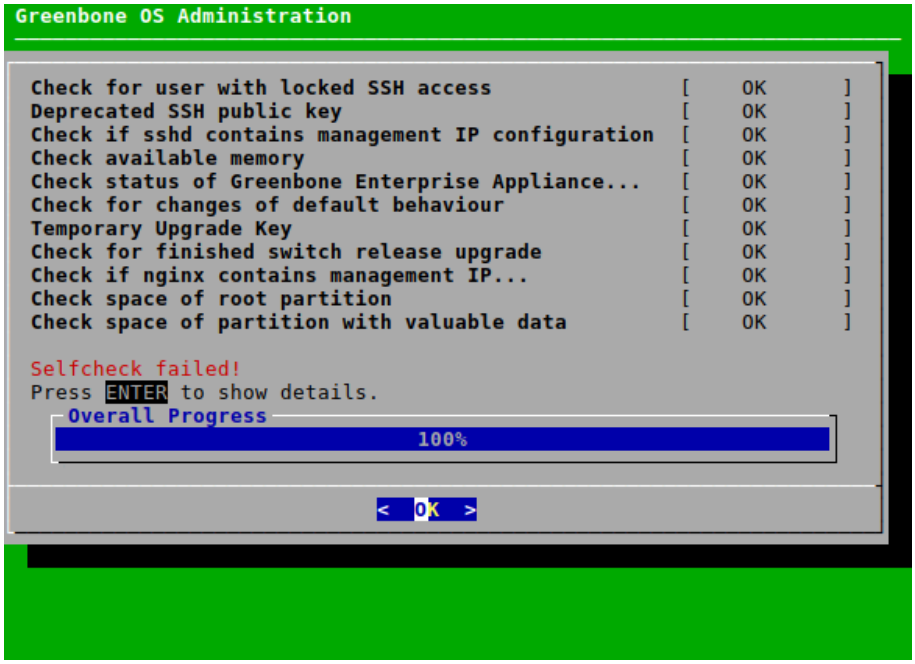


Abb. 7.61: Durchführen eines Self-Checks

7.3.2 Ein Backup durchführen und wiederherstellen

Bemerkung: Regelmäßige, geplante Backups werden im *Setup*-Menü konfiguriert (siehe Kapitel *7.2.5* (Seite 112)).

Zusätzlich zu den geplanten Backups können Backups auch manuell durchgeführt werden. Es gibt zwei verschiedene Backup-Typen mit unterschiedlichen Anwendungsfällen:

- **Inkrementelle Backups**
  - Es werden nur die Daten gesichert, die seit dem letzten Backup geändert wurden.
  - Wenn kein Backup vorhanden ist, wird ein vollständiges Backup durchgeführt.
  - Das inkrementelle Backup kann remote auf einem Server oder lokal auf der Appliance gespeichert werden.
  - Standardmäßig werden die letzten 7 täglichen Backups, die letzten 5 wöchentlichen Backups und die letzten 12 monatlichen Backups gespeichert. Backups, die älter als ein Jahr sind, werden automatisch gelöscht.
- **USB-Backups**
  - Zunächst wird ein separates, vollständiges (temporäres) Backup auf der Appliance erstellt und dann auf den USB-Flash-Speicher kopiert.
  - Das temporäre Backup auf der Festplatte wird anschließend gelöscht.

7.3.2.1 Inkrementelle Backups

Abhängig von dem in Kapitel *7.2.5* (Seite 112) konfigurierten Sicherungsort werden die inkrementellen Backups remote oder lokal gespeichert.

Die Backups umfassen Nutzerdaten (z. B. Aufgaben, Berichte, Ergebnisse) und Systemeinstellungen, d. h. die GOS-Konfiguration.

Ein inkrementelles Backup durchführen

Ein Backup kann wie folgt manuell durchgeführt werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Backup* wählen und `Enter` drücken.
3. *Incremental Backup* wählen und `Enter` drücken (siehe Abb. 7.62).

   → Eine Meldung informiert darüber, dass das Backup im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

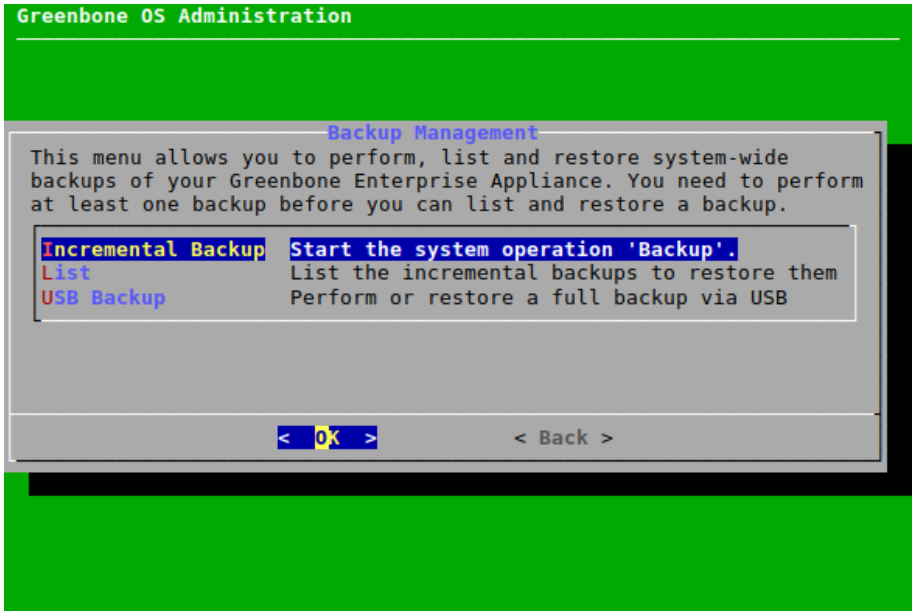


Abb. 7.62: Manuelles Auslösen eines Backups

Ein inkrementelles Backup wiederherstellen

Bemerkung: Es können nur Backups wiederhergestellt werden, die mit der aktuell verwendeten GOS-Version oder der vorherigen GOS-Version erstellt wurden. Bei GOS 22.04 können nur Backups aus GOS 21.04 oder GOS 22.04 importiert werden. Wenn ein älteres Backup, z. B. aus GOS 6 oder GOS 20.08, importiert werden soll, muss eine Appliance mit einer passenden GOS-Version verwendet werden.

Backups, die mit GOS-Versionen erstellt wurden, die neuer sind als die aktuell verwendete GOS-Version, werden ebenfalls nicht unterstützt. Wenn ein neueres Backup importiert werden soll, muss eine Appliance mit einer passenden GOS-Version verwendet werden.

Es können nur Backups wiederhergestellt werden, die mit dem gleichen Appliance-Modell (siehe Kapitel *3* (Seite 20)) erstellt wurden.

Es wird geprüft, ob die Subskription-Schlüssel des Backups und der Appliance, auf der das Backup wiederhergestellt werden soll, identisch sind. Falls die Schlüssel nicht übereinstimmen, wird eine Warnung angezeigt und der Benutzer muss bestätigen, dass der Schlüssel auf der Appliance überschrieben werden soll. Wenn jedoch ein Backup ohne Subskription-Schlüssel wiederhergestellt wird, bleibt der Schlüssel auf der Appliance erhalten.

Falls ein neues Backup-Passwort festgelegt wurde (siehe Kapitel *7.2.5.2* (Seite 113)) und ein Backup wiederhergestellt wird, das mit einem vorherigen Passwort erstellt wurde, wird das vorherige Passwort nicht wiederhergestellt. Die Appliance verwendet immer das neueste festgelegte Backup-Passwort.

Bei Fragen kann der Greenbone Enterprise Support[18] kontaktiert werden.

Ein Backup kann wie folgt wiederhergestellt werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Backup* wählen und `Enter` drücken.
3. *List* wählen und `Enter` drücken.

[18] https://www.greenbone.net/technischer-support/

4. Gewünschtes Backup wählen und `Enter` drücken.
5. *Yes* wählen und `Enter` drücken, falls sowohl Nutzerdaten als auch Systemeinstellungen hochgeladen werden sollen.

   oder

5. *No* wählen und `Enter` drücken, falls nur Nutzerdaten hochgeladen werden sollen.

Bemerkung: Die Systemeinstellungen enthalten alle GOS-Konfigurationen, z. B. Netzwerkeinstellungen.

Die Benutzerdaten enthalten alle Informationen zu Schwachstellenscanning und -management.

→ Eine Warnung informiert darüber, dass alle lokalen Einstellungen verloren gehen, falls das Backup wiederhergestellt wird (siehe Abb. 7.63).

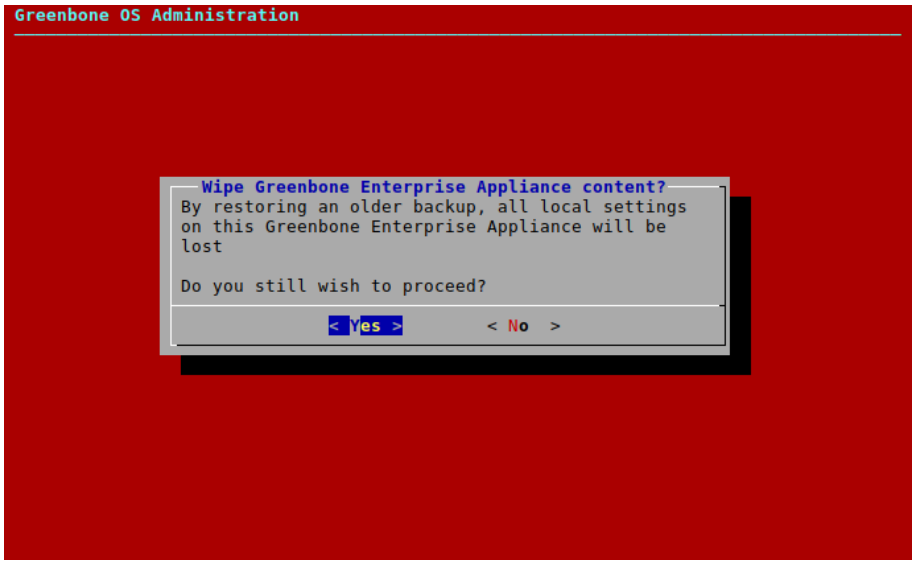


Abb. 7.63: Wiederherstellen eines Backups

6. *Yes* wählen und `Enter` drücken, um die Meldung zu bestätigen.

   → Eine Meldung weist darauf hin, dass die Wiederherstellung im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

7.3.2.2 USB-Backups

Ein USB-Backup durchführen

Backups können wie folgt auf einem USB-Flash-Speicher durchgeführt werden:

1. USB-Speicher mit der Appliance verbinden.
2. *Maintenance* wählen und `Enter` drücken.
3. *Backup* wählen und `Enter` drücken.
4. *USB Backup* wählen und `Enter` drücken.

   → Falls der verwendete USB-Speicher noch nicht für die Verwendung als GOS-Backup-Gerät formatiert ist, fragt eine Meldung, ob der USB-Speicher formatiert werden soll.

   Falls der USB-Speicher bereits für die Verwendung als GOS-Backup-Gerät formatiert ist, wird keine Meldung angezeigt. Mit Schritt 7 fortfahren.
5. *Yes* wählen und `Enter` drücken.

   → Eine Warnung weist darauf hin, dass die gespeicherten Daten gelöscht werden, wenn der Speicher formatiert wird.
6. *Yes* wählen und `Enter` drücken.

   → Der USB-Speicher wird für die Verwendung als GOS-Backup-Gerät formatiert.
7. *Backup* wählen und `Enter` drücken (siehe Abb. 7.64).

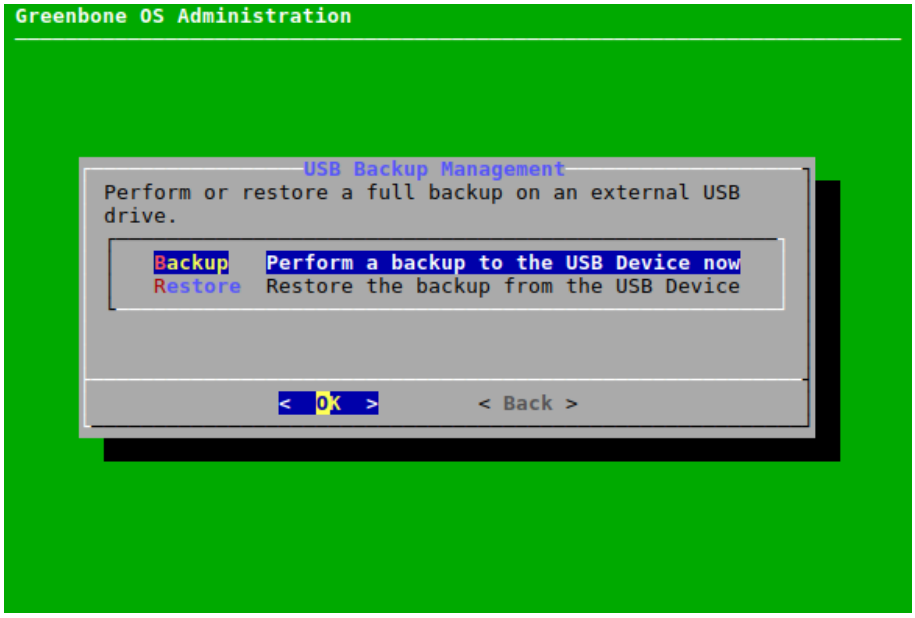


Abb. 7.64: Durchführen eines Backups mithilfe eines USB-Speichers

   → Eine Meldung fordert den Benutzer auf, das Backup zu bestätigen.
8. *Yes* wählen und `Enter` drücken.

   → Eine Meldung informiert darüber, dass das Backup im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

Ein USB-Backup wiederherstellen

Bemerkung: Es können nur Backups wiederhergestellt werden, die mit der aktuell verwendeten GOS-Version oder der vorherigen GOS-Version erstellt wurden. Bei GOS 22.04 können nur Backups aus GOS 21.04 oder GOS 22.04 importiert werden. Wenn ein älteres Backup, z. B. aus GOS 6 oder GOS 20.08, importiert werden soll, muss eine Appliance mit einer passenden GOS-Version verwendet werden.

Backups, die mit GOS-Versionen erstellt wurden, die neuer sind als die aktuell verwendete GOS-Version, werden ebenfalls nicht unterstützt. Wenn ein neueres Backup importiert werden soll, muss eine Appliance mit einer passenden GOS-Version verwendet werden.

Es können nur Backups wiederhergestellt werden, die mit dem gleichen Appliance-Modell (siehe Kapitel *3* (Seite 20)) erstellt wurden.

Es wird geprüft, ob die Subskription-Schlüssel des Backups und der Appliance, auf der das Backup wiederhergestellt werden soll, identisch sind. Falls die Schlüssel nicht übereinstimmen, wird eine Warnung angezeigt und der Benutzer muss bestätigen, dass der Schlüssel auf der Appliance überschrieben werden soll. Wenn jedoch ein Backup ohne Subskription-Schlüssel wiederhergestellt wird, bleibt der Schlüssel auf der Appliance erhalten.

Falls ein neues Backup-Passwort festgelegt wurde (siehe Kapitel *7.2.5.2* (Seite 113)) und ein Backup wiederhergestellt wird, das mit einem vorherigen Passwort erstellt wurde, wird das vorherige Passwort nicht wiederhergestellt. Die Appliance verwendet immer das neueste festgelegte Backup-Passwort.

Bei Fragen kann der Greenbone Enterprise Support[19] kontaktiert werden.

Backups können wie folgt von einem USB-Speicher wiederhergestellt werden:

1. USB-Speicher, der das gewünschte GOS-Backup enthält, mit der Appliance verbinden.

   Bemerkung: Bei Problemen sollte ein anderer USB-Speicher oder ein anderer USB-Anschluss der Appliance verwendet werden.

2. *Maintenance* wählen und `Enter` drücken.
3. *Backup* wählen und `Enter` drücken.
4. *USB Backup* wählen und `Enter` drücken.
5. *Restore* wählen und `Enter` drücken (siehe Abb. 7.64).
6. *Yes* wählen und `Enter` drücken, falls sowohl Nutzerdaten als auch Systemeinstellungen hochgeladen werden sollen.

   oder

6. *No* wählen und `Enter` drücken, falls nur Nutzerdaten hochgeladen werden sollen.

   Bemerkung: Die Systemeinstellungen enthalten alle GOS-Konfigurationen, z. B. Netzwerkeinstellungen.

   Die Benutzerdaten enthalten alle Informationen zu Schwachstellenscanning und -management.

[19] https://www.greenbone.net/technischer-support/

→ Eine Warnung informiert darüber, dass alle lokalen Einstellungen verloren gehen, falls das Backup wiederhergestellt wird (siehe Abb. 7.65).

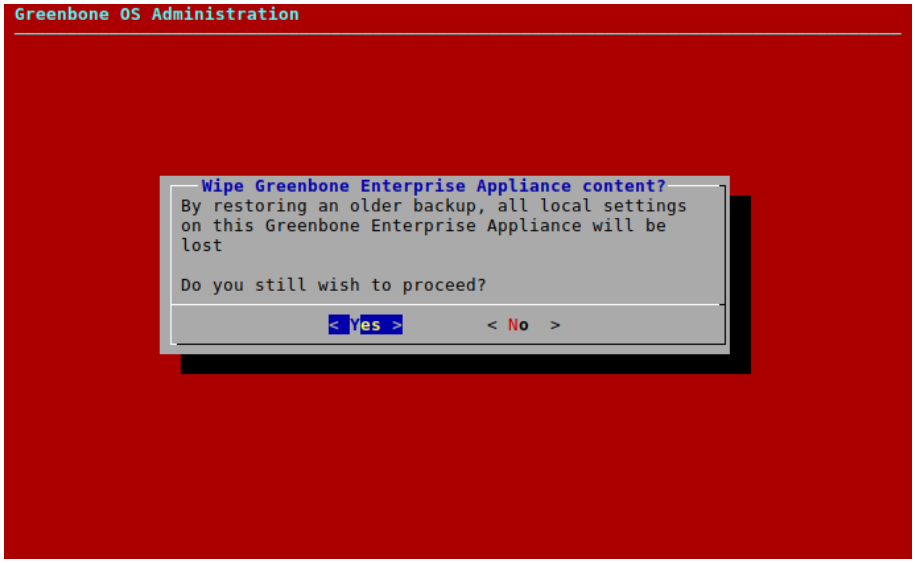


Abb. 7.65: Wiederherstellen eines Backups

7. *Yes* wählen und `Enter` drücken, um die Meldung zu bestätigen.

   → Eine Meldung weist darauf hin, dass die Wiederherstellung im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

7.3.3 Daten und Einstellungen mithilfe von Beaming auf eine andere Appliance kopieren

Der aktuelle Zustand einer Appliance kann auf eine andere Appliance kopiert werden. Dazu gehören Benutzerdaten (z. B. Aufgaben, Berichte, Ergebnisse) und Systemeinstellungen, d. h. die GOS-Konfiguration.

Auf der empfangenden Appliance kann gewählt werden, ob nur die Nutzerdaten oder sowohl Nutzerdaten als auch Systemeinstellungen importiert werden sollen.

Bemerkung: Es können nur Beaming-Images wiederhergestellt werden, die mit der aktuell verwendeten GOS-Version oder der vorherigen GOS-Version erstellt wurden. Bei GOS 22.04 können nur Beaming-Images aus GOS 21.04 oder GOS 22.04 importiert werden. Wenn ein älteres Beaming-Image, z. B. aus GOS 20.08, importiert werden soll, muss eine Appliance mit einer passenden GOS-Version verwendet werden.

Es ist nur möglich, ein Beaming-Image auf eine Appliance zu importieren, wenn die Release-Informationen, d.h. die Liste der verfügbaren GOS-Upgrades, auf der entsprechenden Appliance aktuell sind. Um dies sicherzustellen, sollte ein aktueller Greenbone Enterprise Feed heruntergeladen werden.

Beaming-Images, die mit GOS-Versionen erstellt wurden, die neuer sind als die aktuell verwendete GOS-Version, werden ebenfalls nicht unterstützt. Wenn ein neueres Beaming-Image importiert werden soll, muss eine Appliance mit einer passenden GOS-Version genutzt werden.

Das Beaming ist nur auf eine Appliance der gleichen oder einer höheren Klasse erlaubt (siehe Kapitel *3* (Seite 20)). Das Beaming auf eine Greenbone Enterprise TRIAL wird nicht unterstützt.

Es wird geprüft, ob die Subskription-Schlüssel des Beaming-Images und der Appliance, auf der das Beaming-Image wiederhergestellt werden soll, identisch sind. Falls die Schlüssel nicht übereinstimmen, wird eine Warnung angezeigt und der Benutzer muss bestätigen, dass der Schlüssel auf der Appliance überschrieben werden soll. Wenn jedoch ein Beaming-Image ohne Subskription-Schlüssel wiederhergestellt wird, bleibt der Schlüssel auf der Appliance erhalten.

Bei Fragen kann der Greenbone Enterprise Support[20] kontaktiert werden.

7.3.3.1 Beaming direkt von einer anderen Appliance aus durchführen

Das Beaming-Image kann wie folgt erstellt und direkt kopiert werden:

Bemerkung:

- Appliance A = sendende Appliance
- Appliance B = empfangende Appliance

---

1. Im GOS-Administrationsmenü von Appliance A *Maintenance* wählen und `Enter` drücken.
2. *Beaming* wählen und `Enter` drücken.
3. *Download* wählen und `Enter` drücken (siehe Abb. 7.66).

   → Eine Meldung weist darauf hin, dass die Erstellung des Beaming-Images im Hintergrund gestartet wurde.

   Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

   ---

[20] https://www.greenbone.net/technischer-support/

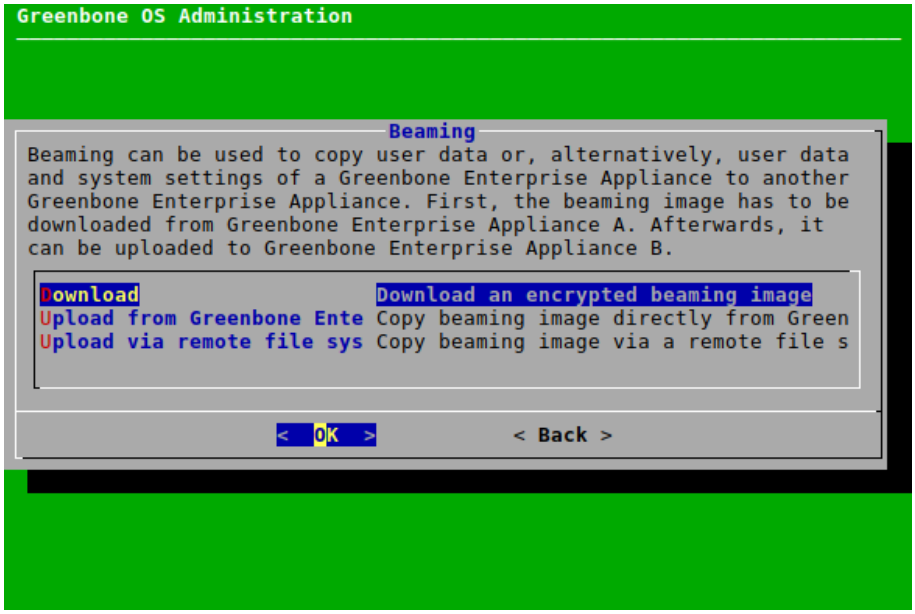


Abb. 7.66: Herunterladen des Beaming-Images

Wenn die Erstellung abgeschlossen ist, weist eine Meldung darauf hin, dass ein zu notierendes Passwort angezeigt werden wird.

4. `Enter` drücken.
5. Passwort notieren. Es wird in Schritt 13 benötigt.
6. `q` drücken, um den Editor zu verlassen.

Wichtig: Meldung, die die URL anzeigt, nicht schließen.

---

7. Im GOS-Administrationsmenü von Appliance B *Maintenance* wählen und `Enter` drücken.
8. *Beaming* wählen und `Enter` drücken.
9. *Upload from Greenbone Enterprise Appliance A* wählen und `Enter` drücken.
10. URL, die im GOS-Administrationsmenü von Appliance A angezeigt wird, in das Eingabefeld eingeben und `Enter` drücken.
11. *Yes* wählen und `Enter` drücken, falls sowohl Nutzerdaten als auch Systemeinstellungen hochgeladen werden sollen.

    oder

11. *No* wählen und `Enter` drücken, falls nur Nutzerdaten hochgeladen werden sollen.

    → Eine Warnung fordert den Benutzer auf, den Vorgang zu bestätigen.
12. *Yes* wählen und `Enter` drücken.
13. Passwort aus Schritt 5 in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.68).

    → Eine Meldung weist darauf hin, dass der Upload des Beaming-Images im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

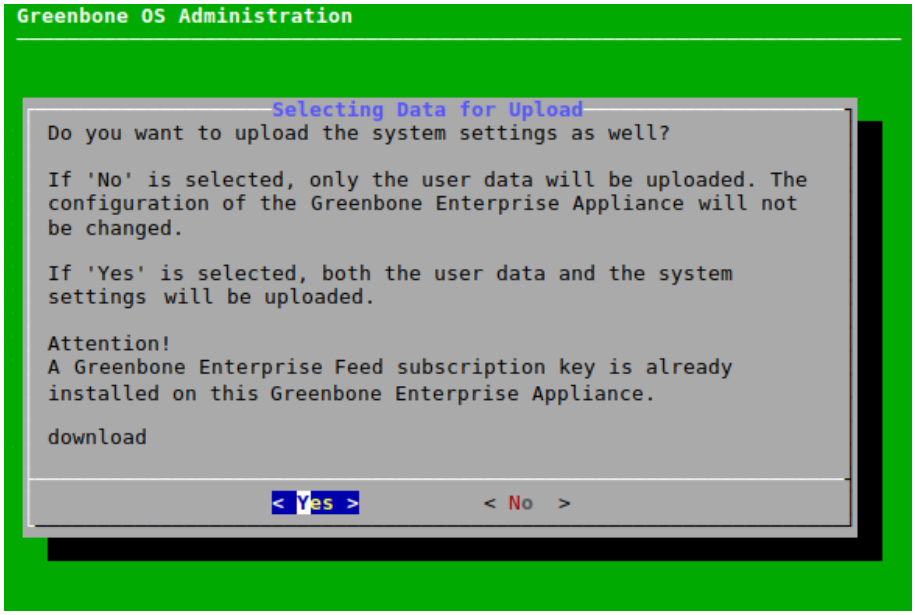


Abb. 7.67: Wählen der Daten und Einstellungen für den Upload

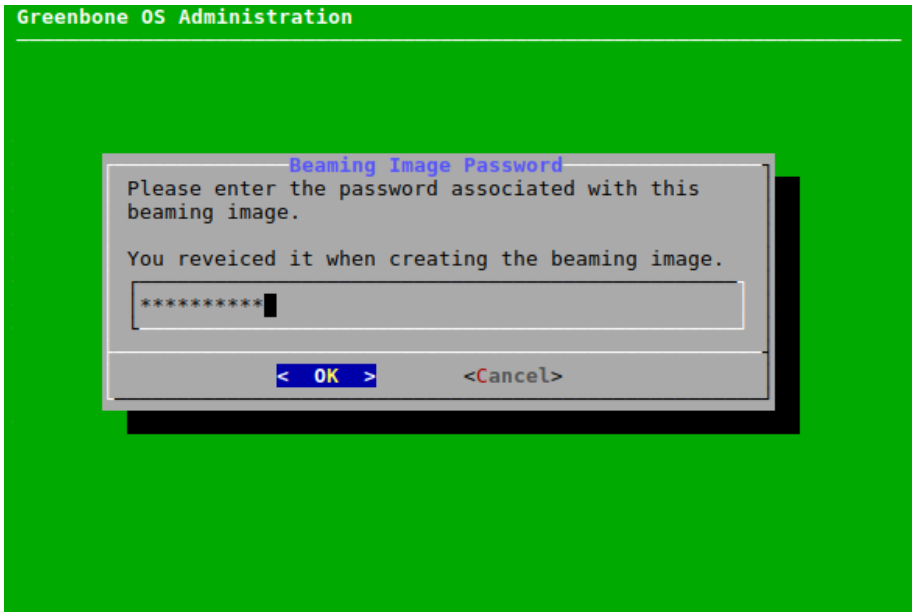


Abb. 7.68: Eingeben des Passworts für das Beaming-Image

Wenn der Upload abgeschlossen ist, wird eine Meldung angezeigt.

14. `Enter` drücken.

7.3.3.2 Beaming über ein Remote-Dateisystem durchführen

Das Beaming-Image kann wie folgt erstellt, heruntergeladen, gespeichert und später über ein Remote-Dateisystem importiert werden:

Bemerkung:

- Appliance A = sendende Appliance
- Appliance B = empfangende Appliance

---

1. Im GOS-Administrationsmenü von Appliance A *Maintenance* wählen und `Enter` drücken.
2. *Beaming* wählen und `Enter` drücken.
3. *Download* wählen und `Enter` drücken (siehe Abb. 7.69).

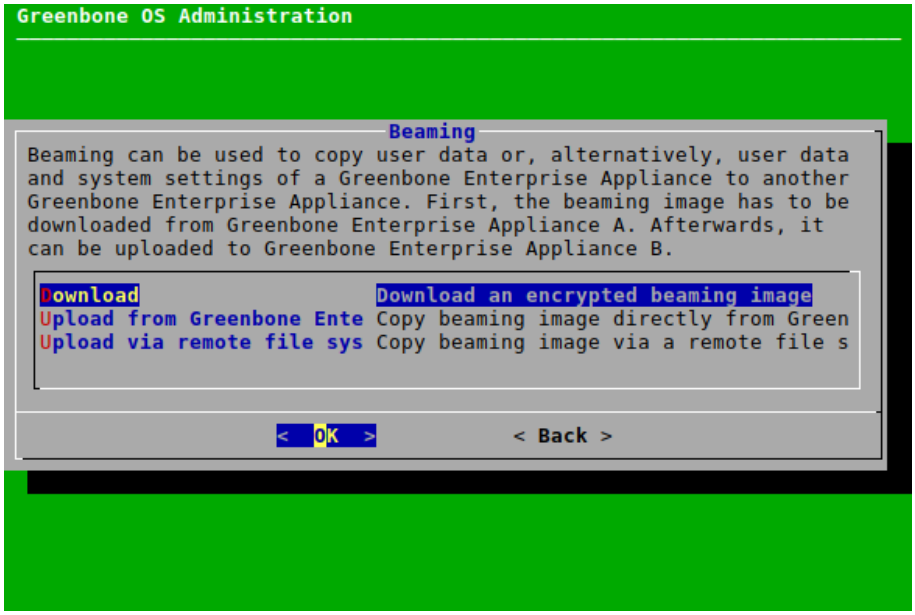


Abb. 7.69: Herunterladen des Beaming-Images

→ Eine Meldung weist darauf hin, dass die Erstellung des Beaming-Images im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

Wenn die Erstellung abgeschlossen ist, weist eine Meldung darauf hin, dass ein zu notierendes Passwort angezeigt werden wird.

4. `Enter` drücken.
5. Passwort notieren. Es wird in Schritt 16 benötigt.
6. `q` drücken, um den Editor zu verlassen.

7. Webbrowser öffnen und angezeigte URL eingeben.
8. GSMB-Datei herunterladen.
9. Im GOS-Administrationsmenü von Appliance B *Maintenance* wählen und `Enter` drücken.
10. *Beaming* wählen und `Enter` drücken.
11. *Upload via remote file system* wählen und `Enter` drücken.
12. Webbrowser öffnen und angezeigte URL eingeben.
13. Auf *Browse...* klicken, die GSMB-Datei wählen und auf *Upload* klicken.

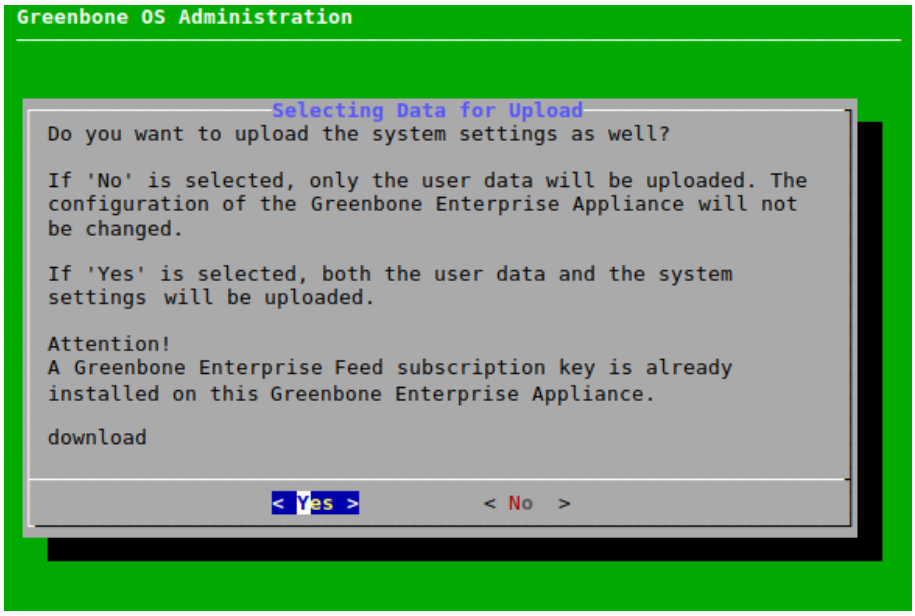


Abb. 7.70: Wählen der Daten und Einstellungen für den Upload

14. *Yes* wählen und `Enter` drücken, falls sowohl Nutzerdaten als auch Systemeinstellungen hochgeladen werden sollen.

    oder

14. *No* wählen und `Enter` drücken, falls nur Nutzerdaten hochgeladen werden sollen.

    → Eine Warnung fordert den Benutzer auf, den Vorgang zu bestätigen.

15. *Yes* wählen und `Enter` drücken.
16. Passwort aus Schritt 5 in das Eingabefeld eingeben und `Enter` drücken (siehe Abb. 7.71).

    → Eine Meldung weist darauf hin, dass der Upload des Beaming-Images im Hintergrund gestartet wurde.

    Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

    Wenn der Upload abgeschlossen ist, wird eine Meldung angezeigt.

17. `Enter` drücken.

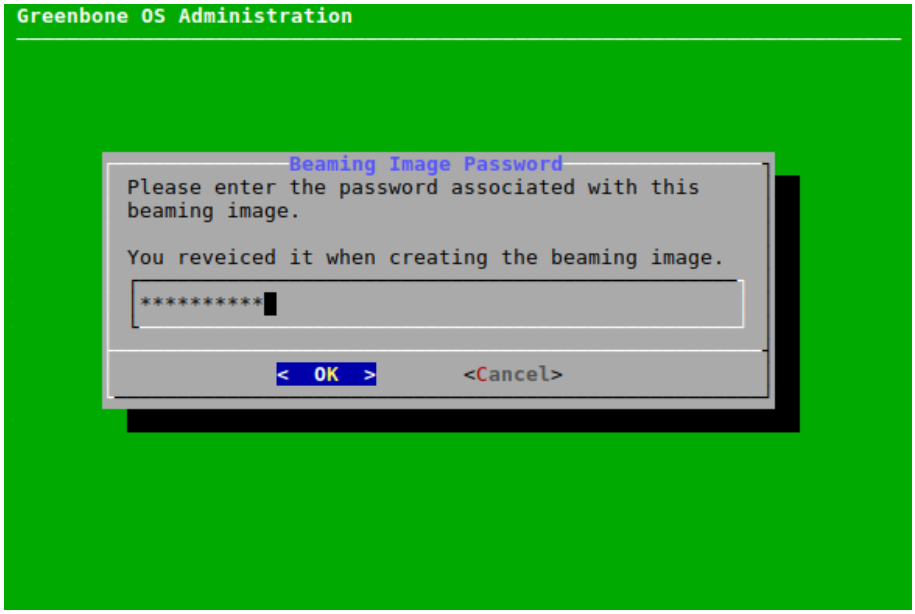


Abb. 7.71: Eingeben des Passworts für das Beaming-Image

7.3.4 Ein GOS-Upgrade durchführen

Während des täglichen Feed-Updates zur Wartungszeit (siehe Kapitel *7.2.13* (Seite 137)) lädt die Appliance auch neue GOS-Upgrades herunter, sofern verfügbar. Die Upgrades werden zwar automatisch heruntergeladen, aber nicht automatisch installiert.

Bemerkung: Da die Upgrades laufende Scanaufgaben unterbrechen können, müssen sie sorgfältig geplant werden.

Upgrades können wie folgt manuell installiert werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Upgrade* wählen und `Enter` drücken.
3. *Upgrade* wählen und `Enter` drücken, um ein Upgrade zu installieren.

   oder

3. *Switch Release* wählen und `Enter` drücken, um zu einem neuen Softwarerelease zu wechseln.

   → Eine Meldung weist darauf hin, dass das Upgrade im Hintergrund gestartet wurde.

   Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

Bemerkung: Treten nach einem GOS-Upgrade Fehler bei der Benutzung der Web-Oberfläche auf, muss der Browser- oder Seitencache geleert werden(siehe Kapitel *6.4* (Seite 61)).

Es ist möglich, dass ein GOS-Upgrade die über das GOS-Administrationsmenü verfügbaren Funktionen verändert. Diese geänderten Funktionen sind erst nach einem erneuten Laden des GOS-Administrationsmenüs verfügbar. Es wird daher empfohlen, sich nach dem GOS-Upgrade vom GOS-Administrationsmenü abzumelden und wieder neu anzumelden.

Gelegentlich ist auch ein Neustart der Appliance erforderlich (siehe Kapitel *7.3.9.1* (Seite 154)). Der Self-Check zeigt in diesem Fall einen entsprechenden Hinweis an (siehe Kapitel *7.3.1* (Seite 138)).

Bemerkung: Ein erfolgreiches GOS-Upgrade auf dem Master startet standardmäßig auch ein GOS-Upgrade auf den angeschlossenen Sensoren. Ein Upgrade kann jedoch auch manuell auf den Sensoren installiert werden (siehe Kapitel *7.3.5* (Seite 151)).

7.3.5 Ein GOS-Upgrade auf Sensoren durchführen

Ein GOS-Upgrade kann wie folgt auf einem Sensor installiert werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Upgrade* wählen und `Enter` drücken.
3. *Sensors* wählen und `Enter` drücken.
4. Gewünschten Sensor wählen und `Leertaste` drücken.

   → Der Sensor wird mit * markiert. Es können mehrere Sensoren zur gleichen Zeit gewählt werden.

   Sensoren, die nicht für ein Upgrade bereit sind, sind entsprechend gekennzeichnet.
5. `Enter` drücken.

   → Eine Meldung weist darauf hin, dass das Upgrade im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

7.3.6 Ein Feed-Update durchführen

Standardmäßig versucht die Appliance, Feed-Updates und GOS-Upgrades täglich zu ihrer Wartungszeit (siehe Kapitel *7.2.13* (Seite 137)) herunterzuladen.

Außerdem kann ein Feed-Update wie folgt manuell ausgelöst werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Update* wählen und `Enter` drücken (siehe Abb. 7.72).

   → Eine Meldung weist darauf hin, dass das Feed-Update im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

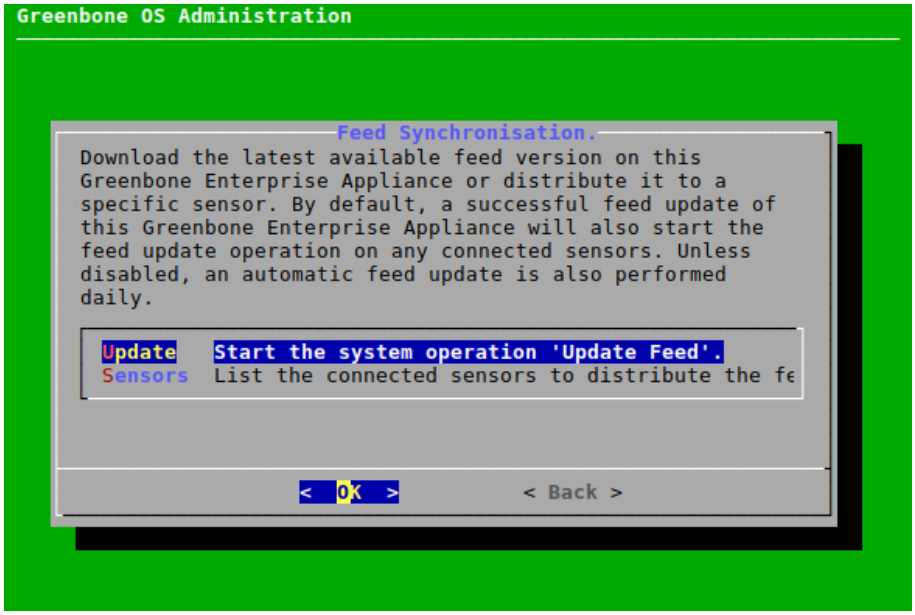


Abb. 7.72: Manuelles Auslösen eines Feed-Updates

Bemerkung: Standardmäßig wird ein erfolgreiches Feed-Update auf dem Master auch ein Feed-Update auf den angeschlossenen Sensoren starten. Ein Feed-Update kann jedoch auch manuell an die Sensoren übertragen werden (siehe Kapitel *7.3.7* (Seite 152)).

7.3.7 Ein Feed-Update auf Sensoren durchführen

Ein Feed-Update kann wie folgt auf einen Sensor übertragen werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Sensors* wählen und `Enter` drücken.
4. Gewünschten Sensor wählen und `Enter` drücken (siehe Abb. 7.73).

   → Eine Meldung weist darauf hin, dass das Feed-Update im Hintergrund gestartet wurde.

Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

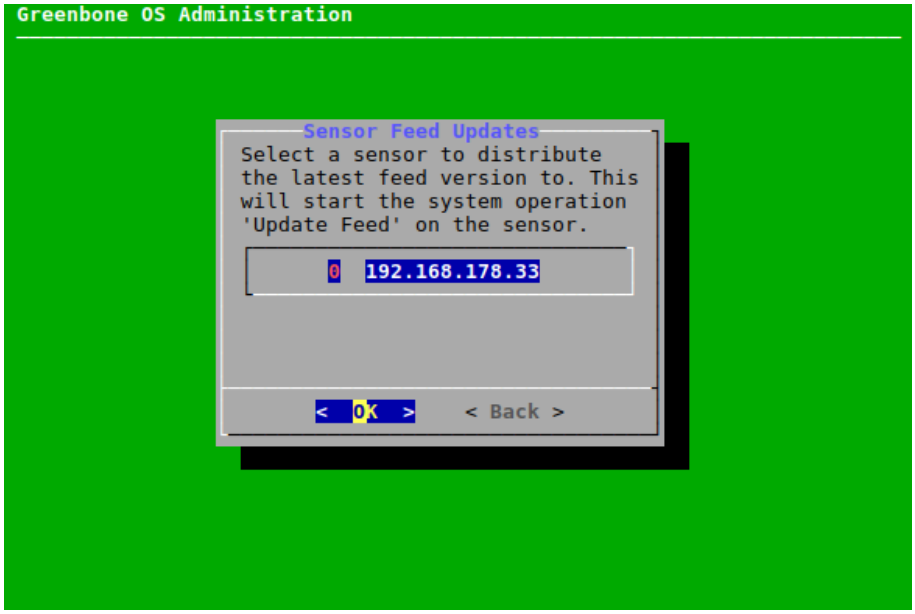


Abb. 7.73: Wählen des Sensors

7.3.8 Die Flash-Partition upgraden

Die Flash-Partition wird für die Durchführung von Resets der Appliance verwendet. Um Factory-Resets zu vereinfachen, sollte sie regelmäßig auf die neueste GOS-Version aktualisiert werden.

Bemerkung: Es muss sichergestellt werden, dass die Appliance selbst eine Verbindung zum Greenbone Feed Server herstellen kann.

Es ist nicht möglich, die Flash-Partitionen von Sensoren über den Master zu aktualisieren.

Die Flash-Partition kann wie folgt aktualisiert werden:

1. Appliance auf die letzte GOS-Version upgraden (siehe Kapitel *7.3.4* (Seite 150)).
2. *Maintenance* wählen und `Enter` drücken.
3. *Flash* wählen und `Enter` drücken.
4. *Download* wählen und `Enter` drücken (siehe Abb. 7.74).

   → Das neueste Flash-Image wird heruntergeladen.

   Tipp: Der Download-Status kann in den Live-Logs (*Advanced* > *Logs* > *Live*, siehe Kapitel *7.4.1* (Seite 156)) überwacht werden.

   ---

5. Wenn das Herunterladen beendet ist, *Write* wählen und `Enter` drücken (siehe Abb. 7.74) .

   → Das Image wird auf die Flash-Partition geschrieben. Der Vorgang kann bis zu 20 Minuten dauern.

   Tipp: Die momentan laufende Systemoperation kann durch Wählen von *About* und Drücken von `Enter` im GOS-Administrationsmenü angezeigt werden.

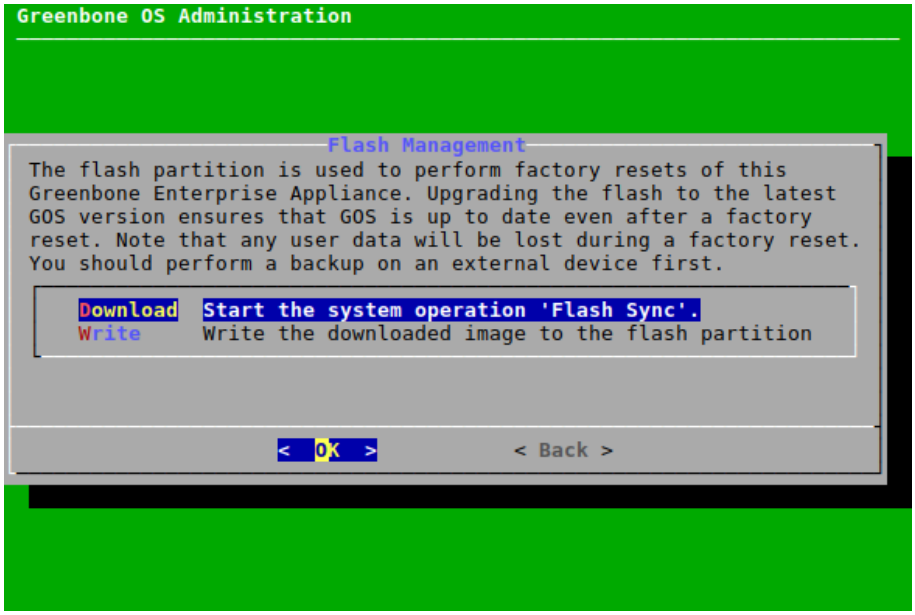


Abb. 7.74: Aktualisieren der Flash-Partition

7.3.9 Die Appliance herunterfahren und neu starten

Bemerkung: Die Appliance sollte nicht über den Netzschalter ausgeschaltet werden.

Stattdessen sollte die Appliance über das GOS-Administrationsmenü heruntergefahren und neu gestartet werden. Dadurch wird sichergestellt, dass die obligatorischen Bereinigungsprozesse während des Herunterfahrens und Neustarts ausgeführt werden.

7.3.9.1 Die Appliance neu starten

Die Appliance kann wie folgt neu gestartet werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Power* wählen und `Enter` drücken.
3. *Reboot* wählen und `Enter` drücken.

   → Eine Meldung fordert den Benutzer auf, den Neustart zu bestätigen (siehe Abb. 7.75).
4. *Yes* wählen und `Enter` drücken.

   → Die Appliance startet neu. Der Vorgang kann einige Minuten dauern.

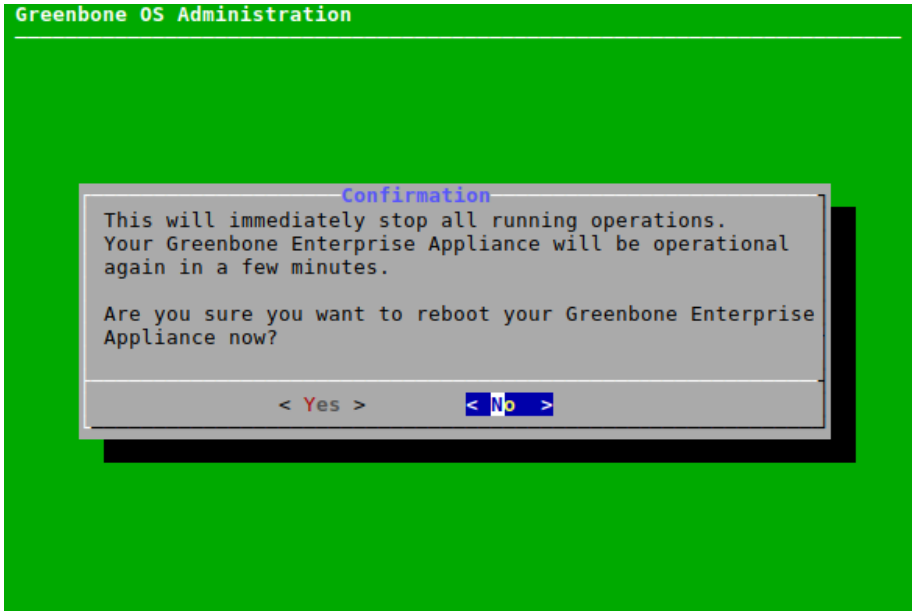


Abb. 7.75: Neustarten der Appliance

7.3.9.2 Die Appliance herunterfahren

Die Appliance kann wie folgt heruntergefahren werden:

1. *Maintenance* wählen und `Enter` drücken.
2. *Power* wählen und `Enter` drücken.
3. *Shutdown* wählen und `Enter` drücken.

   → Eine Meldung fordert den Benutzer auf, das Herunterfahren zu bestätigen (siehe Abb. 7.76).

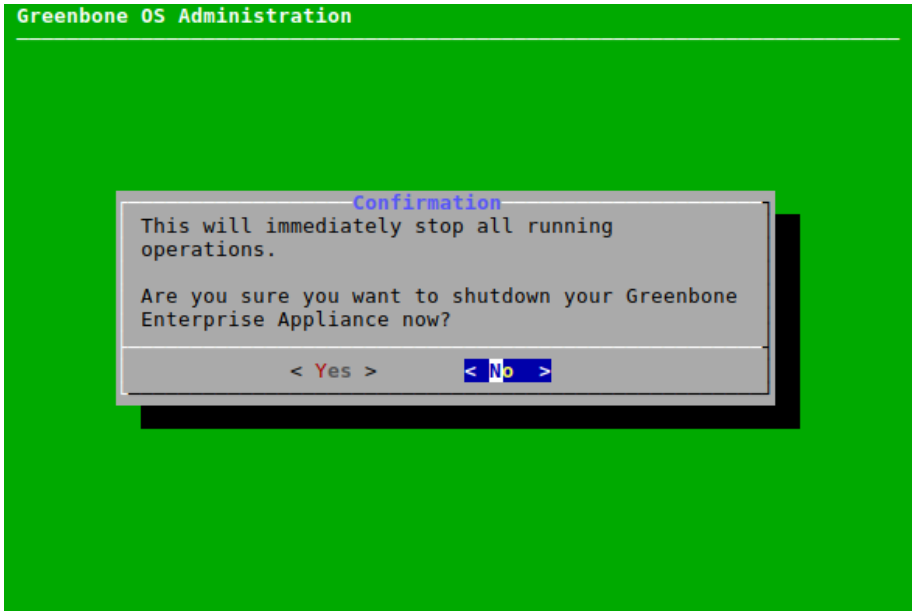


Abb. 7.76: Herunterfahren der Appliance

4. *Yes* wählen und `Enter` drücken.

   → Die Appliance fährt herunter. Der Vorgang kann einige Minuten dauern.

7.4 Advanced-Menü

7.4.1 Die Log-Dateien der Appliance anzeigen

Die Log-Dateien der Appliance können wie folgt angezeigt werden:

1. *Advanced* wählen und `Enter` drücken.
2. *Logs* wählen und `Enter` drücken.
3. Gewünschte Logs wählen und `Enter` drücken (siehe Abb. 7.77).

   → Die Log-Dateien werden in einem Viewer angezeigt.
4. `q` oder `Strg` + `C` drücken, um den Viewer zu verlassen.

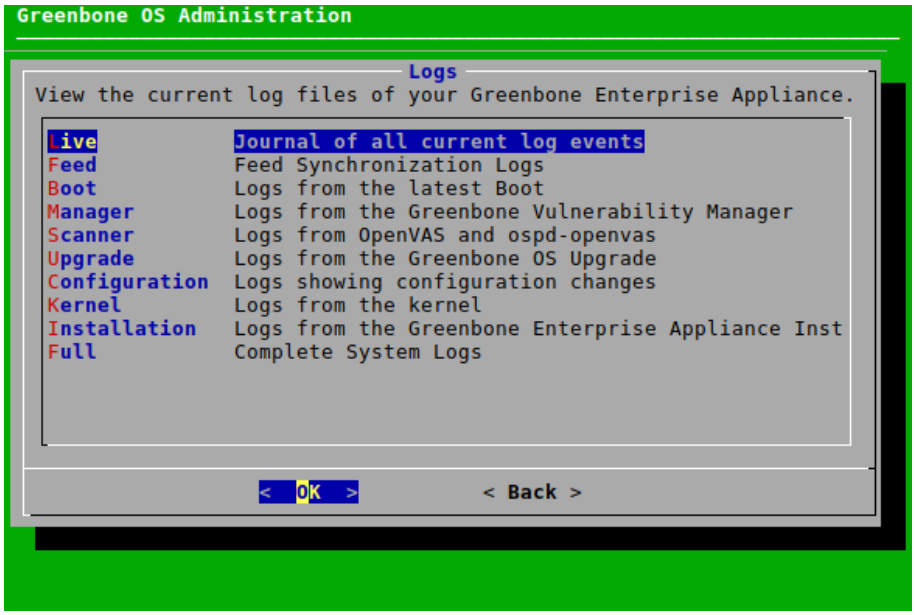


Abb. 7.77: Wählen der Log-Dateien

7.4.2 Fortgeschrittene, administrative Tätigkeiten durchführen

7.4.2.1 Den Superuser-Account verwalten

Wenn auf die Shell zugegriffen wird, wird eine Linux-Befehlszeile mit dem unprivilegierten Benutzer *admin* angezeigt (siehe Kapitel *7.4.2.3* (Seite 160)). Jeder Debian GNU/Linux-Befehl kann ausgeführt werden, allerdings können einige Befehle auf den privilegierten Benutzer *root* beschränkt sein.

Bemerkung: Der privilegierte Account *root* (Superuser) sollte nur in Absprache mit dem Greenbone Enterprise Support[21] genutzt werden.

Werden Änderungen ohne Rücksprache vorgenommen, erlischt der Anspruch auf Unterstützung durch den Greenbone Enterprise Support.

Um Root-Rechte auf der Appliance zu erhalten, muss der Befehl `su -` in der Shell eingegeben werden. Die Verwendung von `su -` zum Wechsel vom Benutzer *admin* zum Benutzer *root* ist standardmäßig deaktiviert.

Der Superuser muss wie folgt aktiviert und mit einem Passwort ausgestattet werden:

1. *Advanced* wählen und `Enter` drücken.
2. *Support* wählen und `Enter` drücken.
3. *Superuser* wählen und `Enter` drücken.
4. *Superuser State* wählen und `Enter` drücken (siehe Abb. 7.78).

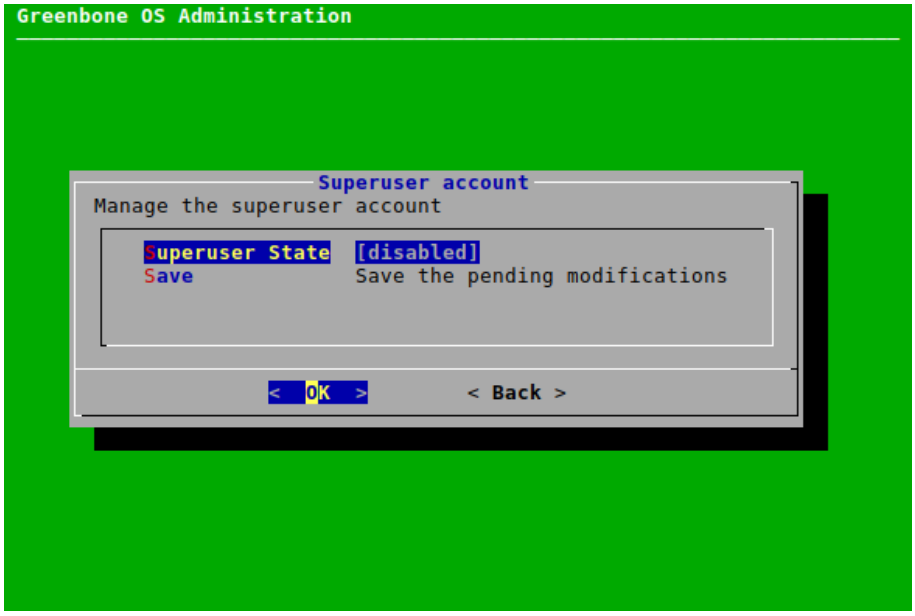


Abb. 7.78: Aktivieren des Superusers

→ Eine Warnung weist darauf hin, dass Root-Rechte nur in Ausnahmefällen und in Abstimmung mit dem Greenbone Enterprise Support erlangt werden sollten.

5. *Yes* wählen und `Enter` drücken.

   → Eine Meldung weist darauf hin, dass die Änderungen gespeichert werden müssen.

6. `Enter` drücken, um die Meldung zu schließen.

[21] https://www.greenbone.net/technischer-support/

7. *Password* wählen und `Enter` drücken.
8. Passwort zweimal eingeben, *OK* wählen und `Enter` drücken (siehe Abb. 7.79).

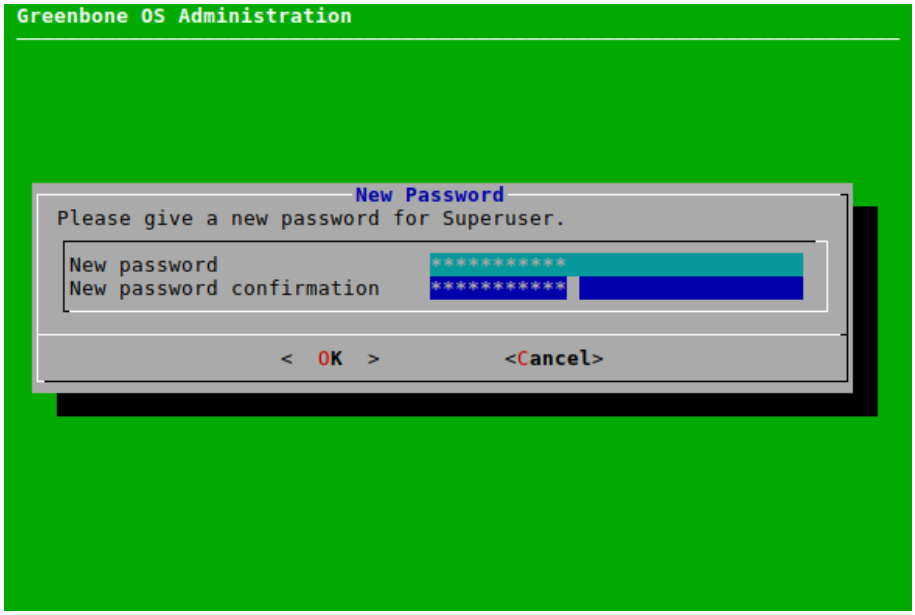


Abb. 7.79: Festlegen des Passworts des Superusers

7.4.2.2 Ein Supportpaket generieren und herunterladen

Manchmal benötigt der Greenbone Enterprise Support zusätzliche Informationen, um Fehler zu beheben und die Kundschaft zu unterstützen. Die erforderlichen Daten werden als (verschlüsseltes) Supportpaket gesammelt, das alle Konfigurationsdaten der Appliance enthält.

Das Paket kann mit dem öffentlichen GPG-Schlüssel des Greenbone Enterprise Supports verschlüsselt werden. Das Supportpaket wird auf der Appliance gespeichert.

Ein Supportpaket kann wie folgt erstellt werden:

1. *Advanced* wählen und `Enter` drücken.
2. *Support* wählen und `Enter` drücken.
3. *Support Package* wählen und `Enter` drücken.

   → Eine Meldung fordert den Benutzer auf, die Generierung des Supportpakets zu bestätigen.
4. *Yes* wählen und `Enter` drücken.

   → Eine Meldung fragt, ob das Supportpaket verschlüsselt werden soll (siehe Abb. 7.80).
5. *Yes* wählen und `Enter` drücken, um das Supportpaket zu verschlüsseln.

   oder
5. *No* wählen und `Enter` drücken, um das Supportpaket nicht zu verschlüsseln.

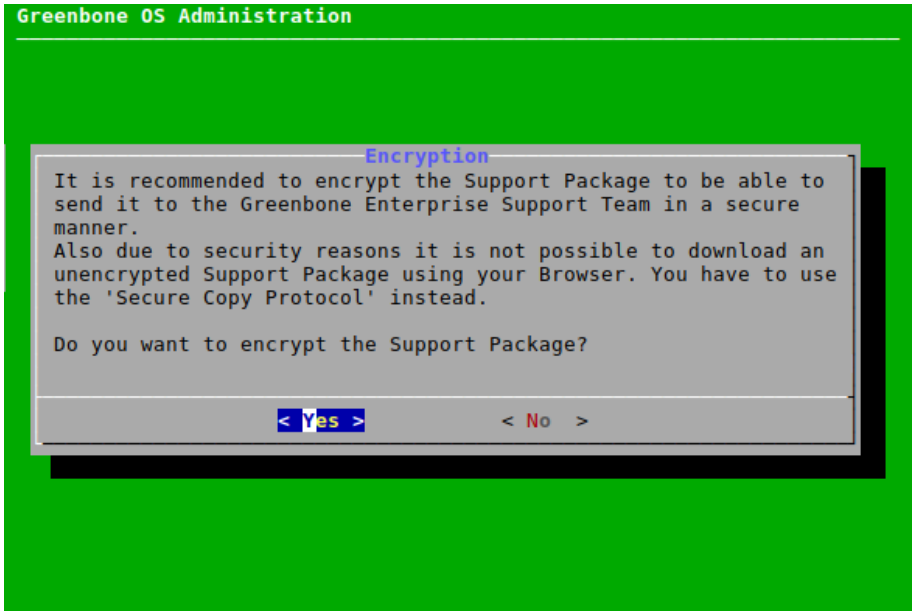


Abb. 7.80: Herunterladen eines Supportpakets

6. Falls ein verschlüsseltes Supportpaket gewählt wurde, Webbrowser öffnen, angezeigte URL eingeben und GPG-Schlüssel herunterladen (verschlüsselter ZIP-Ordner).

   oder

   Bemerkung: Falls das Support Package nicht verschlüsselt ist, muss der Download über das Secure Copy Protocol (SCP) erfolgen. Dazu muss zunächst SSH aktiviert werden (siehe Kapitel *7.2.4.4* (Seite 107)).

6. Falls ein unverschlüsseltes Supportpaket gewählt wurde, angezeigten Befehl mithilfe von SCP eingeben (siehe Abb. 7.81) und Supportpaket (ZIP-Ordner) herunterladen.

   Bemerkung: Der „.“ am Ende kann durch einen Pfad ersetzt werden. Falls der „.“ beibehalten wird, wird der aktuelle Ordner genutzt.

7. ZIP-Ordner an den Greenbone Enterprise Support[22] senden.

Auf Microsoft Windows-Systemen kann das Supportpaket entweder mit `pscp`, einem in PuTTY enthaltenen Kommandozeilenwerkzeug, oder mit smarTTY, einem grafischen Werkzeug, das SCP implementiert, heruntergeladen werden.

[22] https://www.greenbone.net/technischer-support/

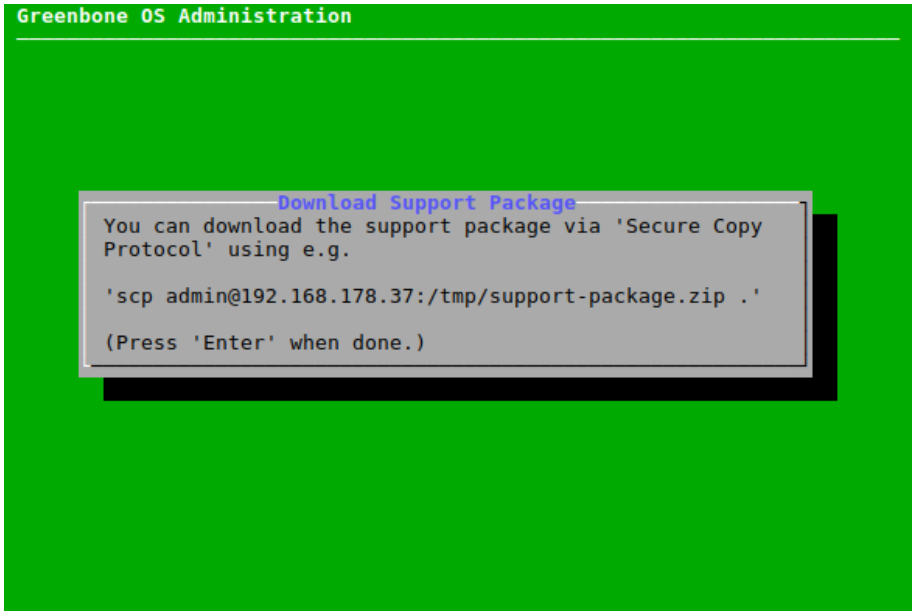


Abb. 7.81: Herunterladen eines unverschlüsselten Supportpakets

7.4.2.3 Auf die Shell zugreifen

Der Shell-Zugang ist für administrative Arbeiten nicht erforderlich, kann aber vom Greenbone Enterprise Support zu Diagnose- und Support angefordert werden.

Auf die Shell kann wie folgt zugegriffen werden:

1. *Advanced* wählen und `Enter` drücken.
2. *Support* wählen und `Enter` drücken.
3. *Shell* wählen und `Enter` drücken.

   → Eine Warnung informiert darüber, dass die Shellebene nicht dokumentiert wird und nicht für administrative Einstellungen genutzt werden sollte (siehe Abb. 7.82).
4. *Continue* wählen und `Enter` drücken.

   → Eine Linux-Shell wird mit dem unprivilegierten Benutzer *admin* geöffnet (siehe Abb. 7.83).

   Bemerkung: Der Zugriff als *root* erfordert die Aktivierung des Superusers und das Setzen eines Passworts (siehe Kapitel *7.4.2.1* (Seite 157)). Danach ist der Wechsel zu *root* mit dem Befehl `su -` möglich.

   ---
5. `exit` eingeben oder `Strg` + `D` drücken, um die Shell zu verlassen.

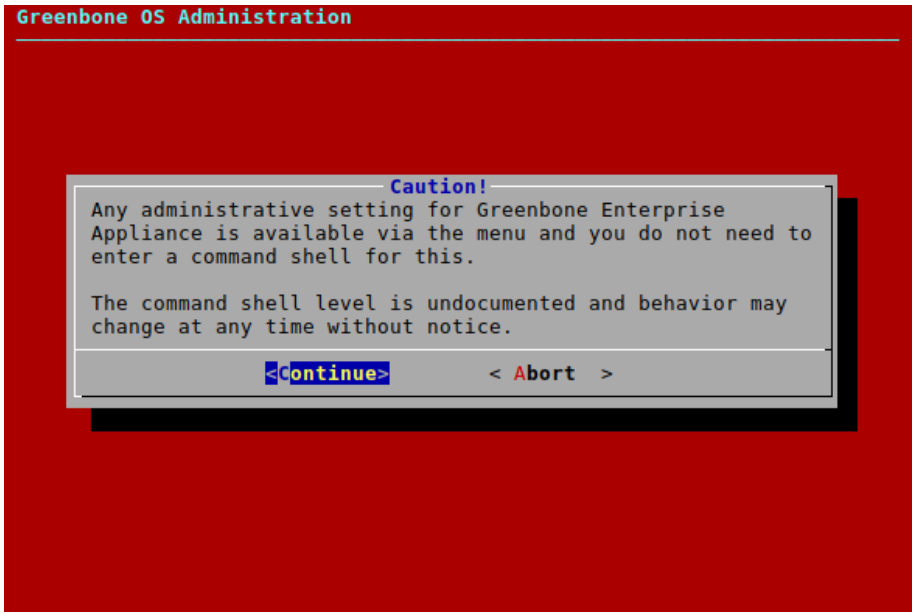


Abb. 7.82: Warnung beim Zugriff auf die Shell

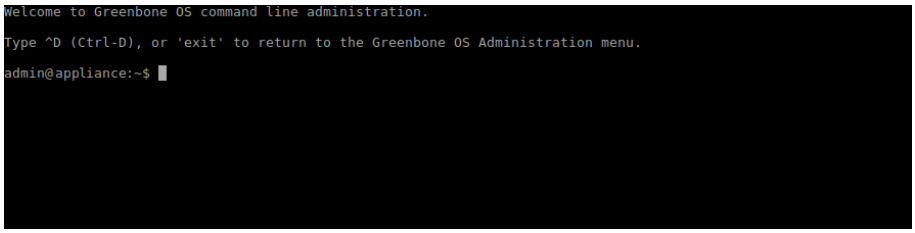


Abb. 7.83: Zugriff auf die lokale Shell

7.4.3 Den Greenbone-Enterprise-Feed-Subskription-Schlüssel anzeigen

Der Subskription-Schlüssel (siehe Kapitel *7.2.7.1* (Seite 118)) kann wie folgt angezeigt werden:

1. *Advanced* wählen und `Enter` drücken.
2. *Subscription* wählen und `Enter` drücken (siehe Abb. 7.84).

   → Der Subskription-Schlüssel wird in einem Viewer angezeigt.
3. `q` drücken, um den Viewer zu verlassen.

7.4.4 Die Copyright- und Lizenzinformationen anzeigen

Die Copyright-Datei kann wie folgt angezeigt werden:

1. *Advanced* wählen und `Enter` drücken.
2. *Copyright and Licenses* wählen und `Enter` drücken (siehe Abb. 7.84).

   → Die Copyright-Datei wird in einem Viewer angezeigt.
3. `q` drücken, um den Viewer zu verlassen.

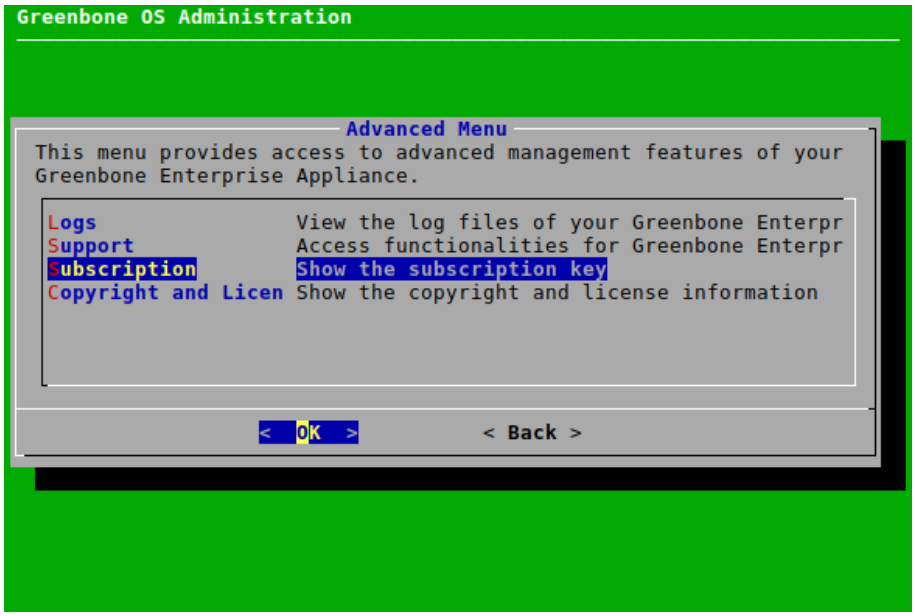


Abb. 7.84: Anzeigen des Subskription-Schlüssels oder der Copyright-Datei

7.5 Informationen über die Appliance anzeigen

Informationen über die Appliance können durch Wählen von *About* und Drücken von `Enter` angezeigt werden.

Die folgenden Informationen werden angezeigt:

- Appliance-Modell
- GOS-Version
- Feedversion
- Name des Subskription-Schlüssels
- IP-Adresse der Web-Oberfläche
- Konfigurierte Sensoren
- Aktuell laufende Systemoperationen

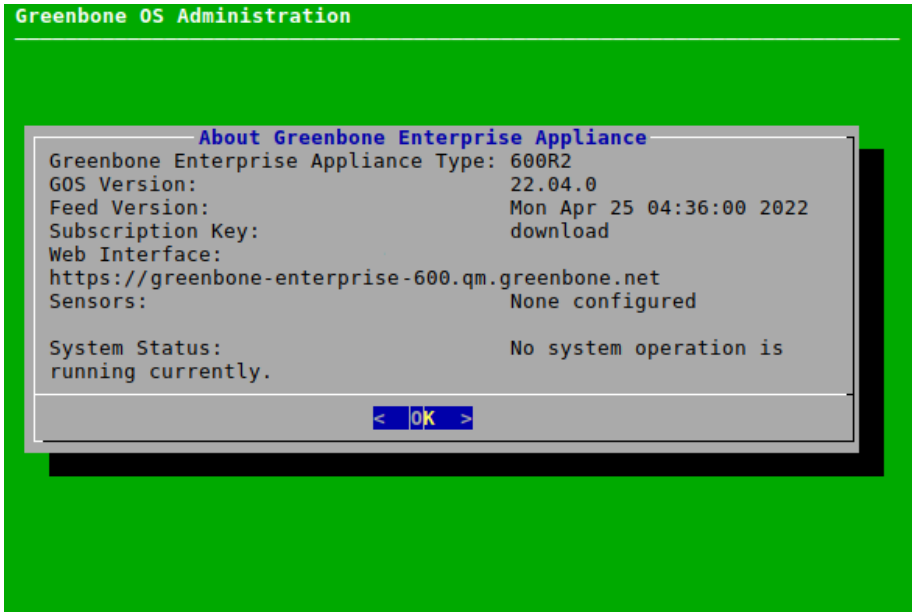


Abb. 7.85: Informationen über die Appliance anzeigen

KAPITEL 8

Die Web-Oberfläche kennenlernen

8.1 In die Web-Oberfläche einloggen

Die wichtigste Schnittstelle der Appliance ist die Web-Oberfläche, auch Greenbone Security Assistant (GSA) genannt. Die Web-Oberfläche kann wie folgt aufgerufen werden:

1. Webbrowser öffnen.
2. IP-Adresse der Web-Oberfläche der Appliance eingeben.

   Tipp: Die IP-Adresse der Web-Oberfläche der Appliance kann entweder beim Login in die Konsole angezeigt werden oder indem im GOS Administrationsmenü *About* gewählt und `Enter` gedrückt wird.

3. Mit dem Web-Administrator, der während des Setups erstellt wurde (siehe Kapitel *5* (Seite 28)), einloggen.

8.2 Dashboards und Dashboardanzeigen

Abhängig vom Seiteninhalt zeigen viele Seiten der Web-Oberfläche Dashboardanzeigen oben auf der Seite.

Es gibt zwei Arten von Dashboardanzeigen: Diagramme und Tabellen.

Für jede Seite gibt es eine Standardeinstellung von Anzeigen. Die Standardeinstellung kann durch Klicken auf ↻ auf der rechten Seite über den Anzeigen wiederhergestellt werden.

8.2.1 Dashboardanzeigen hinzufügen und entfernen

Eine neue Anzeige kann wie folgt hinzugefügt werden:

1. Auf der rechten Seite über den Anzeigen auf ⊡★ klicken.
2. Gewünschte Anzeige in der Drop-down-Liste auswählen (siehe Abb. 8.1).

Tipp: Das Eingabefeld über den wählbaren Optionen kann genutzt werden, um die Optionen zu filtern.

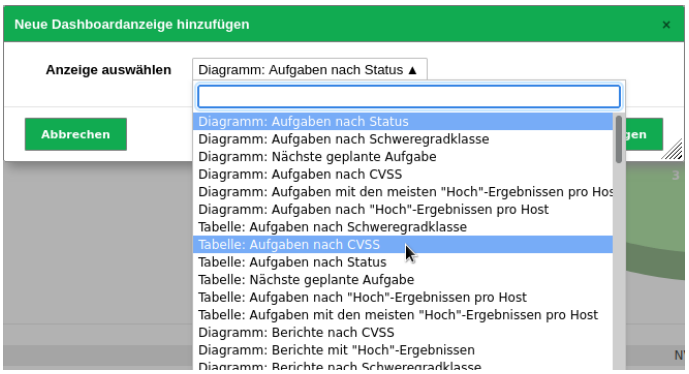


Abb. 8.1: Hinzufügen einer Anzeige

3. Auf *Hinzufügen* klicken.

Eine Anzeige kann durch Klicken auf ✕ in der rechten oberen Ecke der Anzeige gelöscht werden (siehe Abb. 8.2).

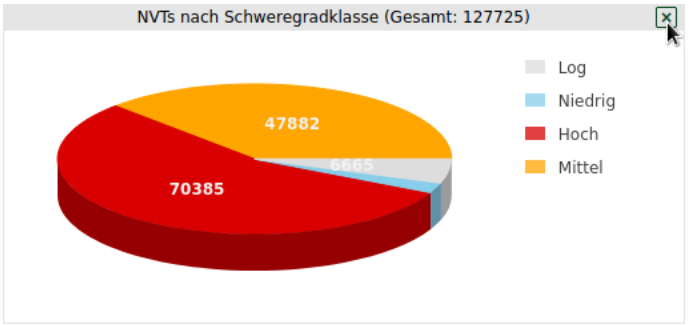


Abb. 8.2: Löschen einer Anzeige

8.2.2 Eine Dashboardanzeige bearbeiten

Abhängig von der Anzeige können verschiedene Optionen gewählt werden, indem die Maus zum rechten Rand der Anzeige bewegt wird (siehe Abb. 8.3):

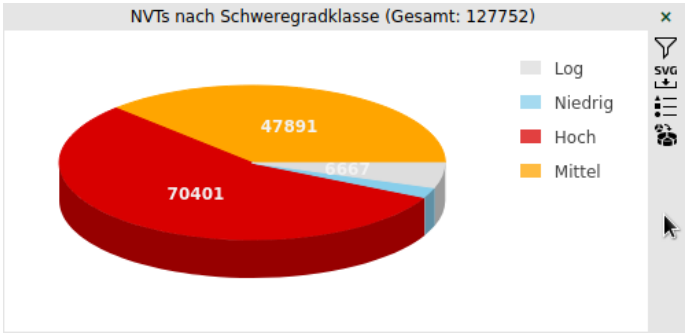


Abb. 8.3: Optionen für eine Anzeige wählen

- Einen Filter auf die Anzeige anwenden. Der Filter muss für den Objekttyp, der in der Anzeige dargestellt ist, konfiguriert sein.
- Das Diagramm als eine SVG-Datei herunterladen (nur für Diagramme).
- Die Tabelle als eine CSV-Datei herunterladen (nur für Tabellen).
- Eine Legende ein- oder ausblenden (nur für Diagramme).
- Zwischen 2D- und 3D-Darstellung wechseln (nur für Diagramme).

8.2.3 Anzeigen in Dashboards organisieren

Dashboardanzeigen können zu Dashboards zusammengefasst werden. Dashboards können individuelle Sammlungen von Anzeigen sein, allerdings stehen auch vordefinierte Dashboards zur Verfügung, die gewählt werden können.

Es kann bis zu 10 Dashboards geben.

Standardmäßig gibt es nur das Dashboard *Übersicht*, welches einen kurzen Überblick über Aufgaben, CVEs und VTs gibt (siehe Abb. 8.4).

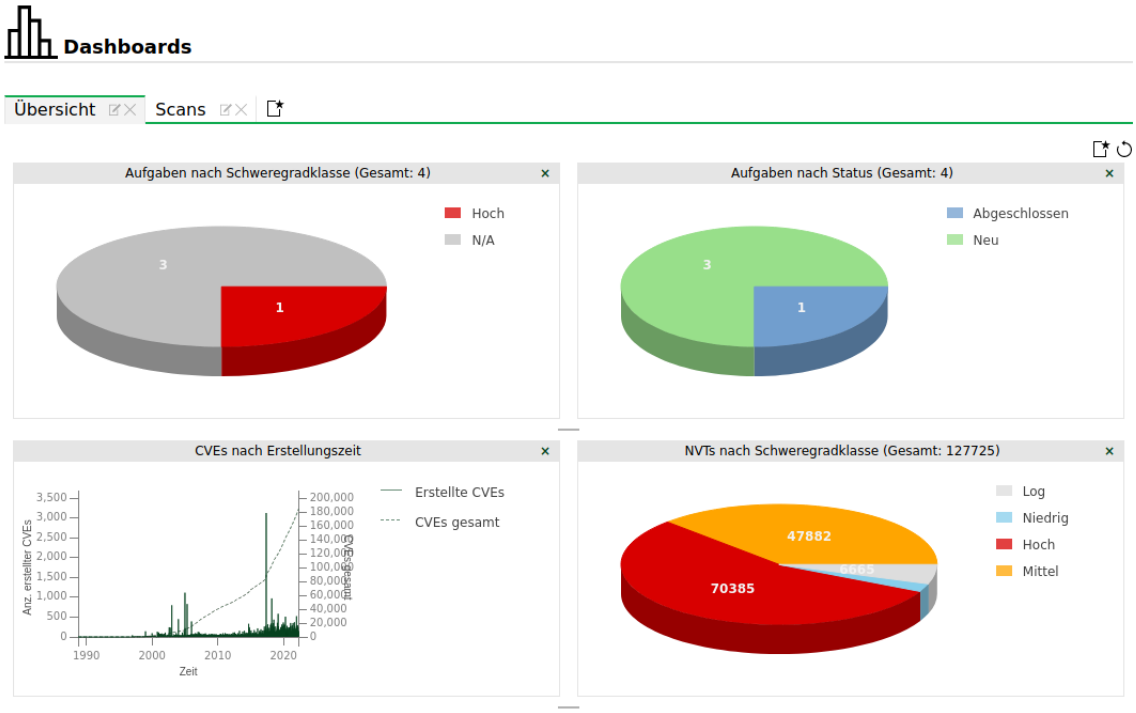


Abb. 8.4: Dashboard *Übersicht*

Die Dashboards können angezeigt werden, indem *Dashboards* in der Menüleiste gewählt wird.

8.2.3.1 Ein neues Dashboard hinzufügen

Ein neues Dashboard kann wie folgt erstellt werden:

1. In der Registerleiste über den Dashboards auf klicken (siehe Abb. 8.5).

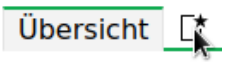


Abb. 8.5: Hinzufügen eines neuen Dashboards

2. Namen des Dashboards in das Eingabefeld *Dashboard-Titel* eingeben.
3. Anzeigen, die standardmäßig dargestellt werden sollen, in der Drop-down-Liste *Erste Anzeigen* auswählen (siehe Abb. 8.6).

   Die folgenden Standardeinstellungen für die dargestellten Anzeigen sind möglich:

   - Standard: Das Dashboard enthält die gleichen Anzeigen wie das Dashboard *Übersicht*.
   - Scan-Anzeigen: Das Dashboard enthält Anzeigen, die Aufgaben, Ergebnisse und Berichte betreffen.
   - Asset-Anzeigen: Das Dashboard enthält Anzeigen, die Hosts und Betriebssysteme betreffen.
   - SecInfo-Anzeigen: Das Dashboard enthält Anzeigen, die VTs, CVEs und CERT-Bund-Advisories betreffen.
   - Leeren: Das Dashboard enthält keine Anzeigen.

   Zusätzlich können bereits vorhandene Dashboards gewählt werden.

Tipp: Die Anzeigen können später auch bearbeitet werden (siehe Kapitel *8.2.1* (Seite 164) und *8.2.2* (Seite 165)).

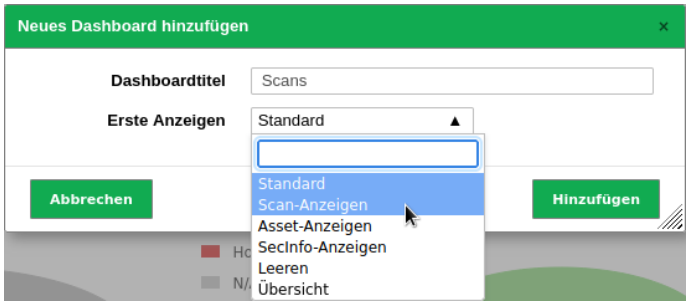


Abb. 8.6: Hinzufügen eines neuen Dashboards

4. Auf *Hinzufügen* klicken.

   → Das Dashboard wird erstellt und in der Registerleiste angezeigt (siehe Abb. 8.7).

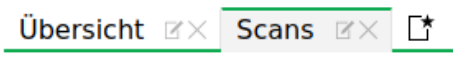


Abb. 8.7: Register der vorhandenen Dashboards

8.2.3.2 Ein Dashboard bearbeiten

Anzeigen können zu einem Dashboard hinzugefügt oder von einem Dashboard entfernt werden (siehe Kapitel *8.2.1* (Seite 164)).

Die Anzeigen eines Dashboards können bearbeitet werden (siehe Kapitel *8.2.2* (Seite 165)).

Dashboards können wie folgt umbenannt werden:

1. Im Register des Dashboards in der Registerleiste auf klicken (siehe Abb. 8.8).

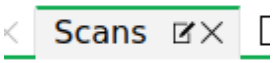


Abb. 8.8: Umbenennen oder Löschen eines Dashboards

2. Namen im Eingabefeld *Dashboard-Titel* ändern.
3. Auf *Speichern* klicken.

8.2.3.3 Ein Dashboard löschen

Ein Dashboard kann durch Klicken auf im Register des Dashboards in der Registerleiste gelöscht werden (siehe Abb. 8.8).

8.3 Den Seiteninhalt filtern

Fast jede Seite der Web-Oberfläche bietet die Möglichkeit, den angezeigten Inhalt zu filtern.

8.3.1 Die Filterparameter anpassen

Abb. 8.9: Filterleiste am oberen Rand der Seite

Mehrere Filterparameter werden kombiniert, um den Powerfilter zu bilden.

Bemerkung: Der Filter ist kontextsensitiv, was bedeutet, dass die Filterparameter von der momentan geöffneten Seite abhängen.

Die Filterparameter können entweder in das Eingabefeld in der Filterleiste (siehe Abb. 8.9) unter Verwendung der spezifischen Filtersyntax (siehe Kapitel *8.3.2* (Seite 170)) eingegeben oder wie folgt angepasst werden:

1. In der Filterleiste auf klicken (siehe Abb. 8.9).
2. Filterparameter auswählen und anpassen (siehe Abb. 8.10).

   Stichwörter, nach denen gesucht werden soll, können in das Eingabefeld *Filter* eingegeben werden.

   Bemerkung: Der Powerfilter unterscheidet nicht zwischen Groß- und Kleinbuchstaben. Alle Großbuchstaben werden vor dem Anwenden des Filters in Kleinbuchstaben umgewandelt.

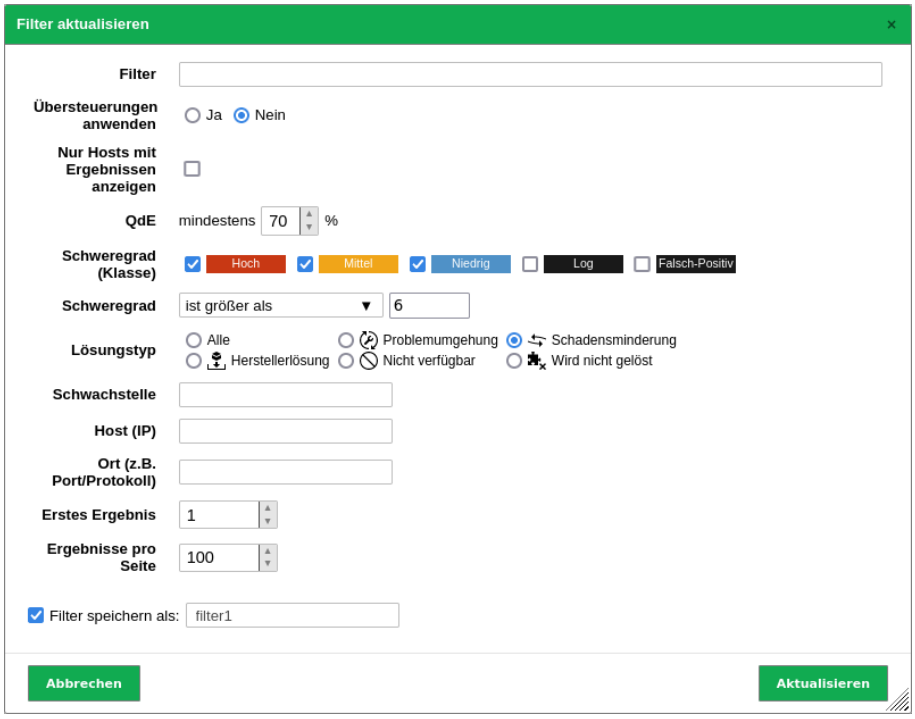


Abb. 8.10: Anpassen des Filters

3. Checkbox *Filter speichern als* aktivieren, falls der Filter für die Wiederverwendung gespeichert werden soll.
4. Namen für den Filter in das Eingabefeld *Filter speichern als* eingeben.
5. Auf *Aktualisieren* klicken.

   → Die Filterparameter werden angewendet.

Neben dem Eingabefeld in der Filterleiste sind die folgenden Aktionen verfügbar:

- Den aktuell angewendeten Filter entfernen.
- Den Filter mit der momentanen Eingabe aktualisieren.
- Filterparameter auf die Standardeinstellungen zurücksetzen.
- Ein gespeicherter Powerfilter kann angewendet, indem er in der Drop-down-Liste ausgewählt wird (siehe Abb. 8.11).

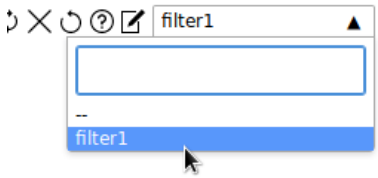


Abb. 8.11: Auswählen eines gespeicherten Powerfilters

Tipp: Falls ein bestimmter Filter immer auf einer Seite aktiviert sein soll, kann er in den Benutzereinstellungen als Standardfilter festgelegt werden (siehe Kapitel *8.7* (Seite 181)).

Powerfilter können wie folgt auch unter Nutzung der Seite *Filter* erstellt werden:

1. *Konfiguration* > *Filter* in der Menüleiste wählen.
2. Neuen Filter durch Klicken auf erstellen.
3. Namen des Filters festlegen.
4. Filterkriterien im Eingabefeld *Filterbefehl* festlegen (siehe Kapitel *8.3.2* (Seite 170)).
5. Objekttyp, für den der Filter angewendet werden soll, in der Drop-down-Liste *Typ* wählen (siehe Abb. 8.12).

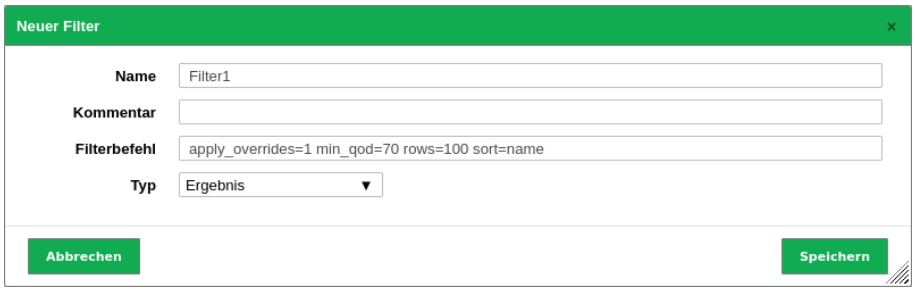


Abb. 8.12: Erstellen eines neuen Filters

6. Auf *Speichern* klicken.

   → Der Filter kann für den Objekttyp, für den er erstellt wurde, genutzt werden.

8.3.2 Filter-Stichwörter

Nach dem Anwenden werden die Filterparameter in der linken unteren Ecke der Seite angezeigt (siehe Abb. 8.13).

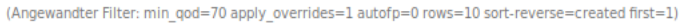


Abb. 8.13: Angewendete Filterparameter

Der Filter verwendet eine bestimmte Syntax, welche bei der direkten Eingabe der Filter-Stichwörter in das Eingabefeld in der Filterleiste zu beachten ist.

Tipp: Eine vollständige Liste aller Filter-Stichwörter mit möglichen Werten, sortiert nach Seite/Objekttyp, befindet sich hier[23].

---

[23] https://www.greenbone.net/wp-content/uploads/Filterkeywords_EN.pdf

8.3.2.1 Globale Stichwörter

Grundsätzlich ist die Angabe der folgenden Stichwörter immer möglich:

Bemerkung: Diese Stichwörter gelten für die gesamte Filteranfrage und sollten nur einmal genannt werden.

Beispiel: Filteranfragen wie `name~test and rows=20 or name~def and rows=30` sind nicht erlaubt. In diesem Fall würde nur `rows=30` angewendet werden.

- ***rows*:** Anzahl der Zeilen, die pro Seite angezeigt werden. Standardmäßig ist dieser Wert *rows=10*. Durch Eingabe des Werts `-1` werden alle Ergebnisse dargestellt. Durch Eingabe des Werts `-2` wird der Wert genutzt, der auf der Seite *Eigene Einstellungen* unter *Zeilen pro Seite* (siehe Kapitel *8.7* (Seite 181)) voreingestellt wurde.

  Bemerkung: Das Nutzen von `rows=-1` kann Leistungsprobleme verursachen, falls große Datenmengen verarbeitet werden müssen.

  Falls lange Seitenladezeiten entstehen, sollte ein anderer Filter für die Zeilen genutzt werden.

- ***first*:** Festlegung des ersten Objekts, das angezeigt wird. Beispiel: Falls der Filter 50 Ergebnisse ausgibt, zeigt *rows=10 first=11* die Ergebnisse 11 bis 20.
- ***sort*:** Festlegung der Spalte, die für die Sortierung der Ergebnisse genutzt wird. Die Ergebnisse werden aufsteigend sortiert. Beispiel: *sort=name* sortiert die Ergebnisse nach dem Inhalt der Spalte *Name*. Die Sortierung kann auch durch Klicken auf den Spaltentitel durchgeführt werden. Nach dem Anwenden des Filters werden die Großbuchstaben des Spaltennamens zu Kleinbuchstaben und Leerzeichen zu Unterstrichen geändert. Typische Spaltennamen sind:
  - *name*
  - *severity*
  - *host*
  - *location*
  - *qod* (engl. Quality of detection)
  - *comment*
  - *modified*
  - *created*

  Bemerkung: *sort* ist nicht auf der Detailseite von Berichten anwendbar (siehe Kapitel *11.2.1* (Seite 293)).

- ***sort-reverse*:** Bestimmung der Spalte, die für die Sortierung der Ergebnisse genutzt wird (siehe oben). Die Ergebnisse werden absteigend sortiert.

  Bemerkung: *sort-reverse* ist nicht auf der Detailseite von Berichten anwendbar (siehe Kapitel *11.2.1* (Seite 293)).

- ***tag*:** Auswahl der Ergebnisse mit einem bestimmten Tag (siehe Kapitel *8.4* (Seite 176)). Es kann nach einem bestimmten Tag-Wert (*tag="server=mail"*) oder nur nach einem Tag (*tag="server"*) gefiltert werden. Reguläre Ausdrücke sind ebenfalls zulässig.

Bemerkung: Durch das Nutzen von Tags zum Filtern können benutzerdefinierte Kategorien erstellt und genutzt werden. Dies ermöglicht eine vielseitige und detaillierte Filterfunktionalität.

- ***tag_id*:** Auswahl der Ergebnisse mit einem bestimmten Tag (siehe Kapitel *8.4* (Seite 176)). Es wird nach der UUID des Tags gefiltert. Die UUID eines Tags kann auf der Detailsseite des Tags gefunden werden (siehe Kapitel *8.4.4* (Seite 178)). Der Filter bleibt auch dann gültig, wenn sich der Name des Tags ändert.

8.3.2.2 Operatoren

Zum Präzisieren der Komponenten werden die folgenden Operatoren genutzt:

- = gleich, z. B. *rows=10*
- ~ enthält, z. B. *name~admin*
- < kleiner als, z. B. *created<-1w* → älter als eine Woche
- > größer als, z. B. *created>-1w* → jünger als eine Woche
- `regexp` regulärer Ausdruck, z. B. *regexp 192.168.[0-9]+.[0-9]*

Die folgenden Operatoren werden **nicht** unterstützt:

- `<=`
- `>=`
- `( )`

Es gibt eine Reihe spezieller Funktionen:

- Falls kein Wert auf = folgt, werden alle Ergebnisse ohne diesen Filterparameter angezeigt. Dieses Beispiel zeigt alle Ergebnisse ohne einen Kommentar:

```
comment=
```

- Falls ein Stichwort gefunden werden soll, aber nicht angegeben wird, welche Spalte durchsucht werden soll, werden alle Spalten durchsucht. Dieses Beispiel überprüft, ob mindestens eine Spalte den angegebenen Wert enthält:

```
=192.168.15.5
```

- Die Daten sind normalerweise oder-kombiniert. Dies kann mit dem Stichwort `or` angegeben werden. Um eine und-Kombination zu erhalten, muss das Stichwort `and` angegeben werden:

```
modified>2019-01-01 and name=services
```

- `and` wird vor `or` aufgelöst, d. h. `x and y or a and b` → `(x and y) or (a and b)`

  Ausdrücke wie `x and (a or b)` müssen als `x and a or x and b` geschrieben werden.

- Die Nutzung von `not` negiert den Filter. Dieses Beispiel zeigt alle Ergebnisse, die nicht „192.168.81.129“ enthalten:

```
not ~192.168.81.129
```

8.3.2.3 Textphrasen

Im Allgemeinen, können Textphrasen, nach denen gesucht wird, festgelegt werden.

Die folgenden Beispiele zeigen die Unterschiede:

`overflow` Findet alle Ergebnisse, die das Wort *overflow* enthalten. Dies gilt sowohl für *overflow* als auch für *Bufferoverflow*. Ebenso zeigt *192.168.0.1* sowohl Ergebnisse für *192.168.0.1* als auch für *192.168.0.100*.

`remote exploit` Findet alle Ergebnisse, die *remote* oder *exploit* enthalten. Natürlich werden auch Ergebnisse, die beide Wörter enthalten, angezeigt.

`remote and exploit` Findet alle Ergebnisse, die sowohl *remote* als auch *exploit* enthalten. Diese müssen nicht in der gleichen Spalte gefunden werden.

`"remote exploit"` Es wird nach der exakten Zeichenkette und nicht nach einzelnen Wörtern gesucht.

`regexp 192.168.[0-9]+.[0-9]` Es wird nach dem regulären Ausdruck gesucht.

8.3.2.4 Zeitangaben

Zeitangaben im Powerfilter können absolut oder relativ sein.

Absolute Zeitangaben Eine absolute Zeitangabe hat das folgende Format:

```
2023-04-21T13h50
```

Falls die Zeit ausgelassen wird, wird automatisch eine Zeit von 12:00 angenommen. Die Zeitangabe kann im Filter genutzt werden, z. B. *created>2023-04-21*.

Relative Zeitangaben Relative Zeitangaben werden immer in Bezug zur aktuellen Zeit berechnet. Zeitangaben in der Vergangenheit werden mit einem vorangestellten Minus (-) angegeben. Zeitangaben ohne ein vorangestelltes Zeichen werden als zukünftige Zeiten interpretiert. Für Zeiträume können die folgenden Buchstaben genutzt werden:

- *s* Sekunde
- *m* Minute
- *h* Stunde
- *d* Tag
- *w* Woche
- *m* Monat (30 Tage)
- *y* Jahr (365 Tage)

Beispielsweise zeigt die Eingabe von *created>-5d* alle Ergebnisse, die in den letzten 5 Tagen erstellt wurden. Eine Kombination wie z. B. *5d1h* ist nicht zulässig, sondern muss durch *121h* ersetzt werden.

Um den Zeitraum zu begrenzen, z. B. auf einen Monat, für den die Informationen dargestellt werden sollen, kann der folgende Ausdruck genutzt werden:

```
modified>2023-03-01 and modified<2023-03-31
```

8.3.3 Beispiele für Powerfilter

Hier sind ein paar Beispiele für Powerfilter:

- `127.0.0.1` zeigt alle Objekte, die „127.0.0.1“ irgendwo im Text einer Spalte haben.
- `127.0.0.1 iana` zeigt alle Objekte, die „127.0.0.1“ oder „iana“ irgendwo im Text einer Spalte haben.
- `127.0.0.1 and iana` zeigt alle Objekte, die „127.0.0.1“ und „iana“ irgendwo im Text einer Spalte haben.
- `regexp 192.168.[0-9]+.[0-9]` zeigt alle Objekte, die eine Zeichenkette im Stil einer IP-Adresse und beginnend mit „192.168“ irgendwo im Text einer Spalte haben.
- `name=localhost` zeigt alle Objekte mit dem exakten Namen „localhost“.
- `name~local` zeigt alle Objekte, die „local“ irgendwo in ihrem Namen haben.
- `name:^local` zeigt alle Objekte, deren Name mit „local“ beginnt.
- `port_list~tcp` zeigt alle Objekte, die „tcp“ irgendwo im Text des Namens der Portliste haben.
- `modified>2023-04-03 and modified<2023-04-05` zeigt alle Objekte, die zwischen dem 03.04.2023 0:00 und dem 05.04.2023 0:00 verändert wurden.
- `created>2023-04-03T13h00` zeigt alle Objekte, die nach 13:00 am 03.04.2023 erstellt wurden.
- `rows=20 first=1 sort=name` zeigt die ersten zwanzig Objekte, sortiert nach der Spalte *Name*.
- `created>-7d` zeigt alle Objekte, die innerhalb der letzten 7 Tage erstellt wurden.
- `=127.0.0.1` zeigt alle Objekte, die die exakte Zeichenkette „127.0.0.1“ irgendwo im Text einer Spalte haben.
- `tag="geo:long=52.2788` zeigt alle Objekte, die den Tag „geo:long“ mit dem Wert „52.2788“ haben.
- `tag~geo` zeigt alle Objekte, die einen Tag haben, dessen Name „geo“ enthält.

8.3.4 Powerfilter verwalten

Listenseite

Alle vorhandenen Powerfilter können angezeigt werden, indem *Konfiguration > Filter* in der Menüleiste gewählt wird (siehe Abb. 8.14).

Für alle Powerfilter werden die folgenden Informationen dargestellt:

Name Name des Filters.

Filterbefehl Filterbefehle, die den Powerfilter bilden (siehe Kapitel *8.3.2* (Seite 170)).

Typ Objekttyp, für den der Powerfilter angewendet werden kann.

Für alle Powerfilter sind die folgenden Aktionen verfügbar:

- Den Powerfilter in den Papierkorb verschieben.
- Den Powerfilter bearbeiten.
- Den Powerfilter klonen.
- Den Powerfilter als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Filtern können mehrere Filter zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Filter in den Papierkorb verschoben oder exportiert werden.

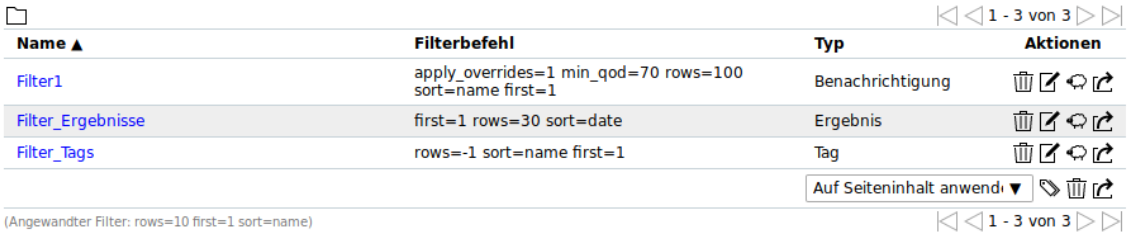


Abb. 8.14: Powerfilter verwalten

Detailseite

Durch Klicken auf den Namen eines Filters werden Details des Filters angezeigt. Durch Klicken auf wird die Detailseite des Filters geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über den Powerfilter.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Powerfiltern anzeigen.
- Einen neuen Powerfilter erstellen (siehe Kapitel *8.3.1* (Seite 168)).
- Den Powerfilter klonen.
- Den Powerfilter bearbeiten.
- Den Powerfilter in den Papierkorb verschieben.
- Den Powerfilter als XML-Datei exportieren.

8.4 Tags benutzen

Tags sind Informationen, die zu einem Objekt hinzugefügt werden können. Tags werden direkt mit dem Objekt zusammen erstellt und können nur mit dem Objekttyp, für den sie erstellt wurden, verknüpft werden.

Tags können genutzt werden, um Objekte zu filtern (siehe Kapitel *8.3* (Seite 168)).

Beispiel: Wenn nach `tag=target` gefiltert wird, muss der konkrete Tag festgelegt sein. Andernfalls würde das gewünschte Ergebnis nicht gefunden werden. Für `tag="target=mailserver"` muss der exakte Tag mit dem entsprechenden Wert festgelegt sein (siehe Abb. 8.15).

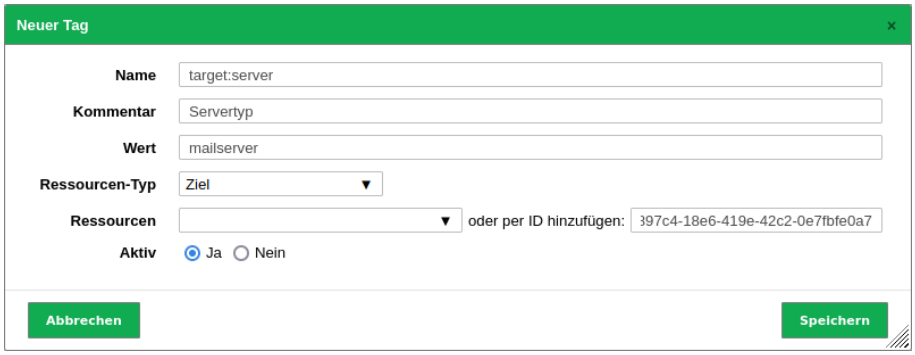


Abb. 8.15: Tag für den Objekttyp *Target*

8.4.1 Einen Tag mit einem einzelnen Objekt verknüpfen

Ein Tag für ein einzelnes Objekt kann wie folgt erstellt werden:

1. Detailseite des Objekts durch Klicken auf den Objektnamen und anschließendes Klicken auf öffnen.
2. Auf den Register *Benutzer-Tags* klicken.
3. Im geöffneten Bereich *Benutzer-Tags* auf klicken.
4. Tag definieren (siehe Abb. 8.15).
5. Auf *Speichern* klicken.

8.4.2 Einen Tag mit mehreren Objekten verknüpfen

Ein Tag kann mit mehreren Objekten des gleichen Typs (z. B. Aufgaben, Ziele, Scanner) wie folgt verknüpft werden:

1. Listenseite eines Objekttyps öffnen.
2. Liste filtern, sodass nur die Objekte angezeigt werden, die den Tag erhalten sollen.
3. In der Drop-down-Liste unterhalb der Liste von Objekten wählen, mit welchen Objekten der Tag verknüpft werden soll (siehe Abb. 8.16).

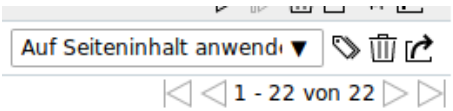


Abb. 8.16: Auswählen der Objekte

Bemerkung: *Auf Seiteninhalt anwenden* verknüpft den Tag mit allen Objekten, die auf der aktuellen Seite angezeigt werden.

Auf gesamte Filterauswahl anwenden verknüpft den Tag mit allen Objekten, die im Filter enthalten sind, selbst wenn sie nicht auf der aktuellen Seite angezeigt werden.

oder

2. In der Drop-down-Liste unterhalb der Liste von Objekten *Auf Auswahl anwenden* wählen.
3. Die Checkboxen der Objekte, mit denen der Tag verknüpft werden soll, in der Spalte *Aktionen* aktivieren.
4. Unterhalb der Liste von Objekten auf klicken.
5. Den Tag in der Drop-down-Liste *Tag auswählen* wählen (siehe Abb. 8.17).

Bemerkung: Nur Tags, die für den ausgewählten Objekttyp erstellt wurden, können gewählt werden.

Zusätzlich kann ein neuer Tag durch Klicken auf erstellt werden.

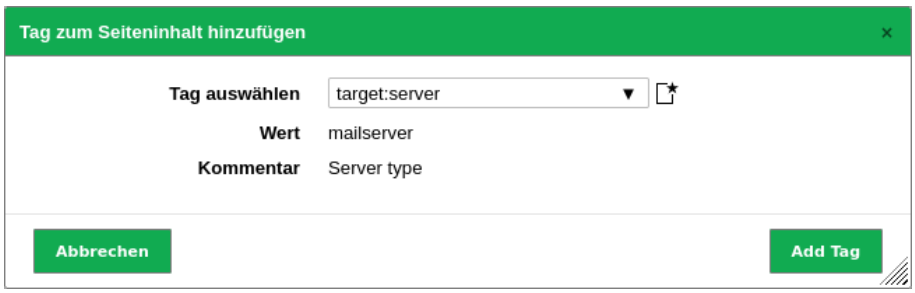


Abb. 8.17: Auswahl eines Tags für mehrere Objekte

6. Auf *Add Tag* klicken.

8.4.3 Einen Tag erstellen

Zusätzlich zum direkten Verknüpfen von Tags mit einem Objekt, können Tags auf der Seite *Tags* erstellt und später zugewiesen werden.

1. *Konfiguration* > *Tags* in der Menüleiste wählen.
2. Neuen Tag durch Klicken auf erstellen.
3. Tag definieren. Objekttyp, für den der Tag zugewiesen werden kann in der Drop-down-Liste *Ressourcen-Typ* wählen.
4. Auf *Speichern* klicken.

8.4.4 Tags verwalten

Listenseite

Alle vorhandenen Tags können angezeigt werden, indem *Konfiguration > Tags* in der Menüleiste gewählt wird.

Für alle Tags sind die folgenden Aktionen verfügbar:

- Den Tag deaktivieren, falls er aktiviert ist.
- Den Tag aktivieren, falls er deaktiviert ist.
- Den Tag in den Papierkorb verschieben.
- Den Tag bearbeiten.
- Den Tag klonen.
- Den Tag als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Tags können mehrere Tags zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Tags in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen eines Tags werden Details des Tags angezeigt. Durch Klicken auf wird die Detailseite des Tags geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über den Tag.

Zugewiesene Objekte Objekte, mit denen der Tag verknüpft ist. Die Objekte werden nur angezeigt, falls der Tag aktiv ist.

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Tags anzeigen.
- Einen neuen Tag erstellen (siehe Kapitel *8.4.3* (Seite 177)).
- Den Tag klonen.
- Den Tag bearbeiten.
- Den Tag in den Papierkorb verschieben.
- Den Tag als XML-Datei exportieren.
- Den Tag deaktivieren, falls er aktiviert ist.
- Den Tag aktivieren, falls er deaktiviert ist.

8.5 Den Papierkorb benutzen

Die Seite *Papierkorb* kann durch Wählen von *Administration* > *Papierkorb* in der Menüleiste geöffnet werden. Die Seite listet alle Objekte, die sich momentan im Papierkorb befinden, gruppiert nach Objekttyp auf.

Bemerkung: Objekte im Papierkorb gelten noch nicht als gelöscht. Sie werden erst endgültig gelöscht, wenn sie manuell aus dem Papierkorb gelöscht werden oder wenn der gesamte Papierkorb geleert wird.

Die zusammenfassende Tabelle *Hilfe Übersicht* zeigt alle möglichen Arten von gelöschten Objekten mit entsprechender Objektanzahl. Durch Klicken auf einen Objektnamen wird der entsprechende Bereich angezeigt (siehe Abb. 8.18).

Der Papierkorb kann durch Klicken auf *Papierkorb leeren* geleert werden.

Abb. 8.18: Inhalte des Papierkorbs

Im Bereich des entsprechenden Objekttyps können die einzelnen Objekte verwaltet werden (siehe Abb. 8.19):

- Durch Klicken auf wird das Objekt aus dem Papierkorb zurück auf seine reguläre Seite verschoben. Das Objekt kann nicht wiederhergestellt werden, falls es von anderen Objekten im Papierkorb abhängig ist.
- Durch Klicken auf wird ein Objekt endgültig aus dem System gelöscht. Das Objekt kann nicht gelöscht werden, falls andere Objekten im Papierkorb von ihm abhängig sind.

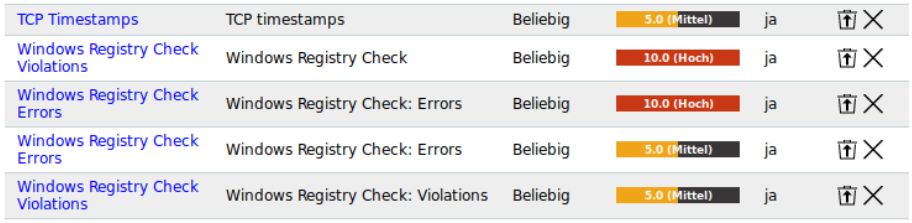


Abb. 8.19: Wiederherstellen oder Löschen eines Objekts im Papierkorb

8.6 Den Feed-Status anzeigen

Der Synchronisationsstatus aller Sicherheitsinfos kann angezeigt werden, indem *Administration* > *Feed-Status* in der Menüleiste gewählt wird.

Die folgenden Informationen werden dargestellt (siehe Abb. 8.20):

Typ Feedtyp (*NVT*, *SCAP*, *CERT* oder *GVMD_DATA*).

Inhalte Art der Information, die vom Feed bereitgestellt wird.

Ursprung Name des Feedservices, der genutzt wird, um die Sicherheitsinfos zu synchronisieren.

Version Versionsnummer der Feeddaten.

Status Statusinformation des Feeds, z. B. Zeit seit dem letzten Update.

Falls gerade ein Feed-Update durchgeführt wird, wird *Aktualisierung läuft...* angezeigt. Dieser Status wird für alle Feeds angezeigt, auch wenn gerade nur ein Feed aktualisiert wird.

Abb. 8.20: Darstellen des Feed-Status

8.7 Die Benutzereinstellungen ändern

Jeder Benutzer der Appliance kann seine eigenen Einstellungen für die Web-Oberfläche verwalten. Auf diese Einstellungen kann zugegriffen werden, indem die Maus über in der rechten oberen Ecke bewegt und auf *Eigene Einstellungen* geklickt wird (siehe Abb. 8.21).

Abb. 8.21: Öffnen der Benutzereinstellungen

Die Einstellungen können durch Klicken auf bearbeitet werden.

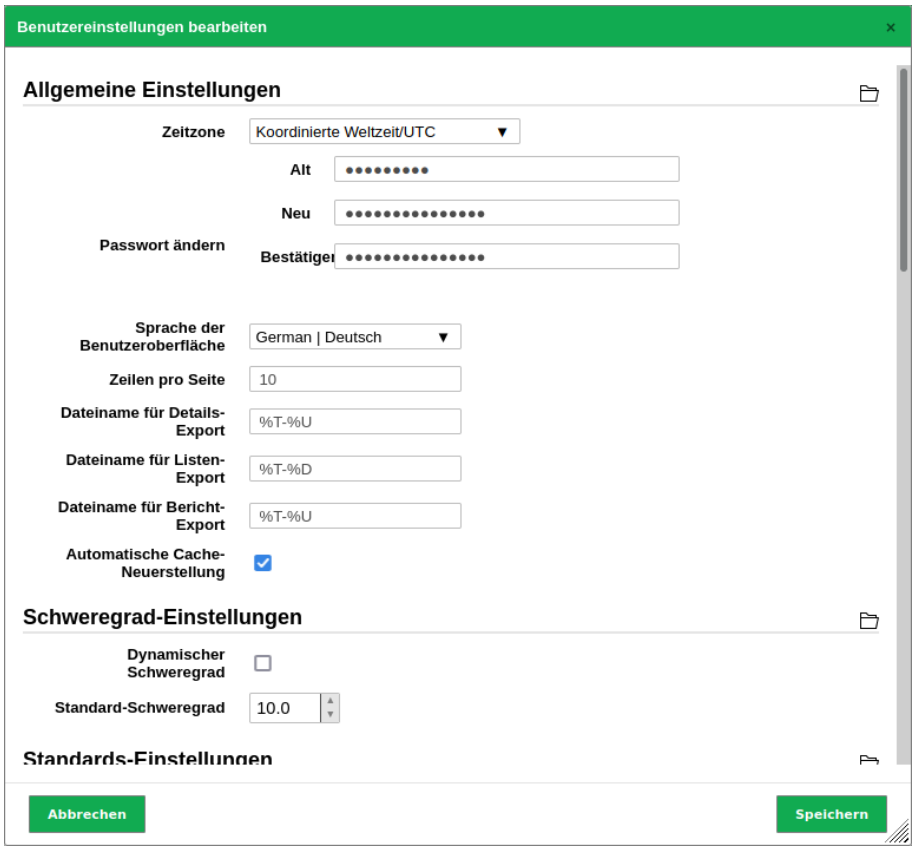


Abb. 8.22: Verwalten der Benutzereinstellungen

Wichtige Einstellungen sind:

Zeitzone Die Appliance speichert intern alle Informationen in der Zeitzone UTC±00:00. Um die Daten in der Zeitzone des Benutzers darzustellen, muss die entsprechende Auswahl getroffen werden.

Passwort ändern Das Benutzerpasswort kann hier geändert werden.

Sprache der Benutzeroberfläche Die Sprache kann hier festgelegt werden. Standardmäßig werden die Browsereinstellungen genutzt.

Zeilen pro Seite Dies definiert die Standardanzahl von Objekten, die pro Listenseite auf der Web-Oberfläche angezeigt werden. Eine hohe Anzahl von Zeilen pro Seite erhöht die Ladezeiten. Benutzerdefinierte Filter können diese Einstellung überschreiben (siehe Kapitel *8.3* (Seite 168)).

Dateiname für Details-Export Dies legt den Standarddateinamen für exportierte Objektdetails fest. Für den Dateinamen können die folgenden Platzhalter genutzt werden:

- %C: Erstellungsdatum im Format YYYYMMDD. Wird zum aktuellen Datum geändert, falls kein Erstellungsdatum verfügbar ist.
- %C: Erstellungszeit im Format HHMMSS. Wird zur aktuellen Zeit geändert, falls keine Erstellungszeit verfügbar ist.
- %D: Aktuelles Datum im Format YYYYMMDD.
- %F: Name des genutzten Berichtformats (XML für Listen und andere Typen als Berichte).
- %M: Modifizierungsdatum im Format YYYYMMDD. Wird zum Erstellungsdatum oder zum aktuellen Datum geändert, falls kein Modifizierungsdatum verfügbar ist.
- %m: Modifizierungszeit im Format HHMMSS. Wird zur Erstellungszeit oder zur aktuellen Zeit geändert, falls keine Modifizierungszeit verfügbar ist.
- %N: Name des Objekts oder, im Falle von Berichten, der zugehörigen Aufgabe. Listen und Typen ohne Namen nutzen den Typ (siehe %T).
- %T: Objekttyp, z. B. „task“, „port_list“. Pluralisiert für Listenseiten.
- %t: Aktuelle Zeit im Format HHMMSS.
- %U: Eindeutige ID des Objekts oder „list“ für Listen aus mehreren Objekten.
- %u: Name des aktuell eingeloggten Benutzers.
- %%: Prozentzeichen (%).

Dateiname für Listen-Export Dies legt den Standardnamen der Datei exportierter Objektlisten fest (siehe oben).

Dateiname für Bericht-Export Dies legt den Standardnamen der Datei exportierter Berichte fest (siehe oben).

Automatische Cache-Neuerstellung Die automatische Cache-Neuerstellung kann hier aktiviert oder deaktiviert werden. Falls mehrere Aktionen (z. B. das Löschen mehrerer Objekte) mit aktivierter automatischer Cache-Neuerstellung nacheinander ausgeführt werden, löst jede Aktion die Cache-Neuerstellung aus, was zu einem verlangsamten Prozess führt. Für solche Fälle kann die automatische Cache-Neuerstellung vorübergehend deaktiviert werden.

Dynamischer Schweregrad Dies legt fest, ob der Schweregrad eines bestehenden Ergebnisses geändert wird, falls sich der Schweregrad des zugrundeliegenden VTs ändert. Andernfalls gilt der neue Schweregrad nur für zukünftige Scans.

Standard Schweregrad Der Standard-Schweregrad kann hier festgelegt werden. Falls einem VT kein Schweregrad zugewiesen ist, wird der Standard-Schweregrad genutzt.

Standards-Einstellungen Die standardmäßig gewählten Optionen und Einträge für unterschiedliche Einstellungen können hier festgelegt werden.

Filter-Einstellungen Bestimmte Standardfilter können hier für jede Seite festgelegt werden. Die Filter werden dann automatisch aktiviert, wenn die Seite geladen wird.

8.8 Das Handbuch öffnen

Das Handbuch kann geöffnet werden, indem *Hilfe > Benutzerhandbuch* in der Menüleiste gewählt wird.

Zusätzlich kann das Handbuch von jeder Seite aus durch Klicken auf ⓘ in der linken oberen Ecke geöffnet werden. Das zum Seiteninhalt gehörende Kapitel wird geöffnet.

8.9 Aus der Web-Oberfläche ausloggen

Das Ausloggen kann durchgeführt werden, indem die Maus über 👤 in der rechten oberen Ecke bewegt und auf * Log Out* geklickt wird (siehe Abb. 8.23).

Falls für eine bestimmte Zeit keine Aktion auf der Web-Oberfläche durchgeführt wird, wird der Benutzer automatisch ausgeloggt (siehe Kapitel *7.2.4.1.1* (Seite 96)). Das Timeout beträgt standardmäßig 15 Minuten.

Die verbleibende Zeit, bis der Nutzer automatisch ausgeloggt wird, kann angezeigt werden, indem die Maus über 👤 bewegt wird. Durch Klicken auf 🔄 kann der Timeout zurückgesetzt werden.

Abb. 8.23: Ausloggen aus der Web-Oberfläche

KAPITEL 9

Den Zugriff auf die Web-Oberfläche verwalten

Bemerkung: Dieses Kapitel dokumentiert alle möglichen Menüoptionen.

Allerdings unterstützen nicht alle Appliance-Modelle alle Menüoptionen. Um festzustellen, ob ein bestimmtes Feature für das genutzte Appliance-Modell verfügbar ist, können die Tabellen in Kapitel *3* (Seite 20) genutzt werden.

9.1 Benutzer

Die Greenbone Enterprise Appliance ermöglicht die Definition und Verwaltung verschiedener Benutzer mit unterschiedlichen Rollen und Berechtigungen. Beim Initialisieren der Appliance wird der erste Benutzer – der Web-/Scanadministrator – bereits im GOS-Administrationsmenü erstellt. Mit diesem Benutzer können weitere Benutzer erstellt und verwaltet werden.

Rollen Die Benutzerverwaltung der Appliance unterstützt für den Zugriff auf die Web-Oberfläche ein rollenbasiertes Berechtigungskonzept. Verschiedene Rollen sind bereits standardmäßig eingerichtet. Zusätzliche Rollen können mithilfe eines Administrators erstellt und genutzt werden. Die Rolle definiert, welche Optionen auf der Web-Oberfläche für den Benutzer sichtbar und nutzbar sind. Die Rollenzuordnung ist nicht in der Web-Oberfläche, sondern im zugrundeliegenden Greenbone Management Protocol (GMP) implementiert und betrifft somit alle GMP-Clients.

Gruppen Zusätzlich zu Rollen unterstützt die Benutzerverwaltung der Appliance auch Gruppen. Dies dient hauptsächlich dem logischen Gruppieren.

Gruppen und Rollen können genutzt werden, um Berechtigungen mehreren Benutzern gleichzeitig zuzuweisen.

Jedem Benutzer wird ein IP-Adressbereich zugewiesen, der die erlaubten oder verweigerten Ziele enthält. Die Appliance verweigert den Scan von anderen IP-Adressen als den angegebenen. Gleichermaßen kann der Zugriff auf bestimmte Schnittstellen der Appliance erlaubt oder verweigert werden.

Die Benutzerverwaltung wird vollständig mit der Appliance durchgeführt. Externe Quellen für die Benutzerverwaltung werden nicht unterstützt. Dennoch kann ein zentraler LDAPS- oder RADIUS-Server in die Appliance integriert werden, um eine zentrale Authentifizierung zu unterstützen und eine Passwortsynchronisierung zu

ermöglichen (siehe Kapitel *9.5* (Seite 205)). Der Server wird nur genutzt, um das Passwort während des Logins des Benutzers zu verifizieren. Alle anderen Einstellungen werden in der Benutzerverwaltung der Appliance vorgenommen.

9.1.1 Benutzer erstellen und verwalten

9.1.1.1 Einen Benutzer erstellen

Benutzer können wie folgt erstellt werden:

Bemerkung: Nur Administratoren dürfen zusätzliche Benutzer erstellen und verwalten.

1. Als Administrator einloggen.
2. *Administration* > *Benutzer* in der Menüleiste wählen.
3. Neuen Benutzer durch Klicken auf erstellen.
4. Benutzer definieren (siehe Abb. 9.1).

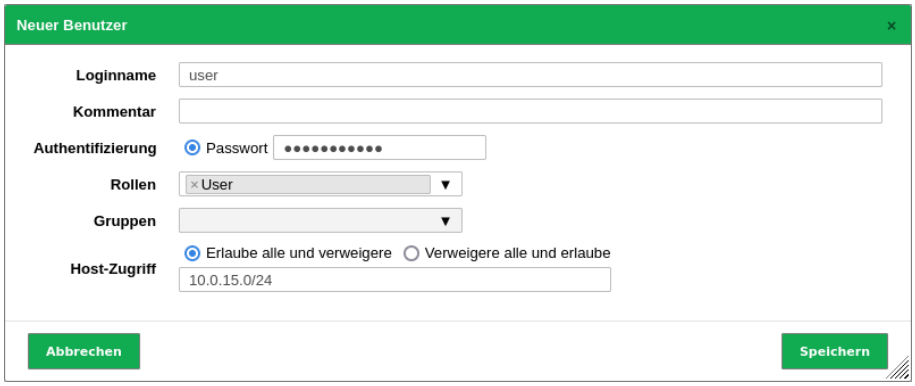


Abb. 9.1: Erstellen eines neuen Benutzers

5. Auf *Speichern* klicken.

   → Der Benutzer wird erstellt und auf der Seite *Benutzer* angezeigt.

Die folgenden Details des Benutzers können festgelegt werden:

Loginname Dies ist der Name, der für den Login genutzt wird. Für den Loginnamen sind nur die folgenden Zeichen zulässig:

- Alle alphanumerischen Zeichen
- - (Bindestrich)
- _ (Unterstrich)
- . (Punkt)

Bemerkung: Bei Verwendung einer zentralen Benutzerverwaltung (siehe Kapitel *9.5* (Seite 205)) können je nach LDAP- oder RADIUS-Server Einschränkungen hinsichtlich der Länge und der Zeichentypen gelten. Außerdem muss der Benutzer mit genau demselben Namen (rDN) erstellt werden, den der Server verwendet.

Authentifizierung Dies ist die Methode, die für den Login genutzt wird.

- **Passwort** Für die Verwendung der lokalen Authentifizierung mit dem Loginnamen und einem Passwort.

  Das Passwort kann jede Art von Zeichen enthalten und hat praktisch keine Längenbegrenzung.

  Bei der Verwendung von Sonderzeichen ist zu beachten, dass diese auf allen verwendeten Tastaturen vorhanden sein müssen und von jeder Client-Software und allen Betriebssystemen korrekt unterstützt werden. Das Kopieren und Einfügen von Sonderzeichen für Passwörter kann je nach diesen externen Faktoren zu ungültigen Passwörtern führen.

- **Nur LDAP-Authentifizierung** Für die Verwendung einer zentralen Benutzerverwaltung siehe Kapitel *9.5* (Seite 205).

- **Nur RADIUS-Authentifizierung** Für die Verwendung einer zentralen Benutzerverwaltung siehe Kapitel *9.5* (Seite 205).

Rollen Jeder Benutzer kann mehrere Rollen haben. Die Rollen definieren die Berechtigungen eines Benutzers bei der Anwendung von GMP. Die Rollen *Admin*, *User*, *Info*, *Observer*, *Guest* und *Monitor* sind verfügbar. Zusätzlich ist es möglich, benutzerdefinierte Rollen hinzuzufügen und zu konfigurieren (siehe Kapitel *9.2.2* (Seite 190)).

Wenn ein Benutzer mit einer benutzerdefinierten Rolle in der Lage sein soll, die Web-Oberfläche zu nutzen, sind mindestens die folgenden Berechtigungen für diese Rolle erforderlich:

- *authenticate*
- *get_settings*
- *help*

Für weitere Details siehe Kapitel *9.2* (Seite 189).

Gruppen Jeder Benutzer kann Mitglied in mehreren Gruppen sein. Die Verwaltung von Berechtigungen kann ebenfalls mithilfe von Gruppen durchgeführt werden (siehe Kapitel *9.4* (Seite 195)).

Host-Zugriff Hosts, auf denen es dem Benutzer erlaubt ist, Scans durchzuführen. Die Beschränkungen gelten auch für Administratoren, welche diese jedoch selbst entfernen können. Normale Benutzer (*User*) und Rollen ohne Zugriff auf die Benutzerverwaltung können die Beschränkungen nicht umgehen. Grundsätzlich ist entweder eine Whitelist (alle verweigern und einzelne erlauben) oder eine Blacklist (alle erlauben und einzelne verweigern) möglich.

- **Whitelist** Das Scannen aller Systeme wird grundsätzlich verweigert. Nur explizit gelistete Systeme dürfen gescannt werden.

- **Blacklist** Das Scannen aller Systeme wird grundsätzlich erlaubt. Nur explizit gelistete Systeme dürfen nicht gescannt werden.

Tipp: Allgemein wird die Whitelist-Methode empfohlen. Dies stellt sicher, dass Benutzer keine Systeme scannen, die außerhalb ihrer Verantwortung liegen, irgendwo im Internet lokalisiert sind oder versehentlich auf defekte Scans reagieren.

Sowohl Systemnamen als auch IPv4- und IPv6-Adressen können eingegeben werden. Einzelne IP-Adressen oder IP-Adressenbereiche und Netzwerksegmente können angegeben werden. Die folgende Liste zeigt einige Beispiele:

- 192.168.15.5 (IPv4-Adresse)
- 192.168.15.5-192.168.15.27 (IPv4-Adressbereich, lange Form)
- 192.168.15.5-27 (IPv4-Adressbereich, kurze Form)
- 192.168.15.128/25 (IPv4-Adressbereich, CIDR-Notation)

- 2001:db8::1 (IPv6-Adresse)
- 2001:db8::1-2001:db8::15 (IPv6-Adressbereich, lange Form)
- 2001:db8::1-15 (IPv6-Adressbereich, kurze Form)
- 2001:db8::/120 (IPv4-Adressbereich, CIDR-Notation)

Alle Optionen können gemischt und angepasst und als kommagetrennte Liste eingegeben werden. Standardmäßig ist die Subnetzmaske in der CIDR-Schreibweise auf ein Maximum von 20 für IPv4 und 116 für IPv6 beschränkt. Der Grund dafür ist, dass die maximale Anzahl von IP-Adressen pro Ziel bei den meisten Appliances 4096 beträgt. Ist die maximale Anzahl der IP-Adressen höher, z.B. bei der Greenbone Enterprise 6500, können entsprechend größere Subnetzmasken konfiguriert werden.

9.1.1.2 Benutzer verwalten

Listenseite

Alle vorhandenen Benutzer können angezeigt werden, indem als Administrator *Administration > Benutzer* in der Menüleiste gewählt wird.

Für alle Benutzer werden die folgenden Informationen angezeigt:

Name Name des Benutzers. Globale Benutzer sind Benutzer, die im GOS-Administrationsmenü erstellt werden (siehe Kapitel *7.2.1* (Seite 70)) und mit markiert sind.

Rollen Rolle des Benutzers (siehe Kapitel *9.2* (Seite 189)).

Gruppen Gruppen, zu denen der Benutzer gehört (siehe Kapitel *9.3* (Seite 193)).

Host-Zugriff Hosts, auf denen der Benutzer Scans durchführen darf.

Authentifizierungstyp Art der Authentifizierung: *Lokal*, falls ein Passwort genutzt wird, *RADIUS* oder *LDAP*, falls ein zentrales Benutzermanagement genutzt wird (siehe Kapitel *9.5* (Seite 205)).

Für alle Benutzer sind die folgenden Aktionen verfügbar:

- Den Benutzer löschen. Nur Benutzer, die aktuell nicht eingeloggt sind und die nicht Super-Administrator sind, können gelöscht werden.
- Den Benutzer bearbeiten.
- Den Benutzer klonen.
- Den Benutzer als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Benutzern können mehrere Benutzer zur gleichen Zeit gelöscht oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Benutzer gelöscht oder exportiert werden.

Detailseite

Durch Klicken auf den Namen eines Benutzers werden Details des Benutzers angezeigt. Durch Klicken auf wird die Detailseite des Benutzers geöffnet (siehe Abb. 9.2).

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über den Benutzer.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Berechtigungen des Benutzers oder anderer Benutzer/Rollen/Gruppen für Objekte des Benutzers (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Benutzern anzeigen.
- Einen neuen Benutzer erstellen (siehe Kapitel *9.1.1.1* (Seite 185)).
- Den Benutzer klonen.
- Den Benutzer bearbeiten.
- Den Benutzer löschen. Nur Benutzer, die aktuell nicht eingeloggt sind und die nicht Super-Administrator sind, können gelöscht werden.
- Den Benutzer als XML-Datei exportieren.

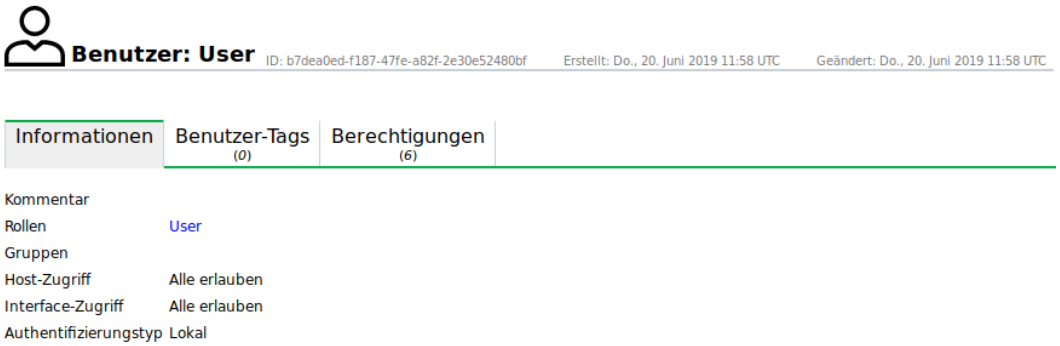


Abb. 9.2: Details eines Benutzers

9.1.2 Zeitgleicher Login

Es ist möglich, dass zwei Benutzer gleichzeitig eingeloggt sind.

Falls derselbe Benutzer sich mehrmals zur gleichen Zeit einloggen will, muss der Login mit unterschiedlichen PCs oder Browsern stattfinden. Ein weiterer Login im selben Browser setzt den ersten Login außer Kraft.

9.1.3 Einen Gastlogin erstellen

Der Gast-Benutzer hat nur eingeschränkten Zugriff auf die Web-Oberfläche.

Um einem Gast den Zugriff zu ermöglichen, kann ein Benutzer mit der Rolle *Guest* erstellt werden (siehe Kapitel *9.1.1* (Seite 185)).

Mit dem Passwort kann sich der Gast einloggen und bekommt die Seite *Dashboards* angezeigt.

Um einem Gast den Login ohne Passwort zu ermöglichen, muss diese Funktion im GOS-Administrationsmenü aktiviert sein (siehe Kapitel *7.2.1.4* (Seite 73)).

9.2 Rollen

Die Web-Oberfläche unterstützt das Erstellen und Konfigurieren eigener Benutzerrollen.

Die folgenden Rollen sind standardmäßig verfügbar:

- **Admin** Diese Rolle hat standardmäßig alle Berechtigungen. Sie ist insbesondere berechtigt, andere Benutzer, Rollen und Gruppen zu erstellen und zu verwalten.
- **Benutzer** Diese Rolle hat standardmäßig alle Berechtigungen, abgesehen von der Benutzer-, Rollen und Gruppenverwaltung. Diese Rolle kann den Feed nicht synchronisieren und verwalten. Auf der Web-Oberfläche besteht kein Zugang zur Seite *Administration*.
- **Info** Diese Rolle (Information Browser) hat nur Lesezugriff auf VTs und SCAP-Informationen. Alle anderen Informationen sind nicht zugänglich. Die Rolle kann die eigenen Einstellungen ändern, z. B. das Passwort ändern.
- **Guest** Diese Rolle ist mit der Rolle *Info* identisch, kann aber die eigenen Einstellungen nicht ändern.
- **Monitor** Diese Rolle hat Zugriff auf die Systemberichte der Appliance (siehe Kapitel *17.1* (Seite 388)).
- **Observer** Diese Rolle hat Lesezugriff auf das System, aber kann keine Scans starten oder erstellen. Sie hat nur Lesezugriff auf Scans, für die sie zugelassen wurde.
- **Super Admin** Diese Rolle hat Zugriff auf alle Objekte aller Benutzer. Es besteht keine Verbindung zum super user (*su/root*) im GOS-Administrationsmenü. Diese Rolle kann nicht über die Web-Oberfläche konfiguriert werden und Benutzer mit dieser Rolle können nicht über die Web-Oberfläche gelöscht werden. Benutzer mit dieser Rolle sollten über das GOS-Administrationsmenü verwaltet werden (siehe Kapitel *9.2.5* (Seite 192)).

Bemerkung: Nur Administratoren sind berechtigt, zusätzliche Rollen zu erstellen und zu verwalten.

Bemerkung: Das Verändern der voreingestellten Rollen ist nicht möglich. Allerdings kann eine Rolle kopiert (geklont) und anschließend die Kopie bearbeitet werden.

Dies stellt ein gleichbleibendes Verhalten nach einem Softwareupgrade sicher.

9.2.1 Eine vorhandene Rolle klonen

Wenn eine vorhandene Rolle genau die benötigten Anforderungen erfüllt, kann eine Rolle erstellt werden, indem eine vorhandene Rolle geklont wird:

1. Als Administrator einloggen.
2. *Administration* > *Rollen* in der Menüleiste wählen.
3. In der Zeile einer vorhandenen Rolle auf klicken.
4. In der Zeile des Klons auf klicken.
5. Namen der Rolle in das Eingabefeld *Name* eingeben (siehe Abb. 9.3).
6. Benutzer, die die Rolle haben sollen, in der Drop-down-Liste *Benutzer* wählen.
7. Berechtigung durch Wählen der Berechtigung in der Drop-down-Liste *Name* und Klicken auf *Berechtigung erstellen* hinzufügen.

8. Super-Berechtigung durch Wählen der entsprechenden Gruppe in der Drop-down-Liste *Gruppe* und Klicken auf *Berechtigung erstellen* hinzufügen.

   Berechtigung durch Klicken auf in der Liste *Generelle Berechtigungen für Befehle* löschen.

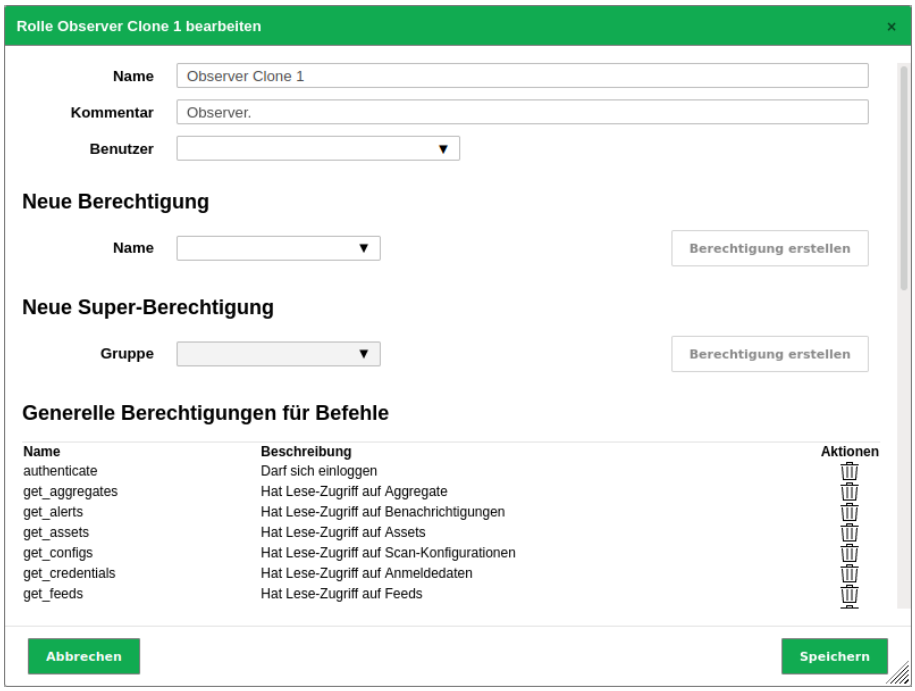


Abb. 9.3: Bearbeiten einer geklonten Rolle

9. Auf *Speichern* klicken.

9.2.2 Eine Rolle erstellen

Wenn eine Rolle mit eingeschränkter Funktionalität erstellt werden soll, kann mit einer neuen, leeren Rolle begonnen werden:

1. Als Administrator einloggen.
2. *Administration* > *Rollen* in der Menüleiste wählen.
3. Neue Rolle durch Klicken auf erstellen.
4. Rolle definieren.

   Die folgenden Details der Rolle können festgelegt werden:

   Name Der Name der Rolle kann Buchstaben und Zahlen enthalten und darf maximal 80 Zeichen lang sein.

   Kommentar (optional) Ein Kommentar beschreibt die Rolle genauer.

   Benutzer Die Benutzer mit dieser Rolle können in der Drop-down-Liste *Benutzer* gewählt werden. Alternativ können die Rollen im Benutzerprofil verwaltet werden (siehe Kapitel *9.1.1* (Seite 185)).

5. Auf *Speichern* klicken.

   → Die Rolle wird erstellt und auf der Seite *Rollen* angezeigt.

6. In der Zeile der neu erstellen Rolle auf klicken.

7. Berechtigung durch Wählen der Berechtigung in der Drop-down-Liste *Name* und Klicken auf *Berechtigung erstellen* hinzufügen.

   Bemerkung: Wenn Benutzer mit der Rolle in der Lage sein sollen, die Web-Oberfläche zu benutzen, sind mindestens die folgenden Berechtigungen erforderlich:

   - *authenticate*
   - *get_settings*
   - *help*

   Die Berechtigung *write_settings* erlaubt es Benutzern, ihr eigenes Passwort, ihre Zeitzone und andere persönliche Einstellungen zu ändern.

   ---

8. Super-Berechtigung durch Wählen der entsprechenden Gruppe in der Drop-down-Liste *Gruppe* und Klicken auf *Berechtigung erstellen* hinzufügen.

   Berechtigung durch Klicken auf 🗑 in der Liste *Generelle Berechtigungen für Befehle* löschen.

9. Auf *Speichern* klicken.

9.2.3 Rollen verwalten

Listenseite

Alle vorhandenen Rollen können angezeigt werden, indem *Administration > Rollen* in der Menüleiste gewählt wird.

Für alle Rollen werden die folgenden Informationen angezeigt:

Name Name der Rolle. Alle Standardrollen sind globale Rollen und mit markiert.

Für alle Rollen sind die folgenden Aktionen verfügbar:

- 🗑 Die Rolle in den Papierkorb verschieben. Nur selbst erstellte Rollen können in den Papierkorb verschoben werden.
- Die Rolle bearbeiten. Nur selbst erstellte Rollen können bearbeitet werden.
- Die Rolle klonen.
- Die Rolle als XML-Datei exportieren.

Bemerkung: Durch Klicken auf 🗑 oder unterhalb der Liste von Rollen können mehrere Rollen zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Rollen in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Rolle werden Details der Rolle angezeigt. Durch Klicken auf wird die Detailseite der Rolle geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Rolle.

Generelle Berechtigungen für Befehle GMP-Befehle, die von dieser Rolle ausgeführt werden können.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Berechtigungen der Rolle oder anderer Benutzer/Rollen/Gruppen für Objekte der Rolle (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Rollen anzeigen.
- Eine neue Rolle erstellen (siehe Kapitel *9.2.2* (Seite 190)).
- Die Rolle klonen.
- Die Rolle bearbeiten. Nur selbst erstellte Rollen können bearbeitet werden.
- Die Rolle in den Papierkorb verschieben. Nur selbst erstellte Rollen können in den Papierkorb verschoben werden.
- Die Rolle als XML-Datei exportieren.

9.2.4 Rollen einem Benutzer zuweisen

Um Berechtigungen zu gruppieren, kann ein Benutzer mehr als eine Rolle haben.

Die Rollen werden beim Erstellen eines neuen Benutzers zugewiesen (siehe Abb. 9.4, siehe Kapitel *9.1.1* (Seite 185)). Falls dem Benutzer mehr als eine Rolle zugewiesen wird, werden die Berechtigungen der Rollen addiert.

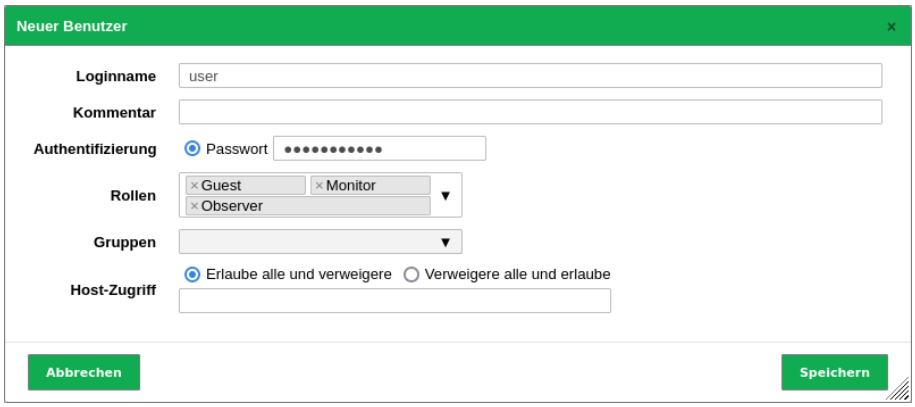


Abb. 9.4: Erstellen eines neuen Benutzers mit mehreren Rollen

9.2.5 Einen Super-Administrator erstellen

Die Rolle *Super Admin* stellt die höchste Zugriffsstufe dar.

Die Rolle *Admin* kann Benutzer erstellen, verändern und löschen. Zusätzlich kann sie Berechtigungen sehen, verändern und löschen. Allerdings ist sie diesen Berechtigungen ebenfalls untergeordnet. Falls ein Benutzer eine private Scan-Konfiguration erstellt, aber nicht teilt, kann der Administrator nicht auf diese zugreifen.

Die Rolle *Super Admin* ist für Diagnosezwecke geeigneter. Der Super-Administrator ist von Einschränkungen durch Berechtigungen ausgenommen und kann jede Konfiguration jedes Nutzers sehen und bearbeiten.

Der Super-Administrator muss im GOS-Administrationsmenü erstellt werden (siehe Kapitel *7.2.1.5* (Seite 74)).

Bemerkung: Der Super-Administrator kann nur durch den Super-Administrator selbst bearbeitet werden.

9.3 Gruppen

Gruppen werden genutzt, um Benutzer logisch zusammenzufassen. Es können beliebig viele Gruppen erstellt werden.

Berechtigungen können einer Gruppe zugewiesen werden (siehe Kapitel *9.4* (Seite 195)). Standardmäßig sind keine Gruppen vorhanden.

9.3.1 Eine Gruppe erstellen

Eine Gruppe kann wie folgt erstellt werden:

Bemerkung: Nur Administratoren dürfen Gruppen erstellen und verwalten.

1. Als Administrator einloggen.
2. *Administration* > *Gruppen* in der Menüleiste wählen.
3. Neue Gruppe durch Klicken auf erstellen.
4. Gruppe definieren (siehe Abb. 9.5).

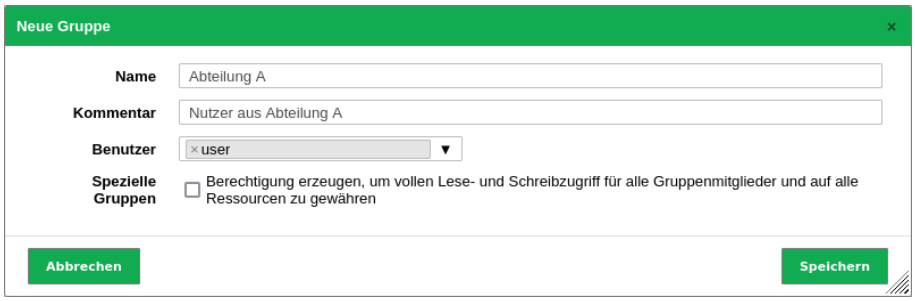


Abb. 9.5: Erstellen einer neuen Gruppe

5. Auf *Speichern* klicken.

   → Die Gruppe wird erstellt und auf der Seite *Gruppen* angezeigt.

Die folgenden Details der Gruppe können festgelegt werden:

Name Der Name der Gruppe kann Buchstaben und Zahlen enthalten und darf maximal 80 Zeichen lang sein.

Kommentar (optional) Ein Kommentar beschreibt die Gruppe näher.

Benutzer Die Mitglieder der Gruppe können in der Drop-down-Liste *Benutzer* gewählt werden. Alternativ können die Gruppen im Benutzerprofil verwaltet werden (siehe Kapitel *9.1.1* (Seite 185)).

Spezielle Gruppen Checkbox aktivieren, falls alle Gruppenmitglieder Lese- und Schreibrechte auf alle Objekte der Gruppe haben sollen.

9.3.2 Gruppen verwalten

Listenseite

Alle vorhandenen Gruppen können angezeigt werden, indem *Administration > Gruppen* in der Menüleiste gewählt wird.

Für alle Gruppen werden die folgenden Informationen angezeigt:

Name Name der Gruppe.

Für alle Gruppen sind die folgenden Aktionen verfügbar:

- Die Gruppe in den Papierkorb verschieben.
- Die Gruppe bearbeiten.
- Die Gruppe klonen.
- Die Gruppe als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Gruppen können mehrere Gruppen zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Gruppen in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Gruppe werden Details der Gruppe angezeigt. Durch Klicken auf wird die Detailseite der Gruppe geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Gruppe.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Berechtigungen der Gruppe oder anderer Benutzer/Rollen/Gruppen für Objekte der Gruppe (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Gruppen anzeigen.
- Eine neue Gruppe erstellen (siehe Kapitel *9.3.1* (Seite 193)).
- Die Gruppe klonen.
- Die Gruppe bearbeiten.
- Die Gruppe in den Papierkorb verschieben.
- Die Gruppe als XML-Datei exportieren.

9.4 Berechtigungen

Durch Wählen von *Administration* > *Berechtigungen* in der Menüleiste, werden alle Berechtigungen angezeigt, die auf dem System vorhanden sind. Falls mehrere Rollen erstellt wurden, können leicht hunderte Berechtigungen vorhanden sein.

Jede Berechtigung betrifft genau ein Subjekt. Eine Berechtigung erlaubt es dem Subjekt, eine zugehörige Aktion durchzuführen.

Subjekte können vom folgenden Typ sein:

- Benutzer
- Rollen
- Gruppen

Es gibt zwei Arten von Berechtigungen:

- **Berechtigungen für Befehle** Berechtigungen für Befehle sind mit dem Greenbone Management Protocol (GMP) verknüpft. Jede Berechtigung gilt für einen bestimmten GMP-Befehl, wobei der Name der Berechtigung der entsprechende Befehl ist.

  Eine Berechtigung für Befehle ist entweder eine Berechtigung auf Befehlslevel oder auf Ressourcenlevel.

  - **Befehlslevel** Falls keine Ressource angegeben ist, wird eine Berechtigung auf Befehlslevel erstellt. Eine Berechtigung auf Befehlslevel ermöglicht es dem Subjekt, den vorgegebenen GMP-Befehl auszuführen.
  - **Ressourcenlevel** Falls eine Ressource angegeben ist, wird eine Berechtigung auf Ressourcenlevel erstellt. Eine Berechtigung auf Ressourcenlevel ermöglicht es dem Subjekt, den vorgegebenen GMP-Befehl auf eine bestimmte Ressource auszuführen.
- **Super-Berechtigungen** (siehe Kapitel (*9.4.2* (Seite 199))

9.4.1 Berechtigungen erstellen und verwalten

Bemerkung: Üblicherweise werden Berechtigungen auf der Web-Oberfläche mithilfe der Rollenverwaltung zugewiesen (siehe Kapitel *9.2* (Seite 189)).

Das Erstellen und Verwalten von Berechtigungen über die Seite *Berechtigungen* wird nur erfahrenen Benutzern empfohlen, die nach einer bestimmten Berechtigung suchen.

9.4.1.1 Eine Berechtigung erstellen

Eine neue Berechtigung kann wie folgt erstellt werden:

1. *Administration* > *Berechtigungen* in der Menüleiste wählen.
2. Neue Berechtigung durch Klicken auf ☆ erstellen.
3. Berechtigung definieren (siehe Abb. 9.6).
4. Auf *Speichern* klicken.

   → Die Berechtigung wird erstellt und auf der Seite *Berechtigungen* angezeigt.

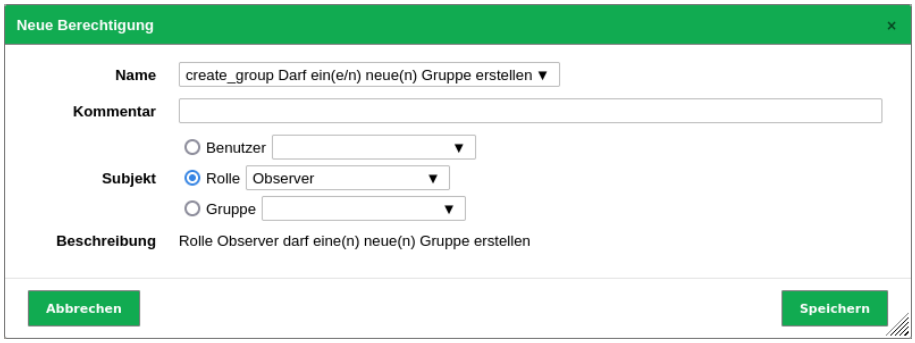


Abb. 9.6: Erstellen einer neuen Berechtigung

Die folgenden Details der Berechtigung können festgelegt werden:

Name Berechtigung, die erteilt werden soll.

Kommentar (optional) Ein Kommentar beschreibt die Berechtigung genauer.

Subjekt Subjekt (Benutzer, Rolle oder Gruppe), das die Berechtigung erhalten soll.

Bemerkung: Die Subjekte, denen die Berechtigung zugewiesen werden kann, hängen von der Rolle des aktuell eingeloggten Benutzers ab. Normale Benutzer (*User*) können anderen Benutzern Berechtigungen erteilen, während Administratoren Benutzern, Rollen und Gruppen Berechtigungen erteilen können.

Ressourcen-Typ (nur für die Berechtigung *Super (hat Super-Zugriff)*) Ressourcentyp (Benutzer/Rolle/Gruppe), auf welchen der Benutzer/die Rolle/die Gruppe Super-Zugriff hat.

Benutzer-/Rollen-/Gruppen-ID (nur für die Berechtigung *Super (hat Super-Zugriff)*) ID der Ressource (Benutzer/Rolle/Gruppe), auf welche der Benutzer/die Rolle/die Gruppe Super-Zugriff hat.

Beschreibung Textliche Beschreibung der Berechtigung.

9.4.1.2 Berechtigungen von der Detailseite einer Ressource aus erstellen

Berechtigungen können wie folgt direkt von der Detailseite einer Ressource, z. B. einer Aufgabe, aus erstellt werden:

1. Detailseite der Ressource öffnen.

   Beispiel: *Scans* > *Aufgaben* in der Menüleiste wählen.

2. Auf den Namen der Aufgabe klicken.
3. Auf 🔍 klicken, um die Detailseite der Aufgabe zu öffnen.
4. Auf den Register *Berechtigungen* klicken.
5. Im geöffneten Abschnitt *Berechtigungen* auf 🆕 klicken.
6. Berechtigung definieren (siehe Abb. 9.7).
7. Auf *Speichern* klicken.

   → Die Berechtigung wird erstellt und im Abschnitt *Berechtigungen* auf der Detailseite der Ressource angezeigt.

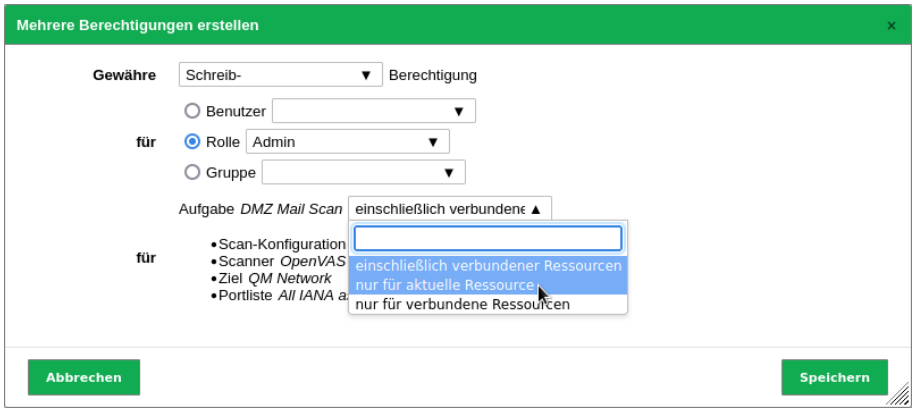


Abb. 9.7: Erstellen einer Berechtigung von der Detailseite einer Ressource aus

Es gibt zwei Arten von Berechtigungen, die direkt auf der Detailseite der Ressource erteilt werden können:

- ***lesen*** Die Berechtigung *lesen* bedeutet, dass die Ressource auf Listenseiten sichtbar ist und ihre Detailseite geöffnet werden kann.
- ***schreiben*** Die Berechtigung *schreiben* bedeutet, dass die Ressource auf Listenseiten sichtbar ist, ihre Detailseite geöffnet werden kann und die Ressource bearbeitet (aber nicht gelöscht) werden kann.

Einige Ressourcen bringen zusätzliche Berechtigungen mit sich:

- **Aufgaben** Wenn die Berechtigung *schreiben* für eine Aufgabe erteilt wird, werden die Berechtigungen, die Aufgabe zu starten (*start_task*), zu stoppen (*stop_task*) und fortzusetzen (*resume_task*) automatisch hinzugefügt.
- **Benachrichtigungen** Wenn die Berechtigung *schreiben* für eine Benachrichtigung erteilt wird, wird die Berechtigungen, die Benachrichtigung zu testen (*test_alert*) automatisch hinzugefügt.
- **Berichtformate und Scanner** Wenn die Berechtigung *schreiben* für ein Berichtformat oder einen Scanner erteilt wird, wird die Berechtigung, das Berichtformat/den Scanner zu verifizieren (*verify_report_format*/*verify_scanner*) automatisch hinzugefügt.

Für einige Ressourcentypen kann gewählt werden, ob die Berechtigungen auch für verbundene Ressourcen erteilt werden sollen (siehe Abb. 9.7).

- **Aufgaben** Für Aufgaben schließt dies Benachrichtigungen und deren Filter, Ziele und deren verknüpfte Anmeldedaten und Portlisten, Zeitpläne, den Scanner und die Scan-Konfiguration mit ein.
- **Ziele** Für Ziele schließt dies Anmeldedaten und Portlisten mit ein.
- **Benachrichtigungen** Für Benachrichtigungen schließt dies den Filter, der auf den Bericht angewendet wird, mit ein.

Bemerkung: Berechtigungen können auch nur für die angegebene Ressource erstellt werden.

Die Details der zugehörigen Ressource werden unterhalb der Drop-down-Liste angezeigt.

9.4.1.3 Berechtigungen verwalten

Listenseite

Alle vorhandenen Berechtigungen können angezeigt werden, indem *Administration* > *Berechtigungen* in der Menüleiste gewählt wird.

Für alle Berechtigungen werden die folgenden Informationen angezeigt:

Name Name der Berechtigung. Eine globale Berechtigung ist mit gekennzeichnet.

Beschreibung Textliche Beschreibung der Berechtigung.

Ressourcen-Typ Ressourcentyp, auf welchen der Benutzer/die Rolle/die Gruppe Zugriff hat.

Ressource Name der Ressource, auf die der Benutzer/die Rolle/die Gruppe Zugriff hat.

Subjekttyp Subjekttyp (Benutzer/Rolle/Gruppe), der die Berechtigung erhält.

Subjekt Subjekt, das die Berechtigung erhält.

Für alle Berechtigungen sind die folgenden Aktionen verfügbar:

- Die Berechtigung in den Papierkorb verschieben. Nur selbst erstellte Berechtigungen können in den Papierkorb verschoben werden.
- Die Berechtigung bearbeiten. Nur selbst erstellte Berechtigungen können bearbeitet werden.
- Die Berechtigung klonen. Nur selbst erstellte Berechtigungen können geklont werden.
- Die Berechtigung als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Berechtigungen können mehrere Berechtigungen zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Berechtigungen in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Berechtigung werden Details der Berechtigung angezeigt. Durch Klicken auf wird die Detailseite der Berechtigung geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Berechtigung.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Berechtigungen anzeigen.
- Eine neue Berechtigung erstellen (siehe Kapitel *9.4.1.1* (Seite 195)).
- Die Berechtigung klonen. Nur selbst erstellte Berechtigungen können geklont werden.
- Die Berechtigung bearbeiten. Nur selbst erstellte Berechtigungen können bearbeitet werden.
- Die Berechtigung in den Papierkorb verschieben. Nur selbst erstellte Berechtigungen können in den Papierkorb verschoben werden.
- Die Berechtigung als XML-Datei exportieren.

9.4.2 Super-Berechtigungen erteilen

Jede Ressource, die auf der Appliance erstellt wird (z. B. ein Benutzer, eine Aufgabe, ein Ziel) ist entweder global oder gehört einem bestimmten Benutzer. Globale Ressourcen sind mit gekennzeichnet.

Nicht-globale Ressourcen sind nur für ihren Eigentümer sicht- und nutzbar. Individuelle Berechtigungen sind nötig, um eine Ressource für andere Benutzer verfügbar zu machen, was sehr mühsam ist.

Um das zu vermeiden, können Benutzer, Rollen und Gruppen Super-Berechtigungen erhalten. Diese ermöglichen den Zugriff auf alle Objekte anderer Benutzer, Rollen oder Gruppen.

Ein Benutzer kann Super-Berechtigungen für Folgendes erhalten:

- Benutzer
- Rollen
- Gruppen
- Alles

Diese Super-Berechtigungen ermöglichen den Zugriff auf alle Ressourcen, die dem Benutzer/der Rolle/der Gruppe gehören oder auf im Grunde alle vorhandenen Ressourcen.

Bemerkung: Die Super-Berechtigung *Alles* kann nicht explizit vergeben werden. Sie ist auf den Super-Administrator (siehe Kapitel *9.2.5* (Seite 192)) beschränkt und kann nur beim Erstellen eines solchen erteilt werden.

Ein Benutzer kann Super-Berechtigungen nur für selbst erstellte Objekte erteilen. Nur der Super-Administrator kann allen anderen Benutzern, Rollen und Gruppen Super-Berechtigungen erteilen.

1. Auf den Namen des Benutzers/der Rolle/der Gruppe auf der Seite *Benutzer*/*Rollen*/*Gruppen* klicken, für den oder für die die Super-Berechtigungen erteilt werden sollen.
2. Detailseite durch Klicken auf öffnen.

   → Die ID der Ressource befindet sich in der rechten oberen Ecke (siehe Abb. 9.8).

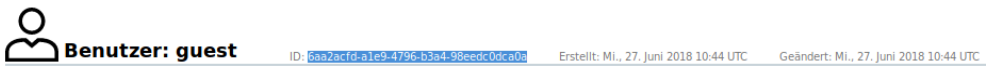


Abb. 9.8: ID einer Ressource

3. ID notieren oder kopieren.
4. *Administration* > *Berechtigungen* in der Menüleiste wählen.
5. Neue Berechtigung durch Klicken auf erstellen.
6. *Super (hat Super-Zugriff)* in der Drop-down-Liste *Name* wählen (siehe Abb. 9.9).
7. Radiobutton des Subjekttyps, der die Super-Berechtigungen erhalten soll, wählen.
8. Benutzer/Rolle/Gruppe, der oder die die Super-Berechtigungen erhalten soll, in der entsprechenden Drop-down-Liste wählen.
9. Ressourcentyp, für den die Super-Berechtigungen erteilt werden sollen, in der Drop-down-Liste *Ressourcen-Typ* wählen.
10. Zuvor ermittelte ID in das Eingabefeld *Benutzer-ID*/*Rollen-ID*/*Gruppen-ID* eingeben oder einfügen.
11. Auf *Speichern* klicken.

    → Die Super-Berechtigung wird erstellt und auf der Seite *Berechtigungen* angezeigt.

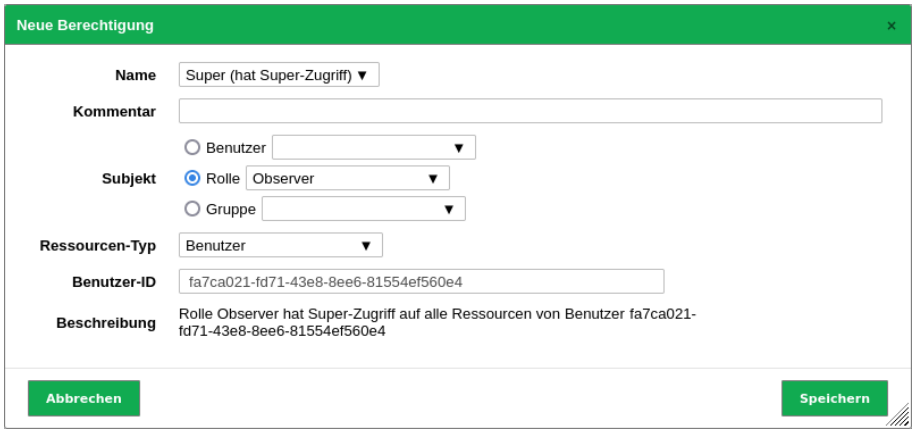


Abb. 9.9: Erstellen einer neuen Super-Berechtigung

Tipp: Super-Berechtigungen vereinfachen die Berechtigungsverwaltung auf der Appliance. Sie können einfach an gesamte Gruppen vergeben werden. Dies ermöglicht allen Benutzern der Gruppen den Zugriff auf alle Ressourcen, die von anderen Mitgliedern der Gruppe erstellt wurden.

9.4.3 Anderen Benutzern Lesezugriff erteilen

9.4.3.1 Anforderungen, um Lesezugriff zu erteilen

Jeder Benutzer kann eine unbegrenzte Anzahl selbst erstellter Ressourcen teilen. Dazu benötigt der Nutzer sowohl die **globale** *get_users*-Berechtigung als auch die **spezifische** *get_users*-Berechtigung für den Nutzer, der Lesezugriff erhalten soll.

Bemerkung: Der einfachste und empfohlene Weg, selbst erstellte Ressourcen zu teilen, ist es, einen Administratoraccount zu nutzen und die Accounts, die Lesezugriff erhalten sollen, mit diesem Administratoraccount zu erstellen.

Alle anderen hier beschriebenen Wege sind umständlich und zeitaufwendig.

Anforderungen für Administratoren

Administratoren haben standardmäßig bereits die globale *get_users*-Berechtigung.

Der Administrator kann die spezifische *get_users*-Berechtigung für den Account, der Lesezugriff erhalten soll, auf zwei Arten bekommen:

- Den Account selbst erstellen, da Administratoren automatisch die spezifische *get_users*-Berechtigung für von ihnen erstellte Accounts haben.
- Mithilfe eines Super-Administrators.

Ein Super-Administrator kann einem Administrator spezifische *get_users*-Berechtigungen wie folgt erteilen:

1. Als Super-Administrator in die Web-Oberfläche einloggen (siehe Kapitel *7.2.1.5* (Seite 74) und *9.2.5* (Seite 192)).
2. *Administration* > *Benutzer* in der Menüleiste wählen.
3. Auf den Namen des Accounts klicken, der Lesezugriff vom Administrator erhalten soll.
4. Auf 🔍 klicken.

5. Auf den Register *Berechtigungen* klicken.
6. Neue Berechtigung durch Klicken auf ☆ im Abschnitt *Berechtigungen* erstellen.
7. *lesen* in der Drop-down-Liste *Gewähre* wählen (siehe Abb. 9.10).

Abb. 9.10: Erteilen einer spezifischen *get_users*-Berechtigung an einen Administrator

8. Radiobutton *Benutzer* wählen.
9. Administrator, der in der Lage sein soll, Lesezugriff zu erteilen, in der Drop-down-Liste *Benutzer* wählen.
10. Auf *Speichern* klicken.

    → Die spezifische *get_users*-Berechtigung wird erstellt und in der Liste angezeigt (siehe Abb. 9.11).

    Der Administrator ist nun in der Lage, dem entsprechenden Nutzer Lesezugriff, wie in Kapitel *9.4.3.2* (Seite 203) beschrieben, zu erteilen.

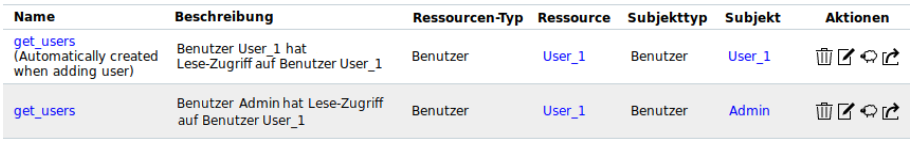


Abb. 9.11: Spezifische *get_users*-Berechtigung für einen Administrator

Anforderungen für normale Nutzer

Normale Nutzer haben die globale *get_users*-Berechtigung nicht standardmäßig. Sie kann wie folgt hinzugefügt werden:

1. Als Administrator einloggen.
2. *Administration* > *Rollen* in der Menüleiste wählen.
3. Neue Rolle durch Klicken auf ☆ erstellen.
4. `LeserechtGewähren` in das Eingabefeld *Name* eingeben.
5. Auf *Speichern* klicken.

   → Die Rolle wird erstellt und auf der Seite *Rollen* angezeigt.
6. In der Zeile der neu erstellen Rolle auf ✎ klicken.
7. *get_users* in der Drop-down-Liste *Name* im Abschnitt *Neue Berechtigung* wählen (siehe Abb. 9.12).
8. Auf *Berechtigung erstellen* klicken.

   → Die Berechtigung wird im Abschnitt *Generelle Berechtigungen für Befehle* angezeigt (siehe Abb. 9.12).
9. Auf *Speichern* klicken.
10. *Administration* > *Benutzer* in der Menüleiste wählen.

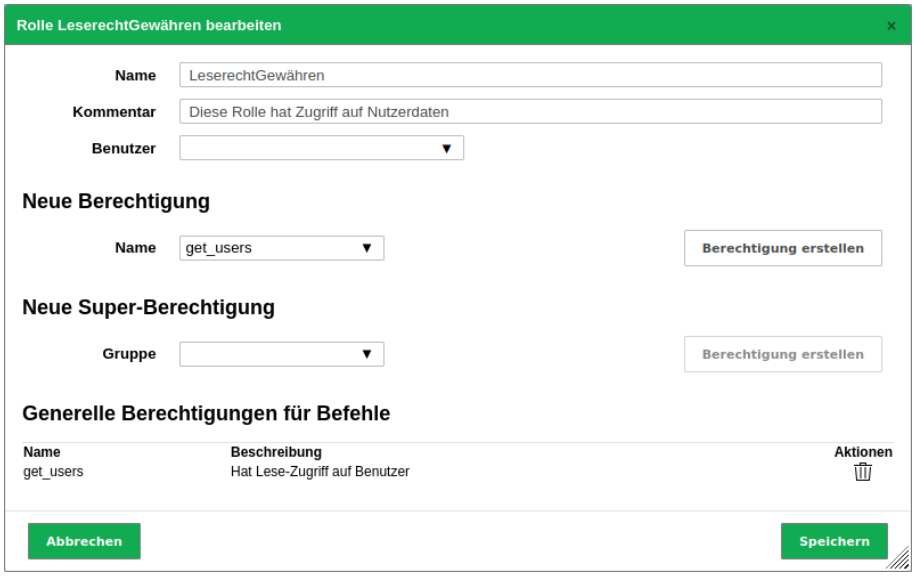


Abb. 9.12: Wählen der Berechtigungen für eine neue Rolle

11. In der Zeile des Benutzers, welchem die neu erstellte Rolle zugewiesen werden soll, auf klicken.
12. Rolle *LeserechtGewähren* in der Drop-down-Liste *Rollen* hinzufügen.
13. Auf *Speichern* klicken.

Ein Super-Administrator kann einem Nutzer spezifische *get_users*-Berechtigungen wie folgt erteilen:

1. Als Super-Administrator in die Web-Oberfläche einloggen (siehe Kapitel *7.2.1.5* (Seite 74) und *9.2.5* (Seite 192)).
2. *Administration* > *Benutzer* in der Menüleiste wählen.
3. Auf den Namen des Accounts klicken, der Lesezugriff vom Nutzer erhalten soll.
4. Auf klicken.
5. Auf den Register *Berechtigungen* klicken.
6. Im Abschnitt *Berechtigungen* auf klicken.
7. *lesen* in der Drop-down-Liste *Gewähre* wählen (siehe Abb. 9.13).

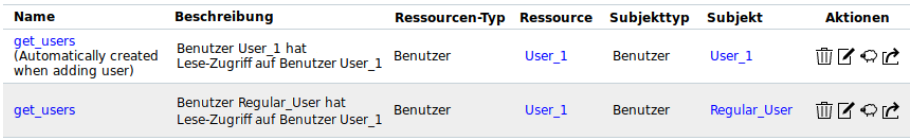
Abb. 9.13: Erteilen einer spezifischen *get_users*-Berechtigung an einen Nutzer

8. Radiobutton *Benutzer* wählen.
9. Nutzer, der in der Lage sein soll, Lesezugriff zu erteilen, in der Drop-down-Liste *Benutzer* wählen.

10. Auf *Speichern* klicken.

    → Die spezifische *get_users*-Berechtigung wird erstellt und in der Liste angezeigt (siehe Abb. 9.14).

    Der Nutzer ist nun in der Lage, dem entsprechenden Nutzer Lesezugriff, wie in Kapitel *9.4.3.2* (Seite 203) beschrieben, zu erteilen.



Name	Beschreibung	Ressourcen-Typ	Ressource	Subjekttyp	Subjekt	Aktionen
get_users (Automatically created when adding user)	Benutzer User_1 hat Lese-Zugriff auf Benutzer User_1	Benutzer	User_1	Benutzer	User_1	
get_users	Benutzer Regular_User hat Lese-Zugriff auf Benutzer User_1	Benutzer	User_1	Benutzer	Regular_User	

Abb. 9.14: Spezifische *get_users*-Berechtigung für einen Nutzer

9.4.3.2 Lesezugriff erteilen

Wenn ein Nutzer die **globale** und die **spezifische** *get_users*-Berechtigung hat (siehe Kapitel *9.4.3.1* (Seite 200)), kann der Nutzer Ressourcen wie folgt teilen:

1. Auf der entsprechenden Seite auf den Namen der Ressource klicken, die geteilt werden soll.
2. Detailseite durch Klicken auf 🔍 öffnen.

   → Die ID der Ressource befindet sich in der rechten oberen Ecke (siehe Abb. 9.15).

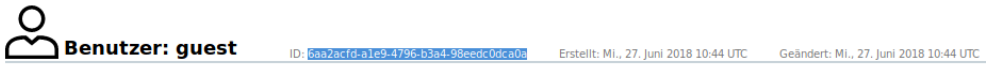


Abb. 9.15: ID einer Ressource

3. ID notieren oder kopieren.
4. *Administration > Berechtigungen* in der Menüleiste wählen.
5. Neue Berechtigung durch Klicken auf erstellen.
6. Die Berechtigung für das Objekt, das geteilt werden soll, in der Drop-down-Liste *Name* wählen.
   - Filter: *get_filters*
   - Scan-Konfiguration: *get_configs*
   - Benachrichtigung: *get_alerts*
   - Notiz: *get_notes*
   - Übersteuerung: *get_overrides*
   - Tag: *get_tags*
   - Ziel: *get_targets*
   - Aufgabe einschließlich Bericht: *get_tasks*
   - Zeitplan: *get_schedules*
7. Radiobutton *Benutzer* wählen (siehe Abb. 9.16).
8. Benutzer, mit dem das Objekt geteilt werden soll, in der entsprechenden Drop-down-Liste wählen.
9. Zuvor ermittelte ID in das Eingabefeld *Ressourcen-ID* eingeben oder einfügen.
10. Auf *Speichern* klicken.

    → Die Berechtigung wird erstellt und auf der Seite *Berechtigungen* angezeigt.

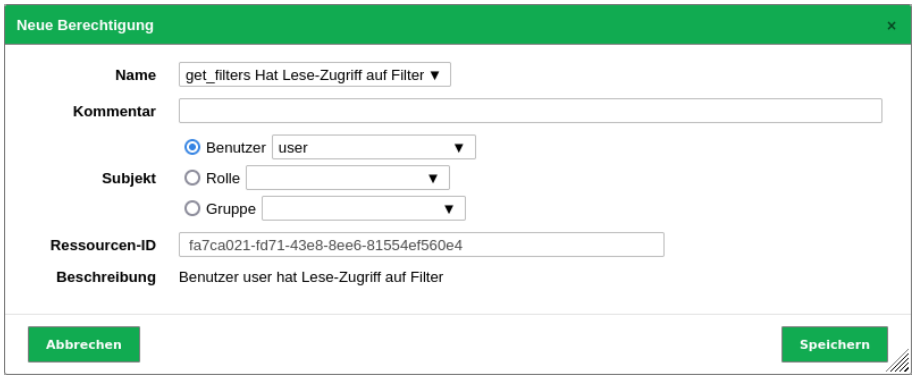


Abb. 9.16: Objekte mit anderen Benutzern teilen

Bemerkung: Zusätzlich können Ressourcen mit Rollen oder Gruppen geteilt werden.

Dazu werden die globalen und spezifischen Berechtigungen *get_groups* – einer Gruppe Lesezugriff erteilen – oder *get_roles* – einer Rolle Lesezugriff erteilen – benötigt. Diese folgen dem gleichen Prinzip wie in Kapitel *9.4.3.1* (Seite 200) beschrieben.

Ausnahme: Nutzer mit einer Standardrolle haben die spezifischen *get_roles*-Berechtigungen für alle Standardrollen.

9.5 Eine zentrale Benutzerverwaltung nutzen

Besonders in großen Umgebungen mit mehreren Benutzern ist es schwierig, eine Passwortsynchronisierung zu verwirklichen. Der Aufwand, um Passwörter zu erstellen oder zurückzusetzen ist oft sehr hoch. Um dies zu vermeiden, unterstützt die Appliance die Nutzung eines zentralen Passwortspeichers mit LDAPS oder RADIUS.

Die Appliance nutzt den Service für die Authentifizierung auf einer Pro-Benutzer-Basis, das heißt, jeder Benutzer, der sich mithilfe des Service authentifizieren soll, muss für die Authentifizierung konfiguriert und auch auf der Appliance vorhanden sein.

Bemerkung: Voraussetzung für die Nutzung der zentralen Authentifizierung ist die Benennung der Benutzer mit denselben Namen wie die Objekte im LDAPS-Baum oder dem RADIUS-Server.

9.5.1 LDAPS

Die Appliance unterstützt nur verschlüsselte Verbindungen über LDAP mit StartTLS (Port 389) oder LDAPS mit SSL/TLS (Port 636). Der LDAPS-Server muss seinen Service für SSL/TLS verfügbar machen.

Die folgenden Referenzen sind für die exakte Konfiguration aller verfügbaren LDAPS-Servern hilfreich:

- Microsoft: https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
- OpenLDAP: https://www.openldap.org/doc/admin24/tls.html

9.5.1.1 Das Zertifikat des Servers auf der Appliance speichern

Zum Verifizieren der Identität des LDAPS-Servers, muss die Appliance dem Zertifikat des Servers vertrauen. Dafür muss das Zertifikat der herausgebenden Zertifizierungsstelle auf der Appliance gespeichert werden.

Dazu muss das Zertifikat der Zertifizierungsstelle als Base64-codierte Datei exportiert werden. Eine Base64-codierte Datei hat oft die Dateiendung `.pem`. Die Datei selbst beginnt mit `------BEGIN CERTIFICATE-------`.

Falls die Zertifizierungsstelle eine zwischenliegende Zertifizierungsstelle ist, muss die komplette Zertifizierungskette importiert werden. Dies trifft oft zu, wenn eine offizielle Zertifizierungsstelle genutzt wird, da die ursprüngliche Zertifizierungsstelle von der ausgebenden Zertifizierungsstelle getrennt ist.

In diesen Fällen sieht der Inhalt der Datei wie folgt aus:

```
-----BEGIN CERTIFICATE-----
......
Issuing CA
......
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
......
Root CA
......
-----END CERTIFICATE-----
```

Der tatsächliche Speicherort, an der das Zertifikat gefunden werden kann, kann basierend auf der Umgebung variieren.

- Univention Corporate Server (UCS)

  Hier wird das Zertifikat von der Datei `/etc/univention/ssl/ucsCA/CAcert.pem` abgerufen. Diese Datei enthält bereits das Zertifikat im korrekten Format und muss beim Aktivieren von LDAPS hochgeladen werden.

- Active-Directory-LDAPS

  Falls der Service Active-Directory-LDAP noch nicht LDAPS nutzt, könnte der folgende Artikel hilfreich sein: https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx.

  Das Zertifikat der Zertifizierungsstelle, die das Active-Directory-LDAPS-Zertifikat ausstellt, kann dann wie folgt exportiert werden:

  Bemerkung: Die Schritte müssen von einem Desktop-PC oder einem Server mit Zugang zur Zertifizierungsstellenkonsole ausgeführt werden.

  ---

  1. Zertifizierungsstellenkonsole von einem an eine Domäne angeschlossenen Computer oder Server aus öffnen.
  2. Auf den Namen der Zertifizierungsstelle rechtsklicken und *Properties* wählen.
  3. Im Zertifikat-Fenster den Tab *General* wählen.
  4. Zertifikat, auf das zugegriffen werden soll, für die Zertifizierungsstelle wählen.
  5. Auf *View Certificate* klicken.
  6. Im Fenster *Certificate* den Tab *Certification Authority* wählen.
  7. Namen der ursprünglichen Zertifizierungsstelle wählen und auf *View Certificate* klicken.
  8. Im Fenster *Certificate* den Tab *Details* wählen.
  9. Auf *Copy to File* klicken.

     → Der Wizard zum Exportieren des Zertifikats wird geöffnet.
  10. Auf *Next* klicken.
  11. *Base-64 encoded X.509 (.CER)* auf der Seite *Export File Format* wählen.
  12. Auf *Next* klicken.
  13. Pfad und Namen für das Zertifikat in das Eingabefeld *File to Export* eingeben.
  14. Auf *Next* klicken.
  15. Auf *Finish* klicken.

      → Die CER-Datei wird am angegebenen Speicherort erstellt. Das Fenster informiert den Benutzer darüber, dass der Export erfolgreich war.
  16. Auf *OK* klicken.

  Der Inhalt der Datei muss hochgeladen werden, wenn LDAPS aktiviert wird.

9.5.1.2 Mit dem LDAPS-Baum verbinden

Für die Verbindung mit einem LDAPS-Baum nutzt die Appliance eine einfache Schnittstelle und eine simple Bind-Operation mit einem fest codierten Objektpfad. Die LDAPS-Authentifizierung wird wie folgt durchgeführt:

1. Als Administrator einloggen.
2. *Administration* > *LDAP* in der Menüleiste wählen.
3. Auf ✎ klicken.
4. Checkbox *Aktivieren* aktivieren (siehe Abb. 9.17).

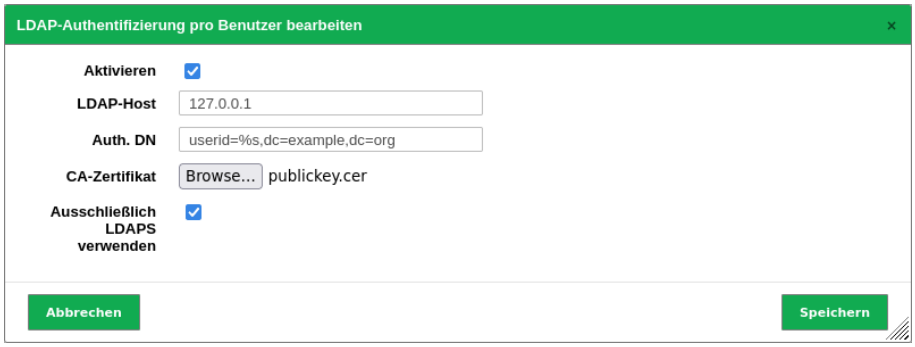


Abb. 9.17: Konfigurieren einer LDAPS-Authentifizierung

5. LDAPS-Host in das Eingabefeld *LDAP-Host* eingeben.

Bemerkung: Nur ein System kann per IP-Adresse oder Name eingegeben werden.

Die Appliance greift mithilfe von SSL/TLS auf den LDAPS-Host zu. Um den Host zu verifizieren, muss das Zertifikat des Hosts auf die Appliance hochgeladen werden (siehe Kapitel *9.5.1.1* (Seite 205)). Ohne SSL/TLS wird die LDAPS-Authentifizierung nicht akzeptiert.

---

6. Distinguished name (DN) des Objekts in das Eingabefeld *Auth. DN* eingeben.

Bemerkung: Der Platzhalter `%s` ersetzt den Benutzernamen.

Beispiele für *Auth. DN* sind:

- **`cn=%s,ou=people,dc=domain,dc=de`** Dieses Format funktioniert für jeden LDAPS-Server mit den korrekten Attributen. Das Attribut *cn* (common name) wird genutzt. Benutzer in anderen Teilbäumen oder anderen rekursiven Tiefen des LDAPS-Baums werden nicht unterstützt. Alle Benutzer, die sich in die Appliance einloggen, müssen sich im selben Zweig und auf dem gleichen Level des LDAPS-Baums befinden.
- **`uid=%s,ou=people,dc=domain,dc=de`** Dieses Format funktioniert für jeden LDAPS-Server mit den korrekten Attributen. Das Attribut *uid* (user ID) wird als Filter genutzt. Es sollte an erster Stelle stehen. Die Attribute *ou=people,dc=domain,dc=de* werden als Basisobjekte für die Suche und für den Abruf des entsprechenden DN genutzt.
- **`%s@domain.de`** Dieses Format wird typischerweise von Active Directory genutzt. Der exakte Speicherort eines Benutzerobjekts ist irrelevant.
- **`domain.de\%s`** Dieses Format wird typischerweise von Active Directory genutzt. Der exakte Speicherort eines Benutzerobjekts ist irrelevant.

---

7. Zum Verifizieren des Hosts auf *Browse...* klicken, um das Zertifikat des Hosts hochzuladen.

8. Checkbox *Ausschließlich LDAPS verwenden* aktivieren, falls nur Verbindungen über LDAPS erlaubt sein sollen.

   Bemerkung: Mit dieser Option werden StartTLS- und Klartextverbindungen zum LDAP-Server deaktiviert und nur Verbindungen über LDAPS zugelassen. Dies ist nützlich, wenn der LDAP-Port durch eine Firewall blockiert ist.

9. Auf *OK* klicken.

   → Wenn die LDAPS-Authentifizierung aktiviert ist (siehe Abb. 9.18), ist die Option *Nur LDAP-Authentifizierung* beim Erstellen oder Bearbeiten eines Benutzers verfügbar. Standardmäßig ist diese Option deaktiviert.

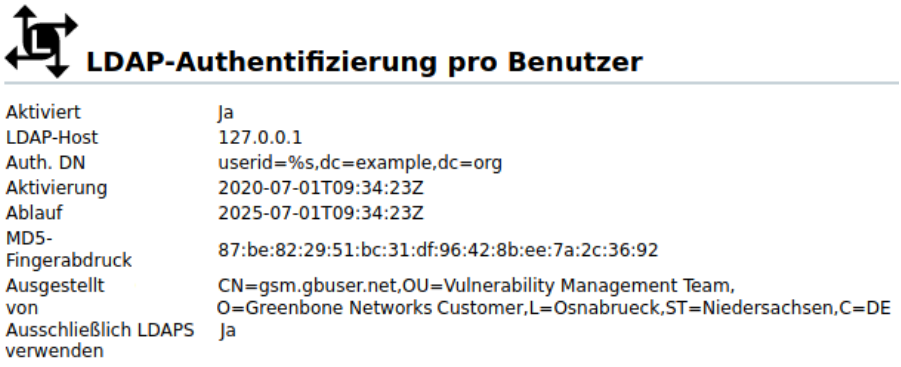


Abb. 9.18: Aktivierte LDAPS-Authentifizierung

10. Neuen Benutzer erstellen oder vorhandenen Benutzer bearbeiten (siehe Kapitel *9.1* (Seite 184)).
11. Checkbox *Nur LDAP-Authentifizierung* aktivieren, falls der Benutzer die Möglichkeit haben soll, sich per LDAPS zu authentifizieren (siehe Abb. 9.19).

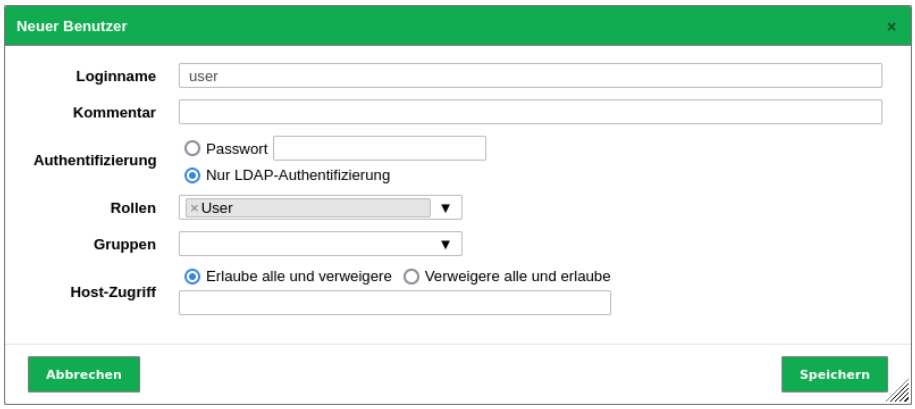


Abb. 9.19: Aktivieren der Authentifizierung mit LDAPS

Bemerkung: Der Benutzer muss mit demselben Namen wie in LDAPS vorhanden sein, bevor LDAPS genutzt werden kann. Die Appliance kann keine Benutzer in LDAPS hinzufügen, bearbeiten oder entfernen und erteilt Benutzern von LDAPS keinen automatischen Zugriff auf die Appliance.

Falls die LDAPS-Authentifizierung nicht funktioniert, muss überprüft werden, ob der Eintrag im Eingabefeld *LDAP-Host* mit dem commonName des Zertifikats des LDAPS-Servers übereinstimmt. Falls es Abweichungen gibt, verweigert die Appliance die Nutzung des LDAPS-Servers.

9.5.2 RADIUS

Die RADIUS-Authentifizierung wird wie folgt durchgeführt:

1. Als Administrator einloggen.
2. *Administration* > *Radius* in der Menüleiste wählen.
3. Auf ☑ klicken.
4. Checkbox *Aktivieren* aktivieren (siehe Abb. 9.20).
5. Hostnamen oder IP-Adresse des RADIUS-Servers in das Eingabefeld *RADIUS-Host* eingeben.
6. Gemeinsamen geheimen Schlüssel in das Eingabefeld *Geheimer Schlüssel* eingeben.

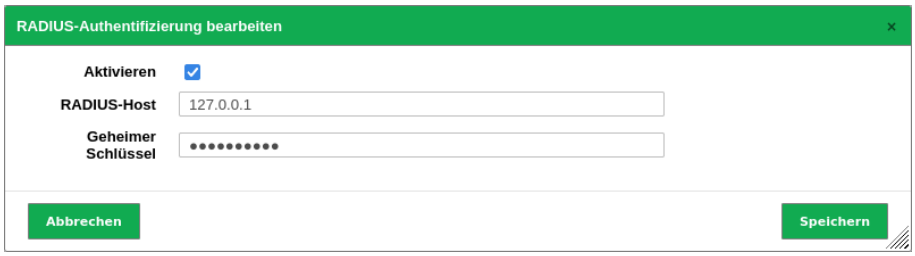


Abb. 9.20: Konfigurieren einer RADIUS-Authentifizierung

7. Auf *OK* klicken.

   → Wenn die RADIUS-Authentifizierung aktiviert ist, ist die Option *Nur RADIUS-Authentifizierung* beim Erstellen oder Bearbeiten eines Benutzers verfügbar. Standardmäßig ist diese Option deaktiviert.
8. Neuen Benutzer erstellen oder vorhandenen Benutzer bearbeiten (siehe Kapitel *9.1* (Seite 184)).
9. Checkbox *Nur RADIUS-Authentifizierung* aktivieren, falls der Benutzer die Möglichkeit haben soll, sich per RADIUS zu authentifizieren (siehe Abb. 9.21).

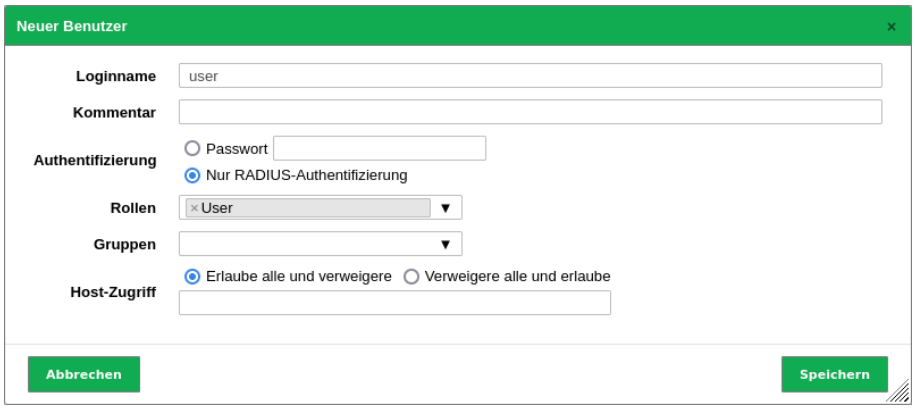


Abb. 9.21: Aktivieren der Authentifizierung mit RADIUS

KAPITEL 10

Ein System scannen

Bemerkung: Dieses Kapitel dokumentiert alle möglichen Menüoptionen.

Allerdings unterstützen nicht alle Appliance-Modelle alle Menüoptionen. Um festzustellen, ob ein bestimmtes Feature für das genutzte Appliance-Modell verfügbar ist, können die Tabellen in Kapitel *3* (Seite 20) genutzt werden.

10.1 Den Aufgaben-Wizard für einen ersten Scan nutzen

Der Aufgaben-Wizard kann einen Basisscan mit minimalem Input vom Benutzer konfigurieren und starten.

10.1.1 Den Aufgaben-Wizard nutzen

Eine neue Aufgabe kann wie folgt mit dem Aufgaben-Wizard konfiguriert werden:

1. *Scans > Aufgaben* in der Menüleiste wählen.
2. Wizard durch Bewegen der Maus über und Klicken auf *Aufgaben-Wizard* starten.
3. IP-Adresse oder Hostnamen des Zielsystems in das Eingabefeld eingeben (siehe Abb. 10.1).

   Bemerkung: Beim Nutzen eines DNS-Namens muss die Appliance in der Lage sein, diesen Namen aufzuschlüsseln.

4. Auf *Scan starten* klicken.

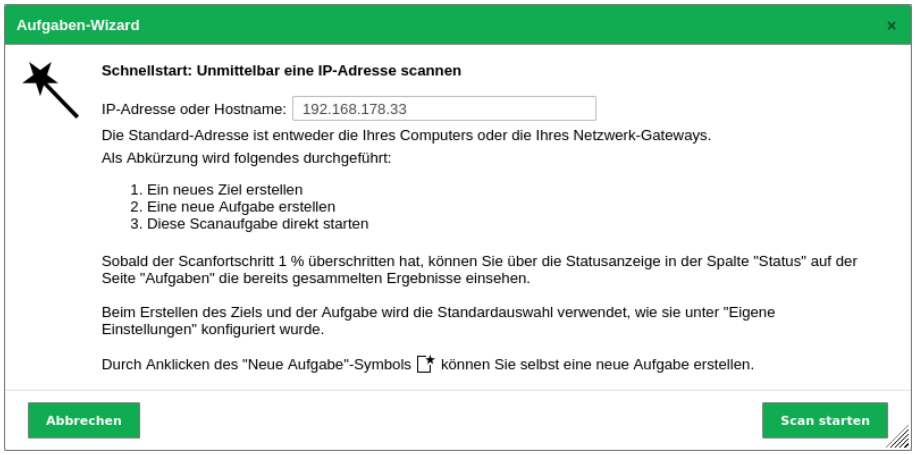


Abb. 10.1: Den Aufgaben-Wizard konfigurieren

→ Der Aufgaben-Wizard führt die folgenden Schritte automatisch aus:

1. Erstellen eines neuen Scanziels auf der Appliance.
2. Erstellen einer neuen Scanaufgabe auf der Appliance.
3. Unmittelbares Starten der Scanaufgabe.
4. Darstellen der Seite *Aufgaben*.

Nachdem die Aufgabe gestartet wurde, kann der Fortschritt überwacht werden (siehe Abb. 10.2).

Abb. 10.2: Seite *Aufgaben* mit Fortschritt der Aufgabe

Für den Status einer Aufgabe siehe Kapitel *10.8* (Seite 257).

Tipp: Sobald eine Aufgabe gestartet wurde, kann der Bericht der Aufgabe durch Klicken auf den Balken in der Spalte *Status* dargestellt werden. Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *11* (Seite 288).

Sobald sich der Status zu *Abgeschlossen* ändert, ist der gesamte Bericht verfügbar. Zu jeder Zeit können Zwischenergebnisse angesehen werden (siehe Kapitel *11.2.1* (Seite 293)).

Bemerkung: Die Fertigstellung des Scans kann einige Zeit in Anspruch nehmen. Die Seite aktualisiert automatisch, falls neue Daten verfügbar sind.

10.1.2 Den erweiterten Aufgaben-Wizard nutzen

Neben dem einfachen Aufgaben-Wizard stellt die Appliance auch einen erweiterten Aufgaben-Wizard mit mehr Konfigurationsmöglichkeiten bereit.

Eine neue Aufgabe kann wie folgt mit dem erweiterten Aufgaben-Wizard konfiguriert werden:

1. *Scans* > *Aufgaben* in der Menüleiste wählen.
2. Wizard durch Bewegen der Maus über und Klicken auf *Erweiterter Aufgaben-Wizard* starten.
3. Aufgabe festlegen (siehe Abb. 10.3).

Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *10.2.1* (Seite 214) und *10.2.2* (Seite 218).

Falls eine E-Mail-Adresse in das Eingabefeld *E-Mail-Bericht an* eingegeben wird, wird eine Benachrichtigung erstellt, die eine E-Mail versendet, sobald die Aufgabe abgeschlossen ist (siehe Kapitel *10.12* (Seite 277)).

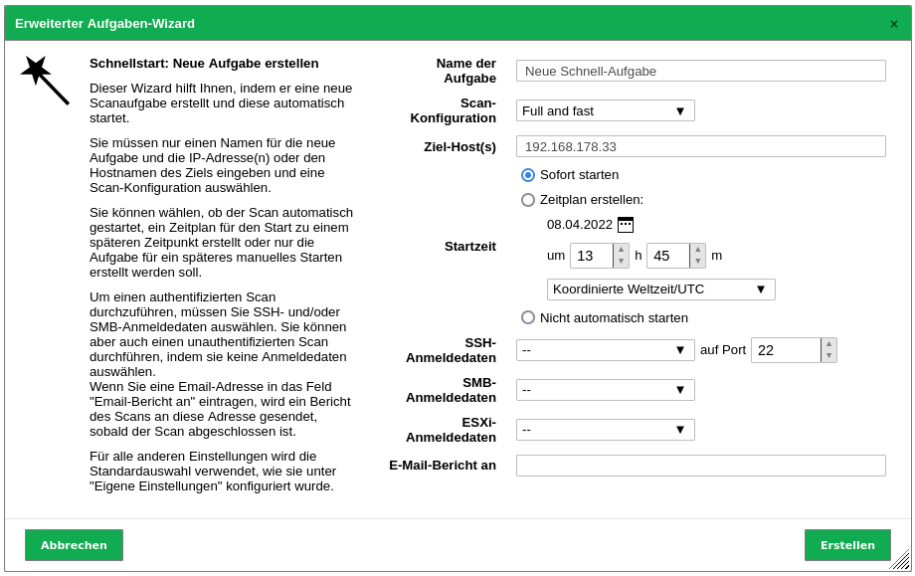


Abb. 10.3: Konfigurieren des erweiterten Aufgaben-Wizards

4. Auf *Erstellen* klicken.

   → Der erweiterte Aufgaben-Wizard führt die folgenden Schritte automatisch aus:

   1. Unmittelbares Starten der Scanaufgabe.
   2. Darstellen der Seite *Aufgaben*.

Für den Status einer Aufgabe siehe Kapitel *10.8* (Seite 257).

Tipp: Sobald eine Aufgabe gestartet wurde, kann der Bericht der Aufgabe durch Klicken auf den Balken in der Spalte *Status* dargestellt werden. Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *11* (Seite 288).

Sobald sich der Status zu *Abgeschlossen* ändert, ist der gesamte Bericht verfügbar. Zu jeder Zeit können Zwischenergebnisse angesehen werden (siehe Kapitel *11.2.1* (Seite 293)).

Bemerkung: Die Fertigstellung des Scans kann einige Zeit in Anspruch nehmen. Die Seite aktualisiert automatisch, falls neue Daten verfügbar sind.

10.1.3 Den Wizard zum Verändern einer Aufgabe nutzen

Ein weiterer Wizard kann eine vorhandene Aufgabe verändern:

1. *Scans* > *Aufgaben* in der Menüleiste wählen.
2. Wizard durch Bewegen der Maus über und Klicken auf *Aufgabe-Bearbeiten-Wizard* starten.
3. Aufgabe, die verändert werden soll, in der Drop-down-Liste *Aufgabe* wählen (siehe Abb. 10.4).

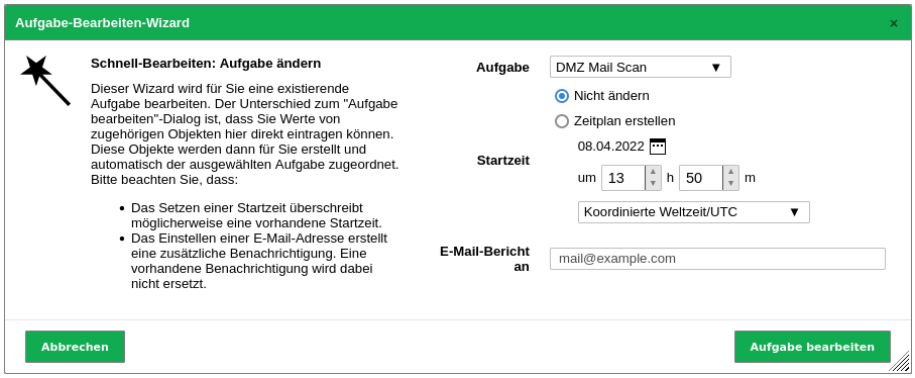


Abb. 10.4: Verändern einer Aufgabe mithilfe des Wizards

4. Zeitplan für die Aufgabe durch Wählen des Radiobuttons *Zeitplan erstellen* erstellen (siehe Kapitel *10.10* (Seite 272)).

   Das Datum des ersten Scans kann duch Klicken auf gewählt und die Zeit kann mithilfe der Eingabefelder festgelegt werden.
5. E-Mail-Adresse, an die ein Bericht gesendet werden soll, in das Eingabefeld *E-Mail-Bericht an* eingeben.
6. Auf *Aufgabe bearbeiten* klicken.

10.2 Einen einfachen Scan manuell konfigurieren

Im Allgemeinen kann die Appliance zwei unterschiedliche Vorgehensweisen nutzen, um ein Ziel zu scannen:

- Einfacher Scan
- Authentifizierter Scan mithilfe lokaler Sicherheitskontrollen

Die folgenden Schritte müssen ausgeführt werden, um einen einfachen Scan zu konfigurieren:

- Erstellen eines Ziels (siehe Kapitel *10.2.1* (Seite 214))
- Erstellen einer Aufgabe (siehe Kapitel *10.2.2* (Seite 218))
- Ausführen der Aufgabe (siehe Kapitel *10.2.3* (Seite 220))

10.2.1 Ein Ziel erstellen

Der erste Schritt ist es, ein Scanziel wie folgt zu erstellen:

1. *Konfiguration* > *Ziele* in der Menüleiste wählen.
2. Neues Ziel durch Klicken auf erstellen.
3. Ziel definieren (siehe Abb. 10.5).

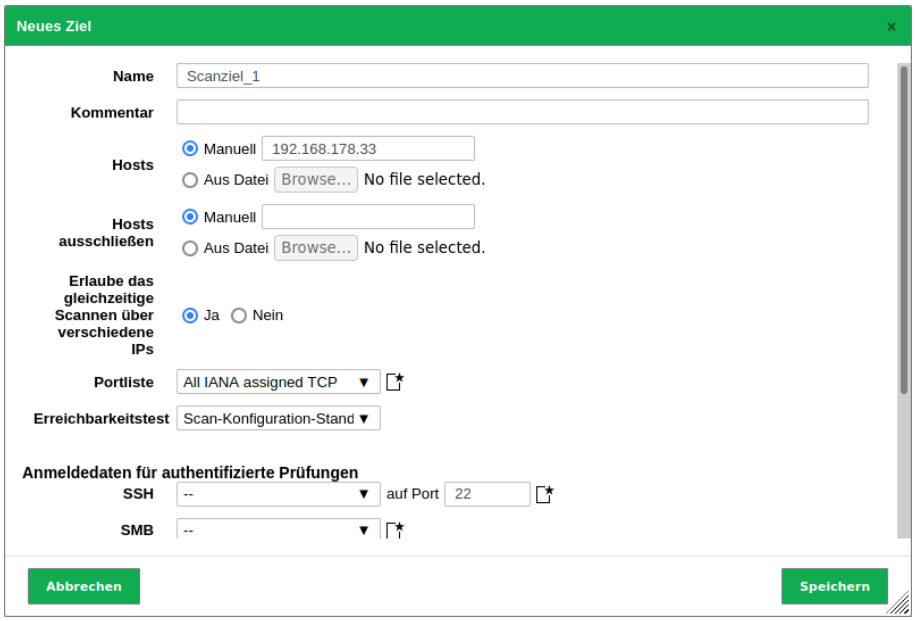


Abb. 10.5: Erstellen eines neuen Ziels

4. Auf *Speichern* klicken.

Die folgenden Informationen können eingegeben werden:

Name Der Name kann frei gewählt werden. Falls möglich, sollte ein aussagekräftiger Name gewählt werden. Möglichkeiten sind Mailserver, ClientNetwork, Webserverfarm, DMZ oder eine nähere Beschreibung des Systems.

Kommentar Der optionale Kommentar erlaubt es, Hintergrundinformationen festzulegen. Diese erleichtern später das Verständnis des konfigurierten Ziel.

Hosts Manuelle Eingabe der Hosts, die gescannt werden sollen, getrennt durch Kommas oder Importieren einer Hostliste.

Bemerkung: Die IP-Adresse oder der Hostname wird benötigt. In beiden Fällen ist es nötig, dass sich die Appliance mit dem System verbinden kann. Falls der Hostname verwendet wird, muss die Appliance in der Lage sein, den Namen aufzuschlüsseln.

Die maximal konfigurierbare Anzahl von IP-Adressen beträgt bei den meisten Appliance-Modellen 4096. Für die Greenbone Enterprise 6500 beträgt die maximal konfigurierbare Anzahl von IP-Adressen 16777216.

Für die manuelle Eingabe sind die folgenden Optionen möglich:

- Einzelne IP-Adresse, z. B. 192.168.15.5
- Hostname, z. B. mail.example.com
- IPv4-Adressbereich in langem Format, z. B. 192.168.15.5-192.168.15.27
- IPv4-Adressbereich in kurzem Format, z. B. 192.168.55.5-27
- IPv4-Adressbereich in CIDR-Schreibweise, z. B. 192.168.15.0/24

Bemerkung: Aufgrund der maximal konfigurierbaren Anzahl von IP-Adressen (siehe oben) beträgt die maximale Subnetzmaske /20 für IPv4, wenn keine weiteren Hosts Teil der Konfiguration sind. Ist die maximale Anzahl der IP-Adressen höher, z. B. bei der Greenbone Enterprise 6500, können entsprechend größere Subnetzmasken konfiguriert werden.

Üblicherweise werden die erste IP-Adresse (Netzwerkadresse, z.B. 192.168.15.0) und die letzte IP-Adresse (Broadcast-Adresse, z.B. 192.168.15.255) eines Subnetzes nicht in die Anzahl der nutzbaren IP-Adressen einbezogen und daher bei Scans nicht berücksichtigt, wenn diese Schreibweise verwendet wird. Wenn die IP-Adressen tatsächlich nutz- und scanbar sind, müssen sie explizit zum Scanziel hinzugefügt werden, z.B. `192.168.15.0/24, 192.168.15.0, 192.168.15.255`.

- Einzelne IPv6-Adresse, z. B. fe80::222:64ff:fe76:4cea
- IPv6-Adressbereich in langem Format, z. B. ::12:fe5:fb50-::12:fe6:100
- IPv6-Adressbereich in kurzem Format, z. B. ::13:fe5:fb50-fb80
- IPv6-Adressbereich in CIDR-Schreibweise, z. B. fe80::222:64ff:fe76:4cea/120

Bemerkung: Aufgrund der maximal konfigurierbaren Anzahl von IP-Adressen (siehe oben) ist die maximale Subnetzmaske für IPv6 /116, wenn keine weiteren Hosts Teil der Konfiguration sind. Ist die maximale Anzahl der IP-Adressen höher, z. B. beim Greenbone Enterprise 6500, können entsprechend größere Subnetzmasken konfiguriert werden.

Mehrere Optionen können gemischt werden. Falls eine Datei importiert wird, muss dieselbe Syntax genutzt werden. Einträge können durch Kommas oder durch Zeilenumbrüche getrennt werden. Falls mehrere Systeme gescannt werden müssen, ist es einfacher eine Datei mit den Hosts zu nutzen, statt alle Hosts manuell einzugeben. Die Datei muss die ASCII-Zeichenkodierung verwenden.

Alternativ kann das System aus der Host-Assetdatenbank importiert werden.

Bemerkung: Das Importieren eines Hosts aus der Assetdatenbank ist nur möglich, falls das Ziel von der Seite *Hosts* aus erstellt wurde (siehe Kapitel *13.1.3* (Seite 352)).

Hosts ausschließen Manuelle Eingabe der Hosts, die vom Scan ausgeschlossen werden sollen, getrennt durch Kommas oder Importieren einer Hostliste.

Es gelten die gleichen Vorgaben wie für *Hosts*.

Erlaube das gleichzeitige Scannen über verschiedene IPs Einige Geräte, insbesondere IoT-Geräte, können abstürzen, wenn sie über mehrere Verbindungen, die vom selben Host kommen, gleichzeitig gescannt werden. Dies kann z. B. passieren, wenn das Gerät über IPv4 und IPv6 verbunden ist.

Durch Wählen des Radiobuttons *Nein* wird das gleichzeitige Scannen über mehrere Adressen verhindert.

Portliste Portliste, die für den Scan genutzt wird (siehe Kapitel *10.7* (Seite 255)).

Bemerkung: Eine Portliste kann durch Klicken auf neben der Drop-down-Liste erstellt werden.

Erreichbarkeitstest Diese Option legt die Methode fest, mit der geprüft wird, ob ein Ziel erreichbar ist. Die Möglichkeiten sind:

- Scan Config Default (die Erreichbarkeitstestmethode *ICMP Ping* wird standardmäßig verwendet)
- ICMP Ping
- TCP-ACK Service Ping
- TCP-SYN Service Ping
- ICMP & TCP-ACK Service Ping
- ICMP & ARP Ping
- TCP-ACK Service & ARP Ping
- ICMP, TCP-ACK Service & ARP Ping
- Consider Alive

Manchmal gibt es Probleme mit diesem Test. In einigen Umgebungen antworten Router- und Firewallsysteme auf einen TCP-Serviceping mit einem TCP-RST, obwohl der Host in Wirklichkeit nicht erreichbar ist (siehe Kapitel *10.13* (Seite 286)).

Es gibt Netzwerkkomponenten, die Proxy-ARP unterstützen und auf einen ARP-Ping antworten. Deshalb benötigt dieser Test oft lokale Anpassungen an die Umgebung.

SSH-Anmeldedaten Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein Linux- oder Unix-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *10.3.2* (Seite 222) und *10.3* (Seite 220)).

- **Berechtigungen erweitern** Es ist auch möglich, Anmeldedaten für erweiterte Berechtigungen zu speichern, z. B. root. Dazu müssen zunächst SSH-Anmeldedaten ausgewählt werden. Dann wird eine neue Drop-down-Liste zur Auswahl der erweiterten Anmeldedaten angezeigt.

  Bemerkung: Um die neue Funktion für erweiterte SSH-Anmeldedaten zu sehen, muss der Cache des Browsers, der für die Web-Oberfläche genutzt wird, möglicherweise geleert werden. Das Leeren des Browsercaches kann in den Einstellungen des genutzten Browsers vorgenommen werden.

  Alternativ kann der Seitencache geleert werden, indem `Strg` und `F5` gedrückt wird.

  Bemerkung: Das Feature ist noch experimentell. Je nach Zielsystem und dessen Konfiguration ist das Feature möglicherweise nicht zuverlässig.

  Mehr Informationen über Root-Rechte für Scans befinden sich in Kapitel *10.3.5* (Seite 238).

  Die erweiterten Berechtigungen des Nutzers müssen vorher auf dem Zielsystem konfiguriert werden. Die Appliance führt nur den Befehl `su - <Benutzername>` aus, der keine Kontrolle über die Nutzungsrechte hat.

  Wenn erweiterte SSH-Anmeldedaten konfiguriert sind, werden die Standard-SSH-Anmeldedaten nur für die Anmeldung auf dem Zielsystem verwendet. Die erweiterten Anmeldedaten werden für den Scan verwendet.

Die Programme *stty* und *unset* müssen für den Nutzer mit erweiterten Berechtigungen verfügbar/zugänglich sein.

Der Nutzer mit erweiterten Berechtigungen muss berechtigt sein, die Login-Aufforderung durch ein `export PS1=` zu ändern, das den gesendeten Befehlen vorangestellt wird.

Wenn erweiterte SSH-Anmeldedaten konfiguriert sind, werden diese immer verwendet, auch wenn die Scan-Konfiguration keine relevanten Schwachstellentests enthält.

Standard- und erweiterte SSH-Anmeldedaten dürfen nicht identisch sein.

Bemerkung: Die Verwendung von erweiterten SSH-Anmeldedaten kann zu einer erhöhten Last auf der Appliance sowie zu einer erhöhten Anzahl von SSH-Verbindungen von der Appliance zum Zielsystem führen. Dies muss ggf. bei Firewalls, Intrusion-Detection- und Logging-Systemen berücksichtigt werden.

Darüber hinaus kann die Dauer von Scans mit erweiterten SSH-Anmeldedaten aufgrund der oben erwähnten Systemlast wesentlich länger sein als bei Scans ohne erweiterte Anmeldedaten.

SMB-Anmeldedaten Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein Microsoft-Windows-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *10.3.2* (Seite 222) und *10.3* (Seite 220)).

ESXi-Anmeldedaten Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein VMware-ESXi-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *10.3.2* (Seite 222) und *10.3* (Seite 220)).

SNMP-Anmeldedaten Auswahl eines Benutzers, der sich in das Zielsystem einloggen kann, falls dieses ein SNMP-Aware-System ist. Dies ermöglicht einen authentifizierten Scan mit lokalen Sicherheitskontrollen (siehe Kapitel *10.3.2* (Seite 222) und *10.3* (Seite 220)).

Bemerkung: Alle Anmeldedaten können durch Klicken auf ☆ neben den Anmeldedaten erstellt werden.

Nur Invers-Lookup Nur IP-Adressen scannen, die sich in einen DNS-Namen auflösen können.

Invers-Lookup-Vereinheitlichung Falls sich mehrere IP-Adressen zum gleichen DNS-Namen auflösen, wird der DNS-Name nur einmal gescannt.

Bemerkung: Für die Invers-Lookup-Vereinheitlichung werden alle Zieladressen vor dem Scan geprüft, um die Anzahl tatsächlich gescannter Adressen zu reduzieren. Für große Ziele und für Netzwerke, in denen Invers-Lookups Verzögerungen verursachen, führt dies zu einer langen Phase, in der die Aufgabe bei 1 % Fortschritt steht.

Diese Option wird nicht für große Netzwerke oder Netzwerke, in denen Invers-Lookups Verzögerungen verursachen, empfohlen.

10.2.2 Eine Aufgabe erstellen

Der zweite Schritt ist das Erstellen einer Aufgabe.

Die Appliance steuert die Ausführung von Scans mithilfe von Aufgaben. Diese Aufgaben können regelmäßig wiederholt oder zu bestimmten Zeiten ausgeführt werden (siehe Kapitel *10.10* (Seite 272)).

Eine Aufgabe kann wie folgt erstellt werden:

1. *Scans* > *Aufgaben* in der Menüleiste wählen.
2. Neue Aufgabe durch Bewegen der Maus über ☆ und Klicken auf *Neue Aufgabe* erstellen.
3. Aufgabe definieren (siehe Abb. 10.6).

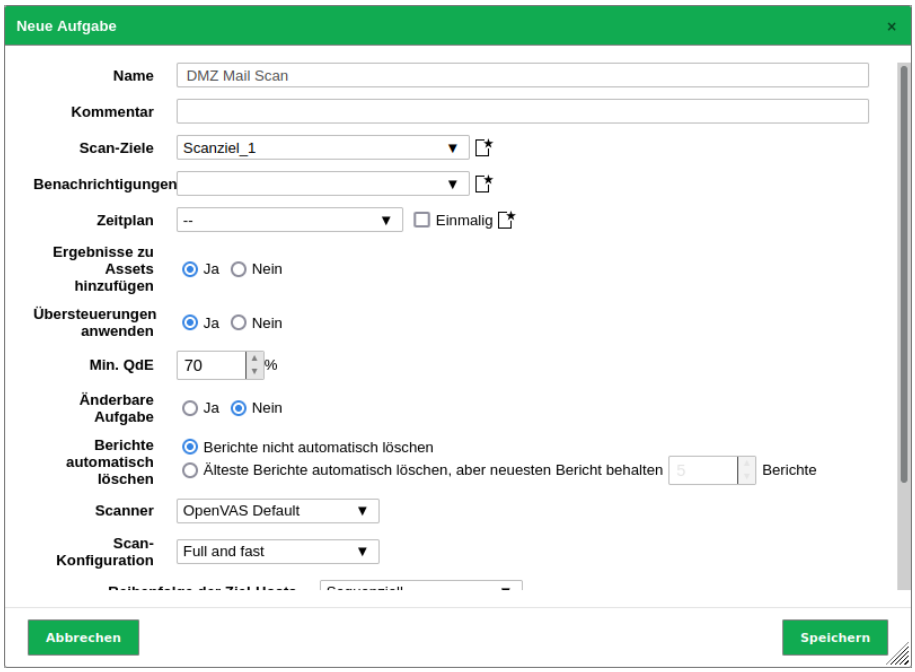


Abb. 10.6: Erstellen einer neuen Aufgabe

4. Auf *Speichern* klicken.

   → Die Aufgabe wird erstellt und auf der Seite *Aufgaben* angezeigt.

Die folgenden Informationen können eingegeben werden:

Name Der Name kann frei gewählt werden. Falls möglich, sollte ein aussagekräftiger Name gewählt werden. Möglichkeiten sind Mailserver, ClientNetwork, Webserverfarm, DMZ oder eine nähere Beschreibung des Systems.

Kommentar Der optionale Kommentar erlaubt es, Hintergrundinformationen festzuhalten. Diese erleichtern später das Verständnis der konfigurierten Aufgabe.

Scan-Ziele Zuvor konfiguriertes Ziel aus der Drop-down-Liste wählen (siehe Kapitel *10.2.1* (Seite 214)).

Alternativ kann das Ziel durch Klicken auf ☆ neben der Drop-down-Liste erstellt werden.

Benachrichtigungen Zuvor konfigurierte Benachrichtigung aus der Drop-down-Liste wählen (siehe Kapitel *10.12* (Seite 277)). Statusänderungen der Aufgabe können über E-Mail, System-Logger, HTTP oder einen Konnektor mitgeteilt werden.

Alternativ kann die Benachrichtigung durch Klicken auf ☆ neben der Drop-down-Liste erstellt werden.

Zeitplan Zuvor konfigurierten Zeitplan aus der Drop-down-Liste wählen (siehe Kapitel *10.10* (Seite 272)). Die Aufgabe kann einmalig oder wiederholt zu einer festgelegten Zeit, z. B. jeden Montagmorgen um 6:00, ausgeführt werden.

Alternativ kann ein Zeitplan durch Klicken auf neben der Drop-down-Liste erstellt werden.

Ergebnisse zu Assets hinzufügen Das Auswählen dieser Option macht die Systeme automatisch für die Assetverwaltung der Appliance verfügbar (siehe Kapitel *13* (Seite 349)). Diese Auswahl kann später geändert werden.

Übersteuerungen anwenden Übersteuerungen können direkt angewendet werden, wenn die Ergebnisse zur Assetdatenbank hinzugefügt werden (siehe Kapitel *11.8* (Seite 315)).

Min QdE Hier kann die minimale Qualität der Erkennung für das Hinzufügen der Ergebnisse zur Assetdatenbank festgelegt werden (siehe Kapitel *11.2.6* (Seite 302)).

Änderbare Aufgabe Änderung von Scan-Ziel(en), Scanner und Scan-Konfiguration der Aufgabe ermöglichen, auch wenn bereits Berichte erstellt wurden. Die Übereinstimmung zwischen Berichten kann nicht mehr garantiert werden, wenn Aufgaben geändert werden.

Berichte automatisch löschen Diese Option löscht alte Berichte automatisch. Die maximale Anzahl an gespeicherten Berichten kann konfiguriert werden. Falls das Maximum überschritten wird, wird der älteste Bericht automatisch gelöscht. Die Werkseinstellung ist *Berichte nicht automatisch löschen*.

Scanner Standardmäßig werden nur die integrierten OpenVAS- und CVE-Scanner unterstützt (siehe Kapitel *10.11* (Seite 275)). Sensoren können als zusätzliche Scanmaschinen genutzt werden, müssen jedoch erst konfiguriert werden (siehe Kapitel *16* (Seite 380)).

Bemerkung: Die folgenden Optionen sind nur für den OpenVAS-Scanner relevant. Der CVE-Scanner unterstützt keine dieser Optionen.

Scan-Konfiguration Die Appliance wird mit mehreren vorkonfigurierten Scan-Konfigurationen für den OpenVAS-Scanner geliefert (siehe Kapitel *10.9* (Seite 261)). Pro Aufgabe kann nur eine Scan-Konfiguration konfiguriert werden.

Reihenfolge der Ziel-Hosts Wählen, in welcher Reihenfolge die angegebenen Zielhosts bei Schwachstellentests verarbeitet werden. Verfügbare Optionen sind:

- Sequenziell
- Zufällig
- Rückwärts

Um die Abschätzung des Scanfortschritts zu verbessern, wird die Einstellung *Zufällig* empfohlen (siehe Kapitel *17.2.3* (Seite 392)).

Diese Einstellung hat keinen Einfluss auf den Erreichbarkeitstest, bei dem aktive Hosts in einem Zielnetzwerk identifiziert werden. Der Erreichbarkeitstest ist immer zufällig.

Maximal gleichzeitig ausgeführte NVTs pro Host/Maximal gleichzeitig gescannte Hosts Auswahl der Geschwindigkeit des Scans auf einem Host. Die Standardwerte sind bewusst gewählt. Falls mehrere VTs gleichzeitig auf einem System laufen oder mehrere Systeme zur gleichen Zeit gescannt werden, könnte der Scan negative Auswirkungen auf die Leistung der gescannten Systeme, des Netzwerks oder der Appliance selbst haben. Die Werte „maxhosts“ und „maxchecks“ können optimiert werden.

Tag Zuvor konfigurierten Tag aus der Drop-down-Liste wählen (siehe Kapitel *8.4* (Seite 176)), um ihn mit der Aufgabe zu verbinden.

10.2.3 Die Aufgabe starten

In der Zeile der neu erstellen Aufgabe auf ▷ klicken.

Bemerkung: Für Aufgaben mit Zeitplan wird zusätzlich 🕒 angezeigt. Die Aufgabe startet zu der Zeit, die im Zeitplan festgelegt wurde (siehe Kapitel *10.10* (Seite 272)).

→ Die Aufgabe wird zur Warteschlange hinzugefügt. Danach beginnt der Scanner mit dem Scan.

Bemerkung: In einigen Fällen kann die Aufgabe in der Warteschlange bleiben. Weitere Informationen befinden sich in Kapitel *17.3* (Seite 393).

Für den Status einer Aufgabe siehe Kapitel *10.8* (Seite 257).

Sobald eine Aufgabe gestartet wurde, kann der Bericht der Aufgabe durch Klicken auf den Balken in der Spalte *Status* dargestellt werden. Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *11* (Seite 288).

Sobald sich der Status zu *Abgeschlossen* ändert, ist der gesamte Bericht verfügbar. Zu jeder Zeit können Zwischenergebnisse angesehen werden (siehe Kapitel *11.2.1* (Seite 293)).

Bemerkung: Die Fertigstellung des Scans kann einige Zeit in Anspruch nehmen. Die Seite aktualisiert automatisch, falls neue Daten verfügbar sind.

10.3 Einen authentifizierten Scan mit lokalen Sicherheitskontrollen konfigurieren

Ein authentifizierter Scan kann mehr Details über Schwachstellen auf dem gescannten System bereitstellen. Während eines authentifizierten Scans wird das Ziel sowohl von außen über das Netzwerk als auch von innen mithilfe eines gültigen Benutzerlogins gescannt.

Während eines authentifizierten Scans loggt sich die Appliance in das Zielsystem ein, um lokale Sicherheitskontrollen (engl. local security checks, LSCs) durchzuführen. Der Scan benötigt die vorherige Erstellung von Anmeldedaten. Diese Anmeldedaten werden für die Authentifizierung auf unterschiedlichen Diensten auf dem Zielsystem genutzt. Unter manchen Umständen können die Ergebnisse durch die Berechtigungen des Benutzers eingeschränkt werden.

Die VTs in der entsprechenden VT-Familie (LSCs) werden nur ausgeführt, falls sich die Appliance in das Zielsystem einloggen konnte. Die VTs der lokalen Sicherheitskontrollen im resultierenden Scan sind minimalinvasiv.

Die Appliance bestimmt nur die Risikostufe, aber nimmt keine Änderungen am Zielsystem vor. Trotzdem wird der Login der Appliance wahrscheinlich in den Protokollen des Zielsystems vermerkt.

Die Appliance kann unterschiedliche Anmeldedaten, basierend auf den Eigenschaften des Ziels, nutzen. Die wichtigsten sind:

- **SMB** Auf Microsoft-Windows-Systemen kann die Appliance das Patchlevel und lokal installierte Software wie Adobe Acrobat Reader oder die Java-Suite prüfen.
- **SSH** Dieser Zugang wird für das Prüfen des Patchlevels von Unix- und Linuxsystemen genutzt.
- **ESXi** Dieser Zugang wird für das lokale Prüfen von VMware-ESXi-Servern genutzt.
- **SNMP** Netzwerkkomponenten wie Router und Switches können mithilfe von SNMP geprüft werden.

Die folgende Tabelle listet den erforderlichen Port – vorausgesetzt, der Authentifizierungsdienst verwendet den Standardport – und die zulässigen Anmeldedatentypen (siehe Kapitel *10.3.2* (Seite 222)) für jede Authentifizierungsmethode auf:

	Erforderlicher Port	Erlaubte Anmeldedatentypen
SMB	• 445/tcp, 139/tcp	• *Benutzername + Passwort*
SSH	• 22/tcp, konfigurierbar im Dialog *Neues Ziel*/*Ziel bearbeiten* (siehe Kapitel *10.2.1* (Seite 214))	• *Benutzername + Passwort* • *Benutzername + SSH-Schlüssel*
ESXi	• Siehe https://kb.vmware.com/s/article/2039095	• *Benutzername + Passwort*
SNMP	• 161/udp	• *SNMP*

10.3.1 Vorteile und Nachteile authentifizierter Scans

Der Umfang und Erfolg der Prüfroutinen für authentifizierte Scans hängen stark von den Berechtigungen des genutzten Benutzeraccounts ab.

Auf Linux-Systemen ist ein unprivilegierter Benutzer ausreichend und kann auf die meisten relevanten Informationen zugreifen, während ein unprivilegierter Benutzer auf Microsoft-Windows-Systemen sehr eingeschränkt ist und ein administrativer Benutzer mehr Ergebnisse liefert. Ein unprivilegierter Benutzer hat keinen Zugriff auf die Microsoft-Windows-Registrierungsdatenbank („Registry“) und den Microsoft-Windows-Systemorder `\windows`, welcher Informationen zu Updates und Patchlevels enthält.

Lokale Sicherheitskontrollen (LSCs) sind die schonendste Methode, um nach Schwachstellendetails zu suchen. Während Remote-Sicherheitsheitskontrollen ebenfalls versuchen, möglichst nicht-invasiv zu sein, verursachen sie einige Auswirkungen.

Einfach gesagt ähnelt ein authentifizierter Scan einem Whitebox-Ansatz. Die Appliance hat Zugriff auf frühere Informationen und kann von innen auf das Ziel zugreifen. Insbesondere sind die Registrierung, Softwareversionen und Patchlevels zugänglich.

Ein Remotescan ähnelt einem Blackbox-Ansatz. Die Appliance nutzt die gleichen Techniken und Protokolle wie potenzielle Angreifende, um von außen auf das Ziel zuzugreifen. Die einzigen verfügbaren Informationen werden von der Appliance selbst gesammelt. Während einer Prüfung kann die Appliance Fehlfunktionen auslösen, um Informationen über die genutzte Software zu erhalten, z. B. kann der Scanner eine fehlerhafte Anfrage an einen Dienst senden, um eine Antwort auszulösen, die weitere Informationen über das eingesetzte Produkt enthält.

Während eines Remotescans mit der Scan-Konfiguration *Full and fast* sind alle Remoteprüfungen sicher. Die genutzten VTs haben möglicherweise einige invasive Komponenten, aber keiner der genutzten VTs versucht, einen Defekt oder eine Fehlfunktion auf dem Ziel auszulösen (siehe Beispiel unten). Dies wird durch die Scanner-Vorgabe `safe_checks=yes` in der Scan-Konfiguration sichergestellt (siehe Kapitel *10.9.4* (Seite 267)). Alle VTs mit sehr invasiven Komponenten oder solche, die einen Denial of Service (DoS) auslösen, werden automatisch von der Prüfung ausgeschlossen.

Beispiel für einen invasiven VT

Ein Beispiel für einen invasiven, aber sicheren VT ist der Heartbleed-VT. Er wird sogar ausgeführt, wenn `safe_checks` aktiviert ist, da der VT keine negativen Auswirkungen auf das Ziel hat.

Der VT ist trotzdem invasiv, da er die Speicherlecks des Ziels prüft. Falls das Ziel angreifbar ist, wird tatsächlicher Speicher des Ziels geleaked. Die Appliance bewertet die geleakten Informationen nicht. Die Informationen werden umgehend gelöscht.

10.3.2 Anmeldedaten nutzen

Anmeldedaten für lokale Sicherheitsprüfungen werden benötigt, um VTs das Einloggen in ein Zielsystem zu ermöglichen, z. B. um das Vorhandensein aller Sicherheitspatches des Herstellers lokal zu prüfen.

10.3.2.1 Anmeldedaten erstellen

Neue Anmeldedaten können wie folgt erstellt werden:

1. *Konfiguration* > *Anmeldedaten* in der Menüleiste wählen.
2. Neue Anmeldedaten durch Klicken auf erstellen.
3. Anmeldedaten definieren (siehe Abb. 10.7).

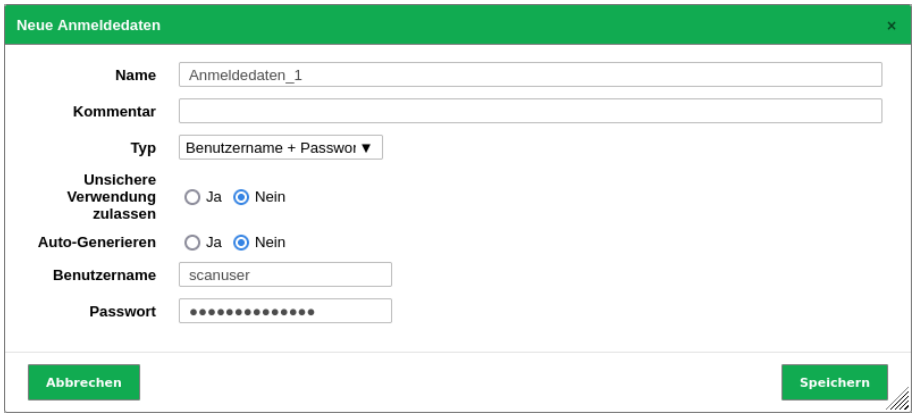


Abb. 10.7: Erstellen neuer Anmeldedaten

4. Auf *Speichern* klicken.

Die folgenden Details der Anmeldedaten können festgelegt werden:

Name Festlegung des Namens. Der Name kann frei gewählt werden.

Bemerkung: Für den Namen sind nur die folgenden Zeichen zulässig:

- Alle englischen alphanumerischen Zeichen
- - (Bindestrich)
- _ (Unterstrich)
- \ (Backslash)
- . (Punkt)
- @ (At-Zeichen)

Dies schließt auch die deutschen Umlaute aus, die wie folgt ersetzt werden müssen:

- „ß“ → „ss“
- „ä“ → „a“
- „ö“ → „o“
- „ü“ → „u“

Kommentar Ein optionaler Kommentar kann zusätzliche Informationen enthalten.

Typ Festlegung des Typs der Anmeldedaten. Die folgenden Typen sind möglich:

- Benutzername + Passwort
- Benutzername + SSH-Schlüssel
- SNMP
- S/MIME-Zertifikat
- PGP-Verschlüsselungsschlüssel
- Nur Passwort

Unsichere Verwendung zulassen Wahl, ob die Appliance die Anmeldedaten für unverschlüsselte oder anderweitig unsichere Authentifizierungsmethoden nutzen kann.

Abhängig vom gewählten Typen werden weitere Optionen angezeigt:

Benutzername + Passwort

- **Auto-generieren** Wahl, ob die Appliance ein zufällig Passwort erstellt.

  Bemerkung: Falls der Radiobutton *Ja* gewählt wird, ist es nicht möglich, im Eingabefeld *Passwort* ein Passwort festzulegen.

- **Benutzername** Festlegung des Loginnamens, der von der Appliance genutzt wird, um sich auf dem gescannten Zielsystem zu authentifizieren.

  Bemerkung: Für den Benutzernamen sind nur die folgenden Zeichen zulässig:

  – Alle englischen alphanumerischen Zeichen

  – - (Bindestrich)

  – _ (Unterstrich)

  - \ (Backslash)
  - . (Punkt)
  - @ (At-Zeichen)

  Dies schließt auch die deutschen Umlaute aus, die wie folgt ersetzt werden müssen:

  - „ß“ → „ss“
  - „ä“ → „a“
  - „ö“ → „o“
  - „ü“ → „u“

- **Passwort** Festlegung des Passworts, das von der Appliance genutzt wird, um sich auf dem gescannten Zielsystem zu authentifizieren.

Benutzername + SSH-Schlüssel

- **Auto-generieren** Wahl, ob die Appliance ein zufällig Passwort erstellt.

  Bemerkung: Falls der Radiobutton *Ja* gewählt wird, ist es nicht möglich, im Eingabefeld *Passwort* ein Passwort festzulegen.

- **Benutzername** Festlegung des Loginnamens, der von der Appliance genutzt wird, um sich auf dem gescannten Zielsystem zu authentifizieren.

  Bemerkung: Für den Benutzernamen sind nur die folgenden Zeichen zulässig:

  - Alle englischen alphanumerischen Zeichen
  - - (Bindestrich)
  - _ (Unterstrich)
  - \ (Backslash)
  - . (Punkt)
  - @ (At-Zeichen)

  Dies schließt auch die deutschen Umlaute aus, die wie folgt ersetzt werden müssen:

  - „ß“ → „ss“
  - „ä“ → „a“
  - „ö“ → „o“
  - „ü“ → „u“

- **Passphrase** Festlegung der Passphrase des privaten SSH-Schlüssels.
- **Privater Schlüssel** Hochladen des privaten SSH-Schlüssels.
- **Zertifikat** Hochladen der Zertifikatdatei.
- **Privater Schlüssel** Hochladen des zugehörigen privaten Schlüssels.

SNMP SNMPv3 erfordert einen Benutzernamen, ein Authentifizierungs-Passwort und ein Privacy-Passwort, während alle älteren SNMP-Versionen (SNMPv1 und SNMPv2) nur eine SNMP-Community benötigen.

Bemerkung: Aufgrund der Einzigartigkeit der SNMP-Anmeldedaten ist es derzeit nicht möglich, entweder den SNMPv1/v2- oder den SNMPv3-Modus zu konfigurieren.

Das bedeutet, dass die Appliance immer versuchen wird, sich mit allen SNMP-Protokollversionen einzuloggen. Es ist möglich, sowohl das Ergebnis *SNMP Login Successful For Authenticated Checks* als auch das Ergebnis *SNMP Login Failed For Authenticated Checks* für einen Scan zu sehen, z. B. wenn die SNMPv3-Logininformationen in den Anmeldedaten korrekt sind, aber die SNMPv1/2-Informationen falsch sind.

- **SNMP-Community** Festlegung der Community für SNMPv1 oder SNMPv2c.
- **Benutzername** Festlegung des Benutzernamens für SNMPv3.

  Bemerkung: Für den Benutzernamen sind nur die folgenden Zeichen zulässig:

  – Alle englischen alphanumerischen Zeichen

  – - (Bindestrich)

  – _ (Unterstrich)

  – \ (Backslash)

  – . (Punkt)

  – @ (At-Zeichen)

  Dies schließt auch die deutschen Umlaute aus, die wie folgt ersetzt werden müssen:

  – „ß“ → „ss“

  – „ä“ → „a“

  – „ö“ → „o“

  – „ü“ → „u“

- **Passwort** Festlegung des Passworts für SNMPv3.
- **Privacy-Passwort** Festlegung des Passworts für die Verschlüsselung für SNMPv3.
- **Auth-Algorithmus** Wahl des Authentifizierungsalgorithmus (MD5 oder SHA1)
- **Privacy-Algorithmus** Wahl des Verschlüsselungsalgorithmus (AES, DES oder keiner).

S/MIME-Zertifikat

- **S/MIME-Zertifikat** Hochladen der Zertifikatdatei.

PGP-Verschlüsselungsschlüssel

- **Öffentlicher PGP-Schlüssel** Hochladen der Schlüsseldatei.

Nur Passwort

- **Passwort** Festlegung des Passworts, das von der Appliance genutzt wird, um sich auf dem gescannten Zielsystem zu authentifizieren.

Bemerkung: Die Anmeldedaten müssen mit mindestens einem Ziel verknüpft sein. Dies erlaubt es der Scanmaschine, die Anmeldedaten anzuwenden.

10.3.2.2 Anmeldedaten verwalten

Listenseite

Alle vorhandenen Anmeldedaten können angezeigt werden, indem *Konfiguration > Anmeldedaten* in der Menüleiste gewählt wird.

Für alle Anmeldedaten werden die folgenden Informationen angezeigt:

Name Name der Anmeldedaten.

Typ Gewählter Anmeldedatentyp.

Unsichere Verwendung zulassen Hinweis, ob die Appliance die Anmeldedaten für unverschlüsselte oder andersweitig unsichere Authentifizierungsmethoden nutzen kann.

Login Benutzername für die Anmeldedaten, falls ein Anmeldedatentyp gewählt wurde, der einen Benutzernamen benötigt.

Für alle Anmeldedaten sind die folgenden Aktionen verfügbar:

- Die Anmeldedaten in den Papierkorb verschieben. Nur Anmeldedaten, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Die Anmeldedaten bearbeiten.
- Die Anmeldedaten klonen.
- Die Anmeldedaten als XML-Datei exportieren.

Abhängig vom gewählten Anmeldedatentyp (siehe Kapitel *10.3.2.1* (Seite 222)) sind mehr Aktionen verfügbar:

- Ein EXE-Paket für Microsoft Windows herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + Passwort* gewählt wurde.
- Ein RPM-Paket für Red Hat Enterprise Linux und dessen Derivate herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + SSH-Schlüssel* gewählt wurde.
- Ein Debian-Paket für Debian GNU/Linux und dessen Derivate herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + SSH-Schlüssel* gewählt wurde.
- Einen öffentlichen Schlüssel herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + SSH-Schlüssel* gewählt wurde.

Diese Installationspakete vereinfachen die Installation und das Erstellen von Accounts für authentifizierte Scans. Sie erstellen den Benutzer und die wichtigsten Berechtigungen für den authentifizierten Scan und setzen diese während der Deinstallation wieder zurück.

Bemerkung: Falls die automatische Generierung eines Passworts aktiviert ist (siehe Kapitel *10.3.2.1* (Seite 222)), müssen die Pakete genutzt werden. Andernfalls ist die Nutzung optional.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Anmeldedaten können mehrere Anmeldedaten zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Anmeldedaten in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen von Anmeldedaten werden Details der Anmeldedaten angezeigt. Durch Klicken auf wird die Detailseite der Anmeldedaten geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Anmeldedaten.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Anmeldedaten anzeigen.
- Neue Anmeldedaten erstellen (siehe Kapitel *10.3.2.1* (Seite 222)).
- Die Anmeldedaten klonen.
- Die Anmeldedaten bearbeiten.
- Die Anmeldedaten in den Papierkorb verschieben. Nur Anmeldedaten, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Die Anmeldedaten als XML-Datei exportieren.

Abhängig vom gewählten Anmeldedatentyp (siehe Kapitel *10.3.2.1* (Seite 222)) sind mehr Aktionen verfügbar:

- Ein EXE-Paket für Microsoft Windows herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + Passwort* gewählt wurde.
- Ein RPM-Paket für Red Hat Enterprise Linux und dessen Derivate herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + SSH-Schlüssel* gewählt wurde.
- Ein Debian-Paket für Debian GNU/Linux und dessen Derivate herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + SSH-Schlüssel* gewählt wurde.
- Einen öffentlichen Schlüssel herunterladen. Diese Aktion ist verfügbar, falls *Benutzername + SSH-Schlüssel* gewählt wurde.

10.3.3 Anforderungen auf Zielsystemen mit Microsoft Windows

10.3.3.1 Allgemeine Hinweise zur Konfiguration

- Der Dienst der Remote-Registrierung muss gestartet werden, um auf die Registrierung zuzugreifen.

  Dies wird erreicht, indem das automatischte Starten des Diensts eingestellt wird. Falls ein automatischer Start nicht gewünscht wird, kann ein manueller Start konfiguriert werden. In diesem Fall wird der Dienst, während das System von der Appliance gescannt wird, gestartet und anschließend wieder deaktiviert. Um dieses Verhalten sicherzustellen, muss der folgende Punkt über LocalAccountTokenFilterPolicy beachetet werden.

- Es ist notwendig, dass für alle gescannten Systeme der Datei- und Druckerzugriff aktiviert ist. Falls Microsoft Windows XP genutzt wird, muss die Einstellung *Use Simple File Sharing* deaktiviert sein.

- Für einzelne Systeme, die nicht mit einer Domäne verbunden sind, muss der folgende Registrierungsschlüssel festgelegt werden:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- Auf Systemen mit Domänen-Controller muss der genutzte Benutzeraccount Mitglied der Gruppe *Domain Administrators* sein, um die bestmöglichen Ergebnisse zu erhalten. Aufgrund des Berechtigungskonzepts ist es nicht möglich, alle Schwachstellen zu erkennen, wenn der *Local Administrator* oder der von der Domain zugewiesene Administrator genutzt wird. Alternativ können die Anweisungen in Kapitel *10.3.3.2* (Seite 228) befolgt werden.

→ Sollte ein *Local Administrator* gewählt werden – was ausdrücklich nicht empfohlen wird – ist es auch notwendig, den folgenden Registrierungsschlüssel festzulegen:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
DWORD: LocalAccountTokenFilterPolicy = 1
```

- Generiertes Installationspaket für Anmeldedaten: Das Installationsprogramm stellt den Remote-Registrierungsdienst auf automatisches Starten ein. Falls das Installationsprogramm auf einem Domänen-Controller ausgeführt wird, wird der Benutzeraccount der Gruppe *BUILTIN/Administratoren* (SID S-1-5-32-544) zugeordnet.
- Auf der Microsoft-Windows-Firewall muss eine Ausnahmeregel für die Appliance erstellt werden. Zusätzlich muss auf XP-Systemen der Dienst *File and Printer Sharing* auf *enabled* eingestellt sein.
- Generiertes Installationspaket für Anmeldedaten: Während der Installation bietet das Installationsprogramm einen Dialog, um die IP-Adresse der Appliance einzugeben. Wenn die Eingabe bestätigt wird, wird eine Regel für die Firewall konfiguriert. Der Dienst *File and Printer Sharing* wird in den Regeln der Firewall aktiviert.
- Powershell-Ausführungsberechtigungen auf einem Zielsystem können für das Konto erforderlich sein, das in einem authentifizierten Scan verwendet wird. Bei Richtlinien- und Schwachstellentests können gelegentlich Powershell-Befehle ausgeführt werden, um die Genauigkeit der Ergebnisse zu erhöhen, wofür Berechtigungen für die Dauer eines Scans erforderlich sind.
- Für Compliance-Audits, die auf Windows-Betriebssysteme ausgerichtet sind, wird empfohlen, die Einstellung *Maximal gleichzeitig ausgeführte NVTs pro Host/Maximal gleichzeitig gescannte Hosts* auf `1` zu setzen, um die Genauigkeit der Ergebnisse zu erhöhen (siehe Kapitel *12.2.1.1* (Seite 325)).
- Für einen voll funktionsfähigen Zugriff auf Windows Management Instrumentation (WMI), der z. B. für die Dateisuche oder Richtlinien-Scans verwendet wird, sind die folgenden Einstellungen erforderlich:
  - WMI-Zugriff in den Einstellungen der Windows Firewall[24] oder einer möglichen Firewall-Lösung eines Drittanbieters zulassen.
  - Verifizieren, dass der Benutzer oder die Gruppe des Scan-Benutzers für den Remote-Zugriff auf WMI zugelassen ist.

10.3.3.2 Einen Domänenaccount für authentifiziert Scans konfigurieren

Für authentifizierte Scans von Microsoft-Windows-Zielsystemen wird die Nutzung eines Domänenaccounts mit einer Domänenrichtlinie, die lokale Administratorprivilegien erteilt, empfohlen. Dies hat mehrere Vorteile:

- Eine Domänenrichtlinie muss nur einmal erstellt werden und kann dann für unterschiedliche Benutzer angewendet oder widerrufen werden.
- Das lokale Bearbeiten der Registrierung von Microsoft Windows ist nicht länger nötig. Die Benutzerverwaltung ist somit zentralisiert, was auf lange Sicht Zeit spart und mögliche Konfigurationsfehler reduziert.
- Aus Sicht der Schwachstellenbewertung ermöglicht nur ein Domänenaccount die Erkennung domänenzugehöriger Scanergebnisse. Diese Ergebnisse fehlen, falls ein ein lokaler Benutzeraccount genutzt wird.
- Es gibt auch einige Sicherheitsvorteile beim Nutzen eines Domänenaccounts mit einer Domänenrichtlinie, die von Greenbone empfohlen wird: Der zugehörige Benutzer kann sich möglicherweise nicht lokal oder über die Remotedesktopverbindung einloggen, was etwaige Angriffsvektoren begrenzt. Zusätzlich werden die Anmeldedaten via Kerberos geschützt, während bei einem Passwort eines lokalen Benutzers ein höheres Risiko des Ausnutzens besteht.

Um einen Domänenaccounts für hostbasierte Remote-Audits auf einem Microsoft-Windows-Ziel zu nutzen, muss die folgende Konfiguration unter Windows XP Professional, Windows Vista, Windows Server 2003, Win-

[24] https://learn.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista#windows-firewall-settings

dows Server 2008, Windows Server 2012, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 oder Windows 10 geschehen. Das System muss auch Teil der Domäne sein.

Eine Sicherheitsgruppe erstellen

1. In einen Domänen-Controller einloggen und *Active Directory Users and Computers* öffnen.
2. *Aktion* > *Neu* > *Gruppe* in der Menüleiste wählen.
3. `Greenbone Local Scan` in das Eingabefeld *Name* eingeben.
4. *Global* für *Gruppenbereich* und *Sicherheit* für *Gruppentyp* wählen.
5. Account, der unter Microsoft Windows für die lokalen authentifizierten Scans von der Appliance genutzt wird, zur Gruppe hinzufügen.
6. Auf *OK* klicken.

Eine Gruppenrichtlinie (engl. Group Policy Object, GPO) erstellen

1. Im linken Panel die Konsole *Gruppenrichtlinienverwaltung* öffnen.
2. Auf *Gruppenrichtlinienobjekte* rechtsklicken und *Neu* wählen.
3. `Greenbone Local SecRights` in das Eingabefeld *Name* eingeben (siehe Abb. 10.8).

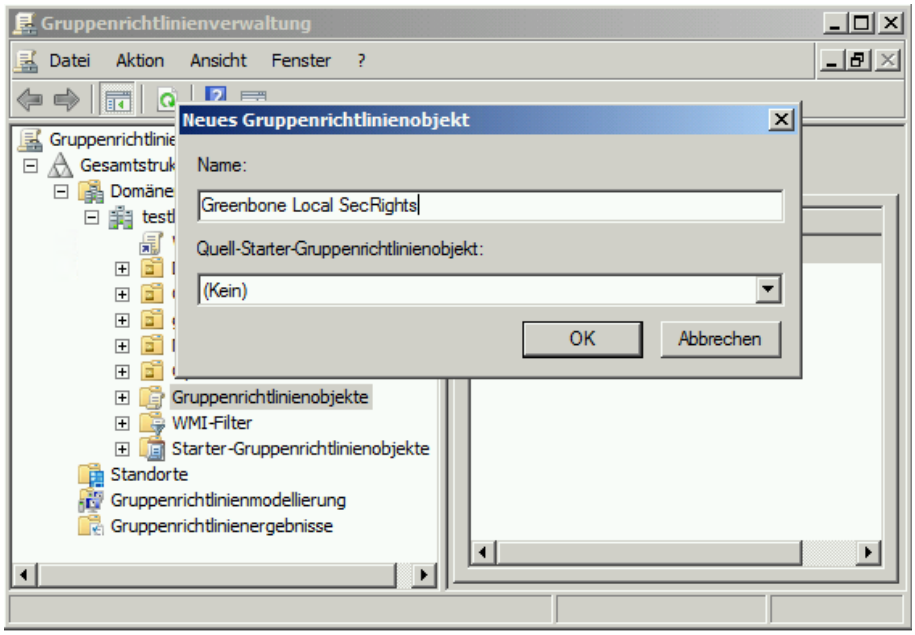


Abb. 10.8: Erstellen einer neuen Microsoft-Windows-Gruppenrichtlinie für Scans durch Greenbone

4. Auf *OK* klicken.

Konfigurieren der Richtlinie

1. Auf die Richtlinie *Greenbone Local SecRights* klicken und *Bearbeiten...* wählen.
2. *Computerkonfiguration* > *Richtlinien* > *Windows-Einstellungen* > *Sicherheitseinstellungen* im linken Panel wählen.
3. Auf *Eingeschränkte Gruppen* klicken und *Gruppe hinzufügen* wählen.
4. Auf *Durchsuchen...* klicken und `Greenbone Local Scan` in das Eingabefeld eingeben (siehe Abb. 10.9).

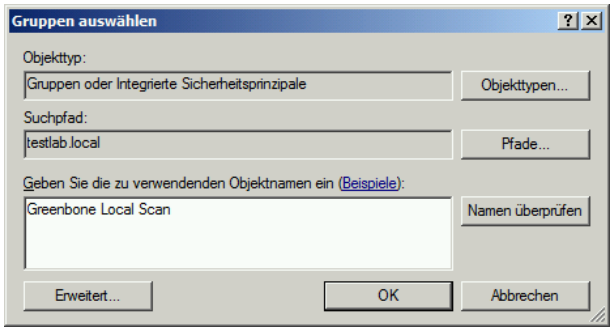


Abb. 10.9: Prüfen der Microsoft-Windows-Gruppennamen

5. Auf *Namen überprüfen* klicken.
6. Zweimal auf *OK* klicken, um die offenen Fenster zu schließen.
7. Bei *Diese Gruppe ist Mitglied von* auf *Hinzufügen...* klicken.
8. `Administrators` in das Eingabefeld *Gruppe* eingeben (siehe Abb. 10.10) und zweimal auf *OK* klicken, um die offenen Fenster zu schließen.

Bemerkung: Auf nicht-englischsprachigen Systemen den entsprechenden Namen der lokalen Administratorengruppe eingeben.

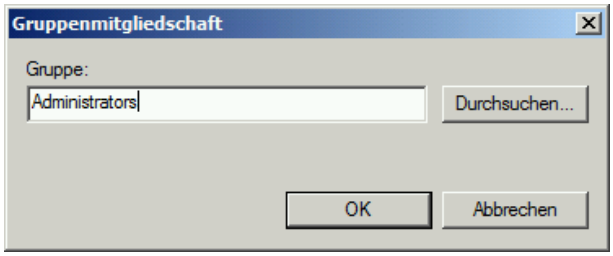


Abb. 10.10: Hinzufügen einer Gruppenmitgliedschaft

Konfigurieren der Richtlinie, sodass der Gruppe „Greenbone Local Scan“ das lokale Einloggen in das System verweigert wird

1. Auf die Richtlinie *Greenbone Local SecRights* klicken und *Bearbeiten...* wählen.
2. *Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten* im linken Panel wählen.
3. Im rechten Panel auf *Lokal anmelden verweigern* doppelklicken.
4. Checkbox *Diese Richtlinieneinstellungen definieren* aktivieren und auf *Benutzer oder Gruppe hinzufügen* klicken.
5. Auf *Durchsuchen...* klicken und `Greenbone Local Scan` in das Eingabefeld eingeben (siehe Abb. 10.11).
6. Auf *Namen überprüfen* klicken.

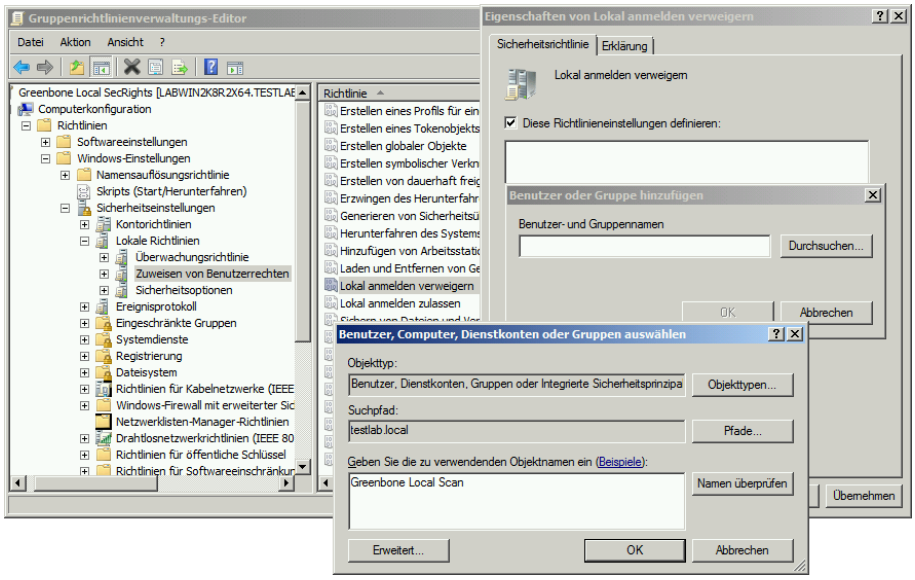


Abb. 10.11: Bearbeiten der Richtlinie

7. Dreimal auf *OK* klicken, um die offenen Fenster zu schließen.

Konfigurieren der Richtlinie, sodass der Gruppe „Greenbone Local Scan“ das Einloggen per Remote Desktop in das System verweigert wird

1. Auf die Richtlinie *Greenbone Local SecRights* klicken und *Bearbeiten...* wählen.
2. *Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisen von Benutzerrechten* im linken Panel wählen.
3. Im rechten Panel auf *Anmelden über Remotedesktopdienst verweigern* doppelklicken.
4. Checkbox *Diese Richtlinieneinstellungen definieren* aktivieren und auf *Benutzer oder Gruppe hinzufügen* klicken.
5. Auf *Durchsuchen...* klicken und `Greenbone Local Scan` in das Eingabefeld eingeben (siehe Abb. 10.12).
6. Auf *Namen überprüfen* klicken.
7. Dreimal auf *OK* klicken, um die offenen Fenster zu schließen.

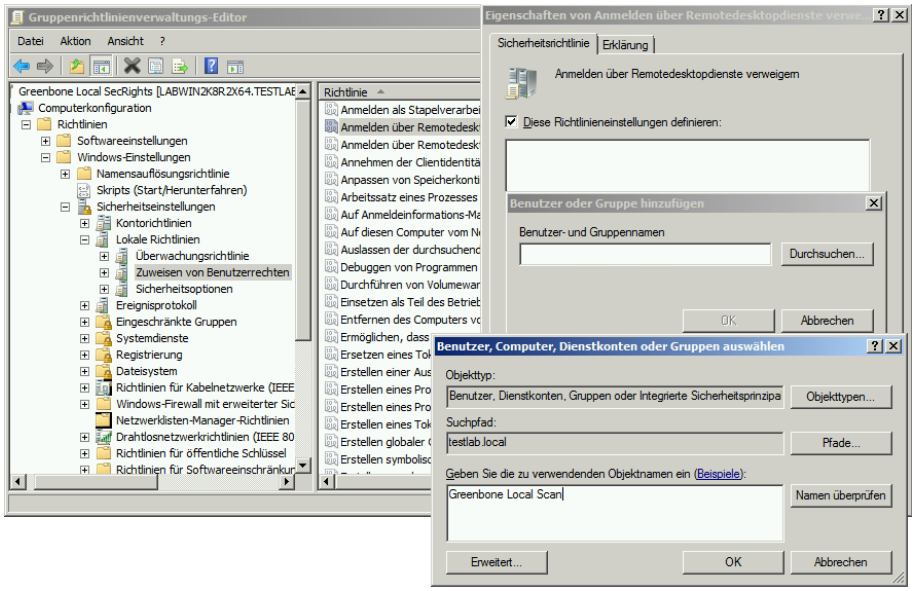


Abb. 10.12: Bearbeiten der Richtlinie

Konfigurieren der Richtlinie, sodass die Gruppe „Greenbone Local Scan“ auf der Registrierung nur Leserechte hat

---

Wichtig: Diese Einstellung ist auch nach Entfernen der Gruppenrichtlinie vorhanden („tattooing GPO“).

Dies ändert grundlegende Privilegien, welche nicht einfach durch Entfernen der Gruppenrichtlinie rückgängig gemacht werden können.

Es muss geprüft werden, ob die Einstellungen mit der Umgebung kompatibel sind.

Bemerkung: Die folgenden Schritte sind optional.

---

1. Im linken Panel auf *Registrierung* klicken und *Schlüssel hinzufügen. . .* wählen.
2. *USERS* wählen und auf *OK* klicken (siehe Abb. 10.13).
3. Auf *Erweitert* und *Hinzufügen* klicken.
4. `Greenbone Local Scan` in das Eingabefeld eingeben und auf *OK* klicken (siehe Abb. 10.14).
5. *Dieses Objekt und untergeordnete Objekte* in der Drop-down-Liste *Übernehmen für* wählen.
6. Alle Checkboxen für *Zulassen* deaktivieren und Checkboxen *Wert festlegen*, *Unterschlüssel erstellen*, *Link erstellen*, *Löschen*, *Berechtigungen ändern* und *Besitz übernehmen* für *Verweigern* aktivieren (siehe Abb. 10.15).
7. Zweimal auf *OK* klicken und Warnung durch Klicken auf *Ja* bestätigen.
8. Auf *OK* klicken.

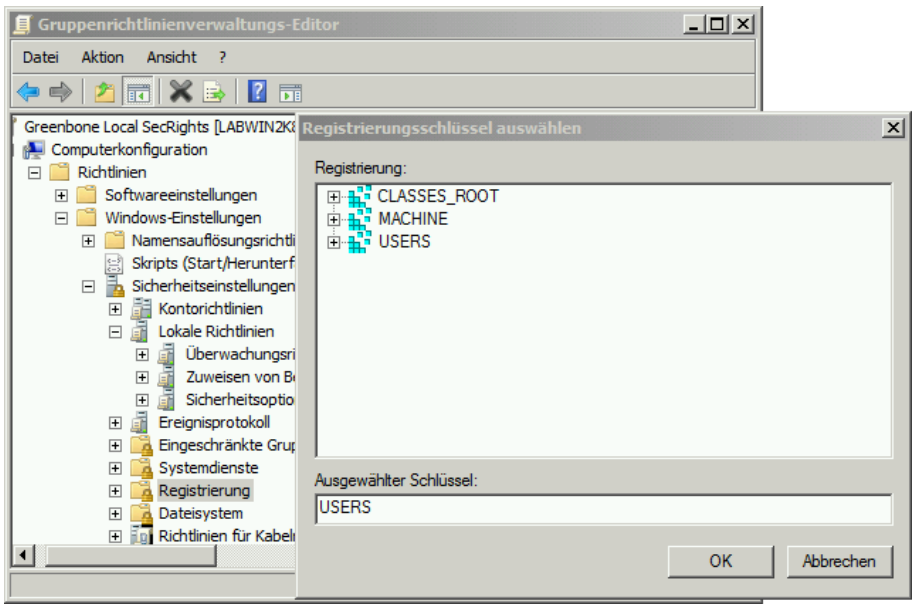


Abb. 10.13: Wählen des Registrierungsschlüssels

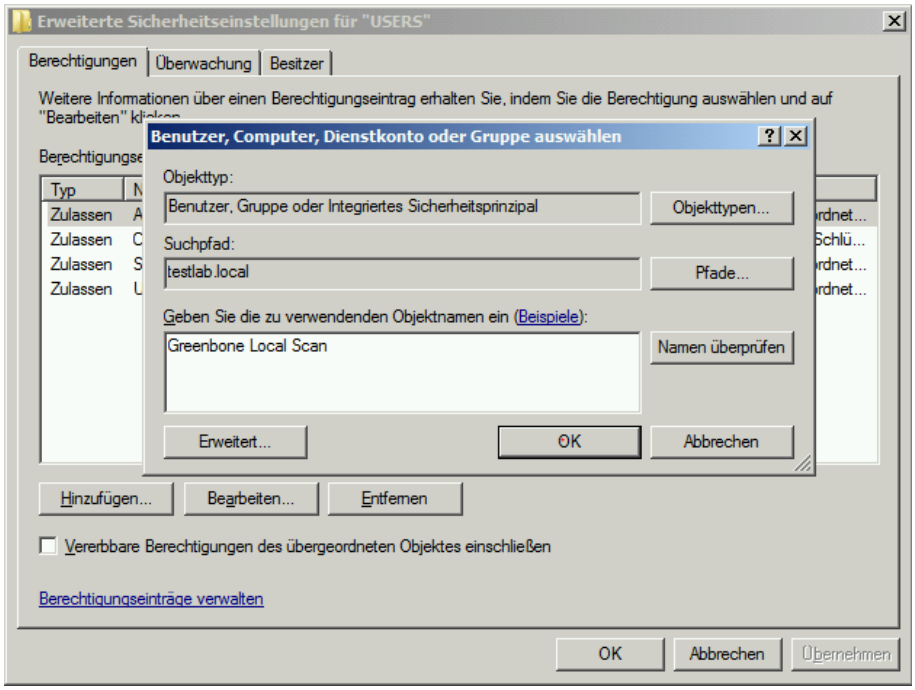


Abb. 10.14: Wählen der Gruppe *Greenbone Local Scan*

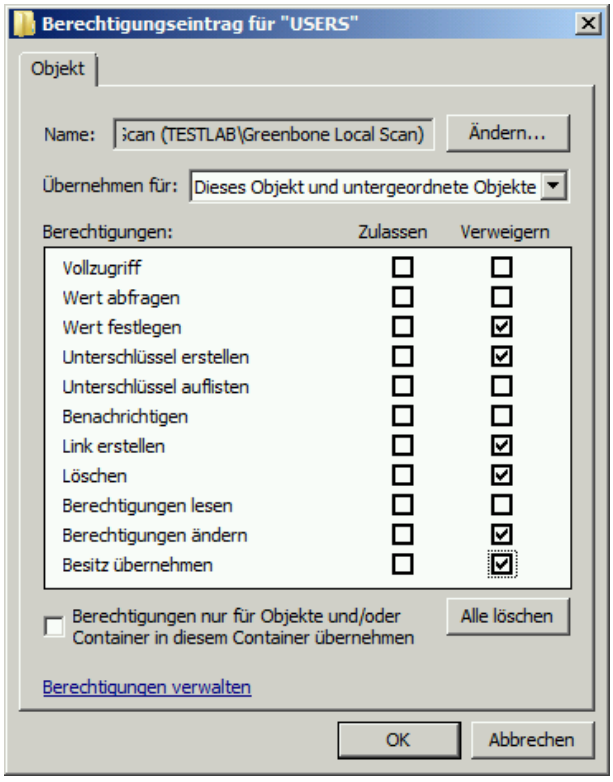


Abb. 10.15: Verweigern der Bearbeitung der Registrierung

9. Radiobuttons *Diesen Schlüssel konfigurieren* und *Vererbbare Berechtigungen an alle Unterschlüssel verteilen* wählen und auf *OK* klicken (siehe Abb. 10.16).

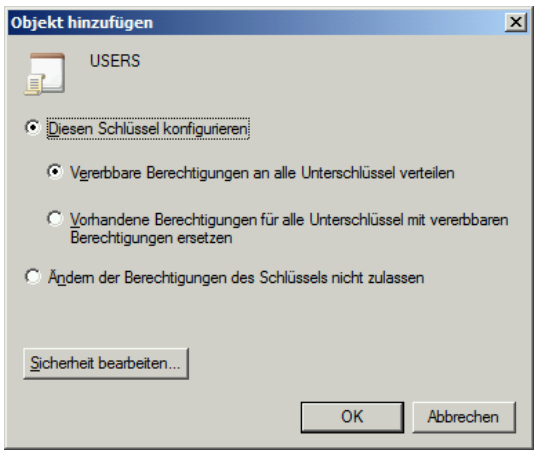


Abb. 10.16: Rekursivmachen der Berechtigungen

10. Schritte 2 bis 9 für *MACHINE* und *CLASSES_ROOT* wiederholen.

Die Gruppenrichtlinie verbinden

1. Im rechten Panel auf die Domäne rechtsklicken und *Vorhandenes Gruppenrichtlinienobjekt verknüpfen* wählen.
2. *Greenbone Local SecRights* im Abschnitt *Gruppenrichtlinienobjekte* wählen und auf *OK* klicken (siehe Abb. 10.17).

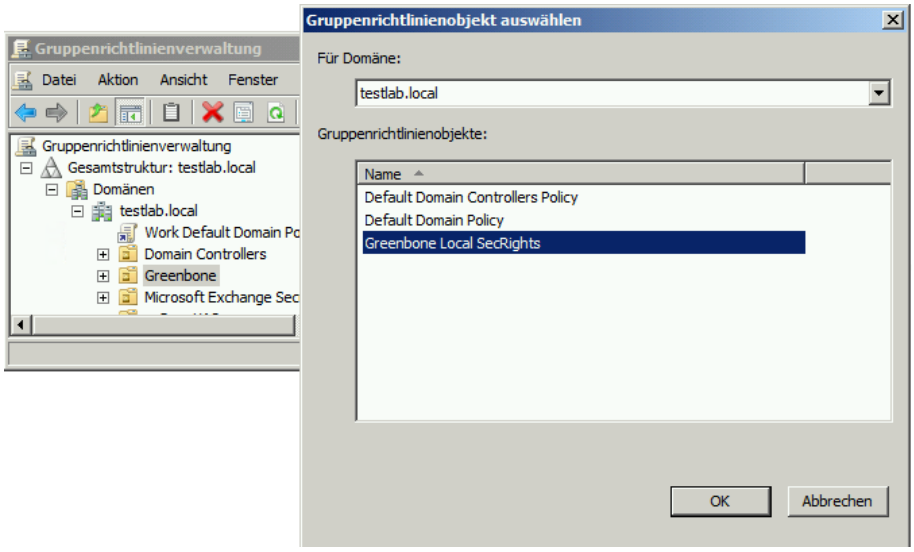


Abb. 10.17: Verbinden der Richtlinie

10.3.3.3 Einschränkungen

Da Schreibrechte auf der Registrierung und dem Systemlaufwerk entfernt wurden, funktionieren die beiden folgenden Tests nicht mehr:

- ***Leave information on scanned Windows hosts* (OID 1.3.6.1.4.1.25623.1.0.96171)** Falls gewünscht, erstellt dieser Test Informationen über den Start und das Ende eines Scans unter HKLM\Software\VulScanInfo. Da HKLM die Schreibrechte verweigert werden, ist dies nicht länger möglich. Falls der Test ausgeführt werden soll, muss das Gruppenrichtlinienobjekt entsprechend angepasst werden.
- ***Windows file Checksums* (OID 1.3.6.1.4.1.25623.1.0.96180)** Falls gewünscht, speichert dieser Test das Tool ReHash unter C:\Windows\system32 (auf 32-Bit-Systemen) oder C:\Windows\SysWOW64 (auf 64-Bit-Systemen). Da die Schreibrechte verweigert werden, ist dies nicht länger möglich. Falls der Test ausgeführt werden soll, muss das Tool separat gespeichert werden oder das Gruppenrichtlinienobjekt entsprechend angepasst werden.

  Mehr Informationen können in Kapitel *12.4.3* (Seite 336) gefunden werden.

10.3.3.4 Scannen ohne Domänenadministrator und lokale Administratorberechtigungen

Es ist möglich, eine Gruppenrichtlinie zu erstellen, in der der Benutzer keine lokalen Administratorberechtigungen hat. Allerdings ist der Aufwand, die entsprechenden Leserechte zu jedem Zweig und Ordner der Registrierung hinzuzufügen, sehr hoch. Leider ist das Vererben von Berechtigungen für viele Ordner und Zweige deaktiviert. Außerdem können diese Änderungen zwar durch die Gruppenrichtlinie festgelegt werden, aber nicht wieder entfernt werden („tattooing GPO“). Bestimmte Berechtigungen könnten überschrieben werden, sodass zusätzliche Probleme auftreten.

Das Erstellen einer Gruppenrichtlinie, in der der Benutzer keinerlei Administratorberechtigungen hat, ist aus technischer und administrativer Sicht nicht sinnvoll.

10.3.4 Anforderungen auf Zielsystemen mit ESXi

Bemerkung: Wenn eine vCenter Server Appliance (VCSA) zur Steuerung von ESXi-Hosts verwendet wird und User auf der VCSA erstellt werden, sind sie nur auf der VCSA und nicht auf den ESXi-Hosts bekannt.

Scan-User müssen auf jedem ESXi-Host, der gescannt wird, erstellt werden.

Standardmäßig sind lokale ESXi-User auf Rollen ohne Schreibrechte beschränkt. Es muss entweder ein administrativer Account oder eine Read-only-Rolle mit Berechtigung für globale Einstellungen genutzt werden.

Eine Read-only-Rolle mit Berechtigung für globale Einstellungen kann wie folgt eingerichtet werden:

1. Web-Oberfläche der VMware-ESXi-Instanz öffnen und einloggen.
2. *Host* > *Verwalten* in der Spalte *Navigator* links wählen.
3. Register *Sicherheit und Benutzer* wählen.
4. *Rollen* im linken Menüpanel wählen (siehe Abb. 10.18).

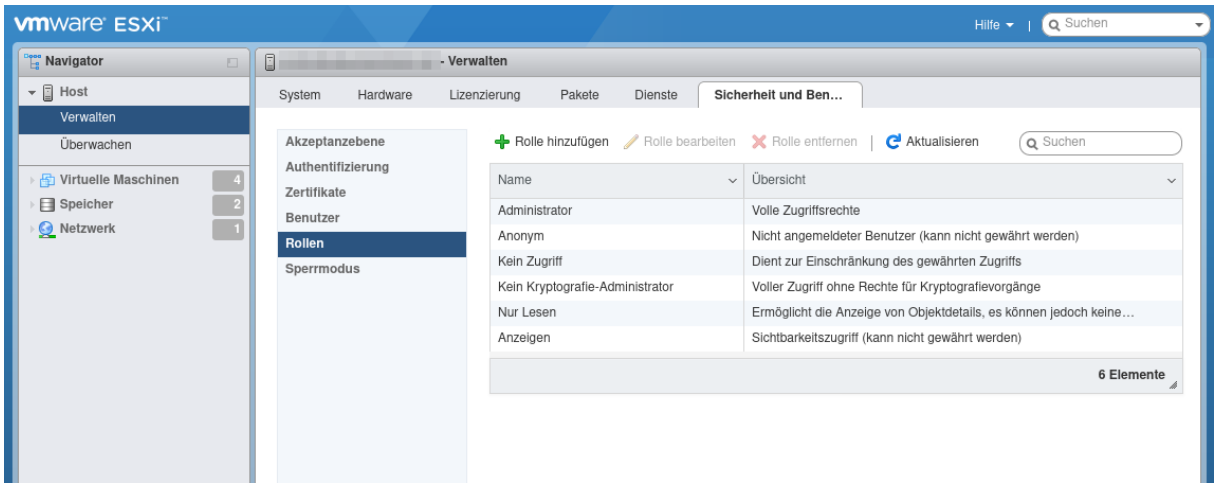


Abb. 10.18: Anzeigen der Rollen

5. Auf *Rolle hinzufügen* klicken.
6. Namen für die Rolle in das Eingabefeld *Rollenname* eingeben.
7. Checkbox *System* aktivieren.
8. Auf *Global* klicken und Checkbox *Settings* aktivieren (siehe Abb. 10.19).
9. Auf *Hinzufügen* klicken.
10. Auf *Host* in der Spalte *Navigator* links rechtsklicken und *Berechtigungen* wählen.
11. Scan-Benutzeraccount, der von der Appliance genutzt wird, wählen.
12. Auf *Rolle zuweisen* klicken.
13. Zuvor erstellte Rolle in der Drop-down-Liste wählen (siehe Abb. 10.20).
14. Auf *Rolle zuweisen* klicken.
15. Auf *Schließen* klicken.

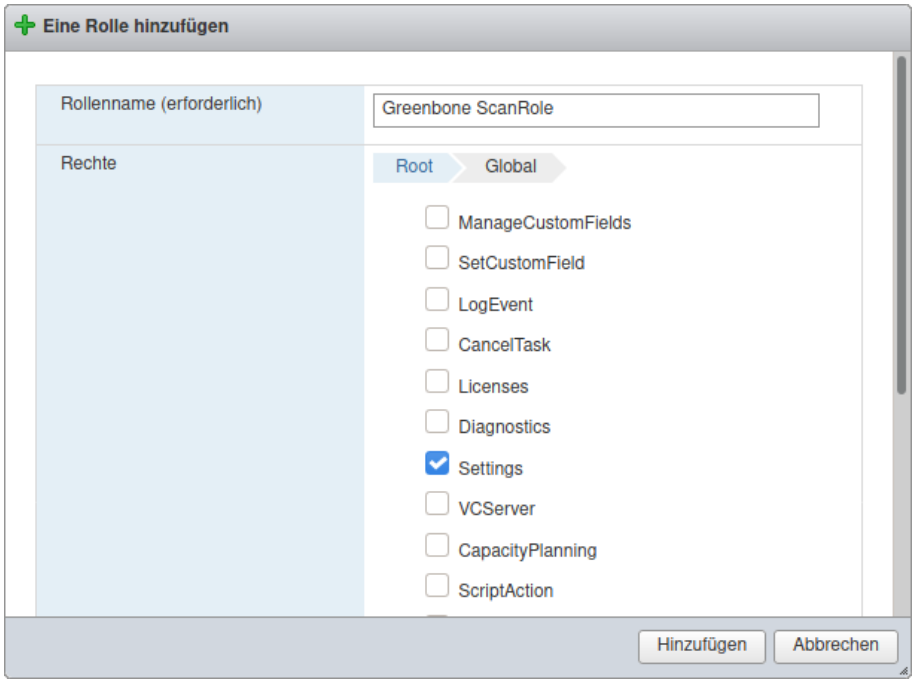


Abb. 10.19: Erstellen einer Rolle

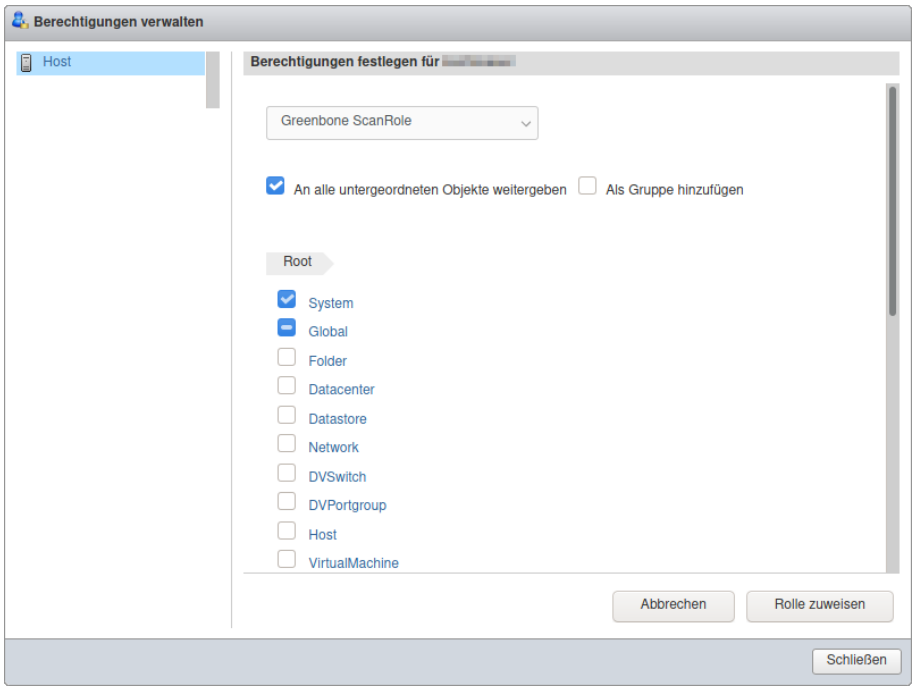


Abb. 10.20: Zuweisen der Rolle an den Scan-Benutzer

10.3.5 Anforderungen auf Zielsystemen mit Linux/Unix

- Für authentifizierte Scans auf Linux- oder Unix-Systemen ist normalerweise der reguläre Benutzerzugang ausreichend. Der Login wird mithilfe von SSH vorgenommen. Die Authentifizierung wird entweder mit Passwörtern oder einem auf der Appliance gespeicherten privaten SSH-Schlüssel durchgeführt.
- Ein Remote-SSH-Server sollte die folgenden Standardeinstellungen in der Datei `sshd_config` konfiguriert haben:
  - `MaxSessions`: 10
  - `MaxAuthTries`: 6

  Wenn andere als die Standardwerte und niedrigere Werte verwendet werden, kann es zu fehlgeschlagenen Logins kommen.
- Generiertes Installationspaket für Anmeldedaten: Das Installationspaket für Linux-Distributionen basierend auf Debian ist eine DEB-Datei, das Installationspaket für Linux-Distributionen basierend auf RedHat ist eine RPM-Datei. Beide Installationspakete erstellen einen neuen Benutzer ohne besondere Berechtigungen. Ein öffentlicher SSH-Schlüssel, der auf der Appliance erstellt wird, wird im Home-Verzeichnis des Benutzers gespeichert. Für Benutzer anderer Linux-Distributionen oder Unix-Derivaten, wird der öffentliche Schlüssel zum Herunterladen angeboten. Das Erstellen eines Benutzers und Speichern des öffentlichen Schlüssels mit den korrekten Dateiberechtigungen liegt in der Verantwortung des Benutzers.
- In beiden Fällen muss sichergestellt werden, dass die Authentifizierung mithilfe des öffentlichen Schlüssels nicht durch den SSH-Daemon verhindert wird. Die Zeile `PubkeyAuthentication no` darf nicht vorhanden sein.
- Vorhandene SSH-Schlüsselpaare können auch genutzt werden. SSH-Schlüsselpaare können mithilfe des Befehls `ssh-keygen` auf Linux oder `puttygen.exe` beim Nutzen von PuTTY auf Microsoft Windows generiert werden. Um ein vorhandenes SSH-Schlüsselpaar nutzen zu können, muss der private Schlüssel beim Erstellen der Anmeldedaten hinterlegt werden. Der private SSH-Schlüssel muss im PEM- oder OpenSSH-Format vorliegen. Die Schlüsselarten Ed25519, ECDSA, RSA und DSA werden unterstützt.
- Für Scans, die das Prüfen von Richtlinien beinhalten, sind möglicherweise root-Berechtigungen oder die Mitgliedschaft in bestimmten Gruppe (oft `wheel`) nötig. Aus Sicherheitsgründen sind einige Konfigurationsdateien nur von Super-Benutzern oder Mitgliedern bestimmter Gruppen lesbar.
- Je mehr Berechtigungen ein Nutzer hat, desto mehr Ergebnisse und Einstellungen können auf einem System erkannt werden. In einigen Fällen ist möglicherweise ein Root-Zugang nötig.
- Die folgenden Befehle werden während eines authentifizierten Scans mit einem Root-Account ausgeführt.

  Wichtig:

  - Diese Liste ist nicht statisch. Neue oder geänderte VTs könnten jederzeit neue Befehle hinzufügen.
  - Abhängig von der gefundenen Software könnten zusätzliche Befehle ausgeführt werden.
  - Die ausgeführten Befehle hängen von der Linux-Distribution und der gewählten Scan-Konfiguration ab.

  - bash
  - cat
  - date
  - dpkg
  - egrep

  - find
  - grep
  - host
  - id
  - ip
  - lastlog
  - locate
  - ls
  - md5sum
  - mlocate
  - netstat
  - perl
  - ps
  - rpm
  - sh
  - sha1sum
  - slocate
  - uname
  - uptime
  - whereis
  - which

- Die Installation des Pakets `locate` (alternativ `mlocate`), um den Befehl `locate`/`mlocate` auf dem Zielsystem verfügbar zu machen, wird empfohlen. Die Nutzung dieses Befehls reduziert Aufrufe des Befehls `find`, der für die Suche nach Dateien genutzt wird, und verbessert somit die Scanleistung und verringert die Ressourcennutzung auf dem Zielsystem.

  Damit die Befehle funktionieren, müssen möglicherweise die entsprechenden Datenbank-Berechtigungen und regelmäßige Datenbank-Updates, z. B. mithilfe eines Cronjobs, konfiguriert werden.

10.3.6 Anforderungen auf Zielsystemen mit Cisco OS

Die Appliance kann auch Netzwerkkomponenten wie Router und Switches auf Schwachstellen prüfen. Während die üblichen Netzwerkdienste über das Netzwerk gefunden und geprüft werden, können einige Schwachstellen nur durch einen authentifizierten Scan entdeckt werden. Für einen authentifizierten Scan kann die Appliance entweder SNMP oder SSH nutzen.

10.3.6.1 SNMP

Die Appliance kann das Protokoll SNMP nutzen, um auf die Cisco-Netzwerkkomponenten zuzugreifen. Die Appliance unterstützt SNMPv1, v2c und v3. SNMP nutzt den Port 161/udp. Die standardmäßige Portliste enthält keine UDP-Ports. Deshalb wird dieser Port während eines Schwachstellentests mit der Scan-Konfiguration *Full and fast* ignoriert und keine SNMP-Prüfung durchgeführt. Um Netzwerkkomponenten zu scannen, sollte die Portliste bearbeitet werden, sodass mindestens die folgenden Ports enthalten sind:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP-Server
- 69/udp TFTP
- 123/udp NTP
- 161/udp SNMP
- 162/udp SNMP-Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6
- 6161/udp 6162/udp Unified CM

Der Administrator kann besondere Portlisten erstellen, die nur für solche Netzwerkkomponenten genutzt werden.

Die Appliance benötigt zu sehr wenigen Objekten des SNMP-Baums Zugriff. Für einen weniger privilegierten Zugriff sollte eine SNMP-Sicht genutzt werden, um die Sichtbarkeit des SNMP-Baums für die Appliance einzuschränken. Die folgenden zwei Beispiele erklären, wie solch eine Sicht mithilfe eines Community-Strings oder eines SNMPv3-Benutzers eingestellt wird.

Um den SNMP-Community-String zu nutzen, werden die folgenden Befehle auf dem Ziel benötigt:

```
# configure terminal
```

Mithilfe einer Zugriffsliste kann die Nutzung der Community beschränkt werden. Die IP-Adresse der Appliance ist in diesem Beispiel 192.168.222.74:

```
(config) # access-list 99 permit 192.168.222.74
```

Die Sicht `gsm` sollte nur den Zugriff auf die Systembeschreibung erlauben:

```
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

Der letzte Befehl verbindet die Community `gsm-community` mit der Sicht `gsm` und der Zugriffsliste 99:

```
(config) # snmp-server community gsm-community view gsm RO 99
```

Falls ein SNMPv3-Benutzer mit Verschlüsselung genutzt wird, werden die folgenden Konfigurationszeilen auf dem Ziel benötigt:

```
# configure terminal
(config) # access-list 99 permit 192.168.222.74
(config) # snmp-server view gsm system included
(config) # snmp-server view gsm system.9 excluded
```

SNMPv3 benötigt zuerst das Einrichten einer Gruppe. Hier wird die Gruppe `gsmgroup` mit der Sicht `gsm` und der Zugriffsliste 99 verbunden:

```
(config) # snmp-server group gsmgroup v3 priv read gsm access 99
```

Nun kann der Benutzer mit dem Passwort `gsm-password` und dem Verschlüsselungsschlüssel `gsm-encrypt` erstellt werden. Die Authentifizierung wird durch MD5 und die Verschlüsselung durch AE128 durchgeführt:

```
(config) # snmp-server user gsm-user gsm-group v3 auth md5 gsm-password priv
aes 128 gsm-encrypt
```

Um entweder die Community oder den SNMPv3-Benutzer auf der Appliance zu konfigurieren, als Administrator *Konfiguration > Anmeldedaten* in der Menüleiste wählen (siehe Kapitel *10.3.2* (Seite 222)).

10.3.6.2 SSH

Der authentifizierte Scan kann auch über SSH ausgeführt werden. Falls SSH genutzt wird, wird die Nutzung besonderer unprivilegierter Benutzer empfohlen. Die Appliance benötigt aktuell nur den Befehl `show version`, um die aktuelle Version der Firmware des Geräts zu erhalten.

Um einen weniger privilegierten Benutzer einzurichten, der nur diesen Befehl ausführen darf, sind verschiedene Ansätze möglich. Das folgende Beispiel nutzt die rollenbasierte Zugriffskontrollenfunktionalität.

Bemerkung: Bevor eines der folgenden Beispiele genutzt wird, muss sichergestellt werden, dass alle Nebeneffekte der Konfiguration verstanden werden. Falls sie ohne Verifizierung genutzt wird, beschränkt das System möglicherweise weitere Logins über SSH oder die Konsole.

Um die rollenbasierte Zugriffskontrolle zu nutzen, müssen AAA und Views aktiviert werden:

```
> enable
# configure terminal
(config)# aaa new-model
(config)# exit
> enable view
# configure terminal
```

Die folgenden Befehle erstellen eine eingeschränkte Sicht, die nur den Befehl `show version` beinhaltet. Das gelieferte Passwort `view-pw` ist nicht kritisch:

```
(config)# parser view gsm-view
(config-view)# secret 0 view-pw
(config-view)# commands exec include show version
(config-view)# exit
```

Nun wird der Benutzer `gsm-user` mit dem Passwort `gsm-pw` erstellt und mit der Sicht `gsm-view` verknüpft:

```
(config)# username gsm-user view gsm-view password 0 gsm-pw
(config)# aaa authorization console
(config)# aaa authorization exec default local
```

Falls SSH noch nicht aktiviert ist, erledigt dies der folgende Befehl. Der entsprechende Hostname und die entsprechende Domäne müssen genutzt werden:

```
(config)# hostname switch
(config)# ip domain-name greenbone.net
(config)# crypto key generate rsa general-keys modulus 2048
```

Schließlich SSH-Logins mithilfe der folgenden Befehle aktivieren:

```
(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# Crtl-Z
```

Bemerkung: Um einen vollständigen Scan auszuführen, z. B. mit der Scan-Konfiguration *Full and fast*, muss die Einstellung *ssh server rate-limit* auf `240` gesetzt werden. Vor dem Scannen sollte dieser Wert überprüft und ggf. angepasst werden.

Die Anmeldedaten des Benutzers müssen auf der Appliance eingegebene werden. *Konfiguration* > *Anmeldedaten* in der Menüleiste wählen und den entsprechenden Benutzer erstellen (siehe Kapitel *10.3.2* (Seite 222)).

Anmeldedaten mit dem Ziel verbinden, damit sie als SSH-Anmeldedaten genutzt werden können.

10.3.7 Anforderungen auf Zielsystemen mit Huawei VRP

Die Appliance kann auch Netzwerkkomponenten wie Router und Switches auf Schwachstellen prüfen. Während die üblichen Netzwerkdienste über das Netzwerk gefunden und geprüft werden, können einige Schwachstellen nur durch einen authentifizierten Scan entdeckt werden. Für einen authentifizierten Scan kann die Appliance entweder SNMP oder SSH nutzen.

Bemerkung: Die Befehle in diesem Kapitel dienen als Beispiel und sollten auf den meisten Huawei-Routern funktionieren.

Abhängig von der Softwareversion oder von der Hardware, könnten einige Befehle abweichen (z. B. die Reihenfolge der Parameter oder Werte), nicht nötig sein oder nicht verfügbar sein.

Weitere Informationen befinden sich in der zugehörigen Dokumentation für das entsprechende Gerät und die entsprechende Software-Version.

10.3.7.1 SNMP

Die Appliance kann das Protokoll SNMP nutzen, um auf die Huawei-Netzwerkkomponenten zuzugreifen. Die Appliance unterstützt SNMPv1, v2c und v3. SNMP nutzt den Port 161/udp. Die standardmäßige Portliste enthält keine UDP-Ports. Deshalb wird dieser Port während eines Schwachstellentests mit der Scan-Konfiguration *Full and fast* ignoriert und keine SNMP-Prüfung durchgeführt. Um Netzwerkkomponenten zu scannen, sollte die Portliste bearbeitet werden, sodass mindestens die folgenden Ports enthalten sind:

- 22/tcp SSH
- 80/tcp 8080/tcp HTTP
- 443/tcp 8443/tcp HTTPS
- 2000/tcp SCCP
- 2443/tcp SCCPS
- 5060/tcp 5060/udp SIP
- 5061/tcp 5061/udp SIPS
- 67/udp DHCP-Server
- 69/udp TFTP
- 123/udp NTP

- 161/udp SNMP
- 162/udp SNMP-Traps
- 500/udp IKE
- 514/udp Syslog
- 546/udp DHCPv6

Der Administrator kann besondere Portlisten erstellen, die nur für solche Netzwerkkomponenten genutzt werden.

Die Appliance benötigt zu sehr wenigen Objekten des SNMP-Baums Zugriff. Für einen weniger privilegierten Zugriff sollte eine SNMP-Sicht genutzt werden, um die Sichtbarkeit des SNMP-Baums für die Appliance einzuschränken. Die folgenden zwei Beispiele erklären, wie solch eine Sicht mithilfe eines Community-Strings oder eines SNMPv3-Benutzers eingestellt wird.

Um den SNMP-Community-String zu nutzen, werden die folgenden Befehle auf dem Ziel benötigt:

```
<HUAWEI>system-view
```

Mithilfe einer Zugriffsliste kann die Nutzung der Community beschränkt werden. Die IP-Adresse der Appliance ist in diesem Beispiel 192.168.222.74:

```
[~HUAWEI]acl 2000
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000]commit
[~HUAWEI-acl4-basic-2000]quit
```

Version 2c von SNMPv erlauben:

```
[~HUAWEI]snmp-agent sys-info version v3 v2c
[*HUAWEI]commit
```

Die Sicht `gsm` sollte nur den Zugriff auf die Systembeschreibung erlauben:

```
[~HUAWEI]snmp-agent mib-view included gsm system
[*HUAWEI]snmp-agent mib-view excluded gsm system.9
[*HUAWEI]commit
```

Der letzte Befehl verbindet die Community `gsm-community` mit der Sicht `gsm` und der Zugriffsliste 2000:

```
[~HUAWEI]snmp-agent community read gsm-community mib-view gsm acl 2000
[*HUAWEI]commit
```

Falls ein SNMPv3-Benutzer mit Verschlüsselung genutzt wird, werden die folgenden Konfigurationszeilen auf dem Ziel benötigt:

```
<HUAWEI>system-view
[~HUAWEI]acl 2000
[~HUAWEI-acl4-basic-2000]rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000]quit
[*HUAWEI]snmp-agent sys-info version v3
[*HUAWEI]snmp-agent mib-view included gsm system
[*HUAWEI]snmp-agent mib-view excluded gsm system.9
[*HUAWEI]commit
```

SNMPv3 benötigt zuerst das Einrichten einer Gruppe. Hier wird die Gruppe `gsmgroup` mit der Sicht `gsm` und der Zugriffsliste 2000 verbunden:

```
[~HUAWEI]snmp-agent group v3 gsmgroup privacy read-view gsm acl 2000
[*HUAWEI]commit
```

Nun kann der Benutzer mit dem Passwort `gsm-password` und dem Verschlüsselungsschlüssel `gsm-encrypt` erstellt werden. Die Authentifizierung wird durch MD5 und die Verschlüsselung durch AE128 durchgeführt. Dies wird in drei Schritten durchgeführt:

Passwort `gsm-password` konfigurieren:

```
[~HUAWEI]snmp-agent usm-user v3 gsm-user authentication-mode md5
Please configure the authentication password (8-255)
[*HUAWEI]commit
```

Verschlüsselungsschlüssel `gsm-encrypt` konfigurieren:

```
[~HUAWEI]snmp-agent usm-user v3 gsm-user privacy-mode aes128
Please configure the privacy password (8-255)
[*HUAWEI]commit
```

Nutzer zur Gruppe hinzufügen:

```
[*HUAWEI]snmp-agent usm-user v3 gsm-user group gsmgroup
[*HUAWEI]commit
```

Um entweder die Community oder den SNMPv3-Benutzer auf der Appliance zu konfigurieren, als Administrator *Konfiguration > Anmeldedaten* in der Menüleiste wählen (siehe Kapitel *10.3.2* (Seite 222)).

10.3.7.2 SSH

Der authentifizierte Scan kann auch über SSH durchgeführt werden. Falls SSH genutzt wird, wird die Verwendung eines speziellen unprivilegierten Benutzers empfohlen. Die Appliance benötigt derzeit nur die Befehle `display device`, `display version` und `display patch-information`, um die aktuelle Firmware-Version des Geräts abzufragen.

Bemerkung: Falls ein Compliance-Scan ausgeführt wird, könnten die folgenden zusätzlichen Befehle genutzt werden:

- `display arp speed-limit`
- `display arp-miss speed-limit source-ip`
- `display current-configuration`
- `display current-configuration configuration bgp`
- `display current-configuration configuration pim`
- `display current-configuration configuration user-interface`
- `display current-configuration configuration vpn-instance`
- `display current-configuration interface`
- `display current-configuration | include multicast`
- `display current-configuration | include ntp`
- `display current-configuration | include snmp`
- `display current-configuration | include ssh`
- `display ftp-server`

- `display isis peer`
- `display mpls ldp session verbose`
- `display mpls rsvp-te interface`
- `display ospf peer brief`
- `display ospfv3 peer`
- `display snmp-agent sys-info version`
- `display ssh server status`
- `display telnet server`
- `display telnet server status`
- `display vrrp`

Um einen weniger privilegierten Benutzer einzurichten, der nur diesen Befehl ausführen darf, sind verschiedene Ansätze möglich. Das folgende Beispiel nutzt die rollenbasierte Zugriffskontrollenfunktionalität.

Bemerkung: Bevor eines der folgenden Beispiele genutzt wird, muss sichergestellt werden, dass alle Nebeneffekte der Konfiguration verstanden werden. Falls sie ohne Verifizierung genutzt wird, beschränkt das System möglicherweise weitere Logins über SSH oder die Konsole.

Die folgenden Befehle erstellen eine eingeschränkte Sicht, die nur die Befehle `display device`, `display version` und `display patch-information` beinhaltet. Das gelieferte Passwort `Hello-secret123` ist nicht kritisch.

```
<HUAWEI> system-view
[~HUAWEI]aaa
[~HUAWEI-aaa]local-user gsm-user password cipher Hello-secret123
[*HUAWEI-aaa]local-user gsm-user level 0
[*HUAWEI-aaa]local-user gsm-user service-type ssh
[*HUAWEI-aaa]commit
[~HUAWEI-aaa]quit
[~HUAWEI]ssh user gsm-user authentication-type password
[*HUAWEI]ssh user gsm-user service-type stelnet
[*HUAWEI]commit
```

Die folgenden Befehle fügen nur die Befehle `display version`, `display patch-information` und `display device` zu „level 0“ hinzu, sodass `gsm-user` beschränkt ist:

```
[~HUAWEI] command-privilege level 0 view global display device
[*HUAWEI] command-privilege level 0 view global display version
[*HUAWEI] command-privilege level 0 view global display patch-information
[*HUAWEI]commit
```

Falls SSH noch nicht aktiviert ist, erledigt dies der folgende Befehl:

```
[~HUAWEI] rsa local-key-pair create
[*HUAWEI]commit
```

SSH-Logins mithilfe der folgenden Befehle aktivieren:

```
[~HUAWEI] user-interface vty 0 4
[*HUAWEI-ui-vty0-4] authentication-mode aaa
[*HUAWEI-ui-vty0-4] protocol inbound ssh
[*HUAWEI-ui-vty0-4] quit
[*HUAWEI]commit
```

Den STelnet-Server aktivieren:

```
[~HUAWEI] stelnet server enable
[*HUAWEI] ssh authentication-type default password
[*HUAWEI]commit
```

Mithilfe einer Zugriffsliste kann die Nutzung des SSH-Logins beschränkt werden. Die IP-Adresse der Appliance ist in diesem Beispiel 192.168.222.74.

Bemerkung: Dies könnte jegliche SSH-Anmeldungen von anderen IP-Adressen einschränken und das Gerät über das Netzwerk unzugänglich machen.

```
[~HUAWEI]acl 2000
[*HUAWEI-acl4-basic-2000] rule permit source 192.168.222.74 32
[*HUAWEI-acl4-basic-2000] quit
[*HUAWEI] HUAWEI acl 2000
[*HUAWEI] commit
```

In Abhängigkeit von den Sicherheitseinstellungen muss das Passwort für `gsm-view` beim ersten Login geändert werden. Dies sollte durch einmaliges Einloggen via SSH geprüft werden.

Die Anmeldedaten des Benutzers müssen auf der Appliance eingegebene werden. *Konfiguration > Anmeldedaten* in der Menüleiste wählen und den entsprechenden Benutzer erstellen (siehe Kapitel *10.3.2* (Seite 222)).

Anmeldedaten mit dem Ziel verbinden, damit sie als SSH-Anmeldedaten genutzt werden können.

10.3.8 Anforderungen auf Zielsystemen mit EulerOS

- Für authentifizierte Scans auf EulerOS ist normalerweise der reguläre Benutzerzugang ausreichend. Der Login wird mithilfe von SSH vorgenommen. Die Authentifizierung wird entweder mit Passwörtern oder einem auf der Appliance gespeicherten privaten SSH-Schlüssel durchgeführt.
- Generiertes Installationspaket für Anmeldedaten: Das Installationspaket für EulerOS ist eine RPM-Datei. Das Installationspaket erstellt einen neuen Benutzer ohne besondere Berechtigungen. Ein öffentlicher SSH-Schlüssel, der auf der Appliance erstellt wird, wird im Home-Verzeichnis des Benutzers gespeichert. Für Benutzer anderer Linux-Distributionen oder Unix-Derivaten, wird der öffentliche Schlüssel zum Herunterladen angeboten. Das Erstellen eines Benutzers und Speichern des öffentlichen Schlüssels mit den korrekten Dateiberechtigungen liegt in der Verantwortung des Benutzers.
- In beiden Fällen muss sichergestellt werden, dass die Authentifizierung mithilfe des öffentlichen Schlüssels nicht durch den SSH-Daemon verhindert wird. Die Zeile `PubkeyAuthentication no` darf nicht vorhanden sein.
- Vorhandene SSH-Schlüsselpaare können auch genutzt werden. SSH-Schlüsselpaare können mithilfe des Befehls `ssh-keygen` auf EulerOS oder `puttygen.exe` beim Nutzen von PuTTY auf Microsoft Windows generiert werden. Um ein vorhandenes SSH-Schlüsselpaar nutzen zu können, muss der private Schlüssel beim Erstellen der Anmeldedaten hinterlegt werden. Der private SSH-Schlüssel muss im PEM- oder OpenSSH-Format vorliegen. Die Schlüsselarten Ed25519, ECDSA, RSA und DSA werden unterstützt.

- Für Scans, die das Prüfen von Richtlinien beinhalten, sind möglicherweise root-Berechtigungen oder die Mitgliedschaft in bestimmten Gruppe (oft `wheel`) nötig. Aus Sicherheitsgründen sind einige Konfigurationsdateien nur von Super-Benutzern oder Mitgliedern bestimmter Gruppen lesbar.
- Je mehr Berechtigungen ein Nutzer hat, desto mehr Ergebnisse und Einstellungen können auf einem System erkannt werden. In einigen Fällen ist möglicherweise ein Root-Zugang nötig.
- Die folgenden Befehle werden während eines authentifizierten Scans mit einem Root-Account ausgeführt.

  Wichtig:

  – Diese Liste ist nicht statisch. Neue oder geänderte VTs könnten jederzeit neue Befehle hinzufügen.

  – Abhängig von der gefundenen Software könnten zusätzliche Befehle ausgeführt werden.

  – bash
  – cat
  – date
  – dpkg
  – egrep
  – find
  – grep
  – host
  – id
  – ip
  – lastlog
  – locate
  – ls
  – md5sum
  – mlocate
  – netstat
  – perl
  – ps
  – rpm
  – sh
  – sha1sum
  – slocate
  – uname
  – uptime
  – whereis
  – which

- Die Installation des Pakets `locate` (alternativ `mlocate`), um den Befehl `locate`/`mlocate` auf dem Zielsystem verfügbar zu machen, wird empfohlen. Die Nutzung dieses Befehls reduziert Aufrufe des Befehls `find`, der für die Suche nach Dateien genutzt wird, und verbessert somit die Scanleistung und verringert die Ressourcennutzung auf dem Zielsystem.

  Damit die Befehle funktionieren, müssen möglicherweise die entsprechenden Datenbank-Berechtigungen und regelmäßige Datenbank-Updates, z. B. mithilfe eines Cronjobs, konfiguriert werden.

10.3.9 Anforderungen auf Zielsystemen mit GaussDB

Bemerkung: Es muss sichergestellt werden, dass der Scan von einem Benutzer ausgeführt wird, der GaussDB-Ausführungsberechtigungen besitzt.

10.3.9.1 Anforderungen für den Systembenutzer *root*

Bemerkung: Im Allgemeinen wird nicht empfohlen, mit dem Benutzer *root* zu scannen.

Ein Root-Nutzer hat die folgenden Anforderungen für das Scannen auf einem Zielsystem mit GaussDB:

- Auf der Appliance:
  - Anmeldedaten für den/die Zielhost(s), entweder als Passwort oder als SSH-Schlüssel
- Auf dem Zielsystem:
  - Root-Benutzer ist in der Lage `zsq`/`zengine` auszuführen (z. B. `LD_LIBRARY_PATH` ist korrekt eingestellt und nicht auf Standard)
  - `PermitRootLogin yes` in `sshd_config` oder `PermitRootLogin prohibit-password` in `sshd_config` für auf SSH-Schlüssel basierenden Anmeldedaten

10.3.9.2 Anforderungen für einen Datenbankadministrator-Account (z. B. *gaussdba*)

Ein Datenbankadministrator hat die folgenden Anforderungen für das Scannen auf einem Zielsystem mit GaussDB:

- Auf der Appliance:
  - Anmeldedaten für den/die Zielhost(s), entweder als Passwort oder als SSH-Schlüssel
- Auf dem Zielsystem:
  - Benutzer *gaussdba* ist der Datenbankinstallationsbenutzer

10.3.9.3 Anforderungen für einen normalen Benutzer-Account

Ein normaler Benutzer hat die folgenden Anforderungen für das Scannen auf einem Zielsystem mit GaussDB:

- Auf der Appliance:
  - Anmeldedaten für den/die Zielhost(s), entweder als Passwort oder als SSH-Schlüssel
- Auf dem Zielsystem:
  - Benutzer ist in der Lage `zsq`/`zengine` auszuführen (z. B. `LD_LIBRARY_PATH` ist korrekt eingestellt und nicht auf Standard)

10.3.9.4 Anforderungen für einen normalen Datenbankbenutzer-Account (z. B. *gauss*)

Ein normaler Datenbankbenutzer hat die folgenden Anforderungen für das Scannen auf einem Zielsystem mit GaussDB:

- Auf der Appliance:
  - Anmeldedaten mit dem Benutzernamen `gauss` und einem Passwort, konfiguriert in jeder genutzten Scan-Konfiguration
- Auf dem Zielsystem:
  - Öffentlich zugänglicher Datenbankserver-Port

10.4 Einen CVE-Scan konfigurieren

Nicht jede Schwachstelle rechtfertigt einen neuen Scan des Netzwerks oder einzelner Systeme. Falls der GSM durch frühere Scans bereits Informationen über Schwachstellen erhalten hat, kann er eine Prognose darüber erstellen, welche Sicherheitsrisiken derzeit bestehen könnten.

Die Verwendung des CVE-Scanners ermöglicht eine schnelle Vorhersage möglicher Sicherheitsrisiken, ohne dass ein weiterer Schwachstellenscan erforderlich ist. Dies ist vor allem für Umgebungen interessant, in denen die meisten Schwachstellen durch den Einsatz der Appliance beseitigt oder behoben worden sind. Falls neue Sicherheitsrisiken vorhergesagt werden, kann ein tatsächlicher Schwachstellenscan durchgeführt werden, um die Prognose zu überprüfen.

Der CVE-Scanner überprüft die CPEs der Zielhosts, die im letzten Bericht für dieselbe IP-Adresse vorhanden sind, auf zugewiesene CVEs in den aktuellen Sicherheitsinfos (siehe Kapitel *14* (Seite 357)). Es werden nur Berichte von Aufgaben berücksichtigt, bei denen die Einstellung *Ergebnisse zu Assets hinzufügen* aktiviert ist. Dabei ist es irrelevant, ob die Einstellung vor oder nach dem Scan aktiviert wurde.

Bemerkung: Der CVE-Scanner kann aus den folgenden Gründen Falsch-Positiv-Meldungen anzeigen:

- Der Scanner prüft nicht, ob die Schwachstelle tatsächlich vorhanden ist.
- Der Scanner ist nicht in der Lage, „rückportierte“ Sicherheitskorrekturen, z. B. auf Unix-ähnlichen Systemen, zu erkennen, da er von der National Vulnerability Database (NVD)[25] abhängig ist, die diesen Korrekturstatus nicht pflegt und da der Korrekturstatus in der Produktversion nicht vermerkt ist.

Bemerkung: Es gibt einige Voraussetzungen für einen erfolgreichen CVE-Scan:

- Um erkannt zu werden, muss der CVE in der National Vulnerability Database (NVD)[26] eine CPE zugewiesen sein.
  - Solange *Undergoing analysis* auf der zugehörigen NVD-Webseite[27] angezeigt wird, sind keine Ergebnisse für eine CVE zu erwarten, wenn ein CVE-Scan durchgeführt wird.
  - Außerdem muss der CVE in der NVD eine *korrekte* CPE zugewiesen sein. Im Zweifelsfall sollte die CPE-CVE-Zuordnung manuell auf der/den entsprechenden NVD-Webseite(n) überprüft werden.
- Die Assetdatenbank benötigt aktuelle Daten für den CVE-Scanner. Um die Produkte zu erkennen, muss vor der Ausführung des CVE-Scans ein vollständiger Scan durchgeführt werden, z. B. mit der Scan-Konfiguration *Full and fast*.
  - Ob ein Produkt gefunden wurde, kann im Register *Anwendungen* des Berichts des vollständigen Scans überprüft werden.

[25] https://nvd.nist.gov/
[26] https://nvd.nist.gov/
[27] https://nvd.nist.gov/vuln/full-listing

- Für den vollständigen Scan muss die Option *Ergebnisse zu Assets hinzufügen* für die Aufgabe aktiviert sein, damit die Ergebnisse zur Assetdatenbank hinzugefügt werden und dem CVE-Scanner zur Verfügung stehen.
- Die Ausführung eines vollständigen Scans mit Authentifizierung kann die vom CVE-Scan gefundenen Ergebnisse erhöhen.
- Ein vollständiger Scan der Systeme sollte regelmäßig erfolgen.

Ein CVE-Scan kann wie folgt ausgeführt werden:

1. Einen vollständigen Scan ausführen (siehe Kapitel *10.2* (Seite 213)).

   Bemerkung: Eine „Full“-Scan-Konfiguration muss gewählt werden, z. B. *Full and fast*.

   Zusätzlich muss der Radiobutton *Ja* für *Ergebnisse zu Assets hinzufügen* gewählt werden.

2. *Scans > Aufgaben* in der Menüleiste wählen.
3. Neue Aufgabe durch Bewegen der Maus über ☐★ und Klicken auf *Neue Aufgabe* erstellen.
4. Aufgabe definieren (siehe Kapitel *10.2.2* (Seite 218)).
5. *CVE* in der Drop-down-Liste *Scanner* wählen.
6. Auf *Speichern* klicken.
7. In der Zeile der Aufgabe auf ▷ klicken.

   → Der Scan wird ausgeführt. Für den Status einer Aufgabe siehe Kapitel *10.8* (Seite 257).

   Tipp: Sobald eine Aufgabe gestartet wurde, kann der Bericht der Aufgabe durch Klicken auf den Balken in der Spalte *Status* dargestellt werden. Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *11* (Seite 288).

   Sobald sich der Status zu *Abgeschlossen* ändert, ist der gesamte Bericht verfügbar. Zu jeder Zeit können Zwischenergebnisse angesehen werden (siehe Kapitel *11.2.1* (Seite 293)).

   Bemerkung: Die Fertigstellung des Scans kann einige Zeit in Anspruch nehmen. Die Seite aktualisiert automatisch, falls neue Daten verfügbar sind.

8. Wenn der Scan abgschlossen ist, *Scans > Berichte* in der Menüleiste wählen.
9. Ergebnisse durch Klicken auf das Datum des Berichts anzeigen lassen.

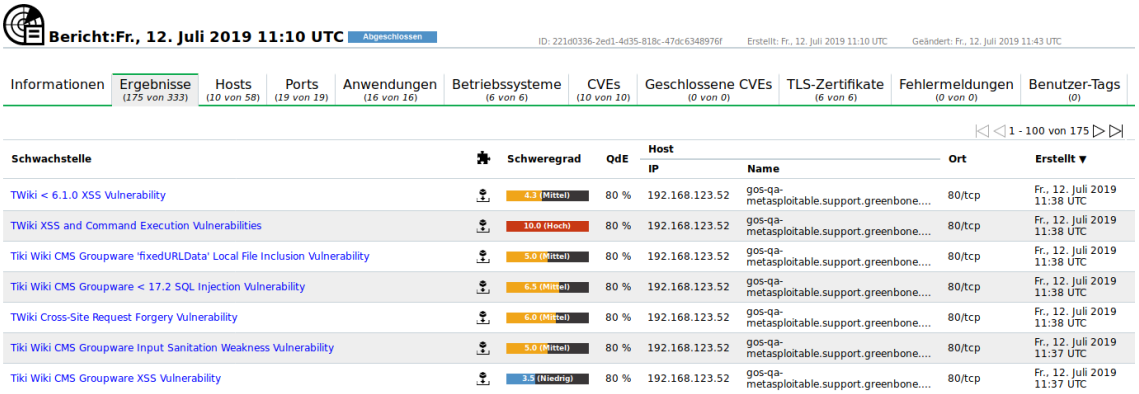
   → Der Bericht zeigt jede gefundene CVE als Schwachstelle (siehe Abb. 10.21).

10. Auf eine Schwachstelle und anschließend auf 🔍+ klicken.

    → Die Detailseite der Schwachstelle wird geöffnet.

    Der VT, zu dem das Ergebnis zugeordnet ist, wird im Abschnitt *Erkennungsmethode* angezeigt (siehe Abb. 10.22). Durch Klicken auf den VT wird die Detailseite des zugehörigen VTs geöffnet.

    Tipp: Für auf dieser Seite verfügbare Aktionen siehe Kapitel *11.2.1* (Seite 293).



Bericht:Fr., 12. Juli 2019 11:10 UTC Abgeschlossen

ID: 221d0336-2ed1-4d35-818c-47dc6348976f Erstellt: Fr., 12. Juli 2019 11:10 UTC Geändert: Fr., 12. Juli 2019 11:43 UTC

Informationen | Ergebnisse (175 von 333) | Hosts (10 von 58) | Ports (19 von 19) | Anwendungen (16 von 16) | Betriebssysteme (6 von 6) | CVEs (10 von 10) | Geschlossene CVEs (0 von 0) | TLS-Zertifikate (6 von 6) | Fehlermeldungen (0 von 0) | Benutzer-Tags (0)

1 - 100 von 175

Schwachstelle	Schweregrad	QdE	Host IP	Host Name	Ort	Erstellt ▾
TWiki < 6.1.0 XSS Vulnerability	4.3 (Mittel)	80 %	192.168.123.52	gos-qa-metasploitable.support.greenbone....	80/tcp	Fr., 12. Juli 2019 11:38 UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (Hoch)	80 %	192.168.123.52	gos-qa-metasploitable.support.greenbone....	80/tcp	Fr., 12. Juli 2019 11:38 UTC
Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability	5.0 (Mittel)	80 %	192.168.123.52	gos-qa-metasploitable.support.greenbone....	80/tcp	Fr., 12. Juli 2019 11:38 UTC
Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability	6.5 (Mittel)	80 %	192.168.123.52	gos-qa-metasploitable.support.greenbone....	80/tcp	Fr., 12. Juli 2019 11:38 UTC
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Mittel)	80 %	192.168.123.52	gos-qa-metasploitable.support.greenbone....	80/tcp	Fr., 12. Juli 2019 11:38 UTC
Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability	5.0 (Mittel)	80 %	192.168.123.52	gos-qa-metasploitable.support.greenbone....	80/tcp	Fr., 12. Juli 2019 11:37 UTC
Tiki Wiki CMS Groupware XSS Vulnerability	3.5 (Niedrig)	80 %	192.168.123.52	gos-qa-metasploitable.support.greenbone....	80/tcp	Fr., 12. Juli 2019 11:37 UTC

Abb. 10.21: Ergebnisse eines CVE-Scans

Ergebnis: OS End Of Life Detection

Informationen | Benutzer-Tags (0)

Schwachstelle

Name OS End Of Life Detection
Schweregrad 10.0 (Hoch)
QdE 80 %
Host 192.168.123.1
Ort general/tcp

Zusammenfassung

OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should not be used anymore.

Erkennungsergebnis

The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:debian:debian_linux:7
Installed version, build or SP: 7
EOL date: 2018-05-31
EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table

Ergebnis zur Produkterkennung

Produkt cpe:/o:debian:debian_linux:7
Methode OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)
Log Details der Produkterkennung anzeigen

Erkennungsmethode

Details: OS End Of Life Detection OID: 1.3.6.1.4.1.25623.1.0.103674
Genutzte Version: 2018-02-22T15:42:48Z

Abb. 10.22: Details der gefundenen CVE

10.5 Container-Aufgaben nutzen

10.5.1 Eine Container-Aufgabe erstellen

Eine Container-Aufgabe kann zum Importieren und Bereitstellen von Berichten, die auf anderen Appliances erstellt wurden, genutzt werden.

Eine Container-Aufgabe kann wie folgt erstellt werden:

1. *Scans* > *Aufgaben* in der Menüleiste wählen.
2. Neue Container-Aufgabe durch Bewegen der Maus über und Klicken auf *Neue Container-Aufgabe* erstellen.
3. Namen der Container-Aufgabe in das Eingabefeld *Name* eingeben (siehe Abb. 10.23).

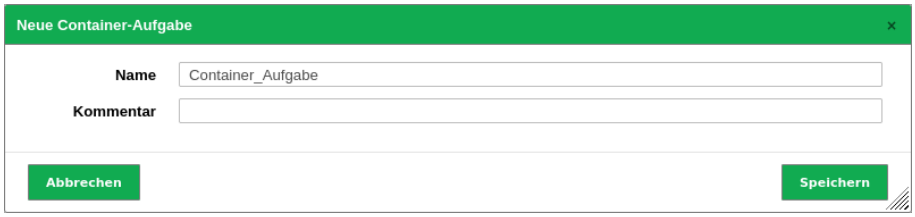


Abb. 10.23: Erstellen einer Container-Aufgabe

4. Auf *Speichern* klicken.
5. In der Zeile der Container-Aufgabe auf klicken, um einen Bericht zur Container-Aufgabe hinzuzufügen.
6. Auf *Browse. . .* klicken und die XML-Datei des Berichts wählen (siehe Abb. 10.24).

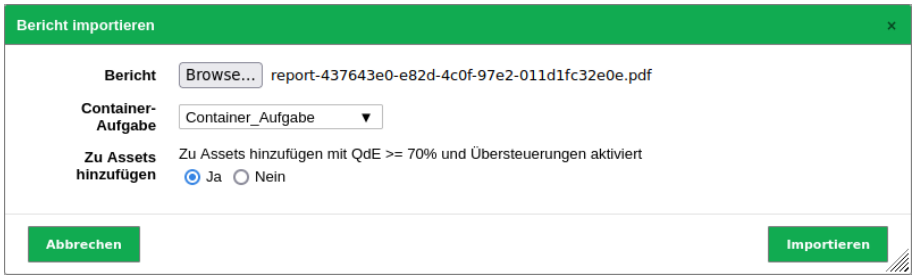


Abb. 10.24: Hinzufügen eines Berichts zu einer Container-Aufgabe

7. Radiobutton *Ja* wählen, um den Bericht zu den Assets hinzuzufügen (siehe Kapitel *13* (Seite 349)).
8. Auf *Importieren* klicken.

10.5.2 Container-Aufgaben verwalten

Listenseite

Alle vorhandenen Container-Aufgaben können angezeigt werden, indem *Scans* > *Aufgaben* in der Menüleiste gewählt wird.

Bemerkung: Container-Aufgaben sind durch Container in der Spalte *Status* gekennzeichnet.

Für alle Container-Aufgaben sind die folgenden Aktionen verfügbar:

- Berichte in die Container-Aufgabe importieren.
- Die Container-Aufgabe in den Papierkorb verschieben.
- Die Container-Aufgabe bearbeiten.
- Die Container-Aufgabe klonen.
- Die Container-Aufgabe als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Aufgaben können mehrere Aufgaben zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Aufgaben in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Container-Aufgabe werden Details der Container-Aufgabe angezeigt. Durch Klicken auf wird die Detailseite der Container-Aufgabe geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Container-Aufgabe.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Container-Aufgaben anzeigen.
- Eine neue Aufgabe (siehe Kapitel *10.2.2* (Seite 218)) oder Container-Aufgabe (siehe Kapitel *10.5* (Seite 252)) erstellen.
- Die Container-Aufgabe klonen.
- Die Container-Aufgabe bearbeiten.
- Die Container-Aufgabe in den Papierkorb verschieben.
- Die Container-Aufgabe als XML-Datei exportieren.
- Berichte in die Container-Aufgabe importieren.
- Den letzten Bericht der Container-Aufgabe oder alle Berichte der Container-Aufgabe anzeigen.
- Die Ergebnisse der Container-Aufgabe anzeigen.
- Die Notizen der Container-Aufgabe anzeigen.
- Die Übersteuerungen der Container-Aufgabe anzeigen.

10.6 Ziele verwalten

Listenseite

Alle vorhandenen Ziele können angezeigt werden, indem *Konfiguration > Ziele* in der Menüleiste gewählt wird.

Für alle Ziele werden die folgenden Informationen angezeigt:

Name Name des Ziels.

Hosts Hosts, die gescannt werden, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *10.2.2* (Seite 218)).

IPs Anzahl gescannter Hosts.

Portliste Portliste, die genutzt wird, falls das Ziel für einen Scan genutzt wird (siehe Kapitel *10.2.2* (Seite 218)).

Anmeldedaten Anmeldedaten, die für das Ziel konfiguriert wurden.

Für alle Ziele sind die folgenden Aktionen verfügbar:

- Das Ziel in den Papierkorb verschieben. Nur Ziele, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Das Ziel bearbeiten.
- Das Ziel klonen.
- Das Ziel als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Zielen können mehrere Ziele zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Ziele in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen eines Ziels werden Details des Ziels angezeigt. Durch Klicken auf wird die Detailseite des Ziels geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das Ziel.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Zielen anzeigen.
- Ein neues Ziel erstellen (siehe Kapitel *10.2.1* (Seite 214)).
- Das Ziel klonen.
- Das Ziel bearbeiten.
- Das Ziel in den Papierkorb verschieben. Nur Ziele, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Das Ziel als XML-Datei exportieren.

10.7 Portlisten erstellen und verwalten

Falls Anwendungen auf unüblichen Ports laufen und mit der Appliance überwacht und geprüft werden sollen, sollten die standardmäßigen Portlisten angepasst werden. Falls nötig, kann eine individuelle Portliste, die die gewünschten Ports enthält, erstellt werden.

Alle Standardportlisten von Greenbone sind Datenobjekte, die über den Feed verteilt werden. Sie werden mit jedem Feed-Update heruntergeladen und aktualisiert.

Falls keine Standardportlisten verfügbar sind, ist möglicherweise ein Feed-Update nötig oder der Feed Import Owner muss festgelegt werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Standardportlisten können nicht bearbeitet werden. Außerdem können sie nur temporär vom Feed Import Owner oder von einem Super-Administrator gelöscht werden. Während des nächsten Feed-Updates werden sie wieder heruntergeladen.

Bemerkung: Um eine Standardportliste dauerhaft zu löschen, muss der Feed Import Owner sie löschen. Anschließend muss der Feed Import Owner auf *(Unset)* geändert werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Zusätzlich zu den Standardportlisten können benutzerdefinierte Portlisten erstellt (siehe Kapitel *10.7.1* (Seite 255)) oder importiert (siehe Kapitel *10.7.2* (Seite 256)) werden.

10.7.1 Eine Portliste erstellen

Eine neue Portliste kann wie folgt erstellt werden:

1. *Konfiguration* > *Portlisten* in der Menüleiste wählen.
2. Neue Portliste durch Klicken auf ☆ erstellen.
3. Portliste definieren (siehe Abb. 10.25).

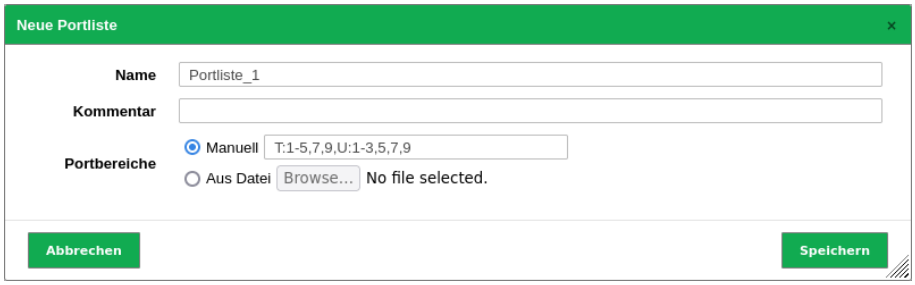


Abb. 10.25: Erstellen einer neuen Portliste

4. Auf *Speichern* klicken.

Die folgenden Details der Portliste können festgelegt werden:

Name Festlegung des Namens. Der Name kann frei gewählt werden.

Kommentar Ein optionaler Kommentar kann zusätzliche Informationen enthalten.

Portbereiche Manuelle Eingabe des Portbereichs oder Importieren einer Liste von Portbereichen. Falls sie manuell eingegeben werden, werden die Portbereiche durch Kommas getrennt. Falls eine Datei importiert wird, können die Einträge durch Kommas oder durch Zeilenumbrüche getrennt werden. Die Datei muss die ASCII-Zeichenkodierung verwenden.

Jeder Wert in der Liste kann ein einzelner Port (z. B. `7`) oder ein Portbereich (z. B. `9-11`) sein. Diese Optionen können gemischt werden (z. B. `5, 7, 9-11, 13`).

Einem Eintrag in der Liste kann eine Protokollbezeichnung vorangestellt sein (`T:` für TCP, `U:` für UDP), z. B. `T:1-3, U:7, 9-11` (TCP-Ports 1, 2 und 3, UDP-Ports 7, 9, 10 und 11). Falls keine Bezeichnung angegeben ist, wird TCP angenommen.

10.7.2 Eine Portliste importieren

Eine Portliste kann wie folgt importiert werden:

1. *Konfiguration* > *Portlisten* in der Menüleiste wählen.
2. Auf klicken.
3. Auf *Browse...* klicken und die XML-Datei der Portliste wählen.
4. Auf *Importieren* klicken.

   → Die importierte Portliste wird auf der Seite *Portlisten* angezeigt.

10.7.3 Portlisten verwalten

Listenseite

Alle vorhandenen Portlisten können angezeigt werden, indem *Konfiguration* > *Portlisten* in der Menüleiste gewählt wird.

Für alle Portlisten werden die folgenden Informationen angezeigt:

Name Name der Portliste.

Portanzahlen – Summe Gesamte Anzahl an Ports in der Portliste.

Portanzahlen – TCP Anzahl an TCP-Ports in der Portliste.

Portanzahlen – UDP Anzahl an UDP-Ports in der Portliste.

Für alle Portlisten sind die folgenden Aktionen verfügbar:

- Die Portliste in den Papierkorb verschieben. Nur Portlisten, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden. Solange die Portliste nicht aus dem Papierkorb gelöscht wird, wird sie beim nächsten Feed-Update nicht neu heruntergeladen.
- Die Portliste bearbeiten. Nur selbst erstellte Portlisten, die aktuell nicht genutzt werden, können bearbeitet werden.
- Die Portliste klonen.
- Die Portliste als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Portlisten können mehrere Portlisten zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Portlisten in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Portliste werden Details der Portliste angezeigt. Durch Klicken auf wird die Detailseite der Portliste geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Portliste.

Portbereiche Alle Portbereiche in dieser Portliste. Der erste und letzte Port des Bereichs sowie die Protokollbezeichnung werden angezeigt.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Portlisten anzeigen.
- Eine neue Portliste erstellen (siehe Kapitel *10.7.1* (Seite 255)).
- Die Portliste klonen.
- Die Portliste bearbeiten. Nur selbst erstellte Portlisten, die aktuell nicht genutzt werden, können bearbeitet werden.
- Die Portliste in den Papierkorb verschieben. Nur Portlisten, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden. Solange die Portliste nicht aus dem Papierkorb gelöscht wird, wird sie beim nächsten Feed-Update nicht neu heruntergeladen.
- Die Portliste als XML-Datei exportieren.

10.8 Aufgaben verwalten

Listenseite

Alle vorhandenen Aufgaben können angezeigt werden, indem *Scans* > *Aufgaben* in der Menüleiste gewählt wird.

Abb. 10.26: Seite *Aufgaben* mit allen vorhandenen Aufgaben

Für alle Aufgaben werden die folgenden Informationen angezeigt:

Name Name der Aufgabe. Die folgenden Icons könnten angezeigt werden:

Die Aufgabe ist als änderbar gekennzeichnet. Scan-Ziel(e), Scanner und Scan-Konfiguration der Aufgabe können bearbeitet werden, auch wenn bereits Berichte erstellt wurden.

Die Aufgabe ist für die Durchführung auf einem Remote-Scanner konfiguriert (siehe Kapitel *16* (Seite 380)).

Die Aufgabe ist für einen oder mehrere andere Benutzer sichtbar.

Die Aufgabe gehört einem anderen Benutzer.

Status Aktueller Status der Aufgabe. Die folgenden Statusbalken sind möglich:

Neu Es gibt keine Ausführungen/Berichte für die Aufgabe.

Angefragt Die Aufgabe wurde gerade gestartet. Die Appliance bereitet den Scan vor. Aufgaben mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

In Warteschlange Die Aufgabe wurde zur Warteschlange hinzugefügt. In einigen Fällen kann sie in der Warteschlange bleiben. Weitere Informationen befinden sich in Kapitel *17.3* (Seite 393).

Die Aufgabe wird gerade ausgeführt. Die Prozentangabe basiert auf der Anzahl ausgeführter VTs auf den gewählten Hosts. Aus diesem Grund hängt der Wert nicht zwingend mit der bereits verstrichenen Zeit zusammen.

Der Scanvorgang bzw. der Upload in die Container-Aufgabe ist abgeschlossen und die Appliance verarbeitet Daten. Aufgaben mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Die Aufgabe wurde erfolgreich abgeschlossen.

Die Aufgabe wurde vor Kurzem aufgefordert, zu stoppen. Die Scanmaschine hat noch nicht auf die Anfrage reagiert. Aufgaben mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Die Aufgabe wurde gestoppt. Der neueste Bericht ist möglicherweise noch nicht komplett. Andere Gründe für diesen Status können der Reboot der Appliance oder ein Stromausfall sein. Nach dem Neustart des Scanners wird die Aufgabe automatisch fortgesetzt.

Die Aufgabe wurde gerade fortgesetzt. Die Appliance bereitet den Scan vor. Aufgaben mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Beim Fortsetzen eines Scans werden alle nicht abgeschlossenen Hosts komplett aufs Neue gescannt. Die Daten der bereits vollständig gescannten Hosts bleiben erhalten.

Die Aufgabe wurde gelöscht. Der tatsächliche Löschvorgang kann einige Zeit in Anspruch nehmen, da Berichte ebenfalls gelöscht werden müssen. Aufgaben mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Ein Fehler ist aufgetreten und die Aufgabe wurde unterbrochen. Der neueste Bericht ist möglicherweise noch nicht komplett oder fehlt vollständig.

Die Aufgabe ist eine Container-Aufgabe.

Der Bericht wird gerade in die Container-Aufgabe hochgeladen.

Berichte Anzahl der Berichte für die Aufgabe. Durch Klicken auf die Anzahl der Berichte wird die Seite *Berichte* geöffnet. Ein Filter ist angewendet, um nur die Berichte für die gewählte Aufgabe anzuzeigen.

Letzter Bericht Datum und Zeit des neuesten Berichts. Durch Klicken auf die Angabe wird die Detailseite des neuesten Berichts geöffnet.

Schweregrad Höchster Schweregrad, der durch den Scan gefunden wurde.

Trend Änderung der Schwachstellen zwischen dem neuesten und dem zweitneuesten Bericht (siehe Kapitel *11.5* (Seite 307)).

Für alle Aufgaben sind die folgenden Aktionen verfügbar:

- ▷ Die Aufgabe starten. Nur Aufgaben, die aktuell nicht ausgeführt werden, können gestartet werden.
- □ Die aktuell ausgeführte Aufgabe stoppen. Alle gefundenen Ergebnisse werden in der Datenbank gespeichert.
- ◷ Die Details des zugewiesenen Zeitplans anzeigen (nur für Aufgaben mit Zeitplan verfügbar, siehe Kapitel *10.10* (Seite 272)).
- ⏭ Die gestoppte Aufgabe fortsetzen. Alle nicht abgeschlossenen Hosts werden komplett aufs Neue gescannt. Die Daten der bereits vollständig gescannten Hosts bleiben erhalten.
- 🗑 Die Aufgabe in den Papierkorb verschieben.
- ✎ Die Aufgabe bearbeiten.
- Die Aufgabe klonen.
- Die Aufgabe als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Aufgaben können mehrere Aufgaben zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Aufgaben in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Aufgabe werden Details der Aufgabe angezeigt. Durch Klicken auf wird die Detailseite der Aufgabe geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Aufgabe.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Aufgaben anzeigen.
- Eine neue Aufgabe (siehe Kapitel *10.2.2* (Seite 218)) oder Container-Aufgabe (siehe Kapitel *10.5* (Seite 252)) erstellen.
- Die Aufgabe klonen.
- Die Aufgabe bearbeiten.
- Die Aufgabe in den Papierkorb verschieben.
- Die Aufgabe als XML-Datei exportieren.
- Die Aufgabe starten. Nur Aufgaben, die aktuell nicht ausgeführt werden, können gestartet werden.
- Die aktuell ausgeführte Aufgabe stoppen. Alle gefundenen Ergebnisse werden in der Datenbank gespeichert.
- Die gestoppte Aufgabe fortsetzen. Alle nicht abgeschlossenen Hosts werden komplett aufs Neue gescannt. Die Daten der bereits vollständig gescannten Hosts bleiben erhalten.
- Den letzten Bericht der Aufgabe oder alle Berichte der Aufgabe anzeigen.
- Die Ergebnisse der Aufgabe anzeigen.
- Die Notizen der Aufgabe anzeigen.
- Die Übersteuerungen der Aufgabe anzeigen.

10.8.1 Berechtigungen für eine Aufgabe erteilen

Auf der Detailseite einer Aufgabe können die Berechtigungen für die Aufgabe wie folgt verwaltet werden:

Bemerkung: Standardmäßig können normale Nutzer keine Berechtigungen für andere Nutzer erstellen, da sie keinen Zugriff auf die Nutzerdatenbank haben. Um in der Lage zu sein, Berechtigungen für andere Nutzer zu erstellen, benötigt ein Nutzer die globale und die spezifische *get_users*-Berechtigung (siehe Kapitel *9.4.3* (Seite 200)).

---

1. *Scans* > *Aufgaben* in der Menüleiste wählen.
2. Durch Klicken auf den Namen einer Aufgabe werden Details der Aufgabe angezeigt. Durch Klicken auf 🔍 wird die Detailseite der Aufgabe geöffnet.
3. Auf den Register *Berechtigungen* klicken.
4. Im Abschnitt *Berechtigungen* auf 🆕 klicken.
5. Berechtigungsart in der Drop-down-Liste *Gewähre* wählen.
6. Radiobutton *Benutzer*, *Gruppe* oder *Rolle* wählen und Benutzer/Gruppe/Rolle in der entsprechenden Drop-down-Liste wählen (siehe Abb. 10.27).

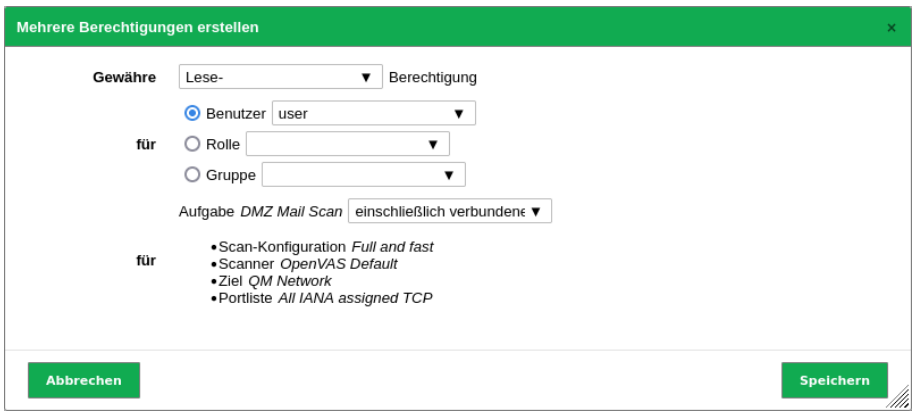


Abb. 10.27: Erstellen einer neuen Berechtigung

7. Auf *Speichern* klicken.

   → Die Berechtigung wird auf der Detailseite der Aufgabe angezeigt (siehe Abb. 10.28).

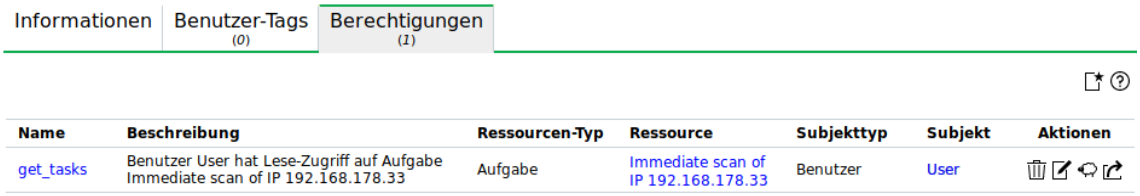


Abb. 10.28: Berechtigung auf der Detailseite der Aufgabe

Nach dem Einloggen kann der Benutzer die Aufgaben sehen und auf die entsprechenden Berichte zugreifen.

10.9 Scan-Konfigurationen konfigurieren und verwalten

Die Appliance bietet einige vordefinierte Scan-Konfigurationen. Diese können angepasst werden und neue Scan-Konfigurationen können erstellt werden.

10.9.1 Standard-Scan-Konfigurationen

Alle Standard-Scan-Konfigurationen von Greenbone sind Datenobjekte, die über den Feed verteilt werden. Sie werden mit jedem Feed-Update heruntergeladen und aktualisiert.

Falls keine Standard-Scan-Konfigurationen verfügbar sind, ist möglicherweise ein Feed-Update nötig oder der Feed Import Owner muss festgelegt werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Standard-Scan-Konfigurationen können nicht bearbeitet werden. Außerdem können sie nur temporär vom Feed Import Owner oder von einem Super-Administrator gelöscht werden. Während des nächsten Feed-Updates werden sie wieder heruntergeladen.

Bemerkung: Um eine Standard-Scan-Konfiguration dauerhaft zu löschen, muss der Feed Import Owner sie löschen. Anschließend muss der Feed Import Owner auf *(Unset)* geändert werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Bemerkung: Zusätzlich zu den Standard-Scan-Konfigurationen können benutzerdefinierte Scan-Konfigurationen erstellt (siehe Kapitel *10.9.2* (Seite 263)) oder importiert (siehe Kapitel *10.9.3* (Seite 266)) werden.

Die folgenden Scan-Konfigurationen sind standardmäßig verfügbar:

Empty Diese Scan-Konfiguration ist ein leeres Template und enthält keine VTs. Sie kann geklont werden und damit als Vorlage für komplett individuell erstellte Scan-Konfigurationen dienen.

Die VT-Familien sind statisch, das heißt neue VTs der gewählten VT-Familien werden nicht automatisch hinzugefügt und berücksichtigt.

Base Diese Scan-Konfiguration nutzt nur VTs, die Informationen über das Zielsystem sammeln. Dabei werden keine Schwachstellen erkannt. Sie kann geklont werden und damit als Vorlage für komplett individuell erstellte Scan-Konfigurationen dienen.

Es wird der Portscanner *Ping Host* genutzt, welcher erkennt, ob ein Host erreichbar ist. Außerdem werden Informationen über das Betriebssystem gesammelt.

Die VT-Familien sind statisch, das heißt neue VTs der gewählten VT-Familien werden nicht automatisch hinzugefügt und berücksichtigt.

Discovery Diese Scan-Konfiguration nutzt nur VTs, die Informationen über das Zielsystem sammeln. Dabei werden keine Schwachstellen erkannt.

Zu den gesammelten Informationen gehören unter anderem Informationen über offene Ports, genutzte Hardware, Firewalls, genutzte Dienste, installierte Software und Zertifikate. Das System wird komplett inventarisiert.

Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Host Discovery Diese Scan-Konfiguration wird nur zum Erkennen der Zielsysteme genutzt. Dabei werden keine Schwachstellen erkannt.

Es wird der Portscanner *Ping Host* genutzt, welcher erkennt, ob ein Host erreichbar ist.

Die VT-Familien sind statisch, das heißt neue VTs der gewählten VT-Familien werden nicht automatisch hinzugefügt und berücksichtigt.

System Discovery Diese Scan-Konfiguration wird nur zum Erkennen der Zielsysteme, der Betriebssysteme und der verwendeten Hardware genutzt. Dabei werden keine Schwachstellen erkannt.

Es wird der Portscanner *Ping Host* genutzt, welcher erkennt, ob ein Host erreichbar ist.

Die VT-Familien sind statisch, das heißt neue VTs der gewählten VT-Familien werden nicht automatisch hinzugefügt und berücksichtigt.

Full and fast Für viele Umgebungen ist das für den Anfang die beste Option.

Diese Scan-Konfiguration basiert auf den Informationen, die in einem vorherigen Portscan gesammelt wurden und nutzt fast alle VTs. Nur VTs, die das Zielsystem nicht beschädigen, werden genutzt. VTs sind bestmöglich optimiert, um die potentielle Falsch-Positiv-Rate besonders niedrig zu halten. Die anderen „Full“-Konfigurationen bieten nur in selten Fällen einen Mehrwert bei höherem Aufwand.

Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Full and fast ultimate Diese Scan-Konfiguration erweitert die Scan-Konfiguration *Full and fast* mit VTs, die Dienst- oder Systemstörungen oder sogar Abstürze hervorrufen könnten.

Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Diese Scan-Konfiguration ist je nach Umgebungsbedingungen möglicherweise nicht immer absolut zuverlässig, was sich in einer erhöhten Falsch-positiv-Rate zeigen kann. Die Eingrenzung der vermuteten falsch-positiven Sonderfälle kann eine manuelle Analyse und das Einrichten von Übersteuerungen erfordern (siehe Kapitel *11.8* (Seite 315)).

Full and very deep Diese Scan-Konfiguration basiert auf der Scan-Konfiguration *Full and fast*, allerdings haben die Ergebnisse des Portscans oder der Anwendungs-/Diensterkennung keinen Einfluss auf die Auswahl der VTs. Deshalb werden VTs genutzt, die auf einen Timeout warten oder die nach Schwachstellen einer Anwendung/eines Diensts suchen, die vorher nicht entdeckt wurden. Ein Scan mit dieser Scan-Konfiguration ist sehr langsam.

Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Full and very deep ultimate Diese Scan-Konfiguration erweitert die Scan-Konfiguration *Full and very deep* mit gefährlichen VTs, die Dienst- und Systemstörungen hervorrufen können. Ein Scan mit dieser Scan-Konfiguration ist sehr langsam.

Die VT-Familien sind dynamisch, das heißt neue VTs der gewählten VT-Familien werden automatisch hinzugefügt und berücksichtigt.

Diese Scan-Konfiguration ist je nach Umgebungsbedingungen möglicherweise nicht immer absolut zuverlässig, was sich in einer erhöhten Falsch-positiv-Rate zeigen kann. Die Eingrenzung der vermuteten falsch-positiven Sonderfälle kann eine manuelle Analyse und das Einrichten von Übersteuerungen erfordern (siehe Kapitel *11.8* (Seite 315)).

10.9.2 Eine Scan-Konfiguration erstellen

Bemerkung: Jede benutzerdefinierte Scan-Konfiguration, bei der die Scanner-Vorgabe *safe_checks* auf *no* gesetzt ist (siehe Kapitel *10.9.4.1* (Seite 267)), ist je nach Umgebungsbedingungen möglicherweise nicht immer absolut zuverlässig, was sich in einer erhöhten Falsch-positiv-Rate zeigen kann. Die Eingrenzung der vermuteten falsch-positiven Sonderfälle kann eine manuelle Analyse und das Einrichten von Übersteuerungen erfordern (siehe Kapitel *11.8* (Seite 315)).

Eine neue Scan-Konfiguration kann wie folgt erstellt werden:

1. *Konfiguration* > *Scan-Konfigurationen* in der Menüleiste wählen.
2. Neue Scan-Konfiguration durch Klicken auf erstellen.

   Bemerkung: Alternativ kann eine Scan-Konfiguration importiert werden (siehe Kapitel *10.9.3* (Seite 266)).

3. Namen der Scan-Konfiguration in das Eingabefeld *Name* eingeben (siehe Abb. 10.29).
4. Radiobutton der Basis, die genutzt werden soll, wählen.

   Es kann zwischen *Base with a minimum set of NVTs*, *Empty, static and fast*, *Full and fast* und einer bereits erstellten Scan-Konfiguration gewählt werden.

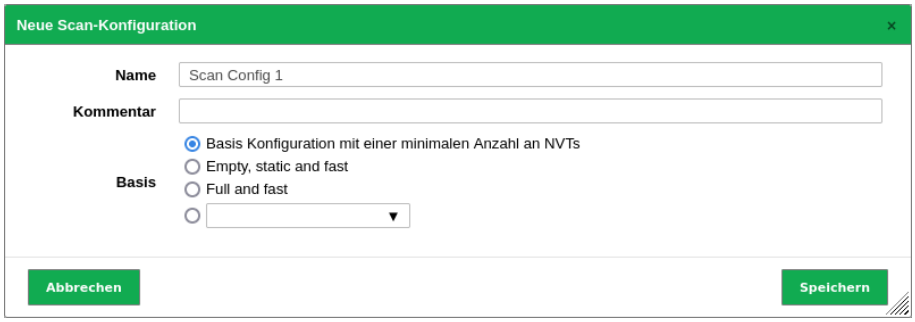


Abb. 10.29: Erstellen einer neuen Scan-Konfiguration

5. Auf *Speichern* klicken.

   → Die Scan-Konfiguration wird erstellt und auf der Seite *Scan-Konfigurationen* angezeigt.

6. In der Zeile der Scan-Konfiguration auf klicken.
7. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* den Radiobutton wählen, falls neue VT-Familien automatisch hinzugefügt und aktiviert werden sollen (siehe Abb. 10.30).
8. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* die Checkboxen *Alle NVTs auswählen* aktivieren, falls alle VTs einer Familie aktiviert werden sollen.

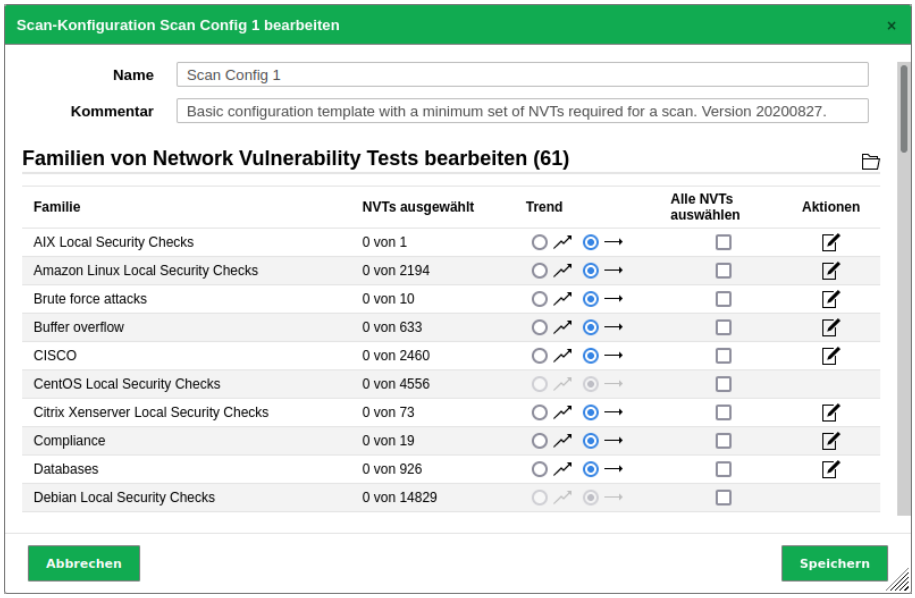


Abb. 10.30: Bearbeiten der neuen Scan-Konfiguration

9. Für eine VT-Familie auf klicken, um sie zu bearbeiten (siehe Abb. 10.31).

Bemerkung: Die folgenden VT-Familien können nicht bearbeitet werden:

- AIX Local Security Checks
- AlmaLinux Local Security Checks
- Amazon Linux Local Security Checks
- CentOS Local Security Checks
- Debian Local Security Checks
- Fedora Local Security Checks
- FreeBSD Local Security Checks
- Gentoo Local Security Checks
- HP-UX Local Security Checks
- Huawei EulerOS Local Security Checks
- Mageia Linux Local Security Checks
- Mandrake Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- Rocky Linux Local Security Checks
- Slackware Local Security Checks
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

Mehr Informationen befinden sich in Kapitel *6.5.1* (Seite 61).

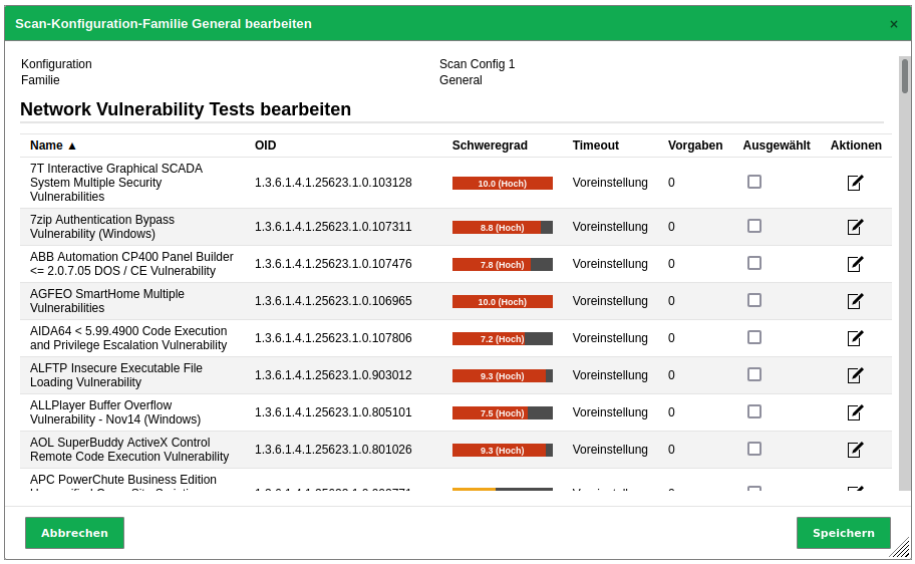


Abb. 10.31: Eine VT-Familie bearbeiten

10. Die Checkboxen der VTs, die aktiviert werden sollen, in der Spalte *Ausgewählt* aktivieren.

Bemerkung: Damit der Notus-Scanner (siehe Kapitel *6.5.1* (Seite 61)) funktioniert, muss der VT *Determine OS and list of installed packages via SSH login* (OID: 1.3.6.1.4.1.25623.1.0.50282) aktiviert sein.

11. Für einen VT auf ✎ klicken, um ihn zu bearbeiten (siehe Abb. 10.32).

Bemerkung: Falls das Bearbeiten eines VT das Hochladen einer Textdatei beinhaltet, sollte die Datei mit UTF-8 codiert sein.

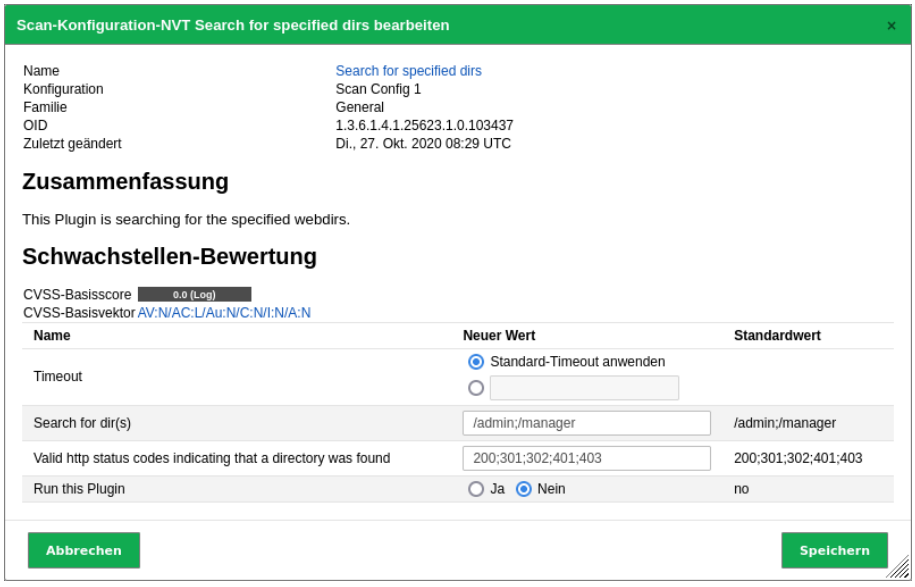


Abb. 10.32: Bearbeiten eines VTs

12. Auf *Speichern* klicken, um den VT zu speichern.
13. Auf *Speichern* klicken, um die VT-Familie zu speichern.
14. Optional: Scanner-Vorgaben bearbeiten (siehe Kapitel *10.9.4* (Seite 267)).
15. Optional: VT-Vorgaben bearbeiten (siehe Kapitel *10.9.5* (Seite 268)).
16. Auf *Speichern* klicken, um die Scan-Konfiguration zu speichern.

10.9.3 Eine Scan-Konfiguration importieren

Bemerkung: Es sollten nur Scan-Konfigurationen importiert werden, die mit der aktuell verwendeten GOS-Version erstellt wurden. Der Import von Scan-Konfigurationen aus anderen GOS-Versionen kann zu einer Fehlermeldung oder unerwartetem Verhalten führen.

Jede benutzerdefinierte Scan-Konfiguration, bei der die Scanner-Vorgabe *safe_checks* auf *no* gesetzt ist (siehe Kapitel *10.9.4.1* (Seite 267)), ist je nach Umgebungsbedingungen möglicherweise nicht immer absolut zuverlässig, was sich in einer erhöhten Falsch-positiv-Rate zeigen kann. Die Eingrenzung der vermuteten falsch-positiven Sonderfälle kann eine manuelle Analyse und das Einrichten von Übersteuerungen erfordern (siehe Kapitel *11.8* (Seite 315)).

Eine Scan-Konfiguration kann wie folgt importiert werden:

1. *Konfiguration* > *Scan-Konfigurationen* in der Menüleiste wählen.
2. Auf ↥ klicken.
3. Auf *Browse* klicken und die XML-Datei der Scan-Konfiguration wählen.
4. Auf *Importieren* klicken.

   Bemerkung: Falls der Name der importierten Scan-Konfiguration bereits vorhanden ist, wird ein Zusatz an den Namen angehängt.

   → Die importierte Scan-Konfiguration wird auf der Seite *Scan-Konfigurationen* angezeigt.
5. Schritte 6 bis 16 aus Kapitel *10.9.2* (Seite 263) durchführen, um die Scan-Konfiguration zu bearbeiten.

10.9.4 Die Scanner-Vorgaben bearbeiten

Die Scanner-Vorgaben können wie folgt bearbeitet werden:

1. *Konfiguration* > *Scan-Konfigurationen* in der Menüleiste wählen.
2. In der Zeile der Scan-Konfiguration auf klicken.
3. Im Abschnitt *Scanner-Vorgaben bearbeiten* auf klicken, um die Scanner-Vorgaben zu bearbeiten (siehe Abb. 10.33).

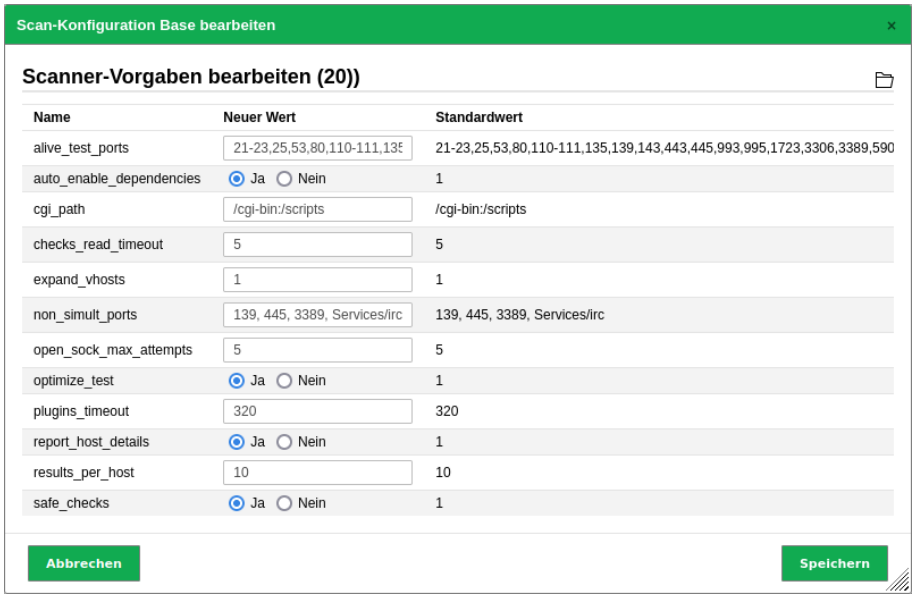


Abb. 10.33: Bearbeiten der Scanner-Vorgaben

4. Nach dem Bearbeiten der Scanner-Vorgaben auf *Speichern* klicken, um die Scan-Konfiguration zu speichern.

10.9.4.1 Beschreibung der Scanner-Vorgaben

Bemerkung: Das Dokumentieren aller Scanner-Vorgaben wäre für dieses Handbuch zu umfangreich. Nur die wichtigsten Vorgaben der Scanner werden abgedeckt.

Nicht dokumentierte Vorgaben könnten auch veraltet sein, obwohl sie noch sichtbar sind. Diese Vorgaben werden vom Scanner ignoriert und sollten nicht beachtet werden.

- *alive_test_ports*: TCP-Ports, die vom Boreas-Erreichbarkeitsscanner für die Erreichbarkeitstests verwendet werden. Diese Einstellung betrifft nur die Erreichbarkeitstest-Methoden *TCP-ACK Service Ping* und *TCP-SYN Service Ping*. Es dürfen nur gültige Ports (Portbereich 0–65535) konfiguriert werden. Wenn ein ungültiger Wert konfiguriert wird, verwendet der Boreas-Erreichbarkeitsscanner die Standard-Ports.
- *auto_enable_dependencies*: Dies legt fest, ob VTs, die von anderen VTs benötigt werden, automatisch aktiviert werden.
- *cgi_path*: Pfad, der von den VTs genutzt wird, um auf CGI-Skripte zuzugreifen.
- *checks_read_timeout*: Timeout für die Netzwerksockets während eines Scans.
- *test_alive_wait_timeout*: Timeout für den Boreas-Erreichbarkeitsscanner, um auf Antworten zu warten, nachdem das letzte Paket gesendet wurde. Zugelassen sind Werte zwischen 1 und 20.

- *test_empty_vhost*: Der Scanner scannt das Ziel auch unter Nutzung leerer vhost-Werte, zusätzlich zu den dem Ziel zugewiesenen vhost-Werten.
- *max_sysload*: Maximale Last auf der Appliance. Wenn diese Last erreicht wird, werden keine weiteren VTs gestartet, bis die Last wieder unter den angegebenen Wert sinkt.
- *min_free_mem*: Minimal verfügbarer Speicher (in MB), der auf der Appliance freigehalten werden sollte. Wenn dieses Limit erreicht wird, werden keine weiteren VTs gestartet, bis wieder ausreichend Speicher verfügbar ist.
- *non_simult_ports*: Diese Ports werden nicht gleichzeitig von VTs geprüft.
- *optimize_test*: VTs werden nur gestartet, falls bestimmte Voraussetzungen erfüllt werden (z. B. offene Ports oder erkannte Anwendungen).
- *plugins_timeout*: Maximale Laufzeit eines VTs.
- *safe_checks*: Einige VTs können Schaden am Hostsystem anrichten. Diese Einstellung deaktiviert die entsprechenden VTs.
- *scanner_plugins_timeout*: Maximale Laufzeit (in Sekunden) für alle VTs der VT-Familie *Port scanners*. Falls ein VT länger läuft, wird er abgebrochen.
- *expand_vhosts*: Die Hostliste des Ziels wird mit Werten erweitert, die durch Quellen wie Invers-Lookup-Anfragen und VT-Prüfungen für SSL/TLS-Zertifikate erhalten wurden.
- *time_between_request*: Wartezeit (in Millisekunden) zwischen zwei Aktionen wie dem Öffnen eines TCP-Sockets, dem Senden einer Anfrage durch das offene TCP-Socket und dem Schließen des TCP-Sockets.
- *timeout_retry*: Anzahl an neuen Versuchen, falls eine Socketverbindung einen Timeout hat.
- *unscanned_closed*: Dies legt fest, ob TCP-Ports, die nicht gescannt wurden, wie geschlossene Ports behandelt werden sollen.
- *unscanned_closed_udp*: Dies legt fest, ob UDP-Ports, die nicht gescannt wurden, wie geschlossene Ports behandelt werden sollen.

10.9.5 Die VT-Vorgaben bearbeiten

1. *Konfiguration* > *Scan-Konfigurationen* in der Menüleiste wählen.
2. In der Zeile der Scan-Konfiguration auf ✎ klicken.
3. Im Abschnitt *Vorgaben für Network Vulnerability Tests* auf 🗀 klicken, um die Vorgaben für jeden VT anzuzeigen.
4. In der Zeile der VT-Vorgabe auf ✎ klicken.
5. VT-Vorgabe bearbeiten.
6. Auf *Speichern* klicken, um die VT-Vorgabe zu speichern.
7. Auf *Speichern* klicken, um die Scan-Konfiguration zu speichern.

10.9.5.1 Beschreibung der VT-Vorgaben

Bemerkung: Das Dokumentieren aller VT-Vorgaben wäre für dieses Handbuch zu umfangreich. Nur die VT-Vorgaben der Portscanner Nmap und Ping Host werden abgedeckt.

Vorgaben des VT *Ping Host*

Bemerkung: Die meisten der *Ping Host*-Parameter werden in GOS 22.04 nicht mehr unterstützt, da sie mit dem neuen Boreas-Erreichbarkeitsscanner inkompatibel sind. Parameter, die hier nicht dokumentiert sind, werden nicht unterstützt und sind möglicherweise nicht funktionsfähig.

Der VT *Ping Host* in der VT-Familie *Port scanners* enthält den folgenden Konfigurationsparameter:

- *Report about reachable Hosts*: Dies legt fest, ob ein Host, der von diesem VT gefunden wurde, gelistet werden soll.

Vorgaben des VT *Nmap (NASL wrapper)*

Die folgenden Optionen des VT *Nmap (NASL wrapper)* der VT-Familie *Port scanners* werden direkt in Optionen für die Ausführung des Nmap-Befehls übersetzt. Zusätzliche Informationen können in der Dokumentation für Nmap[28] gefunden werden.

- *Do not randomize the order in which ports are scanned*: Nmap scannt die Ports in aufsteigender Reihenfolge.
- *Do not scan targets not in the file*: Siehe *File containing grepable results*.
- *Fragment IP packets*: Nmap teilt die Pakete für die Angriffe. Dies erlaubt es, einfache Paketfilter zu umgehen.
- *Identify the remote OS*: Nmap versucht, das Betriebssystem zu identifizieren.
- *RPC port scan*: Nmap prüft das System auf Sun-RPC-Ports.
- *Run dangerous ports even if safe checks are set*: UDP- und RPC-Scans können Probleme verursachen und sind normalerweise durch die Einstellung *safe_checks* deaktiviert. Mit dieser Einstellung können sie trotzdem aktiviert werden.
- *Service scan*: Nmap versucht, Dienste zu identifizieren.
- *Use hidden option to identify the remote OS*: Nmap führt die Identifikationen aggressiver durch.
- *Data length*: Nmap fügt zufällige Daten bestimmter Länger zum Paket hinzu.
- *Host Timeout*: Host-Timeout.
- *Initial RTT timeout*: Ursprünglicher Timeout der Paketumlaufzeit. Nmap kann diesen Timeout, abhängig von der Ergebnissen, anpassen.
- *Max RTT timeout*: Maximale Paketumlaufzeit.
- *Min RTT timeout*: Minimale Paketumlaufzeit.
- *Max Retries*: Maximale Anzahl an neuen Versuchen.
- *Maximum wait between probes*: Dies steuert die Geschwindigkeit des Scans.

[28] https://nmap.org/docs.html

- *Minimum wait between probes*: Dies steuert die Geschwindigkeit des Scans.
- *Ports scanned in parallel (max)*: Dies legt fest, wie viele Ports maximal gleichzeitig gescannt werden sollten.
- *Ports scanned in parallel (min)*: Dies legt fest, wie viele Ports minimal gleichzeitig gescannt werden sollten.
- *Source port*: Dies ist der Quellport. Dies ist von Interesse, wenn durch eine Firewall gescannt wird, falls Verbindungen von einem bestimmten Port allgemein erlaubt sind.
- *File containing grepable results*: Ermöglicht die Festlegung einer Datei, die Zeilen in der Form `Host: IP address` enthält. Falls die Option *Do not scan targets not in the file* zur gleichen Zeit aktiviert ist, werden nur Systeme, die in dieser Datei enthalten sind, gescannt.
- *TCP scanning technique*: Tatsächliche Scantechnik.
- *Timing policy*: Statt die Zeitwerte einzeln zu ändern, kann auch die Timing-Richtlinie verändert werden.

Die Timing-Richtlinie nutzt folgende Werte:

	Paranoid	Sneaky	Polite	Normal	Aggressive	Insane
initial_rtt_timeout	5 min	15 s	1 s	1 s	500 ms	250 ms
min_rtt_timeout	100 ms	100 ms	100 ms	100 ms	100 ms	50 ms
max_rtt_timeout	10 s	10 s	10 s	10 s	1250 ms	300 ms
max_parallelism	seriell	seriell	seriell	parallel	parallel	parallel
scan_delay	5 min	15 s	400 ms	0 s	0 s	0 s
max_scan_delay	1 s	1 s	1 s	1 s	10 ms	5 ms

10.9.6 Scan-Konfigurationen verwalten

Listenseite

Alle vorhandenen Scan-Konfigurationen können angezeigt werden, indem *Konfiguration > Scan-Konfigurationen* in der Menüleiste gewählt wird (siehe Abb. 10.34).

Für alle Scan-Konfigurationen werden die folgenden Informationen angezeigt:

Name Name der Scan-Konfiguration.

Typ Art der Scan-Konfiguration.

Familie – Summe Anzahl der aktivierten VT-Familien für die Scan-Konfiguration.

Familie – Trend Trend der VT-Familien

↗ Nach einem Feed-Update werden neue VT-Familien automatisch hinzugefügt und aktiviert. Dies stellt sicher, dass neue VTs sofort und ohne durch den Administrator notwendige Handlungen verfügbar sind.

→ Nach einem Feed-Update werden neue VT-Familien nicht automatisch hinzugefügt.

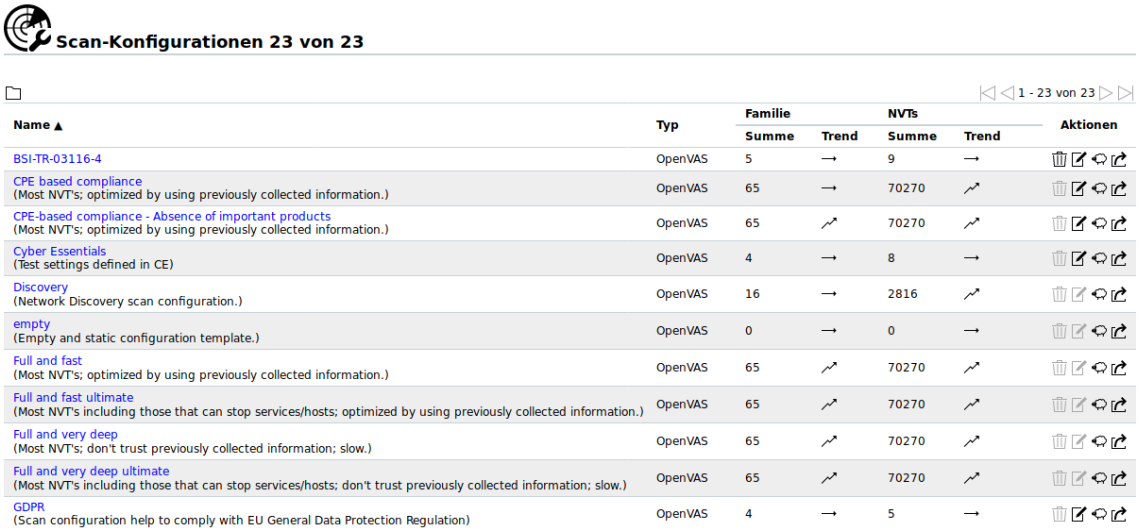
NVTs – Summe Anzahl der aktivierten VTs für die Scan-Konfiguration.

NVTs – Trend Trend der VTs.

↗ Nach einem Feed-Update werden neue VTs der aktivierten VT-Familien automatisch hinzugefügt und aktiviert. Dies stellt sicher, dass neue VTs sofort und ohne durch den Administrator notwendige Handlungen verfügbar sind.

→ Nach einem Feed-Update werden neue VTs nicht automatisch hinzugefügt.

Bemerkung: Greenbone veröffentlich regelmäßig neue VTs. Neue VT-Familien können ebenfalls durch den Greenbone Enterprise Feed hinzugefügt werden.



Scan-Konfigurationen 23 von 23

1 - 23 von 23

Name ▲	Typ	Familie		NVTs		Aktionen
		Summe	Trend	Summe	Trend	
BSI-TR-03116-4	OpenVAS	5	→	9	→	
CPE based compliance (Most NVT's; optimized by using previously collected information.)	OpenVAS	65	→	70270	↗	
CPE-based compliance - Absence of important products (Most NVT's; optimized by using previously collected information.)	OpenVAS	65	↗	70270	↗	
Cyber Essentials (Test settings defined in CE)	OpenVAS	4	→	8	→	
Discovery (Network Discovery scan configuration.)	OpenVAS	16	→	2816	↗	
empty (Empty and static configuration template.)	OpenVAS	0	→	0	→	
Full and fast (Most NVT's; optimized by using previously collected information.)	OpenVAS	65	↗	70270	↗	
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	OpenVAS	65	↗	70270	↗	
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	OpenVAS	65	↗	70270	↗	
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	OpenVAS	65	↗	70270	↗	
GDPR (Scan configuration help to comply with EU General Data Protection Regulation)	OpenVAS	4	→	5	→	

Abb. 10.34: Seite *Scan-Konfigurationen* mit allen verfügbaren Scan-Konfigurationen

Für alle Scan-Konfigurationen sind die folgenden Aktionen verfügbar:

- Die Scan-Konfiguration in den Papierkorb verschieben. Nur Scan-Konfigurationen, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden. Solange die Scan-Konfiguration nicht aus dem Papierkorb gelöscht wird, wird sie beim nächsten Feed-Update nicht neu heruntergeladen.
- Die Scan-Konfiguration bearbeiten. Nur selbst erstellte Scan-Konfigurationen, die aktuell nicht genutzt werden, können bearbeitet werden.
- Die Scan-Konfiguration klonen.
- Die Scan-Konfiguration als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Scan-Konfigurationen können mehrere Scan-Konfigurationen zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Scan-Konfigurationen in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Scan-Konfiguration werden Details der Scan-Konfiguration angezeigt. Durch Klicken auf wird die Detailseite der Scan-Konfiguration geöffnet.

Die folgenden Register sind verfügbar:

Scanner-Vorgaben Alle Scanner-Vorgaben für die Scan-Konfiguration mit aktuellen und Standardwerten (siehe Kapitel *10.9.4.1* (Seite 267)).

NVT-Familien Alle VT-Familien für die Scan-Konfiguration mit der Anzahl aktivierter VTs und dem Trend.

NVT-Vorgaben Alle VT-Vorgaben für die Scan-Konfiguration (siehe Kapitel *10.9.5.1* (Seite 269)).

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Scan-Konfigurationen anzeigen.
- Eine neue Scan-Konfiguration erstellen (siehe Kapitel *10.9.2* (Seite 263)).
- Die Scan-Konfiguration klonen.
- Die Scan-Konfiguration bearbeiten. Nur selbst erstellte Scan-Konfigurationen, die aktuell nicht genutzt werden, können bearbeitet werden.
- Die Scan-Konfiguration in den Papierkorb verschieben. Nur Scan-Konfigurationen, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden. Solange die Scan-Konfiguration nicht aus dem Papierkorb gelöscht wird, wird sie beim nächsten Feed-Update nicht neu heruntergeladen.
- Die Scan-Konfiguration als XML-Datei exportieren.
- Eine Scan-Konfiguration importieren (siehe Kapitel *10.9.3* (Seite 266)).

10.10 Einen geplanten Scan ausführen

Für ein durchgehendes Schwachstellenmanagement ist das manuelle Ausführen von Aufgaben umständlich. Die Appliance unterstützt zur Automatisierung die Zeitplanung von Aufgaben und bezeichnet automatische Scans zu festgelegten Zeiten als Zeitpläne. Sie können einmalig oder wiederholt ausgeführt werden.

Die Appliance stellt standardmäßig keine Zeitpläne bereit.

10.10.1 Einen Zeitplan erstellen

Ein neuer Zeitplan kann wie folgt erstellt werden:

1. *Konfiguration* > *Zeitpläne* in der Menüleiste wählen.
2. Neuen Zeitplan durch Klicken auf erstellen.
3. Zeitplan definieren (siehe Abb. 10.35).
4. Auf *Speichern* klicken.

   → Der Zeitplan wird erstellt und kann beim Erstellen einer neuen Aufgabe gewählt werden (siehe Kapitel *10.2.2* (Seite 218)).

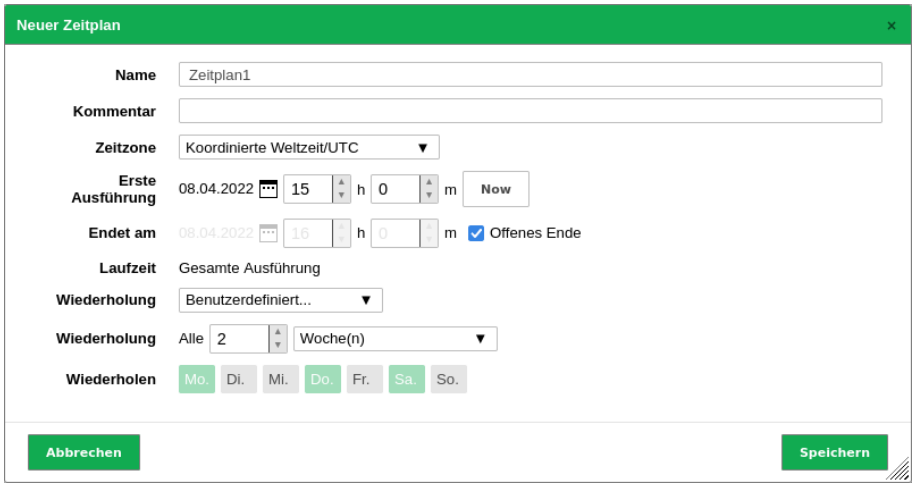


Abb. 10.35: Erstellen eines neuen Zeitplans

Die folgenden Details des Zeitplans können festgelegt werden:

Name Festlegung des Namens. Der Name kann frei gewählt werden.

Kommentar Ein optionaler Kommentar kann zusätzliche Informationen enthalten.

Zeitzone Festlegen der Zeitzone, auf die sich die Zeit bezieht. UTC±00:00 ist standardmäßig eingestellt.

Bemerkung: Da die Appliance intern in der Zeitzone UTC±00:00 läuft, ist die gewählte Zeitzone sehr wichtig. Für Eastern Standard Time (EST) muss *America/New York* gewählt werden.

Erste Ausführung Festlegen des Datums und der Uhrzeit für den Start des ersten Scans.

Durch Klicken auf kann das Datum gewählt werden. Durch Klicken auf *Now* werden das aktuelle Datum und die aktuelle Zeit für den ersten Durchlauf festgelegt.

Endet am Festlegen des Datums und der Uhrzeit für das Ende des ersten Scans. Aufgaben mit einer festgelegten Endzeit können nicht manuell gestartet werden.

Durch Klicken auf kann das Datum gewählt werden. Durch Aktivieren der Checkbox *Offenes Ende* kann die Endzeit offen gelassen werden.

Laufzeit Festlegen der maximalen Laufzeit, die eine Aufgabe für ihre Ausführung andauern kann. Die Dauer hängt von der angegebenen Start- und Endzeit ab. Falls eine Endzeit festgelegt wurde und diese Zeit abläuft, wird die Aufgabe abgebrochen und ausgesetzt, bis das nächste planmäßige Zeitfenster verfügbar ist. So kann sichergestellt werden, dass der Scan immer in einem bestimmten (Wartungs-)Zeitfenster ausgeführt wird.

Wiederholung Festlegen der Wiederholrate der Aufgabe. Es kann zwischen *Einmalig*, *Stündlich*, *Täglich*, *Wöchentlich*, *Monatlich*, *Jährlich*, *Werktage (Montag bis Freitag)* oder *Benutzerdefiniert...* gewählt werden. Falls die Option *Benutzerdefiniert...* gewählt wird, können die Wiederholrate und die Tage, an denen die Aufgabe ausgeführt werden soll, gewählt werden.

10.10.2 Zeitpläne verwalten

Listenseite

Alle vorhandenen Zeitpläne können angezeigt werden, indem *Konfiguration* > *Zeitpläne* in der Menüleiste gewählt wird.

Für alle Zeitpläne werden die folgenden Informationen angezeigt:

Name Name des Zeitplans.

Erste Ausführung Startzeit der ersten Ausführung der Aufgabe.

Nächste Ausführung Nächste Ausführung der Aufgabe gemäß des aktuellen Datums und der aktuellen Zeit.

Wiederholung Wiederholrate der Aufgabe.

Laufzeit Maximalen Laufzeit, die eine Aufgabe für ihre Ausführung andauern kann. Die Dauer hängt von der angegebenen Start- und Endzeit ab. Falls eine Endzeit festgelegt wurde und diese Zeit abläuft, wird die Aufgabe abgebrochen und ausgesetzt, bis das nächste planmäßige Zeitfenster verfügbar ist. So kann sichergestellt werden, dass der Scan immer in einem bestimmten (Wartungs-)Zeitfenster ausgeführt wird.

Für alle Zeitpläne sind die folgenden Aktionen verfügbar:

- Den Zeitplan in den Papierkorb verschieben. Nur Zeitpläne, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Den Zeitplan bearbeiten.
- Den Zeitplan klonen.
- Den Zeitplan als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Zeitplänen können mehrere Zeitpläne zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Zeitpläne in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen eines Zeitplans werden Details des Zeitplans angezeigt. Durch Klicken auf wird die Detailseite des Zeitplans geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über den Zeitplan.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Zeitplänen anzeigen.
- Einen neuen Zeitplan erstellen (siehe Kapitel *10.10.1* (Seite 272)).
- Den Zeitplan klonen.
- Den Zeitplan bearbeiten.
- Den Zeitplan in den Papierkorb verschieben. Nur Zeitpläne, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Den Zeitplan als XML-Datei exportieren.

10.11 Scanner erstellen und verwalten

Die Appliance bietet zwei voreingestellte Scanner. Diese können verwaltet werden und neue Scanner können erstellt werden.

Die folgenden Scanner sind bereits verfügbar:

- OpenVAS Default
- CVE: Der CVE-Scanner ermöglicht das Vorhersagen eventueller Sicherheitsrisiken, basierend auf aktuellen Informationen über bekannte Schwachstellen aus den Sicherheitsinfos (siehe Kapitel *14* (Seite 357)), ohne dass ein neuer Scan nötig ist (siehe Kapitel *10.4* (Seite 249)).

Bemerkung: Der gewünschte Scanner für eine Aufgabe kann beim Erstellen der Aufgabe gewählt werden (siehe Kapitel *10.2.2* (Seite 218)).

10.11.1 Einen Scanner erstellen

Bemerkung: Das Erstellen eines neuen Scanners wird nur für das Erstellen eines neuen Remote-Scanners genutzt (siehe Kapitel *16.4* (Seite 386)).

10.11.2 Scanner verwalten

Listenseite

Alle vorhandenen Scanner können angezeigt werden, indem *Konfiguration* > *Scanner* in der Menüleiste gewählt wird (siehe Abb. 10.36).

Für alle Scanner sind die folgenden Aktionen verfügbar:

- Den Scanner in den Papierkorb verschieben. Nur selbst erstellte Scanner können in den Papierkorb verschoben werden.
- Den Scanner bearbeiten. Nur selbst erstellte Scanner können bearbeitet werden.
- Den Scanner klonen. Nur selbst erstellte Scanner können geklont werden.
- Den Scanner als XML-Datei exportieren.
- Verifizieren, dass der Scanner online ist und dass sich der Manager mithilfe der bereitgestellten Zertifikate und Anmeldedaten mit ihm verbinden kann.
- Das Zertifikat oder das Zertifikat der Zertifizierungsstelle herunterladen. Das Zertifikat oder das Zertifikat der Zertifizierungsstelle kann nur für selbst erstellte Scanner heruntergeladen werden.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Scannern können mehrere Scanner zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Scanner in den Papierkorb verschoben oder exportiert werden.

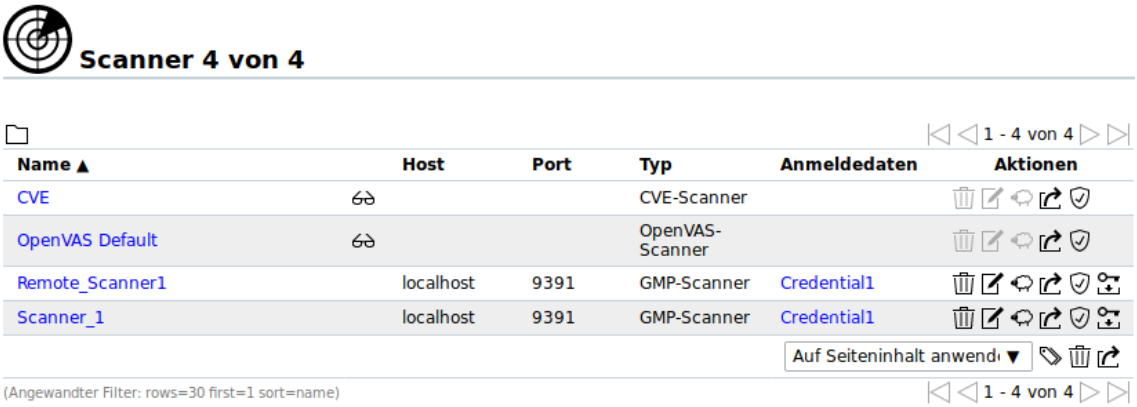


Abb. 10.36: Seite *Scanner* mit allen vorhandenen Scannern

Detailseite

Durch Klicken auf den Namen eines Scanners werden Details des Scanners angezeigt. Durch Klicken auf wird die Detailseite des Scanners geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über den Scanner.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Scannern anzeigen.
- Einen neuen Scanner erstellen (siehe Kapitel *10.11.1* (Seite 275)).
- Den Scanner klonen. Nur selbst erstellte Scanner können geklont werden.
- Den Scanner bearbeiten. Nur selbst erstellte Scanner können bearbeitet werden.
- Den Scanner in den Papierkorb verschieben. Nur selbst erstellte Scanner können in den Papierkorb verschoben werden.
- Den Scanner als XML-Datei exportieren.
- Verifizieren, dass der Scanner online ist und dass sich der Manager mithilfe der bereitgestellten Zertifikate mit ihm verbinden kann.

10.12 Benachrichtigungen nutzen

Benachrichtigungen sind im System verankert. Falls ein konfiguriertes Ereignis (z. B. eine Aufgabe ist abgeschlossen) geschieht, wird eine festgelegte Bedingung (z. B. es wurde eine Schwachstelle mit hohem Schweregrad gefunden) geprüft. Falls die Bedingung erfüllt wird, wird eine Aktion ausgeführt (z. B. eine E-Mail wird an eine bestimmte Adresse gesendet).

10.12.1 Eine Benachrichtigung erstellen

Eine neue Benachrichtigung kann wie folgt erstellt werden:

1. *Konfiguration* > *Benachrichtigungen* in der Menüleiste wählen.
2. Neue Benachrichtigung durch Klicken auf erstellen.
3. Benachrichtigung definieren (siehe Abb. 10.37).
4. Auf *Speichern* klicken.

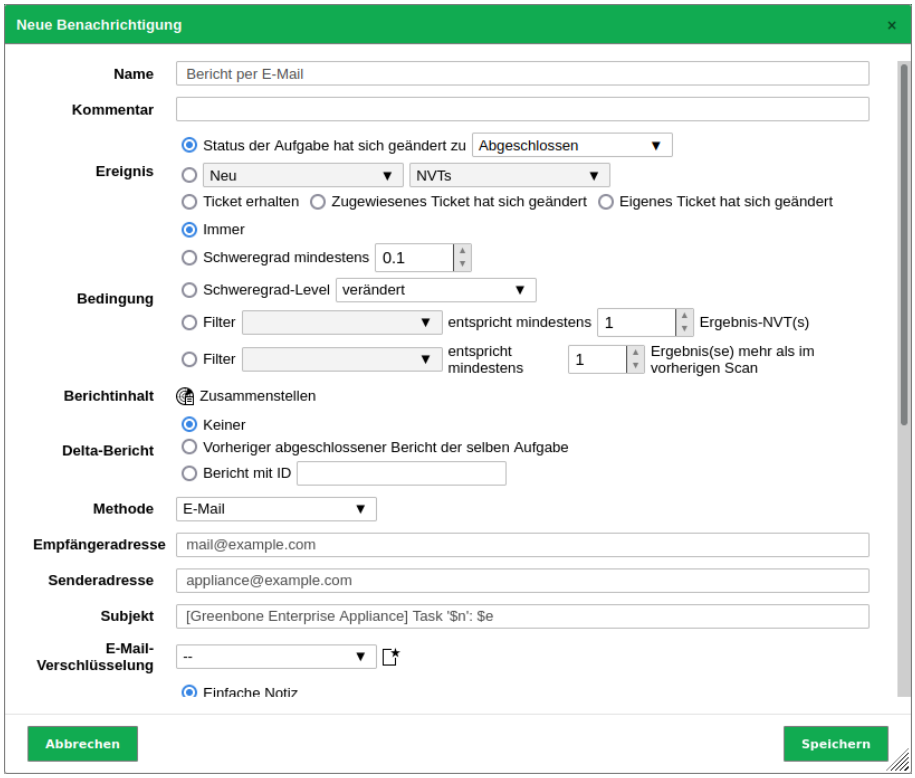


Abb. 10.37: Erstellen einer neuen Benachrichtigung

Die folgenden Details der Benachrichtigung können festgelegt werden:

Name Festlegung des Namens. Der Name kann frei gewählt werden.

Kommentar Ein optionaler Kommentar kann zusätzliche Informationen enthalten.

Ereignis Festlegen des Ereignisses, für das die Benachrichtigung gesendet wird. Benachrichtigungen können gesendet werden, falls sich der Status einer Aufgabe ändert, Sicherheitsinfos (VTs, CVEs, CPEs, CERT-Bund-Advisories, DFN-CERT-Advisories) hinzugefügt werden oder ein Ticket zugewiesen oder geändert wird (siehe Kapitel *11.6* (Seite 308)).

Bedingung Festlegen der zusätzlichen Bedingungen, die erfüllt werden müssen.

> **Bemerkung:** Die Optionen unterscheiden sich für Benachrichtigungen in Verbindung mit Aufgaben, Sicherheitsinfos und Tickets.

Die Benachrichtigung kann auftreten, wenn:

- Immer
- Falls ein bestimmter Schweregrad erreicht wird.
- Falls der Schweregrad sich ändert, erhöht oder sinkt.
- Falls der Powerfilter mindestens der angegebenen Anzahl von Ergebnissen mehr im Vergleich zum vorherigen Scan entspricht.

Berichtinhalt (nur für Benachrichtigungen in Verbindung mit Aufgaben) Der Berichtinhalt kann mit einem zusätzlichen Filter beschränkt werden. Durch Klicken auf kann der Inhalt des Berichts zusammengestellt und ein Powerfilter gewählt werden (siehe Kapitel *11.2.2* (Seite 298)). Der Filter muss zuvor erstellt werden (siehe Kapitel *8.3* (Seite 168)). Für *Einfügen* die Checkbox *Notizen* aktivieren, um Notizen hinzuzufügen und die Checkbox *Übersteuerungen* aktivieren, um aktivierte Übersteuerungen zu kennzeichnen und den Inhalt ihrer Textfelder einzufügen. Für *Seitenadressierung* die Checkbox *Ignorieren* aktivieren, damit die Filtereinstellungen für die Ergebnisse, die pro Seite auf der Web-Oberfläche angezeigt werden, nicht für die Ergebnisse im gesendeten Bericht übernommen werden.

Details-URL (nur für Benachrichtigungen in Verbindung mit Sicherheitsinfos) Festlegen der URL, von der die Sicherheitsinfos erhalten werden.

Delta-Bericht (nur für Benachrichtigungen in Verbindung mit Aufgaben) Optional kann ein Delta-Bericht erstellt werden, entweder als Vergleich mit einem vorherigen Bericht oder mit einem Bericht mit einer bestimmten ID.

Methode Wählen der Methode der Benachrichtigung. Nur eine Methode kann pro Benachrichtigung gewählt werden. Falls unterschiedliche Benachrichtigungen für das gleiche Ereignis ausgelöst werden soll, müssen mehrere Benachrichtigungen erstellt und mit dem gleichen Ereignis verknüpft werden.

> **Bemerkung:** Einige Methoden können nicht für Benachrichtigungen in Verbindung mit Sicherheitsinfos oder Tickets genutzt werden.

Die folgenden Methoden sind möglich:

E-Mail Der Bericht wird an eine angegebene E-Mail-Adresse gesendet.

Um diese Methode nutzen zu können, muss der verwendete Mailhub mithilfe des GOS-Administrationsmenüs konfiguriert sein (siehe Kapitel *7.2.11* (Seite 129)).

Die Einstellungen *Empfängeradresse*, *Senderadresse* und *Inhalte* müssen konfiguriert werden, damit die E-Mail-Benachrichtigung funktioniert. Die E-Mail-Verschlüsselung ist optional.

- **Empfängeradresse** E-Mail-Adresse, an die die E-Mail gesendet wird.
- **Senderadresse** E-Mail-Adresse, die als E-Mail-Absender genutzt wird.
- **Subjekt** Für den Betreff können die folgenden Platzhalter genutzt werden:
  - $d: Datum der letzten Prüfung der Sicherheitsinfos oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $e: Beschreibung des Ereignisses.
  - $n: Name der Aufgabe oder leer für Benachrichtigungen in Verbindung mit Sicherheitsinfos/Tickets.

  - $N: Name der Benachrichtigung.
  - $q: Art des Ereignisses für Sicherheitsinfos (*Neu*, *Aktualisiert*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $s: Art der Sicherheitsinfos (z. B. *NVT*, *CERT-Bund-Advisory*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $S: Siehe *$s*, aber pluralisiert (z. B. *NVTs*, *CERT-Bund-Advisories*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $T: Gesamtanzahl der Objekte in der Liste für Benachrichtigungen in Verbindung mit Sicherheitsinfos oder 0 für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $u: Besitzer der Benachrichtigung oder aktuell eingeloggter Benutzer, falls die Benachrichtigung manuell ausgelöst wird.
  - $U: UUID der Benachrichtigung.
  - $$: Dollarzeichen ($).

- **E-Mail-Verschlüsselung** Die E-Mail kann mithilfe eines konfigurierbaren S/MIME- oder PGP-Schlüssels verschlüsselt werden. Der Schlüssel kann in der Drop-down-Liste *E-Mail-Verschlüsselung* gewählt oder durch Klicken auf ☆ erstellt werden. Die Zertifikatdatei muss die folgenden Bedingungen erfüllen:
  - PEM-kodiert (eine binäre DER-Datei kann nicht genutzt werden)
  - Nutzung des X.509-Formats
  - Ausgestellt für die E-Mail-Adresse des Empfängers (*Empfängeradresse*) und gültig (nicht abgelaufen)
  - Falls das Zertifikat ursprünglich in gebündeltem Format vorlag, das auch den privaten Schlüssel enthielt, muss nur das unverschlüsselte Zertifikat hochgeladen werden.

  Im Falle von S/MIME-Anmeldedaten muss die Zertifikatdatei zusätzlich die folgende Bedingung erfüllen:
  - Kombiniert alle Zertifikate der Kette (root-Zertifikate und alle zwischenliegende Zertifikate)
- **Inhalte** Der Inhalt der E-Mail kann eine einfache Notiz, ein eingefügter oder ein angehängter Bericht sein.
  - **Bericht einfügen** Der Bericht kann direkt in die E-Mail eingefügt werden. Jedes Berichtformat, das einen Inhaltstyp beginnend mit *text/* nutzt, kann gewählt werden, da E-Mails binären Inhalt nicht direkt unterstützen.
  - **Bericht anhängen** Der Bericht kann an die E-Mail angehängt werden. Jedes Berichtformat kann gewählt werden. Der Bericht wird in seinem korrekten MIME-Typ an die generierte E-Mail angehängt.

  Der Inhalt der E-Mail-Nachricht kann sowohl für den eingefügten als auch für den angehängten Bericht bearbeitet werden. Für die Nachricht können die folgenden Platzhalter genutzt werden:
  - $c: Beschreibung der Bedingung.
  - $d: Datum der letzten Prüfung der Sicherheitsinfos oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $e: Beschreibung des Ereignisses.
  - $F: Name des Filters.
  - $f: Filterausdruck.
  - $H: Zusammenfassung der Hosts.

  - $i: Berichttext oder Liste von Sicherheitsinfo-Objekten (nur, falls der Bericht/die Liste eingefügt wird).
  - $n: Name der Aufgabe oder leer für Benachrichtigungen in Verbindung mit Sicherheitsinfos/Tickets.
  - $N: Name der Benachrichtigung.
  - $q: Art des Ereignisses für Sicherheitsinfos (*Neu*, *Aktualisiert*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $r: Name des Berichtformats.
  - $s: Art der Sicherheitsinfos (z. B. *NVT*, *CERT-Bund-Advisory*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $S: Siehe *$s*, aber pluralisiert (z. B. *NVTs*, *CERT-Bund-Advisories*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $t: Notiz, falls der Bericht gekürzt wurde.
  - $T: Gesamtanzahl der Objekte in der Liste für Benachrichtigungen in Verbindung mit Sicherheitsinfos oder 0 für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
  - $u: Besitzer der Benachrichtigung oder aktuell eingeloggter Benutzer, falls die Benachrichtigung manuell ausgelöst wird.
  - $U: UUID der Benachrichtigung.
  - $z: Die genutzte Zeitzone.
  - $$: Dollarzeichen ($).

HTTP-Get Die URL wird als HTTP Get ausgegeben. Beispielsweise kann eine SMS-Textnachricht via HTTP-Get-Gateway gesendet oder ein Bug-Bericht in einem Problemtracker erstellt werden. Für die URL können die folgenden Platzhalter genutzt werden:

- $n: Name der Aufgabe oder leer für Benachrichtigungen in Verbindung mit Sicherheitsinfos/Tickets.
- $e: Beschreibung des Ereignisses.
- $c: Beschreibung der Bedingung.
- $$: Dollarzeichen ($).

Beispiel: `https://example.com/$n` → `https://example.com/Scan_Aufgabe_1`

SCP Der Bericht wird über das Secure Copy Protocol (SCP) unter Nutzung der angegebenen Anmeldedaten für die Authentifizierung auf das festgelegte Ziel kopiert.

Alle Einstellungen (*Anmeldedaten*, *Host*, *Bekannte Hosts* und *Pfad*) müssen konfiguriert werden, damit die SCP-Benachrichtigung funktioniert.

- **Anmeldedaten** Benutzername und Passwort oder Benutzername und SSH-Schlüssel, welche gültige Logininformationen für das Zielsystem enthalten.
- **Host** Der Hostname oder die IP-Adresse des Zielsystems. Pro SCP-Benachrichtigung wird nur ein Zielsystem unterstützt.
- **Port** Standardmäßig wird Port 22 verwendet. Es werden nur Werte unterstützt, die der Liste der standardisierten Ports[29] (zwischen 1 und 65535) entsprechen. Wird ein nicht unterstützter Wert gespeichert, wird stattdessen entweder der Standardwert `22` verwendet oder der eingegebene Wert gekürzt, z. B. `70000` wird zu `7000`.

[29] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt

- **Bekannte Hosts** Der öffentliche SSH-Schlüssel des Zielsystems im Format „Host Protokoll öffentlicher_Schlüssel“, z. B. `localhost ssh-rsa AAAAB3NzaC1y...P3pCquVb`. Der „Host“-Teil muss entsprechend mit dem Hostnamen oder der IP-Adresse übereinstimmen.
- **Pfad** Der vollständige Pfad des Zielverzeichnisses und der Zieldatei, z. B. `/home/user/Downloads/report.xml`. Das Verkürzen des Pfads, z. B. durch Nutzen von `~` wird nicht unterstützt. Für den Dateinamen können die folgenden Platzhalter genutzt werden:
  - $$: Dollarzeichen ($).
  - $n: Name der Aufgabe.
- **Bericht** Format des kopierten Berichts.

Sende an Host Der Bericht wird via TCP an eine beliebige Host-Port-Kombination gesendet. Die IP-Adresse oder der Hostname ist zulässig.

Das Format des Berichts kann aus den installierten Berichtformaten gewählt werden.

SMB Der Bericht wird über Server Message Block (SMB) unter Nutzung der angegebenen Anmeldedaten für die Authentifizierung auf das festgelegte Ziel kopiert.

Die Einstellungen *Anmeldedaten*, *Freigabepfad* und *Dateipfad* müssen konfiguriert werden, damit die SMB-Benachrichtigung funktioniert. Die Wahl eines Berichtformats ist optional.

- **Anmeldedaten** Benutzername und Passwort, welche gültige Logininformationen für das Zielsystem enthalten.
- **Freigabepfad** Der Freigabepfad enthält den Teil des UNC-Pfads, der den Host und den Freigabenamen enthält, z. B. `\\host\share`. Der Freigabepfad muss auf dem Zielsystem angelegt werden, bevor die Benachrichtigung genutzt werden kann.
- **Dateipfad** Ort des Berichts im Freigabeordner, der durch den Freigabepfad festgelegt wird.

Bemerkung: Falls der Dateipfad Unterordner enthält, die nicht existieren, werden die benötigten Unterordner erstellt.

Die Dateiendung wird dem in der Drop-down-Liste *Berichtformat* gewählten Format entsprechend angehängt.

Der Standardname für exportierte Berichte (siehe Kapitel *8.7* (Seite 181)) wird an den Dateipfad angehängt, falls dieser mit `\` endet.

Bemerkung: Falls eine Aufgabe den Tag `smb-alert:file_path` mit einem Wert nutzt, wird der Wert als Dateipfad genutzt und nicht der Pfad, der mit der Benachrichtigung konfiguriert wurde (siehe Kapitel *8.4* (Seite 176)). Beispiel: `smb-alert:file_path=alert_1` weist den Dateipfad `alert_1` zu.

Für den Dateipfad können die folgenden Platzhalter genutzt werden:

- %C: Erstellungsdatum im Format YYYYMMDD. Wird zum aktuellen Datum geändert, falls kein Erstellungsdatum verfügbar ist.
- %C: Erstellungszeit im Format HHMMSS. Wird zur aktuellen Zeit geändert, falls keine Erstellungszeit verfügbar ist.
- %D: Aktuelles Datum im Format YYYYMMDD.
- %F: Name des genutzten Berichtformats (XML für Listen und andere Typen als Berichte).
- %M: Modifizierungsdatum im Format YYYYMMDD. Wird zum Erstellungsdatum oder zum aktuellen Datum geändert, falls kein Modifizierungsdatum verfügbar ist.

  - %m: Modifizierungszeit im Format HHMMSS. Wird zur Erstellungszeit oder zur aktuellen Zeit geändert, falls keine Modifizierungszeit verfügbar ist.
  - %N: Name des Objekts oder, im Falle von Berichten, der zugehörigen Aufgabe. Listen und Typen ohne Namen nutzen den Typen (siehe %T).
  - %T: Objekttyp, z. B. „task“, „port_list“. Pluralisiert für Listenseiten.
  - %t: Aktuelle Zeit im Format HHMMSS.
  - %U: Eindeutige ID des Objekts oder „list“ für Listen aus mehreren Objekten.
  - %u: Name des aktuell eingeloggten Benutzers.
  - %%: Prozentzeichen (%).

- **Berichtformat** Format des kopierten Berichts. Falls kein Berichtformat festgelegt wird, wird standardmäßig XML genutzt.
- **Max Protocol** SMB-Version, falls der SMB-Server nur eine bestimmte Version unterstützt. Die folgenden Optionen können gewählt werden:
  - Standard
  - SMB3
  - SMB2
  - NT1 (für SMBv1)

  Falls keine SMB-Version oder *Standard* gewählt wird, wird die aktuellste unterstützte Version verwendet.

SNMP Ein SNMP-Trap wird an den angegebenen Agenten gesendet. Der festgelegte Community-String wird genutzt, um den SNMP-Trap zu authentifizieren. Der Agent ist der als Ziel gesetzte SNMP-Trap-Empfänger. Für die Nachricht können die folgenden Platzhalter genutzt werden:

- $$: Dollarzeichen ($).
- $d: Datum der letzten Prüfung der Sicherheitsinfos oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
- $e: Beschreibung des Ereignisses.
- $n: Name der Aufgabe oder leer für Benachrichtigungen in Verbindung mit Sicherheitsinfos/Tickets.
- $q: Art des Ereignisses für Sicherheitsinfos (*Neu*, *Aktualisiert*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
- $s: Art der Sicherheitsinfos (z. B. *NVT*, *CERT-Bund-Advisory*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
- $S: Siehe *$s*, aber pluralisiert (z. B. *NVTs*, *CERT-Bund-Advisories*) oder leer für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.
- $T: Gesamtanzahl der Objekte in der Liste für Benachrichtigungen in Verbindung mit Sicherheitsinfos oder 0 für Benachrichtigungen in Verbindung mit Aufgaben/Tickets.

Sourcefire-Schnittstelle Die Daten können automatisch an das Cisco Firepower Management Center (früher als Sourcefire Defense Center bekannt) gesendet werden. Für mehr Informationen siehe Kapitel *18.3* (Seite 404).

Aufgabe starten Die Benachrichtigung kann eine zusätzliche Aufgabe starten. Die Aufgabe wird in der Dropdown-Liste *Aufgabe starten* gewählt.

System-Logger Die Benachrichtigung wird an einen Syslog-Daemon gesendet. Der Syslog-Server wird mithilfe des GOS-Administrationsmenüs festgelegt (siehe Kapitel *7.2.12* (Seite 133)).

Bemerkung: Die Zeitzone der Appliance (UTC±00:00) wird für die Zeitstempel der Protokolle verwendet, sofern dies nicht auf dem Syslog-Server angepasst wurde.

---

verinice.PRO-Konnektor Die Daten können automatisch an eine verinice.PRO-Installation gesendet werden. Für mehr Informationen siehe Kapitel *18.1* (Seite 395).

TippingPoint SMS Eine HTTPS-API wird verwendet, um einen Bericht im CSV-Format in das TippingPoint Security Management System (SMS) hochzuladen.

- **Hostname** / **IP** Hostname oder IP-Adresse des TippingPoint SMS. Der CSV-Bericht wird dann an `https://<address>/vulnscanner/import` gesendet, wobei `<address>` der/die eingegebene Hostname/IP-Adresse ist.
- **Anmeldedaten** Benutzername und Passwort, welche gültige Logininformationen für das TippingPoint SMS enthalten.
- **SSL** / **TLS Certificate** Ein CA-Zertifikat zur Überprüfung, ob es sich bei dem Host, mit dem sich die Benachrichtigung verbindet, um das TippingPoint SMS handelt. Die Zertifikatdatei muss die folgenden Bedingungen erfüllen:
  - PEM-kodiert (eine binäre DER-Datei kann nicht genutzt werden)
  - Nutzung des X.509-Formats
- **Problemumgehung für Standard-Zertifikat verwenden** Standardmäßig verwendet das Zertifikat *Tippingpoint* als Common Name (CN), der in den meisten Fällen nicht mit dem Hostnamen/der IP-Adresse des TippingPoint SMS übereinstimmt. Falls aktiviert, ändert der Workaround den CN vorübergehend und löst ihn innerhalb des internen Konnektorskripts in den tatsächlichen Hostnamen/die IP-Adresse auf.

Alemba vFire In der Anwendung zur Dienstverwaltung vFire wird ein neues Ticket erstellt. Der Bericht kann in einem oder mehreren Formaten angehängt werden. Für mehr Informationen siehe Kapitel *18.4* (Seite 407).

10.12.2 Eine Benachrichtigung einer Aufgabe zuweisen

Falls eine Benachrichtigung genutzt werden soll, muss die Benachrichtigung wie folgt für eine bestimmte Aufgabe festgelegt werden:

Bemerkung: Bereits definierte und genutzte Aufgaben können ebenfalls bearbeitet werden, da dies keinen Einfluss auf bereits erstellte Berichte hat.

---

1. *Scans* > *Aufgaben* in der Menüleiste wählen.
2. In der Zeile der Aufgabe auf ✎ klicken.
3. Benachrichtigung in der Drop-down-Liste *Benachrichtigungen* wählen (siehe Abb. 10.38).

   Bemerkung: Eine neue Benachrichtigung kann durch Klicken auf ✎★ erstellt werden.

   ---

4. Auf *Speichern* klicken.

   → Anschließend wird die Aufgabe, die die Benachrichtigung nutzt, auf der Detailseite der Benachrichtigung angezeigt (siehe Abb. 10.39).

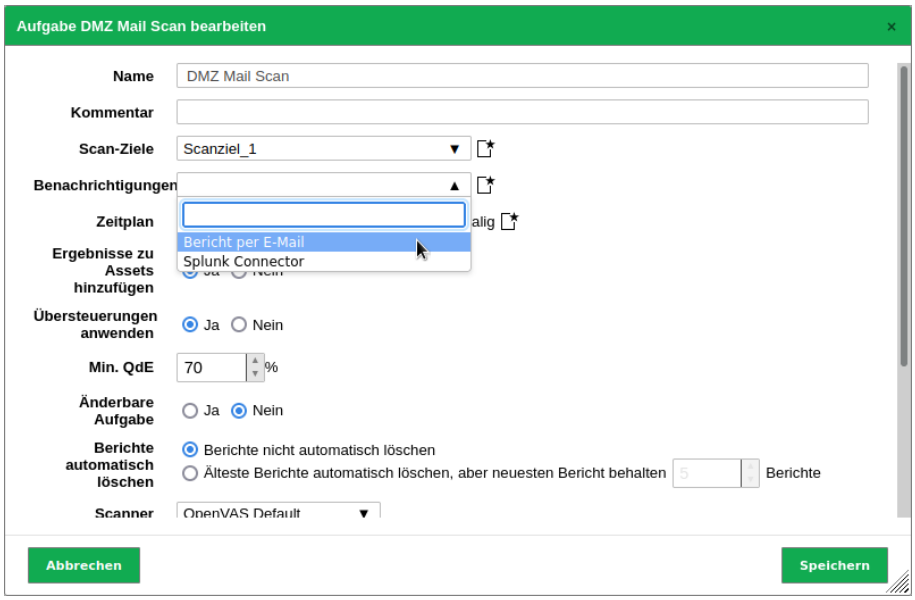


Abb. 10.38: Konfigurieren einer Aufgabe mit einer Benachrichtigung

Abb. 10.39: Aufgabe, die eine bestimmte Benachrichtigung nutzt

10.12.3 Benachrichtigungen verwalten

Listenseite

Alle vorhandenen Benachrichtigungen können angezeigt werden, indem *Konfiguration > Benachrichtigungen* in der Menüleiste gewählt wird.

Für alle Benachrichtigungen werden die folgenden Informationen angezeigt:

Name Name der Benachrichtigung.

Ereignis Ereignis, für das die Benachrichtigung ausgelöst wird.

Bedingung Bedingung, die erfüllt werden muss, um die Benachrichtigung auszulösen.

Methode Gewählte Benachrichtigungsmethode mit zusätzlichen Informationen, z. B. an welche IP- oder E-Mail-Adresse die Benachrichtigung gesendet wird.

Filter (nur für Benachrichtigungen in Verbindung mit Aufgaben) Filter, der auf den Inhalt des Berichts angewendet wird.

Aktiv Hinweis, ob die Benachrichtigung aktiviert oder deaktiviert ist.

Für alle Benachrichtigungen sind die folgenden Aktionen verfügbar:

- Die Benachrichtigung in den Papierkorb verschieben. Nur Benachrichtigungen, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Die Benachrichtigung bearbeiten.
- Die Benachrichtigung klonen.
- Die Benachrichtigung als XML-Datei exportieren.
- Die Benachrichtigung testen.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Benachrichtigungen können mehrere Benachrichtigungen zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Benachrichtigungen in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Benachrichtigung werden Details der Benachrichtigung angezeigt. Durch Klicken auf wird die Detailseite der Benachrichtigungen geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Benachrichtigung.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Benachrichtigungen anzeigen.
- Eine neue Benachrichtigungen erstellen (siehe Kapitel *10.12.1* (Seite 277)).
- Die Benachrichtigung klonen.
- Die Benachrichtigung bearbeiten.

- Die Benachrichtigung in den Papierkorb verschieben. Nur Benachrichtigungen, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden.
- Die Benachrichtigung als XML-Datei exportieren.

10.13 Hindernisse beim Scannen

Es gibt eine Reihe typischer Probleme, welche während eines Scans mit den Standardwerte der Appliance auftreten können. Während die Standardwerte der Appliance für die meisten Umgebungen und Nutzenden passend sind, benötigen sie möglicherweise etwas Optimierung, abhängig von der tatsächlichen Umgebung und der Konfiguration der gescannten Hosts.

10.13.1 Hosts nicht gefunden

Während eines typischen Scans (entweder *Discovery* oder *Full and fast*) nutzt die Appliance standardmäßig zuerst den Pingbefehl, um die Verfügbarkeit der konfigurierten Ziele zu prüfen. Falls ein Ziel nicht auf die Pinganfrage antwortet, wird es als tot angenommen und nicht vom Portscanner oder einem VT gescannt.

In den meisten LAN-Umgebungen stellt dies kein Problem dar, da alle Geräte auf eine Pinganfrage antworten. Allerdings unterdrücken (lokale) Firewalls oder andere Konfigurationen manchmal die Pingantwort. Falls dies passiert, wird das Ziel nicht gescannt und ist nicht in den Ergebnissen und im Bericht enthalten.

Um dieses Problem zu beseitigen, müssen sowohl die Konfiguration des Ziels als auch die Scan-Konfiguration die Einstellung des Erreichbarkeitstest unterstützen (siehe *Alive Test* (Seite 216)).

Falls das Ziel nicht auf die Pinganfrage reagiert, könnte ein TCP-Ping getestet werden. Falls sich das Ziel in derselben Übertragungsdomäne befindet, könnte auch ein ARP-Ping genutzt werden.

10.13.2 Lang andauernde Scans

Wenn mithilfe des Pingbefehls erkannt wurde, dass das Ziel erreichbar ist, nutzt die Appliance einen Portscanner, um das Ziel zu scannen. Standardmäßig wird eine TCP-Portliste mit ungefähr 5000 Ports genutzt. Falls das Ziel durch eine (lokale) Firewalls geschützt wird, die die meisten dieser Pakete weglässt, muss der Portscan auf das Timeout jedes einzelnen Ports warten. Falls die Hosts durch (lokale) Firewalls geschützt werden, müssen die Portlisten oder die Firewalls angepasst werden. Falls die Firewall die Anfrage nicht fallen lässt, aber sie ablehnt, muss der Portscanner nicht auf das Timeout warten. Dies gilt insbesonders für UDP-Ports, die im Scan enthalten sind.

10.13.3 VT nicht genutzt

Dies passiert besonders oft, falls UDP-basierte VTs wie die, die SNMP nutzen, verwendet werden. Falls die Standardkonfiguration *Full and fast* genutzt wird, werden die SNMP-VTs eingeschlossen. Falls das Ziel allerdings so konfiguriert ist, dass es die Standardportliste nutzt, werden die VTs nicht ausgeführt. Dies geschieht, da die Standardportliste keine UDP-Ports beinhaltet. Deshalb wird der Port 161/udp (SNMP) nicht gefunden und von späteren Scans ausgeschlossen. Der Discoveryscan und die empfohlene Scan-Konfiguration *Full and fast* optimieren den Scan basierend auf den gefundenen Diensten. Falls der UDP-Port nicht entdeckt wird, werden keine SNMP-VTs ausgeführt.

Es sollten nicht alle Ports in der Portliste standardmäßig aktiviert sein. Dies verlängert den Scan wesentlich. Die bewährte Methode ist es, die Portliste auf die Ports einzustellen, die in der Umgebung genutzt werden und von den Firewalls unterstützt werden.

10.13.4 vHosts scannen

Der Scanner ist in der Lage, alle Beziehungen zwischen Hostnamen und IP-Adressen zu finden, ohne dass zusätzliches Input durch den Benutzer nötig ist.

In Umgebungen mit virtuellen Hosts (vHosts)[30] haben die Scanberichte weniger Ergebnisse, da Duplikate vermieden werden.

Zwei Scanner-Vorgaben steuern das Scannen von vHosts (siehe Kapitel *10.9.4* (Seite 267)):

test_empty_vhost Falls diese Vorgabe aktiviert ist, scannt der Scanner Scanner das Ziel auch unter Nutzung leerer vhost-Werte, zusätzlich zu den dem Ziel zugewiesenen vhost-Werten.

expand_vhosts Falls diese Vorgabe aktiviert ist, wird die Hostliste des Ziels wird mit Werten erweitert, die durch Quellen wie Invers-Lookup-Anfragen und VT-Prüfungen für SSL/TLS-Zertifikate erhalten wurden.

[30] https://httpd.apache.org/docs/current/de/vhosts/

KAPITEL 11

Berichte und Schwachstellenmanagement

Bemerkung: Dieses Kapitel dokumentiert alle möglichen Menüoptionen.

Allerdings unterstützen nicht alle Appliance-Modelle alle Menüoptionen. Um festzustellen, ob ein bestimmtes Feature für das genutzte Appliance-Modell verfügbar ist, können die Tabellen in Kapitel *3* (Seite 20) genutzt werden.

Die Scanergebnisse werden in einem Bericht zusammengefasst. Berichte können auf der Web-Oberfläche angezeigt und in unterschiedlichen Formaten heruntergeladen werden.

Die Appliance speichert alle Berichte aller Scans in der lokalen Datenbank. Nicht nur der letzte Bericht wird gespeichert, sondern alle Berichte aller jemals gelaufenen Scans. Dies ermöglicht den Zugriff auf vergangene Informationen. Die Berichte enthalten erkannte Schwachstellen und Informationen über den Scan.

Nach dem Starten eines Scans kann der Bericht der bis dahin gefundenen Ergebnisse angesehen werden. Wenn der Scan abgeschlossen ist, ändert sich der Status zu *Abgeschlossen* und keine weiteren Ergebnisse werden hinzugefügt.

11.1 Berichtformate konfigurieren und verwalten

Berichtformate sind die Formate, aus denen ein Bericht basierend auf den Scanergebnissen erstellt wird. Viele Berichtformate reduzieren die verfügbaren Daten, um sie auf sinnvolle Weise darzustellen.

Die Berichtformate können genutzt werden, um Berichtinformationen in andere Dokumentformate zu exportieren, sodass sie von Dritt-Anwendungen (Konnektoren) verarbeitet werden können.

Der Name des exportierten Berichts kann in den Benutzereinstellungen konfiguriert werden (siehe Kapitel *8.7* (Seite 181)).

Das von der Appliance verwendete XML-Format enthält alle Daten und kann genutzt werden, um exportierte Berichte in andere Appliances zu importieren. Dazu muss eine Container-Aufgabe erstellt werden (siehe Kapitel *10.5* (Seite 252)).

11.1.1 Standard-Berichtformate

Alle Standardberichtformate von Greenbone sind Datenobjekte, die über den Feed verteilt werden. Sie werden mit jedem Feed-Update heruntergeladen und aktualisiert.

Bemerkung: Berichtformate können veraltet sein. Sie werden auf der Web-Oberfläche mit *(Veraltet)* gekennzeichnet und in der folgenden Liste nicht mehr dokumentiert.

Veraltete Berichtformate können nicht mehr verwendet werden. Wenn ein Bericht in einem solchen Format exportiert wird, kann die heruntergeladene Datei leer oder anderweitig nicht verwendbar sein.

Falls keine Standardberichtformate verfügbar sind, ist möglicherweise ein Feed-Update nötig oder der Feed Import Owner muss festgelegt werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Standardrichtlinien können nicht bearbeitet werden. Außerdem können sie nur temporär vom Feed Import Owner oder von einem Super-Administrator gelöscht werden. Während des nächsten Feed-Updates werden sie wieder heruntergeladen.

Bemerkung: Um ein Standardberichtformat dauerhaft zu löschen, muss der Feed Import Owner es löschen. Anschließend muss der Feed Import Owner auf *(Unset)* geändert werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Die folgenden Berichtformate sind standardmäßig verfügbar:

Anonymous XML Dies ist die anonyme Version des XML-Formats. IP-Adressen werden durch zufällige IP-Adressen ersetzt.

ARF: Asset Reporting Format v1.0.0 Dieses Format erzeugt einen Bericht, der dem NIST Asset Reporting Format entspricht.

CPE – Common Platform Enumeration CSV-Tabelle Dieser Bericht wählt alle CPE-Tabellen und erstellt eine einzelne kommagetrennte Datei.

CSV Hosts Dieser Bericht erstellt eine kommagetrennte Datei, die alle gefundenen Systeme enthält.

CSV Results Dieser Bericht erstellt eine kommagetrennte Datei, die alle gefundenen Ergebnisse enthält.

GCR PDF – Greenbone Compliance Report Dies ist der vollständige Greenbone Compliance Report für Compliance-Audits (siehe Kapitel *12.2* (Seite 325)) mit allen Schwachstellen in grafischem Format als PDF-Datei. Die Sprache des Berichts ist Englisch.

GSR HTML – Greenbone Security Report Dies ist der vollständige Greenbone Security Report mit allen Schwachstellen und Ergebnissen. Er kann mit einem Webbrowser geöffnet werden, in dem JavaScript aktiviert sein muss. Er enthält von der Web-Oberfläche bekannte, dynamisch sortierbare Listen. Die Sprache des Berichts ist Englisch.

GSR PDF – Greenbone Security Report Dies ist der vollständige Greenbone Security Report mit allen Schwachstellen in grafischem Format als PDF-Datei. Der Topologiegraph ist nicht enthalten, falls mehr als 100 Hosts mit dem Bericht abgedeckt sind. Die Sprache des Berichts ist Englisch.

GXCR PDF – Greenbone Executive Compliance Report Dies ist der gekürzte Greenbone Compliance Report für Compliance-Audits (siehe Kapitel *12.2* (Seite 325)) für das Management mit allen Schwachstellen in grafischem Format als PDF-Datei. Die Sprache des Berichts ist Englisch.

GXR PDF – Greenbone Executive Report Dies ist der gekürzte Greenbone Security Report für das Management mit allen Schwachstellen in grafischem Format als PDF-Datei. Der Topologiegraph ist nicht enthalten, falls mehr als 100 Hosts mit dem Bericht abgedeckt sind. Die Sprache des Berichts ist Englisch.

LaTeX Dieser Bericht wird als LaTeX-Quelltext bereitgestellt. Die Sprache des Berichts ist Englisch.

NBE Dies ist das alte OpenVAS-/Nessus-Berichtformat. Es bietet keine Unterstützung für Notizen, Übersteuerungen und einige weitere Informationen.

PDF Dies ist ein vollständiger Bericht als PDF. Wie das HTML-Format ist es neutral. Die Sprache des Berichts ist Englisch.

TLS Map Dies ist das Berichtformat für TLS-Map-Scans (siehe Kapitel *12.6* (Seite 347)).

Topology SVG Dies stellt die Ergebnisse in einem SVG-Bild dar.

TXT Dies erstellt eine Textdatei. Dieses Format ist insbesondere beim Senden von E-Mail nützlich. Die Sprache des Berichts ist Englisch.

Verinice ISM Erstellt eine Importdatei für das ISMS-Tool *verinice* (siehe Kapitel *18.1* (Seite 395)).

Verinice ISM all results Erstellt eine Importdatei für das ISMS-Tool *verinice* (siehe Kapitel *18.1* (Seite 395)).

Verinice ITG (veraltet) Erstellt eine Importdatei für das ISMS-Tool *verinice* (siehe Kapitel *18.1* (Seite 395)).

Vulnerability Report HTML (empfohlen) Dies ist der neue vollständige Greenbone Security Report mit allen Schwachstellen und Ergebnissen. Er kann mit einem Webbrowser oder einem HTML-Viewer geöffnet werden. Die Sprache des Berichts ist Englisch.

Vulnerability Report PDF (empfohlen) Dies ist der vollständige Greenbone Security Report mit allen Schwachstellen in grafischem Format als PDF-Datei. Die Sprache des Berichts ist Englisch.

Berichte mit diesem Berichtformat sind auf die ersten 500 Ergebnisse pro Host beschränkt. Nachfolgende Ergebnisse pro Host werden ausgelassen und eine Warnung wird auf der Titelseite des Berichts angezeigt.

XML Der Bericht wird im ursprünglichen XML-Format exportiert. Im Gegensatz zu anderen Formaten enthält dieses Format alle Ergebnisse und formatiert diese nicht.

11.1.2 Berichtformate verwalten

Listenseite

Alle vorhandenen Berichtformate können angezeigt werden, indem *Konfiguration > Berichtformate* in der Menüleiste gewählt wird.

Für alle Berichtformate werden die folgenden Informationen angezeigt:

Name Name des Berichtformats.

Dateiendung Der Dateiname des heruntergeladenen Berichts besteht aus der UUID (einzigartige, interne ID des Berichts) und diese Erweiterung. Unter anderem unterstützt die Erweiterung den Browser beim Starten einer kompatiblen Anwendungen, falls ein bestimmter Inhaltstyp nicht erkannt wird.

Inhaltstyp Der Inhaltstyp bestimmt das genutzte Format und wird beim Herunterladen übertragen. Dadurch kann eine kompatible Anwendung vom Browser gestartet werden.

Zusätzlich ist der Inhaltstyp intern wichtig: Er wird genutzt, um in seinem Kontext ein geeignetes Plug-in anzubieten. Beispielsweise werden beim Senden eines Berichts per E-Mail alle Plug-ins des Typs `text/\*` angeboten, da sie auf lesbare Weise in eine E-Mail eingebettet werden können.

Vertrauen (Zuletzt Verifiziert) Einige Plug-ins bestehen aus einer Datentransformation, während andere komplexere Operationen ausführen und auch Hilfsprogramme nutzen. Um einen Missbrauch zu vermeiden, muss jedes Berichtformat-Plug-in von Greenbone digital signiert werden. Die digitalen Signaturen werden über den Greenbone Enterprise Feed verteilt. Falls die Signatur echt ist und dem Herausgeber vertraut wird, ist sichergestellt, dass das Berichtformat in exakt dem vom Herausgeber beglaubigten Format vorliegt. Die Vertrauensprüfung läuft automatisch ab und das Ergebnis wird in der Spalte *Vertrauen (Zuletzt Verifiziert)* angezeigt.

Aktiv Die Berichtformate sind in den entsprechenden Auswahlmenüs nur verfügbar, wenn sie aktiviert wurden. Neu importierte Berichtformate sind am Anfang immer deaktiviert. Ein Berichtformat kann nur aktiviert werden, wenn ihm vertraut wird.

Für alle Berichtformate sind die folgenden Aktionen verfügbar:

- Das Berichtformat in den Papierkorb verschieben. Solange das Berichtformat nicht aus dem Papierkorb gelöscht wird, wird es beim nächsten Feed-Update nicht neu heruntergeladen.
- Das Berichtformat bearbeiten. Nur selbst erstellte Berichtformate können bearbeitet werden.

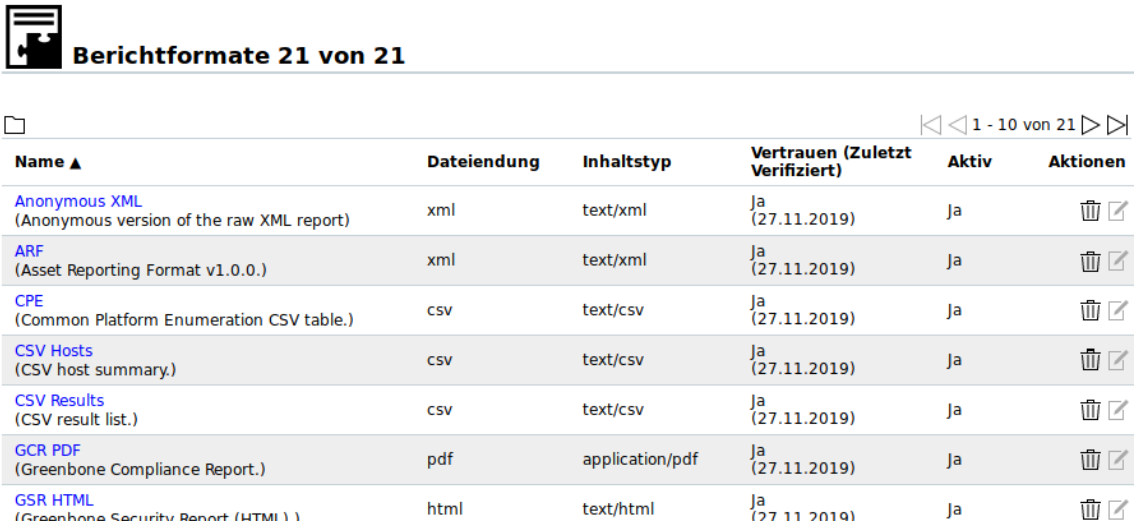
Bemerkung: Durch Klicken auf unterhalb der Liste von Berichtformaten können mehrere Berichtformate zur gleichen Zeit in den Papierkorb verschoben werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Berichtformate in den Papierkorb verschoben werden.

Detailseite

Durch Klicken auf den Namen eines Berichtformats werden Details des Berichtformats angezeigt. Durch Klicken auf wird die Detailseite des Berichtformats geöffnet.

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Berichtformaten anzeigen.
- Ein neues Berichtformat hinzufügen (siehe Kapitel *11.1.3* (Seite 292)).
- Das Berichtformat bearbeiten. Nur selbst erstellte Berichtformate können bearbeitet werden.
- Das Berichtformat in den Papierkorb verschieben. Solange das Berichtformat nicht aus dem Papierkorb gelöscht wird, wird es beim nächsten Feed-Update nicht neu heruntergeladen.



Berichtformate 21 von 21

1 - 10 von 21

Name ▲	Dateiendung	Inhaltstyp	Vertrauen (Zuletzt Verifiziert)	Aktiv	Aktionen
Anonymous XML (Anonymous version of the raw XML report)	xml	text/xml	Ja (27.11.2019)	Ja	
ARF (Asset Reporting Format v1.0.0.)	xml	text/xml	Ja (27.11.2019)	Ja	
CPE (Common Platform Enumeration CSV table.)	csv	text/csv	Ja (27.11.2019)	Ja	
CSV Hosts (CSV host summary.)	csv	text/csv	Ja (27.11.2019)	Ja	
CSV Results (CSV result list.)	csv	text/csv	Ja (27.11.2019)	Ja	
GCR PDF (Greenbone Compliance Report.)	pdf	application/pdf	Ja (27.11.2019)	Ja	
GSR HTML (Greenbone Security Report (HTML).)	html	text/html	Ja (27.11.2019)	Ja	

Abb. 11.1: Seite *Berichtformate* mit allen verfügbaren Berichtformaten

11.1.3 Ein Berichtformat hinzufügen

Bemerkung: Um einen Missbrauch zu vermeiden, muss jedes zusätzlich importierte Berichtformat von Greenbone überprüft und digital signiert werden. Berichtformate, die nicht von Greenbone signiert sind, werden in GOS nicht unterstützt und können nicht genutzt werden.

Für mehr Informationen siehe Kapitel *11.1.2* (Seite 290) – *Vertrauen (Zuletzt Verifiziert)*.

Ein neues Berichtformat kann wie folgt importiert werden:

1. Berichtformat-Plug-in, das von Greenbone geprüft und akzeptiert wurde, bereitstellen oder besorgen.
2. *Konfiguration* > *Berichtformate* in der Menüleiste wählen.
3. Auf klicken.
4. Auf *Browse. . .* klicken und das Berichtformat-Plug-in wählen (siehe Abb. 11.2).

Abb. 11.2: Importieren eines Berichtformat-Plug-ins

5. Auf *Speichern* klicken.

   → Das importierte Berichtformat wird auf der Seite *Berichtformate* angezeigt.
6. In der Zeile des Berichtformats auf klicken.
7. Für *Aktiv* den Radiobutton *Ja* wählen (siehe Abb. 11.3).
8. Auf *Speichern* klicken.

Abb. 11.3: Aktivieren eines neuen Berichtformats

11.2 Berichte nutzen und verwalten

Alle vorhandenen Berichte aller Scans können angezeigt werden, indem *Scans > Berichte* in der Menüleiste gewählt wird.

Die gesamte Anzahl an Berichten für eine bestimmte Aufgabe wird auf der Seite *Aufgaben* in der Spalte *Berichte* angezeigt.

Der Bericht einer bestimmten Aufgabe kann wie folgt angezeigt werden:

1. *Scans > Aufgaben* in der Menüleiste wählen.
2. Zum Anzeigen aller Berichte bei gewünschter Aufgabe auf die Gesamtanzahl an Berichten in der Spalte *Berichte* klicken.

   → Die Seite *Berichte* wird geöffnet. Ein Filter ist angewendet, um nur die Berichte für die gewählte Aufgabe anzuzeigen.

Tipp: Durch Klicken auf das Datum in der Spalte *Letzter Bericht* wird die Detailseite des letzten Berichts geöffnet (siehe Kapitel *11.2.1* (Seite 293)).

Berichte	Letzter Bericht
6	Do., 18. Okt. 2018 14:54 UTC
5	Do., 18. Okt. 2018 14:36 UTC

Abb. 11.4: Gesamtanzahl an gespeicherten Berichten und Datum des letzten Berichts

Für alle Berichte werden die folgenden Informationen angezeigt:

Datum Datum und Zeit der Berichterstellung.

Status Status der zugehörigen Aufgabe.

Aufgabe Zugehörige Aufgabe.

Schweregrad Höchster Schweregrad, der durch den Scan gefunden wurde.

Hoch/Mittel/Niedrig/Log/Falsch-Positiv Anzahl der gefundenen Schwachstelle für jeden Schweregrad.

Für alle Berichte sind die folgenden Aktionen verfügbar:

- Δ Einen Delta-Vergleich erstellen (siehe Kapitel *11.2.5* (Seite 300)).
- ⨯ Den Bericht löschen.

Bemerkung: Durch Klicken auf ⨯ unterhalb der Liste von Berichten können mehrere Berichte zur gleichen Zeit gelöscht werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Berichte gelöscht werden.

11.2.1 Einen Bericht lesen

Durch Klicken auf das Datum eines Berichts werden Details des Berichts angezeigt.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über den entsprechenden Scan.

Ergebnisse Liste aller Ergebnisse in diesem Bericht (siehe Kapitel *11.2.1.1* (Seite 295)).

Hosts Gescannte Hosts mit Hostnamen und IP-Adressen. Die gefundenen Betriebssysteme, die Anzahl gefundener Schwachstellen für jeden Schweregrad und der höchste durch den Scan gefundene Schweregrad werden angezeigt.

Ports Gescannte Ports mit Portnamen, Anzahl der Hosts und höchstem durch den Scan gefundenen Schweregrad.

Anwendungen Gescannte Anwendung mit CPE der Anwendung, Anzahl der Hosts, Anzahl der Ergebnisse, die diese CPE festgestellt haben und höchstem durch den Scan gefundenen Schweregrad.

Betriebssysteme Gescannte Betriebssysteme mit Systemnamen, Hostnamen, Anzahl gescannter Hosts und höchstem durch den Scan gefundenen Schweregrad.

CVEs Durch den Scan gefundene CVEs.

Geschlossene CVEs CVEs von ursprünglich erkannten Schwachstellen, die während des Scans bereits als gelöst bestätigt wurden.

TLS-Zerifikate Durch den Scan gefundene TLS-Zertifikate.

Fehlermeldungen Fehlermeldungen, die während des Scans auftraten.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Der Inhalt des Bericht kann nach einer gewählten Spalte sortiert werden, indem auf den Spaltentitel geklickt wird. Der Inhalt kann auf- oder absteigend sortiert werden:

- ▲ im Spaltentitel zeigt, dass die Objekte aufsteigend sortiert sind.
- ▼ im Spaltentitel zeigt, dass die Objekte absteigend sortiert sind.

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Berichtformaten anzeigen.
- Die Inhalte des Berichts, die mindestens eine QdE von 70 % und aktivierte Übersteuerungen haben, zu den Assets hinzufügen.
- Die Inhalte des Berichts aus den Assets entfernen.
- Die zugehörige Aufgabe anzeigen.
- Die Seite *Ergebnisse* öffnen. Ein Filter ist angewendet, sodass nur die Ergebnisse für diesen Bericht angezeigt werden.
- Die Seite *Schwachstellen* öffnen. Ein Filter ist angewendet, sodass nur die Schwachstellen für diesen Bericht angezeigt werden.
- Die Seite *TLS-Zertifikate* öffnen. Ein Filter ist angewendet, sodass nur die TLS-Zertifikate für diesen Bericht angezeigt werden.
- Die Seite *Leistungsdaten* öffnen. Die Systemleistung für die Dauer des Scans wird angezeigt.
- Einen gefilterten Bericht herunterladen (siehe Kapitel *11.2.2* (Seite 298)).
- ▷ Eine Benachrichtigung zum Senden eines Berichts auslösen (siehe Kapitel *11.2.4* (Seite 299)).

11.2.1.1 Ergebnisse eines Berichts

Der Register *Ergebnisse* enthält eine Liste aller Schwachstellen, die durch die Appliance gefunden wurden (siehe Abb. 11.5).

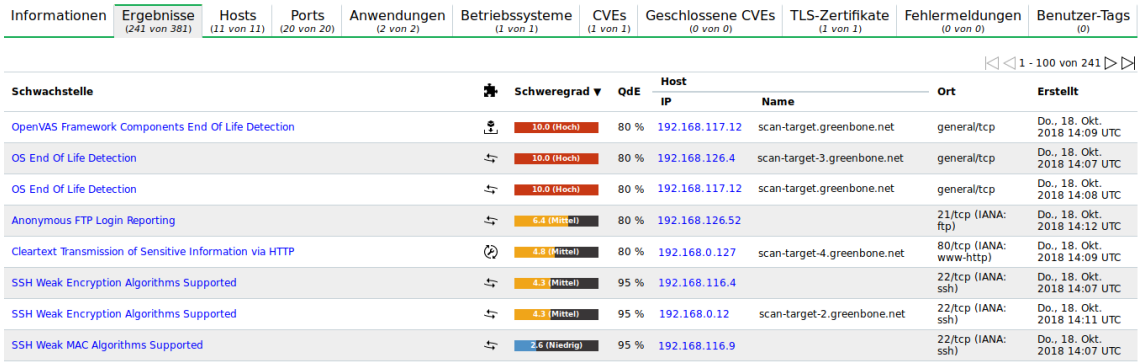


Abb. 11.5: Register *Ergebnisse* mit einer Liste der gefundenen Schwachstellen

---

Bemerkung: Standardmäßig werden Übersteuerungen nicht angewendet. Sie können durch Filtern des Berichts angewendet werden (siehe Kapitel *11.2.1.3* (Seite 297)).

Für jedes Ergebnis werden die folgenden Informationen angezeigt:

Schwachstelle Name der gefundenen Schwachstelle. Durch Klicken auf den Namen der Schwachstelle werden Details der Schwachstelle angezeigt (siehe Abb. 11.6). Durch Klicken auf wird die Detailseite der Schwachstelle geöffnet.

Schwachstellen mit einer angehängten Notiz sind mit gekennzeichnet. Schwachstellen mit einem angehängten Ticket sind mit gekennzeichnet.

Bemerkung: Falls die Spalte der Schwachstelle leer ist, wurde der entsprechende VT noch nicht aktualisiert.

Abb. 11.6: Detaillierte Informationen über die Schwachstelle

Lösungstyp Lösung für die gefundene Schwachstelle. Die folgenden Lösungen sind möglich:

- Eine Herstellerlösung ist verfügbar.
- Eine Problemumgehung ist verfügbar.
- Eine Schadensminderung ist verfügbar.
- Es ist kein Fix verfügbar oder wird verfügbar sein.
- Es ist keine Lösung vorhanden.

Schweregrad Der Schweregrad der Schwachstelle (CVSS, siehe Kapitel *14.2.3* (Seite 363)) wird als Balken angezeigt, um die Analyse der Ergebnisse zu unterstützen.

QdE Die Qualität der Erkennung (QdE) ist ein Wert zwischen 0 % und 100 % und beschreibt die Zuverlässigkeit der ausgeführten Schwachstellen- oder Produkterkennung.

Standardmäßig werden nur Ergebnisse angezeigt, die durch VTs mit einer QdE von 70 % oder höher erkannt wurden. Der Filter kann angepasst werden, sodass auch Ergebnisse mit niedrigerer QdE angezeigt werden (siehe Kapitel *8.3.1* (Seite 168)).

Für mehr Informationen über die QdE siehe Kapitel *11.2.6* (Seite 302).

Host Host, für den das Ergebnis gefunden wurde. Die IP-Adresse und der Name des Hosts werden getrennt voneinander angezeigt.

Ort Zum Entdecken der Schwachstelle auf dem Host genutzte Portnummer und genutzter Protokolltyp.

Erstellt Datum und Zeit der Berichterstellung.

11.2.1.2 Einen Bericht interpretieren

Um die Ergebnisse zu interpretieren, müssen die folgenden Informationen beachtet werden:

- **Falsch-Positiv** Falsch-Positiv Ein Falsch-Positiv-Ergebnis (Falschmeldung) beschreibt ein Ergebnis, das nicht wirklich vorhanden ist. Oft finden Schwachstellenscanner Hinweise, die auf eine Schwachstelle hindeuten, allerdings kann keine endgültige Entscheidung getroffen werden. Es gibt zwei Möglichkeiten:
  - Melden einer potenziell nicht vorhandenen Schwachstelle (falsch-positiv).
  - Ignorieren einer potenziell vorhandenen Schwachstelle (falsch-negativ).

  Da ein Mensch in der Lage ist, Falsch-Positiv-Meldungen zu erkennen und sie somit verwalten und mit ihnen umgehen kann – was für Falsch-Negativ-Meldungen nicht der Fall ist – meldet der Schwachstellenscanner der Appliance alle potenziell vorhandenen Schwachstellen. Falls bekannt ist, dass Falsch-Positiv-Meldungen existieren, kann eine Übersteuerung konfiguriert werden (siehe Kapitel *11.8* (Seite 315)).
- **Mehrere Ergebnisse können dieselbe Ursache haben.** Falls ein besonders altes Softwarepaket installiert ist, existieren oft mehrere Schwachstellen. Jede dieser Schwachstellen wird von einem anderen VT geprüft und löst eine Benachrichtigung aus. Die Installation eines aktuellen Pakets entfernt viele Schwachstellen auf einmal.
- **Hoch** Hoch **und Mittel** Mittel Ergebnisse der Schweregrade *Hoch* und *Mittel* sind am wichtigsten und sollten priorisiert behandelt werden. Bevor Ergebnisse mittleren Schweregrads behandelt werden, sollten Ergebnisse hohen Schweregrads thematisiert werden. Nur in außergewöhnlichen Fällen sollte von diesem Ansatz abgewichen werden, z. B. falls bekannt ist, dass die Ergebnisse mit hohem Schweregrad weniger beachtet werden müssen, da der Dienst durch die Firewall nicht erreichbar ist.

- **Niedrig** Niedrig **und Log** Log Ergebnisse mit dem Schweregrad *Niedrig* und *Log* sind hauptsächlich für das Detailverständnis hilfreich. Diese Ergebnisse werden standardmäßig ausgefiltert, können jedoch interessante Informationen enthalten. Ihr Berücksichtigen erhöht die Sicherheit des Netzwerks und der Systeme. Oftmals ist für ihr Verständnis eine tiefergehende Kenntnis der Anwendung nötig. Typisch für ein Ergebnis mit dem Schweregrad *Log* ist, dass ein Dienst ein Banner mit seinem Namen und seiner Versionsnummer nutzt. Dies kann für Angreifer hilfreich sein, falls diese Versionsnummer eine bekannte Schwachstelle besitzt.

11.2.1.3 Einen Bericht filtern

Da ein Bericht oft viele Ergebnisse enthält, kann sowohl der gesamte als auch ein gefilterter Bericht angezeigt und heruntergeladen werden.

Der Bericht kann wie folgt gefiltert werden:

1. In der Filterleiste auf klicken.
2. Ein Stichwort, nach dem gesucht werden soll, in das Eingabefeld *Filter* eingeben (siehe Abb. 11.7).

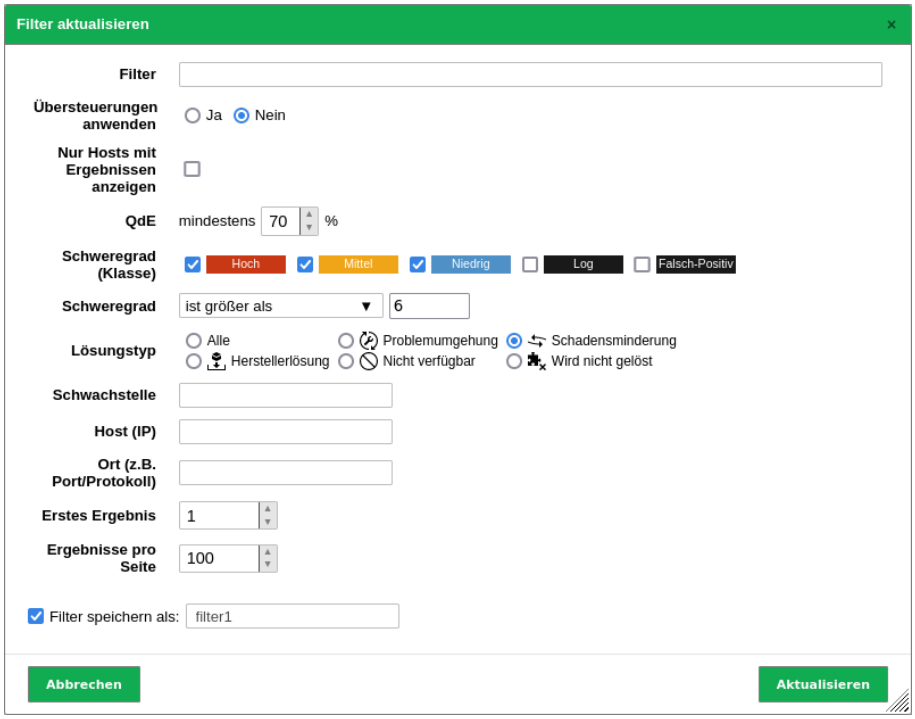


Abb. 11.7: Anpassen des Filters für den Bericht

3. Radiobutton *Ja* für *Übersteuerungen anwenden* wählen, um Übersteuerungen zu aktivieren (siehe Kapitel *11.8* (Seite 315)).

   Radiobutton *Nein* für *Übersteuerungen anwenden* wählen, um Übersteuerungen zu deaktivieren.
4. Checkbox *Nur Hosts mit Ergebnissen anzeigen* aktivieren, falls nur Hosts mit Ergebnissen enthalten sein sollen.
5. Für *QdE* gewünschte QdE wählen (siehe Kapitel *11.2.6* (Seite 302)).
6. Für *Schweregrad (Klasse)* Checkboxen der gewünschten Schweregrade aktivieren.
7. Für *Lösungstyp* Radiobuttons der gewünschten Lösungstypen wählen.
8. (Teil eines) Schwachstellennamens, Hosts oder Orts in das entsprechende Eingabefeld eingeben.

9. *Aktualisieren* klicken.

11.2.2 Einen Bericht exportieren

Für unterstützte Exportformate siehe Kapitel *11.1* (Seite 288).

Ein Bericht kann wie folgt exportiert werden:

1. *Scans* > *Berichte* in der Menüleiste wählen.
2. Details des Berichts durch Klicken auf das Datum eines Berichts anzeigen lassen.
3. Auf klicken.

   → Ein Fenster zum Zusammenstellen des Berichtinhalts wird geöffnet (siehe Abb. 11.8).

Bemerkung: Der angewendete Filter wird im Eingabefeld *Filter* angezeigt und kann nicht verändert werden. Zum Ändern des Filters sieht Kapitel *11.2.1.3* (Seite 297).

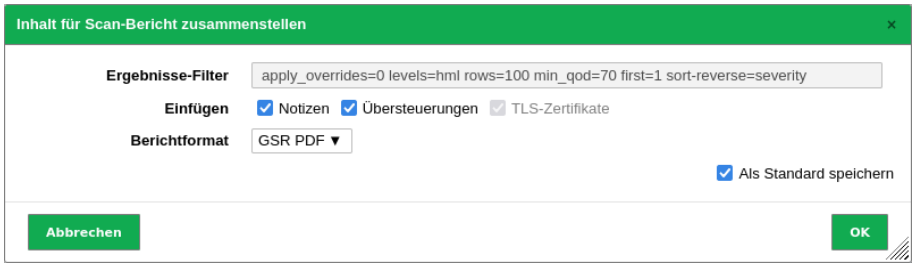


Abb. 11.8: Zusammenstellen des Inhalts eines Berichtexports

4. Checkbox *Notizen* aktivieren, um Notizen hinzuzufügen. Checkbox *Übersteuerungen* aktivieren, um aktivierte Übersteuerungen kennzuzeichnen und den Inhalt ihrer Textfeld einzufügen.

Bemerkung: Übersteuerungen werden nur berücksichtigt, wenn sie beim Filtern des Berichts angewendet werden (siehe Kapitel *11.2.1.3* (Seite 297)).

---

5. Berichtformat in der Drop-down-Liste *Berichtformat* wählen.
6. Einstellungen für zukünftige Exporte durch Aktivieren der Checkbox *Als Standard speichern* speichern.
7. Auf *OK* klicken.
8. Bericht durch Klicken auf *Datei speichern* speichern.

11.2.3 Einen Bericht importieren

Berichte können wie folgt in die Appliance importiert werden:

1. *Scans* > *Berichte* in der Menüleiste wählen.
2. Auf klicken.
3. Auf *Browse. . .* klicken und die XML-Datei des Berichts wählen (siehe Abb. 11.9).
4. Container-Aufgabe, zu der der Bericht hinzugefügt werden soll in der Drop-down-Liste *Containeraufgabe* wählen.

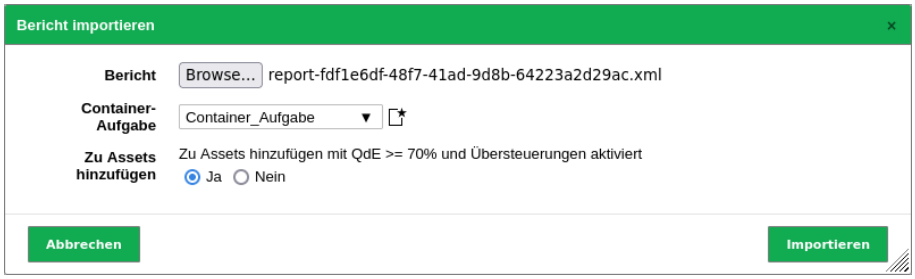


Abb. 11.9: Importieren eines Berichts

Tipp: Durch Klicken auf kann eine neue Container-Aufgabe erstellt werden (siehe Kapitel *10.5* (Seite 252)).

5. Radiobutton *Ja* wählen, um den Bericht zu den Assets hinzuzufügen.
6. Auf *Importieren* klicken.

11.2.4 Eine Benachrichtigung für einen Bericht auslösen

Oft beinhaltet eine Benachrichtigung das Senden eines Berichts. Der Bericht, der durch die Benachrichtigung gesendet wird, unterliegt dem Filter, der beim Erstellen der Benachrichtigung festgelegt wurde (siehe Kapitel *10.12* (Seite 277)). Das Auslösen einer Benachrichtigung für einen Bericht fügt einen zweiten Filter hinzu, der aus dem Zusammenstellen des Berichtinhalts hervorgeht (siehe Kapitel *11.2.2* (Seite 298)).

Die Benachrichtigung kann manuell wie folgt ausgelöst werden:

1. *Scans* > *Berichte* in der Menüleiste wählen.
2. Ergebnisse durch Klicken auf das Datum eines Berichts anzeigen lassen.
3. Bericht mithilfe des Powerfilters (siehe Kapitel *11.2.1.3* (Seite 297)) oder durch Wählen eines Registers filtern, sodass nur die Ergebnisse, die gesendet werden sollen, angezeigt werden.

   Bemerkung: Der Filter, der beim Erstellen der Benachrichtigung konfiguriert wurde (siehe Kapitel *10.12* (Seite 277)), wird automatisch hinzugefügt.

   Um das Verhalten dieses Filters zu imitieren, Filter des Berichts so anpassen, dass keine Ergebnisse herausgefiltert werden.

4. Auf ▷ klicken.

   → Ein Fenster zum Zusammenstellen des Berichtinhalts wird geöffnet (siehe Abb. 11.8).

   Bemerkung: Der angewendete Filter zum Anzeigen der Ergebnisse wird im Eingabefeld *Filter* angezeigt und kann nicht verändert werden. Zum Ändern des Filters siehe *11.2.1.3* (Seite 297).

5. Checkbox *Notizen* aktivieren, um Notizen hinzuzufügen. Checkbox *Übersteuerungen* aktivieren, um aktivierte Übersteuerungen kennzuzeichnen und den Inhalt ihrer Textfeld einzufügen.

   Bemerkung: Übersteuerungen werden nur berücksichtigt, wenn sie beim Filtern des Berichts angewendet werden (siehe Kapitel *11.2.1.3* (Seite 297)).

6. Benachrichtigung in der Drop-down-Liste *Benachrichtigung* wählen.

Tipp: Eine neue Benachrichtigung kann durch Klicken auf erstellt werden. Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *10.12* (Seite 277).

---

7. Einstellungen für zukünftiges Senden des Berichts durch Aktivieren der Checkbox *Als Standard speichern* speichern.
8. Auf *OK* klicken.

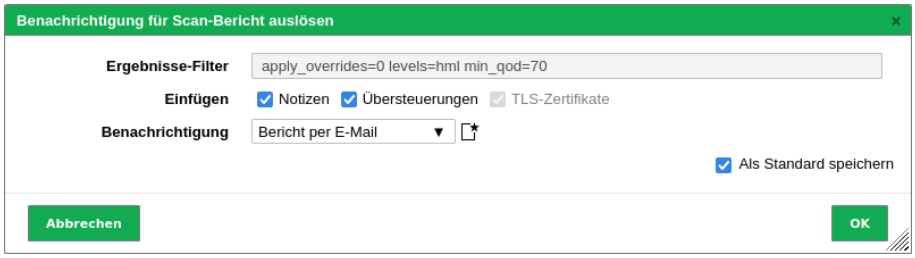


Abb. 11.10: Manuelles Auslösen einer Benachrichtigung

11.2.5 Einen Delta-Bericht erstellen

Falls mehr als ein Bericht für eine einzelne Aufgabe verfügbar ist (siehe Kapitel *11.2* (Seite 293)), kann wie folgt ein Delta-Bericht erstellt werden:

1. *Scans* > *Aufgaben* in der Menüleiste wählen.
2. Auf die Gesamtanzahl der Berichte in der Spalte *Berichte* klicken.

   → Die Seite *Berichte* wird geöffnet. Ein Filter ist angewendet, um nur die Berichte für die gewählte Aufgabe anzuzeigen.
3. Neueren Bericht durch Klicken auf Δ in der Spalte *Aktionen* wählen (siehe Abb. 11.11).

   → Das Icon Δ wird für den gewählten Bericht ausgegraut.

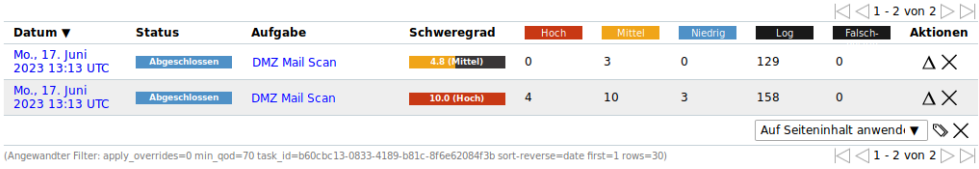


Abb. 11.11: Wählen des ersten Berichts

4. Älteren Bericht durch Klicken auf in der Spalte *Aktionen* wählen (siehe Abb. 11.12).

   → Der Delta-Bericht mit den Delta-Ergebnissen wird angezeigt (siehe Abb. 11.13) und kann exportiert werden.

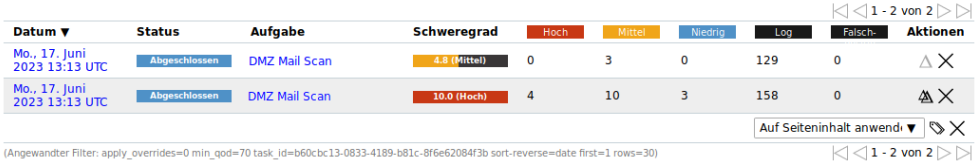


Abb. 11.12: Wählen des zweiten Berichts

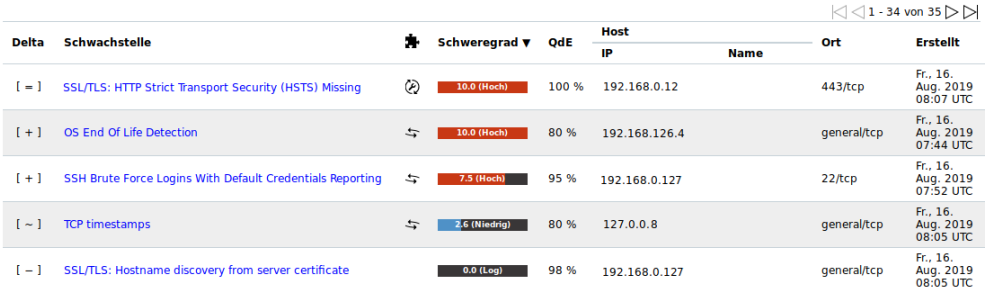


Abb. 11.13: Delta-Bericht mit Delta-Ergebnissen

Der Typ eines Delta-Ergebnisses wird in der Spalte *Delta* dargestellt. Es gibt vier Typen von Delta-Ergebnissen:

- **Entfallen *[–]*** Das Ergebnis ist im zweiten (älteren), aber nicht im ersten (neueren) Bericht vorhanden.
- **Neu *[+]*** Das Ergebnis ist im ersten (neueren), aber nicht im zweiten (älteren) Bericht vorhanden.
- **Gleich *[=]*** Das Ergebnis ist in beiden Berichten vorhanden und gleich.
- **Verändert *[~]*** Das Ergebnis ist in beiden Berichten vorhanden, unterscheidet sich jedoch.

Der Ausdruck `delta_states=` kann in die Filterleiste eingegeben werden, um nur einen bestimmten Typen von Delta-Ergebnissen anzeigen zu lassen (siehe Kapitel *8.3* (Seite 168)).

- `delta_states=g` zeigt alle Ergebnisse des Typs *Entfallen*.
- `delta_states=n` zeigt alle Ergebnisse des Typs *Neu*.
- `delta_states=s` zeigt alle Ergebnisse des Typs *Gleich*.
- `delta_states=c` zeigt alle Ergebnisse des Typs *Verändert*.

Tipp: Mehrere Typen können zeitgleich angezeigt werden, z. B. zeigt `delta_states=gs` alle Ergebnisse des Typs *Entfallen* und *Gleich* .

11.2.6 Konzept der Qualität der Erkennung

Die Qualität der Erkennung (QdE) ist ein Wert zwischen 0 % und 100 % und beschreibt die Zuverlässigkeit der ausgeführten Schwachstellen- oder Produkterkennung.

Obwohl der QdE-Bereich es erlaubt, die Qualität detailgenau darzustellen, nutzen die meisten Prüfroutinen eine Standardmethodik. Deshalb werden den QdE-Werten QdE-Typen zugewiesen. Die aktuelle Typenliste wird möglicherweise mit der Zeit erweitert.

Bemerkung:

- Die QdE eines „Erkennungs“-Ergebnisses ist höher als die eines tatsächlichen „Schwachstellen“-Ergebnisses, da sie die Qualität der Produkterkennung selbst widerspiegelt – die zuverlässig ist – und nicht die Qualität der zugehörigen Schwachstellentests, die aus verschiedenen Gründen unzuverlässig sein können (siehe Tabelle).
- Es wird immer die niedrigste verfügbare QdE verwendet, beispielsweise im Falle mehrerer Erkennungsmethoden (remote oder lokal/authentifiziert).

QdE	QdE-Typ	Beschreibung
100 %	exploit	Die Erkennung erfolgte durch die Ausnutzung einer Sicherheitslücke und ist daher vollständig bestätigt.
99 %	remote_vul	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort eindeutig das Vorhandensein der Schwachstelle zeigt.
98 %	remote_app	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort eindeutig das Vorhandensein der gefährdeten Anwendung zeigt.
97 %	package	Authentifizierte paketbasierte Prüfungen für z. B. Linux(oide) Systeme.
97 %	registry	Authentifizierte Prüfungen auf Basis der Registry von Microsoft Windows.
95 %	remote_active	Aktive Prüfung auf dem Zielsystem (Codeausführung, Traversal-Angriff, SQL-Einschleusung etc.), bei welcher die Antwort das wahrscheinliche Vorhandensein der gefährdeten Anwendung oder der Schwachstelle zeigt. „Wahrscheinlich“ bedeutet, dass die Erkennung nur in seltenen Fällen inkorrekt ist.
80 %	remote_banner	Prüfung von Anwendungsbannern auf dem Zielsystem, die den Patch-Status als Information anbieten. Zum Beispiel ist dies für viele proprietäre Produkte der Fall.
80 %	executable_version	Authentifizierte Versionsprüfung über eine ausführbare Datei für Linux(oide) und Microsoft Windows Systeme, bei denen Anwendungen den Patch-Status in der Version anbieten.
75 %		Wenn Ergebnisse ohne QdE-Informationen verarbeitet werden (z. B. bei der Migration von Daten aus einem Altsystem in ein aktuell unterstütztes System), wird ihnen dieser Wert zugewiesen.

QdE	QdE-Typ	Beschreibung
70 %	remote_analysis	Prüfungen auf dem Zielsystem, die einige Analysen durchführen, jedoch je nach Umgebungsbedingungen nicht immer vollständig zuverlässig sind. Die Eingrenzung von vermuteten falsch-positiven oder falsch-negativen Sonderfällen kann eine Analyse durch den Nutzer erfordern (siehe Kapitel *11.8* (Seite 315)).
50 %	remote_probe	Prüfung auf dem Zielsystem, bei welcher zwischenliegende Systeme wie Firewalls die korrekte Erkennung vortäuschen können, sodass nicht eindeutig ist, ob die Anwendung selbst geantwortet hat. Zum Beispiel kann dies für Verbindungen ohne TLS geschehen.
30 %	remote_banner_unreliable	Prüfung von Anwendungsbannern des Zielsystems, die den Patch-Status nicht als Information anbieten. Zum Beispiel ist dies für viele Open-Source-Produkte aufgrund von Backport-Patches der Fall.
30 %	executable_version_unreliable	Authentifizierte Versionsprüfung über eine ausführbare Datei für Linux(oide) Systeme, bei denen Anwendungen den Patch-Status nicht in der Version anbieten.
30 %	package_unreliable	Authentifizierte paketbasierte Prüfungen, die nicht immer vollständig zuverlässig sind, für z. B. Linux(oide) Systeme.
1 %	general_note	Allgemeine Notiz zu einer potenziellen Schwachstelle ohne konkrete Erkennung einer vorhandenen Anwendung.

Standardmäßig werden nur Ergebnisse angezeigt, die durch VTs mit einer QdE von 70 % oder höher erkannt wurden. Ergebnisse, die von einem Test mit einer niedrigeren QdE erkannt werden, sind anfällig für Falsch-Positiv-Ergebnisse. Der Filter kann angepasst werden, sodass auch Ergebnisse mit niedrigerer QdE angezeigt werden (siehe Kapitel *8.3.1* (Seite 168)).

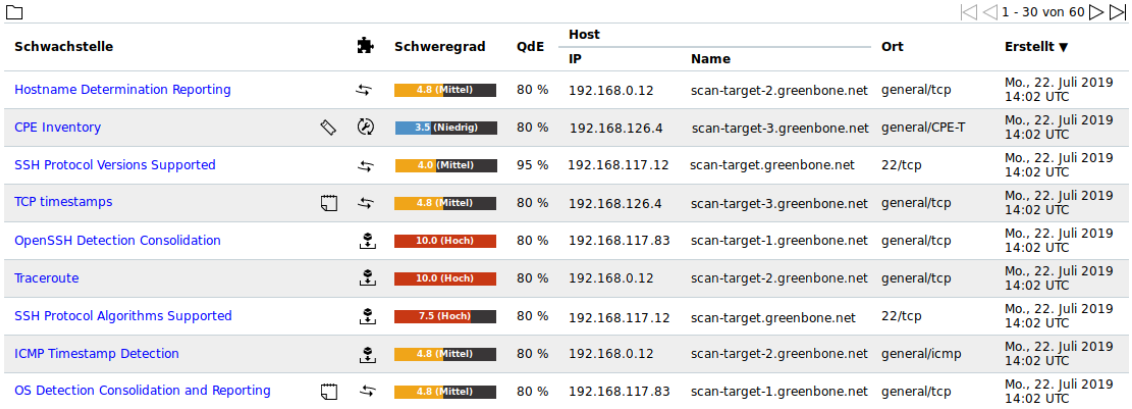
Bemerkung: Wenn der Standardfilter geändert wird, um Ergebnisse anzuzeigen, die von einem Test mit einer niedrigen QoD erkannt wurden, liegt es in der eigenen Verantwortung, festzustellen, ob es sich um ein Falsch-Positiv-Ergebnis handelt.

11.3 Alle vorhandenen Ergebnisse anzeigen

Listenseite

Während ein Bericht nur die Ergebnisse eines einzelnen Scans beinhaltet, werden alle Ergebnisse in der internen Datenbank gespeichert und können durch Wählen von *Scans* > *Ergebnisse* in der Menüleiste angezeigt werden.

Powerfilter können genutzt werden, um nur Ergebnisse von Interesse darzustellen (siehe Kapitel *8.3* (Seite 168)).



Schwachstelle	Schweregrad	QdE	Host IP	Host Name	Ort	Erstellt ▼
Hostname Determination Reporting	4.8 (Mittel)	80 %	192.168.0.12	scan-target-2.greenbone.net	general/tcp	Mo., 22. Juli 2019 14:02 UTC
CPE Inventory	3.5 (Niedrig)	80 %	192.168.126.4	scan-target-3.greenbone.net	general/CPE-T	Mo., 22. Juli 2019 14:02 UTC
SSH Protocol Versions Supported	4.0 (Mittel)	95 %	192.168.117.12	scan-target.greenbone.net	22/tcp	Mo., 22. Juli 2019 14:02 UTC
TCP timestamps	4.8 (Mittel)	80 %	192.168.126.4	scan-target-3.greenbone.net	general/tcp	Mo., 22. Juli 2019 14:02 UTC
OpenSSH Detection Consolidation	10.0 (Hoch)	80 %	192.168.117.83	scan-target-1.greenbone.net	general/tcp	Mo., 22. Juli 2019 14:02 UTC
Traceroute	10.0 (Hoch)	80 %	192.168.0.12	scan-target-2.greenbone.net	general/tcp	Mo., 22. Juli 2019 14:02 UTC
SSH Protocol Algorithms Supported	7.5 (Hoch)	80 %	192.168.117.12	scan-target.greenbone.net	22/tcp	Mo., 22. Juli 2019 14:02 UTC
ICMP Timestamp Detection	4.8 (Mittel)	80 %	192.168.0.12	scan-target-2.greenbone.net	general/icmp	Mo., 22. Juli 2019 14:02 UTC
OS Detection Consolidation and Reporting	4.8 (Mittel)	80 %	192.168.117.83	scan-target-1.greenbone.net	general/tcp	Mo., 22. Juli 2019 14:02 UTC

Abb. 11.14: Seite *Ergebnisse* mit allen Ergebnissen aller Scans

Für alle Ergebnisse werden die folgenden Informationen angezeigt:

Schwachstelle Name der gefundenen Schwachstelle.

Schwachstellen mit einer angehängten Notiz sind mit gekennzeichnet. Schwachstellen mit einem angehängten Ticket sind mit gekennzeichnet.

Bemerkung: Falls die Spalte der Schwachstelle leer ist, wurde der entsprechende VT noch nicht aktualisiert.

Bemerkung: Obwohl die Ergebnisse viele Informationen beinhalten, werden in den Details immer externe Referenzen aufgelistet.

Diese beziehen sich auf Webseiten, auf denen die Schwachstelle bereits diskutiert wurde.

Zusätzliche Hintergrundinformationen sind verfügbar, wie der Entdecker, die Auswirkungen und die Beseitigung der Schwachstelle.

Lösungstyp Um die Beseitigung einer Schwachstelle zu erleichtern, bietet jedes Ergebnis eine Lösung für das Problem. Die Spalte *Art der Lösung* zeigt das Vorhandensein einer Lösung. Die folgenden Lösungen sind möglich:

- Eine Herstellerlösung ist verfügbar.
- Eine Problemumgehung ist verfügbar.
- Eine Schadensminderung ist verfügbar.
- Es ist kein Fix verfügbar oder wird verfügbar sein.
- Es ist keine Lösung vorhanden.

Schweregrad Der Schweregrad der Schwachstelle (CVSS, siehe Kapitel *14.2.3* (Seite 363)) wird als Balken angezeigt, um die Analyse der Ergebnisse zu unterstützen.

QdE Die Qualität der Erkennung (QdE) ist ein Wert zwischen 0 % und 100 % und beschreibt die Zuverlässigkeit der ausgeführten Schwachstellen- oder Produkterkennung.

Standardmäßig werden nur Ergebnisse angezeigt, die durch VTs mit einer QdE von 70 % oder höher erkannt wurden. Der Filter kann angepasst werden, sodass auch Ergebnisse mit niedrigerer QdE angezeigt werden (siehe Kapitel *8.3.1* (Seite 168)).

Für mehr Informationen über die QdE siehe Kapitel *11.2.6* (Seite 302).

Host Host, für den das Ergebnis gefunden wurde. Die IP-Adresse und der Name des Hosts werden getrennt voneinander angezeigt.

Ort Zum Entdecken des Ergebnisses auf dem Host genutzte Portnummer und genutzter Protokolltyp.

Erstellt Datum und Zeit der Berichterstellung.

Bemerkung: Durch Klicken auf unterhalb der Liste von Ergebnissen können mehrere Ergebnisse zur gleichen Zeit exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Ergebnisse exportiert werden.

Detailseite

Durch Klicken auf den Namen eines Ergebnisses werden Details des Ergebnisses angezeigt. Durch Klicken auf wird die Detailseite des Ergebnisses geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das Ergebnis.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

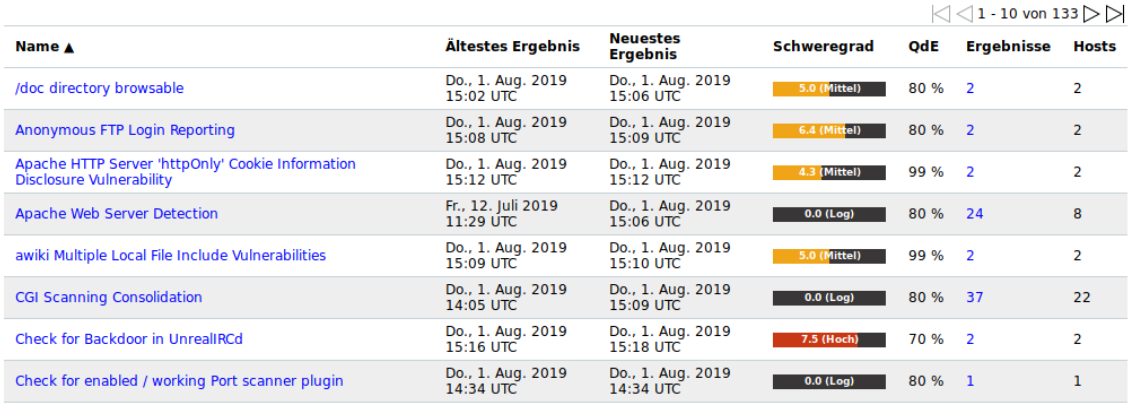
- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Ergebnissen anzeigen.
- Die Ergebnisse als XML-Datei exportieren.
- Eine neue Notiz für das Ergebnis erstellen (siehe Kapitel *11.7.1* (Seite 312)).
- Eine neue Übersteuerung für das Ergebnis erstellen (siehe Kapitel *11.8.1* (Seite 315)).
- Ein neues Ticket für das Ergebnis erstellen (siehe Kapitel *11.6.1* (Seite 308)).
- Die zugehörige Aufgabe anzeigen.
- Den zugehörigen Bericht anzeigen.

11.4 Alle vorhandenen Schwachstellen anzeigen

Listenseite

Während ein Bericht nur die Schwachstellen eines einzelnen Scans beinhaltet, werden alle Schwachstellen in der internen Datenbank gespeichert und können durch Wählen von *Scans > Schwachstellen* in der Menüleiste angezeigt werden.

Powerfilter können genutzt werden, um nur Schwachstellen von Interesse darzustellen (siehe Kapitel *8.3* (Seite 168)).



1 - 10 von 133

Name ▲	Ältestes Ergebnis	Neuestes Ergebnis	Schweregrad	QdE	Ergebnisse	Hosts
/doc directory browsable	Do., 1. Aug. 2019 15:02 UTC	Do., 1. Aug. 2019 15:06 UTC	5.0 (Mittel)	80 %	2	2
Anonymous FTP Login Reporting	Do., 1. Aug. 2019 15:08 UTC	Do., 1. Aug. 2019 15:09 UTC	6.4 (Mittel)	80 %	2	2
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	Do., 1. Aug. 2019 15:12 UTC	Do., 1. Aug. 2019 15:12 UTC	4.3 (Mittel)	99 %	2	2
Apache Web Server Detection	Fr., 12. Juli 2019 11:29 UTC	Do., 1. Aug. 2019 15:06 UTC	0.0 (Log)	80 %	24	8
awiki Multiple Local File Include Vulnerabilities	Do., 1. Aug. 2019 15:09 UTC	Do., 1. Aug. 2019 15:10 UTC	5.0 (Mittel)	99 %	2	2
CGI Scanning Consolidation	Do., 1. Aug. 2019 14:05 UTC	Do., 1. Aug. 2019 15:09 UTC	0.0 (Log)	80 %	37	22
Check for Backdoor in UnrealIRCd	Do., 1. Aug. 2019 15:16 UTC	Do., 1. Aug. 2019 15:18 UTC	7.5 (Hoch)	70 %	2	2
Check for enabled / working Port scanner plugin	Do., 1. Aug. 2019 14:34 UTC	Do., 1. Aug. 2019 14:34 UTC	0.0 (Log)	80 %	1	1

Abb. 11.15: Seite *Schwachstellen* mit allen Schwachstellen aller Scans

Für alle Schwachstellen werden die folgenden Informationen angezeigt:

Name Titel der Schwachstelle.

Ältestes Ergebnis Datum und Zeit des ältesten Ergebnisses, das für die Schwachstelle gefunden wurde.

Neuestes Ergebnis Datum und Zeit des neuesten Ergebnisses, das für die Schwachstelle gefunden wurde.

Schweregrad Der Schweregrad der Schwachstelle (CVSS, siehe Kapitel *14.2.3* (Seite 363)) wird als Balken angezeigt, um die Analyse der Ergebnisse zu unterstützen.

QdE Die Qualität der Erkennung (QdE) ist ein Wert zwischen 0 % und 100 % und beschreibt die Zuverlässigkeit der ausgeführten Schwachstellen- oder Produkterkennung.

Standardmäßig werden nur Ergebnisse angezeigt, die durch VTs mit einer QdE von 70 % oder höher erkannt wurden. Der Filter kann angepasst werden, sodass auch Ergebnisse mit niedrigerer QdE angezeigt werden (siehe Kapitel *8.3.1* (Seite 168)).

Für mehr Informationen über die QdE siehe Kapitel *11.2.6* (Seite 302).

Ergebnisse Anzahl der Ergebnisse, die für diese Schwachstelle gefunden wurden. Durch Klicken auf die Anzahl wird die Seite *Ergebnisse* geöffnet. Ein Filter ist angewendet, um nur die Ergebnisse für die gewählte Schwachstelle anzuzeigen.

Bemerkung: Durch Klicken auf unterhalb der Liste von Ergebnissen können mehrere Ergebnisse zur gleichen Zeit exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Ergebnisse exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Schwachstelle wird die Detailseite der Schwachstelle geöffnet.

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Schwachstellen anzeigen.
- Die Schwachstelle als XML-Datei exportieren.
- Eine neue Notiz für die Schwachstelle erstellen (siehe Kapitel *11.7.1* (Seite 312)).
- Eine neue Übersteuerung für die Schwachstelle erstellen (siehe Kapitel *11.8.1* (Seite 315)).
- Die dazugehörigen Ergebnisse anzeigen.
- Die zugehörige Schwachstelle anzeigen.

11.5 Trend einer Schwachstelle

Falls eine Aufgabe mehrere Male durchgeführt wurde, wird der Trend der gefundenen Schwachstellen auf der Seite *Aufgaben* angezeigt (siehe Abb. 11.16).

Abb. 11.16: Aufgabe mit Trend

Um dorthin zu gelangen, *Scans* > *Aufgaben* in der Menüleiste wählen.

Der Trend beschreibt die Änderung der Schwachstellen zwischen dem neuesten und zweitneuesten Bericht. Er wird in der Spalte *Trend* angezeigt.

Die folgenden Trends sind möglich:

- Im neuesten Bericht ist der höchste Schweregrad höher als der höchste Schweregrad im zweitneuesten Bericht.
- Der höchste Schweregrad ist für beide Berichte gleich. Trotzdem enthält der neueste Bericht mehr Sicherheitsprobleme dieses Schweregrads als der zweitneueste Bericht.
- Der höchste Schweregrad und die Anzahl an Sicherheitsproblemen ist für beide Berichte gleich.
- Der höchste Schweregrad ist für beide Berichte gleich. Trotzdem enthält der neueste Bericht weniger Sicherheitsprobleme dieses Schweregrads als der zweitneueste Bericht.
- Im neuesten Bericht ist der höchste Schweregrad kleiner als der höchste Schweregrad im zweitneuesten Bericht.

11.6 Tickets nutzen

Benutzer können andere Benutzer oder sich selbst mit der Beseitigung eines Scanergebnisses beauftragen.

Bemerkung: Wenn ein Ticket für einen anderen Benutzer erstellt wird, erhält dieser Benutzer Lese- und Schreibzugriff auf das Ticket. Außerdem erhält der Benutzer automatisch Lesezugriff auf die entsprechende Aufgabe sowie deren Berichte und Ergebnisse.

Wenn einem Benutzer die Zuweisung eines Tickets entzogen wird, bleibt der Lesezugriff auf die Aufgabe und die Berichte erhalten. Die Berechtigungen für eine Aufgabe können auf der Detailseite einer Aufgabe überprüft und entzogen werden (siehe Kapitel *10.8* (Seite 257)). Wenn mehrere Tickets für Ergebnisse desselben Berichts erstellt und demselben Benutzer zugewiesen werden, erscheint dieselbe Berechtigung mehrfach.

Wenn der Bearbeiter eines Tickets geändert wird, erhält der neue Bearbeiter nicht automatisch Lesezugriff auf die Aufgabe. Stattdessen muss der Ticketbesitzer die Berechtigungen auf der Detailseite der Aufgabe bearbeiten (siehe Kapitel *10.8* (Seite 257)) und dem neuen Bearbeiter Lesezugriff gewähren.

11.6.1 Ein neues Ticket erstellen

Ein Ticket kann wie folgt erstellt werden:

1. *Scans* > *Berichte* in der Menüleiste wählen und Ergebnisse durch Klicken auf das Datum eines Berichts anzeigen lassen.
2. Auf ein Objekt in der Spalte *Schwachstelle* und auf klicken, um die Detailseite des Ergebnisses zu öffnen.

   oder

1. *Scans* > *Ergebnisse* in der Menüleiste wählen.
2. Auf ein Objekt in der Spalte *Schwachstelle* und auf klicken, um die Detailseite des Ergebnisses zu öffnen.
3. Neues Ticket durch Klicken auf erstellen.
4. Benutzer, dem das Ticket zugewiesen werden soll, in der Drop-down-Liste *Benutzer zuweisen* wählen (siehe Abb. 11.17).
5. Notiz für das Ticket in das Eingabefeld *Notiz* eingeben.

Abb. 11.17: Erstellen eines neuen Tickets

6. Auf *Speichern* klicken.

   → Die Anzahl an Tickets für ein Ergebnis werden in der linken oberen Ecke der Detailseite angezeigt (siehe Abb. 11.18). Durch Klicken auf werden die zugehörigen Tickets angezeigt.

Abb. 11.18: Anzahl zugewiesener Tickets

11.6.2 Den Status eines Tickets ändern

Ein Ticket kann die folgenden Status haben:

- Offen: Die Schwachstelle wurde noch nicht beseitigt.
- Behoben: Die Schwachstelle wurde behoben.
- Behoben und verifiziert: Die Aufgabe wurde noch einmal durchgeführt und die Schwachstelle wurde nicht mehr gefunden. Dieser Status wird automatisch vergeben.
- Geschlossen: Die Behebung der Schwachstelle wurde verifiziert oder das Ticket wird nicht mehr benötigt.

Der Status eines Tickets kann wie folgt geändert werden:

1. *Resilience* > *Remediation Tickets* in der Menüleiste wählen.
2. In der Zeile des Tickets auf klicken.
3. Neuen Status in der Drop-down-Liste *Status* wählen (siehe Abb. 11.19).
4. Benutzer, dem das Ticket mit dem neuen Status zugewiesen werden soll, in der Drop-down-Liste *Zugewiesener Benutzer* wählen.
5. Notiz für den neuen Status in das entsprechende Eingabefeld eingeben.

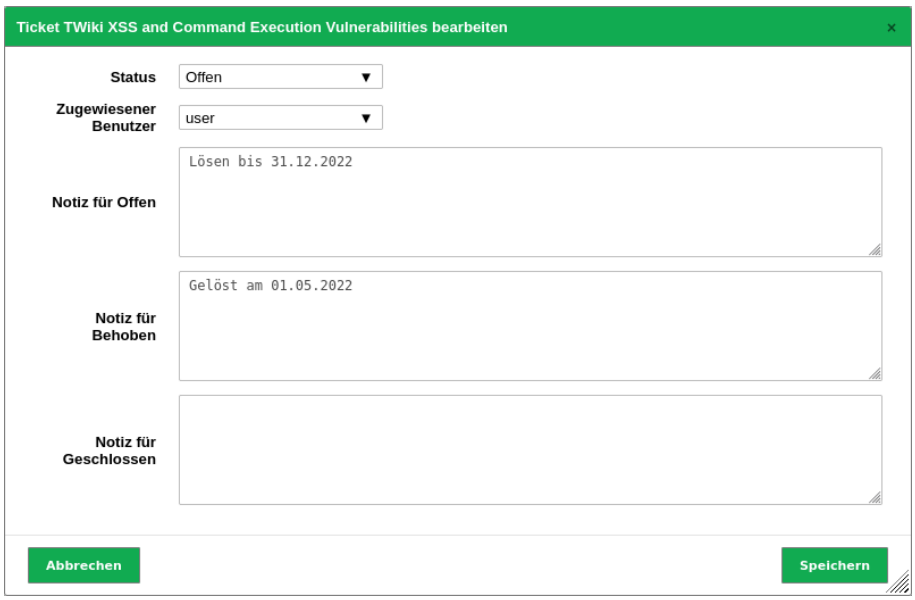


Abb. 11.19: Ändern des Status eines Tickets

6. Auf *Speichern* klicken.

11.6.3 Eine Benachrichtigung für ein Ticket einrichten

Benachrichtigungen für Tickets können für die folgenden Ereignisse eingerichtet werden:

- Ein neues Ticket wurde erhalten.
- Der Status eines zugewiesenen Tickets hat sich verändert.
- Der Status eines eigenen Tickets hat sich verändert.

Eine Benachrichtigung für ein Ticket wird wie folgt eingerichtet:

1. *Konfiguration* > *Benachrichtigungen* in der Menüleiste wählen.
2. Neue Benachrichtigung durch Klicken auf erstellen.
3. Benachrichtigung definieren (siehe Abb. 11.20).
4. Auf *Speichern* klicken.

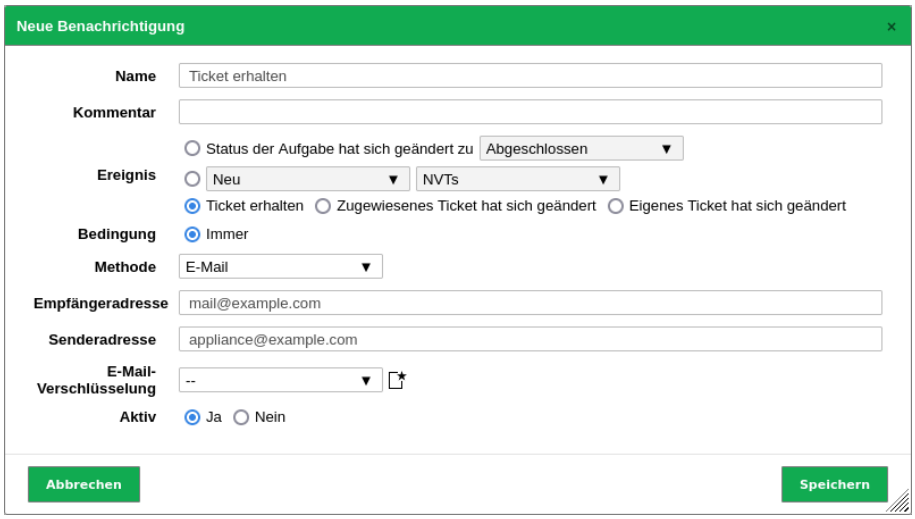


Abb. 11.20: Einrichten einer Benachrichtigung für ein Ticket

Die folgenden Details der Benachrichtigung können festgelegt werden:

Name Festlegen des Namens. Der Name kann frei gewählt werden.

Kommentar Ein optionaler Kommentar kann zusätzliche Informationen enthalten.

Ereignis *Ticket erhalten* wählen, falls eine Benachrichtigung gesendet werden soll, wenn einem selbst ein neues Ticket zugewiesen wird.

Zugewiesenes Ticket hat sich geändert wählen, falls eine Benachrichtigung gesendet werden soll, wenn sich der Status eines zugewiesenen Tickets ändert.

Eigenes Ticket hat sich geändert wählen, falls eine Benachrichtigung gesendet werden soll, wenn sich der Status eines Tickets ändert, das einem anderen Benutzer zugewiesen wurde.

Methode Auswahl der Methode für die Benachrichtigung. Pro Benachrichtigung kann nur eine Methode gewählt werden.

Falls unterschiedliche Benachrichtigungen für das gleiche Ereignis ausgelöst werden sollen, müssen mehrere Benachrichtigungen erstellt und der gleichen Aufgabe zugewiesen werden.

Die folgenden Methoden sind möglich:

E-Mail Eine E-Mail wird an die angegebene Adresse gesendet.

Die Übertragung der E-Mail kann mithilfe eines S/MIME-Zertifikats oder eines PGP-Verschlüsselungsschlüssel verschlüsselt sein. Die Verschlüsselung kann in der Drop-down-Liste *E-Mail-Verschlüsselung* gewählt oder durch Klicken auf erstellt werden.

Aufgabe starten Die Benachrichtigung kann eine zusätzliche Aufgabe starten. Die Aufgabe wird in der Drop-down-Liste *Aufgabe starten* gewählt.

System-Logger Eine Benachrichtigung wird an einen Syslog-Daemon gesendet.

Der Syslog-Server wird mithilfe der Konsole festgelegt (siehe Kapitel *7.2.12* (Seite 133)).

11.6.4 Tickets verwalten

Listenseite

Alle vorhandenen Tickets können angezeigt werden, indem *Resilience > Remediation Tickets* in der Menüleiste gewählt wird.

Für alle Tickets werden die folgenden Informationen angezeigt:

Schwachstelle Schwachstelle, für die das Ticket erstellt wurde.

Schweregrad Schweregrad der Schwachstelle, für die das Ticket erstellt wurde.

Host Host, für den die Schwachstelle gefunden wurde.

Lösungstyp Art der Lösung für die Schwachstelle, für die das Ticket erstellt wurde.

Zugewiesener Benutzer Benutzer, dem das Ticket zugewiesen wurde.

Änderungszeit Datum und Zeit der letzten Veränderung des Tickets.

Status Status des Tickets.

Für alle Tickets sind die folgenden Aktionen verfügbar:

- Das Ticket in den Papierkorb verschieben. Nur der Ticketbesitzer kann ein Ticket in den Papierkorb verschieben.
- Das Ticket bearbeiten.
- Das Ticket klonen.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Tickets können mehrere Tickets zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Tickets in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen eines Tickets werden Details des Tickets angezeigt. Durch Klicken auf wird die Detailseite des Tickets geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das Ticket.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Tickets anzeigen.
- Das Ticket klonen.

- Das Ticket bearbeiten.
- Das Ticket in den Papierkorb verschieben. Nur der Ticketbesitzer kann ein Ticket in den Papierkorb verschieben.
- Das Ticket als XML-Datei exportieren.

11.7 Notizen nutzen

Notizen ermöglichen das Hinzufügen von Kommentaren zu einem VT und werden auch in den Berichten angezeigt. Eine Notiz kann einem Ergebnis, einer Aufgabe, einem Schweregrad, einem Port oder einem Host hinzugefügt werden und erscheint somit nur in bestimmten Berichten.

11.7.1 Eine Notiz erstellen

11.7.1.1 Eine Notiz über ein Scanergebnis erstellen

Notizen können auf unterschiedliche Arten erstellt werden. Der einfachste Weg ist das Erstellen über das entsprechende Scanergebnis in einem Bericht:

1. *Scans* > *Berichte* in der Menüleiste wählen.
2. Ergebnisse durch Klicken auf das Datum eines Berichts anzeigen lassen.
3. Register *Ergebnisse* wählen.
4. Auf ein Ergebnis in der Spalte *Schwachstelle* klicken.
5. Detailseite des Ergebnisses durch Klicken auf öffnen.
6. Auf in der linken oberen Ecke der Seite klicken.
7. Notiz definieren (siehe Abb. 11.21).

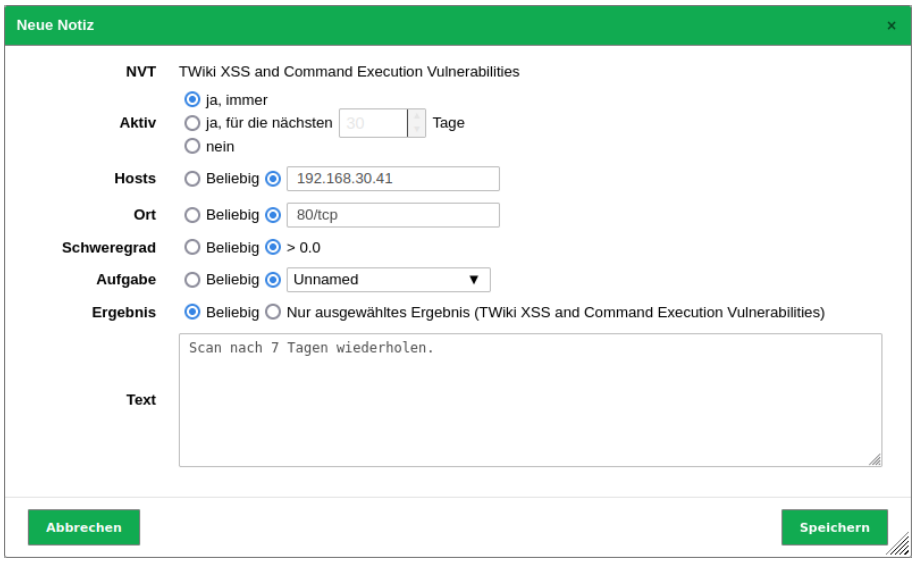


Abb. 11.21: Erstellen einer neuen Notiz

8. Auf *Speichern* klicken.

   → Die Notiz wird auf der Detailseite des Ergebnisses angezeigt (siehe Abb. 11.22).

Abb. 11.22: Bericht mit einer Notiz

11.7.1.2 Eine Notiz auf der Seite *Notizen* erstellen

Notizen können auch auf der Seite *Notizen* erstellt werden:

1. *Scans* > *Notizen* in der Menüleiste wählen.
2. Neue Notiz durch Klicken auf erstellen.
3. ID des VTs in das Eingabefeld *NVT-OID* eingeben.
4. Notiz definieren.

   Tipp: Es ist möglich, Bereiche von IP-Adressen oder CIDR-Blöcke in das Eingabefeld *Hosts* einzugeben. Auf diesem Weg können Notizen für gesamte Teilnetze erstellt werden, ohne dass jeder Host in einer kommagetrennten Liste aufgeführt werden muss.

   Notizen können durch Wählen des Radiobuttons *Beliebig* für Hosts, Orte, Schweregrade, Aufgaben oder Ergebnisse generalisiert werden.

   ---

5. Auf *Speichern* klicken.

11.7.2 Notizen verwalten

Listenseite

Alle vorhandenen Notizen können angezeigt werden, indem *Scans* > *Notizen* in der Menüleiste gewählt wird (siehe Abb. 11.23).

Für alle Notizen sind die folgenden Aktionen verfügbar:

- Die Notiz in den Papierkorb verschieben.
- Die Notiz bearbeiten.
- Die Notiz klonen.
- Die Notiz als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Notizen können mehrere Notizen zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Notizen in den Papierkorb verschoben oder exportiert werden.

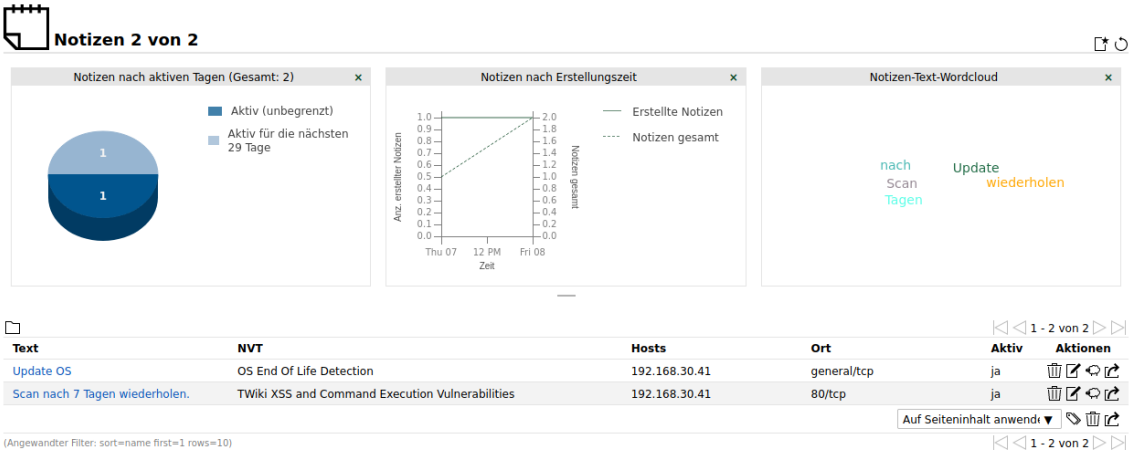


Abb. 11.23: Verwalten von Notizen

Detailseite

Durch Klicken auf den Namen einer Notiz werden Details der Notiz angezeigt. Durch Klicken auf wird die Detailseite der Notiz geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Notiz.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Notizen anzeigen.
- Eine neue Notiz erstellen (siehe Kapitel *11.7.1* (Seite 312)).
- Die Notiz klonen.
- Die Notiz bearbeiten.
- Die Notiz in den Papierkorb verschieben.
- Die Notiz als XML-Datei exportieren.

11.8 Übersteuerungen und Falsch-Positiv-Meldungen nutzen

Der Schweregrad eines Ergebnisses kann verändert werden. Dies wird Übersteuerung genannt.

Übersteuerungen sind insbesondere nützlich, um Ergebnisse zu verwalten, die als falsch-positiv erkannt wurden oder denen ein kritischer Schweregrad zugeordnet wurde, wobei der Schweregrad zukünftig ein anderer sein soll.

Das gleiche gilt für Ergebnisse, denen der Schweregrad *Log* zugeordnet wurde, die lokal aber einen höheren Schweregrad haben sollen. Dies kann auch mithilfe von Übersteuerungen verwaltet werden.

Übersteuerungen werden auch zum Verwalten vertretbarer Risiken gentuzt.

11.8.1 Eine Übersteuerung erstellen

11.8.1.1 Eine Übersteuerung über ein Scanergebnis erstellen

Übersteuerungen können auf unterschiedliche Arten erstellt werden. Der einfachste Weg ist das Erstellen über das entsprechende Scanergebnis in einem Bericht:

1. *Scans* > *Berichte* in der Menüleiste wählen.
2. Ergebnisse durch Klicken auf das Datum eines Berichts anzeigen lassen.
3. Register *Ergebnisse* wählen.
4. Auf ein Ergebnis in der Spalte *Schwachstelle* klicken.
5. Detailseite des Ergebnisses durch Klicken auf 🔍 öffnen.
6. Auf 🪄 in der linken oberen Ecke der Seite klicken.
7. Übersteuerung definieren. Neuen Schweregrad in der Drop-down-Liste *Neuer Schweregrad* wählen (siehe Abb. 11.24).

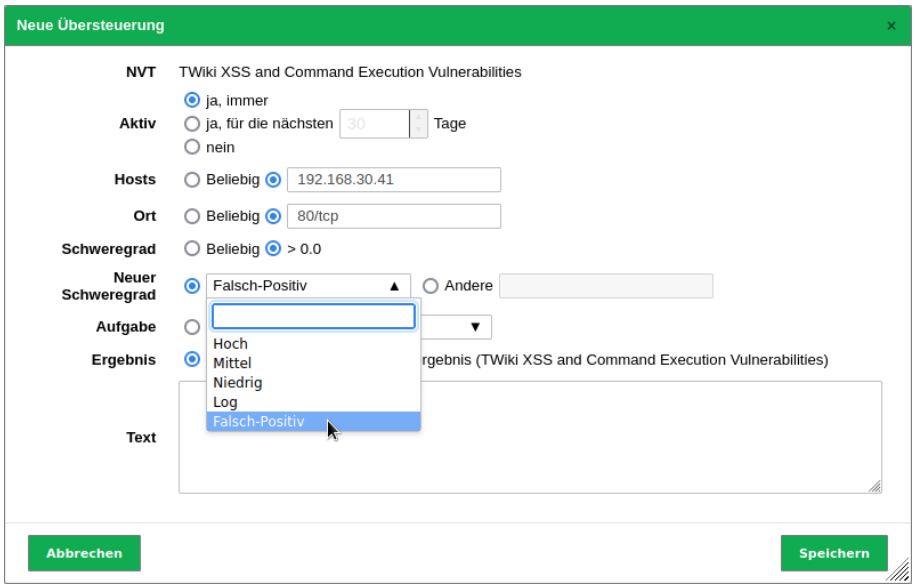


Abb. 11.24: Erstellen einer neuen Übersteuerung

8. Auf *Speichern* klicken.

Die folgenden Informationen können eingegeben werden:

Bemerkung: Falls die Übersteuerung über ein Scanergebnis erstellt wird, sind einige Einstellungen bereits ausgefüllt.

NVT VT, für den die Übersteuerung angewendet wird.

Aktiv Wahl, ob die Übersteuerung aktiviert werden soll. Eine Aktivierung für eine beliebige Anzahl an Tagen ist möglich.

Hosts Host oder Bereich von Hosts, für den das Ergebnis gefunden werden muss, damit die Übersteuerung angewendet wird.

> **Tipp:** Es ist möglich, Bereiche von IP-Adressen oder CIDR-Blöcke einzugeben. Auf diesem Weg können Übersteuerungen für gesamte Teilnetze erstellt werden, ohne dass jeder Host in einer kommagetrennten Liste aufgeführt werden muss.
>
> Hostbereiche werden mit einem Minus angegeben, z. B. `198.168.1.1-198.168.1.25`. Bereiche größer als 4096 werden nicht unterstützt.

> **Bemerkung:** Widersprüchliche Übersteuerungen, z. B. eine Übersteuerung für einen Hostbereich und eine andere Übersteuerung für einen Host in diesem Bereich, sind nicht zulässig.

Ort Port, für den das Ergebnis gefunden werden muss, damit die Übersteuerung angewendet wird. Nur ein spezifischer Port oder die Einstellung *Beliebig* werden pro Übersteuerung unterstützt. Ein konkreter Port muss als Zahl gefolgt von `/tcp` oder `/udp` eingegeben werden.

Schweregrad Bereich des Schweregrads des VTs, für den die Übersteuerung angewendet werden soll.

Neuer Schweregrad Schweregrad, den der VT nach Anwenden der Übersteuerung haben soll.

Aufgabe Wahl der Aufgaben, für die die Übersteuerung angewendet werden soll.

Ergebnis Wahl der Ergebnisse, für die die Übersteuerung angewendet werden soll.

> **Bemerkung:** Falls die Übersteuerung auf zukünftige Berichte angewendet werden soll, muss der Radiobutton *Beliebig* gewählt werden.

Text Ein Text beschreibt die Übersteuerung näher.

Bemerkung: Falls mehrere Übersteuerungen für denselben VT im selben Bericht angewendet werden, wird die neueste Übersteuerung genutzt und angewendet.

11.8.1.2 Eine Übersteuerung auf der Seite *Übersteuerungen* erstellen

Übersteuerungen können auch auf der Seite *Übersteuerungen* erstellt werden:

1. *Scans > Übersteuerungen* in der Menüleiste wählen.
2. Neue Übersteuerung durch Klicken auf ☆ erstellen.
3. ID des VTs in das Eingabefeld *NVT-OID* eingeben.

4. Übersteuerung definieren.

   Bemerkung: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *11.8.1.1* (Seite 315).

5. Neuen Schweregrad in der Drop-down-Liste *Neuer Schweregrad* wählen.
6. Auf *Speichern* klicken.

11.8.2 Übersteuerungen verwalten

Listenseite

Alle vorhandenen Übersteuerungen können angezeigt werden, indem *Scans > Übersteuerungen* in der Menüleiste gewählt wird.

Für alle Übersteuerungen sind die folgenden Aktionen verfügbar:

- Die Übersteuerung in den Papierkorb verschieben.
- Die Übersteuerung bearbeiten.
- Die Übersteuerung klonen.
- Die Übersteuerung als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Übersteuerungen können mehrere Übersteuerungen zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Übersteuerungen in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Übersteuerung werden Details der Übersteuerung angezeigt. Durch Klicken auf wird die Detailseite der Übersteuerung geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Übersteuerung.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Übersteuerungen anzeigen.
- Eine neue Übersteuerung erstellen (siehe Kapitel *11.8.1* (Seite 315)).
- Die Übersteuerung klonen.
- Die Übersteuerung bearbeiten.
- Die Übersteuerung in den Papierkorb verschieben.
- Die Übersteuerung als XML-Datei exportieren.

11.8.3 Übersteuerungen aktivieren und deaktivieren

Falls Übersteuerungen die Anzeige der Ergebnisse ändern, können die Übersteuerungen aktiviert oder deaktiviert werden.

Dies wird durch Anpassen des Filters wie folgt durchgeführt:

1. In der Filterleiste auf ✎ klicken.
2. Übersteuerungen durch Wählen des Radiobuttons *Ja* für *Übersteuerungen anwenden* aktivieren.

   Radiobutton *Nein* für *Übersteuerungen anwenden* wählen, um Übersteuerungen zu deaktivieren.
3. *Aktualisieren* klicken.

Tipp: Übersteuerungen können in exportierten Berichten gekennzeichnet werden (siehe Kapitel *11.2.2* (Seite 298)).

KAPITEL 12

Compliance-Scans und besondere Scans durchführen

In der Informationstechnologie ist die Einhaltung von Vorschriften der wichtigste Ansatz für Unternehmen, um ihre Informationen und Vermögenswerte zu schützen und zu sichern.

Organisationen und Verbände für Informationssicherheit wie die Information Systems Audit and Control Association (ISACA) oder das Center for Internet Security (CIS) veröffentlichen IT-Sicherheitsstandards, -rahmenwerke und -richtlinien. Diese fordern von den Unternehmen, geeignete Sicherheitsmaßnahmen zu ergreifen, um sich selbst und ihre Informationsbestände vor Angriffen zu schützen.

Schwachstellenbewertungssysteme wie die Greenbone Enterprise Appliance können bei der Bewertung der IT-Sicherheitsvorkehrungen helfen, indem sie Audits auf der Grundlage von Richtlinien durchführen.

Die Kapitel *12.4* (Seite 330), *12.5* (Seite 343) und *12.6* (Seite 347) zeigen einige Beispiele für Richtlinienaudits.

Bemerkung: Da das Ziel der meisten Audits die Überprüfung lokaler Sicherheitskonfigurationen auf den Zielsystemen ist, ist es im Allgemeinen und im Zweifelsfall empfehlenswert, authentifizierte Audits durchzuführen (siehe Kapitel *10.3.2* (Seite 222)). Ausnahmen bestehen für Audits, die nur extern verfügbare Dienste überprüfen, z.B. SSL/TLS.

12.1 Richtlinien konfigurieren und verwalten

Richtlinien sind Scan-Konfigurationen mit der Kennzeichnung *Richtlinie*.

Alle Standardrichtlinien von Greenbone sind Datenobjekte, die über den Feed verteilt werden. Sie werden mit jedem Feed-Update heruntergeladen und aktualisiert.

Falls keine Standardrichtlinien verfügbar sind, ist möglicherweise ein Feed-Update nötig oder der Feed Import Owner muss festgelegt werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Standardrichtlinien können nicht bearbeitet werden. Außerdem können sie nur temporär vom Feed Import Owner oder von einem Super-Administrator gelöscht werden. Während des nächsten Feed-Updates werden sie wieder heruntergeladen.

Bemerkung: Um eine Standardrichtlinie dauerhaft zu löschen, muss der Feed Import Owner sie löschen. Anschließend muss der Feed Import Owner auf *(Unset)* geändert werden (siehe Kapitel *7.2.1.10.1* (Seite 79)).

Zusätzlich zu den Standardrichtlinien können benutzerdefinierte Richtlinien erstellt (siehe Kapitel *12.1.1* (Seite 320)) oder importiert (siehe Kapitel *12.1.2* (Seite 323)) werden.

12.1.1 Eine Richtlinie erstellen

Eine neue Richtlinie kann wie folgt erstellt werden:

1. *Resilience > Compliance Richtlinien* in der Menüleiste wählen.
2. Neue Richtlinie durch Klicken auf erstellen.

   Bemerkung: Alternativ kann eine Richtlinie importiert werden (siehe Kapitel *12.1.2* (Seite 323)).

   ---

3. Namen der Richtlinie in das Eingabefeld *Name* eingeben (siehe Abb. 12.1).

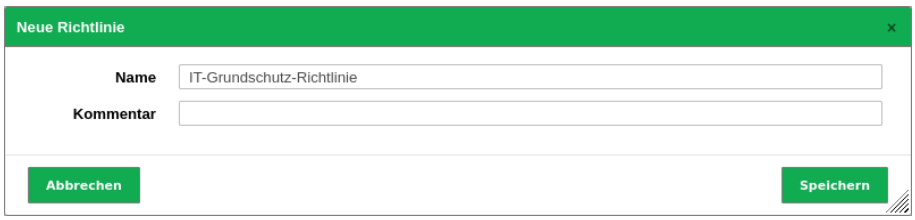


Abb. 12.1: Erstellen einer neuen Richtlinie

4. Auf *Speichern* klicken.

   → Die Richtlinie wird erstellt und auf der Seite *Richtlinien* angezeigt.

5. In der Zeile der Richtlinie auf klicken.
6. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* den Radiobutton wählen, falls neue VT-Familien automatisch hinzugefügt und aktiviert werden soll (siehe Abb. 12.2).
7. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* die Checkboxen *Alle NVTs auswählen* aktivieren, falls alle VTs einer Familie aktiviert werden sollen.

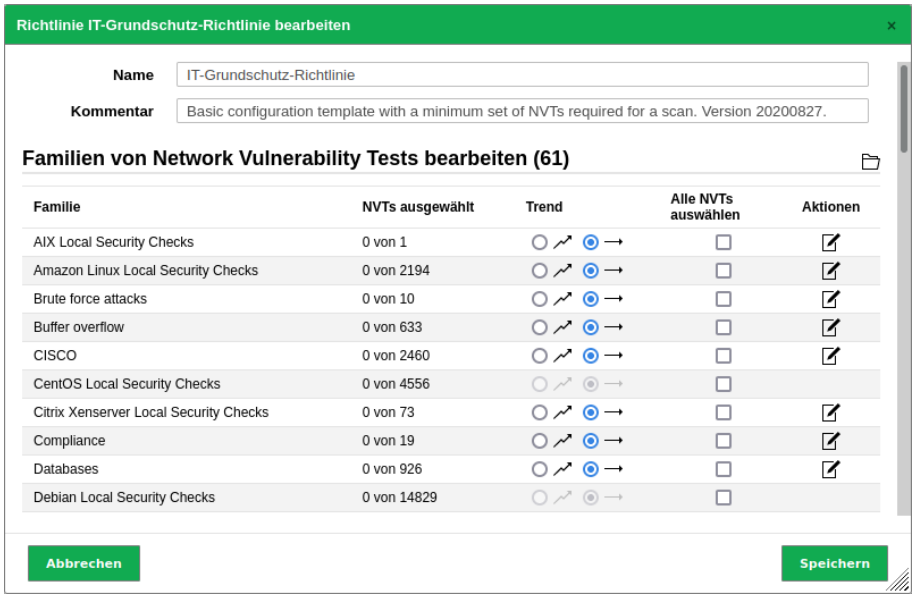


Abb. 12.2: Bearbeiten der neuen Richtlinie

8. Für eine VT-Familie auf klicken, um sie zu bearbeiten (siehe Abb. 12.3).

Bemerkung: Die folgenden VT-Familien können nicht bearbeitet werden:

- CentOS Local Security Checks
- Debian Local Security Checks
- Fedora Local Security Checks
- Huawei EulerOS Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks

9. Die Checkboxen der VTs, die aktiviert werden sollen, in der Spalte *Ausgewählt* aktivieren.
10. Für einen VT auf klicken, um ihn zu bearbeiten (siehe Abb. 12.4).

Bemerkung: Falls systemspezifische VTs der VT-Familie *Policy* genutzt werden (z. B. beginnend mit „Linux“, „Microsoft Windows“, „Microsoft Office“), muss der Radiobutton *Ja* für *Verbose Policy Controls* im VT *Compliance Tests* (VT-Familie *Compliance*) gewählt werden.

Bemerkung: Falls das Bearbeiten eines VT das Hochladen einer Textdatei beinhaltet, sollte die Datei mit UTF-8 codiert sein.

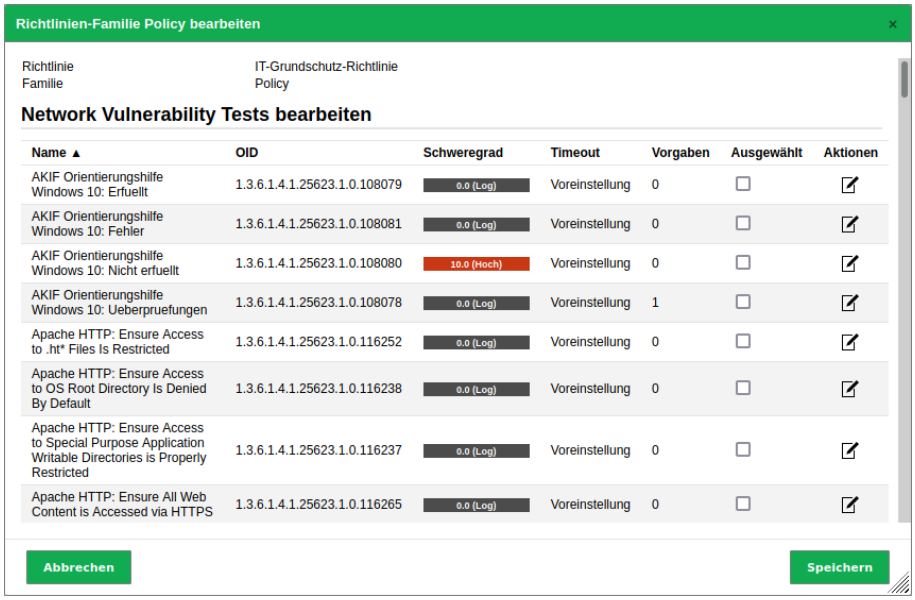


Abb. 12.3: Bearbeiten einer VT-Familie

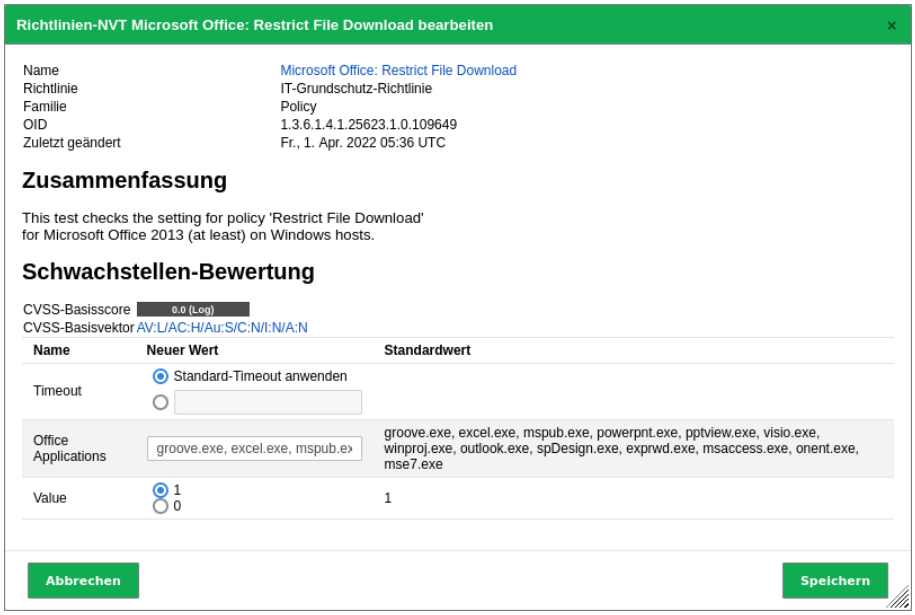


Abb. 12.4: Bearbeiten eines VTs

11. Auf *Speichern* klicken, um den VT zu speichern.
12. Auf *Speichern* klicken, um die VT-Familie zu speichern.
13. Optional: Scanner-Vorgaben bearbeiten (siehe Kapitel *10.9.4* (Seite 267)).
14. Optional: VT-Vorgaben bearbeiten (siehe Kapitel *10.9.5* (Seite 268)).
15. Auf *Speichern* klicken, um die Richtlinie zu speichern.

12.1.2 Eine Richtlinie importieren

Eine Richtlinie kann wie folgt importiert werden:

1. *Resilience* > *Compliance Richtlinien* in der Menüleiste wählen.
2. Auf klicken.
3. Auf *Browse. . .* klicken und die XML-Datei der Richtlinie wählen (siehe Abb. 12.5).

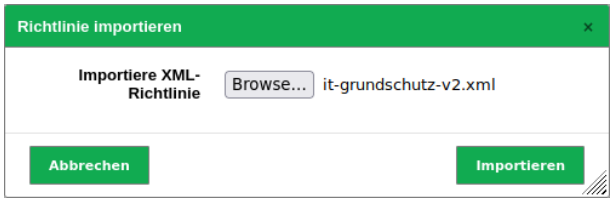


Abb. 12.5: Importieren einer Richtlinie

4. Auf *Importieren* klicken.

Bemerkung: Falls der Name der importierten Richtlinie bereits vorhanden ist, wird ein Zusatz an den Namen angehängt.

→ Die importierte Richtlinie wird auf der Seite *Richtlinien* angezeigt.

5. Schritte 5 bis 15 aus Kapitel *12.1.1* (Seite 320) durchführen, um die Richtlinie zu bearbeiten.

12.1.3 Richtlinien verwalten

Listenseite

Alle vorhandenen Richtlinien können angezeigt werden, indem *Resilience* > *Compliance Richtlinien* in der Menüleiste gewählt wird (siehe Abb. 12.6).

Für alle Richtlinien werden die folgenden Informationen angezeigt:

Name Name der Richtlinie.

Für alle Richtlinien sind die folgenden Aktionen verfügbar:

- Die Richtlinie in den Papierkorb verschieben. Nur Richtlinien, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden. Solange die Richtlinie nicht aus dem Papierkorb gelöscht wird, wird sie beim nächsten Feed-Update nicht neu heruntergeladen.
- Die Richtlinie bearbeiten. Nur selbst erstellte Richtlinien, die aktuell nicht genutzt werden, können bearbeitet werden.
- Die Richtlinie klonen.
- Ein neues Audit für die Richtlinie erstellen (siehe Kapitel *12.2.1.2* (Seite 326)).

Abb. 12.6: Seite *Richtlinien* mit allen verfügbaren Richtlinien

- Die Richtlinie als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Richtlinien können mehrere Richtlinien zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Richtlinien in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen einer Richtlinie werden Details der Richtlinie angezeigt. Durch Klicken auf wird die Detailseite der Richtlinie geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die Richtlinie.

Scanner-Vorgaben Alle Scanner-Vorgaben für die Richtlinie mit aktuellen und Standardwerten.

NVT-Familien Alle VT-Familien für die Richtlinie mit der Anzahl aktivierter VTs und dem Trend.

NVT-Vorgaben Alle VT-Vorgaben für die Richtlinie.

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Richtlinien anzeigen.
- Eine neue Richtlinie erstellen (siehe Kapitel *12.1.1* (Seite 320)).
- Die Richtlinie klonen.
- Die Richtlinie bearbeiten. Nur selbst erstellte Richtlinien, die aktuell nicht genutzt werden, können bearbeitet werden.
- Die Richtlinie in den Papierkorb verschieben. Nur Richtlinien, die aktuell nicht genutzt werden, können in den Papierkorb verschoben werden. Solange die Richtlinie nicht aus dem Papierkorb gelöscht wird, wird sie beim nächsten Feed-Update nicht neu heruntergeladen.
- Die Richtlinie als XML-Datei exportieren.
- Eine Richtlinie importieren (siehe Kapitel *12.1.2* (Seite 323)).

12.2 Audits konfigurieren und verwalten

Audits sind Scanaufgaben mit der Kennzeichnung *Audit*.

12.2.1 Ein Audit erstellen

12.2.1.1 Ein Audit auf der Seite *Audits* erstellen

Ein Audit kann auf der Seite *Audits* wie folgt erstellt werden:

1. *Resilience* > *Compliance Audits* in der Menüleiste wählen.
2. Neues Audit durch Klicken auf ☆ erstellen.
3. Audit definieren (siehe Abb. 12.7).
4. Auf *Speichern* klicken.

   → Das Audit wird erstellt und auf der Seite *Audits* angezeigt.

Die folgenden Informationen können eingegeben werden:

Name Der Name kann frei gewählt werden. Falls möglich, sollte ein aussagekräftiger Name gewählt werden.

Kommentar Der optionale Kommentar erlaubt es, Hintergrundinformationen festzuhalten. Diese erleichtern später das Verständnis des konfigurierten Audits.

Scan-Ziele Zuvor konfiguriertes Ziel aus der Drop-down-Liste wählen (siehe Kapitel *10.2.1* (Seite 214)).

Zusätzlich kann das Ziel durch Klicken auf ☆ neben der Drop-down-Liste erstellt werden.

Benachrichtigungen Zuvor konfigurierte Benachrichtigung aus der Drop-down-Liste wählen (siehe Kapitel *10.12* (Seite 277)). Statusänderungen des Audits können über E-Mail, System-Logger, HTTP oder einen Konnektor mitgeteilt werden.

Zusätzlich kann eine Benachrichtigung durch Klicken auf ☆ neben der Drop-down-Liste erstellt werden.

Zeitplan Zuvor konfigurierten Zeitplan aus der Drop-down-Liste wählen (siehe Kapitel *10.10* (Seite 272)). Das Audit kann einmalig oder wiederholt zu einer festgelegten Zeit, z. B. jeden Montagmorgen um 6:00, ausgeführt werden.

Zusätzlich kann ein Zeitplan durch Klicken auf ☆ neben der Drop-down-Liste erstellt werden.

Ergebnisse zu Assets hinzufügen Das Auswählen dieser Option macht die Systeme automatisch für die Assetverwaltung der Appliance verfügbar (siehe Kapitel *13* (Seite 349)). Diese Auswahl kann später geändert werden.

Änderbares Audit Änderung von Scan-Ziel(en) und Scanner des Audits ermöglichen, auch wenn bereits Berichte erstellt wurden. Die Übereinstimmung zwischen Berichten kann nicht mehr garantiert werden, wenn Audits geändert werden.

Berichte automatisch löschen Diese Option löscht alte Berichte automatisch. Die maximale Anzahl an gespeicherten Berichten kann konfiguriert werden. Falls das Maximum überschritten wird, wird der älteste Bericht automatisch gelöscht. Die Werkseinstellung ist *Berichte nicht automatisch löschen*.

Richtlinie Die Appliance wird mit mehreren vorkonfigurierten Richtlinien geliefert. Pro Audit kann nur eine Richtlinie konfiguriert werden.

Reihenfolge der Ziel-Hosts Wählen, in welcher Reihenfolge die angegebenen Zielhosts bei Schwachstellentests verarbeitet werden. Verfügbare Optionen sind:

- Sequenziell
- Zufällig

- Rückwärts

Um die Abschätzung des Scanfortschritts zu verbessern, wird die Einstellung *Zufällig* empfohlen (siehe Kapitel *17.2.3* (Seite 392)).

Diese Einstellung hat keinen Einfluss auf den Erreichbarkeitstest, bei dem aktive Hosts in einem Zielnetzwerk identifiziert werden. Der Erreichbarkeitstest ist immer zufällig.

Maximal gleichzeitig ausgeführte NVTs pro Host/Maximal gleichzeitig gescannte Hosts Auswahl der Geschwindigkeit des Scans auf einem Host. Die Standardwerte sind bewusst gewählt. Falls mehrere VTs gleichzeitig auf einem System laufen oder mehrere Systeme zur gleichen Zeit gescannt werden, könnte der Scan negative Auswirkungen auf die Leistung der gescannten Systeme, des Netzwerks oder der Appliance selbst haben. Die Werte „maxhosts“ und „maxchecks“ können optimiert werden.

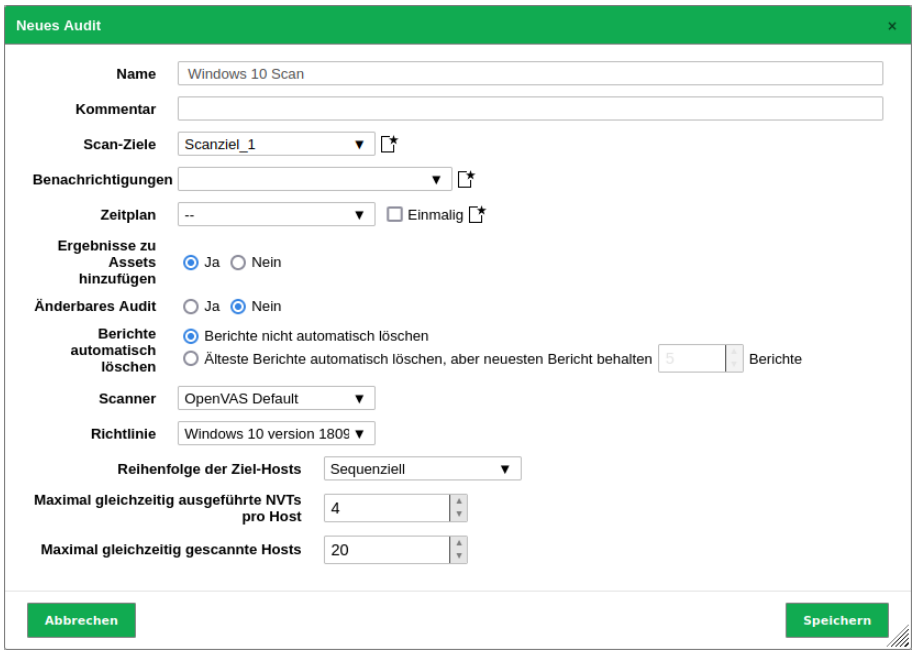


Abb. 12.7: Erstellen eines neuen Audits

12.2.1.2 Ein Audit über eine Richtlinie erstellen

Ein Audit kann wie folgt direkt für eine Richtlinie erstellt werden:

1. *Resilience > Compliance Richtlinien* in der Menüleiste wählen.
2. In der Zeile der gewünschten Richtlinie auf klicken.

   → Die Richtlinie ist bereits in der Drop-down-Liste *Richtlinie* ausgewählt.
3. Audit definieren.

Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *12.2.1.1* (Seite 325).

4. Auf *Speichern* klicken.

   → Das Audit wird erstellt und auf der Seite *Audits* angezeigt.

12.2.2 Ein Audit starten

In der Zeile des neu erstellten Audits auf ▷ klicken.

Bemerkung: Für Audits mit Zeitplan wird 🕒 angezeigt. Das Audit startet zu der Zeit, die im Zeitplan festgelegt wurde (siehe Kapitel *10.10* (Seite 272))

→ Das Audit wird zur Warteschlange hinzugefügt. Danach beginnt der Scanner mit dem Scan.

Bemerkung: In einigen Fällen kann das Audit in der Warteschlange bleiben. Weitere Informationen befinden sich in Kapitel *17.3* (Seite 393).

Für den Status eines Audits siehe Kapitel *12.2.3* (Seite 327).

Sobald ein Audit gestartet wurde, kann der Bericht des Audits durch Klicken auf den Balken in der Spalte *Status* angezeigt werden. Für das Lesen, Verwalten und Herunterladen von Berichten siehe Kapitel *11* (Seite 288).

Sobald sich der Status zu *Abgeschlossen* ändert, ist der gesamte Bericht verfügbar. Zu jeder Zeit können Zwischenergebnisse angesehen werden (siehe Kapitel *11.2.1* (Seite 293)).

Bemerkung: Die Fertigstellung des Scans kann einige Zeit in Anspruch nehmen. Die Seite aktualisiert automatisch, falls neue Daten verfügbar sind.

12.2.3 Audits verwalten

Listenseite

Alle vorhandenen Audits können angezeigt werden, indem *Resilience* > *Compliance Audits* in der Menüleiste gewählt wird (siehe Abb. 12.8).

Abb. 12.8: Seite *Audits* mit allen verfügbaren Audits

Für alle Audits werden die folgenden Informationen angezeigt:

Name Name des Audits. Die folgenden Icons könnten angezeigt werden:

Das Audit ist als änderbar gekennzeichnet. Scan-Ziel(e) und Scanner des Audits können bearbeitet werden, auch wenn bereits Berichte erstellt wurden.

Das Audit ist für die Durchführung auf einem Remote-Scanner konfiguriert (siehe Kapitel *16* (Seite 380)).

Das Audit ist für einen oder mehrere andere Benutzer sichtbar.

Das Audit gehört einem anderen Benutzer.

Status Aktueller Status des Audits. Die folgenden Statusbalken sind möglich:

Neu Es gibt keine Ausführungen/Berichte für das Audit.

Angefragt Das Audit wurde gerade gestartet. Die Appliance bereitet den Scan vor. Audits mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

In Warteschlange Das Audit wurde zur Warteschlange hinzugefügt. In einigen Fällen kann es in der Warteschlange bleiben. Weitere Informationen befinden sich in Kapitel *17.3* (Seite 393).

21 % Das Audit wird gerade ausgeführt. Die Prozentangabe basiert auf der Anzahl ausgeführter VTs auf den gewählten Hosts. Aus diesem Grund hängt der Wert nicht zwingend mit der bereits verstrichenen Zeit zusammen.

Verarbeiten Der Scanvorgang ist abgeschlossen und die Appliance verarbeitet Daten. Audits mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Abgeschlossen Das Audit wurde erfolgreich abgeschlossen.

Stopp Angefragt Das Audit wurde vor Kurzem aufgefordert, zu stoppen. Die Scanmaschine hat noch nicht auf die Anfrage reagiert. Audits mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Angehalten bei 84 % Das Audit wurde gestoppt. Der neueste Bericht ist möglicherweise noch nicht komplett. Andere Gründe für diesen Status können der Reboot der Appliance oder ein Stromausfall sein. Nach dem Neustart des Scanners wird das Audit automatisch fortgesetzt.

Fortsetzen Angefragt Das Audit wurde gerade fortgesetzt. Die Appliance bereitet den Scan vor. Audits mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Beim Fortsetzen eines Scans werden alle nicht abgeschlossenen Hosts komplett aufs Neue gescannt. Die Daten der bereits vollständig gescannten Hosts bleiben erhalten.

Löschen Angefragt Das Audit wurde gelöscht. Der tatsächliche Löschvorgang kann einige Zeit dauern, da Berichte ebenfalls gelöscht werden müssen. Audits mit diesem Status können nicht gestoppt, fortgesetzt oder gelöscht werden.

Unterbrochen bei 42 % Ein Fehler ist aufgetreten und das Audit wurde unterbrochen. Der neueste Bericht ist möglicherweise noch nicht komplett oder fehlt vollständig.

Bericht Datum und Zeit des neuesten Berichts. Durch Klicken auf die Angabe wird die Detailseite des neuesten Berichts geöffnet.

Compliance Status Anforderungen, die als konform erkannt wurden im Verhältnis zu Anforderungen, die als nicht konform erkannt wurden (in Prozent).

Für alle Audits sind die folgenden Aktionen verfügbar:

- Das Audit starten. Nur Audits, die aktuell nicht ausgeführt werden, können gestartet werden.
- Das aktuell ausgeführte Audit stoppen. Alle gefundenen Ergebnisse werden in der Datenbank gespeichert.

- Die Details des zugewiesenen Zeitplans anzeigen (nur für Audits mit Zeitplan verfügbar, siehe Kapitel *10.10* (Seite 272)).
- Das gestoppte Audit fortsetzen. Alle nicht abgeschlossenen Hosts werden komplett aufs Neue gescannt. Die Daten der bereits vollständig gescannten Hosts bleiben erhalten.
- Das Audit in den Papierkorb verschieben.
- Das Audit bearbeiten.
- Das Audit klonen.
- Das Audit als XML-Datei exportieren.
- Den Bericht des Audits als GCR-Datei (Greenbone Compliance Report im PDF-Format) herunterladen.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von Audits können mehrere Audits zur gleichen Zeit in den Papierkorb verschoben oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Audits in den Papierkorb verschoben oder exportiert werden.

Detailseite

Durch Klicken auf den Namen eines Audits werden Details des Audits angezeigt. Durch Klicken auf wird die Detailseite des Audits geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das Audit.

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Audits anzeigen.
- Ein neues Audit erstellen (siehe Kapitel *12.2.1.1* (Seite 325)).
- Das Audit klonen.
- Das Audit bearbeiten.
- Das Audit in den Papierkorb verschieben.
- Das Audit als XML-Datei exportieren.
- Das Audit starten. Nur Audits, die aktuell nicht ausgeführt werden, können gestartet werden.
- Das aktuell ausgeführte Audit stoppen. Alle gefundenen Ergebnisse werden in der Datenbank gespeichert.
- Das gestoppte Audit fortsetzen. Alle nicht abgeschlossenen Hosts werden komplett aufs Neue gescannt. Die Daten der bereits vollständig gescannten Hosts bleiben erhalten.
- Den letzten Bericht des Audits oder alle Berichte des Audits anzeigen.
- Die Ergebnisse des Audits anzeigen.

12.3 Richtlinienberichte nutzen und verwalten

Berichte für Audits sind den Berichten aller anderen Aufgaben ähnlich.

Nach dem Starten eines Scans kann der Bericht der bis dahin gefundenen Ergebnisse angesehen werden. Wenn der Scan abgeschlossen ist, ändert sich der Status zu *Abgeschlossen* und keine weiteren Ergebnisse werden hinzugefügt.

12.3.1 Einen Richtlinienbericht nutzen

Ein Richtlinienbericht kann auf die gleiche Weise wie jeder andere Bericht genutzt werden. Kapitel *11.2* (Seite 293) enthält Informationen über das Lesen, Interpretieren, Filtern, Exportieren, Importieren und Vergleichen von Berichten.

Für weitere Informationen über Ergebnisse und Schwachstellen siehe Kapitel *11.3* (Seite 304) und *11.4* (Seite 306).

12.3.2 Einen Richtlinienbericht exportieren

Bemerkung: Ein Richtlinienbericht muss immer im Berichtformat *Greenbone Compliance Report PDF (GCR PDF)* heruntergeladen werden. Das Herunterladen in einem anderen Berichtformat führt zu einem leeren Bericht.

Zusätzlich kann der Bericht von der Seite *Audits* wie folgt heruntergeladen werden:

1. *Resilience > Compliance Audits* in der Menüleiste wählen.
2. In der Zeile des gewünschten Audits auf ✎ klicken.
3. PDF-Datei herunterladen.

12.4 Allgemeine Richtlinienscans

Beim Durchführen von Richtlinienscans gibt es vier Gruppen von VTs in der VT-Familie *Policy*, die entsprechend konfiguriert werden können.

Mindestens der Basis-VT und ein zusätzlicher VT sind erforderlich, um einen Richtlinienscan durchzuführen.

Die vier VT-Arten sind:

Basis Dieser VT führt den eigentlichen Scan der Richtlinie durch.

Errors Dieser VT fasst alle Elemente zusammen, in denen beim Ausführen des Basis-VTs Fehler auftraten.

Matches Dieser VT fasst alle Elemente zusammen, auf die die vom Basis-VT ausgeführten Prüfungen zutreffen.

Violations Dieser VT fasst alle Elemente zusammen, auf die die vom Basis-VT ausgeführten Prüfungen nicht zutreffen.

Bemerkung: Der Basis-VT muss für einen Richtliniencheck immer gewählt werden, da er die eigentliche Prüfung durchführt. Die andren drei VTs können entsprechend der Anforderungen gewählt werden. Falls beispielsweise das Erkennen von Mustern nicht von Bedeutung ist, sollte zusätzlich nur ein VT der Art *Violations* gewählt werden.

12.4.1 Dateiinhalt prüfen

Prüfungen des Dateiinhalts gehören zu den Richtlinienprüfungen, die nicht explizit nach Schwachstellen suchen, sondern die Erfüllung von Dateiinhalten (z. B. Konfigurationsdateien) bezüglich bestimmter Vorgaben kontrollieren.

Die Appliance stellt ein Richtlinienmodul bereit, um zu prüfen, ob der Dateiinhalt mit einer gegebenen Richtlinie übereinstimmt.

Im Allgemeinen ist dies ein authentifizierter Scan, was bedeutet, dass sich die Scanmaschine in das Zielsystem einloggen muss, um die Prüfung durchzuführen (siehe Kapitel *10.3* (Seite 220)).

Die Prüfung des Dateiinhalts kann nur auf Systemen durchgeführt werden, die den Befehl `grep` unterstützen. Dabei handelt es sich meist um Linux oder Linux-ähnliche Systeme.

Vier unterschiedliche VTs der VT-Familie *Policy* bieten die Prüfung des Dateiinhalts:

- *File Content*: Dieser VT führt die eigentliche Prüfung des Dateiinhalts durch.
- *File Content: Errors*: Dieser VT zeigt die Dateien, in denen Fehler auftraten (z. B. die Datei wurde nicht auf dem Zielsystem gefunden).
- *File Content: Matches*: Dieser VT zeigt die Muster und Dateien, die die Prüfung des Dateiinhalts bestanden haben (die vorgegebenen Muster stimmen in der Datei überein).
- *File Content: Violations*: Dieser VT zeigt die Muster und Dateien, die die Prüfung des Dateiinhalts nicht bestanden haben (die vorgegebenen Muster stimmen in der Datei nicht überein).

12.4.1.1 Muster des Dateiinhalts prüfen

1. Referenzdatei mit den zu prüfenden Mustern erstellen. Folgend ist ein Beispiel:

```
filename|pattern|presence/absence
/tmp/filecontent_test|^paramter1=true.*$|presence
/tmp/filecontent_test|^paramter2=true.*$|presence
/tmp/filecontent_test|^paramter3=true.*$|absence
/tmp/filecontent_test_notthere|^paramter3=true.*$|absence
```

Bemerkung: Die Datei muss die Zeile `filename|pattern|presence/absence` enthalten.

Die nachfolgenden Zeilen enthalten jeweils einen Prüfeintrag.

Jede Zeile enthält drei Felder, die durch `|` getrennt sind.

Das erste Feld enthält den Pfad und Dateinamen, das zweite Feld enthält das zu prüfende Muster (als regulären Ausdruck) und das dritte Feld gibt an, ob das Muster vorhanden sein muss oder nicht vorhanden sein darf.

---

2. *Resilience > Compliance Richtlinien* in der Menüleiste wählen.
3. In der Zeile der gewünschten Richtlinie auf klicken.

   → Die geklonte Richtlinie wird auf der Seite *Richtlinien* angezeigt.
4. In der Zeile der geklonten Richtlinie auf klicken.
5. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* für die VT-Familie *Policy* auf klicken.

   → Alle VTs, die eine besondere Konfiguration erlauben, werden aufgelistet (siehe Abb. 12.9).
6. Für *File Content* auf klicken.

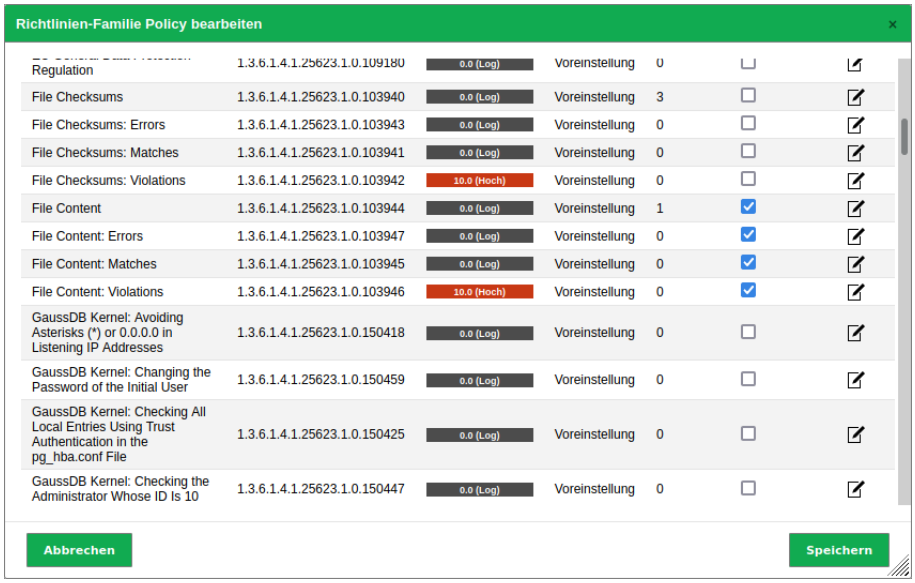


Abb. 12.9: Bearbeiten einer VT-Familie

7. Checkbox *Datei hochladen* aktivieren (siehe Abb. 12.10).

Tipp: Falls bereits eine Referenzdatei hochgeladen wurde, wird stattdessen die Checkbox *Existierende Datei ersetzen* angezeigt. Die Referenzdatei kann nur geändert werden, falls die Richtlinie aktuell nicht genutzt wird.

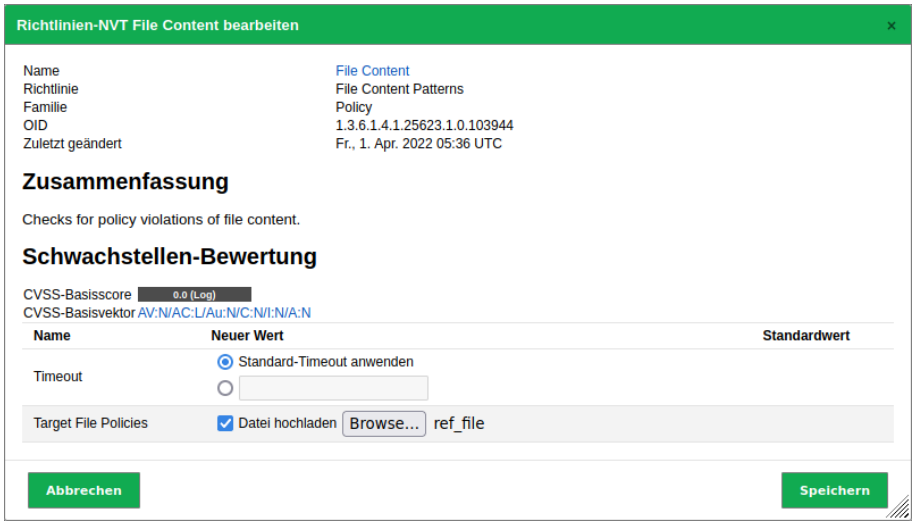


Abb. 12.10: Hochladen der Referenzdatei

8. Auf *Browse...* klicken und die zuvor erstellte Referenzdatei wählen.
9. Auf *Speichern* klicken, um den VT zu speichern.
10. Auf *Speichern* klicken, um die VT-Familie zu speichern.
11. Auf *Speichern* klicken, um die Richtlinie zu speichern.

12.4.1.2 Den Schweregrad ändern

VTs der Art *Violations* haben einen standardmäßigen Schweregrad von 10.

Dieser Standard-Schweregrad kann wie in Kapitel *11.2.1* (Seite 293) beschrieben geändert werden.

Durch das Aufteilen in drei unterschiedlichen VTs ist es möglich, abhängig von den Anforderungen, verschiedene Übersteuerungen für den Schweregrad zu erstellen.

Im folgenden Beispiel wurden die Schweregrade von *File Content: Violations* und *File Content: Errors* geändert, was entsprechend in den Berichten angezeigt wird (siehe Abb. 12.11).

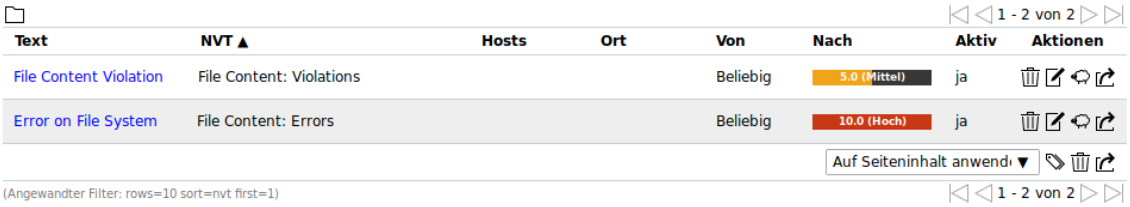


Abb. 12.11: Ändern des Schweregrads durch Übersteuerungen

12.4.2 Registryinhalt prüfen

Die Registrierungsdatenbank (Registry)[31] ist eine Datenbank in Microsoft Windows, die wichtige Informationen über Systemhardware, installierte Programme und Benutzeraccounts auf dem Computer enthält. Microsoft Windows verweist kontinuierlich auf die Informationen in der Registry.

Aufgrund der Beschaffenheit der Microsoft-Windows-Registry trägst sich jedes Programm und jede Anwendung unter Microsoft Windows selbst in die Registry ein. Sogar Malware und anderer schädlicher Code hinterlassen normalerweise Spuren in der Registry.

Die Registry kann genutzt werden, um nach bestimmten Anwendungen oder mit Malware verbundenen Informationen, wie Versionslevel und -nummer, zu suchen. Außerdem können fehlende oder veränderte Registryeinstellungen auf potentielle Verletzungen der Sicherheitsrichtlinie an einem Endpunkt hinweisen.

Die Appliance stellt ein Richtlinienmodul bereit, um Registryeinträge auf dem Zielsystem zu verifizieren. Dieses Modul prüft sowohl die An- oder Abwesenheit von Registryeinstellungen als auch Registryverletzungen.

Da die Registry auf Microsoft-Windows-Systeme beschränkt ist, kann diese Prüfung nur auf diesen Systemen durchgeführt werden.

Um auf die Regsitry des Zielsystems zuzugreifen, muss ein authentifizierter Scan ausgeführt werden.

Vier unterschiedliche VTs der VT-Familie *Policy* bieten die Prüfung des Registryinhalts:

- *Windows Registry Check*: Dieser VT führt die eigentliche Prüfung des Registryinhalts auf den Dateien durch.
- *Windows Registry Check: Errors*: Dieser VT zeigt die Dateien, in denen Fehler auftraten (z. B. der Registryinhalt wurde nicht auf dem Zielsystem gefunden).
- *Windows Registry Check: OK*: Dieser VT zeigt die Registryeinstellungen, die die Prüfung der Registry bestanden haben (korrekter Registryinhalt).
- *Windows Registry Check: Violations*: Dieser VT zeigt den Registryinhalt, der die Prüfung der Registry nicht bestanden haben (fehlerhafter Registryinhalt).

[31] https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry

12.4.2.1 Muster des Registryinhalts prüfen

1. Referenzdatei mit dem Referenzinhalt erstellen. Folgend ist ein Beispiel:

```
Present|Hive|Key|Value|ValueType|ValueContent
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|33
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer|Version|REG_SZ|9.11.10240.16384
TRUE|HKLM|SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
 System|LocalAccountTokenFilterPolicy|REG_DWORD|1
FALSE|HKLM|SOFTWARE\Virus
TRUE|HKLM|SOFTWARE\ShouldNotBeHere
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|*
```

Bemerkung: Die Datei muss die Zeile `Present|Hive|Key|Value|ValueType|ValueContent` enthalten.

Die nachfolgenden Zeilen enthalten jeweils einen Prüfeintrag.

Jede Zeile enthält sechs Felder, die durch `|` getrennt sind.

Das erste Feld gibt an, ob ein Registryeintrag vorhanden sein muss oder nicht, das zweite enthält die logische Untereinheit, in der sich der Registryinhalt befindet, das dritte den Schlüssel, das vierte den Wert, das fünfte den Werttyp und das sechste den Wertinhalt. Falls ein Sternchen `*` in der letzten Spalte genutzt wird, ist jeder Wert gültig und akzeptiert.

2. *Resilience > Compliance Richtlinien* in der Menüleiste wählen.
3. In der Zeile der Richtlinie *Microsoft Windows Registry Check* auf klicken.

   → Die geklonte Richtlinie wird auf der Seite *Richtlinien* angezeigt.
4. In der Zeile der geklonten Richtlinie auf klicken.
5. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* für die VT-Familie *Policy* auf klicken.

   → Alle VTs, die eine besondere Konfiguration erlauben, werden aufgelistet (siehe Abb. 12.12).

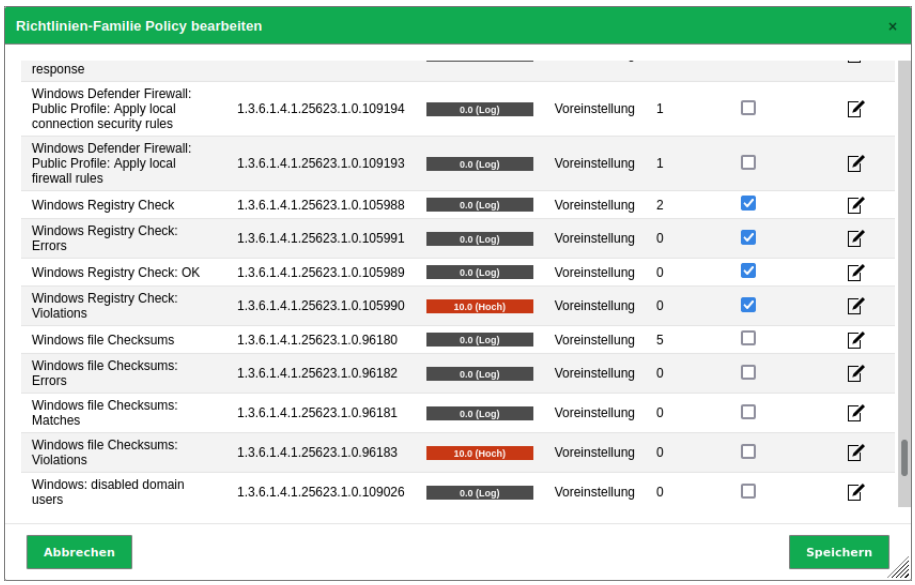


Abb. 12.12: Bearbeiten einer VT-Familie

6. Für *Windows Registry Check* auf klicken.
7. Checkbox *Datei hochladen* aktivieren (siehe Abb. 12.13).

Tipp: Falls bereits eine Referenzdatei hochgeladen wurde, wird stattdessen die Checkbox *Existierende Datei ersetzen* angezeigt. Die Referenzdatei kann nur geändert werden, falls die Richtlinie aktuell nicht genutzt wird.

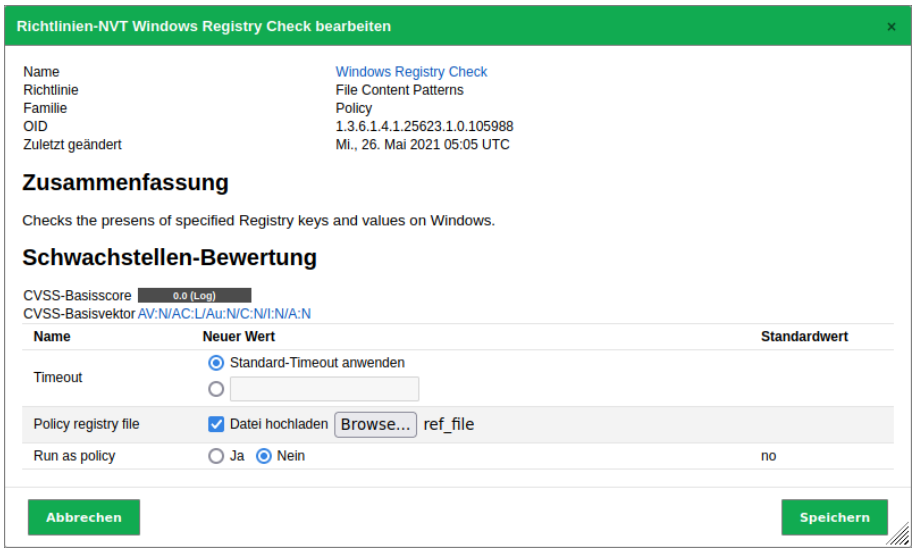


Abb. 12.13: Hochladen der Referenzdatei

8. Auf *Browse...* klicken und die zuvor erstellte Referenzdatei wählen.
9. Auf *Speichern* klicken, um den VT zu speichern.
10. Auf *Speichern* klicken, um die VT-Familie zu speichern.
11. Auf *Speichern* klicken, um die Richtlinie zu speichern.

12.4.2.2 Den Schweregrad ändern

VTs der Art *Violations* haben einen standardmäßigen Schweregrad von 10.

Dieser Standard-Schweregrad kann wie in Kapitel *11.2.1* (Seite 293) beschrieben geändert werden.

Durch das Aufteilen in drei unterschiedlichen VTs ist es möglich, abhängig von den Anforderungen, verschiedene Übersteuerungen für den Schweregrad zu erstellen.

Im folgenden Beispiel wurden die Schweregrade von *Windows Registry Check: Violations* und *Windows Registry Check: Errors* geändert, was entsprechend in den Berichten angezeigt wird (siehe Abb. 12.14).

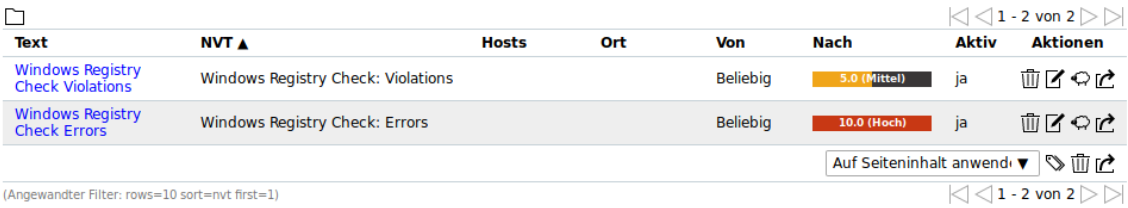


Abb. 12.14: Ändern des Schweregrads durch Übersteuerungen

12.4.3 Datei-Prüfsummen prüfen

Prüfungen der Datei-Prüfsummen gehören zu Richtlinienaudits, die nicht ausdrücklich auf Schwachstellen prüfen, sondern stattdessen auf Integrität einer Datei.

Die Appliance stellt ein Richtlinienmodul bereit, um die Dateiintegrität auf dem Zielsystem zu verifizieren. Dieses Modul prüft den Dateiinhalt durch MD5- oder SHA1-Prüfsummen.

Im Allgemeinen ist dies ein authentifizierter Scan, was bedeutet, dass sich die Scanmaschine in das Zielsystem einloggen muss, um die Prüfung durchzuführen.

Die Prüfung von Prüfsummen kann nur auf Systemen durchgeführt werden, die Prüfsummen unterstützen. Normalerweise sind dies Linux- oder linuxähnliche Systeme. Trotzdem bietet die Appliance auch ein Modul für die Prüfung von Prüfsummen auf Microsoft-Windows-Systemen (siehe Kapitel *12.4.3.3* (Seite 338)).

Vier unterschiedliche VTs der VT-Familie *Policy* stellen die Prüfung der Datei-Prüfsummen bereit:

- *File Checksums*: Dieser VT führt die eigentliche Prüfung der Prüfsummen auf den Dateien durch.
- *File Checksums: Errors*: Dieser VT zeigt die Dateien, in denen Fehler auftraten (z. B. die Datei wurde nicht auf dem Zielsystem gefunden).
- *File Checksums: Matches*: Dieser VT zeigt die Dateien, die die Prüfung der Prüfsummen bestanden haben (übereinstimmende Prüfsummen).
- *File Checksums: Violations*: Dieser VT zeigt die Dateien, die die Prüfung der Prüfsummen nicht bestanden haben (falsche Prüfsummen).

12.4.3.1 Muster der Datei-Prüfsummen prüfen

1. Referenzdatei mit den zu prüfenden Prüfsummen erstellen. Folgend ist ein Beispiel:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

Bemerkung: Die Datei muss die Zeile `Checksum|File|Checksumtype` enthalten.

Die nachfolgenden Zeilen enthalten jeweils einen Prüfeintrag.

Jede Zeile enthält drei Felder, die durch `|` getrennt sind.

Das erste Feld enthält die Prüfsumme in hexadezimaler Schreibweise, das zweite den Pfad und Dateinamen und das dritte den Prüfsummentyp. Aktuell werden MD5 und SHA1 unterstützt.

Wichtig: Prüfsummen und Prüfsummentypen müssen in Kleinbuchstaben geschrieben werden.

---

2. *Resilience > Compliance Richtlinien* in der Menüleiste wählen.
3. In der Zeile der gewünschten Richtlinie auf klicken.

   → Die geklonte Richtlinie wird auf der Seite *Richtlinien* angezeigt.
4. In der Zeile der geklonten Richtlinie auf klicken.
5. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* für die VT-Familie *Policy* auf klicken.

   → Alle VTs, die eine besondere Konfiguration erlauben, werden aufgelistet (siehe Abb. 12.15).
6. Für *File Checksums* auf klicken.

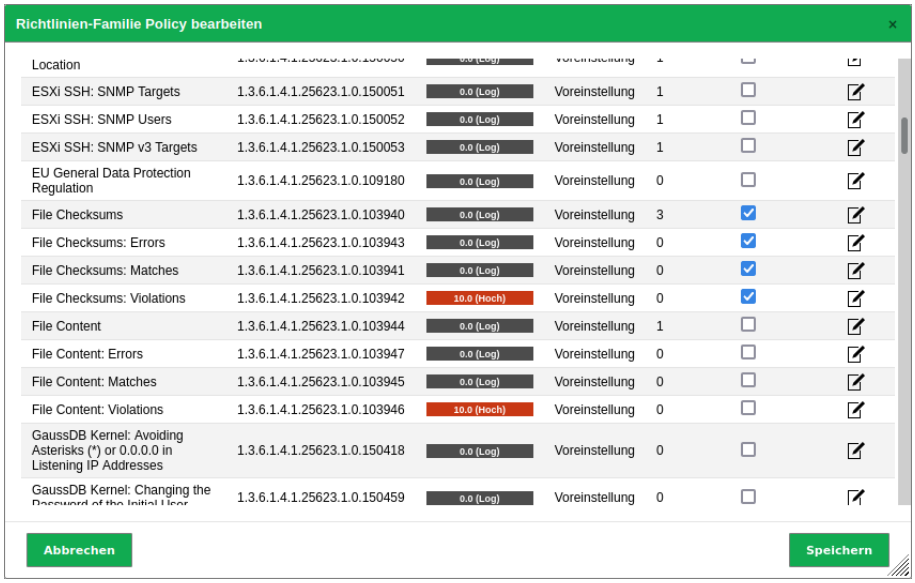


Abb. 12.15: Bearbeiten einer VT-Familie

7. Checkbox *Datei hochladen* aktivieren (siehe Abb. 12.16).

Tipp: Falls bereits eine Referenzdatei hochgeladen wurde, wird stattdessen die Checkbox *Existierende Datei ersetzen* angezeigt. Die Referenzdatei kann nur geändert werden, falls die Richtlinie aktuell nicht genutzt wird.

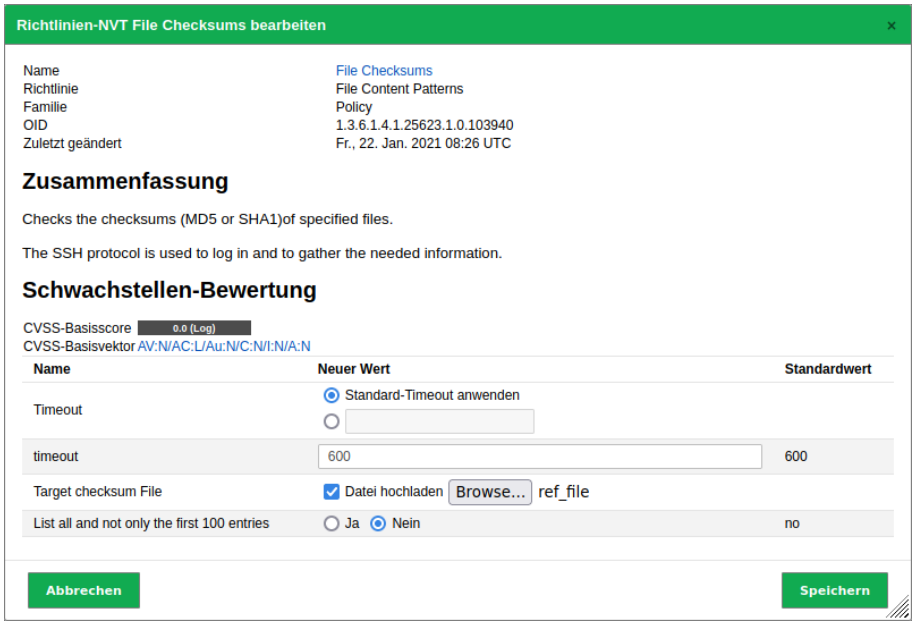


Abb. 12.16: Hochladen der Referenzdatei

8. Auf *Browse...* klicken und die zuvor erstellte Referenzdatei wählen.

9. Auf *Speichern* klicken, um den VT zu speichern.
10. Auf *Speichern* klicken, um die VT-Familie zu speichern.
11. Auf *Speichern* klicken, um die Richtlinie zu speichern.

12.4.3.2 Den Schweregrad ändern

VTs der Art *Violations* haben einen standardmäßigen Schweregrad von 10.

Dieser Standard-Schweregrad kann wie in Kapitel *11.2.1* (Seite 293) beschrieben geändert werden.

Durch das Aufteilen in drei unterschiedlichen VTs ist es möglich, abhängig von den Anforderungen, verschiedene Übersteuerungen für den Schweregrad zu erstellen.

Im folgenden Beispiel wurden die Schweregrade von *File Checksum: Violations* und *File Checksum: Errors* geändert, was entsprechend in den Berichten angezeigt wird (siehe Abb. 12.17).

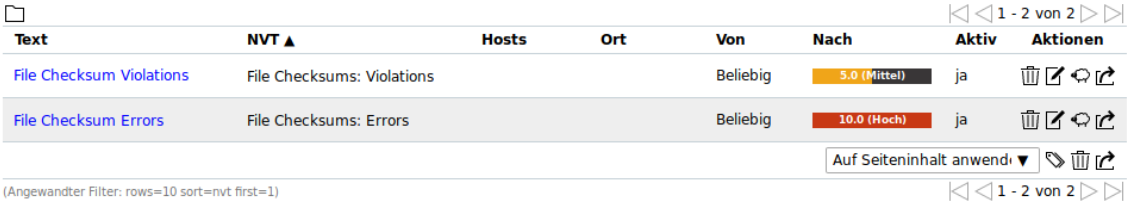


Abb. 12.17: Ändern des Schweregrads durch Übersteuerungen

12.4.3.3 Muster der Datei-Prüfsummen für Microsoft Windows prüfen

Die Appliance stellt ein ähnliches Modul für Microsoft-Windows-Systeme für die Prüfung der Datei-Prüfsummen bereit.

Da Microsoft Windows kein internes Programm für das Erstellen von Prüfsummen anbietet, muss eines entweder manuell oder automatisch durch den VT erstellt werden. Die Appliance nutzt ReHash[32] zum Erstellen von Prüfsummen auf Microsoft-Windows-Systemen.

Bemerkung: Es gibt zwei Betriebsarten für diese Prüfungen:

- Nutzung eines Tools, das manuell auf dem Zielsystem installiert wurde.
- Falls gewünscht, wird das Tool ReHash während der Prüfroutine auch automatisch auf dem Zielsystem installiert und deinstalliert.

Wie für Linuxsysteme befinden sich die VTs für die Prüfung der Prüfsummen in der VT-Familie *Policy*.

1. Referenzdatei mit den zu prüfenden Mustern erstellen. Folgend ist ein Beispiel:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

2. In der Zeile der entsprechenden Richtlinie auf ✎ klicken.
3. Im Abschnitt *Familien von Network Vulnerability Tests bearbeiten* für die VT-Familie *Policy* auf ✎ klicken.

   → Alle VTs, die eine besondere Konfiguration erlauben, werden aufgelistet (siehe Abb. 12.18).

[32] https://rehash.sourceforge.net/

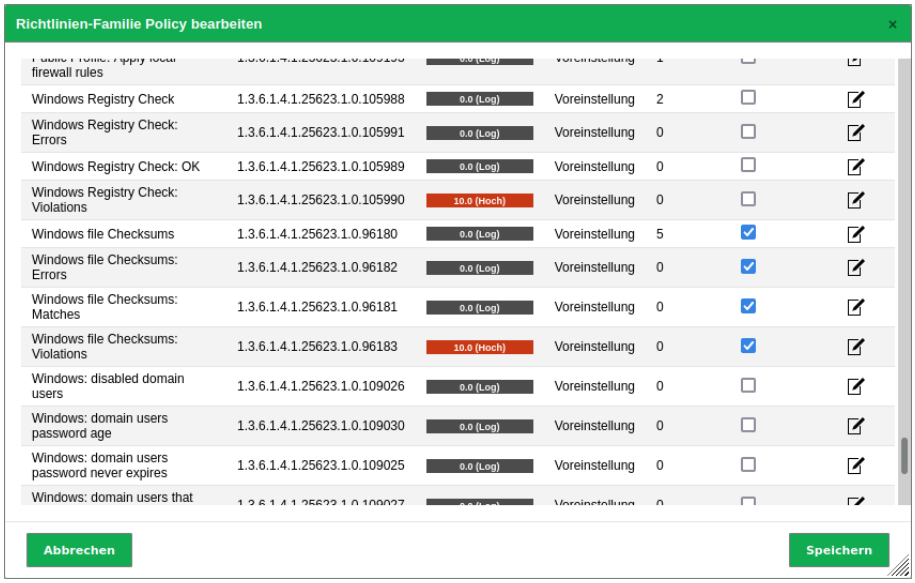


Abb. 12.18: Bearbeiten einer VT-Familie

4. Für *Windows file Checksums* auf ✎ klicken.
5. Für *Delete hash test Programm after the test* den Radiobutton *Ja* wählen, falls das Prüfsummenprogramm ReHash nach der Prüfung gelöscht werden soll (siehe Abb. 12.19).

Tipp: Das Programm kann auf dem Zielsystem verbleiben, z. B. um nachfolgende Prüfungen zu beschleunigen, und muss deshalb nicht jedes Mal übertragen werden.

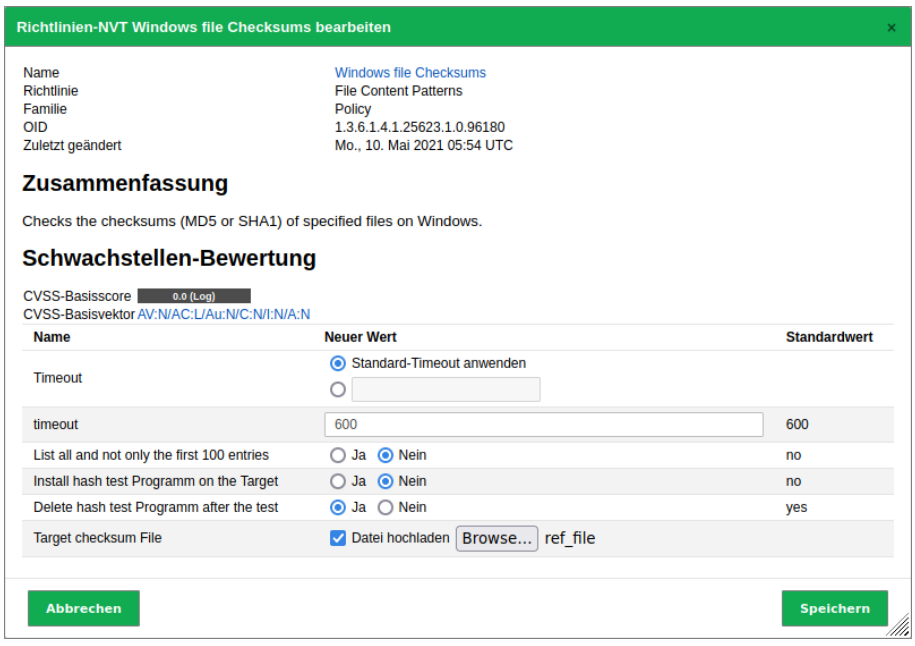


Abb. 12.19: Hochladen der Referenzdatei

6. Für *Install hash test Programm on the Target* den Radiobutton *Ja* wählen, falls das Prüfsummenprogramm ReHash automatisch auf dem Zielsystem installiert werden soll.

Bemerkung: Falls es nicht automatisch installiert wird, muss es manuell unter `C:\Windows\system32` (auf 32-Bit-Systemen) oder `C:\Windows\SysWOW64` (auf 64-Bit-Systemen) installiert werden und für den authentifizierten Benutzer ausführbar sein.

7. Checkbox *Datei hochladen* aktivieren.

Tipp: Falls bereits eine Referenzdatei hochgeladen wurde, wird stattdessen die Checkbox *Existierende Datei ersetzen* angezeigt. Die Referenzdatei kann nur geändert werden, falls die Richtlinie aktuell nicht genutzt wird.

8. Auf *Browse...* klicken und die zuvor erstellte Referenzdatei wählen.
9. Auf *Speichern* klicken, um den VT zu speichern.
10. Auf *Speichern* klicken, um die VT-Familie zu speichern.
11. Auf *Speichern* klicken, um die Richtlinie zu speichern.

12.4.4 CPE-basierte Prüfungen durchführen

Für detaillierte Informationen über Common Platform Enumeration (CPE) siehe Kapitel *14.2.2* (Seite 362).

12.4.4.1 Einfache CPE-basierte Prüfungen für Sicherheitsrichtlinien

Mit jedem ausgeführten Scan werden CPEs für die gefundenen Produkte gespeichert. Dies geschieht unabhängig davon, ob das Produkt tatsächlich ein Sicherheitsproblem darstellt oder nicht. Auf dieser Basis ist es möglich, einfache Sicherheitsrichtlinien und die Prüfungen für die Compliance mit diesen zu beschreiben.

Mit der Greenbone Enterprise Appliance ist es möglich, Richtlinien zu beschreiben, die sowohl das Vorhandensein als auch das Fehlen eines Produkt prüfen. Diese Fälle können mit einem Schweregrad in Verbindung gebracht werden, um im Scanbericht zu erscheinen.

Die Beispiele zeigen, wie die Compliance einer Richtlinie bezüglich bestimmter Produkte in einer IT-Infrastruktur geprüft wird und wie das Melden mit den entsprechenden Schweregraden durchgeführt wird.

Die Informationen darüber, ob ein bestimmtes Produkt auf dem Zielsystem vorhanden ist, wird von einem einzigen Vulnerability Test (VT) oder sogar unabhängig von einer Anzahl besonderer VTs gesammelt. Dies bedeutet, dass für ein bestimmtes Produkt eine optimierte Richtlinie bestimmt werden kann, die sich nur auf dieses Produkt konzentriert und keinerlei andere Scanaktivität durchführt.

12.4.4.2 Das Vorhandensein problematischer Produkte entdecken

Dieses Beispiel zeigt, wie das Vorhandensein eines problematischen Produkts in einer IT-Infrastruktur als schwerwiegendes Problem klassifiziert und als solches gemeldet wird.

1. *Resilience > Compliance Richtlinien* in der Menüleiste wählen.
2. Neue Richtlinie durch Klicken auf erstellen.
3. Namen der Richtlinie festlegen.
4. Auf *Speichern* klicken.

   → Die Richtlinie wird erstellt und auf der Seite *Richtlinien* angezeigt.
5. In der Zeile der Richtlinie auf klicken.

6. In der Zeile der VT-Familie *Policy* auf klicken.
7. In der Zeile des VT *CPE Policy Check* auf klicken.
8. Es kann entweder nach einer einzelnen CPE oder nach mehreren CPEs gleichzeitig gesucht werden.

   Eine einzelne CPE in das Eingabefeld *Single CPE* eingeben, z. B. `cpe:/a:microsoft:ie:6` (siehe Abb. 12.20).

   oder

   Checkbox *Datei hochladen* aktivieren, auf *Browse...* klicken und eine Datei wählen, die eine Liste von CPEs enthält.

   Bemerkung: Die Datei muss eine Textdatei sein, in der die CPEs durch Kommas oder Zeilenumbrüche getrennt sind.

9. Das problematische Produkt soll **nicht** vorhanden sein, d. h. die Bedingung muss auf *missing* gesetzt werden. Wenn das Produkt allerdings entdeckt wird, wird dies als kritisch bewertet.

   Radiobutton *missing* wählen.

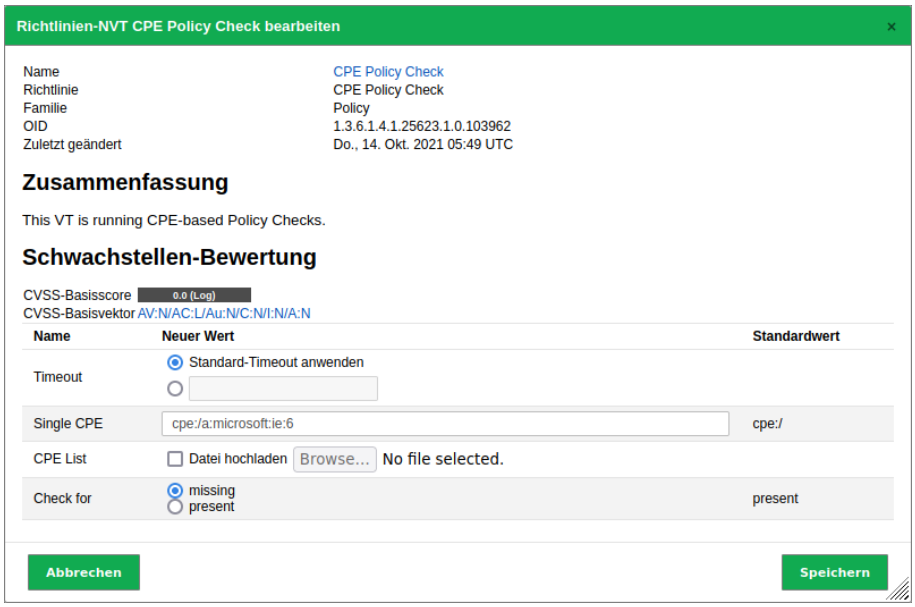


Abb. 12.20: Bearbeiten von *CPE Policy Check*

10. Auf *Speichern* klicken, um den VT zu speichern.
11. Checkbox *Ausgewählt* für folgende VTs aktivieren: *CPE Policy Check*, *CPE-based Policy Check Error*, *CPE-based Policy Check OK* und *CPE-based Policy Check Violations*.
12. Auf *Speichern* klicken, um die VT-Familie zu speichern.
13. Checkbox *Ausgewählt* für die VT-Familie *Product Detection* aktivieren (siehe Abb. 12.21).
14. Auf *Speichern* klicken, um die Richtlinie zu speichern.

Bemerkung: Falls die bloße Verfügbarkeit eines Produkts betrachtet werden soll, muss ein Remotezugriff mit Anmeldedaten konfiguriert werden, um lokale Sicherheitsprüfungen anzuwenden (siehe Kapitel *10.3.2* (Seite 222)). Falls nur nach laufenden Netzwerkdiensten gesucht werden soll, hilft dies normalerweise nicht, sondern erhöht stattdessen die Anzahl an Falsch-Positiv-Meldungen.

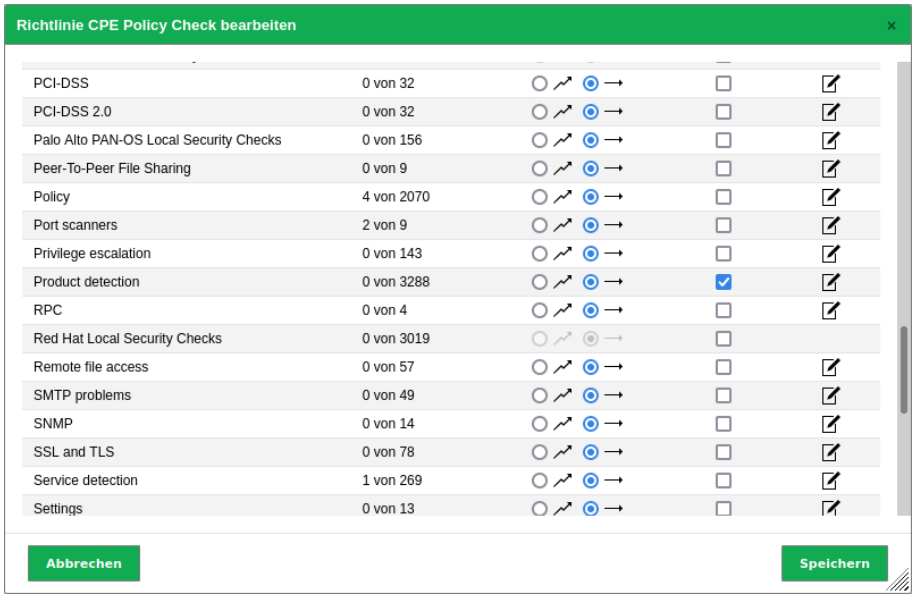


Abb. 12.21: Aktivierte VT-Familien

15. Neues Ziel erstellen (siehe Kapitel *10.2.1* (Seite 214)), neues Audit erstellen (siehe Kapitel *12.2.1.1* (Seite 325)) und Audit ausführen (siehe Kapitel *12.2.2* (Seite 327)).

    Beim Erstellen des Audits die zuvor erstellte Richtlinie nutzen.

16. Wenn der Scan abgschlossen ist, *Scans* > *Berichte* in der Menüleiste wählen.

Tipp: Um nur die Ergebnisse der CPE-basierten Richtlinienprüfungen anzuzeigen, kann ein passender Filter angewendet werden.

---

17. `cpe` in das Eingabefeld *Filter* eingeben.

    → Die Berichte für die CPE-basierten Richtlinienprüfungen werden angezeigt.

18. Auf das Datum eines Berichts klicken.

    → Der Bericht für die CPE-basierten Richtlinienprüfungen wird angezeigt.

    Der Bericht kann wie in Kapitel *11.2.1* (Seite 293) beschrieben genutzt werden.

Bemerkung: VTs der Art *Violations* haben einen standardmäßigen Schweregrad von 10.

Dieser Standard-Schweregrad kann wie in Kapitel *11.2.1* (Seite 293) beschrieben geändert werden.

Falls das problematische Produkt auf einem der Zielsysteme gefunden wurde, wird dies als Problem gemeldet.

12.5 Standardrichtlinien prüfen

12.5.1 IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI)[33] veröffentlicht das IT-Grundschutz-Kompendium[34], welches 2017 die IT-Grundschutz-Kataloge ablöste und nützliche Informationen für das Erkennen von Schwachstellen und das Bekämpfen von Angriffen auf IT-Umgebungen liefert.

Greenbone stellt eine Richtlinie bereit, die die Compliance mit den folgenden Modulen des IT-Grundschutz-Kompendiums prüft:

- SYS.1.2.2 Windows Server 2012
- SYS.1.3 Server unter Linux und Unix
- SYS.2.2.2 Clients unter Windows 8.1
- SYS.2.2.3 Clients unter Windows 10
- SYS.2.3 Clients unter Linux und Unix

Ein IT-Grundschutz-Scan kann wie folgt ausgeführt werden:

1. Neues Ziel erstellen (siehe Kapitel *10.2.1* (Seite 214)), neues Audit erstellen (siehe Kapitel *12.2.1.1* (Seite 325)) und Audit ausführen (siehe Kapitel *12.2.2* (Seite 327)).

   Beim Erstellen des Audits die Richtlinie *IT-Grundschutz Kompendium* nutzen.

2. Wenn der Scan abgschlossen ist, *Scans > Berichte* in der Menüleiste wählen.
3. Auf das Datum des Berichts klicken.

   → Der Bericht für den IT-Grundschutz-Scan wird angezeigt.

   Der Bericht kann wie in Kapitel *11.2.1* (Seite 293) beschrieben genutzt werden. Der Bericht enthält detaillierte Informationen über konforme, nicht konforme und unvollständige Anforderungen.

4. Auf klicken, um den Bericht herunterzuladen.
5. Notizen durch Aktivieren der Checkbox *Notizen* hinzufügen und Übersteuerungen durch Aktivieren der Checkbox *Übersteuerungen* kennzeichnen und ihr Textfeld einfügen (siehe Kapitel *11.2.2* (Seite 298)).
6. *GCR PDF* in der Drop-down-Liste *Berichtformat* wählen.
7. Auf *OK* klicken und die PDF-Datei herunterladen.

[33] https://www.bsi.bund.de/DE/Home/home_node.html
[34] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

12.5.2 BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte eine technische Richtlinie TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung[35]. Teil 4 dieser Richtlinie beschreibt die Sicherheitsanforderungen für Dienste der Bundesregierung unter Nutzung der kryptografischen Protokolle SSL/TLS, S/MIME und OpenPGP.

Die Anforderungen basieren auf Vorhersagen für die Sicherheit der Algorithmen und Schlüssellängen für die nächsten Jahre.

Greenbone stellt eine Richtlinie bereit, die die Compliance der Dienste mit der technischen Richtlinie „TR-03116“ prüft.

Die Richtlinie prüft, ob die gescannten Hosts und Dienste SSL/TLS nutzen. Falls dies der Fall ist, wird die Compliance mit der Richtlinie getestet.

Die Richtlinie nennt drei Hauptanforderungen:

TLS-Version TLS-Versionen unter 1.2 sind nicht zulässig.

Unterstützte Ciphers Wenn TLS 1.2 aktiviert ist, muss eine der folgenden Ciphers unterstützt werden:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Wenn TLS 1.3 aktiviert ist, muss die Cipher TLS_AES_128_GCM_SHA256 unterstützt werden.

Erlaubte Cipher-Suites Wenn TLS 1.2 aktiviert ist, sind nur die folgenden Cipher-Suites zulässig:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

[35] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html

Wenn TLS 1.3 aktiviert ist, sind nur die folgenden Cipher-Suites zulässig:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256

Ein BSI-TR-03116-Scan kann wie folgt ausgeführt werden:

1. Neues Ziel erstellen (siehe Kapitel *10.2.1* (Seite 214)), neues Audit erstellen (siehe Kapitel *12.2.1.1* (Seite 325)) und Audit ausführen (siehe Kapitel *12.2.2* (Seite 327)).

   Beim Erstellen des Audits die Richtlinie *BSI TR-03116: Part 4* nutzen.

2. Wenn der Scan abgschlossen ist, *Scans > Berichte* in der Menüleiste wählen.

3. Auf das Datum des Berichts klicken.

   → Der Bericht für den BSI-TR-03116-Scan wird angezeigt.

   Der Bericht kann wie in Kapitel *11.2.1* (Seite 293) beschrieben genutzt werden. Der Bericht enthält detaillierte Informationen über konforme, nicht konforme und unvollständige Anforderungen.

4. Auf ⬇ klicken, um den Bericht herunterzuladen.

5. Notizen durch Aktivieren der Checkbox *Notizen* hinzufügen und Übersteuerungen durch Aktivieren der Checkbox *Übersteuerungen* kennzeichnen und ihr Textfeld einfügen (siehe Kapitel *11.2.2* (Seite 298)).

6. *GCR PDF* in der Drop-down-Liste *Berichtformat* wählen.

7. Auf *OK* klicken und die PDF-Datei herunterladen.

12.5.3 BSI TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht eine technische Richtlinie TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen[36]. Teil 4 dieser Richtlinie beschreibt die Empfehlungen für die Nutzung des kryptographischen Protokolls Secure Shell (SSH).

Greenbone stellt eine Richtlinie bereit, die die Compliance der Dienste mit der technischen Richtlinie „TR-02102“ prüft.

Die folgenden SSH-Einstellungen in der Datei `/etc/ssh/sshd_config` werden in der Richtlinie getestet:

- Protocol (OID: 1.3.6.1.4.1.25623.1.0.150066): SSH-Version 2 muss genutzt werden.
- KexAlgorithms (OID: 1.3.6.1.4.1.25623.1.0.150077): Die folgenden Algorithmen sind für den Schlüsselaustausch während des SSH-Verbindungsaufbaus erlaubt: diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha256, diffie-hellman-group15-sha512, diffie-hellman-group16-sha512, rsa2048-sha256, ecdh-sha2-*
- ReKeyLimit (OID: 1.3.6.1.4.1.25623.1.0.150560): Das Schlüsselmaterial einer Verbindung muss nach 1 Stunde oder nach 1GiB übertragener Daten erneuert werden.
- Ciphers (OID: 1.3.6.1.4.1.25623.1.0.150225): Die folgenden Verschlüsselungsmethoden sind zulässig: AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes256-cbc, aes192-cbc, aes128-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- MACs (OID: 1.3.6.1.4.1.25623.1.0.109795): Die folgenden MACs sind zulässig: hmac-sha1, hmac-sha2-256, hmac-sha2-512

[36] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html?nn=451438

- HostKeyAlgorithms (OID: 1.3.6.1.4.1.25623.1.0.150559): Die folgenden Methoden zur Server-Authentisierung sind zulässig: pgp-sign-rsa, pgp-sign-dss, ecdsa-sha2-*, x509v3-rsa2048-sha256, x509v3-ecdsa-sha2-*
- AuthenticationMethods (OID: 1.3.6.1.4.1.25623.1.0.150561): Die Public-Key-Authentifizierungsmethode (*publickey*) muss genutzt werden.
- PubkeyAuthentication (OID: 1.3.6.1.4.1.25623.1.0.150222): Die Public-Key-Authentifizierungsmethode (*publickey*) muss zulässig sein.

Ein BSI-TR-02102-Scan kann wie folgt ausgeführt werden:

1. Neues Ziel erstellen (siehe Kapitel *10.2.1* (Seite 214)), neues Audit erstellen (siehe Kapitel *12.2.1.1* (Seite 325)) und Audit ausführen (siehe Kapitel *12.2.2* (Seite 327)).

   Beim Erstellen des Audits die Richtlinie *BSI TR-02102-4* nutzen.

2. Wenn der Scan abgschlossen ist, *Scans > Berichte* in der Menüleiste wählen.
3. Auf das Datum des Berichts klicken.

   → Der Bericht für den BSI-TR-02102-Scan wird angezeigt.

   Der Bericht kann wie in Kapitel *11.2.1* (Seite 293) beschrieben genutzt werden. Der Bericht enthält detaillierte Informationen über konforme, nicht konforme und unvollständige Anforderungen.

4. Auf klicken, um den Bericht herunterzuladen.
5. Notizen durch Aktivieren der Checkbox *Notizen* hinzufügen und Übersteuerungen durch Aktivieren der Checkbox *Übersteuerungen* kennzeichnen und ihr Textfeld einfügen (siehe Kapitel *11.2.2* (Seite 298)).
6. *GCR PDF* in der Drop-down-Liste *Berichtformat* wählen.
7. Auf *OK* klicken und die PDF-Datei herunterladen.

12.6 Einen TLS-Map-Scan durchführen

Das Protokoll Transport Layer Security (TLS) stellt die Vertraulichkeit, Authentizität und Integrität der Kommunikation in unsicheren Netzwerken sicher. Es richtet eine vertrauliche Kommunikation zwischen Sender und Empfänger, z. B. Webserver und Webbrowser, ein.

Mit der Greenbone Enterprise Appliance können Systeme gefunden werden, die Dienste anbieten, die SSL/TLS-Protokolle nutzen. Zusätzlich erkennt die Appliance die Protokollversionen und bietet Verschlüsselungsalgorithmen. Weiterführende Details eines Diensts können gewonnen werden, falls er korrekt identifiziert werden kann.

12.6.1 Auf TLS prüfen und die Scanergebnisse exportieren

Für einen Überblick über die TLS-Verwendung im Netzwerk oder auf einzelnen Systemen, empfiehlt Greenbone die Nutzung der Scan-Konfiguration *TLS-Map*. Diese Scan-Konfiguration erkennt die genutzten Protokollversionen und die angebotenen Verschlüsselungsalgorithmen. Zusätzlich versucht sie, tiefergehende Details des Diensts zu identifizieren.

1. *Konfiguration > Portlisten* in der Menüleiste wählen, um die vorkonfigurierten Portlisten anzusehen.

   Bemerkung: Durch Klicken auf ☆ können eigene Portlisten erstellt werden (siehe Kapitel *10.7.1* (Seite 255)).

2. Passende Portliste, die gescannt werden soll, wählen.

   Bemerkung: Es muss darauf geachtet werden, dass alle Ports von Interesse durch die Liste abgedeckt werden.

   Je umfangreicher die Liste ist, desto länger dauert der Scan. Allerdings werden möglicherweise auch Dienste auf unüblichen Ports gefunden.

   Das TLS-Protokoll basiert hauptsächlich auf TCP. Eine Portliste mit UDP-Ports verlangsamt den Scan, ohne gleichzeitig Vorteile zu bringen. Falls TCP-Ports abgedeckt werden sollen, sollte *All TCP* gewählt werden.

3. Neues Ziel erstellen (siehe Kapitel *10.2.1* (Seite 214)), neue Aufgabe erstellen (siehe Kapitel *10.2.2* (Seite 218)) und Aufgabe ausführen (siehe Kapitel *10.2.3* (Seite 220)).

   Beim Erstellen der Aufgabe die Scan-Konfiguration *TLS-Map* nutzen.

4. Wenn der Scan abgschlossen ist, *Scans > Berichte* in der Menüleiste wählen.

5. Auf das Datum des Berichts klicken.

   → Der Bericht für den TLS-Map-Scan wird angezeigt.

   Der Bericht kann wie in Kapitel *11.2.1* (Seite 293) beschrieben genutzt werden.

6. Auf ⤓ klicken, um den Bericht herunterzuladen.

7. Notizen durch Aktivieren der Checkbox *Notizen* hinzufügen und Übersteuerungen durch Aktivieren der Checkbox *Übersteuerungen* kennzeichnen und ihr Textfeld einfügen (siehe Kapitel *11.2.2* (Seite 298)).

8. *TLS Map* in der Drop-down-Liste *Berichtformat* wählen.

9. Auf *OK* klicken und die CSV-Datei herunterladen.

   → Der Bericht kann in Anwendungen zur Tabellenkalkulation genutzt werden.

Die Datei enthält jeweils eine Zeile pro Port und System, auf dem ein Dienst unter Verwendung eines SSL-/TLS-Protokolls angeboten wird:

```
IP,Host,Port,TLS-Version,Ciphers,Application-CPE
192.168.12.34,www.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22;cpe:/a:php:php:5.4.4
192.168.56.78,www2.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22
```

Jede Zeile enhält die folgenden, kommagetrennten Informationen:

- **IP** Die IP-Adresse des Systems, auf dem der Dienst gefunden wurde.
- **Host** Falls verfügbar, der DNS-Name des Systems.
- **Port** Der Port, auf dem der Dienst gefunden wurde.
- **TLS-Version** Die Protokollversion, die vom Dienst angeboten wird. Falls mehr als eine Version angeboten wird, werden die Versionen durch Semikolons getrennt.
- **Ciphers** Die Verschlüsselungsalgorithmen, die vom Dienst angeboten werden. Falls mehr als ein Algorithmus angeboten wird, werden die Algorithmen durch Semikolons getrennt.
- **Application-CPE** Die gefundene Anwendung im CPE-Format. Falls mehr als eine Anwendung gefunden wird, werden die Anwendungen durch Semikolons getrennt.

KAPITEL 13

Assets verwalten

Zu den Assets gehören Hosts, Betriebssysteme und TLS-Zertifikate. Sie werden während der Schwachstellenscans gesammelt.

Bei der Erstellung einer neuen Aufgabe kann angegeben werden, ob die bei einer Prüfung gesammelten Host-Details in der Asset-Datenbank gespeichert werden sollen (siehe Kapitel *10.2.2* (Seite 218)). Die Details werden gespeichert, wenn die Standardaufgabeneinstellungen verwendet werden.

13.1 Hosts erstellen und verwalten

Während eines Scans werden Informationen über jeden gescannten Host gesammelt. Die Hosts werden anhand ihrer IP-Adressen identifiziert.

Für jeden identifizierten Host wird geprüft, ob er bereits in den Host-Assets vorhanden ist. Wenn nicht, wird ein neues Host-Asset erstellt.

Sowohl beim Scannen eines neu erstellten Hosts als auch beim Scannen eines vorhandenen Hosts werden verschiedene Hostdetails (Hostnamen, IP- und MAC-Adressen, Betriebssysteme, SSH-Schlüssel und X.509-Zertifikate) als Identifikatoren zum Host-Asset hinzugefügt.

Wenn das Scannen von vHosts[37] aktiviert ist – was standardmäßig der Fall ist – (siehe Kapitel *10.13.4* (Seite 287)), wird jeder vHost als eigener Asset-Eintrag hinzugefügt. Aufgrund der Beschaffenheit von vHosts können IP-Adressbezeichner daher mehrfach vorkommen. Solche Assets müssen dann durch ihre anderen Host-Identifikatoren unterschieden werden.

[37] https://httpd.apache.org/docs/current/de/vhosts/

13.1.1 Einen Host erstellen

Hosts können auch manuell zur Assetverwaltung hinzugefügt werden, um Ziele aus ihnen zu erstellen (siehe Kapitel *13.1.3* (Seite 352)).

Außer der IP-Adresse können keine weiteren Details zum Host definiert werden, diese werden jedoch beim Scannen des manuell hinzugefügten Hosts ergänzt.

Ein Host kann wie folgt erstellt werden:

1. *Assets* > *Hosts* in der Menüleiste wählen.
2. Neuen Host durch Klicken auf in der linken oberen Ecke der Seite erstellen.
3. IP-Adresse des Hosts in das Eingabefeld *Name* eingeben (siehe Abb. 13.1).

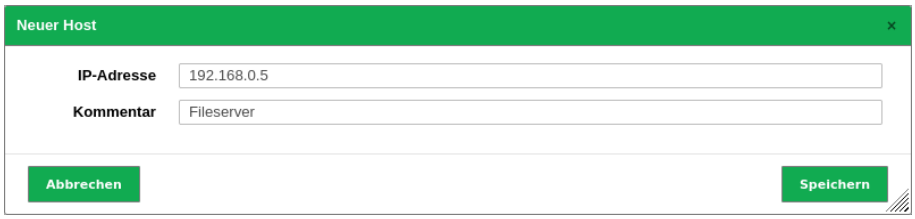


Abb. 13.1: Erstellen eines neuen Hosts

4. Auf *Speichern* klicken.

Diese Funktion ist auch über GMP verfügbar (siehe Kapitel *15* (Seite 370)). Der Import von Hosts aus einer Datenbank zum Verwalten von Konfigurationen kann durch diese Option umgesetzt werden.

13.1.2 Hosts verwalten

Listenseite

Alle vorhandenen Hosts können angezeigt werden, indem *Assets* > *Hosts* in der Menüleiste gewählt wird (siehe Abb. 13.2).

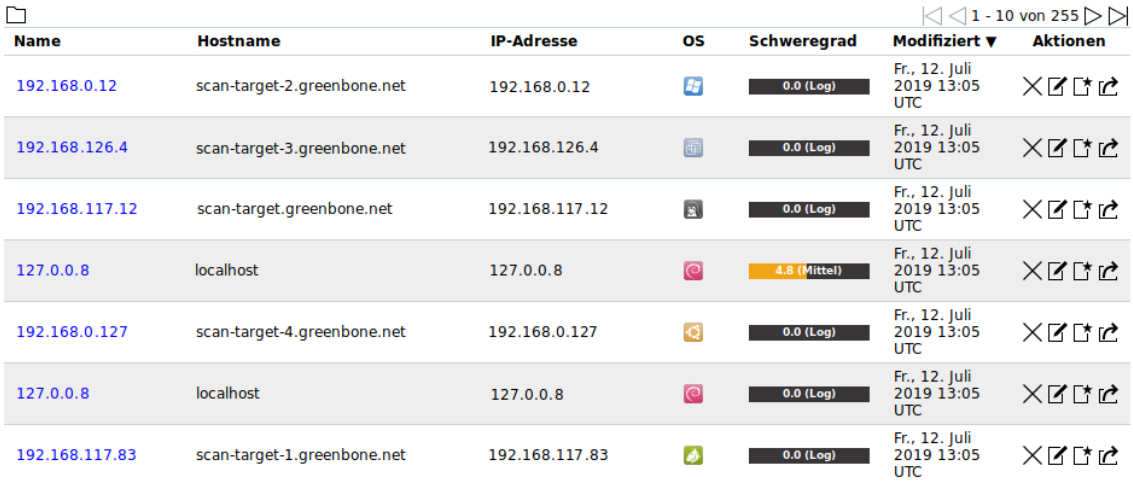


Abb. 13.2: Seite *Hosts* mit allen gescannten Hosts

Für alle Hosts sind die folgenden Aktionen verfügbar:

- Den Host löschen.
- Den Host bearbeiten.
- Ein Ziel aus dem Host erstellen (siehe Kapitel *13.1.3* (Seite 352)).
- Den Host als XML-Datei exportieren.

Bemerkung: Durch Klicken auf , oder unterhalb der Liste von Hosts können mehrere Hosts zur gleichen Zeit gelöscht, exportiert oder für das Erstellen eines neuen Ziels genutzt werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Hosts gelöscht, exportiert oder für das Erstellen eines neuen Ziels genutzt werden.

Detailseite

Durch Klicken auf den Namen eines Hosts werden Details des Hosts angezeigt. Durch Klicken auf wird die Detailseite des Hosts geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über den Host.

Alle identifizierenden Informationen, die für einen Host während der Scans gesammelt werden, z. B. Hostnamen, IP- und MAC-Adressen, Betriebssysteme, SSH-Schlüssel und X.509-Zertifikate, werden im Abschnitt *Alle Identifikatoren* angezeigt (siehe Abb. 13.3).

Bemerkung: Falls Identifikatoren Duplikate besitzen, werden nur die neuesten Identifikatoren angezeigt. In diesem Fall heißt der Abschnitt *Neueste Identifikatoren* und alle Identifikatoren können durch Klicken auf *Alle Identifikatoren anzeigen* unterhalb der Tabelle angezeigt werden.

Für alle Host-Identifikatoren ist die folgende Aktion verfügbar:

- Den Identifikator löschen.

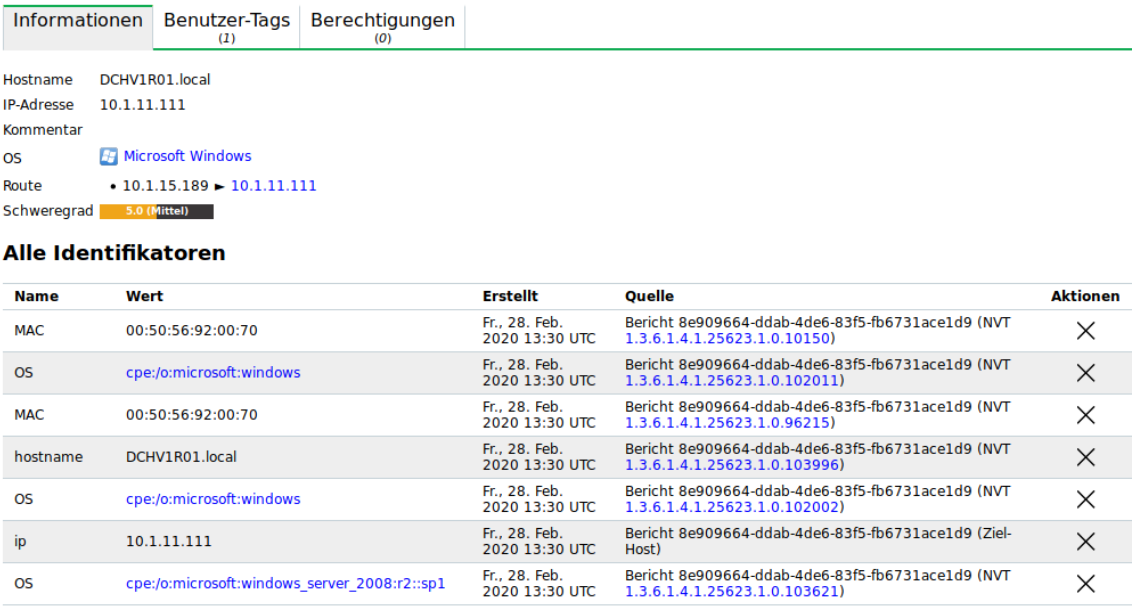


Abb. 13.3: Alle Identifikatoren

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Hosts anzeigen.
- Einen neuen Host erstellen (siehe Kapitel *13.1.1* (Seite 350)).
- Den Host bearbeiten.
- Den Host löschen.
- Den Host als XML-Datei exportieren.
- Die dazugehörigen Ergebnisse anzeigen.

13.1.3 Ein Ziel aus Hosts erstellen

Ein Ziel mit einem Set von Hosts kann wie folgt erstellt werden:

1. Hosts filtern, sodass nur die Hosts angezeigt werden, die für das Ziel genutzt werden sollen (z. B. nur Microsoft-Windows-Hosts) (siehe Kapitel *8.3* (Seite 168)).
2. Neues Ziel durch Klicken auf unterhalb der Liste von Hosts erstellen (siehe Abb. 13.4).

   → Das Fenster zum Erstellen eines neuen Ziels wird geöffnet. Das Eingabefeld *Hosts* ist bereits mit dem Set von Hosts ausgefüllt.

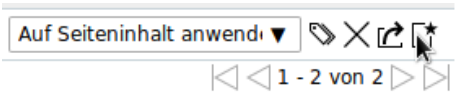


Abb. 13.4: Erstellen eines Ziels mit den angezeigten Hosts

3. Ziel definieren und auf *Speichern* klicken.

Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *10.2.1* (Seite 214).

Bemerkung: Falls zusätzliche, passende Hosts in zukünftigen Scans auftauchen, werden diese **nicht** zum Ziel hinzugefügt.

13.2 Betriebssysteme verwalten

Die Betriebssystemansicht in der Assetverwaltung bietet eine andere Sicht auf die gespeicherten Daten. Während die Hostansicht auf die einzelnen Hosts ausgerichtet ist, konzentriert sich diese Ansicht auf die Betriebssysteme, die bei allen Schwachstellenscans erkannt wurden.

Bemerkung: Für eine zuverlässige Betriebssystemerkennung müssen im Greenbone Enterprise Feed spezifische VTs für das/die betreffende(n) Betriebssystem(e) verfügbar sein. Wenn keine spezifischen VTs verfügbar sind, versucht die Appliance trotzdem, das/die Betriebssystem(e) zu identifizieren, aber die Identifizierung erfolgt mit einer geringeren Erkennungsqualität und ist anfällig für falsch-positive Erfassungen.

Listenseite

Alle vorhandenen Betriebssysteme können angezeigt werden, indem *Assets* > *Betriebssysteme* in der Menüleiste gewählt wird (siehe Abb. 13.5).

Für alle Betriebssysteme werden die folgenden Informationen angezeigt:

Name CPE (siehe Kapitel *14.2.2* (Seite 362)) des Betriebssystems.

Titel Klartextname des Betriebssystems.

Schweregrad – Neueste Schweregrad, der für das Betriebssystem beim letzten Scan, bei dem dieses Betriebssystem auf einem Host gefunden wurde, bestimmt wurde. Es werden nur Hosts berücksichtigt, bei denen das betreffende Betriebssystem als passendstes Betriebssystem ermittelt wurde.

Schweregrad – Höchster Höchster Schweregrad, der für das Betriebssystem bei allen Scans, die dieses Betriebssystem auf einem Host gefunden haben, beestimmt wurde. Es werden nur Hosts berücksichtigt, bei denen das betreffende Betriebssystem als passendstes Betriebssystem ermittelt wurde.

Schweregrad – Durchschnitt Durchschnittlicher Schweregrad, der für das Betriebssystem bei allen Scans, die dieses Betriebssystem auf einem Host gefunden haben, bestimmt wurde. Es werden nur Hosts berücksichtigt, bei denen das betreffende Betriebssystem als passendstes Betriebssystem ermittelt wurde.

Hosts – Alle Alle Hosts, auf denen das Betriebssystem erkannt wurde. Durch Klicken auf die Anzahl der Hosts wird die Seite *Hosts* geöffnet. Ein Filter ist angewendet, um nur die Hosts anzuzeigen, für die das gewählte Betriebssystem erkannt wurde.

Hosts – Bestes OS Alle Hosts, auf denen das Betriebssystem als passendstes Betriebssystem erkannt wurde. Durch Klicken auf die Anzahl der Hosts wird die Seite *Hosts* geöffnet. Ein Filter ist angewendet, um nur die Hosts anzuzeigen, für die das gewählte Betriebssystem als passendstes Betriebssystem erkannt wurde.

Geändert Datum und Zeit der letzten Veränderung.

Für alle Betriebssysteme sind die folgenden Aktionen verfügbar:

- ✕ Das Betriebssystem löschen. Nur Betriebssysteme, die aktuell nicht genutzt werden, können gelöscht werden.
- ⇪ Das Betriebssystem als XML-Datei exportieren.

Bemerkung: Durch Klicken auf ✕ oder ⇪ unterhalb der Liste von Betriebssystemen können mehrere Betriebssysteme zur gleichen Zeit gelöscht oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche Betriebssysteme gelöscht oder exportiert werden.

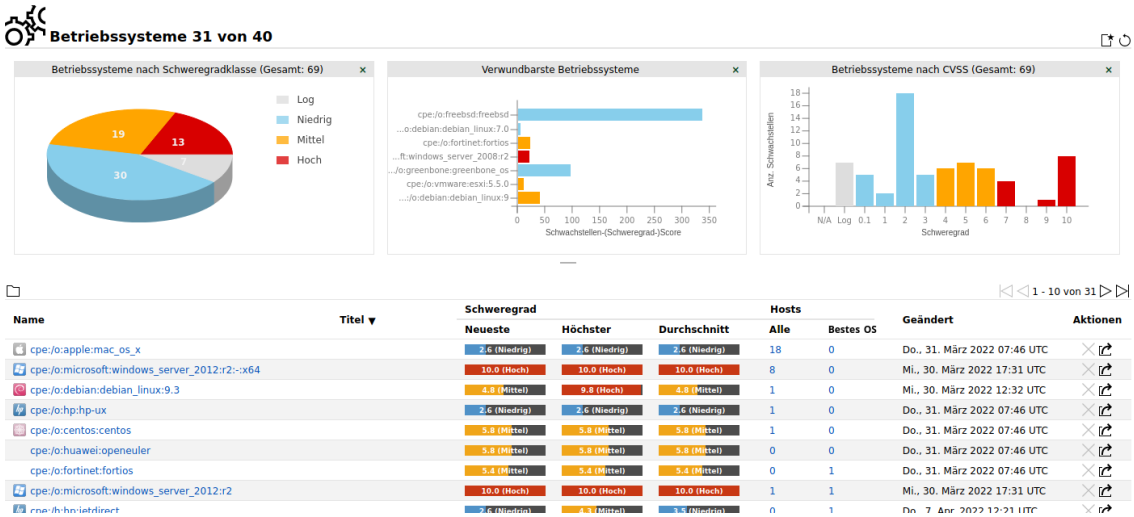


Abb. 13.5: Seite *Betriebssysteme* mit allen gescannten Betriebssystemen

Detailseite

Durch Klicken auf den Namen eines Betriebssystems wird die Detailseite des Betriebssystems geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das Betriebssystem.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen Betriebssystemen anzeigen.
- Das Betriebssystem löschen. Nur Betriebssysteme, die aktuell nicht genutzt werden, können gelöscht werden.
- Das Betriebssystem als XML-Datei exportieren.
- (links) Die Hosts anzeigen, für die das Betriebssystem erkannt wurde.
- (rechts) Die Hosts anzeigen, für die das Betriebssystem als passendstes Betriebssystem erkannt wurde.

13.3 TLS-Zertifikate verwalten

Diese Ansicht konzentriert sich auf die TLS-Zertifikate, die bei allen Schwachstellenscans gesammelt wurden, und bietet einen schnellen Überblick darüber, ob sie gültig oder abgelaufen sind.

Bemerkung: Nur grundlegende Zertifikatsinformationen (Host, Port, Aktivierungs- und Ablaufdatum, Fingerprints) sind enthalten.

Es gibt keine Unterstützung für die Funktionen des Online Certificate Status Protocol (OCSP) oder der Certificate Revocation List (CRL).

Listenseite

Alle vorhandenen TLS-Zertifikate können angezeigt werden, indem *Assets* > *TLS-Zertifikate* in der Menüleiste gewählt wird (siehe Abb. 13.6).

Für alle TLS-Zertifikate sind die folgenden Aktionen verfügbar:

- Das TLS-Zertifikat löschen.
- Das TLS-Zertifikat herunterladen.
- Das TLS-Zertifikat als XML-Datei exportieren.

Bemerkung: Durch Klicken auf oder unterhalb der Liste von TLS-Zertifikaten können mehrere TLS-Zertifikate zur gleichen Zeit gelöscht oder exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche TLS-Zertifikate gelöscht oder exportiert werden.

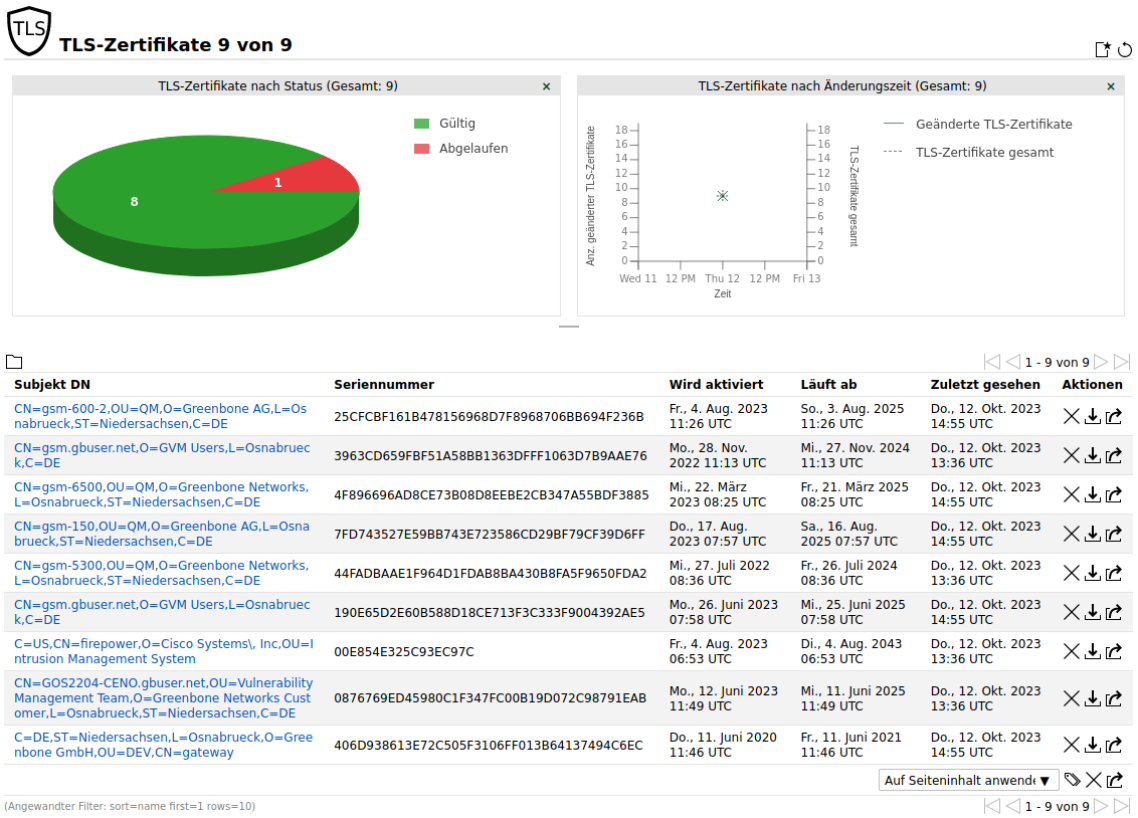


Abb. 13.6: Seite *TLS-Zertifikate* mit allen gesammelten TLS-Zertifikaten

Detailseite

Durch Klicken auf den Namen eines TLS-Zertifikats werden Details des TLS-Zertifikats angezeigt. Durch Klicken auf 🔍 wird die Detailseite des TLS-Zertifikats geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das TLS-Zertifikat.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Berechtigungen Zugewiesene Berechtigungen (siehe Kapitel *9.4* (Seite 195)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- ⓘ Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- ☰ Die Listenseite mit allen TLS-Zertifikaten anzeigen.
- ✕ Das TLS-Zertifikat löschen.
- ⬇ Das TLS-Zertifikat herunterladen.
- ⇪ Das TLS-Zertifikat als XML-Datei exportieren.

KAPITEL 14

Sicherheitsinfos verwalten

Die Verwaltung der Sicherheitsinfos bietet einen zentralen Zugang zu einer Vielzahl von Sicherheitsinformationen bezüglich der Informationstechnologie (IT), einschließlich der folgenden Kategorien:

Vulnerability Tests (VT) VTs prüfen das Zielsystem auf potentielle Schwachstellen.

Common Vulnerabilities and Exposures (CVE) CVEs sind Schwachstellen, die von den Herstellern oder Sicherheitsforschern veröffentlich wurden.

Common Platform Enumeration (CPE) CPE bietet standardisierte Namen für Produkte, die in der IT genutzt werden.

CERT-Bund-Advisories CERT-Bund-Advisories werden vom CERT-Bund[38], dem Computer Emergency Response Team des Bundesamts für Sicherheit in der Informationstechnik (BSI)[39], veröffentlicht. Die Hauptaufgabe des CERT-Bunds ist der Betrieb eines Warn- und Informationsdiensts, welcher Informationen über neue Schwachstellen und Sicherheitsrisiken sowie über Bedrohungen für IT-Systeme herausgibt.

DFN-CERT-Advisories DFN-CERT-Advisories werden vom DFN-CERT[40], dem Computer Emergency Response Team des Deutschen Forschungsnetzes (DFN)[41], veröffentlicht.

CVEs und CPEs werden vom National Institute of Standards and Technology (NIST)[42] als Teil der National Vulnerability Database (NVD)[43] veröffentlicht und zugänglich gemacht (siehe Kapitel *14.2* (Seite 359)).

Bemerkung: Greenbone bietet alle Sicherheitsinfodaten zusätzlich online über das SecInfo-Portal[44] an. Das SecInfo-Portal stellt alle Sicherheitsinfos, welche im folgenden Kapitel beschrieben werden, und den CVSS-Rechner bereit.

Zugang zum SecInfo-Portal ist durch Aktivierung eines Gastzugangs umgesetzt (siehe Kapitel *9.1.3* (Seite 188)).

[38] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html
[39] https://www.bsi.bund.de/DE/Home/home_node.html
[40] https://www.dfn-cert.de/index.html
[41] https://www.dfn.de/
[42] https://www.nist.gov
[43] https://nvd.nist.gov/
[44] https://secinfo.greenbone.net

14.1 Vulnerability Tests (VT)

VTs sind Prüfroutinen, die von der Appliance genutzt werden. Sie sind Teil des Greenbone Enterprise Feeds, welcher regelmäßig aktualisiert wird. VTs enthalten Informationen über das Entwicklungsdatum, die betroffenen Systeme, die Auswirkungen von Schwachstellen und die Beseitigung.

Listenseite

Alle vorhandenen VTs können angezeigt werden, indem *Sicherheitsinfos > NVTs* in der Menüleiste gewählt wird.

Für alle VTs werden die folgenden Informationen angezeigt:

Name Name des VTs.

Familie VT-Familie, zu der der VT gehört.

Erstellt Datum und Zeit der Erstellung.

Modifiziert Datum und Zeit der letzten Veränderung.

CVE CVE, die mithilfe des VTs geprüft wird.

Art der Lösung Lösung für die Schwachstelle. Die folgenden Lösungen sind möglich:

- Eine Herstellerlösung ist verfügbar.
- Eine Problemumgehung ist verfügbar.
- Eine Schadensminderung ist verfügbar.
- Es ist kein Fix verfügbar oder wird verfügbar sein.
- Es ist keine Lösung vorhanden.

Schweregrad Der Schweregrad der Schwachstelle (CVSS, siehe Kapitel *14.2.3* (Seite 363)) wird als Balken angezeigt, um die Analyse der Ergebnisse zu unterstützen.

QdE QdE ist kurz für Qualität der Erkennung und gibt an, wie verlässlich die Erkennung einer Schwachstelle ist.

Mit der Einführung von QdE wurde der Parameter *Paranoid* in der Scan-Konfiguration (siehe Kapitel *10.9* (Seite 261)) ersatzlos entfernt. In der Vergangenheit nutzte eine Scan-Konfiguration mit diesem Parameter nur VTs mit einer QdE von mindestens 70 %. Nun werden alle VTs einer Scan-Konfiguration genutzt und ausgeführt.

Bemerkung: Durch Klicken auf unterhalb der Liste von VTs können mehrere VTs zur gleichen Zeit exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche VTs exportiert werden.

Detailseite

Durch Klicken auf den Namen eines VTs werden Details des VTs angezeigt. Durch Klicken auf wird die Detailseite des VTs geöffnet.

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen VTs anzeigen.
- Den VT als XML-Datei exportieren.
- Eine neue Notiz für den VT erstellen (siehe Kapitel *11.7.1* (Seite 312)).
- Eine neue Übersteuerung für den VT erstellen (siehe Kapitel *11.8.1* (Seite 315)).

- Die zugehörigen Ergebnisse anzeigen.
- Die zugehörige Schwachstelle anzeigen.

14.2 Security Content Automation Protocol (SCAP)

Das National Institute of Standards and Technology (NIST)[45] bietet die National Vulnerability Database (NVD)[46] an. Die NVD ist ein Datenspeicher für das Schwachstellenmanagement der US-Regierung. Das Ziel ist die standardisierte Bereitstellung von Daten für eine automatisierte Bearbeitung. Damit wird das Schwachstellenmanagement unterstützt und die Implementierung von Compliance-Richtlinien verifiziert.

Die NVD liefert verschiedene Datenbanken, einschließlich der Folgenden:

- Checklisten
- Schwachstellen
- Fehlkonfigurationen
- Produkte
- Gefährdungsmaße

Die NVD nutzt das Security Content Automation Protocol[47] (SCAP). SCAP ist eine Kombination aus unterschiedlichen interoperablen Standards. Viele Standards wurden aus öffentlichen Diskussionen entwickelt oder abgeleitet.

Die öffentliche Teilnahme der Gemeinschaft bei der Entwicklung ist ein wichtiger Aspekt für die Annahme und Verteilung von SCAP-Standards. SCAP ist aktuell in Version 1.3 definiert und enthält die folgenden Komponenten:

- **Sprachen**
  - XCCDF: Extensible Configuration Checklist Description Format
  - OVAL: Open Vulnerability and Assessment Language
  - OCIL: Open Checklist Interactive Language
  - Asset Identification
  - ARF: Asset Reporting Format
- **Sammlungen**
  - CCE: Common Configuration Enumeration
  - CPE: Common Platform Enumeration
  - CVE: Common Vulnerabilities and Exposure
- **Maße**
  - CVSS: Common Vulnerability Scoring System
  - CCSS: Common Configuration Scoring System
- **Integrität**
  - TMSAD: Trust Model for Security Automation Data

[45] https://www.nist.gov
[46] https://nvd.nist.gov/
[47] https://csrc.nist.gov/projects/security-content-automation-protocol/

OVAL, CCE, CPE und CVE sind Warenzeichen des NIST.

Die Greenbone Enterprise Appliance nutzt CVE, CPE und CVSS. Durch die Nutzung dieser Standards wird die Interoperabilität mit anderen Systemen gewährleistet. Zusätzlich erlauben die Standards den Vergleich von Ergebnissen.

Schwachstellen-Bewertungssysteme wie die Greenbone Enterprise Appliance können entsprechend durch NIST validiert werden. Die Greenbone Enterprise Appliance wurde hinsichtlich SCAP Version 1.0[48] validiert.

14.2.1 CVE

Um die mehrfache Benennung derselben Schwachstelle durch verschiedene Organisationen zu vermeiden und eine einheitliche Namenskonvention zu gewährleisten, gründete MITRE[49] das Projekt Common Vulnerabilities and Exposure (CVE)[50]. Jeder Schwachstelle wird ein eindeutiger Bezeichner zugewiesen, der aus dem Jahr der Veröffentlichung und einer einfachen Nummer besteht. Diese Kennung dient als zentrale Referenz.

Die CVE-Datenbank von MITRE ist jedoch keine Schwachstellendatenbank. Stattdessen verbindet sie die Schwachstellendatenbank und andere Systeme miteinander und ermöglicht den Vergleich von Sicherheitswerkzeugen und -diensten. Die CVE-Datenbank enthält keine detaillierten technischen Informationen oder Informationen über das Risiko, die Auswirkungen oder die Behebung der Schwachstelle, sondern nur die Identifikationsnummer mit dem Status, eine kurze Beschreibung und Verweise auf Berichte und Advisories.

Die National Vulnerability Database (NVD)[51] bezieht sich auf die CVE-Datenbank und ergänzt den Inhalt mit Informationen über die Beseitigung, den Schweregrad, die möglichen Auswirkungen und die betroffenen Produkte der Schwachstelle. Greenbone bezieht sich auf die CVE-Datenbank der NVD und die Appliance kombiniert die CVE-Informationen, VTs und CERT-Bund-/DFN-CERT-Advisories.

Listenseite

Alle vorhandenen CVEs können angezeigt werden, indem *Sicherheitsinfos > CVEs* in der Menüleiste gewählt wird.

Bemerkung: Die Verfügbarkeit einer CVE auf der Appliance hängt von ihrer Verfügbarkeit in der NVD ab. Sobald sie dort veröffentlicht wurde, dauert es 1–2 Arbeitstage, bis sie in den Sicherheitsinfos erscheint.

Spalten wie *Schweregrad* können aus einem der folgenden Gründe *N/A* anzeigen:

- Die CVE wurde veröffentlicht, aber es wurde vom NVD noch keine Schwachstellenanalyse/Schweregradbewertung vorgenommen. Dies kann von einigen Tagen bis zu einigen Wochen dauern.

  Solche CVEs können erkannt werden, wenn der zugehörigen Eintrag[52] durchsucht wird. Solange dort *Undergoing Analysis* angezeigt wird, wird für die CVE in den Spalten *N/A* gezeigt.

- Zwischen der Schwachstellenanalyse/Schweregradbewertung und der Anzeige der aktualisierten Informationen in den Sicherheitsinfos liegt immer eine Verzögerung von 1–2 Werktagen.

Die Spalte *CVSS Base Vector* zeigt den CVSS-Vektor, der für die Berechnung des Schweregrads einer CVE verwendet wird. Dieser Vektor enthält die für die CVE definierte CVSS-Version.

Durch Klicken auf den Vektor wird die Seite *CVSSv2/CVSSv3 Basis-Score-Rechner* geöffnet. Die Felder des entsprechenden Rechners sind bereits ausgefüllt, je nachdem, welche CVSS-Version zur Berechnung des Schweregrads der CVE verwendet wird (siehe Kapitel *14.2.3* (Seite 363)).

[48] https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases
[49] https://www.mitre.org/
[50] https://cve.mitre.org/
[51] https://nvd.nist.gov/
[52] https://nvd.nist.gov/vuln/full-listing

Bemerkung: Durch Klicken auf unterhalb der Liste von CVEs können mehrere CVEs zur gleichen Zeit exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche CVEs exportiert werden.

Detailseite

Durch Klicken auf den Namen einer CVE werden Details der CVE angezeigt. Durch Klicken auf wird die Detailseite der CVE geöffnet (siehe Abb. 14.1).

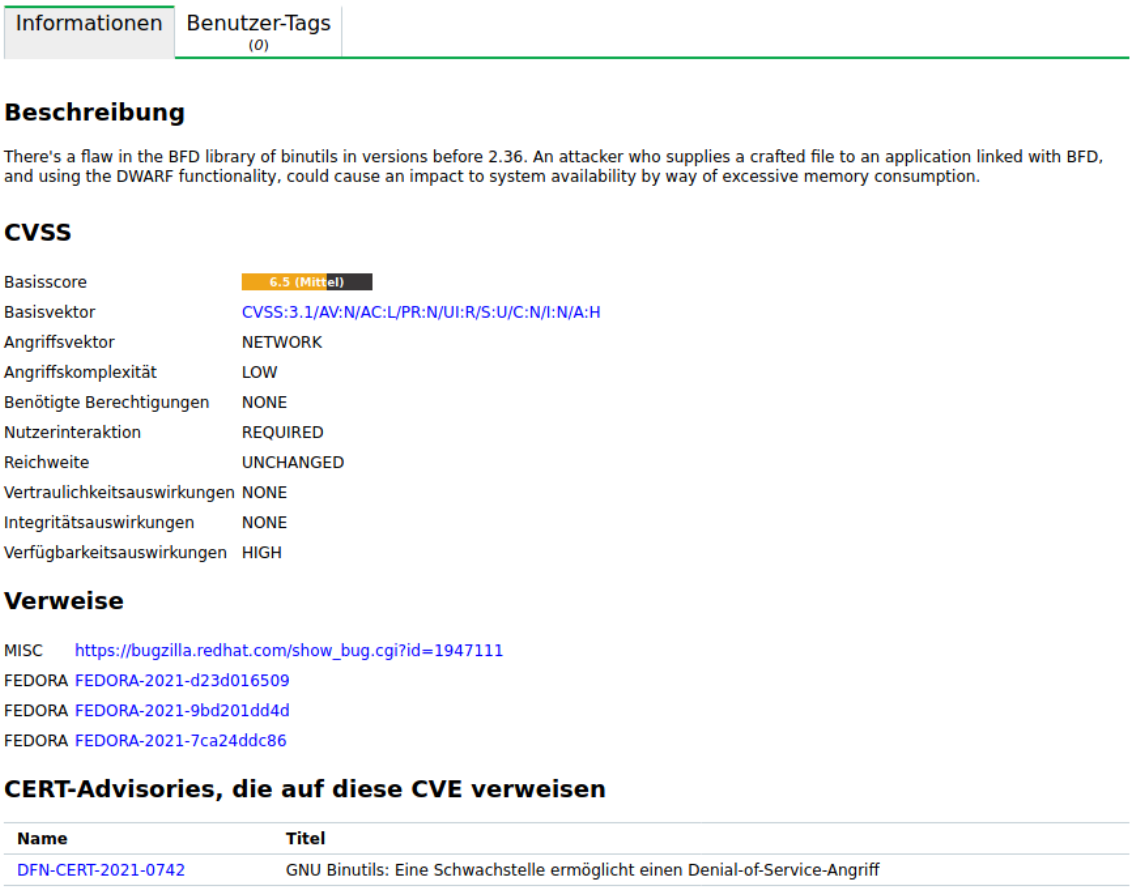


Abb. 14.1: Detailseite einer CVE

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die CVE.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen CVEs anzeigen.
- Die CVE als XML-Datei exportieren.

14.2.2 CPE

Die Common Platform Enumeration (CPE)[53] ist CVE nachempfunden. Es ist ein gegliedertes Benennungsschema für Anwendungen, Betriebssysteme und Hardwaregeräte.

Die CPE wurde von MITRE[54] eingeführt und wird von NIST als Teil der National Vulnerability Database (NVD)[55] gewartet. CPE basiert auf der allgemeinen Syntax des Uniform Resource Identifiers (URI).

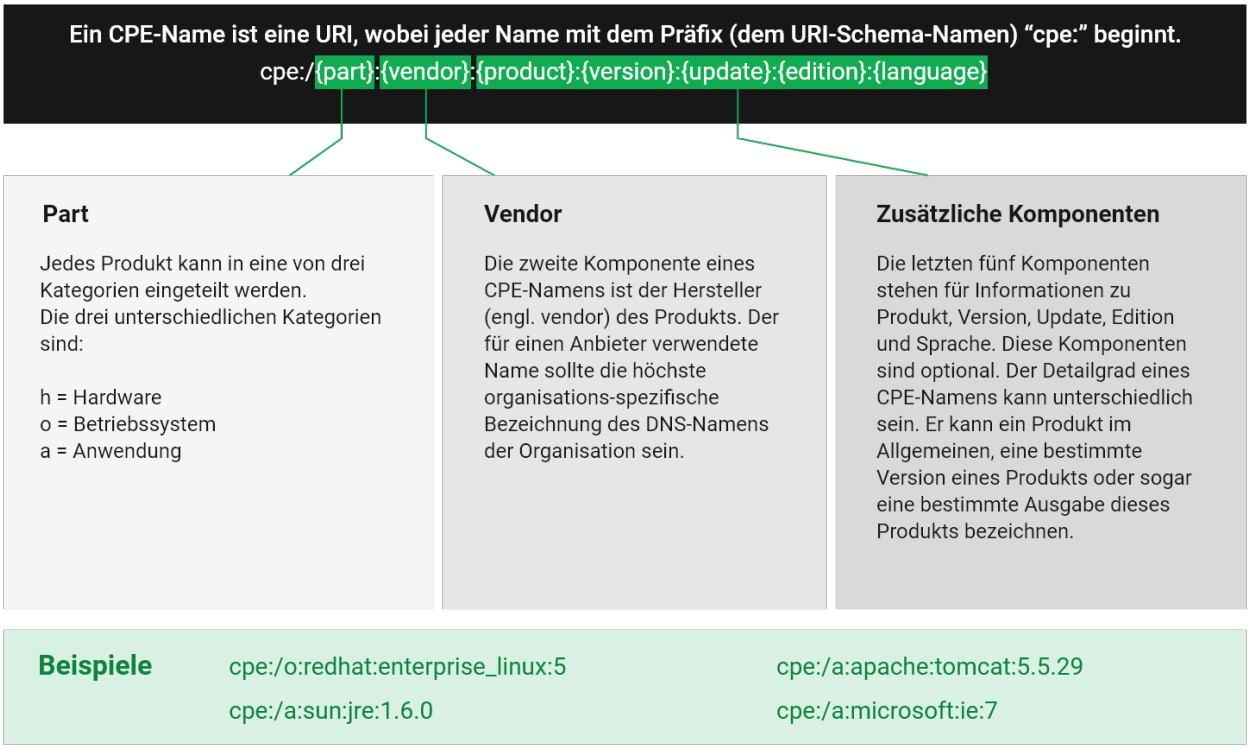


Abb. 14.2: Namensstruktur eines CPE-Namens

Die Kombination von CPE- und CVE-Standards ermöglicht den Rückschluss auf vorhandene Schwachstelle beim Entdecken einer Plattform oder eines Produkts.

CPE besteht aus den folgenden Komponenten:

- **Naming** Die Naming-Spezifikation beschreibt die logische Struktur von sogenannten well-formed names (WFNs), ihre Verbindung zu URIs und formatierten Zeichenketten sowie ihre Umwandlung.
- **Name Matching** Die Name-Matching-Spezifikation beschreibt die Methoden, um WFNs mit anderen zu vergleichen. Dies ermöglicht die Überprüfung, ob sich einige oder alle WFNs auf das gleiche Produkt beziehen.
- **Dictionary** Das Wörterbuch ist ein Verzeichnis von CPE-Namen und -Metadaten. Jeder Name definiert eine einzige Klasse von IT-Produkten. Die Dictionary-Spezifikation beschreibt die Prozesse zum Nutzen des Wörterbuchs, z. B. das Suchen nach einem bestimmten Namen oder nach Einträgen, die zu einer allgemeineren Klasse gehören.

[53] https://csrc.nist.gov/projects/security-content-automation-protocol/specifications/cpe
[54] https://www.mitre.org/
[55] https://nvd.nist.gov/

- **Applicability Language** Die Applicability-Language-Spezifikation beschreibt die Erstellung komplexer, logischer Ausdrücke mithilfe von WFNs. Diese Anwendbarkeitsangaben können zum Taggen von Checklisten, Richtlinien oder anderen Dokumenten und damit für die Beschreibung, für welche Produkte die Dokumente relevant sind, genutzt werden.

Listenseite

Alle vorhandenen CPEs können angezeigt werden, indem *Sicherheitsinfos > CPEs* in der Menüleiste gewählt wird.

Bemerkung: Die Verfügbarkeit einer CPE auf der Appliance hängt von ihrer Verfügbarkeit in der NVD ab. Sobald sie dort veröffentlicht wurde, dauert es 1–2 Arbeitstage, bis sie in den Sicherheitsinfos erscheint.

Bemerkung: Durch Klicken auf unterhalb der Liste von CPEs können mehrere CPEs zur gleichen Zeit exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche CPEs exportiert werden.

Detailseite

Durch Klicken auf den Namen einer CPE werden Details der CPE angezeigt. Durch Klicken auf wird die Detailseite der CPE geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über die CPE.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen CPEs anzeigen.
- Die CPE als XML-Datei exportieren.

14.2.3 CVSS

Um die Interpretation von Schwachstellen zu unterstützen, wurde das Common Vulnerability Scoring System (CVSS) entwickelt. Das CVSS ist ein Industriestandard zum Beschreiben des Schweregrads eines Sicherheitsrisikos in Computersystemen.

Sicherheitsrisiken werden mithilfe unterschiedlicher Kritierien bewertet und verglichen. Dies ermöglicht das Erstellen einer Prioritätenliste von Gegenmaßnahmen.

Das CVSS wurde von der CVSS Special Interest Group (CVSS-SIG)[56] des Forum of Incident Response and Security Teams[57] (FIRST) entwickelt. Die aktuelle CVSS-Scoreversion ist 4.0.

GOS 22.04 unterstützt CVSS v3.0/v3.1. Der Umfang der CVSS v3.0/v3.1-Unterstützung hängt vom Greenbone Enterprise Feed ab. VTs und CVEs können jedoch Daten von CVSS v2 und/oder CVSS v3.0/v3.1 enthalten.

- Wenn ein/e VT/CVE sowohl Daten von CVSS v2 als auch von CVSS v3.0/v3.1 enthält, werden immer die Daten von CVSS v3.0/v3.1 verwendet und angezeigt.
- Der *CVSS-Basisvektor*, der in der Detailvorschau und auf der Detailseite eines VTs angezeigt wird, kann v2, v3.0 oder v3.1 sein.

[56] https://www.first.org/cvss/
[57] https://www.first.org/

- Der *CVSS-Basisvektor*, der in der Tabelle auf der Seite *CVEs* gezeigt wird, kann v2, v3.0 oder v3.1 sein. Durch Klicken auf den CVSS-Basisvektor wird die Seite *CVSSv2/CVSSv3 Basis-Score-Rechner* geöffnet. Die Eingabefelder des entsprechenden Rechners sind bereits vorausgefüllt.

Der CVSS-Score unterstützt Base-Score-Metrics, Temporal-Score-Metrics und Environmental-Score-Metrics.

Base-Score-Metrics Base-Score-Metrics prüfen die Nutzbarkeit einer Schwachstelle und ihre Auswirkung auf das Zielsystem. Zugang, Komplexität und Anforderungen der Authentifizierung werden eingestuft. Zusätzlich bewerten die Maße, ob die Vertraulichkeit, Integrität oder Verfügbarkeit gefährdet ist.

Temporal-Score-Metrics Temporal-Score-Metrics prüfen, ob ein vollständiger Beispielcode existiert, der Anbieter einen Patch anbietet und die Schwachstelle bestätigt. Der Score ändert sich stark im Laufe der Zeit.

Environmental-Score-Metrics Environmental-Score-Metrics beschreiben den Effekt einer Schwachstelle innerhalb einer Organisation. Sie berücksichtigen Schaden, Verteilung der Ziele, Vertraulichkeit, Integrität und Verfügbarkeit. Die Beurteilung hängt stark von der Umgebung, in der das gefährdete Produkt genutzt wird, ab.

Da im Allgemeinen lediglich die Base-Score-Metrics aussagekräftig sind und dauerhaft bestimmt werden können, stellt die Appliance sie als Teil der Sicherheitsinfodaten bereit.

Der CVSS-Rechner kann geöffnet werden, indem *Hilfe > CVSS-Rechner* in der Menüleiste gewählt wird (siehe Abb. 14.3). Es wird sowohl der Rechner für CVSS-Version 2.0 als auch der Rechner für CVSS-Version 3.0/3.1 angezeigt.

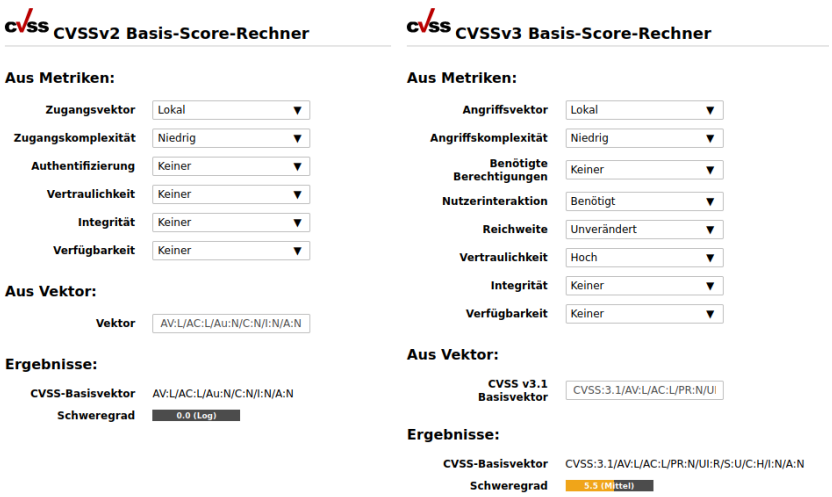


Abb. 14.3: CVSS-Rechner zum Berechnen von Schweregraden

14.2.3.1 CVSS-Version 2.0

Die folgende Formel wird vom CVSS-Rechner für Version 2.0 genutzt:

```
BaseScore = roundTo1Decimal( ( ( 0.6 * Impact ) +
            ( 0.4 * Exploitability ) - 1.5 ) * f( Impact ) )
```

„Impact“ wird wie folgt berechnet:

```
Impact = 10.41 * (1 - (1 - ConfImpact) *
         (1 - IntegImpact) * (1 - AvailImpact))
```

„Exploitability“ wird wie folgt berechnet:

```
Exploitability = 20 * AccessVector * AccessComplexity * Authentication
```

Bemerkung: Die Funktion `f( Impact )` ist 0, falls „Impact“ 0 ist.

In allen anderen Fällen ist der Wert 1,176.

Die anderen Werte sind Konstanten:

- **Zugangsvektor („AccessVector“)**
  - Lokal: 0,395
  - Angrenzend: 0,646
  - Netzwerk: 1,0
- **Zugangskomplexität („AccessComplexity“)**
  - Hoch: 0,35
  - Mittel: 0,61
  - Niedrig: 0,71
- **Authentifizierung („Authentication“)**
  - Mehrfach (benötigt mehrere Instanzen für die Authentifizierung): 0,45
  - Einzeln (benötigt eine einzelne Instanz für die Authentifizierung): 0,56
  - Keiner (benötigt keine Authentifizierung): 0,704
- **Vertraulichkeit („ConfImpact“)**
  - Keiner: 0,0
  - Partiell: 0,275
  - Vollständig: 0,660
- **Integrität („IntegImpact“)**
  - Keiner: 0,0
  - Partiell: 0,275
  - Vollständig: 0,660
- **Verfügbarkeit („AvailImpact“)**
  - Keiner: 0,0
  - Partiell: 0,275
  - Vollständig: 0,660

14.2.3.2 CVSS-Version 3.0/3.1

Die folgende Formel wird vom CVSS-Rechner für Version 3.0/3.1 genutzt:

```
* If Impact <= 0, BaseScore = 0

* If Scope is "Unchanged":
   BaseScore = Roundup (Minimum ((Impact + Exploitability), 10))

* If Scope is "Changed":
   BaseScore = Roundup (Minimum (1.08 * (Impact + Exploitability), 10))
```

„ISS“ (Impact Sub-Score) wird wie folgt berechnet:

```
ISS = 1 - ((1 - Confidentiality) * (1 - Integrity) * (1 - Availability))
```

„Impact“ wird wie folgt berechnet:

```
* If Scope is "Unchanged":
   Impact = 6.42 * ISS

* If Scope is "Changed":
   Impact = 7.52 * (ISS - 0.029) - 3.25 * (ISS - 0.02)^15
```

„Exploitability“ wird wie folgt berechnet:

```
Exploitability = 8.22 * Attack Vector * Attack Complexity
```

Die anderen Werte sind Konstanten:

- **Angriffsvektor („Attack Vector“)**
  - Netzwerk: 0,85
  - Angrenzend: 0,62
  - Lokal: 0,55
  - Physisch: 0,2
- **Angriffskomplexität („Attack Complexity“)**
  - Niedrig: 0,77
  - Hoch: 0,44
- **Benötigte Privilegien („Privileges Required“)**
  - Keine: 0,85
  - Niedrig: 0,62 (oder 0,68, falls Reichweite „Verändert“ ist)
  - Hoch: 0,27 (oder 0,5, falls Reichweite „Verändert“ ist)
- **Nutzerinteraktion („User Interaction“)**
  - Keine: 0,85
  - Benötigt: 0,62
- **Vertraulichkeit („Confidentiality“)**
  - Keiner: 0,0
  - Niedrig: 0,22
  - Hoch: 0,56

- **Integrität**
  - Keiner: 0,0
  - Niedrig: 0,22
  - Hoch: 0,56
- **Verfügbarkeit („Availability“)**
  - Keiner: 0,0
  - Niedrig: 0,22
  - Hoch: 0,56

14.3 CERT-Bund-Advisories

Der CERT-Bund[58], das Computer Emergency Response Team des Bundesamts für Sicherheit in der Informationstechnik (BSI), ist ein zentraler Kontaktpunkt für vorbeugende und reaktionsfähige Maßnahmen, die sicherheitsbezogene Computervorfälle betreffen.

Mit der Intention, Schäden zu vermeiden und potentielle Verluste einzugrenzen, umfasst die Arbeit des CERT-Bunds das Folgende:

- Erstellen und Veröffentlichen von Empfehlungen für vorbeugende Maßnahmen
- Aufzeigen von Schwachstellen in Hardware- und Softwareprodukten
- Vorschlagen von Maßnahmen, die bekannte Schwachstellen behandeln
- Unterstützen von Einrichtungen des öffentlichen Rechts beim Reagieren auf IT-Sicherheitsvorfälle
- Vorschlagen unterschiedlicher Schadensminderungsmaßnahmen
- Enge Zusammenarbeit mit dem Nationalen IT-Lagezentrum[59] und dem Nationalen IT-Krisenreaktionszentrum[60]

Die Dienste des CERT-Bunds sind hauptsächlich für Bundesbehörden verfügbar und beinhalten das Folgende:

- 24-Stunden-Rufbereitschaft in Zusammenarbeit mit dem IT Situation Centre
- Analyse eingehender Vorfallberichte
- Erstellen von Empfehlungen, die von Vorfällen abgeleitet wurden
- Unterstützung von Bundesbehörden während IT-Sicherheitsvorfällen
- Betreiben eines Warn- und Informationsdiensts
- Aktives Benachrichtigen der Bundesverwaltung im Falle drohender Gefahr

CERT-Bund bietet einen Warn- und Informationsdienst (WID) an. Derzeit bietet dieser Dienst zwei verschiedene Arten von Informationen:

Advisories Dieser Informationsdienst ist nur für Bundesbehörden als nichtöffentliche Liste verfügbar. Die Advisories beschreiben aktuelle Informationen über sicherheitskritische Vorfälle in Computersystemen und detaillierte Maßnahmen zum Beseitigen von Sicherheitsrisiken.

[58] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

[59] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/IT-Lagezentrum/it-lagezentrum_node.html

[60] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/IT-Krisenreaktionszentrum/it-krisenreaktionszentrum_node.html

Kurzinformationen Kurzinformationen sind die kurze Beschreibung aktueller Informationen bezüglich Sicherheitsrisiken und Schwachstellen. Diese Information ist nicht immer verifiziert und könnte unvollständig oder sogar ungenau sein.

Der Greenbone Enterprise Feed enthält die CERT-Bund-Kurzinformationen. Es sind sowohl die Informationen im alten Format[61] (bis Juni 2022) als auch die Informationen im neuen Format[62] (ab Juni 2022) enthalten.

- Zwischen beiden Formaten gibt es nur sehr geringe Unterschiede in den Advisory-Metadaten. Die Formate können für alle Anwendungsfälle austauschbar verwendet werden.
- Informationen des alten Formats folgen dem Schema `CB-KJJ/ID`, z. B. `CB-K22/0704`.
- Informationen des neuen Formats folgen dem Schema `WID-SEC-JJJJ-ID`, z.B. `WID-SEC-2022-0311`.

Listenseite

Alle vorhandenen CERT-Bund-Advisories können angezeigt werden, indem *Sicherheitsinfos > CERT-Bund-Advisories* in der Menüleiste gewählt wird.

Bemerkung: Durch Klicken auf unterhalb der Liste von CERT-Bund-Advisories können mehrere CERT-Bund-Advisories zur gleichen Zeit exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche CERT-Bund-Advisories exportiert werden.

Detailseite

Durch Klicken auf den Namen eines CERT-Bund-Advisorys werden Details des CERT-Bund-Advisorys angezeigt. Durch Klicken auf wird die Detailseite des CERT-Bund-Advisorys geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das CERT-Bund-Advisory.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- Die Listenseite mit allen CERT-Bund-Advisories anzeigen.
- Das CERT-Bund-Advisory als XML-Datei exportieren.

[61] https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Warnmeldungen/warnmeldungen_node.html
[62] https://wid.cert-bund.de/portal/wid/kurzinformationen

14.4 DFN-CERT-Advisories

Während die einzelnen VTs, CVEs und CPEs vorrangig erstellt wurden, um von Computersystemen verarbeitet zu werden, veröffentlicht das DFN-CERT[63] regelmäßig neue Advisories.

Das DFN-CERT ist für hunderte Universitäten und Forschungsinstitute, die mit dem Deutschen Forschungsnetz (DFN)[64] verbunden sind, verantwortlich. Zusätzlich stellt es entscheidende Sicherheitsdienste für die Regierung und die Industrie bereit.

Ein Advisory beschreibt besonders kritische Risiken, die eine schnelle Reaktion erfordern. Der DFN-CERT-Advisory-Dienst enthält die Kategorisierung, Verteilung und Bewertung von Advisorythemen durch verschiedene Softwarehersteller und -händler. Die Greenbone Enterprise Appliance erhält die Advisories und speichert sie als Referenz in der Datenbank.

Listenseite

Alle vorhandenen DFN-CERT-Advisories können angezeigt werden, indem *Sicherheitsinfos > DFN-CERT-Advisories* in der Menüleiste gewählt wird.

Bemerkung: Durch Klicken auf ⎘ unterhalb der Liste von DFN-CERT-Advisories können mehrere DFN-CERT-Advisories zur gleichen Zeit exportiert werden. Die Drop-down-Liste wird genutzt, um auszuwählen, welche DFN-CERT-Advisories exportiert werden.

Detailseite

Durch Klicken auf den Namen eines DFN-CERT-Advisories werden Details des DFN-CERT-Advisories angezeigt. Durch Klicken auf 🔍 wird die Detailseite des DFN-CERT-Advisories geöffnet.

Die folgenden Register sind verfügbar:

Informationen Allgemeine Informationen über das DFN-CERT-Advisory.

Benutzer-Tags Zugewiesene Tags (siehe Kapitel *8.4* (Seite 176)).

Die folgenden Aktionen sind in der linken oberen Ecke verfügbar:

- ⓘ Das entsprechende Kapitel im Anwenderhandbuch öffnen.
- ☰ Die Listenseite mit allen DFN-CERT-Advisories anzeigen.
- ⎘ Das DFN-CERT-Advisory als XML-Datei exportieren.

[63] https://www.dfn-cert.de/
[64] https://www.dfn.de/

KAPITEL 15

Das Greenbone Management Protocol nutzen

Die Schwachstellenverwaltung der Greenbone Enterprise Appliance ist auch über das Greenbone Management Protocol (GMP) verfügbar.

Greenbone stellt Greenbone Vulnerability Management Tools (gvm-tools) bereit, um diese Funktion mit GMP verfügbar zu machen (siehe Kapitel *15.3* (Seite 371)). Dieses Anwenderhandbuch deckt gvm-tools bis zu Version 2.0.0 beta ab.

Die neueste GMP-Version ist unter https://docs.greenbone.net/API/GMP/gmp-22.4.html dokumentiert.

15.1 Änderungen am GMP

GMP wird regelmäßig aktualisiert, um Änderungen in der Funktionalität, die durch den zugrunde liegenden Dienst bereitgestellt werden, anzuwenden und eine einheitliche und umfassende Oberfläche zur Verfügung zu stellen.

Updates führen zu einer neuen Version von GMP. Jede neue Version enthält eine Liste hinzugefügter, veränderter oder entfernter Protokollelementen (Befehle oder Attribute). Die neueste Version der Liste ist unter https://docs.greenbone.net/API/GMP/gmp-22.4.html#changes verfügbar.

Abhängig von den Änderungen ist die veraltete Version noch für einige Zeit verfügbar. Während dieser Übergangsphase sind sowohl die veraltete als auch die neue Version erhältlich.

Die Liste kann bei der frühstmöglichen Vorbereitung auf kommende Veränderungen helfen. Sie stellt nicht die komplette Liste an bevorstehenden Veränderungen dar.

15.2 GMP aktivieren

Bevor GMP genutzt werden kann, muss es auf der Appliance aktiviert werden.

Während die Web-Oberfläche GMP lokal auf der Appliance nutzt, kann standardmäßig nicht remote über das Netzwerk auf GMP zugegriffen werden.

Der Remote-GMP-Dienst kann mithilfe des GOS-Administrationsmenüs aktiviert werden (siehe Kapitel *7.2.4.2* (Seite 106)).

Allgemein wird der Zugriff auf GMP mit SSL/TLS authentifiziert und verschlüsselt. Dieselben Benutzer wie für die Web-Oberfläche werden genutzt. Die Benutzer unterliegen denselben Beschränkungen und haben dieselben Berechtigungen.

15.3 Die gvm-tools nutzen

Die Greenbone Vulnerability Management Tools (gvm-tools) sind eine Sammlung von Werkzeugen, die Zugang zu den Funktionen des Greenbone Management Protocols (GMP) bereitstellen. GMP-Skripte, die mit `gvm-script` ausgeführt werden, benutzen die API, die von der Bibliothek python-gvm[65] zur Verfügung gestellt wird.

Bemerkung: python-gvm wird bei der Installation von gvm-tools automatisch installiert.

Die gvm-tools sind als Befehlszeilenschnittstelle (CLI) und als Python-Shell für Microsoft Windows und jedes andere Betriebssystem, das Python unterstützt (einschließlich Linux), verfügbar.

Bemerkung: Sowohl gvm-tools als auch python-gvm verwenden ein anderes Versionsschema als GOS, sodass die Versionen von gvm-tools, python-gvm und GOS nicht unbedingt identisch sind.

Es wird empfohlen, die neuesten Versionen von gvm-tools und python-gvm zu verwenden.

Die gvm-tools können vom GitHub-Repository des Projekts[66] heruntergeladen werden. Python 3.5 oder höher wird benötigt. Um gvm-tools zu installieren, müssen die Anweisungen unter https://gvm-tools.readthedocs.io/en/latest/install.html befolgt werden.

Zusätzlich sind die gvm-tools als statisch verknüpfte EXE-Dateien für alle unterstützten Versionen von Microsoft Windows[67] verfügbar.

Die EXE-Versionen der gvm-tools benötigen Python nicht und können direkt von Greenbone heruntergeladen werden:

- CLI: gvm-cli.exe[68]
- Python-Shell: gvm-pyshell.exe[69]

Wichtig: Externe Links zur Greenbone-Downloadseite unterscheiden Groß- und Kleinbuchstaben.

Großbuchstaben, Kleinbuchstaben und Sonderzeichen müssen exakt so, wie sie in den Fußnoten stehen, eingegeben werden.

Bemerkung: Die gvm-tools sind unter der GNU General Public License v3.0 lizensiert und können möglicherweise für andere Anwendungsfälle, basierend auf dem Quellcode, angepasst und gebaut werden.

---

[65] https://python-gvm.readthedocs.io/en/latest/
[66] https://github.com/greenbone/gvm-tools
[67] https://learn.microsoft.com/en-us/lifecycle/faq/windows
[68] https://download.greenbone.net/tools/gvm-cli.exe
[69] https://download.greenbone.net/tools/gvm-pyshell.exe

15.3.1 Mit `gvm-cli.exe` zugreifen

GMP ist XML-basiert. Jeder Befehl und jede Antwort ist ein GMP-Objekt.

Das Kommandozeilenprogramm `gvm-cli.exe`, das von Greenbone angeboten wird, bietet direktes Senden und Empfangen von XML-Befehlen und -Antworten.

`gvm-cli.exe` unterstützt die folgenden Verbindungen:

- SSH
- TLS
- Unix Domain Socket

`gvm-cli.exe` unterstützt zahlreiche Befehlszeilenoptionen, die wie folgt angezeigt werden können:

```
$ gvm-cli -h
usage: gvm-cli [-h] [-c [CONFIG]]
               [--log [{DEBUG,INFO,WARNING,ERROR,CRITICAL}]]
               [--timeout TIMEOUT] [--gmp-username GMP_USERNAME]
               [--gmp-password GMP_PASSWORD] [-V] [--protocol {GMP,OSP}]
               CONNECTION_TYPE ...

optional arguments:
  -h, --help            show this help message and exit
  -c [CONFIG], --config [CONFIG]
                        Configuration file path (default: ~/.config/gvm-
                        tools.conf)
  --log [{DEBUG,INFO,WARNING,ERROR,CRITICAL}]
                        Activate logging (default level: None)
  --timeout TIMEOUT     Response timeout in seconds, or -1 to wait
                        indefinitely (default: 60)
  --gmp-username GMP_USERNAME
                        Username for GMP service (default: '')
  --gmp-password GMP_PASSWORD
                        Password for GMP service (default: '')
  -V, --version         Show version information and exit
  --protocol {GMP,OSP}  Service protocol to use (default: GMP)

connections:
  valid connection types

  CONNECTION_TYPE       Connection type to use
    ssh                 Use SSH to connect to service
    tls                 Use TLS secured connection to connect to service
    socket              Use UNIX Domain socket to connect to service
```

Obwohl `gvm-cli.exe` noch mehr Befehlszeilenoptionen unterstützt, werden die zusätzlichen Optionen nur angezeigt, wenn der Verbindungstyp angegeben wird:

```
$ gvm-cli ssh -h
usage: gvm-cli ssh [-h] --hostname HOSTNAME [--port PORT]
                   [--ssh-username SSH_USERNAME]
                   [--ssh-password SSH_PASSWORD] [-X XML] [-r] [--pretty]
                   [--duration]
                   [infile]

positional arguments:
  infile                File to read XML commands from.

optional arguments:
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
  -h, --help            show this help message and exit
  --hostname HOSTNAME   Hostname or IP address
  --port PORT           SSH port (default: 22)
  --ssh-username SSH_USERNAME
                        SSH username (default: 'gmp')
  --ssh-password SSH_PASSWORD
                        SSH password (default: 'gmp')
  -X XML, --xml XML     XML request to send
  -r, --raw             Return raw XML
  --pretty              Pretty format the returned xml
  --duration            Measure command execution time
```

Alle aktuellen Appliances nutzen SSH zum Verschlüsseln von GMP. Die Nutzung von TLS ist veraltet, wird nicht offiziell unterstützt und könnte in zukünftigen Versionen entfernt werden.

Die gvm-tools sind hauptsächlich für den Batch-Modus (`batch processing`, `scripting`) hilfreich.

Mit `gvm-cli.exe` kann GMP einfach genutzt werden:

```
gvm-cli --xml "<get_version/>"
gvm-cli --xml "<get_tasks/>"
gvm-cli < file
```

15.3.1.1 Den Client konfigurieren

Für die Nutzung des Befehls `gvm-cli` ist das Einloggen in die Appliance nötig.

Die benötigten Informationen werden entweder mithilfe von Befehlszeilenoptionen oder einer Konfigurationsdatei (~/.config/gvm-tools.conf) geliefert.

Um dem GMP-Benutzer Befehlszeilenoptionen zur Verfügung zu stellen, können die folgenden Befehle genutzt werden:

- `--gmp-username`
- `--gmp-password`

Alternativ kann eine Konfigurationsdatei ~/.config/gvm-tools.conf, die die Informationen enthält, erstellt werden:

```
[Auth]
gmp_username=webadmin
gmp_password=kennwort
```

Diese Konfigurationsdatei wird nicht standardmäßig gelesen. Die Befehlszeilenoption `--config` oder `-c` muss hinzugefügt werden, um die Konfigurationsdatei zu lesen.

15.3.1.2 Einen Scan mithilfe des Befehls `gvm-cli` starten

Ein typisches Beispiel für die Nutzung von GMP ist der automatische Scan eines neuen Systems.

In diesem Beispiel wird angenommen, dass ein Intrusion Detection System (IDS) genutzt wird, das die Systeme in der Demilitarisierten Zone (DMZ) überwacht und unmittelbar neue Systeme und unübliche TCP-Ports, die noch nicht genutzt wurden, entdeckt. Falls solch ein Fall beobachtet wird, sollte das IDS mithilfe eines Skripts automatisch einen Scan des neuen Systems einleiten.

Dafür kann der Befehl `gvm-cli` genutzt werden, obwohl der Befehl `gvm-pyshell` oder die Nutzung selbst geschriebener Python-Skripte geeigneter sein könnte (siehe Kapitel *15.3.2.1* (Seite 376)). Die Verarbeitung der XML-Ausgabe wird durch Python besser unterstützt, als durch die Nutzung der Shell.

Startpunkt ist die IP-Adresse des neuen, verdächtigen Systems. Auf der Appliance muss ein Ziel für diese IP-Adresse erstellt werden.

Der Befehl `create_target` ist hier beschrieben:

https://docs.greenbone.net/API/GMP/gmp-22.4.html#command_create_target.

1. Falls die IP-Adresse in der Variable `IPADDRESS` gespeichert ist, entsprechendes Ziel wie folgt erstellen:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml "<create_target><name>Suspect Host</name>\
<hosts>$IPADDRESS</hosts></create_target>"

<create_target_response status="201" status_text="OK, resource
created" id="4574473f-a5d0-494c-be6f-3205be487793"/>
```

2. Aufgabe wie folgt erstellen:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml "<create_task><name>Scan Suspect Host</name> \
<target id=\"4574473f-a5d0-494c-be6f-3205be487793\"></target> \
<config id=\"daba56c8-73ec-11df-a475-002264764cea\"></config></create_task>"


<create_task_response status="201" status_text="OK, resource
created" id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>
```

→ Die Ausgabe ist die ID der Aufgabe. Diese wird für das Starten und Überwachen der Aufgabe benötigt.

Die anderen vom Befehl genutzten IDs können durch Nutzung der folgenden Befehle, die die verfügbaren Ziele und Scan-Konfigurationen anzeigen, erhalten werden:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml "<get_targets/>"

$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml "<get_configs/>"
```

Bemerkung: Die Ausgabe der Befehle ist XML.

3. Aufgabe wie folgt starten:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<start_task task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>'
```

→ Die Verbindung wird von der Appliance getrennt. Die Aufgabe läuft.

4. Status der Aufgabe wie folgt anzeigen:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<get_tasks task_id="ce225181-c836-4ec1-b83f-a6fcba70e17d"/>'

<get_tasks_response status="200" status_text="OK"><apply_overrides>
...<status>Running</status><progress>98<host_progress>
<host>192.168.255.254</host>98</host_progress></progress>.../>
```

→ Sobald der Scan abgeschlossen ist, kann der Bericht heruntergeladen werden.

Dafür wird die ID benötigt, die beim Erstellen der Aufgabe ausgegeben wurde. Außerdem muss ein sinnvolles Berichtformat eingegeben werden.

5. IDs für die Berichtformate wie folgt anzeigen:

```
$ $ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 --xml '<get_report_formats/>'
```

6. Bericht wie folgt laden:

```
$ gvm-cli --gmp-username webadmin --gmp-password kennwort ssh \
--hostname 192.168.222.115 \
--xml '<get_reports report_id="23a335d6-65bd-4be2-a83e-be330289eef7" \
format_id="35ba7077-dc85-42ef-87c9-b0eda7e903b6"/>'
```

Tipp: Um die Daten vollständig und automatisch zu verarbeiten, kann die Aufgabe mit einer Benachrichtigung kombiniert werden, die den Bericht, basierend auf den gegebenen Bedingungen, weiterleitet.

15.3.2 Mit `gvm-pyshell.exe` zugreifen

Das Kommandozeilenprogramm `gvm-pyshell.exe`, das von Greenbone angeboten wird, bietet direktes Senden und Empfangen von XML-Befehlen und -Antworten mithilfe von Python-Befehlen. Die Befehle sorgen für das Erzeugen und Parsen der XML-Daten.

Das Werkzeug unterstützt die folgenden Transportkanäle:

- TLS
- SSH
- Socket

Während die aktuellen Appliances SSH nutzen, um GMP zu schützen, haben ältere Appliances TLS und Port 9390 für den Transport von GMP genutzt. Die gvm-tools können sowohl mit dem älteren als auch mit dem aktuellen GOS genutzt werden.

Die gvm-tools sind hauptsächlich für den Batch-Modus (`batch processing`, `scripting`) hilfreich.

Die Konfiguration der Authentifizierung des Befehls `gvm-pyshell` kann in einer Datei im Home-Verzeichnis des Benutzers gespeichert werden. Die Syntax ist in Kapitel *15.3.1.1* (Seite 373) erklärt.

Die Python-Implementierung folgt der GMP-API (https://docs.greenbone.net/API/GMP/gmp-22.4.html). Optionale Argumente in der API sind durch ein `?` gekennzeichnet. Das folgende Beispiel erklärt die Nutzung der Python-Funktion:

```
gmp.create_task("Name","Config","Scanner","Target",comment="comment")
```

Tipp: Während zwingend notwendige Parameter in der korrekten Reihenfolge eingegeben werden können und automatisch identifiziert werden, können sie auch mithilfe ihres Bezeichners angegeben werden:

```
gmp.create_task(name="Name",config_id="Config",scanner_id="Scanner",
target_id="Target",comment="comment")
```

15.3.2.1 Einen Scan mithilfe des Befehls `gvm-pyshell` starten

Ein typisches Beispiel für die Nutzung von GMP ist der automatische Scan eines neuen Systems.

In diesem Beispiel wird angenommen, dass ein Intrusion Detection System (IDS) genutzt wird, das die Systeme in der Demilitarisierten Zone (DMZ) überwacht und unmittelbar neue Systeme und unübliche TCP-Ports, die noch nicht genutzt wurden, entdeckt. Falls solch ein Fall beobachtet wird, sollte das IDS mithilfe eines Skripts automatisch einen Scan des neuen Systems einleiten.

Der Befehl `gvm-pyshell` ist dafür sehr geeignet. Die Verarbeitung der XML-Ausgabe wird durch Python besser unterstützt als durch Nutzung der Shell.

Startpunkt ist die IP-Adresse des neuen, verdächtigen Systems. Auf der Appliance muss ein Ziel für diese IP-Adresse erstellt werden.

Der Befehl `create_target` ist hier beschrieben:

https://docs.greenbone.net/API/GMP/gmp-22.4.html#command_create_target.

1. Die folgenden Zeilen zeigen die Befehle, die benötigt werden, wenn `gvm-pyshell` genutzt wird:

```
$ gvm-pyshell \
--gmp-username webadmin --gmp-password kennwort \
ssh --hostname 192.168.222.115
GVM Interactive Console 2.0.0 API 1.1.0. Type "help" to get information about
  functionality.
>>> res=gmp.create_target("Suspect Host", make_unique=True, \
  hosts=['192.168.255.254'])
>>> target_id = res.xpath('@id')[0]
```

Die Variable `target_id` enthält die ID des erstellten Ziels. Diese ID kann genutzt werden, um die zugehörige Aufgabe zu erstellen.

Bemerkung: Die Erzeugung der Aufgabe erfordert den folgenden Angaben:

- target_id
- config_id
- scanner_id
- task_name
- task_comment

---

2. Alle verfügbaren Scan-Konfigurationen können wie folgt angezeigt werden:

```
>>> res = gmp.get_configs()
>>> for i, conf in enumerate(res.xpath('config')):
...     id = conf.xpath('@id')[0]
...     name = conf.xpath('name/text()')[0]
...     print('\n({0}) {1}: ({2})'.format(i, name, id))
```

3. Alle verfügbaren Scanner können mithilfe der gleichen Methode angezeigt werden. Falls nur die integrierten Scanner genutzt werden, sind die folgenden IDs fest codiert:
   - OpenVAS-Scanner: 08b69003-5fc2-4037-a479-93b440211c73
   - CVE-Scanner: 6acd0832-df90-11e4-b9d5-28d24461215b

4. Aufgabe wie folgt erstellen:

```
>>> res=gmp.create_task(name="Scan Suspect Host",
... config_id="daba56c8-73ec-11df-a475-002264764cea",
... scanner_id="08b69003-5fc2-4037-a479-93b440211c73",
... target_id=target_id)
>>> task_id = res.xpath('@id')[0]
```

5. Aufgabe wie folgt starten:

```
>>> gmp.start_task(task_id)
```

→ Die aktuelle Verbindung wird unmittelbar geschlossen. Zusätzliche Befehle sind nicht erforderlich.

Alle Befehle können in ein Python-Skript eingefügt werden, das von der Python-Shell aufgerufen werden kann:

```
len_args = len(args.script) - 1
if len_args is not 2:
    message = """
    This script creates a new task with specific host and vt!
    It needs two parameters after the script name.
    First one is name of the target and the second one is the
    chosen host. The task is called target-task

    Example:
        $ gvm-pyshell ssh newtask target host
    """
    print(message)
    quit()

target = args.script[1]
host = args.script[2]
task = target + " Task"

# Full and Fast
myconfig_id = "daba56c8-73ec-11df-a475-002264764cea"

# OpenVAS Scanner
myscanner_id = "08b69003-5fc2-4037-a479-93b440211c73"

res=gmp.create_target(target, True, hosts=host)
mytarget_id = res.xpath('@id')[0]

res=gmp.create_task(name=task,
                    config_id=myconfig_id,
                        scanner_id=myscanner_id,
                            target_id=mytarget_id)
mytask_id = res.xpath('@id')[0]

gmp.start_task(mytask_id)
```

15.3.3 Beispielskripte

Die gvm-tools bringen eine Sammlung von Beispielskripten mit sich, welche vom Befehl `gvm-script` genutzt werden können.

Aktuell sind die folgenden Skripte für die gvm-tools Version 2.0.0 verfügbar (https://github.com/greenbone/gvm-tools/tree/main/scripts):

- application-detection.gmp.py: Dieses Skript zeigt alle Hosts mit der gesuchten Anwendung.
- cfg-gen-for-certs.gmp.py: Dieses Skript erstellt eine neue Scan-Konfiguration mit VTs basierend auf einem gegebenen CERT-Bund-Advisory.
- clean-sensor.gmp.py: Dieses Skript entfernt alle Ressourcen, abgesehen von aktiven Aufgaben, von einem Sensor.
- create-dummy-data.gmp.py: Dieses Skript erstellt Dummy-Daten.
- DeleteOverridesByFilter.gmp.py: Dieses Skript entfernt Übersteuerungen von einem Filter.
- monthly-report2.gmp.py: Dieses Skript zeigt alle Schwachstellen, die auf dem Bericht eines vorgegebenen Monats basieren. Geeignet für GOS 4.x.
- monthly-report.gmp.py: Dieses Skript zeigt alle Schwachstellen, die auf dem Bericht eines vorgegebenen Monats basieren. Geeignet für GOS 3.1.
- nvt-scan.gmp.py: Dieses Skript erstellt eine neue Aufgabe mit einem bestimmten Host und einem bestimmten VT, die eine fest codierte Basis-Konfiguration nutzt.
- startNVTScan.gmp.py: Dieses Skript erstellt interaktiv eine neue Aufgabe mit einem bestimmten Host und einem bestimmten VT.
- SyncAssets.gmp.py: Dieses Skript lädt Assets in die Asset-Datenbank hoch.
- SyncReports.gmp.py: Dieses Skript lädt Berichte von einer Appliance herunter und lädt sie mithilfe von Container-Aufgaben in eine zweite Appliance hoch.

Tipp: Diese Skripte können als Startpunkt für die Entwicklung benutzerdefinierter Skripte dienen.

15.4 Statuscodes

GMP nutzt Statuscodes, die HTTP-Statuscodes ähnlich sind. Die folgenden Codes werden genutzt:

2xx: Das Kommando wurde erfolgreich übertragen, verstanden und akzeptiert.

200: OK

201: Resource created

202: Request submitted

4xx: Es liegt ein Benutzerfehler vor.

400: Syntax-Fehler Dies beinhaltet verschiedene Syntaxfehler. Oft fehlen Elemente oder Attribute im GMP-Befehl. Der Statustext zeigt zusätzliche Informationen.

Aktuell wird dieser Statuscode auch für fehlende oder falsche Authentifizierungen genutzt.

401: Authenticate First Dieser Fehlercode wird für eine fehlende oder falsche Authentifizierung genutzt. Aktuell wird noch der Wert 400 genutzt.

403: Access to resource forbidden Dieser Fehlercode wird genutzt, wenn nicht genug Berechtigungen vorhanden sind. Oft wird stattdessen *400: Permission denied* angezeigt.

404: Resource missing Die Ressource konnte nicht gefunden werden. Die Ressourcen-ID ist leer oder falsch.

409: Resource busy Dieser Fehlercode tritt beispielsweise dann auf, wenn die Synchronisierung des Feeds gestartet wird, während sie bereits läuft.

5xx: Es liegt ein Serverfehler vor.

500: Internal Error Dies kann durch Einträge, die die interne Puffergröße übersteigen, ausgelöst werden.

503: Scanner loading NVTs Der Scanner lädt gerade VTs aus seinem Speicher. Die Anfrage sollte zu einem späteren Zeitpunkt noch einmal gestellt werden.

503: Service temporarily down Möglicherweise läuft der Scanner-Daemon nicht. Oft wird dieses Problem durch abgelaufene Zertifikate hervorgerufen.

503: Service unavailable Der GMP-Befehl ist auf der Appliance gesperrt.

KAPITEL 16

Ein Master-Sensor-Setup nutzen

Bemerkung: Dieses Kapitel dokumentiert alle möglichen Menüoptionen.

Allerdings unterstützen nicht alle Appliance-Modelle alle Menüoptionen. Um festzustellen, ob ein bestimmtes Feature für das genutzte Appliance-Modell verfügbar ist, können die Tabellen in Kapitel *3* (Seite 20) genutzt werden.

Aus Sicherheitsgründen ist es oft nicht möglich, bestimmte Netzwerksegmente direkt zu scannen. Zum Beispiel kann der direkte Zugang zum Internet untersagt sein. Um dieses Problem zu beheben, unterstützt die Greenbone Enterprise Appliance die Einrichtung eines verteilten Scansystems: Zwei oder mehr Appliances in unterschiedlichen Netzwerksegmenten können sicher verbunden werden, um Schwachstellentests in den Netzwerksegmente durchzuführen, die andernfalls nicht erreichbar sind.

In diesem Fall steuert eine Appliance eine oder mehr andere Appliances fern. Eine steuernde Appliance wird als „Master“ und eine kontrollierte Appliance wird als „Sensor“ bezeichnet.

Master

- Alle Appliance-Modelle ab Greenbone Enterprise 400/DECA können als Master genutzt werden (siehe Kapitel *3* (Seite 20)).

Sensor

- Alle Appliance-Modelle, abgesehen von der Greenbone Enterprise ONE, können als Sensor genutzt werden.
- Die Appliance-Modelle Greenbone Enterprise 35 und 25V können ausschließlich als Sensor genutzt werden und werden immer von einem Master gesteuert.
- Alle Sensoren können direkt vom Master verwaltet werden. Dies schließt automatische oder manuelle Feed-Updates und Upgrades vom Greenbone Operating System (GOS) ein.
- Ein Sensor benötigt keine andere Netzwerkverbindung außer zum Master und zu den Scanzielen.
- Ein Sensor benötigt nach dem anfänglichen Setup keine weiteren administrativen Schritte.
- Falls ein Sensor Scans ferngesteuert durchführen soll, muss er als Remote-Scanner konfiguriert werden.
  - Der Benutzer kann Scans für den Remote-Scanner individuell mithilfe der Web-Oberfläche des Masters, abhängig von Anforderungen und Berechtigungen, erstellen.

  - Der Remote-Scanner führt die Scans durch und leitet die Ergebnisse an den Master weiter, wo alle Schwachstelleninformationen verwaltet werden.
  - Die Verbindung zu einem Remote-Scanner wird mithilfe vom Open Scanner Protocol (OSP) über SSH aufgebaut.

Die Verbindung zwischen Master und Sensor wird mithilfe des Secure-Shell-Protokolls (SSH) über Port 22/TCP aufgebaut.

Zum Unterscheiden zwischen den Begriffen „Sensor“ und „Remote-Scanner“:

- **Sensoren** Diese Funktion erfordert das Einrichten einer Master-Sensor-Verknüpfung über die GOS-Administrationsmenüs von Master und Sensor. Die Funktion unterstützt dann die ferngesteuerte Feedsynchronisation und die Upgradeverwaltung des Sensors.
- **Remote-Scanner** Diese Funktion erfordert das Einrichten des Remote-Scanners mithilfe der Web-Oberfläche des Masters. Die Funktion unterstützt dann die Ausführung von Scans über den Sensor.

16.1 Ein Master-Sensor-Setup konfigurieren

Ein Master kann wie folgt mit einem Sensor verknüpft werden:

1. GOS-Administrationsmenü des Masters und des Sensors öffnen (siehe Kapitel *7.1.2.2* (Seite 66)).
2. Im GOS-Administrationsmenü des Masters *Setup* wählen und `Enter` drücken.
3. *Master* wählen und `Enter` drücken.
4. *Master Identifier* wählen und `Enter` drücken.
5. *Download* wählen und `Enter` drücken (siehe Abb. 16.1).

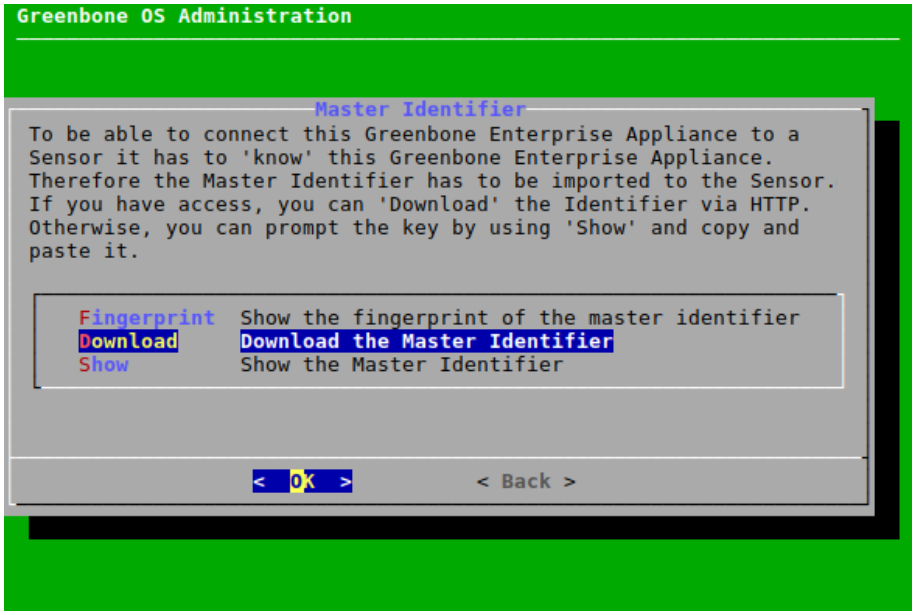


Abb. 16.1: Konfiguration des Masters

6. Webbrowser öffnen und angezeigte URL eingeben.
7. PUB-Datei herunterladen.

   → Wenn der Schlüssel heruntergeladen wurde, zeigt das GOS-Administrationsmenü des Masters den Fingerprint des Schlüssels zur Verifizierung an.

Wichtig: Der Fingerprint darf nicht bestätigt werden, bevor der Schlüssel in den Sensor hochgeladen wurde.

8. Im GOS-Administrationsmenü des Sensors *Setup* wählen und `Enter` drücken.
9. *Sensor* wählen und `Enter` drücken.
10. *Configure Master* wählen und `Enter` drücken (siehe Abb. 16.2).

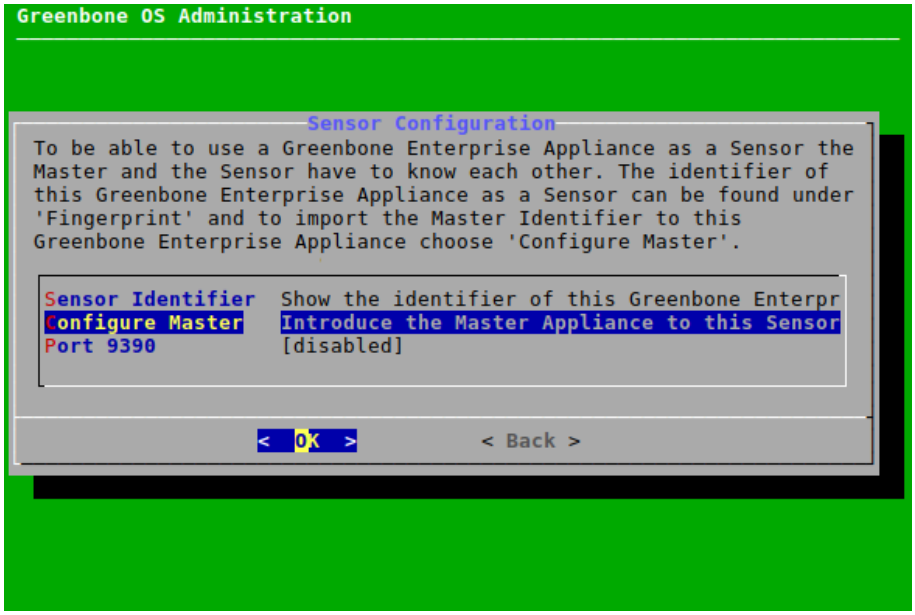


Abb. 16.2: Konfiguration des Sensors

11. *Upload* wählen und `Enter` drücken.
12. Webbrowser öffnen und angezeigte URL eingeben.
13. Auf *Browse...* klicken, die zuvor heruntergeladene PUB-Datei wählen und auf *Upload* klicken.

    → Wenn der Schlüssel hochgeladen wurde, zeigt das GOS-Administrationsmenü des Sensors den Fingerprint des Schlüssels zur Verifizierung an.
14. Fingerprint mit dem Fingerprint, der im GOS-Administrationsmenü des Masters angezeigt wird, vergleichen.

    Falls die Fingerprints übereinstimmen, *Enter* in beiden GOS-Administrationsmenüs drücken.
15. Im GOS-Administrationsmenü des Sensors *Save* wählen und `Enter` drücken.
16. Zweimal durchführen: `Tab` drücken und anschließend `Enter` drücken.
17. *Services* wählen und `Enter` drücken.
18. *SSH* wählen und `Enter` drücken.
19. *SSH State* wählen und `Enter` drücken.

    → SSH ist auf dem Sensor aktiviert.
20. *Save* wählen und `Enter` drücken.
21. `Tab` drücken, um *Back* zu wählen und `Enter` drücken.
22. *OSP* wählen und `Enter` drücken.

23. `Enter` drücken, um OSP zu aktivieren.

    → Eine Nachricht informiert den Benutzer darüber, dass die Änderungen gespeichert werden müssen (siehe Kapitel *7.1.3* (Seite 68)).

24. `Enter` drücken, um die Nachricht zu schließen.

25. *Save* wählen und `Enter` drücken.

    → OSP ist auf dem Sensor aktiviert.

26. Im GOS-Administrationsmenü des Masters *Setup* wählen und `Enter` drücken.

27. *Master* wählen und `Enter` drücken.

28. *Sensors* wählen und `Enter` drücken.

29. *Add a new sensor* wählen und `Enter` drücken.

30. IP-Adresse oder Hostnamen des Sensors in das Eingabefeld eingeben und `Enter` drücken.

    → Zusätzliche Menüoptionen für die Sensorkonfiguration werden angezeigt (siehe Abb. 16.3, siehe Kapitel *16.2* (Seite 384)).

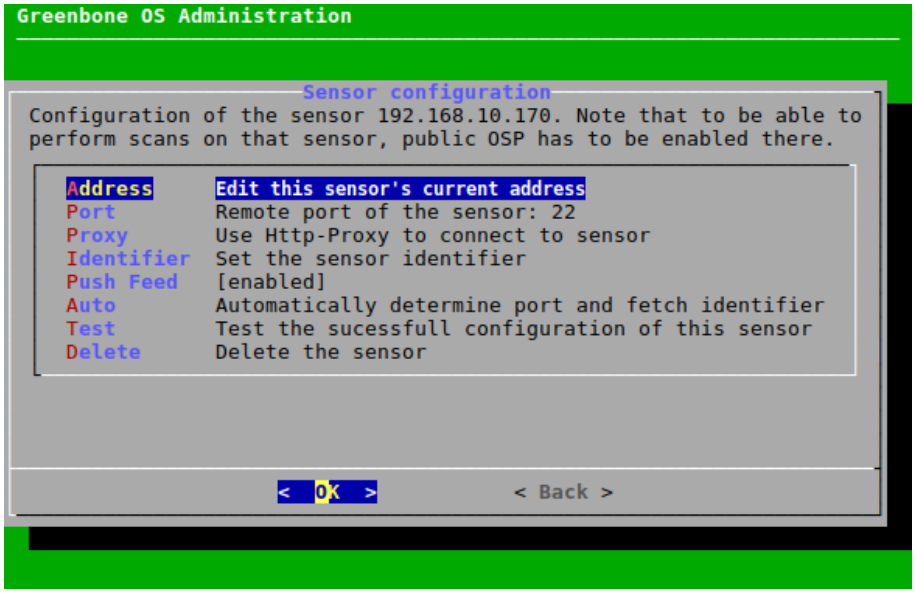


Abb. 16.3: Menü für die Sensorkonfiguration

31. *Auto* wählen und `Enter` drücken.

    → Der Master verbindet sich automatisch mit dem Sensor und ruft den Identifier ab.

    Der Fingerprint des Identifiers wird im GOS-Administrationsmenü des Masters angezeigt.

32. Im GOS-Administrationsmenü des Sensors *Setup* wählen und `Enter` drücken.

33. *Sensor* wählen und `Enter` drücken.

34. *Sensor Identifier* wählen und `Enter` drücken.

35. *Fingerprint* wählen und `Enter` drücken.

36. Fingerprint mit dem Fingerprint, der im GOS-Administrationsmenü des Masters angezeigt wird, vergleichen.

    Falls die Fingerprints übereinstimmen, *Enter* im GOS-Administrationsmenüs des Masters drücken.

37. *Save* wählen und `Enter` drücken.

38. *Test* wählen und `Enter` drücken.

    → Die Konfiguration des Sensors wird getestet.

    Falls der Test fehlschlägt, wird eine Warnung mit Anweisungen angezeigt (siehe Abb. 16.4).

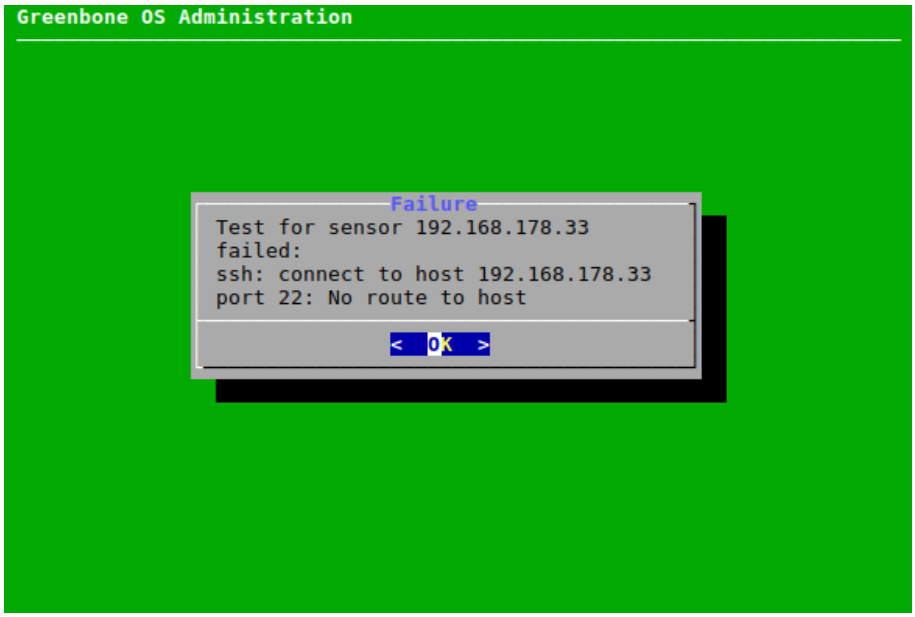


Abb. 16.4: Testen der Sensorkonfiguration

Bemerkung: Wenn sie erfolgreich konfiguriert wurden, können Sensoren direkt vom Master aus über das GOS-Administrationsmenü verwaltet werden (siehe Kapitel *7.3.5* (Seite 151) und *7.3.7* (Seite 152)).

16.2 Alle konfigurierten Sensoren verwalten

Alle auf einem Master konfigurierten Sensoren können wie folgt angezeigt werden:

1. *Setup* wählen und `Enter` drücken.
2. *Master* wählen und `Enter` drücken.
3. *Sensors* wählen und `Enter` drücken.

   → Aktionen für alle konfigurierten Sensoren werden angezeigt (siehe Abb. 16.5).

Die folgenden Aktionen sind verfügbar:

Testing all sensor connections Die korrekte Konfiguration aller Sensoren testen. Falls der Test fehlschlägt, wird eine Warnung mit Anweisungen angezeigt.

Update all sensor protocols Alle Konfigurationen der Sensorprotokolle auf dem Master aktualisieren.

Edit/Delete the sensor . . . Das Menü zum Konfigurieren eines bestimmten Sensors öffnen (siehe Abb. 16.3). Die folgenden Aktionen sind verfügbar:

- Die Adresse des Sensors festlegen.
- Den Remoteport des Sensors festlegen.
- Den Proxy für den Sensor festlegen.

- Den Identifier des Sensors festlegen.
- Automatische Feed-Updates auf dem Sensor aktivieren/deaktivieren. Diese werden ausgeführt, falls auf dem Master ein Feed-Update durchgeführt wird.
- Den Port und den Identifier automatisch festlegen.
- Die korrekte Konfiguration des Sensors testen.
- Den Sensor löschen.

Add a new sensor Einen neuen Sensor konfigurieren (siehe Kapitel *16.1* (Seite 381)).

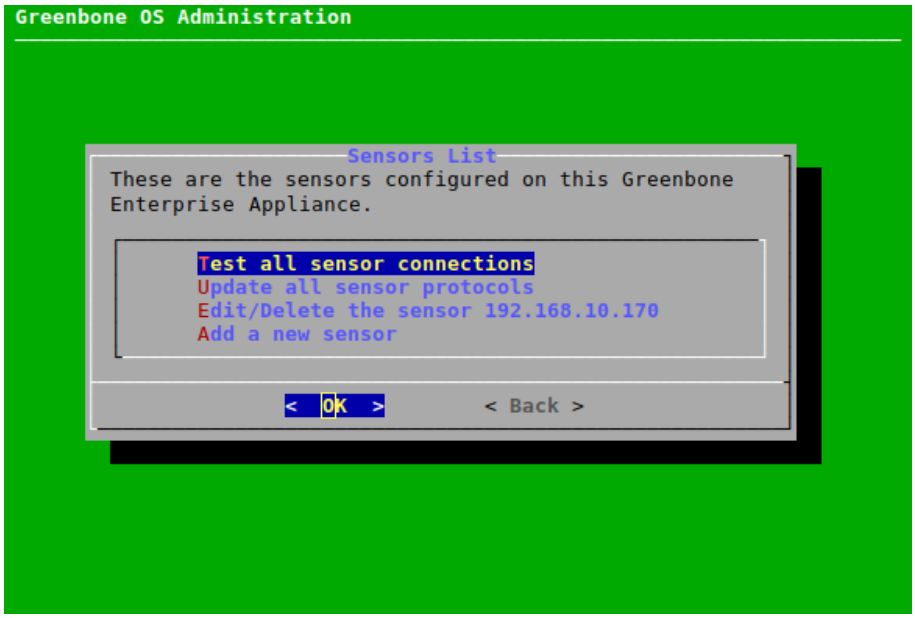


Abb. 16.5: Verwalten aller konfigurierter Sensoren

16.3 Sensoren in sicheren Netzwerken einsetzen

Bei einem Master-Sensor-Setup speichert der Master alle Schwachstelleninformationen und Anmeldedaten. Der Sensor speichert keine Informationen dauerhaft (abgesehen von VTs).

Aus diesem Grund muss der Master in der höchsten Sicherheitszone mit Kommunikation nach außen (zu den Sensoren) platziert sein. Jegliche Kommunikation wird vom Master in der höheren Sicherheitszone aus zum Sensor in der niedrigeren Sicherheitszone veranlasst.

Bemerkung: Eine Firewall, die die unterschiedlichen Zonen trennt, muss nur die Verbindung zum Master zum Sensor erlauben. Zusätzliche Verbindungen in die höhere Sicherheitszone müssen nicht zugelassen werden.

Master und Sensor kommunizieren über das SSH-Protokoll. Der Port 22/TCP wird standardmäßig genutzt. Für Abwärtskompatibilität kann der Port 9390/TCP genutzt werden. Dieser kann wie folgt konfiguriert werden:

1. Im GOS-Administrationsmenü des Sensors *Setup* wählen und `Enter` drücken.
2. *Sensor* wählen und `Enter` drücken.
3. *Port 9390* wählen und `Enter` drücken.
4. *Save* wählen und `Enter` drücken.

Auf Sensoren können Updates des Greenbone Enterprise Feeds und GOS-Upgrades entweder direkt vom Greenbone-Server oder mithilfe des Masters heruntergeladen werden. Im zweiten Fall kontaktiert nur der Master den Greenbone-Server und verteilt die zugehörigen Dateien an alle verbundene Sensoren.

Um zu verhindern, dass der Sensor den Greenbone-Server kontaktiert, kann die automatische Synchronisierung wie folgt deaktiviert werden:

1. Im GOS-Administrationsmenü des Sensors *Setup* wählen und `Enter` drücken.
2. *Feed* wählen und `Enter` drücken.
3. *Synchronisation* wählen und `Enter` drücken.
4. *Save* wählen und `Enter` drücken.

Tipp: Als zusätzlicher Schutz kann eine Regel für Source- und Destination-NAT auf einer Firewall mit Stateful-Packet-Inspection (SPI) genutzt werden, um die Notwendigkeit von Standardrouten auf der Appliance zu vermeiden.

16.4 Einen Sensor als Remote-Scanner konfigurieren

Bemerkung: Um einen Sensor als Remote-Scanner zu konfigurieren, müssen zuerst alle Schritte in Kapitel *16.1* (Seite 381) erledigt werden.

Master können Sensoren als Remote-Scan-Maschinen (Scanner) zusätzlich zu den voreingestellten Scannern OpenVAS und CVE nutzen. Dazu muss der Sensor mithilfe der Web-Oberfläche des Masters als Remote-Scanner konfiguriert sein.

Ein neuer Remote-Scanner kann wie folgt konfiguriert werden:

1. In die Web-Oberfläche des Masters einloggen.
2. *Konfiguration* > *Scanner* in der Menüleiste wählen.
3. Neuen Scanner durch Klicken auf erstellen.
4. Namen des Remote-Scanners in das Eingabefeld *Name* eingeben (siehe Abb. 16.6).

Abb. 16.6: Konfiguration des Remote-Scanners auf dem Master

5. *Greenbone Sensor* in der Drop-down-Liste *Typ* wählen.

   Bemerkung: Die Wahl von *Greenbone Sensor* ist zwingend notwendig. Der Typ *OSP-Scanner* darf nicht verwendet werden.

   ---

6. IP-Adresse oder Hostnamen des Sensors in das Eingabefeld *Host* eingeben.

7. Auf *Speichern* klicken, um den Remote-Scanner zu erstellen.

   → Der Scanner wird erstellt und auf der Seite *Scanner* angezeigt.

8. In der Zeile des neu erstellen Scanners auf klicken, um den Scanner zu verifizieren.

   → Falls das Setup korrekt ist, wird der Scanner erfolgreich verifiziert.

Tipp: Scanner werden pro Benutzer erstellt. Sie können entweder für jeden Benutzer einzeln erstellt werden oder alternativ kann anderen Benutzern die Berechtigung für die Nutzung erteilt werden (siehe Kapitel *9.4* (Seite 195)).

16.5 Einen Remote-Scanner nutzen

Nachdem ein Sensor als Remote-Scanner konfiguriert wurde, kann er als Scanner ausgewählt werden, wenn eine neue Scanaufgabe oder ein neues Audit erstellt wird (siehe Kapitel *10.2.2* (Seite 218) und *12.2* (Seite 325)).

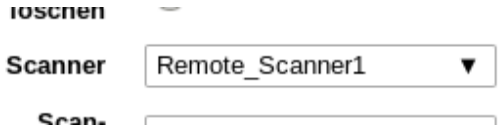


Abb. 16.7: Auswählen des Remote-Scanners für eine Aufgabe oder ein Audit

---

Tipp: Es gibt zwei Möglichkeiten, den Remote-Scanner für ein/e bereits vorhandene/s Aufgabe oder Audit zu verwenden:

- Falls die Aufgabe/das Audit in der Spalte *Name* als änderbar markiert ist (siehe Kapitel *10.8* (Seite 257) und *12.2.3* (Seite 327)), Scanner der Aufgabe/des Audits ändern.
- Die Aufgabe/das Audit klonen und den Scanner des Klons ändern.

KAPITEL 17

Die Leistung verwalten

Beim Betreiben der Greenbone Enterprise Appliance kann eine erhebliche Datenmenge zwischen der Appliance, den Scanzielen und jeder Sensor-Appliance übertragen werden. Zusätzlich müssen die Scanergebnisse von der Appliance analysiert, gefiltert und verarbeitet werden. Abhängig vom Appliance-Modell, von der Anzahl der Benutzer und von der Konfiguration der Scanaufgaben laufen viele dieser Prozesse gleichzeitig ab.

17.1 Die Applianceleistung überwachen

Die Gesamtleistung der Greenbone Enterprise Appliance kann überwacht werden, indem *Administration* > *Leistungsdaten* in der Menüleiste gewählt wird (siehe Abb. 17.1).

Die Ressourcennutzung der Appliance der letzten Stunde, des letzten Tags, der letzten Woche, des letzten Monats oder des letzten Jahrs können angezeigt werden.

Bemerkung: Die Leistung eines konfigurierten Sensors kann ebenfalls auf dem Master angezeigt werden.

Die folgenden Abschnitte sind wichtig:

Prozesse (*Processes*) Eine hohe Anzahl an Prozessen ist nicht kritisch. Es sollten jedoch in erster Linie nur schlafende (*Sleeping*) und laufende (*Running*) Prozesse angezeigt werden.

Systemlast (*System Load*) Eine andauernde Nutzung ist kritisch. Eine Last von 4 auf einem System mit 4 Kernen wird als akzeptabel angesehen.

CPU-Nutzung (*CPU Usage*) Insbesondere ein hoher Wait-IO ist kritisch.

Speichernutzung (*Memory Usage*) Die Appliance nutzt aggressives Caching. Die Nutzung eines Großteils des Speichers als Cache ist akzeptabel.

Swap-Nutzung (*Swap Usage*) Die Nutzung des Swap-Speichers weist auf eine potentielle Systemüberlastung hin.

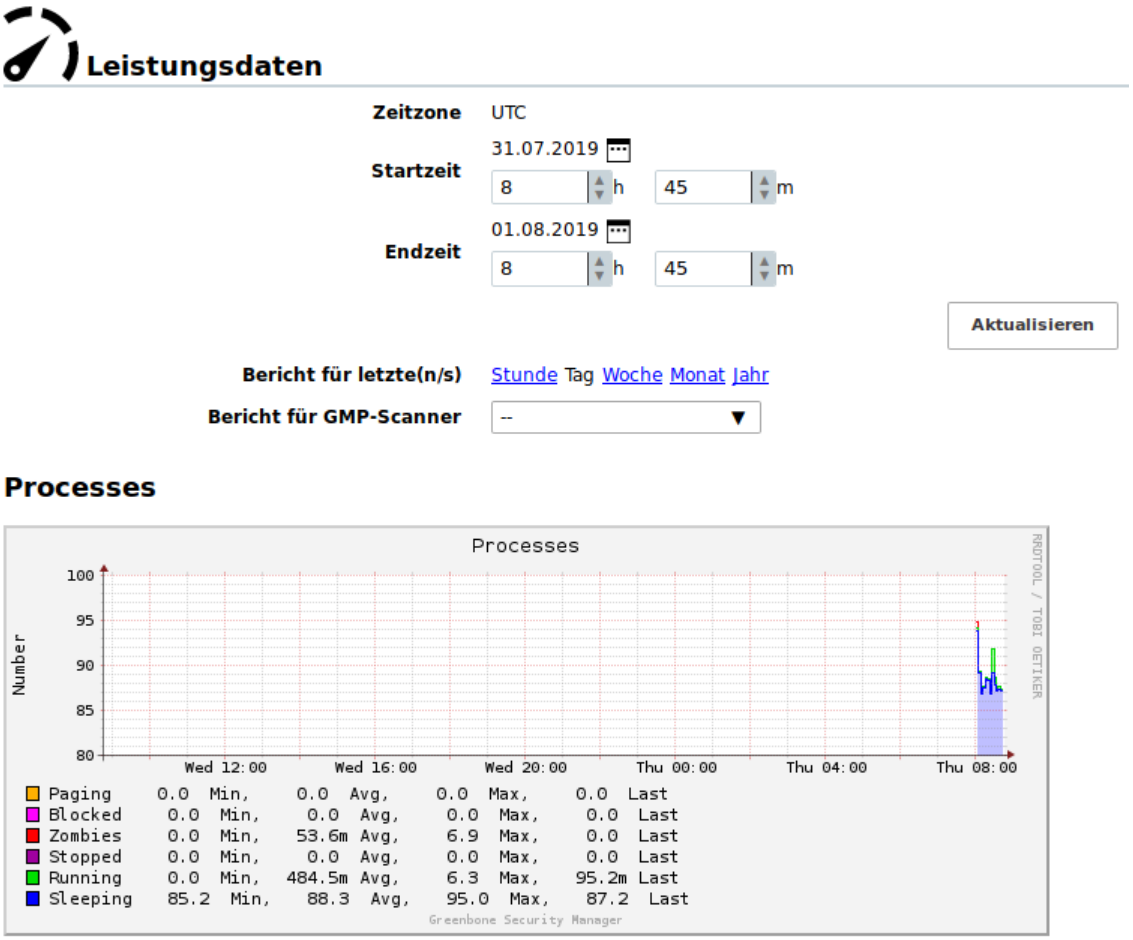


Abb. 17.1: Die Leistung der Appliance anzeigen

17.2 Die Scanleistung optimieren

Die Geschwindigkeit eines Scans hängt von vielen Parametern ab:

- Gewählte Ports
- Gewählte Scan-Konfiguration
- Scanreihenfolge der Ziele

17.2.1 Eine Portliste für eine Aufgabe wählen

Die Portliste, die für ein Ziel konfiguriert wurde, hat einen großen Einfluss auf die Dauer des Erreichbarkeitstests und des Schwachstellenscans dieses Ziels.

17.2.1.1 Allgemeine Informationen über Ports und Portlisten

Ports sind die Verbindungspunkte der Netzwerkkommunikation. Jeder Port eines Systems verbindet sich mit dem Port eines anderen Systems.

Transmission Control Protocol (TCP) Ports

- 65535 TCP-Ports für jedes System
- Datenübertragung zwischen zwei TCP-Ports geschieht in beide Richtungen.
- Der Scan von TCP-Ports wird normalerweise schnell und einfach durchgeführt.

User Datagram Protocol (UDP) Ports

- 65535 UDP-Ports für jedes System
- Datenübertragung zwischen zwei UDP-Ports geschieht nur in eine Richtung.
- Der Empfang von Daten, die über UDP übertragen werden, wird nicht zwingend bestätigt, sodass das Prüfen von UDP-Ports normalerweise länger dauert.

Port 0 bis 1023 sind privilegierte oder Systemports und können nicht von Benutzeranwendungen geöffnet werden[72].

Die Internet Assigned Numbers Authority (IANA)[70] weist Standardprotokollen Ports zu, z. B. Port 80 zu „http“ oder Port 443 zu „https“. Über 5000 Ports sind registriert.

Das Scannen aller Ports dauert in vielen Fällen zu lang und viele Ports werden normalerweise nicht genutzt. Um dieses Problem zu beheben, können Portlisten genutzt werden.

Alle Ports aller Systeme aller per Internet zugänglichen Systeme wurden untersucht und Listen der meist genutzten Ports wurden erstellt. Diese spiegeln nicht unbedingt die IANA-Liste wider, da es keine Pflicht ist, für einen bestimmten Diensttyp einen entsprechenden Port zu registrieren. Nmap[71], ein Open-Source-Portscanner und der OpenVAS-Scanner nutzen standardmäßig unterschiedliche Listen und prüfen nicht alle Ports.

Für die meisten Scans ist es oft ausreichend die Ports zu scannen, die bei IANA registriert sind.

Die folgenden Portlisten sind auf der Appliance vordefiniert:

- All IANA assigned TCP: Alle von der Internet Assigned Numbers Authority (IANA) zugewiesenen TCP-Ports, laufend aktualisiert

[72] Unter Unix-ähnlichen Systemen ist der Zugriff auf diese privilegierten Ports nur für privilegierte Benutzer (d. h. root) erlaubt. Ports ab 1024 sind auch für nicht-privilegierte Benutzer verfügbar.

[70] https://www.iana.org/

[71] https://nmap.org/

- All IANA assigned TCP and UDP: Alle von der Internet Assigned Numbers Authority (IANA) zugewiesenen TCP- und UDP-Ports, laufend aktualisiert
- All privileged TCP
- All privileged TCP and UDP
- All TCP
- All TCP and Nmap top 100 UDP: Alle TCP-Ports und die 100 meistgenutzten UDP-Ports gemäß dem Nmap-Netzwerkscanner, laufend aktualisiert
- All TCP and Nmap top 1000 UDP: Alle TCP-Ports und die 1000 meistgenutzten UDP-Ports gemäß dem Nmap-Netzwerkscanner, laufend aktualisiert
- Nmap top 2000 TCP and top 100 UDP: Die 2000 meistgenutzten TCP-Ports und die 100 meistgenutzten UDP-Ports gemäß dem Nmap-Netzwerkscanner, laufend aktualisiert
- OpenVAS Default: Die TCP-Ports, die vom OpenVAS-Scanner beim Übergeben der standardmäßigen Portbereichpräferenz, gescannt werden

Bemerkung: Zusätzliche Portlisten können, wie in Kapitel *10.7* (Seite 255) beschrieben, erstellt werden.

17.2.1.2 Die richtige Portliste wählen

Beim Wählen einer Portliste muss die Erkennungsleistung und die Scandauer beachtet werden.

Die Dauer eines Scans wird hauptsächlich durch die Netzwerkkonfiguration und die Anzahl der zu prüfenden Ports bestimmt.

Dienste, die nicht an Ports auf der Liste gebunden sind, werden nicht auf Schwachstellen untersucht. Zusätzlich werden schädliche Anwendungen, die an solche Ports gebunden sind, nicht entdeckt. Schädliche Anwendungen öffnen meistens Ports, die für gewöhnlich nicht genutzt werden und weit von den Systemports entfernt sind.

Other criteria are the defense mechanisms that are activated by exhaustive port scans and initiate countermeasures or alerts. Even with normal scans, firewalls can simulate that all 65535 ports are active and as such slow down the actual scan with so called time-outs.

Zusätzlich reagiert der Dienst hinter jedem Port, der abgefragt wird, mindestens einen Log-Eintrag. Aus organisatorischen Gründen dürfen einige Dienste nur zu bestimmten Zeiten gescannt werden.

Scandauer

In Situationen, in denen Portdrosselung auftritt, kann das Scannen aller TCP- und UDP-Ports eines einzelnen Systems bis zu 24 Stunden oder länger dauern. Da alle Scans parallel ausgeführt werden, benötigen zwei Systeme nur unwesentlich mehr Zeit als ein einzelnes System. Trotzdem hat die Parallelisierung aufgrund von Systemressourcen und der Netzwerkleistung ihre Grenzen.

Alle IANA TCP-Ports benötigen normalerweise nur einige Minuten, um gescannt zu werden.

Since some countermeasures can increase the duration of a scan, throttling can be prevented by making configuration changes on the defense system.

Bei Verdachtsfällen einer Kompromittierung oder höchsten Sicherheitsansprüchen ist ein vollständiger Scan unerlässlich.

Totale Sicherheit

Für Portscans besteht keine totale Sicherheit, was bedeutet, dass selbst beim Scannen aller TCP- und aller UDP-Ports das voreingestellte Timeout für die Portprüfung zu kurz sein kann, um eine versteckte schädliche Anwendung zu einer Antwort zu zwingen.

Falls ein anfänglicher Verdacht besteht, sollte ein erfahrener Penetrationstester hinzugezogen werden.

17.2.2 Eine Scan-Konfiguration für eine Aufgabe wählen

Auch die Scan-Konfiguration hat eine Auswirkung auf die Dauer des Scans. Die Appliance bietet für den Schwachstellenscan vier verschiedene Scan-Konfigurationen:

- Full and fast
- Full and fast ultimate
- Full and very deep
- Full and very deep ultimate

Die Scan-Konfigurationen *Full and fast* und *Full and fast ultimate* optimieren den Scanprozess durch die Nutzung von Informationen, die zuvor im Scan gefunden wurden. Nur VTs, die nützlich sind, werden ausgeführt, was zu einer reduzierten Scandauer führt.

Scans, die die Scan-Konfigurationen *Full and very deep* und *Full and very deep ultimate* nutzen, ignorieren bereits gefundene Informationen und führen alle verfügbaren VTs ohne Ausnahme aus.

17.2.3 Die Scanreihenfolge der Ziele wählen

Während eines Scans zeigt der entsprechende Statusbalken auf der Seite *Aufgaben* den Fortschritt des Scans in Prozent (siehe Kapitel *10.8* (Seite 257)).

In den meisten Fällen ist der Fortschritt eine grobe Schätzung, da es für die Appliance schwierig ist, hochzurechnen, wie sich die Systeme oder Dienste, die noch nicht gescannt wurden, im Vergleich zu den bereits gescannten Systemen und Diensten, verhalten.

Beispiel Ein Zielnetzwerk `192.168.0.0/24`, welches nur 5 erreichbare Hosts mit den IP-Adressen `192.168.0.250-254` hat, soll gescannt werden. Wenn die Aufgabe für dieses Ziel mit Standardeinstellungen erstellt wird, versucht der Scanner, alle möglichen Hosts im Zielnetzwerk der Reihe nach zu scannen.

Da für die IP-Adressen `192.168.0.1-249` keine Hosts gescannt werden können, überspringt der Scanner dieses Hosts und der Scanfortschritt erreicht sehr schnell 95 %. Dies lässt vermuten, dass der Scan fast abgeschlossen ist.

Dann werden die Hosts mit den IP-Adressen `192.168.0.250-254` gescannt und für jeden Host nehmen die Schwachstellentests einige Zeit in Anspruch. Aus diesem Grund ist der Scanfortschritt zwischen 95 % und 100 % deutlich langsamer.

Um die Schätzung des Fortschritts zu verbessern, kann die Einstellung *Reihenfolge der Ziel-Hosts* beim Erstellen einer neuen Aufgabe angepasst werden (siehe Kapitel *10.2.2* (Seite 218)).

Die Einstellung *Zufällig* wird empfohlen (siehe Abb. 17.2).

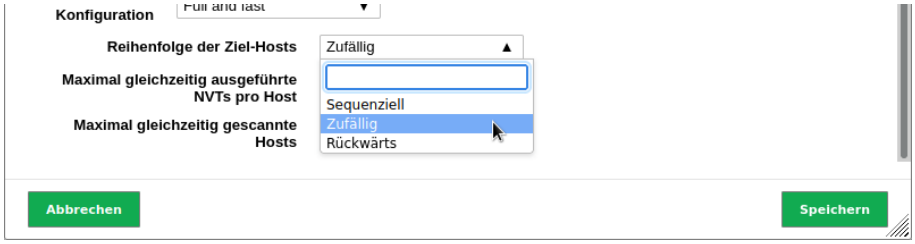


Abb. 17.2: Auswählen der Reihenfolge der Ziele

17.3 Scan-Warteschlange

Wenn ▷ für eine Aufgabe oder ein Audit geklickt wird, wird sie/es einer Warteschlange hinzugefügt und erhält den Status *In Warteschlange*. Der Scanner beginnt nur dann mit dem Scan, wenn genügend Systemressourcen verfügbar sind. Die verfügbaren Ressourcen hängen vom Appliance-Modell, der verwendeten GOS-Version und der aktuellen Arbeitslast des Systems ab. Außerdem werden die Scans in der Warteschlange in Abständen von 1 Minute gestartet, um eine Überlastung des Systems zu vermeiden.

Die wichtigste Ressource ist Random-Access Memory (RAM). Jeder Scan benötigt ein bestimmtes Minimum an RAM, um korrekt ausgeführt zu werden, da derselbe Scanprozess nicht mehrere Scans unterschiedlicher Nutzer oder auch vom gleichen Nutzer bearbeiten kann. Der RAM hat physische Grenzen und kann nicht auf zufriedenstellende Weise geteilt werden.

CPU, Netzwerkverbindung und Festplatten-E/A sind ebenfalls wichtige Systemressourcen. Allerdings können diese im Gegensatz zum RAM auf Kosten einer langsameren Scanausführung geteilt werden.

Die Diagramme zur Systemleistung stellen detaillierte Informationen über den RAM im Verlauf der Zeit bereit (siehe Kapitel *17.1* (Seite 388)).

In manchen Fällen bleiben Aufgaben/Audits in der Warteschlange:

- Es werden zu viele Aufgaben/Audits gleichzeitig gestartet und ausgeführt, und es ist nicht genügend RAM verfügbar.
- Die Appliance führt ein Feed-Update durch und lädt momentan neue VTs.
- Die Appliance wurde gerade gestartet und lädt gerade die VTs.

Wenn der benötigte RAM wieder verfügbar oder das Laden der VTs beendet ist, werden die Scans aus der Warteschlange nach dem Prinzip „first in, first out“ gestartet.

Das Auslastungsmangement unterliegt dem Scanner. Falls ein Master-Sensor-Setup genutzt wird, verwaltet jeder Sensor seine Kapazität selbst. Sensorscans beeinflussen die Scankapazität des Masters nur minimal.

KAPITEL 18

Die Greenbone Enterprise Appliance mit anderen Systemen verbinden

Die Greenbone Enterprise Appliance kann mit anderen System verbunden werden.

Einige Systeme wurden bereits von Greenbone in die Appliance integriert:

- Verinice ITSM-System (siehe Kapitel *18.1* (Seite 395))
- Nagios-Monitoring-System (siehe Kapitel *18.2* (Seite 400))
- Cisco Firepower Management Center (siehe Kapitel *18.3* (Seite 404))

Die Appliance bietet zahlreiche Schnittstellen für die Kommunikation mit anderen Systemen:

Greenbone Management Protocol (GMP) Das Greenbone Management Protocol ermöglicht die vollständige Fernsteuerung der Appliance. Das Protokoll unterstützt das Erstellen von Benutzern, das Erstellen und Starten von Scanaufgaben und das Exportieren von Berichten.

Berichtformat Die Appliance kann die Scanergebnisse in jedem Format wiedergeben. Dafür ist auf der Appliance bereits eine Vielzahl an Berichtformaten vorinstalliert (siehe Kapitel *11.1* (Seite 288)). Zusätzliche Berichtformate können in Zusammenarbeit mit Greenbone entwickelt werden.

Benachrichtigung über Syslog, E-Mail, SNMP-Trap oder HTTP (siehe Kapitel *10.12* (Seite 277))

Automatische Weiterleitung der Ergbnisse über Konnektoren Diese Konnektoren werden durch Greenbone erstellt, verifiziert und in die Appliance integriert.

Überwachung mithilfe von SNMP Die Webseite https://docs.greenbone.net/API/SNMP/snmp-gos-22.04.de.html stellt das aktuelle Management-Information-Base-Datei (MIB-Datei) bereit. MIB-Dateien beschreiben die Dateien, die SNMP über das Gerät abfragen kann.

18.1 Verinice nutzen

Verinice[73] ist ein freies Open-Source-ISMS (Information Security Management System), das von SerNet[74] entwickelt wurde.

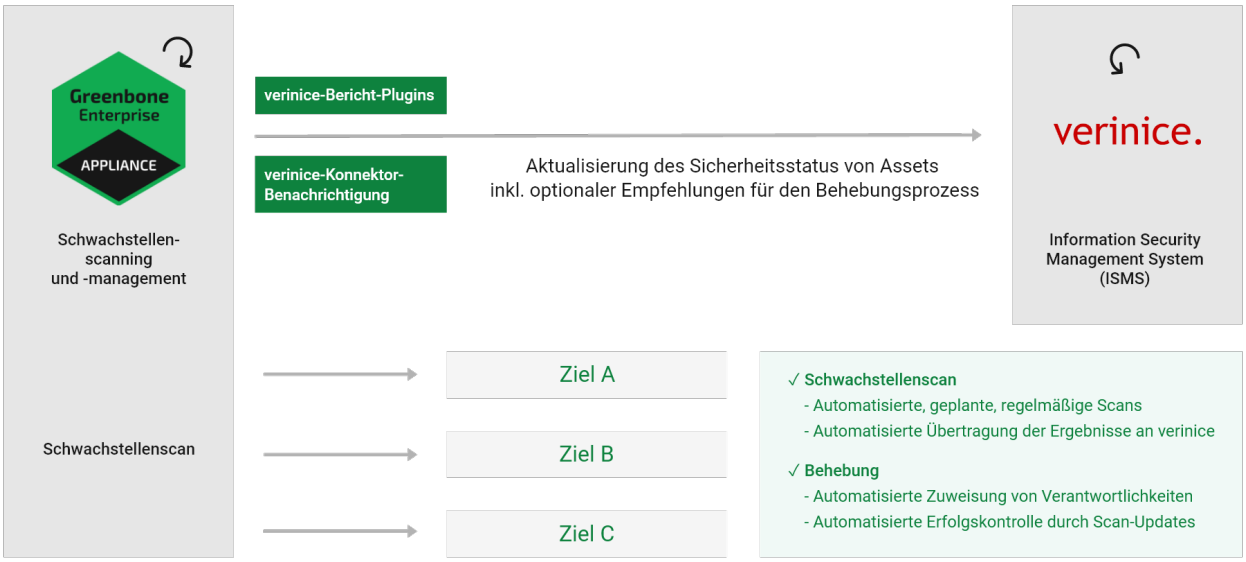


Abb. 18.1: Die Appliance mit verinice verbinden

Verinice eignet sich für:

- Workflow zur Schwachstellenbeseitigung
- Durchführen von Risikoanalysen basierend auf ISO 27005
- Betreiben eines ISMS basierend auf ISO 27001
- Durchführen einer IS-Bewertung per VDA-Spezifikationen
- Nachweisen der Konformität mit Standards wie ISO 27002, IDW PS 330

Die Appliance kann den Betrieb eines ISMS unterstützen. Dafür bietet Greenbone zwei Berichtformate für den Export der Daten aus der Appliance in verinice an:

- Verinice ISM
- Verinice ISM all results

Es ist möglich, die Daten vollkommen automatisch von der Appliance auf verinice.PRO, der Servererweiterung von verinice, zu übertragen.

Bemerkung: Zur Unterstützung bei der Nutzung des Konnektors kann SerNet oder der Greenbone Enterprise Support[75] kontaktiert werden.

---

[73] https://verinice.com/
[74] https://www.sernet.de/
[75] https://www.greenbone.net/technischer-support/

18.1.1 IT-Sicherheitsmanagement

Die Berichtformate *Verinice ISM* und *Verinice ISM all results* für verinice sind über den Greenbone Enterprise Feed verfügbar. Mit diesen Berichtformaten unterstützt Greenbone den Workflow zur Behebung von Schwachstellen in verinice.

Verinice ISM Bei Verwendung des Berichtformats *Verinice ISM* verwendet verinice die Notizfunktion (siehe Kapitel *11.7* (Seite 312)), um Objekte für die Verarbeitung zu erstellen. Jedem Scan-Ergebnis, das an verinice übertragen werden soll, muss eine Notiz beigefügt werden. Wenn dieses Berichtformat verwendet wird und keine Notizen in einer Aufgabe vorhanden sind, werden nur die Assets sowie der komplette Schwachstellenbericht importiert.

Verinice ISM all results Bei Verwendung des Berichtformats *Verinice ISM all results* werden standardmäßig alle Ergebnisse übertragen. Es ist nicht notwendig, die Ergebnisse, die in verinice übertragen werden sollen, mit einer Notiz zu versehen.

Nachdem der Scan abgeschlossen ist, muss der Bericht mithilfe eines der oben genannten Berichtformate exportiert werden (siehe Kapitel *11.2.2* (Seite 298)). Eine VNA-Datei wird erstellt. Dies ist eine ZIP-Datei, die die Scandaten enthält.

Bemerkung: Im folgenden Beispiel wurde SerNet verinice 1.18.1 genutzt.

Falls eine andere Version genutzt wird, unterscheiden sich die Schritte möglicherweise. Der Support von verinice kann zur Unterstützung kontaktiert werden.

18.1.1.1 Den ISM-Scanbericht importieren

Der Bericht kann wie folgt in verinice importiert werden:

1. Verinice starten.
2. *Ansicht* > *Zeige Perspektive. . .* > *Information Security Management* in der Menüleiste wählen (siehe Abb. 18.2).

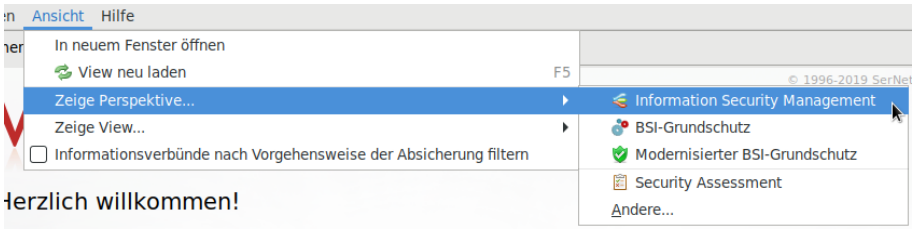


Abb. 18.2: Die Perspektive *Information Security Management* öffnen

3. Im Fenster *Kataloge* auf klicken, um den gewünschten Katalog zu importieren.

4. Auf klicken, um eine Organisation zu erstellen (siehe Abb. 18.3).

Bemerkung: Das Fenster zum Festlegen der Details der Organisation kann einfach geschlossen werden.

Abb. 18.3: Erstellen einer neuen Organisation

5. Im Fenster *ISM* auf klicken.
6. Auf *Datei auswählen...* klicken und den ISM-Bericht wählen. Die übrigen Parameter können mit ihren Standardeinstellungen übernommen werden (siehe Abb. 18.4).

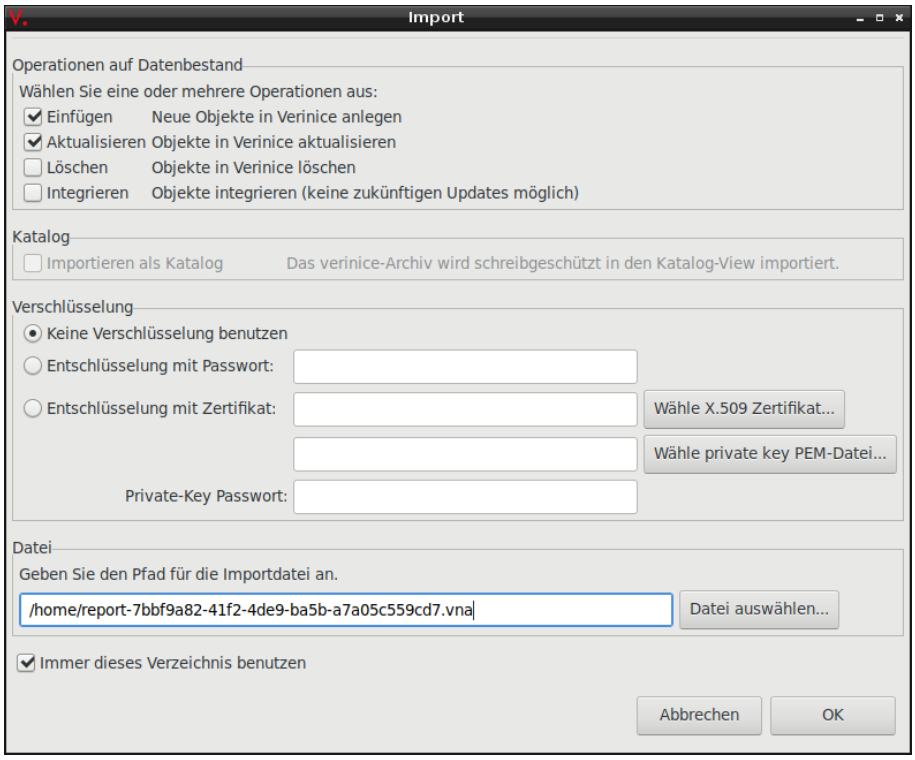


Abb. 18.4: Wählen des ISM-Berichts

7. Auf *OK* klicken.

   → Die Ergebnisse des ISM-Berichts werden importiert und können in verinice ausgeklappt werden (siehe Abb. 18.5).

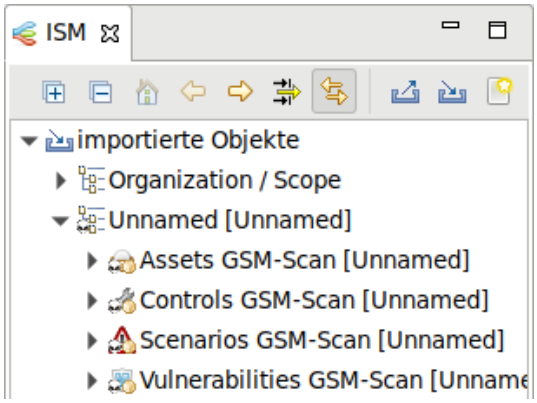


Abb. 18.5: Ausklappen der Ergebnisse des ISM-Berichts

Der Prozess zur Verfolgung von Schwachstellen für die importierte Organisation gliedert sich in zwei Unterprozesse:

- Erstellen von Aufgaben
- Beseitigen von Schwachstellen

18.1.1.2 Aufgaben erstellen

Vor dem Erstellen der Aufgaben müssen die Daten für die Organisation wie folgt vorbereitet werden:

1. Nach dem ersten Importieren einer Organisation muss diese von der Gruppe importierter Objekte auf die oberste Ebene verschoben werden.

   Auf die Organisation rechtsklicken und *Ausschneiden* wählen. In die oberste Ebene im Fenster *ISM* rechtsklicken und *Einfügen* wählen.

2. Die Assets und Controls müssen gruppiert werden.

   Auf *Assets GSM-Scan* rechtsklicken und *Gruppiere mit Tags. . .* wählen (siehe Abb. 18.6).

   Nachricht durch Klicken auf *OK* bestätigen.

3. Auf *Controls GSM-Scan* rechtsklicken und *Gruppiere mit Tags. . .* wählen.

   Nachricht durch Klicken auf *OK* bestätigen.

4. Alle Assetgruppen müssen einer verantwortlichen Person zugeordnet werden.

   Organisation ausklappen, auf *Persons* rechtsklicken und *Neue Person* wählen.

5. Neu erstellte Person per Drag-and-Drop der Assetgruppe zuweisen.

   → Die erfolgreiche Zuweisung kann im Fenster *Verknüpfungen* durch Klicken auf *Assets GSM-Scan* angezeigt werden (siehe Abb. 18.7).

6. Auf die Organisation rechtsklicken und *Aufgaben > Greenbone: Starte Schwachstellenverfolgung. . .* wählen.

   → Es wird verifiziert, ob alle Assets und Controls gruppiert sind und ob alle Assetgruppen einer Person zugewiesen sind. Eine Nachricht zeigt das Ergebnis der Verifizierung an.

7. Mit dem Erstellen der Aufgabe fortfahren oder das Erstellen abbrechen.

   Die Aufgabe zum Beseitigen von Schwachstellen heißt „Remediate Vulnerabilities“.

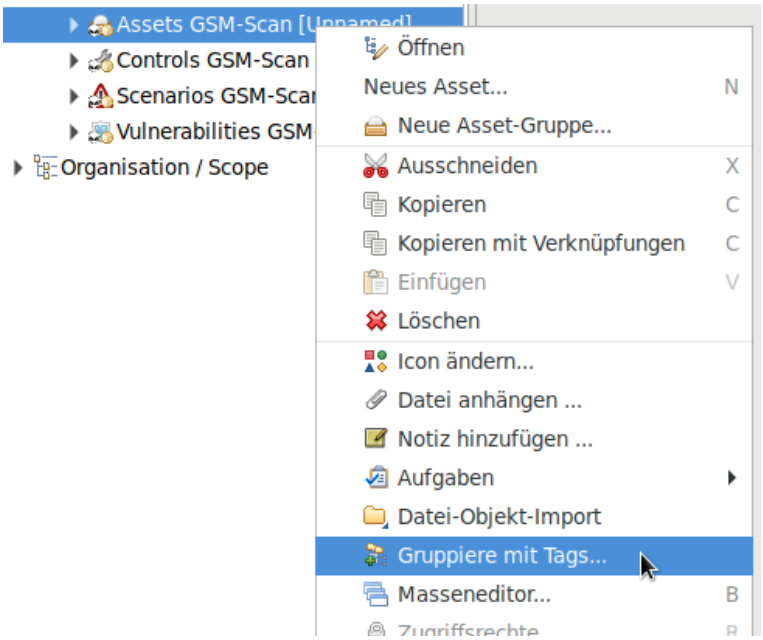


Abb. 18.6: Gruppieren der Assets

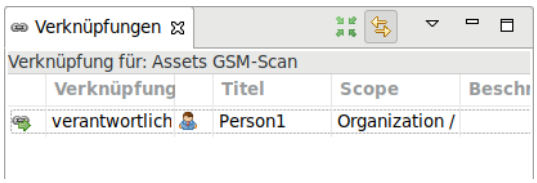


Abb. 18.7: Anzeigen der Beziehungen einer Gruppe

18.1.1.3 Schwachstellen beseitigen

Die erstellten Aufgaben können mithilfe der Ansicht *Aufgaben* (*Ansicht > Zeige View... > Aufgaben* in der Menüleiste) oder des Web-Frontends der verinice.PRO-Version (unter: ISO 27000 tasks) verwaltet werden.

Eine Aufgabe enthält Controls, Scenarios und Assets, welche mit einer Kontrollgruppe verbunden und einer verantwortlichen Person zugeordnet sind. Die verantwortliche Person beseitigt die Schwachstelle für alle Assets.

Bemerkung: Falls die Deadline für die Aufgabe „Remediate Vulnerabilities“ abläuft, wird eine E-Mail mit einer Erinnerung an die verantwortliche Person gesendet.

Nachdem die Aufgabe abgeschlossen ist, werden alle Verbindungen zwischen den Assets und Scenarios, die der Aufgabe zugeordnet waren, gelöscht.

Die folgenden Zustände eines Controls sind möglich:

- Implemented: Dem Scenario ist kein Asset mehr zugeordnet.
- Partly: Andere Verbindungen zu den Assets sind noch vorhanden.

18.2 Nagios nutzen

Nagios kann die Scanergebnisse als zusätzlichen Test in seine Überwachungsaufgaben integrieren. Die gescannten Systeme werden automatisch den überwachten Systemen zugeordnet. Damit sind die Scanergebnisse schlussendlich für Benachrichtigungsregeln und andere Prozesse von Nagios verfügbar.

Abb. 18.8: Verbinden von Nagios mit der Appliance

Beim Verbinden von Nagios mit der Appliance übernimmt Nagios die steuernde Rolle.

Nagios erhält die neuesten Scanergebnisse regelmäßig und automatisch von der Appliance. Dies geschieht mithilfe eines Nagios-Befehls, der das Tool `gvm-script` nutzt, um das Skript `check-gmp.gmp.py` aufzurufen.

Bemerkung: Andere Produkte, die mit Nagios kompatibel sind, wie Open Monitoring Distribution, Icinga, Centreon etc. sollten in der Regel funktionieren, könnten allerdings kleinere Anpassungen der beschriebenen Schritte benötigen.

18.2.1 Den Appliance-Benutzer konfigurieren

Für den Zugang benötigt Nagios einen Benutzer zum Einloggen in die Appliance. Für diesen Benutzer muss ein Scanziel (oder mehrere Scanziele) mit allen Hosts, für die der Sicherheitsstatus überwacht werden soll, erstellt werden.

Bemerkung: Die hier genutzte Beispielkonfiguration nimmt an, dass es nur ein relevantes Ziel gibt, aber streng genommen ist es möglich, komplexe Setups mit mehreren Zielen und mehreren Appliances einzubinden.

Der Appliance-Benutzeraccount, der für Abfragen vom GMP-Skript bereitgestellt wird, muss der Besitzer der relevanten Scanziele sein oder zumindest uneingeschränkten Lesezugriff auf diese haben.

Die Aufgaben sollten regelmäßig als geplante Scans laufen.

Zusätzlich muss der Netzwerkzugriff auf die Appliance über GMP möglich sein. Dafür muss der GMP-Zugriff im GOS-Administrationsmenü aktiviert werden (siehe Kapitel *15.2* (Seite 370)).

18.2.2 Das Skript konfigurieren

Greenbone stellt das Skript `check-gmp.gmp.py` als Teil der Skriptsammlung der gvm-tools bereit (siehe Kapitel *15.3* (Seite 371)). Dieses Skript kann von der Überwachungslösung mithilfe von `gvm-script` aufgerufen werden.

Bemerkung: Im Folgenden wird angenommen, dass Nagios unter `/usr/local/nagios/`, nachfolgend als `/.../` bezeichnet, installiert ist.

Der Speicherort kann bei Bedarf angepasst werden.

1. Plug-in nach `/.../libexec/` kopieren.
2. Prüfen, ob das Skript die Appliance über das Netzwerk erreichen kann, GMP aktiviert wurde und der Benutzer korrekt erstellt wurde:

   Bemerkung: Im folgenden Befehl müssen die IP-Adresse durch die IP-Adresse der Appliance ersetzt und der Benutzername und das erstellte Passwort angegeben werden.

```
nagios-host# gvm-script --gmp-username="user name" --gmp-password="password" \
ssh --hostname 192.168.10.169 /.../libexec/check-gmp.gmp.py --ping \
GMP OK: Ping successful
```

3. Prüfen, ob auf die Daten zugegriffen werden kann:

```
nagios-host# gvm-script --gmp-username="user name" --gmp-password="password" \
ssh --hostname 192.168.10.169 /.../libexec/check-gmp.gmp.py \
-F 192.168.10.130 --last-report -T "Scan Suspect Host" --status
GMP CRITICAL: 284 vulnerabilities found - High: 118 Medium: 153 Low: 13
Report did contain 1 errors for IP 192.168.10.130
|High=118 Medium=153 Low=13
```

Das Skript unterstützt mehrere Befehlszeilenoptionen. Diese können wie folgt dargestellt werden:

```
nagios-host# gvm-script -c /.../etc/gvm-tools.conf ssh --hostname
  192.168.10.169 scripts/check-gmp.gmp.py -H
usage: check-gmp [-H] [-V] [--cache [CACHE]] [--clean] [-F HOSTADDRESS] [-T TASK]
...

Check-GMP Nagios Command Plugin 2.0.0 (C) 2017-2019 Greenbone Networks GmbH
...


optional arguments:
-H                    Show this help message and exit.
-V, --version         Show program's version number and exit
--cache [CACHE]       Path to cache file. Default: /tmp/check_gmp/reports.db.
--clean               Activate to clean the database.
...
```

4. Falls die Tests erfolgreich waren, kann der Check in den Nagios-Monitor integriert werden.

   Host, der überwacht werden soll, der Nagios-Konfigurationsdatei `/.../etc/objects/localhost.cfg` im Abschnitt `HOST DEFINITIONS` hinzufügen.

   In diesem Beispiel ist der Host ein Metasploitable Linux.

```
define host{
     use                     linux-server
     host_name               metasploitable
     alias                   metasploitable
     address                 192.168.10.130
     }
```

5. In der gleichen Konfigurationsdatei im Abschnitt `SERVICE DEFINITIONS` einen neuen Dienst, der den Nagios-Befehl `check_gmp_status` aufruft, festlegen.

   Wie das Beispiel zeigt, wird der Name der Aufgabe, von der der Bericht abgerufen wird, als Argument an den Befehl übergeben.

```
define service{
     use                     local-service    ; Name of service template to use
     host_name               metasploitable
     service_description     GMP task last report status
     check_command           check_gmp_status!metasploitable
     }
```

6. Befehl `check_gmp_status` in der Datei `/.../etc/objects/commands.cfg` erstellen.

```
define command{
    command_name    check_gmp_status
    command_line    gvm-script -c /.../etc/gvm-tools.conf ssh
       --hostname 192.168.10.169 $USER1$/check-gmp.gmp.py -F $HOSTADDRESS$
         --last-report -T $ARG1$ --status
    }
```

Bemerkung: In der Kommandozeile ist sichtbar, dass kein Benutzername- und Passwortoptionen, sondern eine Konfigurationsdatei an das Tool `gvm-script` übergeben wird (sie Kapitel *15.3* (Seite 371)).

7. Zum Anwenden der neuen Konfiguration Nagios neu starten.

```
nagios-host# systemctl restart nagios
```

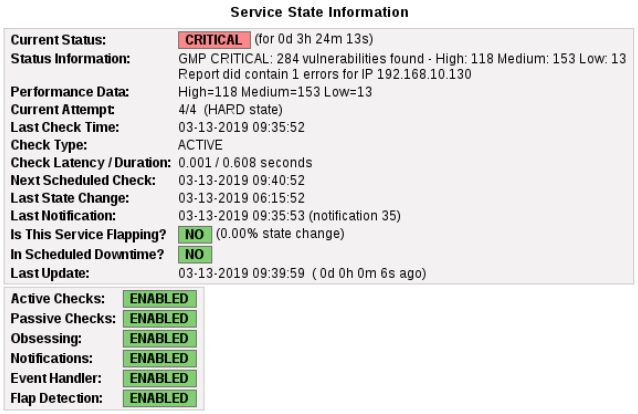


Abb. 18.9: Status der überwachten Hosts in Nagios

18.2.3 Caching und Multiprocessing

Das Skript `check-gmp.gmp.py` überstützt Caching. Alle neuen Berichten werden in einer SQLite-Datenbank zwischengespeichert. Der erste Aufruf mit einem unbekannten Host dauert länger, da der Bericht erst von der Appliance abgerufen werden muss. Darauffolgende Aufrufe holen nur dann den aktuellen Bericht von der Appliance, falls sich die Endzeit vom Scan unterscheidet. Andernfalls wird die Information aus der Datenbank genutzt. Dies reduziert die Belastung auf dem überwachenden Server sowie der Appliance.

Die Cachedatei wird standardmäßig auf `/tmp/check_gmp/reports.db` geschrieben. Ein anderer Speicherort der Datenbank kann mithilfe der Befehlszeilenoption `--cache` bestimmt werden.

Um die Belastung des überwachenden Servers sowie der Appliance weiter zu reduzieren, kann das Plug-in die maximale Anzahl gleichzeitig laufender Plug-in-Instanzen beschränken. Zusätzlich gestartete Instanzen werden gestoppt und warten auf Fortsetzung. Der Standardwert von `MAX_RUNNING_INSTANCES` ist 10 und kann mithilfe der Befehlszeilenoption `-I` geändert werden.

18.3 Das Cisco Firepower Management Center nutzen

Das Cisco Firepower Management Center (früher Sourcefire Intrusion Prevention System (IPS)) ist eine der führenden Lösungen für Eindringungserkennung und -abwehr in Computernetzwerken. Als ein Network Intrusion Detection System (NIDS) sind seine Aufgaben die Erkennung von Gefährdungen, die Alarmierung und die Verteidigung gegen Angriffe auf das Netzwerk.

Um Angriffe korrekt zu identifizieren und klassifizieren, benötigt das Firepower Management Center so viele Informationen wie möglich über die Systeme im Netzwerk, die auf den Systemen installierten Anwendungen sowie die potenziellen Schwachstellen für beides. Zu diesem Zweck hat das Firepower Management Center seine eigene Asset-Datenbank, welche mit Informationen von der Appliance erweitert werden kann. Zusätzlich kann das Firepower Management Center automatisch Scans starten, falls es einen Verdacht hat.

Die folgenden Verbindungsmethoden sind verfügbar:

Automatische Datenübertragung von der Appliance zum NIDS/IPS Falls die Appliance und das NIDS/IPS entsprechend konfiguriert sind, kann die Datenübertragung von der Appliance zum NIDS/IPS einfach wie jede andere Benachrichtigungsfunktion der Appliance durchgeführt werden. Nach dem Abschluss des Scans wird der Bericht als Benachrichtigung bezüglich der gewünschten Kriterien an das NIDS/IPS weitergeleitet. Falls die Scanaufgabe automatisch auf wöchentlicher Basis läuft, wird ein vollautomatisches Benachrichtigungs- und Optimierungssystem erzielt.

Aktive Steuerung der Appliance durch das NIDS/IPS Beim Betrieb des NIDS/IPS können Verdachtsfälle auf Systemen mit hoher Gefährdung auftreten. Das NIDS/IPS kann in einem solchen Fall die Appliance anweisen, das System zu überprüfen[78].

Bemerkung: Um die Verbindungsmethoden zu nutzen, muss die Option zum Empfang der Daten im Firepower Management Center aktiviert sein.

18.3.1 Die Clients der Host-Eingabe-API konfigurieren

Die Host-Eingabe-API ist eine Schnittstelle durch die das Firepower Management Center Daten von anderen Anwendungen für seine Asset-Datenbank akzeptiert.

1. In das Firepower Management Center einloggen.
2. *System* > *Integration* in der Menüleiste wählen.
3. Register *Host Input Client* wählen.
4. IP-Adresse der Appliance in das Eingabefeld *Hostname* eingeben (siehe Abb. 18.10).

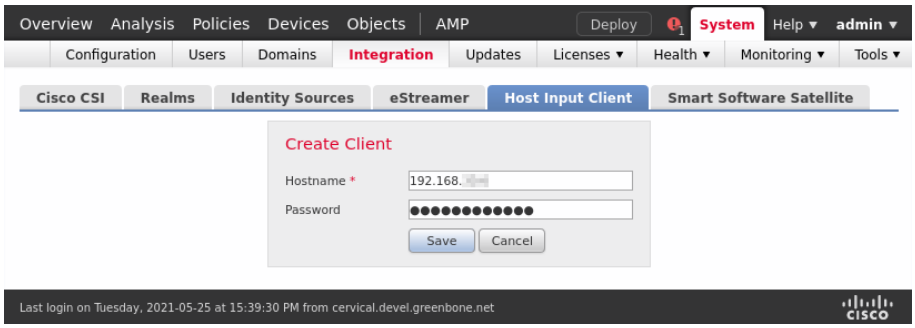


Abb. 18.10: Erstellen eines Host-Eingabe-Clients

[78] Diese Steuerung existiert nicht als fertige *Remediation* für das Firepower Management Center, aber kann mithilfe von GMP implementiert werden (siehe Kapitel *15* (Seite 370)).

5. Passwort in das Eingabefeld *Password* eingeben.
6. Auf *Save* klicken.

Bemerkung: Die Verbindung ist TLS-verschlüsselt.

→ Das Firepower Management Center erstellt automatisch einen privaten Schlüssel und ein Zertifikat.

Im Zertifikat wird die oben eingegebene IP-Adresse als gemeinsamer Name genutzt und verifiziert, wenn der Client eine Verbindung herstellt. Falls der Client eine andere IP-Adresse nutzt, schlägt die Verbindung fehl.

Die erstellte PKCS#12-Datei kann optional durch ein Passwort geschützt werden.

Anschließend werden das Zertifikat und der Schlüssel erstellt und können heruntergeladen werden.

7. Datei durch Klicken auf herunterladen (siehe Abb. 18.11).

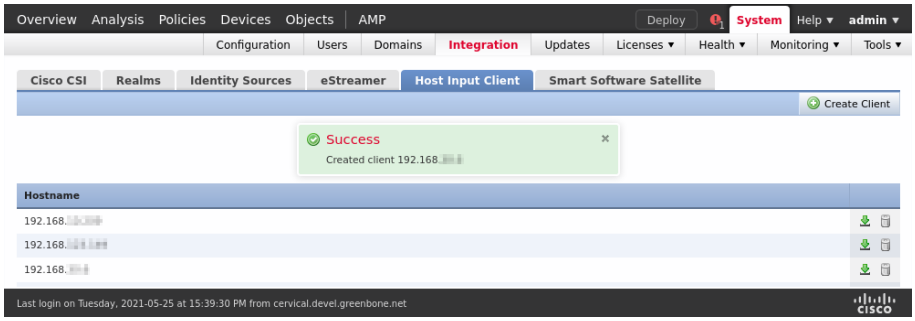


Abb. 18.11: Herunterladen der erstellten PKCS#12-Datei

18.3.2 Eine Benachrichtigung durch eine Sourcefire-Schnittstelle konfigurieren

Nun muss die entsprechende Benachrichtigung auf der Appliance eingerichtet werden.

1. *Konfiguration* > *Benachrichtigungen* in der Menüleiste wählen.
2. Neue Benachrichtigung durch Klicken auf erstellen.
3. Benachrichtigung definieren (siehe Abb. 18.12).

Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *10.12* (Seite 277).

4. *Sourcefire-Schnittstelle* in der Drop-down-Liste *Methode* wählen.
5. IP-Adresse des Management Centers in das Eingabefeld *Defense Center IP* und den Port, der für die Verbindung verwendet wird, in das Eingabefeld *Defense Center Port* eingeben.

Bemerkung: Wenn bei der Erstellung des Clients ein Passwort vergeben wurde, muss das Passwort für die PKCS#12-Datei als Anmeldedaten angegeben werden (siehe Kapitel *10.3.2.1* (Seite 222)).

6. Anmeldedaten in der Drop-down-Liste *PKCS12-Anmeldedaten* wählen.

Bemerkung: Neue Anmeldedaten können durch Klicken auf erstellt werden.

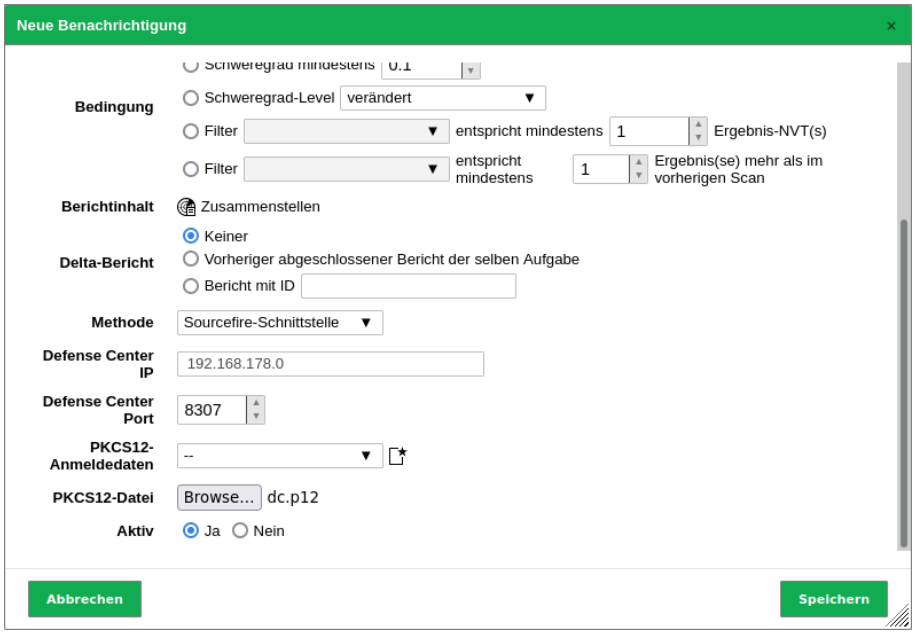


Abb. 18.12: Erstellen einer Benachrichtigung durch eine Sourcefire-Schnittstelle

7. PKCS#12-Datei durch Klicken auf *Browse...* bereitstellen.
8. Auf *Speichern* klicken.

18.4 Alemba vFire nutzen

vFire ist eine Enterprise-Service-Management-Anwendung, die von Alemba[76] entwickelt wurde.

Die Appliance kann konfiguriert werden, sodass sie Tickets in einer Instanz von vFire erstellt, beispielsweise basierend auf beendeten Scans.

18.4.1 Voraussetzungen für Alemba vFire

Damit die Integration korrekt funktioniert, müssen die folgenden Voraussetzungen auf dem vFire-System gegeben sein:

- Die vFire-Installation muss die RESTful-AlembaAPI unterstützen, welche in Version 9.7 zu vFire hinzugefügt wurde. Die veraltete API älterer Versionen wird nicht von der Greenbone-Verbindung unterstützt.
- Ein Alemba-API-Client mit dem korrekten Sitzungstyp (analyst/user) und Passwort-Login muss aktiviert sein.
- Der Benutzeraccount, der genutzt werden soll, benötigt die Berechtigung, die Alemba-API zu nutzen.

18.4.2 Eine Benachrichtigung durch Alemba vFire konfigurieren

Damit die Appliance automatisch Tickets (sogenannte „Calls“) in vFire erstellen kann, muss die Benachrichtigung wie folgt eingerichtet werden:

1. *Konfiguration* > *Benachrichtigungen* in der Menüleiste wählen.
2. Neue Benachrichtigung durch Klicken auf erstellen.
3. Benachrichtigung definieren (siehe Abb. 18.13).

   Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *10.12* (Seite 277).

4. *Alemba vFire* in der Drop-down-Liste *Methode* wählen.
5. Auf *Speichern* klicken.

Die folgenden Details der Benachrichtigung können festgelegt werden:

Berichtformate Die für Anhänge genutzten Berichtformate. Mehrere Berichtformate können gewählt werden oder die Auswahl kann leer gelassen werden, falls keine Anhänge erwünscht sind.

Basis URL Dies ist die URL der Alemba-Instanz, einschließlich des Servernamen und des virtellen Verzeichnisses. Falls beispielsweise über `https://alemba.example.com/vfire/core.aspx` auf die Benutzerschnittstelle zugegriffen wird, wäre die Basis-URL `https://alemba.example.com/vfire`.

Anmeldedaten Benutzername und Passwort für das Einloggen in Alemba vFire.

Sitzungstyp Genutzer Sitzungstyp. Dies kann entweder „analyst“ oder „user“ sein.

Als „analyst“ ist es möglich einige Aktionen durchzuführen, die als „user“ nicht verfügbar sind. Der „user“ benötigt besondere Berechtigungen für diese Aktionen und die Anzahl aufeinanderfolgender Logins könnte begrenzt sein.

Alemba-Client-ID Dies ist die ID des Alemba-Clients (siehe Kapitel *18.4.1* (Seite 407)).

Partition Die Partition, in der das Ticket erstellt wird. Die Alemba-vFire-Hilfe enthält weitere Informationen über die Partitionierung .

[76] https://alemba.com/

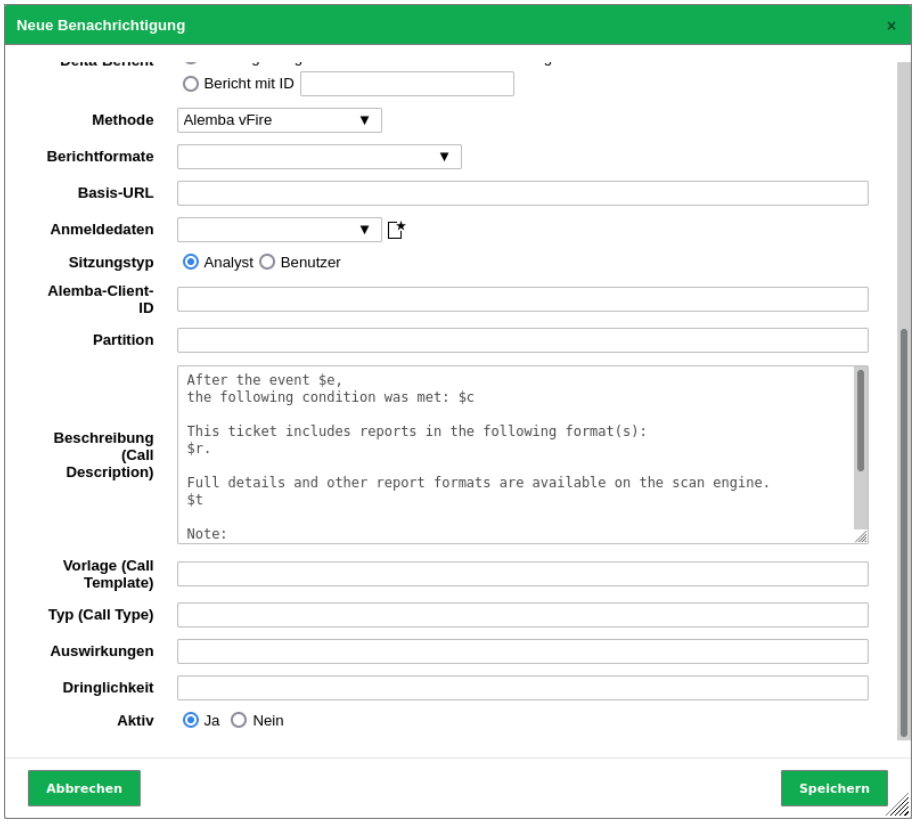


Abb. 18.13: Erstellen einer Benachrichtigung durch Alemba vFire

Beschreibung (Call Description) Dies ist die Vorlage für den Beschreibungstext, der für neu erstellte Calls genutzt wird. Dieselben Platzhalter wie für das Eingabefeld der Nachricht einer E-Mail-Benachrichtigung können genutzt werden (siehe Kapitel *10.12* (Seite 277)).

Vorlage (Call Template) Der Name der Call-Vorlage, die für durch die Benachrichtigung erstellte Calls genutzt wird. Eine Call-Vorlage kann in vFire so konfiguriert werden, dass alle Felder ausgefüllt werden, die nicht direkt in der Benachrichtigung festgelegt werden können.

Typ (Call Type) Der Name eines Call-Typs, der für durch die Benachrichtigung erstellte Calls genutzt wird.

Auswirkungen Der vollständige Name eines Auswirkungswerts.

Dringlichkeit Der vollständige Name eines Dringlichkeitswerts.

18.5 Splunk nutzen

Die Appliance kann so konfiguriert werden, dass sie die Scanergebnisse für die weitere Untersuchung und Zuordnung an eine Splunk-Enterprise-Installation weiterleitet.

Die Verbindung einer Appliance mit einer Splunk-Lösung ist nicht Teil der Appliance-Kernfunktionalität. Als Add-On stellt Greenbone eine App für die Integration mit On-Premise-Lösungen von Splunk Enterprise zur Verfügung. Die App ist derzeit unter https://download.greenbone.net/tools/Greenbone-Splunk-App-1.0.1.tar.gz verfügbar.

Wichtig: Externe Links zur Greenbone-Downloadseite unterscheiden Groß- und Kleinbuchstaben.

Großbuchstaben, Kleinbuchstaben und Sonderzeichen müssen exakt so, wie sie in den Fußnoten stehen, eingegeben werden.

Bemerkung: Falls es Probleme beim Herunterladen oder Testen der App gibt, kann der Greenbone Enterprise Support[77] kontaktiert werden.

Im Folgenden wird Splunk Enterprise Version 8.5 genutzt. Die Installation der App auf Splunk Light wird nicht unterstützt. Das Verbinden einer Appliance mit Splunk Cloud wird nicht unterstützt.

18.5.1 Die Greenbone-Splunk-App einrichten

18.5.1.1 Die App installieren

Die Greenbone-Splunk-App kann wie folgt installiert werden:

1. Splunk Enterprise öffnen.
2. Im linken Menüpanel auf  klicken (siehe Abb. 18.14).

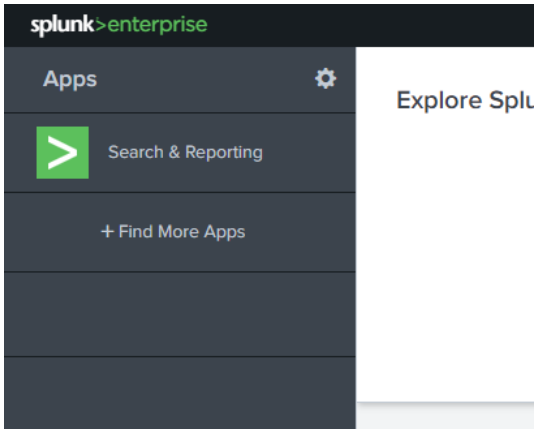


Abb. 18.14: Installieren der Greenbone-Splunk-App

3. Auf *Install app from file* klicken.
4. Auf *Browse...* klicken.
5. TAR-Datei der Greenbone-Splunk-App wählen.

[77] https://www.greenbone.net/technischer-support/

6. Auf *Upload* klicken.

18.5.1.2 Die Greenbone-Splunk-App konfigurieren

Der Port der Greenbone-Splunk-App wird für die Konfiguration auf der Appliance benötigt.

Port der Greenbone-Splunk-App wie folgt überprüfen:

1. Greenbone-Splunk-App im linken Menüpanel wählen.
2. *Settings* > *Data inputs* in der Menüleiste wählen.
3. Auf *TCP* klicken (siehe Abb. 18.15).

Bemerkung: Die Greenbone-Splunk-App richtet einen Dateneingang auf Port 7680/tcp (Standardport) ein und kennzeichnet die eingehenden Daten als *Greenbone Scan Results* und ordnet sie in den Index *default* ein.

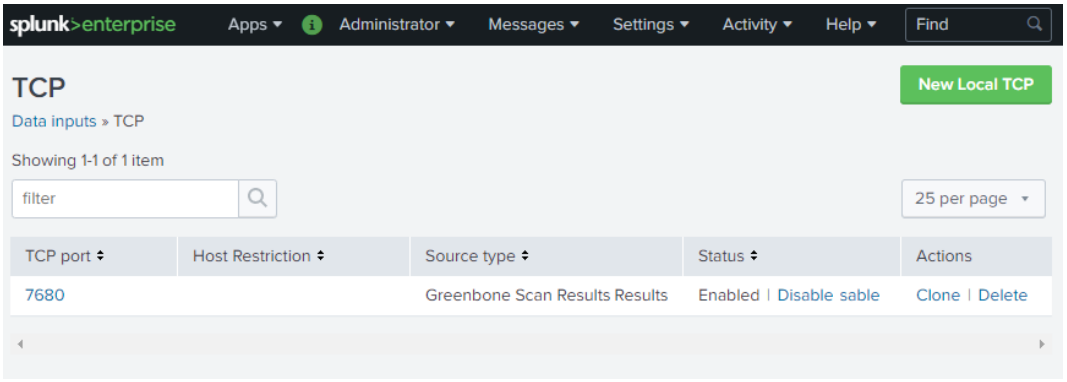


Abb. 18.15: Prüfen des Ports der Greenbone-Splunk-App

Um die Daten benutzerfreundlicher machen, können die Feldnamen wie folgt ersetzt werden:

1. Im linken Menüpanel auf  klicken.
2. In der Zeile von *Greenbone* auf *View objects* klicken.
3. Auf *Greenbone Scan Results: FIELDALIAS-reportfields* klicken.
4. Feldnamen-Alias in die entsprechenden Eingabefelder eingeben (siehe Abb. 18.16).

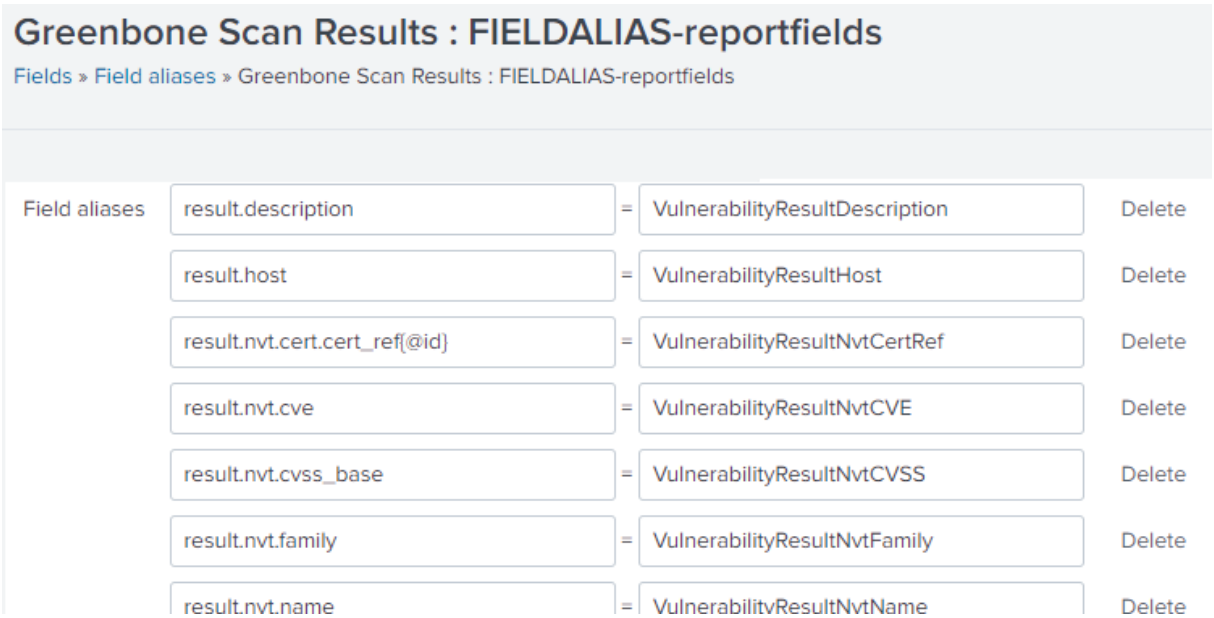


Abb. 18.16: Ändern der Feldnamen-Alias

18.5.2 Eine Benachrichtigung durch Splunk konfigurieren

Die Appliance überträgt die Scanergebnisse in Form eines XML-Berichts über eine Benachrichtigung direkt an den Splunk-Hauptserver.

Bemerkung: Das Dashboard der Greenbone-Splunk-App zeigt nur Ergebnisse von Berichten an, die weniger als 7 Tage alt sind.

Falls ein Bericht gesendet wird, der älter als 7 Tage ist, zeigt das Dashboard die Ergebnisse nicht an. Die Ergebnisse befinden sich jedoch im Hauptindex des Splunk-Servers.

18.5.2.1 Die Splunk-Benachrichtigung erstellen

Die Benachrichtigung kann wie folgt erstellt werden:

1. *Konfiguration* > *Benachrichtigungen* in der Menüleiste wählen.
2. Neue Benachrichtigung durch Klicken auf erstellen.
3. Benachrichtigung definieren (siehe Abb. 18.17).

   Tipp: Für die Informationen, die in die Eingabefelder eingegeben werden müssen, siehe Kapitel *10.12* (Seite 277).

   ---

4. *Sende an Host* in der Drop-down-Liste *Methode* wählen.

5. IP-Adresse des Splunk-Servers in das Eingabefeld *Sende an Host* und `7680` in das Eingabefeld *auf Port* eingeben.

   Bemerkung: Der TCP-Port ist standardmäßig 7680.

   Die Einstellung kann in der Greenbone-Splunk-App, wie in Kapitel *18.5.1.2* (Seite 410) beschrieben, geprüft werden.

   ---

6. *XML* in der Drop-down-Liste *Bericht* wählen.

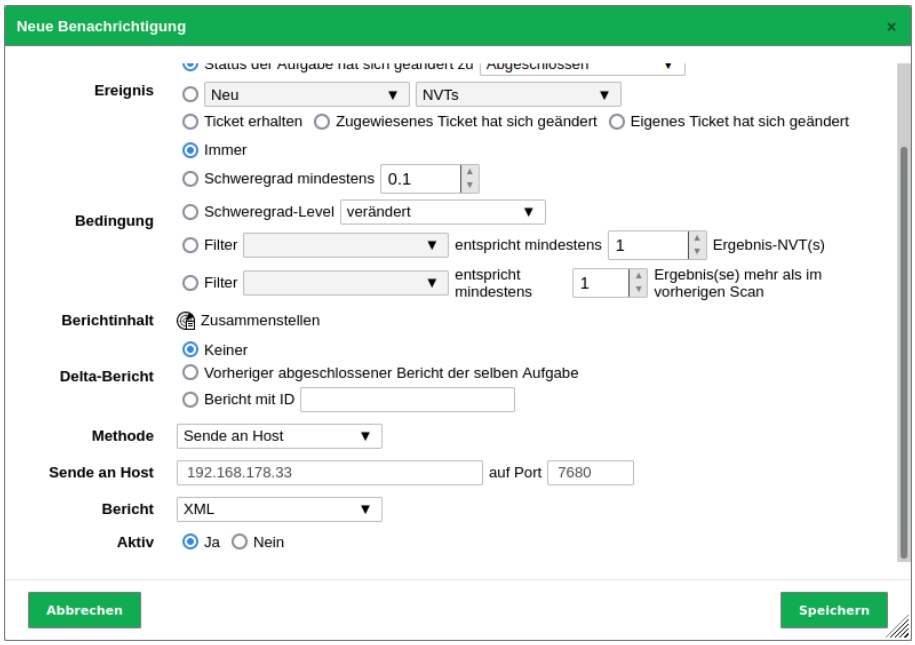


Abb. 18.17: Konfiguration der Benachrichtigung durch Splunk

7. Auf *Speichern* klicken.

18.5.2.2 Die Splunk-Benachrichtigung zu einer Aufgabe hinzufügen

Die Benachrichtigung kann nun beim Erstellen einer neuen Aufgabe gewählt (siehe Kapitel *10.2.2* (Seite 218)) oder zu einer bestehenden Aufgabe hinzugefügt (siehe Kapitel *10.12.2* (Seite 283)) werden.

18.5.2.3 Die Splunk-Benachrichtigung testen

Zu Testzwecken können Berichte von der Benachrichtung verarbeitet werden.

1. *Scans* > *Berichte* in der Menüleiste wählen.
2. Auf das Datum eines Berichts klicken.
3. Auf ▷ klicken.
4. Benachrichtigung in der Drop-down-Liste *Benachrichtigung* wählen (siehe Abb. 18.18).
5. Auf *OK* klicken.

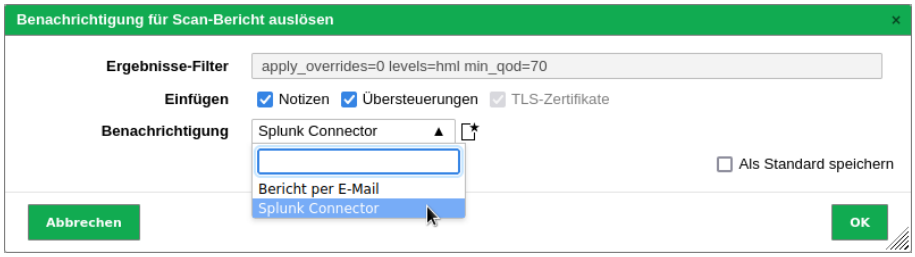


Abb. 18.18: Auslösen der Benachrichtigung

18.5.3 Die Greenbone-Splunk-App nutzen

18.5.3.1 Auf die Informationen in Splunk zugreifen

Um in Splunk auf die Informationen zuzugreifen, kann das Greenbone-Dashboard wie folgt geöffnet werden:

1. Splunk Enterprise öffnen.
2. Greenbone-Splunk-App im linken Menüpanel wählen.
3. *Dashboards* in der Menüleiste wählen.
4. Auf *Greenbone Dashboard* klicken.

Bemerkung: Das Dashboard der Greenbone-Splunk-App zeigt nur Ergebnisse von Berichten an, die weniger als 7 Tage alt sind.

Falls ein Bericht gesendet wird, der älter als 7 Tage ist, zeigt das Dashboard die Ergebnisse nicht an. Die Ergebnisse befinden sich jedoch im Hauptindex des Splunk-Servers.

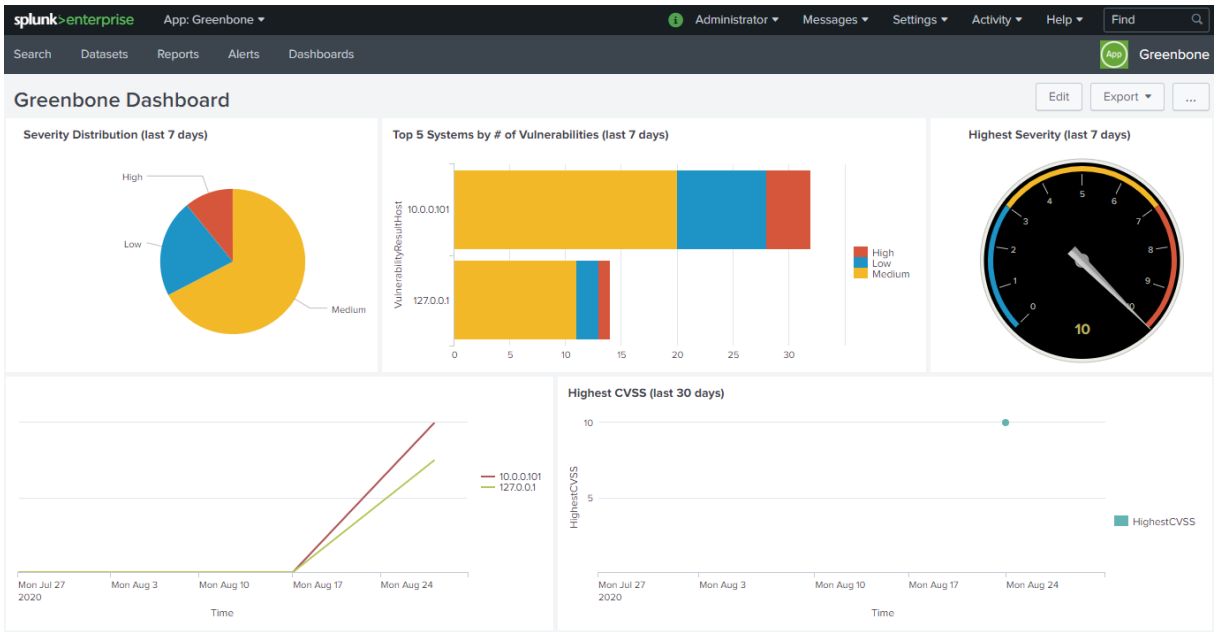


Abb. 18.19: Greenbone-Dashboard in der Greenbone-Splunk-App

Das Eingabefeld *CVE-ID* unterhalb des Dashboards kann verwendet werden, um die Anzahl der von einer bestimmten CVE betroffenen Hosts im Laufe der Zeit anzuzeigen.

Bemerkung: Falls das Eingabefeld leer gelassen und `Enter` gedrückt wird, wird die Anzahl der von allen CVEs betroffenen Hosts angezeigt.

18.5.3.2 Eine Suche durchführen

Da die von der Appliance übermittelten Informationen von Splunk indiziert werden, kann die Suchansicht zur Suche nach beliebigen Daten wie folgt verwendet werden:

1. Splunk Enterprise öffnen.
2. Greenbone-Splunk-App im linken Menüpanel wählen.
3. *Search* in der Menüleiste wählen.
4. Den Index und den Wert, nach dem gesucht werden soll, in das Eingabefeld eingeben.
5. Zeitfenster in der Drop-down-Liste rechts vom Eingabefeld wählen.
6. Auf klicken.

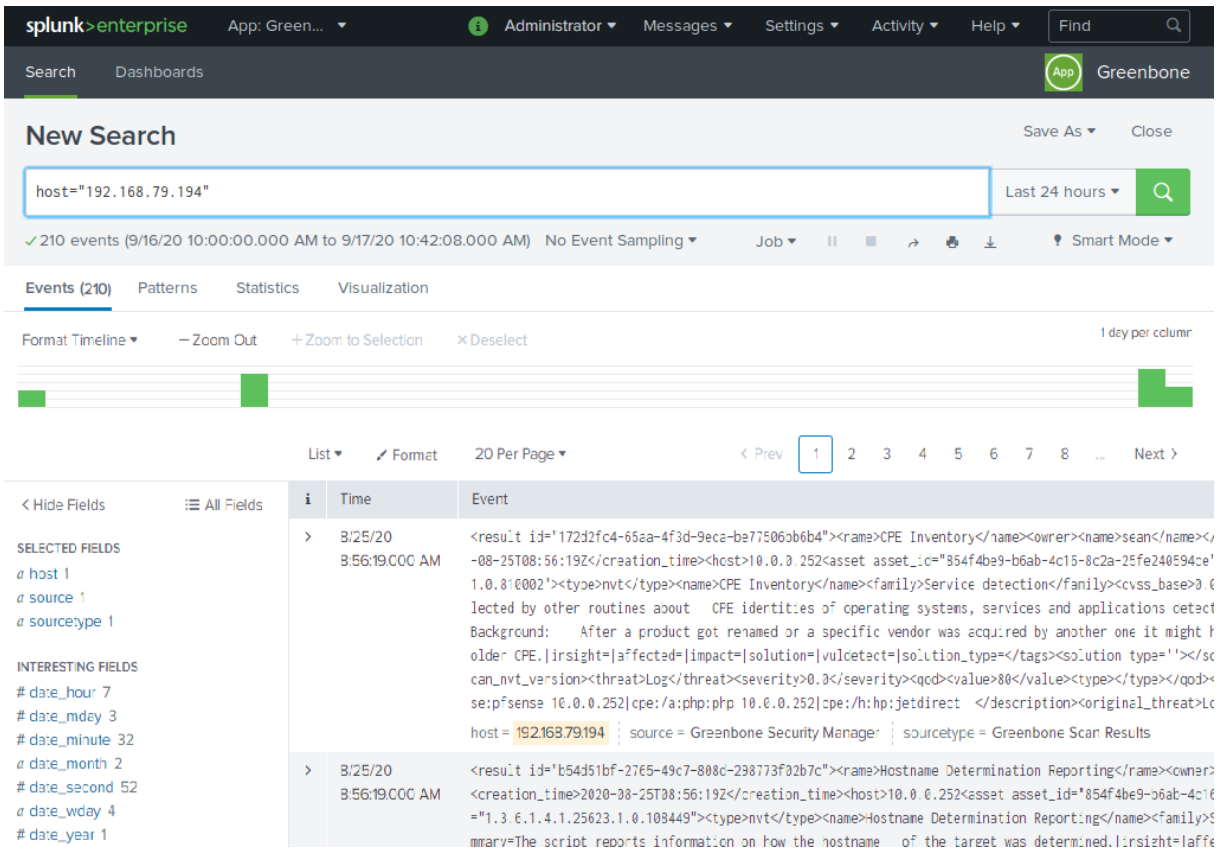


Abb. 18.20: Durchführen der Suche in der Greenbone-Splunk-App

Einige unterstützte Indizes sind:

- host
- source, sourcetype

- date_hour, date_minute, date_month, date_year, date_mdate, date_wday, date_zone
- VulnerabilityResultNvtCVE
- VulnerabilityResultNvtCVSS
- VulnerabilityResultQod
- VulnerabilityResultSeverity
- VulnerabilityResultThreat

18.5.3.3 Ein Dashboard für die 5 am stärksten betroffenen Hosts und für eingehende Berichte erstellen

Es kann ein neues Dashboard erstellt werden, das die 5 am stärksten betroffenen Hosts aller Zeiten und die eingehenden Berichte von der Appliance anzeigt. Das Dashboard zeigt für das vergangene Jahr jeden Zeitpunkt an, zu dem ein neuer Bericht auf dem Splunk-Server einging.

1. Splunk Enterprise öffnen.
2. Greenbone-Splunk-App im linken Menüpanel wählen.
3. *Dashboards* in der Menüleiste wählen.
4. Auf *Create New Dashboard* klicken.
5. Einen Titel in das Eingabefeld *Title* eingeben, z. B. `Greenbone incoming stats`.
6. Auf *Create Dashboard* klicken.
7. Auf *Source* klicken.
8. Das Folgende kopieren und in das Eingabefeld einfügen (ersetzt alles):

```
<dashboard>
  <label>Greenbone incoming stats</label>
  <row>
        <panel>
          <title>Top 5 all time</title>
          <chart>
                <search>
                  <query>sourcetype = "Greenbone Scan Results"␣
↪VulnerabilityResultSeverity &gt; 0 | chart count over VulnerabilityResultHost by␣
↪VulnerabilityResultThreat | fillnull High | fillnull Medium | fillnull Low | eval␣
↪_count= High+Low+Medium | sort by _count desc | head 5</query>
                  <earliest>0</earliest>
                  <latest></latest>
                </search>
                <option name="charting.axisLabelsX.majorLabelStyle.overflowMode">
↪ellipsisNone</option>
                <option name="charting.axisLabelsX.majorLabelStyle.rotation">0</
↪option>
                <option name="charting.axisTitleX.visibility">visible</option>
                <option name="charting.axisTitleY.visibility">visible</option>
                <option name="charting.axisTitleY2.visibility">visible</option>
                <option name="charting.axisX.scale">linear</option>
                <option name="charting.axisY.scale">linear</option>
                <option name="charting.axisY2.enabled">0</option>
                <option name="charting.axisY2.scale">inherit</option>
                <option name="charting.chart">bar</option>
                <option name="charting.chart.bubbleMaximumSize">50</option>
                <option name="charting.chart.bubbleMinimumSize">10</option>
                <option name="charting.chart.bubbleSizeBy">area</option>
                <option name="charting.chart.nullValueMode">gaps</option>
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
                <option name="charting.chart.showDataLabels">none</option>
                <option name="charting.chart.sliceCollapsingThreshold">0.01</option>
                <option name="charting.chart.stackMode">stacked</option>
                <option name="charting.chart.style">shiny</option>
                <option name="charting.drilldown">all</option>
                <option name="charting.fieldColors">{"High":0xD6563C,"Medium
↪":0xF2B827, "Low":0x1E93C6}</option>
                <option name="charting.layout.splitSeries">0</option>
                <option name="charting.layout.splitSeries.allowIndependentYRanges">0
↪</option>
                <option name="charting.legend.labelStyle.overflowMode">
↪ellipsisMiddle</option>
                <option name="charting.legend.placement">right</option>
                <option name="refresh.display">progressbar</option>
          </chart>
        </panel>
  </row>
  <row>
        <panel>
          <chart>
                <title>Incoming feed to Greenbone App</title>
                <search>
                  <query>| tstats count where sourcetype = "Greenbone Scan Results"␣
↪by sourcetype _time | timechart span=1d count by  sourcetype</query>
                  <earliest>@y</earliest>
                  <latest>now</latest>
                </search>
                <option name="charting.chart">line</option>
                <option name="refresh.display">progressbar</option>
          </chart>
        </panel>
  </row>
</dashboard>
```

9. Auf *Save* klicken.

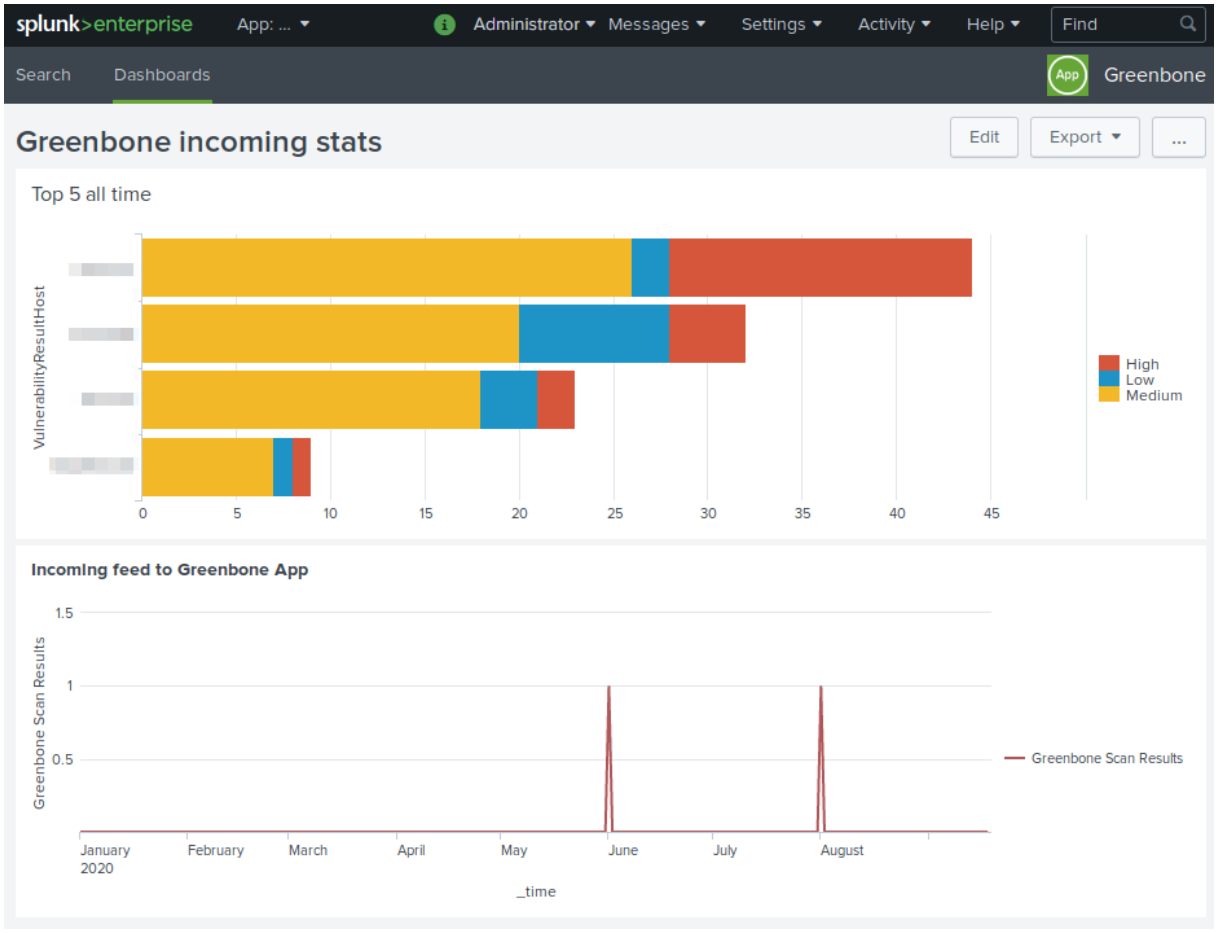


Abb. 18.21: Dashboard für die 5 am stärksten betroffenen Hosts und für eingehende Berichte

KAPITEL 19

Architektur

19.1 GOS-Architektur

Das Greenbone Operating System (GOS) ist das Betriebssystem der Greenbone Enterprise Appliance. Hier ist eine Architekturübersicht für GOS 22.04.

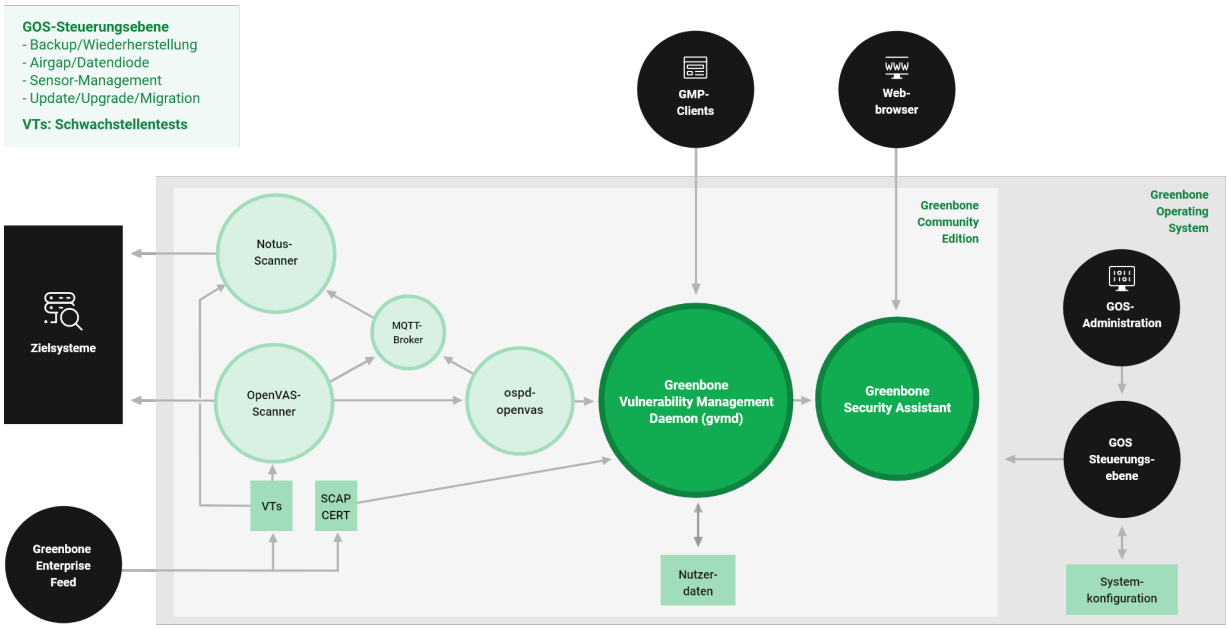


Abb. 19.1: GOS-22.04-Architektur

Die GOS-Steuerungsebene ermöglicht den Zugriff auf die Administration des Greenbone Operating Systems (GOS). Nur ein einziger Systemadministrator wird unterstützt. Der Systemadministrator kann Systemdateien nicht direkt verändern, aber das System anweisen, Konfigurationen zu ändern.

GOS wird über eine menübasierte, grafische Oberfläche (GOS-Administrationsmenü) verwaltet. Der Systemadministrator muss nicht zwingend die Befehlszeile (Shell) für Konfigurations- oder Wartungsaufgaben nutzen. Zugriff auf die Shell ist nur für den Support und für die Problemlösung vorgesehen.

Für den Zugriff auf die Systemebene wird entweder ein Konsolenzugriff (seriell, Hypervisor oder Monitor/Tastatur) oder eine SSH-Verbindung benötigt.

Mit GOS können Nutzer alle Dienste der Greenbone Community Edition konfigurieren, starten und stoppen.

Greenbone Community Edition

Die Greenbone Community Edition besteht aus einem Framework mit verschiedenen Diensten. Sie wird als Teil der Greenbone-Enterprise-Produkte entwickelt.

Die Greenbone Community Edition wurde ursprünglich als Community-Projekt mit dem Namen „OpenVAS“ entwickelt und hauptsächlich von Greenbone weiterentwickelt. Sie besteht aus dem Greenbone Vulnerability Management Daemon (gvmd), dem Greenbone Security Assistant (GSA) mit dem Greenbone Security Assistant Daemon (gsad) und der ausführbaren Scan-Anwendung, die Schwachstellentests (VT) gegen Zielsysteme ausführt.

Die Greenbone Community Edition wird unter Open-Source-Lizenzen veröffentlicht. Mit ihrer Hilfe können Linux-Distributionen die Softwarekomponenten in Form von Installationspaketen erstellen und bereitstellen.

Greenbone Vulnerability Management Daemon (gvmd)

Der Greenbone Vulnerability Management Daemon (gvmd)[79] – auch Greenbone Vulnerability Manager genannt – ist der zentrale Dienst, der einfache Schwachstellenscans zu einer vollständigen Schwachstellenmanagement-Lösung zusammenführt. gvmd steuert den OpenVAS-Scanner über das Open Scanner Protocol (OSP)[80]. Es ist XML-basiert, zustandslos und benötigt keine dauerhafte Kommunikationsverbindung.

Der Dienst selbst stellt das XML-basierte Greenbone Management Protocol (GMP)[81] zur Verfügung. gvmd steuert außerdem eine SQL-Datenbank (PostgreSQL), in der alle Konfigurations- und Scanergebnisdaten zentral gespeichert werden. Darüber hinaus übernimmt gvmd auch die Benutzerverwaltung inklusive der Berechtigungssteuerung mit Gruppen und Rollen. Außerdem verfügt der Dienst über ein internes Laufzeitsystem für geplante Aufgaben und andere Ereignisse.

Greenbone Security Assistant (GSA)

Der Greenbone Security Assistant (GSA)[82] ist die Web-Oberfläche, mit der ein Nutzer Scans steuert und auf Schwachstelleninformationen zugreift. Es ist der Hauptkontaktpunkt für einen Nutzer mit der Appliance. Er verbindet sich über den Webserver Greenbone Security Assistant Daemon (gsad) mit gvmd, um eine voll funktionsfähige Webanwendung für das Schwachstellenmanagement bereitzustellen. Die Kommunikation erfolgt über das Greenbone Management Protocol (GMP), mit dem der Nutzer auch direkt über verschiedene Tools kommunizieren kann.

OpenVAS Scanner

Der Hauptscanner OpenVAS-Scanner[83] ist eine voll funktionsfähige Scan-Maschine, die Schwachstellentests (VTs) gegen Zielsysteme ausführt. Dazu nutzt er die täglich aktualisierten und umfangreichen Feeds: den vollumfänglichen, ausführlichen, kommerziellen Greenbone Enterprise Feed oder den frei verfügbaren Greenbone Community Feed[84].

Der Scanner besteht aus den Komponenten ospd-openvas[85] und openvas-scanner[86]. Der OpenVAS-Scanner wird über OSP gesteuert. Der OSP-Daemon für den OpenVAS-Scanner (ospd-openvas) kommuniziert über

[79] https://github.com/greenbone/gvmd
[80] https://docs.greenbone.net/API/OSP/osp-22.4.html
[81] https://docs.greenbone.net/API/GMP/gmp-22.4.html
[82] https://github.com/greenbone/gsa
[83] https://github.com/greenbone/openvas-scanner
[84] https://www.greenbone.net/feedvergleich/
[85] https://github.com/greenbone/ospd-openvas
[86] https://github.com/greenbone/openvas-scanner

OSP mit gvmd: VT-Daten werden gesammelt, Scans werden gestartet und gestoppt und Scan-Ergebnisse werden über ospd an gvmd übertragen.

Notus-Scanner

Der Notus-Scanner scannt bei jedem regulären Scanvorgang, sodass keine Nutzerinteraktion erforderlich ist. Er bietet eine bessere Leistung, da er weniger Systemressourcen verbraucht und somit schneller scannt.

Der Notus-Scanner ersetzt die Logik potenziell aller NASL-basierten lokalen Sicherheitskontrollen (engl. local security checks, LSCs). Statt für jeden LSC ein VT-Skript auszuführen, wird ein Vergleich der auf einem Host installierten Software mit einer Liste bekannter anfälliger Software durchgeführt.

Der reguläre OpenVAS-Scanner lädt jeden NASL-LSC einzeln und führt ihn nacheinander für jeden Host aus. Eine einzelne bekannte Schwachstelle wird dann mit der installierten Software verglichen. Dies wird für alle LSCs wiederholt.

Mit dem Notus-Scanner wird die Liste der installierten Software auf die gleiche Weise geladen, aber direkt mit der gesamten bekannten anfälligen Software für das Betriebssystem des gescannten Hosts verglichen. Dadurch entfällt die Notwendigkeit, die LSCs auszuführen, da die Informationen über die bekannte anfällige Software in einer einzigen Liste gesammelt und nicht in einzelnen NASL-Skripten verteilt werden.

GMP Clients

Die Greenbone Vulnerability Management Tools (gvm-tools)[87] sind eine Sammlung von Werkzeugen, die bei der Fernsteuerung einer Greenbone Enterprise Appliance und des zugrundeliegenden Greenbone Vulnerability Management Daemons (gvmd) helfen. Die Tools helfen beim Zugriff auf die Kommunikationsprotokolle GMP (Greenbone Management Protocol) und OSP (Open Scanner Protocol).

Dieses Modul besteht aus interaktiven und nicht interaktiven Clients. Die Programmiersprache Python wird direkt für die interaktive Skripterstellung unterstützt. Es ist aber auch möglich, Remote-GMP-/Remote-OSP-Befehle ohne Programmierung in Python zu erteilen.

[87] https://github.com/greenbone/gvm-tools

19.2 Protokolle

Es gibt obligatorische und optionale Protokolle. Einige Protokolle werden nur in bestimmten Setups genutzt.

Die Appliance benötigt einige Protokolle um voll funktionsfähig zu sein. Diese Protokolle stellen Feed-Updates, die Domain-Name-System-Auflösung (DNS-Auflösung), die Zeit etc. bereit.

19.2.1 Appliance als Client

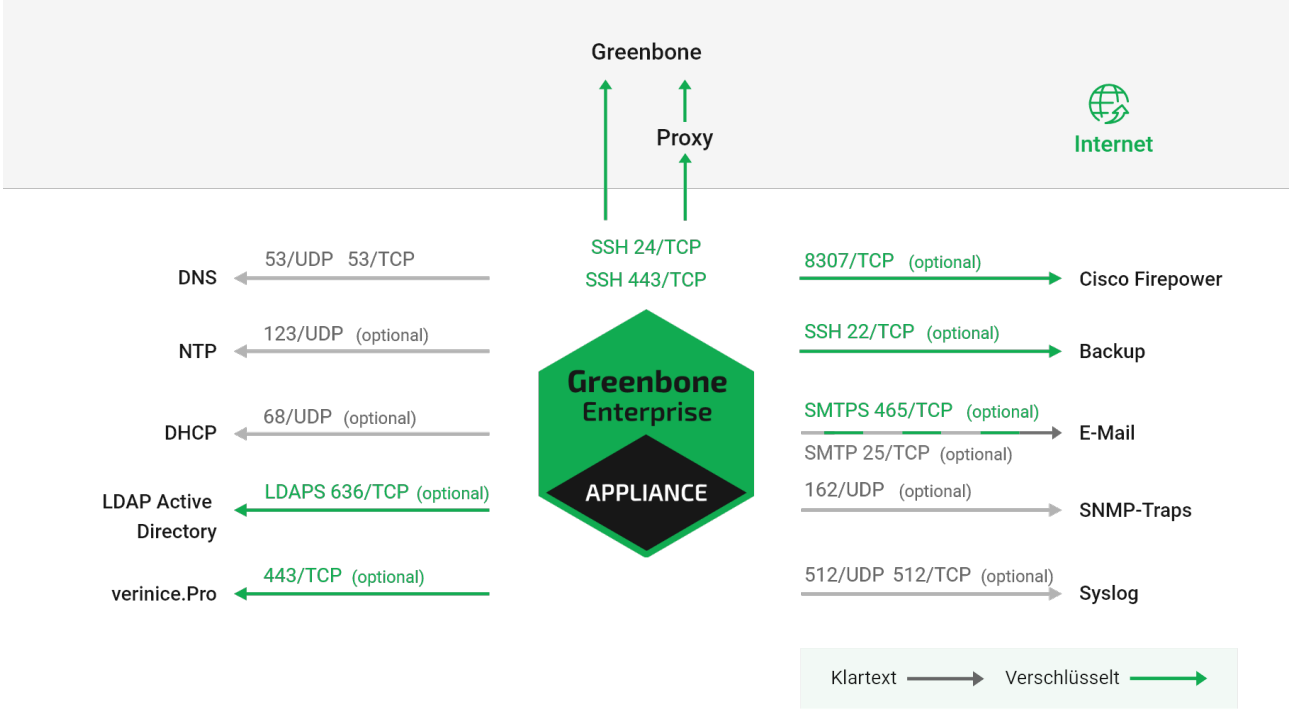


Abb. 19.2: Appliance handelt als Client

Die folgenden Protokolle werden von eigenständigen Systemen oder einer Master-Appliance genutzt, um Verbindungen als Client zu initiieren:

DNS – Namensauflösung

- Verbindet zu 53/udp und 53/tcp
- Obligatorisch
- Nicht verschlüsselt
- Kann interne DNS-Server nutzen

NTP – Zeitsynchronisierung

- Verbindet zu 123/udp
- Obligatorisch
- Nicht verschlüsselt
- Kann interne NTP-Server nutzen

Feeds (siehe unten)

- Direkt
  - Verbindet zu 24/tcp oder 443/tcp
  - Direkter Internetzugang erforderlich
- Über Proxy
  - Verbindet zu internem HTTP-Proxy, der CONNECT-Methode auf konfigurierbarem Port unterstützt
- Verbindet zu apt.greenbone.net und feed.greenbone.net
- Obligatorisch auf eigenständigen und Master-Appliances
- Genutztes Protokoll ist SSH
- Verschlüsselt und in beide Richtungen authentifiziert über SSH
  - Server: öffentlicher Schlüssel
  - Client: öffentlicher Schlüssel

DHCP

- Verbindet zu 67/udp und 68/udp
- Optional
- Nicht verschlüsselt

LDAPS – Benutzerauthentifizierung

- Verbindet zu 636/tcp
- Optional
- Verschlüsselt und authentifiziert über SSL/TLS
  - Server: Zertifikat
  - Client: Benutzername/Passwort

Syslog – Remote-Protokollierung und -Benachrichtigungen

- Verbindet zu 512/udp oder 512/tcp
- Optional
- Nicht verschlüsselt

SNMP-Traps für Benachrichtigungen

- Verbindet zu 162/udp
- Optional
- Nur SNMPv1
- Nicht verschlüsselt

SMTP(S) für E-Mail-Benachrichtigungen

- Verbindet zu 465/tcp für SMTPS, zu 25/tcp für SMTP, verbindet alternativ zu 587/tcp
- Optional
- SMTPS kann erzwungen werden, damit es immer verwendet wird
- Verschlüsselt über STARTTLS, falls SMTPS nicht erzwungen wird
- Nicht verschlüsselt, falls Verschlüsselung über STARTTLS nicht möglich ist

SSH für Backups

- Verbindet zu 22/tcp
- Optional
- Verschlüsselt und in beide Richtungen authentifiziert über SSH
  - Server: öffentlicher Schlüssel
  - Client: öffentlicher Schlüssel

Cisco Firepower (Sourcefire) für IPS-Integration

- Verbindet zu 8307/tcp
- Optional
- Verschlüsselt und in beide Richtungen authentifiziert über SSL/TLS
  - Server: Zertifikat
  - Client: Zertifikat

verinice.PRO

- Verbindet zu 443/tcp
- Optional
- Verschlüsselt über SSL/TLS
  - Server: optional über Zertifikat
  - Client: Benutzername/Passwort

TippingPoint SMS

- Verbindet zu 443/tcp
- Optional
- Verschlüsselt über SSL/TLS
  - Server: Zertifikat
  - Client: Zertifikat, Benutzername/Passwort

19.2.2 Appliance als Server

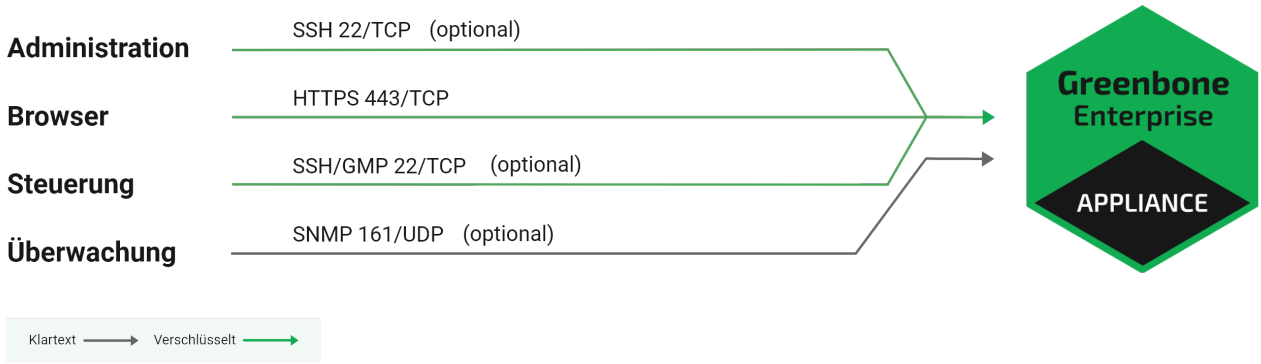


Abb. 19.3: Appliance handelt als Server

Die folgenden Verbindungen werden von einer Appliance, die als Server agiert, genutzt:

HTTPS – Web-Oberfläche

- 443/tcp
- Obligatorisch auf eigenständigen und Master-Appliances
- Verschlüsselt und authentifiziert über SSL/TLS
  - Server: optional über Zertifikat
  - Client: Benutzername/Passwort

SSH – CLI-Zugang und GMP

- 22/tcp
- Optional
- Verschlüsselt und authentifiziert über SSH
  - Server: öffentlicher Schlüssel
  - Client: Benutzername/Passwort

SNMP

- 161/udp
- Optional
- Optional verschlüsselt, falls SNMPv3 genutzt wird

19.2.3 Master-Sensor-Setup

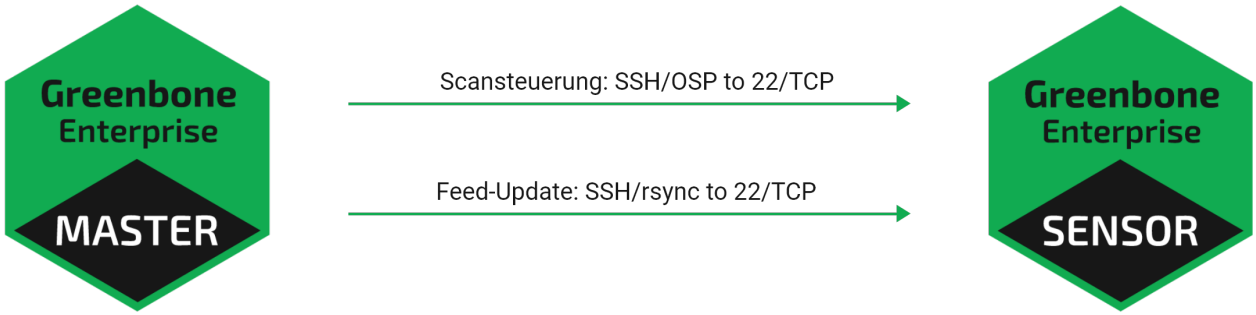


Abb. 19.4: Appliance-Master und -Sensor

In einem Master-Sensor-Setup gelten die folgenden zusätzlichen Anforderungen. Der Master (Server) veranlasst bis zu drei zusätzliche Verbindungen zum Sensor (Client):

SSH für GOS-Upgrades, Feed-Updates, GMP und OSP

- 22/tcp
- Obligatorisch
- Verschlüsselt und in beide Richtungen authentifiziert über SSH
  - Server: öffentlicher Schlüssel
  - Client: öffentlicher Schlüssel

19.3 Hinweise zur Nutzung eines Sicherheitsgateways

Viele Unternehmen setzen Sicherheitsgateways ein, um den Internetzugang zu beschränken. Diese Sicherheitsgateways können als Paketfilter oder Gateways auf der Anwendungsebene wirken.

Einige Produkte unterstützen tiefgreifende Untersuchungen und versuchen das tatsächlich in den Kommunikationskanälen genutzte Protokoll zu bestimmen. Sie versuchen möglicherweise sogar, jede verschlüsselte Kommunikation zu entschlüsseln und zu analysieren.

19.3.1 Eigenständige oder Master-Appliance

Während viele Kommunikationsprotokolle, die die Appliance unterstützt, nur intern verwendet werden, benötigen manche Protokolle Zugang zum Internet. Diese Protokolle können möglicherweise durch solche Sicherheitsgateways gefiltert werden.

Beim Einsetzen einer Appliance als eigenständige Appliance oder als Master, muss die Appliance in der Lage sein, auf den Greenbone Enterprise Feed zuzugreifen. Der Greenbone Enterprise Feed kann direkt über die Ports 24/tcp oder 443/tcp oder durch Nutzung eines Proxys erreicht werden.

Bemerkung: In allen Fällen ist das genutzte Protokoll SSH, auch wenn der Port 443/tcp oder ein HTTP-Proxy genutzt wird.

Eine Deep-Inspection-Firewall könnte die Nutzung des SSH-Protokolls auf Port 443/tcp entdecken und den Verkehrt abbrechen oder blockieren.

Falls das Sicherheitsgateway versucht, den Verkehr mithilfe von Man-in-the-Middle-Techniken zu entschlüsseln, fällt die Kommunikation zwischen der Appliance und dem Feedserver aus. Das SSH-Protokoll, das eine doppeltgerichtete Authentifizierung basierend auf öffentlichen Schlüsseln nutzt, verhindert jeden Man-in-the-Middle-Angriff, indem es die Kommunikation beendet.

Zusätzliche Protokolle, die Internetzugang benötigen, sind DNS und NTP. Sowohl DNS als auch NTP können für die Nutzung von internen DNS- und NTP-Servern konfiguriert werden.

19.3.2 Sensor-Appliance

Falls Sicherheitsgateways zwischen dem Master und dem Sensor eingesetzt werden, muss das Sicherheitsgateway SSH-Verbindungen (22/tcp) vom Master zum Sensor erlauben.

KAPITEL 20

Häufig gestellte Fragen

20.1 Warum ist der Scanprozess so langsam?

Die Geschwindigkeit eines Scans hängt von vielen Faktoren ab.

- Es wurden mehrere Portscanner gleichzeitig aktiviert.

  Falls eine individuelle Scan-Konfiguration genutzt wird, sollte nur ein einziger Portscanner in der VT-Familie *Port scanners* gewählt werden (siehe Kapitel *10.9.2* (Seite 263)). Der VT *Ping Host* kann trotzdem aktiviert sein.

- Unbelegte IP-Adressen werden zeitintensiv gescannt.

  Im ersten Schritt wird festgestellt, ob für jede IP-Adresse ein aktives System vorhanden ist oder nicht. Falls nicht, wird die IP-Adresse nicht gescannt. Firewalls und andere Systeme können solch eine erfolgreiche Feststellung verhindern. Der VT *Ping Host* (1.3.6.1.4.1.25623.1.0.100315) in der VT-Familie *Port scanners* bietet eine Feineinstellung der Feststellung.

- Die zu scannenden Ports führten zu einer Portdrosselung oder es wurde UDP-Port-Scanning gewählt.

  Weitere Informationen befinden sich in Kapitel *17.2.1.2* (Seite 391) und *17.2.1.2.1* (Seite 391).

20.2 Wodurch wird die Scankapazität beeinflusst?

Die Scankapazität – die scannbare Anzahl an IP-Adressen pro 24 Stunden – hängt vom Appliance-Modell ab (siehe Kapitel *3* (Seite 20)). Die angegebenen Werte für die geschätzte Scankapazität können jedoch nur als Richtwerte verstanden werden, da die Scankapazität von vielen Faktoren beeinflusst wird.

Die folgenden Faktoren beeinflussen die Scankapazität:

- **Komplexität der verwendeten Scan-Konfiguration** In derselben Zeitspanne können viel mehr Discoveryscans als Schwachstellenscans ausgeführt werden. Weitere Informationen zu den Scan-Konfigurationen befinden sich in Kapitel *10.9* (Seite 261).
- **Verwendung der Appliance außerhalb ihrer Spezifikationen** Das Starten zu vieler Scans oder das gleichzeitige Scannen zu vieler Ziele kann zu Leistungsproblemen führen.

- **Leistung der Netzwerk-Infrastruktur und des/der Zielsysteme(s)** Wenn die Systeme nur langsam auf Netzwerkanfragen reagieren, wird der Scanvorgang langsamer.
- **Art des gescannten Zielsystems/der gescannten Zielsysteme** Die Art bestimmt, welche und wie viele Schwachstellentests während eines Scans ausgeführt werden. Mehr Schwachstellentests bedeuten in der Regel langsamere Scans.

  Einige Scanszenarien erhöhen die Ressourcennutzung, was sich auf die Leistung auswirken kann, z. B. das Scannen von virtuellen Hosts (vHosts) oder das Scannen von Webservern mit aktiviertem CGI-Caching. Weitere Informationen zu den Konfigurationsoptionen für diese Szenarien befinden sich in Kapitel *10.9* (Seite 261).
- **Parallele Verwendung der Appliance während des Scannens** Wenn andere ressourcenintensive Vorgänge (z. B. Feed-Updates, Erstellung großer Berichte) laufen, stehen weniger Systemressourcen für Scans zur Verfügung.
- **Verwendung von Sensoren** Die Verwendung von Sensoren kann die Anzahl der scannbaren IP-Adressen pro 24 Stunden erhöhen.

20.3 Warum wird ein Dienst/Produkt nicht gefunden?

- Das Ziel wird nicht als online/erreichbar erkannt.

  Lösung(en):

  - Netzwerkeinrichtung/Routing zum Ziel korrigieren.
  - Die Kriterien/die Testkonfiguration, um das Ziel als erreichbar zu erkennen, aktualisieren (siehe Kapitel *10.2.1* (Seite 214)).
  - Sicherstellen, dass die Scan-Konfiguration die folgenden VTs aus der VT-Familie *Port scanners* enthält:
    - *Nmap (NASL wrapper)* (OID: 1.3.6.1.4.1.25623.1.0.14259)
    - *Ping Host* (OID: 1.3.6.1.4.1.25623.1.0.100315)
  - Alle Netzwerkgeräte (Firewall, IDS/IPS, WAF usw.) zwischen dem Scanner und dem Ziel sowie alle Sicherheitsmechanismen auf dem Ziel selbst überprüfen und entfernen. IP-Adresse des Scanners auf die Whitelist setzen.
- Der Dienst/das Produkt läuft auf einem bestimmten Port, der nicht in der Portliste enthalten ist.

  Lösung(en):

  - Eine geeignete Portliste erstellen (siehe Kapitel *10.7* (Seite 255)). Dies ist besonders wichtig für UDP-Ports.
- Es gibt einen Erkennungs-VT für einen Dienst/ein Produkt, aber der Dienst/das Produkt wird bei einem Scan nicht gefunden.

  Lösung(en):

  - Netzwerkeinrichtung/Routing zum Ziel korrigieren.
  - Die Kriterien/die Testkonfiguration, um das Ziel als erreichbar zu erkennen, aktualisieren (siehe Kapitel *10.2.1* (Seite 214)).
  - Alle Netzwerkgeräte (Firewall, IDS/IPS, WAF usw.) zwischen dem Scanner und dem Ziel sowie alle Sicherheitsmechanismen auf dem Ziel selbst überprüfen und entfernen. IP-Adresse des Scanners auf die Whitelist setzen.
  - Eine geeignete Portliste erstellen (siehe Kapitel *10.7* (Seite 255)). Dies ist besonders wichtig für UDP-Ports.

  - Wenn die oben genannten Lösungen nicht helfen, kann der Greenbone Enterprise Support[88] kontaktiert werden. Dafür weitere Informationen über den Dienst/das Produkt (Produktname, konkret laufende Version usw.) bereitstellen.

- Das Ziel ist nicht stabil/reagiert langsam während eines Scans.

  Lösung(en):

  - Gleichzeitig ausgeführte VTs reduzieren (siehe Kapitel *10.2.2* (Seite 218)).
  - Den Dienst/das Produkt auf eine neuere Version aktualisieren (z. B. um ausgelöste Bugs zu beheben).
  - Dem Ziel mehr Ressourcen (CPU, RAM usw.) zuweisen, um es bei Scans stabiler zu machen.

20.4 Warum wird eine Schwachstelle nicht gefunden?

- Der betroffene Dienst/das betroffene Produkt wird überhaupt nicht erkannt.

  Lösung(en):

  - Siehe Kapitel *20.3* (Seite 428).

- Der Dienst/das Produkt wurde erkannt, aber die Erkennung einer Version war nicht möglich.

  Lösung(en):

  - Einen authentifizierten Scan durchführen (siehe Kapitel *10.3* (Seite 220)).
  - Wenn die oben genannten Lösungen nicht helfen, kann der Greenbone Enterprise Support[89] kontaktiert werden. Dafür weitere Informationen über den Dienst/das Produkt (Produktname, konkret laufende Version usw.) bereitstellen.

- Es gibt nur eine Versionsprüfung mit einer niedrigeren Qualität der Erkennung (QdE) und die Schwachstelle wird standardmäßig nicht angezeigt.

  Lösung(en):

  - QdE-Wert im Ergebnisfilter ändern (siehe Kapitel *11.2.1.3* (Seite 297)).
  - Einen authentifizierten Scan durchführen (siehe Kapitel *10.3* (Seite 220)).

- Falls ein authentifizierter Scan durchgeführt wurde, ist der Login fehlgeschlagen.

  Lösung(en):

  - Korrektheit der Anmeldedaten prüfen.
  - Verifizieren, dass der Nutzer nicht geblockt ist.
  - Verifizieren, dass sich der Benutzer auf dem Ziel anmelden darf.
  - Wenn die oben genannten Lösungen nicht helfen, kann der Greenbone Enterprise Support[90] kontaktiert werden. Dafür weitere Informationen über den Dienst/das Produkt (Produktname, konkret laufende Version usw.) bereitstellen.

[88] https://www.greenbone.net/technischer-support/
[89] https://www.greenbone.net/technischer-support/
[90] https://www.greenbone.net/technischer-support/

- Der Dienst/das Produkt selbst stürzte ab oder reagierte nicht mehr während des Scans.

  Lösung(en):

  - Gleichzeitig ausgeführte VTs reduzieren (siehe Kapitel *10.2.2* (Seite 218)).
  - Den Dienst/das Produkt auf eine neuere Version aktualisieren (z. B. um ausgelöste Bugs zu beheben).
  - Dem Ziel mehr Ressourcen (CPU, RAM usw.) zuweisen, um es bei Scans stabiler zu machen.

- Die Schwachstelle wurde erst vor Kurzem entdeckt und es existiert noch kein VT dafür.

  Lösung(en):

  - Den Greenbone Enterprise Support[91] kontaktieren und einen neuen VT anfragen oder erfragen, ob ein VT bereits geplant ist.

- Die spezifische Erkennung ist veraltet.

  Lösung(en):

  - Den Greenbone Enterprise Support[92] kontaktieren.

20.5 Warum unterscheiden sich die Ergebnisse für dasselbe Ziel bei mehreren aufeinanderfolgenden Scans?

Die Ergebnisse aufeinanderfolgender Scans können aus folgenden Gründen voneinander abweichen:

- Es gab einen Verbindungsverlust über unzuverlässige Netzwerkverbindungen (zwischen dem Scanner-Host und dem Ziel).
- Die Netzwerkverbindung oder die Ausrüstung (zwischen dem Scanner-Host und dem Ziel) war überlastet.
- Ein überlasteter Zielhost und/oder -dienst hat aufgehört zu reagieren.
- „Fragile“ Protokolle (z. B. das Remote Desktop Protocol) reagieren nicht immer wie erwartet.
- Eine frühere Prüf-/Angriffsanfrage hat dazu geführt, dass der Dienst für eine kurze Zeit nicht reagiert hat.

Obwohl der Scanner versucht, das Auftreten solcher Situationen durch interne Wiederholungsroutinen zu reduzieren, können sie nicht vollständig ausgeschlossen werden.

20.6 Warum ist es nicht möglich, Scan-Konfigurationen, Portlisten, Compliance-Richtlinien oder Berichtformate zu bearbeiten?

Scan-Konfigurationen, Portlisten, Compliance-Richtlinien und Berichtformate von Greenbone (im Folgenden als „Objekte“ bezeichnet) werden über den Feed verteilt. Diese Objekte müssen einem Nutzer, dem Feed Import Owner, gehören. Die Objekte werden während eines Feed-Updates heruntergeladen und aktualisiert, falls ein Feed Import Owner festgelegt wurde.

Die Objekte können nicht bearbeitet werden. Dies ist beabsichtigt, damit sichergestellt ist, dass die Objekte wie von Greenbone beabsichtigt funktionieren.

[91] https://www.greenbone.net/technischer-support/
[92] https://www.greenbone.net/technischer-support/

20.7 Warum ist es nicht möglich, Scan-Konfigurationen, Portlisten, Compliance-Richtlinien oder Berichtformate zu löschen?

Scan-Konfigurationen, Portlisten, Compliance-Richtlinien und Berichtformate von Greenbone (im Folgenden als „Objekte“ bezeichnet) werden über den Feed verteilt. Diese Objekte müssen einem Nutzer, dem Feed Import Owner, gehören. Die Objekte werden während eines Feed-Updates heruntergeladen und aktualisiert, falls ein Feed Import Owner festgelegt wurde.

Nur der Feed Import Owner, ein Super-Administrator oder Nutzer, die entsprechende Berechtigungen erhalten haben, können Objekte löschen.

Wenn die Objekte gelöscht werden, werden sie während des nächsten Feed-Updates erneut heruntergeladen. Falls keine Objekte heruntergeladen werden sollen, darf kein Feed Import Owner festgelegt sein.

20.8 Warum erscheint ein VNC-Dialog auf dem gescannten Zielsystem?

Beim Prüfen des Ports 5900 oder beim Konfigurieren eines VNC-Ports, erscheint ein Fenster zum Erlauben der Verbindung auf dem gescannten System. Dies wurde für UltraVNC Version 1.0.2 beobachtet.

Lösung: Port 5900 oder andere konfigurierte VNC-Ports von der Zielspezifikation ausschließen. Alternativ könnte ein Upgrade auf eine neuere Version von UltraVNC hilfreich sein (UltraVNC 1.0.9.6.1 nutzt lediglich Sprechblasen zum Informieren von Benutzern).

20.9 Wie kann ein Factory-Reset auf der Appliance durchgeführt werden?

Ein Factory-Reset kann durchgeführt werden, um Benutzerdaten sicher von der Appliance zu entfernen.

Bemerkung: Der Greenbone Enterprise Support[93] kann kontaktiert werden, um detaillierte Informationen zum Factory-Reset zu erhalten.

20.10 Warum funktionieren nach einem Factory-Reset weder Feed-Update noch GOS-Upgrade?

Der Factory-Reset löscht das gesamte System, einschließlich des Subskription-Schlüssels für den Greenbone Enterprise Feed. Der Subskription-Schlüssel ist für Feed-Updates und GOS-Upgrades zwingend erforderlich.

1. Den Subskription-Schlüssel reaktivieren:

   Ein Backup-Schlüssel wird mit jeder Appliance geliefert (siehe Kapitel *7.1.1* (Seite 65)). Dieser Schlüssel kann genutzt werden, um die Appliance zu reaktivieren. Die Aktivierung ist im Setup-Guide des entsprechenden Appliance-Modells beschrieben (siehe Kapitel *5* (Seite 28)).

2. Das System auf die aktuelle Version aktualisieren:

   Abhängig von der GOS-Version muss der entsprechende Upgradevorgang durchgeführt werden.

[93] https://www.greenbone.net/technischer-support/

20.11 Warum löst der Scan Alarme bei anderen Sicherheitstools aus?

Bei vielen Schwachstellenprüfungen wird das Verhalten eines echten Angriffs simuliert. Zwar findet kein tatsächlicher Angriff statt, aber einige Sicherheitstools könnten einen Alarm ausgeben.

Ein bekanntes Beispiel ist:

Symantec meldet einen Angriff bezüglich CVE-2009-3103, falls der VT *Microsoft Windows SMB2 ‚_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability* (1.3.6.1.4.1.25623.1.0.100283) ausgeführt wird. Dieser VT wird nur ausgeführt, falls der Radiobutton *Nein* für *safe_checks* in den Scanner-Vorgaben gewählt wird (siehe Abb. 20.1). Andernfalls kann das Zielsystem betroffen sein.

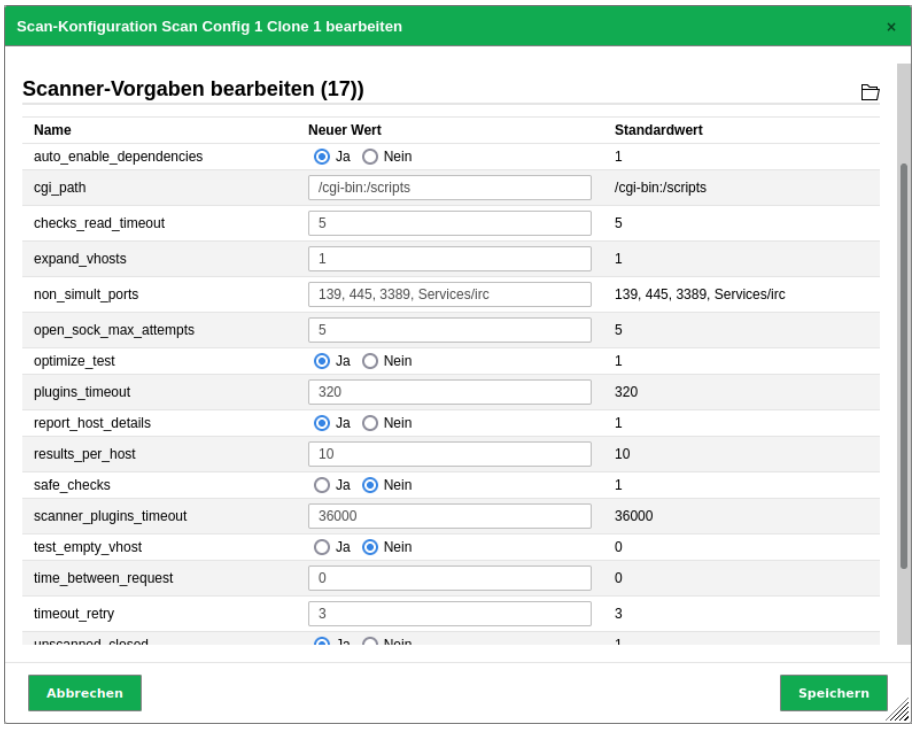


Abb. 20.1: Deaktivieren der Scanner-Vorgabe *safe_checks*

20.12 Wie kann ein älteres Backup oder Beaming-Image wiederhergestellt werden?

Ausschließlich Backups und Beaming-Images, die mit der momentan genutzten GOS-Version oder der Vorgängerversion erstellt wurden, können wiederhergestellt werden. Für GOS 22.04 können nur Backups und Beaming-Images aus GOS 21.04 oder GOS 22.04 importiert werden. Falls ein älteres Backup oder Beaming-Image importiert werden soll, z. B. aus GOS 6 oder GOS 20.08, muss eine Appliance mit der passenden GOS-Version genutzt werden.

Backups und Beaming-Images aus GOS-Versionen, die neuer sind als die momentan genutzte GOS-Version, werden ebenfalls nicht unterstützt. Falls ein neueres Backup oder Beaming-Image importiert werden soll, muss eine Appliance mit der passenden GOS-Version genutzt werden.

Falls Fragen auftreten, kann der Greenbone Enterprise Support[94] kontaktiert werden.

[94] https://www.greenbone.net/technischer-support/

20.13 Was kann getan werden, falls das GOS-Administrationsmenü nicht korrekt in PuTTY dargestellt wird?

Window > Translation im linken Panel wählen, um die Einstellungen in PuTTY zu prüfen. *UTF-8* muss in der Drop-down-Liste *Remote character set* gewählt werden (siehe Abb. 20.2).

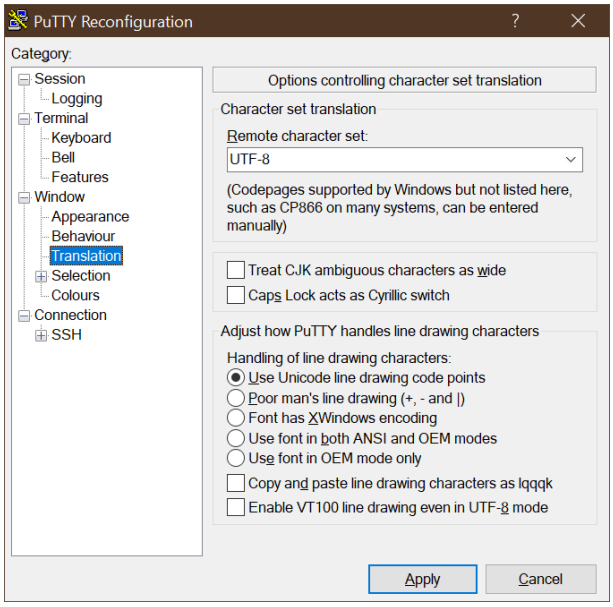


Abb. 20.2: Auswahl des Remotezeichensatzes

20.14 Wie kann der GMP-Status ohne Anmeldedaten geprüft werden?

1. Eine SSH-Verbindung zur Appliance mithilfe der Kommandozeile unter Nutzung des GMP-Benutzers aufbauen:

```
ssh gmp@<appliance>
```

   `<appliance>` durch die IP-Adresse oder den DNS-Namen der Appliance ersetzen.

   Bemerkung: Es wird keine Eingabeaufforderung angezeigt, aber der Befehl kann trotzdem eingegeben werden.

2. `<get_version/>` eingeben.

   → Falls GMP aktiviert ist, sollte die Ausgabe wie folgt aussehen: `<get_version_response status="200" status_text="OK"><version>8.0</version></get_version_response>`.

20.15 Was ist zu tun, wenn der Self-Check „RAID Array degraded“ anzeigt?

Die Appliance-Modelle Greenbone Enterprise 6500/6400/5400/5300 verwenden RAID (Redundant Array of Independent Disks) 6 als Software-RAID. RAID ist eine Technologie zur Datenspeichervirtualisierung, bei der mehrere Festplattenkomponenten zum Zwecke der Datenredundanz zu einer oder mehreren logischen Einheiten zusammengefasst werden. Für RAID 6 sind mindestens 4 Festplatten erforderlich, damit das RAID und damit die Datenredundanz funktioniert. Die Appliance selbst funktioniert noch, wenn bis zu 2 Festplatten ausfallen.

Falls eine oder mehrere Festplatte(n) ausfallen, zeigt GOS die Self-Check-Warnungen `RAID Array degraded` mit dem Hinweis `Replace the failed disk` und `Check for system integrity status` mit dem Hinweis `The system integrity may be endangered. Please contact the support.` an. Die Integritätsprüfung schlägt aufgrund der ausgefallenen Festplatte(n) fehl.

Ausgefallene Festplatten müssen ersetzt und das RAID muss repariert werden. Der Greenbone Enterprise Support[95] bietet hierzu Unterstützung an.

[95] https://www.greenbone.net/technischer-support/

KAPITEL 21

Glossar

Dieser Abschnitt definiert relevante Begriffe die immer wieder im gesamten System verwendet werden.

21.1 Benachrichtigung

Eine Benachrichtigung ist eine Aktion, die durch bestimmte Ereignisse ausgelöst werden kann. In den meisten Fällen bedeutet dies die Ausgabe einer Mitteilung, z. B. eine E-Mail bei neu gefundenen Schwachstellen.

21.2 Asset

Assets werden während eines Schwachstellenscans im Netzwerk entdeckt oder manuell vom Benutzer eingegeben. Aktuell enthalten Assets Hosts und Betriebssysteme.

21.3 CERT-Bund-Advisory

Ein Advisory, das vom CERT-Bund herausgegeben wird. Siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html für weitere Informationen.

21.4 Compliance-Audit

Ein Compliance-Audit ist eine Scanaufgabe mit der Kennzeichnung *Audit*. Es wird genutzt, um die Erfüllung von Compliances zu prüfen.

21.5 Compliance-Richtlinie

Eine Compliance-Richtlinie ist eine Scan-Konfiguration mit der Kennzeichnung *Richtlinie*. Sie wird genutzt, um die Erfüllung von Compliances zu prüfen.

21.6 CPE

Common Platform Enumeration (CPE) ist ein strukturiertes Benennungsschema für Systeme, Plattformen und Pakete der Informationstechnologie (IT). Basierend auf der allgemeinen Syntax für Uniform Resource Identifiers (URI), enthält CPE ein formales Namensformat, eine Sprache zum Beschreiben komplexer Plattformen, eine Methode zum Vergleichen von Namen mit einem System und ein Beschreibungsformat, um Texte und Tests an einen Namen zu binden.

Ein CPE-Name beginnt mit „cpe:/“, gefolgt von bis zu sieben Komponenten, die durch Doppelpunkte getrennt sind:

- Part („h“ für Hardware, „o“ für Betriebssystem oder „a“ für Anwendung)
- Vendor
- Product
- Version
- Update
- Edition
- Language

Beispiel: cpe:/o:linux:kernel:2.6.0

21.7 CVE

Common Vulnerabilities and Exposures (CVE) ist ein Verzeichnis öffentlich bekannter Schwachstellen und Risiken in der Informationssicherheit.

21.8 CVSS

Das Common Vulnerability Scoring System (CVSS) ist ein offenes Framework zum Kennzeichnen von Schwachstellen.

21.9 DFN-CERT-Advisory

Ein Advisory, das vom DFN-CERT herausgegeben wird. Siehe https://www.dfn-cert.de/ für weitere Informationen.

21.10 Filter

Ein Filter beschreibt, wie eine bestimmte Teilmenge aus einer Gruppe von Ressourcen ausgewählt wird.

21.11 Gruppe

Eine Gruppe ist eine Sammlung von Benutzern.

21.12 Host

Ein Host ist ein einzelnes System, das mit einem Computernetzwerk verbunden ist und gescannt werden kann. Ein oder mehrere Hosts bilden die Basis eines Scanziels.

Ein Host ist auch ein Assettyp. Jeder gescannte oder gefundene Host kann in die Asset-Datenbank aufgenommen werden.

Hosts in Scanzielen und Scanberichten können mithilfe ihrer Netzwerkadresse (IP-Adresse oder Hostname) identifiziert werden.

In der Asset-Datenbank ist die Identifizierung unabhängig von der tatsächlichen Netzwerkadresse, welche dennoch als standardmäßige Identifikation genutzt wird.

21.13 Notiz

Eine Notiz ist ein Textkommentar in Verbindung mit einem VT. Notizen befinden sich in Berichten, unterhalb der Ergebnisse, die vom VT erzeugt wurden. Eine Notiz kann sich auf ein spezielles Objekt (Ergebnis, Aufgabe, Schweregrad, Port und/oder Host) beziehen, sodass die Notiz nur in bestimmten Berichten auftaucht.

21.14 Vulnerability Test (VT)

Ein Vulnerability Test (VT) ist eine Routine, die ein Zielsystem auf das Vorhandensein von konkreten bekannten und potentiellen Sicherheitsproblemen untersucht.

VTs sind in Familien aus ähnlichen VTs gruppiert. Die Auswahl der Familien und/oder einzelner VTs ist Teil der Scan-Konfiguration.

21.15 Übersteuerung

Eine Übersteuerung ist eine Regel zum Ändern des Schweregrads eines Elements innerhalb eines oder mehrerer Berichte.

Übersteuerungen sind inbesondere nützlich, um Elemente eines Berichts als Falschmeldungen (z. B. ein fehlerhaftes oder erwartetes Ergebnis) zu kennzeichnen oder um Elemente hervorzuheben, die im beobachteten Szenario einen höheren Schweregrad haben.

21.16 Berechtigung

Eine Berechtigung erteilt einem Benutzer, einer Rolle oder einer Gruppe das Recht eine bestimmte Aktion auszuführen.

21.17 Portliste

Eine Portliste ist eine Liste von Ports. Jedes Ziel wird mit einer Portliste verbunden. Diese bestimmt, welche Ports während eines Scans des Ziel untersucht werden.

21.18 Qualität der Erkennung (QdE)

Die Qualität der Erkennung (QdE) ist ein Wert zwischen 0 % und 100 % und beschreibt die Zuverlässigkeit der ausgeführten Schwachstellen- oder Produkterkennung. Der Wert von 70 % ist das standardmäßige Minimum, das für das Filtern der angezeigten Ergebnisse in den Berichten verwendet wird.

Für mehr Informationen über die QdE siehe Kapitel *11.2.6* (Seite 302).

21.19 Remediation-Ticket

Remediation-Tickets werden genutzt, um Schwachstellen zu beseitigen. Tickets können dem aktuellen Benutzer oder anderen Benutzern zugewiesen werden. Alle nützlichen Informationen, um das Problem zu verstehen und zu lösen sind verknüpft und für den zugewiesenen Benutzer verfügbar.

Alle Tickets haben einen bestimmten Status (z. B. offen, behoben), um den Fortschritt zu überwachen.

Zusätzlich können Benachrichtigungen für bestimmte Ereignisse bezüglich Tickets, z. B. Statusänderungen zugewiesener Tickets, erstellt werden.

Das Ticketverwaltungssystem ist dazu in der Lage, automatisch die Wiederholung von Scans zu erwägen, um zu verifizieren, dass ein Problem gelöst wurde.

21.20 Bericht

Ein Bericht ist das Ergebnis eines Scans und enthält eine Zusammenfassung dessen, was die ausgewählten VTS für jeden der Zielhosts festgestellt haben.

Ein Bericht ist immer mit einer Aufgabe verknüpft. Die Scan-Konfiguration, die den Umfang des Berichts festlegt, ist Teil der verknüpften Aufgabe und kann nicht verändert werden. Daher ist für jeden Bericht sichergestellt, dass die ausführende Konfiguration erhalten wird und verfügbar ist.

21.21 Berichtformat

Ein Format, in dem ein Bericht heruntergeladen werden kann.

Ein Beispiel ist TXT, welches den Inhaltstyp „text/plain“ hat, was bedeutet, dass der Bericht ein einfaches Textdokument ist.

21.22 Ergebnis

Ein einzelnes Ergebnis, das vom Scanner als Teil des Berichts erzeugt wurde, z. B. eine Schwachstellenwarnung oder eine Log-Nachricht.

21.23 Rolle

Eine Rolle legt eine Menge von Berechtigungen fest, die einem Benutzer oder einer Gruppe zugewiesen werden können.

21.24 Scan

Ein Scan ist eine Aufgabe, die ausgeführt wird. Für jede Aufgabe kann jeweils nur ein Scan aktiv sein. Das Ergebnis ist ein Scanbericht.

Die Status aller aktiven Scans sind auf der Seite *Aufgaben* sichtbar.

Der Fortschritt wird als Prozentsatz der Gesamtanzahl aller auszuführenden Tests angezeigt. Die Dauer eines Scans wird aus der Anzahl von Zielen und der Komplexität der Scan-Konfiguration bestimmt und reicht von wenigen Minuten bis zu einigen Stunden oder sogar Tagen.

Die Seite *Aufgaben* bitet die Möglichkeit, einen Scan zu stoppen.

Falls ein gestoppter oder unterbrochener Scan fortgesetzt wird, werden alle nicht abgeschlossenen Hosts komplett aufs Neue gescannt. Die Daten der bereits vollständig gescannten Hosts bleiben erhalten.

21.25 Scanner

Ein Scanner ist ein OpenVAS-Scanner-Daemon oder ein kompatibler OSP-Daemon, auf dem der Scan läuft.

21.26 Scan-Konfiguration

Eine Scan-Konfiguration deckt die Auswahl an VTs sowie genereller und spezieller Parameter für den Scanserver und für einige der VTs ab.

Die Scan-Konfiguration beinhaltet nicht die Auswahl der Ziele.

21.27 Zeitplan

Ein Zeitplan legt fest, zu welcher Zeit eine Aufgabe automatisch starten soll, nach welcher Zeitspanne die Aufgabe automatisch wiederholt werden soll und/oder welche maximale Laufzeit eine Aufgaben haben darf.

21.28 Schweregrad

Der Schweregrad ist ein Wert zwischen 0.0 (kein Schweregrad) und 10.0 (höchster Schweregrad) und zeigt auch die Schweregradklasse (*Log*, *Niedrig*, *Mittel* oder *Hoch*).

Dieses Konzept basiert auf CVSS, aber wird auch in Fällen angewendet, in denen kein vollständiger CVSS-Basisvektor verfügbar ist.

Der Vergleich, die Gewichtung und die Priorisierung aller Scanergebnisse oder VTs ist möglich, da das Schwachstellenkonzepts konsequent über das ganze System hinweg angewendet wird. Jedem neuen VT wird ein vollständiger CVSS-Vektor zugewiesen, selbst wenn die CVE keinen zur Verfügung stellt.

Die Schweregradklassen *Log*, *Niedrig*, *Mittel* und *Hoch* werden als Unterbereiche des Hauptbereichs 0.0 – 10.0 definiert. Benutzer können festlegen, ob andere Klassifizierungen genutzt werden sollen. Standard ist die NVD-Klassifizierung, welche die am häufigsten gebrauchte ist.

Scanergebnissen, die gefunden werden, wird ein Schweregrad zugewiesen. Der Schweregrad des zugehörigen VTs ändert sich möglicherweise mit der Zeit. Falls *Dynamischer Schweregrad* in den Benutzereinstellungen ausgewählt wurde, nutzt das System immer den aktuellsten Schweregrad eines VTs für das Ergebnis.

21.29 Art der Lösung

Diese Information zeigt mögliche Lösungen für die Beseitigung einer Schwachstelle.

- Problemumgehung: Informationen über Konfigurationen oder Einsatzszenarien, die die Belastung durch die Schwachstelle vermeiden, sind verfügbar. Es können keine, eine oder mehrere Problemumgehungen verfügbar sein. Dies ist normalerweise die „erste Verteidigungslinie“ gegen neue Schwachstellen, bevor eine Schadensminderung oder Herstellerlösung entdeckt oder ausgegeben wurde.
- Schadensminderung: Informationen über Konfigurationen oder Einsatzszenarien, die das Risiko der Schwachstelle reduzieren, sind verfügbar, was die Schwachstelle auf dem betroffenden Produkt allerdings nicht entfernt.
- Herstellerlösung: Informationen über einen offiziellen Fix des betroffenen Produkts durch den ursprünglichen Urheber, sind verfügbar. Sofern nicht anders vermerkt, wird angenommen, dass der Fix die Schwachstelle komplett beseitigt.
- Nicht verfügbar: Aktuell ist kein Fix verfügbar. Informationen sollten Details darüber enthalten, weshalb dies der Fall ist.
- Wird nicht gelöst: Es gibt keinen Fix für die Schwachstelle und es wird auch zukünftig keinen geben. Dies ist oft der Fall, wenn ein Produkt verwaist ist, nicht länger gewartet wird oder andersweitig überholt ist. Informationen sollten Details darüber enthalten, weshalb dies der Fall ist.

21.30 Tag

Ein Tag ist ein kleines Datenpaket, das aus einem Namen und einem Wert besteht und einer Ressource jeglicher Art hinzugefügt wird. Der Tag enthält vom Benutzer festgelegte Informationen zur Ressource.

21.31 Ziel

Ein Ziel definiert ein Set aus Systemen (Hosts), das gescannt wird. Die Systeme werden entweder durch ihre IP-Adresse, durch ihre Hostnamen oder mithilfe einer CIDR-Netzwerkschreibweise gekennzeichnet.

21.32 Aufgabe

Eine Aufgabe wird zunächst duch ein Ziel und eine Scan-Konfiguration gebildet. Das Ausführen der Aufgabe leitet den Scan ein. Jeder Scan erzeugt einen Bericht. Als Ergebnis sammelt eine Aufgabe eine Reihe von Berichten.

Das Ziel und die Scan-Konfiguration einer Aufgabe sind statisch. Deshalb beschreibt eine Folge von Berichten die Änderung des Sicherheitsstatus mit der Zeit. Dennoch kann eine Aufgabe als änderbar gekennzeichnet werden, falls es noch keine Berichte gibt. Für solch eine Aufgabe können das Ziel und die Scan-Konfiguration jederzeit geändert werden, was in bestimmten Situationen vorteilhaft sein kann.

Eine Container-Aufgabe ist eine Aufgabe mit der Funktion, importierte Berichte zu enthalten. Das Durchführen einer Container-Aufgabe ist nicht möglich.

21.33 TLS-Zertifikat

Ein TLS-Zertifikat (Transport-Layer-Security-Zertifikat) ist ein Zertifikat, das für die Authentifizierung genutzt wird, wenn eine durch TLS gesicherte Verbindung hergestellt wird.

Der Scanbericht enthält alle TLS-Zertifikate, die während eines Schwachstellenscans gesammelt werden.

Stichwortverzeichnis

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X