



Release-Notes zu GeNUGate 7.0

In diesen Release-Notes finden Sie Informationen zu der GeNUGate 7.0 Produktfamilie. Lesen Sie diese bitte aufmerksam durch! Wir empfehlen Ihnen unbedingt, dieses Upgrade zu installieren, da wir mit diesem Release viele neue Features und Vereinfachungen in der Bedienung zur Verfügung stellen.

Achtung!

Vor einem Upgrade empfehlen wir dringend, ein Konfigurations- oder besser noch ein vollständiges Backup der GeNUGate durchzuführen.

Eine ausführliche Anleitung zur Vorgehensweise beim Upgrade finden Sie in Kapitel 6 dieser Release-Notes.

Wichtig – Plattenspiegelung:

Die GeNUGate-Modelle 400, 600 und 800 sind mit Spiegelplatten ausgerüstet.

Es gehört zum normalen Upgradevorgang, dass das Mirroring auf Maschinen, die mit einem sogenannten Offlinemirror (Spiegelplatten) ausgerüstet sind, im Rahmen eines Upgrades **deaktiviert** wird. Dies ermöglicht es, den Erfolg eines Upgradevorganges zu testen.

Das Vorgehen bei Modellen mit Plattenspiegelung ist wie folgt:

- Führen Sie das Upgrade durch wie in Kapitel 6 beschrieben. Die Synchronisierung der Spiegelplatten wird dadurch automatisch deaktiviert.
- Test: In der Regel genügt es, das System mehrere Tage unter normalen Bedingungen laufen zu lassen.
- Mirror reaktivieren: Löschen Sie dazu die Datei `/var/db/.NOMIRROR`. Dadurch wird die Synchronisierung der Spiegelplatten wieder eingeschaltet, und der Mirror wird beim nächsten Lauf (in der Regel jede Nacht um 2:05) aktualisiert.

Wichtig – Upgrade Test im Multi-User-Mode:

Mit Version 7.0 wurden zahlreiche Datenstrukturen in der Registry des Systems geändert. In Kapitel 5.2 wird die Durchführung eines „Test-Upgrades“ beschrieben, das eine neue Registry erzeugt und auf Inkonsistenzen prüft.

Sollte diese Prozedur Fehlermeldungen ausgeben, empfehlen wir, die Inkonsistenzen **vor** dem eigentlichen Upgrade zu beseitigen.



Inhaltsverzeichnis

1	Umfang der Release-Notes	4
2	Neuerungen in GeNUGate 7.0	4
2.1	Unterstützung für IPv6	4
2.1.1	Regelkonfiguration	4
2.1.2	DNS	4
2.1.3	Hochverfügbarkeit	5
2.2	Erweiterung des Verbindungskonzeptes	5
2.2.1	PFL-Regeln	5
2.2.2	Routing	6
2.3	Performanceverbesserungen	6
2.3.1	TCP-, WWW- und FTP-Verbindungen ohne Inhaltsanalyse werden beschleunigt	6
2.3.2	Caching der Scanergebnisse des Virenschanners	6
2.3.3	Virenschscan in einer RAM-Disk	6
2.4	Fernwartung via GeNUCenter	7
2.5	Authentisierungsmethode: „Passwortdatei“	7
2.6	SMTP-AUTH	7
2.7	DNS-Regeln	7
2.8	PFL Remote-Upgrade	7
2.8.1	Zertifikatsketten	8
2.8.2	Neue Logwatch-Pattern	8
2.9	Usability	8
3	Software-Updates und Verhaltensänderungen	9
3.1	Betriebssystem	9
3.2	Abkündigung der VPN-Option	9
3.3	Option High Availability	9
3.3.1	Manuelle Anpassungen der bisherigen OSPF-Konfiguration	9
3.4	Aktualisierung der MIME-Magic-Datei	10
3.5	PFL	10
3.5.1	Unterstützung für Disketten entfernt	10
3.5.2	Log- und Zeitserver	10
3.5.3	Interne Dienste: Aktives FTP	10
3.6	SSH-Keygenerator in der GUI entfernt	10
3.7	Option „Kompatibilitätspaket“ entfernt	11
4	Überblick über die Versionen mit Updatesupport	11
5	Vor dem Upgrade	11
5.1	Systemvoraussetzungen	11
5.2	Test-Upgrade im Multi-User-Mode	12



6	Installation des Upgrades	12
6.1	Upgradepfad	12
6.2	Datensicherung	12
6.3	Minimaler freier Festplattenspeicher	13
6.4	Durchführung des Upgrades	13
7	Informationen im Web	17
8	So erreichen Sie uns	18



1 Umfang der Release-Notes

Diese Release-Notes bieten einen Überblick über Änderungen und Erweiterungen im Funktionsumfang der GeNUGate beim Wechsel von Version 6.3 zu Version 7.0. Genauere Erläuterungen zur Konfiguration finden Sie im GeNUGate-Handbuch.

Eine elektronische Variante dieser Release-Notes, die Software selbst und das aktuelle Handbuch können Sie auf unseren Kundenseiten unter www.genua.de im „Internen Kundenbereich“ herunterladen. Gern schicken wir Ihnen auch per Post eine CD zu; bitte senden Sie uns hierzu eine kurze E-Mail an auftrag@genua.de.

2 Neuerungen in GeNUGate 7.0

2.1 Unterstützung für IPv6

Das größte Feature der Produktfamilie 7.0 ist die Unterstützung für das Internet Protocol Version 6. Auf den Netzwerkschnittstellen werden automatisch Link-Local-Adressen gesetzt, aber ALG und PFL nehmen keine Autokonfiguration vor und auch keine Router-Advertisements an. Bis auf SIP unterstützen alle Regeln auf der GeNUGate IPv4 und IPv6.

Bei der Eingabe von IP-Adressen für die GeNUGate und bei Host- und Netzwerkobjekten wird automatisch erkannt, ob es sich um IPv4- oder IPv6-Adressen handelt. Regeln auf dem ALG und PFL werden dann, je nachdem welche Host- und Netzwerkobjekte verwendet werden, entweder auf eine der beiden IP-Versionen eingeschränkt oder automatisch für beide Versionen konfiguriert. Solange keine IPv6-Adressen und -Routen angelegt werden, wird IPv6 nicht über die GeNUGate geleitet.

2.1.1 Regelkonfiguration

Wie beschrieben wird bei Regeln automatisch entschieden, ob diese für IPv4 und IPv6 gelten oder nur für eine der beiden Protokollversionen. Als Entscheidungskriterien dienen dazu die Quell- oder Ziel-ACLs und die Transparenzeinstellungen der Verbindung.

Um zieltransparente Regeln weiterhin auf IPv4 einzuschränken ist es ausreichend in mindestens eine der ACLs nur IPv4-Einträge aufzunehmen. Um alle IPv4-Adressen auszuwählen ist eine ACL „0.0.0.0/0“ möglich (analog „::/0“ für IPv6).

Alle Regeln mit Proxyadresse auf der GeNUGate sind automatisch auf die Protokolfamilie dieser Proxyadresse eingeschränkt.

Weitere Informationen zu diesem Thema finden Sie in den Handbuchkapiteln 4.4.2 „ALG-Regeln“ und 4.4.6 „PFL-Regeln“.

2.1.2 DNS

Sobald passende IPv6-Routen vorhanden sind, stellt der DNS-Server auf der GeNUGate auch Anfragen mittels IPv6. Außerdem verbinden sich der Squid-Cache und Sendmail zunächst auf IPv6-Adressen, wenn die Namensauflösung IPv4- und IPv6-Adressen zurückliefert. **Bitte beachten Sie diesen Punkt vor allem, wenn Sie zum ersten Mal eine IPv6-Default-Route einrichten.**



Der Hintergrund ist, dass DNS-Anfragen auf der GeNUGate sowohl nach IPv6-Records („AAAA“) als auch nach IPv4-Records („A“) gestellt werden. Wenn für einen Hostname eine oder mehrere Adressen aus beiden Familien zurückgeliefert werden, richtet sich die Auswahl der Zieladresse nach der „Default Policy Table“ aus RFC 3484. Damit wird die IPv6-Kommunikation gegenüber IPv4 präferiert.

Die Konfiguration von IPv6-DNS-Einträgen im DNS-GUI der GeNUGate wird erst mit der kommenden GeNUGate-Version 7.1 möglich sein. Bis dahin ist weder die Eingabe von „AAAA“- noch von „ipv6.arpa“-Records im GeNUGate-GUI möglich.

2.1.3 Hochverfügbarkeit

Auch bei IPv6 wird OSPF verwendet, um in HA-Clustern die Hochverfügbarkeit sicher zu stellen. Da für die Kommunikation der OSPF-Neighbors die Link-Local-Adressen verwendet werden, gibt es im GUI keine zusätzlichen OSPF-Eingabefelder. Nur die manuell konfigurierten IPv6-Adressen müssen, wie bei IPv4, unter SYSTEM → HA → KONFIGURATION → HA-ADRESSEN für alle Systeme des Clusters erweitert werden.

2.2 Erweiterung des Verbindungskonzeptes

Mit GeNUGate Version 6.3 wurde das Verbindungskonzept für die Konfiguration von ALG-Regeln eingeführt. Hintergrundinformationen dazu finden Sie zum Beispiel im Handbuchabschnitt 2.4 „Verbindungen der GeNUGate“. Dieses Konzept wird mit GeNUGate Version 7.0 jetzt auch auf die Konfiguration des PFL und das Routing erweitert.

Damit einher geht eine Vereinfachung der Menüstruktur. Sowohl das Routing, als auch die PFL-Regeln, werden jetzt im GUI unter VERBINDUNGEN konfiguriert. Der Zugriff auf die Konfigurationsobjekte, wie „Hosts & Netzwerke“, ist so direkt möglich.

2.2.1 PFL-Regeln

Für die PFL-Konfiguration werden die Dienste, Policies und Netzwerkobjekte des ALG wiederverwendet. Dabei legt der Typ der Policy fest, welche IP-Protokolle am PFL zugelassen werden. Eine DNS-Policy betrifft am PFL zum Beispiel automatisch TCP- und UDP-Verbindungen. Außerdem werden die eingehenden Absender- und Zielports aus dem Service weiterverwendet, um Verbindungen am PFL zu filtern.

Im Gegensatz zum ALG gibt es auf dem PFL nur zwei Assoziationstypen:

- Pass
- Block

Sie legen fest, ob die Verbindung zugelassen wird oder nicht.

Ob bestimmte Verbindungen auf dem PFL geloggt werden sollen, wird, wie für den ALG, im Modul „Logging“ der Policy definiert. Außerdem können Sie im Policymodul „Optionen“ noch weitere Filtereigenschaften festlegen.

Genauere Informationen zu diesen Änderungen finden Sie im Handbuch im Abschnitt 4.4.6 „PFL-Regeln“.



2 NEUERUNGEN IN GENUGATE 7.0

2.2.2 Routing

Die Routing-Tabellen greifen wie die Regeln auf „Hosts & Netzwerke“ zurück. Als Zielnetzwerke dürfen sowohl Host- als auch Netzwerk-Objekte, als Gateway dagegen nur Host-Objekte, die direkt am GeNUGate angeschlossen sind, ausgewählt werden.

Im Handbuchkapitel 4.9.1 „Routing“ finden Sie weitere Informationen.

2.3 Performanceverbesserungen

2.3.1 TCP-, WWW- und FTP-Verbindungen ohne Inhaltsanalyse werden beschleunigt

Eingehende TCP-Verbindungen werden wie bisher auf dem ALG beendet und eine neue Verbindung zum Zielrechner aufgebaut. An dieser Stelle werden auch die ACLs und andere Policyeinstellungen überprüft und die IP- und TCP-Stacks des Zielsystems durch die Erzeugung neuer IP-Pakete mit neuem TCP-Header geschützt. Als Änderung in GeNUGate Version 7.0 kommt hinzu, dass die Nutzdaten im Hintergrund direkt im Kernel – und damit deutlich schneller – weitergereicht werden können.

Dies gilt auch für FTP- und WWW-Verbindungen, falls keine Inhaltsanalyse (Virensan oder Weeding) aktiviert ist. Es werden neue IP-Pakete mit neuem TCP-Header erzeugt und das jeweilige Protokoll weiterhin überprüft und umgesetzt.

Durch die Einsparung des Wechsels zwischen Kernel und Userlandprozess entstehen bei vielen Verbindungen deutliche Performanceverbesserungen.

2.3.2 Caching der Scanergebnisse des Virensanners

Dateien werden in der Standardkonfiguration jetzt nur noch beim ersten Download auf Viren gescannt. Dabei wird in einem Cache für den Inhalt der Datei (SHA256-Summe) das Ergebnis des Scans hinterlegt und jeder weitere Download verwendet dann dieses Resultat. Falls die gleiche Datei mehrfach parallel gescannt werden soll läuft ab GeNUGate Version 7.0 nur der erste Scan durch – alle weiteren warten auf dessen Durchführung.

Bei Patternupdates und Änderungen an der Virensannerkonfiguration wird der Cache natürlich invalidiert. Tritt während des Scanvorgangs ein Fehler auf, z.B. aus mangelndem Festplattenplatz, wird für die betroffene Datei kein Eintrag im Cache vorgenommen.

2.3.3 Virensan in einer RAM-Disk

Stehen im System mindestens 16GB RAM zur Verfügung so wird mit GeNUGate Version 7.0 automatisch eine RAM-Disk angelegt, in der Downloads entpackt und dann gescannt werden. Der Download selbst erfolgt dabei wie bisher auf die normale Festplatte unter `/cage/vscan`. Falls Fehler auftreten, weil nicht ausreichend Speicher in der RAM-Disk zur Verfügung steht, wird der Virensan automatisch auf der normalen Festplatte wiederholt.

Je nach Dateityp und Inhalt wird der Scan durch die RAM-Disk um bis zu einen Faktor 10 schneller. Dieses Feature funktioniert auch im Zusammenspiel mit dem Virensanner-Cache.



2.4 Fernwartung via GeNUCenter

GeNUGate Version 7.0 ist wieder für die Verwaltung mittels GeNUCenter vorgesehen. Einer der nächsten GeNUCenter-Releases wird die noch nötigen Anpassungen vornehmen und im README Einzelheiten zur Funktionalität erläutern.

2.5 Authentisierungsmethode: „Passwortdatei“

Zusätzlich zu den bisherigen Authentisierungsmethoden gibt es mit GeNUGate Version 7.0 die Möglichkeit, Usernamen und Passwörter in einer Datei zu hinterlegen. Dazu gibt es in den Policies mit Authentisierung, z.B. SMTP oder FTP, im Modul „Authentisierung“ die Option „Passwortdatei“ und „Pfad zur Passwortdatei“.

Genauere Informationen zu den unterstützten Formaten finden Sie im Handbuch in den Abschnitten der jeweiligen Policies.

2.6 SMTP-AUTH

In der SMTP-Policy kann im Modul „Authentisierung“ angegeben werden, ob eingehende Mailserver sich nach RFC 4954 mit Username und Passwort authentisieren müssen. Unterstützt werden als Methoden:

- PLAIN
- CRAM-MD5

Das unverschlüsselte Verfahren „PLAIN“ wird nur fuer TLS-gesicherte Verbindungen empfohlen. Soll es auch für ungesicherte Verbindungen genutzt werden, muss die Option „Unsichere Authentisierung“ aktiviert werden.

2.7 DNS-Regeln

Mit GeNUGate Version 7.0 wird die DNS-Policy als neuer Policytyp eingeführt. Dienste, die diese Policy verwenden, werden direkt auf den Zielport 53 und für TCP und UDP konfiguriert. Um Ressourcen zu sparen, wird außerdem für jedes UDP-Anfragepaket genau nur ein Rückpaket durchgelassen. Danach wird die Verbindung geschlossen und verwendete Ressourcen werden direkt wieder freigegeben.

Die Option „Nach letztem Antwortpaket schließen“, die beim DNS-Relay verwendet wird, kann auch manuell in jeder UDP-Policy im Modul „Optionen“ ausgewählt werden.

2.8 PFL Remote-Upgrade

Als neuer Betriebsmodus des PFL kann „USB Remote-Upgrade“ ausgewählt werden. Damit kann nicht nur die gesamte Konfiguration erneuert (vgl. „USB Remote-Administration“), sondern auch der Kernel bei Patches ausgetauscht werden. Mit diesem Feature ist also eine vollständige Fernwartung des PFL möglich.

Der nötige PFL-Reboot, um die Konfiguration zu aktivieren oder Patches einzuspielen kann jetzt auch im GUI unter PAKETFILTER → BOOTMEDIUM vorgenommen werden.



2 NEUERUNGEN IN GENUGATE 7.0

Genauere Informationen zu diesem Betriebsmodus finden Sie im Handbuchkapitel „4.6.3 Paketfilter Hardware“.

2.8.1 Zertifikatsketten

Die Zertifikatsverwaltung der GeNUGate unterstützt mit GeNUGate Version 7.0 nun auch Zertifikatsketten. WWW- und TCP-Relays mit eingeschalteter SSLify-Option übermitteln also das Root-Zertifikat sowie die nötigen Zwischenzertifikate. Voraussetzung ist, dass diese Zertifikate beim Erstellen von Server- oder Proxy-Zertifikaten mit angegeben worden sind.

2.8.2 Neue Logwatch-Pattern

Unter SYSTEM → SYSADMIN → EINSTELLUNGEN → LOGWATCH gibt es zwei neue vordefinierte Pattern. Das eine alarmiert bei möglichen ARP-Spoofing-Angriffen und das andere bei doppelt vergebenen IP-Adressen. Beide Pattern können über die Auswahl „kern“-Log oder „screen“-Log auf den ALG oder den PFL angewandt werden.

2.9 Usability

Im Bereich der Usability gab es etliche kleine Änderungen, die den Betrieb der GeNUGate vereinfachen. Hier finden Sie eine Auswahl der prominenteren Anpassungen:

- **Tabellensortierung:** Tabellen können jetzt nach beliebigen Spalten sortiert werden. Ausgenommen sind die Regelansichten für das ALG und den PFL, da deren Reihenfolge für die Verarbeitung relevant ist.
- **Backlinks bei Konfigurationslauf:** Die Darstellung beim Abspeichern und Aktivieren der Konfiguration wurde verbessert und es gibt einen Link zurück auf die letzte übergeordnete Konfigurationsseite.
- **Boot von der Mirrordisk:** Bisher kam es auf den im GeNUGate verbauten (RAID-)Controller an, ob der Boot von der Mirrordisk bei Festplattendefekt bzw. Konfigurationsproblemen ohne manuelle Anpassungen, z.B. im RAID-BIOS, möglich war. Ab GeNUGate Version 7.0 bootet die Mirrordisk jetzt in allen Anwendungsfällen automatisch.
Sowohl auf der Kommandozeile, als auch im GUI gibt es entsprechende Warnmeldungen, die auf die Verwendung der Mirrordisk hinweisen.
- **Benutzername und kompletter Hostname im GUI:** Oben rechts wird im GUI der eingeloggte Benutzer und der vollqualifizierte Hostname der GeNUGate angezeigt.
- **Aufforderung zum PFL-Konfigurationsupdate nur wenn nötig:** Die Erkennung bei Änderungen der PFL-Konfigurationen wurde korrigiert. Die Erinnerung an das nötige PFL-Update erfolgt bei Konfigurationsanpassungen jetzt nur noch, wenn auch für den PFL Änderungen vorliegen.



3 Software-Updates und Verhaltensänderungen

3.1 Betriebssystem

- **Enthaltene Patches:** In GeNUGate Version 7.0 sind alle Änderungen und Patches der Version 6.3 bis einschließlich Patch 9 enthalten.
- **Update auf OpenBSD Version 4.6:** Das Betriebssystem OpenBSD wurde mit sämtlichen Komponenten auf die Version 4.6 aktualisiert.

3.2 Abkündigung der VPN-Option

Wie auch schon zum Release von GeNUGate Version 6.3 angekündigt, wird mit GeNUGate Version 7.0 die VPN-Option für die GeNUGate entfernt. Es ist also nicht mehr möglich VPN-Verbindungen auf dem ALG selbst zu terminieren.

VPN-Appliances, die in einer DMZ der GeNUGate stehen, sind von diesen Änderungen nicht betroffen. Zur Migration eines bestehenden GeNUGate VPNs empfehlen wir den Einsatz von GeNUCrypts oder GeNUScreens, die dann gemeinsam mit der GeNUGate im GeNUCenter verwaltet werden können.

Eine bestehende VPN-Konfiguration wird durch das Upgrade auf GeNUGate Version 7.0 komplett entfernt.

3.3 Option High Availability

- **Netzwerkinterfaces:** Ab dieser Version kann HA nur noch betrieben werden, wenn alle HA-Systeme innerhalb eines Clusters auf ALG und PFL die selbe Anzahl von konfigurierten Netzwerkinterfaces aufweisen.
- **HA-Abgleich PFL-Interfaces:** Damit der HA-Abgleich funktioniert, muss nach erfolgreichem Upgrade auf dem HA-Master das Netzwerkinterface- und Adress-Mapping für den PFL vervollständigt werden. Dies geschieht über die GUI-Seiten SYSTEM → HA → KONFIGURATION → HA-ADRESSEN oder SYSTEM → PAKETFILTER → PFL-ADRESSEN → HA-INTERFACES.

Auf dem HA-Master ist dadurch die komplette Konfiguration des HA-Clusters vorhanden.

3.3.1 Manuelle Anpassungen der bisherigen OSPF-Konfiguration

Bisher konnten über die Registry und eine lokale Konfigurationsdatei Anpassungen an der OSPF-Konfiguration vorgenommen werden. Mit GeNUGate Version 7.0 ändert sich die Semantik dieser Anpassungen von Adressen zu Interfaces.

Zum Beispiel konnte man bisher in der Registry festlegen, dass bestimmte Adressen aus der GeNUGate vom OSPF-Export ausgenommen werden. Diese Einstellung bezieht sich nun nicht mehr auf einzelne Adressen, sondern auf ganze Interfaces und all deren Adressen. Im Gegenzug ist die Konfiguration dieses Parameters im GUI unter SYSTEM → ALG-INTERFACES möglich.



3 SOFTWARE-UPDATES UND VERHALTENSÄNDERUNGEN

Falls einzelne Adressen vom Export ausgenommen werden sollen ist eine lokale Konfigurationsdatei nötig. Bitte kontaktieren Sie wegen der korrekten Syntax für Ihre Konfiguration vor dem Upgrade Ihren Service-Partner.

3.4 Aktualisierung der MIME-Magic-Datei

In Policies mit Virenschanner kann über die „MIME-Typ ACL“ eingestellt werden, ob Dateien eines bestimmten MIME-Typs generell blockiert oder zugelassen werden sollen. Diese heuristische Erkennung funktioniert auch im Zusammenspiel mit Archiven, da sie erst angewandt wird, wenn die Originaldatei bereits vollständig entpackt ist.

Für GeNUGate Version 7.0 wurde die Musterdatei von MIME-Typen auf den neuesten Stand gebracht, womit mehr Typen zur Verfügung stehen und die Erkennung eventuell einen neuen Typ zurück liefert.

Auf der Kommandozeile der GeNUGate kann mit `mime_type` für einzelne Dateien überprüft werden, welcher MIME-Typ von der neuen Datei erkannt wird.

3.5 PFL

3.5.1 Unterstützung für Disketten entfernt

Aufgrund der Größe des PFL-Kernels mit IPv6 wurde die Unterstützung für Disketten entfernt. Die Konfiguration und der Boot erfolgt jetzt immer per USB-Stick, der wie bisher auf dem ALG verwaltet wird.

Auch die Backups des ALG (`cfgbu`), die unter früheren Versionen auf Diskette gespeichert werden konnten, sollten Sie schon jetzt auf einen USB-Stick umziehen, da in neueren Hardwarevarianten kein Diskettenlaufwerk mehr verbaut ist.

3.5.2 Log- und Zeitserver

Bisher war es möglich für den PFL separate Log- und Zeitserver zu hinterlegen. Um das Verhalten zu standardisieren, entfallen diese Konfigurationsoptionen mit GeNUGate Version 7.0 und der PFL verwendet für diese Dienste immer das ALG. Die hierfür nötigen Regeln werden automatisch im Hintergrund verwaltet.

3.5.3 Interne Dienste: Aktives FTP

Da die Aktivierung des „internen Diensts“ FTP in der PFL-Konfiguration vor GeNUGate Version 7.0 in zwei Szenarien genutzt werden konnte ist es möglich, dass der automatische Upgrade der bisherigen Konfiguration nicht ausreichend Regeln freischaltet.

Bitte kontrollieren Sie nach dem Upgrade die Regeln für aktives FTP in der PFL-Regelansicht.

3.6 SSH-Keygenerator in der GUI entfernt

In der Benutzerverwaltung konnte man bisher unter dem Punkt „Remotenzugang“ auch direkt SSH-Schlüsselpaare erzeugen. Diese Möglichkeit steht ab GeNUGate Version 7.0 nicht mehr zur Verfügung



und auf der GeNUGate erzeugte Schlüssel werden mit dem Upgrade vom System gelöscht. Im Handbuchabschnitt „5.2.2 Installation von SSH auf einem Client“ finden Sie weitere Informationen zur Erzeugung von SSH-Schlüsselpaaren.

Die bestehenden Remotezugänge von Usern sind von dieser Änderung nicht betroffen. Hierfür wird der öffentliche Teil des Schlüsselpaars direkt in der Registry der GeNUGate gespeichert.

3.7 Option „Kompatibilitätspaket“ entfernt

Im „Kompatibilitätspaket“ wurden viele Dateien als symbolische Links zu Pfaden zur Verfügung gestellt, unter denen sie in GeNUGate-Versionen vor 6.0 zu finden waren. Dieses Paket wird mit dem Upgrade auf GeNUGate Version 7.0 entfernt.

4 Überblick über die Versionen mit Updatesupport

Neben GeNUGate Version 7.0 werden aktuell noch folgende GeNUGate-Versionen mit Korrekturen und Sicherheitsupdates versorgt:

- **GeNUGate 6.0:** Diese Version ist die letzte nach CC EAL4+ zertifizierte GeNUGate-Version und wird im Updatesupport noch bis Mai 2011 unterstützt.
- **GeNUGate 6.2:** Sicherheitsupdates für GeNUGate Version 6.2 werden noch bis Mai 2011 ausgeliefert. Danach läuft diese Version aus dem Updatesupport heraus.
- **GeNUGate 6.3:** Diese Version wurde Ende September 2010 nach CC EAL4+ zertifiziert und ersetzt damit GeNUGate 6.0. Unterstützt wird dieser GeNUGate-Release noch mindestens bis Ende 2012.

Frühere Softwareversionen werden, wie auch in unseren allgemeinen Vertragsbedingungen für die Pflege von Software beschrieben, seit dem Release von GeNUGate 6.3 nicht mehr unterstützt. Dies betrifft insbesondere auch GeNUGate Version 6.1. Bitte upgraden Sie möglicherweise noch aktive Systeme dieser Versionen baldmöglichst.

5 Vor dem Upgrade

5.1 Systemvoraussetzungen

- Der Upgrade auf Version 7.0 wird von jedem Patchlevel der Version 6.3 unterstützt.
- Zum Betrieb der Version 7.0 werden mindestens 512MB RAM im ALG und 128 MB RAM im PFL empfohlen.
- Um den Upgrade erfolgreich durchführen zu können, muss ausreichend freier Festplattenspeicher auf dem ALG vorhanden sein. Die Prozedur zur Feststellung des Plattenspeichers wird in Kapitel 6.3 beschrieben.



5.2 Test-Upgrade im Multi-User-Mode

Um in der aktuellen Konfiguration Inkonsistenzen, die zu Problemen beim Upgrade führen, rechtzeitig erkennen und beheben können, sollte unbedingt ein „Test-Upgrade“ des Systems durchgeführt werden. Dazu muss wie folgt vorgegangen werden:

- Legen Sie im normalen Multi-User-Mode die CD in das Laufwerk Ihres Systems ein
- Führen Sie als Benutzer `'root'` das Kommando `'ggupgrade'` aus

Im Rahmen dieses Test-Upgrades wird als Erstes die Registry des Systems konvertiert und in die Datei `/etc/configfw/fw.cfg.pretty-G700_000` geschrieben („human readable“). Die Registry des laufenden Systems wird jedoch **nicht** modifiziert. Sollte es hierbei zu Problemen kommen, werden entsprechende Hinweise ausgegeben. Probleme mit weitreichenden Konsequenzen müssen außerdem explizit bestätigt werden.

Beachten Sie bitte, dass das Test-Upgrade nicht sicher feststellen kann, ob der Plattenplatz in älteren Systemen ausreicht. Die Prozedur zur Feststellung des Plattenspeichers wird in Abschnitt 6.3 beschrieben.

Im Anschluss an die Probekonvertierung der Registry wird ein `configfw`-Lauf angestoßen. Dieser stellt sicher, dass die Erzeugung der Konfigurationsdateien aus der konvertierten Registry reibungslos funktioniert. Anschließend kann das System entweder unverändert weiterbetrieben werden oder der eigentliche Upgrade (wie unter 6 beschrieben) durchgeführt werden.

Sollten bei der Durchführung des Test-Upgrades Probleme auftreten, wenden Sie sich bitte an Ihren Service-Partner. Zusätzliche Informationen zum Upgrade werden in den Dateien

`/var/gg/patches/G700_000.upgrade.log` (Registry-Upgrade) und
`/var/gg/patches/G700_000.configfw.log` abgelegt.

6 Installation des Upgrades

6.1 Upgradepfad

GeNUGate-Systeme ab der Version 6.3 können auf die Version 7.0 aktualisiert werden.

Ein bestimmtes Patchlevel der Version 6.3 ist hierbei nicht erforderlich.

6.2 Datensicherung

Bei dem Upgrade auf GeNUGate 7.0 bleiben die Logdateien und E-Mails im Spool-Verzeichnis auf dem System erhalten.

Trotzdem sollten Sie vor dem Upgrade mittels

```
# cfgbu -s
```

ein Backup Ihrer Konfiguration durchführen.

Um ebenfalls E-Mails und Logdateien zu sichern, muss ein Kompletbackup des Systems erstellt werden. Das Vorgehen hierzu ist im Handbuch, Kapitel 6.1 „Datensicherung“, beschrieben.



6.3 Minimaler freier Festplattenspeicher

Um den Upgrade erfolgreich durchzuführen, muss auf den verschiedenen Partitionen der Festplatte genügend freier Speicher vorhanden sein. Insbesondere sollten die Partitionen / und /usr mehr als das Doppelte des bereits belegten Platzes als freien Speicherplatz zur Verfügung haben. Durch Eingabe des Kommandos `df -h` können Sie die Belegung der Festplatte prüfen.

```
admin@ggd132:~# df -h
Filesystem      Size  Used Avail Capacity  Mounted on
/dev/wd0a        126M  40.8M  78.9M   34%    /
/dev/wd0f        1.5G  113M   1.3G    8%    /cage
mfs:6239         62.9M  2.0K  59.8M    0%    /tmp
/dev/wd0d        502M  238M  239M   50%    /usr
/dev/wd0e        251M  33.5M  205M   14%    /var
```

In der Spalte „Capacity“ wird der Füllgrad des jeweiligen Dateisystems angegeben.

6.4 Durchführung des Upgrades

Bitte beachten Sie:

Sie benötigen zur Durchführung des Upgrades physikalischen Zugang zur GeNUGate, da CD-ROM und USB-Stick eingelegt bzw. gewechselt werden müssen.

Legen Sie die GeNUGate 7.0 CD-ROM in das Laufwerk, loggen Sie sich als Benutzer „admin“ auf das System ein und verwenden Sie das Kommando `su` um „root“ zu werden.

```
admin@ggd132:~# su -
Password:
Sep 18 08:06:33 ggd132 su: admin to root on /dev/console
root@ggd132:~#
```

Starten Sie `ggupgrade`, um den Upgrade zu beginnen.

```
root@ggd132:~# /usr/local/gg/sbin/ggupgrade
Executing upgrade script from cdrom.
Starting /cdrom/usr/local/gg/sbin/ggupgrade ...

Vor dem Upgrade werden jetzt die Patches fuer das neue Release
geholt. Daher wird Ihr GeNUGate nach dem Upgrade gleich mit dem
aktuellsten Patchlevel arbeiten.

Before the upgrade the patches for the new release are fetched now.
That way your GeNUGate will start working with the latest patchlevel
right after upgrade.

Get upgrade patch from cdrom ...
Retrieving G700_000.tar
Extracting G700_000.tar

Die Patches fuer die neue Version koennen ueber das Internet von
GeNUA geholt werden.

The patches for the new version can be fetched from GeNUA over the
internet.

Patches von GeNUA (ja nein) [ja]? Patches from GeNUA (yes no) [yes]? ja
```



6 INSTALLATION DES UPGRADES

Sie können bereits vor dem Neustart des Systems nach veröffentlichten Patches suchen, wenn Sie hier **yes** oder **ja** eingeben.

Unter Umständen kündigt das System jetzt an, dass einige Fragen zur Installation gestellt werden. Bestätigen Sie dies einfach mit [RETURN] das System wird die Fragen zur Installation überspringen und mit dem Upgrade weitermachen.

Nun wird ein Test-Upgrade der Registry und ein testweiser Lauf von `configfw` durchgeführt, um herauszufinden, ob beim Upgrade Probleme zu erwarten sind. Sollte es hierbei zu Problemen kommen, kontaktieren Sie bitte Ihren Service-Partner.

Starten Sie nun das System neu.

```
root@ggd132:~# reboot
Sep 18 08:11:42 ggd132 reboot: rebooted by admin
/etc/rc.shutdown in progress...
IP is OFF
/etc/rc.shutdown complete.
Sep 18 08:11:45 ggd132 syslogd: exiting on signal 15
syncing disks... done
rebooting...
```

Achten Sie darauf, dass das System von der eingelegten GeNUGate 7.0 CD-ROM bootet. Dies wird durch den Text *CDBOOT 2.02* im Bootprompt bestätigt.

```
>> OpenBSD/i386 CDBOOT 2.02
boot>
booting cd0a:bsd.install: 4020108+930528 [52+215856+195731]=0x51d3d8
entry point at 0x200120

[ using 412012 bytes of bsd ELF symbol table ]
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California. All rights reserved.
Copyright (c) 1995-2008 OpenBSD. All rights reserved. http://www.OpenBSD.org

OpenBSD 4.6-stable (ALG.install) #0: Fri Oct  1 19:52:17 CEST 2010
bluhm@g701.genua.de:/build/gg.70/70.D020/ALG.install
cpu0: Dual Core AMD Opteron(tm) Processor 265 ("AuthenticAMD" 686-class, 1024KB L2 cache) 1.80 GHz
cpu0: FPU,V86,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,PAT,PSE36,CFLUSH,MMX,FXSR,SSE,SSE2,SSE3
...
```

Nachdem der Kernel geladen ist, werden Sie von der GeNUGate 7.0 Installation begrüßt und müssen die Installationsprache und Tastaturbelegung auswählen. Bei der Auswahl des Installationsmodus wählen Sie **upgrade**.

```
GeNUGate Installation

Sprache auswaehlen.
Sprache/Language (de en) [de] ? [RETURN]

Belegung der an der GeNUGate angeschlossenen Tastatur auswaehlen.
Tastaturbelegung (us de de.nodead ... pl hu si cf cf.nodead) [de.nodead] ? [RETURN]
kbd: keyboard mapping set to de.nodead

Systemerkennung.

Installieren, Upgrade durchfuehren oder System vom Backup restaurieren.
Modus (installation upgrade restaurieren) [installation] ? upgrade
```

Es werden nun die Festplatten geprüft, in das System eingebunden und für den Upgrade vorbereitet.



6 INSTALLATION DES UPGRADES

```
Festplatte mounten.  
Boot-Festplatte festlegen.  
Erkenne Festplatten im System.  
Boot-Festplatte erfolgreich festlegen.  
Alle Partition unmounten.  
Fstab auslesen.  
Dateisysteme ueberpruefen.  
/dev/rwd0a: file system is clean; not checking  
/dev/rwd0f: file system is clean; not checking  
/dev/rwd0d: file system is clean; not checking  
/dev/rwd0e: file system is clean; not checking  
Alle Partition mounten.  
Flags entfernen.  
GeNUGate Lizenzen.  
Lizenz initialisieren.
```

Die Lizenznummer und Hardware-Seriennummer Ihrer GeNUGate wird abgefragt. Die Werte aus GeNUGate 6.3 gelten weiterhin und Sie müssen nur **[RETURN]** drücken, um diese beizubehalten.

```
Lizenz eingeben.  
Der einzugebende Wert hat das Format 1234-GG-ABCD-EFGH-IJKL-MNOP.  
Lizenz [1234-GG-ABCD-EFGH-IJKL-MNOP] ? [RETURN]  
  
Seriennummer eingeben.  
Der einzugebende Wert hat das Format XXXXX-XX-XXXX.  
Seriennummer [12345-CD-89AB] ? [RETURN]
```

Es besteht nun die Möglichkeit, Patches vom USB-Stick, vom HA-Peer oder via Netzwerk zu beziehen.

```
Patches vom USB-Stick holen.  
Patches vom USB-Medium holen (ja nein) [nein] ? [RETURN]  
  
Patches vom HA-Peer holen.  
Patches vom HA-Netzwerk holen (ja nein) [nein] ? [RETURN]  
  
Patches von GeNUA holen.  
Patches vom Netzwerk holen (ja nein) [nein] ? [RETURN]
```

Das Upgrade wird nun begonnen. Die neue Software wird auf das System kopiert und die Konfiguration durchgeführt.

```
Upgrade beginnen.  
  
Upgrade-Patch von Cdrom kopieren.  
Retrieving G700_000.tar  
  
Das System wird f"ur den Upgrade vorbereitet.  
Using new ggpatch /var/gg/patches/ggpatch.  
...
```

Am Ende des Upgrade-Vorgangs werden Sie gefragt, ob Sie die Passwörter für den Administrator „admin“ und „root“ neu setzen wollen. Um die bestehenden Passwörter zu übernehmen, wählen Sie **nein** durch Drücken von **[RETURN]**.

```
Administrator Passwoerter setzen.  
Passwoerter setzen (ja nein) [nein] ? [RETURN]
```



6 INSTALLATION DES UPGRADES

Das Upgrade ist nun beendet. Drücken Sie **[RETURN]**, um das System neu zu starten und entfernen Sie die CD-ROM aus dem Laufwerk.

```
Druecken Sie <Return> zum Neustart und entfernen Sie nach der Meldung
'rebooting...' die CDROM aus dem Laufwerk.
Jetzt neu starten (neustart) [neustart] ? [RETURN]
```

Das System startet nun die neue Software. Nach dem Laden des Kernels werden Sie aufgefordert, das „root“-Passwort einzugeben, da noch ein Bootinstall-Skript für die Aktualisierung des Paketfilters ausgeführt werden muss.

```
Es wurde mindestens ein Bootinstall-Skript gefunden. Diese Skripten koennen
nur vom Systemverwalter ausgefuehrt werden. Daher wird jetzt nach dem
Passwort des Systemverwalters (root) gefragt. Wird das Passwort dreimal
falsch eingegeben, kann weiter gebootet werden, ohne dass die Bootsripten
ausgefuehrt wurden. Geben Sie bitte jetzt das root Passwort ein!
Sie haben 60 Sekunden sich zu authentisieren!
```

```
Root Passwort eingeben
```

```
Password:
```

Wählen Sie das Script aus der Liste durch die Auswahl von **1** und **[RETURN]**. Führen Sie es durch Eingabe von **j** aus.

```
Waehlen Sie eine Liste von Bootinstall-Skripten aus, indem Sie die
entsprechenden Nummern eingeben, oder alle durch Eingabe von '*'
=====
```

```
1) /var/gg/boot/bootinst.2010.10.02-15.12.02.exe
    Paketfilter-Diskette Initialisieren
```

```
Auswahl (1) []: 1
```

```
1) /var/gg/boot/bootinst.2010.10.02-15.12.02.exe
    Paketfilter-Diskette Initialisieren
```

```
Ist das ok? (j/n) [n]: j
```

Stecken Sie die PFL-Diskette in das Laufwerk des ALG oder den PFL-USB-Stick in einen freien USB-Slot im ALG und schreiben das PFL-Medium. Starten Sie den PFL gemäß den Anweisungen neu. Wenn Sie sich nach Beendigung des Startvorgangs auf das ALG einloggen, werden Sie mit einer Meldung begrüßt, in der die neue Versionsnummer steht.

```
login: admin
Password:
Last login: Mon Sep 10 15:05:02 on console

        Welcome to your GeNUGate Firewall System.

        This system is running GeNUGate Version 7.0 000 based on OpenBSD 4.6

admin@ggd132:/var/home/admin$
```

Verwenden Sie das Kommando `su um „root“` zu werden. Anschliessend führen Sie das Kommando `configfw` aus. Dies ist nötig, da beim Upgrade selbst keinerlei Syntax-Checks für die erzeugten Konfigurationsdateien stattgefunden haben, um ein reibungsloses Upgrade durchführen zu können:



```
root@ggdl32:~# configfw
zone file /cage/ALG_2_INTERN/etc/namedb/gg.de.db: new serial (2009081061) <= current (2009081061)
zone file /cage/ALG_2_INTERN/etc/namedb/18.172.in-addr.arpa.db: new serial (2009081061)
<= current (2009081061)
zone file /cage/ALG_2_INTERN/etc/namedb/16.172.in-addr.arpa.db: new serial (2009081061)
<= current (2009081061)
zone file /cage/ALG_2_INTERN/etc/namedb/19.172.in-addr.arpa.db: new serial (2009081061)
<= current (2009081061)
zone file /cage/ALG_1_EXTERN/etc/namedb/gg.de.db: new serial (2009081061)
<= current (2009081061)
zone file /cage/ALG_1_EXTERN/etc/namedb/16.172.in-addr.arpa.db: new serial (2009081061)
<= current (2009081061)
SYSLOG: Sep 10 15:19:17 configfw[14384]: I5200 1249910357 SubSystem: Installiere /etc/licenses
SYSLOG: Sep 10 15:19:17 configfw[14384]: I5200 1249910357 SubSystem: Kommando:
/usr/local/gg/sbin/licctl -M read -M store
SYSLOG: Sep 10 15:19:18 configfw[14384]: I5200 1249910358 SubSystem: Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/LOOPBACK
SYSLOG: Sep 10 15:19:19 configfw[14384]: I5200 1249910359 SubSystem: Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/ALG_1_EXTERN
SYSLOG: Sep 10 15:19:20 configfw[14384]: I5200 1249910360 SubSystem: Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/ALG_2_INTERN
SYSLOG: Sep 10 15:19:21 configfw[14384]: I5200 1249910361 SubSystem: Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/ALG_3_ADMIN
SYSLOG: Sep 10 15:19:22 configfw[14384]: I5200 1249910362 SubSystem: Kommando:
ln -sf /usr/share/zoneinfo/CET /etc/localtime
SYSLOG: Sep 10 15:19:22 configfw[14384]: I5200 1249910362 SubSystem: Kommando:
/sbin/pfctl -f /etc/pf.conf
...
```

Um sicherzustellen, dass alle Dateien korrekt installiert wurden, sollten Sie nun `filecop` ausführen:

```
root@ggdl32:~# filecop
filecop: Phase 1 - Datenbank(en) werden mit Dateisystem verglichen
filecop: Phase 2 - Dateisystem wird mit Datenbank(en) verglichen
```

Falls Sie für Ihr System zusätzlich die Option GeNUScan besitzen, müssen Sie im Anschluss an das Update auch noch Ihre Virens Scanner auf den aktuellsten Stand bringen. Dazu führen Sie als Benutzer `root` noch das Kommando `getpatterns` aus:

```
root@ggdl32:~# getpatterns
...
```

Wir wünschen Ihnen viel Spaß mit dem neuen System!

7 Informationen im Web

Diese Release-Notes sind auch online im Bereich „Kundenservice“ unseres Webserver erreichbar:

<http://www.genua.de/customer/index.html> ,

Bereich „GeNUGate Support“ -> „Release-Notes“.

Ausführlichere Beschreibungen und weiterführende Informationen finden Sie nach der Anmeldung im „Internen Kundenbereich“ unter „GeNUGate Support“ -> „Knowledge Base“ .



8 So erreichen Sie uns

GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH

Domagkstraße 7, 85551 Kirchheim bei München

Tel. (089) 99 19 50-900, Fax. (089) 99 19 50-999

E-Mail: info@genua.de, WWW: <http://www.genua.de/>

© 2010 GeNUA mbH, Kirchheim, Alle Rechte vorbehalten. GeNUGate und GeNUA sind eingetragene
Warenzeichen der GeNUA mbH.