

GeNUCenter 1.1 Release Notes

Information on the GeNUCenter 1.1 product family is available in these release notes. Please read this document carefully! You are advised to install this upgrade, as this release both resolves various problems, and provides new features.

Attention!

We strongly recommend performing a configuration backup of your GeNUCenter system BEFORE upgrading.

Detailed instructions on how to perform this upgrade are available in section 5 of these release notes.

Inhaltsverzeichnis

1	Scope of Delivery	2
2	New Features in GeNUCenter 1.1	2
2.1	Operating system update	2
2.2	GUI improvements	2
2.3	GeNUGate administration	3
2.4	Organisation of partly meshed VPN topologies	3
2.5	Logging	3
2.6	GeNUCenter operation in high availability mode	4
3	Modified Functionality	4
3.1	Negated source and destination in filter rules	4
4	New Features Affecting GeNUScreen and GeNUCrypt Systems	4
4.1	Enhanced performance:	4
4.2	High availability	4
4.3	Filter	5
5	Upgrade Installation	5
6	How to Contact Us	6

1 Scope of Delivery

With the current GeNUCenter version 1.1 you have received:

- these release notes
- a bootable CD-ROM

2 New Features in GeNUCenter 1.1

2.1 Operating system update

The operating system OpenBSD, on which the product is based, has been upgraded to version 4.1. A complete of changes due to this version upgrade is available at

<http://www.openbsd.org/plus40.html>

and

<http://www.openbsd.org/plus41.html>

2.2 GUI improvements

The GeNUCenter GUI was revised and substantially improved:

- Inline editing: Referenced definitions now can be created and edited in dialogs. E.g., new networks and services now can be added to filter rules definitions.
- Based on JavaScript, GeNUCenter page elements now are available without having to reload the entire page. E.g., the online help can be displayed or hidden without losing previous, as yet unsaved entries.
- Maps: A new overview page positions appliances on a geographic map. Appliance status is automatically updated every five minutes.
- Arbitrary grouping of services in filter rules now is available. E.g., all IPsec relevant IP protocols and and UDP services can be grouped as to require only a single filter rule.
- Filer rules now may contain comments.
- Subdomains: Appliances now can be grouped to *subdomains* that share common definitions. Administrator accounts can be restricted to access only certain subdomains.
- Bulk actions: Filter rules or VPN partners can be simultaneously assigned to selected appliances in a subdomain. This simplifies the administration of numerous machines.
- Tagging: Any object can be “tagged” and searched for in the overview pages.

- Search: All managed objects can be searched for strings and networks. This simplifies the administration of numerous appliances with many filter rules and network definitions.

2.3 GeNUGate administration

Previously installed GeNUGate systems (version 6.2 patch 1 and higher) now can be integrated into remote management by GeNUCenter systems.

- Convenient and concise relay management.
- Several relay definitions can reference shared sources, destinations, and listeners.
- Central collection of logs, reports, and accounting data.
- Configuration backups can be collected on the GeNUCenter system.
- GeNUGate systems can be updated by the GeNUCenter Management Server. This however needs local manual intervention.

2.4 Organisation of partly meshed VPN topologies

When managing complex VPN topologies, it now is possible to define one appliance as the central *hub* of a star-shaped VPN connection group. Appliances connected to the hub can initiate VPN communication to each other through it. As the hub sees the data stream as plain text, filter rules can be applied.

2.5 Logging

Major extensions were added to logging.

- Detailed searching of log data for filter processes, IP addresses and networks now is available.
- Graphical statistical reports of configurable time spans.
- Statistics on the GeNUCenter system itself also are generated, including disk usage.
- Reports in PDF format covering connection data, application of filter rules etc. can be generated for each appliance separately for varying time spans.
- Accounting data can be generated per connection. This enables recording of filter rule data such as source, destination, and data volume per individual TCP or UDP connection.

2.6 GeNUCenter operation in high availability mode

Fail-safe operation of the GeNUCenter system now is available. A second GeNUCenter machine is installed and registered as a “slave” system on the first machine (i.e., high availability setup).

3 Modified Functionality

This update will cause changes that may call for modifying your system’s configuration.

3.1 Negated source and destination in filter rules

GeNUCenter 1.0 permitted applying rules on “negated” sources and destinations. The upgrade moves this feature to the network definitions to enable re-use in other rules.

A warning will be displayed during the GeNUCenter upgrade process if rules with such source or destination networks are found. The upgrade program will output a list of URLs to directly display the affected rules. To modify a rule, define a network object with the respective negated addresses, and add – without negation – the network `0.0.0.0/0`. Use this network object as the filter rule’s source or destination.

If negated interfaces are used as source or destination, all addresses of the respective interface must be moved to the network definition.

4 New Features Affecting GeNUScreen and GeNUCrypt Systems

The upgrade also affects the managed appliances.

4.1 Enhanced performance:

Numerous performance enhancements and improved scalability were introduced.

- Faster filtering: On the compact hardware 100C (revisions 2 and 3), filtering now is performed at twice the previous speed.
- Faster VPN : VPN connections by the 100C revision 3 hardware with the VIA C7 processor now are significantly faster due to usage of internal processor crypto functions.

4.2 High availability

- `trunk` interfaces: Several ethernet interfaces can be bundled to `trunk` interfaces on GeNUScreen systems. If the physical cabling runs over different switches, a layer 2 based fail-safe setup is possible.

4.3 Filter

Filter features on the GeNUScreen system were extended and the GUI improved.

- Detailed VPN filtering: VPN data traffic can be filtered in greater detail. Filter rules now permit stating VPN partners as source and destination interfaces.
- Predefined services: Services for various well-known protocols now are available per default.
- Individual connection accounting: Connection duration, source, destination, and data volume of individual connections now can be logged.
- *NetFlow*TM support: GeNUScreen systems now can transmit collected logs to a collector via the *NetFlow*TM protocol (versions 1 and 5).
- Real-time monitoring of filter states: The GUI now displays all currently active connections. This overview permits direct viewing of all involved filter rules, as well as termination of selected connections.
- Several source and destination addresses per rule: A rule definition now can contain several source and destination addresses.
- Combined TCP and UDP services: Services now can be grouped for filter rules. For example, the TCP and UDP services on port 53 can be grouped together to the DNS service.

5 Upgrade Installation

Before upgrading the GeNUCenter system, be sure to patch the system to version 1.0p5. The upgrade process consists of a new GeNUCenter installation and a subsequent database backup restore. You therefore will be able to check the results in the Web interface after the database restore before activating the configuration.

Before starting the upgrade, please check if you have SSH access to the GeNUCenter system, and set it up if necessary.

To upgrade, perform the following steps:

- Log in as `root` on the GeNUCenter machine.
- Generate the database backup by executing the following command:

```
$ db_backup -f /var/tmp/upgrade_config_backup.dbak center_production
```

Log data is backed up in the same way:

```
$ db_backup -f /var/tmp/upgrade_logging_backup.dbak logging_center_production
```

- Copy the two files

```
/var/tmp/upgrade_config_backup.dbak
```

and

```
/var/tmp/upgrade_logging_backup.dbak
```

to a different machine (e.g. with `scp`).

- Now install your GeNUCenter system with the new version.
- Log in over the Web and activate SSH access. (Take note of the SSH ACL.)
- Copy the two previously generated database backups (see above) to your GeNUCenter system in the directory `/var/tmp`.

- Restore the backups:

```
$ db_restore -d logging_center_production /var/tmp/upgrade_logging_backup.dbak
```

```
$ db_restore -d center_production /var/tmp/upgrade_config_backup.dbak
```

This step migrates the database to the new version and tests them. Please note any warnings displayed. You may be asked to check your configuration syntax in the GUI. The necessary steps are explained in section 3.

- Now log in at the Web interface and check the results. It is recommended to – at the very least – check the GeNUCenter configuration itself to prevent losing access to the Management Server due to errors.
- After checking, activate the GeNUCenter configuration in the GUI maintenance menu.

6 How to Contact Us

GeNUA Gesellschaft für Netzwerk– und Unix–Administration mbH

Domagkstraße 7, 85551 Kirchheim near Munich

Tel. +49 89 99 19 50-0, Fax. +49 89 99 19 50-999

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

© 2008 GeNUA mbH, Kirchheim, all rights reserved. GeNUGate and GeNUA are registered trademarks of GeNUA mbH.