How to upgrade to Zorp Professional 6 (6.0)

November 30, 2016

Copyright © 1996-2016 BalaSys IT Ltd.

Table of Contents

1. Preface

Welcome to Zorp Professional (Zorp) version 6 and thank you for choosing our product. This document describes the process to upgrade existing Zorp installations to Zorp 6. The main aim of this paper is to aid system administrators in planning the migration to the new version of Zorp.

Warning
Read the entire document thoroughly before starting the upgrade.

This document covers the Zorp Professional 6 product and its related components.

2. Prerequisites to upgrading to Zorp

This section describes the requirements and steps to perform before starting the Zorp upgrade process.

Warning
A direct OS-level upgrade from previous versions is NOT SUPPORTED.

To upgrade an existing Zorp installation to version 6, backup your configuration files, perform a clean install on every host of your Zorp Firewall System, then restore your configuration. Plan your maintenance window and downtime accordingly.

Upgrading to Zorp version 6 is supported from Zorp versions 3.4, 3.5, and 5.

When upgrading from version 3.4 or 3.5, read *Section 3.1, Upgrading from Zorp version 3.4 or 3.5 (p. 5)* carefully before starting the upgrade.

- You must have a valid software subscription to be able to download the new version of Zorp, and also the new license file.
- You will need a MyBalaBit account to download the required files and the license. If you have not done so yet, sign up for a MyBalaBit account at *http://www.balabit.com/mybalabit/*. Note that the registration is not automatic, and might require up to two working days to process.

3. Notes and warnings about the upgrade

The following is a list of important notes and warnings about the upgrade process and changes in Zorp 6.

Warning
A direct OS-level upgrade from previous versions is NOT SUPPORTED.

To upgrade an existing Zorp installation to version 6, backup your configuration files, perform a clean install on every host of your Zorp Firewall System, then restore your configuration. Plan your maintenance window and downtime accordingly.

Upgrading to Zorp version 6 is supported from Zorp versions 3.4, 3.5, and 5.

When upgrading from version 3.4 or 3.5, read *Section 3.1, Upgrading from Zorp version 3.4 or 3.5 (p. 5)* carefully before starting the upgrade.

3.1. Upgrading from Zorp version 3.4 or 3.5

Upgrading to Zorp version 6 is supported also from Zorp versions 3.4 and 3.5. If you are upgrading from Zorp 3.4 or 3.5, note the following points and configuration changes.

- Zorp 6 requires a new kernel. If you are using a customized kernel, contact your local BalaBit Support Team or directly BalaBit IT Security to help you with the upgrade process.
- Upgrade is supported only for hosts that are managed using the Zorp Management Server (ZMS). If a host is managed locally without using ZMS, request help from the BalaBit Support Team for manually upgrading the configuration files.
- IPSec will be available after the upgrade is completed, provided that ZMC can connect to ZMS without using IPSec (typically this is not a problem unless you manage Zorp remotely from an external network).
- If you have manually modified any configuration files (for example, Postfix configuration file), make sure to create a backup before starting the upgrade. Configuration files that were modified manually are automatically reset to their ZorpOS default. Files that were managed using the Text editor ZMC plugin are not affected.
- Upgrading removes every custom package from the hosts that are not part of the standard installation. If you need any custom packages, reinstall them after the upgrade.

Main changes in the Zorp configuration between versions 3.4 and 3.5

- The package `ip6tables-utils` is automatically installed.
- By default, every IPv6 address belongs to the internet zone. You can change that by adding IPv6 subnets to other zones.
- Zorp 3 F5 uses Strongswan instead of OpenSwan to handle IPSec VPN connections.
- The *`process-limit`* option of *`zorp-ctl`* has been removed. If you need similar functionality, set the *`nproc`* option in `/etc/security/limits.conf`. For details, see the `limits.conf(5)` manual page.

Main changes in the Zorp configuration between versions 3.5 and 5

- The configuration of zones has been removed from `policy.py` and moved into `zones.py` residing in the same directory as the policy file. There have been no changes to the syntax of the zone configuration.
- As of Zorp 5.0, underscores in hostnames are not supported anymore. Underscores will be automatically converted to dash when using the Zorp Management System, but a manual review of the hostname is desirable.
- To better reflect its purpose, the kzorp utility has been renamed to `kzorp-client`.
- As of Zorp 5.0, only US ASCII characters are supported in zone names.
- The Zorp Firewall python libraries have been moved from the `/usr/share/zorp/pylib/` directory to the OS-standard python library path `/usr/lib/pyshared/`.

4. Procedure – Upgrading your Zorp Firewall System to version 6

Purpose:

To upgrade every host of a Zorp Firewall System to version 6, complete the following steps. Before starting the following procedure, read this entire document carefully.

Warning
A direct OS-level upgrade from previous versions is NOT SUPPORTED.

To upgrade an existing Zorp installation to version 6, backup your configuration files, perform a clean install on every host of your Zorp Firewall System, then restore your configuration. Plan your maintenance window and downtime accordingly.

Upgrading to Zorp version 6 is supported from Zorp versions 3.4, 3.5, and 5.

When upgrading from version 3.4 or 3.5, read *Section 3.1, Upgrading from Zorp version 3.4 or 3.5 (p. 5)* carefully before starting the upgrade.

Note
This procedure is a high-level overview of the upgrade process and references detailed procedures that describe the individual steps.

Steps:

Step 1. Update your Zorp Management Server to the latest revision of Zorp 3.4, 3.5, or 5, as described in *Procedure 10, Updating a host to the latest Zorp 5 version (p. 12)*.

Step 2. Update your Zorp hosts to the latest revision of Zorp 3.4, 3.5, or 5, as described in *Procedure 10, Updating a host to the latest Zorp 5 version (p. 12)*.

Step 3. Upgrade your Zorp Management Server as described in *Procedure 5, Upgrading Zorp Management Server to version 6 (p. 7)*.

Step 4. Upgrade your other hosts as described in *Procedure 7, Upgrading a host to Zorp 6 (p. 9)*.

Step 5. Test your environment and check that your Zorp services are operating properly.

Step 6. In case you encounter any problems, refer to the upgrade logs, or contact your BalaBit Support Team.

5. Procedure – Upgrading Zorp Management Server to version 6

Purpose:

To upgrade a Zorp Firewall System to version 6, first the Zorp Management Server must be upgraded. Complete the following steps. Before starting the following procedure, read this entire section carefully.

Prerequisites:

The configuration of every Zorp component must be uploaded and active on the host. Upload and reload every configuration change from ZMC before starting the upgrade. Also, check the general prerequisites described in *Section 2, Prerequisites to upgrading to Zorp (p. 4)*.

Warning
After starting to upgrade ZMS, you will not be able to modify the configuration of other hosts until you have finished upgrading ZMS and the other hosts as well.

Steps:

Step 1. Update your Zorp Management Server to the latest revision of the Zorp version it is running as described in *Procedure 10, Updating a host to the latest Zorp 5 version (p. 12)*.

Step 2. Login to the Zorp Management Server and execute the following command: `/usr/lib/zms-upgrade-check`. If your ZMS database is not located in its default directory (`/var/lib/zms`), use the `/usr/lib/zms-upgrade-check <path-to-zms-database>` command. This utility checks the configurations stored in the ZMS database to prevent any problems during the upgrade. If the utility reports any problems, correct them (in there are no problems, the utility returns an empty prompt). If you need help in solving the problems, contact the BalaBit Support Team.

Warning
Do not proceed with the upgrade until you have solved all problems reported by zms-upgrade-check.

Step 3.

- If you have configured ZMS to automatically backup its configuration, verify that you have not modified your ZMS configuration since the latest configuration backup.
- If you do not have configuration backup from ZMS, create a backup now. For details, see *Procedure 13.1.2.1, Configuring automatic ZMS database backups* in *Zorp Professional 6 Administrator Guide*.

Step 4. Copy the latest configuration backup to your computer.

Step 5.

Warning
Hazard of data loss: every data stored on the Zorp Management Server will be irrevocably deleted (for example, log files, configuration files not managed from ZMS, and so on).

Reinstall your ZMS host. During the installation, select the **Zorp Management Server** role for this host. For details, see *Zorp Professional 6 Installation Guide*.

Step 6. Restore the configuration of ZMS. For details, see *Procedure 13.1.2.2, Restoring a ZMS database backup* in *Zorp Professional 6 Administrator Guide*.

Step 7. Upgrade Zorp Management Console (ZMC) on your desktop machines. ZMC is available on the Zorp 6 Installation DVD-ROM and on the BalaBit website at *http://www.balabit.com/network-security/zorp-gateway/support/upgrade/*.

Warning
Do not connect to ZMS 6 using ZMC 5.

The Zorp Management Client version 6 no longer supports the Windows XP operating system, as it has reached its End of Life. You can use ZMC on Windows Vista and later.

Step 8. Connect to your upgraded ZMS host using ZMC 6. When you connect to the upgraded ZMS engine for the first time with ZMC 6, a warning is displayed that the ZMS database must be upgraded. Click **Convert**.

Step 9. ZMC converts the configuration database to the 6 format. The main changes in the configuration are described in *Section 6, Main changes in the Zorp configuration (p. 9)*.

Step 10. Upload and restart the configuration of the ZMS host.

Step 11. Upgrade the other hosts of your Zorp Firewall System.

6. Main changes in the Zorp configuration

- The default number of processes (the number of CPU cores that the instance can maximally use) was decreased from 4 to 1. This change affects only newly created instances, existing instances are not modified.
- The deprecated PSSL class has been removed and converted to the new SSL configuration method.
- The deprecated VirusBuster search engine has been removed, configurations still using this engine have been updated to explicitly drop traffic with an error message referencing the removal.
- The Zorp Management Client version 6 no longer supports the Windows XP operating system, as it has reached its End of Life. You can use ZMC on Windows Vista and later.
- Zorp Professional 6 introduces Encryption policies that make encryption settings (including SSL/TLS settings, certificates, and so on) easily reusable between Services and firewall rules. Also, the Zorp SSL framework has been redesigned to make configuration easier and clearer, by allowing you to configure encryption settings based on the scenario you need, for example, ClientOnlyEncryption, ForwardStartTLS, and so on. For details, see *Chapter 3, The Zorp SSL framework* in *Zorp Professional 6 Reference Guide*, *Section 5.6, Module Encryption* in *Zorp Professional 6 Reference Guide*, and *How to configure SSL proxying in Zorp 6*.
- The **Zorp > Instance > Edit parameters > General > Thread stack limit** option has been removed. From now on, a Zorp process uses the default value of the stack size of the host (which is currently 8 Mb for Ubuntu 14.04 LTS). Zorp uses this memory only when it is actually needed by the thread, it is not allocated in advance, thus resident memory consumption and performance are not affected by the change.

7. Procedure – Upgrading a host to Zorp 6

Purpose:

To upgrade an existing Zorp installation to version 6, complete the following steps. Before starting the following procedure, read this entire section carefully. This procedure describes how to upgrade the operating system on a host of the Zorp Firewall System.

Prerequisites:

The configuration of every Zorp component must be uploaded and active on the host. Upload and reload every configuration change from ZMC before starting the upgrade. Also, check the general prerequisites described in *Section 2, Prerequisites to upgrading to Zorp (p. 4)*.

Download the Zorp 6 ISO file from MyBalaBit.

Steps:

Step 1. Make your new Zorp licenses accessible from the host you want to upgrade. The licenses can be installed from a local webserver via HTTP, or from a USB drive.

Warning
The directory structure of the webserver, floppy, or USB drive must be identical to the one of the Zorp License Media you received from BalaBit or your local distributor.

If you fail to install the new licenses during the upgrade, you must copy the license files to the host manually to the following locations:

- Zorp Management Server (ZMS): `/etc/zms/license.txt`
- Zorp Application Level Firewall (Zorp): `/etc/zorp/license.txt`
- Zorp Authentication Server (ZAS): `/etc/zas/license.txt`
- Zorp Content Vectoring Server (ZCV): `/etc/zcv/license.txt`
- NOD32 Antivirus engine: `/etc/nod32/license/`

Zorp and its components will not operate without the new license files.

Step 2.

Warning
Hazard of data loss: every data stored on the computer will be irrevocably deleted.

Reinstall the host. During the reinstallation, you will have to provide a One-Time-Password (OTP) that the host will use to connect to ZMS. Enter a password, and store it temporarily for later use.

For details on the steps of the installation, see *Zorp Professional 6 Installation Guide*.

Step 3.

Warning
Perform this step only after you have upgraded your Zorp Management Server and Zorp Management Console application to 6.

Step a. Login to your Zorp Management Server using ZMC.

Step b. Select the reinstalled host in ZMC, and click **Recovery connection**.

Step c. Enter the same One-Time-Password (OTP) that you set during the installation on the host.

Step d. Upload and reload the configuration of every component of the host.

8. Upgrading ZAS and ZCV

The Zorp Content Vectoring Server (ZCV) and the Zorp Authentication Server (ZAS) are upgraded as part of the Zorp upgrade.

When running on separate hosts from the Zorp Application Level Gateway, upgrading the ZCV and ZAS host is identical to upgrading other Zorp hosts as described in *Procedure 7, Upgrading a host to Zorp 6 (p. 9)*.

Warning
Content vectoring of the traffic and authentication of the users will not be possible during the upgrade. Perform the upgrade during maintenance hours, or if that is not an option for you, modify your Zorp policies accordingly for the duration of the upgrade.

9. Procedure – Upgrading Zorp clusters

Purpose:

To upgrade an existing Zorp cluster to version 6, complete the following steps. Before starting the following procedure, read this entire section carefully.

Warning
After beginning upgrading the current slave host, the HA functionality will not be available until all nodes are upgraded.

Prerequisites:

The configuration of every Zorp component must be uploaded and active on the hosts of the cluster. Upload and reload every configuration change from ZMC before starting the upgrade. Also, check the general prerequisites described in *Section 2, Prerequisites to upgrading to Zorp (p. 4)*.

Before starting to upgrade the cluster, upgrade your ZMS host as described in *Procedure 5, Upgrading Zorp Management Server to version 6 (p. 7)*.

Steps:

Step 1. Upgrade the slave node of the cluster as described in *Procedure 7, Upgrading a host to Zorp 6 (p. 9)*.

Warning
When uploading the configuration from ZMC, upload the configuration only to the slave node.

Step 2. Initiate a takeover on the upgraded slave node, and test it for some time. To initiate a takeover, login to the slave node, and issue the following command: `/usr/lib/heartbeat/hb_takeover`

Step 3. If the upgraded slave node is stable under your usual traffic, upgrade the master node. If you encounter any problems on the upgraded slave node, you can return the traffic to the master node that is running the not-upgraded Zorp by issuing the `/usr/lib/heartbeat/hb_standby` command on the slave node, or issuing the `/usr/lib/heartbeat/hb_takeover` command on the master node.

10. Procedure – Updating a host to the latest Zorp 5 version

Purpose:

Upgrading to Zorp 6 is supported only from stock Zorp 5 systems. The system must be up-to-date, the upgrading process will automatically stop if not the latest Zorp 5 packages are installed on the host.

To update a Zorp host to the latest version of Zorp 5, complete the following steps.

Steps:

Step 1. Login to the host as root from a local console or using SSH.

Step 2. Issue the following commands: `apt-get update; apt-get -u dist-upgrade`
The latest upgrades will be downloaded and installed. The result should state that there are no packages on the system that have to be updated or modified (that is, the last line of the output should be something like: *`0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded`*). In order to perform the upgrade to Zorp 6, any conflict or problem with the existing packages must be solved. This includes packages that were excluded from previous updates (that is, their version was locked, or on hold). The upgrade script automatically stops if it finds any packages that are on hold. Note that the above apt command might occasionally state that a package is on hold (also called "kept back") even if there is some other problem with a package.

Step 3. *Optional step*: To remove the hold flag from packages, complete the following steps:

Step a. Issue the following command to find the packages on hold: `dpkg --get-selections| grep hold > packagesonhold.txt`

Step b. Edit the `packagesonhold.txt` file (for example, using the `joe packagesonhold.txt` command) and everywhere change "hold" to "install".

Step c. Issue the following command as root: `dpkg --set-selections<packagesonhold.txt`