How to upgrade to Zorp Professional 7 (7.0)

Publication date March 04, 2024

BALASYS

Table of Contents

List of Procedures

Chapter 1. Preface

Welcome to Zorp Professional (Zorp) version 7 and thank you for choosing our product. This document describes the process to upgrade existing Zorp installations to Zorp 7. 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 7 product and its related components.

Chapter 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 7, 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 7 is supported from the latest revision of Zorp 6.

- 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 two accounts: a personal and a technical account. For details on creating these accounts, see *Chapter 5, Account requirements (p. 14)*. Note that the registration is not automatic, and might require up to two working days to process.
  The **Personal account** on *https://support.balasys.hu* will be required for the following:
  - Downloading the Windows and Linux installers of ZMC and ZAA.
  - Downloading the Ubuntu and Zorp installer media.

  The **Technical account** will be required for the following:
  - Downloading the binary (Debian) packages of Zorp, ZAS, ZCV, ZMS.
  - Downloading the URL filter database.

Chapter 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 7.

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

To upgrade an existing Zorp installation to version 7, 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 7 is supported from the latest revision of Zorp 6.

Chapter 4. Upgrading Zorp

The following sections describe the procedures for upgrading Zorp and its components.

4.1. Procedure – Updating a host to the latest Zorp 6 version

Purpose:

Upgrading to Zorp 7 is supported only from official Zorp 6 systems. The system must be up-to-date.

To update a Zorp host to the latest version of Zorp 6, complete the following steps.

Steps:

Step 1. Login to the host from a local console or using SSH. After the login, become root by using the `sudo su -` or the `su` command.

Step 2. Run the following command:

```
apt update
```

If the update is successful, run the following command:

```
apt -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
```

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 change `hold` to `install` everywhere.

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

4.2. Procedure – Upgrading your Zorp Firewall System to version 7 - an overview

Purpose:

To upgrade every host of a Zorp Firewall System to version 7, complete the following steps.

For details on upgrading a Zorp cluster, see *Procedure 4.7, Upgrading Zorp clusters (p. 11)*-

Note

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

Prerequisites:

Warning

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

To upgrade an existing Zorp installation to version 7, 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 7 is supported from the latest revision of Zorp 6.

Before starting the following procedure, read this entire document carefully.

Steps:

Step 1. Update your Zorp Management Server to the latest revision of Zorp 6, as described in *Procedure 4.1, Updating a host to the latest Zorp 6 version (p. 4)*.

Step 2. Update your Zorp hosts to the latest revision of Zorp 6, as described in *Procedure 4.1, Updating a host to the latest Zorp 6 version (p. 4)*.

Step 3. Upgrade your Zorp Management Server as described in *Procedure 4.3, Upgrading Zorp Management Server (ZMS) to version 7 (p. 5)*.

Step 4. Upgrade your other hosts as described in *Procedure 4.5, Upgrading a host to Zorp 7 (p. 9)*.

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

Step 6. If you encounter any problems, refer to the upgrade logs, or *contact the Balasys Support Team*.

4.3. Procedure – Upgrading Zorp Management Server (ZMS) to version 7

Purpose:

To upgrade a Zorp Firewall System to version 7, first the Zorp Management Server must be upgraded. Complete the following steps.

Prerequisites:

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

During the upgrade, the ZMS database must be converted to the new version. To prevent data loss, make sure to create a new backup of the ZMS database before starting the upgrade procedure.

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 too.

Before starting the procedure, read it thoroughly.

Steps:

Step 1. Update your Zorp Management Server to the latest revision of the Zorp version it is running as described in *Procedure 4.1, Updating a host to the latest Zorp 6 version (p. 4)*.

Step 2. Login to the Zorp Management Server and execute the following command: `/usr/lib/zms/zms-upgrade-check`. If your ZMS database is not located in its default directory (`/var/lib/zms`), use the `/usr/lib/zms/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 there are no problems, the utility returns an empty prompt.
- If the utility reports any problems, correct them. If you need help in solving the problems, *contact the Balasys 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 7 Administrator Guide*.

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

Step 5.

> **Warning**
> Hazard of data loss! All 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. For details, see *Zorp Professional 7 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 7 Administrator Guide*.

Step 7. Install the new version of Zorp Management Console (ZMC) on your desktop machines. ZMC is available on the Zorp 7 Installation DVD-ROM and on the Balasys download site at *https://download.balasys.hu/zorp-pro/7.0latest/cd/*.

> **Warning**
> Do not connect to ZMS 7 using ZMC 6.
>
> The Zorp Management Console version 7 no longer supports the Windows XP or Windows Vista operating systems, as they have reached their End of Life. You can use ZMC on Windows 10 LTS, Windows Server 2012R2, 2016 and 2019.

Step 8. Connect to your upgraded ZMS host using ZMC 7. When you connect to the upgraded ZMS engine for the first time with ZMC 7, a warning is displayed that the ZMS database must be upgraded. Click **Convert**.

> ⚠ **Warning**
> Hazard of data loss! The **Convert** operation is an irreversible change. Make sure that you create a new backup of the ZMS database before clicking **Convert**.

Step 9. ZMC converts the configuration database to the 7 format. The main changes in the configuration are described in *Section 4.4, Main changes in the Zorp configuration between 7 and 6 (p. 7)*.

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

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

4.4. Main changes in the Zorp configuration between 7 and 6

4.4.1. Predictable interface names

With the update of the base OS in Zorp 7, the network interface naming scheme has *changed*. The traditional interface names (for example, `eth0`) are not used anymore and the new network interface names depend on the properties of the network interface (for example, `enp2s0`). To determine the new network interface names, you will have to take different steps depending on whether you upgrade to Zorp 7 on the same machine or on a new one.

- *If you upgrade to Zorp 7 on the same machine*: Determine the MAC address of the machine.
- *If you upgrade to Zorp 7 on a new machine*: Refer to the *Ubuntu Server Guide*

The following two procedures describe the best practice of determining and saving the MAC address of the machine in Zorp 6 and then using it after reinstalling your hosts to Zorp version 7.

4.4.1.1. Procedure – Best practice: Saving the MAC address of the machine in Zorp 6 for later use in Zorp 7

Purpose:

To determine the MAC address of the machine in Zorp 6 so that you can use it after reinstalling your hosts to Zorp version 7, complete the following steps.

Make sure that you are still using Zorp version 6 during this procedure.

Prerequisites:

The **Networking** component in Zorp 6 must be in the **Running** state.

Steps:

Step 1. Login to the ZMS Engine with ZMC.

Step 2. Determine and copy the MAC address of a machine.

   Step a. Select a **Networking** component

   Step b. On the **Interfaces** tab, in the **Network interface configuration** list, select an interface that has `static` as the value of the **Type** column.

   Step c. Right-click on the interface and click **Status Details...**

   Step d. Select and right-click the value of the *`ether`* parameter and copy that value. This is be the MAC address of the machine.

   Step e. Click **Close**.

Step 3. Paste the MAC address of the machine.

   Step a. To edit the interface properties, under the **Network interface configuration** list, click **Edit**.

   Step b. In the **Description** field, paste the previously copied value (MAC address). Make sure to prefix this pasted value with `_MAC: _`. If there is a pre-existing value in the **Description** field, paste it before that value.

   Step c. Click **OK**.

Step 4. Repeat Step 2 and 3 for all `static` **Networking** interfaces.

Step 5. To commit your changes, click **Commit changes**.

Step 6. To upload your changes, click **Upload current configuration**.

Step 7. Navigate to **Configuration** and click **Mark as Running**. This will set the state of the **Networking** component to **Running** without having to **Reload** or **Restart** the networking service. Therefore, this procedure can be performed without service outage, because you have only changed the description of the interface, and this does not affect the operation of network interfaces.

4.4.1.2. Procedure – Using the previously saved MAC address from Zorp 6 after reinstalling your hosts to Zorp 7

Prerequisites:

Make sure that you have successfully installed a Zorp version 7 host and that you have connected it to ZMS

Steps:

Step 1. Login to the host through SSH:

```
ssh <your-hostname>
```

Step 2. To list all interfaces and their MAC addresses, enter the following command:

```
ip link show
```

Save this list, you will need it later during the procedure.

Step 3. Log out the host.

Step 4. Login to ZMS through ZMC.

Step 5. Select the **Networking** component on the host.

Step 6. On the **Interfaces** tab, in the **Network interface configuration** list, order the list by **Description**. To do this, click on the **Description** header of the table column.

Step 7. Edit the interface.

Step a. Find the first interface that you have listed with the `ip link show` command in the **Network interface configuration** list by the MAC address in the **Description** column.

Step b. Select the interface in the **Network interface configuration** list which MAC address matches to the first item in the list that you have listed with the `ip link show` command.

Step c. To edit the interface properties, under the **Network interface configuration** list, click **Edit**.

Step d. Copy the name of the first interface in the list that you have listed with the `ip link show` command

Step e. Overwrite the existing value of the **Name** field with this name.

Step f. Deselect **Stop interface before rename**.

Step g. Click **OK**.

Step 8. Repeat the substeps of the previous step for all `static` **Networking** interfaces.

Step 9. To commit your changes, click **Commit changes**.

Step 10. To upload your changes, click **Upload current configuration**.

Step 11. To restart the **Networking** component, click **Control service** and click **Restart**.

4.4.2. High Availability daemon

For Zorp clusters, a new HA component, *Keepalived* has been introduced. It generates configuration for the Keepalived software. It is a more modern approach for Virtual IP Address transition between cluster nodes.

Keepalived is now the supported daemon instead of *Heartbeat*.

Install *keepalived* package in cluster hosts with the following command. It is available in the main repository of Ubuntu Bionic.

```
apt install keepalived
```

4.5. Procedure – Upgrading a host to Zorp 7

Purpose:

To upgrade an existing Zorp host to version 7, complete the following steps. Please note that an OS-level upgrade from Zorp 6 to Zorp 7 is not supported.

Prerequisites:

Download the Zorp 7 ISO file from the download site at *https://download.balasys.hu/zorp-pro/7.0latest/cd/*.

Steps:

Step 1. The license of Zorp 6 is not working with Zorp 7, therefore you must acquire a new license from your sales contact. If you need futher assistance, please contact the Balasys Sales Team at `<sales@balasys.hu>`. Make your new Zorp licenses accessible from the host you want to upgrade. The licenses can be installed from a local webserver through HTTP, or from a USB drive.

> ⚠ **Warning**
> Zorp and its components will not operate without the new license files.
>
> The directory structure of the webserver or USB drive must be identical to the one of the Zorp License Media you received from Balasys 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 System (ZCV): `/etc/zcv/license.txt`
>
> Alternatively, you can manage the license files from ZMS by adding a **Text editor** component with the **Licences** template to the host:

Step a. Login to ZMS through ZMC.

Step b. Select the host that you want to use for managing the licences.

Step c. Select the host you want to add a new component to in the **Configuration** tree.

Step d. Navigate to the **Host** tab, and under the **Components in use** section, click **New**.

Step e. Select the **Text editor** component from the **Components available** list.

Step f. From the **Component templates** list, select the **Licences** template.

Step g. Click **OK**.

Step h. From the **Configuration** tree, select the **Licences** component.

Step i. To remove unnecessary license files from the component, select the obsolete license file and click ✖ **Remove file**. Click **Yes**.

Step j. To add the licence content, do one of the following:

- Click in the text box of the license file name and copy-paste the licence content from the licence file.
- Click **Insert file**, browse for the licence file. Click **OK**.

Step k. To upload your changes, click **Upload current configuration**.

Step l. Navigate to **Configuration** and click **Mark as Running**.

Step 2.

> ⚠ **Warning**
> Hazard of data loss! All 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 7 Installation Guide*.

Step 3. **Warning**
Perform this step only after you have upgraded your Zorp Management Server and Zorp Management Console application to 7.

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 configured during the installation on the host.

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

Step 4. To upload your the host configuration, click the arrow next to **Upload current configuration** and click **All**.

Step 5. Click **Shutdown** and then click **Reboot**.

4.6. Upgrading ZAS and ZCV

The Zorp Content Vectoring System (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 4.5, Upgrading a host to Zorp 7 (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.

4.7. Procedure – Upgrading Zorp clusters

Purpose:

To upgrade an existing Zorp cluster to version 7, complete the following steps. Before starting the following procedure, read this entire section carefully. The currently active cluster node will be referred to as `node1` in this section. The currently inactive cluster node is designated as `node2`.

Warning
After starting this procedure, the HA functionality will not be available until all nodes are upgraded.

Warning
After completing this procedure the HA functionality will by provided be *Keepalived* and the current Heartbeat configuration will be obsolete.

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 *Chapter 2, Prerequisites to upgrading to Zorp (p. 2)*.

Before starting to upgrade the cluster, upgrade your ZMS host as described in *Procedure 4.3, Upgrading Zorp Management Server (ZMS) to version 7 (p. 5)*.

Note
You can keep the current ZMS host to make sure that `node1` remains configurable after starting the upgrade procedure. In this case, install a new ZMS instance as described in *Zorp Professional 7 Installation Guide* and perform and upgrade as described in *Procedure 4.3, Upgrading Zorp Management Server (ZMS) to version 7 (p. 5)*.

Steps:

Step 1. Upgrade `node2` as described in *Procedure 4.5, Upgrading a host to Zorp 7 (p. 9)*.

Warning
When uploading the configuration from ZMC, upload the configuration only to `node2`

Step 2. Initiate a takeover on `node2` and perform a comprehensive test of the firewall services. To initiate a takeover, login to `node2`, and issue the following command: `/usr/lib/heartbeat/hb_takeover`

Step 3. *Optional step*: If you kept your previous ZMS installation, disconnect `node2`. As a result, if you modify the configuration on `node1` and you upload the changes to ZMS, it will not attempt to upload the changes to `node2`

Step a. Login to the not upgraded ZMS (version 6) with ZMC.

Step b. Navigate to **Management** > **Connections...**.

Step c. Select `node2`.

Step d. Click **Disconnect**.

Step 4. *Optional step*: If you kept your previous ZMS installation, tighten the local service rule (for details, see *Section 9.4, Local services on Zorp* in *Zorp Professional 7 Administrator Guide*) so that `node1` only accepts management connections from the corresponding ZMS (version 6) instance.

- Login to the kept ZMS instance with ZMC (version 6).

Step 5. Configure keepalived on `node2`.

Step 6. Stop Heartbeat on `node1`.

Step 7. Start keepalived on `node2`.

Step 8. Closing steps:

Step a. Perform a comprehensive test of the firewall services while `node2` is active. After the testing period is finished and you determine that the upgraded node is stable, start the following steps:

Step b. Upgrade `node1`.

Step c. Bootstrap `node1` from Zorp Management Server. For details, see *Procedure 13.3.4, Configuring recovery connections* in *Zorp Professional 7 Administrator Guide*.

> ⚠ **Warning**
> If you kept your previous ZMS installation, bootstrap `node1` from the newly installed ZMS instance (version 7)

Step d. Mark `node1` as the active node by perfoming a HA takeover.

Step e. Perform a comprehensive test of the firewall services while `node1` is active. After the testing period is finished and you determine that the upgraded node is stable, perform a standby on `node1`.

Step 9. On the Zorp Management Server:

Step a. Restore the Zorp Management Server database from the backup. For details, see *Procedure 13.1.2.2, Restoring a ZMS database backup* in *Zorp Professional 7 Administrator Guide*.

Step b. Connect to the Zorp Management Server with the Zorp Management Console.

Step c. To upload the host configuration to the host, click **Upload/All**.

Step d. Reboot.

Chapter 5. Account requirements

This section describes the details on the account types that will be required at certain points of the installation or upgrade process.

5.1. Personal account

You will need a personal account to access the following sites:

- download.balasys.hu
- upload.balasys.hu
- support.balasys.hu

The personal account is also used to download files manually.

To register a personal account, send an email to `<sales@balasys.hu>` with the following personal data:

- full name
- phone number
- company name
- job title

Note
During a product evaluation period, the Sales Department grants time-limited access rights for the personal account.

After closing a sales process, access is granted for the required number of employees of the organization and a technical account is created. For details on a technical account, see *Section 5.2, Technical account (p. 14)*

5.2. Technical account

You will need a *Balasys Support System* technical account to access the following sites:

- apt.balasys.hu

The technical account is not used for manual access, but for machine access. For example, it is used to upgrade Zorp hosts using apt.

Note
During a product evaluation period, creating a technical account is not possible.

After closing a sales process, a technical account is created automatically.