Backup and restore strategies

- Awingu 5.3.1
- Awingu 5.3.2
- Parallels Secure Workspace 5.4.0
- Parallels Secure Workspace 5.4.2
- Parallels Secure Workspace 5.4.4
- Parallels Secure Workspace 5.3.3
- Parallels Secure Workspace 5.5.1
- Parallels Secure Workspace 5.6.0

Resolution

All scenarios assume a restore to **exactly the same application and database version**.

Mind that a typical Parallels Secure Workspace environment consists of one or more appliances (virtual machines).

It's also important to check if Parallels Secure Workspace relies on an external database.

- This is always the case for multi-node environments.
- It is optional for a single-node environment; alternatively the single-node environment

For example: When restoring an appliance that is on version 5.6.0; the database scheme should also be 5.6.0.

All scenarios: before restoring

1. Consider taking a backup of the remaining infrastructure (if applicable).
2. Shut down every appliance that is still running.
   After a successful restore and confirming Parallels Secure Workspace is up and running again, delete them after this restore procedure.

Scenario 1: using backups or snapshots of virtual machines

Requirements

- A backup of the virtual machines is available.
- A backup of the external database (if applicable - see above).

Restoring

1. If applicable: Restore the backup of the external database.
2. Restore the backup(s) of the virtual machine(s) and boot them.
   For a multi-node environment, the nodes must use their original IP address.

Scenario 2: using an environment backup

Limitations

Mind that an environment backup does not include all data: metrics and shares (shared files) are not recovered when using this backup strategy.

Requirements

- A backup of the Parallels Secure Workspace environment.
- A new appliance: Download Parallels Secure Workspace appliance .
- A backup of the external database (if applicable - see above).

Creating the environment backup

If applicable: also back up the external database.
The environment backup itself does not include the external database.
If Parallels Secure Workspace uses an internal database, it will be included.

There are some different ways to create environment backups. It can be triggered manually (**System Settings > Global > Troubleshoot** and select the appropriate action) or through the API.

It's also possible however to schedule an automatic daily backup. Navigate to **System Settings > Global > Connectivity: Environment Backups** to adjust the settings. **SFTP** credentials can be specified here.

It's also possible to configure whether the vault should be backed up as well. Mind that this may lead to a very short service interruption for single sign-on (SSO) each time the daily backup is created. It's also possible to leave this disabled, in which case SSO will fall back to pre-authentication after restoring the backup.

Be sure to **regularly download these backups** using an SFTP connection to the appliance.

Restoring the environment backup

1. Prior to restoring:
2. Restore the database (if necessary).
3. Deploy a new appliance. Note: the version must be equal to the one that generated the environment backup.
4. Start the installation wizard by surfing to https://<workspace_appliance_ip>:8080/
5. After accepting the EULA, import the backup file.
6. Continue to follow the steps in the wizard. Information such as IP addresses, hostnames, and credentials of the appliance (and if applicable, external database) will be prefilled. It is possible to change these.
7. If this was a multi-node before: it is necessary to manually scale again, so deploy additional appliances and add them through **System Settings > Global > Service Management**.

Depending on whether there was a backup of the vault, it may also be necessary to reconfigure Single Sign-On (SSO).
