

Adding nodes for increased user capacity and high-availability / multi-node environment

- Parallels Secure Workspace

Resolution

Having a multi-node Parallels Secure Workspace configuration means there are more Parallels Secure Workspace appliances available to handle the workload of additional tasks such as a high number of RDP streams, drive actions, auditing, etc. when the environment is heavily utilized.

There is also a [reference video](#) available.

When setting up a multi-node configuration, there are certain things to immediately take into consideration:

- For a multi-node deployment, all TCP, UDP, and ICMP traffic should be allowed between the nodes. This traffic is not encrypted. Each node has an internal firewall only allowing traffic from other nodes (based on the IP address).
- Always use static IP addresses in a multi-node environment.

A two-node Parallels Secure Workspace cluster has no high availability (HA). If the first node goes down, there will also be an impact on the second node as there are no back-end roles available anymore at this time. A HA-capable set-up requires three appliances, each with back-end and front-end services (and an external HA database).

Although 10 nodes is not a hard limit, it's recommended not to go above 10 nodes in a single cluster. If more users are needed, it's recommended to set up a second cluster and connect this cluster to the same Microsoft Windows backend.

Due to reasons related to "split-brain" scenarios, it is recommended to distribute the back-end roles over three racks with a different power source.

The **front-end role** takes care of all RDP and file activity. There should be at least one appliance with this role. The more concurrent users there are, the more appliances there should be deployed.

The **back-end role** takes care of the auditing. In a multi-node deployment, there should be either **one or three back-end nodes**. No other combinations are allowed.

See [System requirements](#) .

Adding an additional node

1. **Install** an additional appliance as usual.
2. Configure the network settings (**static IP**) via the virtual machine console.
3. **Do NOT configure the appliance** (unlike the first appliance).
4. Log in as the built-in management user (local admin) on the already configured and running environment.
5. Navigate to **System Settings > Global > Service Management**.
6. Click **[Add appliance]**.

7. Select the discovered appliance or manually enter the IP address of the appliance.
Choose a hostname for this appliance. It cannot be the same as another appliance in the cluster.
Click **[Add]**.
8. The appliance will be added to the cluster.
Select **which services** should be enabled on this node: front-end and/or back-end services.
For back-end services, it's only possible to have this role installed on either one or three nodes per cluster.
9. Click **[Update]**.
10. After a short validation, there will be a pop-up where the changes must be confirmed.
Click **[Confirm]**.
11. A reconfiguration of the cluster will be triggered. **Do NOT reboot** any of the appliances during this process.
There will be a service disruption during the automatic cluster reconfiguration. This may take a while.
12. After the update is done, go back to the **Workspace** and open the **Dashboard** application (only available to administrators).
 - ◆ On the status page, the new appliance should be listed, and the installed services should be green.

Parallels Secure Workspace will do some internal load balancing on RDS sessions etc. However, if there is a requirement for load balancing the initial connections (and login to the Parallels Secure Workspace environment), an external load balancer needs to be used.

Backup strategy for multi nodes

It is always a good practice to regularly back up the Parallels Secure Workspace environment, especially before upgrades. If the hypervisor allows consistent live snapshots, it's possible to use that feature.

If consistency is not guaranteed, then create a snapshot/backup as follows:

- For **back-end** nodes: Perform this procedure on each node:
 - ◆ Shut down one node.
 - ◆ Snapshot/backup the node.
 - ◆ Start the node.
 - ◆ Wait until all services in the Dashboard are green.
 - For **front-end** nodes: It's possible to shut them down (and later restart) all at once.
 - When using an external database, use the snapshot feature of the database to create a consistent snapshot.
-