

Platform Connection Settings G4

This White Paper is only applicable for Prelude and Nemesis G4 series, which uses Proxmox as the virtualization layer. It also assumes that the audience has knowledge in virtualization and basic understanding of Proxmox.

Although Prelude and Nemesis G4 series should come with preconfigured settings to connect the workspace to the hypervisor, certain units were shipped without those settings. This white paper gives instructions to configure them.

Overview

The Connection Settings found in the Workspace's System > Settings > Platform > Virtualization page requires the following parameters:

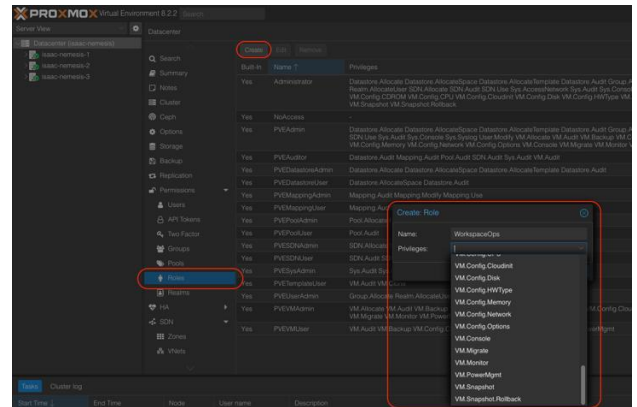
- **Hostname/IP address** This is the address to reach the hypervisor.
- **Username** This is the user used to create the token (see below).
- **Token** A token with the appropriate permissions (see below).
- **Secret** The secret is automatically generated upon the token creation.

Prerequisites steps

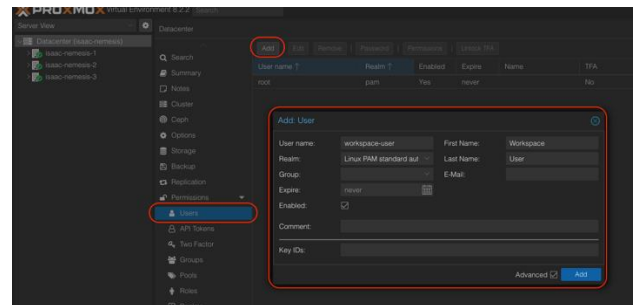
Prior to generating the Token and Secret used for the connection, a few steps need to happen:

- Connect to Proxmox hypervisor (the procedure for identifying the connection address can be found in the Prelude or Nemesis series Quick Start Guide).
- Create Roles e.g. Workspace-1, with at least the following permissions ⁽¹⁾ for each path in the table below:

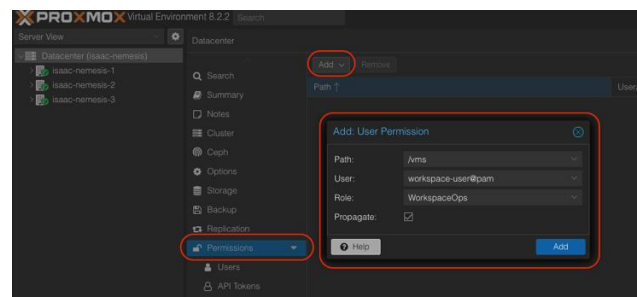
Path	Role	Permissions
/	Workspace-1	Sys.Audit Sys.Modify Sys.Console
/nodes	Workspace-2	Sys.Audit Sys.PowerMgmt
/storage	Workspace-3	Datastore.Audit
/vms	Workspace-4	VM.Audit VM.PowerMgmt VM.Snapshot VM.Snapshot.Rollback



- Create a user e.g. workspace-user in the PAM realm (the user doesn't need to belong to a group), as the token relies on the associated user permissions.



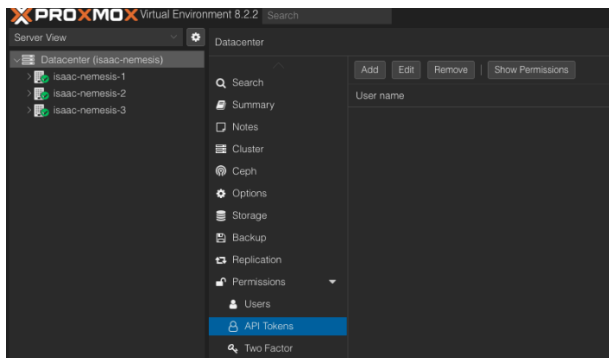
- Create a User Permissions for each path listed in the table with the following parameters:
 - Path: <path-x>
 - User: `workspace-user` (example above)
 - Role: <role-x>
 - Propagate: checked



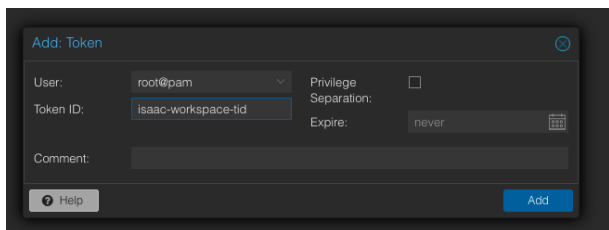
Steps to generate the token

While the prerequisite steps may be done once, generating the token and the secret may be done several times, if the intent is to change the token regularly. Note that in this case, the settings will have to be changed in the Workspace as well.

- Connect to Proxmox hypervisor (the procedure for identifying the connection address can be found in the Prelude or Nemesis series Quick Start Guide).
- Select the Datacenter top node on the left pane, and then Select API Tokens menu under Permissions.

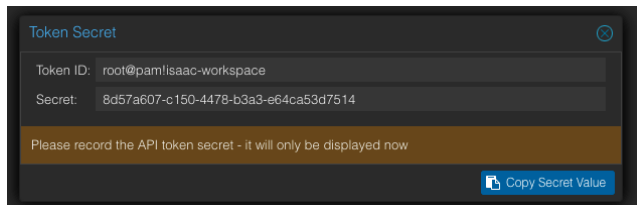


- Click Add, and enter the following parameters:



- **User** The name of the user defined in prerequisite steps.
- **Token ID** An id/name for the token. It can be as a GUID format or a human readable format, however, it's better to restrict alphanumerical letters and dash.
- **Privilege Separation** Uncheck this option (the Token will then rely solely on the user's permissions).
- **Expire** Optionally define an expiration date if the intent is to change the configuration regularly.
- Click the **"Add"** button.

- When the validation dialog opens, take note and secure the Secret associated with the token.
IMPORTANT: Please record the API token secret - it will only be displayed here.



(1) In Proxmox, permissions are given to a user, a group or a token, based on a path to resource(s), with one or multiple roles (a series of access rights) defining the permissions on that path. Multiple pair [path, roles] can be given to a user, group or token.