**How to access the EGI VMOps dashboard**

To access the EGI VMOps dashboard, you need to:

1.) [Obtain a personal X.509 access certificate](https://www.eugridpma.org/members/worldmap/) from a recognised Certification Authority (unless you have one already).

2.) Join an existing VO, or form a VO if none of the existing ones suit your purpose:

* The [fedcloud.egi.eu](https://perun.metacentrum.cz/cert/registrar/?vo=fedcloud.egi.eu) Virtual Organisation serves as a test ground for users to try the EGI cloud and to prototype and validate applications. It can be used for up to 6 month by any new user.

3.) Check the fedcloud entitlements in the user’s certificate subject DN. User should check whether his/her DN is available through the **distinguishedName** attribute when logging in using Check-in. If not, there are generally two alternatives for a user to include their DN when logging with Check-in :

Direct sign-in:

User links their X509 DN to their EGI SSO account by visiting <https://sso.egi.eu/admin/user> from a browser with access to the certificate. Uses will then be able to sign into the AppDB dashboard via Check-in using EGI SSO.

Sign-up for EGI ID:

* User visits <https://aai.egi.eu/signup> using EGI SSO and follows the registration process (requires email address verification before registration can be completed).
* User visits <https://aai.egi.eu/registry> and requests to “Link new identity” as described here [1].
* It’s important to select “IGTF Certificate Proxy” as the additional identity provider.
* After the linking process has been completed, the user needs to re-login to <https://aai.egi.eu/registry> using “IGTF Certificate Proxy” as their identity provider to link their DN to your EGI ID. The user will then be able to access the VMOps dashboard with the required fedcloud entitlement using either the “EGI SSO” or the “IGTF Certificate Proxy” identity provider.

[1] <https://wiki.egi.eu/wiki/AAI_usage_guide#Linking_Additional_Organisational.2FSocial_Identities_to_your_EGI_Account>