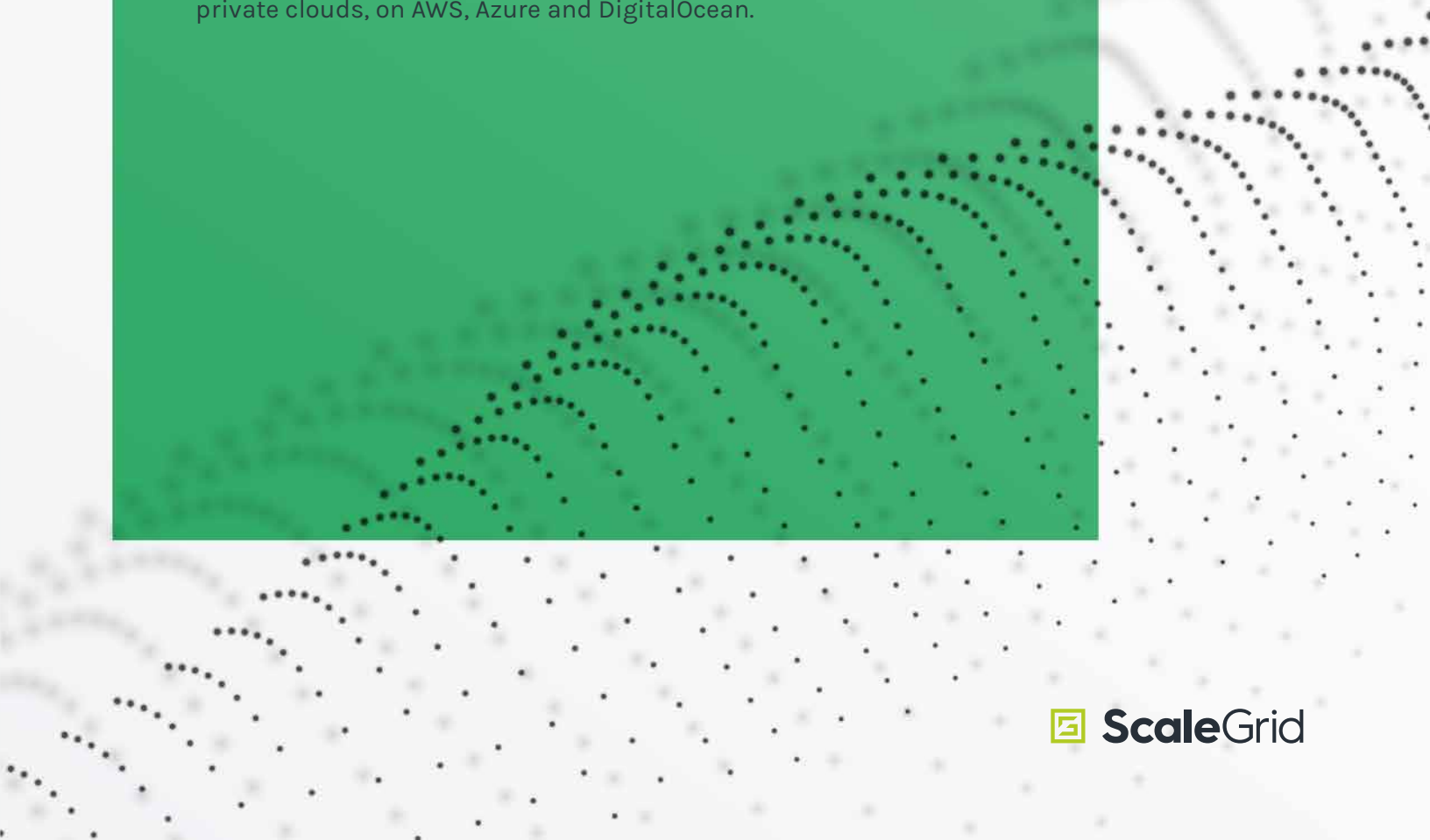
DBaaS

SECURING YOUR MONGODB CLUSTERS WITH SCALEGRID.

ScaleGrid Database-as-a-Service (DBaaS) solution is a fully managed MongoDB and Redis hosting and monitoring platform for public and private clouds, on AWS, Azure and DigitalOcean.



ScaleGrid

SCALEGRID SECURITY OVERVIEW

At ScaleGrid we take the security of your data very seriously. In this document, we detail the various security constructs available to secure your databases hosted or managed by ScaleGrid. If you have further questions please contact us at support@scalegrid.io.

DATABASE & NETWORK SECURITY

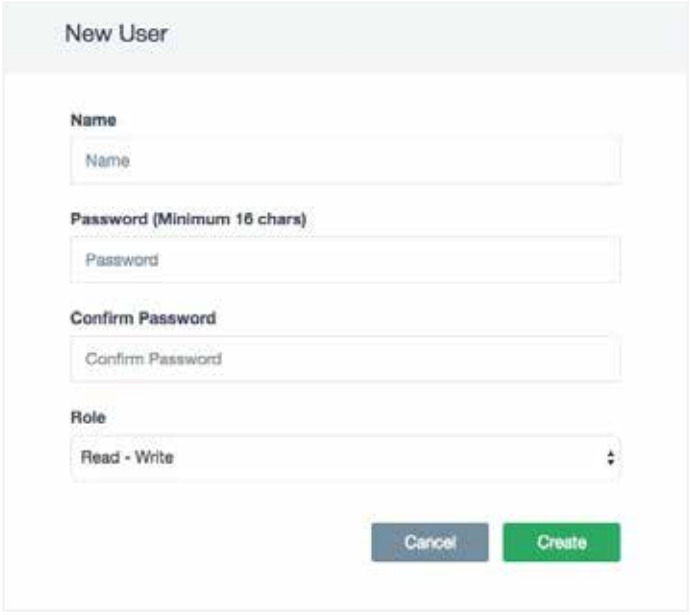
AUTHENTICATION

All MongoDB clusters created with ScaleGrid have "Authentication" enabled, so a username and password combination is required to connect to the cluster.

Users can be created on the 'admin' database or they can be created on any of the custom application databases. By default, ScaleGrid creates an 'admin' user on the 'admin' database. This user is a 'root' user and should only be used for administrative purposes. A sixteen (16) character random password is generated for the admin/admin user and can be reset on request.

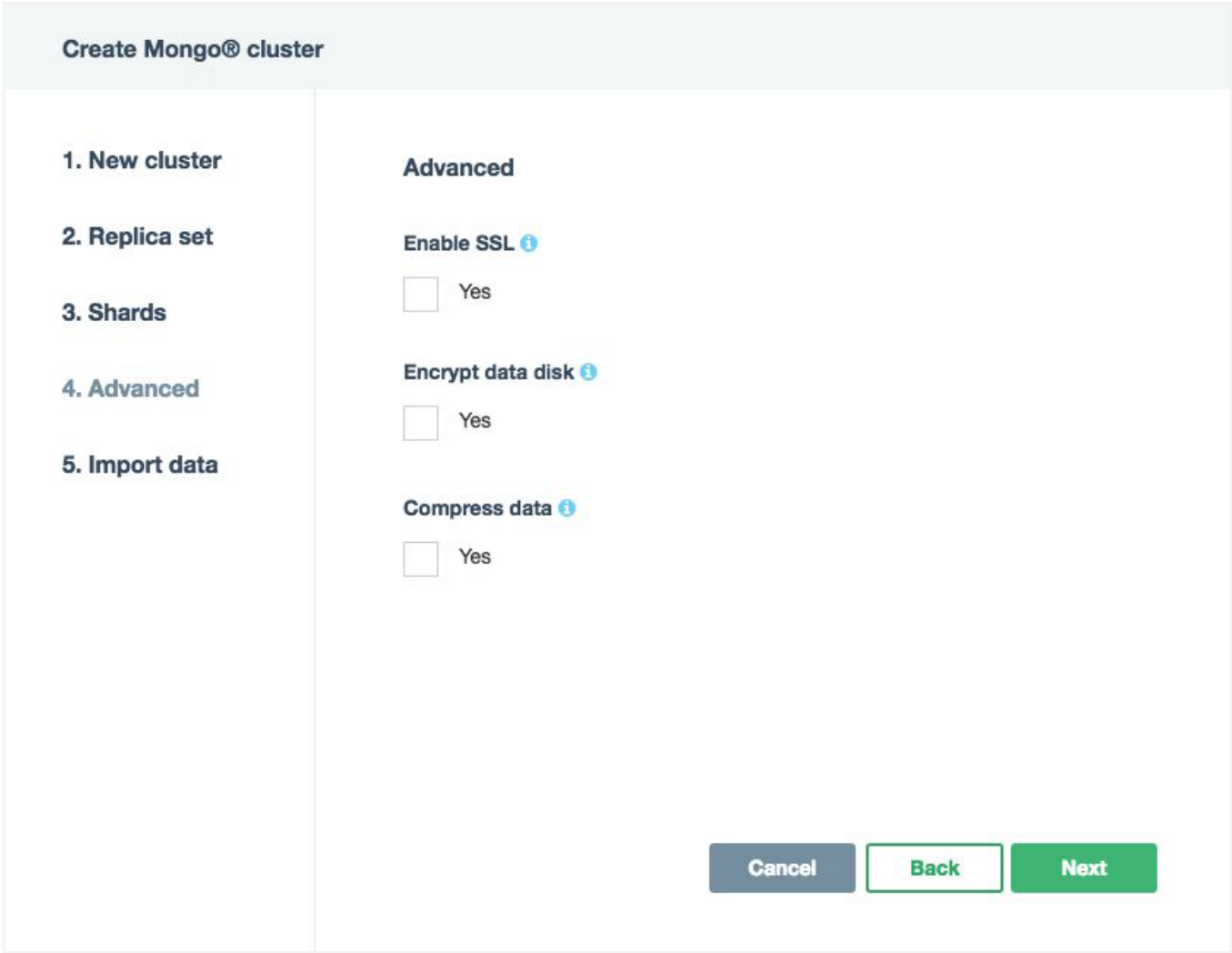
Application-level users should typically be created on a particular database. You can also specify the permissions you need for each user (Read/Write etc).

You can create custom MongoDB user roles to reflect the permissions needed by various roles in your organization. The ScaleGrid web UI allows you to add users with 'ReadOnly' and 'ReadWrite' roles. For more custom roles you need to use the mongo command line. More details here: Getting Started with User Management in MongoDB



ENCRYPTION IN TRANSIT: SSL

ScaleGrid provides you the option to encrypt your MongoDB data "in transit" using SSL. The "SSL" option can only be selected during the creation time of your cluster. Once selected, MongoDB is deployed in "requireSSL" mode, which requires SSL on all inbound connections. Replication traffic between the MongoDB replicas is also encrypted with SSL.



By default, self-signed certificates are installed during the creation of the cluster. There are two other options available to configure your SSL certificates:

1. Bring your own certificates – You can bring your own wildcard certificates and install them on the servers.

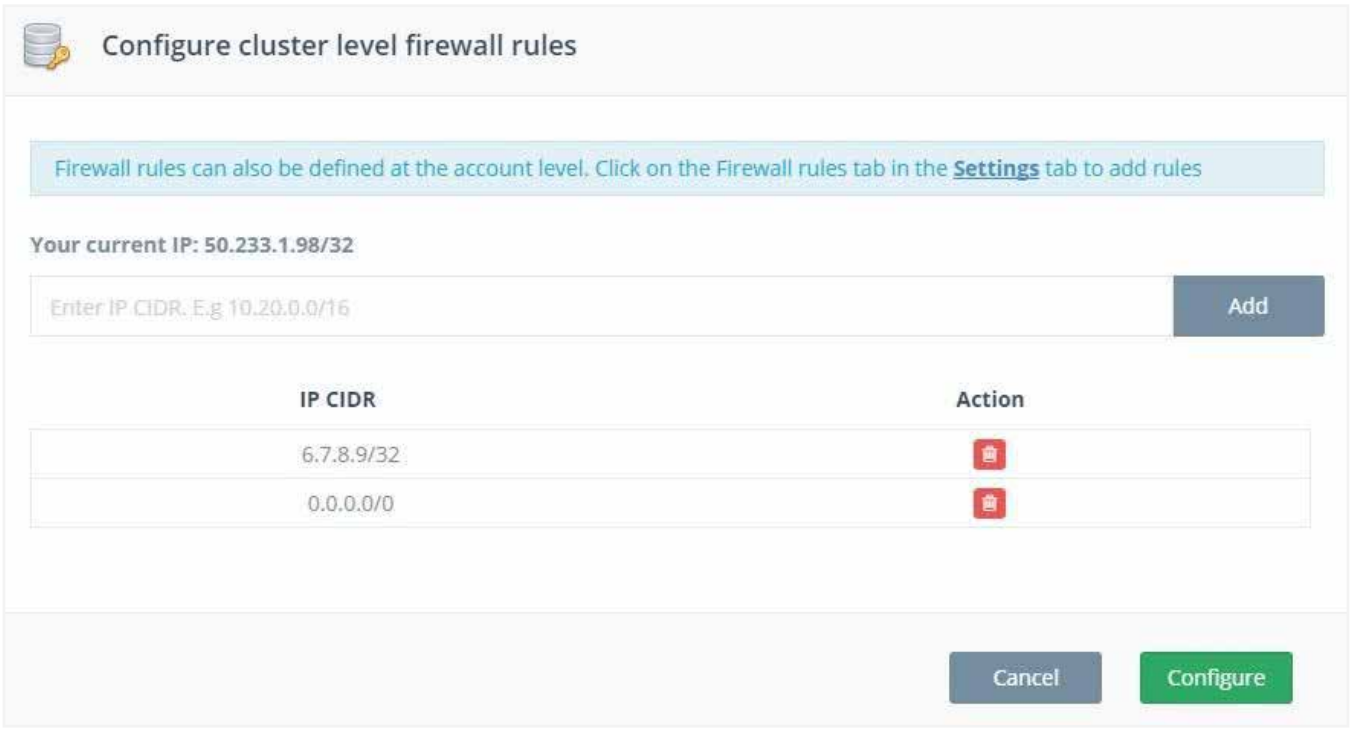
2. Public SSL certificates – You can purchase public SSL certificates for your servers. The certificates cost $80/server/year.

FIREWALLS

In this section, we'll highlight the three different options available to lock down access to your MongoDB servers using firewall configurations.

1 IP Whitelists

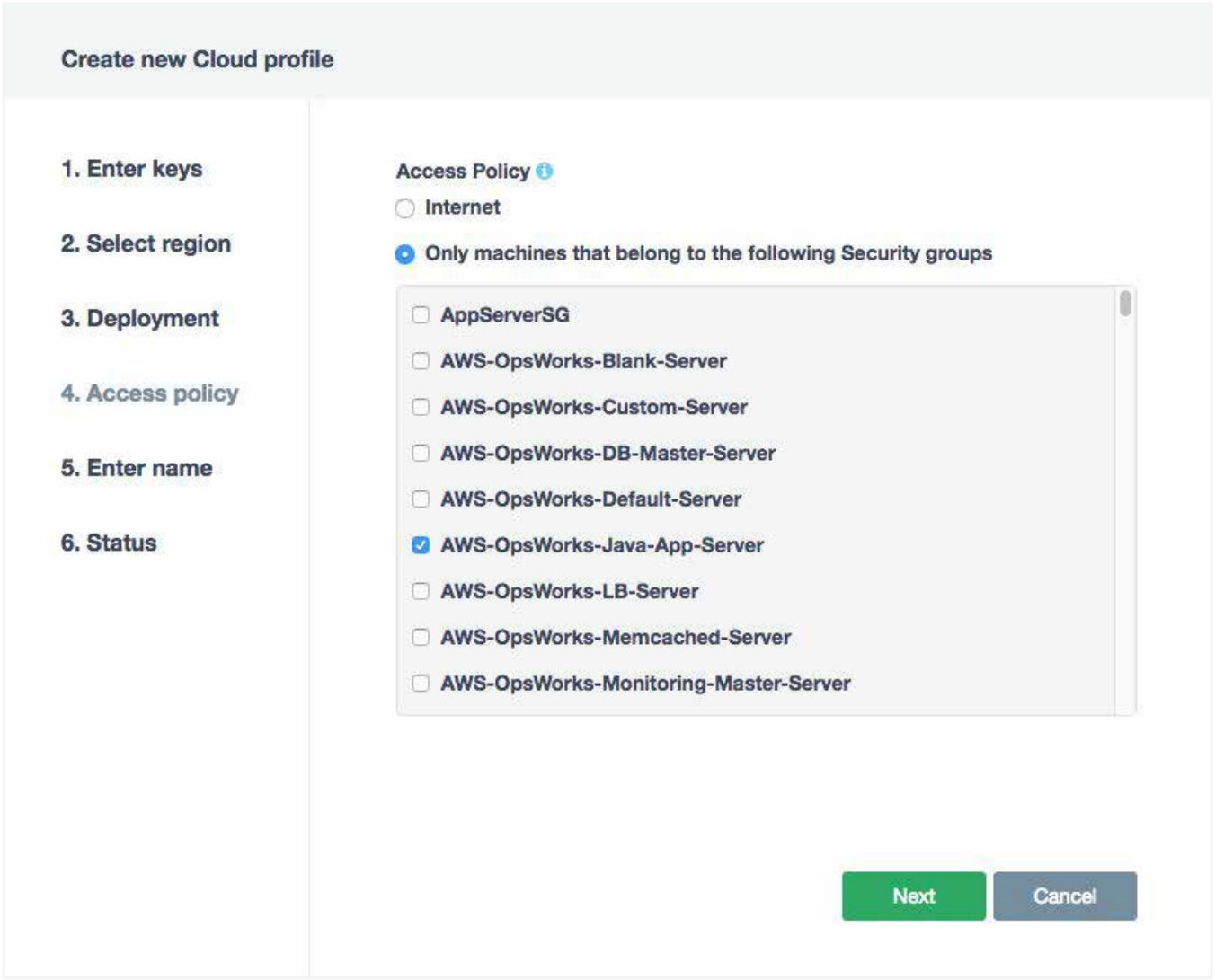
You can lock down access to your MongoDB servers using an IP whitelist. Administrators are able to restrict access of the MongoDB servers by specifying a list of IP CIDR. The IP whitelist can be specified at the cluster level or at the account level to apply rules across all clusters deployed in the account.



The IP whitelist option is available only for clusters open to the Internet. For other configurations, we recommend you use other options like AWS Security groups or Azure Network Security groups outlined below.

2
AWS Security Groups

On AWS, our 'Bring Your Own Cloud' plans allow you to lock down access to your MongoDB servers to specific Security Groups to ensures your database servers are only accessible from servers in those groups. It also integrates the MongoDB firewall management with the rest of your AWS machines firewall management.



3
Azure Network Security Groups (NSG)

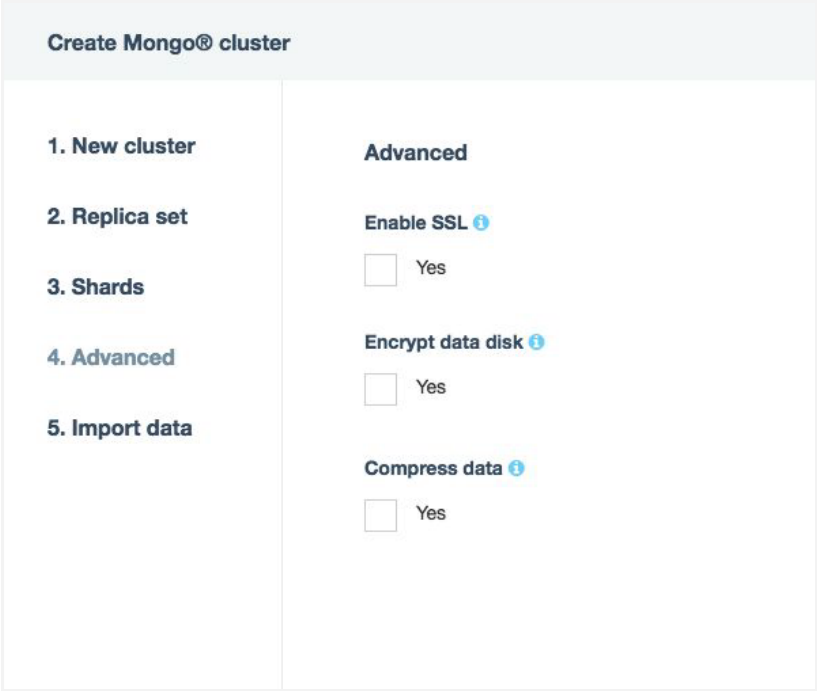
On Azure, our 'Bring Your Own Cloud' plans allow you to lock down access to your MongoDB servers to specific Network Security Groups (NSG). You can edit the NSG in Azure to lock down access to the MongoDB servers from the Azure UI.

ENCRYPTION AT REST

ScaleGrid supports encryption at rest by implementing volume-level encryption using Linux Unified Key storage (LUKS). LUKS is the standard for volume based encryption in Linux. More information on LUKS can be found in Linux Unified Key Setup. Here are the encryption parameters used by LUKS:

> Cipher:aes-xts-plain64, Key size: 256bit

The LUKS key encrypting keys are stored both on the ScaleGrid controller servers and on the database servers. The option to enable 'Encryption at rest' needs to be selected at the time when the cluster is created.



On the database servers, the keys are stored under root credentials and are used to mount the volumes when the server restarts. This ensures that the data volumes are encrypted and can only be mounted on the servers of this cluster.

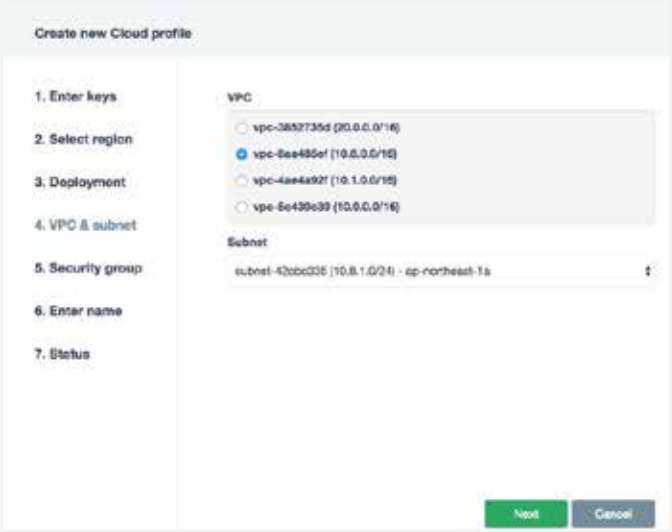
The encryption functionality typically increases the CPU load on the servers 20-40%, so testing should be done to understand the impact of encryption on your workload.

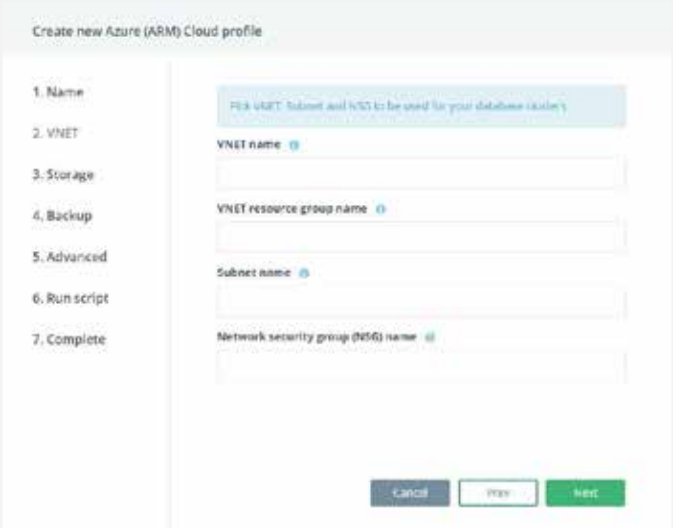
When 'Encryption at rest' is enabled, the backups are encrypted as well. This ensures that the backups can only be restored to the servers of this cluster.

PRIVATE NETWORKS

AWS VPC Support

On AWS, ScaleGrid supports deploying your MongoDB clusters in your own Virtual Private Cloud (VPC). Deploy your database clusters on private subnets - this enables you to isolate your databases in your own networks and not expose to the public Internet.





Azure VNET Support

On Azure, ScaleGrid supports deploying your MongoDB clusters in your own Virtual Networks (VNET). This enables you to isolate your databases in your own network and not expose to the public Internet.

OS PATCHING

Database clusters managed and hosted by ScaleGrid are patched on a monthly basis. The clusters are typically patched on the last weekend of the month, and only security related patches are installed. A custom maintenance time window can also be specified for the patching operation.

You are also able to trigger an on-demand OS patching job from the ScaleGrid console. The OS patching is performed on a “rolling” basis – one server at a time is patched and brought back into operation. This allows the entire cluster to be patched without any downtime.

WEB CONSOLE SECURITY

Two-Factor Authentication

Two-factor authentication can be enabled for access to your ScaleGrid console account to implement an additional layer of security over your username and password. Any application that supports time-based One-Time Password (OTP) protocol may be used. The most popular application used by our customers is the Google Authenticator App.

Here are the steps to enable Two-factor authentication:

Login to your ScaleGrid console: https://console.scalegrid.io

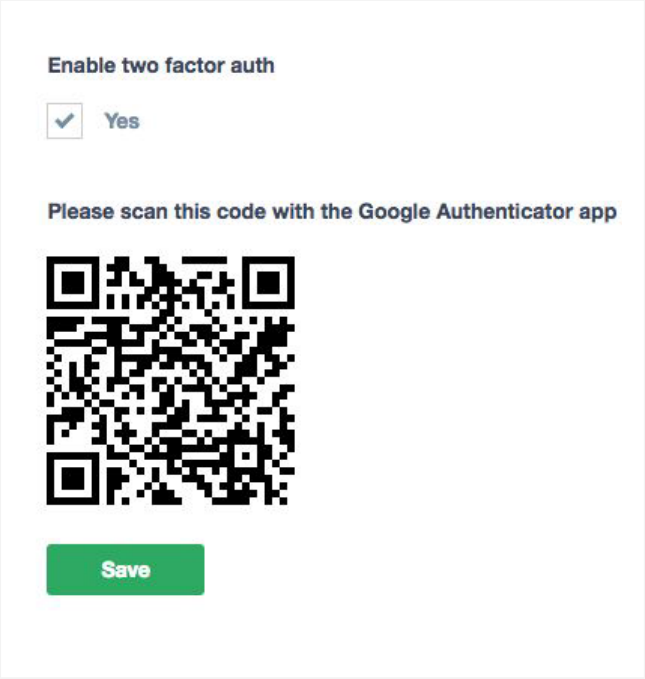
Navigate to the Settings tab.

Click two-factor authentication in the tab on the left.

Enable two-factor authentication by scanning the QR code in the Google Authenticator App.

Save the settings.

Logout and log back in to validate that two factor authentication is working.



If you have any further questions about securing your database server setup on ScaleGrid, please contact us at support@scalegrid.io.