ScaleGrid **Infrastructure Security**

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 INFRASTRUCTURE

This document details the various infrastructure components of ScaleGrid including production, non-production and support. The associated security infrastructure for each of the above categories is summarized below. If you have further questions, please contact our experts at support@scalegrid.io.

IT INFRASTRUCTURE

ScaleGrid IT infrastructure includes development, testing machines and workstations used by the ScaleGrid team. These machines do not handle or participate in any production workloads.

MACHINES & NETWORK

ScaleGrid does not use any physical servers and our IT infrastructure is deployed on Amazon EC2 across multiple regions. AWS Virtual Private Cloud (VPC) is used to configure a private network space for ScaleGrid machines.

All ScaleGrid non-production servers and workstations are Windows servers deployed in Amazon EC2. Direct remote desktop access is not allowed to any of the machines, and remote desktop access is achieved through the VPN server. Additional configurations:

- All machines are domain-joined and managed with Group policy
- All servers are configured to auto-lock idle screens in 120 seconds

AUTHENTICATION

Authentication for ScaleGrid employees is set up using Active Directory (AD) hosted in AWS Directory Service. All workstation and VPN logins are based on Active Directory accounts.

VPN ACCESS

All access to ScaleGrid machines is over VPN. The authentication for VPN is provided by Active Directory (AD). Two-factor authentication is also configured, and all employees are required to use two-factor authentication before they're granted access to our IT infrastructure.

OS PATCHING

All ScaleGrid workstations (Windows server and client) are configured to automatically download and install all appropriate patches every 7 days.

ANTIVIRUS

Antivirus is installed on all ScaleGrid workstations. The antivirus software used is Microsoft Security essentials and Windows Defender.

FIREWALL

Windows firewall is enabled on all the machines. Only the necessary ports for development and testing are opened.

EMAIL INFRASTRUCTURE

ScaleGrid uses Google (Gmail) as our email provider. All employees are required to enable two-factor authentication on their Google account.

TICKETING INFRASTRUCTURE

ScaleGrid uses Zendesk as our ticketing provider. All employees are required to enable two-factor authentication on their Zendesk account.

VULNERABILITY & SCANNING

ScaleGrid uses Qualys for periodic scanning of IT infrastructure for vulnerabilities. The Qualys appliance is installed and configured on the ScaleGrid VPC and it periodically scans all the assets and sends reports. Our IT team regularly monitors these reports, and when a new vulnerability is detected, the appropriate changes are made to the underlying infrastructure to address the vulnerability.

PRODUCTION INFRASTRUCTURE

PRODUCTION SERVERS

ScaleGrid production servers use Amazon Linux and are hosted in the AWS US-East-1 and US-East-2 regions. The production machines are located in a separate AWS account from the ScaleGrid non-production machines.

FIREWALL

ScaleGrid production systems and Support Console are locked down using firewall rules. The ScaleGrid firewall configuration is implemented using AWS Security Groups.

Production systems and support console can only be accessed from "lock boxes". Access to the "lock boxes" is restricted using Active Directory authentication and firewall as explained in the Support Infrastructure section.

ANTIVIRUS

No antivirus is installed on production systems.

OS PATCHING POLICY

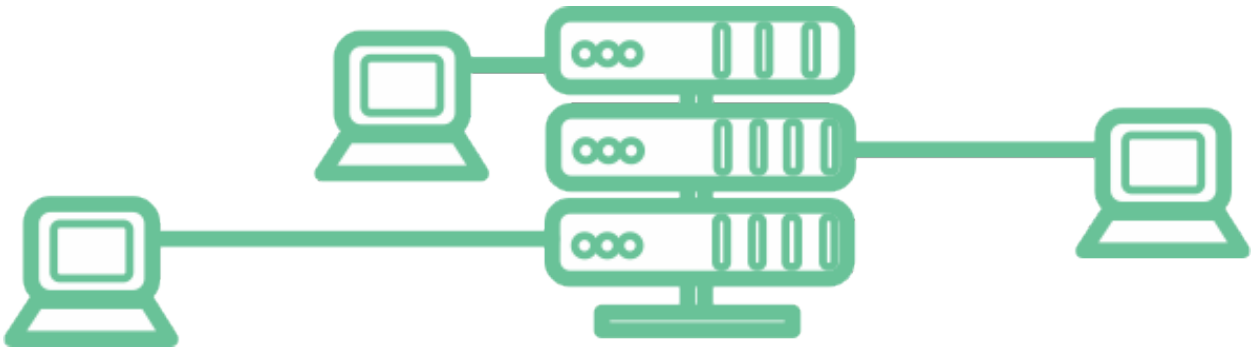
Internet-facing production servers (Amazon Linux) are patched once a month or on-demand as needed by Tier 3 support.

BACKUPS

ScaleGrid backups are implemented using periodic EBS snapshots. The snapshots are also copied to a second region for availability of backups.

CLOUD ACCOUNTS

All ScaleGrid production cloud accounts (AWS, DigitalOcean, and Azure) are enabled with two-factor authentication.



SUPPORT INFRASTRUCTURE

SUPPORT TIERS

ScaleGrid employees use a custom 'Support Console' to actively provide customer support. The Support Console software is part of the production software deployed at scalegrid.io, and access of the support team to the production system is based on three tiers. Support tiers are actively managed whenever an employee exits or has a change in their work assignment.

Tier 01	Tier 1 support handles support tickets, alert review, communication and scheduling. They can also suggest solutions to common problems based on our historical support data, but do not have access to production data. Tier 1 only has access to the ticket console, and are located both in the United States and India.
Tier 02	Tier 2 support is able to run certain predetermined tasks on the system if deemed necessary. E.g. run the restart service task on a server, reboot server, etc. Tier 2 employees do not have access to production data, but can review database logs to troubleshoot common problems. Tier 2 support is located both in the United States and India.
Tier 03	Tier 3 support has full access to production data. At this point, Tier 3 access is restricted to US-based employees only. If deemed necessary, support Tier 3 employees can SSH into the database machines and run commands or connect to the MongoDB cluster directly.

ADDITIONAL SUPPORT CONSOLE SECURITY REQUIREMENTS

All support accounts are accounts on the ScaleGrid production system.

1) Two-factor authentication needs to be enabled for all ScaleGrid support accounts. This is in addition to the two-factor authentication that is enabled for VPN access.
2) Access to the Support Console is locked down to certain whitelisted IP's. At this point, the Support Console can only be opened from ScaleGrid controlled "lock boxes".
3) "Lock boxes" are deployed in the ScaleGrid IT VPC in AWS.
4) Access to the "lock box" is controlled using AD authentication and firewalls.

EMPLOYEES

BACKGROUND CHECKS

Background checks are performed on all ScaleGrid employees hired in the United States. The background check involves the following checks:

- Criminal history
- Education history

TRAINING

ScaleGrid has commissioned Wombat Security to provide periodic security training for employees.

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