



Information Security

From the Experts at
Scale Computing

Table of Contents

- Preface 3
- Security: Inherent Design 3
- True Hyperconvergence..... 3
- Software Development Lifecycle 4
 - Trusted Software 4
 - Automated Tests..... 4
 - Rapid Response 4
- Custom-Built Storage Layer 5
- Isolated Networking 5
- Secure Management, Secure Data¹ 6
- HyperCore Access Control 6
- Scale Computing Fleet Manager Cloud Security 7
- Support In Your Hands 7
- Security In Summary 8



Preface

The security of your information and data is paramount to Scale Computing; all platforms must adapt quickly in order to be agile in their response to new threats in the security landscape. That's why security sits at the forefront of Scale Computing Platform's design, from the custom-built storage layer to the most current software patches and upgrades.

Scale Computing Platform delivers everything you need to manage your environment and removes what you don't. By eliminating additional clients, protocols, and other potential sources of licensing (costs) and frustrations (management), we also eliminate attack surfaces. This simplicity inherently increases the security of your infrastructure.

Remember [RFC 1925 - 12](#):

*In protocol design, perfection has been reached not when there is nothing left to add,
but when there is nothing left to take away.*

Security: Inherent Design

Scale Computing Platform was designed to provide highly available and scalable compute and storage services while maintaining operational simplicity through highly intelligent software automation and architecture simplification. Scale Computing tightly controls, reviews, and maintains all third-party and open-source software used within Scale Computing HyperCore; common vulnerabilities and exposures (CVEs) are monitored and patched as needed at the source-code level by Scale Computing employees (with no dependencies on outside third parties); and no root or privileged access is granted to end-users or other outside representatives.

Scale Computing has complete ownership and control over SC//Platform's design, the components included, and the updates applied to our products. Trusted Scale Computing engineers manage all software - not unreliable third-party entities or outsourced engineering teams. No root or privileged access is available to general users or outside vendors.

True Hyperconvergence

Some hyperconverged solutions leave hooks to plug in your own hypervisor and related management tools. This can be a complex and dangerous combination, especially concerning security management.

SC//Platform avoids opening the system to outside parties. First, the hypervisor and management tools are included in SC//HyperCore and locked behind the software and a built-in firewall. Second, and more critical, the entire virtualization layer is completely embedded into the system itself. There is no "controller" VM or VSA needed to access or manage the cluster.

Simply put, Scale Computing has created a true hyperconverged solution. SC//HyperCore does not rely on third-party software, high resource overhead, a running VM, or an easily accessible (and exploitable) file system to store and manage the system and data. This all has the added benefit of closing security threats from additional products, management tools, and protocols.

Software Development Lifecycle

Scale Computing has purpose-built our engineering and development team the same way that we have purpose-built our product. While we do leverage a carefully curated set of open source packages, all software we develop is developed in-house by full-time Scale Computing employees.

Trusted Software

Scale Computing HyperCore is the foundation of SC//Platform. It is the hypervisor for Scale Computing clusters and bundles a variety of adapted open source and proprietary, intelligent software to create a simplified operating system. Custom-built utilizing KVM architecture to integrate with the Scale Computing Reliable Independent Block Engine (SCRIBE) storage layer directly, SC//HyperCore makes virtualization and software automation look easy—and it is.

The software self-monitors and self-heals in almost all scenarios.

We utilize a unique development and testing process at Scale Computing, combining common Scrum and Kanban processes as necessary to work with and maintain multiple branches of code for current releases as well as new releases in development. With this method, the development and product teams are able to release software updates to SC//Platform using the procedures described below, ensuring that all functionality and security are considered with each release.

Automated Tests

The quality assurance team and automated testing process are fundamental to ensuring product stability and security while maintaining a focused development team. There are hundreds of thousands of system and unit tests performed each week—all of which are under constant observation, review, and improvement to ensure a premier product in all aspects of security, stability, and performance.

We perform a specific set of automated and manual security tests with every release of every product we ship, including port scans, specific security scans, and penetration tests.

Rapid Response

This agile development environment and software interoperability open communication channels between the product, support, and engineering teams to create an innovative, trusted, and secure system that can actively benefit from customer feedback and respond quickly and easily to security needs.

When a security exploit is found, your data protection comes first at Scale Computing. As we are not dependent on third-party companies or vendors to create or test patches to ensure functionality, we can build and release a security patch to address core concerns when needed while we still ensure full-stack stability and compatibility in the process.

We constantly monitor upstream packages for vulnerabilities and deliver security patches as part of weekly releases of SC//Fleet Manager and monthly releases of SC//HyperCore.

Custom-Built Storage Layer

The Scale Computing Reliable Independent Block Engine (SCRIBE) is the storage management layer conceptualized, designed, and embedded in SC//HyperCore. SCRIBE treats all storage in the cluster as a single logical pool for management and scalability purposes. The real benefits of SCRIBE come from the intelligent distribution of blocks redundantly across the cluster to maximize availability and performance for the SC//HyperCore virtual machines.

SCRIBE is not a repurposed file system with the performance and security overhead introduced by local files or file system abstractions such as virtual hard disk files that attempt to act as a block storage device. SCRIBE inherently manages all data in a more secure fashion. Virtual disks storing customer data are not made accessible or mountable by the underlying operating system, command line, or external users via standard storage protocols. Additionally, limited information could be retrieved from a single SC//HyperCore cluster hard drive due to the system's block distribution and redundancy requirements.

Isolated Networking

Nodes running SC//HyperCore participate in two distinct networks—a public LAN network and a private backplane network. The LAN connection provides a path to the management interface and virtual machines, including tagged VLAN packets directed only to specified virtual NICs to allow for virtual network isolation. The internal firewall will drop any traffic trying to reach the node directly; access is only allowed to the HyperCore UI on the LAN network. No traditional external storage protocols (such as iSCSI or NFS) are available to access virtual machine data. This provides further layers of security by not exposing unnecessary ports or opening the cluster to potential protocol exploits.

The backplane connection is for intra-cluster communication only, and has additional security measures to the internal firewall already in use. The backplane bond is prevented from being assigned an IP in the same subnet range as those of the LAN IPs (to ensure the backplane IPs are isolated on the network as an additional security measure). In SC//HyperCore, for nodes with four network ports, two are reserved to physically separate the backplane network from the public LAN network. In nodes with one or two network ports, the backplane network utilizes a tagged VLAN for logical isolation of backplane traffic.



Secure Management, Secure Data¹

The term hyperconvergence means different things to different people. In the broadest sense, it means combining core infrastructure components such as compute, storage, and networking in an easy-to-manage system.

At Scale Computing, hyperconvergence means that we own and manage the stack at all levels—storage, hypervisor, operating system, hardware, management, monitoring, and more. We understand that we are your infrastructure, and we take great care in ensuring that we are aware of the impact that can be felt anywhere in the stack by changes made to the product.

Minimizing the number of packages installed on an SC//HyperCore cluster limits the attack surface. And the packages that are used are monitored for CVEs and updated in a timely manner.

HyperCore Access Control

SC//HyperCore access is browser-based HTTPS for security and supports user-generated certificates if desired. Built-in replication for disaster recovery utilizes 256-bit AES encryption to secure the SSH connection transporting data between SC//HyperCore clusters. The replication connection also requires the HyperCore UI password to authenticate access to the target location in order to initiate the remote connection.

Access to the HyperCore UI and REST API is restricted to authenticated user accounts that can be maintained locally on each cluster or centrally by leveraging OpenID Connect (OIDC) integration for Single Sign-On.

HyperCore Role-Based Access Control (RBAC) allows specific user accounts to be restricted to performing very specific tasks and actions. For example - certain accounts can be “read-only” allowing view/monitoring access to the HyperCore UI (and REST API) only - with no ability to create new VMs, delete or modify existing VMs or cluster settings. Other accounts might be established strictly for backup purposes - for example in conjunction with third-party backup products such as Acronis that integrate with SC//HyperCore via API.

Create User [X]

Username []

Full Name []

Password []

Confirm Password []

Role [Customize]

NOTE: Read role is automatically supplied for custom roles

- Backup
Clone, Export, Import, Add/Pause Replication to a VM, Create/Delete snapshots, and Create/Delete/Modify snapshot schedules.
- Cluster Settings
Create/Modify all settings within Control Center, except for User Management and Control (system/cluster shutdown).
- Cluster Shutdown
Shutdown the system/cluster and any running VMs.
- VM Create/Edit
Import VMs and Create, Modify, Clone, and Add/Modify VM block (virtual disk) and network devices.
- VM Delete
Delete VMs and their associated snapshots and devices.
- VM Power Controls
Start, Shutdown/Power Off, and Live Migrate VMs.

OK

¹ Data Compliance Regulations: Various markets and sectors require different compliance regulations. Scale Computing does not access personal information about our customers' end-users, and therefore is not subject to sectoral laws that may govern that information, such as HIPAA or GLBA. However, Scale Computing takes security seriously and makes every effort to meet industry security standards. Always review your required compliance rules to ensure you are meeting or exceeding the terms.

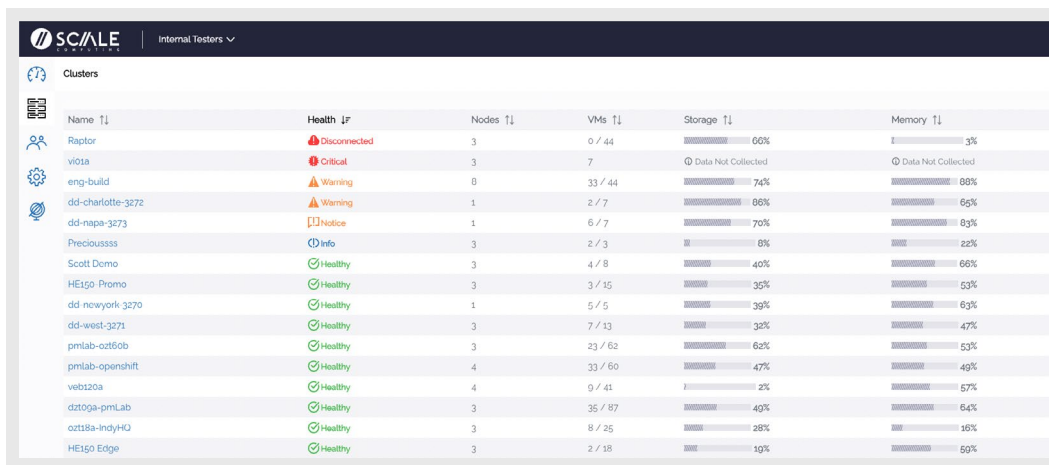
Scale Computing Fleet Manager Cloud Security

Scale Computing Fleet Manager assists with the management of clusters using cluster-initiated (outbound) 2-way SSL communication via ports 443 (ssl) and 8883 (mqtt) to `api.scalecomputing.com` and `broker.scalecomputing.com`. Data is only accessible to customer-authorized SC//Fleet Manager users and designated Scale Computing Support personnel. SC//Fleet Manager communication is not required for SC//HyperCore to fully function and take self-corrective-action, and access to SC//HyperCore cannot be granted via SC//Fleet Manager.

Access to SC//Fleet Manager is restricted to authenticated role-based user accounts. Authentication is handled by Google's Firebase, which stores passwords securely in such a way that even Scale Computing cannot access them. This also enables easy authentication via Google SSO or Microsoft Azure AD, for enhanced security.

SC//Fleet Manager's Role-Based Access Control (RBAC) restricts user accounts to performing specific tasks and actions. For example, certain accounts can be "Cluster Viewer" allowing view/monitoring access to the organization's clusters only, with no ability to add new clusters or update the firmware.

SC//Fleet Manager is securely hosted on fault-tolerant infrastructure with a major USA data center provider, and data is securely backed up in case of the need for quick disaster recovery with little to no data loss. Access to this infrastructure and the data is limited to a handful of trained, authorized employees of Scale Computing and is always treated according to the strict standards of our privacy policy (never shared, never sold).



Name	Health	Nodes	VMs	Storage	Memory
Raptor	Disconnected	3	0 / 44	0%	3%
vi01a	Critical	3	7	Data Not Collected	Data Not Collected
eng-build	Warning	0	33 / 44	74%	88%
dd-charlotte-3272	Warning	1	2 / 7	86%	65%
dd-napa-3273	Notice	1	6 / 7	70%	83%
Precioussss	Info	3	2 / 3	8%	22%
Scott Demo	Healthy	3	4 / 8	40%	66%
HEIgo Promo	Healthy	3	3 / 15	35%	53%
dd-newyork-3270	Healthy	1	5 / 5	39%	63%
dd-west-3271	Healthy	3	7 / 13	32%	47%
pmlab-oct60b	Healthy	3	23 / 62	62%	53%
pmlab-openshift	Healthy	4	33 / 60	47%	49%
web120a	Healthy	4	9 / 41	2%	57%
dztoga-pmlab	Healthy	3	35 / 87	40%	64%
oxttsa-indyHQ	Healthy	3	8 / 25	28%	16%
HEIgo Edge	Healthy	3	2 / 18	10%	50%

Support In Your Hands

In order to provide near real-time support for customers on SC//Platform, the Scale Computing ScaleCare Support team members will sometimes provide a code and ask for a "tunnel" to be opened for support access for the purposes of providing remote support.

Access to SC//HyperCore can be granted by a system administrator to ScaleCare Support utilizing the given code; ScaleCare Support is unable to initiate a connection to SC//HyperCore. This outbound-only connection can be revoked at any time from the web interface.

ScaleCare Support does not have direct access to any data within the virtual machines once a connection has been established. As there is no file system to navigate, data is stored in RAW virtual disk images with storage blocks distributed across the cluster. ScaleCare Support will only be able to monitor the self-healing functions of the cluster and manage other system services with your approval.

Security In Summary

SC//Platform has always had a focus on security, from the first concepts to the latest designs. SC//HyperCore and SC//Fleet Manager development are kept in-house by full-time Scale employees. Every aspect of SC//HyperCore: the custom SCRIBE storage management layer, the proven hardware, a field-tested and enterprise-capable hypervisor, automated testing, encrypted connections, password protected and encrypted replication, and more, combine to create a secure and contained solution with inherent security and control. Any open-source packages deployed as part of any Scale Computing software are tightly controlled.

The tight-knit, highly-skilled, and dedicated teams of engineers, product experts, and developers research, review, and refine all aspects of SC//Platform to ensure it meets the high standards Scale Computing requires for security, system stability, and management simplicity. Every decision is made with these core tenets in mind.

Scale Computing understands the importance of security foresight, preparation, and responsiveness in the shifting security field. As often as the laws and regulations change, and as quickly as the vulnerabilities to an organization can appear, SC//Platform and the team are ready to ensure your peace of mind.

Corporate Headquarters
525 S. Meridian Street - 3E
Indianapolis, IN 46225
P. +1 317-856-9959
scalecomputing.com

EMEA B.V.
Europalaan 28-D
5232BC Den Bosch
The Netherlands
+1 877-722-5359

