Information Security with HC3

White Paper

Technical Support and Resources

There are many technical support resources available for use. Access this document, and many others, at http://www.scalecomputing.com/support/login/.

Online Support

You can submit support cases and view account information online through the Portal at http://www.scalecomputing.com/support/login/. You can also Live Chat with support through www.scalecomputing.com during standard hours Monday-Friday 8 AM to 6 PM ET.

Telephone Support

Support is available for critical issues 24/7 by phone at 1-877-SCALE-59 (877-722-5359) in the US and at 0808 234 0699 in Europe. Telephone support is recommended for the fastest response on priority issues.

Professional Resources

Scale Computing offers many professional service options for both remote and on-site assistance in getting your cluster up and running quickly and knowledgeably. Contact your Scale Computing sales representative today to discuss our service offerings. Find additional information at http://www.scalecomputing.com/products/support/.

Document Version 1.4: 03/2017

Corporate Headquarters
5225 Exploration Drive
Indianapolis, IN 46241
P. +1 317-856-9559

West Coast Office
795 Folsom Street
Suite 1038
San Francisco, CA 94107

EMEA Office
Saunders House
52-53 The Mall
London
W5 3TA
United Kingdom

www.scalecomputing.com 1-877-SCALE-59 (877-722-5359)

Contents

Preface

The security of your information and data is paramount to Scale Computing. In order to be agile in the ever-changing security landscape, all technology platforms must adapt quickly. Threat vectors from new avenues are emerging on a daily basis.

Our culture has always been about having an exceptionally efficient and focused engineering team. A tight-knit, highly skilled team of engineers and developers cuts back on the red tape and delay that may be present in other organizations and keeps the focus on what matters in this ever-changing and always demanding landscape: innovation, stability, and security for the customer. In keeping with this culture, we have built the HC3 appliance using our own proprietary software in combination with common building blocks of well-tested open source technologies.

As newer endpoint security technologies evolve to isolate, identify, and mitigate risks, there will also be requirements for regulated industries that require specific infrastructure security and audit reviews. From the initial design to the custom-built storage layer and most current software patches and upgrades, the HC3 appliance has data security at the forefront.

Scale Computing has a focus on simplicity, stability, and security without compromising performance or design. We understand your data is integral to your business, and you can trust in the integrity and safety of that data on the HC3 appliance.

The laws and regulations often change as quickly as the vulnerabilities to an organization do, and it is important to be as prepared and educated as you can be in this shifting field.

Security: Inherent Design

As a hardened appliance and platform, HC3 delivers everything you need to manage your environment and removes what you don't. By eliminating additional clients, databases, and other potential sources of licensing (costs) and frustrations (management), we also eliminate the vulnerabilities of yet another protocol, product, IP address, or management interface.

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.

In the same sense, the simplification of the HC3 appliance has also greatly secured it. Scale Computing's HC3 appliance 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 manages and maintains all layers of the HC3 appliance. In conjunction with the patented Scale Computing software designed and built in-house, open source software is utilized to create the complete HC3 system. This means that there is no third party software, agent, or script in use on the HC3 appliance, and no root or privileged access to end users or other outside representatives.

Development Life Cycle

Scale Computing has purpose-built our engineering and development team the same way that we have purpose-built our product. By creatively participating in and leveraging open source technologies, we continue to develop and deploy innovative products with a much smaller engineering effort than a traditional in-house approach.

Patented software built in-house has been combined and folded with open source software to create the complete HC3 appliance. This includes core components like the **custom-built SCRIBE storage management layer**, the open source *KVM hypervisor*, and the Scale Computing designed, real-time state machine that allows the HC3 appliance to be self-monitoring and self-healing in almost all scenarios.

With a process centering around an agile work flow, we are utilizing common "scrum" and "kanban" tools as necessary to work and maintain multiple branches of code for current releases as well as new releases in development. This environment of constant change and interoperability opens communication channels between the product, support, and engineering teams to create an innovative, trusted, and secure appliance that can actively benefit from customer feedback and respond quickly and easily to security needs.

Trusted Software

We utilize a unique development and testing process at Scale Computing. While complex, this development process is paramount to ensuring security and stability in the product. This section is an abbreviated example of the code development process, but does provide a general review of the thorough suite of testing, approval, and consensus needed for new code to be considered for release in the HC3 appliance.

Due to the nature of how the HC3 appliance is designed, we have complete ownership and control over the components included and the updates applied to the system. The software is all managed by trusted Scale Computing engineers, not unreliable third party entities or outsourced engineering teams. There is no root or privileged access available to general users or other outside vendors.

In order to make a change to the existing code, a Scale Computing developer must first review the code to be changed. Then, a local sandbox must be used to work on the code and run any necessary tests. Once the intended changes have been completed and tested in the sandbox the new code is allowed to be queued for even further review.

When code is queued it triggers an automated review to ensure the code changes themselves will not break any existing automated tests that are designed to run on that branch of firmware in the quality assurance lab. Once confirmed, the queued code will trigger an alert to multiple other developers to manually review the new code sections for any issues. After developers have agreed the new code has no issues, and it has completed and passed the suite of automated tests in the quality assurance lab, the code is then put into the pool for potential release in upcoming software branches.

Automated Tests

The quality assurance team and automated testing process are fundamental to how we are able to ensure product stability and security while maintaining a focused development team. Combined, the quality assurance and development teams are able to run a barrage of tests against any new changes to ensure that all functionality is able to perform properly in a wide array of scenarios.

These tests include many different common failure scenarios, such as a drive failure, node failure, NIC failure, and others. The tests also monitor various workloads under stress, such as a high CPU load, high disk I/O queue, login storms, boot storms, and even more. All core functionality of the HC3 appliance must be able to run without error in all of these different scenarios before a new software branch can be added into the product. All new branches must be able to complete a sufficient amount of automated tests as well as run without failure in "soak" tests before being integrated into a software release for customer systems.

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.

Software Releases

New software, features, or patches on the HC3 appliance are not released on an individual basis. We have designed our update process to be built around regular, stable releases following the stringent testing process of new software branches described in **Trusted Software** and **Automated Tests**. This ensures that when applying software updates to the HC3 appliance (which are almost always non-disruptive or "rolling" updates) there is not a need to worry about another update coming only days later.

All code improvements are combined into a unified set once the necessary automated and manual tests have been completed to ensure stability and security. Utilizing field-proven, open source components we are able to monitor and selectively include sections from an approved software branch once we are sure patches are needed and/or desired. Using this method, the development and product teams are able to release software updates to the entire HC3 appliance and ensure that all functionality and security is considered with each release and at each level of the system. This ensures minimal interference for maximum results in the security and stability of your infrastructure.

Rapid Response

There is, of course, always an exception to this process of regular updates. When a security exploit is found, the security of your data comes first at Scale Computing. Our agile software development process is a boon in these rare instances.

Although all platforms will occasionally have security exploits found due to compliance with standards,

the design and intended use of the HC3 appliance has allowed the system to avoid many concerning exploits in recent time, such as the "Heartbleed OpenSSL" exploit and the "Shell Shock" vulnerability.

When the HC3 appliance may be impacted by a security concern, our process of automated testing and utilizing open source components allows us to quickly respond to any needs for a necessary security update.

For example, when the VENOM (CVE-2015-3456) vulnerability was found it was a potential security hole in most hypervisors. Although the vulnerability required a privileged user (which is locked down by design on the HC3 appliance), Scale Computing was still able to quickly address and release an update for this issue.

As we are not dependent on 3rd 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.

Secure Management, Secure Data

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, management, monitoring, and everything else. 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.

True Hyperconvergence

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

In the HC3 appliance, Scale Computing avoids opening the system to outside parties. First, the hypervisor and management tools are included in HC3 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 system.

Simply put, from top to bottom (so to speak), Scale Computing has created a true hyperconverged solution. At the top is the HyperCore software as a whole which includes the real-time monitoring, self-healing state machine and components of the KVM hypervisor. KVM has been part of the Linux mainline kernel for many years and has been extensively field-proven in large-scale environments, making it an ideal choice for the SMB market. At the foundation of the system is the proprietary SCRIBE storage management layer, discussed further in the next section.

Scale Computing does not rely on third party software, high resource overhead, a running VM, or an easily accessible 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.

Custom-Built Storage Layer

SCRIBE (Scale Computing Reliable Independent Block Engine) is the storage management layer conceptualized and designed by the Scale Computing team and embedded in the HC3 appliance. 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 HC3 virtual machines.

SCRIBE is not a re-purposed 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 like a block storage device. It does not store customer data in easily accessible files, folders, or shares. SCRIBE, as a block engine, manages all data in an inherently more secure fashion.

Customer data stored on VMs cannot be read from the command line. Additionally, limited information

could be retrieved from a single HC3 appliance hard drive due to the block distribution and redundancy requirements on the system. This is not the same as data encryption; find out more about data encryption options in the **Appendix**.

HyperCore integrates the SCRIBE storage pool directly into the KVM hypervisor. This means that virtual machines running on HC3 have direct block-level access to the SCRIBE virtual disks in the clustered storage pool without introducing the complexity and potential security overhead of using remote storage protocols or accessing remote storage over a network. Although the backplane network on the HC3 appliance is used to communicate data, you can read the benefits and security enhancements for the backplane network in **Dedicated Networking**.

Internal Firewall

All access to the HC3 appliance is browser based for security. The HC3 web interface is only available through ports 80 and 443. An internal firewall on all HC3 nodes ensures node access is limited to these ports. Any attempted access to the nodes in the system outside of these ports will be blocked.

As an example, all incoming SSH connections are blocked by default on the HC3 appliance. There is no incoming access available to the HyperCore operating system. Only an outbound SSH connection can be established from the HC3 web interface to the designated Remote Support server for real-time assistance from the ScaleCare Support team. This connection can never be initiated by ScaleCare Support. You, as the customer, have full control over access to your HC3 appliance. See **Live Support in Your Hands** for more information on Remote Support security.

Dedicated Networking

HC3 nodes have two distinct physical networks in which they participate—a public LAN network and a private Backplane network. All current HC3 nodes offer two ports for each of the LAN and Backplane networks, available in an active/passive bond to allow for full network redundancy.

The LAN connection provides a path to the management interface and virtual machines. Any traffic trying to reach the node directly will be dropped by the internal firewall; access is only allowed on ports 80 and 443 to the HC3 web interface on the LAN network. There are no external storage protocols (iSCSI or NFS) required to access virtual machine data. This provides further layers of security by not exposing unnecessary ports or opening the system to potential protocol exploits.

The Backplane connection is for intra-cluster communication only, and has additional security measures to those already in use on the LAN (the internal firewall). These additional security enhancements include blocking access to node ports, even those as common as 80 and 443, dropping packets from public IP ranges completely, and preventing the Backplane bond 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).

No outside access is available through the Backplane network to the nodes, not even if a machine were connected directly to the node through the Backplane NICs. Any traffic outside of the established and

authenticated HC3 system Backplane IPs will be dropped and disregarded. The Backplane is even stricter than the LAN connection in regards to security and access.

Having this separate private network through the Backplane secures data transfer between the nodes and allows easy adaptation for new or changing security measures by isolating data through switching, VLANs, and other networking means as needed.

As there is no external management server, "controller" VM, or other type of external "brain" required to access the HC3 appliance across a network link this adds additional security to the system. All management, monitoring, and access is web based and/or built directly into the HC3 appliance, creating a secure and self-contained appliance.

Live Support in Your Hands

In order to provide near real-time support for customers on HC3, Scale Computing ScaleCare Support team members will sometimes provide a code and ask for a "tunnel" to be opened for support access. This code is always unique and establishes a secure connection outbound from the HC3 appliance to the Remote Support server. Access to the Remote Support server is secured by several password-protected public and private keys for each ScaleCare Support engineer.

In the HC3 web interface the unique code can be entered to provide access to the HC3 node. Only a single code can be open at a time for each node. This code establishes an outbound SSH connection from the HC3 cluster to the Remote Support server using 256-bit AES encryption.

There are no inbound connections established from the Remote Support server to the HC3 appliance, and each node has a firewall that specifically prevents inbound SSH access. The connection to the Remote Support server can be closed at any time from the HC3 web interface and ScaleCare Support access will be disabled to the HC3 cluster.

ScaleCare Support does not have 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 distributed across the cluster. ScaleCare Support will only be able to monitor the self-healing functions of the cluster and manage other cluster services with your approval.

Security in Summary

The HC3 appliance has always had a focus in data security and stability, from the first concepts to the latest design of the system. Every aspect from the custom SCRIBE storage management layer to the real-time monitoring and self-healing state machine has been built with security and stability in mind.

The tight-knit, highly skilled, and dedicated teams of engineers, product experts, and developers research, review, and moderate all aspects of the HC3 appliance to ensure it meets the high standards Scale Computing requires for data security, system stability, and management simplicity. Every decision is made with these core tenants in mind.

Your data is integral to your business, and you can be confident in the integrity and safety of that data on the HC3 appliance. Trusted software, proven hardware, a field-tested and enterprise-capable hypervisor, automated testing, encrypted connections for live support, password protected and encrypted replication, a custom-built storage management layer, and more combine to create a secure and contained appliance with inherent security and control.

As often as the laws and regulations change, and as quickly as the vulnerabilities to an organization can appear, Scale Computing understands it is important to be educated, prepared, and responsive in the shifting security field. This is why the HC3 appliance always has data security and product stability at the forefront of every design decision.

Appendix: Further Recommendations

Account Security
The Scale Computing HC3 appliance is accessed through the HC3 web interface. Access is meant for members of the IT staff to use to manage the HC3 appliance and the virtual machines running on the system. Scale Computing recommends standard security administration practices such as:

- Using a secure password
- Keeping the password case sensitive
- Using numbers and letters
- Using special characters
- Regularly changing the password
- Only providing the credentials to necessary staff who need to manage the system
- If storing the credentials, doing so in a encrypted application

Data Compliance Regulations
Various markets and sectors require different compliance regulations. Depending on the implementation and your unique environment, the Scale Computing HC3 appliance can meet most compliance regulations, including but not limited to ISO standards and HIPAA standards. Always review your required compliance rules to ensure you are meeting or exceeding the terms.

Data Encryption
Although the design of the SCRIBE storage management layer provides some general protection for data stored on a single hard drive, it is not the same as data encryption. If data encryption is required it is recommended to use in-guest encryption tools to ensure data protection.

Network Security
The HC3 appliance allows for virtual machines running on the system to utilize separate VLANs from the assigned LAN network of the HC3 nodes. Scale Computing recommends isolating management of the HC3 appliance to a "management only" VLAN that is inaccessible to the rest of the network. This can be accomplished by making the LAN connections for the HC3 appliance VLAN "trunk" ports and tagging VLANs that you want virtual machines to run on. You can then use the built-in VLAN functionality to isolate the virtual machines onto separate VLANs.

Replication Security
The built-in HC3 replication utilizes 256-bit AES encryption to secure the SSH connection between two clusters, allowing secure replication to take place. The replication connection also requires the HC3 web interface password to the target location to initiate the remote connection.

If replicating between sites it is still recommended to utilize standard security best practices such as utilizing an encrypted VPN tunnel between the sites for the replication to take place.