RACKTOP

Security Hardening Guide for BrickStor SP

Version 1.0

Terms of Use and Copyright and Trademark Notices

Disclaimers

The Documentation and any information available from it may include inaccuracies or typographical errors. RackTop Systems may change the documentation from time to time. RackTop Systems makes no representations or warranties about the accuracy or suitability of any RackTop Systems-controlled website, the Documentation and/or any product information. RackTop Systems-controlled websites, the Documentation and all product information are provided "as is" and RackTop Systems disclaims any and all express and implied warranties, including but not limited to warranties of title and the implied warranties of merchantability and/or fitness for a particular purpose. In no event shall RackTop Systems be liable to you for any direct, indirect, incidental, special, exemplary, punitive, or consequential damages (including but not limited to procurement of substitute goods or services, loss of data, loss of profits, and/or business interruptions), arising out of or in any way related to RackTop Systems-controlled websites or the documentation, no matter how caused and/or whether based on contract, strict liability, negligence or other tortuous activity, or any other theory of liability, even if RackTop Systems is advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitations may not apply to you.

Table of Contents

Purpose

This guide will provide the procedures necessary to harden the BrickStor Security Platform to meet the most rigorous security requirements and operate within a specific customer environment. This guide has been used to achieve approval to operate in classified and unclassified government environments and will provide admins with all the steps necessary to securely connect BrickStor SP to the local infrastructure. The procedures in this document are a subset of steps listed in the general BrickStor SP Configuration Guide.

Background

The secure by design culture at RackTop includes security reviews as part of the product architecture. A security analysis is performed against implementations to detect security weaknesses and common security vulnerabilities.

RackTop uses automated scanning tools, such as Nessus, to continuously monitor, detect, and remediate vulnerabilities. RackTop is vigilant about preventing vulnerabilities from entering the product during the development and product delivery phases, while providing corrective configuration actions or updates to eliminate vulnerabilities in fielded products.

The system is already designed to be hardened and operate successfully in most enterprise environments. The steps in this document provide certain customizations that need to be made on a per environment basis to meet the specific operational requirements of the environment or changes in requirements.

Out of the Box

BrickStor SP is inherently secure by design and eliminates work for an admin to achieve approval to operate. The steps in this guide provide a quick reference for an admin to ensure that all of the settings are correctly calibrated to be in the most secure configuration and connected to environmental specific systems, such as the log repository, NTP time source, LDAP/Active Directory, etc.

Code Signing

RackTop secures software updates by providing signed code in a proprietary RAP format. Fielded systems validate the signature before installing the software update. BrickStor SP's Operating System will not allow unsigned binaries to persist a reboot to provide further protection against malware and advanced persistent threats. Firmware for RackTop provided hardware is also managed in a similar way using signed binaries to protect the authenticity and integrity of the software and hardware.

Vulnerability Patching

As part of the product lifecycle, the project management team tracks and reviews serious findings from vulnerability scans and security reviews. The project team ensures any findings are addressed with the highest development priority for security updates and product releases.

Read Only Boot Image

The boot image is a read only verified image and operates from memory. During a reboot, the system re-reads the image. Unsigned binaries will not persist a reboot.

RackTop Secure Architecture and Supply Chain

BrickStor SP runs BrickStor OS, RackTop's own proprietary UNIX operating system. The OS is compiled in accordance with the company's Software Secure Supply Chain procedures, which include 100% RackTop controlled US based code repositories, US based build and QA process, and a restricted code signing process which ensures software which is released to the public is authentic.

The operating system cryptographically validates the signature of the OS on installation and on boot. BrickStorOS is installed as an image, similar to firmware, and is read only.

The operating state of the OS is non-persistent so that each reboot returns the system to its original state. Customer data is kept separate from the operating environment.

BrickStor OS is not a general purpose operating system. It is designed to run and operate like a hardened black box appliance.

BrickStor OS does not allow end users to perform patch management. Updates and patches are delivered as a new OS image which the system boots into. Management of the OS is performed over HTTPS/REST and requires both authentication and authorization (via access Groups).

For further information regarding ports and firewall rules, refer to Hardening and Customizations.

Management data in flight is encrypted using TLS. Protocol data in flight is encrypted using AES256. Data at rest is protected for encrypted datasets using AES256. If using self-encrypting disks, data is also encrypted using a different set of keys on the disk itself.

RackTop Secure Supply Chain for Information Assurance

RackTop employs cybersecurity best practices throughout the entire product lifecycle from development, deployment, sustainment and system retirement.

RackTop provides company wide training to promote security awareness and foster an understanding of the risks facing the company and our customers. Additionally, RackTop fosters an environment where the software development organization understands the principles of secure software design.

The secure by design culture of RackTop includes security reviews as part of product designs and architectures. A security analysis is performed against implementations to detect security weaknesses and common security vulnerabilities.

RackTop uses automated scanning tools such as Nessus to continuously monitor, detect and remediate vulnerabilities. RackTop is vigilant about preventing vulnerabilities from entering the product during the development and product delivery process; and providing corrective configuration actions or updates to eliminate vulnerabilities in fielded products.

As part of the product lifecycle, the project management team tracks and reviews serious findings from vulnerability scans and security reviews. The project management team ensures they are being worked with the highest development priority for security updates and product releases.

RackTop secures software updates by providing signed code in a proprietary RAP format. Fielded systems validate the signature before installing the software update. RackTop's operating system will

not allow unsigned binaries to persist a reboot to provide further protection against malware and advanced persistent threats. Firmware for RackTop provided hardware is also managed in a similar way using signed binaries to protect the authenticity and integrity of the software and hardware.

Updates are provided to internet connected machines over a secure channel with certificate based authentication. For customers who do not have internet connectivity RackTop provides secure password protected access to a web accessible repository. Customers can securely import the software via their organizationally approved methods and upload it to their RackTop System to perform the secure update process.

RackTop understands the need for end-to-end security in both software and hardware. RackTop ensures that it orders original manufacturer’s authentic hardware through authorized manufacturers and distributors. To further improve security, RackTop always uses TAA compliant hardware and BAA compliant hardware whenever available.

RackTop employs FIPS Validated 140-2 Level 2 Self Encrypting Drives within its systems to protect the data at rest. The data on the drives are encrypted using a data encryption key that is never exposed to the user or an external application.

Cryptographic data purge features along with statements of volatility allow end user organizations to appropriate destroy and retire the information system. RackTop is continuously increasing the security and resiliency of the product to defend against evolving advanced persistent threats.

Hardening and Customizations

Administrative Accounts

Administrative Accounts can be configured to use Active Directory for authentication and authorization. If local accounts are required, users should be added and placed in the `bsradmins` and `allowssh` groups.

Password Restrictions

BrickStor SP enables admins to configure the strength and expiration of passwords. In addition, BrickStor SP prevents users from reusing the same password. Configure password strength for the system by editing the 'passwd' settings file:

```
vi /etc/default/passwd
```

Add the following entries with the appropriate values to the file:

```
MAXWEEKS=
MINWEEKS=
PASSLENGTH=
```

Log Forwarding

System Log

You can forward RFC-5424 compliant system logs to a log repository. Edit the following document with the proper end point:

```
vi /etc/rsyslog.d/remote.conf
```

Example UDP Configuration

```
*.* @192.168.1.123:514
```

Example TCP Configuration

```
*.* @@192.168.1.123:514
```

Then restart the `system-log` service:

```
svcadm restart system-log
```

User Behavior Activity Log

User Behavior activity can be forwarded to a SIEM or log centralization for off system processing and analysis. To configure User Behavior Activity to forward to another host, edit the following configuration file:

`/etc/racktop/ubcollectd/ubcollectd.conf`:

```
[Syslog]
Protocol = "udp"
Server = "<IP Address>:514"
CertFile = ""
Facility = "local0"
Enabled = true
```

File Protocols

SMB

BrickStor SP supports up to version SMB 3.0.2 and admins can enable, disable and require signing and protocol encryption. Signing can slow down client connections because it requires more communication between the client and server; however, newer SMB clients are faster because they have reduced the amount of communication responses.

The storage admin can also set a minimum protocol and a max protocol. The admin should set a minimum protocol of version 2.1 from the command line, using the following command:

```
sharectl set -p min_protocol=2.1 smb
```

Enable SMB signing and encryption by running the following commands:

```
sharectl set -p encrypt=enabled smb
```

```
sharectl set -p signing_enabled=true smb
```

By requiring SMB signing and encryption, BrickStor SP will refuse unsigned connections or clients that can not encrypt the protocol.

Require SMB signing and encryption by running the following commands:

```
sharectl set -p encrypt=required smb
```

```
sharectl set -p signing_required=true smb
```

NFS

Context Security Labels

From the myRack Manager user interface, admins can enable context security labels on version

NFS 4.2 to enable Mandatory Access Control (MAC). This can be configured on a per share basis or set globally from the command line to enforce it across all NFS shares. If using the system in an MLS environment, the minimum NFS server version should be set to version 4.2.

Minimum NFS Server Protocol

Admins can configure the minimum protocol to version 3, 4, 4.1, or 4.2 for BrickStor SP as an NFS server. From the command line, run the following command:

```
sharectl set -p server_versmin=<num> NFS
```

Example to set it to minimum version 4.1:

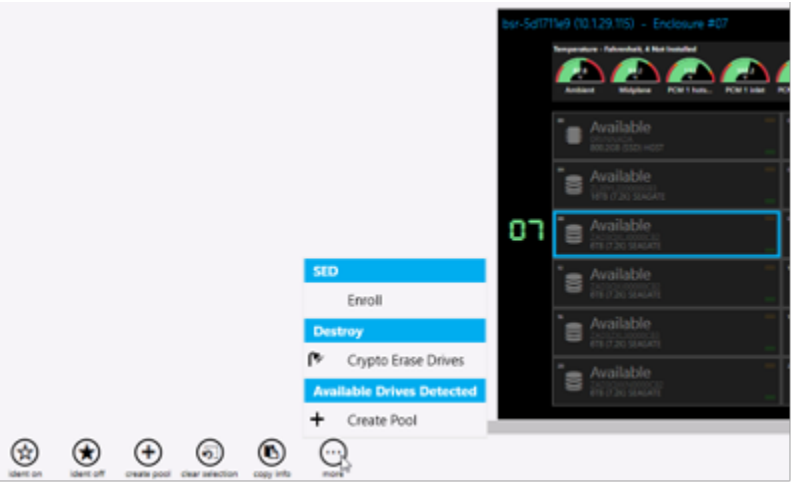
```
sharectl set -p server_versmin=4.1 NFS
```

Key Manager

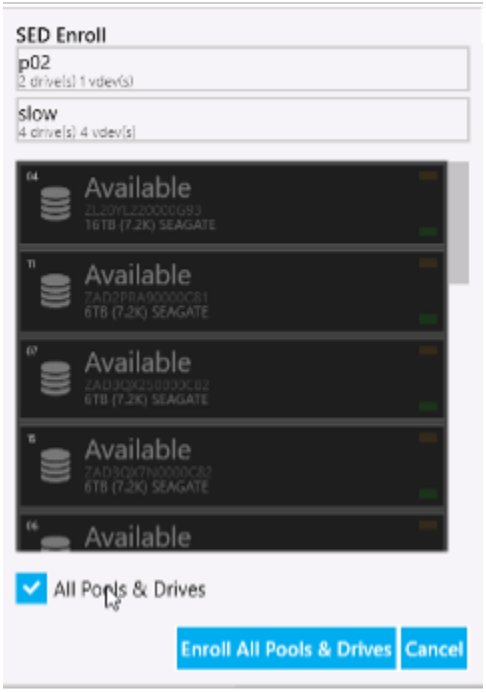
BrickStor SP's Key Manager can store the keys for Self-Encrypting Drives (SEDs) and dataset/volume encryption or be configured to an external key manager over KMIP. This must be configured before the use of SEDs or dataset encryption. The key manager should be configured from the command line, using `setup.sh` and following the menu prompts under menu option 8.

Data Encryption

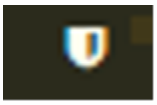
BrickStor SP supports two levels of FIPS encryption by using Self Encrypting Drives and dataset/volume level encryption. Self-Encrypting Drives must be enrolled into the system. Admins can use the myRack Manager Rack View.



Click on any of the drives in Rack View, select the more option, and then click enroll. Select all pools and drives.



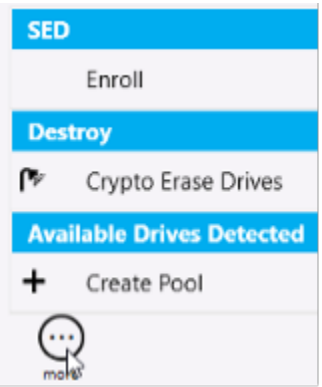
Once the drives are enrolled, they will display with a shield in the hardware view:



The shield indicates the drive is enrolled and the FIPS ownership process has been completed. Now the system will manage the drive encryption keys.

Media Sanitization

Drives can be crypto erased in compliance with NIST purge standards by selecting the drive(s) you wish to erase and selecting Crypto Erase Drives.



Data Replication

Data can be replicated to another pool or system on a per dataset basis. Data in flight is protected with TLS encryption. Datasets and volumes that are encrypted on the source will also be encrypted

on the destination. These datasets are not mounted or decrypted on the destination during normal operations. To recover a file or snapshot on the destination, the decryption keys for encrypted datasets and volumes must be imported on the destination system. Replication supports automatically forwarding keys and is configurable on a per dataset basis.

Telemetry Information

BrickStor SP includes features for sending telemetry data automatically to the myRackTop cloud for improved support. This information stream can be disabled with the following steps:

Edit the file `/etc/racktop/myrackd/myrackd.conf` and change the line below:

```
DisableMyrack = true
```

Then restart the `myrackd` service:

```
svcadm restart myrackd
```

Online Update Support

BrickStor SP checks for online updates daily for Internet connected systems. To disable this, perform the following steps:

Edit the file `/etc/bsrupdated/bsrupdated.conf` and change the line below:

```
DisableUpdateServer = true
```

Then restart the `bsrupdated` service:

```
svcadm restart bsrupdated
```

Timing

It is important to have consistent time across all systems for security and event logs. BrickStor SP should be connected to an NTP time source. By default, the system will look to Active Directory as the time source after a domain join. However, NTP can be configured to point to any compatible time source. The system will use the time source and time zone selected for all log Information. However, the GUI will adjust the times to the local time zone set on the desktop that launched the GUI.

Active Directory/LDAP

BrickStor SP can be joined to Active Directory and LDAP servers to support users and group permissions.

User Behavior Auditing

User Behavior Auditing can be enabled on a per dataset basis. The log provides the identity, source IP address, file path, file protocol, and operation. It also can provide permission changes.

Open Network Port Requirements

By default, the following ports are open to allow BrickStor SP to take advantage of various features and functionality. The following table lists these ports.

Table 1. BrickStor SP Open Network Port Requirements

Ports	Description/Service	Protocol	Direction	This port is open to/Purpose
22	SSH	TCP	bidirectional	Receive Management and Replication data
22, 8444, 8544	TCP Replication	TCP	outbound	Send Replication
25, 587	mail	TCP	outbound	send notification emails
53	DNS	UDP	bidirectional	Domain name Service
88	Kerberos	UDP	outbound	Authentication
111	NFS/rpc	TCP/UDP	bidirectional	NFS client access
123	NTP	UDP	bidirectional	Time synchronization
139, 445	SMB	TCP/UDP	inbound	SMB/CIFS client access
161	SNMP	UDP	bidirectional	Monitoring with SNMP
162	SNMP traps	UDP	outbound	Sending alerts to SNMP stations
389, 636	LDAP	TCP/UDP	outbound	Access to directory service servers
443	HTTPS	TCP	outbound	Call Home for Software Updates (https://myracktop.com)
443	HTTPS	TCP	inbound	RMM/iLO Out of Band Management
443	hiavd	TCP	outbound	High Availability Windows Witness

Ports	Description/Service	Protocol	Direction	This port is open to/Purpose
514	syslog	TCP/UDP	outbound	Logging
623	RMCP	TCP/UDP	inbound	HA Power/IPMI access
2049	NFS/portmap	TCP/UDP	inbound	NFS client access
2379,2380	confd	TCP	inbound	Configuration database
3205, 3260	iSCSI	TCP	inbound	iSCSI client/initiator access
4045	NFS/lockmgr	TCP/UDP	inbound	NFS client access
4746	hiavd	TCP	bidirectional	High Availability (between HA nodes)
5696, 8445	KMIP	TCP	outbound	Access to key management server
5697	keymgrd	TCP	bidirectional	Key replication/sync
5699	bsrlicensed	TCP	bidirectional	HA license check
8086, 8088	influxdb	TCP	inbound	Used for BrickStor SP Manager (charts)
80, 443, 8443	bsrapid	TCP	inbound	Used for BrickStor SP Manager (http/https)

NOTE ICMP echo (Ping) is required between all HA nodes, including the Witness.

NOTE Port 4746 for hiavd relates to the **first** instance of hiavd. If there is a second instance of hiavd running on a witness, then you need to unlock port 4747. The Nth instance of hiavd will be at port 4745+N, and so on. The same logic is used for confd.

NOTE Enable IPV4 ICMP echo ensuring all nodes in cluster can ping each other.