

Limiting Network Connections to Shares

To restrict access to specific shares, BrickStor uses Host based access controls to restrict access network level. This can be set through the sharing tab of the dataset

The screenshot displays the BrickStor management interface. On the left, a sidebar lists various datasets, with 'bsterling03 (10.2.22.197)' selected. The main panel shows the configuration for this dataset, divided into several sections:

- General:** Shows 1 problem and 1 warning. A red arrow points to the 'Sharing' tab.
- Sharing:** Indicates 1 descendant SMB share.
- Permissions:** Section for setting access rights.
- Auto Snapshot Data Protection:** Enabled (storage profile).
- Replication:** Disabled (no targets).
- Settings:** Section for dataset configuration.
- Storage Utilization:** Shows 81.6MB free snapshots of 231.8MB and 421.5MB free of 731.8MB.
- Notifications:** Lists 1 Problem(s) (Auto-snapshot(s) failed) and 1 Warning(s) (Additional SMB share(s) on descendants).
- Location:** Shows the dataset is located at 'bsterling03 (10.2.22.197)' with sub-sections for 'p01', 'global', and 'test', each with storage utilization bars.
- Children:** Shows a 'testchild' sub-section with 81.6MB free data of 81.7MB.

The screenshot displays the 'SMB Share' configuration page in Azure Storage Explorer. On the left sidebar, the 'Permissions' section is expanded, showing 'Auto Snapshot Data Protection' (Enabled), 'Replication' (Disabled), and 'Settings'. The 'Storage Utilization' section shows two progress bars: '81.6MB free snapshots of 231.8MB' and '421.5MB free of 731.8MB'. The main content area shows 'User Behavior' (Off), 'Descendant SMB Shares' (1 descendant), and a warning box: '1 Warning(s) • Additional SMB share(s) on descendants.' Below this, the 'Connect Using' section shows the path '\\10.2.22.197\test' and a list of options: 'On' (checked), 'Hide from users that don't have permission (ABE)' (checked), 'Hide previous versions' (unchecked), and 'Host based access control' (unchecked). A red arrow points to the 'Host based access control' checkbox. The 'Encryption' dropdown is set to 'Encryption disabled'. At the bottom, 'Excessive File Access' is set to 'Off'.

Once you select this option you will be prompted to set network address ranges to restrict or allow access to the share. These options work in conjunction with the dataset permissions. (ex. A user connects to an SMB share from a subnet granted Read/Write access, yet the dataset permission only allows Read operations for that user. The example user will only be allowed Read permissions to the dataset)

For SMB shares you can assign the following permissions via Host Based Access Control

- Read-Only
- Read/Write
- Deny

Read-only

[Empty field] ▼

Read/Write

@10.32.12.0/24 ▼

Deny

[Empty field]

Encryption disabled ▼

For NFS share you can assign the following permissions via Host Based Access Control

- Read-Only
- Read/Write
- Full Control (Root)
- Deny

Read-only

[Empty field] ▼

Read/Write

[Empty field] ▼

Full Control (Root)

@10.210.0.0/22 ▼

Deny

[Empty field]

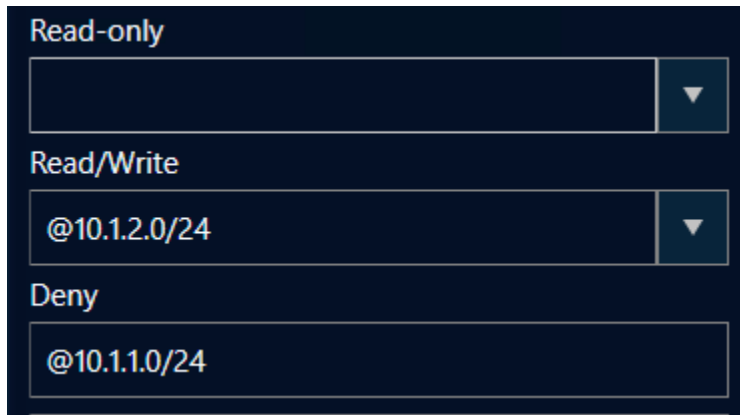
Security Mode

local ▼

Hide descendant datasets

Data security labels

It is important to note that setting **ANY** of the Host Based Access Controls will automatically apply an implicit Deny rule. This means that in the case of wanting to deny a specific subnet or Ip addresses, you would also need to apply allow rules for any desired subnets or IP address otherwise all connections will be denied. Below is an example of how to configure Host Based Access Control to deny connections from the 10.1.1.0/24 subnet and allow connections from the 10.1.2.0/24 subnet.



The screenshot shows a configuration interface with three sections: 'Read-only', 'Read/Write', and 'Deny'. Each section has a text input field and a dropdown arrow on the right. The 'Read-only' field is empty. The 'Read/Write' field contains '@10.1.2.0/24'. The 'Deny' field contains '@10.1.1.0/24'.

Since explicit deny rules are always processed first, an alternative method would be to allow everyone and add deny rules for any desired subnets or IP addresses. The below example would deny access to the share from the 10.1.1.0/24 subnet and allow connections from any other source.



The screenshot shows a configuration interface with four sections: 'Read-only', 'Read/Write', 'Deny', and 'Encryption disabled'. Each section has a text input field and a dropdown arrow on the right. The 'Read-only' field is empty. The 'Read/Write' field contains 'Everyone'. The 'Deny' field contains '@10.2.21.12'. The 'Encryption disabled' field contains 'Encryption disabled'.

To assign everyone permission with Host Based Access, you can use one of the following

- 0.0.0.0/0
- * (The BrickStor will translate this into Everyone once committed)
- Everyone

Limiting Admin Access (Brickstor SP Manager and ssh)

BrickStor SP Manager

In order to restrict access to the BrickStor SP Manager you must modify the bsrapid.conf file. This will set an explicit listen address for the UI, which should be on an Admin network. Run the following command to open this file in vi text editor

```
vi /etc/racktop/bsrapid/bsrapid.conf
```

Once open move the cursor with the arrow keys to following position

```
# Copyright 2023 RackTop Systems, Inc.
# Name: bsrapid
# Version: 23.4.2.23

ListenAddress = "0.0.0.0:8443"
ListenAddressPub = ":443"
SslCertPath = "/etc/racktop/certs/star.local.pem"
SslKeyPath = "/etc/racktop/certs/private/star.local.key"
Debug = false
AdminGroups = ["bsadmins"]
StaticDir = "/var/racktop/bsrapid/static"
EnableLocalAD = true
AdTimeout = 5000000000

[Audit]
Connection = ""
[Audit.Syslog]
Protocol = "udp"
Server = "127.0.0.1:514"
CertFile = ""
Facility = "audit"
Format = "logfmt"
Enabled = false
Tag = ""

~
~
```

When the cursor is there press "i" on the keyboard to enter insert mode and then type the IP address of the admin0 interface for the BrickStor. The line should look similar to this

```
# Copyright 2023 RackTop Systems, Inc.
# Name: bsrapid
# Version: 23.4.2.23

ListenAddress = "10.3.12.60:8443"
ListenAddressPub = ":443"
SslCertPath = "/etc/racktop/certs/star.local.pem"
SslKeyPath = "/etc/racktop/certs/private/star.local.key"
Debug = false
AdminGroups = ["bsradmins"]
StaticDir = "/var/racktop/bsrapid/static"
EnableLocalAD = true
AdTimeout = 5000000000

[Audit]
Connection = ""
[Audit.Syslog]
Protocol = "udp"
Server = "127.0.0.1:514"
CertFile = ""
Facility = "audit"
Format = "logfmt"
Enabled = false
Tag = ""

~
~
~
```

Once this file looks correct, press ESC and then type :wq and press enter to write the changes and exit the file

Lastly restart bsrapid with the below command

```
svcadm restart bsrapid
```

This change will only allow UI connections to the 10.3.12.60 address. If the network is configured to allow other subnets to route to the admin network, hosts on other subnets could still potentially access the UI

SSH

To restrict ssh access, the process is similar however with the /etc/ssh/sshd_config file. Run the below command to open the file with a text editor

```
vi /etc/ssh/sshd_config
```

Once open find the line the reads "#ListenAddress 0.0.0.0" and move the cursor to the following position

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Restrict us to NIST approved ciphers. Chacha20 is not on the NIST
# approved list. AES-GCM is also significantly faster on modern hardware.
Ciphers -chacha20*
```

Next press "i" to enter insert mode and press backspace to delete the "#"

After that line is no longer commented out, using the arrow keys move the cursor to the end of the line and remove "0.0.0.0" then type in the admin0 address. The line should look like the below screenshot

```
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

#Port 22
#AddressFamily any
ListenAddress 10.3.12.60
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Restrict us to NIST approved ciphers. Chacha20 is not on the NIST
# approved list. AES-GCM is also significantly faster on modern hardware.
Ciphers -chacha20*
```

Once this looks correct, press ESC and then type :wq and press enter to write the changes and exit the file

Lastly restart the ssh service with the below command

```
svcadm restart ssh
```

Similar to restricting UI access, this change will only allow ssh connections to the specified address. If the network is configured to allow other subnets to route to the admin network, hosts on other subnets could still potentially access the BrickStor over ssh