LOGZILLA DOCUMENTATION

Qnap Qts

LogZilla App Store application: Qnap Qts

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/qnap-qts

Overview

QNAP QTS is a Linux-based operating system for QNAP Network Attached Storage (NAS) devices. QTS provides file storage, sharing, backup, virtualization, and multimedia applications for home and business users.

App Function

- Parse QNAP QTS connection logs for file access and authentication events
- Extract user, source IP, computer name, and action metadata
- Categorize events by Event Class (auth, system)
- Map authentication failures to MITRE ATT&CK T1110 (Brute Force)
- Alert on login failures and file deletions

Vendor Documentation

- QNAP QTS (https://www.qnap.com/qts/5.0/en-us/)
- Configuring Log Sender Settings (https://docs.qnap.com/operating-system/qts/5.0.x/en-us/configuring-log-sender-settings-66DE0C94.html)

Device Configuration

Configure the QNAP NAS to forward syslog messages to LogZilla:

Open **QuLog Center** from the QTS desktop
Navigate to **QuLog Service > Log Sender > Send to Syslog Server**
Enable **Send logs to a remote syslog server**
Click **Add Destination**
Enter the LogZilla server IP address in **Hostname/IP Address**
Set **Port** to `514`
Select **Transfer protocol** (UDP or TCP)
Select **Log type** (Event logs, Access logs, or both)
Click **Apply**

Verification

Perform a file operation or login attempt, then verify events appear in LogZilla with `Vendor: QNAP`.

Incoming Log Format

QNAP QTS connection logs use a structured format:

```
<date> <hostname> <pid> conn log: Users: <user>, Source IP: <ip>,
Computer name: <computer>, Connection type: <protocol>,
Accessed resources: <resource>, Action: <action>
```

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	QNAP	Device vendor
Product	QTS	Device product
Event Class	auth	Cross-vendor event classification
User	admin	Username performing the action
SrcIP	192.168.1.100	Source IP address
Computer Name	WORKSTATION01	Client computer name
Connection Type	smb	Protocol (smb, ftp, afp, nfs, webdav)
Action	Login OK	Action performed
Resource	file.txt	Accessed file or folder
MitreId	T1110	MITRE ATT&CK technique ID
MITRE Tactic	Credential Access	MITRE ATT&CK tactic

Log Examples

File Write

```
Jan  1 00:00:00 nas01 1234 conn log: Users: jsmith, Source IP: 10.1.1.1,
Computer name: PC1, Connection type: ftp, Accessed resources: file.txt,
Action: Write
```

Successful Login

```
Jan  1 00:00:00 nas01 1234 conn log: Users: admin, Source IP: 192.168.1.100,
Computer name: WORKSTATION, Connection type: smb, Accessed resources: ,
Action: Login OK
```

Failed Login

```
Jan  1 00:00:00 nas01 1234 conn log: Users: guest, Source IP: 10.0.0.50,
Computer name: LAPTOP, Connection type: afp, Accessed resources: ,
Action: Login Fail
```

Triggers

Trigger	Description
`QNAP: MITRE ATT&CK Threat Detected`	Any event with MITRE mapping
`QNAP: Login Failed`	Authentication failure (brute force indicator)
`QNAP: Login Success`	Successful login (audit trail)
`QNAP: File Deleted`	File deletion (potential data loss)