Data Security with NVMe over Fabric Technology

04.05.2021

Student Names

1. Ashu Goyal - 18BIT0168
2. Shaifali Choudhary - 18BCE2242
3. Rashmitha Challa - 18BCE7273
4. Abhimanyu Atri - 18BCE2192

College Mentor

- Dr. Sureshkumar N.

Goals

1. Understand evolving trends with NVMe over Fabric (NVMe-oF) and analyze potential vulnerability points in transport and data at rest.
2. What are the current challenges with NVMe over Fabric technology?
3. What are the vulnerability points with existing NVMeOF reference implementations of initiator and targets?
4. What is the viewpoint of data at rest security from the specification perspective?
5. How NVMe-oF can enable Storage as a service in the cloud?
6. What are the aspects covering security vs. performance for reference implementations?

Milestones

I. Two weeks

- Understand Storage array, NVMe and NVMeOF protocol, Data security.
- Storage array functionality
- NVMe architecture and commands.
- Secure Erase
- Network Security/Data Security - Authentication

Outcome: Understanding of storage concepts and protocols.

II. One week

- NVMe commands and Security related aspects in spec.

III. One week

- Network security for NVMeOF – read about vulnerabilities in Ethernet that can impact.
- Read about error handling and recovery in NVMe and NVMeOF.

IV. Two weeks

- Install Initiator/target on Linux system and do IOs.

V. One week

- Read about error handling and recovery in NVMe and NVMeOF.

1. What Is a Storage Array?

Definition - A storage array, also called a disk array, is a data storage system for block-based storage, file-based storage, or object storage.

Rather than storing data on a server, storage arrays use multiple drives in a collection capable of storing a huge amount of data, managed by a central management system. The drives on which data is stored are usually spinning hard disk drives (HDDs) or solid-state drives (SSDs).

How Do Storage Arrays Work?

1. Storage arrays keep storage separate from servers using a collection of hard disk drives (HDDs) or solid-state drives (SSDs). In some cases, they use a combination of both so they can scale much more efficiently than the storage capacity of a collection of servers.

    - **HDD storage arrays- HDD storage arrays**, or disk arrays, are commonly used in business environments for storage purposes and have excellent redundancy features to help protect data. For example, **Redundant Arrays of Independent Disks (RAID)** controllers are used to make copies of the same data across multiple hard disks. This protects the data from loss if one of the disks fails, as all the backup copies are still available.
    - **SSD storage array-** An **SSD storage array**, also called a flash storage array, has the same basic storage array architecture as an HDD array but will operate much faster. However, HDDs are cheaper, so they're sometimes used in combination.

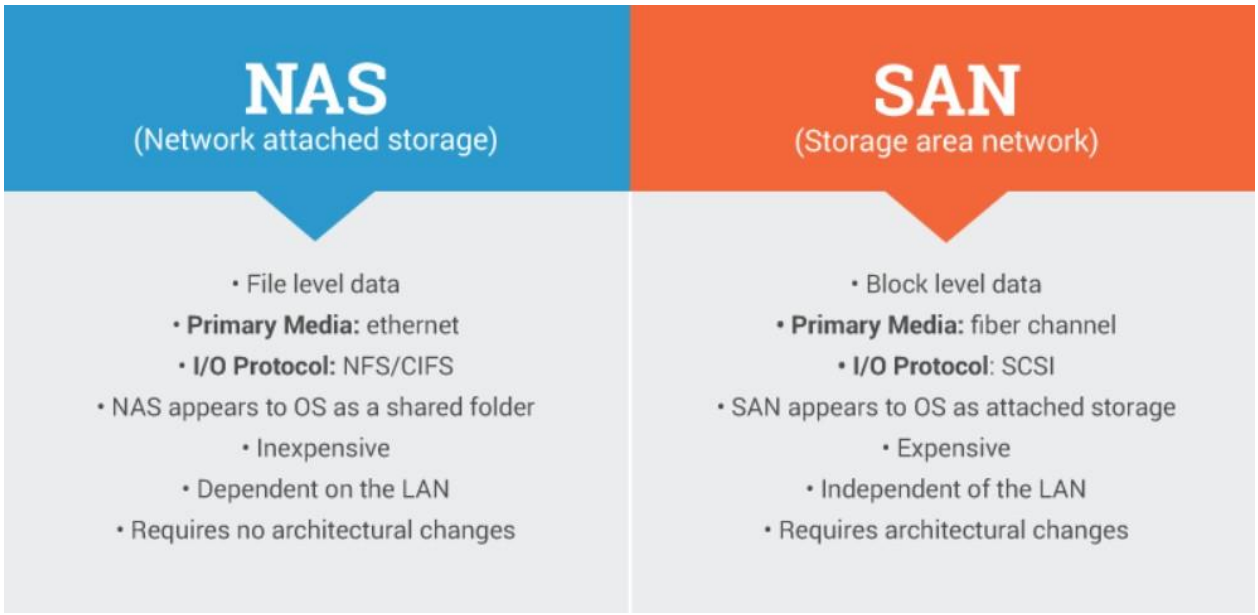
Applications of Storage Arrays

Storage arrays form key components of storage networks, such as **Storage Area Networks (SANs)** for block storage and **Network-Attached Storage (NAS)** for file storage. These networks enable storage to be managed separately from the local area network (LAN) or wide area network (WAN) that connects other devices inside an organization.

Types of Storage Arrays:

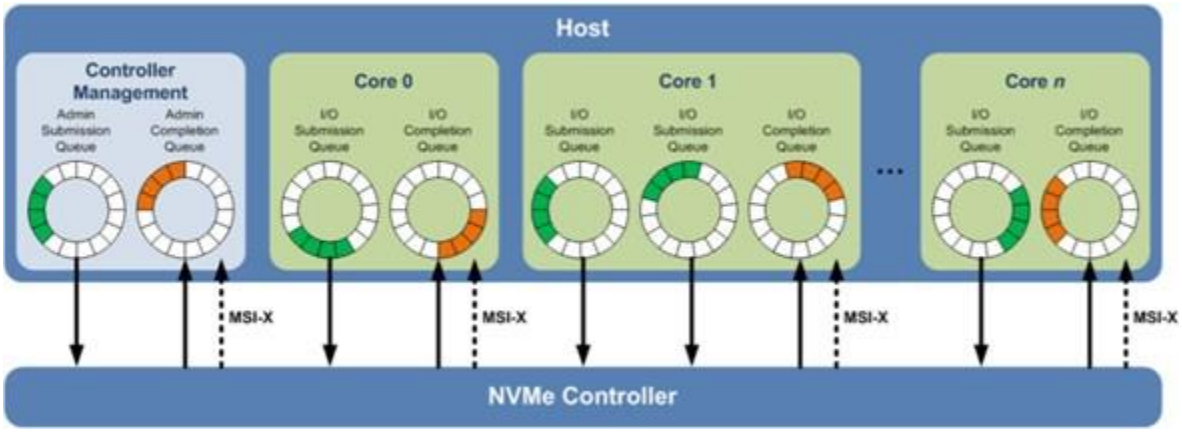
1. **Storage Area Networks (SANs) arrays:** A **Storage Area Network (SAN) or Storage Network** is a computer network which provides access to consolidated, block-level data storage. SANs are primarily used to access data storage devices, such as **storage arrays** and tape libraries from servers so that the devices appear to the operating system as direct-attached storage. A SAN typically is a dedicated network of storage devices not accessible through the local area network (LAN).
2. **Network-attached storage**(**NAS**)- **Network-attached storage**(**NAS**) is a file-level (as opposed to block-level storage) computer data storage server connected to a computer network providing data access to a heterogeneous group of clients. NAS is specialized for serving files either by its hardware, software, or configuration.

Network-attached storage(NAS) vs Storage Area Networks(SAN)



2. NVMe architecture and commands.

NVMe upholds 64K orders per line and up to 64K lines. These lines are planned to such an extent that I/O orders and reactions to those orders work on a similar processor center and can exploit the equal preparing abilities of multi-center processors. Every application or string can have its own autonomous line, so no I/O locking is required. NVMe likewise upholds MSI-X and intrude on guiding, which forestalls bottlenecking at the CPU level and empowers gigantic adaptability as frameworks extend.



Only 10 admin commands are required

ADMIN COMMANDS
Create I/O Submission Queue
Delete I/O Submission Queue
Create I/O Completion Queue
Delete I/O Completion Queue
Get Log Page
Identify
Abort
Set Features
Get Features
Asynchornous Event Requests
Firmware Activate (Optional)
Firmware Image Download (Optional)
Format NVM (Optional)
Security Send (Optional)
Security Receive (Optional)

Only 3 I/O commands are required

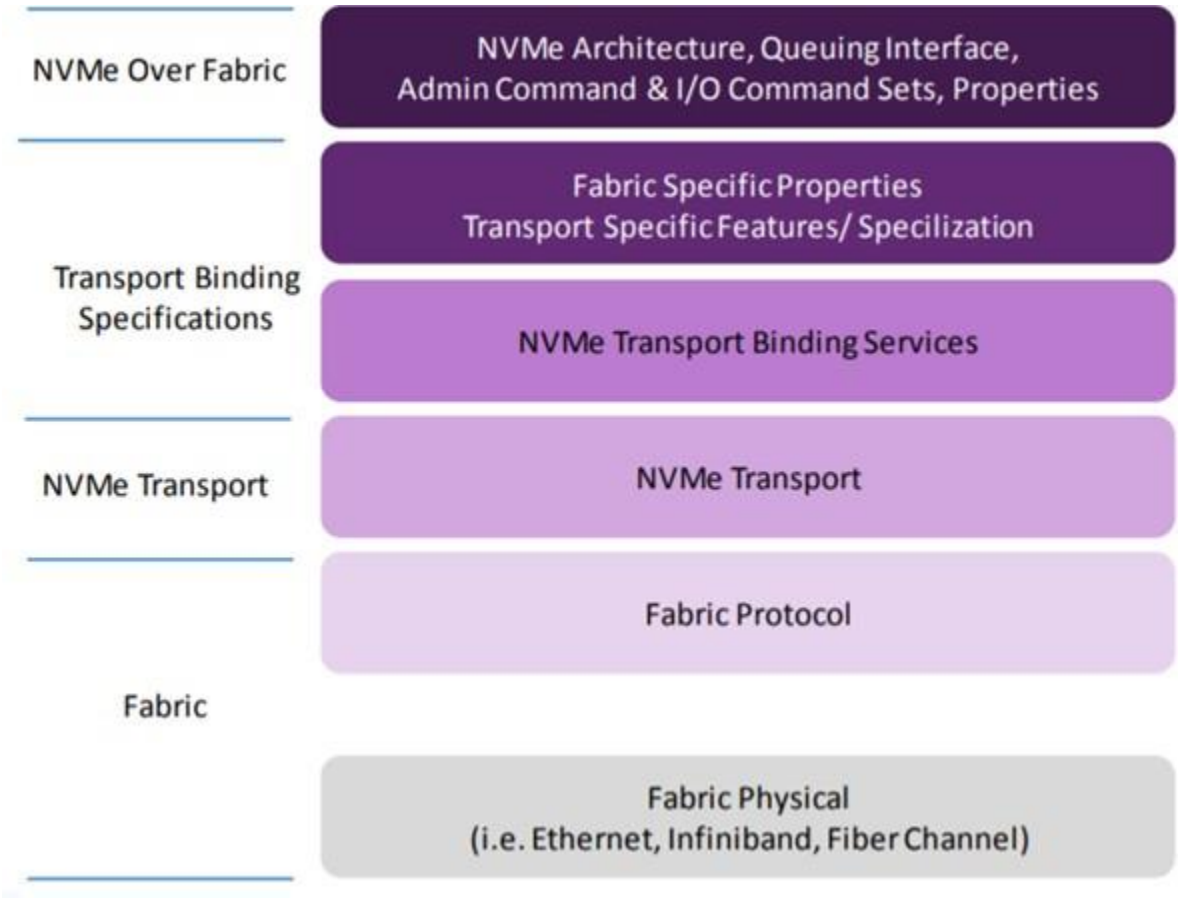
NVM I/O COMMANDS
Read
Write
Flush
Write Uncorrectable (Optional)
Compare (Optional)
Dataset Management (Optional)
Write Zeros (Optional)
Reservation Register (Optional)
Reservation Report (Optional)
Reservation Acquire (Optional)
Reservation Release (Optional)

What is NVMe over Fabric?

1. The best thing about NVMe using PCIe is that it is very fast. But the only drawback is that it is contained inside of a single computer.
2. NVMe over Fabrics (NVMe-oF) is an extension of the NVMe network protocol specification designed to connect hosts to storage across a network fabric using the NVMe protocol.
3. It is designed to enable data transfers between a host computer and a target storage device or system over a network. Data can be transferred through methods such as Ethernet, Fibre Channel (FC) or InfiniBand.

Need of NVMe over Fabric Technology.

1. NVM Express over Fabrics defines a common architecture that supports a range of storage networking fabrics for NVMe block storage protocol over a storage networking fabric.
2. This includes enabling a front-side interface into storage systems, scaling out to large numbers of NVMe devices and extending the distance within a datacenter over which NVMe devices and NVMe subsystems can be accessed.



Architecture of NVMe-OF

3. What is Secure Erase?

Data security is a top priority for everyone who uses electronic devices. Being able to completely wipe drives of data is essential, especially on devices that contain sensitive information, such as those used in military applications. **Secure Erase** is a feature that was initially designed for HDDs, or hard disk drives. However, it can also be used with solid state drives, or SSDs, which are now more common. Secure Erase completely wipes clean all of the data found on a drive and does not allow that data to be retrieved. It is a permanent solution that provides the maximum level of security for sensitive data that must be erased.

How Secure Erase Works

- Many people try to erase data by moving files to the recycle bin or trash can on their device, but that does not fully erase the files. Although the files may not be visible in your folders any more after this action, they are still recoverable on your device.

- Secure Erase is different. It completely overwrites all of the data on your drive, making the data impossible to recover. It works by writing a binary one or zero over each piece of data in the drive, and because it is programmed into the firmware, the internal monitoring system will flag any missed write operations and ensure they are completed. As such, when the Secure Erase

process is performed, you can be confident that is has worked completely and that the files are thoroughly written over. It is impossible to recover any of the previous data using data recovery software.

- Secure Erase is part of all SSDs that have PATA or SATA firmware. It is important to note that Secure Erase can only be used to scrub data from the entire drive. If you need to permanently delete individual files without wiping the whole drive, you will need to also have a file shredding software system.

4. Who Can Benefit from Secure Erase?

Secure Erase is a feature that can benefit anyone who stores data on a SATA SSD, but those who have **industrial grade devices** may find this feature particularly useful. With an industrial device, the stored data may contain sensitive customer, financial, or security information. When it becomes necessary to get rid of the drive, using Secure Erase to ensure it is wiped clean will prevent this information from being leaked.

5. Authentication:

NVMe over Fabrics supports both **fabric secure channel** (that includes authentication) and **NVMe in-band authentication.**Determination of which NVMe Transport identities are authorized to be used with which NVMe identities is part of the security policy for the deployed subsystem.

1. **Fabric secure Channel:**

An NVM subsystem that requires use of a fabric secure channel (i.e., as indicated by the TREQ field in the associated Discovery Log entry) shall not allow capsules to be transferred until a secure channel has been established for the NVMe Transport connection.

2. **Nvme in -band authentication:**

If all bits in the AUTHREQ field are cleared to '0', then the controller does not require the host to authenticate, and the subsystem shall not abort any command with a status value of Authentication Required. A controller shall report the same value of AUTHREQ in the Connect response capsules sent by all of that controller's queues. All controllers in an NVM subsystem should report the same value of AUTHREQ.

Authentication requirements for security commands are based on the security protocol indicated by the SECP field in the command.