Glossary

The following terms are useful in understanding the Nasuni Filer.

A

Access Control List (ACL)

An access control list (ACL) is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

ACL (Access Control List)

See “Access Control List (ACL)” on page 1.

Active Directory (AD)

Microsoft Active Directory (AD) is a directory service for Windows domain networks. It is part of most Windows Server operating systems. Microsoft Active Directory enables administrators to assign policies, deploy software, and apply critical updates to an organization. Active Directory stores its information and settings in a central database.

AD (Active Directory)

See “Active Directory (AD)” on page 1.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is used worldwide. AES is approved by the National Security Agency (NSA) for top secret information.

Advanced Message Queuing Protocol (AMQP)

The Advanced Message Queuing Protocol (AMQP) is an open standard for passing business messages between applications or organizations. It connects systems, feeds business processes with the information they need, and reliably transmits onward the instructions that achieve their goals.

AES (Advanced Encryption Standard)

See “Advanced Encryption Standard (AES)” on page 1.

AMQP (Advanced Message Queuing Protocol)

See “Advanced Message Queuing Protocol (AMQP)” on page 1.

Antivirus (AV)

The Antivirus Service provides protection against viruses and other malware in files on a volume. The Antivirus Service scans every new or modified file for the presence of viruses and other malware. If a scanned file is found to be infected, the authorized administrator has the option to ignore the infection. Only files with no detected malware, or infected files that the authorized administrator deliberately ignores, are allowed into cloud storage. The Nasuni Filer Antivirus Service uses the Clam AntiVirus (ClamAV®) open-source antivirus engine.

Authorization Code

A 6-character code used in conjunction with a Serial Number to validate an installation. Authorization Codes are good for one use; one successful use causes an authorization code to be changed automatically. Generating a new authorization code for a serial number does not cause a Nasuni Filer or NMC that uses that serial number to stop working. The authorization code is only used once during initial setup of a new or recovered Nasuni Filer or NMC. Because an Authorization Code is only used once, an administrator can safely issue it to a user in order to install a single Nasuni Filer or NMC without revealing Nasuni account credentials. To obtain an Authorization code for a Serial Number, visit https://account.nasuni.com/account/serial_numbers/, or the Account Status page of the Nasuni Management Console.

Auto Cache or autocache or autofault

A feature that immediately brings new data into the local cache from other Nasuni Filers that are attached to a volume. Otherwise, new data is brought into the local cache from other Nasuni Filers when that data is accessed next.

AV (Antivirus)

See “Antivirus (AV)” on page 2.

B

bucket

A bucket is a logical unit of storage in object storage services, such as Amazon Web Services (AWS) Simple Storage Solution (S3), EMC ECS, and EMC ViPR. Buckets can be thought of as containers that are used to store objects, which consist of data and metadata.

byte-range locking

Byte-range locking is a form of global file locking that applies to locking a collection of bytes within a file, rather than the entire file. Certain applications benefit from byte-range locking.

C

cache

A cache is a computer component that stores data locally so that future requests for that data can be served faster. While all data and metadata are stored in cloud storage, data that requires regular access is kept locally. This includes files that are re-written and data that is read often. If the requested data does not reside locally, it is staged into the cache and provided for the request.

cache miss

If requested data does not reside in the local cache, and must be staged into the cache for the request, this is called a “cache miss”.

Challenge-Handshake Authentication Protocol (CHAP)

A protocol that authenticates a user or network host to an authenticating entity.

CHAP (Challenge-Handshake Authentication Protocol)

See “Challenge-Handshake Authentication Protocol (CHAP)” on page 3.

chunks

Before sending data to the cloud, Nasuni breaks files into optimally-sized pieces for transport between the on-premises cache and cloud storage. This not only disguises the actual sizes of files, but also improves performance. These chunks are then deduplicated, compressed, and encrypted.

CIFS (Common Internet File Service)

A standard protocol that allows Windows users to share files across a network.

ClamAV (Clam antivirus)

See “Antivirus (AV)” on page 2.

copy-on-write (COW) disk

The copy-on-write (COW) disk is used during the snapshot process. If any writes to the Nasuni Filer occur during a snapshot, the previous data from the cache disk is copied to the COW disk, and the new data is written to the cache disk. Hence, the term “copy-on-write”. This allows new writes to take place at any time, even during the snapshot process.

COW (copy-on-write) disk

See “copy-on-write (COW) disk” on page 3.

D

DAS (Direct Attached Storage)

See “Direct Attached Storage (DAS)” on page 4.

data

Data is transmittable and storable computer information. Nasuni handles data in the form of files, including text, images, audio, and video.

Direct Attached Storage (DAS)

Direct-attached storage (DAS) is computer storage that is directly attached to one computer or server and is not, without special support, directly accessible to other ones. The main alternatives to direct-attached storage are network-attached storage (NAS) and a storage area network (SAN).

directory quota

A limit on the amount of data in a directory. You can configure that quota reports are sent to administrators or users when directories near or exceed their quota.

Directory Services

Services, including authentication, provided by Active Directory or LDAP.

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a network configuration protocol that provides a network IP address for a host on an IP network automatically.

E

encryption

The Nasuni Filer encrypts data sent to cloud storage using the OpenPGP standard, with AES-256 as the default encryption.

eviction

Data that has been copied from the Nasuni Filer to cloud storage, and that is rarely used again, is eventually removed (“evicted”) from the Nasuni Filer’s cache to free up space for new data. If one of these evicted files is later requested for reads or writes, the Nasuni Filer retrieves the file from cloud storage and puts it back into the cache automatically.

export

A directory on a server volume that a client on your network can access.

F

faulting

If requested data does not reside in the local cache, it is staged into the cache and provided for the request. This is informally called “faulting”.

file system

A method for storing and organizing computer files and the data that they contain in order to make it easy to find and access them.

file transfer protocol (FTP)

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

firewall

You can configure inbound traffic to the Nasuni Filer user interface and the Nasuni Support SSH port, which provides firewall protection.

FTP (file transfer protocol)

See “file transfer protocol (FTP)” on page 5.

G

GB/GiB

GB is an abbreviation of gigabyte, meaning 1,000,000,000 bytes. Usually used to refer to hard disk capacity.

GiB is an abbreviation of gibibyte, meaning 2^{30} (1,073,741,824) bytes. Usually used to refer to RAM memory.

global file locking

The purpose of the global file locking feature is to prevent conflicts when two or more users attempt to change the same file on different Nasuni Filers. If you enable the global file locking feature for a directory and its descendants, any files in that directory or its descendants can only be changed by one user at a time. Any other users cannot change the same file at the same time.

You can also manually break the locking of a file. This might become necessary if a user leaves a file open and another user needs to open that file.

I

initiator

An initiator functions as an iSCSI client. An iSCSI initiator sends SCSI commands over an IP network.

instance

The Nasuni Filer is either a hardware appliance or virtual machine. An instance refers to a single virtual machine that provides virtualization of the Nasuni Filer software.

Internet Small Computer System Interface (iSCSI)

An Internet Protocol (IP)-based storage networking standard for linking data storage facilities. By carrying SCSI commands over IP networks, iSCSI facilitates transferring data over intranets and managing storage over long distances. The protocol allows clients (called initiators) to send SCSI commands (CDBs) to SCSI storage devices (targets) on remote servers. iSCSI is a Storage Area Network (SAN) protocol.

IQN (iSCSI Qualified Name)

See "iSCSI Qualified Name (IQN)" on page 6.

iSCSI (Internet Small Computer System Interface)

See "Internet Small Computer System Interface (iSCSI)" on page 6.

iSCSI Qualified Name (IQN)

The iSCSI Qualified Name includes these fields:

- `iqn.`
- date that the naming authority took ownership of the domain, in `yyyy-mm` format.
- reversed domain name of the authority, such as `com.nasuni`.
- ":" followed by a storage target name specified by the naming authority.

  Example: `iqn.2008-11.com.nasuni:filer.nasuni.net:51`

K

Kerberos

Kerberos is a computer network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It provides mutual authentication: both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default.

L

LDAP (Lightweight Directory Access Protocol)

LDAP is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services allow sharing information about users, systems, networks, services, and applications throughout the network. A common use of LDAP is to provide a central place to store usernames and passwords. This allows applications and services to connect to the LDAP server to validate users.

K

Kerberos

Kerberos is a network protocol that is used to authenticate users. After a client has correctly authenticated with a Kerberos server, the client is issued a ticket that allows the client to access the requested service as long as it is within a Kerberos realm (domain). A Kerberos keytab file contains encryption keys associated with services (the service principal names) located on servers hosting Kerberos-enabled protocols.

K

Kerberos

Kerberos is a computer network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It provides mutual authentication: both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default.

L

LDAP (Lightweight Directory Access Protocol)

LDAP is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services allow sharing information about users, systems, networks, services, and applications throughout the network. A common use of LDAP is to provide a central place to store usernames and passwords. This allows applications and services to connect to the LDAP server to validate users.

L

LDAP (Lightweight Directory Access Protocol)

See “Lightweight Directory Access Protocol (LDAP)” on page 7.

least recently used (LRU)

When the cache starts getting too full, the Nasuni Filer releases the least recently used (LRU) data first, using a sophisticated algorithm. This helps to ensure that the most recently used data, and the data most likely to be used, remains in the cache.

Lightweight Directory Access Protocol (LDAP)

LDAP is a network protocol that is used to identify users. After a user is authenticated with Kerberos and has a valid ticket, the information from the ticket is used to look up additional details on that user from a directory server using the LDAP protocol.

Linux

Linux is a family of free and open-source software operating systems built around the Linux kernel. Typically, Linux is packaged in a form known as a Linux distribution (or distro for short) for both desktop and server use.

LRU (least recently used)

See “least recently used (LRU)” on page 7.

K

Kerberos

Kerberos is a computer network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It provides mutual authentication: both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default.

L

LDAP (Lightweight Directory Access Protocol)

LDAP is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services allow sharing information about users, systems, networks, services, and applications throughout the network. A common use of LDAP is to provide a central place to store usernames and passwords. This allows applications and services to connect to the LDAP server to validate users.

M

management information base (MIB)

A database for managing entities in a network, such as with the Simple Network Management Protocol (SNMP).

maximum transmission unit (MTU)

The maximum transmission unit (MTU) is the size (in bytes) of the largest protocol data unit that the layer can pass onwards. A larger MTU brings greater efficiency, because each packet carries more user data while protocol overheads, such as headers, remain fixed; the resulting higher efficiency means a slight improvement in the bulk protocol throughput. A larger MTU also means processing fewer packets for the same amount of data. However, large packets can occupy a slow link for some time, causing greater delays to following packets, and increasing lag and minimum latency. MTU settings should not exceed 1500.

MB/MiB

MB is an abbreviation of megabyte, meaning 1,000,000 bytes. Usually used to refer to hard disk capacity.

MiB is an abbreviation of mebibyte, meaning 2^{20} (1,048,576) bytes. Usually used to refer to RAM memory.

metadata

Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted.

MIB (management information base)

See “management information base (MIB)” on page 8.

MTU (maximum transmission unit)

See “maximum transmission unit (MTU)” on page 8.

N

NAS (Network Attached Storage)

See “Network Attached Storage (NAS)” on page 10.

Nasuni Filer

The Nasuni Filer is a storage controller that runs in your data center and provides primary storage with built-in backup and offsite protection. The Nasuni Filer is available as both a hardware appliance and a virtual machine. The Nasuni Filer can be used instead of, or in combination with, traditional file servers. It fully supports Windows CIFS Shares as well as Active Directory and LDAP or LDAP Directory Services. A single volume in a Nasuni Filer has unlimited capacity, due to the integration of its caching algorithms with provisioning.

Nasuni Filer user interface (UI)

The Web-based user interface to the Nasuni Filer.

Nasuni Management Console (NMC)

The Nasuni Management Console enables you to monitor and manage many Nasuni Filers from one central application. Using the Nasuni Management Console, you can view the status of all of your managed Nasuni Filers, as well as configure their settings. With the Nasuni Management Console, you can ensure consistent settings on all your Nasuni Filers.

Using the Nasuni Management Console, you can manage Nasuni Filers even if they are not presently connected. Any configuration changes made will propagate to the Nasuni Filer when it becomes connected.

Nasuni's cloud storage

The secure unlimited online storage provided through the Nasuni Filer.

Network Attached Storage (NAS)

Network-attached storage (NAS) is file-level computer data storage connected to a computer network. NAS devices are a convenient method of sharing files among multiple computers. NAS systems typically provide access to files using network file sharing protocols such as NFS, SMB/CIFS, or AFP.

Network File System (NFS)

A protocol and file system for accessing and sharing files across a computer network using UNIX and Linux.

Network Operations Center (NOC)

Nasuni's Network Operations Center (NOC) provides a variety of behind-the-scenes services that make the Nasuni Service possible. These services include security patches, component updates, system scaling, performance tuning, response time monitoring and analysis, optimization, staging and deployment of new software, support of new Nasuni Filer functionality, single sign on management, cloud provisioning, cloud monitoring, account management, and customer support.

NFS (Network File System)

See "Network Attached Storage (NAS)" on page 10.

NMC (Nasuni Management Console)

See "Nasuni Management Console (NMC)" on page 9.

NOC (Network Operations Center)

See "Network Operations Center (NOC)" on page 10.

O

object store

An object store, or object storage, is a data storage architecture that manages data as objects. File systems manage data as a file hierarchy, and block storage manages data as blocks within sectors and tracks. Each object typically includes the data itself, metadata about the data, and a globally unique identifier.

offsite data protection

Storing copies of critical data away from the original data centers to protect this information from natural disasters and accidental or malicious modification.

on-demand provisioning

The Nasuni Filer simplifies provisioning by offering instant provisioning in increments as small as 1 TB.

P

pinning

Pinning a folder specifies that the folder and its contents must remain in the local cache at all times. This can improve performance and reduce the time necessary to return accessed data to clients. This reduces the available cache by the size of the folder. Pinning a folder does not bring the folder's data into the cache. All iSCSI (SAN) volume data is already pinned in the cache, so it is not necessary to pin iSCSI volumes.

proxy

A server that acts as an intermediary for requests from clients seeking resources from other servers.

pruning

Pruning is the process of removing unneeded data. For example, you can specify removing log files older than a certain number of days. Similarly, you can specify snapshot retention for a set number of snapshots or for a set amount of time: the unwanted snapshots are removed.

Q

QoS (Quality of Service)

See "Quality of Service (QoS)" on page 11.

Quality of Service (QoS)

Quality of Service (QoS) settings indicate the inbound and outbound bandwidth limits of the Nasuni Filer for data moving to or from the Nasuni Filer, such as transmitting snapshots to cloud storage.

quota

A limit on the amount of usable storage space on a volume.

R

Remote Support Service

The Remote Support Service allows authorized Nasuni Technical Support personnel to remotely and securely access your Nasuni Filer. This can help Nasuni Technical Support to diagnose and resolve any issues with your Nasuni Filer quickly and proactively. No changes to your corporate firewalls are necessary. This service is disabled by default and is strictly opt-in.

S

SAN (Storage Area Network)

See "Storage Area Network (SAN)" on page 12.

Serial Number

A unique 32-digit hexadecimal number associated with your account for use with Nasuni Filer and Nasuni Management Console (NMC) installations. Each account has multiple Serial Numbers. Unused Serial Numbers may be used to set up a new Nasuni Filer or an NMC. Serial Numbers already in use may be used to recover existing Nasuni Filers or your existing NMC. Serial Numbers are used in conjunction with Authorization Codes. To obtain a Serial Number, visit https://account.nasuni.com/account/serial_numbers/.

share

A folder on a volume that can be shared on your network. Access to a share can be customized on a user or group-level basis.

Side Load

As part of the recovery process, the Side Load feature enables you to transfer cache data directly from the original source decommissioned Nasuni Filer to the new destination Nasuni Filer. This saves the time and bandwidth necessary to manually re-populate the new cache with data.

Simple Network Management Protocol) (SNMP)

An Internet-standard protocol for managing devices on IP networks.

snapshot

An instantaneous, non-changing, read-only image of a volume. Snapshots let you view any past version of the file system and restore all or part of the version quickly.

A snapshot is a complete picture of the files and folders in your file system at a specific point in time. With snapshots, the Nasuni Filer can identify new or changed data. Snapshots offer data protection by enabling you to recover a file deleted in error or to restore an entire file system. After a snapshot has been taken and is sent to cloud storage, it is not possible to modify that snapshot.

SNMP (Simple Network Management Protocol)

See “Simple Network Management Protocol) (SNMP)” on page 12.

Storage Area Network (SAN)

An architecture to attach remote computer storage devices (such as disk arrays, tape libraries, and optical jukeboxes) to servers in such a way that the devices appear as locally attached to the operating system.

sync

You can schedule when, and with what frequency, the selected volume updates data (“syncs”) from Nasuni, merging your local data with any new or changed data from other Nasuni Filers connected to this volume. This helps to ensure that everyone in your organization is using the most current data.

T

target

A storage resource located on an iSCSI server. A target is a storage server instance.

U

UI (Nasuni Filer user interface)

See “Nasuni Filer user interface (UI)” on page 9.

UniFS

UniFS is Nasuni’s cloud-native global file system, storing all files, file versions, and metadata in your preferred private or public cloud object store. UniFS is the first file system designed to have its inode structure reside in the cloud. UniFS enables the Nasuni platform to inherit the virtually unlimited capacity, durability, and georedundancy of the cloud object stores.

Unix

Unix is a family of multitasking, multiuser computer operating systems that derive from the original AT&T Unix.

V

versioning

The Nasuni Filer provides the versioning necessary to eliminate the need for separate backup and restore procedures.

virtual machine (VM)

A virtual machine is a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer. A virtual machine behaves exactly like a physical computer and contains its own virtual (software-based) CPU, RAM, hard disk, and network interface card (NIC).

virtualization

Virtualization lets you run multiple virtual machines on a single physical machine, sharing the resources of that single computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer.

VM (virtual machine)

See “virtual machine (VM)” on page 13.

volume

A set of files and directories. A volume can consist of multiple shares. With the Nasuni Filer, each volume can be stored in cloud storage.