A system and method are provided for securely sharing storage resources in a storage network. One or more organizations are modeled in a structure where each organization includes one or more units. Users are assigned to a unit and are also assigned a command access level. The command access level grants access to certain management commands that may be performed on storage resources. Storage resources are then bound to units in the organization and may be accessed by users in the unit. Once command access levels are assigned and storage resources are bound, access for a user in the unit is restricted to the command access level assigned to the user and the storage resources bound to the user’s unit. When a command from a user is received, the command access level of the user and the bound storage resources for the unit of the user is determined. Then, a management command is performed using the bound storage for the user’s unit if the command is available for the command access level.
FIG. 1
Host Computers 106

Switch Fabric

Storage Server 100

Storage Devices 104

FIG. 2
FIG. 3
FIG. 4
FIG. 5
Modeling an organization in a structure including one or more units

Associate command access levels to users in the units

Binding storage devices to units in the organization

User logs into VSX

Restricting access for the user to commands corresponding to the assigned command access level

Restricting access for the user to storage resources bound to the user's unit

FIG. 6
User Logs Into VSX

User Issues A Management Command

Determine Command Access Level For User

Determine Storage Devices That Are Bound To User's Unit

Perform Command Using Bound Storage Devices If Command Is Available For User's Command Access Level

Update List Of Bound Storage Elements As Necessary

Update Command Access Levels If Necessary

FIG. 7
VIRTUAL DATA CENTER
CROSS-REFERENCE TO RELATED APPLICATIONS


BACKGROUND OF THE INVENTION

[0002] The present invention generally relates to computer storage and more specifically, to a system and method for securely sharing storage resources in a storage network.

[0003] As businesses increasingly rely on computing applications, it becomes imperative to effectively store data created by the businesses. Typically, businesses use a data center, either in-house or through a storage service provider, to facilitate the storing of and access to data. Thus, as the storage requirements of businesses increase, data centers are growing exponentially in size to meet the requirements. One way of effectively provisioning and managing mass storage systems in the data centers is a storage area network (SAN). As business storage requirements and the complexity of resulting storage area networks increase, managing these networks becomes extremely costly.

[0004] As the data centers grow in size, an increasing number of “customers” with widely varying requirements within their SAN have to be supported. A customer may include a single organization, such as a large financial enterprise that may be divided into several divisions, such as investment banking, asset management, and research. Additionally, each of these divisions may be further divided into smaller organizations, and so on. In order to guarantee security and Quality of Storage Service (QoS), each of the divisions of the organization is typically allocated their own unique server, storage, and networking resources within the SAN. One problem with this approach is that large amounts of storage at a very high cost to businesses are wasted.

[0005] Another problem is created when storage needs are trusted to a Storage Service Provider (SSP). SSPs provide storage to a number of clients that range from large companies requiring many terabytes of storage space to small companies requiring just a few hundred gigabytes of storage.

Clients in this case may include different companies in addition to several divisions for each company. Thus, a storage service provider has to maintain security for shared storage resources among divisions in an organization in addition to sharing resources between distinct organizations. As the number of clients grow for a storage service provider, providing secure storage services and maintaining a high level of quality of storage service becomes increasingly difficult.

[0006] Also, a problem with accounting and asset management is created as the size of the SAN and the number of customers using the SAN grow. A data center typically needs to track the storage allocated to each of its customers and determine an appropriate cost based on the quality of that storage. Additionally, the cost of quality of service may have to be broken down between different divisions of one organization. The task becomes very difficult and tedious to perform as SANs become more complicated and are mapped to increasing numbers of customers.

BRIEF SUMMARY OF THE INVENTION

[0007] In one embodiment of the present invention, a system and method are provided for securely sharing storage resources in a storage network. One or more organizations are modeled in a structure where each organization includes one or more units. Users are assigned to a unit and are also assigned a command access level. The command access level grants access to certain management commands that may be performed on storage resources. Storage resources are then bound to units in the organization. Thus, if a storage resource is bound to the unit in the organization, that storage resource may be accessed by users in the unit. Once command access levels are assigned and storage resources are bound, access for a user in the unit is restricted to the command access level assigned to the user and the storage resources bound to the user’s unit. When a command from a user is received, the command access level for the user and the bound storage resources for the unit of the user is determined. Then, a management command is performed using the bound storage for the user’s unit if the command is available for the command access level.

[0008] In one embodiment, a method for sharing storage resources for an organization is provided, where the organization is modeled in one or more units and one or more users are assigned to the one or more units. The method comprises: associating one or more command access levels with the one or more users in the one or more units, wherein a command access level specifies access to one or more commands; binding storage resources to the one or more units in the organization wherein storage resources bound to a unit are available for access to users in the unit; restricting access for a user of the one or more users to commands corresponding to a command access level assigned to the user; and restricting access for the user to storage resources bound to the user’s unit.

[0009] A further understanding of the nature and advantages of the invention herein may be realized by reference to the remaining portions in the specifications and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 shows a storage server according to an embodiment of the present invention;
FIG. 2 is a block diagram of the storage server showing the hardware components related to embodiments of the present invention;

FIG. 3 illustrates a unified modeling language (UML) representation for modeling an organizational structure according to one embodiment;

FIG. 4 is a UML representation for restricting access to management commands according to one embodiment;

FIG. 5 illustrates a UML representation for binding the organizational model to storage resources according to one embodiment;

FIG. 6 illustrates a method for sharing resources according to one embodiment; and

FIG. 7 illustrates a method for securely managing storage resources according to one embodiment.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 shows a storage server 100 according to an embodiment of the present invention. The figure also shows a storage area network (SAN) 102, a number of physical storage devices 104, and a number of host computers 106. The storage server 100 is also referred to as a Virtual Storage Exchange (VSX).

The SAN 102 can be any type of computer network. It is referred to as an area network in the present application because it is its relevant function with respect to the embodiments of the present invention. In an embodiment of the present invention, the SAN 102 is a Fibre Channel network, the host computers 106 and the storage devices 104 are configured to communicate with a Fibre Channel network, and the storage server 100 is also configured to communicate with a Fibre Channel network. Thus, the storage server 100 can be easily added to an existing SAN.

The physical storage devices 104 include tape drives, disk arrays, JBODs ("just a bunch of disks"), or other types of data storage devices. The physical storage devices 104 can be connected directly to the host computers 106 via the SAN 102 or be indirectly connected to the host computers 106 via the SAN 102 and the storage server 100. Management of storage virtualization is improved by using the storage server 100 to indirectly connect the storage devices 104 to the host computers 106.

The host computers 106 can be servers or stand-alone computers. The host computers 106 can be directly connected to the SAN 102 or indirectly connected via a switch, router, or other communication link.

FIG. 2 is a block diagram of the storage server 100 showing the hardware components related to embodiments of the present invention, including a storage processor 110, a line card 112, a virtual server card 114, and a switch fabric 116.

The storage server 100 may include one or more storage processors 110. The storage processors 110 process the storage commands and data to be stored as information flows between the host computers 106 and the storage devices 104. One or more of the storage processors 110 may be included on each line card 112. The storage server 100 includes space for numerous line cards 112, so the capabilities of the storage server 100 can be modularly increased by adding more line cards 112 or more storage processors 110. Each storage processor 110 is associated with one or more ports of the storage server 100.

The storage server 100 may include one or more virtual server cards 114. The virtual server cards control the operation of the storage server 100 and control the line cards 112, which perform the actual work of transferring commands and data.

The switch fabric 116 connects the storage processors 110. The switch fabric switches information received at one port to another port of the storage server 100. For example, when a host computer 106 wants to read data stored on the storage area network 102, its request is processed by the storage processor 110 associated with the port associated with that host computer 106. That storage processor 110 is referred to as the upstream storage processor 110. The upstream storage processor 110 communicates with a downstream storage processor 110 associated with the port associated with the storage device 104 storing the data to be read, via the switch fabric 116. Then the switch fabric 116 transfers the data read from the storage device to the host computer 106, via the downstream and upstream storage processors 110.

In one embodiment, VSX 100 centralizes the management layer in the SAN. By using a scalable virtual storage pool of storage resources, VSX 100 provides security for storage resources in a heterogeneous storage environment across SAN 102. Thus, storage devices 104 may be shared between organizations or units in an organization. In one embodiment, secure sharing of storage devices 104 is provided by modeling an organizational structure, restricting access to management commands, and binding the organizational model to storage resources.

FIG. 3 illustrates a unified modeling language (UML) representation 300 for modeling an organizational structure according to one embodiment. A detailed description of UML is published by Object Management Group and is known in the art. As shown, representation 300 includes an organization 302 and users 304. Although the representation shows only one organization 302, it will be understood that any number of organizations may be modeled.

Organization 302 includes one or more units. For example, organization 302 may include a single company divided into divisions as units, many different companies with each company divided into divisions as units, or any other organization capable of being divided into units.

Organization 302 may be structured in any way. In one embodiment, organization 302 is modeled hierarchically in a parent-child relationship. This relationship is shown in FIG. 3. The structure starts with a root organization or parent unit. The root organization is then divided into child organizations or child units. The child units may also be considered parent units to children connected to the child units. Using the above example, the financial enterprise may be modeled with a parent unit and children units for the investment banking, asset management, and research divisions.

Users 304 are assigned or mapped to different units of the organization in the hierarchy. For example, employees of the investment banking division are mapped to the investment banking unit, employees of the asset management division are mapped to the asset management unit, and so on. The model is then stored locally in VSX 100 or may be stored externally where it is accessible by VSX 100. For example, the model may be derived from an external directory via a Lightweight Directory Access Protocol (LDAP) client interface.

FIG. 4 illustrates a UML representation 400 for restricting access to management commands according to one embodiment. Management commands are provided for
users to access to storage elements 104. For example, management commands include query for available storage elements, map Xgigabytes of storage with a specific QoS to a given Logical Unit Number (LUN) consumer, start a snapshot copy of a given virtualized storage element, etc.  

[0031] In one embodiment, users 304 are assigned command access levels. Each level designates commands that are permitted for users in the level and any number of command access levels may be available. Also, command access levels may be customized for each user and include a list of accessible commands for each user.  

[0032] In one embodiment, command access levels may be implemented using roles 402 and features 404. Roles 402 are determined for each command access level and provide different levels of command access. In one example, roles 402, such as administrator, privileged operator, and basic operator, are separated based on the roles that different users of organizations might fall under. Each role 402 is granted access to one or more features 404 where a feature is a list of commands that are permitted for that feature. The use of features allows the logical grouping of commands into a single entity.  

[0033] In one example, the administrator role may be assigned access to all features, the privileged operator assigned access to features with read commands and write commands, and the basic operator assigned access to features with read-only commands. Thus, users 302 are assigned roles based on the desired command access level for specific users.  

[0034] When a user logs into VSX 100, the user’s corresponding access to various management commands is determined. For example, VSX 100 determines the user’s role 402 and corresponding features 404. The user may then execute only the commands found in the user’s role and corresponding features.  

[0035] The use of features 404 also allows the licensing of access levels. Different access levels may be priced at different levels based on the commands that are included and/or the number of included features. Also, different features may be licensed.  

[0036] FIG. 5 illustrates a UML representation 500 for binding the organizational model to storage resources according to one embodiment. A map 502 of storage elements 104 is stored in or accessible to VSX 100. Map 502 may include a map of hosts 106, storage elements 104, and various ports and connections for hosts 106 and storage elements 104. In one embodiment, map 502 is discovered and created using systems and methods disclosed in U.S. Pat. No. 7,203,730 entitled, “Method and Apparatus for Identifying Storage Devices,” U.S. Pat. No. 6,801,992 entitled, “System and Method for Policy Based Storage Provisioning and Management,” and U.S. Pat. No. 7,272,848 entitled, “Method for Device Security in a Heterogeneous Storage Network Environment.”  

[0037] Storage resources of SAN 102, such as storage devices 104, host computers 106, and the like, are mapped to specific units in organization 102 and may be shared among multiple organizations, among multiple units, or be dedicated to one unit. When a storage resource is bound to an organization or unit, it is accessible to the organization or unit. The management of the virtual storage pool of VSX 100 is secured via a user’s role and storage resources assigned to the user’s unit or organization. However, it is important to note that the centralized location of VSX 100 actually secures the access of the storage at the port level, as only the upstream host 106 ports to which the storage is mapped may see the storage on their physical SAN connections. For example, LUN on a storage device and even ports on a storage device may be mapped to an organization.  

[0038] VSX 100 determines which storage elements 104 are available for management for each unit of organization 102. Using map 502 and model 302, a list of storage elements 104 is bound to each unit of organization 302.  

[0039] Storage devices 104 may be bound to organization 302 by VSX 100 after receiving a command from an administrator of organization 302. Also, VSX 100 may discover storage devices and automatically bind them to organization 302. Thus, the administrator or VSX 100 may initiate assignments of storage elements 104 to units in organization 302 and VSX 100 binds the assigned storage elements using map 502 and model 302.  

[0040] Once storage devices 104 have been bound to units, users may access storage elements 104 that are assigned to the user’s unit. Additionally, in one embodiment, a user may access all storage devices bound to units that are children of the user’s unit. Storage devices 104 that are bound to a user’s unit affect the results of management commands for the user. For example, VSX 100 determines the unit that a user is assigned to when the user logs into VSX 100. Once the unit is known, the list of storage devices that are bound to the unit is retrieved. As mentioned above, the bound storage devices may also include storage devices that are bound to children units. When the user queries for a list of hosts or available storage (assuming the command is allowed by the user’s command access level), the results of the query are filtered to return only the list of hosts or available storage bound to the user’s unit.  

[0041] A user may also change the unit the user is associated with to another unit to ensure that commands will only affect storage devices 104 bound to the new unit. For example, the user may change to a unit lower in the hierarchy, such as a child unit. Commands will then affect only resources bound to the child unit and not all the resources bound to the user’s former unit. For example, an administrator in the root unit may wish to change to the finance unit if the administrator is configuring storage for the finance organization. Thus, only resources accessible to the finance unit are used during the configuration.  

[0042] FIG. 6 illustrates a method for sharing resources according to one embodiment. In step S600, organization 302 is modeled in a structure including one or more units. In step S602, command access levels are associated with users in the units. An administrator may issue commands to VSX 100 to assign the levels to users or VSX 100 may assign the levels.  

[0043] In step S604, storage devices 104 are bound to units in the organization. The administrator may issue commands to VSX 100 to bind specific storage elements 104 to specific units or VSX 100 may automatically bind storage elements 104. In one embodiment, storage elements 104 are bound to units by their port addresses.  

[0044] Once storage devices 104 are bound and command access levels are assigned, storage may be securely shared among units. In step S605, a user logs into VSX 100. In step S606, VSX 100 restricts access to commands corresponding to a user’s command access level. Additionally, in step S608, VSX 100 restricts access for the user to storage resources bound to the user’s unit.  

[0045] Thus, VSX 100 allows the secure sharing of storage resources among different units and users. VSX 100 facili-
tates managing resources in an organization by restricting access to commands for users and restricting access to storage elements 104 for units.

[0046] FIG. 7 illustrates a method for securely managing storage resources according to one embodiment. In step S700, a user logs into VSX 100. In step S702, the user issues a management command.

[0047] VSX 100 then determines the command access level for the user (S704) and storage devices 104 that are bound to the user's unit (S706). In step S708, VSX 100 performs the command using one or more storage devices 104 bound to the unit if the management command is available for the user's command access level. The user's management command may affect all storage devices 104 bound to the user's unit or only specific storage devices 104 bound to the user's unit.

[0048] The execution of management commands may affect the list of bound storage elements 104 to units or command access levels of users. Thus, in step S710, the list of bound storage elements 104 is updated for organization 102. Additionally, in step S712, command access levels are updated.

[0049] Embodiments of the present invention may also be used to provide asset management, enforce port/packet level LUN security, and enforce Service Level Agreements (SLAs).

[0050] VSX 100 provides asset management for organization 302 by discovering storage elements 104 that are bound to units in organization 302. Thus, an organization may track the organization's assets through VSX 100 at a unit and organization level. Also, the tracking may even be broken down at a port level.

[0051] Additionally, quotas limiting the quantity of storage elements 104 that are bound to organization 302 and/or to units of organization 302 may be assigned. The quotas may include a specific number of storage elements or specific number of ports in a storage element. Quotas prevent an organization from acquiring too many storage elements 104 or too much of a single storage element shared across units or organizations.

[0052] VSX 100 also enforces port/packet level LUN security. For example, port/packet level LUN security is disclosed in U.S. Pat. No. 7,272,848 entitled, “Method for Device Security in a Heterogeneous Storage Network Environment.” Thus, in addition to providing security through access control to commands and storage elements, VSX 100 provides security at the port level.

[0053] Service level agreements (SLAs) may also be bound to organizations or units of the organizations. The SLAs are then enforced by VSX 100. Quality of Storage Service (QoS) is then ensured for storage bound to units and may be monitored on a unit by unit basis. For example, QoS is enforced is disclosed in U.S. Pat. No. 6,801,992 entitled, “System and Method for Policy Based Storage Provisioning and Management.”

[0054] Embodiments of the present invention allow the secure sharing of storage devices between one or more units. VSX 100 provides access control through assigned command access levels for users and bound storage devices for units. When a user logs in to VSX 100, access is restricted to a list of commands and to bound storage devices. Thus, storage may be securely shared between organizations and units of organizations using access control through VSX 100.

[0055] The above description is illustrative but not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

What is claimed is:

1. A method for sharing a plurality of storage resources for an organization, wherein the organization is modeled as an organizational model having a plurality of units, wherein one or more users are assigned to each unit of the plurality of units of the organizational model, the method comprising:

   - mapping the plurality of storage resources to the plurality of units of the organizational model, wherein, for each unit of the plurality of units, one or more storage resource of the plurality of storage resources is mapped to a corresponding unit of the plurality of units;
   - establishing access restrictions to storage resource management commands by the one or more users assigned to each unit, wherein command access levels assigned to the one or more users assigned to each unit are used to establish the access restrictions to storage resource management commands; and
   - securing access to the plurality of storage resources using the storage resource mapping and the access restrictions to provide secure unit-based storage resource access, wherein the secure unit-based storage resource access is secured at a port level through use of the mapping whereby storage resources of the plurality of storage resources are only visible via ports of host devices to which a storage resource of the storage resources is mapped, and wherein the secure unit-based storage resource access is secured at a user level through use of the access restrictions whereby storage resource management commands are only available to users assigned to each unit in accordance with the access restrictions to the storage resource management commands.

2. The method of claim 1, further comprising:

   - binding the storage resources to the mapped corresponding units of the plurality of units, wherein storage resources bound to a unit are available for access to users assigned to the unit to which a storage resource is bound.

3. The method of claim 2, wherein the securing access to the plurality of storage resources comprises:

   - imposing the access restrictions for a user and limiting application of storage resource commands by the user to the one or more storage resource of the plurality of storage resources bound to a unit to which the user is assigned.

4. The method of claim 2, wherein storage resources bound to a particular unit of the plurality of units are available for access to users assigned to the particular unit in accordance with the access restrictions established for that particular unit.

5. The method of claim 1, wherein the organizational model provides a hierarchical organization of the plurality of units.

6. The method of claim 5, wherein the hierarchical organization comprises a parent-child relationship of units.

7. The method of claim 6, wherein a user is allowed access to storage resources bound to all units that are children of a unit to which the user is assigned.

8. The method of claim 1, further comprising:

   - implementing the access restrictions to storage resource management commands using roles and features for each unit of the plurality of units, wherein the roles
provide different levels of command access for each command access level, wherein each feature provides commands that are permitted for that feature, and wherein each role is granted access to one or more features.

9. A storage management system for sharing a plurality of storage resources for an organization, the system comprising: an organizational model, stored in memory of the storage management system, of an organization having a plurality of units, wherein one or more users are assigned to each unit of the plurality of units of the organizational model, wherein, for each unit of the plurality of units, one or more storage resource of the plurality of storage resources is mapped to a corresponding unit of the plurality of units;

access restrictions to storage resource management commands, stored in memory of the storage management system, by the one or more users assigned to each unit, wherein command access levels assigned to the one or more users assigned to each unit establish access restrictions to storage resource management commands; and

instructions, operable upon a device of the system, securing access to the plurality of storage resources using the storage resource mapping and the access restrictions to provide secure unit-based storage resource access, wherein the secure unit-based storage resource access is secured at a port level through use of the mapping whereby storage resources of the plurality of storage resources are only visible via ports of host devices to which a storage resource of the storage resources is mapped, and wherein the secure unit-based storage resource access is secured at a user level through use of the access restrictions whereby storage resource management commands are only available to users assigned to each unit in accordance with the access restrictions to the storage resource management commands.

10. The system of claim 9, further comprising: instructions, operable upon a device of the system, binding the storage resources to the mapped corresponding units of the plurality of units, wherein storage resources bound to a unit are available for access to users assigned to the unit to which a storage resource is bound.

11. The system of claim 10, further comprising: instructions, operable upon a device of the system, imposing the access restrictions upon a user and limiting application of storage resource commands by the user to the one or more storage resource of the plurality of storage resources bound to a unit to which the user is assigned.

12. The system of claim 10, wherein storage resources bound to a particular unit of the plurality of units are available for access to users assigned to the particular unit in accordance with the access restrictions established for that particular unit.

13. The system of claim 9, wherein the organizational model provides a hierarchical organization of the plurality of units.

14. The system of claim 13, wherein the hierarchical organization comprises a parent-child relationship of units.

15. The system of claim 14, wherein a user is allowed access to storage resources bound to all units that are children of a unit to which the user is assigned.

16. The system of claim 9, further comprising: instructions, operable upon a device of the system, implementing the access restrictions to storage resource management commands using roles and features for each unit of the plurality of units, wherein the roles provide different levels of command access for each command access level, wherein each feature provides commands that are permitted for that feature, and wherein each role is granted access to one or more features.

17. A method for sharing a plurality of storage resources for an organization, wherein the organization is modeled as an organizational model having a plurality of units, wherein one or more users are assigned to each unit of the plurality of units of the organizational model, the method comprising:

mapping the plurality of storage resources to the plurality of units of the organizational model, wherein, for each unit of the plurality of units, one or more storage resource of the plurality of storage resources is mapped to a corresponding unit of the plurality of units; and

establishing access restrictions to storage resource management commands by the one or more users assigned to each unit, wherein the access restrictions comprise command access levels having roles and features for each unit of the plurality of units, wherein the roles provide different levels of command access for each command access level, wherein each feature provides commands that are permitted for that feature, wherein each role is granted access to one or more feature, and wherein command access levels assigned to the one or more users assigned to each unit are used to establish the access restrictions to storage resource management commands in accordance with its roles and features.

18. The method of claim 17, further comprising:

securing access to the plurality of storage resources using the storage resource mapping and the access restrictions to provide secure unit-based storage resource access, wherein the secure unit-based storage resource access is secured at a port level through use of the mapping whereby storage resources of the plurality of storage resources are only visible via ports of host devices to which a storage resource of the storage resources is mapped, and wherein the secure unit-based storage resource access is secured at a user level through use of the access restrictions whereby storage resource management commands are only available to users assigned to each unit in accordance with the access restrictions to the storage resource management commands.

19. The method of claim 18, further comprising:

binding the storage resources to the mapped corresponding units of the plurality of units, wherein storage resources bound to a unit are available for access to users assigned to the unit to which a storage resource is bound, wherein storage resources bound to a particular unit of the plurality of units are available for access to users assigned to the particular unit in accordance with the access restrictions established for that particular unit.

20. The method of claim 19, wherein the securing access to the plurality of storage resources comprises:

imposing the access restrictions for a user and limiting application of storage resource commands by the user to the one or more storage resource of the plurality of storage resources bound to a unit to which the user is assigned.