Utilizing VMware vSphere Virtual Volumes (VVOL) with the FUJITSU Storage ETERNUS DX S3 series

Reference Architecture for Virtual Platforms (15VM/iSCSI)

The ETERNUS DX S3 series now supports VMware vSphere Virtual Volumes (VVOL).
This document provides an overview of VVOL and explains how to implement this function.

Table of Contents

List of Figures

List of Tables

Preface

Purpose of this document

This document shows a verified reference architecture for virtual platforms that are created with the FUJITSU Storage ETERNUS DX S3 series and FUJITSU Server PRIMERGY using VMware vSphere Virtual Volumes (hereinafter referred to as VVOL).

The following information is provided in this document:

- VVOL configuration procedure
- VVOL operation procedure

Intended audience

This document is intended for personnel who have knowledge of VMware vSphere and are engaged in designing, configuring, or operating the system.

Therefore, basic information for creating VVOLs such as the procedures from the installation to the setup of VMware ESXI and vCenter Server, and the setup procedure of vSphere HA is omitted here.

Other information

Note that because the procedures and screens that are used here are based on our verification machine, different operations may be necessary depending on the system configuration and the environment used.

October 2015

1 VVOL Overview and Implementation Requirements

This chapter provides an overview of VVOLs and the requirements for implementing VVOLs.

1.1 VVOL Overview

1.1.1 What is VVOL?

VMware Virtual Volume (VVOL) is a new storage management technology added to VMware vSphere 6.0.

Conventional storage operations using VMFS required complicated volume assignments and operations while taking into account resource allocations for virtual machines due to multiple VMDK (virtual disk) assignments to a single storage volume (LUN).

In storage operations using VVOLs, a storage volume is assigned to each VMDK of the virtual machine to allow the storage system to manage the storage for each virtual machine.

By allowing the storage to be used by each virtual machine, functions such as backup and performance management that were previously performed only for storage volumes can be set for each virtual machine.
In addition, reducing the administrative workload that is caused by separating the storage administrators from the virtual machine administrators is possible.

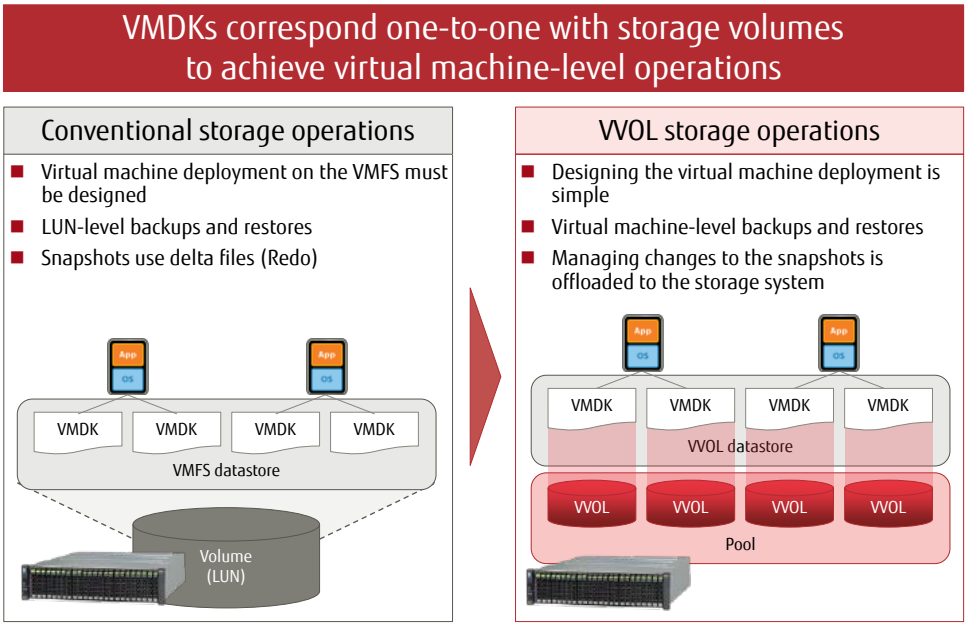

Figure-1 Storage operations with VVOLs

1.1.2 Main Features of the VVOLs that Fujitsu Provides

Fujitsu provides VVOL environments with the implementation of the ETERNUS DX S3 series (excluding the DX60 S3), ETERNUS SF, and ETERNUS VMware vSphere Storage APIs for Storage Awareness (VASA) Provider.
The following figure shows the storage systems that support VVOLs.

- ETERNUS DX S3 series (excluding the ETERNUS DX60 S3)

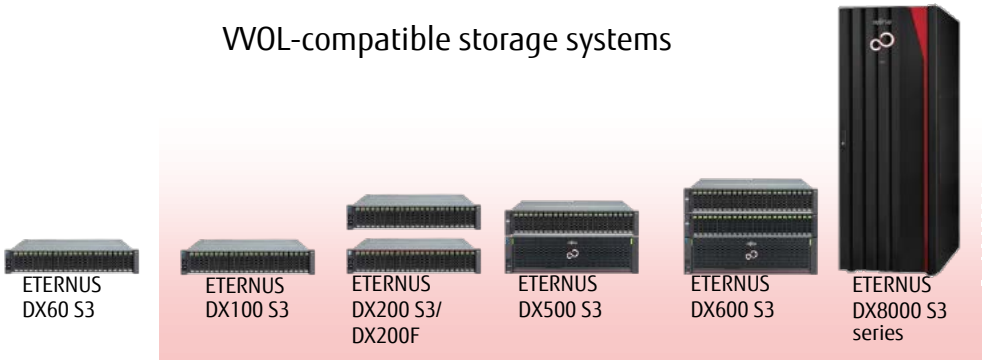

Figure-2 VVOL-compatible storage systems

- ETERNUS SF

  General name for Storage Software.
  ETERNUS SF Storage Cruiser and ETERNUS SF AdvancedCopy Manager used for implementing VVOLs are described below.

  - ETERNUS SF Storage Cruiser

    An integrated management software for storage systems. This software ensures stable operations of entire storage systems that are composed of the ETERNUS as the main device and other devices such as SAN network devices by managing the configuration, performance, and failures of the entire storage system.
    ETERNUS SF Storage Cruiser can further reduce costs and provide more stable operation in combination with various optional features for different purposes; Automated Storage Tiering to optimize storage investments, Automated QoS to automatically adjust I/O resource allocations according to business requirements, guaranteeing data integrity between storage systems, and automatic switchovers of I/O access paths.
    In VVOL environments, VVOL operations that are performed from vCenter Server are run via ETERNUS VASA Provider.

  - ETERNUS SF AdvancedCopy Manager

    This software allows high-speed backups/restores and replication operations using the Advanced Copy functions.
    In VVOL environments, clone backups and snapshot backups can be performed.

- ETERNUS VASA Provider

  An API that enables vCenter Server to acquire device information by linking with the storage system.
  By installing ETERNUS VASA Provider in the operation management server for ETERNUS SF Storage Cruiser, the ETERNUS Disk storage system becomes VASA compatible, and virtual infrastructures of the storage can be integrated and operations can be managed.

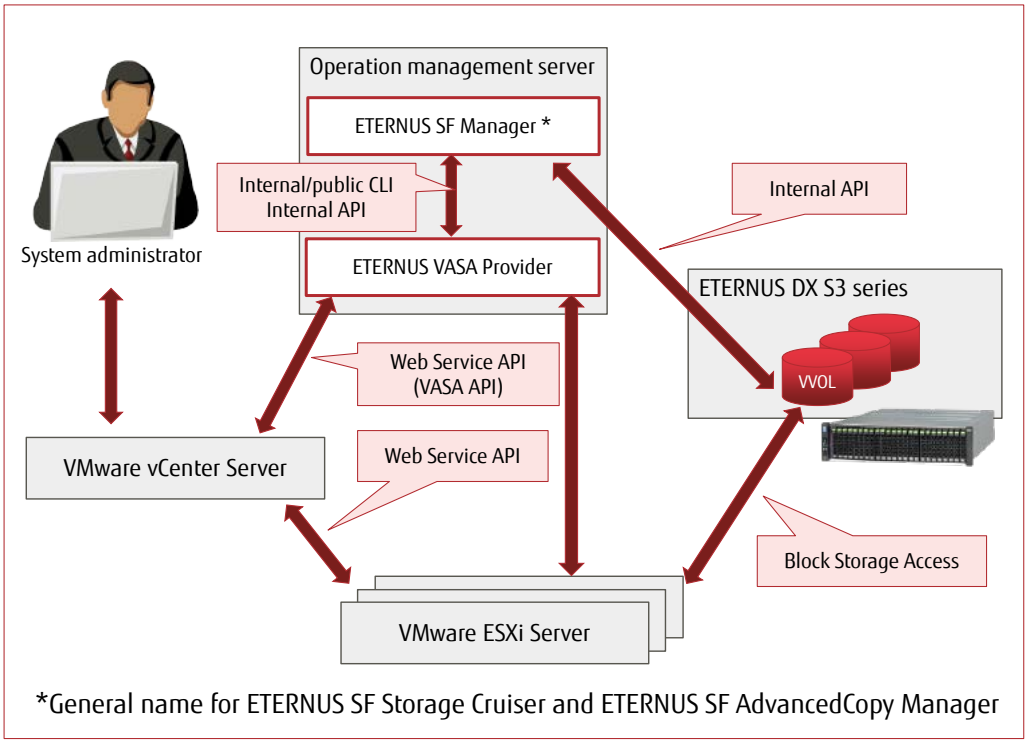

Figure-3 Structure for creating a VVOL environment

Implementation of VVOLs can provide the following operational efficiencies:

- Simple design and scalability
  Multiple virtual machines with different operational requirements can be deployed in the same datastore.
  Volumes can be properly allocated from the datastore to easily add virtual machines without having to consider VMDK assignments.
  When creating virtual machines, the system administrator can also operate and manage the storage simply by operating vCenter Server.

- Workload reduction during implementation
  A complicated design to divide volumes is not necessary since the only requirement for implementing VVOLs is to create a pool. The man-hours are greatly reduced during the configuration since LUN masking only needs to be performed when a pool is created. Furthermore, the necessary system environment can be easily deployed just by configuring a storage policy while creating virtual machines from vCenter Server.

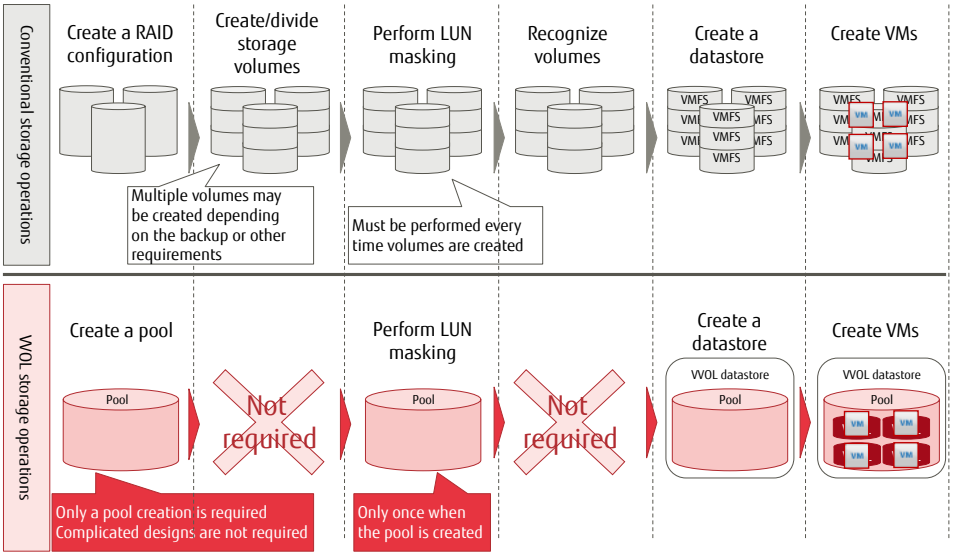

Figure-4 Comparison of implementation works

- Simple operation from vCenter Server (storage policy)
  The service level (such as performance, availability, and backup) that is required for the storage can be set as storage policies from the vCenter Server screens. Virtual machines can be created or volumes can be added simply by selecting storage policies and datastores from the vCenter Server screens.
  Operations using storage policies substantially reduce time and effort in the design phase by automatically distributing resources among the virtual machines. In the operation phase, management of the virtual machines and the storage can be unified.

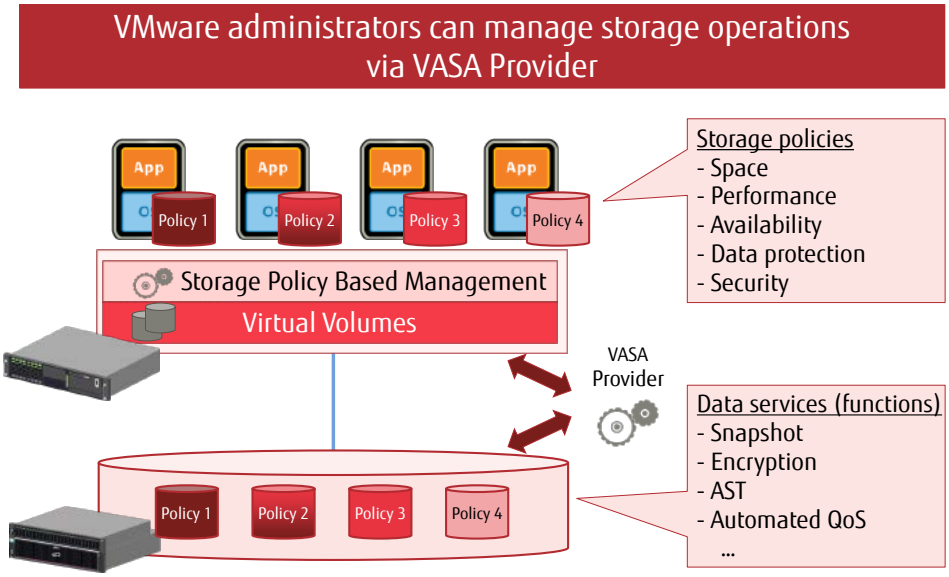

Figure-5 Storage policy

- Easy, reliable virtual machine backups

  In a VVOL environment, backup operations are automatically performed by setting backup policies that define schedules and the number of generations.
  By acquiring full clones, the system can be immediately recovered even in the unlikely event of a physical failure.
  With Fujitsu's original function, clone backups can be taken at the same time as snapshot backups.

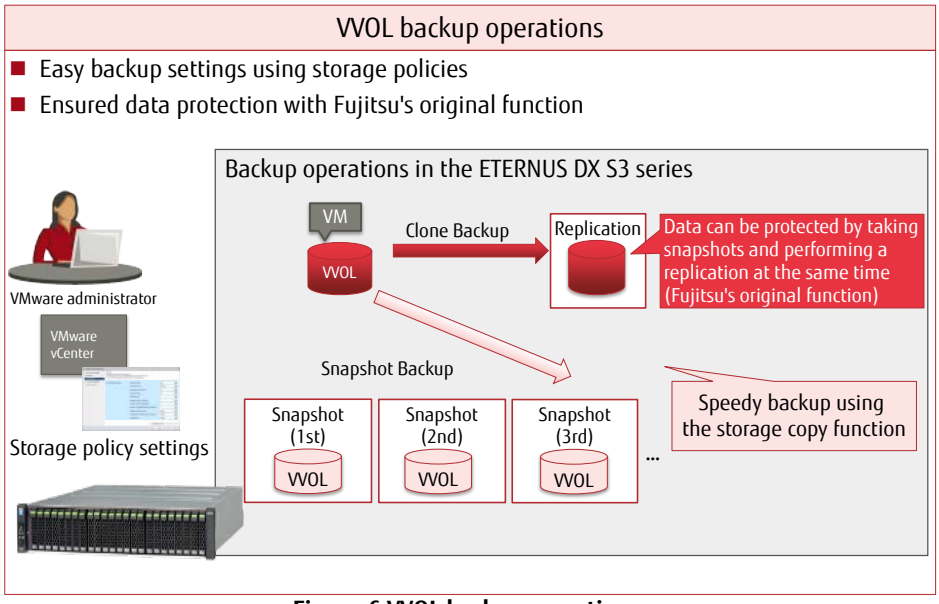

Figure-6 VVOL backup operations

- Virtual machine-level/file-level restores

  VVOLs allow virtual machine-level restores because virtual disks (VMDK) have a one-to-one relationship with storage volumes.
  In addition, file-level restores are also supported by Fujitsu's original function.
  For file-level restores, only the necessary files are restored from snapshots using temporary volumes.

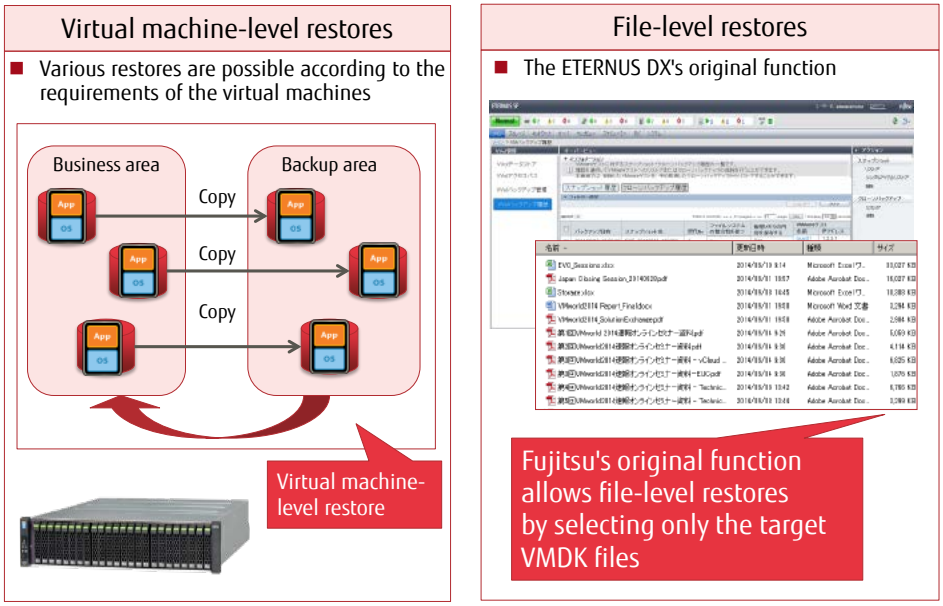

Figure-7 Virtual machine-level/file-level restores

- Efficient operation using Fujitsu's original policy settings
  Items related to storage operations such as backup policies and the priority level of Automated QoS can be easily set as policies from vCenter Server. Simply by applying policies when creating the virtual machines, the VMware administrator can easily assign datastores that match the requirements of the virtual machines without the need to coordinate with the storage administrator. In this way, operational efficiency can be improved.
  In addition, with Fujitsu's original user-friendly policy setting screens, various storage functions can be easily set up.

Various storage functions can easily be set up from vCenter

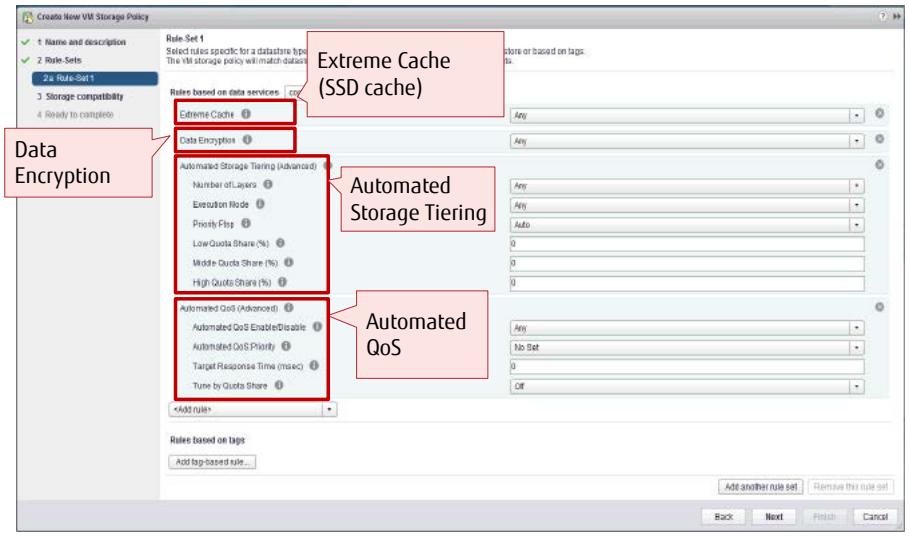

Figure-8 Storage policy setting screen

1.2 Requirements for Implementing VVOLs Using the ETERNUS DX S3 series
The following sections describe the requirements for implementing VVOLs using the ETERNUS DX S3 series:

1.2.1 Configuration Requirements
The following configuration is required for implementing VVOLs:

- VMware ESXi host (physical server)
  VMware vSphere 6.0 or later is required to use VVOLs. The Standard Edition or higher license is also required.
  Prepare the required number of physical servers that are compatible with VMware ESXi 6.0.

- Disk storage system
  Prepare the VVOL-compatible ETERNUS DX S3 series or the ETERNUS DX200F.
  Fibre Channel (FC) and iSCSI connections are supported. Fibre Channel switches are required for Fibre Channel environments.

- Management server
  - vCenter server
    A server in which vCenter Server is installed. This server can also be installed in a virtual machine.
    With VMware vCenter Server Appliance, vCenter Server can be installed as pre-configured virtual machine.

  - Operation management server
    A Windows server in which ETERNUS SF Manager (ETERNUS SF Storage Cruiser) and ETERNUS VASA Provider are installed. This server can also be installed in a virtual machine.
    Install ETERNUS VASA Provider and ETERNUS SF Manager in the same server. vCenter Server and ETERNUS VASA Provider cannot be installed in the same server.

- DNS server
  This server is required for vCenter Server, VMware ESXi hosts, and the operation management server to check the FQDN of one another.
  An Active Directory server can be used as an alternative.
  When using vCenter Appliance, the DNS must be able to resolve the vCenter Server's FQDN during the installation.

- NTP server
  A server for synchronizing the clocks of vCenter Server, VMware ESXi hosts, the operation management server, and the ETERNUS DX S3 series using the NTP service.

1.2.2 Software Requirements

The following software is required for implementing VVOLs:

- VMware vSphere 6.0 Standard or higher
- VMware vCenter Server 6.0 or vCenter Appliance 6.0
- ETERNUS SF Storage Cruiser (V16.2 or later)*
- ETERNUS VASA Provider (V2.0 or later)

* The ETERNUS SF Storage Cruiser Optimization Option is required for Automated Storage Tiering.
The ETERNUS SF Storage Cruiser QoS Management Option is required for Automated QoS.

The following software is also required to perform snapshot backups using storage policies and clone backups for the virtual machines:

-ETERNUS SF AdvancedCopy Manager (V16.2 or later)

1.2.3 Licenses

The following software licenses are required for implementing VVOLs:

- VMware vSphere 6.0 Standard or higher
- VMware vCenter Server 6.0 Foundation or Standard
- Windows Server 2012 Standard (for the operation management server)
- ETERNUS SF Storage Cruiser Standard Edition

The following software license is required to perform snapshot backups using storage policies and clone backups for the virtual machines:

- ETERNUS SF AdvancedCopy Manager Standard Edition

Install the required number of licenses for VMware vSphere 6.0 and Windows Server 2012 according to the number of CPUs of the physical servers that are to be used.
(Separately install the licenses that are required for the business servers that operate as virtual machines.)

1.2.4 Points to Consider for Implementing VVOLs

This section provides points to consider when implementing VVOLs.

■ Management server

The vCenter server and the operation management server are necessary for the operation of the virtual machines that use VVOLs.
In order to configure the vCenter server and the operation management server on the virtual machines, datastores must be created in VMFS volumes.

■ Storage operation

- Storage policy

The ETERNUS DX S3 series provides the following storage policies:

(1) Virtual machine backups (clone backups and snapshot backups)
(2) Automated QoS
(3) Automated Storage Tiering (AST)
(4) Cache (policy related to the Extreme Cache settings or the Extreme Cache Pool settings)
(5) Security (policy related to encryption)

Clone backups (1) and (2) to (5) are expansion functions.
This document describes virtual machine backups (1).

- Volume management

When VVOLs are used, the number of management volumes is included in the maximum number of volumes that can be created in the storage system. In addition, multiple VVOLs are required for each virtual machine. Therefore, a design that does not exceed the maximum number of volumes is necessary.*

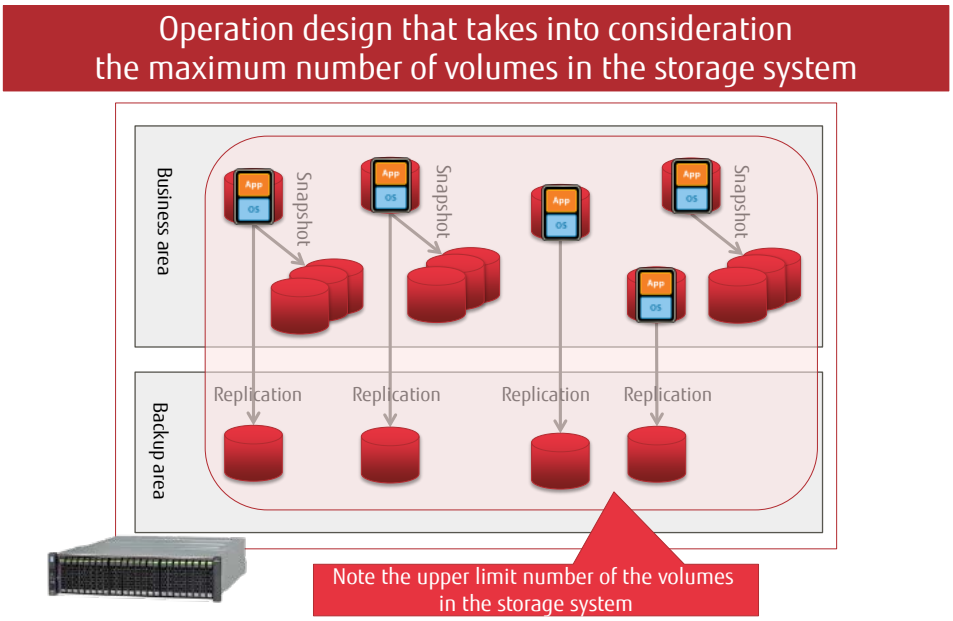

Figure-9 Operation design that takes into consideration the maximum number of volumes in the storage system

* For the number of volumes, refer to "4 Notes".

2 VVOL Configuration Workflow

This chapter describes the VVOL configuration workflow and the procedures to operate VVOLs based on the verified configuration.

2.1 Configuration Environment

For virtual machine operations that use VVOLs, management servers are required. In this configuration, a vCenter server and an operation management server that are required for VVOL operations are configured as virtual machines and redundancy is ensured using vSphere HA.
Fifteen business servers are also configured on the same vSphere HA.
iSCSI is used to connect between the ESXi hosts and the storage system, and the SAN is configured in the IP network.

- System overview

The procedures in this chapter are based on the following system configuration.
The contents in this document are described on the assumption that vCenter Server is installed using vCenter Server Appliance.

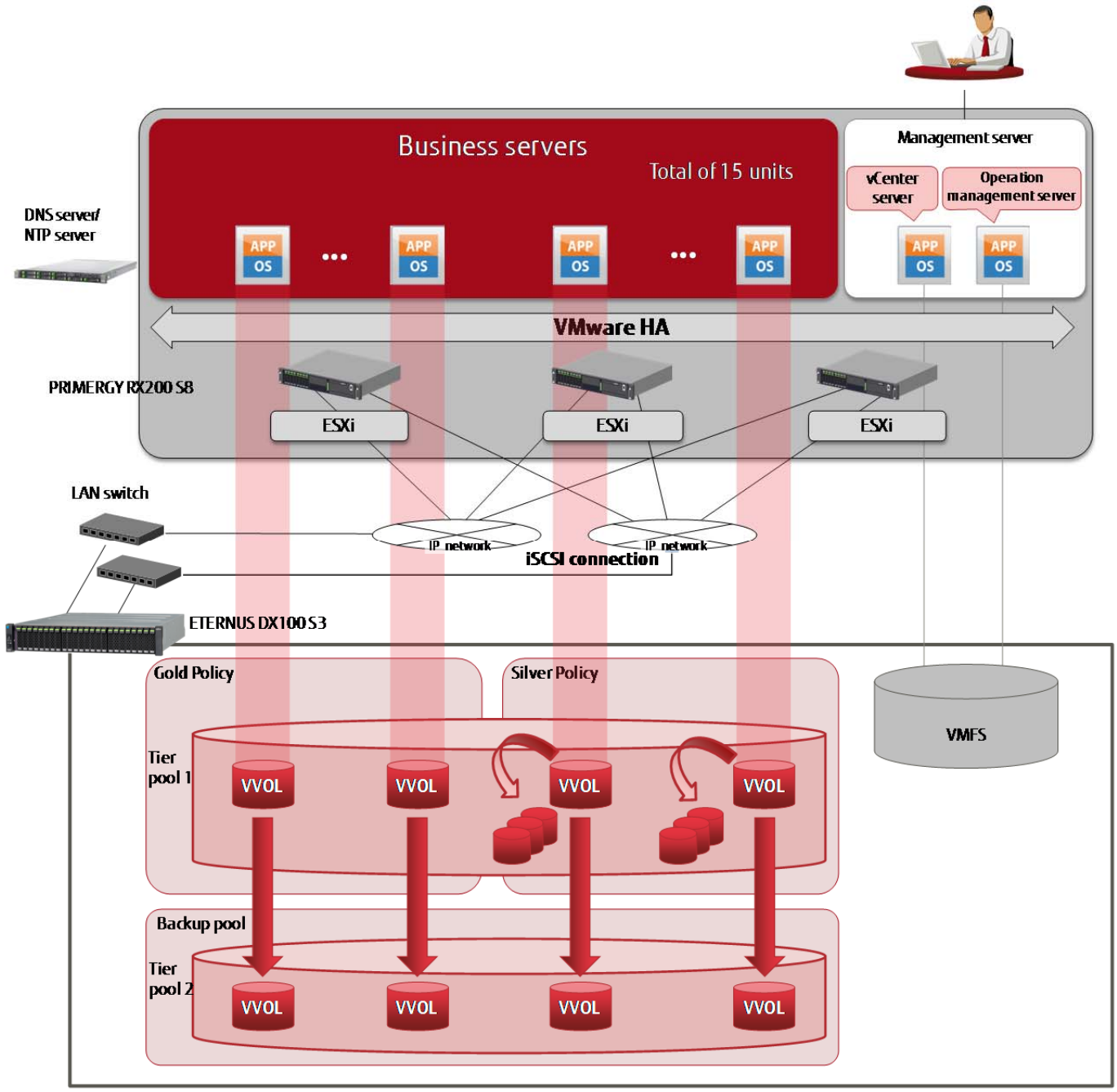

Figure-10 System overview

2.1.1 Component List

■ Hardware/software
- Hardware
  - Disk storage system: ETERNUS DX100 S3 × 1
  - Industry standard server: PRIMERGY RX200 S8 × 3
  - Layer 2 switch × 8

- Software
  - VMware vSphere 6.0 (ESXi)
  - VMware vCenter Server Appliance 6.0
  - Windows Server 2012 R2 (for the operation management server)
  - ETERNUS SF Storage Cruiser V16.2
  - ETERNUS VASA Provider V2.0
  - ETERNUS SF AdvancedCopy Manager V16.2 (for clone backups of the virtual machines)
  - Red Hat Enterprise Linux 7 (for the business server)

■ Configuration information
- Management servers and business servers (physical machines)
  vSphere HA was configured with three PRIMERGY RX200 S8 servers and virtual machines were created with two management servers and 15 business servers.
  The following table shows the physical configuration of each physical server.

CPU	Memory	Internal disk [RAID level]	LAN port
Intel® Xeon® processor 2.40GHz 12 cores × 2 CPUs	64GB	300GB × 2 [RAID1]	1GB × 8 ports (Quad port LAN card × 2)

Table-1 Physical configuration of each physical server

- Management servers (virtual machines)
  A vCenter server and an operation management server were created in a VMFS datastore.

Server type	Software	CPU	Memory	Disk	Remarks
vCenter server	VMware vCenter Server Appliance 6.0	2vCPU	8GB	120GB (thick)	Appliance size: minimal
Operation management server	Windows Server 2012 R2	4vCPU	5GB	50GB	
	ETERNUS SF Storage Cruiser V16.2				
	ETERNUS SF AdvancedCopy Manager V16.2				
	ETERNUS VASA Provider V2.0				

Table-2 Configuration of the management servers (virtual machines)

- Business servers* (virtual machines)
  Fifteen business servers were created on VVOL datastores.
  For the specifications of the business servers, the 15 virtual machines were configured based on the assumption that they have the standard specifications provided by the cloud service.
  Red Hat Enterprise Linux was installed as the OS.

Server type	No. of units	Software	CPU	Memory	Disk	Snapshot backups	Clone backups
Business server with the Gold policy	5	Red Hat Enterprise Linux 7	2vCPU	4GB	140GB	Without	With
Business server with the Silver policy	10					With	With

Table-3 Configuration of the business servers (virtual machines)

* Although the above business server configuration is used in this document, depending on the virtual machine requirements to be used in actual operations, consider not only the configuration but also the physical resources.

- Disk storage system

Datastores for all the virtual machines (management servers and business servers) were placed in the ETERNUS DX100 S3.
The management servers were placed in a VMFS datastore. (The management servers are necessary to operate the virtual machines on the VVOLs.)

This document assumes that two storage policies are available for the business servers.

- ✓ Gold policy stores systems such as database servers that have frequently updated data
- ✓ Silver policy stores systems such as AP servers that do not require storage performance

When a virtual machine is created, backup operations that use snapshot backups and clone backups are automatically set with a storage policy. Snapshot backups are created in the same Tier pool as the virtual machine. Clone backups require a Tier pool that is different from the Tier pool for VVOLs. Prepare a Tier pool for clone backups.

The following figure shows the disk configuration.

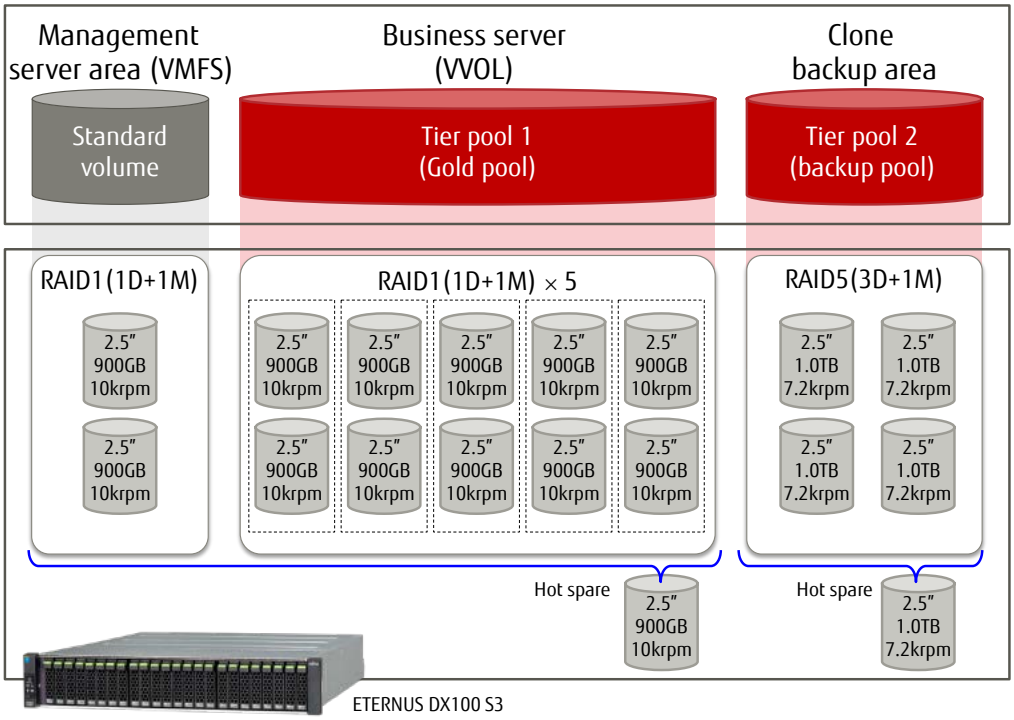

Figure-11 Configuration of the Disk storage system (disks)

Area	Virtual machine usage capacity	Required capacity	Disk	RAID configuration	Available area	Usage
Management server area (VMFS)	170GB	170GB	900GB/10krpm	RAID1(1D+1M)	900GB	vCenter Server, operation management server
Business server area (VVOL)	2,250GB	3,750GB	900GB/10krpm	RAID1(1D+1M) × 5 RAID groups	4,500GB	Business server, snapshots for the business server
Backup area (VVOL)	-	2,250GB	1,000GB/7.2krpm	RAID5(3D+1P)	3,000GB	Backup pool (for clone backups)

Table-4 Configuration of the storage system (disks)

- Switches

Network switches were used for iSCSI connections, management, business, and vMotion.
Each network was redundantly configured.

Type	Model name	Transmission speed / Number of ports	No. of units
Network switch	SR-X316T2	1Gbit/s / 16 ports	8

Table-5 List of switches

- Storage policies

ETERNUS SF's virtual machine backup policies were used in this configuration.

Snapshot backups and clone backups are available as virtual machine backups and the following policies can be set.

Item	Description
Operation Mode	Select the operation mode that specifies how the virtual machine backup function should operate. - Auto: Enables the virtual machine backup function. Backups are automatically performed. - Manual: Enables the virtual machine backup function. Backups are only performed manually. - Disable: Disables the virtual machine backup function. Even if [Auto] or [Manual] is selected for this item, [Disable] is automatically set by the following property settings (or settings that do not take backups). - [0] is specified for [Number of Snapshot Backup Generations] and - [Disable] is specified for [Clone Backup]
Execution Period	Select an interval to automatically perform backups. This item is enabled only when [Auto] is specified for [Operation Mode]. - Hourly: Performs at the specified hourly intervals. If this interval is selected, [Execution Interval(Hour)] must also be set. - Daily: Performs every day at the time specified for [Execution Start Time]. - Weekly: Performs every week on the specified day. If this interval is selected, [Execution Week] must also be set. - Monthly: Performs every month on the specified day. If this interval is selected, [Execution Day] must also be set.
Execution Interval (Hour)	When [Hourly] is specified for [Execution Period], select the hourly execution interval. The time interval that can be selected is 1, 2, 3, 4, 6, 8, or 12.
Execution Week	If [Weekly] is specified for [Execution Period], select an execution day of the week. Multiple days can be selected.
Execution Day	If [Monthly] is specified for [Execution Period], select an execution day. The selectable day is from [1] to [31] or [Last]. Only one day can be selected. When a day is selected from 1 to 31, a backup is performed on the specified day. For the months that do not have the selected day, a backup is not performed. When [Last] is selected, a backup is performed on the last day of the month.
Execution Start Time (Hour)	Select the time (hour) to start an automatic backup. The selectable value is from 0 to 23. This item is enabled only when [Auto] is specified for [Operation Mode].
Execution Start Time (Minute)	Select the time (minute) to start an automatic backup. The selectable value is from 0 to 55 (in 5 minute increments). This item is enabled only when [Auto] is specified for [Operation Mode].
Number of Snapshot Backup Generations	Select the number of generations of snapshot backups to store. The selectable generation number is from 0 to 28. When [0] is selected, snapshot backups are not saved. When using single item restore, snapshot backups are required. For this reason, select [1] or a larger number for this item. When performing only clone backups, specify [Enable] for [Clone Backup] and select [0] for this item. This item is enabled only when [Auto] or [Manual] is specified for [Operation Mode]. When performing a snapshot backup that exceeds the number of generations to store, the oldest generation is automatically deleted after the backup operation.
Quiesce guest file system	Select whether to maintain the integrity of the file system content when a backup is performed. This item is enabled only when [Auto] or [Manual] is specified for [Operation Mode]. - Enable: Maintains the integrity of the file system when a backup is performed. - Disable: Does not maintain the integrity of the file system when a backup is performed.
Snapshot the virtual machine's memory	Select whether to include the memory content when snapshot backups are taken. This item is enabled only when [Auto] or [Manual] is specified for [Operation Mode]. - Enable: Includes the memory content in the snapshot backups. - Disable: Does not include the memory content in the snapshot backups.
Clone Backup	Select whether to take a clone backup. This item is enabled only when [Auto] or [Manual] is specified for [Operation Mode]. - Enable: Takes a clone backup. - Disable: Does not take a clone backup.

Table-6 Virtual machine backup policies

With virtual machine storage policies, backup operations for virtual machines can be set when the virtual machines are created.
In this document, the Gold and Silver policies were created.

Item	Settings for the Gold storage policy	Settings for the Silver storage policy
Operation Mode	Auto	Auto
Execution Period	Daily	Weekly
Execution Interval(Hour)		
Execution Week		Sun
Execution Day		
Execution Start Time(Hour)	22	1
Execution Start Time(Minute)	30	0
Number of Snapshot Backup Generations	0	1
Quiesce guest file system	Enable	Enable
Snapshot the virtual machine's memory	Enable	Enable
Clone Backup	Enable	Enable

Table-7 Created virtual machine storage policies

For Gold storage policies, clone backups are taken with the performance prioritized by setting 0 to the number of snapshot backup generations.
For Silver storage policies, clone backups are taken and snapshot backups that are available for quick recoveries and single item restores are also taken.
By creating multiple policies, the storage policies can satisfy various usages of virtual machines.

■ Physical connection diagram

The business LAN, the operation management LAN, and the LAN for vMotion were connected to all the ESXi hosts.
The ETERNUS DX100 S3 was connected only to the operation management LAN.
A DNS server and an NTP server that were required for the ESXi hosts, the vCenter server, and the operation management server were connected to the operation management LAN.

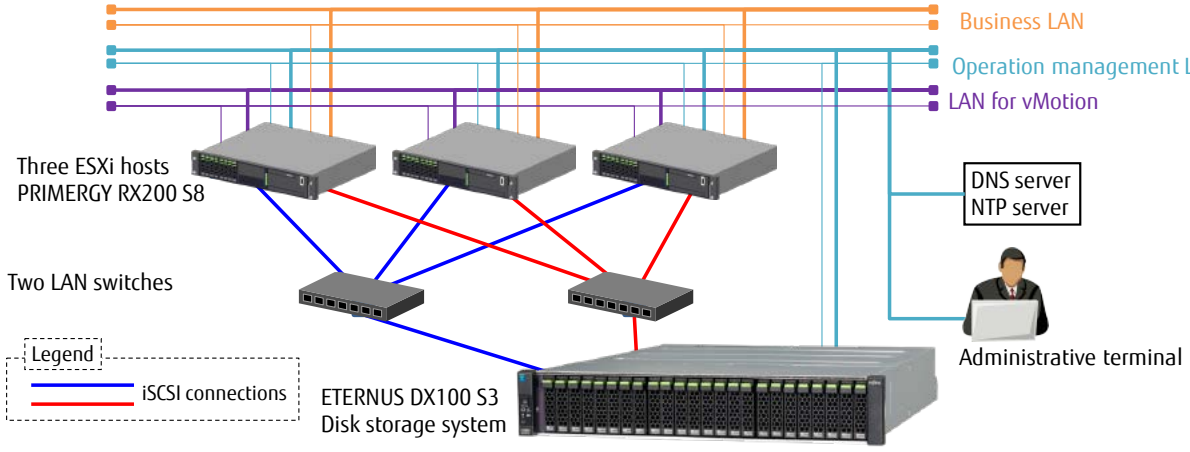

Figure-12 Physical connection diagram

■ Logical connection diagram

The two CMs of the Disk storage system and two NICs on each ESXi host were connected.
iSCSI for the ESXi hosts was connected using the IP address of the VMkernel adapter. A virtual switch was created for each path to be connected to the disk storage system and the VMkernel adapter was connected to the physical NIC.
For the host affinity settings between the management server area and the ESXi hosts, the ETERNUS SF was used normally.
Tier pools 1 to 2 for VVOLs were set as VVOL access paths when VVOL datastores were created.

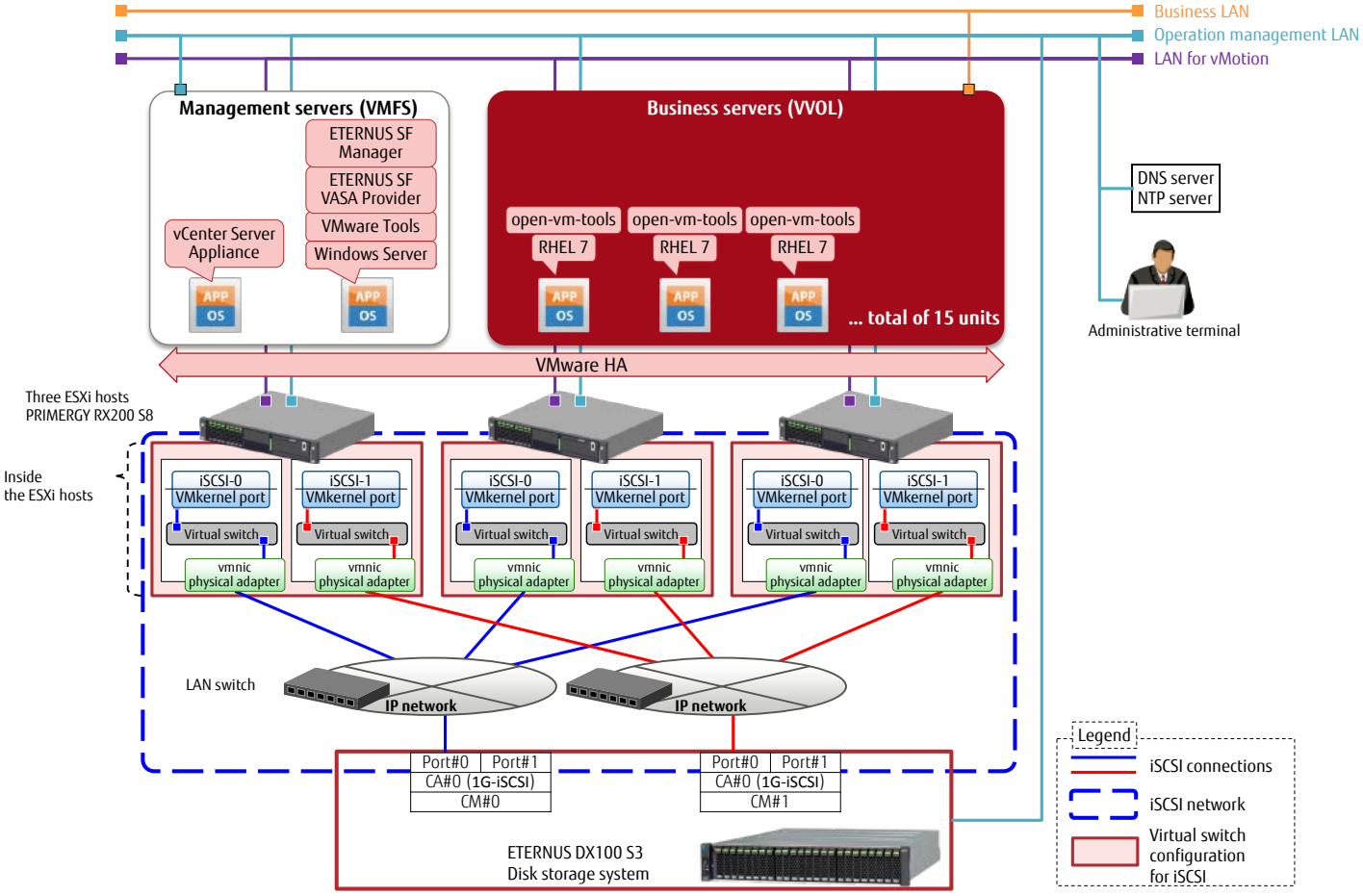

Figure-13 Logical connection diagram

2.2 Configuration Procedures

■ VVOL configuration workflow

The procedures to configure a VVOL environment are described according to the following workflow.

For details, refer to "FUJITSU Storage ETERNUS SF Storage Cruiser V16.2 / AdvancedCopy Manager V16.2 Operation Guide for VMware vSphere Virtual Volumes".

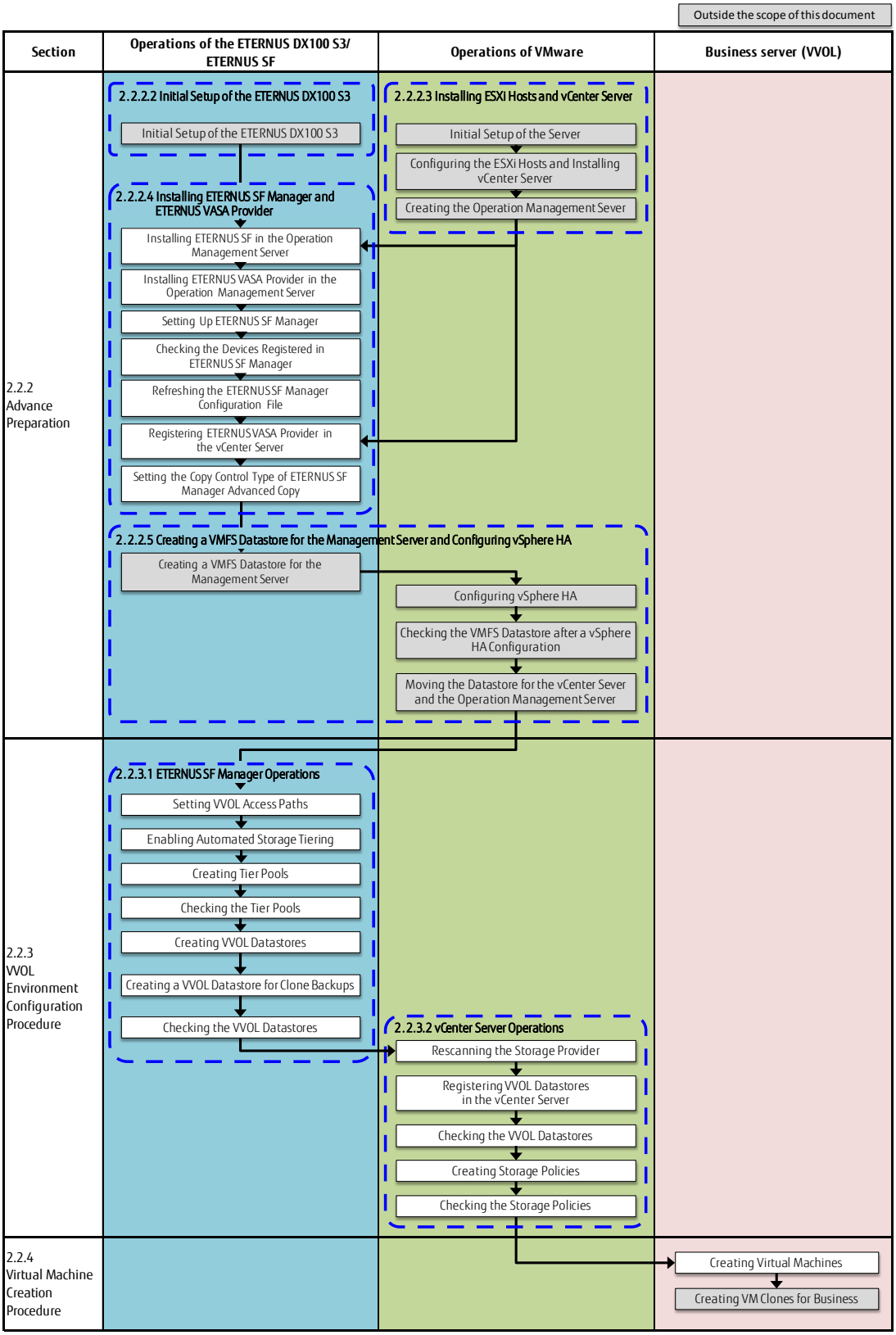

Figure-14 Configuration workflow

2.2.1 Description of ETERNUS SF Web Console

2.2.1.1 Web Console Screen Configuration

The following figure shows the Web Console screen.
This document uses the following screen elements to explain the operations.

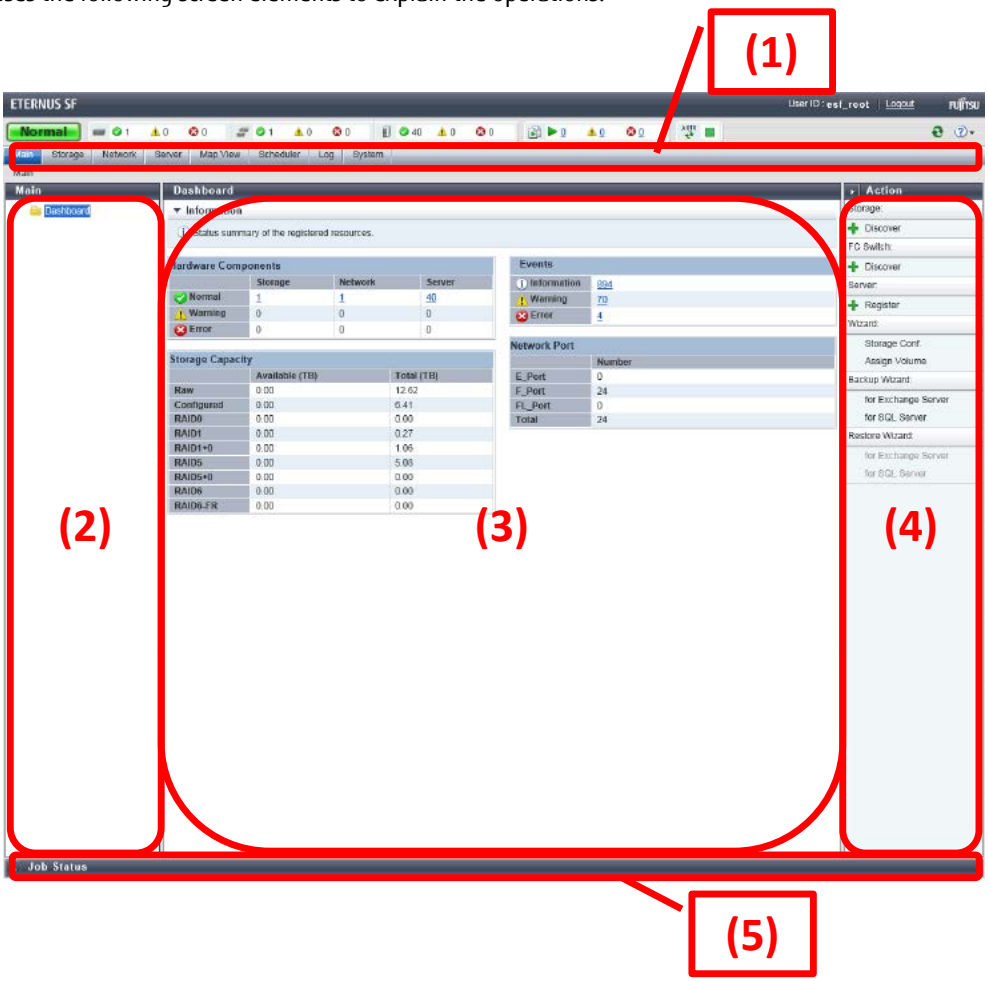

Figure-15 Description of the ETERNUS SF Web Console screen

No.	Item	Description
(1)	Global navigation tab	When a category is clicked in the global navigation tab, the top menu of the category is displayed on the category pane.
(2)	Category pane	Displays a list of categories that can be selected. When each item is clicked, information for the item is displayed on the main pane.
(3)	Main pane	Menus and setting information are displayed. Details of the current main pane are displayed in the [Information] field.
(4)	Action pane	Displays a list of actions that can be performed for an item that is displayed on the main pane.
(5)	Job Status pane	Displays the processing status of the operation that is performed with ETERNUS SF Web Console and a dialog message starting with "The job has been submitted for processing." that can be checked. The bar expands or closes when clicked.

Table-8 Descriptions of the ETERNUS SF Web Console screen

2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations

The ETERNUS SF displays the message "The job has been submitted for processing." when settings are performed. Whether the setting is successful must be checked by a different operation.
Because this confirmation operation is common to almost all ETERNUS SF Web Consoles, refer to this chapter for the settings confirmation.

Points

Open the Job Status pane to check the result of the process that was performed with ETERNUS SF Web Console.
Confirm that "Success" is displayed on the pane and proceed to the next steps.

After a while, the currently running processes are counted as successful or failed and are displayed on the operation status bar on the upper part of the screen.

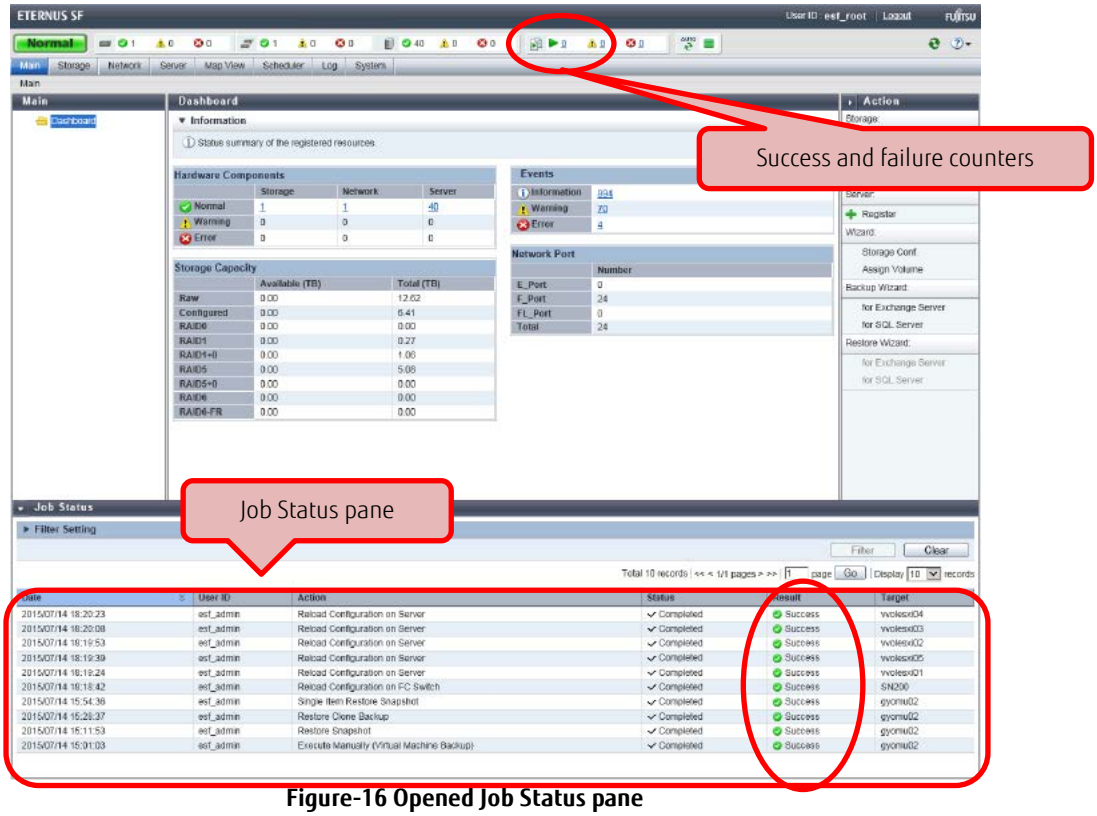

Figure-16 Opened Job Status pane

2.2.2 Advance Preparation

This section explains the required settings of the ETERNUS DX100 S3, ETERNUS SF, and VMware vSphere before starting the work related to VVOLs.

2.2.2.1 Checking Prior to Working

Before starting the work, check the following necessary environments.

- The NTP server is available.
- The host names of the ESXi hosts, vCenter server, operation management server (ETERNUS SF/ETERNUS VASA Provider) are compatible with the standard naming convention in RFC952/1123*.
  (Windows DNS supports extended ASCII and Unicode characters, but the extended characters cannot be used for the ESXi hosts.)
  *Standard naming convention in RFC952/1123: The characters that can be used are "0 to 9", "a to z", "A to Z", "- (hyphen)", and ". (period [only as domain delimiter])".
- The names of the ESXi hosts, the vCenter server, and the operation management server (ETERNUS SF/ETERNUS VASA Provider) can be resolved (with a forward and reverse mapping) using the DNS server.
- Initial setup for the Fibre Channel switches has been completed.

2.2.2.2 Initial Setup of the ETERNUS DX100 S3

Perform an initial setup so that the ETERNUS DX100 S3 can be operated from ETERNUS SF.
To use VVOLs, the Thin Provisioning Pool function must be enabled.

In this document, the following settings are performed to use bidirectional CHAP.

1. On the [Connectivity] Category pane, click [Port Group] and then [iSCSI].
2. In the list of iSCSI ports, select the checkbox for the port to set CHAP authentication and click [Modify iSCSI Port Parameters] on the Action pane.
3. Set the security setting for CHAP to "ON" and specify the CHAP username and password of the server that is to be connected.

For details on the settings and procedures, refer to "Disk Array and All Flash Arrays" under "Environment Configuration" in "FUJITSU Storage ETERNUS SF Storage Cruiser V16.2 Operation Guide".
For details on the settings, refer to "FUJITSU Storage ETERNUS DX Configuration Guide (Web GUI)".

Points

The RAID groups and access paths that are used for the VVOLs must be created and managed with ETERNUS SF Manager.
Therefore, volumes for VMFS that are used by the management server must also be created and managed with ETERNUS SF Manager.
The creation and management of RAID groups and access paths are all performed from ETERNUS SF Manager.
To use VVOLs, the Thin Provisioning Pool function of the ETERNUS DX100 S3 must be enabled.

Checklist

Confirm the following items before proceeding to the next procedure.

- The storage system name has been set.
- The network has been set.
- A user with the Software role has been created.
- The CHAP setting has been enabled and the CHAP user name and password have been set.

The following values will be required in "2.2.2.4.3 Setting Up ETERNUS SF Manager".

Item	Parameter
IP address	(IP address of the management LAN)
SNMP community name	(Arbitrary)
User name	(Name of the user that has the Software role)
Password	(Password)

Table-9 Initial setup of the ETERNUS DX100 S3

2.2.2.3 Installing ESXi Hosts and vCenter Server

Set the ETERNUS DX100 S3 using ETERNUS SF Storage Cruiser that is installed in the operation management server.
Configure the operation management server and the vCenter server in the local disks of the ESXi hosts.

Points

The ETERNUS DX100 S3 must be set using ETERNUS SF Manager. Therefore, configure and set the virtual machines of the management server on the local disks of the ESXi hosts, and then move the virtual machines to the ETERNUS DX100 S3.

2.2.2.3.1 Configuring the ESXi Hosts and Installing vCenter Server

- Configure the ESXi hosts.
  Create a VMFS datastore in a local disk of a single ESXi host.
  Install vCenter Server Appliance in the created datastore.

- Register the ESXi host to the vCenter server.
  (For details on the procedure related to the ESXi hosts and vCenter Server, refer to the VMware vSphere 6.0 documents provided by VMware.)

- Check the LAN card for iSCSI connections.
  Log in to vCenter Server from vSphere Web Client.
  Click [Hosts and Clusters] in the [Home] screen and select the target host on the left pane.
  Select the [Manage] tab - [Networking] - [Physical adapters] to confirm that the LAN card for iSCSI connections is recognized.

- Create virtual switches for iSCSI.
  Add two virtual switches (vSwitch) for iSCSI to VMware ESX. Add one [vmnic] and one [VMkernel] for each vSwitch.
  Perform the following procedure for each vmnic that configures the iSCSI SAN.
  In this document, vSphere Standard Switch is used.

  1. Log in to vSphere Web Client.
     Click [Hosts and Clusters] in the [Home] screen and select the target host on the left pane.

  2. Select the [Manage] tab - [Networking] - [Virtual switches].

  3. Select [Add host networking] on the right pane.
     After the [Add Networking] pop-up screen is displayed, follow the instructions on the screen to add a network.
     (1) Select [VMkernel Network Adapter] and click [Next].
     (2) Select [New standard switch] and click [Next].
     (3) Click [Add adapters] of [Active adapters] on the right pane, select the target NIC, and then click [Next].
     (4) Set a port as necessary and click [Next].
     (5) Set an IP address and a subnetmask for [VMkernel] and click [Next].
     (6) Check the settings and click [Finish].

  4. Repeat Step 3 to add Virtual Switch vSwitch2.

  5. Check that Virtual Switch and VMkernel are set for a single vmnic.

- Enable the Software Initiator of the ESXi host.
  1. Log in to vSphere Web Client.
     Click [Hosts and Clusters] in the [Home] screen and select the target host on the left pane.
  2. Select the [Manage] tab - [Storage] - [Storage Adapters].

  3. Select [iSCSI Software Adapter].

  4. Check the iSCSI Name that is displayed in [Adapter Details].
     If the iSCSI Name is not displayed, perform [Add new storage adapter].

  5. Select the [Targets] tab of [Adapter Details].
  6. Click [Add] of [Dynamic Discovery].

7. In [iSCSI Server], enter the IP address of the iSCSI port for the ETERNUS DX that is to be connected, check that the port is [3260] (default), and then click [OK].

8. Repeat Steps 6 and 7 to set the iSCSI ports of all the ETERNUS DX storage systems that are to be connected.

Checklist

Confirm the following items before proceeding to the next procedure.

- The ESXi host and vCenter Server can communicate with each other correctly.
- A name resolution can be performed correctly.
- The clock has been synchronized.
- The LAN card for iSCSI has been set correctly.

The following values will be required in "2.2.2.4.3 Setting Up ETERNUS SF Manager".
In this document, root users of vCenter Server are assigned Administrator privileges.

Item	IP address	Host name	User name with administrator privileges	Password	Web Client port number	Remarks
vCenter Server	(IP address of the management LAN)	vCenter	root (arbitrary)	********		Record the Web Client port number if it is changed. Default value: 443
ESXi host 1		vvolesxi01	root (arbitrary)	********		
ESXi host 2		vvolesxi02	root (arbitrary)	********		
ESXi host 3		vvolesxi03	root (arbitrary)	********		

Table-10 ESXi and vCenter Server initial setup

2.2.2.3.2 Creating the Operation Management Sever

Configure a virtual machine for the operation management server in the local disk of the ESXi host.
Install Windows Server 2012 R2 in the virtual machine.
(For details on the procedure related to Windows Server 2012 R2, refer to the documents that are provided on the Microsoft website.)

2.2.2.4 Installing ETERNUS SF Manager and ETERNUS VASA Provider

This section provides the procedures that must be performed before creating VVOLs.

2.2.2.4.1 Installing ETERNUS SF Manager in the Operation Management Server

Install ETERNUS SF Manager in the virtual machine of the operation management server that was configured on the ESXi host.
For details, refer to "FUJITSU Storage ETERNUS SF Express V16.2 / Storage Cruiser V16.2 / AdvancedCopy Manager V16.2 Installation and Setup Guide".

1. Install ETERNUS SF Manager in the operation management server.
   Log in to the operation management server with a user that has Administrator privileges.

2. Read "ETERNUS SF SC/ACM/Express Mediapack for Windows Manager Program (1/2)".

3. The initial screen is displayed. Click [Manager installation].

4. The [Choose Setup Language] dialog box is displayed. Select the appropriate language and click the [OK] button.
   The language selected in this dialog box will be used during the installation.

5. In the [Welcome to the InstallShield Wizard for ETERNUS SF Manager] screen, click the [Next] button.

6. In the [License Agreement] screen, read the displayed terms and conditions. If the conditions are agreeable, select [I accept the terms of the license agreement], and then click the [Next] button.

7. In the [Install option] screen, select [ETERNUS SF Manager is installed.] and click the [Next] button.

8. In the [Start Copying Files] screen, check the settings. If the settings are correct, click the [Next] button. To change the settings, click the [Back] button.

9. When the [Installation Complete] screen is displayed, click the [Finish] button.

Checklist

Confirm the following item before proceeding to the next procedure.

- [ETERNUS SF Manager] is displayed in the [Programs and Features] screen of Control Panel.

* *To use the VVOL functions with FUJITSU Storage ETERNUS SF V16.2, patches must be applied.*
For details, contact your Fujitsu sales representative or the support division of your FUJITSU Storage ETERNUS SF V16.2 contract.

2.2.2.4.2 Installing ETERNUS VASA Provider

Install ETERNUS VASA Provider in the virtual machine for the operation management server that was configured on the ESXi host.
For details, refer to "ETERNUS VASA Provider 2.0 User's Guide".

1. Install ETERNUS VASA Provider V2.0.
   Run the installer and click the [Next] button in the [Welcome to the InstallShield Wizard for ETERNUS VMware Support Package] screen.

2. In the [Setup Type] screen, select a setup type and click the [Next] button.
   [Complete] is selected in this document.

3. In the [License Agreement] screen, read the displayed terms and conditions. If the conditions are agreeable, click the [Yes] button.

4. In the [Create ETERNUS VASA Provider Account] screen, enter the items shown in the following table, and then click the [Next] button.
   The account information that is created here will be used to register ETERNUS VASA Provider in vCenter Server.

Item	Information
Provider User name	Arbitrary
Provider Password	Arbitrary

Table-11 Account creation information

5. In the [Setup Server Certificate] screen, enter the items shown in the following table, and then click the [Next] button.

Item	Information
Common Name (Necessary)	Arbitrary (FQDN)
Organization Unit	Arbitrary
Organization Name	Arbitrary
Locality Name	Arbitrary
State Name	Arbitrary
Country Code	Arbitrary

Table-12 Server certificate creation

6. In the [Start Copying Files] screen, review the settings and click the [Install] button.

7. When the [InstallShield Wizard Complete] screen is displayed, click the [Finish] button.

Checklist

Confirm the following item before proceeding to the next procedure.

- [ETERNUS VMware Support Package] is displayed in the [Programs and Features] screen of Control Panel.

2.2.2.4.3 Setting Up ETERNUS SF Manager

- Registration of the target storage system for management

1. Log in to ETERNUS SF Manager of the operation management server.

2. Click the [Storage] tab on the global navigation tab.
   On the Action pane, click [Add].

3. Add an ETERNUS DX S3 series.
   The ETERNUS DX S3 series can be added by searching a subnet or specifying an IP address. The IP address method is used in this document.
   Register the ETERNUS DX100 S3 using the values that were specified in "2.2.2.2 Initial Setup of the ETERNUS DX100 S3".
   Select the [IP Address] radio button.
   Enter the IP address and SNMP community name of the ETERNUS DX S3 series, and click the [Discover] button.

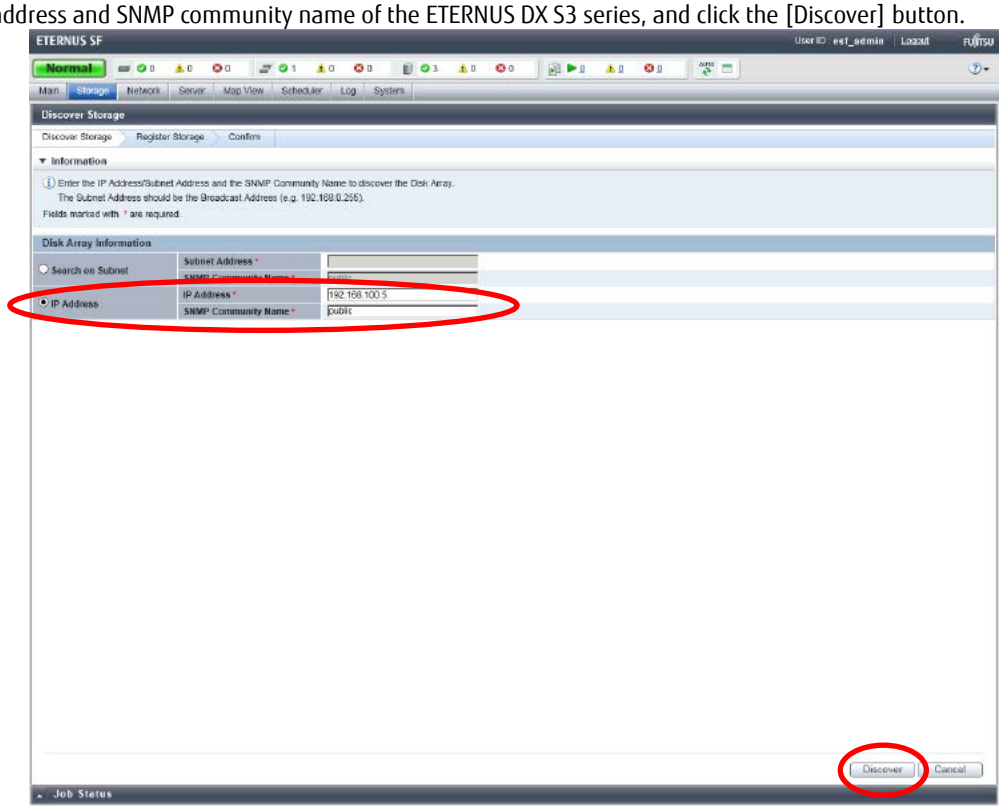

Figure-17 ETERNUS DX S3 series detection

4. When the target ETERNUS DX S3 series is displayed, enter the necessary information and click the [Register] button on the lower right corner of the screen.

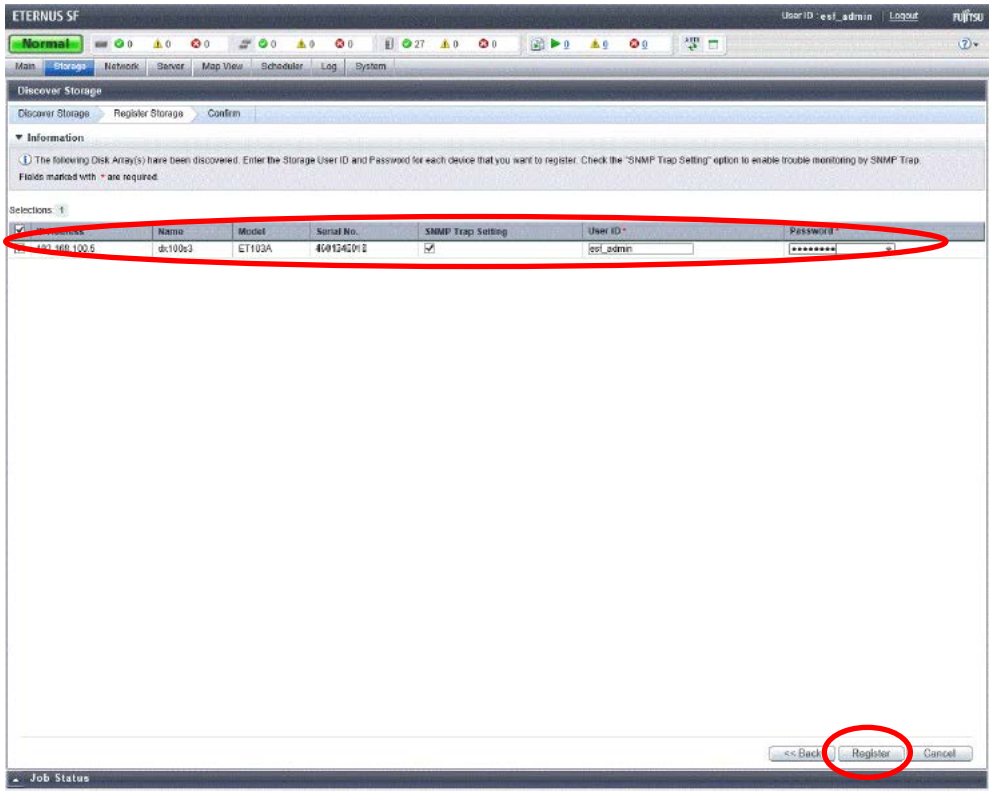

Figure-18 ETERNUS DX S3 series registration

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next step.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".
The registration process may take several minutes to several tens of minutes depending on the storage system configuration.
Wait for the registration process to finish before operating the ETERNUS DX.

5. Register licenses.
   Click the [Storage] tab on the global navigation tab.
   On the Main pane, click the ETERNUS DX S3 series link under [Name].

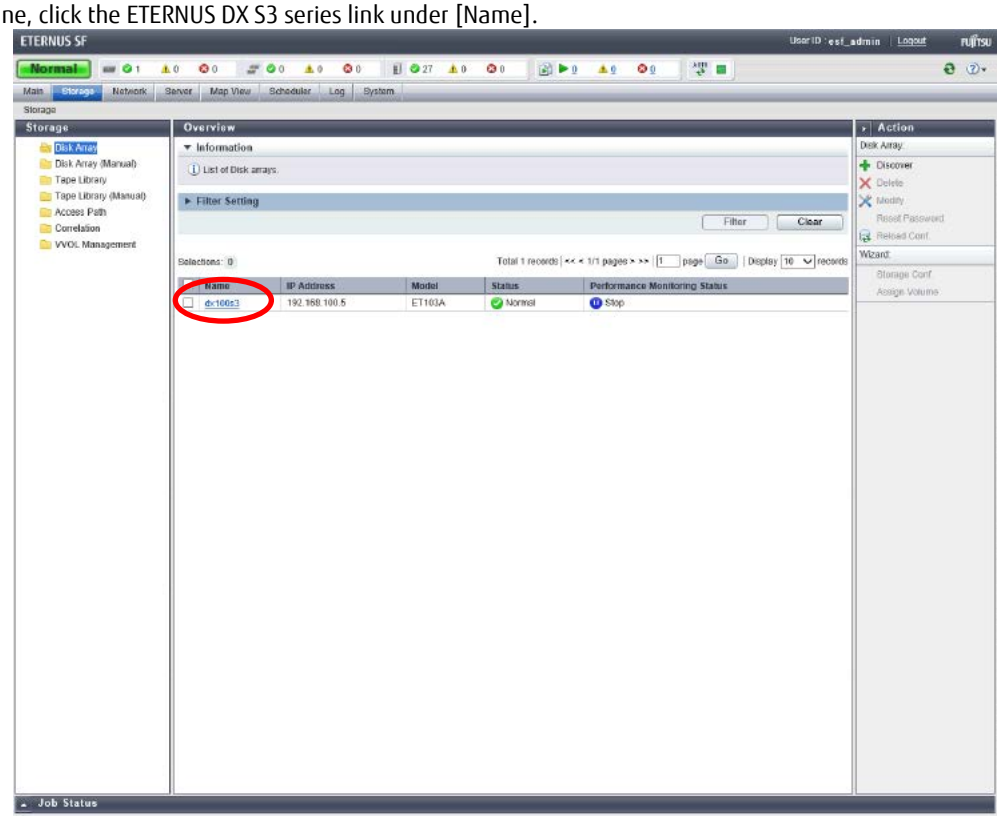

Figure-19 Storage

6. On the Category pane, click [System].

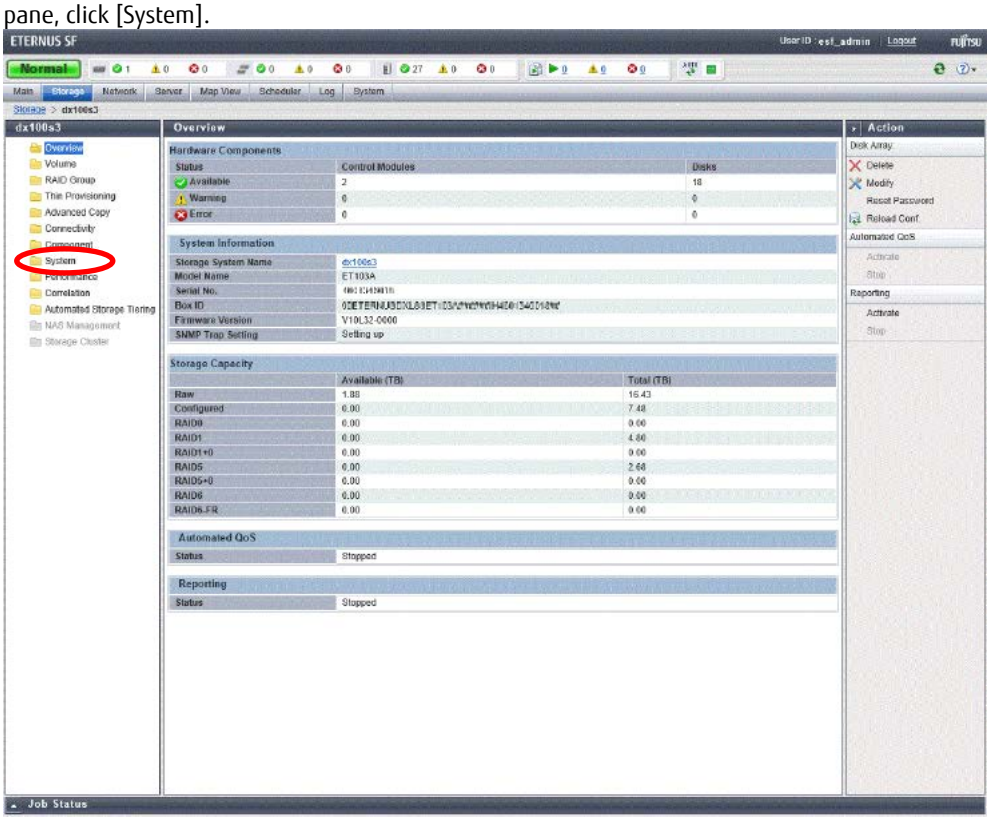

Figure-20 dx100s3

7. Click [License Management] on the Category pane. A list of licenses that can be registered is displayed on the Main pane.
Select the checkboxes for the licenses that are to be registered.
On the Action pane, click [Register] under [License].

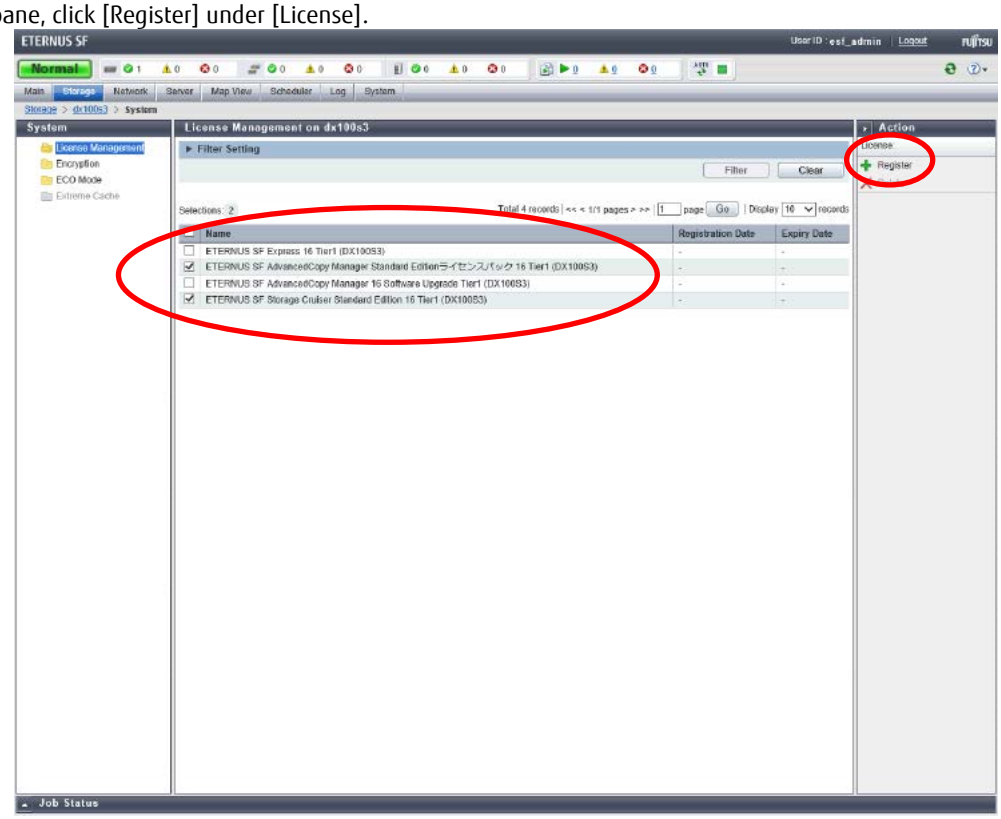

Figure-21 System

The information input screen is displayed.
Enter the license keys, and then click [Register] on the lower right corner of the screen.

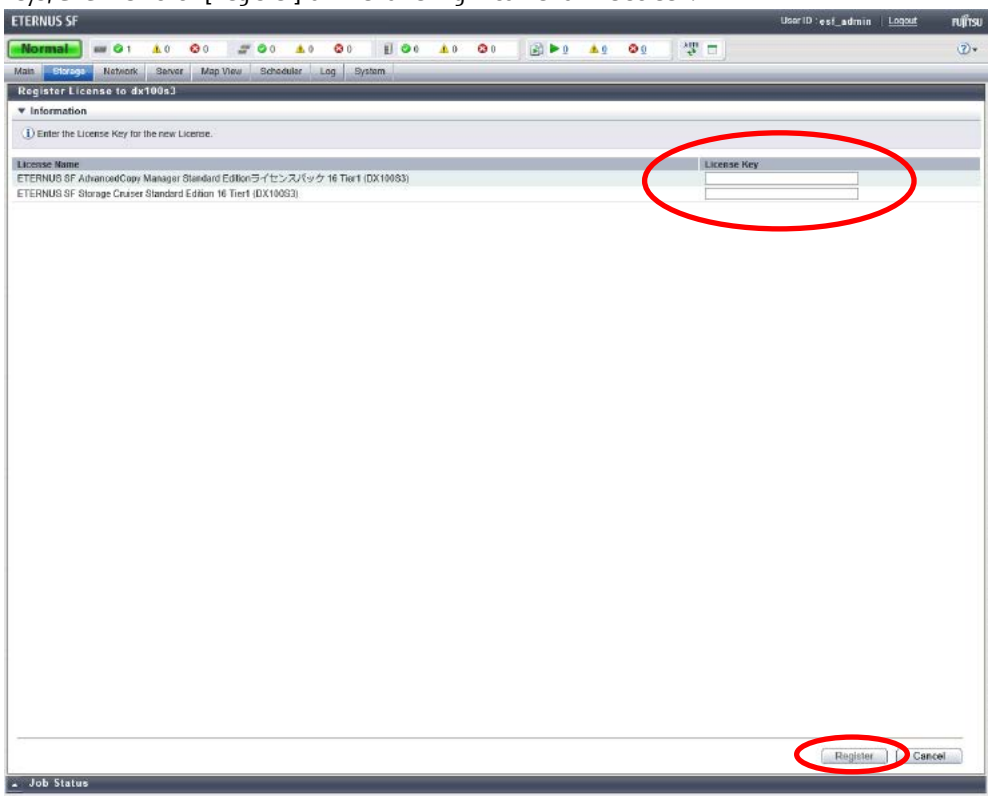

Figure-22 Register License

8. Register the VMware ESXi host.
   Click the [Server] tab on the global navigation tab. On the Action pane, click [Register] to display the information input screen.
   Register the ESXi host using values that were specified in "2.2.2.3.1 Configuring the ESXi Hosts and Installing vCenter Server".

9. Select [Yes] for [VMware ESX].
   A user ID and password can be entered in the VMware Options field.
   Enter the necessary information and click the [Next] button.

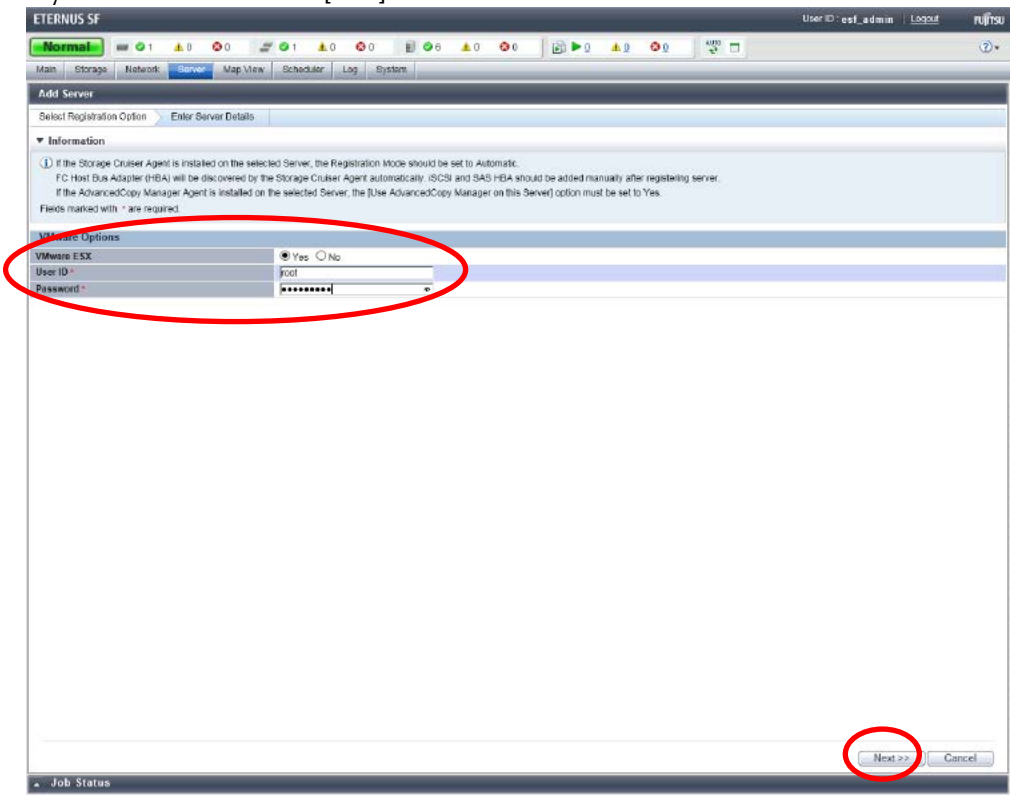

Figure-23 Input of information on VMware ESXi host server

10. Enter an IP address and click the [Register] button.

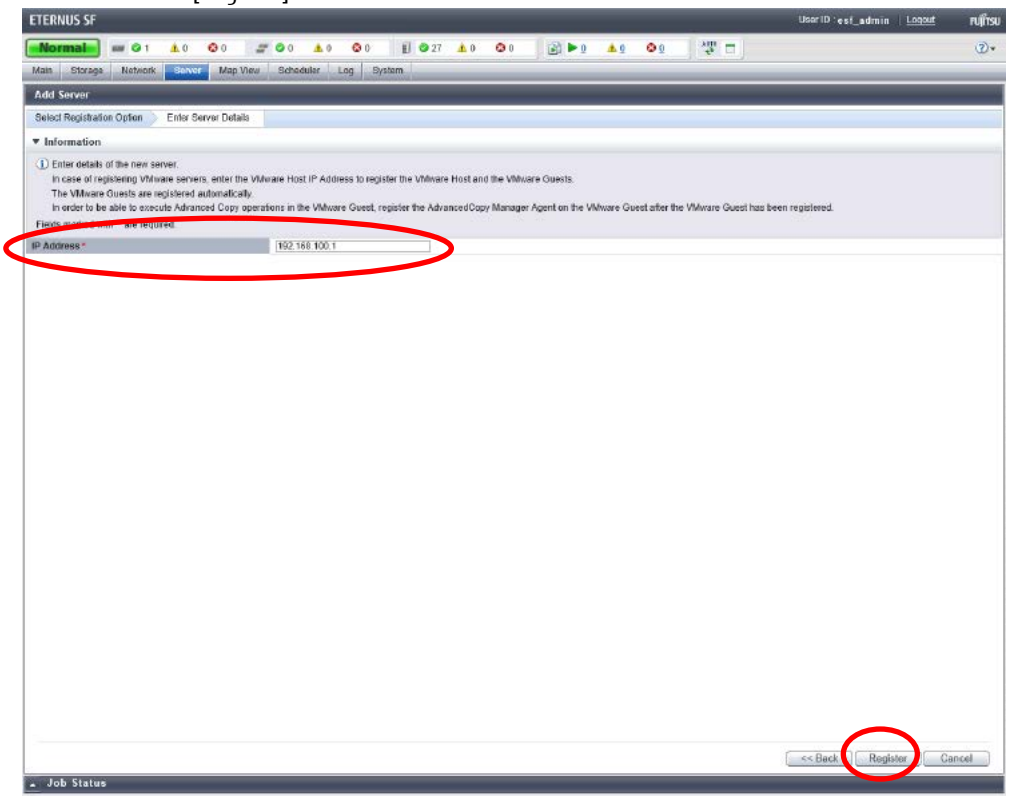

Figure-24 Registration of VMware ESXi host server

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next step.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".
Wait for the registration process to finish before operating the server.

Repeat Steps 8 through 10 for every VMware ESXi host server.

11. Register vCenter Server.
    Click the [Storage] tab on the global navigation tab, and then the link of the target ETERNUS DX S3 series under [Name].

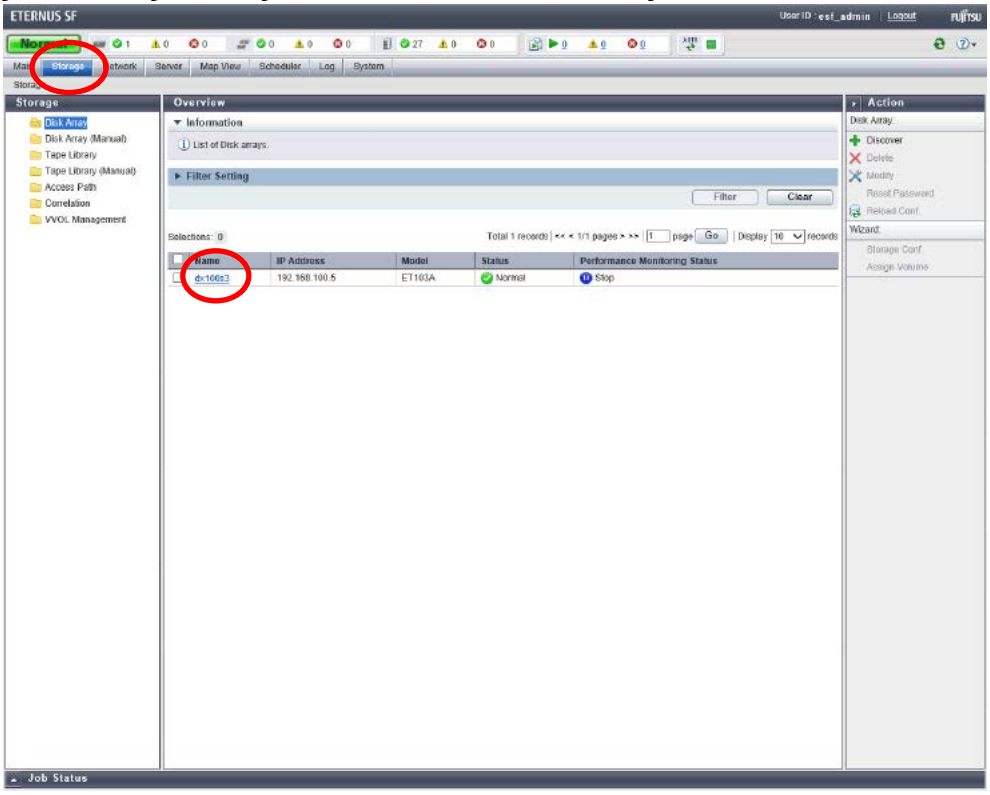

Figure-25 vCenter Server registration

12. On the Category pane, click [Correlation].

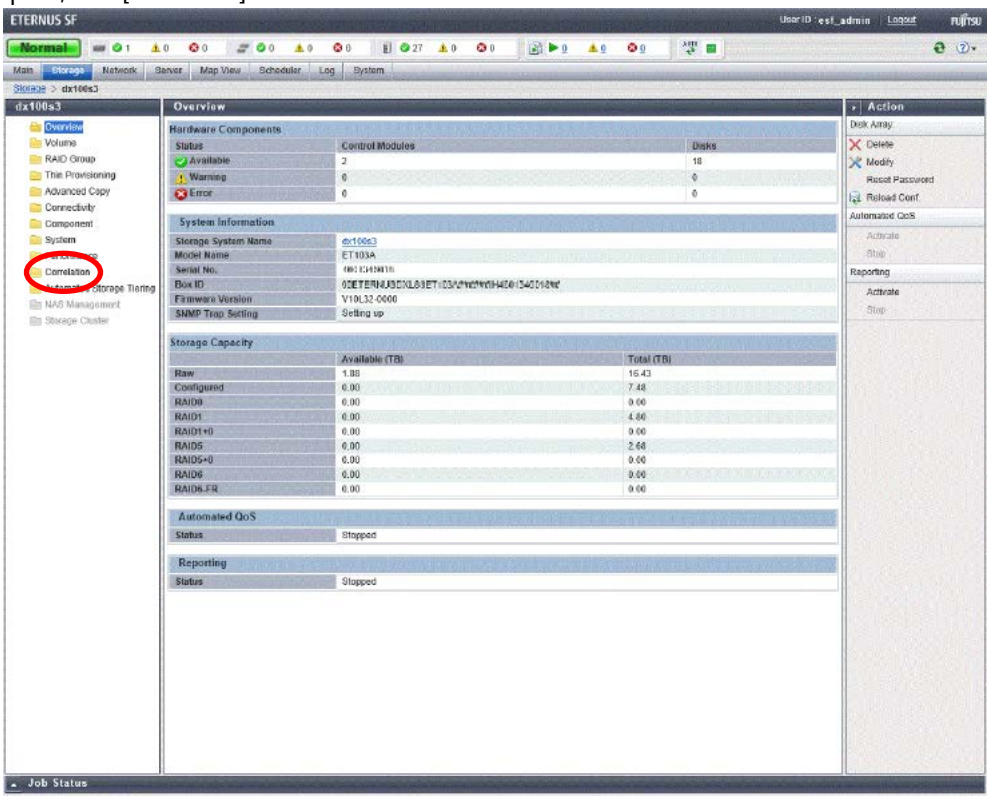

Figure-26 Correlation

13. On the Category pane, click [End to End View (VMware)].

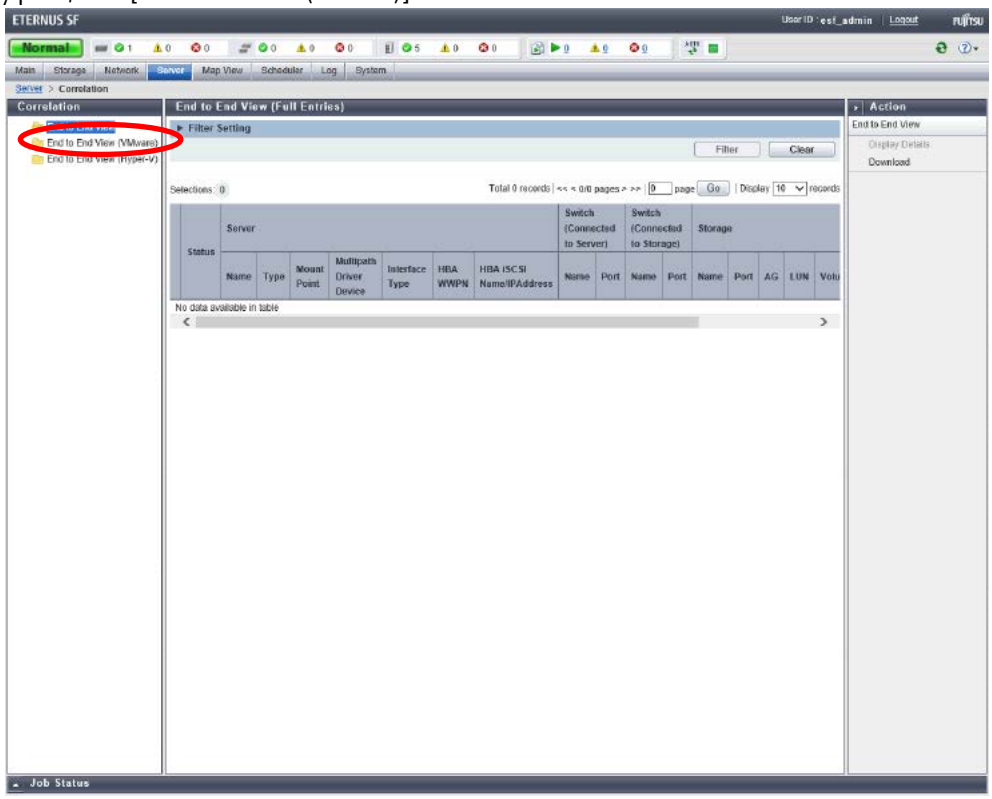

Figure-27 End to End View

14. On the Action pane, click [Register/Reload] under [VMware vCenter Sever].

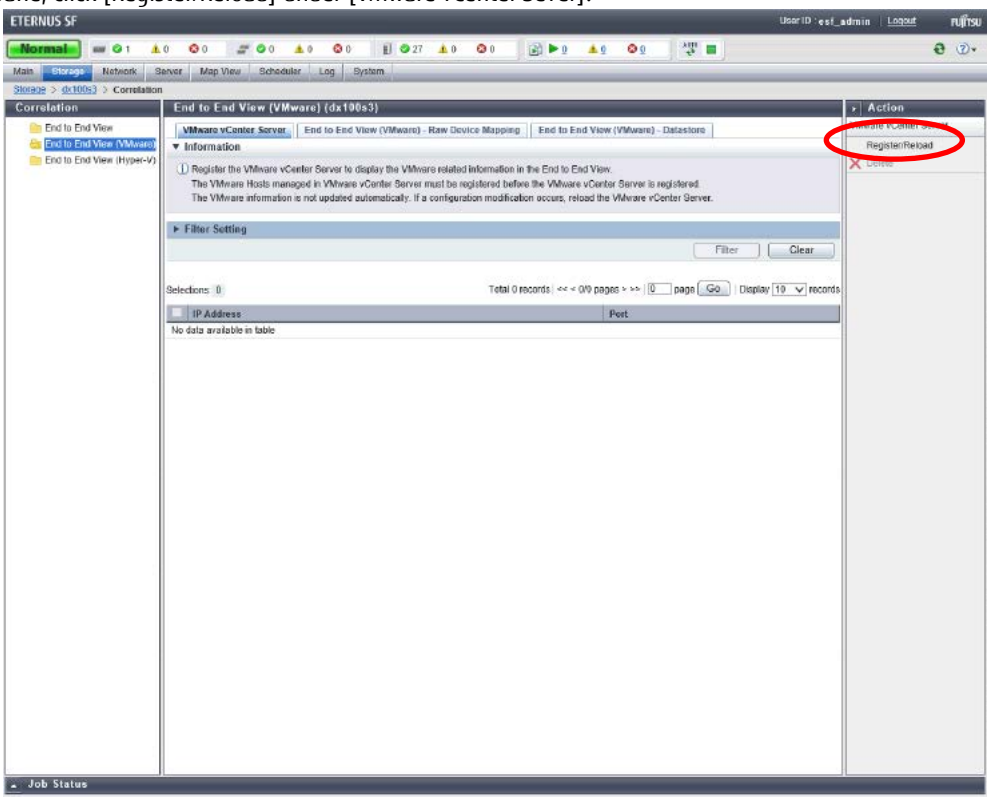

Figure-28 End to End View (VMware)

15. Enter an IP address, user name, and password, and then click the [Confirm] button on the lower right corner of the screen.

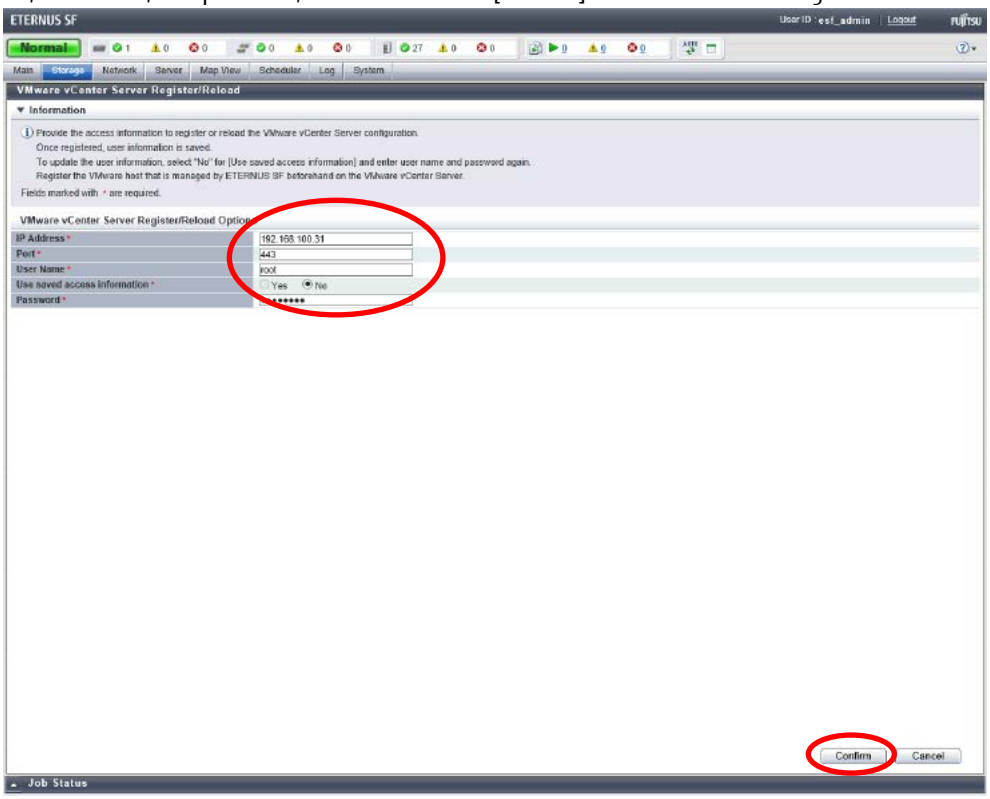

Figure-29 Register/Reload option for the VMware vCenter server

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next procedure.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

2.2.2.4.4 Checking the Devices Registered in ETERNUS SF Manager

Check that all the devices are registered.

Network switches including the ones for iSCSI connections do not need to be registered in the storage system.

Devices to check	Confirmation screen	Devices to check	Check ☑
ETERNUS DX100 S3	Click the [Storage] tab on the global navigation tab. Check that the registered ETERNUS DX S3 series is displayed on the Main pane.	dx100s3	□
ESXi host	Click the [Server] tab on the global navigation tab. Check that the registered ESXi hosts are displayed on the Main pane.	vvolesxi01	□
		vvolesxi02	□
		vvolesxi03	□
vCenter Serer	Check that the registered vCenter Server is displayed on the Main pane in the [End to End View (VMware)] screen.	vCenter	□

Table-13 Checking the devices registered in ETERNUS SF Manager

After checking that the devices are registered, proceed to the next procedure.

2.2.2.4.5 Refreshing the ETERNUS SF Manager Config File

Enable the synchronization between ETERNUS VASA Provider and the device event information.

1. Log in to ETERNUS SF Manager of the operation management server.

2. Click the [System] tab on the global navigation tab.
   On the Category pane, click [System Settings].

3. On the Action pane, click [Refresh Config File].

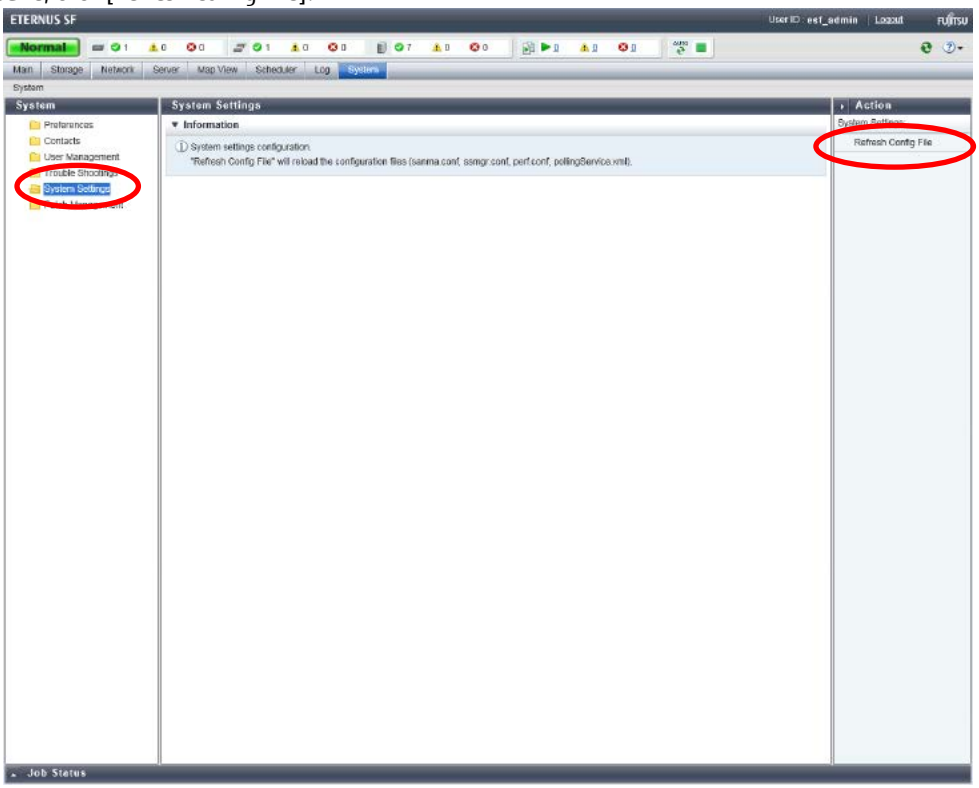

Figure-30 Refreshing the config file (system)

4. Check the [Information] screen and click the [Refresh] button.

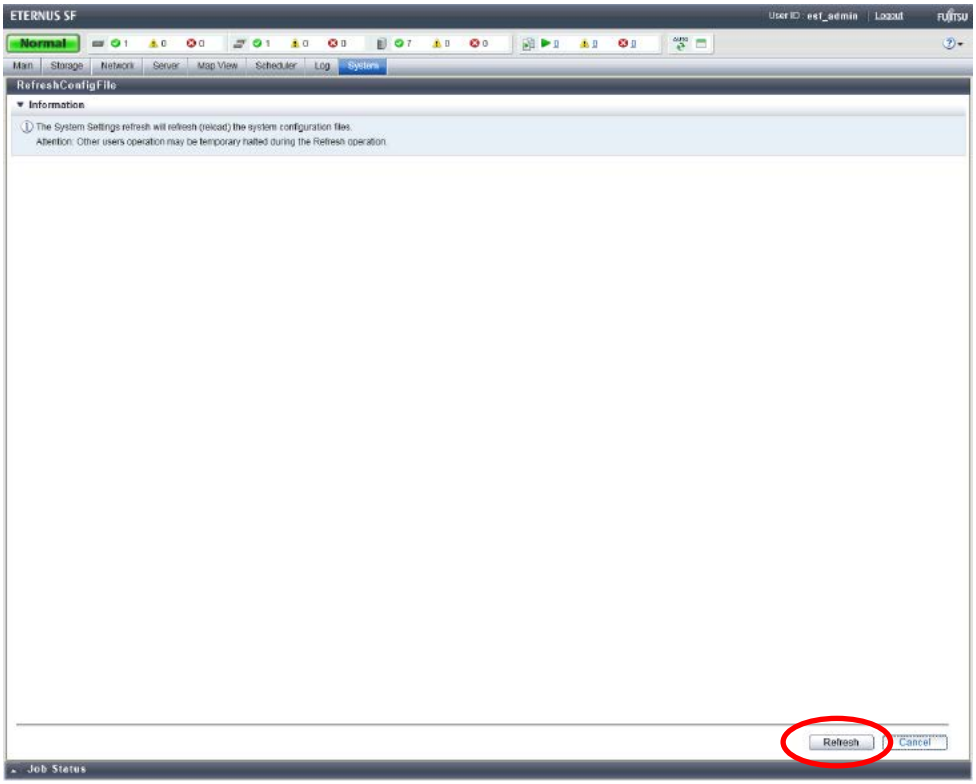

Figure-31 Refreshing the config file

5. Confirm that the "Refresh Config File successful" message is displayed and click the [OK] button.

2.2.2.4.6 Registering ETERNUS VASA Provider in vCenter Server

1. Register ETERNUS VASA Provider in vCenter Server.
   Log in to vCenter Server from vSphere Web Client.

2. Click [vCenter Inventory Lists] in the [Home] screen.

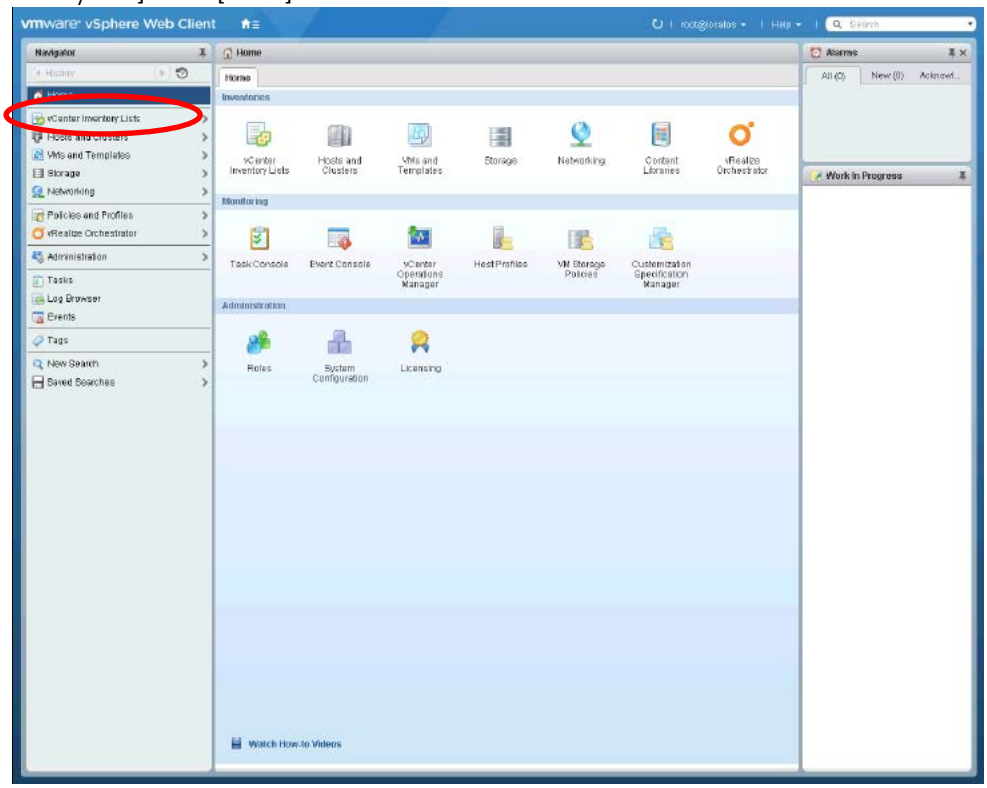

Figure-32 vSphere Web Client home

3. Click the [Manage] tab.

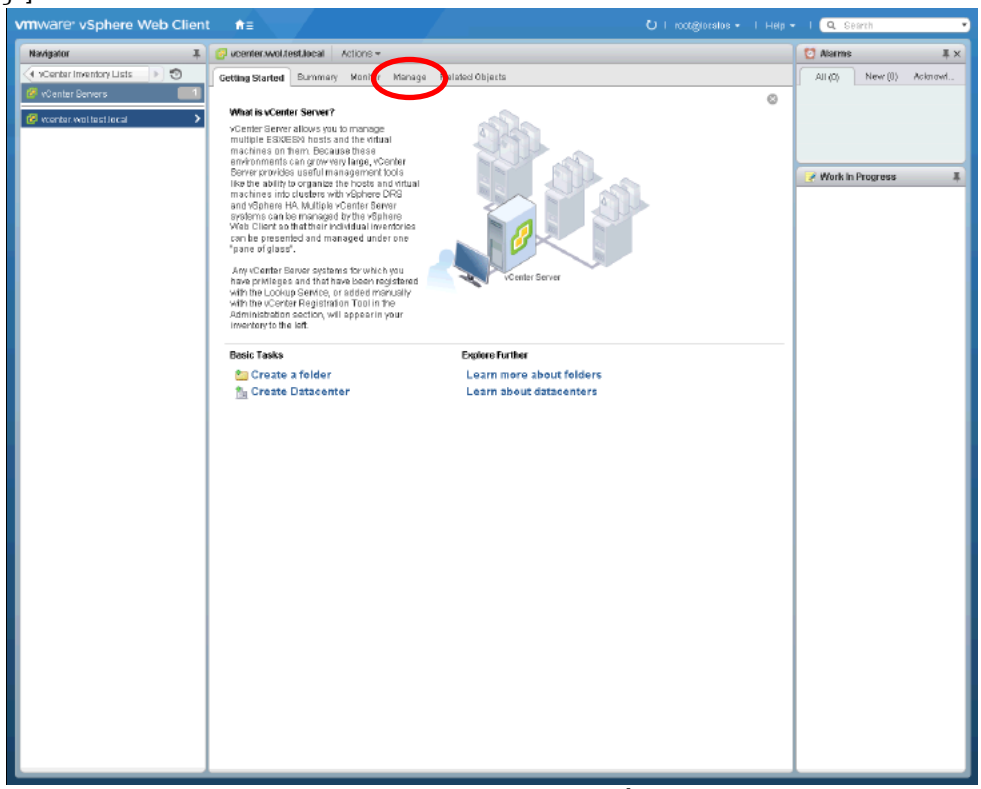

Figure-33 vCenter inventory list

4. Click [Storage Providers].

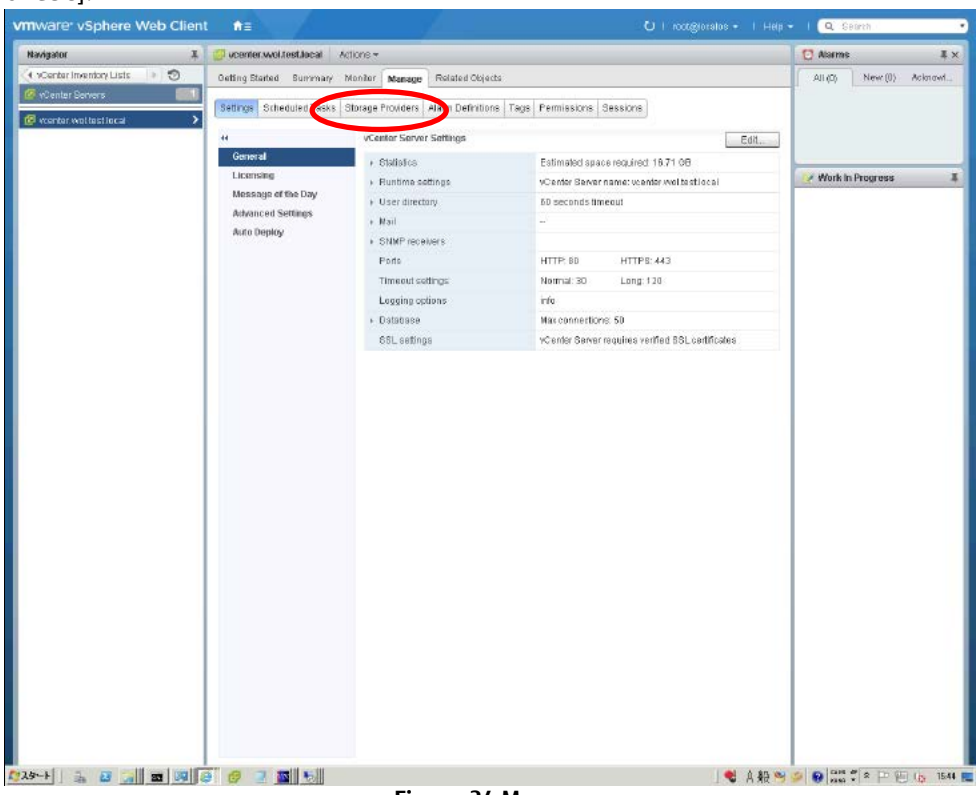

Figure-34 Manage

5. Click the [+] (register) button.

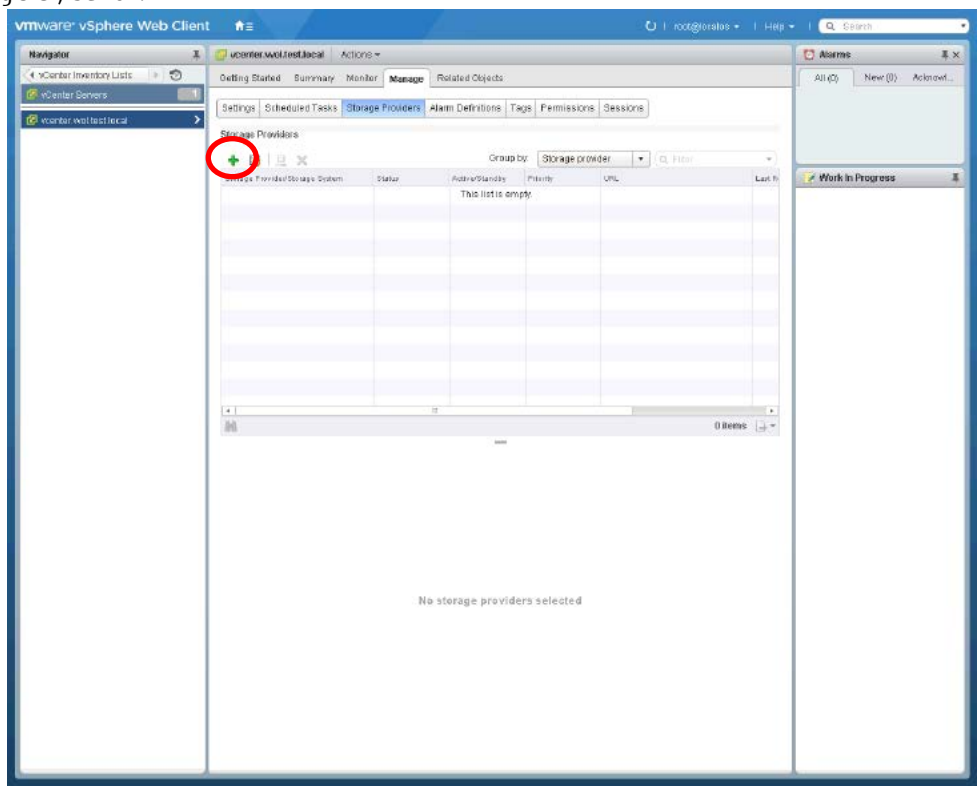

Figure-35 Registering storage providers

6. Enter the items shown in the following table and click the [OK] button.

Figure-36 New Storage Provider

Item	Information
Name	Arbitrary
URL	https://"FQDN that was registered when installing ETERNUS VASA Provider":31443/vasa/version.xml
User name	The use name that was registered when installing ETERNUS VASA Provider
Password	The password that was registered when installing ETERNUS VASA Provider

Table-14 Settings for a new storage provider

Checklist

Confirm the following item before proceeding to the next procedure.

- The ETERNUS VASA Provider that was registered is displayed in the [Storage Providers] screen.

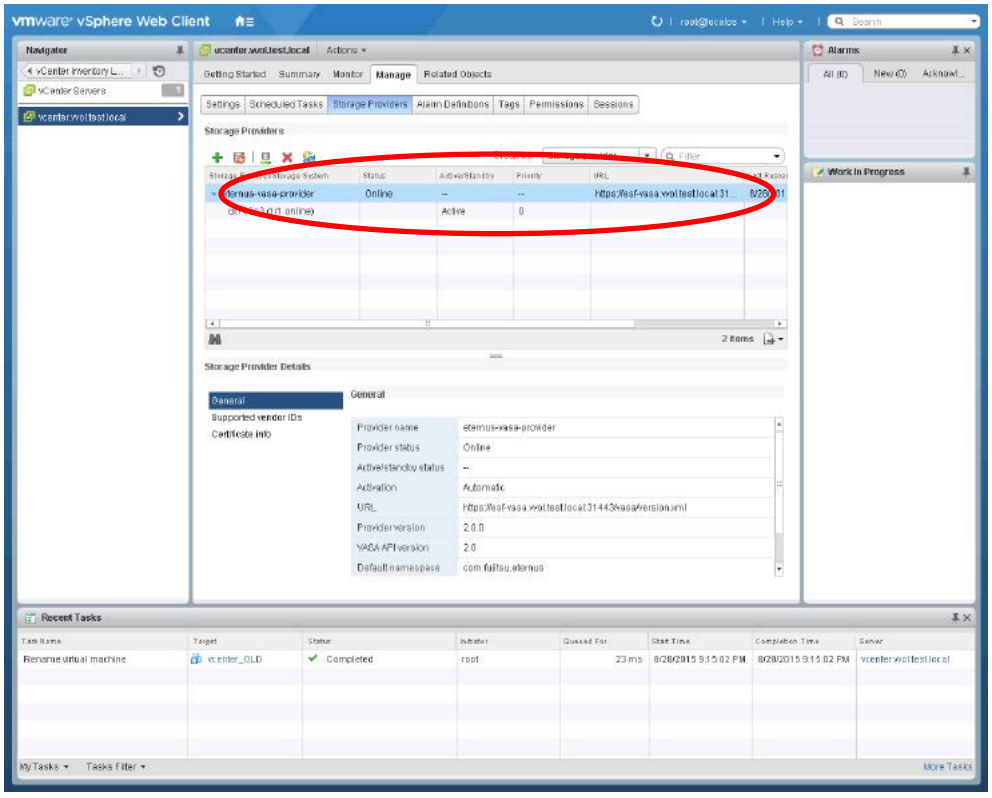

Figure-37 Checking the registered storage provider

2.2.2.4.7 Setting the Copy Control Type of ETERNUS SF Manager Advanced Copy

Configure the settings that are required to use ETERNUS SF AdvancedCopy Manager.

1. Set the copy control type of the Advanced Copy functions that is required to back up virtual machines.
   Click [Storage] on the global navigation tab of ETERNUS SF Web Console.

2. On the Main pane, click the ETERNUS DX S3 series link under [Name].

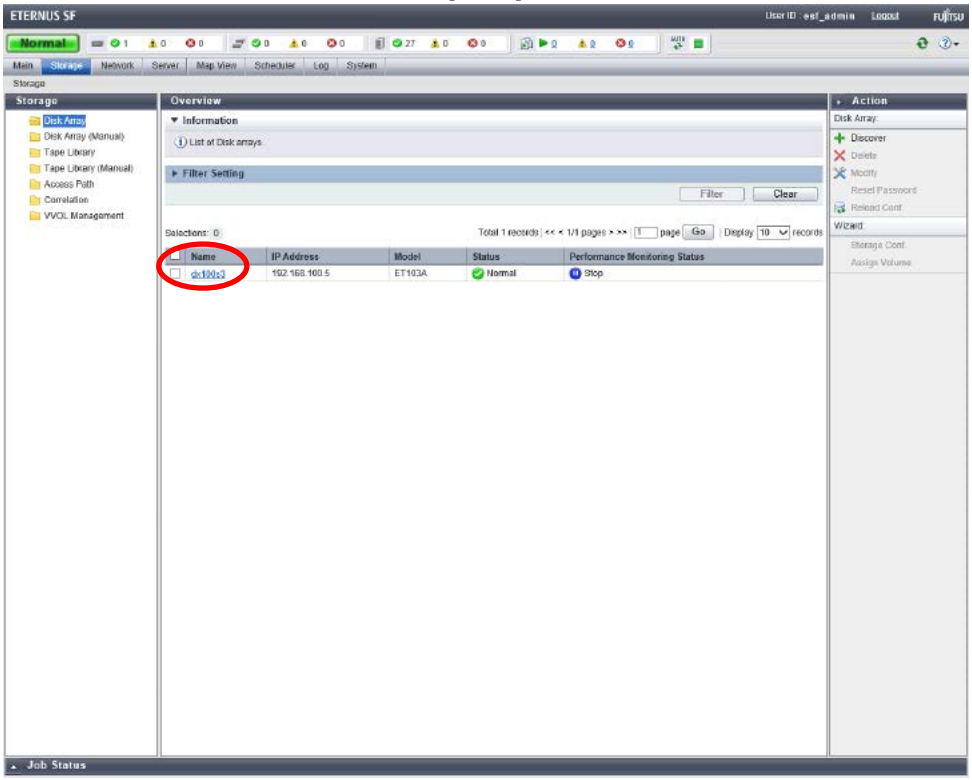

Figure-38 Storage

3. On the Category pane, click [Advanced Copy].

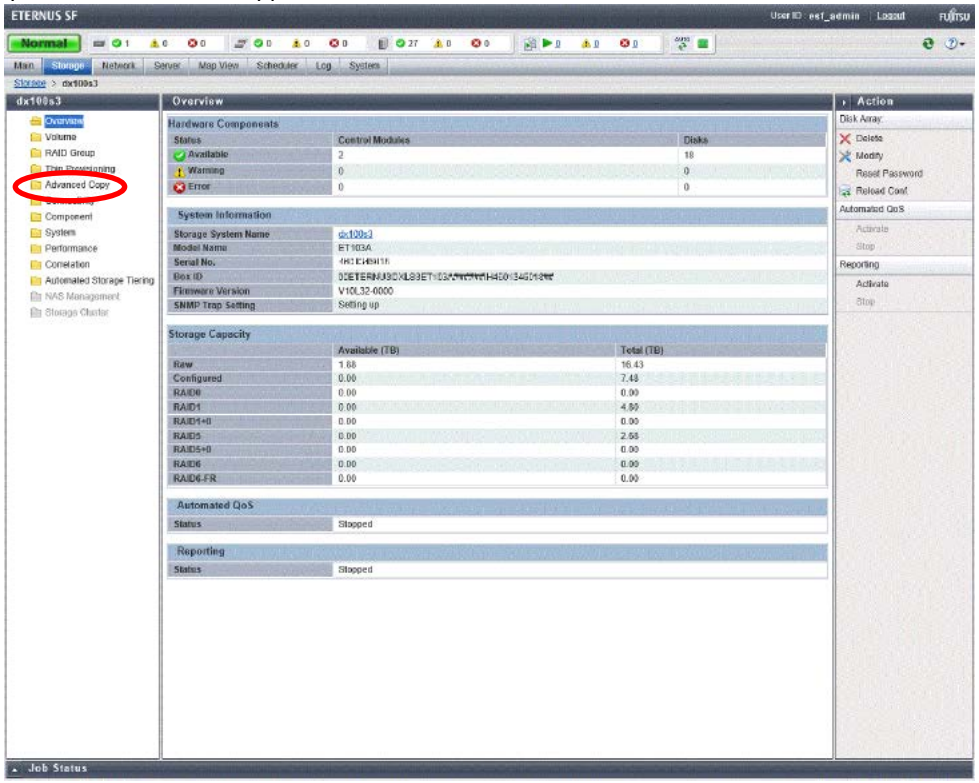

Figure-39 Advanced Copy (storage)

4. On the Category pane, click [Configuration].

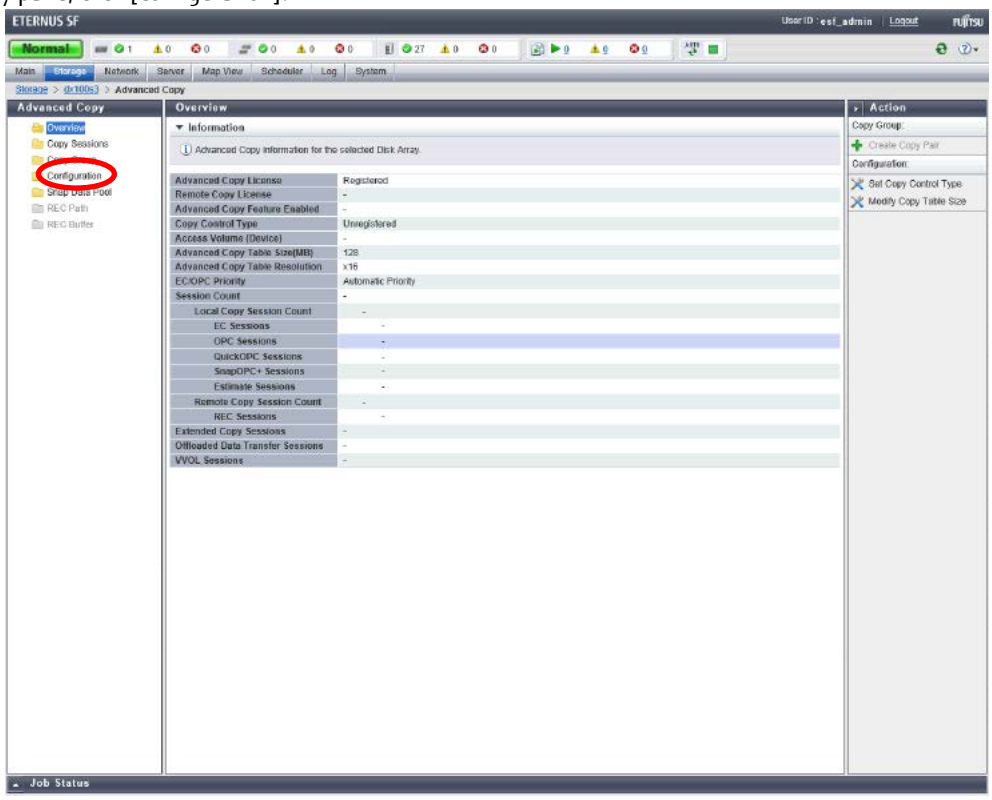

Figure-40 Advanced Copy (Advanced Copy)

5. On the Action pane, click [Set] under [Copy Control Type].

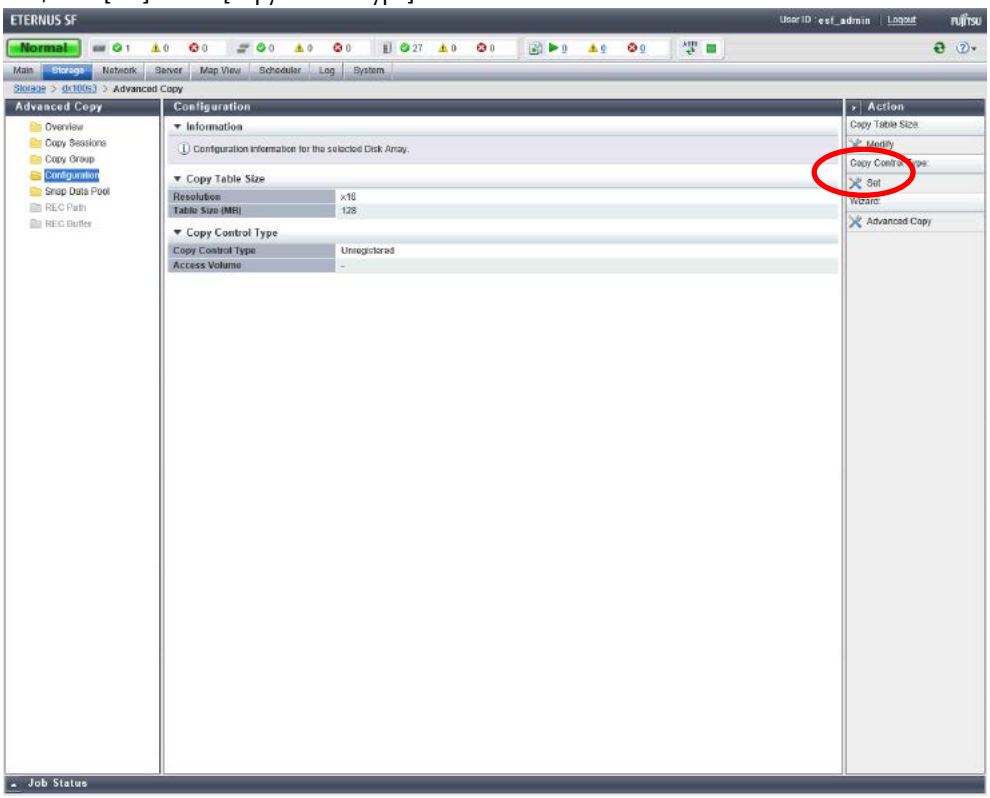

Figure-41 Advanced Copy (set)

6. Select [Access through network] and click the [Set] button on the lower right corner of the screen.

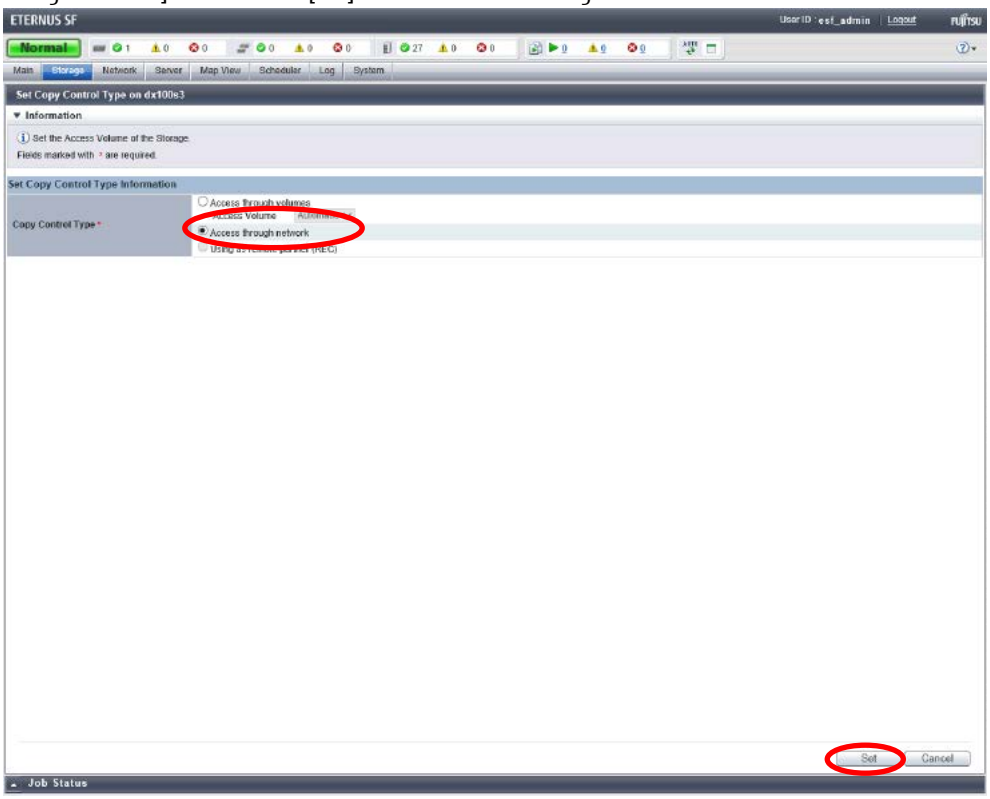

Figure-42 Setting the copy control type

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next procedure.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

Checklist

Confirm the following item before proceeding to the next procedure.

- On the Main pane in the [Advanced Copy] screen, [Access through Network] is displayed for [Copy Control Type].

2.2.2.5 Creating a VMFS Datastore for the Management Server and Configuring vSphere HA

Create a VMFS datastore where the management servers are assigned and configure vSphere HA.
Because the following procedure describes general operations for standard volumes, only a brief explanation is provided here.

2.2.2.5.1 Creating a VMFS Datastore for the Management Server

Create a standard volume for the VMFS where the management servers are assigned.
Create a RAID group in the ETERNUS DX100 S3 using ETERNUS SF Manager and create a standard volume in the RAID group.
Refer to "Create Volume" in "ETERNUS SF Web Console Guide" for the procedure to create volumes.

- Log in to ETERNUS SF Manager of the operation management server.
  Click the [Storage] tab. On the Main pane where [Storage] is displayed, click the registered "dx100s3" storage system.
  On the Category pane where [dx100s3] is displayed, click [RAID Group].
  On the Action pane where [RAID Group] is displayed, click [Create].
  In the [Create RAID Group] screen, create the following RAID group.

Name	RAID Type	Disk Type	Creation Mode	RAID Group Capacity	RAID group settings				
					Enclosure No.	Slot No.	Disk Type	Capacity	Speed (rpm)
rgp001	Mirroring (RAID1)	Online	Manual	819.5GB	-	0	SAS	900GB	10000
					-	1	SAS	900GB	10000

Table-15 RAID group for VMFS

- Click the [Storage] tab. On the Main pane where [Storage] is displayed, click the registered "dx100s3" storage system.
  On the Category pane where [dx100s3] is displayed, click [Volume].
  On the Action pane where [Volume] is displayed, click [Create].
  In the [Create Volume] screen, create the following volume.

Name	Capacity	Type	RAID Group Setting	
			RG Name	Number of Volumes
vol001	819.5GB	Standard	rgp001	1

Table-16 Volume for VMFS

- Set access paths for the ESXi host and the volume that was created using ETERNUS SF Manager.
  For details on the procedure, refer to "Assign ETERNUS Disk Storage System Volumes to Server" in "ETERNUS SF Web Console Guide".

- Perform settings for the iSCSI ports of the ETERNUS DX100 S3.
  Click the [Storage] tab. On the Main pane where [Storage] is displayed, click the registered "dx100s3" storage system.
  On the Category pane where [dx100s3] is displayed, click [Connectivity].
  On the Category pane where [Connectivity] is displayed, click [Port].
  On the Main pane where [Port] is displayed, click the number for ports for the iSCSI type.
  Select one iSCSI port on the Main pane where [iSCSI Port] is displayed and click [Modify iSCSI Port] on the Action pane.
  In the [Set Port Parameters] screen, set the following values.

Port (display only)			Port (settings)						
Port	Type	Mode	Host Affinity	iSCSI Name	IP Version	IP Address	Subnet Mask	Reset Scope	Release Reservation if Chip is Reset
CM#0 CA#0 Port#0	iSCSI	CA	Enable	Arbitrary* (Use alphanumeric characters, "." [period], ":" [colon], or "-" [hyhen] within 223 characters.)	IPv4	Arbitrary	Arbitrary	I_T_L	Disable
CM#1 CA#0 Port#0									

Table-17 iSCSI port settings for the ETERNUS DX100 S3

* For iSCSI ports that configure multiple paths, set a unique iSCSI name between each iSCSI port.
If a duplicate iSCSI name is set, the multipath configuration may not be connected.

- Create an affinity group or a LUN group.
  Click the [Storage] tab. On the Main pane where [Storage] is displayed, click the registered "dx100s3" storage system.
  On the Category pane where [dx100s3] is displayed, click [Connectivity].
  On the Category pane where [Connectivity] is displayed, click [Affinity/LUN Group].
  In the [Affinity/LUN Group] screen, click [Create] under [Affinity/LUN Group] on the Action pane.
  In the [Create Affinity/LUN Group] screen, set the following values.

Name	Number of LUNs (display only)	Assigned Volumes				
		LUN No.	Volume No.	Name	Type	Capacity
kanri01	1	0	0	vol001	Standard	819.50 GB

Table-18 Creating a LUN group of the volume for VMFS

- Add the iSCSI interface as an HBA.
  Click the [Server] tab. On the Main pane where [Server] is displayed, click the [vvolesxi01] ESXi host that was registered.
  On the Action pane where [vvolesxi01] is displayed, click [Add] under [HBA].
  In the screen where [Set HBA Information] is displayed, set the following values manually and click [Add]. Repeat this step for all the HBAs that are to be added.

Interface Type	Manual Input	
	iSCSI Name	IP Address
iSCSI	Arbitrary	Arbitrary

Table-19 HBA settings

Select the checkbox for the HBA that is to be added in [HBA Information] and click [Next].
In the screen where [Confirm] is displayed, check the settings and click [Add].

Perform the same procedure for vvolesxi02 and vvolesxi03.

- Set the access path.
  Click the [Server] tab. On the Category pane where [Server] is displayed, click [Access Path].
  On the Action pane, click [Add (ETERNUS)] under [Access Path].
  In the [Create Access Path] screen, set the following values.

Select Server	Select HBA				Select Storage	Select Host Response and Port		Select Affinity Group	Affinity Group Details
Name	Logical No.	Interface Type	iSCSI Name	IP Address	Name	Host Response	Port	Name	Name
vvolesxi01	vmhba1	iSCSI	(Check that the displayed value matches the actual connection.)	(Check that the displayed value matches the actual connection.)	Dx100s3	default	CM#0 CA#0 Port#0	kanri01	VVOL001
	vmhba2						CM#1 CA#0 Port#0		
vvolesxi02	vmhba1						CM#0 CA#0 Port#0		
	vmhba2						CM#1 CA#0 Port#0		
vvolesxi03	vmhba1						CM#0 CA#0 Port#0		
	vmhba2						CM#1 CA#0 Port#0		

Table-20 List of access path values for VMFS

- Check the LUNs.
  This section provides the procedure to check whether the LUNs are recognized using vSphere Web Client.
  Log in to VMware ESX from vSphere Web Client and check the device.

  1. Log in to vSphere Web Client.
     Click [Hosts and Clusters] in the [Home] screen and select the target host on the left pane.

  2. Select the [Manage] tab -[Storage] - [Storage Adapters].

  3. Click the rescan button.
     When the rescan button is clicked, the LUNs are once again recognized to the ETERNUS DX from VMware ESX.

  4. Select the iSCSI Software Adapter (example: vmhba34) in the [Storage Adapters] frame.
     The recognized device is displayed under the [Devices] tab in the [Adapter Details] frame.

  5. Check [Path selection policy] for all the LUNs in the ETERNUS DX.
     When VMware ESX recognizes the LUNs, the operation path for each LUN is automatically set.

     The default setting is [Most Recently Used (VMware)]. However, changing [Path selection policy] for all the LUNs to [Round Robin (VMware)] is recommended.

  6. In multipath configurations, check that all the LUNs in the ETERNUS DX are configured to use multiple paths.
     When the LUNs are configured to use multiple paths, multiple runtime names and targets are displayed for [Paths].

- Set the CHAP authentication.
  Log in to VMware ESX from vSphere Web Client, check the device, and then enable CHAP authentication.
  The procedure is provided below.

  1. Log in to vSphere Web Client.
     Click [Hosts and Clusters] in the [Home] screen and select the target host on the left pane.

  2. Select the [Manage] tab - [Storage] - [Storage Adapters].

  3. Select the target iSCSI Software Adapter.

  4. Click [Edit] in [Authentication] at the bottom under the [Properties] tab in the [Adapter Details] frame.

5. Set the CHAP authentication. In this document, bidirectional CHAP is used.
   Select [Use bidirectional CHAP] for [Authentication Method], and set [Name] and [Secret] for [Outgoing CHAP Credentials] and [Incoming CHAP Credentials].

2.2.2.5.2 Configuring vSphere HA

In the vCenter server, configure a single vSphere HA in all the ESXi hosts.
For details on the procedure, refer to the VMware vSphere manuals.

- In vCenter Server, mount the created standard volume on the ESXi hosts as a VMFS datastore.
- Check that the datastore can be referred to from all the ESXi servers.
- In vCenter Server, configure all the ESXi hosts and the vSphere HA.

2.2.2.5.3 Checking the VMFS Datastore after a vSphere HA Configuration

After a vSphere HA configuration, check that the VMFS datastore that was created in the ETERNUS DX100 S3 can be used by all the ESXi hosts.

1. Confirm that all the ESXi hosts are synchronized with the NTP server clock by checking the following items;
   - The NTP client of the ESXi host is started.
   - The NTP client is set to synchronize with the host.
   - The other NTP clients are set to start.

2. Check if VMware Tools is installed in the vCenter server and the operation management server that consist of virtual machines.

3. Check if the vCenter server and the operation management server that consist of virtual machines are synchronous with the NTP server's or the ESXi host's clock.

4. Create virtual machines for tests that use the VMFS datastore for the operation management server.
   Check that the created virtual machines can be moved to all the ESXi hosts (vvolesxi01 to vvolesxi03).
   After checking, delete the virtual machines that were created for the test.

In addition, perform a separate check of the vSphere HA configuration.

2.2.2.5.4 Moving the Datastore for the vCenter Sever and the Operation Management Server

Move the virtual machines for the vCenter server and the operation management server that were created on the local disks of the ESXi host to the VMFS datastore that was created on the ETERNUS DX100 S3.
Assigning the virtual machines to the VMFS datastore that was created in the ETERNUS DX100 S3 provides redundancy with vSphere HA.

Checklist

Confirm the following items before proceeding to the next procedure.

- The operation management server and the vCenter sever are running on the VMFS datastore that was created in the ETERNUS DX100 S3's volume.
- vCenter Server and ETERNUS SF Manager are running normally.

2.2.3 VVOL Environment Configuration Procedure

2.2.3.1 ETERNUS SF Manager Operations

2.2.3.1.1 Setting VVOL Access Paths

1. From ETERNUS SF Web Console, click [Storage] on the global navigation tab.

2. On the Category pane, click [VVOL Management].

3. On the Category pane, click [VVOL Access Path].
   On the Action pane, click [Set] under [VVOL Access Path].

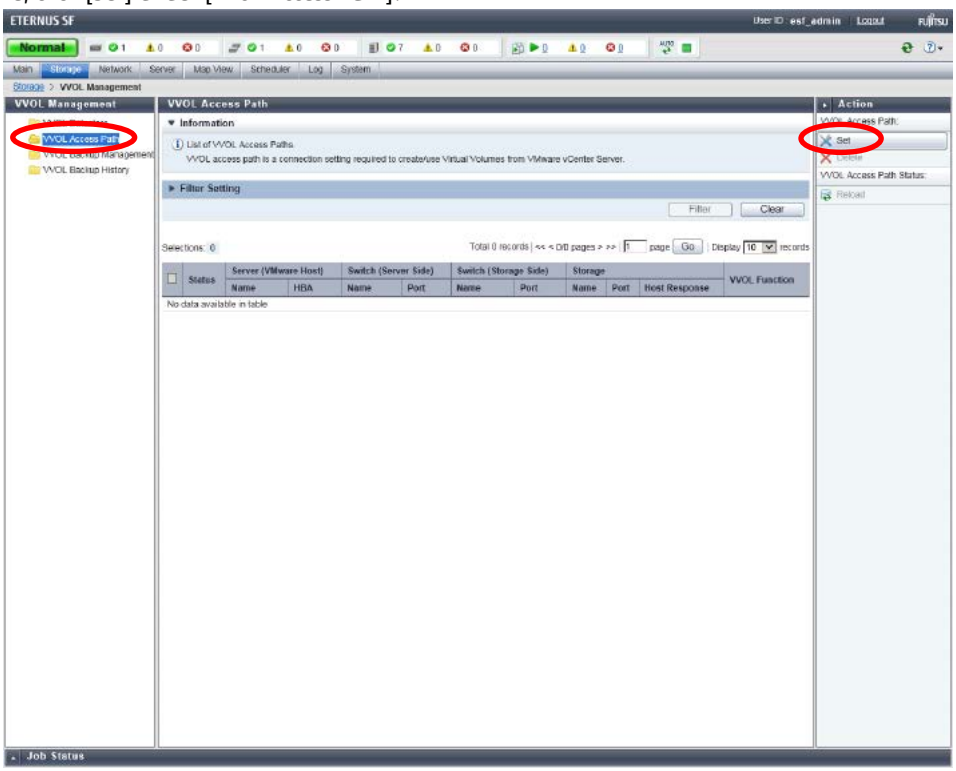

Figure-43 VVOL Access Path

4. The Welcome screen of [VVOL Access Path Setting] is displayed.
   Click the [Next] button.

5. On the [Select Disk Array and Server] screen, select the ETERNUS DX S3 series and the server for setting the VVOL access path, and then click the [Next] button.

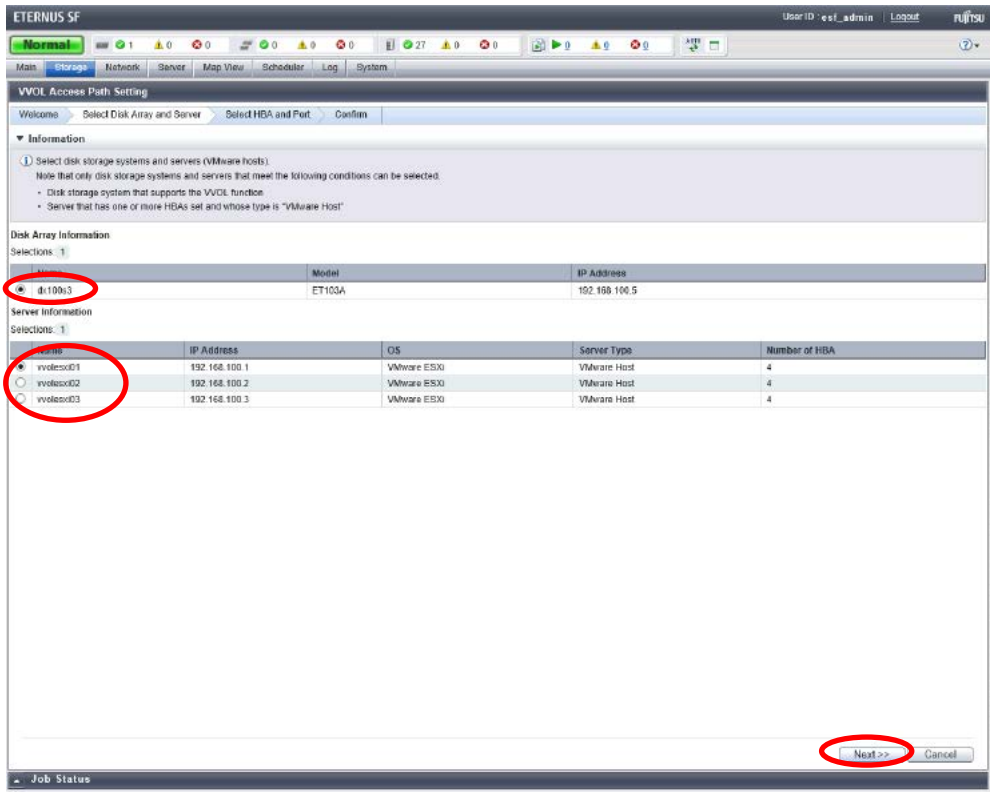

Figure-44 Select Disk Array and Server

Points

Check that the storage system and the ESXi hosts that were registered with "2.2.2.4.3 Setting Up ETERNUS SF Manager" are displayed.

Display area	Displayed device	Check ☑
Disk Array Information	Dx100s3	□
Server Information	vvolesxi01	□
	vvolesxi02	□
	vvolesxi03	□

Table-21 Checklist for the storage system and servers

6. In the [Select HBA and Port] screen, perform the following settings.
   - For [Zoning Setting], select [No].
   - Select the [Set Access Path] checkbox of the HBA where the setting is performed.
   - For the other settings, enter the items shown in the following table.

   After setting all the paths that are displayed on the screen, click the [Next] button.

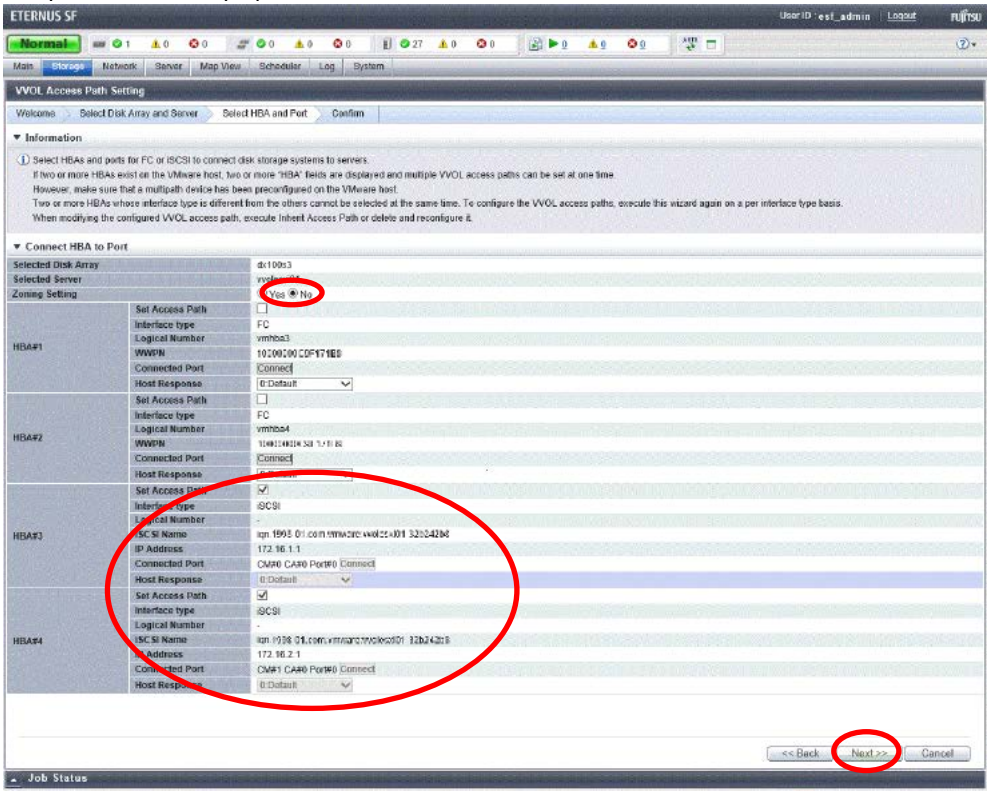

Figure-45 Select HBA and Port

Host name	Item	Information	
vvolesxi01	HBA#1	Connected Port	CM#0 CA#0 Port#0
		Host Response	0:Default
	HBA#2	Connected Port	CM#1 CA#0 Port#0
		Host Response	0:Default
vvolesxi02	HBA#1	Connected Port	CM#0 CA#0 Port#0
		Host Response	0:Default
	HBA#2	Connected Port	CM#1 CA#0 Port#0
		Host Response	0:Default
vvolesxi03	HBA#1	Connected Port	CM#0 CA#0 Port#0
		Host Response	0:Default
	HBA#2	Connected Port	CM#1 CA#0 Port#0
		Host Response	0:Default

Table-22 List of VVOL access path settings

7. The information confirmation screen is displayed. Confirm the information, and then click the [Set] button on the lower right corner of the screen.

   Points
   Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next procedure.
   For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

Repeat Steps 3 to 7 to set all the VVOL access paths.

Checklist
Confirm the following item before proceeding to the next procedure.
- On the Main pane of the [VVOL Access Path] screen, the VVOL access paths for all the ESXi hosts are displayed.

2.2.3.1.2 Enabling Automated Storage Tiering

1. On the ETERNUS SF Web Console screen, click [Storage] in the global navigation tab.

2. On the Category pane, click [Automated Storage Tiering].

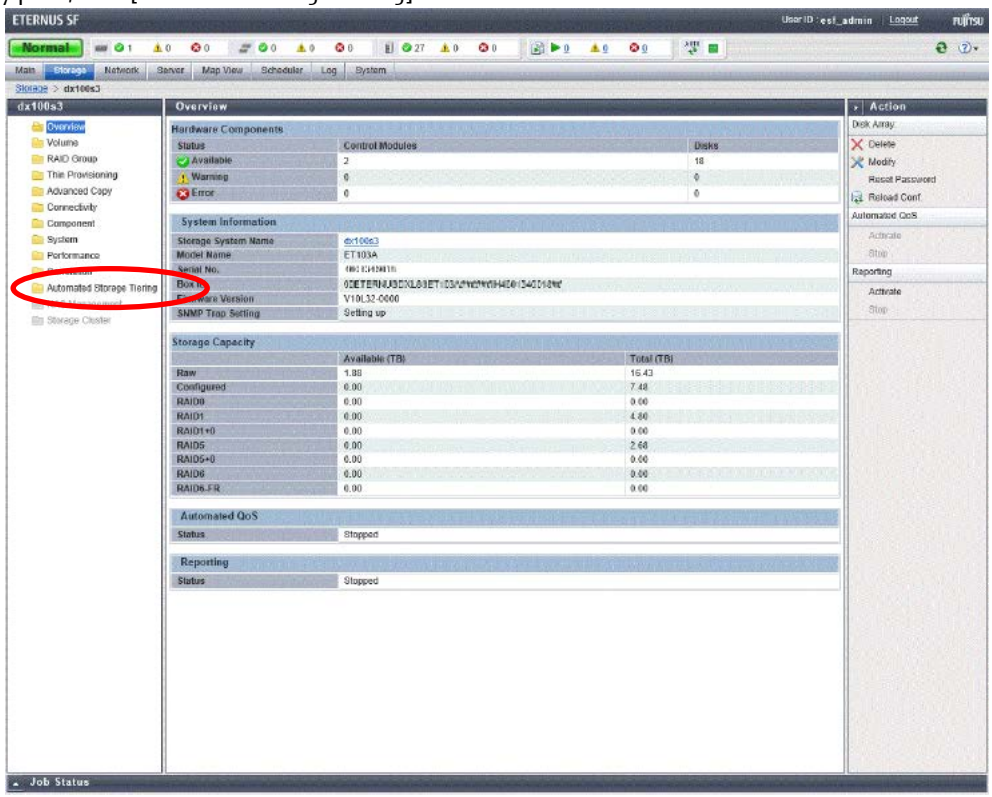

Figure-46 Automated Storage Tiering

3. On the Category pane, click [Setting].
   On the Action pane, click [On].

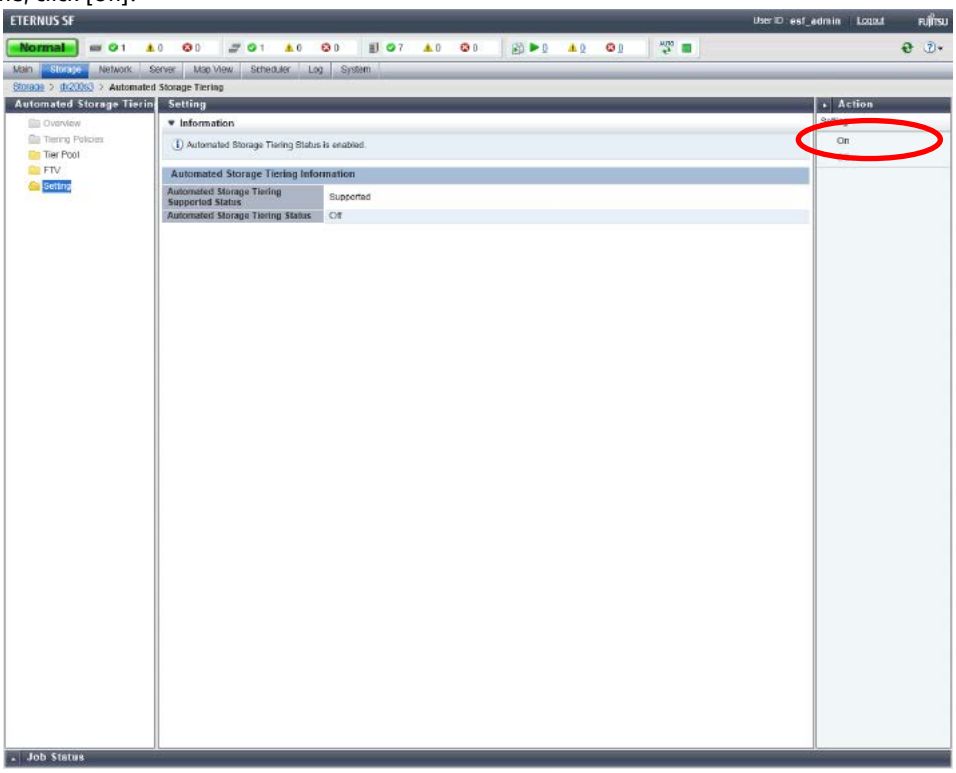

Figure-47 Enabling Automated Storage Tiering

2.2.3.1.3 Creating Tier Pools

1. Create a Tier pool (gold) for VVOL datastores.
   On the ETERNUS SF Web Console screen, click [Storage] in the global navigation tab.

2. On the Category pane, click [VVOL Management].
   On the Action pane, click [Create (One Layer)].

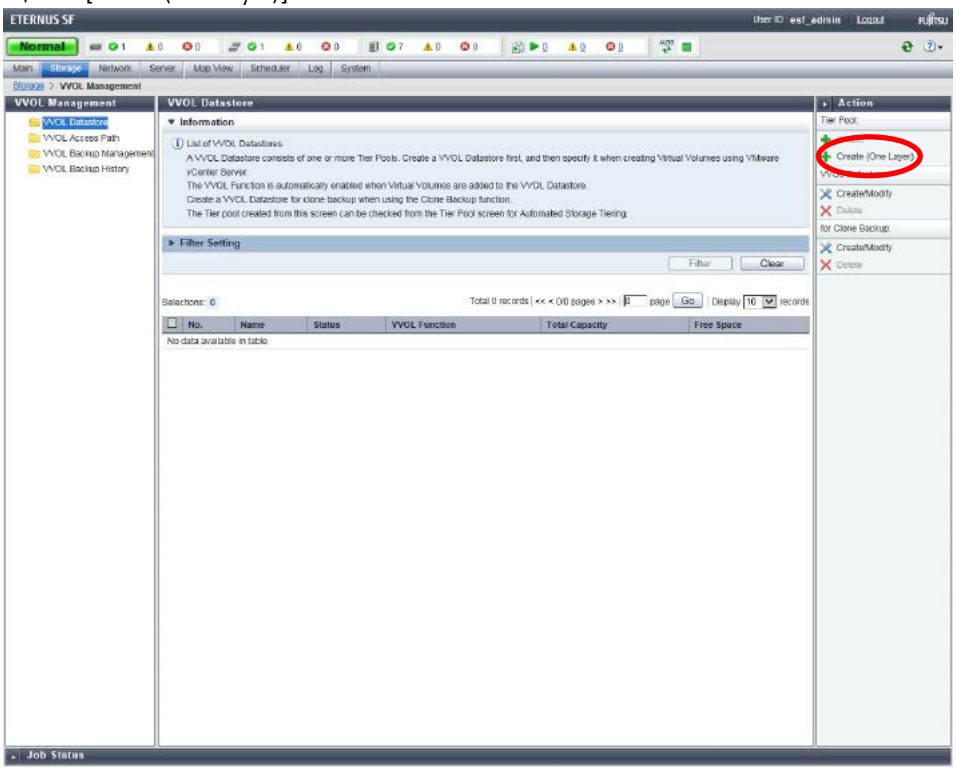

Figure-48 VVOL Management

3. The [Select Disk Array] screen is displayed. Select the ETERNUS DX S3 series for creating the Tier pool, and then click the [Next] button.

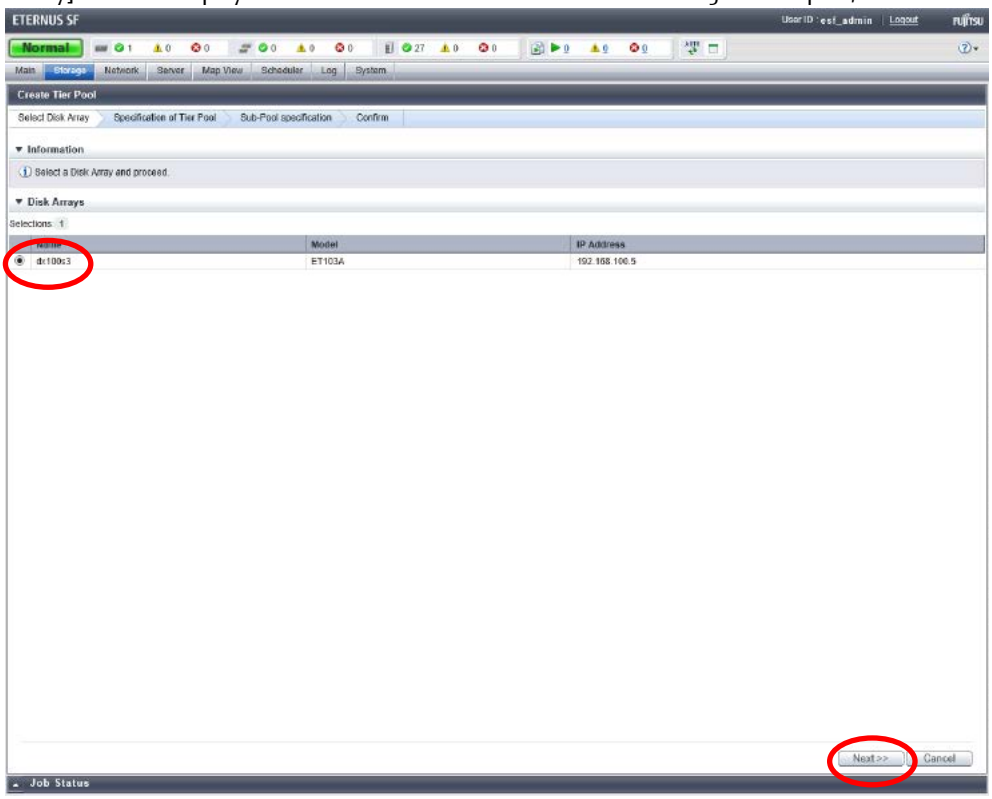

Figure-49 Select Disk Array

4. The information input screen is displayed.
   Enter the items shown in the following table, and then click [Next] on the lower right corner of the screen.

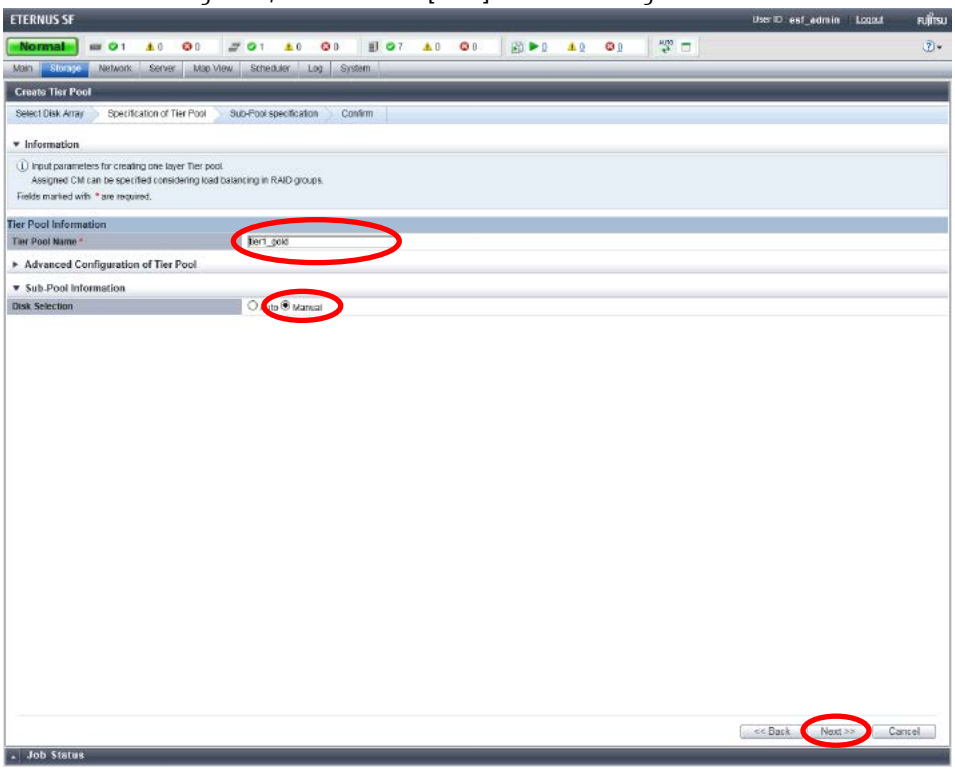

Figure-50 Specification of Tier Pool

Item	Description	Value in this document
Tier Pool Name	Specify a unique pool name in the ETERNUS SF system. Any alphanumeric character (from 1 to 16 characters), a hyphen (-), an underscore (_), and a pound symbol (#) can be specified. The characters are case insensitive.	tier1_gold
Disk Selection	Specify the method for the selection of disks that configure the sub-pool. The default setting is [Auto] (automatic selection). When [Auto] is selected, the minimum required capacity for the Low sub-pool, Middle sub-pool, and High sub-pool must be specified in the screen to configure each of these sub-pools. When [Manual] is selected, the disks for configuring the Low sub-pool, Middle sub-pool, and High sub-pool must be specified in the screen to configure each of these sub-pools.	Manual

Table-23 Values for specifying a Tier pool (gold)

5. Enter the items shown in the following table, and then click [Create]. A RAID group is created.

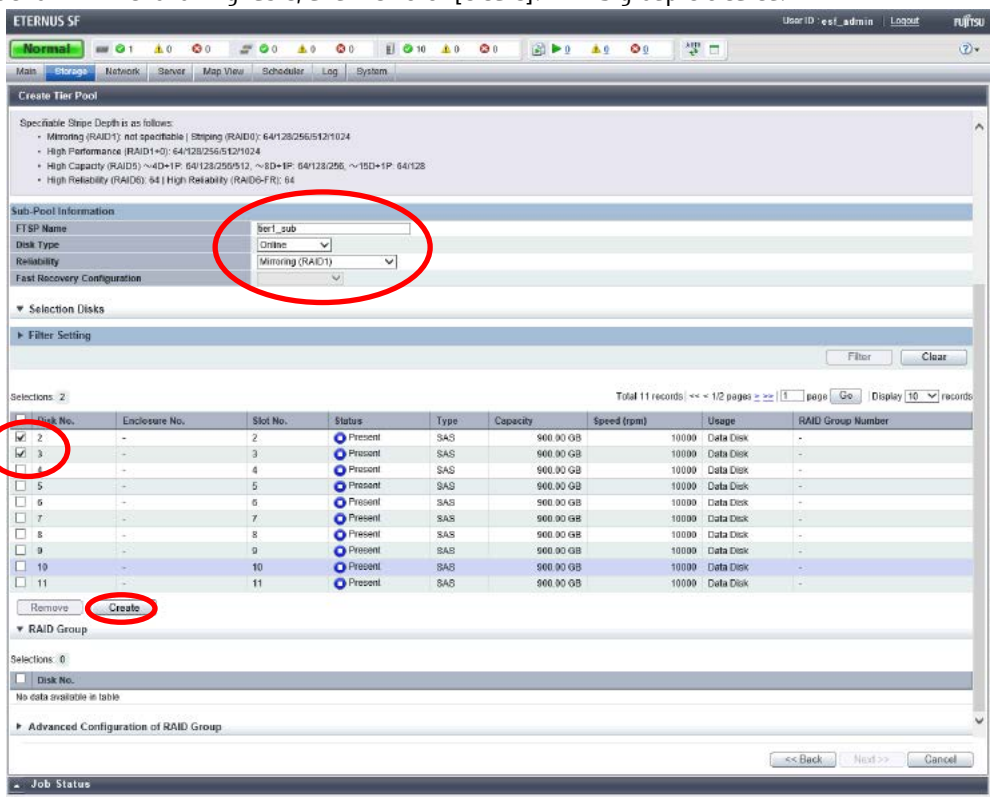

Figure-51 Specifying a sub-pool (gold)

Item	Description	Information
FTSP Name	Specify a unique sub-pool name in the storage system. Any alphanumeric character (from 1 to 16 characters), a hyphen (-), an underscore (_), and a pound symbol (#) can be specified. The characters are case insensitive.	tier1_sub
Disk Type	Specify the type of disk that configures the sub-pool. Make a selection from the disk types (Online, Nearline, SSD, SED-SAS) that are displayed in the pull-down list.	Online

Reliability	Specify the RAID level of the sub-pool. Select one of the following options that are displayed in the pull-down list. - High Performance(RAID1+0) - High Capacity(RAID5) - High Reliability(RAID6) - High Reliability(RAID6-FR) - Mirroring(RAID1) - Striping(RAID0)	Mirroring(RAID1)
Fast Recovery Configuration	Set this item when [High Reliability(RAID6-FR)] is selected for [Reliability]. A RAID group must be created based on the number of disks for the specified configuration. When a level other than [High Reliability(RAID6-FR)] is selected for [Reliability], specification is not necessary.	Unspecified
Disk No.	Number of the disk for configuring the sub-pool.	2 and 3

Table-24 Values for specifying a sub-pool (gold)

Points
Not all available combinations of the RAID levels and the number of member disks are supported for RAID groups that can be used as Tier pools.
For details, refer to "FUJITSU Storage ETERNUS SF Storage Cruiser V16.2 Operation Guide for Optimization Function".

6. Select the created RAID group, and then click [Next].

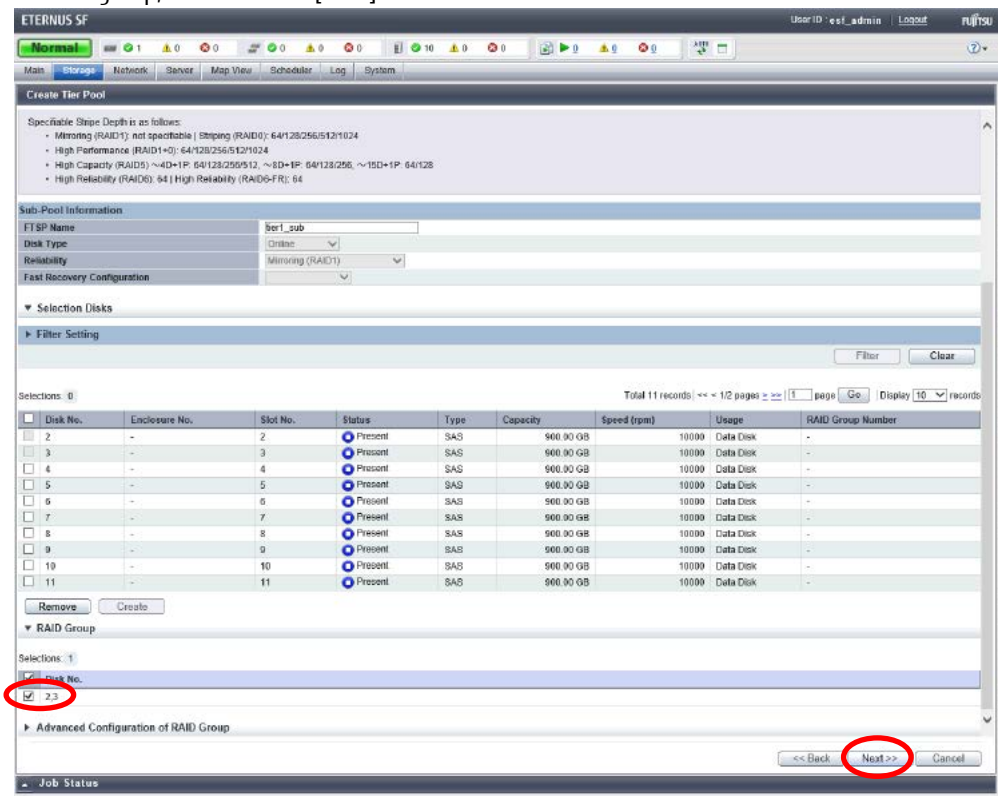

Figure-52 Disk No. for configuring the RAID group

7. The information confirmation screen is displayed.
Confirm the information, and then click the [Create] button on the lower right corner of the screen.

Points
Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next step.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

8. Add the RAID group to a Tier pool (gold) for the VVOL datastores to expand the capacity.
Click [Storage] on the global navigation tab.

9. On the Main pane, click the ETERNUS DX S3 series link under [Name].

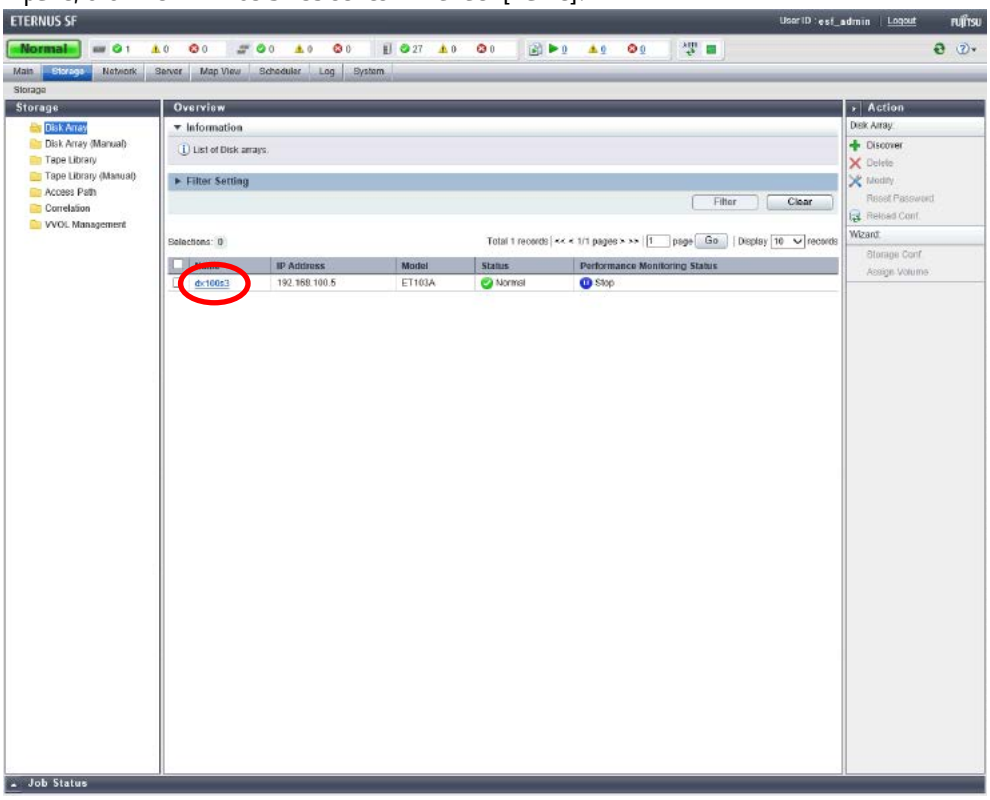

Figure-53 Storage

10. On the Category pane, click [Automated Storage Tiering].

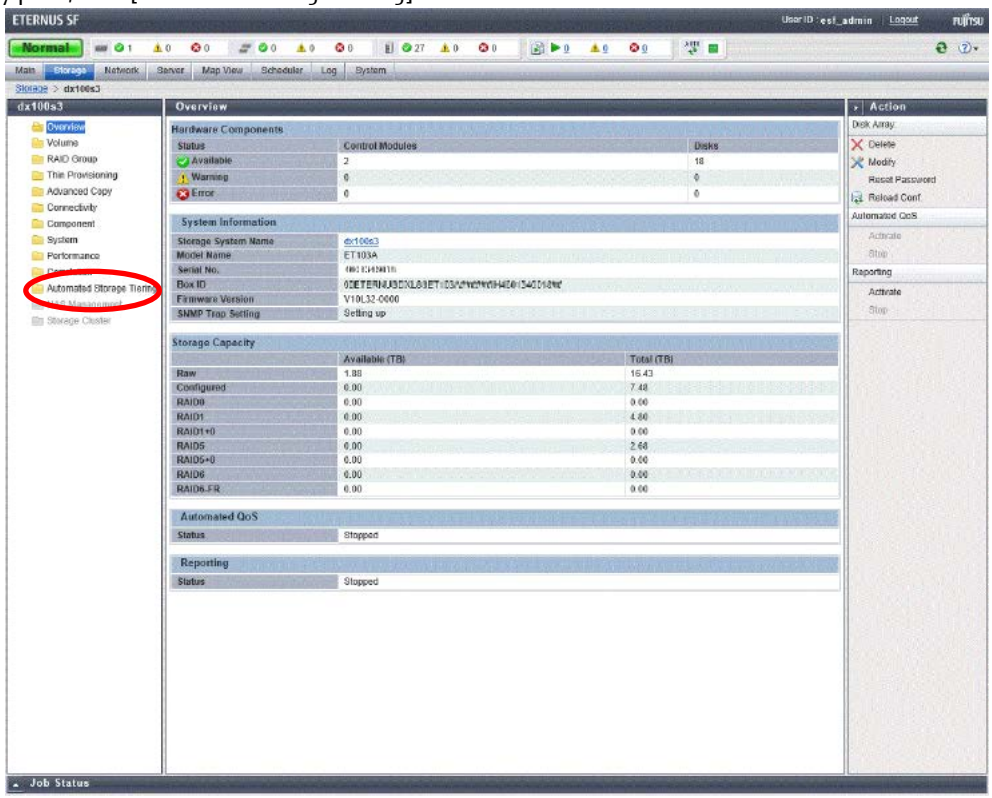

Figure-54 dx100s3

11. On the Category pane, click [Tier Pool].
    From the Tier pools that are displayed on the Main pane, click the pool number of Tier1_gold.

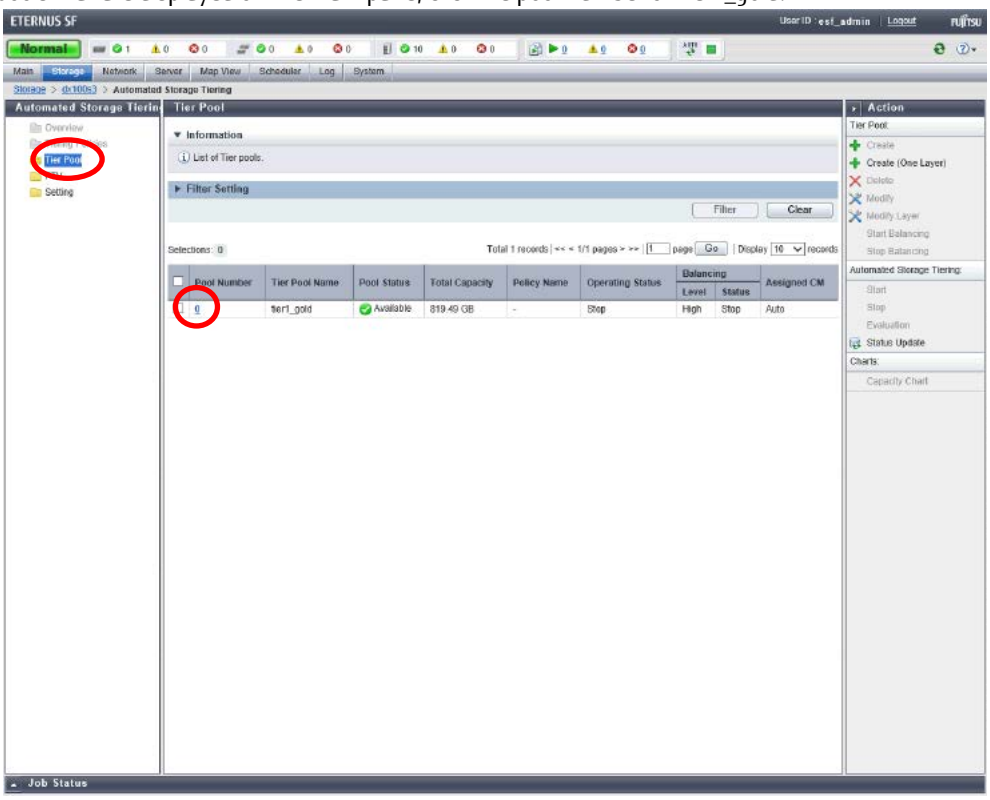

Figure-55 Tier pool list

12. On the Main pane, click the [Sub-Pool] tab.

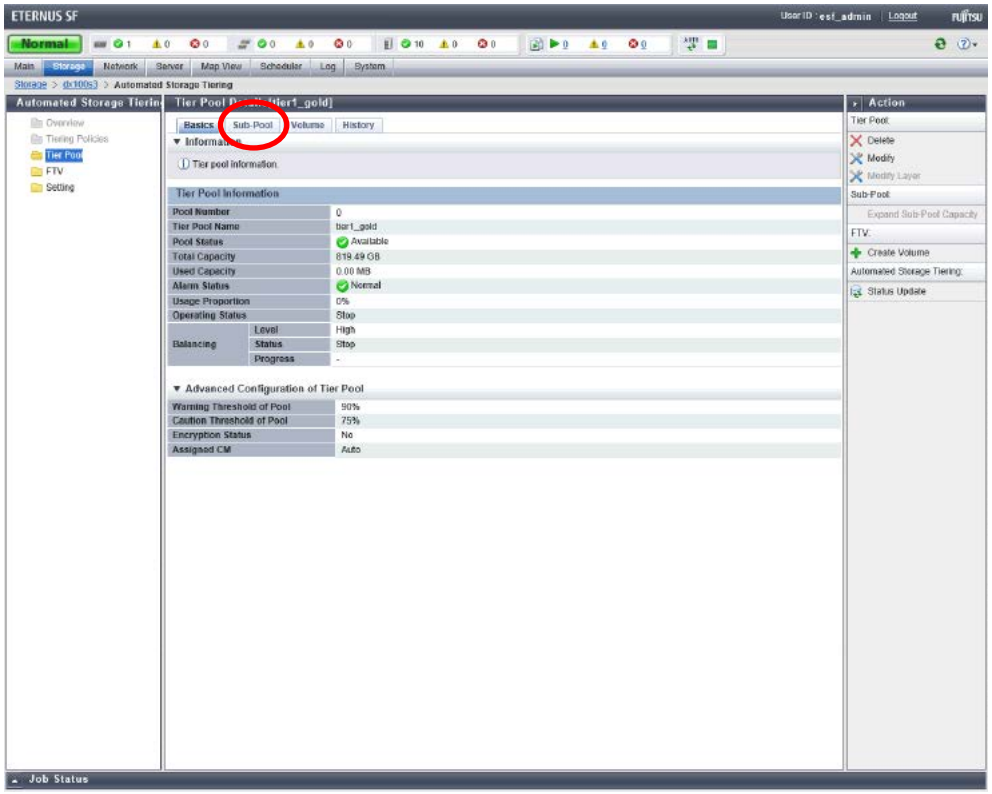

Figure-56 Tier pool information

13. Select [tier1_sub] and click [Expand Sub-Pool Capacity].

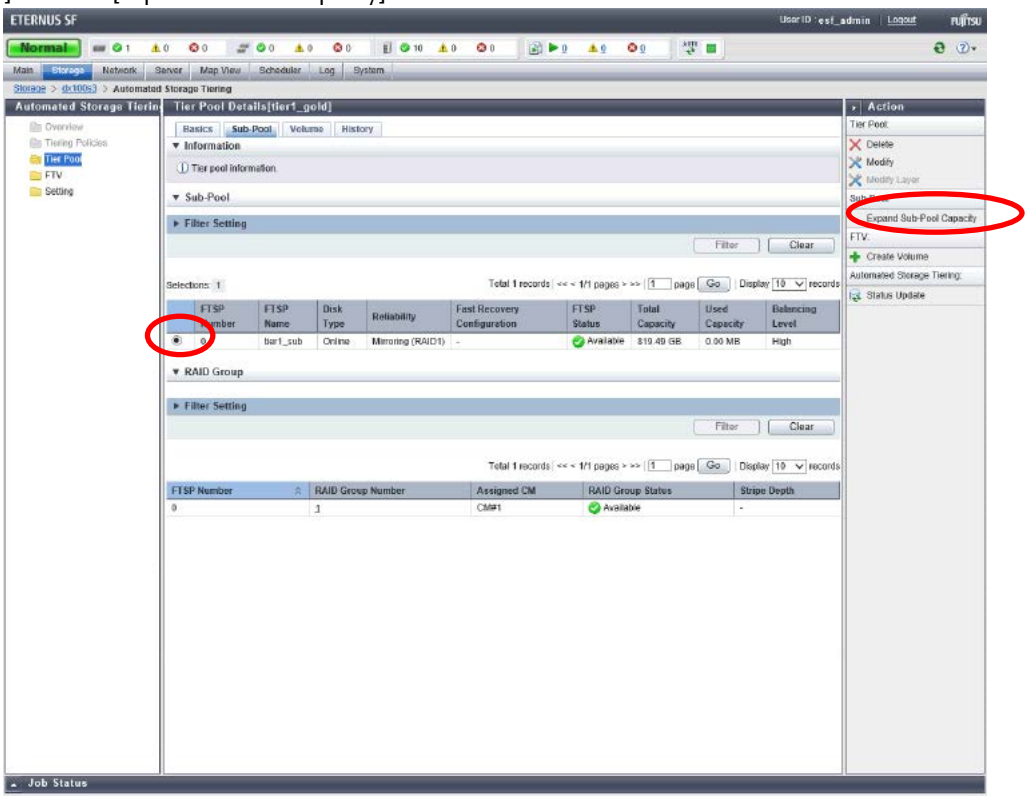

Figure-57 Tier pool information (Sub-Pool)

14. In the [Confirm target Tier Pool] screen, select [Manual] for [Disk Selection] in [Sub-Pool Information] and click [Next].

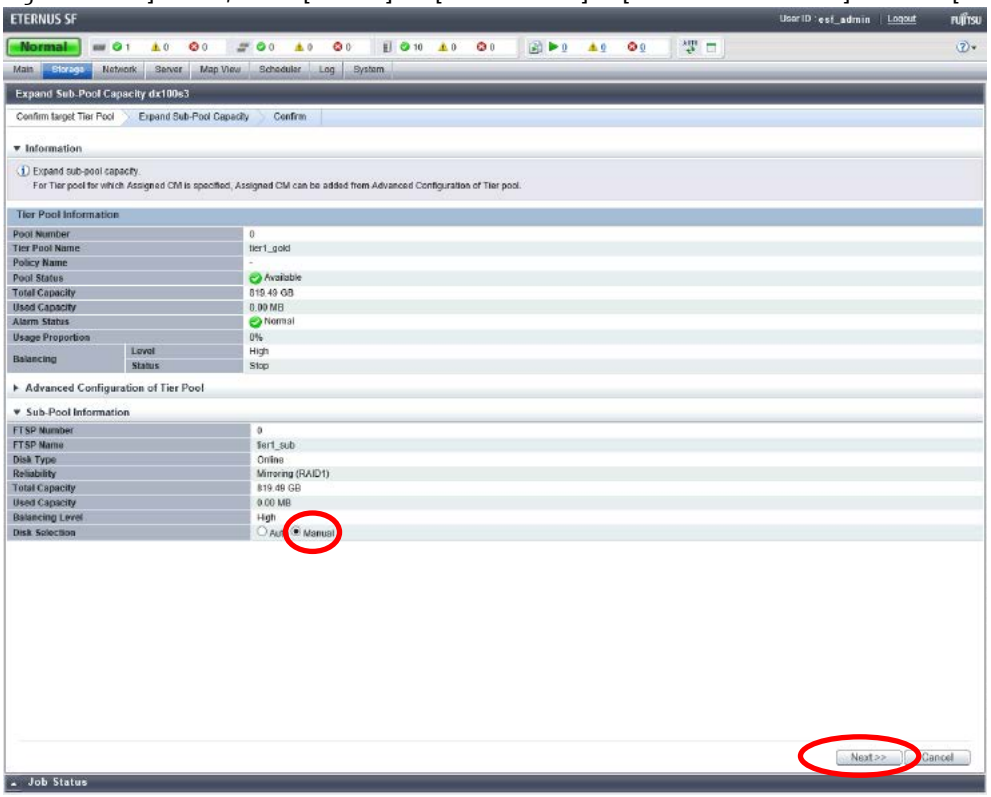

Figure-58 Confirm target Tier Pool

15. Enter the information that is provided in the following table and click [Create]. The RAID group is created.

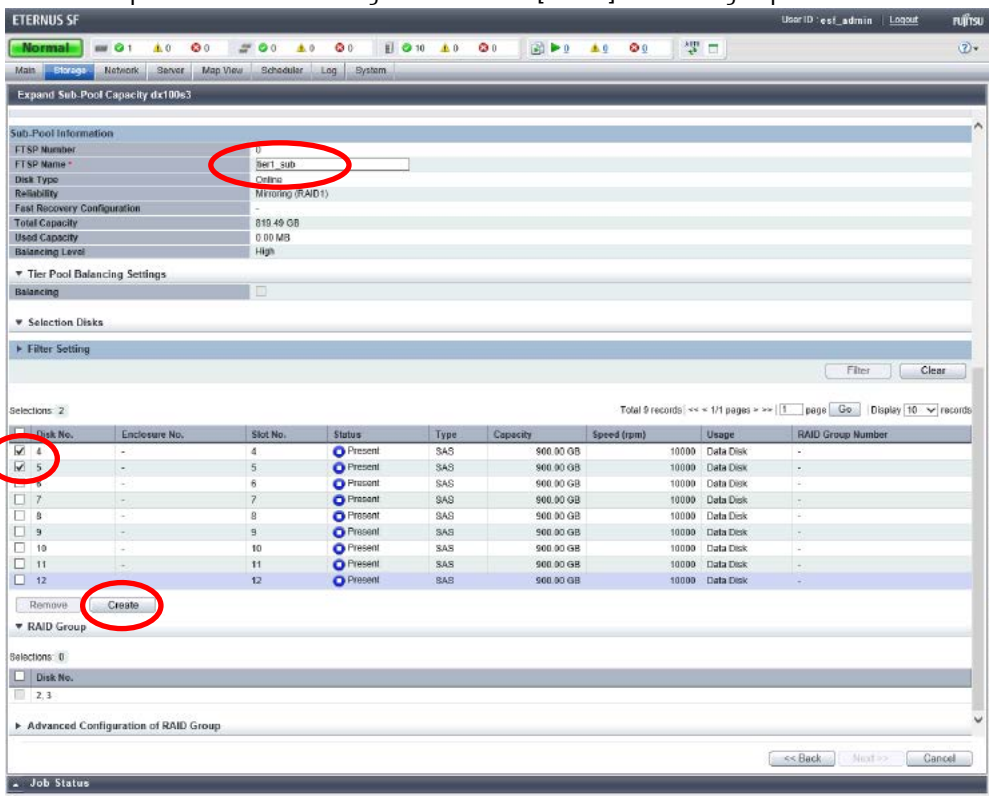

Figure-59 Expand Sub-Pool Capacity (Creating a RAID group)

Item	Description	Information
FTSP Name	Specify a unique name in the storage system. Any alphanumeric character (from 1 to 16 characters), a hyphen (-), an underscore (_), and a pound symbol (#) can be specified. The characters are case insensitive.	tier1_sub
Disk Type	The same disk types are displayed as when the sub-pool was created.	Online
Reliability	The same RAID levels are displayed as when the sub-pool was created.	Mirroring(RAID1)
Fast Recovery Configuration	Specification is not necessary.	-
Disk No.	Disk number that is used to expand the sub-pool	4 and 5

Table-25 Values for specifying a sub-pool (expansion)

16. Select the created RAID group and click [Next].

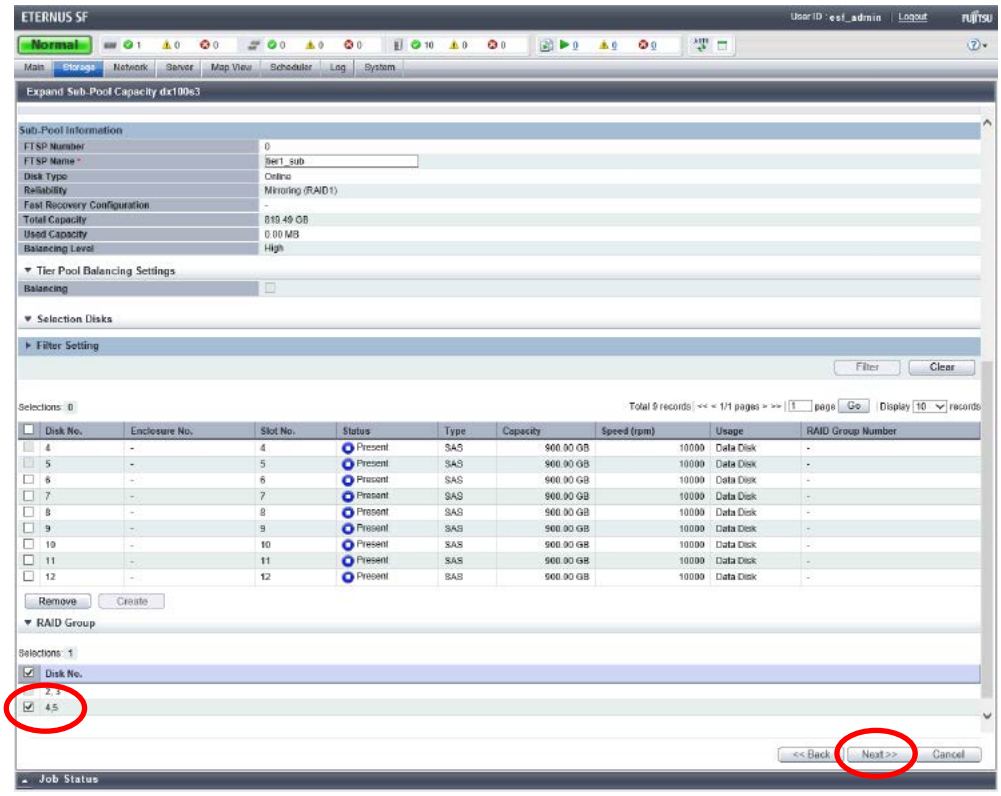

Figure-60 Expand Sub-Pool Capacity (adding a RAID group)

17. Check the settings and click [Expand].

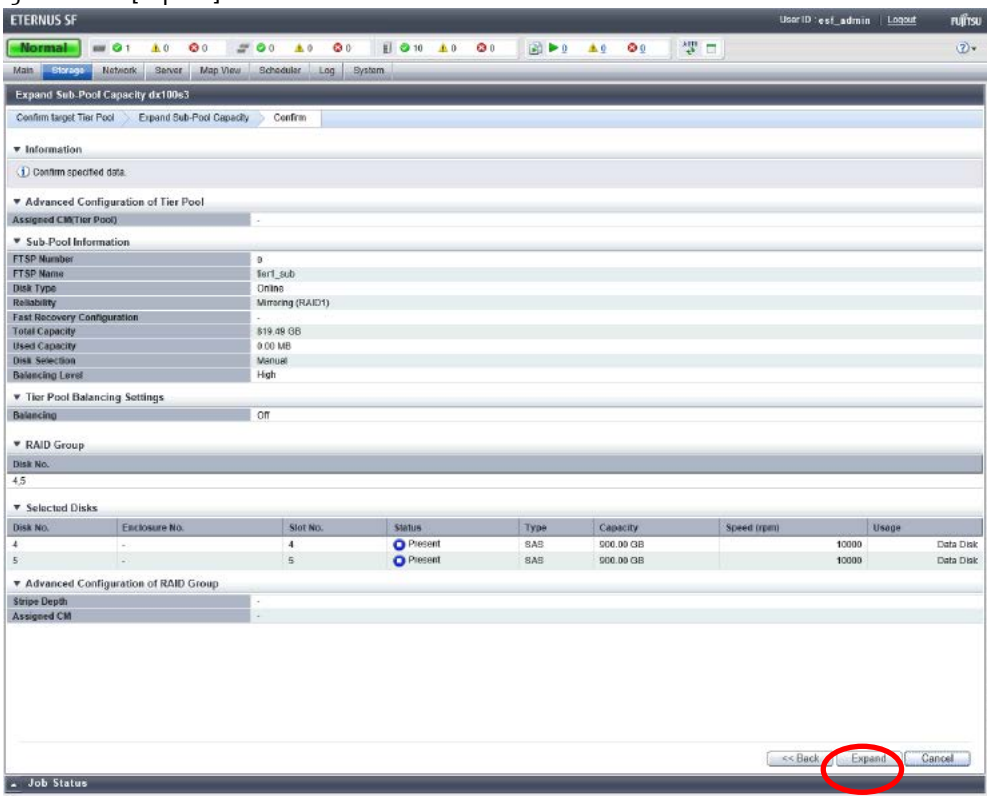

Figure-61 Confirm

18. Repeat Steps 8 to 17 to add Disk No.6 to 11.

Item	Description	Information
FTSP Name	Specify a unique name in the storage system. Any alphanumeric character (from 1 to 16 characters), a hyphen (-), an underscore (_), and a pound symbol (#) can be specified. The characters are case insensitive.	tier1_sub
Disk Type	The same disk types are displayed as when the sub-pool was created.	Online
Reliability	The same RAID levels are displayed as when the sub-pool was created.	Mirroring(RAID1)
Fast Recovery Configuration	Specification is not necessary.	-
Disk No.	Disk number that is used to expand the sub-pool.	6 and 7
		8 and 9
		10 and 11

Table-26 Values for specifying a sub-pool (expansion)

19. Repeat Steps 1 to 7 to create a Tier pool (clone backup) for the VVOL datastores.
    For each setting, enter the items shown in the following table.

Item	Information
Tier Pool Name	tier2_bkup
Disk Selection	Manual

Table-27 Values for specifying a Tier pool (backup)

Item	Information
FTSP Name	tier2_sub
Disk Type	Nearline
Reliability	High Capacity(RAID5)
Fast Recovery Configuration	Unspecified
Disk No.	13, 14, 15, and 16

Table-28 Values for specifying a sub-pool (backup)

2.2.3.1.4 Checking the Tier Pools

Confirm that the Tier pools are created.

1. In the global navigation tab, click [Storage].
2. On the Main pane, click the ETERNUS DX S3 series link under [Name].

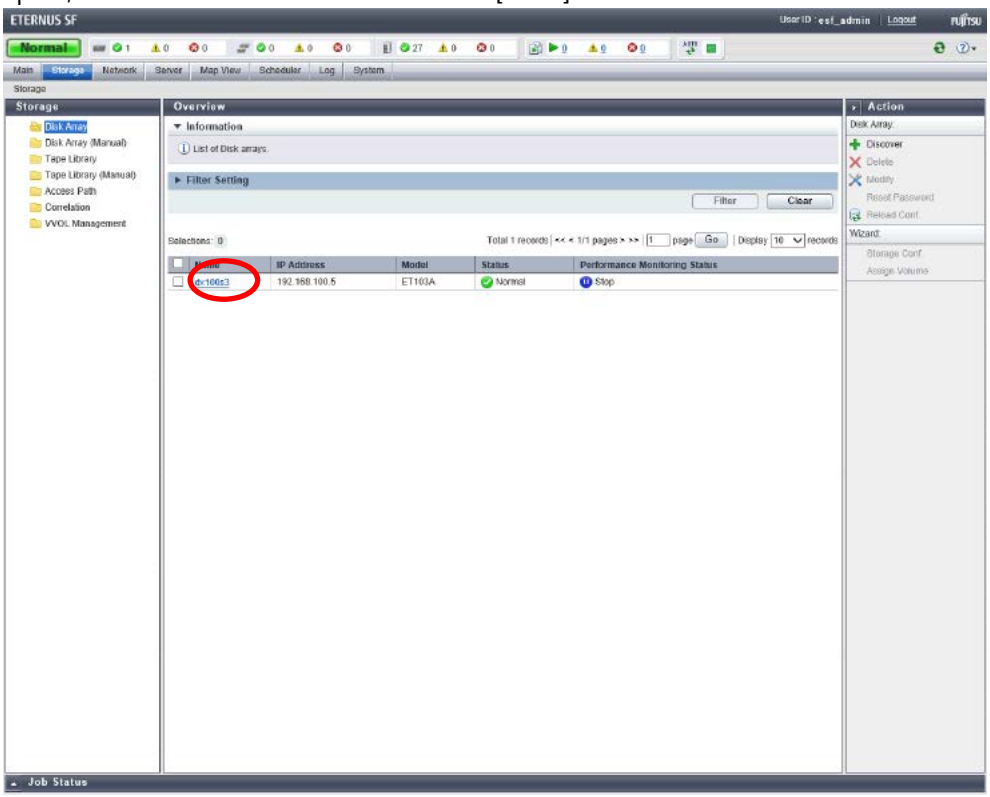

Figure-62 Storage

3. On the Category pane, click [Automated Storage Tiering].

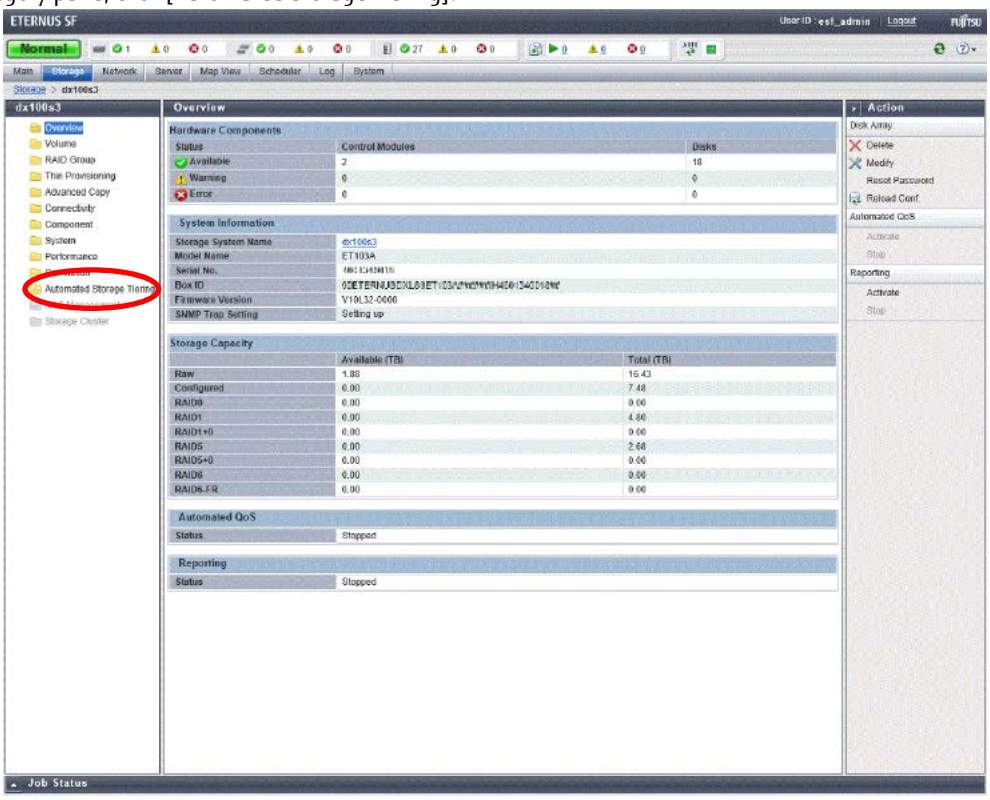

Figure-63 dx100s3

4. On the Category pane, click [Tier Pool].
   The registered Tier pools are displayed on the Main pane.

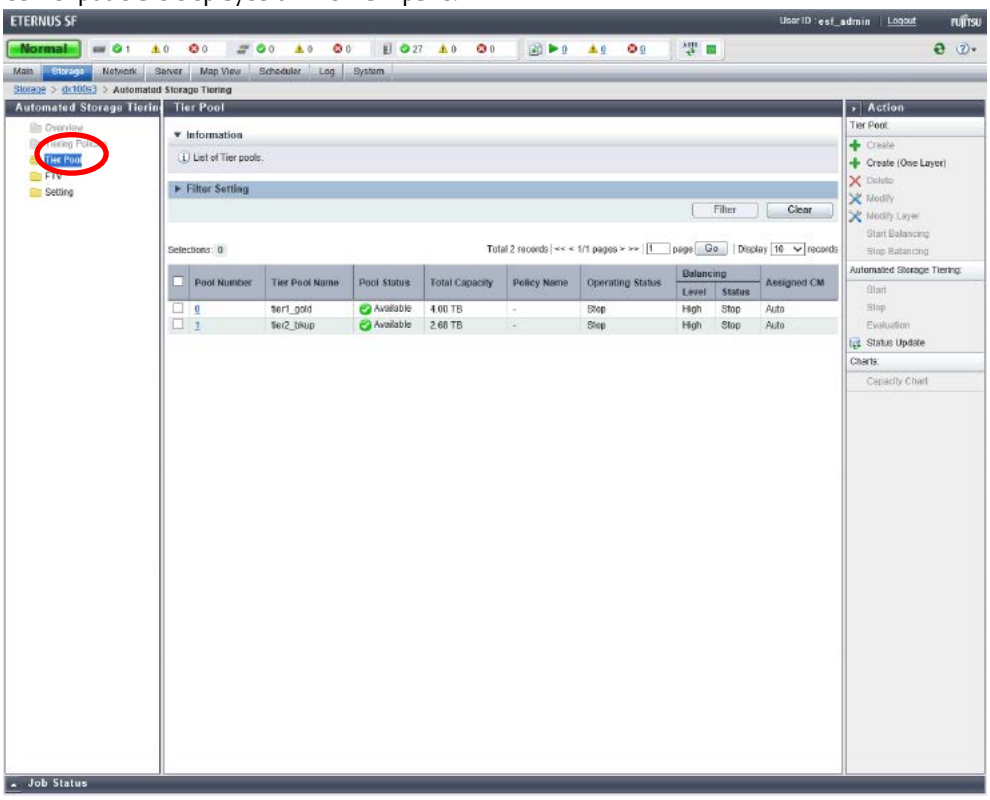

Figure-64 List of Tier pools

5. Check that the pools that were created in "2.2.3.1.3 Creating Tier Pools" are registered.

Tier Pool Name	Pool Status	Check ☑
tier1_gold	Available	□
tier2_bkup	Available	□

Table-29 Checklist for the created Tier pools

Check that all the Tier pools are created and that the status is [Available], and then proceed to the next procedure.

2.2.3.1.5 Creating VVOL Datastores

1. Create a VVOL datastore (gold).
   From ETERNUS SF Web Console, click [Storage] on the global navigation tab.
   On the Category pane, click [VVOL Management].

2. On the Action pane, click [Create/Modify] under [VVOL Datastore].

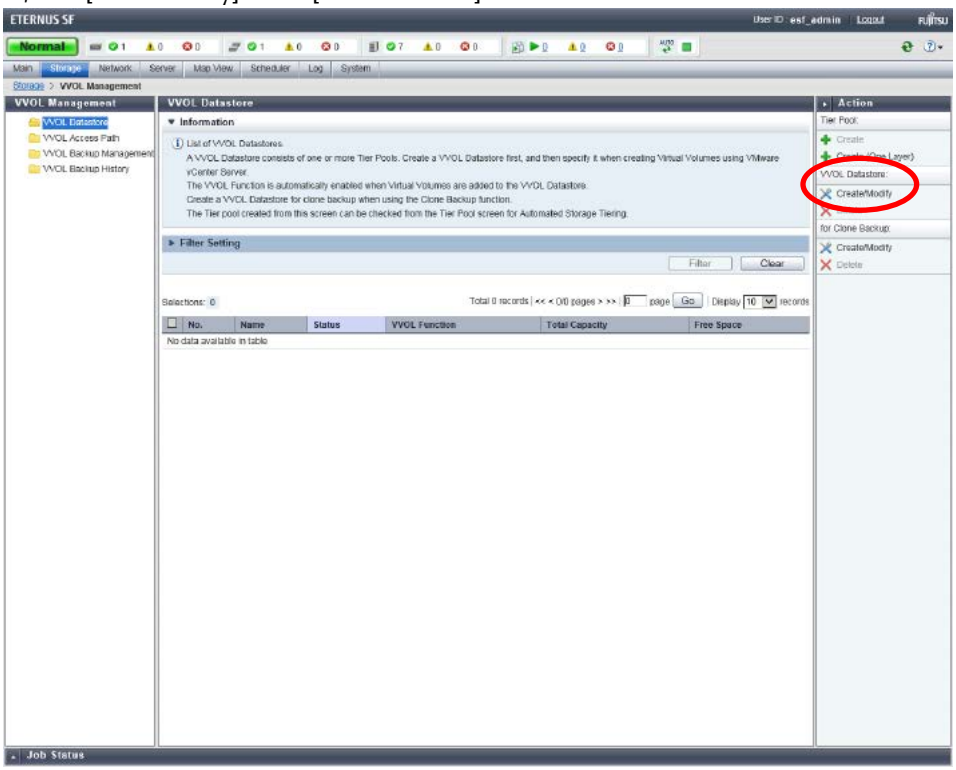

Figure-65 VVOL Management

3. Enter the items shown in the following table, and then click [Add].

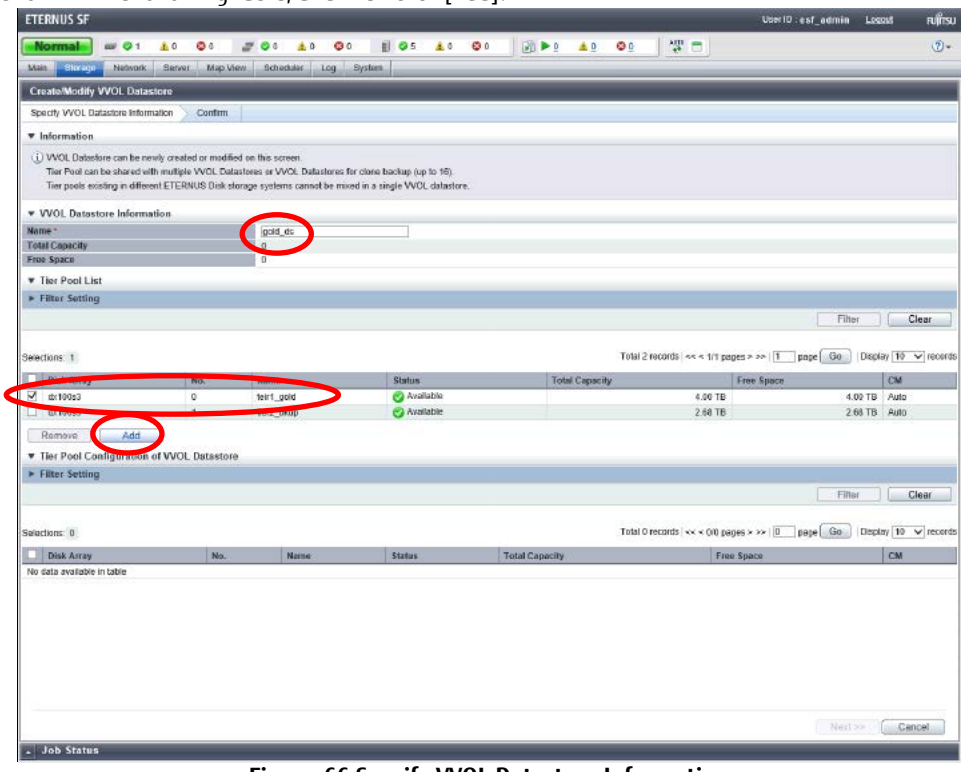

Figure-66 Specify VVOL Datastore Information

Item	Information
Name	gold_ds
Tier Pool List	tier1_gold

Table-30 Values for the "Specify VVOL Datastore Information" setting (gold)

4. Select the checkbox for the added Tier pool, and then click the [Next] button.

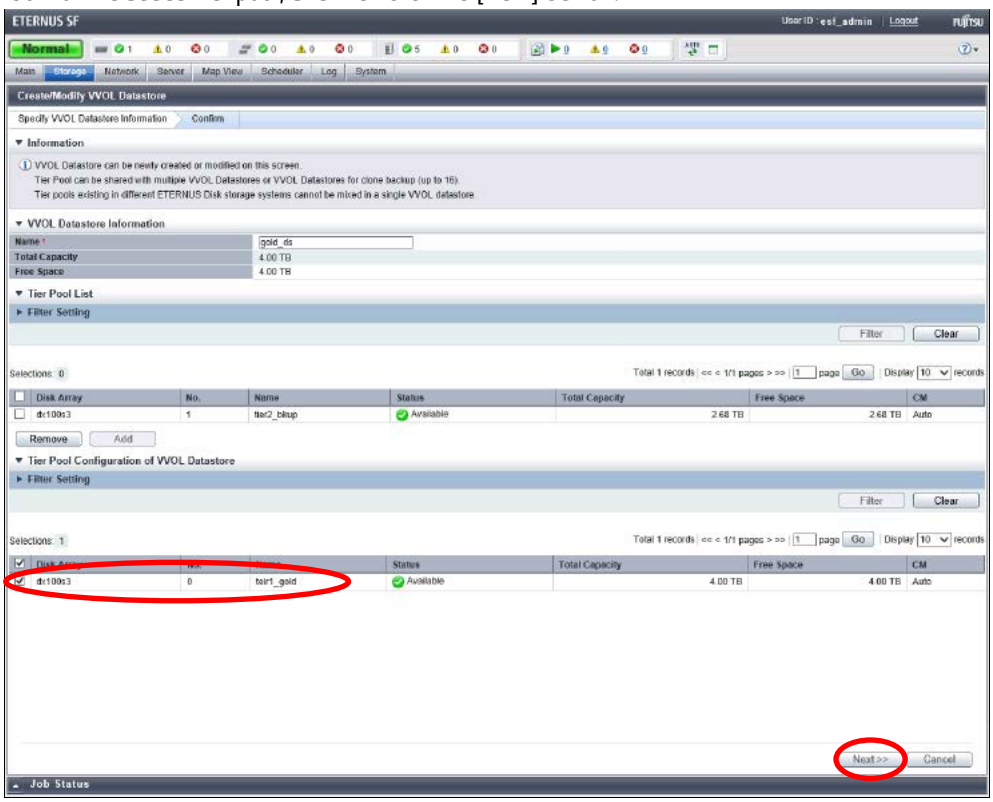

Figure-67 Tier Pool Configuration of VVOL Datastore

5. The information confirmation screen is displayed. Confirm the information, and then click [Create / Modify] on the lower right corner of the screen.

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next step.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

2.2.3.1.6 Creating a VVOL Datastore for Clone Backups

1. Create a VVOL datastore for clone backups.
   On the ETERNUS SF Web Console screen, click [Storage] in the global navigation tab.
   On the Category pane, click [VVOL Management].

2. On the Action pane, click [Create/Modify] under [for Clone Backup].

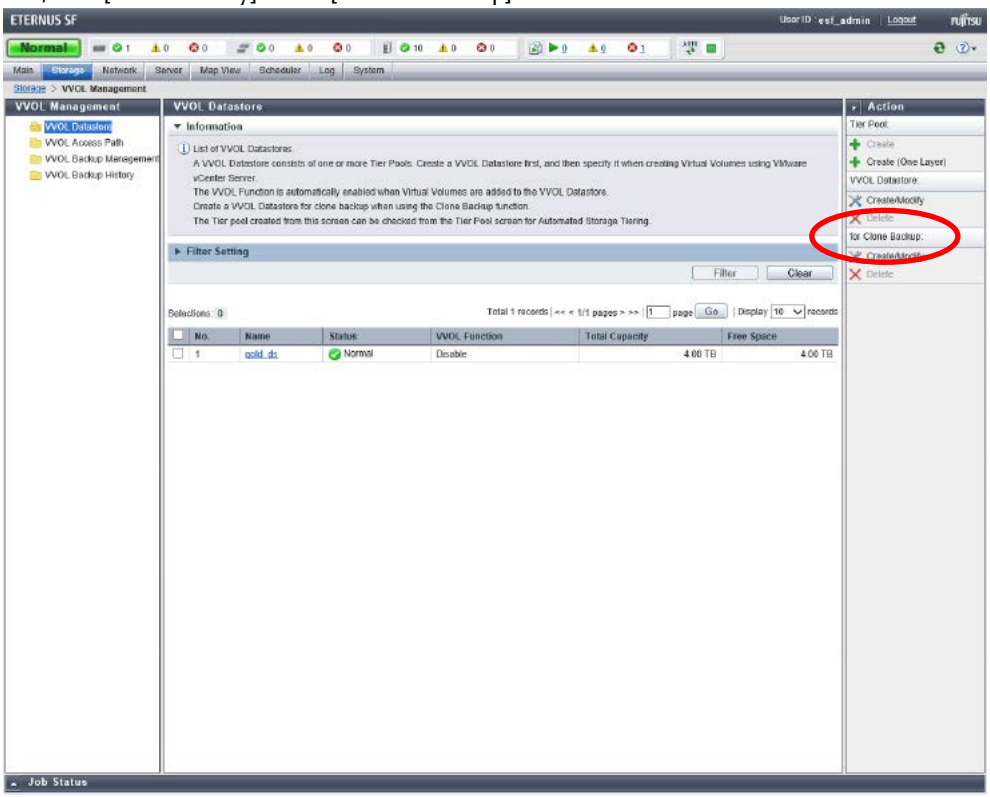

Figure-68 VVOL Management

3. Enter the items shown in the following table, and then click [Add].

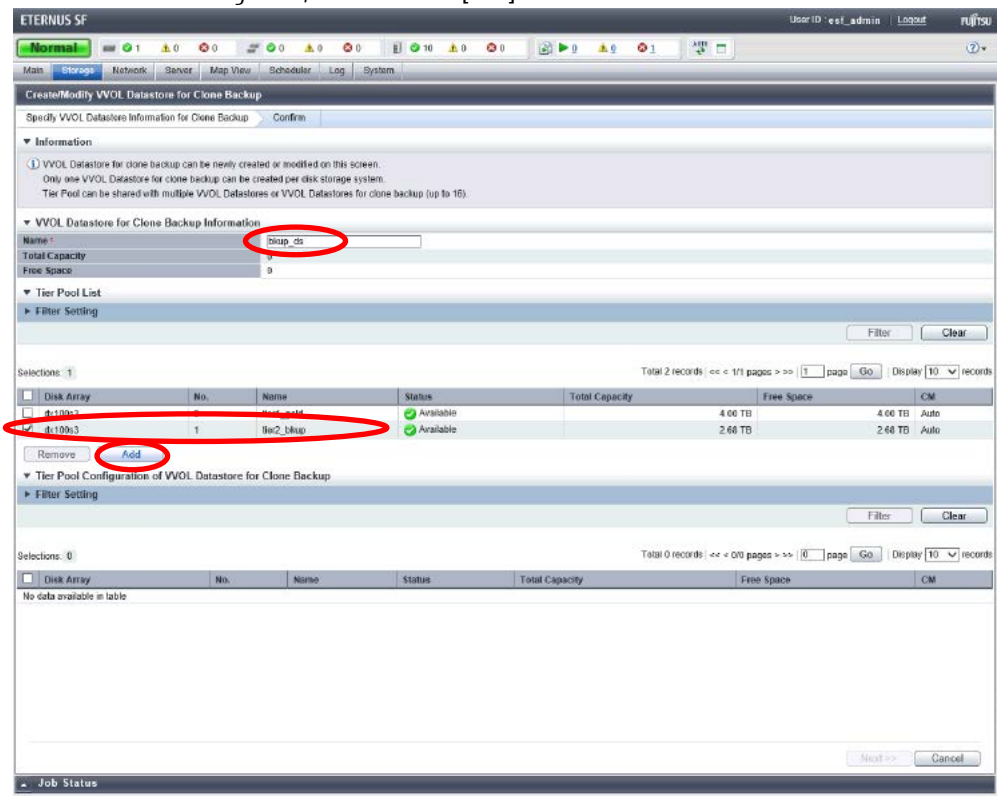

Figure-69 Specify VVOL Datastore Information for Clone Backup

Item	Information
Name	bkup_ds
Tier Pool List	tier2_bkup

Table-31 Values for the "Specify VVOL Datastore information for Clone Backup" setting

4. Select the checkbox for the added Tier pool, and then click the [Next] button.

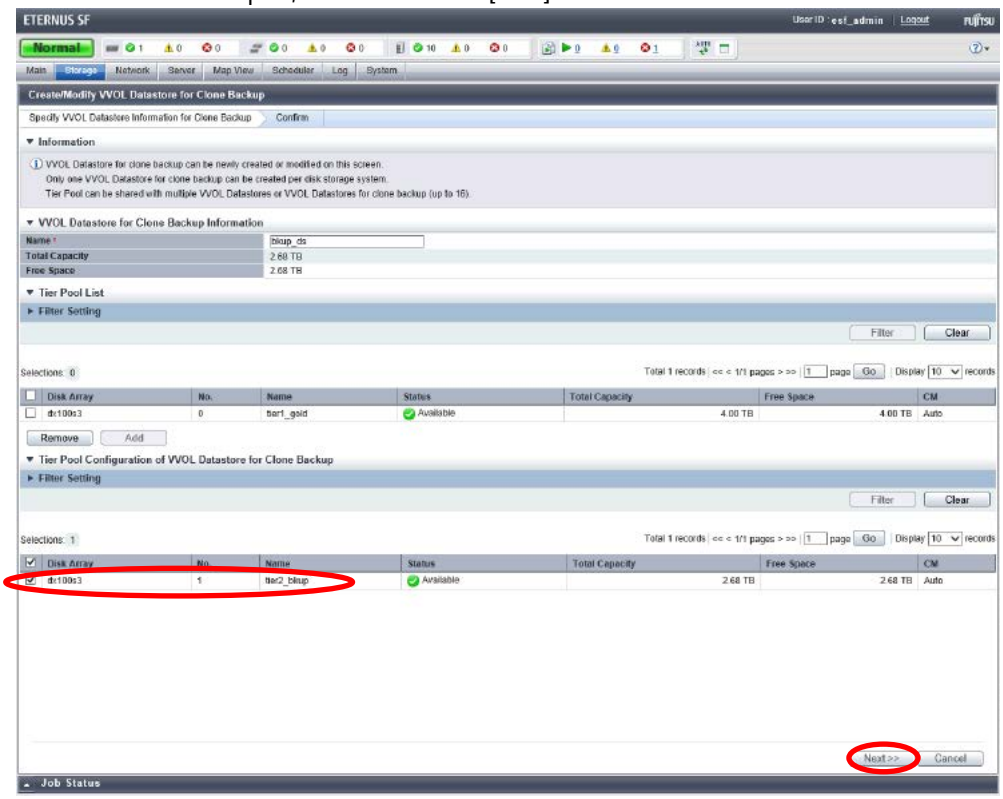

Figure-70 Tier Pool Configuration of VVOL Datastore for Clone Backup

5. The information confirmation screen is displayed. Confirm the information, and then click [Create / Modify] on the lower right corner of the screen.

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next procedure.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

2.2.3.1.7 Checking the VVOL Datastores

Confirm that the VVOL datastores are created.

1. In the global navigation tab, click [Storage].

2. On the Category pane, click [VVOL Management].
   The registered VVOL datastores are displayed on the Main pane.

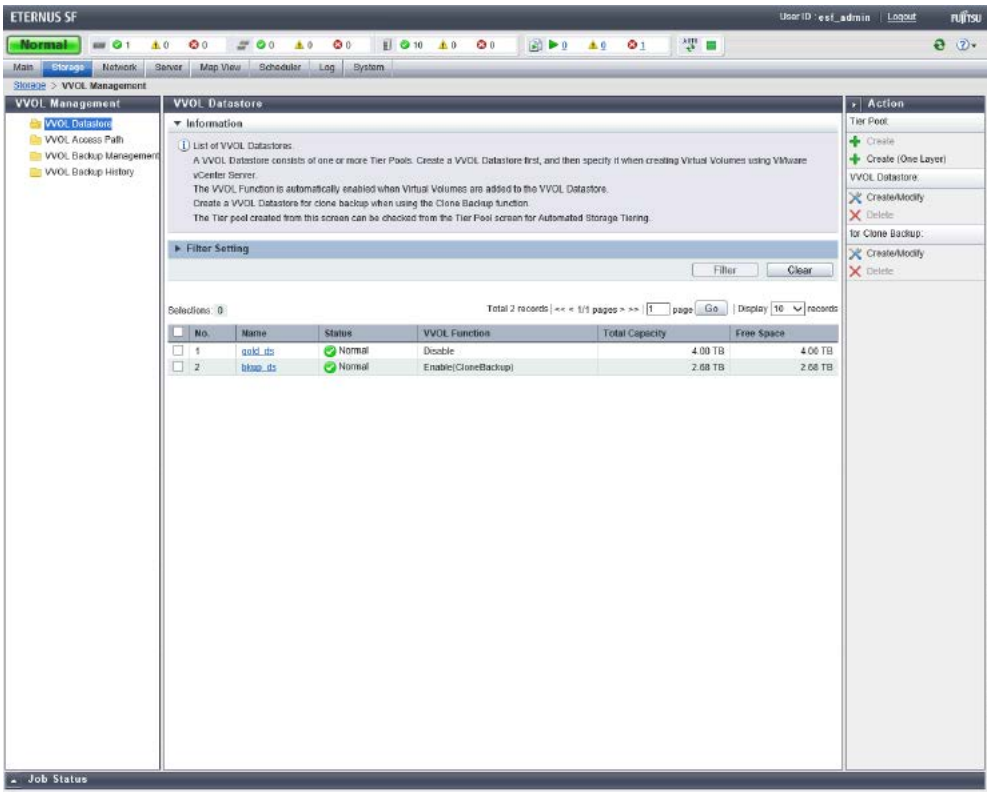

Figure-71 List of VVOL datastores

3. Check that the VVOL datastores that were created in "2.2.3.1.5 Creating VVOL Datastores" are registered.

Name	Status	VVOL Function	Check ☑
gold_ds	Normal	Enable(VVOL)	□
bkup_ds	Normal	Enable(CloneBackup)	□

Table-32 Checklist for the created VVOL datastores

Check that all of the VVOL datastores are created, and then proceed to the next procedure.

2.2.3.2 vCenter Server Operations

2.2.3.2.1 Rescanning the Storage Provider

1. Make the vCenter server recognize the VVOL datastores that were created in "2.2.3.1.5 Creating VVOL Datastores". Click the [Rescan] button on the [Storage Providers] screen.

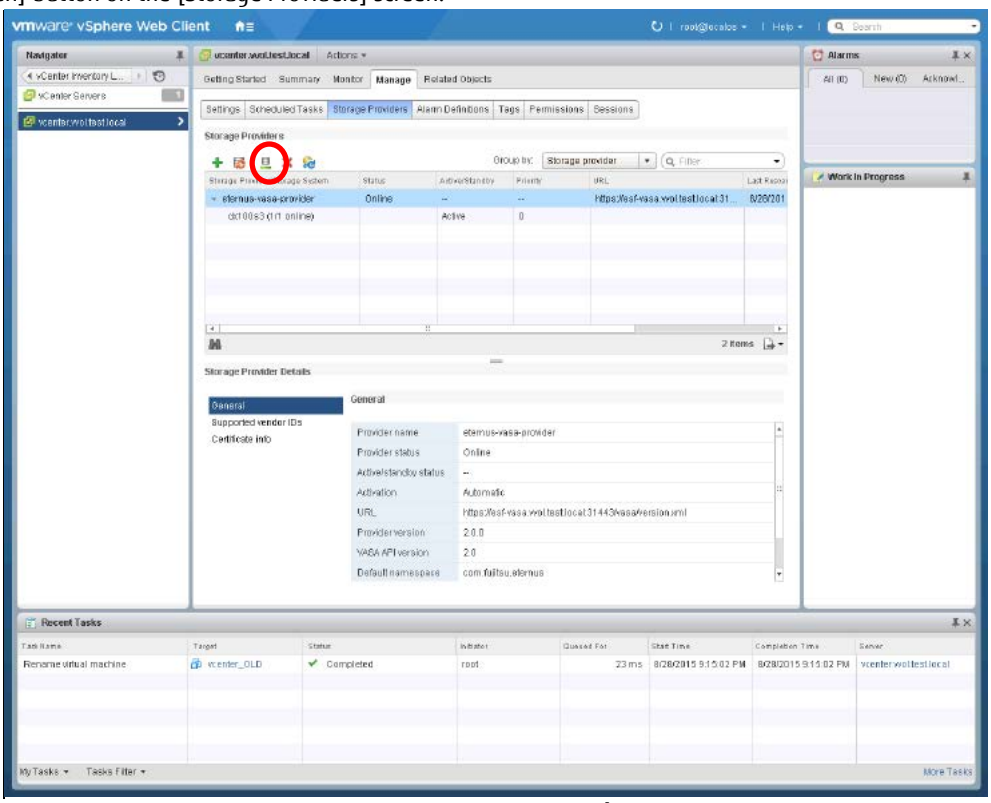

Figure-72 Storage Providers

2.2.3.2.2 Registering VVOL Datastores

1. Register the VVOL datastore (gold) in the vCenter server.
   Click [Actions] - [Storage] - [New Datastore].

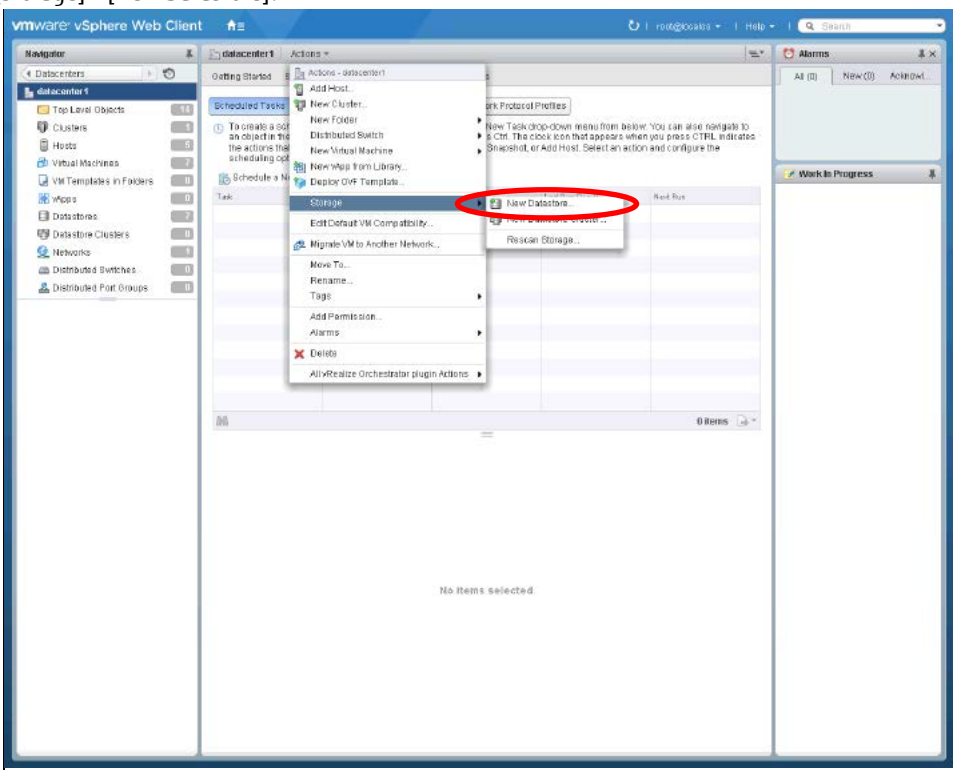

Figure-73 New Datastore

2. Confirm the location, and then click [Next].

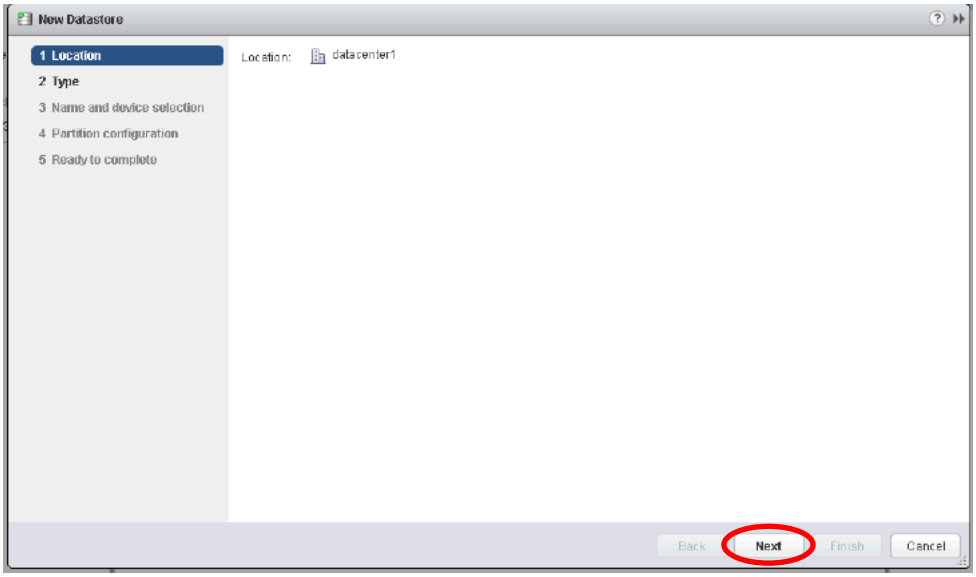

Figure-74 Location

3. Select [VVOL], and then click [Next].

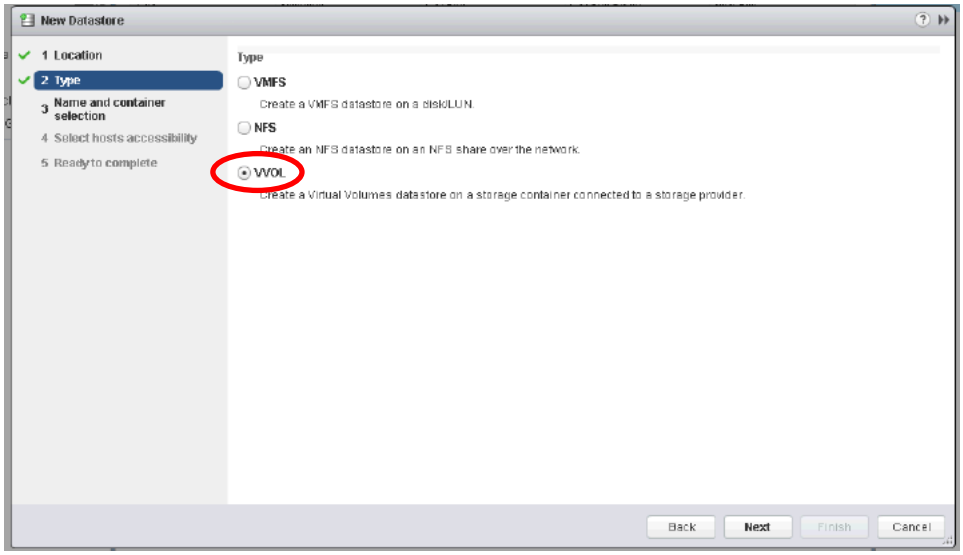

Figure-75 Type

4. Type "g_datastore" for [Datastore name], select [gold_ds] in [Backing Storage Container], and then click [Next].

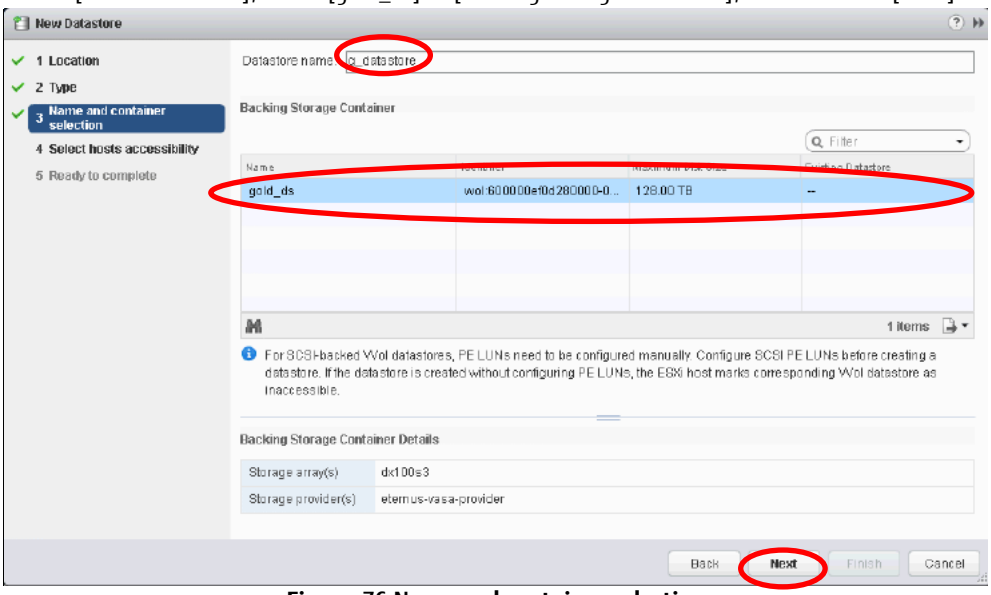

Figure-76 Name and container selection

5. Select the hosts, and then click [Next].

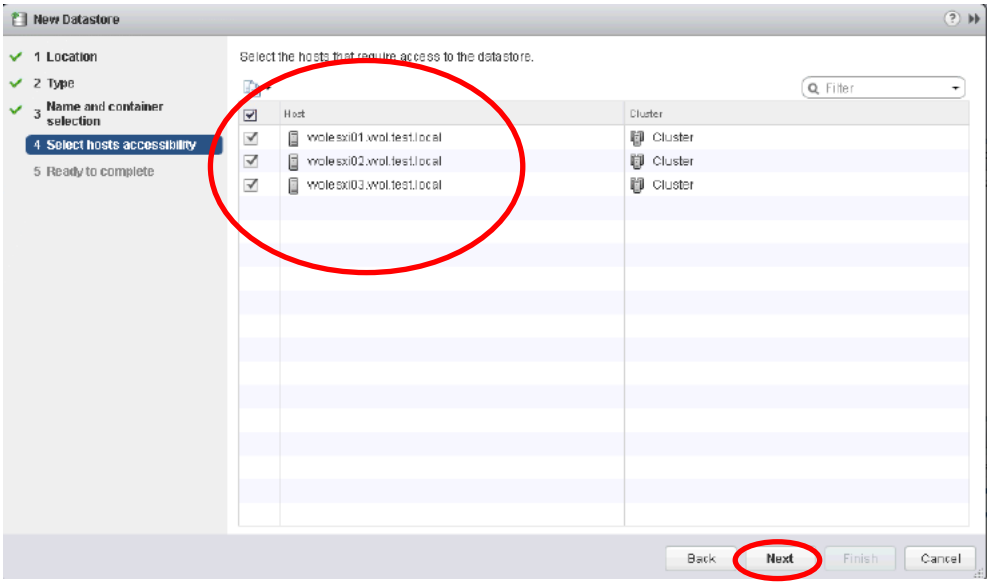

Figure-77 Select hosts accessibility

6. Check the configuration values, and then click [Finish].

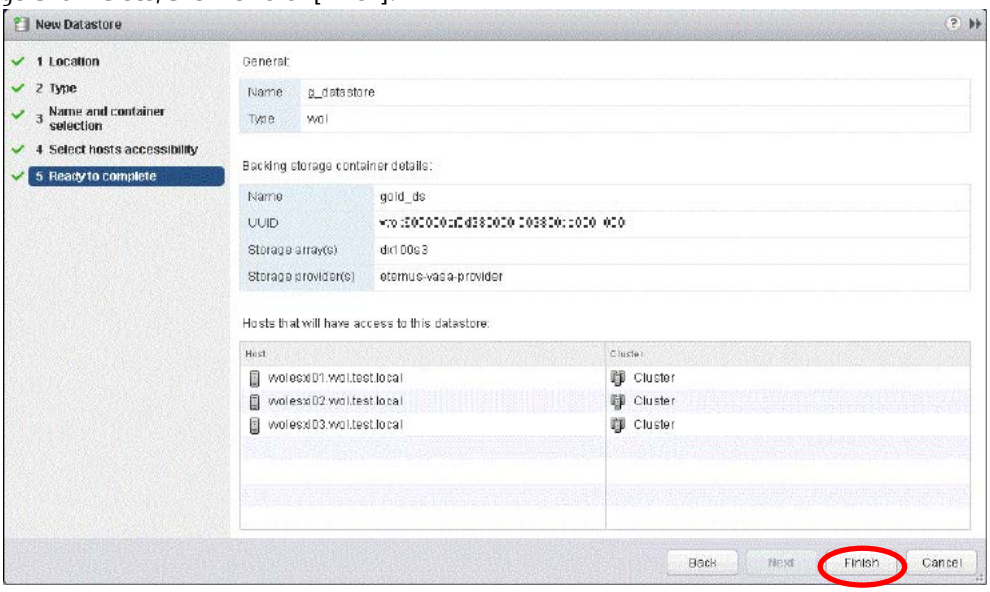

Figure-78 Ready to complete

For each setting, enter the items shown in the following table.

Item	Information
Location	Datacenter1
Type	VVOL
Datastore name	g_datastore
Backing Storage Container	gold_ds
Host	vvolesxi01 - vvolesxi03

Table-33 Values for registering VVOL datastores (gold)

2.2.3.2.3 Checking the VVOL Datastores

Confirm that the registered VVOL datastores are mounted on all the ESXi hosts.

1. From Navigator, click [Hosts and Clusters].

2. From the Navigator tree, click an ESXi host.

3. For the ESXi host, select [Related Objects] - [Datastores].

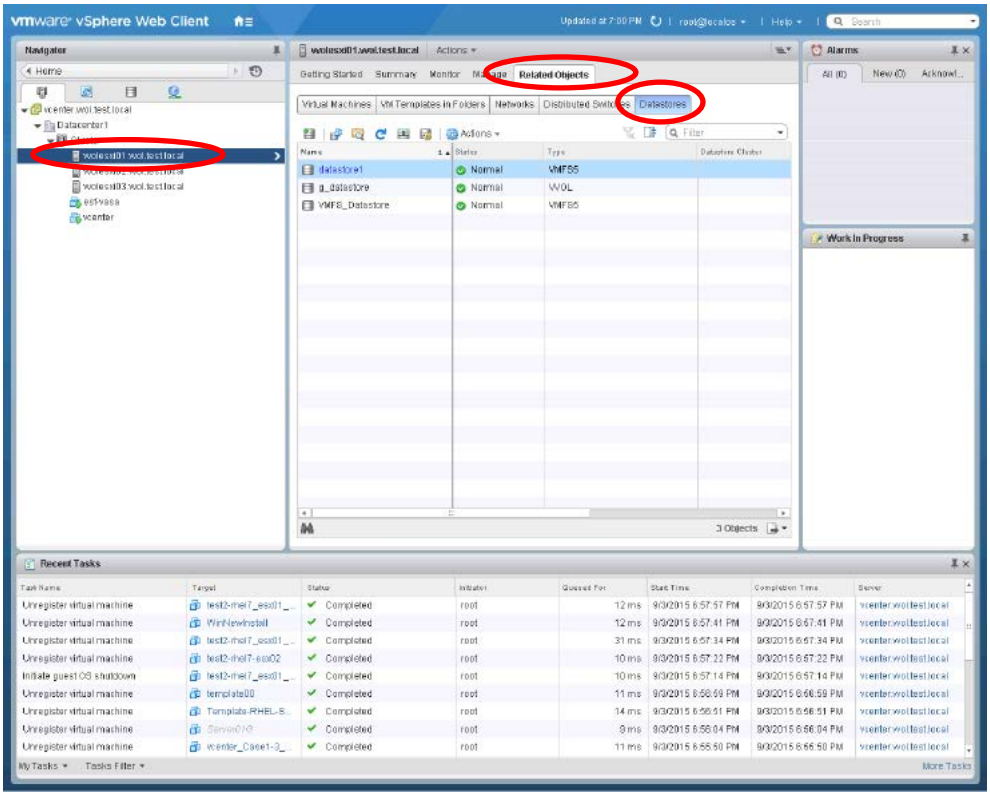

Figure-79 Checking the created vCenter Server VVOL datastores

Check that the VVOL datastores that were mounted on the ESXi hosts in "2.2.3.2.2 Registering VVOL Datastores" are mounted on each ESXi host.

ESXi host	VVOL datastore	Check ☑
vvolesxi01	g_datastore	□
vvolesxi02	g_datastore	□
vvolesxi03	g_datastore	□

Table-34 Checklist for the VVOL datastores mounted on the ESXi hosts

Check that the VVOL datastores are mounted on all the ESXi hosts, and then proceed to the next procedure.

2.2.3.2.4 Creating Policies

1. Create a policy for gold.
   In vSphere Web Client, click [VM Storage Policies] in [Home].

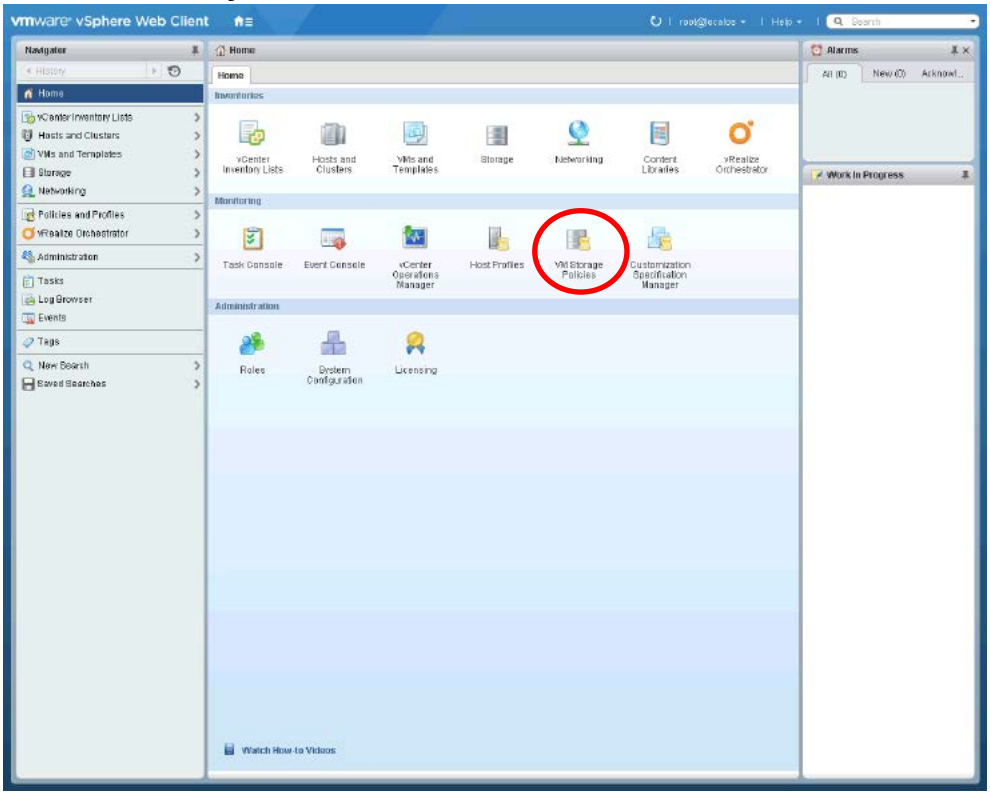

Figure-80 Home

2. Click the [Create New VM Storage Policy] icon.

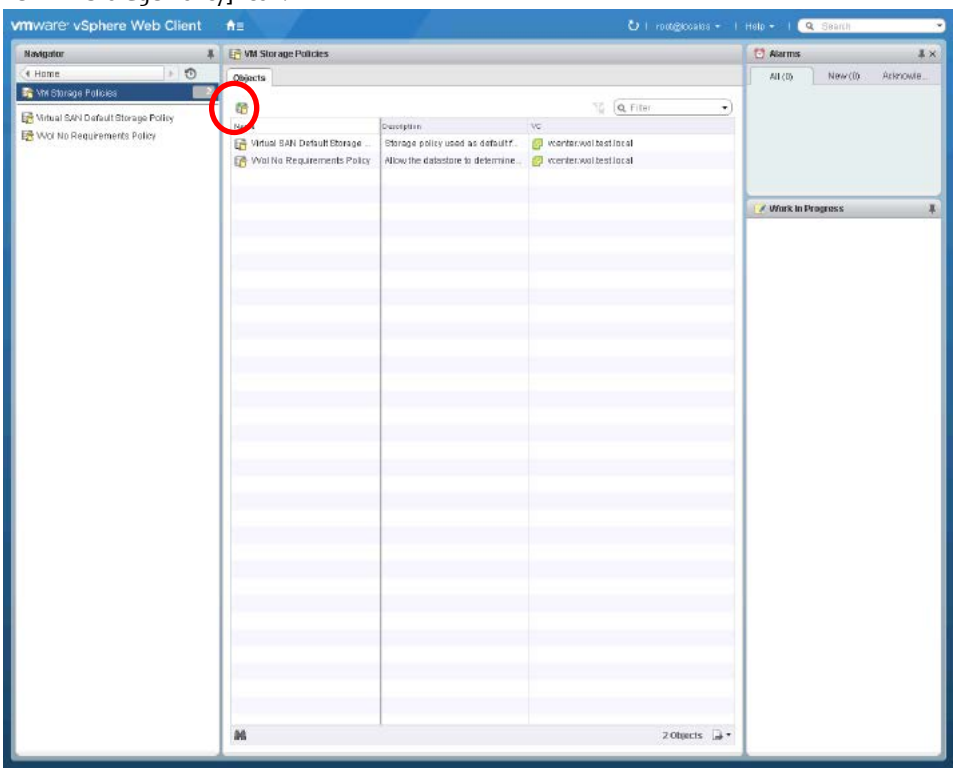

Figure-81 Creating a new virtual machine storage policy

3. In [Name and description], type "gold_policy" in [Name], and then click [Next].

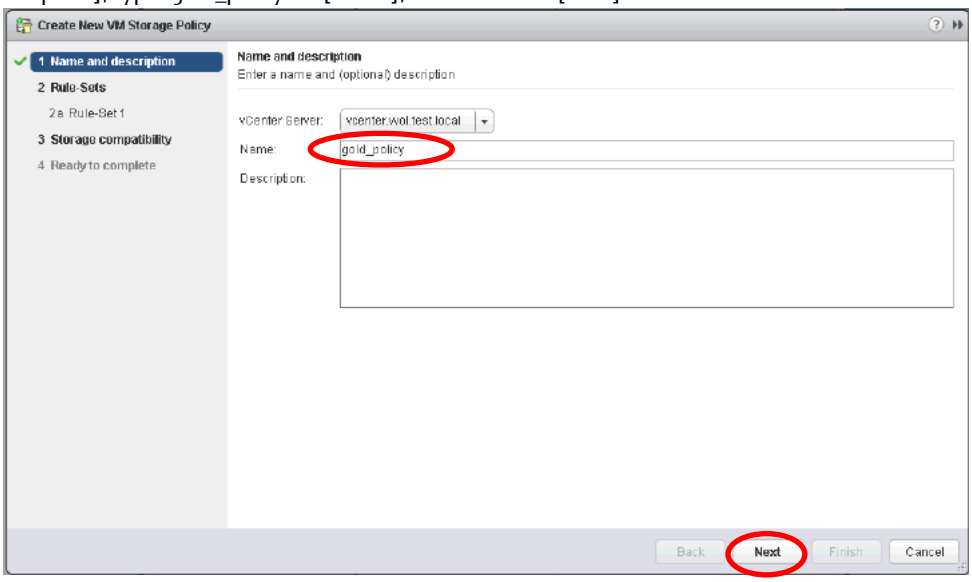

Figure-82 Name and description

4. In [Rule-Sets], specifying [Rules based on data services] as [com.fujitsu.eternus] displays the [Add rule] pull-down list.
Use this pull-down list to specify the values for the virtual machine backup settings. For each setting, enter the items shown in the following table.
After entering the information, click [Next].

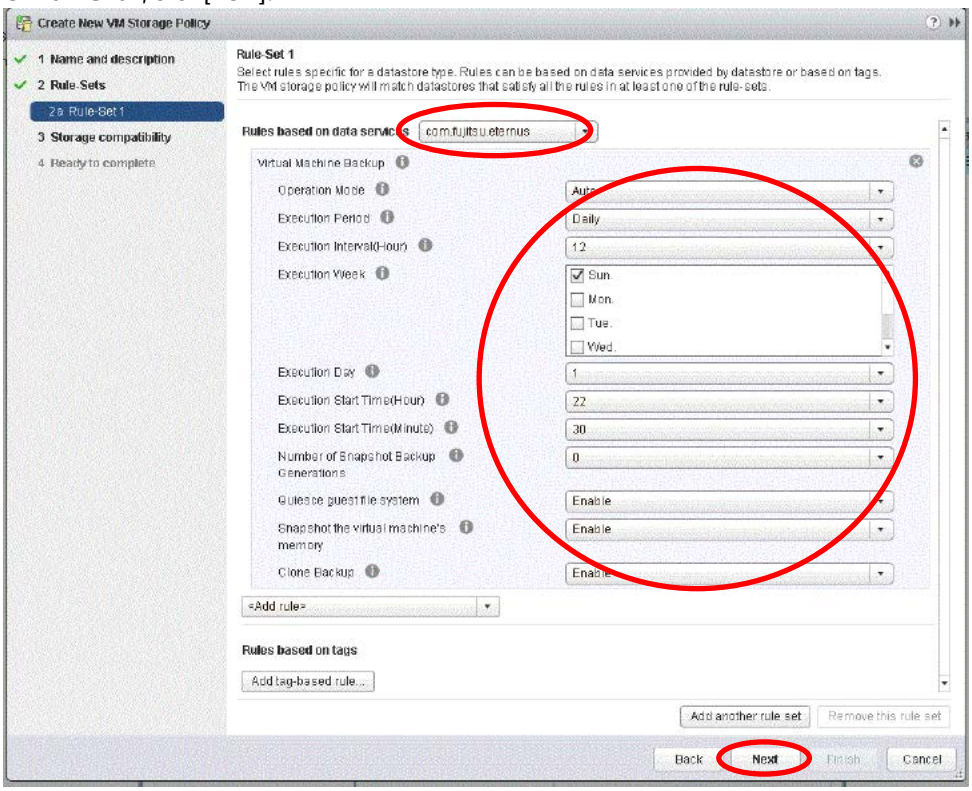

Figure-83 Virtual machine backup policy (Rule-Set 1)

Item	Information
Name	gold_policy
Operation Mode	Auto
Execution Period	Daily
Execution Start Time(Hour)	22
Execution Start Time(Minute)	30
Number of Snapshot Backup Generations	0
Quiesce guest file system	Enable
Snapshot the virtual machine's memory	Enable
Clone Backup	Enable

Table-35 Values for the virtual machine backup settings (gold)

5. In [Storage compatibility], [Compatible storage] displays the VVOL datastores that can fulfill the created policy. Select [g_datastore], and then click [Next].

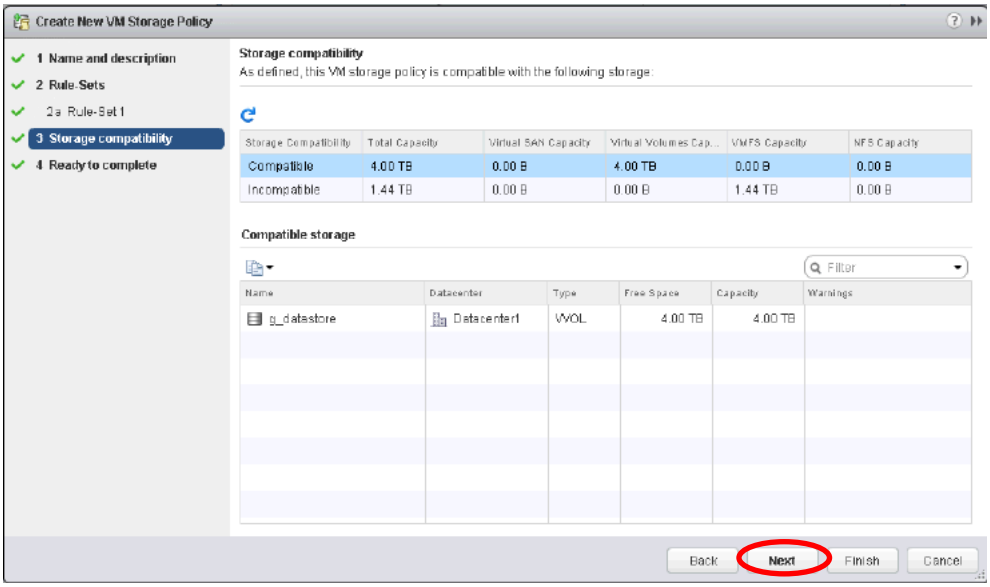

Figure-84 Storage compatibility

6. In [Ready to complete], click [Finish].

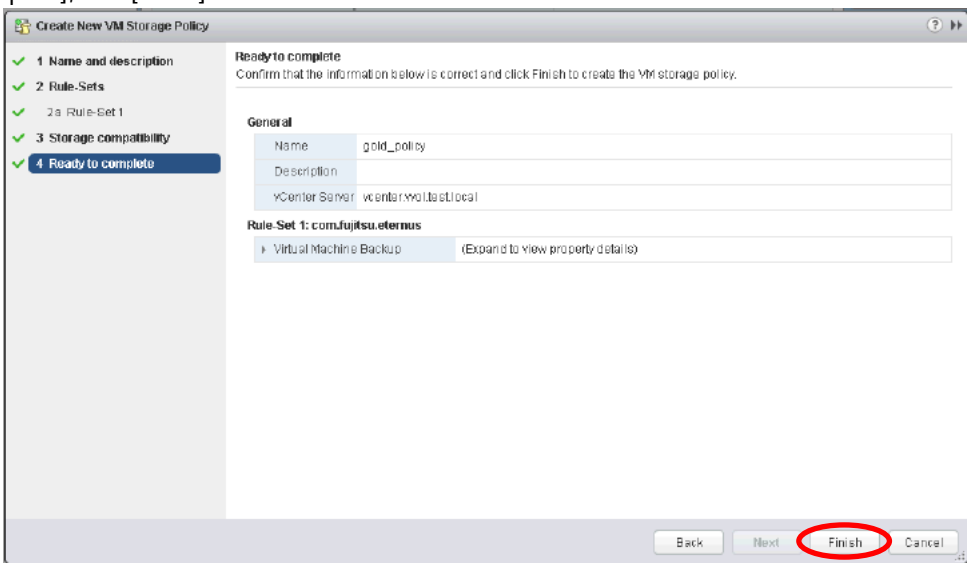

Figure-85 Ready to complete

7. Create a policy for silver.
   For each setting, enter the items shown in the following table.

Item	Information
Name	silver_policy
Operation Mode	Auto
Execution Period	Weekly
Execution Week	Sun.
Execution Start Time(Hour)	01
Execution Start Time(Minute)	00
Number of Snapshot Backup Generations	3
Quiesce guest file system	Enable
Snapshot the virtual machine's memory	Enable
Clone Backup	Enable

Table-36 Values for the virtual machine backup settings (silver)

2.2.3.2.5 Checking the Policies

Check that the virtual machine storage policies are registered correctly.

1. From Navigator, click [Home].

2. In [Home], click [VM Storage Policies] under [Monitoring].

3. Check that [VM Storage Policies] displays the created policies.

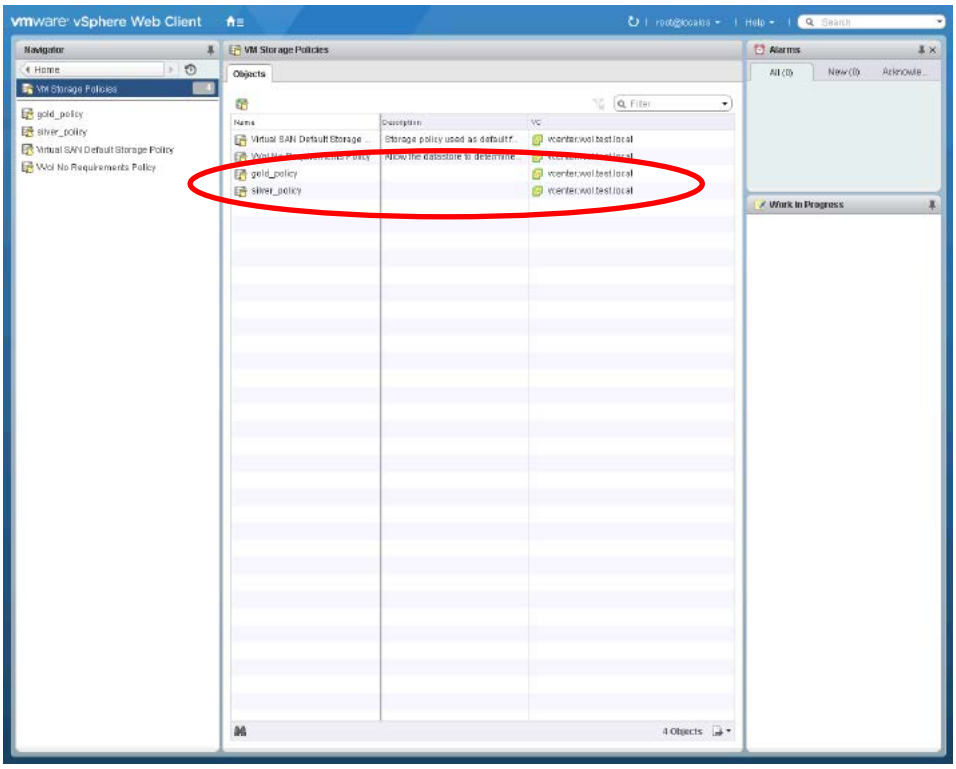

Figure-86 Checking the virtual machine storage policy of vCenter Server

Check that the VVOL datastores that were mounted on ESXi hosts in "2.2.3.2.2 Registering VVOL Datastores" are mounted on each ESXi host.

Name	Check ☑
gold_policy	□
silver_policy	□

Table-37 Checklist for the virtual machine storage policies

Check that the virtual machine storage policies are created, and then proceed to the next procedure.

2.2.4 Virtual Machine Creation Procedure

Create virtual machines to be used as business servers.
As an example, this procedure creates a virtual machine named "gyomu01".

1. Click [Actions] - [New Virtual Machine] - [New Virtual Machine].

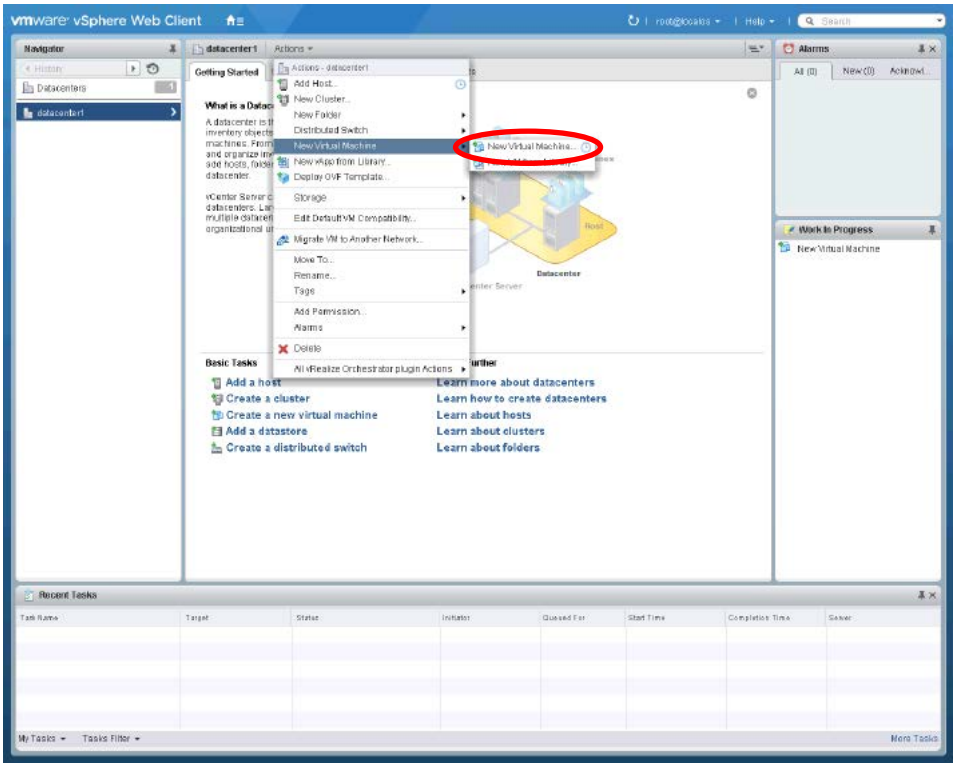

Figure-87 Creating a new virtual machine

2. In [Select a creation type], select [Create a new virtual machine], and then click [Next].

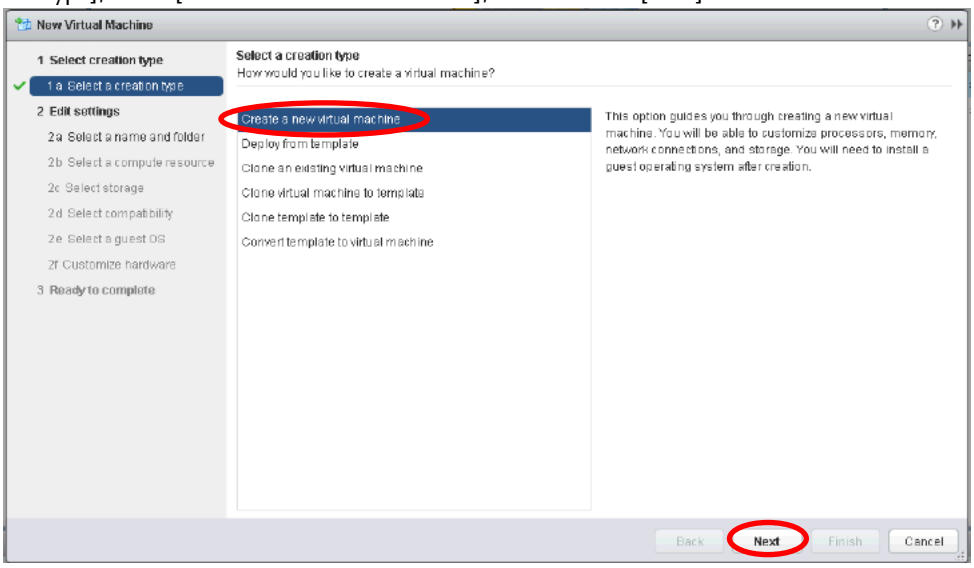

Figure-88 Select a creation type

3. In [Select a name and folder], type "gyomu01", and then click [Next].

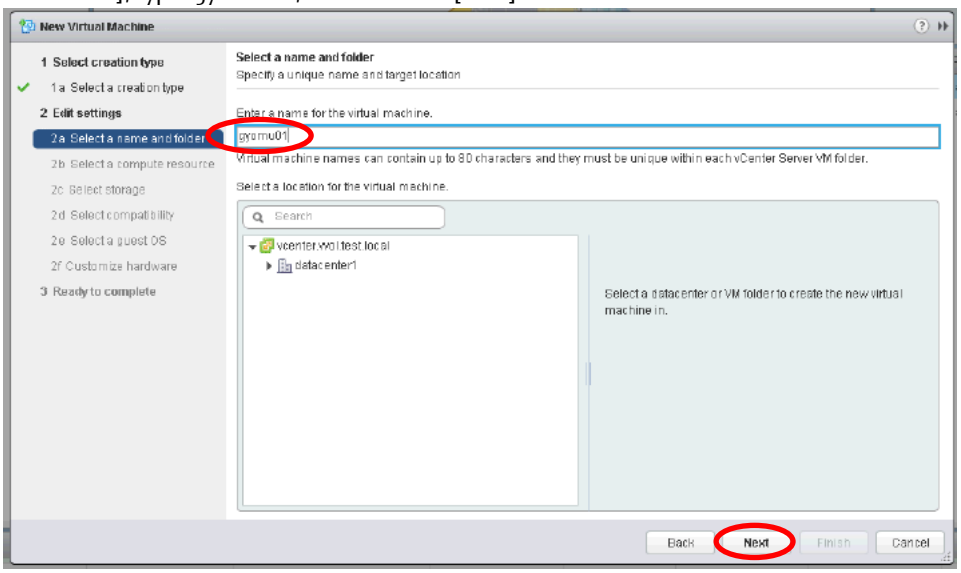

Figure-89 Select a name and folder

4. In [Select a compute resource], select a host, and then click [Next].

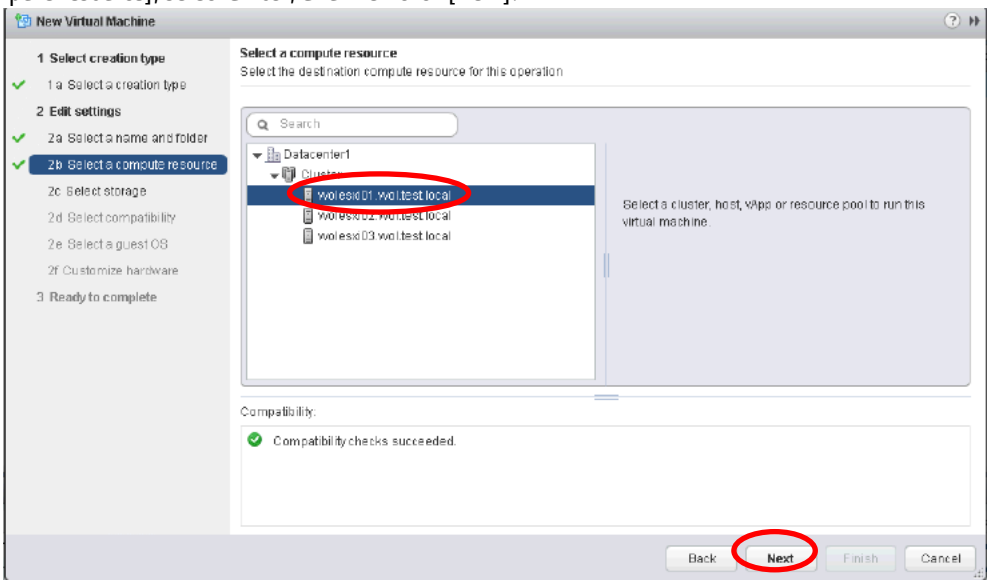

Figure-90 Select a compute resource

5. In [Select storage], select the values shown in the following table, and then click [Next].

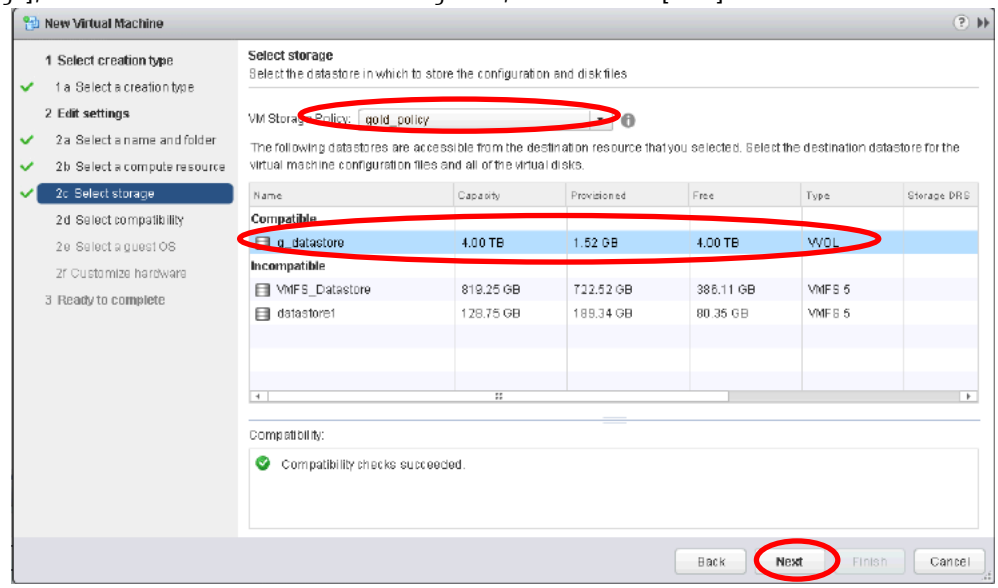

Figure-91 Select storage

Item	Information
VM Storage Policy	gold_policy
Datastore	g_datastore

Table-38 Values for the "Select storage" setting

6. In [Select compatibility], click [Next].

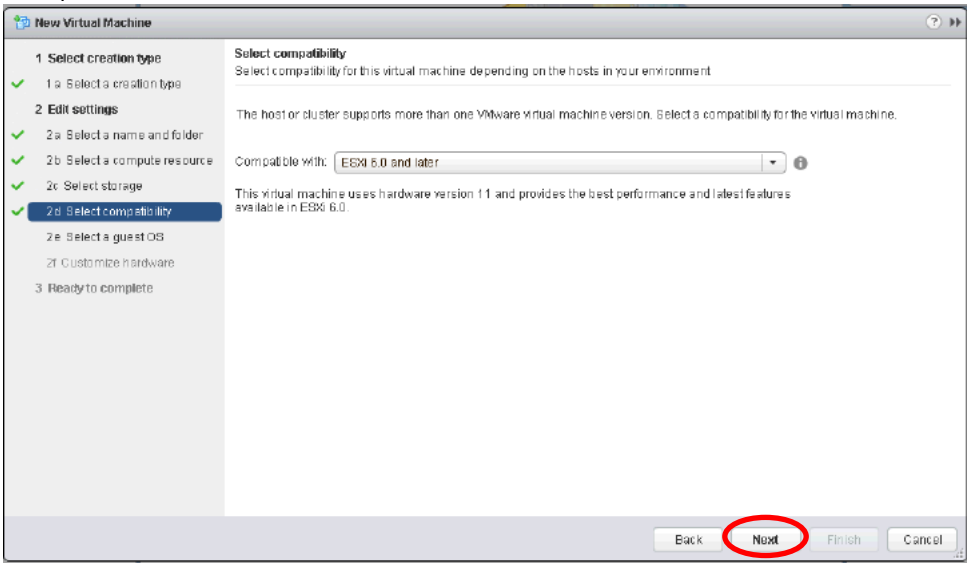

Figure-92 Select compatibility

7. In [Select a guest OS], enter the items shown in the following table, and then click [Next].

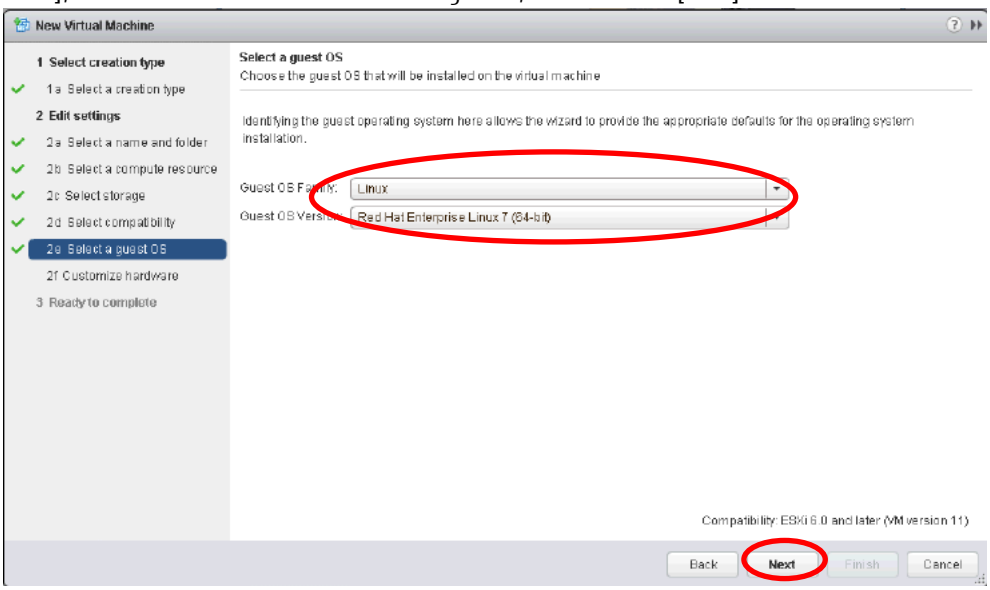

Figure-93 Select a guest OS

Item	Information
Guest OS Family	Linux
Guest OS Version	Red Hat Enterprise Linux 7 (64-bit)

Table-39 Values for the "Select a guest OS" setting

8. In [Customize hardware], enter the items shown in the following table, and then click [Next].

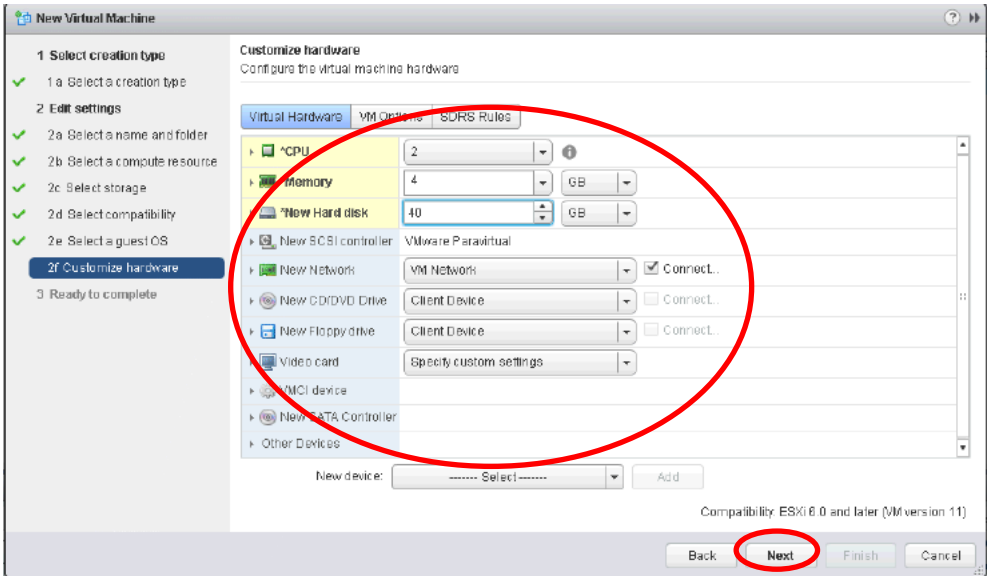

Figure-94 Customize hardware

Item	Information
CPU	2
Memory	4GB
New Hard disk	40GB (system area) 100GB (data area)

Table-40 Values for the "Customize hardware" setting

9. In [Ready to complete], click [Finish].
   When a virtual machine is powered on, it is automatically registered to the ETERNUS SF system.

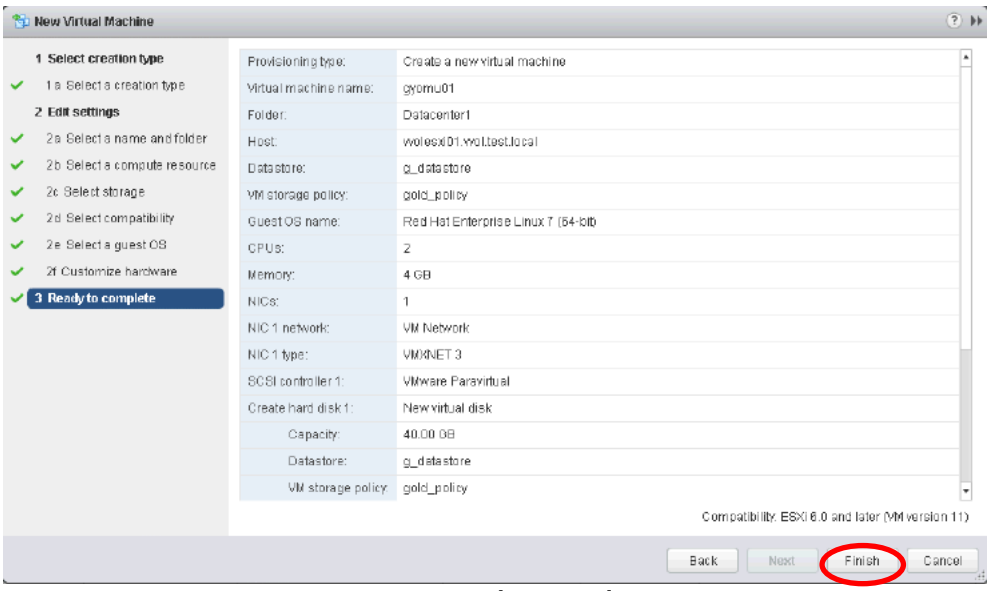

Figure-95 Ready to complete

10. Install and set up Windows Server 2012 R2.
    Create new virtual machines or clone the created virtual machine to prepare the required number of virtual machines.

Checklist

Confirm the following item.

- On vSphere Web Client, clicking [VMs and Templates] in [Home] displays the created virtual machines.

2.3 Operational Procedure

2.3.1 Virtual Machine Backup/Restore Procedure

- Backing up snapshots/clones

1. On the virtual machine, create a file for confirming that a backup/restore has been successfully executed.
   For the Command Line User Interface (CUI), perform the following steps.

```
# touch <file for confirmation>

Example
# touch /data/test1.txt
# touch /data/test2.txt
# ls -l /data
  :
-rw- r--r-- .1 root root 0 … test1.txt
-rw- r--r-- .1 root root 0 … test2.txt
```

The following screenshot is a display example of the GUI.

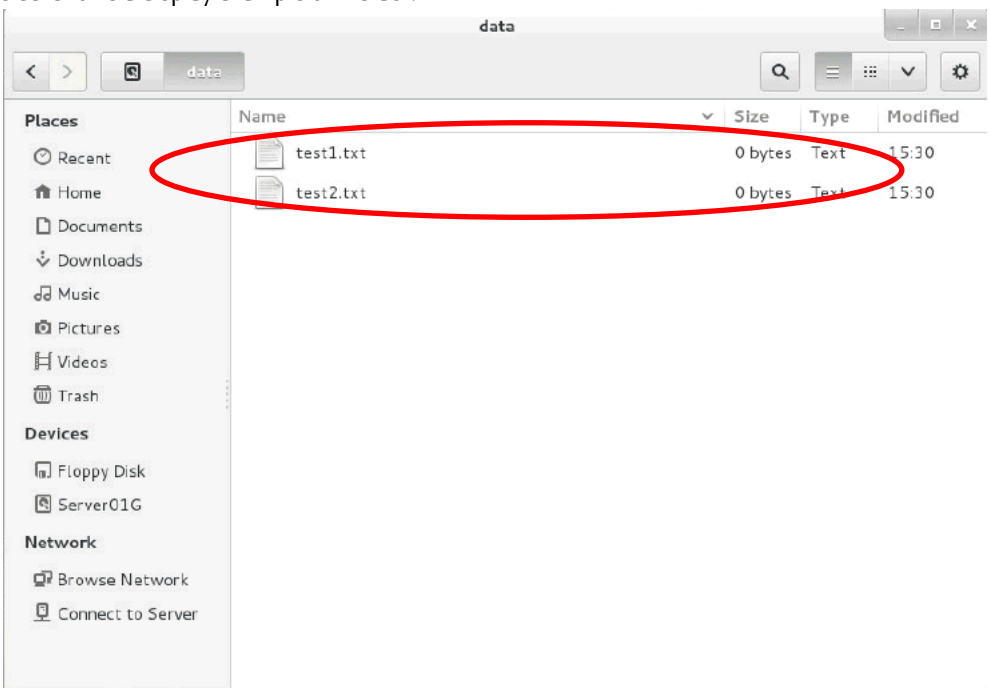

Figure-96 Creating files for confirmation

2. In the global navigation tab, click [Storage].
   On the Category pane, click [VVOL Management].

3. On the Category pane, click [VVOL Backup Management].

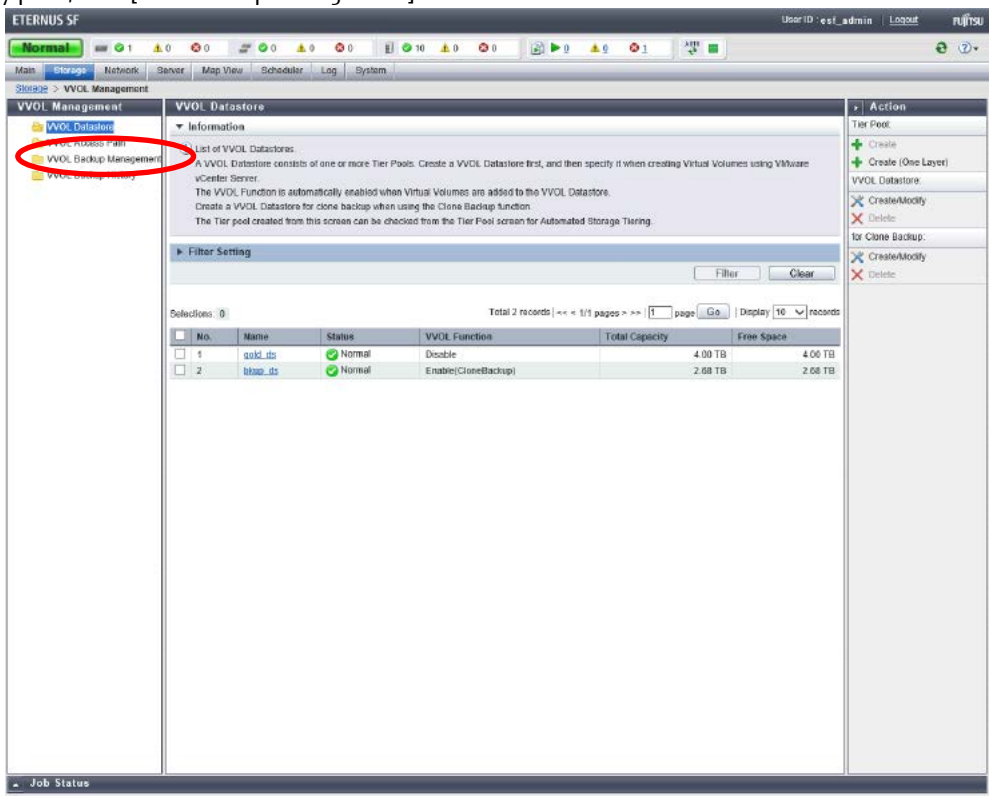

Figure-97 VVOL Management

4. On the Main pane, select a virtual machine to back up.
   On the Action pane, click [Execute] under [Manual Execution].

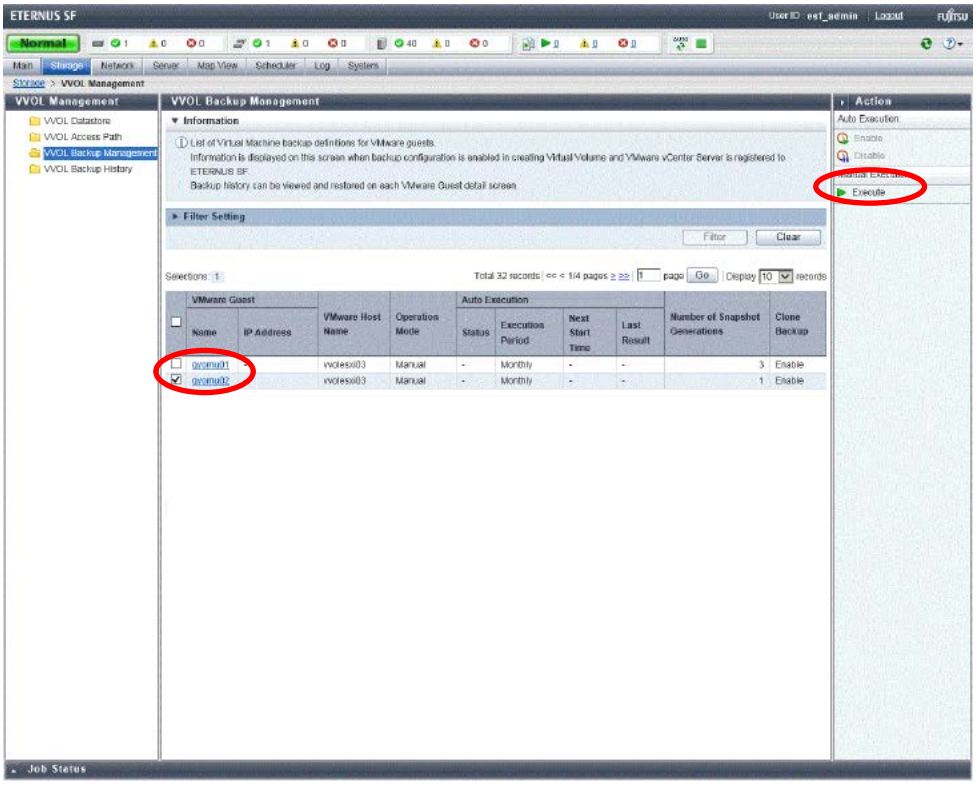

Figure-98 VVOL Backup Management

5. The warning dialog box is displayed. Confirm that the backup operation will not cause a problem, and then click [OK].

6. A message is displayed to inform that the process has been accepted. Click the [Done] button.

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next procedure.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

Checklist

Confirm the following items.

- On the Main pane of the [VVOL Backup History] screen, the snapshot backup history list displays the snapshot backups.
- On the Main pane of the [VVOL Backup History] screen, clicking the [Clone Backup History] tab displays the clone backups in the clone backup history list.

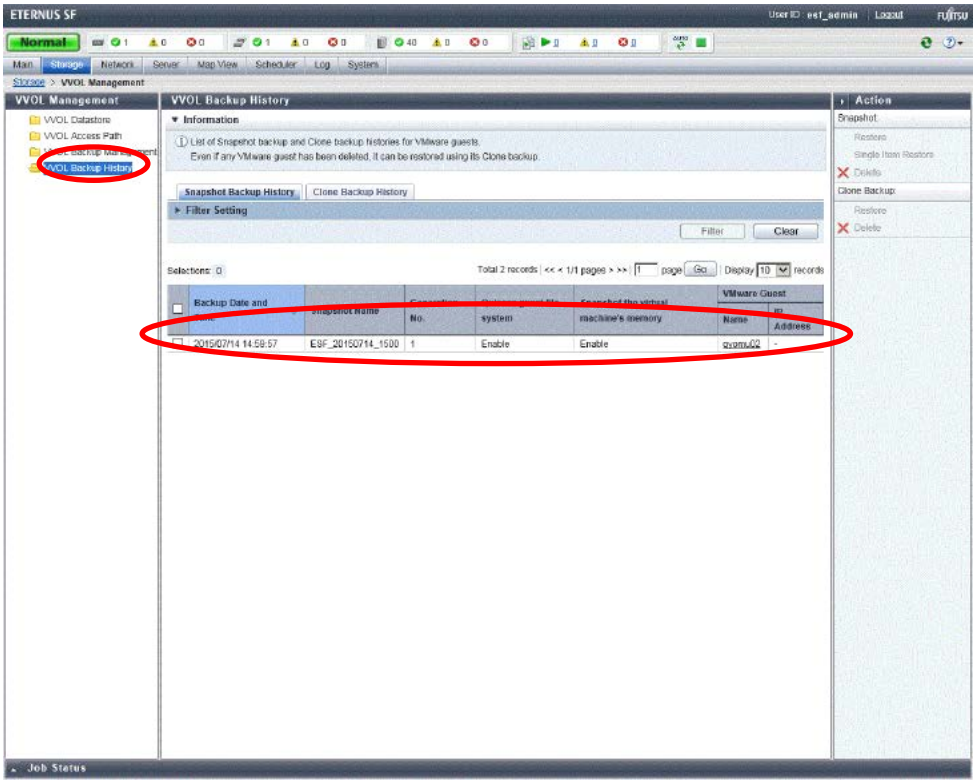

Figure-99 Snapshot Backup History

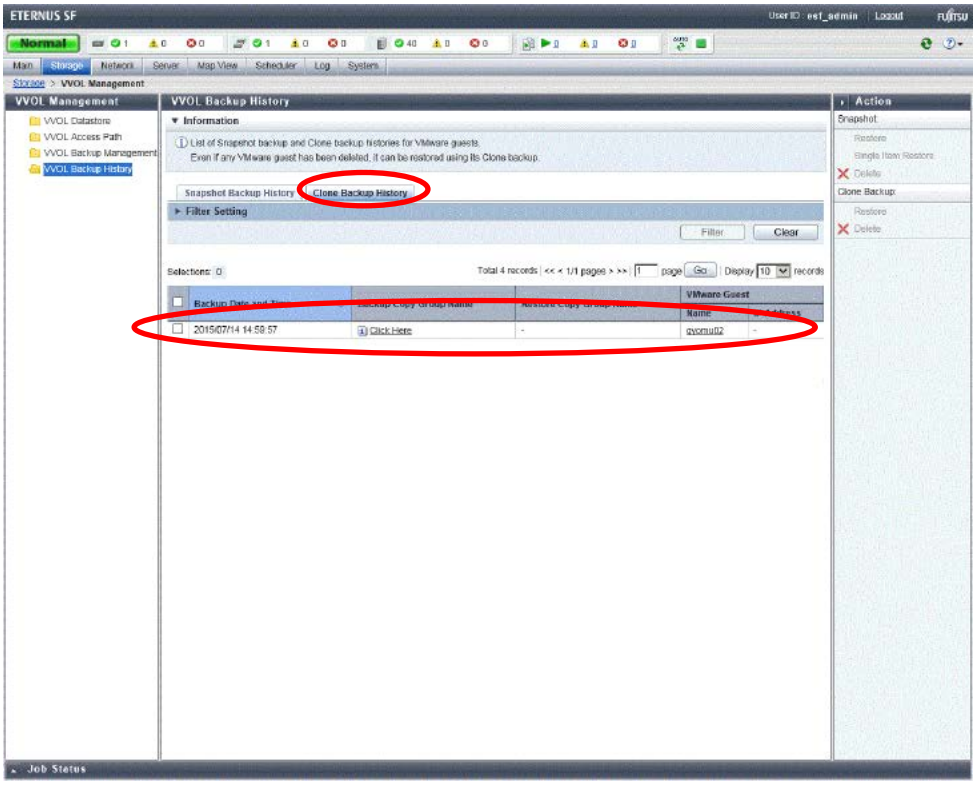

Figure-100 Clone Backup History

■ Restoring snapshots

1. On the virtual machine, delete the file created for confirmation in Step 1 of the "Backing Up Snapshots/Clones" procedure.
   For the CUI, perform the following steps.

```
# rm -f <file for confirmation>

Example
# rm -f /data/test2.txt
# ls -l /data
  :
-rw- r--r-- .1 root root 0 … test1.txt
```

The following screenshot is a display example of the GUI.

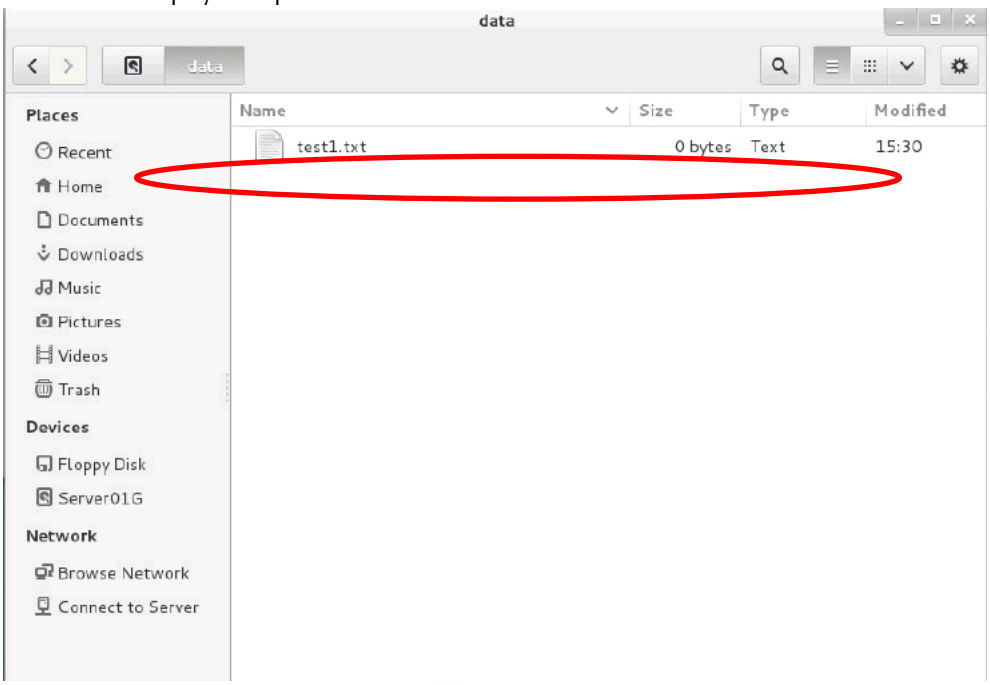

Figure-101 Deleting the file for confirmation

2. In the global navigation tab, click [Storage].
   On the Category pane, click [VVOL Management]. This changes the items of the Category pane to items related to VVOL management.

3. On the Category pane, click [VVOL Backup History].
   Select a snapshot backup to restore, and then click [Restore] under [Snapshot] on the Action pane.

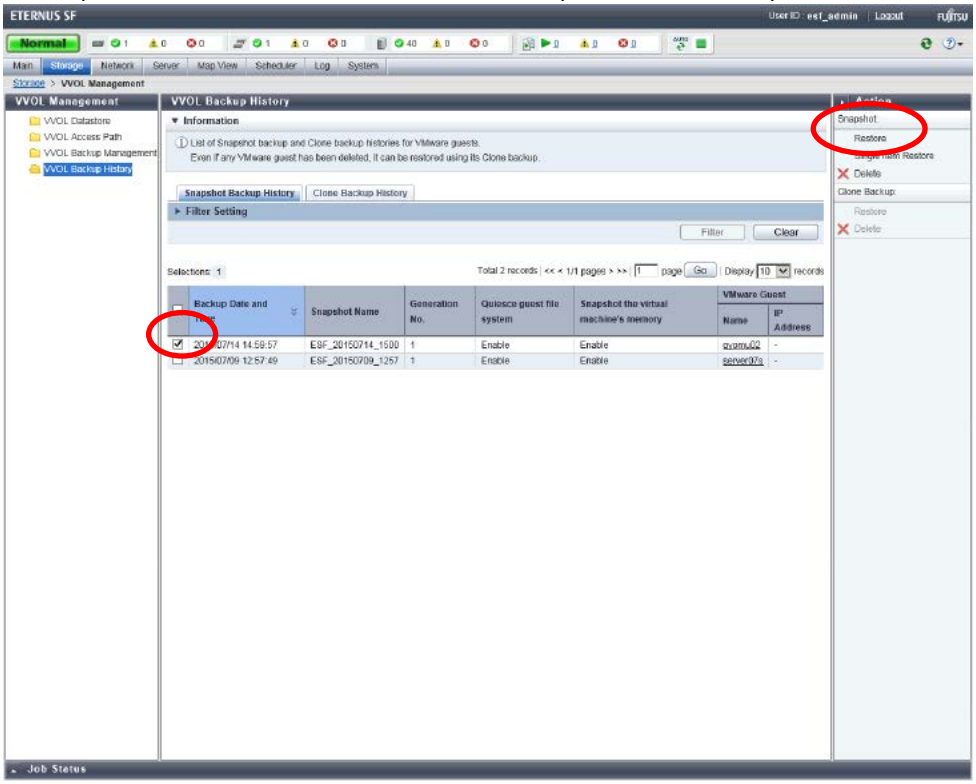

Figure-102 Snapshot Backup History

4. The warning dialog box is displayed. Confirm that the backup operation will not cause a problem, and then click [OK].

5. A message is displayed to inform that the process has been accepted. Click the [Done] button.

   Points
   Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next step.
   For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

6. Check that the file for confirmation that was deleted on the virtual machine is restored.
   For the CUI, perform the following step.

```
# ls -l <directory of the files for confirmation>

Example
# ls -l /data
  :
-rw- r—r-- .1 root root 0 … test1.txt
-rw- r—r-- .1 root root 0 … test2.txt
```

The following screenshot is a display example of the GUI.

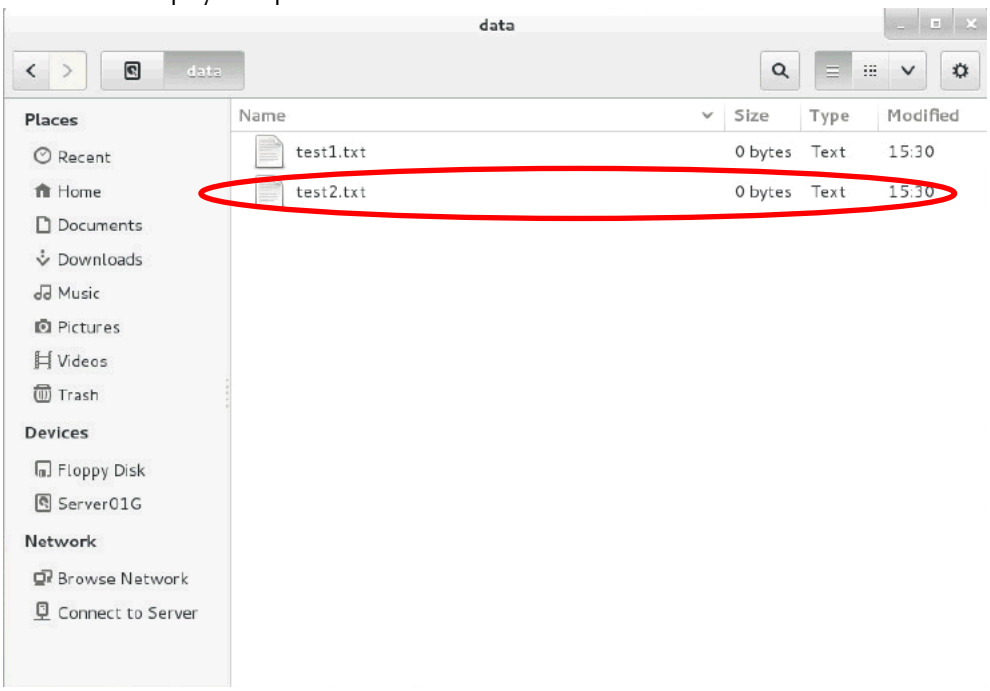

Figure-103 Restoring the file for confirmation

■ Restoring clone backups

1. On the virtual machine, delete the file created for confirmation in Step 1 of the "Backing Up Snapshots/Clones" procedure.
   For the CUI, perform the following steps.

```
# rm -f <file for confirmation>

Example
# rm -f /data/test2.txt
# ls -l /data
  :
-rw- r--r-- .1 root root 0 … test1.txt
```

The following screenshot is a display example of the GUI.

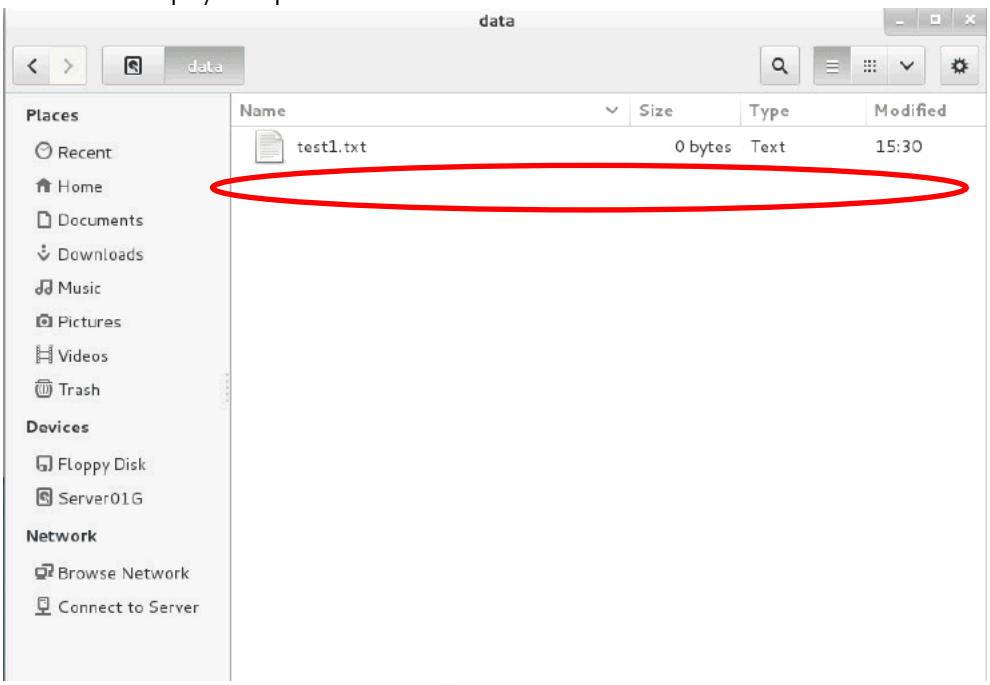

Figure-104 Deleting the file for confirmation

2. Shut down the virtual machine and then on vCenter Web Client, make sure that the virtual machine to be restored is powered off.

3. In the global navigation tab, click [Storage]. Then, on the Category pane, click [VVOL Management].

4. On the Category pane, click [VVOL Backup Management]. Then, on the Main pane, click the [Clone Backup History] tab.

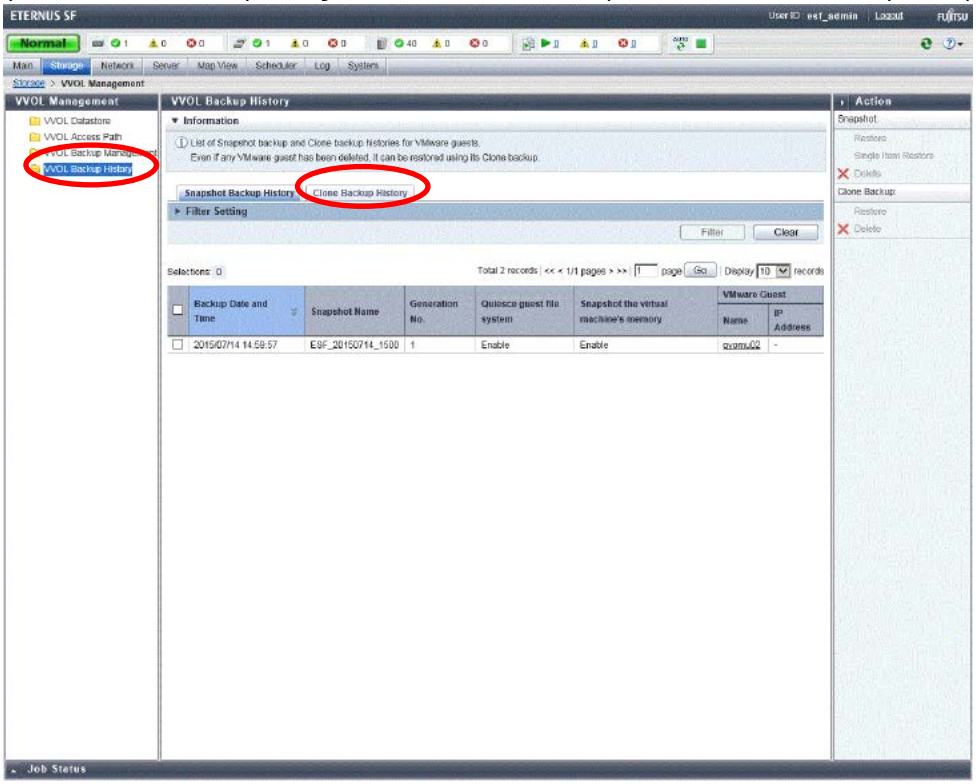

Figure-105 VVOL Backup Management

5. In [Clone Backup History], select a clone backup to restore.
Then, on the Action pane, click [Restore] under [Clone Backup].

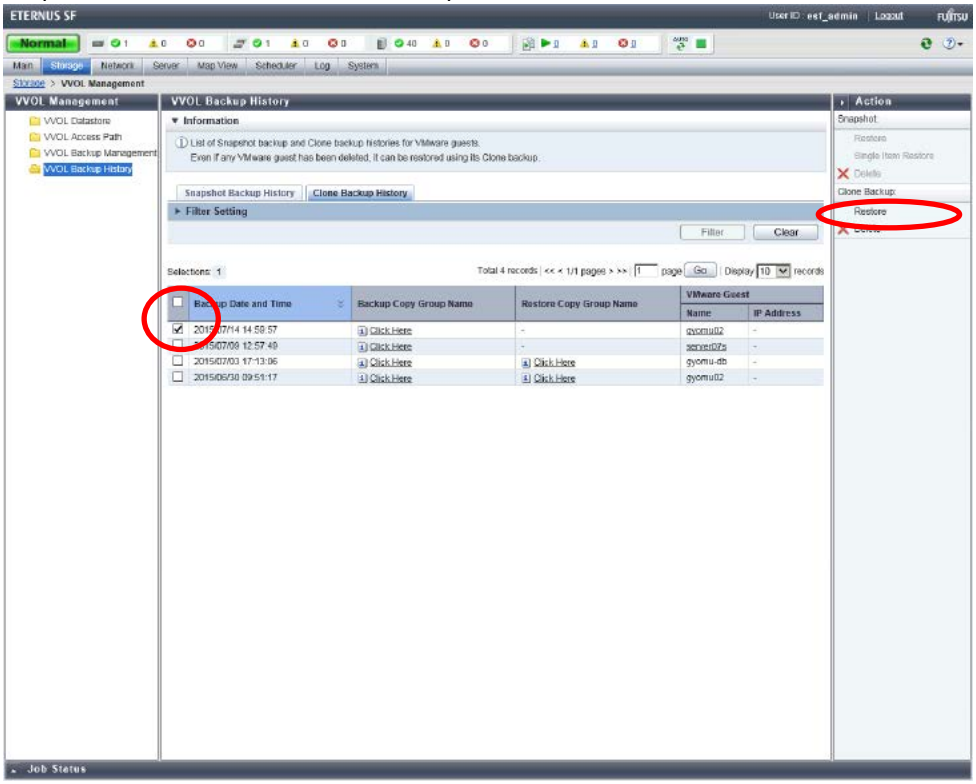

Figure-106 Clone Backup History

6. Enter the VMware guest name for the restore destination, and then click the [Restore] button.

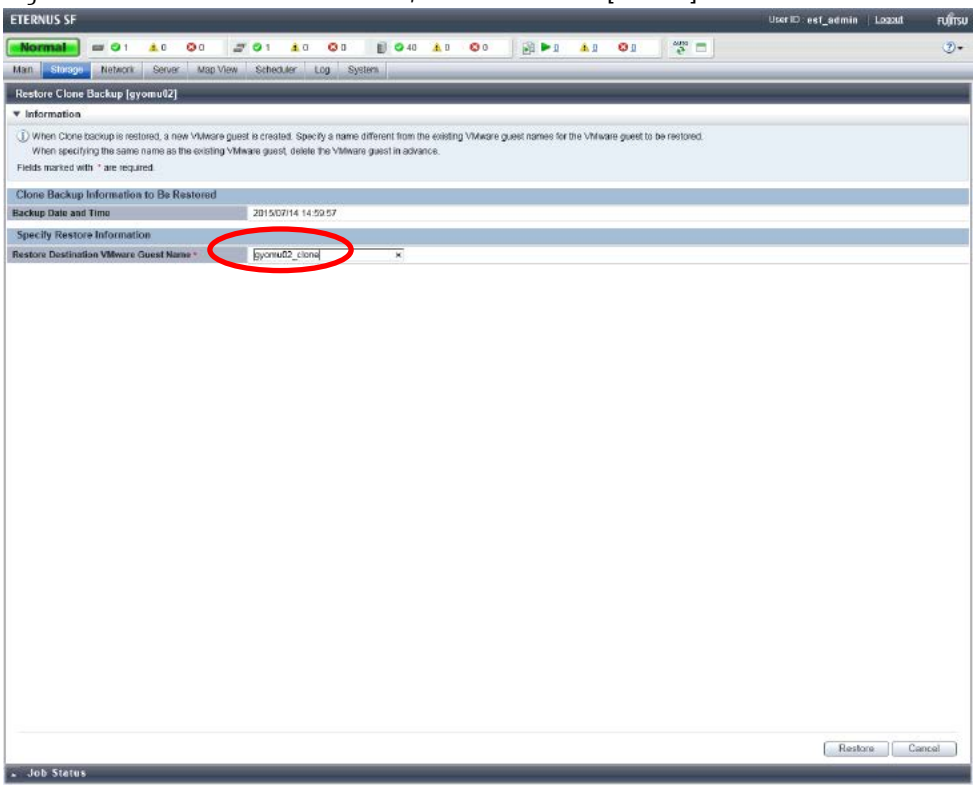

Figure-107 Restore Clone Backup

7. A message is displayed to inform that the process has been accepted. Click the [Done] button.

Points

Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next step.
For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

8. On vCenter Web Client, check the restored virtual machine.

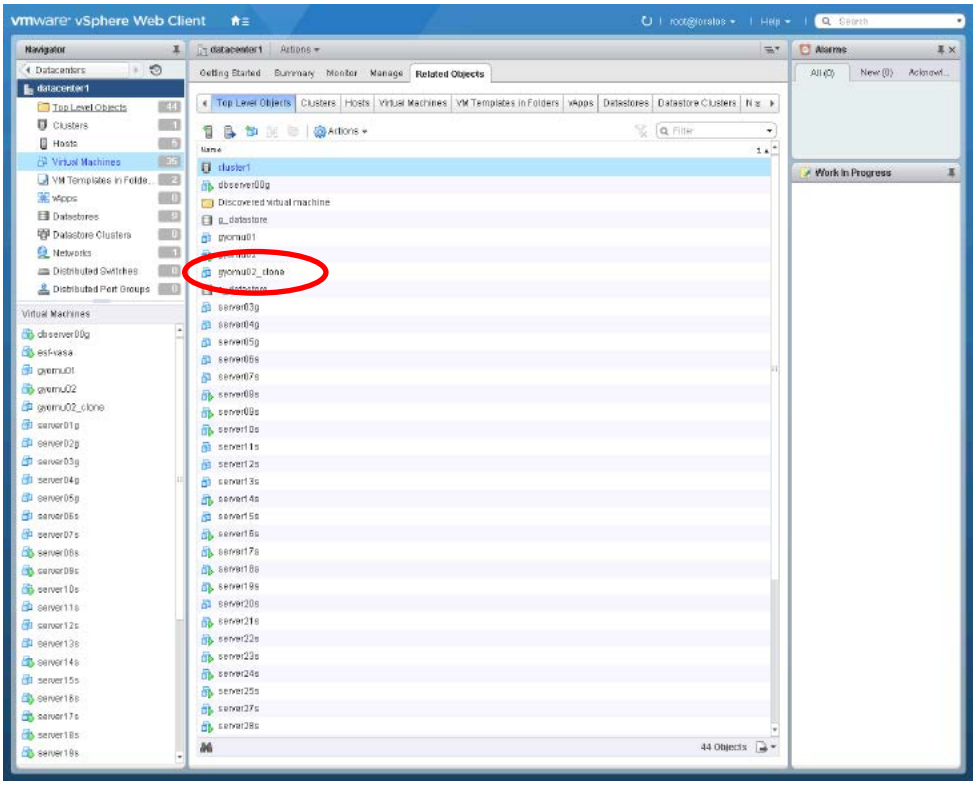

Figure-108 Checking the restored virtual machine

9. Check that the file for confirmation that was deleted on the virtual machine is restored.
   For the CUI, perform the following step.

```
# ls -l <directory of the files for confirmation>

Example
# ls -l /data
:
-rw- r--r-- .1 root root 0 … test1.txt
-rw- r--r-- .1 root root 0 … test2.txt
```

The following screenshot is a display example of the GUI.

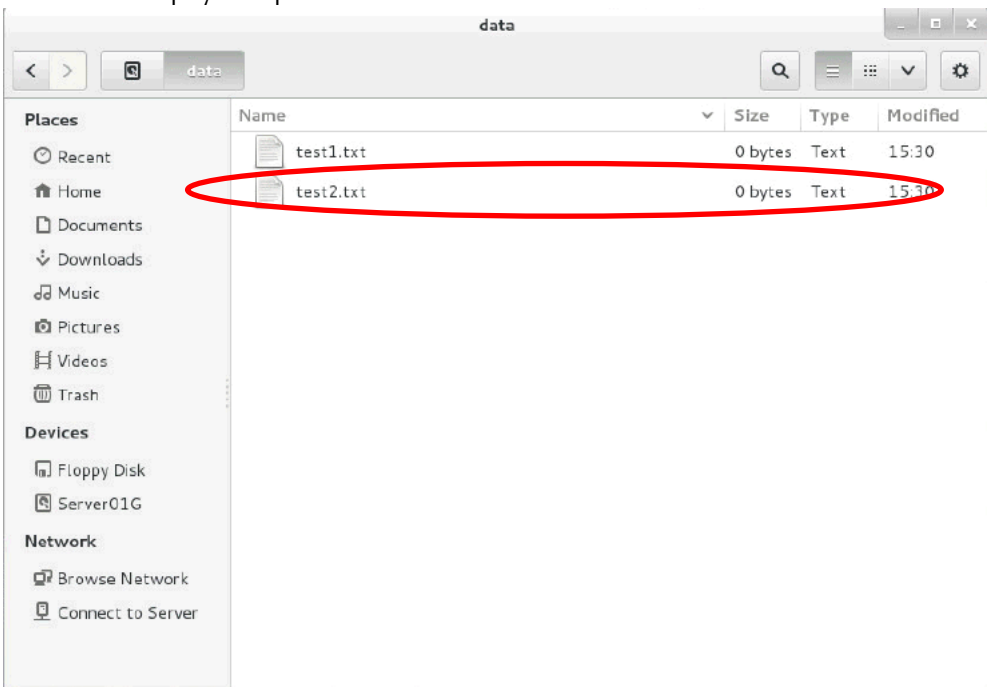

Figure-109 Restoring the file for confirmation

■ Restoring a single item

This section provides the procedure for restoring files that were created in the virtual disk of the data area.
This procedure was performed using Red Hat Enterprise Linux 7.

1. On the virtual machine, delete the file created for confirmation in Step 1 of the "Backing Up Snapshots/Clones" procedure.
   For the CUI, perform the following steps.

```
# rm -f <file for confirmation>

Example
# rm -f /data/test2.txt
# ls -l /data
  :
-rw- r—r-- .1 root root 0 … test1.txt
```

The following screenshot is a display example of the GUI.

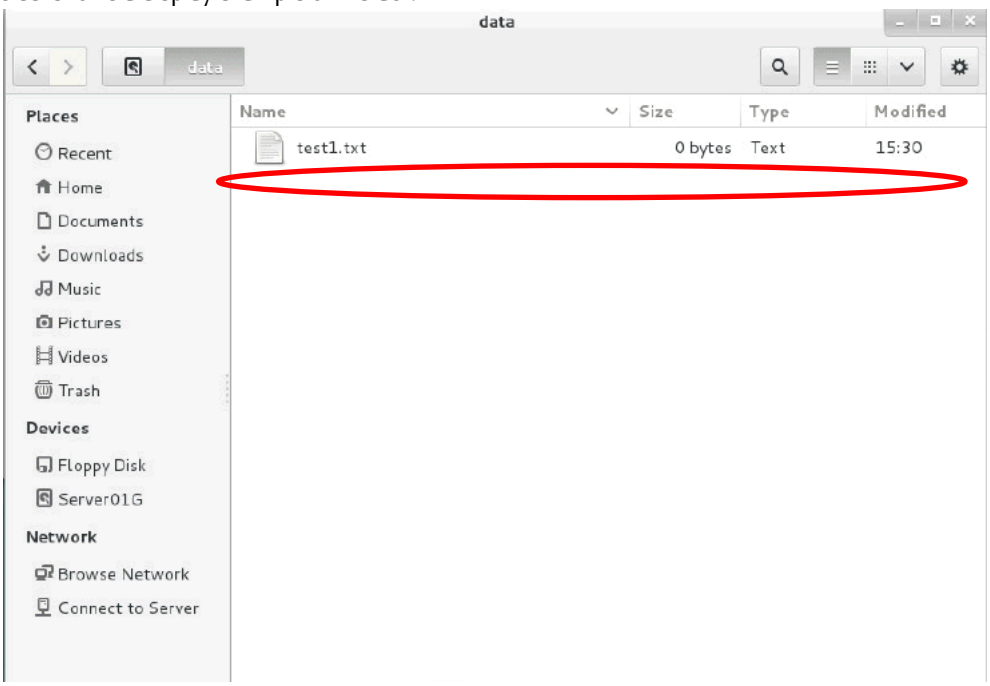

Figure-110 Deleting the file for confirmation

2. In the global navigation tab, click [Storage].
   On the Category pane, click [VVOL Management].

3. On the Category pane, click [VVOL Backup Management].
   Select a snapshot backup to restore, and then click [Single Item Restore] under [Snapshot] on the Action pane.

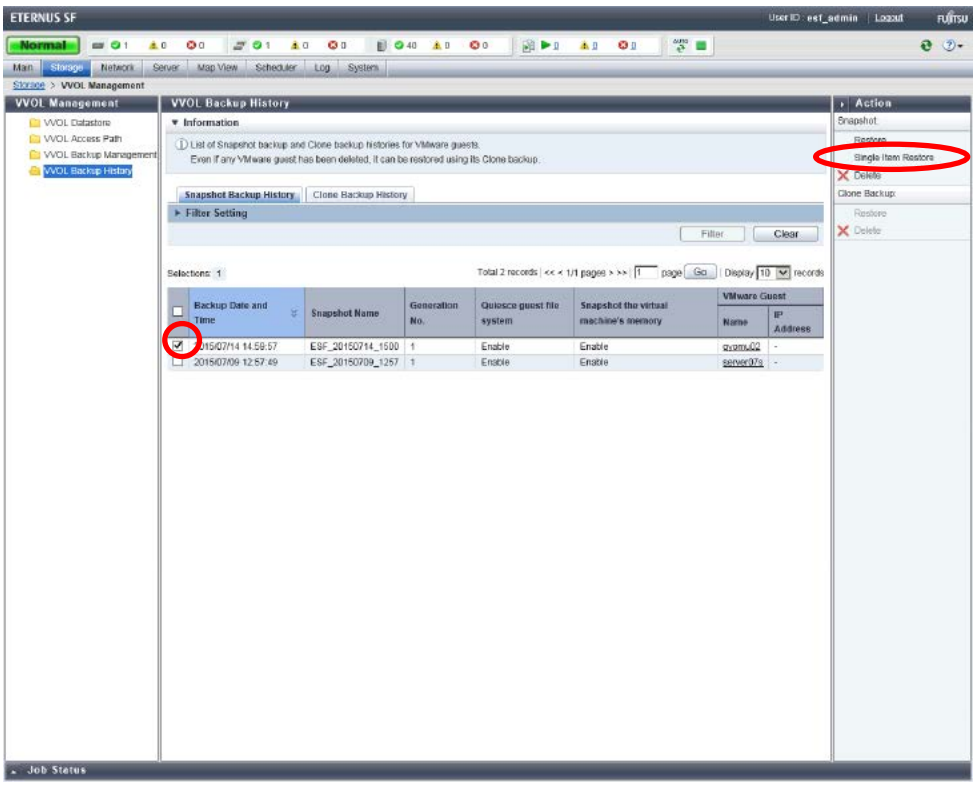

Figure-111 Snapshot Backup History

4. Set [Allocation duration of temporary volume] to 24 and in the VMDK file list, select the VMDK file to restore. Then, click the [Restore] button.

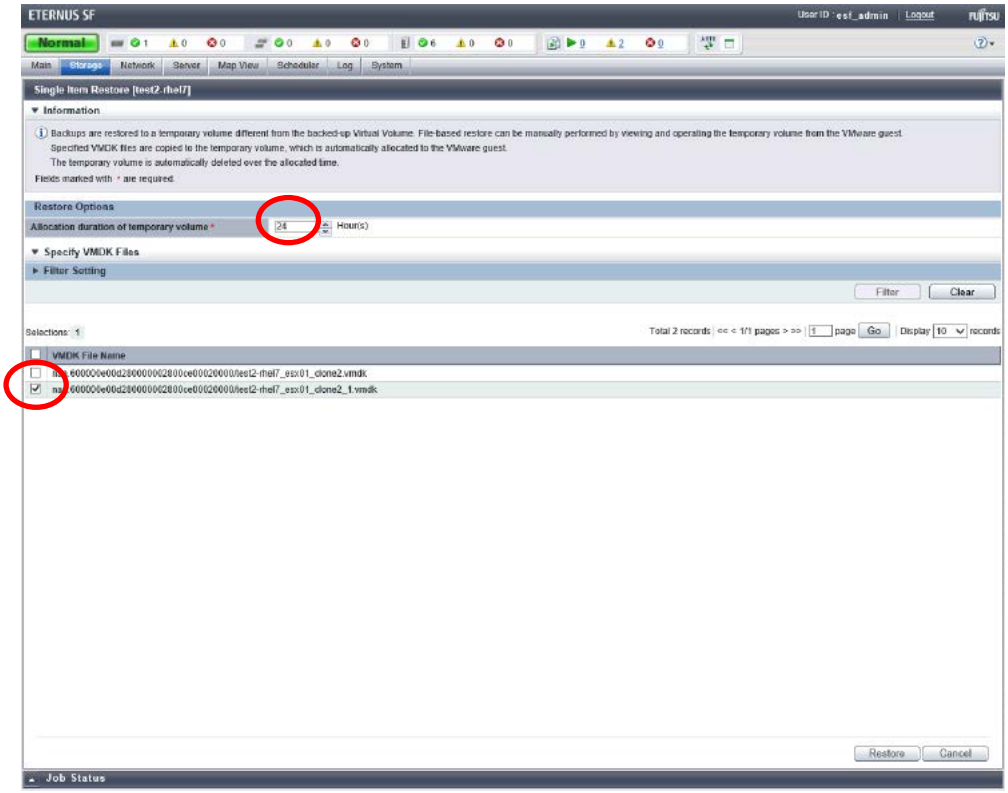

Figure-112 Restore

5. A message is displayed to inform that the process has been accepted. Click the [Done] button.

   Points
   Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next step.

6. In the virtual machine, rescan the disk and partition.
   For the CUI, perform the following step.

```
# sfdisk –R <device name of the temporary volume (/dev/sd*)>

Example
# sfdisk –R dev/sdc
```

7. Mount the temporary volume on the virtual machine.
   For the CUI, perform the following steps.
   For a single item restore, a disk is automatically added to the virtual machine.
   Therefore, when a compatible device is used and the system is rebooted while the temporary volume exists, a device name mismatch may occur.
   Using a device name that does not change is recommended. In this document, UUID is used.

```
# udevadm info -q symlink -n <compatible device name>
<by-path name> <by-uuid name>

# mount <by-uuid name of the temporary volume> <mount point>

Example
# udevadm info -q symlink -n /dev/sdc1
disk/by-path/pci-0000: … disk/by-uuid/8454c293…

# mount /dev/disk/by-uuid/8454c293…. /mnt
```

   For the GUI, perform the following steps.
   Select [Applications] - [Utilities] - [Disks].

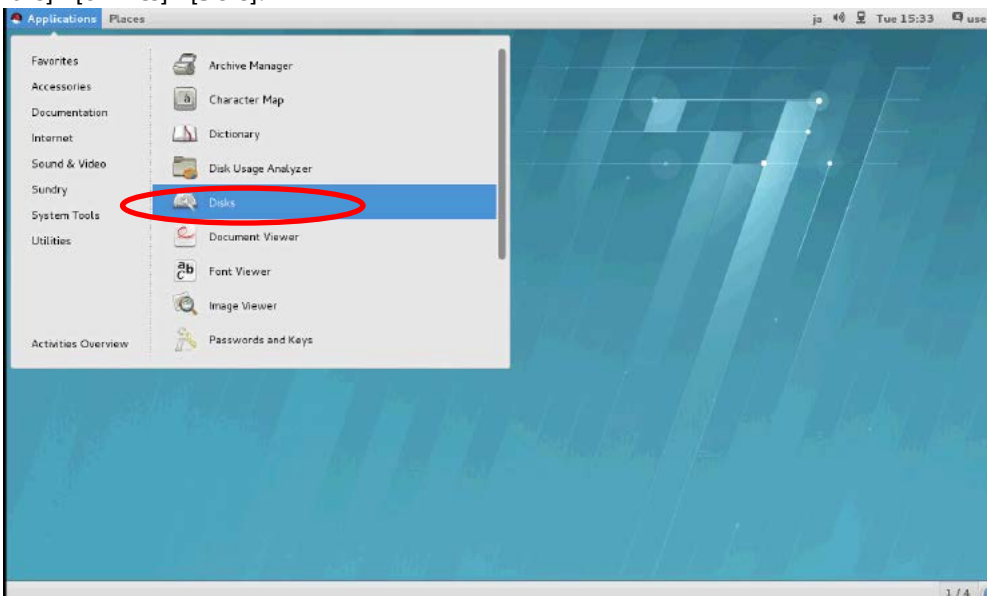

Figure-113 Desktop

Select the temporary volume from [Devices] and click the mount button.
The temporary volume is mounted in "/mnt/<UUID>" by default.

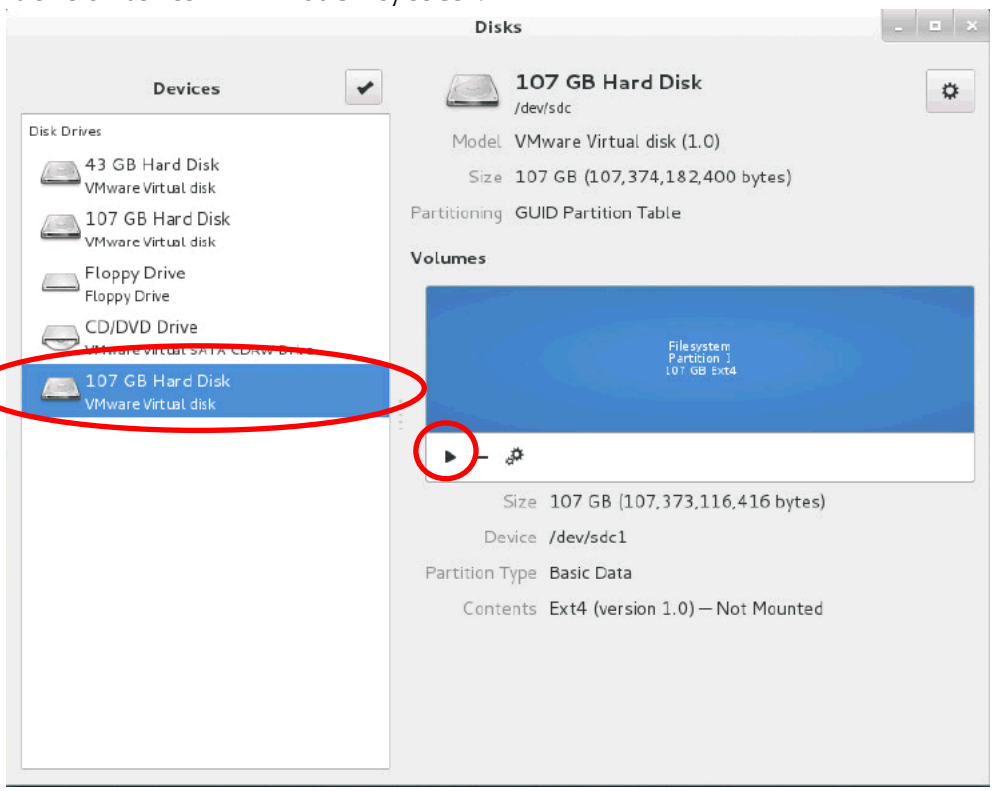

Figure-114 Disks

8. Check the mounted temporary volume.
   For the CUI, perform the following step.

```
# ls -l <directory of the temporary volume>

Example
# ls -l /mnt
:
-rw- r—r-- .1 root root 0 … test1.txt
-rw- r—r-- .1 root root 0 … test2.txt
```

The following screenshot is a display example of the GUI.

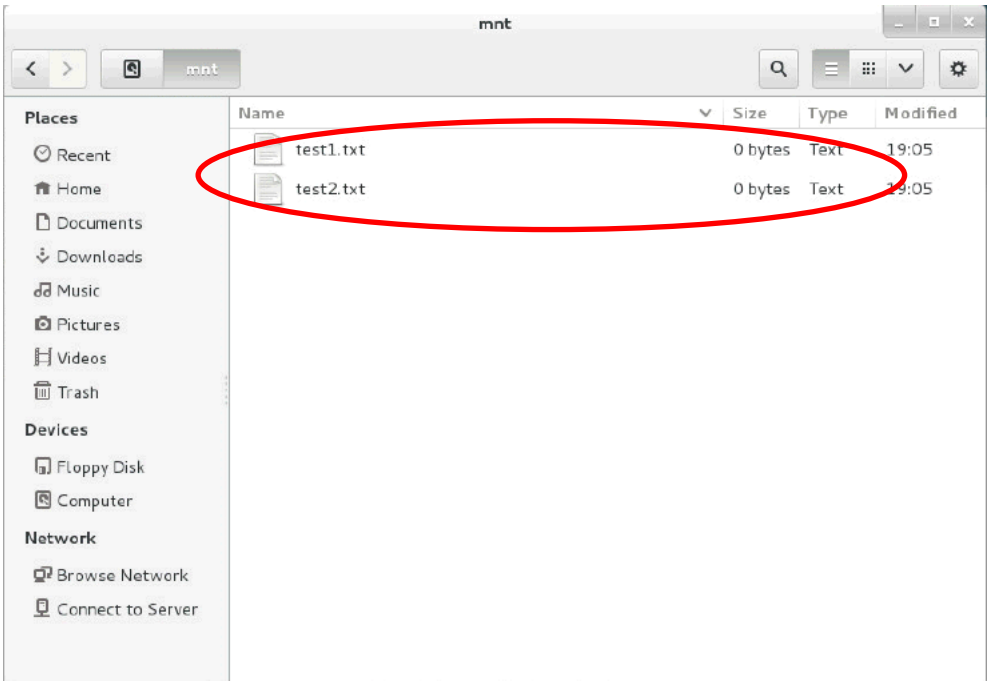

Figure-115 Checking the temporary volume

9. Copy the file from the temporary volume to the restore destination.
   For the CUI, perform the following step.

```
# cp -p <target file to restore> <restore destination>

Example
# cp -p /mnt/test2.txt /data
```

The following screenshot is a display example of the GUI.

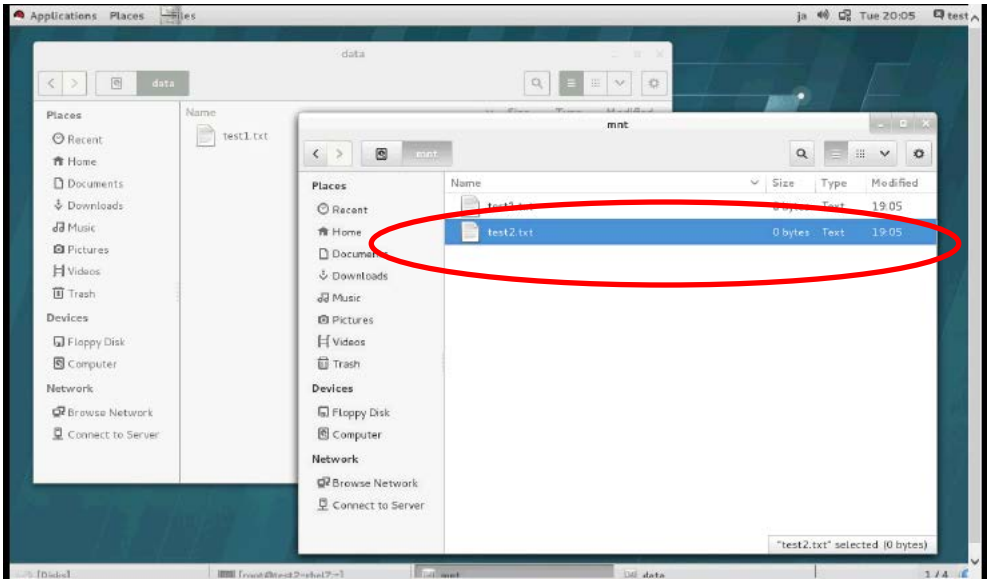

Figure-116 Copying the file

10. Check that the restore is successfully completed.
    For the CUI, perform the following step.

```
# ls -l <directory of the files for confirmation>

Example
# ls -l /data
:
-rw- r--r-- .1 root root 0 … test1.txt
-rw- r--r-- .1 root root 0 … test2.txt
```

The following screenshot is a display example of the GUI.

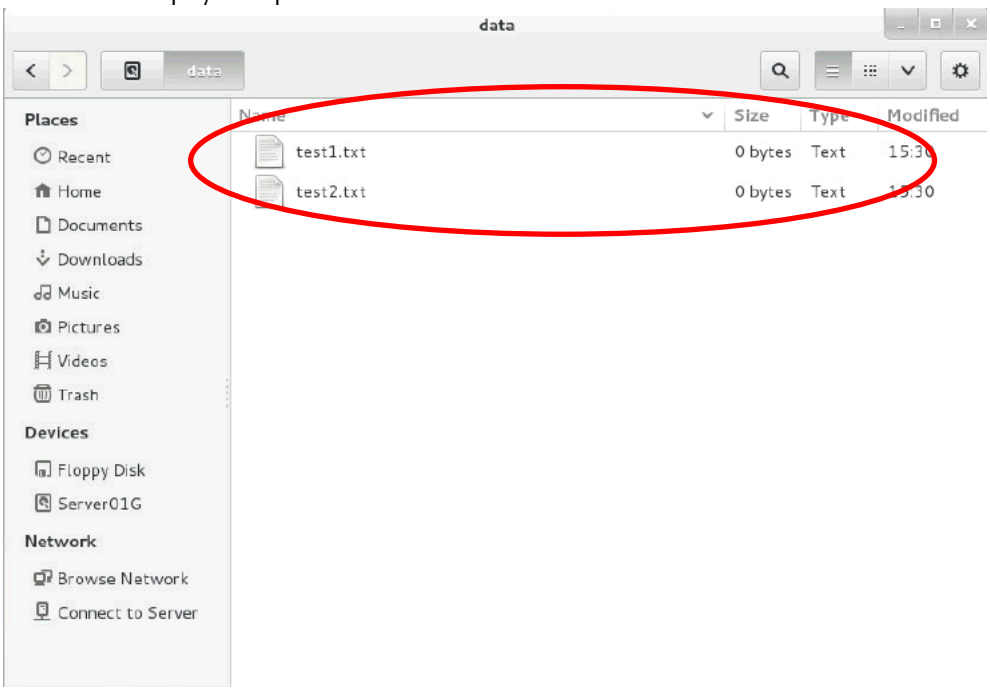

Figure-117 Checking the restored file

11. Unmount the temporary volume.
    For the CUI, perform the following step.

```
# umount <mount point of the temporary volume>

Example
# umount /mnt
```

For the GUI, perform the following steps.
Select [Applications] - [Utilities] - [Disks].

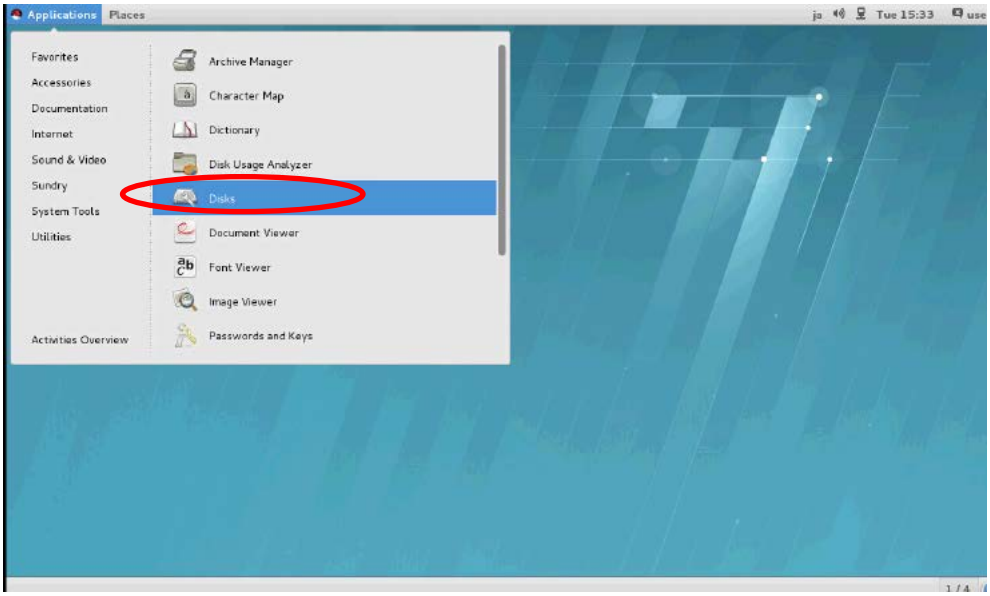

Figure-118 Desktop

Select the temporary volume from [Devices] and click the unmount button.

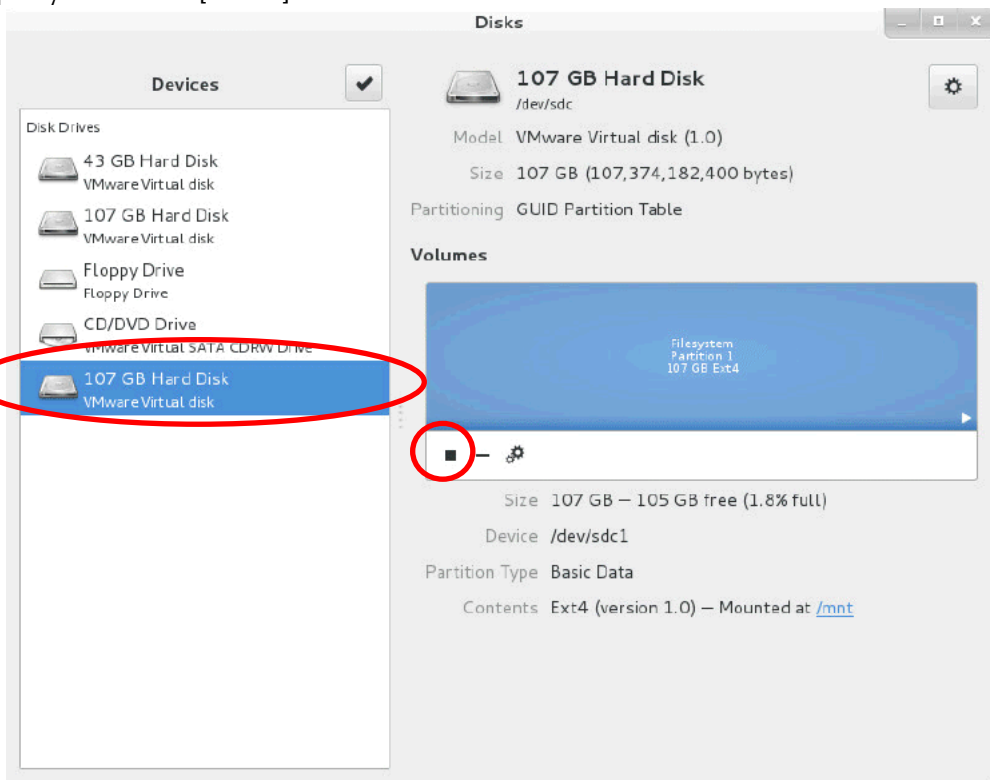

Figure-119 Disks

12. Delete the temporary volume.
    In the global navigation tab, click [Scheduler].
    On the Main pane, select a task. Then, on the Action pane, click [Execute immediately] under [Operation].

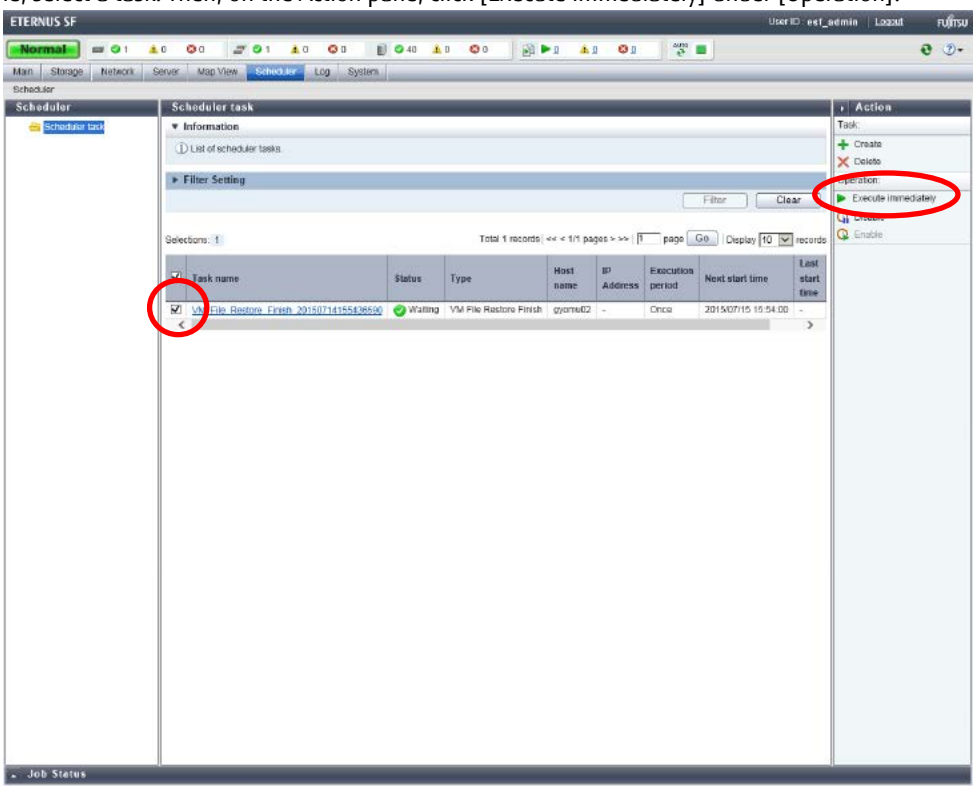

Figure-120 Scheduler task

13. Check the operation to be executed, and then click the [Execute] button.

14. In the message notifying the immediate execution of the scheduler task, click the [Done] button.

    Points
    Check the Job Status pane and make sure that the result changes to [Success] before proceeding to the next procedure.
    For details on how to use the Job Status pane, refer to "2.2.1.2 Checking the Common Processes of the ETERNUS SF Web Console Operations".

Checklist

Confirm the following items.

- On the Main pane of the [Scheduler] screen, no scheduler tasks are displayed.
- The temporary volume is unmounted.

3 Verification of the VVOL Reference Architecture

A test was performed for environments configured using this reference architecture to determine whether they were able to secure the capacity for the virtual machines and support the operations of the various functions.

3.1 Confirming the Normal Operation of the Virtual Machines

A test was performed to check if the capacity required to run 15 business systems that operate as virtual machines and two management servers can be secured when two ESXi hosts are used.

Server type	No. of units	Software	CPU	Memory	Disk	Snapshot backups	Clone backups
vCenter server	1	VMware vCenter Server Appliance 6.0	2vCPU	8GB	120GB	–	–
Operation management server	1	Windows Server 2012 R2	4vCPU	5GB	50GB	–	–
Business server with the Gold policy	5	Red Hat Enterprise Linux 7	2vCPU	4GB	140GB	Without	With
Business server with the Silver policy	10					With	With

3.2 Confirming the Operation of VMware vSphere 6.0

VMware vSphere 6.0 was confirmed to operate without any problems in this configuration by checking the following items.

- Storage vMotion operations between VVOL and VMFS

  Migrating virtual machines between different datastores formats, VVOL (volume) datastore and VMFS (file system) datastore, was tested. The following operations were tested and confirmed that Storage vMotion was executable between a VVOL datastore and a VMFS datastore.

  Powered-off virtual machines: Cold migration from a VVOL datastore to a VMFS datastore*
  Cold migration from a VMFS datastore to a VVOL datastore*
  Powered-on virtual machines: Storage vMotion from a VVOL datastore to a VMFS datastore*
  Storage vMotion from a VMFS datastore to a VVOL datastore*

  * A "Datastore does not match current VM policy" message is displayed while migration is performed.

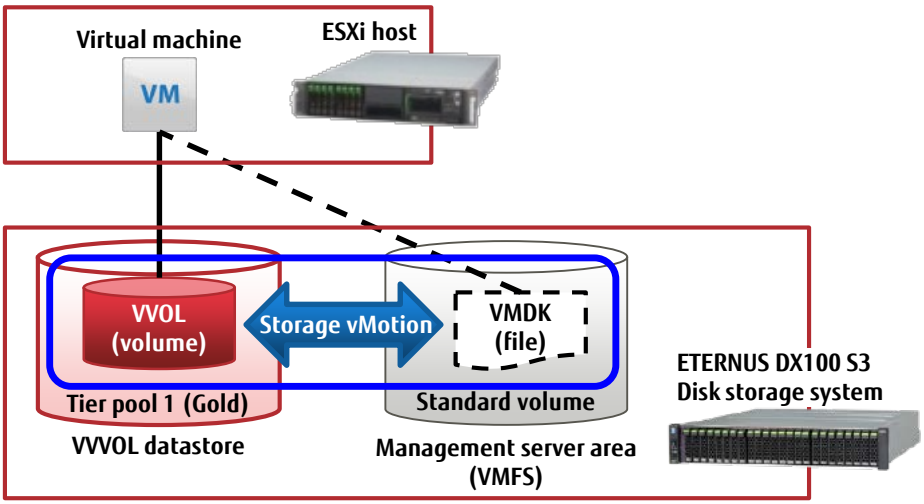

Figure-121 Confirmation of Storage vMotion

- Failover for the operation management server due to vSphere HA
  The availability of redundancy provided by vSphere HA was tested for situations where an operation management server and a business server were installed on the same ESXi host.
  An operation management server is necessary for virtual machine operations that use VVOLs. This is why an operation management server was placed on the VMFS.
  These virtual machines were tested to determine whether they were started in different ESXi hosts when a failover was performed for the ESXi host that has business servers that are in a VVOL and an operation management server.
  The following items were tested and confirmed that vSphere HA was valid even in VVOL environments.
  - Whether a different ESXi host can start these virtual machines after a failover is performed for an ESXi host that runs a business server
  - Whether a different ESXi host can start these virtual machines after a failover is performed for an ESXi host that runs the operation management server, the vCenter server, and a business server.

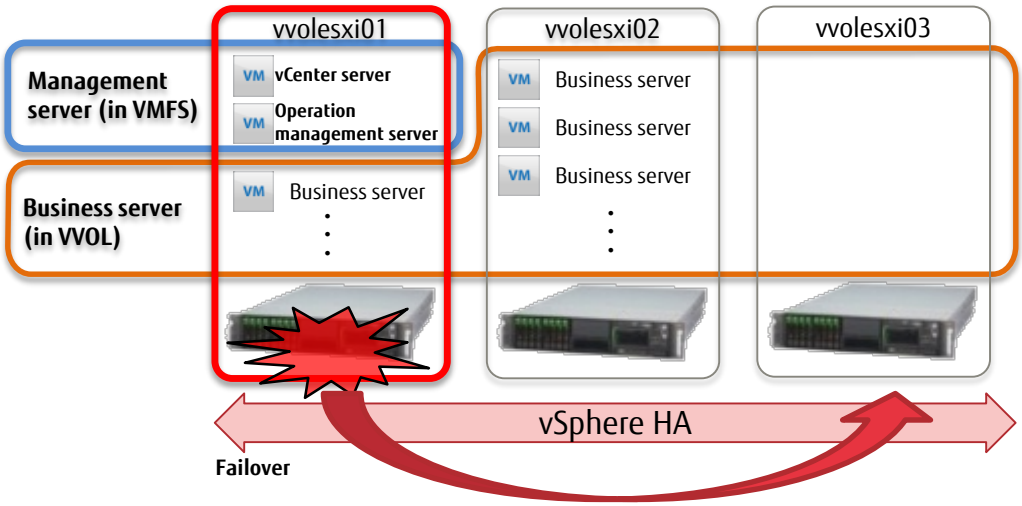

Figure-122 vSphere HA for the operation management server

4 Notes

1. Tier pools and volumes that can be used in the ETERNUS DX S3 series

   - The following table shows the number of Tier pools that can be registered in each storage system model.

Storage system	Maximum number of Tier pools	Maximum number of sub-pools	Maximum pool capacity
ETERNUS DX100 S3	30	72	256TB
ETERNUS DX200 S3	30	132	256TB
ETERNUS DX500 S3	60	256	384TB
ETERNUS DX600 S3	64	256	768TB
ETERNUS DX8700 S3/DX8900 S3	64	256	1,024TB
ETERNUS DX200F	12	12	32TB

Table-41 Maximum numbers of Tier pools in a storage system

   - The following table shows the number of volumes that can be created in each storage system model.

Storage system	Maximum number of volumes in the storage system	Number of available volumes*1	Recommended number of volumes for VVOLs*1
ETERNUS DX100 S3	2,048	2,009	1,808
ETERNUS DX200 S3	4,096	4,057	3,651
ETERNUS DX500 S3	16,384	16,313	14,681
ETERNUS DX600 S3			
ETERNUS DX8700 S3/DX8900 S3*2	65,535	65,464	58,917
ETERNUS DX200F	1,536	1,497	1,347

*1 Values when pools are configured with six RAID groups.
*2 For details on the support range and operation environment, contact your Fujitsu sales representative.

Table-42 Maximum numbers of volumes that can be created in a storage system

2. VMware vCenter Server Appliance
   - By default, the password for a Single Sign On user is valid for 90 days.
     Change the default password policy according to the operational requirements.

Password policy setting item	Default value
Maximum lifetime	Password must be changed every 90 days
Restrict reuse	Users cannot reuse any previous 5 passwords
Maximum length	20 characters
Minimum length	8 characters
Character requirements	At least 2 alphabetic characters
	At least 1 special characters
	At least 1 uppercase characters
	At least 1 lowercase characters
	At least 1 numeric characters
	Identical adjacent characters:3

Table-43 Password policy for VMware vCenter Server Appliance

   - The clocks of each component of VMware ESXi Server must be synchronized.
     For SSL communications between unsynchronized servers, SSL certificates that require time synchronization are recognized as disabled and services in VMware may fail to start.

3. ETERNUS SF Storage Cruiser

   - The Thin Provisioning function in the ETERNUS DX S3 series must be enabled to use VVOLs.
     Automated Storage Tiering must also be enabled with ETERNUS SF Manager.
     (One layer Tier pool of Automated Storage Tiering becomes available for ETERNUS SF Storage Cruiser.)

     For more details, refer to "3.3 Activation of Automated Storage Tiering" in "FUJITSU Storage ETERNUS SF Storage Cruiser V16.2 Operation Guide for Optimization Function".

   - In vSphere HA configurations, when a VVOL datastore is mounted on vCenter Server, management volumes are automatically created in the VVOL datastore of the ETERNUS DX S3 series.
     When deleting a VVOL datastore from ETERNUS SF Web Console, the management volumes in vSphere HA must be deleted.
     In order to delete the management volumes of vSphere HA, unmount the VVOL datastore from vCenter Server, and then execute the following ETERNUS SF Manager command.

     ```
     storageadm volume delete -ipaddr [IP_address_of_the_ETERNUS_DX_S3_series] -volume [volume_number]
     ```

5 Reference

1. Product information
   - Fujitsu's ETERNUS DX Disk storage systems
     http://www.fujitsu.com/eternus/
     Disk Storage Systems > ETERNUS DX
   - Storage Foundation Software : FUJITSU Storage ETERNUS SF
     http://www.fujitsu.com/eternus/
     Storage software > ETERNUS SF

2. Software to download
   - ETERNUS VASA Provider 2.x

3. Related manuals
   - FUJITSU Storage ETERNUS DX100 S3/DX200 S3 Disk storage system Configuration Guide (Basic)
   - FUJITSU Storage ETERNUS DX Configuration Guide (Web GUI)
     FUJITSU Storage ETERNUS DX Configuration Guide -Server Connection- (iSCSI) for VMware® ESX
   - FUJITSU Storage ETERNUS SF Express V16.2 / Storage Cruiser V16.2 / AdvancedCopy Manager V16.2 Installation and Setup Guide
     FUJITSU Storage ETERNUS SF Express V16.2 / Storage Cruiser V16.2 / AdvancedCopy Manager V16.2 Web Console Guide
   - FUJITSU Storage ETERNUS SF Storage Cruiser V16.2 Operation Guide
     FUJITSU Storage ETERNUS SF Storage Cruiser V16.2 Operation Guide for VMware vSphere Virtual Volumes
     FUJITSU Storage ETERNUS SF Storage Cruiser V16.2 Operation Guide for Optimization Function
   - ETERNUS VASA Provider 2.x User's Guide

CONTACT
FUJITSU Limited
Website: http://www.fujitsu.com/eternus/