White Paper

Storage Security Guide

Table of Contents

1. Secure Communication

1.1. Robust communication encryption using SSL/SSH

ETERNUS AF/ETERNUS DX supports SSL (Secure Socket Layer)/SSH (Secure Shell) for encryption and secure transfer of data over a network.

Normal data transmission without encryption bears the risk of possible unauthorized accesses from malicious Web browsers/CLI that appear authorized while attempting to steal or alter data.

SSL enables secure transmission of important data using SSL server certification (public key and secret key) on both browser and web server. Note: Https (Hyper Text Transfer Protocol over SSL) used on the Web, applies this SSL encryption technology to http.

SSH encrypts data using common key encryption methodologies (DES, AES) as it is forwarded from one computer to another via a TCP/IP network. By this and by also hiding the common key using public key encryption methodologies, SSH achieves high data security.

Encrypted communication between ETERNUS storage and ETERNUS SF as well as user terminals using these technologies prevents alteration and theft of important information.

In the case of ETERNUS SF, all communications also implement SSL/SSH. The passwords for SSH authentication are stored encrypted in the ETERNUS SF internal database to remove the risk of them being stolen. Authentication applies to the following connections between ETERNUS SF and the SAN network hardware components:

- Connection to DX/AF storage
- Connection to SAN switch
- Connection to LAN switch
- Connection to physical server
- Connection to Esxi and vCenter
- Connection to Hyper-V

Just like ETERNUS, ETERNUS SF implements https for its web-based interface and SSH for its CLI to ensure that no third party intrusion is done during operation. On a case-by-case basis, additional hardening measures are possible such as restricting the range of IP addresses able to access the ETERNUS SF GUI.

1.2. Authentication per operation

ETERNUS SF accesses the ETERNUS storage as well as registered servers and switches using SSL encrypted communication. Furthermore, for added security, the access to ETERNUS from ETERNUS SF is re-authenticated for each transaction, for example when an operation on ETERNUS is requested from the ETERNUS SF Manager.

1.3. RADIUS authentication support

RADIUS authentication supports ETERNUS Web GUI and the ETERNUS CLI login authentication for the ETERNUS DX, and authentication for connections to the ETERNUS DX through a LAN using operation management software.

- RADIUS authentication

RADIUS authentication uses the Remote Authentication Dial-In User Service (RADIUS) protocol to consolidate authentication information for remote access.

An authentication request is sent to the RADIUS authentication server that is outside the ETERNUS system network.

The authentication method can be selected from CHAP and PAP. Two RADIUS authentication servers (the primary server and the secondary server) can be connected to balance user account information and to create a redundant configuration. When the primary RADIUS server failed to authenticate, the secondary RADIUS server attempts to authenticate.

User roles are specified in the Vendor Specific Attribute (VSA) of the Access-Accept response from the server.

The following table shows the syntax of the VSA based account role on the RADIUS server.

Table 1.3. Syntax of the Vendor Specific Attribute (VSA) based account role

Item	**Size(octets)**	**Value**	**Description**
Type	1	26	Attribute number for the Vendor Specific Attribute
Length	1	7 or more	Attribute size (calculated by server)
Vendor-Id	4	211	Fujitsu Limited (SMI Private Enterprise Code)
Vendor type	1	1	Eternus-Auth-Role
Vendor length	1	2 or more	Attribute size described after Vendor type (calculated by the server)
Attribute-Specific	1 or more	ASCII characters	List of one or more role names assignable to successfully authenticated users (*1)

*1: The server-side role names must be identical to the role names of the ETERNUS DX. Match the letter case when entering the role names.

1.4. Port Open/Close control

ETERNUS AF/ETERNUS DX can control ports Open/Close by the Firewall settings.

You can control the Firewall settings from web GUI/CLI, and the changes are applied to the ports immediately without power cycle the system.

The table below shows the controllable ports.

Table 1.4. Open/Close controllable ports and services

Service	Protocol	Default status		
		MNT port	RMT port	FST port
Web GUI	http	Open	Open	Open
	https	Open	Open	Open
CLI	telnet	Open	Open	Open
	ssh	Open	Open	Open
SNMP	agent	Open	Open	Close (Non-changeable)
NIM-PCC	NIM-PCC(secure)	Open	Open	Open
Ping	ICMP[23]	Open	Open	Open
ETERNUS DX Discovery	ETERNUS DX Discovery	Open	Close (Non-changeable)	Close (Non-changeable)

- MNT port

The MNT port is used for general communication between the ETERNUS DX/AF and the external hosts.

- RMT port

The RMT port is used when the line must be separated from the MNT port. This port is also used for maintenance of the ETERNUS DX/AF.

- FST port

The FST port is used for maintenance of the ETERNUS DX/AF.

1.5. SSL version settings

ETERNUS AF/DX can set SSL version (TLS1.0/TLS1.1/TLS1.2) for each of the following protocols to realize more secure communication.

- HTTPS (GUI)
- HTTPS (SMI-S)
- Maintenance-Secure

2. Secure User Management

2.1. Role Based Access Control (RBAC)

2.1.1 ETERNUS

When creating a user account, at least one role must be applied to the account.

There are two types of roles; a default role and a custom role. The default role is already prepared in the ETERNUS AF/DX and the custom role can be managed by the user.

- Default Role

  Default roles cannot be deleted nor changed. The following table shows the default roles and policies applied to each default role.

Table 2.1.1. Default roles and applied policies

Policies	Default Roles						
	Monitor	Admin	Storage Admin	Account Admin	Security Admin	Main-tainer	Software (*1)
Status Display	Yes	Yes	Yes	No	Yes	Yes	No
RAID Group Management	No	Yes	Yes	No	No	Yes	No
Volume – Create / Modify	No	Yes	Yes	No	No	Yes	No
Volume – Delete / Format	No	Yes	Yes	No	No	Yes	No
Hot Interface Management	No	Yes	Yes	No	No	Yes	No
NAS Management	No	Yes	Yes	No	No	Yes	No
Advanced Copy Management	No	Yes	Yes	No	No	Yes	No
Copy Session Management	No	Yes	Yes	No	No	Yes	No
Storage Migration Management	No	Yes	Yes	No	No	Yes	No
Storage Management	No	Yes	No	No	No	Yes	No
User Management	No	Yes	No	Yes	No	No	No
Authentication / Role	No	Yes	No	Yes	No	No	No
Security Setting	No	Yes	No	No	Yes	No	No
Maintenance Information	No	Yes	No	No	Yes	Yes	No
Firmware Management	No	Yes	No	No	No	Yes	No
Maintenance Operation	No	No	No	No	No	Yes	No

*1: The role "Software" cannot log in to ETERNUS GUI. It is used for external software.

- Custom Role

  This function combines several user policies and creates a user-specific role. Up to 20 roles can be created per storage system.

  The 16 types of access privileges shown below are available.

Table 2.1.2. Policies for custom roles

Policies	Description
Status Display	Status display functions (storage system status, RAID group list, volume list, copy session list, etc.)
RAID Group Management	RAID group, Thin Provisioning Pool, Eco-mode, hot spare disk setting functions, etc.
Volume - Create / Modify	Volume setting functions (register/modify/expand), etc.
Volume - Delete / Format	Volume setting functions (delete/format), etc.
Host Interface Management	Host interface management functions (host group settings, Channel Adapter (CA) port group settings, Logical Unit Number (LUN) group settings, host affinity settings),etc.
NAS Management(* in Unified Storage environment only)	NAS setting functions (create NAS interface, create NAS shared folders), etc.
Advanced Copy Management	Local Advanced Copy setting functions, Remote Advanced Copy setting functions, etc.
Copy Session Management	Advanced Copy session management functions (start/stop/delete), etc.
Storage Migration Management	Storage Migration setting functions (start/suspend/stop/restart/delete path), etc.
Storage Management	Configuration setting functions of the ETERNUS DX/AF (date and time, network, remote support), etc.
User Management	User account setting functions (create/change/delete), etc.
Authentication / Role	External authentication and role setting functions (create/change/delete), etc.
Security Setting	Encryption setting functions of drives, etc.
Maintenance Information	Exporting and deleting functions of maintenance information (performance information, configuration information, events, storage system logs, panic dumps), etc.
Firmware Management	Firmware management functions (for users without the "Maintenance Operation" policy who need to set the controller firmware)
Maintenance Operation	Maintenance operation/preventive maintenance operation of hardware and firmware

2.1.2 ETERNUS SF

ETERNUS SF uses RBAC (Role Based Authentication Control) to manage the application's users. Two roles are defined, Administrator and Monitor. The Administrator role allows configuration as well as monitoring, while the Monitor role is restricted to monitoring the SAN component status only.

2.2. Modify User Policy

This function specifies a user policy (Password Policy and Lockout Policy) for user accounts to be registered in the ETERNUS DX/AF.

"Password Policy" indicates the creation guidelines for a password such as the complexity and lifetime. This setting is applied when the password for the new user account is registered or when the password for an existing user account is changed. "Lockout Policy" indicates the guidelines for a lockout when the authentication fails. This setting is used when users log in to the ETERNUS DX/AF.

You can set the following user policy.

- Password Policy
  - ✓ Minimum Password Length
  - ✓ Password Complexity
  - ✓ Password History
  - ✓ Minimum Password Age
  - ✓ Maximum Password Age

- Lockout Policy
  - ✓ Lockout Threshold
  - ✓ Lockout Duration

2.3. OS-level authentication support for ETERNUS SF

User management in ETERNUS SF leverages the underlying OS-level user management (Windows Active Directory (Local Domain), Linux, Solaris), allowing to benefit from the strong authentication features at the Operating System level and to avoid carrying user accounts and passwords in the storage software itself, reducing the risks of intrusion and theft.

It is possible to manage which user accounts can log into Storage Cruiser with which privileges by adding or removing user accounts from the ESFAdmin user group (administrators) and the ESFMon user group (Monitors). Using this feature, it is possible to remove login accounts with administrative privilege completely once the configuration has been done for tighter security.

2.4. Stored password encryption

The passwords are not stored in clear text. They are one-way encrypted and stored in the storage system.

3. Secure Operation Auditing

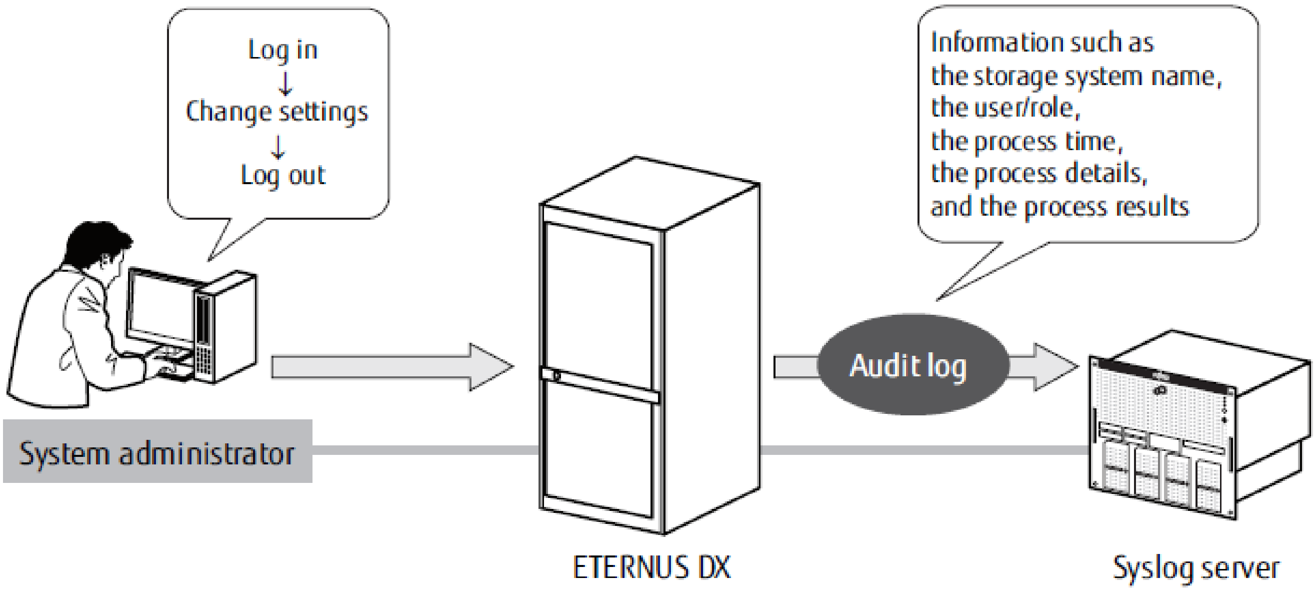
3.1. Support for system/remote syslog server

3.1.1 ETERNUS

The ETERNUS AF/DX can send information such as access records by the administrator and setting changes as audit logs to the Syslog servers. For example, Log in, Log out, and Log in failure records as Access logs, and setting changes are recorded as Operation logs. (See the document "Massage list (P3AM-7922-19ENZ0)" for the details. http://docs.ts.fujitsu.com/dl.aspx?id=94f60b39-faa5-42fc-8fa6-1a7ed9aeab1d)

Audit logs are audit trail information that record operations that are executed for the ETERNUS AF/DX and the response from the system. This information is required for auditing.

The audit log function enables monitoring of all operations and any unauthorized access that may affect the system. Syslog protocols (RFC3164 and RFC5424) are supported for audit logs. Information that is to be sent is not saved in the ETERNUS AF/DX and the Syslog protocols are used to send out the information. Two Syslog servers can be set as the destination servers in addition to the Syslog server that is used for event notification.



3.1.2 ETERNUS SF

ETERNUS SF keeps a log of user Login-Logout as well as a log of operations for Audit purposes. The events recorded in the logs that are displayed in the Storage Cruiser Web Console are maintained internally in the Storage Cruiser database, but they can be exported for review in CSV format using the log export function. The logs that can be exported include Event, Operation History, Login/Logout history, and Performance threshold monitoring alarms.

It is possible to redirect the Event log output destination to a remote syslog server with the Linux and Solaris versions of Storage Cruiser manager.

Alternatively, The Storage Cruiser Operation Guide, Chapter provides an example of batch file that will generate a Windows system event based on the Event log contents.

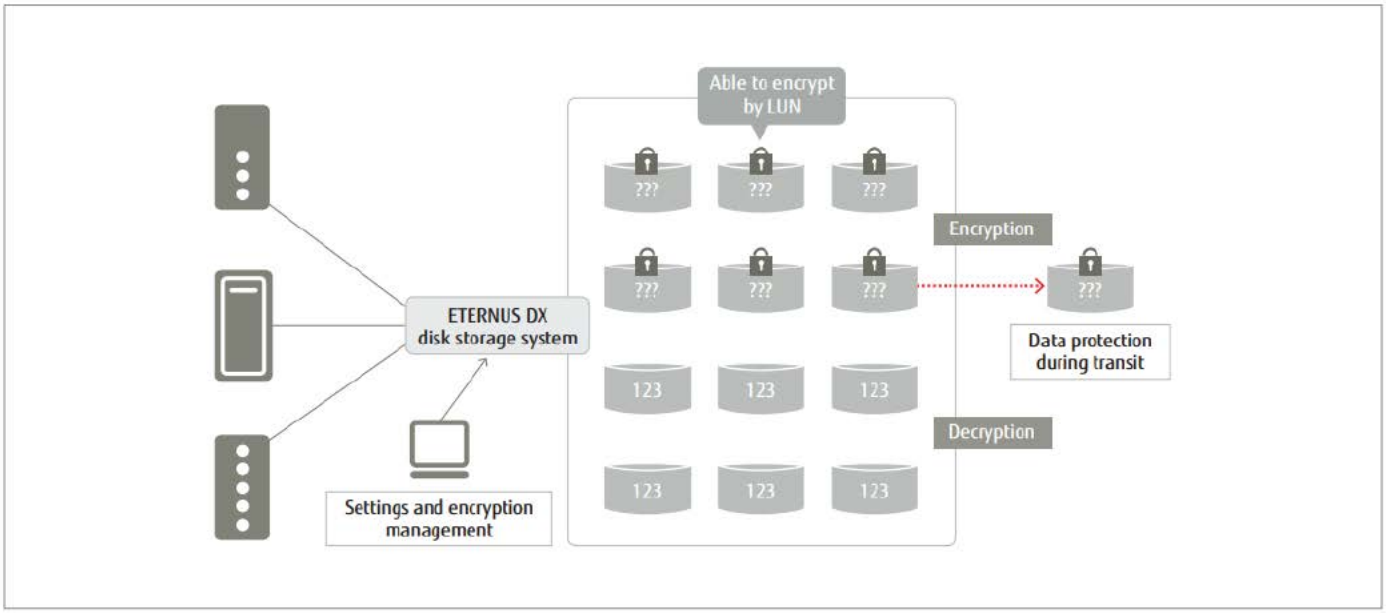
4. Secure Data Storage

4.1. Controller-based Encryption

ETERNUS AF/DX series support controller based encryption function.

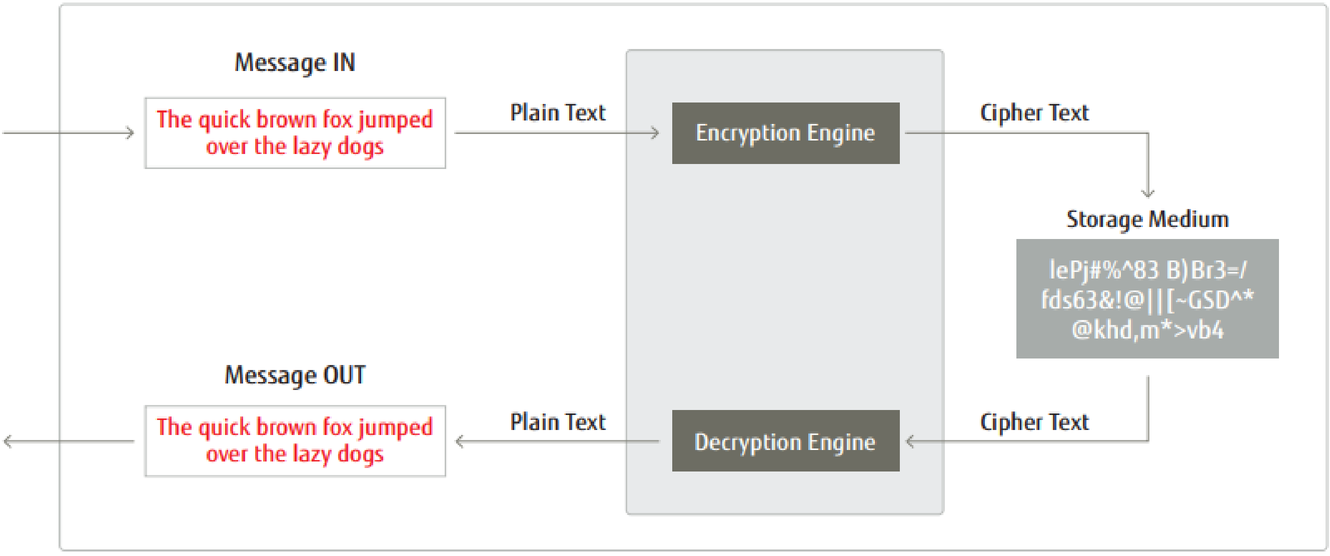
Controller based encryption prevents unauthorized data access LUNwise, whereas Self-Encrypting Disks do not offer this kind of granularity.

The selected encryption technology can either be the world-standard 128-bit AES technology, 256-bit AES or Fujitsu's unique encryption with high-process performance.


Able to encrypt by LUN
???
Encryption
Data protection during transit
ETERNUS DX disk storage system
123
Decryption
Settings and encryption management

4.2. Self-Encrypting Drive (SED) support

ETERNUS AF/DX series support Self-Encrypting Drive (SED). Here the disk drive uses hardware encryption instead of firmware. This enables data encryption without performance loss as no load is placed on the system by firmware operation.


Message IN
The quick brown fox jumped over the lazy dogs
Plain Text
Encryption Engine
Cipher Text
Storage Medium
lePj#%^83 B)Br3=/ fds63&!@||[~GSD^* @khd,m*>vb4
Message OUT
The quick brown fox jumped over the lazy dogs
Plain Text
Decryption Engine
Cipher Text

4.3. Encryption Key Management application (KM)

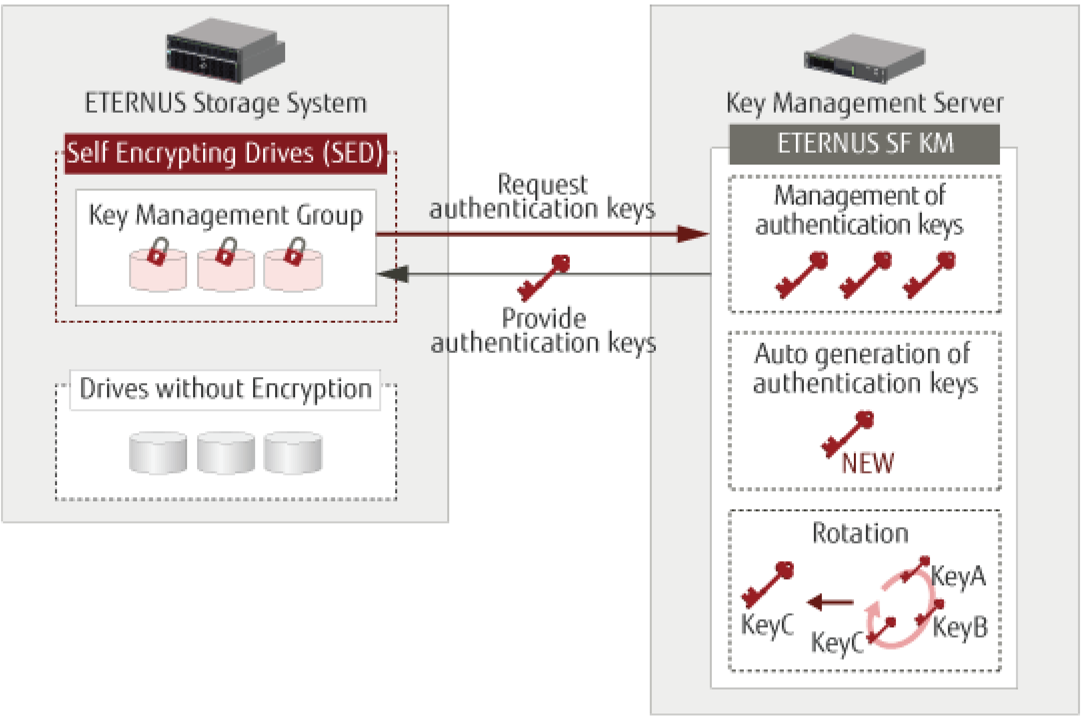
Required authentication keys are provided for the key management group in which Self Encrypting Drives (SED) are registered. Authentication keys generated and stored by a key management server are provided for a required device when required.

Secure uniform management can achieve authentication key management and reduce risk of important data leakage.

In addition, secure communication is carried out between the key management server and an ETERNUS AF/ETERNUS DX using mutual certificate authentication to prevent any illegal access from outside.

The certificate generation and expiration notification functions make it easy to install and use certificates.

KM V3.0 Feature


ETERNUS Storage System
Self Encrypting Drives (SED)
Key Management Group
Drives without Encryption
Request authentication keys
Provide authentication keys
Key Management Server
ETERNUS SF KM
Management of authentication keys
Auto generation of authentication keys
NEW
Rotation
KeyA
KeyB
KeyC
KeyC

- Key lifecycle management

  The ETERNUS SF KM has auto generation/rotation functions of authentication keys and backup function of those key information to achieve authentication key lifecycle management and reduce operations management costs. It also supports high availability by replication.

- Global security

  ETERNUS SF KM enhance data security and help facilitate compliance management of regulations and standards such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxleyand the Health Insurance Portability and Accountability Act (HIPAA). The standard communication specification for Key Management Interoperability Protocol (KMIP) is supported.

5. Secure Software Management

5.1. OSS software vulnerability monitoring policy

Fujitsu as an organization includes a dedicated department monitoring the security advisories for the Open Source Software components used in the Fujitsu Software, including ETERNUS and ETERNUS SF. When a security advisory regarding one of the OSS components used in ETERNUS SF is published, the risk is assessed systematically. If the vulnerability is severe and the risk is recognized, Fujitsu will create a specific patch including the fix for this vulnerability for ETERNUS SF and distribute the patch through the support channel to customers as soon as possible.

5.2. Regular patch distribution policy

Patches for ETERNUS firmware ETERNUS SF are issued both on regular and ad hoc bases through the support channel. Patches come as individual patches, and can be applied with a dedicated tool called Update Advisor, and come also in consolidated patches, issued every two months, aggregating the individual patches of the period. This system allows the user to have an up-to-date software easily.

Contact
FUJITSU LIMITED
Website: https://www.fujitsu.com/eternus/

■Registered trademarks
Active Directory is a registered trademark or trademark of Microsoft Corporation in the United States, and other countries. Linux is a registered trademark or trademark of Linus Torvalds in the U.S. and other countries. Trademark symbols such as (R) and (TM) may be omitted from system names and product names in this document. The product names and company names in this document are registered trademarks or trademarks of their respective companies.

■ Disclaimer
All rights reserved, including intellectual property rights. Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded.
FUJITSU LIMITED is not responsible for any damage or indemnity that might be caused by the content in this document.