Technical Support Bulletin

Dual SFA Controller Replacement with Self-Encrypting Drives

ALERT! **Always engage DDN Engineering** prior to replacing both SFA controllers on storage arrays with self-encrypting drives. Your DDN Support TSE will engage Engineering on your behalf.

Statement of Policy

It is DDN policy to require DDN Engineering engagement on every support case that replaces both SFA controllers in a storage cluster with self-encrypting drives (SEDs). *Failure to follow this policy will put customer data at risk.*

DDN Support customers should be aware of this policy when planning for dual controller replacements and allow additional time for Engineering engagement when assigning a maintenance window.

Issue Summary

Self-encrypting drives use on-drive processing to locally encrypt drive data when encryption is enabled. This keeps the data secure when the drive is removed from the storage system. The authentication key to access SED data is created and stored either by a storage system controller (which shares it with the partner controller) or by a server-based authentication key management system such as KMIP. The customer should also store a backup copy of the key on external media in a secure location. (See SPT-TSB-0110, *Securing SFA Storage Systems*.)

ALERT! If the authentication key for a self-encrypting drive (SED) is lost, data on the affected drive **cannot be recovered.**

Replacing a single SFA controller does not normally raise concerns about preserving the SED authentication key. The remaining controller retains that key and will share it with the new controller when it joins the couplet. However, *replacing both controllers could remove the authentication key from the storage system, making all data on installed SEDs inaccessible.*

Preserving the SED authentication key throughout a dual controller replacement involves more than just keeping one of the partner controllers running at all times. The replacement procedure varies by:

- SFA OS version
- SFA hardware platform model
- BIOS and BMC firmware variants
- KMIP server authentication management versus SFA authentication management
- Online versus offline maintenance requirements

Due to complex interactions among these factors, as well as the high risk to data in the event an incorrect procedure is followed, *DDN Engineering has asked to be engaged in every SFA dual-controller replacement involving self-encrypting drives*.

Affected Products

This policy directive applies to all SFA storage platforms and SFA OS versions, including legacy SFA OS (versions prior to 11.x).

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or need assistance. Support can be reached online, by email, or by phone as listed below.

Web

DDN Community Support Portal	https://community.ddn.com/login
Portal Assistance	webportal.support@ddn.com

Email

Support Email	support@ddn.com

Telephone

DDN Support Worldwide Directory	https://www.ddn.com/support/global-services-overview/

Bulletins & Notices

Support Bulletins	http://www.ddn.com/support/technical-support-bulletins
End-of-Life Notices	http://www.ddn.com/support/end-of-life-notices
Release Notes	https://community.ddn.com/login
Subscription Requests	support-tsb@ddn.com