Disk Encryption on System x Servers with IBM Security Key Lifecycle Manager

Planning / Implementation (withdrawn product)

Securing sensitive client and company data is becoming an IT task of paramount importance. Often organizations invest heavily in protection against network attacks, but fail to safeguard against the costly exposure that can result from the loss, replacement, redeployment, or retirement of disk drives. Other organizations invest in software-based encryption to secure their data, but receive limited protection at a great cost to performance.

Self-encrypting drives (SEDs) can satisfy the requirement for data-at-rest security with cost-effective inline encryption without the performance trade off that is required by software-based encryption. The addition of IBM Security Key Lifecycle Manager (SKLM) allows for lower operating costs by streamlining the configuration and management of SED authentication through one SKLM interface that controls the authentication of several System x servers. Whether you want to protect personal data for legal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), better secure banking information, or ensure the safety of company and employee records in an efficient manner, this Solution Guide provides an overview of how SEDs and SKLM can help accomplish that goal. Figure 1 shows the main components of an SKLM environment, which includes the following features:

- The interaction between SKLM and the RAID controller to exchange a hidden password.
- Verification of encryption keys between SEDs and the encryption-capable RAID controller to allow the system to boot and use the drives.

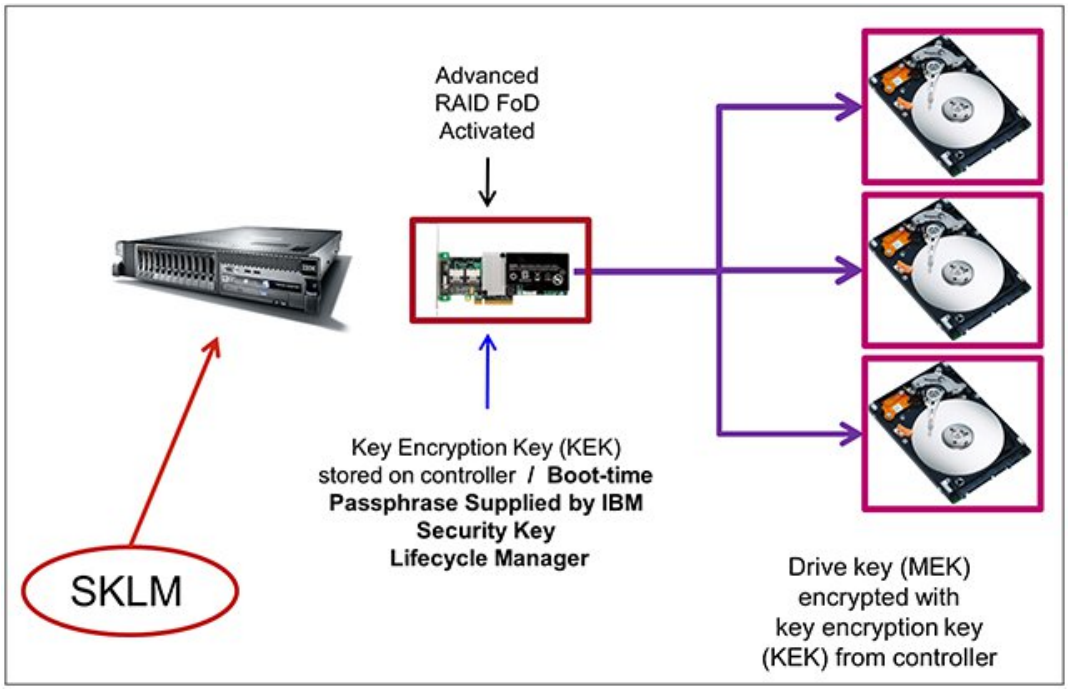

Figure 1. Main components for SKLM and SED key exchange

Did you know?

The traditional methods of destroying and degaussing disk drives are not standardized and might not guarantee the destruction and protection of data, while overwriting data can take hours or days. SEDs adhere to a certified government standard, the Federal Information Processing Standards or FIPS 140-2 Security Requirements for Cryptographic Models recognized by the US National Institute of Standards and Technology (NIST) and Canadian Communications Security Establishment (CSE). The standards assert that the encryption that is used by self-encrypting drives protects Sensitive but Unclassified and Protect Class Data.

AES encryption ensures that sensitive data is safely stored while SEDs are in use. The data also is protected when SEDs are retired from use. When implemented, a solution that uses SEDs eliminates the need to recover lost or stolen drives, and end-of-life drives can be discarded or recycled without any need for costly or inefficient data destruction processes. With the addition of SKLM to the security solution, systems with SEDs become easier to track and maintain and the theft or loss of an entire server is no longer a data security issue because the SEDs cannot function without their SKLM authentication.

Business value

Independently SEDs can add significant security value with minimal cost for any business that must protect its stored data without cumbersome processes for physical security and destruction of failed and retired drives.

These SEDs include the following benefits:

- Inline hardware encryption ensures no performance degradation or risk of data loss because operating system or software corruption.
- Instant secure erasure allows data to be cleared immediately by using encryption keys. Drives can then be safely reused, sold, or discarded or recycled.
- Even without performing a secure instant erasure, encryption ensures that data is protected if a drive is removed, stolen, or fails. An SED must be matched back to the same disk controller or data cannot be decrypted. Alternatively, the ability to back up a controller's media encryption keys allows for protection against server and disk controller failure so no SED data is lost.
- The Federally backed (FIPS: 140-2) data encryption standard provides confidence that erased, disposed of, or stolen drives cannot result in data exposure.
- SED encryption is always on, which means that self-encrypting capable drives, controllers, and servers can be purchased and used in default configurations with encryption enforcement off. When ready for encryption, turn on encryption at the controller for the wanted RAID arrays or virtual disks and continue with secure operation. Inline encryption eliminates the need for lengthy retroactive data encryption as is necessary with software encryption.

Figure 2 shows the interaction between an SED and an encryption-capable RAID controller. At power-on, the encryption processor on the SED begins its key exchange with the RAID controller to ensure that they have matching keys and data can be safely decrypted for use by the server. After that key exchange is successful between the controller and the drive, the encryption processor provides unencrypted data to the server. If the key exchange is unsuccessful, the server boot is halted.

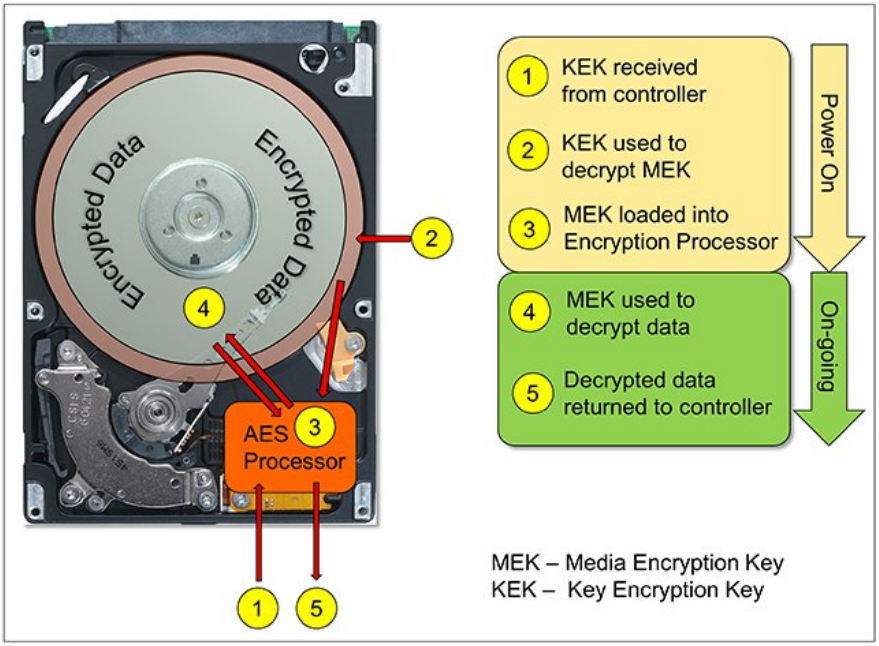

Figure 2. Encryption key exchanges between drive and RAID controller

When paired with IBM SKLM, SED management and deployment can be simplified. SKLM provides a low-touch, centralized way to manage the authentication exchanges with SEDs and includes the following benefits:

- With SKLM integration, no SED in the environment can be compromised, even if an entire server is stolen.
- Management of multiple SEDs, multiple encryption enable controllers, multiple encryption enabled servers, even multiple platforms in one interface.
- Remote management of SEDs allows keys to be expired and reissued, and drives or servers to be securely retired or reused with only a connection to the System x server's Integrated Management Module (IMM).

These concepts are shown in Figure 3.

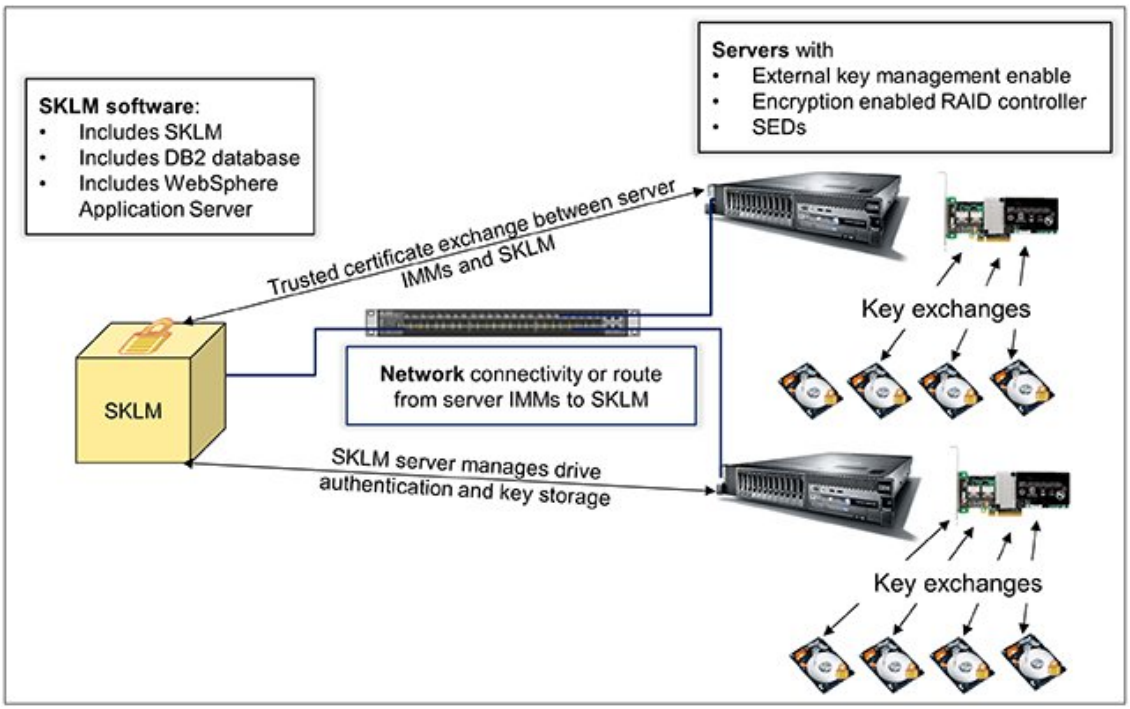

Figure 3. Encryption solution with SKLM for centralized management

Solution overview and architecture

A solution to centrally manage access to SEDs in System x servers by using IBM SKLM requires the following main components:

- IBM SKLM software

  The software must be installed on a supported operating system, but can be installed in a virtual instance of that operating system to use high availability safeguards and streamline backup methods. SKLM is a self-contained installer; the necessary components (including DB2 and WebSphere Application Server) are included.

- Supported System x server (or servers)

  At least one System x server that supports SEDs is required. To enable the server (or servers) to use external key management for SEDs, one Feature on Demand (FoD) activation key must be purchased for each server and applied to the servers' IMM.

- Supported RAID controller

  Specific RAID controllers support SEDs. Any server that uses SEDs must have those drives connected to an encryption-enabled RAID controller. The controller also might need a cache or RAID upgrade added to enable SED support. Some of these upgrades are no-charge.

- SEDs

  At least two SEDs are required to set up an encrypted solution on a virtual disk or RAID array of SEDs.

Implementing a centrally managed SED solution is often easiest from the ground up. Figure 4 shows the components that interact at each stage of the configuration (top to bottom) from local encryption only to centrally managed encryption.

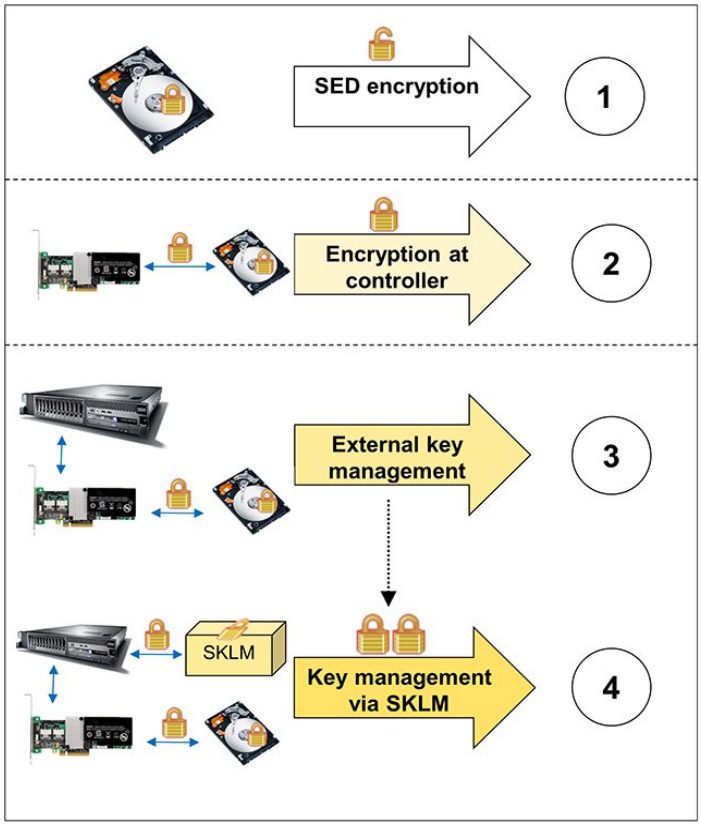

Figure 4. Stages of an encryption solution and component communication

Each stage features the following activities:

1. Data is always being encrypted at the SED level. At first installation, the controller is not requiring a key exchange to enforce matching the SED to the controller and securing the system; therefore, no automatic protection is offered at this point.
2. When disk encryption is enabled at the controller and virtual disks, SEDs must exchange an encryption password with the controller to allow data access, which protects data against drive theft and allows easy and secure retirement or reuse.
3. With external key management enabled at the controller, the controller password exchange with the SEDs is no longer the only requirement for a server to boot and an SED's data to be accessed. The server's IMM now must complete a certificate and password exchange with a key management server for the SED to function.
4. With the SKLM server in place, the server's IMM now completes a certificate exchange with SKLM. SKLM supersedes the authority of the controller and requires a network connection to the server's IMM upon start. SKLM then exchanges the encryption key (or keys) with the controller and protects against drive theft or retirement or reuse and server theft, retirement, and reuse.

With centralized key management, the SKLM server and its database become critical components of the SED solution. The loss of SKLM results in the loss of access to the data on all SEDs it is managing. For this reason, it is critical that a backup or disaster recovery process is in place, and preferably high availability. The default SKLM license allows for the installation of two instances (one master and one clone). SKLM can replicate to up to three clone instances of the software with a System x environment. This limitation is based on the FoD limitation of the System x IMMs, not the SKLM clone maximum (which is five).

In the “Usage scenario” section, we build on the fundamentals that are shown in Figure 4 with an example of a customer production scenario.

Usage scenario

Many organizations must protect data on their disk drives that are in their data centers and in remote locations. Banking institutions provide an excellent example of businesses that benefit from local encryption authentication, but need a centralized authentication solution to operate efficiently and securely.

Companies that provide banking servers often have servers in data centers and in local branches, both of which contain sensitive client data. The use of self-encrypting drives in each local branch with encryption enabled on the controller and its virtual disks protects against drive theft and provides easy disk retirement via secure instant erase. However, this solution still leaves clients vulnerable to server theft and presents a complex solution from a key management and backup standpoint. IBM SKLM can alleviate these problems by cryptographically securing data over the company network.

To protect against server theft or allow for safe retirement or reuse of an entire server, SKLM requires a connection back to SKLM to access data and boot the server from SEDs. With centralized key authentication in place with SKLM, a server that is removed from the company network has the option to secure instant erase its drives upon boot only, which automatically protects against sensitive data form being exposed. Also, SKLM now allows holds all of the data that must be managed and backed up up without much more setup effort than a locally managed SED solution. With SKLM in place, backups are significantly more simple and server certificates or drive encryption keys can be removed safely when servers or drives must be retired.

Figure 5 shows multiple bank branches that are use servers with SEDs. Those servers connect to servers that are running SKLM in the corporate data centers to authenticate and allow access to the drive's data in the local branch. The use of SKLM clones to replicate data protects against the corruption or loss of an SKLM instance. In addition, the use of a clustered solution (such as a VMware vSphere High Availability set up with ESXi and vCenter) allows for resiliency to server failures or maintenance that can normally result in a downtime for your SKLM solution. The example in Figure 5 also shows replication to a disaster recovery (DR) site for SKLM. This configuration is also strongly recommended because of the critical nature of the data that is stored by SKLM.

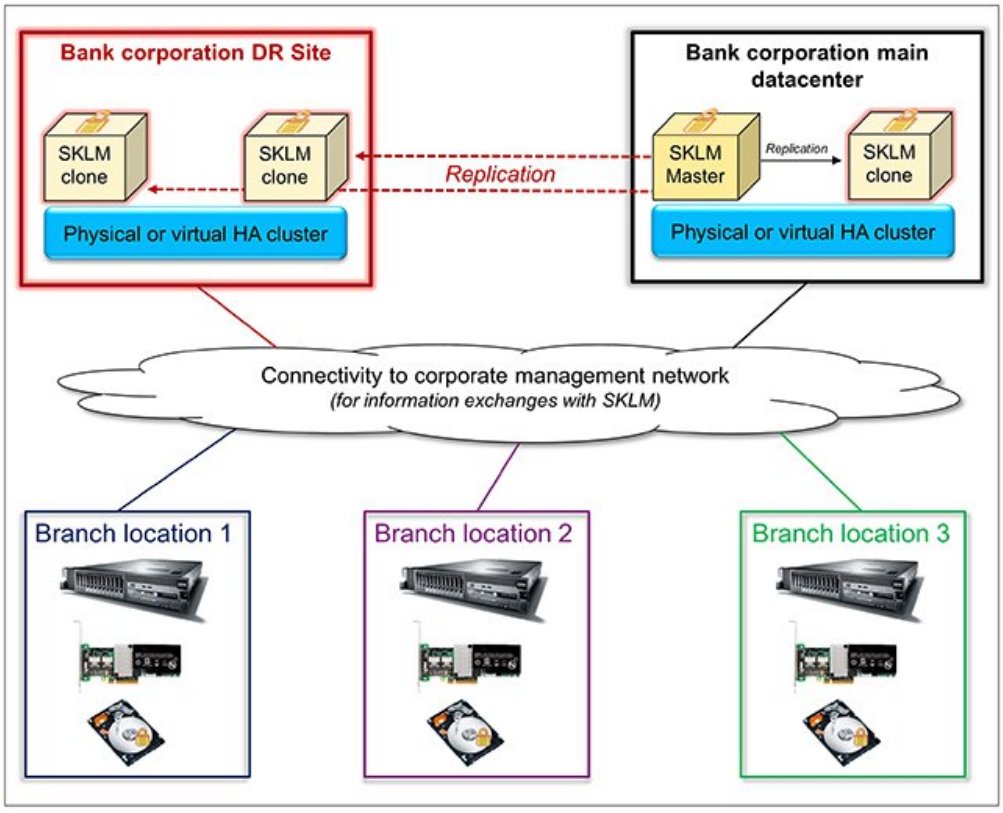

Figure 5. SKLM banking example

Integration and supported platforms

Several IBM platforms support the use of many sizes and types of SEDs, not only System x. System z and System p, as well as multiple IBM storage platforms, including NAS, SAN, and tape storage. Each of these platforms are supported by SKLM to centrally manage the exchanges that are required for their encrypted drives in a similar fashion, and all from one interface.

System x installation requirements

The following components are required for a centrally managed encryption solution:

- IBM SKLM software
- At least one SED
- RAID controller supporting encryption
- System x server that supports encryption and FoD enablement key to activate external key management on that server

The following SKLM hardware requirements must be met:

- System memory: 4 GB
- Processor speed: One 3.0 GHz CPU
- Disk space: 12 GB

The following SKLM Windows operating systems are supported:

- Windows Server 2008 R2 Enterprise and Standard Editions
- Windows Server 2012 Standard Edition
- Windows Server 2012 R2 Standard Edition

The following SKLM Linux operating systems are supported:

- SUSE Linux Enterprise Server (SLES) 11
- SUSE Linux Enterprise Server (SLES) 10
- Red Hat Enterprise Linux (RHEL) Server 6
- Red Hat Enterprise Linux (RHEL) Server 5

Ordering information

Ordering information is listed in the following tables.

At the time of this writing, the System x server systems that are listed in Table 1 are supported for external key management.

For more information about supported configurations, see the following Server Proven website:

http://www.ibm.com/systems/info/x86servers/serverproven/compat/us/

Table 1. Supported servers

Server	Machine Type
System x3100 M5	5457
System x3250 M5	5458
System x3300 M4	7382
System x3500 M4	7383
System x3500 M4 (E5-xxxxV2)	7383, E5-xxxxV2
System x3530 M4	7160
System x3530 M4 (E5-xxxxV2)	7160, E5-xxxxV2
System x3630 M4	7158
System x3630 M4 (E5-xxxxV2)	7158, E5-xxxxV2
System x3550 M4	7914
System x3550 M4 (E5-xxxxV2)	7914, E5-xxxxV2
System x3550 M5	5463
System x3650 M4	7915
System x3650 M4 (E5-xxxxV2)	7915, E5-xxxxV2
System x3650 M4 HD	5460
System x3650 M5	5462
System x3750 M4	8722/8733
System x3750 M4	8752/8718
System x3850 X6/x3950 X6	3837
NeXtScale nx360 M5	5465

Table 2 lists the supported RAID adapters and the corresponding upgrades.

For more information about the supported controllers and options, see the following ServerProven website:

http://www.ibm.com/systems/info/x86servers/serverproven/compat/us/

Table 2. Supported RAID adapters and the corresponding upgrades

Option part number	Description
Supported RAID adapters M5110	
81Y4481	ServeRAID M5110 SAS/SATA Controller for System x
Onboard	ServeRAID M5110e SAS/SATA Controller for System x
One of the upgrades below is required to support SEDs with the M5110 RAID controller	
81Y4544	ServeRAID M5100 Series Zero Cache/RAID 5 Upgrade for System x
81Y4484	ServeRAID M5100 Series 512MB Cache/RAID 5 Upgrade for System x
81Y4487	ServeRAID M5100 Series 512MB Flash/RAID 5 Upgrade for System x
81Y4559	ServeRAID M5100 Series 1GB Flash/RAID 5 Upgrade for System x
47C8670	ServeRAID M5100 Series 2GB Flash/RAID 5 Upgrade for System x
Supported RAID adapters M5210	
46C9110	ServeRAID M5210 SAS/SATA Controller for System x
Onboard	ServeRAID M5210e SAS/SATA Controller for System x
One of the upgrades below is required to support SEDs with the M5210 RAID controller	
47C8708	ServeRAID M5200 Series Zero Cache/RAID 5 Upgrade for IBM Systems-FoD
47C8656	ServeRAID M5200 Series 1GB Cache/RAID 5 Upgrade for IBM Systems
47C8660	ServeRAID M5200 Series 1GB Flash/RAID 5 Upgrade for IBM Systems
47C8664	ServeRAID M5200 Series 2GB Flash/RAID 5 Upgrade for IBM Systems
47C8668	ServeRAID M5200 Series 4GB Flash/RAID 5 Upgrade for IBM Systems
Supported RAID adapters M1215	
46C9114	ServeRAID M1215 SAS/SATA Controller for System x
The upgrade below is required to support SEDs with the M1215 RAID controller	
46C9114	ServeRAID M1215 SAS/SATA Controller for System x

Table 3 lists the supported SEDs as of this writing. This rapidly growing list of devices should be considered as a sub-set of supported options only. For more information about the supported SEDs for a specific server model, see the following IBM ServerProven website:

http://www.ibm.com/systems/info/x86servers/serverproven/compat/us/

Table 3. Supported SEDs

Option part number	Description
90Y8944	IBM 146GB 15K 6Gbps SAS 2.5" SFF G2HS SED
00AJ116	IBM 146GB 15K 6Gbps SAS 2.5" G3HS SED
00NA281	IBM 300GB 15K 12Gbps SAS 2.5" G3HS 512e SED
00NA286	IBM 600GB 15K 12Gbps SAS 2.5" G3HS 512e SED
90Y8913	IBM 300GB 10K 6Gbps SAS 2.5" SFF G2HS SED
00AJ106	IBM 300GB 10K 6Gbps SAS 2.5" G3HS SED
90Y8908	IBM 600GB 10K 6Gbps SAS 2.5" SFF G2HS SED
00AJ101	IBM 600GB 10K 6Gbps SAS 2.5" G3HS SED
00NA291	IBM 600GB 10K 12Gbps SAS 2.5" G3HS 512e SED
81Y9662	IBM 900GB 10K 6Gbps SAS 2.5" SFF G2HS SED
00AJ076	IBM 900GB 10K 6Gbps SAS 2.5" G3HS SED
00NA296	IBM 900GB 10K 12Gbps SAS 2.5" G3HS 512e SED
00AD085	IBM 1.2TB 10K 6Gbps SAS 2.5" G2HS SED
00AJ151	IBM 1.2TB 10K 6Gbps SAS 2.5" G3HS SED
00NA301	IBM 1.2TB 10K 12Gbps SAS 2.5" G3HS 512e SED
00NA476	IBM 1.8TB 10K 6Gbps SAS 2.5" G2HS 512e SED
00NA306	IBM 1.8TB 10K 12Gbps SAS 2.5" G3HS 512e SED
00W1533	IBM 2TB 7.2K 6Gbps NL SAS 3.5" G2HS SED
00ML218	IBM 2TB 7.2K 6Gbps NL SAS 3.5" G2HS 512e SED
00FN238	IBM 2TB 7.2K 12Gbps NL SAS 3.5" G2HS 512e SED
00W1543	IBM 4TB 7.2K 6Gbps NL SAS 3.5" G2HS SED
00ML223	IBM 4TB 7.2K 6Gbps NL SAS 3.5" G2HS 512e SED
00FN248	IBM 4TB 7.2K 12Gbps NL SAS 3.5" G2HS 512e SED
00ML228	IBM 6TB 7.2K 6Gbps NL SAS 3.5" G2HS 512e SED
00FN258	IBM 6TB 7.2K 12Gbps NL SAS 3.5" G2HS 512e SED

Not all drives are supported in all servers. For more information about the supported drives, see the ServerProven website.

For more information about which drives are supported in a server, see the Configuration and Options Guide that is published quarterly and is available at this website:

http://www.ibm.com/systems/xbc/cog/

Related information

For more information, see the following resources:

- IBM Redbooks: *Centrally Managing Access to Self-Encrypting Drives in System x Servers Using IBM Security Key Lifecycle Manager*, SG24-8247:
  http://lenovopress.com/sg248247
- IBM Redbooks Product Guide: *Self-Encrypting Drives for System x*, TIPS0761:
  http://lenovopress.com/tips0761
- IBM Security Key Lifecycle Manager product page:
  http://www.ibm.com/software/products/en/key-lifecycle-manager/

Related product families

Product families related to this document are the following:

- Drives

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, TIPS1288, was created or updated on March 10, 2015.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/TIPS1288
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/TIPS1288.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
NeXtScale
ServeRAID
ServerProven®
System x®

The following terms are trademarks of other companies:

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Windows Server® and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.