Redbooks
ibm.com/redbooks

IBM FlashSystem 9100 Architecture, Performance, and Implementation

Andrew Greenfield

Jon Herd

Corne Lottering

Tony Pacheco

Jagadeesh Papaiah

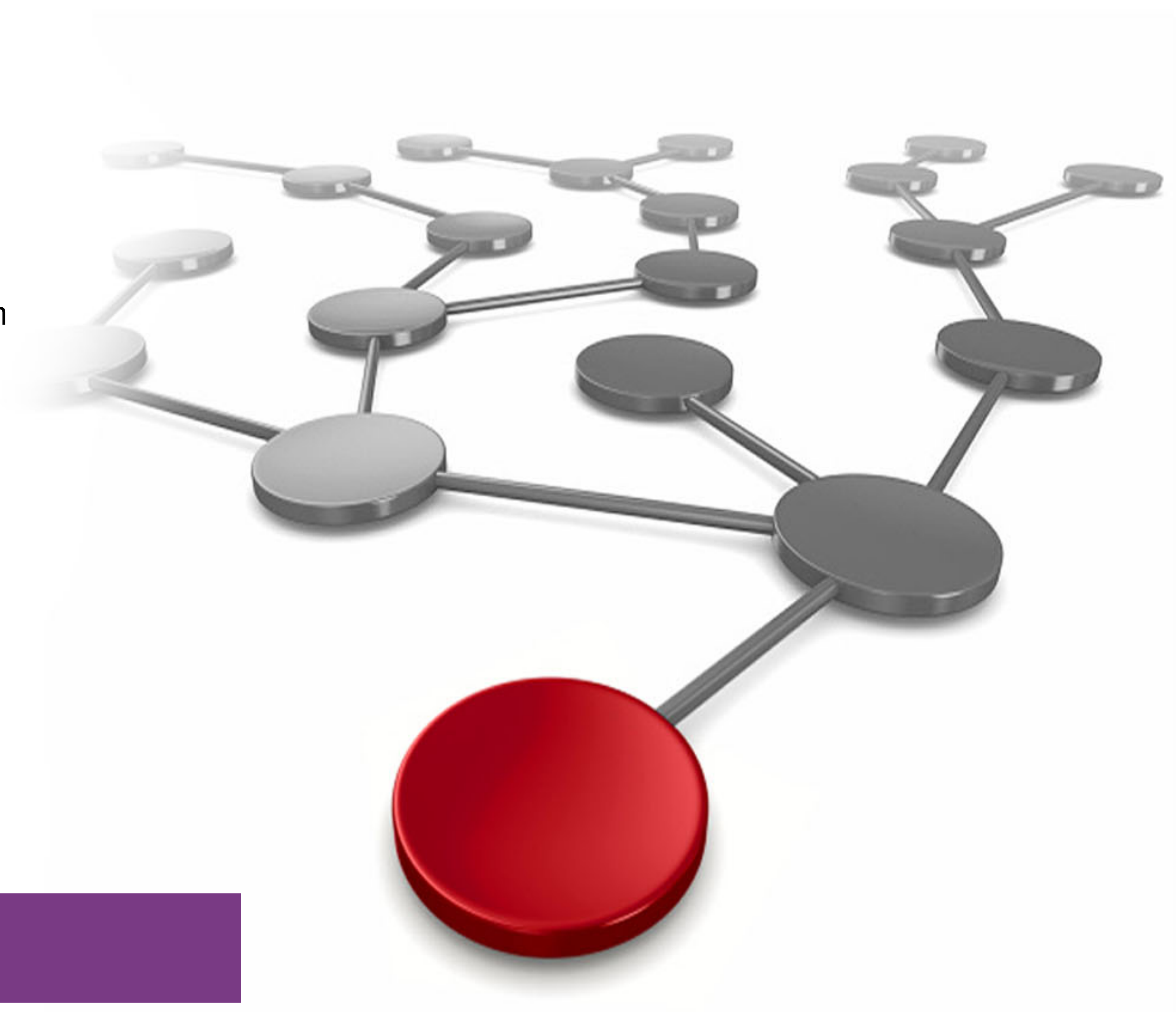
Thomas Ploski

Stephen Solewin

Leandro Torolho

Alexander Watson

Jon Tate



Storage

IBM

Redbooks

International Technical Support Organization

IBM FlashSystem 9100 Architecture, Performance, and Implementation

March 2019

SG24-8425-00

Note: Before using this information and the product it supports, read the information in “Notices” on page ix.

First Edition (March 2019)

This edition applies only to the hardware and software products and features described and documented in this book.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION 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. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

Preface

IBM® FlashSystem 9100 combines the performance of flash and Non-Volatile Memory Express (NVMe) with the reliability and innovation of IBM FlashCore® technology and the rich features of IBM Spectrum™ Virtualize — all in a powerful 2U storage system. Providing intensive, data-driven, multi-cloud storage capacity, FlashSystem 9100 is deeply integrated with the software-defined capabilities of IBM Spectrum Storage™ enabling you to easily add in the multi-cloud solutions that best support your business.

This IBM Redbooks® publication describes the product features, planning steps, architecture, installation, configuration, and hints and tips.

Authors

This book was produced by a team of specialists from around the world working at IBM Houston.

Andrew Greenfield is an IBM Global Engineer based in Phoenix, Arizona. He holds numerous technical certifications from Cisco, Microsoft, and IBM. He is also responsible for many of the photos and videos that are featured in various IBM Redbooks publications and YouTube videos. Andrew brings over 24 years of data center experience inside the Fortune 100 to the IBM team. He graduated with Honors, Magna c. Laude, from the University of Michigan, Ann Arbor. Andrew has also written many earlier IBM FlashSystem® A9000 and IBM XIV® Gen3 Redbooks publications.

Jon Herd is an IBM Storage Technical Advisor working for the ESCC, Germany. He covers the United Kingdom, Ireland, and Sweden, advising customers on a portfolio of IBM storage products, including FlashSystem products. Jon has been with IBM for more than 40 years, and has held various technical roles, including Europe, Middle East, and Africa (EMEA) level 2 support on mainframe servers and technical education development. He has written many IBM Redbooks on the FlashSystems products and is a IBM Redbooks Platinum level author. He holds IBM certifications in Supporting IT Solutions at an expert level, and is an Technical IT Specialist at an experienced level. He is also a certified Chartered Member of the British Computer Society (MBCS - CITP), and a Certified Member of the Institution of Engineering and Technology (MIET).

Corne Lottering is a Storage Client Technical Specialist in the US, focusing on technical sales in Texas, Oklahoma, Louisiana, Arkansas, and Missouri, within the Public Sector industry. He has been with IBM for more than 17 years, and has experience in a wide variety of storage technologies, including the IBM System Storage® DS5000™, IBM DS8000®, IBM Storwize®, XIV, FlashSystems, IBM SAN switches, IBM Tape Systems, and Software Defined Storage software. Since joining IBM, he has fulfilled roles in support, implementation, and pre-sales support across various African and Middle Eastern countries. Corne is the author of several IBM Redbooks publications related to the midrange IBM System Storage DS® Storage Manager range of products, as well as FlashSystem products.

Tony Pacheco is an IBM Technical Advisor based in Raleigh, North Carolina. He works with customers as a Trusted Advisor supporting multiple IBM Storage products, such as FlashSystem, SAN Volume Controller, A9000, XIV, and DS8880. Tony has over 32 years of experience performing numerous roles across IBM organizations, product development, Systems Test, Support, and Client Technical Advisor. He holds a Bachelor of Science Degree in Management and has achieved IBM certification with emphasis on FlashSystem.

Jagadeesh Papaiah is a Corporate Solutions Architect. As a member of the IBM Worldwide FlashSystem Solutions Engineering team, he works with customers, IBM Business Partners, and IBM employees worldwide on consulting, designing, and implementing infrastructure solutions. He holds a Bachelor of Engineering Degree in Industrial and Production Engineering. He has over 23 years of experience in information management, integration architecture, infrastructure services, IT strategy & architecture, and solution design.

Thomas Ploski works in the IBM Systems Client Care organization as a Storage Technical Advisor located in Tucson, Arizona. Tom has more than 38 years of experience with IBM. Before joining the Storage Technical Advisor team in 2015, Tom spent 30 years in storage development and test. Tom holds a Bachelor of Science in Electrical Engineering from the University of Maryland.

Stephen Solewin is a Storage Solutions Architect in Tucson, Arizona. He spends his time helping customers create solutions using FlashSystems products, educating the field, creating demonstrations, and technology previews, among other things. He has 22 years of experience working on IBM storage, including IBM Spectrum Virtualize, LTO, Enterprise Disk, and SAN products. He holds a BS degree in Electrical Engineering from the University of Arizona, where he graduated with honors.

Leandro Torolho is a Storage Client Technical Specialist for US Public Market (West). Before joining the technical sales team in 2015, he worked as a SAN/Storage subject matter expert (SME) for several international clients. Leandro is an IBM Certified IT Specialist and holds a Bachelor's degree in Computer Science, as well as a post graduate degree in Computer Networks. He has 11 years of experience in storage services and support, and is also a Certified Distinguished IT Specialist by The Open Group.

Alexander Watson is a FlashSystem Product Engineer with 5 years of experience with FlashSystems. He is a Subject Matter Expert on IBM system storage products and SAN switches. He has over twenty years of experience in planning, managing, designing, implementing, problem analysis, and tuning of storage systems and SAN environments. He has worked at IBM for eighteen years. His areas of expertise include IBM FlashSystems, IBM Storage solutions, SAN fabric networking, and Open System Storage I/O performance. Al has been a co-author of more than fifteen IBM Redbooks and IBM Redpapers™ publications.

Jon Tate is a Project Manager for IBM System Storage SAN Solutions at the ITSO, San Jose Center. Before joining the ITSO in 1999, he worked in the IBM Technical Support Center, providing Level 2/3 support for IBM mainframe storage products. Jon has 32 years of experience in storage software and management, services, and support. He is an IBM Certified IT Specialist, an IBM SAN Certified Specialist, and is Project Management Professional (PMP) certified. He is also the UK Chairman of the Storage Networking Industry Association (SNIA).

Thanks to the following people for their contributions to this project:

Alex Ainscow
Dave Gimpl
Shelly Howrigon
Richard Mawson
Claudette Mital
Michael Nealon
Long Nguyen
Evelyn Perez
Jon Short
Matt Smith

Now you can become a published author, too

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time. Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

IBM FlashSystem 9100 introduction

This chapter introduces the IBM FlashSystem 9100 (FS9100) storage system and its key features, benefits, and technology.

This chapter includes the following topics:

- IBM FlashSystem 9100 high-level features
- Integration with different environments
- Why FlashCore matters
- Clustering rules and upgrades
- Migration of V9000 storage
- Advanced software features
- IBM HyperSwap
- Licensing

1.1 IBM FlashSystem 9100 high-level features

This IBM Redbooks publication describes IBM FlashSystem 9100, which is a comprehensive all-flash, NVMe enabled, enterprise storage solution that delivers the full capabilities of IBM FlashCore technology. In addition, it provides a rich set of software-defined storage features, including data reductions, de-duplication, dynamic tiering, thin provisioning, snapshots, cloning, replication, data copy services, and IBM HyperSwap® for high availability. Scale out, scale up configurations further enhance not only the capacity but also the throughput, giving even better availability.

The success or failure of businesses often depends on how well organizations use their data assets for competitive advantage. Deeper insights from data require better information technology. As organizations modernize their IT infrastructure to boost innovation, they need a data storage system that can keep pace with highly virtualized environments, cloud computing, mobile and social systems of engagement, and in-depth, real-time analytics.

Making the correct decision on storage investment is critical. Organizations must have enough storage performance and agility to innovate because they need to implement cloud-based IT services, deploy virtual desktop infrastructure, enhance fraud detection, and use new analytics capabilities. At the same time, future storage investments must lower IT infrastructure costs while helping organizations to derive the greatest possible value from their data assets.

IBM FlashSystem storage solutions can accelerate the transformation of the modern organizations into an IBM Cognitive Business®. IBM FlashSystem all-flash storage arrays are purpose-engineered to support the organization’s active data sets. FlashSystem solutions offer a broad range of industry-leading storage virtualization and data management features that can provide improved storage system performance, efficiency, and reliability. Even better, FlashSystem can be less expensive than conventional enterprise storage solutions.

With the release of IBM FlashSystem 9100 Software V8.2, extra functions and features are available, including support for new and more powerful NVMe based IBM FlashCore Modules (FCM) within the control enclosure. Software features added include GUI enhancements, a new dashboard, remote support assistance, data deduplication and Storage Insights configuration.

Figure 1 shows the IBM FlashSystem 9100 Control Enclosure with one of the IBM NVMe drives partially removed.

Figure 1   IBM FlashSystem 9100 control enclosure with one NVMe drive partially removed.

The IBM FlashSystem 9100 system has two different types of enclosures: control enclosures and expansion enclosures.

- A *control enclosure* manages your storage systems, communicates with the host, and manages interfaces. In addition, it can also house up to 24 NVMe capable flash drives. These drives can be either industry-standard NVMe type or the exclusive IBM NVMe FlashCore Modules (FCM).
- An *expansion enclosure* enables you to increase the available capacity of the IBM FlashSystem 9100 cluster. it communicates with the control enclosure via a dual pair of 12 Gbps SAS connections. These expansion enclosures can house a large number of flash (SSD) SAS type drives, depending on which model of enclosure is ordered.

1.1.1 Control enclosures

Each control enclosure can have multiple attached expansion enclosures, which expands the available capacity of the whole system. The IBM FlashSystem 9100 system supports up to four control enclosures and up to two chains of SAS expansion enclosures per control enclosure.

The IBM FlashSystem 9100 control enclosure supports up to 24 NVMe capable flash drives in a 2U high form factor.

There are two standard models of IBM FlashSystem 9100: 9110-AF7 and 9150-AF8.

There are also two utility models of the IBM FlashSystem 9100: the 9110-UF7 and 9150-UF8.

Note: The IBM 9848-UF7 and 9150-UF8 are the IBM FlashSystem 9110 with a three-year warranty, to be utilized in the Storage Utility Offering space. These models are physically and functionally identical to the IBM FlashSystem 9848-AF7 and AF8 respectively, with the exception of target configurations and variable capacity billing.

The variable capacity billing uses IBM Spectrum Control™ Storage Insights to monitor the system usage, allowing allocated storage usage above a base subscription rate to be billed per TB, per month. Allocated storage is identified as storage that is allocated to a specific host (and unusable to other hosts), whether data is written or not. For thin-provisioning, the data that is actually written is considered used. For thick provisioning, total allocated volume space is considered used.

1.1.2 Expansion enclosures

New SAS-based small form factor (SFF) and large form factor (LFF) expansion enclosures support flash-only MDisks in a storage pool, which can be used for IBM Easy Tier®:

- The new IBM FlashSystem 9100 SFF expansion enclosure Model AAF offers new tiering options with solid-state drive (SSD flash drives). Up to 480 drives of serial-attached SCSI (SAS) expansions are supported per IBM FlashSystem 9100 control enclosure. The expansion enclosure is 2U high.
- The new IBM FlashSystem 9100 LFF expansion enclosure Model A9F offers new tiering options with solid-state drive (SSD flash drives). Up to 736 drives of serial-attached SCSI (SAS) expansions are supported per IBM FlashSystem 9100 control enclosure. The expansion enclosure is 5U high.

The IBM FlashSystem 9100 control enclosure can be recognized by the nomenclature IBM FlashSystem 9100 on the left hand side of the bezel cover which covers the rack mounting screws.

Figure 2 shows the IBM FlashSystem 9100 bezel and NVMe drive description.

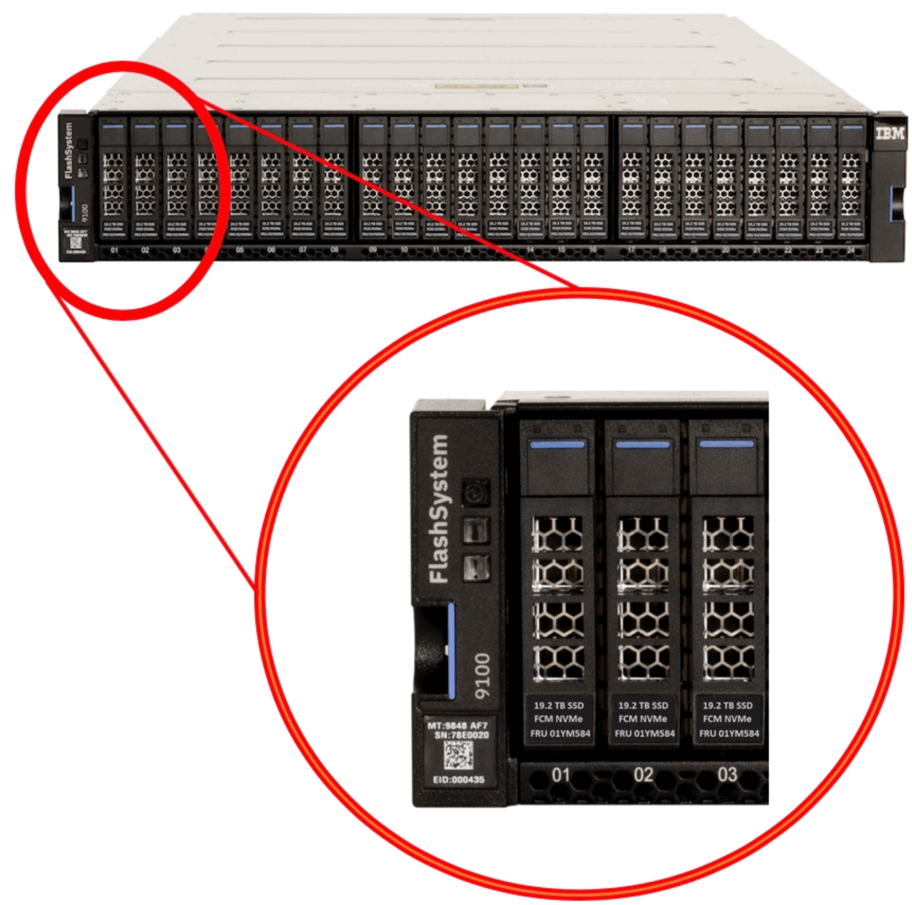


Figure 2   IBM FlashSystem 9100 bezel and FCM description.

Labeling on the NVMe drive itself gives the drive type, capacity, the type of drive and the FRU number. The example shown in Figure 2 is the IBM 19.2 TB NVMe FlashCore Module type.

The FS9110 has a total of 32 cores (16 per canister) while the 9150 has 56 cores (28 per canister).

The FS9100 supports six different memory configurations as shown in Table 1-1.

Table 1-1   FS9100 memory configurations

Memory per Canister	Memory per Control Enclosure
64 GB	128 GB
128 GB	256 GB
192 GB	384 GB

Memory per Canister	Memory per Control Enclosure
384 GB	768 GB
576 GB	1152 GB
768 GB	1536 GB

Note: FS9100 refers to both the FS9110 (Model AF7) and the FS9150 (model AF8). If a feature or function is specific to one of the models, then FS9110 or FS9150 will be used.

The FS9100 supports NVMe attached flash drives, both the IBM Flash Core Modules (FCM) and commercial off the shelf (COTS) SSDs. The IBM FCMs support hardware compression at line data rates. IBM offers the FCMs in three capacities: 4.8 TB, 9.6 TB and 19.2 TB, Standard NVMe SSDs are offered in four capacities, 1.92 TB, 3.84 TB, 7.68 TB, and 15.36 TB.

The FS9100 also supports additional capacity in serial-attached SCSI (SAS) expansion enclosures. Up to 20 2U enclosures (Model AFF) or up to 8 5U enclosures (Model AF9) can be attached. Only SAS SSD drives are supported in the AFF and AF9 enclosures.

Host interface support includes 8 gigabit (Gb) and 16 Gb Fibre Channel (FC), and 10 Gb Fibre Channel over Ethernet (FCoE) or Internet Small Computer System Interface (iSCSI). Advanced Encryption Standard (AES) 256 hardware-based encryption adds to the rich feature set.

The IBM FlashSystem 9100 includes a single easy-to-use management graphical user interface (GUI) to help you monitor, manage, and configure your system.

1.1.3 FlashSystem 9100 utility models UF7 and UF8

IBM FlashSystem 9100 utility models UF7 and UF8 provide a variable capacity storage offering. These models offer a fixed capacity, with a base subscription of 35% of the total capacity.

IBM Storage Insights (free edition or pro) is used to monitor system usage, and capacity used beyond the base 35% is billed on a per month, per terabyte basis. This enables you to grow or shrink usage, and only pay for the configured capacity.

IBM FlashSystem utility models are provided for customers who can benefit from a variable capacity system, where billing is based only on actually provisioned space. The hardware is leased through IBM Global Finance on a three-year lease, which entitles the customer to utilize up to 35% of the total system capacity at no additional cost. If storage needs increase beyond that 35% capacity, usage is billed based on the average daily provisioned capacity per terabyte, per month, on a quarterly basis.

1.2 Integration with different environments

The IBM FlashSystem 9100 is integrated with Windows HyperV, through Microsoft Off-load Data Transfer (ODX) features, and with VMware environments through vSphere Storage API Array Integration (VAAI) and vSphere APIs for Storage Awareness (VASA). it also provides a REST API and a full function command line interface (CLI).

For more information about support restrictions and limitations, go to IBM Support.

1.3 Why FlashCore matters

Solid state storage is widely used, both in the data center, as well as in consumer electronics. One of the key distinctions is the efficiency of the technology that is created around this widely used storage media.

Solid state storage becomes slower and less reliable (fewer program/erase cycles before the bit error rate (BER) exceeds the ability to recover bits) as capacity grows. IBM FlashCore technology uses many features to mitigate or completely hide these effects. Health binning, heat segregation, variable stripe RAID, strong error correction and voltage threshold calibration are some of the technologies IBM has created to ensure that FlashCore Modules provide the density, performance, and longevity demanded by enterprise solutions.

SSDs that do not include the IBM FlashCore technology cannot offer the same reliability, performance, and longevity that FlashCore enables.

1.4 Clustering rules and upgrades

The IBM FlashSystem 9100 can be clustered with up to four FS9100 enclosures, using four I/O groups.

The FS9100 also allows for clustering with the IBM Storwize V7000 with a maximum of four enclosures total, if done following these guidelines:

- Both systems must have the same level of V8.2 code installed to be able to cluster.
- To cluster the Storwize V7000, it must have an all-inclusive license.
- When clustered, the clustered system, presents itself as a FlashSystem 9100.
- Migration must be done through additional I/O Groups.
- The default layer is storage, but a replication layer is supported.

Note: At the time of writing the supported release for clustering was V8.2.1.

1.5 Migration of V9000 storage

At first release, the migration of V9000 to the FS9100 requires host support of a remote copy or mirroring function (for example, IBM AIX® Logical Volume Manager (LVM)).

1.5.1 FlashSystem V9000 flash enclosure re-purposed

Future plans are being worked for the V9000 flash enclosures to be capable of re-purposing as an external flash enclosure which will be recognized by the 9100 as an already licensed storage requiring no additional External Storage license key to be purchased.

1.5.2 IBM FlashSystem 9100: IBM Tier 1 storage

The market for all-flash arrays is saturated with products aiming to replace enterprise storage arrays but consistently failing to deliver the breadth of data lifecycle, storage services, or the scalability delivered by incumbent solutions. Alternatively, hybrid arrays loaded with storage services consistently lack the low latency and performance scalability delivered by all-flash arrays.

The IBM FlashSystem 9100 merges IBM software-defined storage with the scalable performance of IBM FlashSystem storage to accelerate critical business applications and decrease data center costs simultaneously. As a result, your organization can gain a competitive advantage through a more flexible, responsive, and efficient storage environment.

1.6 Advanced software features

The IBM FlashSystem FS9100 can function as a feature-rich, software-defined storage layer that virtualizes and extends the functionality of all managed storage. These include data reduction, dynamic tiering, copy services, and high-availability configurations. In this capacity, it acts as the virtualization layer between the host and other external storage systems, providing flexibility and extending functionality to the virtualized external storage capacity.

1.6.1 Advanced functions for data reduction

The IBM FlashSystem FS9100 employs several features to assist with the reduction of data and the ability to increase its effective capacity.

IBM Real-time Compression

With the FS9100 with FCMs, hardware compression is built in. For other drives used with the FS9100, the IBM Real-time Compression™ within the IBM FS9100 addresses this requirement of storage data reduction. This is handled without sacrificing performance by the use of dedicated compression acceleration hardware. It does so by implementing a purpose-built technology called Real-time Compression using the Random Access Compression Engine (RACE).

Customers can expect data reduction and effective capacity increases of up to 5x for relevant data sets. When the initial virtual disk (VDisk) volume, also known as the *logical unit number* (LUN), is created and a thin provisioned volume is allocated, then as data is stored into the VDisk it is compressed in real time.

Data reduction pools

Data reduction pools (DRP) represent a significant enhancement to the storage pool concept. This is because the virtualization layer is primarily a simple layer that executes the task of lookups between virtual and physical extents. Now with the introduction of data reduction technology, compression, and deduplication, it has become more of a requirement to have an uncomplicated way to stay “thin”.

Deduplication

Deduplication can be configured with thin-provisioned and compressed volumes in data reduction pools for added capacity savings. The deduplication process identifies unique chunks of data, or byte patterns, and stores a signature of the chunk for reference when writing new data chunks. If the new chunk’s signature matches an existing signature, the new chunk is replaced with a small reference that points to the stored chunk. The same byte pattern may occur many times, resulting in the amount of data that must be stored being greatly reduced.

Thin provisioning

In a shared storage environment, thin provisioning is a method for optimizing the use of available storage. It relies on allocation of blocks of data on demand versus the traditional method of allocating all of the blocks up front.

This methodology eliminates almost all white space, which helps avoid the poor usage rates (often as low as 10%) that occur in the traditional storage allocation method. Traditionally, large pools of storage capacity are allocated to individual servers, but remain unused (not written to).

Thin-provisioned flash copies

Thin-provisioned IBM FlashCopy® (or snapshot function in the GUI) uses disk space only when updates are made to the source or target data, and not for the entire capacity of a volume copy.

1.6.2 Data migration

The IBM FlashSystem 9100 provides online volume migration while applications are running, which is possibly the greatest single benefit for storage virtualization. This capability enables data to be migrated on and between the underlying storage subsystems without any effect on the servers and applications. In fact, this migration is performed without the knowledge of the servers and applications that it even occurred. The IBM FlashSystem 9100 delivers these functions in a homogeneous way on a scalable and highly available platform over any attached storage and to any attached server.

1.6.3 Advanced copy services

Advanced copy services are a class of functionality within storage arrays and storage devices that enable various forms of block-level data duplication locally or remotely. By using advanced copy services, you can make mirror images of part or all of your data eventually between distant sites. Copy services functions are implemented within an IBM FlashSystem 9100 (FlashCopy and Image Mode Migration), or between one IBM FlashSystem 9100 and another IBM FlashSystem 9100 in three different modes:

- Metro Mirror
- Global Mirror
- Global Mirror with Change Volumes

Remote replication can be implemented using both Fibre Channel and Internet Protocol (IP) network methodologies.

FlashCopy

FlashCopy is the IBM branded name for point-in-time copy, which is sometimes called time-zero (T0) copy. This function makes a copy of the blocks on a source volume and can duplicate them on 1 - 256 target volumes.

Remote mirroring

The three remote mirroring modes are implemented at the volume layer within the IBM FlashSystem 9100. They are collectively referred to as remote copy capabilities. In general, the purpose of these functions is to maintain two copies of data. Often, but not necessarily, the two copies are separated by distance. The remote copy can be maintained in one of two modes: synchronous or asynchronous, with a third asynchronous variant:

- *Metro Mirror* is the IBM branded term for synchronous remote copy function.

- *Global Mirror* is the IBM branded term for the asynchronous remote copy function.
- *Global Mirror with Change Volumes* is the IBM branded term for the asynchronous remote copy of a locally and remotely created FlashCopy.

1.6.4 External virtualization

The IBM FlashSystem 9100 includes data virtualization technology to help insulate hosts, hypervisors, and applications from physical storage. This enables them to run without disruption, even when changes are made to the underlying storage infrastructure. The IBM FlashSystem 9100 functions benefit all virtualized storage.

For example, Easy Tier and Real-time Compression help improve performance and increase effective capacity, where high-performance thin provisioning helps automate provisioning. These benefits can help extend the useful life of existing storage assets, reducing costs. Additionally, because these functions are integrated into the IBM FlashSystem 9100, they can operate smoothly together, reducing management effort.

1.6.5 Easy Tier

Easy Tier is a performance function that automatically migrates or moves extents of a volume to or from one storage tier to another storage tier. With IBM FlashSystem 9100, Easy Tier supports four kinds of storage tiers.

Consider the following information about Easy Tier:

- Easy Tier monitors the host volume I/O activity as extents are read, and migrates the most active extents to higher performing tiers.
- The monitoring function of Easy Tier is continual but, in general, extents are migrated over a 24-hour period. As extent activity cools, Easy Tier moves extents to slower performing tiers.
- Easy Tier creates a migration plan that organizes its activity to decide how to move extents. This plan can also be used to predict how extents will be migrated.

1.7 IBM HyperSwap

HyperSwap capability enables each volume to be presented by two IBM FlashSystem 9100 I/O groups. The configuration tolerates combinations of node and site failures, using host multipathing driver based on the one that is available for the IBM FlashSystem 9100. IBM FlashSystem 9100 provides GUI management of the HyperSwap function.

1.8 Licensing

The base license that is provided with your system includes the use of its basic functions. However, extra licenses can be purchased to expand the capabilities of your system. Administrators are responsible for purchasing extra licenses and configuring the systems within the license agreement, which includes configuring the settings of each licensed function on the system.

2

IBM FlashSystem 9100 architecture

This chapter describes the FlashSystem 9100 architectural components, available models, enclosure, software features, and licensing options.

In this chapter we cover the following topics:

- FS9100 hardware components
- FS9100 Control Enclosure
- FlashCore Module and NVMe drives
- NVMe and adapter support
- Software features and licensing
- Data Protection on FS9100

2.1 FS9100 hardware components

Each FlashSystem 9100 consists of a control enclosure and IBM FlashCore module drives.The control enclosure is the storage server that runs the IBM Spectrum Virtualize software that controls and provides features to store and manage data on the FlashCore module or industry-standard NVMe drives. See Figure 2-1.

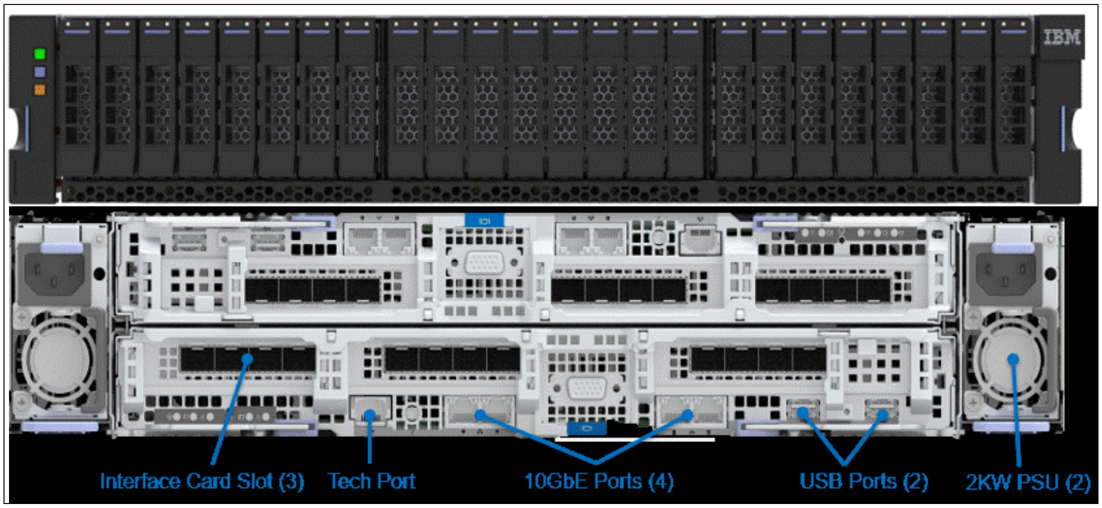


Figure 2-1 FS9100

Following are the core IBM FlashSystem FS9100 components:

- FlashSystem FS9100 control enclosure:
  - Power supply units
  - Battery modules
  - Fan modules
  - Interface cards
  - Skylake CPUs and Memory Slots
- FlashSystem FlashCore modules:
- FlashSystem FS9100 expansion enclosures (SAS attached)

2.2 FS9100 Control Enclosure

FS9100 is a 2U model and can support up to 24 IBM FCMs (IBM built NVMe drives) with hardware compression and encryption or industry-standard NVMe drives of various capacities. FS9100 can be configured with up to 1.5 TB of cache.

Figure 2-2 shows the internal architecture.

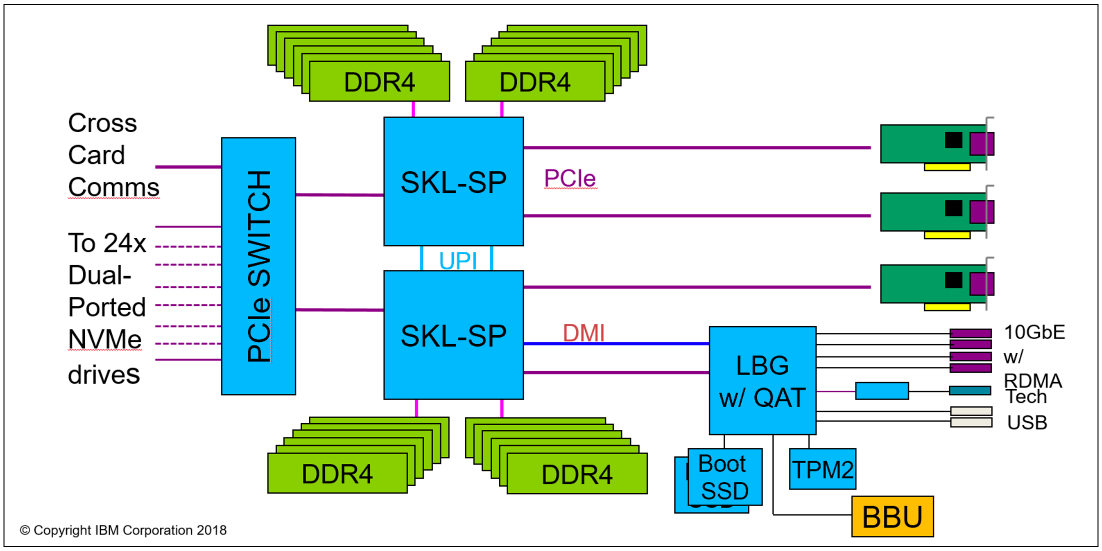


Figure 2-2 Internal Architecture

A FlashSystem 9100 clustered system can contain up to four FlashSystem 9100 systems and up to 3,040 drives. FlashSystem 9100 systems can be added into existing clustered systems that include Storwize V7000 systems.

Figure 2-3 shows the enclosure rear view.

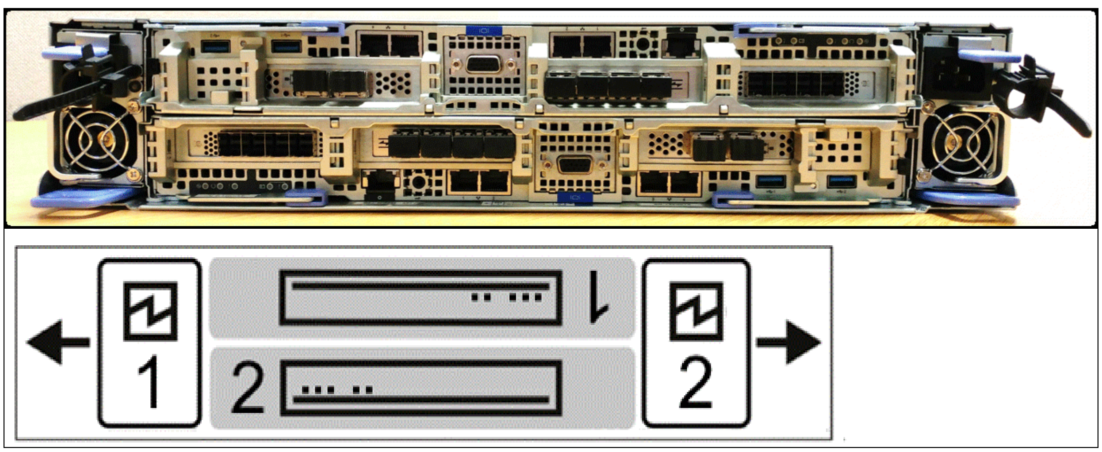


Figure 2-3 Enclosure rear view

As shown in Figure 2-3 the FS9100 enclosure consists of redundant power supply units, node canisters and fan modules to provide redundancy and high availability.

Figure 2-4 on page 14 shows a picture of internal hardware components of a node canister. To the left of the picture is the front of the canister where fan modules and battery backup are located, followed by two Skylake CPUs and memory DIMM slots and PCIe risers for adapters on the right.

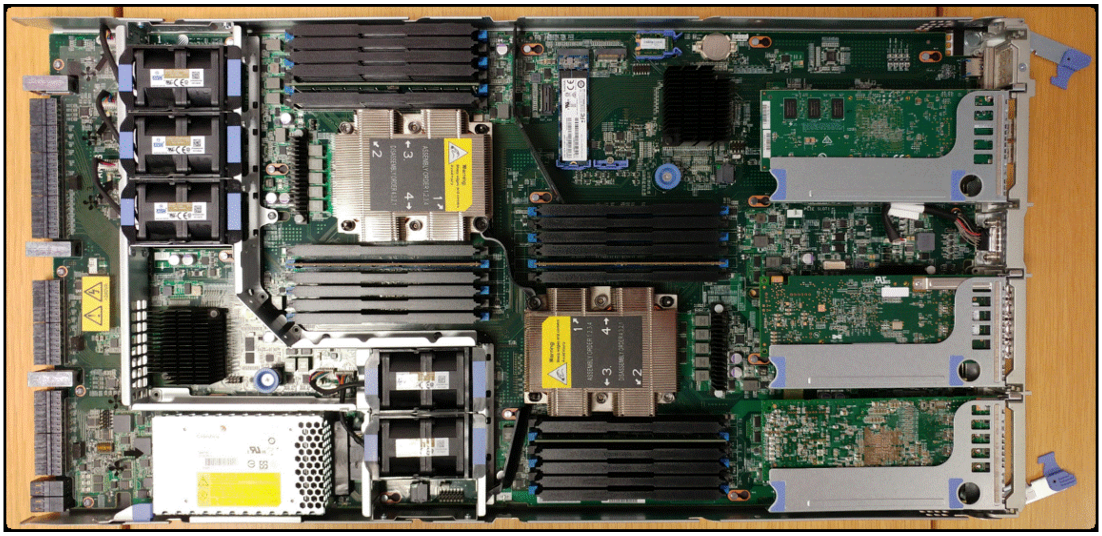


Figure 2-4 Internal hardware components

2.2.1 Model 9110 Control Enclosure AF7

FS9100 model 9110 offers:

- 2 Node canisters with 4 x 8 cores 1.7 GHz Skylake CPUs with compression assist up to 40 Gbps
- Cache options from 128 GB (64 GB per canister) to 1.5 TB (768 GB per canister)
- Eight 10 Gb Ethernet ports standard for iSCSI connectivity.
- 16 Gb FC, 25 Gb Ethernet, and 10 Gb Ethernet ports for FC and iSCSI connectivity
- 12 Gb SAS ports for expansion enclosure attachment
- Twenty-four slots for 2.5-inch NVMe flash drives
- 2U, 19-inch rack mount enclosure with AC power supplies
- 1 Boot drive

2.2.2 Model 9150 Control Enclosure AF9

FS9100 model 9150 offers: 4 x14 cores 2.2 GHz Skylake CPUs with dual boot drive and Other hardware features and software functions are common to both models of FS9100.

- 2 node canisters, each with 4 x14 cores 2.2 GHz Skylake CPUs with compression assist up to 100 Gbps
- Cache options from 128 GB (64 GB per canister) to 1.5 TB (768 GB per canister)
- Eight 10 Gb Ethernet ports standard for iSCSI connectivity.
- 16 Gb FC, 25 Gb Ethernet, and 10 Gb Ethernet ports for FC and iSCSI connectivity
- 12 Gb SAS ports for expansion enclosure attachment
- Twenty-four slots for 2.5-inch NVMe flash drives
- 2U, 19-inch rack mount enclosure with AC power supplies
- 2 Boot drive

2.2.3 Model 9150 expansion enclosure models AFF and AF9

All Flash expansions models AFF and AF9 can be attached to FS9100 control enclosure using the SAS adapter.

Model AFF

Model AFF holds up to 24 2.5 inch SAS flash drives in a 2U, 19-inch rack mount enclosure. Intermix of capacity drives are allowed in any drive slot and up to 20 AFF enclosures can be attached to the Control enclosure(490) drives.

Model AF9

Model A9F holds up to 92 3.5 inch SAS flash drives in a 5U, 19-inch rack mount enclosure. Intermix of capacity drives are allowed in any drive slot and up to 8 A9F enclosures can be attached to the Control enclosure(736) drives.

2.2.4 FlashSystem 9100 Utility Models UF7 and UF8

IBM FlashSystem9100 utility models UF7 and UF8 provide a variable capacity storage offering. These models offer a fixed capacity, with a base subscription of 35% of the total capacity.

IBM Storage Insights (free edition or pro) is used to monitor system usage, and capacity used beyond the base 35% is billed on a per-month, per-terabyte basis. This enables you to grow or shrink usage, and only pay for the configured capacity.

IBM FlashSystem utility models are provided for customers who can benefit from a variable capacity system, where billing is based only on actually provisioned space. The hardware is leased through IBM Global Finance on a three-year lease, which entitles the customer to utilize up to 35% of the total system capacity at no additional cost. If storage needs increase beyond that 35% capacity, usage is billed based on the average daily provisioned capacity per terabyte, per month, on a quarterly basis.

Example: Total system capacity of 115 TB

A customer has an IBM FlashSystem 9100 utility model with 4.8 TB NVMe drives, for a total system capacity of 115 TB. The base subscription for such a system is 40.25 TB. During the months where the average daily usage is below 40.25 TB, there is no additional billing.

The system will monitor daily provisioned capacity and will average those daily usage rates over the month term. The result is the average daily usage for the month.

If a customer uses 45 TB, 42.5 TB, and 50 TB in three consecutive months, Storage Insights will calculate the overage as shown in Table 1, rounding to the nearest terabyte.

Table 1 Billing calculations based on customer usage

Average Daily	Base	Overage	To be Billed
45 TB	40.25 TB	4.75 TB	5 TB
42.5 TB	40.25 TB	2.25 TB	2 TB
50 TB	40.25 TB	9.75 TB	10 TB

The total capacity billed at the end of the quarter will be 17 TB per month in this example.

Flash drive expansions may be ordered with the system, in all supported configurations.

Table 2 shows the feature codes associated with the UF7 and UF8 utility model billing.

Table 2   9100 UF7 and UF8 utility model billing feature codes

Feature Code	Description
# AE00	Variable Usage 1 TB per month
# AE01	Variable Usage 10 TB per month
# AE02	Variable Usage 100 TB per month

These features are used to purchase the variable capacity used in the utility models. The features (feature code AE00, AE01, AE02:) provide TBs of capacity beyond the base subscription on the system. Usage is based on the average capacity used, per month. The total of the prior three months' usage should be totaled, and the corresponding number of AE00, AE01, and AE02 features ordered quarterly.

2.3 FlashCore Module and NVMe drives

Figure 2-5 shows an IBM FlashCore Module (NVMe) with a capacity of 19.2 TB built using 64-layer TLC flash memory and an Everspin MRAM cache into a U.2 form factor.

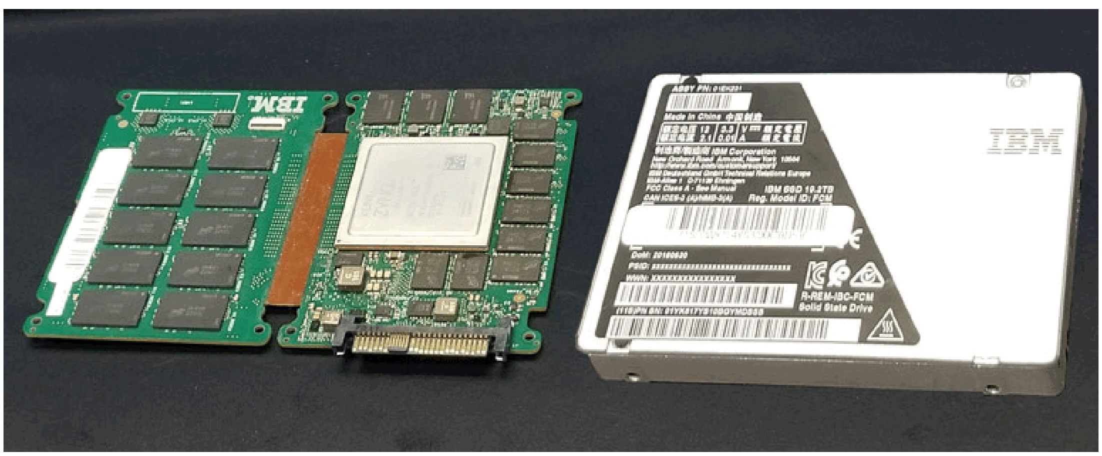


Figure 2-5   FlashCore Module (NVMe)

IBM FCMs (NVMe) are designed for high parallelism and optimized for 3D TLC and updated FPGAs. IBM also enhanced the FCMs by adding read cache to reduce latency on highly compressed pages, and four-plane programming to lower the overall power during writes. FCMs offer hardware-assisted compression up to 3:1, and are FIPS 140-2 complaint.

FCMs carry the IBM patented Variable Stripe RAID™ at the FCM level, and utilizes DRAID to protect data at the system level. VSR and DRAID together optimizes raid rebuilds by offloading rebuilds to DRAID and offers protection against FCM failures.

FCMs on FS9100 can be configured to use 4.8 TB, 9.6 TB, and 19.2 TB.

2.3.1 Industry-standard NVMe drives

FS9100 provides an option to use industry-standard NVMe drives, which are sourced from Samsung and Toshiba and available in the following capacity variations: NVMe 1.92 TB, 3.84 TB, 7.68 TB, and 15.36 TB.

2.4 NVMe and adapter support

NVMe is a NUMA-optimized, high-performance and highly scalable storage protocol designed to access non-volatile storage media using a host PCIe bus. NVMe uses low latency and available parallelism, and reduces I/O overheads. NVMe supports multiple I/O queues up to 64K queues and each queue can support up to 64K entries. Legacy SAS and SATA supports single queue with only 254 and 32 entries, and uses many more CPU cycles to access data. NVMe handles more workload for the same infrastructure footprint.

NVMe over Fabrics (NVMe-oF) is a technology specification designed to enable nonvolatile memory express message-based commands to transfer data between a host computer and a target solid-state storage device or system. Data is transferred over a network, such as Ethernet, Fibre Channel (FC), or InfiniBand.

2.4.1 Support for host platforms, adapters, and switches

The following host platforms, adapters, and switches are supported:

- Host Platforms:
  - RHEL 7.4
  - CentOS 7.4
  - ESX 6.7
- Transport Protocols:
  - Fibre Channel 4 x 16 Gb
  - iSCSI 8 x 10 Gb
  - Ethernet 2 x 1 Gb System management
  - iSER over RoCE with 2 x 25 Gb Mellanox ConnectX4-LX
  - iSER over iWARP with 2 x 25 Gb Chelsio T6 adapters
  - SAS expansion 2 x 12 Gb
- Switches:
  - Cisco 3232C
  - Arista 7060
  - Dell

2.5 Software features and licensing

Figure 2-6 shows the software offerings orderable with FlashSystem 9100.

Ordering	BASE	OPTIONAL	OPTIONAL	OPTIONAL
Software Offerings Orderable with FlashSystem 9100	Multi-Cloud Enabled Base Software for FlashSystem 9100	IBM FlashSystem 9100 Solution for Data Reuse, Protection and Efficiency (per TB)	IBM FlashSystem 9100 Solution for Business Continuity and Data Reuse (per TB)	IBM FlashSystem 9100 Solution for Private Cloud Flexibility, and Data Protection (per TB)
Products				
Spectrum Storage Insights	✓			
Spectrum Connect	✓			
Spectrum Virtualize	✓			
Spectrum Protect Plus	✓ (5TB Starter Kit)	✓		
Spectrum CDM	✓ (5TB Starter Kit)	✓	✓	✓
Spectrum Virtualize for Public Cloud	✓ (5TB Starter Kit)		✓	
Blueprint	✓	✓	✓	Spectrum Access
Lab Services (Post GA)		✓ (optional)	✓ (optional)	✓ (optional)

Figure 2-6 FS9100 software included for base and optional licensing

2.5.1 IBM Spectrum Virtualize for IBM FlashSystem 9100

FS9100 uses IBM Spectrum Virtualize™ software that combines a variety of software-defined functionality for Flash Storage to manage data:

- Deduplication
- Compression
- Thin provisioning
- Easy Tier (automatic and dynamic tiering)
- Encryption for internal and virtualized external storage
- SCSI Unmap
- HyperSwap (high availability active-active)
- FlashCopy (snapshot)
- Remote data replication

For additional information about IBM FlashSystem 9100 functional capabilities and software, see *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933.

2.5.2 IBM Multi-Cloud starter software for FlashSystem 9100

FS9100 Multi-cloud starter software with IBM Spectrum Virtualize includes the following software stack

- IBM Spectrum Protect™ Plus
- IBM Spectrum Copy Data Management
- IBM Spectrum Virtualize for Public Cloud

The software bundle is included with FlashSystem 9100 control enclosures, and enables you to develop a multi-cloud strategy to harness the power of data. It increases the flexibility to manage data through choice, security, and protection. Licensing includes 5 TB of managed capacity and provides a base to migrate to a complete IBM FlashSystem 9100 Multi-Cloud Solution by following an IBM validated blueprint.

2.5.3 IBM FlashSystem 9100 Multi-Cloud solutions

FlashSystem 9100 Multi-Cloud solutions are a set of proven solutions designed to support today's data-driven, multi-cloud architectures. These are NVMe-ready, cloud-enabled software solutions that are validated according to a set of multi-cloud blueprints. These solutions enable modernization of infrastructure by expanding IBM FlashSystem 9100 to be used for multi-cloud architectures that include data protection, business continuity, and data reuse.

IBM FlashSystem 9100 Multi-Cloud Solution for Data Reuse, Protection, and Efficiency

This solution is comprised of IBM Spectrum Protect Plus and IBM Spectrum Copy Data Management, and is designed to secure and reuse your company's most precious asset, protect your data, and drive secondary data efficiencies within multi-cloud environments.

IBM FlashSystem 9100 Multi-Cloud Solution for Business Continuity and Data Reuse

This solution is comprised of IBM Spectrum Virtualize for Public Cloud and IBM Spectrum Copy Data Management. Through the use of IBM Spectrum Virtualize for Public Cloud, data can be copied using synchronous or asynchronous real-time replication from FlashSystem 9100 to IBM Cloud™. IBM Spectrum Copy Data Management can be used to create secondary data reuse snapshots of data managed by IBM Spectrum Virtualize for Public Cloud in IBM Cloud.

IBM FlashSystem 9100 Solution for Private Cloud Flexibility and Data Protection

This solution is comprised of IBM Spectrum Copy Data Management and is designed to simplify and transform multi-cloud environments by combining private cloud management with enabling tools, all managed through a single user interface.

IBM Storage Insights

Cloud-based IBM Storage Insights provides a single dashboard that gives you a clear view of all IBM block storage. It enables predictive analysis and displays real-time and historical charts to monitor performance and capacity. Storage health information enables Customers to focus on areas needing attention.

When IBM support is needed, IBM Storage Insights simplifies uploading logs, speeds resolution with online configuration data, and provides an overview of open tickets all in one place. IBM Storage Insights Pro is a subscription service that provides longer historical views of data, more reporting and optimization options, and supports IBM file and block storage together with EMC VNX and VMAX.

2.5.4 FS9100 high availability

IBM FlashSystem 9100 is designed to offer high system and data availability with the following features:

- HyperSwap support
- Dual-active, intelligent node canisters with mirrored cache
- Dual-port flash drives with automatic drive failure detection and RAID rebuild
- Redundant hardware, including power supplies and fans
- Hot-swappable and customer replaceable components
- Automated path failover support for the data path between the server and the drives

2.6 Data Protection on FS9100

Data protection from NAND chip and controller failures are managed using two IBM technologies: Variable Stripe RAID (VSR) and DRAID. VSR protects failures at the IBM FlashCore modules chip level, and DRAID protects data from failure of IBM FlashCore modules and industry-standard NVMe drives.

2.6.1 Variable Stripe RAID

Variable Stripe RAID is a patented IBM technology that provides data protection at the page, block, or chip level. It eliminates the necessity to replace a whole flash module when a single chip or plane fails. This, in turn, expands the life and endurance of flash modules and reduces considerably maintenance events throughout the life of the system.

For additional information on VSR see *Introducing and Implementing IBM FlashSystem V9000*, SG24-8273.

2.6.2 DRAID

Distributed RAID functionality is managed by IBM Spectrum Virtualize, which enables a storage array to distribute RAID5 or RAID6 to the largest set of drives. For example, on traditional RAID5, if 8 drives were used the data was striped across 7 and the parity was on 8.

DRAID enhanced this method by specifying the stripe width and the number of drives separately. As a result, the setup still has 7 data stripes protected by a parity stripe, but the 8 drives are selected from the larger set. In addition, with distributed sparing, each drive in the array gives up some of its capacity to make a spare instead of an unused spare drive.

The benefit of DRAID is improved rebuild performance. During a drive failure, the data rebuild is done from a larger set of drives, increasing the number of reads. The data is rebuilt to a larger set of distributed sparing drives, which also increases the number of writes as compared to traditional RAID (where reads are done from a smaller set of drives written to a single drive).

DRAID on FS9100

DRAID6 is advised for FS9100, and is the only allowed option from the GUI. DRAID5 is configurable using the CLI. DRAID6 creates spare space across all NVMe SSDs or FCMs on the array and, during failure, the array rebuilds data using the spare space faster than traidional RAID rebuilds.

DRAID Rebuild

The spare area for rebuild on FS9100 is reserved against the physical capacity of the drives. As the rebuild progresses, the data is copied to the remaining drives, increasing the capacity threshold as shown in Figure 2-7.

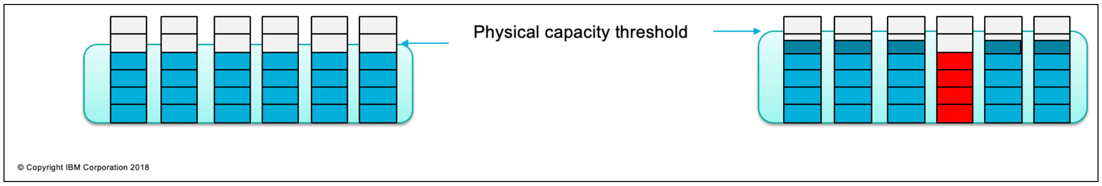


Figure 2-7 Physical capacity threshold

DRAID copyback

DRAID copyback is a similar process to the rebuild process. Upon completion, FS9100 releases the space area by UNMAP-ing the area that was used, as shown in Figure 2-8.

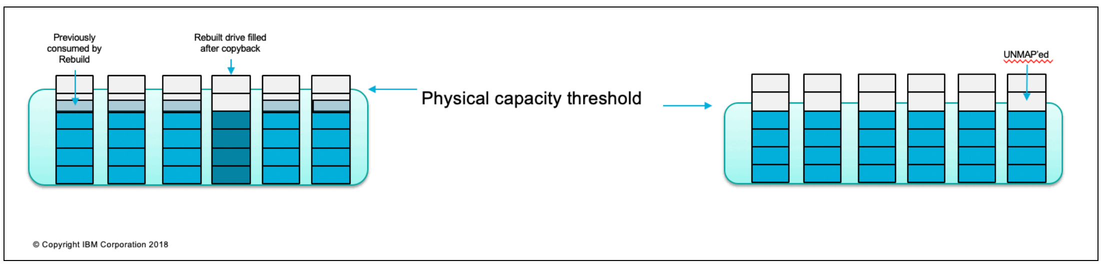


Figure 2-8 DRAID copyback

3

Data reduction and tools

This chapter covers the following topics:

- Compression and deduplication techniques
- Data Reduction Pools inside the FS9100
- RACE compared to Data Reduction Pools
- Data Reduction Pools and Unmap
- Data Reduction Pools with Easy Tier
- Garbage collection
- Data Reduction Pools with deduplication
- Estimating Data Reduction using various tools
- When to use Flash Core Modules or Data Reduction Pools
- General guidelines for performance, capacity, and availability options
- Availability considerations when configuring the FS9100

3.1 Compression and deduplication techniques

In today's modern environment, the need to store ever increasing data and sets of data are constant pressures for storage administrators that can be alleviated by using a combination of data compression and deduplication.

With massive advances in hardware, for example CPU speeds, cores, and RAM, we now can very easily use many methods to reduce the actual footprint of data being stored with minimal performance trade-offs. All of the processes are completely transparent to the host and applications.

The processes ensure the complete integrity of the data and metadata of that I/O stream, so this chapter describes only *lossless* reduction items. This means that all of the data can, and will be, fully decompressed to its original, and full, uncompressed state whenever the Host, VM, or Cluster, requests it from the IBM FlashSystem 9100 array.

While there are other types of compression, they are considered *lossy* because they actually remove parts of the original data stream during the compression process. Therefore, the data can never regain its original information, even when fully decompressed. This type of compression is not used in any IBM storage systems; however, these methods are used frequently for streaming media, such as MP3 and most video streaming services.

The parts of the data that are removed are considered less important to the customer, so although the resulting data is serviceable it is reduced in size and quality. A good example is how a professional Compact Disc of a song sounds compared to an MP3 version of the same song on the same sound system. Similarly, watching a movie in a commercial digital theater is far superior to watching the same movie from an MPEG2, MPEG4, or similar lossy compressed file type.

These differences are critical because it is very important for modern applications, such as SQL, IBM DB2®, or IBM WebSphere®, to be able to read and write their data exactly as they expect it.

> **Important:** Most modern applications, operating systems, and HyperVisors can also perform their own internal compression and even data encryption *before they send the data to the IBM array*. However, *this will drastically reduce* the compression and deduplication rates the array will be able to perform, due to the data being drastically altered and even obfuscated.
>
> This does not affect the performance of the array for various reads or writes, because the array identifies that the data stream has been pre-compressed, or encrypted, and simply store and retrieve the data as it has been presented, without any further data reduction.
>
> The benefits of data reduction and encryption are best realized solely at the array level, because this ensures that the host or VM is operating at peak CPU application performance. It is enefficient to use precious host or application compute cycles to perform the reduction or encryption operations that a storage array does at far faster speeds and efficiencies, especially with regards to data deduplication.
>
> One such example would be that many DB2 volumes and instances across several departments (and across test, development ,and build cycles) could be easily deduplicated using the same FlashSystem FS9100 array. The array can easily recognize similar patterns, and then store only the delta or unique data items.

In summary, there are many ways to accomplish data reduction. This chapter describes the key concepts of compression and deduplication methods that are employed by the FlashSystem 9100 array. It is important to note the order of operations for the I/O flow: if enabled for each stage individually, for every host write, deduplication occurs first, then compression, then encryption.

At the time of writing, compression is available in several methods:

- Using inline hardware chips inside specific media, such as the IBM FlashCore Modules (FCM)
- Using the FS9100 onboard motherboard

Compression can be turned on for volumes in traditional pools, and in the Data Reduction Pool (DRP) pool type.

Deduplication can only be engaged inside the DRP, and uses various pattern matching techniques to reduce the total data written by leveraging metadata pointers.

Important: On FS9100, you should use fully-allocated Data Reduction Pools with compression and no deduplication. Alternatively, use Data Reduction Pools with compression and deduplication.

3.1.1 Compression Items

IBM uses several compression methods, such as IBM Real-time Compression™ (RtC) and other technologies including over 50 patents that are not primarily about compression. Rather, they define how to make industry-standard Lempel-Ziv (LZ) compression of primary storage operate in real time and allow random access. The primary intellectual property behind this technology is the Real-time Analytical Compression Engine (RACE) component.

At a high level, when compression is enabled outside of DRP, data is written into the storage system dynamically. All compression occurs transparently, so Fibre Channel and iSCSI connected hosts are not aware of the compression. See “What is in a Data Reduction Pool” on page 38 to learn more about the differences in how compression is handled inside that particular pool type.

RACE is an inline compression technology, which means that each host write (to a compressed pool) is analyzed and compressed as it passes through the FS9100 to the disks. This technology has a clear benefit over other compression technologies that are solely post-processing based.

RACE is based on the Lempel-Ziv (LZ) lossless data compression algorithm, and operates using a real-time method. When a host sends a write request, the request is acknowledged by the write cache of the FS9100 system, and is then staged to the storage pool.

As part of its staging, the write request passes through the compression engine and is then stored in a compressed format onto the storage pool. Therefore, writes are acknowledged immediately after they are received by the write cache, with compression occurring as part of the staging to internal or external physical storage.

Capacity is saved when the data is written by the host, because the host writes are smaller when they are written to the storage pool. The entire process is completely self-tuning, similar to the SVC system. It adapts to the workload that runs on the system at any particular moment.

Random Access Compression Engine (RACE)

To understand why RACE is unique, you need to review the traditional compression techniques. This description is not about the compression algorithm itself (how the data structure is *reduced in size mathematically*). Rather, the description is about how the data is *laid out within the resulting compressed output.*

Compression utilities

Compression is probably most known to users because of the widespread use of compression utilities, such as ZIP or TAR. At a high level, these utilities take a file as their input, and parse the data by using a *sliding window* technique. Repetitions of data are detected within the sliding window history, most often 32 KiB. Repetitions outside of the window cannot be referenced. Therefore, the file cannot be reduced in size unless data is repeated when the window “slides” to the next 32 KiB slot.

Figure 3-1 shows compression that uses a sliding window, where the first two repetitions of the string ABCD fall within the same compression window, and can therefore be compressed by using the same dictionary. The third repetition of the string falls outside of this window, and therefore cannot be compressed by using the same compression dictionary as the first two repetitions, reducing the overall achieved compression ratio.

Figure 3-1 Compression that uses a sliding window

Traditional data compression in storage systems

The traditional approach that is taken to implement data compression in storage systems is an extension of how compression works in the compression utilities previously mentioned. Similar to compression utilities, the incoming data is broken into fixed chunks, and then each chunk is compressed and extracted independently.

However, drawbacks exist to this approach. An update to a chunk requires a read of the chunk followed by a recompression of the chunk to include the update. The larger the chunk size chosen, the heavier the I/O penalty to recompress the chunk. If a small chunk size is chosen, the compression ratio is reduced because the repetition detection potential is reduced.

Figure 3-2 shows an example of how the data is broken into fixed-size chunks (in the upper-left corner of the figure). It also shows how each chunk gets compressed independently into variable length compressed chunks (in the upper-right side of the figure). The resulting compressed chunks are stored sequentially in the compressed output.

Although this approach is an evolution from compression utilities, it is limited to lower-performance use cases mainly because this approach does not provide real random access to the data.

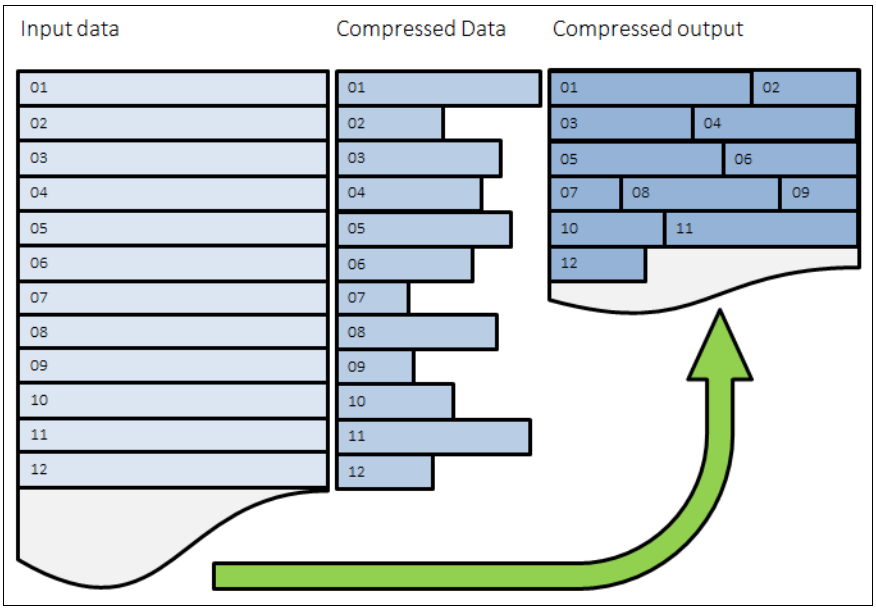


Figure 3-2 Traditional data compression in storage systems

Random Access Compression Engine

RACE implements an inverted approach when compared to traditional approaches to compression. RACE uses variable-size chunks for the input, and produces fixed-size chunks for the output.

This method enables an efficient and consistent method to index the compressed data, because the data is stored in fixed-size containers (Figure 3-3).

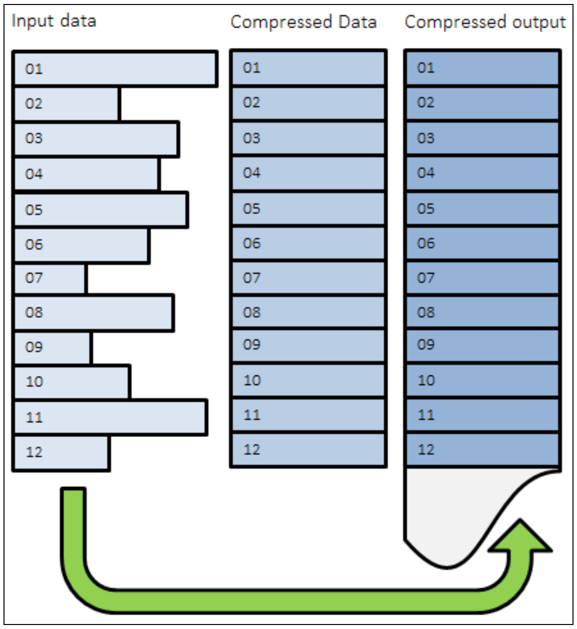


Figure 3-3 Random Access Compression

Location-based compression

Both *compression utilities* and *traditional storage system compression* compress data by finding repetitions of bytes within the chunk that is being compressed. The compression ratio of this chunk depends on how many repetitions can be detected within the chunk. The number of repetitions is affected by how much the bytes stored in the chunk are related to each other.

Furthermore, the relationship between bytes is driven by the format of the object. For example, an office document might contain textual information, and an embedded drawing, such as this page.

Because the chunking of the file is arbitrary, it has no notion of how the data is laid out within the document. Therefore, a compressed chunk can be a mixture of the textual information and part of the drawing. This process yields a lower compression ratio because the different data types mixed together cause a suboptimal dictionary of repetitions. That is, fewer repetitions can be detected because a repetition of bytes in a text object is unlikely to be found in a drawing.

This traditional approach to data compression is also called *location-based compression*. The data repetition detection is based on the location of data within the same chunk.

This challenge was addressed with the *predecide* mechanism introduced in IBM Spectrum Virtualize version 7.1.

Predecide mechanism

Certain data chunks have a higher compression ratio than others. Compressing some of the chunks saves little space but still requires resources, such as processor (CPU) and memory. To avoid spending resources on uncompressible data, and to provide the ability to use a different, more effective (in this particular case) compression algorithm, IBM invented a *predecide* mechanism.

The chunks that are below a certain compression ratio are skipped by the compression engine, saving CPU time and memory processing. These chunks are not compressed with the main compression algorithm, but can still be compressed with another algorithm. They are marked and processed. The results can vary because predecide does not check the entire block, but only a sample of it.

Figure 3-4 shows how the detection mechanism works.

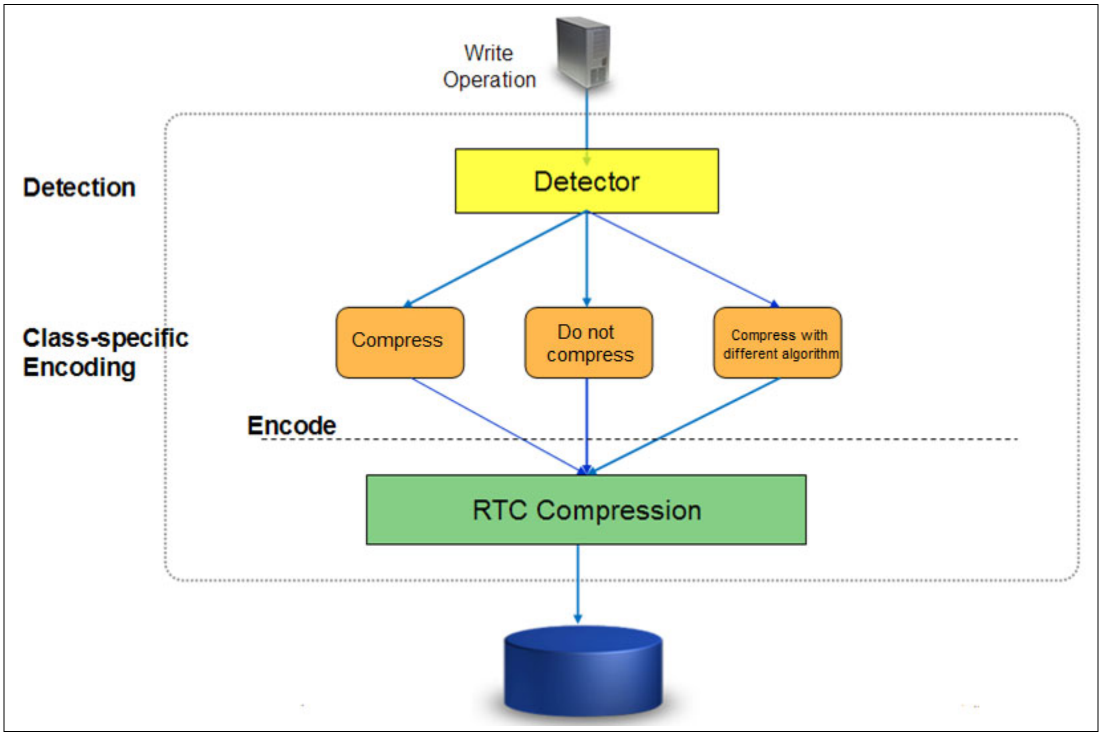


Figure 3-4 Detection mechanism

Temporal compression

RACE offers a technology leap beyond location-based compression, called *temporal compression*. When host writes arrive at RACE, they are compressed and fill fixed-size chunks that are also called *compressed blocks*. Multiple compressed writes can be aggregated into a single compressed block. A dictionary of the detected repetitions is stored within the compressed block.

When applications write new data or update existing data, the data is typically sent from the host to the storage system as a series of writes. Because these writes are likely to originate from the same application and be from the same data type, more repetitions are usually detected by the compression algorithm. This type of data compression is called *temporal compression* because the data repetition detection is based on the time that the data was written into the same compressed block.

Temporal compression adds the time dimension that is not available to other compression algorithms. It offers a higher compression ratio because the compressed data in a block represents a more homogeneous set of input data.

Figure 3-5 shows how three writes sent one after the other by a host end up in different chunks. They get compressed in different chunks because their location in the volume is not adjacent. This approach yields a lower compression ratio because the same data must be compressed non-natively by using three separate dictionaries.

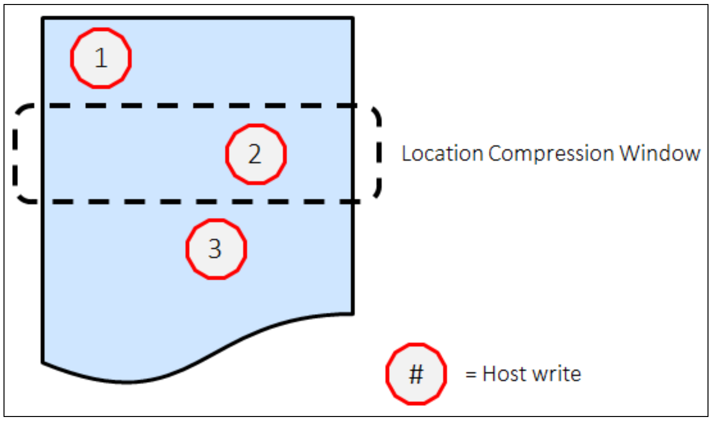


Figure 3-5 Location-based compression

When the same three writes are sent through RACE, as shown in Figure 3-6, the writes are compressed together by using a single dictionary. This approach yields a higher compression ratio than location-based compression.

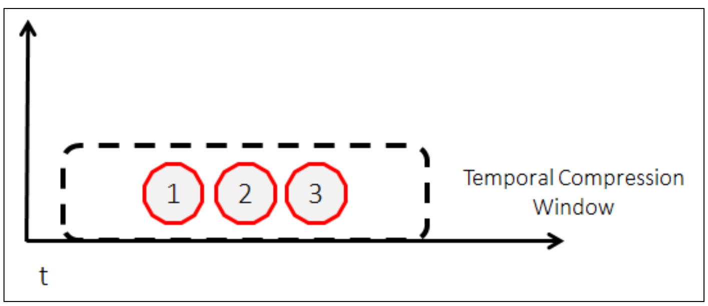


Figure 3-6 Temporal compression

3.1.2 Deduplication items

This topic covers deduplication and the techniques that it employs.

Pattern matching and removal

This first layer of data reduction comes from pattern matching.

Pattern matching mechanisms match incoming host writes with a preconfigured set of known patterns that are stored in the system.

When a write is processed, it is split into 8 KB blocks, as shown in Figure 3-7.

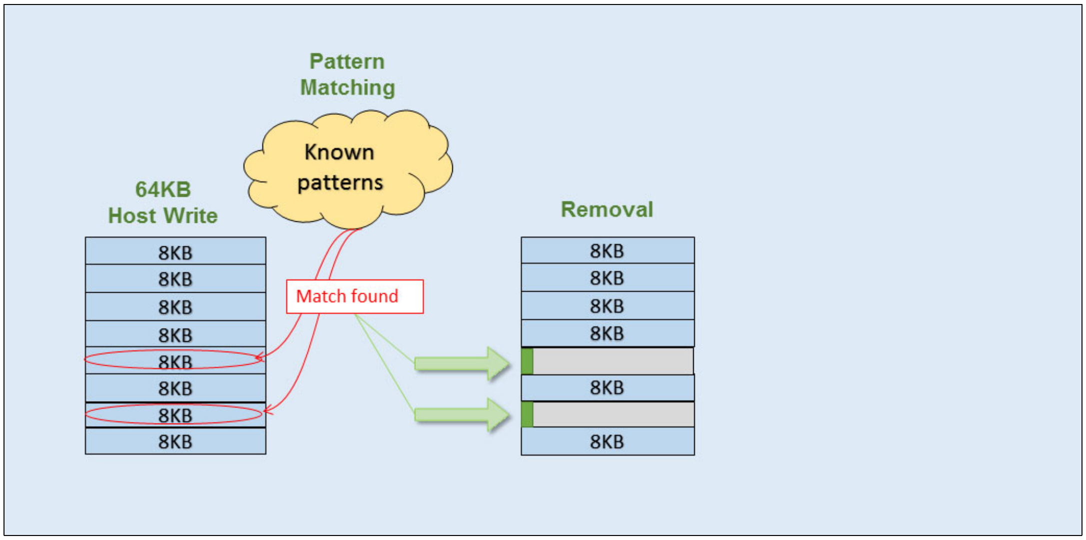


Figure 3-7   Pattern matching and removal

Then, each block is hashed, and the hash value, which is also known as a *fingerprint*, is compared to a table of well-known hashes. If a match is found, the corresponding pattern ID, which is only 2 bytes (green rectangle in Figure 3-7) is stored.

Data deduplication

Data deduplication is the ability to store data only once, although it can be written many times by various hosts or applications.

The data deduplication mechanism identifies identical blocks of data and stores only one copy of that data in the system. All other identical blocks point to that copy.

In Figure 3-8, each color represents unique data. Every square represents an 8 KB block. The system can detect duplicates, and it stores only one copy of the duplicate 8 KB blocks. For duplicates, Figure 3-8 shows that only the pointers to the data are stored in the system.

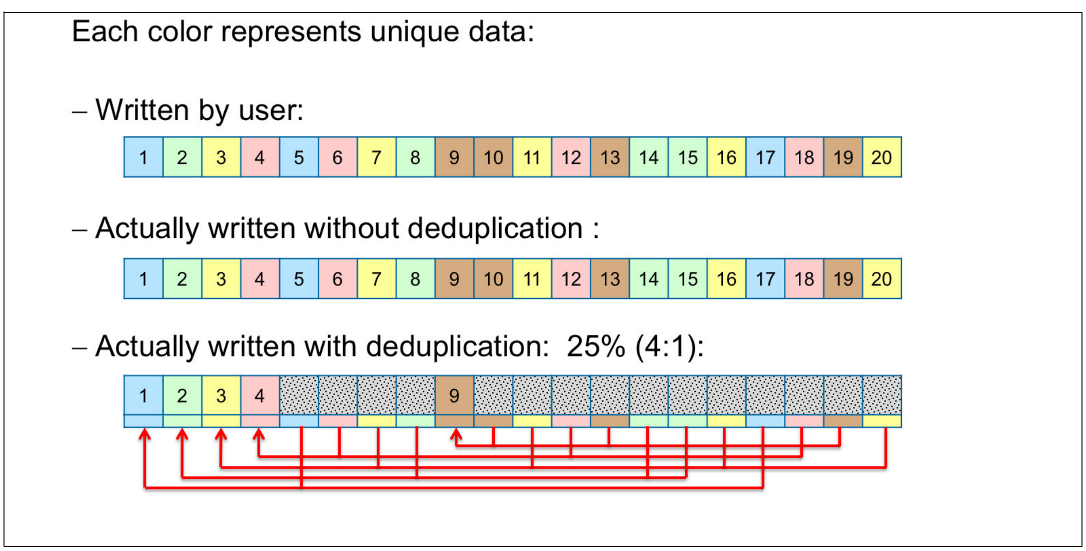


Figure 3-8   Data deduplication principle

In the FlashSystem 9100 family, each 8 KB block for which a duplicate exists is replaced by a pointer to the hash of the duplicate, as shown on the right side of Figure 3-9. Notice that the green block for deduplication is larger than the green block for pattern matching. This is because more metadata has to be stored for deduplication than for pure pattern matching.

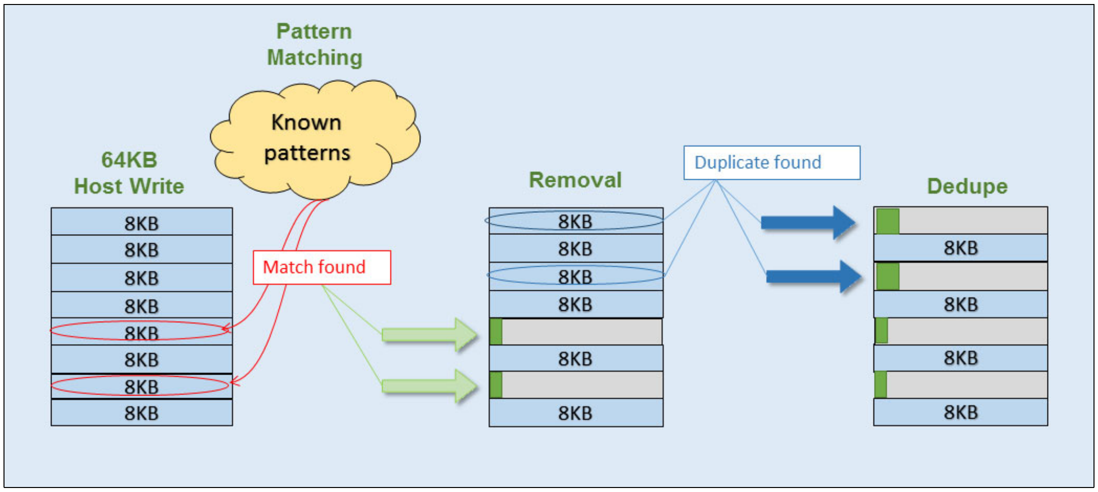


Figure 3-9 Data deduplication in FlashSystem 9100 family

Whenever a new unique block is found, a new hash is created and stored in a repository. Any future 8 KB writes' hash is checked against the repository for a match.

Note: Deduplication only applies to data blocks of 8 KB or larger.

Data deduplication is performed in sequences, and the system stores hashes in a memory construct, which is known as a *segment*. Each hash (data) has an owning segment, and a certain segment can also contain references to a hash that it owns, or references to a hash in another owning segment. See Figure 3-10. The owning segment of a referenced hash is indicated by the corresponding background color.

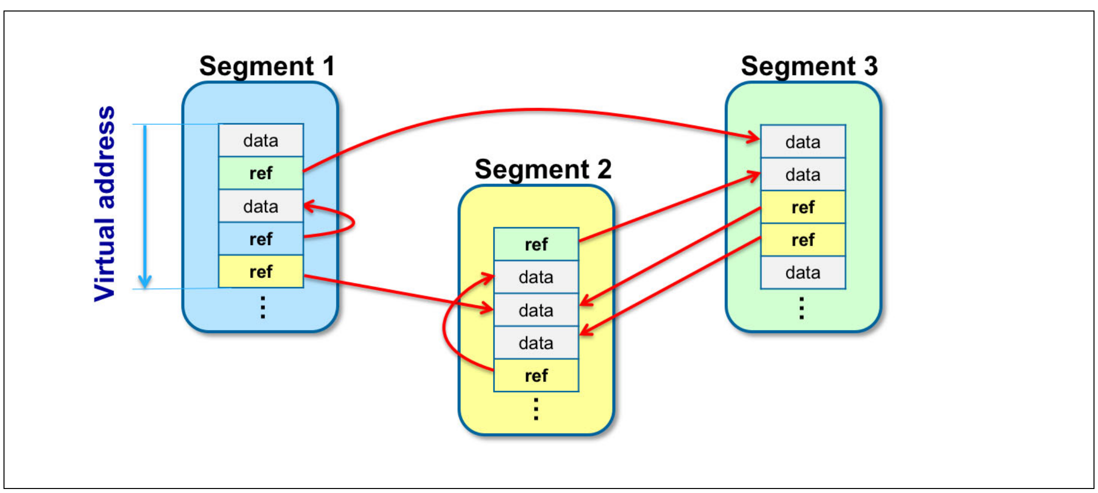


Figure 3-10 Hashes and references in segments

Segments maintain a list of other segments that they created references to recently. Therefore, when the system looks for a match, the recent segments are checked first, which typically speeds up the matching process.

As illustrated in Figure 3-11, the data deduplication of the 8 KB blocks is performed over a 4 KB alignment, which increases the probability of finding a match, resulting in a higher data deduplication percentage.

Note: The 4 KB alignment augments the probability to find a match for deduplication within 8 KB blocks.

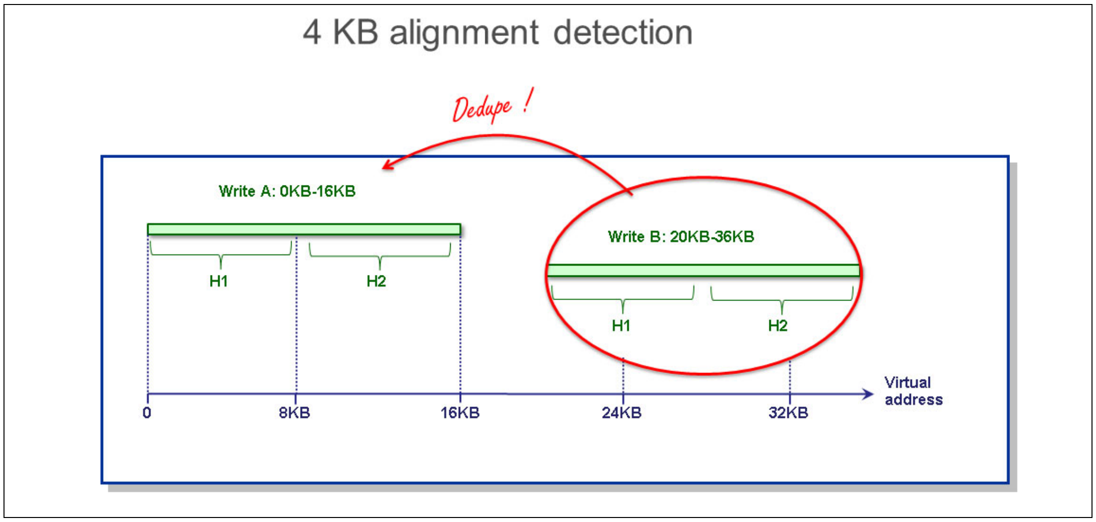


Figure 3-11 Data deduplication with 4 KB alignment detection

Maintaining integrity

Integrity of user data is a major aspect of the system design. There are several data integrity concerns when deduplication is involved, including the following:

- When creating a deduplication reference, the reference must be created to the correct data.
- When reading the data, the read path over the original reference must fetch the correct data.
- When deleting data, the data must not be deleted if there remain any references to this (current) data anywhere in the system.

The first measure of protection in the IBM FlashSystem 9100 code design is a dual-layered CRC check. The first CRC is on user data as it enters the system and before compression modifies the data. The second CRC covers what is actually written to the storage after data reduction, and covers both data and metadata.

FlashSystem 9100 uses the industry-standard SHA1 to fingerprint user data. References are created and defined by their SHA1. The SHA1 is stored in every reference in addition to the SHA1 stored with the data itself. In other referencing methods, such as using ID number or position, there is a risk of reading incorrect data if there is a problem in the management of the ID or position. Using the SHA1 as the reference avoids any such potential problems.

Another mechanism protects the reference counters. This mechanism modifies the counter in a transactional manner that is capable of surviving any type of failure, including crashes and communication failures.

As a last resort, the system includes a unique offline recovery capability that scrubs the data and reconstructs the metadata, including references and reference counters.

Compression

Finally, data moves on to the compression step (Figure 3-12) for more data reduction.

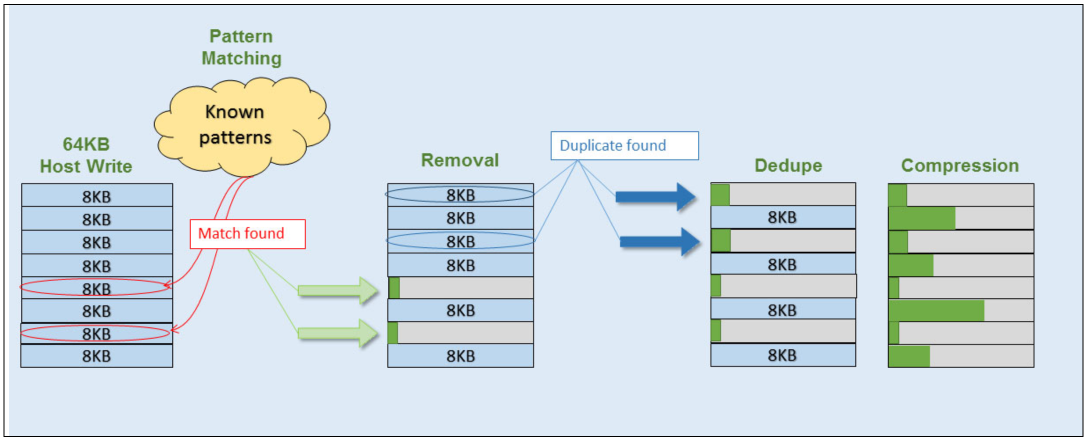


Figure 3-12 Data flow using both Deduplication and Compression

For details about the compression phase, see “Compression that uses a sliding window” on page 26. Figure 3-13 on page 35 summarizes the data reduction process flow.

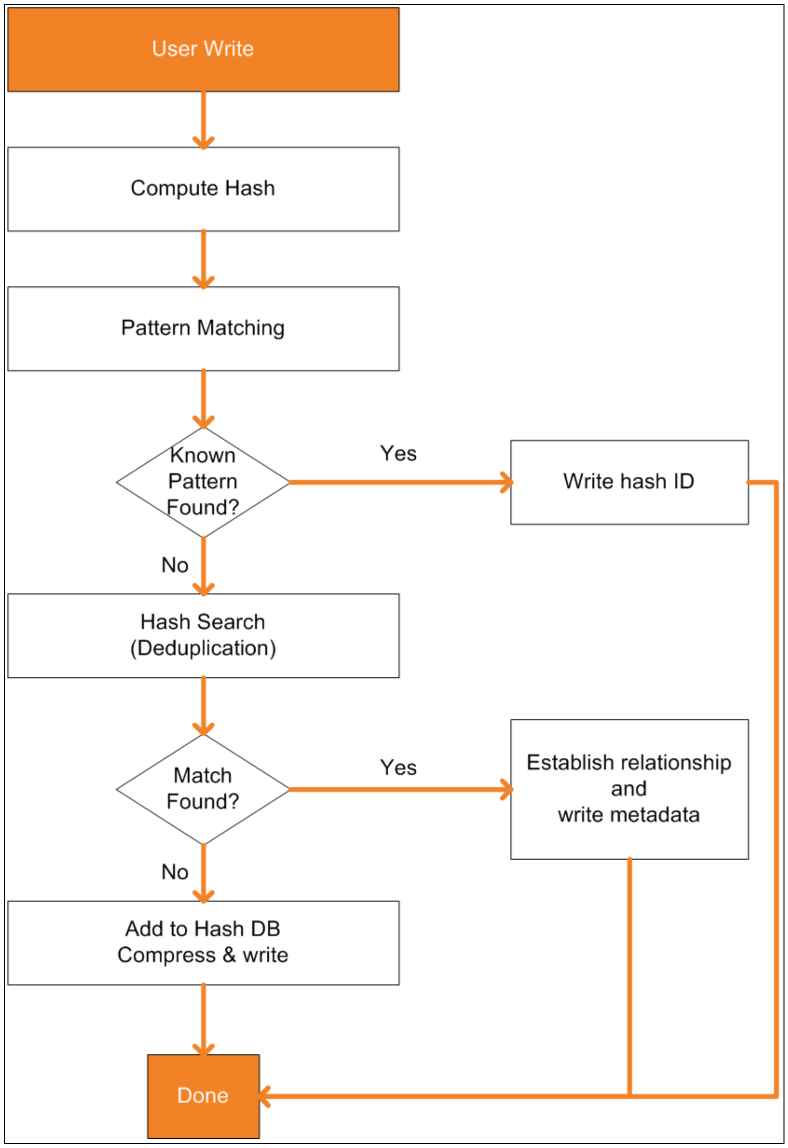


Figure 3-13 Data reduction process flow

3.2 Data Reduction Pools inside the FS9100

Data Reduction Pools represent a significant enhancement to the storage pool concept. This is because the virtualization layer is primarily a simple layer that runs the task of lookups between virtual and physical extents. Now, with the introduction of data reduction technology, it has become more of a requirement to have an uncomplicated way to stay thin.

> **Important:** On FS9100, use fully-allocated, Data Reduction Pools with compression and no deduplication; or Data Reduction Pools with compression and deduplication.

Data Reduction Pools increase existing infrastructure capacity utilization by leveraging new efficiency functions and reducing storage costs. The pools enable you to automatically de-allocate (not to be confused with deduplication) and reclaim capacity of thin-provisioned volumes containing deleted data.

For the first time, DRP enables this reclaimed capacity to be reused by other volumes. With a new log-structured pool implementation, data reduction pools help deliver more consistent performance from compressed volumes. DRP also supports compression of all volumes in a system, potentially extending the benefits of compression to all data in a system.

Traditional storage pools have a fixed allocation unit of an extent, and that itself will not be changing with Data Reduction Pools. However, features like Thin Provisioning and Real-time Compression (RtC) use smaller allocation units and manage this allocation with their own metadata structures. These are described as Binary Trees or Log Structured Arrays (LSA).

In order to stay thin, you need to be able to reclaim capacity that is no longer used, or in the case of an LSA (where all writes go to new capacity), garbage collect the old overwritten data blocks. This also needs to be done at the smaller allocation unit size (KB) per extents.

Figure 3-14 shows the DRP mirroring structure.

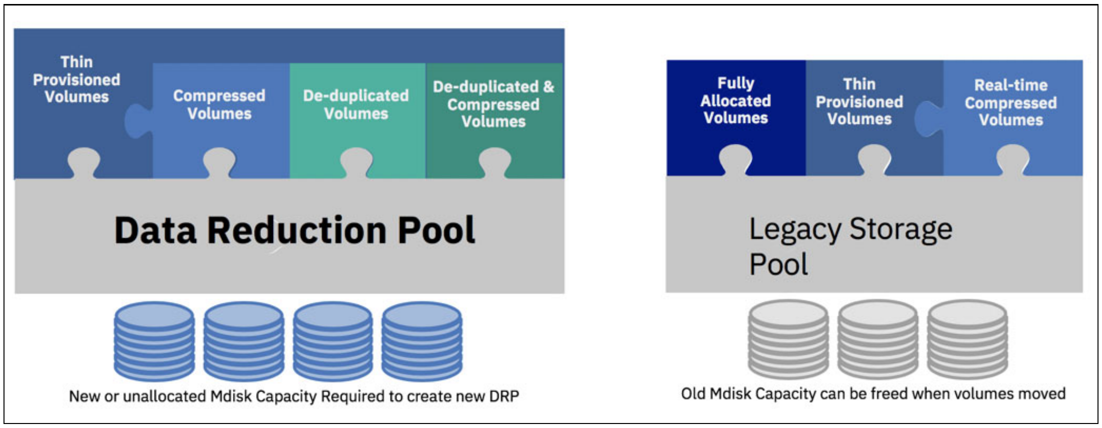


Figure 3-14 New data reduction pool volume mirroring structure

Note: Use volume mirroring to clone data to a new DRP, because DRP does not support `migrate` commands.

3.2.1 DRP volume types

DRP technology allows you to create the following types of volumes:

- Fully allocated

  This type provides no storage efficiency but the best performance, and is available for migration.

- Thin

  This type provides storage efficiency but no compression or deduplication.

- Thin and Compressed

  This type provides storage efficiency with compression, and this combination provides the best performance numbers.

- Thin and Deduplication

  This type provides storage efficiency but without compression.

- Thin, Compressed and Deduplication

  This type provides storage efficiency with maximum capacity savings.

With storage efficiency, DRP thin and compressed volumes provide the best performance numbers. This is due to the new compression implementation, because this provides better load balancing and consistent performance.

Figure 3-15 shows the types of volumes in the DRP pools.

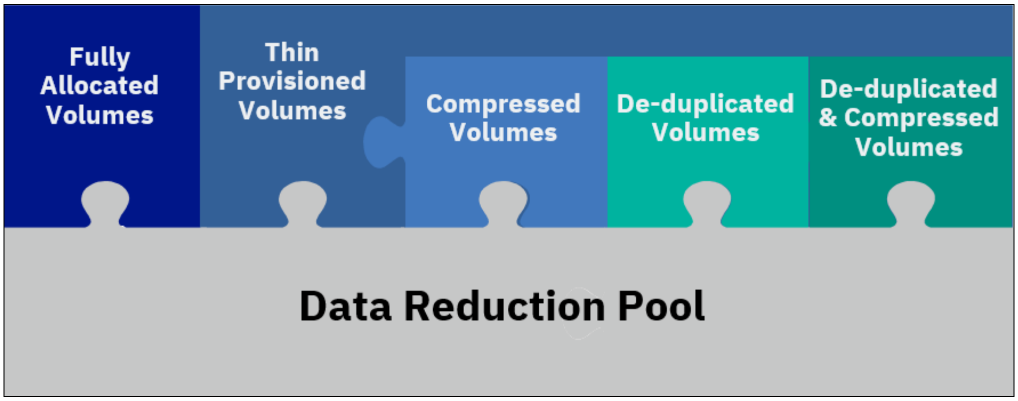


Figure 3-15 Volume types

There are four main characteristics that make up the IBM Data Reduction Pool design:

- Fine-grained allocation of data blocks
- The ability to free back unused (unmapped or overwritten) capacity at a fine grain
- Give consistent, predictable performance
- Optimize performance for solid state storage, such as Flash

A data reduction pool, at its core, uses an LSA to allocate capacity. Therefore, the volume that you create from the pool to present to a host application consists of a directory that stores the allocation of blocks within the capacity of the pool.

All writes for data reduction pools take place at the upper cache layer to the host. Reads have to go through the lower cache layer. The heart of the new DRP functionality is in the new implementation of the Log Structured Array. This includes lower cache, virtualization, Easy Tier, and RAID. LSA understands what works best for each of these components.

A log structured array allows a “tree-like” directory to be used to define the physical placement of data blocks independent of size and logical location. Each logical block device has a range of logical block addresses (LBAs). Starting from 0 and ending with the block address that fills the capacity. When written, an LSA allows you to allocate data sequentially and provide a directory that provides a lookup to match the logical block address with the physical address within the array.

Note: LSA always appends new data to the end of the array. When data is overwritten, the old location and capacity utilized needs to be marked as `free`. UNMAP functions can also request that you *free* no longer needed capacity. Compression overwrites can result in a different capacity being used. Deduplication might find new duplicates when data is rewritten.

Figure 3-16 shows the IBM Spectrum Virtualize I/O stack structure.

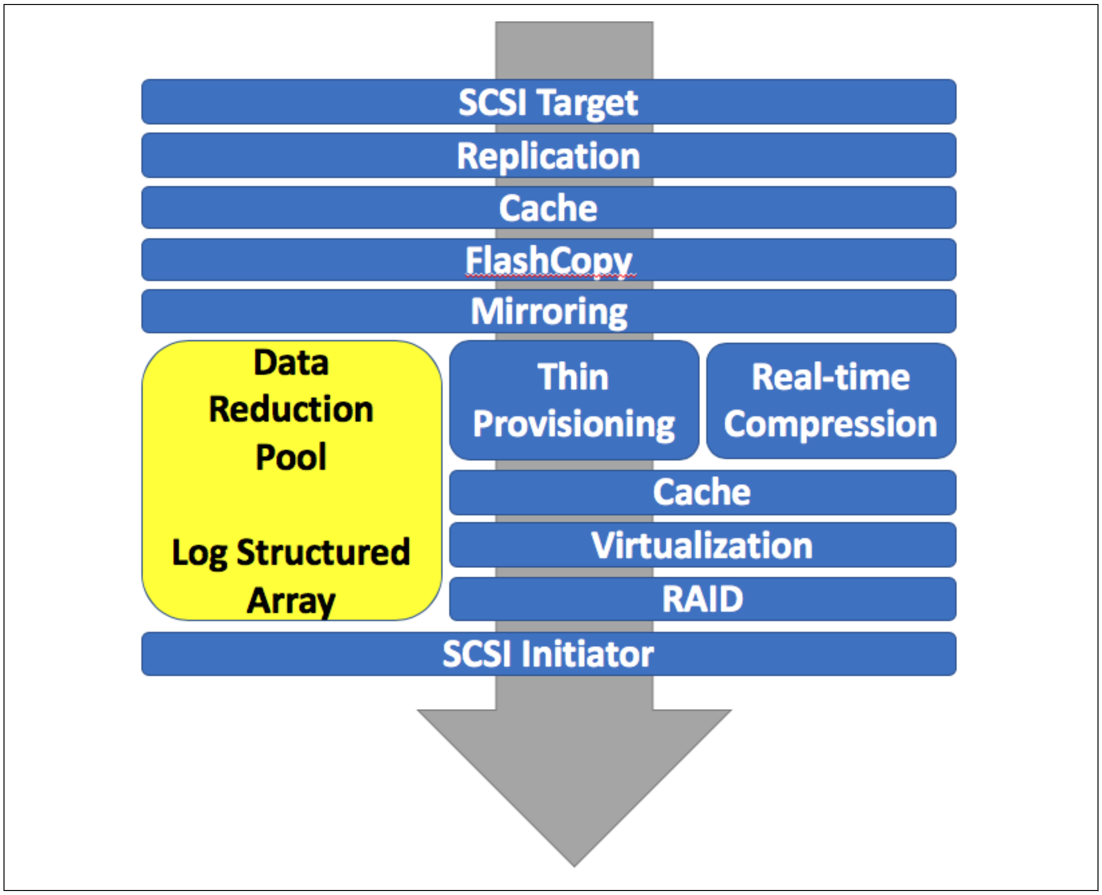


Figure 3-16 Data Reduction Pools/LSA is located in the IBM Spectrum Virtualize I/O stack

3.2.2 What is in a Data Reduction Pool

As shown in Figure 3-17 on page 39, the user sees a sample of four volumes in a Data Reduction Pool. Internally, there will be four directory volumes, one customer data volume (per I/O Group), and one Journal Volume (per I/O Group).

Figure 3-17 shows the view of DRP.

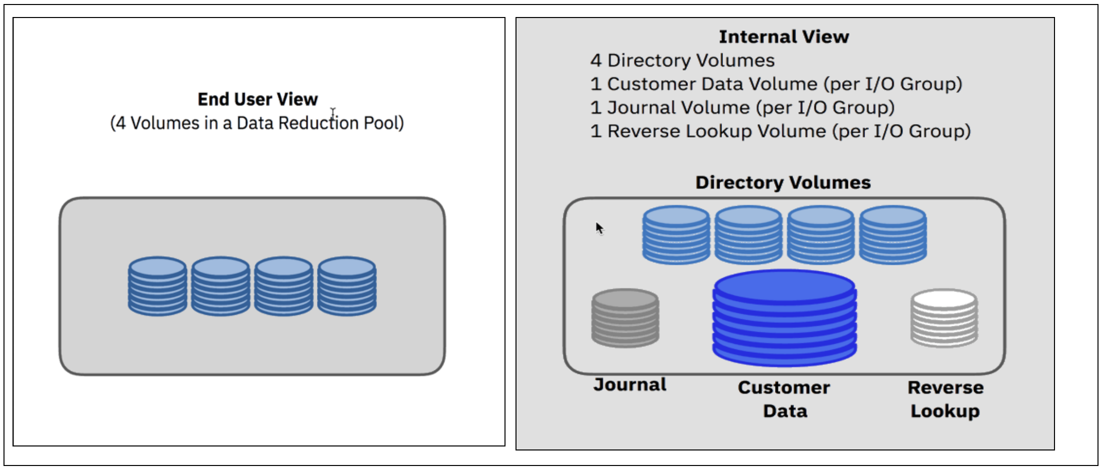


Figure 3-17 Both the front-end and back-end view of DRP

Each Internal volume type has very specific I/O patterns with its own percentage used of the total capacity of the pool shown in Table 3-1.

Table 3-1 I/O Patterns per internal volumes

Customer Data Volumes	Directory Volumes	Journal Volumes	Reverse Lookup
98% of Pool Capacity	1% of Pool Capacity	Less than 1% of Pool Capacity	Less than 1% of Pool Capacity
Large sequential write pattern & Short random read pattern	Short 4 KB random read and write pattern	Large sequential write I/O & Only read for recovery scenarios (for example, T3 and so on)	Short, semi-random read write pattern

3.2.3 Allocation block size

The allocation size of these blocks is now 8 KB: previously, thin provisioned volumes used 32 KB and RACE Compression write of 32 KB of compressed data. Here are some key reasons behind the 8 KB allocation:

- UNMAP requests as small as 8 KB can be catered for.
- The addressability of data in the pool is at an 8 KB (uncompressed) boundary, compared to 32 KB compressed with previous RACE compression.
- All random read requests are of 8 KB size (or less if compressed), which is ideal for Flash storage.
- With a common metadata access size served by lower cache, performance is much more consistent.

Figure 3-18 shows the DRP Compression I/O Amplification.

I/O Type	Space Allocated	I/O Amplification including Size
8K Read	Unallocated	0.50 (1x4K metadata + no data I/O)
	Allocated	1.00 (1x4K metadata + 1x4K data read)
32k Read	Unallocated	0.125 (1x4K metadata + no data I/O)
	Allocated	0.625 (1x4K metadata + 1x16K data read)
8K Write	Unallocated	1.50 (2x4K metadata + 1x4K data write)
	Allocated	1.50 (2x4K metadata + 1x4K data write)
32k Write	Unallocated	0.75 (2x4K metadata + 1x16K data write)
	Allocated	0.75 (2x4K metadata + 1x16K data write)

Figure 3-18 I/O Amplification of space allocated (assumes 50% compression rate)

Note: Writes to already allocated space will drive the need for Garbage Collection (GC). The cost of GC depends on the amount of valid data in the extent that has not been overwritten.

3.3 RACE compared to Data Reduction Pools

RACE uses a variable input with a fixed output of the inbound data stream, all of which is inline without any post process. However, RACE has to wait intermittently or pause to see if more I/O is coming for a particular volume, as shown in Figure 3-19 on page 41. The RACE minimum block size to read from the back end is 32 KB.

One of the benefits of RACE is that it enables at least 4 - 8 times more data through decompression hardware than DRP, for a true random workload. However, DRP Compression uses fixed input with a variable output, or the opposite of RACE.

As shown in Figure 3-20 on page 41, the DRP maximum block size to read from the back end is 8 KB (typically 4 KB or less though). With the use of 8 KB input sizes, there is a small loss in compression ratio but a gain in lower latency when all workloads are put into the same predictable small block size.

Host I/O that is put in these small-grained block sizes in DRP results in the following functionality:

- Enables fine-grained allocation of block data
- Provides the ability to free back unused capacity at a fine grain
- Gives consistent, predictable performance
- Optimizes performance for Flash storage

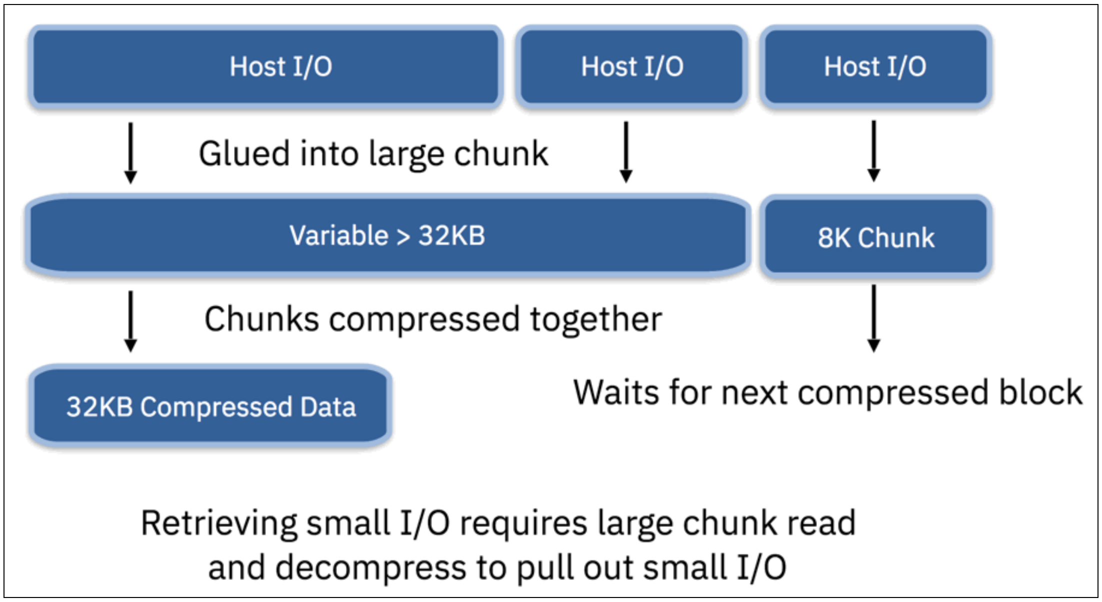


Figure 3-19 RACE compression I/O stack

Figure 3-20 shows the DRP compression I/O stack.

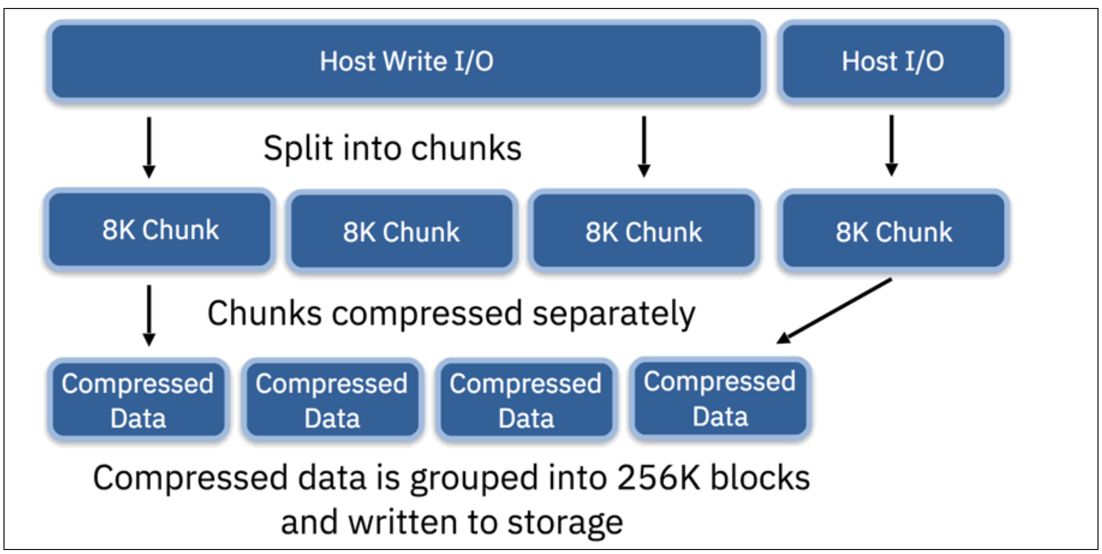


Figure 3-20 DRP compression I/O stack

Here are some of the key differences in DRP when compared to RACE:

- CPU
  - Data reduction uses the same threads as the main I/O process
  - No separate compression CPU utilization
  - No dedicated CPU cores for compression
- Memory
  - Data reduction shares memory with the main I/O process
  - 1 GB memory taken from cache when data reduction is enabled

- Compression Hardware
  - Shared with existing RtC compression and compression for IP replication
  - New DRP compression achieves up to 4.8 GB/s per node (compression card limit)

3.3.1 Benefits of Data Reduction Pools (DRP)

There are many advantages to data reduction pools:

- Designed to be highly scalable to support hardware with more cores and more memory
- Tightly integrated compression shares available cores with other processes for greater efficiency
- Optimization for flash storage through conversion of random write I/Os into larger sequential writes
- No limit on the number of compressed volumes enables greater use of compression (up to 5x as many volumes), and so more compression benefit and reduced storage cost
- Up to 3x better throughput for compressed data, enabling its use with a wider range of data types
- Ability to release and reuse storage in response to server needs, reducing overall storage required
- Designed for future data reduction technologies
- Separation of metadata and user data improves cache effectiveness
- Compression integrated within I/O stack
- Shared resource design
- Active/Active: Mirrored non-volatile metadata means significantly improved failover/failback response times due to no revalidation of metadata
- No limit on the number of compressed volumes
- Space reclamation: Unmap available, see 3.4, “Data Reduction Pools and Unmap” on page 43
- Designed for deduplication
- Smaller 8 KB chunks means less compression bandwidth for small I/Os
- Metadata and user data are separated, providing a better use of cache prefetch/destage
- On average 1.8x I/O amplification on host I/O: much more predictable latency compared to RACE
- Able to use maximum compression bandwidth
- Comprestimator support

Table 3-2 shows DRP disk limitations.

Table 3-2 DRP disk limitations

Extent Size	Volume size	4 I/O groups
1 GB	128 TB	512 TB
2 GB	256 TB	1 PB
4 GB	512 TB	2 PB
8 GB	1 PB	4 PB

3.4 Data Reduction Pools and Unmap

DRPs support end-to-end Unmap functionality. Space that is freed from the hosts is a process called *Unmap*. A host can issue a small file Unmap (or a large chunk of Unmap space if you are deleting a volume that is part of a data store on a host), and these unmaps result in the freeing of all of the capacity allocated within that Unmap. Similarly, deleting a volume at the DRP level frees all of the capacity back to the pool.

When a data reduction pool is created, the system monitors the pool for reclaimable capacity from host Unmap operations. This capacity can be reclaimed by the system and redistributed into the pool. Create volumes that use thin provisioning or compression within the data reduction pool to maximize space within the pool.

3.5 Data Reduction Pools with Easy Tier

DRP uses an LSA, as mentioned previously. RACE has used a form of LSA since its introduction in 2011, and this means that there is a normal garbage collection that needs to be done regularly. An LSA always appends new writes to the end of the allocated space. Even if data already exists, and the write is an overwrite, the new data is not written in that place. Instead, the new write is appended at the end and the old data is marked as needing garbage collected.

This process provides the following advantages:

- Writes to a DRP volume are always sequential: so we can build all the 8 KB chunks into a larger 256 KB chunk and destage the writes from cache, either as full stripe writes, or as large as a 256 KB sequential stream of smaller writes.
- This should give the best performance both in terms of RAID on back-end systems, and also on Flash, where it becomes easier for the Flash device to perform garbage collection on a larger boundary.

We can start to record metadata about how frequently certain areas of a volume are overwritten. We can then bin sort the chunks into a heat map in terms of rewrite activity, and then group commonly rewritten data onto a single extent. This is so that Easy Tier will operate correctly for not only read data, but write data, when data reduction is in use.

Previous writes to compressed volumes held lower value to the Easy Tier algorithms, because writes were always to a new extent, so the previous heat was lost. Now, we can maintain the heat over time and ensure that frequently rewritten data gets grouped together. This also aids the garbage collection process where it is likely that large contiguous areas will end up being garbage collected together.

3.6 Garbage collection

DRP has built-in services to enable garbage collection of unused blocks. This means that many smaller unmaps end up enabling a much larger chunk (extent) to be freed back to the pool. In addition, if the storage behind Virtualize supports Unmap, we pass an **unmap** command to the backend storage. Again, this is equally important with today’s Flash backend systems, especially so when they themselves implement some form of data reduction.

Trying to fill small holes is very inefficient. Too many I/Os would be needed to keep reading and rewriting the directory. So, Garbage Collection (GC) waits until an extent has many small holes. Move the remaining data in the extent: compact and rewrite. When we have an empty extent, it can be freed back to the virtualization layer (and back end with UNMAP) or start writing into the extent with new data (or rewrites).

The reverse lookup metadata volumes track the extent usage, or more importantly the holes created by overwrites or unmaps. Garbage Collection looks for extents with the most unused space.

When a whole extent has had all of its data moved elsewhere, it will be marked as `free`, put back into the set of unused extents, into that pool, or reused for new written data.

3.7 Data Reduction Pools with deduplication

Deduplication can be configured with thin-provisioned and compressed volumes in data reduction pools for added capacity savings. The deduplication process identifies unique chunks of data, or byte patterns, and stores a signature of the chunk for reference when writing new data chunks. If the new chunk's signature matches an existing signature, the new chunk is replaced with a small reference that points to the stored chunk. The same byte pattern may occur many times, resulting in the amount of data that must be stored being greatly reduced.

Duplicate matches are found using SHA1 hashes created for each 8 KB align region of client data to a deduplicated copy. The matches are detected when the data is written. For Data Reduction Pools, deduplication data can work in two separate ways. It can be grouped into 256 KB blocks and written to storage, or it can be passed as 8 KB chunks, and compressed first.

Deduplication has specific I/O characteristics in the handling of data and data copies. When a matching fingerprint is found, the metadata is updated to point to the metadata of the existing copy of the data. Each copy of the data can have up to 255 8 KiB virtual chunks referring to it. Each virtual 8 KiB chunk can track up to 3 versions of data. I/O performance takes precedence over finding duplicate copies of data. Host I/Os smaller than 8 KiB will not attempt to find duplicates.

Before utilizing DRP, it is important for storage administrators to analyze individual volumes or all volumes that are being considered for potential compression savings. This will help you determine if the workload that you are analyzing is a good candidate for DRP.

3.8 Estimating Data Reduction using various tools

IBM has provided several options to ensure accurate decisions can be made about using any level of data reduction. The following sections examine both Comprestimator and the Data Reduction Estimation Tool (DRET). In both cases, these tools are available from Fix Central and can be run on any host that has at least read access to the source volume. Running them against the volumes does not impact production performance, because they are looking for various patterns and calculating the reduction savings.

3.8.1 Comprestimator

Compestimator is an integrated GUI and CLI host-based utility that estimates the space savings achieved when using compressed volumes for block devices. This utility provides a quick and easy view of showing the benefits of using compression. The utility performs read-only operations, and therefore will have no effect on the data that is being stored on device.

If the compression savings prove to be beneficial in your environment, volume mirroring can be used to convert volumes to compressed volumes, then add those volumes to the data reduction pools.

When using the CLI, use the **analyzevdisk** command shown in Example 3-1 to run volume analysis against a single volume.

Example 3-1 The analyzevdisk command

```
IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>svctask analyzevdisk -h

analyzevdisk

Syntax

>>- analyzevdisk -- --+----------+-- --+- vdisk_id ---+--------><
                      '- -cancel-'     '- vdisk_name -'



For more details type 'help analyzevdisk'.

IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>svctask analyzevdisk vol1
IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>
```

When using the CLI, you can also use the **analyzevdiskbysystem** command shown in Example 3-2 to run volume analysis against the entire system.

Example 3-2 The analyzevdiskbysystem command

```
IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>svctask analyzevdiskbysystem -h

analyzevdiskbysystem

Syntax

>>- analyzevdiskbysystem -- --+----------+-- ------------------><
                              '- -cancel-'

For more details type 'help analyzevdiskbysystem'.

IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>svctask analyzevdiskbysystem
vol1
IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>
```

Note: The CLI Commands: **analyzevdisk** and **analyzevdiskbysystem** return back to the command prompt.

If you want to see the results of the volumes that you are analyzing, run the command **lsvdiskanalysis**, shown in Example 3-3.

Example 3-3 The lsvdiskanalysis and lsvdiskanalysis progress commands

```
IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>lsvdiskanalysisprogress
vdisk_count pending_analysis estimated_completion_time
12          12               180622091300
IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>
```

As stated previously, the utility can be used from the IBM Spectrum Virtualize™ GUI.

Figure 3-21 shows how to start a complete system analysis on compression estimates.

The sequence is to go to **Volumes** → **Actions** → **Space Savings** → **Estimate Compression Savings**.

A window prompt displays with the estimated time of completing the estimate on compression savings. This process can be monitored by adding the volumes that show compression savings in the volume table, as shown in Figure 3-21.

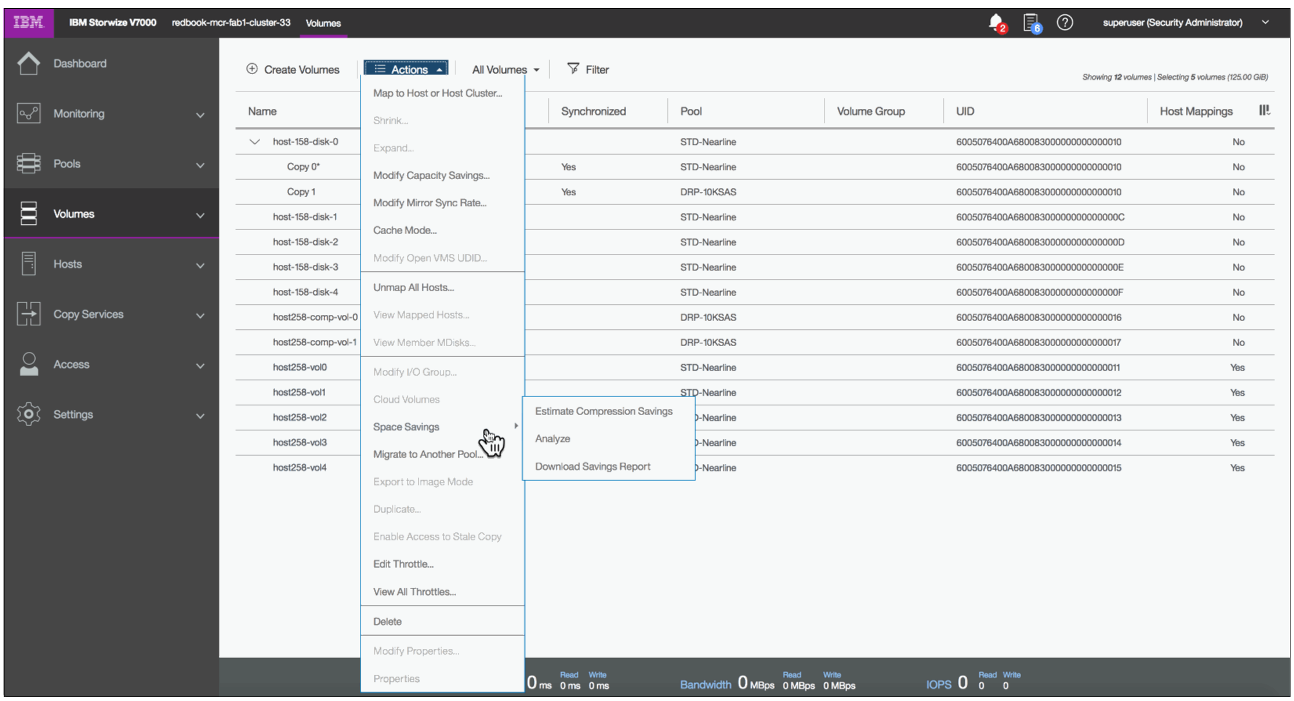


Figure 3-21 Estimate compression savings

3.8.2 Comprestimator using the host-based CLI utility

If you would like to estimate the compression savings of a volume *outside* of the IBM FlashSystem 9100, or on another array, the IBM Comprestimator utility can be installed on a host that is connected to the device that needs to be analyzed. More information and the latest version of this utility can be found at Fix Central.

There are several preferred practices for using Comprestimator:

- Run the Comprestimator utility before implementing an IBM Spectrum Virtualize solution, and before implementing the Data Reduction Pools technology.
- Download the latest version of the Comprestimator utility if you are not using one that is included in your IBM Spectrum Virtualize solution.
- Use Comprestimator to analyze volumes that contain as much active data as possible rather than volumes that are nearly empty or newly created. This ensures more accuracy when sizing your environment for compression and data reduction pools.

Note: Comprestimator can run for a long period (a few hours) when it is scanning a relatively empty device. The utility randomly selects and reads 256 KB samples from the device. If the sample is empty (that is, full of null values), it is skipped. A minimum number of samples with actual data are required to provide an accurate estimation.

When a device is mostly empty, many random samples are empty. As a result, the utility runs for a longer time as it tries to gather enough non-empty samples that are required for an accurate estimate. If the number of empty samples is over 95%, the scan is stopped.

3.8.3 Using Data Reduction Estimation Tool

Data Reduction Estimator Tool (DRET) is a CLI-operated execution file that runs from the host to analyze a given block device. It provides a report of what it would expect the deduplication savings to be from data written to the disk. There are no additional adjustments or requirements to run this tool on your IBM Spectrum Virtualize solution.

DRET displays its accuracy best with sequential workloads, and with volumes that contain the most active data in a storage environment. DRET is accurate at analyzing a range of workloads to identify the range at which the capacity of a volume can be used. Furthermore, it is able to complete these tasks within a reasonable amount of time, as shown in Table 3-3.

Table 3-3 Estimated time per block size

Volume Size	Time Taken (minutes)
15 GB	1
35 GB	1
100 GB	41
1 TB	32

When using DRET to analyze a block device used by a file system, all underlying data in the device is analyzed, regardless of whether this data belongs to files that were already deleted from the file system. For example, you can fill a 100 GB file system and make it 100% used, then delete all the files in the file system making it 0% used. When scanning the block device used for storing the file system in this example, DRET will access the data that belongs to the files that are already deleted.

Important: The preferred method of using DRET is to analyze volumes that contain as much active data as possible rather than volumes that are mostly empty of data. This increases the accuracy level and reduces the risk of analyzing old data that is already deleted, but might still have traces on the device.

As shown in Figure 3-22, DRET lists both compression and deduplication savings per volume, so in many ways it can save time to use DRET versus running the Comprestimator tool alone.

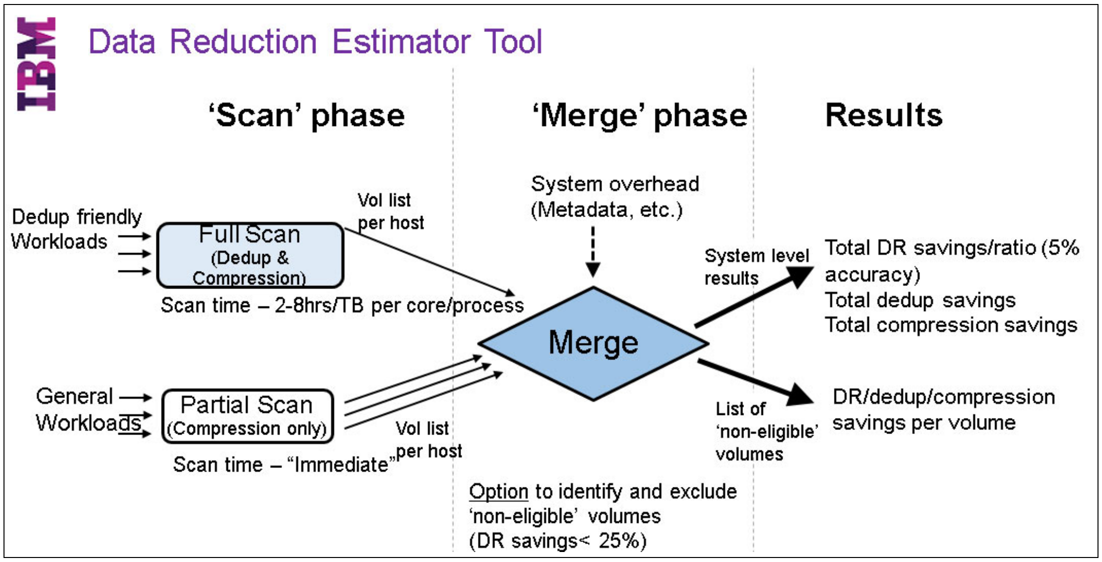


Figure 3-22 DRET overview and flow

The first step in analysis is the block device scan phase. During this phase, DRET reads a block device and then estimates the deduplication and compression savings. Each block device is analyzed separately.

The scan time varies 2 - 8 hours per TB, per core or process, which is adjustable on the command line when run. Also of note is that for systems that are not deduplication friendly, a partial scan can be run to gather only compression savings. The scan time for a partial scan of devices is very quick: usually 1 minute or less.

As DRET runs, each Volume/Device scan creates its own output file, which can then be merged into a complete system analysis.

After all devices have been scanned, results need to be merged to get overall reduction information.

Figure 3-23 shows an example.

Data Reduction Estimator Tool
Batch Run Example
Run Estimator Using Batchfile Option

```
[root@flashsem4-1:/tmp] ./Data-Reduction-Estimator --command scan --batchfile batchfile
./Data-Reduction-Estimator -d /vmfs/devices/disks/naa.600507640082000b080000000000007d
Result data filename not given, auto-generating: file_7506C27F.dat
2.00 TB | 502.83 MBps: 0% [#####################] 100%
Estimated Dedupe Savings:        71.861%
Estimated Compression Savings:   36.878%
Data Reduction Savings:          82.238%
-----------------------------------------
Zeroes Detected Savings:         36.187%
Total Data efficiency Savings:   88.666%
Time Consumed:                   04:26:34
./Data-Reduction-Estimator -d /vmfs/devices/disks/naa.6005076aa18f082aa000000001000002
Result data filename not given, auto-generating: file_BB7E2482.dat
300.00 GB | 61.30 MBps: 0% [#####################] 100%
Estimated Dedupe Savings:        10.172%
Estimated Compression Savings:   10.775%
Data Reduction Savings:          19.851%
-----------------------------------------
Zeroes Detected Savings:         16.677%
Total Data efficiency Savings:   33.218%
Time Consumed:                   01:45:11
```

Figure 3-23 DRET example

Figure 3-23 shows the individual runs, which can be scripted to run as a batch job. After each volume has been analyzed, they can be merged together to give a complete analysis, as shown in Figure 3-24.

Data Reduction Estimator Tool
Batch Run Example
Merge Estimator Output Files To Obtain Overall Estimate For System

```
[root@flashsem4-1:/tmp] ./Data-Reduction-Estimator --command merge --mergefiles
file_7506C27F.dat,file_BB7E2482.dat
Result data filename not given, auto-generating: merge_out
Estimated Dedupe Savings:        62.437%
Estimated Compression Savings:   27.114%
Data Reduction Savings:          72.349%
-----------------------------------------
Zeroes Detected Savings:         33.694%
Total Data efficiency Savings:   81.666%
Time Consumed:                   00:00:01
```

Figure 3-24 DRET merge example

More information and the latest version of this utility can be found at this website:

http://www14.software.ibm.com/webapp/set2/sas/f/dretool/home.html

3.9 When to use Flash Core Modules or Data Reduction Pools

Flash and solid state drive (SSD) technology is improving constantly in performance, and this technology provides low latency for application workloads.

Flash technology is cheaper than before. It has also reduced TCO because it requires less cooling and rack space, although it is currently still more expensive than traditional spinning disks. For this reason, storage administrators optimize the amount of data stored on Flash storage to drive the TCO even lower.

Data Reduction Pool technology is developed to optimize the Flash workload to provide cost savings by storing less data but at the same time providing stable and predictable performance. Flash Core Modules (FCM) offer on-board inline compression that provides excellent application performance without significant additional latencies.

Data Reduction Pools are useful if the underlying media does not have hardware acceleration, or if the goal is to ensure the most data reduction possible, by enabling deduplication. As described previously, DRP uses various technologies that add some small latency to the volumes on which it is enabled. We cover more examples in the following sections.

3.9.1 Flash Core Modules advantages

Flash Core Modules have some of these advantages over standard SSDs:

- Highly parallel design that enables better performance across many workloads
- On-board, always on, inline compression, without any need for configuration or concerns for latency sensitive applications
- No penalty for data that is encrypted or compressed from the host or application
- Added read-ahead cache enabling improved read latency on highly compressed data
- Four-plane programming to lower the overall power during write operations
- Hardware compression uses dedicated chips running proven IBM enhanced GZIP compression routines, alongside ECC, that have been used in IBM Z mainframe offerings for many decades

In summary, for the best application performance, using FCM in normal pools provides a good deal of data reduction with the on-board compression without any additional latencies, however small, that can occur with deduplication inside DRP.

3.9.2 Data Reduction Pool advantages

DRP has some excellent advantages, such as the best-in-class data reduction and space savings, especially when the underlying media does not have any other hardware-based compression abilities. In some respects, certain data volumes have better compression ratios with DRP than in a normal pool due to the compression methods.

Note that DRP volumes should be run with at least compression switched on, because there are not any performance trade-offs with this reduction. Only when deduplication is also enabled are there additional metadata with Garbage Collection and the LSA operations.

If you want to use DRP with an existing thin provisioned (overallocated) back-end array, you need to reclaim storage and configure that back-end storage array according to the best practices of that device.

DRP technology is ideal for Flash storage without on-board compression. For example, with a compression pattern of 2:1 or higher, host I/O will be sliced up into 8 KB equal chunks, plus each 8 KB chunk is compressed to 4 KB or less, and is the optimal block size for leveraging Flash performance. This DRP compression implementation may lead up to 4x throughput for compressed workload with consistent performance.

There is no performance penalty for writing non-compressible data, and for application workloads with a 2:1 or higher compression ratio there is significant capacity saving with no performance overhead. This will cut down on a lot of planning work and simplify capacity savings for any storage solution.

DRP deduplication with compression provides the best storage efficiency. This combination deduplicates and then compresses the data, reducing the storage capacity usage. It is advised to use this option when the data pattern is compressible and it has a high duplication ratio, identified by the DRET tool. For more information, see 3.8.3, "Using Data Reduction Estimation Tool" on page 47.

3.10 General guidelines for performance, capacity, and availability options

This section describes performance, capacity, and availability options. We also describe data reduction choices in a little more depth.

3.10.1 Performance

First, determine which of the workloads are performance and which are capacity. Use Disk Magic to validate the IOPS requirements. Create a balanced system with the performance workloads using fully allocated volumes and FCM compression, and the capacity workloads using Data Reduced volumes.

If your workload is an absolute mystery, the best approach is to assume everything is a performance workload and use fully allocated volumes with FCM compression; or use Disk Magic to understand the performance of a configuration with DRP, and determine if it meets with expectations.

Port bandwidth

A single Fibre Channel port can deliver over 1.5 GBps (allowing for overheads) and an FC card in each canister with 8 ports can deliver more than 12 GBps. An NVMe device can perform at over 1 GBps.

A single Fibre Channel port can deliver 80,000 - 100,000 IOPS with a 4 Kb block size. An FC card in each canister with 8 ports can deliver up to 800,000 IOPS. An IBM FlashSystem 9100 can support over 1.1 million 4 Kb read miss IOPS.

So, if you have more than 12 NVMe devices, use two Fibre Channel cards per container, and a third Fibre Channel card enables you to achieve up to 33 GBps.

If you want to drive more than 600,000 IOPS, use two Fibre Channel cards per container.

How much cache do I need?

256 GB per system (128 GB base plus a 128 GB upgrade) is a good starting point. If you're using DRP or making heavy use of copy services, add a further 128 GB per system.

As your capacity increases (especially with the 19.2 TB FCM devices) add more cache to accommodate more of the working set (most accessed workloads, excluding snapshots, backups, and so on). A truly random working set might not benefit from a right-sized cache. If you're consolidating from multiple controllers, consider at least matching the amount of cache across those controllers.

Multiple volumes

IBM FlashSystem 9100 is optimized for multiple volumes, and around 30 volumes are required to unlock the maximum performance. A workload can become unnecessarily limited when backed by a single volume, and a single volume is limited to up to 10% of the ultimate performance.

If a single host or workload has a high performance requirement, consider creating multiple volumes and stripe data across them at the host level (for example, using Logical Volume Manager).

Adding volumes initially scales performance linearly and enables the workload to be balanced across the ports and canisters. You must verify the CPU core usage using the performance data.

Multiple Data Reduction Pools

A single Data Reduction Pool backed by a single DRAID6 array optimizes the amount of storage available, and in addition enables ease of management. However, the trade-off is that it can limit performance potential.

Two Data Reduction Pools backed by two DRAID6 arrays requires twice the amount of parity and spare capacity as a single DRAID6 array. However, workloads can be shared across two pools. Sharing all available resources increases the performance potential by 30 - 50%. It can also improve redundancy.

The IBM FlashSystem 9100 and Storwize V7000 are designed for complex, multi volume environments. Adhering to these best practices ensures the best experience.

What should I do?

Be realistic about your workload requirements and make every attempt to right size your system with appropriate cache and I/O cards and ports. Configure a balanced system with performance and capacity targeted volumes, and spread the resources by using multiple volumes and combining them at the host. If you're running many workloads, then a single volume might be good enough for each workload. If the balance of the system is leaning towards DRP, consider two Data Reduction Pools.

3.10.2 Capacity terminology

Before we go into detail about capacity planning, it is useful to define the terminology that is used in order to establish a common understanding.

These are the definitions IBM applies to capacity:

Raw capacity The reported capacity of the drives in the system before formatting or RAID.

Usable capacity The amount of capacity after formatting and RAID available for storing data on a system, pool, array, or MDisk. Usable capacity is the total of used and available capacity. For example, 50 TiB used and 50 TiB available is a usable capacity of 100 TiB.

Used capacity The amount of usable capacity taken up by data in a system, pool, array, or MDisk after data reduction techniques have been applied.

Available capacity The amount of usable capacity that is not yet used in a system, pool, array, or MDisk.

Effective capacity The amount of provisioned capacity that can be created in the system or pool without running out of usable capacity given the current data reduction savings being achieved. This capacity equals the physical capacity divided by the data reduction savings percentage.

Provisioned capacity Total capacity of all volumes in a pool or system.

Written capacity The amount of usable capacity that would have been used to store written data in a pool or system before data reduction is applied.

Overhead capacity The amount of usable capacity occupied by metadata in a pool or system and other data used for system operation.

Total capacity savings The total amount of usable capacity saved in a pool, system or volume through thin-provisioning and data reduction techniques. This capacity saved is the difference between the used usable capacity and the provisioned capacity.

Data reduction The techniques used to reduce the size of data including deduplication and compression.

Data reduction savings The total amount of usable capacity saved in a pool, system, or volume through the application of a compression or deduplication algorithm on the written data. This capacity saved is the difference between the written capacity and the used capacity.

Thin provisioning savings

The total amount of usable capacity saved in a pool, system, or volume by using usable capacity when needed as a result of write operations. The capacity saved is the difference between the provisioned capacity minus the written capacity.

Over provisioned A storage system or pool where there is more provisioned capacity than there is usable capacity.

Over provisioned ratio The ratio of provisioned capacity to usable capacity in the pool or system.

Provisioning limit (maximum provisioned capacity) over provisioning limit

In some storage systems, restrictions in the storage hardware or configured by the user that define a limit the maximum provisioned capacity allowed in a pool or system.

3.10.3 Capacity options

The IBM FlashSystem 9100 has 24 x 2.5" slots to populate with NVMe storage. NVMe Flashcore Modules (FCMs) use inline hardware compression to reduce the amount of physical space required, and these are available in 4.8 TB, 9.6 TB, and 19.2 TB sizes.

Industry-standard NVMe drives *don't* have hardware compression and are available in 1.92 TB, 3.84 TB, 7.68 TB, 15.36 TB sizes.

NVMe Flashcore Modules

FCMs compress and encrypt the data using hardware as it's written to the device at line speed. This gives the best performance with compression.

The drive attempts to compress data so that it uses less physical space. The potential capacity, taking into account the workload compressibility, is known as the effective capacity.

So, for example, if you have a 4.8 TB drive, and fill it with 2:1 compressible data, it can write nearly double the amount of data, meaning the effective capacity is close to 9.6 TB.

However, FCMs have a maximum effective capacity, beyond which they cannot be filled.

Data Reduction Pools (DRP) can be used with FCMs to increase the data reduction potential and increase the effective capacity.

Industry-standard NVMe drives

Industry-standard NVMe drives can encrypt data, but they don't compress it. Data Reduction Pools (DRP) can be used to reduce the amount of data sent to the drives, but the use of DRP results in a lower maximum performance threshold. The effective capacity is determined by the use of DRP, how compressible the workload is, and whether the system contains a lot of duplicate data.

3.10.4 NVMe storage frequently asked questions

The following questions are a sample of some that have been raised:

Can I use the FCMs in my FlashSystem 900 or V9000 in the FlashSystem 9100?

No. These modules use the same technology as the FlashSystem 9100 FCMs, but have a different form factor and interface.

Why do FCMs have a maximum effective capacity?

FCM drives contain a fixed amount of space for metadata. The maximum effective capacity is the amount of data it takes to fill the metadata space.

Can I fill up FCMs past 85%?

If you fill the system more than 85% full, the system has more work to do to manage the free space, which may impact performance.

What are the maximum effective capacities for each FCM?

For 4.8 TB, the maximum is 21.99 TB, which effectively limits the compression ratio to 4.5:1. 9.6 TB is 21.99 TB or 2.3:1, and 19.2 TB is 43.98 TB or 2.3:1. However, assuming you only fill the system to 85% to maintain the expected performance, you can increase these effective compression ratios by *(1/0.85).

Why does the 4.8 TB FCM have a higher compression ratio?

It has the same amount of metadata space as the 9.6 TB.

What capacity is shown for FCMs in the GUI and on the CLI?

The GUI shows you an estimate of the free physical space based on the data that's been written and the data reduction achieved.

What happens if I write a highly compressible workload to an FCM?

Even if you write a 10:1 compressible workload to an FCM, it will still be full when it reaches the maximum effective capacity. Any spare data space remaining at this point will be used to improve the performance of the module and extend the wear.

What happens if I write an uncompressible workload to an FCM?

The data will fill the drive to the physical capacity. If the data cannot be compressed further, or compressing the data causes it to grow in size, the uncompressed data will be written. In either case, because the FCM compression is done in hardware, there is no performance impact.

Why would I use DRP with FCMs?

Predominantly to take advantage of further data reduction savings that can be made using deduplication.

Should I use FCMs or industry-standard NVMe drives?

Industry-standard NVMe drives start at a smaller capacity point, accomodating a smaller system.

Can I mix NVMe drive types and sizes?

Yes, but why would you? NVMe drives must be put into a DRAID6 configuration (or DRAID5 if necessary, but this will give less protection), and must all be the same size. If you have mixed drive types and sizes, you need to purchase the drives in blocks of 6 or more, and manage them as two independent RAID arrays as opposed to one big one.

What size RAID array should I target?

The GUI selects the right geometry. For DRAID6, you need 6 - 24 drives, ideally configured as a single RAID array with 2 parity and 1 spare. You can define multiple RAID arrays if you want, but this will be at the cost of some capacity.

Can I add drives to the system later?

Yes, you can create another array. A future release may support DRAID expansion.

Figure 3-25 shows the maximum capacity.

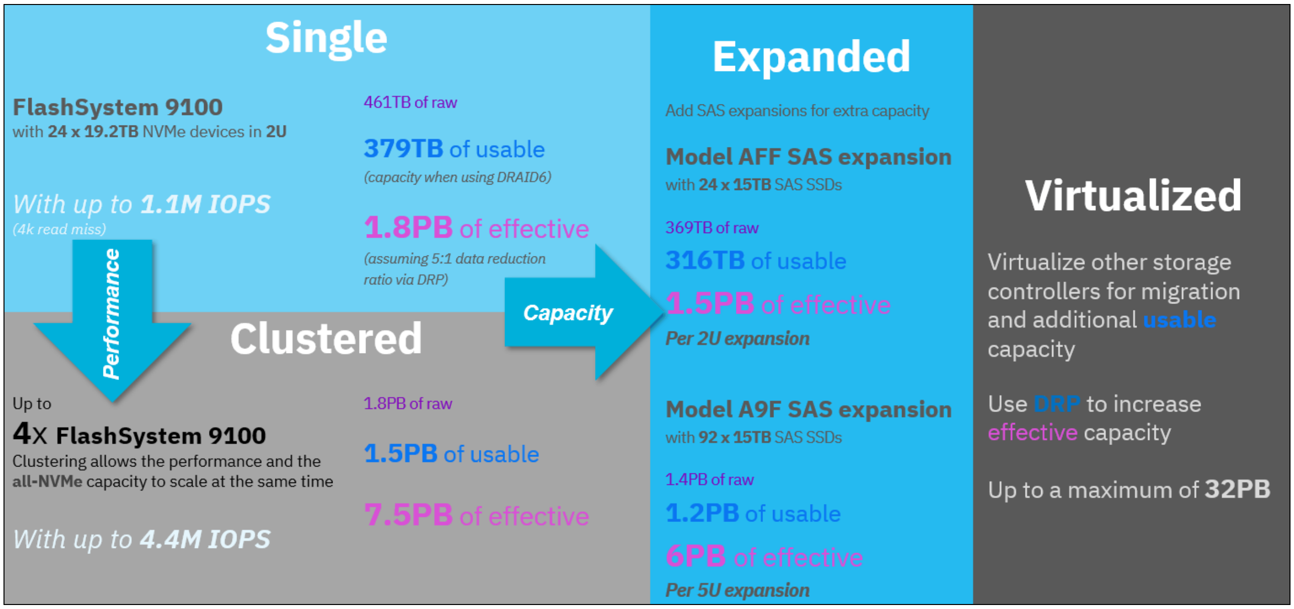


Figure 3-25 Maximum capacity

3.10.5 Size your system

These are the suggested steps to size your system:

1. Identify the size and performance of the workloads, along with any future growth.
2. Consider how data reduction technologies will be used (with FCMs and DRP).
3. Use the appropriate data reduction tooling to discover the compression and deduplication potential.
4. Use the Pre-sales tooling to size the system to meet the performance and capacity requirements.
5. IBM FlashSystem 9100 is optimized for 16 - 24 NVMe devices, to balance performance, rebuild times, and usable capacity. Fewer devices are fine for smaller capacity systems that don’t have a high performance requirement, but avoid a small number of large drives.

Data reduction tooling is shown in Figure 3-26 on page 57.

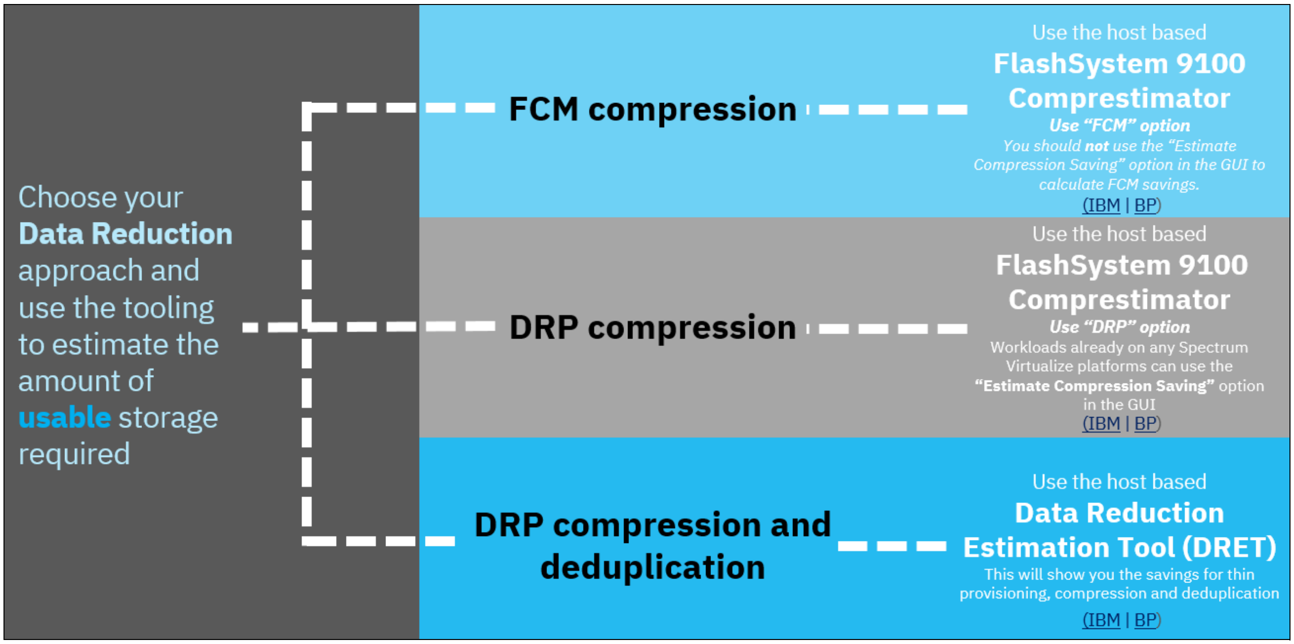


Figure 3-26 Data reduction tooling

Pre-sales tooling is shown in Figure 3-27.

Figure 3-27 Pre-sales tooling

3.10.6 Capacity planning frequently asked questions

The following questions are a sample of some that have been raised:

What does "optimized for 16 - 24 devices" mean'?

Data, parity, and spare space need to be striped across the number of devices available. The higher the number of devices, the lower the percentage of overall capacity the spare and parity devices consume, and the more bandwidth that is available during rebuild operations. Use Disk Magic to understand the performance of your proposed system better.

Can I mix NVMe and SAS drives in the same system?

Yes, but NVMe drives can only exist in the control enclosure, and SAS drives can only exist in SAS expansion enclosures.

Can I use Easy Tier?

Yes, all NVMe drives are tier 0, and all SAS SSD drives are tier 1. If you're tiering between compressing and non-compressing drives, you should be careful to ensure that you have enough physical capacity as data is moved between the tiers.

What are the SAS drive options?

Options include tier 1 SAS SSDs in 1.92 TB, 3.84 TB, 7.68 TB, and 15.36 TB sizes.

Can I mix SAS drive sizes?

SAS drives can be TRAID10, DRAID5, or DRAID6, with drives within those arrays being of the same size. As with NVMe, you can mix and match in different RAID arrays, but why?

Can I use spinning drives?

No, the FlashSystem 9100 is an All Flash Array. Storwize V7000 offers hybrid configurations. You can also virtualize other storage controllers behind the FlashSystem 9100, and optionally use EasyTier to create a tiered hybrid storage environment.

What's the maximum capacity?

32 PB, like other IBM Spectrum Virtualize products. This is a total of all virtualized storage.

Can I fill up the system to 100%?

If you fill the system more than 85% full then this will mean that the system has more work to do to manage the free space which may impact performance.

How many systems can I cluster together?

Up to 4. They can be a mixture of FlashSystem 9100, Storwize V7000 Gen2, and Gen2+.

How many enclosures are supported?

A single FlashSystem 9100 can support up to 20 AFF enclosures to a total of 504 drives (including NVMe), or it can support up to 8 A9F enclosures to a total of 760 drives. If you cluster FlashSystem 9100s together, the total number of drives increases linearly to a maximum of 3040. More details are available in the FlashSystem 9100 Sales Manual.

Why would I choose to use SAS enclosures over clustering more control enclosures?

Clustering scales performance with the additional NVMe storage. To just scale capacity within the performance envelope of a single controller, add SAS enclosures.

Can I use expansion enclosures from other IBM Spectrum Virtualize products?

No.

Why does DRET take a long time to run compared to Comprestimator?

DRET needs to read entire volumes to identify deduplicated data. Comprestimator samples volumes to derive an overall likely compression ratio.

Why do I need to use so many tools?

These tools have evolved over the years. IBM is seeking ways to streamline this process.

3.10.7 Data reduction choices

Typically there are two choices:

- Performance optimized
  - Fully allocated volumes
  - Highest performance
  - Lowest average response time
  - Compression is done inline with NVMe FCMs

Or

- Capacity optimized data reduction volume
  - Deduplication
  - Compression with NVMe, SAS, and virtualized drives
  - Lower maximum performance threshold

Performance optimized

Fully allocated volumes are the best performing, lowest latency option.

> **Note:** A fully allocated volume does not use a log structured array and enables the best performance. If the underlying storage is not compressing, the size of the volume is reserved on that storage so that out-of-space conditions are avoided.

Use fully allocated volumes for performance-critical workloads, and achieve data reduction using the inline hardware compression in FCM. Be aware that this does not provide for deduplication. Also, there is no thin provisioning or compression when using fully allocated volumes with non-compressing NVMe, SAS, or virtualized volumes.

Capacity optimized

Data reduction volumes provide for maximum data reduction, and uses Data Reduction Pool (DRP) technology. There is a trade-off and that is maximum performance for a gain in better data reduction. There are low response times for all but the most demanding workloads, and a 5:1 or more compression ratio for highly compressible workloads using Intel QuickAssist hardware. Deduplication is also available for workloads with a high degree of duplicate data (such as VDI). Data reduction volumes enable data reduction for all storage, not just FCMs.

Fully allocated and data reduction volumes can exist together in the same Data Reduction Pool, which provides the ability to manage all of the storage from a single pool. You might need to vary each individual volume type based on the characteristics of the workload.

Combining performance and capacity

So, use the performance optimized choice where the workload compresses, but performance and lowest latency is required. Balance a compression-only data reduction ratio (more storage) with low latency and high IOPS (less hardware), and get performance benefits even with non-compressing workloads.

Use the capacity optimized choice where the workload can benefit from deduplication, for example VDI, DevOps (production, pre-production, QA, and so on), and environments where there are a lot of copies of data. Environments with suitable workloads can deliver deduplication ratios up to 3:1 before compression.

Combining performance and capacity in the same system requires that you identify performance workloads that will represent the majority of your I/O, and assume data reduction using inline hardware compression.

In addition, you must identify capacity workloads that can maximise capacity with modest I/O, and assume data reduction with deduplication and compression.

Identifying the workload demands enables you to create a balanced high-performance, high-capacity system with a single point of management. As the workload evolves, you might need to migrate between fully allocated and data reduction volumes, so careful monitoring is required.

3.10.8 Evaluating workload using Disk Magic

Besides using test volumes, and observing actual performance for the application, IBM also has a tool called *Disk Magic* that is designed specifically for modeling performance.

Disk Magic for IBM is a performance analysis and hardware configuration planning tool for IBM storage disk subsystems that runs only on Microsoft Windows (XP or later). It is licensed by IBM from IntelliMagic for exclusive use by IBMers and IBM Business Partners in the selling of new or upgraded IBM disk storage solutions.

Proper initial sizing greatly helps to avoid future sizing problems. Disk Magic is one tool that is used for sizing and modeling storage subsystems for various open systems environments and various IBM platforms.

It provides accurate performance and capacity analysis and planning for IBM Spectrum Virtualize products, other IBM storage solutions, and other vendors' storage subsystems. Disk Magic provides in-depth environment analysis, and is an excellent tool to estimate the performance of a system that is running (DRP) Data Reduction Pools.

For IBM Business Partners who would like more information about Disk Magic, and the latest version, can be found at the Disk Magic website (login required).

3.11 Availability considerations when configuring the FS9100

This section highlights the implications storage pool configurations and host volume assignments have on availability.

This section includes:

- Availability considerations when configuring storage pools
- Availability considerations for host volume assignments

3.11.1 Availability considerations when configuring storage pools

Although the FS9100 provides many advantages through consolidation of storage, it is important to understand the implications that various configurations have on defining failure domains within the IBM Spectrum Virtualize Storwize cluster. When you select MDisks for a storage pool, performance is often the primary consideration. However, in many cases, the availability of the configuration is traded for little or no performance gain.

Remember that IBM Spectrum Virtualize and Storwize must take the entire storage pool offline if a single MDisk in that storage pool goes offline. Consider an example where you have 40 arrays of 1 TB each for a total capacity of 40 TB with all 40 arrays in the same storage pool.

In this case, you place the entire 40 TB of capacity at risk if one of the 40 arrays fails (which causes the storage pool to go offline). If you then spread the 40 arrays out over multiple storage pools, the effect of an array failure (an offline MDisk) affects less storage capacity, which limits the failure domain.

Consider the following preferred practices for availability:

- In an FS9100 clustered environment, create storage pools with IOgrp or Control Enclosure affinity. That means only use arrays or MDisks supplied by the internal storage that is directly connected to one IOgrps SAS chain. This configuration avoids having the availability of the storage pool dependent on the availability of all IOgrps in the cluster.
- When configuring storage pools from external storage, it is advised that each storage pool only contain MDisks from a single storage subsystem. An exception exists when implementing IBM System Storage Easy Tier, in which case having multiple storage controllers in a single pool is a requirement and cannot be avoided.
- It is suggested that each storage pool contains only MDisks from a single storage tier (SSD or Flash, Enterprise, or NL_SAS). An exception exists when implementing IBM System Storage Easy Tier, in which case multiple storage controllers in a single storage pool is required and cannot be avoided.
- A balance between the number and size of the storage pools is required. A small number of very large pools has a large failure boundary in the event the pools are taken offline due to a problem with one of the MDisks or its backing storage array. Too many small pools lead to performance issues. A general rule is to keep pools to under 250 TB, and the total number of pools to 8 or less.

3.11.2 Availability considerations for host volume assignments

Reducing the failure domain for back-end storage is only part of what should be considered from an availability standpoint. When you are determining the storage pool layout, you must also consider application boundaries and dependencies to identify any availability benefits that one configuration might have over another.

As we saw with storage pools in the previous section, host volume assignment can also have significant implications on failure domains. When multiple volumes from a single host are mapped to multiple IOgrps and Storage Pools within the FS9100 cluster, the failure domain for that host is expanded. This occurs because the availability of that host becomes dependent upon the availability of all IOgrps and Storage Pools its volumes are mapped to.

> **Note:** Limiting or reducing failure domains from an individual host perspective is not always advantageous in cases where redundancy exists outside of the individual host domain, such as within the database or application layer.

Consider the following preferred practices for availability:

- In an FS9100 clustered environment, allocate or map all volumes for a given host to a single IOgrp.
- In an FS9100 clustered environment, allocate or map all volumes for a given host to a single backend storage pool.

4

Planning

This chapter describes the steps that are required when you plan the installation of the IBM FlashSystem 9100 in your environment. This chapter considers the implications of your storage network from both the host attachment side and the virtualized storage expansion side. This chapter also describes all the environmental requirements that you must consider.

This chapter includes the following topics:

- FlashSystem 9100
- General planning introduction
- Physical planning
- Logical planning
- IBM Storage Insights
- IBM FlashSystem 9100 system configuration
- Licensing and features
- IBM FlashSystem 9100 configuration backup procedure
- Multi-cloud offerings and solutions

This planning guide is based on the IBM FlashSystem 9100 models AF7 and AF8. It also covers the SAS expansion enclosures models A9F and AFF.

4.1 FlashSystem 9100

The IBM FlashSystem 9100 storage system has the node canisters and the NVMe drives in one 2U high enclosure. On the previous product, the IBM FlashSystem V9000 AC2 / AC3 and the AE2 / AE3 combinations, the storage enclosures were separate 2U units and managed by the AC2 or AC3 control enclosures. This would make the V9000 clusters 6U high or more.

> **Note:** The IBM FlashSystem 9100 *node canisters* are also sometimes referred to as *controllers* or *nodes*. These terms are all interchangeable.

Figure 4-1 shows the relation of the previous IBM FlashSystem V9000 AC3 control enclosures, the managed AE2 enclosure, and the virtualized AE3 storage enclosure.

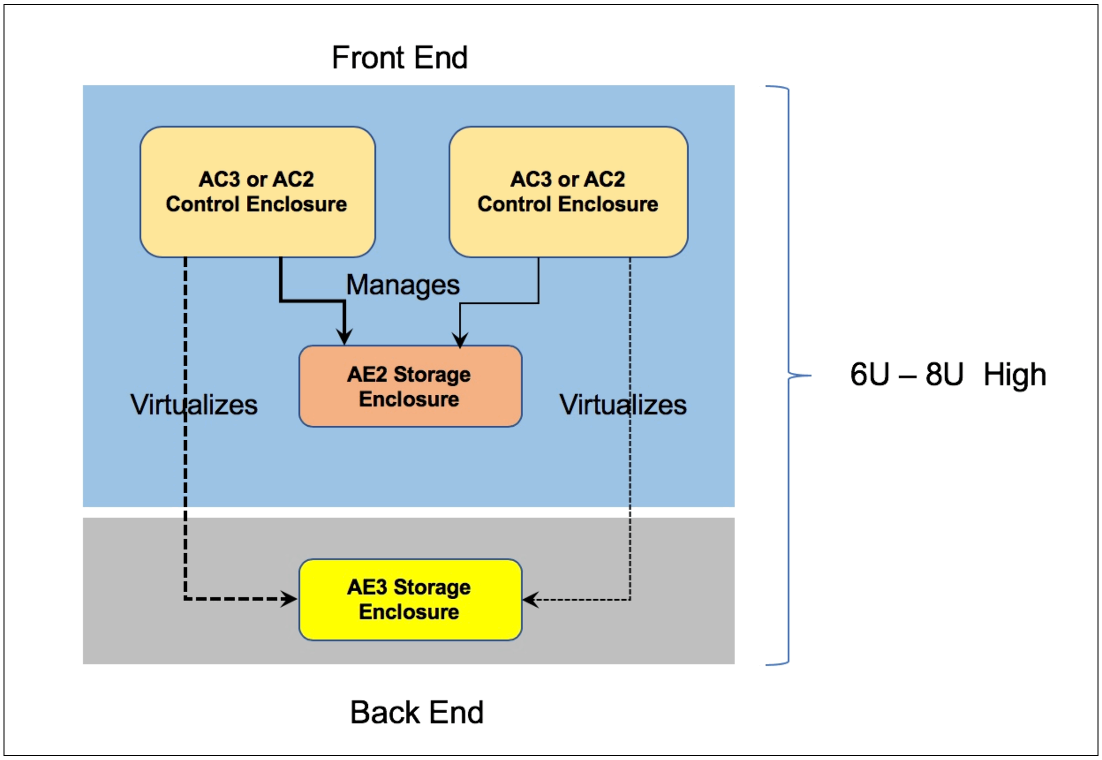


Figure 4-1 IBM FlashSystem V9000 AC2 / AC3 / AE2 / AE3 enclosure combinations

Figure 4-2 shows the relation of the IBM FlashSystem 9100 node canisters and the NVMe storage array. The complete system is contained in a 2U high enclosure, thus reducing the amount of rack space needed per system.

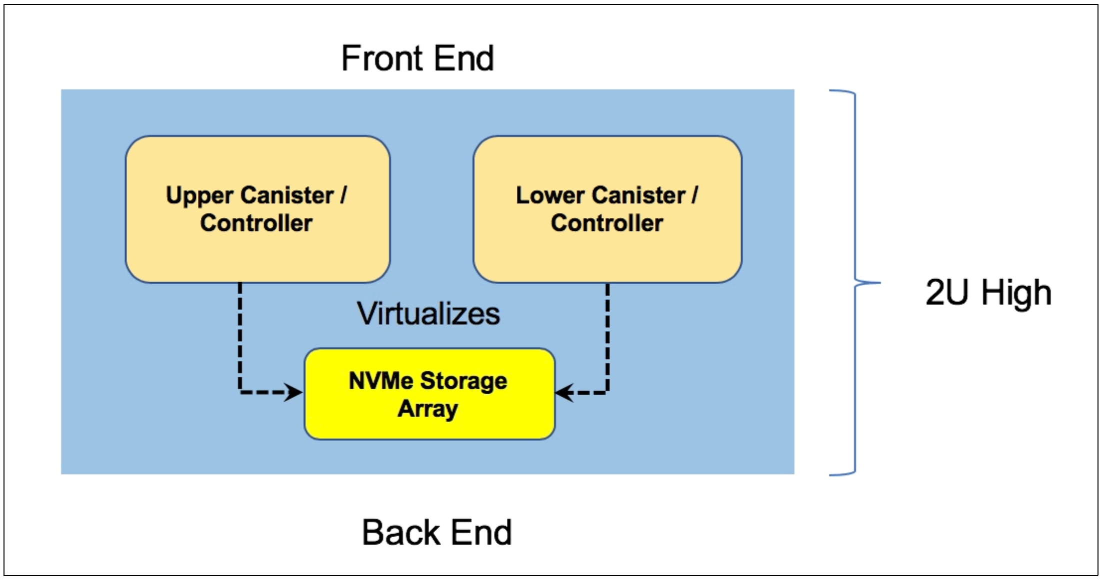


Figure 4-2 IBM FlashSystem 9100 node canisters and the NVMe storage array

4.2 General planning introduction

To achieve the most benefit from the IBM FlashSystem 9100, preinstallation planning must include several important steps. These steps can ensure that the IBM FlashSystem 9100 provides the best possible performance, reliability, and ease of management to meet the needs of your solution. Proper planning and configuration also helps minimize future downtime by avoiding the need for changes to the IBM FlashSystem 9100 and the storage area network (SAN) environment to meet future growth needs.

Important steps include planning the IBM FlashSystem 9100 configuration and completing the planning tasks and worksheets before system installation.

Figure 4-3 shows the IBM FlashSystem 9100 front view with one of the NVMe Flash Core Module drives partially removed.

Figure 4-3 IBM FlashSystem 9100 front view

IBM FlashSystem 9100 can be grown in two directions depending on the needs of the environment. This is known as the *scale-up, scale-out* capability:

- If extra capacity is needed, so *scale-up*, it can be increased by adding up to 24 NVMe drives per control enclosure.
- The IBM FlashSystem 9100 can have its capabilities increased, so *scale-out*, by adding up to four control enclosures in total to the solution to form a cluster. This increases both the capacity and the performance alike.
- The total capacity can be further extended by the addition of SAS all-flash expansion enclosures.This again is part of the *scale-up* strategy.

A fully configured IBM FlashSystem 9100 cluster consists of four control enclosures, each with 24 NVMe drives per enclosure.

This chapter covers planning for the installation of a single IBM FlashSystem 9100 solution, consisting of a single control enclosure. When you plan for larger IBM FlashSystem 9100 configurations, consider the required SAN and networking connections for the appropriate number of control enclosures and scale-up expansion of the SAS external enclosures.

For details about scalability and multiple control enclosures, see Chapter 5, “Scalability” on page 117.

Requirement: A pre-sale Technical Delivery Assessment (TDA) must be conducted to ensure that the configuration is correct and the solution being planned for is valid. A preinstallation TDA must be conducted shortly after the order is placed and before the equipment arrives at the customer’s location to ensure that the site is ready for the delivery, and that roles and responsibilities are documented regarding all the parties who will be engaged during the installation and implementation.

Before the system is installed and configured, you must complete all the planning worksheets. When the planning worksheets are completed, you submit them to the IBM service support representative (SSR).

Follow these steps when you plan for an IBM FlashSystem 9100 solution:

1. Collect and document the number of hosts (application servers) to attach to the IBM FlashSystem 9100, the traffic profile activity (read or write, sequential, or random), and the performance expectations for each user group (input/output (I/O) operations per second (IOPS) and throughput in megabytes per second (MBps)).
2. Collect and document the storage requirements and capacities:
   - Total external storage that will be attached to the IBM FlashSystem 9100
   - Required storage capacity for local mirror copy (Volume mirroring)
   - Required storage capacity for point-in-time copy (IBM FlashCopy)
   - Required storage capacity for remote copy (Metro Mirror and Global Mirror)
   - Required storage capacity for use of the IBM HyperSwap function
   - Required storage capacity for compressed volumes
   - Per host for storage capacity, the host logical unit number (LUN) quantity, and sizes
   - Required virtual storage capacity that is used as a fully managed volume and used as a thin-provisioned volume
3. Define the local and remote IBM FlashSystem 9100 SAN fabrics to be used for both the internal connections, if this is a multi-enclosure system, and the host and any external storage. Also plan for the remote copy or the secondary disaster recovery site as needed.

4. Define the number of IBM FlashSystem 9100 control enclosures and additional expansion storage controllers required for the site solution. Each IBM FlashSystem 9100 control enclosure that makes up an I/O Group is the container for the volume. The number of necessary I/O Groups depends on the overall performance requirements.
5. If applicable, also consider any IBM FlashSystem 9100 AFF or A9F expansion enclosure requirements and the type of drives needed in each expansion enclosure. See. 4.3.5, "SAS expansion enclosures" on page 79 for information on planning for the expansion enclosures.
6. Design the host side of the SAN according to the requirements for high availability and best performance. Consider the total number of ports and the bandwidth that is needed between the host and the IBM FlashSystem 9100, and the IBM FlashSystem 9100 and the external storage subsystems.
7. Design the internal side of the SAN according to the requirements as outlined in the cabling specifications for the number of IBM FlashSystem 9100 control enclosures being installed. This SAN network is used for both the IBM FlashSystem 9100 control enclosures and any external storage, if installed, data transfers. Connecting this network across inter-switch links (ISL) is not supported.

> **Important:** Check and carefully count the required ports for the wanted configuration. Equally important, consider future expansion when planning an initial installation to ensure ease of growth.

8. If your solution uses Internet Small Computer System Interface (iSCSI), design the iSCSI network according to the requirements for high availability (HA) and best performance. Consider the total number of ports and bandwidth that is needed between the host and the IBM FlashSystem 9100.
9. Determine the IBM FlashSystem 9100 cluster management and service Internet Protocol (IP) addresses needed. The IBM FlashSystem 9100 system requires the following addresses:
   - One cluster IP address for the IBM FlashSystem 9100 system as a whole
   - Two service IP addresses, one for each node canister within the control enclosures

   So for example, an IBM FlashSystem 9100 cluster comprising three control enclosures would need one management IP Address and six service IP addresses assigned.
10. Determine the IP addresses for the IBM FlashSystem 9100 system and for the hosts that connect through the iSCSI network.
11. Define a naming convention for the IBM FlashSystem 9100 control enclosures, host, and any external storage subsystem planned. For example, `ITSO_FS9100-1` shows that the IBM FlashSystem 9100 is mainly used by the International Technical Support Organization (ITSO) Redbooks team, and is the first IBM FlashSystem 9100 in the department.
12. Define the managed disks (MDisks) from any external storage subsystems.
13. Define storage pools. The use of storage pools depends on the workload, any external storage subsystem connected, more expansions or control enclosures being added, and the focus for their use. There might also be a need for defining pools for use by data migration requirements or Easy Tier. Easy Tier is discussed in detail in 4.6.3, "Easy Tier" on page 105.
14. Plan the logical configuration of the volumes within the I/O Groups and the storage pools to optimize the I/O load between the hosts and the IBM FlashSystem 9100.

15. Plan for the physical location of the equipment in the rack. IBM FlashSystem 9100 planning can be categorized into two types:
   - Physical planning
   - Logical planning

   The following sections describe these planning types in more detail.

> **Note:** IBM FlashSystem 9100 V8.2.0 provides GUI management of the HyperSwap function. HyperSwap enables each volume to be presented by two I/O groups. If you plan to use this function, you must consider the I/O Group assignments in the planning for the IBM FlashSystem 9100.

4.3 Physical planning

Use the information in this section as guidance when you are planning the physical layout and connections to use for installing your IBM FlashSystem 9100 in a rack and connecting to your environment.

Industry-standard racks are defined by the Electronic Industries Alliance (EIA) as 19-inch wide by 1.75-inch tall rack spaces or units, each of which is commonly referred to as *1U of the rack*. Each IBM FlashSystem 9100 control enclosure requires 2U of space in a standard rack. Additionally, each add-on SAS expansion enclosure requires either another 2U of space for the AFF or 5U of space for the A9F.

> **Important:** IBM FlashSystem 9100 is approximately 850mm deep, so will require a rack of these dimensions to house it. Also it *must* have the required service clearance at the rear of the rack to allow for concurrent maintenance of the node canisters.
>
> For the IBM T42 rack this is specified in IBM Knowledge Center:
> https://www.ibm.com/support/knowledgecenter/9009-22A/p9had/p9had_t00t42svc.htm
>
> For non-IBM racks the service clearance at the rear *must* be ar least 36 inches (915mm) to allow for installation and concurrent maintenance of the node canisters.

When growing the IBM FlashSystem 9100 solution by adding control enclosures and expansions, the best approach is to plan for all of the members to be installed in the same rack for ease of cabling the internal dedicated SAN fabric connections. One 42U rack can house an entire maximum configuration of an IBM FlashSystem 9100 solution, and also its SAN switches and an Ethernet switch for management connections. Depending on the number of additional expansion enclosers, you may need to plan for extra racks.

Figure 4-4 on page 69 shows a partially configured solution of two IBM FlashSystem 9100 control enclosures plus two additional scale out A9F expansion enclosures and two AFF expansion enclosures in a 42U rack.

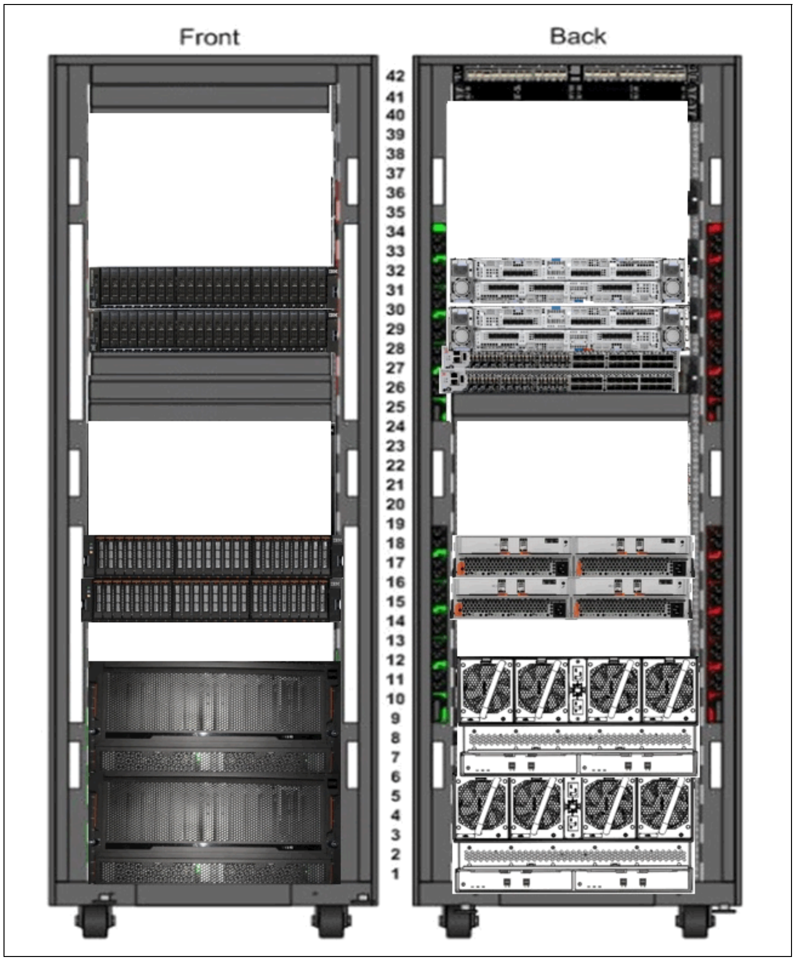


Figure 4-4 Control enclosures plus additional scale out expansion enclosures

4.3.1 IBM FlashSystem 9100 control enclosures

Each IBM FlashSystem 9100 (FS9100) control enclosure can support up to six PCIe expansion I/O cards to provide a range of connectivity and capacity expansion options.

Four types of I/O adapter options can be ordered, as shown in Table 4-1.

Table 4-1 IBM FlashSystem 9100 control enclosure adapter card options

Number of Cards	Ports	Protocol	Possible Slots	Comments
0 - 3	4	16 Gb Fibre Channel	1, 2, 3	
0 - 3	2	25 Gb Ethernet (iWarp)	1, 2, 3	
0 - 3	2	25 Gb Ethernet (RoCE)	1, 2, 3	
0 - 1	2 - see comment	12 Gb SAS Expansion	1, 2, 3	Card is 4 port with only 2 ports active (ports 1 and 3)

Feature Code AHB3: 16 Gb FC 4 Port Adapter Cards (Pair)

- This feature provides two I/O adapter cards, each with four 16 Gb FC ports and shortwave SFP transceivers. It is used to add 16 Gb FC connectivity to the FS9100 control enclosure.
- This card also supports longwave transceivers that can be intermixed on the card with shortwave transceivers in any combination. Longwave transceivers are ordered using feature ACHU.
- Minimum required: None.
- Maximum allowed:
  - None when the total quantity of features AHB6, AHB7, and AHBA is three.
  - One when the total quantity of features AHB6, AHB7, and AHBA is two.
  - Two when the total quantity of features AHB6, AHB7, and AHBA is one.
  - Three when the total quantity of features AHB6, AHB7, and AHBA is zero.

Feature Code AHB6: 25 GbE (RoCE) Adapter Cards (Pair)

- This feature provides two I/O adapter cards, each with two 25 Gb Ethernet ports and SFP28 transceivers. It is used to add 25 Gb Ethernet connectivity to the FlashSystem 9100 control enclosure and are designed to support RDMA with RoCE v2.
- Note: This adapter does not support FCoE connectivity. When 2 of these adapters are installed, clustering with other FlashSystem 9100 systems would not be possible.
- Minimum required: None.
- Maximum allowed:
  - None when the total quantity of features AHB3, AHB7, and AHBA is three.
  - One when the total quantity of features AHB3, AHB7, and AHBA is two.
  - Two when the total quantity of features AHB3, AHB7, and AHBA is one.
  - Three when the total quantity of features AHB3, AHB7, and AHBA is zero.

Feature Code AHB7: 25GbE (iWARP) Adapter Cards (Pair)

- This feature provides two I/O adapter cards, each with two 25 Gb Ethernet ports and SFP28 transceivers. It is used to add 25 Gb Ethernet connectivity to the FlashSystem 9100 control enclosure, and is designed to support RDMA with iWARP.
- Note: This adapter does not support FCoE connectivity. When 2 of these adapters are installed, clustering with other FlashSystem 9100 systems would not be possible.
- Minimum required: None.
- Maximum allowed:
  - None when the total quantity of features AHB3, AHB6, and AHBA is three.
  - One when the total quantity of features AHB3, AHB6, and AHBA is two.
  - Two when the total quantity of features AHB3, AHB6, and AHBA is one.
  - Three when the total quantity of features AHB3, AHB6, and AHBA is zero.

Feature Code AHBA: SAS Expansion Enclosure Attach Card (Pair)

- This feature provides two four port 12 Gb SAS expansion enclosure attachment card.
- This feature is used to attach up to twenty expansion enclosures to a FlashSystem 9100 control enclosure.
- Minimum required: None.
- Maximum allowed:
  - None when the total quantity of features AHB3, AHB6, and AHB7 is three.
  - One when the total quantity of features AHB3, AHB6, and AHB7 is two or less.

Note: Only two of the four SAS ports on the SAS expansion enclosure attachment card are used for expansion enclosure attachment. Only ports 1 and 3 are used; the other two SAS ports are inactive.

Figure 4-5 shows the IBM FlashSystem 9100 PCIe slot locations.

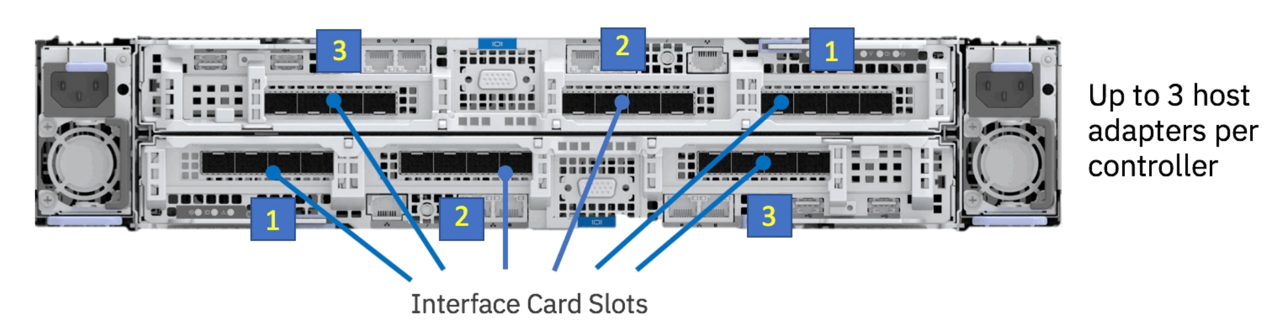


Figure 4-5 IBM FlashSystem 9100IBM FlashSystem 9100 PCIe slot locations

Attention: The upper controller PCIe slot positions are counted *right to left* because the node canister hardware is mounted upside down in the enclosure.

4.3.2 Racking considerations and IBM FlashSystem 9100 location

IBM FlashSystem 9100 is installed as a minimum of a one control enclosure configuration. Each control enclosure is designed with the two node canisters and up to 24 NVMe drives installed (it is 2U high). Ensure that the space for the entire system is available if more than one IBM FlashSystem 9100 control enclosure, or additional expansion encloses, are to be installed.

Use Table 4-2 to help plan the rack locations that you use for up to a 42U rack. Complete the table for the hardware locations of the IBM FlashSystem 9100 system and other devices.

Table 4-2 Hardware location planning of the IBM FlashSystem 9100 in the rack

Rack unit	Component
EIA 42	
EIA 41	
EIA 40	
EIA 39	
EIA 38	
EIA 37	
EIA 36	
EIA 35	
EIA 34	
EIA 33	

Rack unit	Component
EIA 32	
EIA 31	
EIA 30	
EIA 29	
EIA 28	
EIA 27	
EIA 26	
EIA 25	
EIA 24	
EIA 23	
EIA 22	
EIA 21	
EIA 20	
EIA 19	
EIA 18	
EIA 17	
EIA 16	
EIA 15	
EIA 14	
EIA 13	
EIA 12	
EIA 11	
EIA 10	
EIA 9	
EIA 8	
EIA 7	
EIA 6	
EIA 5	
EIA 4	
EIA 3	
EIA 2	
EIA 1	

4.3.3 Power requirements

Each IBM FlashSystem 9100 control enclosure requires two IEC-C13 power cable connections to connect to their 2000 W (2 KW) power supplies. Country-specific power cables are available for ordering to ensure that proper cabling is provided for the specific region. A total of two power cords are required to connect each IBM FlashSystem 9100 control enclosures to the rack power.

Figure 4-6 shows an example of a FlashSystem 9100 control enclosure with the two 2000 W power supplies and the connection points for the power cables in each node canister.

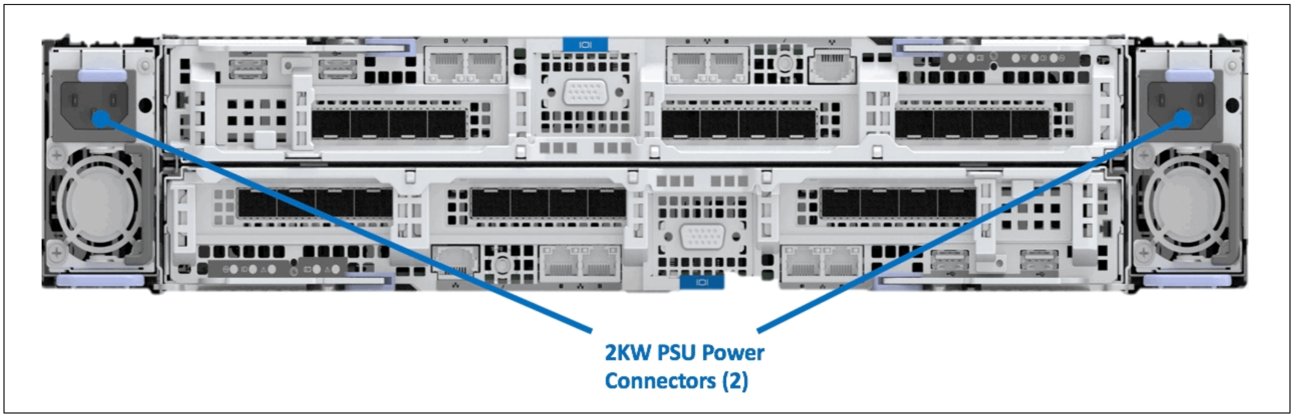


Figure 4-6 IBM FlashSystem 9100 control enclosure power connections

Each IBM FlashSystem 9100 Model AFF SAS expansion enclosure requires two IEC-C13 power cable connections to connect to their 764 W power supplies. Country-specific power cables are available for ordering to ensure that proper cabling is provided for the specific region. A total of two power cords are required to connect each IBM FlashSystem 9100 AFF expansion enclosures to the rack power.

Figure 4-7 shows an example of a IBM FlashSystem 9100 AFF expansion enclosure with the two 764 W power supplies and the connection points for the power cables in each node canister.

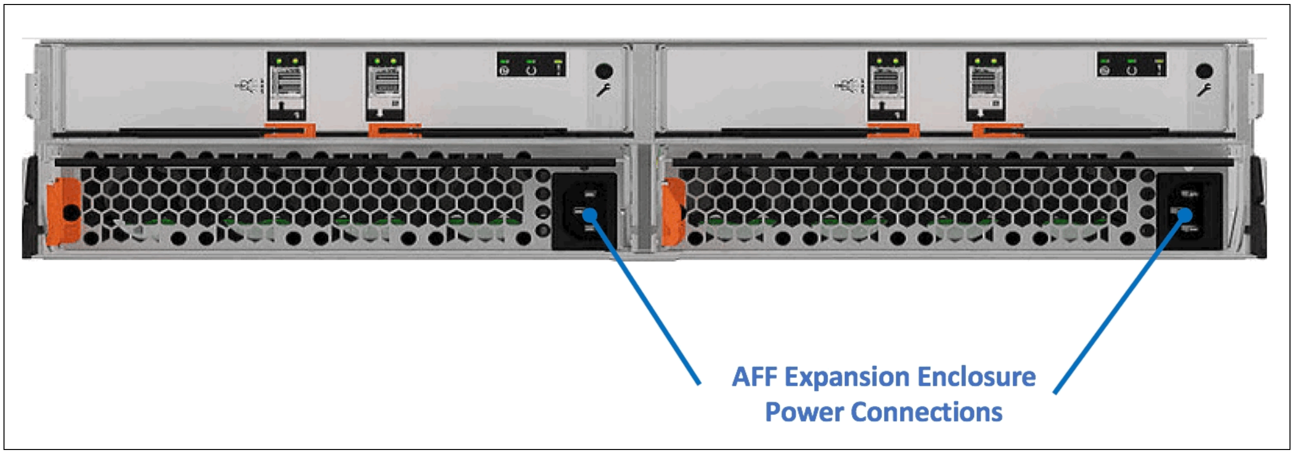


Figure 4-7 IBM FlashSystem 9100 AFF expansion enclosure power connections

Each IBM FlashSystem 9100 Model A9F SAS expansion enclosure requires two IEC-C19 power cable connections to connect to their 2400 W (2.4 KW) power supplies. Country-specific power cables are available for ordering to ensure that proper cabling is provided for the specific region. A total of two power cords are required to connect each IBM FlashSystem 9100 A9F expansion enclosures to the rack power.

Figure 4-8 shows an example of a IBM FlashSystem 9100 A9F expansion enclosure with the two 2400 W power supplies and the connection points for the power cables in each controller.

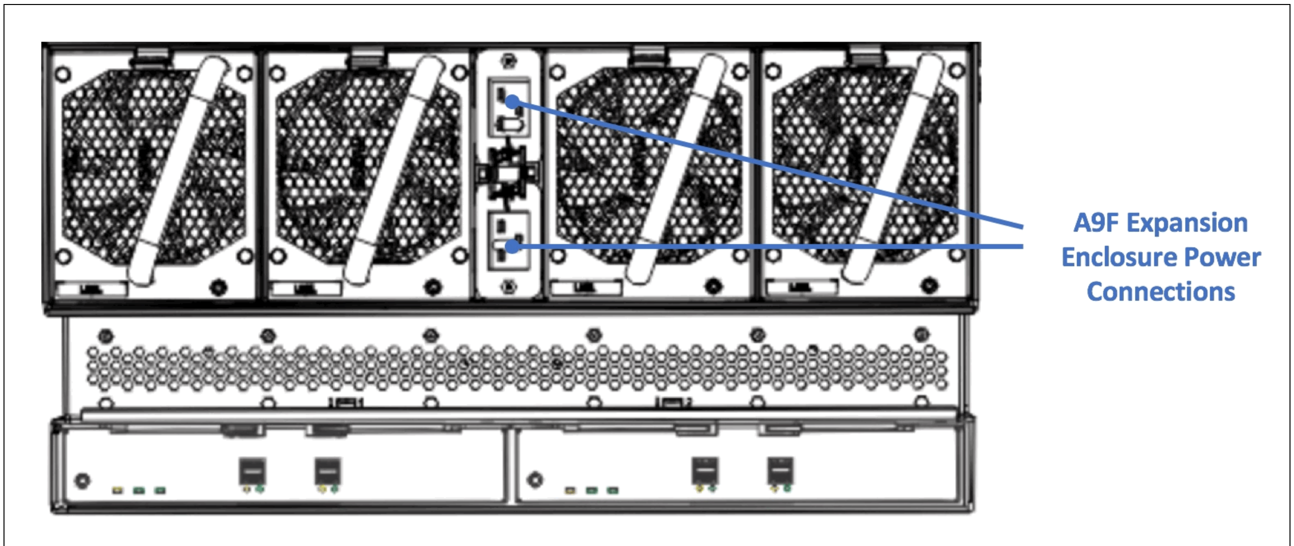


Figure 4-8 IBM FlashSystem 9100 A9F expansion enclosure power connections

Upstream redundancy of the power to your cabinet (power circuit panels and on-floor Power Distribution Units (PDUs)), within cabinet power redundancy (dual power strips or in-cabinet PDUs), and upstream high availability structures (uninterruptible power supply (UPS), generators, and so on) influence your power cabling decisions.

If you are designing an initial layout that will have future growth plans to follow, you should plan to enable the additional control enclosures to be co-located in the same rack with your initial system for ease of planning for the additional interconnects required. A maximum configuration of the FlashSystem 9100, with dedicated internal switches for SAN and local area network (LAN) and additional expansion enclosures, can almost fill a 42U 19-inch rack.

> **Tip:** When cabling the power, connect one power cable from each enclosure to the left side internal PDU and the other power supply power cable to the right side internal PDU. This enables the cabinet to be split between two independent power sources for greater availability. When adding more FlashSystem 9100 control or expansion enclosures to the solution, continue the same power cabling scheme for each additional enclosure.

You must consider the maximum power rating of the rack: *do not exceed it*. For more power requirement information, see Planning for Power in IBM Knowledge Center.

4.3.4 Network cable connections

There are various checklists and tables that you can use to plan for all the various types of network connections (for example FC, Ethernet, iSCSI, SAS, and so on) on the IBM FlashSystem 9100.

You can download the latest cable connection tables from the IBM FlashSystem 9100 page of IBM Knowledge Center by using the following steps:

1. Go to the IBM FlashSystem 9100 page in IBM Knowledge Center.
2. Go to the **Table of Contents.**
3. Click **Planning** on the left side panel.
4. In the list of results, select **Planning worksheets (customer task)**.
5. Here you can select from the following options for download:
   – Planning worksheets for system connections
   – Planning worksheets for network connections
   – Planning for management and service IP addresses
   – Planning for SAS Expansion enclosures (if installed)

Some sample worksheets are included here to give an overview of required information.

PCIe adapters and connections

Figure 4-9 shows the FC port locations. These are identified for all the possible fiber connections across the two IBM FlashSystem 9100 node canisters.

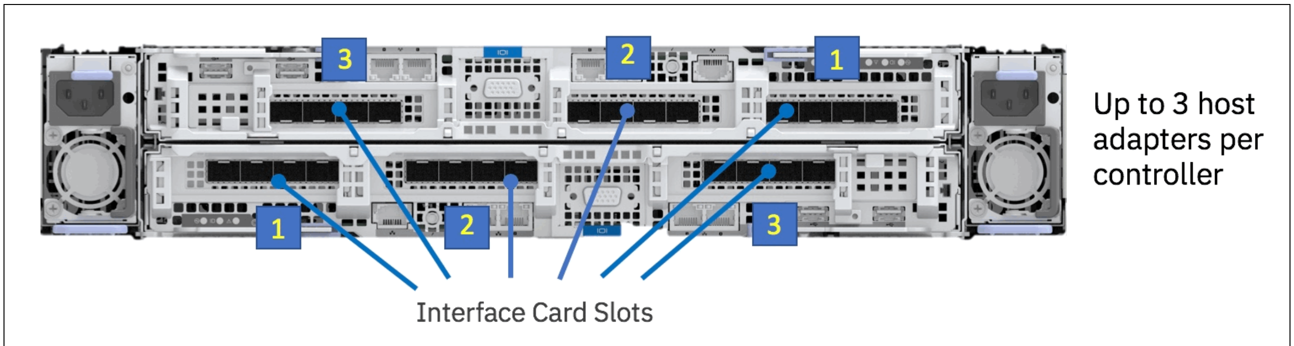


Figure 4-9 IBM FlashSystem 9100 FC port locations

Note: The upper node canister FC card PCIe slot positions are counted *right to left* because the node canister hardware is installed upside down in the IBM FlashSystem 9100 control enclosure.

Create a cable connection table or similar documentation to track all of the connections that are required for the setup of these items:

- Ethernet
- FC ports: Host and internal
- iSCSI (iWarp or ROCE)

Slot numbers and adapter types are listed in Table 4-3.

Table 4-3 IBM FlashSystem 9100 node canister PCIe slot numbers and adapter type

PCIe slot	Adapter types
1	Fibre Channel or Ethernet or SAS
2	Fibre Channel or Ethernet or SAS
3	Fibre Channel or Ethernet or SAS

The following charts are sample ones for the various network connections. See the previous IBM Knowledge Center links for the latest versions of these planning sheets.

Fibre Channel Ports

Use Table 4-4 to document FC port connections for a single control enclosure.

Table 4-4 Fibre Channel (FC) port connections

Location	Item	Fibre Channel port 1	Fibre Channel port 2	Fibre Channel port 3	Fibre Channel port 4
Node canister 1 Fibre Channel card 1	Switch host:				
	Port:				
	Speed:				
Node canister 1 Fibre Channel card 2	Switch host:				
	Port:				
	Speed:				
Node canister 1 Fibre Channel card 3	Switch host:				
	Port:				
	Speed:				
Node canister 2 Fibre Channel card 1	Switch host:				
	Port:				
	Speed:				
Node canister 2 Fibre Channel card 2	Switch host:				
	Port:				
	Speed:				
Node canister 2 Fibre Channel card 3	Switch host:				
	Port:				
	Speed:				

Ethernet Port Connections

Support for ethernet connections is via either the onboard ports or by adding extra ethernet PCIe adapters. Table 4-5 shows the layout of the onboard ethernet connections.

Table 4-5 Node canister onboard Ethernet port connections

Component	Ethernet port 1	Ethernet port 2	Ethernet port 3	Ethernet port 4	Technician port
Node Canister 1 (upper)					
Switch					none
Port					none
Speed	10 Gbps or 1 Gbps	10 Gbps or 1 Gbps	10 Gbps or 1 Gbps	10 Gbps or 1 Gbps	1 Gbps only
Node Canister 2 (lower					
Switch					none
Port					none
Speed	10 Gbps or 1 Gbps	10 Gbps or 1 Gbps	10 Gbps or 1 Gbps	10 Gbps or 1 Gbps	1 Gbps only

Each node canister also supports up to three optional two-port 25 Gbps Internet wide-area RDMA Protocol (iWARP) or RDMA over Converged Ethernet (RoCE) Ethernet adapters.

The following guidelines must be followed if 25 Gbps Ethernet adapters are installed:

- iWARP and RoCE Ethernet adapters cannot be mixed within a node canister.
- Fibre Channel adapters are installed before Ethernet adapters, beginning with slot 1, then slot 2 and slot 3.
- Ethernet adapters are installed beginning with the first available slot.
- If an SAS adapter is required to connect to expansion enclosures, it must be installed in slot 3.

Table 4-6 shows the 25 GbE adapter port connections, speeds, and switch port assignments.

Table 4-6 25 Gbps Ethernet adapter port connections

Component	Adapter 1 Ethernet port 1	Adapter 1 Ethernet port 2	Adapter 2 Ethernet port 1	Adapter 2 Ethernet port 2	Adapter 3 Ethernet port 1	Adapter 3 Ethernet port 2
Node Canister 1 (upper)						
Switch						
Port						
Speed	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps
Node Canister 2 (lower)						
Switch						
Port						
Speed	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps	25 or 10 Gbps

Management and Service IP Addresses

Figure 4-10 shows the locations of the onboard ethernet ports and the technician port. The technician port is used by the SSR when installing the IBM FlashSystem 9100.

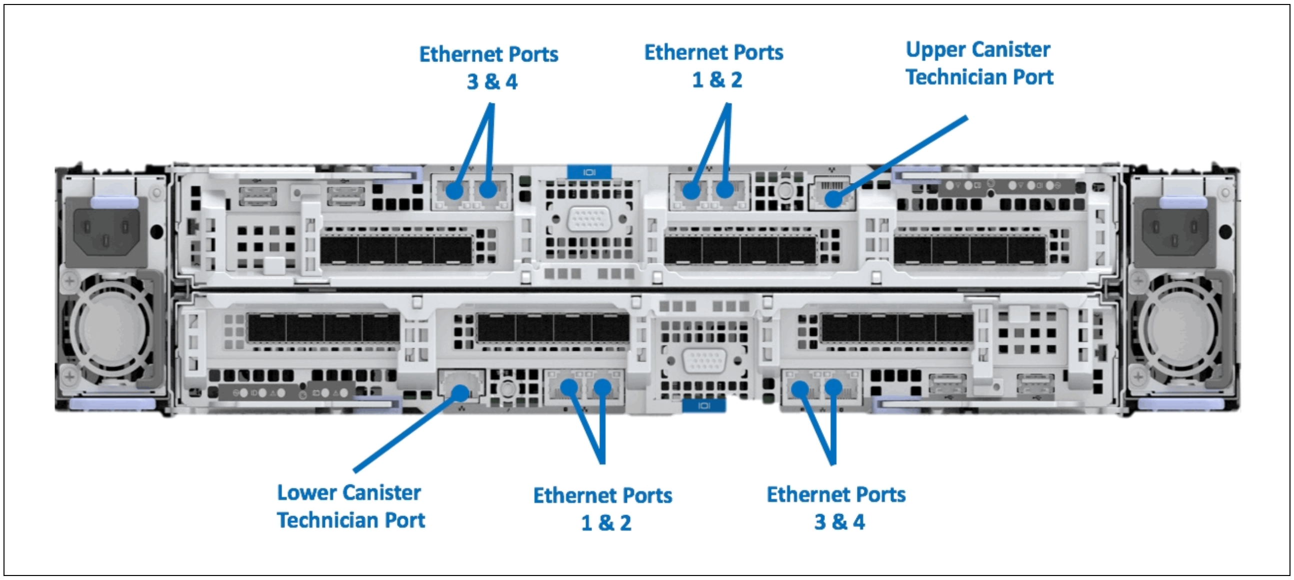


Figure 4-10 IBM FlashSystem 9100 technician and ethernet port locations

Use Table 4-7 to document the management and service IP address settings for the IBM FlashSystem 9100 control enclosure in your environment.

> **Important:** The upper node canister ethernet port positions are counted *right to left* because the upper node canister hardware is installed upside down in the IBM FlashSystem 9100 control enclosure.

Table 4-7 IP addresses for the IBM FlashSystem 9100 control enclosure

Cluster name:	
IBM FlashSystem 9100 control enclosure:	
Management IP address:	
IP:	
Subnet mask:	
Gateway:	
Node canister #1 Service IP address:	
IP:	
Subnet mask:	
Gateway:	
Node canister #2 Service IP address:	
IP:	
Subnet mask:	
Gateway:	

Note: If you have more than one IBM FlashSystem 9100 control enclosure to configure, you need two extra service IP addresses per additional IBM FlashSystem 9100 control enclosure. Only one management IP address is required per IBM FlashSystem 9100 cluster.

The assignments of the additional ethernet ports that can be used for host I/O are explained in the Logical Planning section in 4.4.1, “Management IP addressing plan” on page 81.

4.3.5 SAS expansion enclosures

Two models of SAS expansion enclosures are offered:

- 9846/9848-A9F
- 9846/9848-AFF

The following list describes the maximum individual expansion enclosure capacities:

- A 9846/9848-AFF SAS expansion enclosure contains up to 24 2.5 inch high capacity SSDs, and up to 368.6 TB raw capacity.
- A 9846/9848-A9F SAS expansion enclosure supports up to 92 drives, 2.5 inch high capacity SSDs (in 3.5 inch carriers), and up to 1.413 TB raw capacity.

To support a flash-optimized tiered storage configuration for mixed workloads, up to 20 9846/9848-AFF SAS expansion enclosures can be connected to each IBM FlashSystem 9100 control enclosure in the system. A maximum of eight A9F expansion enclosures can be attached. See Enclosures in IBM Knowledge Center for the rules on mixing the AFF and A9F expansion enclosures, attached to each IBM FlashSystem 9100 control enclosure.

A single FlashSystem 9100 control enclosure can support up to twenty FlashSystem 9100 SFF expansion enclosures with a maximum of 504 drives per system or up to eight FlashSystem 9100 LFF HD expansion enclosures with a maximum of 760 drives per system. Intermixing of expansion enclosures in a system is supported. Expansion enclosures are designed to be dynamically added with virtually no downtime, helping to quickly and seamlessly respond to growing capacity demands.

With four-way system clustering, the size of the system can be increased to a maximum of 3,040 drives. FlashSystem 9100 systems can be added into existing IBM FlashSystem 9100 clustered systems.

Further scalability can be achieved with virtualization of external storage. When FlashSystem 9100 virtualizes an external storage system, capacity in the external system inherits the functional richness and ease of use of FlashSystem 9100.

Expansion enclosure model AFF

The IBM FlashSystem 9100 SFF Expansion Enclosure Model AFF has the following features:

- Two expansion canisters
- 12 Gb SAS ports for control enclosure and expansion enclosure attachment
- Support for up to twenty four 2.5-inch SAS SSD flash drives
- 2U, 19-inch rack mount enclosure with AC power supplies

Expansion enclosure model A9F

The IBM FlashSystem 9100 High-Density (HD) Expansion Enclosure Model A9F delivers increased storage density and capacity for IBM FlashSystem 9100 with cost-efficiency while maintaining its highly flexible and intuitive characteristics:

- 5U, 19-inch rack mount enclosure with slide rail and cable management assembly
- Support for up to ninety-two 3.5-inch large-form factor (LFF) 12 Gbps SAS top-loading SSD drives
- Redundant 200 - 240 VA power supplies (new PDU power cord required)
- Up to 8 HD expansion enclosures are supported per IBM FlashSystem 9100 control enclosure, providing up to 368 drives and 11.3 PB SSD capacity in each enclosure (up to a maximum of 32 PB total)
- With four enclosures, a maximum of 32 HD expansion enclosures can be attached, supporting a maximum 32 PB of raw SSD capacity

All drives within an expansion enclosure must be the SSD type, but a variety of drive models are supported for use in the IBM FlashSystem 9100 expansion enclosures. These drives are hot swappable and have a modular design for easy replacement.

The following 12 Gb SAS industry-standard drives are supported in IBM FlashSystem 9100 AFF and A9F expansion enclosures:

- 1.92 TB 12 Gb SAS flash drive (2.5-inch and 3.5-inch form factor features)
- 3.84 TB 12 Gb SAS flash drive (2.5-inch and 3.5-inch form factor features)
- 7.68 TB 12 Gb SAS flash drive (2.5-inch and 3.5-inch form factor features)
- 15.36 TB 12 Gb SAS flash drive (2.5-inch and 3.5-inch form factor features)

Note: To support SAS expansion enclosures, an AHBA - SAS Enclosure Attach adapter card must be installed in each node canister of the IBM FlashSystem 9100 control enclosure.

SAS expansion enclosure worksheet

If the system includes optional SAS expansion enclosures, you must record the configuration values that will be used by the IBM SSR during the installation process.

Complete Table 4-8 on page 81 based on your particular system, and provide this worksheet to the IBM SSR prior to system installation.

Table 4-8 Configuration values: SAS enclosure x, controller block x, and SAS enclosure n, controller block n

Configuration setting	Value	Usage in CLI
MDisk group name	xxxx	**`mkmdiskgrp -name mdisk_group_name -ext extent_size`**
MDisk extent size in MB	xxxx	
RAID level (DRAID5 or DRAID6)	xxxx	**`mkdistributedarray -level raid_level -driveclass driveclass_id -drivecount x -stripewidth x -rebuildareas x mdiskgrp_id | mdiskgrp_name`**
`driveclass_id`: The class that is being used to create the array, which must be a numeric value.	xxxx	
`drivecount`: The number of drives to use for the array. The minimum drive count for DRAID5 is 4; the minimum drive count for DRAID6 is 6.	xxxx	
`stripewidth`: The width of a single unit of redundancy within a distributed set of drives. For DRAID5, it is 3 - 16; for RAID6, it is 5 - 16.	xxxx	
`rebuildareas`: The reserved capacity that is distributed across all drives available to an array. Valid values for DRAID5 and DRAID6 are 1, 2, 3, and 4.	xxxx	

If SAS expansion intermix of enclosures is required, see 5.3, “Scale up for capacity” on page 121.

External storage systems

You can attach, and virtualize, many types of external storage systems to the IBM FlashSystem 9100, both IBM and non-IBM varieties.

For more information about how to do this, see this extensive guide in IBM Knowledge Center.

4.4 Logical planning

Each IBM FlashSystem 9100 control enclosure creates a single I/O Group, and can contain up to four I/O Groups, with a total of four control enclosures, configured as one cluster.

This section includes the following topics:

- Management IP addressing plan
- SAN zoning and SAN connections
- IP replication and mirroring
- Native IP replication
- Advanced Copy Services
- Call Home option
- Remote Support Assistance (RSA)

4.4.1 Management IP addressing plan

To manage the IBM FlashSystem 9100 system, you access the management GUI of the system by directing a web browser to the cluster’s management IP address.

The IBM FlashSystem 9100 also uses a *technician port* feature. This is defined on node canisters and marked with the letter “T”. All initial configuration for the IBM FlashSystem 9100 is performed through the technician port. The port broadcasts a Dynamic Host Configuration Protocol (DHCP) service so that any notebook or computer with DHCP enabled can be automatically assigned an IP address on connection to the port.

Note: The hardware installation process for the IBM FlashSystem 9100 is completed by the IBM SSR. If the IBM FlashSystem 9100 is a scalable solution, the SSR works in conjunction with the IBM Lab Services team to complete the installation.

After the initial cluster configuration has been completed, the technician port automatically routes the connected user directly to the service GUI for the specific node canister.

Table 4-9 shows a summary of the onboard ethernet ports, speeds, and functions.

Table 4-9 Onboard ethernet ports, speeds, and functions

Ethernet Port	Speed	Function	Comments
1	10 Gbps	Management IP, Service IP, Host I/O	Primary Management Port
2	10 Gbps	Management IP, Service IP, Host I/O	Secondary Management Port
3	10 Gbps	Host I/O	Cannot be used for internal control enclosure communications
4	10 Gbps	Host I/O	Cannot be used for entangle control ensure communications
T	1 Gbps	Technician Port - DHCP/DNS for direct attach service management	SSR Use Only

Each IBM FlashSystem 9100 node canister requires one Ethernet cable connection to an Ethernet switch or hub. The cable must be connected to port 1. For each cable, a 10/100/1000 Mb Ethernet connection is required. Both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) are supported.

Note: For increased redundancy, an optional second Ethernet connection is supported for each node canister. This cable can be connected to Ethernet port 2.

To ensure system failover operations, Ethernet port 1 on all IBM FlashSystem 9100 node canisters must be connected to the common set of subnets. If used for increased redundancy, Ethernet port 2 on all IBM FlashSystem 9100 node canisters must also be connected to a common set of subnets. However, the subnet for Ethernet port 1 does not have to be the same as the subnet for Ethernet port 2.

Each IBM FlashSystem 9100 cluster must have a cluster management IP address and also a service IP address for each of the IBM FlashSystem 9100 node canisters in the cluster. The service IP addesss does not have its own unique ethernet cable. It uses the same physical cable as the management IP addresses use.

Example 4-1 shows details.of the IBM FlashSystem 9100 Management IP addresses for one control enclosure.

Example 4-1 IBM FlashSystem 9100 Management IP address example (single control enclosure configuration)

```
management IP add. 10.11.12.120
node 1 service IP add. 10.11.12.121
node 2 service IP add. 10.11.12.122
```

Requirement: Each IBM FlashSystem 9100 node canister in a clustered system must have at least one Ethernet connection.

Support for iSCSI on the IBM FlashSystem 9100 is also available from the onboard 10 GbE ports 3 & 4, and requires extra IPv4 or extra IPv6 addresses for each of those 10 GbE ports used on each of the IBM FlashSystem 9100 node canisters. These IP addresses are independent of the IBM FlashSystem 9100 cluster management IP addresses on the 10 GbE port 1 and port 2 of the node canisters within the control enclosures.

If further iSCSI support is required, this must be via ordering and installing additional PCIe adapters with Feature Code AHB6: 25 GbE (RoCE) Adapter Cards (Pair), or Feature Code AHB7: 25 GbE (iWARP) Adapter Cards (Pair). For more details about these feature codes, see the IBM FlashSystem 9100 announcement materials on the Family 9848 IBM website.

When accessing the IBM FlashSystem 9100 through the GUI or Secure Shell (SSH), choose one of the available management or service IP addresses to connect to. In this case, no automatic failover capability is available. If one network is down, use an IP address on the alternative network.

Note: The Service Assistant tool described in this book is a web-based GUI that is used to service individual node canisters, primarily when a node has a fault and is in a service state. This GUI is usually used only with guidance from IBM remote support. On the IBM FlashSystem 9100 control enclosures, the service ports in the node canisters should be assigned IP addresses and connected to the network.

4.4.2 SAN zoning and SAN connections

IBM FlashSystem 9100 can connect to 8 Gbps or 16 Gbps Fibre Channel (FC) switches for SAN attachments. From a performance perspective, connecting the IBM FlashSystem 9100 to 16 Gbps switches is better. For the internal SAN attachments, 16 Gbps switches are both better-performing and more cost-effective.

Both 8 Gbps and 16 Gbps SAN connections require correct zoning or VSAN configurations on the SAN switch or directors to bring security and performance together. Implement a dual-host bus adapter (HBA) approach at the host to access the IBM FlashSystem 9100. Examples of the HBA connections are shown in Zoning examples in IBM Knowledge Center.

Note: The IBM FlashSystem 9100 V8.2 supports 16 Gbps direct host connections without a switch.

Port configuration

With the IBM FlashSystem 9100, there are up to twenty four 16 Gbps Fibre Channel (FC) ports per enclosure when feature code AHB3 is ordered. Some of these are used for internal communications when the IBM FlashSystem 9100 is running in a clustered solution with more than one control enclosure.

The iSCSI ports can also be used for clustering the IBM FlashSystem 9100 enclosures if required. See additional information in Chapter 5, “Scalability” on page 117.

The remaining ports are used for host connections and any externally virtualized storage, if installed. For more information and best practices on the zoning for inter-cluster, hosts, and external storage FC connections, see the rules summary in IBM Knowledge Center.

Consider the following important points:

- Configuring SAN communication between nodes in the same I/O group is optional. All internode communication between ports in the same I/O group must not cross ISLs.
- Each node in the system must have at least two ports with paths to all other nodes that are in different enclosures in the same system.
- A node cannot have more than 16 paths to another node in the same system.
- Fibre Channel connections between the system and the switch can vary based on fibre types and different SFPs (longwave and shortwave).

> **Note:** New IBM FlashSystem 9100 systems that are installed with version 8.2.0 or later have N_Port ID Virtualization (NPIV) enabled as the default status. If an existing system is updated to version 8.2.0, it retains the NPIV status of the existing system.

Customer-provided SAN switches and zoning

This topic applies to anyone using customer-provided SAN switches or directors.

External virtualized storage systems are attached along with the host on the front-end FC ports for access by the control enclosures of the IBM FlashSystem 9100. Carefully create zoning plans for each additional storage system so that these systems will be properly configured for use and best performance between storage systems and the IBM FlashSystem 9100. Configure all external storage systems with all IBM FlashSystem 9100 control enclosures; arrange them for a balanced spread across the system.

All IBM FlashSystem 9100 control enclosures in the system must be connected to the same SANs, so that they all can present volumes to the hosts. These volumes are created from storage pools that are composed of the virtualized control enclosure MDisks, and if licensed, the external storage systems MDisks that are managed by the IBM FlashSystem 9100.

For suggested fabric zoning, see some Zoning examples in IBM Knowledge Center.

4.4.3 IP replication and mirroring

This topic describes IP replication and mirroring, and the iSCSI IP addressing plan.

IBM FlashSystem 9100 supports host access through iSCSI (as an alternative to FC).

The following considerations apply:

- IBM FlashSystem 9100 can use the built-in Ethernet ports for iSCSI traffic.
- Two optional 2-port 25 Gbps Ethernet adapters are supported in each node canister after V8.2.0, for iSCSI communication with iSCSI-capable Ethernet ports in hosts via Ethernet switches:
  - However, using two 25 Gbps Ethernet adapters per node canister prevents adding this control enclosure to an existing system, or adding another control enclosure to a system made from this controller (sometimes known as *clustering*). This is true until a future software release adds support for clustering via the 25 Gbps Ethernet ports.
  - These 2-port 25 Gbps Ethernet adapters do not support FCoE.
  - There are two types of 25 Gbps Ethernet adapter Feature supported:
    - RDMA over Converged Ethernet (RoCE)
    - Internet Wide-area RDMA Protocol (iWARP)

    Either will work for standard iSCSI communications (*not* using Remote Direct Memory Access (RDMA)). A future software release might add (RDMA) links using new protocols that support RDMA, such as NVMe over Ethernet.
- IBM FlashSystem 9100 supports the Challenge Handshake Authentication Protocol (CHAP) authentication methods for iSCSI.
- iSCSI IP addresses can fail over to the partner node in the I/O Group if a node fails. This design reduces the need for multipathing support in the iSCSI host.
- iSCSI IP addresses can be configured for one or more nodes.
- iSCSI simple name server (iSNS) addresses can be configured in IBM FlashSystem 9100.
- Because the IQN contains the clustered system name and the node name, it is important not to change these names after iSCSI is deployed.
- Each node can be given an iSCSI alias, as an alternative to the IQN.
- The IQN of the host to a IBM FlashSystem 9100 host object is added in the same way that you add FC worldwide port names (WWPNs).
- Host objects can have both WWPNs and IQNs.
- Standard iSCSI host connection procedures can be used to discover and configure IBM FlashSystem 9100 as an iSCSI target.

4.4.4 Native IP replication

IBM FlashSystem 9100 supports native IP replication, which enables the use of lower-cost Ethernet connections for remote mirroring. The capability is available as an option (Metro Mirror or Global Mirror) on all IBM FlashSystem 9100 systems. The function is transparent to servers and applications in the same way that traditional FC-based mirroring is.

All remote mirroring modes (Metro Mirror, Global Mirror, and Global Mirror with Changed Volumes) are supported.

Configuration of the system is straightforward: IBM FlashSystem 9100 systems can normally find each other in the network, and can be selected from the GUI. IP replication includes Bridgeworks SANSlide network optimization technology, and is available at no additional charge. Remote mirror is a chargeable option, but the price does not change with IP replication. Existing remote mirror users can access the new function at no additional charge.

Information: Full details of how to set up and configure IP replication are available in the *IBM SAN Volume Controller and Storwize Family Native IP Replication*, REDP-5103 Redbooks publication.

4.4.5 Advanced Copy Services

The IBM FlashSystem 9100 offers these Advanced Copy Services:

- FlashCopy
- Metro Mirror
- Global Mirror

IBM FlashSystem 9100 Advanced Copy Services must apply the following guidelines.

FlashCopy guidelines

Follow these guidelines for FlashCopy:

- Identify each application that must have a FlashCopy function implemented for its volume.
- FlashCopy is a relationship between volumes. Those volumes can belong to separate storage pools and separate storage subsystems.
- You can use FlashCopy for backup purposes by interacting with IBM Spectrum Control, or for cloning a particular environment.
- Define which FlashCopy best fits your requirements: No copy, Full copy, Thin-Provisioned, or Incremental.
- Define which FlashCopy rate best fits your requirement in terms of the performance and the amount of time to complete the FlashCopy.

Table 4-10 shows the relationship of the background copy rate value to the attempted number of grains to be split per second.

Table 4-10 Grain splits per second

User percentage	Data copied per second	256 KB grain per second	64 KB grain per second
1% - 10%	128 KB	0.5	2
11% - 20%	256 KB	1	4
21% - 30%	512 KB	2	8
31% - 40%	1 MB	4	16
41% - 50%	2 MB	8	32
50% - 60%	4 MB	16	64
61% - 70%	8 MB	32	128
71% - 80%	16 MB	64	256
81% - 90%	32 MB	128	512
91% - 100%	64 MB	256	1024

- Define the grain size that you want to use. A grain is the unit of data that is represented by a single bit in the FlashCopy bitmap table. Larger grain sizes can cause a longer FlashCopy elapsed time, and a higher space usage in the FlashCopy target volume. Smaller grain sizes can have the opposite effect. Remember that the data structure and the source data location can modify those effects.

In an actual environment, check the results of your FlashCopy procedure in terms of the data that is copied at every run and in terms of elapsed time, comparing them to the new IBM FlashSystem 9100 FlashCopy results. Eventually, adapt the grain per second and the copy rate parameter to fit your environment's requirements.

Metro Mirror and Global Mirror guidelines

IBM FlashSystem 9100 supports inter-cluster Metro Mirror and Global Mirror. Inter-cluster operation needs at least two clustered systems that are separated by several moderately high-bandwidth links.

Figure 4-11 shows a schematic of Metro Mirror connections.

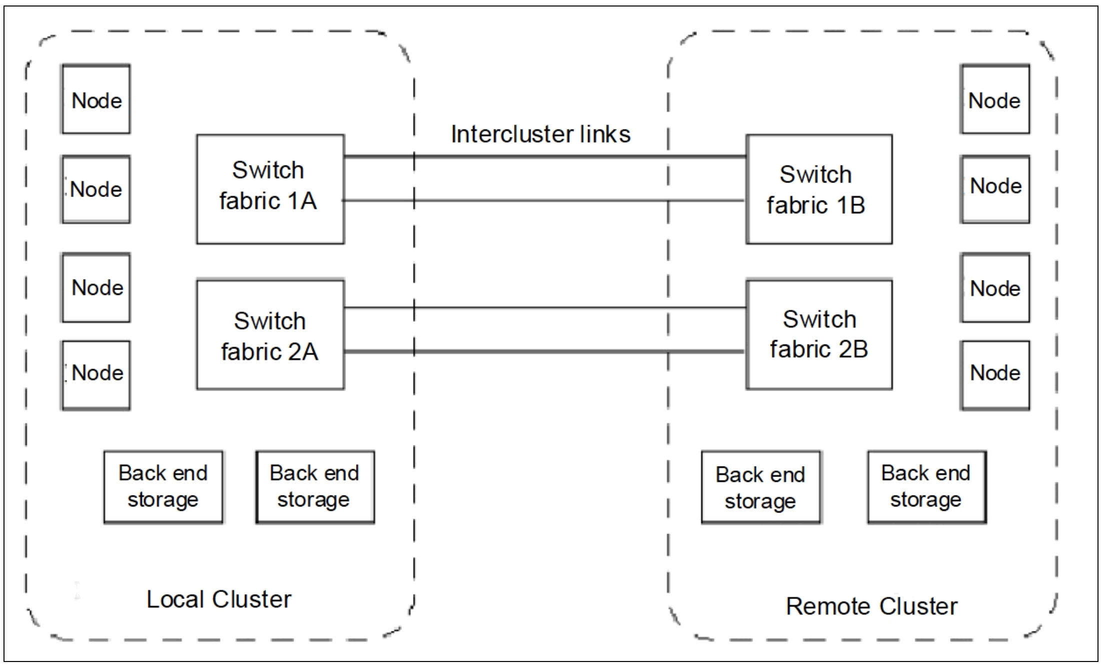


Figure 4-11 Metro Mirror connections

Figure 4-11 contains two redundant fabrics. Part of each fabric exists at the localclustered system and at the remote clustered system. No direct connection exists between the two fabrics.

Technologies for extending the distance between two IBM FlashSystem 9100 clustered systems can be broadly divided into two categories: FC extenders and SAN multiprotocolrouters.

Due to the more complex interactions involved, IBM explicitly tests products of this class for interoperability with the IBM FlashSystem 9100. You can obtain the current list of supported SAN routers in the supported hardware list on the IBM FlashSystem 9100 support web site .

IBM has tested several FC extenders and SAN router technologies with the IBM FlashSystem 9100. You must plan, install, and test FC extenders and SAN router technologies with the IBM FlashSystem 9100 so that the following requirements are met:

- The round-trip latency between sites must not exceed 80 milliseconds (ms), 40 ms one way.
- For Global Mirror, this limit enables a distance between the primary and secondary sites of up to 8000 kilometers (km), 4970.96 miles, using a planning assumption of 100 km (62.13 miles) per 1 ms of round-trip link latency.
- The latency of long-distance links depends on the technology that is used to implement them. A point-to-point dark fiber-based link typically provides a round-trip latency of 1 ms per 100 km (62.13 miles) or better. Other technologies provide longer round-trip latencies, which affects the maximum supported distance.
- The configuration must be tested with the expected peak workloads.
- When Metro Mirror or Global Mirror is used, a certain amount of bandwidth is required for IBM FlashSystem 9100 inter-cluster heartbeat traffic. The amount of traffic depends on how many nodes are in each of the two clustered systems.
- The bandwidth between sites must, at the least, be sized to meet the peak workload requirements, in addition to maintaining the maximum latency that has been specified previously. You must evaluate the peak workload requirement by considering the average write workload over a period of one minute or less, plus the required synchronization copy bandwidth.
- Determine the true bandwidth that is required for the link by considering the peak write bandwidth to volumes participating in Metro Mirror or Global Mirror relationships, and adding it to the peak synchronization copy bandwidth.
- If the link between the sites is configured with redundancy so that it can tolerate single failures, you must size the link so that the bandwidth and latency statements allow the link to continue to function.
- The configuration is tested to simulate the failure of the primary site (to test the recovery capabilities and procedures), including eventual failback to the primary site from the secondary.
- The configuration must be tested to confirm that any failover mechanisms in the inter-cluster links interoperate satisfactorily with the IBM FlashSystem 9100.
- The FC extender must be treated as a normal link.
- The bandwidth and latency measurements must be made by, or on behalf of, the client. They are *not* part of the standard installation of the IBM FlashSystem 9100 by IBM. Make these measurements during installation, and record the measurements. Testing must be repeated after any significant changes to the equipment that provides the inter-cluster link.

Global Mirror guidelines

For Global Mirror, the following guidelines apply:

- When using IBM FlashSystem 9100 Global Mirror, all components in the SAN must be capable of sustaining the workload that is generated by application hosts and the Global Mirror background copy workload. Otherwise, Global Mirror can automatically stop your relationships to protect your application hosts from increased response times. Therefore, it is important to configure each component correctly.
- Use a SAN performance monitoring tool, such as IBM Spectrum Control Center, which enables you to continuously monitor the SAN components for error conditions and performance problems. This tool helps you detect potential issues before they affect your disaster recovery solution.

- The long-distance link between the two clustered systems must be provisioned to provide for the peak application write workload to the Global Mirror source volumes, plus the client-defined level of background copy.
- The peak application write workload ideally must be determined by analyzing the IBM FlashSystem 9100 performance statistics.
- Statistics must be gathered over a typical application I/O workload cycle, which might be days, weeks, or months, depending on the environment on which the IBM FlashSystem 9100 is used. These statistics must be used to find the peak write workload that the link must be able to support.
- Characteristics of the link can change with use. For example, latency can increase as the link is used to carry an increased bandwidth. The user must be aware of the link's behavior in such situations, and ensure that the link remains within the specified limits. If the characteristics are not known, testing must be performed to gain confidence of the link's suitability.
- Users of Global Mirror must consider how to optimize the performance of the long-distance link, which depends on the technology that is used to implement the link.
- For example, when transmitting FC traffic over an IP link, it can be desirable to enable jumbo frames to improve efficiency.
- Using Global Mirror and Metro Mirror between the same two clustered systems is supported.
- Using Global Mirror and Metro Mirror between the IBM FlashSystem 9100 clustered system and IBM Storwize systems with a minimum code level of 7.2 is supported. For more details on the code level matrix for support, see the IBM Spectrum Virtualize Family of Products Inter-System Metro Mirror and Global Mirror Compatibility Cross Reference.
- It is supported for cache-disabled volumes to participate in a Global Mirror relationship; however, it not a preferred practice to do so.
- The **gmlinktolerance** parameter of the remote copy partnership must be set to an appropriate value. The default value is 300 seconds (five minutes), which is appropriate for most clients.
- During SAN maintenance, the user must choose to reduce the application I/O workload for the duration of the maintenance (so that the degraded SAN components are capable of the new workload):
  - Disable the **gmlinktolerance** feature.
  - Increase the **gmlinktolerance** value (meaning that application hosts might see extended response times from Global Mirror volumes).
  - Stop the Global Mirror relationships.
- If the **gmlinktolerance** value is increased for maintenance lasting *x* minutes, it must only be reset to the normal value *x* minutes after the end of the maintenance activity.
- If **gmlinktolerance** is disabled for the duration of the maintenance, it must be re-enabled after the maintenance is complete.
- Global Mirror volumes must have their preferred nodes evenly distributed between the nodes of the clustered systems. Each volume within an I/O Group has a preferred node property that can be used to balance the I/O load between nodes in that group.

Figure 4-12 shows the correct relationship between volumes in a Metro Mirror or Global Mirror solution.

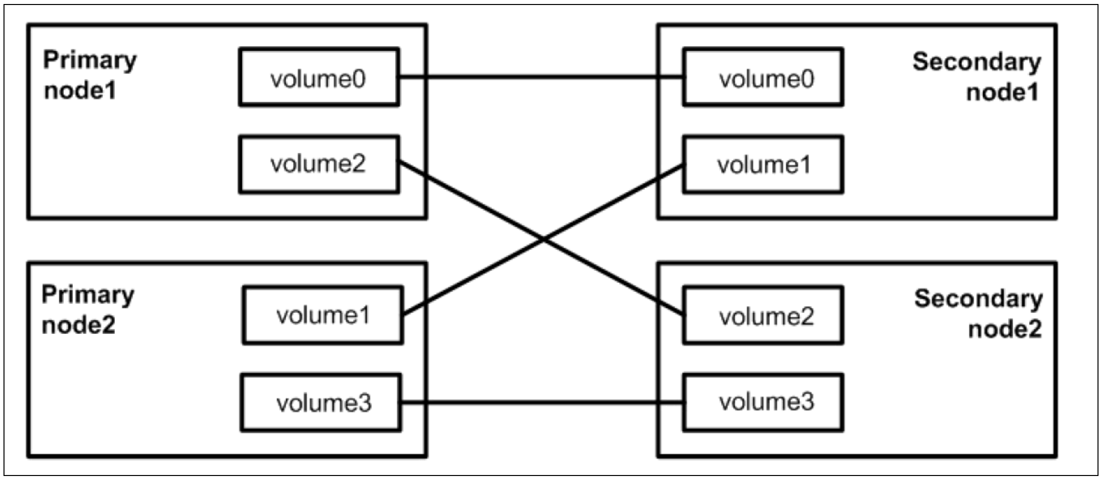


Figure 4-12 Correct volume relationship

- The capabilities of the storage controllers at the secondary clustered system must be provisioned to provide for the peak application workload to the Global Mirror volumes, plus the client-defined level of background copy, plus any other I/O being performed at the secondary site. The performance of applications at the primary clustered system can be limited by the performance of the back-end storage controllers at the secondary clustered system to maximize the amount of I/O that applications can perform to Global Mirror volumes.
- It is necessary to perform a complete review before using Serial Advanced Technology Attachment (SATA) for Metro Mirror or Global Mirror secondary volumes. Using a slower disk subsystem for the secondary volumes for high-performance primary volumes can mean that the IBM FlashSystem 9100 cache might not be able to buffer all of the writes, and flushing cache writes to SATA might slow I/O at the production site.
- Storage controllers must be configured to support the Global Mirror workload that is required of them:
  - Dedicate storage controllers to only Global Mirror volumes.
  - Configure the controller to ensure sufficient quality of service (QoS) for the disks being used by Global Mirror.
  - Ensure that physical disks are not shared between Global Mirror volumes and other I/O (for example, by not splitting an individual RAID array).
- MDisks in a Global Mirror storage pool must be similar in their characteristics, for example, RAID level, physical disk count, and disk speed. This requirement is true of all storage pools, but it is particularly important to maintain performance when using Global Mirror.
- When a consistent relationship is stopped, for example, by a persistent I/O error on the intercluster link, the relationship enters the `consistent_stopped` state. I/O at the primary site continues, but the updates are not mirrored to the secondary site. Restarting the relationship begins the process of synchronizing new data to the secondary disk.

  While this synchronization is in progress, the relationship is in the `inconsistent_copying` state. Therefore, the Global Mirror secondary volume is not in a usable state until the copy has completed and the relationship has returned to a Consistent state.

For this reason, it is highly advisable to create a FlashCopy of the secondary volume before restarting the relationship. When started, the FlashCopy provides a consistent copy of the data, even while the Global Mirror relationship is copying. If the Global Mirror relationship does not reach the Synchronized state (if, for example, the intercluster link experiences further persistent I/O errors), the FlashCopy target can be used at the secondary site for disaster recovery purposes.

- If you plan to use a Fibre Channel over IP (FCIP) intercluster link, it is extremely important to design and size the pipe correctly.

  Example 4-2 shows a best-guess bandwidth sizing formula, assuming that the write/change rate is consistent.

Example 4-2 Bandwidth sizing

```
Amount of write data within 24 hours times 4 to allow for peaks
Translate into MB/s to determine WAN link needed
Example:
250 GB a day
250 GB * 4 = 1 TB
24 hours * 3600 secs/hr. = 86400 secs
1,000,000,000,000/ 86400 = approximately 12 MB/s,
Which means OC3 or higher is needed (155 Mbps or higher)
```

- If compression is available on routers or wide area network (WAN) communication devices, smaller pipelines might be adequate. Note that workload is probably not evenly spread across 24 hours. If there are extended periods of high data change rates, consider suspending Global Mirror during that time frame.
- If the network bandwidth is too small to handle the traffic, the application write I/O response times might be elongated. For the IBM FlashSystem 9100, Global Mirror must support short-term *Peak Write* bandwidth requirements.
- You must also consider the initial sync and resync workload. The Global Mirror partnership's background copy rate must be set to a value that is appropriate to the link and secondary back-end storage. The more bandwidth that you give to the sync and resync operation, the less workload can be delivered by the IBM FlashSystem 9100 for the regular data traffic.
- Do not propose Global Mirror if the data change rate exceeds the communication bandwidth, or if the round-trip latency exceeds 80 - 120 ms. A greater than 80 ms round-trip latency requires Solution for Compliance in a Regulated Environment and request for price quotation (SCORE/RPQ) submission.

4.4.6 Call Home option

IBM FlashSystem 9100 supports setting up a Simple Mail Transfer Protocol (SMTP) mail server for alerting the IBM Support Center of system incidents that might require a service event. This is the *call home* option. You can enable this option during the setup.

Tip: Setting up call home involves providing a contact that is available 24 x 7 if a serious call home issue occurs. IBM support strives to report any issues to clients in a timely manner; having a valid contact is important to achieving service level agreements (SLAs).

Table 4-11 lists the necessary items required for setting up the IBM FlashSystem 9100 call home function.

Table 4-11 IBM FlashSystem 9100 Call Home function settings

Configuration item	Value
Primary Domain Name System (DNS) server	
SMTP gateway address	
SMTP gateway name	
SMTP “From” address	Example: `FS9100_name@customer_domain.com`
Optional: Customer email alert group name	Example: `group_name@customer_domain.com`
Network Time Protocol (NTP) manager	
Time zone	

Complete the following tables for your facility so that the SSR can set up Call Home and Remote Support Assistance (RSA) contact information.

Table 4-12 Call Home and Remote Support Assistance contact information

Contact Information	
Contact name	
Email address	
Phone (Primary)	
Phone (Alternate)	
Machine location	
System location information	
Company name	
Street address	
City	
State or province	
Postal code	
Country or region	
Proxy server IP addresses for remote support assistance	
IP address 1 Port 1	
IP address 2 Port 2	
IP address 3 Port 3	
IP address 4 Port 4	
IP address 5 Port 5	
IP address 6 Port 6	

See Chapter 6, “Installation and configuration” on page 167 for additional information in setting up the IBM FlashSystem 9100 control enclosure call home function.

4.4.7 Remote Support Assistance (RSA)

The IBM FlashSystem 9100 control enclosure supports the new Remote Support Assistance (RSA) feature.

By using RSA, the customer is able to initiate a secure connection from the FlashSystem 9100 to IBM, when problems arise. An IBM remote support specialist can then connect to the system to collect system logs, analyze a problem, if possible run repair actions remotely, or assist the client or an IBM SSR who is on site.

The RSA feature can also be used for remote code upgrades, where the remote support specialist will upgrade the code on the machine, without the need to send an SSR on site.

> **Important:** IBM encourages all customers to use the high-speed remote support solution that is enabled by RSA. Problem analysis and repair actions without a remote connection can get more complicated and time-consuming.

RSA uses a high-speed internet connection, but it gives the customer the ability to initiate an outbound Secure Shell (SSH) call to a secure IBM server. Firewall rules might need to be configured at the customer’s firewall to allow the FlashSystem V9000 Cluster and Service IPs to establish a connection to the IBM Remote Support Center via SSH.

> **Note:** The type of access that is required for a remote support connection is outbound port TCP/22 (SSH) from the IBM FlashSystem 9100 Cluster and Service IPs. See the note box on page 94 for a list of the IBM IP Addresses used for RSA.

RSA consists of IBM FlashSystem 9100 internal functions with a set of globally deployed supporting servers. Together, they provide secure remote access to the FlashSystem 9100 when necessary and when authorized by the customer’s personnel.

Figure 4-13 shows the overview of the RSA set-up, which has three major components.

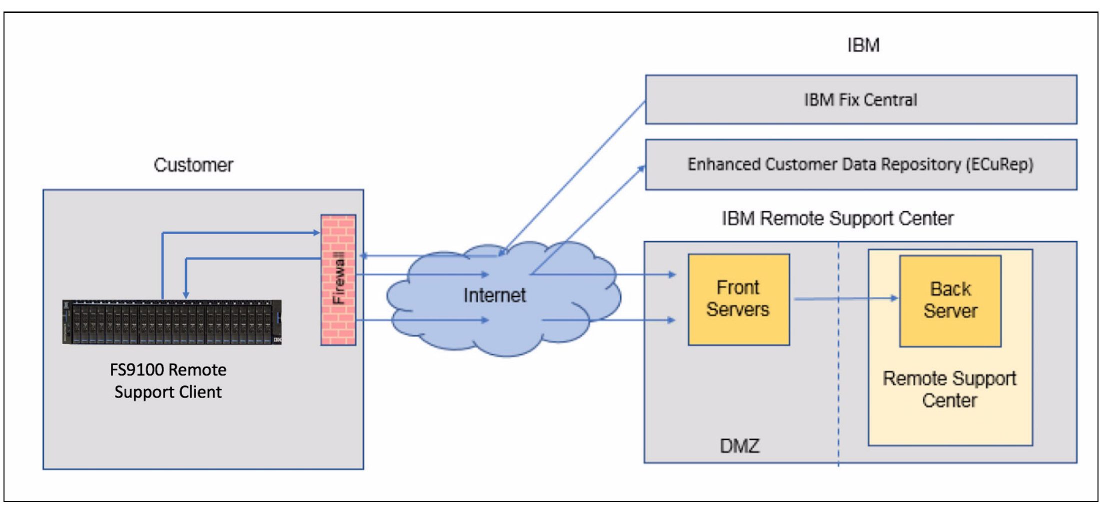


Figure 4-13 IBM FlashSystem 9100 Remote Support Set Up

Remote Support Client (machine internal)

The Remote Support Client is a software component inside FlashSystem 9100 that handles remote support connectivity. It resides on both canister nodes of the IBM FlashSystem 9100 control enclosure. The software component relies only on a single outgoing Transmission Control Protocol (TCP) connection, and it cannot receive inbound connections of any kind.

The Remote Support Client is controlled either by using the CLI or the GUI. The customer can therefore control the connection progress by using the CLI to open or close it, They can also add a password that IBM will need to ask for before logging in via the RSA link.

Remote Support Center Front Server (Internet)

Front Servers are on an IBM Demilitarized Zone (DMZ) of the internet and receive connections from the Remote Support Client and the IBM Remote Support Center Back Server. Front Servers are security-hardened machines that provide a minimal set of services, such as maintaining connectivity to connected Clients and to the Back Server.

They are strictly inbound, and never initiate anything on their own accord. No sensitive information is ever stored on the Front Server, and all data that passes through the Front Server from the client to the Back Server is encrypted so that the Front Server cannot access this data.

> **Note:** When activating Remote Support Assistant, the following four Front Servers are used via port TCP/22 (SSH):
>
> - 204.146.30.139
> - 129.33.206.139

Remote Support Center Back Server (IBM Intranet)

The Back Server manages most of the logic of the Remote Support Assistance system. It is located within the IBM Intranet. The Back Server maintains connection to all FrontServers and is access-controlled. Only IBM employees who are authorized to perform remote support of the FlashSystem 9100 are allowed to use it. The Back Server is in charge of authenticating a support person.

It provides the support person with a user interface (UI) through which to choose a system to support based on the support person's permissions. It also provides the list of systems that are currently connected to the Front Servers, and it manages the remote support session as it progresses (logging it, allowing additional support persons to join the session, and so on).

In addition, the IBM FlashSystem 9100 remote support solution can take advantage of the following two IBM internet support environments.

IBM Enhanced Customer Data Repository (ECuRep)

Further, if a remote connection exists, the IBM remote support specialists can offload the required support logs by themselves. For additional information about ECuRep, see IBM Support.

IBM Fix Central

Fix Central provides fixes and updates for IBM system's software, hardware, and operating system. The IBM FlashSystem 9100 control enclosure provides the possibility to allow an IBM remote support specialist to perform software updates remotely.

During this process, the IBM FlashSystem 9100 control enclosure automatically downloads the required software packages from the IBM.

Note: To download software update packages, the following six IP addresses are used via outbound port TCP/22 (SSH) from the IBM FlashSystem 9100 control enclosure to Fix Central:

- 170.225.15.105
- 170.225.15.104
- 170.225.15.107
- 129.35.224.105
- 129.35.224.104
- 129.35.224.107

Firewall rules might need to be configured. Further it is required to configure a DNS server to allow the download function to work.

If the user wants to download the code manually from IBM Fix Central, see the Select Fixes page.

You need the machine type/origin/serial during this process to validate the entitlement for software downloads, so its best you have this available.

Remote Support Proxy

Optionally, an application called Remote Support Proxy can be used when one or more FlashSystem 9100 systems do not have direct access to the Internet (for example, because of firewall restrictions). The Remote Support Client within the FlashSystem will then connect through this optional proxy server to the Remote Support Center Front Servers. The Remote Support Proxy runs as a service on a Linux system that has Internet connectivity to the Remote Support Center, and local network connectivity to the FlashSystem 9100.

Figure 4-14 illustrates the connection through the Remote Support Proxy.

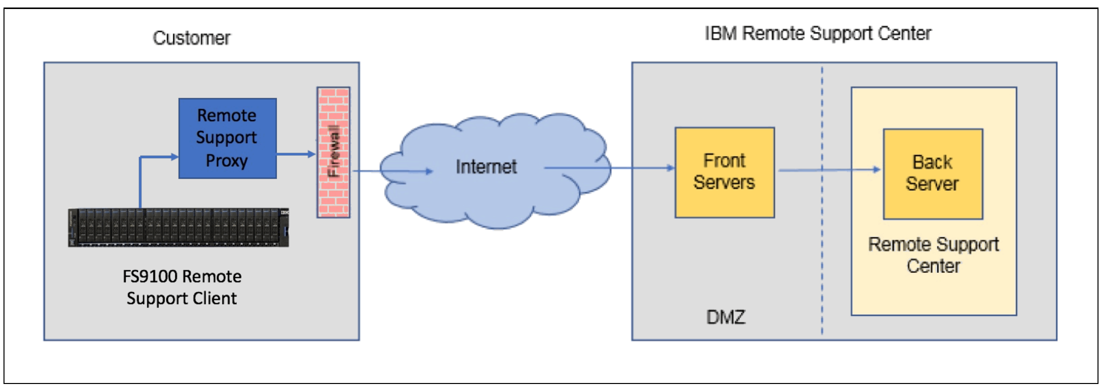


Figure 4-14 Connections through the Remote Support Proxy.

The communication between the Remote Support Proxy and the Remote Support Center is encrypted with an additional layer of Secure Sockets Layer (SSL).

Note: The host that is running the Remote Support Proxy must have TCP/443 (SSL) outbound access to Remote Support Front Servers.

Remote Support Proxy application

The Support Center Proxy is a network proxy that connects one or more IBM storage systems to IBM remote-support servers in the IBM Remote Support Center. The Remote

Support Proxy runs as a service on a Linux system that has Internet connectivity to the IBM Remote Support Center and local network connectivity to the storage system. The connection to the IBM Remote Support Center is initiated by the storage system through the IBM Storage Management GUI or the command-line interface (CLI). Refer to Remote Support Proxy for more details and installation instructions.

4.5 IBM Storage Insights

IBM Storage Insights is an integral part of the monitoring and ensuring continued availability of the IBM FlashSystem 9100.

Available at no charge, cloud-based IBM Storage Insights provides a single dashboard that gives you a clear view of all of your IBM block storage. You'll be able to make better decisions by seeing trends in performance and capacity. Storage health information enables you to focus on areas needing attention. In addition, when IBM support is needed, Storage Insights simplifies uploading logs, speeds resolution with online configuration data, and provides an overview of open tickets all in one place.

The following features are some of those included:

- A unified view of IBM systems:
  - Provides a single pane to see all of your system’s characteristics
  - See all of your IBM storage inventory
  - Provides a live event feed so you know, up to the second, what is going on with your storage and enables you to take action fast
- IBM Storage Insight® collects telemetry data and call home data, and provides up-to-the-second system reporting of capacity and performance.
- Overall storage monitoring:
  - The overall health of the system
  - Monitor the configuration to see if it meets the best practices
  - System resource management: determine if the system is being overly taxed and provide proactive recommendations to fix it
- Storage Insights provides advanced customer service with an event filter that enables the following functions:
  - The ability for you and support to view support tickets, open and close them, and track trends.
  - Auto log collection capability to enable you to collect the logs and send them to IBM before support starts looking into the problem. This can save as much as 50% of the time to resolve the case.

In addition to the free Storage Insights, there is also the option of Storage Insights Pro, which is a subscription service that provides longer historical views of data, offers more reporting and optimization options, and supports IBM file and block storage together with EMC VNX and VMAX.

Figure 4-15 shows the comparison of Storage Insights and Storage Insights Pro.

Product Comparison

	Capability	IBM Storage Insights (Free)	IBM Storage Insights Pro (Subscription)
Monitoring	Health, Performance and Capacity	✓	✓
	Filter events to quickly isolate trouble spots	✓	✓
	Drill down performance workflows to enable deep troubleshooting		✓
	Application / server storage performance troubleshooting		✓
	Customizable multi-conditional alerting		✓
Support Services	Simplified ticketing / log workflows and ticket history	✓	✓
	Proactive notification of risks (select systems)	✓	✓
Device Analytics	Part failure prediction	✓	✓
	Configuration best practice	✓	✓
	Customized upgrade recommendation	✓	✓
TCO Analytics	Capacity planning		✓
	Performance planning		✓
	Application / server storage consumption		✓
	Capacity optimization with reclamation planning		✓
	Data optimization with tier planning		✓

Figure 4-15 Storage Insights and Storage Insights Pro comparison chart

4.5.1 Architecture, security, and data collection

Figure 4-16 shows the architecture of the Storage Insights application, the products supported, and the three main teams of people who can benefit from using the tool.

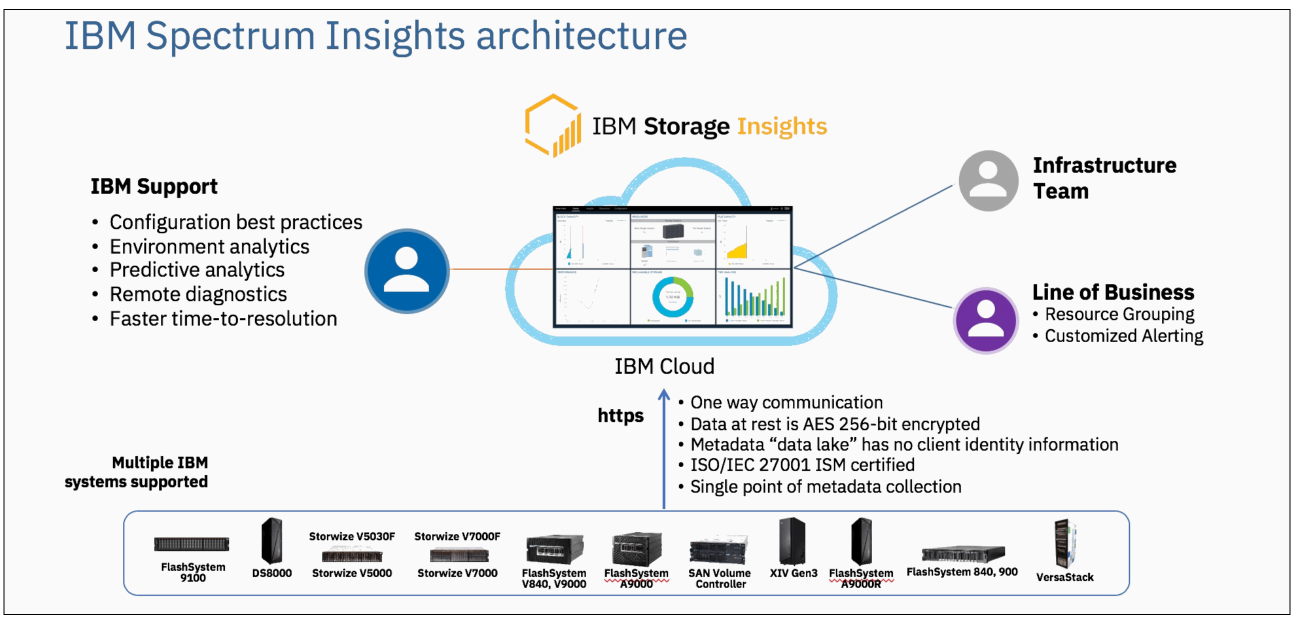


Figure 4-16 Storage Insights Architecture

Storage Insights provides a very lightweight data collector that is deployed on a customer supplied server. This can be either a Linux, Windows, or AIX server, or a guest in a virtual machine (for example, a VMware guest).

The data collector streams performance, capacity, asset, and configuration metadata to your IBM Cloud instance.

The metadata flows in one direction: from your data center to IBM Cloud over HTTPS. In the IBM Cloud, your metadata is protected by physical, organizational, access, and security controls. IBM Storage Insights is ISO/IEC 27001 Information Security Management certified.

Figure 4-17 shows the data flow from systems to the IBM Storage Insights cloud.

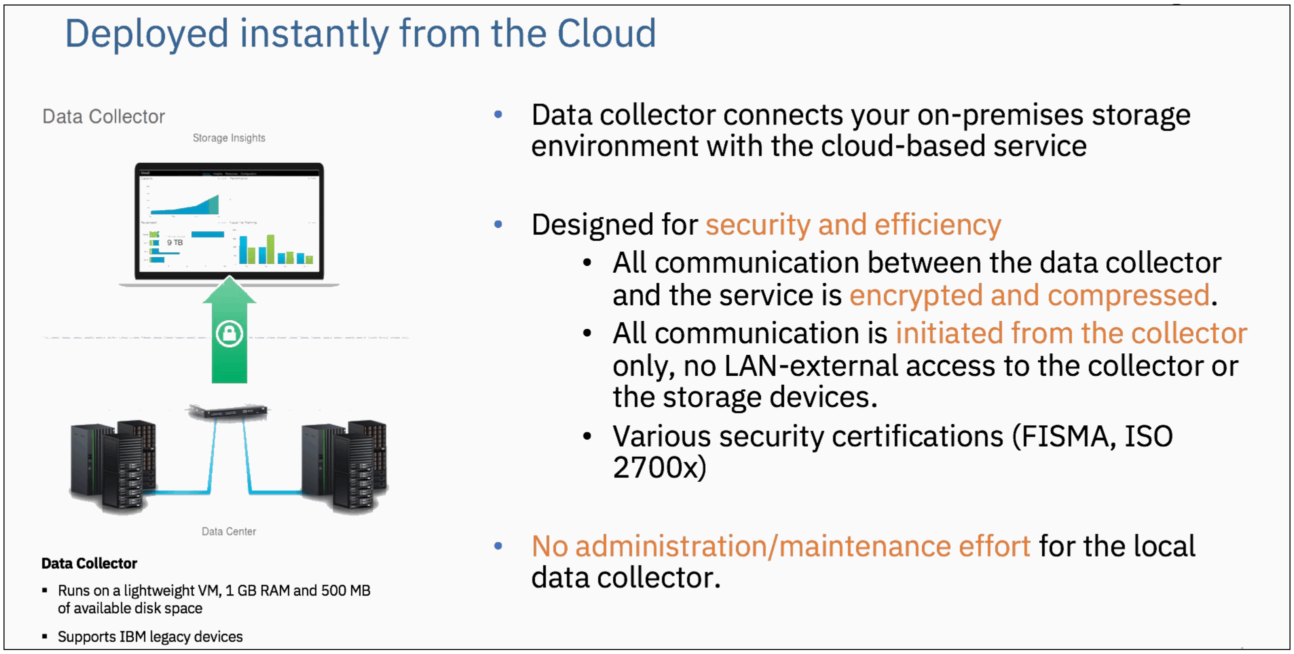


Figure 4-17 Data flow from the storage systems to the IBM Storage Insights cloud

What metadata is collected

Metadata about the configuration and operations of storage resources is collected:

- Name, model, firmware, and type of storage system
- Inventory and configuration metadata for the storage system's resources, such as volumes, pools, disks, and ports
- Capacity values, such as capacity, unassigned space, used space and the compression ratio
- Performance metrics, such as read and write data rates, I/O rates, and response times
- The actual application data that is stored on the storage systems can't be accessed by the data collector

Who can access the metadata

Access to the metadata that is collected is restricted to the following users:

- The customer who owns the dashboard
- The administrators who are authorized to access the dashboard, such as the customer's operations team
- The IBM Cloud team that is responsible for the day-to-day operation and maintenance of IBM Cloud instances
- IBM Support for investigating and closing service tickets

4.5.2 Customer dashboard

Figure 4-18 on page 99 shows a view of the Storage Insights main dashboard and the systems that it is monitoring.

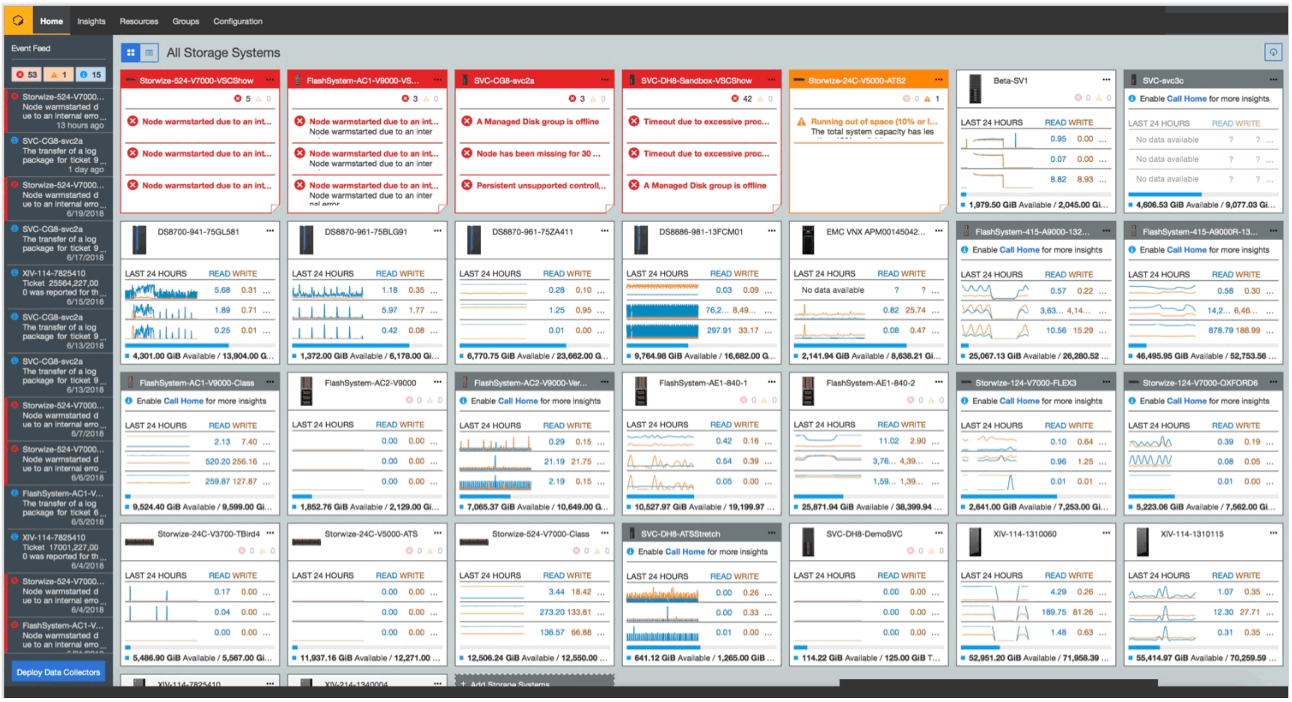


Figure 4-18 Storage Insights dashboard

Further views and images of dashboard displays and drill downs can be found in the supporting documentation listed in the following sections.

The following links can be used for further information about Storage Insights and also for the user to sign up and register for the free service:

- Fact Sheet: ibm.biz/insightsfacts
- Demonstration: ibm.biz/insightsdemo
- Security Guide: ibm.biz/insightssecurity
- Knowledge Center: ibm.biz/insightsknowledge
- Registration link**:** bm.biz/insightsreg

4.6 IBM FlashSystem 9100 system configuration

This section describes IBM FlashSystem 9100 system configuration considerations.

4.6.1 Configuration elements

To ensure proper performance and high availability in the IBM FlashSystem 9100 installations, consider the following guidelines when you design a SAN to support the IBM FlashSystem 9100:

- All nodes in a clustered system must be on the same LAN segment, because any node in the clustered system must be able to assume the clustered system management IP address. Make sure that the network configuration allows any of the nodes to use these IP addresses.

If you plan to use the second Ethernet port on each node, it is possible to have two LAN segments. However, port 1 of every node must be in one LAN segment, and port 2 of every node must be in the other LAN segment.

- To maintain application uptime in the event of an individual IBM FlashSystem 9100 node canister failing, the IBM FlashSystem 9100 control enclosure houses two node canisters forming one I/O Group. If a node canister fails or is removed from the configuration, the remaining node canister operates in a degraded mode, but the configuration is still valid for the I/O Group.

> **Important:** IBM FlashSystem 9100 V8.2 and later releases include the HyperSwap function, which enables each volume to be presented by two I/O groups. If you plan to use this function, you must consider the I/O Group assignments in the planning for the IBM FlashSystem 9100.

- The FC SAN connections between the IBM FlashSystem 9100 control enclosures are optical fiber. These connections can run at either 8 Gbps or 16 Gbps depending on your switch hardware, but 16 Gbps is advised to ensure best performance.
- Direct connections between the IBM FlashSystem 9100 control enclosures and hosts are supported with some exceptions.
- Direct connection of IBM FlashSystem 9100 control enclosures and external storage subsystems is not supported.
- Two IBM FlashSystem 9100 clustered systems cannot have access to the same external virtualized storage LUNs within a disk subsystem.

> **Attention:** Configuring zoning so that two IBM FlashSystem 9100 clustered systems have access to the same external LUNs (MDisks) can result in data corruption.

The storage pool and MDisk

The storage pool, which is an *mdiskgroup*, is at the center of the relationship between the MDisks and the volumes (VDisk). It acts as a container from which MDisks contribute chunks of physical capacity known as *extents*, and from which VDisks are created.

With the IBM FlashSystem 9100, we now have a new type of storage pool: the Data Reduction Pool (DRP). The DRP enables the users to define volumes that use the new data reduction and deduplication capabilities introduced in IBM Spectrum Virtualize software.

Therefore, the following pools represent a complete compliment of storage pool types:

- Regular non thin-provisioned pools
- Thin-provisioned pools
- DRP thin-provisioned, compressed pools

In addition, the DRP pools can also support deduplication. This is turned on at a volume level when creating the volumes within a pool. For more detailed information on DRP and deduplication, refer to Chapter 3, “Data reduction and tools” on page 23.

> **Important:** On FS9100, you want to use fully-allocated Data Reduction Pools with compression and no deduplication; or Data Reduction Pools with compression and deduplication.

After system setup, you must configure storage by creating pools and assigning storage to specific pools. Ensure that a pool or pools have been created before assigning storage. In the management GUI, select **Pools** → **Actions** → **Add Storage**. The Add Storage automatically configures existing drives into arrays. Use the **lsarrayrecommendation** command to display the system recommendations for configuring an array.

For greatest control and flexibility, you can use the **mkarray** command-line interface (CLI) command to configure a nondistributed array on your system. However, the suggested organization for the IBM FlashSystem 9100 is to configure a distributed array (DRAID6). You can use the **mkdistributedarray** command to do this.

> **Note:** DRAID6 arrays give better performance and rebuild times in the event of a FCM or NVMe drive failing, because the spare capacity allocated for the rebuild is shared across all of the drives in the system, and not reserved to one physical drive, as we have in the traditional RAID arrays.

Additionally, MDisks are also created for each external storage-attached LUN assigned to the IBM FlashSystem 9100 as a managed or as un-managed MDisk for migrating data. A managed MDisk is an MDisk that is assigned as a member of a storage pool:

- A storage pool is a collection of MDisks. An MDisk can only be contained within a single storage pool.
- IBM FlashSystem 9100 can support up to 1,024 storage pools.
- The number of volumes that can be allocated per system limit is 10,000.
- Volumes are associated with a single storage pool, except in cases where a volume is being migrated or mirrored between storage pools.

> **Information:** For the most up-to-date IBM FlashSystem 9100 configuration limits, go to the configuration for the IBM FlashSystem 9100 family.

Extent size

Each MDisk is divided into chunks of equal size called *extents*. Extents are a unit of mapping that provides the logical connection between MDisks and volume copies.

The extent size is a property of the storage pool and is set when the storage pool is created. All MDisks in the storage pool have the same extent size, and all volumes that are allocated from the storage pool have the same extent size. The extent size of a storage pool cannot be changed. If you want another extent size, the storage pool must be deleted and a new storage pool configured.

The IBM FlashSystem 9100 supports extent sizes of 16 MB, 32 MB, 64 MB, 128 MB, 256 MB, 512 MB, 1024 MB, 2048 MB, 4096 MB, and 8192 MB. By default, the MDisks created for the internal storage of flash memory in the IBM FlashSystem 9100 are created with an extent size of 1024 MB. To use a value that differs from the default requires the use of CLI commands to delete and re-create with different value settings. For information about the use of the CLI commands, search for CLI commands in IBM Knowledge Center.

Table 4-13 lists all of the extent sizes that are available in an IBM FlashSystem 9100.

Table 4-13 Extent size and maximum clustered system capacities

Extent size	Maximum clustered system capacity
16 MB	64 TB
32 MB	128 TB
64 MB	256 TB
128 MB	512 TB
256 MB	1 petabyte (PB)
512 MB	2 PB
1024 MB	4 PB
2048 MB	8 PB
4096 MB	16 PB
8192 MB	32 PB

This table only shows the maximum extent sizes versus the maximum cluster size when up to four IBM FlashSystem 9100s are clustered together.

For more information on the extents in regular, thin, and compressed pools, and the most up-to-date information on the IBM FlashSystem 9100 configuration limits, go to the configuration for the IBM FlashSystem 9100 family.

When planning storage pool layout, consider the following aspects:

- Pool extent size:
  - Generally, use 1 GB or higher:
    - If using DRP, then it is essential to use 4 GB.
    - If not using DRP, then 1 GB is acceptable.
    - Note that 4 GB is the default now.
  - For all of the values and rules for extents, see the previous link.
  - Pick the extent size and then use that size for all storage pools.
  - You cannot migrate volumes between storage pools with different extent sizes. However, you can use volume mirroring to create copies between storage pools with different extent sizes.
- Storage pool reliability, availability, and serviceability (RAS) considerations:
  - The number and size of storage pools affects system availability.
  - Using a larger number of smaller pools reduces the failure domain in case one of the pools goes offline. However, an increased number of storage pools introduces management overhead, impacts storage space use efficiency, and is subject to the configuration maximum limit.
  - An alternative approach is to create a few large storage pools. All MDisks that constitute each of the pools should have the same performance characteristics.
  - The storage pool goes offline if an MDisk is unavailable, even if the MDisk has no data on it. Do not put MDisks into a storage pool until they are needed.
  - Put image mode volumes in a dedicated storage pool or pools.

- Storage pool performance considerations:
  - It might make sense to create multiple storage pools if you are attempting to isolate workloads to separate disk drives.
  - Create storage pools out of MDisks with similar performance. This technique is the only way to ensure consistent performance characteristics of volumes created from the pool.
  - The previous rule does not apply when you consciously place MDisks from different storage tiers in the pool with the intent to use Easy Tier to dynamically manage workload placement on drives with appropriate performance characteristics.

4.6.2 Volume Considerations

An individual volume is a member of one storage pool and one I/O Group:

- The storage pool defines which MDisks provided by the disk subsystem make up the volume.
- The I/O Group (two node canisters make an I/O Group) defines which IBM FlashSystem 9100 nodes provide I/O access to the volume. In a single-enclosure FS9100, there is only one I/O group.

Important: No fixed relationship exists between I/O Groups and storage pools.

Perform volume allocation based on the following considerations:

- Optimize performance between the hosts and the IBM FlashSystem 9100 by attempting to distribute volumes evenly across available I/O Groups and nodes in the clustered system.
- Reach the level of performance, reliability, and capacity that you require by using the storage pool that corresponds to your needs (you can access any storage pool from any node). Choose the storage pool that fulfills the demands for your volumes regarding performance, reliability, and capacity.
- I/O Group considerations:
  - With the IBM FlashSystem 9100, each control enclosure that is connected into the cluster is an additional I/O Group for that clustered IBM FlashSystem 9100 system.
  - When you create a volume, it is associated with one node of an I/O Group. By default, every time that you create a new volume, it is associated with the next node using a round-robin algorithm. You can specify a *preferred access node*, which is the node through which you send I/O to the volume rather than using the round-robin algorithm. A volume is defined for an I/O Group.
  - Even if you have eight paths for each volume, all I/O traffic flows toward only one node (the preferred node). Therefore, only four paths are used by the IBM Subsystem Device Driver (SDD). The other four paths are used only in the case of a failure of the preferred node or when concurrent code upgrade is running.
- Thin-provisioned volume considerations:
  - When creating the thin-provisioned volume, be sure to understand the usage patterns by the applications or group users accessing this volume. You must consider items such as the actual size of the data, the rate of creation of new data, and modifying or deleting existing data.

– Two operating modes for thin-provisioned volumes are available:

  - *Autoexpand volumes* allocate storage from a storage pool on demand with minimal required user intervention. However, a misbehaving application can cause a volume to expand until it has consumed all of the storage in a storage pool.
  - *Non-autoexpand volumes* have a fixed amount of assigned storage. In this case, the user must monitor the volume and assign additional capacity when required. A misbehaving application can only cause the volume that it uses to fill up.

– Depending on the initial size for the real capacity, the grain size and a warning level can be set. If a volume goes offline, either through a lack of available physical storage for autoexpand, or because a volume that is marked as non-expand had not been expanded in time, a danger exists of data being left in the cache until storage is made available. This situation is not a data integrity or data loss issue, but you must not rely on the IBM FlashSystem 9100 cache as a backup storage mechanism.

> **Important:** Consider the following preferred practices:
>
> - Keep a warning level on the used capacity so that it provides adequate time to respond and provision more physical capacity.
> - Warnings must not be ignored by an administrator.
> - Use the autoexpand feature of the thin-provisioned volumes.

– When you create a thin-provisioned volume, you can choose the grain size for allocating space in 32 kilobyte (KB), 64 KB, 128 KB, or 256 KB chunks. The grain size that you select affects the maximum virtual capacity for the thin-provisioned volume. The default grain size is 256 KB, and is the preferred option. If you select 32 KB for the grain size, the volume size cannot exceed 260,000 GB. The grain size cannot be changed after the thin-provisioned volume is created.

– Generally, smaller grain sizes save space but require more metadata access, which could adversely affect performance. If you *will not be* using the thin-provisioned volume as a FlashCopy source or target volume, use 256 KB to maximize performance. If you *will be* using the thin-provisioned volume as a FlashCopy source or target volume, specify the same grain size for the volume and for the FlashCopy function.

– Thin-provisioned volumes require more I/Os because of directory accesses. For truly random workloads with 70% read and 30% write, a thin-provisioned volume requires approximately one directory I/O for every user I/O.

– The directory is two-way write-back cached (just like the IBM FlashSystem V9000 fast write cache), so certain applications perform better.

– Thin-provisioned volumes require more processor processing, so the performance per I/O Group can also be reduced.

– A thin-provisioned volume feature called *zero detect* provides clients with the ability to reclaim unused allocated disk space (zeros) when converting a fully allocated volume to a thin-provisioned volume using volume mirroring.

- Volume mirroring guidelines:

  – With the IBM FlashSystem 9100 system in a high performance environment, this capability is only possible with a *scale up* or *scale out* solution. If you are considering volume mirroring for data redundancy, a second control enclosure with its own storage pool would be needed for the mirror to be on.

  – Create or identify two separate storage pools to allocate space for your mirrored volume.

- If performance is of concern, use a storage pool with MDisks that share the same characteristics. Otherwise, the mirrored pair can be on external virtualized storage with lesser-performing MDisks.

- Data Reduction Pool (DRP) volumes
  - When configuring DRP-based volumes, there are special considerations required and procedures to be followed. See Chapter 3, "Data reduction and tools" on page 23.

4.6.3 Easy Tier

IBM Easy Tier is a function that automatically and non-disruptively moves frequently accessed data from various types of MDisks to flash drive MDisks, thus placing such data in a faster tier of storage. Easy Tier supports four tiers of storage.

The IBM FlashSystem 9100 supports the following tiers:

- Tier 0 flash: Specifies a `tier0_flash` IBM Flash Core Modules or an external MDisk for the newly discovered or external volume.
- Tier 1 flash: Specifies a `tier1_flash` (or flash SSD drive) for the newly discovered or external volume.
- Enterprise tier: Enterprise tier exists when the pool contains enterprise-class MDisks, which are disk drives that are optimized for performance.
- Nearline tier: Nearline tier exists when the pool contains nearline-class MDisks, which are disk drives that are optimized for capacity.

> **Note:** In the IBM FlashSystem 9100 these Enterprise or Nearline drives would be in external arrays. All managed arrays on the IBM FlashSystem 9100 system contain either NVMe class drives in the IBM FlashSystem 9100 control enclosures, or SSD class drives in the SAS expansion enclosures.

All MDisks belong to one of the tiers, which includes MDisks that are not yet part of a pool.

If the IBM FlashSystem 9100 control enclosure is used in an Easy Tier pool and is enabled on the pool, the node canisters will send encrypted, incompressible data to the NVMe drives. IBM Spectrum Virtualize software detects if an MDisk is encrypted by the FlashSystem 9100. Therefore, if an IBM FlashSystem 9100 control enclosure will be part of an encrypted easy-tier pool, encryption must be enabled on the IBM FlashSystem 9100 *before* it is enabled in the Easy Tier pool.

IBM Spectrum Virtualize does not attempt to encrypt data in an array that is already encrypted. This enables the hardware compression of the IBM FlashSystem 9100 to be effective if using the FCM type NVMe drives. However, there are cases in which using IBM FlashSystem 9100 software compression is preferred, such as if there is highly compressible data, (for example 3:1 or higher). In these cases, both encryption and compression can be done by the IBM FlashSystem 9100 node canisters.

For more information about Easy Tier, see the IBM Redbooks publication *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933. In addition, see the Easy Tier function section in the FlashSystem 9100 IBM Knowledge Center.

Storage pools have an Easy Tier setting that controls how Easy Tier operates. The setting can be viewed through the management GUI but can only be changed by the CLI.

By default the storage pool setting for Easy Tier is set to `Auto` (`Active`). In this state, storage pools with all managed disks of a single tier have Easy Tier status of `Balanced`.

If a storage pool has managed disks of multiple tiers, the Easy Tier status is changed to `Active`. The **`chmdiskgrp -easytier off 1`** command sets the Easy Tier status for storage pool 1 to `Inactive`. The **`chmdiskgrp -easytier measure 2`** command sets the Easy Tier status for storage pool 2 to `Measured`.

Figure 4-19 shows four possible Easy Tier states.

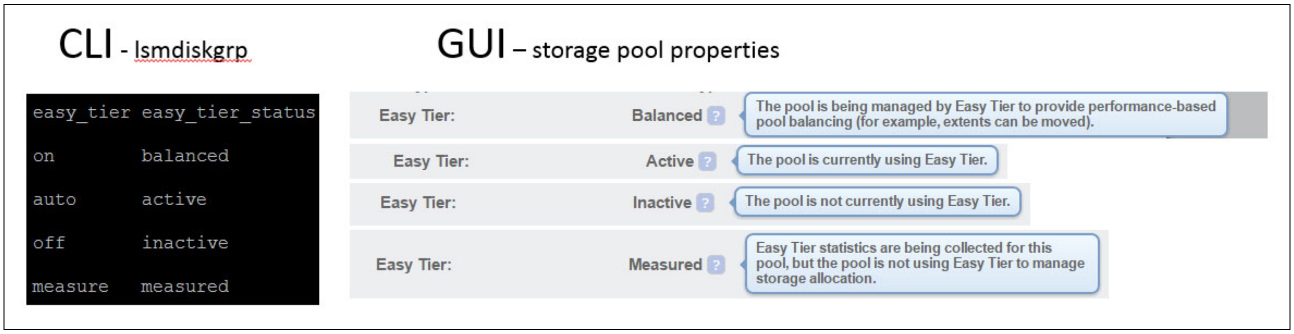


Figure 4-19 Easy Tier status for CLI and GUI

Easy Tier evaluation mode

Easy Tier evaluation mode is enabled for a storage pool with a single tier of storage when the status is changed to `Measured` using the command line. In this state, Easy Tier collects usage statistics for all the volumes in the pool. These statistics are collected over a 24-hour operational cycle, so you will have to wait several days to have multiple files to analyze. The statistics are copied from the control enclosures and viewed with the IBM Storage Tier Advisor Tool.

Instructions for downloading and using the tool are available in Extracting and viewing performance data with the IBM Storage Tier Advisor Tool.

This tool is intended to supplement and support, but *not* replace, detailed preinstallation sizing and planning analysis.

Easy Tier considerations

When a volume is created in a pool that has Easy Tier active, the volume extents are initially allocated only from the Enterprise tier. If that tier is not present or all the extents have been used, the volume is assigned extents from other tiers.

To ensure optimal performance, all MDisks in a storage pool tier must have the same technology and performance characteristics.

Easy Tier functions best for workloads that have hot spots or data. Synthetic random workloads across an entire tier are not a good fit for this function. Also, you should not allocate all the space in the storage pool to volumes. You should leave some capacity free on the fastest tier for Easy Tier to use for migration.

For more information about Easy Tier considerations and recommendations, see Easy Tier automatic data placement under the technical overview.

4.6.4 SAN boot support

The IBM FlashSystem 9100 supports SAN boot or startup for IBM AIX, Microsoft Windows Server, and other operating systems. SAN boot support can change, so check the IBM SSIC web page regularly.

4.7 Licensing and features

The following topics cover base product licenses and feature licensing.

4.7.1 IBM FlashSystem 9100 products licenses

The following licenses are for the IBM FlashSystem 9100 base products:

- IBM FlashSystem 9110 Base Model AF7- PID 5639-FA2
- IBM FlashSystem 9150 Base Model AF8- PID 5639-FA3

The following functions and features are included in the base IBM FlashSystem 9100 products licenses:

- Enclosure Virtualization
- Thin Provisioning
- FlashCopy
- Encryption
- Easy Tier
- DRP Compression

4.7.2 SAS Expansion Enclosures

Each SAS expansion enclosure requires the following license:

- IBM FlashSystem 9100 Expansion Enclosure Base Model AFF- PID 5639-FA1

> **Note:** Each IBM FlashSystem 9100 Expansion Enclosure Base Model A9F requires a quantity of *four* licenses per enclosure. The IBM FlashSystem 9100 Expansion Enclosure Base Model AFF only requires a quantity of *one* license per enclosure.

4.7.3 Externally virtualized expansion enclosures or external arrays

Each externally virtualized expansion enclosure or storage array requires *one* of the following licenses:

- IBM Spectrum Virtualize for SAN Volume Controller: PID 5641-VC8

  or

- IBM Virtual Storage Center (VSC): PID 5648-AE1

> **Note:** IBM FlashSystem 9100 *internal* enclosures are licensed to the hardware (HW) serial number. IBM Spectrum Virtualize software and VSC packages are perpetual and not tied to any HW serial number.

In addition to one of these licenses, the capacity of each enclosure or array has an SCU value applied.

An SCU is measured by category of usable capacity being virtualized/managed:

- **Category 1**: 1 SCU = 1 TiB or **1 TiB = 1.0 SCU**
  - Flash and SSD
- **Category 2**: 1 SCU = 1.18 TiB or **1 TiB = 0.847 SCU**
  - Serial Attached SCSI (SAS), Fibre Channel, systems using Cat 3 drives with advanced architectures (for example XIV or Infinidat)
- **Category 3**: 1 SCU = 4 TiB or **1 TiB = 0.25 SCU**
  - NL-SAS and SATA

Note: Calculations are rounded up to the nearest whole number in each category.

The following topics cover other license feature codes that might be required.

4.7.4 Encryption

The IBM FlashSystem 9100 Encryption feature is offered with the IBM FlashSystem 9100 under the following features:

- Feature code ACE7: Encryption Enablement Pack:
  - Enables data encryption at rest on the IBM FlashSystem 9100 control enclosure assigned MDisks.
  - USB flash drives (feature ACEA) or IBM Security Key Lifecycle Manager (SKLM) are required for encryption key management.
  - Only a quantity of one of these features is needed per IBM FlashSystem 9100 cluster.

    This feature enables the encryption function. A single instance of this feature enables the function on the entire IBM FlashSystem 9100 system (FlashSystem 9100 control enclosure and all attached FlashSystem 9100 expansion enclosures) and on externally virtualized storage subsystems.
- Feature code ACEA: Encryption USB Flash Drives (Four Pack):
  - This feature provides four USB flash drives for storing the encryption master access key.
  - Unless SKLM is used for encryption keys management, a total of three USB flash drives are required per FlashSystem 9100 cluster when encryption is enabled in the cluster, regardless of the number of systems in the cluster. If encryption will be used in a cluster, this feature should be ordered on one FlashSystem 9100 system, resulting in a shipment of four USB flash drives.
  - You must have three USB keys when you enable encryption in order to store the master key. These should just be plugged into active nodes in your cluster. In order to boot the system you must have one working USB stick plugged into one working canister in the system. Therefore you need to have three copies of the encryption master key before you are allowed to use encryption.

There are two ways to enable the encryption feature on the IBM FlashSystem 9100:

- USB Keys on each of the control enclosures
- IBM Security Key Lifecycle Manager (SKLM)

You can use one or both ways to enable encryption. Using both USB and SKLM methods together gives the most flexible availability of the encryption enablement.

> **Note:** To invoke either method requires the purchase of the Feature code ACE7: Encryption Enablement Pack as a minimum.

USB Keys

This feature supplies four USB keys to store the encryption key when the feature is enabled and installed. If necessary, there is a rekey feature that can also be performed. When the UBS keys encryption feature is being installed, the IBM FlashSystem 9100 GUI is used for each control enclosure that will have the encryption feature installed. The USB keys must be installed in the USB ports in the rear of the node canisters.

Figure 4-20 (rear view) shows the location of USB ports on the IBM FlashSystem 9100 node canisters.

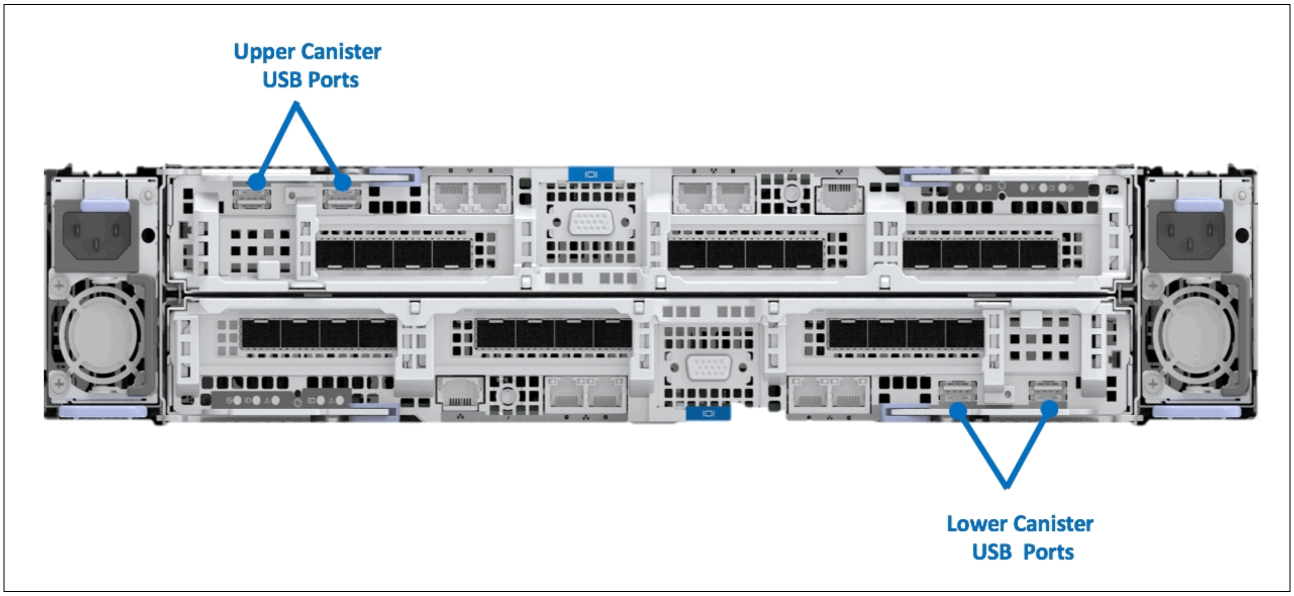


Figure 4-20 Location of USB ports

IBM Security Key Lifecycle Manager

IBM FlashSystem 9100 Software V7.8 added improved security with support for encryption key management software that complies with the Key Management Interoperability Protocol (KMIP) standards, such as IBM Security Key Lifecycle Manager (SKLM) to help centralize, simplify, and automate the encryption key management process.

Before IBM FlashSystem 9100 Software V7.8, you could enable encryption by using USB flash drives to copy the encryption key to the system.

> **Note:** If you are creating a new cluster, you have the option to use USB encryption, key server encryption, or both. The USB flash drive method and key server method can be used in parallel on the same system. Existing clients that are currently using USB encryption can move to key server encryption.

Encryption summary

Encryption can take place at the hardware or software level.

Hardware Encryption at the IBM FlashSystem 9100

Hardware encryption is the preferred method for IBM FlashSystem 9100 enclosures because this method works with the hardware compression that is built in to the Flash Core Modules of the IBM FlashSystem 9100 storage enclosure.

Software Encryption at the IBM FlashSystem 9100

Software encryption should be used with other storage that does not support its own hardware encryption. For more information about encryption technologies supported by other IBM storage devices, see *IBM DS8880 Data-at-rest Encryption*, REDP-4500.

4.7.5 Compression

There are two ways to compress data on the IBM FlashSystem 9100 depending on the type of storage installed in the control enclosure and also attached to the system:

- NVMe FCM inline hardware compression
- Data Reduction Pool (DRP) compression

The IBM FlashSystem 9100 software does not support Real-time Compression (RtC) type compressed volumes. If users want to use these legacy volumes on the IBM FlashSystem 9100, they have to migrate these to the new DRP model. They have to use volume mirroring to clone data to a new DRP. DRP pools no longer support legacy `migrate` commands.

> **Important:** On FS9100, use fully-allocated Data Reduction Pools with compression and no deduplication; or Data Reduction Pools with compression and deduplication.

Figure 4-21 shows the way that traditional volumes and those compressed under the RtC process need to be migrated to the new DRP pools model.

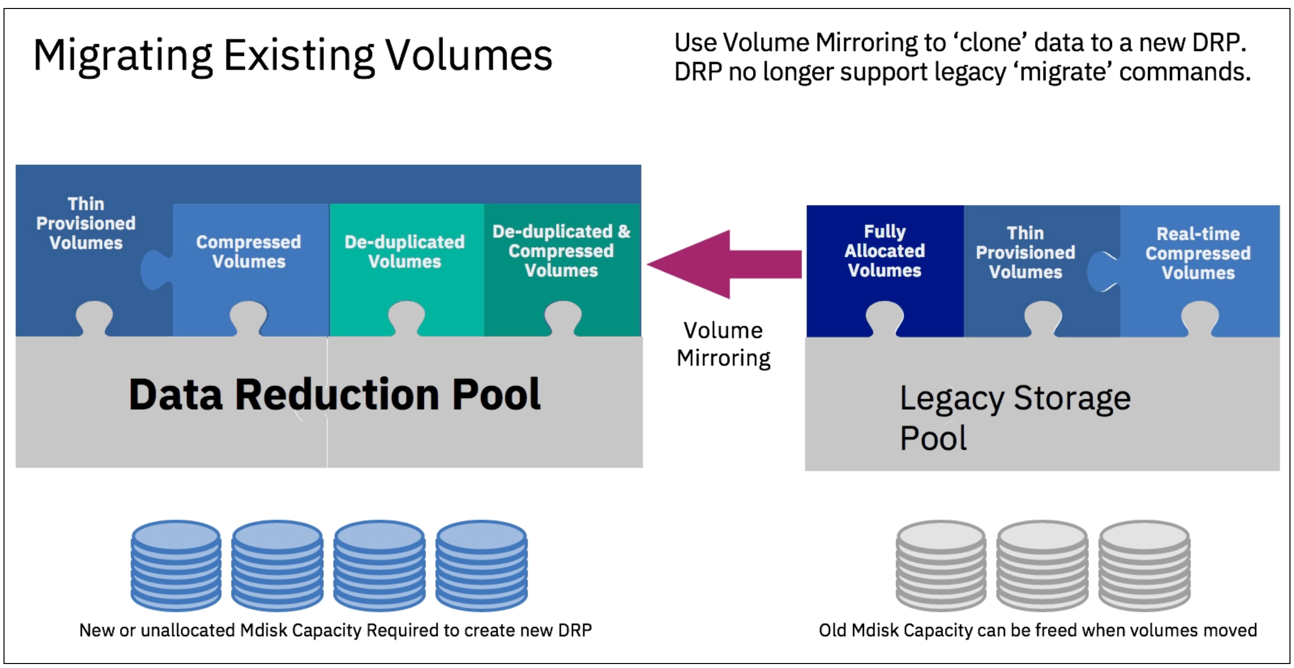


Figure 4-21 RtC to DRP Volume Migration

IBM FlashSystem 9100 enclosure using the IBM Flash Core Modules (FCM), have inline hardware compression as always on. The best usable to maximum effective capacity ratio is dependent on the FCM capacity.

Some workloads not demanding the lowest latency and having a good possible compression rate could be a candidate for using software-based compression or the DRP. See Chapter 3, “Data reduction and tools” on page 23 for more information.

The IBM FlashSystem 9100 enclosure using industry-standard NVMe drives does not have built-in hardware compression, so needs to rely on the use of DRP pools to provide a level of data reduction, if required.

The user can also opt for standard pools and fully allocated volumes, and then use the FCM in built-in hardware compression to give a level of data reduction, depending on the data pattern stored.

DRP software compression

The IBM FlashSystem 9100 DRP software compression uses additional hardware that is dedicated to the improvement of the compression functionality, and this hardware is built in on the node canister motherboard. There are no separate PCIe type compression cards as used on previous products. These accelerators work in conjunction with the DRP software within the control enclosure, for the I/O Group to support compressed volumes.

> **Important:** On FS9100, you want to use fully-allocated, Data Reduction Pools with compression and no deduplication; or Data Reduction Pools with compression and deduplication.

Inline hardware compression

The IBM FlashSystem 9100 FCM type drives have inline hardware compression as part of its architecture, if they are installed. The industry-standard NVMe drives rely on SW with HW assisted compression or the use of the DRP pools. This type of FCM compression is always on and cannot be switched off. For further details about the compression, its architecture, and its operation, see Chapter 2, “IBM FlashSystem 9100 architecture” on page 11.

Data reduction at two levels

It is possible to create solutions where data reduction technologies are applied at both the storage and the virtualization appliance levels.

It is important to understand which of these make most sense to ensure performance is not impacted and space is used in the best way possible.

Table 4-14 shows the best practices when using IBM FlashSystem 9100 and other external storage.

Table 4-14 IBM FlashSystem 9100 and external storage best practices

Front End	External Storage	Recommendations
IBM FlashSystem 9100: DRP above simple RAID	Storwize 5000 or any other fully allocated volumes	**Yes** ► Use DRP at the top level to plan for deduplication and snapshot optimizations. ► DRP at the top level provides the best application capacity reporting (volume written capacity). ► Always use compression in DRP to get the best performance. ► Bottlenecks in compression performance come from metadata resource use, not compression processing.
IBM FlashSystem 9100: fully allocated	IBM FlashSystem A9000	**Use with care** ► Need to track physical capacity use carefully to avoid out-of-space issues. ► SVC can report physical use but does not manage to avoid the out-of-space state. ► No visibility of each application's use at the SVC layer. ► If actual out-of-space happens, there is very limited ability to recover. Consider creating a sacrificial emergency space volume.
IBM FlashSystem 9100: fully allocated above multitier data, reducing back end	IBM FlashSystem A9000 and IBM Storwize 5000 with DRP	**Use with great care** ► Easy Tier is unaware of the physical capacity in the tiers of the hybrid pool. ► Easy Tier tends to fill the top tier with the "hottest" data. ► Changes in compressibility of data in the top tier can overcommit the storage, leading to out-of-space.
IBM FlashSystem 9100: DRP above data, reducing back end	IBM FlashSystem 900 AE3	**Yes** ► Assume 1:1 compression in back-end storage: do not overcommit. ► Small extra savings can be realised from compressing metadata.

Front End	External Storage	Recommendations
IBM FlashSystem 9100: DRP and fully allocated above data, reducing back end	IBM FlashSystem 900 AE3	**Use with great care** ► Makes it very difficult to measure physical capacity use of the fully allocated volumes. ► The temptation is to exploit capacity savings, which might overcommit the back end. ► DRP garbage collection acts as if Fully Allocated volumes are 100% used.
IBM FlashSystem 9100: DRP	IBM V7000 or other DRP	**No: avoid** ► Creates two levels of I/O amplification on metadata. ► There are two levels of capacity resource use. ► DRP at the bottom layer provides no benefit.

Further information about compressed volumes can be found in the IBM FlashSystem 9100 Knowledge Center.

4.8 IBM FlashSystem 9100 configuration backup procedure

Configuration backup is the process of extracting configuration settings from a clustered system and writing it to disk. The configuration restore process uses backup configuration data files for the system to restore a specific system configuration. Restoring the system configuration is an important part of a complete backup and disaster recovery solution.

Only the data that describes the system configuration is backed up. You must back up your application data by using the appropriate backup methods.

To enable routine maintenance, the configuration settings for each system are stored on each node. If power fails on a system, or if a node in a system is replaced, the system configuration settings are automatically restored when the repaired node is added to the system.

To restore the system configuration in a disaster (if all nodes in a system are lost simultaneously), plan to back up the system configuration settings to tertiary storage. You can use the configuration backup functions to back up the system configuration. The preferred practice is to implement an automatic configuration backup by applying the configuration backup command.

The virtualization map is stored on the quorum disks of external MDisks, and is accessible to every IBM FlashSystem 9100 control enclosure.

For complete disaster recovery, regularly back up the business data that is stored on volumes at the application server level or the host level.

Before making major changes to the IBM FlashSystem 9100 configuration, be sure to save the configuration of the system. By saving the current configuration, you create a backup of the licenses that are installed on the system. This can assist you in restoring the system configuration. You can save the configuration by using the **`svcconfig backup`** command.

The next two steps show how to create a backup of the IBM FlashSystem 9100 configuration file, and to copy the file to another system.

1. Log in to the cluster IP using an SSH client, and back up the IBM FlashSystem 9100 configuration. Example 4-3 shows the output of the **svcconfig backup** command.

   Example 4-3 Output of the svcconfig backup command

   ```
   superuser> svcconfig backup
   ..................................................................
   CMMVC6155I SVCCONFIG processing completed successfully
   ```

2. Copy the configuration backup file from the system. Using secure copy, copy the following file from the system and store it:

   `/tmp/svc.config.backup.xml`

   For example, use **pscp.exe**, which is part of the PuTTY commands family. Example 4-4 shows the output of the **pscp.exe** command.

   Example 4-4 Using pscp.exe

   ```
   pscp.exe superuser@<cluster_ip >:/tmp/svc.config.backup.xml .
   superuser@ycluster_ip> password:
   svc.config.backup.xml | 163 kB | 163.1 kB/s | ETA: 00:00:00 | 100%
   ```

This process also needs to be completed on any external storage in the IBM FlashSystem 9100 cluster. If you have the IBM FlashSystem 900 AE3 as external storage, you need to log in to each of the AE3 cluster IP addresses. Then, using an SSH client, run the **svcconfig backup** command on each of the FlashSystem AE3 attached storage enclosures. The same applies to any IBM Storwize system being used as external storage on the cluster.

Note: This process saves *only* the configuration of the IBM FlashSystem 9100 system. User data must be backed up by using normal system backup processes

4.9 Multi-cloud offerings and solutions

The IBM FlashSystem 9100 includes software that can help you start to develop a multi-cloud strategy if your storage environment includes cloud services, whether public, private, or hybrid cloud.

The IBM FlashSystem 9100 offers a series of multi-cloud software options. A set of base software options is provided with the system purchase, and you can investigate the integration of the FlashSystem 9100 with the following cloud-based software offerings:

- IBM Spectrum Protect Plus Multi-Cloud starter for FlashSystem 9100
- IBM Spectrum Copy Data Management Multi-Cloud starter for FlashSystem 9100
- IBM Spectrum Virtualize for Public Cloud Multi-Cloud starter for FlashSystem 9100

In addition, IBM offers a set of integrated software solutions that are associated with the FlashSystem 9100. These multi-cloud solutions are provided as optional software packages that are available with the FlashSystem 9100. Each of the following software solutions includes all of the software that is needed to construct the solution and an IBM-tested blueprint that describes how to construct the solution:

- IBM FlashSystem 9100 Multi-Cloud Solution for Data Reuse, Protection, and Efficiency

- IBM FlashSystem 9100 Multi-Cloud Solution for Business Continuity and Data
- IBM FlashSystem 9100 Multi-Cloud Solution for Private Cloud Flexibility and Data Protection

For more information and details about the software products included with the FS9100 purchase, refer to the hIBM FlashSystem 9100 Knowledge Center.

5

Scalability

This chapter describes the scaling capabilities of IBM FlashSystem 9100:

- Can be clustered to deliver greater performance, bandwidth, and scalability
- Can scale out for capacity and performance

A single IBM FlashSystem 9100 storage building block consists of one IBM FlashSystem 9100 control enclosure with NVMe FlashCore Modules or NVMe industry-standard drives. Additionally, the control enclosures can be configured with SAS-enclosures for capacity expansion.

The examples of scaling in this chapter show how to add control enclosures, add an expansion enclosure, and how to configure scaled systems. This chapter demonstrates scaling out with additional building blocks and adding additional storage expansion enclosure.

This chapter includes the following topics:

5.1 Overview

IBM FlashSystem 9100 has a scalable architecture that enables flash capacity to be added (scaled up) to support multiple applications. The virtualized system can also be expanded (scaled out) to support higher input/output operations per second (IOPS) and bandwidth, or the solution can be simultaneously scaled up and out to improve capacity, IOPS, and bandwidth while maintaining IBM MicroLatency®.

Model AF7 and Model AF8 FlashSystem 9100 systems scale up to 760 drives with the attachment of FlashSystem 9100 expansion enclosures. FlashSystem 9100 systems can be clustered to help deliver greater performance, bandwidth, and scalability. A FlashSystem 9100 clustered system can contain up to four FlashSystem 9100 systems and up to 3,040 drives. FlashSystem 9100 systems can be added into existing clustered systems that include IBM Storwize V7000 systems.

FlashSystem 9100 offers two 12 Gb SAS expansion enclosure models. The FlashSystem 9100 SFF Expansion Enclosure Model AFF supports up to twenty-four 2.5-inch flash drives. The FlashSystem 9100 LFF HD Expansion Enclosure Model A9F supports up to ninety-two flash drives in a 3.5-inch carrier. SFF and LFF HD expansion enclosures can be intermixed within a FlashSystem 9100 system.

As a result, your organization can gain a competitive advantage through MicroLatency response times and a more efficient storage environment. IBM FlashSystem 9100 has the following scalability features:

- IBM FlashSystem 9100 has the following flexible scalability configuration options:
  - Add more internal FlashCore Modules.
  - Add up to four control enclosures to form a cluster.
  - Add more SAS SSD expansion enclosure capacity.
  - Expand with virtualized external Storage systems.
- Configurable usable capacity for increased flexibility per storage enclosure
- NVMe internal slots for up to 24 hot-swappable FlashCore Modules (FCMs):
  - 4.8 TB, 9.6 TB, 19.2 TB modules.
  - In-line performance-neutral hardware compression reduces data as it’s written to the drive.
  - Distributed RAID5; *Distributed RAID6* (default, preferred).
- NVMe internal slots for up to 24 hot-swappable, industry-standard NVMe drives:
  - 800 GB, 1.92 TB, 3.84 TB, 7.68 TB, or 15.36 TB.
  - Encryption capable.
  - Distributed RAID5; *Distributed RAID6* (preferred).
  - **Note**: Array members should be uniform in capacity size to avoid bottlenecks and issues replacing drives.
- Attachment for up to 20 FlashSystem 9100 model AFF SAS expansion enclosures per control enclosure or 8 model A9F SAS enclosures using SAS SSDs
  - Tier 1 SSDs in many capacities.
  - SAS card encrypted.
  - Distributed RAID5; **Distributed RAID6** (preferred); Traditional RAID10,0,1

The following types of control and expansion enclosures are discussed in this chapter:

- IBM FlashSystem 9100 control enclosure:
  - Control Enclosures AF7 (FlashSystem 9110)
  - Control Enclosures AF8 (FlashSystem 9150)
  - Native IBM FlashSystem 9100 NVMe storage:
    - NVMe FlashCore Modules
    - NVMe Industry Standard drives
- IBM FlashSystem FS9100 expansion enclosure:
  - Expansion drawer model AFF (up to 24 drives)
  - Expansion drawer model A9F (up to 96 drives)
  - SAS drive-based SSD drives
  - SAS attached
  - Used for capacity expansion

5.2 Scaling features

A single FlashSystem 9100 control enclosure can support multiple attached expansion enclosures. Expansion enclosures can be dynamically added with virtually no downtime, helping to quickly and seamlessly respond to growing capacity demands. Intermixing expansion enclosure types in a system is supported.

A single IBM FlashSystem 9100 storage system consists of one control enclosure with internal storage, representing a 2U building block.

For balanced increase of performance and scale, up to four IBM FlashSystem 9100 control enclosures can be clustered into a single storage system, multiplying performance and capacity with each addition.

Clustering FlashSystem 9100 will scale the performance with additional NVMe storage. With four-way system clustering, the size of the system can be increased to a maximum of 3,040 drives.

Deployments requiring higher scalability and density can take advantage of FlashSystem 9100 Expansion Enclosures using 12 Gb SAS flash drives.

For more capacity within the performance envelope of a single control enclosure, SAS enclosures can be added.

To summarize:

- Add I/O groups for performance.
- Add additional SAS expansion enclosures for capacity.

Further scalability can be achieved with the virtualization of external storage systems. When IBM FlashSystem 9100 virtualizes an external disk system, capacity in the external system inherits the functional richness and ease of use of FlashSystem 9100.

Note: FlashSystem 9100 systems can be added into existing Storwize V7000 clustered systems.

To improve performance, consider the cache options available:

- 128 GB base configuration.
- Upgrade options: 256 GB, 358 GB, 768 GB, 1.1 TB, or 1.5 TB memory cache per control enclosure can be added for increased performance.

Compression is available as a hardware and software feature in the IBM FlashSystem 9100 control enclosures. Compression enables users to deploy compression where it is applicable.

5.2.1 Scaling Concepts

IBM FlashSystem 9100 provides these scaling concepts:

- Scale up. Add additional NVMe drives to increase internal capacity:
  - Add NVMe FlashCore modules.
  - Add NVMe SSD Industry Standard drives.
- Scale up and out. Add control enclosures for tremendous scaling and performance. Add NVMe internal capacity:
  - Add up to four IBM FlashSystem 9100 control enclosures for extra performance.
  - Add IBM FlashSystem 9100 control enclosures for capacity.
- Scale up. Add capacity with more SAS expansion enclosures:
  - Add a 12 Gb SAS adapter to control enclosure for scale up of capacity without scaling out to another AF7 or AF8 controller.
  - Add up to 20 IBM FlashSystem 9100 model AFF SAS expansion enclosures.
  - Add up to 8 IBM FlashSystem 9100 model A9F SAS expansion enclosures.
- Scale up. Add storage controller virtualization, external storage system capacity:
  - FlashSystem 9100 uses IBM Spectrum Virtualize with support up to 32 PB. This is the maximum total of all NVMe, SAS, and virtualized storage.
  - Enables migration and reuse of storage assets.

5.2.2 Building Blocks

Figure 5-1 shows the building blocks: NVMe control enclosure with 24 and 96 SAS SSD expansion enclosures.

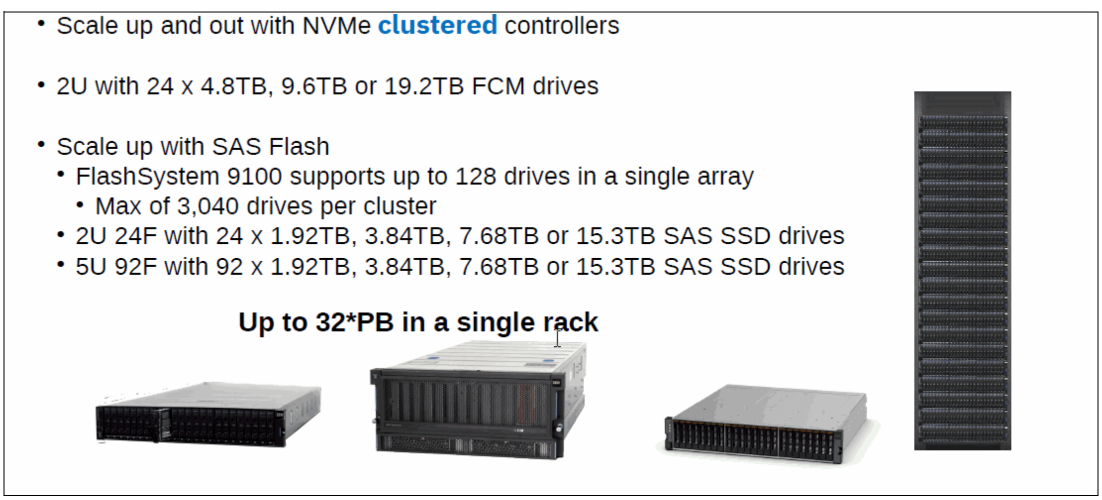


Figure 5-1 Scale Up, Scale Up building blocks

Figure 5-2 shows maximum configurations:

- Single control enclosure IOPS, and usable and effective capacity
- Scale up with four clustered control enclosures providing increased IOPS, usable and effective capacity
- Scale out expanded capacity with SAS enclosures
- Scale out capacity with supported virtualize storage controllers

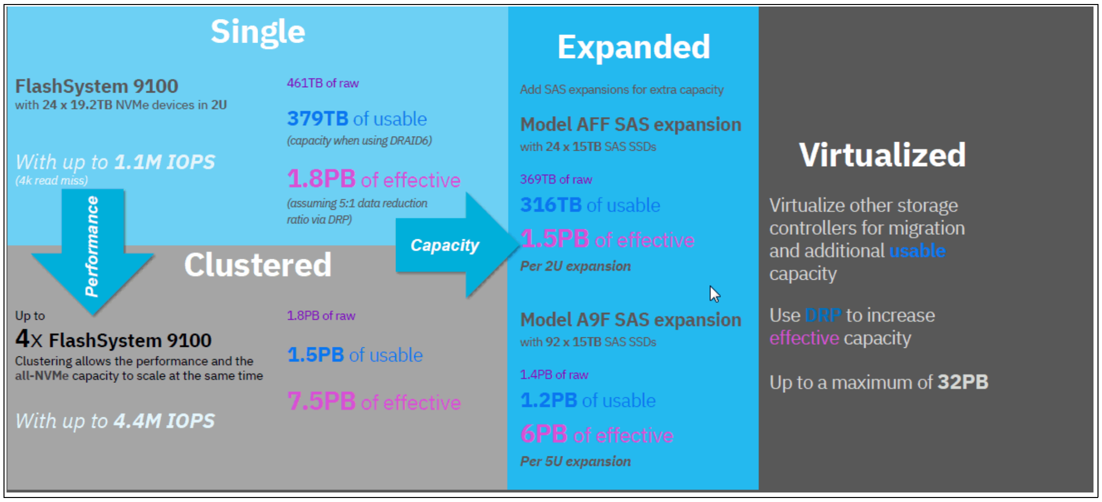


Figure 5-2 Maximum configuration: scaled up (IOPS & capacity), scaled out (capacity)

5.3 Scale up for capacity

Add capacity to existing IBM FlashSystem 9100 single or clustered systems:

- Add internal NVMe drives
- Add SAS expansion enclosures
- Add external virtualized storage systems

Scale up and out options (by adding up to four Control Enclosures and AFF/A9F Expansion Enclosures) are shown in Figure 5-3.

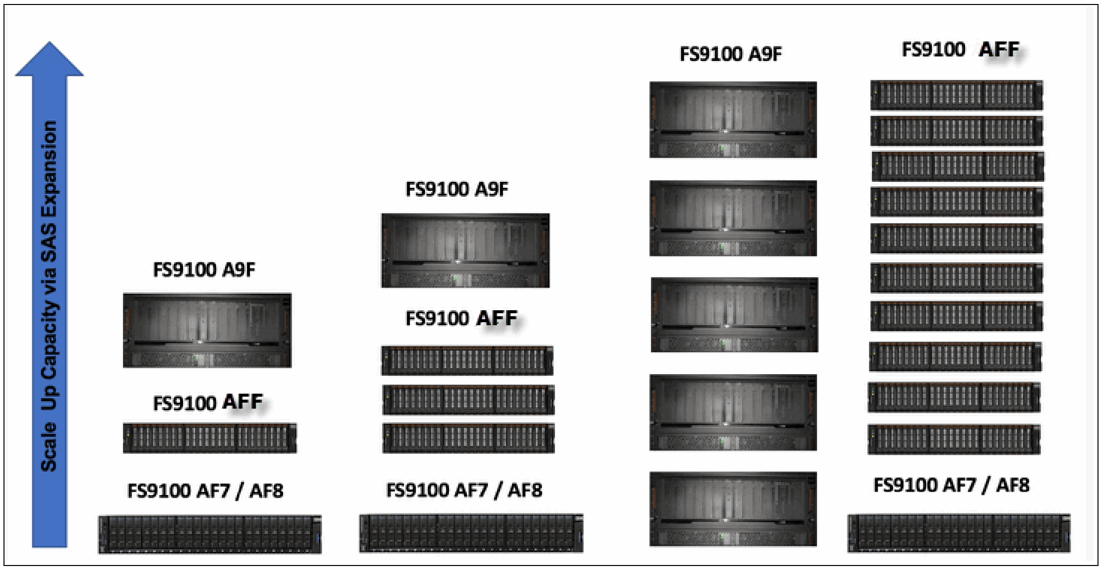


Figure 5-3 Add Control Enclosures and Storage Enclosures.

Add scale up capacity with FS9100 AFF/A9F SAS SSD Expansion Enclosure configurations, as shown in Figure 5-4.

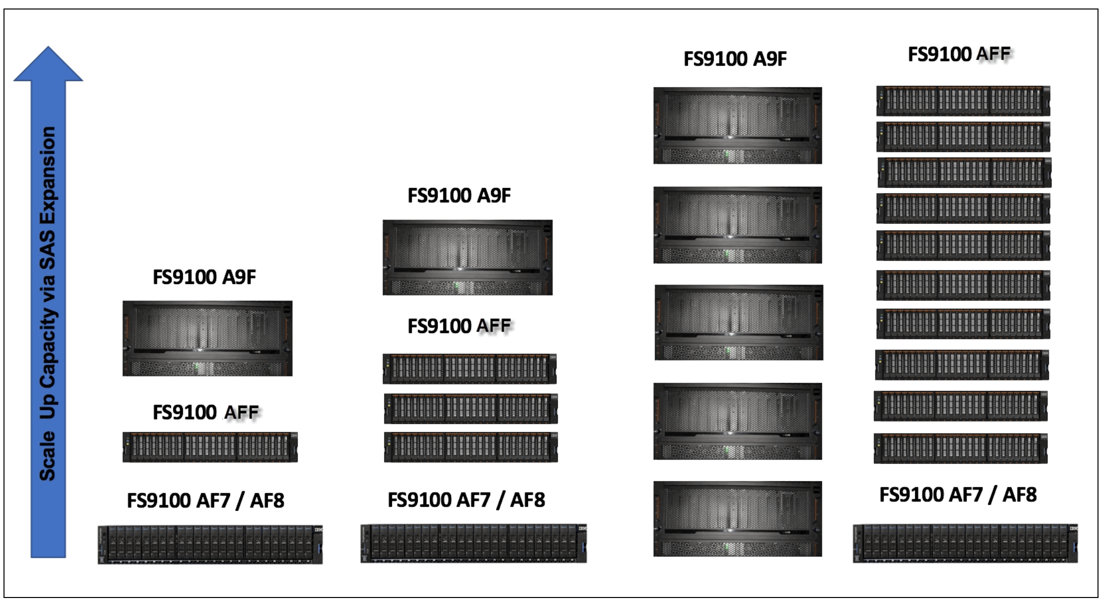


Figure 5-4 Scale Up Capacity with AFF/A9F SAS SSD expansion enclosure configurations

Scale up and out for performance and capacity configurations, as shown in Figure 5-5.

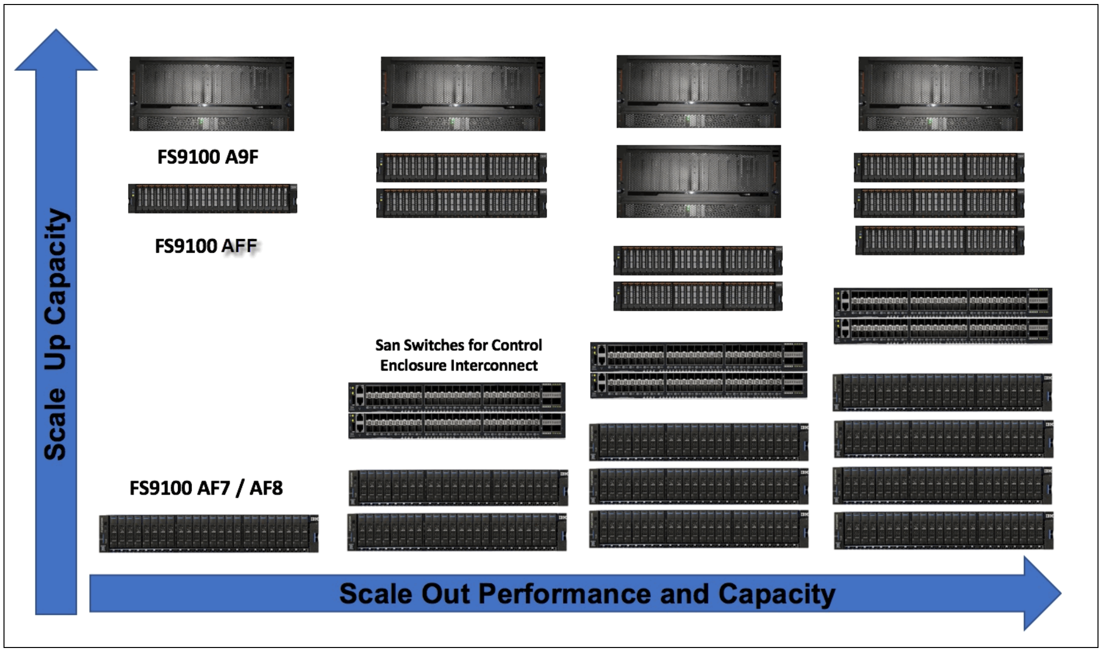


Figure 5-5 Scale up and out for performance and capacity

5.4 Adding internal NVMe storage

NVMe-accelerated enterprise Flash arrays (100% NVMe) have the following characteristics:

- ► FlashSystem 9100 has 24 x 2.5 inch slots to populate with NVMe storage (Figure 5-6)
- ► Industry-leading performance and scale:
  - – NVMe IBM FlashCore modules with inline compression
  - – NVMe industry-standard SSD
- ► NVMe IBM FlashCore modules and NVMe industry-standard SSD, offering unprecedented storage capacity in 2U of rack space
- ► Up to 8 PB of NVMe data storage in 8U with data reduction

Figure 5-6 IBM FlashSystem 9100 with 24 NVMe drives

> **Note:** Internal storage is licensed on a per-enclosure basis.

NVMe FlashCore Modules (FCMs) use inline hardware compression to reduce the amount of physical space required.

FCMs can easily provide significant amounts of capacity, either by employing performance optimized hardware compression or by using Data Reduction Pools:

- Six-drive minimum.
- Distributed RAID6 (recommended), Distributed RAID5 (supported through the CLI).
- FlashCore Modules in the same RAID array must be of the same capacity.
- Feature Codes and drive capacity types:
  - (AHS1): 4.8 TB, 2.5-inch NVMe FlashCore Module
  - (AHS2): 9.6 TB, 2.5-inch NVMe FlashCore Module
  - (AHS3): 19.2 TB, 2.5-inch NVMe FlashCore Module

Industry-standard NVMe Flash drives don't have hardware compression. The drives offer significant amounts of capacity and high performance:

- Two-drive minimum (varies by RAID type).
- Traditional RAID 10 and Distributed RAID 6 (recommended), Distributed RAID 5 (supported).
- Industry-standard NVMe drives in the same RAID array must be of the same capacity.
- Feature Codes and drive capacity types:
  - (AHT1): 800 GB, 2.5-inch NVMe Flash drive
  - (AHT2): 1.92 TB, 2.5-inch NVMe Flash drive
  - (AHT3): 3.84 TB, 2.5-inch NVMe Flash drive
  - (AHT4): 7.68 TB, 2.5-inch NVMe Flash drive
  - (AHT5): 15.36 TB, 2.5-inch NVMe Flash drive

> **Best practice:** FlashSystem 9100 is optimized for 16 - 24 NVMe devices, balancing performance, rebuild times, and usable capacity. Fewer devices are fine for smaller capacity systems that don't have a high performance requirement, but avoid a small number of large devices.

Figure 5-7 shows the minimum and maximum capacities per NVMe drive type, and capacity ranges when using either inline compression or DRP features.

Flash Media	Capacity per Drive with Inline Compression (max ratio varies 2:1 – max)	Capacity per Drive with Data Reduction Pools (2:1 – 5:1)	Max System Capacity in 2U with Inline Compression (max ratio varies 2:1 – max)	Max System Capacity in 2U with Data Reduction Pools (2:1 – 5:1)
FCM 4.8TB	9.6TB – 22TB	9.6TB – 24TB	230.4TB – 552TB	230.4TB – 576TB
FCM 9.6TB	19.2TB – 22TB	19.2TB – 48TB	460.8TB – 552TB	460.8TB – 1.1PB
FCM 19.2TB	38.4TB – 44TB	38.4TB – 96TB	921.6TB – 1PB	921.6TB – 2.3PB

Flash Media	Capacity per Drive with Data Reduction Pools (2:1 – 5:1)	Max Capacity in just 2U with Data Reduction Pools (2:1 – 5:1)
NVMe 1.92TB	3.84TB – 9.6TB	92.6TB – 230.4TB
NVMe 3.84TB	7.68TB – 19.2TB	184.32TB – 460TB
NVMe 7.68TB	15.36TB – 38.4TB	368.64TB – 921.6TB
NVMe 15.36TB	30.72TB – 76.8TB	737.28TB – 1.8PB

Figure 5-7 NVMe FCMs and Industry Standard drive and system capacities

5.4.1 Installing NVMe FCMs or NVMe SSD drives

This example shows adding a minimum of 6 NVMe drives for a new DRAID6 array.

Use the following procedures to remove a drive slot filler and replace it with a new NVMe drive. Drive slot fillers are passive components that regulate airflow through the control enclosure.

Note: Every drive slot of an operational control enclosure must contain either a drive or a drive slot filler. A drive slot must not be left empty for more than *10 minutes* during servicing. Ensure that you have read and understood the removal and drive install instructions, and have the drive unpacked before you remove the existing drive slot filler.

No tools are required to complete this task. Do not remove or loosen any screws.

Complete the following steps:

1. Unpack the NVMe drive from its packaging.
2. Use your thumb and forefinger to pinch the latch of the drive blank.
3. Gently slide the release latch up to unlock the handle.
4. Pull the drive slot filler from the drive slot to remove it, as shown in Figure 5-8.

Figure 5-8 NVMe drive slot filler

Figure 5-9 shows an example of an NVMe internal drive.

Figure 5-9 NVMe internal drive

5. Have new NVMe drive ready to install (Figure 5-10).

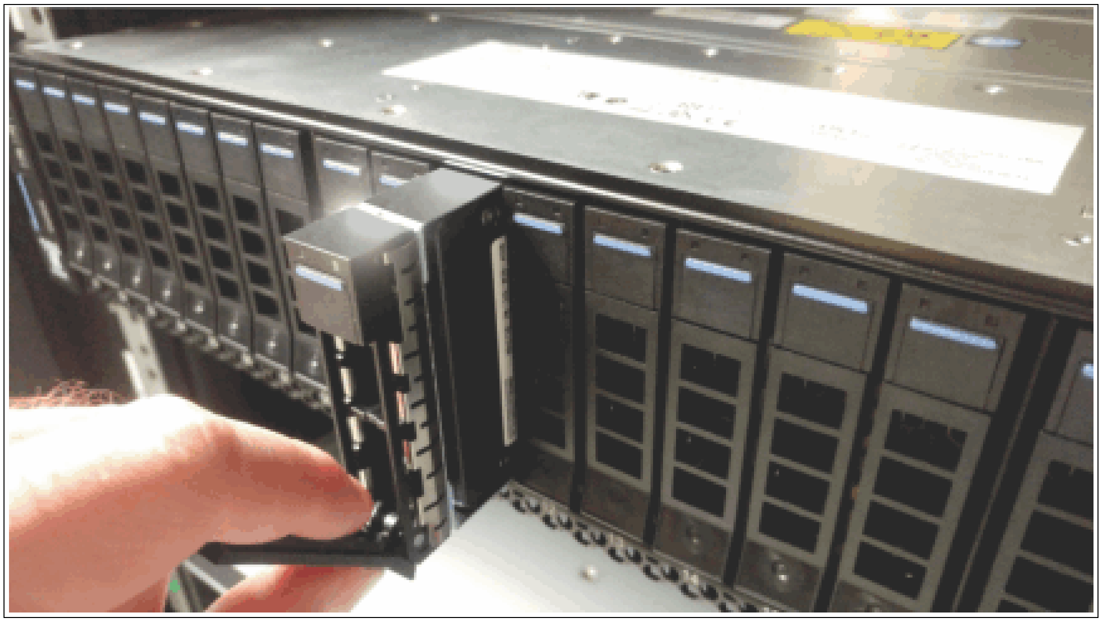


Figure 5-10 Insert NVMe drive

6. Ensure that the LED indicators are at the top of the drive.
7. Press the blue touchpoint to unlock the latching handle on the new drive.
8. Slide the new drive into the control canister, as shown in Figure 5-11. Press on the drive label near the bottom of the drive to ensure that the drive is fully inserted into the slot.

Figure 5-11 Insert new drive

9. Finish inserting the new drive by closing the handle until the latch clicks into place (Figure 5-12).

Figure 5-12 Completing the drive installation

10. Repeat steps 1 - 9 to install the remaining NVMe drives.

5.4.2 Configuring NVMe drives for MDisk and Storage Pool

After NVMe drives are installed into the control enclosure, go to the management GUI to view and configure the newly installed NVMe drives.

Figure 5-13 shows the IBM FlashSystem 9100 GUI Dashboard page.

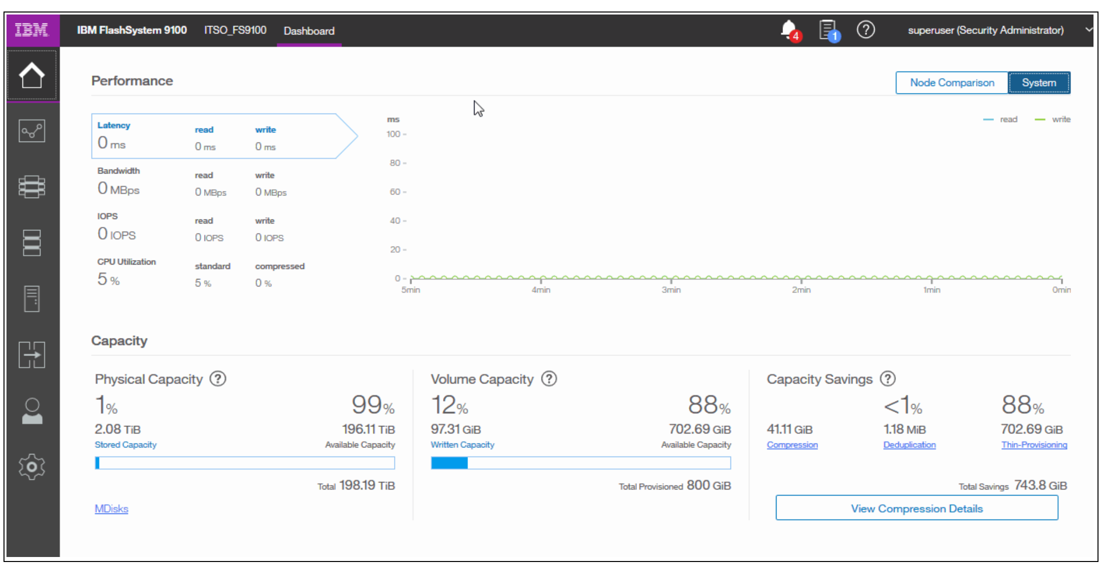


Figure 5-13 Management GUI Dashboard page

Review the new NVMe drives installed:

1. Select **Monitoring** → **System** for the System - Overview page.
2. Select **Enclosure Actions** → **Drives** to view internal drives, as shown in Figure 5-14.

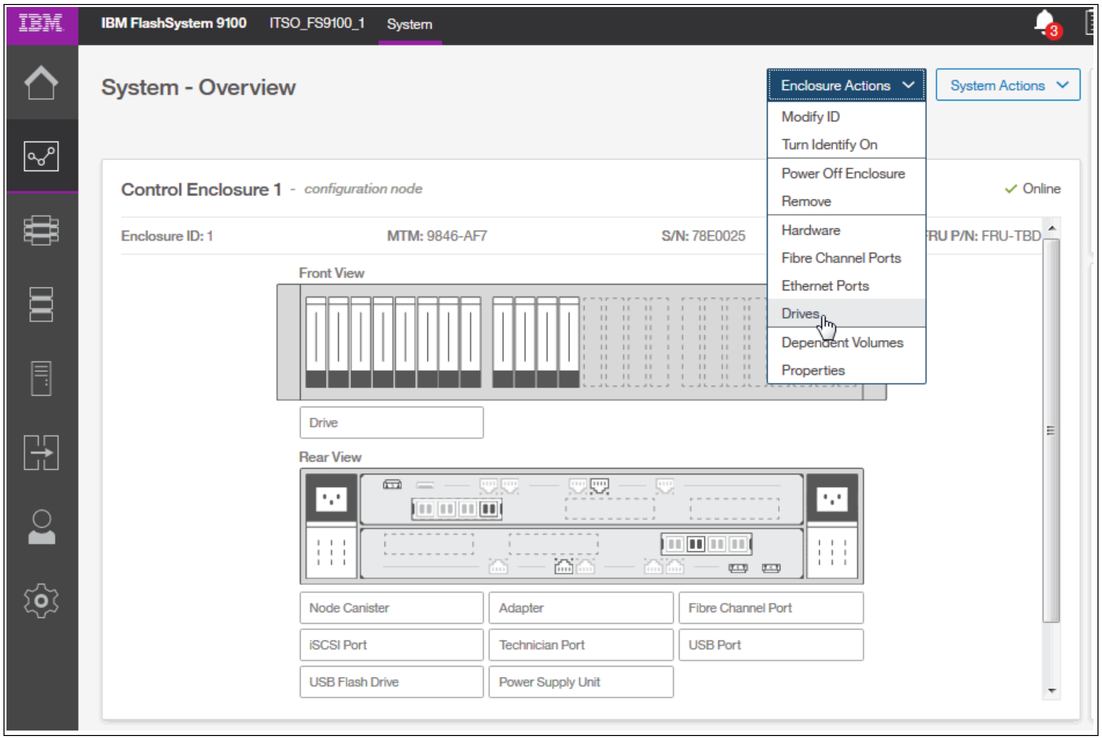


Figure 5-14 Enclosure Actions - Drives. View new NVMe drives.

The 6 new NVMe drives show in the Use column with a state of `Unused`, as shown in Figure 5-15.

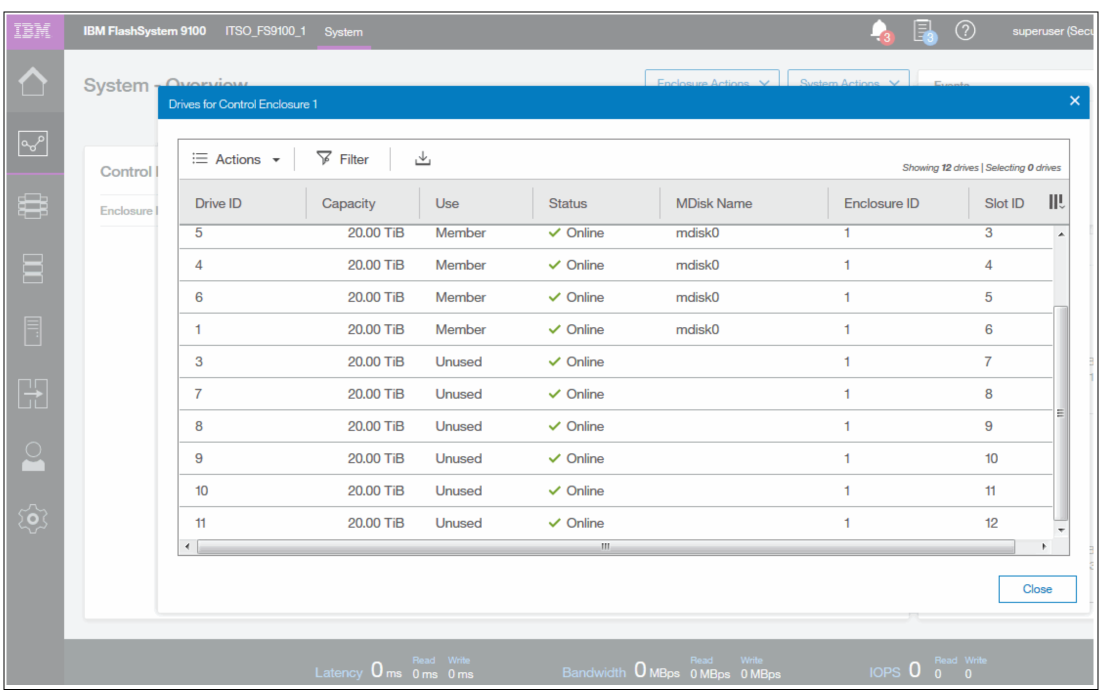


Figure 5-15 Internal NVMe drives with a Use state of Unused

Note: DRAID6 requires a minimum of 6 drives.

3. From the Drives for Control Enclosure 1 panel, perform the following actions:
   a. Click and select the new 6 NVMe drives.
   b. Select the **Actions** → **Mark As** → **Candidate** status for MDisk creation, as shown in Figure 5-16.

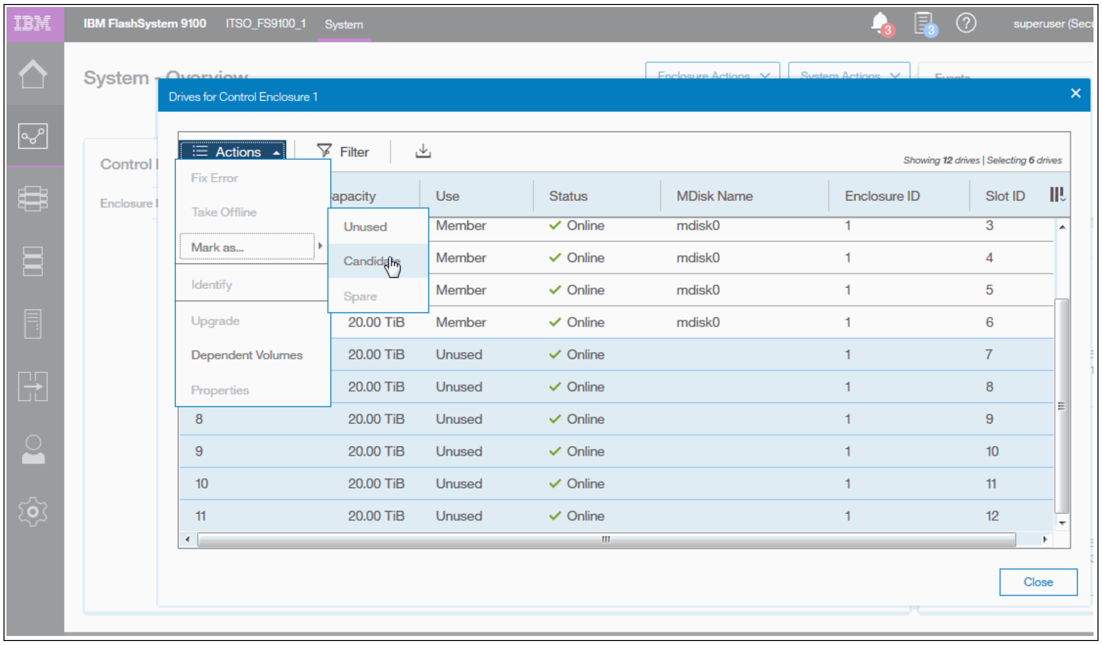


Figure 5-16 Create MDisk, select drives, and mark as Candidate

4. Click **Yes** to assign the drives to candidate use, as shown in Figure 5-17.

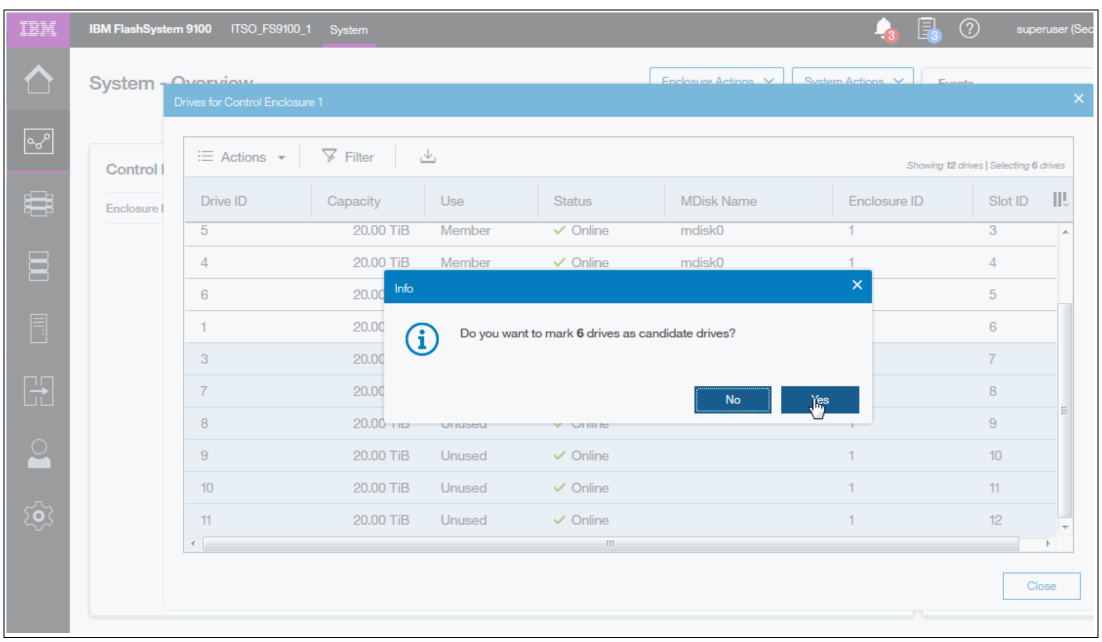
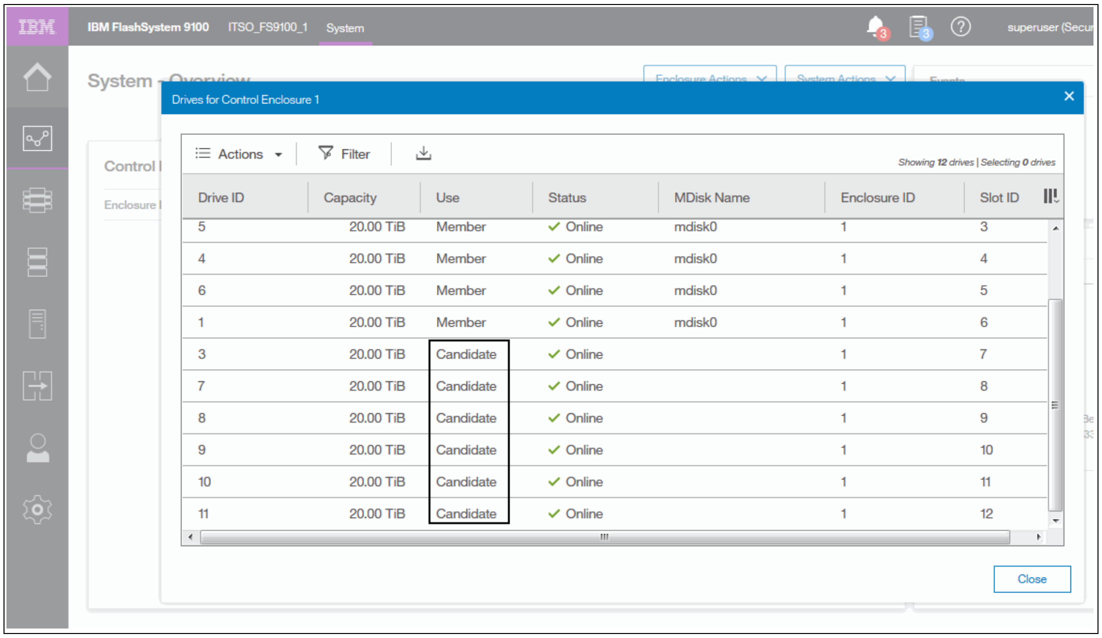


Figure 5-17 Setting drives to a Candidate state

Drives are now in the **Candidate** state, as shown in Figure 5-18.



Drive ID	Capacity	Use	Status	MDisk Name	Enclosure ID	Slot ID
5	20.00 TiB	Member	Online	mdisk0	1	3
4	20.00 TiB	Member	Online	mdisk0	1	4
6	20.00 TiB	Member	Online	mdisk0	1	5
1	20.00 TiB	Member	Online	mdisk0	1	6
3	20.00 TiB	Candidate	Online		1	7
7	20.00 TiB	Candidate	Online		1	8
8	20.00 TiB	Candidate	Online		1	9
9	20.00 TiB	Candidate	Online		1	10
10	20.00 TiB	Candidate	Online		1	11
11	20.00 TiB	Candidate	Online		1	12

Figure 5-18 Drives Use set to Candidate

5. Select **Pools** → **MDisks by Pools** to view the drives that are available for creation of MDisks and Storage Pools, as shown in Figure 5-19.

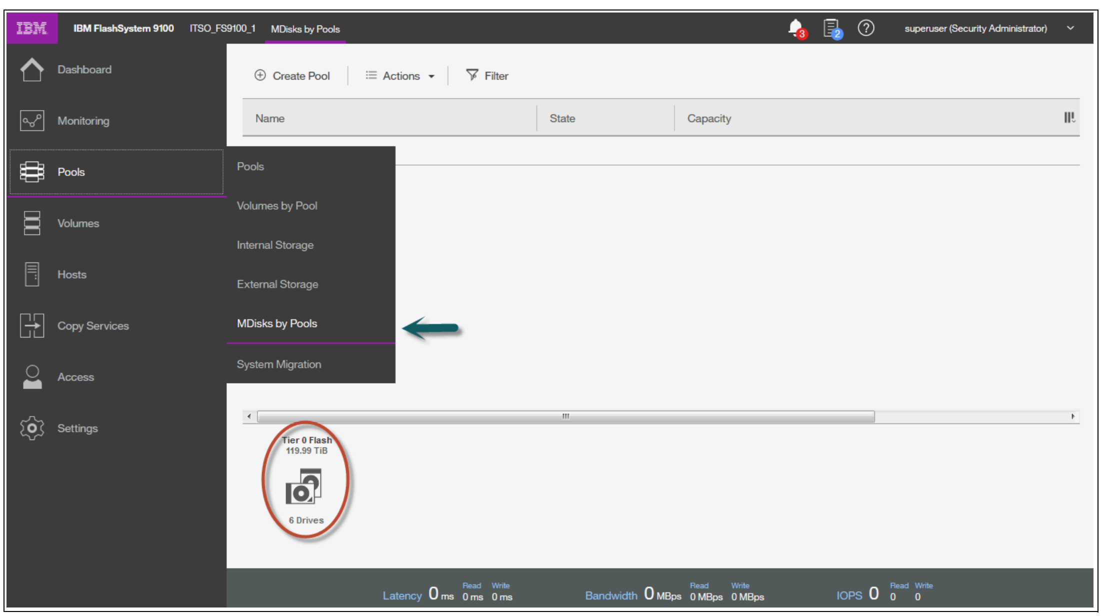


Figure 5-19 Select Pools → MDisks by Pools

5.4.3 Working with and creating storage pools

A managed disk (MDisk) is a logical unit (LU) of physical storage. MDisks are either arrays (RAID) from internal storage or LUs that are exported from external storage systems. Storage pools act as a container for MDisks by dividing the MDisks into extents. Storage pools provision the available capacity from the extents to volumes.

Figure 5-20 provides an overview of how storage pools, MDisks, and volumes are related. The system shown has four LUs from internal disks arrays, no LUs from external storage, four storage pools, and 93 defined volumes, mapped to four hosts.

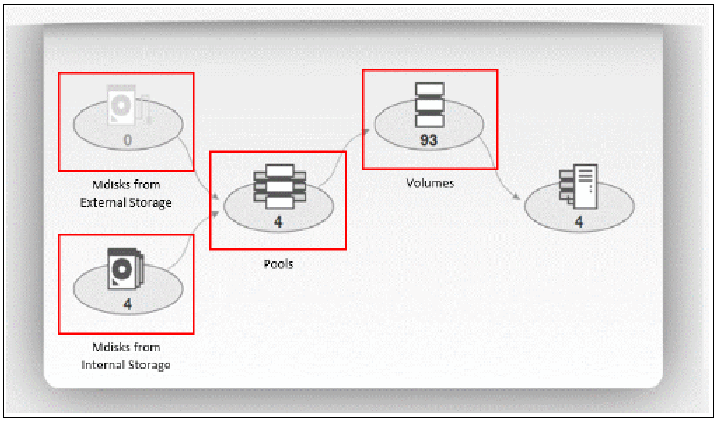


Figure 5-20 Relationship between MDisks, storage pools, and volumes

IBM FlashSystem 9100 organizes storage into pools to ease storage management and make it more efficient. All MDisks in a pool are split into extents of the same size and volumes are created out of the available extents. The extent size is a property of the storage pool, and cannot be changed after the pool is created. It is possible to add MDisks to an existing pool to provide additional extents.

Storage pools can be further divided into subcontainers that are called *child pools*. Child pools inherit the properties of the parent pool (extent size, throttle, and reduction feature) and can also be used to provision volumes.

Note: Storage Pools default to 4 GB extents.

Storage pools are managed either by using the Pools pane or the MDisks by Pool pane. Both panes allow you to run the same actions on parent pools. However, actions on child pools can be performed only through the Pools pane.

To create a storage pool, compete the following steps:

1. To access the Pools pane, click **Pools** → **Pools**.
2. Navigate to **Pools** → **MDisks by Pools** and click **Create Pool**, as shown in Figure 5-21.

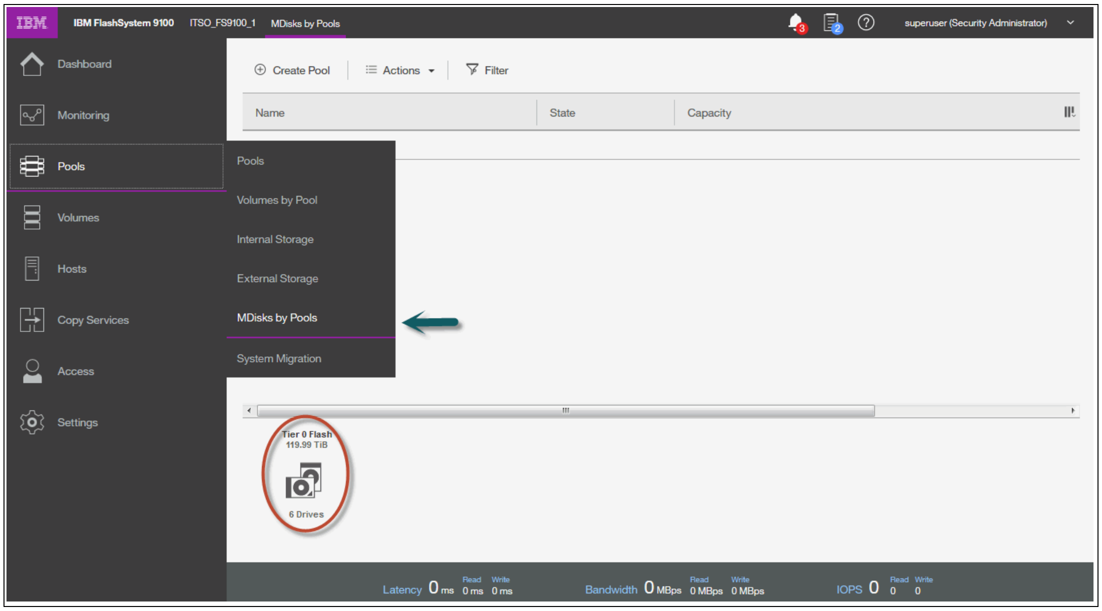


Figure 5-21 Option to create a storage pool in the MDisks by Pools pane

3. Select **Assign** to add the 6 NVMe drives to the storage pool, as shown in Figure 5-22.

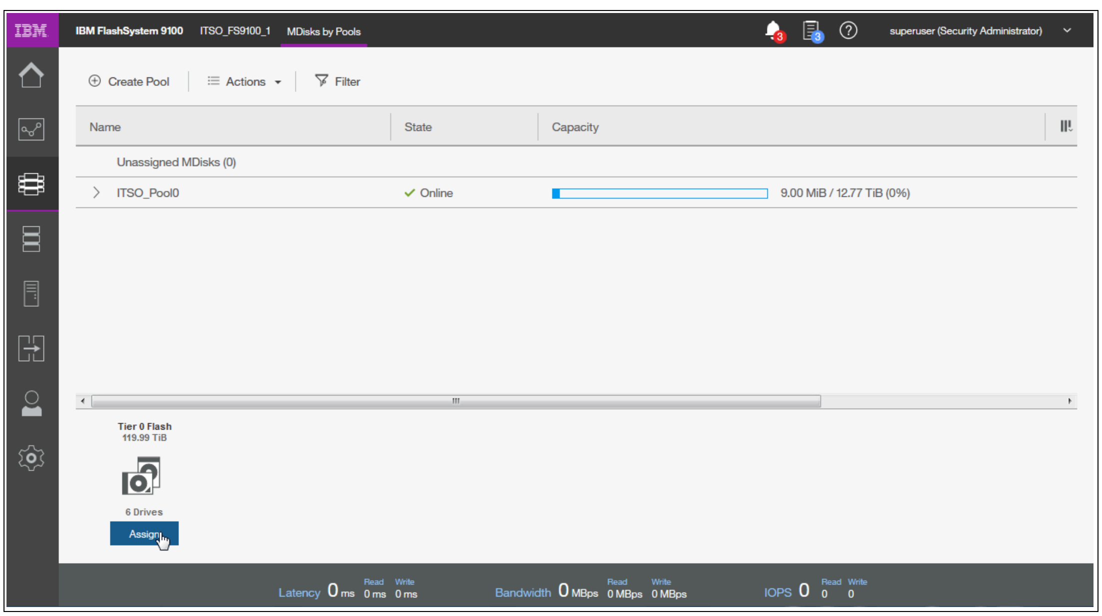


Figure 5-22 Creating an Mdisk

4. Open the Dialog box shown in Figure 5-23. Enter the Name of a new storage pool, `ITSO_Pool1`, and then click **Create**.

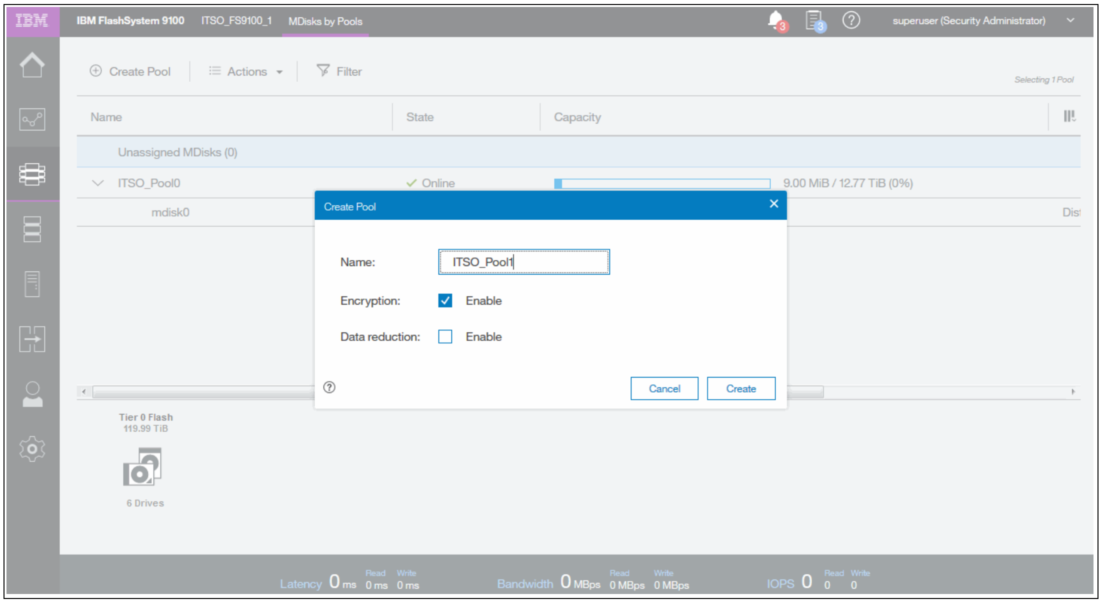


Figure 5-23 Create Pool dialog box

The new storage pool is created with no assigned drives, as shown in Figure 5-24.

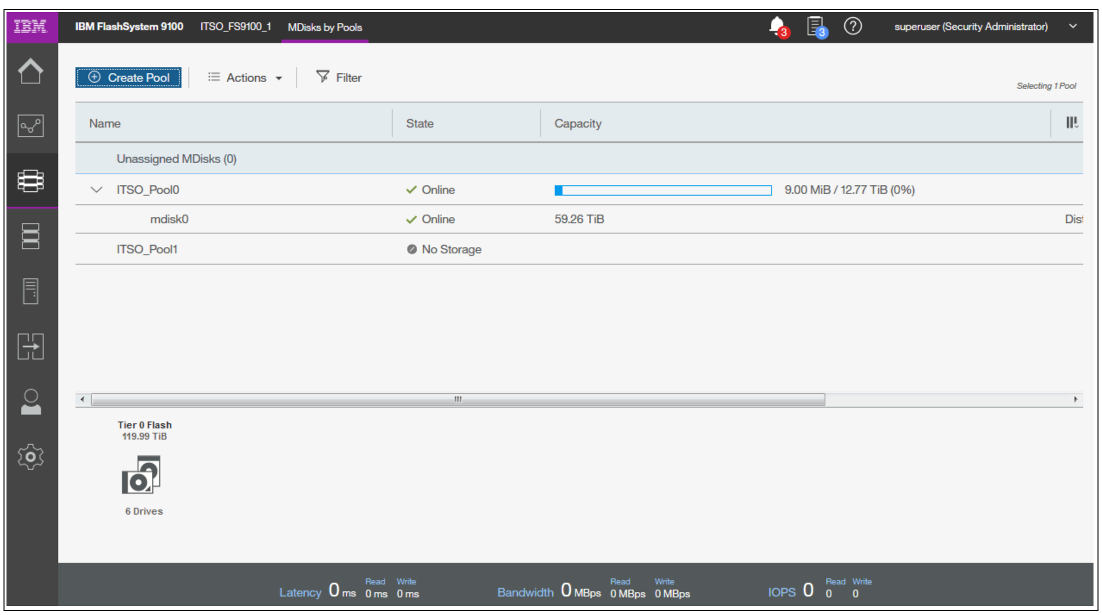


Figure 5-24 Storage pool created

5. Select **Assign Internal Storage** to add the internal NVMe drives to the storage pool, as shown in Figure 5-25.

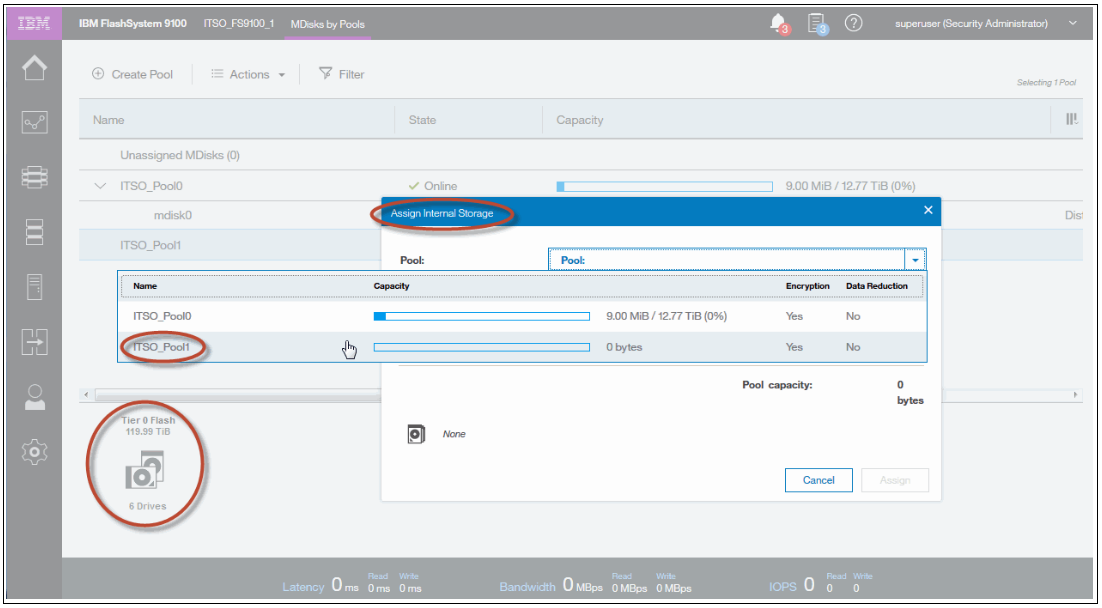


Figure 5-25 Assign internal drives to a storage pool

6. Enter a quantity of 6 drives for DRAID6 to add to the storage pool, as shown in Figure 5-26.

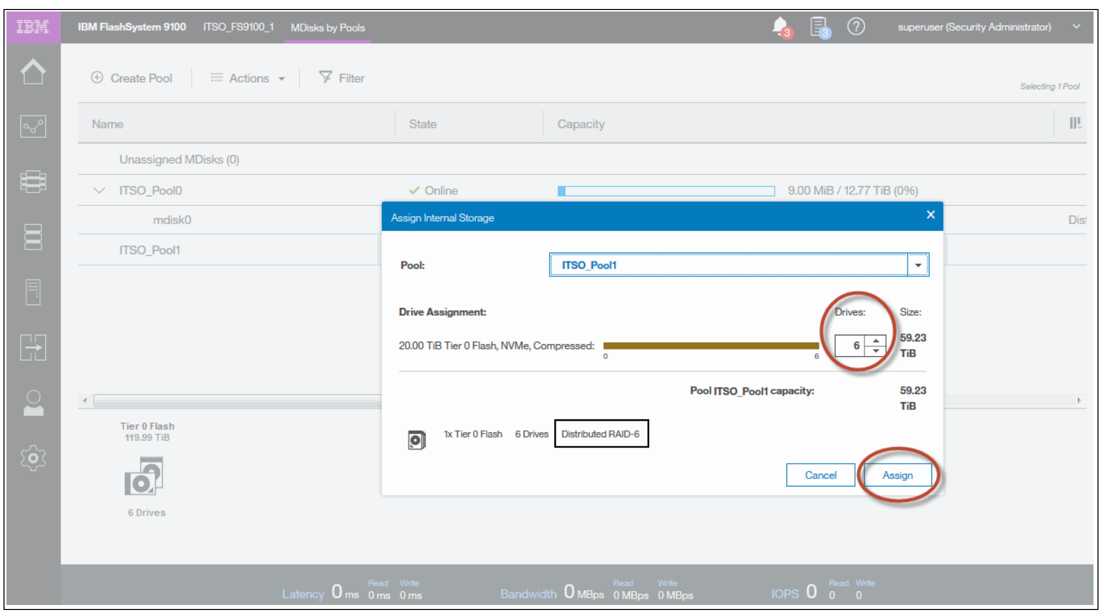


Figure 5-26 Number of drives is 6

An MDisk with 6 internal NVMe drives has been added to the storage pool, as shown in Figure 5-27.

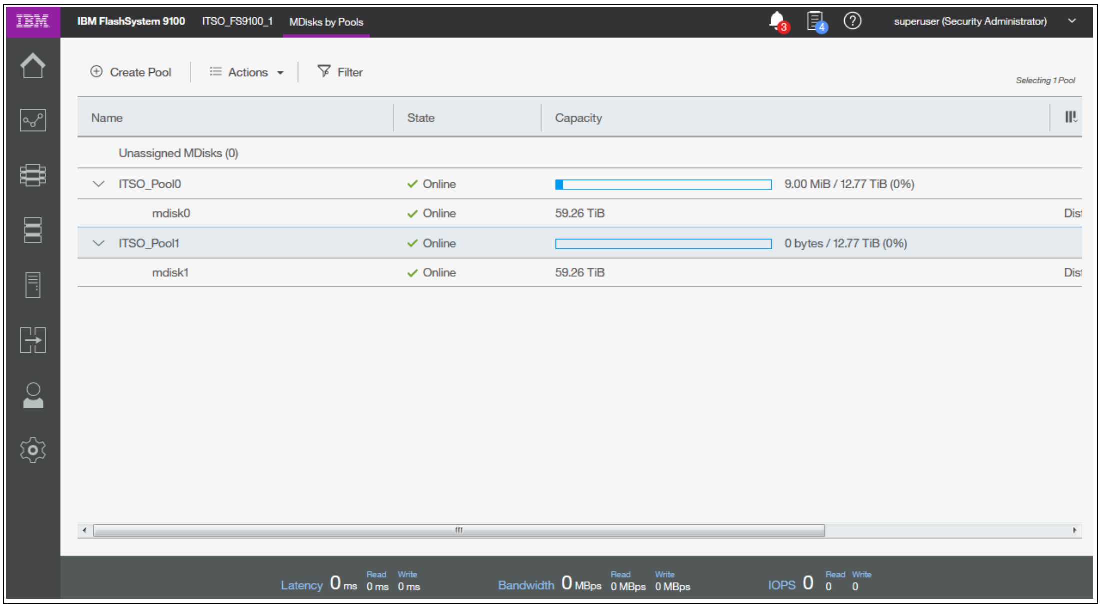


Figure 5-27   New MDisk mdisk1 in a storage pool with 6 new NVMe drives

The MDisk in the storage pool with new internal NVMe drives is available.

5.5 Adding another Control Enclosure into an existing system

Scaling out for performance is done by adding additional control enclosures to an existing cluster. These additional NVMe control enclosures are managed by the same GUI or CLI as the existing IBM FlashSystem 9100.

Scale out adds additional control enclosures to an existing IBM FlashSystem 9100 and the maximum number of control enclosures is four. Adding an enclosure to the system increases the capacity of the entire system. When you add an enclosure to a system, check that the licensed functions of the system support the additional enclosure. For more information, see Licensed functions in IMB Knowledge Center.

> **Note:** There can be up to four systems in a cluster, a mixture of FlashSystem 9110, FlashSystem 9150 and Storwize V7000 Gen 2 and Gen 2+.

Before beginning this process, ensure that the new control enclosure is correctly installed and cabled to the existing FlashSystem 9100 system. Ensure that the Ethernet and Fibre Channel connectivity is correctly configured and that the enclosure is powered on.

5.5.1 SAN configuration and zoning

For more information about configuration and zoning, see the following sections in IBM Knowledge Center:

- SAN configuration and zoning rules summary
- Configuring N_Port ID Virtualization

Note: FlashSystem 9100 with V8.2.0 or later have N_Port ID Virtualization (NPIV) enabled as the default status. On NPIV-enabled configurations, for switch zone use the *physical WWPN* for the intracluster zoning.

An example SAN configuration is shown in Figure 5-28.

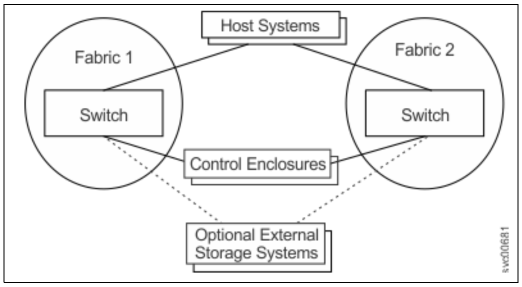


Figure 5-28 Simple SAN Configuration

Zoning

In FlashSystem 9100 deployments, the SAN fabric must have two distinct zone classes:

- Host zones: Allows communication between FlashSystem 9100 and hosts.
- Storage zone: Allows communication between FlashSystem 9100 and back-end storage.

In clustered configurations a third zone is required, allowing communication between storage system nodes (intra-cluster traffic).

Figure 5-29 shows the FlashSystem 9100 zoning classes.

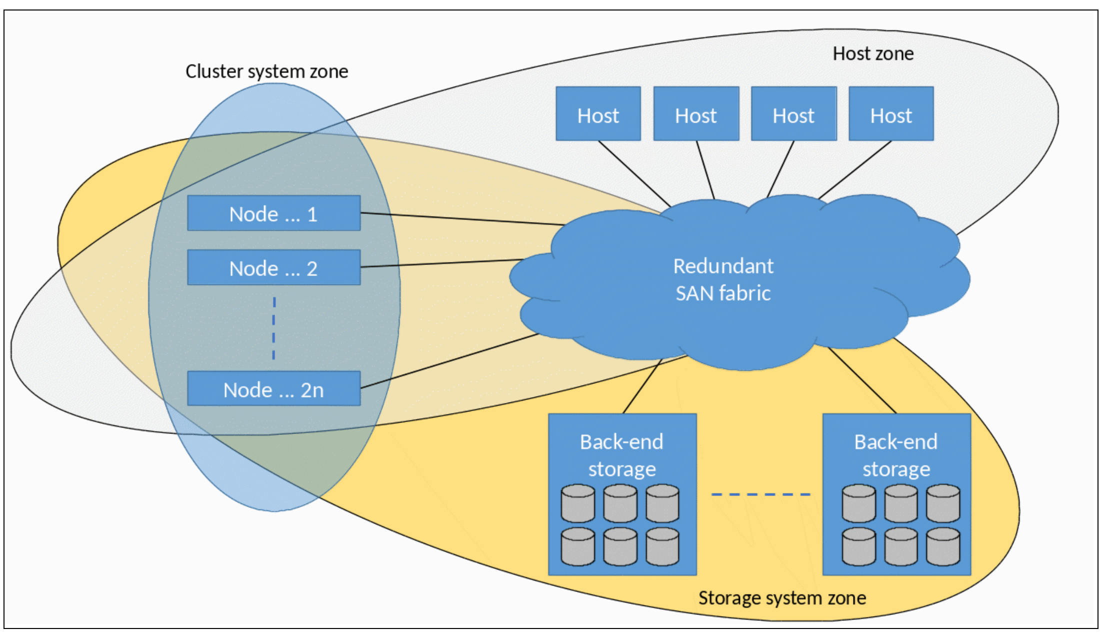


Figure 5-29 FlashSystem 9100 zoning classes

5.5.2 Adding a Control Enclosure that was previously removed

> **Note:** If the Control Enclosure was previously configured or part of another FlashSytem 9100 cluster, perform the procedure in 5.5.2, "Adding a Control Enclosure that was previously removed".
>
> If you are adding a new FlashSystem 9100 control enclosure that was not previously configured, proceed to 5.5.3, "Add Control Enclosure using the management GUI" on page 139.

Ensure that these conditions are met:

- All hosts that accessed the removed enclosure through its WWPNs are reconfigured to use the WWPN for the new enclosure, or to no longer access the enclosure. Failure to do so can result in data corruption.
- Ensure that the system ID is reset on the new Control Enclosure. On the new Control Enclosure, you can use either the Service command-line interface or the Service Assistant to verify the system ID:
  - To use the command-line interface, enter the following command:

    ```
    satask chvpd -resetclusterid
    ```

  - To use the Service Assistant on the new Control Enclosure, complete the following steps:
    i. Connect to the service assistant on either of the nodes in the Control Enclosure.
    ii. Select **Configure Enclosure**.
    iii. Select the **Reset the system ID** option. Do not make any other changes on the panel.
    iv. Click **Modify** to make the changes.

Next, complete the following steps:

1. Sign into the Service Assistant (Figure 5-30) on the main Control Enclosure, then change the new node's status to `Candidate`.

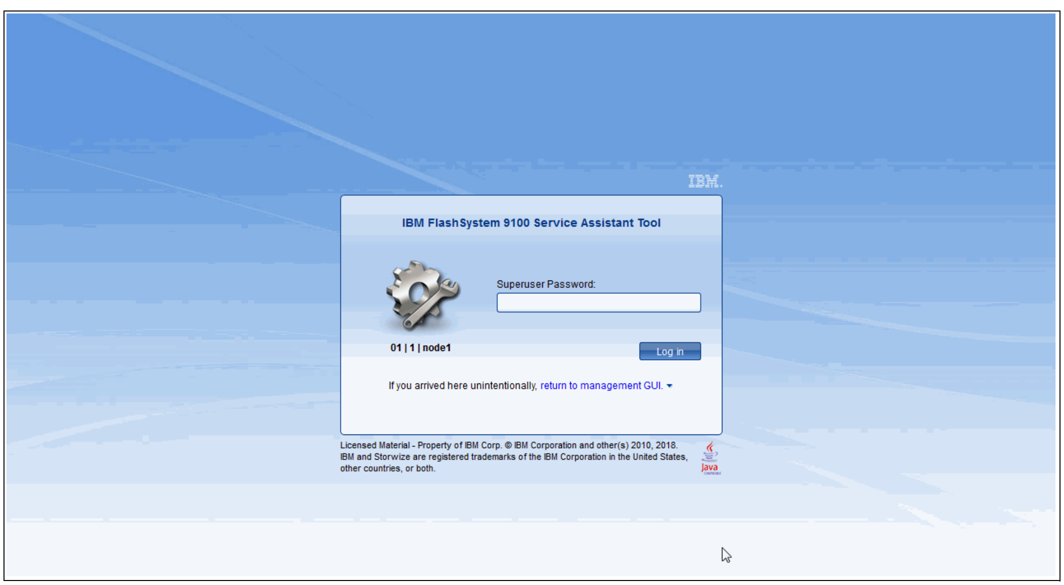


Figure 5-30 Service Assistant Login screen

2. Node 1 and 2 are in Service status. Click node 1, select **Exit Service State** to change the node from `Service` to `Candidate` status, as shown in Figure 5-31.

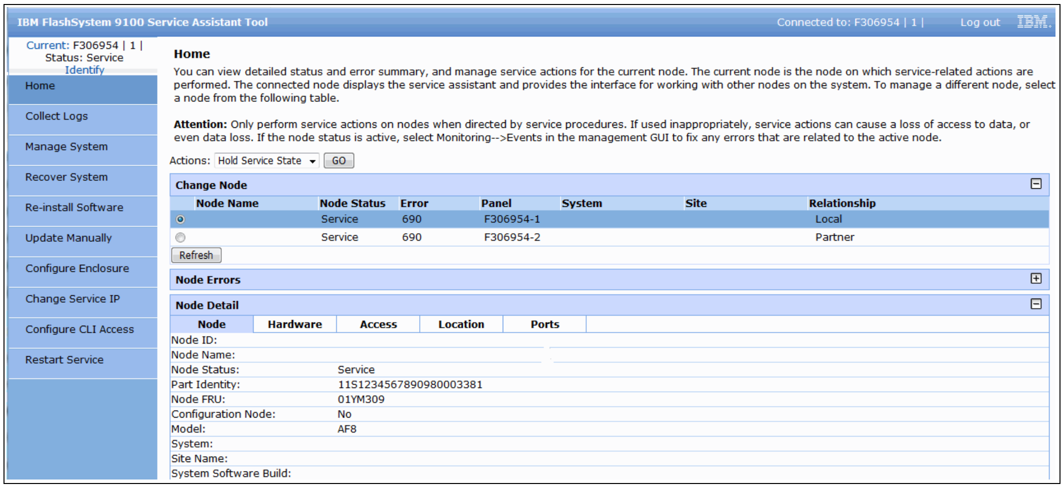


Figure 5-31 Change Node 1 status to Candidate

3. Click node 2, select **Exit Service State** to change the node from `Service` to `Candidate` status as shown in Figure 5-32.

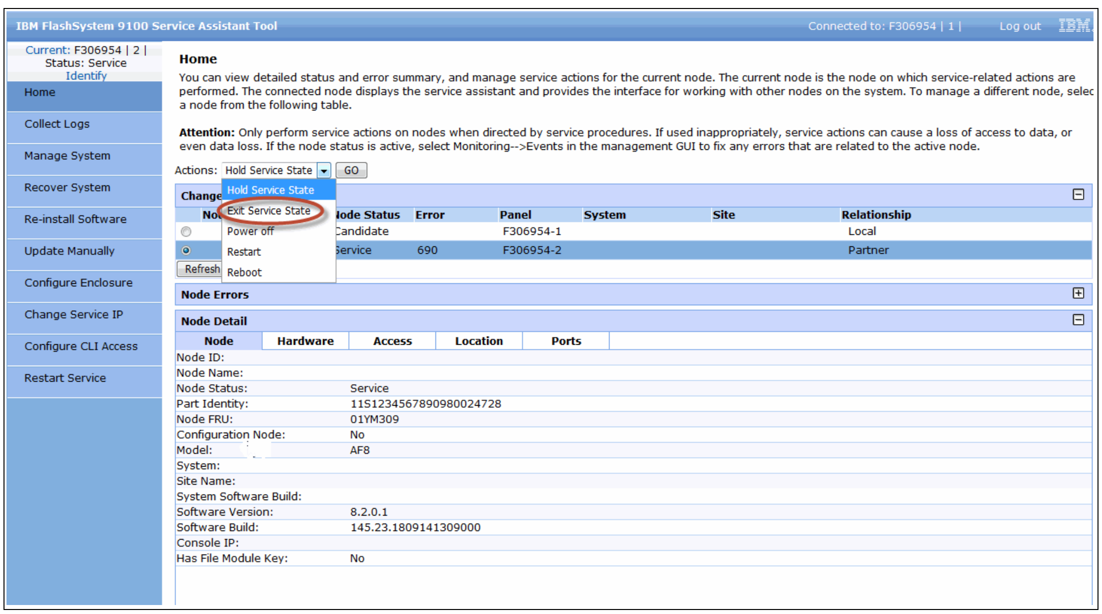


Figure 5-32 Change Node 2 status to Candidate

Node 1 and 2 are in `Candidate` status and ready for MDisk creation as shown in Figure 5-33.

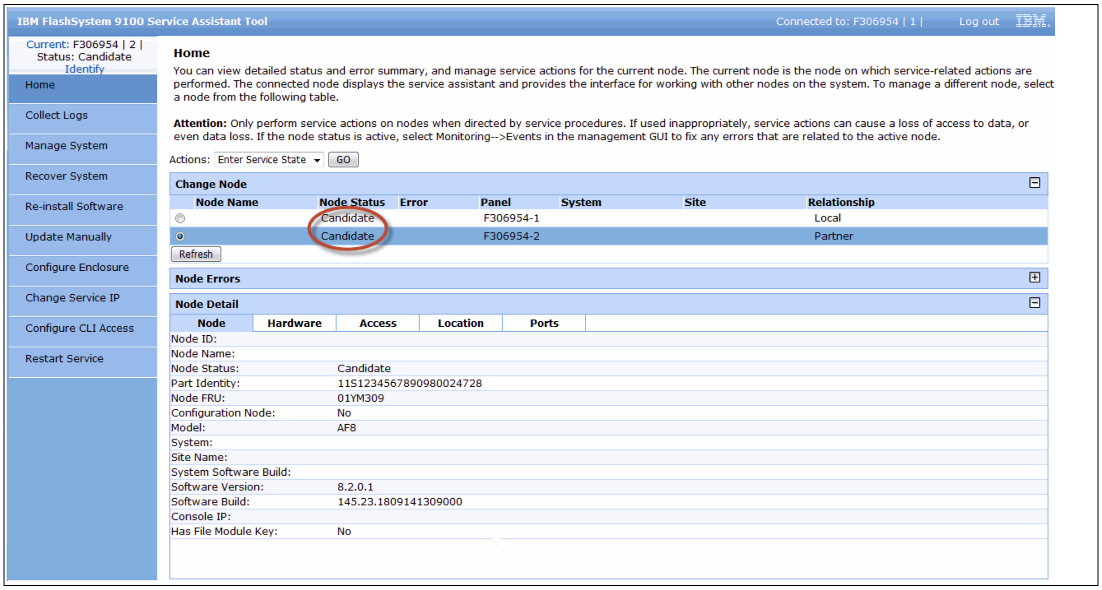


Figure 5-33 Node Status set to Candidate on both nodes

4. Using Service Assistant on the cluster IP, the FlashSystem 9100 Control Enclosures 1 and 2 are shown as in Figure 5-34.

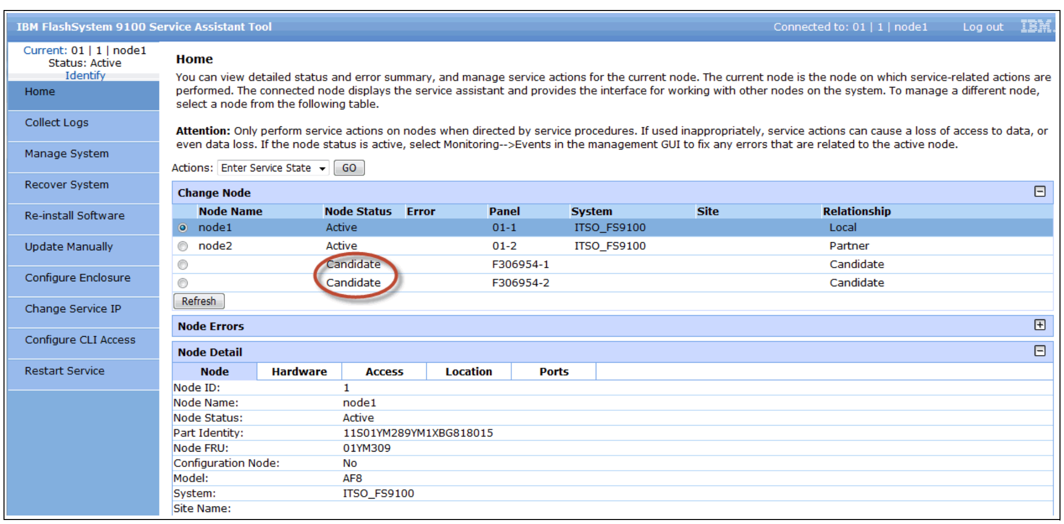


Figure 5-34 View from cluster Service Assistant showing Control Enclosure 1 and 2

5.5.3 Add Control Enclosure using the management GUI

Either use the management GUI or the CLI to add a Control Enclosure to the system.

Use either the **`addcontrolenclosure`** CLI command or the **Add Enclosure** wizard in the management GUI.

To access the **Add Enclosure** wizard, select **Monitoring > System.** On the **System -- Overview** page. If **Add Enclosure** is not displayed, it indicates a potential cabling issue. Check the installation information to ensure that the enclosure was cabled correctly.

Complete the following steps to add a new control enclosure to the system:

1. Click **Add Enclosure** to start the wizard, as shown in Figure 5-35.

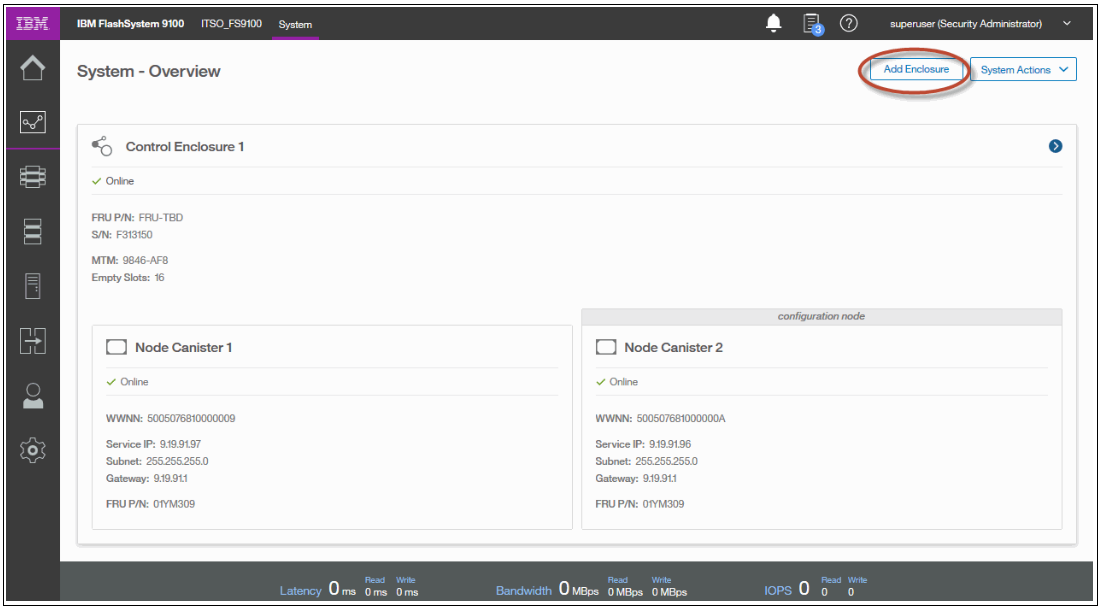


*Figure 5-35 Select **Add enclosure***

2. The first dialog box displays the available control enclosure and its details, as shown in Figure 5-36. Note that the first control enclosure has encryption licensed and enabled.

Note: The expansion enclosures that are directly cabled to the new Control Enclosure are not listed. However, they are added automatically when the control enclosure is added.

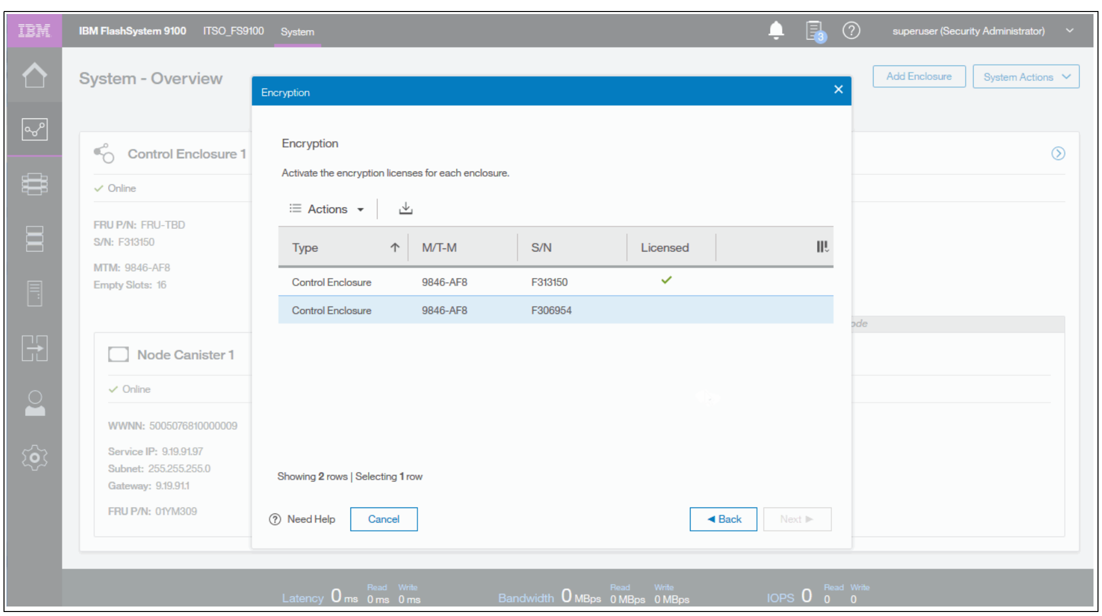


Figure 5-36 Adding a control enclosure to the system

3. Select the new control enclosure to **Activate License** Automatically or Manually, as shown in Figure 5-37.

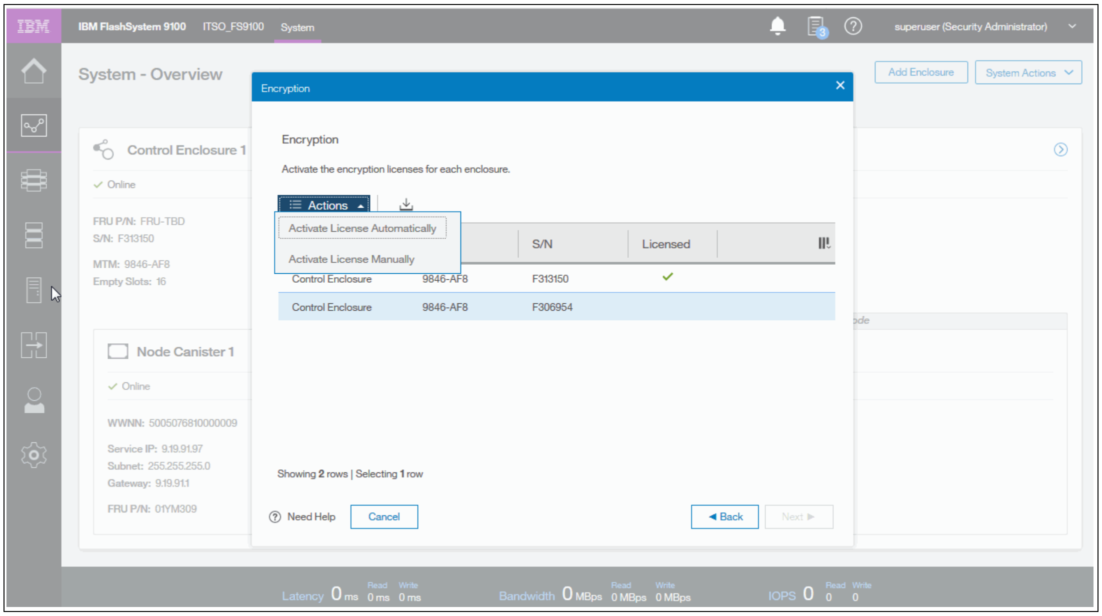


Figure 5-37 Select node for Encryption license enablement

4. Enter the **Authorization Code for control enclosure**, as shown in Figure 5-38.

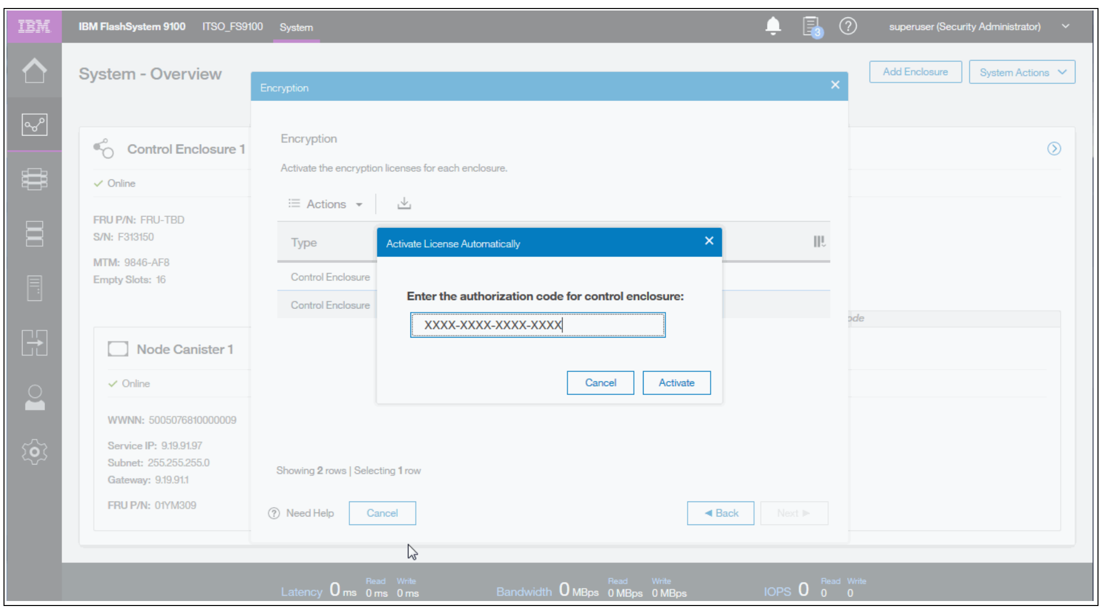


Figure 5-38 Enter Activation encryption key

5. The new Control Enclosure Encryption License has been enabled, as shown in Figure 5-39.

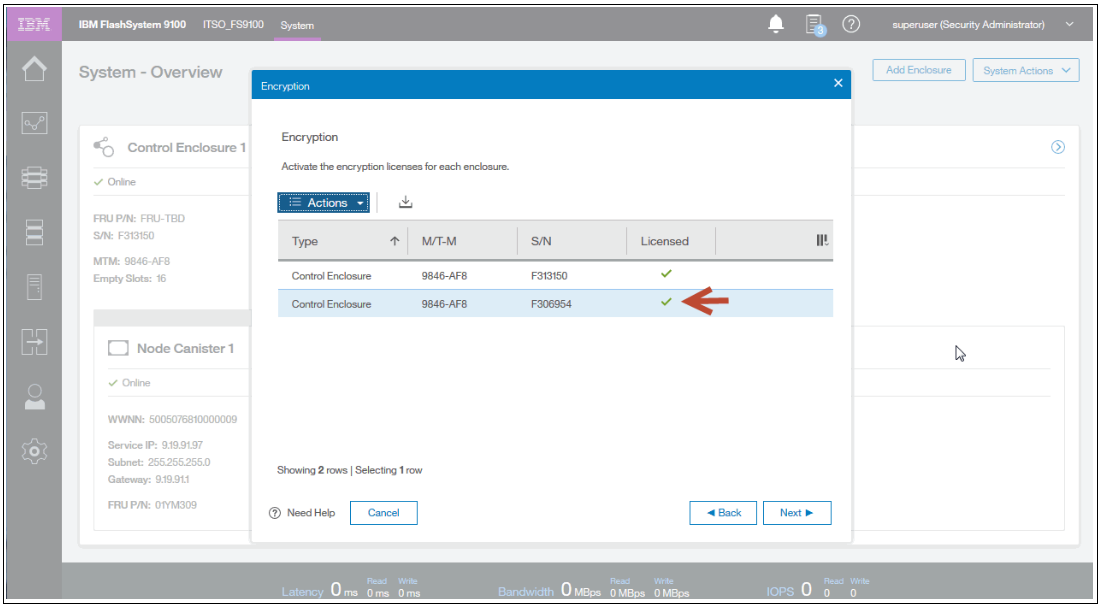


Figure 5-39 Encryption enabled

6. Review the summary in the next window and click **Finish** to add the control enclosure and all its expansions to the system as shown in Figure 5-40.

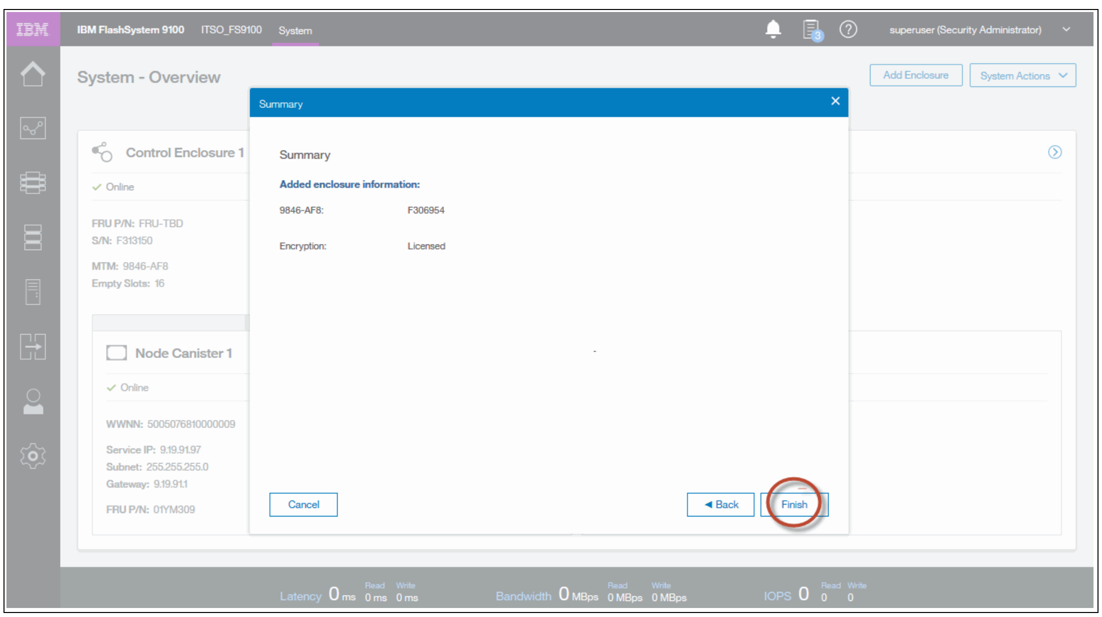


Figure 5-40 Select **Finish**

Figure 5-41 shows the task has completed.

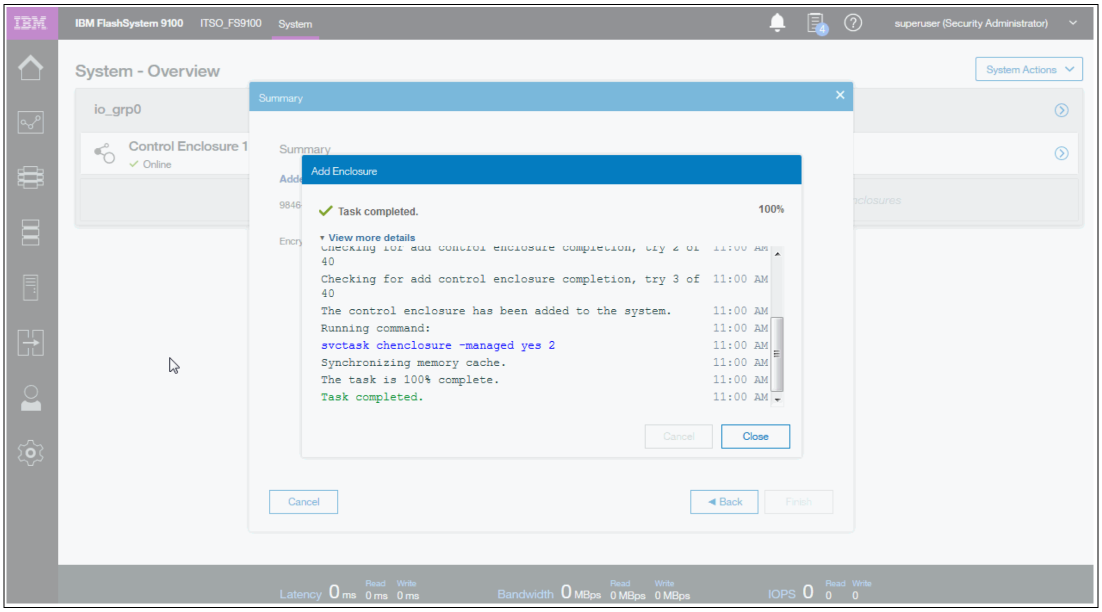


Figure 5-41 Add Enclosure task completed

7. After the control enclosure has been successfully added to the system, a success message displays, as shown in Figure 5-42. Click **Close**.

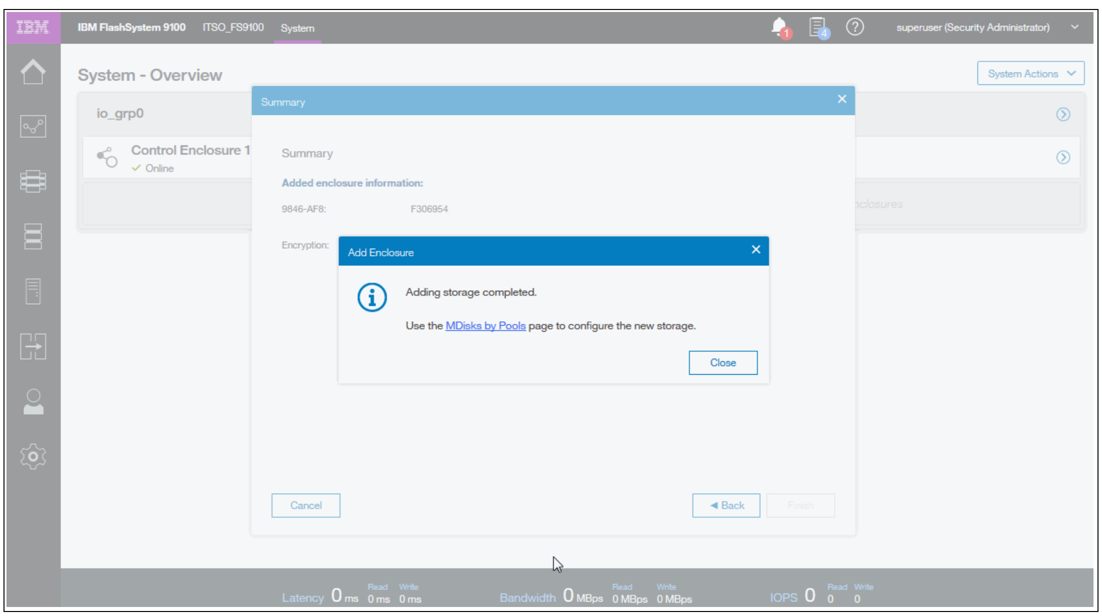


Figure 5-42 Add Control Enclosure completed

8. Navigate to **System - Overview** page to view details of Control Enclosures as shown in Figure 5-43 with an empty I/O Group.

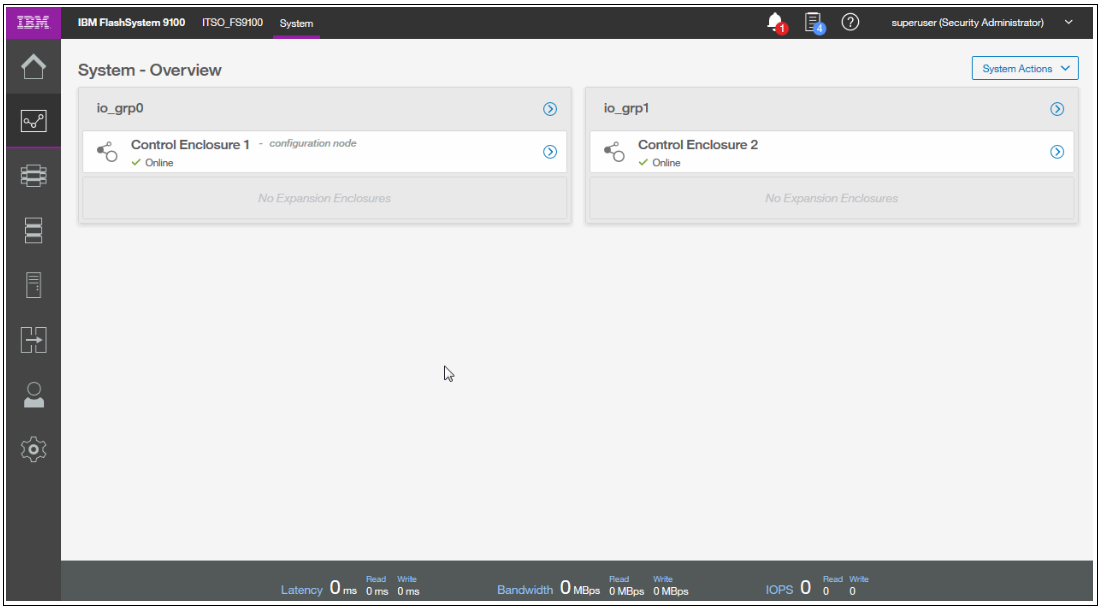


Figure 5-43 System - Overview Control Enclosures view

9. Click > on Control Enclosure 2 to view enclosure details, as shown in Figure 5-44.

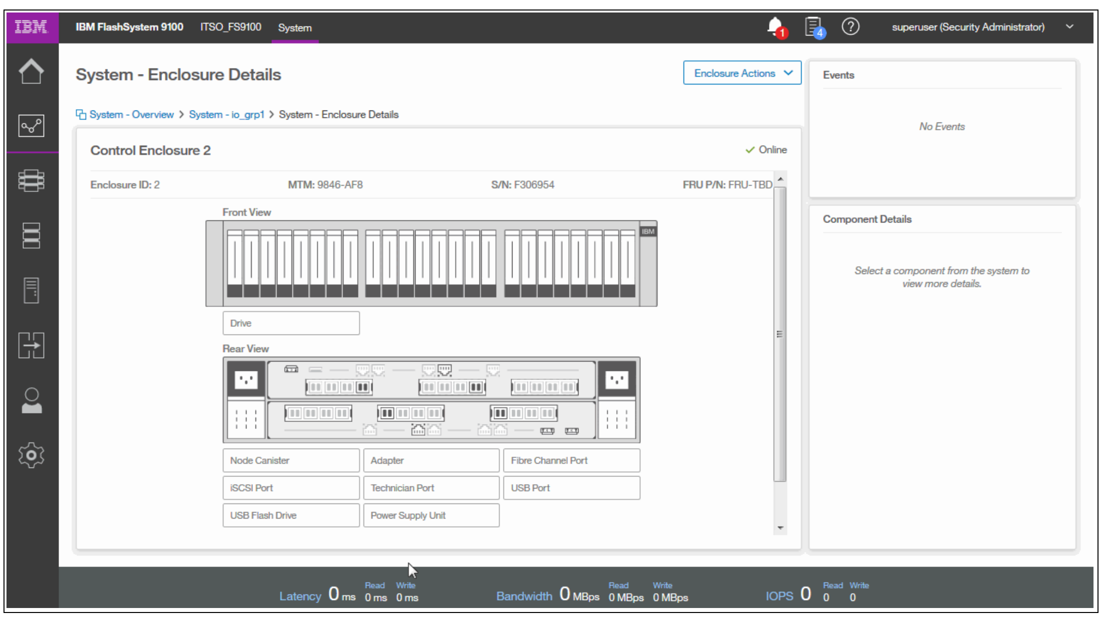


Figure 5-44 Control Enclosure 2 details

10. An error displays in the Event Log, `Error Code 3124 No Active quorum device found`, as shown in Figure 5-45. The error can be cleared by running **Run Fix** wizard or can be ignored until MDisk, and Storage Pool is created.

11. Click **Run Fix** to run the wizard and create an MDisk.

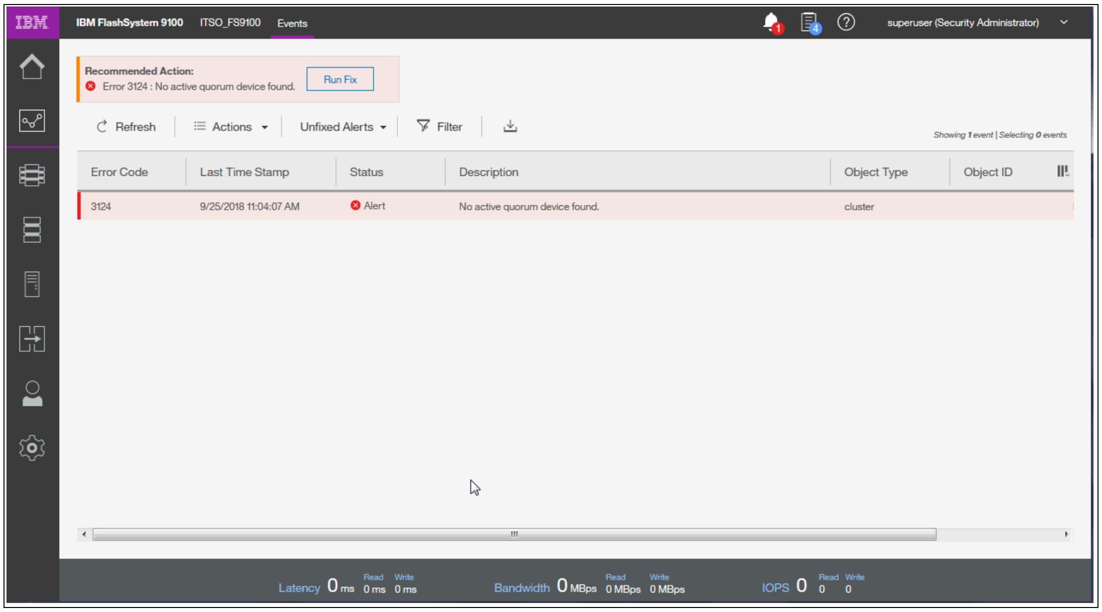


Figure 5-45 Error Code 3124 - No Active quorum device found

12. Select **Create some managed disks** and click **Next**, as shown in Figure 5-46.

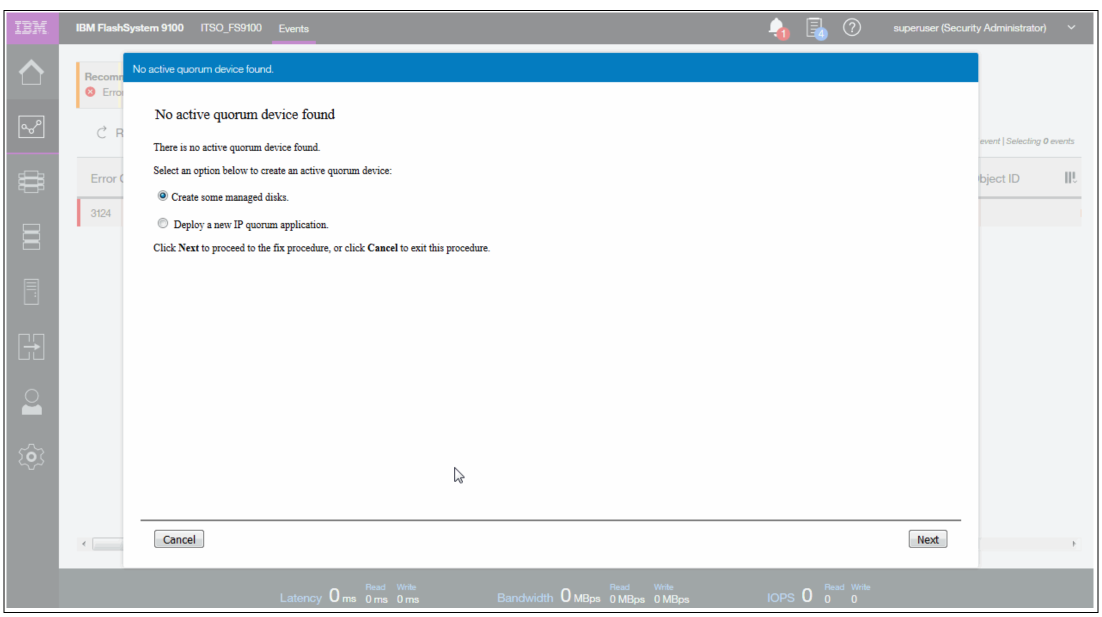


Figure 5-46 Create some managed disks

13.Select **Next** to create the MDisk, as shown in Figure 5-47.

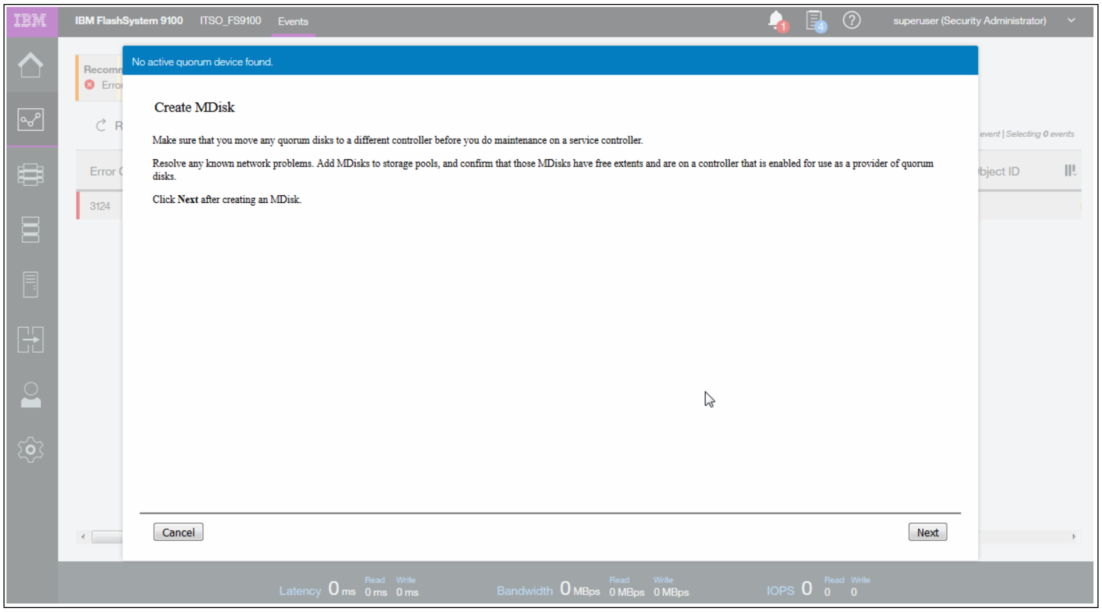


Figure 5-47 Create MDisk

The system checks **Quorum Device Status** for 60 seconds. When the screen refreshes the next screen displays, as shown in Figure 5-48.

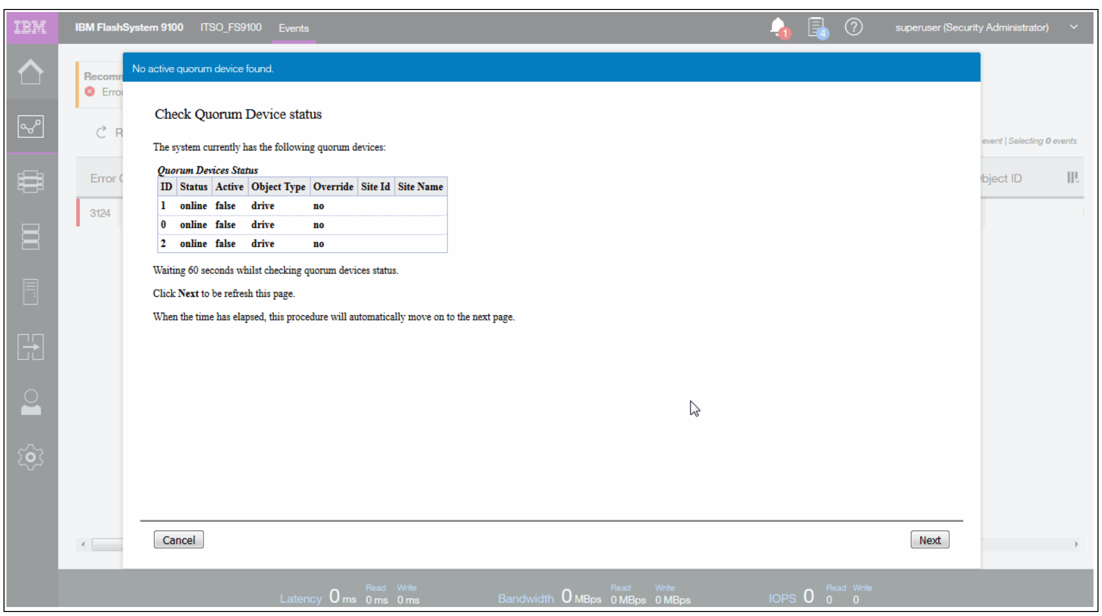


Figure 5-48 Check Quorum Device status

Error 3124 has been fixed, Quorum Devices are online, and the managed disk (MDisk) was created, as shown in Figure 5-49.

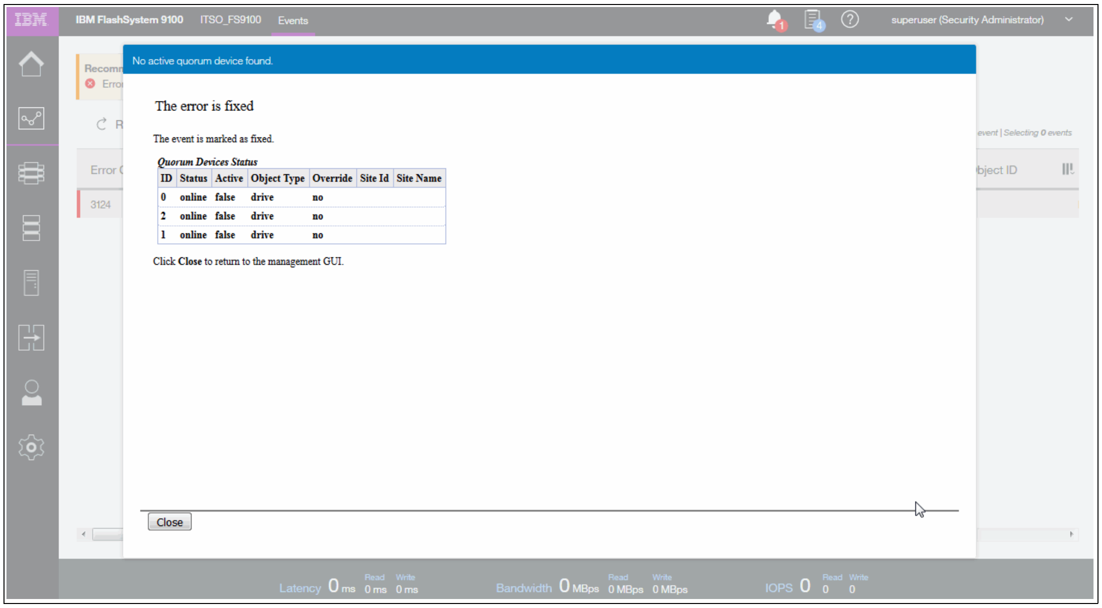


Figure 5-49 Error is fixed

There are now no errors in the Event Log, as shown in Figure 5-50.

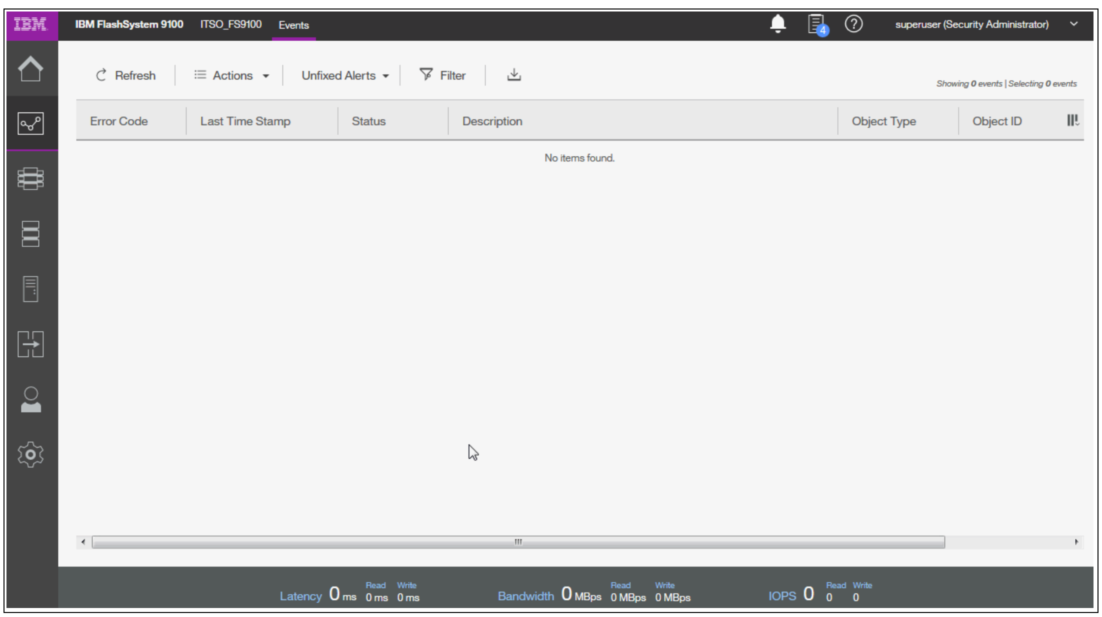


Figure 5-50 Error Event Log

NVMe internal drives on new Control Enclosure are available to be assigned to a Storage Pool, as shown in Figure 5-51.

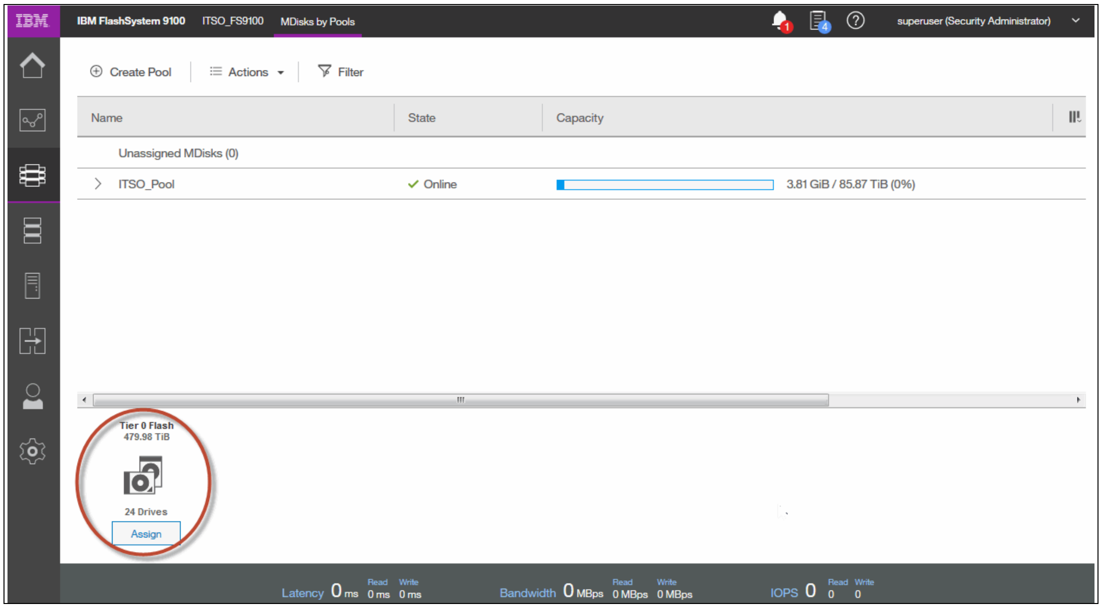


Figure 5-51 Assign new available NVMe drives to Storage Pool

14. Enter the name of the new Storage Pool, for example `ITSO_Pool2`, as shown in Figure 5-52.

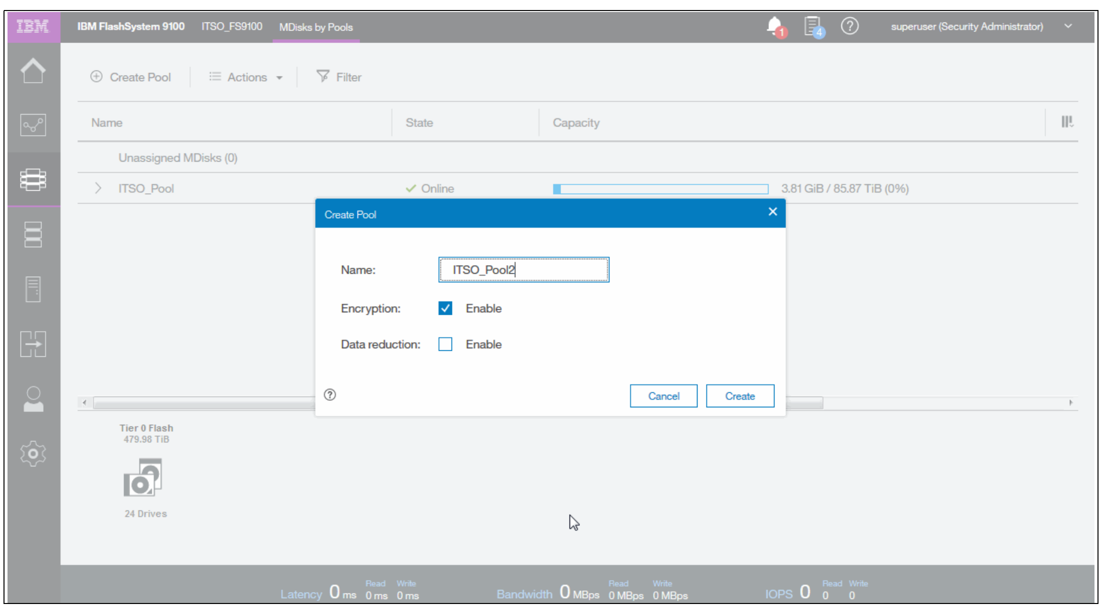


Figure 5-52 Create Storage Pool.

5.5.4 Add Control Enclosure - management CLI method

Complete these steps to add an enclosure to the system by using the command-line interface:

1. Using the **sainfo lsservicestatus** command (on the service CLI of the new enclosure), record the WWNN of the new enclosure, as shown in Figure 5-53.

```
IBM_FlashSystem:ITSO_FS9100:superuser>sainfo lsservicestatus | grep WWNN
node_WWNN
disk_WWNN_suffix
panel_WWNN_suffix
enclosure_WWNN_1 5005076810000009
enclosure_WWNN_2 500507681000000a
node_WWNN_1_copy 5005076810000009
node_WWNN_2_copy 500507681000000a
```

Figure 5-53 Obtain WWNN using the sainfo lsservicestatus CLI command

2. Enter the **lscontrolenclosurecandidate** command to verify that the enclosure is detected on the fabric, as shown in Figure 5-54.
3. Record the serial number of the enclosure, which is needed in later steps. In this case, it is Serial Number F306954 from the **lscontrolenclosurecandidate** output.

```
IBM_FlashSystem:ITSO_FS9100:superuser>lscontrolenclosurecandidate
serial_number product_MTM machine_signature
F306954       9846-AF8    95B1-BDD6-61BE-B02C
```

Figure 5-54 Execute CLI command lscontrolenclosurecandidate

4. Enter the **lsiogrp** command to determine the next I/O group where the enclosure will be added, as shown in Figure 5-55. In this example, `io_grp1` is the next available I/O group.

```
IBM_FlashSystem:ITSO_FS9100:superuser>IBM_FlashSystem:ITSO_FS9100:superuser>lsiogrp
id name            node_count vdisk_count host_count site_id site_name
0  io_grp0         2          5           3
1  io_grp1         0          0           2
2  io_grp2         0          0           2
3  io_grp3         0          0           2
4  recovery_io_grp 0          0           0
```

Figure 5-55 Execute CLI command lsiogrp

5. Record the name or ID of the first I/O group that has a node count of zero. You will need the ID for the next step.
6. Enter the **addcontrolenclosure -iogrp iogrp_name | iogrp_id -sernum enclosureserialnumber** command to add the enclosure to the system where *iogrp_name | iogrp_id* is the name or ID of the I/O group and *enclosureserialnumber* is the serial number of the enclosure. An example is shown in Figure 5-56.

```
IBM_FlashSystem:ITSO_FS9100:superuser>addcontrolenclosure -iogrp 1 -sernum F306954
Enclosure containing Node, id [11], successfully added
```

Figure 5-56 Run the addcontrolenclousure CLI command

7. Enter the **`lsnodecanister`** command to verify that the node canisters in the enclosure are online, as shown in Figure 5-57. Repeat the command until the status changes from `adding` to `online`.

```
IBM_FlashSystem:ITSO_FS9100:superuser>lsnodecanister
id name  UPS_serial_number WWNN             status IO_group_id IO_group_name config_node UPS_unique_id hardware iscsi_name
iscsi_alias panel_name enclosure_id canister_id enclosure_serial_number site_id site_name
1  node1                   5005076810000009 online 0           io_grp0       yes                       AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node1             01-1       1            1          F313150
2  node2                   500507681000000A online 0           io_grp0       no                        AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node2             01-2       1            2          F313150
11 node3                   500507681000A5C8 adding 1           io_grp1       no                        AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node3             F306954-1               1
12 node4                   5005076810005488 adding 1           io_grp1       no                        AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node4

IBM_FlashSystem:ITSO_FS9100:superuser>lsnodecanister
id name  UPS_serial_number WWNN             status IO_group_id IO_group_name config_node UPS_unique_id hardware iscsi_name
iscsi_alias panel_name enclosure_id canister_id enclosure_serial_number site_id site_name
1  node1                   5005076810000009 online 0           io_grp0       yes                       AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node1             01-1       1            1          F313150
2  node2                   500507681000000A online 0           io_grp0       no                        AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node2             01-2       1            2          F313150
11 node3                   500507681000A5C8 online 1           io_grp1       no                        AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node3             02-1       2            1          F306954
12 node4                   5005076810005488 online 1           io_grp1       no                        AF8      iqn.1986-
03.com.ibm:2145.itsofs9100.node4             02-2       2            2          F306954
```

Figure 5-57 Output from the lsnodecanister CLI command

> **Note:** **`IBM_FlashSystem:ITSO_FS9100:superuser>chenclosure -managed yes 2`**

`chenclosure -managed yes <enclosure_id>`

`-managed yes`

Changes the enclosure to a managed enclosure.

`enclosure_id`

Specifies the enclosure that you want to modify.

5.6 Adding an IBM FlashSystem 9100 Expansion Enclosure

There are two types of available SAS expansion enclosures:

- FlashSystem 9100 SFF Model AFF
- FlashSystem 9100 LFF Model A9F

A single FlashSystem 9100 can support up to 20 AFF expansion enclosures, or it can support up to 8 A9F expansion enclosures:

- The following Expansion Enclosures and drives are supported using the SAS adapter for attachment of the All-Flash expansions, models AFF and A9F:
  - AFF Drive Feature codes and drive capacity types:
    - (AH2A): 1.92 TB 12 Gb SAS 2.5 Inch Flash Drive
    - (AH2B): 3.84 TB 12 Gb SAS 2.5 Inch Flash Drive
    - (AH2C): 7.68 TB 12 Gb SAS 2.5 Inch Flash Drive
    - (AH2D): 15.36 TB 12 Gb SAS 2.5 Inch Flash Drive
  - A9F Drive Feature codes and drive capacity types:
    - (AH7J): 1.92 TB 12 Gb SAS 3.5 Inch Flash Drive
    - (AH7K): 3.84 TB 12 Gb SAS 3.5 Inch Flash Drive
    - (AH7L): 7.68 TB 12 Gb SAS 3.5 Inch Flash Drive
    - (AH7M): 15.36 TB 12 Gb SAS 3.5 Inch Flash Drive

- AFF: 2U with 24 SFF drives slots: Attachment for up to 20 AFF enclosures to each control enclosure (480 drives)
- A9F: 5U with 92 LFF drive slots: Attachment for up to 8 A9F enclosures to each control enclosure (736 drives)
- Intermix of AFF/A9F expansions supported.
- SAS drives can be TRAID1, DRAID5 or DRAID6, with drives within those arrays being the same size.

Note: Intermix with Storwize V7000 expansions is not permitted.

SAS Adapter

The (Feature Code AHBA) SAS Expansion Enclosure Attach Card (Pair) provides two four-port 12 Gb SAS Expansion Enclosure attachment cards. This feature is used to attach up to twenty Expansion Enclosures to a FlashSystem 9100 Control Enclosure.

Note: Only two of the four SAS ports on the SAS Expansion Enclosure attachment card are used for Expansion Enclosure attachment. The other two SAS ports are inactive.

5.6.1 FlashSystem 9100 SFF Model AFF

Model AFF Expansion Enclosure includes the following components:

- Two expansion canisters.
- 12 Gb SAS ports for control enclosure and expansion enclosure attachment.
- Twenty-four slots for 2.5-inch SAS SSD drives.
- 2U, 19-inch rack mount enclosure with AC power supplies.
- 24 2.5-inch drives (SSDs).
- 2 Storage Bridge Bay (SBB)-compliant enclosure services manager (ESM) canisters.
- Two fan assemblies, which mount between the drive midplane and the Node Canisters. Each fan module is removable when the Node Canister is removed.
- Two Power supplies.
- RS232 port on the back panel (3.5 mm stereo jack), which is used for configuration during manufacturing.

The front of an Expansion Enclosure is shown in Figure 5-58.

Figure 5-58 Front of IBM 9100 SFF Model AFF Expansion Enclosure

Figure 5-59 shows a rear view of an AFF expansion enclosure.

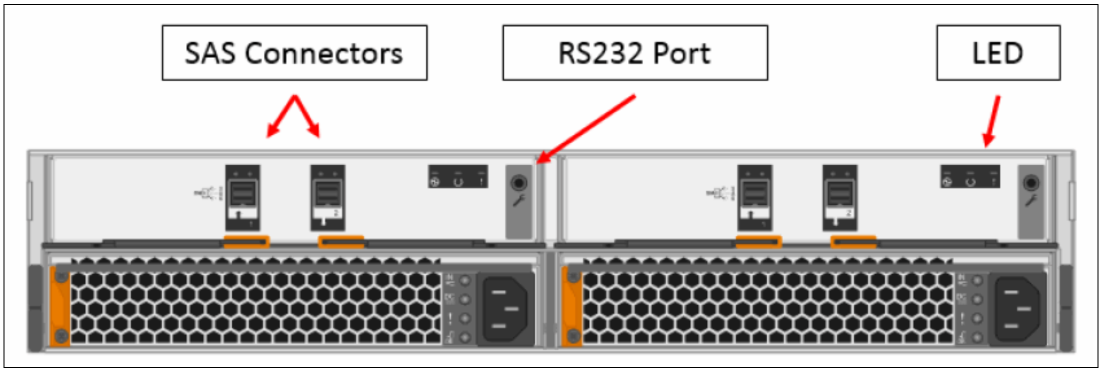


Figure 5-59 Rear of IBM 9100 SFF Model AFF expansion enclosure

5.6.2 FlashSystem 9100 LFF Model A9F

The Model A9F expansion enclosures are SAS SSD disk expansion enclosures that are 5U rack-mounted. Each chassis features two expansion canisters, two power supplies, two expander modules, and a total of four fan modules.

Each A9F expansion drawer can hold up to 92 drives that are positioned in four rows of 14, and an additional three rows of 12 mounted drives assemblies. There are two Secondary Expander Modules (SEM) that are centrally located in the chassis. One SEM addresses 54 drive ports, and the other addresses 38 drive ports. The drive slots are numbered 1 - 14, starting from the left rear slot and working from left to right, back to front.

Each canister in the A9F enclosure chassis features two SAS ports numbered 1 and 2. The use of SAS port 1 is mandatory because the expansion enclosure must be attached to an IBM FlashSystem 9100 node or another expansion enclosure. SAS connector 2 is optional, because it is used to attach to more expansion enclosures.

Each IBM FlashSystem 9100 can support up to eight A9F enclosure drawers per SAS chain.

Figure 5-60 shows an A9F expansion drawer.

Figure 5-60 IBM FlashSystem 9100 A9F enclosure

5.6.3 SAS chain limitations

When attaching expansion enclosures to the control enclosure, you are not limited by type of the enclosure (as long as it meets all generation level restrictions). The only limitation for each SAS chain is its chain weight. Each type of enclosure has defined its own chain weight:

- AFF enclosures have a chain weight of 1.
- A9F enclosures have a chain weight of 2.5.

The maximum chain weight is 10.

For example, you can combine seven AFF and one A9F expansions (7 x 1 + 1 x 2.5 = 9.5 chain weight).

5.6.4 Connecting the SAS cables to the expansion enclosures

If you have installed expansion enclosures, you must connect them to a FlashSystem 9100 control enclosure.

Procedure

To install the SAS cables, complete the following steps.

1. Using the supplied SAS cables, connect the control enclosure to the expansion enclosure at rack position 1, as shown in Figure 5-61 on page 154:
   a. Connect SAS port 1 of the left node canister in the control enclosure to SAS port 1 of the left expansion canister in the first expansion enclosure.
   b. Connect SAS port 1 of the right node canister in the control enclosure to SAS port 1 of the right expansion canister in the first expansion enclosure.

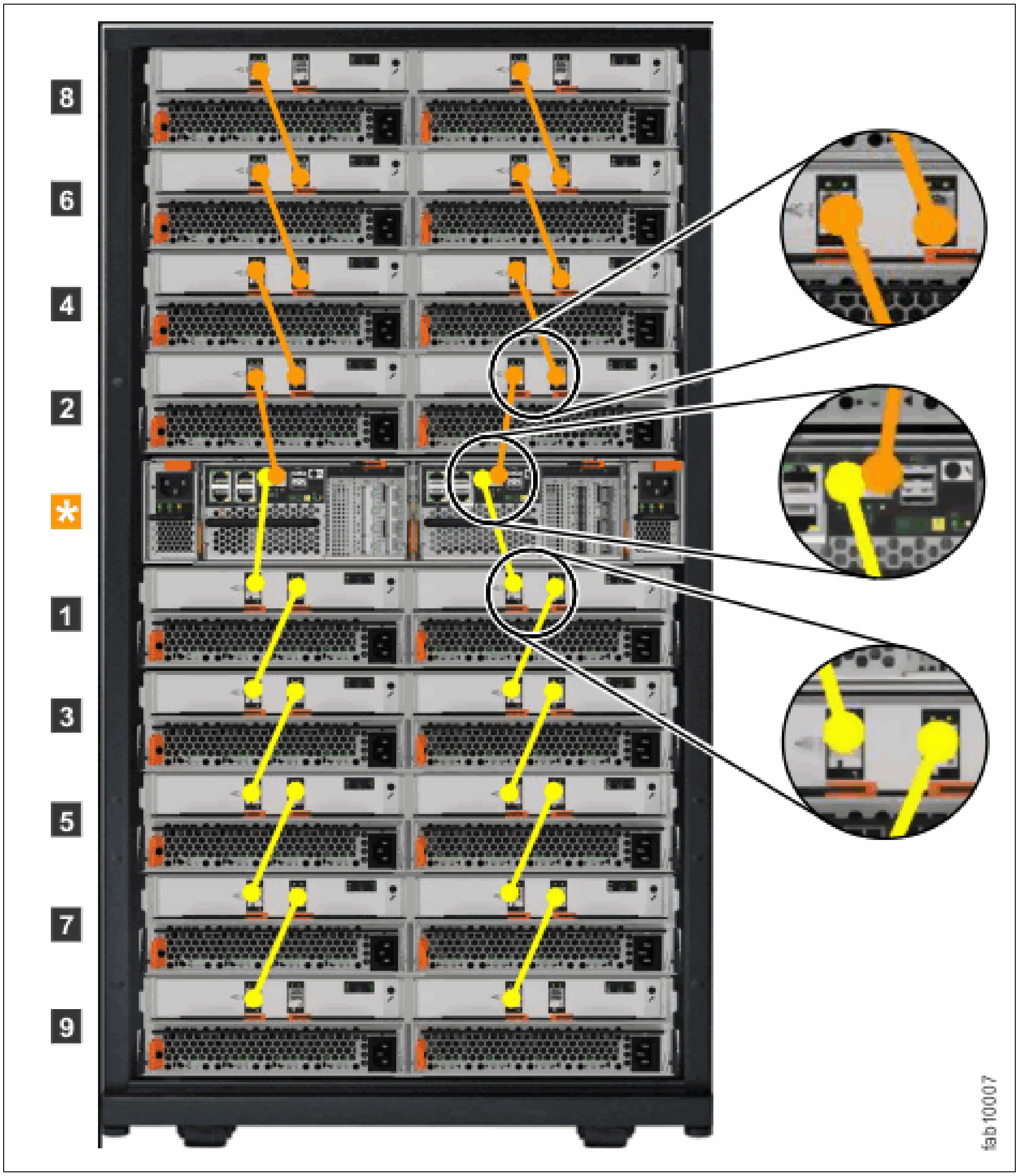


Figure 5-61   Connecting the SAS cables

2. To add a second expansion enclosure chain to the control enclosure, use the supplied SAS cables to connect the control enclosure to the expansion enclosure at rack position 2. See Figure 5-61 for an example.
   a. Connect SAS port 2 of the left node canister in the control enclosure to SAS port 1 of the left expansion canister in the second expansion enclosure.
   b. Connect SAS port 2 of the right node canister in the control enclosure to SAS port 1 of the right expansion canister in the second expansion enclosure.
3. If additional expansion enclosures are installed, connect each one to the previous expansion enclosure in a chain; use two Mini SAS HD to Mini SAS HD cables, as shown in Figure 5-61.

Note: A control enclosure can support up to 20 expansion enclosures (10 above the control enclosure and 10 below the control enclosure).

4. If additional control enclosures are installed, repeat this cabling procedure on each control enclosure and its expansion enclosures.

5.7 Adding external storage systems

IBM Spectrum Virtualize supports external storage controllers attached through iSCSI and through Fibre Channel.

The back-end storage subsystem configuration must be planned for all storage controllers that are attached to the FlashSystem 9100.

For more information about supported storage subsystems, see:

- IBM Support Information for FlashSystem 9100 family: `https://ibm.biz/BdYpAV`
- IBM System Storage Interoperation Center (SSIC): `https://ibm.biz/BdjyuP`

Apply the following general guidelines for back-end storage subsystem configuration planning:

- In the SAN, storage controllers that are used by the FlashSystem 9100 clustered system must be connected through SAN switches. Direct connection between the FlashSystem 9100 and the storage controller is not supported.
- Enhanced Stretched Cluster configurations have additional requirements and configuration guidelines. For more information about performance and preferred practices for the FlashSystem 9100, see *IBM System Storage SAN Volume Controller and Storwize V7000 Best Practices and Performance Guidelines*, SG24-7521.

If your external storage system does not support the FlashSystem 9100 round-robin algorithm, ensure that the number of MDisks per storage pool is a multiple of the number of storage ports that are available. This approach ensures sufficient bandwidth for the storage controller, and an even balance across storage controller ports.

Generally observe these rules:

- Disk drives: Exercise caution with the use of large hard disk drives so that you do not have too few spindles to handle the load.
- Array sizes:
  - FlashSystem 9100 will not queue more than 60 I/O operations per MDisk. Therefore, make sure that the MDisks presented to FlashSystem 9100 can handle about this many requests, which corresponds to about 8 HDDs. If your array can handle a higher load, split it in to several LUNs of equal size to better match back-end storage capabilities with the load that FlashSystem 9100 can generate.

    See *IBM System Storage SAN Volume Controller and Storwize V7000 Best Practices and Performance Guidelines*, SG24-7521 for an in-depth discussion of back-end storage LUN presentation to FlashSystem 9100.
  - Since V7.3, the system uses autobalancing to restripe volume extents evenly across all MDisks in the storage pools.

– The cluster can be connected to a maximum of 1024 WWNNs. The general customs include the following practices:
  - EMC DMX/SYMM, all HDS, and SUN/HP HDS clones use one WWNN per port. Each port appears as a separate controller to the FlashSystem 9100.
  - IBM, EMC CLARiiON, and HP use one WWNN per subsystem. Each port appears as a part of a subsystem with multiple ports, up to a maximum of 16 ports (WWPNs) per WWNN.

However, if you plan a configuration that might be limited by the WWNN maximum, verify the WWNN versus WWPN policy with the external storage vendor.

Note: Externally virtualized storage uses a separate capacity-based license. A tiered capacity-based license varies depending on the drive technology that's being virtualized (this is known as *Storage Capacity Unit* (SCU) based licensing).

IBM FlashSystem 9100 Models AF7 and AF8 support external virtualization. Use of the external virtualization capability is entitled through the acquisition of IBM Spectrum Virtualize Software for SAN Volume Controller (SW PID 5641-VC8 in AAS, and SW PID 5725-M19 in IBM Passport Advantage®).

External storage controllers with both types of attachment can be managed through the External Storage pane. To access the External Storage pane, browse to **Pools** → **External Storage**, as shown in Figure 5-62.

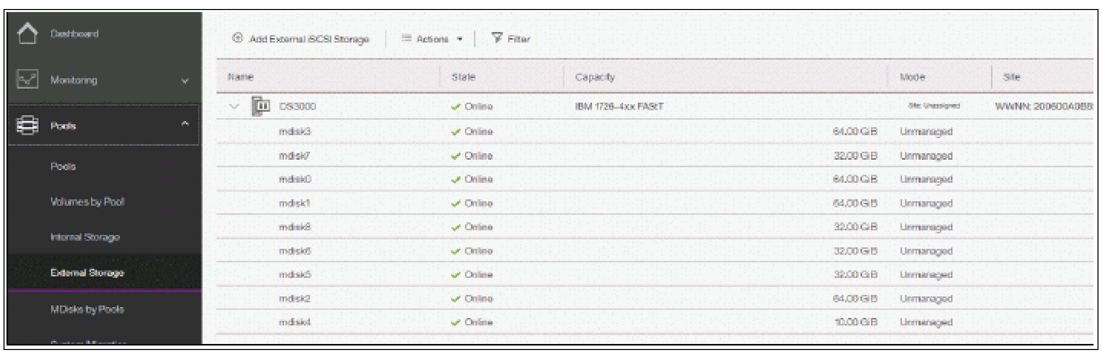


Figure 5-62 External Storage pane

The pane lists the external controllers that are connected to the FlashSystem 9100 system and all the external MDisks detected by the system. The MDisks are organized by the external storage system that presents them. You can toggle the sign to the left of the controller icon to either show or hide the MDisks associated with the controller.

Note: A controller connected through Fibre Channel is detected automatically by the system, providing that the cabling, the zoning, and the system layer are configured correctly. A controller connected through iSCSI must be added to the system manually.

If you have configured logical unit names on your external storage systems, it is not possible for the system to determine this name because it is local to the external storage system. However, you can use the external storage system WWNNs and the LU number to identify each device.

5.7.1 Fibre Channel external storage controllers

A controller connected through Fibre Channel is detected automatically by the system, providing the cabling, the zoning, and the system layer are configured correctly.

If the external controller is not detected, ensure that the FlashSystem 9100 is cabled and zoned into the same storage area network (SAN) as the external storage system. If you are using Fibre Channel, connect the Fibre Channel cables to the Fibre Channel ports of the canisters in your system, and then to the Fibre Channel network.

> **Attention:** If the external controller is a Storwize system, the FlashSystem 9100 must be configured at the replication layer, and the external controller must be configured at the storage layer. The default layer for a Storwize system is storage. Make sure that the layers are correct before zoning the two systems together. Changing the system layer is not available in the GUI. You need to use the command-line interface (CLI).
>
> Ensure that the layer of both systems is correct by entering the following command:
>
> **`svcinfo lssystem`**
>
> If needed, change the layer of the FlashSystem 9100 to `replication` by entering the following command:
>
> **`chsystem -layer replication`**
>
> If needed, change the layer of the Storwize controller to `storage` by entering the following command:
>
> **`chsystem -layer storage`**

5.7.2 iSCSI external storage controllers

Unlike Fibre Channel connections, you must manually configure iSCSI connections between the IBM FlashSystem 9100 and the external storage controller. Until then, the controller is not listed in the External Storage pane.

Before adding an iSCSI-attached controller, ensure that the following prerequisites are fulfilled:

- IBM FlashSystem 9100 and the external storage system are connected through one or more Ethernet switches. Symmetric ports on all nodes of the FlashSystem 9100 are connected to the same switch and configured on the same subnet. Optionally, you can use a virtual local area network (VLAN) to define network traffic for the system ports.
- Direct attachment between this system and the external controller is not supported. To avoid a single point of failure, use a dual switch configuration. For full redundancy, a minimum of two paths between each initiator node and target node must be configured with each path on a separate switch.

Figure 5-63 on page 158 shows an example of a fully redundant iSCSI connection between IBM FlashSystem 9100 and Storwize systems. In this example, the FlashSystem 9100 is composed of two I/O groups. Each node has a maximum of four initiator ports with two ports configured, through two switches, to the target ports on the other Storwize system.

The first ports (orange) on each initiator and target nodes are connected through Ethernet switch 1. The second ports (blue) on each initiator and target nodes are connected through Ethernet switch 2. Each target node on the storage system has one iSCSI qualified name (IQN) that represents all the LUs on that node.

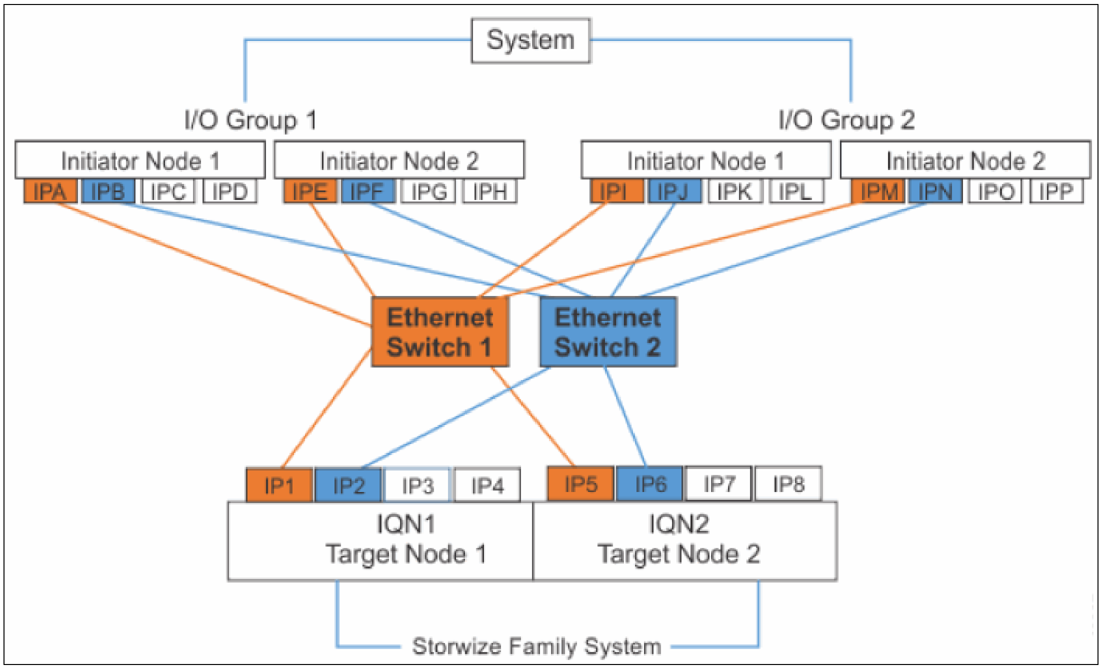


Figure 5-63 Fully redundant iSCSI connection between FlashSystem 9100 and Storwize system

The ports used for iSCSI attachment are enabled for external storage connections. By default, Ethernet ports are disabled for external storage connections. Verify your port settings:

1. Navigate to **Settings** → **Network** and select **Ethernet Ports**, as shown in Figure 5-64.

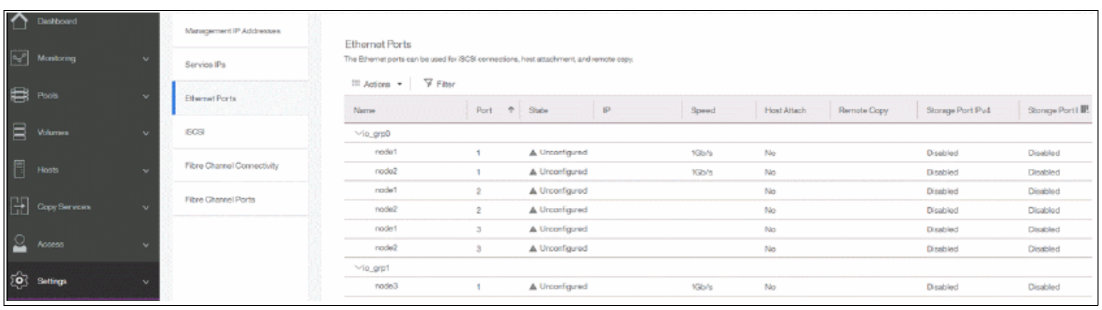


Figure 5-64 Ethernet ports settings

2. To enable the port for external storage connections, select the port, click **Actions** and select **Modify Storage Ports**, as shown in Figure 5-65.

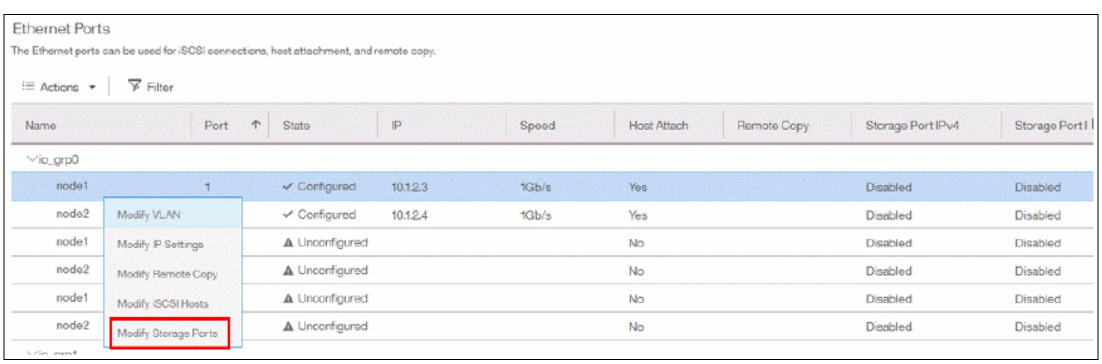


Figure 5-65 Modifying Ethernet port settings

3. Set the port as **Enabled** for either IPv4 or IPv6, depending on the protocol version configured for the connection, as shown in Figure 5-66.

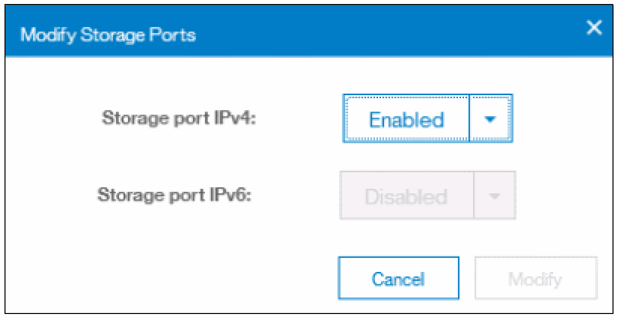


Figure 5-66 Enabling a Storage port

4. When all prerequisites are fulfilled, you are ready to add the iSCSI controller. To do so, navigate to **Pools** → **External Storage** and click **Add External iSCSI Storage**, as shown in Figure 5-67.

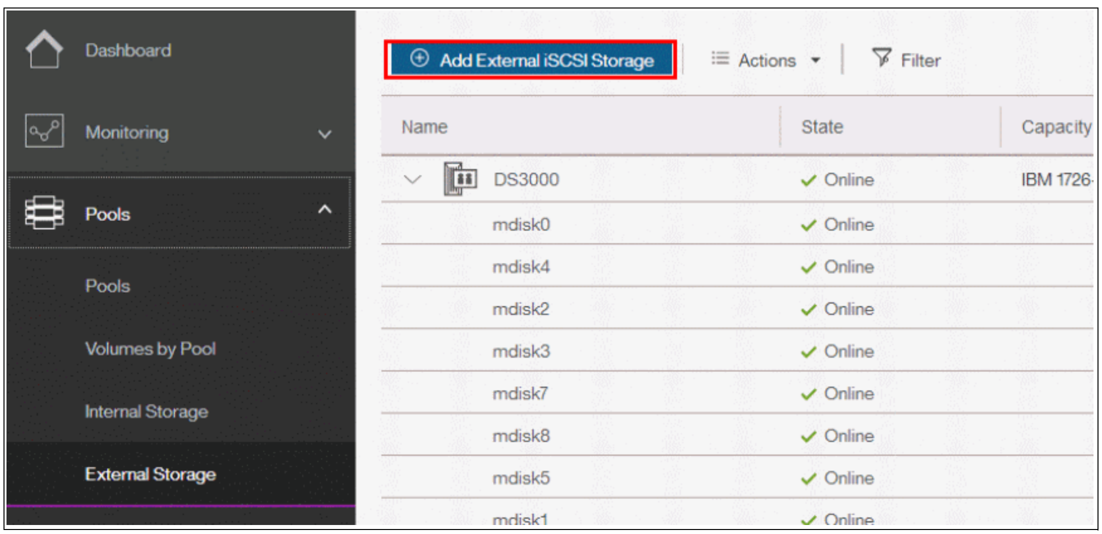


Figure 5-67 Adding external iSCSI storage

5. Select **Convert the system to the replication layer** and click **Next**, as shown in Figure 5-68.

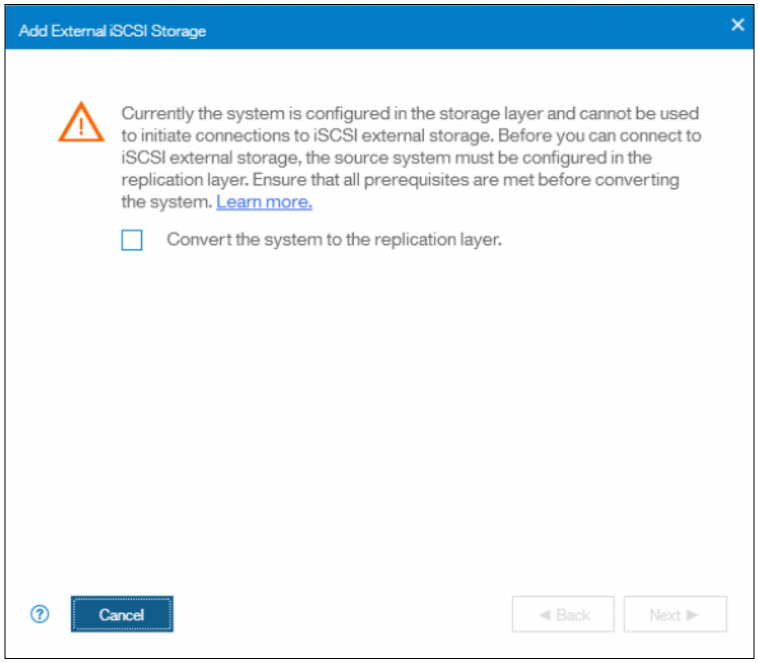


Figure 5-68 Converting the system layer to replication to add iSCSI external storage

6. Select **Convert the system to the replication layer** and click **Next**.
7. Select the type of external storage. For this example, the **IBM Storwize** type is chosen. Click **Next**, as shown in Figure 5-69.

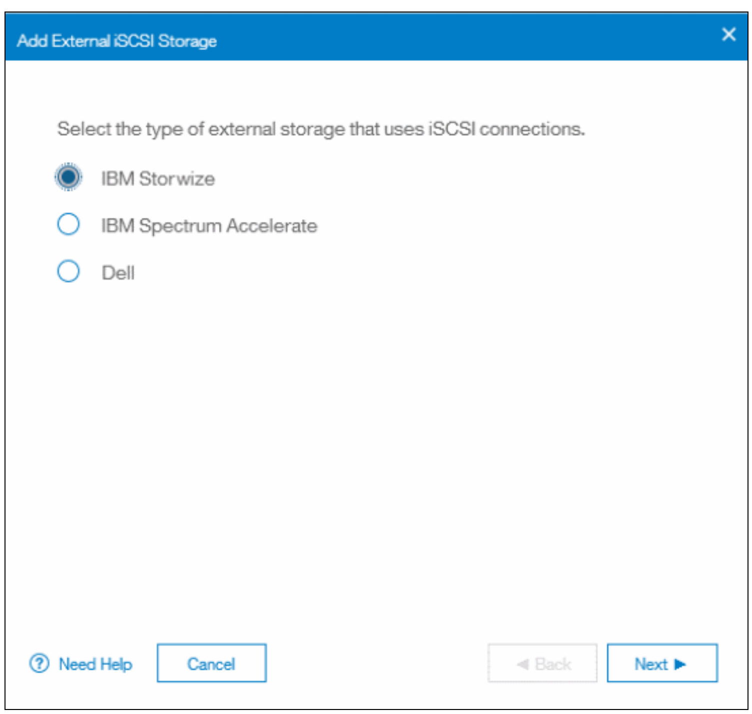


Figure 5-69 Adding an external iSCSI controller: Controller type

8. Enter the iSCSI connection details, as shown in Figure 5-70.

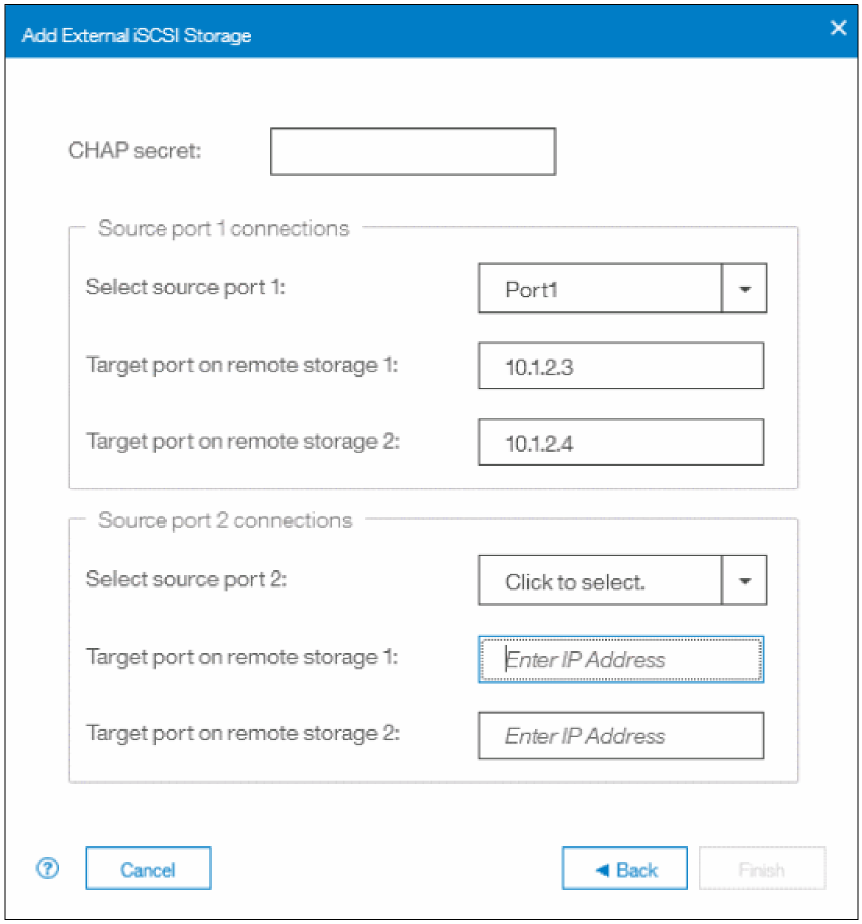


Figure 5-70 Adding an external iSCSI controller: Connection details

9. Complete the following fields as described:
   a. CHAP secret: If the Challenge Handshake Authentication Protocol (CHAP) is used to secure iSCSI connections on the system, enter the current CHAP secret. This field is not required if you do not use CHAP.
   b. Source port 1 connections:
      - Select source port 1: Select one of the ports to be used as initiator for the iSCSI connection between the node and the external storage system.
      - Target port on remote storage 1: Enter the IP address for one of the ports on the external storage system targeted by this source port.
      - Target port on remote storage 2: Enter the IP address for the other port on the external storage system targeted by this source port.
   c. Source port 2 connections:
      - Select source port 2: Select the other port to be used as initiator for the iSCSI connection between the node and the external storage system.
      - Target port on remote storage 1: Enter the IP address for one of the ports on the external storage system targeted by this source port.
      - Target port on remote storage 2: Enter the IP address for the other port on the external storage system targeted by this source port.

The fields available vary depending on the configuration of your system and external controller type. However, the meaning of each field is always kept. The following fields can also be available:

- Site: Enter the site associated with the external storage system. This field is shown only for configurations using HyperSwap.
- User name: Enter the user name associated with this connection. If the target storage system uses CHAP to authenticate connections, you must enter a user name. If you specify a user name, you must specify a CHAP secret. This field is not required if you do not use CHAP. This field is shown only for IBM Spectrum Accelerate™ and Dell EqualLogic controllers.

10. Click **Finish**. The system attempts to discover the target ports and establish iSCSI sessions between source and target. If the attempt is successful, the controller is added. Otherwise, the action fails.

5.7.3 Actions on external storage controllers

A number of actions can be performed on external storage controllers. Some actions are available for external iSCSI controllers only.

To select any action, right-click the controller, as shown in Figure 5-71. Alternatively, select the controller and click **Actions**.

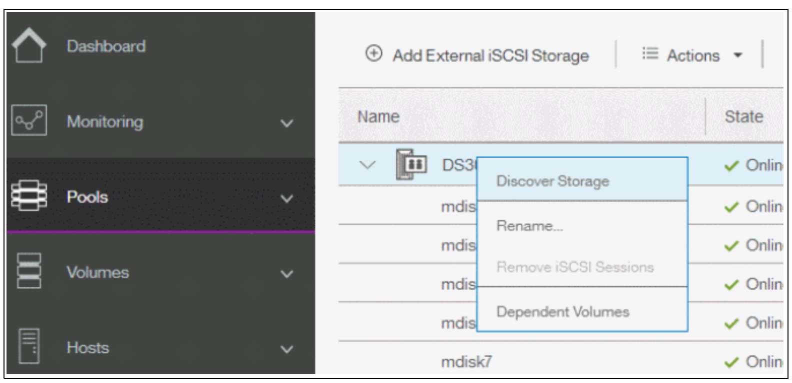


Figure 5-71 Actions on external storage

Discover storage

When you create or remove LUs on an external storage system, the change is not always automatically detected. If that is the case, select **Discover Storage** for the system to rescan the Fibre Channel or iSCSI network. The rescan process discovers any new MDisks that were added to the system and rebalances MDisk access across the available ports. It also detects any loss of availability of the controller ports.

Rename

To modify the name of an external controller, select **Rename**, enter the new name, and click **Rename**, as shown in Figure 5-72.

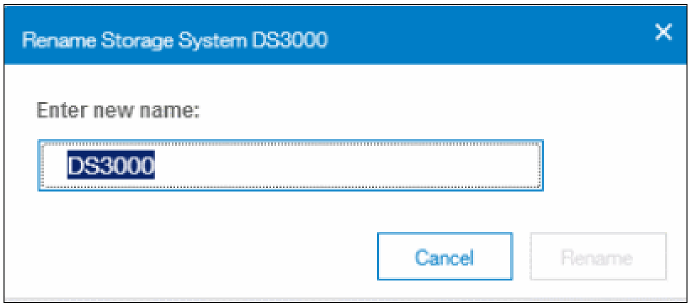


Figure 5-72 Renaming an external storage controller

Naming rules: When you choose a name for a controller, the following rules apply:

- Names must begin with a letter.
- The first character cannot be numeric.
- The name can be a maximum of 63 characters.
- Valid characters are uppercase letters (A - Z), lowercase letters (a - z), digits (0 - 9), underscore (_), period (.), hyphen (-), and space.
- Names must not begin or end with a space.
- Object names must be unique within the object type. For example, you can have a volume and an MDisk both named `ABC`, but you cannot have two volumes named `ABC`.
- The default object name is valid (object prefix with an integer).
- Objects can be renamed to their current names.

Remove iSCSI sessions

This action is available only for external controllers attached with iSCSI. Right-click the session and select **Remove** to remove the iSCSI session established between the source and target port.

Modify site

This action is available only for systems that use HyperSwap. Select **Modify Site** to modify the site with which the external controller is associated, as shown in Figure 5-73.

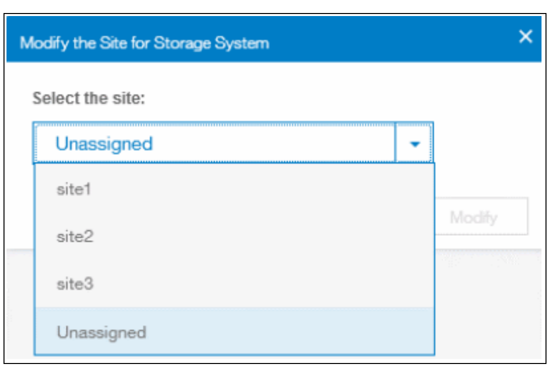


Figure 5-73 Modifying the site of an external controller

5.8 Adding FlashSystem 9100 to a Storwize V7000 system

If you have an existing Storwize V7000 system, you can add a FlashSystem 9100 control enclosure to the system. When the FlashSystem 9100 is added, the new system configuration adopts the attributes and supported features of the FlashSystem 9100 system, such as IBM FlashCore Module support.

You must ensure that the Storwize V7000 system has licenses for all licensed functions. Additionally, if the Storwize V7000 system manages externally virtualized storage, then the licenses for this capacity must be converted to storage capacity units (SCU) or terabyte licenses. Your sales team can help you with this process.

In addition to these licenses, both systems support encryption through an optional license. The support is the same, but if the Storwize V7000 system has an encryption license, the FlashSystem 9100 control enclosure must also have a license before it is added to the Storwize V7000 system. To activate this license on the FlashSystem 9100 control enclosure, see 4.7, “Licensing and features” on page 107 and 4.7.4, “Encryption” on page 108.

Note: The existing Storwize V7000 system must include only models 2076-524 and 2076-624 control enclosures with the same level code as the FlashSystem 9100 control enclosure, which is V8.2.0.0 or later. The minimum required level to upgrade to V8.2.0 is V7.8.1.

There must be *fewer than four control enclosures* in the existing system (the maximum for both Storwize V7000 and FlashSystem 9100 systems is four control enclosures).

5.8.1 Clustering rules

The following list describes the clustering rules:

- Supported cluster with Storwize V7000 and FlashSystem 9100
- Both systems must be at V8.2.0 or higher
- To cluster, the Storwize V7000 must have an all-inclusive license
- Migration must be done through additional I/O Groups
- Default layer is storage but replication layer is supported

This section describes the ways to add a FlashSystem 9100 control enclosure to an existing Storwize V7000 system. If your Storwize V7000 system is currently licensed for compression, you must change the compression value to 0 before adding the FlashSystem 9100 control enclosure. You can change this value using either the GUI or the CLI.

On the Storwize V7000 system, you can change the setting in the V7000 management GUI by completing the following steps:

1. Select **Settings** > **System** > **Licensed Functions**.
2. On the Licensed Functions page, change the current setting for **Compression** to `0`.
3. Click **Apply Changes**.

   Set the Real-time Compression value to `0` on the Storwize V7000 system, as shown in Figure 5-74 on page 165.

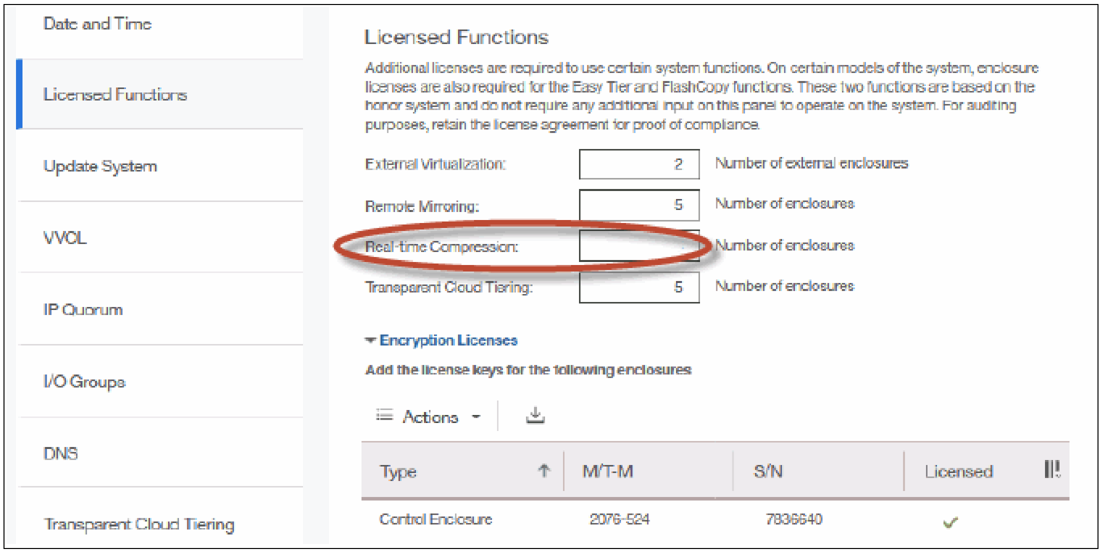


Figure 5-74 Set Real-time Compression value to 0

On the command-line, you can also issue the `chlicense -compression 0` command.

Ensure that the FlashSystem 9100 control enclosure is zoned correctly and is part of the same storage area network (SAN) as the Storwize V7000 system. The IBM SSR installs the FlashSystem 9100 and completes cabling; however, you must complete all SAN configuration prior to installation and update the network planning sheets:

1. In the Storwize V7000 management GUI, select **Monitoring** > **System**. On the System -- Overview page, select **Add Enclosure**.
2. When a new enclosure is cabled correctly to the system, the **Add Enclosures** action automatically displays on the System -- Overview page. If this action does not appear, review the installation instructions to ensure the new enclosure is cabled correctly.
3. You can also add a new enclosure by selecting **Add Enclosure** from the **System Actions** menu.
4. Complete the instructions in the **Add Enclosures** wizard until the FlashSystem 9100 control enclosure is added to the system.

After the FlashSystem 9100 control enclosure is added to the Storwize V7000 system, several post-installation tasks may be necessary to fix potential configuration issues.

Verify that the system attributes have updated the status of the system as a FlashSystem 9100 system by completing these steps:

1. In the Storwize V7000 management GUI, select the Help icon and select **About FlashSystem 9100**.
2. Verify the following attribute to ensure that the system is now identified as an IBM FlashSystem 9100 system:
   – Product name: FlashSystem 9100
   – Other system attributes also change, such as Call Home prefix and support site URLs, when the FlashSystem 9100 control enclosure is added to the Storwize V7000 system. These changes are expected, but might seem confusing unless you are aware of them.

   Any system that has FlashSystem 9100 control enclosures is considered to be a FlashSystem 9100 system.

3. If you did not have any external virtualization licenses on the Storwize V7000 system, then no additional updates to license settings are necessary.
4. If you did have external virtualization licenses on the Storwize V7000 system and contacted your sales team for the setting that converted enclosure-based licenses to capacity-based licenses, use those values to update the license settings on the FlashSystem 9100 system. In the Storwize V7000 management GUI, select **Settings** > **System** > **Licensed Functions** or use the `chlicense` command.

6

Installation and configuration

This chapter describes the installation and initial configuration of the FlashSystem 9100 system.

This chapter includes the following topics:

- Installation and configuration overview
- Installing the hardware
- System initialization
- Service setup
- Initial customer setup

6.1 Installation and configuration overview

The following tasks are completed by the IBM Service Support Representative (SSR):

1. Unpacks and installs the 9846/9848-AF7 or 9846/9848-AF8 control enclosure in the rack.
2. Unpacks and installs optional 9846/9848-A9F or 9846/9848-AFF expansion enclosures in the rack.
3. Connects optional expansion enclosures to the control enclosure.
4. Connects ethernet cables to the control enclosure.
5. Connects fibre optic cables to the control enclosure.
6. Powers on the system.
7. Initializes the system.
8. Performs a service setup of the system.

After the IBM SSR completes the above tasks, the customer completes the system setup using the management GUI.

6.2 Installing the hardware

Important: The information in this section is intended only for IBM authorized service providers. Customers need to consult the terms of their warranty to determine the extent to which they should attempt any IBM FlashSystem hardware installation.

The installation and configuration of the FlashSystem 9100 system is performed by an IBM SSR using the information in the system planning worksheets provided by the customer.

6.2.1 Prerequisites

The following prerequisites must be fulfilled *before* the IBM SSR installs the hardware and initializes the system:

1. The customer has completed the system planning worksheets. The system planning worksheets are in the IBM KnowledgeCenter.
2. Physical site specifications must be met. This includes rack space, power, and environmental conditions. See Chapter 4, “Planning” on page 63 for additional details.
3. Ethernet cables that are to be connected to the control enclosure node canister management ports are available.
4. Fibre optic cables that are to be connected to the control enclosure node canister fibre channel ports are available.

6.2.2 Required tools

The following tools are required:

- Laptop
- Ethernet cable to connect laptop ethernet port to node canister technician port
- Cross-head (Phillips) screw driver
- Flat-head screw driver

6.2.3 Installing the hardware

The FlashSystem 9100 system consists of a control enclosure and optional SAS expansion enclosures. Perform the following steps to install, connect, and power up the system:

1. Starting with the enclosure in the lowest location in the rack, install each enclosure using the appropriate instructions, as shown in Table 6-1.

Table 6-1 FlashSystem 9100 enclosure installation instructions

Enclosure	Instructions
Control enclosure model A7F/A8F	"Installing the FlashSystem 9100 control enclosure" on page 169
SAS expansion enclosure model A9F (52U)	"Installing the model A9F expansion enclosure" on page 173
SAS expansion enclosure model AFF (2U)	"Installing the Model AFF expansion enclosure" on page 187

2. After all the enclosures in the system have been installed, continue with the system installation at 6.2.4, "Connecting the FlashSystem 9100 components".

Installing the FlashSystem 9100 control enclosure

Following are the steps to install the FlashSystem 9100 enclosure.

Unpacking the control enclosure

CAUTION:

Lifting the FlashSystem 9100 control enclosure requires three persons or suitable lifting equipment. If necessary, the control enclosure can be dismantled to reduce the weight of the control enclosure.

1. Open the top of the shipping carton and remove the rail kit box and the power cables.
2. Remove the packing foam and corner reinforcement pieces from the carton.
3. Carefully cut the four corners of the carton from top to bottom.
4. If three persons or suitable lifting equipment are not available, continue by dismantling the control enclosure at step 5. Otherwise, continue the installation at "Installing support rails for the control enclosure" on page 170.
5. Fold the sides and the back of the carton down to uncover the rear of the control enclosure. If necessary, carefully cut along the lower fold line of the sides and remove them.
6. Carefully cut the raised section of the foam packing away from the rear of the control enclosure.
7. Carefully cut open the bag covering the rear of the control enclosure.
8. Remove the left power supply unit from the control enclosure and record the serial number on the back of the power supply unit.
9. Remove the right power supply unit from the control enclosure and record the serial number on the back of the power supply unit.
10. Remove the left power interposer from the control enclosure and record the serial number on the power interposer.

11. Remove the right power interposer from the control enclosure and record the serial number on the power interposer.
12. Remove the upper node canister from the control enclosure and record the serial number on the node canister release handle.
13. .Remove the lower node canister from the control enclosure and record the serial number on the node canister release handle.

Installing support rails for the control enclosure

Note: Refer to the system planning worksheets provided by the customer for the rack location in which to install the control enclosure.

1. Locate the two control enclosure rails.
2. Working at the front of the rack cabinet, identify the two standard rack units (2U) of space in the rack into which you want to install the support rails. See Figure 6-1.

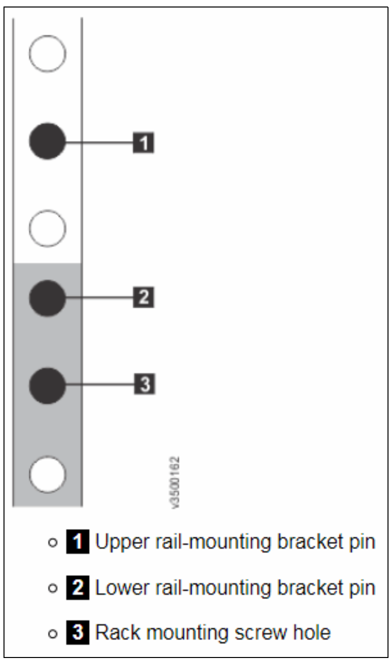


Figure 6-1 Rack hole locations in the front of the rack

3. Ensure that the appropriate bracket pins are installed in the front and rear bracket of each rail. Each rail comes with four medium pins preinstalled (two in the front bracket and two in the rear bracket). Large pins are provided separately. Use the pins that are appropriate for the mounting holes in your rack. Ensure that the appropriate bracket pins are installed in the front and rear bracket of each rail. Each rail comes with four medium pins pre installed (two in the front bracket and two in the rear bracket). Large pins are provided separately.

Use the pins that are appropriate for the mounting holes in your rack. See Table 6-2.

Table 6-2 Selecting bracket pins for the rack

Mounting Holes	Bracket Pins
Round, unthreaded	Use the pre installed medium pins.
Square	Unscrew the medium pins and replace with the large pins that are supplied with the rails.

4. At each end of the rail, grasp the tab 1 and pull firmly to open the hinge bracket. See Figure 6-2.

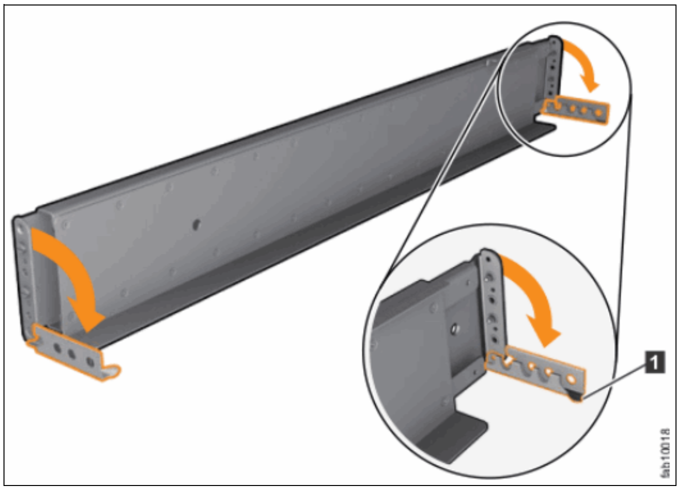


Figure 6-2 Opening the rail hinge brackets

5. Align the holes in the rail bracket with the holes on the front and rear rack cabinet flanges. Ensure that the rails are aligned on the inside of the rack cabinet.
6. On the rear of the rail, press the two bracket pins into the holes in the rack flanges.
7. Close the rear hinge bracket 4 to secure the rail to the rack cabinet flange. See Figure 6-3.

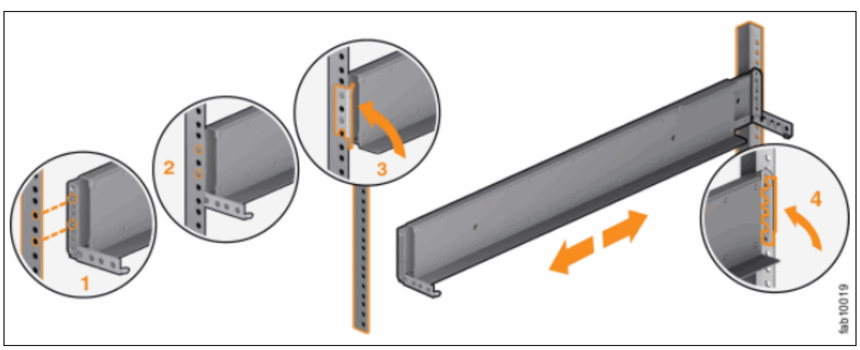


Figure 6-3 Closing the rail hinge brackets

8. On the front of the rail, press the two bracket pins into the holes in the rack flanges.
9. Close the front hinge bracket 3 to secure the rail to the rack cabinet flange. See Figure 6-3.
10. Secure the rear of the rail to the rear rack flange with two black M5 screws.
11. Repeat step 4 on page 171 through step 10 to install the opposite support rail in the rack.

Installing the control enclosure in the rack

1. Remove the left and right end caps from the control enclosure by grasping the handle and pulling the bottom of the end cap free, then clearing the tab on the top of the enclosure. See Figure 6-4.

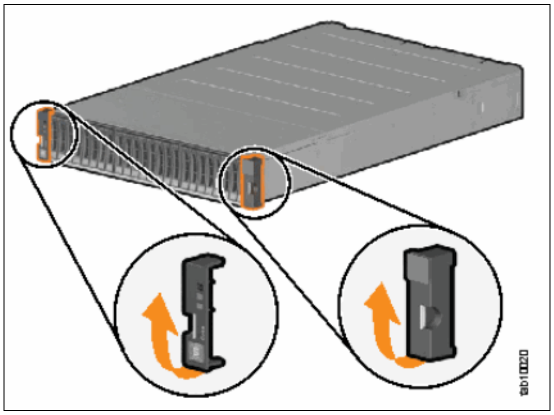


Figure 6-4 Removing the control enclosure end caps

2. Lift the control enclosure from the shipping carton and align the control enclosure with the front of the rack cabinet and the rails.
3. Slide the control enclosure into the rack until it is fully inserted. See Figure 6-5.

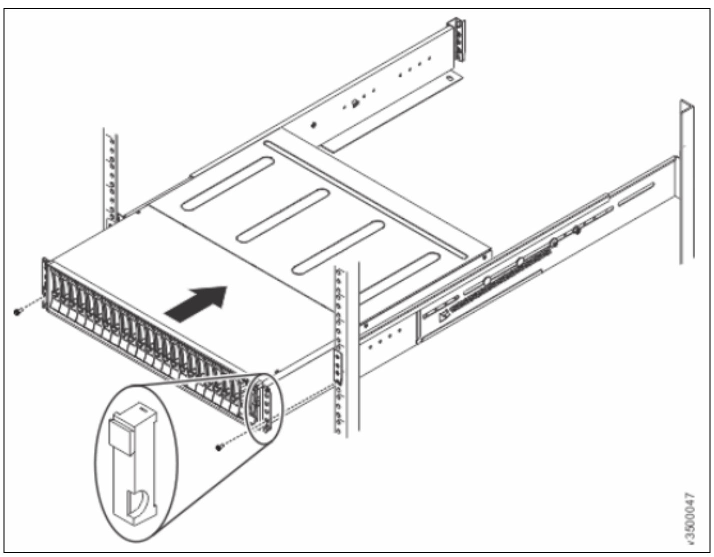


Figure 6-5 Inserting the control enclosure in the rack

4. Secure the enclosure to the front of the rack. Some enclosures are secured by one silver captive screw and one black M5 screw on each flange. In this case, align the enclosure, fasten the two captive screws, then fasten the two M5 screws. See Figure 6-6.

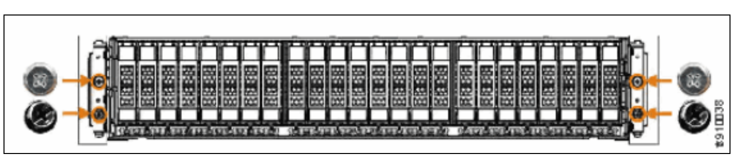


Figure 6-6 Securing the front of the control enclosure to the rack

5. Replace the left and right end caps on the control enclosure. Hook the top edge of the end cap on the control enclosure and rotate the end cap down until it snaps into place.
6. If the control enclosure was dismantled to reduce the weight of the control enclosure before installing it in the rack, continue the installation at step 7 on page 173. Otherwise, continue the hardware installation at step 13.

> **Note:** Ensure that you install the components to the same location from which they were removed when dismantling the control enclosure.

7. Install the lower node canister in the control enclosure.
8. Install the upper node canister in the control enclosure.
9. Install the right power interposer in the control enclosure.
10. Install the right power supply unit in the control enclosure.
11. Install the left power interposer in the control enclosure.
12. Instal the left power supply unit in the control enclosure.
13. Connect the power cords to the power supply units in the control enclosure. See Figure 6-7. Use the cable retainers to secure the power cables from being accidentally pulled out of the enclosure. The cable retainer, which is on the back of each power supply unit, has a curved opening that faces the rear of the power supply unit. After you plug the power cables in to the power supply unit, slip the power cable behind the retainer. Then, pull the cable back into the retainer opening to secure the cable.

> **Note:** Do not connect the power cables to the power source outlets at this time.

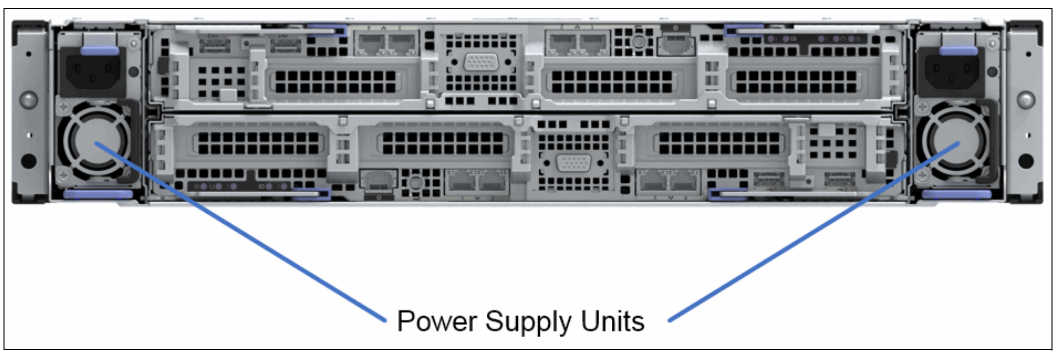


Figure 6-7 Control enclosure power supply units

Installing the model A9F expansion enclosure

The following sections describe installing the expansion enclosure.

Unpacking the model A9F expansion enclosure

> **CAUTION:**
>
> **The weight of this part or unit is more than 55 kg (121.2 lb.). It takes specially trained persons, a lifting device, or both to safely lift this part or unit. To avoid personal injury, before you lift this unit, remove all appropriate subassemblies per instructions to reduce the system weight.**

The model A9F expansion enclosure, the front fascia (1U and 4U pieces), the cable management arm, and the slide rail kit are shipped in one box. The drives for the enclosure are shipped in a separate box.

1. Remove the cardboard tray that contains the slide rails, cable management arm, and fascia from cardboard box in which the expansion enclosure was shipped.
2. Remove the foam end pieces from the top of the expansion enclosure.
3. Cut the corners of the shipping box and fold them down to uncover the sides and faces of the expansion enclosure.
4. With four or more persons, push the expansion enclosure sideways onto an suitably rated lift. Keep the remaining foam block protectors attached to the enclosure.
5. Remove the support rail kit from the box in which it was shipped.
6. Remove the 4U and 1U fascia from the boxes in which they were shipped.
7. Remove the cable management arm assembly from its packaging.

Installing support rails for the model A9F expansion enclosure

> **Note:** Refer to the system planning worksheets provided by the customer for the rack location in which to install the expansion enclosure.

1. Locate the two control enclosure rails and the M4xL6 and M5xL13 screws.
2. Remove the inner member of each rail. Push the tab (a) and slide the middle rail member back. See Figure 6-8.

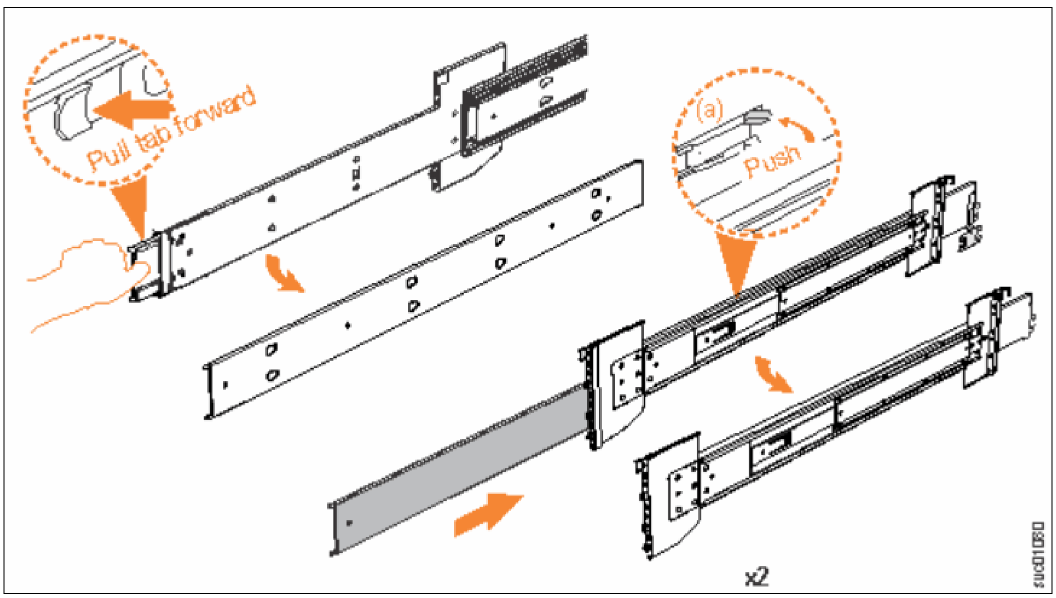


Figure 6-8 Detaching the inner rail member

3. Use four M4xL6 screws to attach the inner rail members to the side of the expansion enclosure. Figure 6-9 shows the screw locations.

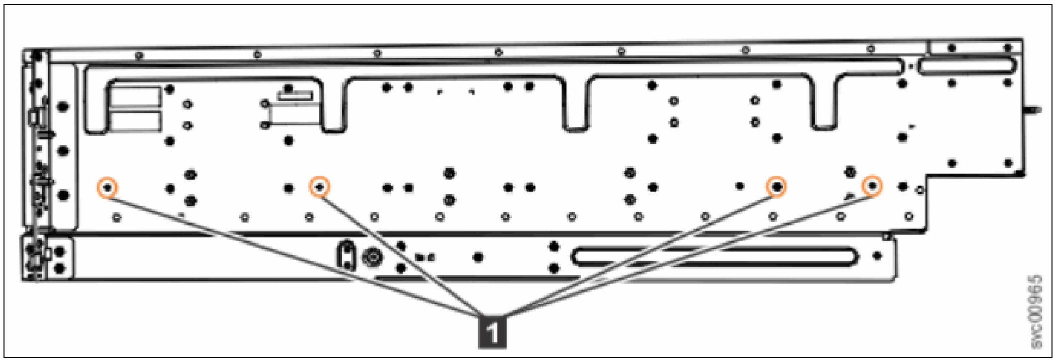


Figure 6-9 Screw locations to attach inner rail member to expansion enclosure

4. Install the inner section of the rail onto each side of the expansion enclosure, as shown in Figure 6-10.

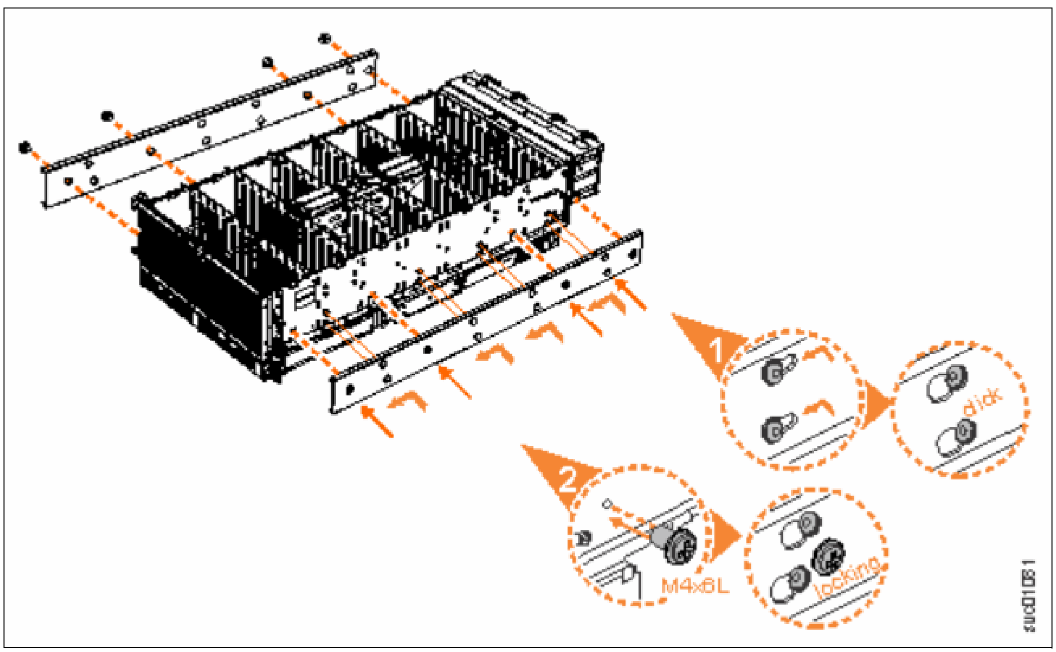


Figure 6-10 Attaching the inner rail members to the expansion enclosure

5. Use the M5xL13 screws to install the outer rail member and bracket assembly in the rack, as shown in Figure 6-11.

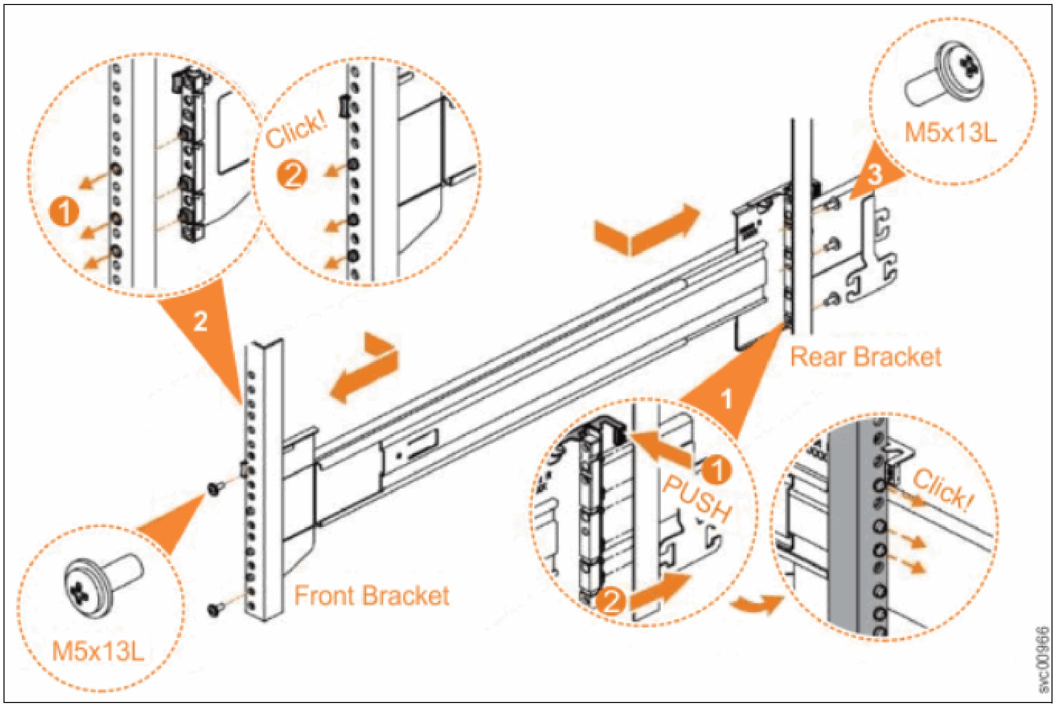


Figure 6-11 Installing the outer rail members in the rack

6. Repeat step 5 to install the opposite outer rail member in the rack.

Figure 6-12 shows the front of an outer rail member installed in the rack.

Figure 6-12 Installed outer rail member

Installing the model A9F expansion enclosure in the rack

CAUTION:

The model A9F expansion enclosure is heavy. Before you install the expansion enclosure in the rack for the first time or replace it in the rack to complete a service task, review and implement the following tasks:

- Always use a suitably rated mechanical lift or four persons to raise the model A9F expansion enclosure to install it in the rack. Even after the drives, power supply units, secondary expander modules, canisters, fans, and top cover are removed, the expansion enclosure weighs 43 kg (95 lb.).
- Install the model A9F expansion enclosure in the lowest available position in the rack.
- Ensure that the drives are easily accessible. Avoid installing the model A9F expansion enclosure above position 22U in the rack.

Complete the following steps:

1. Fully extend the left and right drawer sections from the rack to lock the rails in the extended position. See 1 in Figure 6-13.

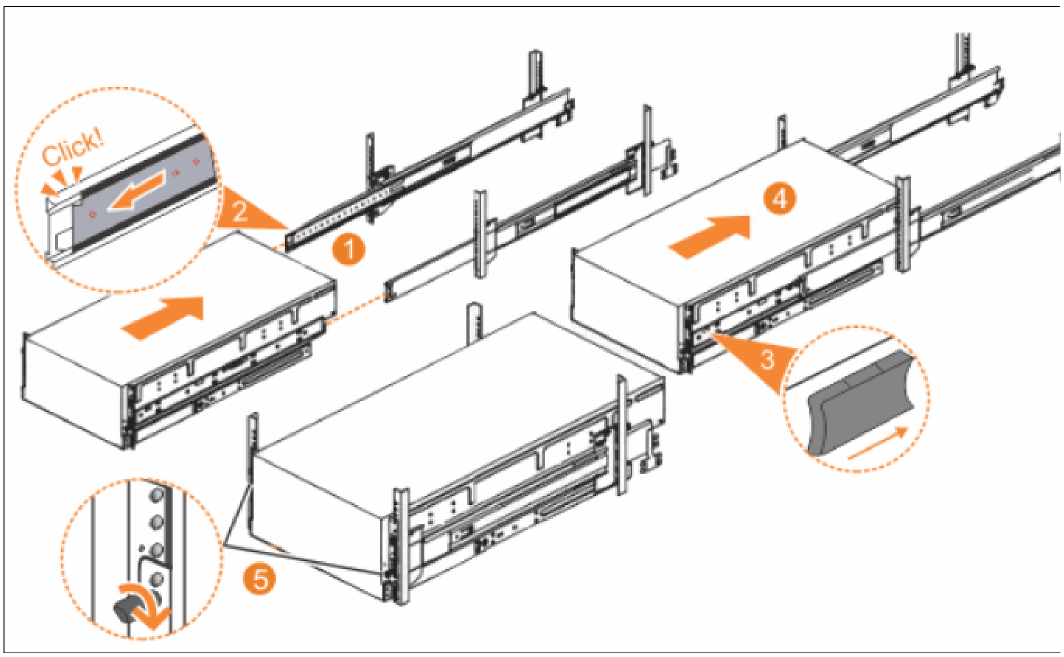


Figure 6-13 Installing the model A9F expansion enclosure in the rack

2. Ensure that the ball bearing retainer clicks into place inside the front of the left and right drawer sections. See [2] in Figure 6-13.
3. Using a suitably rated lift, align the expansion enclosure with the front of the rack cabinet and the rails.
4. Slide the expansion enclosure into the rail outer members until it is fully inserted.

5. Remove the expansion enclosure top cover:
   a. Slide the release latch 1 on the top cover in the direction shown in Figure 6-14.

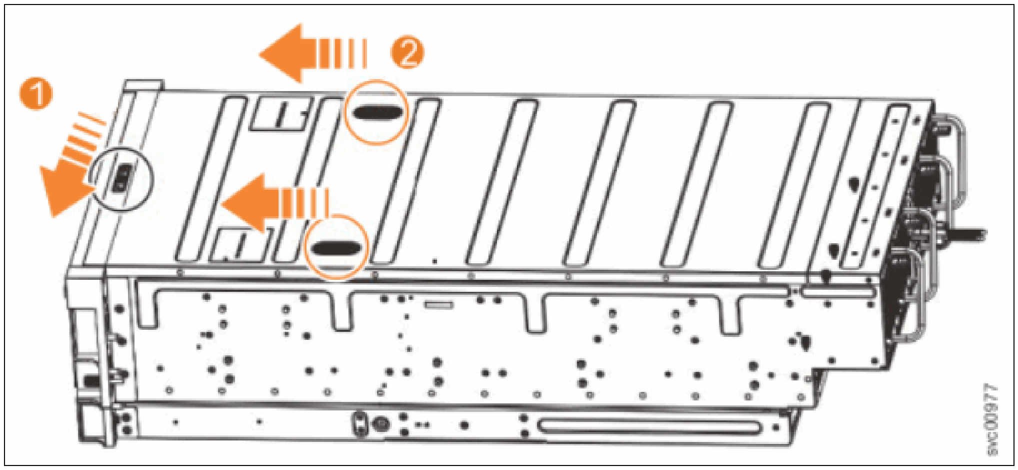


Figure 6-14 Releasing the expansion enclosure top cover

   b. Slide the cover toward the front of the expansion enclosure, as shown in Figure 6-14.
   c. Carefully lift the cover up, as shown in Figure 6-15.

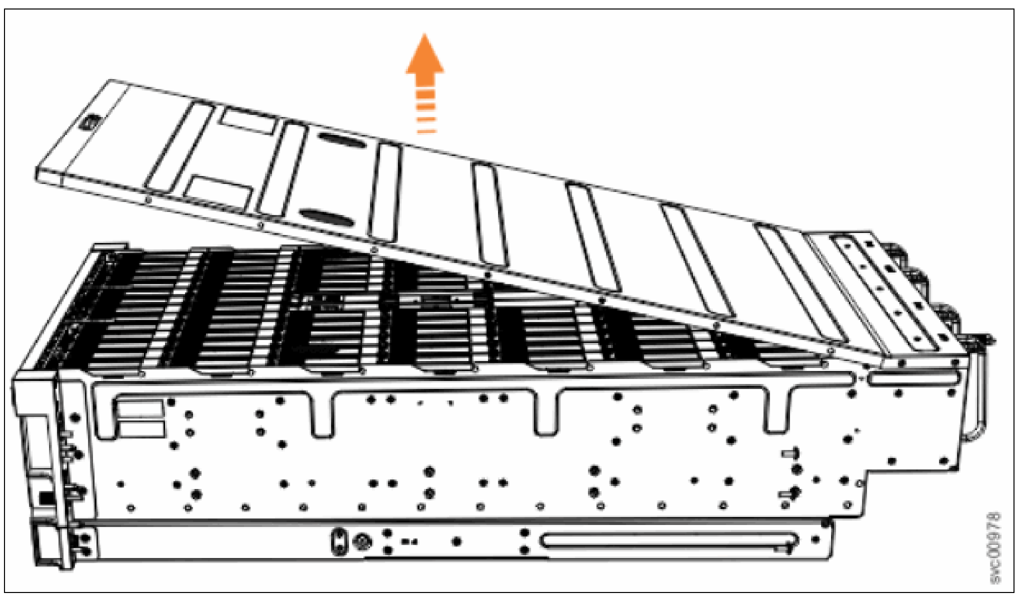


Figure 6-15 Removing the expansion enclosure top cover

6. Install the SAS flash drives in the expansion enclosure. A label on the expansion enclosure cover (Figure 6-16) shows the drive locations in the expansion enclosure. The drive slots are numbered 1 - 14 from left to right and A - G from the back to the front of the enclosure.

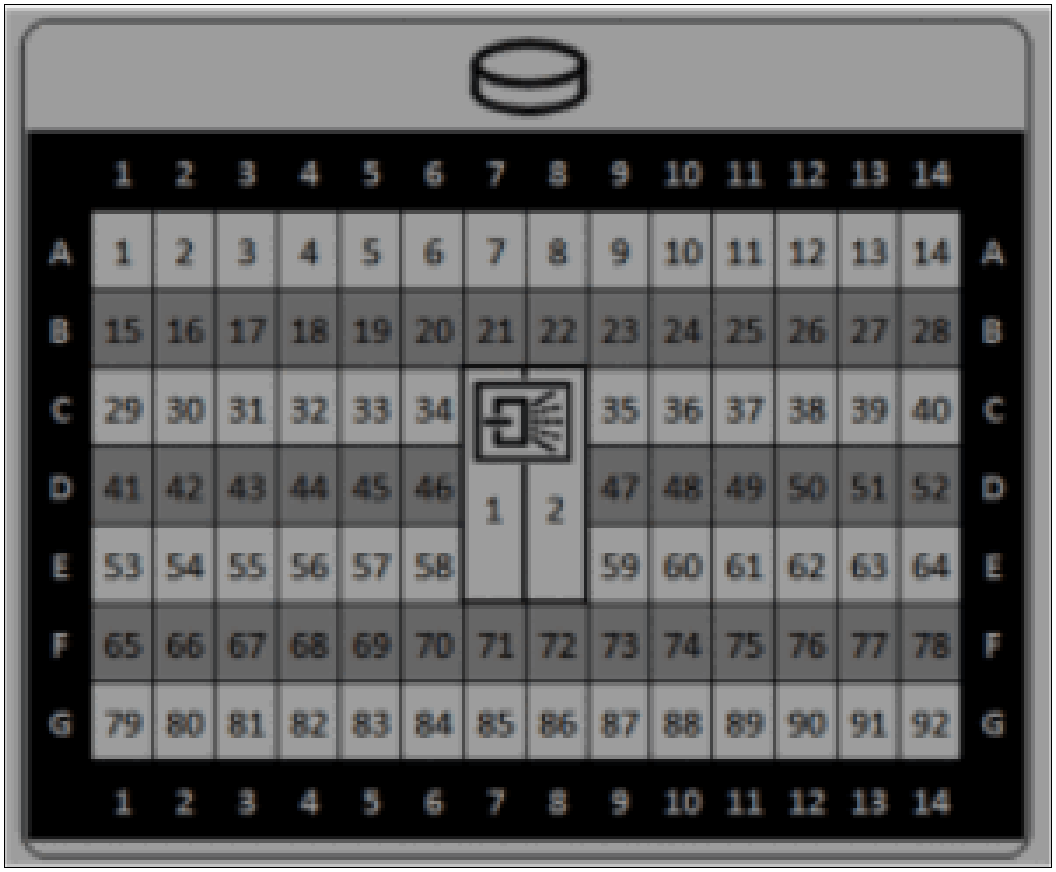


Figure 6-16 Expansion enclosure drive locations

The drive slots must be populated sequentially, starting from the back-left corner position (slot 1, grid A1). Sequentially install the drive in the slots from left to right and back row to front. Always complete a full row before you install drives in the next row.

Complete the following steps for each drive that is to be installed in the expansion enclosure:

a. Touch the static-protective package that contains the SAS flash drive to any unpainted metal surface on the enclosure. Wear an anti-static wrist strap to remove the drive from the package.

b. Move the drive handle to the open (unlocked) position (1 in Figure 6-17 on page 180).

c. Gently push the drive down until it stops and the bottom of the latch is aligned with the top of the partition. Ensure that the handle is not open more than 45 degrees from the drive carrier (2 in Figure 6-17 on page 180).

d. Rotate the handle down to lock the drive assembly into the chassis (3 in Figure 6-17 on page 180).

e. Ensure that the toe on the bottom of the latch is fully engaged with the partition in the chassis.

f. Ensure that the top toe of the latch is also fully engaged (4 in Figure 6-17).

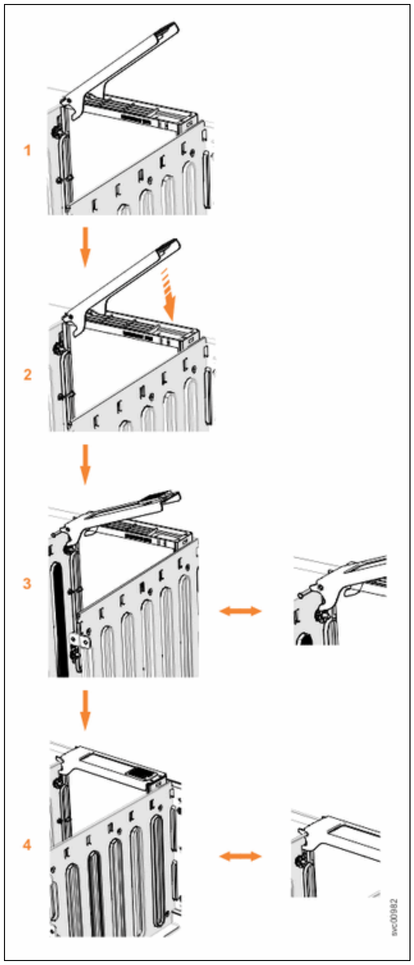


Figure 6-17 SAS flash drive installation in expansion enclosure

7. Install the top cover on the expansion enclosure:

   a. Carefully lower the cover and ensure that it is aligned correctly with the back of the enclosure, as shown in Figure 6-18 on page 181.

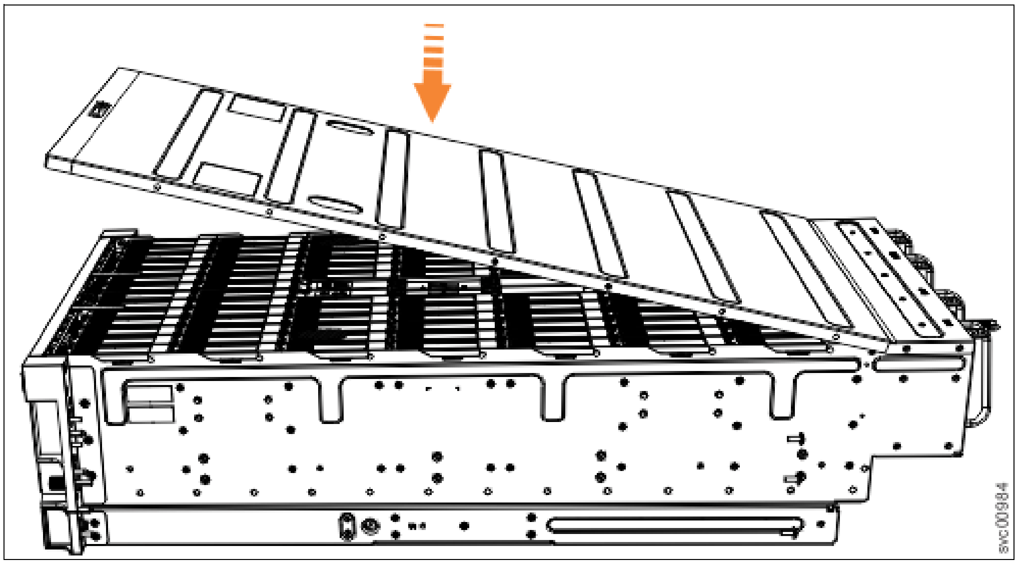


Figure 6-18 Aligning the expansion enclosure top cover

b. Push the cover release lever **2** to the side, as show in Figure 6-19.

c. Slide the cover towards the back of the expansion enclosure **3** back until it stops, as shown in Figure 6-19.

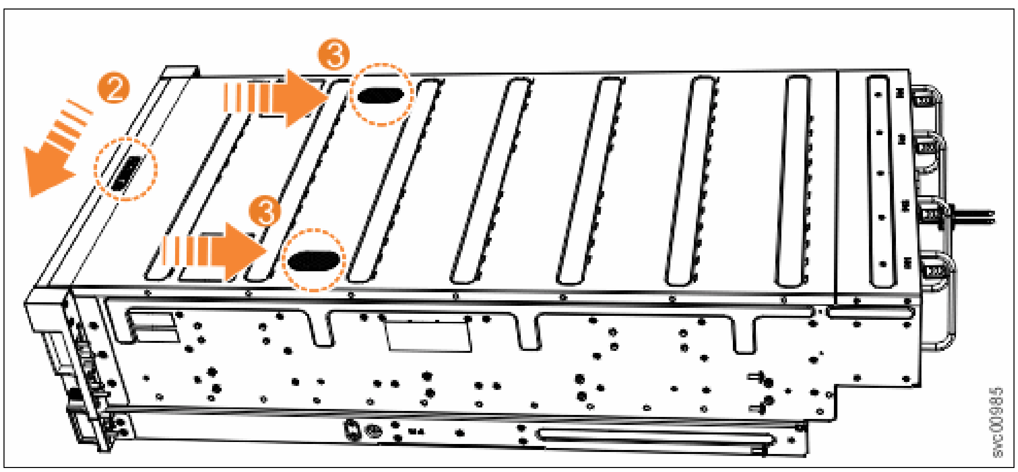


Figure 6-19 Replacing the expansion enclosure top cover

d. Verify that the cover correctly engages the cover release latch and all of the inset tabs on the expansion enclosure.

e. Lock the cover into position by sliding the release lever 4, as shown in Figure 6-20.

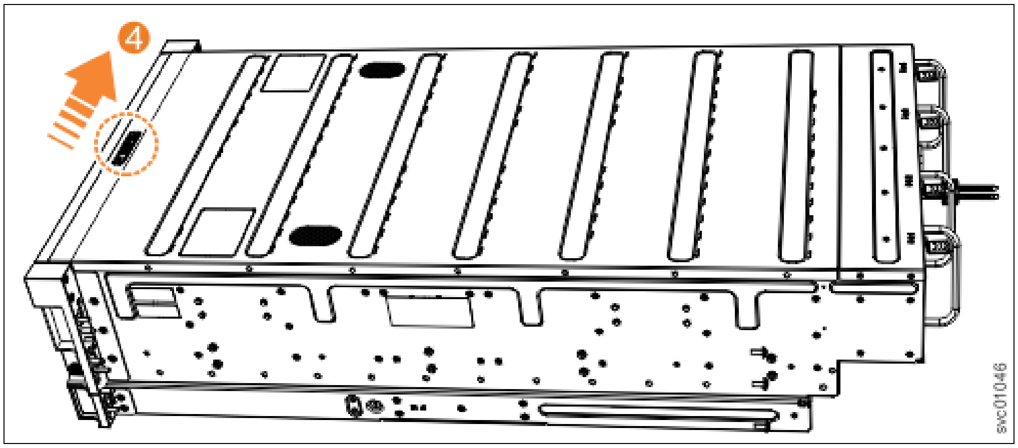


Figure 6-20 Locking the expansion enclosure top cover

8. Slide the expansion enclosure into the rack:

   a. Locate the left and right blue release tabs near the front of the enclosure. Press both release tabs forward to unlock the drawer mechanism (3 in Figure 6-21).

   b. Push the enclosure firmly into the rack (4 in Figure 6-21).

   c. Tighten the locking thumb screws (5 in Figure 6-21) to secure the enclosure in the rack.

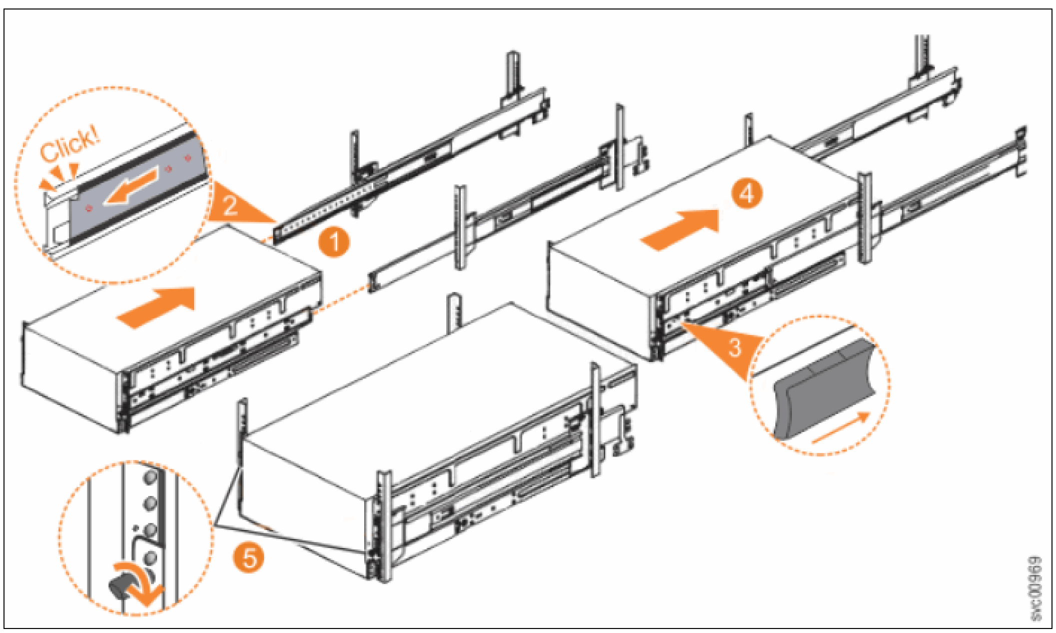


Figure 6-21 Sliding the model A9F expansion enclosure into the rack

9. Install the cable management arms (CMA). The cable management arms consist of an upper arm and a lower arm assembly, as shown in Figure 6-22 on page 183.

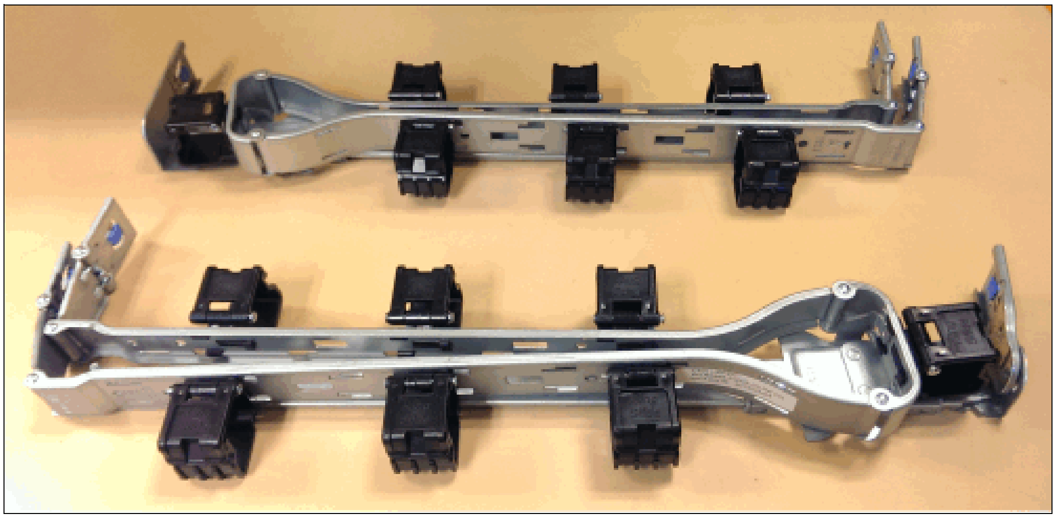


Figure 6-22 Model A9F expansion enclosure cable arm assemblies

The support rail connectors of each CMA assembly are installed on the rail hooks at the end of the support rails, as shown in Figure 6-23.

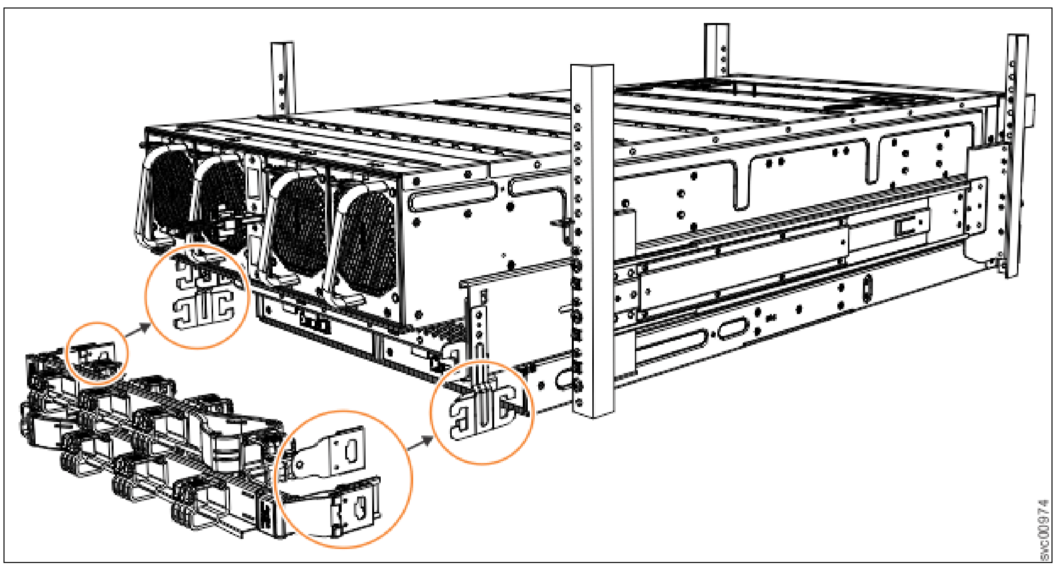


Figure 6-23 Upper and lower cable management arm assemblies

Complete the following substeps:

a. Remove the straps from the upper and lower CMA assemblies. The straps are used only for shipping.

b. Install the upper CMA assembly. Figure 6-24 shows the connectors on the upper CMA assembly.

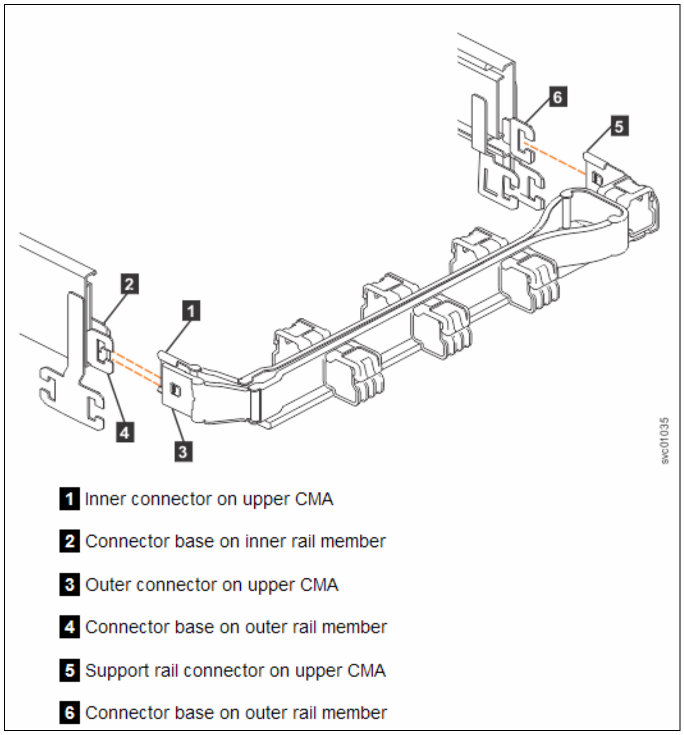


Figure 6-24 Upper CMA assembly connectors

i. Install the inner connector of the upper CMA assembly **1** to the inner member of the left support rail **2** from the outer and inner support rails, as shown in Figure 6-25.

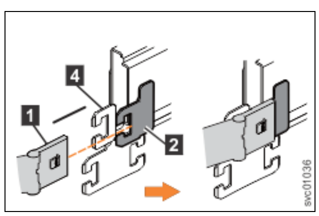


Figure 6-25 Installing the inner connector of the upper CMA to the inner member of the left support rail

ii. Install the outer connector of the upper CMA assembly **3** to the outer member of the left support rail **4**, as shown in Figure 6-26.

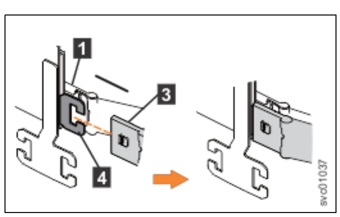


Figure 6-26 installing the outer connector of the upper CMA to the outer member of the left support rail

iii. Attach the support rail connector on the upper CMA assembly 5 to the connector base on the right support rail 6, as shown in Figure 6-27.

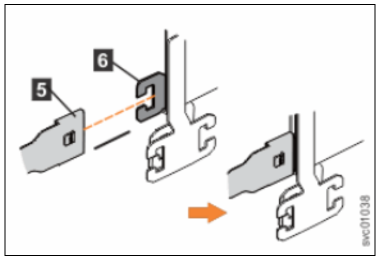


Figure 6-27 installing the support rail connector of the upper CMA to the connector base on the right support rail

iv. Ensure that the upper CMA assembly connectors attach securely to the hooks on the rails.

c. Install the lower cable management arm assembly. The procedure for attaching the lower CMA assembly is the same as the procedure to attach the upper CMA assembly. However, the connector locations are reversed. For comparison, Figure 6-28 shows the upper and lower CMA assemblies as they are aligned to the support rails. The support rail connector of the upper CMA attaches to the right rail. The support rail connector of the lower CMA assembly 11 attaches to the left rail.

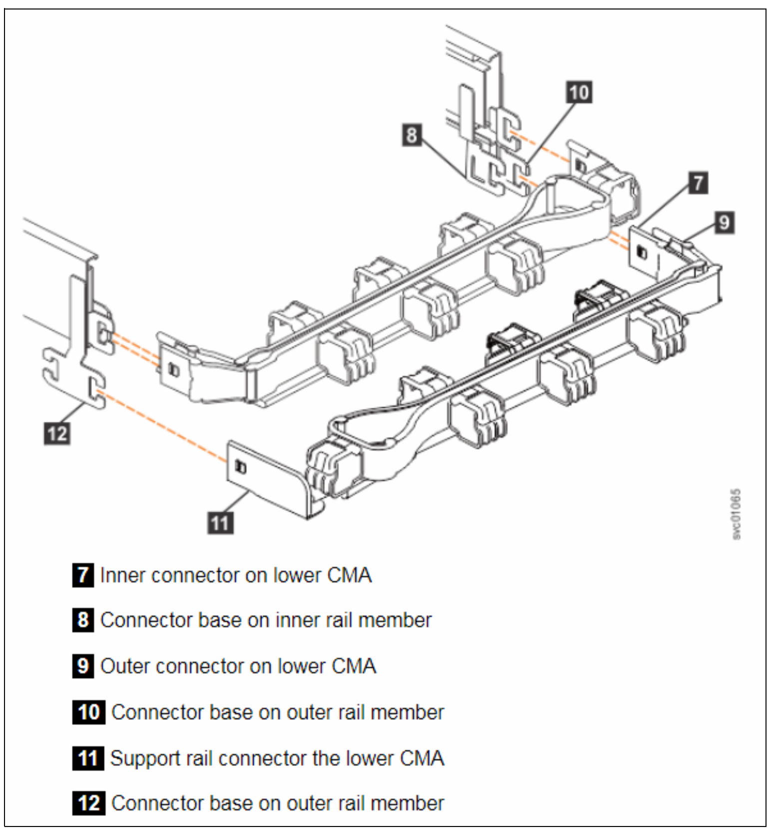


Figure 6-28 Comparison of upper CMA assembly and lower CMA assembly connectors

i. Install the inner connector of the lower CMA assembly 7 to the inner member of the right support rail 8, as shown in Figure 6-28.

ii. Install the outer connector of the lower CMA assembly **9** to the outer member of the right support rail **10** , as shown in Figure 6-28 on page 185.

iii. Attach the support rail connector on the lower CMA assembly **11** to the connector on the left support rail **12**, as shown in Figure 6-28 on page 185.

iv. Ensure that the lower CMA assembly is securely attached to the hooks on the end of the support rails.

10. Connect the power cables to the power connectors on the rear of the expansion enclosure.

Attention: Do not connect the power cables to the power source outlets at this time.

a. Secure the power cables in the cable retainer at each power connector on the rear of the enclosure, as shown in Figure 6-29.

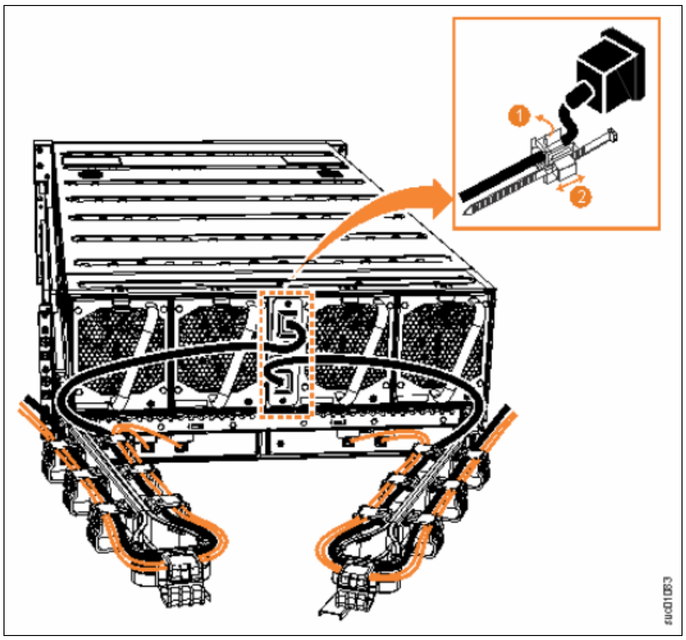


Figure 6-29 Model A9F expansion enclosure power cord connections and routing

b. Ensure that each cable is installed along one of the cable management arms.

11. Install the front fascia panels on the expansion enclosure:

a. Use the slide rails to pull the enclosure out of the rack.

b. Align the front 4U fascia with the enclosure so that the thumbscrews go through the holes on each side. As Figure 6-30 shows, this action aligns the screw holes on the back of the fascia with the screw holes on the front flange of the enclosure.

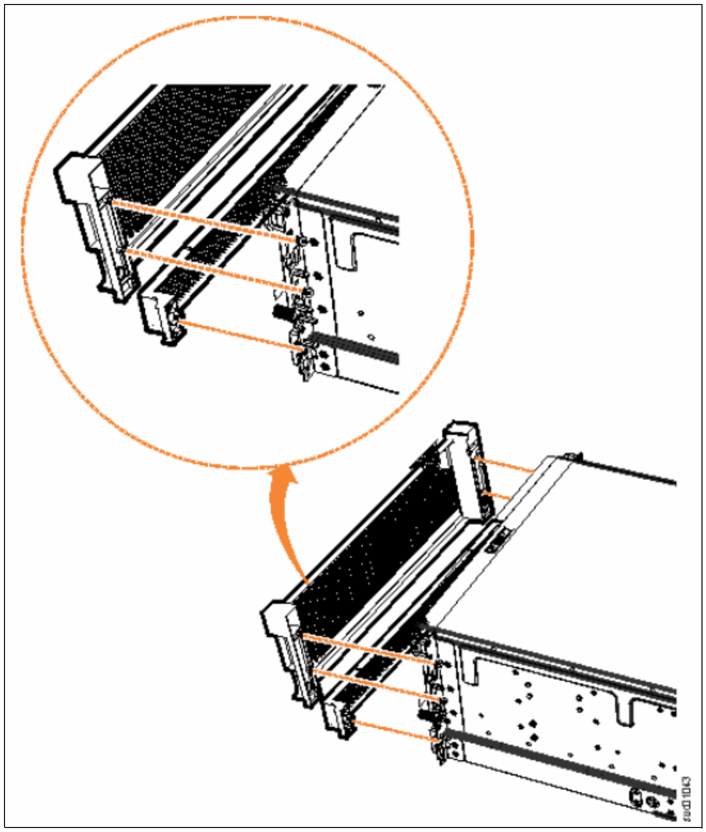


Figure 6-30 Installing fascia panels on the front of the expansion enclosure

c. Replace the four screws to reattach the 4U fascia. Secure the screws from the back of the flange and into the rear of the fascia. Each side of the 4U fascia contains two screws.

d. Attach the bottom 1U fascia that covers the power supply units (PSUs). Align the fascia with the enclosure and gently push it until it clicks into place on the chassis, as shown in Figure 6-30. Align the tab on each side of the 1U fascia with the corresponding slots on the enclosure flange. Pins on each flange must also align with a hole in each side of the 1U fascia.

12. Slide the expansion enclosure into the rack.

Installing the Model AFF expansion enclosure

The following section describes how to install the expansion enclosure.

Unpacking the Model AFF expansion enclosure

CAUTION:

Lifting the FlashSystem 9100 model AFF expansion enclosure requires two persons or suitable lifting equipment. If necessary, the expansion enclosure can be dismantled to reduce the weight of the control enclosure.

Complete the following steps:

1. Cut the box tape and open the lid of the shipping carton.
2. Remove the rail kit box and set it aside.
3. Lift the front and front foam packing pieces from the carton.
4. Remove the four corner reinforcement pieces from the carton.
5. If two persons or suitable lifting equipment are not available, continue by dismantling the control enclosure at step 6. Otherwise, continue the install at , “Installing support rails for the model AFF expansion enclosure”.
6. Using the box knife, carefully cut the four corners of the carton from top to bottom.
7. Fold the sides and back of the carton down to uncover the front of the expansion enclosure. If necessary, carefully cut along the lower fold line of the sides and remove them.
8. Carefully cut the foam packing away from the front of the expansion enclosure.
9. Carefully cut open the bag covering the front of the expansion enclosure.
10. Remove the leftmost drive or drive filler and record its location. If it is a drive, also record its serial number.
11. Repeat step 10 until all drives or drive fillers are removed from the expansion enclosure.

Installing support rails for the model AFF expansion enclosure

> **Note:** Refer to the system planning worksheets provided by the customer for the rack location in which to install the expansion enclosure.

1. Locate the two expansion enclosure rails.
2. Working at the front of the rack cabinet, identify the two standard rack units (2U) of space in the rack into which you want to install the support rails. See Figure 6-31.

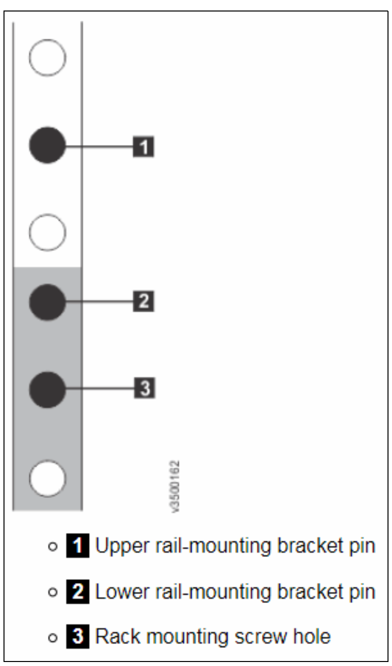


Figure 6-31 Rack hole locations in the front of the rack

3. Ensure that the appropriate bracket pins are installed in the front and rear bracket of each rail. Each rail comes with four medium pins pre installed (two in the front bracket and two in the rear bracket). Large pins are provided separately. Use the pins that are appropriate for the mounting holes in your rack.
4. Ensure that the appropriate bracket pins are installed in the front and rear bracket of each rail. Each rail comes with four medium pins preinstalled (two in the front bracket and two in the rear bracket). Large pins are provided separately. Use the pins that are appropriate for the mounting holes in your rack. See Table 6-3.

Table 6-3 Selecting bracket pins for the rack

Mounting Holes	Bracket Pins
Round, unthreaded	Use the preinstalled medium pins.
Square	Unscrew the medium pins and replace with the large pins that are supplied with the rails.

5. At each end of the rail, grasp the tab **1** and pull firmly to open the hinge bracket. See Figure 6-32.

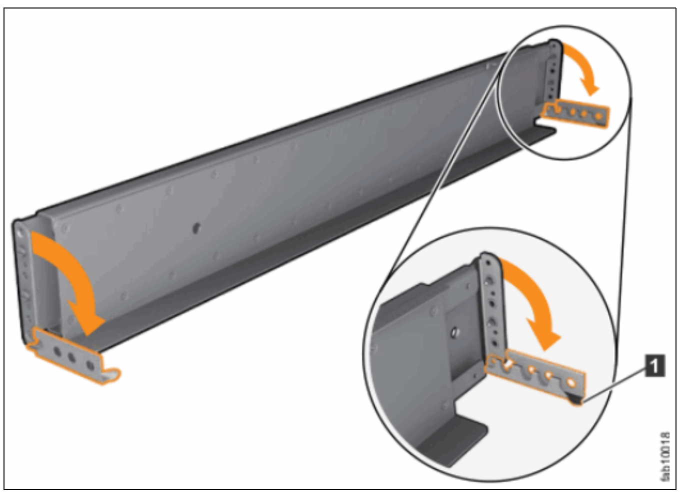


Figure 6-32 Opening the rail hinge brackets

6. Align the holes in the rail bracket with the holes on the front and rear rack cabinet flanges. Ensure that the rails are aligned on the inside of the rack cabinet.
7. On the rear of the rail, press the two bracket pins into the holes in the rack flanges.

8. Close the rear hinge bracket 4 to secure the rail to the rack cabinet flange. See Figure 6-33.

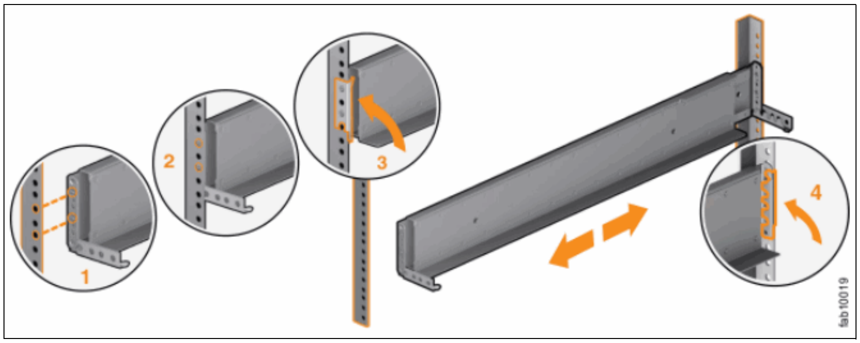


Figure 6-33 Closing the rail hinge brackets

9. On the front of the rail, press the two bracket pins into the holes in the rack flanges.
10. Close the front hinge bracket 3 to secure the rail to the rack cabinet flange. See Figure 6-33 on page 190.
11. Secure the rear of the rail to the rear rack flange with two black M5 screws.
12. Repeat step 5 on page 189 through step 11 to install the opposite rail in the rack.

Installing the model AFF expansion enclosure in the rack

1. Remove the left and right end caps from the expansion enclosure by grasping the handle and pulling the bottom of the end cap free, then clearing the tab on the top of the enclosure. See Figure 6-34.

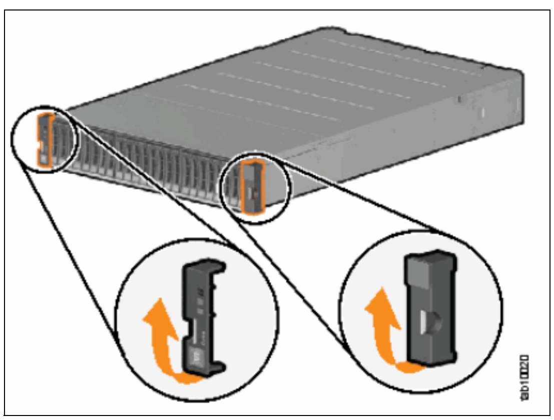


Figure 6-34 Removing expansion enclosure end caps

2. Lift the expansion enclosure from the shipping carton and align the expansion enclosure with the front of the rack cabinet and the rails.

3. Slide the expansion enclosure into the rack until it is fully inserted. See Figure 6-35.

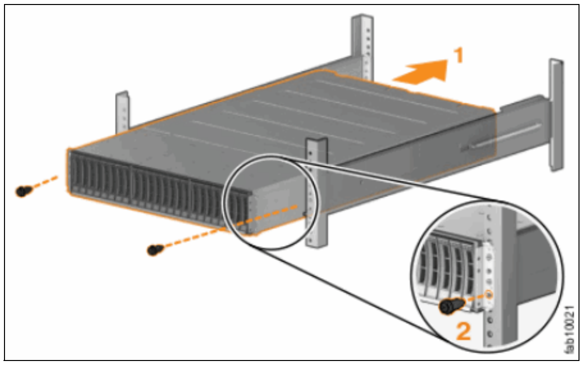


Figure 6-35 Inserting the expansion enclosure in the rack

4. Secure the enclosure with screws in the rack mounting screw holes. See Figure 6-35 and Figure 6-36.

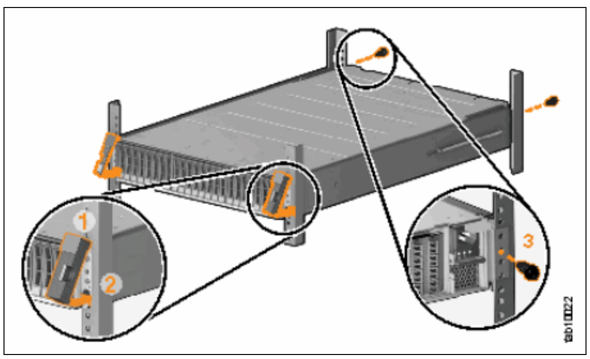


Figure 6-36 Securing the expansion enclosure to the rack

5. Replace the left and right end caps on the expansion enclosure. Hook the top edge of the end cap on the control enclosure and rotate the end cap down until it snaps into place.
6. If the expansion enclosure was dismantled to reduce the weight of the expansion enclosure before installing it in the rack, continue the installation at step 7. Otherwise continue the installation at step 8.

> **Note:** Ensure that you install the flash drives into the same location from which they were removed when dismantling the expansion enclosure.

7. Reinstall the flash drives in the expansion enclosure into the same slot from which they were removed.

8. Connect the power cords to the power supply units in the expansion enclosure. See Figure 6-37.

Note: Do not connect the power cord to the power sources at this time.

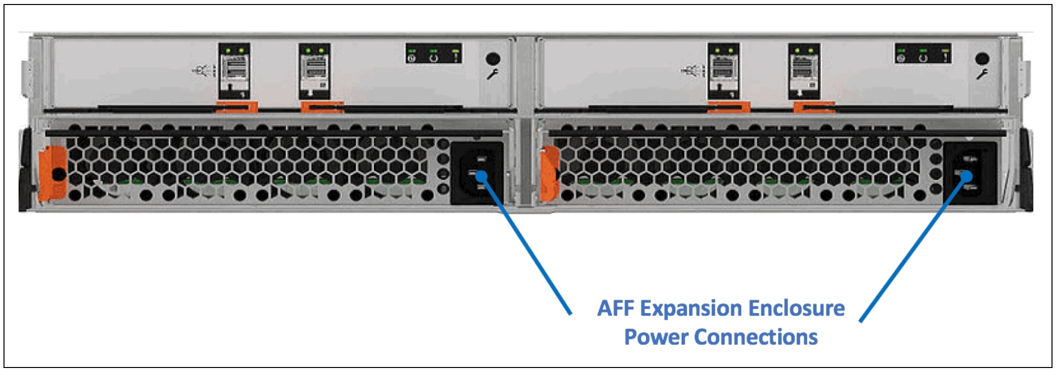


Figure 6-37 Model AFF expansion enclosure power connections

6.2.4 Connecting the FlashSystem 9100 components

Completed the following steps to connect the FlashSystem 9100 components:

1. If the FlashSystem 9100 system includes optional expansion enclosures, connect the expansion enclosures to the control enclosure using the directions in “Connecting the expansion enclosures to the control enclosure”.
2. Connect the ethernet cables to the control enclosure using the directions in “Connecting fibre channel cables to the control enclosure” on page 195.
3. Connect the fibre channel cables to the control enclosure using the directions in “Connecting fibre channel cables to the control enclosure” on page 195.

Connecting the expansion enclosures to the control enclosure

Each FlashSytem 9100 control enclosure in the system can connect to two SAS chains of expansion enclosures. On each SAS chain, the system can support up to a SAS chain weight of 10. Each 9846-A9F or 9848-A9F expansion enclosure adds a value of 2.5 to the SAS chain weight. Each 9846-AFF or 9848-AFF expansion enclosure adds a value of 1 to the SAS chain weight. For additional details, refer to the IBM KnowledgeCenter.

Observe the following guidelines when inserting an SAS cable into an SAS port on the control enclosure or expansion enclosure:

- Ensure that the orientation on the connector matches the orientation on the port before inserting the connector into the port. The cable connector and the port are keyed.
- Insert the cable connector in to the port gently until it clicks into place. If you feel resistance, the orientation of the cable connector is likely wrong.
- When inserted correctly, a cable connector can only be removed by pulling the tab.

Be aware of the following guidelines when connecting the enclosures:

- The FlashSystem 9100 control enclosure supports 4-port SAS interface adapters. However, only ports 1 and 3 on the adapters are used for SAS connections. Ports 2 and 4 on the adapters are inactive.
- A SAS interface adapter can be installed in any of the three PCIe slots in a control enclosure node canister. It is typically installed in PCI3 slot 3 in a control enclosure node canister.
- Node canister 1 is upside down from node canister 2 in an expansion enclosure.
- A SAS cable must not be connected between a port on a left canister and a port on a right canister.
- A SAS cable must not be connected between ports in the same enclosure.
- A connected port on a node canister must connect to a singe port on an expansion canister.
- The last expansion enclosure in a chain must not have SAS cables attached to port 1 of canister 1 or port 1 of canister 2.
- After connecting a SAS cable to a model A9F expansion enclosure, route the SAS cable and power cord connected to the expansion enclosure in the cable management arm assembly. Allow slack in the SAS cable and power cord to prevent tension when the cable management arm assembly moves when the expansion enclosure is moved in or out of the rack. Use the supplied straps to secure the SAS cable and power cord to the cable management arm assembly.

Figure 6-38 on page 194 shows a FlashSystem 9100 system with a control enclosure, two model AFF expansion enclosures, and two model A9F expansion enclosures.

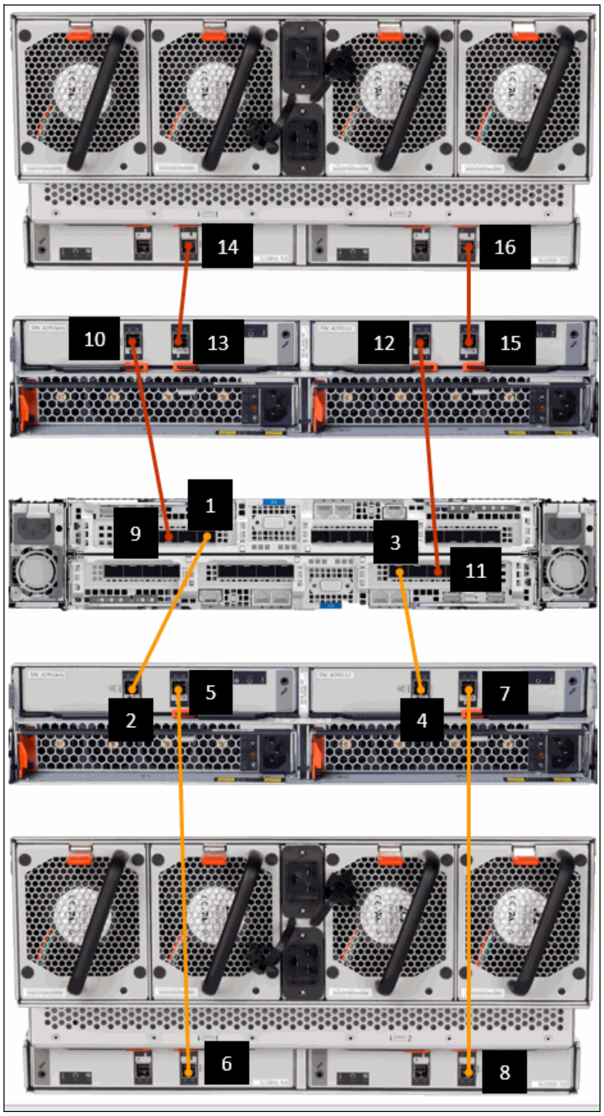


Figure 6-38 FlashSystem 9100 SAS cabling

To install the SAS cables in a FlashSystem 9100 with expansion enclosures, complete the following steps while referring to Figure 6-38.

1. Install the SAS cables for the first SAS chain:
   a. Connect SAS port 1 **1** in the upper node canister to SAS port 1 **2** in the left canister in the first expansion enclosure in the SAS chain.
   b. Connect SAS port 1 **3** in the lower node canister in the control enclosure to SAS port 1 **4** in the right canister in the first expansion enclosure in the SAS chain.
   c. If additional expansion enclosures are to be connected to the first SAS chain, complete the following steps for each additional expansion enclosure:
      i. Connect SAS port 2 **5** in the left canister of the first expansion enclosure in the SAS chain to SAS port 1 **6** in the left canister in the second expansion enclosure in the SAS chain.
      ii. Connect SAS port 2 **7** in the right canister in the first expansion enclosure in the SAS chain to SAS port 1 **8** in the right canister in the second expansion enclosure in the SAS chain.

2. If expansion enclosures are to be installed on a second SAS chain, complete the following steps:
   a. Connect SAS port 3 **9** in the upper node canister to SAS port 1 **10** in the left canister in the first expansion enclosure in the second SAS chain.
   b. Connect SAS port 3 **11** in the lower node canister in the control enclosure to SAS port 1 **12** in the right canister in the first expansion enclosure in the second SAS chain.
   c. If additional expansion enclosures are to be connected to the second SAS chain, complete the following steps for each additional expansion enclosure:
      i. Connect SAS port 2 **13** in the left canister of the first expansion enclosure in the SAS chain to SAS port 1 **14** in the left canister in the second expansion enclosure in the SAS chain.
      ii. Connect SAS port 2 **15** in the right canister in the first expansion enclosure in the SAS chain to SAS port 1 **16** in the right canister in the second expansion enclosure in the SAS chain.

Connecting ethernet cables to the control enclosure

Note: Refer to the system planning worksheets provided by the customer for the ethernet port connections to each node canister in the control enclosure.

To connect the ethernet cables to the node canisters in the control enclosure, complete the following steps:

1. Connect ethernet port 1 of each node canister in the control enclosure to the IP network that will provide connection to the system management interfaces. See Figure 6-39.

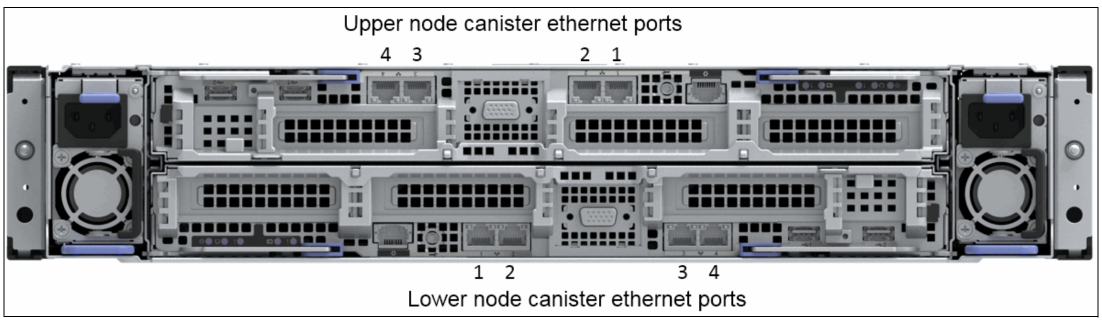


Figure 6-39 Control enclosure ethernet port locations

2. Connect additional ethernet cables to port 2, port 3, and port 4 of each node canister as specified in the system planning worksheets.

Connecting fibre channel cables to the control enclosure

Note: Refer to the system planning worksheets provided by the customer for the fibre channel port connections to each node canister in the control enclosure.

Each node canister in the control enclosure can support up to three 16 Gbps fibre channel host adapter cards. The first fibre channel host adapter in a node canister must be installed in PCIe slot 1. Additional fibre channel host adapters are installed in PCIe slots 2 and 3 in a node canister.

To connect the fibre channel cables to the node canisters, complete the following steps:

1. Refer to the Network cable connection worksheet in the system planning worksheets for the number of cables to connect, and the location of each cable.
2. Connect each fibre channel to the specified port. See Figure 6-40 for the adapter location and port location on each adapter.

Note: Each node canister must have the same number of cables connected to it.

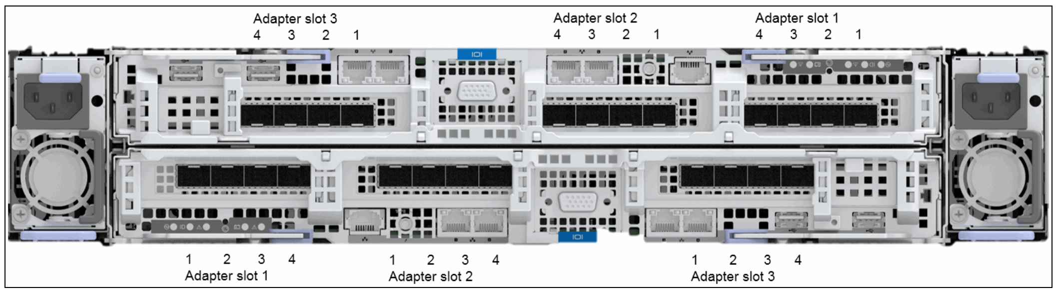


Figure 6-40 Control enclosure fibre channel ports

6.2.5 Powering on the FlashSystem 9100

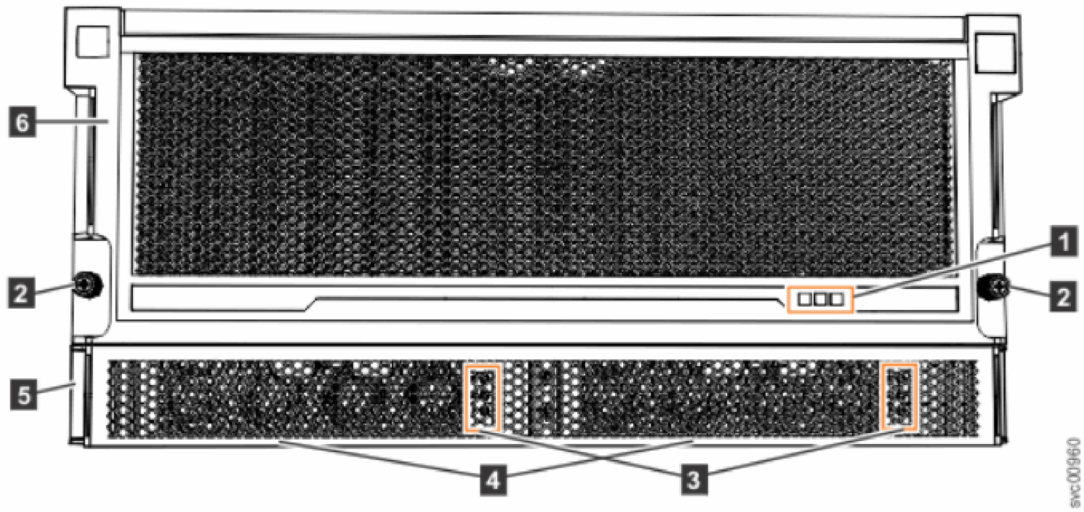
Attention: The information in this section is intended only for IBM authorized service providers. Customers need to consult the terms of their warranty to determine the extent to which they should attempt any IBM FlashSystem hardware installation.

Complete the following steps to power on the FlashSystem 9100:

1. Power on any model A9F expansion enclosures using the directions in "Powering on the model A9F expansion enclosure".
2. Power on any mode AFF expansion enclosures using the directions in "Powering on the model AFF expansion enclosure" on page 198.
3. Power on the control enclosure using the directions in "Powering on the control enclosure" on page 199.

Powering on the model A9F expansion enclosure

The model A9F expansion enclosure has two power supply units that are accessible from the front of the enclosure (4 in Figure 6-41 on page 197). The power supply units are covered by the 1U fascia panel 5. Each power supply unit has a power supply connector and power cord, which are accessible from the back of the expansion enclosure. Power is provided by connecting the power cords to the power source and, if necessary, switching on the power source. The expansion enclosure does not have a power button.



1 Display panel LEDs

2 Rack retention thumb screws

3 Power supply unit LEDs

4 Power supply units (PSUs)

5 PSU fascia (1U)

6 Front fascia (4U)

Figure 6-41 Model A9F expansion enclosure front view

To power on a model A9F expansion enclosure, complete the following steps:

1. Connect the power cords connected to the rear of the expansion enclosure to the power sources. If necessary, switch on the power source. The enclosure automatically powers on and begins power on self tests when connected to a power source.
2. Verify that the expansion enclosure powered on successfully:
   a. On the back of the expansion enclosure, all four fans and the expansion canister indicators (**3** and **8** in Figure 6-42 on page 198) become active when the power is connected.
   b. On the front of the enclosure, the indicators on the front display panel and each power supply unit(**1** and **3** in Figure 6-41) are also lit when the power is connected. See FlashSystem 9100 9846-A9F expansion enclosure LEDs and indicators for information about the status that is provided by the indicators.

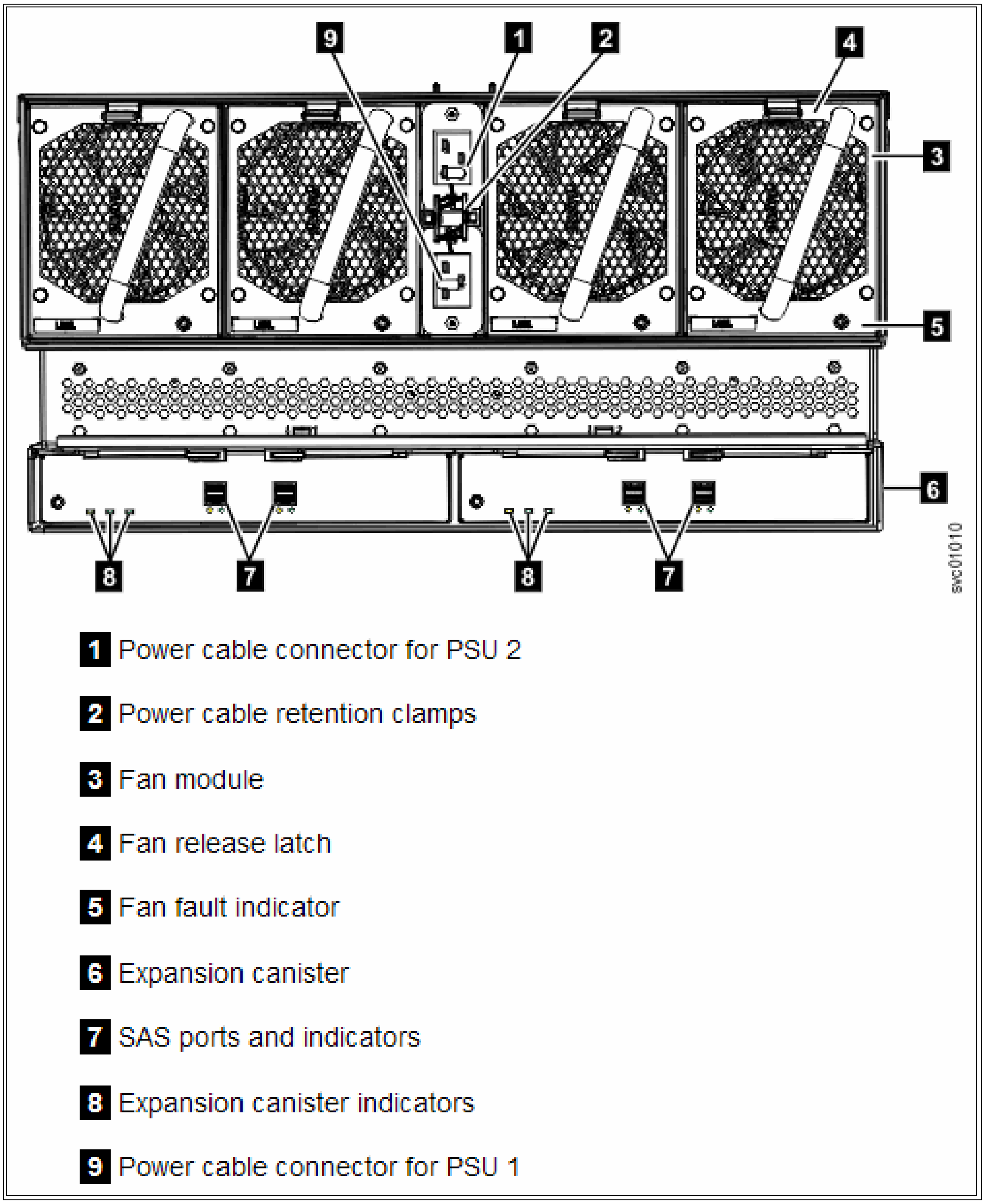


Figure 6-42 Model A9F expansion enclosure rear view

Powering on the model AFF expansion enclosure

To power on a model AFF expansion enclosure, complete the following steps:

Attention: Do not power on an expansion enclosure with any open drive bays. Every unused drive bay must be occupied by a drive blank. Open drive bays disrupt the internal air flow, causing the drives to receive insufficient cooling.

1. Connect the power cords connected to the rear of the expansion enclosure to the power sources. If necessary, switch on the power source. The enclosure automatically powers on and begins power on self tests when connected to a power source.

2. Verify that the expansion enclosure powered on successfully by checking the LEDs on each canister. See Figure 6-43.

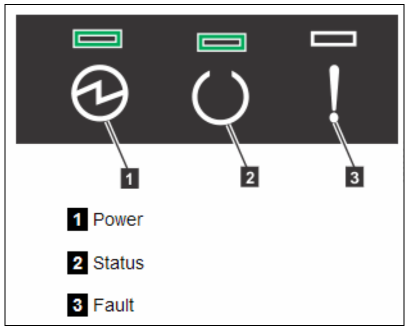


Figure 6-43 Model AFF expansion enclosure LEDs

The canister is ready with no critical errors when Power is illuminated, Status is on, and Fault is off.

Powering on the control enclosure

Attention: Do not power on the control enclosure with any open drive bays or host adapter slots:

- Every unused drive bay must be occupied by a drive blank.
- Filler panels must be installed in all empty host interface adapter slots.

Open drive slots and open host adapter slots disrupt the internal air flow, causing the drives to receive insufficient cooling.

To power on a control enclosure, complete the following steps:

1. Ensure that any expansion enclosures that are part of the system have been successfully powered up.
2. Connect the power cords connected to the rear of the control enclosure to the power sources. If necessary, switch on the power source. The enclosure automatically powers on and begins power on self tests when connected to a power source.

3. Verify that the control enclosure powered on successfully by checking the LEDs on the power supply units in the rear of the control enclosure. Figure 6-44 shows the location of the power status LED on the rear of a power supply unit. The LED on each power supply will be illuminated green when the power supply is functioning properly.

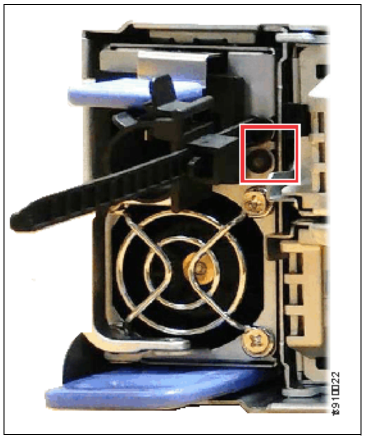


Figure 6-44 Control enclosure power supply unit rear view

6.3 System initialization

Important: The information in this section is intended only for IBM authorized service providers. Customers need to consult the terms of their warranty to determine the extent to which they should attempt any IBM FlashSystem hardware installation.

On an uninitialized system, the node canister technician port provides access to the system initialization wizard. On these systems, all node canisters have the green power LED on, the green status LED blinking, and the amber fault LED off.

The system can be configured as the first enclosure in a new system or as an additional enclosure in an existing system. If you are initializing the first enclosure in a new system, follow the instructions in 6.3.1, "System initialization for first enclosure in a new system". If you are initializing an additional enclosure in an existing system, following the instructions in 6.3.2, "System initialization for additional enclosure in an existing system" on page 205.

6.3.1 System initialization for first enclosure in a new system

Note: Refer to the system planning worksheets provided by the customer for the information required to initialize the system.

Perform the following steps to initialize the system:

1. Configure the ethernet port on your laptop to use Dynamic Host Configuration Protocol (DHCP).
2. Connect the your laptop's ethernet port to the technician port of the upper node canister in the control enclosure. See Figure 6-45 on page 201.

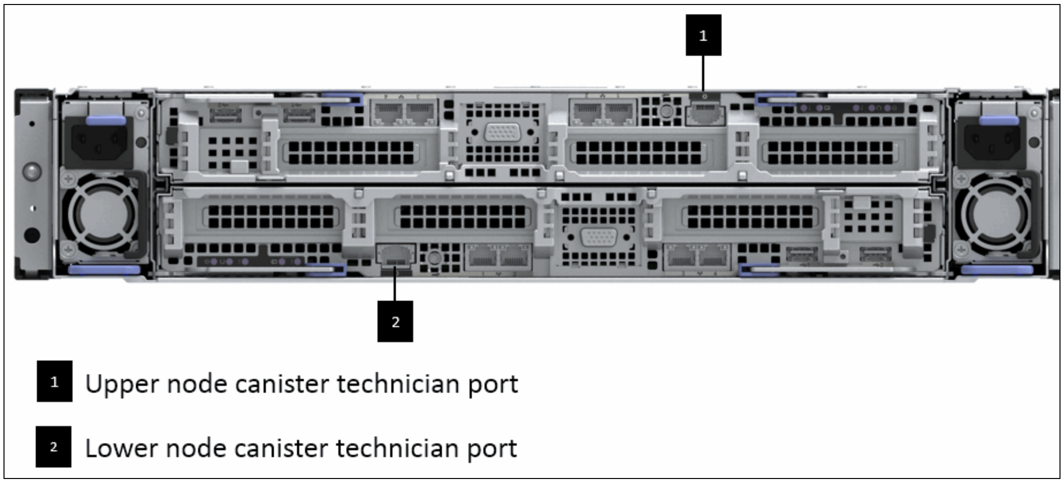


Figure 6-45 Control enclosure technician ports

3. Open a web browser and enter `http://install` in the URL field.
4. Wait for the System Initialization pane to be displayed (Figure 6-46).

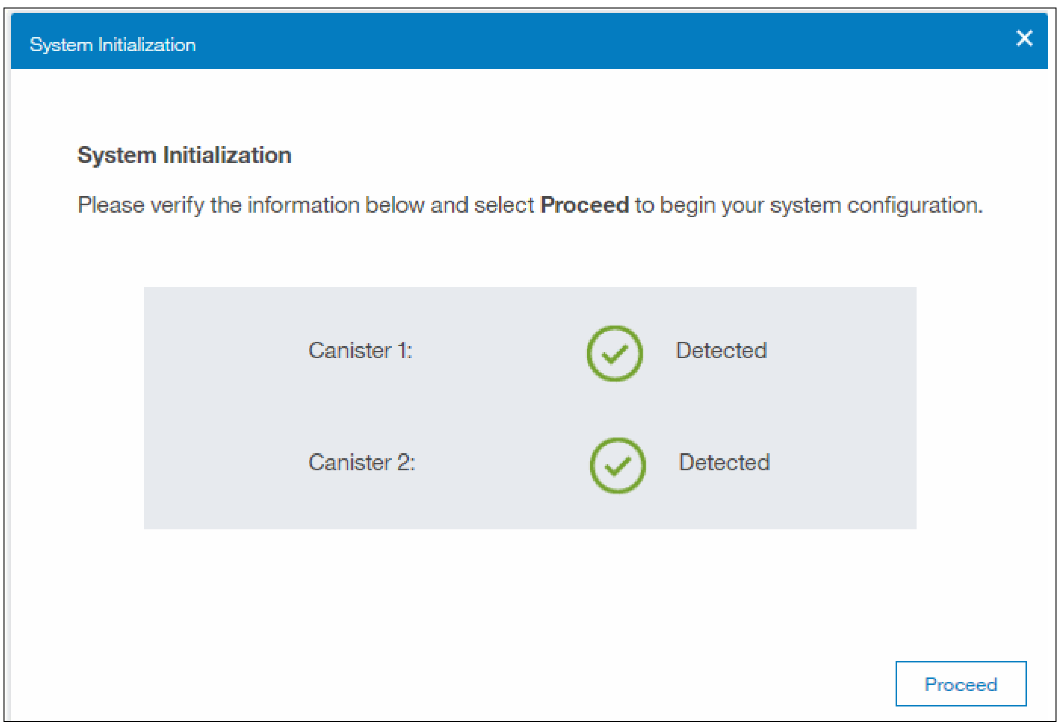


Figure 6-46 System initialization pane

5. Click **Proceed**.

6. The System Initialization Welcome pane is displayed (Figure 6-47).

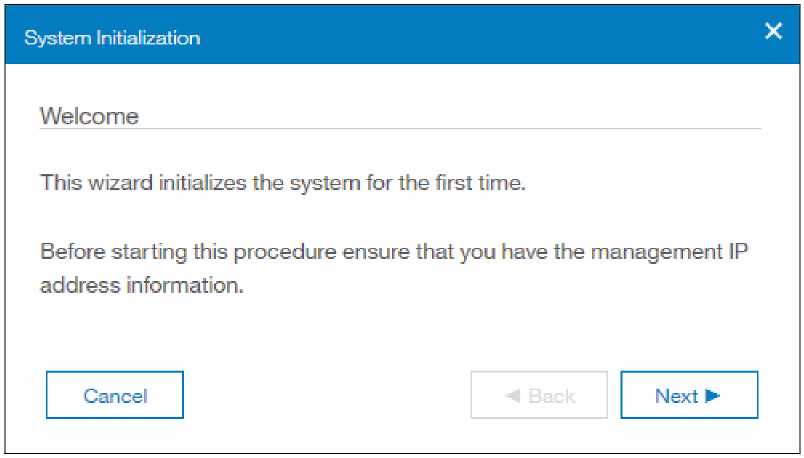


Figure 6-47 System initialization welcome pane

7. Click **Next**.
8. The System Initialization Welcome pane is displayed (Figure 6-48).

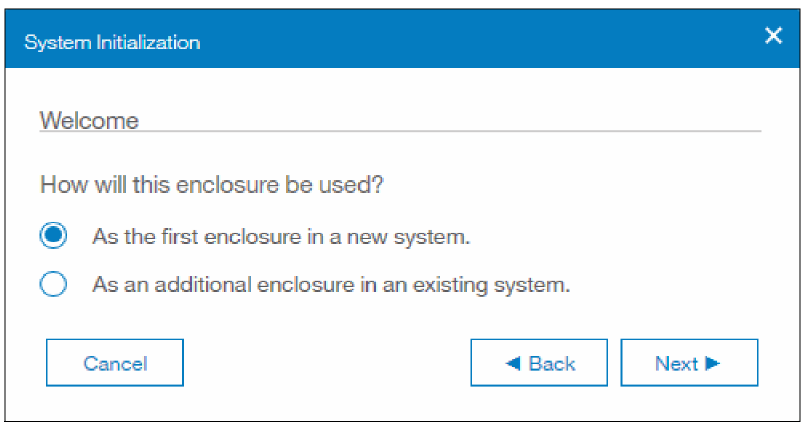


Figure 6-48 System initialization enclosure usage pane

9. Click **As the first enclosure in a new system** and then click **Next**.

10. The System Initialization Create a New System pane is displayed (Figure 6-49).

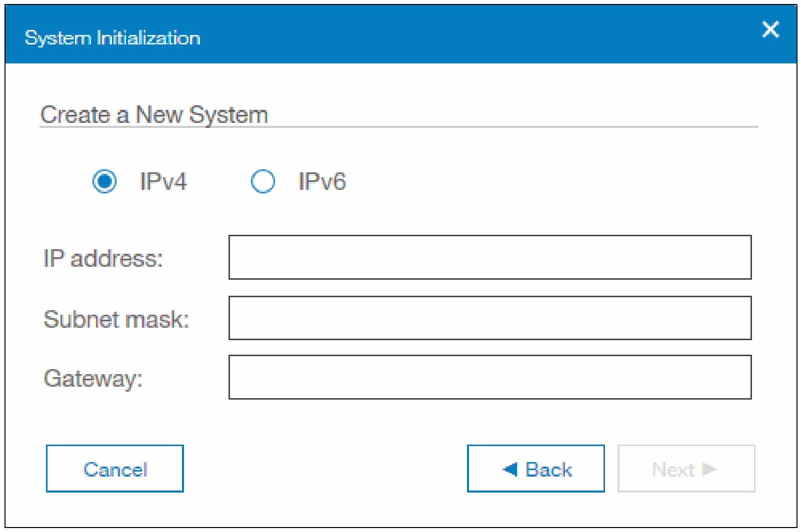


Figure 6-49 System initialization create a new system pane

11. Enter the information from system planning worksheets (Figure 6-50):
    a. Select **IPv4** or **IPv6**.
    b. In the **IP address** field, enter the management IP address.
    c. In the **Subnet mask** field, enter the subnet mask.
    d. In the **Gateway** field, enter the gateway IP address.
    e. Click **Next**.

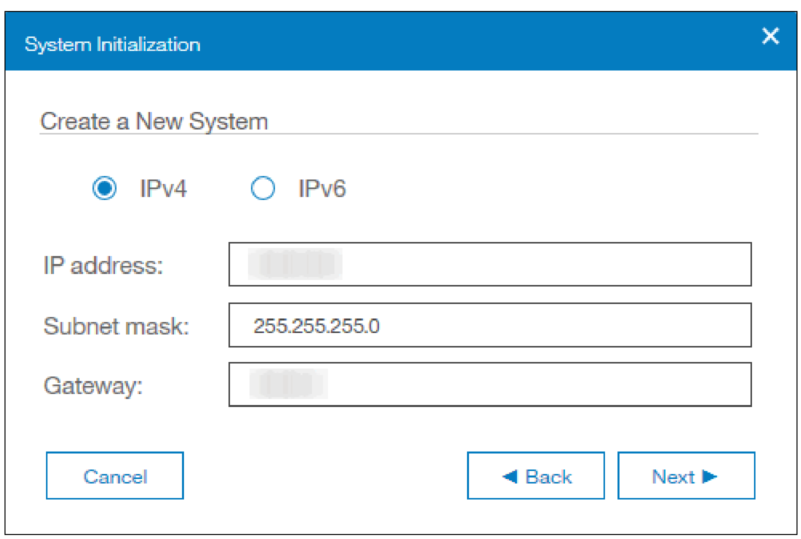


Figure 6-50 System initialization create a new system pane

12. The Task completed pane is displayed (Figure 6-51).

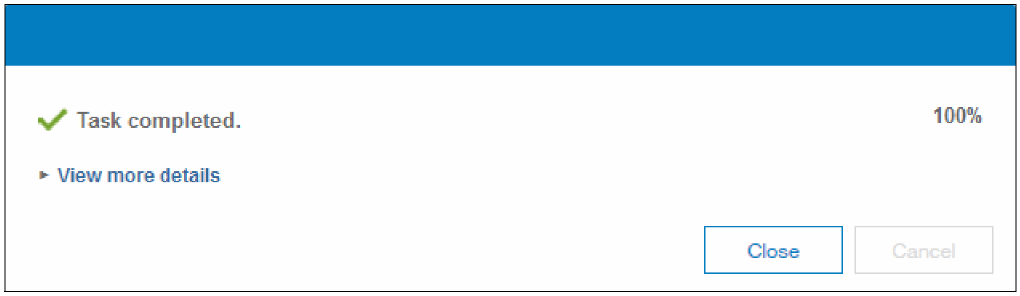


Figure 6-51 System initialization task completed pane

13. Click **Close**.
14. The System Initialization Restarting Web Server pane is displayed (Figure 6-52).

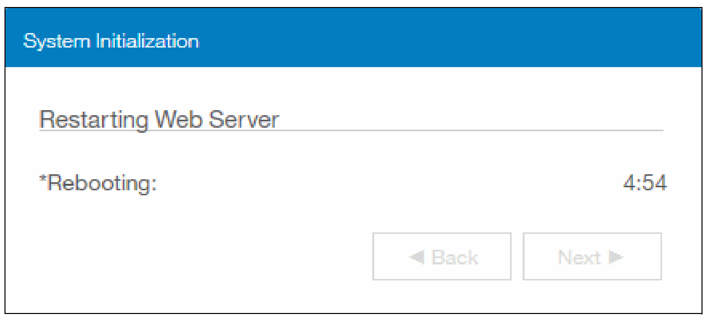


Figure 6-52 System initialization restarting web server pane

15. The System Initialization function implements a 5 minute timer to allow the web server to restart, When the timer reaches zero, click **Next** (Figure 6-53).

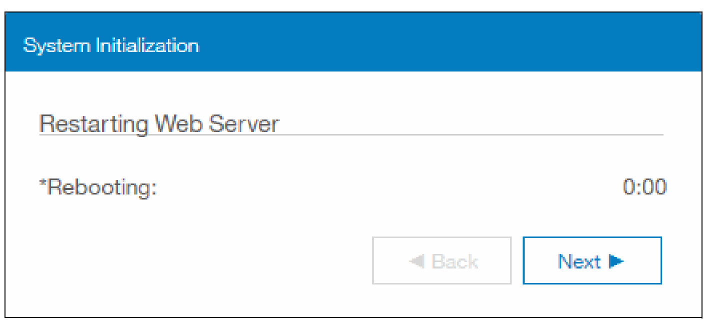


Figure 6-53 System initialization restarting web server pane with no time remaining

16. The System Initialization Summary pane is displayed (Figure 6-54 on page 205).

Important: *Do not* disconnect the ethernet cable connecting your laptop to the technician port on node canister 1 until system initialization has completed.

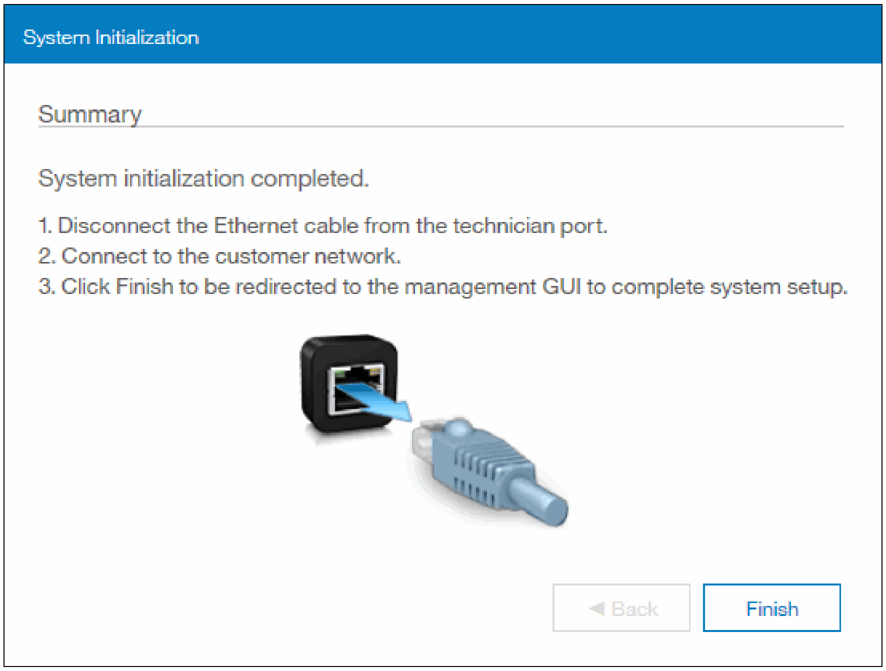


Figure 6-54 System initialization summary screen

17. Click **Finish**.

6.3.2 System initialization for additional enclosure in an existing system

Perform the following steps to initialize the system:

1. Configure the ethernet port on your laptop to use Dynamic Host Configuration Protocol (DHCP).

   Connect the laptop's ethernet port to the technician port of the upper node canister in the control enclosure. See Figure 6-55.

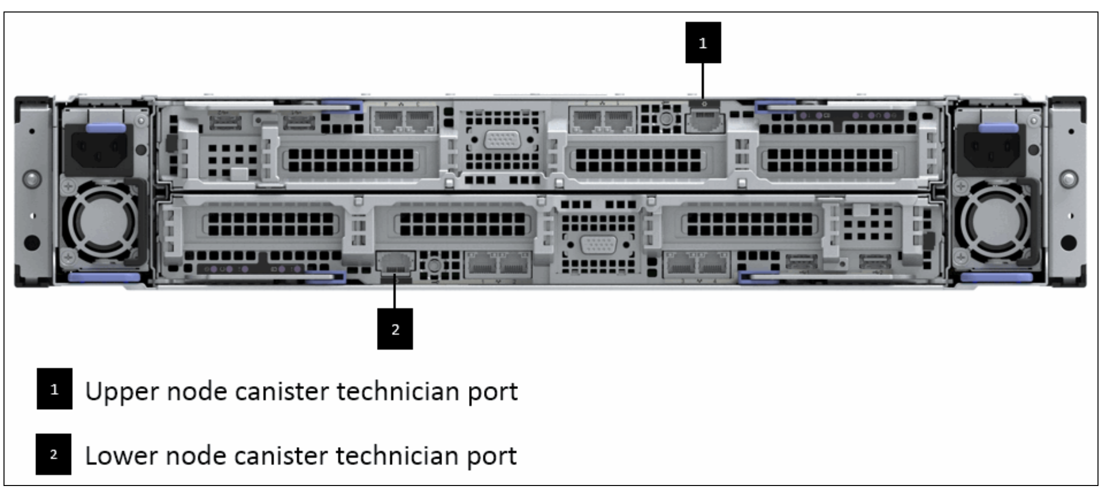


Figure 6-55 Control enclosure technician ports

2. Open a web browser and enter `http://install` in the URL field.

3. Wait for the System Initialization pane to be displayed (Figure 6-56).

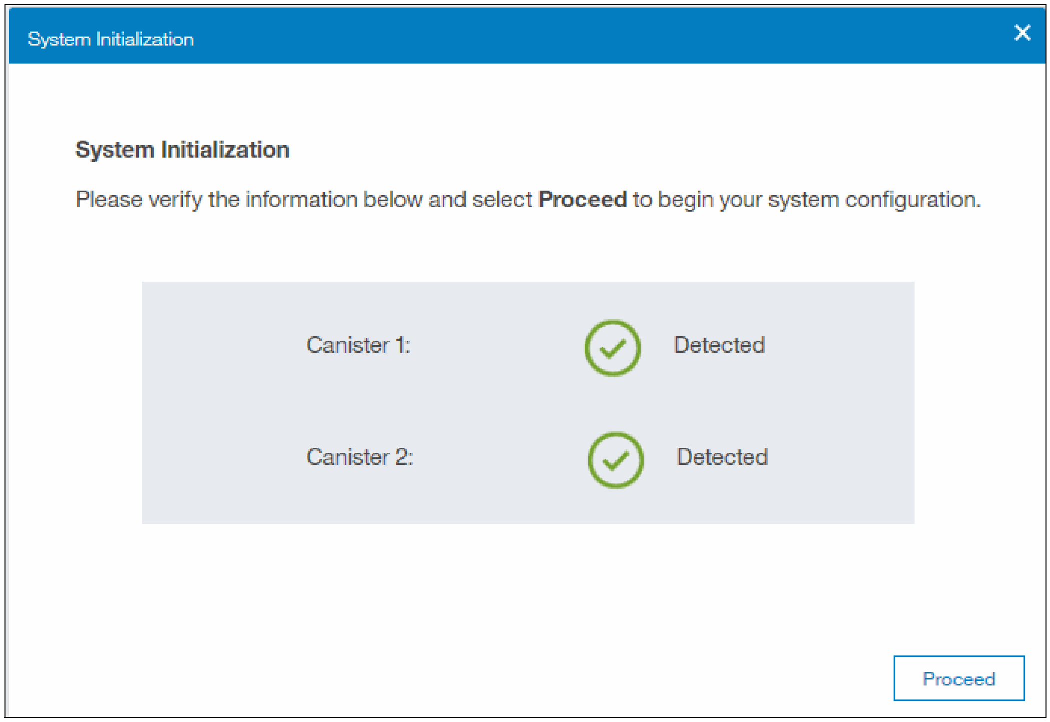


Figure 6-56 System initialization pane

4. Click **Proceed**.
5. The System Initialization Welcome pane is displayed (Figure 6-57).

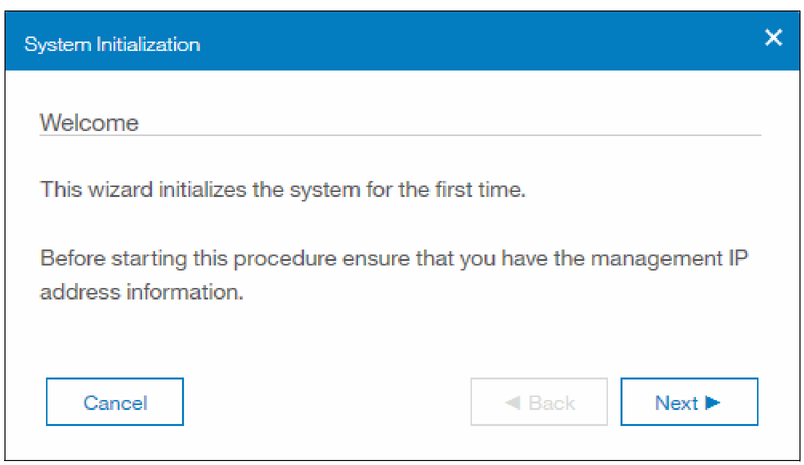


Figure 6-57 System initialization welcome pane

6. Click **Next**.

7. The System Initialization Welcome pane is displayed (Figure 6-58).

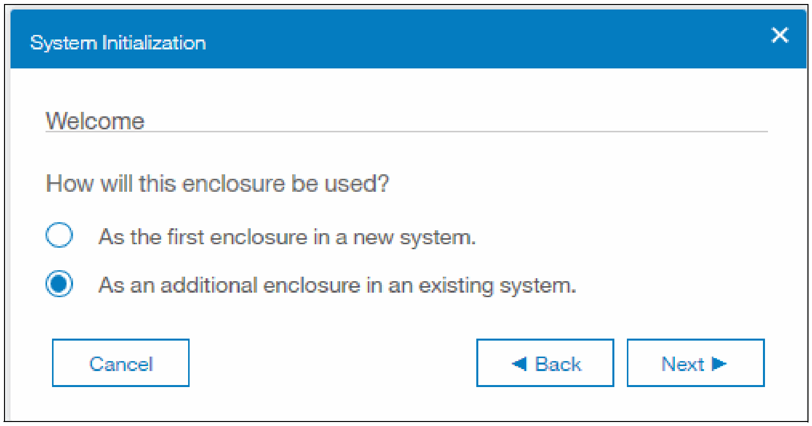


Figure 6-58 System initialization enclosure usage pane

8. Click **As an additional enclosure in an existing system** and then click **Next**.
9. The System Initialization Expand System pane is displayed (Figure 6-59).

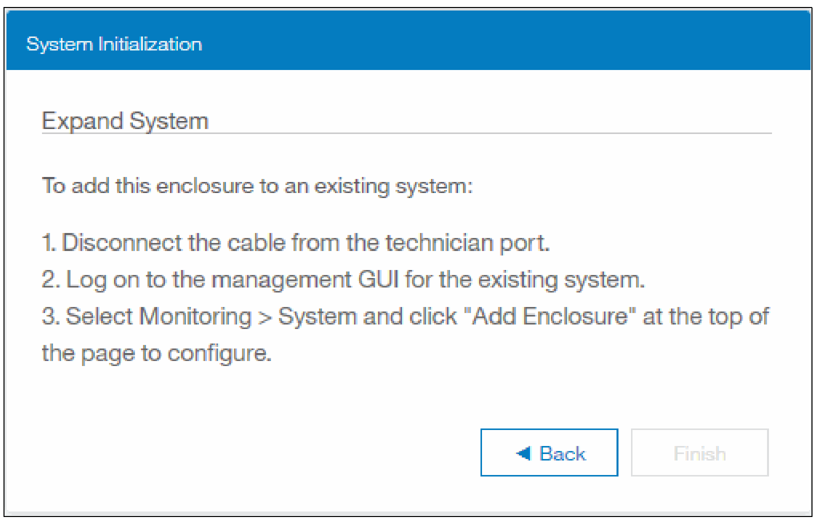


Figure 6-59 System initialization expand system pane

10. The SSR actions to initialize and setup the system are complete. The actions to add the enclosure to an existing system are completed by the customer. See Chapter 5, “Scalability” on page 117 for more information.

6.4 Service setup

> **Important:** The information in this section is intended only for IBM authorized service providers. Customers need to consult the terms of their warranty to determine the extent to which they should attempt any IBM FlashSystem hardware installation.
>
> **Note:** Refer to the system planning worksheets provided by the customer for the information required to setup the system.

Complete the following steps:

1. Open a web browser and enter `http://install` in the URL field.
2. The FlashSystem 9100 Storage Management login screen displays (Figure 6-60).

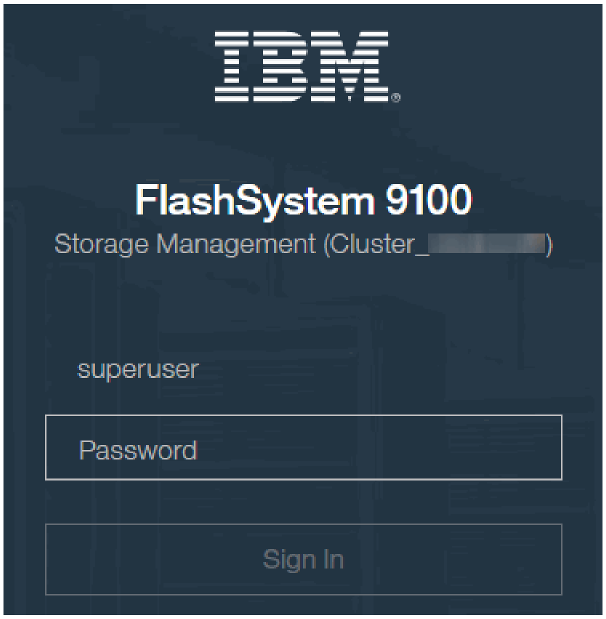


Figure 6-60 FlashSystem 9100 storage management login screen

3. Enter `passw0rd` in the **Password** field and click **Sign In**.
4. The Welcome to Service Setup screen is displays (Figure 6-61).

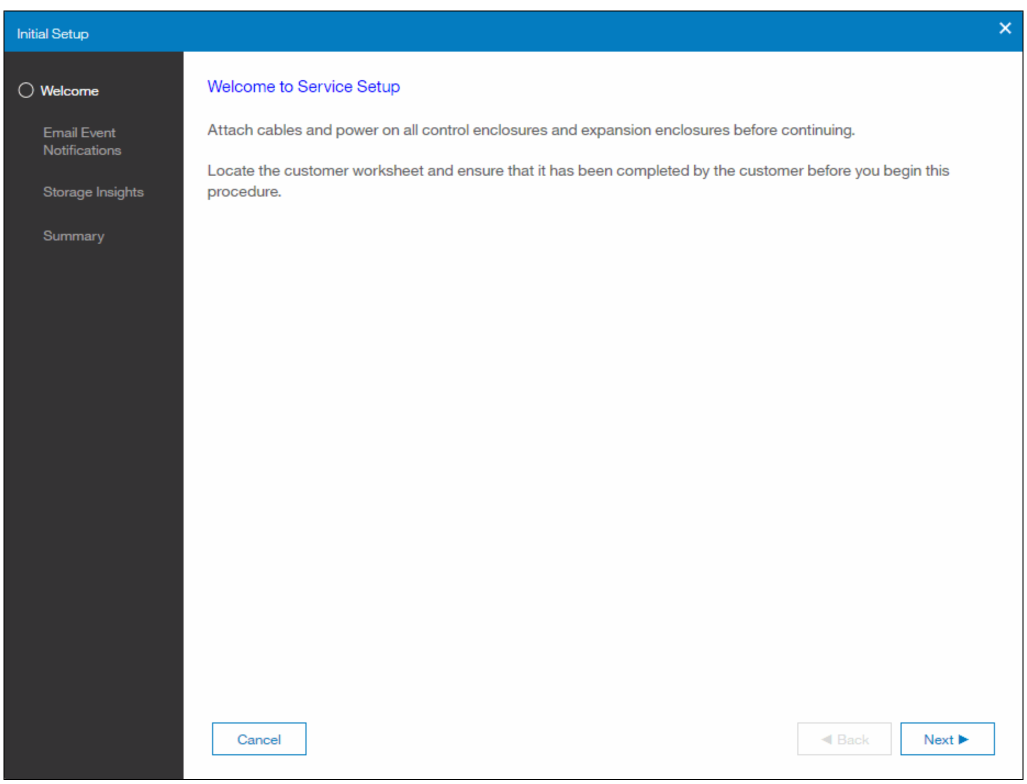


Figure 6-61 Welcome to service setup screen

5. Click **Next**.
6. The Email Event Notifications screen is displayed (Figure 6-62).

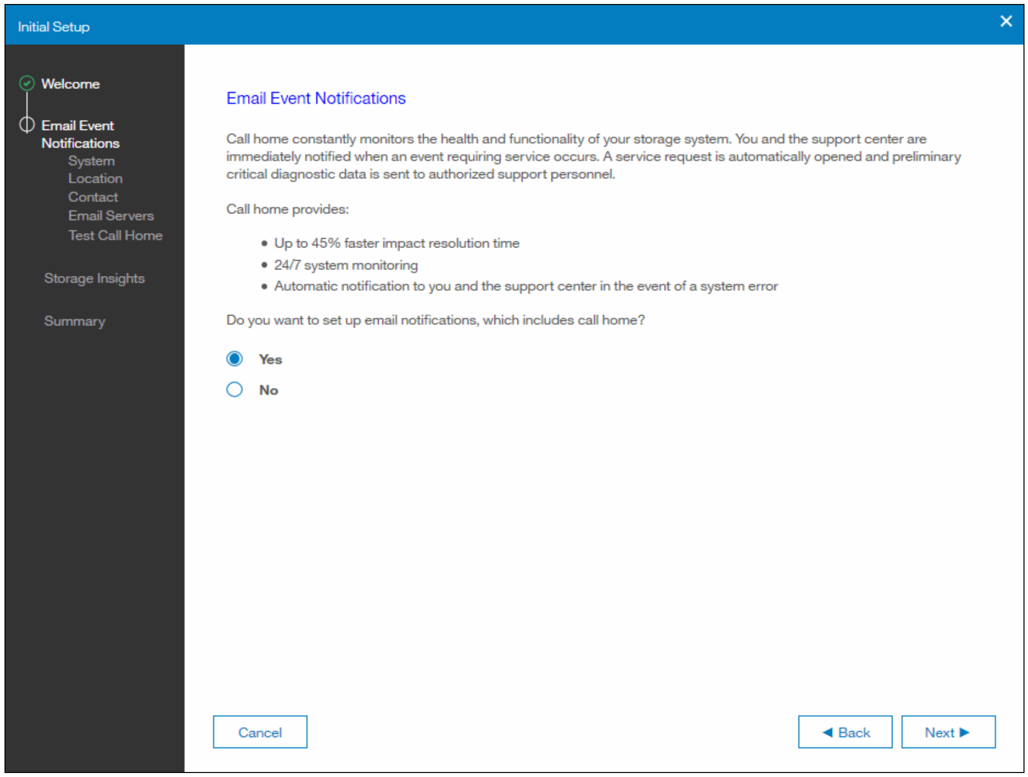


Figure 6-62 Email events notifications screen

7. Select **Yes** or **No** and then click **Next**.

8. The System Location screen displays (Figure 6-63).

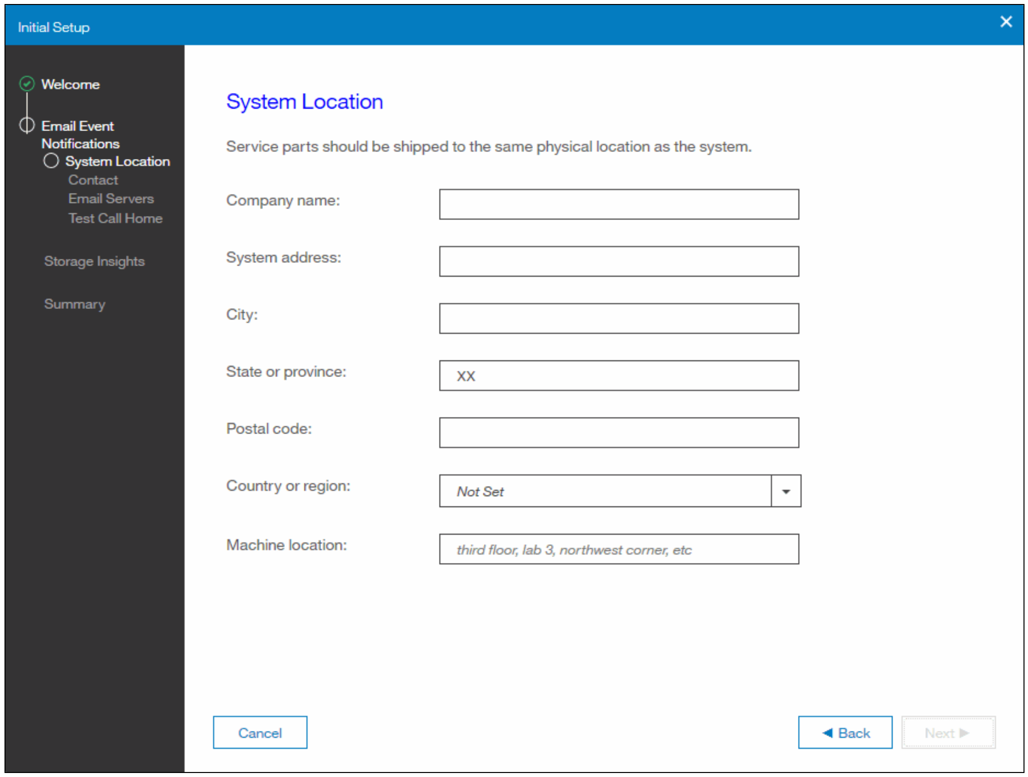


Figure 6-63 System location screen

9. Enter the system location information in the fields on the screen and click **Next**.

10. The Contact screen is displayed (Figure 6-64).

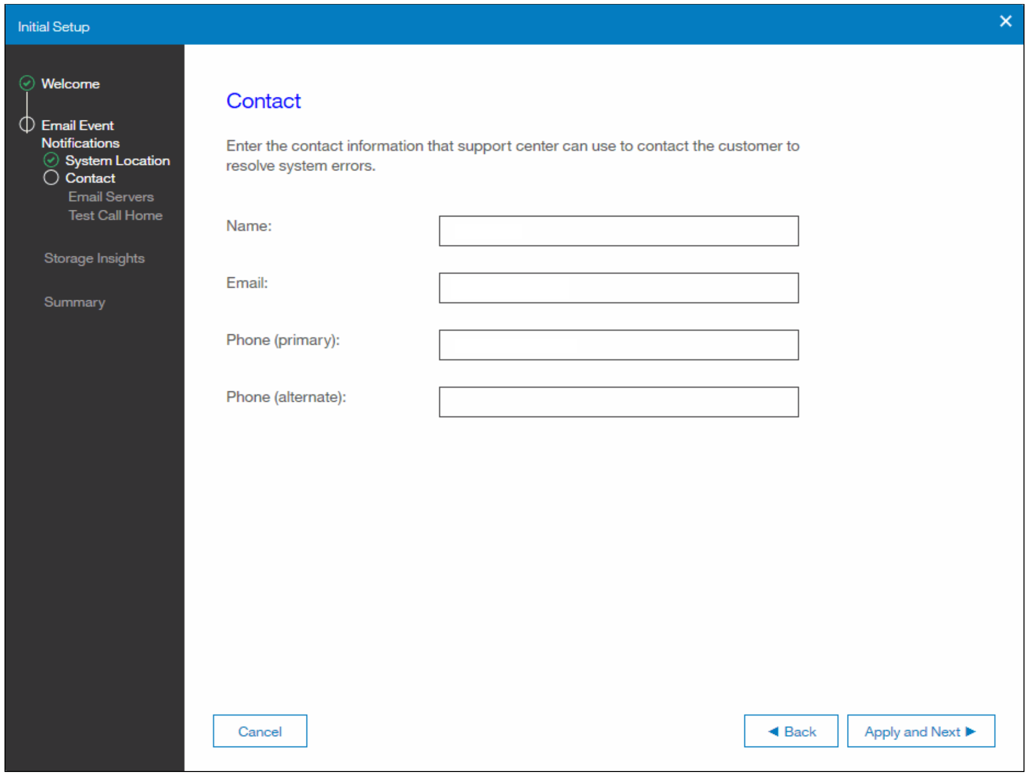


Figure 6-64 Contact screen

11. Enter the contact information in the fields on the screen and click **Apply and Next**.
12. The Configuring Email Settings status pane is displayed (Figure 6-65).

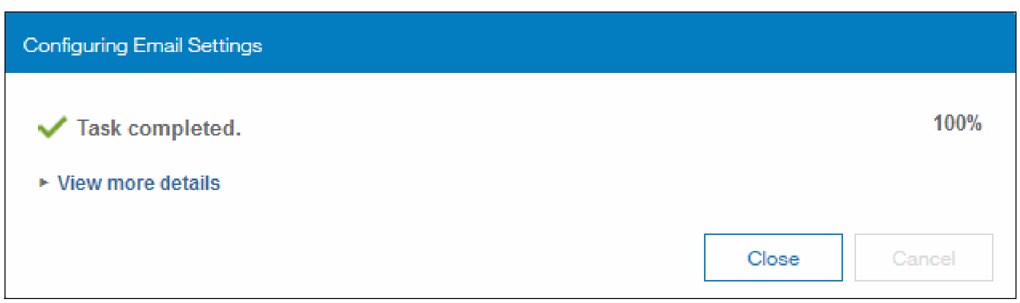


Figure 6-65 Configuring email settings status pane

13. Click **Close**.

14. The Email Servers screen is displayed (Figure 6-66).

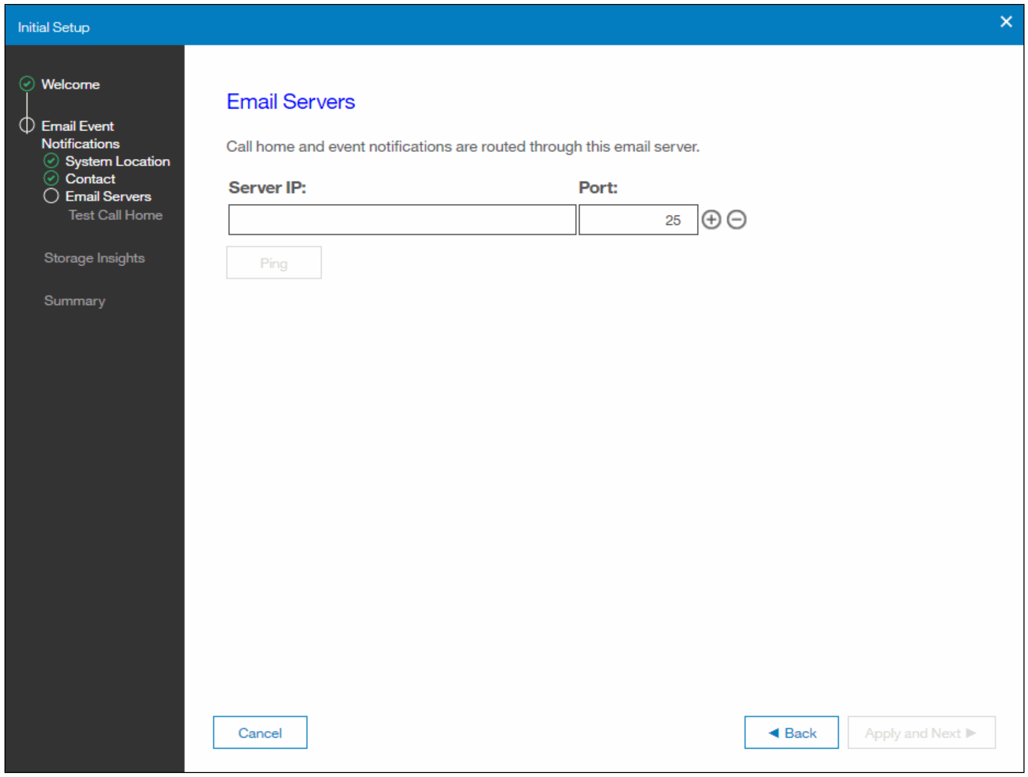


Figure 6-66 Email servers screen

15. Enter the IP address and port of the SMTP server in the **Server IP** and **Port** fields.
16. Click **Ping** to test the connection to the SMTP server.
17. Click **Apply and Next**.
18. The Configuring Email Settings status pane is displayed (Figure 6-67).

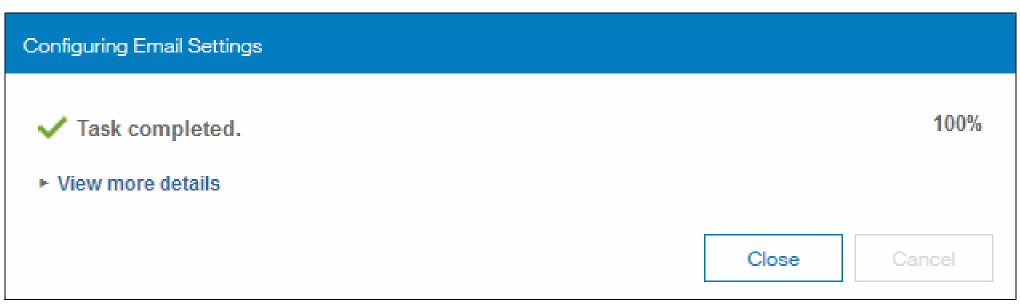


Figure 6-67 Configuring email settings status pane

19. Click **Close**.

20.The Sending Test Email status pane is displayed (Figure 6-68).

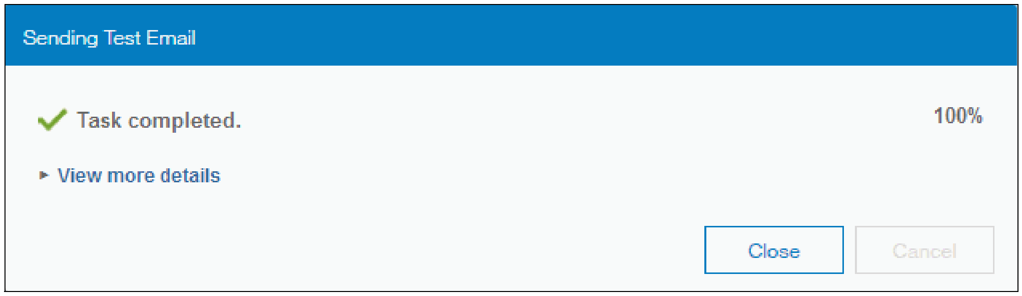


Figure 6-68 Sending test email status pane

21.Click **Close**.

22.The Test Call Home screen is displayed (Figure 6-69).

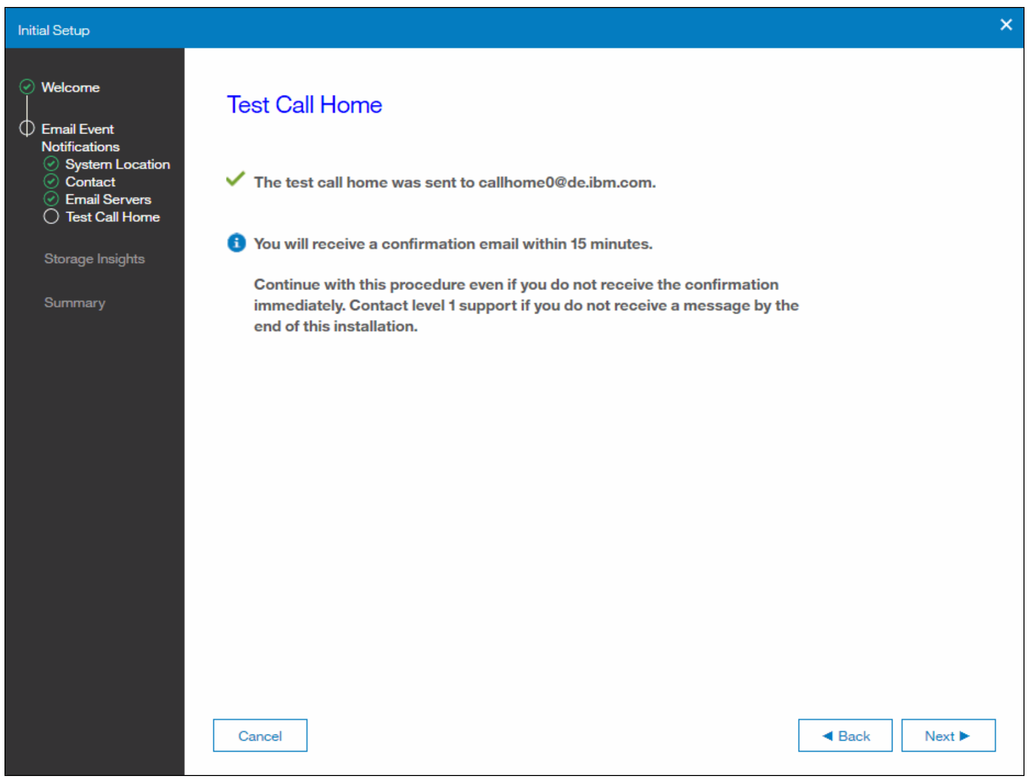


Figure 6-69 Test call home screen

23.Click **Next**.

24. The Storage Insights screen is displayed (Figure 6-70).

> **Note:** Your laptop may not be able to communicate with the internet while connected to the technician port on node canister 1. The customer will be prompted to set up Storage Insights during initial customer setup.

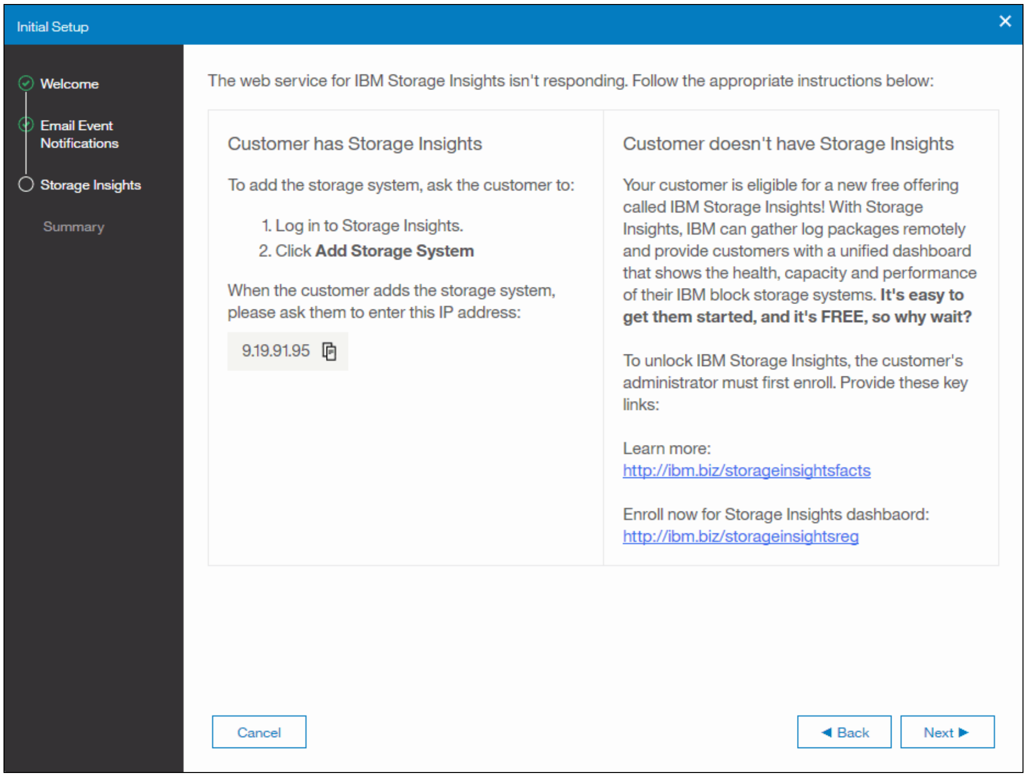


Figure 6-70 Storage Insights screen

25. Click **Next**.

26.The Summary screen is displayed (Figure 6-71).

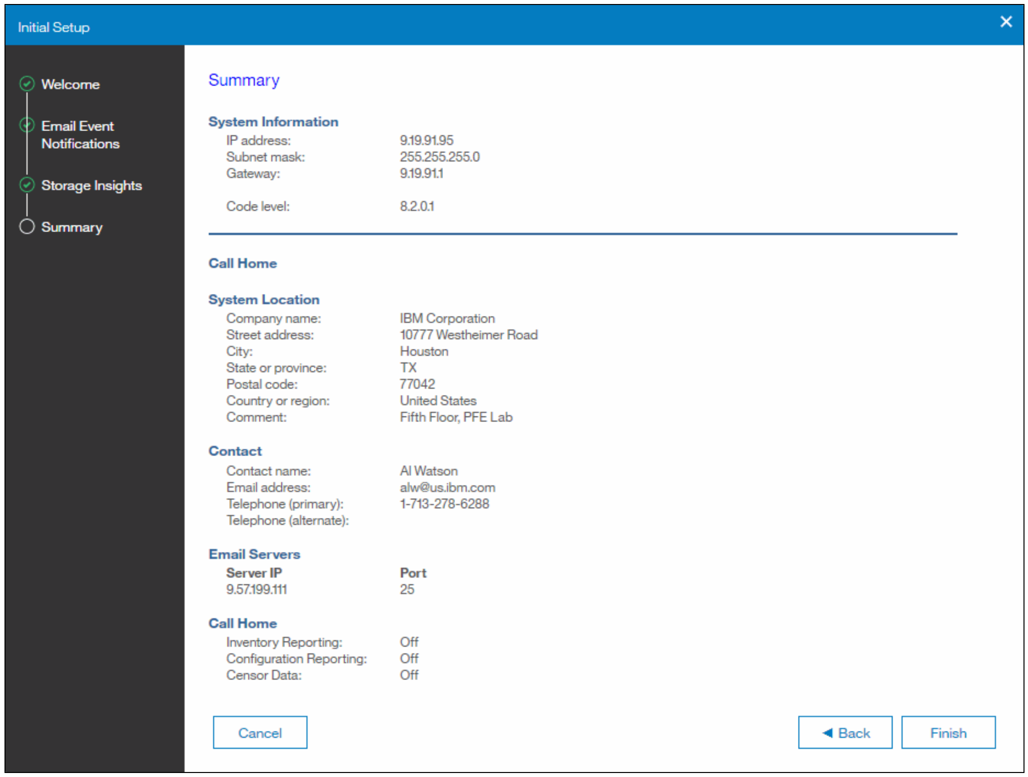


Figure 6-71 Summary screen

27.Click **Finish**.

28.The System Initialization Task completed pane is displayed (Figure 6-72).

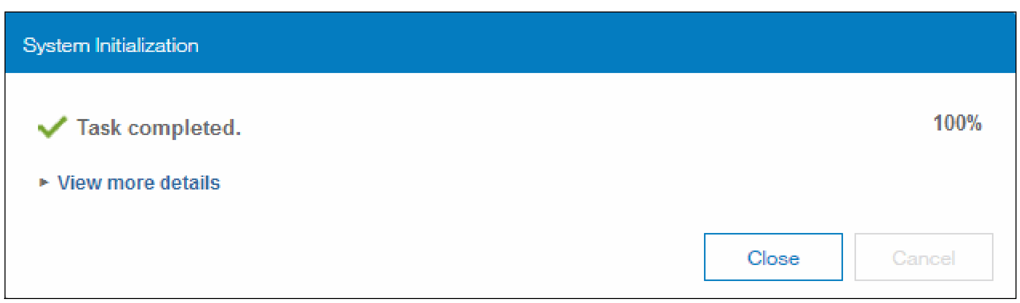


Figure 6-72 System initialization task completed pane

29.Click **Close**.

30. The Setup Complete screen is displayed (Figure 6-73).

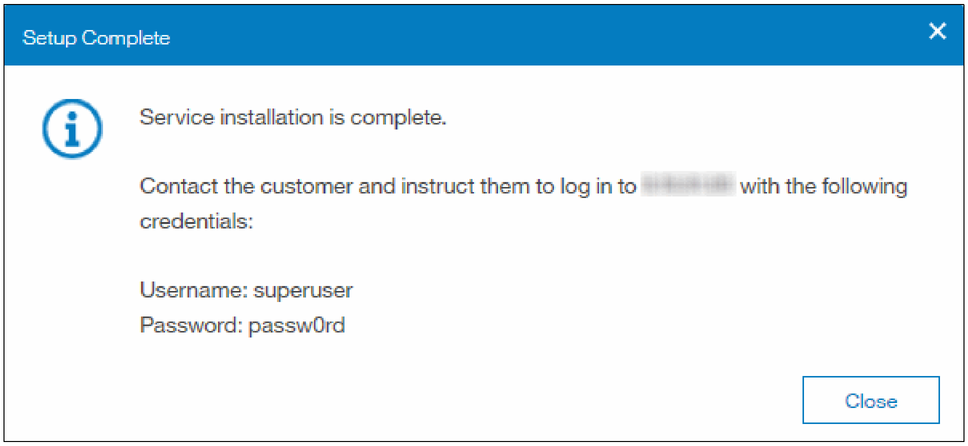


Figure 6-73 Setup Complete screen

31. Click **Close**.
32. Disconnect the ethernet cable from the technician port on node canister 1, and from your laptop.
33. The IBM SSR actions to initialize and set up the system are complete.

6.5 Initial customer setup

To perform the initial setup, complete the following steps:

1. Open a supported web browser and enter `https://<system management IP address>` in the URL field.
2. The FlashSystem 9100 Storage Management login screen is displayed (Figure 6-74).

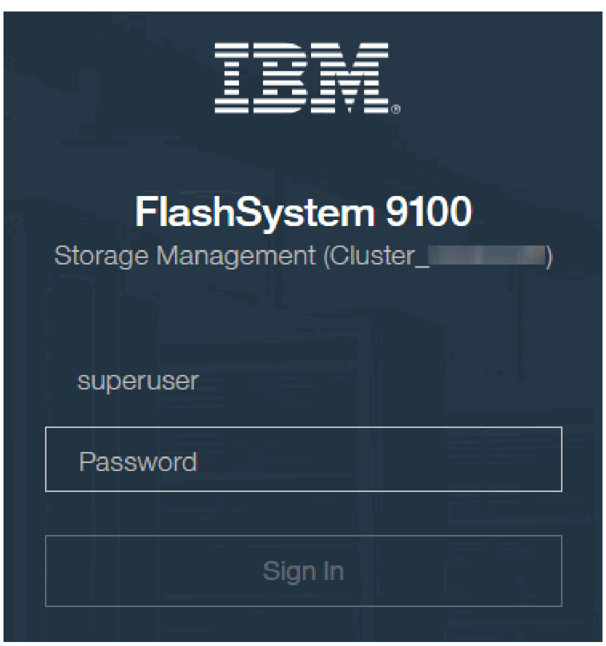


Figure 6-74 FlashSystem 9100 Storage Management login screen

3. Enter `passw0rd` (with a zero) in the **Password** field and click **Sign In**.
4. The Welcome screen is displayed (Figure 6-75).

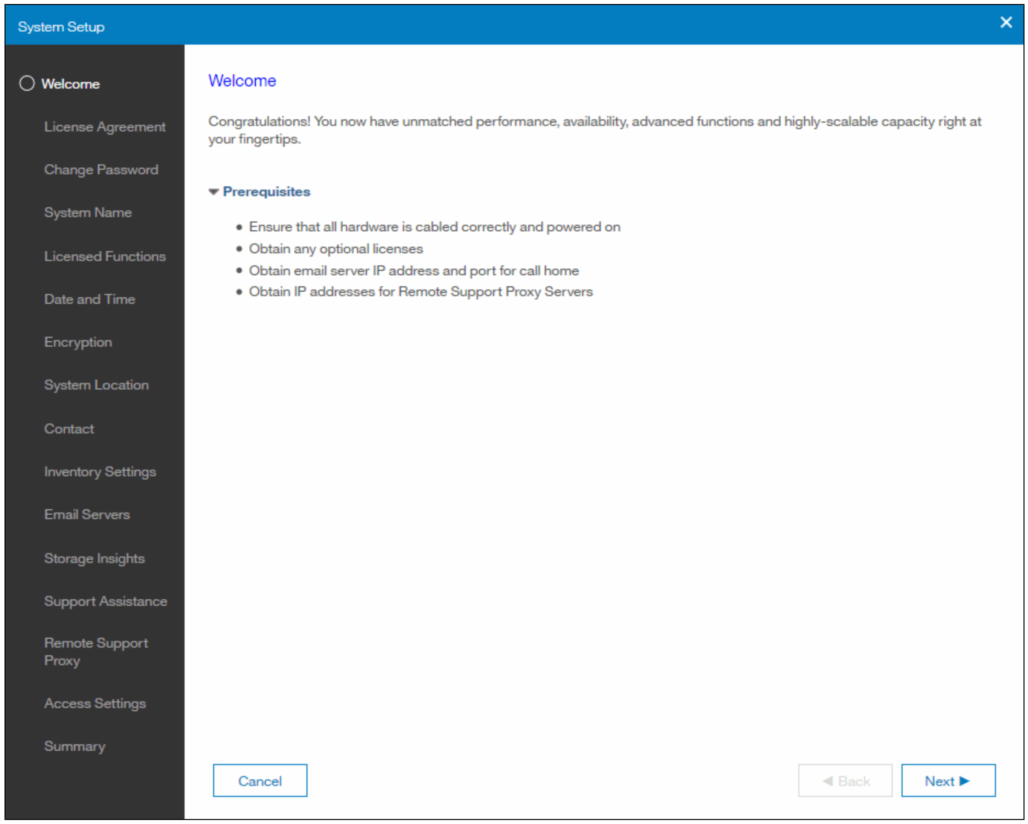


Figure 6-75 Welcome screen

5. Click **Next**.

6.5.1 License agreement

You must read and agree to the terms in the license agreement shown in Figure 6-76 before continuing.

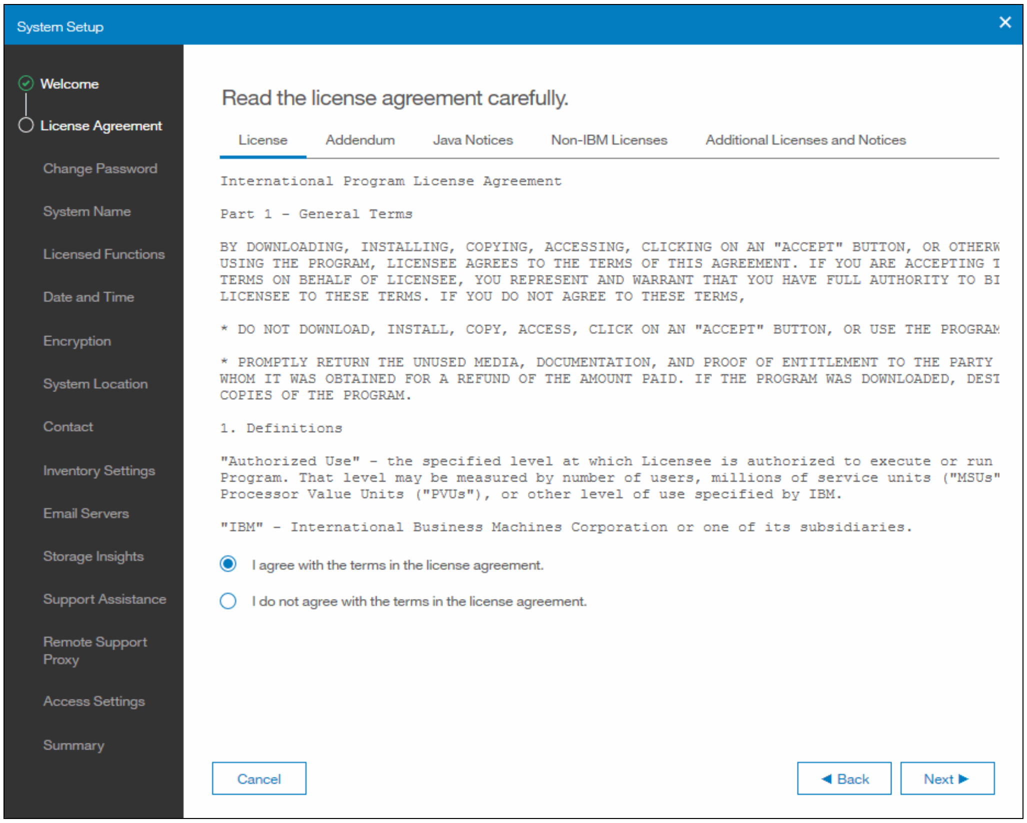


Figure 6-76 License agreement screen

Complete the following steps:

1. Read the license agreement (Figure 6-76).
2. Select **I agree with the terms in the license agreement.**
3. Click **Next**.

6.5.2 Password change

The Change Password screen (Figure 6-77) allows you to change the default password.

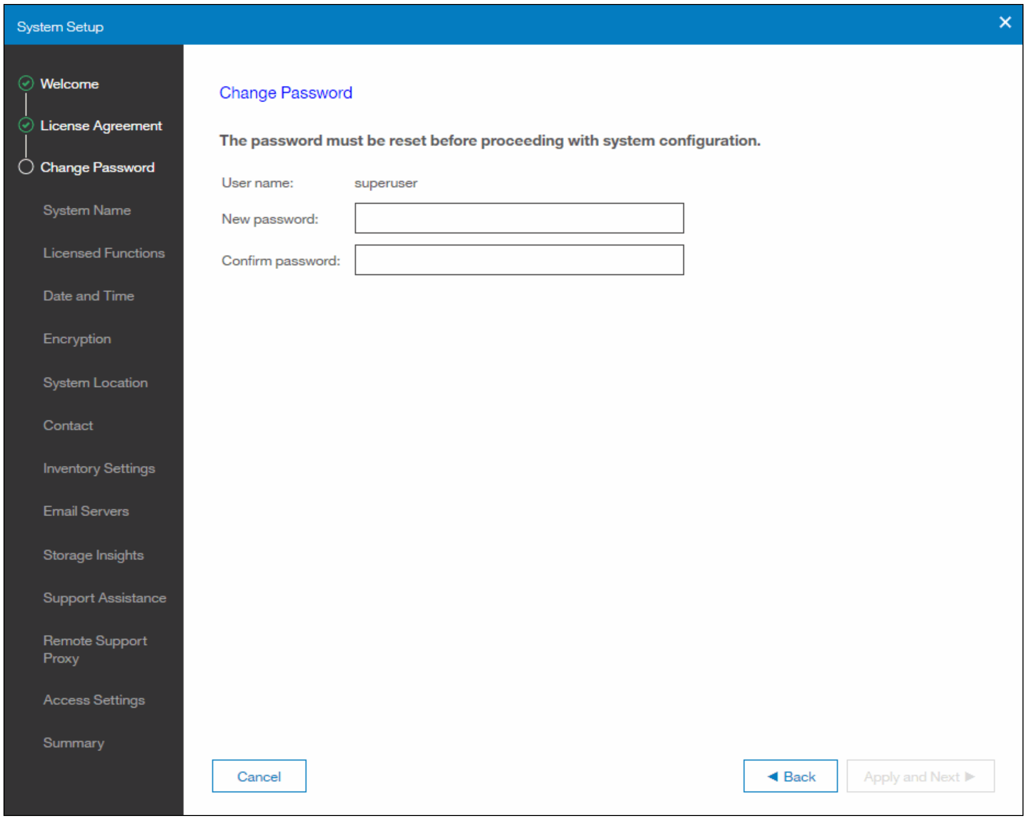


Figure 6-77 Change password screen

Complete the following steps to change the default password:

1. Enter the new password in the **New password** and the **Confirm password** fields.
2. Click **Apply and Next**.
3. The Change Password statue pane is displayed (Figure 6-78).

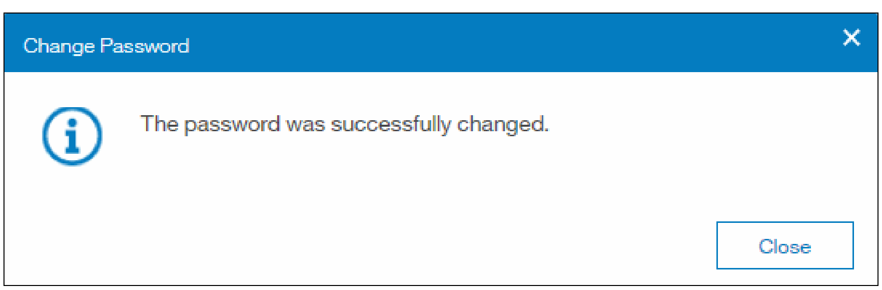


Figure 6-78 Change password status pane

4. Click **Close**.

6.5.3 System name

The System Name screen (Figure 6-79) allows you to specify a name for the system.

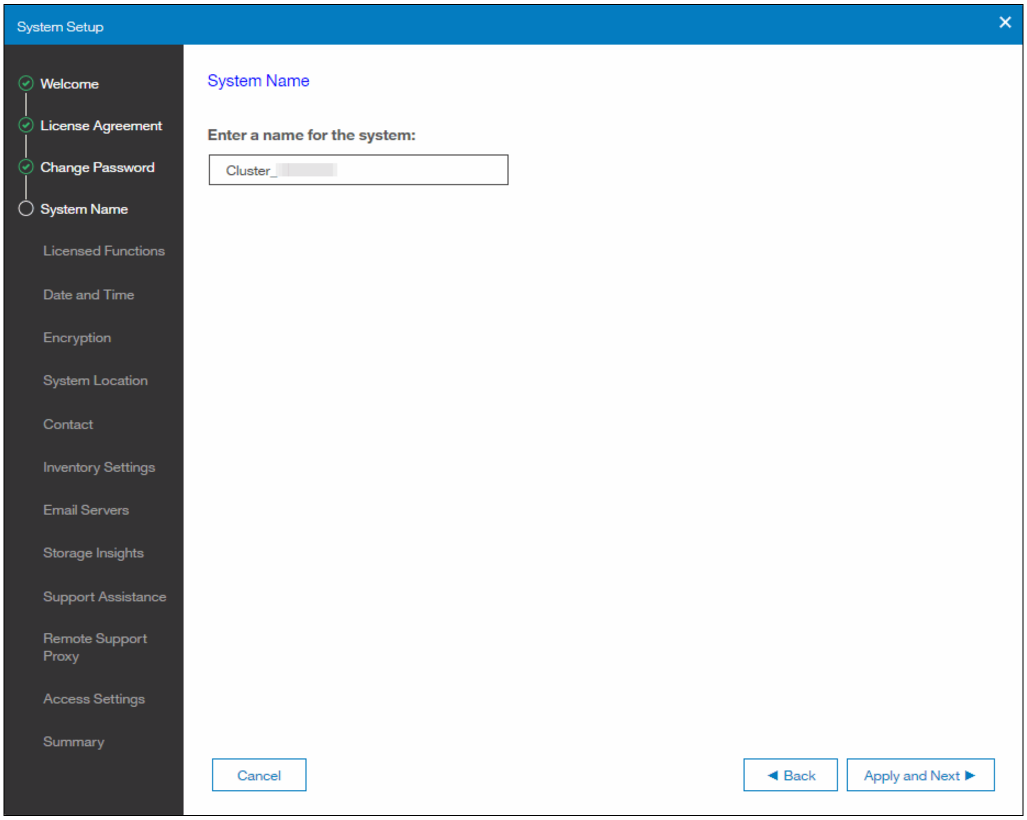


Figure 6-79 System name screen

Complete the following steps to change the system name:

1. Enter the system name in the **Enter a name for the system** field.
2. Click **Apply and Next**.
3. The Modify System Properties status pane is displayed (Figure 6-80).

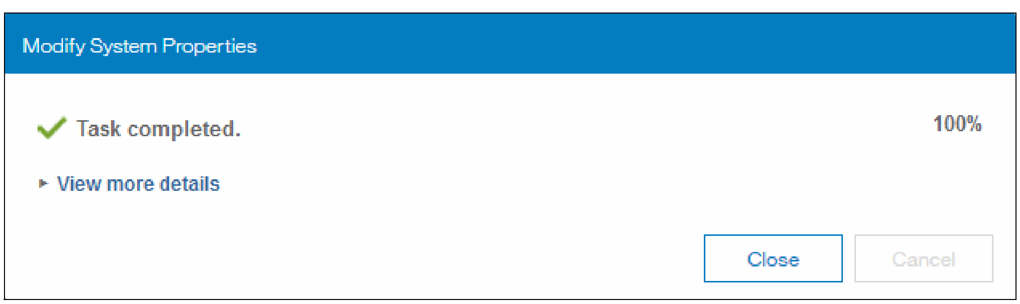


Figure 6-80 Modify system properties status pane

4. Click **Close**.

6.5.4 Licensed functions

Licensed functions must be configured before they can be used. The Licensed Functions screen (Figure 6-81) allows you to configure the licensed functions. To provide the correct values for the licensed functions, refer to the licenses feature codes that you purchased. See “Licensing and features” on page 107 for more information.

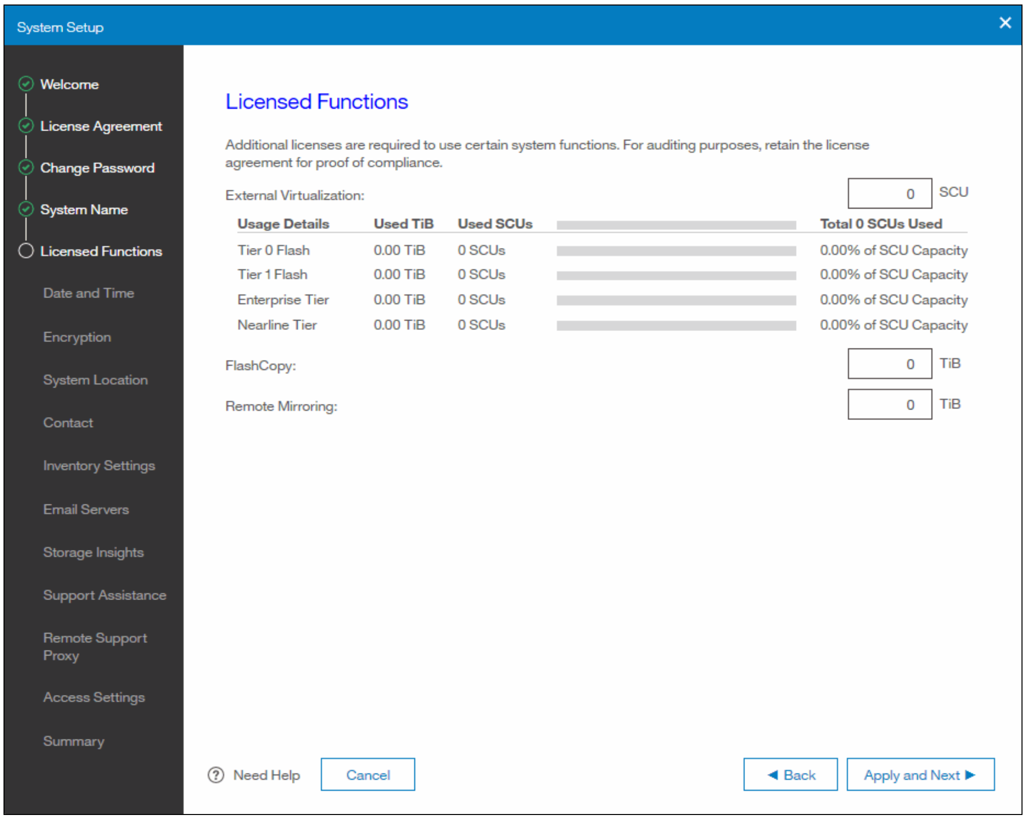


Figure 6-81 Licensed functions screen

Complete the following steps to configure the licensed functions:

1. Enter the values in the **External Virtualization**, **FlashCopy**, and **Remote Mirroring** fields.
2. Click **Apply and Next**.

6.5.5 Date and time

The date and time can be set manually or using an NTP server (Figure 6-82).

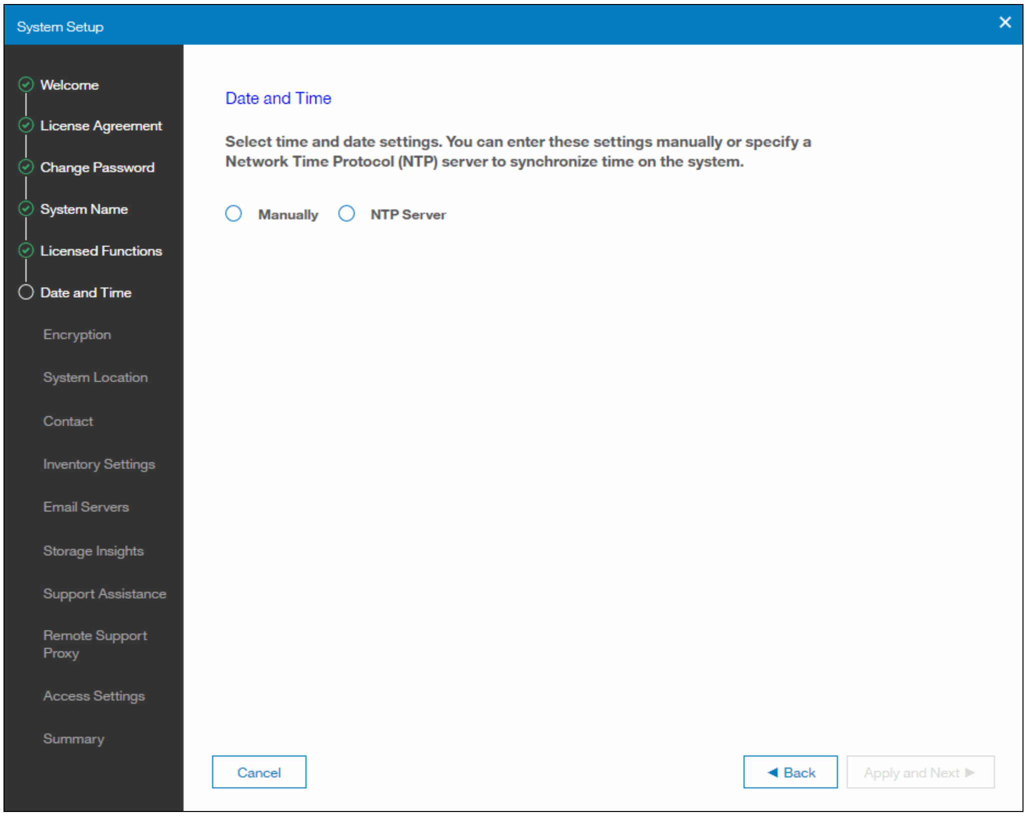


Figure 6-82 Date and Time screen

Setting the date and time manually

To set the date and time, complete the following steps:

1. Select **Manually** (Figure 6-83).

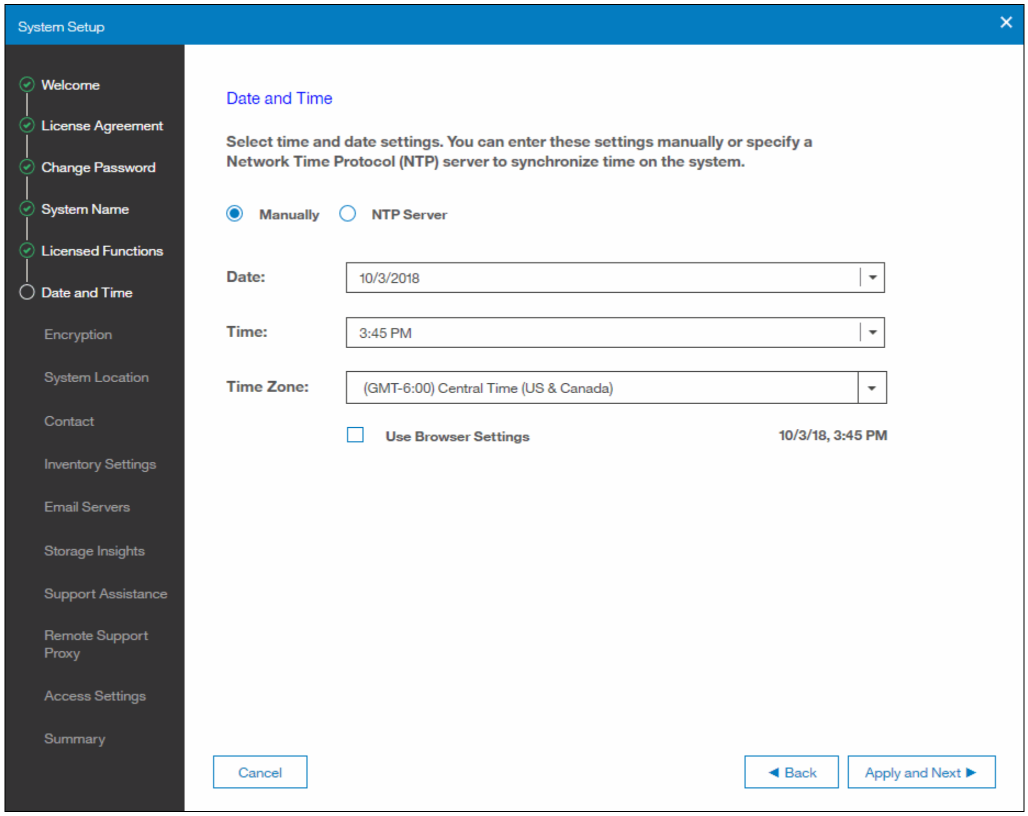


Figure 6-83 Setting the date and time manually

2. To set the date and time using your browser settings, select the **Use Browser Settings** check box and click **Apply and Next**.
3. To specify the date and time, select the date, time, and time zone from the lists and click **Apply and Next.**
4. The Change Date and Time Settings status pane is displayed (Figure 6-84).

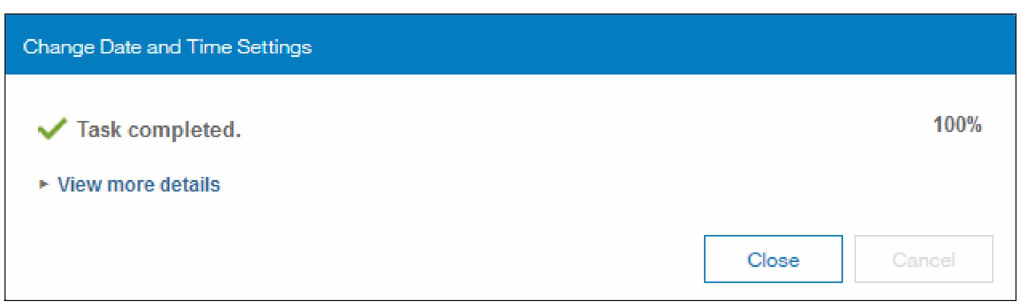


Figure 6-84 Change date and time setting status pane

5. Click **Close**.

Setting the date and time using an NTP server

Using an NTP server to set the date and time is the preferred method. Complete the following steps to set the date and time using an NTP server:

1. Select **NTP Server** (Figure 6-85).

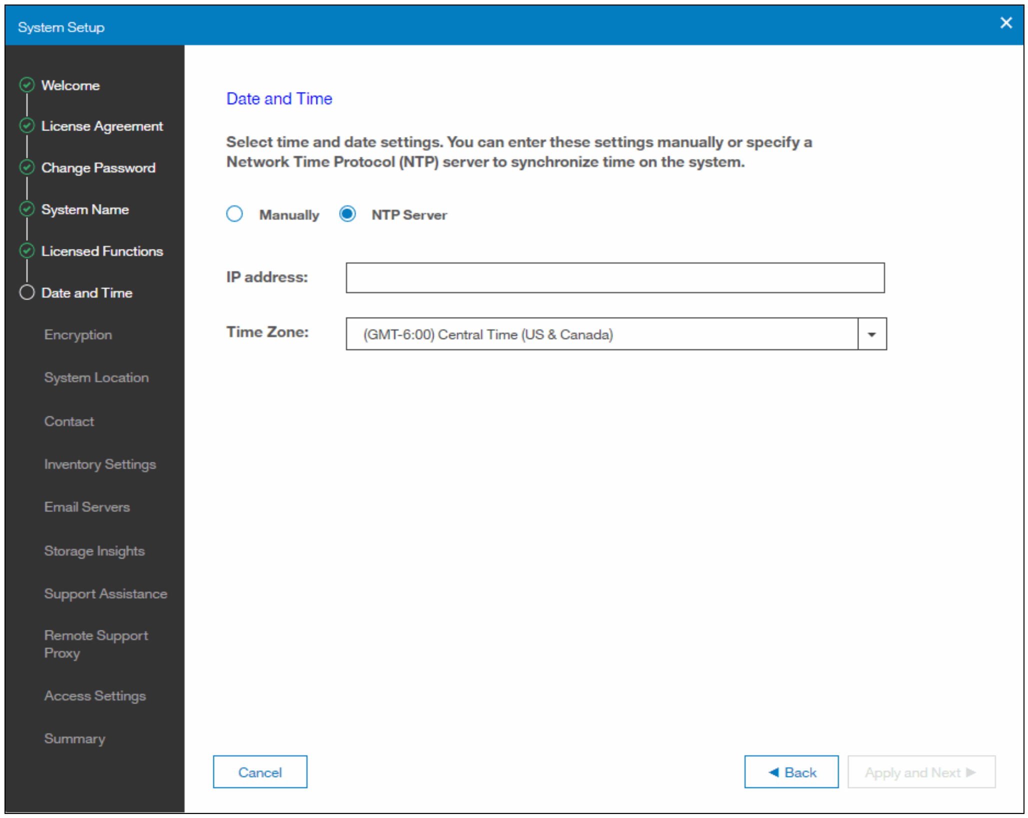


Figure 6-85 Setting the date and time using a NTP server

2. In the **IP address** field, enter the IP address of the NTP server.
3. From the **Time Zone** list, select the time zone.
4. Click **Apply and Next**.
5. The Change Date and Time Setting status pane is displayed (Figure 6-86).

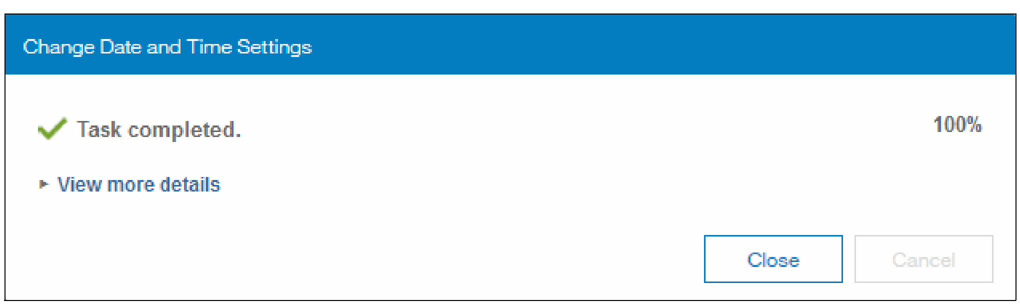


Figure 6-86 Change date and time settings status pane

6. Click **Close**.

6.5.6 Encryption

To use encryption on the system, you must purchase an encryption license and activate the license on the system. The Encryption screen (Figure 6-87) allows you to specify if the encryption feature was purchased for the system.

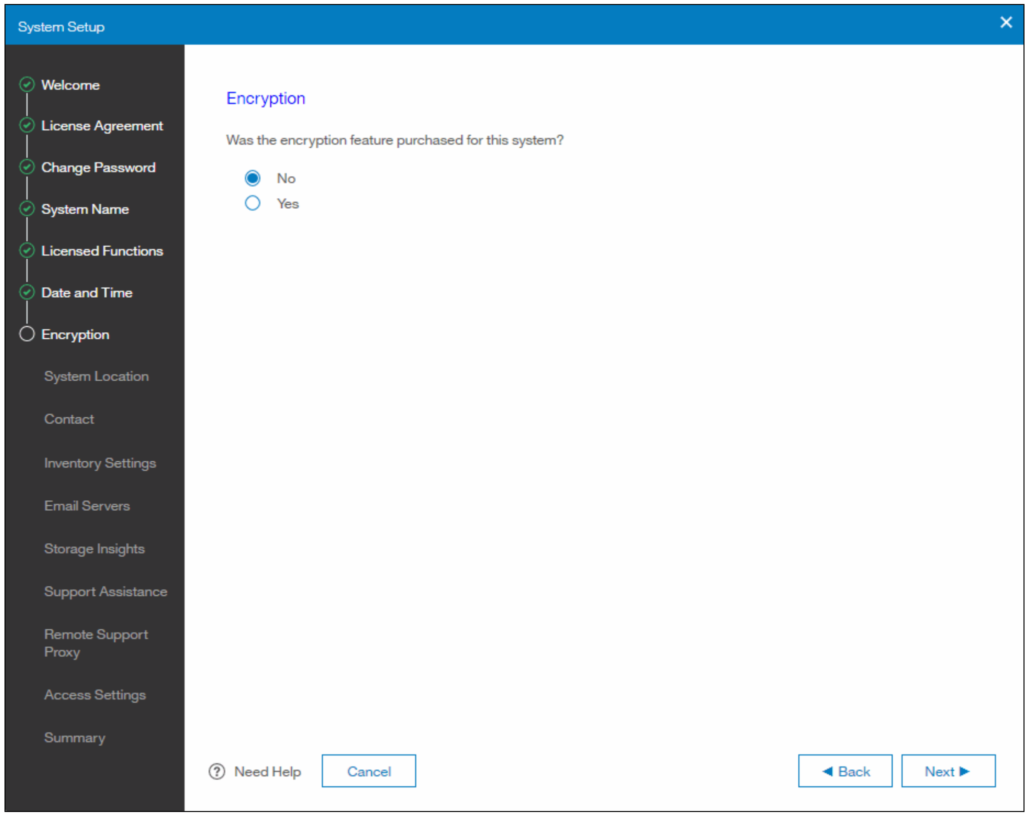


Figure 6-87 Encryption screen

If the encryption feature was not purchased for the system, select **No** and click **Next**.

If the encryption feature was purchased for the system, select **Yes**.

The encryption feature license can be activated automatically or manually. "Activating the encryption feature automatically" on page 226 describes how to activate the encryption feature license automatically. "Activating the encryption feature manually" on page 228 describes how to activate the encryptions feature license manually.

Activating the encryption feature automatically

To activate the encryption feature automatically, complete the following steps:

1. Select the enclosure for which the encryption feature is to be activated (Figure 6-88 on page 226).
2. Select **Actions** → **Activate License Automatically** (Figure 6-88).

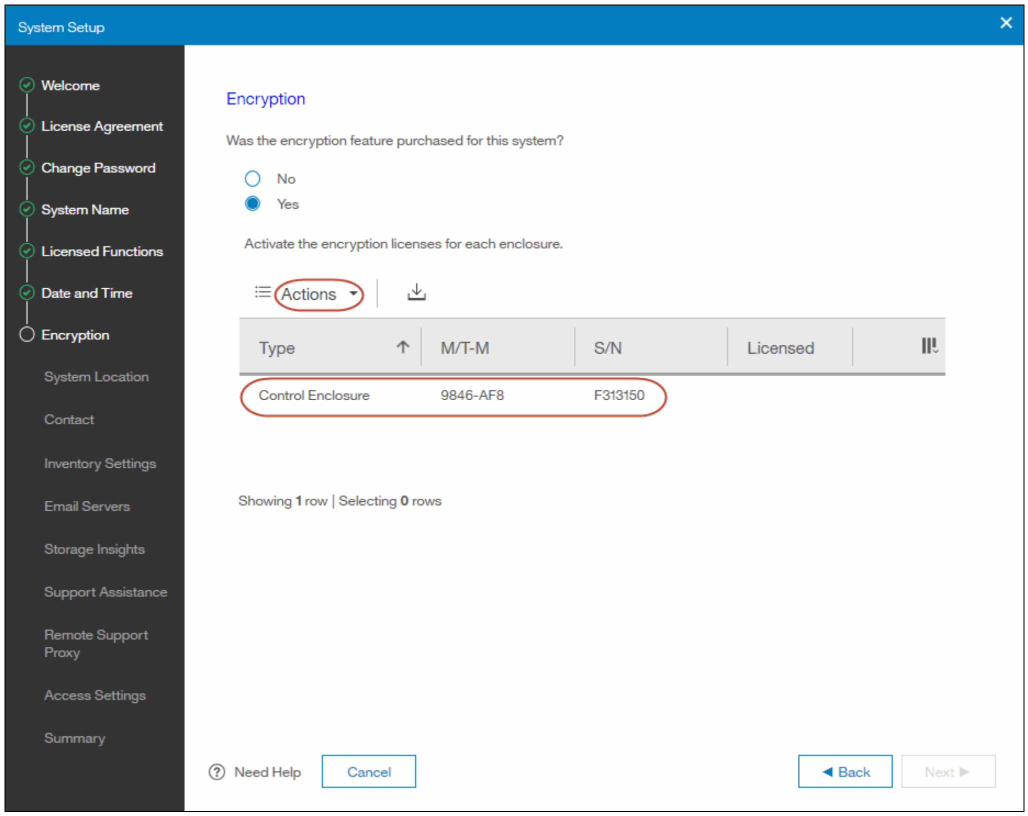


Figure 6-88 Activating the encryption feature license

3. In the **Enter the authorization code for control enclosure** field on the Activate License Automatically pane, enter the authorization code that is specific to the control enclosure that you selected (Figure 6-89).

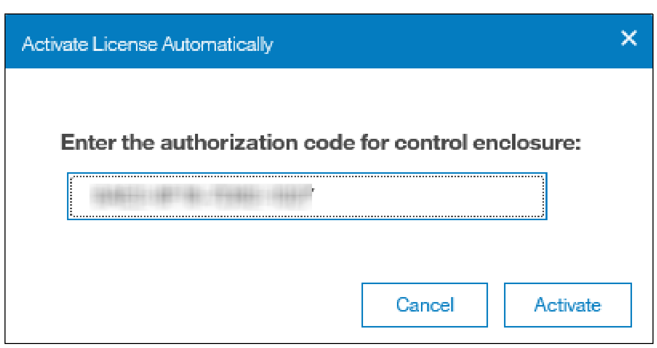


Figure 6-89 Activate license automatically pane with authorization code entered

4. Click **Activate**.

5. The system connects to IBM to verify the authorization code and retrieve the license key. After the license key has been retrieved, it is automatically applied. The Encryption screen is updated to indicate that the encryption feature is licensed (Figure 6-90).

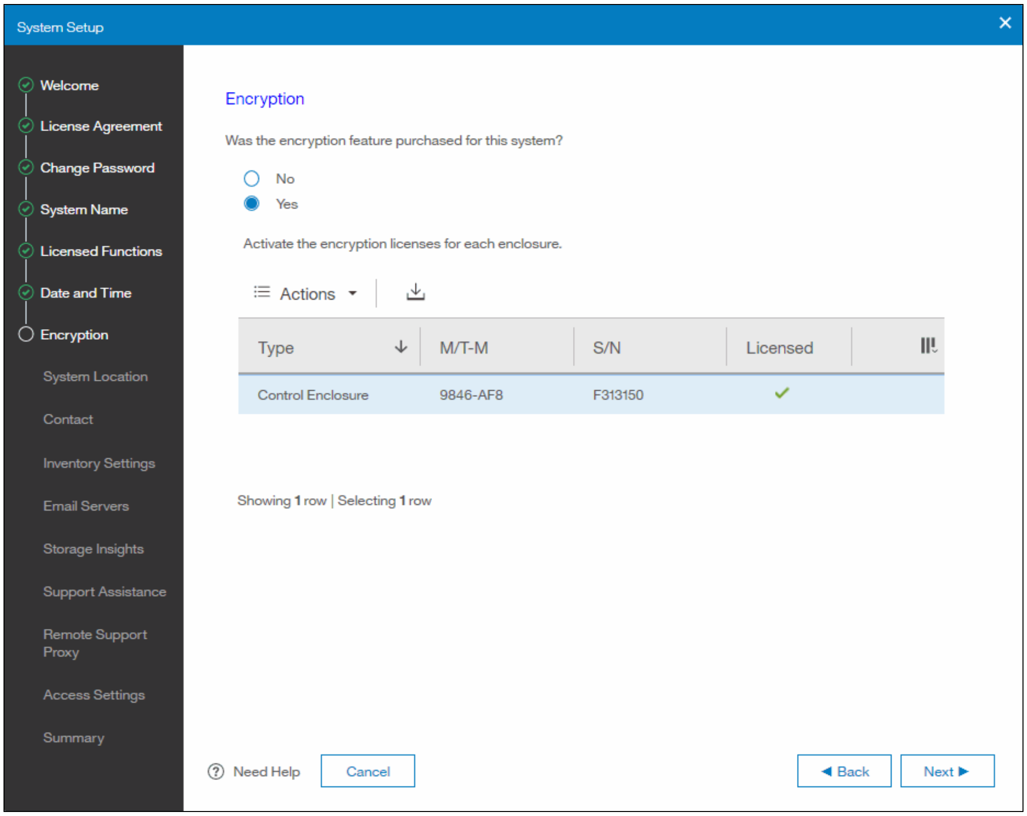


Figure 6-90 Encryption screen showing feature licensed

6. Click **Next**.

Activating the encryption feature manually

To activate the encryption feature manually, complete the following steps:

1. Select the enclosure for which the encryption feature is to be activated (Figure 6-91).
2. Select **Actions** → **Activate License Manually** (Figure 6-91).

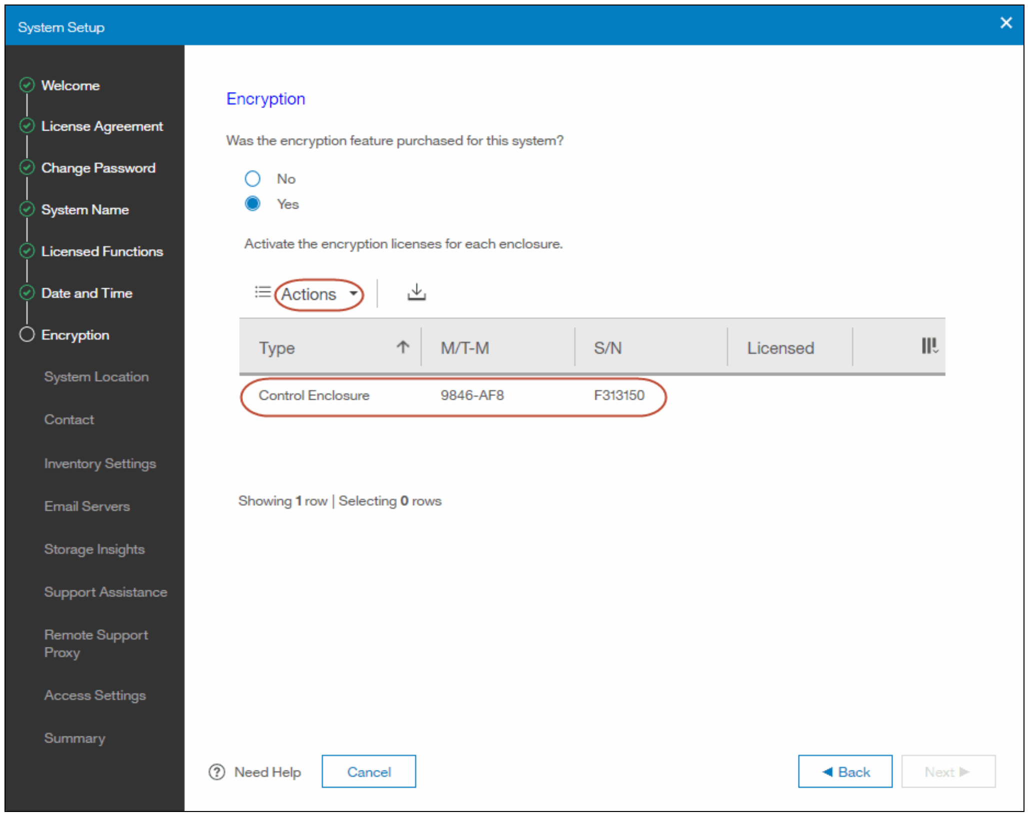


Figure 6-91 Activating the encryption feature license

3. In the **Enter the license key** field on the Manual Activation pane, enter the license key for the encryption feature (Figure 6-92).

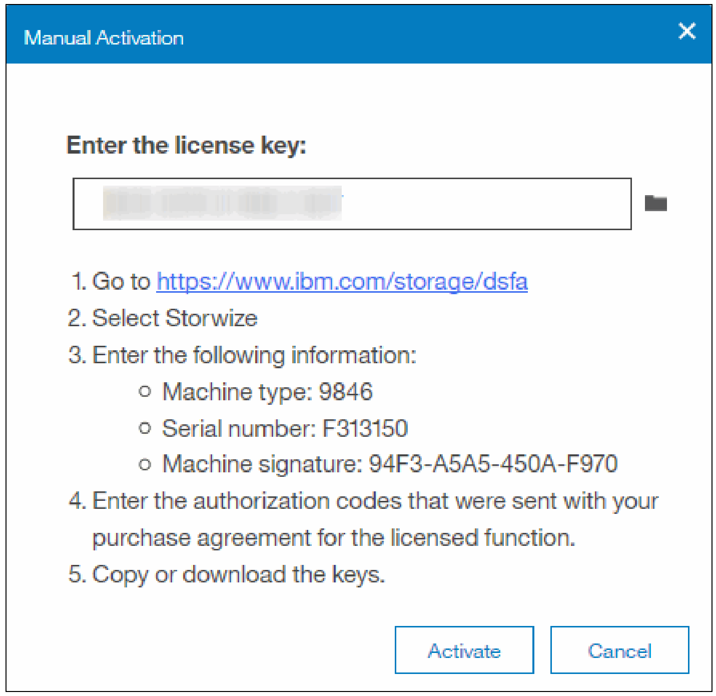


Figure 6-92 Manual activation pane with license key entered

4. Click **Activate**.

5. After the activation completes successfully, the Encryption screen is updated to indicate that the encryption feature is licensed (Figure 6-93).

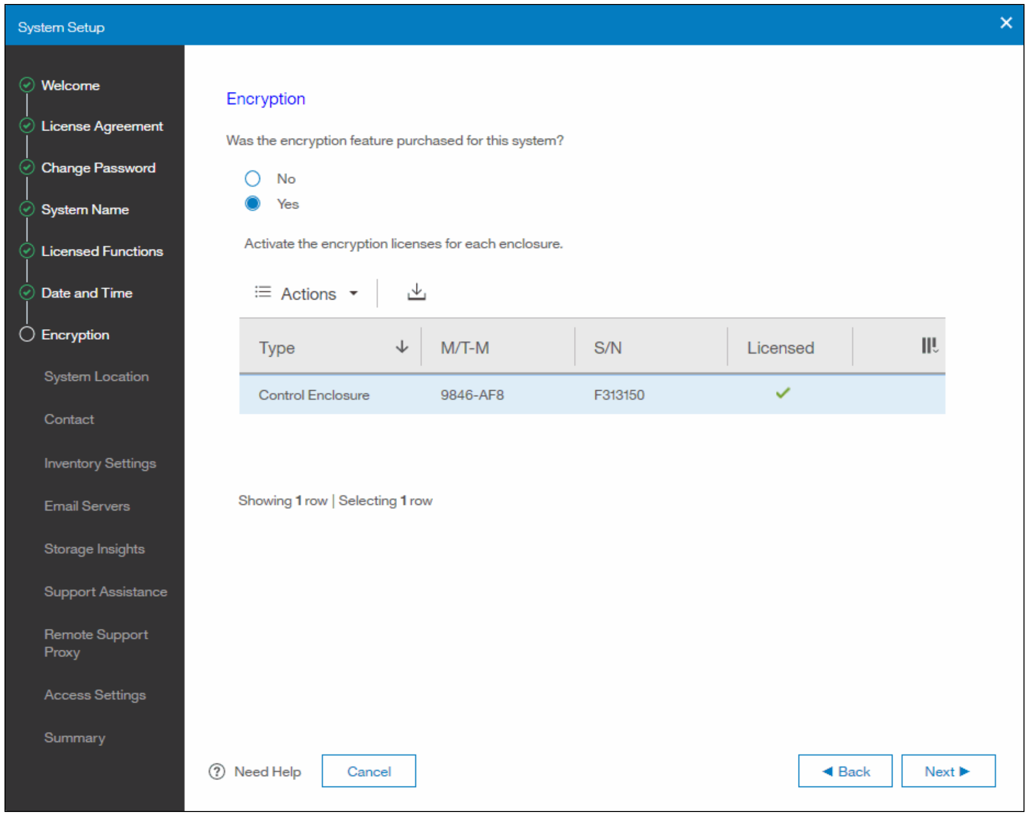


Figure 6-93 Encryption screen showing feature licensed

6. Click **Next**.

6.5.7 System location

The system location information was entered by the IBM SSR during service setup. You can change any of the information on the System Location screen (Figure 6-94).

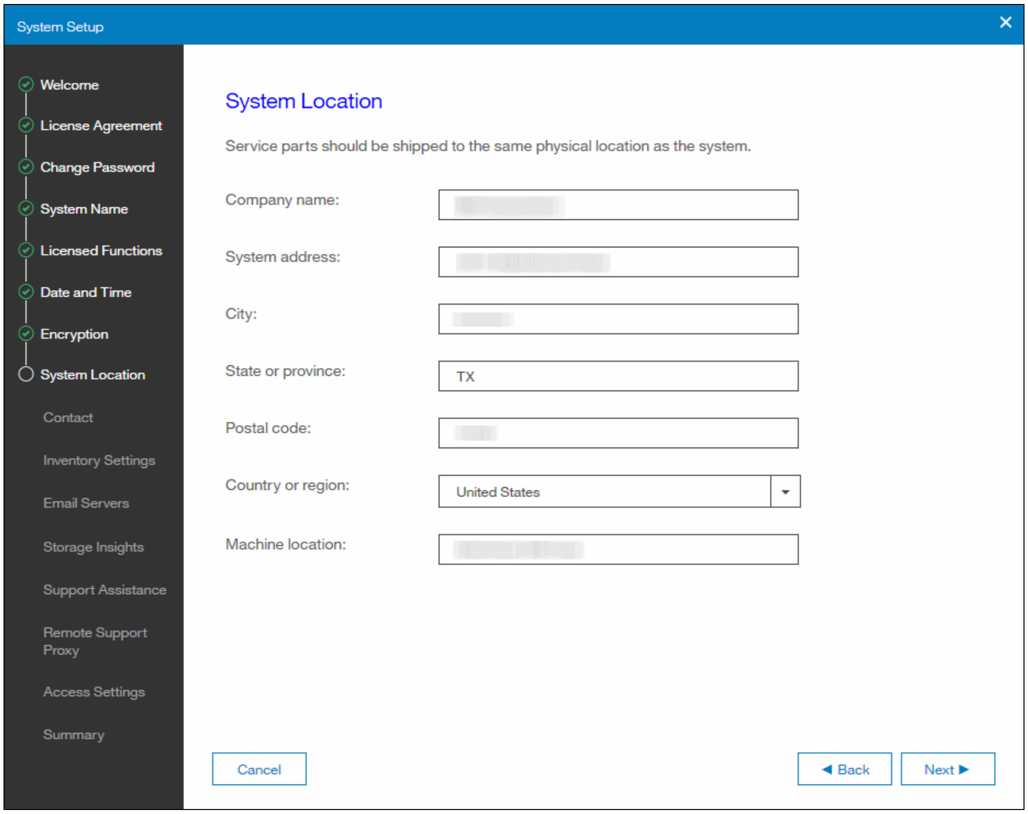


Figure 6-94 System location screen

1. Review the information on the screen and enter any changes in the fields on the screen.
2. Click **Next**.

6.5.8 Contact

The contact information for the system was entered by the IBM SSR during service setup. You can change any of the information on the Contact screen (Figure 6-95).

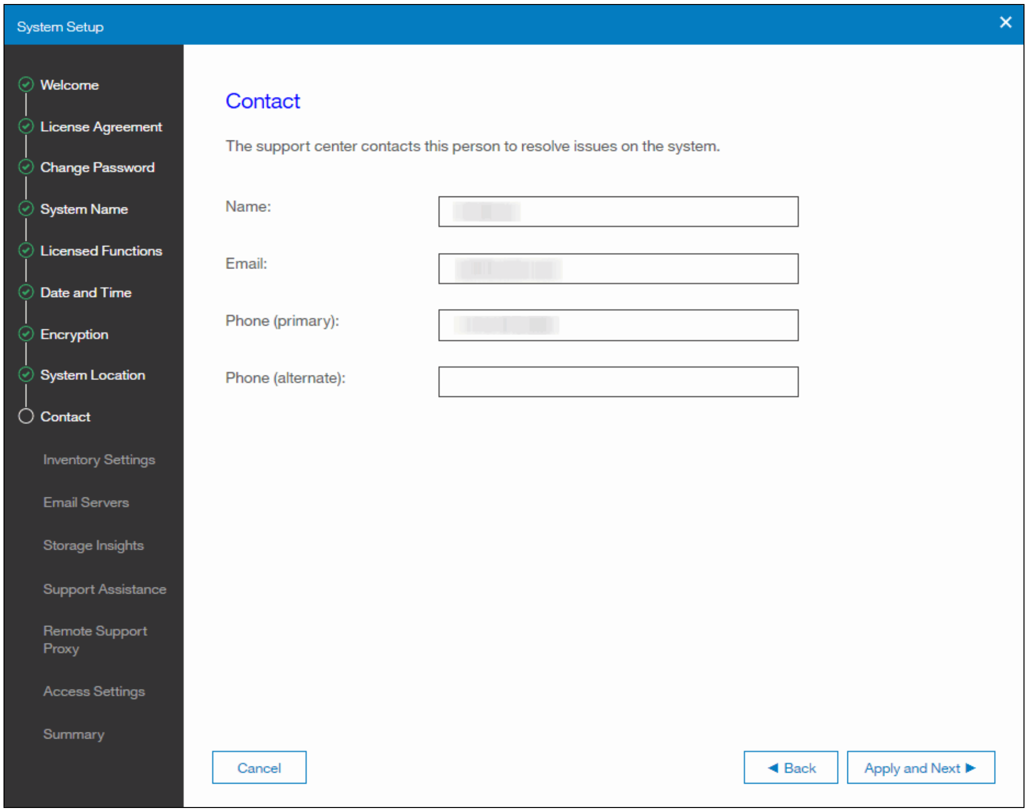


Figure 6-95 Contact screen

1. Review the information on the screen and enter any changes in the fields on the screen.
2. Click **Next**.

6.5.9 Inventory settings

The call home function regularly sends emails to the IBM support center. The Inventory Settings screen is used to control the information included in the emails (Figure 6-96).

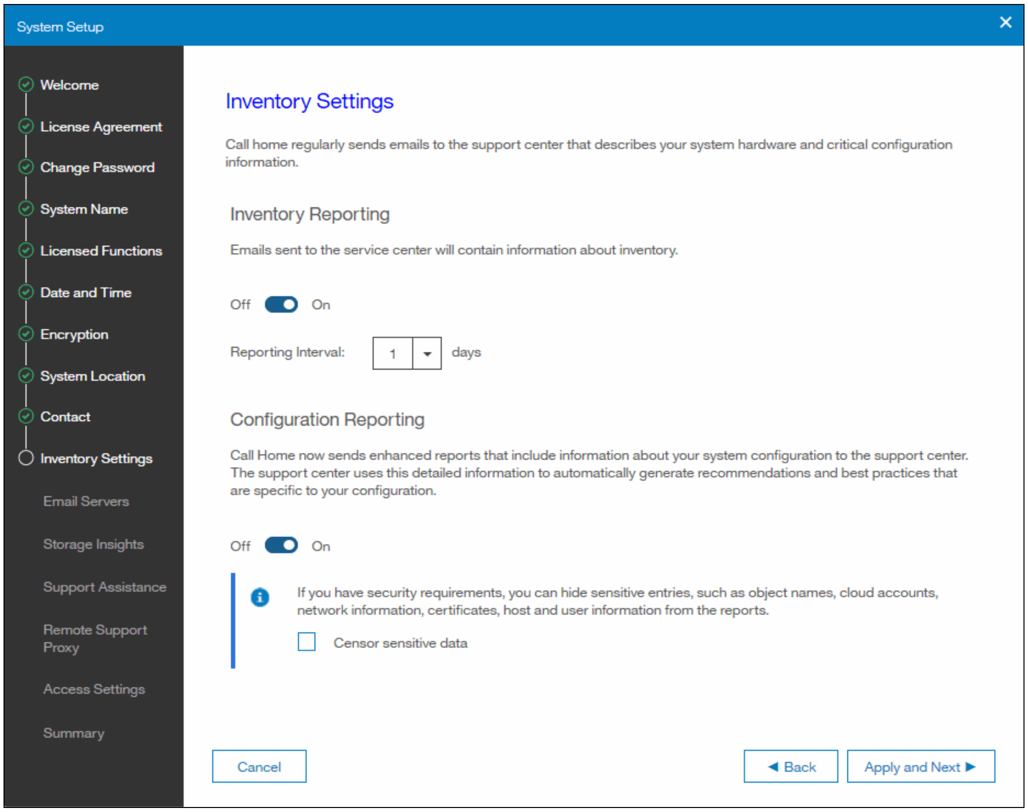


Figure 6-96 Inventory settings screen

Complete the following steps to configure the inventory settings:

1. Select **Off** or **On** to specify if emails sent to the IBM support center will contain inventory information.
2. From the **Reporting Interval** list, select the interval used to include inventory information in emails sent to the IBM support center.
3. Select **Off** or **On** to specify if emails sent to the IBM support center will contain system configuration information.
4. Select the **Censor sensitive data** check box to exclude sensitive entries, such as object names, cloud accounts, network information, certificates, host and user information from the emails sent to IBM support center.
5. Click **Apply and Next**.

6. The Updating Call Home Settings pane is displayed (Figure 6-97).

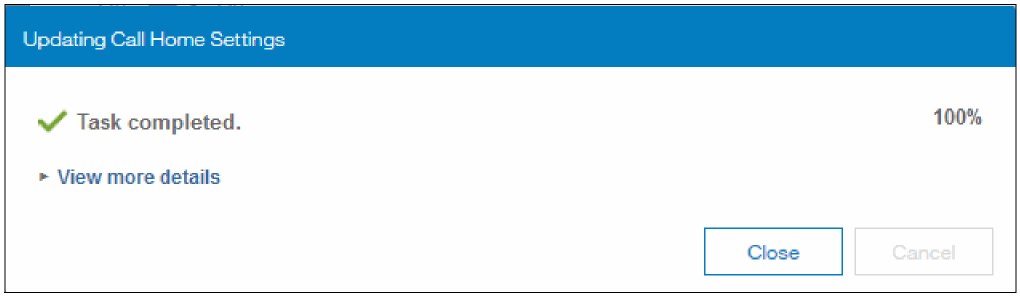


Figure 6-97 Updating call home settings status pane

7. Click **Close**.

6.5.10 Email servers

The SMTP server IP address used by the system was entered by the IBM SSR during service setup. You can change the SMTP server IP address on the Email Servers screen (Figure 6-98).

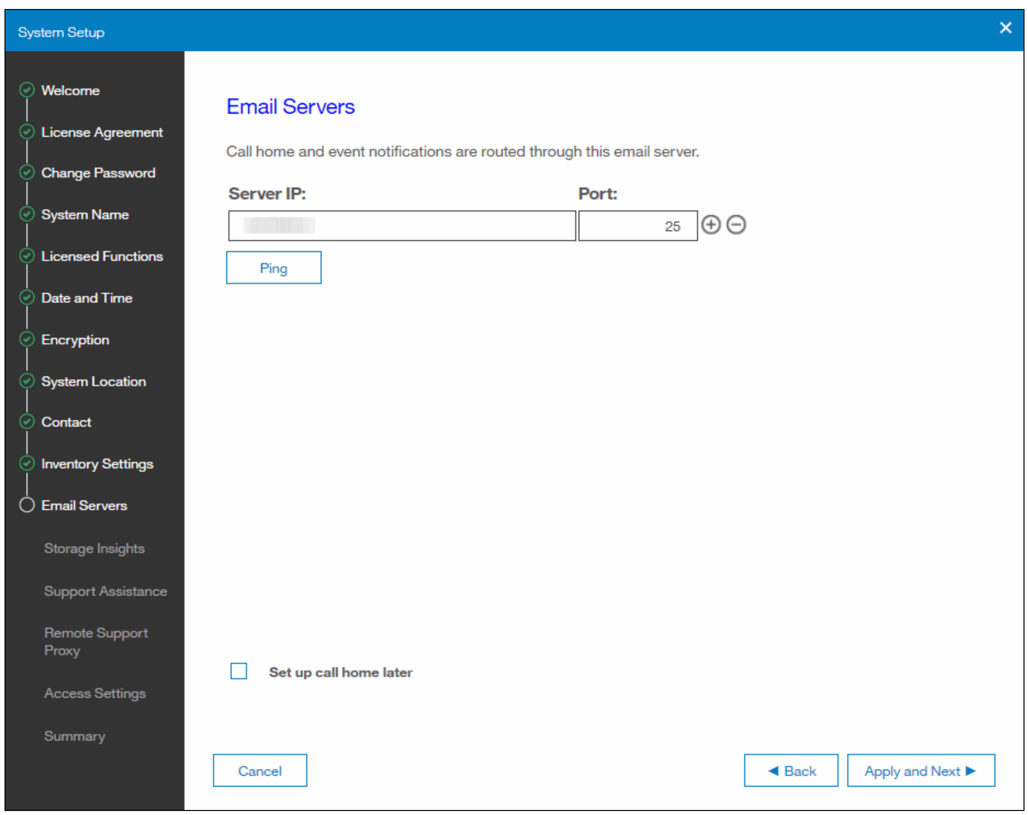


Figure 6-98 Email servers screen

1. Review the SMTP server IP address in the **Server IP** field.
2. Enter a different SMTP server IP address in the **Server IP** field if necessary and click **Ping**.
3. Click **Apply and Next**.

6.5.11 Storage Insights

The Storage Insights screen allows you get started with Storage Insights. (Figure 6-99). For additional information about Storage Insights, see 4.5, “IBM Storage Insights” on page 96.

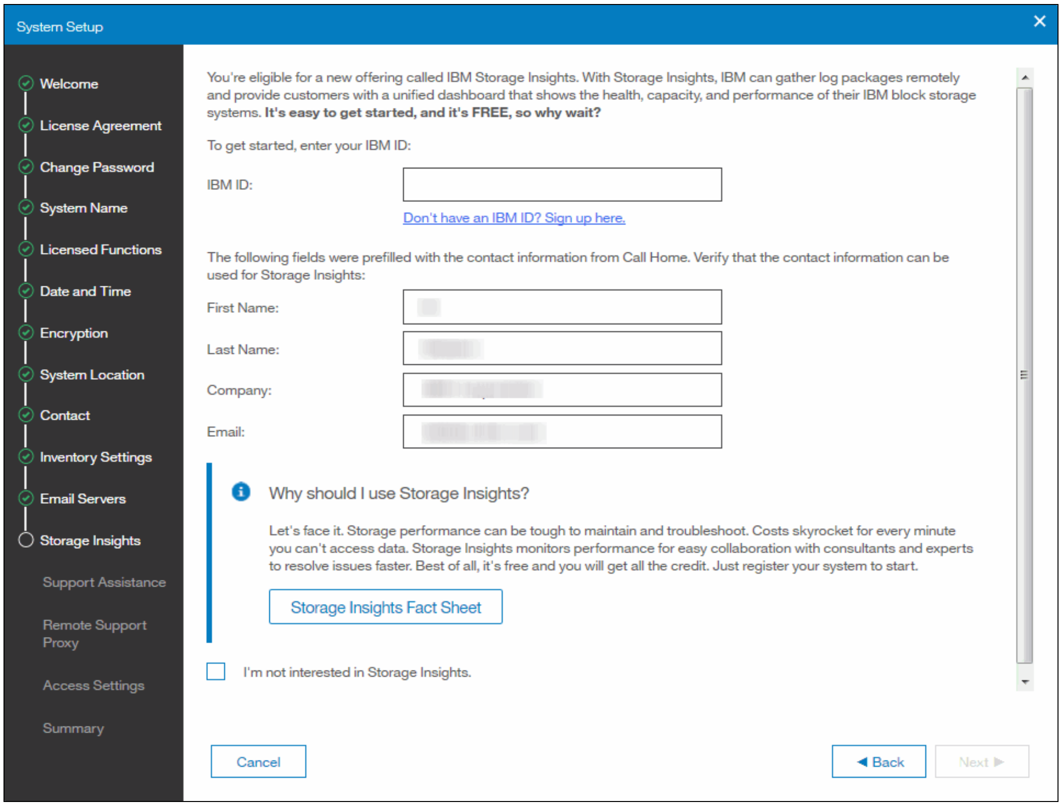


Figure 6-99 Storage Insights screen

1. To get started with Storage Insights, enter your IBM ID in the **IBM ID** field. To defer getting started with Storage Insights at this time, select the **I’m not interested in Storage Insights** check box.
2. Click **Next**.

6.5.12 Support assistance

You can configure either local support assistance, where support personnel visit your site to fix problems with the system, or remote support assistance on the Support Assistance screen (Figure 6-100). Both local and remote support assistance use secure connections to protect data exchange between the support center and system. More access controls can be added by the system administrator. For additional information, see 4.4.7, “Remote Support Assistance (RSA)” on page 93.

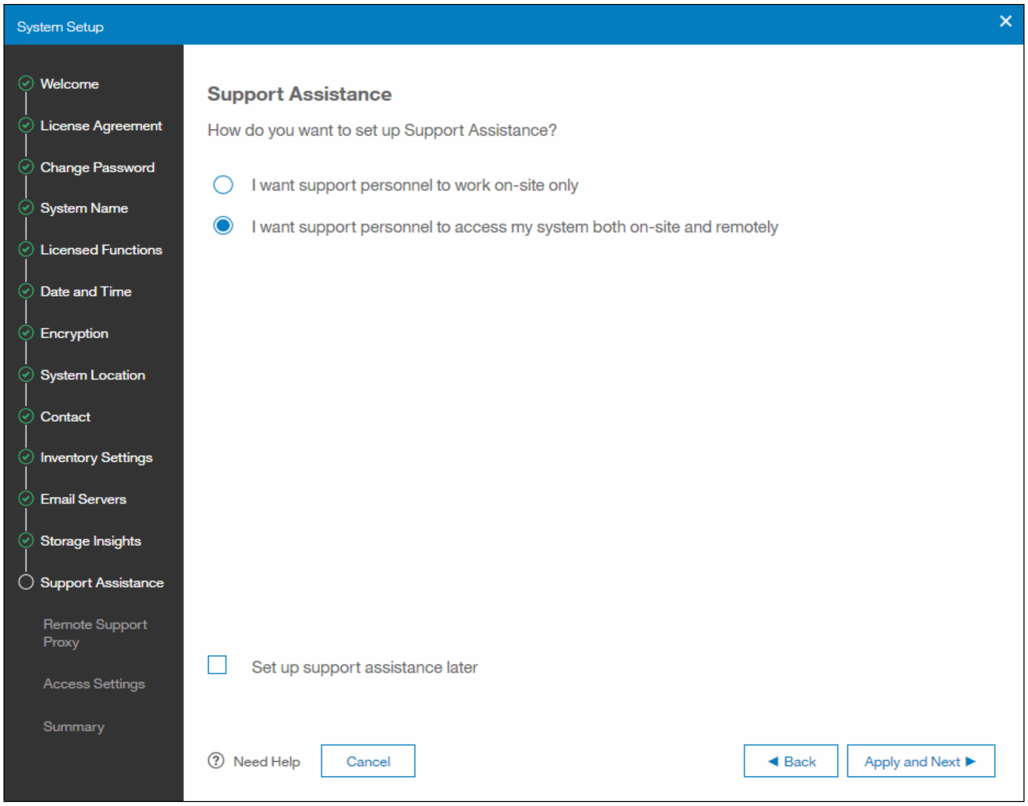


Figure 6-100 Support Assistance screen

To configure support assistance, complete the following steps:

1. Select **I want support personnel to work on-site only** or **I want support personnel to access my system both on-site and remotely**.
2. Click **Apply and Next**.

6.5.13 Support centers

The Support Centers screen (Figure 6-101) lists the IBM Support Center IP addresses and SSH port that are configured on the system. If the system does not have direct access to the internet, a remote support proxy server must be configured. See 4.4.7, “Remote Support Assistance (RSA)” on page 93.

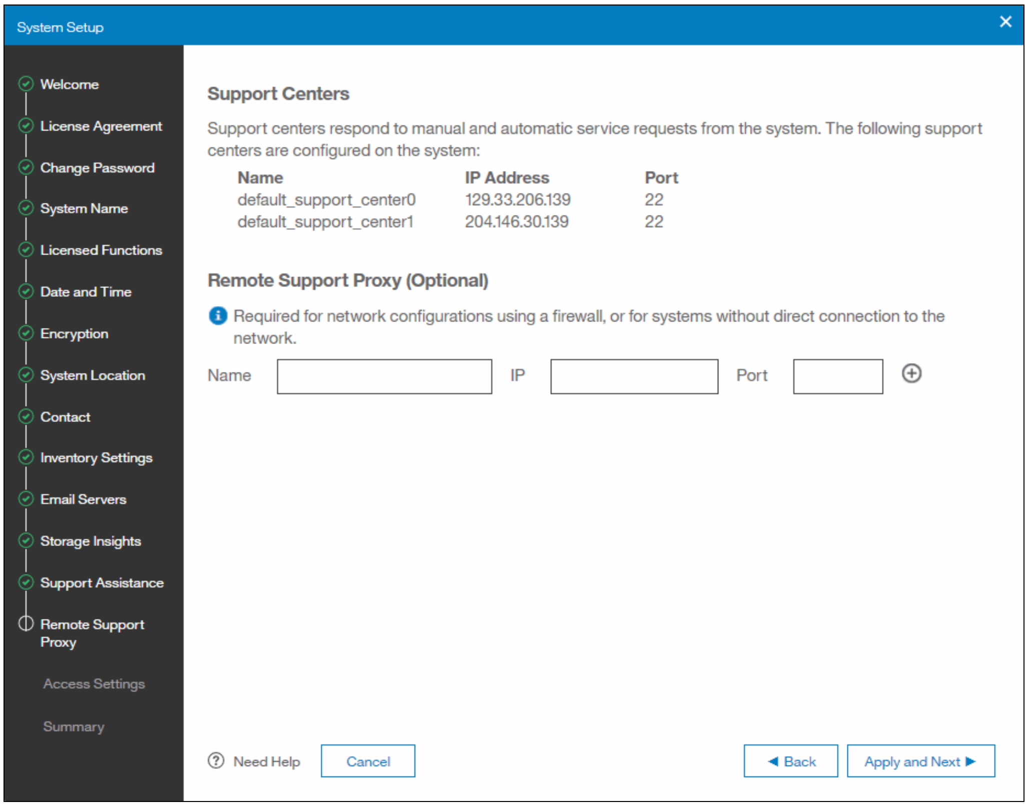


Figure 6-101 Support centers screen

If a remote support proxy server is not required, leave the fields blank and click **Apply and Next**. Otherwise, configure a remote support proxy server by completing the following steps:

1. In the **Name** field, enter the name of the server.
2. In the **IP** field, enter the IP address of the server.
3. In the **Port** field, enter the TCP port.
4. Click **Apply and Next**.

6.5.14 Remote support access settings

You can configure when support personnel can access your system to conduct maintenance and fix problems on the Remote Support Access Settings screen (Figure 6-102).

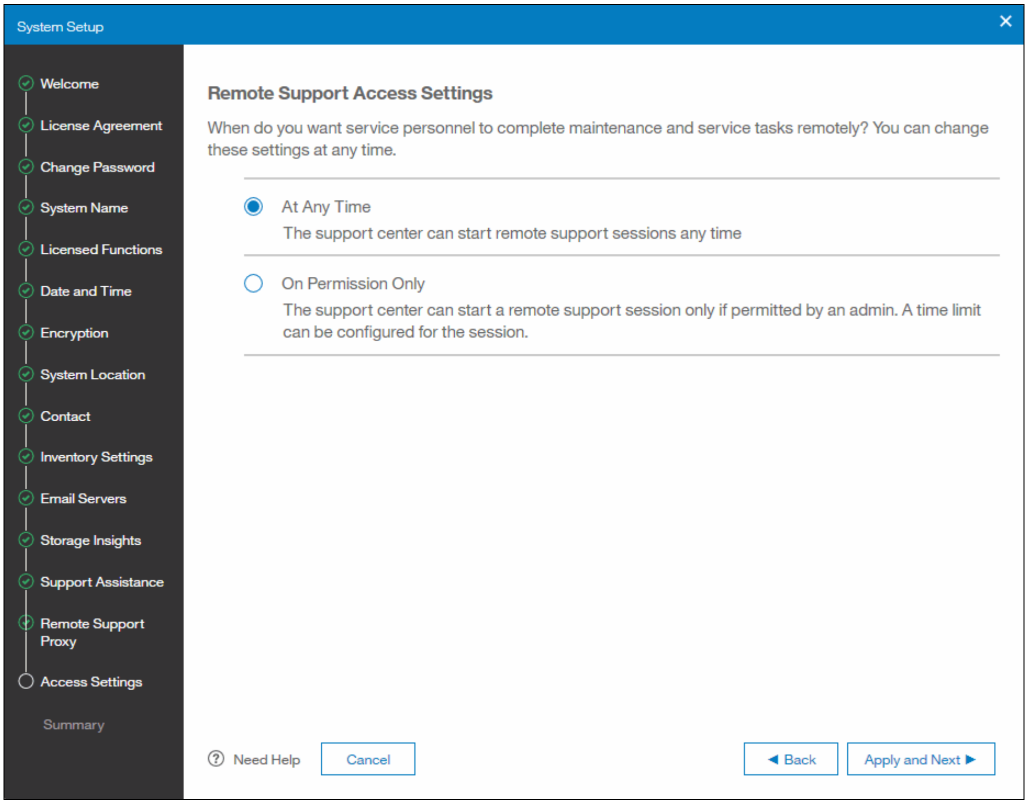


Figure 6-102 Remote support access settings screen

To configure the remote support access setting, complete the following steps:

1. Select **At Any Time** or **On Permission Only**.
2. Click **Apply and Next**.
3. The Enable Support Assistance status pane is displayed (Figure 6-103).

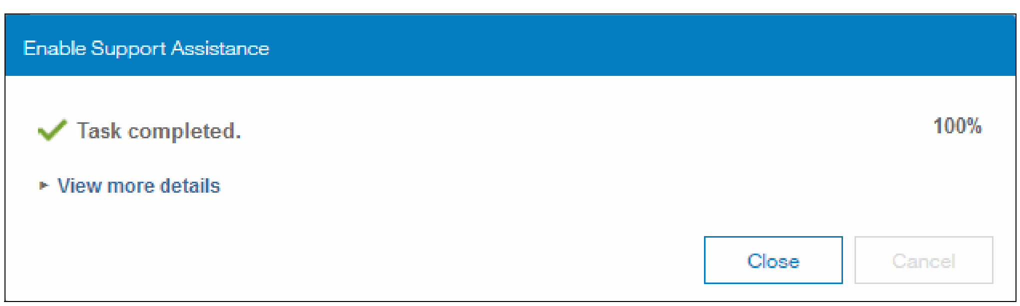


Figure 6-103 Enable support assistance status pane

4. Click **Close**.

6.5.15 Summary

The Summary screen (Figure 6-104) lists the information that was entered during the initial setup:

1. To make changes to the settings or configuration, click **Back**.
2. To complete the initial setup, click **Finish**.

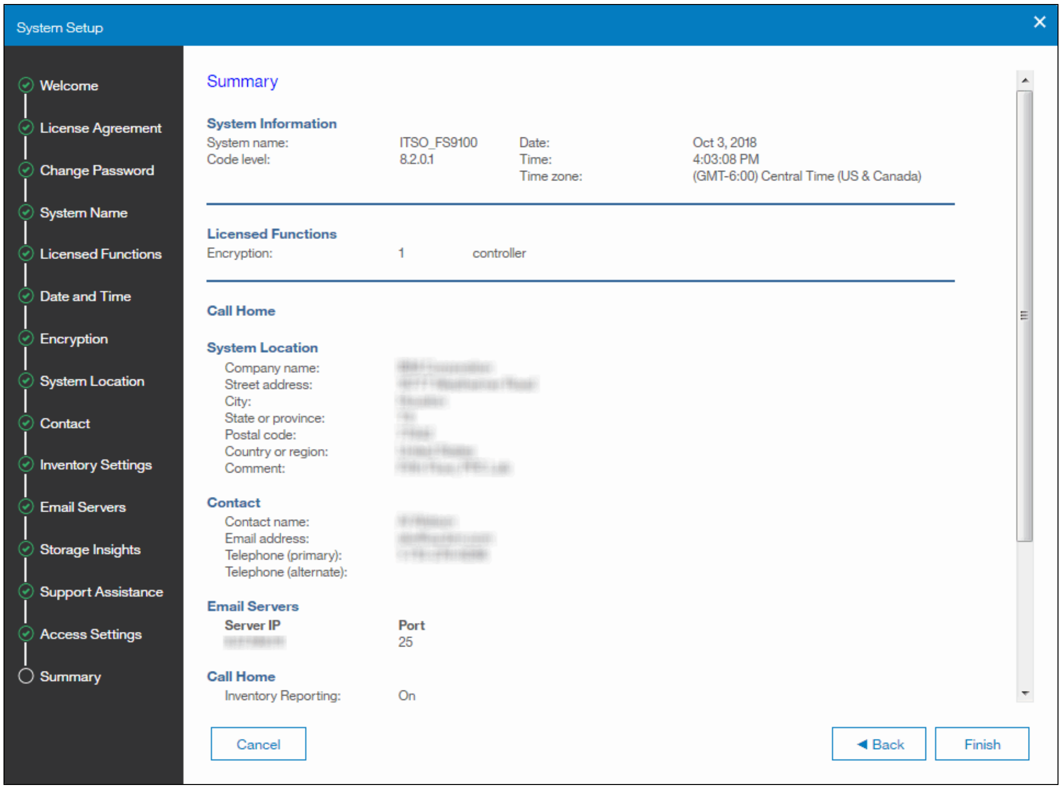


Figure 6-104 Summary screen

3. On the System Initialization pane (Figure 6-105), click **Close**.

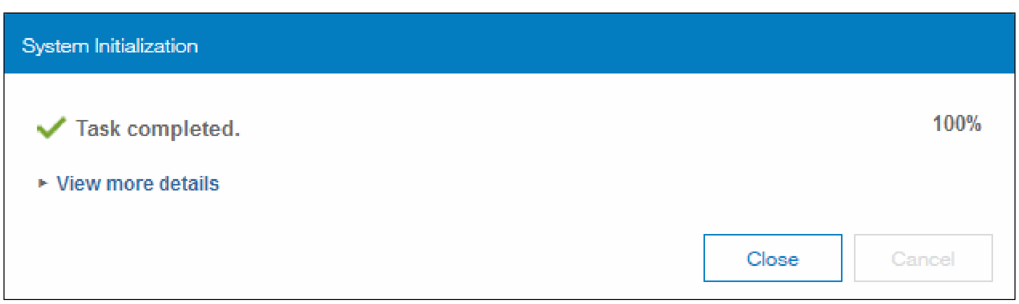


Figure 6-105 System initialization status pane

4. On the Setup Completed (Figure 6-106 on page 240), click **Close**.

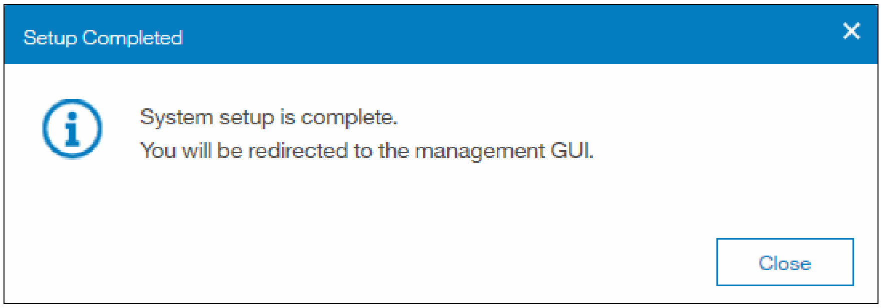


Figure 6-106 Setup Completed status pane

7

Configuring settings

The Settings section of the IBM FlashSystem 9100 graphical user interface (GUI) is described in this chapter and covers various options for monitoring, configuring interfaces, and extracting support logs. It also covers remote authentication and the firmware update process.

This chapter includes the following topics:

- Settings menu
- Notifications menu
- Network
- Security menu
- System menu
- Support menu
- GUI preferences

7.1 Settings menu

Use the Settings pane to configure system options for notifications, network, security, system, support, and preferences that are related to display options in the management GUI (Figure 7-1).

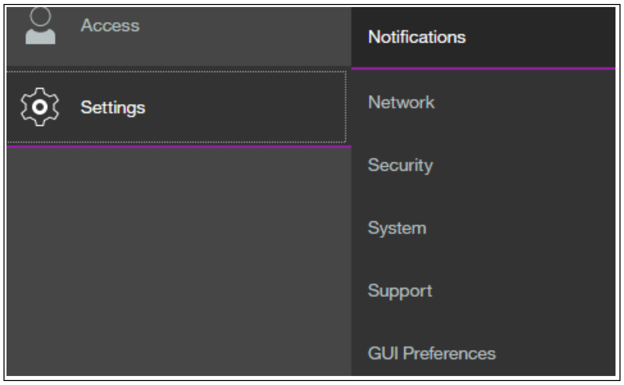


Figure 7-1 Settings menu

The following options are available for configuration from the **Settings** menu:

- **Notifications:** The system can use Simple Network Management Protocol (SNMP) traps, syslog messages, and Call Home emails to notify you and the support center when significant events are detected. Any combination of these notification methods can be used simultaneously.
- **Network:** Use the Network pane to manage the management IP addresses for the system, service IP addresses for the nodes, and iSCSI and Fibre Channel configurations.
- **Security:** Use the Security pane to configure and manage remote authentication services, encryption, and secure communication.
- **System:** Navigate to the **System** menu item to manage overall system configuration options, such as licenses, updates, and date and time settings.
- **Support:** Helps to configure and manage connections, and upload support packages to the support center.
- **GUI Preferences:** Configure welcome message after login, refresh internal cache/inventory, and GUI logout timeouts.

These options are described in more detail in the following sections.

7.2 Notifications menu

The FS9100 can use SNMP traps, syslog messages, and Call Home email to notify you and the IBM Support Center when significant events are detected. Any combination of these notification methods can be used simultaneously.

Notifications are normally sent immediately after an event is raised. However, events can occur because of service actions that are performed. If a recommended service action is active, notifications about these events are sent only if the events are still unfixed when the service action completes.

7.2.1 Email notifications

The Call Home feature transmits operational and event-related data to you and IBM through a Simple Mail Transfer Protocol (SMTP) server connection in the form of an event notification email. When configured, this function alerts IBM service personnel about hardware failures and potentially serious configuration or environmental issues.

For more information on the Call Home feature, refer to 4.4.6, “Call Home option” on page 91.

Complete the following steps to view email event notifications:

1. From the FS9100 System pane, click the **Settings** selection and click **Notifications**, as shown in Figure 7-2.

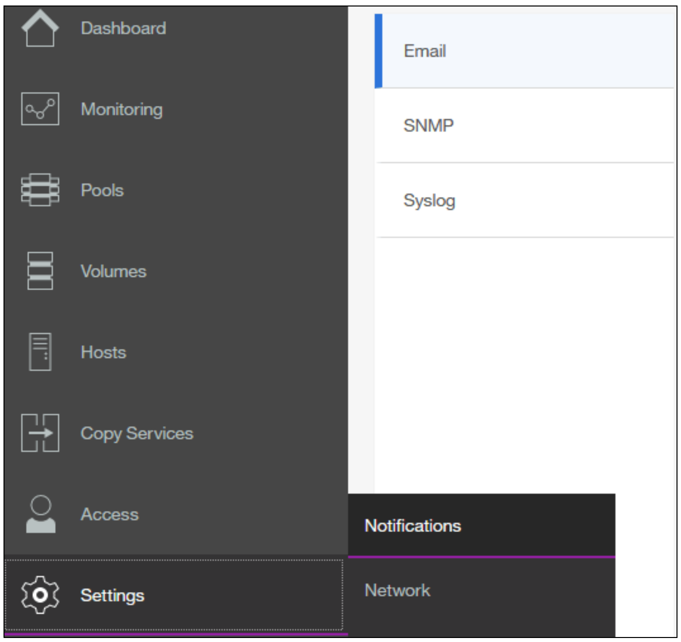


Figure 7-2 Selecting Notifications in the Settings section

2. Click the **Email** section. The **Email** settings appear as shown in Figure 7-3.

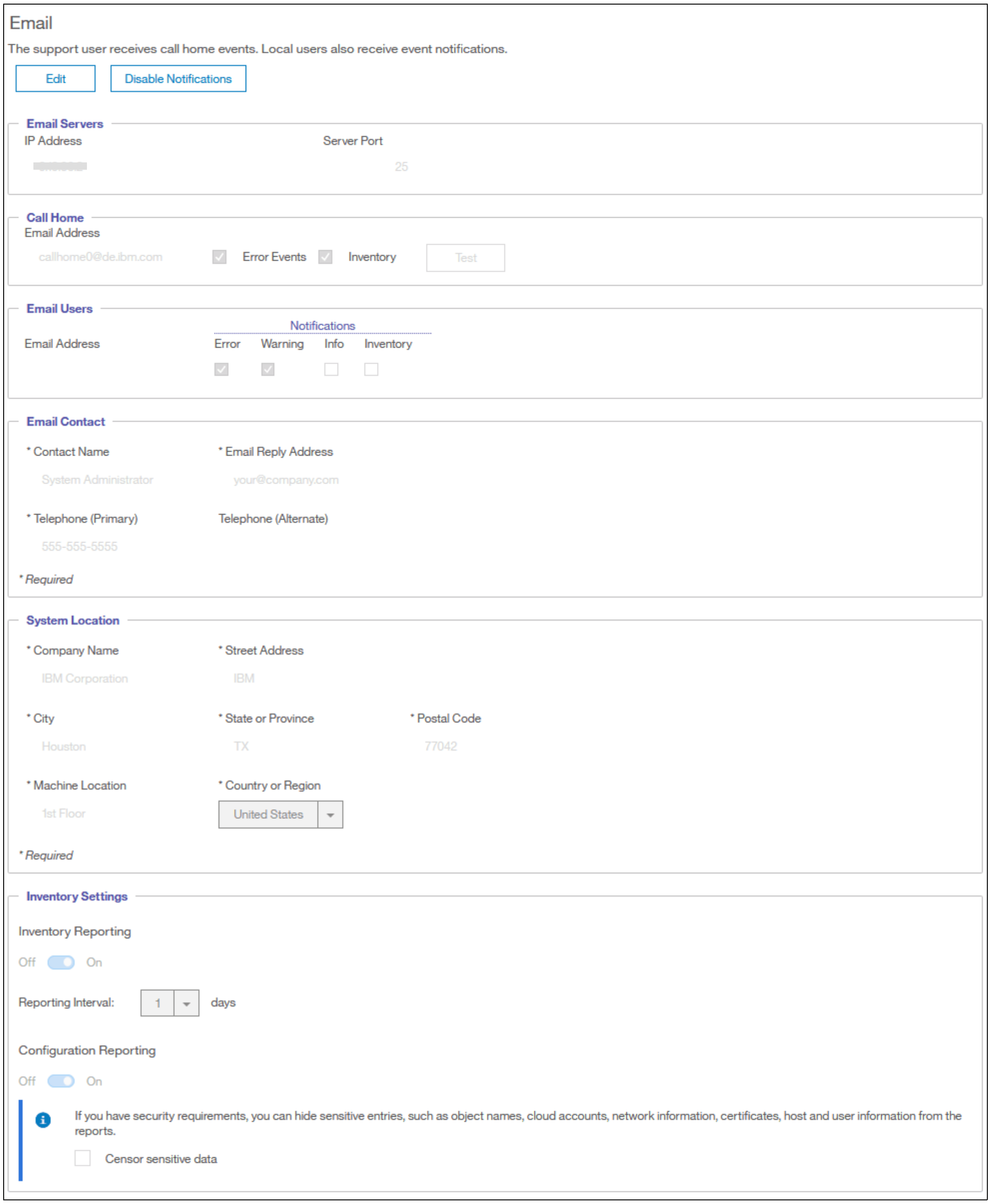


Figure 7-3 Email Notification settings

3. This view provides the following useful information about email notification and call-home information, among others:

- The IP of the email server (SMTP Server) and Port
- The Call-home email address
- The email of one or more users set to receive one or more email notifications
- The contact information of the person in the organization responsible for the system
- System location

7.2.2 SNMP notifications

SNMP is a standard protocol for managing networks and exchanging messages. The system can send SNMP messages that notify personnel about an event. You can use an SNMP manager to view the SNMP messages that are sent by the FS9100.

To view the SNMP configuration, use the System window. Click **Settings** and click **Notification** → **SNMP** as shown in Figure 7-4.

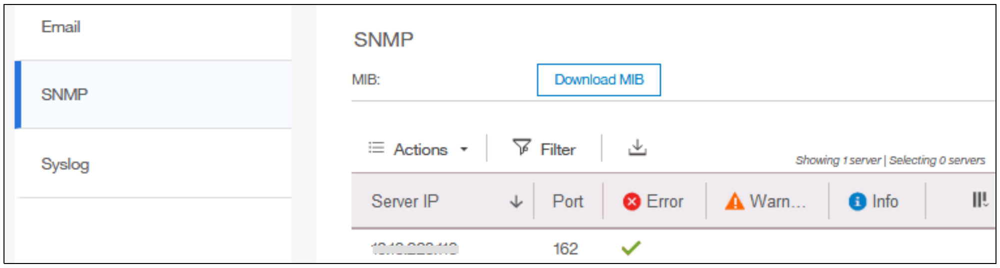


Figure 7-4 Setting SNMP server and traps

From this window (Figure 7-4), you can view and configure an SNMP server to receive various informational, error, or warning notifications by setting the following information:

- **IP Address**

  The address for the SNMP server.

- **Server Port**

  The remote port number for the SNMP server. The remote port number must be a value of 1 - 65535.

- **Community**

  The SNMP community is the name of the group to which devices and management stations that run SNMP belong.

- **Event Notifications**

  Consider the following points about event notifications:

  – Select **Error** if you want the user to receive messages about problems, such as hardware failures, that must be resolved immediately.

  – Select **Warning** if you want the user to receive messages about problems and unexpected conditions. Investigate the cause immediately to determine any corrective action.

  – Select **Info** if you want the user to receive messages about expected events. No action is required for these events.

To remove an SNMP server, click Remove. To add another SNMP server, click Add.

7.2.3 Syslog notifications

The syslog protocol is a standard protocol for forwarding log messages from a sender to a receiver on an IP network. The IP network can be IPv4 or IPv6. The system can send syslog messages that notify personnel about an event. You can use a Syslog pane to view the Syslog messages that are sent by the FS9100.

To view the Syslog configuration, use the System window and click **Settings** and click **Notification** → **Syslog** (Figure 7-5).

Figure 7-5 Setting Syslog messaging

From this window, you can view and configure a syslog server to receive log messages from various systems and store them in a central repository by entering the following information:

- **IP Address**

  The IP address for the syslog server.

- **Facility**

  The facility determines the format for the syslog messages. The facility can be used to determine the source of the message.

- **Message Format**

  The message format depends on the facility. The system can transmit syslog messages in the following formats:

  – The concise message format provides standard detail about the event.
  – The expanded format provides more details about the event.

- **Event Notifications**

  Consider the following points about event notifications:

  – Select **Error** if you want the user to receive messages about problems, such as hardware failures, that must be resolved immediately.

  – Select **Warning** if you want the user to receive messages about problems and unexpected conditions. Investigate the cause immediately to determine whether any corrective action is necessary.

  – Select **Info** if you want the user to receive messages about expected events. No action is required for these events.

  To remove a syslog server, click the Minus sign (**-**). To add another syslog server, click the Plus sign (**+**).

The syslog messages can be sent in concise message format or expanded message format.

Example 7-1 shows a compact format syslog message.

Example 7-1 Compact syslog message example

```
IBM2145 #NotificationType=Error #ErrorID=077001 #ErrorCode=1070 #Description=Node
CPU fan failed #ClusterName=ITSO_9100 #Timestamp=Wed Oct 02 08:00:00 2018 BST
#ObjectType=Node #ObjectName=Node1 #CopyID=0 #ErrorSequenceNumber=100
```

Example 7-2 shows an expanded format syslog message.

Example 7-2 Full format syslog message example

```
IBM2145 #NotificationType=Error #ErrorID=077001 #ErrorCode=1070 #Description=Node
CPU fan failed #ClusterName=ITSO_9100 #Timestamp=Wed Oct 02 08:00:00 2018 BST
#ObjectType=Node #ObjectName=Node1 #CopyID=0 #ErrorSequenceNumber=100 #ObjectID=2
#NodeID=2 #MachineType=9846AF8#SerialNumber=1234567 #SoftwareVersion=8.2.0.0
(build 137.4.1709291021000)#FRU=fan 24P1118, system board 24P1234
#AdditionalData(0->63)=0000000021000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000#Additional
Data(64-127)=000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000
```

7.3 Network

This section describes how to view the network properties of the FS9100 system. The network information can be obtained under the **Settings** section by clicking the **Network** section as shown in Figure 7-6.

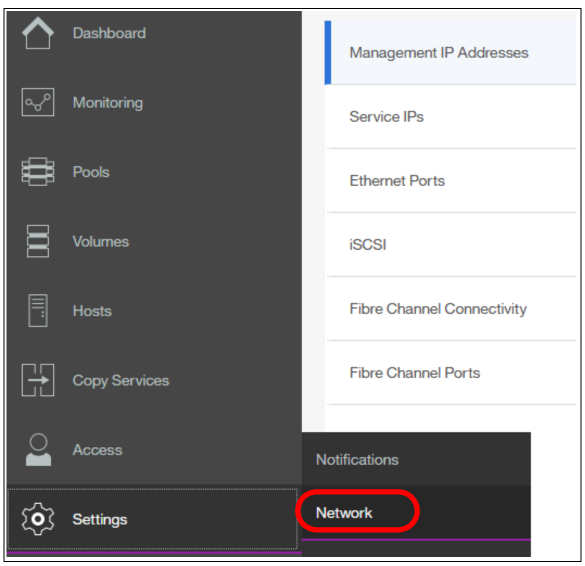


Figure 7-6 Accessing network information

7.3.1 Management IP addresses

To view the management IP addresses of the FS9100, click **Settings** → **Network** and click **Management IP Addresses**. The GUI shows the management IP address by clicking the network ports as shown in Figure 7-7.

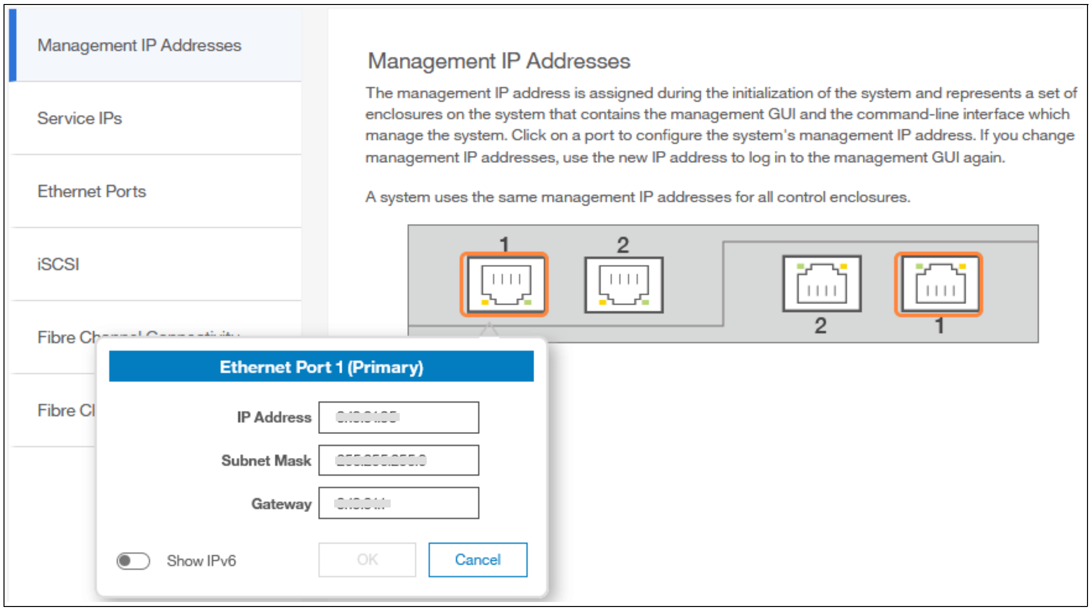


Figure 7-7 Viewing the management IP addresses

7.3.2 Service IP information

To view the Service IP information of your FS9100, click **Settings** → **Network** and click the **Service IP Address**. The GUI displays the service IP address when you click the network ports, as shown in Figure 7-8.

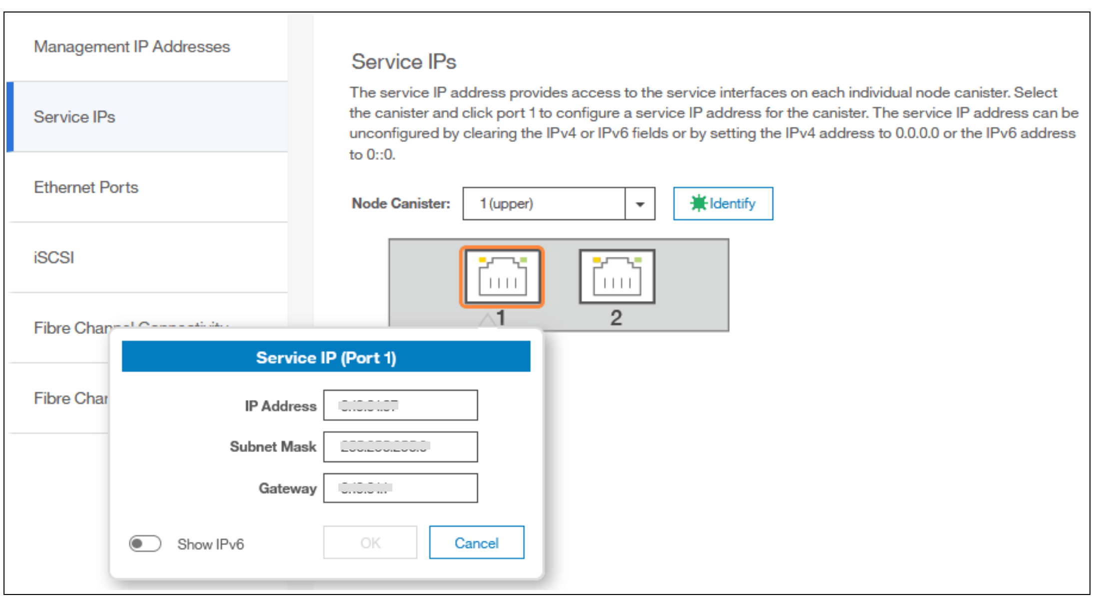


Figure 7-8 Viewing service IP address

The service IP address is commonly used to provide access to the network interfaces on each individual node.

Instead of reaching the Management IP address, the service IP address directly connects to each individual node for service operations, for example. You can select a node from the drop-down list and then click any of the ports that are shown in the GUI. The service IP address can be configured to support IPv4 or IPv6.

7.3.3 iSCSI information

From the **iSCSI** pane in the **Settings** → **Network** menu, you can display and configure parameters for the system to connect to iSCSI-attached hosts, as shown in Figure 7-9.

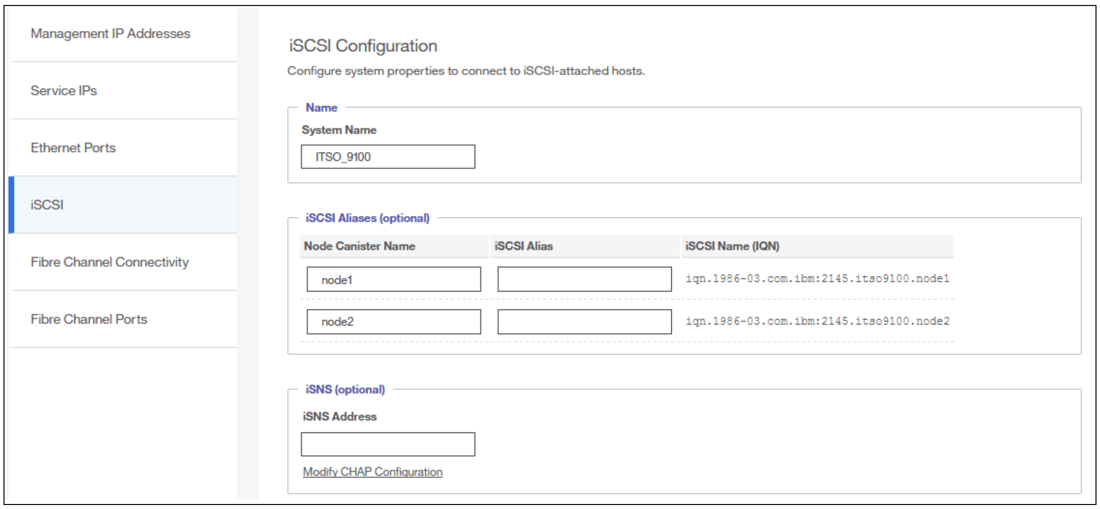


Figure 7-9 iSCSI Configuration pane

The following parameters can be updated:

- **System Name**

  It is important to set the system name correctly because it is part of the IQN for the node.

  > **Important:** If you change the name of the system after iSCSI is configured, you might need to reconfigure the iSCSI hosts.

  To change the system name, click the system name and specify the new name.

  > **System name**: You can use the letters A - Z and a - z, the numbers 0 - 9, and the underscore (_) character. The name can be 1 - 63 characters.

- **iSCSI Aliases** (Optional)

  An *iSCSI alias* is a user-defined name that identifies the node to the host. Complete the following steps to change an iSCSI alias:

  a. Click an iSCSI alias.
  b. Specify a name for it.

  Each node has a unique iSCSI name that is associated with two IP addresses. After the host starts the iSCSI connection to a target node, this IQN from the target node is visible in the iSCSI configuration tool on the host.

- **iSNS** and **CHAP**

  You can specify the IP address for the iSCSI Storage Name Service (iSNS). Host systems use the iSNS server to manage iSCSI targets and for iSCSI discovery.

  You can also enable Challenge Handshake Authentication Protocol (CHAP) to authenticate the system and iSCSI-attached hosts with the specified shared secret.

  The CHAP secret is the authentication method that is used to restrict access for other iSCSI hosts that use the same connection. You can set the CHAP for the whole system under the system properties or for each host definition. The CHAP must be identical on the server and the system/host definition. You can create an iSCSI host definition without the use of a CHAP.

7.3.4 Fibre Channel Information

To view the Fibre Channel Connectivity information of your FS9100, click **Settings** → **Network** and click **Fibre Channel Connectivity**. As shown in Figure 7-10, you can use the **Fibre Channel Connectivity** pane to display the FC connectivity between nodes and other storage systems and hosts that attach through the FC network. You can filter by selecting one of the following fields:

- All nodes, storage systems, and hosts
- Systems
- Nodes
- Storage systems
- Hosts

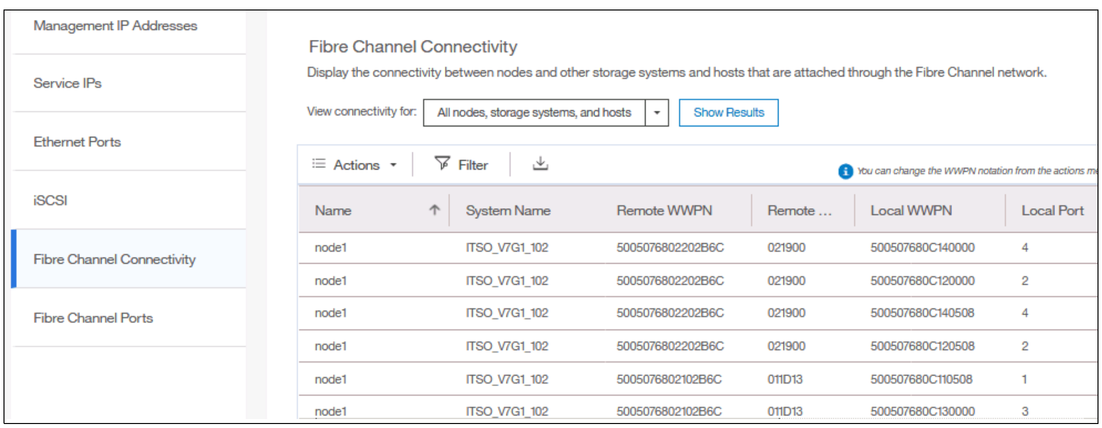


Figure 7-10 Fibre Channel connections

The **Fibre Channel Ports** pane will display how the Fibre Channel port is configured across all control node canisters in the system. This view helps, for example, to determine with which other clusters the port is allowed to communicate (Figure 7-11 on page 251).

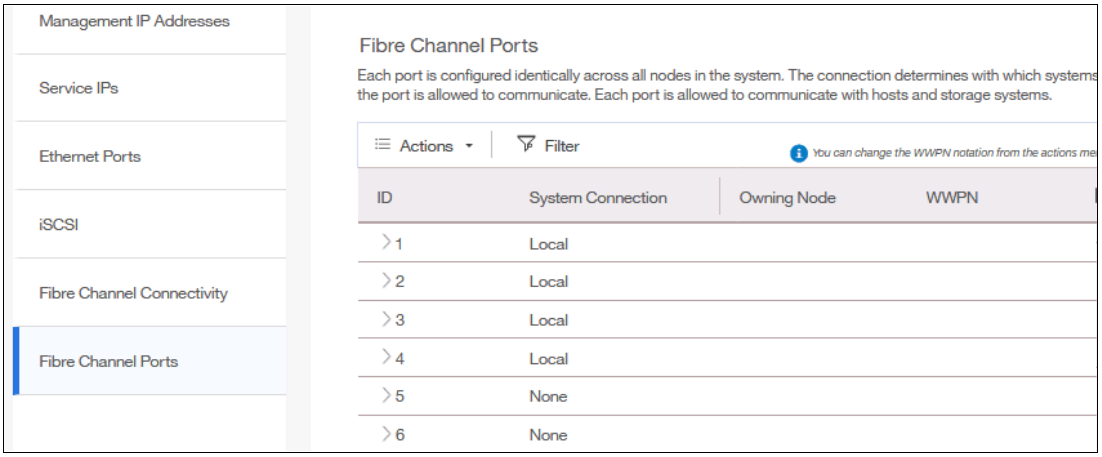


Figure 7-11 Viewing Fibre Channel Port properties

7.4 Security menu

Use the **Security** panel as shown in Figure 7-12, to configure and manage remote authentication, encryption and secure communications settings on the system. With remote authentication services, an external authentication server can be used to authenticate users attempting to access system data and resources. User credentials are managed externally through various supported authentication services, such as LDAP.

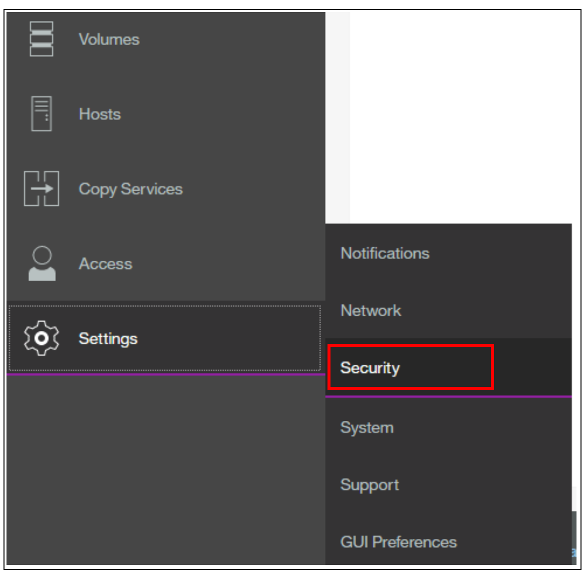


Figure 7-12 Accessing security information

7.4.1 Remote authentication

A *remote user* is authenticated on a remote service with Lightweight Directory Access Protocol (LDAP) support. Remote users who need to access the system when the remote service is down also need to configure local credentials. Remote users have their groups defined by the remote authentication service.

Configuring remote authentication

The FS9100 supports the following types of LDAP servers:

- IBM Security Directory Server
- Microsoft Active Directory
- OpenLDAP

For remote authentication using the Lightweight Directory Access Protocol (LDAP), see the IBM Redbooks publication *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933 section “Configuring user authentication”.

7.4.2 Activating Encryption

To activate encryption on a running system, complete these steps:

1. Click **Settings** → **System** → **Licensed Functions**.
2. Click **Encryption Licenses**, as shown in Figure 7-13.

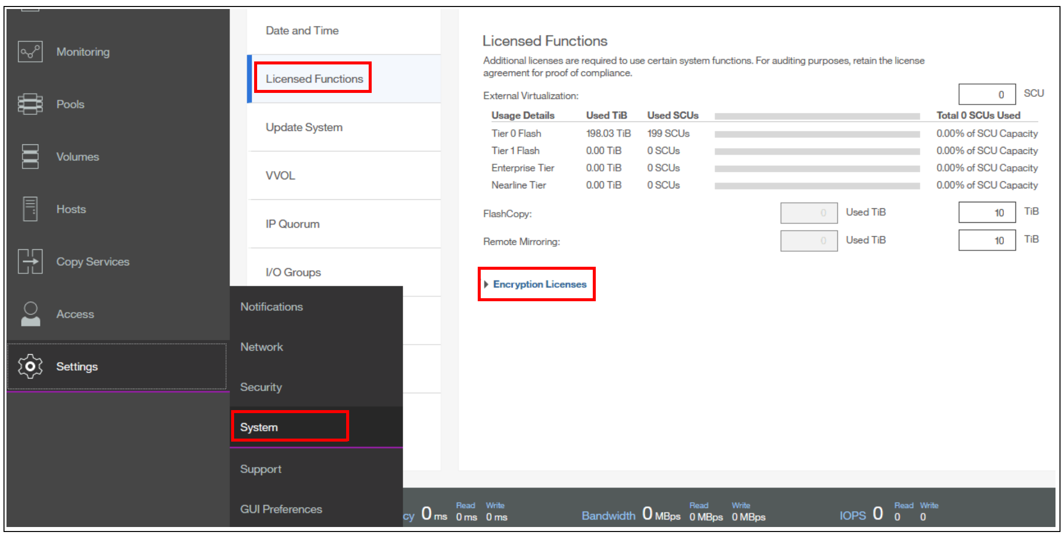


Figure 7-13 Expanding Encryption Licenses section on the Licensed Functions window

3. The Encryption Licenses window displays information about your nodes. Right-click the node on which you want to install an encryption license. This action opens a menu with two license activation options (**Activate License Automatically** and **Activate License Manually**), as shown in Figure 7-14. Use either option to activate encryption. See , “Activate the license automatically” on page 253 for instructions on how to complete an automatic activation process. See, “Activate the license manually” on page 255 for instructions on how to complete a manual activation process.

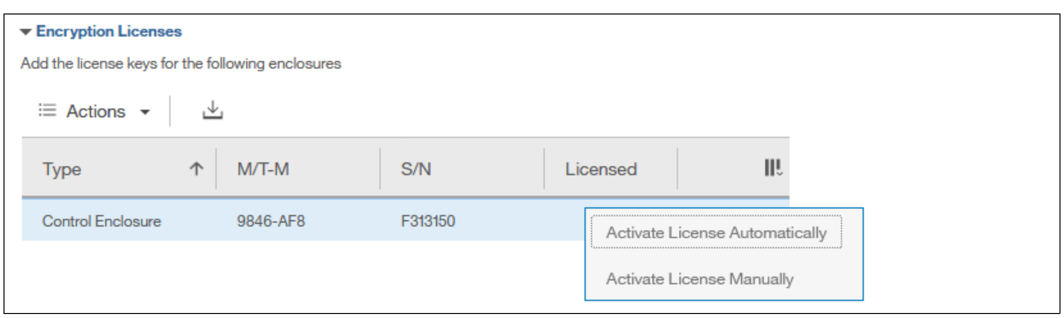


Figure 7-14 Select the node on which you want to enable the encryption

4. After either activation process is complete, you can see a green check mark in the column labeled Licensed for the node, as shown in Figure 7-15.

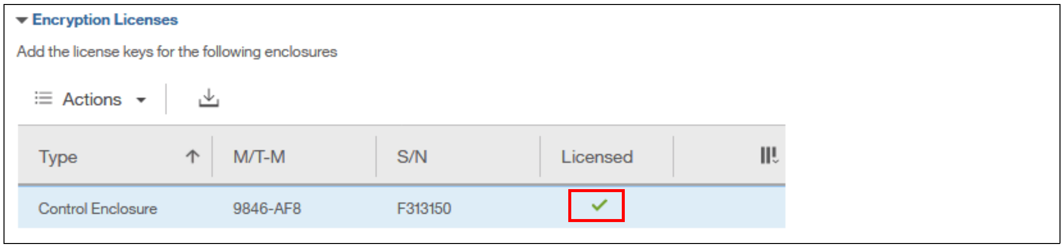


Figure 7-15 Successful encryption license activation on a running system

Activate the license automatically

Important: To perform this operation, the personal computer used to connect to the GUI and activate the license must be able to connect to hosts on the internet.

To activate the encryption license for a node automatically, complete these steps:

1. Select **Activate License Automatically** to open the Activate License Automatically window, as shown in Figure 7-16.

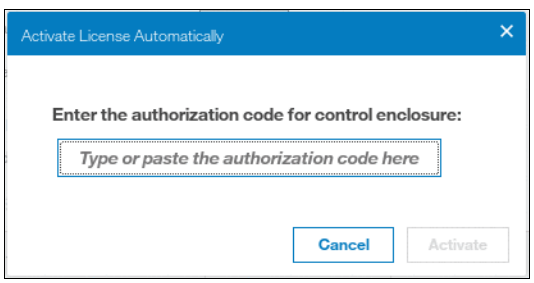


Figure 7-16 Encryption license Activate License Automatically window

2. Enter the authorization code that is specific to the node that you selected, as shown in Figure 7-17. You can now click **Activate**.

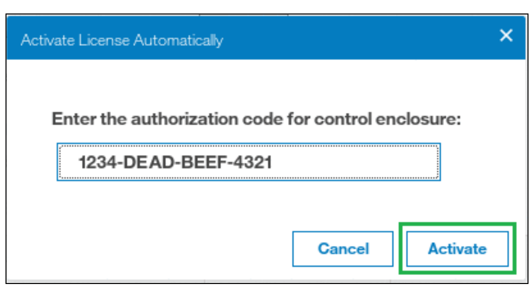


Figure 7-17 Entering an authorization code

The system connects to IBM to verify the authorization code and retrieve the license key. Figure 7-18 shows a window that is displayed during this connection. If everything works correctly, the procedure takes less than a minute.

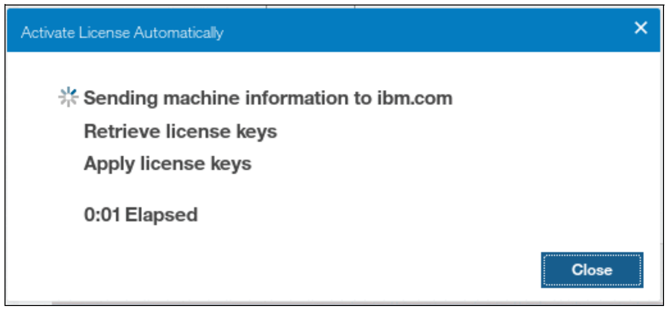


Figure 7-18 Activating encryption

After the license key has been retrieved, it is automatically applied as shown in Figure 7-19.

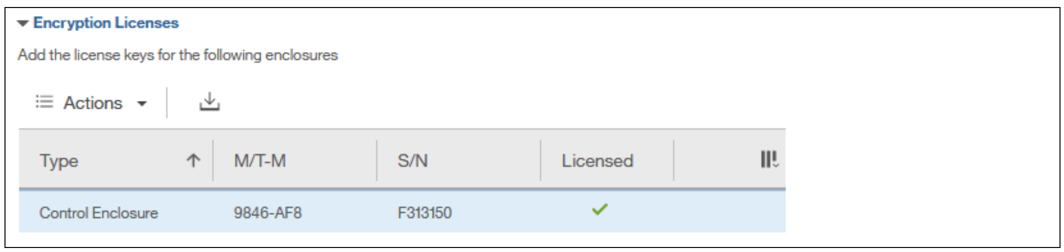


Figure 7-19 Successful encryption license activation

Problems with automatic license activation

If connections problems occur with the automatic license activation procedure, the system times out after 3 minutes with an error. Check whether the personal computer that is used to connect to the FS9100 Controller GUI and activate the license can access the internet. If you are unable to complete the automatic activation procedure, try to use the manual activation procedure that is described in "Activate the license manually" on page 255.

Although authorization codes and encryption license keys use the same format (four groups of four hexadecimal digits), you can only use each of them in the appropriate activation process. If you use a license key when the system expects an authorization code, the system displays an error message, as shown in Figure 7-20.

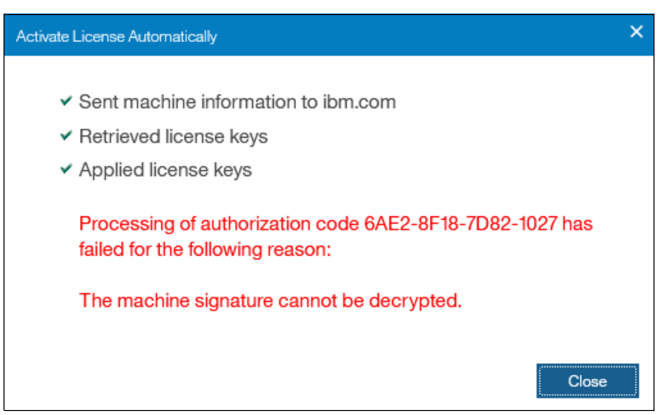


Figure 7-20 Authorization code failure

Activate the license manually

To manually activate the encryption license for a node, follow this procedure:

1. Select **Activate License Manually** to open the Manual Activation window, as shown in Figure 7-21.

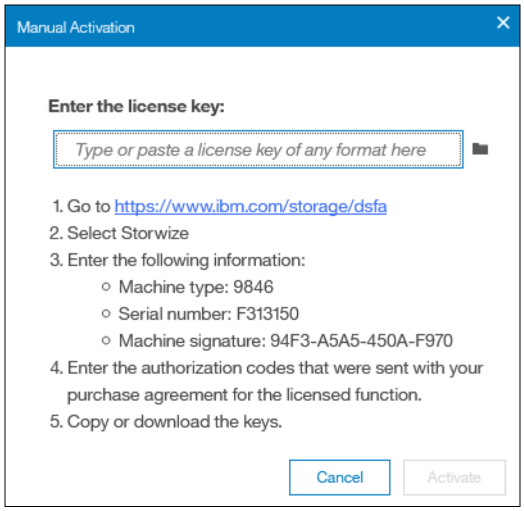


Figure 7-21 Manual encryption license activation window

2. If you have not done so already, obtain the encryption license for the node. The information that is required to obtain the encryption license is displayed in the Manual Activation window.
3. You can enter the license key either by typing it, by using cut or copy and paste, or by clicking the folder icon and uploading to the storage system the license key file downloaded from DSFA. In Figure 7-22, the sample key is already entered. Click **Activate**.

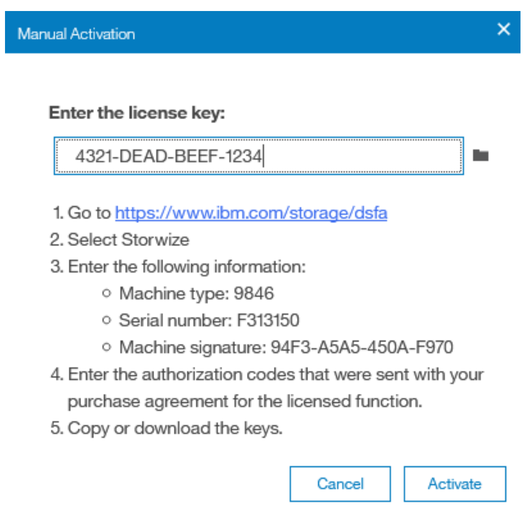


Figure 7-22 Entering an encryption license key

After the task completes successfully, the GUI shows that encryption is licensed for the specified node, as shown in Figure 7-23.

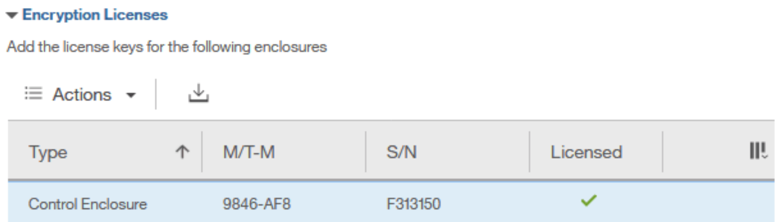


Figure 7-23 Successful encryption license activation

Problems with manual license activation

Although authorization codes and encryption license keys use the same format (four groups of four hexadecimal digits), you can only use each of them in the appropriate activation process. If you use an authorization code when the system expects a license key, the system displays an error message, as shown in Figure 7-24.

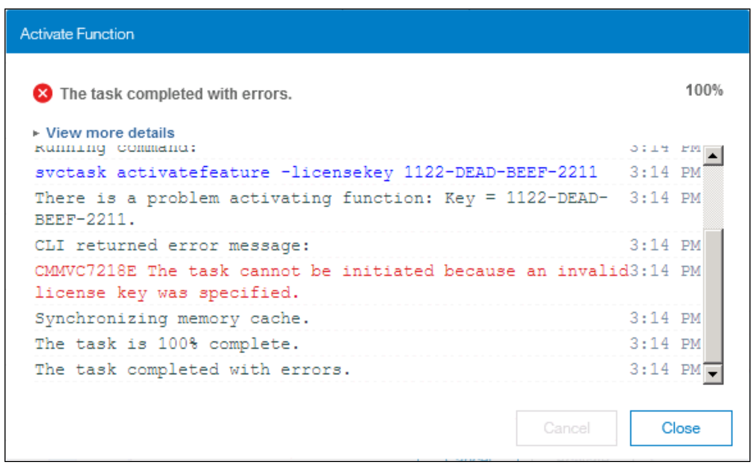


Figure 7-24 License key failure

7.4.3 Enabling Encryption

This section describes the process to create and store system master access key copies, also referred to as *encryption keys*. These keys can be stored on any or both of two key providers: USB flash drives or a key server.

Support for simultaneous use of both USB flash drives and a key server is available in IBM Spectrum Virtualize code V8.1 and later. Organizations that use encryption key management servers might consider parallel use of USB flash drives as a backup solution. During normal operation, such drives can be disconnected and stored in a secure location. However, during a catastrophic loss of encryption servers, the USB drives can still be used to unlock the encrypted storage.

The following list of key server and USB flash drive characteristics might help you to choose the type of encryption key provider that you want to use.

Key servers can have the following characteristics:

- Physical access to the system is not required to perform a rekey operation
- Support for businesses that have security requirements that preclude use of USB ports
- Possibility to use hardware security modules (HSMs) for encryption key generation
- Ability to replicate keys between servers and perform automatic backups
- Implementations follow an open standard (Key Management Interoperability Protocol (KMIP)) that aids in interoperability
- Ability to audit operations related to key management
- Ability to separately manage encryption keys and physical access to storage systems

USB flash drives have the following characteristics:

- Physical access to the system might be required to process a rekey operation
- No moving parts with almost no read or write operations to the USB flash drive
- Inexpensive to maintain and use
- Convenient and easy to have multiple identical USB flash drives available as backups

Important: Maintaining confidentiality of the encrypted data hinges on security of the encryption keys. Pay special attention to ensuring secure creation, management, and storage of the encryption keys.

Starting the Enable Encryption wizard

After the license activation step is successfully completed, you can now enable encryption. You can enable encryption after completion of the initial system setup by using either GUI or CLI. There are two ways in the GUI to start the Enable Encryption wizard. It can be started by clicking **Run Task** next to Enable Encryption on the Suggested Tasks window, as shown in Figure 7-25.

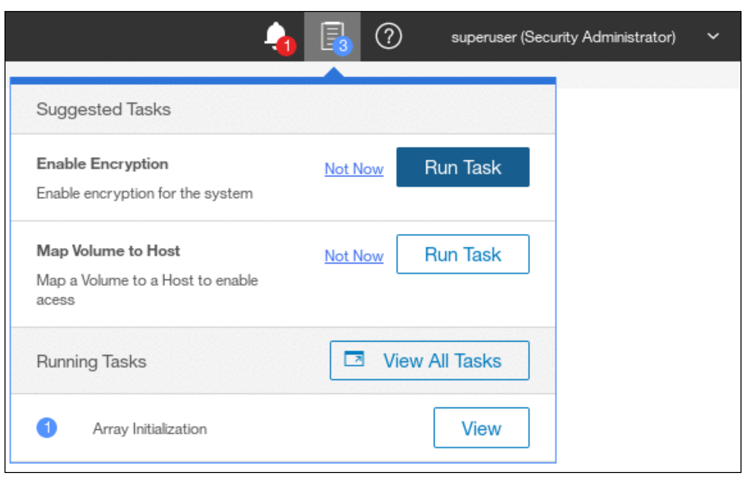


Figure 7-25 Enable Encryption from the Suggested Tasks *window*

You can also click **Settings** → **Security** → **Encryption** and click **Enable Encryption**, as shown in Figure 7-26.

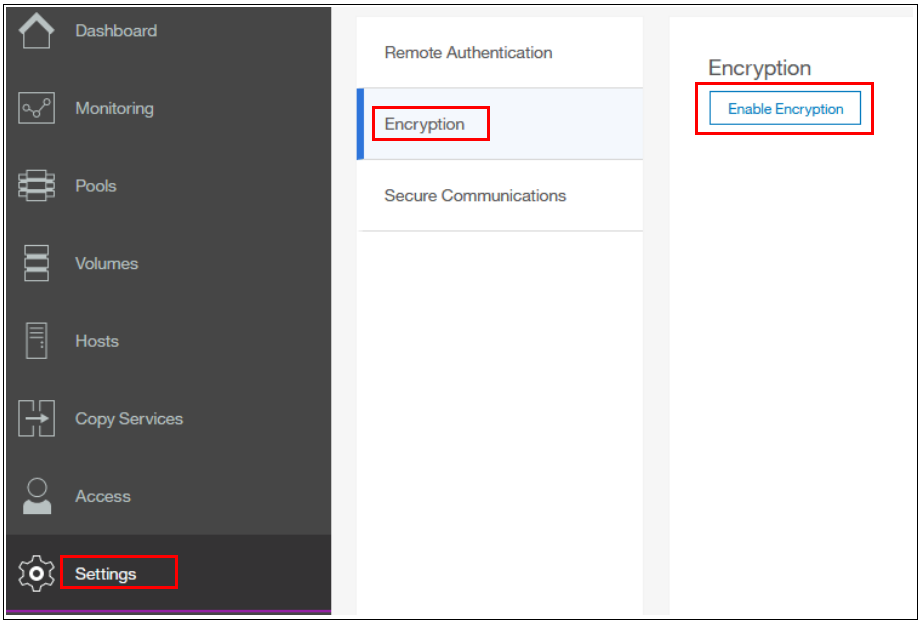


Figure 7-26 Enable Encryption from the Security pane

The Enable Encryption wizard starts by asking which encryption key provider to use for storing the encryption keys, as shown in Figure 7-27. You can enable either or both providers.

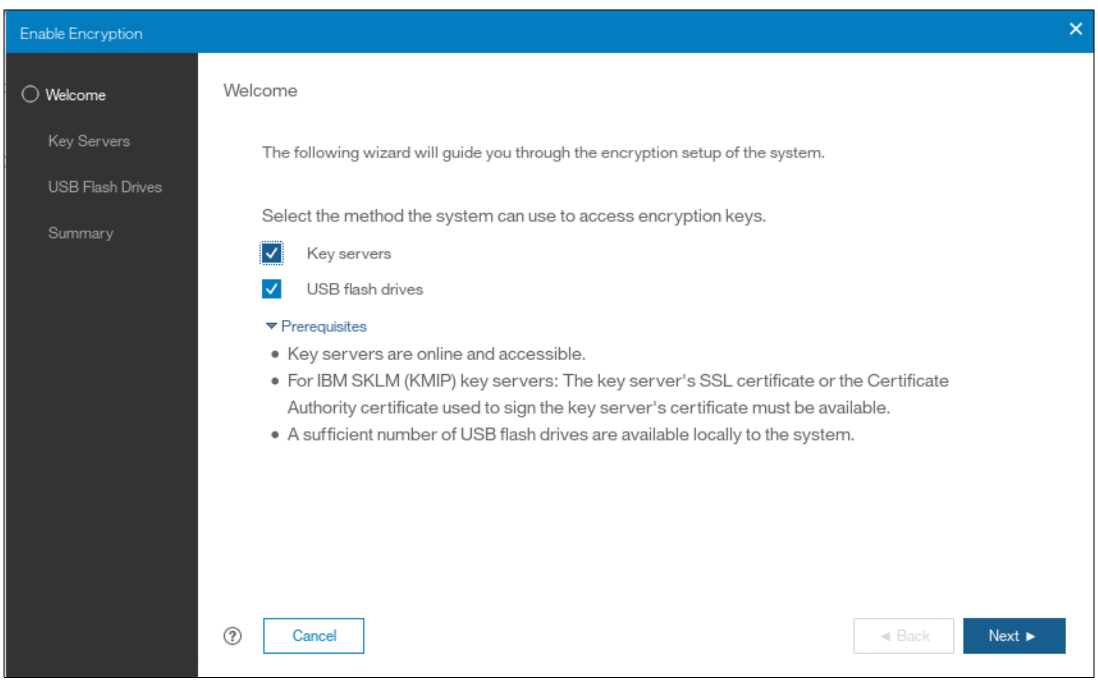


Figure 7-27 Enable Encryption wizard Welcome window

The next section will present a scenario in which both encryption key providers are enabled at the same time. See “Enabling encryption using USB flash drives” on page 259 for instructions on how to enable encryption using only USB flash drives.

See “Enabling encryption using key servers” on page 263 for instructions on how to enable encryption using key servers as the sole encryption key provider.

Enabling encryption using USB flash drives

Note: The system needs at least three USB flash drives to be present before you can enable encryption using this encryption key provider. IBM USB flash drives are preferred, although other flash drives might work. You can use any USB ports in any node of the cluster.

Using USB flash drives as the encryption key provider requires a minimum of three USB flash drives to store the generated encryption keys. Because the system will attempt to write the encryption keys to any USB key inserted into a node port, it is critical to maintain physical security of the system during this procedure.

While the system enables encryption, you are prompted to insert USB flash drives into the system. The system generates and copies the encryption keys to all available USB flash drives.

Ensure that each copy of the encryption key is valid before you write any user data to the system. The system validates any key material on a USB flash drive when it is inserted into the canister. If the key material is not valid, the system logs an error. If the USB flash drive is unusable or fails, the system does not display it as output.

If your system is in a secure location with controlled access, one USB flash drive for each canister can remain inserted in the system. If there is a risk of unauthorized access, then all USB flash drives with the master access keys must be removed from the system and stored in a secure place.

Securely store all copies of the encryption key. For example, any USB flash drives holding an encryption key copy that are not left plugged into the system can be locked in a safe. Similar precautions must be taken to protect any other copies of the encryption key that are stored on other media.

Notes: Generally, create at least one additional copy on another USB flash drive for storage in a secure location. You can also copy the encryption key from the USB drive and store the data on other media, which can provide additional resilience and mitigate risk that the USB drives used to store the encryption key come from a faulty batch.

Every encryption key copy must be stored securely to maintain confidentiality of the encrypted data.

A minimum of one USB flash drive with the correct master access key is required to unlock access to encrypted data after a system restart such as a system-wide reboot or power loss. No USB flash drive is required during a warm reboot, such as a node exiting service mode or a single node reboot. The data center power-on procedure needs to ensure that USB flash drives containing encryption keys are plugged into the storage system before it is powered on.

During power-on, insert USB flash drives into the USB ports on two supported canisters to safeguard against failure of a node, node’s USB port, or USB flash drive during the power-on procedure.

To enable encryption using USB flash drives as the only encryption key provider, complete these steps:

1. In the Enable Encryption wizard Welcome tab, select **USB flash drives** and click **Next**, as shown in Figure 7-28.

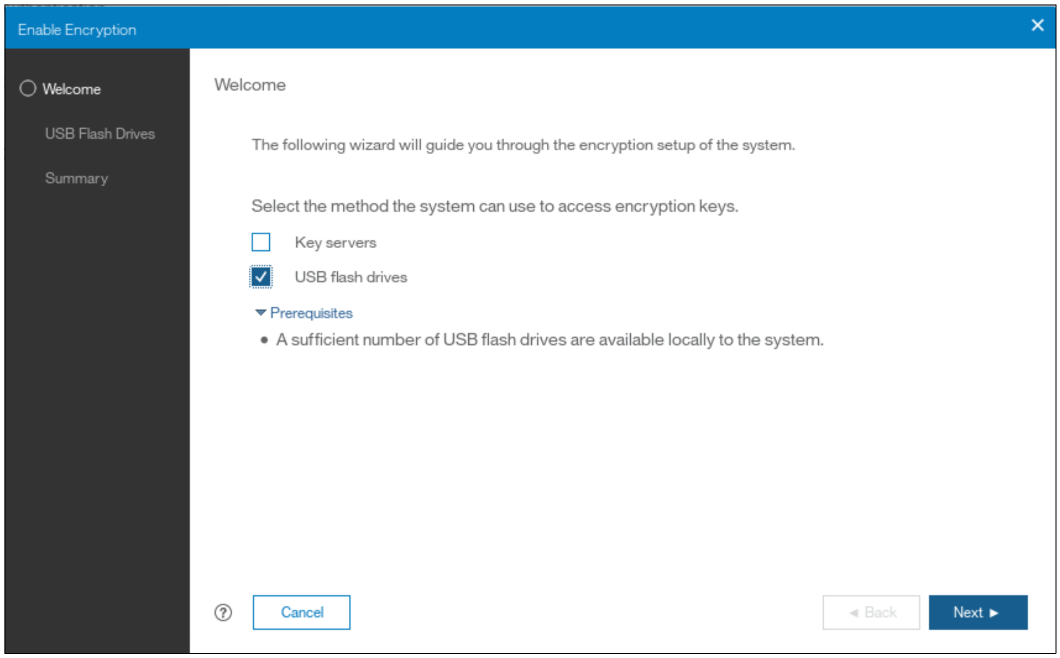


Figure 7-28 Selecting USB flash drives in the Enable Encryption wizard

2. If there are fewer than three USB flash drives inserted into the system, you are prompted to insert more drives, as shown in Figure 7-29. The system reports how many more drives need to be inserted.

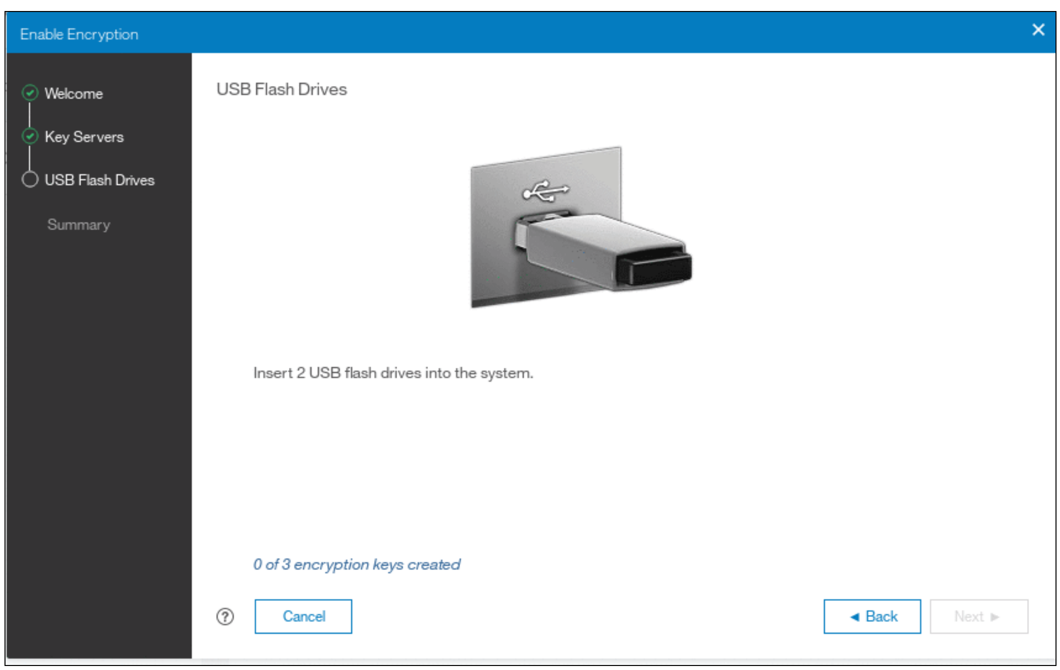


Figure 7-29 Waiting for USB flash drives to be inserted

Note: The **Next** option remains disabled and the status at the bottom is kept at 0 until at least three USB flash drives are detected.

3. Insert the USB flash drives into the USB ports as requested.
4. After the minimum required number of drives is detected, the encryption keys are automatically copied on the USB flash drives, as shown in Figure 7-30.

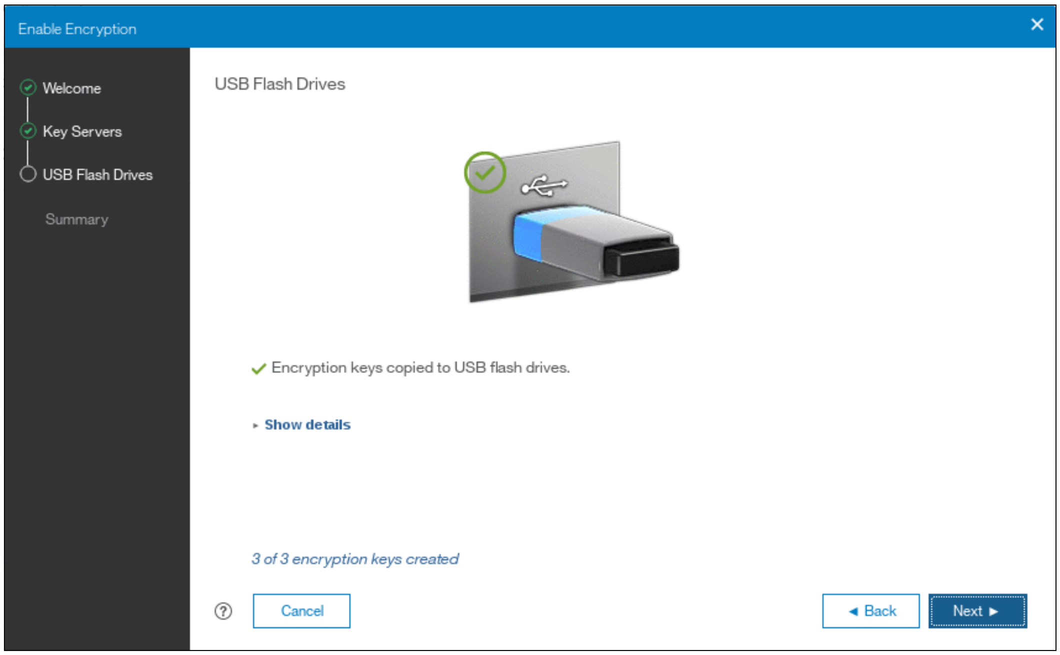


Figure 7-30 Writing the master access key to USB flash drives

5. You can keep adding USB flash drives or replacing the ones already plugged in to create new copies. When done, click **Next**.
6. The number of keys that were created is displayed in the Summary tab, as shown in Figure 7-31 on page 262. Click **Finish** to finalize the encryption enablement.

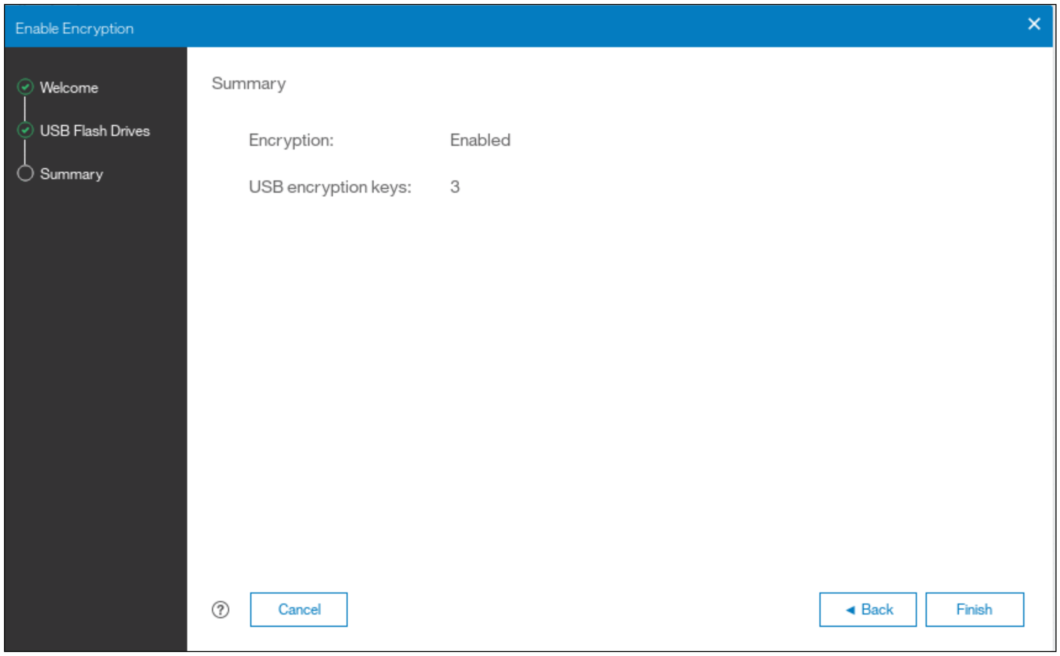


Figure 7-31 Commit the encryption enablement

7. You receive a message confirming that the encryption is now enabled on the system, as shown in Figure 7-32.

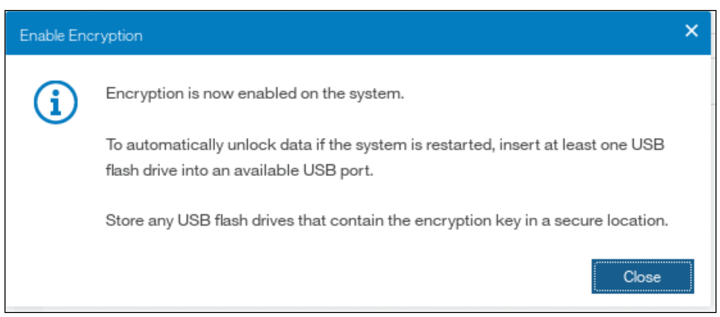


Figure 7-32 Encryption enabled message using USB flash drives

8. You can confirm that encryption is enabled and verify which key providers are in use by going to **Settings** → **Security** → **Encryption**, as shown in Figure 7-33.

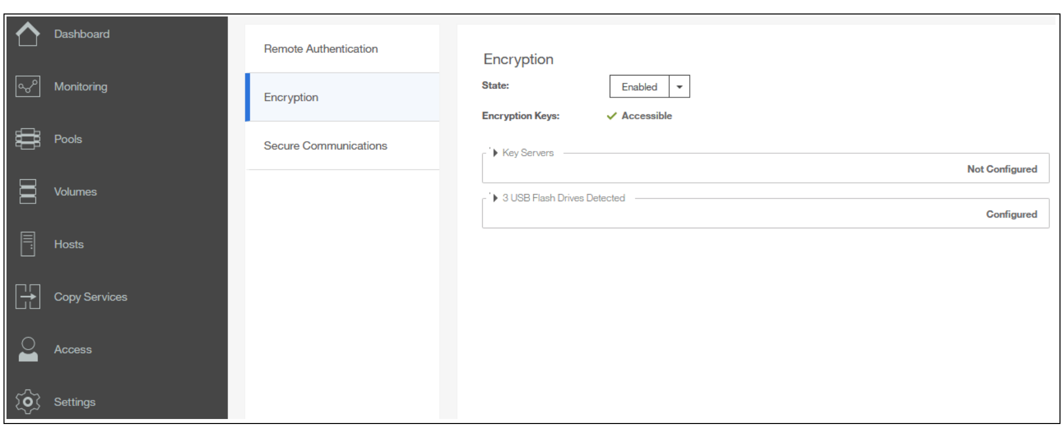


Figure 7-33 Encryption view showing using USB flash drives as the enabled provider

Enabling encryption using key servers

A key server is a centralized system that receives and then distributes encryption keys to its clients, including FlashSystem 9100 systems.

For steps on how to enable encryption using key servers, see the IBM Redbooks publication *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933 Encryption section.

7.4.4 Configuring secure communications

During system initialization, a *self-signed* SSL certificate is automatically generated by the system to encrypt communications between the browser and the system. Self-signed certificates generate web browser security warnings and might not comply with organizational security guidelines.

Signed SSL certificates are issued by a third-party certificate authority. A browser maintains a list of trusted certificate authorities, identified by their *root* certificate. The root certificate must be included in this list in order for the signed certificate to be trusted. If it is not, the browser presents security warnings.

To see the details of your current system certificate, click **Settings** → **Security** and select **Secure Communications**, as shown in Figure 7-34.

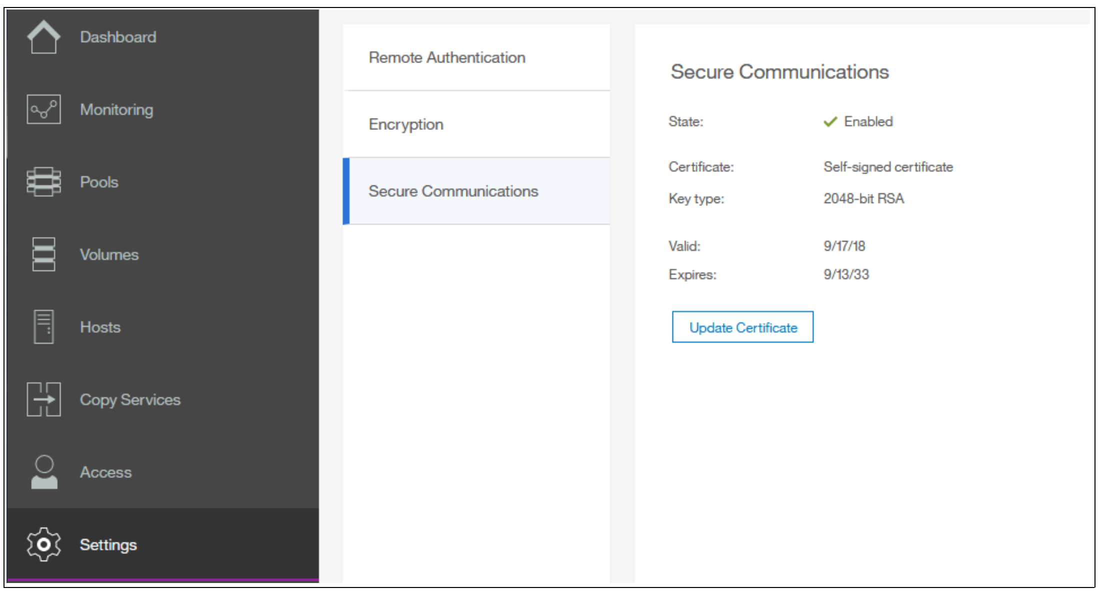


Figure 7-34 Accessing the Secure Communications window

The FS9100 allows you to generate a new self-signed certificate or to configure a signed certificate.

Configuring a signed certificate

Complete the following steps to configure a signed certificate:

1. Select **Update Certificate** on the Secure Communications window.
2. Select **Signed certificate** and enter the details for the new certificate signing request. All fields are mandatory, except for the email address. Figure 7-35 shows some values as an example.

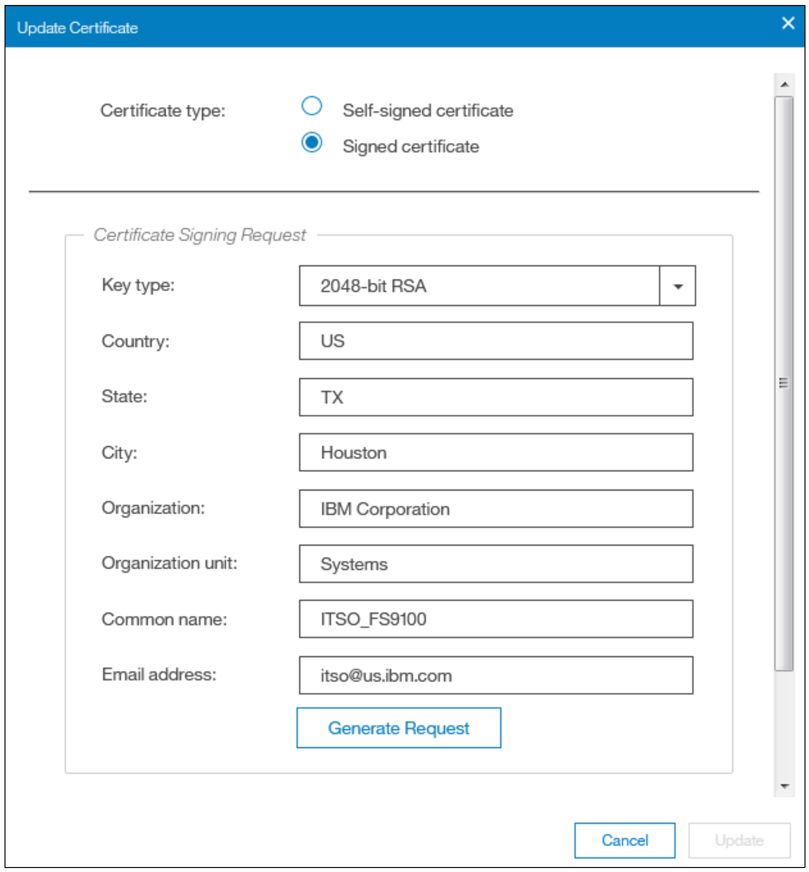


Figure 7-35 Generating a certificate request

> **Attention:** Before generating a request, ensure that your current browser does not have restrictions on the type of keys that are used for certificates. Some browsers limit the use of specific key-types for security and compatibility issues.

3. Click **Generate Request**.
4. Save the generated request file. The Secure Communications window now mentions that there is an outstanding certificate request, as shown in Figure 7-36 on page 265. This is the case until the associated signed certificate is installed.

> **Attention:** If you need to update a field in the certificate request, you can generate a new request. However, do *not* generate a new request after sending the original one to the certificate authority. Generating a new request overrides the original one and the signed certificate associated with the original request *cannot* be installed.

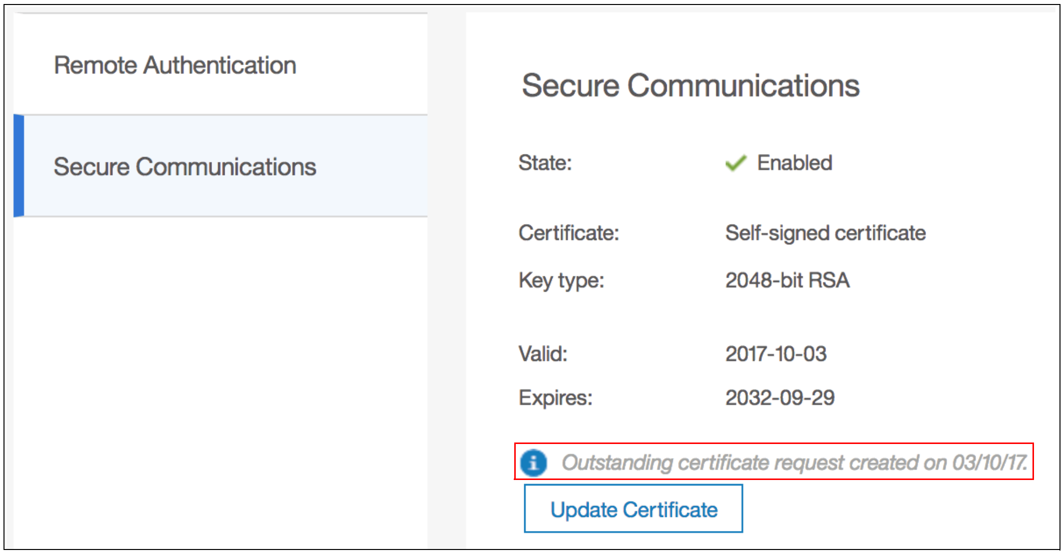


Figure 7-36 Outstanding certificate request

5. Submit the request to the certificate authority to receive a signed certificate.
6. When you receive the signed certificate, select **Update Certificate** on the Secure Communications window again.
7. Click the folder icon to upload the signed certificate, as shown in Figure 7-37. Click **Update**.

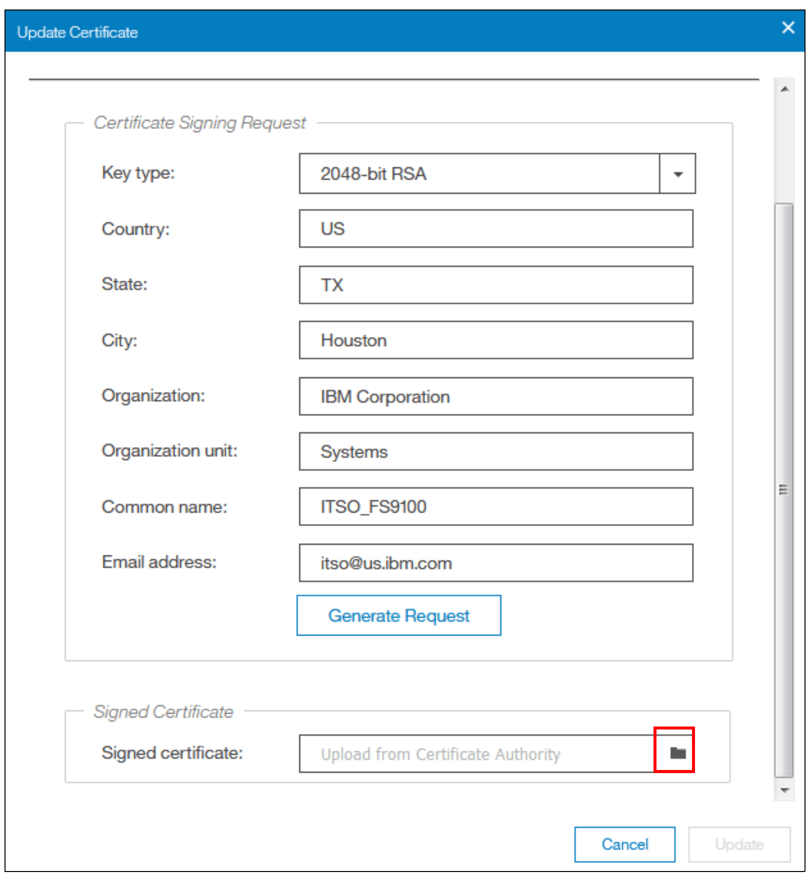


Figure 7-37 Installing a signed certificate

8. You are prompted to confirm the action, as shown in Figure 7-38. Click **Yes** to proceed. The signed certificate is installed.

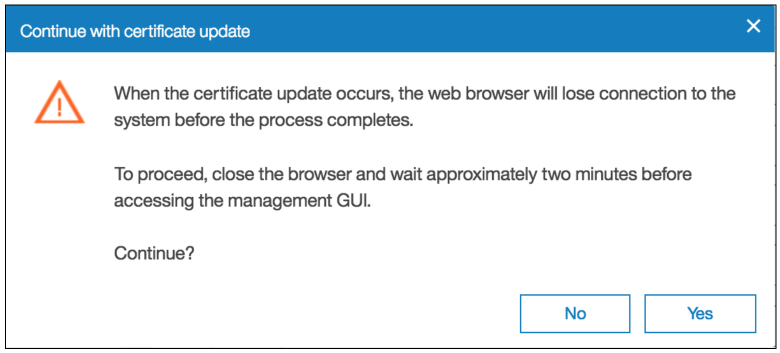


Figure 7-38 Certificate update warning

Generating a self-signed certificate

Complete the following steps to generate a self-signed certificate:

1. Select **Update Certificate** on the Secure Communications window.
2. Select **Self-signed certificate** and enter the details for the new certificate. Key type and validity days are the only mandatory fields. Figure 7-39 shows some example values.

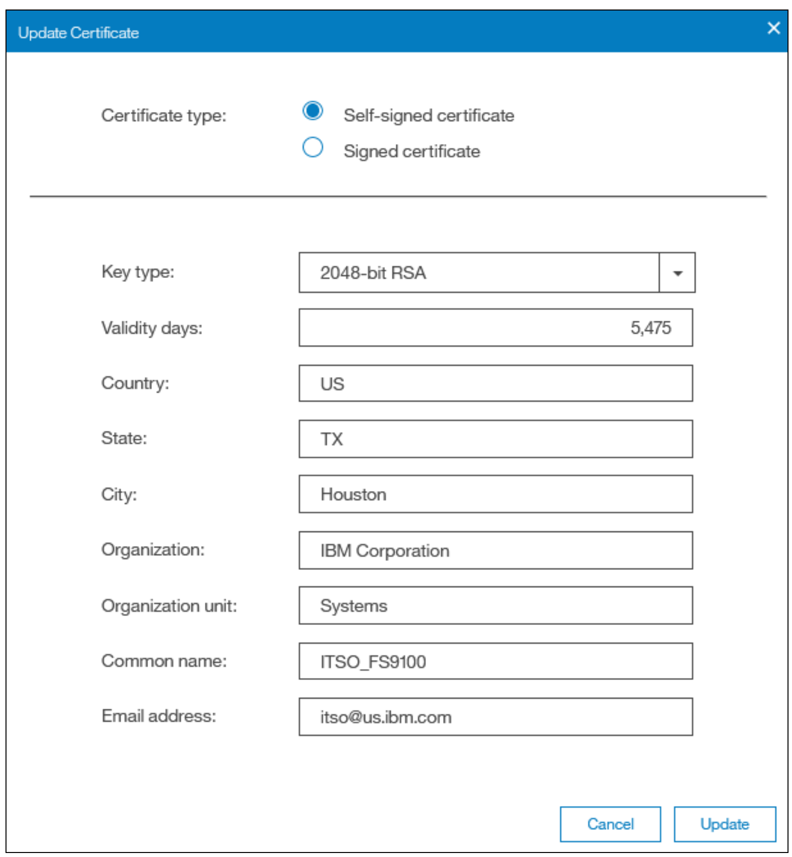


Figure 7-39 Generating a new self-signed certificate

Attention: Before creating a new self-signed certificate, ensure that your current browser does not have restrictions on the type of keys that are used for certificates. Some browsers limit the use of specific key-types for security and compatibility issues.

3. Click **Update**.
4. You are prompted to confirm the action, as shown in Figure 7-40. Click **Yes** to proceed. The self-signed certificate is generated immediately.

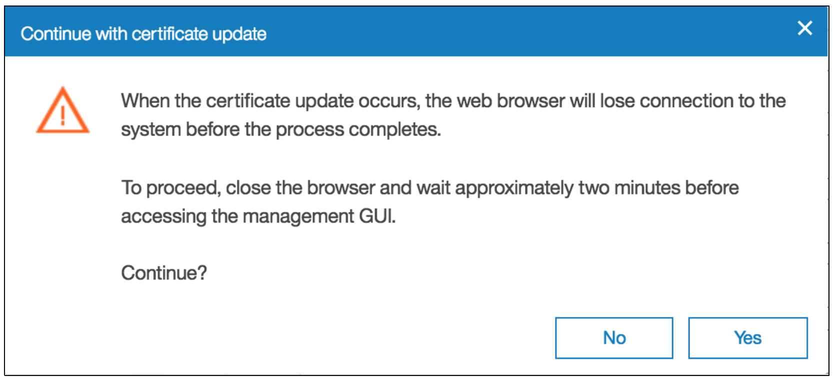


Figure 7-40 Certificate update warning

7.5 System menu

Use the **System** option from the **Settings** menu to view and change the time and date settings, work with licensing options, work with VMware VVOLs and IP Quorum, work with DNS settings, work with Transparent Cloud Tiering, or download software upgrade packages.

7.5.1 Date and time

Complete the following steps to view or configure the date and time settings:

1. From the FS9100 System pane, click the **Settings** menu item and click **System**.
2. In the left column, select **Date and Time**, as shown in Figure 7-41.

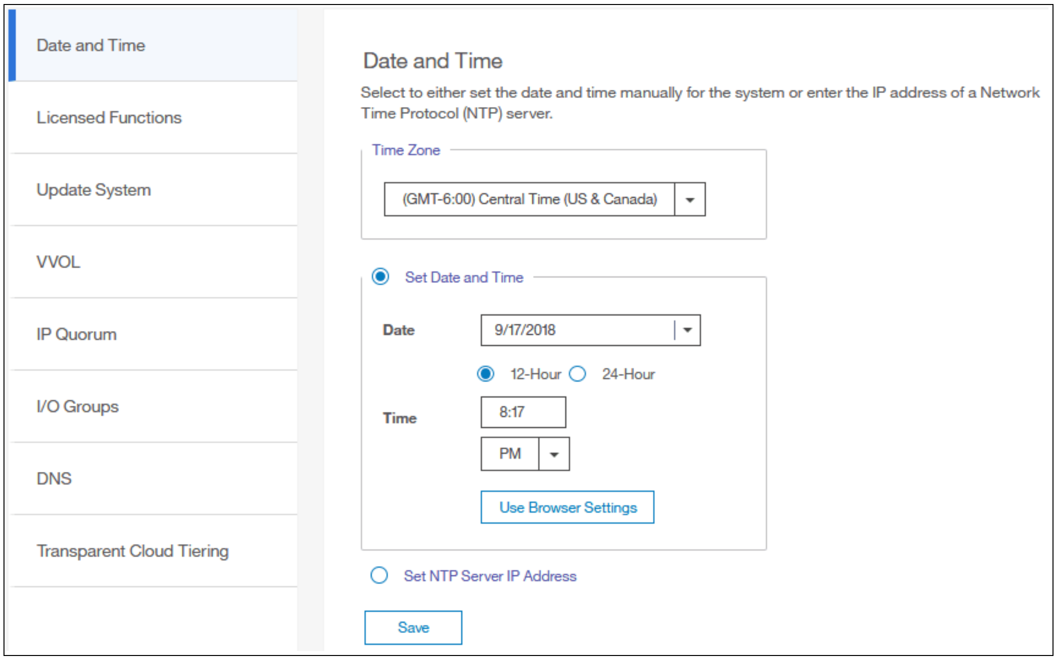


Figure 7-41 Date and Time window

3. From this pane, you can modify the following information:

   – **Time zone**

   Select a time zone for your system by using the drop-down list.

   – **Date and time**

   The following options are available:

   - If you are not using a Network Time Protocol (NTP) server, select **Set Date and Time**, and then manually enter the date and time for your system, as shown in Figure 7-42. You can also click **Use Browser Settings** to automatically adjust the date and time of your FS9100 system with your local workstation date and time.

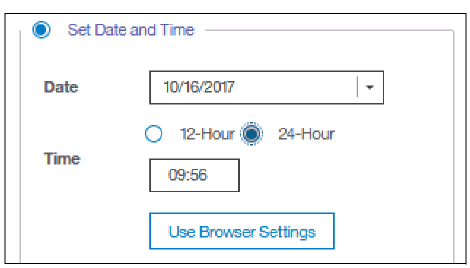


Figure 7-42 Set Date and Time window

   - If you are using an NTP server, select **Set NTP Server IP Address** and then enter the IP address of the NTP server, as shown in Figure 7-43 on page 269.

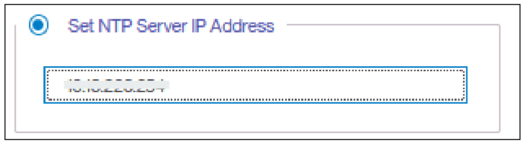


Figure 7-43 Set NTP Server IP Address window

4. Click **Save**.

7.5.2 Licensed Functions

The FS9100 supports an all-inclusive licensing model. For more information see 4.7, “Licensing and features” on page 107.

The system supports both differential and capacity-based licensing for externally virtualized storage. For the virtualization function, differential licensing charges different rates for different types of storage, which provides cost effective management of capacity across multiple tiers of storage. Licensing for these functions is based on the number of Storage Capacity Units (SCUs) purchased. With other functions applicable to externally virtualized storage, like remote mirroring and FlashCopy, the license grants a specific number of terabytes for that function.

Complete the following steps to view or configure the licensing settings:

1. From the FS9100 Settings menu, click **Settings** and click **System**.
2. In the left column, select **License Functions**, as shown in Figure 7-44.

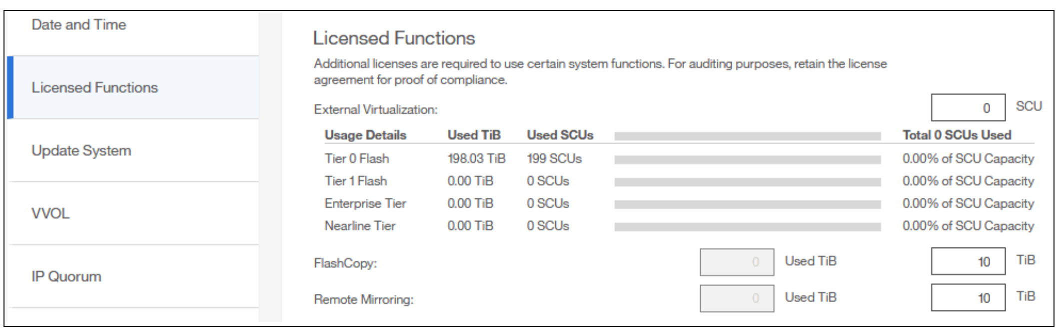


Figure 7-44 Licensing window

3. In the Licensed Functions pane, you can set the licensing options for the FS9100 for the following elements (limits are in TiB):

   – **External Virtualization**

     Enter the number of SCU units that are associated to External Virtualization for your FS9100 environment.

   – **FlashCopy Limit**

     Enter the capacity that is available for FlashCopy mappings, applicable to externally virtualized capacity.

> **Important:** The Used capacity for FlashCopy mapping is the sum of all of the volumes that are the source volumes of a FlashCopy mapping.

– **Remote Mirroring Limit**

Enter the capacity that is available for Metro Mirror and Global Mirror relationships, applicable to externally virtualized capacity.

> **Important:** The Used capacity for Global Mirror and Metro Mirror is the sum of the capacities of all of the volumes that are in a Metro Mirror or Global Mirror relationship. Both master volumes and auxiliary volumes are included.

– **Encryption Licenses**

In addition to the previous licensing models, the system also supports encryption through a key-based license. Key-based licensing requires an authorization code to activate encryption on the system.

During system setup, you can activate the license using the authorization code. The authorization code is sent with the licensed function authorization documents that you receive after purchasing the license.

For more details on encryption activation, see “Activating Encryption” on page 252.

Encryption is activated on a per-system basis. Figure 7-45 shows encryption licenses activated on the FS9100.

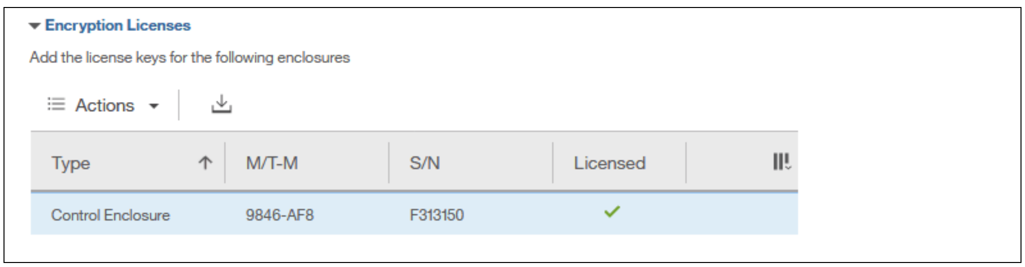


Figure 7-45 Encryption Licenses

7.5.3 Update System

This section describes the operations to update your FlashSystem 9100 software to V8.2.0.1.

The format for the software update package name ends in four positive integers that are separated by dots. For example, a software update package might have the following name:

```
IBM_FlashSystem9100_INSTALL_8.2.0.1
```

Precautions before the update

This section describes the precautions that you should take before you attempt an update.

> **Important:** Before you attempt any FS9100 code update, read and understand the FS9100 concurrent compatibility and code cross-reference matrix. For more information, see the following website and click **Latest FlashSystem 9100 code**:
>
> https://www.ibm.com/support/docview.wss?uid=ssg1S1012236

During the update, each node in your FS9100 clustered system is automatically shut down and restarted by the update process. Because each node in an I/O Group provides an alternative path to volumes, use the Subsystem Device Driver (SDD) to make sure that all I/O paths between all hosts and storage area networks (SANs) work.

If you do not perform this check, certain hosts might lose connectivity to their volumes and experience I/O errors when the FS9100 node that provides that access is shut down during the update process. You can check the I/O paths by using **datapath query** SDD commands.

IBM FlashSystem 9100 update test utility

The software update test utility is a FlashSystem 9100 software utility that checks for known issues that can cause problems during an FS9100 software update. More information about the utility is available on the following website:

http://www.ibm.com/support/docview.wss?rs=591&uid=ssg1S4000585

Download the software update utility from this page where you can also download the firmware. This procedure ensures that you get the current version of this utility. You can use the CLI command **svcupgradetest** utility to check for known issues that might cause problems during a software update, or perform this operation using the GUI.

The software update test utility can be downloaded in advance of the update process. Alternately, it can be downloaded and run directly during the software update, as guided by the update wizard. Always check that you have the latest version.

You can run the utility multiple times on the same IBM FlashSystem 9100 system to perform a readiness check in preparation for a software update. Run this utility for a final time immediately before you apply the software update to ensure that there were no new releases of the utility since it was originally downloaded.

The installation and use of this utility is non disruptive, and does not require restart of any FS9100 nodes. Therefore, there is no interruption to host I/O. The utility is only installed on the current configuration node.

System administrators must continue to check whether the version of code that they plan to install is the latest version. You can obtain the current information on the following website:

https://ibm.biz/BdYeEv

This utility is intended to supplement rather than duplicate the existing tests that are performed by the IBM FlashSystem 9100 update procedure (for example, checking for unfixed errors in the error log).

Concurrent software update of all components is supported through the standard Ethernet management interfaces. However, during the update process, most of the configuration tasks are restricted.

Updating your FlashSystem 9100

To update the IBM FlashSystem 9100 software, complete the following steps:

1. Open a supported web browser and navigate to your cluster IP address. A login window opens (Figure 7-46).

Figure 7-46 IBM FlashSystem 9100 GUI login window

2. Log in with superuser rights. The IBM FlashSystem 9100 management home window opens. Click **Settings** and click **System** (Figure 7-47).

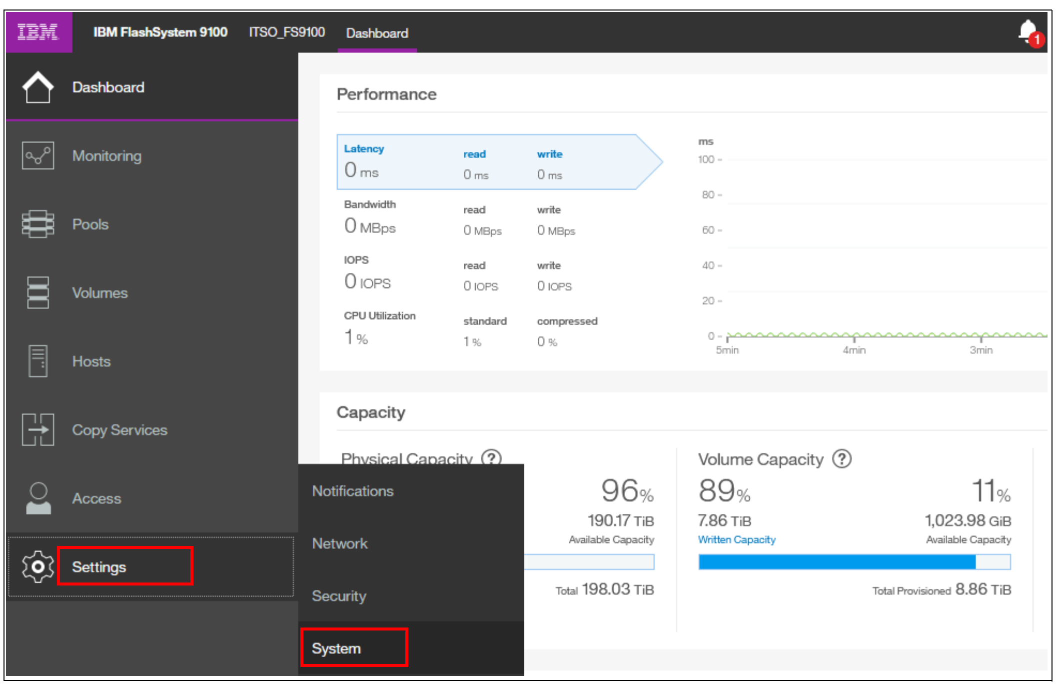


Figure 7-47 Settings menu

3. In the **System** menu, click **Update System**. The Update System window opens (Figure 7-48).

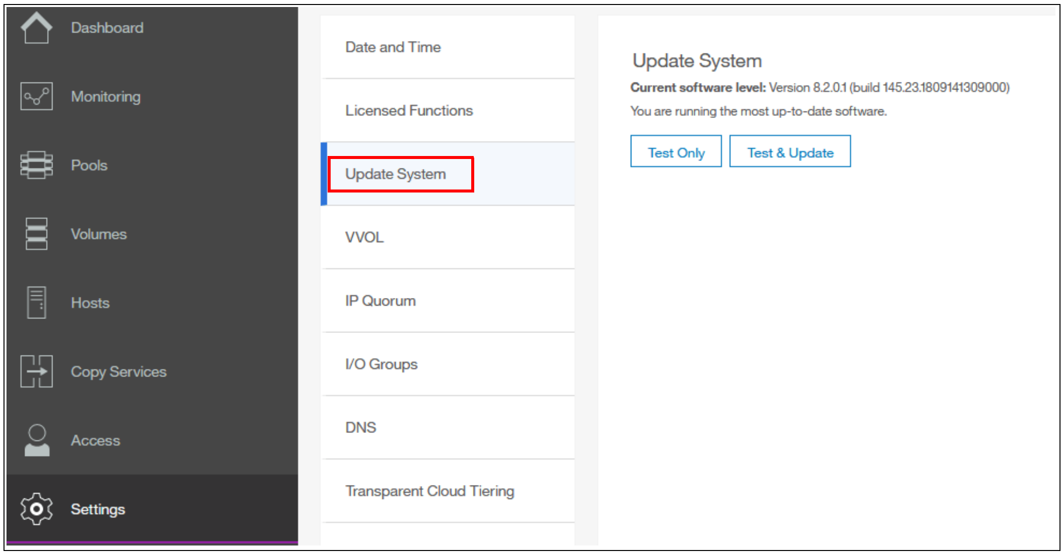


Figure 7-48 Update System window

4. From this window, you can select either to run the update test utility and continue with the code update or just run the test utility. For this example, we click **Test & Update.**

> **My Notifications:** Use the My Notifications tool to receive notifications of new and updated support information to better maintain your system environment, especially in an environment where a direct Internet connection is not possible.
>
> Go to the following address (an IBM account is required) and add your IBM FlashSystem 9100 system to the notifications list to be advised of support information, and to download the current code to your workstation for later upload:
>
> `http://www.ibm.com/software/support/einfo.html`

5. If you have previously downloaded both files from `https://ibm.biz/BdYeEv`, you can click each folder icon, browse to the location where you saved the files, and upload them to the FS9100. If the files are correct, the GUI detects and updates the target code level as shown in Figure 7-49.

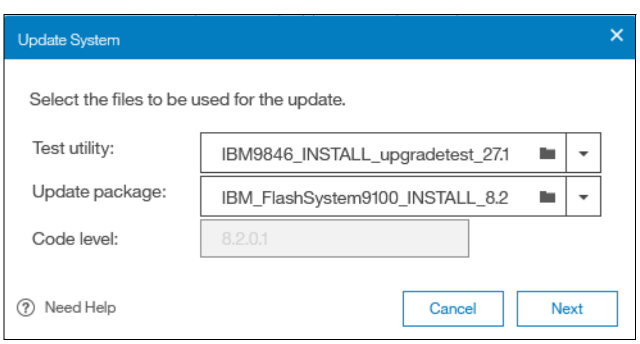


Figure 7-49 Upload option for both Test utility and Update Package

6. Select the type of update you want to perform, as shown in Figure 7-50. Select **Automatic update** unless IBM Support has suggested a **Service Assistant Manual update**. The manual update might be preferable in cases where misbehaving host multipathing is known to cause loss of access. Click **Next** to begin the update package upload process.

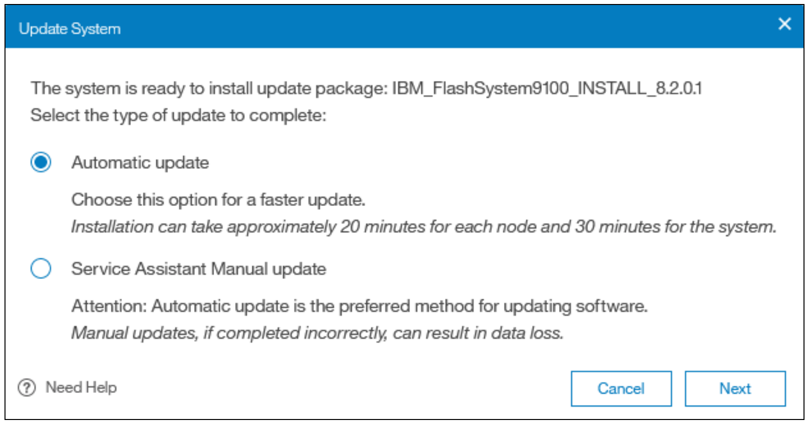


Figure 7-50 The update type selection

7. An additional window is displayed at this point allowing you to choose a fully automated update, one that pauses when half the nodes have completed update, or one that pauses after each node update, as shown in Figure 7-51. The pause options will require the **Resume** button to be clicked to continue the update after each pause. Click **Finish**.

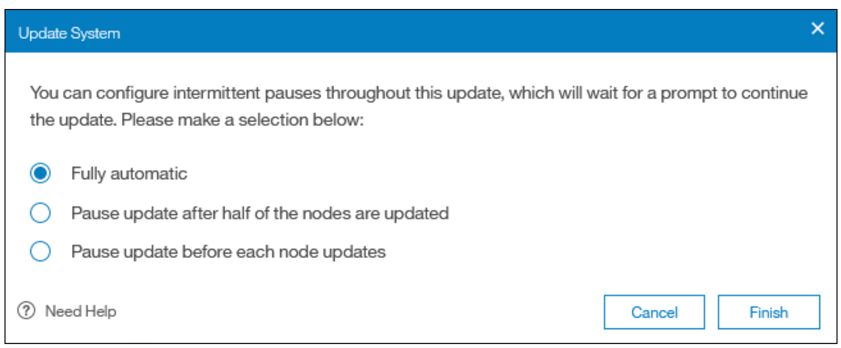


Figure 7-51 Update System options

8. After the update packages have uploaded, the update test utility looks for any known issues that might affect a concurrent update of your system. The GUI helps identify any detected issues.

9. Click **Update System** to return to the Update System window. Here, click **Read more** (Figure 7-52).

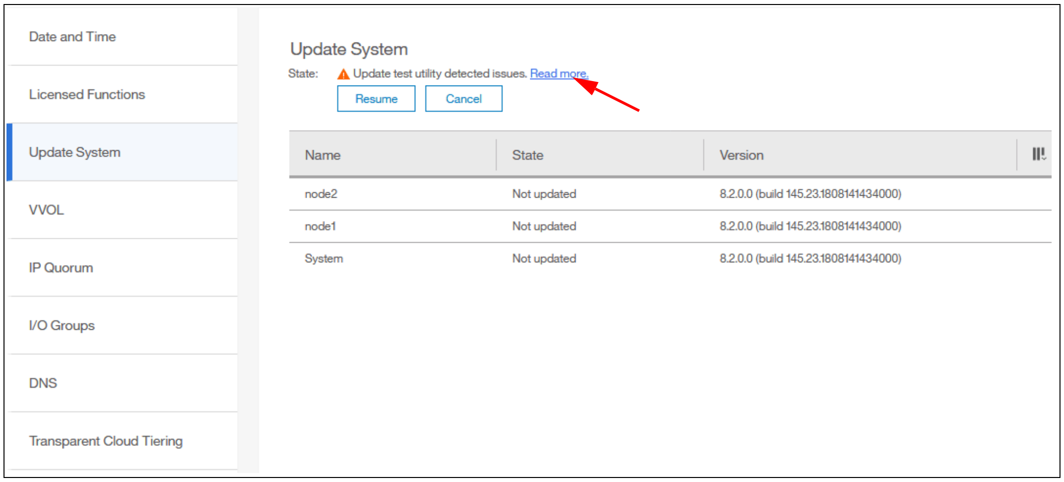


Figure 7-52 Issues detected by the update test utility

10. The results pane opens and shows you what issues were detected (Figure 7-53). In our case, the warning is that we have a potential unsupported character as part of our cluster name. Although this is not a recommended condition, it does not prevent the system update from running. Therefore, we can click **Close** and proceed with the update. However, you might need to contact IBM Support to assist with resolving more serious issues before continuing.

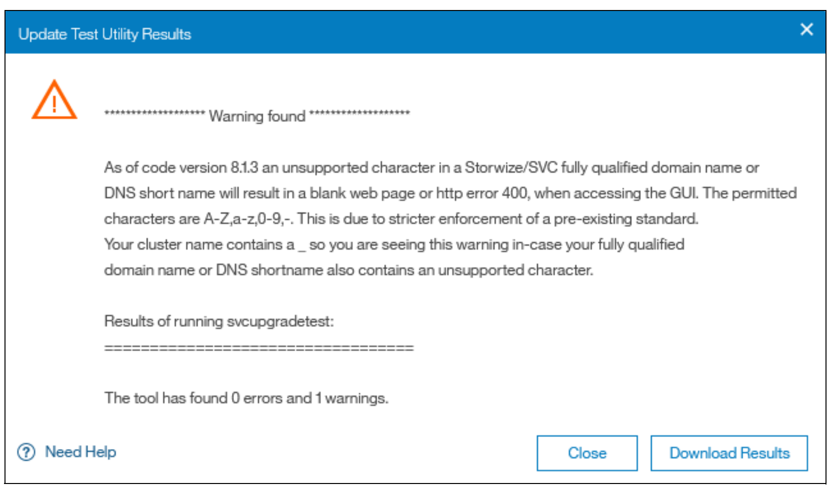


Figure 7-53 Description of the warning from the test utility

11.Click **Resume** on the Update System window and the update proceeds as shown in Figure 7-54.

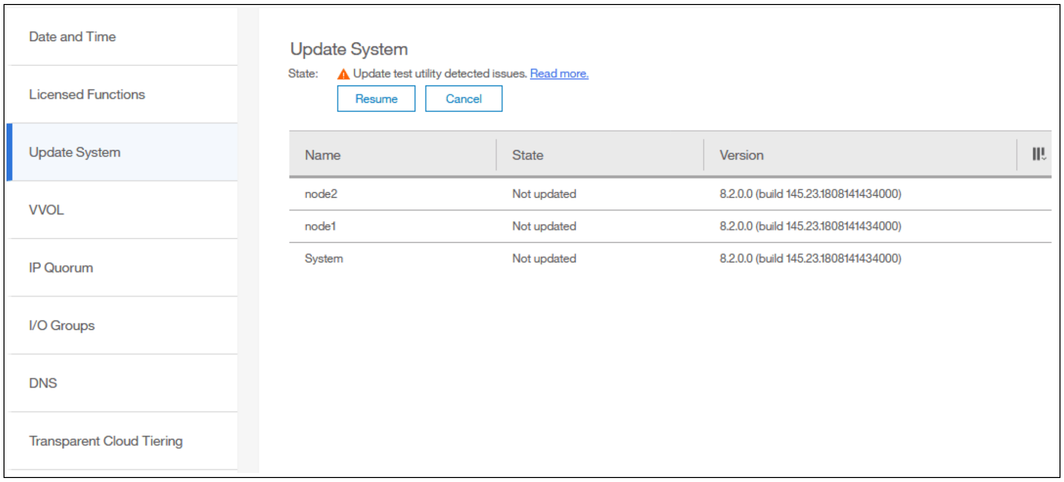


Figure 7-54 Resuming the update

12.Due to the utility detecting issues, another warning comes up to ensure that you have investigated them and are certain you want to proceed, as shown in Figure 7-55. When you are ready to proceed, click **Yes**.

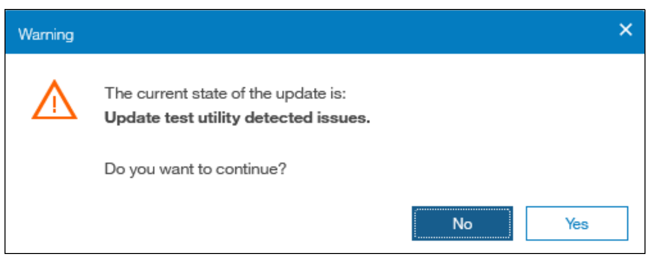


Figure 7-55 Warning before you can continue

13., The system begins updating the IBM FlashSystem 9100 software by taking one node offline and installing the new code. This process takes approximately 20 minutes. After the node returns from the update, it is listed as complete as shown in Figure 7-56.

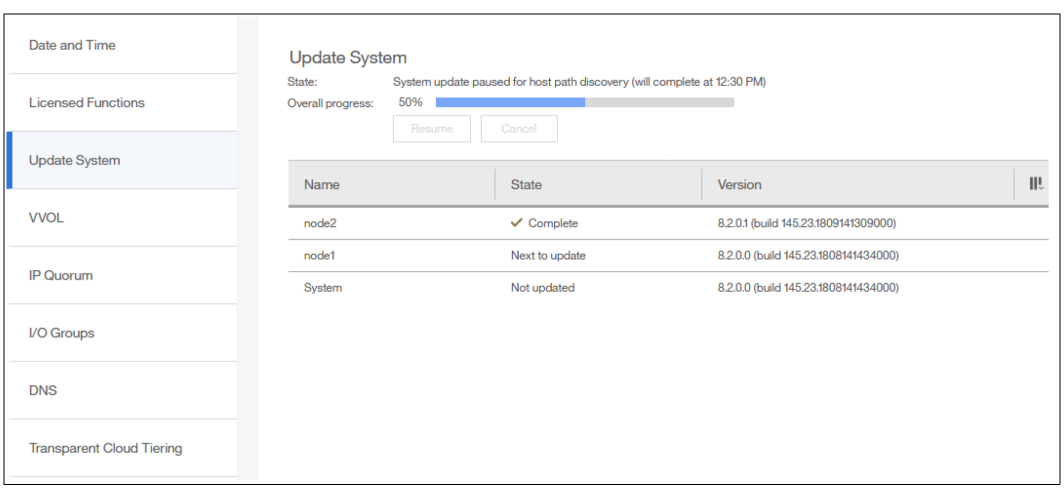


Figure 7-56 Update process paused for host path recovery

14. After a 30-minute pause, to ensure that multipathing has recovered on all attached hosts, a node failover occurs and you temporarily lose connection to the GUI. A warning window displays, prompting you to refresh the current session.

> **Tip:** The 30-minute wait period can be adjusted by using the `applysoftware` CLI command with the `-delay (mins)` parameter to begin the update instead of using the GUI.

15. We now see the status of the second node updating as shown in Figure 7-57.

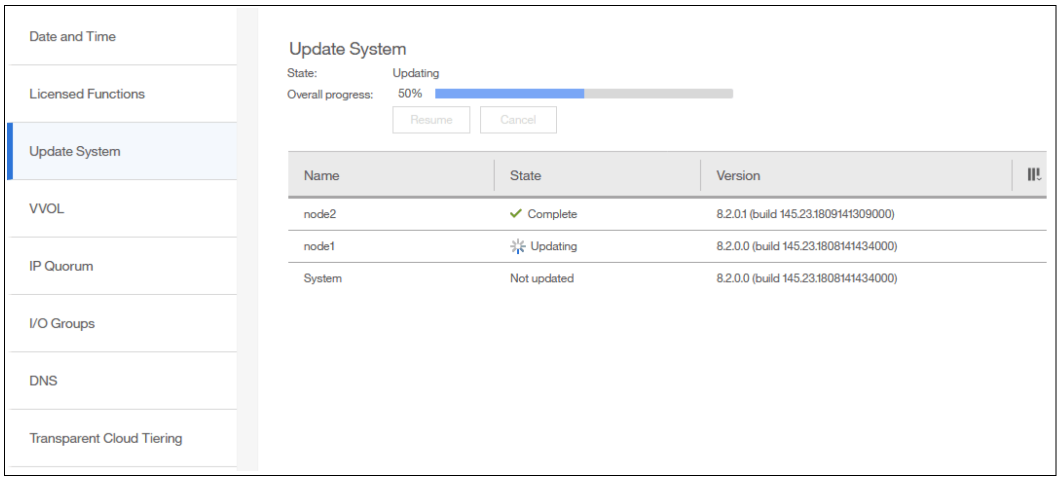


Figure 7-57 new GUI after node failover

After the second node completes, the update is committed to the system, as shown in Figure 7-58.

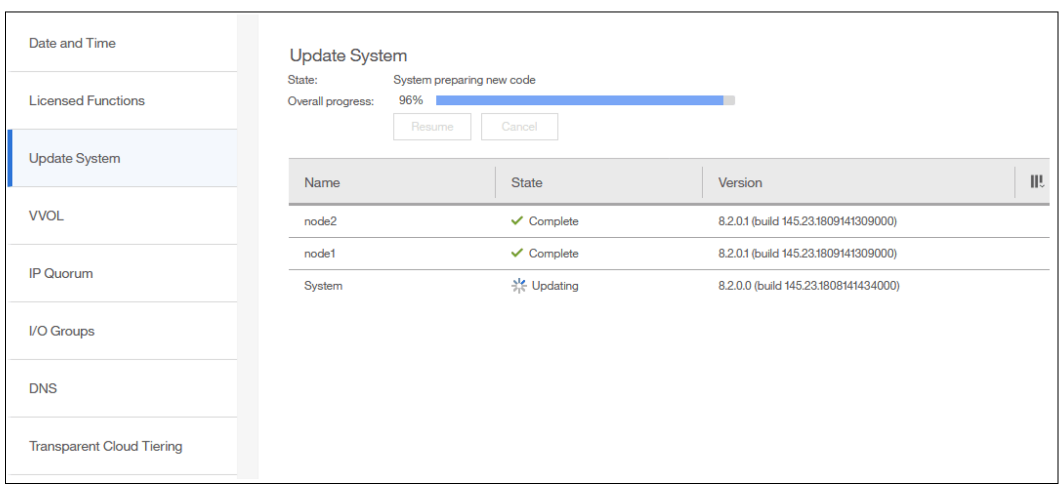


Figure 7-58 Updating system level

16. The update process completes when all nodes and the system unit are committed. The final status indicates the new level of code installed in the system, as shown in Figure 7-59.

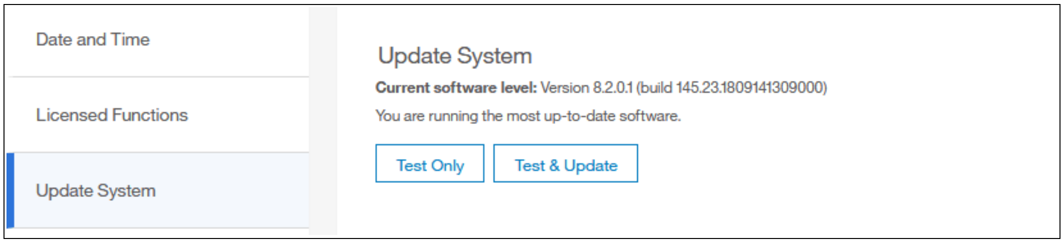


Figure 7-59 New level of installed software shown

Updating FlashSystem 9100 drive code

After completing the FlashSystem 9100 software update detailed in "Updating your FlashSystem 9100" on page 272, if available, also update the firmware of the FlashSystem 9100 drives.

For detailed steps on how to update drive firmware code, see the IBM Redbooks publication *Implementing the IBM Storwize V7000 with IBM Spectrum Virtualize V8.1*, SG24-7938, "RAS, monitoring, and troubleshooting → Software update → Updating IBM Storwize V7000 drive code" chapter.

Manually updating a FlashSystem 9100 scale-out configuration

This example assumes that you have a 4-system cluster of the IBM FlashSystem 9100, as illustrated in Table 7-1.

Table 7-1 The iogrp

iogrp (0)	iogrp (1)	iogrp (2)	iogrp (3)
node 1 (config node)	node 3	node 5	node 7
node 2	node 4	node 6	node 8

After uploading the update utility test and Software update package to the cluster using PSCP, and running the utility test, complete the following steps:

1. Start by removing node 2, which is the partner node of the configuration node in iogrp 0, using either the cluster GUI or CLI.
2. Log in to the service GUI to verify that the removed node is in `candidate` status.
3. Select the candidate node and click **Update Manually** from the left pane.
4. Browse and locate the code that you already downloaded and saved to your PC.
5. Upload the code and click **Update**.

   When the update is completed, a message caption indicating software update completion displays. The node then reboots, and appears again in the service GUI after approximately 20 - 25 minutes in `candidate` status.
6. Select the node and verify that it is updated to the new code.
7. Add the node back by using either the cluster GUI or the CLI.
8. Select node 3 from iogrp1.
9. Repeat steps 1 - 7 to remove node 3, update it manually, verify the code, and add it back to the cluster.

10. Proceed to node 5 in iogrp 2.
11. Repeat steps 1 - 7 to remove node 5, update it manually, verify the code, and add it back to the cluster.
12. Move on to node 7 in iogrp 3.
13. Repeat steps 1 - 7 to remove node 5, update it manually, verify the code, and add it back to the cluster.

> **Note:** At this point, the update is 50% completed. You now have one node from each iogrp updated with the new code manually. Always leave the configuration node for last during a manual software update.

14. Next, select node 4 from iogrp 1.
15. Repeat steps 1 - 7 to remove node 4, update it manually, verify the code, and add it back to the cluster.
16. Again, select node 6 from iogrp 2.
17. Repeat steps 1 - 7 to remove node 6, update it manually, verify the code, and add it back to the cluster.
18. Next, select node 8 in iogrp 3.
19. Repeat steps 1 - 7 to remove node 8, update it manually, verify the code, and add it back to the cluster.
20. Lastly, select and remove node 1, which is the configuration node in iogrp 0.

    > **Note:** A partner node becomes the configuration node because the original config node is removed from the cluster, keeping the cluster manageable.

    The removed configuration node becomes candidate, and you do not have to apply the code update manually. Simply add the node back to the cluster. It automatically updates itself and then adds itself back to the cluster with the new code.
21. After all the nodes are updated, you must confirm the update to complete the process. The confirmation restarts each node in order, which takes about 30 minutes to complete.

The update is complete.

7.5.4 VMware virtual volumes

The IBM FlashSystem FS9100 is able to manage VMware vSphere VVOLs directly in cooperation with VMware. It enables VMware virtual machines to get assigned disk capacity directly from the FS9100 rather than from the ESXi data store. That technique enables storage administrators to control the appropriate usage of storage capacity, and to enable enhanced features of storage virtualization directly to the virtual machine (such as replication, thin-provisioning, compression, encryption, and so on).

VVOL management is enabled in the FS9100 by clicking **Settings** → **System** → **VVOL**, as shown in Figure 7-60 on page 280. The NTP server must be configured before enabling VVOLs management. It is strongly advised to use the same NTP server for ESXi and for the FS9100.

> **Restriction:** You cannot enable VVOLs support until the NTP server is configured in the FS9100.

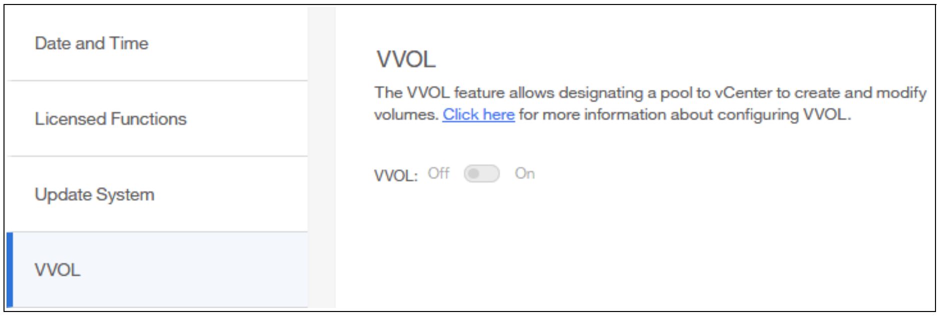


Figure 7-60 Enabling VVOLs management

For a quick-start guide to VVOLs, see *Quick-start Guide to Configuring VMware Virtual Volumes for Systems Powered by IBM Spectrum Virtualize*, REDP-5321.

In addition, see *Configuring VMware Virtual Volumes for Systems Powered by IBM Spectrum Virtualize*, SG24-8328.

7.5.5 IP Quorum

Enhanced stretched systems can use an IP-based quorum application as the quorum device for the third site, therefore no Fibre Channel connectivity is required. Java applications run on hosts at the third site.

To start with IP Quorum, complete the following steps:

1. If your IBM FlashSystem 9100 is configured with IP address version 4, click **Download IPv4 Application,** or select **Download IPv6 Application** for systems running with IP address version 6. In our example, IPv4 is the option as shown in Figure 7-61.

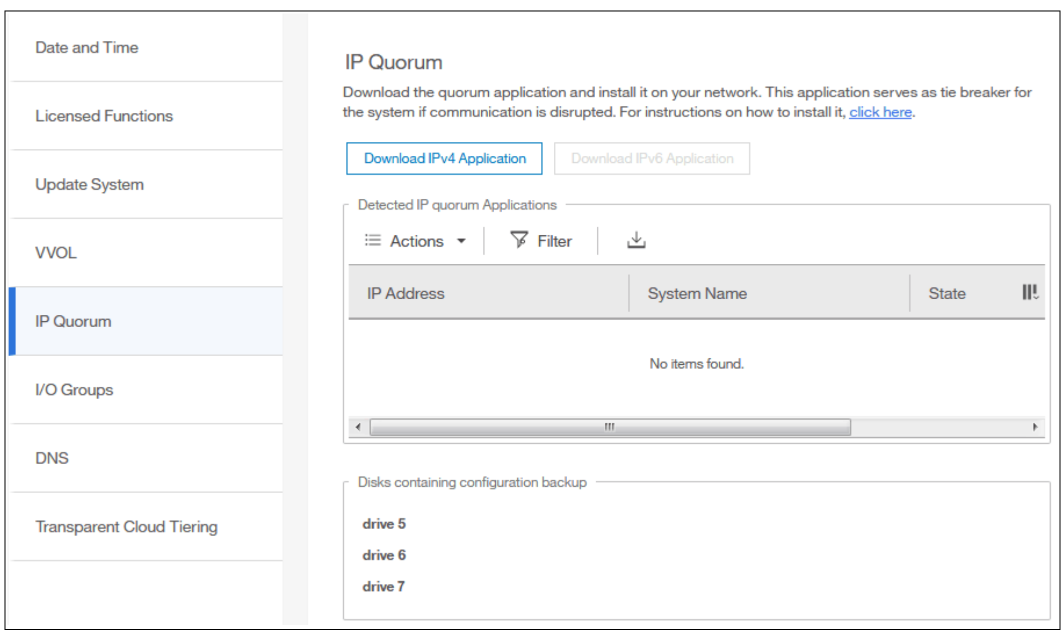


Figure 7-61 IP Quorum

2. Click **Download IPv4 Application** and the FS9100 generates an IP Quorum Java application as shown in Figure 7-62 on page 281. The application can be saved and installed in a host that is to run the IP quorum application.

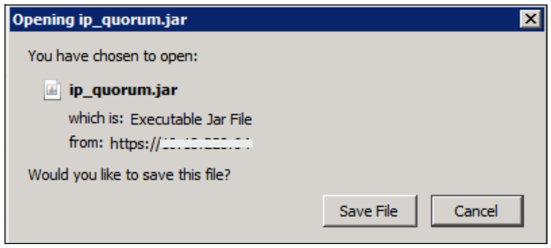


Figure 7-62 IP Quorum Java Application

3. On the host, you must use the Java command line to initialize the IP quorum application. Change to the folder where the application is located and run **`java -jar ip_quorum.jar`**.

7.5.6 I/O Groups

For ports within an I/O group, you can enable virtualization of Fibre Channel ports that are used for host I/O operations. With N_Port ID virtualization (NPIV), the Fibre Channel port consists of both a physical port and a virtual port. When port virtualization is enabled, ports do not come up until they are ready to handle I/O, which improves host behavior around node unpends. In addition, path failures due to an offline node are masked from hosts.

The target port mode on the I/O group indicates the current state of port virtualization:

- **Enabled:** The I/O group contains virtual ports that are available to use.
- **Disabled:** The I/O group does not contain any virtualized ports.
- **Transitional:** The I/O group contains both physical Fibre Channel and virtual ports that are currently being used. You cannot change the target port mode directly from enabled to disabled states, or vice versa. The target port mode must be in transitional state before it can be changed to either disabled or enabled states.

  The system can be in the transitional state for an indefinite period while the system configuration is changed. However, system performance can be affected because the number of paths from the system to the host doubled. To avoid increasing the number of paths substantially, use zoning or other means to temporarily remove some of the paths until the state of the target port mode is enabled.

The port virtualization settings of I/O groups are available by clicking **Settings** → **System** → **I/O Groups**, as shown in Figure 7-63.

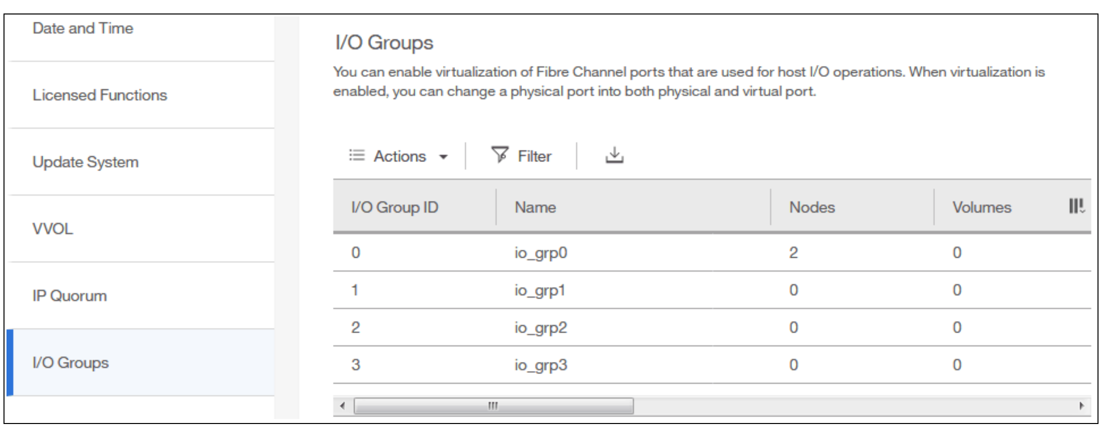


Figure 7-63 I/O Groups port virtualization

You can change the status of the port by right-clicking the wanted I/O group and selecting **Change Target Port Mode** as indicated in Figure 7-64.

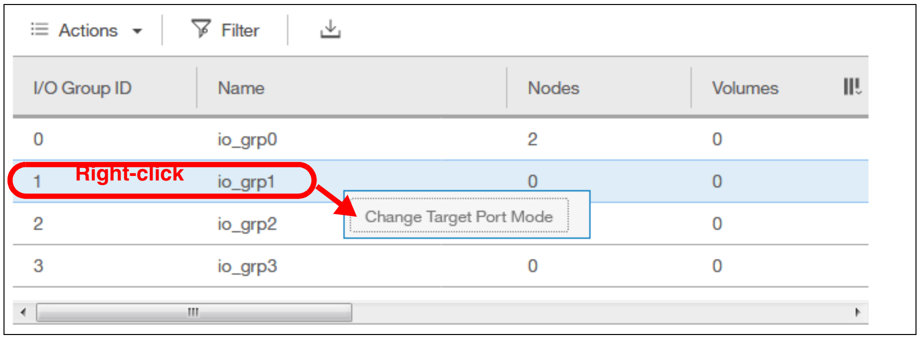


Figure 7-64 Changing port mode

7.5.7 Domain Name Server

The FlashSystem 9100 allows domain name server (DNS) entries to be manually set up. The information about the DNS servers in the FS9100 helps the system to access the DNS servers to resolve names of the computer resources that are in the external network.

To view and configure DNS server information in the FS9100, complete the following steps:

1. In the left pane, click the **DNS** item and enter the **IP address** and the **Name** of each DNS server. The FS9100 supports up two DNS Servers, IPv4 or IPv6. See Figure 7-65.

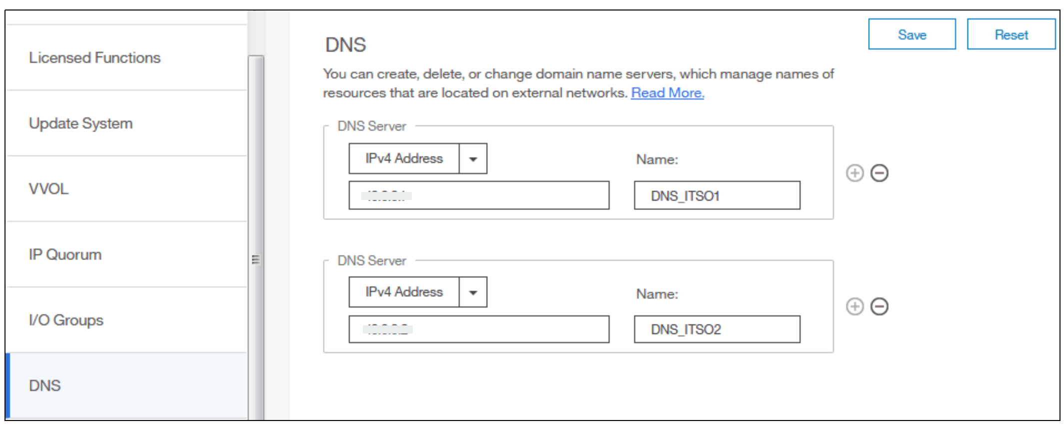


Figure 7-65 DNS information

2. Click **Save** after you enter the DNS server information.

7.5.8 Transparent cloud tiering

Transparent cloud tiering is a licensed function that enables volume data to be copied and transferred to cloud storage. The system supports creating connections to cloud service providers to store copies of volume data in private or public cloud storage.

With transparent cloud tiering, administrators can move older data to cloud storage to free up capacity on the system. Point-in-time snapshots of data can be created on the system and then copied and stored on the cloud storage. An external cloud service provider manages the cloud storage, which reduces storage costs for the system. Before data can be copied to cloud storage, a connection to the cloud service provider must be created from the system.

A cloud account is an object on the system that represents a connection to a cloud service provider by using a particular set of credentials. These credentials differ depending on the type of cloud service provider that is being specified. Most cloud service providers require the host name of the cloud service provider and an associated password, and some cloud service providers also require certificates to authenticate users of the cloud storage.

Public clouds use certificates that are signed by well-known certificate authorities. Private cloud service providers can use either self-signed certificate or a certificate that is signed by a trusted certificate authority. These credentials are defined on the cloud service provider and passed to the system through the administrators of the cloud service provider. A cloud account defines whether the system can successfully communicate and authenticate with the cloud service provider by using the account credentials.

If the system is authenticated, it can then access cloud storage to either copy data to the cloud storage or restore data that had previously been copied to cloud storage back to the system. The system supports one cloud account to a single cloud service provider. Migration between providers is not supported.

Important: Before enabling Transparent Cloud Tiering, consider the following requirements:

- Ensure that the DNS server is configured on your system and accessible.
- Determine whether your company's security policies require enabled encryption. If yes, make sure that the encryption licenses are properly installed and that encryption is enabled.

Each cloud service provider requires different configuration options. The system supports the following cloud service providers:

- IBM Bluemix® (also known as SoftLayer® Object Storage)
- OpenStack Swift
- Amazon S3

To view your system cloud provider settings, from the FS9100 Settings pane, click **Settings** and click **System,** then select **Transparent Cloud Tiering**, as shown in Figure 7-66.

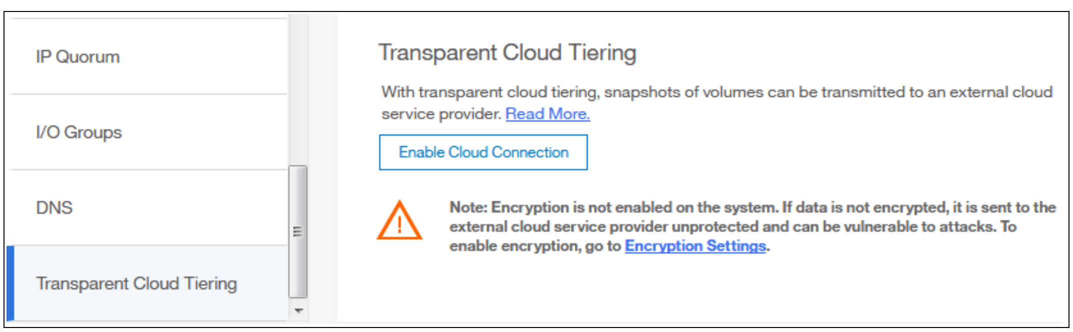


Figure 7-66 Transparent Cloud Tiering settings

Using this view, you can enable and disable features of your Transparent Cloud Tiering and update the system information concerning your cloud service provider. This pane allows you to set a number of options:

- Cloud service provider
- Object Storage URL
- Tenant or the container information that is associated with your cloud object storage
- User name of the cloud object account

- API Key
- The container prefix or location of your object
- Encryption
- Bandwidth

For detailed instructions on how to configure and enable Transparent Cloud Tiering, see the IBM Redbooks publication *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933, Advanced Copy Services → Implementing Transparent Cloud Tiering chapter.

7.6 Support menu

Use the **Support** pane to configure and manage support connections and upload support packages to the support center.

Two options are available from the menu and described in the following sections.

7.6.1 Support assistance

This option enables support personnel to access the system to complete troubleshooting and maintenance tasks. You can configure either local support assistance, where support personnel visit your site to fix problems with the system, or remote support assistance. Both local and remote support assistance use secure connections to protect data exchange between the support center and system. More access controls can be added by the system administrator.

For more information on Support Assistance, see 4.4.7, “Remote Support Assistance (RSA)” on page 93.

To configure Support Assistance, complete the following steps:

1. Click the **Settings** tab.
2. Click **Support**.

3. Click **Support Assistance**, as shown in Figure 7-67.

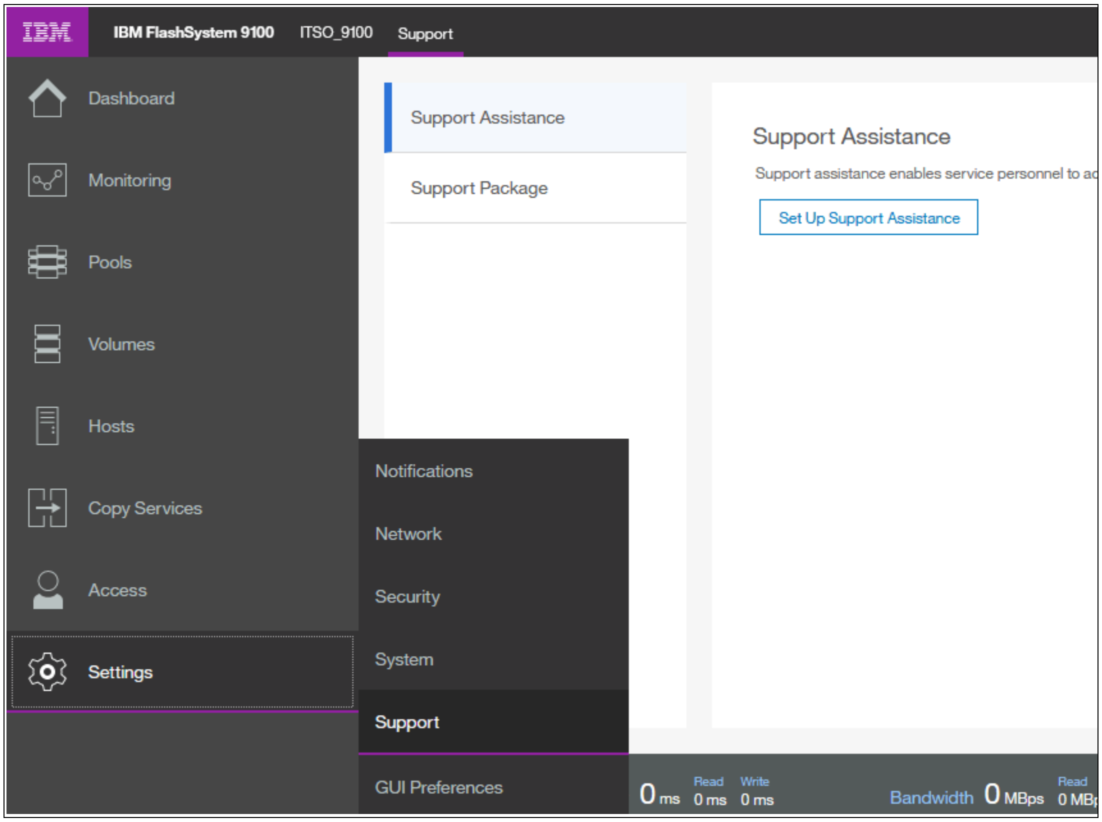


Figure 7-67 Remote Support Assistance menu

4. Click **Set Up Support Assistance,** which opens a wizard to guide you through the remaining configuration steps.
5. Figure 7-68 on page 286 shows the first wizard window. Choose not to enable remote assistance by selecting **I want support personnel to work on-site only** or enable remote assistance by choosing **I want support personnel to access my system both on-site and remotely**. Click **Next**.

> **Note:** Selecting **I want support personnel to work on-site only** does not entitle you to expect IBM support to attend on-site for all issues. Most maintenance contracts are for customer-replaceable units (CRU) support, where IBM diagnoses your problem and will send a replacement component for you to replace if required. If you prefer to have IBM perform replacement tasks for you, then contact your local sales person to investigate an upgrade to your current maintenance contract.

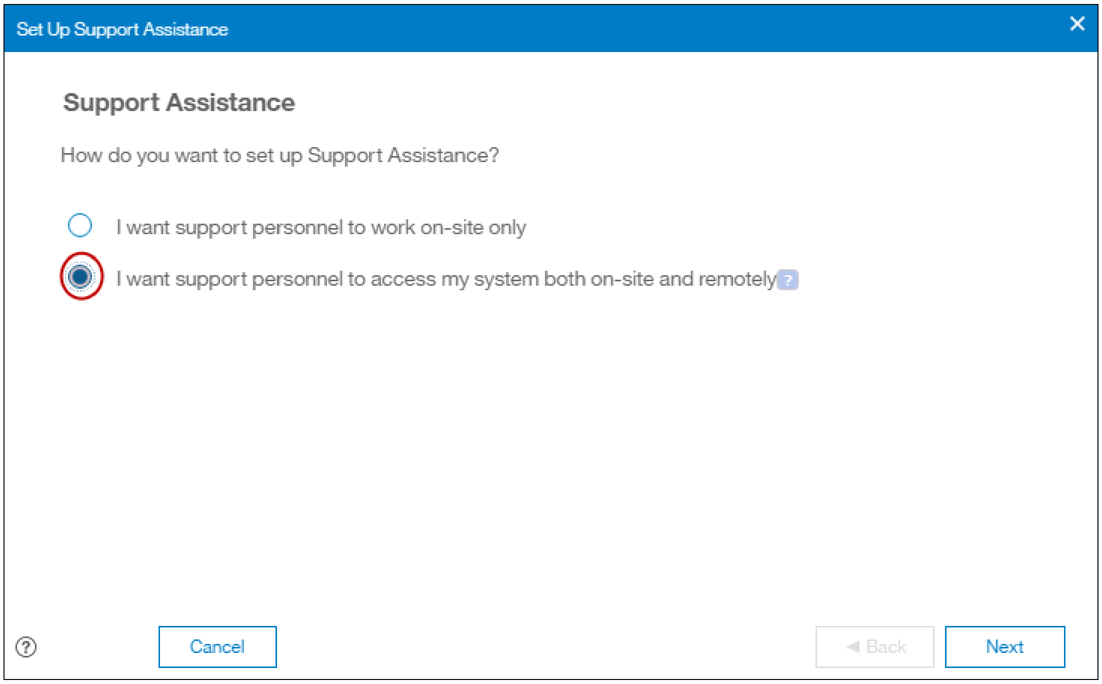


Figure 7-68   Remote Support wizard enable or disable

6. The next window, shown in Figure 7-69, lists the IBM Support center's IP addresses and SSH port that will need to be opened in your firewall. You can also define a Remote Support Assistance Proxy if you have multiple FS9100s or IBM Spectrum Virtualize systems in the data center, allowing for firewall configuration only being required for the Proxy Server rather than for every storage system. Because we do not have a proxy server in our environment, we leave the field blank and then click **Next**.

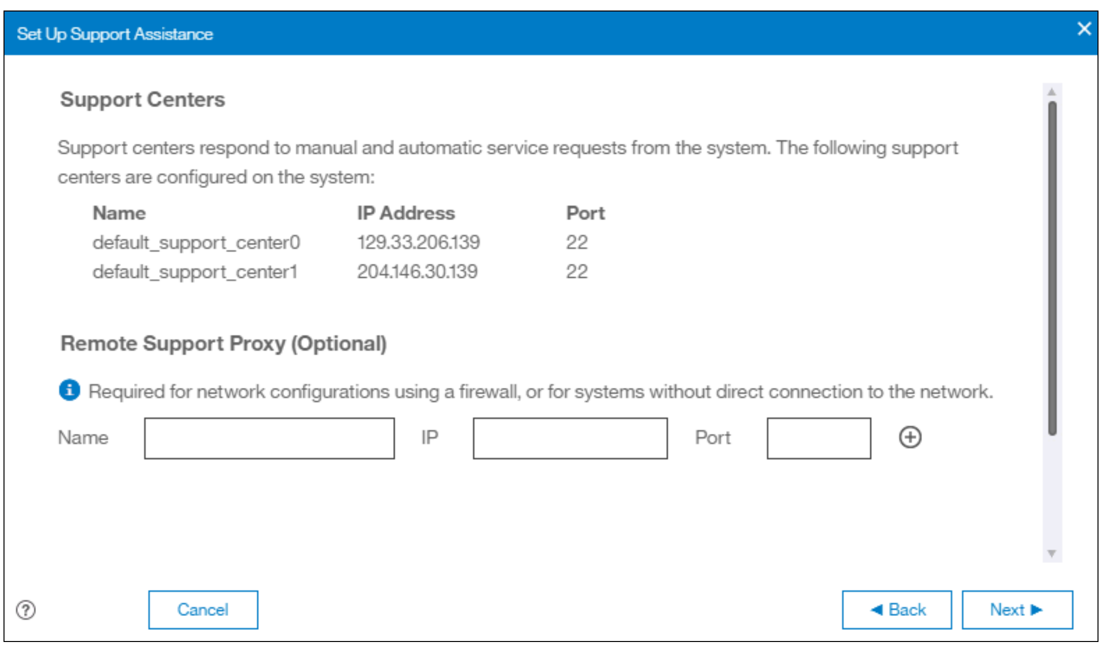


Figure 7-69   Remote Support wizard proxy setup

7. The next window asks if you want to open a tunnel to IBM permanently, allowing IBM to connect to your FS9100 **At Any Time**, or **On Permission Only**, as shown in Figure 7-70. **On Permission Only** requires a storage administrator to log on to the GUI and enable the tunnel when required. Click **Finish**.

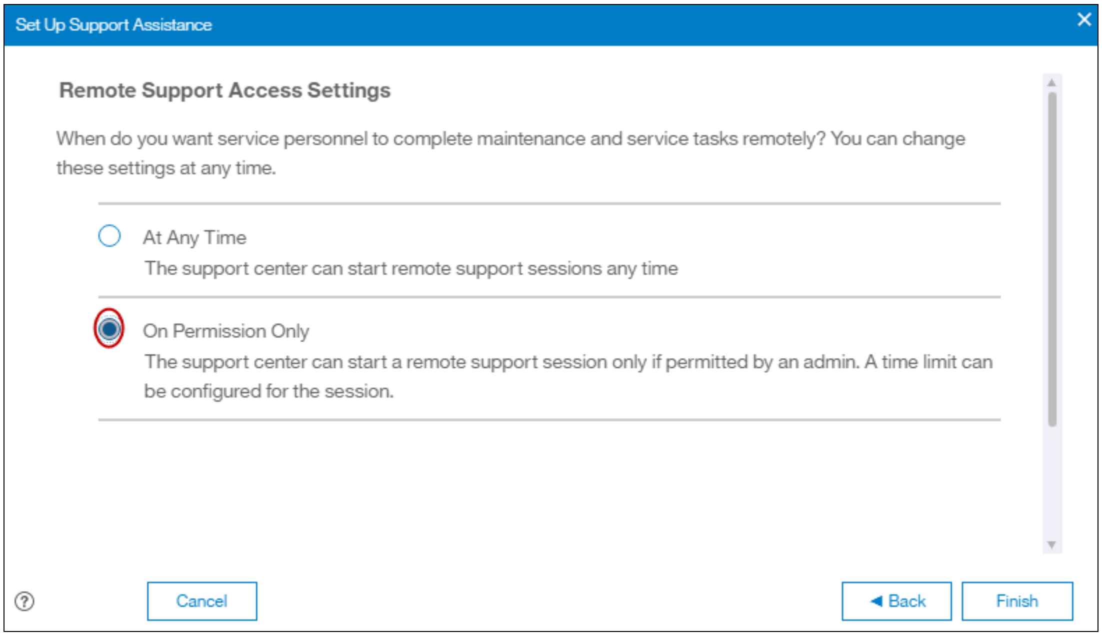


Figure 7-70 Remote Support wizard access choice

8. After completing the remote support setup, you can view the status of any remote connection, start a new session, and reconfigure the setup, as seen in Figure 7-71. Click **Start New Session** to open a tunnel connection to IBM.

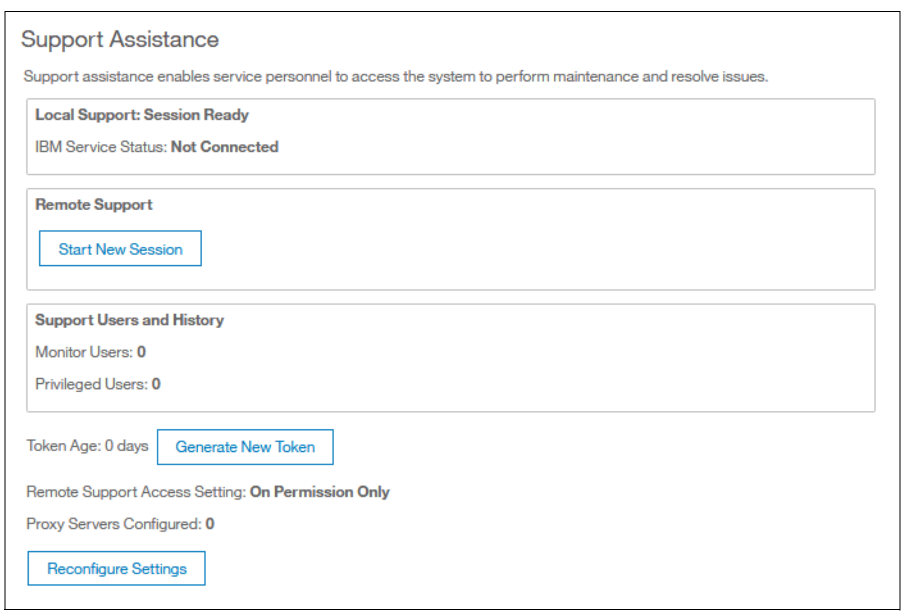


Figure 7-71 Remote Support Status and session management

9. A pop-up window asks how long you would like the tunnel to remain open if there is no activity by setting a timeout value. As shown in Figure 7-72, the connection is established and waits for IBM Support to connect.

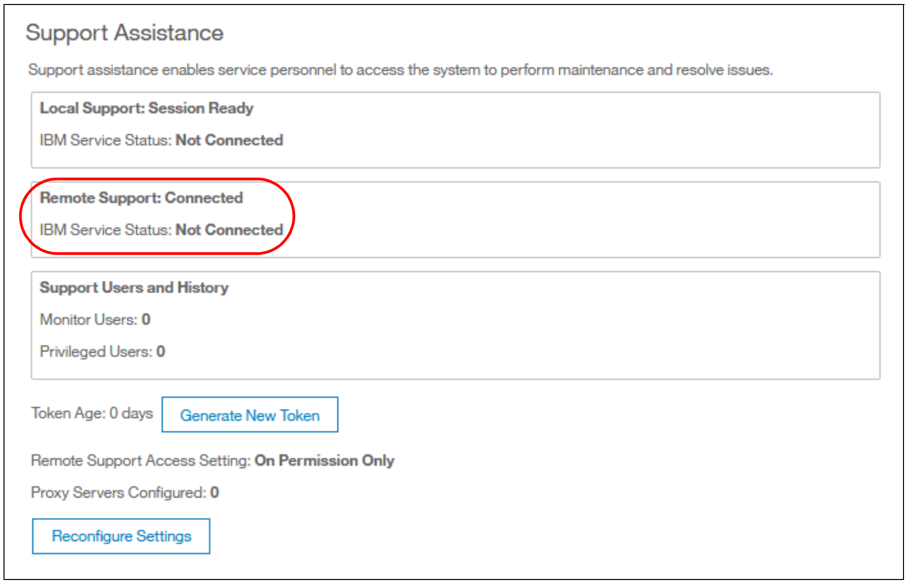


Figure 7-72 Remote Assistance tunnel connected

7.6.2 Support Package

If support assistance is configured on your systems, you can either automatically or manually upload new support packages to the support center to help analyze and resolve errors on the system.

Occasionally, if you have a problem and call the IBM Support Center, they might ask you to provide a support package. You can collect and upload this package from the **Settings** → **Support** menu.

Collecting and uploading information using the GUI

To collect information using the GUI, complete the following steps:

1. Click **Settings** → **Support** and the **Support Package** tab (Figure 7-73).
2. Click the **Upload Support Package** button.

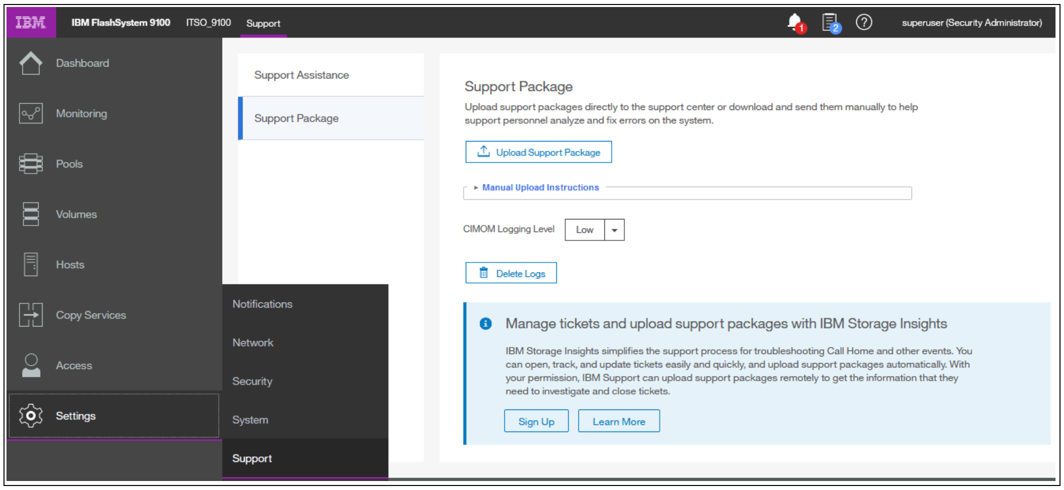


Figure 7-73 Support Package option

Note: To upload support packages, a DNS server must be configured on the system.

It is important to select the correct option, and in this case we are assuming that the problem encountered was an unexpected node restart that has logged a 2030 error. In this case we collect the default logs plus the most recent statesave from each node to capture the most relevant data for support.

Note: When a node unexpectedly reboots, it first dumps its current statesave information before it restarts to recover from an error condition. This statesave is critical for support to analyze what happened. Collecting a snap type 4 creates new statesaves at the time of the collection, which is not useful for understanding the restart event.

3. The Upload Support Package window provides four options for data collection. If you have been contacted by IBM Support due to your system calling home or you have manually opened a call with IBM Support, you will have been given a *PMR number*. Enter that PMR number into the **PMR** field and select the snap type, often referred to as an *option 1, 2, 3, 4 snap*, as requested by IBM Support (Figure 7-74). In our case, we enter our PMR number, select snap type 3 (option 3) because this will automatically collect the statesave created at the time the node restarted, and click **Upload**.

> **Tip:** You can use `https://www.ibm.com/support/servicerequest` to open a service request online.

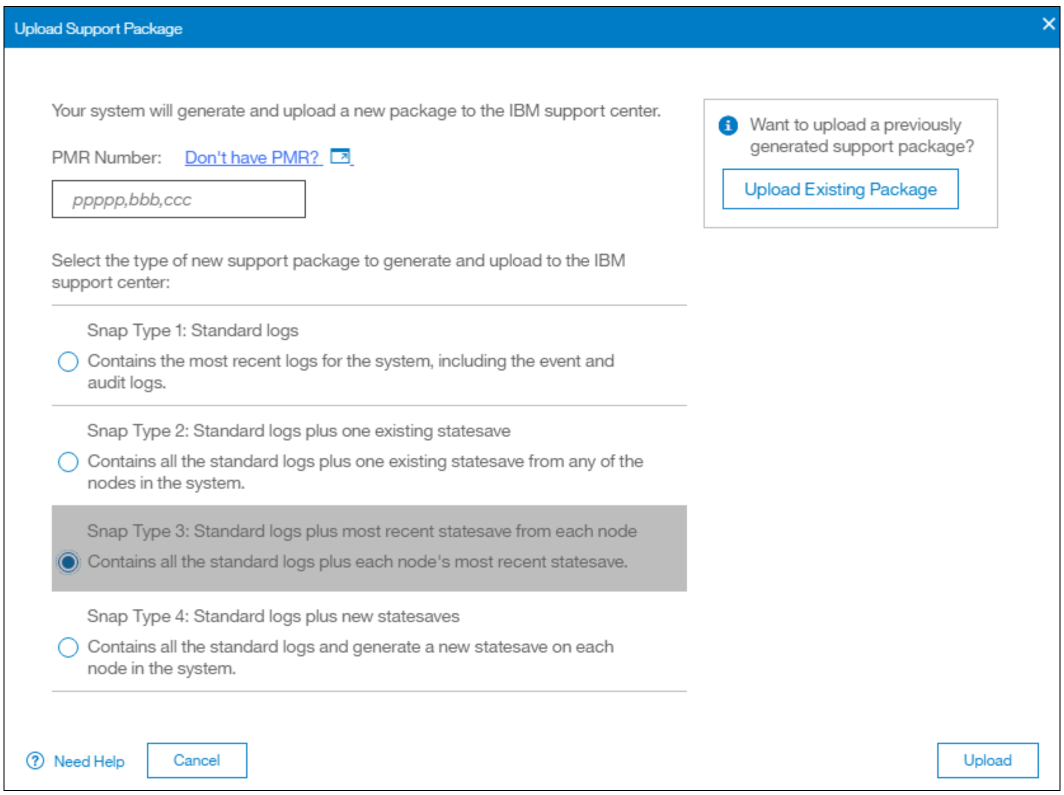


Figure 7-74 Upload Support Package window

4. The procedure to generate the snap on a FS9100 system, including the most recent statesave from each node canister, starts. This process might take a few minutes (Figure 7-75).

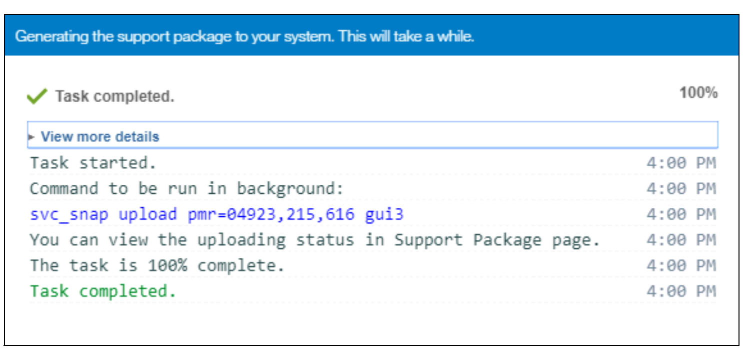


Figure 7-75 Task detail window

7.7 GUI preferences

As shown in Figure 7-76, the **GUI Preferences** menu consists of two options:

- **Login Message**
- **General**

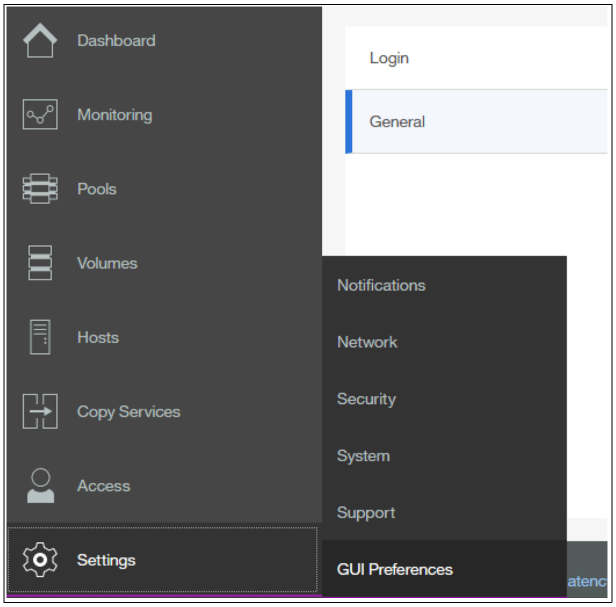


Figure 7-76 GUI Preferences

7.7.1 Login Message

The IBM FlashSystem 9100 enables administrators to configure the welcome banner (login message). This is a text message that appears either in the GUI login window or at the CLI login prompt.

The content of the welcome message is helpful when you need to notify users about some important information about the system, such as security warnings or a location description.

To define and enable the welcome message by using the GUI, edit the text area with the message content and click **Save** (Figure 7-77).

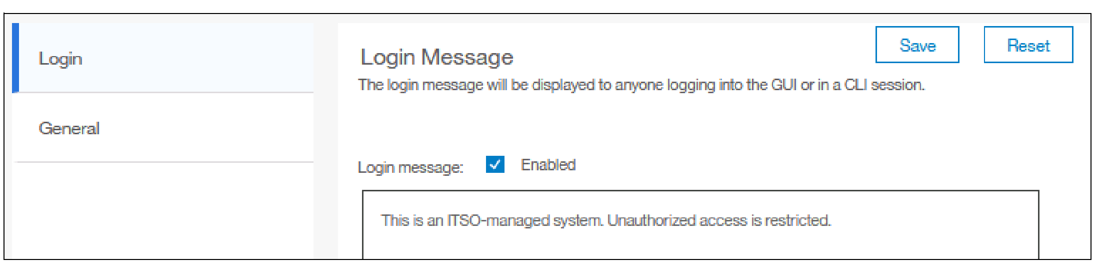


Figure 7-77 Enabling login message

The result of the action before is shown in Figure 7-78. The system shows the welcome message in the GUI before login.

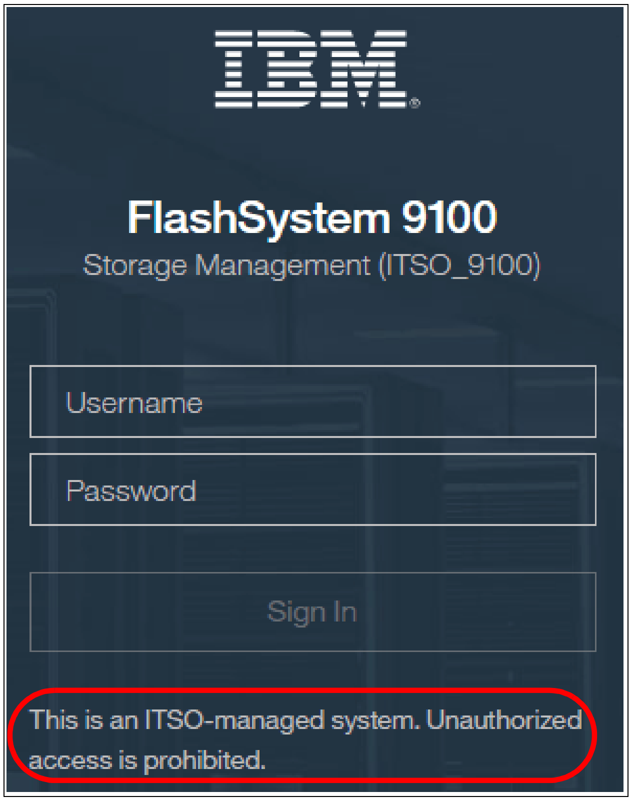


Figure 7-78 Welcome message in GUI

Figure 7-79 shows the welcome message as it appears in the CLI.

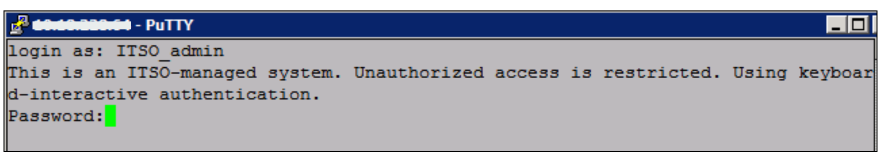


Figure 7-79 Welcome message in CLI

7.7.2 General settings

The **General Settings** menu allows the user to refresh the GUI cache, to set the low graphics mode option, and to enable advanced pools settings.

Complete the following steps to view and configure general GUI preferences:

1. From the FS9100 **Settings** tab, click **GUI Preferences,** and can click **General** (Figure 7-80).

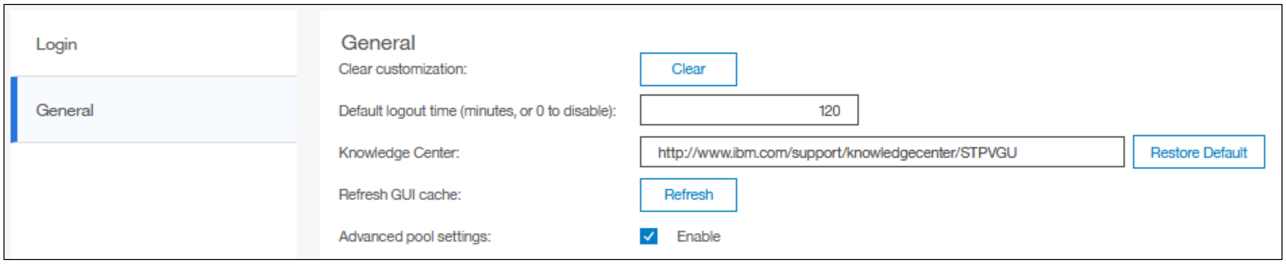


Figure 7-80 General GUI Preferences window

2. You can configure the following elements:

   – Refresh GUI cache

     This option causes the GUI to refresh all of its views and clears the GUI cache. The GUI looks up every object again.

   – Clear Customization

     This option deletes all GUI preferences that are stored in the browser and restores the default preferences.

   – IBM Knowledge Center

     You can change the URL of IBM Knowledge Center for the IBM FlashSystem 9100.

   – Advanced pool settings allow you to select the extent size during storage pool creation.

   – Default logout time in minutes after inactivity in the established session.

8

Hints and tips

This chapter provides helpful hints and tips to explore even further the capabilities offered by IBM FlashSystem 9100. Some of these capabilities might have been described previously in this book so in this chapter we are providing an extra level of information.

The following topics will be covered in this chapter:

- Configuring IBM FlashSystem 9100 for SAN Volume Controller
- General setup guidelines
- Performance data and statistics gathering
- Command-line hints
- Call Home process
- Service support

8.1 Configuring IBM FlashSystem 9100 for SAN Volume Controller

IBM FlashSystem 9100 offers the same external storage virtualization capability as the IBM SAN Volume Controller (SVC) or the Storwize family. Whether you have a heterogeneous, legacy environment or are looking for a Software Defined Storage solution to simplify your storage infrastructure and make your new, or existing, storage more effective, storage virtualization can help you.

To learn more about storage virtualization and all its benefits, visit:

https://www.ibm.com/us-en/marketplace/virtualization-software

On the other hand, the IBM FlashSystem 9100 may be configured as an external storage controller to an SVC cluster.

For IBM SAN Volume Controller clients that appreciate the flexibility offered by SVC with features like Standby Storage Engine (also known as Standby Node) and Enhanced Stretched Cluster and would like to introduce a flash tier into the SVC cluster, the IBM FlashSystem 9100 is a valuable option.

IBM SAN Volume Controller (SVC) Standby Storage Engine in a SAN provides an additional node that is not a part of any cluster, but is a candidate and able to join a cluster at a moment's notice. Enhanced Stretched Cluster splits an io_group in half and distributes the nodes across different locations for High Availability purposes. These features are not available with FlashSystem 9100 or any other Storwize offering.

> **Note:** HyperSwap is an alternative on the Storwize and FlashSystem 9100 if you are looking for High Availability storage options.

8.2 General setup guidelines

When planning the configuration of the IBM FlashSystem 9100 that will be virtualized by SVC, the following recommendations apply:

- Set up your RAID protection as Distributed RAID 6 (DRAID 6) for greater protection and performance.
- Configure a minimum of 16 volumes that will be provisioned to the SVC, but more is usually better and around 30 volumes will unlock the maximum performance.

Based on your goals, there are two options:

- Performance Optimized

  In this scenario, it's recommended to configure the Storage Pool at the SVC layer as a standard pool with no compression, and present over-allocated capacity in the FlashSystem 9100 to SVC. Hardware compression is made at the FlashSystem 9100 layer and Data Reduction Pool is recommended in the FlashSystem 9100.

  This option requires careful monitoring of capacity to not run out of space, for that reason it's recommended to create a sacrificial fully allocated volume as reserved space for additional capacity protection.

- Capacity Optimized

  In this scenario, it’s recommended to configure the Storage Pool at the SVC layer as a Data Reduction Pool (DRP) so you can leverage deduplication and compression. Even though you decide to have only deduplication on, it’s advised to configure those volumes as compressed too. Therefore, a deduplicated volume should always be compressed, providing higher data reduction ratio. In the FlashSystem 9100 it’s suggested to use Traditional Storage Pool with fully allocated volumes.

  This option offers simple capacity monitoring at SVC level with lower risk of running out of space. You may consider also creating a sacrificial fully allocated volume as reserved space for additional capacity protection.

> **Note:** Improvements are continually being made in the graphical user interface (GUI) for easy of capacity management.

8.3 Performance data and statistics gathering

This section provides a brief overview of the performance analysis capabilities of the IBM FlashSystem 9100 and a method for collecting and processing performance statistics. It is beyond the intended scope of this book to provide an in-depth understanding of performance statistics or to explain how to interpret them. For a more in-depth understanding of performance statistics and interpretation, see *IBM System Storage SAN Volume Controller and Storwize V7000 Best Practices and Performance Guidelines*, SG24-7521.

8.3.1 IBM FlashSystem 9100 performance overview

The caching capability of the IBM FlashSystem 9100 controller, its ability to effectively manage multiple flash enclosures along with IBM Spectrum Virtualize software, can deliver significant performance results. Storage virtualization with the IBM Spectrum Virtualize provides many administrative benefits. IBM Spectrum Virtualize and its ability to stripe volumes across multiple external disk arrays can provide a performance improvement over what can otherwise be achieved when midrange disk subsystems are used alone.

To ensure that the wanted performance levels of your system are maintained, monitor performance periodically to provide visibility to potential problems that exist or are developing so that they can be addressed in a timely manner.

Performance considerations

When you are designing the IBM Spectrum Virtualize infrastructure or maintaining an existing infrastructure, you must consider many factors in terms of their potential effect on performance. These factors include, but are not limited to dissimilar workloads competing for the same resources, overloaded resources, insufficient available resources, poor performing resources, and similar performance constraints.

Remember the following high-level rules when you are designing your storage area network (SAN) and IBM FlashSystem 9100 layout:

- Host-to-System inter-switch link (ISL) oversubscription

  This area is the most significant input/output (I/O) load across ISLs. The recommendation is to maintain a maximum of 7-to-1 oversubscription. A higher ratio is possible, but it could lead to I/O bottlenecks. This suggestion also assumes a core-edge design, where the hosts are on the edges and the FlashSystem 9100 is on the core.

- Storage-to-System ISL oversubscription

  This area is the second most significant I/O load across ISLs. The maximum oversubscription is 7-to-1. A higher ratio is not recommended. Again, this suggestion assumes a multiple-switch SAN fabric design.

- Node-to-node ISL oversubscription

  This area does not apply for FlashSystem 9100 clusters composed of a unique control enclosure. This area is the least significant load of the three possible oversubscription bottlenecks. In standard setups, this load can be ignored. Although this area is not entirely negligible, it does not contribute significantly to the ISL load. However, node-to-node ISL oversubscription is mentioned here in relation to the HyperSwap capability that was made available since V6.3.

  When the system is running in this manner, the number of ISL links becomes more important. As with the storage-to-System ISL oversubscription, this load also requires a maximum of 7-to-1 oversubscription. Exercise caution and careful planning when you determine the number of ISLs to implement. If you need assistance, contact your IBM representative and request technical assistance.

- ISL trunking or port channeling

  For the best performance and availability, it is suggested that you use ISL trunking or port channeling. Independent ISL links can easily become overloaded and turn into performance bottlenecks. Bonded or trunked ISLs automatically share load and provide better redundancy in the case of a failure.

- Number of paths per host multipath device

  The maximum supported number of paths per multipath device that is visible on the host is eight. Although the IBM Subsystem Device Driver Path Control Module (SDDPCM), related products, and most vendor multipathing software can support more paths, the FlashSystem 9100 expects a maximum of eight paths. In general, you see only an effect on performance from more paths than eight. Although the IBM Spectrum Virtualize can work with more than eight paths, this design is technically unsupported.

- Do not intermix dissimilar array types or sizes

  Although the IBM FlashSystem 9100 supports an intermix of differing storage within storage pools, the best approach is to always use the same array model, RAID mode, RAID size (RAID 5 6+P+S does not mix well with RAID 6 14+2), and drive speeds. Mixing standard storage with FlashSystem volumes is not advised unless the intent is to use Easy Tier.

Rules and guidelines are no substitution for monitoring performance. Monitoring performance can provide a validation that design expectations are met and identify opportunities for improvement.

IBM Spectrum Virtualize performance perspectives

The software is designed to run on commodity hardware (mass-produced Intel-based processors (CPUs) with mass-produced expansion cards) and to provide distributed cache and a scalable cluster architecture.

IBM FlashSystem 9100 is scalable up to four I/O groups (eight controllers). The performance is near linear when controllers are added into the cluster until performance eventually becomes limited by the attached components. This scalability is significantly enhanced using FlashCore technology which is built on three core principles: hardware accelerated I/O, IBM MicroLatency module, and advanced flash management. The design goals for IBM FlashSystem 9100 are to provide the customer with the fastest and most reliable all flash array on the market, while making it simple to service and support.

The key item for planning is your SAN layout. Switch vendors have slightly different planning requirements, but the end goal is that you always want to maximize the bandwidth that is available to the FlashSystem 9100 ports. The FlashSystem 9100 is one of the few devices that can drive ports to their limits on average, so it is imperative that you put significant thought into planning the SAN layout.

Essentially, IBM FlashSystem 9100 controller performance improvements are gained by optimizing delivery of flash technology resources and with advanced functionality that is provided by the IBM FlashSystem 9100 controller cluster. However, the performance of individual resources to hosts on the SAN eventually becomes the limiting factor.

8.3.2 Performance monitoring

This section highlights several performance monitoring techniques.

Collecting performance statistics

The IBM FlashSystem 9100 components are constantly collecting performance statistics. The default frequency by which files are created is at 5-minute intervals with a supported range of 15 - 60 minutes.

> **Tip:** The collection interval can be changed by using the **startstats** command.

Running the startstats command resets the statistics timer to zero, and give it a new interval at which to sample. Statistics are collected at the end of each sampling period as specified by the -interval parameter. These statistics are written to a file, with a new file created at the end of each sampling period. Separate files are created for MDisks, volumes, and node statistics.

To verify the statistics collection interval, display the system properties as shown in Example 8-1.

Example 8-1 Statistics collection status and frequency

```
IBM_FlashSystem:ITSO_9100:superuser>lssystem | grep statistics
statistics_status on
statistics_frequency 5
IBM_FlashSystem:ITSO_9100:superuser>
```

The statistics files (Volume, managed disk (MDisk), and Node) are saved at the end of the sampling interval. A maximum of 16 files (each) are stored before they are overlaid in a rotating log fashion. This design then provides statistics for the most recent 80-minute period if the default 5-minute sampling interval is used. IBM FlashSystem 9100 supports user-defined sampling intervals of 1 - 60 minutes in increments of 1 minute.

The maximum space that is required for a performance statistics file is around 1 MB (1,153,482 bytes). Up to 128 (16 per each of the three types across eight nodes) different files can exist across eight FlashSystem 9100 node canisters. This design makes the total space requirement a maximum of a bit more than 147 MB (147,645,694 bytes) for all performance statistics from all node canisters in a 4 I/O group FlashSystem 9100 cluster.

Make note of this maximum when you are in time-critical situations. The required size is not otherwise important because IBM FlashSystem 9100 controller enclosure hardware can map the space. You can define the sampling interval by using the **startstats -interval 2** command to collect statistics at 2-minute intervals.

Collection intervals: Although more frequent collection intervals provide a more detailed view of what happens within the IBM FlashSystem 9100, they shorten the amount of time that the historical data is available. For example, rather than an 80-minute period of data with the default 5-minute interval, if you adjust to 2-minute intervals, you have a 32-minute period instead.

Statistics are collected per node. The sampling of the internal performance counters is coordinated across the cluster so that when a sample is taken, all nodes sample their internal counters at the same time. It is important to collect all files from all nodes for a complete analysis. Tools, such as IBM Spectrum Control, perform this intensive data collection for you.

Statistics file naming

For each collection interval, the system creates four statistics files: one for managed disks (MDisks), named `Nm_stat`; one for volumes and volume copies, named `Nv_stat`; one for nodes, named `Nn_stat`; and one for SAS drives, named `Nd_stat`. The files are written to the `/dumps/iostats` directory on the node. To retrieve the statistics files from the non-configuration nodes onto the configuration node, the **`svctask cpdumps`** command must be used.

The statistics files that are generated are written to the `/dumps/iostats/` directory. The file name is in the following formats:

- `Nm_stats_`<*nodepanelname*>`_`<*date*>`_`<*time*> for MDisks statistics
- `Nv_stats_`<*nodepanelname*>`_`<*date*>`_`<*time*> for Volumes statistics
- `Nn_stats_`<*nodepanelname*>`_`<*date*>`_`<*time*> for node statistic
- `Nd_stats_`<*nodepanelname*>`_`<*date*>`_`<*time*> for drives statistic

The *nodepanelname* is the current configuration node panel name. The date is in the form <*yymmdd*> and the time is in the form <*hhmmss*>. The following examples show file names:

- An MDisk statistics file name: *Nm_stats_000229_031123_072426*
- A volume statistics file name: *Nv_stats_000229_031123_072426*
- A node statistics file name: *Nn_stats_000229_031123_072426*

Example 8-2 shows typical MDisk, volume, node, and disk drive statistics file names.

Example 8-2 File names of per node statistics

```
IBM_FlashSystem:ITSO_9100:superuser>lsdumps -prefix /dumps/iostats
id  filename
0   Nm_stats_F306954-1_180925_131918
1   Nd_stats_F306954-1_180925_131918
2   Nn_stats_F306954-1_180925_131918
3   Nv_stats_F306954-1_180925_131918
4   Nm_stats_F306954-2_180925_131918
5   Nv_stats_F306954-2_180925_131918
6   Nn_stats_F306954-2_180925_131918
7   Nd_stats_F306954-2_180925_131918
8   Nm_stats_F306954-1_180925_132418
9   Nv_stats_F306954-1_180925_132418
10  Nd_stats_F306954-1_180925_132418
...
```

T

Tip: The performance statistics files can be copied from the IBM FlashSystem V9000 Controllers to a local drive on your workstation by using the pscp.exe (included with PuTTY) from an MS-DOS command prompt, as shown in this example:

```
C:\>pscp -unsafe -load ITSO_FS9100 superuser@9.19.91.95:/dumps/iostats/*
c:\statsfiles
```

- Specify the **`-unsafe`** parameter when you use wildcards.
- Use the **`-load`** parameter to specify the session that is defined in PuTTY.

The qperf utility

qperf is an unofficial (no initial cost and unsupported) collection of *awk* scripts that was made available for download from IBM Techdocs. It provides a *quick performance* overview using the CLI and a UNIX Korn shell (it can also be used with Cygwin on Windows platforms).

You can download qperf from the following address:

http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/TD105947

The performance statistics files are in `.xml` format. They can be manipulated by using various tools and techniques. Figure 8-1 shows the type of chart that you can produce by using the IBM FlashSystem 9100 performance statistics.

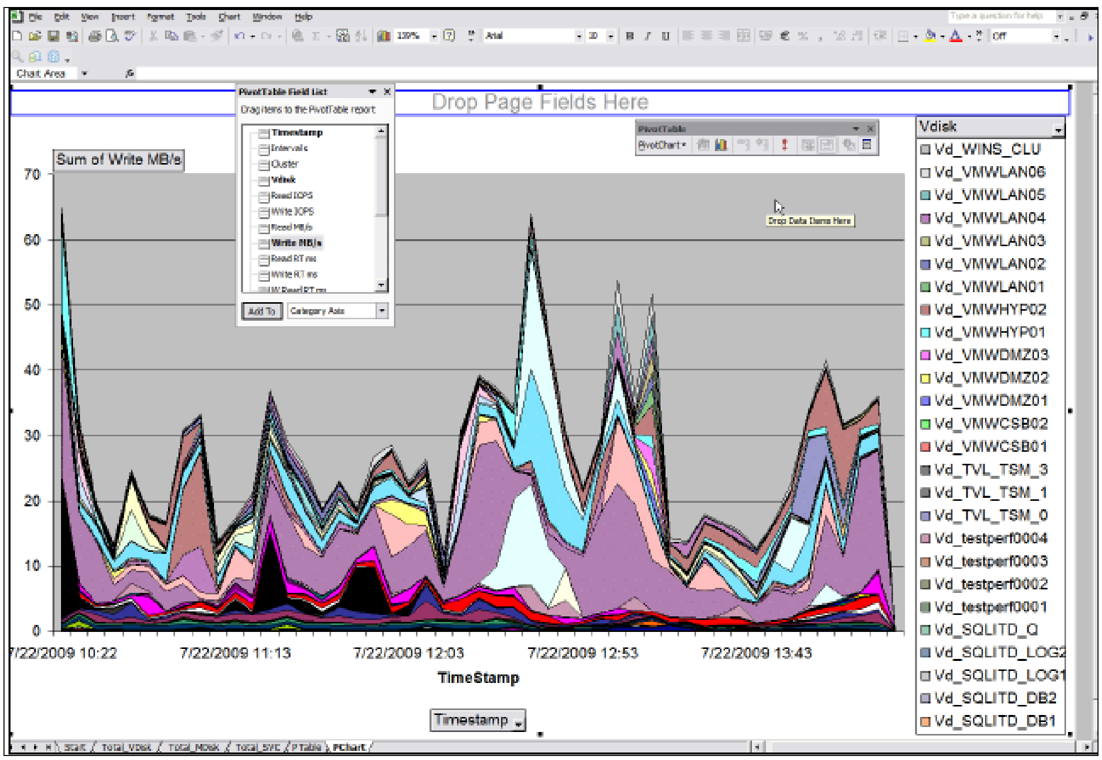


Figure 8-1 Spreadsheet example

Real-time performance monitoring

IBM FlashSystem 9100 controller supports real-time performance monitoring. Real-time performance statistics provide short-term status information for the system. The statistics are shown as graphs in the management GUI or can be viewed from the CLI. With system-level statistics, you can quickly view the CPU usage and the bandwidth of volumes, interfaces, and MDisks. Each graph displays the current bandwidth in megabytes per second (MBps) or I/O per second (IOPS), and a view of bandwidth over time.

Each control enclosure collects various performance statistics, mostly at 5-second intervals, and the statistics that are available from the config node in a clustered environment. This information can help you determine the performance effect of a specific node. As with system statistics, node statistics help you to evaluate whether the node is operating within normal performance metrics.

Real-time performance monitoring gathers the following system-level performance statistics:

- CPU utilization
- Port utilization and I/O rates
- Volume and MDisk I/O rates
- Bandwidth
- Latency

Note: Real-time statistics are not a configurable option and cannot be disabled.

Real-time performance monitoring with the CLI

The **lsenclosurestats/lsnodestats** and **lssystemstats** commands are available for monitoring the statistics through the CLI.

The **lsenclosurestats** command displays the most recent values of statistics (averaged) for all nodes or node canisters, as shown in Example 8-3. It can also display a history of those values for any subset of the available statistics. The output is truncated and shows only part of the available statistics. You can also specify a node name in the command to limit the output for a specific node.

Example 8-3 The lsnodecanisterstats command output

```
IBM_FlashSystem:ITSO_9100:superuser>lsnodecanisterstats
node_id node_name stat_name          stat_current stat_peak stat_peak_time
1       node1     compression_cpu_pc 0            0         180929124104
1       node1     cpu_pc             1            1         180929124104
1       node1     fc_mb              0            0         180929124104
1       node1     fc_io              5            6         180929123644
1       node1     sas_mb             0            0         180929124104
1       node1     sas_io             0            0         180929124104
1       node1     iscsi_mb           0            0         180929124104
1       node1     iscsi_io           0            0         180929124104
1       node1     write_cache_pc     0            0         180929124104
1       node1     total_cache_pc     0            0         180929124104
...
2       node2     compression_cpu_pc 0            0         180929124328
2       node2     cpu_pc             1            1         180929124328
2       node2     fc_mb              0            0         180929124328
2       node2     fc_io              5            5         180929124328
2       node2     sas_mb             0            0         180929124328
2       node2     sas_io             0            0         180929124328
2       node2     iscsi_mb           0            0         180929124328
2       node2     iscsi_io           0            0         180929124328
2       node2     write_cache_pc     0            0         180929124328
2       node2     total_cache_pc     0            0         180929124328
....
```

Example 8-3 on page 302 shows statistics for the two node members of cluster ITSO_9100. For each node, the following columns are displayed:

- `stat_name`. The name of the statistic field.
- `stat_current`. The current value of the statistic field.
- `stat_peak`. The peak value of the statistic field in the last 5 minutes.
- `stat_peak_time`. The time that the peak occurred.

However, the **`lssystemstats`** command lists the same set of statistics that is listed with the **`lsnodestats`** command, but representing all nodes in the cluster. The values for these statistics are calculated from the node statistics values in the following way:

- Bandwidth. Sum of bandwidth of all nodes.
- Latency. Average latency for the cluster, which is calculated by using data from the whole cluster, not an average of the single node values.
- IOPS. Total IOPS of all nodes.
- CPU percentage. Average CPU percentage of all nodes.

Example 8-4 shows the resulting output of the **`lssystemstats`** command.

Example 8-4 The lssystemstats command output

```
IBM_FlashSystem:ITSO_9100:superuser>lssystemstats
stat_name          stat_current stat_peak stat_peak_time
compression_cpu_pc 0            0         180929125231
cpu_pc             1            1         180929125231
fc_mb              0            0         180929125231
fc_io              10           11        180929125146
sas_mb             0            0         180929125231
sas_io             0            0         180929125231
iscsi_mb           0            0         180929125231
iscsi_io           0            0         180929125231
write_cache_pc     0            0         180929125231
total_cache_pc     0            0         180929125231
vdisk_mb           0            0         180929125231
vdisk_io           0            0         180929125231
vdisk_ms           0            0         180929125231
mdisk_mb           0            0         180929125231
mdisk_io           0            0         180929125231
mdisk_ms           0            0         180929125231
drive_mb           0            0         180929125231
drive_io           0            5         180929125211
drive_ms           0            0         180929125231
vdisk_r_mb         0            0         180929125231
vdisk_r_io         0            0         180929125231
vdisk_r_ms         0            0         180929125231
vdisk_w_mb         0            0         180929125231
vdisk_w_io         0            0         180929125231
vdisk_w_ms         0            0         180929125231
mdisk_r_mb         0            0         180929125231
mdisk_r_io         0            0         180929125231
mdisk_r_ms         0            0         180929125231
mdisk_w_mb         0            0         180929125231
mdisk_w_io         0            0         180929125231
mdisk_w_ms         0            0         180929125231
drive_r_mb         0            0         180929125231
```

```
drive_r_io          0            0          180929125231
drive_r_ms          0            0          180929125231
drive_w_mb          0            0          180929125231
drive_w_io          0            5          180929125211
drive_w_ms          0            0          180929125231
power_w             766          766        180929125231
temp_c              22           22         180929125231
temp_f              71           71         180929125231
iplink_mb           0            0          180929125231
iplink_io           0            0          180929125231
iplink_comp_mb      0            0          180929125231
cloud_up_mb         0            0          180929125231
cloud_up_ms         0            0          180929125231
cloud_down_mb       0            0          180929125231
cloud_down_ms       0            0          180929125231
iser_mb             0            0          180929125231
iser_io             0            0          180929125231
```

Table 8-1 gives the description of the different counters that are presented by the **lssystemstats** and **lsnodestats** commands.

Table 8-1 List of counters in lssystemstats and lsnodestats

Value	Description
compression_cpu_pc	Displays the percentage of allocated CPU capacity that is used for compression.
cpu_pc	Displays the percentage of allocated CPU capacity that is used for the system.
fc_mb	Displays the total number of megabytes transferred per second for Fibre Channel traffic on the system. This value includes host I/O and any bandwidth that is used for communication within the system.
fc_io	Displays the total I/O operations that are transferred per second for Fibre Channel traffic on the system. This value includes host I/O and any bandwidth that is used for communication within the system.
sas_mb	Displays the total number of megabytes transferred per second for serial-attached SCSI (SAS) traffic on the system. This value includes host I/O and bandwidth that is used for background RAID activity.
sas_io	Displays the total I/O operations that are transferred per second for SAS traffic on the system. This value includes host I/O and bandwidth that is used for background RAID activity.
iscsi_mb	Displays the total number of megabytes transferred per second for iSCSI traffic on the system.
iscsi_io	Displays the total I/O operations that are transferred per second for iSCSI traffic on the system.
write_cache_pc	Displays the percentage of the write cache usage for the node.
total_cache_pc	Displays the total percentage for both the write and read cache usage for the node.
vdisk_mb	Displays the average number of megabytes transferred per second for read and write operations to volumes during the sample period.

Value	Description
vdisk_io	Displays the average number of I/O operations that are transferred per second for read and write operations to volumes during the sample period.
vdisk_ms	Displays the average amount of time in milliseconds that the system takes to respond to read and write requests to volumes over the sample period.
mdisk_mb	Displays the average number of megabytes transferred per second for read and write operations to MDisks during the sample period.
mdisk_io	Displays the average number of I/O operations that are transferred per second for read and write operations to MDisks during the sample period.
mdisk_ms	Displays the average amount of time in milliseconds that the system takes to respond to read and write requests to MDisks over the sample period.
drive_mb	Displays the average number of megabytes transferred per second for read and write operations to drives during the sample period.
drive_io	Displays the average number of I/O operations that are transferred per second for read and write operations to drives during the sample period.
drive_ms	Displays the average amount of time in milliseconds that the system takes to respond to read and write requests to drives over the sample period.
vdisk_w_mb	Displays the average number of megabytes transferred per second for read and write operations to volumes during the sample period.
vdisk_w_io	Displays the average number of I/O operations that are transferred per second for write operations to volumes during the sample period.
vdisk_w_ms	Displays the average amount of time in milliseconds that the system takes to respond to write requests to volumes over the sample period.
mdisk_w_mb	Displays the average number of megabytes transferred per second for write operations to MDisks during the sample period.
mdisk_w_io	Displays the average number of I/O operations that are transferred per second for write operations to MDisks during the sample period.
mdisk_w_ms	Displays the average amount of time in milliseconds that the system takes to respond to write requests to MDisks over the sample period.
drive_w_mb	Displays the average number of megabytes transferred per second for write operations to drives during the sample period.
drive_w_io	Displays the average number of I/O operations that are transferred per second for write operations to drives during the sample period.
drive_w_ms	Displays the average amount of time in milliseconds that the system takes to respond write requests to drives over the sample period.
vdisk_r_mb	Displays the average number of megabytes transferred per second for read operations to volumes during the sample period.
vdisk_r_io	Displays the average number of I/O operations that are transferred per second for read operations to volumes during the sample period.
vdisk_r_ms	Displays the average amount of time in milliseconds that the system takes to respond to read requests to volumes over the sample period.

Value	Description
mdisk_r_mb	Displays the average number of megabytes transferred per second for read operations to MDisks during the sample period.
mdisk_r_io	Displays the average number of I/O operations that are transferred per second for read operations to MDisks during the sample period.
mdisk_r_ms	Displays the average amount of time in milliseconds that the system takes to respond to read requests to MDisks over the sample period.
drive_r_mb	Displays the average number of megabytes transferred per second for read operations to drives during the sample period.
drive_r_io	Displays the average number of I/O operations that are transferred per second for read operations to drives during the sample period.
drive_r_ms	Displays the average amount of time in milliseconds that the system takes to respond to read requests to drives over the sample period.
iplink_mb	The total number of megabytes transferred per second for Internet Protocol (IP) replication traffic on the system. This value does not include iSCSI host I/O operations.
iplink_comp_mb	Displays the average number of compressed MBps over the IP replication link during the sample period.
iplink_io	The total I/O operations that are transferred per second for IP partnership traffic on the system. This value does not include Internet Small Computer System Interface (iSCSI) host I/O operations.
cloud_up_mb	Displays the average number of MBps for upload operations to a cloud account during the sample period.
cloud_up_ms	Displays the average amount of time (in milliseconds) it takes for the system to respond to upload requests to a cloud account during the sample period.
cloud_down_mb	Displays the average number of MBps for download operations to a cloud account during the sample period.
cloud_down_ms	Displays the average amount of time (in milliseconds) that it takes for the system to respond to download requests to a cloud account during the sample period.

Real-time performance statistics monitoring with the GUI

The IBM FlashSystem 9100 GUI dashboard gives you performance at a glance by displaying some information about the system. You can see the entire cluster (the system) performance by selecting the information between Latency, Bandwidth, IOps, or CPU utilization. You can also display a Node Comparison by selecting the same information as for the cluster, and then switching the button, as shown in Figure 8-2 on page 307 and Figure 8-3 on page 307**.**

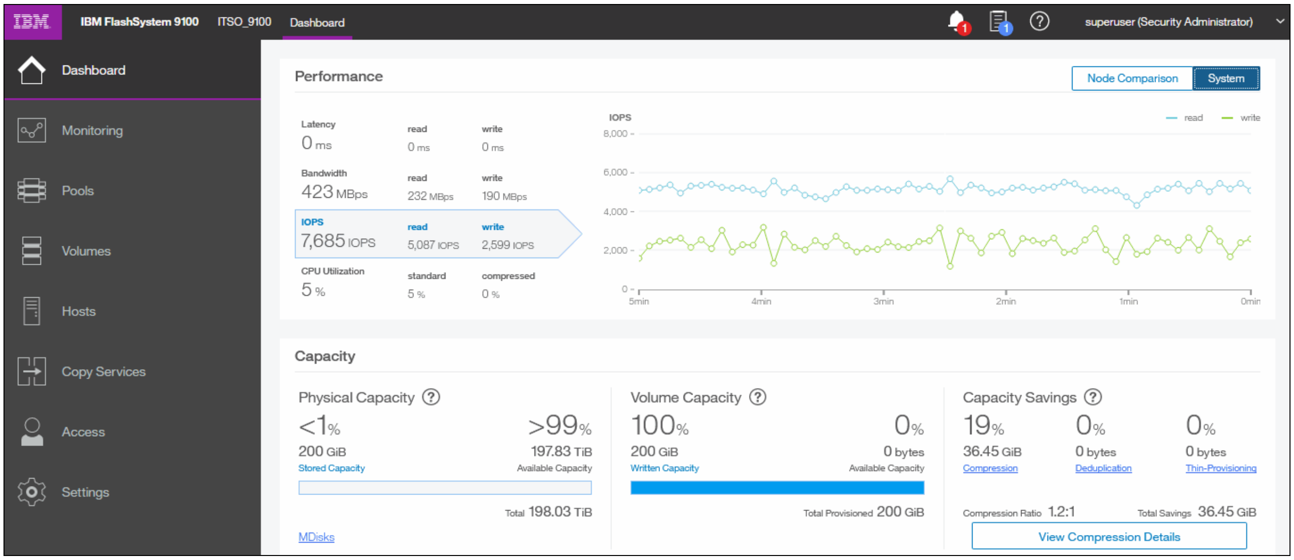


Figure 8-2 IBM FlashSystem 9100 Dashboard displaying System performance overview.

Figure 8-3 shows the display after switching the button.

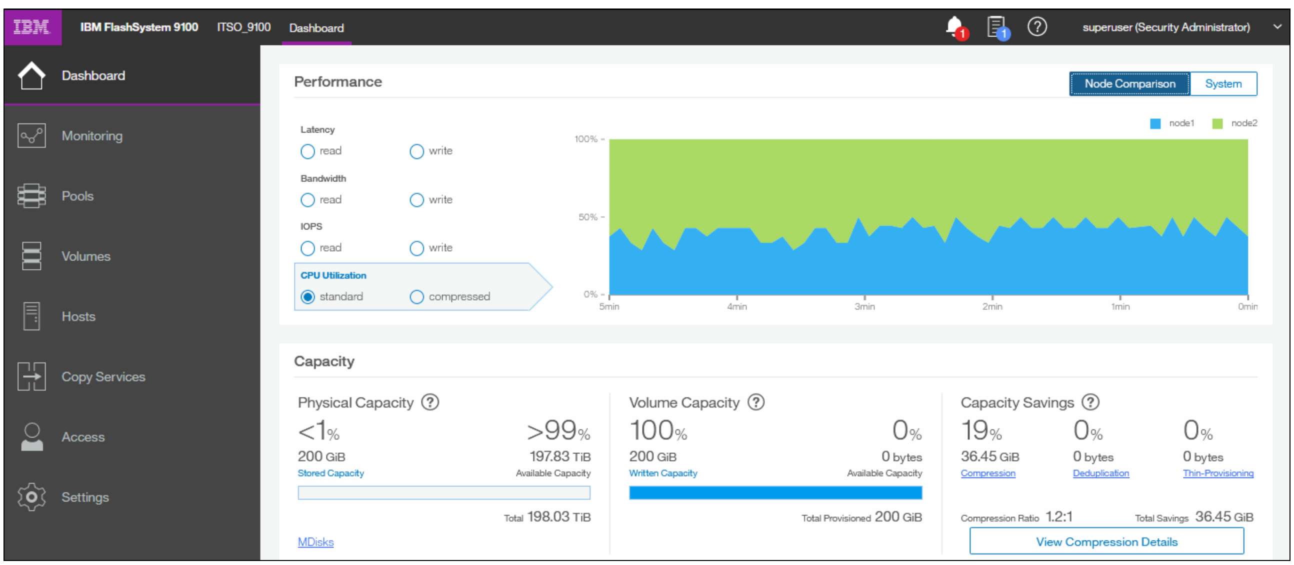


Figure 8-3 IBM FlashSystem 9100 Dashboard displaying Nodes performance overview

You can also use real-time statistics to monitor CPU utilization, volume, interface, and MDisk bandwidth of your system and nodes. Each graph represents five minutes of collected statistics and provides a means of assessing the overall performance of your system.

The real-time statistics are available from the IBM FlashSystem 9100 GUI. Click **Monitoring (1)** → **Performance (2)** (as shown in Figure 8-4) to open the Performance Monitoring window.

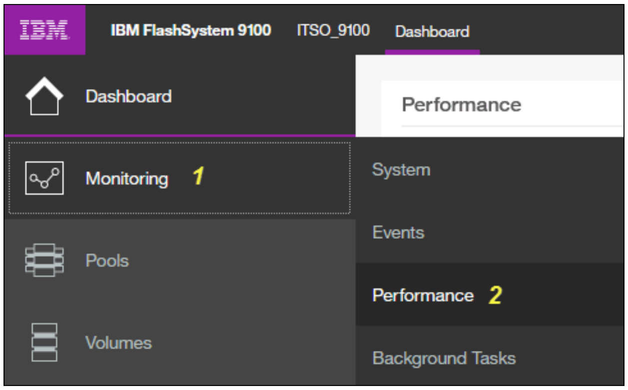


Figure 8-4   Selecting performance pane in the monitoring menu

As shown in Figure 8-5 on page 309, the Performance monitoring window is divided into the following sections that provide utilization views for the following resources:

- CPU Utilization. Shows the overall CPU usage percentage.
- Volumes. Shows the overall volume utilization with the following fields:
  - Read
  - Write
  - Read latency
  - Write latency
- Interfaces. Shows the overall statistics for each of the available interfaces:
  - Fibre Channel
  - iSCSI
  - SAS
  - IP Remote Copy
- MDisks. Shows the following overall statistics for the MDisks:
  - Read
  - Write
  - Read latency
  - Write latency

You can use these metrics to help determine the overall performance health of the volumes and MDisks on your system. Consistent unexpected results can indicate errors in configuration, system faults, or connectivity issues.

The system's performance is also always visible in the bottom of the IBM FlashSystem 9100 window, as shown in Figure 8-5.

Note: The indicated values in the graphics are averaged on a 1 second based sample.

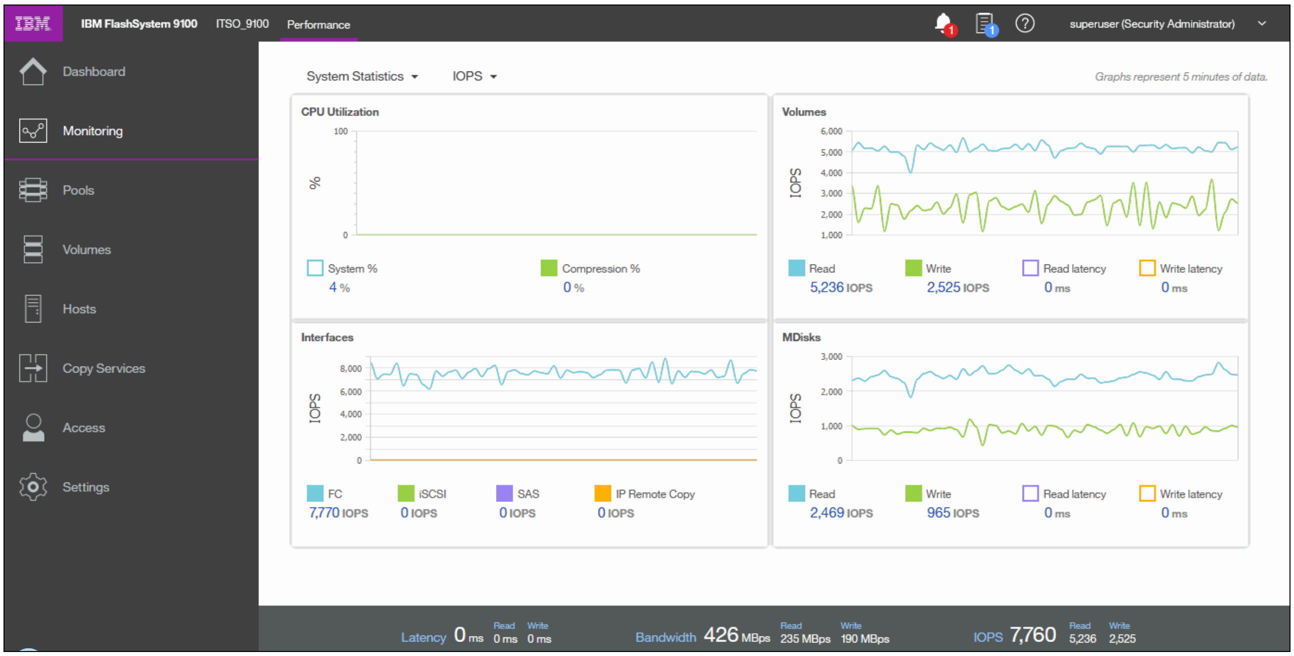


Figure 8-5 IBM FlashSystem 9100 performance window

You can also select to view performance statistics for each of the available nodes of the system (Figure 8-6).

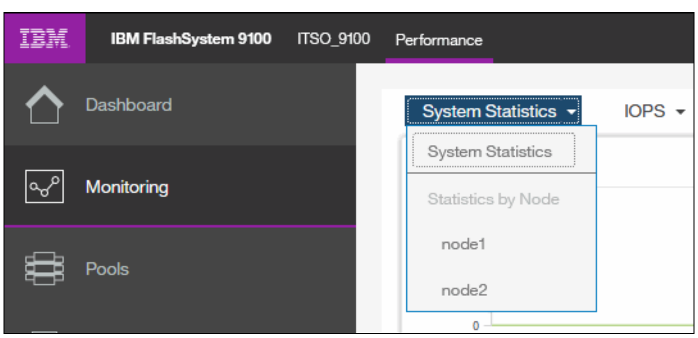


Figure 8-6 View statistics per node or for the entire system

You can also change the metric between IOPS or MBps, as shown in Figure 8-7.

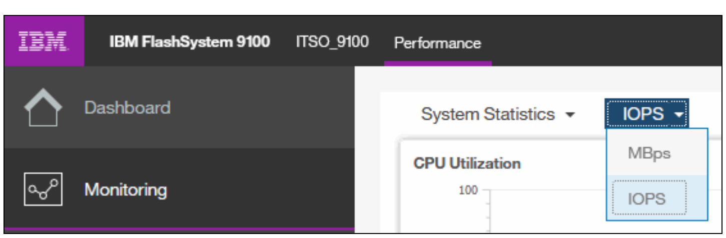


Figure 8-7 View performance metrics by MBps or IOps

On any of these views, you can select any point with your cursor to know the exact value and when it occurred. When you place your cursor over the time line, it becomes a dotted line with the various values gathered, as shown in Figure 8-8.

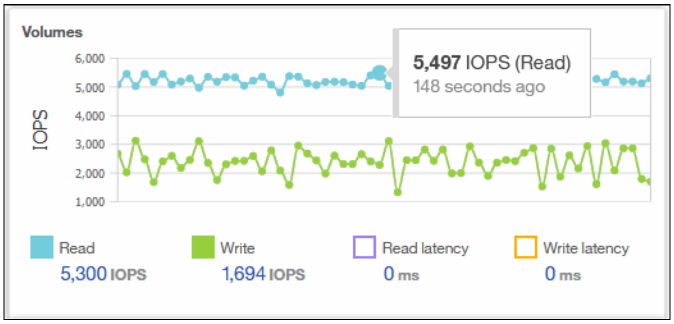


Figure 8-8 Viewing performance with details

For each of the resources, you can view various values by selecting the value. For example, as shown in Figure 8-9, the four available fields are selected for the MDisks view: Read, Write, Read latency, and Write latency. In this example, latencies are not selected.

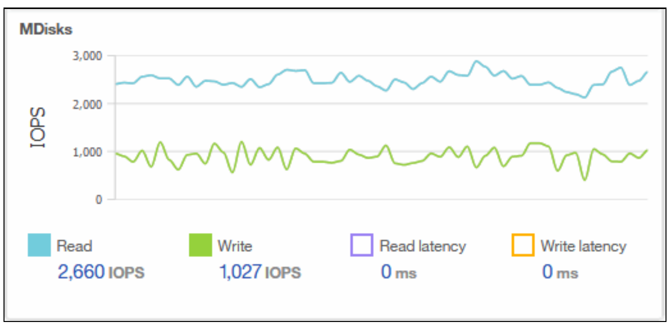


Figure 8-9 Displaying performance counters

Performance data collection with external tools

Although you can obtain performance statistics in standard `.xml` files, the use of `.xml` files is a less practical and more complicated method to analyze the IBM FlashSystem 9100 performance statistics. IBM Spectrum Control is the supported IBM tool to collect and analyze performance statistics.

For more information about the use of IBM Spectrum Control to monitor your storage subsystem, see the following website:

https://www.ibm.com/systems/storage/spectrum/control/

A Software as a Service (SaaS) version of IBM Spectrum Control, called IBM Spectrum Control Storage Insights, allows you to use the solution as a service (no installation) in minutes and offers a trial for 30 days at no charge. For further details about Storage Insights, see 4.5, “IBM Storage Insights” on page 96.

8.4 Command-line hints

IBM FlashSystem 9100 contains a robust command-line interface based on Spectrum Virtualize software. These command-line scripting techniques can be used to automate the following tasks:

- Running command on the cluster
- Creating connections
- Command-line scripting
- Backing up the configuration
- Running the Software Upgrade Test Utility

8.4.1 Running commands on the IBM FlashSystem 9100

The command line interface (CLI) is a powerful tool to automate copy services processes. All automation techniques are achieved through the IBM FlashSystem 9100 command line or the Common Information Model Object Manager (CIMOM), which currently acts as a proxy to the command line.

This section uses the term *user agent*. The user agent can be the CIMOM, which connects to the cluster by using Secure Shell (SSH). Or the user agent can be a user connecting directly with an SSH client, either in an interactive mode or by using a script.

Running commands to the cluster follows this sequence of steps:

1. Connection
2. Authentication
3. Submission
4. Authorization
5. Running a command (Execution)

Connection

Commands are submitted to the cluster during a connection session to the cluster. User agents make connections through the SSH protocol. FlashSystem has several security features that affect how often you can attempt connections. These security features are in place to prevent attacks (malicious or accidental) that can bring down an IBM FlashSystem 9100 controller node. These features might initially seem restrictive, but they are relatively simple to work with to maintain a valid connection.

When creating automation by using the CLI, an important consideration is to be sure that scripts behave responsibly and do not attempt to breach the connection rules. At a minimum, an automation system must ensure that it can gracefully handle rejected connection attempts.

There are two connection queues in action: *Pending Connections* and *Active Connections*. The connection process follows this sequence:

1. A connection request comes into the IBM FlashSystem 9100. If the Pending Connections queue has a free position, the request is added to it otherwise, the connection is explicitly rejected.
2. Pending Connections are handled in one of two ways:
   a. If any of the following conditions are true, the connection request is rejected:
      - No key is provided, or the provided key is incorrect.
      - The provided user name is not admin or service.
      - The Active Connections queue is full. In this case, a warning is returned to the SSH client.

   b. If none of the conditions listed in the previous step are true, the connection request is accepted and moved from the Pending Connections queue to the Active Connections queue.

3. Active Connections end after any of the following events:
   – The user logs off manually.
   – The SAN Volume Controller SSH daemon recognizes that the connection has grown idle.
   – The network connectivity fails.
   – The configuration node fails over.

In this case, both queues are cleared because the SHH daemon stops and restarts on a different node.

Authentication

IBM FlashSystem 9100 enables you to log in with basically a user name and password. The two types of users who can access the system are local users and remote users. These types are based on how the users are authenticated to the system:

- *Local users* must provide a password, a SSH key, or both. Local users are authenticated through the authentication methods that are configured on the system. If the local user needs access to the management GUI, a password is needed for the user. If the user requires access to the CLI through SSH, either a password or a valid SSH key file is necessary.

  Local users must be part of a user group that is defined on the system. User groups define roles that authorize the users within that group to a specific set of operations on the system.

- *Remote users* are authenticated on a remote service with Lightweight Directory Access Protocol (LDAPv3). A remote user does not need local authentication methods. With LDAP, having a password and SSH key is not necessary, although SSH keys optionally can be configured. Remote users who need to access the system when the remote service is down also need to configure local credentials. Remote users have their groups defined by the remote authentication service.

See section 7.4.1, “Remote authentication” on page 251 for more information.

Submission

When connected to a cluster, the user agent can start submitting commands. First, the syntax is checked. If the syntax checking fails, an appropriate error message is returned. Any automation implementation must ensure that all submitted commands have the correct syntax. If they do not, they must be designed to handle syntax errors. Designing a solution that does not generate invalid syntax is easier than designing a solution to handle all potential syntax errors.

Authorization

Next, commands with valid syntax are checked to determine whether the user agent has the authority to submit the command. A role is associated with the key that was used to authenticate the connection. IBM FlashSystem 9100 checks the submitted command against the authorization role. If the user agent is *authorized*, the command is sent to be run.

If the user agent is *not authorized* to run this command, the following error is returned:

```
CMMVC9027E   The task has failed because the user's role is not authorized to
submit the command.
```

Running a command

When a command is run, it can fail (1 possible scenario) or succeed (4 possible scenarios):

- The command fails. An error message is written to STDERR.
- The command succeeds. A warning is written to STDERR.
- The command succeeds. A warning is written to STDERR; information is sent to STDOUT.
- The command succeeds. Information is written to STDOUT.
- The command succeeds. Nothing is written to STDOUT.

Note: Data that is written to STDOUT and STDERR by the IBM FlashSystem 9100 is written to STDOUT and STDERR by your SSH client. However, you must manually verify that the data was written to STDOUT and STDERR by your SSH client.

8.4.2 Creating connections

Connecting to the IBM FlashSystem 9100 cluster is the first step in running commands. Any automation solution requires a connection component. This component must be as robust as possible, because it forms the foundation of your solution.

There are two forms of connection solutions:

- Transient: One command is submitted per connection, and the connection is closed after the command is completed.
- Persistent: The connection is made and stays open. Multiple commands are submitted through this single connection, including interactive sessions and the CIMOM.

Transient connections

Transient connections are simple to create. The most common SSH clients enable the user to submit a command as part of the user's invocation. Example 8-5 shows a user submitting two commands as part of the user's invocation using **ssh** on an Linux server. Using the operating system command, the IBM FlashSystem 9100 output can be processed.

Example 8-5 Transient connection to IBM FlashSystem 9100 from a Linux server

```
# ssh -i publickey -l ITSOadmin ITSO_FS9110 lsenclosure -delim :
id:status:type:managed:IO_group_id:IO_group_name:product_MTM:serial_number:total_c
anisters:online_canisters:total_PSUs:online_PSUs:drive_slots:total_fan_modules:onl
ine_fan_modules:total_sems:online_sems
1:online:control:yes:0:io_grp0:9846-AF8:F313150:2:2:2:2:24:0:0:0:0

# ssh -i publickey -l ITSOadmin ITSO_FS9100 lsenclosure -delim : | cut -f1,2,7,8
-d :
id:status:product_MTM:serial_number
1:online:9846-AF8:F313150
```

Example 8-6 shows a user submitting a command as part of the user's invocation using the **plink** command on a Windows server.

Example 8-6 Transient connection to IBM FlashSystem 9100 from Windows server

```
C:\Program Files\Putty>plink -i private.ppk -l superuser ITSO_FS9100 lsenclosure -delim :
id:status:type:managed:IO_group_id:IO_group_name:product_MTM:serial_number:total_c
anisters:online_canisters:total_PSUs:online_PSUs:drive_slots:total_fan_modules:onl
ine_fan_modules:total_sems:online_sems
```

```
1:online:control:yes:0:io_grp0:9846-AF8:F313150:2:2:2:2:24:0:0:0:0

C:\Program Files\Putty>
```

These transient connections go through all five stages of running a command and return to the command line. You can redirect the two output streams (STDOUT and STDERR) using the operating system's standard redirection operators to capture the responses.

These lengthy invocations can be shortened in client-specific ways. User configuration files can be used with the AIX SSH client. The configuration file in Example 8-7 enables you to create a transient connection.

Example 8-7 Sample SSH configuration file saved as sampleCfg

```
# cat sampleCfg
Host ITSO
HostName ITSO_FS9100
IdentityFile ./privateKey
User ITSOadmin

Host ITSOsu
HostName ITSO_FS9100
IdentityFile .ssh/id_rsa
User superuser
```

The transient connection is shown in Example 8-8.

Example 8-8 Transient connection to IBM FlashSystem 9100 using SSH and configuration file

```
# ssh -F sampleCFG ITSOsu sainfo lsservicenodes
panel_name cluster_id       cluster_name node_id node_name relation  node_status error_data
01-2       0000020428200012 ITSO_FS9100  2       node2     local     Active
01-1       0000020428200012 ITSO_FS9100  1       node1     partner   Active
F306954-1                                                  candidate Service     690
F306954-2                                                  candidate Service     690
```

Shortening the **plink** invocation requires the creation of a PuTTY session:

1. First, open the PuTTY application and enter the following line in the Host Name (or IP address) field:

   `superuser@<Host Name or cluster IP address>`

2. Provide a name in the Saved Sessions then click Save. See sample shown in Figure 8-10 on page 315.

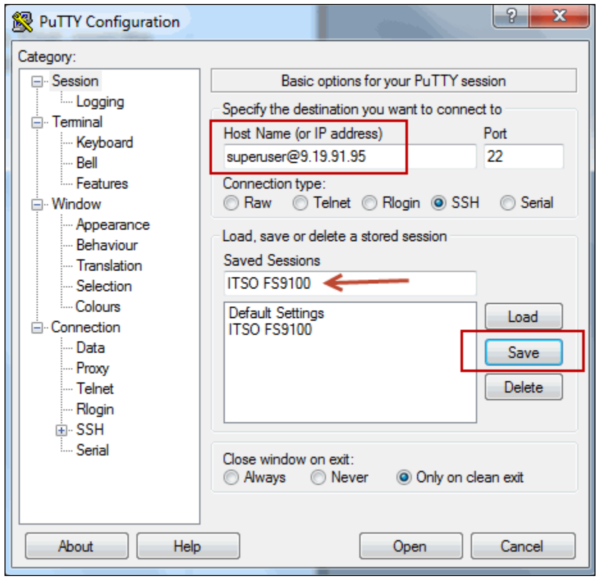


Figure 8-10 Add user name and system name to PuTTY session

3. Configure the private key for this session by making the selections, as shown in steps 1, 2, and 3 of Figure 8-11. Click **Browse** (step 4) to locate the private key file.

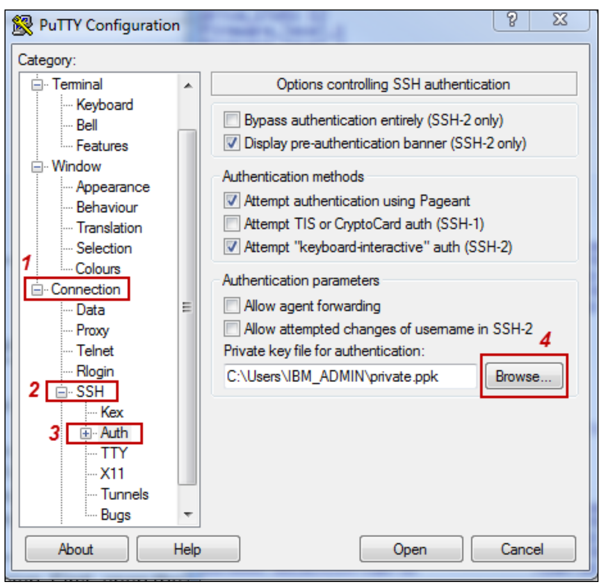


Figure 8-11 Set private key for PuTTY SSH session

4. Complete saving the session (Figure 8-12) by returning to the Session Panel (1), confirming the session name (2), and clicking **Save** (3).

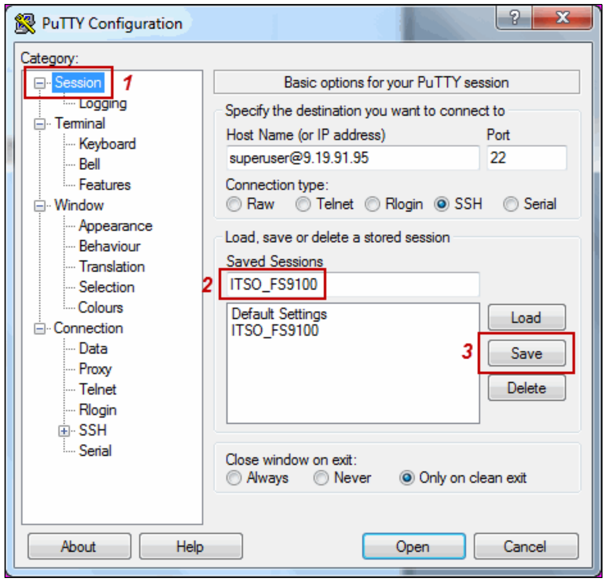


Figure 8-12 Save PuTTY session for use with plink

After a session is saved, you can use it to make transient connections from the command line (Example 8-9).

Example 8-9 Transient connection to IBM FlashSystem 9100 using plink with PuTTY session

```
C:\Users\IBM_ADMIN>plink -load ITSO_FS9100 lsenclosurebattery
enclosure_id battery_id status charging_status recondition_needed percent_charged
end_of_life_warning
1            1          online idle            no                 100 no
1            2          online idle            no                 100 no

C:\Users\IBM_ADMIN>
```

Persistent connections

A persistent connection is a connection that exists beyond the submission and execution of a single command. As outlined previously, the CIMOM provides a persistent connection, but it does not provide direct access to the command line. To provide a persistent connection to the command line, you must use multiple processes.

There are as many ways to provide a persistent connection to the command line as there are programming languages. Most methods involve creating a process that connects to the cluster, writing to its STDIN stream, and reading from its STDOUT and STDERR streams.

You can use persistent connections in several ways:

- On a per-script basis

  A script opens a connection that exists for the life of the script, enabling multiple commands to be submitted. The connection ends when the script ends.

- As a stand-alone script

  A connection is opened and other scripts communicate with this script to submit commands to the cluster. This approach enables the connection to be shared by multiple scripts. This in turn enables a greater number of independent scripts to access the cluster without using up all of the connection slots.

For more information about transient and persistent connections, see *IBM System Storage SAN Volume Controller and Storwize V7000 Replication Family Services*, SG24-7574.

8.4.3 Command-line scripting

When connected to the cluster command line, you can use small amounts of automation for various purposes, including for the following tasks:

- Repeatedly submitting a single command to a set of IBM FlashSystem 9100 objects
- Searching the configuration for objects conforming to certain criteria

The IBM FlashSystem 9100 command line is a highly restricted Bash shell. You cannot access UNIX commands, such as **cd** or **ls**. The only commands that are available are built-in commands, such as **echo** or **read**. In addition, redirecting inputs and outputs is *not* supported, but you can pipe commands together.

> **Note:** IBM FlashSystem 9100 uses IBM Spectrum Virtualize technology, built on the foundation of the SAN Volume Controller. The command lines function in the same secure way, which enables you to use existing scripting for automation and especially replication.

Example 8-10 shows a script that lists all volumes that are not online. This script complements the **filtervalue** parameter of the **lsvdisk** command. The **filtervalue** parameter provides matches only when a property matches a value.

Example 8-10 IBM FlashSystem 9100 command-line script listing volumes that are not online

```
001. lsvdisk -nohdr | while read id name IOGid IOGname status rest
002. do
003. if [ "$status" != "online" ]
004. then
005.  echo "Volume '$name' \($id\) is $status"
006. fi
007. done
```

> **Note:** The message `vdisks offline` is an error condition. In normal operations, you do not find any that are not online.

Line 001 submits the **lsvdisk** command and pipes the output to the **read** command, which is combined with a **while** command. This combination creates a loop that runs once per line of output from the **lsvdisk** command.

The **read** command is followed by a list of variables. A line is read from the **lsvdisk** command. The first word in that line is assigned to the first variable. The second word is assigned to the second variable, and so on, with any remaining words assigned to the final variable (with intervening spaces included).

In this case, the **-nohdr** parameter is used to suppress display of the headings.

Lines 003 - 006 check the status variable.

If it is not equal to `online`, the information is printed to STDOUT.

Submitting command-line scripts

You can submit command-line scripts from an interactive prompt, if required. However, you can also submit the scripts as batch files. Example 8-11 shows how to submit scripts as batch files with **`ssh`**.

Example 8-11 Submission of batch file to IBM FlashSystem 9100 using SSH

```
ssh superuser@ITSO_FS9100 -T < batchfile.sh
Host and WWPN info:

Host 0 (TA_Win2012) : WWPN is =10000000C9B83684
Host 0 (TA_Win2012) : WWPN is =10000000C9B83685
```

Example 8-12 shows how to submit scripts as batch files with **`plink`**.

Example 8-12 Submission of batch file to IBM FlashSystem 9100 using plink

```
C:\>plink -load ITSO_FS9100 -m batchfile.sh

Host and WWPN info:

Host 0 (RedHat) : WWPN is =2100000E1E302C73
Host 0 (RedHat) : WWPN is =2100000E1E302C72
Host 0 (RedHat) : WWPN is =2100000E1E302C51
Host 0 (RedHat) : WWPN is =2100000E1E302C50
Host 1 (AIX) : WWPN is =10000090FA13B915
Host 1 (AIX) : WWPN is =10000090FA13B914
Host 1 (AIX) : WWPN is =10000090FA0E5B95
Host 1 (AIX) : WWPN is =10000090FA0E5B94
Host 1 (AIX) : WWPN is =10000090FA02F630
Host 1 (AIX) : WWPN is =10000090FA02F62F
Host 1 (AIX) : WWPN is =10000090FA02F621
Host 1 (AIX) : WWPN is =10000090FA02F620
Host 2(TA_Win2012) : WWPN is =10000000C9B83684
Host 2(TA_Win2012) : WWPN is =10000000C9B83685
```

Both commands submit a simple batch file, as shown in Example 8-13. This command lists the WWPN for each host defined in the IBM FlashSystem 9100.

Example 8-13 Command-line batch file (batchfile.sh) used in the previous examples

```
echo "Host and WWPN info:"
echo " "
lshost -nohdr | while read name product_name WWPN
do
    lshost $name| while read key value
      do
      if [ "$key" == "WWPN" ]
      then
         echo "Host $name ($product_name) : WWPN is =$value"
      fi
    done
done
```

Server-side scripting

Server-side scripting involves scripting where the majority of the programming logic is run on a server.

Part of server-side scripting is the generation and management of connections to the IBM FlashSystem 9100 system. For an introduction of how to create and manage a persistent connection to a system and how to manage requests coming from multiple scripts, see “Persistent connections” on page 316.

The Perl module handles the connection aspect of any script. Because connection management is often the most complex part of any script, an advisable task is to investigate this module. Currently, this module uses transient connections to submit commands to a cluster, and it might not be the best approach if you plan to use multiple scripts submitting commands independently.

8.4.4 Sample commands of mirrored VDisks

This section contains sample commands that use the techniques demonstrated in 8.4.3, “Command-line scripting” on page 317. These examples are based on sample data designed to support this publication.

> **Note:** Start with small examples to understand the behavior of the commands.

VDisk mirroring to a second enclosure

This example shows how to mirror all VDisks for redundancy or how to vacate a storage system.

The sync rate

Example 8-14 shows mirroring the VDisks to a new managed disk group. In this example, `sync rate` is low so that it does not adversely affect the load on the system. You can check the progress of synchronization with **`lsvdisksyncprogress`** command.

Example 8-14 Mirror all VDisks

```
lsvdisk -filtervalue  copy_count=1 -nohdr |
while read id vdiskname rest
do
   addvdiskcopy -mdiskgrp newgroupname -syncrate 30 $id
done
Vdisk [0] copy [1] successfully created
Vdisk [1] copy [1] successfully created
Vdisk [2] copy [1] successfully created
Vdisk [3] copy [1] successfully created
Vdisk [4] copy [1] successfully created
Vdisk [5] copy [1] successfully created
```

Raise the sync rate

Raise the `sync rate` to 80 for all the VDisks currently not synchronized as shown in Example 8-15.

Example 8-15 Raise syncrate to 80

```
lsvdiskcopy -filtervalue sync=no -nohdr |
while read id vdisk copyid rest
```

```
do
   echo “Processing $vdisk”
   chvdisk -syncrate 80 $vdisk
done
```

Tip: Remember, raising the sync rate causes more I/O to be transferred, which can be an issue for a standard disk array.

Change primary in use to the new MDisk group

In Example 8-16 the primary volume copy is changed to the secondary copy that was created in Example 8-14 on page 319.

Note: Remember, all of these volumes must be in a sync state, as shown by the **lsvdisk** command output.

Example 8-16 Change volume mirror primary to copy in newgroupname

```
lsvdiskcopy -filtervalue mdisk_grp_name=newgroupname -nohdr |
while read id vdisk copyid rest
do
   echo Processing $vdisk
   chvdisk -primary $copyid $vdisk
done
```

Remove all the copies not primary

Example 8-17 removes all volume copies in the previous MDisk group.

Example 8-17 Remove volume copies

```
lsvdiskcopy -filtervalue mdisk_grp_name=prevmdiskgroup -nohdr |
while read id vdisk copyid rest
do
   echo “Processing rmvdiskcopy -copy $copyid $vdisk”
   rmvdiskcopy -copy $copyid $vdisk
done
```

Create compressed mirrored copies of VDisks not currently mirrored

Example 8-18 looks for all volumes that have a single copy and creates a mirrored compressed copy.

Example 8-18 Create compressed VDisk mirrors

```
lsvdisk -filtervalue  copy_count=1 -nohdr |
while read id vdiskname rest
do
addvdiskcopy -mdiskgrp BB1mdiskgrp0 -autoexpand -rsize 50% -syncrate 30
-compressed $id
done
Vdisk [0] copy [1] successfully created
Vdisk [1] copy [1] successfully created
Vdisk [2] copy [1] successfully created
Vdisk [3] copy [1] successfully created
```

```
Vdisk [4] copy [1] successfully created
Vdisk [5] copy [1] successfully created
```

> **Tip:** From the CLI, issue the **`help addvdiskcopy`** command or look in IBM Knowledge Center for details of parameters for this command. All options that are available in the GUI can be issued from the CLI, which helps you more easily work with large numbers of volumes.

8.4.5 Recover lost superuser password

Use the following steps to reset the IBM FlashSystem 9100 superuser password to the factory default value:

1. Locate a blank USB stick and write a file named `satask.txt` into the root directory of the first partition of the USB stick. The file should contain the single **`satask resetpassword`** command.
2. Plug the USB stick into a free USB port on the control enclosure.
3. Wait for the identification blue led to turn on then off.
4. Unplug the USB stick. The command output is written to the USB key in a file named `satask_result.html`. This is successful if no errors are returned.

   > **Tip:** The `satask_result.html` file also contains a report of the system status with several lines of output. The same system status can be obtained at any time by inserting a blank USB key into the control enclosure.

5. Log in to the GUI by using superuser and `passw0rd`, the default password. A prompt guides you to change the default password.

8.4.6 Back up IBM FlashSystem 9100 configuration

Right after configuring the system and before making major changes to the IBM FlashSystem 9100 configuration be sure to save the configuration of the system. This can assist you in restoring the system configuration when recommended by IBM Support. You can save the configuration by using the **`svcconfig backup`** command.

The **`backup`** command extracts and stores configuration information from the system, produces the *`svc.config.backup.xml`*, *`svc.config.backup.sh`*, and *`svc.config.backup.log`* files and saves them in the */tmp* folder. The **.xml** file contains the extracted configuration information; the **.sh** file contains a script of the commands used to determine the configuration information; and the **.log** file contains details about usage.

> **Note:** If a previous *`svc.config.backup.xml`* file exists in the *`/tmp`* folder, it is archived as *`svc.config.bak`*. Only one archive file is stored in the *`/tmp`* folder.

The next steps show how to create a backup of the configuration file and to copy the file to an external system:

1. Log in to the cluster IP using an SSH client and back up the system configuration:

   ```
   superuser> svcconfig backup
   ...............................................................
   CMMVC6155I SVCCONFIG processing completed successfully
   ```

2. List and filter the backup files:

```
IBM_FlashSystem:ITSO_9100:superuser>lsdumps | grep backup
56  svc.config.backup.bak_F313150-1
101 svc.config.backup.xml_F313150-1
102 svc.config.backup.log_F313150-1
103 svc.config.backup.sh_F313150-1
```

3. Copy the configuration backup file from the system. Using secure copy, copy the following file from the system and store it:

```
/tmp/svc.config.backup.xml
```

For example, use **pscp.exe**, which is part of the PuTTY commands family:

```
pscp.exe superuser@<cluster_ip>:/tmp/svc.config.backup.xml .
superuser@ycluster_ip> password:
svc.config.backup.xml     | 163 kB | 163.1 kB/s | ETA: 00:00:00 | 100%
```

Tip: Even though the dump files show the serial number of the system at the end of the filename, when copying the file do not use the serial number, instead use only the *svc.config.backup.xml* filename.

This process saves only the configuration of the system. User data must be backed up by using normal system backup processes.

8.4.7 Using the Software Upgrade Test Utility

Each software update requires that you run the software update test utility and then download the correct software package. In preparation for upgrading firmware on an IBM FlashSystem 9100, be sure to run the Software Upgrade Test Utility to ensures that your system is in a healthy condition to receive the new code.

Overview of Software Upgrade Test Utility

The software upgrade test utility indicates whether your current system has issues that need to be resolved before you upgrade to the next level. The test utility is run as part of the system update process for software or drive firmware. It can be run as many times as needed to assess the readiness of a system for upgrade as part of the upgrade planning process and we strongly recommend running this utility immediately prior to applying the update, making sure that there have not been any new releases of the utility since it was previously downloaded.

The installation and usage of this utility is non-disruptive and does not require any nodes to be restarted, so there is no interruption to host I/O. The utility will only be installed on the current configuration node canister.

Further information about the Software Upgrade Test utility can be found at the following site:

http://www.ibm.com/support/docview.wss?uid=ssg1S4000585

Running the Software Upgrade Test Utility from the command line

First of all, you will have to download the Software Upgrade Test Utility via IBM Fix Central. Details on how to access IBM Fix Central to download fixes, updates and drives can be found at 8.6.5, “Downloading from IBM Fix Central” on page 333. The Software Upgrade Test Utility appears in IBM Fix Central.

Figure 8-13 shows the Software Upgrade Test Utility package for download.

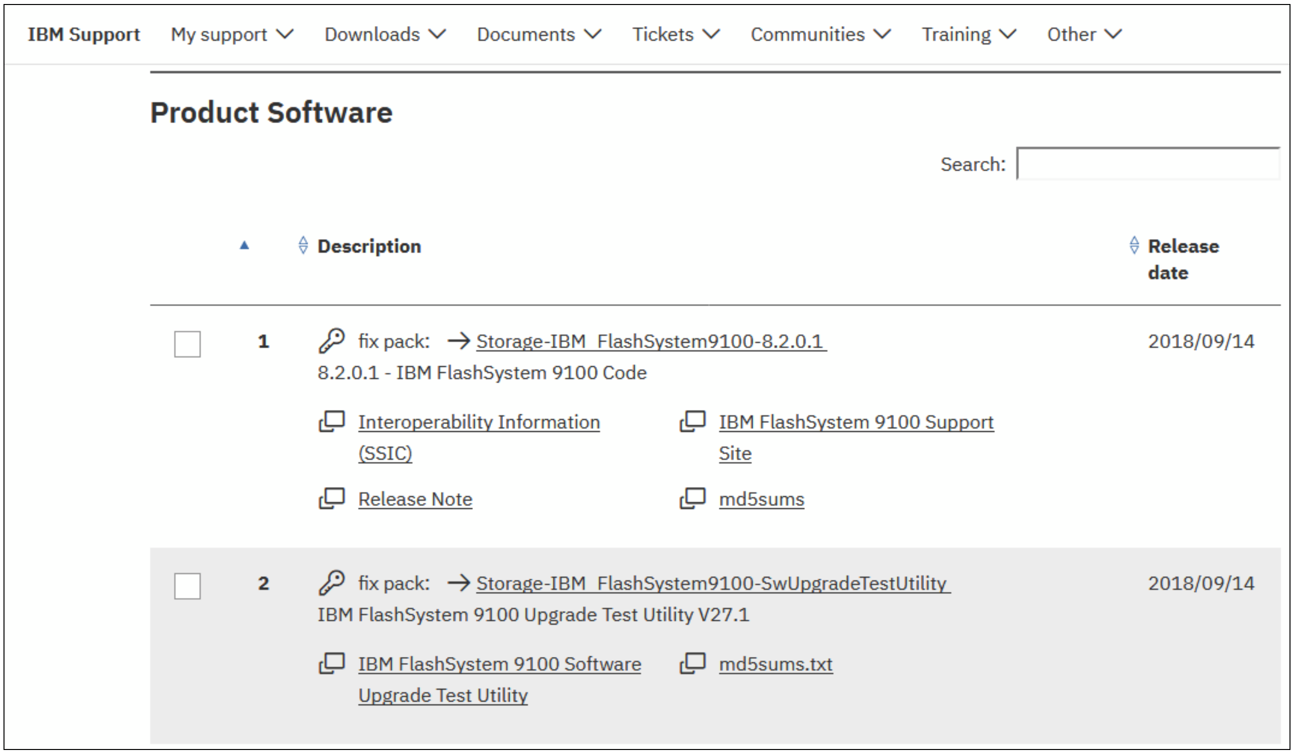


Figure 8-13 Software Upgrade Test Utility selection for download

To run the utility, complete the following steps:

1. Copy the utility to the `/upgrade` directory on the IBM FlashSystem V9000 using a secure copy utility such as Secure Copy Protocol (SCP) or **pscp.exe**:

```
pcsp <test_utility_filename> superuser@<cluster_ip_address>:/upgrade
```

2. Install the utility:

```
applysoftware -file <test_utility_filename>
```

3. Run the test utility:

```
svcupgradetest -v 8.2.0.1
```

The output is displayed in Example 8-19.

Example 8-19 Output from running the Software Upgrade Test Utility

```
IBM_FlashSystem:ITSO_9100:superuser>svcupgradetest -v 8.2.0.1
svcupgradetest version 27.1

Please wait, the test may take several minutes to complete.

******************* Warning found *******************

As of code version 8.1.3 an unsupported character in a Storwize/SVC fully
qualified domain name or DNS short name will result in a blank web page or http
error 400, when accessing the GUI. The permitted characters are A-Z,a-z,0-9,-.
This is due to stricter enforcement of a pre-existing standard. Your cluster name
contains a _ so you are seeing this warning in-case your fully qualified domain
name or DNS shortname also contains an unsupported character.
```

```
Results of running svcupgradetest:
==================================

The tool has found 0 errors and 1 warnings.

IBM_FlashSystem:ITSO_9100:superuser>
```

Tip: There will be a message `******************* Warning found *******************` in the output for each warning detected.

The utility remains installed and you can rerun it as many times as you want. Installing a new version overwrites the old version.

8.5 Call Home process

IBM encourages all clients to take advantage of the following settings to enable you and IBM to partner for your success. With the call home feature enabled, your system is effectively monitored 24 x 7 x 365. As an IBM client you can enjoy faster response times, faster problem determination and effectively reduced risk over an unmonitored system. In the future, IBM plans to use inventory report data to directly notify clients who are affected by known configuration or code issues.

While enabling call home reporting, IBM encourages clients to also enable inventory reporting in order to take advantage of this future offering. For a more detailed explanation, followed by steps to configure, see 7.2.1, “Email notifications” on page 243.

The configuration setup is a simple process and takes several minutes to complete.

8.5.1 Call Home details

The call home function opens a service alert if a serious error occurs on the system, automatically sending details of the error and contact information to IBM Service personnel. If the system is entitled for support, a problem management record (PMR) is automatically created and assigned to the appropriate IBM Service personnel.

The information provided to IBM in this case might be an excerpt from the Event Log containing the details of the error and client contact information from the system. This enables IBM Service personnel to contact you and arrange service on the system, which can greatly improve the speed of resolution by removing the need for you to detect the error and raise a support call.

8.5.2 Email alert

Automatic email alerts can be generated and sent to an appropriate client system administrator or distribution list. This is effectively the same as call home but you can be additionally notified about error, warning, information messages when they occur, and also you can receive inventory emails.

You can view IBM Knowledge Center documentation for your specific IBM FlashSystem 9100 product to determine whether a particular event is classified as error, warning, or informational. Look for the Notification type for each error to determine which you want to be notified for. Because you can customize this, based on the individual, maximum flexibility exists.

8.5.3 Inventory

Rather than reporting a problem, an email is sent to IBM that describes your system hardware and critical configuration information. Object names and other potentially sensitive information, such as IP addresses, are not sent.

IBM suggests that the system inventory be sent on a one-day or seven-day interval for maximum benefit.

8.6 Service support

Understanding how support issues are logged is important information. This section describes support for the IBM FlashSystem 9100, including the IBM Technical Advisor role, Enterprise Class Support, registering components in the Service Request Tool, and calling IBM for support.

8.6.1 IBM Storage Technical Advisor

The IBM Storage Technical Advisor (TA) enhances end-to-end support for complex IT solutions. Customers with Enterprise Class Support as described in 8.6.2, “Enterprise Class Support” on page 326, has an assigned technical advisor throughout the entire warranty period. This section describes the IBM TA program in general with specifics on how customers can work with their TA.

The TA service is built around three value propositions:

- Proactive approach to ensure high availability for vital IT services
- Client Advocate that manages problem resolution through the entire support process
- A trusted consultant for both storage hardware and software

Technical Advisors benefit customers by providing a consultant for questions on the IBM FlashSystem 9100. Most customers meet their TA during a Technical Delivery Assessment (Solution Assurance Meeting) before the initial installation. After this initial meeting, the TA is the focal point for support related activities as follows:

- Maintains a support plan that is specific to each client. This support plan contains an inventory of equipment including customer numbers and serial numbers.
- Coordinates service activities, working with your support team in the background. Monitors progress of open service requests, escalation, expert consultation on problem avoidance.
- Communicates issues with customers, IBM Business Partners, and IBM Sales teams.
- Periodically reviews and provides reports of hardware inventories and service requests. This includes using call home information to provide customer reports on the state of the customer systems.

- Oversight of IBM support activities helps companies anticipate and respond to new problems and challenges faster.
- Proactive planning, advice, and guidance to improve availability and reliability.

The IBM Storage Technical Advisor is an effective way to improve total cost of ownership and free up customer resources. Customers have options to extend the Technical Advisor service beyond the initial hardware warranty using IBM Technical Support Services (TSS) offerings.

Contact your IBM Sales Team or IBM Business Partner for details.

8.6.2 Enterprise Class Support

IBM Enterprise Class Support (ECS) delivers improved response times, hardware and software installation assistance, onsite code upgrades and service coordination across IBM. This enhanced support is available to IBM FlashSystem 9100 customers with the 3-year warranty machine type 9848, which include:

- IBM FlashSystem 9150 Control Enclosure 9848-AF8
- IBM FlashSystem 9110 Control Enclosure 9848-AF7
- IBM FlashSystem 9100 Expansion Enclosure 9848-A9F
- IBM FlashSystem 9100 Expansion Enclosure 9848-AFF

ECS also provides services for these software products:

- IBM Spectrum Virtualize Software for FlashSystem 9110 Controller V8 Software, PID 5639-FA2
- IBM Spectrum Virtualize Software for FlashSystem 9150 Controller V8 Software, PID 5639-FA3

> **Note:** Other software that is used with an IBM FlashSystem 9100 product is not covered under ECS.

For the duration of the Enterprise Class Support warranty period the following service functions are enhanced:

- More of the hardware installation and configuration procedures are performed by IBM service representatives.
- System software is updated to the latest release during the initial installation by the IBM service representative.
- Subsequent software updates are installed by an IBM service representative when requested by the customer or by IBM - up to six (6) software updates (remote, or onsite if necessary) during the warranty period.
- A technical advisor is assigned throughout the entire warranty period. The technical advisor provides a documented support plan, coordinates problem and crisis management, and consults with the customer about FlashSystem software updates.
- A remote account advocate is assigned to the system for the warranty period to provide a single point of contact for managing reported hardware and software issues. The advocate provides an escalation path, as needed, and reviews support issues during regularly scheduled appointments.
- Problem management is enhanced, with faster initial response time for high severity problems, and support for remote support assistance.

IBM Enterprise Support is an evolving service designed to assist you with the support of your storage products. IBM FlashSystem 9100 includes the optional capability for remote support. As with call home, by choosing to enable this capability, you can benefit from Enterprise Class Support as features are developed to enhance the support received.

8.6.3 Providing logs to IBM ECuRep

IBM Enhanced Customer Data Repository (ECuRep) is a secure and fully supported data repository with problem determination tools and functions. It updates problem management records (PMR) and maintains full data lifecycle management.

This server-based solution is used to exchange data between IBM customers and IBM Technical Support. Do not place files on or download files from this server without prior authorization from an IBM representative. The representative is able to provide further instructions as needed.

To use ECuRep, you need a documented problem management record (PMR/Case) number either provided by the IBM support team with a *call home*, or issued by using the IBM Service Request tool on the IBM support portal:

https://www.ibm.com/support/home/

IBM provides the service request (SR) problem submission tool (the link is highlighted in Figure 8-14) to electronically submit and manage service requests on the web. This tool replaces the Electronic Service Request (ESR) tool.

Figure 8-14 shows the IBM Support portal main page.

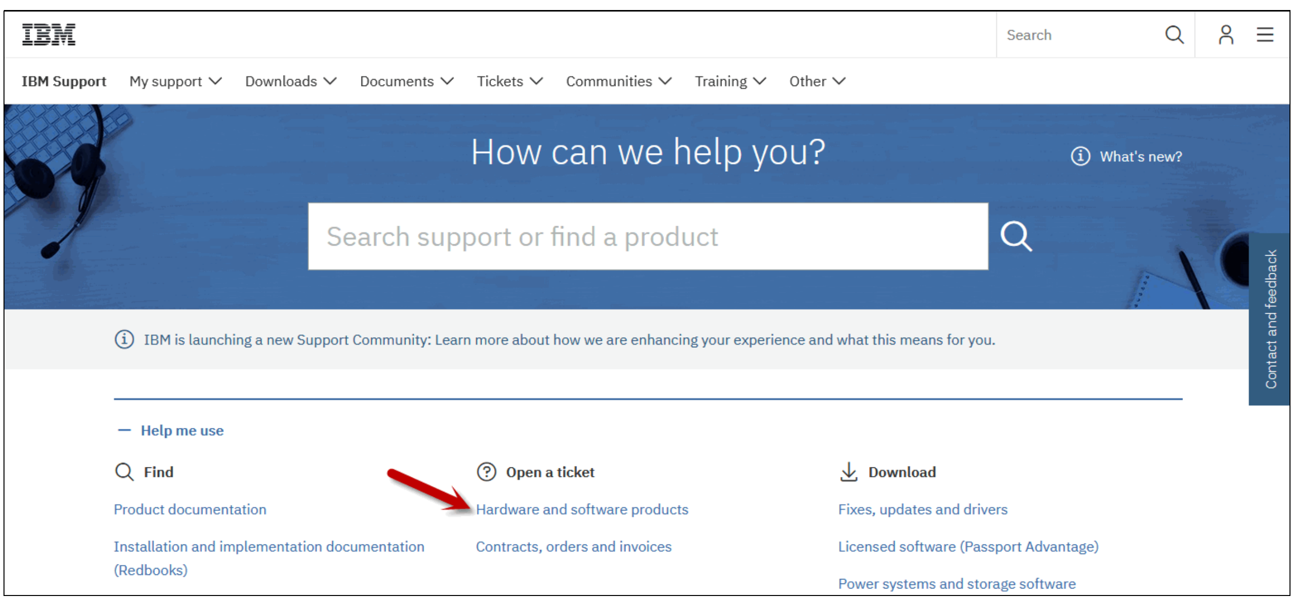


Figure 8-14 Link to Service Request (SR) tool

To provide logs to IBM ECuRep, complete the following steps:

1. Go to the Enhanced Customer Data Repository (ECuRep) web page:

   https://www.secure.ecurep.ibm.com/app/upload

This web page provides information about the repository, instructions for preparing files for upload, and multiple alternatives for sending data. For details, you can click **Help** (see Figure 8-15).

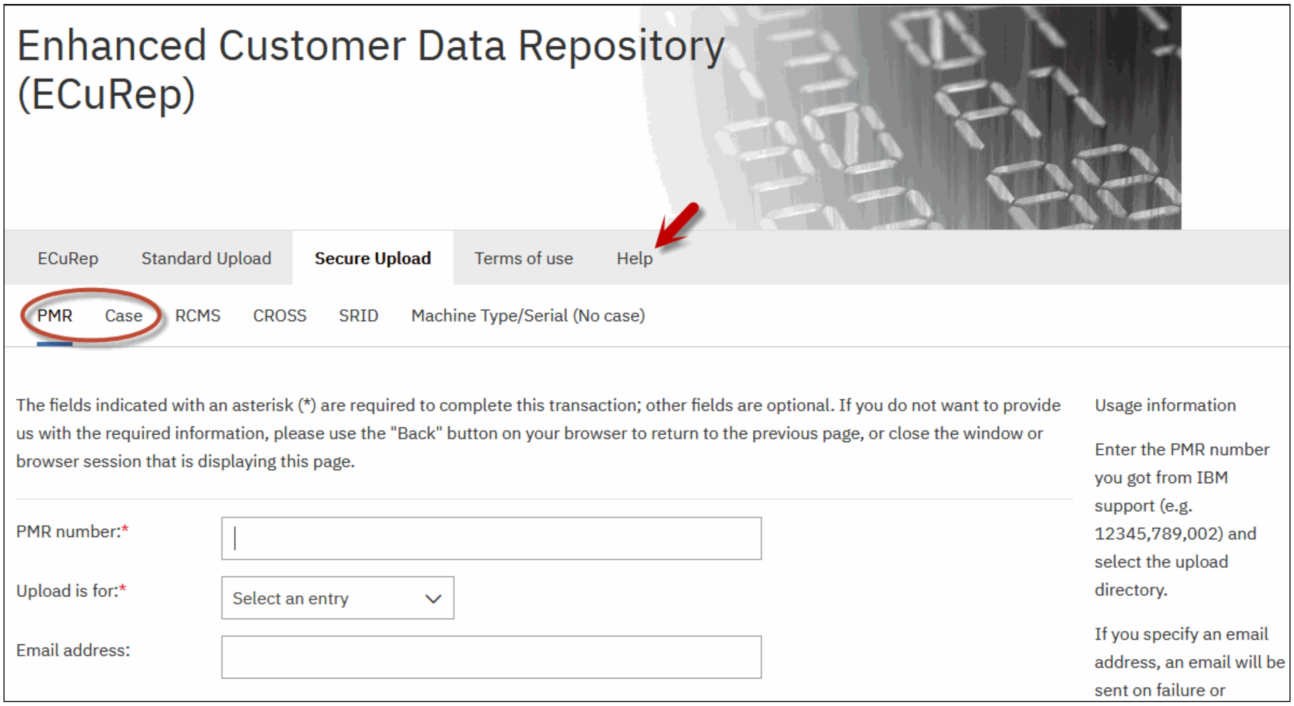


Figure 8-15 ECuRep portal showing Help link and PMR/Case options

> **Note:** This system is connected to the IBM Problem Management Record. Support tickets are automatically updated, with the files uploaded and queued for an IBM support representative response.

2. IBM provides multiple options for uploading data. Review the options for sending data before you complete the PMR/Case number. The following options are shown in Figure 8-16 on page 329:
   - Notice in this description that the Send Data tab is selected.
   - As another way to upload a file other than using the standard method, you can select either FTP (1) or the Java utility (2). The Java utility is the most efficient method to upload a file.
   - Select **Prepare data** tab (3) to see the details about file name conventions.

Figure 8-16 shows the ECuRep Help options.

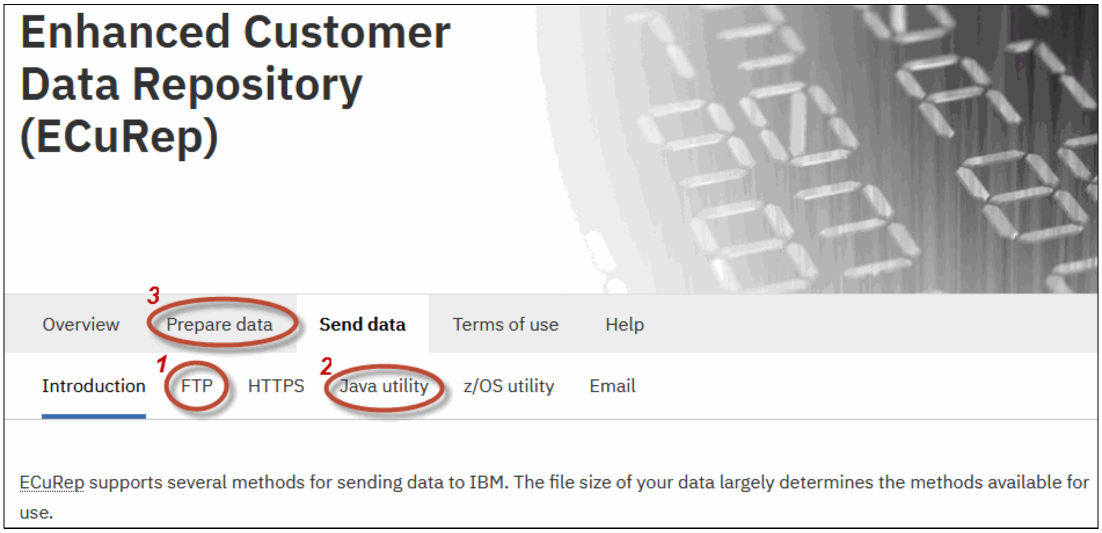


Figure 8-16 Options for sending data

3. Secure Upload (Figure 8-17 on page 330) is the default upload selection. Complete these fields and then click **Continue**:
   – PMR: Using the PMR number on this form accurately logs the files uploaded to the correct PMR.

Note: Remember to select the Case tab in case you are working with a Case number and not a PMR.

   – Upload is for: Select **Hardware** for the IBM FlashSystem 9100.
   – Email address: (Optional) Provide your email address for a confirmation.

Figure 8-17 shows ECuRep Secure Upload option.

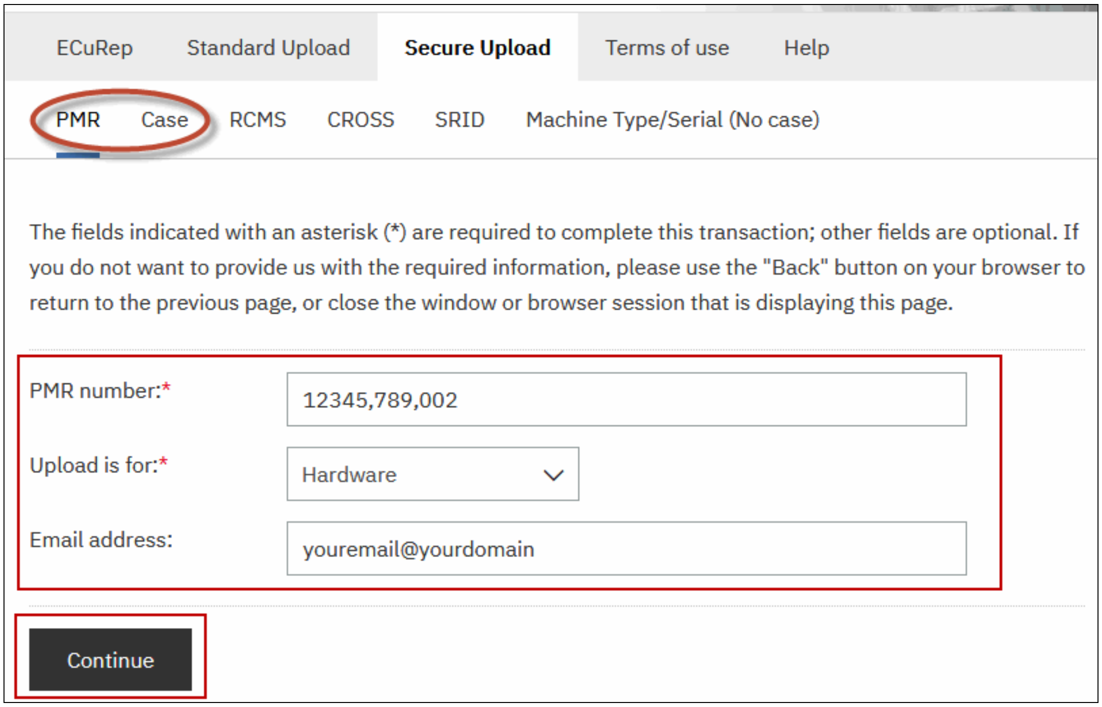


Figure 8-17 Using the standard option

4. The file selection panel opens (Figure 8-18). Select files and click **Upload.**

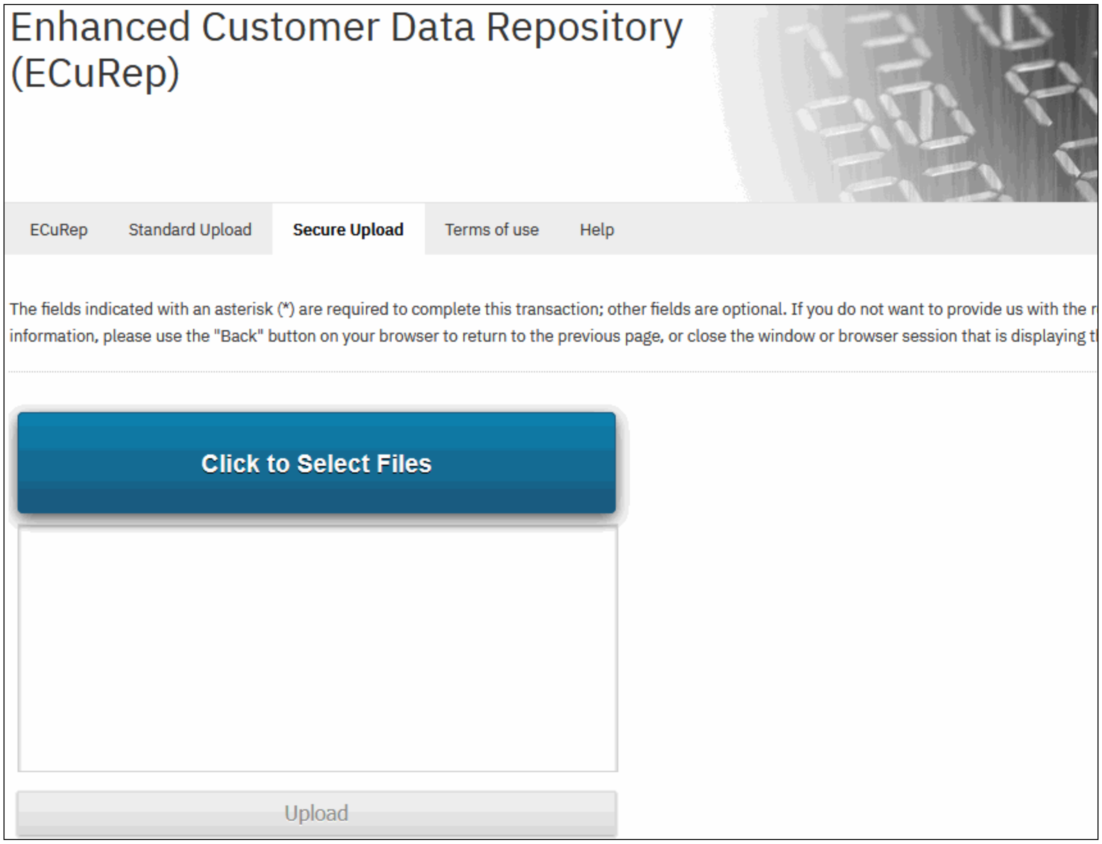


Figure 8-18 ECuRep file selection dialog

> **Tip:** Most clients find this way the most effective method to upload logs. IBM suggests understanding the best method for your organization *in advance* and *documenting the process* to save precious time during a crisis.

8.6.4 Uploading logs to IBM Blue Diamond Lab

IBM has a long history of providing clients with security technologies to protect data. Whether your company is in the Health care industry, you will be making usage of Blue Diamond Enhanced Secure Support. It enables IBM clients to receive worldwide support in a consolidated data security environment by adding layers of security and allowing you to use a secure, Blue Diamond-dedicated portal to upload diagnostic data to IBM Support for problem determination.

Only fully dedicated and Blue Diamond-trained support professionals are authorized to access data within the Blue Diamond environment. To upload data to the secure FTP server, you need an active PMR/Case number.

Follow the guide steps listed below in order to upload support logs to the IBM Blue® Diamond FTP:

1. Log into the Blue Diamond Secure FTP portal at `https://msciportal.im-ies.ibm.com/Portal.aspx`, as shown in Figure 8-19 on page 332.

Figure 8-19 shows the IBM Blue Diamond home page.

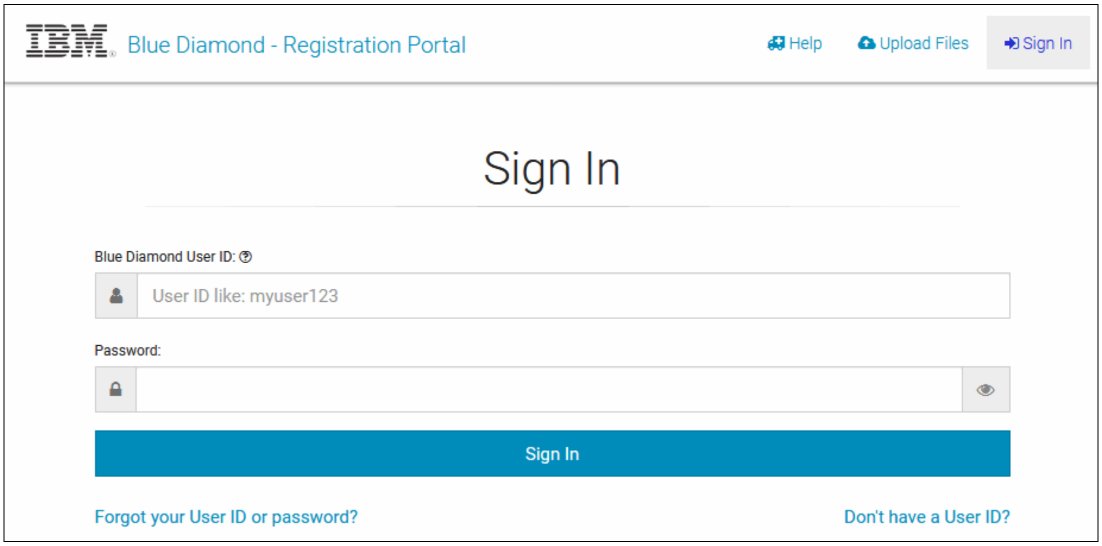


Figure 8-19 Blue Diamond sign in

2. Log into our secure FTP server, using your Blue Diamond credentials, as shown in Figure 8-20.

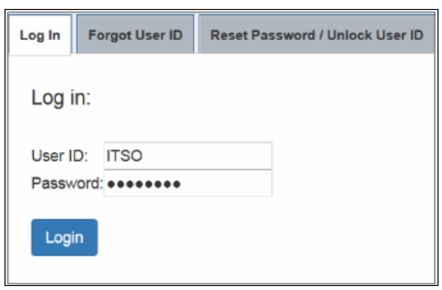


Figure 8-20 Blue Diamond FTP Log in page

3. When you are logged in, click the **Upload Data** button, as shown in Figure 8-21.

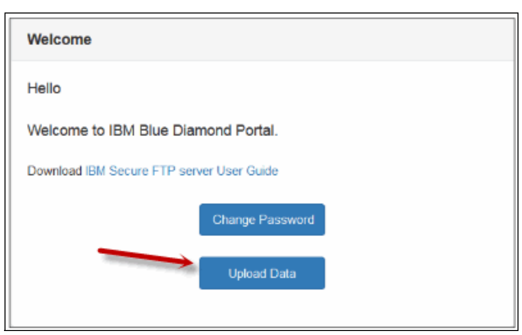


Figure 8-21 Blue Diamond Data Upload page

4. Navigate to the folder that contains your company name (IBM/YourCompanyName). See Figure 8-22.

Note: You are only permitted to see your own company folder.

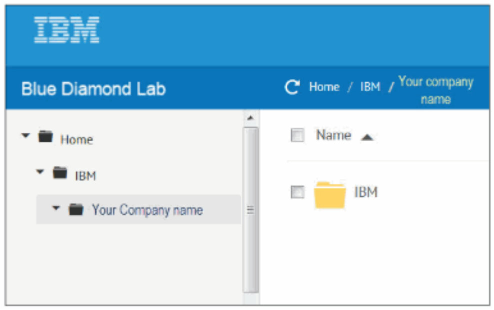


Figure 8-22 Navigate your company folder

5. Create a sub-folder with the name of your PMR/Case number (Example, 12345,678,000 / TS001234567) (Figure 8-23).

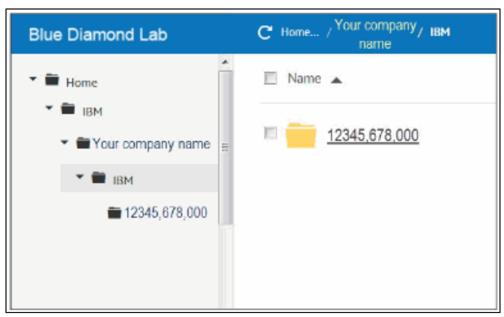


Figure 8-23 Sub-folder with PMR number

6. Upload the diagnostic data to the sub-folder that you have created.

After the file is successfully uploaded to the Blue Diamond Lab, IBM Support receives a notification through your active PMR/Case and can then review the logs.

8.6.5 Downloading from IBM Fix Central

IBM Fix Central provides fixes and updates for your system's software, hardware, and operating system. Go to the IBM Fix Central web page:

http://www.ibm.com/support/fixcentral

If you are not looking for fixes or updates, go to IBM Passport Advantage to download most purchased software products, or My Entitled Systems Support to download system software.

Using an IBMid

To use the IBM Fix Central website, you must have an IBMid. Your IBMid provides access to IBM applications, services, communities, support, online purchasing, and more. Additionally, your information is centralized so you can maintain it in a convenient and secure location. The benefits of having an IBMid will increase over time as more applications migrate to IBMid.

At the IBM Fix Central main page, select the person icon (step number 1 in Figure 8-24) then click the **Sign in** option (step number 2 in Figure 8-24).

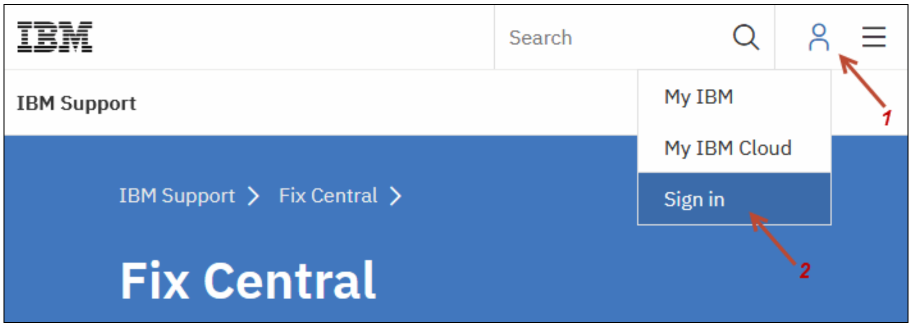


Figure 8-24 IBM Fix Central main page

The login window is shown in Figure 8-25.

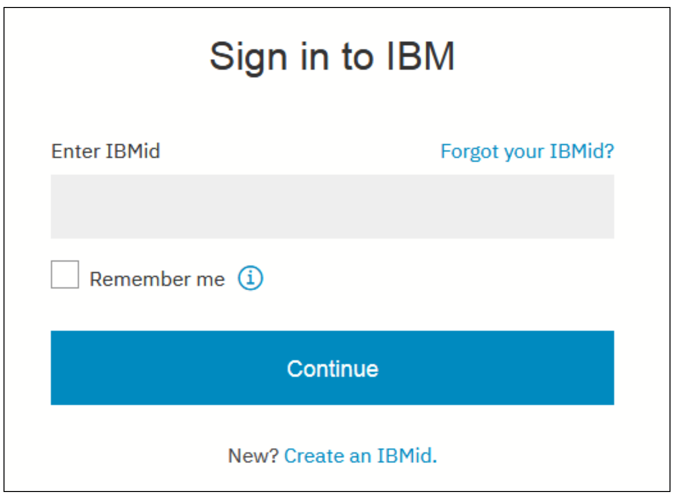


Figure 8-25 IBM id login window

Fix Central

The following steps document the current process for obtaining updates for your IBM FlashSystem 9100. This site is frequently updated based on customer feedback and as IBM documents field experience. It is a good practice to review the support information on this site on a regular basis.

1. After signing in with your IBMid, a page opens to the Support Portal (Figure 8-26 on page 335). In the **Find product (1)** tab, go to **Product selector (2)** field and start typing `FlashSystem 9100` **(3)**. Select **IBM FlashSystem 9100 family** from the list **(4)**. The IBM FlashSystem 9100 specific information is displayed.

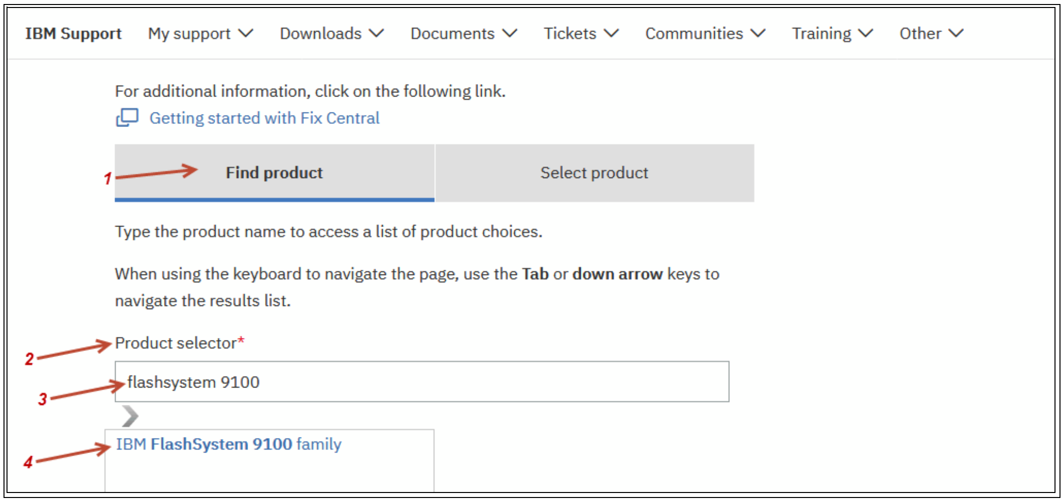


Figure 8-26 IBM Fix Central Support Portal

2. Select the version (Figure 8-27) that you want to download or select All to see all available options, then click **Continue**.

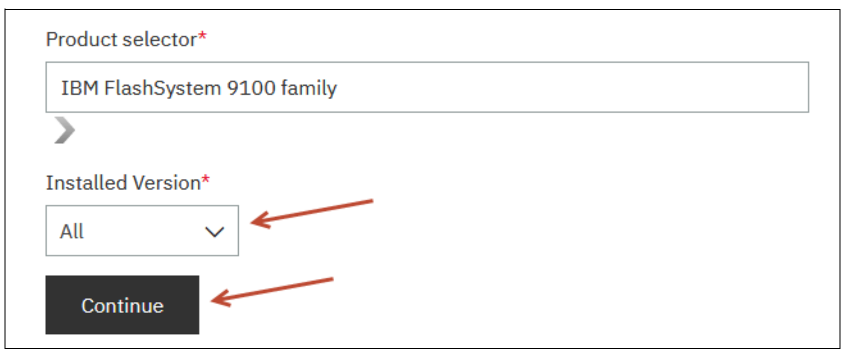


Figure 8-27 Product selector version

3. The Select fixes panel (Figure 8-28) provides download options for the software you are looking for. In this example we are showing where to go to download the Product Software.

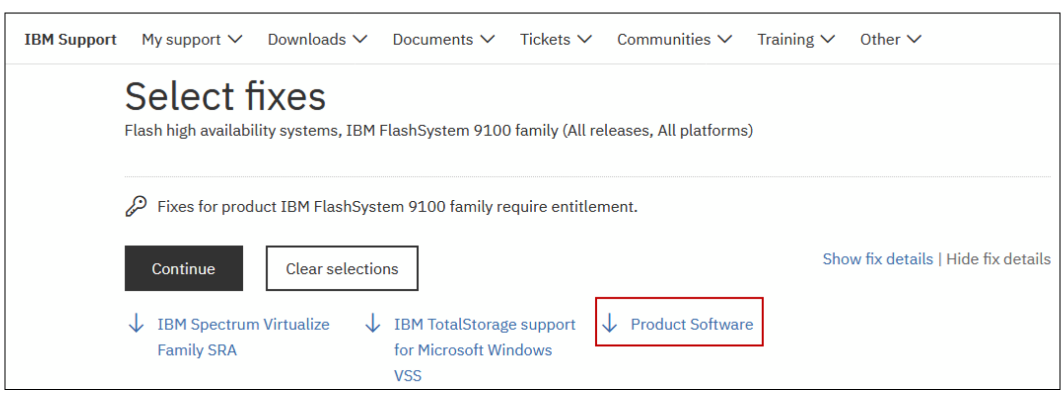


Figure 8-28 Select the Product Software

4. The license agreement is presented. At this time, entitlement is confirmed through the acceptance of this agreement. Click **I agree** to continue.

5. Read the release notes to determine the best fix pack for your environment. Click the fix pack link to be directed to the download page or Select the fix pack (select the box next to it) and click **Continue** at the bottom of the page to initiate the file transfer. Figure 8-29 shows you how to locate the release notes and the software download links.

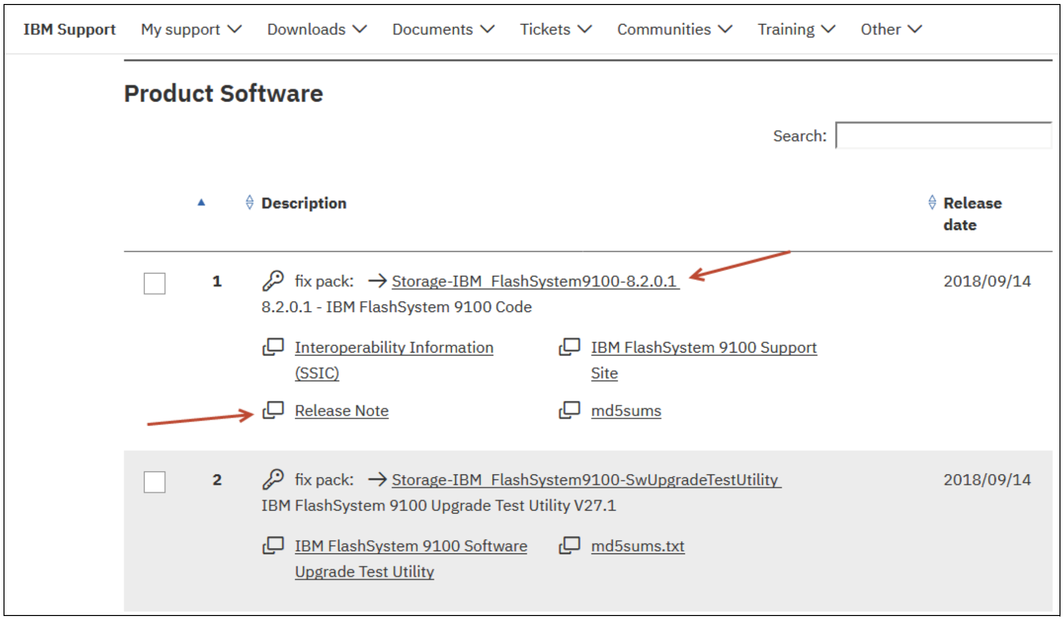


Figure 8-29 Select the desired software level after reading the Release Notes

Note: Always read the release notes. They often contain special instructions related to the upgrade that should be part of your planning.

6. Confirm your selection then click **Download now** (Figure 8-30) to start the download process. Download Director is the preferred method for download because it is multi-threaded.

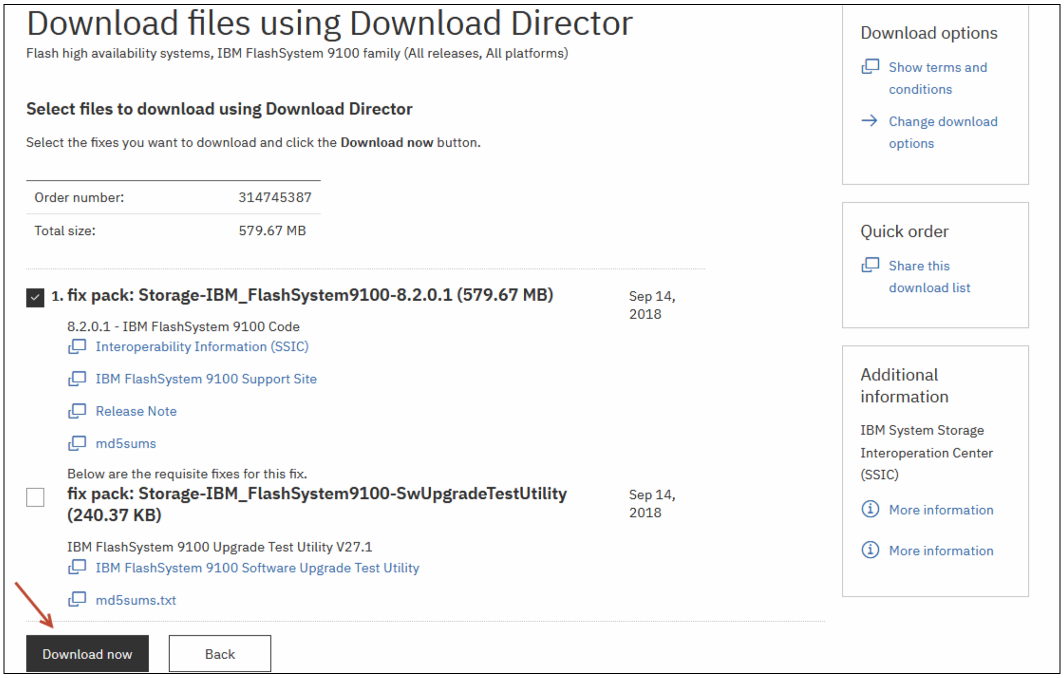


Figure 8-30 Download now

Check that your download completes successfully.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Some publications referenced in this list might be available in softcopy only:

- *Accelerate with IBM FlashSystem V840 Compression*, REDP-5147
- *Deploying IBM FlashSystem V840 Storage in a VMware and Cloud Environment*, REDP-5148
- *IBM FlashSystem 900 Model AE3 Product Guide*, REDP-5467
- *Implementing IBM FlashSystem 900 Model AE3*, SG24-8414
- *IBM FlashSystem V9000 Model AE3 Product IBM FlashSystem V9000 AC3 with Flash Enclosure Model AE3 Product Guide*, REDP-5468
- *IBM FlashSystem V9000 and VMware Best Practices Guide*, REDP-5247
- *IBM FlashSystem V9000 in a VersaStack Environment*, REDP-5264
- *IBM FlashSystem V9000 Version 7.7 Product Guide*, REDP-5409
- *IBM System Storage SAN Volume Controller and Storwize V7000 Best Practices and Performance Guidelines*, SG24-7521
- *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933
- *Implementing the IBM Storwize V7000 with IBM Spectrum Virtualize V8.1*, SG24-7938
- *Introducing and Implementing IBM FlashSystem V9000*, SG24-8273

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Other publications and resources

These websites are also relevant as further information sources:

- IBM FlashSystem 9100

  https://www.ibm.com/uk-en/marketplace/flashsystem-9100/details
- IBM FlashSystem resources

  https://www.ibm.com/uk-en/marketplace/flashsystem-9100/resources
- IBM FlashSystem 9100 in IBM Knowledge Center

  https://www.ibm.com/support/knowledgecenter/STSLR9_8.2.0/com.ibm.fs9100_820.doc/fs9100_ichome.html

- IBM Storage Insights

  https://www.ibm.com/support/knowledgecenter/SSQRB8/com.ibm.spectrum.si.doc/tpch_saas_welcome.html
- IBM FlashSystem family

  https://ibm.biz/BdsaFH
- IBM Flash Storage

  https://www.ibm.com/it-infrastructure/storage/flash
- IBM System Storage Interoperation Center (SSIC)

  https://www.ibm.com/systems/support/storage/ssic/interoperability.wss

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Redbooks

IBM FlashSystem 9100 Architecture, Performance, and

SG24-8425-00

ISBN 0738457485

(0.5” spine)
0.475”<->0.873”
250 <-> 459 pages

SG24-8425-00

ISBN 0738457485

Printed in U.S.A.

Get connected

Redbooks®
ibm.com/redbooks