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** ....................................................... ix
**Trademarks** .................................................... x

**Preface** ........................................................ xi
**Authors** ........................................................ xi
**Now you can become a published author, too!** .................... xiv
**Comments welcome.** .......................................... xiv
**Stay connected to IBM Redbooks** ............................... xv

**Chapter 1. IBM FlashSystem 9100 introduction** .................. 1
  1.1 IBM FlashSystem 9100 high-level features .................. 2
    1.1.1 FlashSystem 9100 Utility Models UF7 and UF8 .......... 5
  1.2 Integration with different environments .................. 6
  1.3 Why FlashCore matters ..................................... 6
  1.4 Clustering rules and upgrades ............................. 6
  1.5 Migration of V9000 storage ................................ 6
    1.5.1 FlashSystem V9000 flash enclosure repurposed ........ 7
    1.5.2 IBM FlashSystem 9100: IBM Tier 1 storage ............ 7
  1.6 Advanced software features ............................... 7
    1.6.1 Advanced functions for data reduction ................ 7
    1.6.2 Data migration ....................................... 8
    1.6.3 Advanced copy services ................................ 8
    1.6.4 External virtualization ................................ 9
    1.6.5 Easy Tier ............................................ 9
  1.7 IBM HyperSwap ............................................. 10
  1.8 Licensing .................................................. 10

**Chapter 2. IBM FlashSystem 9100 architecture** ................. 11
  2.1 FlashSystem 9100 hardware components .................... 12
  2.2 IBM FS9100 Control Enclosure ................................ 13
    2.2.1 Model 9110 Control Enclosure AF7 ..................... 14
    2.2.2 Model 9150 Control Enclosure AF9 ..................... 14
    2.2.3 Model 9150 Expansion Enclosure Models AFF and AF9 .... 15
    2.2.4 Model AFF ............................................ 15
    2.2.5 Model AF9 ............................................. 15
    2.2.6 FlashSystem 9100 Utility Models UF7 and UF8 .......... 15
  2.3 FlashCore Module and NVMe drives .......................... 16
    2.3.1 Industry-standard NVMe drives ........................ 17
  2.4 NVMe and adapter support .................................. 17
    2.4.1 Support for adapters, host platforms, and switches .... 17
  2.5 Software features and licensing ........................... 18
    2.5.1 IBM Spectrum Virtualize for IBM FlashSystem 9100 .... 18
    2.5.2 IBM Multi-Cloud starter software for IBM FlashSystem 9100 19
    2.5.3 IBM FlashSystem 9100 Multi-Cloud solutions ........... 19
    2.5.4 IBM FS9100 high availability ........................ 20
  2.6 Data protection on IBM FS9100 ............................. 20
    2.6.1 Variable Stripe RAID .................................. 20
    2.6.2 DRAID ................................................ 20
### Chapter 3. Data reduction and tools

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Compression and deduplication techniques</td>
<td>24</td>
</tr>
<tr>
<td>3.1.1 Deduplication items</td>
<td>25</td>
</tr>
<tr>
<td>3.2 Data Reduction Pools inside the IBM FS9100</td>
<td>29</td>
</tr>
<tr>
<td>3.2.1 DRP Volume types</td>
<td>30</td>
</tr>
<tr>
<td>3.2.2 Data Reduction Pool components</td>
<td>33</td>
</tr>
<tr>
<td>3.2.3 Allocation block size</td>
<td>33</td>
</tr>
<tr>
<td>3.3 Comparing RACE to Data Reduction Pools</td>
<td>34</td>
</tr>
<tr>
<td>3.3.1 Benefits of Data Reduction Pools</td>
<td>35</td>
</tr>
<tr>
<td>3.4 Data Reduction Pools and unmap</td>
<td>36</td>
</tr>
<tr>
<td>3.5 Data Reduction Pools with Easy Tier</td>
<td>37</td>
</tr>
<tr>
<td>3.6 Garbage collection</td>
<td>37</td>
</tr>
<tr>
<td>3.7 Data Reduction Pools with deduplication</td>
<td>38</td>
</tr>
<tr>
<td>3.7.1 Typical case examples of DRP</td>
<td>38</td>
</tr>
<tr>
<td>3.8 Estimating data reduction by using various tools</td>
<td>38</td>
</tr>
<tr>
<td>3.8.1 Comprestimator utility</td>
<td>38</td>
</tr>
<tr>
<td>3.8.2 Comprestimator using the host-based CLI utility</td>
<td>40</td>
</tr>
<tr>
<td>3.8.3 Using Data Reduction Estimation Tool</td>
<td>41</td>
</tr>
<tr>
<td>3.9 When to use Flash Core Modules or Data Reduction Pools</td>
<td>44</td>
</tr>
<tr>
<td>3.9.1 Flash Core Modules advantages</td>
<td>44</td>
</tr>
<tr>
<td>3.9.2 Data Reduction Pool advantages</td>
<td>44</td>
</tr>
<tr>
<td>3.10 General guidelines for performance, capacity, and availability options</td>
<td>45</td>
</tr>
<tr>
<td>3.10.1 Performance</td>
<td>45</td>
</tr>
<tr>
<td>3.10.2 Capacity</td>
<td>46</td>
</tr>
<tr>
<td>3.10.3 Availability considerations when configuring the IBM FS9100</td>
<td>54</td>
</tr>
</tbody>
</table>

### Chapter 4. Planning

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 FlashSystem 9100</td>
<td>58</td>
</tr>
<tr>
<td>4.2 General planning introduction</td>
<td>59</td>
</tr>
<tr>
<td>4.3 Physical planning</td>
<td>62</td>
</tr>
<tr>
<td>4.3.1 IBM FlashSystem 9100 control enclosures</td>
<td>63</td>
</tr>
<tr>
<td>4.3.2 Racking considerations</td>
<td>65</td>
</tr>
<tr>
<td>4.3.3 Power requirements</td>
<td>67</td>
</tr>
<tr>
<td>4.3.4 Network cable connections</td>
<td>69</td>
</tr>
<tr>
<td>4.3.5 SAS expansion enclosures</td>
<td>74</td>
</tr>
<tr>
<td>4.4 Logical planning</td>
<td>76</td>
</tr>
<tr>
<td>4.4.1 Management IP addressing plan</td>
<td>76</td>
</tr>
<tr>
<td>4.4.2 SAN zoning and SAN connections</td>
<td>78</td>
</tr>
<tr>
<td>4.4.3 IP Replication and Mirroring</td>
<td>79</td>
</tr>
<tr>
<td>4.4.4 Native IP replication</td>
<td>80</td>
</tr>
<tr>
<td>4.4.5 Advanced Copy Services</td>
<td>81</td>
</tr>
<tr>
<td>4.4.6 Call home option</td>
<td>86</td>
</tr>
<tr>
<td>4.4.7 Remote Support Assistance</td>
<td>88</td>
</tr>
<tr>
<td>4.5 IBM Storage Insights</td>
<td>92</td>
</tr>
<tr>
<td>4.5.1 Architecture, security, and data collection</td>
<td>94</td>
</tr>
<tr>
<td>4.5.2 Customer dashboard</td>
<td>96</td>
</tr>
<tr>
<td>4.6 IBM FlashSystem 9100 system configuration</td>
<td>96</td>
</tr>
<tr>
<td>4.6.1 Volume considerations</td>
<td>100</td>
</tr>
<tr>
<td>4.6.2 IBM Easy Tier</td>
<td>102</td>
</tr>
<tr>
<td>4.6.3 SAN boot support</td>
<td>104</td>
</tr>
<tr>
<td>4.7 Licensing and features</td>
<td>104</td>
</tr>
<tr>
<td>4.7.1 IBM FlashSystem 9100 products licenses</td>
<td>104</td>
</tr>
<tr>
<td>4.7.2 SAS Expansion Enclosures</td>
<td>104</td>
</tr>
</tbody>
</table>
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

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX® IBM Cloud™ Real-time Compression™
Bluemix® IBM FlashCore® Redbooks®
Cognitive Business® IBM FlashSystem® Redpaper™
Db2® IBM Spectrum™ Redbooks (logo)®
DS5000™ IBM Spectrum Accelerate™ Storwize®
DS8000® IBM Spectrum Control™ System Storage®
Easy Tier® IBM Spectrum Protect™ System Storage DS®
FlashCopy® IBM Spectrum Storage™ Variable Stripe RAID™
HyperSwap® IBM Spectrum Virtualize™ Watson™
IBM® MicroLatency® WebSphere®
IBM Blue® Passport Advantage® XIV®

The following terms are trademarks of other companies:

SoftLayer, are trademarks or registered trademarks of SoftLayer, Inc., an IBM Company.

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

LTO, the LTO Logo and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.
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™, which allows you to easily add the multi-cloud solutions that best support your business.

In this IBM Redbook publication, we discuss the product’s features and 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 who 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® and YouTube videos. Andrew brings over 24 years of data center experience inside the Fortune 100 to the IBM team. He graduated 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 support on mainframe servers and technical education development. He has written many Redbook publications about the FlashSystems products and is a Redbook Platinum level author. He holds IBM certifications in Supporting IT Solutions at an expert level, and 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 various storage technologies, including the IBM System Storage® DS5000™, IBM DS8000®, 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 that are related to the midrange IBM System Storage DS® Storage Manager range of products, and FlashSystem products.

Tony Pacheco is an IBM Technical Advisor who is 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 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 Engineer from 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. He has 22 years of experience working on IBM storage, including 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 and a post graduate degree in Computer Networks. He has 11 years of experience in storage services and support and is 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 20 years of experience in planning, managing, designing, implementing, problem analysis, and tuning of storage systems and SAN environments. He has worked at IBM for 18 years. His areas of expertise include IBM FlashSystems, IBM Storage solutions, SAN fabric networking, and Open System Storage IO performance. Al has been a co-author of more than 15 IBM Redbook publications and IBM Redpaper™ 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:
- Stay current on recent Redbooks publications with RSS Feeds:
  http://www.redbooks.ibm.com/rss.html
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:

> 1.1, “IBM FlashSystem 9100 high-level features” on page 2
> 1.2, “Integration with different environments” on page 6
> 1.3, “Why FlashCore matters” on page 6
> 1.4, “Clustering rules and upgrades” on page 6
> 1.5, “Migration of V9000 storage” on page 6
> 1.6, “Advanced software features” on page 7
> 1.7, “IBM HyperSwap” on page 10
> 1.8, “Licensing” on page 10
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 that include 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 the capacity and throughput, which gives 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 must 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®. 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 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. Added software features include GUI enhancements, a new dashboard, remote support assistance, data de-duplication, and Storage Insights configuration.

Figure 1-1 shows the IBM FlashSystem 9100 Control Enclosure with one of the IBM NVMe drives 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. It can also house up to 24 NVMe capable flash drives. These drives can be industry standard NVMe type or the exclusive IBM NVMe FCM.
- An expansion enclosure allows you to increase the available capacity of the IBM FlashSystem 9100 cluster. It communicates with the control enclosure by way of a dual pair of 12 Gbps SAS connections. These expansion enclosures can house many flash (SSD) SAS type drives, depending on which model of enclosure is ordered.

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.

Two standard models of IBM FlashSystem 9100 are available: 9110-AF7 and 9150-AF8.

Two utility models of the IBM FlashSystem 9100 are available: 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 used in the Storage Utility Offering space. These models are physically and functionally identical to the IBM FlashSystem 9848-AF7 and AF8 respectively, except for target configurations and variable capacity billing.

The variable capacity billing uses IBM Spectrum Control™ Storage Insights to monitor the system usage, which allows 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 written is considered used. For thick provisioning, total allocated volume space is considered used.

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 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 side of the bezel cover, which covers the rack mounting screws.
Figure 1-2 shows the IBM FlashSystem 9100 bezel and NVMe drive description.

Labeling on the NVMe drive provides the drive type, capacity, the type of drive, and the FRU number. The example that is shown in Figure 1-2 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 listed in Table 1-1.

Table 1-1  FS9100 memory configurations

<table>
<thead>
<tr>
<th>Memory per canister</th>
<th>Memory per control enclosure</th>
</tr>
</thead>
<tbody>
<tr>
<td>64 GB</td>
<td>128 GB</td>
</tr>
<tr>
<td>128 GB</td>
<td>256 GB</td>
</tr>
<tr>
<td>192 GB</td>
<td>384 GB</td>
</tr>
<tr>
<td>384 GB</td>
<td>768 GB</td>
</tr>
<tr>
<td>576 GB</td>
<td>1152 GB</td>
</tr>
<tr>
<td>768 GB</td>
<td>1536 GB</td>
</tr>
</tbody>
</table>

Note: FS9100 refers to both the FS 9110 (Model AF7) and the FS 9150 (model AF8). If a feature or function is specific to one of the models, FS9110 or FS 9150 is used.

The FS9100 supports NVMe attached flash drives, both the IBM Flash Core Modules (FCM) and off-the-shelf SSDs. The IBM FCM’s support hardware compression at line data rates. IBM offers the FCM’s 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 more capacity in 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 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.

1.1.1 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 that is used beyond the base 35% is billed on a per month, per terabyte basis. This ability enables you to grow or shrink usage, and pay for the configured capacity only.

IBM FlashSystem utility models are provided for customers who can benefit from a variable capacity system, where billing is based on only provisioned space. The hardware is leased through IBM Global Finance on a three-year lease, which entitles the customer to use up to 35% of the total system capacity at no extra 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 vstorage 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, see this IBM Support web page.

1.3 Why FlashCore matters

Solid-state storage is widely used in data centers and 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 or 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 created to ensure that FlashCore Modules provide the density, performance, and longevity that is 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 and use four I/O groups.

The FS9100 also allows for clustering with the IBM Storwize V7000 with a maximum of four enclosures total. Consider the following guidelines:

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

Note: At the time of this 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's AIX® - LVM).
1.5.1 FlashSystem V9000 flash enclosure repurposed

Plans are being developed for the V9000 flash enclosures to repurpose as an external flash enclosure that is recognized by the 9100 as a licensed storage that requires no extra 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 that aim to replace enterprise storage arrays but consistently fail to deliver the breadth of data lifecycle, storage services, or the scalability that is delivered by incumbent solutions. Alternatively, hybrid arrays that are loaded with storage services consistently lack the low latency and performance scalability that is 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 functions 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, which provides flexibility and extends functionality to the virtualized external storage capacity.

1.6.1 Advanced functions for data reduction

The IBM FlashSystem FS9100 uses 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 that are used with the FS9100, the IBM Real-time Compression™ within the IBM FS9100 addresses this requirement of storage data reduction. This feature is handled without sacrificing performance by using dedicated compression acceleration hardware. It does so by implementing a purpose-built technology that is called Real-time Compression that uses 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, which is also known as the logical unit number (LUN), is created and a thin provisioned volume is allocated, data is compressed in real time as it is stored in the VDisk.
Data Reduction Pools
Data Reduction Pools (DRP) represent a significant enhancement to the storage pool concept. 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 became 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 new data chunks are written.

If the new chunks signature matches a signature, the new chunk is replaced with a small reference that points to the stored chunk. The same byte pattern can occur many times, which result 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 where 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 the following different modes:

- Metro Mirror
- Global Mirror
- Global Mirror with Change Volumes
Remote replication can be implemented by using 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 feature 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 storage assets, which reduces costs. Because these functions are integrated into the IBM FlashSystem 9100, they can operate smoothly together, which reduces 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 are 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, by using host multipathing driver that is 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.
IBM FlashSystem 9100 architecture

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

This chapter includes following topics:

- 2.1, “FlashSystem 9100 hardware components” on page 12
- 2.2, “IBM FS9100 Control Enclosure” on page 13
- 2.3, “FlashCore Module and NVMe drives” on page 16
- 2.4, “NVMe and adapter support” on page 17
- 2.5, “Software features and licensing” on page 18
- 2.6, “Data protection on IBM FS9100” on page 20
2.1 FlashSystem 9100 hardware components

Each IBM FlashSystem 9100 consists of a control enclosure and IBM FlashCore module drives. The control enclosure is the storage server that runs 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).

![FlashSystem 9100](image)

Figure 2-1  FlashSystem 9100

The IBM FlashSystem FS9100 includes the following core components:

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

IBM 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. IBM FS9100 can be configured with up to 1.5 TB of cache.

Figure 2-2 shows the internal architecture.

![Internal architecture diagram](image)

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

Figure 2-3 shows the rear view of the enclosure.

![Enclosure rear view](image)

As shown in Figure 2-3, the IBM FS9100 enclosure consists of redundant power supply units, node canisters, and fan modules to provide redundancy and high availability.
Figure 2-4 shows the internal hardware components of a node canister. To the left is the front of the canister where fan modules and battery backup are installed, followed by two Skylake CPUs, memory DIMM slots, and PCIe risers for adapters on the right.

2.2.1 Model 9110 Control Enclosure AF7

IBM FS9100 model 9110 offers the following features:

- Two 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
- A total of 24 slots for 2.5-inch NVMe flash drives
- 2U, 19-inch rack mount enclosure with AC power supplies
- One Boot drive

2.2.2 Model 9150 Control Enclosure AF9

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

- Two 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
- A total of 24 slots for 2.5-inch NVMe flash drives
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 by using the SAS adapter.

2.2.4 Model AFF

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

2.2.5 Model AF9

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

2.2.6 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 that is used beyond the base 35% is billed on a per month, per terabyte basis. This feature enables you to grow or shrink usage, and pay for the configured capacity only.

IBM FlashSystem utility models are provided for customers who can benefit from a variable capacity system, where billing is based on provisioned space only. The hardware is leased through IBM Global Finance on a three-year lease, which entitles the customer to use up to 35% of the total system capacity at no extra 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.

**Total system capacity of 115 TB example**

A customer has a 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, no extra billing is needed.

The system monitors daily provisioned capacity and averages 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 calculates the overage as listed in Table 2-1, rounding to the nearest terabyte.

Table 2-1  Billing calculations that are based on customer usage

<table>
<thead>
<tr>
<th>Average daily</th>
<th>Base</th>
<th>Overage</th>
<th>To be billed</th>
</tr>
</thead>
<tbody>
<tr>
<td>45 TB</td>
<td>40.25 TB</td>
<td>4.75 TB</td>
<td>5 TB</td>
</tr>
<tr>
<td>42.5 TB</td>
<td>40.25 TB</td>
<td>2.25 TB</td>
<td>2 TB</td>
</tr>
<tr>
<td>50 TB</td>
<td>40.25 TB</td>
<td>9.75 TB</td>
<td>10 TB</td>
</tr>
</tbody>
</table>

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

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

The feature codes that are associated with the UF7 and UF8 utility model billing are listed in Table 2-2.

Table 2-2  9100 UF7 and UF8 utility model billing feature codes

<table>
<thead>
<tr>
<th>Feature code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td># AE00</td>
<td>Variable Usage 1 TB per month</td>
</tr>
<tr>
<td># AE01</td>
<td>Variable Usage 10 TB per month</td>
</tr>
<tr>
<td># AE02</td>
<td>Variable Usage 100 TB per month</td>
</tr>
</tbody>
</table>

These features are used to purchase the variable capacity that is used in the utility models. The features (feature code AE00, AE01, and AE02) provide TBs of capacity beyond the base subscription on the system. Usage is based on the average capacity that is used, per month. The total of the prior three months’ usage is 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 that uses 64-layer TLC flash memory and an Everspin MRAM cache into a U.2 form factor.
IBM FCMs (NVMe) are designed for high parallelism and optimized for 3DTLC 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 FIPS 140-2 complaint.

carry the IBM patented Variable Stripe RAID™ at the FCM level and use DRAID to protect data at system level. VSR and DRAID together optimize 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 that are sourced from Samsung and Toshiba and available in the following capacity variations:

- NVMe 1.92 TB
- 3.84 TB
- 7.68 TB
- 15.36 TB

### 2.4 NVMe and adapter support

NVMe is a NUMA optimized, high-performance, and highly scalable storage protocol that is designed to access non-volatile storage media by using host PCIe bus. NVMe uses low latency, available parallelism, and reduces I/O overhead.

NVMe supports multiple IO queues up to 64 K queues and each queue can support up to 64 K entries. Older SAS and SATA support single queue with only 254 and 32 entries and use 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 that is 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 over a network, such as Ethernet, Fibre Channel (FC), or InfiniBand.

### 2.4.1 Support for adapters, host platforms, and switches

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

- **Adapters:**
  - Fibre Channel 4x16Gb
  - iSCSI 8x10Gb
  - Ethernet 2x1Gb System management
  - iSER over RoCE with 2x25G Mellanox ConnectX4-LX
  - iSER over iWARP with 2X25G Chelsio T6 adapters
  - SAS expansion 2x12Gb

- **Host platforms:**
  - RHEL 7.4
  - CentOS 7.4
  - ESX 6.7
2.5 Software features and licensing

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

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

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

2.5.1 IBM Spectrum Virtualize for IBM FlashSystem 9100

IBM FS9100 uses IBM Spectrum Virtualize™ software that combines the following software-defined functions 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 more information about IBM FlashSystem 9100 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 IBM FlashSystem 9100

IBM FS9100 Multi-Cloud starter software along with 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 that is included with IBM FlashSystem 9100 control enclosures enables the development of 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 that are designed to support today’s data driven multi-cloud architectures. These NVMe-ready, cloud-enabled software solutions are validated according to a set of multi-cloud blueprints. These solutions also enable modernizing infrastructure by expanding IBM FlashSystem 9100 to be used for multi-cloud architectures that include data protection, business continuity, and data reuse.

The following solutions are available:

- IBM FlashSystem 9100 Multi-Cloud solution for data reuse, protection, and efficiency
  
  This solution consists of IBM Spectrum Protect Plus and IBM Spectrum Copy Data Management. It 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 consists of IBM Spectrum Virtualize for Public Cloud and IBM Spectrum Copy Data Management. By using IBM Spectrum Virtualize for Public Cloud, data can be copied by 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 that is managed by IBM Spectrum Virtualize for Public Cloud in IBM Cloud.

- IBM FlashSystem 9100 Solution for Private Cloud Flexibility and Data Protection
  
  This solution consists 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 that need attention. 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.

  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 IBM 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 IBM FS9100

Data protection from NAND chip and controller failures are managed by using two IBM technologies: Variable Stripe RAID and DRAID. VSR protects failures at IBM FlashCore modules chip level and DRAID protects data from failure of 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 need to replace an entire flash module when a single chip or plane fails. This feature, in turn, expands the life and endurance of flash modules and considerably reduces maintenance events throughout the life of the system.

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

2.6.2 DRAID

Distributed RAID functionality is managed by Spectrum Virtualize, which enables a storage array to distribute RAID5 or RAID6 to a largest set of drives. For example, if eight drives were used on traditional RAID5, the data was striped across seven and the parity was on 8. DRAID enhanced this method by specifying the stripe width and the number of drives separately and as a result still has seven data stripes that are protected by a parity stripe but the eight 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. This ability increases the number of reads and 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 that are written to a single drive.

**DRAID on IBM FS9100**

DRAID6 is recommended for IBM FS9100 and is only allowed option from GUI. DRAID5 is configurable by using CLI only. DRAID6 creates spare space across all NVMe SSDs or FCMs on the array. During failure, the array rebuilds data by using the spare space faster than traditional 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 remaining drives, which increases the capacity threshold, as shown in Figure 2-7.

![Figure 2-7 Physical capacity threshold](image)

**DRAID copyback**

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

![Figure 2-8 DRAID copyback](image)
Data reduction and tools

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

This chapter describes data reduction and the tools that are available.

This chapter covers the following topics:

► 3.1, “Compression and deduplication techniques” on page 24
► 3.2, “Data Reduction Pools inside the IBM FS9100” on page 29
► 3.3, “Comparing RACE to Data Reduction Pools” on page 34
► 3.4, "Data Reduction Pools and unmap" on page 36
► 3.5, "Data Reduction Pools with Easy Tier” on page 37
► 3.6, “Garbage collection” on page 37
► 3.7, “Data Reduction Pools with deduplication” on page 38
► 3.8, “Estimating data reduction by using various tools” on page 38
► 3.9, “When to use Flash Core Modules or Data Reduction Pools” on page 44
► 3.10, “General guidelines for performance, capacity, and availability options” on page 45
► 3.10.3, “Availability considerations when configuring the IBM FS9100” on page 54
3.1 Compression and deduplication techniques

With massive advances in hardware (for example, CPU speeds, cores, and RAM), we now can easily use many methods to reduce the footprint of data that is being stored with minimal performance tradeoffs. Because all of the processes are not apparent to the host and applications and ensure the complete integrity of the data and metadata of that I/O stream, we discuss only lossless of reduction items. Therefore, all of the data can, and is, fully decompressed to its original, and full, uncompressed state whenever the Host, VM, or Cluster requests it from the IBM FlashSystem 9100 array.

Although other types of compression are available, they are considered lossy because they 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. Although the resulting data is serviceable, it is reduced in size and quality. Two examples are how a professional compact disc of a song sounds versus an MP3 version of the same song on the same sound system. The same can be said for watching a movie in a commercial digital theater versus watching the same movie from an MPEG2 or MPEG4 or similar lossy compressed file type.

These differences are critical because it is important for modern applications, such as SQL, IBM Db2®, or IBM WebSphere®, 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 encryption of its data before it sends it to the IBM array. However, the internal compression and encryption drastically reduces the compression and deduplication rates the array can perform because the data is 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 was pre-compressed or encrypted, and stores and retrieves the data as it was presented without any further data reduction.

The benefits of data reduction and encryption are best realized solely at the array level. It ensures that the host or VM is operating at peak CPU application performance, instead of using 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 is how many Db2 volumes and instances across several departments and Test, Development, and build cycles can be easily deduplicated by using the same FlashSystem FS9100 array. The array easily recognizes all of those similar patterns and then stores only the delta or unique data items.

In summary, many methods are available to accomplish data reduction. This chapter examines the key concepts behind compression and deduplication methods that are used by the IBM FlashSystem 9100 array.

**Note:** The order of operations for the I/O flow is important. If enabled for each stage, individually for every host write, deduplication occurs first, then compression, then encryption.
At the time of this writing, compression is available in several methods: by using inline hardware chips inside specific media, such as the IBM FlashCore Modules (FCM), and by using the FS9100 onboard motherboard. Compression can be turned on for volumes in both traditional pools, and the Data Reduction Pool (DRP) pool type.

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

**Important:** On IBM FS9100, you want to use fully allocated, DRPs with compression and no deduplication. DRPs with compression and deduplication also can be used.

### 3.1.1 Deduplication items

In this section, we describe deduplication and the techniques that it uses.

**Pattern matching and removal**

This first layer of data reduction comes from pattern matching.

*Pattern matching mechanisms* match incoming host writes with a pre configured 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 3-1.

![Pattern matching and removal](image)

*Figure 3-1  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 (the green rectangle in Figure 3-1) 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 3-2, 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 3-2 shows that only the pointers to the data are stored in the system.

Each color represents unique data:

- Written by user:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
```

- Actually written without deduplication:

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
```

- Actually written with deduplication: 25% (4:1):

```
1 2 3 4 5 6 7 8 9
```

Figure 3-2  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 3-3. Notice that the green block for deduplication is larger than the green block for pattern matching. This result occurs because more metadata must be stored for deduplication than for pure pattern matching.

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 applies to data blocks of 8 KB or larger only.
Data deduplication is performed in sequences. 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 3-4). The owning segment of a referenced hash is indicated by the corresponding background color.

Figure 3-4  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 shown in Figure 3-5, the data deduplication of the 8 KB blocks is performed over a 4 KB alignment, which increases the probability of finding a match. This process results 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 3-5  Data deduplication with 4 KB alignment detection
Maintaining integrity

Integrity of user data is a major aspect of the system design. Several data integrity concerns must be considered when deduplication is involved:

- 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 any references to this (current) data remains anywhere in the system.

The first measure of protection in the 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 written to the storage after data reduction, and covers data and metadata.

IBM 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. In other referencing methods, such as using ID number or position, a risk exists of reading incorrect data if a problem occurs in the management of the ID or position. The use of 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 can survive 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 (see Figure 3-6) for more data reduction.

![Figure 3-6 Data flow that uses deduplication and compression](image)
The data reduction process flow is shown in Figure 3-7.

![Figure 3-7 Data reduction process flow](image)

### 3.2 Data Reduction Pools inside the IBM FS9100

DRPs represent a significant enhancement to the storage pool concept because the virtualization layer is primarily a simple layer that runs the task of lookups between virtual and physical extents. With the introduction of data reduction technology, it became more of a requirement to have an uncomplicated way to stay thin.

**Important:** On IBM FS9100, you want to use fully allocated, DRPs with compression and no deduplication, or DRPs with compression and deduplication.
DRPs increase infrastructure capacity usage by using 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 that contain deleted data. For the first time, they also enable 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, which potentially extends the benefits of compression to all data in a system.

Traditional storage pools have a fixed allocation unit of an extent, and that itself is not changing with DRPs. However, features, such as thin provisioning and Real-time Compression (RtC), use smaller allocation units and manage this allocation with their own metadata structures. These features are described as Binary Trees or Log Structured Arrays (LSA).

To stay thin, you must 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 reclamation also must be done at the smaller allocation unit size (KB) per extents.

Figure 3-8 shows the DRP mirroring structure.

Figure 3-8   New DRP Volume Mirroring Structure

Note: Use volume mirroring to clone data to a new DRP as 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 performance is the result of the new compression implementation because it provides better load balancing and consistent performance. This feature is also the second best performer to fully allocated volumes, followed by thin, compressed, and deduplication volumes regarding storage efficiency.

Figure 3-9 shows the types of volumes in the DRP pools.

![Figure 3-9 Volume types](image)

The following main characteristics make up the IBM DRP 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

At its core, a data reduction pool uses an LSA to allocate capacity. Therefore, the volume 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 occur at the upper cache layer to the host. Reads must go through the lower cache layer. The heart of the new DRP functionality is in the new implementation of the Log Structured Array. This array 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 that are independent of size and logical location. Each logical block device includes a range of Logical Block Address (LBAs), starting from 0 and ending with the block address that fills the capacity. 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 LBA 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 that is used must be marked as “free”. UNMAP functions can also request that you free no longer needed capacity. Compression overwrites can result in different a capacity that is used. Deduplication might find new duplicates when data is rewritten.

Figure 3-10 shows the Spectrum Virtualize I/O stack structure.

Figure 3-10  DRPs and LSA in the Spectrum Virtualize I/O stack
3.2.2 Data Reduction Pool components

As shown in Figure 3-11, the user sees a sample of four volumes in a DRP. Internally, four directory volumes are available, one customer data volume (per I/O Group), and one Journal Volume (per I/O Group).

Figure 3-11  Both the front-end and back-end view of DRP

Each Internal volume type features specific I/O patterns with its own percentage that is used of the total capacity of the pool, as listed in Table 3-1.

Table 3-1  I/O Patterns per Internal Volumes

<table>
<thead>
<tr>
<th>Customer data volumes</th>
<th>Directory volumes</th>
<th>Journal volumes</th>
<th>Reverse lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td>98% of pool capacity</td>
<td>1% of pool capacity</td>
<td>Less than 1% of pool capacity</td>
<td>Less than 1% of pool capacity</td>
</tr>
<tr>
<td>Large sequential write pattern and short random read pattern</td>
<td>Short 4 KB random read and write pattern</td>
<td>Large sequential write I/O and only read for recovery scenarios (T3, and so on)</td>
<td>Short, semi-random read/write pattern</td>
</tr>
</tbody>
</table>

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. The 8 KB allocation was established for the following key reasons:

- RACE write of 32 KB can be catered.
- 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 that is served by lower cache, performance is much more consistent.
Figure 3-12 shows the DRP Compression I/O Amplification.

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

Figure 3-12  I/O Amplification of space allocated (assumes 50% Compression rate)

Note: Writes to allocated space drives the need for Garbage Collection (GC). The cost of GC depends on the amount of valid data in the extent that was not over-written.

3.3 Comparing RACE to Data Reduction Pools

RACE used a variable input with a fixed output of the inbound data stream, all of which was inline without any post process. However, RACE intermittently had to wait or pause to see whether more I/O is coming for a particular volume (see Figure 3-13). The RACE minimum block size to read from backend is 32 KB.

Figure 3-13  RACE compression I/O stack

One of the benefits of RACE, is that it enabled at least 4 - 8 times more data through decompression hardware than DRP for a true random workload. DRP Compression uses fixed input with a variable output, or the opposite of RACE.
The DRP maximum block size to read from the backend is 8 KB (typically 4 KB or less though), as shown in Figure 3-14.

![Diagram showing DRP compression IO stack]

Figure 3-14  DRP compression IO stack

With the use of 8 KB input sizes, a small loss occurs in compression ratio, but a gain is realized in lower latency when all workload is put into the same predictable small block size. Host I/O that is put in these small grain block sizes in DRP allows for fine grained allocation of block data, frees back unused capacity at a fine grain, gives consistent, predictable performance, and optimizes performance for Flash storage.

DRP differs with RACE in the following key aspects:

- **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 RtC compression and compression for IP replication
  - New DRP compression achieves up to 4.8 GBps per node (compression card limit)

### 3.3.1 Benefits of Data Reduction Pools

DRPs feature the following advantages:

- 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, which enables its use with a wider range of data types
- Ability to release and reuse storage in response to server needs, which reduces overall required storage
- 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; that is, mirrored non-volatile metadata means significantly improved failover and failback response times because of no revalidation of metadata
- No limit on the number of compressed volumes
- Space reclamation (unmap available (for more information, see Chapter 4, “Planning” on page 57)
- Designed for de-duplication
- Smaller 8-k chunks means less compression bandwidth for small I/Os
- Metadata and user data are separated, which provides a better use of cache prefetch and destage
- On average, 1.8x I/O amplification on host I/O, which is much more predictable latency
- uses maximum compression bandwidth
- Comprestimator support

DRP disk limitations are listed in Table 3-2.

Table 3-2  DRP Disk Limitations

<table>
<thead>
<tr>
<th>Extent Size</th>
<th>Volume size</th>
<th>4 IO groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 GB</td>
<td>128 TB</td>
<td>512 TB</td>
</tr>
<tr>
<td>2 GB</td>
<td>256 TB</td>
<td>1 PB</td>
</tr>
<tr>
<td>4 GB</td>
<td>512 TB</td>
<td>2 PB</td>
</tr>
<tr>
<td>8 GB</td>
<td>1 PB</td>
<td>4 PB</td>
</tr>
</tbody>
</table>

### 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 the capacity that is allocated within that unmap. Similarly, deleting a volume at the DRP level frees all 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. RACE used a form of LSA since its introduction in 2011, which means that a normal garbage collection must be done regularly. An LSA always appends new writes to the end of the allocated space (even if data exists) and the write is an over-write. 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.

Consider the following points in regards this process:

- Writes to a DRP volume are always sequential; therefore, we can build all of the 8 KB chunks into a larger 256 KB chunk and destage the writes from cache as full stripe writes or as large as a 256 KB sequential stream of smaller writes.
- This result gives the best performance in terms of RAID on backend systems and 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 over-written.

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 process is done so that Easy Tier operates correctly for read data and 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 made to a new extent, so the previous heat was lost. Now, we can maintain the heat over time and ensure that frequently rewritten data is grouped. This process also aids the garbage collection process where it is likely that large contiguous areas end up garbage collected together.

3.6 Garbage collection

DRP features built-in services to enable garbage collection of unused blocks. Therefore, many of the smaller unmaps end up allowing a much larger chunk (extent) to be freed back to the pool. If the storage behind Virtualize supports unmap, we pass an unmap command to the backend storage (again, equally important with today’s Flash backend systems), especially so when they implement some form of data reduction.

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

The reverse lookup metadata volumes tracks the extent usage, or more importantly, the holes that were created by over-writes or unmaps. GC looks for extents with the most unused space.

When an entire extent’s data is moved elsewhere, it is marked as free and returned to the set of unused extents into that pool, or can be reused for new written data.
3.7 Data Reduction Pools with deduplication

Deduplication can be configured with thin-provisioned and compressed volumes in DRPs 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 new data chunks are written.

If the new chunks signature matches an existing signature, the new chunk is replaced with a small reference that points to the stored chunk. The same byte pattern can occur many times, which results in the amount of data that must be stored being greatly reduced.

Duplicate matches are found by using SHA1 hashes that are created for each 8 KB align region of client data to a deduplicated copy. The matches are detected when the data is written. For DRPs, deduplication data can work in two separate ways: It can be grouped into 256 KB blocks and written to storage, or 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 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 three versions of data. I/O performance takes precedence over finding duplicate copies of data. Host I/Os that are smaller than 8 KiB do not attempt to find duplicates.

3.7.1 Typical case examples of DRP

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

3.8 Estimating data reduction by using various tools

IBM provides several options to ensure that accurate decisions can be made about the use of any level of data reduction. In the following sections, we examine Compressimator 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 affect production performance because they are looking for various patterns and calculating the reduction savings.

3.8.1 Compressimator utility

Compressimator is an integrated GUI and CLI host-based utility that estimates the space savings that are achieved when compressed volumes are used for block devices. This utility provides a quick and easy view of showing the benefits of the use of compression. The utility performs read-only operations and has no effect on the data that is 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 added to the data reduction pools.
When the CLI is used, use the `analyzevdisk` command that is shown in Example 3-1 to run volume analysis against a single volume.

**Example 3-1  analyzevdisk command**

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

`analyzevdisk` command

**Syntax**

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

For more details type 'help analyzevdisk'.

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

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

**Example 3-2  analyzevdiskbysystem**

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

`analyzevdiskbysystem` command

**Syntax**

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

For more details type 'help analyzevdiskbysystem'.

```
IBM_Storwize:redbook-mcr-fab1-cluster-33:superuser>svctask analyzevdiskbysystem voll
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 `lsvdiskanalysis` command, as shown in Example 3-3.

**Example 3-3  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>
```
The utility can be used from the IBM Spectrum Virtualize GUI.

How to start a complete system analysis on compression estimates is shown in Figure 3-15.

![Figure 3-15 Estimate compression savings](image)

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

A window prompt appears 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 3-15 on page 40.

### 3.8.2 Comprestimator using the host-based CLI utility

If you want to estimate the compression savings of a volume that is **outside** of the FlashSystem 9100 or on another array, the IBM Comprestimator Utility can be installed on a host that is connected to the device that must be analyzed. For more information about and the latest version of this utility, see this [IBM Support web page](https://www.ibm.com/support/pages/).

Consider the following recommended best practices for the use of Comprestimator:

- Run the Comprestimator utility before implementing an IBM Spectrum Virtualize solution and the DRP 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 process ensures greater accuracy when sizing your environment for compression and data reduction pools.
3.8.3 Using Data Reduction Estimation Tool

DRET is a CLI-operated execution file that runs from the host to analyze a specific block device. It provides a report of what it expects the deduplication savings to be from data that is written to the disk. No other adjustments or requirements must be made 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 a volume can be used. Also, it can complete these tasks within a reasonable amount of time, as listed in Table 3-3.

<table>
<thead>
<tr>
<th>Volume size</th>
<th>Time taken (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 GB</td>
<td>1</td>
</tr>
<tr>
<td>35 GB</td>
<td>1</td>
</tr>
<tr>
<td>100 GB</td>
<td>41</td>
</tr>
<tr>
<td>1 TB</td>
<td>32</td>
</tr>
</tbody>
</table>

When DRET is used to analyze a block device that is 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 to make it 0% used. When scanning the block device that is used for storing the file system in this example, DRET accesses the data that belongs to the files that were 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 method increases the accuracy level and reduces the risk of analyzing old data that is already deleted, but might still have traces on the device.

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 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.
As shown in Figure 3-16, DRET lists compression and deduplication savings per volume. Therefore, in many ways, it can save time to use DRET against running the Comprestimator tool alone.

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 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 are scanned, the results must be merged to get overall reduction information, as shown in the example in Figure 3-17.

![Data Reduction Estimator Tool](image1)

Figure 3-17  DRET example

Figure 3-17 shows the individual runs, which can be scripted to run as a batch job. After each volume is analyzed, they can be merged to give a complete analysis, as shown in Figure 3-18.

![Data Reduction Estimator Tool](image2)

Figure 3-18  DRE Tool Merge Example

For more information about and the latest version of this utility, see this IBM Support web page.
3.9 When to use Flash Core Modules or Data Reduction Pools

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

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

DRP 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 extra latencies.

DRPs 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. DRP uses various technologies that add some small latency to the volumes on which it is enabled. We describe more examples in the following sections.

3.9.1 Flash Core Modules advantages

FCMs feature the following 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 that enables improved read latency on highly compressed data.
- Four-plane programming to lower the overall power during write operations.
- Hardware compression uses dedicated chips that are running proven IBM enhanced GZIP compression routines alongside ECC that are used in IBM’s Z Mainframe offerings for many decades.

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

3.9.2 Data Reduction Pool advantages

DRPs feature 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 because of the compression methods.

Note: DRP volumes should be run with at least compression enabled because no performance tradeoffs exist with this reduction. Only when deduplication is also enabled do any other metadata exist with Garbage Collection and the LSA operations.
If you want to use DRP with a thin-provisioned (overallocated), back-end array, you must 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 is divided into 8 KB equal chunks, plus each 8 KB chunk is compressed to 4 KB or less, which is the optimal block size for the use of Flash performance. This DRP compression implementation can lead up to 4x throughput for compressed workload with consistent performance.

No performance penalty occurs for writing non-compressible data. For application workloads with a 2:1 or higher compression ratio, a significant capacity saving is realized with no performance overhead. This benefit reduces planning work and simplifies capacity savings for any storage solution.

DRP deduplication with compression provides the best storage efficiency. This combination deduplicates and then compresses the data, which reduces the storage capacity usage. It is recommended to use this option when the data pattern is compressible and has a high duplication ratio as identified by the DRET tool. For more information, see 3.8.3, “Using Data Reduction Estimation Tool” on page 41.

3.10 General guidelines for performance, capacity, and availability options

In this section, we describe performance, capacity, and availability options. We also discuss data reduction choices.

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 by using fully allocated volumes and FCM compression, and the capacity workloads by using Data Reduced volumes.

If your workload is unknown, the best approach is to assume that everything is a performance workload and use fully allocated volumes with FCM compression. As an alternative, use Disk Magic to understand the performance of a configuration with DRP and determine whether it meets with expectations.

Port bandwidth

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

A single Fibre Channel port can deliver 80 k to 100 k IOPS with a 4-k block size an FC card in each canister with eight ports can deliver up to 800 k IOPS. An IBM FlashSystem 9100 can support over 1.1 M 4 k read miss IOPS.

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

If you want to drive more than 600 k IOPS, use two Fibre Channel cards per container.
How much cache do I need?
A 256 GB per system (128 GB base plus a 128 GB upgrade) is a good starting point. If you are using DRP or making heavy use of copy services, add 128 GB per system.

As your capacity increases (especially with the 19.2 TB FCM devices), add 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 are 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 approximately 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, by using Logical Volume Manager).

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

Multiple Data Reduction Pools
A single DRP is backed by a single DRAID6 array optimizes the amount of storage available and allows ease of management. However, the tradeoff is that it can limit performance potential.

Two DRPs that are backed by two DRAID6 arrays require twice the amount of parity and spare capacity as a single DRAID6 array. However, workloads can be shared across two pools and share all available resources and increase 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 or ports. Configure a balanced system with performance and capacity targeted volumes, and spread the resource by using multiple volumes and combining them at the host.

If you are running many workloads, a single volume might be good enough for each workload. If the balance of the system is leaning towards DRP, consider two DRPs.

3.10.2 Capacity
Before we describe capacity planning, we define the terminology that we use to establish a common understanding.
Capacity terminology
IBM applies the following definitions 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, 50 TiB available is a usable capacity of 100 TiB.

- **Used capacity**
  The amount of usable capacity that is taken up by data in a system, pool, array, or MDisk after data reduction techniques are 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 that are 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 was used to store written data in a pool or system before data reduction is applied.

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

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

- **Data reduction**
  The techniques that are 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 saved capacity 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 saved capacity is the difference between the provisioned capacity minus the written capacity.

- **Over provisioned**
  A storage system or pool where more provisioned capacity is available than 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 that is allowed in a pool or system.

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

Industry-standard NVMe drives do not have hardware compression and are available in 1.92, 3.84, 7.68, and 15.36 TB sizes.

NVMe Flashcore Modules
FCMs compress and encrypt the data by using hardware as it is written to the device at line speed. This feature 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.

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, which means the effective capacity is close to 9.6 TB.

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

DRPs 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 do not compress it. DRPs can be used to reduce the amount of data that is sent to the drives, but the use of DRPs means a lower maximum performance threshold. The effective capacity is determined by the use of DRPs, along with how compressible the workload is and whether the system contains much duplicate data.

NVMe storage frequently asked questions
The following questions often are asked:

- Can I use the FCMs in my IBM FlashSystem 900 or V9000 in the IBM FlashSystem 9100?
  No. These modules use the same technology as the IBM 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 must work harder to manage the free space, which might affect 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. For 9.6 TB, it is 21.99 TB or 2.3:1; for 19.2 TB, it is 43.98 TB or 2.3:1. However, assuming you fill the system to only 85% to maintain the expected performance, you can increase these effective compression ratios by $\left(\frac{1}{0.85}\right)$.

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 that is based on the data that is written and the data reduction that is 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 still is full when it reaches the maximum effective capacity. Any spare data space that is remaining at this point is 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 fills 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 is written. In either case, performance is not affected because the FCM compression is done in hardware.

Why would I use DRP with FCMs?
Predominantly to take advantage of further data reduction savings that can be made by using deduplication.

Should I use FCMs or industry-standard NVMe drives?
Industry-standard NVMe drives start at a smaller capacity point, which allows for 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, but it gives less protection), and must all be the same size. Having mixed drive types and sizes mean that you need to purchase the drives in blocks of six or more and manage them as two independent RAID arrays as opposed to one large one.

What size RAID array should I target?
The GUI selects the correct geometry. For DRAID6, you need 6 - 24 drives, ideally configured as a single RAID array with two parity and one spare. You can define multiple RAID arrays if you want, but at the cost of some capacity.

Can I add drives to the system later?
Yes, you can create another array. We plan to support DRAID expansion in a future release.
Figure 3-19 shows the maximum capacity.

Sizing your system
Complete the following 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 are used (by way of 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, balancing performance, rebuild times, and usable capacity. Fewer devices are fine for smaller capacity systems that do not have a high-performance requirement, but avoid fewer large drives.
Data reduction tooling is shown in Figure 3-20.

Pre-sales tooling is shown in Figure 3-21.

Capacity Planning frequently asked questions
The following questions often are asked:

- What does “Optimized for 16 to 24 devices” mean?
  Data, parity, and spare space must 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 use, 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 exist in the control enclosure only, and SAS drives can exist in SAS expansion enclosures only.
Can I use Easy Tier?
Yes, all NVMe drives are tier 0, and all SAS SSD drives are tier 1. You should be careful if you are tiering between compressing and non-compressing drives to ensure that you have enough physical capacity as data is moved between the tiers.

What are the SAS drive options?
Tier 1 SAS SSDs in 1.92, 3.84, 7.68, 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 would you?

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

What is the maximum capacity?
The maximum capacity is 32 PB, as with other Spectrum Virtualized products. This figure is a total of all virtualized storage.

Can I fill up the system to 100%?
If you fill the system more than 85% full, the system has more work to do to manage the free space, which might affect performance.

How many systems can I cluster together?
Up to four. 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 IBM FlashSystem 9100s together, the total number of drives increases linearly to a maximum of 3040. For more information, see the FlashSystem 9100 Sales Manual.

Why would I choose to use SAS enclosures over clustering more control enclosures?
Clustering scales performance with the extra NVMe storage. To scale capacity within the performance envelope of a single controller then add SAS enclosures.

Can I use expansion enclosures from other Spectrum Virtualize products?
No.

Why does DRET take a long time to run compared to Comprestimator?
DRET must 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 evolved over the years. We are actively looking at how we can streamline this process.
**Data reduction choices**
The following choices are available:

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

- **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 allows for 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 by way of the inline hardware compression in FCM. Be aware that this configuration does not provide for deduplication. Also, no thin provisioning or compression is available when fully allocated volumes with non-compressing NVMe, SAS, or virtualized volumes are used.

**Capacity optimized**
Data reduction volumes provide for maximum data reduction and uses DRP technology. A tradeoff exists and that is maximum performance for a gain in better data reduction. Low response times for all but the most demanding workloads occur and a 5:1 or more compression ratio for highly compressible workloads by 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 only FCMs.

Fully Allocated and data reduction volumes can exist in the same DRP, which enables the management all of the storage from a single pool. You might need to vary each volume type based on the characteristics of the workload.

**Combining performance and capacity**
Use performance optimized 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 capacity optimized where the workload can benefit from deduplication; for example, VDI, DevOps (production, pre-production, QA, and so on), and environments where many copies of data exist. 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 represent most of your IO, and assume data reduction by using inline hardware compression.
You also must identify capacity workloads that can maximize capacity with modest I/O, and assume data reduction with deduplication and compression.

Identifying the workload demands allows 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; therefore, careful monitoring is required.

**Evaluating workload by using Disk Magic**

In addition to the use of test volumes and observing actual performance for the application, IBM has a tool available that is used for specifically for modeling performance called Disk Magic.

Disk Magic for IBM is a performance analysis and hardware configuration planning tool for IBM storage disk subsystems that runs on MS Windows (XP or later) only. 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 such 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 also provides in-depth environment analysis, and is an excellent tool to estimate the performance of a system that is running DRPs.

For more information about Disk Magic, and the latest version, see this website (log in required).

### 3.10.3 Availability considerations when configuring the IBM FS9100

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

**Availability considerations when configuring storage pools**

Although the IBM FS9100 provides many advantages through consolidation of storage, it is important to understand the implications 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, the availability of the configuration is traded for little or no performance gain in many cases.

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 a Storwize FS9100 clustered environment, create storage pools with IOgrp or Control Enclosure affinity. In this configuration, use arrays or MDisks that are supplied by the internal storage that is directly connected to one IOgrps SAS chain. This configuration avoids having the availability of the storage pool be dependent on the availability of all IOgrps in the cluster.

- When configuring storage pools from external storage, it is recommended that each storage pool contain only MDisks from a single storage subsystem. An exception exists when implementing IBM System Storage Easy Tier in which case 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 few large pools include a large failure boundary if the pools is taken offline because of a problem with one of the MDisks or its backing storage array. Too many small pools leads to performance issues. It is a good practice to keep pools to under 250 TB and the total number of pools eight or less.

### Availability considerations for host volume assignments

Reducing the failure domain for back-end storage is only part of what must 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, 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 IBM FS9100 cluster, the failure domain for that host is expanded as the availability of that host becomes dependent upon the availability of all IOgrps and Storage Pools to which its volumes are mapped.

**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 a Storwize FS9100 clustered environment, allocate or map all volumes for a specific host to a single IOgrp.

- In a Storwize FS9100 clustered environment, allocate or map all volumes for a specific host to a single backend storage pool.
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 the host attachment and virtualized storage expansion sides.

This chapter also describes all the environmental requirements that you must consider and includes the following topics:

- 4.1, “FlashSystem 9100” on page 58
- 4.2, “General planning introduction” on page 59
- 4.3, “Physical planning” on page 62
- 4.4, "Logical planning" on page 76
- 4.5, “IBM Storage Insights” on page 92
- 4.6, “IBM FlashSystem 9100 system configuration” on page 96
- 4.7, “Licensing and features” on page 104
- 4.8, “IBM FlashSystem 9100 configuration backup procedure” on page 110
- 4.9, “Multi-Cloud offerings and solutions” on page 111

Note: 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. In the previous product (the IBM FlashSystem V9000 AC2 and AC3 and the AE2 and AE3 combinations), the storage enclosures were separate 2U units and managed by the AC2 or AC3 control enclosures. This configuration makes the V9000 clusters 6U high or more.

**Note:** The IBM FlashSystem 9100 term *node canisters* are also sometimes referred to as *controllers* or *nodes*. These terms are 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](image-url)
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, which reduces the amount of rack space that is needed per system.

![Diagram](image)

**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, pre-installation 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.

![Image](image)

**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 feature is known as the scale-up, scale-out capability. Consider the following points:

- If extra capacity is needed (that is, 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 (that is, scale-out), by adding up to four control enclosures in total to the solution to form a cluster. This addition increases the capacity and the performance alike.
- The total capacity can be further extended by the addition of SAS all flash expansion enclosures. This change 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, which consists 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 more information about scalability and multiple control enclosures, see Chapter 5, “Scalability” on page 113.

**Requirement:** A pre-sale Technical Delivery Assessment (TDA) must be conducted to ensure that the configuration is correct and the solution that is planned for is valid. A preinstall 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).

Complete the following 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; that is, input/output (I/O) operations per second (IOPS) and throughput in megabytes per second (MBps).

2. Collect and document the following storage requirements and capacities:
   - Total external storage that is 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 of the internal connections (if this system is multi-enclosure) 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 more expansion storage controllers that are 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 need in each expansion enclosure. For more information about planning for the expansion enclosures, see 4.3.5, “SAS expansion enclosures” on page 74.

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 the IBM FlashSystem 9100 control enclosures and any external storage, if installed, and data transfers. Connecting this network across inter-switch links (ISL) is not supported.

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

   For example, an IBM FlashSystem 9100 cluster that is composed of three control enclosures needs 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 used by the International Technical Support Organization (ITSO) Redbooks publication 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 that is connected, more expansions or control enclosures being added, and the focus for their use. A need might also exist for defining pools for use by data migration requirements or Easy Tier. For more information about Easy Tier, see in 4.6.2, “IBM Easy Tier” on page 102.
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 the following types:
   - Physical planning
   - Logical planning

   The following sections describe these planning types.

   **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 another 2U of space for the AFF or 5U of space for the A9F.

**Important:** IBM FlashSystem 9100 is approximately 850 mm (33.46 inches) deep and 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 more information, see IBM Knowledge Center.

For non-IBM racks, the service clearance at the rear **must** be at least 915 mm (36 inches) to allow for installation and concurrent maintenance of the node canisters.

When the IBM FlashSystem 9100 solution is developed 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, its SAN switches, and an Ethernet switch for management connections. Depending on the number of extra expansion enclosures, you might need to plan for extra racks.
Figure 4-4 shows a partially configured solution of two IBM FlashSystem 9100 control enclosures plus two other scale-out A9F expansion enclosures and two AFF expansion enclosures in a 42U rack.

4.3.1 IBM FlashSystem 9100 control enclosures

Each IBM FlashSystem 9100 control enclosure can support up to six PCIe expansion I/O cards, as listed in Table 4-1, to provide a range of connectivity and capacity expansion options.

<table>
<thead>
<tr>
<th>Number of cards</th>
<th>Ports</th>
<th>Protocol</th>
<th>Possible slots</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 3</td>
<td>4</td>
<td>16 Gb Fibre Channel</td>
<td>1, 2, 3</td>
<td></td>
</tr>
<tr>
<td>0 - 3</td>
<td>2</td>
<td>25 Gb Ethernet (iWarp)</td>
<td>1, 2, 3</td>
<td></td>
</tr>
<tr>
<td>0 - 3</td>
<td>2</td>
<td>25 Gb Ethernet (RoCE)</td>
<td>1, 2, 3</td>
<td></td>
</tr>
</tbody>
</table>
The following types I/O adapter options can be ordered:

- **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 IBM FlashSystem 9100 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 by 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 IBM FlashSystem 9100 control enclosure and are designed to support RDMA with RoCE v2.
  - 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 - 25 GbE (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 IBM FlashSystem 9100 control enclosure and are designed to support RDMA with iWARP.
  - Minimum required: None.

---

<table>
<thead>
<tr>
<th>Number of cards</th>
<th>Ports</th>
<th>Protocol</th>
<th>Possible slots</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 1</td>
<td>2 - See comment</td>
<td>12 Gb SAS Expansion</td>
<td>1, 2, 3</td>
<td>Card is 4-port with only two ports active (ports 1 and 3)</td>
</tr>
</tbody>
</table>

**Note:** This adapter does not support FCoE connectivity. When two of these adapters are installed, clustering with other IBM FlashSystem 9100 systems is not possible.
– 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 4-port 12 Gb SAS expansion enclosure attachment card.
– This feature is used to attach up to 20 expansion enclosures to an IBM 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.

4.3.2 Racking considerations

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 that are installed as is 2U high. Ensure that the space for the entire system is available if more than one IBM FlashSystem 9100 control enclosure or more expansion encloses are to be installed.

Location of IBM FlashSystem 9100 in the rack

Use Table 4-2 on page 66 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>
<thead>
<tr>
<th>Rack unit</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIA 42</td>
<td></td>
</tr>
<tr>
<td>EIA 41</td>
<td></td>
</tr>
<tr>
<td>EIA 40</td>
<td></td>
</tr>
<tr>
<td>EIA 39</td>
<td></td>
</tr>
<tr>
<td>EIA 38</td>
<td></td>
</tr>
<tr>
<td>EIA 37</td>
<td></td>
</tr>
<tr>
<td>EIA 36</td>
<td></td>
</tr>
<tr>
<td>EIA 35</td>
<td></td>
</tr>
<tr>
<td>EIA 34</td>
<td></td>
</tr>
<tr>
<td>EIA 33</td>
<td></td>
</tr>
<tr>
<td>EIA 32</td>
<td></td>
</tr>
<tr>
<td>EIA 31</td>
<td></td>
</tr>
<tr>
<td>EIA 30</td>
<td></td>
</tr>
<tr>
<td>EIA 29</td>
<td></td>
</tr>
<tr>
<td>EIA 28</td>
<td></td>
</tr>
<tr>
<td>EIA 27</td>
<td></td>
</tr>
<tr>
<td>EIA 26</td>
<td></td>
</tr>
<tr>
<td>EIA 25</td>
<td></td>
</tr>
<tr>
<td>EIA 24</td>
<td></td>
</tr>
<tr>
<td>EIA 23</td>
<td></td>
</tr>
<tr>
<td>EIA 22</td>
<td></td>
</tr>
<tr>
<td>EIA 21</td>
<td></td>
</tr>
<tr>
<td>EIA 20</td>
<td></td>
</tr>
<tr>
<td>EIA 19</td>
<td></td>
</tr>
<tr>
<td>EIA 18</td>
<td></td>
</tr>
<tr>
<td>EIA 17</td>
<td></td>
</tr>
<tr>
<td>EIA 16</td>
<td></td>
</tr>
<tr>
<td>EIA 15</td>
<td></td>
</tr>
<tr>
<td>EIA 14</td>
<td></td>
</tr>
<tr>
<td>EIA 13</td>
<td></td>
</tr>
<tr>
<td>EIA 12</td>
<td></td>
</tr>
<tr>
<td>EIA 11</td>
<td></td>
</tr>
<tr>
<td>EIA 10</td>
<td></td>
</tr>
</tbody>
</table>
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 used. A total of two power cords are required to connect each IBM FlashSystem 9100 control enclosure 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.

<table>
<thead>
<tr>
<th>Rack unit</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIA 9</td>
<td></td>
</tr>
<tr>
<td>EIA 8</td>
<td></td>
</tr>
<tr>
<td>EIA 7</td>
<td></td>
</tr>
<tr>
<td>EIA 6</td>
<td></td>
</tr>
<tr>
<td>EIA 5</td>
<td></td>
</tr>
<tr>
<td>EIA 4</td>
<td></td>
</tr>
<tr>
<td>EIA 3</td>
<td></td>
</tr>
<tr>
<td>EIA 2</td>
<td></td>
</tr>
<tr>
<td>EIA 1</td>
<td></td>
</tr>
</tbody>
</table>

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 used. A total of two power cords are required to connect each IBM FlashSystem 9100 AFF expansion enclosure to the rack power.

Figure 4-7 on page 68 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.
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 used. A total of two power cords are required to connect each IBM FlashSystem 9100 A9F expansion enclosure 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.

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 includes future growth plans, plan to allow for the extra control enclosures to be colocated in the same rack with your initial system for ease of planning for the extra interconnects that are required. A maximum configuration of the IBM FlashSystem 9100, with dedicated internal switches for SAN and local area network (LAN) and extra 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. These connections enable the cabinet to be split between two independent power sources for greater availability. When adding IBM FlashSystem 9100 control or expansion enclosures to the solution, continue the same power cabling scheme for each extra enclosure.

You must consider the maximum power rating of the rack; do not exceed it. For more information about requirements, see IBM Knowledge Center.

4.3.4 Network cable connections

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

You can download the latest cable connection tables from the IBM FlashSystem 9100 web page of IBM Knowledge Center by completing 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 download options:
   – Planning worksheets for system connections
   – Planning worksheets for network connections
   – Planning for management and service IP addresses
   – Planning for SAS Expansion enclosures (if installed)

We also included some sample worksheets here to give an overview of what information is required.

PCIe adapters and connections

Figure 4-9 shows the FC port locations, which are identified for all of the possible fiber connections across the two IBM FlashSystem 9100 node canisters.
Create a cable connection table or similar documentation to track all of the connections that are required for setting up the following 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

<table>
<thead>
<tr>
<th>PCIe slot</th>
<th>Adapter types</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fibre Channel or Ethernet or SAS</td>
</tr>
<tr>
<td>2</td>
<td>Fibre Channel or Ethernet or SAS</td>
</tr>
<tr>
<td>3</td>
<td>Fibre Channel or Ethernet or SAS</td>
</tr>
</tbody>
</table>

In the following sections, we provide sample charts for the various network connections.
Fibre Channel ports
Use Table 4-4 to document FC port connections for a single control enclosure.

<table>
<thead>
<tr>
<th>Location</th>
<th>Item</th>
<th>Fibre Channel port 1</th>
<th>Fibre Channel port 2</th>
<th>Fibre Channel port 3</th>
<th>Fibre Channel port 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node canister 1</td>
<td>Switch host</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fibre Channel card 1</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node canister 1</td>
<td>Switch host</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fibre Channel card 2</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node canister 1</td>
<td>Switch host</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fibre Channel card 3</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node canister 2</td>
<td>Switch host</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fibre Channel card 1</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node canister 2</td>
<td>Switch host</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fibre Channel card 2</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node canister 2</td>
<td>Switch host</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fibre Channel card 3</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Ethernet port connections

Support for Ethernet connections is by way of the on-board ports or by adding Ethernet PCIe adapters.

Table 4-5 lists the layout of the on-board Ethernet connections.

Table 4-5   Node canister on-board Ethernet port connections

<table>
<thead>
<tr>
<th>Component</th>
<th>Ethernet port 1</th>
<th>Ethernet port 2</th>
<th>Ethernet port 3</th>
<th>Ethernet port 4</th>
<th>Technician port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Canister 1 (upper)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Speed</td>
<td>10 Gbps or 1 Gbps</td>
<td>10 Gbps or 1 Gbps</td>
<td>10 Gbps or 1 Gbps</td>
<td>10 Gbps or 1 Gbps</td>
<td>1 Gbps only</td>
</tr>
<tr>
<td>Node Canister 2 (lower)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Speed</td>
<td>10 Gbps or 1 Gbps</td>
<td>10 Gbps or 1 Gbps</td>
<td>10 Gbps or 1 Gbps</td>
<td>10 Gbps or 1 Gbps</td>
<td>1 Gbps only</td>
</tr>
</tbody>
</table>

Each node canister also supports up to three optional 2-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 a SAS adapter is required to connect to expansion enclosures, it must be installed in slot 3.

Table 4-6 lists the 25 Gbps Ethernet adapter port connections, speeds, and switch port assignments.

Table 4-6   25 Gbps Ethernet adapter port connections

<table>
<thead>
<tr>
<th>Component</th>
<th>Adapter 1 Ethernet port 1</th>
<th>Adapter 1 Ethernet port 2</th>
<th>Adapter 2 Ethernet port 1</th>
<th>Adapter 2 Ethernet port 2</th>
<th>Adapter 3 Ethernet port 1</th>
<th>Adapter 3 Ethernet port 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Canister 1 (upper)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speed</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
</tr>
<tr>
<td>Node Canister 2 (lower)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Management and service IP addresses

Figure 4-10 shows the locations of the on-board Ethernet ports and the technician port. The technician port is used by the SSR when the IBM FlashSystem 9100 is installed.

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>
<thead>
<tr>
<th>Component</th>
<th>Adapter 1 Ethernet port 1</th>
<th>Adapter 1 Ethernet port 2</th>
<th>Adapter 2 Ethernet port 1</th>
<th>Adapter 2 Ethernet port 2</th>
<th>Adapter 3 Ethernet port 1</th>
<th>Adapter 3 Ethernet port 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speed</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
<td>25 or 10 Gbps</td>
</tr>
</tbody>
</table>
For more information about the assignments of the extra Ethernet ports that can be used for host I/O, see 4.4.1, “Management IP addressing plan” on page 76.

### 4.3.5 SAS expansion enclosures

The following models of SAS expansion enclosures are offered:

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

The following maximum individual expansion enclosure capacities are available:

- 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.

For more information about the rules for mixing the AFF and A9F expansion enclosures that are attached to each IBM FlashSystem 9100 control enclosure, see IBM Knowledge Center.

A single FlashSystem 9100 control enclosure can support up to 20 IBM FlashSystem 9100 SFF expansion enclosures with a maximum of 504 drives per system or up to eight IBM 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 dynamically added with virtually no downtime, which helps 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. IBM FlashSystem 9100 systems can be added into IBM FlashSystem 9100 clustered systems.

Further scalability can be achieved with virtualization of external storage. When IBM FlashSystem 9100 virtualizes an external storage system, capacity in the external system inherits the functional richness and ease of use of IBM FlashSystem 9100.
Expansion enclosure model AFF
The IBM FlashSystem 9100 SFF Expansion Enclosure Model AFF includes the following features:

- Two expansion canisters
- 12 Gb SAS ports for control enclosure and expansion enclosure attachment
- Support for up to 24 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. It includes the following features:

- 5U, 19-inch rack mount enclosure with slide rail and cable management assembly
- Support for up to 92 3.5-inch large-form factor (LFF) 12 Gbps SAS top-loading SSDs
- 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, which provides 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, which gives a maximum of 32 PB of supported raw SSD capacity

All drives within an expansion enclosure must be the SSD type; however, various 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 are used by the IBM SSR during the installation process.

Complete Table 4-8 based on your particular system and provide this worksheet to the IBM SSR before the system is installed (“xxxx” are replaced with your values).

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

<table>
<thead>
<tr>
<th>Configuration setting</th>
<th>Value</th>
<th>Usage in CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDisk group name</td>
<td>xxxx</td>
<td>mkmdiskgrp -name mdisk_group_name</td>
</tr>
<tr>
<td>MDisk extent size in MB</td>
<td>xxxx</td>
<td>-ext extent_size</td>
</tr>
<tr>
<td>RAID level (DRAID5 or DRAID6)</td>
<td>xxxx</td>
<td>mkdistributedarray -level raid_level -driveclass driveclass_id -drivecount x -stripewidth x -rebuildareas x mdiskgrp_id</td>
</tr>
</tbody>
</table>

driveclass_id:  The class that is being used to create the array, which must be a numeric value.

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.

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.

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.

For more information if SAS expansion intermix of enclosures is required, see 5.3, “Scale up for capacity” on page 117.

External storage systems

You can attach and virtualize many types of external storage systems to the IBM FlashSystem 9100 (IBM and non-IBM varieties). For more information, see 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 that are configured as one cluster.

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 feature is defined on node canisters and marked with the letter “T”). All initial configuration for the IBM FlashSystem 9100 is performed by the Throughways 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.
After the initial cluster configuration is completed, the technician port automatically routes the connected user directly to the service GUI for the specific node canister.

Table 4-9 lists the on-board Ethernet ports, speed, and function.

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

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 address does not have its own unique Ethernet cable. It uses the same physical cable that the management IP address uses.
Example 4-1 shows the IBM FlashSystem 9100 Management IP addresses for one control enclosure.

Example 4-1  IBM FlashSystem 9100 Management IP address

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>management IP add.</td>
<td>10.11.12.120</td>
</tr>
<tr>
<td>node 1 service IP add.</td>
<td>10.11.12.121</td>
</tr>
<tr>
<td>node 2 service IP add.</td>
<td>10.11.12.122</td>
</tr>
</tbody>
</table>

**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 on-board 10 GbE ports 3 and 4 and require extra IPv4 or extra IPv6 addresses for each of those 10 GbE ports that are 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.

More iSCSI support is available by ordering and installing PCIe adapters with Feature Code AHB6 - 25 GbE (RoCE) Adapter Cards (Pair) or Feature Code AHB7 - 25 GbE (iWARP) Adapter Cards (Pair).

For more information about these feature codes, see the IBM FlashSystem 9100 announcement materials on this IBM web page.

When accessing the IBM FlashSystem 9100 by using 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 that is described in this book is a web-based GUI that is used to service individual nodes canisters, primarily when a node has a fault, and is in a service state. This GUI is often used only with guidance from IBM remote support. On the IBM FlashSystem 9100 control enclosures, the service ports in the node canisters are 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 GbE switches is better. For the internal SAN attachments, 16 GbE switches are 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.

For more information about examples of the HBA connections, see 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, up to 24 16 Gbps Fibre Channel (FC) ports are available per enclosure when Feature Code AHB3 is ordered. Some of these ports 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. For more information, see Chapter 5, “Scalability” on page 113.

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

Consider the following 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.
- FC 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 a system is updated to version 8.2.0, it retains its NPIV status.

Customer-provided SAN switches and zoning
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 extra storage system so that these systems are 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 more information about suggested fabric zoning, see IBM Knowledge Center.

4.4.3 IP Replication and Mirroring
In this section, we describe IP Replication and mirroring.

iSCSI IP addressing plan
IBM FlashSystem 9100 supports host access through iSCSI (as an alternative to FC). 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 by way of Ethernet switches.
However, the use of two 25-Gbps Ethernet adapters per node canister prevents adding this control enclosure to a system or adding another control enclosure to a system that was made from this controller (sometime known as *clustering*) until a future software release adds support for clustering by way of the 25-Gbps Ethernet ports. These 2-port 25 Gbps Ethernet adapters do not support FCoE.

The following types of 25-Gbps Ethernet adapters are supported:

- RDMA over Converged Ethernet (RoCE)
- Internet Wide-area RDMA Protocol (iWARP)

Either of these adapters work for standard iSCSI communications; that is, not using Remote Direct Memory Access (RDMA). A future software release will add (RDMA) links that use 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.

For more information about the iSCSI-qualified name (IQN) for a IBM FlashSystem 9100 node, see this website.

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 not apparent to servers and applications in the same way that traditional FC-based mirroring is not apparent.

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 extra charge. Remote mirror is a chargeable option, but the price does not change with IP replication. Remote mirror users can access the new function at no extra charge.

**Note:** For more information about how to set up and configure IP replication, see *IBM SAN Volume Controller and Storwize Family Native IP Replication*, REDP-5103.
4.4.5 Advanced Copy Services

The IBM FlashSystem 9100 offers the following Advanced Copy Services:

- FlashCopy
- Metro Mirror
- Global Mirror

IBM FlashSystem 9100 Advanced Copy Services must apply the guidelines that are described next.

**FlashCopy guidelines**

Adhere to the following 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 the 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 lists 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**

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

- Define the grain size that you want to use. A grain is the unit of data that is represented by a single bit in Table 4-10. 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. The data structure and the source data location can modify those effects.
In an 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.

![Metro Mirror connections](image)

Figure 4-11 also contains two redundant fabrics. Part of each fabric exists at the local clustered 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 multiprotocol routers.

Because of the more complex interactions that are involved, IBM tests products of this class for interoperability with the IBM FlashSystem 9100. For more information about the supported SAN routers in the supported hardware list, see the IBM FlashSystem 9100 support website.

IBM 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 km (4970.96 miles) by 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 be sized at least to meet the peak workload requirements, in addition to maintaining the maximum latency that was specified previously. You must evaluate the peak workload requirement by considering the average write workload over a period of 1 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 fail back 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 IBM FlashSystem 9100 Global Mirror is used, all components in the SAN must sustain 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 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 wanted to enable jumbo frames to improve efficiency.

The use of Global Mirror and Metro Mirror between the same two clustered systems is supported.

The use of 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 information about the code level matrix for support, see this IBM Support web page.

Although participating in a Global Mirror relationship is supported for cache-disabled volumes, it is not a preferred practice.

The `gmlinktolerance` parameter of the remote copy partnership must be set to an appropriate value. The default value is 300 seconds (5 minutes), which is appropriate for most clients.

During SAN maintenance, the user must choose to reduce the application I/O workload during the maintenance (so that the degraded SAN components can manage the new workload). Consider the following points:

- 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 \( n \) minutes, it must be reset to only the normal value \( n \) minutes after the end of the maintenance activity.

If `gmlinktolerance` is disabled during the maintenance, it must be reenabled 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 features 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.

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 Serial Advanced Technology Attachment (SATA) is used for Metro Mirror or Global Mirror secondary volumes. The use of 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. Consider the following points:
- Dedicate storage controllers to only Global Mirror volumes.
- Configure the controller to ensure sufficient quality of service (QoS) for the disks that are 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 important to maintain performance when Global Mirror is used.

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 completes and the relationship returns 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 (for example, if 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, the pipe must be sized and designed correctly.

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

**Example 4-2**

- 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. The workload likely is not evenly spread across 24 hours. If extended periods of high data change rates occur, consider suspending Global Mirror during that time.

- 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 option 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 required items for setting up the IBM FlashSystem 9100 call home function.

**Table 4-11  IBM FlashSystem 9100 call home function settings**

<table>
<thead>
<tr>
<th>Configuration item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Domain Name System (DNS) server</td>
<td></td>
</tr>
<tr>
<td>SMTP gateway address</td>
<td></td>
</tr>
<tr>
<td>SMTP gateway name</td>
<td></td>
</tr>
<tr>
<td>SMTP “From” address</td>
<td>Example: <a href="mailto:FS9100_name@customer_domain.com">FS9100_name@customer_domain.com</a></td>
</tr>
<tr>
<td>Optional: Customer email alert group name</td>
<td>Example: <a href="mailto:group_name@customer_domain.com">group_name@customer_domain.com</a></td>
</tr>
<tr>
<td>Network Time Protocol (NTP) manager</td>
<td></td>
</tr>
<tr>
<td>Time zone</td>
<td></td>
</tr>
</tbody>
</table>

**Call Home and Remote Support Assistance information**

Complete Table 4-12 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 RSA contact information**

<table>
<thead>
<tr>
<th>Contact Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact name</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
</tr>
<tr>
<td>Phone (Primary)</td>
<td></td>
</tr>
<tr>
<td>Phone (Alternate)</td>
<td></td>
</tr>
<tr>
<td>Machine location</td>
<td></td>
</tr>
<tr>
<td>System location information</td>
<td></td>
</tr>
<tr>
<td>Company name</td>
<td></td>
</tr>
<tr>
<td>Street address</td>
<td></td>
</tr>
<tr>
<td>City</td>
<td></td>
</tr>
<tr>
<td>State or province</td>
<td></td>
</tr>
<tr>
<td>Postal code</td>
<td></td>
</tr>
<tr>
<td>Country or region</td>
<td></td>
</tr>
<tr>
<td>Proxy server IP addresses for remote support assistance</td>
<td></td>
</tr>
<tr>
<td>IP address 1 Port 1</td>
<td></td>
</tr>
<tr>
<td>IP address 2 Port 2</td>
<td></td>
</tr>
<tr>
<td>IP address 3 Port 3</td>
<td></td>
</tr>
<tr>
<td>IP address 4 Port 4</td>
<td></td>
</tr>
<tr>
<td>IP address 5 Port 5</td>
<td></td>
</tr>
<tr>
<td>IP address 6 Port 6</td>
<td></td>
</tr>
</tbody>
</table>
For more information about setting up the IBM FlashSystem 9100 control enclosure Call Home function, see Chapter 6, “Installing and configuring the IBM FlashSystem 9100 system” on page 165.

4.4.7 Remote Support Assistance

The IBM FlashSystem 9100 control enclosure supports the new RSA feature.

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

The RSA feature can also be used for remote code upgrades, in which the remote support specialist upgrades 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 become more complicated and time-consuming.

RSA uses a high-speed internet connection, but it gives the customer the ability to start an outbound Secure Shell (SSH) call to a secure IBM server. Fire wall rules might need to be configured at the customer’s fire wall to allow the FlashSystem V9000 Cluster and Service IPs to establish a connection to the IBM Remote Support Center by way of 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. For more information about the IBM IP addresses that are used for RSA, see the gray note box on page 89.

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

Figure 4-13 shows the overview of the RSA setup, which includes three major components.
Remote Support Client
The Remote Support Client is a software component that is inside IBM FlashSystem 9100 that handles remote support connectivity. It is on both canister nodes of the IBM FlashSystem 9100 control enclosure. The software component relies on a single outgoing Transmission Control Protocol (TCP) connection only, and it cannot receive inbound connections of any kind.

The Remote Support Client is controlled by using the CLI or the GUI. The customer can control the connection progress by using the CLI to open or close it. They can also add a password that IBM must request before logging in by using the RSA link.

Remote Support Center Front Server
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 start any process 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 by way of port TCP/22 (SSH):
- 204.146.30.139
- 129.33.206.139
- 204.146.30.157
- 129.33.207.37

Remote Support Center Back Server
The Back Server manages most of the logic of the RSA system and is 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 can 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 manages the remote support session as it progresses (logging it, allowing more support persons to join the session, and so on).

In addition, the IBM FlashSystem 9100 remote support solution can use the following two IBM internet support environments:
- IBM Enhanced Customer Data Repository
  If a remote connection exists, the IBM remote support specialists can offload the required support logs.
- IBM Fix Central
  IBM Fix Central provides fixes and updates for IBM system's software, hardware, and operating system. The IBM FlashSystem 9100 control enclosure allows 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 IBM.
**Note:** To download software update packages, the following six IP addresses are used by way of 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. Also, it is required to configure a DNS server to allow the download function to work.

For more information about manually downloading the code from IBM Fix Central, see this website.

**Note:** You must have available the machine type, origin, and serial number during the download process to validate the entitlement for software downloads.

**Remote Support Proxy**

Optionally, an application called Remote Support Proxy can be used when one or more IBM FlashSystem 9100 systems do not have direct access to the internet (for example, because of firewall restrictions). The Remote Support Client within the FlashSystem 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 shows the connection through the Remote Support Proxy.

![Diagram](https://via.placeholder.com/150)

*Figure 4-14   Connections through the Remote Support Proxy.*

The communication between the Remote Support Proxy and the Remote Support Center is encrypted with another 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 software
The Remote Support Proxy is a small program that is supported on some Linux versions. The software is also used for other IBM Storage Systems, such as IBM XIV or FlashSystem A9000. The installation files and documentations are available at the storage portal website.

Note: At the time of this writing, Remote Support Proxy does not support a connection to IBM ECURep for automatically uploading logs. Also, the software download from IBM Fix Central is not supported through the optional Remote Support proxy.

Before you configure remote support assistance, the proxy server must be installed and configured separately. During the setup process for support assistance, specify the IP address and the port number for the proxy server on the Remote Support Centers page.

For more information about the remote support proxy, see this IBM Support Fix Central web page.

Complete the following steps:
1. See this IBM Support Fix Central web page.

Figure 4-15 shows the main page of the IBM XIV software from where the Remote Proxy code can be downloaded.

![Figure 4-15 Locating the XIV Remote Support Proxy software](image)
2. Select the IBM XIV Remote Support Proxy, as shown in Figure 4-15 on page 91. Always use the latest Proxy Server because it references the latest secure front endservers at IBM, as shown in Figure 4-16.

![IBM XIV Remote Support Proxy](image)

Figure 4-16  Select the Latest Proxy Server package

The installation instructions are included in the User’s Guide.

**Note:** The common remote support proxy software package can be used for IBM FlashSystem 900, XIV, IBM FlashSystem A9000, IBM FlashSystem V9000, and IBM FlashSystem 9100.

### 4.5 IBM Storage Insights

IBM Storage Insights is an important part of 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 your IBM block storage. You can make better decisions by seeing trends in performance and capacity.

Storage health information enables you to focus on areas that need attention and 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.

IBM Storage Insights includes the following features:

- A unified view of IBM systems:
  - Provides a single view to see all your systems characteristics.
  - Displays all of your IBM storage inventory.
  - Provides a live event feed so that you know up-to-the-second what is occurring with your storage and enables you to act quickly.

- IBM Storage Insights collects telemetry data and call home data and provides up-to-the-second system reporting of capacity and performance.
Overall storage monitoring, which reviews the following components:
- Overall health of the system
- The configuration to see whether it meets known best practices
- System resource management; that is, checks if the system is overly taxed and provides proactive recommendations to fix it

Storage Insights provides advanced customer service with an event filter to that includes the following features:
- The ability for you and IBM Support to view, open, and close support tickets open and track trends.
- By using the auto-log collection capability, you can collect the logs and send them to IBM before IBM Support reviews the issue. This process can save as much as 50% of the time to resolve the case.

IBM Storage Insights Pro is available in addition to the free IBM Storage Insights. 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 with EMC VNX and VMAX.

The IBM Storage Insights and IBM Storage Insights Pro products are compared in Figure 4-17.

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

*Figure 4-17  IBM Storage Insights and IBM Storage Insights Pro comparison*
4.5.1 Architecture, security, and data collection

Figure 4-18 shows the architecture of the IBM Storage Insights application, the products that are supported, and the three main teams that can benefit from the use of the tool.

IBM Storage Insights provides a lightweight data collector that is deployed on a customer-supplied server. This server can be 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 4-19 shows the data flow from systems to the IBM Storage Insights cloud.

**Deployed instantly from the Cloud**

- **Data collector** connects your on-premises storage environment with the cloud-based service.
- **Designed for security and efficiency**
  - All communication between the data collector and the service is encrypted and compressed.
  - All communication is initiated from the collector only, no LAN-external access to the collector or the storage devices.
  - Various security certifications (FISMA, ISO 2700x)
- **No administration/maintenance effort for the local data collector.**

---

**What metadata is collected**

Metadata about the configuration and operations of storage resources is collected, including the following examples:

- 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 application data that is stored on the storage systems cannot 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 4-20 shows the IBM Storage Insights main dashboard and the systems that it is monitoring.

![Storage Insights dashboard example](image)

Other views and images of dashboard displays and drill downs can be found in the supporting documentation that is described next.

**IBM Storage Insights information resources**

For more information about IBM Storage Insights and to sign up and register for the free service, see the following resources:

- Fact Sheet
- Demonstration (login required)
- IBM Security Insights Security Guide
- IBM Knowledge Center
- Registration (login required)

4.6 IBM FlashSystem 9100 system configuration

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 assume the clustered system management IP address. Ensure 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 if an individual IBM FlashSystem 9100 node canister fails, the IBM FlashSystem 9100 control enclosure houses two node canisters to form 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 release includes the HyperSwap function, which allows 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. Although these connections can run at 8 or 16 Gbps (depending on your switch hardware), 16 Gbps is recommended 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 are 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.

### 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 allows the users to define volumes that use the new data reduction and de-duplication capabilities, which were introduced in Spectrum Virtualize software.

The complete compliment of storage pool types are available:

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

The DRPs also can support de-duplication. This support is enabled at a volume level when the volumes are created within a pool. For more information about DRP and deduplication, see Chapter 3, “Data reduction and tools” on page 23.

**Important:** On IBM FlashSystem 9100, you want to use fully allocated DRPs with compression and no deduplication or DRPS with compression and deduplication.

After the system set-up process is complete, you must configure storage by creating pools and assigning storage to specific pools. Ensure that a pool or pools are created before assigning storage.
In the management GUI, select **Pools → Actions → Add Storage**. The Add Storage automatically configures drives into arrays. Use the `isarrayrecommendation` 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 recommended arrays for the IBM FlashSystem 9100 is to configure a distributed array (DRAID6) by using the `mkdistributedarray` command.

**Note:** DRAID6 arrays give better performance and rebuild times if an FCM or NVMe drive fails because the spare capacity that is allocated for the rebuild is shared across all of the drives in the system. That capacity is *not* reserved to one physical drive as it is in the traditional RAID arrays.

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

- A storage pool is a collection of MDisks. An MDisk can be contained within a single storage pool only.
- 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 more information about IBM FlashSystem 9100 configuration limits, see this IBM Support web page.

**Extent size**

Each MDisk is divided into chunks of equal size, which are 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, 32, 64, 128, 256, 512, 1024, 2048, 4096, and 8192 MB. By default, the MDisk 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 more information about the use of the CLI commands, see 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

<table>
<thead>
<tr>
<th>Extent size</th>
<th>Maximum clustered system capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 MB</td>
<td>64 TB</td>
</tr>
<tr>
<td>32 MB</td>
<td>128 TB</td>
</tr>
<tr>
<td>64 MB</td>
<td>256 TB</td>
</tr>
<tr>
<td>128 MB</td>
<td>512 TB</td>
</tr>
<tr>
<td>256 MB</td>
<td>1 petabyte (PB)</td>
</tr>
<tr>
<td>512 MB</td>
<td>2 PB</td>
</tr>
<tr>
<td>1,024 MB</td>
<td>4 PB</td>
</tr>
<tr>
<td>2,048 MB</td>
<td>8 PB</td>
</tr>
<tr>
<td>4,096 MB</td>
<td>16 PB</td>
</tr>
<tr>
<td>8,192 MB</td>
<td>32 PB</td>
</tr>
</tbody>
</table>

Only the maximum extents sizes versus the maximum cluster size when up to four IBM FlashSystem 9100 are clustered together are listed in Table 4-13.

For more information about the extents in regular, thin, and compressed pools, and the latest information about the IBM FlashSystem 9100 configuration limits, see this IBM Support web page.

When planning storage pool layout, consider the following points:

- Pool extent size:
  - Generally, use 1 GB or higher. Consider the following points:
    - If DRP is used, 4 GB must be used.
    - If DRP is not used, 1 GB can be used.
  
    **Note:** 4 GB is the default now.
  - For more information about all of the values and rules for extents, see this IBM Support web page.
  - Choose 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.
  - The use of larger number of smaller pools reduces the failure domain if one of the pools goes offline. However, more storage pools introduces management overhead, effects storage space use efficiency, and is subject to the configuration maximum limit.
  - An alternative approach is to create few large storage pools. All MDisks that constitute each of the pools must 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 that are created from the pool.

This rule does not apply when you intentionally 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.

### 4.6.1 Volume considerations

An individual volume is a member of one storage pool and one I/O Group. Consider the following points:

- The storage pool defines which MDisks that are provided by the disk subsystem make up the volume.
- The I/O Group (two nodes canisters make an I/O Group) defines which IBM FlashSystem 9100 nodes provide I/O access to the volume. In a single enclosure, IBM FlashSystem 9100 features 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 another 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, whenever you create a volume, it is associated with the next node by 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 the use of 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 if the preferred node fails or when concurrent code upgrade is running.
Thin-provisioned volume considerations:

- When creating the thin-provisioned volume, be sure to understand the use patterns of the applications or group users that are accessing this volume. You must consider items, such as the size of the data, rate of creation of data, and modifying or deleting existing data.

- The following 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 uses all of the storage in a storage pool.
  - *Non-autoexpand volumes* feature a fixed amount of assigned storage. In this case, the user must monitor the volume and assign more capacity when required. A misbehaving application can cause only 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 (through a lack of available physical storage for autoexpand, or because a volume that is marked as non-expand was not expanded in time), a danger exists of data being left in the cache until storage is made available. Although this situation is not a data integrity or data loss issue, you must not rely on the IBM FlashSystem 9100 cache as a backup storage mechanism.

- When you create a thin-provisioned volume, you can choose the grain size for allocating space in 32 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 can adversely affect performance. If you are *not* using the thin-provisioned volume as a FlashCopy source or target volume, use 256 KB to maximize performance. If you *are* 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 (as with the IBM FlashSystem V9000 fast write cache); therefore, certain applications perform better.

- Thin-provisioned volumes require more processor processing; therefore, 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 a fully allocated volume is converted to a thin-provisioned volume by using volume mirroring.
- **Volume mirroring guidelines:**
  - With the IBM FlashSystem 9100 system in a high-performance environment, this capability is possible with a *scale up* or *scale out* solution only. If you are considering volume mirroring for data redundancy, a second control enclosure with its own storage pool is needed for the mirror to be on.
  - Create or identify two separate storage pools to allocate space for your mirrored volume.
  - If performance is a concern, use a storage pool with MDisks that share characteristics. Otherwise, the mirrored pair can be on external virtualized storage with lesser-performing MDisks.

- **Data Reduction Pool volumes**
  When configuring DRP-based volumes, special considerations must be followed. For more information, see Chapter 3, “Data reduction and tools” on page 23.

### 4.6.2 IBM 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. This process places 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 are in external arrays. All managed arrays on the IBM FlashSystem 9100 system contain 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 nodes canisters 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 is 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 encrypted. This feature allows the hardware compression of the IBM FlashSystem 9100 to be effective if the FCM type NVMe drives are used.
However, cases exist in which the use of IBM FlashSystem 9100 software compression is preferred, such as if highly compressible data exists (for example, 3:1 or higher). In these cases, encryption and compression can be done by the IBM FlashSystem 9100 nodes canisters.

For more information about Easy Tier, see Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1, SG24-7933, and 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 be changed by the CLI only.

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

Figure 4-21 shows the four possible Easy Tier states.

![Figure 4-21 Easy Tier status for CLI and GUI](image)

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 by using the command line to Measured. 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 must 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.

For more information about downloading and the use of the tool, see this website.

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 are 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 the Easy Tier considerations and recommendations, see this website.

### 4.6.3 SAN boot support

The IBM FlashSystem 9100 supports SAN boot or startup for IBM AIX, Microsoft Windows Server, and other operating systems. Because SAN boot support can change, see this IBM SSIC web page.

### 4.7 Licensing and features

In this section, we describe base products licenses and feature licensing.

#### 4.7.1 IBM FlashSystem 9100 products licenses

The following IBM FlashSystem 9100 base products licenses are available:

- 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 IBM FlashSystem 9100 Expansion Enclosure Base Model A9F- PID 5639-FA1 license.

**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 requires only 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:

- Spectrum Virtualize for SAN Volume Controller - PID 5641-VC8
- IBM Virtual Storage Center (VSC) - PID 5648-AE1
In addition to one of these licenses, the capacity of each enclosure or array includes an SCU value applied. A SCU is measured by category of usable capacity being virtualized and managed. The following categories are available:

- **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 that use 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.

Next, we describe 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**
  
  This feature enables data encryption at rest on the IBM FlashSystem 9100 control enclosure assigned MDisks. USB flash drives (feature ACEA) or IBM Security Key Manager (SKLM) are required for encryption key management.

  Only 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 (IBM FlashSystem 9100 control enclosure and all attached IBM 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 IBM Security Key Manager (SKLM) is used for encryption keys management, a total of three USB flash drives are required per IBM FlashSystem 9100 cluster when encryption is enabled in the cluster, regardless of the number of systems in the cluster. If encryption is used in a cluster, this feature is ordered on one IBM FlashSystem 9100 system, which results in a shipment of four USB flash drives.

  You must have three USB keys when you enable encryption to store the master key. These keys are plugged into active nodes in your cluster. To start the system, you must have one working USB stick plugged into one working canister in the system. Therefore, you must have three copies of the encryption master key before you are allowed to use encryption.
The following methods can be used to install the encryption feature on the IBM FlashSystem IBM FlashSystem 9100:

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

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

**Note:** To start 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, a rekey feature 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 has the encryption feature installed. The USB keys must be installed in the USB ports in the rear of the nodes canisters.

Figure 4-22 is a rear view of the location of USB ports on the IBM FlashSystem 9100 node canisters.

**IBM Security Key Lifecycle Manager**

IBM FlashSystem IBM FlashSystem 9100 Software V8.2 adds 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 IBM FlashSystem 9100 Software V8.2, you enabled encryption by using USB flash drives to copy the encryption key to the system.
**Encryption summary**

Encryption can occur at the hardware or software level.

**Hardware Encryption at the IBM FlashSystem 9100**

IBM FlashSystem IBM FlashSystem 9100 supports hot encryption activation when encryption is enabled in the control enclosure. With hot encryption activation, you can enable encryption on a flash array without having to remove the data. Enabling encryption in this way is a non-destructive process.

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

### 4.7.5 Compression

The following methods are available to compress data on the IBM FlashSystem 9100, depending on the type of storage that is installed in the control enclosure and attached to the system:

- NVMe FCM In-line Hardware Compression
- Data Reduction Pool (DRP) Compression

The IBM FlashSystem 9100 software does not support Real-time Compression (RtC) type compressed volumes. If the user wants to use these established volumes on the IBM FlashSystem 9100, they must migrate them to the new DRP model. They must use volume mirroring to clone data to a new DRP. DRP pools no longer support older migrate commands.

**Important:** On IBM FlashSystem 9100, you want to use fully allocated DRPs with compression and no deduplication or DRPs with compression and deduplication.
Figure 4-23 shows the method that traditional volumes and those volumes that are compressed under the RtC process use to migrate to the new DRPs model.

IBM FlashSystem 9100 enclosure that use the IBM Flash Core Modules (FCM) have inline hardware compression as always on. The best usable-to-maximum-effective capacity ratio depends on the FCM capacity.

Some workloads that are not demanding the lowest latency and have a good possible compression rate can be a candidate for the use of software-based compression or the DRP. For more information, see Chapter 3, “Data reduction and tools” on page 23.

The IBM FlashSystem 9100 enclosure that uses industry standard NVMe drives do not include built-in hardware compression. Therefore, they must rely on the use of DRPs 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 extra hardware that is dedicated to the improvement of the compression functionality. This hardware is built in on the node canister motherboard.

No separate PCIe type compression cards are used as were used on previous products. These accelerators work with the DRP software within the control enclosure for the I/O Group to support compressed volumes.

**Important:** On IBM FlashSystem 9100, you want to use fully allocated DRPs with compression and no deduplication or DRPs 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 software with hardware-assisted compression or the use of the DRPs. This type of FCM compression is always on and cannot be switched off. For more information about compression, its architecture, and operation, see Chapter 2, “IBM FlashSystem 9100 architecture” on page 11.

**Data reduction at two levels**
Solutions can be created in which where data reduction technologies are applied at the storage and virtualization appliance levels.

It is important to understand which of these options makes the most sense to ensure that performance is not affected and space is used in the best way possible.

Table 4-14 lists known best practices when IBM FlashSystem 9100 and other external storage are used.

<table>
<thead>
<tr>
<th>Front end</th>
<th>External Storage</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| IBM FlashSystem 9100 - DRP above simple RAID | Storwize 5000 or any other Fully Allocated Volumes | Yes  
Consider the following points:  
► Use DRP at top level to plan for de-duplication and snapshot optimizations.  
► DRP at top level provides best application capacity reporting (volume written capacity).  
► Always use compression in DRP to get best performance.  
► Bottlenecks in compression performance come from metadata overheads, not compression processing. |
| IBM FlashSystem 9100 - Fully Allocated | IBM FlashSystem A9000 | Use with care  
Consider the following points:  
► Need to track physical capacity use carefully to avoid out-of-space.  
► SAN Volume Controller can report physical use, but does not manage to avoid out-of-space.  
► No visibility of each application’s use at SAN Volume Controller layer.  
► If actual out-of-space happens, limited ability is available to recover. Consider creating sacrificial emergency space volume. |
| IBM FlashSystem 9100 - Fully Allocated above multtier data reducing back-end | IBM FlashSystem A9000 and IBM Storwize 5000 with DRP | Use with great care  
Consider the following points:  
► Easy Tier is unaware of physical capacity in tiers of hybrid pool.  
► Easy Tier tends to fill the top tier with hottest data.  
► Changes in compressibility of data in top tier can overcommit the storage leading to out-of-space. |
**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. The map 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 backup can assist you in restoring the system configuration. You can save the configuration by using the `svccconfig backup` command.

Complete the following steps to create a backup of the IBM FlashSystem 9100 configuration file and to copy it to another system:

1. Log in to the cluster IP by using an SSH client and back up the IBM FlashSystem 9100 configuration. Example 4-3 shows the output of the `svccconfig backup` command.

   **Example 4-3  Output of the svccconfig backup command**

   ```
   superuser> svccconfig backup
   ...............................................................
   CMMVC6155I SVCCONFIG processing completed successfully
   ```

2. Copy the configuration backup file from the system. By using secure copy, copy the following file from the system and store it, as shown in the following example:

   `/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 must be completed on any external storage in the IBM FlashSystem 9100 cluster. If you have the IBM FlashSystem 900 AE3 as external storage, you must log in to each of the AE3 cluster IP addresses by using an SSH client and run the `svccconfig backup` command on each of the FlashSystem AE3 attached storage enclosures. The same process applies to any IBM Storwize system that is 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. You can explore 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 IBM 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 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 Protection
- IBM FlashSystem 9100 Multi-Cloud Solution for Private Cloud Flexibility, and Data Protection

For more information about the software products that are included with the FlashSystem 9100 purchase, see IBM Knowledge Center.
This chapter describes the following 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 more building blocks and adding storage expansion enclosure.

This chapter includes the following topics:

- 5.1, “Overview” on page 114
- 5.2, “Scaling features” on page 115
- 5.3, “Scale up for capacity” on page 117
- 5.4, “Adding internal NVMe storage” on page 119
- 5.5, “Adding another Control Enclosure into a system” on page 132
- 5.6, “Adding an IBM FlashSystem 9100 expansion enclosure” on page 147
- 5.7, “Adding external storage systems” on page 152
- 5.8, “Adding IBM FlashSystem 9100 to a Storwize V7000 system” on page 161
5.1 Overview

IBM FlashSystem 9100 features 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 IOPS and bandwidth. The solution also can be simultaneously scaled up and out to improve capacity, IOPS, and bandwidth while maintaining IBM MicroLatency®.

Model AF7 and Model AF8 IBM FlashSystem 9100 systems scale up to 760 drives with the attachment of FlashSystem 9100 expansion enclosures. IBM FlashSystem 9100 systems can be clustered to help deliver greater performance, bandwidth, and scalability.

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

IBM FlashSystem 9100 offers two 12 Gb SAS expansion enclosure models. IBM FlashSystem 9100 SFF Expansion Enclosure Model AFF supports up to 24 2.5-inch flash drives; IBM FlashSystem 9100 LFF HD Expansion Enclosure Model A9F supports up to 92 flash drives a 3.5-inch carrier. SFF and LFF HD expansion enclosures can be intermixed within an IBM 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 includes the following scalability features:

- Flexible scalability configuration options:
  - Add internal FlashCore Modules
  - Add up to four control enclosures to form a cluster
  - Add 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 is 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, 15.36 TB
  - Encryption Capable
  - Distributed RAID5; Distributed RAID6 (preferred)

**Note:** Array members must be uniform in capacity size to avoid bottlenecks and issues when drives are replaced.

- Attachment for up to 20 IBM FlashSystem 9100 model AFF SAS expansion enclosures per control enclosure or 8 model A9F SAS enclosures that use 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 (IBM FlashSystem 9110)
  - Control Enclosures AF8 (IBM 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 IBM FlashSystem 9100 control enclosure can support multiple attached expansion enclosures. Expansion enclosures can be dynamically added with virtually no downtime, which helps 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, which represents 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, which multiplies performance and capacity with each addition.

Clustering IBM FlashSystem 9100 scales the performance with extra 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 use IBM FlashSystem 9100 Expansion Enclosures that use 12 Gb SAS flash drives.

SAS enclosures can be added for more capacity within the performance envelope of a single control enclosure.

Consider the following points:

- Add I/O groups for performance
- Add 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 IBM FlashSystem 9100.

**Note:** IBM FlashSystem 9100 systems can be added into Storwize V7000 clustered systems.
For improving performance, consider the cache options of 128 GB base configuration and upgrade options of 256 GB, 358 GB, 768 GB, 1.1 TB, or 1.5 TB memory cache per control enclosure that 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 the following scaling concepts:

- **Scale up.** Add 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:
  - IBM FlashSystem 9100 uses Spectrum Virtualize with support up to 32 PB. This total is the maximum total of all NVMe, SAS, and virtualized storage.
  - Enables migration and reuse of storage assets.

### Building Blocks

Figure 5-1 shows the building blocks: NVMe control enclosure and 24 and 96 SAS SSD expansion enclosures.
Chapter 5. Scalability

Figure 5-2 shows the following maximum configurations:

- Single control enclosure IOPs and usable and effective capacity
- Scale up with four clustered control enclosures, which provides increased IOPs and usable and effective capacity
- Scale out expanded capacity with SAS enclosures
- Scale out capacity with supported virtualize storage controllers

5.3 Scale up for capacity

Add the following capacity to IBM FlashSystem 9100 single or clustered systems:

- Internal NVMe drives
- SAS expansion enclosures
- External virtualized storage systems
Scale up and out options that are available 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 are shown in Figure 5-5.

5.4 Adding internal NVMe storage

NVMe-Accelerated Enterprise Flash Array- 100% NVMe includes the following features:

- IBM FlashSystem 9100 features 24 x 2.5-inch slots to populate with NVMe storage (see 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, which offers unprecedented storage capacity in 2U of rack space
- Up to 8 PB of NVMe data storage in 8U with data reduction

Note: Internal storage is licensed on a per enclosure basis.
NVMe FlashCore Modules (FCMs) use inline hardware compression to reduce the amount of required physical space. FCMs can easily provide the following significant amounts of capacity by using performance-optimized hardware compression or Data Reduction Pools (DRPs):  

- Six drive minimum  
- Distributed RAID 6 (recommended), Distributed RAID5 (supported by 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 Flash Core Module  
  - (AHS2): 9.6 TB 2.5-inch NVMe Flash Core Module  
  - (AHS3): 19.2 TB 2.5-inch NVMe Flash Core Module

Industry-standard NVMe Flash drives do not include hardware compression. The drives offer the following significant amounts of capacity and high performance:  

- Two drive minimum (varies by RAID type).  
- Traditional RAID 10, Distributed RAID 6 (recommended), and 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: IBM FlashSystem 9100 is optimized for 16 - 24 NVMe devices, which balances performance, rebuild times, and usable capacity. Fewer devices are acceptable for smaller capacity systems that do not include a high-performance requirement, but avoid few large devices.
```

Figure 5-7 shows the minimum and maximum capacities per NVMe drive type, and capacity ranges when inline compression or DRP features are used.

```
<table>
<thead>
<tr>
<th>Flash Media</th>
<th>Capacity per Drive with Inline Compression (max ratio varies 2:1 – max)</th>
<th>Capacity per Drive with Data Reduction Pools (2:1 – 5:1)</th>
<th>Max System Capacity in 2U with Inline Compression (max ratio varies 2:1 – max)</th>
<th>Max System Capacity in 2U with Data Reduction Pools (2:1 – 5:1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCM 4.8TB</td>
<td>0.6TB – 22TB</td>
<td>0.6TB – 24TB</td>
<td>230.4TB – 552TB</td>
<td>230.4TB – 576TB</td>
</tr>
<tr>
<td>FCM 9.6TB</td>
<td>10.2TB – 22TB</td>
<td>10.2TB – 48TB</td>
<td>400.8TB – 552TB</td>
<td>400.8TB – 1.1PB</td>
</tr>
<tr>
<td>FCM 19.2TB</td>
<td>38.4TB – 44TB</td>
<td>38.4TB – 96TB</td>
<td>921.6TB – 1PB</td>
<td>921.6TB – 2.3PB</td>
</tr>
<tr>
<td>NVMe 1.92TB</td>
<td>3.84TB – 9.6TB</td>
<td></td>
<td>92.6TB – 230.4TB</td>
<td></td>
</tr>
<tr>
<td>NVMe 3.84TB</td>
<td>7.68TB – 19.2TB</td>
<td></td>
<td>184.32TB – 460TB</td>
<td></td>
</tr>
<tr>
<td>NVMe 7.68TB</td>
<td>15.36TB – 38.4TB</td>
<td></td>
<td>368.64TB – 921.6TB</td>
<td></td>
</tr>
<tr>
<td>NVMe 15.36TB</td>
<td>30.72TB – 76.8TB</td>
<td></td>
<td>737.28TB – 1.8PB</td>
<td></td>
</tr>
</tbody>
</table>
```

**Figure 5-7** NVMe FCMs and Industry Standard drive and system capacities
5.4.1 Installing NVMe FCMs or NVMe SSDs

In this example, we show how to add a minimum of six NVMe drives for a new DRAID6 array.

Removing the drive filler blanks
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 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 read and understand the removal and drive installation instructions, and that the drive is unpacked before you remove the 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. Remove the drive slot filler (see Figure 5-8).

![Figure 5-8 NVMe drive slot filler](image)

3. Use your thumb and forefinger to pinch the latch of the drive blank.
4. Gently slide the release latch up to unlock the handle.
5. Pull the drive slot filler from the drive slot.
Figure 5-9 shows an example of an NVMe internal drive.

6. Have new NVMe drive ready to install (see Figure 5-10).

7. Ensure that the LED indicators are at the top of the drive.
8. Press the blue touchpoint to unlock the latching handle on the new drive.
9. 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](image)

10. Finish inserting the new drive by closing the handle until the latch clicks into place (see Figure 5-12).

![Figure 5-12 Completing the drive installation](image)

Repeat steps 1-9 to install the remaining NVMe drives.
5.4.2 Configuring NVMe drives for MDisk and storage pools

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 dashboard.

![Management GUI dashboard](image)

Figure 5-13  Management GUI dashboard

Complete the following steps to review new NVMe drives that are installed:

1. Select Monitoring → System to open the System - Overview window.
2. Select Enclosure Actions → Drives.
3. Click Enclosure Actions and select Drives to view the internal drives, as shown in Figure 5-14 on page 125.
The six new NVMe drives are listed in Use column status of **Unused**, as shown in Figure 5-15.

**Note:** DRAID6 requires a minimum of six drives.
Complete the following steps from the Drives for Control Enclosure 1 window:

1. Click and select the six new NVMe drives.
2. Select **Actions** → **Mark As** → **Candidate** status for MDisk creation, as shown in Figure 5-16.

![Figure 5-16 Selecting Actions → Mark as → Candidate](image)

3. Click **Yes** to assign the drives to candidate Use, as shown in Figure 5-17.

![Figure 5-17 Setting drives to Candidate state](image)
The drives are now in Candidate state, as shown in Figure 5-18.

Figure 5-18   Drives Use set to Candidate

4. Select Pools → MDisks by Pools to view the drives that are available for creating an MDisk and Storage Pool, as shown in Figure 5-19.

Figure 5-19   Selecting Pools → MDisks by Pools

5.4.3 Working with storage pools

An MDisk is a logical unit (LU) of physical storage. MDisks are 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 shows an overview of how storage pools, MDisks, and volumes are related. The system has four LUs from internal disks arrays, no LUs from external storage, four storage pools, and 93 defined volumes, which are mapped to four hosts.

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. MDisks can be added to a pool to provide more 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 by using the Pools window or the MDisks by Pool window. Both windows allow you to run the same actions on parent pools. However, actions on child pools can be performed by using the Pools window only. To access the Pools window, click **Pools → Pools**.
Creating a storage pool
Complete the following steps to create a storage pool:

1. Click **Pools → MDisks by Pools** and then, click **Create Pool**, as shown in Figure 5-21.

![Figure 5-21 Option to create a storage pool in the MDisks by Pools pane](image)

2. Select **Assign** to add the 6 NVMe drives to storage pool, as shown in Figure 5-22.

![Figure 5-22 Select Assign for creating of Mdisk](image)
3. Open the dialog box that is shown in Figure 5-23. Enter in name of the new storage pool: ITSO_Pool1.

![Create Pool dialog box](image)

**Figure 5-23  Create Pool dialog box**

The new storage pool is created with no assigned drives, as shown in Figure 5-24.

![Storage Pool created](image)

**Figure 5-24  Storage Pool created**
4. Click **Assign Internal Storage** to add the internal NVMe drives to the storage pool, as shown in Figure 5-25.

![Figure 5-25  Assigning internal drives to storage pool](image)

5. Enter 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](image)
An MDisk with six internal NVMe drives is added to the storage pool, as shown in Figure 5-27.

![Figure 5-27](image.png) New MDisk mdisk1 in Storage Pool with six new NVMe drives

The MDisk in the Storage Pool with new internal NVMe drives is now available.

### 5.5 Adding another Control Enclosure into a system

Scaling out for performance is done by adding control enclosures to a cluster. These added NVMe control enclosures are managed by the same GUI or CLI as the IBM FlashSystem 9100.

A maximum of four control enclosures can be added. 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 extra enclosure. For more information, see IBM Knowledge Center.

**Note:** Up to four systems can be 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 IBM 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 SAN configuration and zoning, see IBM Knowledge Center.

For more information about zoning requirements for N_Port ID virtualization, see IBM Knowledge Center.
An example SAN configuration is shown in Figure 5-28.

![Simple SAN Configuration](image)

**Figure 5-28** Simple SAN Configuration

**Zoning**

In IBM FlashSystem 9100 deployments, the SAN fabric must have the following distinct zone classes:

- **Host zones**: Allows communication between IBM FlashSystem 9100 and hosts.
- **Storage zone**: Allows communication between IBM FlashSystem 9100 and back-end storage.

A third zone is required in clustered configurations, which allows communication between storage system nodes (intracluster traffic).

Figure 5-29 shows the IBM FlashSystem 9100 zoning classes.

![IBM FlashSystem 9100 zoning classes](image)

**Figure 5-29** IBM FlashSystem 9100 zoning classes

**Note**: IBM 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.
5.5.2 Adding a control enclosure that was removed

**Note:** If the control enclosure was configured or part of another IBM FlashSystem 9100 cluster, complete the procedure that is described in 5.5.2, “Adding a control enclosure that was removed”.

If a new IBM FlashSystem 9100 control enclosure is added that was not configured, see 5.5.3, “Adding Control Enclosure by using the management GUI” on page 136.

Ensure that the following 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 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:

a. Connect to the service assistant on either of the nodes in the control enclosure.

b. Select **Configure Enclosure**.

c. Select the **Reset the system ID** option. Do not make any other changes.

d. Click **Modify** to make the changes.

By using the Service Assistant (see Figure 5-30) on main control enclosure, change the new node’s status to Candidate.

![Service Assistant login window](image.png)

**Figure 5-30 Service Assistant login window**
Nodes 1 and 2 are in Service status. Click node 1 and select **Exit Service State** to change the node from Service to Candidate status, as shown in Figure 5-31.

Click node 2 and select **Exit Service State** to change the node from Service to Candidate status, as shown in Figure 5-32.
Nodes 1 and 2 are now 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](image)

The use of Service Assistant on the cluster IP the IBM 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](image)

### 5.5.3 Adding Control Enclosure by using the management GUI

Use the management GUI or the CLI to add a Control Enclosure to the system.

Use 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 control enclosure to the system:

1. Click **Add Enclosure** to start wizard, as shown in Figure 5-35.

   ![Figure 5-35 Selecting Add enclosure](image)

   **Figure 5-35 Selecting Add enclosure**

   The first dialog box displays the available control enclosure and its details, as shown in Figure 5-36. Encryption license is enabled for the first control enclosure.

   **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](image)

   **Figure 5-36 Adding a control enclosure to the system**
2. Select the new control enclosure to Activate License Automatically or Manually, as shown in Figure 5-37.

![Figure 5-37 Selecting node for Encryption license enablement](image)

3. Enter in the Authorization Code for control enclosure, as shown in Figure 5-38.

![Figure 5-38 Entering activation encryption key](image)
The new Control Enclosure Encryption License is enabled, as shown in Figure 5-39.

Figure 5-39   Encryption enabled

4. 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 that the task is completed.

![Figure 5-41 Add Enclosure task completed](image)

5. After the control enclosure is successfully added to the system, a success message is displayed, as shown in Figure 5-42. Click Close.

![Figure 5-42 Add Control Enclosure completed](image)
6. Browse to the System - Overview page to view more information about Control Enclosures, as shown in Figure 5-43.

![Figure 5-43 System - Overview Control Enclosures view](image)

7. Click Control Enclosure 2 to view enclosure details, as shown in Figure 5-44.

![Figure 5-44 Control Enclosure 2 details](image)
An error appears 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 the Run Fix wizard or ignored until the MDisk and storage pool are created.

8. Click Run Fix to run the wizard and create an MDisk.
9. Select Create some managed disks and then, click Next, as shown in Figure 5-46.
10. Select **Next** to create the MDisk, as shown in Figure 5-47.

![Figure 5-47 Create MDisk](image)

The system checks Quorum Device Status for 60 seconds. When the window refreshes, a new window opens, as shown in Figure 5-48.

![Figure 5-48 Checking Quorum Device status](image)
Error 3124 is fixed, Quorum Devices are online, and an MDisk was created, as shown in Figure 5-49.

Figure 5-49   Error is fixed

No errors exist in the Event Log, as shown in Figure 5-50.

Figure 5-50   Error Event Log
NVMe internal drives on the new Control Enclosure are available to be assigned to a storage pool, as shown in Figure 5-51.

![Figure 5-51 Assigning new available NVMe drives to Storage Pool](image)

11. Enter name of the new Storage Pool (for example, ITSO_Pool2), as shown in Figure 5-52.

![Figure 5-52 Creating a storage pool](image)
5.5.4 Adding Control Enclosure by using Management CLI method

Complete the following steps to add an enclosure to the system by using the command-line interface:

1. Run the `sainfo lsservicestatus` command (on the service CLI of the new enclosure) and record the WWNN of the new enclosure (see Figure 5-53).

![Figure 5-53 Obtaining WWNN by using sainfo lsservicestatus CLI command](image)

2. Run the `lscontrolenclosurecandidate` command to verify that the enclosure is detected on the fabric, as shown in Figure 5-54.

![Figure 5-54 Running CLI command lscontrolenclosurecandidate](image)

3. Record the serial number of the enclosure, which is needed later. In this case, it is Serial Number F306954 from the `lscontrolenclosurecandidate` command output.

4. Enter the `lsiogrp` command to determine the next I/O group where the enclosure is added, as shown in Figure 5-55. In this example, `io_grp1` is the next available I/O group.

![Figure 5-55 Running CLI command lsiogrp](image)

5. Record the name or ID of the first I/O group that has a node count of zero. You need the ID for the next step.

6. Run 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 (see Figure 5-56).

![Figure 5-56 Running CLI command addcontrolenclosure](image)

7. Run the `lsnodecanister` command to verify that the node canisters in the enclosure are online, as shown in Figure 5-57 on page 147. Repeat the command until the status changes from `adding` to `online`.

![Figure 5-57 Running CLI command lsnodecanister](image)
We use the `chenclosure` command to change the enclosure to become managed. In the following example, we specify that enclosure 2 become managed:

```
chenclosure -managed yes <enclosure_id>
```

- `-managed yes` Changes the enclosure to a managed enclosure.
- `<enclosure_id>` Specifies the enclosure that you want to modify.

```
IBM_FlashSystem:ITSO_FS9100:superuser>chenclosure -managed yes 2
```

### 5.6 Adding an IBM FlashSystem 9100 expansion enclosure

The following types of SAS expansion enclosures are available:

- IBM FlashSystem 9100 SFF Model AFF
- IBM FlashSystem 9100 LFF Model A9F

A single IBM FlashSystem 9100 can support up to 20 AFF expansion enclosures or it can support up to 8 A9F expansion enclosures.

- **Supported Expansion Enclosures and Drives:**
  - 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 and A9F expansions supported
- SAS drives can be TRAID1, DRAID5, or DRAID6, with drives within those arrays being 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 20 expansion enclosures to an IBM 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 IBM FlashSystem 9100 SFF Model AFF

Model AFF expansion enclosure includes the following components:
- A total of 2 expansion canisters
- 12 Gb SAS ports for control enclosure and expansion enclosure attachment
- A total of 24 slots for 2.5-inch SAS SSD drives
- 2U, 19-inch rack mount enclosure with AC power supplies
- A total of 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](image)
The rear view of an AFF expansion enclosure is shown in Figure 5-59.

![Figure 5-59  Rear of IBM 9100 SFF Model AFF expansion enclosure](image)

5.6.2 IBM 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 92 drives that are positioned in four rows of 14 and another three rows of 12 mounted drives assemblies. Two Secondary Expander Modules (SEM) are centrally located in the chassis. One SEM addresses 54 drive ports, and the other SEM 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, which are 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.
5.6.3 SAS chain limitations

When expansion enclosures are attached to the control enclosure, you are not limited by the type of the enclosure (if it meets all generation level restrictions). The only limitation for each SAS chain is its chain weight. Each type of enclosure features the following defined chain weight:

- Enclosures AFF have a chain weight of 1
- Enclosure A9F has a chain weight of 2.5

The maximum chain weight is 10.

For example, you can combine seven AFF and one A9F expansions (7x1 + 1x2.5 = 9.5 chain weight).

5.6.4 Connecting the SAS cables to the expansion enclosures

If you installed expansion enclosures, you must connect them to an IBM FlashSystem 9100 control enclosure.

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 151. Complete the following steps:
   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.

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). Complete the following steps:
   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 more 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 on page 151.

Note: A control enclosure can support up to 20 expansion enclosures (10 that are above the control enclosure and 10 that are below the control enclosure).

4. If more 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 that are attached through iSCSI and Fibre Channel.

The back-end storage subsystem configuration must be planned for all storage controllers that are attached to the IBM FlashSystem 9100.

For more information about supported storage subsystems, see the following resources:

► IBM Support Information for IBM FlashSystem 9100 family
► IBM System Storage Interoperation Center (SSIC)

Apply the following general guidelines for back-end storage subsystem configuration planning:

► In the SAN, storage controllers that are used by the IBM FlashSystem 9100 clustered system must be connected through SAN switches. Direct connection between the IBM FlashSystem 9100 and the storage controller is not supported.

► Enhanced Stretched Cluster configurations have more requirements and configuration guidelines. For more information about performance and preferred practices for the IBM 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 IBM 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.

Observe the following rules:

► Disk drives
  Exercise caution with use of large hard disk drives so that you do not have too few spindles to handle the load.

► Array sizes:
  – IBM FlashSystem 9100 does not queue more than 60 I/O operations per MDisk. Therefore, ensure that the MDisks that are presented to IBM FlashSystem 9100 can handle this many requests, which corresponds to approximately 8 HDDs.
  
If your array can handle higher load, split it into several LUNs of equal size to better match back-end storage capabilities with the load that IBM FlashSystem 9100 can generate.
For more information about back-end storage LUN presentation to IBM FlashSystem 9100, see *IBM System Storage SAN Volume Controller and Storwize V7000 Best Practices and Performance Guidelines*, SG24-7521.

- 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 following general practice guidelines apply:
  - EMC DMX/SYMM, all HDS, and SUN/HP HDS clones use one WWNN per port. Each port appears as a separate controller to the IBM 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 is being virtualized, which 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, click **Pools → External Storage**, as shown in Figure 5-62.

![Figure 5-62 External Storage pane](image)

The pane lists the external controllers that are connected to the IBM 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 show or hide the MDisks that are associated with the controller.

*Note:* A controller that is connected through Fibre Channel is detected automatically by the system, which provides that the cabling, zoning, and system layer are configured correctly. A controller that is connected through iSCSI must be added to the system manually.
If you configured logical unit names on your external storage systems, the system cannot determine this name because it is local to the external storage system. However, you can use the external storage system WWNNs and the LUN to identify each device.

5.7.1 Fibre Channel external storage controllers

A controller that is connected through Fibre Channel is detected automatically by the system, and provides that the cabling, zoning, and system layer are configured correctly.

If the external controller is not detected, ensure that the IBM FlashSystem 9100 is cabled and zoned into the same SAN as the external storage system. If you use 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 IBM 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 must use the command-line interface (CLI).

Ensure that the layer of both systems is correct by running the following command:

```
svcinfo lssystem
```

If needed, change the layer of the IBM FlashSystem 9100 to replication by running the following command:

```
chsystem -layer replication
```

If needed, change the layer of the Storwize controller to storage by running 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 met:

- IBM FlashSystem 9100 and the external storage system are connected through one or more Ethernet switches. Symmetric ports on all nodes of the IBM 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 shows an example of a fully redundant iSCSI connection between IBM FlashSystem 9100 and Storwize systems.

In this example, the IBM 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.

The ports that are used for iSCSI attachment are enabled for external storage connections. By default, Ethernet ports are disabled for external storage connections. You can verify the setting of your Ethernet ports by clicking Settings → Network and selecting Ethernet Ports, as shown in Figure 5-64.
To enable the port for external storage connections, select the port, click **Actions** and then, select **Modify Storage Ports**, as shown in Figure 5-65.

![Figure 5-65  Modifying Ethernet port settings](image)

Set the port as Enabled for either IPv4 or IPv6, depending on the protocol version that is configured for the connection, as shown in Figure 5-66.

![Figure 5-66  Enabling a Storage port](image)

When all prerequisites are fulfilled, you are ready to add the iSCSI controller. To do so, click **Pools** → **External Storage** and then, click **Add External iSCSI Storage**, as shown in Figure 5-67.

![Figure 5-67  Adding external iSCSI storage](image)
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](image)

Select **Convert the system to the replication layer** and click **Next**.

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](image)
Enter the iSCSI connection details, as shown in Figure 5-70.

![Add External iSCSI Storage](image)

**Figure 5-70   Adding an external iSCSI controller: Connection details**

Complete the following fields as described:

- **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.

- **Source port 1 connections:**
  - Select source port 1: Select one of the ports to be used as the 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 that is targeted by this source port.
  - Target port on remote storage 2: Enter the IP address for the other port on the external storage system that is targeted by this source port.

- **Source port 2 connections:**
  - Select source port 2: Select the other port to be used as the 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 that is targeted by this source port.
  - Target port on remote storage 2: Enter the IP address for the other port on the external storage system that is targeted by this source port.
The available fields 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 that is associated with the external storage system. This field is shown only for configurations that use HyperSwap.
- **User name**: Enter the user name that is 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.

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

Several 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](image)

**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**

Selecting *Rename* allows the user to modify the name of an external controller, as shown in Figure 5-72. Enter the new name and click *Rename*.

![Figure 5-72   Renaming an external storage controller](image)

**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 named ABC and an MDisk called ABC, but you cannot have two volumes that are 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 that are 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. Selecting *Modify Site* allows the user to modify the site with which the external controller is associated (see Figure 5-73).

![Figure 5-73   Modifying the site of an external controller](image)
5.8 Adding IBM FlashSystem 9100 to a Storwize V7000 system

If you have a Storwize V7000 system, you can add an IBM FlashSystem 9100 control enclosure to the system. When the IBM FlashSystem 9100 is added, the new system configuration adopts the attributes and supported features of the IBM FlashSystem 9100 system, such as IBM FlashCore Module support.

You must ensure that the Storwize V7000 system has licenses for all licensed functions. Also, if the Storwize V7000 system manages externally virtualized storage, 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 includes an encryption license, the IBM FlashSystem 9100 control enclosure must also have a license before it is added to the Storwize V7000 system. For more information about activating an encryption license on the IBM FlashSystem 9100 control enclosure, see 6.5.6, “Encryption” on page 225.

Note: The Storwize V7000 system must include only models 2076-524 and 2076-624 control enclosures with the same level code as the IBM 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.

Fewer than four control enclosures can be in the system (the maximum for Storwize V7000 and IBM FlashSystem 9100 systems is four control enclosures).

5.8.1 Clustering rules

Consider the following clustering rules:

- Supported cluster with Storwize V7000 and IBM 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 extra I/O Groups
- Default layer is storage, but replication layer is supported

To add an IBM FlashSystem 9100 control enclosure to a Storwize V7000 system, complete the following steps:

1. If your Storwize V7000 system is currently licensed for compression, you must change the compression value to 0 before adding the IBM FlashSystem 9100 control enclosure. On the Storwize V7000 system, you can change the setting in the V7000 management GUI by completing these steps:

   a. Select **Settings → System → Licensed Functions**.
   b. On the Licensed Functions page, change the current setting for Compression to 0.
   c. Click **Apply Changes**.
2. Set Real-time Compression value to 0 on Storwize V7000 system, as shown in Figure 5-74.

![Figure 5-74 Set Real-time Compression value to 0.](image)

On the command-line, you can also issue the `chlicense -compression 0` command.

3. Ensure that the IBM FlashSystem 9100 control enclosure is zoned correctly and is part of the same SAN as the Storwize V7000 system. The IBM SSR installs the IBM FlashSystem 9100 and completes cabling; however, you must complete all SAN configuration before installation and update the network planning sheets.

4. In the Storwize V7000 management GUI, select Monitoring → System. On the System - Overview page, select Add Enclosure. 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 that the new enclosure is cabled correctly. You can also add a new enclosure by selecting Add Enclosure from the System Actions menu.

5. Complete the instructions in the Add Enclosures wizard until the IBM FlashSystem 9100 control enclosure is added to the system.

Post-installation steps
After the IBM FlashSystem 9100 control enclosure is added to the Storwize V7000 system, several post-installation tasks might be necessary to fix potential configuration issues.

Verify that the system attributes updated the status of the system as an IBM FlashSystem 9100 system by completing the following steps:

1. In the Storwize V7000 management GUI, select the help icon and select About FlashSystem 9100. Verify the following attributes to ensure 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 IBM 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 IBM FlashSystem 9100 control enclosures is considered to be an IBM FlashSystem 9100 system.
2. If you did not have any external virtualization licenses on the Storwize V7000 system, no other updates to license settings are necessary.

3. If you have external virtualization licenses on the Storwize V7000 system and contacted your sales team for setting that converted enclosure-based licenses to capacity-based licenses, use those values to update the license settings on the IBM FlashSystem 9100 system. In the V7000 management GUI, select **Settings → System → Licensed Functions** or use the `chlicense` command.
Installing and configuring the IBM FlashSystem 9100 system

This chapter describes the installation and initial configuration of the IBM FlashSystem 9100 system.

This chapter includes the following topics:

- 6.1, “Overview” on page 166
- 6.2, “Installing the hardware” on page 166
- 6.3, “System initialization” on page 198
- 6.4, “Service setup” on page 205
- 6.5, “Initial customer setup” on page 216
6.1 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 these tasks, the customer completes the system setup process by using the management GUI.

6.2 Installing the hardware

Note: The information in this section is intended for IBM authorized service providers only. Customers must consult the terms of their warranty to determine the extent to which they can attempt any IBM FlashSystem hardware installation.

The installation and configuration of the FlashSystem 9100 system is performed by an IBM SSR by using the information in the system planning worksheets that are 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:
- The customer completes the system planning worksheets. The system planning worksheets are available at IBM Knowledge Center.
- Physical site specifications are met, including rack space and power and environmental conditions. For more information, see Chapter 5, “Scaleability” on page 113.
- Ethernet cables that are to be connected to the control enclosure node canister management ports are available.
- 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:

- Notebook
- Ethernet cable to connect notebook Ethernet port to node canister technician port
- Phillips screwdriver
- Flat-head screwdriver

6.2.3 Installing the hardware

The FlashSystem 9100 system consists of a control enclosure and optional SAS expansion enclosures. Complete 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 by using the corresponding instructions as listed in Table 6-1.

<table>
<thead>
<tr>
<th>Enclosure</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control enclosure model A7F/A8F</td>
<td>“Installing the FlashSystem 9100 control enclosure” on page 167</td>
</tr>
<tr>
<td>SAS expansion enclosure model A9F (52U)</td>
<td>“Installing the model A9F expansion enclosure” on page 172</td>
</tr>
<tr>
<td>SAS expansion enclosure model AFF (2U)</td>
<td>“Installing the Model AFF expansion enclosure” on page 186</td>
</tr>
</tbody>
</table>

2. After all of the enclosures in the system are installed, continue with the system installation process that is described in 6.2.4, “Connecting the IBM FlashSystem 9100 components”.

Installing the FlashSystem 9100 control enclosure

In this section, we describe the process that used to install the FlashSystem 9100 enclosure.

Unpacking the control enclosure

Note: 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.

Complete the following steps:

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 is not available, continue by dismantling the control enclosure at step 5. Otherwise, continue the installation (see “Installing support rails for the control enclosure” on page 168).
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 that are provided by the customer for the rack location in which to install the control enclosure.

Complete the following steps:
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](image)

3. Ensure that the appropriate bracket pins are installed in the front and rear bracket of each rail. Each rail includes four medium pins that are 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 includes 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 6-2).

Table 6-2  Selecting bracket pins for the rack

<table>
<thead>
<tr>
<th>Mounting holes</th>
<th>Bracket pins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round, unthreaded</td>
<td>Use the preinstalled medium pins.</td>
</tr>
<tr>
<td>Square</td>
<td>Unscrew the medium pins and replace with the large pins that are supplied with the rails.</td>
</tr>
</tbody>
</table>

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](image)

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](image)

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 on page 169).

10. Secure the rear of the rail to the rear rack flange with two black M5 screws.

11. Repeat step 4 on page 169 - step 10 to install the opposite support rail in the rack.

### Installing the control enclosure in the rack

Complete the following steps:

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, as shown in Figure 6-4.

![Figure 6-4 Removing the control enclosure end caps](image)

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](image)
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, and 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 171. 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. Install 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

**Note:** 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, remove all appropriate subassemblies per instructions to reduce the system weight before you lift this unit.

The model A9F expansion enclosure, front fascia (1U and 4U pieces), cable management arm, and slide rail kit are shipped in one box. The drives for the enclosure are shipped in a separate box.

Complete the following steps:
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 a 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 that are provided by the customer for the rack location in which to install the expansion enclosure.
Complete the following steps:

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 on page 173).

3. Use four M4xL6 screws to attach the inner rail members to the side of the expansion enclosure. The screw locations are shown in Figure 6-9.
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](image)

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](image)

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 that is installed in the rack.

![Figure 6-12 Installed outer rail member](image)

**Installing the model A9F expansion enclosure in the rack**

**Note:** 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 complete 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](image)

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. Complete the following steps to remove the expansion enclosure top cover:
   a. Slide the release latch 1 on the top cover in the direction that is shown in Figure 6-14.

![Figure 6-14 Releasing the expansion enclosure top cover](image)
b. Slide the cover toward the front of the expansion enclosure, as shown in Figure 6-14 on page 176.

c. Carefully lift the cover up, as shown in Figure 6-15.

![Removing the expansion enclosure top cover](image)

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 (see Figure 6-16 on page 178) 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.
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 (see 1 in Figure 6-17 on page 179).

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 (see 2 in Figure 6-17 on page 179).

d. Rotate the handle down to lock the drive assembly into the chassis (3 in Figure 6-17 on page 179).

e. Ensure 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).

7. Complete the following steps to 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 180.
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.

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.

8. Complete the following steps to 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 (see 3 in Figure 6-21).
   b. Push the enclosure firmly into the rack (see 4 in Figure 6-21).
   c. Tighten the locking thumb screws (see 5 in Figure 6-21) to secure the enclosure in 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.

![Figure 6-22 Model A9F expansion enclosure cable arm assemblies](image)

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](image)

Complete the following steps:

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 on page 183 shows the connectors on the upper CMA assembly.
i. Install the inner connector of the upper CMA assembly 1 to the inner member of the left support rail 2 (as shown in Figure 6-25) from the outer and inner support rails.

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.

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 on page 184.
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.

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.
iii. Attach the support rail connector on the lower CMA assembly L1 to the connector on the left support rail L2, as shown in Figure 6-28 on page 184.

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.

Note: Do not connect the power cables to the power source outlets at this time.

Complete the following steps:

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.

b. Ensure that each cable is installed along one of the cable management arms.

11. Install the front fascia panels on the expansion enclosure.

Complete the following steps:

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 shown in Figure 6-30 on page 186, 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

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**

*Note:* Lifting the IBM 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 is not available, continue by dismantling the control enclosure as described in step 6. Otherwise, continue the installation as described in, “Installing support rails for the model AFF expansion enclosure”.

6. By 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 that are provided by the customer for the rack location in which to install the expansion enclosure.

Complete the following steps:

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).

3. Ensure that the appropriate bracket pins are installed in the front and rear bracket of each rail. Each rail includes 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 includes 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

<table>
<thead>
<tr>
<th>Mounting holes</th>
<th>Bracket pins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round, unthreaded</td>
<td>Use the preinstalled medium pins.</td>
</tr>
<tr>
<td>Square</td>
<td>Unscrew the medium pins and replace with the large pins that are supplied with the rails.</td>
</tr>
</tbody>
</table>

4. At each end of the rail, grasp the tab and pull firmly to open the hinge bracket (see Figure 6-32).

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 to secure the rail to the rack cabinet flange (see Figure 6-33).

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 to secure the rail to the rack cabinet flange (see Figure 6-33 on page 188).

10. Secure the rear of the rail to the rear rack flange with two black M5 screws.

11. Repeat step 4 on page 188 - step 10 on page 189 to install the opposite rail in the rack.

**Installing the model AFF expansion enclosure in the rack**

Complete the following steps:

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, and then, clearing the tab on the top of the enclosure (see Figure 6-34).

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 6-34 Removing expansion enclosure end caps

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](image)

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 process at step 7. Otherwise, continue to 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](image)
6.2.4 Connecting the IBM FlashSystem 9100 components

Completed the following steps to connect the IBM FlashSystem 9100 components:

1. If the IBM FlashSystem 9100 system includes optional expansion enclosures, connect the expansion enclosures to the control enclosure by completing the steps that are described in “Connecting the expansion enclosures to the control enclosure” on page 191.

2. Connect the Ethernet cables to the control enclosure by completing the steps that are described in “Connecting Fibre Channel cables to the control enclosure” on page 194.

3. Connect the Fibre Channel cables to the control enclosure by completing the steps that are described in “Connecting Fibre Channel cables to the control enclosure” on page 194.

Connecting the expansion enclosures to the control enclosure

Each FlashSystem 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 more information, see IBM Knowledge Center.

Consider the following guidelines when you are inserting a SAS cable into a 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 into the port gently until it clicks into place. If you feel resistance, the orientation of the cable connector is likely incorrect.
- After it is inserted correctly, a cable connector can be removed only by pulling the tab.

Consider 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 single 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 that are 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 shows a FlashSystem 9100 system with a control enclosure, two model AFF expansion enclosures, and two model A9F expansion enclosures.

To install the SAS cables in a FlashSystem 9100 with expansion enclosures, complete the following steps, while referring to Figure 6-38:

1. Complete the following steps to 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 more expansion enclosures are to be connected to the first SAS chain, complete the following steps for each added 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 in the right canister in the first expansion enclosure in the SAS chain to SAS port 1 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 in the upper node canister to SAS port 1 in the left canister in the first expansion enclosure in the second SAS chain.

   b. Connect SAS port 3 in the lower node canister in the control enclosure to SAS port 1 in the right canister in the first expansion enclosure in the second SAS chain.

   c. If extra expansion enclosures are to be connected to the second SAS chain, complete the following steps for each added expansion enclosure:

      i. Connect SAS port 2 in the left canister of the first expansion enclosure in the SAS chain to SAS port 1 in the left canister in the second expansion enclosure in the SAS chain.

      ii. Connect SAS port 2 in the right canister in the first expansion enclosure in the SAS chain to SAS port 1 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 that are 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 provides connection to the system management interfaces (see Figure 6-39).

![Figure 6-39  Control enclosure Ethernet port locations](image)

2. Connect 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 that are 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 GB Fibre Channel host adapter cards. The first Fibre Channel host adapter in a node canister must be installed in PCIe slot 1. More Fibre Channel host adapters are installed in PCIe slots 2 and 3 in a node canister.

Complete the following steps to connect the Fibre Channel cables to the node canisters:
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. The location of the adapter and port on each adapter are shown in Figure 6-40.

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 IBM FlashSystem 9100

Note: The information in this section is intended only for IBM authorized service providers. Customers must consult the terms of their warranty to determine the extent to which they can attempt any IBM FlashSystem hardware installation.

Complete the following steps to power on the IBM FlashSystem 9100:
1. Power on any model A9F expansion enclosures by completing the steps that are described in “Powering on the model A9F expansion enclosure” on page 194.
2. Power on any mode AFF expansion enclosures by completing the steps that are described in “Powering on the model AFF expansion enclosure” on page 196.
3. Power on the control enclosure by completing the steps that are described in “Powering on the control enclosure” on page 197.

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 (see 4 in Figure 6-41 on page 195). The power supply units are covered by the 1U fascia panel (see 5 in Figure 6-41 on page 195).
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.

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, turn 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 reviewing the following components:
   - On the back of the expansion enclosure, all four fans and the expansion canister indicators (8 and 9 in Figure 6-42 on page 196) become active when the power is connected.
   - On the front of the enclosure, the indicators on the front display panel and each power supply unit (4 and 5 in Figure 6-41) are also lit when the power is connected. For information about the status that is provided by the indicators, see IBM Knowledge Center.
**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, which causes 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, turn 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](image)

The canister is ready with no critical errors when Power is illuminated, Status is on, and Fault is off.

**Powering on the control enclosure**

**Note:** Do not power on the control enclosure with any open drive bays or host adapter slots. Consider the following points:
- 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, which causes 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 are successfully powered up.
2. Connect the power cords that are connected to the rear of the control enclosure to the power sources. If necessary, turn 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 is illuminated green when the power supply is functioning correctly.

![Control enclosure power supply unit rear view](image)

**Figure 6-44  Control enclosure power supply unit rear view**

### 6.3 System initialization

**Note:** The information in this section is intended for IBM authorized service providers only. Customers must consult the terms of their warranty to determine the extent to which they can 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 flashing, and the amber fault LED off.

The system can be configured as the first enclosure in a new system or as an extra enclosure in a system. If you are initializing the first enclosure in a new system, see 6.3.1, “System initialization for first enclosure in a new system”. If you are initializing another enclosure in an existing system, see 6.3.2, “System initialization for extra enclosures in a system” on page 203.

#### 6.3.1 System initialization for first enclosure in a new system

**Note:** Refer to the system planning worksheets that are provided by the customer for the information that is required to initialize the system.

Complete the following steps to initialize the system:

1. Configure the Ethernet port on your notebook to use Dynamic Host Configuration Protocol (DHCP).
2. Connect your notebook’s Ethernet port to the technician port of the upper node canister in the control enclosure (see Figure 6-45).

3. Open a web browser and enter http://install in the URL field.
4. Wait for the System Initialization panel to open (see Figure 6-46).

5. Click Proceed.
The System Initialization Welcome panel opens (see Figure 6-47).

6. Click Next.

The System Initialization Welcome panel opens (see Figure 6-48).

7. Click As the first enclosure in a new system and then, click Next.
8. The System Initialization Create a New System panel opens (see Figure 6-49).

![Figure 6-49 System initialization: Create a New System panel](image)

9. Complete the following steps by enter the information from system planning worksheets (see 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 panel](image)
The Task completed panel opens (see Figure 6-51).

![System initialization task completed panel](image)

**Figure 6-51** System initialization task completed panel

10. Click **Close**.

The System Initialization Restarting Web Server panel opens (see Figure 6-52).

![System initialization restarting web server panel](image)

**Figure 6-52** System initialization restarting web server panel

11. The System Initialization function implements a 5-minute timer to allow the web server to restart. When the timer reaches zero, click **Next** (see Figure 6-53).

![System initialization restarting web server panel that indicates no time remaining](image)

**Figure 6-53** System initialization restarting web server panel that indicates no time remaining

The System Initialization Summary pane is displayed (see Figure 6-54 on page 203).

**Note:** Do **not** disconnect the Ethernet cable connecting your notebook to the technician port on node canister 1.
12. Click **Finish**.

### 6.3.2 System initialization for extra enclosures in a system

Complete the following steps to initialize the system:

1. Configure the Ethernet port on your notebook to use DHCP.

2. Connect your notebook'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](image)

3. Open a web browser and enter `http://install` in the URL field.
4. Wait for the System Initialization panel to open (see Figure 6-56).

![System Initialization pane](image)

Figure 6-56   System initialization pane

5. Click Proceed.

The System Initialization Welcome panel opens (see Figure 6-57).

![System Initialization welcome pane](image)

Figure 6-57   System initialization welcome pane

6. Click Next.
The System Initialization Welcome panel opens (see Figure 6-58).

7. Click **As an additional enclosure in an existing system** and then, click **Next**.
8. The System Initialization Expand System panel opens (see Figure 6-59).

9. The SSR tasks to initialize and set up the system are complete. The required tasks to add the enclosure to a system are completed by the customer. For more information, see Chapter 5, “Scalability” on page 113.

### 6.4 Service setup

**Note:** The information in this section is intended for IBM authorized service providers only. Customers must consult the terms of their warranty to determine the extent to which they can attempt any IBM FlashSystem hardware installation.

Refer to the system planning worksheets that are provided by the customer for the information that is required to set up 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 panel opens (see Figure 6-60).

   ![FlashSystem 9100 Storage Management login panel](image)

   *Figure 6-60  FlashSystem 9100 storage management login panel*

3. Enter password in the Password field and click **Sign In**.
The Welcome to Service Setup panel opens (see Figure 6-61).

4. Click **Next**.
The Email Event Notifications panel opens (see Figure 6-62).

![Email event notifications panel](image)

**Figure 6-62  Email events notifications panel**

5. Select **Yes** or **No** and then, click **Next**.
The System Location panel opens (see Figure 6-63).

![System Location panel](image)

**Figure 6-63  System location panel**

6. Enter the system location information in the fields that are in the panel and click **Next**.
The Contact panel opens (see Figure 6-64).

Figure 6-64  Contact panel

7. Enter the contact information in the fields that are in the panel and click Apply and Next. The Configuring Email Settings status panel opens (see Figure 6-65).

Figure 6-65  Configuring email settings status pane

8. Click Close.
The Email Servers panel opens (see Figure 6-66).

![Email servers panel](image1)

Figure 6-66  Email servers panel

9. Enter the IP address and port of the SMTP server in the **Server IP** and **Port** fields.
10. Click **Ping** to test the connection to the SMTP server.
11. Click **Apply and Next**.
   
The Configuring Email Settings status panel opens (see Figure 6-67).

![Configuring email settings status pane](image2)

Figure 6-67  Configuring email settings status pane

12. Click **Close**.
The Sending Test Email status panel opens (see Figure 6-68).

![Figure 6-68 Sending test email status panel](image)

13. Click **Close**.

The Test Call Home panel opens (see Figure 6-69).

![Figure 6-69 Test call home panel](image)
14. Click **Next**.

The Storage Insights panel opens (see Figure 6-70).

**Note:** Your notebook might not be able to communicate with the internet while it is connected to the technician port on node canister 1. The customer is prompted to set up Storage Insights during the initial customer setup process.

15. Click **Next**.
The Summary panel opens (see Figure 6-71).

![Summary panel](image)

**Figure 6-71  Summary panel**

16. Click **Finish**.

The System Initialization panel opens (see Figure 6-72) in which it is indicated that the task is completed.

![System initialization panel](image)

**Figure 6-72  System initialization panel**

17. Click **Close**.
The Setup Complete panel opens (see Figure 6-73).

![Setup Complete panel](image)

**Figure 6-73** Setup complete panel

18. Click **Close**.

19. Disconnect the Ethernet cable from the technician port on node canister 1 and from your notebook.

The IBM SSR tasks to initialize and set up the system are complete.
6.5 Initial customer setup

Complete the following steps:

1. Open a supported web browser and enter the https://<system management IP address> in the URL field.

2. The FlashSystem 9100 Storage Management login panel opens (see Figure 6-74).

![FlashSystem 9100 storage management login panel](image)

3. Enter password (with a zero) in the Password field and click Sign In.
The Welcome panel opens (see Figure 6-75).

Figure 6-75  Welcome panel

4. Click Next.
6.5.1 Accepting the license agreement

You must read and agree to the terms in the license agreement before continuing, as shown in Figure 6-76.

Figure 6-76  License agreement panel

Complete the following steps:
1. Read the license agreement (see Figure 6-76).
2. Select I agree with the terms in the license agreement.
3. Click Next.
6.5.2 Changing the default password

The Change Password panel (see Figure 6-77) allows you to change the default password.

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 status panel opens (see Figure 6-78).
4. Click **Close**.
6.5.3 Changing the system name

The System Name panel (see Figure 6-79) allows you to specify a name for the system.

![System Name panel](image)

Figure 6-79 System name panel

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 panel opens (see Figure 6-80).

![Modify System Properties status pane](image)

Figure 6-80 Modify system properties status pane

4. Click **Close**.
6.5.4 Configuring licensed functions

Licensed functions must be configured before they can be used. The Licensed Functions panel (see Figure 6-81) allows you to configure the licensed functions. To provide the correct values for the licensed functions, see the licenses feature codes that you purchased. For more information, see “Licensing and features” on page 104.

![Licensed functions panel](image)

**Figure 6-81 Licensed functions panel**

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 Setting the date and time

The date and time can be set manually or by using an NTP server (see Figure 6-82).

![Date and Time panel]

*Figure 6-82  Date and Time panel*
Setting the date and time manually

Complete the following steps:

1. Select **Manually** (see Figure 6-83).

![Figure 6-83 Setting the date and time manually](image)

2. To set the date and time by using your browser settings, select the **Use Browser Settings** option and then, 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**.

   The Change Date and Time Settings status panel opens (see Figure 6-84).

![Figure 6-84 Change date and time setting status panel](image)

4. Click **Close**.
Setting the date and time by using an NTP server

The use of an NTP server to set the date and time is the preferred method. Complete the following steps to set the date and time by using an NTP server:

1. Select **NTP Server** (see Figure 6-85).

   ![Figure 6-85 Setting the date and time by using an NTP server](image)

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**.

   The Change Date and Time Setting status panel opens (see Figure 6-86).

   ![Figure 6-86 Change date and time settings status panel](image)

5. 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 panel (see Figure 6-87) allows you to specify whether the encryption feature was purchased for the system.

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. For more information about how to activate the encryption feature license automatically, see “Activating the encryption feature automatically” on page 225.

For more information about how to activate the encryption feature license manually, see “Activating the encryption feature manually” on page 227.

**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 (see Figure 6-88 on page 226).
2. Select **Actions → Activate License Automatically** (see Figure 6-88 on page 226).
3. In the **Enter the authorization code for control enclosure** field in the Activate License Automatically panel, enter the authorization code that is specific to the control enclosure that you selected (see Figure 6-89).

4. Click **Activate**.
The system connects to IBM to verify the authorization code and retrieves the license key. After the license key is retrieved, it is automatically applied. The Encryption panel is updated to indicate that the encryption feature is licensed (see Figure 6-90).

![Encryption panel that shows feature license](image)

5. 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 (see Figure 6-91 on page 228).
2. Select **Actions → Activate License Manually** (see Figure 6-91 on page 228).
3. In the **Enter the license key** field in the Manual Activation panel, enter the license key for the encryption feature (see Figure 6-92).

![Manual Activation](image)

**Figure 6-92  Manual activation pane with license key entered**
4. Click **Activate**.

   After the activation completes successfully, the Encryption panel is updated to indicate that the encryption feature is licensed (see Figure 6-93).

![Figure 6-93 Encryption panel showing feature licensed](image)

5. Click **Next**.
6.5.7 Changing system location

The system location information was entered by the IBM SSR during service setup. You can change any of the information in the System Location panel (see Figure 6-94).

Figure 6-94  System location panel

Complete the following steps to change the system location:
1. Review the information in the panel and enter any changes in the corresponding fields.
2. Click Next.
6.5.8 Changing contact information

The contact information for the system was entered by the IBM SSR during service setup. You can change any of the information in the Contact panel (see Figure 6-95).

![Contact panel](image)

Figure 6-95  Contact panel

Complete the following steps to change the contact information:

1. Review the information in the widow and enter any changes in the corresponding fields.
2. Click **Next**.

6.5.9 Configuring inventory settings

The call home function regularly sends emails to the IBM support center. The Inventory Settings panel is used to control the information that is included in the emails (see Figure 6-96 on page 232).
Complete the following steps to configure the inventory settings:

1. Select **Off** or **On** to specify whether emails that are sent to the IBM support center contain inventory information.

2. From the **Reporting Interval** list, select the interval that is used to include inventory information in emails sent to the IBM support center.

3. Select **Off** or **On** to specify whether emails sent to the IBM support center contain system configuration information.

4. Select the **Censor sensitive data** option to exclude sensitive entries, such as object names, cloud accounts, network information, certificates, and host and user information from the emails that are sent to IBM support center.

5. Click **Apply and Next**.

   The Updating Call Home Settings panel opens (see Figure 6-97).

---

**Figure 6-96** Inventory settings panel

**Figure 6-97** Updating call home settings status panel
6. Click **Close**.

### 6.5.10 Updating email servers information

The SMTP server IP address that is used by the system was entered by the IBM SSR during the service setup process. You can change the SMTP server IP address in the Email Servers panel (see Figure 6-98).

![Email servers panel](image)

**Figure 6-98**   Email servers panel

Complete the following steps:

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 Getting started with Storage Insights

The Storage Insights panel allows you to get started with Storage Insights (see Figure 6-99). For more information about Storage Insights, see 4.5, “IBM Storage Insights” on page 92.

![Storage Insights panel](image)

Figure 6-99  Storage Insights panel

Complete the following steps:

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** option.

2. Click **Next**.
6.5.12 Configuring support assistance

You can configure local support assistance (where support personnel visit your site to fix problems with the system) or remote support assistance in the Support Assistance panel (see Figure 6-100).

Local and remote support assistance uses secure connections to protect data exchanges between the support center and system. More access controls can be added by the system administrator. For more information, see 4.4.7, “Remote Support Assistance” on page 88.

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 Configuring Support Centers

The Support Centers panel (see 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. For more information, see 4.4.7, “Remote Support Assistance” on page 88.

![Support Centers panel](image1)

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 Configuring remote support access settings

You can configure when support personnel can access your system to conduct maintenance and fix problems by using the Remote Support Access Settings panel (see Figure 6-102).

To configure the remote support access settings, complete the following steps:

1. Select **At Any Time** or **On Permission Only**.
2. Click **Apply and Next**.

   The Enable Support Assistance status panel opens (see Figure 6-103).

3. Click **Close**.
6.5.15 Using the Summary panel

The Summary panel (see Figure 6-104) lists the information that was entered during the initial setup. Change the settings or configuration, click Back. To complete the initial setup, click Finish.

![Summary panel](image1)

In the System Initialization panel (see Figure 6-105), click Close.

![System initialization status panel](image2)
In the Setup Completed panel (see Figure 6-106), click **Close**.

![Setup Completed status panel](image)

*Figure 6-106  Setup Completed status panel*
The Settings section of the IBM FlashSystem 9100 graphical user interface (GUI) and various options for monitoring, configuring interfaces, and extracting support logs also are described in this chapter. Also described is the remote authentication and the firmware update process.

This chapter includes the following topics:

- 7.1, “Settings menu” on page 242
- 7.2, “Notifications menu” on page 242
- 7.3, “Network” on page 247
- 7.4, “Security menu” on page 251
- 7.5, “System menu” on page 270
- 7.6, “Support menu” on page 288
- 7.7, “GUI preferences” on page 295
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 (see Figure 7-1).

![Figure 7-1 Settings menu](image)

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**: The System pane is used to manage overall system configuration options, such as licenses, updates, and date and time settings.
- **Support**: This pane helps to configure and manage connections, and upload support packages to the support center.
- **GUI Preferences**: In this pane, configure welcome message after login, refresh internal cache and inventory, and GUI logout timeouts.

These options are described next.

7.2 Notifications menu

The IBM FlashSystem 9100 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 about the Call Home feature, see 4.4.6, “Call home option” on page 86.

Complete the following steps to view email event notifications:

1. From the IBM FlashSystem 9100 System pane, click **Settings** selection and then, click **Notifications**, as shown in Figure 7-2.

![Figure 7-2   Selecting Notifications in the Settings section](image)
2. Click the **Email** section. The Email settings are displayed, as shown in Figure 7-3.

![Figure 7-3 Email Notification settings](image)

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 that is set to receive one or more email notifications.
- The contact information of the person in the organization who is responsible for the system.
- The 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 IBM FlashSystem 9100.

To view the SNMP configuration, use the System window. Click **Settings** and then, click **Notification** → **SNMP**, as shown in Figure 7-4.

![Setting SNMP server and traps](image)

From this window (see 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 IBM FlashSystem 9100. To view the Syslog configuration, in the System window, click Settings and then, click Notification → Syslog (see Figure 7-5).

![Figure 7-5 Setting Syslog messaging](image)

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)=00000000210000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000#Additional
Data(64-127)=000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000

7.3 Network
This section describes how to view the network properties of the IBM FlashSystem 9100
system. The network information can be obtained by clicking Settings → Network, as shown
in Figure 7-6.

Figure 7-6 Accessing network information

Chapter 7. Configuring settings

247


7.3.1 Management IP addresses

To view the management IP addresses of the IBM FlashSystem 9100, click Settings → Network and then, 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](image)

7.3.2 Service IP information

To view the Service IP information of your IBM FlashSystem 9100, click Settings → Network and then, click the Service IP Address. The GUI shows the service IP address by selecting the network ports, as shown in Figure 7-8.

![Figure 7-8 Viewing service IP address](image)
The service IP address is commonly used to provide access to the network interfaces on each node.

Instead of reaching the Management IP address, the service IP address directly connects to each 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.

![iSCSI Configuration pane](image)

**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 enter 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.

- **iSCSIAliases (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 entire system under the system properties or for each host definition. The CHAP must be identical on the server and the system or host definition. You can create an iSCSI host definition without the use of a CHAP.

7.3.4 Fibre Channel Connectivity information

To view the Fibre Channel Connectivity information of your IBM FlashSystem 9100, click Settings → Network and then, 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

![Fibre Channel Connectivity](image)

*Figure 7-10 Fibre Channel connections*

The Fibre Channel Ports pane displays how the FC port is configured across all control node canisters in the system. For example, this view helps to determine with which other clusters the port is allowed to communicate (see Figure 7-11 on page 251).
7.4 Security menu

Use the Security window (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 who are attempting to access system data and resources. User credentials are managed externally through various supported authentication services, such as LDAP.

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 must configure local credentials. Remote users have their groups defined by the remote authentication service.
Configuring remote authentication
The IBM FlashSystem 9100 supports the following types of LDAP servers:

- IBM Security Directory Server
- Microsoft Active Directory
- OpenLDAP

For more information about remote authentication by using the LDAP, see “Configuring user authentication” in Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1, SG24-7933.

7.4.2 Activating Encryption

To activate encryption on a running system, complete the following steps:

1. Click Settings → System → Licensed Functions.
2. Click Encryption Licenses, as shown in Figure 7-13.
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.
For more information about how to complete an automatic activation process, see “Activating the license automatically” on page 253.

For more information about how to complete a manual activation process, see, “Activating the license manually” on page 255.

After either activation process is complete, you see that a green check mark in the column that is labeled Licensed for the node, as shown in Figure 7-15.

![Figure 7-15 Successful encryption license activation on a running system](image)

### Activating the license automatically

**Important:** To complete this task, the personal computer that is used to connect to the GUI and activate the license must connect to hosts on the internet.

To activate the encryption license for a node automatically, complete the following 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](image)

2. Enter the authorization code that is specific to the node that you selected, as shown in Figure 7-17. Click **Activate**.

![Figure 7-17 Entering an authorization code](image)
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 the process runs successfully, the procedure takes less than 1 minute.

![Activate License Automatically](image)

*Figure 7-18 Activating encryption*

The license key is automatically applied after is retrieved, as shown in Figure 7-19.

![Encryption Licenses](image)

*Figure 7-19 Successful encryption license activation*

**Problems with automatic license activation**

If connection 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 IBM FlashSystem 9100 Controller GUI and activate the license can access the internet. If you cannot complete the automatic activation procedure, attempt to use the manual activation procedure that is described in “Activating 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 use each of them only 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](image)

**Activating the license manually**

To manually activate the encryption license for a node, complete the following steps:

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](image)

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 manually, pasting it, 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](image)

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](image)
Problems with manual license activation

Although authorization codes and encryption license keys use the same format (four groups of four hexadecimal digits), you can use each of them only 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](image)

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 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.

Consider the following points regarding the key server and USB flash drive characteristics that 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; that is, Key Management Interoperability Protocol (KMIP), that aids in interoperability
  - Ability to audit operations that are 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 is successfully activated, encryption can be enabled. You can enable encryption after the initial system setup is done by using the GUI or CLI. The GUI can be used to start the Enable Encryption wizard by clicking **Run Task** that is 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](image)

You can also click **Settings → Security → Encryption** and then, click **Enable Encryption**, as shown in Figure 7-26.

![Figure 7-26 Enable Encryption from the Security pane](image)
The Enable Encryption wizard starts by prompting you which encryption key provider to use for storing the encryption keys, as shown in Figure 7-27. You can enable either or both providers.

Next, we present a scenario in which both encryption key providers are enabled at the same time.

For more information about how to enable encryption by using only USB flash drives, see “Enabling encryption by using USB flash drives” on page 259.

For more information about, see how to enable encryption by using key servers as the sole encryption key provider, see “Enabling encryption by using key servers” on page 264.

**Enabling encryption by using USB flash drives**

**Note:** The system needs at least three USB flash drives to be present before you can enable encryption by 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.

The use of 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 attempts 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 invalid, 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 a risk of unauthorized access exists, 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 that are 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 extra 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 more resilience and mitigate the risk that the USB drives that are 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 restart or power loss. No USB flash drive is required during a warm restart, such as a node that is exiting service mode or a single node restart. The data center power-on procedure must 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 the failure of a node, node's USB port, or USB flash drive during the power-on procedure.
To enable encryption by using USB flash drives as the only encryption key provider, complete the following 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](image)

*Figure 7-28  Selecting USB flash drives in the Enable Encryption wizard*

If fewer than three USB flash drives are inserted into the system, you are prompted to insert more drives, as shown in Figure 7-29. The system reports how many more drives must be inserted.

![Figure 7-29](image)

*Figure 7-29  Waiting for USB flash drives to be inserted*
2. Insert the USB flash drives into the USB ports, as required.

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.

![Enable Encryption](image)

**Figure 7-30  Writing the master access key to USB flash drives**

You can continue to add USB flash drives or replace the flash drives that are plugged in to create copies. When complete, click **Next**.
3. The number of keys that were created is shown in the Summary tab, as shown in Figure 7-31. Click Finish to finalize the encryption enablement.

![Figure 7-31 Commit the encryption enablement](image)

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 by using USB flash drives](image)
4. You can confirm that encryption is enabled and verify which key providers are in use by selecting **Settings → Security → Encryption**, as shown in Figure 7-33.

![Encryption view showing by using USB flash drives as the enabled provider](image)

**Figure 7-33** Encryption view showing by using USB flash drives as the enabled provider

**Enabling encryption by using key servers**

A key server is a centralized system that receives and then distributes encryption keys to its clients, including IBM FlashSystem 9100 systems.

For more information about how to enable encryption by using key servers, see the topic “Encryption” in *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933.

**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, which are identified by their **root** certificate. The root certificate must be included in this list for the signed certificate to be trusted. If it is not, the browser presents security warnings.
To see more information about your current system certificate, click **Settings → Security** and then, select **Secure Communications**, as shown in Figure 7-34.

![Figure 7-34 Accessing the Secure Communications window](image)

The IBM FlashSystem 9100 allows you to configure a signed certificate or generate a new self-signed certificate.
Configuring a signed certificate

Complete the following steps to configure a signed certificate:

1. Select **Update Certificate** in the Secure Communications window.
2. Select **Signed certificate** and enter the information about the new certificate signing request. All fields are mandatory, except for the email address. Figure 7-35 shows some values as an example.

![Image of Update Certificate window](image)

**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 informs you that an outstanding certificate request exists, as shown in Figure 7-36. This issue persists until the associated signed certificate is installed.

![Figure 7-36 Outstanding certificate request](image)

**Attention:** If you must update a field in the certificate request, you can generate a new request. However, do *not* generate a new request after the original request is sent to the certificate authority. Generating a new request overrides the original request and the signed certificate that is associated with the original request *cannot* be installed.

5. Submit the request to the certificate authority to receive a signed certificate.

6. When you receive the signed certificate, select **Update Certificate** in 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](image)

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](image)
Generating a self-signed certificate
Complete the following steps to generate a self-signed certificate:

1. Select **Update Certificate** in the Secure Communications window.

2. Select **Self-signed certificate** and enter the information about the new certificate. Key type and validity days are the only mandatory fields. Figure 7-39 shows some values as an example.

**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.

![Figure 7-39](image)

Click **Update**.
3. You are prompted to confirm the action, as shown in Figure 7-40. Click Yes to proceed. The self-signed certificate is generated immediately.

![Certificate update warning](image)

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, download software upgrade packages, and work with licensing options, VMware VVOLs and IP Quorum, DNS settings, and Transparent Cloud Tiering.

#### 7.5.1 Date and time

Complete the following steps to view or configure the date and time settings:

1. From the IBM FlashSystem 9100 System pane, click Settings and then, click System.
2. In the left column, select Date and Time, as shown in Figure 7-41.

![Date and Time window](image)

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 IBM FlashSystem 9100 system with your local workstation date and time.

   ![Figure 7-42 Set Date and Time window](image)

   ![Figure 7-43 Set NTP Server IP Address window](image)

   - 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.

4. Click *Save*.

### 7.5.2 Licensed Functions

The IBM FlashSystem 9100 supports an all-inclusive licensing model. For more information, see 4.7, “Licensing and features” on page 104.

The system supports 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) that are purchased. With other functions applicable to externally virtualized storage, such as 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 IBM FlashSystem 9100 Settings menu, click Settings and then, click System.
2. In the left column, select License Functions, as shown in Figure 7-44.

![Figure 7-44 Licensing window](image)

3. In the Licensed Functions pane, you can set the licensing options for the IBM FlashSystem 9100 for the following elements (limits are in TiB):

   - **External Virtualization**
     Enter the number of SCU units that are associated to External Virtualization for your IBM FlashSystem 9100 environment.

   - **FlashCopy Limit**
     Enter the capacity that is available for FlashCopy mappings, which is 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, which is 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 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 by using the authorization code. The authorization code is sent with the licensed function authorization documents that you receive after purchasing the license.

     For more information about encryption activation, see “Activating Encryption” on page 252.

     Encryption is activated on a per system basis. Figure 7-45 on page 273 shows encryption licenses activated on the IBM FlashSystem 9100.
7.5.3 Updating the system

This section describes the operations to update your IBM 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 updating

This section describes the precautions that you should take before you attempt an update.

**Important:** Before you attempt any IBM FlashSystem 9100 code update, read and understand the IBM FlashSystem 9100 concurrent compatibility and code cross-reference matrix. For more information, see this [website](#) and click Latest FlashSystem 9100 code.

During the update, each node in your IBM FlashSystem 9100 clustered system is automatically shut down and restarted by the update process. Because each node that is in an I/O Group provides an alternative path to volumes, use the Subsystem Device Driver (SDD) to ensure 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 IBM FlashSystem 9100 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 an IBM FlashSystem 9100 software utility that checks for known issues that can cause problems during an IBM FlashSystem 9100 software update. For more information about the utility, see this [IBM Support web page](#).

Download the software update utility from this web page where you can also download the firmware. This procedure ensures that you receive 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 task by 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 no new releases of the utility were made available since it was originally downloaded.

The installation and use of this utility is nondisruptive, and does not require restarting any IBM FlashSystem 9100 nodes. Therefore, no interruption to host I/O occurs. The utility is installed on the current configuration node only.

System administrators must continue to check whether the version of code that they plan to install is the latest version. For more information, see this IBM Support web page.

This utility is intended to supplement rather than duplicate the tests that are performed by the IBM FlashSystem 9100 update procedure (for example, checking for unfixed errors in the error log).

A concurrent software update of all components is supported through the standard Ethernet management interfaces. However, most of the configuration tasks are restricted during the update process.

**Updating IBM FlashSystem 9100 software**

To update the IBM FlashSystem 9100 software, complete the following steps:

1. Open a supported web browser and browse to your cluster IP address. A login window opens (see Figure 7-46).

![Figure 7-46 IBM FlashSystem 9100 GUI login window](image)
2. Log in by using superuser rights. The IBM FlashSystem 9100 management home window opens. Click **Settings → System** (see Figure 7-47).

![Figure 7-47 Settings menu](image)

3. In the System menu, click **Update System**. The Update System window opens (see Figure 7-48).

![Figure 7-48 Update System window](image)

4. From this window, you can select to run the update test utility and continue with the code update or run only the test utility. For this example, we click **Test & Update**.
If you downloaded both files from this IBM Support web page, you can click each folder icon, browse to the location where you saved the files, and upload them to the IBM FlashSystem 9100. If the files are correct, the GUI detects and updates the target code level, as shown in Figure 7-49.

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.

See this web page (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.

5. If you downloaded both files from this IBM Support web page, you can click each folder icon, browse to the location where you saved the files, and upload them to the IBM FlashSystem 9100. 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 Test utility and Update Package](image)

6. Select the type of update you want to perform, as shown in Figure 7-50. Select Automatic update unless IBM Support suggested a Service Assistant Manual update. The manual update might be preferable in cases where malfunctioning host multipathing is known to cause loss of access. Click Next to begin the update package upload process.

![Figure 7-50  Selecting update type](image)
Another window opens in which you can choose a fully automated update, one that pauses when half the nodes completed the update, or one that pauses after each node update, as shown in Figure 7-51. The pause options require you to click **Resume** to continue the update after each pause. Click **Finish**.

![Figure 7-51  Update System options](image)

After the update packages are 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.

7. Click **Update System** to return to the Update System window. Then, click **Read more** (see Figure 7-52).

![Figure 7-52  Issues that are detected by the update test utility](image)
The results pane opens and shows any issues that were detected (see Figure 7-53).

![Update Test Utility Results](image1)

**Figure 7-53**  Description of the warning from the test utility

In our case, the warning is that we have a potential unsupported character as part of our cluster name. Although this condition is not recommended, it does not prevent the system update from running. Therefore, click **Close** and proceed with the update. However, you might need to contact IBM Support to assist with resolving more serious issues before continuing.

8. Click **Resume** in the Update System window and the update proceeds, as shown in Figure 7-54.

![Update System](image2)

**Figure 7-54**  Resuming the update
9. Because of the utility detecting issues, another warning is displayed to ensure that you 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](image)

10. 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](image)

After a 30-minute pause to ensure that multipathing recovered on all attached hosts, a node failover occurs and you temporarily lose connection to the GUI. A warning window displays, in which you are prompted 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 the use of the GUI.
We now see the status of the second node updating, as shown in Figure 7-57.

![Figure 7-57  New GUI after node failover](image)

After the second node completes, the update is committed to the system, as shown in Figure 7-58.

![Figure 7-58  Updating system level](image)

The update process completes when all nodes and the system unit are committed. The final status indicates the new level of code that is installed in the system, as shown in Figure 7-59.

![Figure 7-59  New level of installed software shown](image)
Updating IBM FlashSystem 9100 drive code

After completing the IBM FlashSystem 9100 software update as described in “Updating IBM FlashSystem 9100 software” on page 274, update the firmware of the IBM FlashSystem 9100 drives, if available.

Because multiple models and types of drives are supported by the IBM FlashSystem 9100, the process that is used to update these drives differs from previous IBM FlashSystems and IBM Storwize platforms. For more information about how to update drive firmware code, see IBM Knowledge Center.

Manually updating an IBM FlashSystem 9100 scale-out configuration

In this example, we assume that you have a four-system cluster of the IBM FlashSystem 9100, as listed in Table 7-1.

Table 7-1  The iogrps

<table>
<thead>
<tr>
<th>iogrps (0)</th>
<th>iogrps (1)</th>
<th>iogrps (2)</th>
<th>iogrps (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>node 1 (config node)</td>
<td>node 3</td>
<td>node 5</td>
<td>node 7</td>
</tr>
<tr>
<td>node 2</td>
<td>node 4</td>
<td>node 6</td>
<td>node 8</td>
</tr>
</tbody>
</table>

After uploading the update utility test and software update package to the cluster by 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 iogrps 0, by using 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 downloaded and saved to your PC.
5. Upload the code and click Update.
   
   When the update is completed, a message caption is displayed that indicates that software update completed. The node then reverts, 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 the cluster GUI or the CLI.
8. Select node 3 from iogrps 1.
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 iogrps 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 iogrps 3.
13. Repeat steps 1 - 7 to remove node 7, update it manually, verify the code, and add it back to the cluster.

**Note:** At this point, the update process is 50% completed. You now have one node from each iogrps that is updated with the new code manually. Always leave the configuration node for last during a manual software update.
14. 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. 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, which keeps the cluster manageable.

   The removed configuration node becomes candidate, and you do not have to apply the code update manually. Add the node back to the cluster. It automatically updates 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 approximately 30 minutes to complete.

   The update is complete.

### 7.5.4 VMware virtual volumes

The IBM FlashSystem 9100 can manage VMware vSphere VVOLs directly in cooperation with VMware. It enables VMware virtual machines to get assigned disk capacity directly from the IBM FlashSystem 9100 rather than from the ESXi data store. That technique enables storage administrators to control the appropriate usage of storage capacity. It also enables enhanced features of storage virtualization directly to the virtual machine (such as replication, thin-provisioning, compression, and encryption).

VVOL management is enabled in the IBM FlashSystem 9100 by clicking **Settings → System → VVOL**, as shown in Figure 7-60 on page 283. 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 IBM FlashSystem 9100.

**Restriction:** You cannot enable VVOLs support until the NTP server is configured in the IBM FlashSystem 9100.
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.

For more information, see *Configuring VMware Virtual Volumes for Systems Powered by IBM Spectrum Virtualize*, SG24-8328.

### 7.5.5 IP Quorum

Because enhanced stretched systems can use an IP-based quorum application as the quorum device for the third site, 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.
2. Click **Download IPv4 Application** and the IBM FlashSystem 9100 generates an IP Quorum Java application, as shown in Figure 7-62. The application can be saved and installed in a host that is to run the IP quorum application.

![IP Quorum Java Application](image)

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 a physical port and a virtual port.

When port virtualization is enabled, ports are not available until they are ready to handle I/O, which improves host behavior around node unpends. In addition, path failures that are the result of an offline node are masked from hosts.

The target port mode on the I/O group indicates the following 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 physical Fibre Channel and virtual ports that are 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 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.

![I/O Groups port virtualization](image)

**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.

![Changing port mode](image)

**Figure 7-64  Changing port mode**

### 7.5.7 Domain name server

The IBM FlashSystem 9100 allows domain name server (DNS) entries to be manually set up. The information about the DNS servers in the IBM FlashSystem 9100 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 IBM FlashSystem 9100, 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 IBM FlashSystem 9100 supports up two DNS Servers, IPv4 or IPv6 (see Figure 7-65 on page 286).
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 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 access cloud storage to copy data to the cloud storage or restore data that was 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.
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 IBM FlashSystem 9100 Settings pane, click **Settings** and then, click **System**. Select **Transparent Cloud Tiering** (see Figure 7-66).

![Figure 7-66  Transparent Cloud Tiering settings](image)

By 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 the following 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 more information about how to configure and enable Transparent Cloud Tiering, see *Implementing the IBM System Storage SAN Volume Controller with IBM Spectrum Virtualize V8.1*, SG24-7933.

**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, ensure that the encryption licenses are properly installed and that encryption is enabled.
7.5.9 Updating FlashSystem 9100 drive code

After completing the FlashSystem 9100 software update as described in “Updating IBM FlashSystem 9100 software” on page 274, also update the firmware of the FlashSystem 9100 drives, if available.

Because multiple models and types of drives are supported by the IBM FlashSystem 9100, the update of these drives differs from previous IBM FlashSystems and IBM Storwize platforms. For more information about how to update drive firmware code, see IBM Knowledge Center.

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: Support Assistance and Support Package. Both options are described next.

7.6.1 Support Assistance

This option enables support personnel to access the system to complete troubleshooting and maintenance tasks. You can configure local support assistance, where support personnel access your site to fix problems with the system, or remote support assistance.

Local and remote support assistance uses secure connections to protect data that is exchanged between the support center and system. More access controls can be added by the system administrator.

For more information about Support Assistance, refer to 4.4.7, “Remote Support Assistance” on page 88.
To configure Support Assistance, click **Settings → Support → Support Assistance**, as shown in Figure 7-67.

![Remote Support Assistance menu](image)

**Figure 7-67  Remote Support Assistance menu**

Click **Set Up Support Assistance**, which opens a wizard to guide you through the configuration. Complete the following steps:

1. Figure 7-68 on page 290 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 the **I want support personnel to work on-site only** option 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, in which IBM diagnoses your problem and sends a replacement component for you to replace, if required.

   If you prefer to have IBM perform replacement tasks for you, contact your local sales person for more information about upgrading your current maintenance contract.
2. The next window (see Figure 7-69) lists IBM Support Center’s IP addresses and SSH port that must be opened in your firewall. You can also define a Remote Support Assistance Proxy if you have multiple IBM FlashSystem 9100s or Spectrum Virtualize systems in the data center, which allow for firewall configuration being required only 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 click Next.
3. The next window prompts if you want to open a tunnel to IBM permanently, which allows IBM to connect to your IBM FlashSystem 9100 *At Any Time*, or *On Permission Only*, as shown in Figure 7-70. The *On Permission Only* option requires a storage administrator to log on to the GUI and enable the tunnel when required. Click *Finish*.

![Remote Support wizard access choice](image)

Figure 7-70 Remote Support wizard access choice

4. After completing the remote support setup, you can view the status of any remote connection, start a new session, and reconfigure the setup, as shown in Figure 7-71. Click *Start New Session* to open a tunnel connection to IBM.

![Remote Support Status and session management](image)

Figure 7-71 Remote Support Status and session management
5. A pop-up window prompts you for how long you want the tunnel to remain open if no activity is detected by setting a timeout value. As shown in Figure 7-72, the connection is established and waits for IBM Support to connect.

![Support Assistance](image)

Figure 7-72  Remote Assistance tunnel connected

### 7.6.2 Support package

If support assistance is configured on your systems, you can automatically or manually upload new support packages to the support center to help analyze and resolve errors on the system.

Occasionally, if you encounter a problem and call IBM Support Center, they most likely ask you to provide a support package. You can collect and upload this package by clicking **Settings → Support**.
Collecting and uploading information by using the GUI

To collect information by using the GUI, complete the following steps:

1. Click **Settings → Support** and then, the **Support Package** tab (see Figure 7-73).
2. Click **Upload Support Package**.

![Figure 7-73 Support Package option](image)

**Note:** To upload support packages, a DNS server must be configured on the system.

It is important to select the correct option. In our example, we assume that the problem encountered was an unexpected node restart that 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 restarts, 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 occurred. Collecting a snap type 4 creates 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 were contacted by IBM Support because your system was calling home or you manually opened a call with IBM Support, you are given a PMR number. Enter that PMR number in the PMR field and select the snap type (often referred to as an option 1, 2, 3, 4 snap), as requested by IBM Support (see Figure 7-74). In our example, we enter our PMR number, select snap type 3 (option 3) because it automatically collects the statesave that was created at the time the node restarted, and click Upload.

**Tip:** You can open a service request online at this website.

![Upload Support Package window](image1)

4. The procedure to generate the snap on a IBM FlashSystem 9100 system, including the most recent statesave from each node canister, starts. This process might take a few minutes (see Figure 7-75).

![Task detail window](image2)
7.7 GUI preferences

As shown in Figure 7-76, the GUI Preferences menu consists of the following options:

- Login Message
- General

![GUI Preferences](image)

Figure 7-76   GUI Preferences

7.7.1 Login Message option

The IBM FlashSystem 9100 enables administrators to configure the welcome banner (login message). This message is a text message that appears in the GUI login window or at the CLI login prompt.

The content of the welcome message is helpful when you must 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** (see Figure 7-77).

![Login Message](image)

Figure 7-77   Enabling login message
The result of the action before the log in message that is shown in Figure 7-77 is shown in Figure 7-78. The system shows the welcome message in the GUI before login.

![Welcome message in GUI](image)

*Figure 7-78  Welcome message in GUI*

Figure 7-79 shows the welcome message as it appears in the CLI.

![Welcome message in CLI](image)

*Figure 7-79  Welcome message in CLI*
7.7.2 General window

The General window allows the user to refresh the GUI cache, set the low graphics mode option, and enable advanced pools settings.

From the IBM FlashSystem 9100 Settings tab, click **GUI Preferences**, and then, click **General** (see Figure 7-80).

![General GUI Preferences window](image)

The following elements can be configured:

- **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 log out time in minutes after inactivity in the established session.**
Hints and tips

This chapter provides helpful hints and tips to explore more the capabilities that are offered by IBM FlashSystem 9100.

This chapter includes the following topics:

- 8.1, “Configuring IBM FlashSystem 9100 for SAN Volume Controller” on page 300
- 8.2, “General setup guidelines” on page 300
- 8.3, “Performance data and statistics gathering” on page 301
- 8.4, “Command-line hints” on page 315
- 8.5, “Call Home process” on page 329
- 8.6, “Service support” on page 330
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 or the Storwize family. Whether you have a heterogeneous, older 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, see this web page.

However, the IBM FlashSystem 9100 can be configured as an external storage controller to a SAN Volume Controller cluster.

For IBM SAN Volume Controller clients that appreciate the flexibility that is offered by SAN Volume Controller with features, such as Standby Storage Engine (also known as Standby Node) and Enhanced Stretched Cluster and want to introduce a flash tier into the SAN Volume Controller cluster, the IBM FlashSystem 9100 is a valuable option.

IBM SAN Volume Controller Standby Storage Engine in a SAN provides another node that is not a part of any cluster, but is a candidate and can 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 IBM FlashSystem 9100 or any other Storwize offering.

Note: HyperSwap is an alternative on the Storwize and IBM 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 SAN Volume Controller, 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 are provisioned to the SAN Volume Controller, but more is better. Approximately 30 volumes unlock the maximum performance.

Based on your goals, the following options are available:

- Performance Optimized

In this scenario, it is recommended to configure the Storage Pool at the SAN Volume Controller layer as a standard pool with no compression and present over-allocated capacity in the IBM FlashSystem 9100 to SAN Volume Controller. Hardware compression is made at the IBM FlashSystem 9100 layer and Data Reduction Pool (DRP) is recommended in the IBM FlashSystem 9100.

This option requires careful monitoring of capacity to not run out of space. For that reason, it is recommended to create a sacrificial, fully allocated volume as reserved space for more capacity protection.
Capacity Optimized

In this scenario, it is recommended to configure the Storage Pool at the SAN Volume Controller layer as a DRP so you can use deduplication and compression. Even if you decide to have only deduplication on, it is recommended to configure those volumes as compressed as well, meaning a deduplicated volume should always be compressed. This configuration provides a higher data reduction ratio. In the IBM FlashSystem 9100, it is recommended to use Traditional Storage Pool with fully allocated volumes.

This option offers simple capacity monitoring at the SAN Volume Controller level with lower risk of running out of space. You might consider also creating a sacrificial fully allocated volume as reserved space for more 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 more information about 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 and 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 infrastructure, you must consider many factors in terms of their potential effect on performance. These factors include, but are not limited to, dissimilar workloads that are 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 can lead to I/O bottlenecks. This suggestion also assumes a core-edge design, where the hosts are on the edges and the IBM 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 IBM FlashSystem 9100 clusters that are 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 IBM 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 by 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 IBM FlashSystem 9100 ports. The IBM 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 gives 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 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 approximately 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 IBM 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 four I/O group IBM FlashSystem 9100 cluster.

Consider 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 occurs 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 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, use the `svctask cpdumps` command.

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>`. Consider the following examples:

- 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
...

**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 the following example:

```
C:\>pscp -unsafe -load ITSO_FS9100 superuser@9.19.91.95:/dumps/iostats/* c:\statsfiles
```

Consider the following points:

- Specify the `-unsafe` parameter when you use wildcards.
- Use the `-load` parameter to specify the session that is defined in PuTTY.

**The qperf utility**

The `qperf` utility 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* by using the CLI and a UNIX Korn shell (it can also be used with Cygwin on Windows platforms).

You can download `qperf` from [this web page](#).

The performance statistics files are in `.xml` format. They can be manipulated by using various tools and techniques.
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 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  Output of `lsnodecanisterstats` command

```plaintext
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
....
```

The example 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 use of the `lssystemstats` command lists the same set of statistics that is listed by using the `lsnodestats` command, but represents 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.

<table>
<thead>
<tr>
<th>stat_name</th>
<th>stat_current</th>
<th>stat_peak</th>
<th>stat_peak_time</th>
</tr>
</thead>
<tbody>
<tr>
<td>compression_cpu_pc</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>cpu_pc</td>
<td>1</td>
<td>1</td>
<td>180929125231</td>
</tr>
<tr>
<td>fc_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>fc_io</td>
<td>10</td>
<td>11</td>
<td>180929125146</td>
</tr>
<tr>
<td>sas_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>sas_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>iscsi_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>iscsi_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>write_cache_pc</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>total_cache_pc</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>drive_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>drive_io</td>
<td>0</td>
<td>5</td>
<td>180929125211</td>
</tr>
<tr>
<td>drive_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_r_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_r_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_r_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_w_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_w_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>vdisk_w_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_r_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_r_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_r_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_w_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_w_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>mdisk_w_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>drive_r_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>drive_r_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>drive_r_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>drive_w_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>drive_w_io</td>
<td>0</td>
<td>5</td>
<td>180929125211</td>
</tr>
<tr>
<td>drive_w_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>power_w</td>
<td>766</td>
<td>766</td>
<td>180929125231</td>
</tr>
<tr>
<td>temp_c</td>
<td>22</td>
<td>22</td>
<td>180929125231</td>
</tr>
<tr>
<td>temp_f</td>
<td>71</td>
<td>71</td>
<td>180929125231</td>
</tr>
<tr>
<td>iplink_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>iplink_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>iplink_comp_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>cloud_up_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>cloud_up_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>cloud_down_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>cloud_down_ms</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>iser_mb</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
<tr>
<td>iser_io</td>
<td>0</td>
<td>0</td>
<td>180929125231</td>
</tr>
</tbody>
</table>
The counters that are presented by the `lssystemstats` and `lsnodestats` commands are listed in Table 8-1.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>compression_cpu_pc</td>
<td>Displays the percentage of allocated CPU capacity that is used for compression.</td>
</tr>
<tr>
<td>cpu_pc</td>
<td>Displays the percentage of allocated CPU capacity that is used for the system.</td>
</tr>
<tr>
<td>fc_mb</td>
<td>Displays the total number of megabytes that is 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.</td>
</tr>
<tr>
<td>fc_io</td>
<td>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.</td>
</tr>
<tr>
<td>sas_mb</td>
<td>Displays the total number of megabytes that is 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.</td>
</tr>
<tr>
<td>sas_io</td>
<td>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.</td>
</tr>
<tr>
<td>iscsi_mb</td>
<td>Displays the total number of megabytes that is transferred per second for iSCSI traffic on the system.</td>
</tr>
<tr>
<td>iscsi_io</td>
<td>Displays the total I/O operations that are transferred per second for iSCSI traffic on the system.</td>
</tr>
<tr>
<td>write_cache_pc</td>
<td>Displays the percentage of the write cache usage for the node.</td>
</tr>
<tr>
<td>total_cache_pc</td>
<td>Displays the total percentage for the write and read cache usage for the node.</td>
</tr>
<tr>
<td>vdisk_mb</td>
<td>Displays the average number of megabytes transferred per second for read and write operations to volumes during the sample period.</td>
</tr>
<tr>
<td>vdisk_io</td>
<td>Displays the average number of I/O operations that are transferred per second for read and write operations to volumes during the sample period.</td>
</tr>
<tr>
<td>vdisk_ms</td>
<td>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.</td>
</tr>
<tr>
<td>mdisk_mb</td>
<td>Displays the average number of megabytes that is transferred per second for read and write operations to MDisks during the sample period.</td>
</tr>
<tr>
<td>mdisk_io</td>
<td>Displays the average number of I/O operations that are transferred per second for read and write operations to MDisks during the sample period.</td>
</tr>
<tr>
<td>mdisk_ms</td>
<td>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.</td>
</tr>
<tr>
<td>drive_mb</td>
<td>Displays the average number of megabytes that is transferred per second for read and write operations to drives during the sample period.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>drive_io</td>
<td>Displays the average number of I/O operations that are transferred per second for read and write operations to drives during the sample period.</td>
</tr>
<tr>
<td>drive_ms</td>
<td>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.</td>
</tr>
<tr>
<td>vdisk_w_mb</td>
<td>Displays the average number of megabytes that is transferred per second for read and write operations to volumes during the sample period.</td>
</tr>
<tr>
<td>vdisk_w_io</td>
<td>Displays the average number of I/O operations that are transferred per second for write operations to volumes during the sample period.</td>
</tr>
<tr>
<td>vdisk_w_ms</td>
<td>Displays the average amount of time in milliseconds that the system takes to respond to write requests to volumes over the sample period.</td>
</tr>
<tr>
<td>mdisk_w_mb</td>
<td>Displays the average number of megabytes that is transferred per second for write operations to MDisks during the sample period.</td>
</tr>
<tr>
<td>mdisk_w_io</td>
<td>Displays the average number of I/O operations that are transferred per second for write operations to MDisks during the sample period.</td>
</tr>
<tr>
<td>mdisk_w_ms</td>
<td>Displays the average amount of time in milliseconds that the system takes to respond to write requests to MDisks over the sample period.</td>
</tr>
<tr>
<td>drive_w_mb</td>
<td>Displays the average number of megabytes that is transferred per second for write operations to drives during the sample period.</td>
</tr>
<tr>
<td>drive_w_io</td>
<td>Displays the average number of I/O operations that are transferred per second for write operations to drives during the sample period.</td>
</tr>
<tr>
<td>drive_w_ms</td>
<td>Displays the average amount of time in milliseconds that the system takes to respond write requests to drives over the sample period.</td>
</tr>
<tr>
<td>vdisk_r_mb</td>
<td>Displays the average number of megabytes that is transferred per second for read operations to volumes during the sample period.</td>
</tr>
<tr>
<td>vdisk_r_io</td>
<td>Displays the average number of I/O operations that are transferred per second for read operations to volumes during the sample period.</td>
</tr>
<tr>
<td>vdisk_r_ms</td>
<td>Displays the average amount of time in milliseconds that the system takes to respond to read requests to volumes over the sample period.</td>
</tr>
<tr>
<td>mdisk_r_mb</td>
<td>Displays the average number of megabytes that is transferred per second for read operations to MDisks during the sample period.</td>
</tr>
<tr>
<td>mdisk_r_io</td>
<td>Displays the average number of I/O operations that are transferred per second for read operations to MDisks during the sample period.</td>
</tr>
<tr>
<td>mdisk_r_ms</td>
<td>Displays the average amount of time in milliseconds that the system takes to respond to read requests to MDisks over the sample period.</td>
</tr>
<tr>
<td>drive_r_mb</td>
<td>Displays the average number of megabytes that is transferred per second for read operations to drives during the sample period.</td>
</tr>
<tr>
<td>drive_r_io</td>
<td>Displays the average number of I/O operations that are transferred per second for read operations to drives during the sample period.</td>
</tr>
<tr>
<td>drive_r_ms</td>
<td>Displays the average amount of time in milliseconds that the system takes to respond to read requests to drives over the sample period.</td>
</tr>
</tbody>
</table>
Real-time performance statistics monitoring by using 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 and Figure 8-3 on page 312.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iplink_mb</td>
<td>The total number of megabytes that is transferred per second for Internet Protocol (IP) replication traffic on the system. This value does not include iSCSI host I/O operations.</td>
</tr>
<tr>
<td>iplink_comp_mb</td>
<td>Displays the average number of compressed MBps over the IP replication link during the sample period.</td>
</tr>
<tr>
<td>iplink_io</td>
<td>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.</td>
</tr>
<tr>
<td>cloud_up_mb</td>
<td>Displays the average number of Mbps for upload operations to a cloud account during the sample period.</td>
</tr>
<tr>
<td>cloud_up_ms</td>
<td>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.</td>
</tr>
<tr>
<td>cloud_down_mb</td>
<td>Displays the average number of Mbps for download operations to a cloud account during the sample period.</td>
</tr>
<tr>
<td>cloud_down_ms</td>
<td>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.</td>
</tr>
</tbody>
</table>

Figure 8-2  IBM FlashSystem 9100 Dashboard displaying System performance overview
Figure 8-3 shows the display after switching the button.

You can also use real-time statistics to monitor CPU utilization, volume, interface, and MDisk bandwidth of your system and nodes. Each graph represents 5 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 → Performance (as shown in Figure 8-4) to open the Performance Monitoring window.

As shown in Figure 8-5 on page 313, 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
Chapter 8. Hints and tips

- **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 figures are averaged on a 1 second-based sample.
You can also select to view performance statistics for each of the available nodes of the system, as shown in Figure 8-6.

![Figure 8-6 View statistics per node or for the entire system](image)

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](image)

In 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 timeline, it becomes a dotted line with the various values gathered, as shown in Figure 8-8.

![Figure 8-8 Viewing performance with details](image)
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](image)

**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 this web page.

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 more information about Storage Insights, see 4.5, “IBM Storage Insights” on page 92.

### 8.4 Command-line hints

IBM FlashSystem 9100 contains a robust command-line interface that is 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 use to automate copy services processes. All automation techniques are done by using the IBM FlashSystem 9100 command line or the Common Information Model Object Manager (CIMOM), which acts as a proxy to the command line.

In this section, the term **user agent** is used. The user agent can be the CIMOM, which connects to the cluster by using Secure Shell (SSH), or a user that is connecting directly with an SSH client in an interactive mode or by using a script.
Running commands to the cluster uses the following steps:

1. Connection
2. Authentication
3. Submission
4. Authorization
5. Running a command (Execution)

These steps are described next.

**Connection**

Commands are submitted to the cluster during a connection session to the cluster. User agents make connections through the SSH protocol. IBM FlashSystem 9100 includes 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.

Two connection queues are in action: *Pending Connections* and *Active Connections*. The connection process uses the following 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 rejected.

2. Pending Connections are handled in one of the following 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 these conditions 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 is idle.
   - The network connectivity fails.
   - The configuration node fails over.

In this case, both queues are cleared because the SSH daemon stops and restarts on a different node.
Authentication
IBM FlashSystem 9100 enables you to log in with 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. Consider the following points:

- **Local users** must provide a password, SSH key, or both. Local users are authenticated by using 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, 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 must access the system when the remote service is down also must configure local credentials. Remote users have their groups that are defined by the remote authentication service.

For more information, see 7.4.1, “Remote authentication” on page 251.

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 (one possible scenario) or succeed (four 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.

The following forms of connection solutions are available:

- **Transient**: One command is submitted per connection. 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 by using `ssh` on an Linux server. By using the operating system command, the IBM FlashSystem 9100 output can be processed.

*Example 8-5  Transient connection to IBM FlashSystem 9100 from Linux Server*

```bash
# ssh -i publickey -l ITSOadmin ITSO_FS9110 lsenclosure -delim :
id:status:type:managed:IO_group_id:IO_group_name:product_MTM:serial_number:total_canisters:online_canisters:total_PSUs:online_PSUs:drive_slots:total_fan_modules:online_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 by 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_canisters:online_canisters:total_PSUs:online_PSUs:drive_slots:total_fan_modules:online_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) by 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 that is shown in Example 8-7 enables you to create a transient connection.

*Example 8-7 Sample SSH configuration file saved as sampleCfg*

```bash
# 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*

```bash
# 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. First, open the PuTTY application and enter the following line in the Host Name (or IP address) field (see Figure 8-10):

```
superuser@<Host Name or cluster IP address>
```

![PuTTY Configuration](image)

*Figure 8-10 Add user name and system name to PuTTY session*

Also, enter a name in the Saved Sessions then, click *Save.*
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](image)

Complete saving the session (see Figure 8-12) by returning to the Session Panel (1), confirm the session name (2), and then, click **Save** (3).

![Figure 8-12  Save PuTTY session for use with plink](image)
After a session is saved, you can use it to make transient connections from the command line (see 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. 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.

Many methods are available 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 STDOU and STDERR streams.

You can use persistent connections in the following ways:

- **On a per-script basis**
  
  A script opens a connection that exists for the life of the script, which enables 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 shared connection, 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 together commands.

**Note:** IBM FlashSystem 9100 uses IBM Spectrum Virtualize technology, which is built on the foundation of the SAN Volume Controller. The command lines function in the same secure way, which enables you to use 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 *vdisk 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 by using `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
```

Note: The message *vdisk offline* is an error condition. In normal operations, you do not find any that are not online.
Example 8-12 shows how to submit scripts as batch files by using `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 that is 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 most 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 more information about 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 321.

The Perl module handles the connection aspect of any script. Because connection management is often the most complex part of any script, we suggest investigating this module. Currently, this module uses transient connections to submit commands to a cluster, which might not be the best approach if you plan to use multiple scripts that submit commands independently.
8.4.4 Sample commands of mirrored VDisks

This section includes sample commands that use the techniques that are shown in 8.4.3, “Command-line scripting” on page 321. These examples are based on sample data that is 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 by using the `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
```

**Raising the sync rate**
Raise the sync rate to 80 for all of the VDisks that are not synchronized, as shown in Example 8-15.

**Example 8-15  Raising 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.
**Changing 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 324.

```
Note: 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
```

**Removing all copies that are not primary**

Example 8-17 shows the removal all volume copies in the previous MDisk group.

```
Example 8-17   Removing 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
```

**Creating compressed mirrored copies of VDisks that are not mirrored**

Example 8-18 shows looking for all volumes that have a single copy and creating a mirrored compressed copy.

```
Example 8-18   Creating 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
```

**Tip:** From the CLI, issue the help addvdiskcopy command or see IBM Knowledge Center for more information about 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 Recovering lost superuser password

Complete 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 that is 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 that is named satask_result.html. This process 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 Backing up IBM FlashSystem 9100 configuration

Be sure to save the configuration of the system immediately after the system is configured and before any major changes are made to the IBM FlashSystem 9100 configuration. This save can help you in restoring the system configuration when recommended by IBM Support.

You can save the configuration by using the svcconfig backup command.

The use of 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 that is used to determine the configuration information. 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.

Complete the following steps to create a backup of the configuration file and copy the file to an external system:

1. Log in to the cluster IP by using an SSH client and back up the system configuration, as shown in the following example:

   superuser> svcconfig backup

   ...............................................................
   CMMVC6155I SVCCONFIG processing completed successfully

2. List and filter the following 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, as shown in the following example:

```
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:** Although the dump files show the serial number of the system at the end of the filename, use only the `svc.config.backup.xml` filename when the file is copied (do not use the serial number).

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 ensure that your system is in a healthy condition to receive the new code.

**Software Upgrade Test Utility overview**

The Software Update Test Utility indicates whether your current system has issues that must be resolved before you upgrade to the next level. The 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.

We strongly recommend running this utility immediately before the update is applied, making sure no new releases of the utility are available since it was downloaded.

Because the installation and usage of this utility is nondisruptive and does not require any nodes to be restarted, host I/O is not interrupted. The utility is installed on the current configuration node canister only.

For more information about the Software Upgrade Test utility, see this IBM Support web page.
Running the Software Upgrade Test Utility from the command line

Download the Software Upgrade Test Utility by way of IBM Fix Central. For more information about how to access IBM Fix Central to download fixes, updates, and drivers, see 8.6.5, “Downloading from IBM Fix Central” on page 338. The Software Upgrade Test Utility appears in IBM Fix Central as shown in Figure 8-13.

![Software Upgrade Test Utility selection for download](image)

Complete the following steps:

1. Copy the utility to the /upgrade directory on the IBM FlashSystem V9000 by using a secure copy utility, such as Secure Copy Protocol (SCP) or pscp.exe, as shown in the following example:
   ```
   pscp <test_utility_filename> superuser@<cluster_ip_address>:/upgrade
   ```

2. Install the utility, as shown in the following example:
   ```
   applysoftware -file <test_utility_filename>
   ```

3. Run the test utility, as shown in the following example:
   ```
   svcupgradetest -v 8.2.0.1
   ```
   The output is shown 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: The following message appears in the output for each detected warning:

******************* Warning found *******************

The utility remains installed and you can rerun as many times as you need. Installing a new version overwrites the old version.

8.5 Call Home process

IBM encourages all clients to take advantage of the available 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 reduced risk over a system that is not monitored. 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 to use this future offering. For more information, 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 function

The Call Home function opens a service alert if a serious error occurs on the system, which automatically sends details about the error and contact information to IBM Service personnel. If the system is eligible for support, a problem management record (PMR) is automatically created and assigned to the appropriate IBM Service personnel.

The information that is provided to IBM in this case might be an excerpt from the Event Log that includes information about the error and client contact information from the system. This process enables IBM Service personnel to contact you and arrange service for 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 alert is effectively the same as Call Home, but you can be notified about error, warning, and information messages when they occur. You also can receive inventory emails.

For more information about documentation that is specific to your IBM FlashSystem 9100 product, see IBM Knowledge Center. This documentation can help you determine whether a specific event is classified as error, warning, or informational. Look for the Notification type for each error to determine for which you want to be notified. Maximum flexibility exists because you can customize notification types to display only the information about you want to see.

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 is 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 331), have an assigned technical advisor throughout the entire warranty period.

This section describes the IBM Technical Advisor program in general with specifics on how customers can work with their Technical Advisor.

The Technical Advisor service is built around the following 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 storage hardware and software

Technical Advisors benefit customers by providing a consultant for questions about the IBM FlashSystem 9100. Most customers meet their Technical Advisor during a Technical Delivery Assessment (Solution Assurance Meeting) before the initial installation. After this initial meeting, the Technical Advisor is the focus for support-related tasks, such as the following examples:

- 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 and works with your support team in the background. Monitors progress of open service requests, escalation, and 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 process includes the use of Call Home information to provide customer reports about 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 by using IBM Technical Support Services offerings.

For more information, contact your IBM Sales Team or IBM Business Partner.

### 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 includes the following products:

- 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 the following 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.

During 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 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 to assist you with the support of your storage products. IBM FlashSystem 9100 includes the optional capability for remote support. As with Call Home, you can benefit from Enterprise Class Support as features are developed to enhance the support received by choosing to enable this capability.

### 8.6.3 Providing logs to IBM Enhanced Customer Data Repository

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 authorization from an IBM representative. The representative can provide more information, as needed.

To use ECuRep, you need a documented problem management record (PMR/Case) number that is provided by the IBM support team with a *call home*, or issued by using the IBM Service Request tool at the IBM Support portal.

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](image)
To provide logs to IBM ECuRep, complete the following steps:

1. Go to the IBM ECuRep web page.

   This web page provides information about the repository, instructions for preparing files for upload, and multiple alternatives for sending data. For more information, click Help (see Figure 8-15).

![ECuRep portal showing Help link and PMR/Case options](image)

**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.

IBM provides multiple options for uploading data. Review the options for sending data before you complete the PMR/Case number. The available options are shown in Figure 8-16 on page 334 (the Send Data tab is selected in this description).

As another way to upload a file other than the use of the standard method, you can select FTP (1) or the Java utility (2). The Java utility is the most efficient method to upload file.

2. Select **Prepare data** tab (3) to see the information about file name conventions.
3. Secure Upload (see Figure 8-17 on page 335) is the default upload selection. Complete the following fields and then, click **Continue**:

- PMR: The use of the PMR number on this form accurately logs the files that are uploaded to the correct PMR.

  **Note:** Remember to select the Case tab if 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.
The ECuRep Secure Upload option is shown in Figure 8-17.

![Figure 8-17 Using the standard option](image)

4. The file selection panel opens (see Figure 8-18 on page 336). Select the files and click **Upload**.
8.6.4 Uploading logs to IBM Blue Diamond Lab

IBM has a long history of providing clients with security technologies to protect data. Blue Diamond Enhanced Secure Support 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.

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 valuable time during a crisis.
Complete the following steps to upload support logs to the IBM Blue® Diamond FTP:

1. Log in to the Blue Diamond Secure FTP portal, as shown in Figure 8-19.

![Figure 8-19 Blue Diamond sign-in](image)

2. Log in to our secure FTP server by using your Blue Diamond credentials, as shown in Figure 8-20.

![Figure 8-20 Blue Diamond FTP Login page](image)

3. Click **Upload Data**, as shown in Figure 8-21.

![Figure 8-21 Blue Diamond Data Upload page](image)
4. Browse to the folder that contains your company name (IBM/YourCompanyName), as shown in Figure 8-22.

**Note:** You are permitted to see only your own company folder.

![Figure 8-22 Browse your company folder](image)

5. Create a subfolder with the name of your PMR/Case number; for example, 12345,567,000 / TS001234567, as shown in Figure 8-23.

![Figure 8-23 Subfolder with PMR number](image)

6. Upload the diagnostic data to the subfolder that you 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. For more information, see the IBM Fix Central web page.

If you do not need fixes or updates, see 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. Also, your information is centralized so you can maintain it in a convenient and secure location. The benefits of having an IBMid increase over time as more applications migrate to IBMid.
At the IBM Fix Central main page, select the person icon (step 1 in Figure 8-24). Then, click **Sign in** (step 2 in Figure 8-24).

![IBM Fix Central main page](image1)

*Figure 8-24  IBM Fix Central main page*

The login window is shown in Figure 8-25.

![IBMid login window](image2)

*Figure 8-25  IBMid login window*
Fix Central
The following steps describe the current process that is used 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 regularly:

1. After signing in with your IBMid, a page opens to the Support Portal (see Figure 8-26). In the Find product (1) tab, go to the Product selector (2) field and enter 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](image)

2. Select the version (see 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](image)
3. The Select fixes panel (see Figure 8-28) provides download options for the software for which you are looking. In this example, we are showing where to go to download the Product Software.

![Figure 8-28 Select the Product Software](image)

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 option and click **Continue** at the bottom of the window to start the file transfer. Figure 8-29 shows the location of the release notes and the software download links.

![Figure 8-29 Select the wanted software level after reading the Release Notes](image)

**Note:** Always read the release notes. They often contain special instructions that are related to the upgrade that should be part of your planning.
6. Confirm your selection and then, click **Download now** (see Figure 8-30) to start the download process. Download Director is the preferred method for downloading because it is multi-threaded.

![Download files using Download Director](image)

Figure 8-30 **Download now**

7. Check that your download completes successfully.
Related publications

The publications that are listed in this section are considered particularly suitable for a more detailed discussion of the topics that are covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide more information about the topic in this document. Some publications that are 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
- *FlashSystem V9000 Product Guide*, REDP-5468
- *IBM FlashSystem V9000 and VMware Best Practices Guide*, REDP-5247
- *IBM FlashSystem V9000 in a VersaStack Environment*, REDP-5264
- *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

The following websites are also relevant as further information sources:

- IBM FlashSystem 9100:
- IBM FlashSystem resources:
- IBM FlashSystem 9100 in IBM Knowledge Center:
- IBM Storage Insights:
  https://ibm.biz/Bd2zwG
- 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
IBM FlashSystem 9100 Architecture, Performance, and