IBM Spectrum Protect Plus
Practical Guidance for Deployment, Configuration, and Usage

Andre Gaschler
Axel Westphal
Wilhelm Gardt
Mikael Lindstrom
Peter Minig
Joerg Walter
Daniel Wendler
Bert Dufrasne
Note: Before using this information and the product it supports, read the information in “Notices” on page ix.
## Contents

Notices .......................................................................................... ix  
Trademarks .................................................................................. x  

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

**Chapter 1. IBM Spectrum Protect Plus Product Architecture and Components** ............................................. 1  
1.1 IBM Spectrum Protect Plus overview ..................................... 2  
    1.1.1 Key concepts .................................................................. 3  
1.2 IBM Spectrum Protect Plus architecture ................................. 5  
    1.2.1 IBM Spectrum Protect Plus server .................................... 5  
    1.2.2 Site .............................................................................. 11  
    1.2.3 vSnap Backup Storage server ....................................... 12  
    1.2.4 VADP proxy server ...................................................... 14  
1.3 SLA backup policies ............................................................... 15  

**Chapter 2. Solution Architecture, Planning, and Design** ................................................................. 19  
2.1 System context ....................................................................... 20  
2.2 Roles and responsibilities ....................................................... 22  
2.3 Solution design considerations .............................................. 23  
    2.3.1 Dedicated or shared environment .................................... 24  
    2.3.2 Network ....................................................................... 24  
    2.3.3 Encryption ................................................................... 24  
2.4 Solution requirements ............................................................ 27  
    2.4.1 Architectural decisions .................................................. 29  

**Chapter 3. Installation and deployment** .................................................. 37  
3.1 Review the prerequisites for an IBM Spectrum Protect Plus deployment ......................................................... 38  
    3.1.1 Requirements for IBM Spectrum Protect server ............... 38  
    3.1.2 Requirements for the vSnap Backup Storage server ........ 39  
    3.1.3 Requirements for the VADP proxy server ....................... 39  
3.2 Installation and deployment ..................................................... 40  
    3.2.1 Deploy the IBM Spectrum Protect Plus server ................. 41  
    3.2.2 Deploy the vSnap Backup Storage and VADP proxy server 44  
3.3 Configuration of the IBM Spectrum Protect Plus environment ................................................................. 45  
    3.3.1 Configure the IBM Spectrum Protect Plus server ............ 45  
    3.3.2 Configure the vSnap Backup Storage server ................. 52  
    3.3.3 Configure NTP for the IBM Spectrum Protect Plus and the vSnap server ..................................... 53  
    3.3.4 Connect the vSnap and VADP Proxy server with the IBM Spectrum Protect Plus server .................. 55  
    3.3.5 Add a SLA for IBM Spectrum Protect Plus catalog backup 63  
    3.3.6 Backing up the vSnap server System Configuration .......... 65  
    3.3.7 Change and verify the schedules of the predefined jobs .... 68
Chapter 4. Backup and Restore VM ........................................... 71
  4.1 VM backup configuration basics ........................................ 72
    4.1.1 Create an Identity ........................................... 72
    4.1.2 Add a Hypervisor Resource ................................. 72
    4.1.3 Assign an SLA policy ....................................... 73
    4.1.4 Run a backup job for an SLA ............................... 76
    4.1.5 Run a backup for a single VM ................................ 77
    4.1.6 Distributing VM backups to multiple vSnaps ............... 78
    4.1.7 Backup Options ............................................. 79
  4.2 Catalog file metadata for single file restore ...................... 80
    4.2.1 Configure requirements .................................... 80
    4.2.2 Catalog file metadata discovery ........................... 82
    4.2.3 Restore single files and directories ....................... 84
  4.3 VM restore and data reuse ......................................... 87
    4.3.1 Restore Schedule ........................................... 87
    4.3.2 Restore Source (Location) and Restore Points ............. 88
    4.3.3 Restore Destination ......................................... 89
    4.3.4 Restore methods ............................................ 89
    4.3.5 Restore Options ............................................ 90
    4.3.6 Restore a virtual disk ...................................... 91
    4.3.7 Restore a VM ................................................. 94

Chapter 5. Backup and Restore databases .................................. 99
  5.1 Database backup configuration basics ................................ 100
    5.1.1 Create an Identity ........................................... 100
    5.1.2 Add an application server ................................... 101
    5.1.3 Assign an SLA policy ....................................... 102
    5.1.4 Run a backup .................................................. 102
  5.2 IBM Spectrum Protect Plus database restore and data reuse ...... 103
    5.2.1 Test restore .................................................. 104
    5.2.2 Instant access ............................................... 107
    5.2.3 Production restore ........................................... 107
  5.3 Oracle-specific information ........................................ 110
    5.3.1 Server registration .......................................... 110
    5.3.2 Oracle multi-threading ..................................... 110
    5.3.3 Oracle backup information ................................ 110
    5.3.4 Oracle Block Change Tracking .............................. 110
    5.3.5 Compression ............................................... 111
    5.3.6 Troubleshooting hint ....................................... 111

Chapter 6. Backup and restore MongoDB databases .......................... 113
  6.1 IBM Spectrum Protect Plus requirements for MongoDB ............. 114
    6.1.1 Fundamental IBM Spectrum Protect Plus requirements for MongoDB .................................... 114
    6.1.2 MongoDB databases without authentication ................. 115
    6.1.3 MongoDB databases with authentication enabled .......... 115
    6.1.4 Register a MongoDB server .................................. 116
  6.2 MongoDB backup and restore with Spectrum Protect Plus .......... 118
    6.2.1 MongoDB backup ............................................. 118
    6.2.2 MongoDB restore ............................................ 120

Chapter 7. Backup and Restore of Db2 databases ............................ 125
  7.1 IBM Spectrum Protect Plus Db2 features ........................... 126
  7.2 Prerequisites for Db2 databases ................................... 126
Chapter 12. Maintenance ................................................................. 201
  12.1 Update IBM Spectrum Protect Plus components ......................... 202
    12.1.1 Update sequence .................................................. 202
    12.1.2 Updating IBM Spectrum Protect Plus virtual appliance ............ 202
    12.1.3 Updating vSnap servers ............................................. 204
    12.1.4 Updating VADP proxies ............................................. 205
    12.1.5 Applying early availability updates (efix) ......................... 206
  12.2 IBM Spectrum Protect Plus troubleshooting (log files) ................... 206
  12.3 Managing the vSnap server .................................................. 208
  12.4 LDAP and SMTP configuration ............................................... 215
    12.4.1 Adding an LDAP server ............................................. 215
    12.4.2 Adding an SMTP server ............................................. 216
    12.4.3 Editing settings for an LDAP or SMTP server ....................... 217
    12.4.4 Deleting an LDAP or SMTP server ................................ 217
  12.5 Administrative Console .................................................. 218
    12.5.1 Log in to the Administrative Console ................................ 218
    12.5.2 System Management .................................................. 220
  12.6 Global Preferences ......................................................... 220
  12.7 Managing the IBM Spectrum Protect Plus catalog ........................ 222
    12.7.1 Restoring the IBM Spectrum Protect Plus application .............. 222
    12.7.2 Deleting IBM Spectrum Protect Plus resources from the catalog ... 223
    12.7.3 Managing IBM Spectrum Protect Plus restore points ............... 223
  12.8 Search guidelines .......................................................... 224
    12.8.1 Searching with wildcards ........................................... 224
    12.8.2 Match a single character with a question mark: .................... 225
  12.9 Testing network connectivity ............................................. 225
    12.9.1 Running the Service Tool from a command-line interface .......... 227
    12.9.2 Running the Service Tool remotely ................................ 227
  12.10 Messages ................................................................. 228
    12.10.1 IBM Spectrum Protect Plus message prefixes ....................... 229

Chapter 13. The vSnap CLI. ......................................................... 231
  13.1 vSnap server CLI .......................................................... 232
  13.2 vSnap server initialization ............................................... 233
  13.3 vSnap server preferences ............................................... 233
    13.3.1 Changing replication streams and timeouts .......................... 235
  13.4 vSnap volumes and snapshots .............................................. 236
    13.4.1 Volumes and snapshots for backup data ............................ 236
    13.4.2 Volumes and snapshots for replication data ....................... 239

Chapter 14. REST API. ............................................................. 245
  14.1 REST API Overview ........................................................ 246
  14.2 IBM Spectrum Protect Plus REST API .................................... 246
    14.2.1 REST API documentation .......................................... 247
  14.3 Discovering the REST API ................................................. 248
    14.3.1 CURL ................................................................. 249
    14.3.2 Swagger UI .......................................................... 252
    14.3.3 Firefox RESTClient ................................................ 253
  14.4 Use Case: initiate backup of VMs via REST API with Python .......... 257
    14.4.1 Motivation .......................................................... 257
    14.4.2 Trace GUI REST operations with Firefox browser .................. 258
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™       Redbooks (logo)®
Db2®       IBM Spectrum®    Storwize®
IBM®       Redbooks®        System Storage™

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

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.

Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware, VMware vSphere, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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

IBM® Spectrum Protect Plus is a data protection solution that provides near-instant recovery, replication, retention, and reuse for virtual machines, databases, and applications in hybrid multicloud environments.

IBM Knowledge Center for IBM Spectrum® Protect Plus provides extensive documentation for installation, deployment, and usage. In addition, IBM Spectrum Protect Plus Blueprint (https://ibm.biz/IBMSpectrumProtectPlusBlueprints) provides guidance about how to build and size an IBM Spectrum Protect Plus solution.

The goal of this IBM Redpaper publication is to summarize and complement the available information by providing useful hints and tips based on the authors’ practical experience in installing and supporting IBM Spectrum Protect Plus in actual customer environments. Over time, our aim is to compile a set of best practices that cover all aspects of the product, from planning and installation to tuning, maintenance, and troubleshooting.

The paper is structured as follows:

- This first and current version of the document starts with an overview, and probably just a reminder for most readers, of key components and characteristics of IBM Spectrum Protect Plus version 10.1.4. It is followed by a deeper dive into the architecture, concepts, and operational features, including encryption.

- Chapter two discusses architectural planning considerations, such as the system context, roles and responsibilities, and functional and non-functional requirements. It also reviews architectural decisions that should drive the design of the solution for deployment in your environment.

- Chapter three is about installation and deployment, but focuses on additional configuration actions that need to take place after the initial installation. For the installation itself, the reader must refer to detailed steps found in IBM Knowledge Center, or in the Installation and User’s Guide.

- Chapters four to eighth successively discuss backup, restore, and reuse operations for Virtual Machines and supported databases (Oracle, MongoDB, IBM Db2®, and Microsoft SQL Server).

- Chapter nine explains options for creating additional copies of data, either for disaster recovery purposes or for long-term archiving, on tape or in the Cloud.

- Chapter ten gives advice for setting up the network environment and separation, if necessary, between backup data traffic and system management traffic.

- Chapter eleven discusses specifics of the Role Based Access Control concept and its implementation in IBM Spectrum Protect Plus.

- Chapter twelve is about maintenance, troubleshooting and monitoring.

- Chapter thirteen describes details of the vSnap Backup Storage server command-line interface (CLI), which is used to administer the vSnap server and configure advanced options.

- Finally, chapter fourteen provides practical information and examples on how to take advantage of the REST API services.
Authors

This paper was produced by a team of specialists from around the world:

**Andre Gaschler** is an IBM Certified IT Specialist at the IBM EMEA Storage Competence Center (ESCC) in Kelsterbach, Germany. He has been working at IBM for 25 years with more than 15 years of experience with IBM Spectrum Protect. He is a member of IBM’s Systems Storage Lab Services team, supporting customers with designing, planning and implementation solutions based on IBM Spectrum Protect and IBM Spectrum Protect Plus. He contributed to the backup chapter of the book *Speichernetze*, and is an author of the IBM Redbooks® publication *IBM Tivoli Storage Manager Versions 5.4 and 5.5 Technical Guide*, SG24-7447.

**Axel Westphal** is an IBM Certified IT Specialist at the IBM EMEA Storage Competence Center (ESCC) in Kelsterbach, Germany. He joined IBM in 1996, working for IBM Global Services as a Systems Engineer. His areas of expertise include setup and demonstration of IBM System Storage™ products and solutions in various environments. He has written several storage white papers and co-authored several IBM publications.

**Wilhelm Gardt** worked as a software developer and IT specialist, designing and implementing database and SAP environments, before he joined IBM in 2001. Since 2004, he is a member of the Advanced Technical Skills (ATS) team for IBM Storage in EMEA. He provides technical pre-sales support, proof of concepts, workshops, and implementation services. Wilhelm is a regular author of IBM Redbooks publications, and a speaker at IBM and external technical conferences. He holds a degree in Computer Sciences from the University of Kaiserslautern, Germany.

**Mikael Lindstrom** is a Senior Technical Staff Member in Resiliency and an IBM Inventor within the IBM Global Services. He has 19 years of IT experience in different environments, of which 16 years has been with IBM Spectrum Protect products and Storage. Mikael advises executive management and offers senior leadership on emerging technology and design elements. Mikael also provides customer-facing expertise for projects worldwide, helping to solve their challenges around resiliency, and to build future-proof Software Defined Resiliency Cloud infrastructure. He has co-authored over 10 Redbooks publications and white papers related to IBM Spectrum Protect products and Software Defined Storage.
Thanks to the following people for their contributions to this project:

Peter Minig holds a diploma in electrical engineering and computer sciences in Germany. He joined IBM in 1998 and started by supporting client and server infrastructure, gaining experience in systems management. He is a member of IBM’s Systems Storage Lab Services team, supporting customers with designing, planning, and implementing DP&R related products like IBM Spectrum Protect, IBM Spectrum Protect Plus, and Tape Storage.

Joerg Walter is a member of IBM’s Systems Storage Lab Services team in Germany, supporting customers with the planning and implementation of IBM Data Protection and Retention (DP&R)-related HW & SW products, like IBM Spectrum Protect, IBM Spectrum Protect Plus, IBM Spectrum Protect Snapshot, and physical and virtual tape. He holds a diploma in electrical engineering and computer sciences.

Daniel Wendler holds a diploma in computer sciences. After completing his studies at the University of Applied Sciences in Wiesbaden, Germany, he joined IBM in 2005. He worked in various technical positions within IBM. He is a member of IBM’s EMEA Systems Storage Lab Services pre-sales team, supporting customers with the planning and implementation of DP&R and IBM Security Key Lifecycle Manager encryption solutions.

Bert Dufrasne is an IBM Certified Consulting IT Specialist and Project Leader for IBM System Storage disk products at the International Technical Support Organization (ITSO), San Jose Center. He has worked at IBM in various IT areas. He has authored many Redbooks publications, and he has also developed and taught technical workshops. Before Bert joined the ITSO, he worked for IBM Global Services as an Application Architect. He holds a Master’s degree in Electrical Engineering.

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

Jason Basler
Stefan Bender
Frank Lautenbach
Dominic Mueller-Wicke
Jim Smith

IBM
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 IBM Redbooks 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 papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online Contact us review Redbooks form:
  ibm.com/redbooks
- Send your comments in an email:
  redbooks@us.ibm.com
- Mail your comments:
  IBM Corporation, IBM Redbooks
  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 Spectrum Protect Plus
product architecture and components

This chapter starts with a general overview of the IBM Spectrum Protect Plus solution and its key concepts.

The chapter continues with more details about the product architecture and its main components, including the IBM Spectrum Protect Plus server, the vSnap Backup Storage server, and the VMware vSphere Storage APIs for Data Protection (VADP) server. It briefly explains how service level agreement (SLA) policies and sites are used to manage backup data.

This chapter includes the following topics:

- IBM Spectrum Protect Plus overview
- IBM Spectrum Protect Plus architecture
- SLA backup policies
1.1 IBM Spectrum Protect Plus overview

IBM Spectrum Protect Plus provides data availability using snapshot technology for rapid backup, recovery, and data management. It features secure, self-service, end-user facing portals for data protection management and monitoring. Designed to be used by virtual machines and application administrators, it also provides data cloning functionality to support and automate DevOps workflows. Unlike other data availability solutions, IBM Spectrum Protect Plus uses automated Service Level Agreements (SLA) to provide backup status and support retention compliance.

Figure 1-1 shows an overview of the IBM Spectrum Protect Plus architecture.

The IBM Spectrum Protect Plus server is the component that manages and orchestrates the entire system and is the “brain” that provides the web interface used for configuring and operating the solution, as well as performing centralized scheduling of activities. The vSnap server is the component that is responsible for storing and processing the backup data received from customer systems. The VADP proxy is the component that shifts processing load off the Spectrum Protect Plus server component.

A typical deployment includes a single Backup Server (IBM Spectrum Protect Plus server) with multiple Backup Storage servers (vSnap servers) according to customer requirements and needs. Because IBM Spectrum Protect Plus is an agentless data protection solution, a traditional Backup Client software component is not required.

Figure 1-1 describes the key components on the left side, where IBM Spectrum Protect Plus is deployed as a virtual machine on either a VMware or Microsoft Hyper-V hypervisor infrastructure. IBM Spectrum Protect communicates via standardized API calls with the virtual environments, databases, and applications, which can run on virtual machines or on physical servers. This is part of the cataloging processes, as well as backup scheduling, during the backup window. The IBM Spectrum Protect Plus server then initiates a block-level forever backup to the vSnap pool.
Each backup is stored as a read/write snapshot and moves the data to the storage component, which is a scalable storage pool built on a combination of IBM Spectrum Protect Plus software and the vSnap server repository. This vSnap pool can run on either a virtual or physical server, and can be replicated to a second vSnap server as an operational protection. In addition if required, you can tier data to IBM Spectrum Protect, onto multiple different storage options, such as tape or object storage, for additional protection.

Finally, you can then use any backup image to restore, whether back to the virtual environment for recovery, or for any of the multi-purpose use cases, such as instant data recovery boot via vSnap repository or data reuse of existing data copies for tests and DevOps.

The built-in role-based access control (RBAC) model enables you to allocate access to specific areas and resources within an IBM Spectrum Protect Plus data protection solution, and to dedicated teams. You can use the RBAC role model to assign different roles for VM administrators or database administrators. After these roles are allocated, these users can create backup jobs, restore data, or apply any of the multiple data reuse cases.

Backups taken from virtual machines, databases, and applications are cataloged (backup metadata) on the IBM Spectrum Protect Plus server and stored according to the Backup Policies (SLA) directly on the vSnap server.

A vSnap server can be deployed as a virtual machine on either a VMware or Microsoft Hyper-V hypervisor infrastructure, or installed on a physical server. The vSnap server is responsible to store, manage, and maintain the backup data. Backups are sent directly from the source system to the vSnap server.

The vSnap server manages the backup traffic and workload. The backup metadata is sent to the IBM Spectrum Protect Plus server. To achieve local backup data placement using SAN or LAN networks and to scale-out, multiple vSnap servers are typically used within an IBM Spectrum Protect Plus solution. For efficient performance, proper sizing of the vSnap server is crucial. The IBM Spectrum Protect Plus Blueprints provide the required guidance:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

Instant access and restore capabilities are provided by the different backup storage pools, including vSnap pool, IBM Spectrum Protect disk container, and tape and object storage, such as IBM Cloud™ Object Storage.

1.1.1 Key concepts

This section discusses key concepts in IBM Spectrum Protect Plus.

The primary users for the IBM Spectrum Protect Plus solution are customers running virtualized workloads in a traditional data center, cloud data center, and remote branch offices. IBM Spectrum Protect Plus is also capable of providing multitenantity for service providers and business partners with multiple end customers. See also Chapter 2, “Solution architecture, planning, and design” on page 19.

- Native data format. Traditional backup products take the data that they ingest from client systems and package it in proprietary formats on disk or tape. Before the data is usable, the backup application must first extract it from the packaged format. IBM Spectrum Protect Plus, by contrast, stores data in the format created by the application it is protecting, such as .vmdk files for VMware or Hyper-V .VHDX files.
- **Instant data recovery boot via vSnap repository** is at the core of the IBM Spectrum Protect Plus solution. It allows users rapid recovery or access to data, without having to wait for traditional data restore operations to move data.

- **Agentless backup and recovery** of virtual machines (VMware, Hyper-V) and selected applications on physical machine. Traditional backup approaches require the installation of a heavyweight application on each protected machine, which can be time-consuming and intrusive. IBM Spectrum Protect Plus uses a modern agentless approach with remote code injection/execution to avoid the need to manually roll out and configure application code across the environment. These benefits also extend beyond implementation, because upgrades are no longer required for every client in the environment.

- **RESTful API** functions supported by REST, such as automation, integration, configuration, and data collection. By leveraging the REST API, IBM Spectrum Protect Plus is able to integrate with automation tools like Jenkins, Puppet, and others.

- **Encryption at rest.** Encryption at rest is a requirement for many service providers and business partners in the General Data Protection Regulation (GDPR), Europe’s new data privacy regulation that went into effect on May 25th of 2018. IBM Spectrum Protect Plus offers the option to encrypt data using AES 256-bit encryption in the vSnap server at-rest.

- **On-demand data reuse** of existing backup copies for Test/Dev, DevOps, analytics, and reporting.

- **Scale-out architecture.** Some traditional backup products handle larger environments by augmenting the size and performance of a single “island” installation of the product. IBM Spectrum Protect Plus scale-out architecture aligns with future growth needs and handles increases in hardware size with multiple load handlers, known as vSnap servers.

- **The data lifecycle is service level agreement (SLA) policy-driven,** enabling flexible configurations with local and replica copies, and with copies with on tape or object storage. This configuration provides long-term retention protection on low-cost, low-performance storage, each with independently managed retentions. The solution allows for a cloud-friendly scale out architecture for future growth needs.

- **Role-based access control (RBAC)** is an easy to use self-service access capable web-based user interface where users can run traditional restore operations. Customers can define users and assign them roles, such as that of a hypervisor admin or a database admin, so that those users can run actions like restores jobs while having their scope limited to the systems or data types for which they are responsible. Teams can access and reuse existing data copies for Test/Dev, DevOps, analytics, and reporting on demand.

- **Data reduction.** Deduplication is a technology used for several years to reduce the size of backup data stored on disk. It works by examining incoming backup data streams and looking for pieces of data that already reside on storage. When the deduplication engine encounters a piece of data that it has seen before, rather than storing it again the engine makes metadata references to where the data is already stored on disk.

  From an overall data reduction standpoint, IBM Spectrum Protect Plus uses a full-once, incremental forever backup technology, which minimizes the amount of redundant data that the system must process. If you compare this to a backup system that periodically requires a full backup of data that mostly has not changed, there is naturally more potential for data deduplication because there is more redundant data.

- **DR and High Availability Replication.** In the context of backup replication, this refers to taking backups from the initial server, storing them, and sending a copy to another server (normally in a separate physical location). This action protects against the loss of data and safeguards the primary backup server and associated storage infrastructure. When replication is done in backup software rather than at the storage layer, the software can determine the retention for each copy of the data as well as store it on different types of storage. This action ensures that the replica is properly accounted for and reported on.
1.2 IBM Spectrum Protect Plus architecture

This section focuses on the IBM Spectrum Protect Plus architecture and its components. Figure 1-2 illustrates the deployment of IBM Spectrum Protect Plus in two active locations, showing the following key components:

- A single IBM Spectrum Protect Plus server
- A single or multiple vSnap servers (multiple in the example)
- A single or multiple VADP proxy servers (either a separate server, or colocated with a vSnap server, multiple in the example)

![IBM Spectrum Protect Plus deployed in two active locations](image)

In the following sections, we explain the roles and features of these key components and how they interact with each other and further elaborate on key concepts Sites and SLA policies.

1.2.1 IBM Spectrum Protect Plus server

This is the component of the infrastructure that manages and orchestrates the entire system. The server consists of several catalogs that track various system aspects, such as recovery points, configuration, access, customizations, and so on. The server is deployed and configured as a Virtual Machine, and provides the web-based graphical user interface (GUI) and a job scheduler.

**Important:** There is always only one IBM Spectrum Protect Plus server in a deployment, even if the deployment is spread across multiple locations.

**User interfaces**

The server provides two web-based graphical user interfaces (GUIs):

- The Day-to-day GUI with access to the Dashboard, Backup Configuration, and so on
- The Administrative Console GUI with access to License and Certificates Management, Network and System Settings, and to apply Software Updates.
In addition to the GUI, a command-line interface (CLI) is provided to access advanced networking and system settings. A REST API interface can also be used for system automation. The CLI is further explained in Chapter 3, “Installation and deployment” on page 37 and Chapter 13, “The vSnap CLI” on page 233. The REST API interface is discussed in the Chapter 14, “REST API” on page 247.

After logging in to the regular GUI using https (for example, https://spp-server/) the Dashboard view is loaded, as shown in Figure 1-3. The Dashboard view provides a direct overview and links to the following information:

- **Jobs and Operations**: Currently running jobs, and a history of jobs in the categories of Failed, Warning, and Success, are displayed together with a job success rate for a given time frame.

- **Backup Storage Destination**: Capacity overview is provided, together with a Device status (inactive and full) and overall Data Reduction statistics.

- **Protection Coverage**: Providing an overview of how many discovered resources are protected using different policies.

![IBM Spectrum Protect Plus Dashboard](image)

Figure 1-3   IBM Spectrum Protect Plus Dashboard
The left menu bar provides one-click access to the following areas:

- **Jobs and Operations** with details about running and previous jobs, and their corresponding logs. On the Schedule tab, an overview of all scheduled jobs is provided, and the schedule of system jobs could be changed. Furthermore, on the Active Resources tab of the Instant Access section, Restore options for Applications and Hypervisor are listed. Find more information in the IBM Knowledge Center for IBM Spectrum Protect Plus: [https://www.ibm.com/support/knowledgecenter/en/SSNQFQ_10.1.4/spp/c_spp_jobs.htm1](https://www.ibm.com/support/knowledgecenter/en/SSNQFQ_10.1.4/spp/c_spp_jobs.htm1)


- **System Configuration** includes configuration items for the Backup Storage Options Disk (vSnap Backup Storage), Cloud (for example, Amazon S3), and Repository Server (IBM Spectrum Protect). In the Global Preferences area, Sites, VADP proxies, LDAP, and SMTP settings can be configured. For more information, see IBM Knowledge Center for IBM Spectrum Protect Plus: [https://www.ibm.com/support/knowledgecenter/en/SSNQFQ_10.1.4/spp/c_spp_system_overview.html](https://www.ibm.com/support/knowledgecenter/en/SSNQFQ_10.1.4/spp/c_spp_system_overview.html)


- **Accounts** is used to configure user access using a role-based access control model, and enables you to manage IBM Spectrum Protect Plus used identities to access different resources. Find more information in IBM Knowledge Center for IBM Spectrum Protect Plus: [https://www.ibm.com/support/knowledgecenter/en/SSNQFQ_10.1.4/spp/c_spp_user_access.html](https://www.ibm.com/support/knowledgecenter/en/SSNQFQ_10.1.4/spp/c_spp_user_access.html)

The Administrative Console GUI can be entered using `https` and port 8090 (for example, `https://spp-server:8090`) using an IBM Spectrum Protect Plus user account or the System ID `serveradmin`. In the console, you can perform the following actions:

- Get details about the installed product versions
- Manage and install the licenses
- Manage and install certificates, for example, Active Directory LDAP certificates
- Apply and install IBM Spectrum Protect Plus software updates
- Perform System Actions, such as Start/Stop the server, reboot the virtual machine, and configure the time zone
Data catalogs
The IBM Spectrum Protect Plus server maintains several data catalogs, all running on the server appliance. Recovery points of Virtual Machine, Database, and Application backups are tracked in addition to the information for file-level recovery. System configuration is also tracked in these catalogs. The default sizes provisioned for the catalogs should be sufficient for most workloads, but can be expanded if necessary. In general, place the IBM Spectrum Protect Plus appliance on high-performing, flash storage to optimize catalog performance.

In order to protect your IBM Spectrum Protect Plus installation, the catalogs and all required information need to be backed up on a daily basis. This backup is configured under the menu item Manage Protection → IBM Spectrum Protect Plus → Backup. Backup Schedule and Retention are managed through an SLA and stored on a vSnap Backup Storage from where it can also be restored. Find more information in the IBM Knowledge Center for IBM Spectrum Protect Plus:

Scheduler (Jobs and Operations)
Figure 1-4 shows the overview page of the Scheduler, which could be accessed by selecting Jobs and Operations on the Schedule tab.

![Scheduler (Jobs and Operations)](image)

Figure 1-4 IBM Spectrum Protect Plus Schedule tab

In this view, all backup, restore, and system-defined (Maintenance and Inventory) jobs from IBM Spectrum Protect Plus are listed with the information about the last and next run time. Above the Actions pull-down menu, these jobs can be started manually, or their schedule can be paused (deactivated).

An adjustment of the scheduled runtime for system-defined and restore jobs can be performed by clicking the [ ] calendar icon. A restore job can be deleted by clicking the X sign before the job name. The schedule time for backup jobs can be adjusted under the Manage Protection → Policy Overview menu item by modifying the associated SLA Policy.
System-defined jobs
In IBM Spectrum Protect Plus, there are one Maintenance and several Inventory jobs predefined as system-defined jobs.

The maintenance job is predefined with system installation, and runs once a day to remove expired and deleted entries from the catalog and the system configuration. This cleanup procedure recclaims space on storage devices, cleans up the IBM Spectrum Protect Plus catalog, and removes related snapshots. The maintenance job also removes cataloged data that is associated with deleted jobs.

An inventory job is automatically created when you add a resource to IBM Spectrum Protect Plus. The following inventory jobs are available:

- **Hypervisor Inventory** is created when the first Hypervisor (VMware or Hyper-V) is added to IBM Spectrum Protect Plus. On a daily basis, it scans the associated resources on the Hypervisors, such as VMs, storage, and network configuration.

- **Application Server Inventory** is created when the first Database or Application is added to IBM Spectrum Protect Plus. On a daily basis, it scans the available Databases and Application instances on the added systems.

- **Storage Server Inventory** is pre-defined with the system installation, and scans the configured vSnap Backup Storage server resources on a daily basis.

Identities
Some features in IBM Spectrum Protect Plus require credentials to access your resources. For example, IBM Spectrum Protect Plus connects to Oracle servers as the local operating system user that is specified during registration to complete system tasks, such as cataloging, data protection, and data restore. Furthermore, IBM Spectrum Protect Plus components, such as a vSnap Backup Storage server and a VADP proxy server, require credentials to access the resources.

It is a best practice to add user names and passwords for your resources through the Accounts → Identity pane. Then, when using a feature in IBM Spectrum Protect Plus that requires credentials to access a resource, select Use existing user, and select an identity from the drop-down menu. If you use identical credentials for your resources, IBM Spectrum Protect Plus enables you to manage these databases on one Identity.

The following resources require credentials:

- vSnap Backup Storage server
- VADP proxy servers
- Hypervisor servers
- Database instances
- Application instances
- Virtual Machine for file metadata discovery or for specific data reuses cases where VM internal needs to be changed

Figure 1-5 on page 10 shows the Identity window that appears when you click Add Identity (in the right corner) under Accounts → Identity. You can specify a common name that best describes your entry in the Name field, and add the Username and Password in the appropriate fields.
You end up with a list of identity entries, as shown in figure Figure 1-6. Some are default system identities (LocalSnapadmin, serveradmin, and vsnapadmin), and some are users explicitly created for database backup and restore (DB administrator - OS user, Mongo DB user, and Oracle DBA).

A key element in the IBM Spectrum Protect Plus server protection is the regular backup of the catalog data. At least once a day, the IBM Spectrum Protect Plus catalog should be backed up to a vSnap Backup Storage server. In case of a failure, an IBM Spectrum Protect Plus server could be redeployed and, using the previously backed up catalog, used to restore the server to its previous state including all configurations.

An additional option to protect the IBM Spectrum Protect Plus server is to run it either in a vSphere High Availability or Fault Tolerance configuration:

- **High Availability** enables the IBM Spectrum Protect Plus server to be available with a minimum amount of downtime in the case of a VM host failure. This can be achieved through VMware vSphere High Availability or Microsoft failover clustering.
- **Fault Tolerance** enables the IBM Spectrum Protect Plus server to be continuously available in the case of a VM host failure. This can be achieved through VMware vSphere Fault Tolerance (FT).
Further information about these additional configuration options is available in an IBM Technote: [https://www.ibm.com/support/docview.wss?uid=ibm10870652](https://www.ibm.com/support/docview.wss?uid=ibm10870652)

1.2.2 Site

A site is an IBM Spectrum Protect policy construct that is used to manage data placement in the environment. It can be physical, such as a data center, or logical, such as a department or organization. IBM Spectrum Protect Plus components are assigned to sites to localize and optimize data paths. A deployment always has at least one site per physical location.

By default, the IBM Spectrum Protect Plus environment has a primary site, a secondary site, and a demo site. You can change the site name and other options for the default Primary and Secondary sites. The Demo site is available only for the onboard vSnap server. You cannot use this site with any other vSnap server.

**Note:** The Demo site is predefined with the deployment of IBM Spectrum Protect Plus, and is intended to be used only for product demonstration purposes. It should not be used for a production backup and can therefore be deleted in such installations.

Sites in IBM Spectrum Protect Plus are configured and maintained under **System Configuration → Site** as shown in Figure 1-7. Here you can adjust the names or add additional sites. A Throttle Rate can be configured to change and limit the throughput for site replication and offload operations so that you can manage your network activity on a defined schedule.

![Figure 1-7 IBM Spectrum Protect Plus Site Overview](image)

The general philosophy is to localize data movement to the sites by placing vSnap Backup Storage servers and VADP proxies together in the sites. It is advised to always have at least one site per physical location, and at least one vSnap server per site.

The placement of backup data to a site is governed by the SLA policies. Therefore, you specify in which site your backup data will be stored or replicated to, instead of specifying a dedicated vSnap Backup Storage server.
Cases where you want to define multiple sites in a physical location and further considerations together with replication are discussed in the IBM Spectrum Protect Plus Blueprints in *Sites and vSnap server distribution* and *Replication considerations*:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

### 1.2.3 vSnap Backup Storage server

The vSnap Backup Storage server is a pool of disk storage, and the primary backup destination for IBM Spectrum Protect Plus. It receives data from production systems for the purposes of data protection or reuse, and is therefore responsible to store, manage, and maintain this backup data.

A vSnap Backup Storage server provides Compression, Deduplication, and Encryption functionality, and can be deployed as a virtual machine on either a VMware or Microsoft Hyper-V hypervisor infrastructure, or installed on a physical server. Physical installations can use SAN networks for data transfers.

**Note:** A build-in vSnap Backup Storage is predefined with the deployment of IBM Spectrum Protect Plus, and is intended to be used only for product demonstration purposes. It should not be used for a productive backup, and can therefore be deleted in such installations.

The sizing of the vSnap Backup Storage servers is crucial. The IBM Spectrum Protect Plus Blueprints provide the required guidance:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

IBM Spectrum Protect Plus requires at least one vSnap Backup Storage server that is scaled up by adding more disks to increase capacity. Multiple vSnap Backup Storage servers can be deployed in the following ways:

- Per site to scale out for an overall performance increase
- In different sites to achieve local data placement

Redundant Array of Independent Disks (RAID) technology can be used to protect vSnap servers against data loss that is being caused by a hardware failure of a single disk. This protection is either by using software RAID inside the vSnap or by using HW or SW features of the underlying storage system that provides the capacity to the vSnap pool.

The backup data stored by a vSnap server can be replicated to a second vSnap server as an operational protection. Furthermore, backup data can be copied for additional protection to an IBM Spectrum Protect server or to Cloud Storage. Instant access, restore, and data reuse capabilities are provided out of these different backup storage providers.

**Note:** A vSnap Backup Storage server is similar to an IBM Spectrum Protect storage pool in terms of data placement and handling.

### vSnap pool

The disks used by a vSnap Backup Storage server are organized within a vSnap pool. By adding more disks, a vSnap pool is extended. The pool provides log and cache functionalities that are managed on separate disks depending on the size of the pool.
User interfaces

Two user interfaces for the vSnap Backup Storage servers are provided. Graphical access to the vSnap server configuration is provided as part of the web-based IBM Spectrum Protect Plus standard GUI. Under System Configuration → Backup Storage → Disk, all available vSnap Backup Storage servers with their current status and capacity are listed, as shown in Figure 1-8.

![vSnap Backup Storage Overview in the IBM Spectrum Plus GUI](image)

The configuration of the vSnap server could be viewed and changed by clicking the **Edit** icon, which opens the vSnap server configuration page.

The second user interface is a command-line-interface (CLI), which can be entered via SSH using the default serveradmin UserID, as shown in Example 1-1.

**Example 1-1  vSnap Backup Storage CLI**

Using username "serveradmin".

```
serveradmin@spp-vsnap-demo's password:
Last login: Mon Aug 5 13:18:46 2019 from 9.123.45.67
```

----------------------------------------------------------------
Be sure to adhere to vSnap hardware and memory requirements as described in IBM Spectrum Protect Plus Blueprints accessible from the IBM Knowledge Center for IBM Spectrum Protect Plus.

----------------------------------------------------------------

```
[serveradmin@spp-vsnap-demo ~]$ vsnap
Usage: vsnap [OPTIONS] COMMAND [ARGS]...
```

Options:

- `--json` Show output in JSON format.
- `--summary` Show output in summary (tabular) format.
- `--detail` Show output in detail (multiline) format.
- `--help` Show this message and exit.
Commands:
archive       Manage archive resources.
cloud         Manage cloud resources.
disk          Manage disks.
host          Manage volume host mappings.
maint         Manage maintenance sessions.
network       Manage network interfaces.
partner       Manage partner servers.
pool          Manage storage pools.
relationship  Manage replication relationships.
session       Manage replication sessions.
share         Manage volume shares.
snapshot      Manage volume snapshots.
system        Manage vSnap system.
target        Manage storage targets.
throttle      Manage throttling events.
user          Manage vSnap users.
volume        Manage storage volumes.

vSnap configuration
The vSnap Backup Storage server configuration and metadata information can be backed up using the CLI interface, where the vSnap pool data is intact and valid but the configuration or metadata information is lost or not available. A backup file is created locally. The backup can be securely copied to a central location, such as the IBM Spectrum Protect Plus server.

In chapter 3.3.6, “Backing up the vSnap server System Configuration” on page 65, an example configuration is provided. Further information is also available in the Appendix D: Protecting vSnap System Configuration chapter of the IBM Spectrum Protect Plus Blueprints:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

1.2.4 VADP proxy server

The VADP proxy server is the component that is responsible for moving data from the vSphere datastores to the vSnap Backup Storage server to protect VMware virtual machines. As the name implies, it is required only for backing up VMware virtual machines. A VADP proxy could be installed on a virtual or physical machine.

You can install the vSnap server (backup storage provider) and VADP proxy on the same physical or virtual system. IBM Spectrum Protect Plus optimizes data movement by eliminating an NFS mount when these two systems are co-located.

There is always at least one VADP proxy component required for each site, in case VMware virtual machines need to be backed up in this site. Based on sizing needs, more proxy can be required. VADP proxies support the following VMware transport modes: File, SAN, HotAdd, NBDSSL, and NBD. For more information about VMware transport modes, see the vSphere Documentation Center:

The overview and configuration of the VADP proxies can be accessed by selecting **System Configuration → VADP Proxy**, as shown in Figure 1-9.

![VADP Proxy](image.png)

**Figure 1-9  VADP proxy overview in the GUI**

**Note:** A built-in VADP Proxy is predefined with the deployment of IBM Spectrum Protect Plus, and is intended to be used only for product demonstration purposes. It is advised to suspend the **localhost** VADP proxy, and not use it for production backups.

The detailed sizing and configuration of VADP proxies is discussed within the chapter 6. **Configuring VADP Proxies** in the **IBM Spectrum Protect Blueprints**:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

Chapter 3, “Installation and deployment” on page 37 provides more details about installing and deploying a VADP proxy.

### 1.3 SLA backup policies

Backup policies, which are also referred to as **service level agreement** (SLA) policies, define parameters that are applied to backup jobs. The three default SLA policies are Gold, Silver, and Bronze. You can use these policies as they are, modify the policies, or create custom SLA policies. The overview and configuration of SLA policies can be accessed in the GUI by selecting **Manage Protection → Policy Overview**, which displays a **Protection Summary** in the first half of the window, as shown in Figure 1-10 on page 16.
In the second half of the window, the configured and available SLA policies are listed, as shown in Figure 1-11.

**Note:** The Demo SLA is predefined with the deployment of IBM Spectrum Protect Plus and is intended to be used only for product demonstration purposes. It should not be used for a productive backup, and can therefore be deleted in such installations.
To back up virtual machines, databases, and applications, associate them with an appropriate SLA, which creates a corresponding backup job. For example, if a VMware virtual machine is associated with the Bronze SLA, the \texttt{vmware\_Bronze} backup job is created. If a Hyper-V virtual machine is associated with the Silver SLA, the \texttt{hyperv\_Silver} backup job is created.

If a virtual machine is associated with multiple SLA policies, ensure that the policies are not scheduled to run concurrently. Either schedule the SLA policies to run with a significant amount of time between them, or combine them into a single SLA policy.

An SLA defines the following backup parameters, which are applied to virtual machines, databases and applications that are backed up with this SLA:

- How often and when to backup
- How long to retain backups
- How to protect backups

Retention changes in an SLA take effect for future and existing backups associated with that SLA. To delete an SLA policy, ensure that there are no jobs that are associated with the SLA policy. The associated backup instances remain available for recovery until their expiration, as defined previously by the SLA policy.
Solution architecture, planning, and design

This chapter is meant to give you a broad understanding about how to design and implement an IBM Spectrum Protect Plus solution in a virtual environment. It helps you visualize the software interactions with the virtualization layer, operating systems, disk storage, network components, tape storage and other products. It looks at the impact of such deployment within IT teams and the overall IT environment, and discusses how data protection operations can be distributed across the various teams.

This chapter includes the following topics:

- System context
- Roles and responsibilities
- Solution design considerations
- Solution requirements
2.1 System context

In engineering, a *system context diagram* is a diagram that defines the boundary between the system, or part of a system, and its environment, showing the entities that interact with it.

The diagram in Figure 2-1 shows the system context of a typical IBM Spectrum Protect Plus solution. The diagram records the interactions with the existing external systems in the IT infrastructure, and with human actors (users) that might be distributed among several teams.

*Figure 2-1  IBM Spectrum Protect Plus: System context*
Table 2-1 shows how each user or actor interacts with the IBM Spectrum Protect Plus solution in performing their different activities.

**Table 2-1   Users that are involved in an IBM Spectrum Protect Plus solution deployment**

<table>
<thead>
<tr>
<th>Type ID</th>
<th>User/System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT01</td>
<td>IBM Spectrum Protect Plus administrator</td>
<td>The IBM Spectrum Protect Plus administrator manages the IBM Spectrum Protect Plus infrastructure (ES01). ACT01 provides essential services in managing, operating, and configuring infrastructure; scheduling backups, and defining data retention policies. Depending on the IT team in an organization, guest access to protect, restore, or reuse data can also be delegated to users (for example, ACT02, ACT03, and ACT05) by using IBM Spectrum Protect Plus role-based access control (RBAC).</td>
</tr>
<tr>
<td>ACT02</td>
<td>Virtual Infrastructure administrator</td>
<td>ACT02 is the main actor of IBM Spectrum Protect Plus to use it as the backup and restore solution for all of the guests that are hosted in a virtual infrastructure (ES04). ACT02 also provides access to the IBM Spectrum Protect Plus solution for vCenter and the underlying virtual infrastructure components.</td>
</tr>
<tr>
<td>ACT03</td>
<td>Virtual Machine administrator</td>
<td>ACT03 is an IBM Spectrum Protect Plus solution stakeholder whose role is to protect and restore the guests for whom they are responsible.</td>
</tr>
<tr>
<td>ACT04</td>
<td>Network administrator</td>
<td>The network administrator is responsible for the network infrastructure element (ES05), and must provide adequate infrastructure support for the backup and restore requirements.</td>
</tr>
<tr>
<td>ACT05</td>
<td>Application administrator</td>
<td>ACT05 is another stakeholder in the solution who must be aware of how it works and what it can do for their specific database application, such as data reuse and so on.</td>
</tr>
<tr>
<td>ACT06</td>
<td>Storage administrator</td>
<td>ACT06 is responsible to ensure that the IBM Spectrum Protect Plus components have appropriate access to storage components where snapshot copies are retrieved and stored.</td>
</tr>
</tbody>
</table>

Table 2-2 describes how the solution interacts with external systems.

**Table 2-2   External systems involved in the IBM Spectrum Protect Plus solution deployment**

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES01</td>
<td>IBM Spectrum Protect Plus Infrastructure</td>
<td>The IBM Spectrum Protect Plus infrastructure external service is a requirement for the solution to function. It contains several components, such as the IBM Spectrum Protect Plus server, VADP proxy, visnap server, and data retention policy. Without ES01, there cannot be an IBM Spectrum Protect Plus solution.</td>
</tr>
<tr>
<td>ES02</td>
<td>Disk SAN/Object Storage/SCSI Fabric</td>
<td>This external service is where snapshot copies are stored. In some cases, it can also include storage where backups resides before it is migrated to ES03.</td>
</tr>
<tr>
<td>ES03</td>
<td>Tape SAN Fabric</td>
<td>The tape SAN external service is where snapshot copies can be stored to provide a physical air gap. It can be accessed indirectly through the IBM Spectrum Protect server when a second backup copy to physical tape occurs or is accessed.</td>
</tr>
</tbody>
</table>
2.2 Roles and responsibilities

This section presents a summary of the roles, responsibilities, and tasks distributed across the teams and competencies. Depending on the existing structure, the separation of duties, roles, and responsibilities between the teams can vary. An illustration of the distribution of roles and tasks is shown in Figure 2-2 on page 23.

In Figure 2-2 on page 23, bubble intersections represent an operation that can be done by IBM Spectrum Protect administrators, Virtual Machine administrators, or Application administrators, depending on your IT organization. Thus, a bubble intersection indicates that there should be team communication. Each person who is responsible for a task can inform, or request assistance from, other peer users.
2.3 Solution design considerations

The intent of this section is to provide you with examples of key decisions to address when designing a data protection solution for a virtual environment. This information is not intended to replace the analysis of your environment, and is not a complete set of decisions to make. However, it can help you to sketch a design of what your solution might look like, what must be considered to build a data protection solution that meets your requirements, and the typical requirements to consider.

After you have collected the requirements, one of the most important steps in designing a data protection solution is to validate that the architectural decisions meet requirements, including networking, security, and various technology considerations. Because requirements can be met with several approaches, we review these options against their technical advantages or disadvantages, and describe how the specified solution was selected as a result of the following decisions.

Important: Be sure to review the IBM Spectrum Protect Plus Blueprint for essential guidance about how to properly size, build, and place storage components and data movement components.

The latest IBM Spectrum Protect Plus Blueprint can be found at the following website:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints
2.3.1 Dedicated or shared environment

IBM Spectrum Protect Plus can be implemented in a dedicated or in a shared environment. The sizing whether in a dedicated or shared environment. However, in a shared environment, one of the challenges is the security for connecting the VMware or Microsoft HyperV Infrastructure. Another challenge is to access data after it is stored in the IBM Spectrum Protect Plus server.

Depending on your environment, you can consider the implementation of IBM Spectrum Protect Plus components as shared resources. For example, they can be shared between different entities where part of the configuration can be done on the IBM Spectrum Protect Plus server or on the vSnap server.

A shared environment can apply in the following situations:

- A virtual machine to be managed separately (for example, multiple entities in the same office)
- VMware vSphere (ESXi) clusters to be managed separately (for example, one cluster per entity)
- Multiple vCenter servers

With IBM Spectrum Protect Plus server V10.1.4, you can also consider using the implementation of an IBM Spectrum Protect server V8.1.8, enabling you to archive long-term retention data (not mission critical) to physical tape or object storage for an air gap requirement (also explained in 9.4, “Additional Copies to Object, Tape or Archival Storage - Details” on page 160).

archive to physical tape or object storage in chapter 10 here (link)

2.3.2 Network

The network is a crucial component for an IBM Spectrum Protect Plus implementation because the different components need to interact with each other. In one case, dedicated ports for the communication are required. Alternatively, separate networks should be used to cope with the backup and restore workload or to isolate backup traffic from application and user networks. We describe information about network configuration in Chapter 10, “Networking” on page 183.

2.3.3 Encryption

In ransomware attacks and other security breaches, your data protection solution is the last defence and is critical to protect your snapshot copies. Encryption is one solution to “harden” the backup snapshots. As encryption pertains to various layers and elements of an IBM Spectrum Protect Plus environment, there are two encryption approaches to consider: Data at Rest to encrypt stored snapshots and Data in transit to encrypt data transferred between components and sites.

Data at rest: Encryption of data at rest can be accomplished either through the use of encryption capable storage devices, such as the IBM disk or tape storage subsystems, file systems, or applications that support encryption. Encryption capable devices implement in-line transparent encryption of data as it flows onto and off of the associated media.

Encryption of data ensures that, in the event of physical loss of media (either through theft or replacement), the data is unreadable and its confidentiality is maintained.
Data In transit: Data that is being transferred between applications or components is in transit. *Data in transit* is also referred as *data in flight* or *data in motion*. Throughout this publication the term data in flight is used. With IBM Spectrum Protect Plus, SSL is the industry standard used for inter-component communication and data transfer. SSL is a set of rules governing authentication and encrypted communication between clients and servers.

SSL is widely used on the Internet by an increasing number of applications. SSL is positioned as a protocol layer between the Transmission Control Protocol (TCP) layer and the application to form a secure connection between clients and servers so that they can communicate in a secure manner over a network.

Encryption approaches in IBM Spectrum Protect Plus

A user’s decision to enable or disable encryption is driven by several factors:

- Performance considerations
- Security requirements and policies
- Data center design

The following schema in Figure 2-3 presents the various hardware and software components within an IBM Spectrum Protect Plus environment. The orange colored network paths indicate that the network traffic is encrypted when data is in flight by using the SSL protocol. Components that are displayed in green support optional encryption of data at rest.

**Figure 2-3** encryption at rest and in flight in an IBM Spectrum Protect Plus environment

1. IBM Spectrum Protect Plus Server to vSnap: Communication between the server and vSnaps take place over the HTTPS protocol, so it is encrypted using Transport Layer Security (TLS).
2. **vSnap Data Encryption**: IBM Spectrum Protect Plus provides the option to encrypt data using AES 256-bit encryption in the vSnap server at-rest. Data ingested during a backup or replication operation to a vSnap server can be encrypted after the data is compressed or deduplicated. The data remains encrypted in the vSnap server until it is read for a restore, data reuse, or replication operation, at which time it is decrypted.

To use the vSnap encryption feature, a vSnap must be initialized with encryption enabled during creation. All disks of a vSnap pool use the same key file, which is automatically generated upon pool creation. The vSnap is using AES 256-bit encryption. Encryption is a function of the CPUs. The sizing information from the Blueprints and the sizing tool assume that encryption will be used. Encryption consumes 5 - 10% extra CPU resources.

Note: **Encryption** can only be enabled when the pool is created and is not revertible. However, compression and deduplication can be changed on a vSnap pool at any time.

3. **VADP proxy to VMware hypervisors**: VADP proxies in IBM Spectrum Protect Plus support the following VMware transport modes: SAN, HotAdd, NBDSSL, and NBD. Although every enterprise is unique and has different priorities in terms of size, speed, reliability, and complexity, the following general guidelines apply to the Transport Mode selection:

   - SAN transport mode should be used in a direct storage environment because this mode is fast and generally reliable.
   - HotAdd transport mode should be used if the VADP proxy is virtualized. This mode supports all vSphere storage types.
   - NBD or NBDSSL transport mode (LAN) is the fallback mode because it works in physical, virtual, and mixed environments. However, with this mode, data transfer speed might be compromised if network connections are slow. **NBDSSL mode is similar to Network Block device (NBD) mode except that data transferred between the VADP proxy and the hypervisor server is encrypted using SSL.**

4. **vSnap to vSnap replication**: Data that is replicated between two vSnap servers is protected by SSH encryption using Secure Sockets Layer (SSL). When replicating data, the replication process protects the data in-flight. If the data of a vSnap was encrypted at rest, data is decrypted when reading from the source vSnap and encrypted in-flight when data is transferred via a SSL connection.

   You need to ensure that the target vSnap server is also encrypted if you intend to store the replicated data in an encrypted format. There is no dependency between source and target vSnap in terms of encryption configuration as data gets deciphered when data is read from a vSnap.

5. **vSnap to additional protection such as IBM Spectrum Protect, IBM Cloud Object Storage**: The object agent utilizes HTTPS to transfer data to another data store. The communication protocol is encrypted using Transport Layer Security (TLS) and protecting the data in-flight. The user needs to configure the additional protection target system to provide at-rest encryption if the user intends to protect the offloaded data at-rest.

6. **Transparent encryption on VMware datastore or encrypted storage device**: Data can be encrypted at rest utilizing the storage subsystem encryption capabilities, such as self encrypting disks or software encryption at LUNs or pool level. Another option to encrypt VMware related data is the use of an encrypted vSAN instead of encrypting single VMs. The datastore encryption does not rely on the underlaying hardware capabilities and is not mutually exclusive. However, the administrator should not use more than one encryption solution.
7. **Virtual machines:** Encrypted virtual machines are supported in vSphere 6.5 environments and later. These VMs can be backed up and restored at the virtual machine-level to their original location using VMware’s VMcrypt. If you are restoring to an alternative location, the encrypted virtual machine is restored without encryption, and must be encrypted manually through the vCenter Server after the restore completes.

When a virtual machine’s VMDK files are backed up, the files are retrieved decrypted from the hypervisor and are stored decrypted on the vSnap server. If the vSnap is encrypted, the data is protected by the file system encryption.

- More information about VMware vSAN and VMcrypt is documented in the VMware Knowledge base:
  
  https://kb.vmware.com/s/article/2148947

8. **Application Level encryption:** Many applications provide encryption capabilities at the application level. The following section provides a brief overview and introduction to the specific application level encryption implementations:

a. **IBM Db2 native encryption:**

   “Db2 native encryption provides a built-in encryption capability to protect database backup images and key database files from inappropriate access while they are at rest on external storage media.”


b. **Mongo DB - encryption at rest:**

   “The encryption occurs transparently in the storage layer; all data files are fully encrypted from a file system perspective, and data only exists in an unencrypted state in memory and during transmission.”

   https://docs.mongodb.com/manual/core/security-encryption-at-rest
   https://severalnines.com/blog/database-security-how-use-encryption-protect-your-mongodb-data

c. **Oracle - Transparent Data Encryption:**

   “Transparent Data Encryption (TDE) enables you to encrypt sensitive data that you store in tables and table spaces. After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data. TDE helps protect data stored on media (also called data at rest) in the event that the storage media or data file is stolen.”

   https://docs.oracle.com/database/121/ASOAG/introduction-to-transparent-data-encryption.htm

d. **Microsoft SQL Server:**

   Transparent Data Encryption (TDE) encrypts SQL Server, Azure SQL Database, and Azure SQL Data Warehouse data files, known as encrypting data at rest. TDE performs real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK)

2.4 Solution requirements

To design a data protection solution, you need the functional and non-functional requirements. The functional requirements describe what the system has to do: which functions the solution must provide. The non-functional requirements for a business system are usually the capacity, performance, and service level agreements (SLAs).

The non-functional requirements address those aspects of the system that, while not directly affecting the functionality of the system as seen by the users, can have a profound affect on cost. They also affect how the business system is accepted by both the users and the team responsible for supporting that system, while not directly impacting the functionality of the system as seen by the users.

The three most important non-functional requirements in a data protection solution are the recovery time objectives (RTO), recovery point objectives (RPO), and retention policy. These three concepts define backup frequency, retention policy, and the recovery constraints that lead to a consistent implementation of a data protection solution.

RTO refers to the amount of time it takes to restore a data set or application following a service disruption. RPO refers to the available recovery points in time to restore from. In addition to RTO and RPO values, the retention policy requirement defines for how long a backup exists in the IBM Spectrum Protect Plus solution.

Other typical functional requirements include these tasks:

- **VMware and Hyper-V backup and restore:**
  - The system must be able to perform whole VM backups of VMware and Hyper-V virtual machines.
  - The system must be able to restore a virtual machine back into production to replace a lost or damaged production VM.
  - The system must be able to perform test restores of individual virtual machines into an isolated environment separated from production.

- **VM and database cloning**
  The system must be able to clone individual databases or virtual machines for data reuse for test/dev environments with different attributes, such as the name, network location, and so on.

- **Replication:**
  - The solution must be able to replicate backups offsite at least once a day and be available for restore at the destination once data is transferred.
  - The solution must be able to provide a third backup copy on a Cloud provider.

Typical non-functional none requirements are:

- **Availability**
  The system must be available 99.9% of the time, excluding planned downtime for maintenance.

- **Durability**
  The system must be able to avoid data loss due to a single component failure, such as a power supply, a single hard drive, and so on.
Disaster recovery
The system must be capable of recovering from an entire site loss for customers with a requirement for offsite recovery.

Scalability
The solution must be able to scale in place as the customer grows without having to rip and replace existing components with larger hardware. The service can accomplish this by either growing bigger (scale up), or growing wider (scale out), or a combination of the two.

Performance:
- The system must have well defined performance characteristics that provide consistent speeds that grow along with capacity as part of the scalability model.
- Alerting can occur for example via Restful API, e-mail, or syslog.

Capacity management
The system must provide a mechanism for assessing capacity usage, and generating alarms as the system approaches full capacity.

Alerting
The system must provide a mechanism for sending alerts about events, such as performance issues, and about temporary errors indicating emerging problems are quickly acted to typical external alerting tools via standard protocols (syslog, SNMP).

Provide awareness and security
The system must provide encryption at rest functionality and encrypt data transmitted over the WAN.

Billing
Provide usage-based billing based on the amount of data stored in the system by using, for example, API calls to the IBM Spectrum Protect Plus server to generate billing volume data.

Network separation
Provide network separation as an extra security layer so backups are not using management or adversely impacting business applications.

Network bandwidth
Provide the required bandwidth between the hypervisors, application servers, VADP proxies, and the vSnap servers.

Firewall
Specific communication paths through a firewall need to be open for the involved components placed in secured network environments.

2.4.1 Architectural decisions

The purpose of the architectural decision section is to give you guidance and help you make explicit the rationale and justification of different decisions, and to ensure that the architecture is extensible and can potentially support an evolving specification. The architect decisions also provide you a reference of documented decisions to avoid unnecessary reconsideration of the same issues.
Here are the top architectural decisions that you need to consider that can help you to meet the desired outcomes:

- Data reduction AD01
- Disk technology AD02
- Encryption Authentication tool AD03
- Authentication tool AD04
- vSnap server deployment AD05
- Alerting tool
- Sites and vSnap server distribution
- Replication considerations
- Throttling network usage during replication and offload operations
- VADP proxy considerations
- IBM Spectrum Protect Plus server and VADP proxy logical component placement
- IBM Spectrum Protect Plus server component placement
- Billing
- Networking

To illustrate the concept of architecture decisions, we show examples (Table 2-3, Table 2-4 on page 31, Table 2-5 on page 32, Table 2-6 on page 33, Table 2-7 on page 34, and Table 2-8 on page 35) of how to articulate such decisions for a typical enterprise customer.

**Remember:** The examples are only for illustration. Architectural decisions could be different in your environment. You need to evaluate how different options apply to your business requirements and base your own decisions on what fits best in your environment.

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Area of Concern</th>
<th>Topic</th>
<th>Topic of Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>Enable deduplication with compression.</td>
<td>AD ID</td>
<td>AD01</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>What is the technology to use for reducing the data capacity for storing backups copies.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>- Compression is enabled on the vSnap server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Aggressive RTOs requirements such as “boot from backup” to resume production work instantly, such as starting an Oracle database directly from vSnap server, versus first migrating it back to production storage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation</td>
<td>Reducing storage cost while providing rapid recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternatives</td>
<td>- Enable deduplication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Do not enable deduplication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Only use deduplication with flash/SSD disks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>Enable deduplication with compression.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td>You have decided to use SSDs or Flash disk that gives an advantage for using deduplication for saving storage cost.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derived requirements</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Decisions</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject Area</td>
<td>Area of Concern</td>
<td>Topic</td>
<td>Topic of Interest</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Architectural Decision</td>
<td>Use IBM Storwize® v5000 Distributed RAID</td>
<td>AD ID</td>
<td>AD02</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>How do we protect the vSnap server from disk failures e.g. RAID protection?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>There is a pre-existing investment in storage that provides storage hardware RAID such as the IBM Storwize v5000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation</td>
<td>Ensure stable and proven backup storage environment.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Alternatives     | 1. Software RAID  
                      2. Hardware DRAID                                                              |       |                   |
| Decision         | Hardware DRAID                                                                   |       |                   |
| Justification    | Distributed RAID 6 technology protect the vSnap server from disk failures and improve rebuild performance combined with vSnap RAID 0.  
                      If storage hardware RAID is not available in the storage system (for example, a JBOD configuration), use the vSnap server provisioned RAID 6 to take advantage of this that the vSnap server provisioned software RAID can detect and correct data corruption. |       |                   |
<p>| Implications     | N/A                                                                              |       |                   |
| Derived requirements | N/A                          |       |                   |
| Related Decisions | N/A                                                                            |       |                   |</p>
<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Area of Concern</th>
<th>Topic</th>
<th>Topic of Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>Encrypt at rest method by using vSnap server native encryption and encrypt between, for example, data centers where data goes over TLS (https) connection.</td>
<td>AD ID</td>
<td>AD03</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>How do you provide an encryption at rest and in flight solution for data stored on IBM Spectrum Protect Plus vSnap servers that aligns with technical best practices?</td>
<td>Assumptions</td>
<td>All customers are subject to GDPR unless there is a formal letter saying that they are not.</td>
</tr>
<tr>
<td>Motivation</td>
<td>The solution must ensure both the security of the data from physical device theft and minimize the risk of data loss through key loss.</td>
<td>Alternatives</td>
<td>1. Encrypt at rest. 2. Encrypt over TLS (https) connection.</td>
</tr>
<tr>
<td>Decision</td>
<td>Use both alternatives to encrypt at rest method by using Spectrum Protect Plus vSnap server native encryption. Encrypt between e.g. data centers where data goes over a TLS (https) connection.</td>
<td>Justification</td>
<td>IBM Spectrum Protect Plus encrypts both the source and target IBM Spectrum Protect servers at rest. As long as both the source and target servers are configured for encrypt at rest, the data will be encrypted respectively by each of the servers. Encryption between e.g. data centers goes over a TLS (https) connection, so the data is not vulnerable while being transmitted. The built-in encryption functionality is an easy turn on functionality, with no extra license cost needed.</td>
</tr>
<tr>
<td>Implications</td>
<td>N/A</td>
<td>Derived requirements</td>
<td>N/A</td>
</tr>
<tr>
<td>Related Decisions</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2-6  Architect decisions 04

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Area of Concern</th>
<th>Topic</th>
<th>Topic of Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>Microsoft Active Directory authentication</td>
<td>AD ID</td>
<td>AD04</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>What authentication method to use for the administrator that manages the IBM Spectrum Protect Plus infrastructure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>There is a Microsoft Active Directory infrastructure.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation</td>
<td>Centralized authentication management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternatives</td>
<td>Microsoft Active Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>The existing Microsoft Active Directory infrastructure will be used for authentication IBM Spectrum Protect Plus administrator.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td>The centralized authentication management improves the ability to ensure that user identification are appropriately managed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derived requirements</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Decisions</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject Area</td>
<td>Area of Concern</td>
<td>Topic</td>
<td>Topic of Interest</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Architectural Decision</td>
<td>Use physical vSnap servers for large environments and virtual vSnap server for small environments.</td>
<td>AD ID</td>
<td>AD05</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>Determine the deployment of physical or virtual vSnap server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>Most deployments will require both separate vSnap servers and single server deployments of IBM Spectrum Protect Plus.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation</td>
<td>Using both alternatives increases efficiency.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternatives</td>
<td>Virtualize all vSnap servers. Provide physical vSnap servers with hardware RAID.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>For environments of significant scale deploy required separate physical vSnap servers with hardware RAID. Smaller scale deployments can use virtual vSnap servers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td>The virtualization infrastructure is evaluated to avoid common points of failure between vSnap and the workloads that it protects to avoid the risk of single events destroying production and backup including cyber incidents.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derived requirements</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Decisions</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 2-8  Architect decisions 06

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Area of Concern</th>
<th>Topic</th>
<th>Topic of Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Decision</td>
<td>Use Syslog based alerting</td>
<td>AD ID</td>
<td>AD06</td>
</tr>
<tr>
<td>Issue or Problem</td>
<td>What alerting tool to use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assumptions</td>
<td>IBM Spectrum Protect Plus is used in large scale delivery operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motivation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternatives</td>
<td>- API</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- E-mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Syslog</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision</td>
<td>Use Syslog based alerting tooling.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td>The alerting and ticketing platform is designed around receiving SNMP traps or syslog messages for alerting from platforms. Emailing administrators is okay in small environments it does not provide the tracking or accountability needed for large scale delivery operations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derived requirements</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Decisions</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3. Installation and deployment

This chapter reviews the prerequisites for installing and deploying an IBM Spectrum Protect Plus environment, and in particular for the following essential components:

- The IBM Spectrum Protect Plus server
- The vSnap Backup Storage server
- The VADP proxy server

This chapter is not meant to duplicate the installation procedure available in IBM Knowledge Center, but rather provides guidance for the initial configuration and appropriate settings following the installation and deployment.

This chapter includes the following topics:

- Review the prerequisites for an IBM Spectrum Protect Plus deployment
- Installation and deployment
- Configuration of the IBM Spectrum Protect Plus environment
3.1 Review the prerequisites for an IBM Spectrum Protect Plus deployment

Before starting the installation and deployment of an IBM Spectrum Protect Plus environment, prerequisites and planning aspects need to be reviewed and understood. Chapter 2, “Solution architecture, planning, and design” on page 19 discusses what to consider for planning.

The outcome of the planning phase is in part to know the number and size of vSnap Backup Storage servers and the number of VADP proxies that are required for an adequate backup infrastructure.

The IBM Spectrum Protect Plus - All Requirements Doc is a very good reference:

https://www.ibm.com/support/docview.wss?uid=swg22013790

The document lists all requirements categorized for the different IBM Spectrum Protect Plus versions, including the IBM Spectrum Protect Plus components as well as requirements for the hypervisors, databases, and applications. The requirements for the IBM Spectrum Protect Plus server, vSnap server, and VADP proxy is listed under the System requirements for the specific version.

It is essential to also prepare and check your DNS infrastructure to include entries for your IBM Spectrum Protect Plus environment before you start the deployment. All IBM Spectrum Protect Plus system components can use DHCP, but the usage of static IP address assignments, including properly configured DNS names, is desirable for a productive IBM Spectrum Plus environment.

A common time zone and network time protocol server (NTP server) setting is recommended to be used for the IBM Spectrum Plus server, vSnap server, and VADP proxy server. In chapter 3.3.7, “Change and verify the schedules of the predefined jobs” on page 68 we discuss the configuration of the time zone and NTP server configuration.

3.1.1 Requirements for IBM Spectrum Protect server

The IBM Spectrum Protect Plus server must be deployed either on a VMware or Microsoft Hyper-V infrastructure. For VMware, a vCenter server is required to perform backup and restore activities on VMware virtual machines.

The download size of the installation image (.ova for VMware, .exe for Hyper-V) is about 2.6 GB, while the thick provisioned installed IBM Spectrum Protect Plus server virtual machine (VM) size is 528.0 GB in total. The provisioned size of the server VM is preconfigured and also suitable for large IBM Spectrum Protect Plus deployments.

Always use thick provisioned disks for the IBM Spectrum Protect Plus server VM in a production environment, and consider a deployment on SSD or Flash disk datastores to make the VM most performant. The IBM Spectrum Protect Plus server uses several internal catalogs, which benefit especially in larger installations from a faster datastore.

Review the IBM Spectrum Protect Plus - All Requirements Doc for details of supported Hypervisor versions, CPU, and memory requirements:

https://www.ibm.com/support/docview.wss?uid=swg22013790
3.1.2 Requirements for the vSnap Backup Storage server

A vSnap server is the primary backup destination for IBM Spectrum Protect Plus. It could be installed and deployed either on a physical server or as a preconfigured virtual machine in a VMware or Microsoft Hyper-V infrastructure.

The decision if a physical or virtual vSnap server deployment is preferable is a user decision. Most important factor is that you size the vSnap server resources (memory, CPU, and so on) appropriately. The chapter Physical or virtual vSnap server deployment in the IBM Spectrum Protect Plus Blueprints discuss this decision further.

Along with the decision about a physical and virtual deployment, is the disk technology used. Simply said, are you using just storage out of an existing RAID-protected datastore for example in VMware, or are you using a dedicated disk storage sub-subsystem where you need to use the Software RAID feature of the vSnap to protect your backup storage against disk failures.

The chapter Server and Storage Configuration Blueprints documents the detailed requirements and recommendations to build a vSnap Backup Storage server. It also includes details about the required CPU and memory for the system, because this goes along with the planned size of the vSnap server. The IBM Spectrum Protect Plus Blueprints can be found here:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

The IBM Spectrum Protect Plus - All Requirements Doc also lists details of supported Hypervisor and Operating System versions and the minimum CPU and memory requirements:

https://www.ibm.com/support/docview.wss?uid=swg22013790

Note: The OVF package for VMware contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below:

spp.vm.mode = appliance

3.1.3 Requirements for the VADP proxy server

The VADP proxy is required for the moving data from the VMware vSphere datastores to the vSnap Backup Storage server for protection of the VMware virtual machines. It could be installed on a physical and virtual server.

You can install the vSnap server (backup storage provider) and VADP proxy on the same physical or virtual system. IBM Spectrum Protect Plus optimizes data movement by eliminating an NFS mount when these two systems are co-located.
If you choose to collocate these two components make sure the system is sized appropriately for both workloads, taking the sum of the CPU, memory, and storage requirements of the two components.

The *IBM Spectrum Protect Plus - All Requirements Doc* lists all of the details of supported Operating System versions and the CPU and memory requirements, especially when running a combination of vSnap and VADP proxy server:

https://www.ibm.com/support/docview.wss?uid=swg22013790

3.2 Installation and deployment

This chapter discusses the installation of IBM Spectrum Protect Plus and its components. Based on the results of the planning and sizing, the installation of the IBM Spectrum Protect Plus solution can be started. Remember the following aspects from the planning phase:

- An architectural overview of the installed solution is required:
  - VMware and/or Hyper-V infrastructure?
  - How many locations / datacenter will be translated into Site definition to achieve local data placement?
  - What type of disk storage is used for the vSnap servers as primary backup destination?
- How is the backup data protected?
  See Chapter 9, “Additional Copies of Backup Data” on page 153 for details
- A proper solution sizing using the Blueprint Sizing tool is required:
  - How many VMs, databases, and applications should be backed up?
  - What is the expected amount of data to be backed up?
  - How long should the data be retained?

This planning which we discussed in Chapter 2, “Solution architecture, planning, and design” on page 19 will give you the required information for installing the IBM Spectrum Protect Plus solution:

- How many Sites need to be configured?
- How many vSnap servers need to be deployed?
  - Virtual or Physical installation?
- How many VADP proxy server need to be installed?
  - Virtual or Physical installation?
  - Will the VADP proxies run together with vSnap server in the same VM or server?

The result of the planning and sizing phase in our example is that we will install an IBM Spectrum Protect Plus server and three virtual vSnap Backup Storage servers with an integrated VADP proxy server on an existing VMware environment in three locations, as shown in Figure 3-1 on page 41.
In the next sections we show the steps detailing how this solution is installed. Further information about the installation process is documented in two places:

- IBM Knowledge Center for IBM Spectrum Protect Plus:  

- IBM Spectrum Protect Plus Blueprints:  
  [https://ibm.biz/IBMSpectrumProtectPlusBlueprints](https://ibm.biz/IBMSpectrumProtectPlusBlueprints)

After all components are deployed, we continue in chapter 3.3, “Configuration of the IBM Spectrum Protect Plus environment”.

### 3.2.1 Deploy the IBM Spectrum Protect Plus server

Before the deployment of the IBM Spectrum Protect Plus server as a virtual appliance in a VMware environment you need to have the following information available:

- Virtual machine (VM) name for the IBM Spectrum Protect Plus server
- Which Datacenter, ESX host, and datastore to be used for the VM (Virtual disk format: Thick Provision)
- VM Network interface to be used from the VMware infrastructure
- Hostname (most probably the VM name) of the IBM Spectrum Protect Plus server
- Network IP Address for the IBM Spectrum Protect Plus server
- Netmask (Network Prefix) for the IP subnet, for example, 24 for a 255.255.255.0 subnet mask
- Default Gateway
- DNS server names
- DNS domain name used together with the hostname as the fully qualified domain name (FQDN)
Use the VMware vSphere client to deploy an OVA template
When all information is available, deploy the IBM Spectrum Protect Plus server using the VMware vSphere Client.

**Note:** Documentation about how to log in to the vCenter Server by using the vSphere Client is available from VMware:  

After logging in to the vSphere Client start the deployment wizard by right-clicking the used datacenter and selecting **Deploy OVF Template**, as shown in Figure 3-2.

![Figure 3-2  Deploy an OVF or OVA Template in the VMware vSphere Client](image)

**Note:** General information about deployment of OVA templates is available from VMware:  

The deployment wizard guides your through the required settings from the list above. Most settings need to be entered at the **Customize template** section as shown in Figure 3-3 on page 43 for our deployment example.
Chapter 3. Installation and deployment

Finally, a summary page is displayed where you can review all your settings before deploying the VM.

The vSphere Client shows a progress bar for the deployment, as shown in Figure 3-4.

Wait until the deployment is completed and then start the virtual machine (VM).

**Important:** Give the VM several minutes after powering on to initialize completely, especially for the first boot after the deployment.
The next step is to deploy the vSnap and VADP proxy servers. After all components are installed and deployed, go through the configuration steps in 3.3, “Configuration of the IBM Spectrum Protect Plus environment” on page 45.

3.2.2 Deploy the vSnap Backup Storage and VADP proxy server

In our example, we deploy a virtual vSnap Backup Storage server including a VADP proxy server. For the deployment of a physical vSnap server, see the IBM Spectrum Protect Plus Blueprints for more details:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

Before the deployment of the vSnap server as a virtual appliance in an VMware environment you need to have the following information available:

- Virtual machine (VM) name for the vSnap server
- Which Datacenter, ESX host and datastore to be used for the VM
  - Virtual disk format: Thick Provision
- VM Network interface to be used from the VMware infrastructure
- IP Address of the IBM Spectrum Protect Plus server

Important: The VADP proxy is included within the vSnap server deployment automatically. In order to enable and register the VADP proxy during deployment, it is required to specify the IP address of the IBM Spectrum Protect Plus server as the first entry in the Customization template of the deployment wizard.

- Hostname (most probably the VM name) of the vSnap server
- Network IP Address for the vSnap server
- Netmask (Network Prefix) for the IP subnet, e.g. 24 for a 255.255.255.0 subnet mask
- Default Gateway
- DNS servername(s)
- DNS domain name used together with the hostname as Full Qualified Domain Name (FQDN)

After all information is available, deploy the vSnap server using the VMware vSphere Client as shown in “Use the VMware vSphere client to deploy an OVA template” on page 42.

Wait until the deployment is completed and afterwards power on the virtual machine (VM).

This step is repeated to deploy all three vSnap servers as shown in Figure 3-1 on page 41.

Important: Give the VM several minutes after powering on to initialize completely, especially for the first boot after the deployment.
3.3 Configuration of the IBM Spectrum Protect Plus environment

After the deployment of the IBM Spectrum Protect Plus server, the vSnap Backup Storage server, and the VADP proxy, the next step is the configuration of the components. This includes the following steps:

1. Configure the IBM Spectrum Protect Plus server
2. Configure the vSnap Backup Storage server
3. Configure NTP for the IBM Spectrum Protect Plus and the vSnap server
4. Connect the vSnap and VADP Proxy server with the IBM Spectrum Protect Plus server
5. Add an SLA for IBM Spectrum Protect Plus catalog backup
6. Backing up the vSnap server System Configuration

A completion of all configuration steps gives you an IBM Spectrum Protect Plus environment following best practices and ready for taking backups from VMs and Databases, as described in Chapter 4, “Backup and Restore VM” on page 71 and Chapter 5, “Backup and Restore databases” on page 99.

3.3.1 Configure the IBM Spectrum Protect Plus server

In 3.2.1, “Deploy the IBM Spectrum Protect Plus server” on page 41 the IBM Spectrum Protect Plus server is deployed and as a last step the VM is powered on.

**Important:** Give the VM several minutes after powering on to initialize completely, especially for the first boot after the deployment!

The IBM Spectrum Protect Plus graphical user interface (GUI) can be entered using https URL on your preferred supported web-browser (for example, https://spp-server/). Further details about the GUI and its function is explained in “User interfaces” on page 5.
Initial Login to IBM Spectrum Protect Plus
When the IBM Spectrum Protect Plus server VM is up and running, a log in screen displays to enter the GUI web interface, as shown in Figure 3-5.

Note: If this is your first time logging on, the default user name is admin and the default password is password.

At the initial login to IBM Spectrum Protect Plus, three actions must be completed before entering the Dashboard view:
1. Username and password of the administrative ID admin must be changed
2. Password must be changed for the local system user ID serveradmin
3. Built-in vSnap server must be initialized

Changing the username and password of the administrative ID admin
At initial login the default user ID admin must be changed to a meaningful name, as shown in Figure 3-5. As a best practice, the recommendation is to change the ID admin to the name superuser. The background of this recommendation is that this initial administrative account has a dedicated user role with the same name. Even if later personalized user IDs or users from an LDAP directory are added, this user remains and cannot be deleted. If you prefer to set it to another name this will work as well, except for admin, root or test.
In addition to the user name of this administrative ID, the password must also be changed, as shown in Figure 3-6.

![Figure 3-6 Change the initial login credentials](image)

Note: It is not possible to reset the username to admin, root, or test. The minimum password length must be at least eight characters.

Changing the password for the local system user ID serveradmin

In addition you must change the password of the local system user ID serveradmin. This user ID is used for logins at Operating System level and can be used for login to the Administrative Console web interface.

Note: The initial password of the user ID serveradmin is sppDP758.

Figure 3-7 on page 48 shows the change password dialog. The new password for the serveradmin user ID must follow the following password rules:

- Minimum password length of 9 characters
- Minimum of 5 characters in the new password must not be present in the old password
- Minimum of 1 numerical digit in the new password
- Minimum of 1 uppercase character in the new password
- Minimum of 1 lowercase character in the new password
- Minimum of 1 other character in the new password
Initializing the built-in vSnap server

Initialize the built-in vSnap server that belongs to the site DEMO. There is no possibility to skip this step. Select **Initialize without encryption**, as shown in Figure 3-8.

Define and configure the required sites

The definition of sites in IBM Spectrum Protect Plus is used to organize resources and to organize a local backup data placement. Principles of sites are discussed in 1.2.2, “Site” on page 11. Following our example in Figure 3-1 on page 41, we need to configure 3 sites:

- DC1
- DC2
- DMZ
To achieve this we are going to rename the pre-defined **Primary** and **Secondary** site and add a third one under **System Configuration → Site**. To rename a site, click the 🏛️ icon in front of the existing site name. After the two sites are renamed, the third site is added by clicking the right corner on **Add Site**. Figure 3-9 shows the overview of the sites after the described changes.

![Site](image)

**Figure 3-9  Define the required sites in IBM Spectrum Protect Plus**

**Deleting the DEMO configuration**

As explained in Chapter 1, “IBM Spectrum Protect Plus product architecture and components” on page 1, the initial deployment of the IBM Spectrum Protect Plus server includes a configuration of a DEMO setup. This DEMO setup consists of the following configuration items:

- vSnap Backup Storage server with 100 GB capacity
- VADP proxy server
- DEMO SLA configured for a daily backup with a retention of 1 months
- DEMO site

The intention of this DEMO configuration is only for product demonstration purposes. It should not be used for a productive backup and can therefore be deleted in productive installations.

**Delete the local built-in vSnap server**

We are not going to use the built-in vSnap server because of resource and performance reasons. In this step, we delete it.
In the IBM Spectrum Protect Plus GUI, select **System Configuration → Backup Storage → Disk** and delete the vSnap on the localhost in the DEMO site by clicking the X sign on the left side, as shown in Figure 3-10.

![Disk Storage](image)

*Figure 3-10  Local vSnap disk storage for the Demo site*

You must confirm the deletion by entering a confirmation code and clicking the **DELETE** button, as shown in Figure 5-6.

![Confirm](image)

*Figure 3-11  Confirm deletion*

**Suspend local built-in VADP proxy**

As a best practices recommendation, the built-in VADP proxy is not used. We will show how to suspend it because it is not possible to remove it completely.
In the IBM Spectrum Protect Plus GUI, select **System Configuration → VADP Proxy**, select **localhost**, click the three dots on the upper right, and select **Suspend**, as shown in Figure 3-12.

![VADP Proxies](image)

*Figure 3-12  Suspend local built-in VADP proxy*

**Delete DEMO SLA**

The SLA DEMO for demonstration purposes is not used. To delete it go in the IBM Spectrum Protect Plus GUI to **Manage Protection → Policy Overview**, select the SLA Policy **Demo**, and click the X next to it to delete it.

**Delete DEMO Site**

Finally, to clean up the IBM Spectrum Protect Plus environment from the sample configuration, it is also a best practice to delete the site **Demo**. In the IBM Spectrum Protect Plus GUI, select **System configuration → Site**, click the X beside the Site **Demo**, and confirm deletion. After the deletion of the **Demo** site, the **Sites** view displays the remaining configured **DC1**, **DC2** and **DMZ** sites, as shown in Figure 3-13.

![Sites](image)

*Figure 3-13  Sites - Demo site deleted*

The initial configuration of the IBM Spectrum Protect Plus server is now completed.
3.3.2 Configure the vSnap Backup Storage server

In 3.2.2, “Deploy the vSnap Backup Storage and VADP proxy server” on page 44, the vSnap Backup Storage server is deployed and as a last step the VM is powered on.

Important: Give the VM several minutes after powering on to initialize completely, especially for the first boot after the deployment!

After the deployment of the vSnap Backup Storage server perform the following steps to configure the VM for the vSnap server before it can be used:

1. Change the password for the local system user ID serveradmin
2. Create a vSnap user

Change serveradmin password

After a new deployment of the vSnap backup storage appliance you must change the serveradmin password at the initial login.

Log in to the vSnap server with the SSH protocol using a terminal or putty client. Use the serveradmin userid and change the password. It is possible to use the same password that was used for the serveradmin user at the IBM Spectrum Protect Plus server.

Note: The initial password of the user ID serveradmin is sppDP758.

Example 3-1 shows the change password dialog. The new password for the serveradmin user ID must follow the following password rules:

- Minimum password length of 9 characters
- Minimum of 5 characters in the new password must not be present in the old password
- Minimum of 1 numerical digit in the new password
- Minimum of 1 uppercase character in the new password
- Minimum of 1 lowercase character in the new password
- Minimum of 1 other character in the new password

Example 3-1 Initial vSnap server login

login as: serveradmin
serveradmin@t3-spp-vsnap's password:
You are required to change your password immediately (root enforced)

Be sure to adhere to vSnap hardware and memory requirements as described in IBM Spectrum Protect Plus Blueprints accessible from the IBM Knowledge Center for IBM Spectrum Protect Plus.

WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user serveradmin.
Changing password for serveradmin.
(current) UNIX password:
New password:
Retype new password:

After the password is changed, you need to re-login using the new password.
Create vSnap user
To differentiate activities inside an IBM Spectrum Protect Plus environment its recommended to create an additional user which we call vsnapadmin for the vSnap server with the vsnap_admin role by using the vSnap command: vsnap user create --username vsnapadmin --password PASSWORD as shown in Example 3-2. This user is used in a later step to connect the vSnap server and the IBM Spectrum Protect Plus server.

Example 3-2  Create vsnapadmin user

```bash
[serveradmin@t3-spp-vsnap ~]$ vsnap user create --username vsnapadmin --password PASSWORD
vsnap user create --username vsnapadmin --password PASSWORD
UID: 1002
GID: 1002
NAME: vsnapadmin
ROLE: vsnap_admin
```

In our example, we initialize the vSnap servers using the IBM Spectrum Protect Plus GUI in 3.3.4, “Connect the vSnap and VADP Proxy server with the IBM Spectrum Protect Plus server” on page 55. We also use the GUI to add additional virtual disks to the vSnap server. An alternative is to initialize the vSnap server using the CLI and also create the vSnap pool using the CLI. For larger installations this is the recommended approach.

In Chapter 13, “The vSnap CLI” on page 233, we explain the commands required on the CLI. For more information, the chapter vSnap Server Installation and Setup in the IBM Spectrum Protect Plus Blueprints discusses this in detail:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

3.3.3 Configure NTP for the IBM Spectrum Protect Plus and the vSnap server
To help avoid issues that can result from time zone differences, use a Network Time Protocol (NTP) server to synchronize time zones across IBM Spectrum Protect Plus resources that are in your environment, such as the IBM Spectrum Protect Plus virtual appliance, storage arrays, hypervisors, and application servers. If the time zones are out of sync, you might experience errors during application registration, metadata cataloging, inventory, backup, or restore, or file restore jobs.

To synchronize time zones for IBM Spectrum Protect Plus server and the vSnap Backup Storage server, use the CLI on the each of the servers. After the initial deployment the time zone is set to UTC.

Check the current time zone setting
Use the timedatectl command to show the current settings, as shown in Example 3-3.

Example 3-3  CLI - timedatectl

```bash
[serveradmin@t3-spp-server ~]$ timedatectl
  Local time: Wed 2019-07-24 07:25:07 UTC
  Universal time: Wed 2019-07-24 07:25:07 UTC
  RTC time: Wed 2019-07-24 07:25:03
  Time zone: UTC (UTC, +0000)
```
NTP enabled: yes
NTP synchronized: no
RTC in local TZ: yes
DST active: n/a

Warning: The system is configured to read the RTC time in the local time zone. This mode can not be fully supported. It will create various problems with time zone changes and daylight saving time adjustments. The RTC time is never updated, it relies on external facilities to maintain it. If at all possible, use RTC in UTC by calling
'timedatectl set-local-rtc 0'.

[serveradmin@t3-spp-server ~]$ sudo timedatectl set-local-rtc 0

Reconfigure to read the RTC
The Real Time Clock (RTC) is not a good solution to spread time information across several servers.

Use the command sudo timedatectl set-local-rtc 0 to disable using the RTC time.

Configure/set the time zone
As a next step the time zone need to be set using timedatectl command. Using this command avoids deleting /etc/localtime and creating a new link to it.

Use the sudo timedatectl set-timezone Europe/Berlin command to set the time zone in our example to Europe/Berlin.

Edit chrony configuration
To enable the NTP timeserver in your environment, change the server parameter in the /etc/chrony.conf chrony configuration file to a local reachable NTP server and disable the default server settings. In the example below we use the vi editor to show the activation of the timeserver ntp.escc.workshop and the deactivation of the default timeservers by remarking them in the configuration file. Note that Example 3-4 shows the last lines of the config file.

Use the command sudo vi /etc/chrony.conf to edit chrony configuration file.

Example 3-4   The /etc/chrony.conf file

...  
# Serve time even if not synchronized to a time source.  
#local stratum 10  

# Specify file containing keys for NTP authentication.  
#keyfile /etc/chrony.keys  

# Specify directory for log files.  
#logdir /var/log/chrony  

# Select which information is logged.  
#log measurements statistics tracking  
#server 0.north-america.pool.ntp.org  
#server 1.north-america.pool.ntp.org  
#server 2.north-america.pool.ntp.org  
#server 3.north-america.pool.ntp.org  
server ntp.escc.workshop
Restart the chrony daemon
After the change in the /etc/chrony.conf the daemon needs to be restarted.

Use the command `sudo systemctl restart chronyd` to restart the chrony daemon and check the chrony status with the command `sudo systemctl status chronyd` as shown in Example 3-5.

Example 3-5  CLI - systemctl status chronyd

```
[serveradmin@t3-spp-server ~]$ sudo systemctl restart chronyd
[serveradmin@t3-spp-server ~]$ sudo systemctl status chronyd
? chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2019-07-24 10:37:23 CEST; 5s ago
     Docs: man:chronyd(8)
           man:chrony.conf(5)
     Process: 6689 ExecStartPost=/usr/libexec/chrony-helper update-daemon
              (code=exited, status=0/SUCCESS)
     Process: 6685 ExecStart=/usr/sbin/chronyd $OPTIONS (code=exited,
              status=0/SUCCESS)
     Main PID: 6687 (chronyd)
        CGroup: /system.slice/chronyd.service
               ● 6687 /usr/sbin/chronyd

Jul 24 10:37:23 t3-spp-server systemd[1]: Starting NTP client/server...
Jul 24 10:37:23 t3-spp-server chronyd[6687]: chronyd version 3.2 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP...EBUG)
Jul 24 10:37:23 t3-spp-server chronyd[6687]: Frequency -20.168 +/- 46.716 ppm read from /var/lib/chrony/drift
Hint: Some lines were ellipsized, use -l to show in full.
```

Check the active timeserver
To check the current active timeserver in use, use the command `chronyc sources` as shown in Example 3-6.

Example 3-6  chronyc sources

```
[serveradmin@t3-spp-server ~]$ chronyc sources
210 Number of sources = 1
MS Name/IP address Stratum Poll Reach LastRx Last sample
===============================================================================
^? ntp.escc.workshop 1 6 3 2 -20.0s [-20.0s] +/- 10.6s
[serveradmin@t3-spp-server ~]$
```

3.3.4 Connect the vSnap and VADP Proxy server with the IBM Spectrum Protect Plus server
After the deployment of the IBM Spectrum Protect Plus server, the required vSnap Backup Storage servers and the VADP proxies needs to be connected and enabled in IBM Spectrum Protect Plus.
Add additional identities to the environment
To connect a vSnap server and a VADP proxy resource in IBM Spectrum Protect Plus credentials are required. For the vSnap server we use the created vsnapadmin account (see “Create vSnap user” on page 53) and for the VADP proxy we use the local system account serveradmin (see “Change serveradmin password” on page 52). Both credentials are added as identities, which we discussed in “Identities” on page 9. The credentials are added to IBM Spectrum Protect Plus and are then referred to as Use existing user when the resource is added. The Identity view under Accounts → Identity lists both identities after they where added, as shown in Figure 3-14.

![Identity view](Image)

Enable VADP proxy
The VADP proxies installed together with the vSnap Backup Storage servers in the IBM Spectrum Protect Plus GUI under System Configuration → VADP Proxy listed. Immediately after the deployment, the VADP proxies are listed in the view without a Version and Status information, as shown in Figure 3-15 on page 57.
As a next step, each VADP Proxy needs to be enabled and added to the appropriate site. After selecting a vSnap server from the list, the **Enable Proxy** button displays in the right part of the view, as shown in Figure 3-16.

**Figure 3-15  VADP Proxy view after the deployment**

**Figure 3-16  Enable a VADP Proxy**
After clicking the **Enable Proxy** button, a new view appears where you need to add the proxy to the appropriate site and use the existing user **serveradmin** to add the resource, as shown in Figure 3-17.

![VADP Proxy](image)

**Figure 3-17** Specify details to enable the VADP Proxy

Close the **Enable VADP Proxy** view by clicking the **Enable** button at the bottom.

Repeat this step for the remaining two VADP proxies. After all three VADP proxies are enabled the Version and Status information is shown in the VADP Proxy view, as shown in Figure 3-18.

![VADP Proxy](image)

**Figure 3-18** VADP proxy view after all proxies are enabled

**Configure VADP Proxy Settings**

After we have enabled all VADP proxies, we need to adjust their configuration according to the output of the Sizing tool and the recommendations from the IBM Spectrum Protect Plus Blueprints:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints
The configuration menu of the VADP proxy, shown in Figure 3-19, is entered by clicking the three bullets in the right corner of the VADP Proxy view (Figure 3-18 on page 58) and selecting **Set Options**.

![Set VADP Proxy Options](image)

*Figure 3-19  Set VADP Proxy Options*

In our example shown in Figure 3-19, we adjusted the following options:

- **Site**: DC1 (the site for this VADP Proxy)
- **User**: serveradmin
- **Transport Modes**: We disabled SAN transport as it is a mode which could not be used on a virtual VADP proxy. After all initial full backups are done, we consider to disable HotAdd as well.
- **Softcap task limit**: We set it to 4 as recommended in the Blueprints for a smaller virtual VADP Proxy

We kept NBDSSL Compression on **disabled**, because we use a 10 Gb Network and the other settings remain unchanged.

Repeat this configuration task on the remaining two VADP proxies.
Register vSnap Backup Storage server
As the next step, you need to register your vSnap as Disk Storage using the IBM Spectrum Protect Plus GUI.

In the IBM Spectrum Protect Plus GUI select System configuration → Backup Storage → Disk and click Add Disk Storage, as shown in Figure 3-20.

Enter the hostname of the vSnap Backup Storage server, select the Site and choose the existing userid vsnapadmin to add the disk storage. Click Save to finish this task, as shown in Figure 3-21.

Repeat this step for the remaining two vSnap servers.
**vSnap Pool initialization**

After a vSnap server is deployed as a virtual appliance and added to IBM Spectrum Protect Plus, a pool needs to be configured. In the next step, the vSnap pool is initialized.

We use the simple initialization available in the IBM Spectrum Protect Plus GUI. Go to **System Configuration** → **Backup Storage** → **Disk** in the GUI and click **Actions** for your vSnap server. Select either **Initialize** or **Initialize With Encryption** from the pull-down menu, as shown in Figure 3-22. Regarding encryption, see 2.3.3, “Encryption” on page 24.

![Figure 3-22  vSnap server initialization in the Spectrum Protect Plus GUI](image1)

After the simple initialization process is completed, the **Status/Capacity** column shows a utilization bar for your vSnap server, as shown in Figure 3-23.

![Figure 3-23  vSnap server view with all server initialized](image2)
vSnap Backup Storage server Configuration

As a next step, we adjust the configuration of the vSnap server. To enter the configuration click the icon in front of the vSnap server hostname. The Manage Backup Storage window opens, as shown in Figure 3-24.

In the Manage Backup Storage window the following sections are listed for configuring the details of the vSnap server:

- Storage Options:
  - By default compression is enabled and deduplication is disabled. Enable deduplication if you have planned for from a CPU and memory perspective. Both options can be turned on and off at a later point in time as well.
  - If encryption was enabled during initialization it is shown here. It is a one-time decision and cannot be turned on later neither turn off.
  - The number of concurrent backup streams is set to unlimited. Other options is to pause the backup stream or to limit it to a configurable number of streams.
Add New Disks to Backup Storage

The chapter *Adding virtual disks* in the IBM Knowledge Center for IBM Spectrum Protect Plus describes how you could add more virtual disk (vDisks) to the vSnap servers:


Configure Storage Partners

The configuration of a Storage Partner is required to replicate backup data between two vSnap server. This configuration is discussed in 9.3, “Replication of backup data - Details” on page 157.

In the right upper corner a button **Download Logs** is present to initiate a vSnap server log file download.

### 3.3.5 Add a SLA for IBM Spectrum Protect Plus catalog backup

To be able to recover the IBM Spectrum Protect Plus environment in case of a failure or an disaster it is essential to secure the catalog by a regular backup to a different location.

In the IBM Spectrum Protect Plus GUI, select **Manage Protection → Policy Overview** and click **Add SLA Policy**. Name the new SLA policy: **SPP-DB-Backup**.

We recommend to set the following settings:

- Retention time 5 days
- Frequency to 12 hours to run it twice a day
- Start time to 6:00 which causes that a schedule is started at 6am and 6pm.
- Target site is DC1

To protect the catalog backup we configure replication to another vSnap server by using the site DC2, as shown in Figure 3-25 on page 64 with the following settings:

- Frequency to 12 hours to run it twice a day
- Start time to 6:30 which causes that a schedule is started at 6:30am and 6:30pm
- Target Site is DC2
- Same retention is used as on source (5 days)

**Note:** Replication between two vSnap servers requires a two-step configuration, one step is the SLA configuration, which is done and a second step is to set the relationship between both vSnap servers. 9.3, “Replication of backup data - Details” on page 157 explains all the necessary steps to set up replication.
The section **Additional Protection** is kept cleared. Click **Save** to create the SLA policy.

**Assign a SLA Policy for the Catalog Backup**

To assign the SLA policy **SPP-DB-Backup** for the IBM Spectrum Protect Plus Catalogs, select **Manage Protection → IBM Spectrum Protect Plus → Backup** and select the **SPP-DB-Backup** in the SLA Policy section as shown in Figure 3-26 on page 65 and click **Save**.
3.3.6 Backing up the vSnap server System Configuration

A vSnap server consists of two sets of data:

- The vSnap pool (or storage pool) which is the logical organization of disks into a pool of storage which is consumed by the vSnap server component.
- Configuration and metadata information which resides in the /etc/vsnap directory of the vSnap server.

You can back up the configuration and metadata information for use cases where the vSnap pool data is intact and valid but the configuration or metadata information is lost or not available. This can occur in these situations:

- The vSnap server compute environment is lost but the storage is not. An example is a vSnap server that is running as a virtual machine and the storage backing the vSnap pool is on a pRDM disk. In this case the vSnap server virtual machine is lost but the data on the pRDM disk is still valid.
- The vSnap server compute environment needs to be changed but the storage does not. An example is a vSnap server that is running in a virtual machine and the storage backing the vSnap pool is on a pRDM disk. In this case the vSnap server needs to be rebuilt or recreated on a new virtual machine but the data on the pRDM disk is still valid.

The backup procedure is based on the `vsnap system config backup` command, which creates a compressed TAR file. The resulting file can then be securely copied to a central location, such as the IBM Spectrum Protect Plus server. To back up the vSnap system configuration, issue the command shown in Example 3-7.

**Example 3-7 Command to create a vsnap config file backup**

```bash
vsnap system config backup --outfile backup.tgz
```

For reliability and convenience, it is suggested to automate the backup of each vSnap server’s config files and keep a set of historical backups on a centralized location, such as the IBM Spectrum Protect Plus server itself. Therefore, we demonstrate how to achieve this with some simple steps and a script that is creating backups and offloading the backup file to the SPP server.
Perform the following steps on the IBM Spectrum Protect Plus server (Example 3-8):

1. At the Linux command line, create a user vsnapadmin if it does not already exist.
2. Create a directory structure that stores the backup files of all vSnaps.
3. Change permission of the new directory structure, and set the group and ownership to the vsnapadmin user.

   **Example 3-8  Commands to execute on the SPP Server**
   ```
   sudo su
   vsnap user create --username vsnapadmin --password pass4VsnapAdmin
   mkdir /var/opt/spp/
   mkdir /var/opt/spp/backup
   chown vsnapadmin:vsnapadmin /var/opt/spp -R
   ```

Perform the following steps on each vSnap Server, as shown in Example 3-9:

1. At the Linux command line create a user vsnapadmin if it does not already exists.
2. Create a directory structure which stores the backup files of the local vSnap.
3. Change permission if the new directory structure and set the group and ownership to the vsnapadmin user.
4. Create a SSH key pair to enable password less authentication and communication between the vSnap and the Server.
5. Transfer the keys to the server.
6. Create a shell script that generates the backups and transfers the files from the vSnap to the server.
7. Create a crontab entry to schedule a repeating backup job.

   **Example 3-9  Commands to execute on the vSnap server as root user**
   ```
   sudo su
   vsnap user create --username vsnapadmin --password pass4VsnapAdmin
   mkdir /var/opt/spp/
   mkdir /var/opt/spp/backup
   chown vsnapadmin:vsnapadmin /var/opt/spp -R
   exit
   ```

Log in to the vSnap server as vsnapadmin user and create the SSH keys, as shown in Example 3-10. The key pair is stored under the user’s home directory.

   **Example 3-10  Create ssh keys as user vsnapadmin**
   ```
   ssh-keygen
   ```

   Generating public/private rsa key pair.
   Enter file in which to save the key (/home/vsnapadmin/.ssh/id_rsa):
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in /home/vsnapadmin/.ssh/id_rsa.
   Your public key has been saved in /home/vsnapadmin/.ssh/id_rsa.pub.
   The key fingerprint is: SHA256:mY4hr6ceO9XGegAxEcYjke7ko8xR0Xvdhm/AJNY35Cg vsnapadmin0t4-spp-vsnap
   The key's randomart image is:
   +-----[RSA 2048]-----+
   |
   | + + + + + + + + + |
   | + + + + + + + + + |
   | + + + + + + + + + |
   | + + + + + + + + + |
   | + + + + + + + + + |
   +-----[SHA256]-----+
Now transfer the public key of the `vsnapadmin` user to the SPP server and test the connectivity by querying the server's hostname. See Example 3-11, Example 3-12, and Example 3-13.

**Example 3-11  The ssh-copy-id command**

```
Now try logging into the machine, with: "ssh 'vsnapadmin@t4-spp-server'' and check to make sure that only the key(s) you wanted were added.
```

**Example 3-12  Create the sample backup script /home/vsnapadmin/vsnap_backup.sh**

```
#!/bin/bash

keepFilesCnt=5
bakFileName="/var/opt/spp/backup/${HOSTNAME}_backup.$(date +%Y%m%d-%H%M%S).tgz"

echo "creating new vsnap: $bakFileName"
vsnap system config backup --outfile $bakFileName

bakDirSrc="/var/opt/spp/backup"
bakDirTgt="/var/opt/spp/backup"
username="vsnapadmin"
sppServerName="t4-spp-server"

echo "copying backup file to remote location"
scp $bakFileName $username@$sppServerName:${bakDirTgt}

echo "up to $keepFilesCnt newest files on server: <<< $sppServerName >>> for vsnap: <<< $HOSTNAME >>>"

echo "totalBackupFiles-ssh $username@$sppServerName "$bakDirTgt"/backup | wc -l"

echo "total backups on spp server: $totalBackupFiles"

ssh $username@$sppServerName "du -h -s $bakDirTgt" | awk 'NR>cnt' | xargs rm

```

**Example 3-13  Change the script's permissions and make it executable**

```
chmod 755 /home/vsnapadmin/vsnap_backup.sh
```

The script can be run manually as user `vsnapadmin` to create additional backups and to test the functionality. Example 3-14 and Example 3-15 on page 68 show the output of a manual script execution.

**Example 3-14  Run vsnap_backup.sh manually**

```
[vsnapadmin@t4-spp-vsnap backup]$ /home/vsnapadmin/vsnap_backup.sh
```

creating new vsnap: /var/opt/spp/backup/t4-spp-vsnap_backup.20190820-093827.tgz
backup created: /var/opt/spp/backup/t4-spp-vsnap_backup.20190820-093827.tgz

copying backup file to remote location

```
t4-spp-vsnap_backup.20190820-093827.tgz 100%   14KB   9.3MB/s   00:00
```

up to 5 newest files on server: <<< t4-spp-server >>> for vsnap: <<< t4-spp-vsnap >>>
Example 3-15  Crontab entry on vSnap server to create a backup every night at 23:30 / 11:30 pm

```
crontab -e
30 23 * * * /home/vsnapadmin/vsnap_backup.sh
```

**Note:** We have disabled a file version housekeeping which deletes old files on the local vSnap backup directory or on the SPP Server. The reason for this is that the backup files have a very limited size, with just a few KB, and we leave it up to the administrator to decide whether only the most recent files or a longer history of backup files will be kept.

The script could be easily modified by adding or uncommenting the single line in Example 3-16 to remove all files but the last X files for a given vSnap server, where X is specified with the variable `keepFilesCnt`.

Example 3-16  Remove older backup files from SPP server (optional)

```
ssh $username@$sppServerName "ls -t ${bakDirTgt}/${HOSTNAME}* | awk 'NR>cnt' cnt=$keepFilesCnt | xargs rm"
```

### 3.3.7 Change and verify the schedules of the predefined jobs

After the deployment, the schedules for the predefined Inventory and Maintenance jobs are set to default values, which we recommend to change in order to satisfy best practices. The “System-defined jobs” on page 9 give some details on these jobs.

There are three schedules that need to be updated:

- Change the schedule for the maintenance job to run at 13:00.
- Change the schedule for the Storage Server Inventory to 19:00.
- Change the schedule for the Hypervisor / Application Server Inventory to 19:30 after you have added the resources described in Chapter 4, “Backup and Restore VM” on page 71 and Chapter 5, “Backup and Restore databases” on page 99.
Changing the Maintenance job schedule
Go to **Jobs and Operations**, choose **Schedule** from the available tabs, and select **Maintenance** as shown in Figure 3-27.

![Jobs and Operations](image)

*Figure 3-27  Edit Schedule for Maintenance Job*

Select to run it on a daily basis at 1 pm (13:00) and click **Save**, as shown in Figure 3-28.

![Schedule for Maintenance](image)

*Figure 3-28  Schedule for Maintenance job*

**Changing the Inventory job schedule**
Change the schedule for Storage Server **Inventory** job to start at 7pm (19:00) and to a frequency of daily the same way as described in “Changing the Maintenance job schedule” on page 69.

**Changing the Hypervisor and Application Server Inventory schedule**
Change the schedule for **Hypervisor** and **Application Server Inventory** to start at 7:30pm (19:30) and to a frequency of daily the same way as described in “Changing the Maintenance job schedule” on page 69.
In this chapter we discuss the backup, restore, and data reuse of virtual machine (VM) data. IBM Spectrum Protect Plus supports VM backups on either a VMware or Microsoft Hyper-V hypervisors infrastructure. Backups are snapshots based in a block-level incremental forever model: one base full backup is followed by many always incremental backups. Each backup is a \textit{Synthetic Full} backup which means only one restore activity must be started even if it refers to data of base and incremental backups.

Beside the virtual machine backup, the files on the VM itself can be indexed for single file restore without requiring you to restore the full VM or dedicated virtual disks first. The VM Restore Options Test Mode (Instant Access), Clone Mode (Instant Recover), and Production Mode (Instant Recover) support different VM restore scenarios along with data reuse options.

\textbf{Note:} For the latest Hypervisor (Microsoft Hyper-V and VMware) backup and restore requirements, see the \textit{IBM Spectrum Protect Plus - All Requirements Doc}: \url{https://www-01.ibm.com/support/docview.wss?uid=swg22013790}

This chapter includes the following topics:

- VM backup configuration basics
- Catalog file metadata for single file restore
- VM restore and data reuse
4.1 VM backup configuration basics

This section describes how to configure virtual machine backups. You must register the hypervisors that you want to protect in IBM Spectrum Protect Plus, and then create jobs to back up and restore the virtual machines and resources that are associated with the hypervisors.

4.1.1 Create an Identity

To access a Hypervisor, resource credentials are required. It is recommended to create and maintain them before adding a resource. See “Identities” on page 9 for information about how to create an identity for resources.

4.1.2 Add a Hypervisor Resource

To register the Hypervisors in the IBM Spectrum Protect Plus GUI, select Manage Protection → Hypervisor → <your hypervisor type>:

- For VMware, choose Manage vCenter and click Add vCenter to register a VMware vCenter server.
- For Hyper-V, choose Manage Hyper-V Server and click Add Hyper-V Server to register a Microsoft Hyper-V server.

In both cases, you need to enter the following information, such as that shown in Figure 4-1, as an example for adding a VMware vCenter server.

Figure 4-1  Add a VMware vCenter server as Hypervisor resource to IBM Spectrum Protect Plus
In the Manage vCenter window, specify:

- Hypervisor DNS name or IP address.
- A username for the hypervisor, or choose an already configured identity (Use existing user).
- A port to connect and whether a SSL connection should be used to connect to the Hypervisor.
- As an additional option, the maximum number of VMs to process concurrently per Hypervisor server could be configured. The default is 3, which is set per ESX server in a VMware vCenter environment and per Hyper-V server.

Further information about adding a Hypervisor resources is provided in the IBM Knowledge Center about protecting hypervisors in IBM Spectrum Protect Plus:


After a Hypervisor is added, a system-defined Hypervisor Inventory job is created and executed to collect all configured VMs and settings on the Hypervisor. The job runs by default once a day, and the schedule and job log could be adjusted or viewed at Jobs and Operations in the IBM Spectrum Protect Plus GUI. The last run time of the inventory job is shown in the VMware or Hyper-V Backup menu. From there, a new inventory can be started manually by clicking Run Inventory, as shown in Figure 4-2 as an example for VMware.

![Figure 4-2   VMware Backup menu with information about the inventory job](image)

### 4.1.3 Assign an SLA policy

After a Hypervisor resource has been defined in IBM Spectrum Protect Plus, assign one or more SLA policies to the VMs that should be backed up. Use the search function (and filter) to search for available resources, or click through the provided Hypervisor tree to select your VMs. Available options to filter are VMs and Templates, VMs, Datastore, Tags and Categories, or Hosts and Clusters.
In our example for VMware, shown in Figure 4-3, we have searched for `vm-win`, selected both VMs from the search result, and added them to the Bronze SLA by clicking **Select SLA Policy** and choosing **Bronze**.

![Figure 4-3 Adding VMs to a SLA](image)

After the **Save** button is clicked, a new job is created. Scroll to the **SLA Policy Status** section to check the job output, as shown in Figure 4-4 on page 75. Alternatively, switch to the **Jobs and Operations** menu to check the job output.
Section 1.3, “SLA backup policies” on page 15 discusses in more detail how to create and configure an SLA.

Excluding single virtual disks from the SLA policy for a job

After you have saved a backup job definition, you can exclude individual virtual disks (VMDK and VHDX) of a virtual machine from the assigned SLA policy.

To exclude a virtual disk (vDisk) from the SLA policy go to the same view as shown in Figure 4-3 on page 74 and search for the VM where a disk should be excluded. Click the VM to open the VMDK view and select the disk that you would like to exclude, as shown in Figure 4-5.
After you have selected the disk (in our example: Hard disk 2) click **Select SLA Policy**, clear (in our example) the **Bronze** SLA option for the disk, and click the **Save** button. The next backup for the VM will now run without backing up the **Hard disk 2** of the VM **t2-vm-win2**.

### 4.1.4 Run a backup job for an SLA

The backup of an SLA is either run at the scheduled time frame or could be started manually by selecting **Start** from the **Actions** pull-down menu shown in Figure 4-4 on page 75.

As soon as the backup is initiated you can follow the backup process by monitoring the job log by expanding the Bronze section in the same view, as shown in Figure 4-6.

![SLA Policy Status](image)

**Figure 4-6**  SLA Backup Job Log listed directly in the SLA Policy Status at the VMware Backup page

The following steps are performed as part of the backup workflow:

1. Execute the backup job (SLA Policy), either manually or scheduled
2. The vSnap server is determined which is used as target for the snapshot backup
3. A snapshot of the source VM is taken
4. New target volumes (datastores) are created on the vSnap server for the initial base backup, or an existing one is used for the incremental forever backup
5. Volumes mounted...
   - on the VADP proxy server as NFS datastores
     - If the VADP proxy runs together with the vSnap server on the same machine, no NFS mount is required and the data transfer takes place internally on the machine.
   - on the source Hyper-V hosts using iSCSI
6. The backup is performed to the mounted volumes
7. The VM snapshots are deleted
8. A snapshot of the target datastores are taken
9. The datastores are unmounted
10. The Spectrum Protect Plus catalog captures the details of the backup (source, vSnap, retention, schedule, and so on)
4.1.5 Run a backup for a single VM

There are two reasons why you would like to run a backup of a single VM instead of backing up all VMs assigned to an SLA:

- The backup of a VM has failed, and you would like to rerun the backup.
- You plan any maintenance activities for a VM and would like to have a backup first before starting the maintenance.

**Rerun a failed backup**

If you find a warning or error in the Dashboard view, or see a Warning or Failed SLA backup job under Jobs and Operations, you should analyze the log for the details of this status. In case the warning or error was driven by an issue of backing up a VM and you have fixed the problem, you can initiate a rerun of the failed VMs.

As shown in Figure 4-7 on the Job History tab in the Jobs and Operations view the vmware_Bronze job log is selected and you can click the Actions pull down menu in the right corner and select Rerun failed to initiate a backup of the failed VMs.

![Job History with job details and the rerun failed button](image)

**Note:** The existing job log is used to capture activities of the rerun. These informations are added with actual timestamps at the end of the job log.

---

**Note:** 13.4, “vSnap volumes and snapshots” on page 238 provides details about what happens at the vSnap server during a backup.
Start the SLA for a single VM (ad-hoc backup)

There are situations where you would need to run an ad-hoc backup of a single or multiple VMs. One reason could be that a maintenance activity (for example, a software update or system reconfiguration) is planned, and you require a current backup of the VMs that are part of this maintenance activity. In such a scenario, IBM Spectrum Protect Plus offers an ad-hoc backup capability.

In our example for VMware, we want to start an ad-hoc backup for \texttt{t2-vm-win2} VM, which we previously added to the \textbf{Bronze} SLA. In the \textbf{Manage Protection} $\rightarrow$ \textbf{Hypervisors} $\rightarrow$ \textbf{VMware} view, we listed all VMs which are backed up with the \textbf{Bronze} SLA by using the filter, as shown in Figure 4-8.

![Figure 4-8](image)

\textit{Figure 4-8}  List all VMs backed up with the Bronze SLA to run an ad-hoc backup for \texttt{t2-vm-win2}

Now we select the \texttt{t2-vm-win2} and click the Run button to initiate an ad-hoc backup for this particular VM. The success of this backup can be followed while scrolling to the SLA Policy Status and expanding the log view for the \textbf{Bronze} SLA.

4.1.6 Distributing VM backups to multiple vSnaps

In case you have multiple vSnap servers for one site, a distribution of the available VMs to be backed up over the available vSnap server is beneficial. IBM Spectrum Protect Plus offers two ways of doing so:

1. Create on a minimum as many SLAs for the same site as the number of vSnap servers that are available in this site. Distribute the VMs over the available SLAs afterwards. Each SLA chooses one of the available vSnap servers as a backup target. Therefore, all vSnap server are utilized and the VMs are distributed.

2. In the IBM Spectrum Protect configuration under \textbf{System Configuration} $\rightarrow$ \textbf{Global Preferences} in the Hypervisor section, you can configure how VMs are grouped.
Grouping is done within an SLA. The default grouping is by size and the default size is configured to 5120 GB. This results in a certain number of VMs from an SLA being added to a group until their source capacity exceeds a total size of 5120 GB, then a new group is created within the same SLA. Each group is using another available vSnap server. The configuration can also be changed to VM counts instead of size. Then the number of configured VMs are counted until a new group is created.

In our Example 4-1, we changed the Global Preferences setting to a VM count of two. The backup job log of the vmware_Bronze SLA policy includes the following lines, which indicate that the 4 VMs that are backed up are distributed over both available vSnap servers.

Example 4-1 The vmware_Bronze backup log showing VM distribution over the available vSnap servers

```
Selected vm(s) count: 4
Using storage volume spp_1004_2002_16cbd7eb496__group1_53_ on controller t2-spp-vsnap2 for backup
Using storage volume spp_1004_2002_16c86921d3a__group0_70_ on controller t2-spp-vsnap for backup
Backing up VM (t2-vm-lx) from remote proxy (IP: 10.0.250.28, Host name: t2-spp-vsnap2)
Backing up VM (t2-vm-win2) from remote proxy (IP: 10.0.250.27, Host name: t2-spp-vsnap)
Backing up VM (t2-vm-win) from remote proxy (IP: 10.0.250.27, Host name: t2-spp-vsnap)
Backing up VM (t1-vm-lx) from remote proxy (IP: 10.0.250.28, Host name: t2-spp-vsnap2)
```

4.1.7 Backup Options

IBM Spectrum Protect Plus offers backup options to be configured on a SLA or VM level. This section discusses both options and their settings.

**Backup Options on SLA level (backup job level)**

The Backup Options on SLA Level can be accessed by clicking the Policy Options icon from the SLA Policy Status under Manage Protection → Hypervisors → VMware or Hyper-V as shown in Figure 4-4 on page 75. A configuration screen appears where the following options could be configured:

- Specify **Pre- and Post-Scripts** which IBM Spectrum Protect Plus executes either before or after execution of the backup job. To continue running the job if the script fails, select **Continue job/task on script error**. Scripts and script servers are configured and maintained by using the System Configuration → Script pane.

- The option **Run inventory before backup** will execute a inventory job first before a backup is started.

- Use the **Exclude Resources** to exclude specific resources from the backup job by using single or multiple exclusion patterns. Resources can be excluded by using an exact match or with wildcards. Multiple filters need to be separated with a semicolon.

- To force a new full backup for a specific virtual machines or databases use the **Force Base Resources** option to create a new full backup for the specified resource with the next backup job execution. Multiple resources must be separated with a semicolon.

**Backup Options on VM level**

The backup options on VM level are accessed in the same screen as a VM is added to an SLA as shown in the previous Figure 4-3 on page 74. Search for specific VMs, or select all VMs from a specific SLA using the search filter where you would like to change the backup options. After the VMs are selected choose the Select Options button and a new window appears where the following settings could be set:

- **Skip Read-only datastores**: Skips datastores mounted as read-only
Skip temporary datastores mounted for Instant Access: Skip datastores currently mounted by an Instant Access Restore

VADP Proxy: Select the Proxy or a pool of Proxies (Site) to be used for backup

Make VM snapshot application/file system consistent and VM Snapshot retry attempt (default 2): All VSS-compliant applications such as Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL server, and the system state are quiesced

Truncate SQL logs: Truncates Microsoft SQL server logs during backup

Catalog file metadata: Not selected by default. Analyzes and stores metadata about mounted file systems. This metadata is required for Single File Restore functionality.

Exclude Files: Files which are excluded from the catalog file metadata

User: Guest Operating System user information which is required for the following operations:
- File metadata cataloging, see details in the following chapter 4.2, “Catalog file metadata for single file restore”.
- Microsoft SQL server log truncation.
- Certain restore operations such as IP address reconfiguration during restore.

### 4.2 Catalog file metadata for single file restore

IBM Spectrum Protect Plus allows for single file restore out of the VM snapshot backups. This is very helpful and efficient in case only a single file or a couple files needed to be restored instead of restoring the whole VM just to get a couple files back.

The file metadata is discovered when configured as part of the VM backup job locally on the VM, transferred to the IBM Spectrum Protect Plus, and stored there in a global catalog. This enables you to search for files and directories globally from the central IBM Spectrum Protect Plus GUI.

#### 4.2.1 Configure requirements

To allow single file restore cataloging, the file metadata must be enabled as part of the backup job. In order to allow IBM Spectrum Protect Plus to discover the file metadata some Operating System specific prerequisites must be configured and fulfilled.

A detailed requirements list is shown in the section *File indexing and restore requirements* of the IBM Spectrum Protect Plus - All Requirements Doc:

https://www.ibm.com/support/docview.wss?uid=swg22013790

In addition to the supported operating systems, file systems, software, and connectivity requirements to access to a VM, a key requirement is the Authentication and Privilege Requirements.

For Windows the credentials specified for the virtual machine must include a user with the following privileges:
- The user identity must have “Log on as a service” rights.
- The system login credential must have the permissions of the local administrator.
For Linux the credentials specified for the virtual machine must specify a user that has the following sudo privileges:

- The `sudoers` configuration must allow the user to run commands without a password.
- The `requiretty` setting must be set.

The recommended approach is to create a dedicated IBM Spectrum Protect Plus Agent user, which is used for the file metadata discovery. This user should be centrally managed and configured in IBM Spectrum Protect Plus by creating an Identity, as described in "Identities" on page 9 for details.

In a Windows environment, this Agent user can be centrally configured as a standard Domain User within Microsoft Active Directory and added via a Group Policy to the local Administrator group as shown in Figure 4-9.

![Figure 4-9](image)

By adding the Agent user to the local Administrator group the user will automatically have the "Log on as a service" right assigned.

Note: Check the Restrictions sections from the Restoring Files chapter in the IBM Knowledge Center for IBM Spectrum Protect Plus for additional information about the Windows Agent user:


In case the Linux VMs are configured with Microsoft Active Directory authentication, the same Agent user account can also be used in Linux. Otherwise, a local Agent user account with the following privileges, as shown in Example 4-2 on page 82, needs to be created.

Place the lines shown in Example 4-2 on page 82 at the end of your `sudoers` configuration file, typically `/etc/sudoers`. If your existing sudoers file is configured to import configurations from another directory (for example, `/etc/sudoers.d`), you can also place the lines in a new file in that directory.
Example 4-2  sudoers configuration for IBM Spectrum Protect Plus Agent user

t2-vm-lx:~ # useradd -m sppagent
New password:
Retype new password:
passwd: password updated successfully
t2-vm-lx:~ # vi /etc/sudoers
Defaults: sppagent !requiretty
sppagent ALL=(root) NOPASSWD:ALL

4.2.2 Configure file metadata discovery

The file metadata discovery is performed as part of the backup job and enabled as a backup option, which is described in “Backup Options on VM level” on page 79. The following example shows the configuration for the two Windows VMs added in Figure 4-3 on page 74 to the Bronze Backup Policy.

Before we configure the Backup Options, we add the IBM Spectrum Protect Plus Agent user as an Identity under Accounts → Identity to IBM Spectrum Protect Plus, as shown in Figure 4-10.

As a next step, the backup options on the VM level can be accessed in the same screen where a VM is added to an SLA, as shown in the previous Figure 4-3 on page 74. Search for the two Windows VMs or select the Bronze SLA using the search filter drop-down menu. Then, select the two VMs and click the Select Options button.
The window is expanded to configure the file metadata cataloging option (file discovery), as shown Figure 4-11.

![Figure 4-11 Enable Catalog file metadata](image)

You need to select **Catalog file metadata** to enable file metadata cataloging. In the **Exclude Files** section you could specify directories which should be excluded from the catalog process. By checking **Use existing user** you could select the previously configured IBM Spectrum Protect Plus Agent user as a cataloging user.

Otherwise, you could specify the credentials to be used in the username and password field. These credentials are then automatically added as an Identity. A third option is to select an SSH Key, which is configured in **System Configuration → Keys and Certificates** in the section **SSH Keys** by clicking the button **Add SSH Key**.

To store the configuration click the **Save** button.

Next time the **Bronze** SLA backup **vmware_Bronze** is run, the log file under **Jobs and Operations** in the tab **Job History** includes entries about performing file discovery, as shown in Figure 4-12.

![Figure 4-12 File Discovery log entries in the vmware_Bronze job log](image)

The discovered file metadata information is stored temporarily on the client and permanently on the IBM Spectrum Protect Plus server. Metadata collection starts on client after successful snapshot and there is a *.txt file created for each drive/volume. All the *.txt are zipped and sent to the server. On Windows the data is stored temporarily on c:\ProgramData\SPP\temp\output\ and on Linux in /tmp.

The metadata is deleted from the client after it’s sent to the IBM Spectrum Protect Plus server. When the .zip files reach the server repository on /data2/filecatalog/, the Lucene indexing starts and runs in the background, and the file metadata is stored as an index process in /data3/lucene. After a backup image has expired, the file index associated with that image will be deleted as well.
Test file metadata configuration
IBM Spectrum Protect Plus offers a helpful test function to verify the file metadata cataloging after configuration. If you select only a single VM to be configured, a Test button appears next to the Save button, as shown in Figure 4-13.

If you click the Test button, IBM Spectrum Protect Plus will check if all requirements are fulfilled. You can follow this process in the status window which opens. The tests are divided into three steps:

1. Virtual: Basic Hypervisor test for Hypervisor Tools and DNS configuration
2. Remote: Remote executor test for session creation and remote agent deployment
3. Operating System pre-requisites:
   - Basic Windows prerequisites for file and volume operations
   - Basic Linux prerequisites for file and volume operations

In case one or more of the tests are not successful, these errors need to be resolved first before file metadata cataloging will work. The test can be repeated as often as required to verify that all requirements are fulfilled.

4.2.3 Restore single files and directories

A restore of single files and directories is possible after the file metadata cataloging is configured and the file discovery process during the VM backup job has been performed successfully.
To search for files and directories, go to **Manage Protection → File Restore**. A new view opens and in the first part of the File Restore window a search matrix is displayed. From here you can complete the following actions:

1. Search for files
2. Select files for restore
3. Initiate the restore and
4. Monitor the restore process

You can do this as one process flow without changing any menu or view.

### 1. Search for Files

In our example we search for a file called `backup test test file.txt` on the VM `t2-vm-win2`. So we use the search pattern `*test*.txt` on the VM `t2-vm-win2` within folder `e:\*test*`, which results in two files found, as shown in Figure 4-14.

![File Restore view with File Search](image)

Besides the search pattern for file, folder names, and specific VMs, also the data range and OS type could be specified for a more granular search.

### 2. Select files for restore

From the **Search Results** shown in Figure 4-14, the results can be expanded to see the available restore points for the files and the appropriate version can be selected for restoring it, as shown in Figure 4-15 on page 86.
After the appropriate file for the restore is selected, scroll down the screen to specify the restore options. In our example shown in Figure 4-16, we restore the file to another VM called t2-vm-win into the folder c:\restore.

In addition to the settings we use in our example, the file can also be restored to the original location with the option to overwrite an existing version.
3. Initiate the restore
The restore is initiated by clicking the Restore button shown in Figure 4-16 on page 86.

4. Monitor the restore process
After the restore job is started, it can be monitored in the same view by scrolling down to the Job Sessions section and expanding the log as shown in Figure 4-17.

![Job Sessions](image)

Figure 4-17  Monitor the file restore job

4.3 VM restore and data reuse

In this chapter we explain the function of restoring virtual disks (VMDK or VHDX) or complete virtual machines (VMs) for recovery purposes or data reuse cases. Multiple VMs or virtual disks can be part of one restore activity.

IBM Spectrum Protect Plus version 10.1.4 introduces a general restore wizard that simplifies restores for virtual machines, applications, and databases. The wizard guides you through the configuration of restore types and parameters, and optionally schedules a job that performs the actual restore.

The wizard could be accessed either on the right upper corner of the Jobs and Operations view or at the same place in the Manage Protection → Hypervisors → VMware or Hyper-V view. If you open the wizard from the Hypervisor specific view, you already skipped the first step, where you need to decide for which “Backup Client” (VMware or Hyper-V) you would like to create a restore job.

4.3.1 Restore Schedule

IBM Spectrum Protect Plus allows you to create an On-Demand (ad-hoc) restore job, which will be immediately executed after the restore wizard is completed. Alternatively, you can create a Recurring restore, where you can define a schedule and name for the job.

Figure 4-18 on page 88 shows as an example the step where you can decide if you would like to perform an On-Demand (as selected in the example) or a Recurring restore job by using the pull-down menu.
Typically the primary restore source is the one that was used to store the backup initially (for example, the vSnap server from the primary site). In IBM Spectrum Protect Plus, this is the site that is specified in the SLA. As described in Chapter 9, “Additional Copies of Backup Data” on page 153, IBM Spectrum Protect Plus also offers different ways to protect backup data.

Whatever additional destination is chosen to protect the backup data, this destination is known to IBM Spectrum Protect Plus too, and can also be used as a restore source. The different restore sources can be chosen within the restore wizard as shown in the previous Figure 4-18 where - as an example - the Restore Location type Site and the Location Primary is selected using the appropriate pull down menu.

If you are restoring data from a cloud resource or repository server, select Use alternate vSnap server for the restore job to specify an alternative vSnap server, and then select a server from the Select alternate vSnap menu. When you restore data from a restore point that was offloaded or archived to a cloud resource or repository server, a vSnap server is used as a gateway to complete the operation.

By default, the vSnap server that is used to complete the restore operation is the same vSnap server that is used to complete the backup and offload operations. To reduce the load on the vSnap server, you can select an alternative vSnap server to serve as the gateway.

Based on the used restore source and restore Item, IBM Spectrum Protect Plus lists the available Restore Points (with timestamp) from which the best option for the restore scenario can be selected. In the example shown in the previous Figure 4-18, the VM Item t2-vm-win is selected with a Restore Point from Aug 21, 2019 10:09:10 PM.

Because each backup destination can have its own retention settings (dissimilar backup policies between primary backup target and additional copies), this supports different restore scenarios. For example, recovery of the latest version from a VM is taken from the primary vSnap server, whereas the restore of a VM from a version before the previous Operating System patch rollout is taken from the Cloud Offload.

**Note:** Only the schedule of the recurring restore job can be changed later, as explained in “Scheduler (Jobs and Operations)” on page 8. The content of the job is fixed. If the content needs to be changed, a new restore job must be created.
If you define a **Recurring** restore job as explained in 4.3.1, “Restore Schedule”, IBM Spectrum Protect always uses the latest backup version from the source location that you have configured for this job.

### 4.3.3 Restore Destination

Beside the default option to restore to the **Original Host or Cluster**, an **Alternate Host or Cluster** can also be chosen. In case the original ESX host is selected, this also causes the original datastore and network to be used for the restore. If you would like to choose a different datastore or a different network on the original ESX host or cluster, you need to select the **Alternate Host or Cluster** option. With the **Alternate Host or Cluster** option, you are able to change the ESX server, the datastore, and the network used by the VM.

For VMware, a third option called **ESX host if vCenter is down** is available. In other restore scenarios, actions are completed through the VMware vCenter. If vCenter is unavailable, this option restores the vCenter virtual machine or virtual machines that the vCenter is dependent on.

The backup of a VMware vCenter virtual machine is described in the IBM Knowledge Center for IBM Spectrum Protect Plus:


### 4.3.4 Restore methods

IBM Spectrum Protect Plus offers different restore methods:

- **Test mode**
- **Clone mode**
- **Production mode**
- **Instant Access for virtual disk restore**

Each of the methods are explained in the following sub-chapters.

**Test mode**

Test mode creates temporary virtual machines (VMs) for development or testing, snapshot verification, and disaster recovery verification on a scheduled, repeatable basis without affecting production environments. The temporary VMs accesses storage from a vSnap server, which is mounted as temporary datastore via NFS to the Hypervisor.

Test machines are kept running as long as needed to complete testing and verification and are then cleaned up, moved to production, or cloned. Virtual machines that are created in test mode are also given **unique names and identifiers (UUIDs)** to avoid conflicts within your production environment. A test mode restore is also called Instant Access Restore.

**Clone mode**

Clone mode creates copies of virtual machines for use cases that require permanent or long-running copies for data mining or duplication of a test environment in a fenced network. The VMs access storage from the vSnap server and start copying data to the datastore.

Virtual machines created in clone mode are also given **unique names and identifiers (UUIDs)** to avoid conflicts within your production environment. With clone mode, you must be sensitive to resource consumption because clone mode creates permanent or long-term virtual machines. A clone mode restore is also called an Instant Recover.
Production mode
Production mode enables disaster recovery of virtual machines at the local site from primary storage or a remote disaster recovery site, replacing original machine images with recovery images. They access storage from the vSnap server and start copying data to the datastore. All configurations are carried over as part of the recovery, including names and identifiers (UUIDs), and all copy data jobs associated with the virtual machine continue to run. A production mode restore is also called Instant Recover.

Instant Access for instant disk restore
If only a virtual disk (VMDK or VHDX) is selected for a restore operation, IBM Spectrum Protect Plus automatically presents the option for an Instant Disk restore job, which provides instant writable access to data and application restore points. An IBM Spectrum Protect Plus snapshot is mapped from the vSnap server to a target server where it can be accessed or copied as required.

You already have the option to decide during the restore job creation to move the virtual disk to permanent storage and clean up temporary resources from the vSnap server. This can be achieved by selecting the Make IA clone resource permanent restore option in the restore wizard. Alternatively, you can choose later on from the Jobs and Operations view in the Active Resources tab to make the disk permanent or to End Instant Disk Restore (Cleanup).

4.3.5 Restore Options

Through the restore wizard, you have three options to adjust the names of the restored virtual machines (VM):

- Rename the VMs. You can specify for each VM a individual name.
- Append a suffix to all VMs
- Prepend a prefix to all VMs

If you decide to rename the VM, this must be done for each VM that is part of the restore job, whereas if you choose to append a suffix to the name this is used automatically for each VM in the job.

In addition, you have the following options that can be selected in the restore wizard:

- Power on after recovery
- Overwrite virtual machine
- Continue with restore even if it fails (default)
- Allow to overwrite and force clean up of pending old session (default)
- Restore VM tags (default)
- Pre-Script
- Post-Script
- Continue job/task on script error
4.3.6 Restore a virtual disk

In this chapter, we go through the steps to restore a virtual disk (vDisk). In the example used, we restore Hard disk 2 from t2-vm-win2 (Windows VM) and Hard disk 1 from t2-vm-lx (Linux VM), as shown in Figure 4-19.

![Figure 4-19  Select virtual disks (vDisks) for a restore within the restore wizard](image)

We decided to use an On-Demand restore from the Primary Site (vSnap server) using different Restore Points, as shown in Figure 4-20.

![Figure 4-20  Select restore source snapshot for the virtual disk restore](image)

The restore should be mapped to the original VMs, therefore we select the Original Host or Cluster. We do not make the Instant Access (IA) clone resource permanent yet, so we use temporary resources from the vSnap server.

If you need to restore vDisks to an alternate VM, you need to select Alternate Host or Cluster, which after the host selection gives you the additional Destination Virtual Disk option to specify the VM to be used and other disk options, as shown in Figure 4-21.

![Figure 4-21  Choose an alternate VM for the virtual disk restore in the Destination Virtual Disk section](image)
Before the restore job for the vDisks is submitted, you can review your settings, as shown in Figure 4-22.

![Review the restore settings for the virtual disk restore](image)

After the restore job is submitted, you can follow the progress in the Jobs and Operations view using the Running Jobs tab. In case the mount of the vDisks to the VMs was successful, both disks are listed on the Active Resources tab under Hypervisor in the Jobs and Operations view, as shown in Figure 4-23 on page 93.
Figure 4-23  Active virtual disk resources in the Jobs and Operations view
In order to use the vDisk in Windows it must be set to **Online** as shown in Figure 4-24 using the **Computer Management** interface from Windows. This interface is accessible by right-clicking the Windows **Start** button and choosing **Computer Management**. After setting the disk to online, the disk gets a drive letter assigned and can be accessed using the Windows Explorer.

![Figure 4-24  Set virtual disk Online in the Windows Computer Management interface](image)

After the activities on the vDisk are completed we cleanup up the restore mount, as shown in Figure 4-25.

![Figure 4-25  Cleanup virtual disk restore mount](image)

### 4.3.7 Restore a VM

After showing for example how to restore virtual disks in the previous chapter, we now restore a complete VM to a previous state. In the example used, we restore the VM **t2-vm-win** to the restore point created on **17th of August** as shown in Figure 4-26 on page 95.
We use the **Alternate Host or Cluster** selection to select the same host as before, but use a different datastore as the restore destination, as shown in Figure 4-27.

For the network we select a different, fenced network but keep the IP configuration to not interfere with the original VM, as shown in Figure 4-28.
Our restore plan is to check the VM after the test restore and, if everything worked well, create a clone of the VM. In the review pane shown in Figure 4-29, you can verify all settings again before submitting the restore job.

![Figure 4-29   Review pane to verify the settings for the restore job](image)

After the restore job is submitted, you can follow the progress in the **Jobs and Operations** view using the **Running Jobs** tab. As soon as the test restore did complete mounting the restore point from the vSnap server and creating the VM, the VM is listed on the **Active Resources** tab under **Hypervisor** in the **Jobs and Operations** view.
In the vCenter User Interface (UI) we see the VM created using the fenced network and temporary storage resources from the vSnap server, as shown in Figure 4-30.

![Figure 4-30](image)

Figure 4-30   Restored VM is created using the fenced network and storage from the vSnap server

The VM can now be powered on and, after booting the Windows operating system, we log in and verify whether the VM was configured as expected. If everything is OK, we go to the Active Resources tab in the Jobs and Operations view and initiate the Clone operation for this VM, as shown in Figure 4-31. The clone operation initiates a VMware vMotion process, which moves the data from the temporary storage of the vSnap server to the final datastore specified in the restore job. While the clone operation is running, you can continue to work with the VM.

![Figure 4-31](image)

Figure 4-31   Start a clone operation if the VM should be kept

In case the restored VM is not the right version or configuration, we can choose to Cleanup the VM. This removes all configurations from the VMware vCenter, and we can restore another version of the VM if required. The advantage of the Test Mode restore is that data is not copied to access the VM. So you can easily check first if the restored VM is configured as expected before deciding to move it to production, or to create a clone from it.
Backup and Restore databases

This chapter discusses the management of databases with IBM Spectrum Protect Plus. IBM Spectrum Protect Plus supports backup, restore, and data reuse for multiple databases, such as Oracle, IBM Db2, MongoDB, Microsoft Exchange, and Microsoft SQL Server databases. While other IBM Spectrum Protect Plus features focus on virtual environments, the database and application support of IBM Spectrum Protect Plus includes databases on virtual and physical servers.

See the IBM Spectrum Protect Plus Installation and User’s Guide for a current list of supported databases and environments:
https://www.ibm.com/support/knowledgecenter/SSNQFQ

This chapter describes backup and restore of databases as well as data reuse with IBM Spectrum Protect Plus. It includes the following information:

- General database backup / restore considerations
- Setup a database backup
- Schedule a separate database log backup job
- Restore a database to the original destination or to another destination
- Reuse backup data for DevOps scenarios
- Outline backup/restore and data reuse scenarios.
- IBM Spectrum Protect Plus information specific to Oracle database

We use Oracle database examples in this chapter. The chapters about IBM Db2, MongoDB, and Microsoft SQL Server database include more examples for the handling of the particular database.

This chapter describes the following specific topics:

- Database backup configuration basics
- IBM Spectrum Protect Plus database restore and data reuse
- Oracle-specific information

Note: IBM Spectrum Protect Plus offers data reuse functionality in addition to backup and restore. You can use the database backup data to create a permanent copy (or clone) of your production database, or to temporarily establish a database copy directly from the vSnap volumes.
5.1 Database backup configuration basics

This section describes how to configure and run a database backup in IBM Spectrum Protect Plus, and how to schedule a job to regularly backup the database transaction logs.

Backup, restore, and data reuse handling functions for the supported (relational) databases are all similar in IBM Spectrum Protect Plus. Therefore, the examples in this section are valid for all supported databases to a large extent. In some cases, however, the examples and screen captures apply to a specific database. For this chapter, we chose Oracle Database.

The details in chapter 6: Backup and restore MongoDB databases, chapter 7: Backup and Restore of Db2 databases, and chapter 8: Backup and Restore of Microsoft SQL Server in this Redbooks publication provide additional information about data protection of these particular databases.

See the IBM Spectrum Protect Plus Installation and User’s Guide to learn more about the options and parameters to enter.

5.1.1 Create an Identity

An operating system user is required to register a database application server, and discover the databases that exist on this server. You can enter the user ID and the server-specific data, such as IP name or IP address. However, we advise you to create so-called Identities (user definition entries) in advance, to maintain a customized ordering scheme.

In the IBM Spectrum Protect Plus GUI, select Accounts → Identity and enter the user definition for your specific databases, as shown in Figure 5-1. If you use identical operating system users and passwords for multiple database servers, IBM Spectrum Protect Plus allows you to manage these databases on one Identity.

![Identity](image)

Figure 5-1 Create an identity for an operating system user
You end up with a list of identity entries, as shown in Figure 5-2. There are default system identities (LocalvSnapadmin, vsnapadmin or serveradmin) and users explicitly created for database backup and restore (DB administrator - OS user, Mongo DB user, and Oracle DBA).

![Figure 5-2 Identity entries](image)

### 5.1.2 Add an application server

In the IBM Spectrum Protect Plus GUI, select Manage Protection → Applications → `<your database type>`. Then click the Manage application servers and Add application server buttons. Enter the database server’s IP name or address, enter the database administration user or select an Identity that you defined before. Click the Get databases button to start a database discovery job on the server.

Figure 5-3 shows an Oracle database example. The name of the discovered database is `SPP`.

![Figure 5-3 Add an application server](image)

If you save this application server entry, IBM Spectrum Protect Plus automatically starts an inventory job. This job confirms a network connection, adds the application server to the IBM Spectrum Protect Plus database, and then catalogs the instance. Switch to the Job and Operations menu to check the job results.
5.1.3 Assign an SLA policy

After a database instance has been defined in IBM Spectrum Protect Plus, assign an SLA policy to the instance. In general, we recommend that you create dedicated SLA policies for single databases, or for groups of logically related databases.

Section 1.3, “SLA backup policies” on page 15 discusses this topic in more detail.

5.1.4 Run a backup

A complete database backup includes the data files, metadata (such as Oracle control files), and the transaction logs. While an IBM Spectrum Protect Plus database backup includes data and metafiles, transactions logs must be backed up more frequently to enable a future database rollforward to a current point in time. In addition to the backup schedule, IBM Spectrum Protect Plus allows you to automatically create a cron job that regularly starts a transaction log backup.

Click the Select options button to configure a log backup schedule, as shown in Figure 5-4.

If you configure log backup for the database, IBM Spectrum Protect Plus performs two actions:

- Mount an additional target volume for log backup to the database server.
- Schedule a cron job that will regularly start the log backup. Example 5-1 shows a sample crontab entry.

**Example 5-1 Crontab entry**

```bash
# Added by SPP
15 * * * * /opt/IBM/SPP/logbackup/SPP/3524c51a79a84693c152356ad4aed42c/logbackup.sh
```

**Note:** Note that this is an Oracle example. The IBM Spectrum Protect Plus implementation of database log backup varies for different databases.

The SLA policy that you assigned to your database defines the schedule time for the first backup. If you did not define a schedule, or you do not want to wait for the first automatic backup schedule, click the Run button or scroll down to the SLA policy that you provided for this database and select the Actions button to start the database backup.
See Figure 5-5. At this point, you also decide to perform a backup of a single database (Run button) or a backup of all applications included in the SLA policy (Actions button).

**Figure 5-5  Manually start a database backup**

Switch to the Job and Operations menu to check the job results.

### 5.2 IBM Spectrum Protect Plus database restore and data reuse

IBM Spectrum Protect Plus version 10.1.4 introduces a restore wizard that simplifies restores for virtual machines and databases. The wizard guides you through the configuration of restore types and parameters, and optionally schedules a job that performs the actual restore.

IBM Spectrum Protect Plus treats data reuse and data recovery as a restore activity. In either case, you must create a restore job. Both the Applications and the Jobs and Operations menus in IBM Spectrum Protect Plus show an appropriate button to start creating a restore job. The parameters that you select during job creation define which activity is performed.

The following list describes the parameters that control the final restore or data reuse activity:

- **Type of Restore:**
  - On-Demand Snapshot
  - On-Demand Point in Time
  - Recurring

- **Restore Method:**
  - A production restore either overwrites the original database or creates a database copy with a different database name. In the latter case you must specify a new database name and the destination paths.
  - A test restore mounts the vSnap directories with a database backup to a database server, recovers and opens the database. You can choose to rename the database.
  - An instant access restore also mounts the vSnap directories with a database backup to a database server, but does not recover or open the database.

- **Destination:**
  - Restore to the original instance
  - Restore to an alternate instance

The combination of the above selections define which action to perform:

- Restore a database and optionally overwrite an existing database
- Establish a copy of a previously backed up database (DevOps)
- Get access to the database files (data and metadata) of a previous backup and more
The following sections describe examples for these use cases. The sample database is Oracle Database 12c.

**Note:** (1) For test or instant access restores, IBM Spectrum Protect Plus creates an internal snapshot on the vSnap server to prevent any change to the database backup data. The snapshot directory is then mounted to the selected database server.

(2) If you decide to actually open the database after a restore, you can choose the point in time for a database rollforward: either a specific point-in-time or end of backup.

Before you start to create a restore job, you must first select the database and an associated backup to restore, as shown in Figure 5-6.

![Figure 5-6 Select the source for a database restore](image)

### 5.2.1 Test restore

This section describes a possible test restore use case: On every Monday morning, a development tester or application key user requires a fresh copy of a production database for testing: a DevOps scenario.

In the IBM Spectrum Protect Plus restore wizard, you can set up such a user requirement by choosing the following parameter settings:

- **Restore type** = On-demand point in time (or On-demand snapshot, depending on the available backups)
- **Restore method** = Test
- **Destination** = Original or alternate instance

First, select the database instance and an associated database backup, as shown in Figure 5-6. In addition, select a site and a location for the instance to restore. These settings depend on your specific environment, which can include a cloud or offload location, or a secondary site that you use for replication.

In our example, we chose the primary site and we chose **Recurring** to create a repeating restore job that runs on a schedule, as shown in Figure 5-7 on page 105.
For our use case, we have decided to create the new test database in an alternative destination (which means not on the original production server) and give the database a new name. Figure 5-8 and Figure 5-9 show the corresponding parameter selections.

Finally, we define the schedule: Every monday at 8:00 o'clock. Figure 5-10 shows an example. If you do not want to wait for the first test run, you can find the scheduled job in the Jobs and Operations menu of Spectrum Protect Plus. Select the Schedule tab, find the job in the list and start it manually.
IBM Spectrum Protect Plus does not reflect the new database name in the name of the mounted directory or in the datafile names, but it starts the database with the new database identifier (System ID, SID). See Example 5-2 and Example 5-3.

**Example 5-2  Database files on the mounted vSnap directory**

```
t6-vm-lx:/ # df -h | grep vsnap
10.0.250.53:/vsnap/vpool1/fs8  96G  726M  95G   1% /mnt/spp/vsnap/vpool1/fs8

t6-vm-lx:/ # ls /mnt/spp/vsnap/vpool1/fs8/SPP
arch
control01.ctl
controlfile.ctl
controlfile.txt
data_D-SPP_I-2016102274_TS-SYSAUX_FNO-3_38u4doto
data_D-SPP_I-2016102274_TS-SYSTEM_FNO-1_39u4dotv
data_D-SPP_I-2016102274_TS-UNDOTBS1_FNO-4_3au4dou7
data_D-SPP_I-2016102274_TS-USERS_FNO-7_3cu4douc
pfile.txt
redo01.log
redo02.log
tempfile_1.dbf
```

**Example 5-3  Database instance started by an IBM Spectrum Protect Plus restore job**

```
t6-vm-lx:/ # su - oracle

oracle@t6-vm-lx:~> env | grep SID
ORACLE_SID=SPP

oracle@t6-vm-lx:~> sqlplus / as sysdba

SQL*Plus: Release 12.2.0.1.0 Production on Thu Jun 27 11:43:20 2019
Copyright (c) 1982, 2016, Oracle. All rights reserved.

Connected to an idle instance.

SQL> exit
Disconnected

oracle@t6-vm-lx:~> ORACLE_SID=TQQ

oracle@t6-vm-lx:~> sqlplus / as sysdba

SQL*Plus: Release 12.2.0.1.0 Production on Thu Jun 27 11:43:35 2019
Copyright (c) 1982, 2016, Oracle. All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
```

The IBM Spectrum Protect Plus test restore job that you started stays active until you manually terminate it. In the Job and Operations menu, the job status is shown as “Resource active”. To terminate the job, select it and choose End instant disk restore.
5.2.2 Instant access

In **Instant access** restore mode, IBM Spectrum Protect Plus mounts the volume from the vSnap repository. The setup using the restore wizard is similar to the **test restore** setup that is described in “Test restore” on page 104.

In comparison to the **test restore**, an **instant access** restore job does not start a database and consequently you do not need to select a database instance as a restore target.

From the mounted file system, shown in Example 5-4, you can use the data for custom recovery, for example:

- Reload individual files such as control files, configuration files and data files.
- Rebuild a customized database copy.

**Example 5-4  A database backup mounted for instant access**

```
oracle@t6-vm-lx:/mnt/spp/vsnap/vpool1/fs5/SPP> hostname
t6-vm-lx
```

```
oracle@t6-vm-lx:/mnt/spp/vsnap/vpool1/fs5/SPP> df -h|grep vsnap
10.0.250.63:/vsnap/vpool1/fs5  96G  717M  96G   1% /mnt/spp/vsnap/vpool1/fs5
```

```
oracle@t6-vm-lx:/mnt/spp/vsnap/vpool1/fs5/SPP> ls -l
total 733166
drwxr-xr-x 2 oracle oinstall          3 Jun 21 15:57 arch
-rw-r----- 1 oracle oinstall   10698752 Jun 21 15:57 controlfile.ctl
-rw-r--r-- 1 oracle oinstall       5920 Jun 21 15:58 controlfile.txt
-rw-r----- 1 oracle oinstall 1415585792 Jun 21 15:57 data_D-SPP_I-2016102274_TS-SYSBAUX_FNO-3_38u4doto
-rw-r----- 1 oracle oinstall 870326272 Jun 21 15:57 data_D-SPP_I-2016102274_TS-SYSTEM_FNO-1_39u4dotv
-rw-r----- 1 oracle oinstall 330309632 Jun 21 15:57 data_D-SPP_I-2016102274_TS-UNDOTBS1_FNO-4_3au4dou7
-rw-r----- 1 oracle oinstall 5251072 Jun 21 15:57 data_D-SPP_I-2016102274_TS-USERS_FNO-7_3cu4douc
-rw-r--r-- 1 oracle oinstall        974 Jun 21 15:58 pfile.txt
```

As described in 5.2.1, “Test restore”, the instant access job remains active with the “Resource active” state until you terminate it manually. To terminate the job, select it and choose the action “End instant disk restore”.

5.2.3 Production restore

This section describes a common use case for a backup and restore solution: A traditional database restore that overwrites the original database and optionally rolls forward the database to a specific point in time.

In the IBM Spectrum Protect Plus restore wizard, the following parameters initiate a traditional database restore that overwrites the existing database:

- Restore type = On-Demand Point in Time
- Restore method = Production
- Destination = Original Instance

First select the database instance and an associated database backup, as shown in Figure 5-6 on page 104. In addition select a site and a location for the instance to restore. These settings depend on your specific environment, which can include a cloud or offload location, or a secondary site that you use for replication.
In our case, we chose the primary site as shown in Figure 5-11.

![Image of Source snapshot](#)

**Figure 5-11 Select a site to restore the database**

The next two selections quite simply express what we are trying to achieve: A production restore to the original instance as shown in Figure 5-12 and Figure 5-13.

![Image of Restore method](#)

**Figure 5-12 Production restore to the original database**

![Image of Set destination](#)

**Figure 5-13 Database restore to the original instance**

For a restore of a production database, the IBM Spectrum Protect Plus restore wizard assumes a database rollforward to a specific point in time that you can configure in the next menu.

You must also decide whether to overwrite an existing database, as shown in Figure 5-14 on page 109. IBM Spectrum Protect Snapshot provides an auxiliary protection against an unintended data overwrite: If the database still exists and you do not select the overwrite choice box, the restore job fails.
Carefully review the job summary that IBM Spectrum Protect Plus displays (Figure 5-15) and, if the information describes what you are trying to achieve, run the restore job.

Figure 5-15  Restore job summary
The IBM Spectrum Protect Plus restore job verifies whether a database exists or is even up and running. In this case, the **Allow database overwrite** setting is relevant, as shown in the restore job log shown in Example 5-5.

---

**Example 5-5   Restore job log**

```
[t6-vm-1x2] SPP: Another DB with the same name is already running. Proceeding because the overwrite option is enabled.
```

---

### 5.3 Oracle-specific information

This chapter describes the management of databases with IBM Spectrum Protect Plus in general. However, we had to choose a specific database for the description of use cases and chose Oracle database for the examples. While the subsequent chapters specifically address MongoDB, IBM Db2, and Microsoft SQL Server databases, we mention some important facts about IBM Spectrum Protect Plus configuration and handling for Oracle database in the following section.

#### 5.3.1 Server registration

An Oracle server must be registered in IBM Spectrum Protect Plus using an operating system user that exists on the Oracle server. This user must have both database administration permissions and `sudo` permissions to perform system operations.

When registering Oracle Real Application Cluster (RAC) nodes, register each node using its physical IP name or address.

#### 5.3.2 Oracle multi-threading

Oracle 12c introduced the concept of multi-threading. In IBM Spectrum Protect Plus, a multi-threaded database configuration requires Oracle credentials for backup processing. The discovery process in IBM Spectrum Protect Plus identifies if multi-threading processing is enabled, and asks you for credentials. Enter the credentials for multi-threaded databases at the time of registration. IBM Spectrum Protect Plus passes the credentials to the Oracle agent during backup, and the agent uses the credentials to log in to the database.

#### 5.3.3 Oracle backup information

IBM Spectrum Protect Plus writes backup information to the Oracle control files. Writing to a remote Oracle Recovery Manager (RMAN) catalog is not supported at this time.

#### 5.3.4 Oracle Block Change Tracking

IBM Spectrum Protect Plus uses Oracle Block Change Tracking to perform incremental backups. If Block Change Tracking is not enabled, IBM Spectrum Protect Plus enables it automatically during backup.
5.3.5 Compression

IBM Spectrum Protect Plus uses its own compression and deduplication mechanisms. It does not use the Oracle Advanced Compression feature (which requires an additional license).

5.3.6 Troubleshooting hint

For each job, IBM Spectrum Protect Plus records the commands that it uses to handle the database (including SQL and RMAN commands) in a command.log file. There are two options to access these log files:

- Use the Download .zip button in the Jobs and Operations menu to download the collection of logs for a specific job. The .zip file contains folders named application/<uuid> where <uuid> matches the last portion of the log dir location. Check the command.log files in these folders.
- Check the /data/log/guestdeployer/<date> subdirectories on the IBM Spectrum Protect Plus appliance, which also stores the command.log files.

See the IBM Spectrum Protect Plus Installation and User’s Guide for a more detailed list of requirements.
Backup and restore MongoDB databases

This chapter addresses the following MongoDB-specific information:

- Supported environments and prerequisites
- User authentication
- MongoDB database backup
- MongoDB restore and DevOps use cases

**Note:** While database configuration and handling is widely similar for databases in IBM Spectrum Protect Plus, some differences exist for the supported database systems. We describe that information in separate chapters.

Chapter 5. “Backup and Restore databases” on page 99 describes database backup, restore, and DevOps use cases in general, but refers specifically to an Oracle database whenever necessary. If you are interested in generic test restore or DevOps use cases, see that chapter.
6.1 IBM Spectrum Protect Plus requirements for MongoDB

This chapter describes specific IBM Spectrum Protect Plus requirements for MongoDB databases. For a current list, check the MongoDB requirements section in the IBM Spectrum Protect Plus Installation and User’s Guide. The following URL is for IBM Spectrum Protect Plus version 10.1.4:

6.1.1 Fundamental IBM Spectrum Protect Plus requirements for MongoDB

This section provides an overview of important IBM Spectrum Protect Plus requirements in MongoDB environments. See the IBM Spectrum Protect Plus Installation and User’s Guide for a complete list of up-to-date support information.

Operating system support
IBM Spectrum Protect Plus supports MongoDB environments on Linux systems, including Red Hat Enterprise Linux (RHEL), CentOS, and SUSE Linux Enterprise Server.

Logical Volume Manager
IBM Spectrum Protect Plus requires that logical volumes of MongoDB data and log paths are managed by Linux Logical Volume Manager (LVM2). LVM2 is used for creating temporary volume snapshots. The database files and the journal must be located on a single volume.

Operating system user
For the initial discovery of MongoDB databases on an IBM Spectrum Protect Plus server requires an operating system user (called the IBM Spectrum Protect Plus agent user) with the following permissions:

- Execute commands as the root user and as the MongoDB software owner user by using sudo. IBM Spectrum Protect Plus requires this privilege for tasks, such as discovering storage layouts, mounting and unmounting disks, and managing databases. Example 6-1 shows an appropriate /etc/sudoers entry for a user named mosuser.

- Read, write and execute permissions for the database directories. The MongoDB default database directory is /data/db.

Example 6-1  An entry for mosuser

<table>
<thead>
<tr>
<th>Defaults:mosuser !requiretty</th>
</tr>
</thead>
<tbody>
<tr>
<td>mosuser ALL=(ALL) NOPASSWD:ALL</td>
</tr>
</tbody>
</table>

Current restrictions
These restrictions apply to IBM Spectrum Protect Plus version 10.1.4.

MongoDB is configured as a standalone instance or replica set. Currently, IBM Spectrum Protect Plus does not support backup operations of MongoDB sharded cluster instances. A backup always includes all databases in the instance.
6.1.2 MongoDB databases without authentication

After installing the MongoDB software you can immediately start the MongoDB daemon (mongod) or service on your operating system and access a (default) database. On Linux operating systems, a default database is created on the data path /data/db. However, such a database is open to anybody in your network, or even the Internet. Therefore, we strictly recommend that you secure your MongoDB databases more carefully.

IBM Spectrum Protect Plus offers a two-stage process to access a MongoDB database. First you register the database server with an IP name or address, an operating system user, and a corresponding password. IBM Spectrum Protect Plus initiates a database discovery job on this server. If you run your MongoDB without authentication, the database registration in IBM Spectrum Protect Plus is complete at this point.

If you have additionally secured your databases on the database level, you specify further user credentials for each secured database that IBM Spectrum Protect Plus discovered.

6.1.3 “MongoDB databases with authentication enabled” on page 115 describes how to enable MongoDB authentication.

6.1.4 “Register a MongoDB server” on page 116 describes the MongoDB registration in IBM Spectrum Protect Plus.

6.1.3 MongoDB databases with authentication enabled

This section describes additional configuration steps for a MongoDB database that runs with authentication enabled.

If your MongoDB database is configured without credentials, you should secure it. There are many MongoDB databases open on the Internet, providing the opportunity for massive data breaches.

The MongoDB manuals describe the available authentication options in detail:
https://docs.mongodb.com/manual/core/authentication/index.html

MongoDB authentication requires the definition of at least one MongoDB user. If database authentication is enabled, IBM Spectrum Protect Plus must provide a user name and a password to run backup and restore activities.

For each MongoDB user that you plan to use for backup and restore with IBM Spectrum Protect Plus, specify MongoDB access roles by using the `db.grantRolesToUser()` command, such as that shown in Example 6-2.

**Example 6-2  Grant permissions to an existing MongoDB user**

```
> use admin
switched to db admin

> db.grantRolesToUser("mdbuser",
[ { role: "hostManager", db: "admin" },
  { role: "clusterMonitor", db: "admin" } ] )

> db.grantRolesToUser("mdbuser",
[ { role: "clusterManager", db: "admin" } ] )
```
The MongoDB `hostManager` and `clusterMonitor` roles provide access to MongoDB commands that IBM Spectrum Protect Plus requires to monitor, read the state of, and handle the databases including:

- `getCmdLineOpts`
- `serverVersion`
- `replSetGetConfig`
- `replSetGetStatus`
- `shutdown`

The additional role `clusterManager` is required only for running test restore operations of replica sets.

If you decide to create a new or dedicated user for backup and restore purposes, you can use the `db.createUser()` command as shown in Example 6-3. According to the MongoDB manuals the `ClusterAdmin` role includes the `clusterManager`, `clusterMonitor`, and `hostManager` roles.

**Example 6-3  Create a MongoDB user with the permissions required by IBM Spectrum Protect Plus**

```bash
> show dbs
admin   0.000GB
config  0.000GB
local   0.000GB
> use admin
switched to db admin
> db.createUser(
   {
      user: "mdbuser",
      pwd: "mypasswd",
      roles: [ "readWrite", "dbAdmin","clusterAdmin" ]
   }
)
```

Use the `db.getUsers()` command to display existing users and their permissions.

**Note:** Enhanced database administration permissions are required to create users and grant roles. The above mentioned roles required for backup and restore with Spectrum Protect Plus are not sufficient.

For MongoDB authentication to take effect, restart the MongoDB daemon (mongod) with the "--auth" option. Example 6-4 shows how to start the daemon on a Linux command line.

**Example 6-4  Starting mongod on Linux**

```
mongod --bind_ip_all --auth &
```

### 6.1.4 Register a MongoDB server

This section describes the tasks required to register a MongoDB server.

**Create identities**

Based on your decision to run your MongoDB database with or without authentication, one or two user definitions are required: an operating system user and optionally a MongoDB user. You can specify the users in the **Add application server** menu, but we recommend explicitly
creating a so-called Identity with a customized name first. Figure 6-1 and Figure 6-2 show Identities for an operating system and a MongoDB user. The two user names can be identical.

Add an application server
In the IBM Spectrum Protect Plus GUI select Applications → MongoDB, click the Manage application servers button, and finally click Add application servers to register the database server. Enter the database server IP name or address and select an existing identity. Alternatively, enter a user name and a password.

If you want to start a database discovery job on the server, click the Get Instances button. If IBM Spectrum Protect Plus discovers databases, it shows the connection data for these databases: IP name or address, and IP port.

**Important:** If you run your MongoDB database without authentication, the registration procedure is complete at this point. However, you should secure your database. If your database is secured, you must specify additional user credentials to access the database. The IBM Spectrum Protect Plus GUI provides a Set Credential button for the discovered databases. See Figure 6-3 on page 118.

Refer to section 6.1.3, which describes the handling of MongoDB databases with authentication.
6.2 MongoDB backup and restore with Spectrum Protect Plus

In this chapter we describe MongoDB database backup and restore. The sample restore in this chapter is a restore to the original destination.

For details about the configuration of other use cases refer to 5.2 “IBM Spectrum Protect Plus database restore and data reuse” on page 103 of this publication.

6.2.1 MongoDB backup

This section describes the tasks required to register back up a MongoDB server.

Assign an SLA policy

After the MongoDB instance has been defined in IBM Spectrum Protect Plus, assign an SLA policy to the instance. In general, we recommend creating dedicated SLA policies for single databases or groups of logically related databases.

Section 1.3 “SLA backup policies” on page 15 discusses this topic in more detail.

Start the database backup

The SLA policy that you assigned to your database (see Figure 6-4 on page 119) defines the schedule time for the first backup. If you did not define a schedule or do not want to wait for the first automatic backup schedule, click the Run button or scroll down to the SLA policy that you provided for this database and select the Actions button to start the database backup.

At this point you also decide whether to perform a backup of a single database (Run button) or a backup of all applications included in the SLA policy (Actions button).
Chapter 6. Backup and restore MongoDB databases

Figure 6-4  MongoDB instance discovered by IBM Spectrum Protect Plus with an SLA policy assigned

Either wait until a backup is automatically scheduled or scroll down to the SLA policy section on the screen and select Actions → Start to manually initiate a backup. This is IBM Spectrum Protect Plus standard handling, and not specific to MongoDB environments.

Figure 6-5  Manually start a database backup

IBM Spectrum Protect Plus mounts a vSnap directory to the database server in order to copy the backup data. See Example 6-5.

Switch to the Jobs and Operations menu to display and the job protocol and optionally download the job logs and command files.

Example 6-5  A vSnap directory mounted on the database server

```
t6-vm-lx:~ # df -h
Filesystem                       Size  Used  Avail Use% Mounted on
/dev/sda2                        40G   14G   26G   35% /
devtmpfs                        1.9G  8.0K  1.9G   1% /dev
...                               
/dev/mapper/mongovg-mongolv     15G  410M  14G   3% /data
10.0.250.48:/vsnap/vpool1/fs11   49G  128K  49G    1% /mnt/spp/vsnap/vpool1/fs11
```
6.2.2 MongoDB restore

IBM Spectrum Protect Plus offers several restore methods for databases: Production restore, test restore, and instant access. You can select between restore to the original or an alternate destination with or without overwriting an existing database. These features are available for all supported databases.

In this chapter, we demonstrate a MongoDB database restore to the original destination.

For details about the configuration of other use cases, refer to 5.2 “IBM Spectrum Protect Plus database restore and data reuse” on page 103 of this publication.

**Restore of a MongoDB database to the original destination**

In the IBM Spectrum Protect Plus restore wizard, the following parameters initiate a traditional database restore that overwrites the existing database:

- **Restore type = On-Demand Snapshot or Point in Time**
- **Restore method = Production**
- **Destination = Original Instance**

First select the database instance and an associated database backup, as shown in Figure 6-6. In addition, select a site and a location for the instance to restore. These settings depend on your specific environment, which can include a cloud or offload location, or a secondary site that you use for replication. In our case, we choose the primary site, as shown in Figure 6-7 on page 121.

![Figure 6-6](image-url) "Select the source for a database restore"
Chapter 6. Backup and restore MongoDB databases

Figure 6-7  Select a site from which to restore the database

The next two selections simply express what we are trying to achieve: A production restore to the original instance, as shown in figures Figure 6-8 and Figure 6-9.

Figure 6-8  Select the restore method

Figure 6-9  Select the restore destination

For an on-demand snapshot restore of a production database, the IBM Spectrum Protect Plus restore wizard assumes a subsequent database rollforward to the end of logs included in the backup. See Figure 6-10 on page 122.

You must also decide about overwriting an existing database. IBM Spectrum Protect Snapshot provides an auxiliary protection against an unintended data overwrite: If the database still exists and you do not select the overwrite choice box, the restore job fails.
In IBM Spectrum Protect Plus, an on-demand snapshot restore is not scheduled. Spectrum Protect Plus only runs it once as shown in Example 6-11.

Carefully check the job summary that IBM Spectrum Protect Plus displays and, if the information describes what you trying to achieve, run the restore job.
Finally, switch to the **Job and Operations** menu to check the job results. See Figure 6-12.
Backup and Restore of Db2 databases

This chapter describes the management of Db2 databases with IBM Spectrum Protect Plus. Since IBM Spectrum Protect Plus version 10.1.2, the backup, restore, and recovery of single partitioned Db2 databases are supported. With IBM Spectrum Protect Plus V10.1.4, the multi partitioned Db2 databases are also supported.

This chapter contains the following topics:

- IBM Spectrum Protect Plus Db2 features
- Prerequisites for Db2 databases.
- Protecting Db2 database
- Restore Db2 databases
7.1 IBM Spectrum Protect Plus Db2 features

IBM Spectrum Protect Plus supports the following features with Db2 databases:

- Backup, restore, and recovery of single and multi partitioned Db2 databases.
- Automatic discovery of existing Db2 installations on registered machines in IBM Spectrum Protect Plus.
- IBM Spectrum Protect Plus is performing software snapshot-based online backups using LVM2 or journaled file system (JFS2) and the Db2 Advanced Copy Services (ACS) interface.
- IBM Spectrum Protect Plus is using a custom incremental-copying algorithm for data movement from snapshot to vSnap repository. This algorithm is very effective for incremental forever backups.
- There are multiple restore methods available. Production Restore (database is restored by actually copying data), Test Restore (database is restored in-place w/o actual data movement) and Instant Access (IBM Spectrum Protect Plus only mounts the backup volume).
- IBM Spectrum Protect Plus also supports continuous Db2 archive log backup including log truncation. This feature can be used optionally for a backup.
- For Db2, various recovery (transaction rollforward) modes are available in IBM Spectrum Protect Plus, which includes point-in-time recovery using the archive logs.

7.2 Prerequisites for Db2 databases

The supported operating systems for IBM Spectrum Protect Plus with Db2 are:

- On PowerPC: IBM AIX® 7.1, 7.2, and later fixpack and modification levels (64-bit kernel)
- On Linux x86_x64: Red Hat Enterprise Linux 6.8, 7, 11.0 SP4, and 12.0 SP1; SUSE Linux Enterprise Server 11.0 SP4 and 12.0 SP1 and later maintenance and modification levels
- On Linux on Power Systems (little endian): Red Hat Enterprise Linux 7.1, SUSE Linux Enterprise Server 12.0 SP1 and later maintenance and modification levels.

The following IBM Db2 database versions were supported at the time of writing:


To manage Db2 databases with IBM Spectrum Protect Plus the following prerequisites have to be fulfilled:

- Define a dedicated IBM Spectrum Protect Plus agent user, for example `sppagent`, on every Db2 server with the required privileges for sudo, as shown in Example 7-1.

```
Example 7-1   A sudoers file with sppagent user

Defaults:sppagent !requiretty
sppagent ALL=(ALL)
NOPASSWD:ALL
```

- Db2 archive logging is activated and Db2 is in recoverable mode, which requires that at least LOGRETAINT is enabled.
Logical volumes holding IBM Db2 table spaces (data and temporary table spaces), the local database directory, and IBM Db2 log files are managed by Logical Volume Management system (LVM2) on Linux and by the Journaled File System (JFS2) on AIX respectively. LVM2 on Linux and JFS2 on AIX are used for creating temporary volume snapshots. Ensure that there is at least 10% free capacity for logical volume snapshots.

Each Db2 host has to be registered in IBM Spectrum Protect Plus. In a Db2 DPF environment with multiple hosts, every Db2 host has to be registered in IBM Spectrum Protect Plus.

In this IBM Redbooks publication, the Db2 database example consists of a multi partitioned Db2 DPF database version 10.5 that is running on two Red Hat Enterprise Linux Server hosts, as shown in Figure 7-1. IBM uses the abbreviation DPF for the Database Partitioning Feature of the Db2 product.

![Figure 7-1  Db2 DPF environment](image)

In our example, the Db2 partitions 0,1,2, and 3 are spread over the two servers kansasprod1 and floridaprod1, as shown in the db2nodes.cfg file in Example 7-2.

```
bash-4.1$ cat sqllib/db2nodes.cfg
0  kansasprod1 0
1  kansasprod1 1
2  floridaprod1 0
3  floridaprod1 1
```

To be able to manage the Db2 DPF database with IBM Spectrum Protect Plus the parallel backup mode, as shown in Figure 7-2 has to be enabled. To run parallel backup processing of partitions in your Db2 environment, ensure that one of the following prerequisites is met:

- The Db2 registry variable DB2_PARALLEL_ACS is set to YES, for example: `db2set DB2_PARALLEL_ACS=YES`
- In earlier versions of Db2, the backup mode is determined by the Db2 registry variable DB2_WORKLOAD. To enable parallel backup mode, run the Db2 command `db2set Db2_WORKLOAD=SAP`. Check with the Db2 command `db2set -all Db2_WORKLOAD`. 

**Note:** Db2 serial backup mode is not supported with IBM Spectrum Protect Plus due to the fact that logs included in the backup can be inconsistent across partitions.

**Db2 ACS processes each partition individually but in parallel**

![Diagram showing parallel backup mode with Db2 Advanced Copy Services (ACS)]

IBM Spectrum Protect Plus triggers the Db2 agent once per host, and if there is more than one partition on the host, Db2 will trigger ACS for each partition individually. There is also a dedicated protocol file per partition that is later stored on the vSnap volume. The Db2 agent can handle the multiple invocations of its ACS scripted part through Db2.

In parallel backup mode, which is the default mode for an SAP Db2 database, all partitions are suspended before Db2 issues snapshot requests. The requests are then performed in parallel on all partitions, as shown in Figure 7-2. IBM Spectrum Protect Plus runs the Db2 backup command on the Db2 catalog partition. The main Db2 ACS processes are:

1. **prepare** phase: The write operations of the database are suspended; that is, WRITE SUSPEND is set automatically on the database. Db2 prepares the file systems, checks space requirements in the storage system and does other things to keep the database consistent.

2. **snapshot** phase: Db2 instructs the Db2 agent to perform a software snapshot on each partition in parallel. The snapshot request is done by taking software snapshots of the corresponding volumes.

3. **verify** phase: Db2 checks if the snapshot was taken successfully. If the snapshot is correct, the data is moved to the vSnap server by the Db2 agent.

For IBM Spectrum Protect Plus, the Db2 archive logging has to be enabled and Db2 must be in recoverable mode. If log backup is enabled in IBM Spectrum Protect Plus, one of the Db2 parameters, LOGARCHMETH1 or LOGARCHMETH2, will be updated with the path of the
vSnap pool for the log files, as shown in Example 7-3. Therefore, it's important that one of the
LOGARCHMETH parameters has the value OFF and can be used for a vSnap log volume
assignment.

Example 7-3 Log backup enabled in IBM Spectrum Protect Plus

```
db2host$ db2 get db cfg | grep -i LOGARCHMETH1
First log archive method (LOGARCHMETH1) = DISK:/mnt/spp/vsnap/vpool1/fs2/
Archive compression for logarchmeth1 (LOGARCHCOMPR1) = OFF
Options for logarchmeth1 (LOGARCHOPT1) =
```

Note: To successfully enable Db2 log backup in Spectrum Protect Plus, the Db2 agent
expects (and verifies) that all partitions have unique settings for logarchmeth1 and
logarchmeth2.

Refer to the Spectrum Protect Plus- All Requirements document for further details and
updates of the Db2 database prerequisites at the following link:
https://www-01.ibm.com/support/docview.wss?uid=swg22013790

7.3 Protecting Db2 databases

To protect Db2 with IBM Spectrum Protect Plus, the database servers have to be registered
so that IBM Spectrum Protect Plus can discover the Db2 databases. To start the backup, the
Db2 database always has to be assigned to an SLA policy.

7.3.1 Registering the Db2 database server

Before IBM Spectrum Protect Plus can manage the Db2 database, the Db2 servers have to
be registered in IBM Spectrum Protect Plus. To register a Db2 database server, complete the
following steps:

1. In the navigation pane, click Manage Protection → Application → Db2.
2. Click Manage Application Servers → Add Application Server.
3. Enter the required login credentials for the Db2 server, as shown in Figure 7-3.

**Note:** Pre-define the sppagent username as an Identity in Accounts → Identity → Add Identity before you enter the login credentials of the db2 server. Otherwise, IBM Spectrum Protect Plus will append the ip-address or FQDN to the sppagent username to make it a dedicated user. Especially if you have to change the sppagent password, it makes it easier for the IBM Spectrum Protect Plus admin when the sppagent user can be reused for multiple Db2 servers.

![Manage application servers](image)

**Figure 7-3   Add Db2 application server pane**

**Test connection to a Db2 server**

The IBM Spectrum Protect Plus test function verifies communication with the Db2 host and tests Domain Name System (DNS) settings between IBM Spectrum Protect Plus and the host. It also tests that certain services are enabled, and that the specified user has sudo privileges. To start the test, select the host and click Actions → Test. A popup window displays, as shown in Figure 7-4 on page 131.
7.3.2 Backup Db2 data

Before starting a backup of Db2, the Db2 database has to be assigned to one or more SLA policies. There are four predefined policies (Demo, Gold, Silver, and Bronze) available for selection. You can use these policies or specify new policies that meet specific requirements. How to define an SLA policy is described in the chapter “SLA backup policies” on page 15.

Defining a Db2 backup job

Assign the selected Db2 database to a SLA policy to create a backup job. Db2 backups run in a “Base-Once-Incremental-Forever” scheme. During the initial base (full) backup, IBM Spectrum Protect Plus creates a new vSnap volume and mounts it to the Db2 server using NFS.
After assigning the Db2 database to an SLA policy, as shown in Figure 7-5, you can optionally click the Select Options button, to enable Log Backup, as shown in Figure 7-6 on page 133. With log backup enabled, IBM Spectrum Protect Plus will automatically create a log backup volume and mount it to the application server.

![Figure 7-5 Assign a SLA policy to the database](image)

**Enable Log backup**

Archived logs for databases contain committed transaction data. This transaction data can be used to run a rollforward data recovery when you are running a restore operation. Using archive log backups enhances the recovery point objective for your data.

In the Db2 Backup window, select the Db2 database and click Select Options → Enable Log Backup → Save, as shown in Figure 7-6 on page 133 to allow rollforward recovery when you set up a backup job or SLA policy. When selected for the first time, you must run a backup job for the SLA policy to activate log archiving to Spectrum Protect Plus on the database.

This backup creates a separate volume on the vSnap repository, which is mounted persistently on the Db2 application server. The backup process updates either the LOGARCHMETH1 or LOGARCHMETH2 parameters to point to that volume for log archiving purposes. The volume is kept mounted on the Db2 on the Db2 server unless the Enable Log Backup option is cleared and a new backup job is run.
Start the Db2 backup by clicking *Run* in the Db2 backup window, as shown in Figure 7-7. This starts the Db2 backup of the selected database with the shown SLA policy.

**Note:** The *Run* button is only enabled for a single database backup, and the database must have an SLA policy applied.

Log in to one of the Db2 database server via SSH and check where the backup is created. Run the command: `df -h | grep -i vsnap`, as shown in Example 7-4.

**Example 7-4**  
**vSnap volumes for data and log backup**

```
[sppagent@kansasprod1 ~]$ df -h | grep -i vsnap
9.152.168.36:/vsnap/vpool1/fs3
 97G   0  97G   0% /mnt/spp/vsnap/vpool1/fs3
```
One vSnap log volume will be used for multiple Db2 partitions. A single log archive volume on vSnap is sufficient, because the log paths are orthogonal due to the Db2 NODEXXXX element in each of the log paths. When the backup has completed, you will see the status Completed, as shown in Figure 7-8.

![Db2 backup job completed](image)

### 7.3.3 Restoring Db2 databases

With IBM Spectrum Protect Plus 10.1.4, a new restore wizard was released, as shown in Figure 7-9. The restore wizard simplifies restores for virtual machines (VMware and Hyper-V) and application data (Db2, Exchange, MongoDB, Oracle, and SQL) to ensure that you can meet all of your recovery and reuse scenarios. Start the restore wizard by clicking Jobs and Operations → Create Restore Job → Db2.

Db2 database restore with IBM Spectrum Protect Plus supports several restore methods that are explained in the following sections.

The following list describes the parameters that control the restore or data reuse activity:

- **Type of Restore:**
  - On-Demand Snapshot
  - On-Demand Point in Time
  - Recurring

- **Restore Method:**
  - A **production restore** either overwrites the original database or creates a database copy on an alternate host. **Production** is the only restore method that is available for restore operations to the original location.
  - A **test restore** mounts the vSnap directories with a database backup to an alternate database server, recovers and opens the database. You can choose to rename the database.
  - An **instant access restore** also mounts the vSnap directories with a database backup to a database server, but does not recover or open the database

- **Destination:**
  - Restore to the original instance on original host.
  - Restore to the original instance on alternate host, optionally with a new database name.
– Restore to an alternate instance on an alternate host with alternate database name. It’s required to specify a new name for the database and the original instance must exist on the target host.

**Important:** For all restore operations, Db2 must be at the same version level on the source and target hosts. In addition to that requirement, you must ensure that an instance with the same name as the instance that is being restored exists on each host. This requirement applies when the target instance has the same name, and when the names are different. In order for the restore operation to succeed, both instances must be provisioned, one with original name and the other with the new name.

The combination of the above selections define which action to perform:

- Restore a database restore and optionally overwrite an existing database
- Establish a copy of a previously backed up database (DevOps)
- Get access to the database files (data and metadata) of a previous backup

and more.

In this example scenario, a production restore is performed on a multi partitioned Db2 database version 10.5. In Figure 7-9, the first page of the restore wizard is displayed and the user has to choose **Db2**.

**Note:** When you are restoring a multi-partitioned database to an alternate location, ensure that the target instance is configured with the same partition numbers as the original instance. All of those partitions must be on a single host.

For further database examples showing a test restore or instant access, refer to “IBM Spectrum Protect Plus database restore and data reuse” on page 103.

---

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

**Figure 7-9  Spectrum Protect Plus restore wizard**

In Figure 7-9, the user has to select the Db2 database that requires a restore.
By selecting the blue plus sign a backup will be associated with the database, as shown in Figure 7-10.

![Snapshot restore](image)

**Figure 7-10  Db2 source database**

In the IBM Spectrum Protect Plus restore wizard, the following parameters must be selected to initiate a traditional database restore that overwrites the existing database:

- Restore type = On-Demand Point in Time
- Restore location type and location may vary. Here we use Site and Primary.
- Restore method = Production
- Destination = Restore to original Instance
- Restore Method = Production
- Job options = Overwrite existing database

The next step is to select the type of restore, as shown in Figure 7-11. Here *On-demand Point in Time* was selected.

![Snapshot restore](image)

**Figure 7-11  Select type of restore: On-Demand: Point in Time**
Then choose a restore location, as shown in Figure 7-12. These settings depend on your specific environment, which can include a cloud or offload location, or a secondary site that you use for replication. In our example, we chose *Site* and *Primary*, as shown in Figure 7-12.

**Figure 7-12  Select restore location type**

There are three restore methods available, as shown in Figure 7-13. In our scenario we are choosing a *Production* restore.

**Production restore**
A production restore either overwrites the original database or creates a database copy on an alternate host and optionally in an alternate database instance.
In Figure 7-14, click **Restore to original instance** to restore to the Db2 production server.

For DevOps scenarios, it’s also possible to create a restore job that runs periodically at a specific time. In our scenario, we create an on-demand restore job that runs only once. As a further restore job option, we select **Overwrite existing databases**, as shown in Figure 7-15.
Another option, shown in Figure 7-16, is to provide pre- and post-scripts that perform specific actions before and after the Db2 restore. Those scripts have to be uploaded to IBM Spectrum Protect Plus before creating the restore job.

Finally the Review page is displayed and after checking all values, the on-demand restore job can be submitted. See Figure 7-16. To start the on-demand restore job, click **Submit**.
The restore job can be monitored under **Jobs and Operations → Running Jobs**, as shown in Figure 7-18. As soon as the restore job has finished it will disappear from **Running Jobs**.

**Figure 7-18  Monitor the Db2 restore job**
Chapter 8. Backup and Restore of Microsoft SQL Server

This chapter describes the management of Microsoft SQL Server databases with IBM Spectrum Protect Plus. Microsoft SQL Server is supported as a Standalone / Failover Cluster and Always On database.

This chapter contains the following topics:

- IBM Spectrum Protect PLus SQL Server features
- Prerequisites for SQL Server databases.
- Protecting SQL Server databases
- Restore SQL Server databases
8.1 IBM Spectrum Protect Plus SQL Server features

This paragraph lists the features of IBM Spectrum Protect Plus with Microsoft SQL Server. At the time of writing, the following features, SQL Server versions, and operating systems were supported.

- Backup, restore, and recovery of Standalone / Failover Cluster and AlwaysOn Availability groups
- Incremental forever database backup
- Automatic discovery of existing SQL installations on registered machines
- Production Restore (database is restored by actually copying data):
  - To original location
  - To alternate location (i.e. alternate host)
- Test Restore (database is restored in-place without actual data movement)
- Restore to alternate instance and / or database name
- Optionally, continuous log backup including log truncation
- Recovery to end of logs (requires log backups enabled)
- Recovery to point-in-time (requires log backups enabled)

Supported SQL Server versions are:

- SQL Server 2008 R2 SP3
- SQL Server 2012
- SQL Server 2012 SP2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

Supported Operating systems are:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

8.2 Prerequisites for SQL Server databases

Before protecting the SQL Server environment with IBM Spectrum Protect Plus, check that all the prerequisites for IBM Spectrum Protect Plus are fulfilled. The main prerequisites are:

- The Windows Remote Shell (WinRM) must be enabled by running the command `winrm quickconfig`.
- A Microsoft iSCSI Initiator service must be enabled and running.
- The IBM Spectrum Protect Plus user identity must have “Log on as a service” rights on the SQL application server.
- The login credentials must have public and sysadmin permissions enabled, plus permission to access cluster resources in a SQL Server AlwaysOn environment.
To perform log backups, the SQL Server agent service user must be a local Windows administrator and must have the sysadmin permission enabled to manage SQL Server agent jobs.

The hostname of the IBM Spectrum Protect Plus appliance should be resolvable from the SQL application servers.

Please refer to the IBM Spectrum Protect Plus- All Requirements document for further details and updates of the SQL Server database prerequisites at the following link:
https://www-01.ibm.com/support/docview.wss?uid=swg22013790

### 8.3 Protecting SQL Server databases

To protect SQL Server with IBM Spectrum Protect Plus the database server has to be registered in IBM Spectrum Protect Plus so that IBM Spectrum Protect Plus can discover the SQL Server databases. To start the backup, the SQL Server database always has to be assigned to an SLA policy.

#### 8.3.1 Register the SQL Server

Before IBM Spectrum Protect Plus can manage a SQL Server database, the SQL application server has to be registered in IBM Spectrum Protect Plus. To register a SQL application server, complete the following steps:

In the navigation pane, click **Manage Protection → Application → SQL → Manage Application Servers → Add Application Server**.

Enter the required login credentials for the SQL application server, as shown in Figure 8-1. In this example, the IBM Spectrum Protect Plus admin has predefined the SQL Server Admin in **Accounts → Identity**.

![Application Properties](image)

**Figure 8-1  Register SQL application server**
Perform a configuration test of the newly assigned SQL Server in IBM Spectrum Protect Plus, as shown in Figure 8-2.

If SQL application servers are attached to a domain, a user name in the format “domain\Name” should be used. If a user is a local administrator, the format “\local administrator” should be used.

For Failover clusters and Always On availability groups, each node has to be registered by name or IP address. If fully qualified domain names are used, they must be resolvable and routeable from IBM Spectrum Protect Plus.

![Figure 8-2   SQL Server configuration test result](image)
8.3.2 Defining a SQL Server backup job

Before starting a backup of a SQL Server database, the SQL Server database has to be assigned to one or more SLA policies. There are four predefined policies (Demo, Gold, Silver, and Bronze) available for selection. You can use these policies or specify new policies that meet specific requirements. How to define an SLA policy is described in “SLA backup policies” on page 15.

Assign the selected SQL Server database to an SLA policy to create a backup job. SQL Server backups run in a “Base-Once-Incremental-Forever” scheme. During the initial base (full) backup, IBM Spectrum Protect Plus creates a new vSnap volume and mounts it to the SQL application server using iSCSI.

![Figure 8-3 Enable SQL Server log backup](image)

Optionally, the SQL Server admin can click the **Select Options** button to enable Log Backup, as shown in Figure 8-3. With log backup enabled, IBM Spectrum Protect Plus manages the log backup by using the SQL Server agent service.

To complete log backups, the SQL Server agent service user must be a local Windows administrator and must have the sysadmin permission enabled to manage SQL Server agent jobs. The agent uses that administrator account to enable and access log backup jobs. The IBM Spectrum Protect Plus SQL Server agent service user must also be the same as the SQL Server service and SQL Server agent service account for every SQL Server instance to be protected.

---

**Note:** An iSCSI route must be enabled between the SQL Server and vSnap server. For more information, see *Microsoft iSCSI Initiator Step-by-Step Guide:* [https://technet.microsoft.com/en-us/library/ee338476(v=ws.10).aspx](https://technet.microsoft.com/en-us/library/ee338476(v=ws.10).aspx)

---

Set the maximum number of data streams per database to the backup storage. This setting applies to each database in the job definition. Databases can be backed up in parallel if the value of the option is set to 1. Multiple parallel streams might improve backup speed, but high bandwidth consumption might affect overall system performance.
The SQL Server backup job status can be monitored in the SLA Policy Status pane, as shown in Figure 8-4.

![SLA Policy Status](image)

**Figure 8-4 SQL Server backup job with Status: Running**

**SQL Server backup workflow**

Some readers might be interested in the detailed workflow of a SQL Server base backup. Here are the internal steps of the backup workflow:

1. Discover the SQL Server client to get the current SQL Server instance, database information, cluster information, availability group information (for AlwaysOn), disk, and volume information.

2. Request the SQL Server iSCSI initiator information. Create an iSCSI LUN on vSnap, map the LUN to the SQL Server client iSCSI initiator.

3. **Prepare vSnap LUN for Backup**:
   a. Rescan SQL Server
   b. Identify the iSCSI LUN provisioned as backup target
   c. Clear the readonly flag
   d. Bring disk online
   e. Initialize the disk
   f. Create GPT partition table
   g. Create a primary partition
   h. Bring the partition online
   i. Quick format the volume
   j. Label the volume with "SPPB_*"
   k. Collect the volume GUID, serial number information for cataloging
   l. Mount the backup target volume to a volume mount point on "C:\ProgramData\SPP\mnt\subfolder"

4. **Check and enable USN Journaling for block level incremental capability.**

5. **Backup: VSS Snapshots**
   a. Start a VSS backup request & get VSS writer metadata
   b. Collect the source volume information of the selected SQL Server databases
   c. Add the instance and database to the application backup list. Add covering the volumes to the snapshot set.
   d. Commit snapshot set
   e. Copy the database files from the VSS shadow copy to vSnap iSCSI backup target
   f. Notify the writer of the backup status, save the backup document
   g. Report the backup status and backup metadata
6. For incremental backups use USN Journal to identify changed blocks since the last successful snapshot. Copy changed blocks from the VSS shadow copy to vSnap iSCSI backup target.
7. Merge those changes into the last snapshot in the vSnap.
8. Unmount “C:\ProgramData\SPP\mnt\subfolder” and Unmap the iSCSI LUN
9. Rescan on SQL server and ensure cleanup was successful.
10. Take vSnap snapshot of backup volume and log share volume (if applicable)
11. Catalog the backup metadata to the IBM Spectrum Protect Plus Server

8.4 Restore SQL Server databases

IBM Spectrum Protect Plus version 10.1.4 introduces a restore wizard that simplifies restores for virtual machines and databases. The wizard guides you through the configuration of restore types and parameters and optionally schedules a job that performs the actual restore.

IBM Spectrum Protect Plus treats data reuse and data recovery as a restore activity. In either case you must create a restore job. A restore job can be started from either Manage Protection → Applications → SQL → Create Restore Job or Jobs and Operations → Create Restore Job menu in IBM Spectrum Protect Plus. The parameters that you select during job creation define which activity will be performed.

The following list describes the main parameters that control the final restore or data reuse activity:

- **Type of Restore:**
  - On-Demand Snapshot
  - On-Demand Point in Time
  - Recurring

- **Restore Method:**
  - A production restore either overwrites the original database or creates a database copy with a different database name. In the latter case you must specify a new database name and the destination paths.
  - A test restore mounts the vSnap directories with a database backup to a database server, recovers and opens the database. You can chose to rename the database.
  - An instant access restore also mounts the vSnap directories with a database backup to a database server, but does not recover or open the database. An instant access restore of an Always On database is restored to the local destination instance

**Note:** The SQL Server system databases (master, msdb, model) can only be restored with Instant Access mode in IBM Spectrum Protect Plus.

- **Destination:**
  - Restore to the original instance
  - Restore to an alternate instance
The combination of the above selections define which action to perform. Here are some example use cases:

- Perform a database restore and optionally overwrite an existing database
- Establish a copy of a previously backed up database (DevOps)
- Get access to the database files (data and meta data) of a previous backup

and more.

In this example scenario, a production restore of a SQL Server standalone database is performed using SQL Server version 2012. In Figure 8-5, the database SQL_ITSO is selected for the restore. By selecting the blue plus sign, a backup is associated with the database.

For further database examples showing a test restore or instant access, see “IBM Spectrum Protect Plus database restore and data reuse” on page 103.

![Figure 8-5   Select the SQL Server backup source](image)

Other restore parameters that have to be specified are shown in Figure 8-6:

- **Restore type** = **On-Demand: Snapshot**
  - Runs a one-time restore job from a database snapshot. The restore job starts immediately upon the completion of the wizard.

- **Restore location type** = **Site**
  - The site where snapshots were backed up. The site is predefined in IBM Spectrum Protect Plus.

- **Location** = **Primary**
  - The primary site location from which to restore snapshots.

![Figure 8-6   Restore parameters](image)
In production mode, the agent first restores the files from the vSnap volume back to primary storage and then creates the new database by using the restored files. Select the radio button *Production* as shown in Figure 8-7 and click **Next**.

When selecting production mode, you can also specify a new folder for the restored database by expanding the database section and entering a new folder name.

![Figure 8-7  Select the restore method](image)  

In our setup, we perform an on-demand restore to the original instance, as shown in Figure 8-8.

![Figure 8-8  Select the restore destination](image)
Enable the restore job to overwrite the selected database. By default, this option is not enabled, as shown in Figure 8-9.

**Note:** Before you run restore operations in an SQL Server Always On environment by using the production mode with the *Overwrite existing databases* option, ensure that the database is not present on the replicas of the target availability group. As a prerequisite, manually clean up the original databases (to be overwritten) from all replicas of the target availability group.

![Image of Snapshot restore job options](image-url)

*Figure 8-9  Select restore job options*
In the Review page, check all entered restore job parameters, as shown in Figure 8-10. Click Submit to start the on-demand restore job.

**Figure 8-10   SQL Server restore summary**
Monitor the status of the on-demand restore job in Jobs and Operations, as shown in Figure 8-11.

![Jobs and Operations](image)

**Figure 8-11  Restore completed**

IBM Spectrum Protect Plus mounts the vSnap backup volume at the SQL application server and copies the backup data to the source. In our example in Figure 8-12, the vSnap backup volume is mounted as Disk1 during the restore job.

![Disk 0 and Disk 1](image)

**Figure 8-12  Mount of vSnap volume for the restore on the SQL application server**
Additional Copies of Backup Data

This chapter discusses different approaches to increase the level of protection for your valuable backup data by creating additional copies.

Such additional copies can be established in various ways:

- Replication of backup-storage data from one vSnap server to another vSnap server
- Additional copies to secondary backup storage:
  - Additional copies to Object Storage ("Offload"):
    - Incremental copy to Cloud Storage
    - Incremental copy to an IBM Spectrum Protect Container Storage Pool
  - Additional copies to Tape or Archival Storage ("Archive"):
    - Full copy to a Long-Term Cloud Storage (e.g. IBM Cloud Object Storage Archive or Amazon Glacier)
    - Full copy to an IBM Spectrum Protect Tape Storage Pool
- Backing up data to multiple vSnap servers using multiple SLAs

Important: None of the techniques discussed in this chapter is moving or migrating data from one storage tier to another. All methods described are establishing additional copies. However, different lifecycles can be applied to each copy which allows to keep “hot data” on a fast storage while placing “cold data” on a slower low cost storage.

We summarize the different options and also describe a specific scenario (“Hot” and “Cold/Archive” copies to IBM Spectrum Protect) in more detail:

- “Reasons to create additional copies of backup data”
- “Additional copies - Overview and comparison of options”
- “Replication of backup data - Details”
- “Additional Copies to Object, Tape or Archival Storage - Details”
- “Configuring Multi-Site Backup - Details”
- “Example: Creating incremental and full copies of backup data to an IBM Spectrum Protect server”
9.1 Reasons to create additional copies of backup data

In IBM Spectrum Protect Plus (SPP), vSnap servers are the primary target for backup data. A vSnap is a pool of disk storage that receives data from production systems for the purposes of data protection and reuse. The vSnap server consists of one or more disks and can be scaled up (by adding disks to increase capacity) or scaled out (by distributing the workload to multiple vSnap servers to increase overall performance).

Redundant Array of Independent Disks (RAID) technology can be used to protect vSnap servers against data loss that is caused by a hardware failure of a single disk - either by using software RAID inside the vSnap or by using HW or SW features of the underlying storage system that provides the capacity to the vSnap pool.

However, there might be reasons to create additional copies of backup data, e.g. in order to be able to recover from a disaster or to store long-term data on a lower-cost storage.

9.2 Additional copies - Overview and comparison of options

This section presents and compares various options for creating additional copies.

9.2.1 Replication of backup data

Backup data can be replicated between two vSnap servers. This includes backups of VMs, applications and SPP server catalog backups.

Replication of data between vSnap servers can be done for example for the following reasons:
- Protecting the backup data against the complete loss of a vSnap system
- Protecting the backup data against the loss of a whole data center (assuming that the replication target is located in a remote data center)
- Storing a copy of data in a remote site with a longer retention when there is not sufficient space in the primary site, e.g. replicating data from small branch offices to a large central data center

**Note:** As an option, additional copies can be created from the replication target vSnap. An example would be to replicate backup data daily from a vSnap in a small branch office to a remote vSnap in a central data center and from there create a full copy to a Cloud or to a Spectrum Protect server tape pool on a monthly basis.

9.2.2 Additional Copies to Cloud storage

Backup data that resides in a vSnap server can be copied to a Cloud storage provider. At the time of writing this paper, the following Cloud providers are supported:
- Amazon S3
- IBM Cloud Object Storage
- Microsoft Azure Blob
Data can be copied to a cloud storage provider in two ways:

- **Incremental copy to a “hot” cloud tier.** This approach allows to store backup data with longer retentions at a moderate cost and supports instant access recovery.
- **Full copy / Archive to a “cold” cloud tier.** This approach allows to store long-term data at the lowest cost and is intended to be used e.g. for monthly, quarterly or yearly full backups. The backup data is bundled in a tar file and uploaded as a single object. According to this two-step backup approach, the restore operation is a two-step process as well which does not allow for instant access recovery and is slower than the incremental copy.

### 9.2.3 Additional Copies to a Repository server

Backup data that resides in a vSnap server can be copied to a repository server. At the time of writing this paper, the only supported repository server type is IBM Spectrum Protect.

Data can be copied to an IBM Spectrum Protect server in two ways:

- **Incremental copy to a “hot” storage tier.** This approach allows to store backup data with longer retentions to an IBM Spectrum Protect container storage pool (directory container or cloud container) and supports instant access recovery.
- **Full copy / Archive to a “cold” storage tier.** This approach allows to store long-term data at lower cost into an IBM Spectrum Protect Tape storage pool. The backup data is bundled in a tar file and uploaded as a single object. In this case, the restore operation is a two-step process as well which does not allow for instant access recovery and is slower than the incremental copy.

A detailed example on how to configure IBM Spectrum Protect Plus for the creation of additional full and incremental copies to an IBM Spectrum Protect server can be found in Chapter 9.6, “Example: Creating incremental and full copies of backup data to an IBM Spectrum Protect server” on page 170.

### 9.2.4 Dual-Site Backup using multiple SLAs

All methods described earlier in this chapter have one thing in common: Backup objects that are ingested into a primary vSnap server are copied over to another location (e.g. a secondary vSnap, a Cloud or an IBM Spectrum Protect server). The additional copy belongs to the same point-in-time as the primary backup object.

By assigning a virtual machine or an application to more than one SLA it is possible to create backups of the same entity in two different locations (sites) and at different points in time as well. The key difference is the fact that the primary data is being backed up twice, which results in two independent “primary” backup versions of the same VM or application.

The advantage of creating additional copies by backing up the same entity with two different SLAs is that the Recovery Point Objective (RPO) is improved because backup points are created more often.

**Important:** Increasing the backup frequency adds more load to the hypervisor (e.g. VMware snapshots need to be created more often) or to the application (e.g. because it is set to backup mode more often). Because of network latency, additional backups to a distant site might experience slower performance and can not benefit from compression as it is being used when replicating backup data between two vSnap servers.
9.2.5 Comparing the options

Creating additional copies of backup data can be established in various ways. The choice of a particular method and type of storage, is driven by answers to the following questions or requirements:

- How fast can the copy be accessed in case of a restore request?
- Is an instant access recovery possible?
- Is the target storage appropriate for long-term archiving?
- Is the target storage physically disconnected from the production environment and protected against malicious attacks, e.g. Computer viruses (“Air-Gap”)?
- How much cost is assigned with the implementation of the secondary storage?

The following table summarizes the different options and their characteristics:

<table>
<thead>
<tr>
<th>Copy Option</th>
<th>Access to data</th>
<th>Long-term Readiness</th>
<th>Air Gap</th>
<th>Cost</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSnap Replication</td>
<td>fast</td>
<td>no</td>
<td>no</td>
<td>high</td>
<td>incremental copy to fast storage, compressed (opt.)</td>
</tr>
<tr>
<td>incremental copy to Cloud</td>
<td>medium</td>
<td>medium</td>
<td>medium</td>
<td>moderate</td>
<td>incremental copy to object storage</td>
</tr>
<tr>
<td>incremental copy to IBM Spectrum Protect</td>
<td>medium</td>
<td>medium</td>
<td>medium</td>
<td>moderate to high</td>
<td>only with SP container storage pools</td>
</tr>
<tr>
<td>full copy to Cloud (Archive)</td>
<td>slow</td>
<td>yes</td>
<td>medium</td>
<td>low</td>
<td>Cloud archive storage, no instant access recovery</td>
</tr>
<tr>
<td>full copy to IBM Spectrum Protect (Archive)</td>
<td>slow</td>
<td>yes</td>
<td>yes</td>
<td>moderate</td>
<td>Tape, no instant access recovery</td>
</tr>
<tr>
<td>Dual-Site Backup</td>
<td>fast</td>
<td>no</td>
<td>no</td>
<td>high</td>
<td>two initial full backups required</td>
</tr>
</tbody>
</table>

In the next sections we show you how to configure IBM Spectrum Protect Plus in order to create additional copies of your backup data.
9.3 Replication of backup data - Details

The backup data stored by a vSnap server can be replicated to a second vSnap server as an operational protection. This includes backups of VMs, databases, applications and IBM Spectrum Protect Plus server catalog backups. The replication target (receiving) vSnap server must belong to different site as the source (sending) vSnap server. The chapter Replication considerations in the IBM Spectrum Protect Plus Blueprints does elaborate further on the relationship and options of Sites and vSnap servers for replication:

https://ibm.biz/IBMSpectrumProtectPlusBlueprints

9.3.1 Configure vSnap Replication

To replicate data from a primary vSnap server to a secondary vSnap server both vSnap servers need to be configured at the IBM Spectrum Protect Plus server already and need to belong to different sites. In addition two configuration tasks need to be completed to enable replication between both vSnap servers:

- A replication partnership needs to be configured between both vSnap servers.
- The replication policy must be configured as part of the SLA.

vSnap replication partnership

To configure a replication partnership between two vSnap servers use the IBM Spectrum Protect Plus GUI and go to System Configuration → Backup Storage → Disk and click the Edit icon to vSnap server to enter properties page.

Figure 9-1 on page 157 shows the properties page of a vSnap server in the IBM Spectrum Protect Plus GUI. The section Configure Storage Partners does not list any partner yet.
Next click the plus sign below the **Configure Storage Partners** section and choose the partner server from the pull-down menu. Now click the **Add Partner** button to establish the partnership as shown in Figure 9-2.

![Configure Storage Partners](image1)

**Figure 9-2** Add vSnap server as storage partner in the vSnap server properties page.

After the partner is added it is listed as a storage partner with details to which site the partner vSnap server belongs to as shown in Figure 9-3 on page 158.

![Configure Storage Partners](image2)

**Figure 9-3** vSnap Partner server added

In Example 9-1 we use the vSnap CLI command `vsnap partner show` and it lists the vSnap partner server now as well.

**Example 9-1** List vSnap partner server on the Primary site vSnap

```
[serveradmin@t2-spp-vsnap ~]$ vsnap partner show
                      ID | PARTNER TYPE | MGMT ADDRESS | API PORT | SSH PORT
-------------------------------------------------------
5345ec9e347b40d5ae63b2397f64c8da | vsnap        | t2-spp-vsnap-dr | 8900     | 22
```

We run the same command in Example 9-2 on the second vSnap server for the Secondary site, which lists also the partner vSnap server.

**Example 9-2**

```
[serveradmin@t2-spp-vsnap-dr ~]$ vsnap partner show
                      ID | PARTNER TYPE | MGMT ADDRESS | API PORT | SSH PORT
-------------------------------------------------------
bc1c6c4052a744ad86bdc25625e2c516 | vsnap        | t2-spp-vsnap  | 8900     | 22
```

We have now configured a replication partnership between both vSnap servers, which could be used in both directions by a SLA.
SLA replication policy

As a next step choose the SLA which need to be configured to use replication as Operational Protection. Use the IBM Spectrum Protect Plus GUI and go to Manage Protection → Policy Overview click the Edit icon to enter the properties page of the desired SLA where replication should be added. In our example we use the Bronze SLA as shown in Figure 9-4.

![Policy Overview](image)

Figure 9-4  Bronze SLA properties page

The Replication Policy section is not enabled by default. Check the Backup Storage Replication box, adjust the Start Time as required and choose Secondary as Target Site as shown in Figure 9-4. Click the Save button to save your changes.

We have now configured replication from the Primary site to the Secondary site within the Bronze SLA. From a system perspective, data is replicated from the vSnap server t2-spp-vsnap, which belongs to the Primary site to vSnap server t2-spp-vsnap-dr, which belongs to the Secondary site. The relationship from vSnap server to site is shown also under the System Configuration → Backup Storage → Disk in the GUI as shown in Figure 9-5 on page 160.
9.3.2 Run the replication

The replication process runs as part of the backup job created for a corresponding SLA. As we have added replication to the Bronze SLA which we use to backup VMware VMs, this would be the vmware_Bronze job. You could either wait until replication starts at the configured time or start it manually by clicking on Actions drop-down menu behind the Bronze Job, selecting Start and then Replication.

9.4 Additional Copies to Object, Tape or Archival Storage - Details

As an alternative to replicating vSnap data into another vSnap, Object Storage can be used to create additional incremental copies of vSnap backup data into a “hot” storage tier.

Supported Object Storage providers are Amazon S3, IBM Cloud Storage, Microsoft Azure or IBM Spectrum Protect with container storage pools.

When vSnap data is offloaded to object storage, a full copy is created during the first offload operation. Subsequent copies are incremental and capture cumulative changes since the last offload.

Offloading snapshots to object storage is useful if you want relatively fast backup and recovery times and do not require the longer-term protection, lower cost, and security benefits that are provided by tape or cloud archive storage.

Tape or Archival Storage can be used to create additional full copies of backup data into a “cold” storage tier.

Cloud archive storage is a long-term storage method that copies data to one of the following storage services: Amazon Glacier, IBM Cloud Object Storage Archive Tier, or Microsoft Azure Archive.
Tape storage means that data is stored on physical tape media or in a virtual tape library connected to an IBM Spectrum Protect server. By storing tape volumes at a secure, offsite location that is not connected to the internet, you can help to protect your data from online threats such as malware and hackers.

Copying snapshots to tape or cloud archive storage provides extra cost and security benefits. However, because offloading to these storage types requires a full data copy, the time required to copy data increases. In addition, the recovery time can be unpredictable and the data might take longer to process before it is usable.

### 9.4.1 Prerequisites

To create additional copies of vSnap data to **object storage**, some requirements need to be fulfilled:

- A disk cache area needs to be present on the vSnap server
- Certificates from private Certificate Authority (CA) need to be trusted, if a private CA is used
- Network communication needs to be allowed between vSnap and object storage provider
- Object storage provider needs to be configured

To create additional copies of vSnap data to **tape or archival storage**, the requirements are similar to the object storage requirements - however, the vSnap disk cache area is not required for full archival operations.

#### Preparing the disk cache area

The vSnap disk cache area is used as a temporary staging area for objects that are pending upload to the object storage provider endpoint.

During restore operations, the disk cache area is used to cache downloaded objects as well as to store any temporary data that may be written into the restore volume.

The cache area must be configured in the form of an XFS file system mounted at `/opt/vsnap-data` on the vSnap server. If this mount point is not configured, offload or restore jobs will fail.

**Note:** For new virtual vSnap appliance deployments starting at version 10.1.2, a pre-configured disk cache area of 128 GB size is already present and mounted to `/opt/vsnap-data`.

For all custom vSnap server installations and virtual vSnap appliances that have been upgraded from version 10.1.1, the cache area must be configured manually.

For detailed instructions about sizing, installing or increasing the cache area, refer to the following technote: ([https://www-01.ibm.com/support/docview.wss?uid=ibm10869560](https://www-01.ibm.com/support/docview.wss?uid=ibm10869560))

Alternatively, you can review the latest version of the IBM Spectrum Protect Plus Blueprints to find information on sizing and configuring the disk cache area:

[https://ibm.biz/IBMSpectrumProtectPlusBlueprints](https://ibm.biz/IBMSpectrumProtectPlusBlueprints)
**Trusting private CA certificates**

If the cloud endpoint or repository server uses a certificate signed by a private Certificate Authority (CA), the endpoint certificate must be specified (in PEM format) when you register the cloud or repository server in the IBM Spectrum Protect Plus user interface.

In addition, the root/intermediate certificate of the private CA must be added to the system certificate store in each vSnap server using the following procedure:

1. Log in to the vSnap server console as the "serveradmin" user and upload any private CA certificates (in PEM format) to a temporary location.
2. Copy each certificate file to the system certificate store directory (`/etc/pki/ca-trust/source/anchors/`) by running the following command:
   ```
   sudo cp /tmp/private-ca-cert.pem /etc/pki/ca-trust/source/anchors/
   ```
3. To incorporate the newly added custom certificate and update the system certificate bundle, run the following command:
   ```
   $ sudo update-ca-trust
   ```

**Note:** If the cloud endpoint or repository server uses a *self-signed* certificate, the certificate must be specified while registering the cloud or repository server in the IBM Spectrum Protect Plus user interface. As this happens during the registration of the object storage provider in the SPP UI, it does not need to be prepared in advance.

If the cloud endpoint uses a *public CA-signed* certificate, no special action is needed. The vSnap server will validate the certificate by using the default system certificate store.

**Allowing network communication between vSnap and object providers**

The following ports are used for communication between vSnap servers and cloud or repository server endpoints and need to be allowed through any existing firewalls:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Allows a vSnap to communicate with Amazon S3, Microsoft Azure, or IBM Cloud Object Storage endpoints</td>
</tr>
<tr>
<td>9000</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Allows a vSnap to communicate with IBM Spectrum Protect (repository server) endpoints</td>
</tr>
</tbody>
</table>

Any firewalls or network proxies that perform SSL interception or Deep Packet inspection for traffic between vSnap servers and cloud endpoints might interfere with SSL certificate validation on vSnap servers. This interference can also cause cloud offload job failures. To prevent this interference, the vSnap servers must be exempted from SSL interception and inspection in the firewall or proxy configuration.

**Preparing object storage providers**

This section describes how to prepare object storage providers for use with IBM Spectrum Protect Plus.
**Important:** Native lifecycle management performed by the object storage provider is not supported. IBM Spectrum Protect Plus manages the lifecycle of uploaded objects automatically using an incremental-forever approach where older objects can still be used by newer snapshots. Automatic or manual expiration of objects outside of IBM Spectrum Protect Plus will lead to data corruption.

**Amazon S3 offload requirements ("hot" incremental copies)**

An Amazon S3 bucket needs to be prepared in advance. For performance reasons, the selected **Region** should be close to the geographical region where the vSnap server system is located.

**Note:** Amazon S3 supports various storage classes for storing objects into a bucket. IBM Spectrum Protect Plus “hot” incremental copies will store objects to the default storage class, which is **S3 STANDARD**.

**Amazon S3 archive requirements ("cold" full copies)**

An Amazon S3 bucket needs to be prepared in advance. For performance reasons, the selected **Region** should be close to the geographical region where the vSnap server system is located.

**Note:** IBM Spectrum Protect Plus “cold” full copies will be directly uploaded to the **S3 Glacier** storage class. Some small metadata files will be stored in the default class for the bucket. A copy of these metadata files is also placed into the Glacier tier for disaster recovery purposes.

**IBM Cloud Object Storage offload requirements ("hot" incremental copies)**

A bucket must be prepared in advance. If the bucket has a WORM policy that locks objects for a certain time period, IBM Spectrum Protect Plus automatically detects the configuration and deletes snapshots after the WORM policy removes the lock.

**IBM Cloud Object Storage archive requirements ("cold" full copies)**

A bucket must be prepared in advance. If the bucket has a WORM policy that locks objects for a certain time period, IBM Spectrum Protect Plus automatically detects the configuration and deletes snapshots after the WORM policy removes the lock.

**Note:** Object Storage in IBM Cloud supports an Archive tier for long-term data. IBM Spectrum Protect Plus creates a single lifecycle management rule on the bucket to migrate data files to the archive tier.

**Important:** On-prem IBM Cloud Object Storage systems do not support the Archive tier, so Archiving ("cold" full copies) are only supported to IBM Cloud.

**Microsoft Azure offload requirements ("hot" incremental copies)**

A container in a hot or cool storage account must be created in advance.
**Microsoft Azure archive requirements ("cold" full copies)**

A container in a hot or cool storage account must be created in advance. IBM Spectrum Protect Plus moves files between tiers on demand. Data files will be immediately moved to the archive tier and temporarily returned to the hot tier only during a restore operation. Some small metadata files will be stored in the default tier for the container. A copy of these metadata files is also placed in the archive tier for disaster recovery purposes.

**Tip:** For a very detailed description on how to create buckets in Amazon, IBM Cloud Object Storage or Microsoft Azure for use with IBM Spectrum Protect Plus, review the following IBM Technote:


**IBM Spectrum Protect server requirements**

When IBM Spectrum Protect is being used as the object storage provider for IBM Spectrum Protect Plus, you cannot prepare a bucket in advance. IBM Spectrum Protect Plus creates a uniquely named bucket for its own use on demand.

**Note:** For IBM Spectrum Protect Plus Version 10.1.3, the repository server must be an IBM Spectrum Protect server Version 8.1.7 or later. SPP 10.1.3 does not support full copies to cloud archive or tape storage.

For IBM Spectrum Protect Plus Version 10.1.4, the repository server must be an IBM Spectrum Protect server Version 8.1.8 or later.

IBM Spectrum Protect Plus needs to be registered in the IBM Spectrum Protect server as an ObjectClient. If the SPP version is 10.1.3, (which introduced the option to create additional, incremental “hot” copies to object storage using the Amazon S3 protocol) the corresponding ObjectClient in SP needs to be assigned to a policy domain that uses a default management class that points to a directory- or cloud-container storage pool.

With SPP version 10.1.4, the Archive option was introduced, which allows to store additional full copies of backup data into a Spectrum Protect Tape storage pool. In order to support the selection of different target storage types (“storage classes”) via the S3 protocol, IBM Spectrum Protect server version 8.1.8 was enhanced with a new storage pool type ("ColdDataCache") and a new policy domain type ("ObjectDomain"). Due to this, all Spectrum Protect ObjectClient nodes that store data for SPP version 10.1.4 or later need to be assigned to an ObjectDomain in Spectrum Protect.

For a detailed description on how to create a ColdDataCache storage pool in Spectrum Protect, review the following information:


For a detailed description on how to configure an ObjectDomain in Spectrum Protect, review the following information:


A detailed example on how to use Spectrum Protect in order to create additional copies of SPP vSnap data (“hot” or “cold”) can be found later in this paper in Chapter 9.6, “Example: Creating incremental and full copies of backup data to an IBM Spectrum Protect server” on page 170.
9.4.2 Configuring an object storage provider in Spectrum Protect Plus

Once the object storage providers have been prepared, they need to be registered in the IBM Spectrum Protect Plus user interface.

Since all object providers (Amazon S3, IBM Cloud Object Storage, Microsoft Azure Blob and IBM Spectrum Protect) use the Amazon S3 protocol, the process for registering them to IBM Spectrum Protect Plus is similar as well.

Adding Amazon S3 cloud storage as a backup storage provider:
The following is a summary of tasks that need to be performed to add Amazon S3 as a backup storage provider to IBM Spectrum Protect Plus:
1. Navigate to System Configuration → Backup Storage → Cloud
2. Click Add Cloud
3. Select Amazon S3 from the provider list
4. Complete all fields in the Cloud Registration pane:
   – Enter a meaningful name to identify the cloud storage
   – Select the Amazon AWS region endpoint of the cloud storage
   – Use either an existing key or specify the Key name, Access key and Secret key
5. Click Get Buckets to obtain a list of prepared buckets
6. Select which bucket to be used for offload operations (incremental copy to a “hot” tier)
7. Optional: select which bucket to be used for archive operations (to “cold” tier)
8. Click Register in order to add the provider to the cloud servers table

For a detailed description on how to add Amazon S3 as a backup storage provider, review the following information:

Adding IBM Cloud Object Storage as a backup storage provider:
The following is a summary of tasks that need to be performed to add IBM Cloud Object Storage as a backup storage provider to IBM Spectrum Protect Plus:
1. Navigate to System Configuration → Backup Storage → Cloud
2. Click Add Cloud
3. Select IBM Cloud Object Storage from the provider list
4. Complete all fields in the Cloud Registration pane:
   – Enter a meaningful name to identify the cloud storage
   – Select the endpoint of the cloud storage
   – Use either an existing key or specify the Key name, Access key and Secret key
   – Use an existing Certificate, or alternatively upload or copy and paste a new one
     (Note: for public IBM Cloud Object Storage, no certificate is required)
5. Click Get Buckets to obtain a list of prepared buckets
6. Select which bucket to be used for offload operations (incremental copy to a “hot” tier)
7. Optional: select which bucket to be used for archive operations (to “cold” tier)
8. Click Register in order to add the provider to the cloud servers table
For a detailed description on how to add IBM Cloud Object Storage as a backup storage provider, review the following information:

**Adding Microsoft Azure Cloud Storage as a backup storage provider:**
The following is a summary of tasks that need to be performed to add Microsoft Azure Cloud Storage as a backup storage provider to IBM Spectrum Protect Plus:

1. Navigate to **System Configuration → Backup Storage → Cloud**
2. Click **Add Cloud**
3. Select **Microsoft Azure Blob Storage** from the provider list
4. Complete all fields in the **Cloud Registration** pane:
   - Enter a meaningful **name** to identify the cloud storage
   - Select the **endpoint** of the cloud storage
   - Use either an existing key or specify the **Key name**, **Storage Account Name** and **Storage Account Shared Key**
5. Click **Get Buckets** to obtain a list of prepared buckets
6. Select which bucket to be used for offload operations (incremental copy to a “hot” tier)
7. Optional: select which bucket to be used for archive operations (to “cold” tier)
8. Click **Register** in order to add the provider to the cloud servers table

For a detailed description on how to add Microsoft Azure Cloud Storage as a backup storage provider, review the following information:

**Adding an IBM Spectrum Protect server as a backup storage provider:**
The following is a summary of tasks that need to be performed to add IBM Spectrum Protect as a backup storage provider to IBM Spectrum Protect Plus:

- Navigate to **System Configuration → Backup Storage → Repository Server**
- Click **Add Repository Server**
- Complete all fields in the **Register Repository Server** pane:
  - Enter a meaningful **Name** to identify the repository server
  - Enter the high-level-address (HLA) of the repository server object agent in the **Hostname** field
  - Enter the TCP port being used by the object agent (default: 9000)
  - Use either an existing key or specify the **Key name**, **Access key** and **Secret key**
  - Use an existing **Certificate**, or alternatively **upload** or **copy and paste** a new one
- Click **Register** in order to add the provider to the cloud servers table
For a detailed description on how to add IBM Spectrum Protect as a backup storage provider, review the following information:
d.html)

9.4.3 Configuring additional copies to Object storage in the SLA

IBM Spectrum Protect Plus Service Level Agreement (SLA) policies are used to define parameters for backup jobs. In order to better understand how these parameters affect the creation of additional copies to object storage, the basic structure of a SLA is summarized in the following paragraph.

A SLA is divided into two main sections:

1. **Operational Protection**: This section includes all parameters that belong to backup data which is being stored into vSnap servers:
   a. **Main Policy**: Controls Retention, Schedule and Target Site for the primary VM-, application- or a SPP-catalog-backup
   b. **Replication Policy**: Controls Retention, Schedule and Target Site for vSnap replication operations

   **Note**: The Recovery Point Objective (RPO) of a backup object is always controlled by the parameters of the Main Policy in the Operational Protection section.

2. **Additional Protection**: This section includes all parameters that belong to the creation of additional copies of data from a vSnap server into object-, archive- or tape-storage:
   a. **Cloud**: Controls Retention, Schedule, Source and Target for incremental copies to a “hot” storage tier (cloud storage or SP container storage pool)
   b. **Archive**: Controls Retention, Schedule, Source and Target for full copies to a “cold” storage tier (cloud archive storage or SP tape storage pool)

The parameters of the Additional Protection section allow you to control when and where to create additional copies and how long these copies will be retained.
The SLA parameters that control the **Source** of a copy operation are:

- **Main Policy Destination**: The source for the offload or archive operation is the target site that is defined in the **Main Policy** section.

- **Replication Policy Destination**: The source for the offload or archive operation is the target site that is defined in the **Replication Policy** section. This option is available only when Backup Storage Replication is enabled.

The SLA parameters that control the **Destination** of a copy operation are:

- **Cloud Servers**: The target for the offload or archive operation is a cloud storage provider.

- **Repository Servers**: The target for the offload or archive operation is a Spectrum Protect server.

- **Target**: The cloud storage system or repository server to which you want to offload or archive data. For archive operations, only cloud targets that have a defined archive bucket are shown in this list.

The example in Figure 9-6 on page 169 shows how to configure a SLA so that it creates a daily incremental copy of data from the primary vSnap to a Spectrum Protect server container storage pool (using the same retention that is being used for the primary backup) and a monthly full copy to a tape pool at the same SP server (using a retention of 3 months):
For a detailed description on how to create an SLA policy, review the following information: (https://www.ibm.com/support/knowledgecenter/SSNQFQ_10.1.4/spp/t_spp sla_policies_create.html)

9.5 Configuring Multi-Site Backup - Details

All methods to create additional copies of data that have been discussed in the previous sections of this chapter use a single SLA that controls the creation of the primary backup and all subsequent replication or copy operations to secondary storage. Consequently, all of these additional copies belong to the same point-in-time as the primary backup object. The Recovery Point Objective (RPO) of a backup object is always controlled by the parameters of the Main Policy in the Operational Protection section of a SLA.

You can improve (reduce) the RPO by assigning a virtual machine, an application or a SPP catalog backup to more than one SLA in parallel. Similar to replication, this creates backups of the same entity (VM, application or SPP catalog backup) in two different locations (sites). The key difference is the fact that the primary data is being backed up twice, which results in two independent “primary” backup versions of the same entity.

Example 1: SLA with Replication

A VM is assigned to a single SLA with a main policy that runs a daily backup at 8PM and a replication policy replicating data to another vSnap server at 8AM.

The result is to have two copies of backup data with a RPO of 24 hours.
Example 2: Multi-Site / Multi-SLA Backup

A VM is assigned to two SLAs at the same time. One SLA runs a daily backup at 8PM and the second SLA runs a daily backup at 8AM, both are using the same retention, but different target sites and no replication.

The result is to have two copies of backup data with a **RPO of 12 hours**

**Note:** A similar result can be achieved with a single, replication-enabled SLA by changing the schedule from daily to twice daily.

Besides the fact that the RPO can be improved and totally independent copies can be created with Multi-SLA backup, it is important to understand that the method has some limitations and drawbacks compared to a replication approach:

- Increasing the backup frequency adds more load to the hypervisor (e.g. VMware snapshots need to be created more often) or to the application (e.g. because it is set to backup mode more often).
- Additional backups to a distant site might negatively impact performance because they can not benefit from compression as it is being used when replicating backup data between two vSnap servers.
- Microsoft SQL server backups and IBM Db2 backups are limited to a single SLA when log backup is enabled. Having such applications being assigned to two different SLAs at the same time with log backup enabled, this could lead to unpredictable results and require manual intervention.

9.6 Example: Creating incremental and full copies of backup data to an IBM Spectrum Protect server

In this example we will show you how to create additional copies of backup data from IBM Spectrum Protect Plus into an IBM Spectrum Protect server.

**Note:** In this example, we assume that we have a running version 10.1.4 SPP server with a dedicated vSnap server and a running version 8.1.8 SP server on a Linux operating system with a tape library attached. A directory container pool and a tape storage pool already exist.

Both types of additional copies (“hot” incremental copy to a directory container pool and a “cold” full copy / Archive to a tape storage pool) will be configured.

The following tasks need to be performed:

- Preparation of the Spectrum Protect server:
  - Define a ColdDataCache storage pool
  - Define a new Policy Domain of type ObjectDomain
  - Start an ObjectAgent and register an ObjectClient
- Register the SP server as a Repository Server in the SPP user interface
- Create a SLA that performs backups to a vSnap and creates regular additional copies to Spectrum Protect
- Execute the SLA and observe the job results
9.6.1 Preparation of the Spectrum Protect server

**Define a ColdDataCache storage pool**
With Spectrum Protect version 8.1.8, a new storage pool type was introduced which is being used as an intermediate cache to buffer data that shall be copied from an ObjectClient (in this case a SPP vSnap server) to a SP tape storage pool.

In this example, we use the SP server administrative command line to define a ColdDataCache storage pool named *SPP-TAPECACHE*, which uses four directories in a local file system and that uses an existing tape storage pool *TAPEPOOL* as the next storage pool in the hierarchy:

```bash
define stgpool SPP-TAPECACHE stgtype=colddatacache nextstgpool=TAPEPOOL directory=/tsm/stg/colddatacache1,/tsm/stg/colddatacache2,/tsm/stg/colddatacache3,/tsm/stg/colddatacache4
```

ANR2200I Storage pool SPP-TAPECACHE defined (device class *SPP-TAPECACHEDEVCLASS*).

**Define an ObjectDomain**
Once the ColdDataCache storage pool was created, an ObjectDomain needs to be defined. As part of the command that defines an ObjectDomain, two storage pools need to be specified:

- A “StandardPool”, which needs to be a directory- or cloud-container storage pool and will be used for “hot” incremental copies of vSnap backup data.
- A “ColdPool”, which needs to be a ColdDataCache storage pool and will be used for “cold” full copies / archives of vSnap backup data.

The following command creates an ObjectDomain named *SPP* and uses a directory-container storage pool named *DIRECTORYPOOL* for hot data and formerly defined ColdDataCache storage pool named *SPP-TAPECACHE* for cold data:

```bash
define OBJECTDomain SPP STANDARDPool=DIRECTORYPOOL COLDPool=SPP-TAPECACHE
```

ANR1500I Policy domain SPP defined.

ANR1510I Policy set STANDARD defined in policy domain SPP.

ANR1520I Management class STANDARD defined in policy domain SPP, set STANDARD.

ANR1520I Management class COLD defined in policy domain SPP, set STANDARD.

ANR1530I Backup copy group STANDARD defined in policy domain SPP, set STANDARD, management class STANDARD.

ANR1530I Backup copy group STANDARD defined in policy domain SPP, set STANDARD, management class COLD.

ANR1538I Default management class set to STANDARD for policy domain SPP, set STANDARD.

ANR1514I Policy set STANDARD activated in policy domain SPP.
The following example shows the copy group parameters that have been automatically configured:

**Example 9-3  Management classes and copygroup parameters in an ObjectDomain**

```
Protect: ESCC-SP-SRV>query copygroup SPP active

<table>
<thead>
<tr>
<th>Policy Domain Name</th>
<th>Policy Set Name</th>
<th>Mgmt Class Name</th>
<th>Copy Group Name</th>
<th>Version- Exists</th>
<th>Version- Deleted</th>
<th>Retain Extra Versions</th>
<th>Retain Only Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPP</td>
<td>ACTIVE</td>
<td>COLD</td>
<td>STANDARD</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SPP</td>
<td>ACTIVE</td>
<td>STANDARD</td>
<td>STANDARD</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Define an ObjectClient

The easiest way to register an ObjectClient to an IBM Spectrum Protect server is using the SP Operations Center (OC).

**Note:** When defining a policy domain of type ObjectDomain, a policy set and two management classes (*STANDARD* and *COLD*) are automatically defined and activated. The management classes are configured in a way that the application (in this case SPP) controls the data lifecycle.

The following example shows the copy group parameters that have been automatically configured:

**Example 9-3  Management classes and copygroup parameters in an ObjectDomain**

```
Protect: ESCC-SP-SRV>query copygroup SPP active

<table>
<thead>
<tr>
<th>Policy Domain Name</th>
<th>Policy Set Name</th>
<th>Mgmt Class Name</th>
<th>Copy Group Name</th>
<th>Version- Exists</th>
<th>Version- Deleted</th>
<th>Retain Extra Versions</th>
<th>Retain Only Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPP</td>
<td>ACTIVE</td>
<td>COLD</td>
<td>STANDARD</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SPP</td>
<td>ACTIVE</td>
<td>STANDARD</td>
<td>STANDARD</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Define an ObjectClient**

The easiest way to register an ObjectClient to an IBM Spectrum Protect server is using the SP Operations Center (OC).

**Note:** If you register an ObjectClient to a Spectrum Protect server for the first time, the OC wizard will ask you to create also an ObjectAgent, which is enabling the SP server to ingest data through the Amazon S3 protocol.

Once the OC wizard has prepared the configuration, the agent needs to be started from the SP servers operating system command line.

If the ObjectAgent is already running, e.g. because other ObjectClients are already using the SP server, this task can be skipped.

1. Login to the Operations Center (OC) that manages the SP server and start the ObjectClient registration wizard as shown in Figure 9-7 on page 172 by clicking **Clients → Add Client → Object Client** and click **Next**.

![Add ObjectClient wizard in the SP Operations Center](image)
2. In the next dialog the SP server instance can be chosen from a drop-down menu. We select the server ESCC-SP-SRV, which does not yet have an ObjectAgent defined. The wizard automatically asks to create an ObjectAgent and prompts for a name and a port number for the listener. In this example as shown in Figure 9-8, we use \textit{S3OBJECTAGENT} as the name an use the default tcp port 9000.

![Figure 9-8 Specifying the ObjectAgent details](image)

3. When the ObjectAgent configuration is complete, it needs to be started through the operating system command line. In order to obtain the necessary commands, click \textit{View steps}, as shown in Figure 9-9.

![Figure 9-9 Obtaining the command to start the ObjectAgent via the OS command line](image)

4. Log in to the IBM Spectrum Protect server operating system and review the ObjectAgent configuration file which was created by the OC wizard, as it is shown in Example 9-4.

\begin{example}
\textit{Example 9-4 ObjectAgent configuration file}

\begin{verbatim}
[root@escc-sp-srv ~]# cat /tsm/instance/S3OBJECTAGENT/spObjectAgent_S3OBJECTAGENT_1500.config
objagentexe="/opt/tivoli/tsm/server/bin/spObjectAgent" \\
\end{verbatim}
\end{example}
svcnname="IBM Spectrum Protect object agent S3OBJECTAGENT:1500"
agentname=S3OBJECTAGENT
agentport=9000
serverhla=10.0.250.236
serverlla=1500
keystore="/tsm/instance/S3OBJECTAGENT/agentcert.p12"
pwdfile="/tsm/instance/S3OBJECTAGENT/agentcert.pwd"
serverkeypub="/tsm/instance/cert256.arm"
agentconfig="/tsm/instance/S3OBJECTAGENT/spObjectAgent_S3OBJECTAGENT_1500.config"
servercertname="TSM Self-Signed Certificate"

5. Start the ObjectAgent by using the \texttt{startObjectAgent.sh} script, as shown in Example 9-5.

\textit{Example 9-5}

\begin{verbatim}
[root@escc-sp-srv ~]# /opt/tivoli/tsm/server/bin/startObjectAgent.sh
/tsm/instance/S3OBJECTAGENT/spObjectAgent_S3OBJECTAGENT_1500.config
Creating service spObjectAgent_S3OBJECTAGENT_1500 ... 
Starting spObjectAgent ... Succeeded
\end{verbatim}

6. Once the ObjectAgent was started, the ObjectAgent registration continues in the IBM Spectrum Protect Operations Center. As shown in Figure 9-10, specify an ObjectClient name and contact details, then click \textbf{Next}.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{specifying_object_client_name.png}
\caption{Specifying the ObjectClient name}
\end{figure}
7. In the next dialog screen, the policy domain needs to be specified. In this example, as shown in Figure 9-11, we select the ObjectDomain _SPP_, which was prepared in a prior step.

![Add Client](image)

**Figure 9-11  Select the ObjectDomain**

**Note:** The wizard should show the Standard- and Cold copy destinations for the ObjectDomain.

Click **Next** in order to configure the client and get to the final screen of the Add ObjectClient wizard, as shown in Figure 9-12 on page 176.
At this point the preparation of the SP server is complete. As a next step, the SP server needs to be registered in SPP as a Repository server.

9.6.2 Register an IBM Spectrum Protect server as Repository server in IBM Spectrum Protect Plus

To register a Repository server in IBM Spectrum Protect Plus, login to the SPP user interface and go to System Configuration → Backup Storage → Repository Server.

1. Specify a meaningful name, the FQDN, port number (default is 9000) and all the access credentials that have been obtained during the final step of the SP OC Add ObjectClient configuration wizard, as shown in Figure 9-13 on page 177.
2. Click Register in order to start the registration process. When this is complete, you will receive a confirmation message, as shown in Figure 9-14.

3. Click OK to complete the Add Repository server wizard and continue to define a SLA that uses this Repository server in order to create additional copies of backup data.

9.6.3 Create a SLA that creates regular additional copies to IBM Spectrum Protect

In this example, we define a SLA with the following specs:

- **Name:** Primary-with-Tape-Archive
Operational Protection - Main Policy:
- Retention: 7 days
- Frequency: daily
- Start Time: 8 PM
- Target Site: Primary

Operational Protection - Replication:
- no replication between vSnaps is used in this example

Additional Protection - Cloud:
- Retention: Same as source (7 days)
- Frequency: daily
- Start Time: 2 AM
- Source: Main Policy Destination (means: data from original vSnap - not from a replica)
- Destination: Repository Server
- Target: ESCC-SP-SRV

Additional Protection - Archive:
- Retention: 3 months
- Frequency: Weekly, on Sundays
- Start Time: 4 AM
- Source: Main Policy Destination (means: data from original vSnap - not from a replica)
- Destination: Repository Server
- Target: ESCC-SP-SRV

In the SPP user interface, click Manage Protection → Policy Overview → Add SLA Policy in order to define the new SLA. Figure 9-15 shows the configuration of the Main Policy (backup to vSnap for operational protection).

![Policy Overview](image)
Figure 9-16 shows the configuration for the additional copies to IBM Spectrum Protect.

Tip: In this example, we backup data to a vSnap server in the Primary site and create additional copies to a SP server from the same vSnap.

Alternatively, it would be possible to deploy an additional vSnap server in a different site (e.g. “Secondary”), replicate data from the primary site’s vSnap to the secondary site and to create the additional copies to Spectrum Protect from the secondary vSnap.

In order to configure this in the SLA, the SLA parameter “Source” needs to be changed from “Main Policy Destination” to “Replication Policy Destination”

Click Save in order to finish the SLA definition.

9.6.4 Execute the SLA and observe the job results

In order to validate that the configuration was successful, you do not need to wait until the configured start time has come. We assign the “Primary-with-Tape-Archive” SLA to a VM and then execute it manually.
Because the SLA consists of three sections (“Backup to vSnap”, “Offload” and “Archive”) we execute it three times in a sequential manner.

1. First, we need to create a backup of the VM into a vSnap, as shown in Figure 9-17.

   ![Figure 9-17 Execute a SLA - Backup of a VM to vSnap](image)

   Click:
   - Jobs and Operations → Schedule → Action: Start → Backup to vSnap

2. Wait until the backup job is complete. As a next step, as shown in Figure 9-18, the data is copied from the vSnap to the directory container storage pool on the SP server. Note that this is a full copy for the first run, but will be incremental for all subsequent job runs.

   ![Figure 9-18 Execute a SLA - Copy data from vSnap to “Hot” object storage](image)

   Click:
   - Jobs and Operations → Schedule → Action: Start → Offload

3. Wait until the offload job is complete. As a next step, as shown in Figure 9-19, the data is copied from the vSnap to the tape storage pool on the SP server. Note that this is always a full copy.

   ![Figure 9-19 Execute a SLA - Copy data from vSnap to “Cold” Tape storage](image)

   Click:
   - Jobs and Operations → Schedule → Action: Start → Archive
Finally, validate that the backup and copy jobs completed successfully. Figure 9-20 shows the different job logs:

<table>
<thead>
<tr>
<th>SLA Job Log</th>
<th>Type</th>
<th>Status</th>
<th>Duration</th>
<th>Start Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmware_Primary-with-Tape-Archive</td>
<td>Backup - Archive</td>
<td>Completed</td>
<td>0hr 4mins 46secs</td>
<td>Jul 28, 2019 4:00:00 AM</td>
</tr>
<tr>
<td>vmware_Primary-with-Tape-Archive</td>
<td>Backup - Offload</td>
<td>Completed</td>
<td>0hr 1min 21secs</td>
<td>Jul 28, 2019 2:00:00 AM</td>
</tr>
<tr>
<td>vmware_Primary-with-Tape-Archive</td>
<td>Backup</td>
<td>Completed</td>
<td>0hr 1min 42secs</td>
<td>Jul 27, 2019 8:00:00 PM</td>
</tr>
</tbody>
</table>

*Figure 9-20  “Primary-with-Tape-Archive” SLA job logs*

Note that the job logs specify the type of action that has been performed (“Backup”, Backup - Offload” or “Backup - Archive”).
Networking

In larger enterprise environments, it is common practice to implement dedicated networks for different purposes e.g. to isolate backup, application, and management networks from each other. Having a dedicated network for backup and restore workloads brings the following advantages:

- **Performance benefits:** Data protection systems usually handle large amounts of data. Separating backup and restore traffic from application or management data ensures that the performance or the availability of an application is not impacted by running backup or restore jobs.
- **Security benefits:** If an enterprise is hit by a hacker or malware attack, the data protection systems are often your last line of defense where isolated network segments improves the security of the mission critical backups.

This section presents an overview of an environment that uses a separate backup and management network. We will show you how to configure the IBM Spectrum Protect Plus components in order to use the management network for management traffic only, and to route backup traffic to the dedicated backup network.

This chapter describes the following topics:

- “Introduction to Networking with IBM Spectrum Protect Plus”
- “Configuring IBM Spectrum Protect Plus to use a dedicated backup network”
- “Establishing connections through firewalls”
10.1 Introduction to Networking with IBM Spectrum Protect Plus

**Note:** Depending on the design of the existing infrastructure, the number and purpose of network segments might vary. While this example is about separating backup traffic to a dedicated segment, other scenarios might be possible as well:

- Separating replication traffic to a dedicated network
- Separating vSnap servers to different network segments, e.g. DMZ
- Having all components in a single network (e.g. for small test environments)

Figure 10-1 on page 184 shows a logical network diagram for a two-site environment, using a dedicated network to isolate backup and replication workloads from application, user, and admin traffic.
10.2 Configuring IBM Spectrum Protect Plus to use a dedicated backup network

To establish a dedicated backup network, the following components need to be configured properly. Our assumption is that the IBM Spectrum Protect Plus server, vSnap server, and VADP proxy are already installed.

- Physically attach the VMware ESXi or Microsoft Hyper-V Hypervisor(s) to the Backup Network and specify an IP address in the corresponding IP address range.
- Connect the IBM Spectrum Protect Plus server to the Backup Network and specify an IP address in the corresponding IP address range.
- Attach the IBM Spectrum Protect Plus vSnap server(s) to the Backup Network and configure them to use the new connection for all protocols related to backup workloads.
- Connect the IBM Spectrum Protect Plus VADP proxies to the Backup Network (VMware only)

We show you the configuration in more detail in the following sections.

10.2.1 Preparing the VMware ESXi or Microsoft Hyper-V Hypervisors

The VMware ESXi or Microsoft Hyper-V hosts need to be equipped with additional network adapters that will be connected to the Backup Network. Various scenarios would be possible and are highly dependent on the established network infrastructure, e.g., using dedicated physical network adapters or VLAN tagging on the switchports.

Consult your network architect or administrator in order to properly connect the hypervisors to the Backup Network.

**Note:** It is important to understand that each hypervisor needs to have its own IP address in the Backup Network in order to enable VADP, NFS, SMB, or iSCSI connections between the host and the IBM Spectrum Protect VADP proxy (VMware only) and the vSnap storage. Without having an IP address in the Backup Network, the host is not able to mount IBM Spectrum Protect Plus resources for backup or restore.

Figure 10-2 shows a basic setup for VMware using two networks: one application network and a backup network.
In case of VMware, a vmkernel port is required to allow the configuration of an IP address inside a network segment. An example configuration is shown in Figure 10-3.

10.2.2 Preparing the IBM Spectrum Protect Plus server

By default, the IBM Spectrum Protect Plus virtual machine only uses one network adapter during deployment, which should be attached to the management network. Edit the virtual machine configuration of the SPP appliance and add a secondary virtual network interface. Attach it to the newly created Backup Network.

Figure 10-4 shows the addition of a second network adapter to the IBM Spectrum Protect Plus server virtual machine.
After the additional network adapter is attached to the IBM Spectrum Protect Plus server, it needs to be configured properly. Log in to the IBM Spectrum Protect Plus server via the command line using the SSH protocol to configure the new network adapter using the `nmtui` tool in order to assign an IP address that belongs to the backup network IP address range.

Use the `serveradmin` user id to connect to the SPP server command line as shown in Example 10-1.

**Example 10-1  Login to the Spectrum Protect Plus server using the ssh protocol**

```
login as: serveradmin
serveradmin@10.0.250.11's password:*********
Last login: Tue Jul  2 15:46:05 2019 from 10.0.250.70
------------------------------------------------------------------------
IBM Spectrum Protect Plus  10.1.4 build [112]
------------------------------------------------------------------------
```

Validate that the new network adapter is visible in the operating system and note the adapter name, using the `ip a` command, as shown in Example 10-2.

**Example 10-2  Check the SPP operating system for the new network adapter**

```
[serveradmin@t1-spp-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qdisc 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
```

![Figure 10-4  Adding a backup network adapter to the SPP server](image-url)
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever

2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:50:56:98:70:c5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.250.11/24 brd 10.0.250.255 scope global noprefixroute ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe98:70c5/64 scope link
        valid_lft forever preferred_lft forever

3: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:50:56:98:c5:12 brd ff:ff:ff:ff:ff:ff
    inet 172.0.0.11/24 brd 172.0.0.255 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe98:c512/64 scope link
        valid_lft forever preferred_lft forever

[serveradmin@t1-spp-server ~]$  

Start the Network Manager Text User Interface (nmtui) in order to configure the adapter with an IP address, as shown in Example 10-3.

Example 10-3  Starting the nmtui tool to configure the backup network adapter

----------------------------------------------------------------
IBM Spectrum Protect Plus  10.1.4 build [ 112 ]
----------------------------------------------------------------

[serveradmin@t1-spp-server ~]$ nmtui

In nmtui, specify the proper connection type as shown in Figure 10-5 on page 189.
Figure 10-5  Select the connection type for the new backup network adapter

Specify the IP address, subnet mask, gateway, name server, and search domain for the new interface, as shown in Figure 10-6.

Figure 10-6  Adding an IP configuration to the backup network interface

When the configuration is complete, validate that the hypervisors can be pinged via their Backup Network IP address, as shown in Example 10-4.
Example 10-4   Validating the SPP server backup network configuration

[serveradmin@t1-spp-server ~]$ ping 172.0.0.221
PING 172.0.0.221 (172.0.0.221) 56(84) bytes of data.
64 bytes from 172.0.0.221: icmp_seq=1 ttl=64 time=0.720 ms
64 bytes from 172.0.0.221: icmp_seq=2 ttl=64 time=0.238 ms
64 bytes from 172.0.0.221: icmp_seq=3 ttl=64 time=0.279 ms
64 bytes from 172.0.0.221: icmp_seq=4 ttl=64 time=0.269 ms
--- 172.0.0.221 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.238/0.376/0.720/0.199 ms
[serveradmin@t1-spp-server ~]$ 

When the IBM Spectrum Protect Plus server is properly attached to the backup network, the same configuration needs to be done on the VADP proxies and the vSnap servers.

10.2.3 Preparing the IBM Spectrum Protect Plus vSnap server

By default, the IBM Spectrum Protect Plus vSnap server needs to be attached to the management network. In order to route backup traffic to a dedicated backup network, the vSnap servers and VADP proxies need to be connected to the backup network as well.

If the vSnap is a virtual machine, use the hypervisor tools to edit the VM config in order to add a second network adapter and connect it to the new backup network. If the vSnap is a physical machine, you need to add a second physical network adapter and attach it to the backup VLAN.

The following screen captures show how to attach a virtual vSnap server to the backup network, and to configure it so that the backup related protocols (replication, NFS, SMC, and iSCSI) are bound to the backup network adapter.

Because the vSnap is a virtual machine in this scenario, the adapter is added by editing the VM settings, as shown in Figure 10-7 on page 191.
Chapter 10. Networking

After the adapter is added to the vSnap VM, log in to the command line interface using the SSH protocol and use `nmtui` to specify the proper IP settings, as shown in Figure 10-8.

Figure 10-8  Configuring the IP address for a vSnap server backup network adapter
When the configuration is complete, we need to validate that the hypervisors can be pinged via their Backup Network IP address, as shown in Example 10-5.

**Example 10-5  Validating the vSnap server backup network configuration**

```bash
$ login as: serveradmin
$ serveradmin@10.0.250.13's password:
$ Last login: Wed Jul  3 11:13:31 2019 from 10.5.250.31
----------------------------------------------------------------
Be sure to adhere to vSnap hardware and memory requirements as described in IBM Spectrum Protect Plus Blueprints accessible from the IBM Spectrum Protect Plus Knowledge Center.
----------------------------------------------------------------
$ [serveradmin@t1-spp-vsnap-dr ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 00:50:56:98:6e:df brd ff:ff:ff:ff:ff:ff
   inet 10.0.250.13/24 brd 10.0.250.255 scope global noprefixroute ens192
       valid_lft forever preferred_lft forever
   inet6 fe80::250:56ff:fe98:6edf/64 scope link
       valid_lft forever preferred_lft forever
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
   link/ether 00:50:56:98:33:95 brd ff:ff:ff:ff:ff:ff
   inet 172.0.0.13/24 brd 172.0.0.255 scope global noprefixroute ens224
       valid_lft forever preferred_lft forever
   inet6 fe80::250:56ff:fe98:3395/64 scope link
       valid_lft forever preferred_lft forever
$ [serveradmin@t1-spp-vsnap-dr ~]$ ping 172.0.0.221
PING 172.0.0.221 (172.0.0.221) 56(84) bytes of data.
64 bytes from 172.0.0.221: icmp_seq=1 ttl=64 time=1.30 ms
64 bytes from 172.0.0.221: icmp_seq=2 ttl=64 time=0.440 ms
64 bytes from 172.0.0.221: icmp_seq=3 ttl=64 time=0.314 ms
64 bytes from 172.0.0.221: icmp_seq=4 ttl=64 time=0.321 ms
--- 172.0.0.221 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3074ms
rtt min/avg/max/mdev = 0.314/0.594/1.301/0.411 ms
$ [serveradmin@t1-spp-vsnap-dr ~]$
```

After the connection to the backup network is established, the vSnap server needs to be configured to route backup workloads through the backup network adapter.
This can be done by using the `vsnaps network` commands. Use `vsnaps network show` to identify which protocols are enabled on the available network adapters, as shown in Example 10-6.

**Example 10-6  The vsnap network show command**

```
[serveradmin@t1-spp-vsnap-dr ~]$ vsnap network show
ID | NAME   | IPV4 ADDR   | IPV6 ADDR                | SERVICES
--------------------------------------------------------------------------------------------
005056986edf | ens192 | 10.0.250.13 | fe80::250:56ff:fe98:6edf | mgmt, repl, nfs, smb, iscsi
005056983395 | ens224 | 172.0.0.13  | fe80::250:56ff:fe98:3395 | mgmt, repl, nfs, smb, iscsi
[serveradmin@t1-spp-vsnap-dr ~]$
```

Use the `vsnaps network update` command to allow only management traffic on the management network adapter, as shown in Example 10-7.

**Example 10-7  The vsnap network update command**

```
[serveradmin@t1-spp-vsnap-dr ~]$ vsnap network update --id 005056986edf --services mgmt
ID: 005056986edf
NAME: ens192
MAC ADDRESS: 005056986edf
IPV4 ADDRESSES:
    10.0.250.13
IPV6 ADDRESSES:
    fe80::250:56ff:fe98:6edf
SERVICES:
    mgmt

[serveradmin@t1-spp-vsnap-dr ~]$ vsnap network show
ID | NAME   | IPV4 ADDR   | IPV6 ADDR                | SERVICES
--------------------------------------------------------------------------------------------
005056986edf | ens192 | 10.0.250.13 | fe80::250:56ff:fe98:6edf | mgmt
005056983395 | ens224 | 172.0.0.13  | fe80::250:56ff:fe98:3395 | mgmt, repl, nfs, smb, iscsi
[serveradmin@t1-spp-vsnap-dr ~]$
```

This setup ensures that the backup workload is routed to the vSnap through the dedicated backup network adapter.

### 10.2.4 Preparing the IBM Spectrum Protect Plus VADP proxy (VMware only)

It is a common practice to have the VADP proxy component installed on the vSnap server. If the VADP proxy is installed on a separate machine, it needs to have access to both networks (management and backup) as well. No special configuration needs to be done on the VADP proxy to route the different protocol types to their proper adapters. The vSnap server only accepts the backup protocols on the specified network adapter, which ensures that the VADP proxy will also use the same VLAN for backup traffic.

### 10.2.5 Using a dedicated network for vSnap replication

As described in the previous sections, the `vsnaps network update` command can be used to route a specific data protocol to a dedicated network adapter. The same command could be used to force replication traffic between vSnaps to use a dedicated interface.

Usually it should be OK to have replication and backup traffic sharing the same adapter, however there might be reasons to have a separate replication network, e.g. if the replication target vSnap server is located in a distant site and the backup network does not allow routing traffic to the corresponding target segments.
10.3 Establishing connections through firewalls

As all IBM Spectrum Protect Plus and VMware components must communicate with each other, all of the required communication ports need to be opened between those components and associated services.

10.3.1 TCP connections used by IBM Spectrum Protect Plus components

For a complete list of network ports that need to be opened in a firewall, refer to the IBM Spectrum Protect Plus - All Requirements Doc technote:

https://www.ibm.com/support/pages/ibm-spectrum-protect%22%20plus-all-requirements-doc

From there, select the proper version number and browse to the System Requirements document. Here you can review the requirements for each IBM Spectrum Protect Plus component, including a detailed description of incoming and outgoing TCP ports. In addition, you can also review a brief description of the services that are associated with these ports.

10.3.2 Editing firewall ports

While the IBM Spectrum Protect Plus “Master server” and the vSnap server can be deployed from virtual machine images which have all required internal firewall rules in place, some IBM Spectrum Protect Plus components can be installed manually, e.g. the VADP proxy or the vSnap component. In this case the internal firewall rules of the underlying operating system need to be configured to allow the required communication.

See the following IBM technote for examples of how to edit firewall rules in various Linux operating systems:


10.3.3 Testing network connectivity

When all internal and external firewall configurations have been done, the IBM Spectrum Protect Plus Service tool can be used to validate that a connection can be established to a specific component and port.

Details about how to use the Service tool can be found in the Maintenance chapter in “Testing network connectivity” on page 227.
Role Based Access Control

In this chapter we cover the following topics:

- How role-based access control (RBAC) is managed in SPP
- Describe the elements of RBAC
- Define users, roles, and resource groups by way of example
11.1 Role-based access control overview

Through role-based access control, IBM Spectrum Protect Plus can be tailored for individual users, giving them access to the features and resources that they require. This enables you to create self-service models for end-users.

For example, a database admin could spin up an environment with consistent copies of the database without knowing server login credentials or storage credentials. This saves time for the server and storage team.

Role-based access control consists of the following elements:

- **Users**: A user account associates a resource group with a role. To enable a user to log in to SPP and use its functions, you must first add the user as an individual user or as part of an imported group of LDAP users, and then assign resource groups and roles to the user account.

- **Roles**: Roles define the actions that can be performed on the resources that are defined in a resource group. While a resource group defines the resources that will be made available to a user account, a role sets the permissions to interact with the resources defined in the resource group. For example, if a resource group is created that includes backup and restore jobs, the role determines how a user can interact with the jobs.

- **Resources**: A resource group defines the resources that are available to a user. Every resource that is added to SPP can be included in a resource group, along with individual SPP functions and screens. For example, a resource group could include an individual hypervisor, with access to only backup and reporting functionality. When the resource group is associated with a role and a user, the user will see only the screens that are associated with backup and reporting for the assigned hypervisor. Resources are hypervisors, databases, individual screens, and so on.

For further details refer to the IBM SPP User guide or IBM SPP Knowledge-Center:

11.1.1 Plan user, roles, and resource groups

Consider that you are planning to deploy SPP and have to provide access to SPP for specific users. In this example, we create several users with different roles and resource groups:

- **itso_VM**: Virtual machines expert who performs VMware backup / restore with SLA policy Bronze
- **itso_ORA**: Oracle database expert who performs Oracle backup / restore
- **itso_SYS**: SPP expert for SPP administration
- **sppadmin** (default SPP admin user)

Table 11-1 shows the users and their associated roles and resource groups.

<table>
<thead>
<tr>
<th>User</th>
<th>itso_VMW</th>
<th>itso_ORA</th>
<th>itso_SYS</th>
<th>sppadmin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>roleTier1, roleREP</td>
<td>roleTier1, roleTier2</td>
<td>SYSADMIN</td>
<td>SUPERUSER</td>
</tr>
<tr>
<td>Resource group</td>
<td>resourceVMW</td>
<td>resourceORA</td>
<td>(ALL)</td>
<td>(ALL)</td>
</tr>
</tbody>
</table>
The `roleTier1`, `roleTier2` and `roleREP` are described in 11.2, “Create roles” on page 197. The `resourceVMW` and `resourceORA` are described in 11.3, “Create resource groups” on page 199. SPP also has predefined roles and resource groups.

## 11.2 Create roles

Roles define the actions that can be performed on the resources defined in a resource group. To create a custom role, click **Accounts → Role** in the SPP web interface. In our example, we define the roles: `roleTier1`, `roleTier2`, and `roleREP`.

- `roleTier1`: Allows you to view and run jobs and create and view sites in SPP.
- `roleTier2`: Allows everything except managing sites in SPP.
- `roleREP`: Allows you to manage reports in SPP.

Users associated with `roleTier1` should be able to start existing backup jobs and run or view standard and custom reports. The role settings are shown in Table 11-2.

### Table 11-2  The roleTier1

<table>
<thead>
<tr>
<th>roleTier1</th>
<th>Create/register</th>
<th>View</th>
<th>Edit</th>
<th>delete / de-register</th>
<th>Options / run</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Site</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Others)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Users associated with `roleTier2` can do almost anything except manage sites. The role settings are shown in Table 11-3.

### Table 11-3  The roleTier2

<table>
<thead>
<tr>
<th>roleTier2</th>
<th>Create/register</th>
<th>View</th>
<th>Edit</th>
<th>delete / de-register</th>
<th>Options / run</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Others)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Users associated with the role `roleREP` can only work with reports and view backup storage in SPP. The role settings are shown in Table 11-4.

### Table 11-4  The roleREP

<table>
<thead>
<tr>
<th>roleREP</th>
<th>Create/register</th>
<th>View</th>
<th>Edit</th>
<th>delete / de-register</th>
<th>Options / run</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Storage</td>
<td></td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Others)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To add a role, click **Accounts → Role → Create role** in the SPP web interface, as shown in Figure 11-1.

![Create role example for roleTier1](image)

**Figure 11-1  Create role example for roleTier1**

To view the newly created roles, click **Accounts → Role**, as shown in Figure 11-3 on page 199.

**Note:** The SUPERUSER role cannot be assigned to any individual user account, it is dedicated to the sppadmin user.
By selecting the role, the assigned permissions are displayed on the right. To modify or delete a role, click the three dots (…), as shown in Figure 11-2.

![Figure 11-2  Modify a role](image)

11.3 Create resource groups

Resource groups define which resources a user can work with. Every resource added to IBM Spectrum Protect Plus can be included in a resource group, along with individual SPP functions and screens.

For example, a resource group could include a VMware hypervisor, with access to only backup and reporting functionality. When the resource group is associated with a role and a user, the user will only see the screens associated with backup and reporting for the assigned hypervisor.

In our example, we will create two resource groups:

- resourceVMW
  - Resource: Hypervisor > VMware > vCenters > All VMware
  - Resource: Screen > ALL
  - Resource: SLA Policy > Bronze

- resourceORA
  - Resource: Application Server > Oracle > <List of Oracle servers>
  - Resource: Screen > ALL
To add a resource group, click **Accounts → Resource group → Create Resource Group** in the SPP web interface. In Figure 11-4 the resource group `resourceVMW` is created with all required resources. When selecting a resource, always click the lower-left blue *Add Resources* button. Otherwise, it will not be added to the resource group.

*Figure 11-4  Create resource group resourceVMW*

**Note:** The resource *Screen* allows assigned users to open the SPP web interface. Always assign the user to the relevant pages, otherwise the user cannot do anything with the assigned resources in SPP.
11.4 Create users

In this step, we create a custom user and assign the previously created role and resource group. Select Accounts → User → Add User. In Figure 11-5 the user itso_VMW is created and the custom role roleTier1 and roleREP has been assigned. Click continue.

![Create user itso_VMW](image1)

Assign a resource group to the user, as shown in Figure 11-6, and click the blue Add resources button. Then click Create user.

![Assign resources to the new user](image2)
In this section we described how the basic management of RBAC works in SPP by configuring users, roles, and resource groups for a simple scenario with three users, as shown in Figure 11-7. Multiple roles and resource groups can be assigned to an individual user. If an LDAP server has been specified in SPP, it's also possible to assign roles and resource groups to LDAP users.

![Figure 11-7  List of default and custom SPP users](image)

![Table showing list of default and custom SPP users]

<table>
<thead>
<tr>
<th>Username</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>itso_OPA</td>
<td>roleTier1, roleTier2</td>
</tr>
<tr>
<td>itso_SYS</td>
<td>SYSGENADMIN</td>
</tr>
<tr>
<td>itso_VMW</td>
<td>roleREP, roleTier1</td>
</tr>
<tr>
<td>remoteAlert</td>
<td></td>
</tr>
<tr>
<td>spadmin</td>
<td>SUPERUSER</td>
</tr>
</tbody>
</table>
Maintenance

This chapter provides some guidance how IBM Spectrum Protect Plus (SPP) users can maintain this product. We will discuss different approaches to handle daily operations using the Graphical User Interface (GUI) as well as using the Command Line Interface (CLI).

In this chapter, the following maintenance activities are described:

- Update IBM Spectrum Protect Plus components
- IBM Spectrum Protect Plus Troubleshoot (log files)
- Managing the vSnap server
- LDAP and SMTP configuration
- Administrative Console
- Global Preferences
- Managing the IBM Spectrum Protect Plus catalog
- Testing network connectivity
- Search guidelines
- Messages
12.1 Update IBM Spectrum Protect Plus components

If you already have an IBM Spectrum Protect Plus environment running, you might need to upgrade to a newer version. There are several things to consider before you upgrade your systems.

You can update the IBM Spectrum Protect Plus virtual appliance, vSnap servers, and the VADP proxy servers to get the latest features and enhancements. Software patches and updates are installed by using the IBM Spectrum Protect Plus administrative console or command-line interface for these components.

12.1.1 Update sequence

You need to update the IBM Spectrum Protect Plus server first. After the IBM Spectrum Protect Plus update completes, you must update any external vSnap and VADP proxy servers in your environment.

12.1.2 Updating IBM Spectrum Protect Plus virtual appliance

Use the IBM Spectrum Protect Plus Administrative Console to update the virtual appliance. The IBM Spectrum Protect Plus server update can be run offline or online if you have external internet access. Offline means that you need to provide a downloaded upgrade package, while the online update process will download the required packages from the Internet:

- For online updates you need to have access to the FTP site public.dhe.ibm.com. The administrator console checks for available updates automatically and display available updates.

  **Note:** If you want to run online updates but can see only the offline mode, check your internet connectivity and reattempt access to the FTP site, public.dhe.ibm.com.

- For offline updates, download the prerequisite IBM Spectrum Protect Plus update file from the IBM Fix Central Website to a directory on the computer that is running the browser for the Administrative Console. For information about files for IBM Spectrum Protect version 10.1.4.x and how to obtain it from Fix Central, see technote 879861: https://www-01.ibm.com/support/docview.wss?uid=ibm10879861

- Ensure that your IBM Spectrum Protect Plus environment is backed up before you run updates. For more information about backing up your environment, see Backing up the IBM Spectrum Protect Plus application.

- Ensure that no jobs are running during the update procedure. Pause the schedule for any jobs that have a status of **IDLE** or **COMPLETED**.

The following steps are required to update the IBM Spectrum Protect Plus server:

1. From a supported web browser, access the **Administrative Console** at the following address:

   https://hostname:8090/

   Where **hostname** is the IP address of the virtual machine where the application is deployed.

2. In the login window, select **System** from the **Authentication Type** list.

3. Enter the password for the userID serveradmin.
4. The default password is *sppDP758*.

5. Select **Updates and hotfix management**.

6. Click **Browse** to browse for the update (.iso) file to upload to the appliance, and then click **Upload Update Image (or) Hotfix** as shown in Figure 12-1.

**Note:** You can select only one update file at a time.

---

**Note:** The default password for userID serveradmin is *sppDP758*.
7. Acknowledge the Warning, as shown in Figure 12-2.

![Figure 12-2 Are you sure you want to run updates (or) deploy hotfix?](image)

Note: The update process begins once the update image is uploaded to the appliance.

8. When the update is complete, the virtual machine where the application is deployed automatically restarts.

Note: HTML content from previous versions of IBM Spectrum Protect Plus might be stored in your browser cache. Clear the cache before logging in to an updated version of IBM Spectrum Protect Plus to ensure that you are viewing the latest content changes.

9. Do not forget to release the paused jobs, if there are any. Log in to IBM Spectrum Protect Plus GUI and navigate to Jobs and Operations → Schedule and find the jobs that you have paused. From the Actions menu for the paused jobs, select Release Schedule.

12.1.3 Updating vSnap servers

The built-in vSnap server is updated with the IBM Spectrum Protect Plus server. You must update additional vSnap servers that are installed on either virtual or physical appliances separately.

Test restore jobs need to complete prior to initiating an update to vSnap. Jobs that are not completed or canceled when an upgrade is initiated will not be visible when the update has completed. If jobs are not visible when the update has completed, rerun test restore jobs.

You might also be required to update the operating system for the vSnap servers prior to updating the servers. For operating system requirements, see Component requirements on the following website: https://www.ibm.com/support/knowledgecenter/SSNQFQ_10.1.4/spp/r_spp_system_reqs_all.html

Check the current version and operating system

To check the current version and operating system for your vSnap servers, log on to the vSnap server using SSH as the serveradmin user, and use the vSnap command-line interface to issue the vsnap system info command, as shown in Example 12-1.

Example 12-1  The vsnap system info

```
[serveradmin@t3-spp-vsnap ~]$ vsnap system info
ID: 69e6c14f5f0448dbd826f2503712f7
INIT STATUS: Ready
MULTIPOOL SUPPORT: No
LOCAL REPL SUPPORT: No
```
Update a vSnap server

Before you begin the update, ensure that you have backed up your IBM Spectrum Protect Plus environment, as described in Backing up the IBM Spectrum Protect Plus application.

Download the vSnap .run update file and copy it to a temporary location on the vSnap server.

To update a vSnap server, complete the following steps:

1. Log on to the vSnap server using SSH as the serveradmin user.
2. From the directory where the `<updatefilename>.run` file is located, make the file executable and run the installer by issuing the following commands:
   ```
   chmod +x <updatefilename>.run
   sudo ./<updatefilename>.run
   ```
   You are prompted to agree to the License conditions, and after confirmation the vSnap packages are installed.
3. Do not forget to release the paused jobs, if there are any. Log in to IBM Spectrum Protect Plus GUI and navigate to Jobs and Operations → Schedule and find the jobs that you have paused. From the Actions menu for the paused jobs, select Release Schedule.

Updating the operating system for a physical vSnap server

If you have installed the vSnap server on a machine that is running Red Hat Enterprise Linux, you must update the operating system to version 7.5 or 7.6 before you update the vSnap server. For instructions about how to update the operating system, see the Red Hat Enterprise Linux documentation.

Updating the operating system for a virtual vSnap server

If the operating system is CentOS Linux version 7.4 or earlier, you must update the operating system before you update the vSnap server. To update the operating system, follow the instructions in Updating vSnap servers to version 10.1.2. The version 10.1.2 installation includes CentOS Linux version 7.5.

12.1.4 Updating VADP proxies

Updating the IBM Spectrum Protect Plus virtual appliance automatically updates all the VADP proxies that are associated with the virtual appliance. In rare scenarios, such as loss of network connectivity, you must update the VADP proxy manually.
If a VADP proxy update is available for external proxies during a restart of the IBM Spectrum Protect Plus virtual appliance, the update will be automatically applied to any VADP proxy associated with an identity. To associate a VADP proxy with an identity, navigate to **System Configuration → VADP Proxy**. Click the **options icon** and select **Set Options**. Through the User setting, select a previously entered username and password for the VADP proxy server.

To update a VADP proxy manually, complete the following steps:

1. Navigate to the **System Configuration → VADP Proxy** page in IBM Spectrum Protect Plus GUI.
2. The VADP Proxy page displays each proxy server. If a newer version of the VADP proxy software is available, an update icon displays in the **Status** field.
3. Ensure that there are no active jobs that use the proxy, and then click the update icon.

   The proxy server enters a suspended state and installs the latest update. When the update completes, the VADP proxy server automatically resumes and enters an enabled state.

If you are attempting to update as a non-root user, special instructions need to be followed in order to push-install or push-update a VADP proxy:

1. Create a file in the `/etc/sudoers.d/` directory.
   ```bash
   sudo cd /etc/sudoers.d/
   ```
2. Write the text to the file and save it by pressing **CTRL+D** on the keyboard when done.
   ```bash
   sudo cat > 99-vadpuser
   Defaults !requiretty
   vadpuser ALL=NOPASSWD: /tmp/cdm_guestapps_vadpuser/runcommand.sh
   <<Press CTRL+D>>
   ```
3. Set the appropriate permissions on the file.
   ```bash
   sudo chmod 0440 99-vadpuser
   ```

**12.1.5 Applying early availability updates (efix)**

Early availability updates provide fixes for authorized program analysis reports (APARs) and minor issues between IBM Spectrum Protect Plus releases. These updates are available in bundles from the Fix Central Online website, see technote 879861:

https://www-01.ibm.com/support/docview.wss?uid=ibm10879861

Early availability updates might not contain fixes for all IBM Spectrum Protect Plus components. For instructions about how to obtain and install interim fixes, see the download information that is published when the fixes are available.

**12.2 IBM Spectrum Protect Plus troubleshooting (log files)**

For each job that IBM Spectrum Protect Plus records, the commands that it uses to handle the database (including SQL and RMAN commands) in a **command.log** file. There are two options to access these log files:

- Use the **Download .zip** button in the **Jobs and Operations** menu to download the collection of logs for a specific job. The .zip file contains folders named “application/<uuid>” where `<uuid>` matches the last portion of the log dir location. Check the **command.log** files in these folders.
Collecting log files for troubleshooting

To troubleshoot the IBM Spectrum Protect Plus application, you can download an archive of log files that are generated by IBM Spectrum Protect Plus.

To collect log files for troubleshooting, complete the following steps:
1. Click the user menu, and then click Download System Logs. The download process can take some time to complete.
2. Open or save the file log .zip file, which contains individual log files for different IBM Spectrum Protect Plus components.

Log location

IBM Spectrum Protect Plus log location:

To view the real time log files for the different components in IBM Spectrum Protect Plus, SSH to the IBM Spectrum Protect Plus server. The log files can be found in the locations shown in Table 12-1.

<table>
<thead>
<tr>
<th>Log</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virgo logs</td>
<td>/opt/virgo/serviceability/logs</td>
</tr>
<tr>
<td>vSnap log</td>
<td>/opt/vsnap/log</td>
</tr>
<tr>
<td>VMDKbackupproxy</td>
<td>/data/log/vmdkbackupproxy</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>/data/log/rabbitmq</td>
</tr>
<tr>
<td>nodejscdmservice</td>
<td>/data/log/node-cdm-service/</td>
</tr>
<tr>
<td>Mongo</td>
<td>/data/log/mongo</td>
</tr>
<tr>
<td>Guestdeployer</td>
<td>/data/log/guestdeployer</td>
</tr>
<tr>
<td>adminconsole</td>
<td>/data/log/adminconsole/</td>
</tr>
</tbody>
</table>

How to enable logging of IBM Spectrum Protect Plus alerts to the system log

An alert list in the IBM Spectrum Protect Plus user interface displays errors and warnings, helping to quickly identify and resolve issues. Each item in the alert list includes a status icon, a summary of the issue, and a link to associated logs. These alerts can also be logged to the system log on the IBM Spectrum Protect Plus appliance:

How to enable logging Spectrum Protect Plus alerts to the system log
https://www-01.ibm.com/support/docview.wss?uid=ibm10869550

To enable logging of IBM Spectrum Protect Plus alerts to the system log, follow these steps:
1. Before starting, ensure that there are no jobs running on the IBM Spectrum Protect Plus server.
2. Log in to the IBM Spectrum Protect Plus server console via SSH or another remote terminal interface.
3. Modify the property file
   /opt/virgo/repository/ecx-usr/com.syncsort.dp.xsb.persistence.properties by setting
   ```
   mongodb.alertInSystemLogMessages=yes
   ```
4. Restart the virgo service
   ```
   sudo systemctl restart virgo
   ```

Logging to the system log is now enabled. You can check the system log for messages after alerts have been generated by searching on the string SPPalert in the system log, as shown in Example 12-2.

**Example 12-2  SPPalert output**

```bash
[root@t3-spp-server log]# grep SPPAlert /var/log/messages
```

**Note:** Consider the general format of the alerts logged by IBM Spectrum Protect Plus:

- **<Type of Message>:** can be ERROR, WARNING, etc.
- **<Source of Message>:** Indicates the source of the message. This will be SPPAlert for IBM Spectrum Protect Plus messages.
- **<Message>:** This contains the IBM Spectrum Protect Plus alert details.

### 12.3 Managing the vSnap server

The following sections describe aspects of managing the vSnap server.

**Managing disks**

A vSnap creates a storage pool using disks provisioned to the vSnap server. In the case of virtual deployments, the disks can be RDM or virtual disks provisioned from data stores on any backing storage. In the case of physical deployments, the disks can be local or SAN storage attached to the physical server. The local disks might already have external redundancy enabled via a hardware RAID controller, but if not, vSnap can also create RAID-based storage pools for internal redundancy.

Disks that are attached to vSnap servers must be thick provisioned. If disks are thin provisioned, the vSnap server will not have an accurate view of free space in the storage pool, which might lead to data corruption if the underlying data store runs out of space.

If a vSnap was deployed as part of a virtual appliance, it already contains a 100 GB starter virtual disk that can be used to create a pool. You can add more disks before or after creating a pool and accordingly use them to create a larger pool or expand an existing pool. If job logs report that a vSnap server is reaching its storage capacity, additional disks can be added to the vSnap pool. Alternatively, creating new SLA policies will force backups to use an alternate vSnap.

It is essential to protect against vSnap file system corruption which may be caused by a VMware data store on a vSnap server reaching its capacity. Create a stable environment for virtual vSnap servers that do not use RAID configurations by utilizing thick provisioned VMDKs. Replicating to external vSnap servers provides further protection.
A vSnap server will become invalidated if the vSnap pool is deleted or if a vSnap disk is deleted in a non-redundant RAID configuration. All data on the vSnap server will be lost. If your vSnap server becomes invalidated you must unregister the vSnap server using the IBM Spectrum Protect Plus interface, then run the maintenance job. When complete, the vSnap server can be re-registered.

**Detecting disks**
If you add disks to a vSnap server, use the command line or the IBM Spectrum Protect Plus user interface to detect the newly attached disks.

Command line: Run the `vsnap disk rescan` command.

User interface: Click **System Configuration** → **Backup Storage** → **Disk** in the navigation pane, and then click the **Actions menu** next to the relevant vSnap server and select **Rescan**.

**Creating a storage pool**
If you completed the simple initialization procedure described in Chapter 3, “Installation and deployment” on page 37, a storage pool was created automatically, and the information in this section is not applicable.

To complete an advanced initialization, use the `vsnap pool create` command to create a storage pool manually. Before you run the command, ensure that one or more unused disks are available as described in Showing disks. For information about available options, pass the --help flag for any command or subcommand.

Specify a user-friendly display name for the pool and a list of one or more disks. If no disks are specified, all available unused disks are used. You can choose to enable compression and deduplication for the pool during creation. You can also update the compression or deduplication settings at a later time by using the `vsnap pool update` command.

The pool type that you specify during the creation of the storage pool dictates the redundancy of the pool:

- **raid0**
  This is the default option when no pool type is specified. In this case vSnap assumes your disks have external redundancy, for example, if you use virtual disks on a data store backed by redundant storage. In this case, the storage pool will have no internal redundancy.

  Once a disk has been added to a raid0 pool it cannot be removed. Disconnecting the disk will result in the pool becoming unavailable, which can be resolved only by destroying and recreating the pool.

- **raid5**
  When you select this option, the pool is comprised of one or more RAID5 groups each consisting of three or more disks. The number of RAID5 groups and the number of disks in each group depends on the total number of disks you specify during pool creation. Based on the number of available disks, vSnap chooses values that maximize total capacity while also ensuring optimal redundancy of vital metadata.

- **raid6**
  When you select this option, the pool is comprised of one or more RAID6 groups each consisting of four or more disks. The number of RAID6 groups and the number of disks in each group depends on the total number of disks that you specify during pool creation. Based on the number of available disks, vSnap chooses values that maximize total capacity while also ensuring optimal redundancy of vital metadata.
**Initialize vSnap Server Pool**

After a vSnap server is installed physically or deployed as a virtual appliance a pool need to be configured. In Example 12-3 we show with the `vsnap pool show` and the `vsnap volume show` commands on the command line interface (CLI) that no pool or volume is configured yet.

**Example 12-3  The vSnap command line interface (CLI)**

```
[serveradmin@t3-spp-vsnap ~]$ vsnap pool show
TOTAL: 0

[serveradmin@t3-spp-vsnap ~]$ vsnap volume show
ERROR: VolumeInfoError: Failed to collect volume information
```

Before the vSnap pool can be used it needs to be initialized. The simple initialization method available within the IBM Spectrum Protect Plus GUI was shown in “vSnap Pool initialization” on page 61.

For servers that are deployed in a physical environment, the vSnap server console offers more options for initializing the server, including the ability to create a storage pool by using advanced redundancy options and a specific list of disks.

To initialize a vSnap server by using the vSnap server console, complete the following steps:

1. Log in to the vSnap server console with the user ID serveradmin. You can also use a user ID that has vSnap admin privileges that you create by using the `vsnap user create` command.

2. Run the `vsnap system init --skip_pool` command. The command requires no further interaction and completes all initialization tasks except for the creation of a storage pool.
   The process might take 5 - 10 minutes to complete.

After the initialization process is completed, the **Status/Capacity** column shows a utilization bar for your vSnap server. Let's check now what we see on the vSnap CLI when we enter the show command for the vSnap pool again, as shown in Example 12-4.

**Example 12-4  The vsnap pool show command list details of a vSnap pool**

```
[serveradmin@t3-spp-vsnap ~]$ vsnap pool show
TOTAL: 1
ID: 1
NAME: primary
POOL TYPE: raid0
STATUS: ONLINE
HEALTH: 100
COMPRESSION: Yes
COMPRESSION RATIO: 1.01
DEDUPLICATION: No
DEDUPLICATION RATIO: 1.00
ENCRYPTION:
  ENABLED: Yes
  TYPE: disk

TOTAL SPACE: 100.00GB
FREE SPACE: 96.39GB
```

*Note:* The initial password for user ID serveradmin is sppDP758.
The command `vsnap pool show` in Example 12-4 on page 212 lists the details of our vSnap pool. We can see a pool of 100 GB capacity with one disk where compression and encryption is enabled and deduplication is disabled.

In Example 12-5, the `vsnap volume show` command lists one volume in the pool (ID 1). This volume with the ID 1 refers to a cloud cache area that is created with initialization of the vSnap pool. It is not used for backup data. See “Preparing the disk cache area” on page 161 for further details on this.

Example 12-5   The vsnap pool show command list the cloud cache volume after initialization

<table>
<thead>
<tr>
<th>ID</th>
<th>TYPE</th>
<th>POOL</th>
<th>IS CLONE</th>
<th>TOTAL</th>
<th>FREE</th>
<th>USED</th>
<th>NAME</th>
<th>TAGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>filesystem</td>
<td>1</td>
<td>No</td>
<td>100.00GB</td>
<td>96.39GB</td>
<td>24.00KB</td>
<td>vsnap_metadata_cloud</td>
<td>N/A</td>
</tr>
</tbody>
</table>

If we now use the `vsnap snapshot show` command, it does not list any snapshot, which is at this time expected, because no backup was done so far.

**Expanding vSnap storage pool**

If IBM Spectrum Protect Plus reports that a vSnap server is reaching its storage capacity, the vSnap storage pool must be expanded. To expand a vSnap storage pool, you must first add virtual or physical disks on the vSnap server, either by adding virtual disks to the vSnap virtual machine or adding physical disks to the vSnap physical server. See the vSphere documentation for information about creating additional virtual disks.

To expand a vSnap storage pool, complete the following steps:

1. In the navigation pane, click **System Configuration → Backup Storage → Disk**.
2. Select **Actions → Rescan** for the vSnap server that you want to rescan.
3. Click the manage icon the manage icon that is associated with the vSnap server, and then expand the **Add New Disks to Backup Storage** section.
4. Add and save the selected disks. The vSnap pool expands by the size of the disks that are added.

Use the command line to expand a storage pool:

Command line: Run the `vsnap pool expand` command, as shown in Example 12-6. For information about available options, pass the `--help` flag for any command or subcommand.

Example 12-6   The vsnap pool disk expand --help command

```
[serveradmin@t3-spp-vsnap ~]$ vsnap pool expand --help
Usage: vsnap pool expand [OPTIONS]
```
Expand a storage pool by adding disks.

Options:
--id TEXT   ID of the pool to expand. [required]
--disk_list TEXT Comma separated list of disks (name or UUID). If not specified, all available disks are used.
--force     Skip checking if disks are unused. Use this option if you want to use a partition instead of an entire disk.
--help      Show this message and exit.

The following example shows an expansion of the vsnap_pool with an additional disk (100.00 GB).

1. List the current pool by using vsnap pool show. It will show only one disk assigned to this pool. (see last line DISKS IN POOL:) Note the pool ID is 1 and the TOTAL SPACE is 100.00 GB, as shown in Example 12-7.

Example 12-7  The vsnap pool show command before adding an additional disk

[serveradmin@t3-spp-vsnap ~]$ vsnap pool show

TOTAL: 1

ID: 1
NAME: primary
POOL TYPE: raid0
STATUS: ONLINE
HEALTH: 100
COMPRESSION: Yes
COMPRESSION RATIO: 1.36
DEDUPLICATION: Yes
DEDUPLICATION RATIO: 1.01
ENCRIPTION:
   ENABLED: No

TOTAL SPACE: 100.00GB
FREE SPACE: 71.16GB
USED SPACE: 28.84GB
DATA SIZE BEFORE DEDUPLICATION: 25.51GB
DATA SIZE BEFORE COMPRESSION: 34.77GB
CREATED: 2019-08-28 20:41:19 UTC
UPDATED: 2019-09-02 18:34:03 UTC
DISKS PER RAID GROUP: 1
DISKS IN POOL:
   RAID0:
      /dev/sdb1

[serveradmin@t3-spp-vsnap ~]$ vsnap disk show

Example 12-8  The vsnap disk show command

[serveradmin@t3-spp-vsnap ~]$ vsnap disk show

<table>
<thead>
<tr>
<th>UUID</th>
<th>TYPE</th>
<th>VENDOR</th>
<th>MODEL</th>
<th>SIZE</th>
<th>USED AS</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>360000c294686bb281a370e7612e55e153b</td>
<td>SCSI</td>
<td>VMware</td>
<td>Virtual disk</td>
<td>50.00GB</td>
<td>xfs</td>
<td>/dev/sda</td>
</tr>
</tbody>
</table>
3. Use the vCenter to add a new disk to your vSnap VM.

4. After a new disk is added to your vSnap server, check with the `vsnap disk show` command if a new disk is available. Look at the `USED AS` column, it will show the newly added disk as `unused`, as shown in Example 12-9.

**Example 12-9  The vSnap disk show command after adding a new disk**

```
[serveradmin@t3-spp-vsnap ~]$ vsnap disk show

| UUID                              | TYPE | VENDOR | MODEL        | SIZE     | USED AS     | NAME   
|----------------------------------|------|--------|--------------|----------|-------------|--------
| 36000c294686b281a370e7612e55e153b | SCSI | VMware | Virtual disk | 50.00GB  | xfs         | /dev/sda
| 36000c29ac610630aecc2f0c2aa865a8 | SCSI | VMware | Virtual disk | 100.00GB | vsnap_pool  | /dev/sdb
| 36000c2960aa178c16a010c527c249df4 | SCSI | VMware | Virtual disk | 128.00GB | LVM2_member | /dev/sdc
| 36000c291396b40e6b66f62265ac7cf04 | SCSI | VMware | Virtual disk | 100.00GB | unused      | /dev/sdd
```

5. To add the new disk to the vsnap_pool use the `vsnap pool expand --id TEXT --disk_list TEXT` command, as shown in Example 12-10. After completion of the command it will show now 2 disks assigned to this pool (see the last line DISKS IN POOL:), and the TOTAL SPACE has expanded to 200.00 GB.

**Example 12-10  The vsnap pool expand command**

```
[serveradmin@t3-spp-vsnap ~]$ vsnap pool expand --id 1 --disk_list /dev/sdd

ID: 1
NAME: primary
POOL TYPE: raid0
STATUS: ONLINE
HEALTH: 100
COMPRESSION: Yes
COMPRESSION RATIO: 1.36
DEDUPLICATION: Yes
DEDUPLICATION RATIO: 1.01
ENCRYPTION:
   ENABLED: No

TOTAL SPACE: 200.00GB
FREE SPACE: 167.55GB
USED SPACE: 32.45GB
DATA SIZE BEFORE DEDUPLICATION: 25.51GB
DATA SIZE BEFORE COMPRESSION: 34.77GB
CREATED: 2019-08-28 20:41:19 UTC
UPDATED: 2019-09-03 10:55:52 UTC
DISKS PER RAID GROUP: 1
DISKS IN POOL:
   RAID0:
      /dev/sdb1
      /dev/sdd1

[serveradmin@t3-spp-vsnap ~]$
6. Check with the `vsnap disk show` command if the new disk is part of the pool. Look at the `USED AS` column, it will show the newly added disk as part of the `vsnap_pool`, as shown in Example 12-11.

Example 12-11   The vsnap disk show command after expansion

```
[serveradmin@t3-spp-vsnap ~]$ vsnap disk show
+-----------------+-----+--------+----------------+----------+-------------+------+
| UUID            | TYPE | VENDOR | MODEL         | SIZE     | USED AS     | NAME |
|-----------------+-----+--------+----------------+----------+-------------+------+
| 36000c29466b2b2a370e721e55e153 | SCSI | VMware | Virtual disk    | 50.00GB  | xfs         | /dev/sda |
| 36000c29ac6130630ace2f02c2a86b65a8 | SCSI | VMware | Virtual disk    | 100.00GB | vsnap_pool  | /dev/sdb |
| 36000c2960aa178c16a010c527c249df4 | SCSI | VMware | Virtual disk    | 128.00GB | LVM2_member | /dev/sdc |
| 36000c291396b40e6b66f62265a7cf04 | SCSI | VMware | Virtual disk    | 100.00GB | vsnap_pool  | /dev/sdd |
```

Reducing vSnap storage pool

To reduce the vSnap storage pool, it is possible to remove disks similar to expanding disks, as shown in Example 12-12.

Example 12-12   The vsnap pool disk remove --help command

```
[serveradmin@t3-spp-vsnap ~]$ vsnap pool disk remove --help
Usage: vsnap pool disk remove [OPTIONS]
Remove a failed disk in a pool.
Options:
   --id TEXT    ID of the pool to remove disk from. [required]
   --disk TEXT  Disk (name or UUID) to remove. [required]
   --help       Show this message and exit.
```

Uninstall vSnap Server

You can remove a vSnap server from your IBM Spectrum Protect Plus environment.

Ensure that no jobs use SLA policies that define the vSnap server as a backup target. To view the SLA policies that are associated with jobs, see the Backup page for the hypervisor or application that is scheduled for backup. For example, for VMware backup jobs, click Manage Protection → Hypervisors → VMware.

1. Log on to the vSnap server console with the user ID serveradmin.

   **Note:** The default password for userID serveradmin is `sppDP758`.

   You can also use a user ID that has vSnap administrator privileges that you create by using the `vsnap user create` command.

2. Run the following commands:

   ```
   systemctl stop vsnap
   yum remove vsnap
   ```

   After a vSnap server is uninstalled, the configuration is retained in the `/etc/vsnap` directory. The configuration is reused if the vSnap server is reinstalled. The configuration is removed if you ran the optional commands to remove the configuration data.
Optional: If you do not plan to reinstall the vSnap server after it is uninstalled, remove the data and configuration by running the following commands:

```
rm -rf /etc/vsnap
rm -rf /etc/nginx
rm -rf /etc/uwsgi.d
rm -f /etc/uwsgi.ini
```

### 12.4 LDAP and SMTP configuration

You can add a Lightweight Directory Access Protocol (LDAP) and Simple Mail Transfer Protocol (SMTP) server in the IBM Spectrum Protect Plus environment for user account and report features.

#### 12.4.1 Adding an LDAP server

You must add an LDAP server to create IBM Spectrum Protect Plus user accounts by using an LDAP group. These accounts allow users to access IBM Spectrum Protect Plus by using LDAP user names and passwords.

**Note:** Only one LDAP server can be associated with an instance of IBM Spectrum Protect Plus.

You can add a Microsoft Active Directory or OpenLDAP server. Note that OpenLDAP does not support the `sAMAaccountName` user filter that is commonly used with Active Directory. Additionally, the `memberOf` option must be enabled on the OpenLDAP server.

To register an LDAP server, complete the following steps:

1. In the navigation pane, click **System Configuration > LDAP/SMTP**.
2. In the **LDAP Servers** pane, click **Add LDAP Server**.
3. Populate the fields in the **LDAP Servers** pane, as detailed in the following sections.

**Host Address**
The IP address of the host or logical name of the LDAP server.

**Port**
The port on which the LDAP server is listening. The typical default port is 389 for non-SSL connections or 636 for SSL connections.

**SSL**
Enable the SSL option to establish a secure connection to the LDAP server.

**Use existing user**
Enable to select a previously entered user name and password for the LDAP server.

**Bind Name**
The bind distinguished name that is used for authenticating the connection to the LDAP server. IBM Spectrum Protect Plus supports simple bind.
**Password**
The password that is associated with the Bind Distinguished Name.

**Base DN**
The location where users and groups can be found.

**User Filter**
A filter to select only those users in the Base DN that match certain criteria. An example of a valid default user filter is `cn={0}`.

**Tips:**
- To enable authentication by using the sAMAccountName Windows user naming attribute, set the filter to `samaccountname={0}`. When this filter is set, users log in to IBM Spectrum Protect Plus by using only a user name. A domain is not included.
- To enable authentication using the user principal name (UPN) naming attribute, set the filter to `userprincipalname={0}`. When this filter is set, users log in to IBM Spectrum Protect Plus by using the `username@domain` format.
- To enable authentication by using an email address that is associated with LDAP, set the filter to `mail={0}`.

The User Filter setting also controls the type of user name that appears in the IBM Spectrum Protect Plus display of users.

**User RDN**
The relative distinguished path for the user. Specify the path where user records can be found. An example of a valid default RDN is `cn=Users`.

**Group RDN**
The relative distinguished path for the group. If the group is at a different level than the user path, specify the path where group records can be found.

4. Click **Save**.

After the SMTP server is added, the Add LDAP Server button is no longer available.

If your IBM Spectrum Protect Plus server communicates via Secure Socket Layer (SSL) to the LDAP environment, take a look at the following link to register LDAP with SSL authentication:

https://www-01.ibm.com/support/docview.wss?uid=ibm10791677

### 12.4.2 Adding an SMTP server

Adding an SMTP server enables email communications to be sent from IBM Spectrum Protect Plus server.

**Note:** Only one SMTP server can be associated with IBM Spectrum Protect Plus.

To configure a SMTP sever, complete the following steps:

1. In the navigation pane, click **System Configuration > LDAP/SMTP**.
2. In the SMTP Servers pane, click **Add SMTP Server**.
3. Enter the fields in the **SMTP Servers** pane, as shown in the following sections.

**Host Address**
The IP address of the host, or the path and host name of the SMTP server.

**Port**
The communications port of the server that you are adding. The typical default port is 25 for non-SSL connections or 443 for SSL connections.

**Username**
The name that is used to access the SMTP server.

**Password**
The password that is associated with the user name.

**Timeout**
The email timeout value in milliseconds.

**From Address**
The address that is associated with email communications from IBM Spectrum Protect Plus.

**Subject Prefix**
The prefix to add to the email subject lines sent from IBM Spectrum Protect Plus.

4. Click **Save**.

To test the SMTP connection, click the **Test SMTP Server** button, then enter an e-mail address. Click **Send**. A test e-mail message is sent to the e-mail address to verify the connection. After the SMTP server is added, the **Add SMTP Server** button is no longer available.

### 12.4.3 Editing settings for an LDAP or SMTP server

Edit the settings for an LDAP or SMTP server to reflect changes in your IBM Spectrum Protect Plus environment.

To edit the settings for an LDAP or SMTP server, complete the following steps:
1. From the navigation menu, click **System Configuration → LDAP/SMTP**.
2. Click the **edit icon** that is associated with the server. The edit pane is displayed.
3. Revise the settings for the server, and then click **Save**.

### 12.4.4 Deleting an LDAP or SMTP server

Delete an LDAP or SMTP server when it becomes obsolete. Ensure that the server is not in use by IBM Spectrum Protect Plus before deleting the server.

To delete an LDAP or SMTP server, complete the following steps:
1. From the navigation menu, click **System Configuration → LDAP/SMTP**.
2. Click the **delete icon** that is associated with the server.
3. Click **Yes** to delete server.
12.5 Administrative Console

IBM Spectrum Protect Plus provides an additional GUI, the Administrative Console.

Using the administrative console, you can complete the following tasks:
- Get details about the installed product versions.
- Manage and install the licenses.
- Manage and install certificates, e.g. Active Directory LDAP certificates.
- Apply and install Spectrum Protect Plus Software Updates.
- Perform System Actions like Start/Stop the server, reboot the virtual machine, and configure the time zone.

12.5.1 Log in to the Administrative Console

Access the Administrative Console GUI by using the address shown in Example 12-13.

Example 12-13 Administrative Console login

https://spp-server-hostname:8090

In the login window shown in Figure 12-3, select one of the following authentication types shown in the Table 12-2 Authentication Type list.

Table 12-2 Administrative Console - Authentication Type

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Login information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Spectrum Protect Plus</td>
<td>To log in as an IBM Spectrum Protect Plus user with SYSADMIN privileges, enter your administrator user name and password. If you log in by using the admin user account, you are prompted to reset the user name and password. You cannot reset the user name to admin, root, or test.</td>
</tr>
<tr>
<td>System (recommended)</td>
<td>To log in as a system user, enter the server admin password. The default password is sppDP758. You are prompted to change this password during the first login.</td>
</tr>
</tbody>
</table>
After logging on to the Administrative Console, you will see the available options, as shown in Figure 12-4.

Figure 12-4   Administrative Console - System Administrator pane
12.5.2 System Management

Select the **System Management** option to manage your instance of the IBM Spectrum Protect Plus server, including Start, Stop, and Restart, as shown in Figure 12-5.

![System Management](image.png)

**Figure 12-5  Administrative Console - System Management**

12.6 Global Preferences

The user administrator can manage preferences that apply to all IBM Spectrum Protect Plus operations in the **Global Preferences** section.

**Note:** Only users with administrator credentials can manage global preferences.

The **Global Preferences** pane contains default values for parameters that apply to all IBM Spectrum Protect Plus operations. The preferences are organized into three categories: application, protection, and security.
The default values for the global preferences are shown in Table 12-3.

<table>
<thead>
<tr>
<th>Preference</th>
<th>Default value</th>
<th>Unit (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent Application Servers for Backup session</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>vSnap Free Warn Percentage (%)</td>
<td>30</td>
<td>Percentage (%)</td>
</tr>
<tr>
<td>vSnap Free Error Percentage (%)</td>
<td>20</td>
<td>Percentage (%)</td>
</tr>
<tr>
<td>Group VMs by VM Group size (%)</td>
<td>5120</td>
<td>Gigabytes</td>
</tr>
<tr>
<td>Group VMs by Number of VMs in groups</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>VMware Connection Timeout</td>
<td>300</td>
<td>Seconds</td>
</tr>
<tr>
<td>Backup Update Interval</td>
<td>300</td>
<td>Seconds</td>
</tr>
<tr>
<td>Password Minimum Length</td>
<td>8</td>
<td>Characters</td>
</tr>
</tbody>
</table>

To change the default values in the Global Preferences pane, follow this steps:
1. In the navigation pane, click **System Configuration → Global Preferences**.
2. Update the values for the global preferences shown in Table 12-4. To revert to the default value from a previously entered value, click the reset icon.

<table>
<thead>
<tr>
<th>Preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Concurrent Application Servers for Backup session</td>
<td>The maximum number of concurrent application servers per backup session.</td>
</tr>
</tbody>
</table>
| Backup (Hypervisor/Application)     | vSnap Free Warn Percentage (%)  
  The percentage threshold of remaining free space in the vSnap storage pool. Warnings are displayed in the job log. For example, if a value of 10 is specified, a warning is displayed if the vSnap storage pool has 10% or less of remaining free space.  
  
  vSnap Free Error Percentage (%)  
  The percentage threshold of remaining free space in the vSnap storage pool. Errors are displayed in the job log. For example, if a value of 5 is specified, an error is displayed if the vSnap storage pool has 5% or less of remaining free space. |
12.7 Managing the IBM Spectrum Protect Plus catalog

The following sections describe aspects of managing the catalog.

12.7.1 Restoring the IBM Spectrum Protect Plus application

Restore IBM Spectrum Protect Plus configuration settings, restore points, search data, and job information that were backed up to the vSnap server. The data can be restored to the same location or an alternate IBM Spectrum Protect Plus location.

Attention:
An IBM Spectrum Protect Plus restore operation overwrites all data in the IBM Spectrum Protect Plus virtual appliance or alternate virtual appliance location. All IBM Spectrum Protect Plus operations stop while the data is being restored. The user interface is not accessible, and all jobs that are running are canceled. Any snapshots that are created between the backup and restore operations are not saved.

If restoring an offloaded cloud backup, the cloud resource or repository server must be registered on the alternate IBM Spectrum Protect Plus location.

To restore IBM Spectrum Protect Plus data, complete the following steps:

1. In the navigation pane, click Manage Protection → IBM Spectrum Protect Plus → Restore.
2. Select a vSnap server, cloud resource, or repository server.

<table>
<thead>
<tr>
<th>Preference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>Group VMs: Virtual machines can be grouped together. The group can be defined by account of the VMs contained or the size of the VMs contained in the group.</td>
</tr>
<tr>
<td>VMware Connection Timeout: The amount of time that IBM Spectrum Protect Plus waits for commands that are issued to connected vCenters to finish. If the operations do not finish within the specified amount of time, they are logged as errors. This setting applies only to VMware hypervisors.</td>
<td></td>
</tr>
<tr>
<td>Backup Update Interval: The frequency at which messages about the progress of data transfer are updated in the job log.</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Password Minimum Length: The minimum length of passwords for IBM Spectrum Protect Plus. By default, the password has a minimum length of 8 characters, but you can specify a longer password. This value applies to all user accounts.</td>
</tr>
</tbody>
</table>

Note: For VM Grouping, there are four VM groups and each VM group can have a maximum of five VMs. Each group corresponds to one destination volume (data stream). A maximum of 20 VMs (4 data streams) can be done at a time based on size calculations.
Data can be restored to the same location, or an alternate location in disaster recovery scenarios. Available snapshots for the server are displayed.

3. Click **Restore** for the catalog snapshot that you want to restore.

4. Select one of the following restore modes:

   **Restore the catalog and suspend all scheduled jobs**
   The catalog is restored and all scheduled jobs are left in a suspended state. No scheduled jobs are started, which allows for the validation and testing of catalog entries and the creation of new jobs. Typically, this option is used in DevOps use cases.

   **Restore the catalog**
   The catalog is restored and all scheduled jobs continue to run as captured in the catalog backup. Typically, this option is used in disaster recovery.

5. Click **Restore**.

6. To run the restore job, in the dialog box, click **Yes**.

### 12.7.2 Deleting IBM Spectrum Protect Plus resources from the catalog

You can use the Virtual Machines/Databases tab in the Restore Point Retention pane to expire catalog metadata that is associated with a resource from the IBM Spectrum Protect Plus catalog. Resources are added to the catalog through inventory jobs. Expiring a resource removes the metadata that is associated with a restore point from the catalog, which frees up space in the catalog and removes the restore point from recovery screens.

Expiring a resource from the catalog does not remove associated snapshots from a vSnap server or secondary backup storage.

To expire a resource from the catalog:

1. In the navigation pane, click **Manage Protection** → **IBM Spectrum Protect Plus** → **Restore Point Retention**.
2. Click the **Virtual Machines/Databases** tab.
3. Use the filter to search by resource type, then enter a search string to search for a resource by name. For more information about using the search function, see Search guidelines.
4. Click the search icon.
5. Click the delete icon that is associated with a resource.
6. To confirm the expiration, in the dialog box, click **Yes**.

As the result, the catalog metadata associated with the resource is removed from the catalog.

### 12.7.3 Managing IBM Spectrum Protect Plus restore points

You can use the **Restore Point Retention** pane to search for restore points in the IBM Spectrum Protect Plus catalog by backup job name, view their creation and expiration dates, and override the assigned retention.

Expiring a job session will not remove a snapshot and related recovery point if the snapshot is locked by a replication or offload relationship. Run the replication or offload-enabled job to change the lock to a later snapshot. The snapshot and recovery point will be removed during the next run of the maintenance job.
To set a job session to expire, complete the following steps:

1. In the navigation pane, click Manage Protection → IBM Spectrum Protect Plus → Restore Point Retention.

2. In the Backup Sessions tab, search for the desired job session or restore point. For more information about using the search function, see Search guidelines. Alternatively, in the Virtual Machines / Databases tab, select either Applications or Hypervisors to search for the desired catalog entry by entering the name. Names can be searched by entering partial text, using the asterisk (*) as a wildcard character, or using the question mark (?) for pattern matching.

3. Optional: If searching from the Backup Sessions tab, use filters to fine-tune your search across job types and date range when the associated backup job started.

4. Click the search icon the search icon.

5. Select the job sessions you want to expire.

6. From the Actions list, select one of the following options:
   - **Expire** is used to expire a single job session.
   - **Expire All Job Sessions** is used to expire all unexpired job sessions for the selected job.

7. To confirm the expiration, in the dialog box, click Yes.

As a result, the job session is removed during the next run of the maintenance job.

### 12.8 Search guidelines

Use filters to search for an entity, such as a file or a restore point. You can enter a character string to find objects with a name that exactly matches the character string. For example, searching for the term string.txt returns the exact match, string.txt.


You can also include the following special characters in the search. You must use a backslash (\) escape character before any of the special characters:

\+ \- \& \! \{ \} \[ \] \^ \~ \* \? \:\

For example, to search for the file string[2].txt, enter the string\[2\].txt.

### 12.8.1 Searching with wildcards

You can position wildcards at the beginning, middle, or end of a string, and combine them within a string.

**Match a character string with an asterisk**

The following examples show search text with an asterisk:

- **string*** searches for terms like string, strings, or stringency
- **str*ing** searches for terms like string, straying, or straightening
*string searches for terms like string or shoestring

You can use multiple asterisk wildcards in a single text string, but multiple wildcards might considerably slow down a large search.

### 12.8.2 Match a single character with a question mark:

The following examples show search text with a question mark:

- `string?` searches for terms like strings, stringy, or string1
- `st??ring` searches for terms like starring or steering
- `???string` searches for terms like hamstring or bowstring

### 12.9 Testing network connectivity

The IBM Spectrum Protect Plus Service Tool is running tests on host addresses and ports to determine if a connection can be established. You can use the Service Tool to verify whether a connection can be established between IBM Spectrum Protect Plus and a node.

You can run the Service Tool from the IBM Spectrum Protect Plus command line or remotely by using a .jar file. If a connection can be established, the tool returns a green check mark. If a connection cannot be established, the error condition is displayed, along with possible causes and actions.

The tool provides guidance for the following error conditions:

- Timeout
- Connection refused
- Unknown host
- No route

Figure 12-6 on page 228 and Figure 12-7 on page 228 give an outlook of what the tool looks like.
Figure 12-6  Network Connection Test Tool - Settings

Figure 12-7  Network Connection Test Tool - Results

<table>
<thead>
<tr>
<th>Host</th>
<th>Port</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>t3-spp-server</td>
<td>22</td>
<td>Secure Shell (SSH)</td>
<td>✔</td>
</tr>
<tr>
<td>t3-spp-server</td>
<td>443</td>
<td>Default web server secure port used with SPP, VCenter and ESX</td>
<td>✔</td>
</tr>
<tr>
<td>t3-spp-server</td>
<td>111</td>
<td>Remote Procedure Call (RPC) port</td>
<td>✔</td>
</tr>
<tr>
<td>t3-spp-server</td>
<td>8000</td>
<td>VSnap management service</td>
<td>✔</td>
</tr>
</tbody>
</table>
12.9.1 Running the Service Tool from a command-line interface

You can start the Service Tool from the IBM Spectrum Protect Plus virtual appliance command-line interface and run the tool in a web browser. Then, you can use the Service Tool to verify network connectivity between IBM Spectrum Protect Plus and a node. To use the tool follow these steps:

1. Log in to the IBM Spectrum Protect Plus virtual appliance by using the serveradmin user ID and access the command prompt. Issue the following command:
   
   # sudo bash

2. Open port 9000 on the firewall by issuing the following command:

   # firewall-cmd --add-port=9000/tcp

3. Run the tool by issuing the following command:

   # java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxdd.jar

4. To connect to the tool, enter the following URL in a browser:

   http://hostname:9000

   where hostname specifies the IP address of the virtual machine where the application is deployed.

5. To specify the node to test, populate the following fields:

   **Host**
   - The host name or IP address of the node that you want to test.

   **Port**
   - The connection port to test.

6. Click **Save**.

7. To run the tool, hover the cursor over the tool, and then click the green **Run** button.

If a connection cannot be established, the error condition is displayed, along with possible causes and actions.

8. Stop the tool by issuing the following command on the command line:

   `ctl-c`

9. Protect your storage environment by resetting the firewall. Issue the following commands:

   # firewall-cmd --zone=public --remove-port=9000/tcp
   # firewall-cmd --runtime-to-permanent
   # firewall-cmd --reload

**Note:** If the firewall-cmd command is not available on your system, edit the firewall manually to add necessary ports and restart the firewall using ip tables. For more information on editing firewall rules, see the Firewall configuration using iptables section here:


12.9.2 Running the Service Tool remotely

You can download the Service Tool as a .jar file from the IBM Spectrum Protect Plus user interface. Then, you can use the Service Tool to remotely test connectivity between IBM Spectrum Protect Plus and a node.
To use the tool remotely follow these steps:

1. In the IBM Spectrum Protect Plus user interface, click the user menu on the upper right to drop down a list and then click **Download Test Tool**.
   A .jar file is downloaded to your workstation.

2. Launch the tool from a command-line interface. Java is only required on the system where the tool will be launched. Endpoints or target systems that are tested by the tool do not require Java.
   The following command launches the tool in a Linux environment:

   ```bash
   # java -jar -Dserver.port=9000 /<tool path >/ngxdd.jar
   ```

3. Run the tool by issuing the following command:

   ```bash
   # java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxdd.jar
   ```

4. To connect to the tool, enter the following URL in a browser:

   ```url
   http://hostname:9000
   ```
   where hostname specifies the IP address of the virtual machine where the application is deployed.

5. To specify the node to test, populate the following fields:
   - **Host**: The host name or IP address of the node that you want to test.
   - **Port**: The connection port to test.

6. Click **Save**.

7. To run the tool, hover the cursor over the tool, and then click the green **Run** button.

   If a connection cannot be established, the error condition is displayed, along with possible causes and actions.

8. Stop the tool by issuing the following command on the command line:

   ```bash
   ctl-c
   ```

### 12.10 Messages

IBM Spectrum Protect Plus components send messages with prefixes that help to identify which component they come from. Use the search option to find a particular message by using its unique identifier.

Messages consist of the following elements:

- A five-letter prefix.
- A number to identify the message.
- Message text that is displayed on screen and written to message logs.

**Tip:** Use your browser’s search capability by using Ctrl+F to find the message code you are looking for.

The following example contains the Db2 agent prefix. When you click **More**, extra details that explain the reason for the message are shown (Example 12-14 on page 231).
Example 12-14  Messages Example - Warning

Warning
Apr 16, 2019
9:14:37 AM
CTGGH0098
[myserver1.myplace.irl.ibm.com]
Database AC7 will not be backed up as it is ineligible for the backup operation.

12.10.1 IBM Spectrum Protect Plus message prefixes

Messages have different prefixes to help you to identify the component that issues the message.

Table 12-5 identifies the prefix that is associated with each component.

Table 12-5  Messages prefixes by component

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTGGA</td>
<td>IBM Spectrum Protect Plus</td>
</tr>
<tr>
<td>CTGGE</td>
<td>IBM Spectrum Protect Plus for Microsoft SQL Server</td>
</tr>
<tr>
<td>CTGGF</td>
<td>IBM Spectrum Protect Plus for Oracle</td>
</tr>
<tr>
<td>CTGGG</td>
<td>IBM Spectrum Protect Plus for Microsoft Exchange Server</td>
</tr>
<tr>
<td>CTGGH</td>
<td>IBM Spectrum Protect Plus for IBM Db2</td>
</tr>
<tr>
<td>CTGGI</td>
<td>IBM Spectrum Protect Plus for MongoDB</td>
</tr>
</tbody>
</table>

See the IBM Knowledge Center for IBM Spectrum Protect Plus for a complete list of messages:
The vSnap CLI

This chapter describes details of the vSnap Backup Storage server command-line interface (CLI), which is used to administer the vSnap server and configure advanced options.
13.1 vSnap server CLI

The vSnap server has two user interfaces to administer the server. Graphical access to the vSnap server configuration is provided as part of web-based IBM Spectrum Protect Plus Day-to-day GUI. Under **System Configuration → Backup Storage → Disk** all available vSnap Backup Storage servers with their current status and capacity are listed. The second user interface is a command-line interface (CLI), which could be entered via SSH using the default `serveradmin` user ID. The sections “User interfaces” on page 13 and 3.3.2, “Configure the vSnap Backup Storage server” on page 52 provide details about how to use and configure the access to these user interfaces.

In Example 13-1 we show how to log in to the CLI user interface using the `serveradmin` user ID and using the command `v.snap` to list all options for the vSnap CLI.

**Example 13-1  The vSnap Backup Storage CLI**

```
Using username "serveradmin".
serveradmin@spp-vsnap-demo's password:
Last login: Mon Aug  5 13:18:46 2019 from 9.123.45.67
----------------------------------------------------------------
Be sure to adhere to vSnap hardware and memory requirements as described in IBM Spectrum Protect Plus Blueprints accessible from the IBM Spectrum Protect Plus Knowledge Center.
----------------------------------------------------------------

[spp-vsnap-demo ~]$ v.snap
Usage: v.snap [OPTIONS] COMMAND [ARGS]...

Options:
--json     Show output in JSON format.
--summary  Show output in summary (tabular) format.
--detail   Show output in detail (multiline) format.
--help     Show this message and exit.

Commands:
  archive       Manage archive resources.
  cloud         Manage cloud resources.
  disk          Manage disks.
  host          Manage volume host mappings.
  maint         Manage maintenance sessions.
  network       Manage network interfaces.
  partner       Manage partner servers.
  pool          Manage storage pools.
  relationship  Manage replication relationships.
  session       Manage replication sessions.
  share         Manage volume shares.
  snapshot      Manage volume snapshots.
  system        Manage vSnap system.
  target        Manage storage targets.
  throttle      Manage throttling events.
  user          Manage vSnap users.
  volume        Manage storage volumes.

[spp-vsnap-demo ~]$ 
```
13.2 vSnap server initialization

After the deployment or installation on a physical server, the vSnap server must be initialized. This could be either down with the GUI or CLI interface. Using the GUI is described as part of the installation and deployment process in “vSnap Pool initialization” on page 61, and the CLI initialization is described in “Initialize vSnap Server Pool” on page 212.

13.3 vSnap server preferences

The preferences of the vSnap server can be listed using the command `vsnap system pref get` as shown in Example 13-2.

Example 13-2  List vSnap server preferences

```
[serveradmin@spp-vsnap-demo ~]$ vsnap system pref get
NAME                             | DEFAULT VALUE | USER VALUE | TYPE
-----------------------------------------------------------------------
archiveCompressMinSize           | 10485760      | N/A        | integer
archiveDefaultRetrievalTier      | Bulk          | N/A        | string
archiveListObjectsMax            | 1000          | N/A        | integer
archiveLunGranular               | true          | N/A        | boolean
archiveMaxParallelClone          | 2             | N/A        | integer
archiveMaxParallelDelete         | 2             | N/A        | integer
archiveMaxStreams                | 5             | N/A        | integer
archiveObjectSize                | 1048576000000 | N/A        | integer
archiveOffloadMaxAttempts        | 5             | N/A        | integer
archivePartSize                  | 104857600     | N/A        | integer
archiveRestoreDays               | 3             | N/A        | integer
archiveRestoreMaxAttempts        | 50            | N/A        | integer
archiveRestoreSleepSecs          | 30            | N/A        | integer
archiveSimulatorEnabled          | false         | N/A        | boolean
archiveSimulatorRestoreSeconds   | 30            | N/A        | integer
archiveStatusUpdateFrequency     | 300           | N/A        | integer
archiveThreads                   | 4             | N/A        | integer
archiveThrottleRate              | 536870912     | N/A        | integer
archiveThrottleRatePoll          | 120           | N/A        | integer
archiveTransferRetryable         | true          | N/A        | boolean
archiveUnmountMaxAttempts        | 30            | N/A        | integer
archiveWorkers                   | 4             | N/A        | integer
asyncSnapshotWait                | 15            | N/A        | integer
cancelPendingSessionsOnRestart   | true          | N/A        | boolean
cloudBlockSize                   | 4096          | N/A        | integer
cloudBlockmapOperationTimeout    | 86400         | N/A        | integer
cloudChannelSize                 | 536870912     | N/A        | integer
cloudCondenseChunkSize           | 2097152       | N/A        | integer
cloudCondenseInterval            | 3             | N/A        | integer
cloudConnectionTimeout           | 600           | N/A        | integer
cloudCrashOnExportTimeout        | false         | N/A        | boolean
cloudDbBlockmapDownload          | false         | N/A        | boolean
cloudDbBlockmapUpload            | true          | N/A        | boolean
cloudDeviceQueueDepth            | 16            | N/A        | integer
cloudDownloadThreads             | 16            | N/A        | integer
cloudDynamicThrottle             | true          | N/A        | boolean
```
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cloudErrorCleanupTimeout</td>
<td>120</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudIOReadAttempts</td>
<td>3</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudIOReadIntervalSecs</td>
<td>5</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudIOReadTimeout</td>
<td>60</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudIOTimeout</td>
<td>300</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudIOWriteAttempts</td>
<td>5</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudIOWriteIntervalSecs</td>
<td>30</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudKillOnExportTimeout</td>
<td>true</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudLocalBlockmapRetention</td>
<td>3</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudLogMessageBufferSize</td>
<td>24</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudLogMessageFlushIntervalSecs</td>
<td>180</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudMaxAttempts</td>
<td>10</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudMaxParallelClone</td>
<td>2</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudMaxParallelDelete</td>
<td>2</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudMaxStreams</td>
<td>5</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudObjectSize</td>
<td>16777216</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudOffloadCacheSize</td>
<td>8589934592</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudOffloadChunkSize</td>
<td>131072</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudOffloadLogPeriod</td>
<td>300</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudOffloadRate</td>
<td>536870912</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudOffloadThreads</td>
<td>16</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudPendingUploadTimeout</td>
<td>2700</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudPoolExportIntervalSecs</td>
<td>30</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudPoolExportNumAttempts</td>
<td>5</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudPoolImportIntervalSecs</td>
<td>3600</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudPoolImportTimeout</td>
<td>900</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudPoolSyncTimeout</td>
<td>3600</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudPreserveOffloadFailure</td>
<td>false</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudPropagateReadErrors</td>
<td>true</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudReadTimeout</td>
<td>600</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudRecordsCache</td>
<td>128</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudRecordsFlush</td>
<td>64</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudRequireDataDisk</td>
<td>true</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudRestoreCacheSize</td>
<td>6553600000</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudRestoreChunkSize</td>
<td>1048576</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudRestoreMemcacheRetention</td>
<td>30</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudRestoreMemcacheSize</td>
<td>16777216</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudRestoreMinChunkSize</td>
<td>524288</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudScsiCommandTimeout</td>
<td>0</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudSpacemapBinaryFormat</td>
<td>true</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudSpacemapTrimEnabled</td>
<td>false</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudSuccessCleanupTimeout</td>
<td>600</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudThrottleDirtyData</td>
<td>268435456</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudThrottleMemPercent</td>
<td>90</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudThrottleObjectsPoll</td>
<td>5</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudThrottleObjectsRatio</td>
<td>0.9</td>
<td>float</td>
<td></td>
</tr>
<tr>
<td>cloudThrottleRatePoll</td>
<td>120</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudTotalTempSpace</td>
<td>26843545600</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudTransferTimeout</td>
<td>604800</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>cloudUseL2ARC</td>
<td>false</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudUseSLOG</td>
<td>false</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudVerifyBlockmapOnOffload</td>
<td>false</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>cloudWaitBeforeForceExport</td>
<td>20</td>
<td>integer</td>
<td></td>
</tr>
<tr>
<td>createFileBasedLuns</td>
<td>true</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>debugOffloadToFile</td>
<td>false</td>
<td>boolean</td>
<td></td>
</tr>
<tr>
<td>Preference</td>
<td>Value 1</td>
<td>Value 2</td>
<td>Type</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>dedupeVolsWithSmallBlocks</td>
<td>false</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>excludeAllowedHostsPrefix</td>
<td>N/A</td>
<td>N/A</td>
<td>string</td>
</tr>
<tr>
<td>gatewayDeviceWait</td>
<td>10</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>initInstallZFS</td>
<td>true</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>lunTargetQueueDepth</td>
<td>32</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>lunTargetTPU</td>
<td>0</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>maintainCloudObjectsCount</td>
<td>5000</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>maintainCloudObjectsRetention</td>
<td>7</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>maintainServiceCleanupFrequency</td>
<td>21600</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>maintainServiceFrequency</td>
<td>300</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>mvrSkipInputPipeWait</td>
<td>true</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>mvrSkipOutputPipeWait</td>
<td>true</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>passwordMinLength</td>
<td>8</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>poolListTimeout</td>
<td>300</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>replDynamicThrottle</td>
<td>true</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>replMaxStreams</td>
<td>5</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>replMgmtTimeout</td>
<td>840</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>replServiceFrequency</td>
<td>30</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>replSnapshotTimeout</td>
<td>3600</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>replStreamCompress</td>
<td>true</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>replStreamResume</td>
<td>false</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>replTargetSpaceLimitRatio</td>
<td>0.95</td>
<td>N/A</td>
<td>float</td>
</tr>
<tr>
<td>replTransferTimeout</td>
<td>604800</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>requireDiskUUID</td>
<td>true</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>sessionHistoryRetentionHours</td>
<td>48</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>shareIgnoreAllowedHosts</td>
<td>false</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>skipOffloadCleanup</td>
<td>false</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>smbReloadWait</td>
<td>15</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>snapshotCreateTimeout</td>
<td>600</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>snapshotDeleteSync</td>
<td>false</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>snapshotDestroyTimeout</td>
<td>7200</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>systemNotifyEnabled</td>
<td>false</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>volumeCreateTimeout</td>
<td>600</td>
<td>N/A</td>
<td>integer</td>
</tr>
<tr>
<td>volumeDeleteSync</td>
<td>false</td>
<td>N/A</td>
<td>boolean</td>
</tr>
<tr>
<td>volumeDestroyTimeout</td>
<td>7200</td>
<td>N/A</td>
<td>integer</td>
</tr>
</tbody>
</table>

Specific values could be filter by using the `grep` option as shown in Example 13-3, where we list the maximum number of streams archive, cloud and replication operations.

Example 13-3  Filter the preference list for specific values using grep

```
[serveradmin@spp-vsnap-demo ~]$ vsnap system pref get | grep -i MaxStreams
archiveMaxStreams | 5 | N/A | integer
cloudMaxStreams   | 5 | N/A | integer
replMaxStreams    | 5 | N/A | integer
```

13.3.1 Changing replication streams and timeouts

The preferences of the replication process between two vSnap servers can be adjusted if required. By default, five streams are used to replicate data from the source vSnap server to the target vSnap server. If enough bandwidth, CPU and memory resources on both vSnap servers are available, the number of streams could be increased to 10 as shown in Example 13-4 on page 238.
Example 13-4   Increase replication streams
[serveradmin@spp-vsnap-demo ~]$ vsnap system pref set --name replMaxStreams
--value 10

NAME: replMaxStreams
DEFAULT VALUE: 5
USER VALUE: 10
TYPE: integer

Another option is the timeout setting of a replication task. By default the timeout its set to 608400 seconds, which translate to 7 days. A large timeout can be required especially for initial replication tasks. To change this value to a timeout of 24 hours you can set it to 86400 seconds as shown in Example 13-5.

Example 13-5   Change timeout values for the replication
[serveradmin@spp-vsnap-demo ~]$ vsnap system pref set --name replTransferTimeout
--value 86400

NAME: replTransferTimeout
DEFAULT VALUE: 604800
USER VALUE: 86400
TYPE: integer

13.4 vSnap volumes and snapshots

In this section, we explain details on volumes and snapshots used on the vSnap server to manage the backup data. In the first step we look at what happen when a backup is performed while in the second step what happens when backup data is replicated.

Before a backup could be taken, a resource need to assigned to an SLA. Chapter 4.1.3, “Assign an SLA policy” on page 73 explains this as example for virtual machines and chapter 1.3, “SLA backup policies” on page 15 speaks about SLA policies in general.

Replication must be configured before it can be used. In 9.3.1, “Configure vSnap Replication” on page 157 all required steps are explained.

13.4.1 Volumes and snapshots for backup data

When a SLA for backing up data is executed for the first time, immediately a new volume is created while the backup job is running. In Example 13-6 the command vsnap volume show list the newly created volume with the ID 2. The volume with the ID 1 refers to a cloud cache area which is created with initialization of the vSnap pool. See “Preparing the disk cache area” on page 161 for further details about this.

Example 13-6   Execution of a SLA to create a new volume in the vSnap server
[serveradmin@t2-spp-vsnap ~]$ vsnap volume show
<table>
<thead>
<tr>
<th>ID</th>
<th>TYPE</th>
<th>POOL</th>
<th>IS CLONE</th>
<th>TOTAL</th>
<th>FREE</th>
<th>USED</th>
<th>NAME</th>
<th>TAGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>filesystem</td>
<td>1</td>
<td>No</td>
<td>100.00GB</td>
<td>93.62GB</td>
<td>24.00KB</td>
<td>vsnap_metadata_cloud</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>filesystem</td>
<td>1</td>
<td>No</td>
<td>100.00GB</td>
<td>93.62GB</td>
<td>2.77GB</td>
<td>spp_1004_2002_16b6aeb7936__group0_12</td>
<td>N/A</td>
</tr>
</tbody>
</table>
The first number referenced in the volume name (in our example 1004) is the **Job ID** of the job using this volume. In our example we have associated a VMware backup with the Bronze SLA, which created the job **vmware_Bronze** that is listed under the **Jobs and Operations** in the IBM Spectrum Protect Plus GUI. The Job **ID:1004** of **vmware_Bronze** could be figured out when looking into the first line of the job log, as shown in Figure 13-1.

**Figure 13-1  vmware_Bronze Job Log**

The volume is based on a filesystem and the Operating System command `df -h` will list all filesystem of the vSnap server as shown in Example 13-7. The vSnap filesystem belonging to the volume could be identified by using the volume ID, which is part of the filesystem. In our example it is volume **ID 2** corresponding to filesystem `/vsnap/vpool1/fs2`.

**Example 13-7   The df -h command list the vSnap file systems**

```
[serveradmin@t2-spp-vsnap ~]$ df -h
Filesystem          Size  Used Avail Use% Mounted on
devtmpfs            16G     0   16G   0% /dev
tmpfs               16G     0   16G   0% /dev/shm
tmpfs               16G  153M   16G   1% /run
tmpfs               16G     0   16G   0% /sys/fs/cgroup
/dev/mapper/centos-root  34G  2.4G   31G  8% /
/dev/mapper/vsnapdata-vsnapdatalv 126G  33M  126G 1% /opt/vsnap-data
/dev/sda1            1014M  191M  824M 19% /boot
vpool1               85G    0  85G  0% /vsnap/vpool1
vpool1/fs1           85G    0  85G  0% /vsnap/vpool1/fs1
vpool1/fs2           97G  13G   85G 13% /vsnap/vpool1/fs2
tmpfs                3.1G    0  3.1G  0% /run/user/1001
```

When using Operating System commands like `du` or `find` as in our Example 13-8 you could also explore the content of the filesystem to figure out which VM is backed up in which filesystem.

**Example 13-8   Explore the content of a vSnap volume**

```
[serveradmin@t2-spp-vsnap ~]$ du /vsnap/vpool1/fs2
12774239  /vsnap/vpool1/fs2/b97956fe/t2-vm-win.vm-356
12774239  /vsnap/vpool1/fs2/b97956fe
12774240  /vsnap/vpool1/fs2

[serveradmin@t2-spp-vsnap ~]$ find /vsnap/vpool1/fs2
/vsnap/vpool1/fs2
```

Chapter 13. The vSnap CLI  239
As long as the backup job is running we could see a share on the filesystem which is associated with the SLA. The vSnap CLI command `vsnap share show` as shown in Example 13-9 is listing the active share, where the **Volume ID** 2 and the filesystem name `/vsnap/vpool1/fs2` could be identified.

**Example 13-9  Active share**

```
[serveradmin@t2-spp-vsnap ~]$ vsnap share show

<table>
<thead>
<tr>
<th>ID</th>
<th>TYPE</th>
<th>PARENT VOL</th>
<th>PARTNER ID</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>nfs</td>
<td>2</td>
<td>N/A</td>
<td>/vsnap/vpool1/fs2</td>
</tr>
</tbody>
</table>
```

```
[serveradmin@t2-spp-vsnap ~]$ vsnap share show --id 1

ID: 1
NAME: /vsnap/vpool1/fs2
SHARE TYPE: nfs
VOLUME ID: 2
PARTNER ID: N/A
CREATED: 2019-06-18 14:09:12 UTC
UPDATED: 2019-06-18 14:09:33 UTC
SHARE OPTIONS:
ALLOWED HOSTS:
10.0.250.27
READ ONLY: No
```

The share is used to transfer the backup data from the hypervisor, application or database to the vSnap server.

**Note:** For the backup of VMware virtual machines a VADP proxy is required, therefore the backup data is transferred from the hypervisor through the VADP proxy to the vSnap Backup Storage server. The chapter 1.2.4, “VADP proxy server” on page 14 provide details on the VADP proxy.

After the backup is completed, a Snapshot on the filesystem is created, which is the backup entity or the backup version. In Example 13-10 we use the command `vsnap snapshot show` list all snapshots.

**Example 13-10  List available snapshots on the vSnap pool**

```
[serveradmin@t2-spp-vsnap ~]$ vsnap snapshot show

<table>
<thead>
<tr>
<th>ID</th>
<th>PARENT ID</th>
<th>CREATED</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2019-06-18 14:11:53 UTC</td>
<td>spp_1004_2002_2_16b6aee0745</td>
</tr>
</tbody>
</table>
```
The volume where the snapshot is taken from could be identified by the **Parent ID** and the **Parent Name**.

### 13.4.2 Volumes and snapshots for replication data

In this chapter explore what happens on a vSnap Backup Storage server when data is replicated between two vSnap servers. After the configuration for the vSnap replication is completed (refer to 9.3.1, “Configure vSnap Replication”) a replication job could be started.

In our example a vSnap partnership is created between `t2-spp-vsnap` and `t2-spp-vsnap-dr`. When a replication task of an SLA policy is started, the following things happen on the source and target vSnap server:

1. A new replication target volume is created on the target vSnap server.
2. A relationship for the source and target volume is created on the source and target vSnap server.
3. A new and empty snapshot on the target volume is created.
4. A replication session is created on the source vSnap server.
5. The target snapshot is updated on the target vSnap server after the replication session is completed.

In the following replication example we show the previous steps in detail.

As shown in Example 13-11 the replication job creates a target volume (ID 2) on the target vSnap server **t2-spp-vsnap-dr**.

**Example 13-11  Replication target volume is created on the target vSnap server**

```
[serveradmin@t2-spp-vsnap-dr ~] $ vsnap volume show

<table>
<thead>
<tr>
<th>ID</th>
<th>TYPE</th>
<th>POOL</th>
<th>TS CLONE</th>
<th>TOTAL</th>
<th>FREE</th>
<th>USED</th>
<th>NAME</th>
<th>TAGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>filesystem</td>
<td>1</td>
<td>No</td>
<td>100.00GB</td>
<td>84.21GB</td>
<td>12.18GB</td>
<td>vsnap_metadata_cloud</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>filesystem</td>
<td>1</td>
<td>No</td>
<td>100.00GB</td>
<td>84.21GB</td>
<td>12.18GB</td>
<td>spp_16b6b15c8d1_spp_1004_2002_16b6aeb7936__group0_12_</td>
<td>N/A</td>
</tr>
</tbody>
</table>
```

Next the replication relationship between both volumes is configure on both vSnap servers. The vSnap CLI command `vsnap relationship show` is listing these relationships as shown in Example 13-12 for the source vSnap server **t2-spp-vsnap** and in Example 13-13 on page 242 for the target vSnap server **t2-spp-vsnap-dr**.

**Example 13-12  vSnap relationship on the source server created**

```
[serveradmin@t2-spp-vsnap ~] $ vsnap relationship show

<table>
<thead>
<tr>
<th>ID</th>
<th>PARTNER ADDR</th>
<th>PARTNER TYPE</th>
<th>LOCAL ROLE</th>
<th>LAST SYNC</th>
<th>LOCAL VOL</th>
<th>REMOTE VOL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The volume where the snapshot is taken from could be identified by the **Parent ID** and the **Parent Name**.
The fields Partner Address, Local Volume ID, Local Volume Name, Remote Volume ID and Remote Volume Name are used to identify which vSnap servers and volumes are used for this relationship.

A empty Snapshot is created as shown with command vsnap snapshot show in Example 13-14. The details of the snapshot are not yet available using the command vsnap snapshot show --id 1.

Example 13-14  Empty snapshot is created

[serveradmin@t2-spp-vsnap-dr ]$ vsnap snapshot show

Example 13-13  vSnap relationship on the target server created

[serveradmin@t2-spp-vsnap-dr ]$ vsnap relationship show --id 7ce7be815c5f4fc9147c52a55bd6530d

The fields Partner Address, Local Volume ID, Local Volume Name, Remote Volume ID and Remote Volume Name are used to identify which vSnap servers and volumes are used for this relationship.

A empty Snapshot is created as shown with command vsnap snapshot show in Example 13-14. The details of the snapshot are not yet available using the command vsnap snapshot show --id 1.

Example 13-14  Empty snapshot is created

[serveradmin@t2-spp-vsnap-dr ]$ vsnap snapshot show
When the replication is running a session is created for the replication on the source vSnap server. In Example 13-15 the command `vsnap session show` is used to list the replication session on the source server `t2-spp-vsnap`. The status field indicates if it is an **Active** session or a already **Completed** session.

**Example 13-15**  List replication session using the vSnap CLI

```
[serveradmin@t2-spp-vsnap ~]$ vsnap session show
ID | RELATIONSHIP ID | PARTNER TYPE | LOCAL SNAP | REMOTE SNAP | STATUS   | SENT      | STARTED     | ENDED
1  | 7ce7be815c5f4fc9147c52a55bd6530d | vsnap        | 1          | 1           | ACTIVE   | 9.23GB    | 2019-06-18 14:55:26 UTC | N/A
```

```
[serveradmin@t2-spp-vsnap ~]$ vsnap session show --id 1
ID: 1
RELATIONSHIP ID: 7ce7be815c5f4fc9147c52a55bd6530d
PARTNER TYPE: vsnap
REPL ADDRESS: 10.0.250.23
LOCAL SNAP ID: 1
LOCAL SNAP NAME: spp_1004_2002_2_16b6aee0745
REMOTE SNAP ID: 1
REMOTE SNAP NAME: spp_1004_2101_16b6b15c808
PRIORITY: 50
STATUS: ACTIVE
SENT: 9.42GB
QUEUED: 2019-06-18 14:55:20 UTC
ENDED: N/A
MESSAGE: Data transfer in progress
```

```
[serveradmin@t2-spp-vsnap ~]$ vsnap session show --id 1
ID: 1
RELATIONSHIP ID: 7ce7be815c5f4fc9147c52a55bd6530d
PARTNER TYPE: vsnap
REPL ADDRESS: 10.0.250.23
LOCAL SNAP ID: 1
LOCAL SNAP NAME: spp_1004_2002_2_16b6aee0745
REMOTE SNAP ID: 1
REMOTE SNAP NAME: spp_1004_2101_16b6b15c808
PRIORITY: 50
STATUS: COMPLETED
SENT: 12.22GB
QUEUED: 2019-06-18 14:55:20 UTC
ENDED: 2019-06-18 14:57:37 UTC
MESSAGE: Completed
```
After the replication session is completed the snapshot on the target volume is updated and details of the snapshot are available which is listed in Example 13-16 by using the vSnap CLI command `vnap snapshot show`.

**Example 13-16  Snapshot on the replication target is created**

```
[serveradmin@t2-spp-vsnap-dr ~]$ vnap snapshot show
ID | PARENT ID | CREATED                 | NAME
--------------------------------------------------------------------
 1 |         2 | 2019-06-18 14:57:37 UTC | spp_1004_2101_16b6b15c808
```

```
[serveradmin@t2-spp-vsnap-dr ~]$ vnap snapshot show --id 1
ID: 1
NAME: spp_1004_2101_16b6b15c808
PARENT ID: 2
PARENT NAME: spp_16b6b15c8d1_spp_1004_2002_16b6aeb7936__group0_12_
POOL ID: 1
POOL NAME: primary
HAS CLONES: No
USED SPACE: 0.00KB
VERSION ID: 12686594730219022292
CREATED: 2019-06-18 14:57:37 UTC
UPDATED: 2019-06-18 14:57:37 UTC
```

The relationship of the volumes on the source and the target server is updated as shown in Example 13-17 for the source vSnap server and in Example 13-18 for the target vSnap server.

**Example 13-17  vSnap relationship on the source server completed**

```
[serveradmin@t2-spp-vsnap ~]$ vnap relationship show --id 7ce7be815c5f4fc9147c52a55bd6530d
ID: 7ce7be815c5f4fc9147c52a55bd6530d
PARTNER ID: 5345ec9e347b40d5ae63b2397f64c8da
PARTNER TYPE: vnap
PARTNER ADDR: t2-spp-vsnap-dr
LOCAL ROLE: primary
LOCAL POOL ID: 1
LOCAL VOL ID: 2
LOCAL VOL NAME: spp_1004_2002_16b6aeb7936__group0_12_
REMOTE POOL ID: 1
REMOTE VOL ID: 2
REMOTE VOL NAME: spp_16b6b15c8d1_spp_1004_2002_16b6aeb7936__group0_12_
LAST SYNC STATUS: COMPLETED
LAST SYCNED SNAP ID: 1
LAST ATTEMPT SNAP ID: 1
```

**Example 13-18  vSnap relationship on the target server completed**

```
[serveradmin@t2-spp-vsnap-dr ~]$ vnap relationship show --id 7ce7be815c5f4fc9147c52a55bd6530d
ID: 7ce7be815c5f4fc9147c52a55bd6530d
PARTNER ID: bc1c6c4052a744ad86bdc25625e2c516
```
PARTNER TYPE: vsnap
PARTNER ADDR: t2-spp-vsnap
LOCAL ROLE: replica
LOCAL POOL ID: 1
LOCAL VOL ID: 2
LOCAL VOL NAME: spp_16b6b15c8d1_spp_1004_2002_16b6aeb7936__group0_12_
REMOTE POOL ID: 1
REMOTE VOL ID: 2
REMOTE VOL NAME: spp_1004_2002_16b6aeb7936__group0_12_
LAST SYNC STATUS: COMPLETED
LAST SYCNED SNAP ID: 1
LAST ATTEMPT SNAP ID: 1

The fields LAST SYNC STATUS, LAST SYCNED SNAP ID, LAST ATTEMPT SNAP ID in both detailed outputs provide details about the completion status and the snapshots used for this relationship. Note, that the timestamps in the CREATED and UPDATED field are not adjusted, they remain on the values when the relationship was initially created.
Chapter 14. REST API

This chapter provides an introduction into the REST APIs and how IBM Spectrum Protect Plus leverages this technology. Further we demonstrate the REST API documentation and how users can discover and use the API for monitoring, configuration and administration tasks. We will show how to discover API calls and its parameters in order to build a customized Python script for user initiated backups of a single virtual machine from command line via REST API services. Finally we introduce the utility `sppclient` which is a Python module to encapsulate REST API complexity and reuses code for reoccurring tasks. `sppclient` comes with a set of more than 20 Python scripts demonstrating how to realize workflows with REST instead of using the GUI.
14.1 REST API Overview

A REST application programming interface (API) enables client applications to access and manage resources on a server by sending requests and receiving responses using the Hypertext Transfer Protocol (HTTP) or HTTPS protocol. The IBM Spectrum Protect Plus Representational State Transfer (REST) API provide access to the product resources via so called endpoints and enables other applications to interact with the product by sending requests and receiving responses via the HTTP or HTTPS protocols. You can extend the capabilities of the IBM Spectrum Protect Plus application by developing scripts that utilize the API. In general REST APIs are sharing the following characteristics:

- RESTful systems use stateless protocols. That means the server does not hold any record of previous interactions with clients. Every client request and interaction needs to be handled based entirely on information that comes from the client.
- Stateless components can be easily re-deployed after failures occurred and can be started.
- RESTful APIs are very popular in Web deployments as well as in Cloud computing and micro services. RESTful APIs scale out well as they can be started, stopped and restarted easily when needed as they do not need to preserve any client data or session states.
- RESTful clients send requests to a resource’s URI and expects a response i.e. in HTML, XML, JSON. While there are several response formats JSON is the most widely adopted format. IBM Spectrum Protect Plus is using the JSON format for requests and responses over HTTP.
- Available REST operations for HTTP are GET, HEAD, POST, PUT, PATCH, DELETE, CONNECT, OPTIONS and TRACE. IBM Spectrum Protect uses the four operations highlighted in bold.

An example how a REST application programming interface (API) enables client applications is shown in Figure 14-1. The figure demonstrates how to access and manage resources on a server by sending requests and receiving responses using the HTTP or HTTPS protocols.

14.2 IBM Spectrum Protect Plus REST API

IBM Spectrum Protect Plus uses a RESTful API to handle communication between the front end (GUI) and the application server itself. This API can be also leveraged by other client application to realize tasks such as automation, integration, configuration and data collection. By leveraging the REST API IBM Spectrum Protect Plus is able to integrate with automation tools like Jenkins, Puppet, and others. Furthermore any programming language which is capable of making REST calls can be used (e.g. Python, JavaScript, PowerShell, and others). The necessity to have a deeper look at the REST API mostly becomes a hot topic when the Spectrum Protect Plus Environment is scaling out. When tasks are re-occurring frequently a administrator may want to automate these tasks and perform them in scripts or via command line.
Reasons why the GUI may not be always the perfect fit for every client need may be:

- Increasing number of Hypervisors and VMs to configure and protect
- Amount and variety of applications
- Quantity of VSNAPs and VADPs
- The need to check in an automated way the SLAs status, i.e. if it failed, if it ended partial or completed successful
- Monitoring the SPP environment in terms of resource utilization (capacity, CPU, RAM, SNAP capacity), job logs and warnings or error messages

### 14.2.1 REST API documentation

As of today there are two REST API related documentations published. The first one is the IBM Spectrum Protect Plus Version 10.1.1 REST API Developer Guide. The REST API PDF describes the essentials of REST. It provides guidance to session handling and four basic HTTP methods for applications to interact with: GET, POST, PUT, and DELETE. Further it contains several RESTful API examples that demonstrate interaction, basic functions such as retrieving a session ID, assigning a VM, and starting a job.

Secondly, the most recent and up-to-date documentation is the Swagger UI Tool. Starting in IBM Spectrum Protect Plus version 10.1.3 the Swagger UI Tool has been integrated into the GUI for interaction with the API and can be launched from the drop-down menu in the upper right corner in the GUI. Swagger is an open-source framework with tools to develop, build, document and query REST APIs. The figure to the right shows where to launch the Swagger UI tool. The Swagger UI covers the endpoints (URIs) as well as the JSON format of GET, PUT, POST, and DELETE requests and the corresponding responses.

The API endpoints are arranged in categories and for each endpoint the operations one may want to perform are listed. An example for available operations for the API endpoint `site` is shown in Figure 14-2 on page 250. The REST API provides additional API endpoints which are not yet documented in the Swagger UI tool.
We cover the process to identify additional endpoints in 14.4.2, “Trace GUI REST operations with Firefox browser” on page 260.

Figure 14-2 IBM Spectrum Protect Plus REST API Documentation with Swagger UI

API Categories

IBM Spectrum Protect Plus API Documentation

API operations on endpoint: /api/site

14.3 Discovering the REST API

This section demonstrates various methods to query the REST API. As the Swagger UI tool does not yet document all available API endpoints nor is it very convenient for complex operations we demonstrate different methods to achieve the same or similar tasks. As a pre-requisite for the different methods we suggest to use the following or similar tools:

- Firefox browser with an additional browser extension called RESTclient (https://addons.mozilla.org/en-GB/firefox/addon/restclient)
- curl and additionally the tool jq. jq is a lightweight and flexible command-line JSON processor (https://stedolan.github.io/jq) which provides formatting, filtering, mapping and transformation functions
- Python 3.x for the operating system of your choice. The sppclient modules are written in Python language and require additional modules and the Python interpreter itself in version 3 or higher.

During exploration of the REST API endpoint called site we demonstrate the use of several different methods. However all methods are following the sequence depicted in Figure 14-3 on page 251. In the first step the client utility (e.g. Swagger UI, curl, Python libraries) connects to the API and transmits username and password in a HTTP header. In case of valid credentials the API responds with a unique authentication token. The IBM Spectrum Protect Plus API expects a authentication token as the sessionid attribute in all further API requests.
In step 2) the client is performing a POST and in step 3) the client is performing a GET operation on the API endpoint \textit{site}. While a GET operation will only retrieve information from the API with no changes at all a POST or PUT operation will create or update information via the endpoint with data which needs to be specified in the request body. In step 2, 3 and 4 the \textit{sessionid} is used as authentication token. Step 4) is the final step to terminate the session and invalidate the authentication token.

![REST API call to endpoint site, including request of authentication token](image)

On the following pages we demonstrate how to realize the sequence in Figure 14-3 with three different methods:

- CURL
- Swagger UI tool
- Firefox RESTclient

### 14.3.1 CURL

We demonstrate which steps are required to realize the sequence depicted in Figure 14-3 with the command line utility curl and jq. This simple example demonstrates the usage of the REST operations POST, GET and DELETE.

**Login and retrieve a sessionid**

The initial step is to establish a connection to the API and pass a username and password in the HTTP header. This POST operation is sent to the API endpoint \texttt{/api/endeavour/session}. In case of successful authentication the HTTP status code equals to 200 and the response is in JSON format. An excerpt of the JSON response message is shown in Example 14-1. The most important information from this response is the value of the key \textit{sessionid}. 
This authentication token is used for further communication with the API until the token expires or the user has invalidated the token by sending a DELETE command to the endpoint. The response message contains information related to the user account and so called Hypermedia as the Engine of Application State (HATEOAS) components. HATEOAS is a component of a REST architecture which enables the client to interact with the server and discover information dynamically though hypermedia or response links.

This means the client does not require up front knowledge of methods of resource interaction. Example 14-1 shows such response links to change a users password (see changePassword response link in Example 14-2). The response from the API endpoint contains additional links or API endpoints that are related to session or user management.

Example 14-1  Retrieve login information with sessionid from the API with curl (truncated)

```
command: curl -sS -k -X POST -H 'Accept:application/json' -H 'Content-type:application/json' --user
          "restapiuser:pass4AP!" https://spphost/api/endeavour/session

response: { "sessionid": "96531d8d345c417aa7d47b4179ecc03a", "user": { "links": { "self": { "rel": "self", "href": "https://spphost/api/security/user/1001" }, "up": { "rel": "up", "href": "https://spphost/api/security/user" }, "changeMetadata": { "rel": "action", "href": "https://spphost/api/endeavour/session/metadata/NATIVE_USER:1:restapiuser?action=changeMetadata" }, "changePassword": { "rel": "action", "href": "https://spphost/api/security/user/1001?action=changePassword" } }, "name": "restapiuser", "type": "NATIVE_USER", "typeDisplayName": "Native User", "tenantId": 1, "loginCount": 74, "lastLogin": 1561473242064, "failedLogin": 0, ...
```

In addition to the previous example we are using the Python module `json.tool` to format the JSON response and transform it from a single line string into a formatted output with indents and key-value pairs per line.

Example 14-2  Retrieve a sessionid from the API with curl and Python pretty-print formatting

```
command: curl -sS -k -X POST -H 'Accept:application/json' -H 'Content-type:application/json' --user
          "restapiuser:pass4AP!" https://spphost/api/endeavour/session | python -m json.tool

response:

```
```
For advanced JSON parsing, filtering and transformations of the JSON responses, we recommend the tool **jq** ([https://stedolan.github.io/jq](https://stedolan.github.io/jq)). The **jq** tool is a flexible command-line JSON processor and provides powerful options to extract values from the JSON responses. If you simply pipe the JSON output to the **jq** tool (Example 14-3) the output will be formatted nicely similar to the pretty-print function of the **json.tool** Python module.

**Example 14-3  Retrieve a sessionid from the API with curl and JQ for pretty-print formatting**

```bash
result: the formatted result looks almost identical to the output of the Python formatting
```

The **jq** tool provides functions beyond the pretty print formatting. It provides additional functions like customized formatting, key value transformations, calculations and filtering. A simple filter on the key `sessionid` is used in Example 14-4 to display only the value of the desired attribute which will be reused for further authentication.

**Example 14-4  Retrieve a sessionid from the API with curl and JQ for pretty-print formatting and filtering**

```bash
response: 49531dd8d345c417aa7d47b4179ecc03a
```

**List and create new site**

As a first example we create an additional site via the REST API. Therefore we specify the `sessionid` within the HTTP header and use the POST operation. Additionally we need to specify the site information with the `data` parameter (either `-d` or `--data`). In Example 14-5 we specify values for the properties `name`, `description` and `defaultSite`. In addition we declare the parameters `-iL` to include the HTTP response status code in the curl output.

**Note:** When specifying the parameters `-iL` then piping curl output to the **jq** tool fails. The additional parameters are modifying the output in a way that it is not only a JSON formatted string and thus the **jq** tool can not parse and format the output anymore. Therefore we specify the parameters `-iL` for demonstration purposes during dedicated examples where i.e. we need to check the HTTP response code.

**Example 14-5  Create a new site via REST command**

```bash
command: curl -iL -sS -k -X POST -H 'Accept:application/json' -H 'Content-type:application/json' -H 'x-endeavour-sessionid:49531dd8d345c417aa7d47b4179ecc03a' https://spphost/api/site -d '{"name" : "REST_site",  "description":"site created via REST",  "defaultSite":"false"}'
response:
HTTP/1.1 201
X-Application-Context: zuul:443
Date: Fri, 28 Jun 2019 11:33:18 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked

```

i.e. response status code 201 indicates that a new resource has been created successfully.
To confirm that the site creation was successful execute a GET operation on the site endpoint, as shown in Example 14-6.

**Example 14-6  Query sites via REST command**

```
command: curl -sS -k -X GET -H 'Accept:application/json' -H 'Content-type:application/json' -H 'x-endeavour-sessionid:49531dd8345c417aa7d47b4179ecc03a' https://spphost/api/site | jq -c '.sites[] | { name, id, description, defaultSite}'
```

```
output:
   
   { "name": "Secondary", "id": "2000", "description": "secondary site", "defaultSite": false }
   { "name": "Primary", "id": "1000", "description": "Primary Site", "defaultSite": true }
   { "name": "Demo", "id": "3000", "description": "Demo site", "defaultSite": false }
   { "name": "REST_site", "id": "3106", "description": "site created by REST command", "defaultSite": false }
```

A site can be deleted via REST command without any confirmation, as shown in Example 14-7. The response status code 204 indicated that the resource has been deleted successfully. The API method DELETE is executed on endpoint /api/site/siteid whereas the siteid needs to be replaced by the integer value of the corresponding site, i.e. 3106 for the site which was created via REST API.

**Example 14-7  Delete a site via REST command**

```
```

```
response:
   
   HTTP/1.1 204
   X-Application-Context: zuul:443
   Date: Fri, 28 Jun 2019 11:07:48 GMT
```

**Deleting the session**

When the user has completed the desired tasks it is recommended to invalidate the session by sending a DELETE request to the session endpoint, as shown in Example 14-8. This is comparable to gracefully logout from the GUI. This is not a hard requirement and a login with the same user credentials will return a new sessionid regardless if the user has gracefully logged out previously.

**Example 14-8  Delete the authentication token (sessionid=**

```
command: curl -IL -sS -k -X DELETE -H 'Accept:application/json' -H 'Content-type:application/json' -H 'x-endeavour-sessionid:49531dd8345c417aa7d47b4179ecc03a' https://spphost/api/endeavour/session
```

```
response:
   
   HTTP/1.1 204
   X-Application-Context: zuul:443
   Date: Fri, 28 Jun 2019 11:39:19 GMT
```

**14.3.2 Swagger UI**

The Swagger UI tool has been introduced into the IBM Spectrum Protect Plus GUI as a source of documentation of the REST API capabilities. The advantage of the Swagger UI Tool compared to curl or RESTclient is the fact that the session is handled transparently for the user who is logged into the graphical user interface. The user does not need to handle the retrieval or deletion of the sessionid. However the Swagger UI (in the current configuration) does not form complete curl commands based on the users input in the web forms.
This differentiates the Swagger UI Tool from other tools like RESTclient. Similar to Example 14-5 on page 253 a site can be created via the Swagger UI as well. The API endpoint documentation lists the parameters with their name and type, i.e. name, description, defaultSite, throttles and schedules. Beside this kind of declaration there is no further documentation about the endpoint parameters. In Figure 14-4 we create a sample site with Swagger UI Tool. In the body field we enter the following JSON formatted text, as shown in Example 14-9.

**Example 14-9  JSON formatted string to be entered into the HTTP body field**

```
{ "name":"REST_Swagger", "defaultSite":"false", "description":"site created with Swagger UI" }
```

![Figure 14-4  Example to create a site with Swagger UI](image)

### 14.3.3 Firefox RESTclient

We will demonstrate how to realize the steps to retrieve a sessionid and create a new site with the Firefox browser plug-in “RESTclient”. The advantage over curl is that you can reuse frequently used queries and headers. The RESTclient will generate the HTTP request based on several building blocks, such as Authentication header, Content type header, and so on. If you have installed the RESTclient plug-in you can launch the tool within the browser by clicking the icon .
Prepare the RESTclient
When you launch the plug-in the first time you need to specify the IBM Spectrum Protect Plus user credentials to form a base64 encoded authentication. To do so select Authentication → Basic Authentication, as shown in Figure 14-5.

![Figure 14-5 Create basic authentication](image)

Then define the headers shown in Figure 14-6 to specify the type of accepted responses from the server and the message format for request from the client to the server (Content-Type).

![Figure 14-6 Request headers](image)

Retrieve a sessionid
To retrieve a sessionid via RESTclient select the operation POST, enter the URI of the session endpoint, i.e. https://spphostname/api/endeavour/session and click send to submit the request to the IBM Spectrum Protect Plus Server. The RESTclient is displaying the response status code of 200 which indicated that the POST operation was successful. Further the corresponding curl command is generated at the bottom of the browser window (see Figure 14-7 on page 257).
Select the Preview tab in the Response section to view the formatted JSON response from the API. The response itself contains many session and user related information from which we are only interested in the sessionid key-value pair which is highlighted in Figure 14-8.

Copy the value of sessionid attribute and create an additional header which is called x-endavour-sessionid and paste the value of the previous retrieved sessionid as pictured in Figure 14-9 on page 258.
Create a site with RESTclient

Analogical to Example 14-5 on page 253, we create a site via the RESTclient. In the body field we enter the following JSON formatted text shown in Example 14-10.

Example 14-10  JSON formatted string for HTTP body

```json
{
  "name": "RESTclient",
  "defaultSite": "false",
  "description": "site created with RESTclient"
}
```

The RESTclient displays the response status code 201 (created successfully) and the curl command at the bottom of Figure 14-10, which will accomplish the same.

![Figure 14-9  RESTclient: create request header x-endeavour-sessionid](image)

![Figure 14-10  Create a new site via RESTclient](image)
14.4 Use Case: initiate backup of VMs via REST API with Python

This section describes the use case to initiate VM backup.

14.4.1 Motivation

A client might want to initiate a backup of a single VM or a subset of available VMs but not all virtual machines assigned to a certain SLA. This can be achieved either using the GUI and selecting the desired VMs or by executing an appropriate REST operation. There are several use cases where a REST API driven backup may be useful:

- Usage of the GUI is not an option due to huge amount of hypervisors and VMs which results in time consuming GUI operations
- An immediate required backup is a frequently occurring task
- A backup of a VM is part of a customized and automated deployment workflow, i.e. a new VM is created via the hypervisors REST API or other deployment techniques, then it is added to a SLA at the Spectrum Protect Plus Server via scripts / REST operations. Users may want to create a backup and potentially a test restore or clone immediately as part of their deployment process.

Based on clients requirement we like to demonstrate how to identify the required steps to trigger an immediate VM backup via REST commands. As the flow chart in Figure 14-11 on page 260 outlines that there are mainly two options to identify the REST endpoints / URIs, the appropriate methods and input and return values:

1. The API endpoints are either described in the API developer guide(https://www.ibm.com/support/knowledgecenter/SSNQFQ_10.1.1/spp/SPP_APIGuide.pdf) or in the Swagger UI tool. At the time if this writing the Swagger UI tool does not cover endpoints and the in-/output formats for such operation.

2. The IBM Spectrum Protect Plus GUI is communicating to the back-end server via REST calls (client side initiated) we are able to monitor the network traffic within the browser. This is where a browsers development function comes handy. Most modern browsers are providing such functions. Firefox calls them web developer function (CTRL + SHIFT + E), Chrome provides the inspect (CTRL + SHIFT + I) function and with Microsoft Edge you can launch More Tools → Developer tools (F12).

As we will demonstrate in the following paragraph the browser inspect method is quite handy as it helps to identify not only the desired API endpoint but also real information about action, input parameters and their values as well as the API response status codes and API request responses in JSON format.
14.4.2 Trace GUI REST operations with Firefox browser

In this use case preparation we use the Firefox built-in web development function to trace the network traffic which is generated by the IBM Spectrum Protect Plus Web GUI. The Spectrum Protect Plus GUI itself is executing REST API operations to the Spectrum Protect Plus server and is populating the user interface with the required information based on the response. The web developer function can be launched from the menu Tools → Web Developer → Network (keyboard shortcut CTRL + SHIFT + E).

After the network monitoring tool is started switch back to the Spectrum Protect Plus GUI and start a backup job for one or two VMs without executing the whole SLA which would backup all assigned VMs and not only a subset. Under the menu Manage Protection → Hypervisors → VMware choose the desired vCenter and select the vm(s) of your choice. Before you hit the Run button switch to the Web developer window and clear the content.

For ease of debugging it is recommended to switch from the GUI back to the Network monitoring window immediately after the Backup Run has been initiated in order to pause the network monitoring. In Figure 14-12 the three functions are highlighted in red: clear, pause network recording and the Network tab. After the backup has been initiated from the GUI the Networking monitoring window shows one or more entries whereas we are interested in the line with the API operation to the request URL /ngp/hypervisor?action=adhoc.
When the specific line is selected more details can be obtained from the Header tab (Example 14-11) and the Params tab (Example 14-12).

**Example 14-11  Header Tab shows the API operation POST and the API request URL**

| Request URL:https://spphost/ngp/hypervisor?action=adhoc |
| Request method:POST |

From Example 14-11 we identified the required action (POST) and the request URL. From Example 14-12 we figure out the parameter names and their values which we need to pass along with a API request within the request body (Swagger UI) also referred as data (curl) or Payload (Firefox). While slaPolicyName (i.e. Gold, Silver, Bronze, ...) and subtype (either vmware or hyperv) are self-explaining the resource parameter is an array of one or more custom-build URLs, one for each VM to be backed up.

**Example 14-12  Params Tab shows the request payload**

```
{ "slaPolicyName"="Silver", "subtype"="vmware", "resource":["https://spphost/api/hypervisor/1001/vm/1bebb2a3857d152c364c67579be380c?from=hlo"] }
```

![Figure 14-12  web developer function to inspect network traffic](image)

With the gathered information from the Header and the params tab we can summarize the required information for a REST based backup command to the information shown in Figure 14-13 on page 262. In addition to the API url and the method we identified that we need to pass additional information along with the API operation POST as data. This information can be captured during tracing of the network traffic with the web developer (Figure 14-12).

The more complex resource parameters are build upon the API endpoint which includes the hypervisor id and the unique id of the VM:

https://spphost/api/hypervisor/hypervisorId/vm/vmID?from=hlo

The Swagger UI tool provides the documentation for the required API GET operations to retrieve a list of all configured hypervisors and subsequently an endpoint which lists all registered virtual machines for a specific hypervisor id. Figure 14-13 on page 262 lists these endpoints. Figure 14-13 on page 262 summarized the required information from the browser inspection (Figure 14-12) process and the available API documentation in the Swagger UI tool.

The trace showed for the example on ad hoc backup that the resource URI includes the hypervisor id and the VM unique ID. This becomes important during the development of the sample script as the programmer needs to identify this information step by step.
In the following paragraph we will demonstrate the basic steps to implement a Python script which triggers a VM backup. The example does not re-use functions of the sppclient Python package but uses the native request library. The code does not implement command line parsing for input parameters such as vmnames to be backed up.

Further exception handling is out of scope of the following example although exception handling, logging and parameterization of such a script is highly recommended and would be part of a real implementation in most cases. For the sake of ease we stick to the very basics of the required steps and split it into pieces and define functions:

- To login to the API with username & credentials and retrieve a sessionid
- Logout and invalidate the sessionid
- To retrieve (GET) information from the API by specifying an endpoint
- To create a list of all registered hypervisors
- To create a list of all virtual machines for a specific hypervisor
- For initiating a backup of a list of VMs

**Outlook:** in a productive implementation of such a Python script the user may want to specify a list of VMs by their name(s) instead of using their unique id or pass a comma-separated-value list of VMs to the script. The programmer needs to retrieve a list of hypervisors, then retrieve all VMs of each hypervisor and iterate through the list of objects (list of VMs) to finally find the desired VM by it’s name. From hereon it is possible to use the objects vmid to build the resource string.

These additional steps will make such script much more comfortable and dynamically usable but as we are intending to introduce the basic steps to achieve a task over the introduction of Python programming techniques we are keeping the functions as simple as possible.
14.4.3 Python code explained

For the sake of clarity we split the script into smaller pieces and comment parts of the code briefly. In our Python script we require several external modules which needs to be imported. The most important one is the request module which is required to send HTTP requests to the Spectrum Protect Plus API. After importing modules we create a authentication token of type HTTPBasicAuth from username and password which is sent to the API in order to retrieve a sessionid.

While the login function in Example 14-13 is responsible to retrieve the sessionid via a PUT request operation the function logout in Example 14-14 on page 264 will invalidate the sessionid by sending a DELETE operation to the API URL /api/endeavour/session. The sessionid and its value will be reused as parameter in HTTP headers throughout this script until the session is terminated at the end of the script. Each request returns a request status code which can be evaluated to determine if the operation was carried out as expected.

Example 14-13  Login function - POST operation

```python
import requests
import getpass
from requests.auth import HTTPBasicAuth
import urllib3
import sys

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

username  = 'restapiuser'
password  = getpass.getpass()
host      = "https://spphost:443/"
session   = requests.Session()

def login():
    authToken = HTTPBasicAuth(username, password)
    endpoint  = "/api/endeavour/session"
    url       = host + endpoint

    requestHeaders = {'Accept' : 'application/json', 'Content-type' : 'application/json'}
    response      = session.post(url, headers=requestHeaders, auth=authToken, verify=False)
    responseJson  = response.json()
    responseCode  = response.status_code

    sessionid     = responseJson['sessionid']

    if (responseCode != 200):
        print("request not successfull. responseCode: " + responseCode)
        sys.exit(1)
    else:
        return sessionid
```

While the login function Example 14-13 expects a return value of 200 for a successful authentication the logout function Example 14-14 on page 264 is expecting a response return code of 204 for successful DELETE operation. For a list of REST API response codes check 14.6, “API response code” on page 272.
Example 14-14  Logout function - DELETE operation

```python
def logout(sessionid):
    url = host + "api/endeavour/session"
    requestHeaders = {'Accept': 'application/json', 'Content-type': 'application/json'}
    requestHeaders.update({'X-Endeavour-Sessionid': sessionid})
    response = session.delete(url, headers=requestHeaders, verify=False)
    responseCode = response.status_code
    if (responseCode != 204):
        print("request not successful. responseCode: " + str(responseCode))
        sys.exit(1)
    else:
        print("Logout successful")
```

In order to query information from the API the function `query_endpoint` is updating the header with the new `sessionid` so that the specification of username and password no longer required. Further the function is sending a request GET command to the specified `url1`. The function `listHypervisors` in Example 14-15 is querying the API for a list of hypervisors and is evaluating the response. The response contains the response status code and the response to the request in JSON format.

In case the `response.status_code` returns 200 for a successful operation the JSON response is stored in the variable `responseJson`. With Python we can easily access the Objects and variables by referencing them by their name. From a query of the endpoint `/api/hypervisor` within Swagger UI tool or curl we have identified the structure of the returned JSON starting and figured out that the response contains an array called `hypervisors` which can be directly access with `hypervisorList=responseJson['hypervisors']`. Inside the loop for each hypervisor one line is printed out with only selected attributes, here the `id` and the `name`.

Example 14-15  Code: function to query hypervisors

```python
def query_endpoint(sessionid, endpoint):
    url = host + endpoint
    print("endpoint to query: " + url)
    requestHeaders = {'Accept': 'application/json', 'Content-type': 'application/json'}
    requestHeaders.update({'X-Endeavour-Sessionid': sessionid})
    return session.get(url, headers=requestHeaders, verify=False)

def listHypervisors(sessionid):
    endpoint = "/api/hypervisor"
    response = query_endpoint(sessionid, endpoint)
    if response.status_code == 200:
        hypervisor_fmt = " {:<5.5s} | {:<30.30s}"
        print(hypervisor_fmt.format("ID", "Hypervisor Name"))
        print("-
```

After the first functions are defined we call the functions from the main function (Example 14-16). We will modify the main function while the script capabilities expand.

Example 14-16  Add main function and sample code to retrieve all registered Hypervisors

```python
def main():
    sessionid = login()
    listHypervisors(sessionid)
    logout(sessionid)
    if __name__ == "__main__":
        main()
```

264  IBM Spectrum Protect Plus Practical Guidance
When the script is started the user is prompted to provide the user password. The username `restapiuser` and the server hostname `spphost` is hard coded in this script. The function from Example 14-15 on page 264 generates the list in Example 14-17. In a later step, we will reuse a hypervisor’s ID to retrieve a list of all VMs registered to the hypervisor.

**Example 14-17  Output of configured hypervisors**

```python
py listHypervisors.py
Password: *********

<table>
<thead>
<tr>
<th>ID</th>
<th>Hypervisor Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001</td>
<td>vcenter-b.escc.workshop</td>
</tr>
<tr>
<td>1002</td>
<td>vcenter-a.escc.workshop</td>
</tr>
<tr>
<td>1003</td>
<td>vcenter-c.escc.workshop</td>
</tr>
</tbody>
</table>

Logout successful
```

To get a list of VMs for a specified hypervisor (by ID) a new endpoint URL is created. In Example 14-18 we will query hypervisor `vcenter-b.escc.workshop` which results in the API URL: `/api/hypervisor/1001/vm`.

**Example 14-18  Python code: query VMs by hypervisor id**

```python
def listVMs(sessionid, hypervisorID):
    endpoint = '/api/hypervisor/' + str(hypervisorID) + '/vm'
    response = query_endpoint(sessionid, endpoint)
    responseCode = response.status_code
    responseJson = response.json()
    print()
    vmlist_fmt = ' {:<33.33s} | {:<20.20s} | {:<5s}'
    print(vmlist_fmt.format('VM ID', 'VM Name', 'Hypervisor ID'))
    print('-' * 60)
    for vm in responseJson['vms']:
        print(vmlist_fmt.format(vm['id'], vm['name'], str(vm['hypervisorManagementServerID'])))
```

With the function parameters `sessionid` and `hypervisorID=1001` the list shown in Example 14-19 is generated from the function `listVMs`.

**Example 14-19  List of VMs by Hypervisor (ID=1001)**

<table>
<thead>
<tr>
<th>VM ID</th>
<th>VM Name</th>
<th>Hypervisor ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>d332c4589e65335be1909538f25a7363a</td>
<td>t4-vm-sql-template</td>
<td>1001</td>
</tr>
<tr>
<td>d42a2a2a870b944c16b13753598d4a05</td>
<td>t4-vm-lx-template</td>
<td>1001</td>
</tr>
<tr>
<td>1bebb22a3857d152c364c67579be380c</td>
<td>t4-vm-win-skln</td>
<td>1001</td>
</tr>
<tr>
<td>a25b9e25c02b3b9d9d060ce4f1f14fffd</td>
<td>t4-vm-gmt-win</td>
<td>1001</td>
</tr>
</tbody>
</table>

In Example 14-20 on page 266 we define the function `startBackup` where we specify the endpoint to trigger the backup `/ngp/hypervisor?action=adhoc` and create the additional parameters which needs to be specified as data of the HTTP POST operation. From the earlier GUI debugging we identified the required parameters (Figure 14-13 on page 262). The most complex part is the definition of the resource array which contains one or more API URLs, one for each VM to be backed up.

Each resource element is build form the API endpoint for hypervisors plus the hypervisor ID and the VM id, followed by the HTTP parameter `?from=hlo`. There are two primary catalogs we can search through in SPP `recovery` and `hlo`. `Recovery` shows resources that have already been backed up and are available for restore. The `hlo` category lists resources that have been inventoried from various registered providers. An example of a valid resource based on the earlier exampled would be:

`https://spphost/api/hypervisor/1001/vm/1bebb22a3857d152c364c67579be380c?from=hlo`
**Example 14-20  Python code to initiate a vm backup**

```python
def startBackup(sessionid, subtype, slaPolicyName, vmsToBackup):
    endpoint = "/ngp/hypervisor?action=adhoc"
    url = host + endpoint
    resource = []
    requestHeaders = {'Accept': 'application/json', 'Content-type': 'application/json'}
    requestHeaders.update({'X-Endeavour-Sessionid': sessionid})
    for vm in vmsToBackup:
        vmresource = 'https://10.0.250.41/api/hypervisor/' + vm['hypervisorId'] + "/vm/" + vm['vmid'] + "?from=hlo"
        resource.append(vmresource)
        reqData = json.dumps({'subtype': subtype, 'slaPolicyName': slaPolicyName, 'resource': resource})
        print(reqData)
        response = session.post(url, headers=requestHeaders, data=reqData, verify=False)
        responseCode = response.status_code
        responseJson = response.json()
        print("response status code:" + str(responseCode))
        if(responseCode != 200):
            print("response JSON:" + json.dumps(responseJson))
```

Finally we update the main function, declare the list `vmsToBackup` and add two JSON dictionaries to the list with the properties `vmid`, `hypervisorid`, and `subtype`, as shown in Example 14-21. This list is passed to the function `startBackup` and there the resource list with the API URLs is created.

**Example 14-21  Python code - updated main function with list of VMs to backup**

```python
def main():
    sessionid = login()
    #listHypervisors(sessionid)
    #listVMs(sessionid, 1001)
    vmsToBackup = []
    vmsToBackup.append({'vmid': '1bebb22a3857d152c364c67579be380c', 'hypervisorId': '1001', 'subtype': 'vmware'} )
    vmsToBackup.append({'vmid': 'a25b9e25c4b3b94d0cfe4ff514fdd', 'hypervisorId': '1001', 'subtype': 'hyperv'})
    startBackup(sessionid=sessionid, subtype="vmware", slaPolicyName="Silver", vmsToBackup=vmsToBackup)
    logout(sessionid)
```

After execution of Example 14-21 the output will look similar to the output shown in Example 14-22. Note that the script has run twice. While the first run was successful the second run failed with `status_code` 404 as there is still a SLA Policy of the same type (Silver) running. Only one job per SLA can be started at the same time.

**Example 14-22  Output of backup REST command**

```python
py backupVM.py
{'"subtype": "vmware", "slaPolicyName": "Silver", "resource": ["https://10.0.250.41/api/hypervisor/1001/vm/1bebb22a3857d152c364c67579be380c?from=hlo", 
"https://10.0.250.41/api/hypervisor/1001/vm/d42842a87ba64c15b13f535986a240a5?from=hlo"]}
response status code:200 --> OK
Logout successful
```

```python
py backupVM.py
{'"subtype": "vmware", "slaPolicyName": "Silver", "resource": ["https://10.0.250.41/api/hypervisor/1001/vm/1bebb22a3857d152c364c67579be380c?from=hlo", 
"https://10.0.250.41/api/hypervisor/1001/vm/d42842a87ba64c15b13f535986a240a5?from=hlo"]}
response JSON:{"statuscode": 404, "response": {"rc": "Failed to run an already running SLA Policy \"Silver\""}}
Logout successful
```
14.5 The sppclient: a Python library for REST operations

The **sppclient** is a Python project provided by the Spectrum Protect Plus development team. It can be obtained from Github (https://github.com/sppautomation/sppclient). The client is provided AS-IS without guarantee to run and with no support. The project is a collection of scripts as part of the module **sppclient** with more than 20 examples for SPP REST API scripts written in Python. The integration of the sppclient ease interaction with SPP’s REST API and is intended for testing, monitoring and automation. The module is registered in the **Python Package Index (PyPI)** and can be installed with all additional module requirements with the command: `pip install sppclient`

For various aspects in the day-to-day business of using Spectrum Protect Plus the REST API could be helpful to simplify and automate repeating tasks and monitoring activities. The sppclient project is a convenient and easy way forward to implement script-based solutions for Spectrum Protect Plus.

The latest versions of the sppclient and the samples can be obtained from Github: https://github.com/sppautomation/sppclient

While we have demonstrated a simple Python implementation to run vm backups with native Python commands and no logging or exception handling there is script available (vmwareadhocbackup.py) under the sample section of the Git repository. This script is basically realizing the same as the use case implementation from chapter 14.4.3, “Python code explained” on page 263 but adding additional capabilities such as wrapper functions of the sppclient module, logging and command line parameter parsing.

**Note:** the **sppclient** with it’s sample scripts is provided as-is without support or guarantee to run error free. The **sppclient** has been provided for demonstration purposes of REST API capabilities with Python and is neither an official IBM tool nor is the development of additional scripts part of any roadmap. The **sppclient** and the sample scripts are build by users, testers and developers to fulfill their needs for testing and monitoring. Feel free to contribute to the project if you have developed your own solutions based on the **sppclient** module but do not expect active issue tracking, development or bug fixing.

14.5.1 The sppclient scripts - general usage information

All scripts are providing a list of valid parameters (`--help`) and at minimum expecting the parameters `--host`, `--user` and `--pass` whereas the host shall be defined with either the IP address or the fully qualified hostname which is also resolvable from the Spectrum Protect Plus server itself. Specify the format of the hostname with https protocol and the port number, i.g. https://t4-spp-server.workshop.escc

14.5.2 The sppclient script overview and selected examples

As mentioned earlier in this chapter the number of examples is growing and is subject to change. Therefore this section is not intended to be a comprehensive reference for all samples with in- and output data. We will attach a list of script names while we introduce a subset of the list (highlighted in bold) with some more details. Most of the scripts are self-explaining by their script name or do include a tiny help section which describes the purpose of the script.
The following sample scripts have been implemented and made available in the Github repository:

- `appassigntosla.py`
- `createslapolicy.py`
- `deletesite.py`
- `filerestore.py`
- `get_alerts.py`
- `get_sessions.py`
- `getJSON.py`
- `joblist.py`
- `registerhypervisor.py`
- `registervsnap.py`
- `runjob.py`
- `spplogcollect.py`
- `sppvmbbackupinfo.py`
- `sqladhocbackup.py`
- `sqlcopies.py`
- `sqlrestore.py`
- `storageList.py`
- `systemInfo.py`
- `validatevsnapstatus.py`
- `vmware_chargeback.py`
- `vmwareadhocbackup.py`
- `vmwareassigntosla.py`
- `vmwaretestrestore.py`

**appassigntosla.py**

Use this script to assign one or more databases to an SLA policy. A comma separated list of database names along with the desired SLA name needs to be specified. The names are case sensitive.

**Syntax**

```
Usage: appassigntosla.py [options]
```

Options:

```
-h, --help       show this help message and exit
--user=USERNAME  SPP Username
--pass=PASSWORD  SPP Password
--host=HOST      SPP Host, (ex. https://172.20.49.49)
--type=TYPE      Application type: sql, oracle or db2
--dbs=DBS        Database name(s) (comma seperated)
--sla=SLA        SLA Policy Name
```

**Example**

```
python appassigntosla.py --user=restapiuser --pass=pass4AP! --host=https://10.0.250.41:443 --type=sql
--sla=Bronze --dbs="ESCC","SQL_ITSO"
```

INFO:logger:Adding db ESCC to SLA Bronze
INFO:logger:Adding db SQL_ITSO to SLA Bronze
INFO:logger:dbs are now assigned

**get_alerts.py**

The intention if this script is to provide a command line equivalent to the alert message display in the graphical user interface. Various optional parameters can be specified to filter by time frame, acknowledged state and alert type along with an optional full text search. The script shows only alerts and not job related messages (check `get_messages.py`).
**Syntax**

Usage: get_alerts.py [options]

Options:
- `-h, --help` show this help message and exit
- `--user=USERNAME` SPP Username
- `--pass=PASSWORD` SPP Password
- `--host=HOST` SPP Host, (ex. https://172.20.49.49)
- `--type=TYPE` type of alert: ERROR or WARN (optional)
- `--ack=ACK` acknowledged: True or False (optional)
- `--sort=SORT` sort order: DESC or ASC (optional)
- `--timeframe=TIMEFRAME` specify how many hours to look backwards: [int] (optional)
- `--search=SEARCH` search within the alert message text (optional)

**Example**

```bash
git -h, --help            show this help message and exit
--user=USERNAME       SPP Username
--pass=PASSWORD       SPP Password
--host=HOST           SPP Host, (ex. https://172.20.49.49)
--type=TYPE           type of alert: ERROR or WARN (optional)
--ack=ACK             acknowledged: True or False (optional)
--sort=SORT           sort order: DESC or ASC (optional)
--timeframe=TIMEFRAME specify how many hours to look backwards: [int] (optional)
--search=SEARCH       search within the alert message text (optional)
```

```python
git --host="https://spphost" --user=restapiuser --pass=pass4AP! --type=warn --search=low
```

<table>
<thead>
<tr>
<th>last occurrence</th>
<th>Type</th>
<th>ackn</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-07-04 16:43:59</td>
<td>WARN</td>
<td>True</td>
<td>10.0.250.48 (Vsnap): free disk space 19,370 MB (18.92% free) lower than threshold 20%</td>
</tr>
</tbody>
</table>

```python
git --host="https://spphost" --user=restapiuser --pass=pass4AP!
```

<table>
<thead>
<tr>
<th>last occurrence</th>
<th>Type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-06-19 15:45:42</td>
<td>ERROR</td>
<td>Job vmware_Silver (id=1004, session=1,560,951,215) failed.</td>
</tr>
<tr>
<td>2019-06-19 17:32:22</td>
<td>WARN</td>
<td>Job vmware_Silver (id=1004, session=1,560,958,337,185) partially succeeded.</td>
</tr>
<tr>
<td>2019-07-02 22:03:48</td>
<td>WARN</td>
<td>Job sklm_clone_twice (id=1007, session=1,562,097,600,075) partially succeeded.</td>
</tr>
<tr>
<td>2019-07-03 08:16:49</td>
<td>ERROR</td>
<td>Job sklm_clone_twice (id=1007, session=1,562,134,593,162) failed.</td>
</tr>
<tr>
<td>2019-07-03 09:41:03</td>
<td>WARN</td>
<td>Job vmware_Silver (id=1004, session=1,562,139,576,243) partially succeeded.</td>
</tr>
<tr>
<td>2019-07-04 16:43:59</td>
<td>WARN</td>
<td>Job Application Server Inventory (id=1010, session=1,562,585,757,121)</td>
</tr>
</tbody>
</table>

**getJSON.py**

The script `getJSON.py` is a simple Python script to query the Spectrum Protect Plus REST API endpoints with GET operations. It is similar to what a user can do with the build-in Swagger UI tool or with curl commands. However the script provides some advantages over curl and Swagger UI. `getJSON.py` handle the session (login and logout) for the user while with curl it would be required to retrieve a `sessionid` first and pass it along in all GET operations in the headers. Further the `getJSON.py` script will either generate an pretty formatted output or an unformatted output (raw), it implements a verbose option which will then also HATEOAS information such as discoverable links.

The script is helpful if a user is evaluating the REST API responses step-by-step and may want to apply additional commands like `grep` or `jq` for filtering of key-value-pairs or to identify the structure of the JSON formatted response for further programming.

The script provides an additional parameter which is mainly intended for API discovery during script programming. When the user specifies the parameter `-a` then the parameters `--host`, `--user` and `--pass` are obsolete as these information are stored in a file called `auth.txt`. The structure and content of the file are listed in Example 14-23.

**Example 14-23 Structure of auth.txt file**

```txt```
host=https://10.0.250.41
username=restapiuser
password=pass4AP!
```

**Syntax**

Usage: getJSON.py [options]

Options:
- `-h, --help` show this help message and exit
- `--user=USERNAME` SPP Username
Example

The following example demonstrated the usage of the -a flag. As the -v (verbose) parameter is not specified the HATEOAS information is not included in the output. In addition we limit the amount of returned object to one single object by specifying --pagesize=1 and execute the query on endpoint api/site. Note that the filtering is indeed taking place on the server and not within the script code. The server returns only one site object in the response while there are in fact more sites defines. The total number of object in the sites list "total": 5. The simple example demonstrated how to query the API and give the user or programmer an idea of the JSON response and it's structure. This is useful if the objects and it's members should be accessed i.g. in Python code.

```
py getJSON.py -a --endpoint="api/site" --pagesize=1
```

```
Endpoint:       https://10.0.250.41/api/site
restURL:        https://10.0.250.41/api/site?pageSize=1
{
  "page": 1,
  "sites": [
    {
      "defaultSite": true,
      "description": "Primary Site",
      "id": "1000",
      "name": "Primary",
      "rbacPath": "root:0/site:0/site:1000",
      "throttles": null
    }
  ],
  "total": 5
}
```

systemInfo.py

The script is inspired by the Spectrum Protect command "query system" and intends to provide an at-a-glance overview about system and storage utilization, health and database backups.

Example

```
py systemInfo.py -a
```

```
================================================================================================
SPP Server information:
================================================================================================

cpuUtil                  :         20.99
memory_size              :         47.01
memory_util              :          0.62
compressionRatio         :          1.94
deduplicationRatio       :          1.36
sizeFreeAllStorage       :        841.15
sizeTotalAllStorage      :        962.55
sizeUsedAllStorage       :        121.40
unavailable              :             1
================================================================================================

filesystems: 4

------------------------------------------------------------------------
catalog name  | status |  GB Total |  GB used | GB free | % used |  type
------------------------------------------------------------------------
Configuration   | NORMAL |  48.11    |   2.78   |  45.32  |  5.78   |  None
------------------------------------------------------------------------
```
vmwareadhocbackup.py
The script can be used to trigger an ad hoc backup of a virtual machine by specifying the VM’s name. The sla parameter is optional and only required if the virtual machine is assigned to more than one SLA. There can be only one job per SLA running so in case the user intends to run a second VM backup with the same SLA the user needs to wait for completion of the first run. The current implementation of the script allows only one VM name to be passed as argument.

Syntax
Usage: vmwareadhocbackup.py [options]

Options:
-h, --help       show this help message and exit
--user=USERNAME  SPP Username
--pass=PASSWORD  SPP Password
--host=HOST      SPP Host, (ex. https://172.20.49.49)
--filter=FILTER  Filter for unique datacenter, cluster or folder name in case VM name is not unique (optional)
--vm=VM          VM Name
--sla=SLA        SLA policy to run if VM is assigned to multiple

Example
python vmwareadhocbackup.py --user=restapiuser --pass=pass4AP! --host=https://10.0.250.41:443 --vm="t4-vm-win-sklm1" --sla="Silver"

INFO:logger:Running backup job for vm t4-vm-win-sklm1
14.6 API response code

Table 14-1 lists the HTTP status codes. For additional information, visit https://en.wikipedia.org/wiki/List_of_HTTP_status_codes.

<table>
<thead>
<tr>
<th>Status code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>The request completed successfully</td>
</tr>
<tr>
<td>201 Created</td>
<td>A new resource has been created successfully. The resource’s URI is available from the response’s Location header</td>
</tr>
<tr>
<td>204 No Content</td>
<td>An update to an existing resource has been applied successfully</td>
</tr>
<tr>
<td>400 Bad Request</td>
<td>The request was malformed. The response body will include an error providing further information</td>
</tr>
<tr>
<td>401 Unauthorized</td>
<td>Login attempt with invalid credentials</td>
</tr>
<tr>
<td>403 Forbidden</td>
<td>Generally related to permissions through Role Base Access Control</td>
</tr>
<tr>
<td>404 Not Found</td>
<td>The requested resource did not exist</td>
</tr>
<tr>
<td>405 Method Not Allowed</td>
<td>URL is unsupported</td>
</tr>
<tr>
<td>500 Unrecoverable Error</td>
<td>Diagnosed in Virgo log</td>
</tr>
<tr>
<td>503 Service Unavailable</td>
<td>This status is returned when too many requests are going to the same controller</td>
</tr>
</tbody>
</table>
Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *Protecting the VMware Environment with IBM Spectrum Protect*, REDP-5252

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

Online resources

These websites are also relevant as further information sources:

- IBM Spectrum Protect Plus BluePrints
  https://ibm.biz/IBMSpectrumProtectPlusBlueprints

- IBM Spectrum Protect Plus Knowledge Center

Help from IBM

IBM Support and downloads
ibm.com/support

IBM Global Services
ibm.com/services