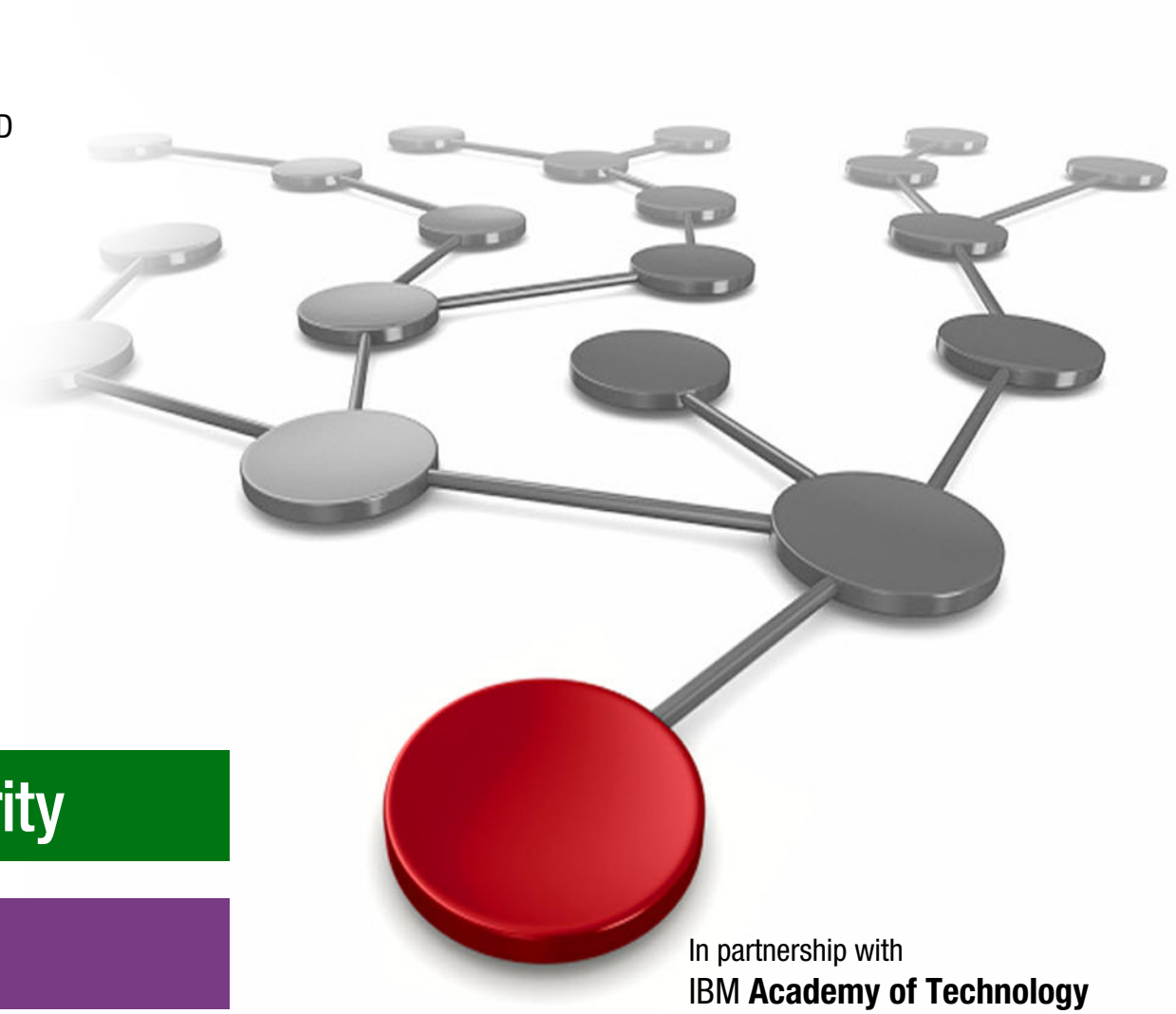
Redbooks
ibm.com/redbooks

Privileged Access Management for Secure Storage Administration

IBM Spectrum Scale with IBM Security Verify Privilege Vault

Vincent Hsu
Sridhar Muppidi, PhD
Sandeep R. Patil
Kanad Jadhav
Sumit Kumar
Nishant Singhai



Security

Storage

In partnership with
IBM **Academy of Technology**

IBM

Redpaper

Privileged Access Management for Secure Storage Administration: IBM Spectrum Scale with IBM Security Verify Privilege Vault

There is a growing insider security risk to organizations. Human error, privilege misuse, and cyberespionage are considered the top insider threats. One of the most dangerous internal security threats is the privileged user with access to critical data, which is the “crown jewels” of the organization. This data is on storage, so storage administration has critical privilege access that can cause major security breaches and jeopardize the safety of sensitive assets. Organizations must maintain tight control over whom they grant privileged identity status to for storage administration. Extra storage administration access must be shared with support and services teams when required. There also is a need to audit critical resource access that is required by compliance to standards and regulations.

IBM® Security™ Verify Privilege Vault On-Premises (Verify Privilege Vault), formerly known as IBM Security™ Secret Server, is the next-generation privileged account management that integrates with IBM Storage to ensure that access to IBM Storage administration sessions is secure and monitored in real time with required recording for audit and compliance. Privilege access to storage administration sessions is centrally managed, and each session can be timebound with remote monitoring. You also can use remote termination and an approval workflow for the session. In this IBM Redpaper, we demonstrate the integration of IBM Spectrum® Scale and IBM Elastic Storage® Server (IBM ESS) with Verify Privilege Vault, and show how to use privileged access management (PAM) for secure storage administration.

This paper is targeted at storage and security administrators, storage and security architects, and chief information security officers.

Introduction

Because data is the crown jewel for organizations, privilege access to data and the storage system hosting the data have become critical access points. You must ensure that privilege access, like storage administration or access to storage for support, services, or maintenance, is secure, centrally managed, and adheres to compliance requirements. Verify Privilege Vault On-Premises, formerly known as IBM Security Secret Server, integration with IBM Storage helps address these needs.

The secure administration of storage systems has the following benefits:

- Centrally manages, records, and audits admin actions for storage CLI and GUI sessions with real-time monitoring.
- Ensures that the storage administrator has no control over the audit logging to prevent tampering.
- Eliminates the need to share privilege administrative credentials (like the root user password on Linux) that are required for some software-defined storage (SDS) products.
- Provides timebound privilege storage admin sessions and remote termination of storage admin sessions.

> **Note:** *Timebound* in this context means that a secret can be accessible for only a certain period, such as 30 minutes or 1 hour.

- Integrates audit logs with external security information and event management (SIEM) (like IBM QRadar®) for real-time internal threat detection.
- Supports multifactor authentication for the users accessing storage admin sessions.
- Can capture keystrokes, process activity, and programs that are running (useful in some SDS offerings).
- Manages and audits privileged storage accounts and authentication secrets, such as passwords and SSH keys.

Secure remote support is managed by the customer, and it has the following benefits:

- Provides timebound audited access to the service, maintenance, or support teams.
- Supports a custom approval workflow (multi-level approval) for each access session.
- Records and audits all activity that is performed in support or service sessions.

This paper demonstrates the integration of IBM Spectrum Scale with Verify Privilege Vault. The concept can be extended and applied to other IBM Storage Systems.

IBM Spectrum Scale

IBM Spectrum Scale is a scalable, high-performance file system that is suitable for various use cases. It provides world-class storage management with scalability, flash-accelerated performance, and automatic storage tiering capabilities. IBM Spectrum Scale reduces storage costs while improving security and management efficiency in cloud, big data, and analytics environments. In a nutshell, IBM Spectrum Scale provides the following benefits:

- Virtually limitless scaling to nine quintillion files and yottabytes of data.
- High performance and simultaneous access to a common set of shared data.
- Integrated information lifecycle management (ILM) functions to automatically move data between storage tiers, including flash, disk, tape, and object storage (public and private cloud). ILM can reduce operational costs because fewer administrators can manage larger storage infrastructures.

With SDS, you can build your infrastructure solution with the following characteristics:

- Easy to scale with relatively inexpensive commodity hardware while maintaining world-class storage management capabilities.
- Deployable on Amazon Web Services (AWS) and IBM Cloud®.

- A cross-platform solution that is available on IBM AIX®, Linux, and Windows server nodes, or a mix of all three. IBM Spectrum Scale is also available for IBM Z®.
- Available as the prepackaged storage solution that is named IBM ESS with declustered RAID included.
- Global data access across geographic distances and unreliable WAN connections.
- Multi-site support to connect a local IBM Spectrum Scale cluster to remote clusters, which provides greater administrative flexibility and control.
- Proven reliability across multiple sites, and support for concurrent hardware and software upgrades.
- State-of-the-art protocol access methods for managing files and objects under the same global namespace, which makes more efficient use of storage space and avoids data islands. The supported protocols include NFS, SMB, POSIX, OpenStack Swift, and S3.
- Seamless integration for Hadoop applications through the Hadoop Distributed File System (HDFS) Transparency feature.
- Proven security features to ensure data privacy, authenticity, and auditability.
- File-level encryption for data at rest and secure erase.
- Policy-driven compression to reduce the size of data at rest and increase storage efficiency.
- Can be used as persistent storage for containers.
- Includes a GUI to simplify storage administration tasks and monitor many aspects of the system.

Figure 1 shows an overview of IBM Spectrum Scale.

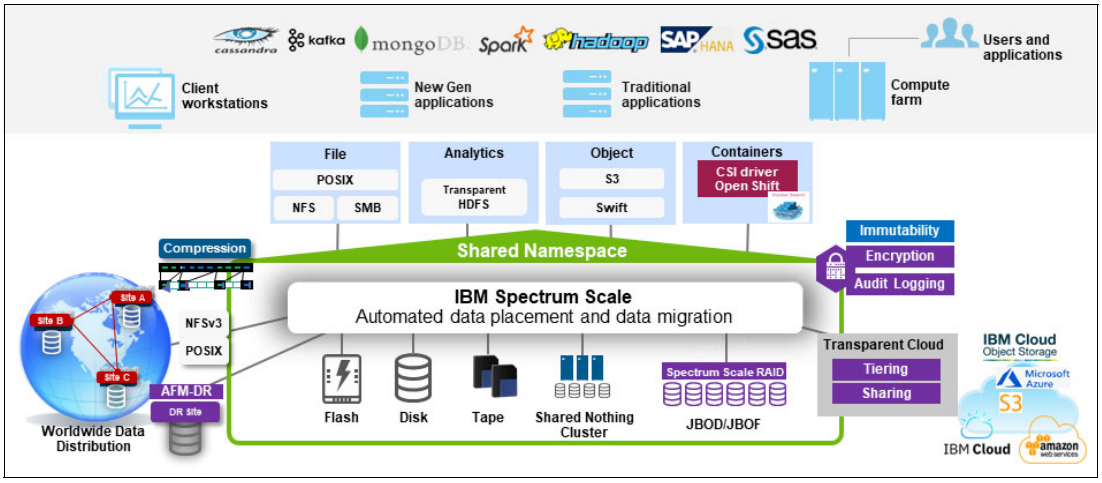


Figure 1 IBM Spectrum Scale overview

IBM Spectrum Scale often is used in high-performance and computationally demanding environments across different areas, such as banking, financial, healthcare, oil and gas, and automotive industries. Its most common use cases are in artificial intelligence (AI) and deep learning, big data analytics, content repository, private cloud, and compute clusters. It also is commonly used for data optimization and resiliency for archive, high-speed backup, and disaster recovery, and ILM.

IBM Spectrum Scale supports various deployment models, and one of them is IBM ESS, which is modern hardware-based implementation. IBM ESS is available as IBM ESS 3000 (high-density all-NVMe storage) and IBM ESS 5000 (high-capacity and high-performance storage).

Verify Privilege Vault

IBM Security Verify Privilege provides on-premises and cloud offerings. Verify Privilege Vault is a cloud-based solution for which organizations do not need to worry about any hardware or software requirements. However, IBM Security Verify Privilege On-Premises requires a dedicated server for installation and an SQL database to store details. Based on the requirements, features, and architecture, your organization can decide which offering to select. In this paper, we refer to Verify Privilege Vault On-Premises, although the information in this paper can be extended to the cloud offering with relevant and required changes.

Privileged access is the route to an organization's most valuable information. As a result, implementing PAM has become a top priority. Verify Privilege Vault is a full-featured PAM solution that is available both on-premises and in the cloud, and it is ready to empower your security and IT ops team to secure and manage all types of privileged accounts quickly and easily. With Verify Privilege Vault, you can:

- Establish a secure vault.
- Discover privileges.
- Protect passwords.
- Meet compliance requirements.
- Control sessions.

Verify Privilege Vault is fast to deploy, easy to use, and scalable for the enterprise. It integrates with the larger IBM Security portfolio for key use cases, such as identity governance and multi-factor authentication.

Table 1 shows the Verify Privilege Vault capabilities.

Table 1 Verify Privilege Vault capabilities

Feature	Description
Vaulting	Used to securely store and share access to secrets.
Session recording	Captures keystrokes, process activity, programs that are running, and screen or terminal activity.
Secret templates	Preconfigured templates for easy storage of common secret types.
Auditing and reporting	More than 50 standard and custom reports.
Groups/folder structure	Controls access to folders and secrets.
Launchers	Launchers provide direct access and authentication to a remote machine.
Features/permissions	Controls what features the secret server users can access within the application.
Password changers	Automatically change passwords.
IP-based restrictions	Control the IP addresses that can access the Verify Privilege Vault.

Feature	Description
Connect with various networks	Active Directory, Blue Coat, Cisco, ESX/ESXi, F5, LDAP, MySQL, Office 365, Oracle, Microsoft SQL, SonicWall, Sybase, UNIX, SAP, AWS, Google, Salesforce, and Windows.
Workflow	Approvals (multi-level), request for access, and checkout.
Session management	Live messaging, session termination, and real-time monitoring.
Custom password changer	Uses PowerShell, SQL, or SSH scripts to extend functions, and uses the list of commands to run on the target systems to change the passwords.
Discovery	Standard discovery and extensible discovery.
Heartbeat	Automatically tests stored secrets for accuracy at a certain interval.
Dependencies for service accounts	Windows Service, Windows Scheduled Tasks, IIS Application Pools, and Component Object Model.

To know more about the capabilities and features of Verify Privilege Vault, see “References” on page 23.

Figure 2 shows the architecture of Verify Privilege Vault.

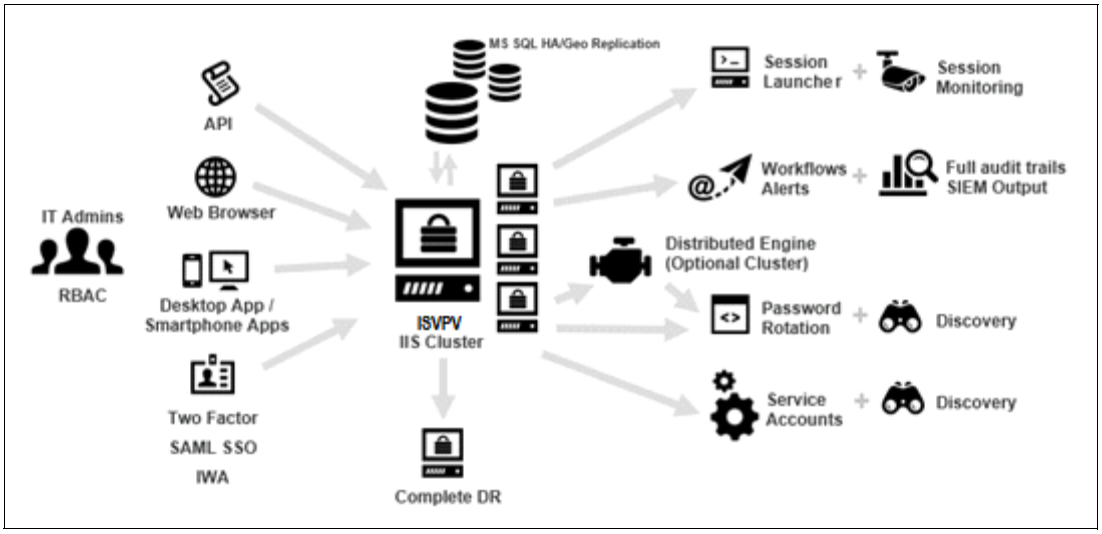


Figure 2 Architecture of Verify Privilege Vault

The following list describes the architecture that is shown in Figure 2:

- Left side of the architecture represents different mediums though which Verify Privilege Vault can be accessed. The right side represents the high-level internal working.
- Verify Privilege Vault requires an SQL server for its configuration and data management. You can configure the setup for high availability as needed.
- Verify Privilege Vault provides session launchers that are tailored to start specific applications based on triggers in a secret template. For example, for the Windows platform, the Remote desktop connection application is invoked when trying to access a Windows account secret. Similarly, for the UNIX or Linux platforms, the PuTTY application is triggered when using a UNIX or Linux account secret.

- There is an alert system capability for receiving real-time event information and SIEM integration (with QRadar).
- A distributed engine is used for remote password changing and discovery of new accounts.

Administration access management of IBM Spectrum Scale with Verify Privilege Vault

IBM Spectrum Scale or IBM ESS administration can be done by using a CLI or GUI. In a typical IBM Spectrum Scale cluster, *root* is the super user, and configured **sudo**-based users are the privileged users for administration through the CLI. The IBM Spectrum Scale GUI supports role-based access control (RBAC) based administration.

Monitoring and auditing of the storage administration action is important and critical for various reasons:

- Tracing any potential malicious actions that are performed by a rogue administrator.
- Adhering to regulations because data that is hosted on a storage system can be subject to compliance.
- Auditing remote sessions by product support or services teams.
- Using auditing for overall threat detection and analysis against any internal cyberevents that are associated with data or storage.

IBM Spectrum Scale supports logging administration actions in syslog, which then can be routed to SIEM-based solutions. One challenge with this approach is that the IBM Spectrum Scale root user can change these settings. In some instances, the root password might be shared among multiple administrators of a data center, which introduces the challenge of tracing administrative user profile mapping to a certain root login session. Another challenge is that such logs are auto-rotate in nature, and if they are not configured to be routed to an external SIEM-based solution, then their effectiveness for threat detection or compliance is reduced.

To enhance the security posture for an overall deployment, you need an external security system that provides the following functions:

- Manages, records, and audits the privilege access for storage administration, which complements internal storage auditing of administrative actions.
- Ensures that the storage administrator has no control over the audit logging of storage administration, which is recorded externally.
- Eliminates the need to share the privilege administrative user credentials (like the root user password), and able to audit and catalog the user details of who is logging in to the storage system (like an IBM Spectrum Scale cluster) by using root credentials.
- Audits the record of administration actions that run through the storage GUI-based administration panel.
- Gives timebound audited administrative access in scenarios where the privileged access might need to be given to service, maintenance, or support teams.

Managing the administrative access of IBM Spectrum Scale by using Verify Privilege Vault helps address these needs by enhancing the overall security posture of the deployment.

Verify Privilege Vault is used for PAM, and it acts as a secure conduit between users and privilege access like IBM Spectrum Scale administration, as shown in Figure 3.

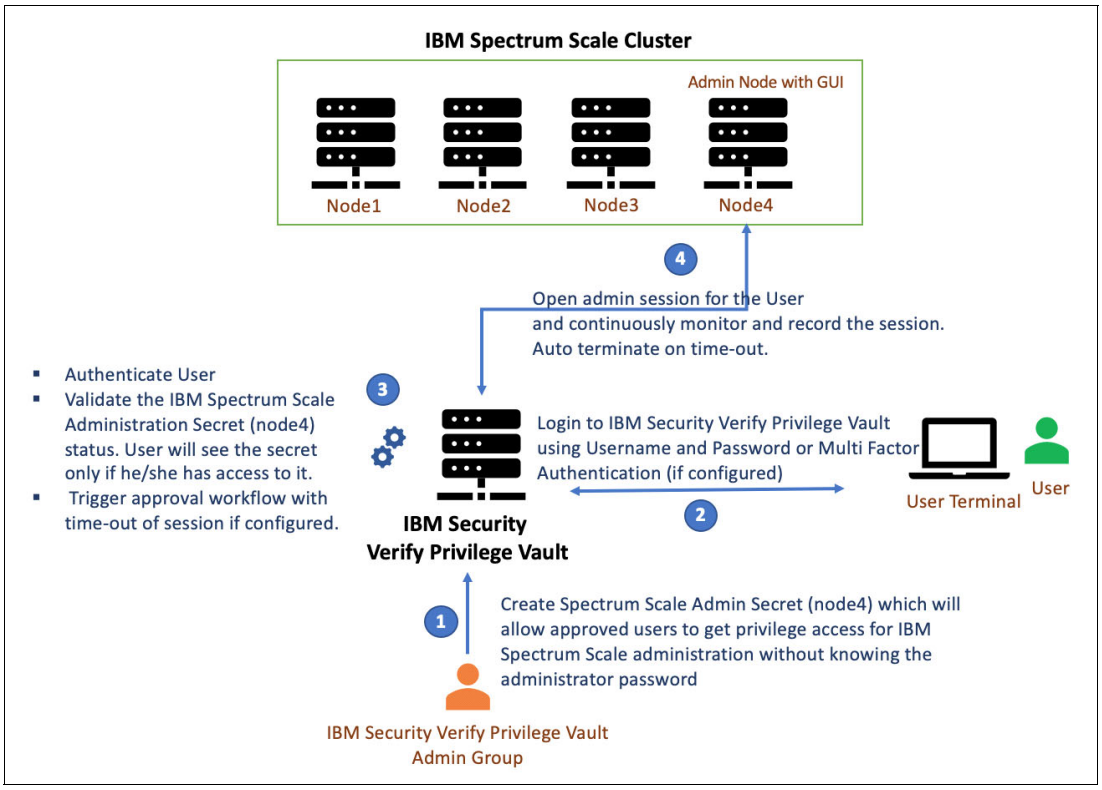


Figure 3 Administration login flow IBM Spectrum Scale with Verify Privilege Vault

Note: The user can see only the name of the secret (for example, Admin Node4) and does not have permission to view the details of the secret like the password (for example, the Admin password of Node4) unless the permission is explicitly given to the user by Verify Privilege Vault Administrator.

In this paper, we walk through some of the practical scenarios of IBM Spectrum Scale storage administration and how Verify Privilege Vault helps in its secure administration.

Note: Verify Privilege Vault can simultaneously manage multiple privilege accesses of different types of applications. In this paper, we are showing only its capability for IBM Spectrum Scale, but it can be easily extended to other types of IBM Storages.

Here are the setup prerequisites:

- IBM Spectrum Scale or an IBM ESS cluster is already deployed with the IBM Spectrum Scale admin mode central setting that enables a limited set of nodes to be the administrator. As shown in Figure 3, in our sample setup we have a 4-node Linux cluster with node4 defined as the admin node. IBM Spectrum Scale GUI also is configured on the admin node.

  For more information about the deployment of IBM Spectrum Scale, see IBM Knowledge Center.

- To begin the integration, you must have Verify Privilege Vault installed on your environment.

For more information about installation and deployment, see *IBM Security Secret Server Version 10.8 Administration Guide*.

- After Verify Privilege Vault is installed, you must log in as the Verify Privilege Vault admin user. Then, you must add the IBM Spectrum Scale admin node (which is the Linux system SSH account) as a *secret* into Verify Privilege Vault. To do that task, the Verify Privilege Vault admin user must provide the details of the SSH account, such as the IP address and credentials, which then are securely stored inside Verify Privilege Vault.

  For more information about creating and editing secrets, see *IBM Security Secret Server Version 10.8 Administration Guide*.

  Note: According to the Verify Privilege Vault documentation, a *secret* is defined as a piece of information that is stored and managed within the secret server. Secrets are derived from secret templates. A typical secret is the privileged passwords on routers, storage systems, servers, applications, and devices. Files can be stored in secrets so that you can store private key files, SSL certificates, license keys, network documentation, Microsoft Word, or Excel documents. For more information, see *IBM Security Secret Server Version 10.8 Administration Guide*.

- Verify Privilege Vault has an SSH Proxy. When it is enabled, the users cannot directly access the SSH account. After the SSH Proxy is enabled, the encrypted credentials are used, and the IP address and host name are replaced with the IP of the proxy server. This setup ensures that only connections from Verify Privilege Vault are accepted at the IBM Spectrum Scale Linux system. All other direct connections are blocked.

  For more information, see “References” on page 23.

- Create and configure a regular user (for example, User A) in Verify Privilege Vault. User A is the use who is assigned to administer the IBM Spectrum Scale cluster. User A is unaware of the IBM Spectrum Scale system's administration login credentials and cannot directly log in to the IBM Spectrum Scale cluster. They can log in to Verify Privilege Vault by using their Verify Privilege Vault credentials.

  For more information about how to create a user in Verify Privilege Vault, see *IBM Security Secret Server Version 10.8 Administration Guide*.

- You can have Verify Privilege Vault configured for multifactor authentication so that, for example, if User A logs in to Verify Privilege Vault, the user is challenged with multifactor authentication.

  For more information about how to configure multifactor authentication, see *IBM Security Secret Server Version 10.8 Administration Guide*.

Important: This list provides important setup information:

- In this setup, the root password and **sudo** user details that enable privilege administrative access to IBM Spectrum Scale are not known to anyone, and they are secretly stored on Verify Privilege Vault.
- The regular users (User A) cannot directly log in to IBM Spectrum Scale cluster because the user is unaware of the login details for administration. The only way for an approved and configured Verify Privilege Vault user to gain administrative access to IBM Spectrum Scale is through Verify Privilege Vault.
- The users that are configured with Verify Privilege Vault typically are organizational users in Active Directory or a local user who has access to the secrets that map to administration of infrastructure systems.
- In this setup, we create an IBM Security Verify Privilege user that is called Admin User who has control over the secrets that are created in Verify Privilege Vault. We use this user for functions like workflow approval, which is described in “Scenario 2: Granting timebound IBM Spectrum Scale administration access with a manager and administrator approval workflow” on page 19.
- Verify Privilege Vault also takes care of the password policy that is associated with the IBM Spectrum Scale administration nodes, which relieves the IBM Spectrum Scale administrators of password management overhead.

For more information about these topics, see *IBM Security Secret Server Version 10.8 Administration Guide*.

Scenario 1: Auditing IBM Spectrum Scale administration actions that run through the CLI or GUI by using the Verify Privilege Vault session monitoring feature

With this scenario, you maintain external audit records of all IBM Spectrum Scale administrative actions, which are useful for security audits, threat analysis, and problem determination. Because these records are recorded by Verify Privilege Vault externally, they cannot be tampered with and are more secure. Additionally, you can have users work as administrators of IBM Spectrum Scale without the users knowing or sharing the IBM Spectrum Scale administrator password (root password or the **sudo** user password).

IBM Spectrum Scale cluster administration is done through the root user or by using the IBM Spectrum Scale **sudo** user. Alternatively, administration is done through the IBM Spectrum Scale GUI. In this scenario, we walk through about how access to administration sessions of IBM Spectrum Scale with Verify Privilege Vault can be done.

Complete the following steps:

1. Log in as the Verify Privilege Vault administrator and create a secret for the IBM Spectrum Scale CLI administration account (either root or the **sudo** user and their SSH password) inside Verify Privilege Vault.

   Figure 4 shows a snapshot of the secret that is associated with the node4 SSH credentials.

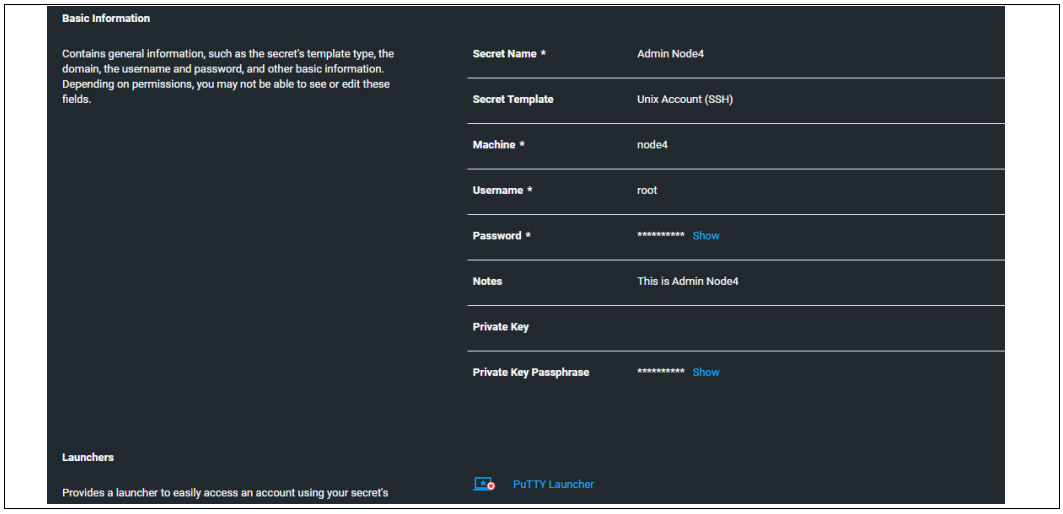


Figure 4 Creating a secret for the IBM Spectrum Scale administration credentials on Verify Privilege Vault

   The secret that is named “Admin Node4” is associated with the node4 SSH credential. Because IBM Spectrum Scale node4 is a Linux machine, we select the UNIX Account (SSH) from the secret template.

2. Create a secret for the IBM Spectrum Scale GUI administration account.

   Figure 5 shows a snapshot of the secret that is associated with the node4 GUI credentials.

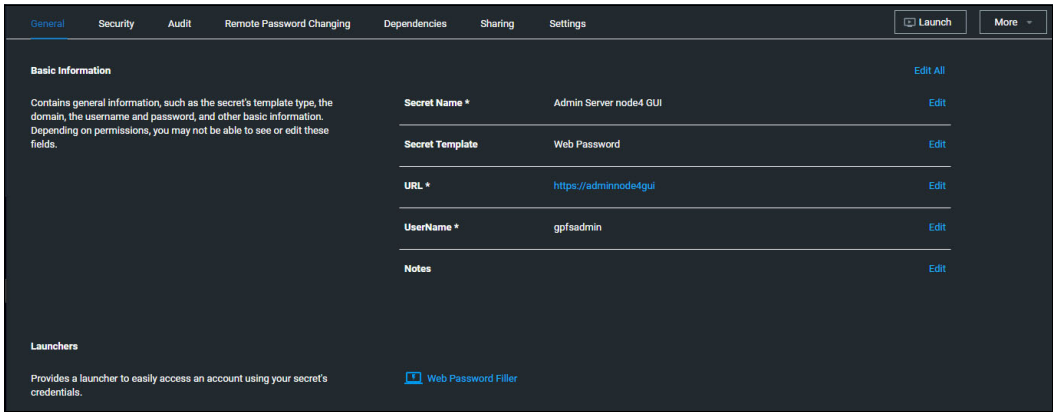


Figure 5 Creating a secret for the IBM Spectrum Scale GUI administrator on Verify Privilege Vault

   The secret that is named “Admin Server Node4 GUI” is associated with the IBM Spectrum Scale GUI administration credential. In this example, the IBM Spectrum Scale GUI URL is `https://adminnode4gui`.

3. Configure and assign privileges to User A for the secrets that were created in steps 1 and 2.

Assign User A the privilege to access the IBM Spectrum Scale administration secrets that were created in steps 1 on page 10 and 2 on page 10 so that User A can log in to the IBM Spectrum Scale node or GUI administration but without knowing the password of those systems.

Figure 6, Figure 7, Figure 8 on page 12, and Figure 9 on page 12 show that the admin secrets that were created are part of the Admin Server folder. Also, User A has access to this Admin Server folder so that it can view the admin node secrets. After the permissions are granted, User A can view the admin secrets.

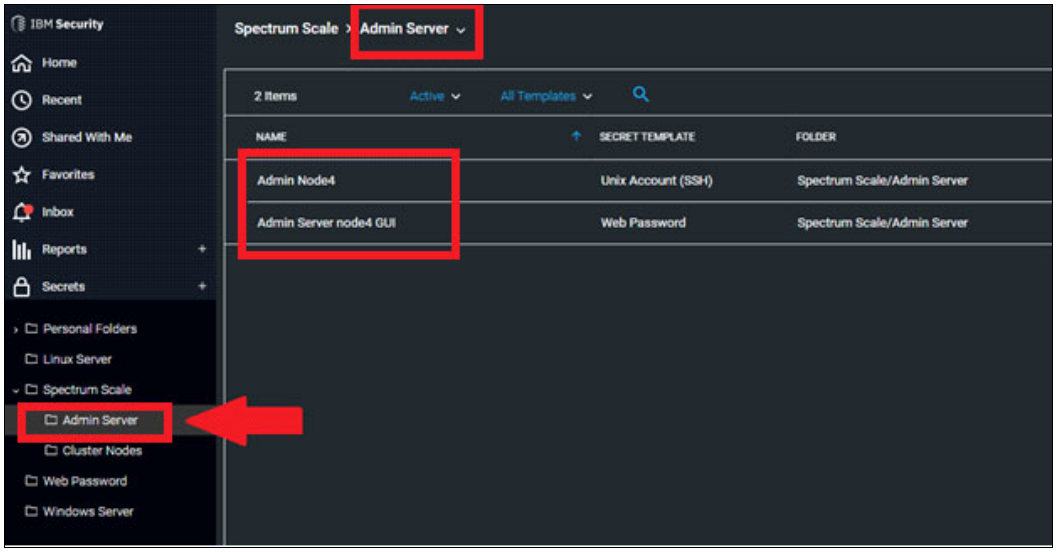


Figure 6 Verify Privilege Vault window with secrets for IBM Spectrum Scale under the Admin Server folder

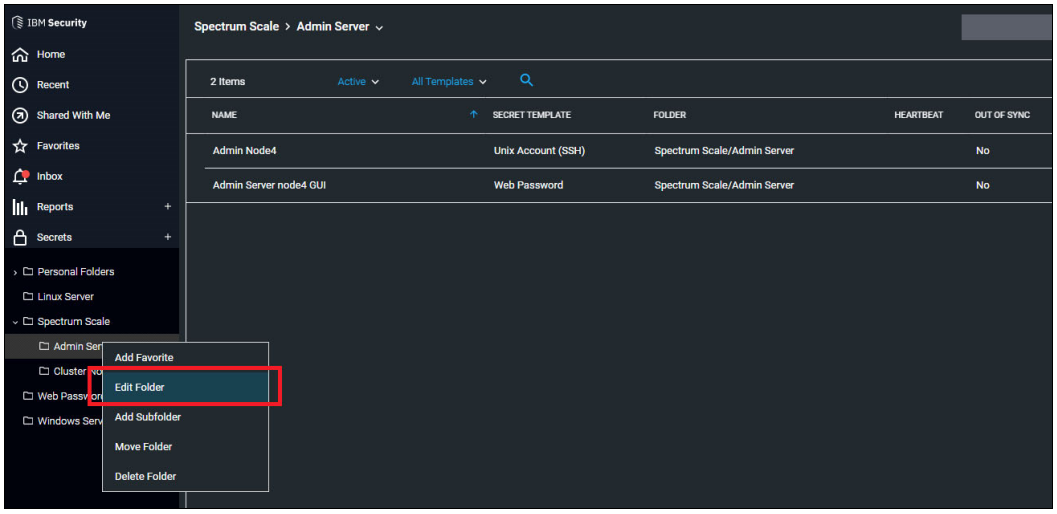


Figure 7 Verify Privilege Vault window with edit options for adding user permissions to the folder

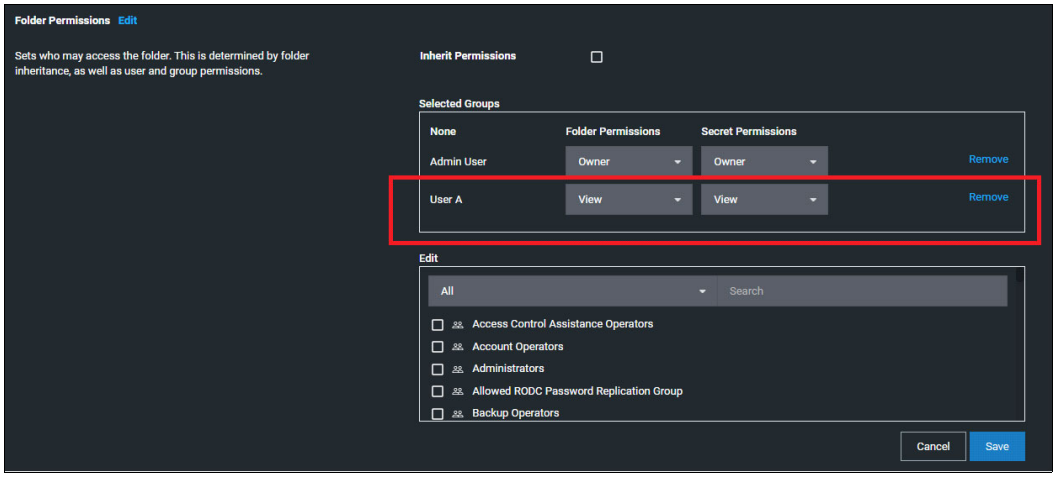


Figure 8 Assigning folder permissions to User A

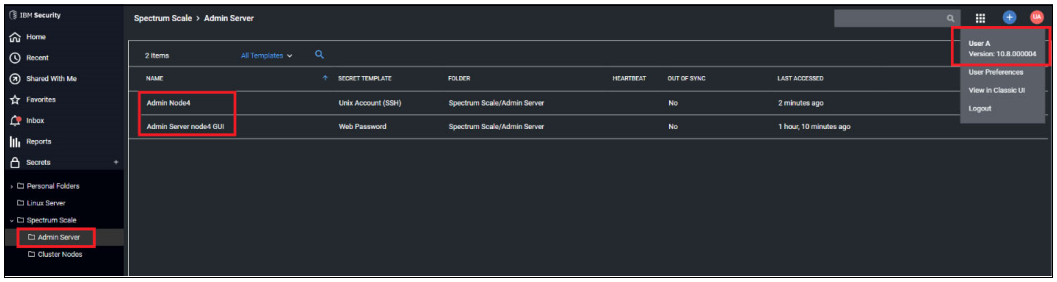


Figure 9 User A logged in with Admin Server folder access

4. Enable the secrets for auditing, recording, and event subscription.

   Ensure that the auditing and recording of access to IBM Spectrum Scale secrets is enabled. By default, all the secrets auditing is enabled, and all the view, edit, update, launch, and password change operations are recorded by Verify Privilege Vault, which can be viewed under the **Audit** tab for each secret. You can verify this setting by clicking the **Audit** tab, as shown in Figure 10.

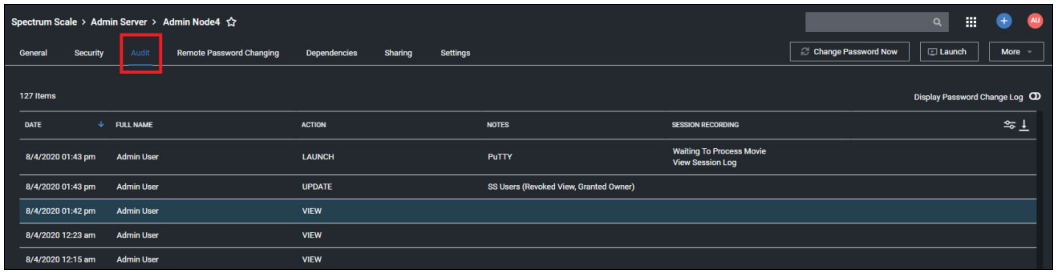


Figure 10 The Audit tab of the “Admin Node4” secret shows the audit configuration for the secret

As shown in Figure 11 on page 13 to record the sessions and live monitoring, set the **Session Recording Enabled** option to **Yes**. In Figure 11 on page 13, the users who are shown under Approvers are the ones who are eligible to approve the secret session if the approval workflow is configured. For more information, see “Scenario 2: Granting timebound IBM Spectrum Scale administration access with a manager and administrator approval workflow” on page 19.

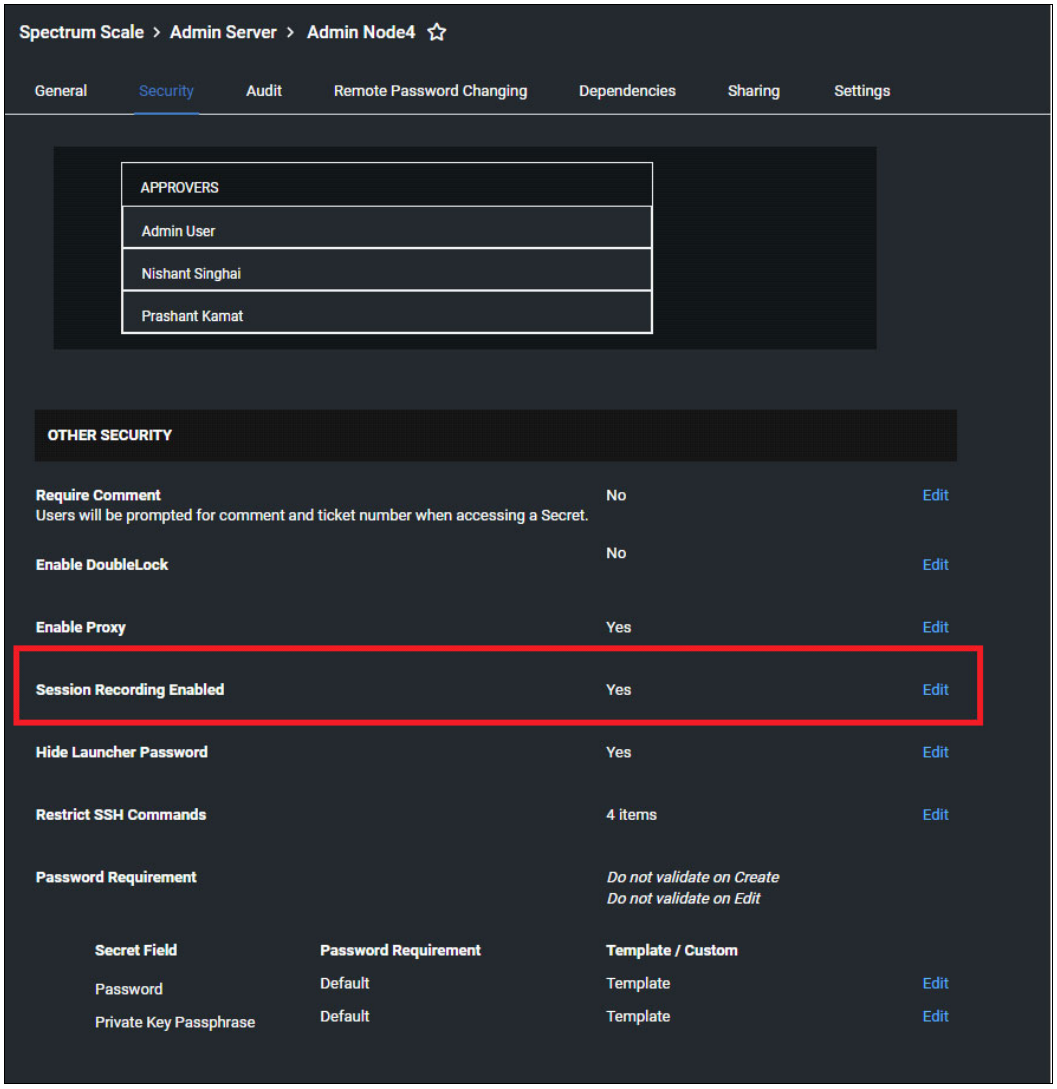


Figure 11 Window that shows that session recording is enabled for the "Admin node4" secret

An Verify Privilege Vault user with the Administrator role can view the session replay by accessing the Session Monitoring window. To view the recording, select **Admin** → **Session Monitoring** → **Secret**. Keystroke logging can be enabled by recording the metadata. Extra configuration of the SSH Proxy is required to enable keystroke logs.

For more information about enabling SSH Proxy and enabling and configuring Verify Privilege Vault session recording, see *IBM Security Secret Server Version 10.8 Administration Guide*.

5. Enable event subscriptions for the IBM Spectrum Scale secrets.

   Enable the event subscriptions that are associated with the IBM Spectrum Scale secrets. Event subscription notifies the specified Verify Privilege Vault administrator or organization's security team about any event (launch, access, view, edit, and others) that is associated with the secret (IBM Spectrum Scale secrets in this case) through email. You can enable event notifications by using event pipelines or by creating policies that send notifications to multiple platforms.

As shown in Figure 12 to enable **Event Subscriptions**, click **Admin** and then select the **Event Subscriptions** option.

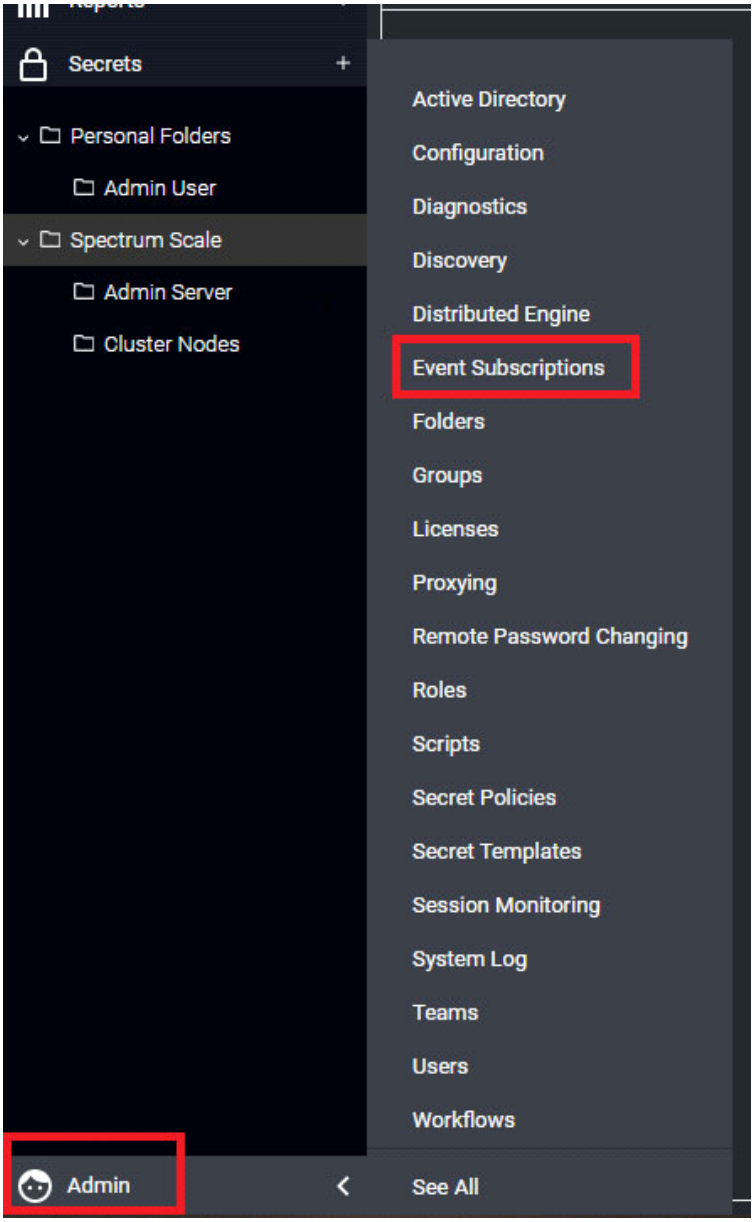


Figure 12 Accessing Event Subscriptions

As shown in Figure 13 on page 15 to configure Event Subscriptions, enter a name into the Subscription Name field. Then, add the Subscribed User to receive events notifications, which in this case is the Admin User.

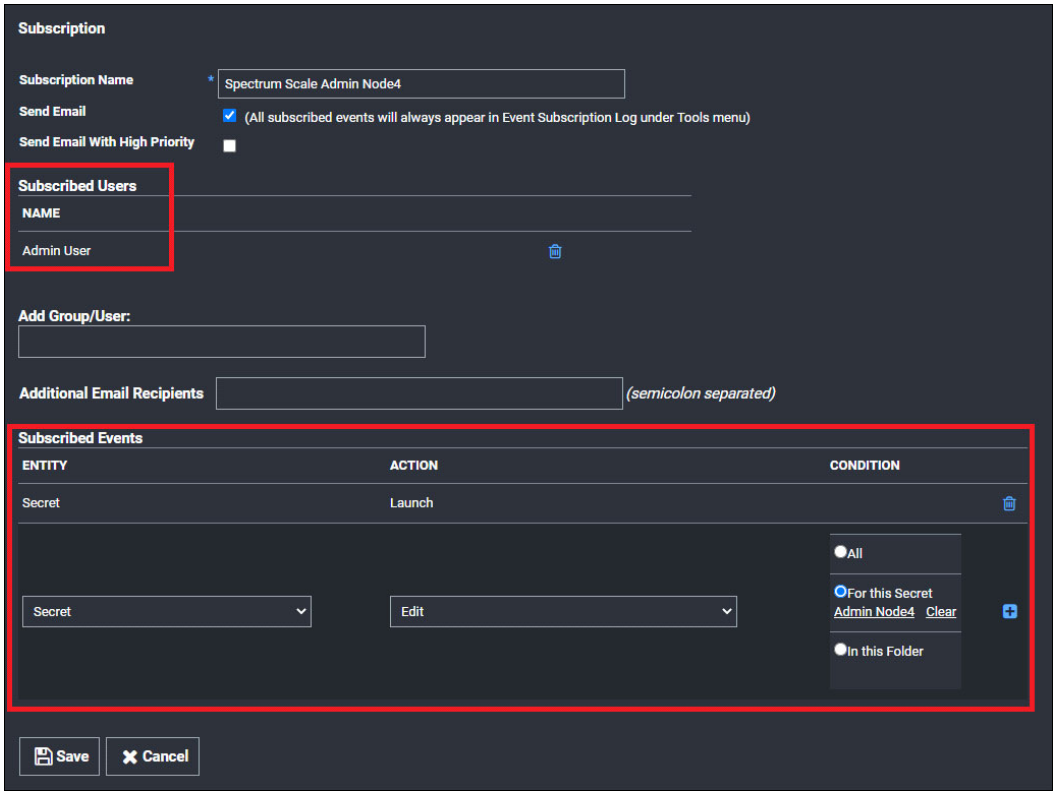


Figure 13 Event Subscriptions Configuration page

For the Subscribed Events field, select “Admin Node4” as a secret and the actions **Launch** and **Edit**. When the IBM Spectrum Scale administration Secret is launched or edited, an event notification is sent to the Admin User's email address. As shown in Figure 14, an email notification shows that User A launched the Secret Admin Node4.

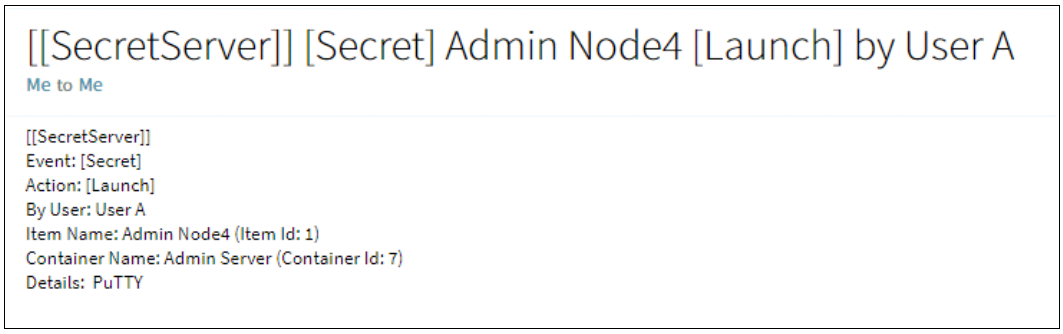


Figure 14 Event Subscription notification received through email

Figure 15 shows a list of actions that the administrator can set for the secret.

For more information about event subscriptions, see *How to set up the email notification on IBM Security Secret Server 10.7 or above*.

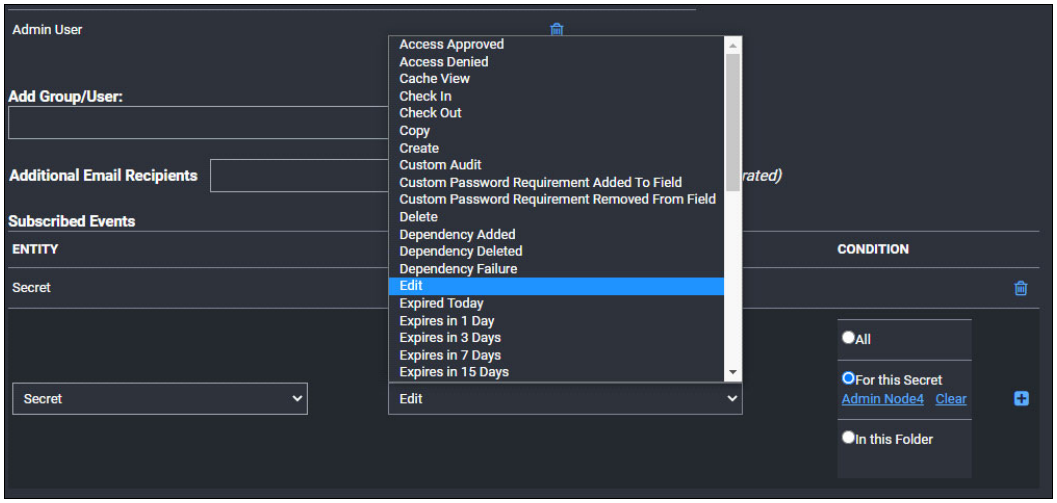


Figure 15 Enabling event subscription for the Edit Secret activity

6. Log in to an IBM Spectrum Scale cluster as User A to perform CLI-based administration. Use the secret that was created in step 1 on page 10.

   When User A logs in to Verify Privilege Vault, they can select the PuTTY Launcher from the Secret Page for “Admin Node4”. This action logs in the user automatically to IBM Spectrum Scale CLI with root user credentials without the user knowing the root user password. Then, User A can run the IBM Spectrum Scale administrative commands, as shown in Figure 16.

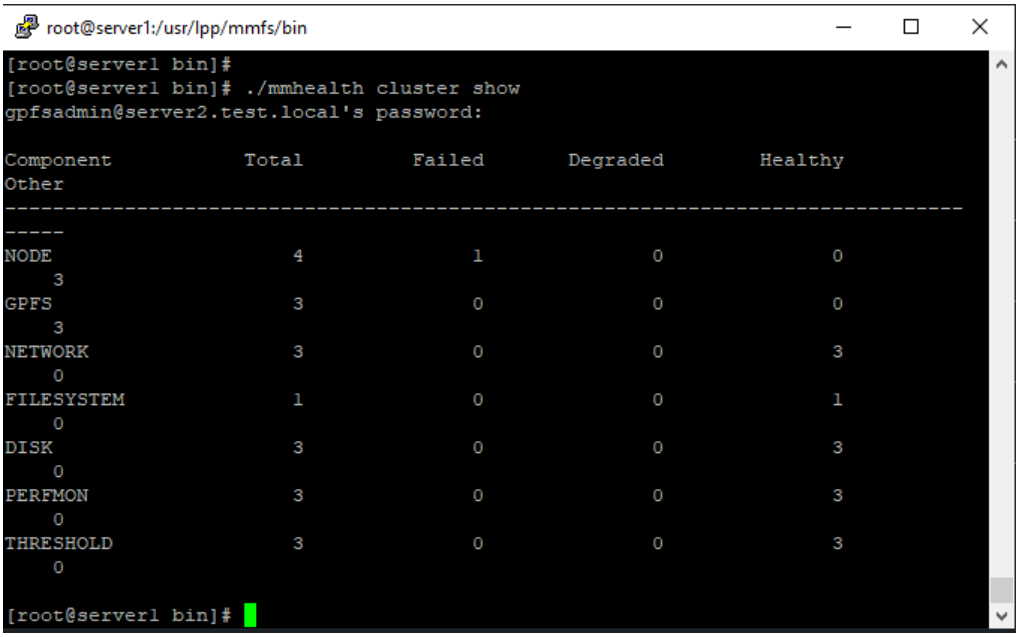


Figure 16 PuTTY session that is launched for User A and showing the IBM Spectrum Scale administrative commands

7. Log in to the IBM Spectrum Scale cluster as User A to perform GUI-based administration. Use the secret that was created in step 2 on page 10.

   User A can view the details of Admin Server Node4 GUI after they select this secret, as shown in Figure 17.

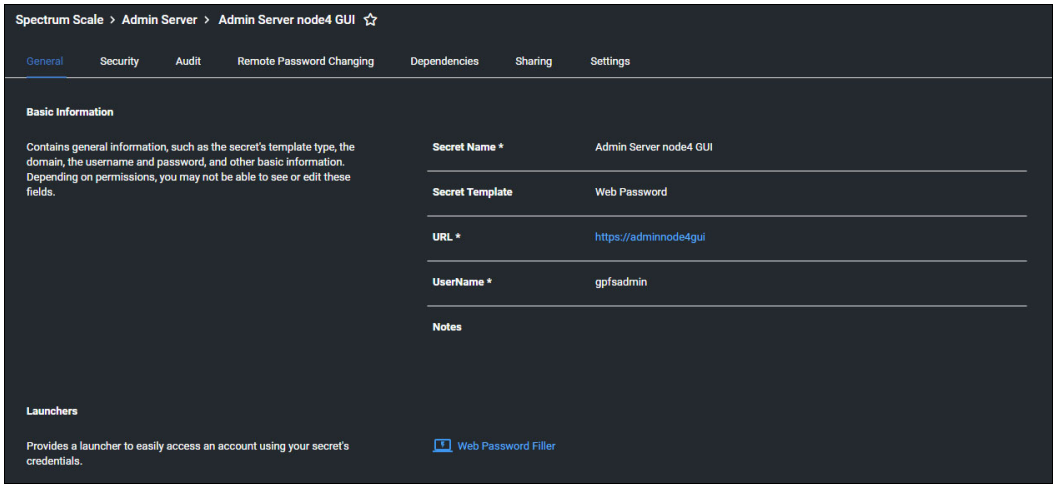


Figure 17 Launching the IBM Spectrum Scale GUI secret

Click **Web Password Filler** to open a browser tab where the IBM Spectrum Scale GUI loads, as shown in Figure 18.

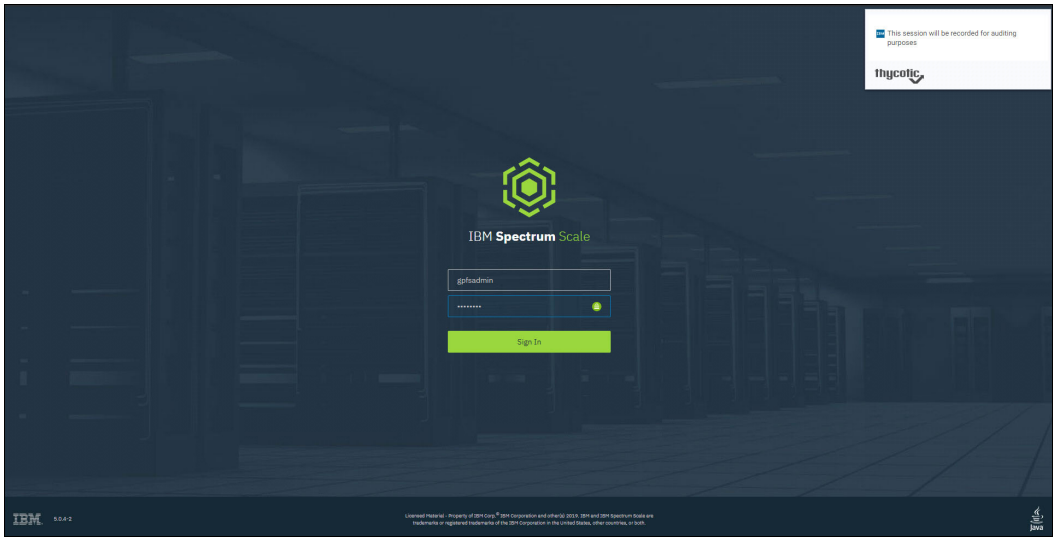


Figure 18 Launching the IBM Spectrum Scale administration GUI with the secret with prefilled credentials

At the upper right, you see that there is a message that shows that the web session is recorded. Verify Privilege Vault records only the activities that are performed on that tab.

After User A is logged in, they can check the Admin GUI Figure 19) for IBM Spectrum Scale and do the required administration, which is audited and recorded by Verify Privilege Vault.

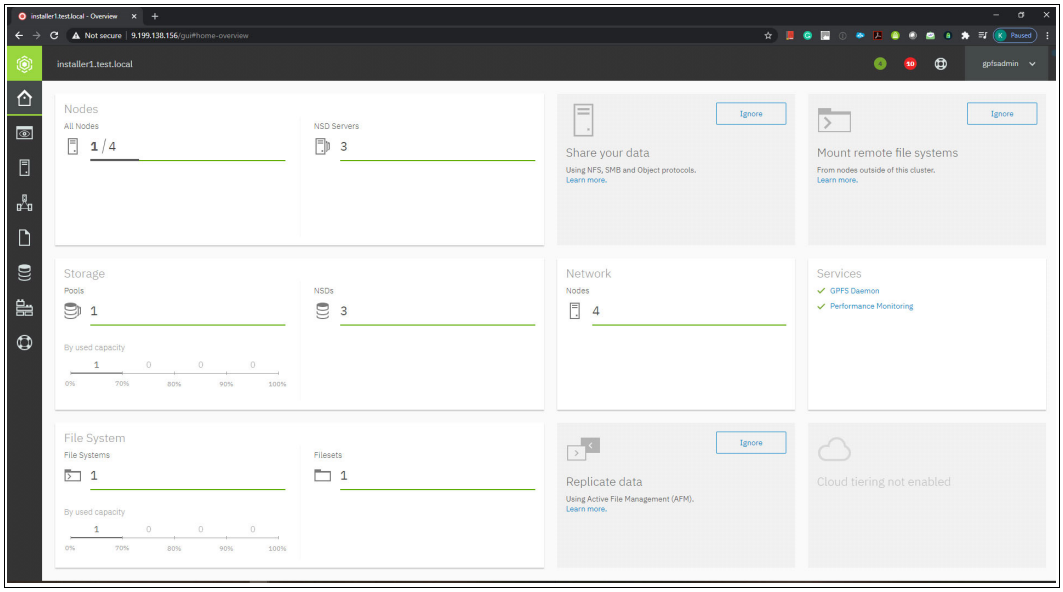


Figure 19 IBM Spectrum Scale administration through the GUI that is launched by the secret

8. View the auditing (session recording) of the administrative work that was done in steps 6 on page 16 and 7 on page 17, which is recorded by Verify Privilege Vault.

   Log in as the Verify Privilege Vault administrator and view the recording, as shown in Figure 20 and Figure 21 on page 19.

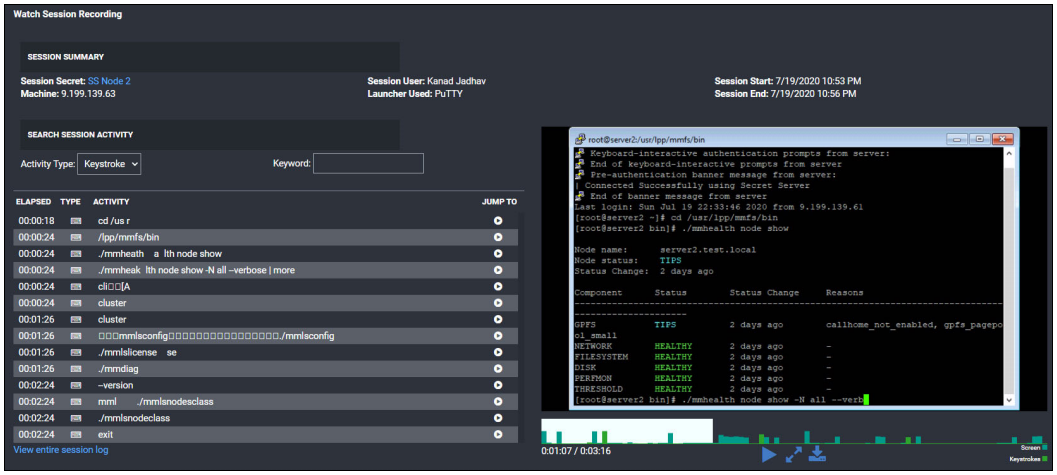


Figure 20 Verify Privilege Vault Session Recording: View of IBM Spectrum Scale CLI administration

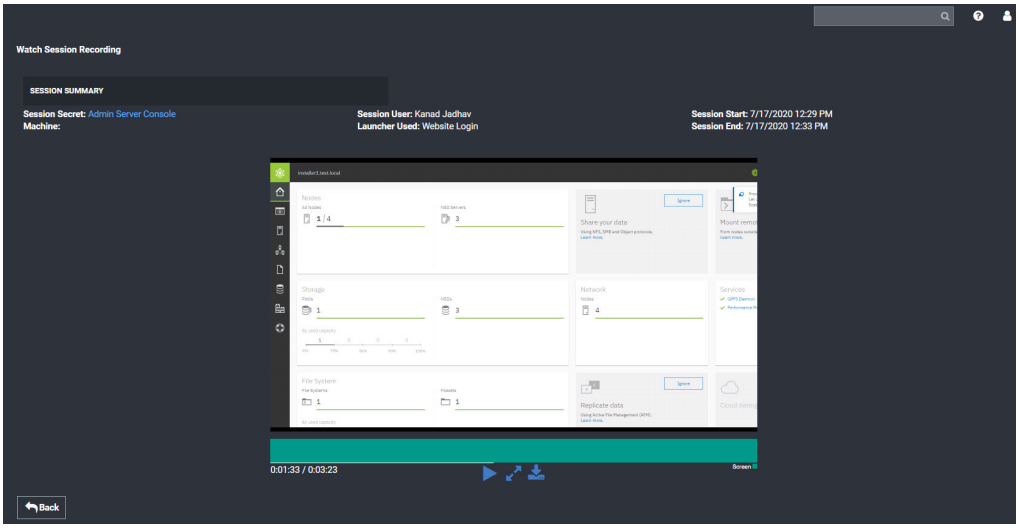


Figure 21 Verify Privilege Vault Session Recording: View of IBM Spectrum Scale GUI administration.

Note: In this example, we used only one user for IBM Spectrum Scale administration. You can have multiple Verify Privilege Vault users who can be granted access to IBM Spectrum Scale administration-related secrets so that you have multiple administrators for IBM Spectrum Scale.

Scenario 2: Granting timebound IBM Spectrum Scale administration access with a manager and administrator approval workflow

Verify Privilege Vault allows the secret administrator to do the following tasks:

1. Set time-based administration sessions.
2. Monitor the ongoing administration session.
3. Terminate the session instantly and at any time.
4. Mandate approval from a manager when a user tries to open a session.

These tasks are useful in times when you must grant privilege access for storage administration to external parties for servicing, maintenance, or problem determination.

Complete the following steps:

1. Configure the manager approval workflow that is associated with the IBM Spectrum Scale administration secret.

   Configure a manager approval workflow for IBM Spectrum Scale GUI-based administration. When a user tries to access IBM Spectrum Scale GUI through the secret that is associated with it, the system triggers a manager approval workflow, and the user gets access only after the manager approves the request.

Figure 22 shows the security setting for adding an approver for the secret Admin Server node4 GUI.

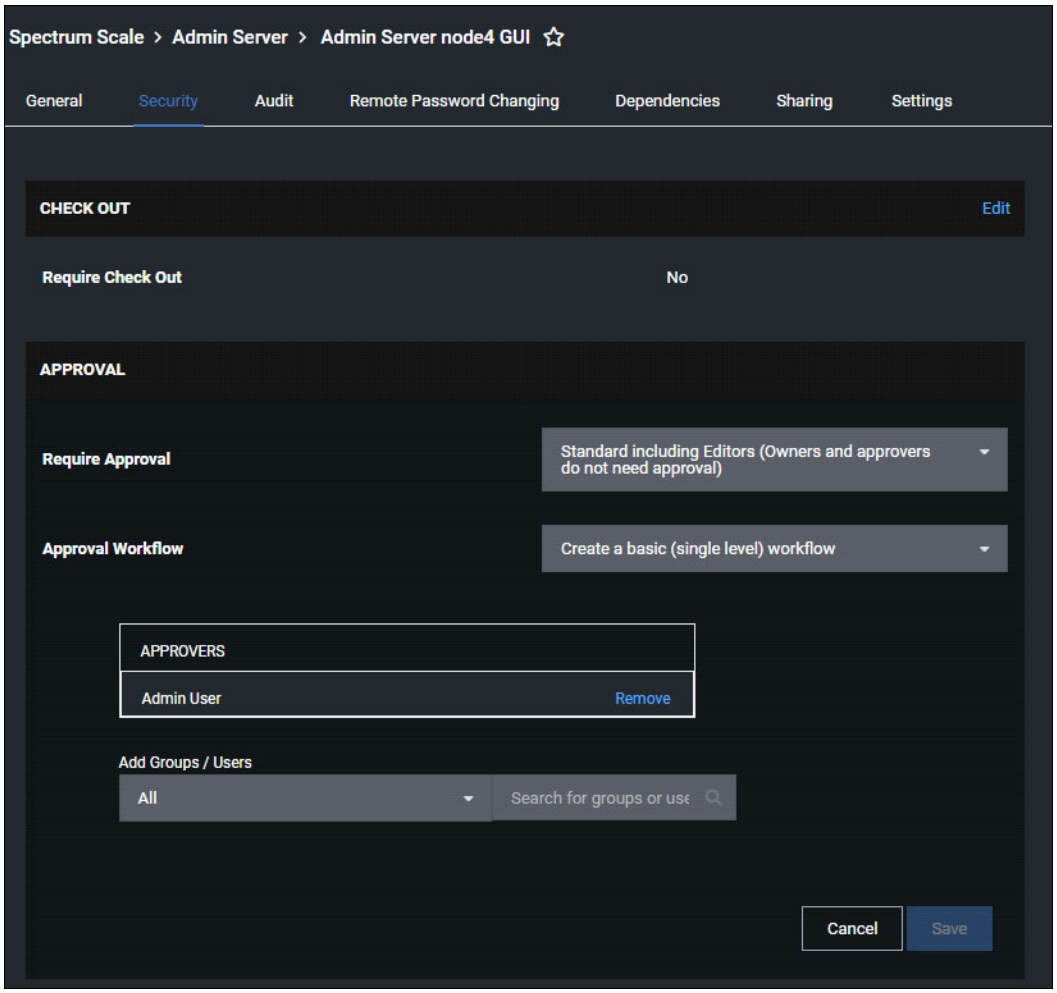


Figure 22 Setting manager approval for a secret

2. Log in to the IBM Spectrum Scale cluster by using User A for CLI-based administration by using the secret that was created in step 1 on page 19. This action requires manager approval.

   Figure 23 on page 21 shows User A initiating the secret, which requires manager approval.

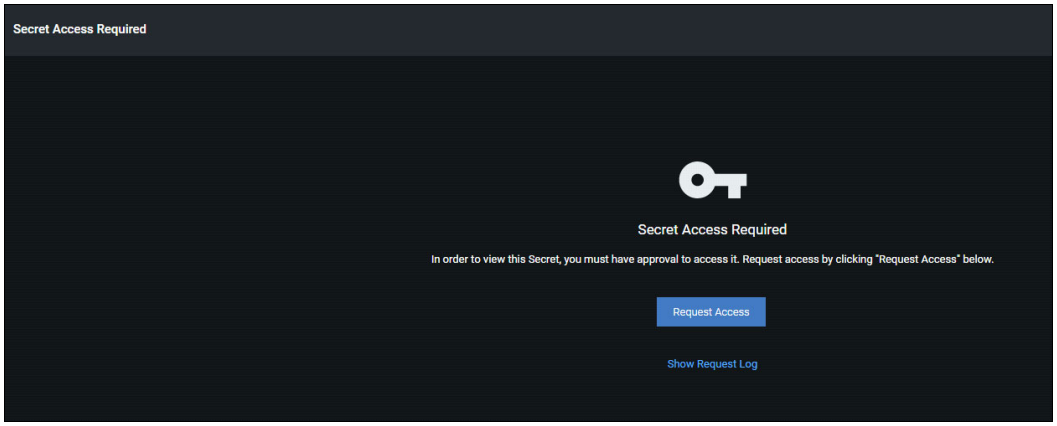


Figure 23 Request access screen for requesting access to a secret

As shown in Figure 24, User A provides details for accessing the Admin Server node4 GUI secret. The details are routed to the manager (Admin User) for their approval.

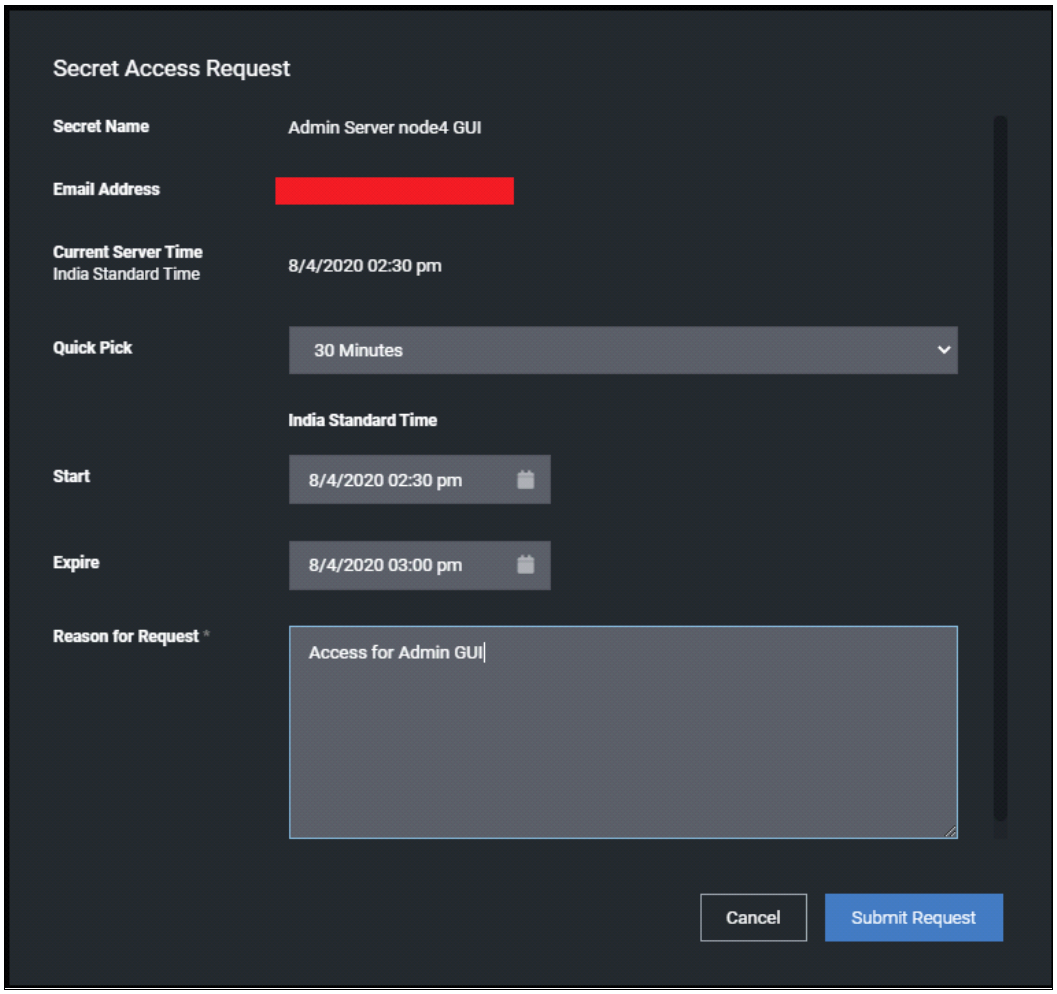


Figure 24 Screen showing a user requesting access to IBM Spectrum Scale Secret with a defined time for the session.

Figure 25 shows manager/approver approving the secret/access request.

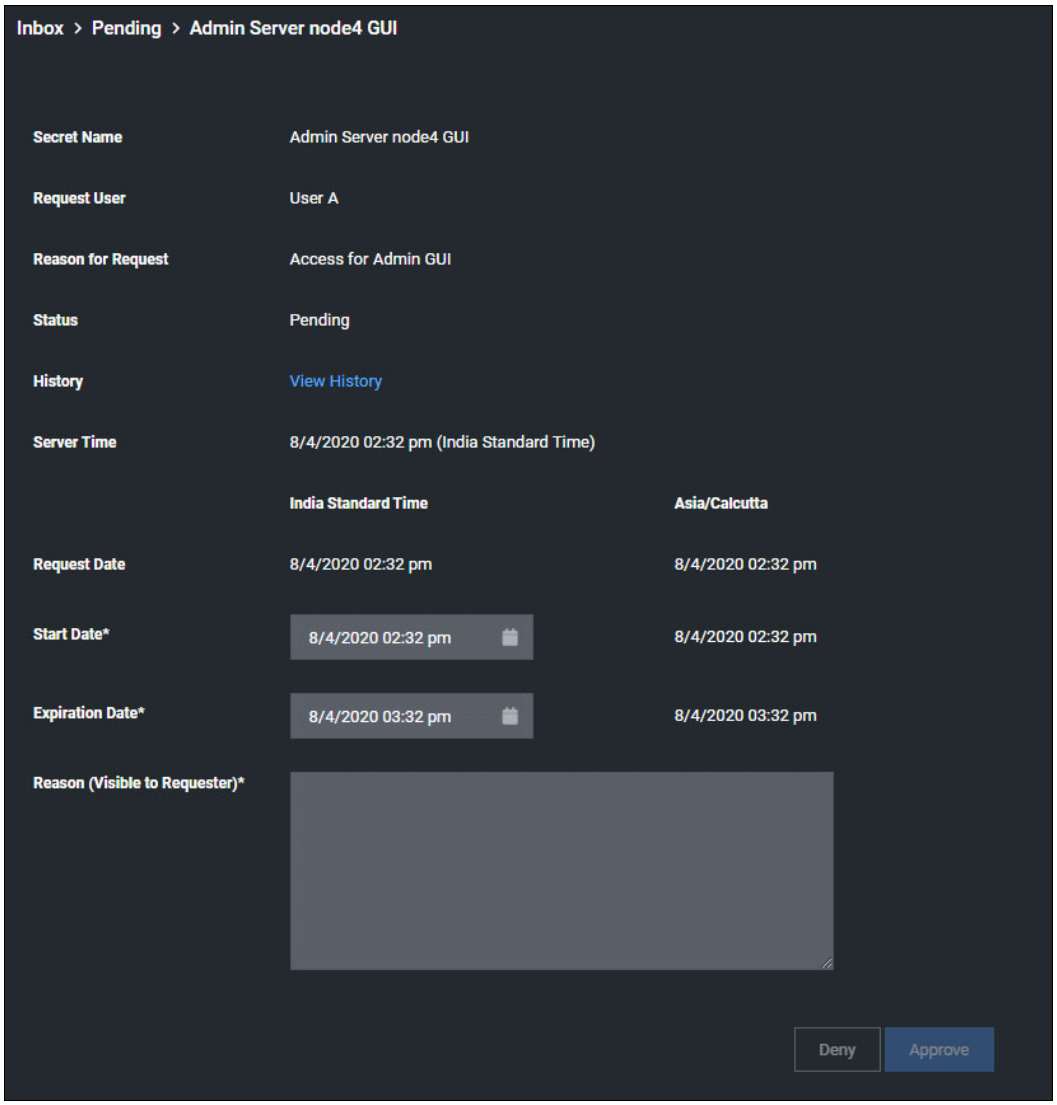


Figure 25 Screen for the manager/approver to approve or deny the login request

Here are more useful features:

- The Verify Privilege Vault administrator can terminate any secret session at any time remotely. This feature is useful in several cases like in one scenario where the administrator sees unsecure usage of the sessions and wants to terminate the access. For more information, see *IBM Security Secret Server Version 10.8 Administration Guide*.
- The Checkout feature can be configured by the Verify Privilege Vault administrator for a set of secrets so that only one user can access the secret at a time. This feature is useful in scenarios where you need a single administrator to access the system at a time for security reasons or serialization or other needs. For more information, see *IBM Security Verify Privilege On-Premises Version 10.9 Administration Guide*.

References

- How to set up the email notification on IBM Security Secret Server 10.7 or above:

  https://www.ibm.com/support/pages/how-set-email-notificaiton-ibm-security-secret-server-107-or-above
- IBM Security Secret Server Features:

  https://www.ibm.com/support/pages/ibm-security-secret-server-features
- *IBM Security Secret Server Version 10.8 Installation Guide*:

  http://public.dhe.ibm.com/software/security/products/isss/10.8.0/isss_basicinstall.pdf
- *IBM Security Secret Server Version 10.8 End User Guide*:

  http://public.dhe.ibm.com/software/security/products/isss/10.8.0/isss_enduserguide.pdf
- *IBM Security Secret Server Version 10.8 Administration Guide*:

  http://public.dhe.ibm.com/software/security/products/isss/10.8.0/isss_adminguide.pdf
- IBM Spectrum Scale at IBM Knowledge Center:

  https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.5/ibmspectrumscale505_welcome.html
- SDK Secret Server Scripting Tool for DevOps:

  https://www.ibm.com/support/pages/node/872206
- Verify Privilege Vault at IBM Knowledge Center:

  https://www.ibm.com/support/knowledgecenter/en/SSWHLP_10.8.0/com.ibm.isss.doc/overview/cpt/whatsnew.html

Authors

This paper was produced by a team of specialists from around the world working with the IBM Redbooks, Tucson Center.

Vincent Hsu is Vice President, IBM® Fellow, and Chief Technical Officer (CTO) for Storage and Software-Defined Infrastructure (SDI). His responsibilities include research and development on future storage technology, storage system architecture, design, and solution integration. Mr. Hsu has devoted his entire 29 years of his career on storage system development. He is a master inventor at IBM. He was named an IBM Fellow in 2012. In 2005, he was named a Distinguished Engineer (executive-level engineer) and Chief Engineer for IBM Enterprise storage. Mr. Hsu is a graduate of the University of Arizona, and holds a Master of Science degree in Computer Engineering and an MBA degree. He is also a member of the IBM Academy of Technology.

Sridhar Muppidi, PhD is an IBM Fellow and Chief Technology Officer in IBM Security Systems. He is an industry recognized technical expert and thought leader in security with 20 years of experience in software product development and security solutions architecture for several industry verticals. Sridhar has an MS and a PhD in computer science from Texas A & M University. He is an IBM Master inventor with 45 patents and has published extensively in technical conferences and journals.

Sandeep R. Patil is a Senior Technical Staff Member who works as a Storage Architect with IBM System Labs. He has over 18 years of product architecture and design experience. Sandeep is an IBM Master Inventor, an IBM Developer Master Author, and a member of the IBM Academy of Technology. Sandeep holds a Bachelor of Engineering (Computer Science) degree from the University of Pune, India.

Kanad Jadhav is a Subject Matter Expert (SME) working in Identity and Access Management with IBM Software Labs. He has 4 years of experience in product support and deployment for IBM Security identity products. He holds a Master of Science (Computer Science) degree from California State University, Long Beach, US.

Sumit Kumar is an Advisory Software Engineer at IBM India. He completed a Master in Computer Application from IGNOU, New Delhi, India, and has 16 years of experience in the software development field. He has been part of IBM ESS deployment code development on IBM POWER8® and IBM POWER9™ processor-based systems, including x86 servers. He also worked on IBM Spectrum Scale and as a deployment developer. Sumit has worked within IBM for over 7 years and previously held roles within the IBM Platform Computing and IBM Systems Director team. He has strong engineering professional skills in software deployment and automation that uses various scripting technologies, such as Python, shell scripting, Ansible, and Linux.

Nishant Singhai is an Advisory Software Engineer working in Identity and Access Management with IBM Software Labs. He has over 12 years of experience in product support and deployment for Identity and Access products. He has delivered technical talks on IBM Security products and wrote many technical articles on IBM Integrated Service Management. Nishant holds a master's degree in scientific computing from the University of Pune, India.

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

Larry Coyne
IBM Redbooks®, Tucson Center

Julio Cesar Hernandez, Glen Jaquette, John T Olson, Christina Orosco, Carl Zetie
IBM Systems

Prashant P Kamat, Elizabeth Silvia, Grey Thrasher, Jane Wilson
IBM Security

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

Stay connected to IBM Redbooks

- Look for us on LinkedIn:

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

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

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

- Stay current on recent Redbooks publications with RSS Feeds:

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

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 Security™	POWER9™
IBM®	IBM Spectrum®	QRadar®
IBM Cloud®	IBM Z®	Redbooks®
IBM Elastic Storage®	POWER8®	Redbooks (logo) ®

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.

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

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

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

REDP-5625-00

ISBN 0738459313

Printed in U.S.A.