

Multi-Factor Authentication Using IBM Security Verify for IBM Spectrum Fusion

Sridhar Muppidi, PhD

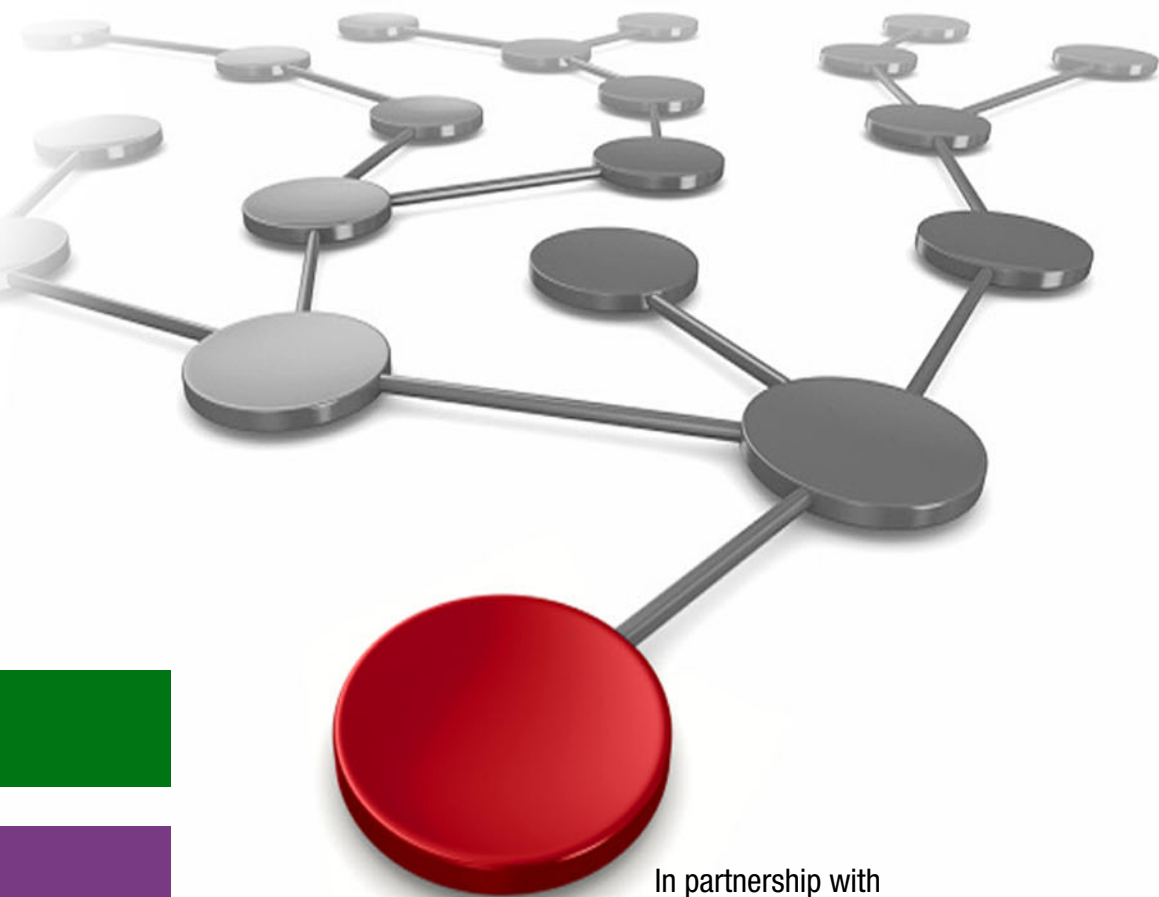
Vincent Hsu

Sandeep Patil

Vivek Jain

Vrushal Chaudhari

Rahul Nema



 **Security**

Storage

In partnership with
IBM Academy of Technology



Introduction

Data is the new crown jewel of any organization. The use of Multi-Factor Authentication (MFA) to safeguard the most critical asset of any organization (the data) became a high-priority need. MFA verifies the identity of the consumers by applying multiple methods that provide an extra layer of security in addition to the login credentials. Regulatory compliances exist that require MFA, such as PCI DSS v3.2, NIST SP 800-171, and DFS 23 NYCRR 500. Implementation of MFA reduces the risk and increases the security posture of your deployments.

Storage is where the data resides. *Compute* is where the application processes the data. In hyperconverged systems, both storage and compute are converged. Therefore, it is critical to have an enhanced security posture for such infrastructure setups. Deployment of an MFA solution with a hyperconverged system is one key security feature where access to such a system should mandate MFA to its consumers.

This paper describes the integration of IBM Spectrum Fusion® Hyperconverged Infrastructure (HCI) with IBM Security™ Verify, which ensures MFA for users who access IBM Spectrum Fusion HCI.

IBM Spectrum Fusion Hyperconverged Infrastructure

IBM® Spectrum Fusion is a hyperconverged configuration of the Red Hat OpenShift Container Platform (OCP). It is a simple turn-key enterprise-grade solution to deploy Red Hat OpenShift and a hybrid cloud data platform.

The following are key highlights of IBM Spectrum Fusion HCI:

- ▶ Integrated HCI appliance for containers
- ▶ Highly scalable containerized file system with erasure coding
- ▶ Data resilience for local and remote backup and recovery
- ▶ Simple installation and maintenance of hardware and software
- ▶ Global data-platform for storage resources
- ▶ IBM Cloud® Satellite™ and Red Hat Advanced Cluster Management (ACM) for Kubernetes native integration
- ▶ Ready for artificial intelligence (AI) applications with optional NVIDIA A100 GPUs
- ▶ Starts small with six servers and scales up to 20

IBM Spectrum Fusion HCI is an ideal hyperconverged system for application modernization.

For more information, see the IBM Storage Solution Brief: [IBM Spectrum Fusion HCI](#)

IBM Security Verify

IBM Security Verify (ISV) is a single identity-as-a-service (IDaaS) solution that delivers both workforce modernization and consumer digital transformation. IBM Security Verify protects users and applications both inside and outside the enterprise, while it enables technical agility and operational efficiency as a cloud-native solution.

Beyond single-sign on and multi-factor authentication, IBM Security Verify is a modernized, modular IDaaS that provides the following features:

- ▶ Deep AI-powered context for risk-based authentication and adaptive access decisions
- ▶ Guided experiences for developer time-to-value and comprehensive cloud-Identity
- ▶ Access management (IAM) capabilities

From privacy and consent-management to holistic risk-detection and identity-analytics, IBM Security Verify centralizes workforce and consumer IAM for any hybrid cloud deployment.

IBM Security Verify provides centralized user management, password-less authentication, risk-based authentication, and out-of-the-box Multi-Factor Verification.

Configure MFA for IBM Spectrum Fusion HCI with IBM Security Verify

This section describes the IBM Spectrum Fusion authentication modules and how they can be configured with IBM Security™ Verify to achieve MFA.

IBM Spectrum Fusion authentication and identity

IBM Spectrum Fusion authentication and identity are a core set of services that enable IBM Spectrum Fusion to provide a seamless experience while working with OpenShift. It establishes a Single Sign On (SSO) for management and storage software with OpenShift, which enables seamless access to the platform that provides multiple options to be used for authentication and authorization. Therefore, the solution supports a wide variety of Identity Providers starting from simple ones (such as file-based), to LDAP, to complex OpenID providers (such as Google and IBM).

Since IBM Spectrum Fusion HCI authentication is based completely on OCP authentication modules, IBM Security Verify can be easily integrated to implement MFA using OpenID Connect. This section describes the configuration for IBM Spectrum Fusion HCI with IBM Security Verify as the OpenID Connect identity provider. The process uses the authorization code flow such that both the first- and second-factor authentication for users is governed by IBM Security Verify. You can customize the setup such that the user is authenticated (first-factor) through the local Active Directory or LDAP while the second-factor authentication occurs through IBM Security Verify.

The OpenShift Container Platform master includes a built-in OAuth server. Users obtain OAuth access tokens to authenticate themselves to the API. The IBM Spectrum Fusion

Management GUI and Storage Software are configured by default with self-SSO. This means that all user-authentication for IBM Spectrum Fusion Management occurs through the configured OCP authentication console.

In this setup, the default IBM Spectrum Fusion HCI configuration is used and OAuth is configured as IBM Security Verify, which is an OpenID Connect Identity provider.

Note: The IBM Spectrum Protect Plus component that is shipped with IBM Spectrum Fusion HCI version 2.1.0 and used for backup and restore does not support OCP SSO and therefore is not covered in this paper.

Note: IBM Security Verify provides various advanced identity-features that can be deployed by practitioners. This paper covers only the multi-factor authentication scenario as an example of the identity features.

Setup details

Figure 1 shows the high-level setup that is used in this paper for demonstration of IBM Spectrum Fusion MFA using IBM Security Verify.

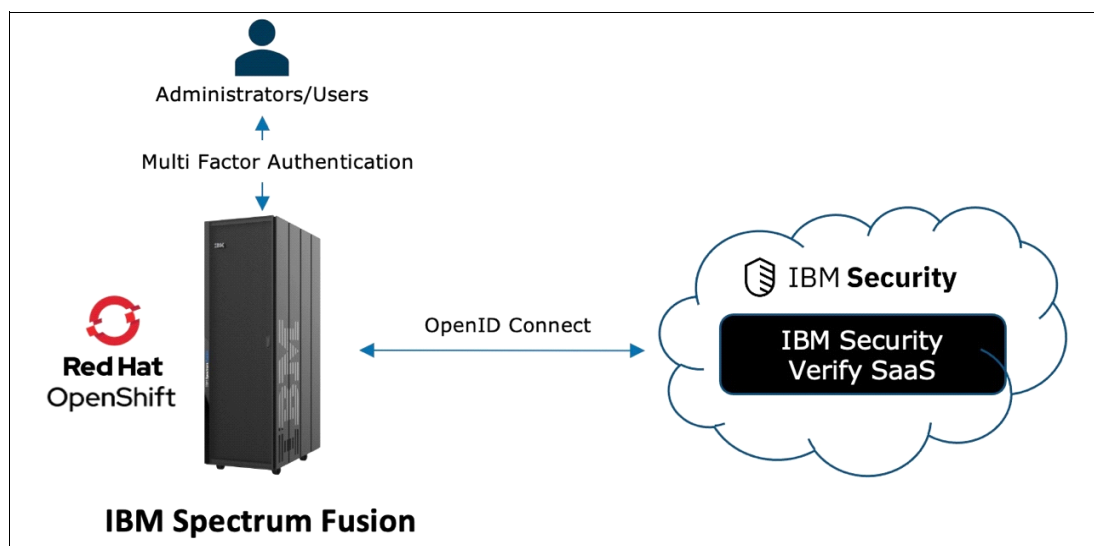


Figure 1 High-level setup: IBM Spectrum Fusion with IBM Security Verify

IBM Spectrum Fusion Version 2.1.0 with Red Hat OpenShift 4.7.16 is used for demonstration.

Configuration steps

This section describes the configuration steps that are required by the system administrator for IBM Security Verify and IBM Spectrum Fusion:

1. Create a trial account on ISV using following link.
<https://www.ibm.com/security/digital-assets/iam/verify-demo-trial/>
2. Log in to ISV as an administrator, as follows:
 - a. Go on the Account URL that you received from ISV after registration. See Figure 2.
<https://<company-name>.verify.ibm.com/ui/admin>

b. Log in using your registered email.

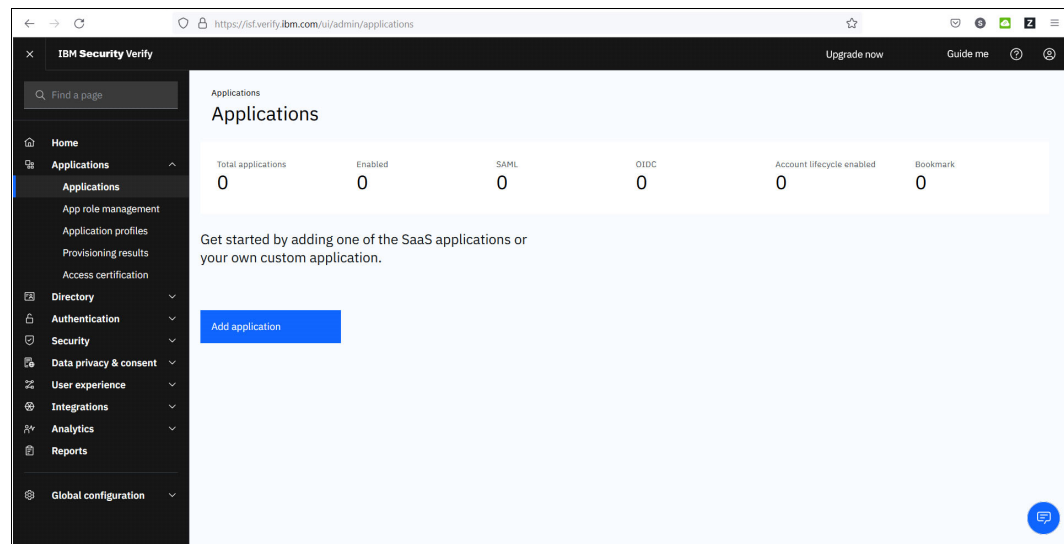


Figure 2 ISV console

3. Add IBM Spectrum Fusion OCP as an application on ISV, as follows:
 - a. Click the **Navigation drawer** menu icon on the upper-left, click **Applications**, and select **Applications** from the expanded list.
 - b. Click **Add application**, search for OpenShift, select Red Hat OpenShift, and click.
The following three tabs options are on the Red Hat OpenShift window:
 - General
 - Sign-on
 - Account lifecycle

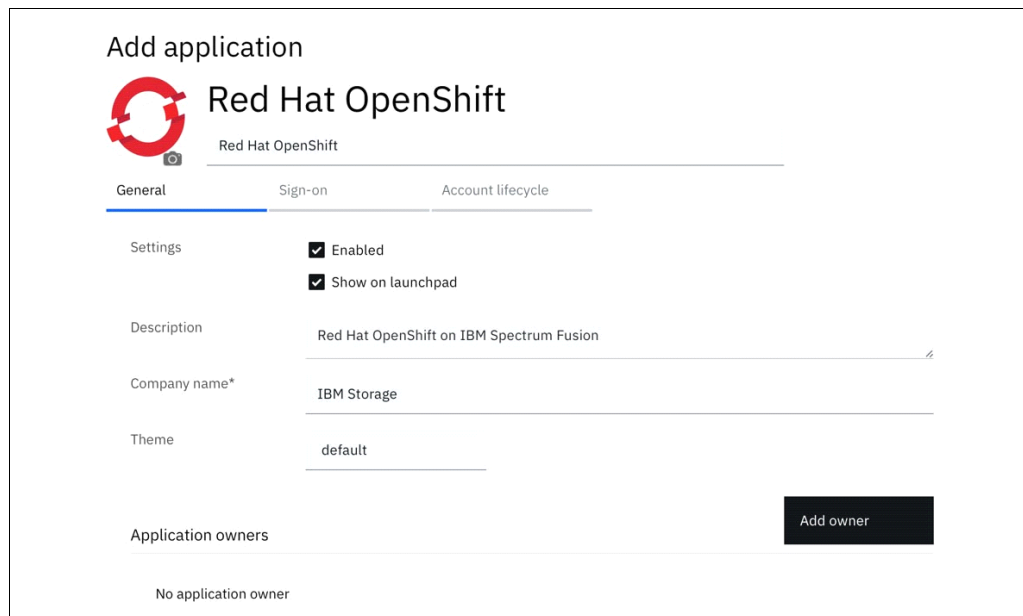


Figure 3 ISV application configuration - General tab

- c. On the **General** tab, change the **Description** and **Company Name** as required. See Figure 3.
- d. Select the **Sign-on** tab and change following fields:
 - i. If you know your OpenShift cluster console URL, enter it In the application URL, enter your OpenShift cluster console URL. For example:
`https://console-OpenShift-console.apps.*****.***.*****.ibm.com/`
 If you do not know your OpenShift cluster console URL on IBM Spectrum Fusion, use the following instructions:
 - 1.) Log in to IBM Spectrum Fusion Dashboard.
 - 2.) Click the **Navigation drawer** menu icon on the upper-left.
 - 3.) Click **OpenShift Console**.
 - 4.) Copy the Console URL, as shown in Figure 4.

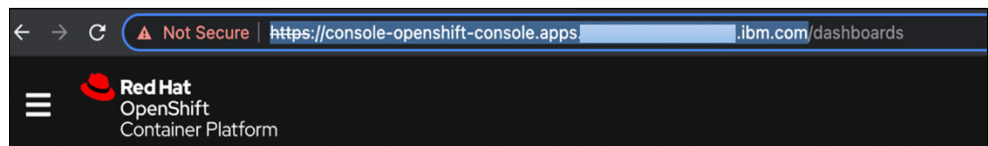


Figure 4 OpenShift console URL

- ii. Formulate the Dashboard URL and Redirect URI as follows:
 - Dashboard URL:
`https://console-OpenShift console.apps.*****.***.*****.ibm.com/`
 - Redirect URI:
`https://oauth-OpenShift.apps.*****.***.*****.ibm.com/oauth2callback/openid`

From the Dashboard URL, replace **console-openshift-console** with **oauth-openshift** and append **oauth2callback/openid** at the end.

In Figure 5, the Redirect URI is
`https://oauth-OpenShift.apps.*****.***.*****.ibm.com/oauth2callback/openid`

Add application

Red Hat OpenShift

Red Hat OpenShift

General **Sign-on** Account lifecycle

Sign-on method* Open ID Connect 1.0

Application URL* https://console-openshift-console.apps. .it

Grant types ☒ Authorization code

Client ID (Generated on save)

☐ Public client (no client secret)

Client secret (Generated on save)

User consent Ask for consent

Redirect URIs* https://oauth-openshift.apps. .ibm

Figure 5 ISV application configuration - Sign-on tab

iii. Scroll down the **Sign-on** tab (which is shown in Figure 5), to set the fields for Access policies, as follows:

1.) Clear the **Use default policy** checkbox and click the edit icon. See Figure 6.

Access policies

Choose the identity sources that can be used to sign in to this application.

☒ Allow all identity sources that are enabled for end users (2 sources) ⓘ

☐ Select specific supported identity sources

Set the access policy to control how users can access the application.

Settings ☐ Use default policy

(Select an access policy)

Figure 6 ISV application configuration - Access policies change

2.) Select **Always require 2FA in all devices** and click **OK**. See Figure 7.

Access policies	Description
Allow access from all devices	Always prompt users to complete a second factor authentication every time the users access an application from desktops and from mobile devices.
Always require 2FA in all devices	
Require 2FA each session in all devices	

Cancel OK

Figure 7 ISV application configuration - Required Access policy selection

- e. Select the **Entitlements** tab and select **Automatic access for all users and groups** and click **Save**, as shown in Figure 8.

Applications / Details

Red Hat OpenShift

Red Hat OpenShift

General Sign-on Account lifecycle **Entitlements**

Access Type

☒ Automatic access for all users and groups

☐ Approval required for all users and groups

☐ Select users and groups, and assign individual accesses

Delete

Cookie Preferences

Cancel Save

Figure 8 ISV application configuration - Entitlements tab

- f. Select the **Sign-on** tab. Copy and save the **Client ID**, **Client secret**, and **Issuer URL**, as shown in Figure 9. These fields are used in step 5.b. vi on page 9.

Figure 9 ISV application configuration - Sign-on tab after configuration is complete

4. Add users (in ISV) who will log in to IBM Spectrum Fusion and to whom you want MFA to be mandated, as follows:
 - a. Click the **Navigation drawer** menu icon on the upper-left, click **Directory**, and select **Users&Groups**.
 - b. Click **Add user** → Select **Identity source as Cloud Directory** → Enter other details → Click **Save**.

The added users are sent an email that contains the link that they must click to reset the password.

The examples in this paper refer to **User Name John**.

5. Set cluster settings for configuring IBM Spectrum Fusion with IBM Security Verify, as follows:
 - a. Log in to IBM Spectrum Fusion Dashboard. Click the **Navigation drawer** menu icon on the top-left and click **OpenShift Console**.
 - b. Log in to your OpenShift web console using the admin userID (kubeadmin), as follows:
 - i. Scroll down and click **Administration** from the left menu.
 - ii. Click **Cluster Settings**.
 - iii. Navigate to the **Global Configuration** tab.
 - iv. Select **OAuth**, as shown in Figure 10.

These steps are also documented in the **Sign-On** tab in ISV.

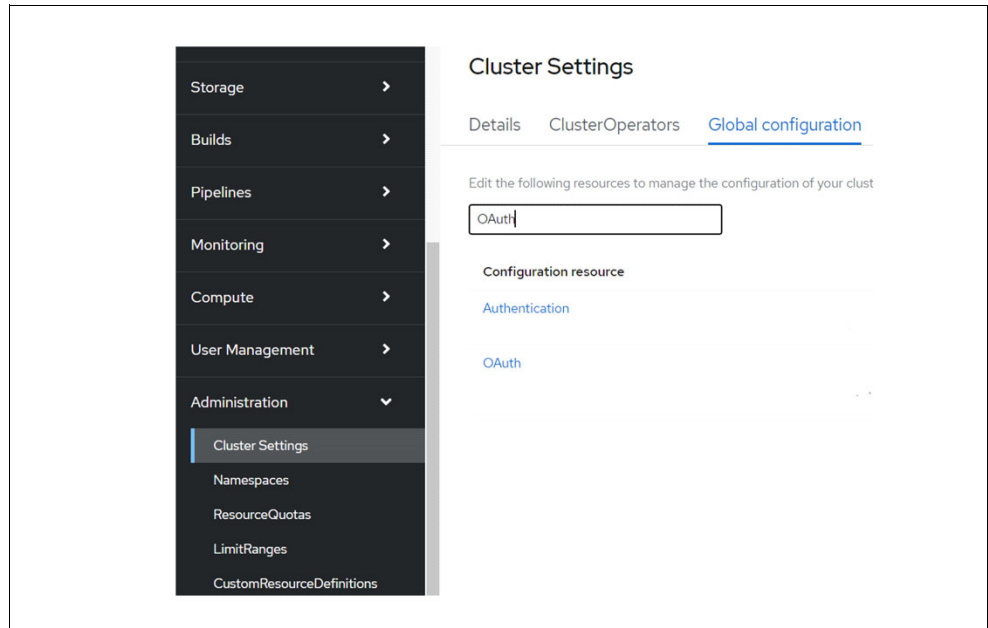


Figure 10 OpenShift Console (**Administration** → **Cluster Settings** → **OAuth Selection**)

- v. In the Identity Providers section, select OpenID Connect from the Add list.
- vi. Specify the following settings on the **Add Identity Provider: OpenID Connect** page as shown in Figure 11.

Name	Provide a meaningful name for this field, which will be used in the redirect URL. In Figure 11, the name is openid . (We are declaring openid as the redirect URL in ISV, so openid is used as the name.)
Client ID	Provide the Client ID attribute value that is generated when you save the OpenID Connect application for Red Hat OpenShift in step 3.f on page 7.
Client Secret	Provide the Client secret attribute value that is generated when you save the OpenID Connect application for Red Hat OpenShift in step 3.f on page 7.
Issuer URL	Provide the Issuer URL value from ISV in step 3.f on page 7.

- vii. Click **Add**.

Add Identity Provider: OpenID Connect

Integrate with an OpenID Connect identity provider using an Authorization Code Flow.

Name *

 Unique name of the new identity provider. This cannot be changed later.

Client ID *

Client secret *


Issuer URL *

 The URL that the OpenID provider asserts as its issuer identifier. It must use the https scheme with no URL query parameters or fragment.

Figure 11 OpenShift Console - Add Identity Provider

6. Log in to IBM Spectrum Fusion - OpenShift Container Platform with MFA enabled, as follows:
 - a. Log in to OCP with MFA provided by ISV.
 - b. Using Incognito mode, log in to the OpenShift Container Platform web console. Select **openid** as the login method, as shown in Figure 12.

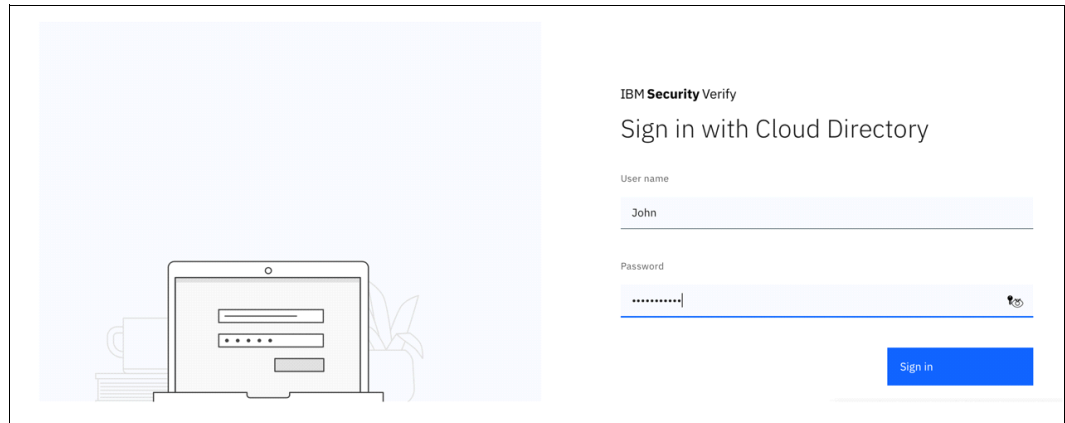
Log in with...



Red Hat
OpenShift Container Platform

Figure 12 OpenShift console login using openid

- c. Log in to ISV as the user (John) that was created in step 4.b on page 8. See Figure 13.



IBM Security Verify

Sign in with Cloud Directory

User name

John

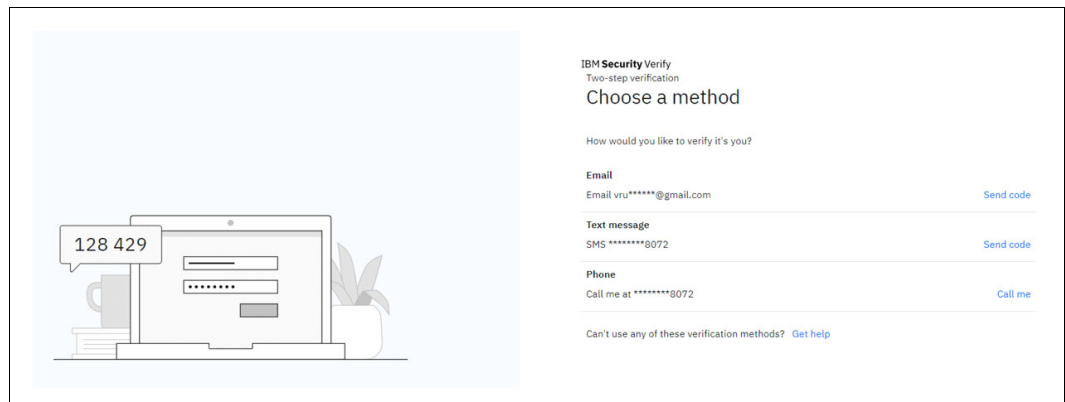
Password

.....

Sign in

Figure 13 ISV login to ISV

- d. Choose a method for the two-factor authentication, as shown in Figure 14.



IBM Security Verify

Two-step verification

Choose a method

How would you like to verify it's you?

Email

Email vru*****@gmail.com [Send code](#)

Text message

SMS *****8072 [Send code](#)

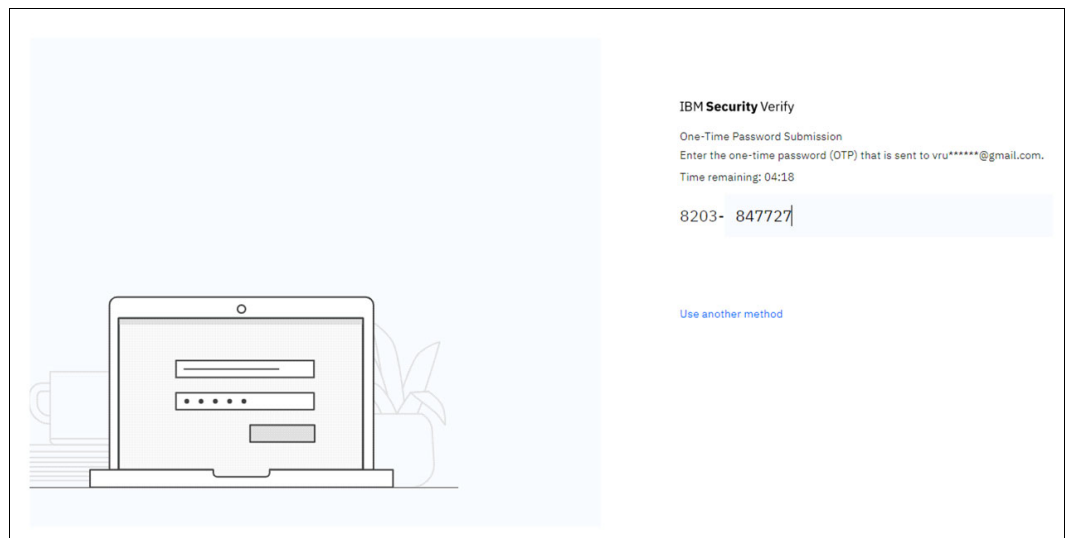
Phone

Call me at *****8072 [Call me](#)

Can't use any of these verification methods? [Get help](#)

Figure 14 ISV - choose MFA method

- e. Enter the one-time passcode (OTP), as shown in Figure 15.



IBM Security Verify

One-Time Password Submission

Enter the one-time password (OTP) that is sent to vru*****@gmail.com.

Time remaining: 04:18

8203- 847727

[Use another method](#)

Figure 15 ISV - Enter the OTP for MFA

- f. Click **Continue on next page** and select **Continue**, as shown in Figure 16.

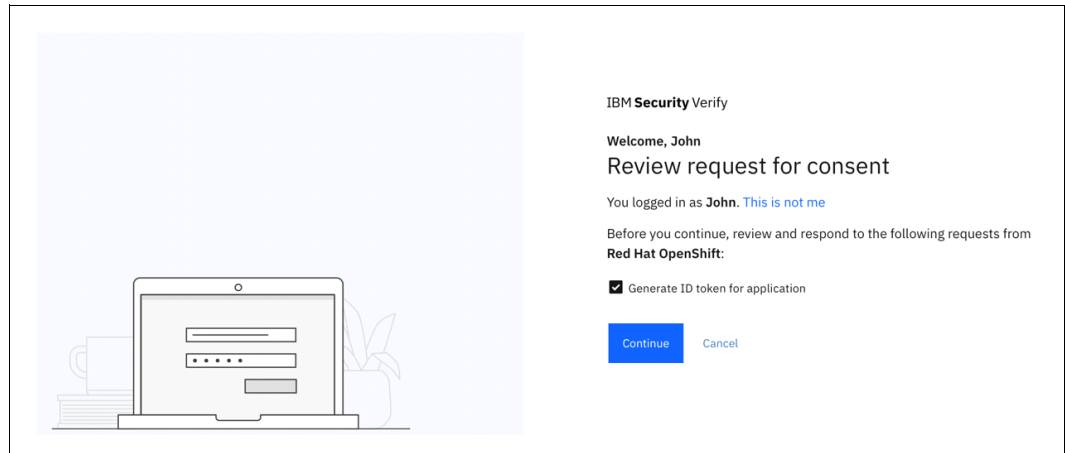


Figure 16 Accepting permission for adding user to OpenShift

7. Add a role to the OpenShift user (John) that was added in step 4.b on page 8, as follows:
 - a. Go back to OpenShift Console where kube:admin is logged in.
 - b. Click **User Management** → **Users** and select the newly-added user (John). See Figure 17.

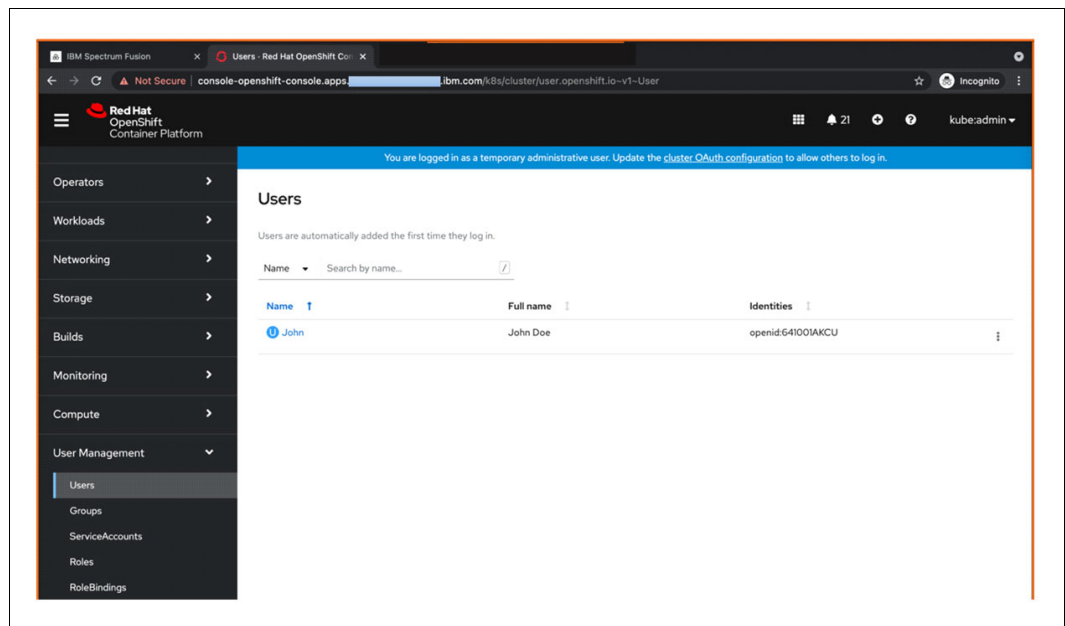


Figure 17 Checking in OpenShift Console to verify that the new user was added

- c. Click **RoleBindings** → **Create binding**, as shown in Figure 18.

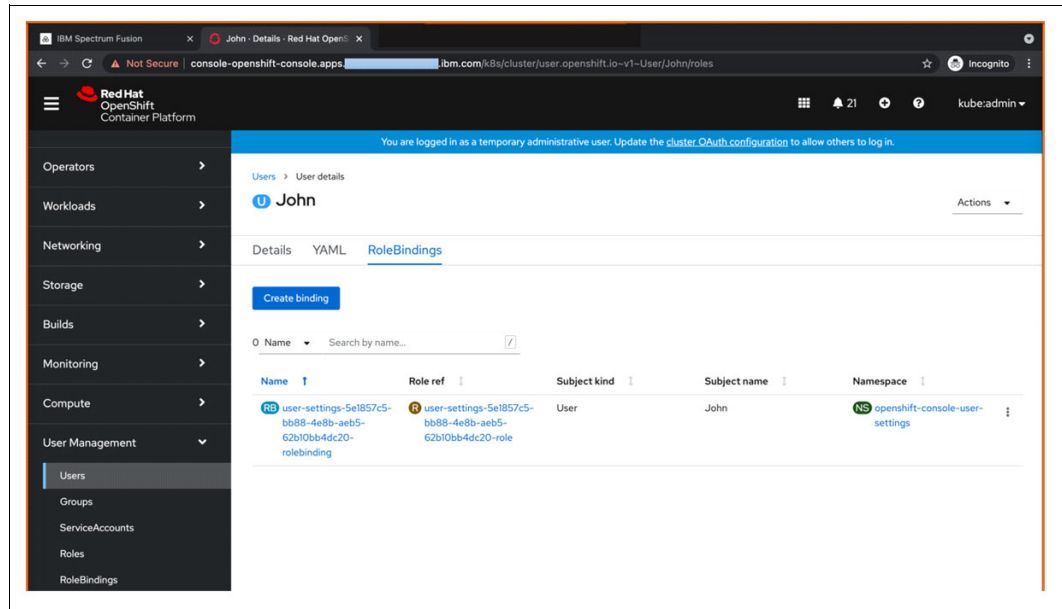


Figure 18 Role Bindings

- d. Set the following fields:
 - i. For **Binding type**, select **Cluster-wide role binding (ClusterRoleBinding)**.
 - ii. In **Role Binding** → **Name**, provide a unique name.
 - iii. In **Role** → **Role name**, select **cluster-admin**, as shown in Figure 19. (Based on your requirement, you can also select **view** as the **Role name**.)

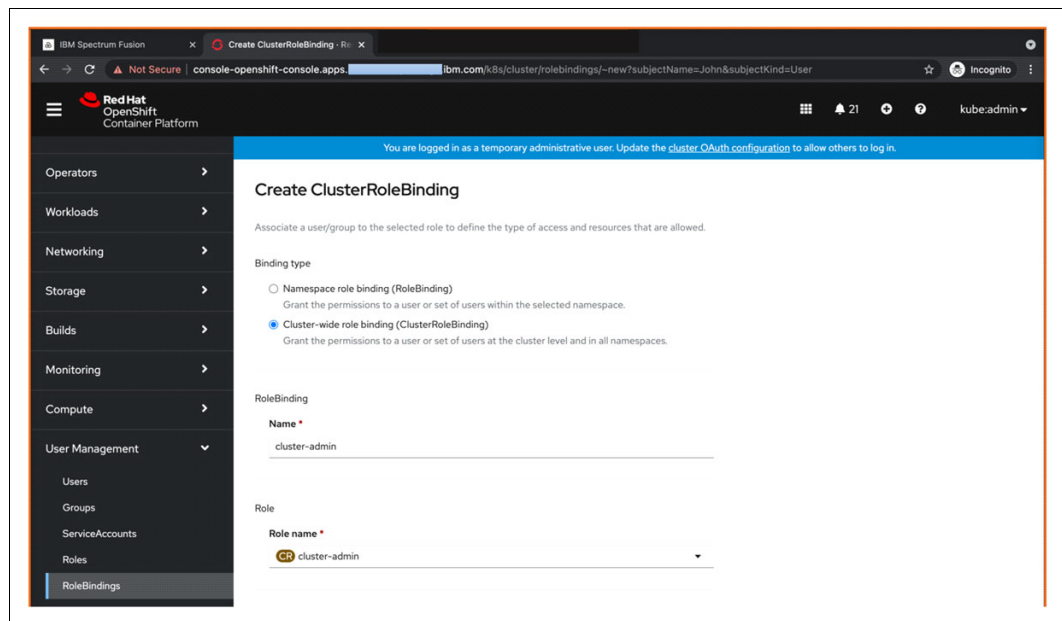


Figure 19 Create ClusterRoleBinding for user

- iv. Click **Create**.
8. Access the IBM Spectrum Fusion Management GUI using the added user, as follows:
 - i. Go to incognito mode, and go to IBM Spectrum Fusion GUI address.

- ii. Click **Get Started** → **openid** and log in using the newly-added user (John) in ISV, as shown in Figure 20.

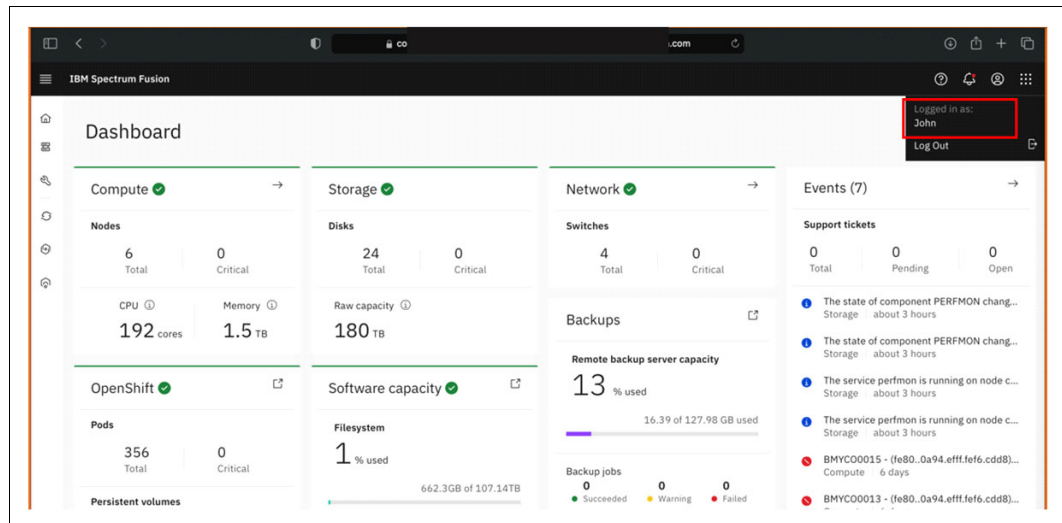


Figure 20 IBM Spectrum Fusion Dashboard with user logged in

9. Access the IBM Spectrum Storage Software GUI using the newly-added user, as follows:
 - i. Click the **Navigation drawer** menu icon on the top-left.
 - ii. Select **Storage Software** and click **Sign in with Red Hat single sign-on (with MFA)** to log in to IBM Spectrum Scale GUI with ISV user (John). See Figure 21.

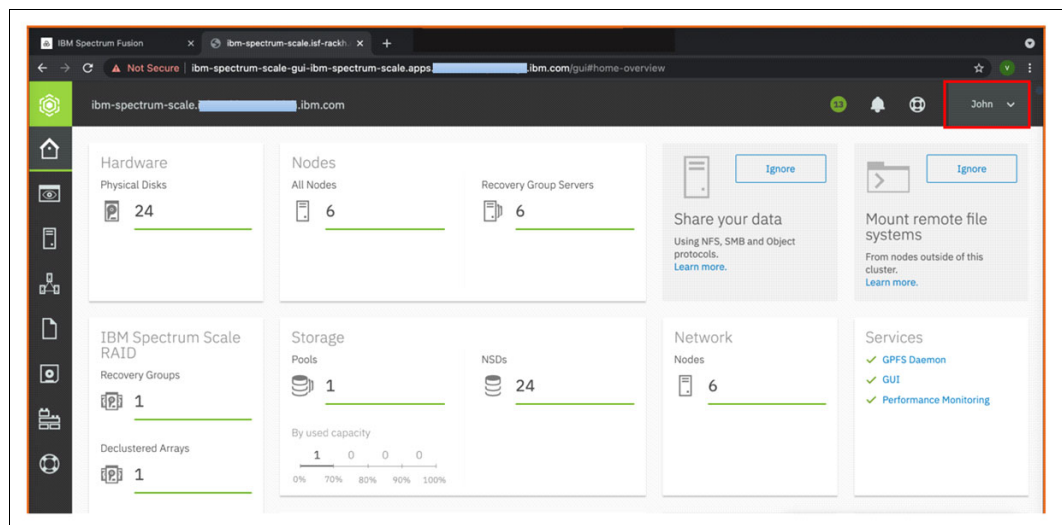


Figure 21 IBM Spectrum Scale GUI console with user logged in

OCP CLI user login

Direct login to OpenShift command line interface (CLI) for users who are registered for MFA with ISV does not work. The users need to obtain a login token from OpenShift web console after successful MFA login to the GUI console and then use that token to log in through CLI. This procedure ensures that the login to CLI also mandates MFA and ensures the required security.

To log in to OCP, follow these steps:

1. Log in to OpenShift console as user (John) created on ISV in step 4.b on page 8.
2. Click the username on the upper-right and select **Copy Login command**. See Figure 22.

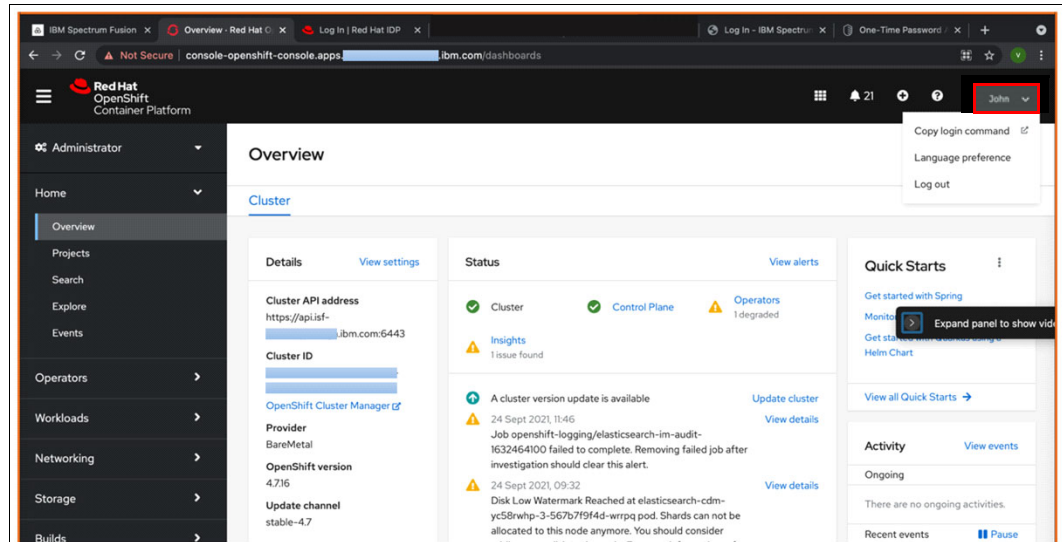


Figure 22 OpenShift console with user logged in

3. If the login prompt opens again, select **openid**. Click **Display Token** and copy the command Login with this token. See Figure 23.

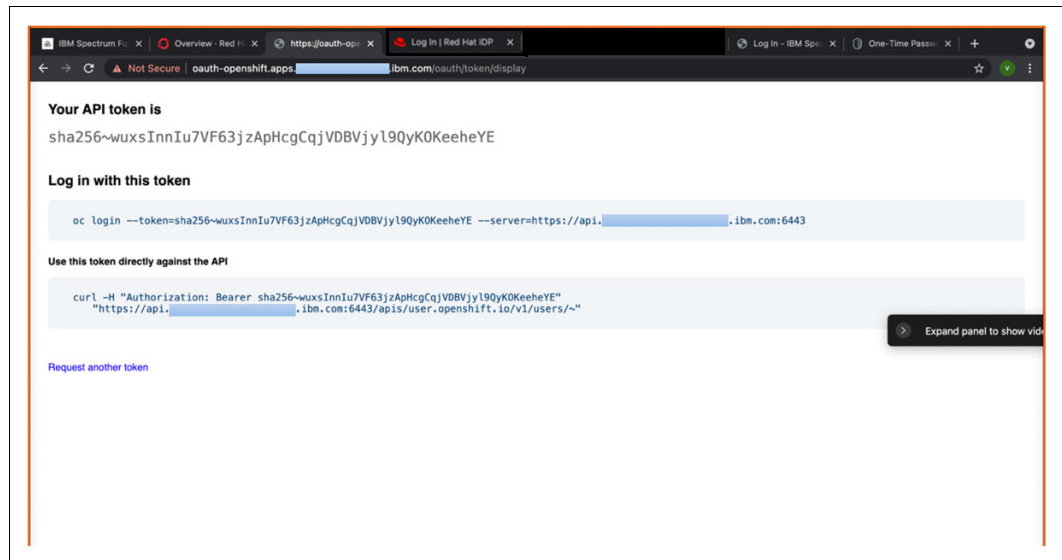
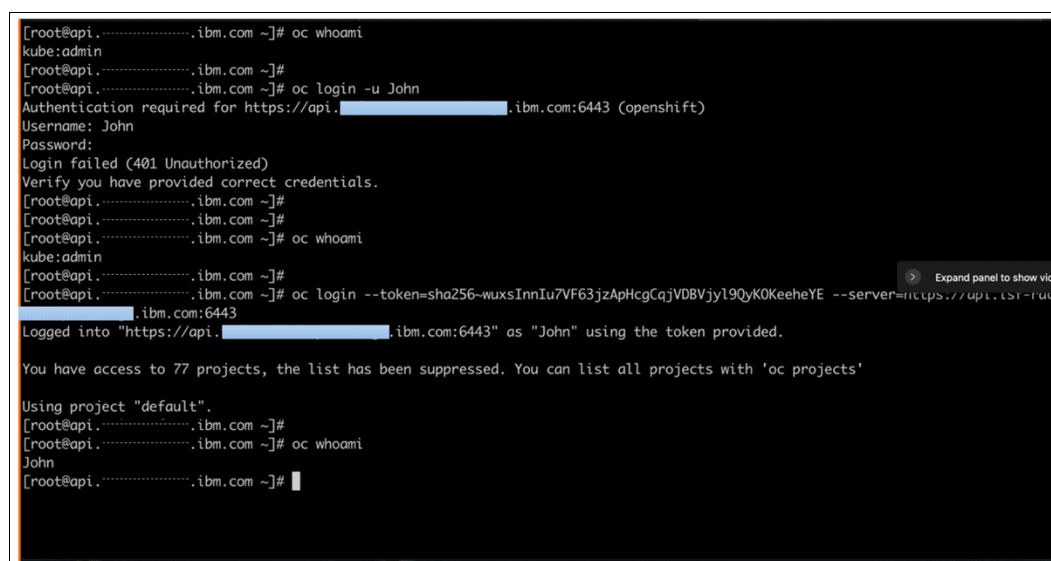


Figure 23 OpenShift page with user API token

4. Paste the copied command on OpenShift CLI. See Figure 24.

A terminal window showing the OpenShift CLI login process. The user is at a root prompt on a machine named 'api'. They run 'oc whoami' and get 'kube:admin'. Then they run 'oc login -u John'. The prompt asks for authentication for 'https://api. [redacted] .ibm.com:6443 (openshift)'. The user enters 'John' as the username and a password. The login fails with a 401 Unauthorized error, stating 'Verify you have provided correct credentials.' The user then runs 'oc login --token=sha256-wuxsInnIu7VF63jzApHcgCqjVDBVjyl9QyK0KeeheYE --server=https://api. [redacted] .ibm.com:6443'. The login is successful, showing 'Logged into "https://api. [redacted] .ibm.com:6443" as "John" using the token provided.' and 'You have access to 77 projects, the list has been suppressed. You can list all projects with \'oc projects\''. The user then runs 'oc whoami' and gets 'John'.

```
[root@api. ....ibm.com ~]# oc whoami
kube:admin
[root@api. ....ibm.com ~]#
[root@api. ....ibm.com ~]# oc login -u John
Authentication required for https://api. [redacted] .ibm.com:6443 (openshift)
Username: John
Password:
Login failed (401 Unauthorized)
Verify you have provided correct credentials.
[root@api. ....ibm.com ~]#
[root@api. ....ibm.com ~]#
[root@api. ....ibm.com ~]# oc whoami
kube:admin
[root@api. ....ibm.com ~]#
[root@api. ....ibm.com ~]# oc login --token=sha256-wuxsInnIu7VF63jzApHcgCqjVDBVjyl9QyK0KeeheYE --server=https://api. [redacted] .ibm.com:6443
Logged into "https://api. [redacted] .ibm.com:6443" as "John" using the token provided.
You have access to 77 projects, the list has been suppressed. You can list all projects with 'oc projects'

Using project "default".
[root@api. ....ibm.com ~]#
[root@api. ....ibm.com ~]# oc whoami
John
[root@api. ....ibm.com ~]#
```

Figure 24 Login with user John on command line

You are now logged in to the OpenShift CLI with your ISV user (John).

Reminder: You cannot log in directly to the OpenShift CLI using ISV user (John). You must perform MFA, obtain the token, and then login.

Conclusion

This Redpaper describes the steps of configuring IBM Spectrum Fusion HCI with IBM Security Verify to enable Multi-Factor Authentication for IBM Spectrum Fusion HCI users and administrators.

References

- ▶ IBM Security Verify IBM documentation
<https://www.ibm.com/docs/en/security-verify?topic=SSCT62/com.ibm.iamservice.doc/kc-homepage.html>
- ▶ IBM Spectrum Fusion IBM documentation:
<https://www.ibm.com/docs/en/spectrum-fusion/2.1?topic=product-overview>
- ▶ Red Hat OpenShift Authentication documentation:
<https://docs.openshift.com/container-platform/4.7/authentication/understanding-authentication.html>

Authors

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

Sridhar Muppidi, PhD is an IBM Fellow and Chief Technology Officer (CTO) 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 holds a Master of Science degree 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.

Vincent Hsu is Vice President, IBM Fellow, and 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 the entire 29 years of his career to 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 a member of the IBM Academy of Technology.

Sandeep Patil is a Senior Technical Staff Member who works as a Storage Architect with IBM System Labs. He has more than 18 years of product architecture and design experience. Sandeep is an IBM Master Inventor, an IBM developerWorks® 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.

Vivek Jain is working as a Senior Software Engineer with IBM Security. He has extensive experience on identity and access-management. He is currently working on IBM Security Verify and is passionate about Solution integration.

Vrushal Chaudhari is a Software Engineer with IBM Systems Development Lab. He has worked with the IBM Spectrum Scale Container Storage Interface (CSI) team for two years. Vrushal holds a Bachelor of Engineering (Information Technology) degree from the University of Pune, India. His area of interest is application-containerization with storage and security for containers.

Rahul Nema is a software architect with IBM India. He is a veteran in Hybrid Cloud Solutions, having worked for 15+ years on various Cloud offerings of IBM. Rahul holds a degree in Civil Engineering from NIT Silchar. His areas of expertise span Cloud and Storage domains. He shares his experience and opinions on building Hybrid Cloud Solutions through his articles.

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

- ▶ Larry Coyne
IBM Redbooks®, Tucson Center
- ▶ Hugh Hockett
- ▶ Sumant Padbidri
- ▶ Pallavi Singh
- ▶ IBM Systems

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

- ▶ Find 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.

developerWorks®


IBM®

IBM Cloud®

IBM Security™

IBM Spectrum®

Redbooks®

Redbooks (logo) ®

Satellite™

The following terms are trademarks of other companies:

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

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



REDP-5662-00

ISBN 0738460249

Printed in U.S.A.

Get connected

