TECHNICAL WHITE PAPER

Security Hardening Best Practices

David Siles, Marcus Faust, Drew Russell, Damani Norman, Marc Creviere

June 2021
RWP-0561

TABLE OF CONTENTS

ABSTRACT

Security is an important part of any data management system. When security is compromised, attackers can disrupt, steal and destroy a company's valuable data. Data management systems are not immune to this type of behavior from attackers. Rubrik strives to protect its customer's valuable data by providing features and best practices that ensure security. This guide provides details on Rubrik's recommended best practices for securing Rubrik Cloud Data Manager (CDM) and Rubrik Polaris against unauthorized use.

The content of this document is based on the features and functionality available in Rubrik Cloud Data Management (CDM) v5.2 and Rubrik Polaris as of July 2020. Some of the recommended best practices may not be available in prior versions of these products. While Rubrik Polaris is automatically kept up to date for customers, it is a recommended best practice that Rubrik CDM be kept up to the latest version. Security is an ongoing concern for Rubrik and new methods and features are added to each product release.

ACCOUNT SECURITY

There are three types of accounts used by Rubrik. These are local accounts, domain or external accounts and API access. Local accounts are those that are local to the Rubrik CDM appliance or Polaris. They are maintained by the local administrator of these applications. Domain or remote accounts are accounts in an external identity store, such as Microsoft Active Directory (AD). These accounts are maintained outside Rubrik CDM and/or Polaris. They are granted access to operate the application on an individual or group basis. API access is given via a local or domain/remote account. Tokens can be used with API access to give time limited access to Rubrik CDM or Polaris.

LOCAL ACCOUNT SECURITY

The following best practices are recommended for local accounts in Rubrik CDM and Polaris.

Use strong and unique passwords - When selecting a password to use with Rubrik CDM or Polaris, it should be sufficiently complex as to make it hard to guess or brute force attack. Several articles exist on what constitutes a strong password. In general this should be a password with a minimum length of 8 characters, use upper and lower case letters, have at least one number and one special character. Rubrik CDM 4.1 implements a new default setting for passwords. The "zxcvbn" library of Dropbox is used to prevent using weak or easily guessed passwords in the following areas:[1]

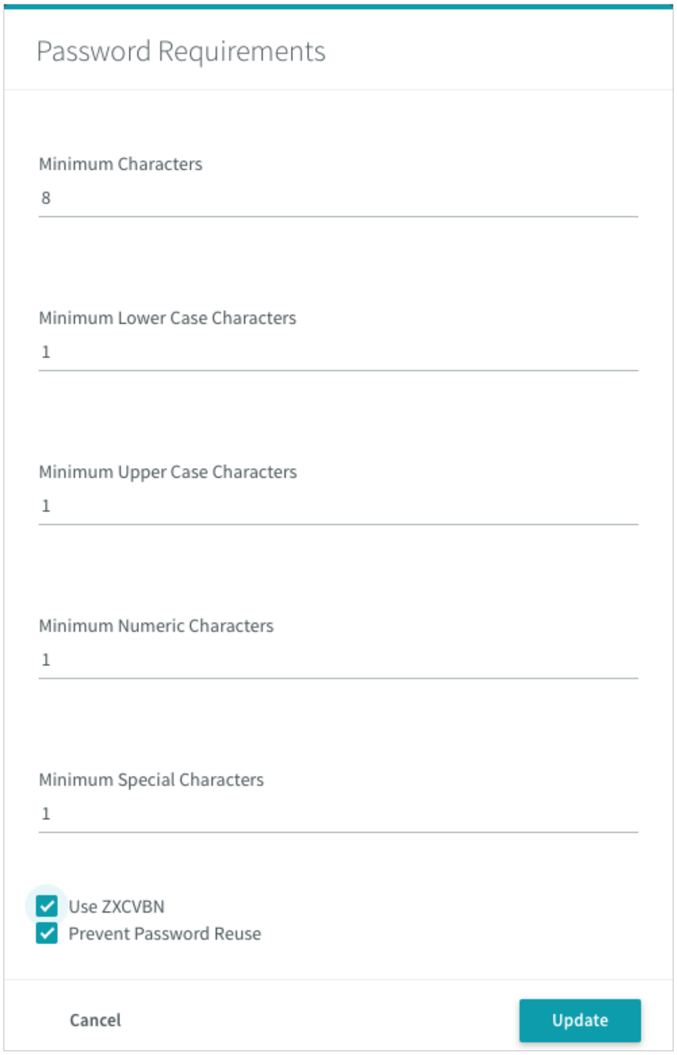
- Bootstrap and setting up "admin" user.
- Local users, including the "admin" user.
- Archival locations (for example, NFS)

It is strongly recommended to use machine generated long passwords (32 characters or more) for any administrative user.

In Rubrik CDM, the use of unique passwords can also be enforced. By enabling Prevent Password Reuse, the cluster will not allow passwords to be re-used when they are changed.

Strong and unique passwords can be enforced by Rubrik CDM. This setting for password requirements can be found under the **Gear icon ⚙ ➔ Users (under Access Management) ➔ Select the Ellipsis (...) ➔ Password Requirements**.

[1] https://support.rubrik.com/s/article/000001333



Password Requirements

Minimum Characters
8

Minimum Lower Case Characters
1

Minimum Upper Case Characters
1

Minimum Numeric Characters
1

Minimum Special Characters
1

☑ Use ZXCVBN
☑ Prevent Password Reuse

Users should refer to the configuration section in the Rubrik CDM User Guide for detailed steps on configuring Password Requirements.

Rotate passwords - Passwords should be changed periodically (30-90 days). This provides a level of security whereby if a password is compromised, the exposure will be short-lived.

No password re-use across clusters or instances - Each Rubrik CDM cluster and Polaris instance should have a unique set of passwords. This is especially true for any of the default users, such as admin. This best practice will help to prevent one compromised set of credentials from being used across multiple systems.

Multi-factor Authentication (MFA) - Rubrik CDM and Polaris have multiple options for MFA. Rubrik recommends that MFA be used on all accounts: local, LDAP, or SSO.

Rubrik CDM has native Time-based One-Time Password (TOTP) support (version 5.2.3+) using common authenticator applications installed on mobile devices or as a browser plugin. Local or LDAP user authentication can be configured with Rubrik TOTP and will require one-time enrollment by each user. SAML 2.0 identity providers as well as RSA SecurID servers are also supported by Rubrik CDM. Most external SAML 2.0 identity providers support MFA, allowing the SSO provider to challenge the user for an additional token as part of the authentication process.

Rubrik Polaris supports SAML 2.0 identity providers for SSO authentication, including MFA.

Using these methods, even if a user's credentials are compromised, access will still be blocked from an attacker.

Encrypt and physically shard default user passwords - If MFA cannot be implemented, the default user passwords such as the one for the admin users should be encrypted and sharded. The shards of the password should be stored separately. The true admin password should never be stored in one place. This best practice prevents any of the default or admin users from being compromised and used to attack the system. Additionally, this provides protection against internal bad actors from any one person having complete access to the local admin account.

Store credentials in a strong/secure vault or key store - Any local passwords and archival location credentials used to access Rubrik CDM, Polaris or an archive should be stored in a strong and secure vault or key store system. That vault system should be secured by industry and the vendor's best practices. Features like MFA, Encryption and a secure location should be used. If the vault is breached, attackers may be able to take destructive actions against Rubrik CDM, Polaris and the archival location.

Separate primary and secondary credential storage - Do not store administrator level credentials for Rubrik or those for any archival locations in the same vault or key store as those for the primary systems and storage. Should an attacker gain access to one vault or key store, exposure can be limited to one set of systems. These independent credential storage locations also should have separate credentials themselves.

When possible, the same system administrators should not have access to both the primary and secondary system credential stores. This practice can prevent a bad actor from gaining administrative access to both the primary and secondary systems.

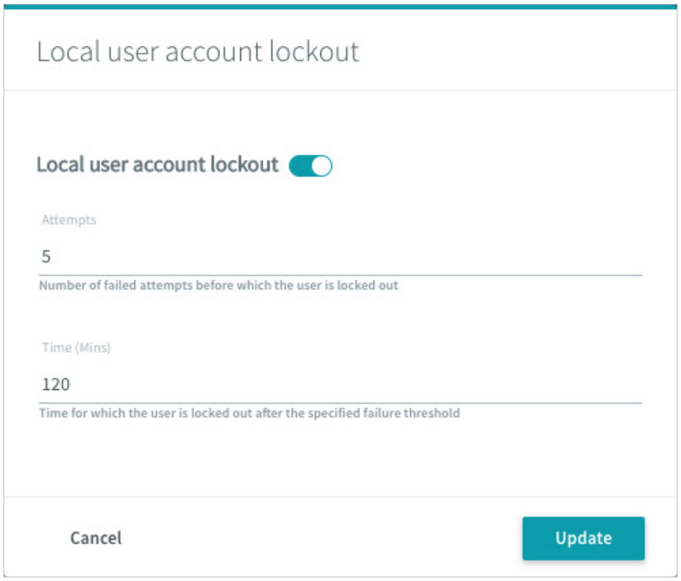
Enable auditing and alerting of failed login attempts - By creating alerts for, and logging failed login attempts, administrators can be alerted to security breaches that are in progress. Preventative steps can then be taken to stop any in progress attacks.

Admin access should be the exception not the rule - Use of the admin login or users with full admin privileges should be restricted to only those operations that require this level of access. Limiting the use of these users reduces the chances of their credentials being intercepted and used by attackers. Day to day administration should be done using users with the least amount of privileges to get their jobs done.

For an additional layer of security, the passwords of admin users can be sharded and stored separately, where no one person has access to all the shards. This provides for a two-person style of authentication whereby two people are required to take administrative actions. This may include any destructive actions.

Enable Local User Account Lockout Settings - Rubrik CDM has the ability to lock out local users for a period of time if too many failed login attempts are made. By default, this setting is disabled. Enable this feature and set the settings appropriately to prevent brute force attacks of local user accounts. In addition, notifications will be issued letting those monitoring the system that an account has been locked out due to multiple failed attempts.

This setting can be found under the **Gear icon** ⚙ **➔ Users (under Access Management) ➔ Select the Ellipsis (...) ➔ Local User Account Lockout Settings**.



Local user account lockout

Local user account lockout ●

Attempts

5

Number of failed attempts before which the user is locked out

Time (Mins)

120

Time for which the user is locked out after the specified failure threshold

Users should refer to the configuration section in the Rubrik CDM User Guide for detailed steps on configuring Local User Account Lockout Settings.

DOMAIN ACCOUNT SECURITY

The following best practices are recommended for Domain or Remote accounts when used with Rubrik CDM and Polaris.

Only use for application or end user level actions - Only use Domain and Remote accounts for application or end user level actions. These include things like taking manual backups, performing restores, scripted backups, reporting, etc… Destructive actions like changing SLA retentions, expiring data, and removing archival locations should only be performed by local administrative accounts. Implementing this best practice eliminates the possibility of credentials from a compromised external identity store from being used to disrupt Rubrik operations. Domain accounts should be restricted by implementing proper RBAC on them.

Align RBAC requirements by need - Identify each group of users that will need to access Rubrik CDM and Polaris. Determine what the minimum set of privileges is that each will need. Then create Role Based Access Control (RBAC) policies that align with these needs. Assign these RBAC policies to the individual or groups of users based on their roles. By limiting domain users to the specific areas and functions that they need, the scope of any breach of domain credentials can be limited.

Enable MFA for all domain accounts - If domain accounts will be used directly with Rubrik CDM, Multi-factor Authentication (MFA) should be configured. Enabling MFA for domain accounts will cause Rubrik CDM to challenge the user for additional information from the MFA system after supplying their username and password. This provides an additional layer of security should the domain account credentials be compromised.

Enable upstream MFA with the SSO provider via SAML - When external Identity Providers are used with Rubrik CDM or Polaris via the Security Assertion Markup Language (SAML) integration, MFA should be enabled with the upstream Single Sign-On (SSO) provider. This provides an additional layer of security should the SSO credentials be compromised.

Do not enroll target replication clusters in AD/LDAP - For Rubrik CDM clusters participating in replication, the replication target cluster should not be enrolled in the same Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain as the source cluster. This best practice protects the replicated Rubrik CDM cluster from any compromised domain credentials being re-used to attack it. Instead, the target replica CDM cluster should be secured using local accounts with strong authentication, as recommended for local accounts above. Alternatively, domain accounts from a separate AD/LDAP domain can be used with the restrictions discussed in this section. The separate AD/LDAP domain should not share the same credentials as the primary domain.

AUTOMATION

The following section details specific best practices when using automation with Rubrik CDM and Polaris.

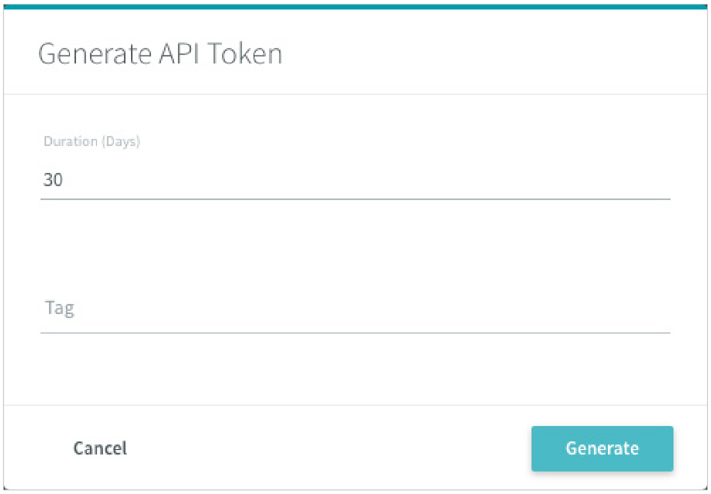
USER ACCOUNTS

A new user account should be created for each automation task you are executing. This account should be assigned to a custom role that provides only the specific privileges required to successfully execute the automation. Special care should also be given to ensure that the User account does not have any data expiry or SLA change and deletion permissions unless absolutely necessary. This ensures that if the credentials for the User account were ever compromised, the possible damage that could be inflicted to the Rubrik cluster is minimized.

AUTHENTICATION MECHANISMS

The Rubrik CDM API supports `Basic` and `Token` authentication. Since it offers several additional benefits, the best practice is to always use `Token` authentication when programmatically connecting to a Rubrik cluster. The most important of which is that a `Token` can easily be deleted, without affecting the User account, if leaked, compromised, or simply is no longer needed.

New API tokens can be created in the Rubrik CDM web UI by selecting: **<Your Username> ➔ API Token Manager ➔ +** icon.



Generate API Token

Duration (Days)

30

Tag

After selecting **Generate** and then **Copy,** the API Token cannot be viewed again.

Users should refer to the configuration section in the Rubrik CDM User Guide for detailed steps on configuring API Tokens.

STORING CREDENTIALS

The most important rule when creating automation tasks is to **never store any credentials directly in that automation code**. This prevents users from accidentally uploading credentials to version control software, while also ensuring there is no easy mechanism for an unauthorized user to find the credentials.

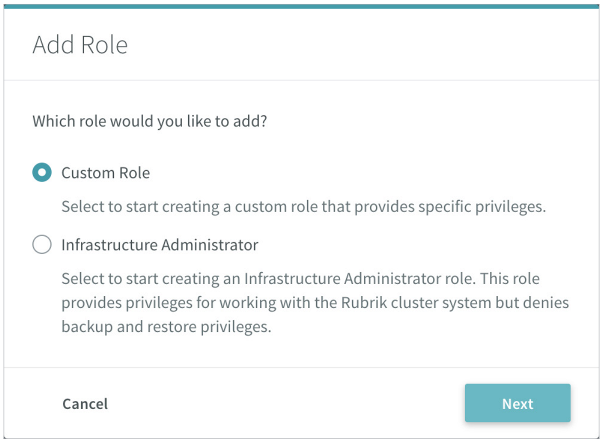
Ideally, a strong and secure vault or key store system will be utilized to access the Rubrik cluster credentials dynamically. The secure vault or key store system should also automatically rotate the API Token used on a regular basis. While not as secure, credentials can also be stored as environment variables which can be dynamically accessed during the execution of the automation.

ROLE BASED ACCESS CONTROL

Rubrik CDM and Polaris provide for enforcement of permissions with a customizable Role Based Access Control (RBAC) framework. Leveraging RBAC allows for the enforcement of the *principle of least privileged access*[2].

Defining Roles - Rubrik CDM provides the ability to define roles on the system with a wizard based approach. Two base templates are made available - **Custom Role** and **Infrastructure Admin,** which can be customized to the desired permissions to be granted.

Gear icon ⚙ ➔ Users (under Access Management) ➔ Select the Ellipsis (...) ➔ Roles ➔ +Add Roles



Add Role

Which role would you like to add?

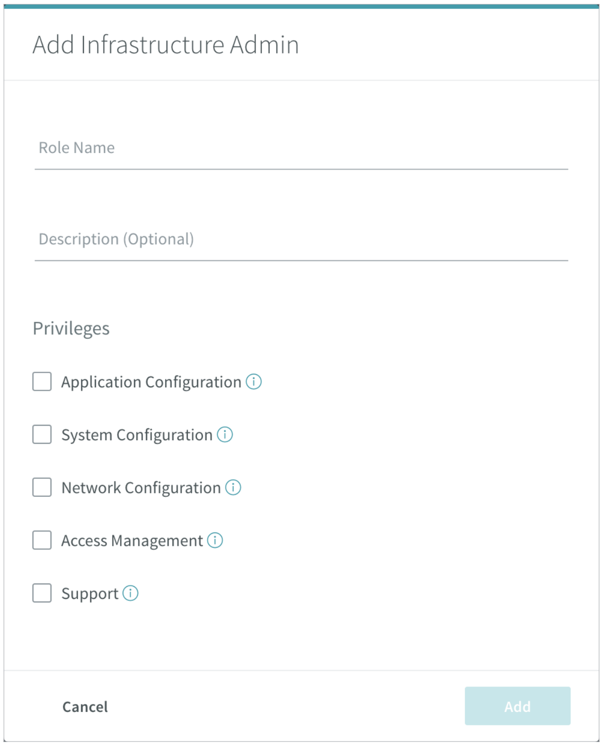
● Custom Role

Select to start creating a custom role that provides specific privileges.

○ Infrastructure Administrator

Select to start creating an Infrastructure Administrator role. This role provides privileges for working with the Rubrik cluster system but denies backup and restore privileges.

Infrastructure Admin Role - The Infrastructure Admin role template provides privileges for working with the Rubrik cluster system but denies backup, restore, and policy creation / deletion privileges. This role should be leveraged for separating the infrastructure operations from data plane operations for scoping limited access accounts.



Add Infrastructure Admin

Role Name

Description (Optional)

Privileges

□ Application Configuration ⓘ

□ System Configuration ⓘ

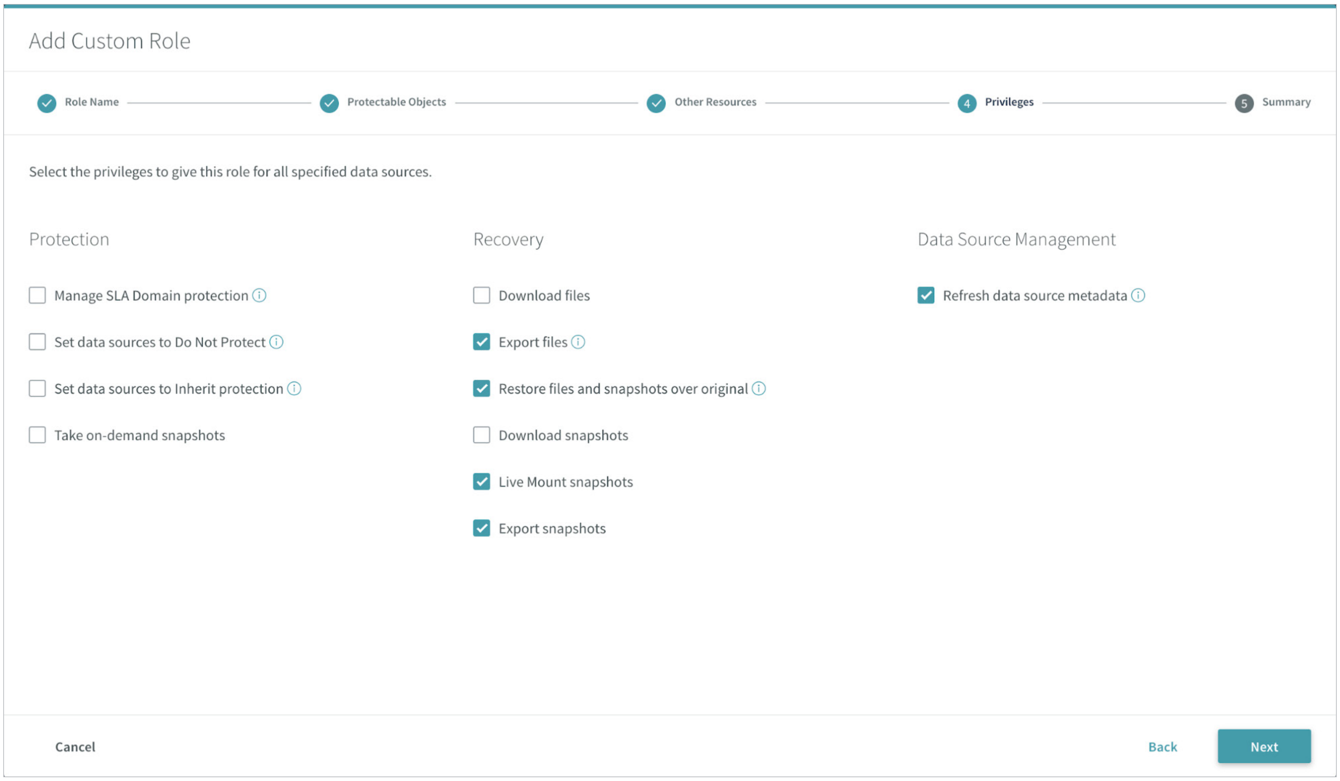
□ Network Configuration ⓘ

□ Access Management ⓘ

□ Support ⓘ

[2] https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege

Custom Role - The custom role provides for defining access to data plane operations for managing Protection, Recovery, and Data Source Management.



Add Custom Role

Select the privileges to give this role for all specified data sources.

Protection

- □ Manage SLA Domain protection
- □ Set data sources to Do Not Protect
- □ Set data sources to Inherit protection
- □ Take on-demand snapshots

Recovery

- □ Download files
- ☑ Export files
- ☑ Restore files and snapshots over original
- □ Download snapshots
- ☑ Live Mount snapshots
- ☑ Export snapshots

Data Source Management

- ☑ Refresh data source metadata

Users should refer to the configuration section in the Rubrik CDM User Guide for detailed steps on configuring Role Based Authentication Control.

WEB SESSION LIMITS AND INACTIVITY TIMEOUTS

The interactive web UI browser session for users and administrators is configured to automatically time out sessions after 30 minutes of inactivity. Customer's may wish to change this timeout to match corporate security requirements. In addition, limiting the number of concurrent sessions allowed for named user accounts is a recommended best practice. By default, there is no limit to the number of concurrent sessions allowed per user.

- To configure the cluster to limit the number of concurrent sessions for all admin accounts to the organization defined limit, submit a support ticket and request that the `webSessionsPerUser` in `crystal` be updated with the desired value. The following command can be used in the Rubrik Admin CLI via SSH to verify the value:

  ```
  cluster rubrik_tool get_config crystal webSessionsPerUser
  ```

- To configure the cluster's default timeout for a web session from 30 minutes to a customer defined target in minutes, submit a support ticket and request that the `webSessionTimeoutMinutes` value in `crystal` be updated with the desired value. The following command can be used in the Rubrik Admin CLI via SSH to verify the value:

  ```
  cluster rubrik_tool get_config crystal webSessionTimeoutMinutes
  ```

After making these changes, login in and verify that the timeout settings take effect after the defined time.

TLS SECURITY AND CERTIFICATE MANAGEMENT

Rubrik CDM upon bootstrap configures a default Rubrik self-signed certificate for web services traffic to enable secure TLS encrypted traffic over HTTPS (port 443). Rubrik clusters support the import and export of TLS certificates signed by a Certificate Signing Request (CSR) or a key phrase, as well as unsigned and wildcard certificates. Imported TLS certificates can be in the Encrypted Private Key and Certificate (PKCS12) format or base64-encoded in the PEM format. Once a TLS certificate is imported to the Rubrik cluster, authentication workflows enable users to select a TLS certificate to use with the specific service.

Users may refer to the Rubrik CDM User Guide for steps on creating a Certificate Signing Request (CSR) and importing an existing TLS certificate.

DISABLE TLS V1.1

Rubrik CDM defaults to TLS v1.2 for all secure network communications by default. Step down to TLS 1.1 is provided for support of legacy systems that still require the older version. If there is no need to support TLS v1.1, or it needs to be disabled for security policy compliance, Rubrik Support can be engaged. Request that they disable cipher step down by setting the value for `sprayMinimumTlsVersion` in `shield` to be set to `TLSv1.2`. This setting can be confirmed on the cluster by logging in to the Rubrik CDM admin CLI and running the command:

```
cluster rubrik_tool get_config shield sprayMinimumTlsVersion
```

AUDITING

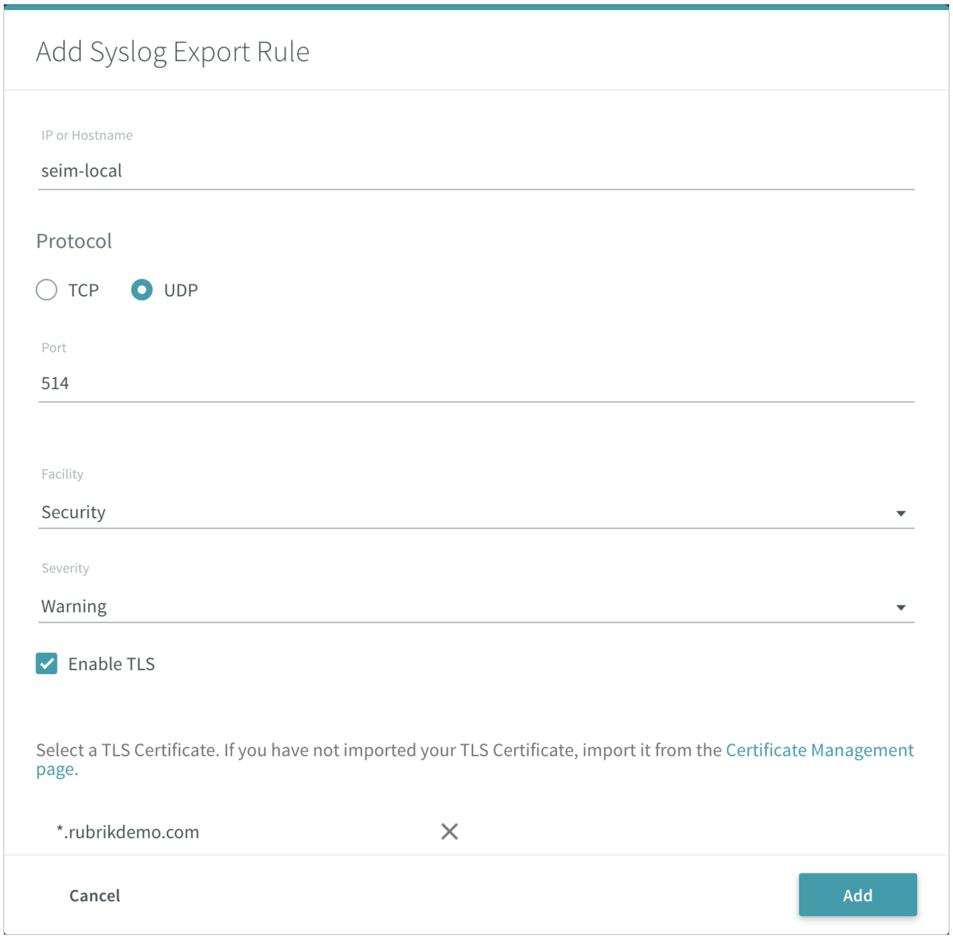
Rubrik provides for full event and activity audit logging at a cluster level. By default, the internal logs are kept for approximately 90 days based on activity volume in a rolling log. The Rubrik cluster supports transmission of system activities to an external syslog server and is a recommended best practice.

The Rubrik cluster uses the standard syslog protocol for formatting and transmission of system notifications. By default, at the transport layer, the Rubrik cluster sets the syslog standard protocol and port (UDP/514). The transport layer protocol and port can be disabled, or can be configured to use custom settings.

At the application layer, the syslog transmissions use the HTTP protocol. Syslog export rules can be set up with TLS, to encrypt in-flight data sent to a syslog server.

When syslog support is enabled, the Rubrik cluster sends server messages to an external syslog server according to how the facility or severity levels are configured. The facility level represents the machine process that created the syslog event. For example, general system processes such as the kernel, a user, mail, but there are also facilities for Rubrik specific logs. The severity level determines how severe the message is displayed in syslogs. For example, critical, warning, or purely informational.

Syslog notifications can be added to Rubrik CDM in the web UI by selecting the **Gear icon ⚙ ➔ Notification Settings ➔ Add Syslog Export Rule**.



Add Syslog Export Rule

IP or Hostname: seim-local

Protocol

○ TCP ● UDP

Port: 514

Facility: Security

Severity: Warning

☑ Enable TLS

Select a TLS Certificate. If you have not imported your TLS Certificate, import it from the Certificate Management page.

*.rubrikdemo.com

Users should refer to the configuration section in the Rubrik CDM User Guide for detailed steps on configuring Syslog Export Rules and for referencing Facility and Severity level classifications.

NETWORK TIME PROTOCOL CONFIGURATION

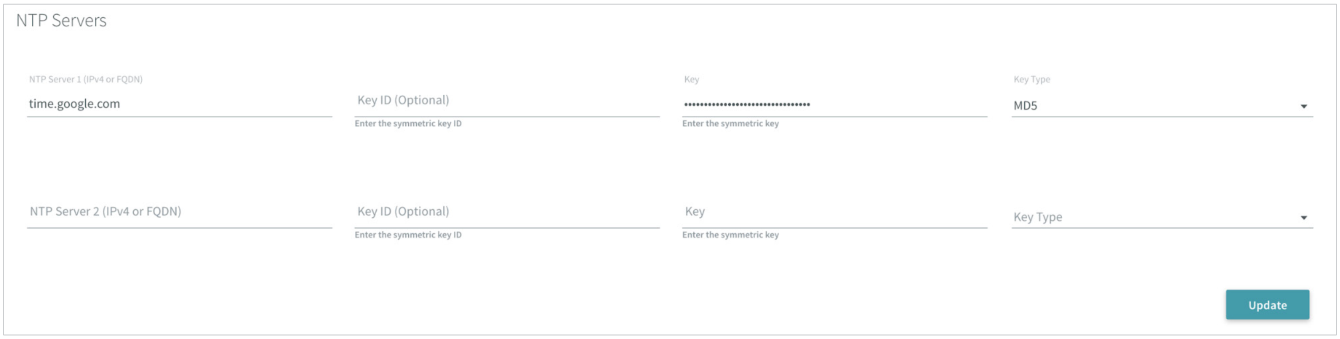
The Network Time Protocol (NTP) is an Internet protocol built to distribute precise time around a computer network. NTP makes use of UDP over TCP/IP to synchronize network time clients to a precise time reference. The NTP protocol can make use of encryption keys to authenticate a time server. Secure NTP Servers will be explained below.

The Network Time Protocol can be used to synchronize numerous time essential processes on distributed computers across a network. The NTP protocol is consequently a great security risk. Hackers or hazardous users could make an effort to interrupt system synchronization by attempting to adjust or replicate NTP time stamps.

Fortunately, NTP has an integral security attribute to put a stop to endeavors to tamper with system time synchronization. NTP may use encrypted keys to authenticate time stamps provided by a timeserver. Network time clients and devices can make use of secure keys to authenticate time stamps and ensure their supply of origin.

NTP executes authentication by employing an agreed set of keys between a server and client, which are encrypted in time stamps. A NTP time server transmits a timestamp to a client with one of a selection of keys encrypted and appended to the message. When a timestamp is obtained by the client, the security key is unencrypted and checked against the listing of filed secure keys. In this way, the client can be sure that the received time stamp came from the expected time source.

Rubrik CDM provides for Secure NTP encrypted time sources as an optional configuration that should be used as best practice. NTP servers can be configured on Rubrik CDM in the web UI by selecting the **Gear icon ⚙ ➔ Network Configuration (Network Settings) ➔ NTP Servers**



NTP Servers

NTP Server 1 (IPv4 or FQDN): time.google.com

Key: ••••••••••••••••••••••••••••••••

Key Type: MD5

For additional information on NTP and best practices on security of NTP time sources reference: https://timetoolsltd.com/ntp/network-time-protocol-ntp-best-practices/[3]

Users should refer to the configuration section in the Rubrik CDM User Guide for detailed steps on configuring NTP.

ENHANCED SYSTEM RESET PROTECTION

Beginning with Rubrik CDM release versions 5.2.1 and forward, a system level configuration change has been integrated into the Rubrik CDM platform to remove admin access to invoke ***sdreset*** operations in the Rubrik CLI as default configuration. This proactively prohibits the accidental or adversarial reset of a Rubrik node or cluster.

Rubrik support can be engaged to re-enable the reset functionality for customer factory reset requirements as needed.

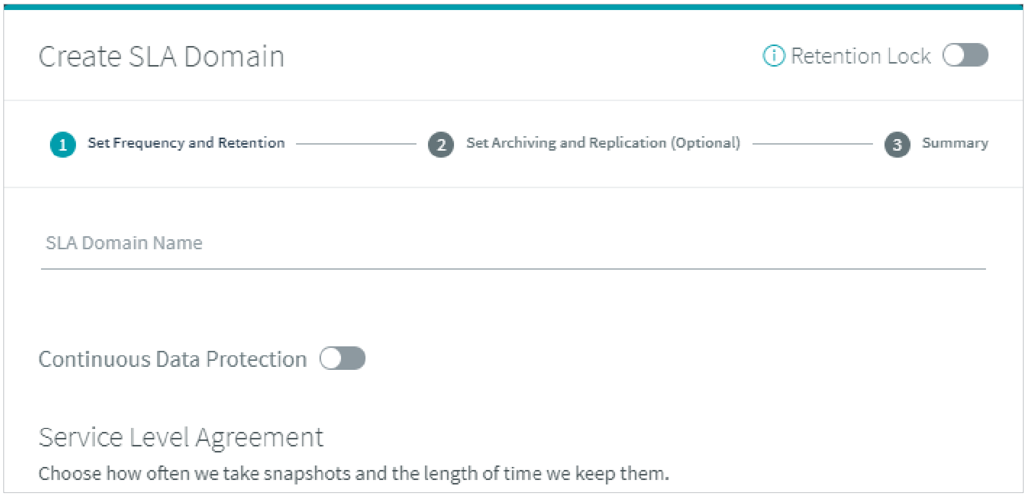
RETENTION LOCK

Retention Lock is a Rubrik CDM feature designed to securely prevent the premature deletion of snapshots, either from malicious or accidental means. Since most attack vectors look for an unauthorized way to delete backups, it is recommended to leverage Retention Lock in order to help protect against this malicious deletion attempt. These may be through SLA Domain modification to reduce retention or through attempting a factory level reset.

> IMPORTANT: Retention Lock is globally disabled on the cluster by default. Rubrik Support must be contacted, and a case must be opened in order to have Retention Lock enabled and configurable within the Rubrik UI. There is also a special authorization step that includes setting up particular customer authorized contacts that the support team will walk through prior to enabling Retention Lock into the Rubrik UI of the cluster.

Once Rubrik Support has enabled Retention Lock within the cluster, a new toggle will appear in the upper right-hand corner of each Create SLA Domain dialog window, as seen below:

[3] https://timetoolsltd.com/ntp/network-time-protocol-ntp-best-practices/

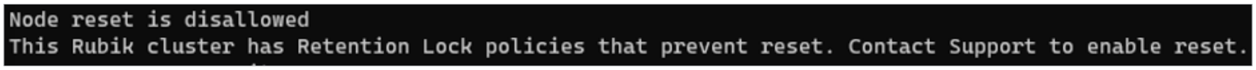

Create SLA Domain
Retention Lock
1 Set Frequency and Retention
2 Set Archiving and Replication (Optional)
3 Summary
SLA Domain Name
Continuous Data Protection
Service Level Agreement

Choose how often we take snapshots and the length of time we keep them.

IMPORTANT: Once globally enabled, Retention Lock must be explicitly enabled on each SLA Domain where the protection is desired. Retention Lock can be enabled upon SLA Domain creation, or it can be enabled on pre-existing SLA Domains, where the protection and restrictions can be applied retro-actively.

The Retention Lock feature actually introduces a number of additional security features into the system, however there are a few important restrictions to highlight that pertain to malicious attacks:

1. **A Factory Reset of the cluster/node cannot be performed once Retention Lock has been enabled by Rubrik Support:** A common attack vector is an immediate attempt to perform a factory reset on the appliance in order to instantly wipe out backup data. This becomes impossible to do without the intervention of Rubrik Support when the Retention Lock feature is globally enabled. Below is the messaging that an administrator is presented with when trying to perform a reset through conventional means:

   ```
   Node reset is disallowed
   This Rubik cluster has Retention Lock policies that prevent reset. Contact Support to enable reset.
   ```

   If a reset absolutely has to be performed for any reason, please contact Rubrik Support.

2. **The only modifications allowed on SLA Domains are for “stronger” and “more secure” configurations:** Any attempt now to reconfigure the SLA Domain that might contribute to a weaker configuration or contribute to the expiration of existing data is prohibited. This is specifically designed to prevent the accidental or malicious attempts at modifying the SLA that causes expiration/pruning of existing data. There are also restrictions in place to prevent the removal of any archival locations or replication targets associated with the SLA. Additional details about the specific restrictions involved here can be found in the Rubrik CDM User Guide.

3. **An external time source is required:** A local time source is no longer allowed with Retention Lock enabled. When combined with using secure time sources in the manner mentioned above, this can be leveraged to prevent rogue time source attacks used to prematurely expire data by fast forwarding past the retention period.

For additional details on all the restrictions Retention Lock introduces, please reference the Rubrik CDM User Guide. Please contact Rubrik Support for additional assistance with enabling or disabling Retention Lock.

SOFTWARE ENCRYPTION AT REST

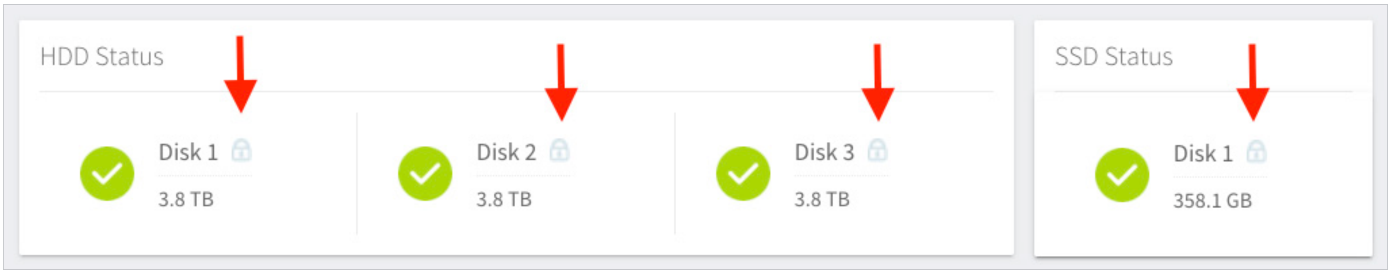
By default, the Rubrik CDM cluster enables the encryption of data at rest using software during the initial bootstrap process.

```
Enable Software Encryption (y/n) (optional) [y]
```

Note: Rubrik clusters running on r528 model Briks will use self-encrypting drives that are certified to meet level 2 of the FIPS 140-2 specification. Since encryption is done at the hardware level on these Briks, they do not have a Software Encryption option.

To verify Software Encryption has been enabled in the Rubrik CDM web UI by select the **System ➔ Nodes (See All) ➔ <Any Node Name>**

Under the **HDD Status** and **SSD Status,** verify that a lock icon appears next to each drive



Alternatively, the `/v1/cluster/{id}/security/encryption` API endpoint can be used, which returns the following response body:

```
{
 “isEncrypted”: true,
 “cipher”: “string”,
 “keyLength”: 0
}
```

When `isEncrypted` is set to True, Software Encryption has been enabled.

Once the initial bootstrap process has been completed, the Software Encryption state can not be changed. If the Rubrik CDM cluster does not have Software Encryption enabled, contact Rubrik support to discuss the options to encrypt the data at rest.

SECURITY BANNER AND CLASSIFICATION SETTINGS

The Rubrik CDM cluster provides the ability to display a custom notice that must be acknowledged before login is permitted. For example, this might be the text of an authorized-use agreement. Rubrik CDM also provides configurable top and bottom banners for the Rubrik CDM web UI pages.

Rubrik CDM provides the ability to add a configurable message to the login page. The message text can be formatted as plain text or can use standard HTML markup.

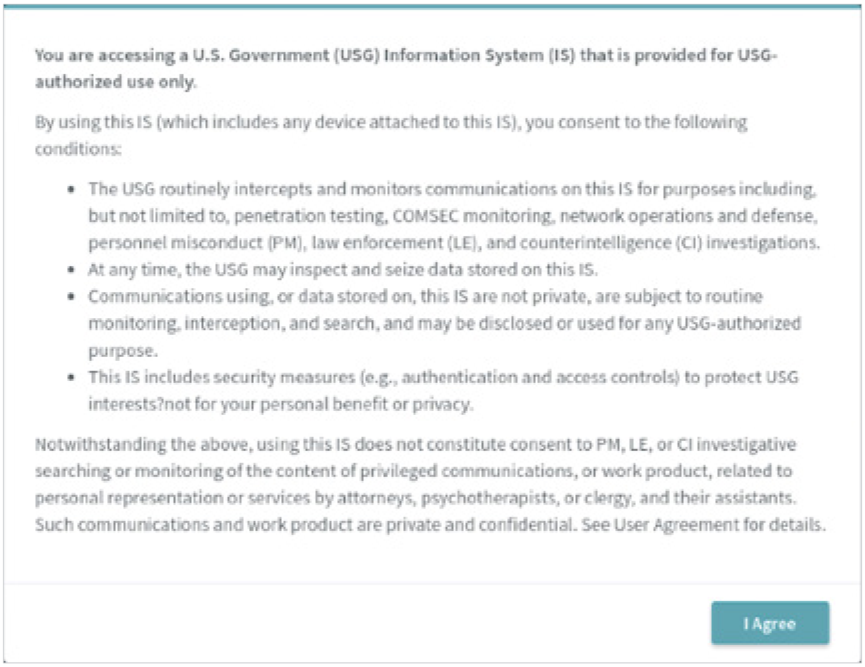
Rubrik CDM also provides the ability to add configurable top and bottom page banners on the web UI. The banner text and the banner background color can be configured.

The Cluster Settings page provides access to the following settings:

- Login notice
- Top and bottom banner background color
- Top and bottom banner text

SETTING THE LOGIN BANNER TEXT

Gear icon ⚙ ➔ Cluster Settings ➔ Select the Login Banner Text ➔ Enter notice text.



You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests?not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

SETTING THE SECURITY CLASSIFICATION COLOR AND TEXT

Use the Rubrik CDM web UI to set the security classification color and text.

Gear icon ⚙ ➔ Cluster Settings ➔ Select Security Classification Color ➔ Enter Security Classification Text.

IP WHITELISTING

Rubrik Polaris allows customers to restrict the IP addresses from which systems can access the account. This ensures that systems outside the customer's environment cannot log in to the Polaris instance. Typically, the whitelist would include the customer's public internet address(es) where traffic egresses from the data center. It is recommended that a backup IP address also be whitelisted in case the primary data center's Internet access is disabled.

Care must be taken for remote users though, as Polaris uses public internet IP addresses for access. Traffic for Polaris from remote users should be routed through the customer's data center and then on to Polaris. In this way, if a remote user leaves the company, their access to Polaris is automatically disabled.

ARCHIVE (EXTERNAL) STORAGE

If the CloudOut feature is being used with Rubrik CDM to archive snapshots for long term retention, it is critical that best practices are followed to secure the archive locations. Most modern malicious attack vectors focus on external archive locations first before going after the local snapshot data when data management products are targeted. Since the data is no longer on the Rubrik appliance once it gets archived, data protection is now up to the customer's security practices. The following are a few security hardening recommendations for the archival data.

NOTE: The concepts covered below around securing cloud archival storage will only touch on them from a high level. More details can be found if needed in the following published documents:

- Security Hardening Rubrik CloudOut for AWS (RWP-0517)
- Security Hardening Rubrik CloudOut for Azure (RWP-0518)

The Principle of Least Privileged Access - As mentioned above, it's recommended to follow the principle of least privileged access and to extend this concept into the Rubrik CloudOut feature as well. For Rubrik CDM, the security principle that is used to access the cloud archival location is built with the absolute minimum privileges needed for both write to and read operations. This concept also applies to creating dedicated security principles for individual buckets/archives as well. The most important idea around this is that if the credentials are ever compromised for the archival location, then the minimum privileges will ensure that the attacker can't get very far within the entire cloud environment with the compromised credentials. More details around specific permissions and policies can be found in the cloud hardening documents.

Rubrik CDM does not integrate directly any versioning features with any of the major cloud providers today. What this means is that Rubrik CDM will not be aware of the versioning that is happening in the background. This can lead to excess capacity being used within the archives as when CloudOut deletes expired data in the archive, the data won't actually be deleted on the backend even though CDM will think it has been purged.

Store archival location credentials securely - As mentioned at the beginning of this document, credentials for the archival location should be well protected. Store them in a separate vault or key store than those for the primary systems. Avoid storing these credentials in unsecured locations.

Store the archival location encryption key securely - Since CloudOut encrypts the data stored in the cloud archive, it requires an encryption key to be created and securely stored. Most archival location types in Rubrik CDM use a manually generated RSA key that must be secured. These keys should be stored in the same manner as discussed for administrative credentials and archival location credentials. It is critical that this key is stored, as it is needed if the cluster is lost and the data needs to be retrieved out of the archive. One of the first things that attackers will search for during enumeration phases is RSA keys accidentally (or intentionally) stored in an unsecured location If the RSA key is compromised, attackers can read and modify the data in the archival location. For Ransomware scenarios, this means that the attackers can read and re-encrypt the data with their own encryption key and therefore lock the customer out of their own archive until the ransom is paid.

In the case of AWS S3 being utilized as the cloud archival location, the AWS Key Management Service can be leveraged to securely store and rotate this key automatically. It is recommended to utilize AWS KMS where available to offer the most secure environment. AWS KMS will further abstract the encryption key by utilizing envelope encryption. The KMS Key ID should also be treated as an administrative level credential and stored as such. The key rotation provided by AWS is automatic and requires no maintenance by the end user.

IMPORTANT: When utilizing AWS KMS, the principle of least privileged access also applies to this technology. Ensure that a different security principle is used with the necessary "key admin" privileges in KMS to create the CMKs while restricting the security principle used to access the CloudOut S3 bucket to just standard "key usage" privileges.

Leverage auditing tools for continuous monitoring - Once a hardened environment is initially set up for cloud archives, it is also critical that the environment is continually monitored and audited to detect any intrusions in the system. Technologies such as AWS' CloudTrail or Azure's Log Analytics can automatically log events that pertain to potential malicious activity such as bucket modifications, object deletions, and permission changes just to name a few. Initially detecting some of these events can actually prevent an attack if caught early. In the event that the environment is already compromised, these technologies can assist in providing historical events for forensic analysis and postmortem activity.

NFS/SMB SECURITY

Rubrik CDM uses the Network Attached Storage (NAS) protocols NFS and SMB for some of its features. These include NAS protection, Live Mount, Managed Volume, Volume Group Snapshots, Bare Metal Recovery and Archival operations. It is important that these NAS protocols be secured to prevent unauthorized access to the protected data. Rubrik CDM's file system is immutable, so the data cannot be altered via these protocols.

Use secure SMB for SMB shares - Rubrik CDM can use secure SMB to require authenticated connections for SMB shares. Implementing this feature will prevent unauthorized users or systems from accessing data during Live Mount or Managed Volume operations.

Use IP whitelists for all NFS archival locations and clients - IP whitelisting should be implemented on all NFS NAS devices that will be backed up and any NFS based archival locations that support them. The IP addresses of the Rubik CDM nodes should be listed in these IP whitelists. This practice can help prevent unauthorized systems from accessing the Rubrik archives and to the NAS shares that Rubrik will protect.

Use Kerberos for NFS archival locations - When a NAS target for a NFS archival location supports Kerberos, this security protocol should be enabled. Kerberos will provide a username and password authentication requirement to the NFS share that is used as the archiving target; thus increasing the security of it. Configuring the archival location in Rubrik CDM will require that a valid username and password be used.

Use Username/Password authentication for NFS filesets - For those NAS clients that support it username and password authentication should be configured for the NFS filesets that will be protected. This practice will help to prevent unauthorized access to the NAS data which is being protected.

Use Client Patterns with Managed Volumes - When defining the fileset for NAS backup, use the Client Pattern feature to whitelist the IP addresses or host names of the systems that are being protected. This will help prevent unauthorized systems from mounting the Managed Volume and reading its data.

CLUSTER DISASTER RECOVERY

Should a Rubrik CDM cluster be lost due to human error, natural disaster or an attack, recovering its configuration will become important. While Rubrik CDM is resistant to operational failure due to its masterless cluster design, some events cannot be recovered from. Currently, configuration data is not backed up externally from the cluster. Instead, a script can be used to back up and restore parts of the configuration. As a best practice, a separate utility server should be used to export the Rubrik CDM configuration. If replication or archiving is configured this utility server can be backed up, and its configuration sent offsite by the Rubrik CDM cluster. Should offsite backups not be an option, other methods must be employed to keep a safe copy of the Rubrik CDM configuration from this utility server.

The Rubrik CDM backup script can be found here: https://github.com/rubrikinc/rubrik-config-backup[4]

CONCLUSION

Rubrik takes security very seriously. Many features and functions have been built into Rubrik CDM and Polaris to ensure that the data and systems remain secure. Even though these features and functions exist, they still must be utilized. By following the best practices presented in this document, organizations can maximize the security posture of their Rubrik Implementations.

[4] https://github.com/rubrikinc/rubrik-config-backup

VERSION HISTORY

Version	Date	Summary of Changes
1.0	July 2020	Initial Release
1.1	September 2020	Errata updates / Enhanced System Protection added
1.2	May 2021	Object Versioning recommendations removed
1.3	June 2021	Update to MFA verbiage and inclusion of TOTP.

rubrik

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

20210629_v1