Alerts

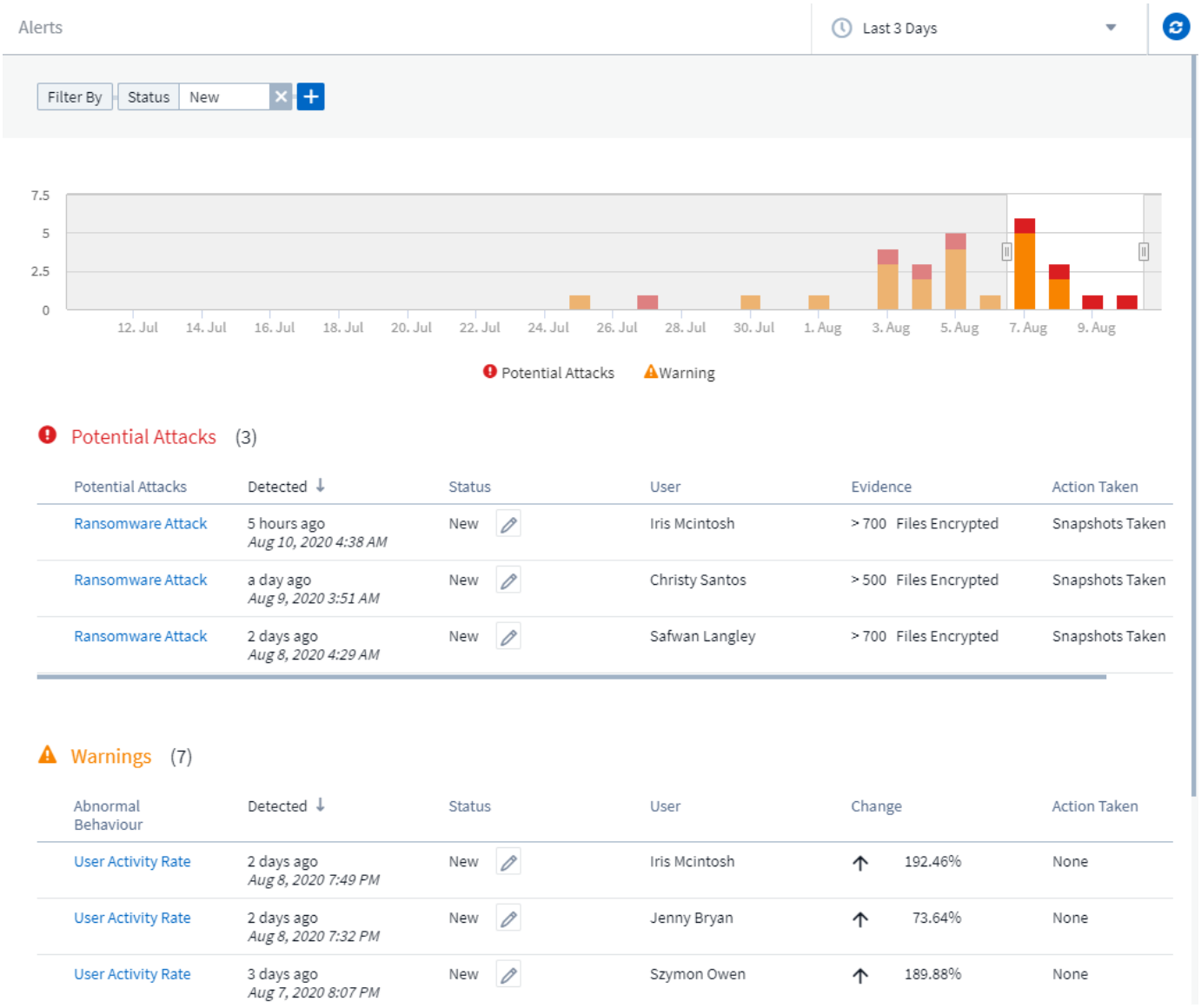
Cloud Insights

Tony Lavoie
December 02, 2020

Table of Contents

Alerts

The Cloud Secure Alerts page shows a timeline of recent attacks and/or warnings and allows you to view details for each issue.



Alert

The Alert list displays a graph showing the total number of Potential Attacks and/or Warnings that have been raised in the selected time range, followed by a list of the attacks and/or warnings that occurred in that time range. You can change the time range by adjusting the start time and end time sliders in the graph.

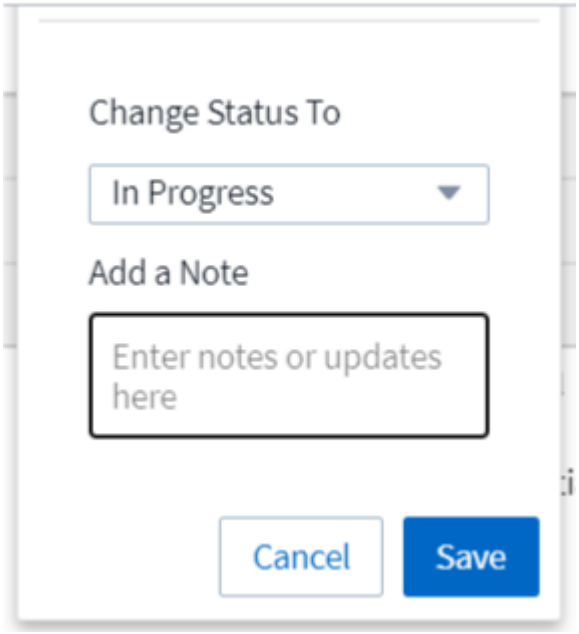
The following is displayed for each alert:

Potential Attacks:

- The *Potential Attack* type (for example, Ransomware)
- The date and time the potential attack was *Detected*

- The *Status* of the alert:
  - New (this is the default for new alerts)
  - In Progress
  - Resolved
  - Dismissed

  An administrator can change the status of the alert and add a note to assist with investigation.



- The *User* whose behavior triggered the alert
- *Evidence* of the attack (for example, a large number of files was encrypted)
- The *Action Taken* (for example, a snapshot was taken)

Warnings:

- The *Abnormal Behavior* that triggered the warning
- The date and time the behavior was *Detected*
- The *Status* of the alert:
  - New (this is the default for new alerts)
  - In Progress
  - Resolved
  - Dismissed

  An administrator can change the status of the alert and add a note to assist with investigation.

- The *User* whose behavior triggered the alert
- A description of the *Change* (for example, an abnormal increase in file access)
- The *Action Taken*

Filter Options

You can filter Alerts by the following:

- The *Status* of the alert
- Specific text in the *Note*
- The type of *Attacks/Warnings*
- The *User* whose actions triggered the alert/warning

The Alert Details page

You can click an alert link on the Alerts list page to open a detail page for the alert. Alert details may vary according to the type of attack or alert. For example, a Ransomware Attack detail page may show the following information:

Summary section:

- Attack type (in this example, Ransomware) and Alert ID (assigned by Cloud Secure)
- Date and Time the attack was detected
- Action Taken (for example, an automatic snapshot was taken. Time of snapshot is shown immediately below the summary section))
- Status (New, In Progress, etc.)

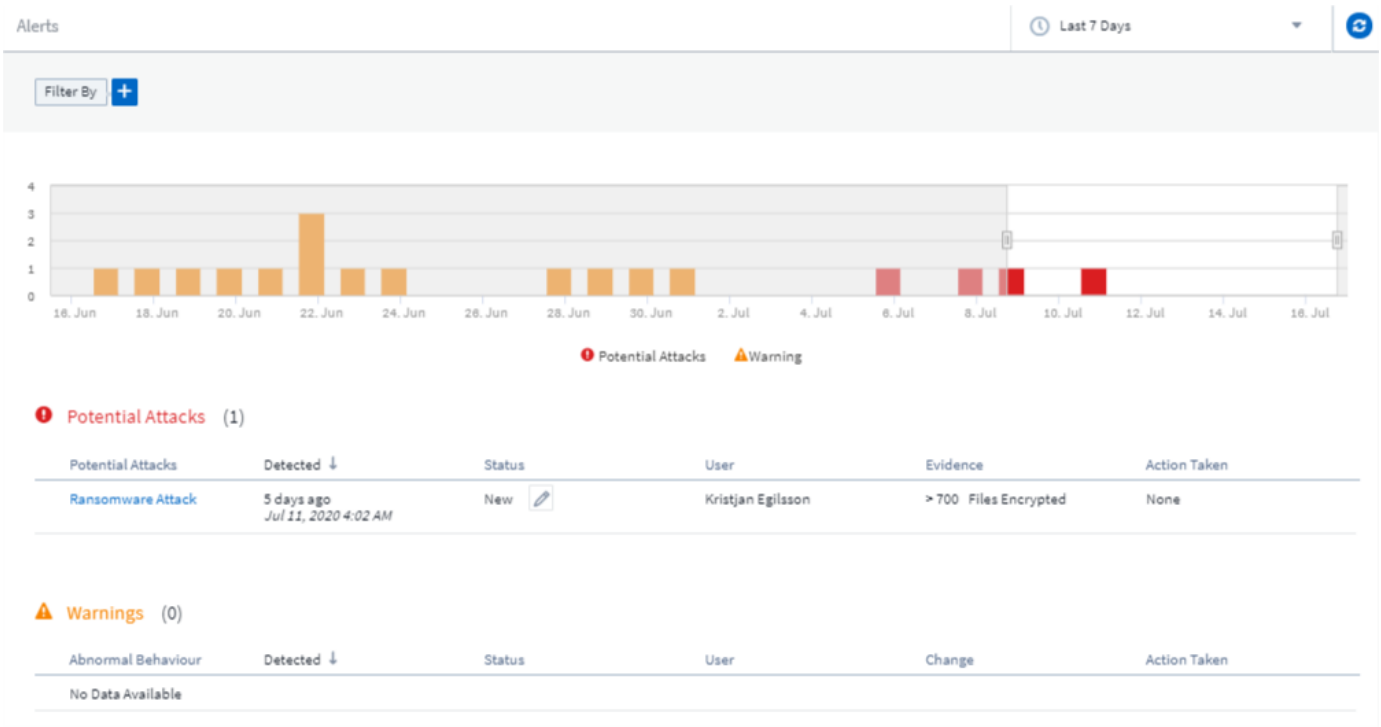
Attack Results section:

- Counts of Affected Volumes and Files
- An accompanying summary of the detection
- A graph showing file activity during the attack

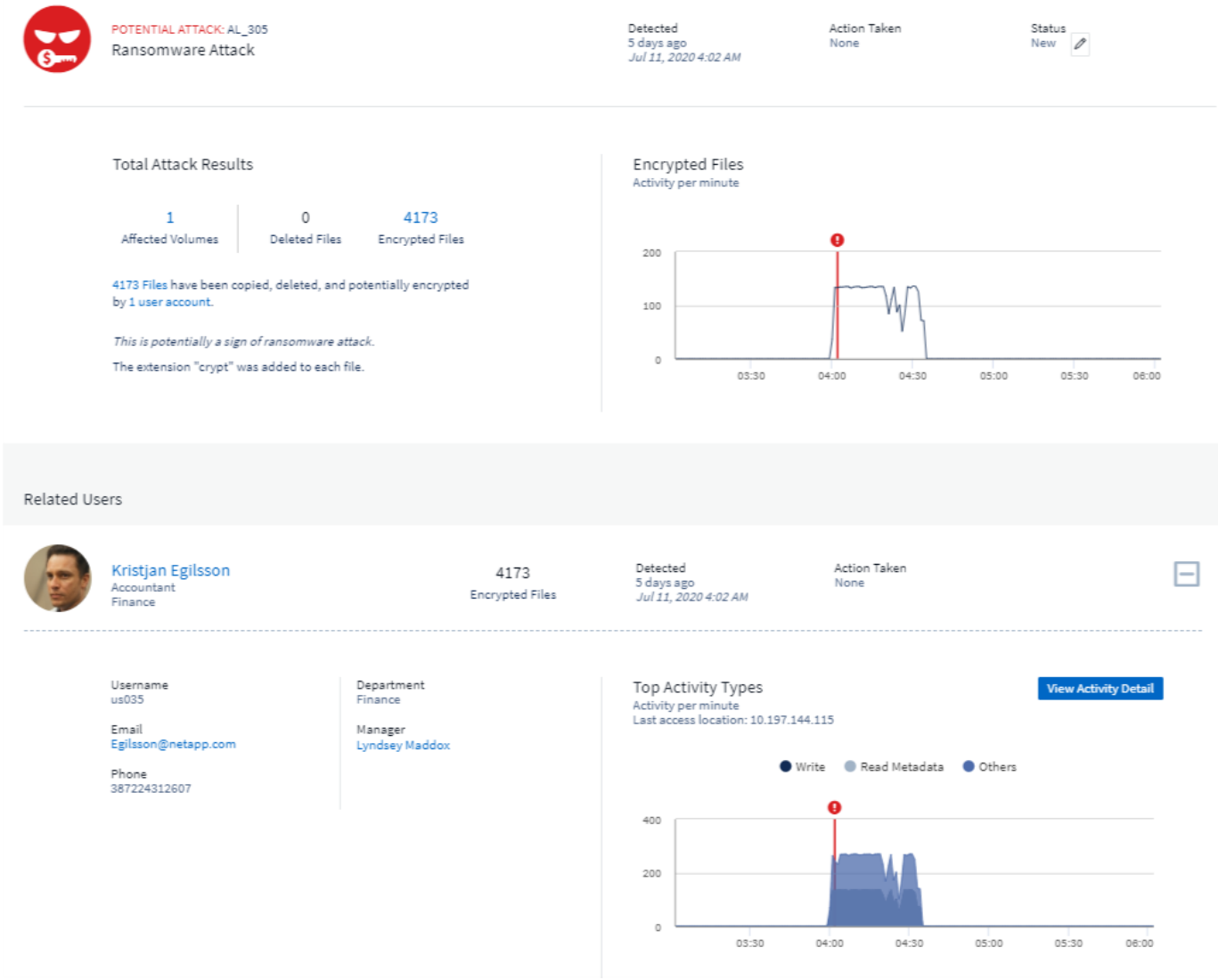
Related Users section:

This section shows details about the user involved in the potential attack, including a graph of Top Activity for the user.

Alerts page showing potential ransomware attack:



Detail page for potential ransomware attack:

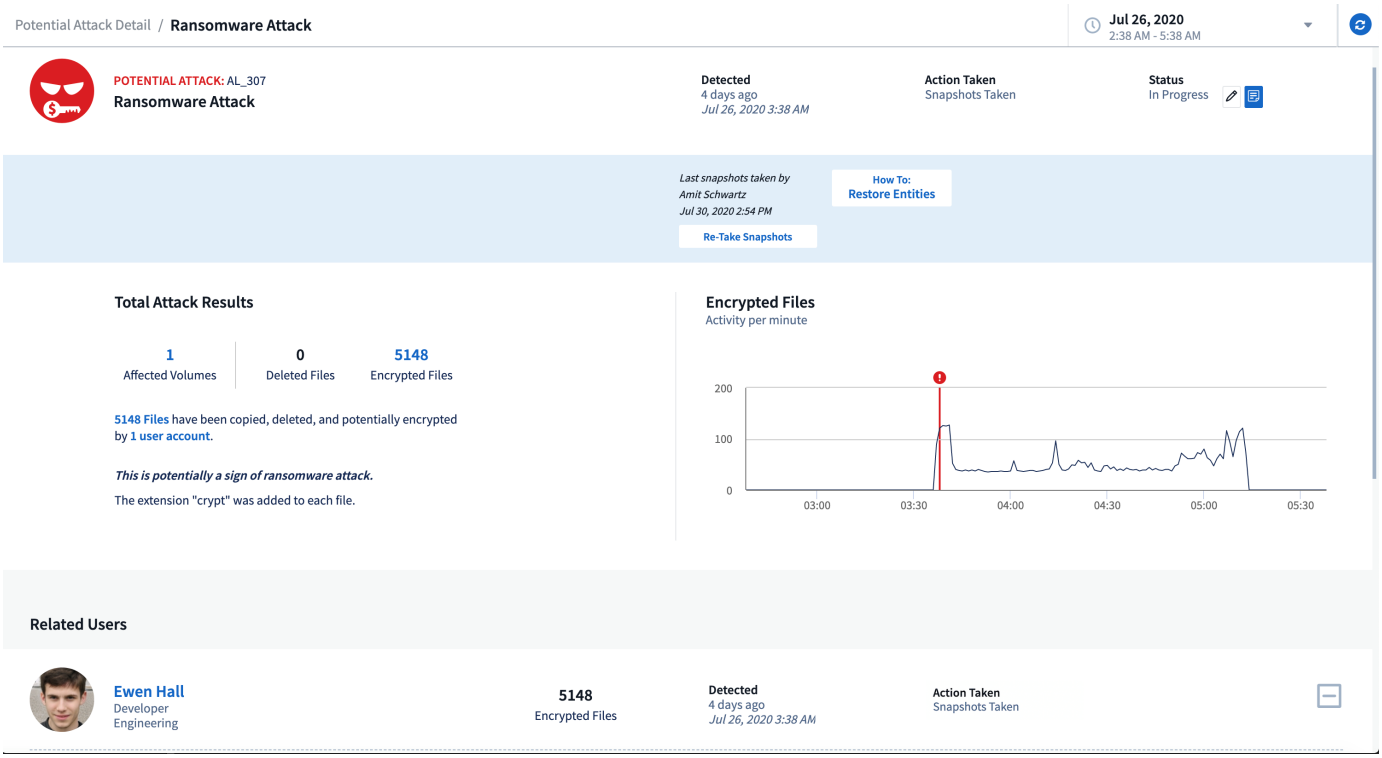


Take a Snapshot **Action**

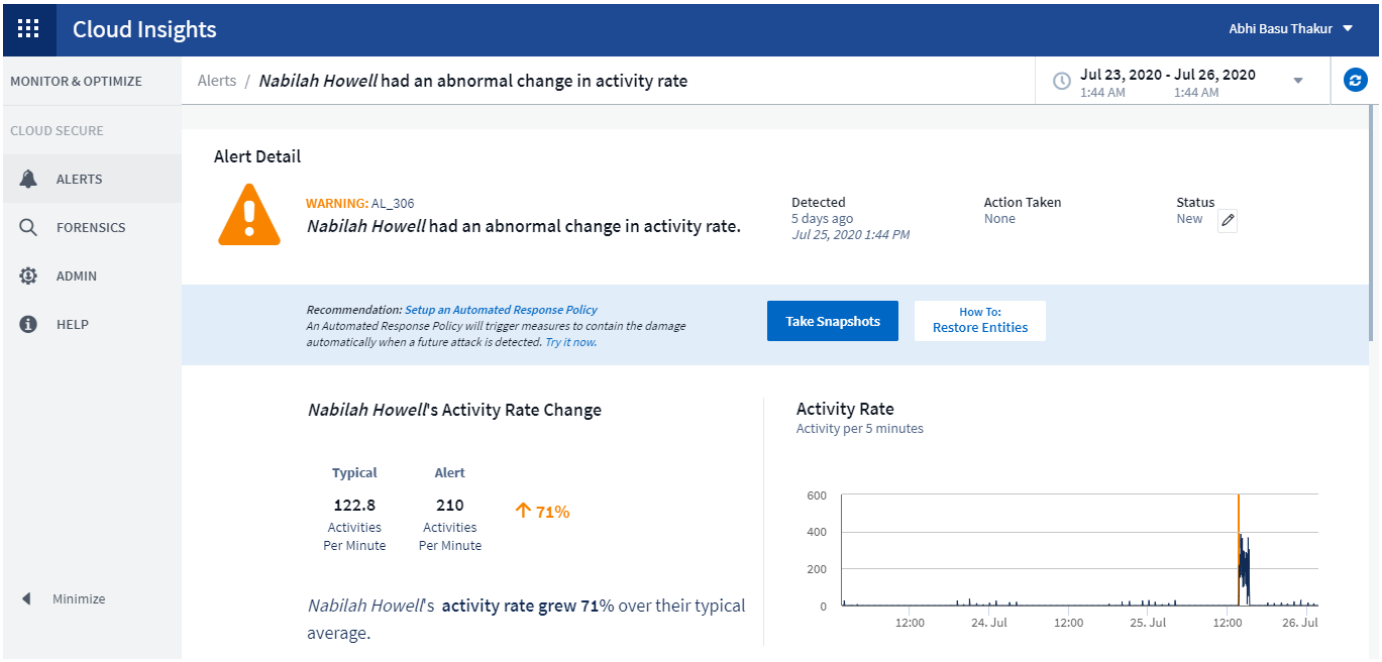
Cloud Secure protects your data by automatically taking a snapshot when malicious activity is detected, ensuring that your data is safely backed up.

You can define automated response policies that take a snapshot when ransomware attack or other abnormal user activity is detected.
You can also take a snapshot manually from the alert page.

Automatic Snapshot taken:



Manual Snapshot:



Alert Notifications

Email notifications of alerts are sent to an alert recipient list for every action on the alert. To configure alert recipients, click on **Admin > Notifications** and enter an email addresses for each recipient.

Retention Policy

Alerts and Warnings are retained for 13 months. Alerts and Warnings older than 13 months will be deleted. If the Cloud Secure environment is deleted, all data associated with the environment is also deleted.

Troubleshooting

Problem:	Try This:
For snapshots taken by Cloud Secure (CS), is there a purging/archiving period for CS snapshots?	No. There is no purging/archiving period set for CS snapshots. The user needs to define purging policy for CS snapshots. Please refer to the ONTAP documentation on how to setup the policies.
There is a situation where, ONTAP takes hourly snapshots per day. Will Cloud Secure (CS) snapshots affect it? Will CS snapshot take the hourly snapshot place? Will the default hourly snapshot get stopped?	Cloud Secure snapshots will not affect the hourly snapshots. CS snapshots will not take the hourly snapshot space and that should continue as before. The default hourly snapshot will not get stopped.
What will happen if the maximum snapshot count is reached in ONTAP?	If the maximum Snapshot count is reached, subsequent Snapshot taking will fail and Cloud Secure will show an error message noting that Snapshot is full. User needs to define Snapshot policies to delete the oldest snapshots, otherwise snapshots will not be taken. In ONTAP 9.3 and earlier, a volume can contain up to 255 Snapshot copies. In ONTAP 9.4 and later, a volume can contain up to 1023 Snapshot copies. See the ONTAP Documentation for information on setting Snapshot deletion policy.
Cloud Secure is unable to take snapshots at all.	Make sure that the role being used to create snapshots has xref: proper rights assigned. Make sure *csrole* is created with proper access rights for taking snapshots: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Snapshots are failing for older alerts on SVMs which were removed from Cloud Secure and subsequently added back again. For new alerts which occur after SVM is added again, snapshots are taken.	This is a rare scenario. In the event you experience this, log in to ONTAP and take the snapshots manually for the older alerts.
In the *Alert Details* page, the message “Last attempt failed” error is seen below the *Take Snapshot* button. Hovering over the error displays “Invoke API command has timed out for the data collector with id”.	This can happen when a data collector is added to Cloud Secure via SVM Management IP, if the LIF of the SVM is in *disabled* state in ONTAP. Enable the particular LIF in ONTAP and trigger *Take Snapshot manually* from Cloud Secure. The Snapshot action will then succeed.