Viewing Cloud Secure Forensic Data

Cloud Insights

NetApp
May 15, 2020

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/alert_data.html on May 15, 2020.
Always check docs.netapp.com for the latest.

Table of Contents

Viewing Cloud Secure Forensic Data 1
- Alerts 1
- Forensic information 2
- Forensic User Overview 4
- Forensic Entity Detail 5
- Forensic Community Detail 6
- Forensic Activity History 7

Viewing Cloud Secure Forensic Data

Alerts

The Alerts page shows all alerts generated by Cloud Secure.

Use this page to identify recent alerts and the users generating the most alerts.

You can also access all alerts that have been raised with the ability to drill down into individual alerts.

History

History shows the number of alerts that have been raised over the last seven days. Hovering over the severity of the alerts displays the number, severity, and occurrence date for each alert type.

Notable Users

- Shows a list of the users that have generated the highest number of alerts.
- Shows the type of alerts generated.
- Shows the total number of alerts generated for each user.

Alert

The Alert list shows the total number of alerts that have been raised and contains details of all alerts:

- The date and time the alert was detected.
- The status of the alert:
  - New
  - In Progress
  - Resolved
  - Dismissed

    New is set by the by Cloud Secure. Administrators set all other status states, and add notes.

*The User that raised the alert and a link to the User Profile

- The severity of the alert:
  - Critical
  - Warning
  - Low

- Synopsis identifies the activity that raised the alert and the user and community responsible.

  Click the link to drill down to the Alert Details and Related User for detailed information.

- Action Taken

  Can include None, Quarantined, or Dismissed.

Filter Options

You can filter Alerts by the following:

- Action Taken
- Alert Type
- Note
- Severity
- Status
- Synopsis
- User

Forensic information

The Forensic view provides access to the User, Entity, Community, and User Activity information.

Examining User Information

Click **Forensic** > **User** to access the User view.

This view shows general user information:

- Name of the user with a link to more detailed information for the user.
- Alerts that have been raised by the user's activities
- Number of communities the user is a member of with a link to the communites page
- Location of the user
- Last entity accessed by the user

Click the user name to access more detailed information in the User Overview

Examining Entity Information

Click **Forensic** > **Entity** to access the Entity view.

This page shows general information for entities being accessed by users:

Describes details including:

- Entity name
- Entity type
- Community relationship with entity
- Entity path
- Last accessed time
- Entity size

Click the Entity Name to access more detailed information in the Entity Overview

Click the Community count to show which communities contain the entity.

Examining Communities Information

Click **Forensic** > **Communities** to access the the Communities page.

This view provides:

- Community names
- Alerts related to the community
- User count for the community
- Entities count for the community

Click or search a Community name to access the Community details page.

Community Profile
Lists the community users locations and the other closest communities.

Community Behaviour
Shows the number of entities accessed and shows read, write, and metea data access operations.

User and Entities
Identifies total users and total entities in the community.

Community Analysis

- Community user trend
- Operations performed on entities
- Alert trend

Click the community name to access more detailed information in the Community Details

Examining User Activity Information

Click **Forensic** > **User Activity** to access the the User Activity view.

For each user being monitored, this view describes:

- Entity access time
- User who accessed the entity with a link to the user overview
- Activity performed:
  - Read
  - Write
  - Create
  - Rename
- Entity path
- Entity type
- Access location
  Click the user name to access more detailed information in the Entity Details

Forensic User Overview

Information for each user is provided in the User Overview. Use these views to understand user characteristics, communities and entities the user is associated with, and the user's recent activities.

User Profile

User Profile information includes contact information and location of the user. The profile provides the following information:

- Name of the user
- Email address of the user
- User's Manager
- Phone contact for the user
- Location of the user

Communities and Entities

The communities and entities information identifies the following:

- The number of communities the user is associated with

- Total users in the associated communities
- Total entities in the associated communities

User Behavior

The user behavior information identifies recent activities and operations performed by the user. This information includes:

- Recent activity
  - Access location
  - Entities accessed
- Operations for the last seven days
  - Number of write operations
  - Number of read operations
  - Number of times meta data was accessed

Forensic Entity Detail

Use the Entity Detail view detailed information about an entity.

Examining Entity Information

Click *Forensic > Entity to access the Entity page.

This page provides:

Entity Profile

Describes details including:

- Name
  - Click to access the [Entity Overview]
- Type
- Communities
- Path
- Last accessed
  - Click user to access the [User Overview]
- Size

User and Community

- The number of times the entity was accessed by users

- The number of times the entity was accessed by Communities.

Entity Bahavior

- Recent Activity:
  - Last accessed date
  - User that last accessed the entity
  - Location the entity was accessed from
- Operations
  - Number of write operations
  - Number of read operations
  - Number of accesses to Meta data

Forensic Community Detail

Use the Forensic Community Page to understand the characteristics of communities that have been created in the Cloud Secure environment.

Community Profile

Use the Community Profile information to understand:

- Entity profile
  - Name
  - Type
  - Most accessed location
  - Owner
  - Size
  - Path

User and community

The user and community shows the number of times an entity has been accessed and from which communities access is being made. This section shows the following information:

- User and Community
  - Users that accessed the entity
  - Communities that accessed the entity

Entity Behaviour

Entity behaviour identifies access information for the entity and details of operations performed on the entity.

- Recent activity
  - Last accessed
  - Last accessed by
  - Last access location
- Operations performed on the entity
  - Writes : 2
  - Read : 0
  - Accessed Meta Data : 0

Forensic Activity History

The Activity History page helps you understand the actions performed on entities in the Cloud Secure environment.

Examining Activity History Data

Click **Forensic** > **Activity History** to access the Activity History page. The data available on this page describes:

- The time an entity was accessed including the year, month, day, and time of the last access.
- The user that accessed the entity with a link to the User Details.
- The activity the user performed:
  - Create
  - Read
  - Read Metadata
  - Copy
  - Delete
  - Write
- The path to the entity with a link to the Entity Detail Data
- The entity type:
  - Stream
  - File

    - Directory
    - Symbolic Link
    - Other Type
- The location (IP address) from which the activity was performed.

Filtering Forensic Activity History Data

You can filter Forensic Activity History data by the following:

- The Activity type:
    - Created
    - Read
    - Read Metadata
    - Copied
    - Deleted
    - Write
- Entity type:
    - Stream
    - File
    - Directory
    - Symbolic Link
    - Other Type
- Location that the entity was accessed from
- Path of the entity
- Time the activity occurred
- User performing the activity

Exporting Activity History

You can export the activity history to a .CSV file by clicking the *Export* button above the Activity History table. Note that only the top 10,000 records are exported.

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.