警

Cloud Insights

Tony Lavoie
August 26, 2021

This PDF was generated from https://docs.netapp.com/zh-cn/cloudinsights/cs_alert_data.html on October 26, 2021. Always check docs.netapp.com for the latest.

目□

警□

Cloud Secure 警□□面□示最近攻□和 / 或警告的□□□，并可用于□看□个□□描述的□□信息。

[警□列表]

警□

警□列表□示一个□形，其中□示了□定□□□□内引□的潜在攻□和 / 或警告□数，然后列出了□□□□□内□生的攻□和 / 或警告。□可以通□□整□中的□始□□和□束□□滑□来更改□□□□。

□于□个警□，将□示以下内容：

- 潜在攻□： *
- 潜在攻□□型（例如勒索□件）
- □□到潜在攻□的日期和□□
- 警□的 *Status* ：
  - 新□（□是新警□的默□□置）
  - 正在□行中
  - 已解决
  - 已取消

    管理□可以更改警□状□并添加注□以□助□□。

  [更改警□状□]
- 其行□触□警□的 *User*
- 攻□的 *Event* （例如，大量文件已加密）
- 已□行操作 _ （例如，已□建快照）
- 警告： *
- 触□警告的 _Abnormal behavior _
- □□到行□的日期和□□
- 警□的 *Status* ：
  - 新□（□是新警□的默□□置）
  - 正在□行中
  - 已解决
  - 已取消

    管理□可以更改警□状□并添加注□以□助□□。

- 其行□触□警□的 *User*
- *Change* 的□□描述（例如，文件□□□常□加）
- 已采取操作 _

□□器□□

□可以按以下方式□□警□：

- 警□的 *Status*
- *Note* 中的特定文本
- _ 攻□ / 警告 _ 的□型
- 操作触□警□ / 警告的 *User*

警□□□信息□面

□可以□□警□列表□面上的警□□接以打□警□的□□信息□面。警□□□信息可能因攻□或警□□型而□。例如，勒索□件攻□□□信息□面可能会□示以下信息：

摘要部分：

- 攻□□型（在此示例中□勒索□件）和警□ ID （由 Cloud Secure 分配）
- □□到攻□的日期和□□
- 已□行操作（例如，已□建自□快照。Snapshot □□□示在摘要部分的正下方）
- 状□（新□，正在□行等）

攻□□果部分：

- 受影□卷和文件的数量
- 随附的□□摘要
- □示攻□期□文件活□的□形

相□用□部分：

此部分□示有□参与潜在攻□的用□的□□信息，包括用□的 "Top Activity" □形。

□示潜在勒索□件攻□的警□□面：[勒索□件警□示例]

潜在勒索□件攻□的□□信息□面：[勒索□件□□信息□面示例]

□行 Snapshot 操作

Cloud Secure 可在□□到□意活□□自□□建快照以保□□的数据，并□保安全地□□□的数据。

□可以定□ "自□□□策略" 在□□到勒索□件攻□或其他□常用□活□□□建快照。□也可以从警□□面手□□建快照。

自□□建快照：[警□操作屏幕， 1000]

手□快照：[警□操作屏幕， 1000]

警□通知

警□的□子□件通知会□送到警□的□个操作的警□收件人列表。要配置警□收件人，□□□ * 管理□ > 通知 * 并□□个收件人□入一个□子□件地址。

保留策略

警□和警告保留 13 个月。超□ 13 个月的警□和警告将被□除。如果□除了 Cloud Secure □境，□与□□境□□的所有数据也将被□除。

故障排除

□□：	□□□以下操作：
□于 Cloud Secure （ CS ）□建的快照， CS 快照是否有清除 / □□期限？	否没有□ CS 快照□置清除 / □□期限。用□需要□ CS 快照定□清除策略。□参□ "ONTAP 文□" 有□如何□置策略的信息。
有□， ONTAP □天□小□□建一次快照。Cloud Secure （ CS ）快照是否会影□它？CS 快照是否会采用□小□快照位置？默□□小□快照是否会停止？	Cloud Secure 快照不会影□□小□快照。CS 快照不会占用□小□快照空□，□像以前一□□□使用。默□的□小□快照不会停止。
如果在 ONTAP 中□到最大快照数，会□生什□情况？	如果□到最大 Snapshot □数，□后□ Snapshot 生成将失□， Cloud Secure 将□示一条□□消息，指出 Snapshot 已□。用□需要定□ Snapshot 策略以□除最早的快照，否□不会□建快照。在 ONTAP 9.3 及更早版本中，一个卷最多可包含 255 个 Snapshot 副本。在 ONTAP 9.4 及更高版本中，一个卷最多可以包含 1023 个 Snapshot 副本。有□的信息，□参□ ONTAP 文□ " 正在□置 Snapshot □除策略"。
Cloud Secure 根本无法□建快照。	□保用于□建快照的角色具有□接：已分配 proper □限。□保□ *csrole* □建了用于□建快照的正□□□□限： security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
□于 SVM 上□早的警□，快照失□，□些警□已从 Cloud Secure 中□除并随后重新添加。□于在重新添加 SVM 后出□的新警□，将□建快照。	□□情况□少。如果□遇到□□情况，□登□到 ONTAP 并□□早的警□手□□建快照。
在 *Alert Details* □面中，在 *Take Snapshot* 按□下方会□示消息 "Last Attempt Failed" □□。将鼠□□停在□□上会□示 "invoke API command has timed out for the data collector with id" 。	如果通□ SVM 管理 IP 将数据收集器添加到 Cloud Secure 中，并且 ONTAP 中 SVM 的 LIF □于 _disabled" 状□，□可能会□生□□情况。在 ONTAP 中□用特定 LIF 并从 Cloud Secure 触□ _Take Snapshot Manually _ 。然后， Snapshot 操作将成功。

Copyright Information

Copyright © 2021 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.