



# **security anti-ransomware commands**

## **ONTAP 9.10.1 commands**

NetApp

February 11, 2024

# Table of Contents

- security anti-ransomware commands . . . . . 1
  - security anti-ransomware volume disable . . . . . 1
  - security anti-ransomware volume dry-run . . . . . 1
  - security anti-ransomware volume enable . . . . . 2
  - security anti-ransomware volume pause . . . . . 2
  - security anti-ransomware volume resume . . . . . 2
  - security anti-ransomware volume show . . . . . 3
  - security anti-ransomware volume attack clear-suspect . . . . . 5
  - security anti-ransomware volume attack generate-report . . . . . 6
  - security anti-ransomware volume space show . . . . . 7
  - security anti-ransomware volume workload-behavior show . . . . . 8

# security anti-ransomware commands

## security anti-ransomware volume disable

Disable anti-ransomware on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `security anti-ransomware volume disable` command disables anti-ransomware monitoring on a volume.

### Parameters

**-vserver <vserver name> - Vserver Name**

Anti-ransomware monitoring is disabled on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

**-volume <volume name> - Volume Name**

Anti-ransomware monitoring is disabled on volumes matching the parameter value.

### Examples

## security anti-ransomware volume dry-run

Dry-run anti-ransomware on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The `security anti-ransomware volume dry-run` command starts anti-ransomware monitoring in the evaluation mode on a volume.

### Parameters

**-vserver <vserver name> - Vserver Name**

Anti-ransomware monitoring is enabled in the evaluation mode on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

**-volume <volume name> - Volume Name**

Anti-ransomware monitoring is enabled in the evaluation mode on volumes matching the parameter value.

### Examples

# security anti-ransomware volume enable

Enable anti-ransomware on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `security anti-ransomware volume enable` command enables anti-ransomware monitoring on a volume.

## Parameters

**-vserver <vserver name> - Vserver Name**

Anti-ransomware monitoring is enabled on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

**-volume <volume name> - Volume Name**

Anti-ransomware monitoring is enabled on volumes matching the parameter value.

## Examples

# security anti-ransomware volume pause

Pause anti-ransomware on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `security anti-ransomware volume pause` command pauses Anti-ransomware monitoring on a volume.

## Parameters

**-vserver <vserver name> - Vserver Name**

Anti-ransomware monitoring is paused in the evaluation mode on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

**-volume <volume name> - Volume Name**

Anti-ransomware monitoring is paused on volumes matching the parameter value.

## Examples

# security anti-ransomware volume resume

Resume anti-ransomware on a volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `security anti-ransomware volume resume` command resumes Anti-ransomware monitoring on a volume.

## Parameters

### **-vserver <vserver name> - Vserver Name**

Anti-ransomware monitoring is resumed on volumes that match the values for the Vserver and volume parameters. If only one data Vserver exists, you do not need to specify this parameter.

### **-volume <volume name> - Volume Name**

Anti-ransomware monitoring is resumed on volumes matching the parameter value.

## Examples

# security anti-ransomware volume show

Show anti-ransomware related information of volumes

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `security anti-ransomware volume show` command displays information related to Anti-ransomware on the volumes in the cluster. The following information is displayed:

- Vserver Name: The Vserver on which the volume is located.
- Volume Name: The volume name
- State: The Anti-ransomware state of the volume. The possible values are *disabled*, *enabled*, *dry-run*, *dry-run-paused*, *enable-paused* and *disable-in-progress*.

## Parameters

### **{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

### **| [-attack ]**

If this parameter is specified, ransomware attack details are displayed.

### **| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

### **[-vserver <vserver name>] - Vserver Name**

If this parameter and the `-volume` parameter are specified, the command displays detailed information related to Anti-ransomware about the specified volume. If this parameter is specified by itself, the command displays information related to the Anti-ransomware about all volumes on the specified Vservee.

### **[-volume <volume name>] - Volume Name**

If this parameter and the `-vserver` parameter are specified, the command displays detailed information related to Anti-ransomware about the specified volume. If this parameter is specified by itself, the command displays information related to the Anti-ransomware about all volumes matching the specified name.

### **[-state {disabled|enabled|dry-run|dry-run-paused|enable-paused|disable-in-progress}] - State**

If this parameter is specified, the command displays information only about the volume or volumes that have the specified Anti-ransomware state. The possible values are *disabled*, *enabled*, *dry-run*, *dry-run-paused*, *enable-paused* and *disable-in-progress*. The possible states are:

- disabled - Anti-ransomware is disabled on the volume.
- enabled - Anti-ransomware is enabled on the volume.
- dry-run - Anti-ransomware is enabled in the dry-run or evaluation mode on the volume.
- dry-run-paused - Anti-ransomware is paused from dry-run or evaluation mode on the volume.
- enable-paused - Anti-ransomware is paused on the volume.
- disable-in-progress - Anti-ransomware disable work is in progress on the volume.

### **[-attack-probability {none|low|moderate|high}] - Attack Probability**

If this parameter is specified, the command displays information only about the volumes that have the specified probability. The possible values are *none*, *low*, *moderate*, and *high*.

- none - No data is suspected for ransomware activity.
- low - Small amount data is suspected for ransomware activity.
- moderate - Moderate amount of data is suspected for ransomware activity.
- high - Large amount data is suspected for ransomware activity.

### **[-attack-timeline <MM/DD/YYYY HH:MM:SS>,...] - Attack Timeline**

If this parameter is specified, the command displays information only about the volumes that have the specified attack-timeline.

### **[-no-of-attacks <integer>] - Number of Attacks**

This provides the number of ransomware attacks observed.

## **Examples**

The following example shows a sample output for this command:

```
cluster1:> security anti-ransomware volume show
```

| Vserver | Volume | State   |
|---------|--------|---------|
| -----   | -----  | -----   |
| vs1     | vol1   | enabled |

# security anti-ransomware volume attack clear-suspect

Clear suspect record

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

The `anti-ransomware volume attack clear-suspect` command removes the specified files from suspect files report. When no optional parameters are provided, the suspect report file is cleared.

## Parameters

**-vserver <vserver name> - Vserver Name**

This parameter specifies the Vserver on which the volume is located.

**-volume <volume name> - Volume Name**

This parameter specifies the name of the volume on which anti-ransomware feature is enabled.

**{ [-sequence-number <integer>] - Sequence Number (privilege: advanced)**

This optionally specifies the sequence number of the suspect file obtained from generated report.

**{ [-extensions <text>, ...] - File Extensions**

This optionally specifies the extensions of ransomware attacked files that needs to be cleared from attack report.

**| [-start-time <MM/DD/YYYY HH:MM:SS>] - Start Time**

This optionally specifies the lower bound of the time to clear a suspect record. Any suspect record with time greater than or equal to start-time is cleared.

**[-end-time <MM/DD/YYYY HH:MM:SS>] - End Time }**

This optionally specifies upper bound of the time to clear a suspect record. Any suspect record with time less than or equal to end-time is cleared.

**-false-positive {true|false} - False Positive?**

This indicates whether the suspect record of specific extensions, time range, and so on, are to be considered a false positive.

## Examples

The following example shows a sample output for clearing all the suspects observed with timestamp in the start-time and end-time range, and with given extension.

```
clus1::> security anti-ransomware volume attack clear-suspect -volume  
testvol -start-time "4/14/2021 04:16:48" -end-time "4/14/2021 06:16:50"  
5 suspect records cleared.
```

The following examples shows output when given sequence-number is not present.

```
clus1::*> security anti-ransomware volume attack clear-suspect -volume  
testvol -sequence-number 1000
```

Error: command failed: No suspect records found.

## security anti-ransomware volume attack generate-report

Generates Report File of the Suspected Attack on the Volume

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

The anti-ransomware volume attack generate-report command copies the report file to the given path.

### Parameters

**-vserver <vserver name> - Vserver Name**

This parameter specifies the Vserver on which the volume is located.

**-volume <volume name> - Volume Name**

This parameter specifies the name of the volume on which anti-ransomware feature is enabled.

**-dest-path <[vserver:]volume/path/to/filename> - Destination path under the volume to copy the file**

This parameter specifies the path where requested file is to be copied.

### Examples

The following example displays command output:

```
node::*> security anti-ransomware volume attack generate-report -volume  
vol1 -dest-path vs1:vol1/  
Report "report_file_vs1vol1_30-03-2021_16-11-38" available at path  
"vs1:vol1/".
```



# security anti-ransomware volume space show

Display the details of anti-ransomware space usage

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

## Description

This `security anti-ransomware volume space show` displays the space usage by Anti-ransomware feature.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>`, ... parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**[-vserver <vserver name>] - Vserver Name**

This parameter specifies the Vserver on which the volume is located.

**[-volume <volume name>] - Volume Name**

This parameter specifies the name of the volume whose space usage details are to be shown.

**[-space-used-by-snapshot {<integer>[KB|MB|GB|TB|PB] } ] - Space Used by snapshots**

This parameter shows space usage by Anti-ransomware Snapshot copies.

**[-space-used-by-logs {<integer>[KB|MB|GB|TB|PB] } ] - Space Used by logs**

This parameter shows the space used by the Anti-ransomware logs.

**[-total-space-used {<integer>[KB|MB|GB|TB|PB] } ] - Total space used by anti-ransomware**

This parameter shows the total space used by the Anti-ransomware feature.

**[-no-of-snapshot <integer>] - Number of Anti-ransomware Snapshot Copies**

This parameter shows the total count of the Anti-ransomware Snapshot copies.

## Examples

The following example shows a sample output for this command:

```
clus1::>> security anti-ransomware volume space show
```

| Vserver | Volume | Space Used By<br>Snapshot | Space Used By<br>logs | Total Space<br>Used | Snapshot<br>Copies |
|---------|--------|---------------------------|-----------------------|---------------------|--------------------|
| vs1     | vol1   | 308KB                     | 8B                    | 308.0KB             | 2                  |

## security anti-ransomware volume workload-behavior show

Display information about the volume's workload-behavior learnt by the analytics algorithm

**Availability:** This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

### Description

This `security anti-ransomware volume workload-behavior show` displays the workload characteristics observed by Anti-ransomware analytics engine.

### Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>, ...` parameter, the command output also includes the specified field or fields. You can use `'-fields ?'` to display the fields to specify.

**| [-instance ] }**

If you specify the `-instance` parameter, the command displays detailed information about all fields.

**-vserver <vserver name> - Vserver Name**

This parameter specifies the Vserver on which the volume is located.

**-volume <volume name> - Volume Name**

This parameter specifies the name of the volume whose workload details are to be shown.

**[-file-extensions-included <text>,...] - File Extensions Expected in the Workload**

This parameter displays the list of extensions observed by Anti-ransomware.

### Examples

The following example shows a sample output for this command:

```
clus1::>> security anti-ransomware volume workload-behavior show -vserver  
vs1 -volume testvol  
Vserver                : vsa  
Volume                 : testvol  
File Extensions Included : pdf, doc, txt
```

## Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## 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.