security protocol commands

ONTAP 9.7 commands

NetApp
February 11, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-97/security-protocol-modify.html on February 11, 2024. Always check docs.netapp.com for the latest.

Table of Contents

security protocol commands . . . 1
- security protocol modify . . . 1
- security protocol show . . . 1
- security protocol ssh modify . . . 2
- security protocol ssh show . . . 3

security protocol commands

security protocol modify

Modify application configuration options

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

The `security protocol modify` command modifies the existing cluster-wide configuration of RSH and Telnet. Enable RSH and Telnet in the cluster by setting the enabled field as *`true`* .

Parameters

`-application <text>` - application (privilege: advanced)

Selects the application. Supported values are *`rsh`* and *`telnet`* .

`[-enabled {true|false}]` - enabled (privilege: advanced)

Enables or disables the corresponding application. The default value is *`false`* .

Examples

The following command enables RSH in the cluster. The default setting for RSH is *`false`* :

```
cluster1::> security protocol modify -application rsh -enabled true
```

The following command enables Telnet in the cluster. The default setting for Telnet is *`false`* :

```
cluster1::> security protocol modify -application telnet -enabled true
```

security protocol show

Show application configuration options

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

The `security protocol show` command displays the cluster-wide configuration of RSH and Telnet in the cluster in advanced privilege mode. RSH and Telnet are disabled by default. Use the security protocol modify command to change the RSH and Telnet configuration that the cluster supports.

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.

[-application <text>] - application (privilege: advanced)

Displays the insecure applications in the cluster.

[-enabled {true|false}] - enabled (privilege: advanced)

Displays whether the application is enabled or disabled in the cluster.

Examples

The following example shows the default security protocol configurations for a cluster:

```
cluster1::> security protocol show

Application      Enabled
------------    -------------
rsh             false
telnet          false
```

The following example shows the security protocol configuration after RSH and Telnet have been enabled:

```
cluster1::> security protocol show
Application      Enabled
------------    -------------
rsh             true
telnet          true
```

Related Links

- security protocol modify

security protocol ssh modify

Modify the SSH configuration

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

The `security protocol ssh modify` command modifies the existing cluster-wide configuration of SSH

Parameters

`[-per-source-limit <integer>]` - Per-Source Limit (privilege: advanced)

Modifies the maximum number of SSH instances per source IP address on a per-node basis.

`[-max-instances <integer>]` - Maximum Number of Instances (privilege: advanced)

Modifies the maximum number of SSH instances that can be handled on a per-node basis.

`[-connections-per-second <integer>]` - Connections Per Second (privilege: advanced)

Modifies the maximum number of SSH connections per second on a per-node basis.

Examples

The following example modifies cluster-wide SSH configuration:

```
cluster1::*> security protocol ssh modify -per-source-limit 30 -max
-instances 60 -connections-per-second 5
```

security protocol ssh show

Show the SSH configuration

Availability: This command is available to *cluster* administrators at the *advanced* privilege level.

Description

The `security protocol ssh show` command displays the cluster-wide SSH configuration in advanced privilege mode. Use the security protocol ssh modify command to change the SSH configuration that the cluster supports.

Examples

The following example displays cluster-wide SSH configuration:

```
cluster1::*> security protocol ssh show
Per-Source Limit: 32
Maximum Number of Instances: 64
     Connections Per Second: 10
```

Related Links

- security protocol ssh modify

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.