security protocol commands

ONTAP 9.9.1 commands

NetApp
February 12, 2024

Table of Contents

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

Trademark information