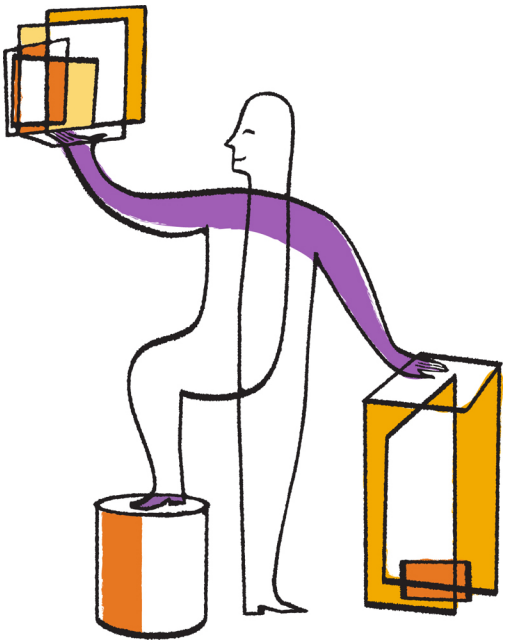
Data ONTAP® 8.2

Remote Support Agent Configuration Guide for 7-Mode

For Use with Data ONTAP



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1(408) 822-6000
Fax: +1(408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08023_A0
May 2013

Contents

What Remote Support Agent is

Remote Support Agent (RSA) is a remote diagnostics data collector that is embedded directly into the storage controller's remote management device firmware. Remote Support Agent enables a NetApp support engineer to remotely request an automated upload of log files, core files, and other diagnostic information stored in the storage controller and to remotely trigger an on-demand AutoSupport collection.

The Remote Support Agent is provided in the latest firmware for storage systems that support an onboard Service Processor (SP) or the Remote LAN Module (RLM) add-on card.

Remote Support Agent can only be installed on systems with the onboard Service Processor or the Remote LAN Module. FAS20xx systems that have the built-in Baseboard Management Controller (BMC) are not supported.

Note: You can access and use the basic SP and RLM features independently of Remote Support Agent.

Remote support architecture

Remote Support Agent is a part of the NetApp Remote Support Diagnostics Tool, which helps NetApp Support solve your storage system issues without the need for staff intervention.

The NetApp Remote Support Diagnostics Tool consists of the following components:

- A remote management device

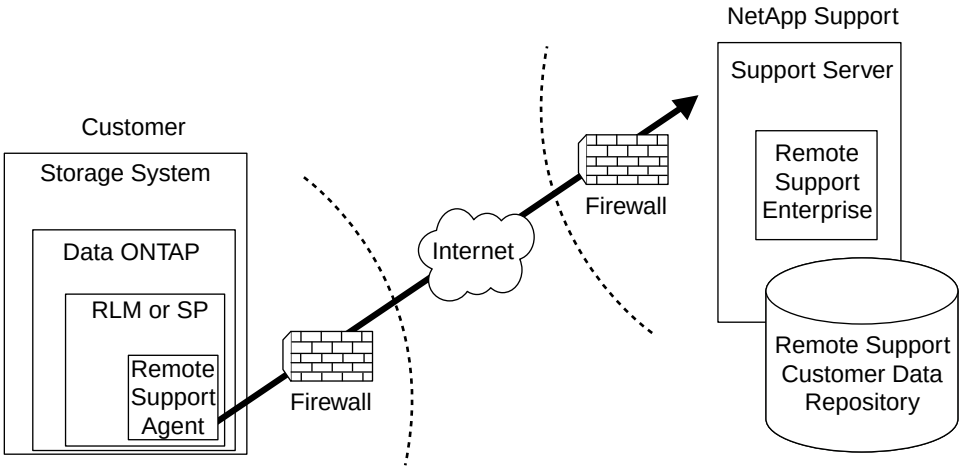
  The remote management device can be the Service Processor (SP) or the Remote LAN Module (RLM), depending on the storage system model.

  The SP/RLM stays operational regardless of the operating state of the system. It provides remote platform management capabilities, including remote access, monitoring, troubleshooting, logging, and alerting features. For more information about the SP/RLM, see the *Data ONTAP System Administration Guide for 7-Mode*.
- Remote Support Agent (RSA)

  Remote Support Agent is part of the SP/RLM firmware.
- Remote Support Enterprise (RSE)

  Remote Support Enterprise is the application and server at NetApp that listens for the customer's Remote Support Agent connection and provides the GUI that a NetApp Technical Support Engineer uses to request diagnostic data. RSA communicates with RSE to receive support action requests and send diagnostic data.

The following diagram illustrates the architecture of the NetApp Remote Support Diagnostics Tool in 7-mode systems:



Related information

NetApp Remote Support Diagnostics Tool page - support.netapp.com/NOW/download/tools/rsa/

What Remote Support Agent does

Remote Support Agent remotely collects data, intelligently handles core files, and sends notification of down storage controllers.

- Remote data collection

  Remote Support Agent enables NetApp Support to request the upload of files from the `/etc/log` and `/etc/crash` directories and their subdirectories. These two directories contain only NetApp storage controller environmental and debugging information and do not contain any customer-sensitive data. Multiple files can be requested from these directories, as required, during case triage. Remote Support Agent also enables NetApp Support to remotely trigger an AutoSupport message on your storage controller and have a complete AutoSupport log returned by using the Data ONTAP AutoSupport mechanism.
- Intelligent core file handling

  When a system panics, Remote Support Agent automatically uploads the core file to NetApp Support without your intervention. Remote Support Agent uploads a core file only if it is not corrupted and the panic signature does not match any known panic message in the NetApp panic message database. In such a condition, the case is updated with the latest information.

  Remote Support Agent handles core file upload failure as follows:

- Failure on the storage controller

  If there is a failure on the storage controller during core file collection, Remote Support Agent retries the core file collection. If unsuccessful, Remote Support Agent terminates the retry and sends a failure alarm to Remote Support Enterprise. When Remote Support Enterprise receives the alarm, it notifies NetApp Support that an automatic core upload failed. NetApp Support then reaches out to customer contacts to request a manual core upload.
- Remote Support Enterprise fault or network outage

  In the event of a network fault or outage during a file transmission, Remote Support Agent retries the file upload several times.
- Notification of down storage controller

  When the SP/RLM detects that a storage controller is down, for example, due to an abnormal reboot, the SP/RLM automatically triggers an AutoSupport message to NetApp Support. A problem case is created and the listed hardware contact is notified. AutoSupport must be enabled for this feature to work correctly.

How Remote Support Agent uses AutoSupport

Remote Support Agent enables a NetApp Support engineer to remotely trigger an AutoSupport request on the storage controller and have the AutoSupport data sent back to NetApp support.

When AutoSupport is configured and enabled on the NetApp storage system, Remote Support Agent enables NetApp Support to begin problem diagnostics immediately without waiting for you to send an updated AutoSupport message. It also enables NetApp Support to effectively troubleshoot cases that occur during off hours when you are not available to send an AutoSupport message.

When Remote Support Agent sends a command to Data ONTAP to trigger an AutoSupport message, the message is uniquely identified by the subject line "Remote Support Agent triggered ASUP."

Remote Support Agent requires the following AutoSupport settings configured on the storage controller:

```
option autosupport.to e-mail_addresses
option autosupport.mailhost { name | IP_address_of_outbound_SMTP }
```

For example, if you subscribe to AutoSupport notifications, you also receive AutoSupport messages that are triggered by Remote Support Agent.

For information about configuring and enabling AutoSupport, see the *Data ONTAP System Administration Guide for 7-Mode*.

How Remote Support Agent uses HTTP or HTTPS

Remote Support Agent uses HTTP or HTTPS to communicate with the storage controller to initiate commands and to collect files. It uses HTTPS to send system logs and core files from the Data ONTAP root volume to Remote Support Enterprise on the NetApp Support side.

During a case triage, the Support team often requires the system logs and core files. Because Remote Support Agent does not have direct hardware access to these files, it uses HTTP or HTTPS to request these files from the storage controller, to manually trigger an AutoSupport message from the storage system, and to monitor the progress of core file operations. It uses HTTPS to communicate with Remote Support Enterprise on the NetApp Support side and to send system logs and core files that are located on the Data ONTAP root volume.

Remote data collection by the NetApp Support team is limited to files within the `/etc/crash` and `/etc/log` directories and their subdirectories.

Using HTTP enables Remote Support Agent's faster access to the diagnostics data on the NetApp controller. Using HTTPS enables enhanced security on the data flow between Remote Support Agent and the NetApp controller within your intranet. You should select the best transport option based on performance and security considerations.

How Remote Support Agent provides data and network security

To ensure data and network security, Remote Support Agent enables you to have full control and visibility over all remote events and activities.

Remote Support Agent uses the following security measures:

- Connections are outbound only.

  Connection between Remote Support Agent and Remote Support Enterprise is always initiated by Remote Support Agent. This ensures that there is only an outbound connection from your site to technical support.

  Remote Support Agent does not allow dial-in access from NetApp to your system. Remote Support Agent periodically connects to Remote Support Enterprise, downloads any action requests, and uploads the system status or results to satisfy previous requests to Remote Support Enterprise.

  The normal health check connection interval is every five minutes for storage controllers that are not being actively assisted by a NetApp Support engineer in case triage. The connection interval changes to every 10 seconds if a NetApp Support engineer requests remote data collection from the storage system. The collection interval returns to the normal interval within a short time after case triage requests have stopped.
- All communications are authenticated.

Communication between Remote Support Agent and Remote Support Enterprise is encrypted using 128-bit VeriSign signed Secure Socket Layer (SSL) certificates. Remote Support Agent retains a copy of the Remote Support Enterprise public certificate to ensure that communication occurs only with NetApp Support. If the authentication fails, the connection is broken and no data is sent.

- Access to diagnostic data is controlled.

  Remote Support Agent connects to the NetApp Support server periodically, to transfer information and respond to service requests. After data exchange, if no session (such as a file transfer) is active, the connection is closed.

  Remote Support Agent does not have access to your user data. The only directory trees that are accessible from the root volume of the storage system are `/etc/crash` and `/etc/log`and their subdirectories.
- Diagnostic data is stored securely.

  Data that is uploaded from Remote Support Agent is stored in a highly secure Oracle database behind the NetApp corporate firewall. Access to this data is restricted to authorized NetApp Support personnel. All actions taken by NetApp Support using Remote Support Enterprise are recorded and can be audited by accessing the Remote Support Enterprise interface at your NetApp Support site login.
- Security assessments are conducted periodically.

  Security assessments help to ensure that Remote Support Agent conforms to industry best practices for protecting your data. For more information, see the Third-Party Security Assessment link under the Additional Information heading to examine the Remote LAN Module Security Assessment white paper by Symantec at *support.netapp.com/NOW/download/tools/rsa/*.
- Security policies are checked at startup.

  When Remote Support Agent starts, it checks the security policies that are configured in the storage controller. Remote Support Agent is notified whenever you change the security policies.

  If the security policy does not allow communication to the Remote Support Enterprise server, then Remote Support Agent does not connect to Remote Support Enterprise. Remote Support Agent features, including remote data collection, core upload, and AutoSupport message generation, are disabled.

  If the security policy is changed from allowing communication to not allowing communication, then Remote Support Agent reports the new policy to Remote Support Enterprise and stops any subsequent contact with Remote Support Enterprise.

You can disable the connection to NetApp Support and all Remote Support Agent features by using the `rsa setup` command with the `policy -enable` option set to No.

How the SP/RLM provides data and network security

The SP/RLM on your storage controller uses single outbound-only ethernet connection, locally secured username and passwords, and a single port for data and network security support.

- A single ethernet connection is the only external interface on the SP/RLM.

The SP/RLM firewall prevents incoming connections from outside your network. It allows only connections from within your network by the Data ONTAP administration accounts (inbound SSH only).

- Connections to NetApp are outgoing only.

  Only an outgoing connection to NetApp on port 443 is allowed. Data collection is only from the `/etc/crash` and `/etc/log` and their subdirectories.
- Administrator user ID and password is required.

  The administrator user ID and password that is configured in Data ONTAP is supplied to the configuration of the Remote Support Agent so that it can communicate with Data ONTAP. The SP/RLM controls access to the storage system. There is no requirement for a special account; you can use any account as long as it is in the Data ONTAP Administrators group. If multiple administrators are sharing the account, then a recommended best practice is to create a special account for Remote Support Agent usage.
- Only one port accepts connections.

  The only SP/RLM port that accepts connection requests is SSH (port 22). The only outbound ports allowed are SMTP (port 25), SNMP (trap port 162), and SSL (port 443).

Where to find more information about Remote Support Agent

You can find additional information about Remote Support Agent, SP, RLM, and Remote Support Enterprise in documents on the NetApp Support Site.

- The NetApp Remote Support Diagnostics Tool section of the NetApp Support Site at *support.netapp.com* contains useful background information, an FAQ section, and a security assessment.
- The *Data ONTAP System Administration Guide for 7-Mode* contains information about SP and RLM, AutoSupport, and Remote Support Enterprise.
- The *Data ONTAP Upgrade and Revert/Downgrade Guide for 7-Mode* contains information about updating the SP and RLM firmware.

Configuring Remote Support Agent

Configuring Remote Support Agent consists of upgrading the SP/RLM, configuring your storage system, and then configuring Remote Support Agent.

Predeployment checklist

Before you begin to configure Remote Support Agent, you should be sure that it satisfies your security policies for Internet access and meets these requirements.

Ensure that all of the following are true. For more information about Data ONTAP commands, see the *Data ONTAP System Administration Guide for 7-Mode* and the appropriate man pages.

- Remote Support Agent is provided as a firmware upgrade to the Remote LAN Module (RLM) card.

  Firmware 3.0 or later is required; release 4.0 or later is recommended.
- Remote Support Agent is included in the Service Processor (SP) firmware on FAS/V 2200, 3200, and 6200 systems.
- FAS20xx systems that have the built-in Baseboard Management Controller (BMC) are not supported.
- You must have a 128-bit, encrypted, outbound HTTPS connection to the Internet over port 443.
- You must have a 10/100 megabits per second full-duplex Ethernet port with autonegotiation enabled.
- You must have the ability to access the target URL *http://support.netapp.com/NOW/download/tools/rsa/*.
- AutoSupport must be enabled on the storage system.
- The SP/RLM must be configured.

  The `sp setup` and `rlm setup` commands display the SP/RLM configuration.
- SP/RLM must be able to send a test AutoSupport message.

  The `options autosupport.to`, `options autosupport.mailhost`, and `rlm test autosupport` or `sp test autosupport` commands enable you to verify whether the SP/RLM is able to send a test message.

Upgrading the SP/RLM firmware

Before you configure Remote Support Agent, you should check whether the SP/RLM needs a firmware upgrade.

Steps

1. Download the latest SP/RLM firmware.

Use the Data ONTAP console or the SP/RLM CLI. Do not use a Data ONTAP telnet or rsh session to upgrade firmware.

For information and detailed instructions about upgrading the SP/RLM firmware, see the *Data ONTAP Upgrade and Revert/Downgrade Guide for 7-Mode*.

2. Configure the SP/RLM for your storage controller and network.

   For information and detailed instructions for configuring the SP/RLM, see the *Data ONTAP System Administration Guide for 7-Mode*.

Configuring your 7-Mode storage system

Before you configure Remote Support Agent software, you must first configure the storage system to enable Remote Support Agent to communicate with Data ONTAP.

About this task

This task configures the following on your storage system:

- Enables AutoSupport
- Configures HTTP and HTTPS
- Creates a user in the administrators group (this is recommended, but not required)

For detailed information about configuring your storage system, see the *Data ONTAP System Administration Guide for 7-Mode*.

Steps

1. To enable AutoSupport collection and delivery, use the `autosupport.enable on` command.

   By default, AutoSupport data collection is enabled on storage systems.

2. To configure HTTPS or HTTP, which enables Remote Support Agent to communicate with Data ONTAP, use the following options.

If you are configuring...	Then...

HTTPS	Set the following options to `on`:
	`httpd.admin.ssl.enable`
	`httpd.autoindex.enable`

HTTP	Set the following options to `on`:
	`httpd.admin.enable`
	`httpd.autoindex.enable`

   If the `httpd.admin.access` or `trusted.hosts` options are used to control access, add the IP address of the remote management device to enable access from the SP/RLM.

3. To create an administrator account for Remote Support Agent, use the `useradmin user add` command.

   Example

   For example, the following command creates an account named NetAppRSA:

   ```
   filer> useradmin user add NetAppRSA -g Administrators
   ```

Configuring Remote Support Agent software on 7-Mode systems

After upgrading SP and RLM, if necessary, and configuring your storage system, you must configure the Remote Support Agent software.

Before you begin

You must have the following information available:

- Network information (the proxy configuration, if required to access the Internet):
  - Proxy IP address
  - Proxy type (SOCKS or HTTP)
  - Proxy user name and password
- Data ONTAP information
  - Administration HTTP or HTTPS IP address
  - Port number
  - Agent administrator user name and password

Steps

1. Use the `% ssh naroot@<RLM` command to connect to SP or RLM with your SSH client.

   The IP address is the node management IP address.

2. Use the SP/RLM `version` command to verify that the remote management device is using the latest firmware.

3. Start an interactive configuration session by using the `rsa setup` command; when prompted to test the configuration, type `yes`.

   When prompted, provide the information needed during the interactive session.

   Example

   Sample output of the `rsa setup` command when no proxy support is needed:

   ```
   RLM or-321> rsa setup
   The Remote Support Agent improves your case resolution time and
   ```

```
minimizes your manual support overhead.

Would you like to enable Remote Support Agent? [yes]:
Do you use a proxy to connect to the internet? [no]:
Enter the HTTP host name or ip-address of your storage controller
[]: or-321.lab.netapp.com
Do you want to use HTTP with SSL? [yes]:
Enter HTTPS port number [443]:
Enter HTTP username []: rsa-http
Enter HTTP password:

Do you want to commit configuration changes entered above? [yes]:
Committing configuration changes... done
Remote Support Agent is enabled.
Do you want to test current configuration? [yes]:
Testing storage controller HTTP connection ..................... ok
Testing Remote Support Enterprise connection ................... ok
All configuration tests passed.
```

Example

Sample output of the `rsa setup` command when proxy support is required:

```
RLM or-321> rsa setup
The Remote Support Agent improves your case resolution time and
minimizes your manual support overhead.

Would you like to enable Remote Support Agent? [yes]:
Do you use a proxy to connect to the internet? [no]: yes
Choose proxy protocol (HTTP or SOCKS) [http]:
Enter proxy host name or ip-address []: proxy.lab.netapp.com
Enter proxy port number [9999]: 8080
Does the proxy require a username and password? [no]:
Enter the HTTP host name or ip-address of your storage controller
[]: or-321.lab.netapp.com
Do you want to use HTTP with SSL? [yes]:
Enter HTTPS port number [443]:
Enter HTTP username []: rsa-http
Enter HTTP password:

Do you want to commit configuration changes entered above? [yes]:
Committing configuration changes... done
Remote Support Agent is enabled.
Do you want to test current configuration? [yes]:
Testing storage controller HTTP connection..................... ok
Testing Remote Support Enterprise connection................... ok
All configuration tests passed.
```

4. After the session is complete, verify that the configuration is correct by entering the `rsa show` command.

   You can also use the `rsa show` command to print the configuration.

Example

Sample output of the `rsa show` command when no proxies are configured:

```
RLM or-321> rsa show
Remote Support Agent is enabled.

Remote Support Enterprise URL:
https://remotesupportagent.netapp.com/eMessage

Use proxy: no

Storage controller HTTP host: or-321.lab.netapp.com
HTTP with SSL enabled: no
Storage controller HTTP port: 80
Storage controller HTTP username: rsa321
```

Example

Sample output of the `rsa show` command when proxies are configured:

```
RLM or-321> rsa show
Remote Support Agent is enabled.

Remote Support Enterprise URL:
https://remotesupportagent.netapp.com/eMessage

Use proxy: yes
Proxy protocol: HTTP
Proxy host: proxy.netapp.com
Proxy port: 8080
Use username/password for proxy authentication: yes
Proxy username: proxyuser

Storage controller HTTP host: or-321.lab.netapp.com
HTTP with SSL enabled: no
Storage controller HTTP port: 80
Storage controller HTTP username: rsa321
```

5. View the status of the Remote Support Agent by using the `rsa status` command.

   You can log in to the Remote Support Enterprise (RSE) server to verify registration and view activity audit logs.

Example

Sample output of the `rsa status` command with the verbose (v) option to retrieve detailed information:

```
RLM or-321> rsa status -v
Remote Support Agent is enabled.

Connection status:
HTTP:
```

```
Status               : ok
Last checked         : 23:11 Apr 30 2011

RSE:
Status               : ok
Last checked         : 23:11 Apr 30 2011

Support Information:
System ID            : 0118041496
Heartbeat check      : every 5 minutes

Recent activity:
Directory listing:
Status               : Success
Start                : 23:11 Apr 30 2011
Completion           : 23:11 Apr 30 2011
```

6. Test the remote support configuration by using the `rsa test` command.

   You can test the remote support configuration at any time after the setup is complete.

Managing and monitoring Remote Support Agent

You use CLI commands to configure, disable and enable, display status, and test connections for Remote Support Agent.

Task	Command
Displaying a list of commands and command options	`rsa help`
Configuring, disabling, and enabling Remote Support Agent	`rsa setup`
Displaying the current remote support configuration	`rsa show`
Printing a status report for Remote Support Agent	`rsa status`
Testing the HTTP, proxy, and enterprise connections	`rsa test`

Disabling and enabling Remote Support Agent

You use the `rsa setup` command to disable the remote support functionality and to enable it at another time. Disabling the functionality only modifies the Remote Support Agent's configuration; all other configured attributes remain unchanged.

About this task

When you disable Remote Support Agent, the time required to resolve a case might increase and your ability to receive remote support might decrease.

Step

1. Start an interactive configuration session by using the `rsa setup` command.

Example

Sample output of the `rsa setup` command for disabling Remote Support Agent.

```
SP|RLM> rsa setup
The Remote Support Agent improves your case resolution time and
minimizes your manual support overhead.

Would you like to enable Remote Support Agent? [yes]: no
```

```
Disabling the Remote Support Agent may increase your case
resolution time and your ability to receive remote support.

Do you want to commit configuration changes entered above? [yes]:
Committing configuration changes... done
Remote Support Agent is disabled.
```

Commands for managing Remote Support Agent

You use CLI commands to configure Remote Support Agent, view the remote support configuration and status, and test the remote support connection.

rsa help

The `rsa help` command displays the syntax and description of each `rsa` command.

Syntax

```
rsa help  [setup]  [show]  [test]  [status]
```

Privilege level

Admin

Description

The `rsa help` command displays the syntax and description of each `rsa` command.

If you do not specify an option, the command displays the syntax and descriptions of all the `rsa` commands.

Options

`[setup]`

Displays information about the `rsa setup` command.

`[show]`

Displays information about the `rsa show` command.

`[test]`

Displays information about the `rsa test` command.

`[status]`

Displays information about the `rsa status` command.

rsa setup

The `rsa setup` command configures Remote Support Agent.

Syntax

```
rsa setup  [help]  [proxy [-hostname hostname] [-port port] [-username
username] [-password password] [-credentials {yes | no}] [-enable {on |
off}] ]  [rse [enterprise rse_url]]  [policy [-enable {yes | no}]]  [http
[-hostname hostname] [-port port] [-username username] [-password
password] [-ssl {yes | no}]]
```

Privilege level

Admin

If you specify the `rse` parameter group, you must have the advanced privilege level.

Description

The `rsa setup` command configures and modifies the following remote support parameters for Remote Support Agent:

- Proxy parameters
- Remote Support Enterprise URL options
- Policies to disable or enable Remote Support Agent
- HTTP parameters

If you do not specify an option, the command starts an interactive session to configure the remote support parameters.

Options by parameter group

[`help`]

Displays the `rsa setup` command syntax.

[`proxy` [`-hostname` *hostname*] [`-port` *port*] [`-username` *username*] [`-password` *password*] [`-credentials` {`yes` | `no`}] [`-enable` {`on` | `off`}]]

Specifies the proxy group of parameters you want to configure or modify. If a group is not specified, the command starts an interactive session to configure all the remote support parameters.

[`rse` [`enterprise` *rse_url*]]

Specifies the Remote Support Enterprise parameter you want to configure or modify. If a group is not specified, the command starts an interactive session to configure all the remote support parameters.

[`policy` [`-enable` {`on` | `off`}]]

Enables or disables Remote Support Agent. If a group is not specified, the command starts an interactive session to configure all the remote support parameters.

[`http` [`-hostname` *hostname*] [`-port` *port*] [`-username` *username*] [`-password` *password*] [`-ssl` {`yes` | `no`}]]

Specifies the HTTP parameters you want to configure or modify. If a group is not specified, the command starts an interactive session to configure all the remote support parameters.

Options

`-hostname`

Specifies the host name or IP address of the proxy server or the storage controller HTTP server.

`-port`

Specifies the port number for the proxy server or the storage controller HTTP server. Valid port numbers are from 0 through 65535.

`-username`

Specifies the user name that SP or RLM uses to establish a connection with Remote Support Enterprise.

`-password`

Specifies the password that is associated with the user name.

`-ssl`

Determines which communication protocol is used. If set to `yes`, the HTTPS protocol is used. If set to `no`, the HTTP protocol is used.

`-credentials`

Determines whether proxies are to be used. If set to `yes`, the proxy user name and password are used. If set to `no`, no proxy user name or password is used.

`-enterprise`

Specifies the Remote Support Enterprise URL.

`-enable`

Enables or disables proxy support and Remote Support Agent.

Example: Changing the HTTP parameters interactively using a Data ONTAP version earlier than 8.1.1

The following example changes the communication parameters; because no HTTP options are specified in the command line, the command starts an interactive session:

```
RLM|SP mysystem> rsa setup http
Enter the HTTP host name or ip-address of your
storage controller []: or-186.lab.netapp.com
Do you want to use HTTP with SSL? [yes]:
Enter HTTPS port number [443]:
Enter HTTP username []: http_user
Enter HTTP password:
Do you want to commit configuration changes entered
above? [yes]:
Committing configuration changes... done
```

Example: Changing the HTTP parameters interactively using Data ONTAP version 8.1.1 or later

The following example changes the communication parameters; because no HTTP options are specified in the command line, the command starts an interactive session:

```
RLM|SP mysystem> rsa setup http
Enter the cluster management IP address of your
storage cluster [10.238.142.53]: 10.238.142.53
Do you want to use HTTP with SSL? [yes]:
Enter HTTPS port number [443]:
Enter HTTP username []: http_user
Enter HTTP password:
Do you want to commit configuration changes entered
above? [yes]:
Committing configuration changes... done
```

Example: Changing the proxy parameters on the command line

The following example changes the proxy parameters:

```
RLM|SP> rsa setup proxy -hostname 10.56.0.1
-port 6060 -user proxy_user -password proxy_password
```

Example: Changing the Remote Support Enterprise URL interactively

The following example changes the URL of Remote Support Enterprise; because no Remote Support Enterprise options are specified in the command line, the command starts an interactive session:

```
RLM|SP> rsa setup rse
Configuring Remote Support Enterprise information.
Current Remote Support URL is
https://remotesupportagent.netapp.com/eMessage.
To restore to the default value of
https://remotesupportagent.netapp.com/eMessage,
just press the return key. Enter URL for Remote
Support (or press return)
[https://remotesupportagent.netapp.com/eMessage]:
```

```
https://remotesupportagent.netapp.com/eMessage
Do you want to commit configuration changes entered
above? [yes]:
Committing configuration changes... done
Remote Support Agent is enabled.
```

rsa show

The `rsa show` command displays the current remote support configuration.

Syntax

```
rsa show  [help]  [proxy]  [rse]  [policy]  [http]
```

Privilege level

Admin

Description

The `rsa show` command displays the current remote support configuration.

If you do not specify an option, the command displays the current configuration of all the remote support parameters. If proxies are not enabled, the output of this command does not display the proxy configuration.

Options

[help]

Displays the `rsa show` command syntax.

[proxy]

Displays the configuration of the `proxy` group of parameters.

[rse]

Displays the configured URL of Remote Support Enterprise.

[policy]

Displays the configuration of the `policy` group of parameters.

[http]

Displays the configuration of the `http` group of parameters.

Example: Displaying the remote support configuration with proxies enabled using a Data ONTAP version earlier than 8.1.1

The following example displays the configuration of all the remote support parameters:

```
RLM|SP> rsa show
Remote Support Agent is enabled.
Remote Support Enterprise URL:
https://remotesupportagent.netapp.com/eMessage
Use proxy: yes
Proxy protocol: HTTP
Proxy host: proxy.netapp.com
Proxy port: 8080
Use username/password for proxy authentication: yes
Proxy username: proxyuser
Storage controller HTTP host: or-321.lab.netapp.com
HTTP with SSL enabled: no
Storage controller HTTP port: 80
Storage controller HTTP username: rsa321
```

Example: Displaying the remote support configuration with proxies enabled using Data ONTAP version 8.1.1 or later

The following example displays the configuration of all the remote support parameters:

```
RLM|SP> rsa show
Remote Support Agent is enabled.
Remote Support Enterprise URL:
https://remotesupportagent.netapp.com/eMessage
Use proxy: yes
Proxy protocol: HTTP
Proxy host: proxy.netapp.com
Proxy port: 8080
Use username/password for proxy authentication: yes
Proxy username: proxyuser
Cluster management LIF: 10.238.142.53
HTTP with SSL enabled: no
Storage controller HTTP port: 80
Storage controller HTTP username: rsa321
```

Example: Displaying the remote support configuration with proxies not enabled

The following example displays the configuration of all the remote support parameters in a system that does not have proxies enabled:

```
RLM|SP> rsa show
Remote Support Agent is enabled

Remote Support Enterprise URL:
https://remotesupportagent.netapp.com/eMessage

Use proxy: no

Storage controller HTTP host: or-321.lab.netapp.com
```

```
HTTP with SSL enabled: no
Storage controller HTTP port: 80
```

rsa status

The `rsa status` command displays the current status of the remote support.

Syntax

```
rsa status  [-verbose]
```

Privilege level

Admin

Description

The `rsa status` command displays the current status of the remote support.

Options

`[-verbose]`

(short form: v) Displays the system ID, the heartbeat check interval, the recent remote support activity information, and the current status of all the remote support parameters.

If this parameter is not specified, the command displays only the system ID, the heartbeat check interval, and the recent remote support activity.

Example: Displaying the status of all the remote support parameters

The following example displays the status of all the remote support parameters. You can view and print the status report.

```
RLM|SP> rsa status -v
Remote Support Agent is enabled.

Connection status:

HTTP:
Status             : ok
Last checked       : 23:11 Aug 30 2011

RSE:
Status             : ok
Last checked       : 23:11 Aug 30 2011

Support Information:
System ID          : 01234567890
```

```
Heartbeat check    : every 5 minutes

Recent activity:
Directory listing:
Status             : Success
Start              : 23:11 Aug 30 2011
Completion         : 23:11 Aug 30 2011
RLM|SP>
```

rsa test

The `rsa test` command tests the remote support HTTP and proxy or enterprise connections.

Syntax

```
rsa test  [http]   [rse]
```

Privilege level

Admin

Description

The `rsa test` command tests the remote support HTTP and proxy or enterprise connections.

If you do not specify an option, the command tests all remote support connections.

Options

`[http]`

Tests the storage controller HTTP connection.

`[rse]`

Tests the connection to Remote Support Enterprise.

Example: Testing a healthy connection using Data ONTAP version earlier than 8.1.1

The following example displays the results of successful tests on all the remote support connections.

```
RLM|SP> rsa test
Testing storage controller HTTP connection....... ok
Testing Remote Support Enterprise connection..... ok
All configuration tests passed.
RLM|SP>
```

Example: Testing a healthy connection using Data ONTAP version 8.1.1 or later

The following example displays the results of successful tests on all the remote support connections.

```
RLM|SP> rsa test
Testing cluster management LIF HTTP connection..... ok
Testing Remote Support Enterprise connection..... ok
All configuration tests passed.
RLM|SP>
```

Example: Testing a connection for which Remote Support Agent is not enabled

The following example displays the results of a test on a storage controller that has Remote Support Agent disabled.

```
RLM|SP> rsa test
The Remote Support Agent has not been enabled.
Please run "rsa setup" command to enable the Remote
Support Agent.
RLM|SP>
```

Example: Testing a connection that has problems

The following example displays the results of a test that failed because of an unresponsive server or incorrect hostname configuration.

```
RLM|SP> rsa test
Testing storage controller HTTP connection... failed
HTTP operation timeout
Testing Remote Support Enterprise connection..... ok
One or more configuration tests failed.
RLM|SP>
```

Accessing the Remote Support Enterprise UI

You can use the Remote Support Enterprise user interface on the NetApp Support Site to obtain status and audit history information about your storage controllers that are registered with Remote Support Enterprise.

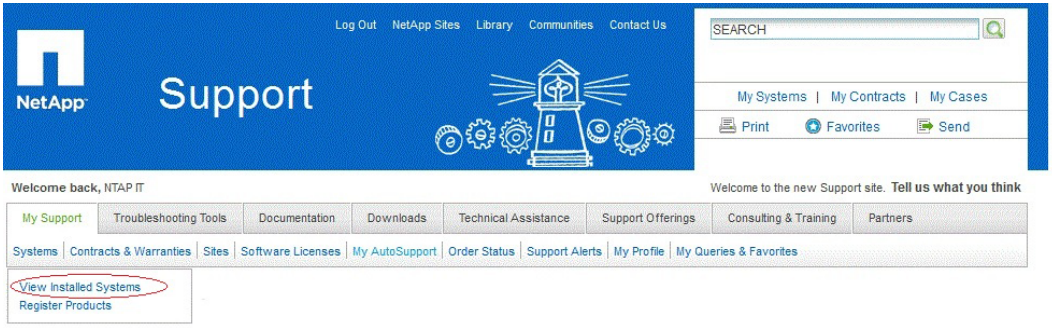
Before you begin

Access to initiate requests to the Remote Support Agent is restricted to NetApp technical support personnel. Access to view status and RSA activity is restricted to the owner of the storage system. You must have a valid account to access the Remote Support Enterprise UI on the NetApp Support Site.

Steps

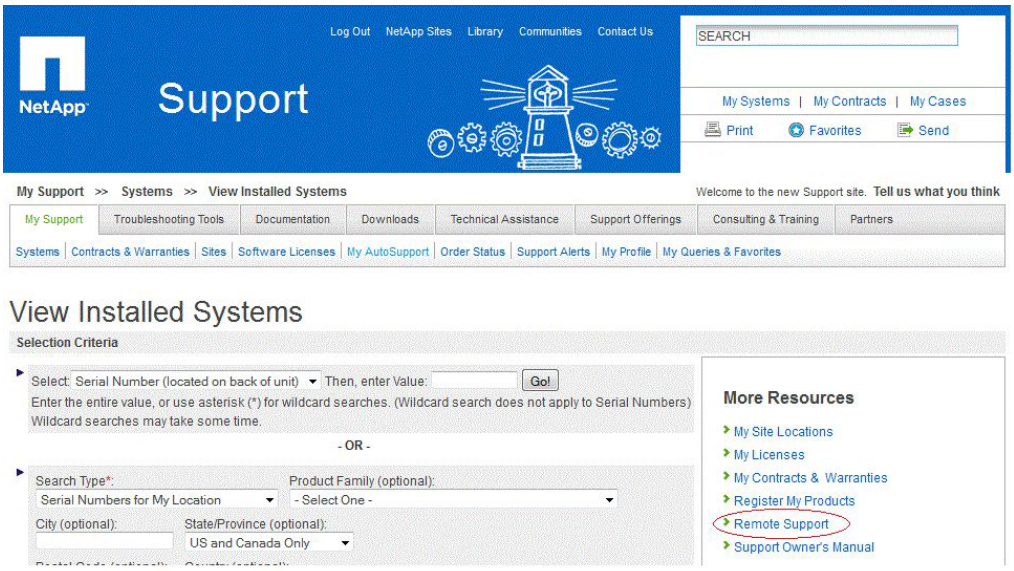
1. Go to support.netapp.com and log in to your NetApp account.
2. On the **Support** page, click **My Support** and select **Systems > View Installed Systems**:

   Example

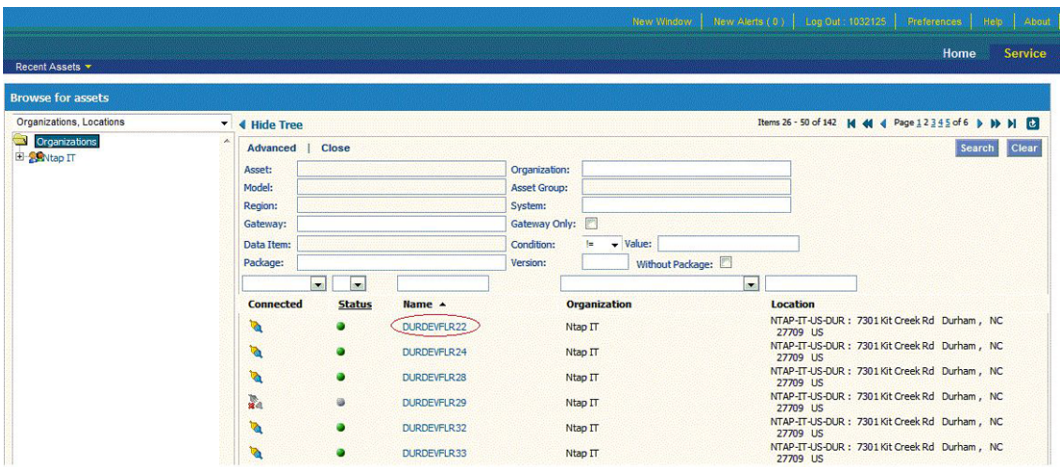
3. On the **View Installed Systems** page, click **More Resources > Remote Support**:

Example



4. In the list of controllers, select the controller for which you want to view remote support activity:

Example



Related references

Remote Support Enterprise service page descriptions on page 29

Remote Support Enterprise service page descriptions

Using the NetApp Support site, you can access the Remote Support Enterprise UI to view all devices registered with the RSE, examine remote actions performed on them, obtain the status information for devices monitored by Remote Support Agent, and obtain an audit history of the actions performed on those devices.

You can access the RSE from the NetApp Support site *support.netapp.com/NOW/download/tools/rsa/*. Select the Systems tab and click the View Installed Systems link. You must log in to the Support site and create a customer account.

RSE Home Page	Displays an overview of the devices that are currently being monitored.
RSE Service Page	Displays a list of all the devices that have been configured with the RSA.
RSE Device Page	Displays a detailed read-only view of the status of your NetApp device, as well as the status of the RSA.
NetApp Controller Summary Panel	Displays a summary of the storage controller status and configuration.
Remote Support Agent Configuration Summary Panel	Displays a summary of the Remote Support Agent status and configuration.
Remote Support Audit Log Panel	Displays a record of all the actions performed on an RSA by technical support.

Troubleshooting

When you receive an error message or experience some other remote support problem, consult the description and corrective action advice.

For up-to-date error information, see the NetApp Remote Support Diagnostics Tool section of the NetApp Support Site at *support.netapp.com*.

Remote support error messages

You can find solutions to remote support error messages by searching product documentation for the strings of error messages, or by the symptom you are experiencing. Follow the instructions in the supplied corrective action, if one is available.

Cannot connect to host

Message	`Cannot connect to host`
Description	This message occurs when Remote Support Agent cannot open the HTTP connection to the storage controller because the storage controller is offline or the storage controller HTTP host name is incorrectly configured.
Corrective action	**1.** Run the `rsa show` command to verify that the storage controller HTTP host name is configured correctly. **2.** If the storage controller host name is incorrect, use the `rsa setup` command to update to the correct host name. **3.** Confirm that the storage controller is online.

Cannot resolve hostname

Message	Cannot resolve hostname
Description	This message occurs when the host name provided for the storage controller HTTP connection is not correct.
Corrective action	**1.** Run the `rsa show` command to verify that the storage controller HTTP host name is configured correctly. **2.** If the storage controller host name is incorrect, use the `rsa setup` command to update the correct host name.

OnCommand System Manager hostname does not match configuration

Message `OnCommand System Manager hostname does not match configuration`

Description This message occurs when the host name or IP address that is provided for the storage controller HTTP connection does not match the configuration of Data ONTAP that is stored in the RLM.

Corrective action

1. Run the `rsa setup` command and enter the correct storage controller HTTP host name or IP address.
2. Run the `rsa show` command to verify that the storage controller HTTP host name and IP address are configured correctly.

HTTP error 403 - access denied

Message `HTTP error 403 - access denied`

Description This message occurs when the user that is configured for the storage controller HTTP connection does not have administrative privileges.

Corrective action Ensure that the user that is configured as the Remote Support Agent belongs to the Administrators group on the storage controller.

HTTP error - invalid username or password...

Message `HTTP error - invalid username or password or insufficient privilege`

Description This message occurs when the user name or password configured for the storage controller HTTP connection is incorrect and when the password used for the storage controller HTTP connection has expired.

Corrective action

1. Run the `rsa setup` command to configure the correct or updated user name and password.
2. Check the password expiration policy that is set for the storage controller. If the password has expired, you must change it.

HTTP health check interface busy

Message `HTTP health check interface busy`

Description This message occurs when the HTTP health check interface is busy.

Corrective action No corrective action is needed. The Remote Support Agent recovers automatically in a few minutes.

HTTP operation timeout

Message `HTTP operation timeout`

Description This message occurs when the storage controller HTTP connection is very busy or when the storage controller is offline.

Corrective action Verify that the storage controller is online.

If it is online, then use the `rsa test` command. If you still get this message, then the HTTP connection is busy with a file transfer operation and no further corrective action is needed.

HTTP version not supported by host

Message `HTTP version not supported by host`

Description This message occurs when the storage controller runs a Data ONTAP version that is incompatible with the host.

Corrective action Ensure that the storage controller is using a Data ONTAP release that is compatible with Remote Support Agent.

Remote Support Policy is disabled

Message Remote Support Policy is disabled

Description This message occurs when the Remote Support Policy is not enabled.

Corrective action Run the `rsa setup` command to enable the Remote Support Agent.

RSE health check interface busy

Message RSE health check interface busy

Description This message occurs when either of the following conditions is encountered:

- The Remote Support Enterprise is not responding, returns an incorrect status, or has an invalid URL.
- Remote Support Agent is processing a file upload.

Corrective action No corrective action is needed. The Remote Support Agent recovers automatically in a few minutes.

RSE or proxy configuration is not valid

Message	RSE or proxy configuration is not valid
Description	This message occurs when the proxy information is configured incorrectly.
Corrective action	1. Run the `rsa setup` command to enter the correct proxy information. 2. Run the `rsa show` command to verify that the proxy information is configured correctly.

Unable to log in to *support.netapp.com*

When you try to log in to the NetApp Support site, you receive a message indicating that the username or password is not valid.

Issue	When you try to log in to *support.netapp.com*, you receive a message indicating that the username or password is not valid.
Cause	You do not have a *support.netapp.com* login ID or the username or password is incorrect.
Corrective action	To create a login ID or to retrieve the forgotten username or password, follow the instructions at *support.netapp.com*.

Unknown host

Message	`Unknown host`
Description	This message occurs when the DNS resolver is not configured correctly in the storage controller.
Corrective action	Run the `rsa setup` command to configure the correct or updated DNS configuration.

Waiting for RLM time to be set

Message	`Waiting for RLM time to be set`
Description	This message occurs when the RLM cannot obtain the time from the storage controller.
Corrective action	Ensure that the storage controller is online. If the storage controller is online, the RLM automatically obtains the time from the storage controller; this usually takes a few minutes. Additional corrective action is not needed.

Remote support problems

You might encounter one of the following remote support problems.

Incorrect field information in NetApp Controller Summary

The information in the NetApp Controller Summary is not correct.

Cause	Remote Support Enterprise did not receive the correct information from Remote Support Agent.
Corrective action	Contact *support.netapp.com*.

Incorrect information in Remote Support Agent Configuration Summary

The information in the Remote Support Agent Configuration Summary is not correct.

Cause	Remote Support Enterprise did not receive the correct information from Remote Support Agent.
Corrective action	Contact *support.netapp.com*.

Incorrect storage controller information

The storage controller site or name, or the company name, is incorrect.

Cause	The records in the NetApp storage controller are incorrect.
Corrective action	Contact *support.netapp.com* to correct the storage controller information.

Unable to log in to *support.netapp.com*

When you try to log in to the NetApp Support site, you receive a message indicating that the username or password is not valid.

Issue	When you try to log in to *support.netapp.com*, you receive a message indicating that the username or password is not valid.
Cause	You do not have a *support.netapp.com* login ID or the username or password is incorrect.
Corrective action	To create a login ID or to retrieve the forgotten username or password, follow the instructions at *support.netapp.com*.

Copyright information

Trademark information

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

S

T