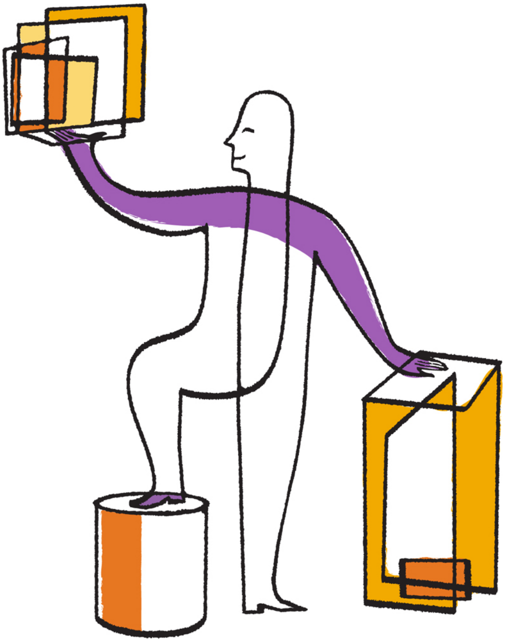
Clustered Data ONTAP® 8.3

Remote Support Agent Configuration Guide

For Use with Clustered 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: 215-09164_A0
November 2014

Contents

What Remote Support Agent is

RSA is a remote diagnostics data collector that is embedded directly in the firmware of the storage controller's remote management device. RSA enables technical support to remotely access log files, core files, and other diagnostic information from the storage controller (using AutoSupport) to solve storage system issues without your intervention.

RSA 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.

RSA can only be installed on systems with the onboard SP or the RLM add-on card. FAS20xx systems that have the built-in Baseboard Management Controller (BMC) are not supported.

Note: You can access and use the basic SP or RLM features independently of RSA.

Component list and architecture of the Remote Support Diagnostics Tool

RSA is part of the NetApp Remote Support Diagnostics Tool, which helps technical support solve your storage system issues without your intervention. The illustrated architecture of this diagnostics tool shows how RSA fits as a component at your site and how technical support accesses it.

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

- A remote management device

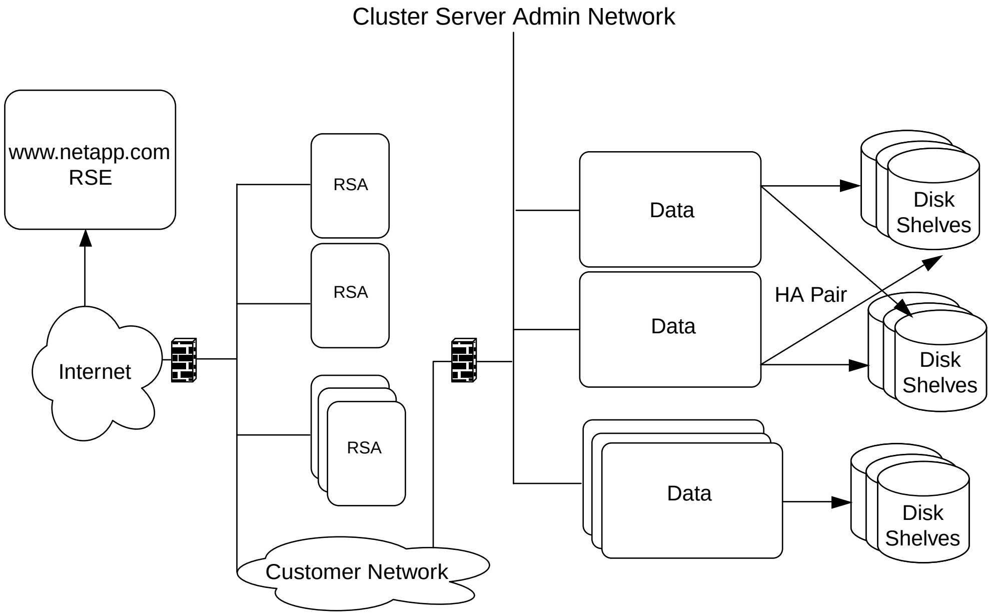
  The remote management device can be the SP or the RLM, depending on the storage system.

  The SP or the RLM remains 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 cluster systems, the SP or the RLM must have access to the Cluster Management LIF. For more information about remote management devices, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.
- RSA

  RSA is part of the SP or the RLM firmware.
- Remote Support Enterprise (RSE)

  RSE is the application and server at NetApp that listens for the customer's RSA connection and provides the GUI that technical support 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 clustered systems:



Related information

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

What RSA does

Configuring RSA at your site allows remote data collection, intelligent core file handling, and notification of down storage controllers for technical support analysis and troubleshooting.

Remote data collection

RSA enables technical support to request the upload of files from the `/mroot/etc/log`, `/mroot/etc/crash`, and`/mroot/etc/mib` directories and their subdirectories in any node that is hosting the Cluster Management LIF. These two directories contain only storage controller environmental and debugging information and do not contain any customer-sensitive data. Multiple files can be uploaded from these directories, as required, during case triage. RSA also enables technical 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, RSA automatically uploads the core file to technical support without your intervention. RSA uploads a core file only if it is not corrupted and the panic signature does not match any known panic message in the panic message database. In such a condition, the case is updated with the latest information.

RSA 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, RSA retries the core file collection. If unsuccessful, RSA terminates the retry and sends a failure alarm to RSE. When RSE receives the alarm, it notifies technical support that an automatic core upload failed. Technical support then requests from customer contacts to request a manual core upload.
- RSE fault or network outage

  In the event of a network fault or outage during a file transmission, RSA retries the file upload several times.

Notification of down storage controllers

When the remote management device detects that a storage controller is down (for example, due to an abnormal reboot) it automatically triggers an AutoSupport message to technical support. A problem case is created and the listed hardware contact is notified. AutoSupport must be enabled on all nodes in the cluster for this feature to work correctly.

How RSA uses AutoSupport

RSA uses AutoSupport to report problem diagnostics from the storage controller on your site to technical support.

AutoSupport is enabled by default on the storage system.

Technical support uses RSA to remotely trigger an AutoSupport request on the storage controller and have the AutoSupport data sent back to technical support.

When RSA 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.”

RSA uses the `system node autosupport` command parameters that are configured on the node.

For information about configuring and enabling AutoSupport, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

How RSA uses HTTP or HTTPS

You must ensure that HTTP or HTTPS is configured and enabled at your site so that RSA can communicate with the storage controller. Technical support uses RSA to initiate file access commands to collect needed files for problem diagnosis.

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

Remote data collection by technical support is limited to files within the `/mroot/etc/crash`, `/mroot/etc/log`, and`/mroot/etc/mib` directories and their subdirectories.

Using HTTP gives RSA fast access to the diagnostics data on the controller. Using HTTPS enables enhanced security on the data flow between RSA and the controller within your intranet. You should select the best transport option based on performance and security considerations.

Related tasks

Configuring your clustered storage system for RSA on page 13

How RSA provides data and network security

RSA involves six major security measures that enable you to have full control and visibility over all remote events and activities.

You can disable the connection to technical support and all RSA features by using the `rsa setup` command with the `policy -enable` option set to **`No`**.

Outbound connections only

Connection between RSA and RSE is always initiated by RSA. This ensures that there is only an outbound connection from your site to technical support.

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

The normal health check connection interval is every five minutes for storage controllers that are not being actively assisted by technical support in case triage. The connection interval changes to every 10 seconds if technical support 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.

Authenticated communications

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

Controlled access to diagnostic data

RSA connects to the 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.

RSA does not have access to your user data. The only directory trees that are accessible from the root volume of the storage system are `/mroot/etc/crash`, `/mroot/etc/log`, and `/mroot/etc/mib` directories and their subdirectories.

Securely stored diagnostic data

Data that is uploaded from RSA is stored in a highly secure Oracle database behind the NetApp corporate firewall. Access to this data is restricted to authorized technical support personnel. All actions taken by technical support using RSE are recorded and can be audited by accessing the RSE interface at your technical support site login.

Periodic security checks

Security assessments help to ensure that RSA conforms to industry best practices for protecting your data.

Security policies checked at startup

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

If the security policy does not allow communication with the RSE server, then RSA does not connect to RSE. RSA 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 RSA reports the new policy to RSE and stops any subsequent contact with RSE.

How the SP or the RLM provides data and network security

For your site's data and network security, the remote management device (which can be the SP or the RLM on your storage controller) uses a single outbound-only Ethernet connection, locally secured username and passwords, and a single port.

- A single Ethernet connection is the only external interface on the SP or the RLM.

The SP or the RLM firewall prevents incoming connections from outside your network. It allows connections only 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 `/mroot/etc/crash`, `/mroot/etc/log`, and`/mroot/etc/mib` directories, 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 RSA so that it can communicate with Data ONTAP. The SP or the 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 RSA usage.
- Only one port accepts connections.

  The only port on the SP or the RLM 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 RSA

You can find additional information about RSA, SP, RLM, and RSE in documents on the NetApp Support Site.

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

Configuring Remote Support Agent

You configure RSA to enable remote technical support. The RSA configuration process consists of verifying that the remote management device (the SP or the RLM) has the latest firmware and, if not, upgrading the device, configuring your storage system for RSA, and then configuring the RSA software on the remote management device.

RSA deployment requirements for cluster environments

Before you begin to configure RSA, you must ensure that it meets the requirements of your site's security policies for Internet access. You must also ensure that requirements for RSA and your storage system are met.

Ensure that all of the following conditions exist before configuring RSA.

RSA requirements

RSA requires the following:

- A remote management device (the SP or the RLM) on your storage systems.

  RSA is provided as a firmware upgrade to the RLM card. Firmware 3.0 or later is required; release 4.1 or later is recommended.

  RSA is included in the SP firmware on 32xx and 62xx systems and on FAS22xx and FAS80xx systems.
- A 128-bit, encrypted, outbound HTTPS connection to the Internet over port 443
- A 10/100 Mbps full-duplex Ethernet port with autonegotiation enabled
- Access to the target URL *https://remotesupportagent.netapp.com*
- Enabled AutoSupport

  AutoSupport is enabled by default. If it has been manually disabled, you must enable it.

Storage system requirements

Storage systems require the following for RSA:

- A configured SP or RLM

  The `sp setup` and `rlm setup` commands display the SP or the RLM configuration.
- Enabled AutoSupport on the storage systems

  AutoSupport is enabled by default. If it has been manually disabled, you must enable it.

- SP or RLM access to the Cluster Management LIF
  You might need to change your network settings to enable RSA to access your systems.
- Permission to configure Data ONTAP Service Processor Infrastructure (spi) web service
  - You must be an authorized cluster administrator who can log in to the administrative Storage Virtual Machine (SVM, formerly known as Vserver).
    The `security login show` command enables you to view the list of valid users.
  - If the firewall at your site prevents **`spi`** web access, or if **`spi`** web access has been manually disabled, you must be authorized to use the following commands to enable **`spi`**: `vserver services web`, `vserver services web access`, `security ssl`, `security certificate`, and `security login`.
- Enabled Web services
  The **`spi`** web service is enabled by default. If it has been manually disabled, you must enable **`spi`**.
  The `system services web node show` command enables you to view the settings and status of the web protocol engine at the node level.

Upgrading the SP or the RLM firmware

Before you configure RSA, you must verify whether the remote management device (the SP or the RLM) has the latest firmware and, if not, you must download it; then you must ensure that the SP or the RLM is configured.

Steps

1. Check to see if the current firmware is the latest available by using the Data ONTAP console or the CLI for the SP or the RLM.

   If the firmware is current, check the network configuration of the SP or the RLM as described in Step 3.

2. Download the latest SP or RLM firmware it is out of date.

   Note: Do not use a Data ONTAP Telnet or rsh session to upgrade firmware.

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

3. Check to see that the SP or the RLM is configured with an IP network configuration (IP address, mask, gateway address).

4. Configure the SP or the RLM for your storage controller and network if it is not already configured.

   For information and detailed instructions for configuring the SP or the RLM, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Upgrading or downgrading Data ONTAP to use the spi web service

To use the **`spi`** web service features on all cluster nodes, you must upgrade all nodes to Data ONTAP 8.1.1 or later.

About this task

When you upgrade or revert to Data ONTAP 8.1.1 or later, the nodes automatically switch the web service to the highest version that is available cluster-wide.

- To upgrade to Data ONTAP 8.1.1 or later from versions of Data ONTAP earlier than 8.1.0, you must reconfigure RSA by following the `rsa setup` procedures.
- To downgrade from Data ONTAP 8.1.1 or later to versions of Data ONTAP earlier than 8.1.0, you must disable RSA by using the RLM console.
- To upgrade to Data ONTAP 8.1.1 or later from version 8.1.0, you must reconfigure the new service.
  Follow the `rsa setup` procedures to complete the configuration and change the RSA IP address to the correct cluster management LIF.
- To downgrade from Data ONTAP 8.1.1 or later to version 8.1.0, you must reconfigure the RSA setup and change the IP address to the correct node management LIF.

Configuring your clustered storage system for RSA

Before you configure the RSA software, you must first configure your storage system to enable RSA to communicate with Data ONTAP. The RSA configuration must be the same on all nodes in the cluster.

Before you begin

AutoSupport data collection and **`spi`** web service are enabled by default on storage systems. If these have been manually disabled, you must enable them before configuring your storage system.

Administrator-level access is also enabled by default. If this is acceptable at your site, then you do not have to set up additional user accounts. However, if you want to create a more restrictive user account for RSA access, then you must configure a user account for the storage system to enable RSA to communicate with Data ONTAP.

About this task

For detailed information about configuring your storage system, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*.

Steps

1. Use the system node `system node autosupport` command to enable AutoSupport collection and delivery.

   You only need to enable AutoSupport if it has been manually disabled.

   #### Example

   The following example shows the commands and output for AutoSupport. The cluster name is **`clusterab`**; the nodes in the cluster are named **`node-01`** and **`node-02`**.

```
[STEP 1: GET COMMAND SYNTAX]

clusterab::> system node autosupport ?

  destinations>               The AutoSupport Destinations directory
  history>                    The AutoSupport History Directory
  invoke                      Generate and send an AutoSupport message
  manifest>                   The AutoSupport Manifest directory
  modify                      Modify AutoSupport configuration
  show                        Display AutoSupport configuration
  trigger>                    The AutoSupport Trigger directory


[STEP 1: SHOW THE AUTOSUPPORT DESTINATIONS DIRECTORY]

clusterab::> system node autosupport destinations show

Node Destinations
----------------------------------------------------------------------
node-01
     https://test.test.mycompany.com/put/AsupPut
     https://testbed.corp.mycompany.com/asupprod/post/1.0/postAsup
node-02
     https://test.test.mycompany.com/put/AsupPut
     https://test.test.mycompany.com/asupprod/post/1.0/postAsup
2 entries were displayed.

[STEP 1: SHOW THE AUTOSUPPORT CONFIGURATION]

clusterab::> system node autosupport show

Node                  State     From          To            Mail Hosts
--------------------- --------- ------------ ------------ ----------
node-01               enable    Postmaster    -             mailhost
node-02               enable    Postmaster    -             mailhost
2 entries were displayed.
```

2. Verify or configure the node HTTP access to technical support and, optionally, to Data ONTAP, by performing the following tasks:

   a. Verify that the node has HTTP enabled and configured by using the `system services web show` command.

   Example

   The following example shows the command and output for the system services web. The cluster name is **`clusterab`**; the nodes in the cluster are named **`node-01`** and **`node-02`**.

```
[STEP 2A: SHOW THE WEB PROTOCOLS CONFIGURATION]

clusterab::> system services web show

External Web Services: true
               Status: online
   HTTP Protocol Port: 80
  HTTPs Protocol Port: 443
         TLSv1 Enabled: true
         SSLv3 Enabled: true
         SSLv2 Enabled: false
```

   b. Verify that the firewall policy for the node LIF allows HTTP by using the `system services firewall policy` command.

If HTTP is not enabled, you can use the `system services web` command to configure it.

Example

The following example shows the commands and output for the firewall status. The cluster name is **`clusterab`**; the nodes in the cluster are named **`node-01`** and **`node-02`**.

```
[STEP 2B: SHOW FIREWALL STATUS]

clusterab::> system services firewall show

Node           Enabled Logging
-------------- ------- -------
node-01        true    false
node-02        true    false
2 entries were displayed.

[STEP 2B: SHOW FIREWALL STATUS FOR POLICIES]

clusterab::> system services firewall policy show -service http|https

Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
```

```
data
                 http       deny   0.0.0.0/0
                 https      deny   0.0.0.0/0
intercluster
                 http       deny   0.0.0.0/0
                 https      deny   0.0.0.0/0
mgmt
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
8 entries were displayed.

[STEP 2B: GET COMMAND SYNTAX]

clusterab::> system services firewall ?

  modify           Modify firewall status
  policy>          Manage firewall policy configuration
  show             Show firewall status
```

3. Perform the following tasks if RSA is using SSL to communicate with Data ONTAP:

   a. Verify or enable HTTPS on the Storage Virtual Machine (SVM, formerly known as Vserver) by using the `security ssl show` and `security ssl modify` commands.

      Use the `system services web` command to verify that configuration. Ensure that one of TLSv1, SSLv3, or SSLv2 is enabled.

      Example

      The following example shows the commands and output for the SSL configuration. The cluster name is **`clusterab`**; the nodes in the cluster are named **`node-01`** and **`node-02`**.

```
[STEP 3A: SHOW SSL CONFIGURATION]

clusterab::> security ssl show

Vserver        Enabled SSL Certificate Name
-------------- ------- ------------------------
node-01        true    node-01.cert
clusterab      true    clusterab.cert
node-02        true    node-02.cert
vs0            true    vs0.cert
4 entries were displayed.
```

   b. Verify that the firewall policy for the node LIF allows HTTPS by using the `system services firewall policy` command.

      Select port 80 for HTTP or port 443 for HTTPS.

   If you are not using HTTPS to access Data ONTAP, then the SSL-only values must be set to **`false`**.

Example

The following example shows the commands and output for the firewall status. The cluster name is **`clusterab`**; the nodes in the cluster are named **`node-01`** and **`node-02`**.

```
[STEP 3B: SHOW FIREWALL STATUS]

clusterab::> system services firewall show

Node           Enabled Logging
-------------- ------- -------
node-01        true    false
node-02        true    false
2 entries were displayed.

[STEP 3B: SHOW FIREWALL STATUS FOR POLICIES]

clusterab::> system services firewall policy show -service http|https

Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
data
                 http       deny   0.0.0.0/0
                 https      deny   0.0.0.0/0
intercluster
                 http       deny   0.0.0.0/0
                 https      deny   0.0.0.0/0
mgmt
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
8 entries were displayed.

[STEP 3B: GET COMMAND SYNTAX]

clusterab::> system services firewall ?

  modify          Modify firewall status
  policy>         Manage firewall policy configuration
  show            Show firewall status
```

4. Create a different user account for RSA access by using the `security login` command.

You only need to create a different account for RSA if you do not want RSA to have administrator-level access.

You must create the user account on the cluster Storage Virtual Machine (SVM), and it must have access to the `vserver options` command. The RSA account configuration must be the same on all nodes in the cluster.

If administrator-level access for RSA is acceptable, then authorize the role for RSA access, as explained in Step 5.

Example

The following example shows the commands and output for creating a user account to access HTTP and ONTAPI. The role name is **`rsa`**; the user name is **`rsauser`**.

```
[STEP 4: GET COMMAND SYNTAX]

clusterab::> security login role create ?

  [ -vserver <vserver name> ]  Vserver (default: clusterab)
   [-role] <text>              Role Name
   [-cmddirname] <text>        Command / Directory
  [[-access] <Access>]         Access Level (default: all)
  [ -query <query> ]           Query (default: "")

[STEP 4: CREATE ROLE "rsa" ON THE DIRECTORY NAMED "DEFAULT"]

clusterab::> security login role create -vserver clusterab -role rsa -
cmddirname DEFAULT

[STEP 4: SHOW THE ROLE CONFIGURATION]

clusterab::> security login role show -vs clusterab

           Role          Command/                       Access
Vserver    Name          Directory                Query Level
---------- ------------- --------- -------------------- --------
clusterab  admin         DEFAULT                        all
clusterab  rsa           DEFAULT                        all
clusterab  none          DEFAULT                        none
clusterab  readonly      DEFAULT                        readonly
clusterab  readonly      security                       none
clusterab  readonly      security login password        all
clusterab  readonly      set                            all
7 entries were displayed.

[STEP 4: SHOW ACCESS. THE NEW "rsa" ROLE DOES NOT SHOW BECAUSE NO
USER ACCOUNT HAS BEEN CREATED.]

clusterab::> security login show

Vserver: clusterab
                             Authentication                Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
admin            console     password       admin            no
                 http        password       admin            no
                 ontapi      password       admin            no
                 service-processor
                             password       admin            no
                 ssh         password       admin            no
public           snmp        community      readonly         -
Vserver: vs0
                             Authentication                Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
```

```
vsadmin          http        password      vsadmin          yes
                 ontapi      password      vsadmin          yes
                 ssh         password      vsadmin          yes
9 entries were displayed.

[STEP 4: GET COMMAND SYNTAX]

clusterab::> security login create ?

  [ -vserver <vserver name> ]  Vserver (default: clusterab)
   [-username] <text>          User Name
   [-application] <text>       Application
   [-authmethod] <text>        Authentication Method
  [[-role] <text>]             Role Name (default: admin)
  [[-comment] <text>]          Comment(more than one word, within
quotes)

[STEP 4: CREATE A USER ACCOUNT "rsauser" FOR HTTP ON THE CLUSTER
VSERVER]

clusterab::> security login create -vserver clusterab -username
rsauser
-application http -authmethod password -role rsa

Please enter a password for user 'rsauser':  [THIS PASSWORD IS THE
AGENT ADMINISTRATOR USER PASSWORD]
Please enter it again:

[STEP 4: CREATE A USER ACCOUNT "rsauser" FOR ONTAPI ON THE CLUSTER
VSERVER]
[PASSWORD IS NOT PROMPTED BECAUSE YOU ENTERED ONE IN THE PREVIOUS
COMMAND]

clusterab::> security login create -vserver clusterab -username
rsauser
-application ontapi -authmethod password -role rsa

[STEP 4: SHOW USER ACCOUNTS]

clusterab::> security login show


Vserver: clusterab
                             Authentication                   Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
admin            console     password       admin            no
                 http        password       admin            no
                 ontapi      password       admin            no
                 service-processor
                             password       admin            no
                 ssh         password       admin            no
public           snmp        community      readonly         -
rsauser          http        password       rsa              no
                 ontapi      password       rsa              no
Vserver: vs0
                             Authentication                   Acct
```

```
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
vsadmin          http        password       vsadmin          yes
                 ontapi      password       vsadmin          yes
                 ssh         password       vsadmin          yes
11 entries were displayed.
```

5. Authorize any account that you create so that RSA can access the **`spi`** web service on the cluster, a node, or a Storage Virtual Machine (SVM) by using the `vserver services web access` command.

Example

For example, you might use a command like the following:

```
vserver services web access create -vserver cluster-admin-vserver-name -
name spi -role role-name.
```

Example

```
STEP 5: SHOW WEB SERVICES CONFIGURATION]

clusterab::> vserver services web show -name spi|ontapi|compat
                    Service
Vserver    Type     Name     Description                  Enabled
---------- -------- -------- ---------------------------- -------
node-01    node     compat   Data ONTAP Classic Services  true
node-01    node     ontapi   Remote Administrative API    true
                                Support
node-01    node     spi      Service Processor            false
                                Infrastructure
clusterab  admin    ontapi   Remote Administrative API    true
                                Support
clusterab  admin    spi      Service Processor            false
                                Infrastructure
node-02    node     compat   Data ONTAP Classic Services  true
node-02    node     ontapi   Remote Administrative API    true
                                Support
node-02    node     spi      Service Processor            false
                                Infrastructure
vs0        cluster  ontapi   Remote Administrative API    true
                                Support
9 entries were displayed.

[STEP 5: GET COMMAND SYNTAX]

clusterab::> vserver services web modify -name spi|ontapi|compat ?

    -vserver <text>           Vserver
  [ -enabled {true|false} ]   Enabled
  [ -ssl-only {true|false} ]  SSL Only

[STEP 5: ENABLE WEB SERVICES FOR spi, ontapi, AND compat]
[USE A WILDCARD FOR THE VSERVER TO CONFIGURE ALL NODES]
```

```
clusterab::> vserver services web modify -name spi|ontapi|compat -
vserver * -enabled true

[STEP 5: SHOW WEB SERVICES CONFIGURATION]

clusterab::> vserver services web show -name spi|ontapi|
compat
                    Service
Vserver    Type     Name     Description                 Enabled
---------- -------- -------- --------------------------- -------
node-01    node     compat   Data ONTAP Classic Services  true
node-01    node     ontapi   Remote Administrative API    true
                                Support
node-01    node     spi      Service Processor            true
                                Infrastructure
clusterab  admin    ontapi   Remote Administrative API    true
                                Support
clusterab  admin    spi      Service Processor            true
                                Infrastructure
node-02    node     compat   Data ONTAP Classic Services  true
node-02    node     ontapi   Remote Administrative API    true
                                Support
node-02    node     spi      Service Processor            true
                                Infrastructure
vs0        cluster  ontapi   Remote Administrative API    true
                                Support
9 entries were displayed.
```

6. Enable **`spi`** on the cluster by using the `vserver services web access create` command.

   You only need to enable **`spi`** if it has been manually disabled.

   The spi web service must be enabled on the cluster management LIF and all node Storage Virtual Machines (SVMs).

   Enabling the **`spi`** web service also enables the **`ontapi`** and **`compat`** web services.

   Use a wildcard for the SVM name to configure all the nodes on the cluster.

   Example

   For example, you might use a command like the following:

   `vserver services web modify -vserver` ***`cluster-admin-vserver-name`*** **`-name spi -enabled true`**

```
[STEP 6: SHOW ROLES CURRENTLY AUTHORIZED FOR ACCESS]

clusterab::> vserver services web access show -name spi|ontapi|compat

Vserver        Type     Service Name     Role
-------------- -------- ---------------- ----------------
clusterab      admin    compat           none
clusterab      admin    ontapi           admin
clusterab      admin    ontapi           guest
clusterab      admin    ontapi          readonly
clusterab      admin    ontapi          none
clusterab      admin    spi             admin
vs0            cluster  ontapi          vsadmin
vs0            cluster  ontapi          vsadmin-protocol
vs0            cluster  ontapi          vsadmin-readonly
vs0            cluster  ontapi          vsadmin-volume
10 entries were displayed.

[STEP 6: IF YOU ARE CREATING A CUSTOM 'rsa' ROLE FOR ACCESS,
AUTHORIZE THE ROLE FOR EACH WEB SERVICE]

clusterab::> vserver services web access create  -name spi -role rsa -
vserver clusterab
clusterab::> vserver services web access create  -name ontapi -role
rsa -vserver clusterab
clusterab::> vserver services web access create  -name compat -role
rsa -vserver clusterab

[STEP 6: SHOW ROLES AUTHORIZED FOR ACCESS]

clusterab::> vserver services web access show -name spi|ontapi|
compat

Vserver        Type     Service Name     Role
-------------- -------- ---------------- ----------------
clusterab      admin    compat           rsa
clusterab      admin    ontapi           admin
clusterab      admin    ontapi           guest
clusterab      admin    ontapi           readonly
clusterab      admin    ontapi           rsa
clusterab      admin    spi              rsa
vs0            cluster  ontapi           vsadmin
vs0            cluster  ontapi           vsadmin-protocol
vs0            cluster  ontapi           vsadmin-readonly
vs0            cluster  ontapi
```

7. Obtain the IP address (or name) of the cluster management LIF needed for RSA setup by using the `network interface show -role cluster-mgmt` command. This command also lets you test the node management and the cluster management configuration.

Example

The following example shows the commands and output for obtaining information that you will need for RSA setup and also for testing teh node and cluster management configurations.

```

[TEST THE NODE-MANAGEMENT LIF TO VERIFY THAT THE CONFIGURATION WORKS]
[TEST STEP 1: DETERMINE THE CORRECT IP ADDRESS THAT RSA USES]

clusterab::> network interface show -role node-mgmt

         Logical    Status     Network          Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask     Node     Port    Home
```

```
-------- ---------- ---------- ------------  -------- ------- ----
node-a   node_mgmt  up/up    11.22.333.444/20 node-02  e0a     false

[TEST STEP 2: USE THE IP ADDRESS IN A WEB BROWSER]
[THE TEST IS SUCCESSFUL IF A TABLE IS DISPLAYED]

http:// 11.22.333.4444/na_admin/logs/
```

```


[TEST THE CLUSTER MANAGEMENT LIF TO VERIFY THAT THE CONFIGURATION
WORKS]
[TEST STEP 1: DETERMINE THE CORRECT IP ADDRESS THAT RSA USES]

clusterab::> network interface show -role cluster-mgmt

          Logical      Status     Network
Vserver  Interface     Admin/Oper Address/Mask
-------- ----------    ---------- -------------
clusterab cluster_mgmt up/up      11.22.333.444/20

          Current  Current Is
          Node     Port    Home
          -------- ------- ----
          node-02  e0a     false

[TEST STEP 2: USE THE IP ADDRESS IN A WEB BROWSER]
[THE TEST IS SUCCESSFUL IF A TABLE IS DISPLAYED]

http:// 11.22.333.4444/spi/
```

8. Run the RSA setup wizard by using the `rsa setup` command.

Related references

rsa setup on page 30

Configuring RSA software for cluster environments

To complete RSA configuration, you must set up RSA on the remote management device.

Before you begin

Before configuring RSA software, ensure that the remote management device (the SP or the RLM) is set up and, if necessary, upgraded. You must have the following information available for RSA configuration:

- Network information (the proxy configuration, if required to access the Internet)
    - Proxy IP address

  - Proxy type (SOCKS/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. Connect to the SP or RLM with your SSH client by entering the applicable command:

   ```
   %> ssh admin@sp-IP
   %> ssh newly-created-account@sp-IP
   ```

2. Use the SP or RLM `version` command to verify that the service processor is using the latest firmware.
3. Start an interactive configuration session by using the `rsa setup` command.
4. When prompted to test the configuration, type `Yes`.
5. Enter the needed information during the interactive session when prompted.

Example

The following example shows the `rsa setup` command when no proxy support is needed:

```
SP f2220-142-53*> 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 cluster management IP address of your storage cluster
[10.238.142.53]: 10.238.142.53
Do you want to use HTTP with SSL? [no]:
Enter HTTPS port number [443]:
Enter HTTP username [admin]:
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 cluster management LIF HTTP connection .....................
ok
```

```
Testing Remote Support Enterprise connection .......................
ok
```

Example

The following example shows 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.
```

6. Verify that the configuration is correct after the session is complete by using the `rsa show` command.

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

Example

The following example shows the `rsa show` command when no proxies are configured:

```
SP f2220-142-53*> rsa show
Remote Support Agent is enabled.

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

Use proxy: no

Cluster management LIF: 10.238.142.53 can be some hostname
HTTP with SSL enabled: yes
```

```
Storage controller HTTP port: 443
Storage controller HTTP username: admin
```

Example

The following example shows 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
```

7. View the status of RSA 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

The following example shows 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
```

8. 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.

Related references

rsa setup on page 30

Managing and monitoring Remote Support Agent

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

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

Disabling and enabling RSA

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

About this task

When you disable RSA, 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

The following example of the `rsa setup` command shows how to disable RSA:

```
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 RSA

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

rsa help

You use the `rsa help` command to display the syntax and description of RSA commands.

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

You use the `rsa setup` command to configure RSA.

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 RSA:

- Proxy parameters
- RSE URL options
- Policies to disable or enable RSA
- 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 RSE 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 RSA. 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 the SP or RLM uses to establish a connection with RSE.

`-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 RSE URL.

`-enable`

Enables or disables proxy support and RSA.

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

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

```
SP|RLM 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 shows the command to change the communication parameters; because no HTTP options are specified in the command line, the command starts an interactive session:

```
SP|RLM 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 shows the command to change the proxy parameters:

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

Example: Changing the RSE URL interactively

The following example shows the command to change the URL of RSE; because no RSE options are specified in the command line, the command starts an interactive session:

```
SP|RLM> 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

You use the `rsa show` command to display 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 RSE URL.

[`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 shows the command to display the configuration of all the remote support parameters:

```
SP|RLM> 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 shows the command to display the configuration of all the remote support parameters:

```
SP|RLM> 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 shows the command to display the configuration of all the remote support parameters in a system that does not have proxies enabled:

```
SP|RLM> 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

You use the `rsa status` command to display 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 shows the command to display the status of all the remote support parameters; you can view and print the status report:

```
SP|RLM> 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
```

rsa test

You use the `rsa test` command to test the remote support HTTP and proxy or the 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 RSE.

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

The following example shows the command to display the results of successful tests on all the remote support connections.

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

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

The following example shows the command to display the results of successful tests on all the remote support connections.

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

Example: Testing a connection for which RSA is not enabled

The following example shows the command to display the results of a test on a storage controller that has RSA disabled.

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

Example: Testing a connection that has problems

The following example shows the command to display the results of a test that failed because of an unresponsive server or incorrect hostname configuration.

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

Accessing the Remote Support Enterprise UI

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

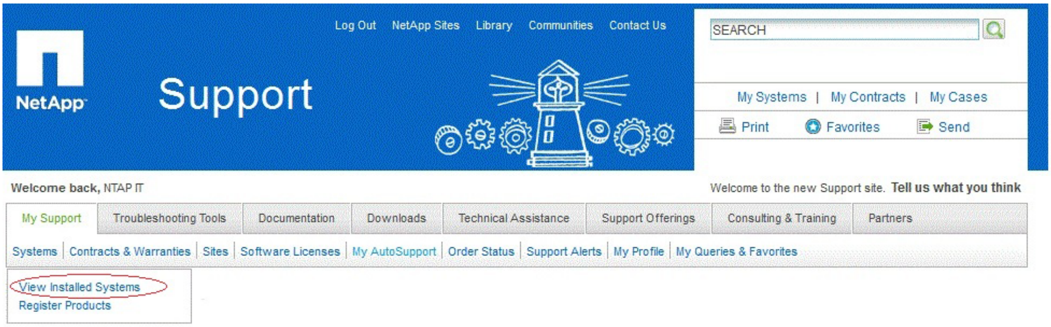
Before you begin

Access to initiate requests to RSA is restricted to 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 RSE UI on the NetApp Support Site.

Steps

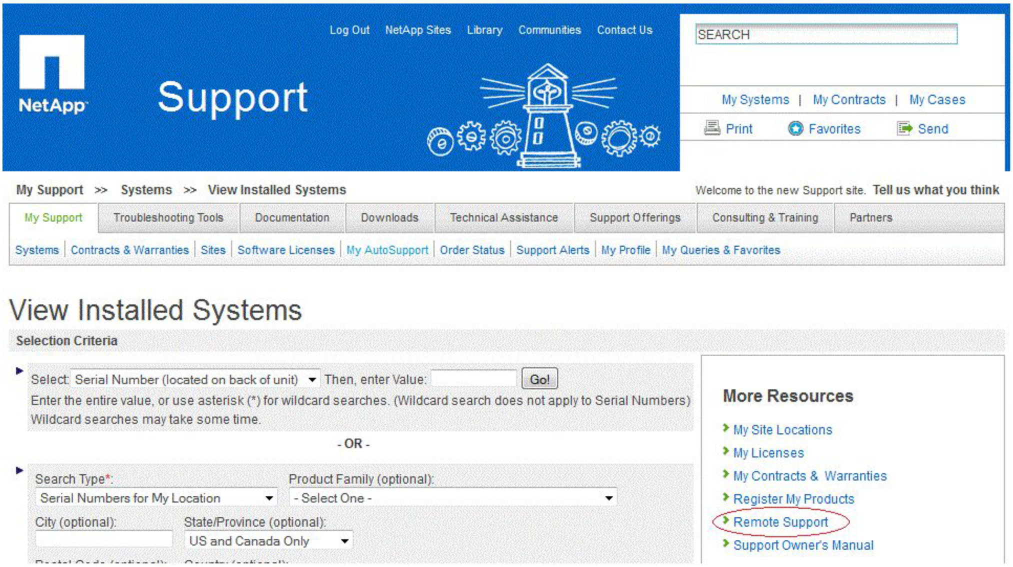
1. Go to support.netapp.com and log in to your NetApp account.
2. On the **Support** page, click **My Support** and select **Systems > View Installed Systems**:

Example



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

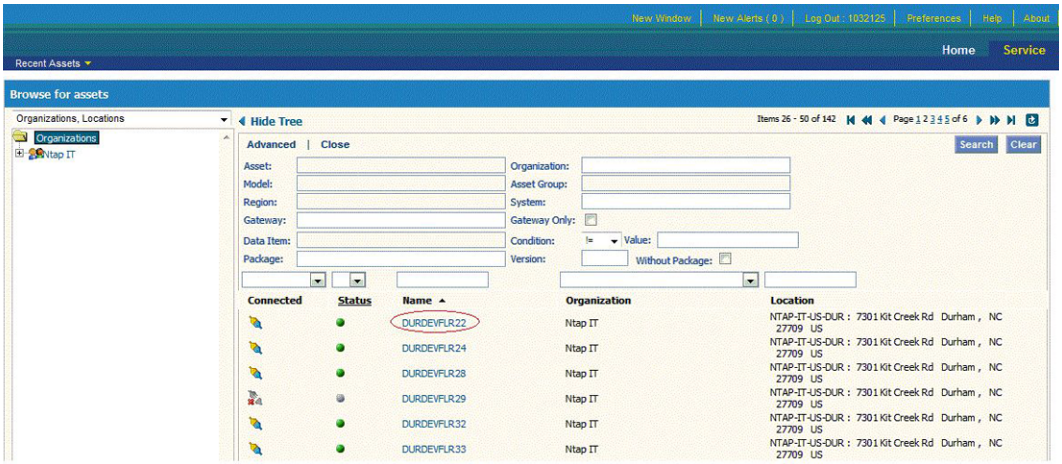
Example


Log Out
NetApp Sites
Library
Communities
Contact Us
SEARCH
NetApp
Support
My Systems | My Contracts | My Cases
Print
Favorites
Send
My Support >> Systems >> View Installed Systems
Welcome to the new Support site. Tell us what you think
My Support
Troubleshooting Tools
Documentation
Downloads
Technical Assistance
Support Offerings
Consulting & Training
Partners
Systems | Contracts & Warranties | Sites | Software Licenses | My AutoSupport | Order Status | Support Alerts | My Profile | My Queries & Favorites
View Installed Systems
Selection Criteria
Select: Serial Number (located on back of unit)
Then, enter Value:
Go!
- OR -
Search Type*:
Serial Numbers for My Location
Product Family (optional):
- Select One -
City (optional):
State/Province (optional):
US and Canada Only
More Resources
My Site Locations
My Licenses
My Contracts & Warranties
Register My Products
Remote Support
Support Owner's Manual

Enter the entire value, or use asterisk (*) for wildcard searches. (Wildcard search does not apply to Serial Numbers) Wildcard searches may take some time.

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

Example



Connected	Status	Name ▲	Organization	Location
	●	DURDEVFLR22	Ntap IT	NTAP-IT-US-DUR : 7301 Kit Creek Rd Durham , NC 27709 US
	●	DURDEVFLR24	Ntap IT	NTAP-IT-US-DUR : 7301 Kit Creek Rd Durham , NC 27709 US
	●	DURDEVFLR28	Ntap IT	NTAP-IT-US-DUR : 7301 Kit Creek Rd Durham , NC 27709 US
	●	DURDEVFLR29	Ntap IT	NTAP-IT-US-DUR : 7301 Kit Creek Rd Durham , NC 27709 US
	●	DURDEVFLR32	Ntap IT	NTAP-IT-US-DUR : 7301 Kit Creek Rd Durham , NC 27709 US
	●	DURDEVFLR33	Ntap IT	NTAP-IT-US-DUR : 7301 Kit Creek Rd Durham , NC 27709 US

Related references

RSE service page descriptions on page 39

RSE service page descriptions

Using the NetApp Support site, you can access the RSE UI to view all devices registered with the RSE, examine remote actions performed on them, obtain the status information for devices monitored by RSA, 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 RSA.

RSE Device Page

Displays a detailed read-only view of the status of your NetApp device, as well as the status of RSA.

NetApp Controller Summary Panel

Displays a summary of the storage controller status and configuration.

RSA Configuration Summary Panel

Displays a summary of RSA 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 *mysupport.netapp.com*.

Remote support error messages

You can find solutions to remote support error messages by searching product documentation for error message strings, or by the symptom you are experiencing. Follow the instructions in the corrective action provided.

Cannot connect to host

Message

`Cannot connect to host`

Description

This message occurs when RSA 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 503 - resource unavailable

Message

`HTTP 503 - resource unavailable`

Description

This message occurs when the na_admin page on the storage controller is not available.

Corrective action

Ensure that the option `httpd.admin.access` is set to one of the following values:

- The host name or IP address of the RLM
- **`*`** (asterisk)
- **`legacy`**

If the option `httpd.admin.access` is set to **`legacy`**, then ensure that the option `trusted.hosts` is set to one of the following values:

- The host name or IP address of the SP or RLM
- **`*`** (asterisk)

If you are using SSL, then ensure that SSL is set up on the storage controller and the option `httpd.admin.ssl.enable` is set to `on`.

To test **`spi`** web service access directly from a web browser, try to access the following URL:

`https://<your Clust-Mgmt-Lif>/spi`

For information about managing access to web services, see the *Clustered Data ONTAP System Administration Guide for Cluster Administrators*

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 RSA account 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. RSA 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 RSA.

option httpd.admin.enable not set to on

Message

`option httpd.admin.enable not set to on`

Description

This message occurs when the **`spi`** and **`compat`** web services are not enabled on the node.

Corrective action

No corrective action is needed. RSA recovers automatically in a few minutes.

option httpd.autoindex.enable

Message

`option httpd.autoindex.enable not set to on`

Description

This message occurs when the web services system experiences a failure. The node might not be healthy.

Corrective action

Contact technical support.

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 RSA.

RSE health check interface busy

Message

```
RSE health check interface busy
```

Description

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

- RSE is not responding, returns an incorrect status, or has an invalid URL.
- RSA is processing a file upload.

Corrective action

No corrective action is needed. RSA 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.

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

RSE did not receive the correct information from RSA.

Corrective action

Contact *mysupport.netapp.com*.

Incorrect information in RSA Configuration Summary

The information in the RSA Configuration Summary is not correct.

Cause

RSE did not receive the correct information from RSA.

Corrective action

Contact *mysupport.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 *mysupport.netapp.com* to correct the storage controller information.

Unable to log in to *mysupport.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 *mysupport.netapp.com*, you receive a message indicating that the username or password is not valid.

Cause

You do not have a *mysupport.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 **Register Now** instructions at *mysupport.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