How to Implement Secure, Unattended Logging in ROS

RUGGEDCOM ROS v4.3 and Higher
RUGGEDCOM ROS v4.2.2.F and Higher

https://support.industry.siemens.com/cs/ww/en/view/109756843

Siemens Industry Online Support

This entry is from the Siemens Industry Online Support. The general terms of use (http://www.siemens.com/terms_of_use) apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement—and continuously maintain—a holistic, state-of-the-art, industrial security concept. Siemens's products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens's guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit http://www.siemens.com/industrialsecurity.

Siemens's products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under http://www.siemens.com/industrialsecurity.

Table of Contents

1 Introduction

The **logs** command, which is available at the RUGGEDCOM ROS Command Line Interface (CLI), displays all log entries to the console as they occur. For security reasons, the **logs** command should only be used when connected to the RUGGEDCOM ROS server via a secure shell (SSH) connection. When **logs** is invoked, RUGGEDCOM ROS will continue to send log entries to the console until the SSH connection is terminated or <Ctrl+C> is entered.

This document describes a shell script that implements secure, unattended logging from RUGGEDCOM ROS v4.3 and ROS v4.2.2.F (or higher). The script uses **AutoSSH**, a simple, open-source tool available in most operating systems, including Linux, Windows (under Cygwin), and Mac OS X.

When the script is executed, AutoSSH will (1) invoke the **logs** command and (2) send periodic requests to the remote server, instructing it to maintain a persistent SSH connection. If RUGGEDCOM ROS fails to respond to a certain number of these requests, AutoSSH automatically reconfigures the SSH connection and re-invokes the **logs** command.

NOTE AutoSSH includes built-in monitoring mechanisms. However, because RUGGEDCOM ROS uses neither SSH port forwarding nor the TCP “echo” service, the script suppresses these monitoring mechanisms.

2 Preliminary Steps

Prior to running the shell script, do the following:

1. Make sure RUGGEDCOM ROS v4.3 and ROS v4.2.2.F (or higher) is running on the device. For instructions on how to upgrade firmware, refer to the relevant RUGGEDCOM ROS User Guide.
2. Install AutoSSH on the PC that will be used to execute the script. In most operating systems, AutoSSH can be installed via the default software installation facility. Otherwise, it can be downloaded from the following URL: `http://www.harding.motd.ca/autossh`.
3. Enable SSH on the device. For instructions, refer to the relevant RUGGEDCOM ROS User Guide.
4. Make sure a valid host key pair has been provisioned in the *ssh.keys* file on the device. For instructions on how to manage SSH keys, refer to the relevant RUGGEDCOM ROS User Guide.
5. Make sure a valid public SSH key has been provisioned in the *sshpub.keys* file on the device. The public SSH key corresponds with the remote PC on which AutoSSH is initiated. For instructions on how to manage SSH keys, refer to the relevant RUGGEDCOM ROS User Guide.

NOTE For the shell script to establish an SSH connection without administrator intervention, the private SSH key must not be encrypted with a passphrase.

3 Script Template

The template of the shell script is as follows:

```
USER=username
KEY=id_rsa_keyless
TOE=ros.internal.net
autossh -M0 \
   -i ${KEY} \
   -o "ServerAliveInterval seconds" \
   -o "ServerAliveCountMax attempts" \
   ${USER}@${TOE} logs | \
   tee syslog-${TOE}-`date -Iminutes`.txt
```

4 Running the Script

To run the shell script, do the following:

1. Create a new script file based on the script template.
2. Customize the script template as follows:
   i. Replace **username** with the name of the RUGGEDCOM ROS user account that will be used to sign in to the device.
   ii. Replace **id_rsa_keyless** with the path and filename of the new private key created for this connection.
   iii. Replace **ros.internal.net** with the DNS name or IP address of the RUGGEDCOM ROS device to be monitored.
   iv. Replace **seconds** with the total number of seconds between successive transmissions of the *keep alive* message. A value of *20* is recommended.

NOTE The key exchange process may take up to 60 seconds, during which time RUGGEDCOM ROS device may be unresponsive. To allow for such exchanges, the SSH connection should never time out before 60 s. For instance, if **`seconds`** is set to *20,* **`attempts`** should be no less than *4* in order to allow for enough time for the link to re-key.

   v. Replace **attempts** with the maximum number of times the RUGGEDCOM ROS server may not respond to the “keep alive” message before the SSH connection times out. A value of *4* is recommended.
3. Execute the shell script in the console.

NOTE If the **`logs`** command is already running on the device, the script will return the following error message: `Command is already active.` To resolve this error, enter <Ctrl+C> to kill the active **`logs`** command and execute the script again.

5 Customer Support

Siemens Customer Support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, please contact Siemens Customer Support through any one of the following methods:

- **Online**

  Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

- **Telephone**

  Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

- **Mobile App**

  Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

  - Access Siemens's extensive library of support documentation, including FAQs, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community via the forum

6 History

Version	Date	Modifications
1	02/2019	Initial release.