Red Hat Insights 2023

Deploying Red Hat Insights on existing RHEL systems managed by Red Hat Update Infrastructure
Deploying Red Hat Insights on existing RHEL systems managed by Red Hat Update Infrastructure
Abstract

The following guidance is for users who wish to deploy Red Hat Insights for Red Hat Enterprise Linux on a provisioned Red Hat Enterprise Linux (RHEL) system managed by Red Hat Update Infrastructure (RHUI). Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.
# Table of Contents

CHAPTER 1. DEPLOYING RED HAT INSIGHTS ON SYSTEMS REGISTERED WITH RED HAT UPDATE INFRASTRUCTURE ................................................................. 3

1.1. INSTALLING THE INSIGHTS CLIENT ............................................. 3

1.2. BASIC AUTHENTICATION OVERVIEW ...................................... 3

   1.2.1. When to use basic authentication ........................................ 3

   1.2.1.1. How to know if you must configure basic authentication .... 4

   1.2.2. Configuration requirements for basic authentication .......... 4

   1.2.3. Configuring basic authentication ....................................... 5

1.3. REGISTERING THE SYSTEM TO RED HAT INSIGHTS .................. 5

1.4. VIEWING YOUR INSIGHTS RESULTS ........................................ 6

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION .......................... 7
CHAPTER 1. DEPLOYING RED HAT INSIGHTS ON SYSTEMS REGISTERED WITH RED HAT UPDATE INFRASTRUCTURE

This guide is for users who wish to deploy Red Hat Insights on an existing, cloud marketplace-purchased Red Hat Enterprise Linux system managed by Red Hat Update Infrastructure (RHUI).

To start using Insights, you must perform the following actions on each system you want to monitor and assess:

- Install the Insights client if it did not come preinstalled.
- Configure the client to use basic authentication.
- Register the system to Insights for Red Hat Enterprise Linux.

1.1. INSTALLING THE INSIGHTS CLIENT

**NOTE**

The Insights client installation procedure is not required on Red Hat Enterprise Linux 8 (RHEL8) systems.

Install the client package on each system.

**Procedure**

1. Enter the following command to install the current version of the Insights client package:

```
[root@server ~]# yum install insights-client
```

1.2. BASIC AUTHENTICATION OVERVIEW

Red Hat Insights can use two types of authentication to validate system access to the Insights for Red Hat Enterprise Linux services. The default authentication method is through certificates. Certificates are generated when you register a system with Red Hat Subscription Manager (RHSM) or when your system is managed by Red Hat Network Satellite system management.

An alternative authentication method is through SSO credentials. A valid Red Hat SSO credential is created when you have a valid Red Hat Customer Portal user name. In order to use SSO credentials with Red Hat Insights for Red Hat Enterprise Linux, you must configure your system to use basic authentication.

1.2.1. When to use basic authentication

You must use basic authentication in any of the following situations:

- Your RHEL system is not registered with Red Hat Subscription Manager (RHSM).
- Your Red Hat Enterprise Linux (RHEL) system is not managed by Red Hat Network Satellite services.
- Your RHEL system is provisioned through a Red Hat Certified Cloud and Service Provider and is updated by Red Hat Update Infrastructure (RHUI).
Your RHEL system is from a cloud marketplace provider and not obtained through Red Hat Cloud Access program.

**NOTE**

If you have valid RHEL subscriptions for your system, you can switch between the default certificate-based authentication for Insights for Red Hat Enterprise Linux and the basic authentication for Insights for Red Hat Enterprise Linux. If you are configuring basic authentication on a new RHEL system, you must complete the basic authentication procedures before you can register the Insights for Red Hat Enterprise Linux client application.

### 1.2.1.1. How to know if you must configure basic authentication

The following messages might appear when you attempt to register a system that does not have a Red Hat authentication certificate. If you see **=== End Upload URL Connection Test: FAILURE ===**, configure your system for basic authentication.

```bash
insights-client --register
Running connection test...
Connection test config:
=== Begin Certificate Chain Test ===
depth=1
verify error:num=0
verify return:1
depth=0
verify error:num=0
verify return:1
=== End Certificate Chain Test: SUCCESS ===

=== Begin Upload URL Connection Test ===
HTTP Status Code: 401
HTTP Status Text: Unauthorized
HTTP Response Text: Connection failed
=== End Upload URL Connection Test: FAILURE ===

=== Begin API URL Connection Test ===
HTTP Status Code: 200
HTTP Status Text: OK
HTTP Response Text: lub-dub
Successfully connected to: https://cert-api.access.redhat.com/r/insights/
=== End API URL Connection Test: SUCCESS ===
```

Connectivity tests completed with some errors
See /var/log/insights-client/insights-client.log for more details.

### 1.2.2. Configuration requirements for basic authentication

When you configure your system to use single sign-on (SSO) credentials for basic authentication instead of the default certificate-based authentication for Red Hat Insights, you provide Red Hat SSO credentials. SSO credentials are a valid Red Hat Customer Portal user name and password.

To configure basic authentication, a plain-text username and password is stored in the configuration file. As a best practice, create a Red Hat Customer Portal account with SSO credentials that are used only
for Red Hat Insights for Red Hat Enterprise Linux basic authentication. This action avoids exposing the SSO credentials of individual users.

1.2.3. Configuring basic authentication

Insights client configuration is managed in `/etc/insights-client/insights-client.conf`. This file provides a configuration template for setting up basic authentication.

The default configuration for certificate-based authentication is as follows:

```
auto_config=TRUE
authmethod=BASIC
username=<your customer portal username>
password=<your customer portal password>
```

Prerequisites

- You have a Red Hat SSO username and SSO password that can be stored in clear text.
- You have read/write permissions in the directory `/etc/insights-client/`.
- The `insights-client` package is installed on your system.

Procedure

1. Use a text editor to open the file `/etc/insights-client/insights-client.conf`
2. Change `auto_config=TRUE` value to `auto_config=FALSE`.
3. Replace `<your customer portal username>` with a Red Hat SSO username.
4. Replace `<your customer portal password>` with a Red Hat SSO password.
5. Save the configuration and exit the editor.
6. Register the system.
   ```
   # insights-client --register
   ```

1.3. REGISTERING THE SYSTEM TO RED HAT INSIGHTS

Register the system to communicate with the Red Hat Insights and to view results displayed in the Red Hat Hybrid Cloud Console.

Prerequisites

- Root access to the system

Procedure

1. Enter the following command to register the system.
   ```
   [root@server ~]# insights-client --register
   ```
1.4. VIEWING YOUR INSIGHTS RESULTS

System and infrastructure results can be viewed in the Red Hat Insights for Red Hat Enterprise Linux application dashboard.

The dashboard provides links to each available Insights service. This includes advisor, drift, vulnerability, compliance, policies and patch. From this starting point, you can proactively identify and manage issues affecting system security, performance, stability and availability.

Prerequisites

- The **insights-client** package is installed on the system.
- You are logged in to the Red Hat Hybrid Cloud Console.

Procedure

1. Navigate to Red Hat Insights > RHEL > Inventory in the Hybrid Cloud Console.
2. Search for your system name and confirm that it exists in the inventory.
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We both appreciate and prioritize your feedback on our documentation. Provide as much detail as possible, so that your request might be quickly addressed.

Prerequisites

- You are logged in to the Red Hat Customer Portal.

Procedure

To provide your feedback, perform the following steps:

1. Click the following link: Create Issue

2. Describe the issue or enhancement in the Summary text box.

3. Provide more details about the issue or enhancement in the Description text box.

4. Type your name in the Reporter text box.

5. Click the Create button.

A documentation issue has been created and will be routed to the appropriate documentation team. Thank you for taking the time to provide feedback.