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 on a provisioned Red Hat Enterprise Linux (RHEL) system managed by Red Hat Update Infrastructure (RHUI). Providing Feedback: If you have a suggestion to improve this documentation, or find an error, submit a Bugzilla report at http://bugzilla.redhat.com. Select the Cloud Software Services (cloud.redhat.com) product and use the Documentation component.
# Table of Contents

1. RED HAT INSIGHTS DEPLOYMENT ON CLOUD MARKETPLACE RHEL MANAGED BY RHUI  

## CHAPTER 1. INSTALLING THE INSIGHTS-CLIENT AND REGISTERING A SYSTEM  

1.1. Red Hat Insights deployment overview  
   1.1.1. Installing the client package  
   1.1.2. Basic authentication overview  
      1.1.2.1. When to use basic authentication  
      1.1.2.2. Configuration requirements for basic authentication  
      1.1.2.3. How to know if you must configure basic authentication  
   1.1.3. Configuring basic authentication  
   1.1.4. Registering the system to Red Hat Insights  
   1.1.5. Viewing your results
1. RED HAT INSIGHTS DEPLOYMENT ON CLOUD MARKETPLACE RHEL MANAGED BY RHUI

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

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

- Install the client.

**NOTE**

Red Hat Enterprise Linux 8 (RHEL 8) ships with Red Hat Insights preinstalled, so the Insights client installation procedure is not required on RHEL 8 systems. All RHEL systems, no matter which version, must be registered with the Red Hat Insights service.

- Configure the client to use basic authentication.

- Register the system to Insights.

### 1.1.1. Installing the client package

**NOTE**

The insights-client installation procedure is not required on Red Hat Enterprise Linux 8 (RHEL 8) systems.

Install the client package on each system.

Procedure

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

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

### 1.1.2. Basic authentication overview

Red Hat Insights can use two types of authentication to validate system access to the Insights 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, you must configure your system to use basic authentication.

#### 1.1.2.1. 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 and the basic authentication for Insights. If you are configuring basic authentication on a new RHEL system, you must complete the basic authentication procedures before you can register the Insights client application.

### 1.1.2.2. 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 basic authentication. This action avoids exposing the SSO credentials of individual users.

### 1.1.2.3. 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
```
1.1.3. Configuring basic authentication

Red Hat Insights 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:

```plaintext
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.
   ```bash
   # insights-client --register
   ```

1.1.4. Registering the system to Red Hat Insights

Register the system to communicate with the Red Hat Insights service and to view results displayed in the Red Hat Insights console.

Prerequisites

- Root-level access to Red Hat Insights

Procedure

1. Enter the following command to register the system.
1.1.5. Viewing your results

System and infrastructure results can be viewed in the Red Hat Insights console.

The Overview provides a view of current risks to your infrastructure. From this starting point, you can investigate how a specific rule is affecting your systems, or take a system-based approach and see all the rules that pose risk to a selected system.

Procedure

1. Select Rule hits by severity to view rules by the Total Risk they pose to your infrastructure.
   Or

2. Select Rule hits by category to see the type of risk they pose to your infrastructure.

3. Search for a specific rule by name, or scroll through the list of rules to see high-level information about risk, systems exposed, and availability of Ansible Playbook to automate the remediation.

4. Click on a rule to see a description of the rule, learn more from relevant knowledgebase articles, and view a list of systems at risk.

5. Click on a system to see specific information about detected issues and steps to resolve the issue.