Administrator Quick Start Guide

Contents

Before You Configure

Before you start configuring PHEMI Central, the system must be installed and you should have your organization's governance policy clearly defined.

Installation may include populating your system with some of your organization's pre-existing data.

System Installation

PHEMI Central may be shipped as an appliance, deployed on Amazon Web Services (AWS), or deployed on your organization's VMware environment. Regardless of the deployment type, PHEMI Professional Services will install and set up the base system of cluster nodes with a management node and will install the PHEMI Central software on the cluster.

The representative will create an administrator account for you on PHEMI Central, and will provide you with the user name and password for the account, together with the URL of the PHEMI Central Management and Governance Console. At that point, you can log on to the Management and Governance Console.

Governance

A governance policy is a coordinated approach to protecting data and assigning privileges to users. To control and protect your data, your organization should have a clearly defined policy governing data.

Governance Policies

Information governance is about controlling an organization’s data. The data may be sensitive; or perhaps it is important that the data be absolutely accurate; or perhaps the organization must achieve legislative and compliance targets. Data governance includes the process and policies around the protection, curation, and access to data and encompasses all of privacy protection, data security, and data audit.

Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name
enforces governance policies for privacy and security within the data warehouse, rather than at the application layer. In-system governance ensures that data custodians, not application developers, retain control over privacy and security. Managing privacy and security within the data store also simplifies application development and the use of analytics tools.

Your governance policies will drive how you configure
Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name
. Therefore, before configuring
Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name
, you should make sure you have your organization's governance policy available to you. If you are uncertain as to the appropriate data visibilities, user authorizations, or access policies to define for your organization, consult with your Information Officer, Privacy Officer, or with someone in a comparable role.

Defining a Governance Policy

Make sure your organization's governance policy is defined before you begin configuration.

1. Identify the different sensitivity levels of the data you will be storing in
   Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name
   .
   In
   Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name

, these sensitivity levels are called data visibilities, and are used to tag ingested data for purposes of privacy and access control. Examples of data visibilities are "CONFIDENTIAL," "SECRET," or "PII" (Personally Identifiable Information).

2. Identify what authorizations your organization assigns to different users to allow them to access data.

   Your user authorizations should reflect the actual permissions your personnel are granted to interact with data of different visibility.

3. Specify the allowed combinations of user authorizations and data visibilities.

   For example, a user with C_LEVEL authorization (perhaps a CEO, CIO, COO, or CTO) might be permitted to access CONFIDENTIAL data, a user with RESEARCH authorization might only be permitted to access only DE-IDENTIFIED data, and a user with DOCTOR authorization might be allowed to see data of all sensitivity. In Content-Reference to:../_Variables/PHEMI_Central/con_Product-Vars.xml#product-name , the allowed access combinations are implemented as access policies.

Initial Configuration Workflow

Since some configuration tasks must be completed before others can be performed, PHEMI Administrators can use this workflow to configure PHEMI Central.

In these first steps, order matters. You cannot create users until you have defined user authorizations. Likewise, you cannot create access policies without defining both user authorizations and data visibilities.

1. Log on to the PHEMI Central Management and Governance Console.
2. Define user authorizations.
3. Create users. Create at least one PHEMI Administrator, at least one privacy officer, and at least one data analyst.
4. Define data visibilities.

Data categories must be added before you can define data sources. Access policies are optional for data source configuration. If you are using a Data Processing Function (DPF) to create derived data from raw data, you upload the DPF archive as part of data source configuration.

5. Add data categories.
6. Create access policies.
7. Define data sources.

In general, it is the data analyst, not the PHEMI Administrator, who builds and executes datasets. However, configuring dataset destinations is part of system configuration.

8. Configure dataset destinations.