*HPC Data MANAGEMENT*

SAML Authentication and iRODS Standard Authentication Setup Guide

Version *0.1 Draft*

*05/28/2019*

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version Number** | **Implemented**  **By** | **Revision**  **Date** | **Approved**  **By** | **Approval**  **Date** | **Description of Change** |
| 0.1 | Yuri Dinh | 5/28/19 |  |  | Initial Draft |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

TABLE OF CONTENTS

[1. Purpose 4](#_Toc13647852)

[1.1. Intended Audience 4](#_Toc13647853)

[1.2. Assumptions 4](#_Toc13647854)

[2. Instructions for setting up SAML authentication and iRODS Standard authentication 4](#_Toc13647855)

[2.1. Deploy application 4](#_Toc13647856)

[2.1.1. Build HPC DME 4](#_Toc13647857)

[2.1.2. Deploy HPC DME into ServiceMix 4](#_Toc13647858)

[2.2. Set to iRODS standard authentication, key and the signature properties in config file 4](#_Toc13647859)

[2.3. Configure idp.properties to point to the trust store 5](#_Toc13647860)

[2.4. Setting iRODS user standard password via iCommand using a script 5](#_Toc13647861)

[2.5. Start the service 6](#_Toc13647862)

[3. Connecting to iRODS through iCommand 6](#_Toc13647863)

[3.1. Obtaining the new password 6](#_Toc13647864)

[3.2. Setting to the new password through iinit 6](#_Toc13647865)

[4. Add a new IDP public certificate to the trust store 6](#_Toc13647866)

[4.1. Converting IDP public certificate into a crt file 6](#_Toc13647867)

[4.2. Checking into the repository 7](#_Toc13647868)

[4.3. Build and deploy 7](#_Toc13647869)

# Purpose

**This document is for historical record only**.

This document describes installation instructions to setup HPC Data Management Services allowing the use of SAML assertion for user authentication, in addition to the existing basic authentication and HPC DME token authentication support. It also provides instructions on switching to iRODS Standard authentication in order to allow SAML assertion for user authentication.

## Intended Audience

The HPC DME System Administrators.

## Assumptions

General pre-requisites:

* User has sudo permissions in the environment to be setup.
* User has access to irods user.

# Instructions for setting up SAML authentication and iRODS Standard authentication

## Deploy application

## Build HPC DME

Refer to the Admin guide for build instructions for the intended environment.

## Deploy HPC DME into ServiceMix

Refer to Admin guide for deployment instructions for the intended environment.

## Set to iRODS standard authentication, key and the signature properties in config file

**hpc.integration.irods.key=<key>  
hpc.integration.irods.algorithm=<algorithm>  
hpc.integration.irods.ldapAuthentication=false**

**############################################################**

**# Crypto Properties.**

**############################################################**

**hpc.ws.rs.security-signature-properties=file://${karaf.base}/etc/hpc-server/idp.properties**

## Configure idp.properties to point to the trust store

**org.apache.ws.security.crypto.merlin.truststore.file=/opt/apache-servicemix-7.0.0.M3/etc/hpc-server/cacerts.jks**

**org.apache.ws.security.crypto.merlin.truststore.password=<password>**

## Setting iRODS user standard password via iCommand using a script

Login to the iRODS server and run the script, dm\_update\_irods\_user.sh <key> to set standard authentication password. Key is the random string configured in 2.2.

**#! /bin/bash**

**if [ -z "$1" ]**

**then**

**echo "USAGE: dm\_update\_irods\_user.sh <key>"**

**exit 1**

**fi**

**excluded\_users=(rods dice\_user dice\_user\_group\_admin dice\_user\_sys\_admin)**

**iadmin lu | while read user; do**

**user\_name=$(echo "$user" | cut -d'#' -f 1)**

**#Skip the dice test created accounts**

**if [[ $user\_name == testid-\* ]]**

**then**

**continue**

**fi**

**#Skip the excluded users**

**(for e in "${excluded\_users[@]}"; do [[ "$e" == "$user\_name" ]] && exit 0; done; exit 1)**

**if [ $? == 1 ]**

**then**

**echo "$user\_name"**

**new\_pass=$(echo -n "$1$user\_name"| openssl dgst -md5 -binary|base64)**

**#Remove the LDAP temporary password**

**iadmin rpp $user\_name**

**#Update the standard auth password for user**

**iadmin moduser $user\_name password $new\_pass**

**fi**

**done**

## Start the service

Start the service using the service account.

# Connecting to iRODS through iCommand

Since the authentication is now set to Standard authentication, once the user logs into the irods server with user credentials, in order to use the iCommands, we need to provide the standard auth credentials.

## Obtaining the new password

Use the key and algorithm configured in 2.2 to obtain new password.

**echo -n "<key><user>"| openssl <algorithm>|base64**

## Setting to the new password through iinit

Remove the following line from irods\_environment.json file in ~/.irods folder then issue an iinit command to authenticate using the password obtained in 3.1.

**"irods\_authentication\_scheme": "PAM",**

# Add a new IDP public certificate to the trust store

## Converting IDP public certificate into a crt file

Save the Identity Provider’s public certificate into a file, idp.cer.

**-----BEGIN CERTIFICATE-----**

**xxxx**

**….**

**xxxx**

**-----END CERTIFICATE----**

Issue an openssl command to convert to crt file.

**openssl x509 -inform PEM -in idp.cer -out certificate.crt**

## Checking into the repository

Check-in the crt file to:

**HPC\_Data\_Management/src/hpc-server/hpc-ws-rs-impl/src/main/resources/certs/idp.crt**

## Build and deploy

The deployment will replace the cacert trust store with the new trust store including the new public certificate.