**Security Layer – User Manual**

****

****



|  |  |
| --- | --- |
| Document Owners | Liudmila Dobriakova [RPLY] |
| Contributors | Lorenzo Bracco [RPLY] |
| Dissemination | Public |
| Date | 30/05/2016 |
| Version | 1.0 |

Table of Contents

1 Authentication and Authorization Introduction 3

1.1 Overview 3

1.2 First use case 5

# Authentication and Authorization Introduction

The goal of the security authentication layer is to create a trusted access to the Osmose platform and a correct granting of the resources based on the client that requests the access.

This layer will manage authentication and authorizazion to the Osmose platform and, eventually, among some of its sub-systems.

Security is a one of the most important aspects of any IoT platform and it has several key concepts, such as:

* Confidentiality
* Integrity
* Availability
* Authentication
* Authorization

## Overview

This document describes the use of the OSMOSE Authorization and Authentication Layer to protect two example resources created to show the functionality.



Figure 1 – The basic IdP-SP setup for Osmose platform

No additional software components have been developed.

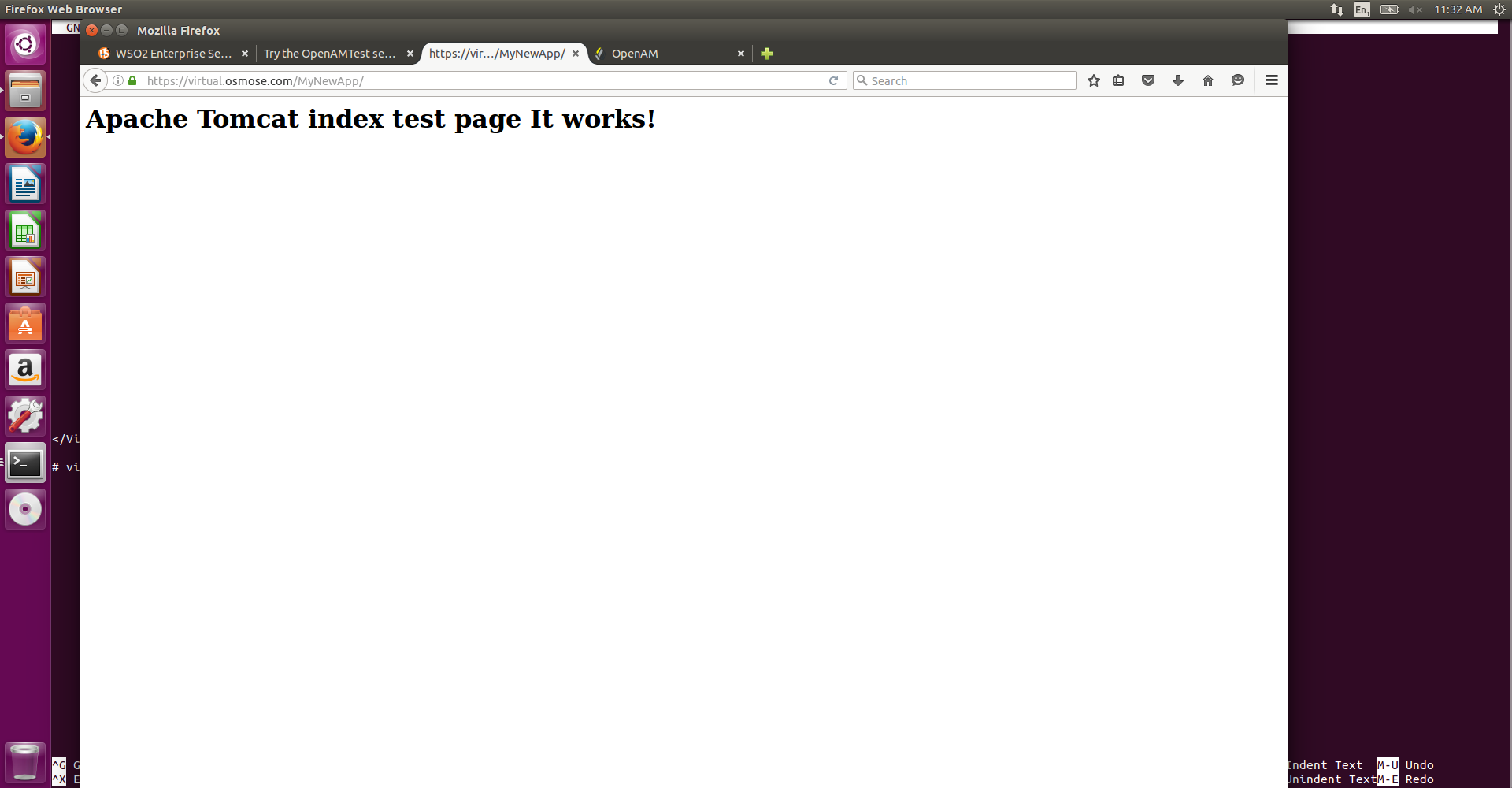
Refer to the official guides of the used tools to retrieve the specific user manual:

* OpenAM: <http://openam.forgerock.org/openam-documentation/openam-doc-source/doc/admin-guide/index.html>

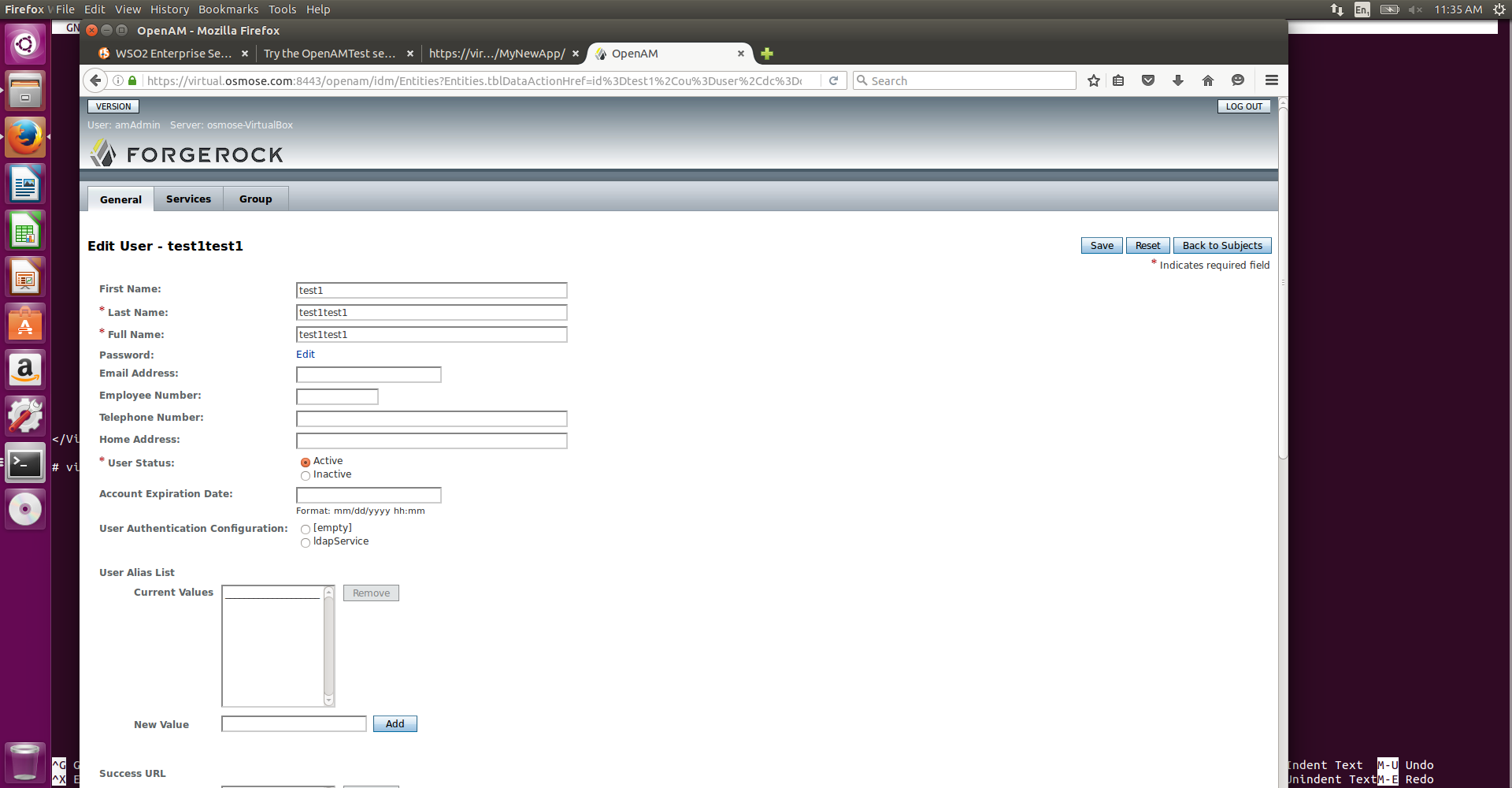
## Setting up the security layer

Let’s assume we have some resources to protect, for example this one:

<https://virtual.osmose.com/MyNewApp/>

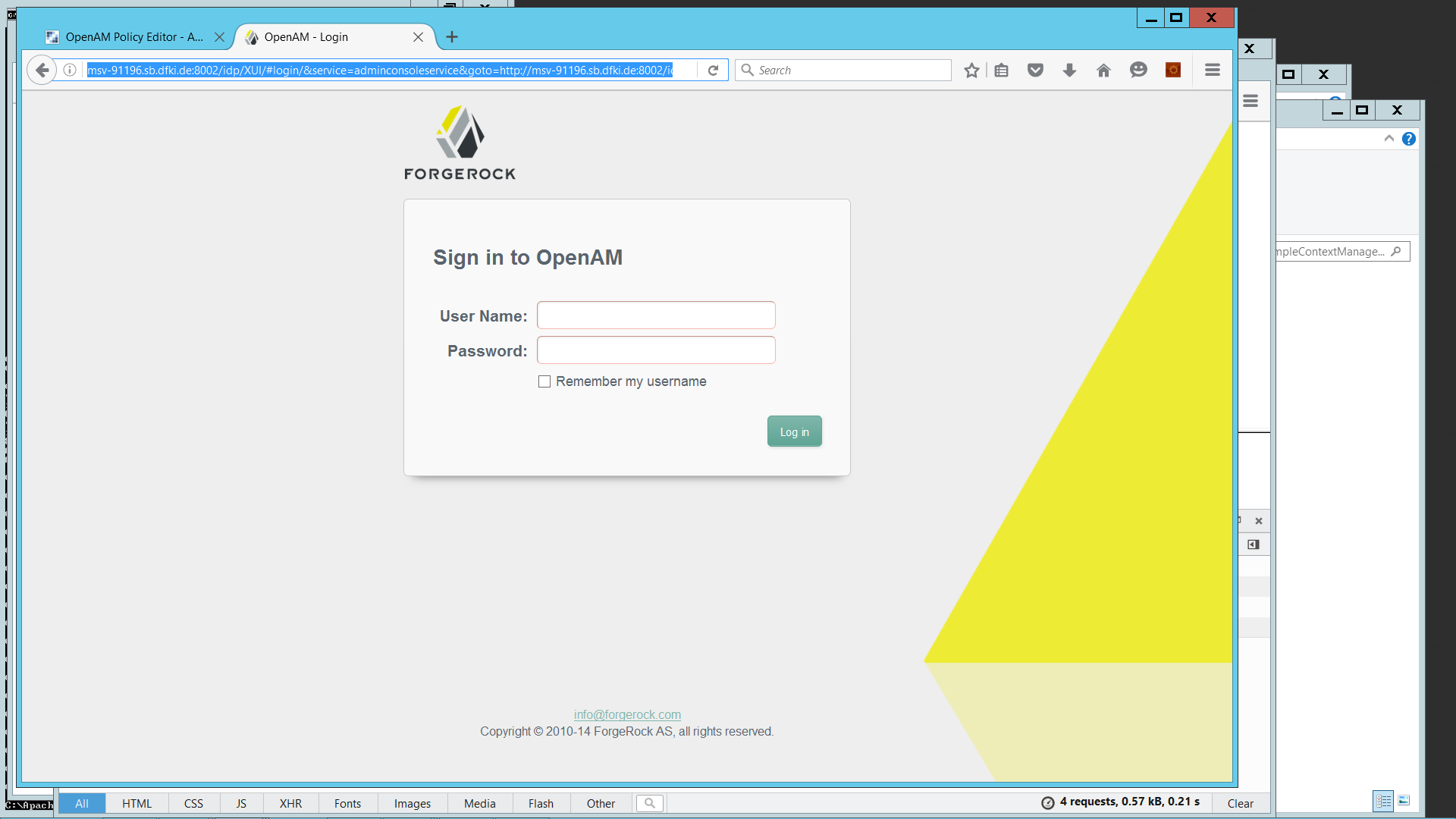


And the user test1.

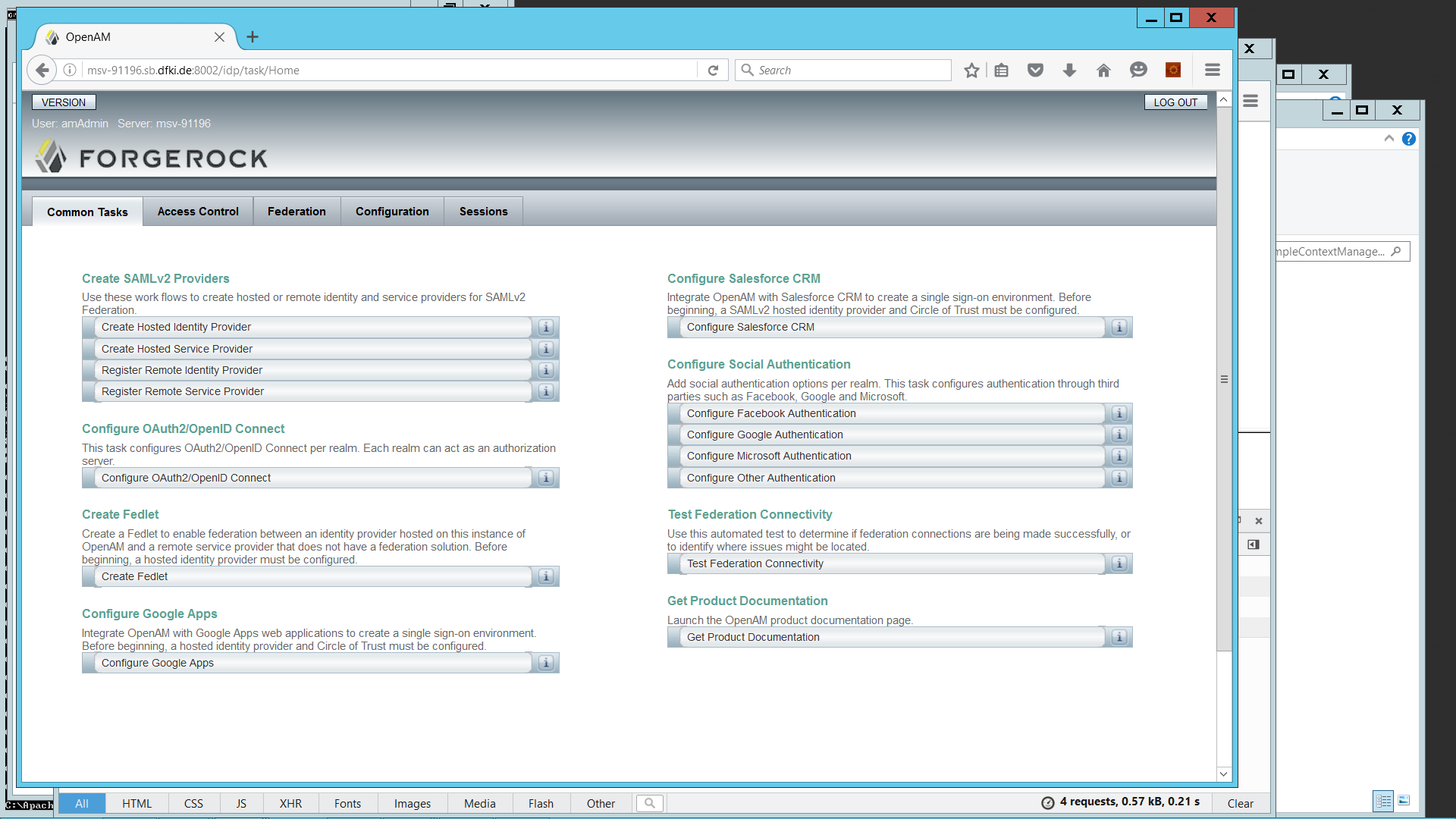


Let's create the policie to made all resources not available for the user “test1“.

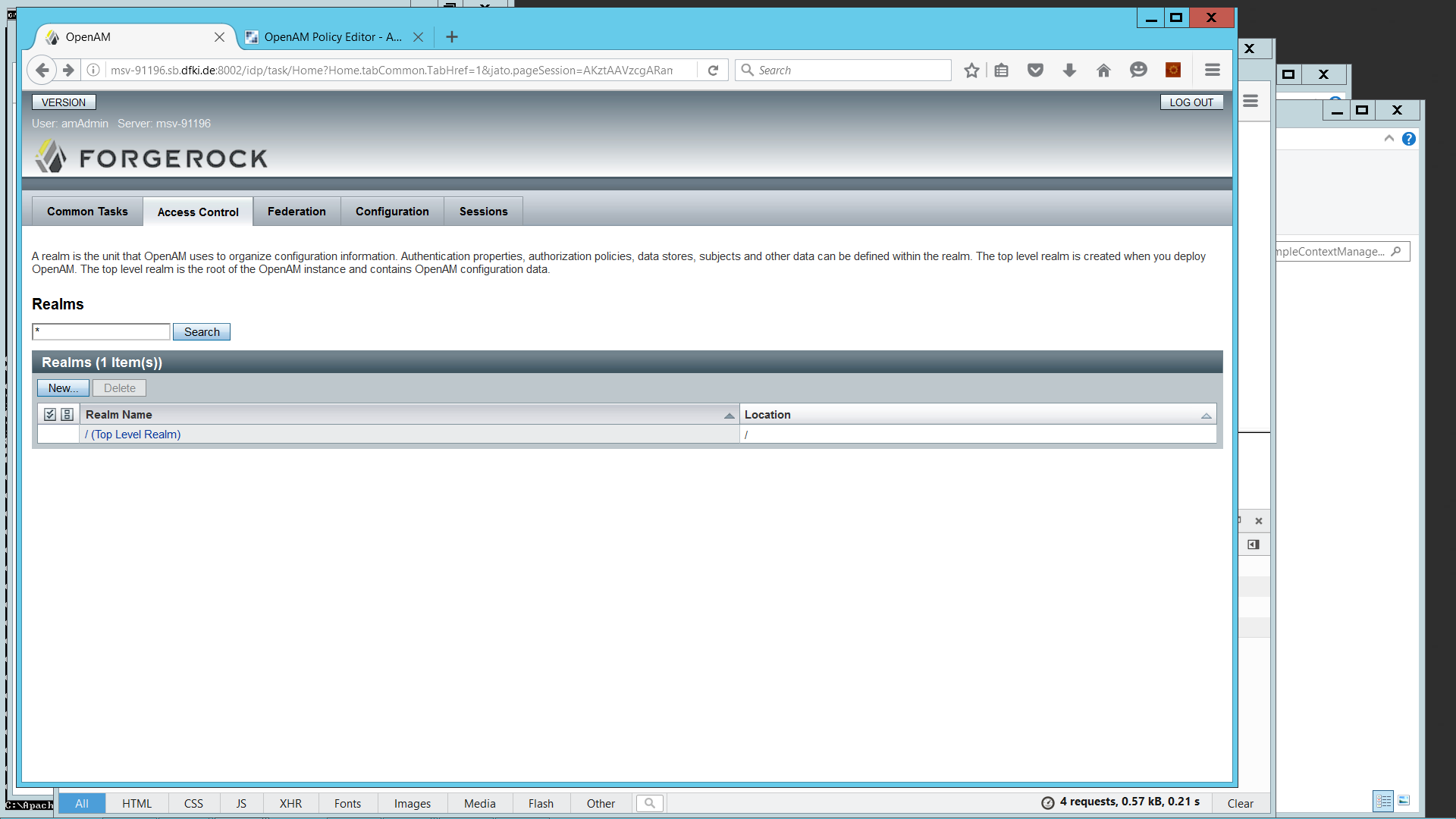
Go to the url: <http://localhost:8002/idp/task/Home> to get an access to the OpemAM management console.



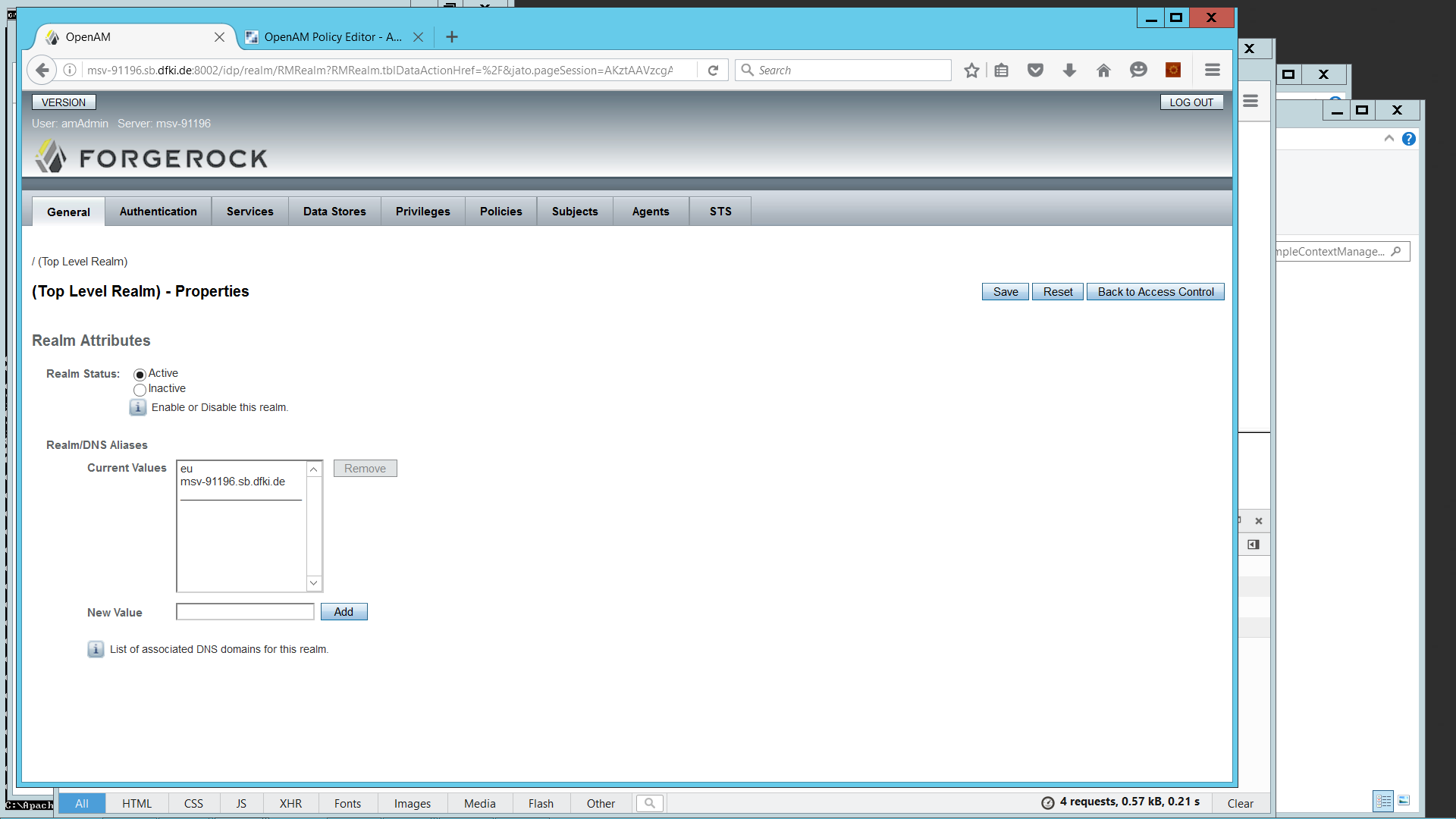
Sign in with the credentials: amAdmin/osmose2015 to get the following page:



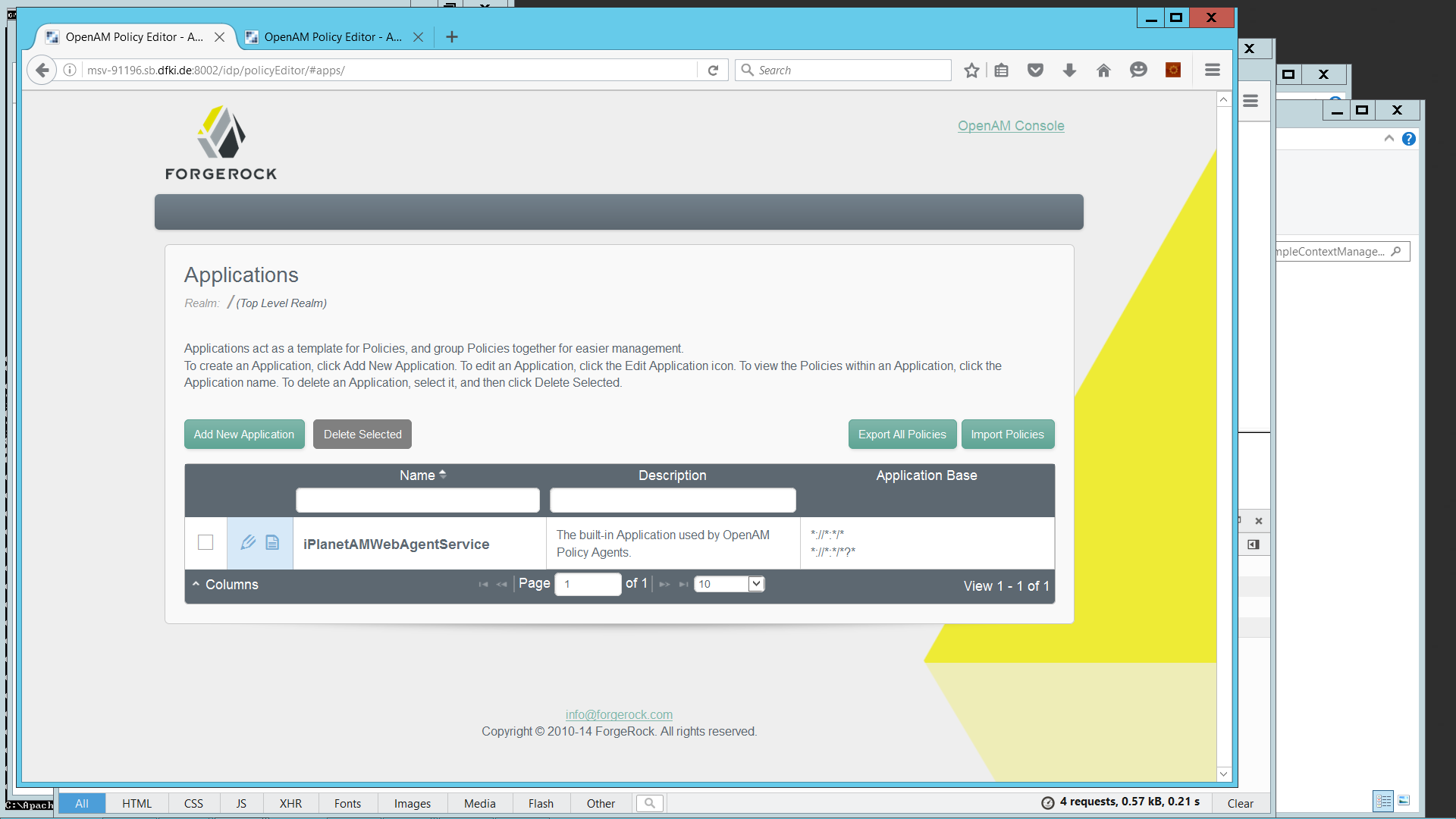
Go to Access Control



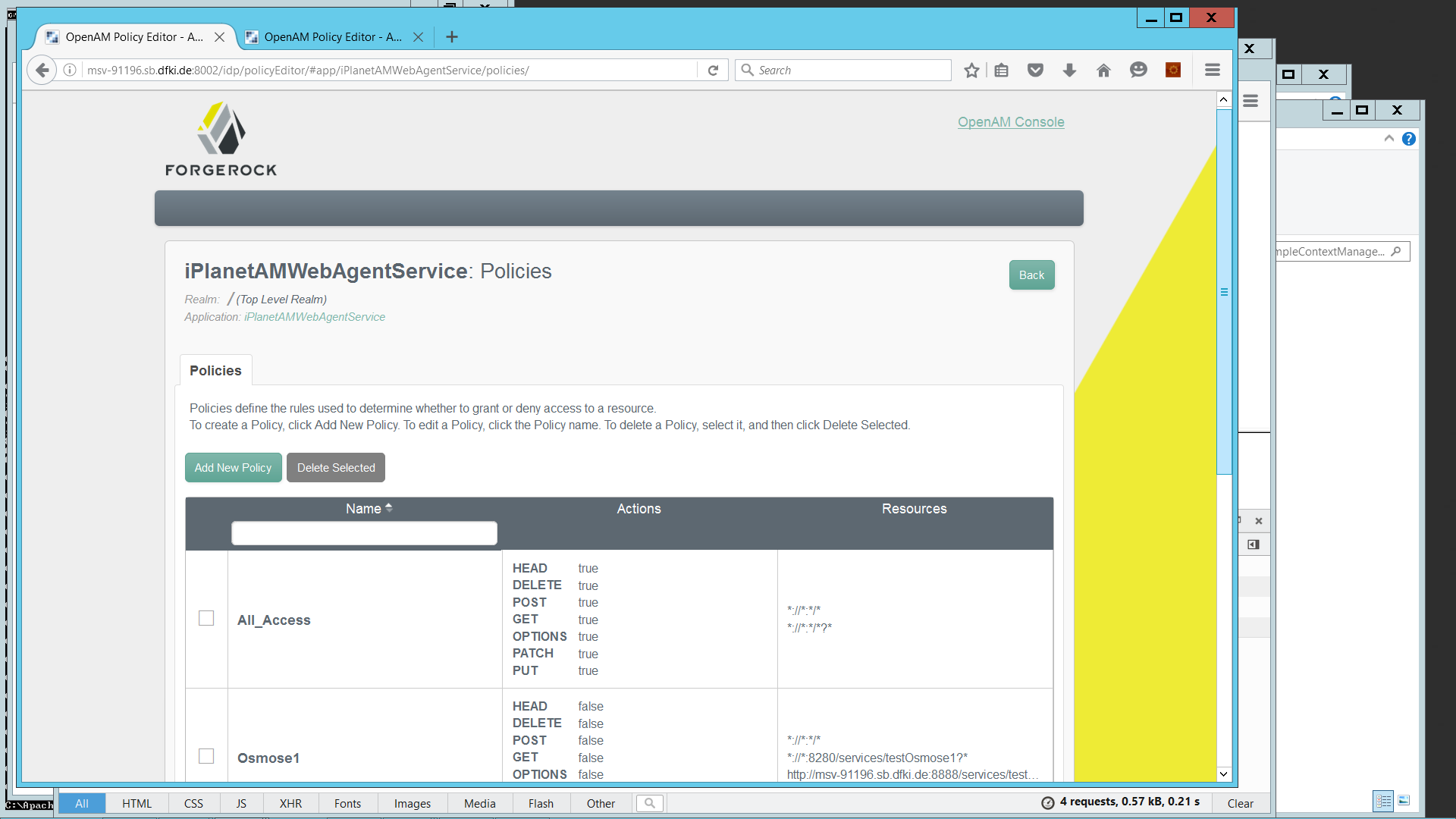
Click on “Top Level Realm”



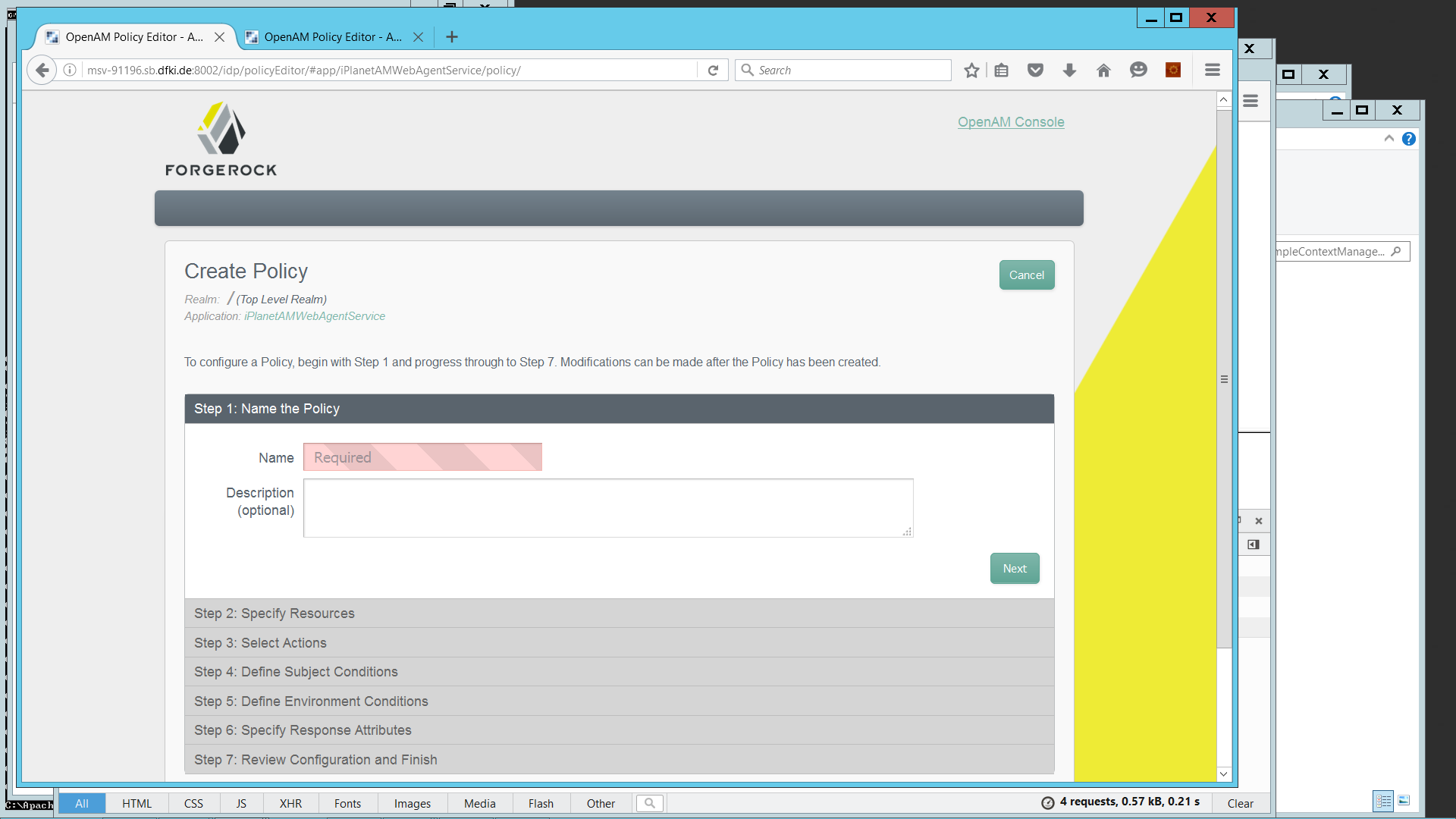
Then on “Policies”



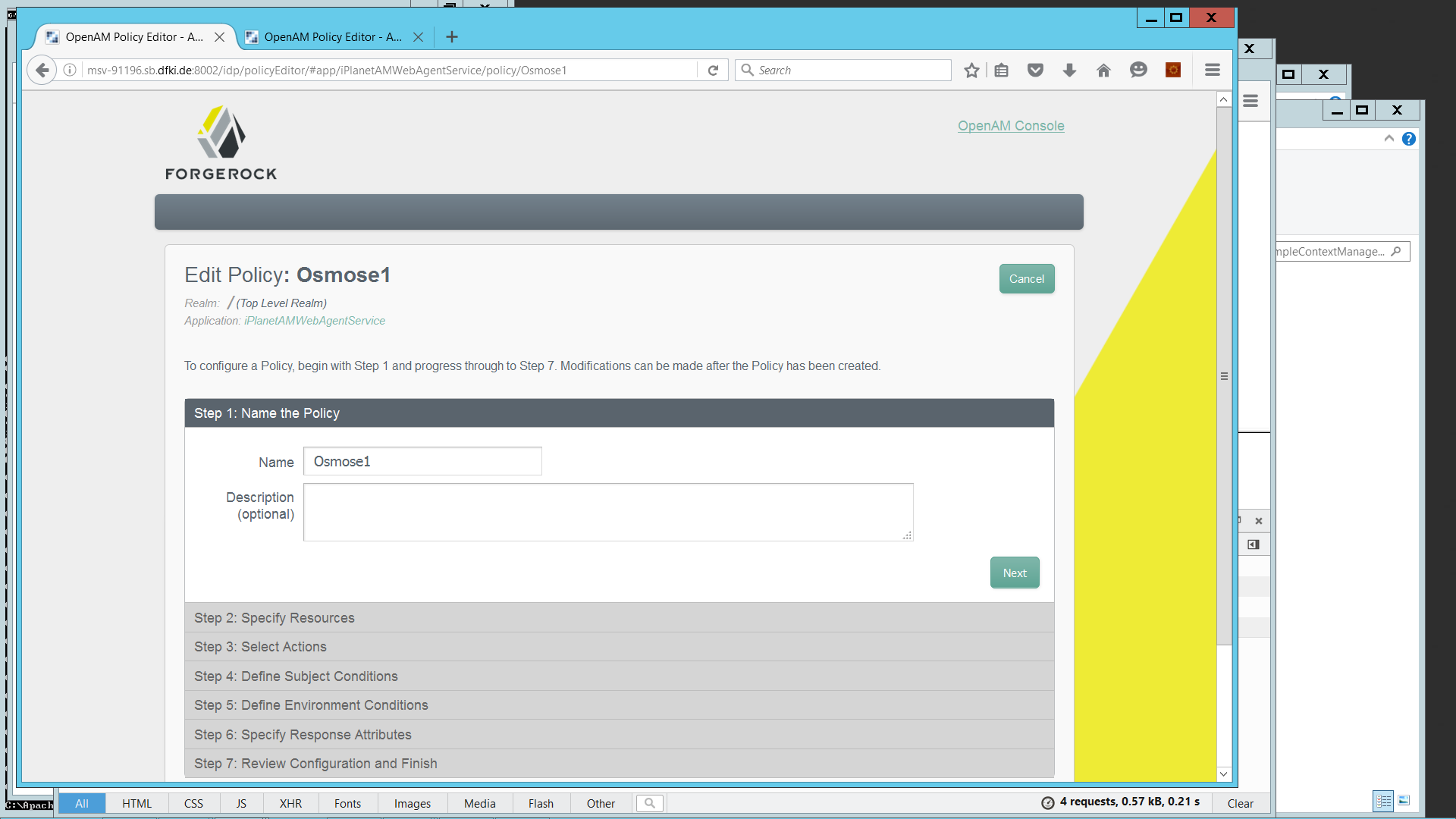
Click on iPlanetAMWebAgentService to add or modify policies.



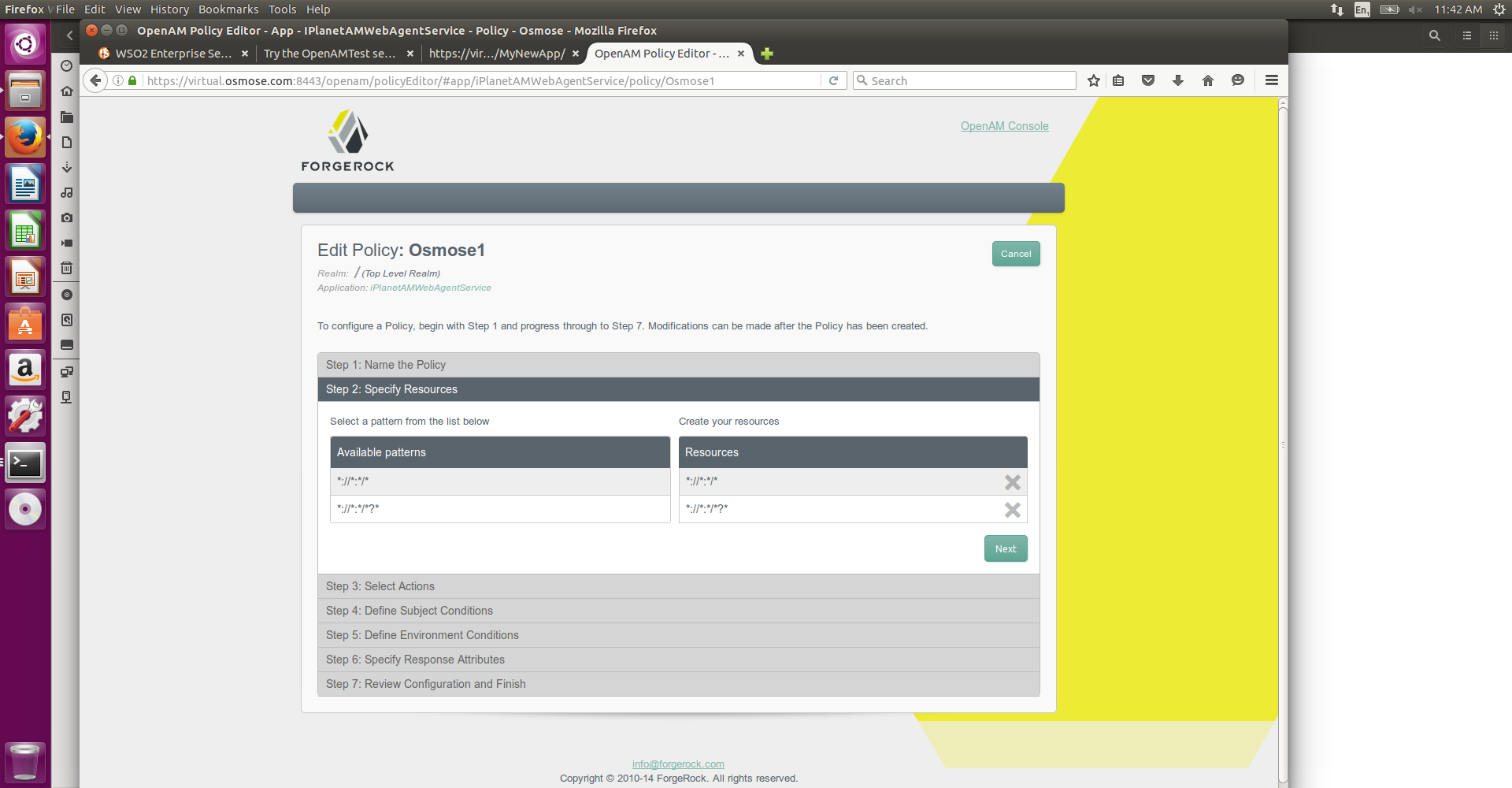
Click on “Add New Policy”



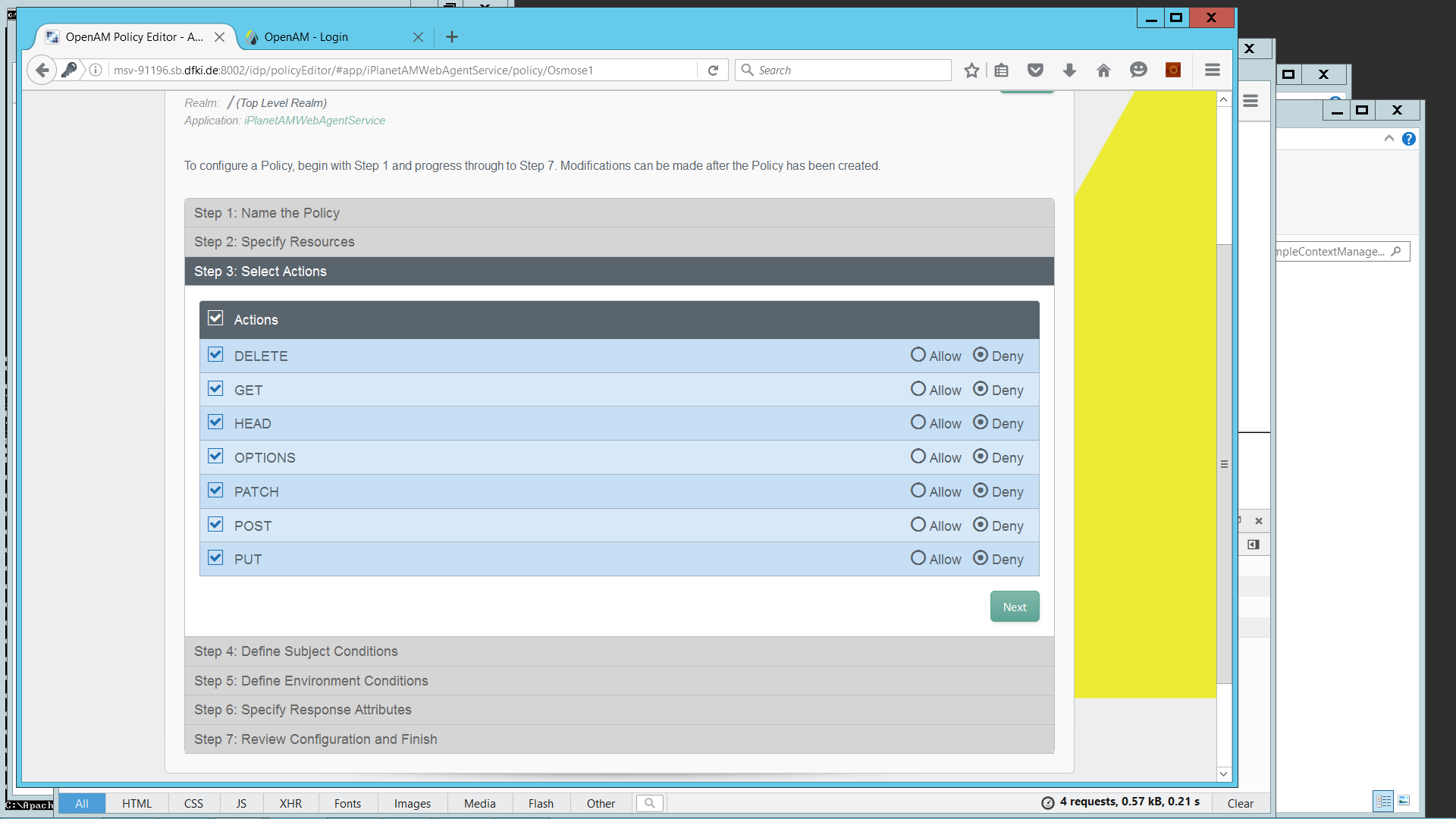
Step 1 - Give it a name



Step 2: click on the first pattern and fill in the fields so that you have the resource to protect, and then click the plus symbol to add it

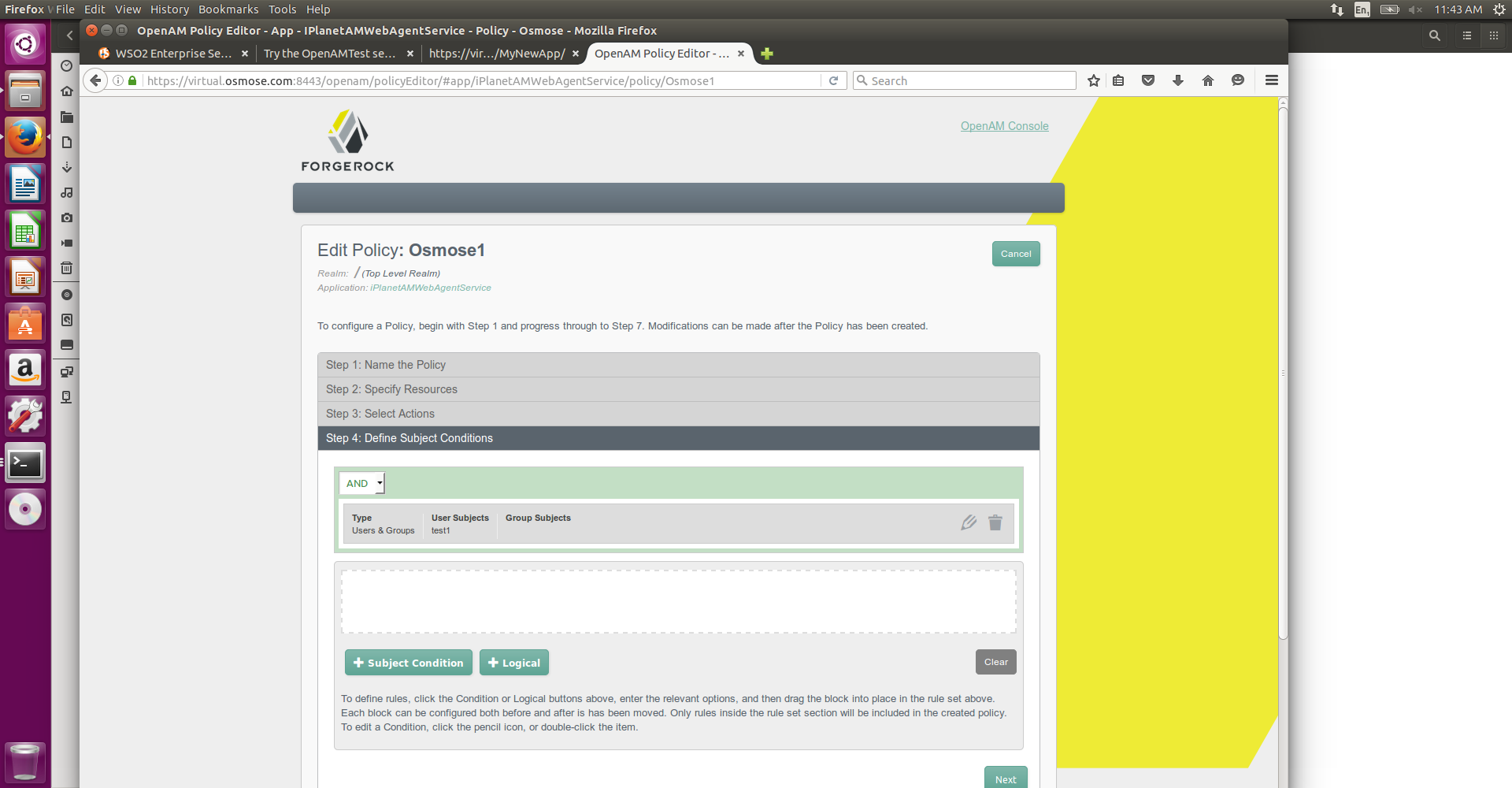
****

Step3: Actions



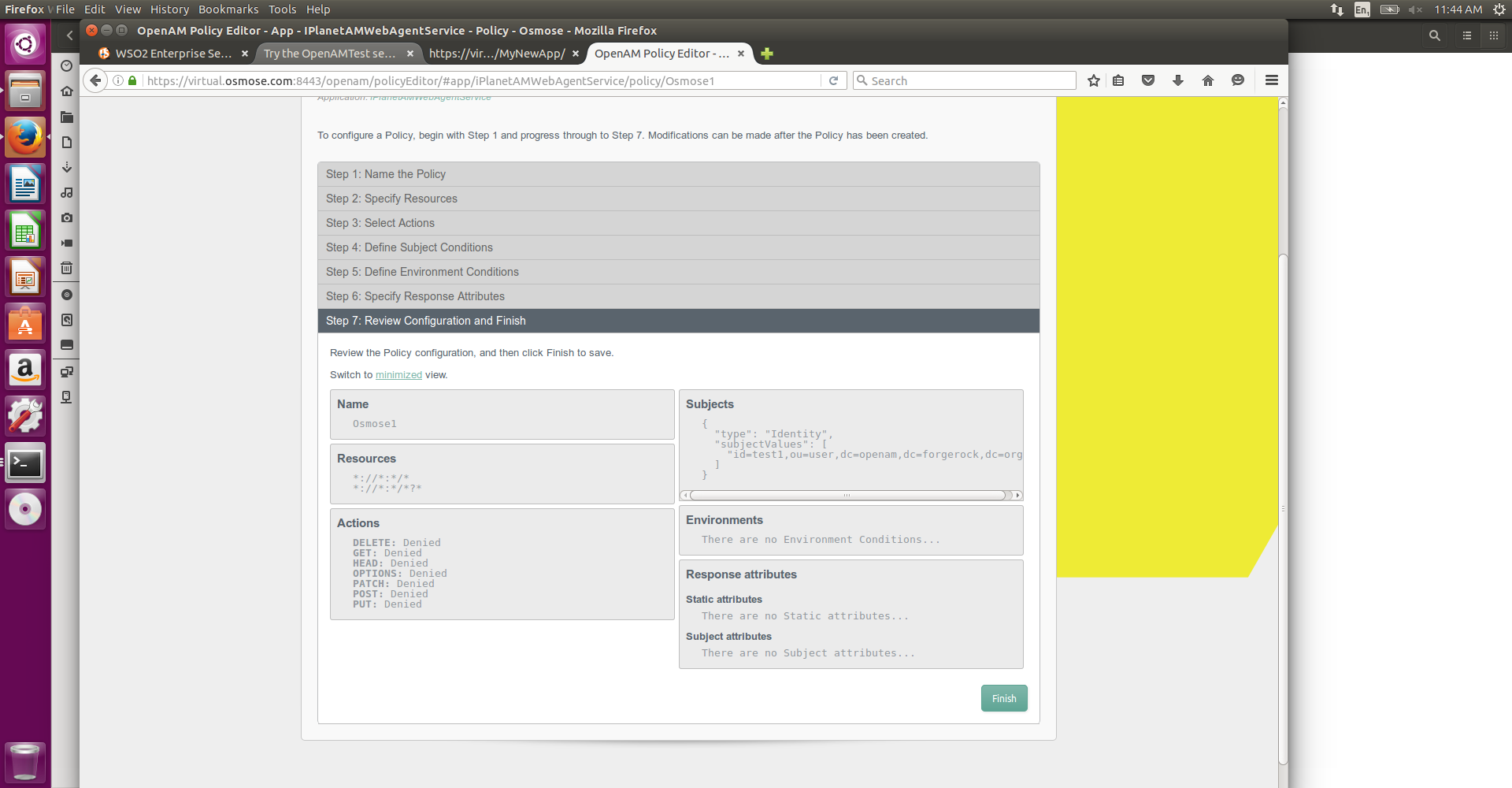
Check all the boxes and deny everything.

Step 4 – Define subject conditions



add a subject condition, choose type “Users & Groups”, add “test1” as user subject and drag the condition under the “AND”.

Jump to step 7 and verify if everything is correct.



Repeat the same procedure for the other resource or user if you need.

To verify if the functionality of the just created policy, log out from the OpenAM as amAdmin and go to the url defined in the beginning of this tutorial: <https://virtual.osmose.com/MyNewApp/>

Now trying to access this url the browser will be redirected to the OpenAM page to verify the user credential. In case the test1 user logged in, the following page showed up denying the acces to the resource.

