FORUMSYSTEMS™

MANAGING & ACCELERATING XML WEB SERVICES SECURITY

FORUM SYSTEMS HANDS-ON TRAINING

LAB 13. IDENTITY – LDAP INTEGRATION

Published: September 2014
Forum Systems Hands-on Training – Lab 13. Identity – LDAP Integration
D-ASF-SE-010029

Contents

Introduction

Lab 13. Identity – LDAP Integration

Skill Level

This lab is Beginner Skill Level. Little to no prior experience with Forum Sentry or SOAPSonar is required.

Prerequisites

This lab requires the Forum Sentry Training Image, with a licensed copy Forum Sentry.

Refer to the "FS_Training_Labs_v8-1_Introduction" document for information on the Forum Sentry Training Image and licensing SOAPSonar Enterprise Edition.

Internet access to the Forum Systems online LDAP server is required. If using the online Training Image access is available. If using a local VM image, ensure your system can communicate with ldap.forumsys.com on port 389. For more information on this test LDAP server see: http://www.forumsys.com/tutorials/integration-how-to/ldap/online-ldap-test-server/

Lab Overview

This lab focuses on integrating Sentry with an LDAP server. Sentry can communicate with any LDAPv3 server to validate both runtime and admin credentials.

For admin credentials, LDAP Policies can enable full "privileged access" rights or apply a role restriction.

When validating runtime credentials with an LDAP server, Sentry also retrieves various user attributes for the user record in the LDAP directory.

Integrating Sentry with an LDAP server is a very common use case for both Sentry administrators (configuring admin access) and Sentry developers (configuring runtime auth policies).

The LDAP server we will utilize in this lab is an online LDAP server provided by Forum Systems. Internet access to the LDAP server is required.

This lab will provide instructions for creating LDAP Policies in Forum Sentry. Topics include:

1. Creating LDAP Policies
2. Copying LDAP Policies
3. Testing LDAP Policies
4. LDAP Policies for Admin Access
5. LDAP Policies for Runtime Access

Building an LDAP Policy

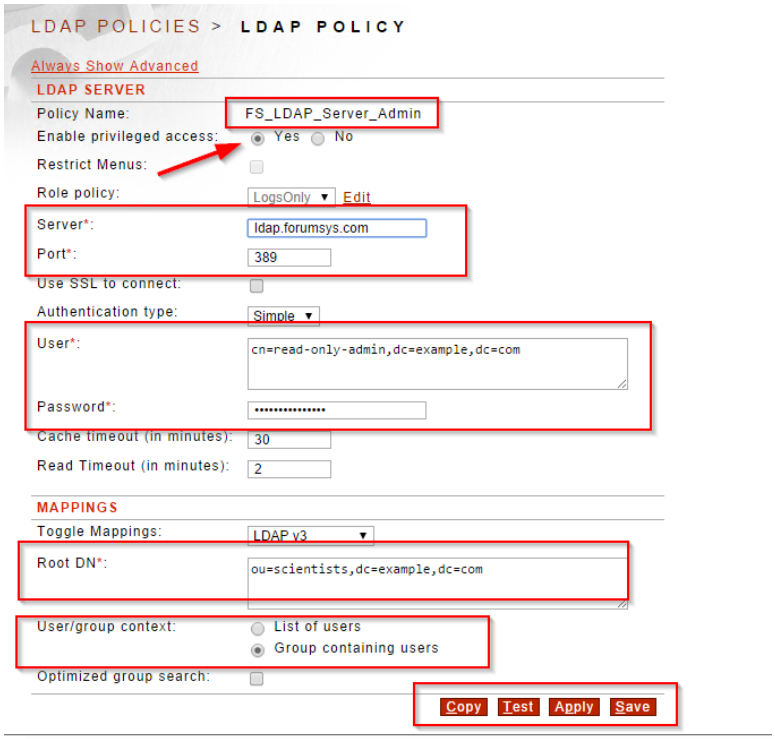
We will now build simple LDAP Policies in Sentry for both runtime access and admin access.

Build a Privileged User LDAP Policy

In this step we will build a new LDAP Policy in Sentry for validating Sentry WebAdmin login credentials (admin credentials). The LDAP user credentials will allow full access to Sentry (privileged user access).

Follow the steps below to build a Privileged User Admin Access LDAP Policy in Sentry

1. Navigate to the Access→User Policies→LDAP Policies page
2. Click New and create an LDAP Policy with the following criteria:
    a. Name: FS_LDAP_Server_Admin
    b. Enable Privileged Access: YES
    c. Server: ldap.forumsys.com
    d. Port: 389
    e. User: cn=read-only-admin,dc=example,dc=com
    f. Password: password
    g. Root DN: ou=scientists,dc=example,dc=com
    h. User/group Context: Group containing users
    i. Leave all other defaults
    j. Click Apply
    k. Click Test (it should return a success message at the top)
    l. Click Save



3. To test this new LDAP policy, simply log out of the WebAdmin (button at bottom right) and

attempt to log in with any of the following user accounts. The password for each is “password” (without the quotes).

a. einstein
b. newton
c. galieleo
d. tesla

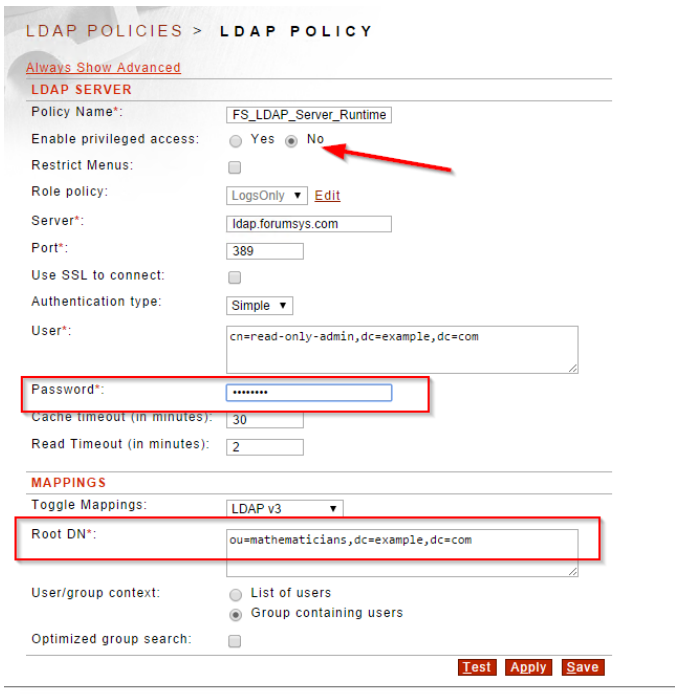
4. After logging in, check the Sentry Audit log for details of the WebAdmin login. Set the log threshold to DEBUG and log in again to see more details.

Build a Runtime User LDAP Policy

In this step we will create a copy of the LDAP Policy built in the previous step. We will adjust the LDAP policy to point to a different Root DN and remove the privileged user rights.

Follow the steps below to build a Runtime User LDAP Policy in Sentry

1. Navigate to the Access→User Policies→LDAP Policies page.
2. Open the “FS_LDAP_Server_Admin” LDAP Policy.
3. Click the Copy button at the bottom, this will clone the policy.
4. Make the following modifications to the new LDAP Policy (leave everything else the same):
   a. Name: FS_LDAP_Server_Runtime
   b. Password: password (the passwords are not copied so it needs to be reentered)
   c. Root DN: ou=mathematicians,dc=example,dc=com
   d. Click Apply
   e. Click Test (it should return a success message at the top)
   f. Click Save



5. The users in the mathmeticians group should not be able to log into the WebAdmin interface, as the “Enable privileged access” option is disabled. To test this runtime user LDAP policy, you will need to add the LDAP policy to a User ACL and associate the User ACL to a runtime policy. This will be covered in a different lab in this series.

   The following user accounts (all with password of “password” without the quotes) will work for this Root DN:

   a. riemann
   b. gauss
   c. euler
   d. euclid

END

Additional Testing and More Reading

BACK IT UP!

It is recommended that you export your full Sentry configuration after completing this lab.

To export your full Sentry configuration, navigate to the System→Configuration→Import/Export screen and use the Export option in the center of the page to export the full Sentry configuration file as a password encrypted FSX file. This can later be imported on the same screen.

Additional Tests

1. With the "FS_LDAP_Server_Admin" policy, remove the privileged access, but apply enable the Restrict Menus option and apply a Role policy.
2. Review the Sentry Audit log for details of the LDAP calls. Use the same credentials multiple times. Is Sentry pulling from the local cache? Set the cache value to 0 and try again.
3. Build a REST policy and enable password authentication with the users validated against LDAP.
4. Configure Sentry for your own LDAP or Active Directory.

Additional Information

Details of the online LDAP Server from Forum Systems:
http://www.forumsys.com/tutorials/integration-how-to/ldap/online-ldap-test-server/

For more information on LDAP Policies see the following Helpdesk FAQs:

Validating LDAP Policies: https://helpdesk.forumsys.com/entries/20330257-How-To-Validating-LDAP-Policies-Settings

Sample LDAP Filters: https://helpdesk.forumsys.com/entries/39402778-FAQ-Sample-LDAP-Filter

For more information, review the following Forum Sentry Admin Guide:

1. Access Control Guide

About Forum Systems

Forum Systems is the global leader in API and Cloud Security technology with industry-certified, patented, and proven products deployed in the most rigorous and demanding customer environments worldwide. Forum Systems has been an industry leader for over 12 years and has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP. Forum Systems security-first mindset enables trusted, network edge deployments of its technology for protecting critical enterprise transactions.

Our product technology is purpose-built and designed for mission-critical, enterprise-class scalable solutions where business solutions require the modern day security and identity enforcement protection, while enabling a scalable architecture and low-latency, high-volume throughput.

Forum Systems supports global enterprise customers across industries in commercial, government, and military sectors. Forum Systems technology provides the leading-edge of modern-day cyber-security innovation with integrated identity and SSO features that enable out-of-the box business solutions with point-and-click technology.

Forum's patented; FIPS 140-2 and NDPP certified hardware and virtual products make modern-day business communications secure by actively protecting and accelerating data exchange and API service access across networks and business boundaries. For more information, please visit www.forumsys.com.