Identity Integration with SimpleSAMLphp

Recipes for Becoming a SAML Superhero

Steve Moitozo II

Identity Integration with SimpleSAMLphp

Recipes for Becoming a SAML Superhero

Steve Moitozo II

This book is for sale at http://leanpub.com/simplesamlphp

This version was published on 2014-03-10

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Tweet This Book!

Please help Steve Moitozo II by spreading the word about this book on Twitter!

The suggested hashtag for this book is #simplesamlphp.

Find out what other people are saying about the book by clicking on this link to search for this hashtag on Twitter:

https://twitter.com/search?q=#simplesamlphp

Contents

A Note About "Lean" **1**
An Offer of Help 1
Feedback 1

Chapter 1: Beyond Single Sign-on **2**

Chapter 3: SimpleSAMLphp **4**

Chapter 4: Case Studies **5**
Cisco, Drupal and SimpleSAMLphp 5

A Note About “Lean”

The perfectionist in me wants to stop everything and write you the perfect book on SimpleSAMLphp but I know from experience that I would fail. I also know that it’s possible no one will want to read it. So, rather than worry about all that I have decided to go the lean approach. I will write as I have time and try to improve the value of this work through your feedback.

I plan to leave “breadcrumbs” throughout the book as a way of sparking discussion or leaving notes to myself on topics people might want me to cover at some point. If one of them is of interest to you please let me know.

An Offer of Help

I realize you’re taking a risk buying a book that’s under development and I want you to get real value. So, I am offering a half hour of consulting for buying my book just to make sure you get what you need. Of course, you will also get free updates to the book because you purchased it on leanpub.com.

Please buy the book to find out how to take advantage of this offer.

Feedback

Don’t want to talk to me but have feedback on the book? Please leave it at leanpub.com[1]

[1] https://leanpub.com/simplesamlphp

Chapter 1: Beyond Single Sign-on

In the early 2000s I worked at a small liberal arts college. The Web was taking over and we were deploying Web applications left and right. When I first arrived the average user had about seven passwords to remember for our various systems. We needed to consolidate these credentials to enforce security policies and help reduce the burden on users. Single sign-on seemed like the best way to go. At the time systems like Pubcookie, Yale CAS (now JA-SIG CAS) and CoSign were all the rage among academic institutions and many of our peer institutions were looking to implement them.

In 2005 I attended a meeting of Engineers from several universities to discuss these issues. I remember hearing that the University of Washington had implemented a single sign-on solution but was going to convert from it to Shibboleth. They were doing this so they could have a single sign-on solution that worked with their locally hosted applications as well as applications hosted at peer institutions. That was the moment I realized the power of federated identity systems; single sign-on that works across organizational boundaries.

Today this type of arrangement is even more compelling. Cloud vendors are supporting federated identity, making it possible to do integrations with commercial vendors without the need to give them access to passwords. In larger contexts where Web applications are deployed by different divisions of an organization the use of federated identity can reduce the risks to passwords by ensuring that users only authenticate to a central identity provider, not to individual applications. This also has the added benefit of making custom applications simpler because there is no need to re-implement user and password management features in each application.

In the realm of inter-organization federated identity management Security Assertion Markup Language (SAML) has emerged as the de facto mechanism of choice. SAML is implemented in Shibboleth and Microsoft Active Directory Federation Services (ADFS). Google, Box.net, and Salesforce.com all support SAML. But federated identity with SAML is viewed as black magic. Just the mention of SAML among developers often results in blank stares from many and the urge to call in sick from others. Visions of complexity and endless documentation dance in their heads.

It doesn't have to be this way. *Identity Integration with SimpleSAMLphp* is designed to make you a SAML superhero. After reading this book you will be able to speak intelligently about SAML and SimpleSAMLphp, the premiere implementation of SAML in the PHP programming language. The book explains important SAML concepts in plain language and presents numerous recipes for using SimpleSAMLphp to integrate applications, even non-PHP applications.

Whether you want to connect Google Apps to your corporate directory, connect your custom application to a SAML identity provider, hook multiple Drupal Web sites together, bridge Facebook and SAML, or set up a SAML federation this book will help you with practical examples in plain language.

Breadcrumbs

- SAMLization as preparation for multi-factor auth

Chapter 3: SimpleSAMLphp

SimpleSAMLphp is an open source lightweight implementation of SAML written in the PHP programmming language. The project was commissioned by UNINETT AS–the operator of the national research and education computer network in Norway–and authored by Andreas Akre Solberg and Olav Morken. UNINETT received the 2008 Emerging Application IDDY Award from the Liberty Alliance for SimpleSAMLphp. The software has been well received by the PHP community and as a result a cadre of developers and implementers has gathered around the open source project, fueled by the work of Andreas and Olav to provide basic integrations for common PHP applications like Drupal, DokuWiki, Moodle, and others. Every day millions of users in European research and higher education federations like FEIDE (Finland), WAYF (Denmark), and RedIRIS (Spain) use SimpleSAMLphp.

SimpleSAMLphp implements the SAML 2.0 Web Browser SSO Profile for both Identity Providers and Service Providers, the SAML Single Logout Profile, and the SAML Identity Provider Discovery Profile. In addition the software implements SAML 1.1, Shibboleth 1.3, A-Select, OpenID, WS-Federation, and OAuth. Out of the box it can authenticate users against LDAP, Active Directory, CAS, Radius, OpenID, SQL databases, and YubiKey to name a few. The interface has been translated into 20 languages and is fully themable.

Beside the vast array of included features, SimpleSAMLphp is also quite extensible. The modular structure of the software makes it easy to extend through custom modules. In fact, I wrote an authentication source[2] for SimpleSAMLphp that will authenticate users against the API of a local Drupal site in about 100 lines of code.

[2] druplauth - http://code.google.com/p/drupalauth/

Chapter 4: Case Studies

Cisco, Drupal and SimpleSAMLphp

Cisco Systems, the California based manufacturer of networking equipment, has been leveraging Internet collaboration for years. In support of this strategy Cisco operates a SAML 2.0 Identity Provider that provides identity services for numerous Web resources geared for employees, partners, distributors, and the general public.

As a long standing client of Cloudbiz, Cisco approached them to develop a new collaboration site called the "Solutions Acceleration Partner Center" and they wanted it to integrate with their SAML IdP. Cloudbiz (an Acquia Partner), routinely employs Acquia's DevCloud platform for production Drupal sites. So, Cloudbiz founder, Richard Bennion, began researching the feasibility of integrating Drupal and SAML on DevCloud. Richard recalls, "After doing some research into using SAML with Drupal on DevCloud a couple of people told me it would be tricky, if not impossible, to get working on DevCloud. It was looking like we'd have to upgrade to Managed Cloud or use a different hosting platform altogether." Always up for a challenge, he believed there had to be someone who could get SAML and Drupal to work on DevCloud. After researching various approaches Richard contacted me because I was listed as the maintainer of the simplesamlphp_auth module for Drupal.

Since I was not familiar with the details of the Acquia's DevCloud platform Richard and I conducted some exploritory tests to see what it would take to get SimpleSAMLphp running on DevCloud. Our initial testing was positive and we decided to proceed, first by installing and configuring SimpleSAMLphp as a SAML 2.0 Service Provider, then by integrating it with the Drupal site using the simplesamlphp_auth module. Our testing revealed a number of challenges that we would have to work around but ultimately after a couple of adjustments to the default configuration we were able to prove that we could run SimpleSAMLphp DevCloud.

DevCloud, like other high end Drupal hosting platforms uses NGiNX, a high performance reverse proxy server, and Varnish, a caching reverse proxy. Initial testing indicated a negative interaction between varnish's caching activity and SimpleSAMLphp. We needed SimpleSAMLphp to run over HTTPS, and as it turned out HTTPS traffic by-passes varnish. As soon as we by-passed varnish with HTTPS, SimpleSAMLphp began responding properly. The second challenge was deciding how to store session data for SimpleSAMLphp, since the default phpsession option is not compatible with way Drupal handles sessions. SimpleSAMLphp supports memcache and SQL for session storage, beside the phpsession option. To get us moving we decided to use the SQL option and sqlite, this worked so well we never pursued other options. With these two issues behind us we were able to perform a successful set of tests with SimpleSAMLphp on DevCloud.

With SimpleSAMLphp working we turned our attention to integrating it with Drupal using the simplesamlphp_auth module. This was as simple as installing, enabling, and configuring the

module to use the working SimpleSAMLphp Service Provider. The simplesamlphp_auth module can automatically provision users into the Drupal site at the time of login so that eliminated the need for Cisco to batch provision users. However, Cisco wanted to populate the Drupal user profiles with more information than the simplesamlphp_auth module handles. Since we were pressed for time Richard called on the services of Karen Stevenson from Lullibot to produce a submodule for simplesamlphp_auth that allowed us to map additional user attributes from Cisco's Identity Provider into the user's Drupal profile.

Next, Cisco wanted us to layer access control on top of our working identity integration so they could control content visibility based on identity attributes. To make this happen we needed to evaluate the identity attributes that Cisco's IdP was sending and grant or revoke Drupal roles accordingly. Since the simplesamlphp_auth module already had the ability to do basic role assignment based on identity attributes we decided the simplest way to achieve our goal was to process the identity attributes from the IdP using SimpleSAMLphp's authentication processing filter capabilities. At login time these authentication processing filters would build a set of calculated attributes that the simplesamlphp_-auth module could use to assign or revoke Drupal roles. This approach provided a good balance of automation and customization.

Cisco was so pleased with the results they asked Cloudbiz to do another collaboration site for their distributors. So far, Cloudbiz and I have deployed two SAMLized Drupal-based collaboration sites for Cisco.

For technical details and step-by-step instructions visit Acquia's technical guide for configuring SAML support in Drupal on DevCloud[3].

[3]Using SimpleSAMLphp with your Acquia Cloud site - https://docs.acquia.com/articles/using-simplesamlphp-acquia-cloud-site (Requires free registration)