Integrating CloudStack in your Organization using Single Sign On

Rohit Yadav

Software Architect

rohit.yadav@shapeblue.com

Twitter: @_bhaisaab

cloud STACK COLLABORATION CONFERENCE

Shape Blue The Cloud Specialists

apachecloudstack open source cloud computing

About Me

- Software Architect with ShapeBlue
- Specialise in….
  - 3rd party integrations and features in CloudStack
  - KVM, API, DB, Upgrades, SystemVM, Build system, various subsystems
- Contributor and Committer since 2012
- Author and maintainer of CloudMonkey
- Rides castorboards like a boss™
- Loves to experiment with woodwinds such as Bansuri, Concert Flutes. Rusty beatboxing skills

About ShapeBlue

"ShapeBlue are expert builders of public & private clouds. They are the leading global Apache CloudStack integrator & consultancy"

… and we're hiring!


AcenTek
Ascending Technology
coredesktop
Business Cloud Synergy
თბილისის მერია
TBILISI CITY HALL
eSkyCity
LSP
Trader Media Group
PADDYPOWER.
paragus
SWISS TXT
Ascenty
csg
Tomorrow's Technology Today
sagepay
orange
SCHUBERG PHILIS
pacific interactive
USS
inps
BT
EVRY
cloudera
CSN GROEP
TEAM CYMRU
Klarna
sky
cloudcentral
DSS
interoute
from the ground to the cloud
SUNGARD AVAILABILITY SERVICES
TOMTOM
CISCO
Vonage
colt
nodilex
IaaS Cloud Computing
Kumo
wateen
جـــو چاهـــو
Virtela
An NTT Communications Company
Penn
University of Pennsylvania
FOUR Js
The Power of Simplicity
Flemish Government
control circle
The Datacentre People
M5 INTERNET HOSTING
EveryWare
eCommunications
ASG
your it
GLOBAL
IP SOFT
SURFBOXX
IT-SOLUTIONS
Guzool

Agenda

- CloudStack in your organization
- Authentication and Authorization in CloudStack
- SAML2 SSO Plugin for CloudStack
- Design and Implementation
- Assumptions and limitations
- Real world usage and example
- Demo and Q&A

CloudStack in your organization

- CloudStack provides notion of accounts, users (aliases to an account), domains and roles
- Organization creates and maps users in their user directory services either manually or using LDAP plugin to import users or some custom automation scripts
- Organization may create their own UI/business layer and integrate on unauthenticated port 8096 (default integration port)
- Bypass or proxied authentication using single pre-shared key

Authentication & Authorization in CloudStack

- Authentication: “you are what you say you are”
- Authorization: “you can do what you’re trying to do”
- Existing authentication methods:
  - CloudStack own cookie based authentication
  - Signature/HMAC based authentication (apikey/secretkey)
  - Single pre-shared key based authentication
  - Authentication bypass on integration port (default: 8096)
- Static Role based Authorization: Admin, Resource Admin, Domain Admin, User. Statically set in command.properties file

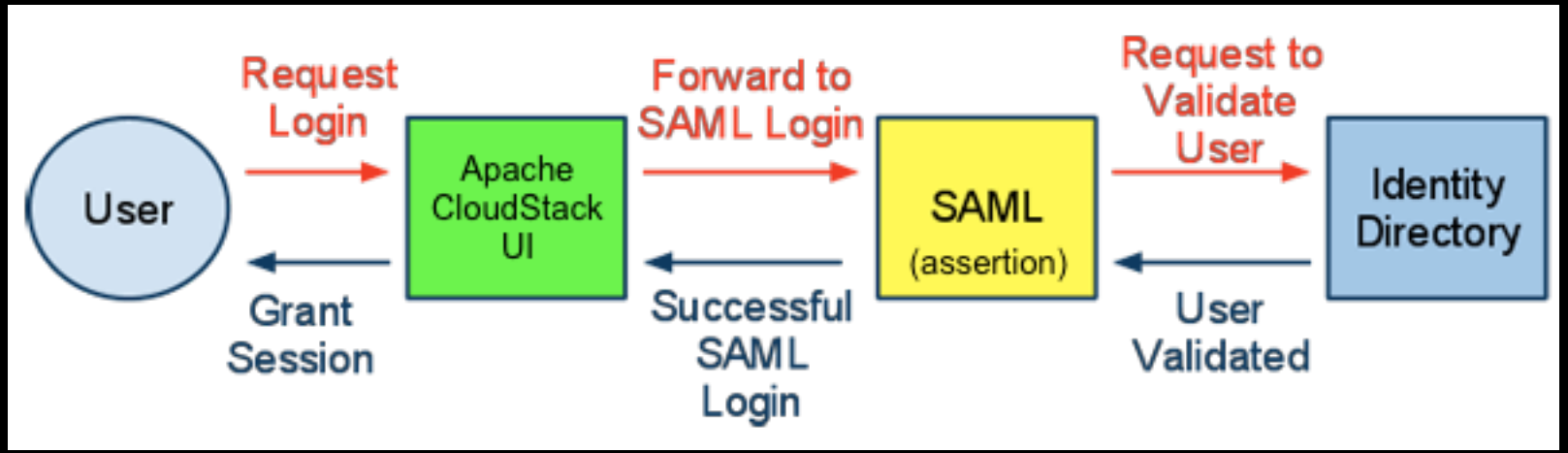
Single Sign On in your Organization

- SSO is widely used in many small to large organizations
- Typical user management using a directory service such as LDAP or Microsoft AD
- Common use-case: Authentication using SAML Identity Provider server backed by LDAP/AD
- SAML server provider means to authentication (protocol) and LDAP/AD providers means to user/group management (identity)

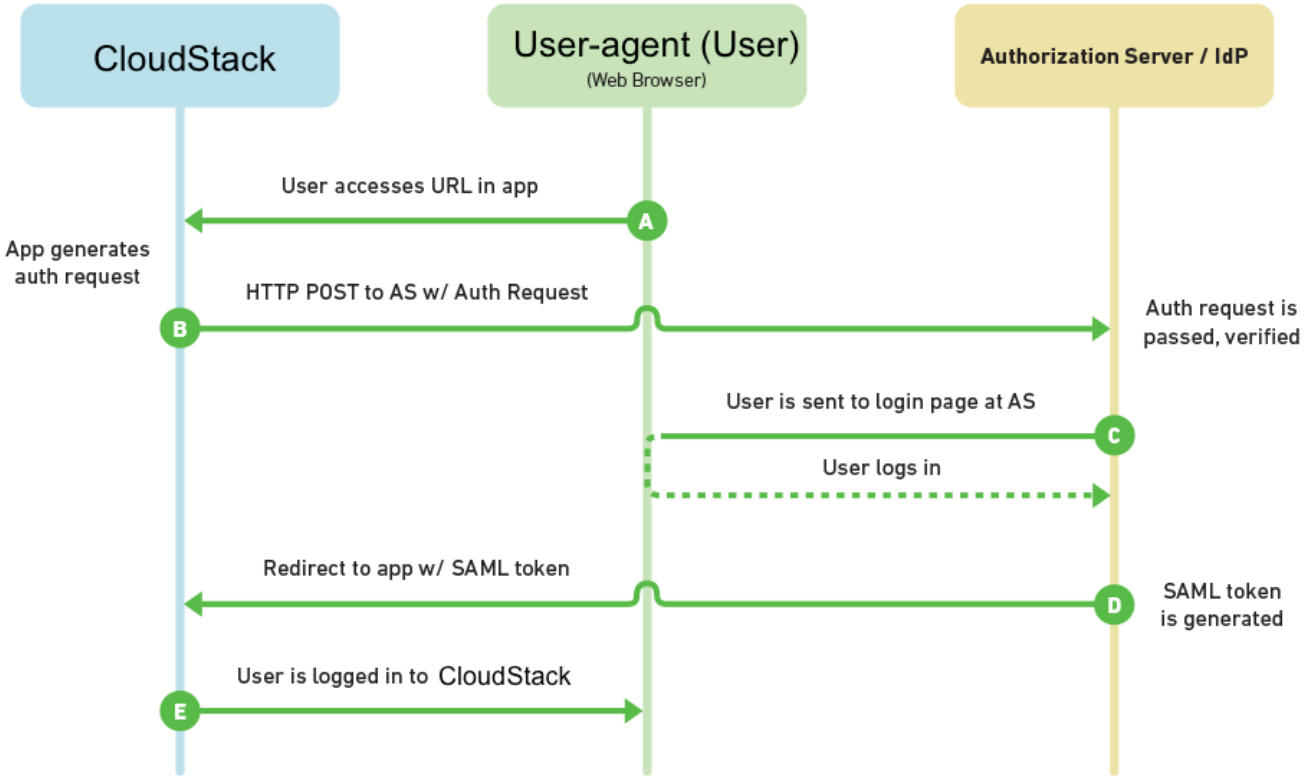
SAML Concepts

- Service Provider: Your application that communicates with IdP in order to obtain information about the user it interacts with
- Identity Provider: Entity that knows how to authenticate users and provide information about their identify to service providers or relaying parties
- Agent: User or the browser
- Metadata: XML describing IdP or SP used to establish federation
- Bindings: Mechanism used to delivery SAML messages such as HTTP-POST, HTTP-Redirect etc.

How SAML works?



SAML 2.0 Flow


CloudStack
User-agent (User)
(Web Browser)
Authorization Server / IdP
User accesses URL in app
A
App generates auth request
HTTP POST to AS w/ Auth Request
B
Auth request is passed, verified
User is sent to login page at AS
C
User logs in
Redirect to app w/ SAML token
D
SAML token is generated
User is logged in to CloudStack
E

CloudStack SAML2 Plugin SSO Process

- Admin imports or adds user. Enables SAML SSO for a user account against a specific IdP server.
- User visits CloudStack login page, selects a IdP server from the dropdown (or local login, in case of CloudStack's own username/ password based login)
- User is taken to the IdP login page, on successful authentication browser is redirected to CloudStack
- CloudStack SAML2 plugin checks if the authenticated user exists in CloudStack for the IdP server and is allowed to proceed
- User is logged into CloudStack or is shown an error message

SAML2 SSO CloudStack Plugin features

- Support for multiple IdP servers and federated SSO
- Pre-authorization based workflow
- UI enhancements
- Supports both file and URL based metadata discovery
- Switching across multiple SAML enabled domain/accounts
- Tested and works with Shibboleth IdP server, Microsoft AD with SAML SSO, OneLogin, OpenFiede etc.

Assumptions and Limitations

- CloudStack's SAML2 SP Plugin requires pre-authorization i.e. user account need to be added (if they don't exist) and authorized to allow SAML based SSO, by an admin or domain admin, prior to SSO
- SSO is SP initiated, IdP provider cannot initiate SSO. This means users need to start the SSO process from CloudStack's screen

Configuring/Using CloudStack SAML2 Plugin

- Available with CloudStack 4.5.2+
- Global settings (Demo)
- Configuring IdP server to allow CloudStack SP, using SP Metadata
- Both file and URL based

Real World Usage and Examples

- USP's CloudStack cloud uses SAML2 SSO Plugin
- CAFe federated SSO login tested
- Dev-test environments know to be running successfully against Microsoft ADFS
- Upcoming Brazilian universities to use federated SAML2 based SSO, CAFe compliant

Thank You

Questions?