Integrating Identity with LDAP for SUSE CaaS Platform

Rodolfo Bejarano
Solutions Engineer
rbejarano@suse.com

Michael Carrington
Solutions Engineer
mcarrington@suse.com
Agenda

• What is SUSE Containers-as-a-Service Platform?
• How do we integrate identity with LDAP?
• Demo
• Q&A
SUSE CaaS Platform

Speed application delivery to improve business agility

SUSE CaaS Platform is an enterprise-class container management solution that enables IT and DevOps professionals to more easily deploy, manage and scale container-based applications and services.
Achieve Faster Time-to-Value

With everything you need to quickly offer container services

- Kubernetes container orchestration
- Container runtime and Image registry
- SUSE Micro OS Container operating system
- Complementary technologies
Achieve Faster Time-to-Value

With everything you need to quickly offer container services

<table>
<thead>
<tr>
<th>Curated Package</th>
<th>SUSE Enterprise Hardening &amp; Support</th>
</tr>
</thead>
</table>
|  • Maintained holistically  
  • Tested to ensure interoperability |  • Meet internal compliance standards  
  • Reliable, scalable and robust |
Exceptional Platform Operator Experience

What’s new in SUSE CaaS Platform 3+?

Rapid delivery of new features

• External Authentication support
  • LDAP
  • OIDC
• NGINX Ingress Controller
• Update to Kubernetes 1.10.11
Coming Soon to SUSE CaaSP version 4+

• Container Host OS
  • Codebase: SUSE Linux Enterprise 15
  • Container isolated via virtualization (Kata containers)
  • Monitoring (Prometheus)

• Orchestration
  • Network options (Cilium as first plugin)
  • Kubernetes 1.11
Ready Today!

SUSE CaaS Platform Partners
Why Would We Want to Integrate Identity with LDAP?

• Environment isolation without the need for deploying multiple clusters
• Seamless role assignment
• Incorporate Single Sign-On (SSO) benefits
• Avoid the need for management of another user repository
• Security teams will appreciate it
How Do We Integrate Identity with LDAP?
Prerequisites

• Working LDAP server ✓
  • An LDAP server and the credentials for a user/service account with permissions to search the directory.

• Working SUSE Container-as-a-Service Platform cluster ✓
• …And you are done! Ready to configure it! ✓
LDAP Connectors

Name

Ldap.geeko.land
### New LDAP Connector

**Name**

Ldap.geeko.land  
Name shown to user when selecting a connector

**Server**

**Host**

ldap.geeko.land  
Host name of LDAP server reachable from the cluster

**Port**

389  
The port on which to connect to the host (e.g. StartTLS On: 385 , StartTLS Off: 636 )

**StartTLS**

On  
When enabled use StartTLS otherwise TLS will be used

**Certificate**

Upload the certificate of the root CA that issued the LDAP server certificate

Choose File  
No file chosen
Velum LDAP server configuration

**DN**

`cn=administrator,dc=geeko,dc=land`

Bind DN of user that can do user searches

**Password**

`....................`

Password of the user

**User Search**

**Identifying User Attribute**

`cn`

Label of LDAP attribute users will enter to identify themselves (e.g. `username`)

**Base DN**

`ou=people,dc=geeko,dc=land`

BaseDN where users are located (e.g. `cn=users,dc=example,dc=com`)

**Filter**

`(objectClass=inetOrgPerson)`

Filter to specify type of user objects (e.g. `(objectClass=person)`)

**User Attribute Map**

**Username**

`cn`
Velum LDAP server configuration

**Email**

Attribute containing email of users

**Name**

Attribute used as username used within OIDC tokens

**Group Search**

**Base DN**

cn=group, dc=geeko, dc=land

BaseDN where groups are located (e.g. `cn=groups, dc=example, dc=com`)

**Filter**

(objectClass=posixGroup)

Filter to specify type of group objects (e.g. `(objectClass=group)`)

**Group Attribute Map**

**User**

cn

Attribute to map as user (e.g. `uid`)

**Group**

memberUid

Attribute identifying membership (e.g. `member`)

**Name**

cn

Attribute to map as name (e.g. `name`)

Save  Cancel  Test Connection
Once Your Config Is Ready…You Can Login

Log in to dex

Log in with LDAP

Log in with ldap.geeko.land
And You Get a kubeconfig!
But...You Need Rights

Authenticate with Kubernetes
You can return to the dashboard once you have prepared your kubeconfig file

Option 1: Download your kubeconfig file
You will see a download dialog that will allow you to download your kubeconfig file. Please, accept it and save it in a known location.
You can refer to it using kubectl by setting the KUBECONFIG environment variable, like KUBECONFIG=/~/Downloads/kubeconfig kubectl get nodes.
Alternatively, you can also save it to your home in `~/.kube/config`, `kubectl` will automatically read this file without the need to specify the KUBECONFIG environment variable.
Click here if the download has not started automatically.

Option 2: Manually configure kubeconfig file
You can manually configure a client by running these commands:

```
# Create a file containing the Kubernetes API CA Certificate
echo "\"LS0tLS1CRUdJTiBDRUZExI10g\" | base64 -d > ~/.kube/caas-ca.crt

# Create the cluster entry in the ~/.kube/config file
kubectl config set-cluster caasp
  --server=https://caasp-master.caasp.geeko.land:6443

# Create the User entry in the ~/.kube/config file
kubectl config set-credentials "rbejarano@suse.com"
  --server=https://caasp-master.caasp.geeko.land:6443

# Create and use the cluster context
kubectl config use-context "caasp-rbejarano@suse.com" --cluster caasp --user="rbejarano@suse.com"
```

SUSE CaaS Platform 3.0.0 © SUSE Linux 2019
Role Based Access Control (RBAC)

- In enterprise settings, access might be based on the job function or role of the user
- Users authenticate themselves to the system
- (Some) Users can activate one or more roles for themselves
SUSE CaaS Platform 3

RBAC Examples

Cluster-Admin
- Operate the infrastructure
- Block access to the infrastructure level
- Allow developers to interact with Kubernetes

Cluster-Member
- Full access for my team to manage the application
- No access to other teams’ work
- No access from other teams to our work

Manager
- Check the usage
- Have an overview of resources
Cluster-Admin Role

Leap15:/home/rodolfo # kubectl describe clusterrole cluster-admin
Name: cluster-admin
Labels: kubernetes.io/bootstrapping=rbac-defaults
PolicyRule:

<table>
<thead>
<tr>
<th>Resources</th>
<th>Non-Resource URLs</th>
<th>Resource Names</th>
<th>Verbs</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>.</em></td>
<td></td>
<td>[]</td>
<td>[*]</td>
</tr>
<tr>
<td>[*]</td>
<td></td>
<td>[]</td>
<td>[*]</td>
</tr>
</tbody>
</table>

Leap15:/home/rodolfo # kubectl describe clusterrolebinding ldap-administrators
Name: suse:caasp:ldap-administrators
Labels: <none>
Role:
  Kind: ClusterRole
  Name: cluster-admin
Subjects:
  Kind  Name          Namespace
  ----   ----          --------
  Group  Administrators
Cluster-Member Role

Leap15:/home/rodolfo # kubectl describe clusterrole cluster-member
Name: cluster-member
Labels: kubernetes.io/bootstrapping=rbac-defaults
Annotations: rbac.authorization.kubernetes.io/autoupdate=true

<table>
<thead>
<tr>
<th>PolicyRule: Resources</th>
<th>Non-Resource URLs</th>
<th>Resource Names</th>
<th>Verbs</th>
</tr>
</thead>
<tbody>
<tr>
<td>nodes.*</td>
<td></td>
<td></td>
<td>[get list watch]</td>
</tr>
<tr>
<td>persistentvolumes.*</td>
<td></td>
<td></td>
<td>[get list watch]</td>
</tr>
<tr>
<td>storageclasses.*</td>
<td></td>
<td></td>
<td>[get list watch]</td>
</tr>
<tr>
<td>namespaces</td>
<td></td>
<td></td>
<td>[get list watch]</td>
</tr>
<tr>
<td>namespaces/status</td>
<td></td>
<td></td>
<td>[get list watch]</td>
</tr>
<tr>
<td>persistentvolumeclaims</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
<tr>
<td>pods</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
<tr>
<td>pods/attach</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
<tr>
<td>pods/exec</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
<tr>
<td>pods/log</td>
<td></td>
<td></td>
<td>[get list watch]</td>
</tr>
<tr>
<td>pods/portforward</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
<tr>
<td>pods/proxy</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
<tr>
<td>pods/status</td>
<td></td>
<td></td>
<td>[get list watch]</td>
</tr>
<tr>
<td>replicationcontrollers</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
<tr>
<td>replicationcontrollers/s</td>
<td></td>
<td></td>
<td>[create delete deletecollection get list patch update watch]</td>
</tr>
</tbody>
</table>
Cluster-Member Rolebinding

Leap15:/home/rodolfo # kubectl describe clusterrolebinding ldap-users
Name: suse:caasp:ldap-users
Labels: <none>
Role:
  Kind: ClusterRole
  Name: cluster-member
Subjects:
  Kind   Name    Namespace
    ----   ----    ---------
Group  users
Demo Time
Additional Resources

Setting up an LDAP server

External LDAP directory

Internal containerized LDAP directory

Role Management
General Disclaimer
This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of SUSE LLC. in the United States and other countries. All third-party trademarks are the property of their respective owners.