December 10, 2018

OpenShift at USAA

Secrets Management

Ankur Lamba
IAM Technical Architect
USAA Enterprise Security Group

OUR MISSION

The mission of the association is to facilitate the financial security of its members, associates and their families through provision of a full range of highly competitive financial products and services; in so doing, USAA seeks to be the provider of choice for the military community.

THE USAA STANDARD

- Keep our membership and mission first
- Live our core values: **Service, Loyalty, Honesty, Integrity**
- Be authentic and build trust
- Create conditions for people to succeed
- Purposefully include diverse perspectives for superior results
- Innovate and build for the future

Agenda

OpenShift at USAA

Secrets Management Requirements

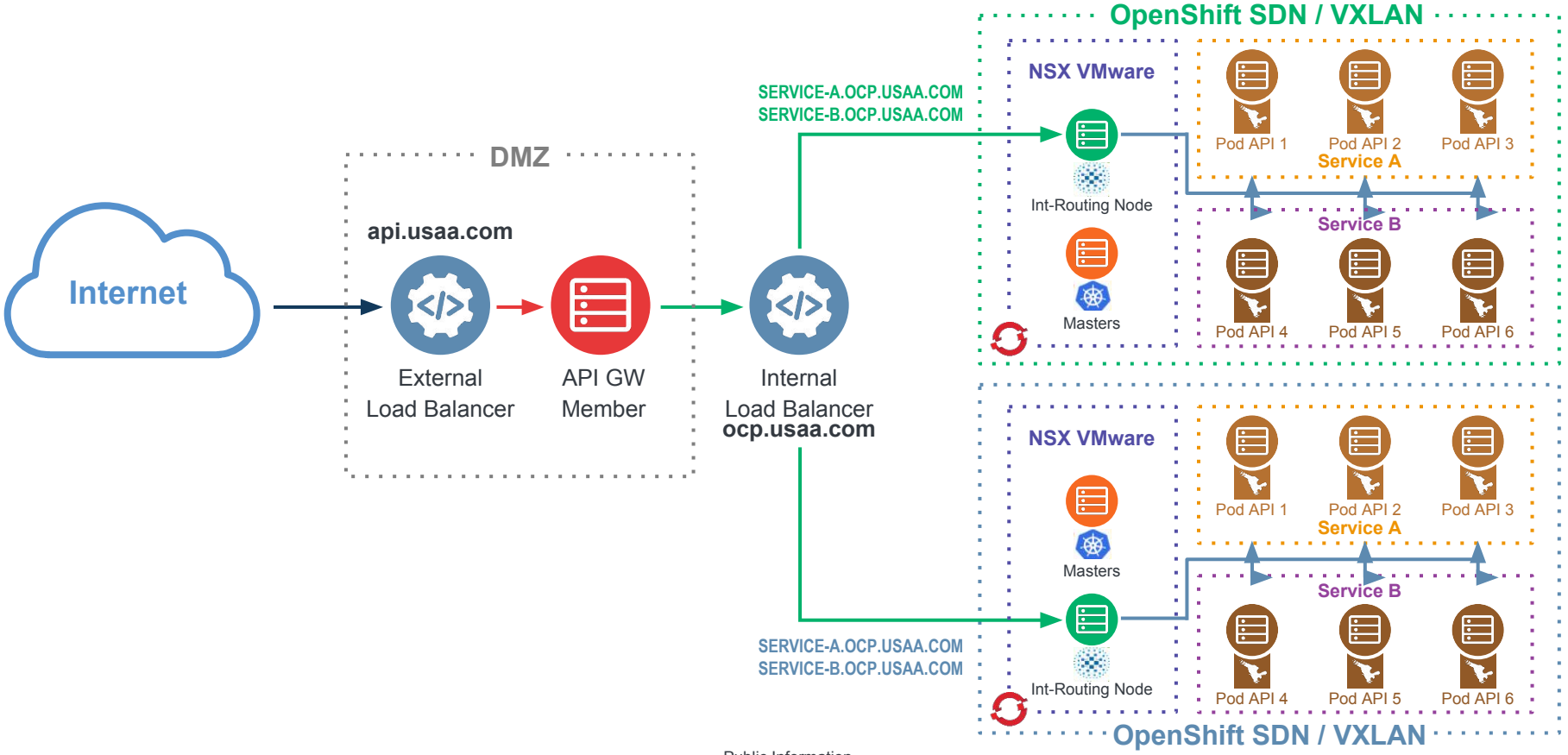
CyberArk for OpenShift

Conjur for OpenShift

Developer’s Perspective

Future Enhancements

OpenShift at USAA



Secrets Management Requirements

Highly-Available, Highly Scalable, Vaulting and Management System

Centrally Manage Application Service Accounts, for all Environments

- A Set of an ID and a Password, Referenced via an Alias

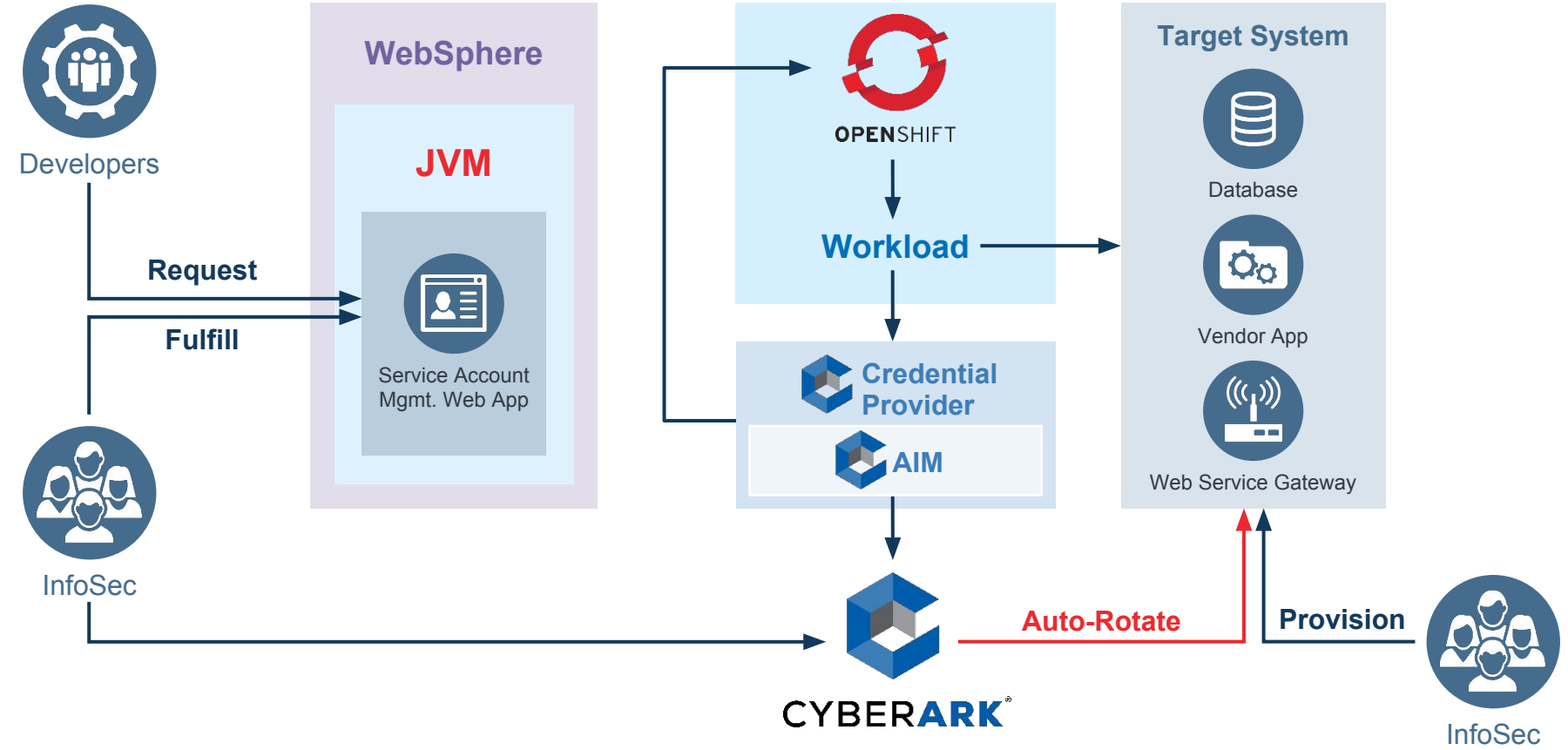
Ability to Rotate Passwords Without Application Downtime

Regional Access to Service Accounts

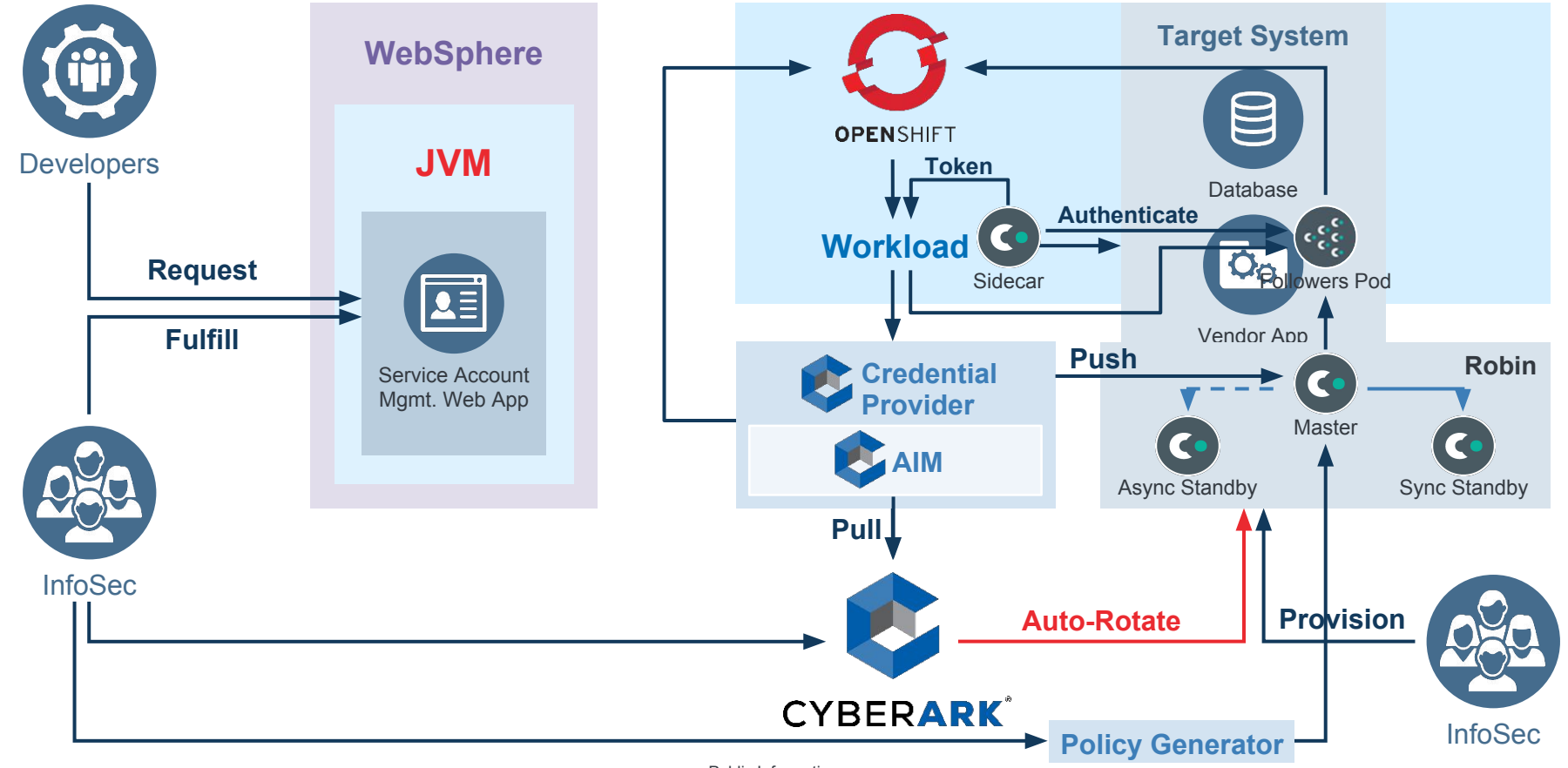
Enforcement at Each Consuming Application Level

Usage Tracking of Every Service Account

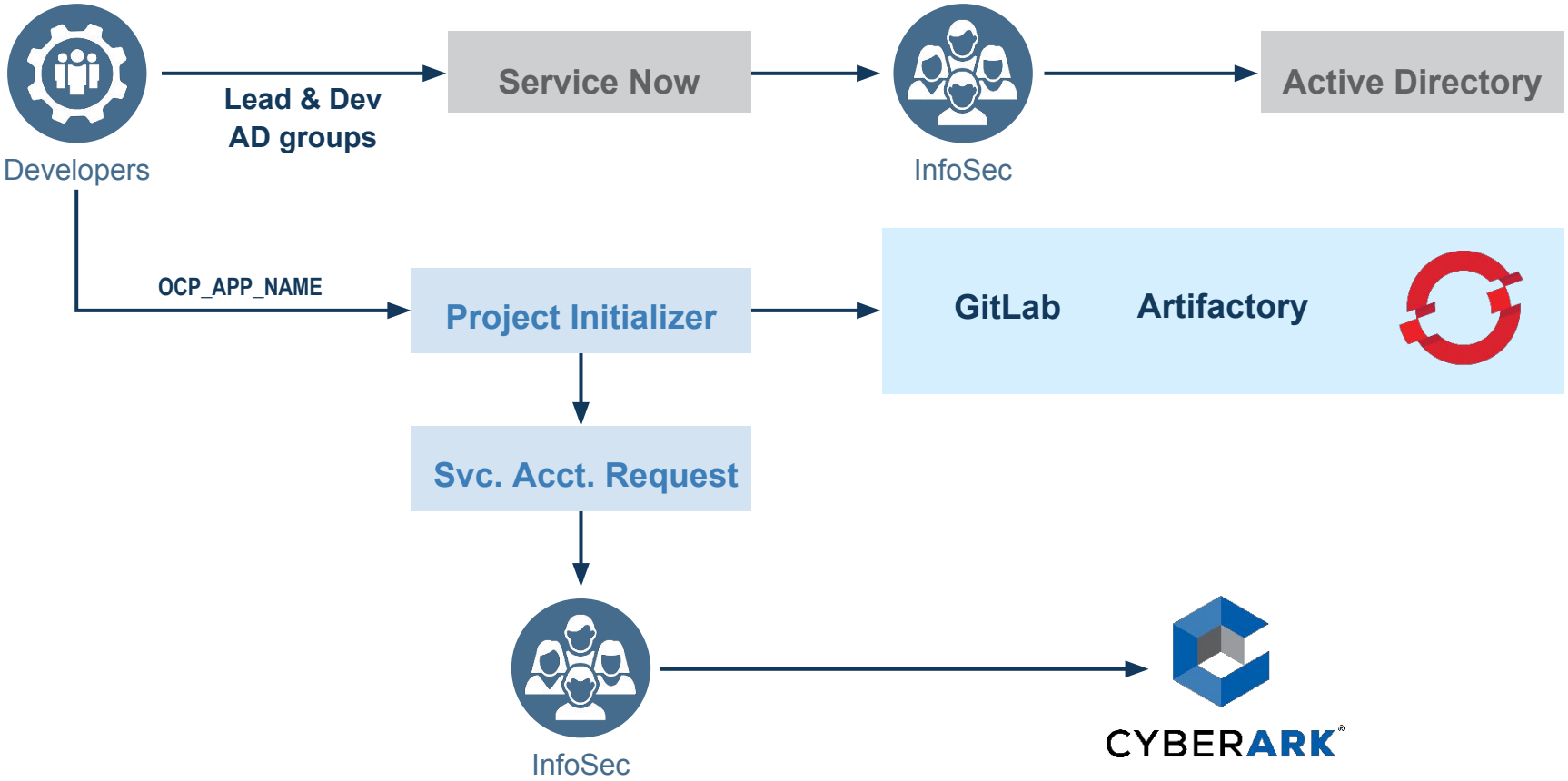
CyberArk for OpenShift



Conjur for OpenShift



The Foundation Tasks



DeploymentConfig.yaml
Conjur Follower Config

```
env:
        - name: CONJUR_MAJOR_VERSION
          value: "5"
        - name: CONJUR_APPLIANCE_URL
          value: https://${RUNTIME_ENV}-conjur-follower.grp-inf-csi-conjur.svc.cluster.local
        - name: CONJUR_ACCOUNT
          value: usaa
        - name: CONJUR_SSL_CERTIFICATE
          valueFrom:
            configMapKeyRef:
              name: ${OCP_APP_NAME}
              key: ssl-certificate
        - name: CONJUR_AUTHN_TOKEN_FILE
          value: /run/conjur/access-token
volumeMounts:
        - mountPath: /run/conjur
          name: conjur-access-token
          readOnly: true
```

DeploymentConfig.yaml
Sidecar Image Config

```
- image: docker.repo.usaa.com/cyberark/conjur-kubernetes-authenticator:0.11.1
      imagePullPolicy: Always
      name: authenticator
      env:
        - name: MY_POD_NAME
          valueFrom:
            fieldRef:
              fieldPath: metadata.name
        - name: MY_POD_NAMESPACE
          valueFrom:
            fieldRef:
              fieldPath: metadata.namespace
        - name: MY_POD_IP
          valueFrom:
            fieldRef:
              fieldPath: status.podIP
```

DeploymentConfig.yaml

Sidecar Conjur Follower Config

```
- name: CONJUR_MAJOR_VERSION
    value: "5"
  - name: CONJUR_APPLIANCE_URL
    value: https://${RUNTIME_ENV}-conjur-follower.grp-inf-csi-conjur.svc.cluster.local
  - name: CONJUR_AUTHN_URL
    value: https://${RUNTIME_ENV}-conjur-follower.grp-inf-csi-conjur.svc.cluster.local/authn-k8s/ocp
  - name: CONJUR_ACCOUNT
    value: usaa
  - name: CONJUR_AUTHN_LOGIN
    value: host/conjur/authn-k8s/ocp/apps/${OCP_APP_NAME}/*/*
  - name: CONJUR_SSL_CERTIFICATE
    valueFrom:
      configMapKeyRef:
        name: ${OCP_APP_NAME}
        key: ssl-certificate
  volumeMounts:
    - mountPath: /run/conjur
      name: conjur-access-token
  volumes:
```

Future Enhancements

- Shared Mount Volume Across Pods
- Auto Generate Conjur Config Sections in DeploymentConfig Template
- Auto Generate Conjur Policy at Secret Sync
- Highly Available Synchronizer
- Highly Scalable Synchronizer
- Metadata Sync and Metadata Aware Sync
- Secretless Broker (www.secretless.io)

Q&A and Contact Info

QUESTIONS

Ankur Lamba
ankur.lamba@usaa.com