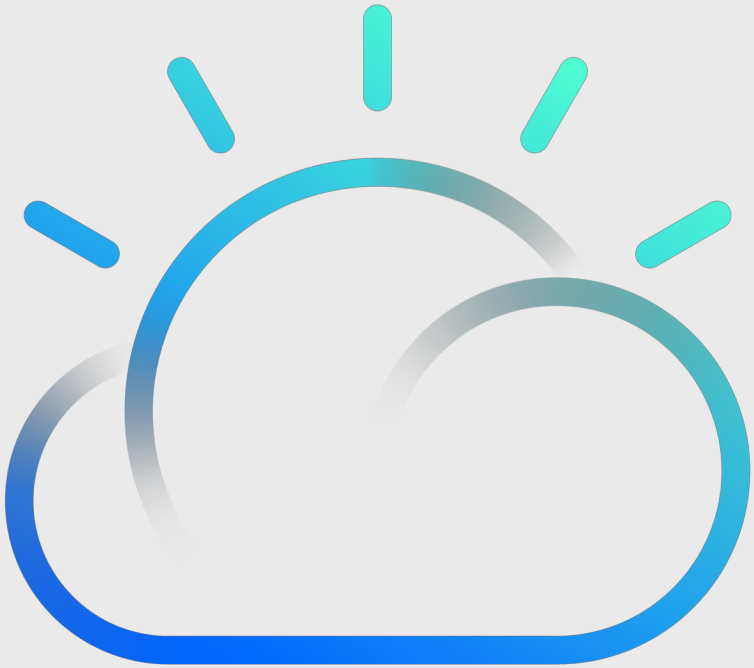
IBM

# IBM Cloud Private Security



IBM Cloud

# Agenda

- **Key Security Scenarios**
- Awareness and Training - Penetration Testing
- Identification and Authentication - Access Control
- System and Information Integrity
- System and Communications Protection
- Audit and Accountability
- What’s New in IBM Cloud Private Security

# Key security scenarios

- Standards-based security control framework: NIST
- Support open standards for various security controls: OIDC, OAuth, LDAP
- Ease of integration with client's enterprise security infrastructure
- Enable forensic analysis
- Support industry specific requirements: financial, federal, healthcare
- Industry leading security capability for containerized applications
- Support both Kubernetes and Cloud Foundry in one framework
- Provide both platform and application security

# Security Control Framework – based on NIST 800-53

Client owns enabling and management of ALL security controls for ICP. IBM provides security capabilities within ICP for some of these security controls that clients can use to meet this goal.

**Data Governance**

- Media protection
- Awareness & training
- Privacy authorization
- Physical and environmental Protection planning
- Contingency planning
- Personnel security
- Individual participation

**Operational Security**

- Audit and accountability
- Configuration management
- Incident response
- Maintenance
- Systems and services acquisition
- Penetration testing
- Security operations center

**Technical Security**

- Access control
- Identification and authentication
- Authorization and monitoring
- Program management
- Risk assessment
- System protection
- Communications protection
- System and information integrity

# Agenda

- Key Security Scenarios
- **Awareness and Training - Penetration Testing**
- Identification and Authentication - Access Control
- System and Information Integrity
- System and Communications Protection
- Audit and Accountability
- What’s New in IBM Cloud Private Security

# Secure Engineering

IBM takes security seriously and has separate processes for handling it

- All IBM personnel are required to have annual Cyber Security Training
- IBM Secure Engineering education available to all developers

Application scans incorporated into development process:

- AppScan source (or Zap for GO) for static code scans
- AppScan Web for web application scans

Penetration testing performed for every IBM Cloud Private release

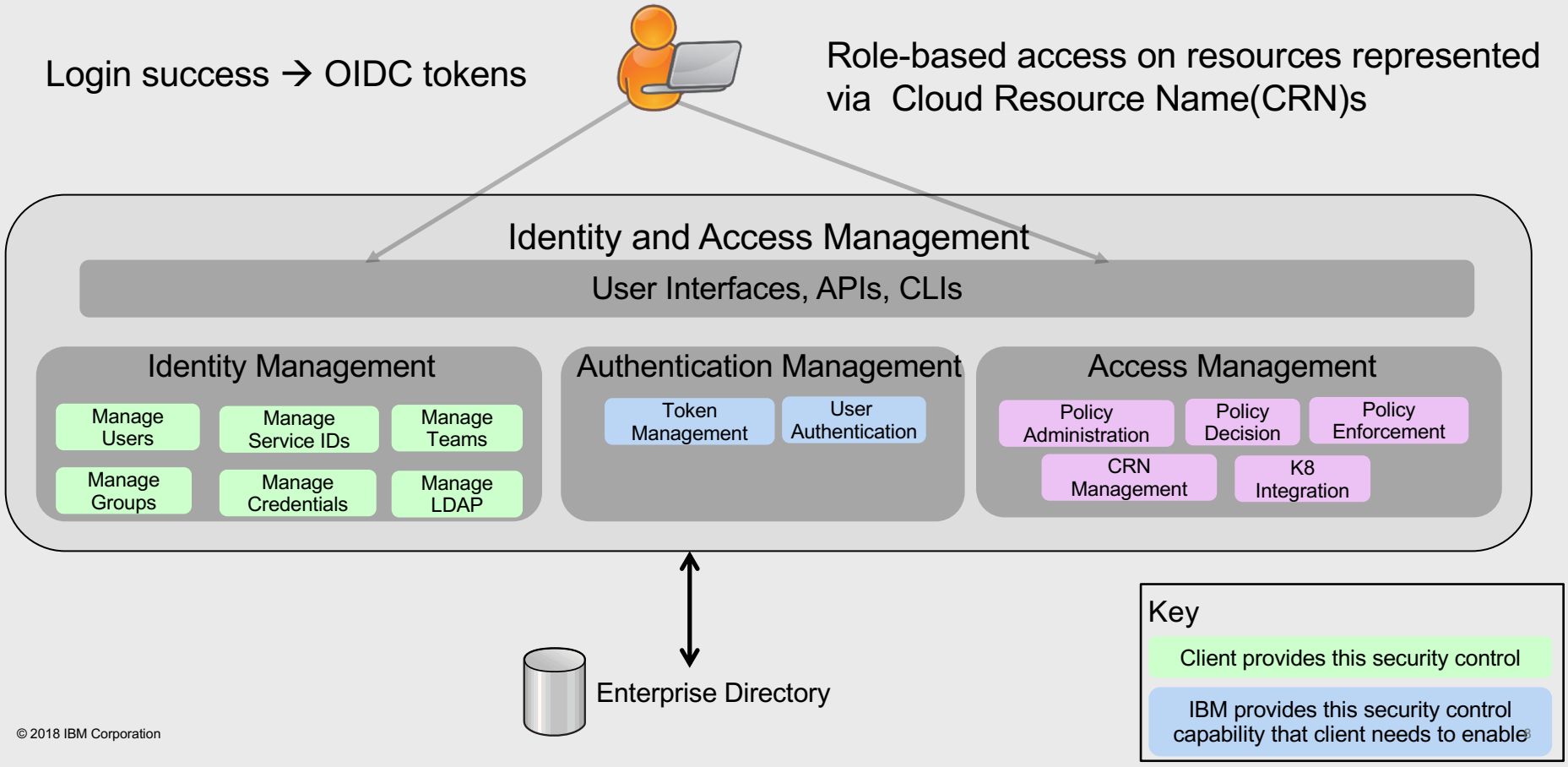
IBM PSIRT process used for handling application security vulnerabilities. Subscribe to get notifications here:

https://www.ibm.com/blogs/psirt/

# Agenda

- Key Security Scenarios
- Awareness and Training - Penetration Testing
- **Identification and Authentication - Access Control**
- System and Information Integrity
- System and Communications Protection
- Audit and Accountability
- What’s New in IBM Cloud Private Security

# Identity and Access Management (IAM)



# Supported User Registries

- IBM Tivoli Directory Server
- IBM Lotus Domino
- IBM SecureWay Directory Server
- Novell eDirectory
- Sun Java™ System Directory Server
- Netscape Directory Server
- Microsoft Active Directory
- Custom

# Identification and Authentication

- OpenID Connect provider in Liberty profile is used to authenticate users
- Integrates with client's enterprise LDAP
- Users and groups are imported into the ICP platform for authorization purposes
- Client owns identity lifecycle of all users in the enterprise directory
- One local user with super admin access to bootstrap

# Access control

Role-based access control based on **teams**

- A '**team**' is a logical grouping of resources, users, and user groups
- Teams can be restricted to all resources within a namespace

Users and user groups are assigned roles within a team that gives them permissions associated with each assigned role on resources within this team

Access control gateway enforces role based access control for all registered services

Service can also invoke the Authorization API to enforce role based access control

# IBM Cloud Private roles

| Roles | Description |
|---|---|
| Cluster administrator | Complete access for all operations for ICP platform. |
| Viewer | Read-only access. Assigned by default to users when they are added to a team. |
| Editor | Read and edit access to team resources. |
| Operator | Read, edit, and create access to team resources. |
| Administrator | Add, update, view, and delete access to team resources. |

# Access control for IBM Cloud Private APIs

To use any ICP API, you need access to an ICP token which must be added to the header of the API

API documentation:

- https://www.ibm.com/support/knowledgecenter/SSBS6K_3.1.1/apis/cfc_api.html

# Agenda

- Key Security Scenarios
- Awareness and Training - Penetration Testing
- Identification and Authentication - Access Control
- **System and Information Integrity**
- System and Communications Protection
- Audit and Accountability
- What’s New in IBM Cloud Private Security

# Data-in-transit protection

TLS and IPSec are used to provide data-in-transit protection

Management-ingress-controller exports TLS which can be leveraged by APIs using it as a front end

All inter-node data traffic can be encrypted using IPSec without changing any applications

Documentation:

- https://www.ibm.com/support/knowledgecenter/SSBS6K_3.1.1/apis/cfc_api.html

Network / Transport Layer Protection

PROJECT CALICO

A new approach to virtual networking and network security for containers, VMs, and bare metal services, that provides a rich set of security enforcement capabilities running on top of a highly scalable and efficient virtual network

- The calico/node Docker container runs on the Kubernetes master and each Kubernetes node in the cluster
- The calico-cni plugin integrates directly with the Kubernetes kubelet process on each node to discover which pods have been created, and adds them to Calico networking
- The calico/kube-policy-controller container runs as a pod on top of Kubernetes and implements the NetworkPolicy API
- Calico makes use of Layer 3

Calico network policy enforcement ensures that the only packets that flow to and / or from a workload are the ones the developer expects

# Security with Istio

- Free developers to focus on security at the application level
- Istio manages authentication, authorization, and encryption of service communication at scale
- Service communications are secured by default with little or no changes to the application
- Via integration with the platform secure pod-to-pod or service-to-service communication at the network AND application layers

# Network security

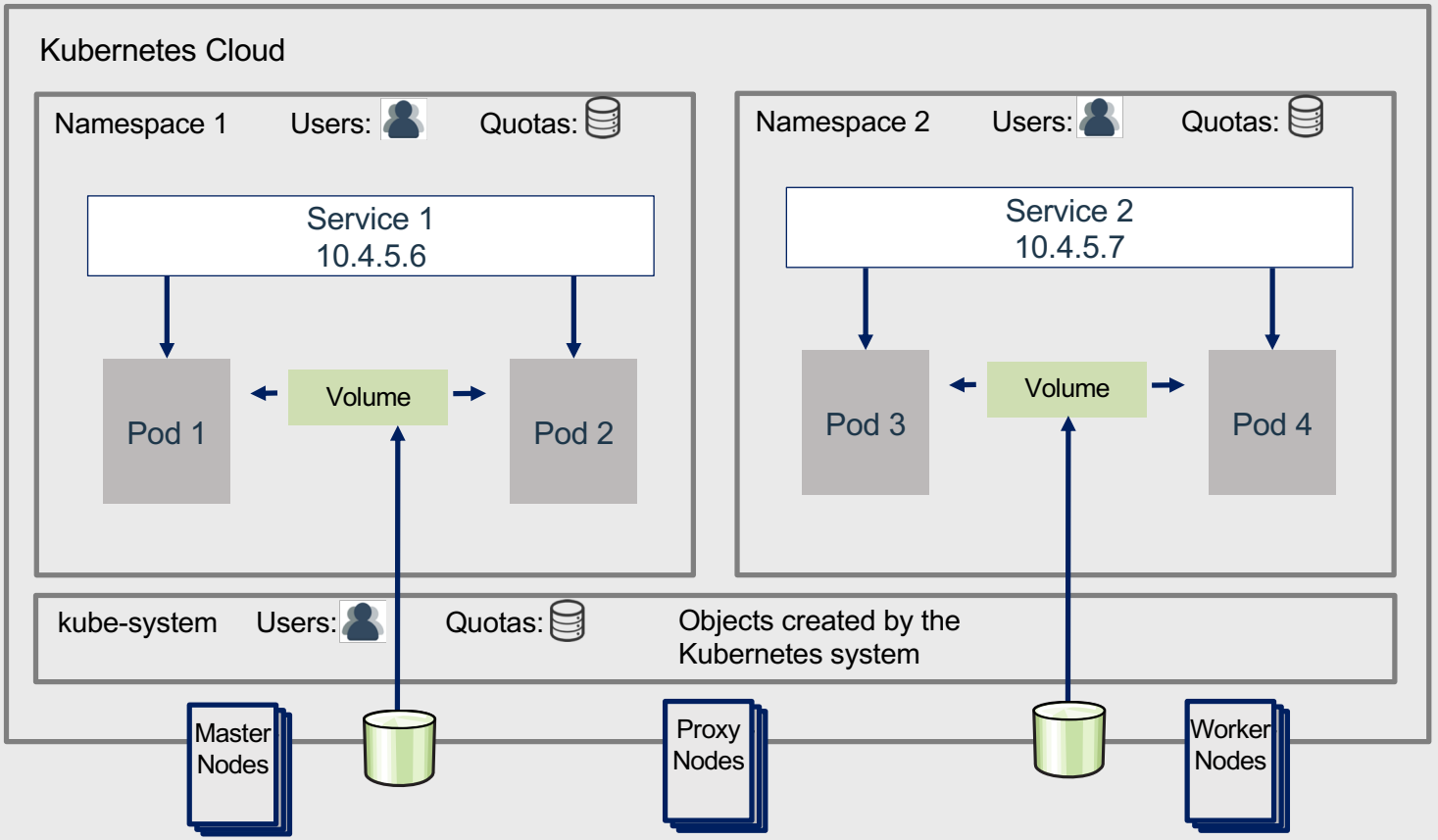
Calico-based configuration of network connectivity:

- Isolated subnet for each project inside an IBM Cloud Private cluster
- Fine grained control over the sharing of objects within a single namespace

# Agenda

- Key Security Scenarios
- Awareness and Training - Penetration Testing
- Identification and Authentication - Access Control
- System and Information Integrity
- **System and Communications Protection**
- Audit and Accountability
- What’s New in IBM Cloud Private Security

# One cloud – isolation across teams




Set quotas for these categories in a namespace:

- Compute
- Storage
- Object count (pods, services, PVC, …)
- Scope

# Private image repository

Built-in storage for Docker images

## Bundled images

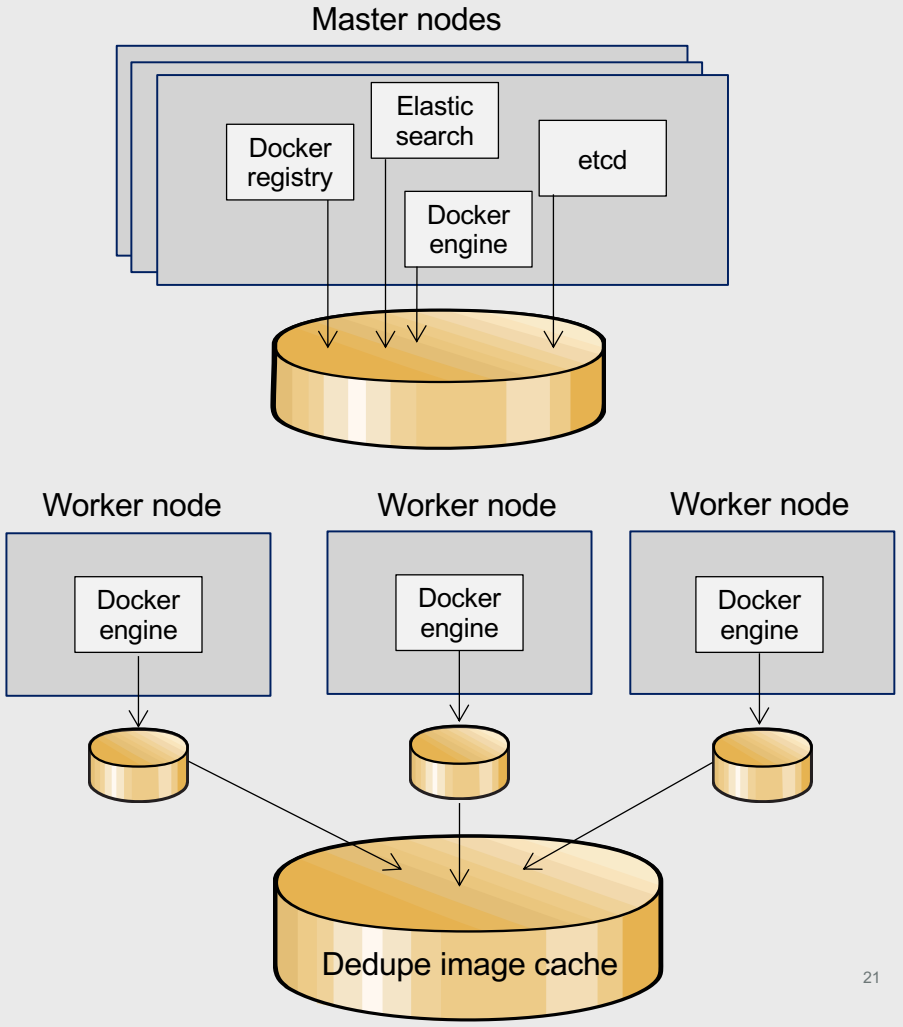
Import Docker images from bundle into private registry, or import any Docker image to deploy across nodes.

## Secure access

Add only approved images so developers have trusted, validated images.

Command to deploy pods to access private image repo:

```
kubectl get serviceaccounts default -o json | jq
'del(.metadata.resourceVersion)' | jq
'setpath(["imagePullSecrets"];[{"name":"admin.registrykey"}])'
| kubectl replace serviceaccount default -f -
```



# Vulnerability assessment

# Data at rest protection

Any ICP state must be protected by using file system-level or block device-level encryption, such as Kubernetes:

- Kubernetes etcd (`/var/lib`)
- Image manager (`/var/lib/registry`)
- Other ICP services (`/var/lib/icp` and `/opt/ibm/cfc`)

All ICP secrets are accessible only to users who have **admin** role for the ICP console or operating system level admin access.

# Agenda

- Key Security Scenarios
- Awareness and Training - Penetration Testing
- Identification and Authentication - Access Control
- System and Information Integrity
- System and Communications Protection
- **Audit and Accountability**
- What’s New in IBM Cloud Private Security

# Security:  Audit Logging

Kubernetes audit logs are used for tracking and storing data that is related to your IBM Cloud Private usage. Audit policies are used to define the rules for the type of data to be saved in the audit logs. IBM Cloud Private uses the default Kubernetes audit policy. For more information about the default Kubernetes audit policy, see https://kubernetes.io/docs/tasks/debug-application-cluster/audit/ .

By default, Kubernetes audit logs are unavailable in IBM Cloud Private. To generate these logs, set the auditlog_enabled parameter to true in the /<installation_directory>/config.yaml file. See Kubernetes settings.

The log files are saved in /var/lib/icp/audit folder.

# Agenda

- Key Security Scenarios
- Awareness and Training - Penetration Testing
- Identification and Authentication - Access Control
- System and Information Integrity
- System and Communications Protection
- Audit and Accountability
- **What's New in IBM Cloud Private Security**

# Features of IBM Cloud Private Security

Role-Based Access Control (RBAC)

- For Helm repos and individual charts within a repo
- Control which teams have access to which charts, limiting who can deploy, update, and delete your most critical applications.

Use the IBM Cloud Private CLI to manage Kubernetes Secret passwords

- For secure communications to key services in the IBM Cloud Private platform.
- Example: set your own password for the built-in MongoDB service that stores authorization and authentication information.
- Set up password rules that ensure only strong passwords are used.

# Features of IBM Cloud Private Security (continued)

Audit logging of authentication and authorization actions on your system.

Service IDs and Service API Keys

- To better control which programs can access services running on your platform and to customize their access privileges.

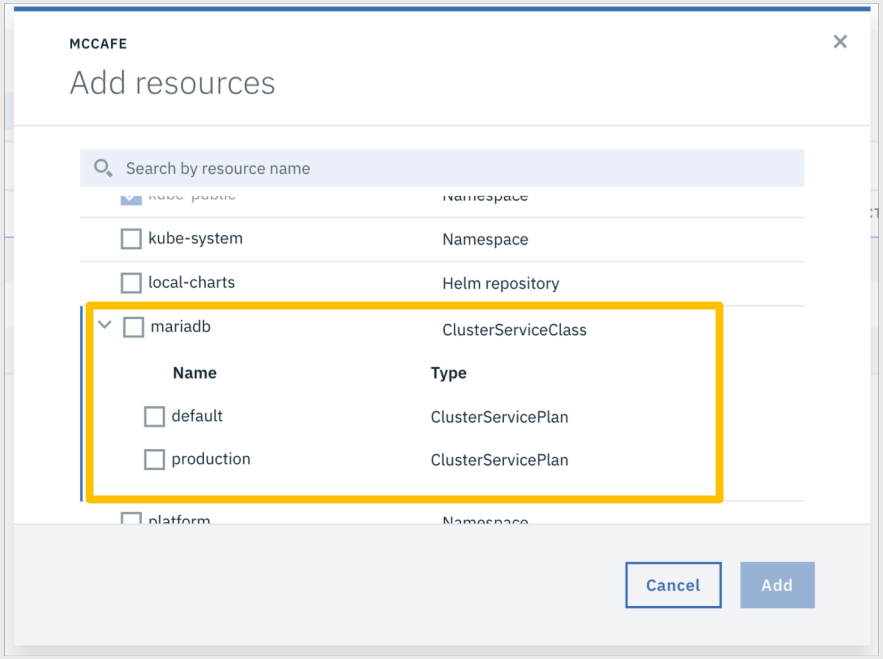
End-to-end TLS encryption for the ELK stack (when enabled)

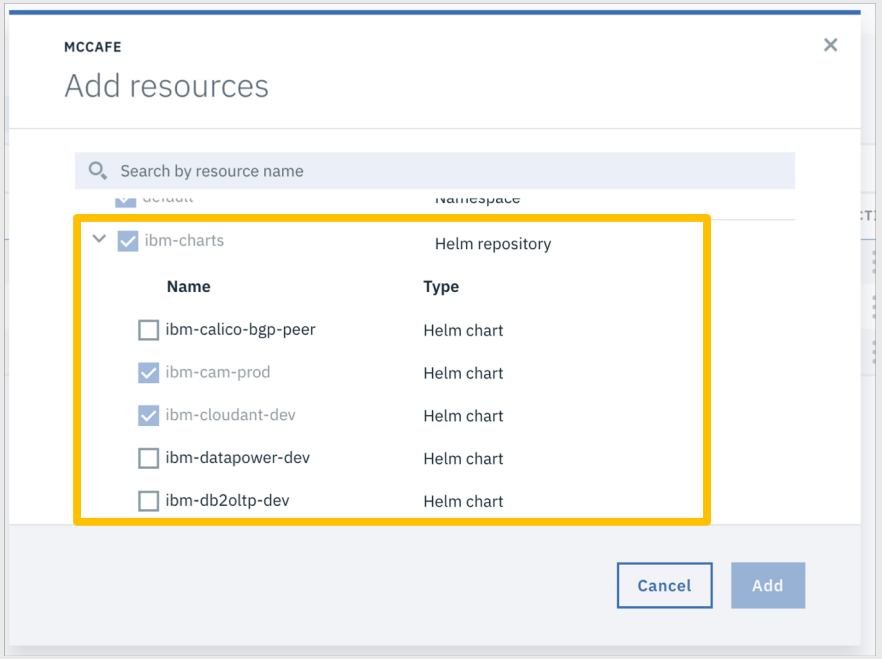
- All data passed between the ElasticSearch, Logstash and Kibana components is encrypted and secured with PKI-based authentication.

# Finer grained RBAC

| Role | Permissions |
|---|---|
| Cluster admin | Permitted to view all routes |
| Admin | *Not permitted* to view Dashboard, Nodes, and Pod Security |
| Editor | *Not permitted* to view Dashboard, Nodes, Authentication, Pod Security, Teams and logs |
| Operator | *Not permitted* to view Dashboard, Nodes, Authentication, Pod Security & Teams |
| Viewer | *Not permitted* to view Dashboard, Secrets, Nodes, Authentication, Pod Security, Teams and logs |

# Team resources




**ClusterServicePlan** and **Helm Chart** can be added as a Team resource.

# Team resources

These team resources are nested:

- Helm charts
- Helm repos
- Cluster Service Classes
- Cluster Service Plans

- If a user selects a **helm repo**, all charts within it are added to the team
- If a user selects a **ClusterServiceClass**, all plans are added to the team
- User can select/unselect individual charts/plans **while initially adding the team resources**
- The only way to **update** the nested selection is to remove the the nested team resource and re-add them with the new selection
- Only the top level resource is included in the search. The user cannot search for items in the nested table.

# Service ID

Identifies a service or application similar to how a user ID identifies a user

Can be used to enable an application outside of IBM Private Cloud to access IBM Private Cloud services

Assign specific access policies to the service ID that restrict permissions for using specific services

Create a Service API Key to authenticate services in IBM Cloud Private

Service IDs are not tied to a specific user

- If a user leaves an organization and is deleted from the account, the service ID remains ensuring that your application or service stays up and running.

# Service policy

Key points about service policies:

- Controls the level of access to a service
- You assign service policies to a service ID
- Access policies associated with a service ID enable specific actions that can be taken when that service ID is used to access a specific service

A single service ID can have multiple policies assigned that define the level of access allowed when accessing multiple identity and access-enabled services

You can assign roles to the service instances of a service

**Important**: If you delete or edit an existing policy for a service ID currently being used, that action may cause a service interruption.

# Service API key

An application programming interface key (API key) is a unique code that is passed in to an application programming interface (API) to identify the calling application or user

The API key often acts as both a unique identifier and a secret token for authentication

The API key generally has a set of access rights specific to the identity associated with it

You can create API keys that are associated with service ID

# Service ID command list

```
[root@rsun-rhel-bootmaster01 demo]# ibmcloud pr iam
NAME:
   ibmcloud pr iam - Group of commands to manage identities and access to resources.
USAGE:
   ibmcloud pr iam command [arguments...] [command options]

COMMANDS:
   roles                     List roles
   service-api-key           List details of a service API key
   service-api-key-create    Create a service API key
   service-api-key-delete    Delete a service API key
   service-api-key-update    Update a service API key
   service-api-keys          List all API keys of a service
   service-id                Display details of a service ID
   service-id-create         Create a service ID
   service-id-delete         Delete a service ID
   service-id-update         Update a service ID
   service-ids               List all service IDs.
   service-policies          List all service policies of specified service
   service-policy            Display details of a service policy
   service-policy-create     Create a service policy
   service-policy-delete     Delete a service policy
   service-policy-update     Update a service policy
   services                  List services
   help

Enter 'ibmcloud pr iam help [command]' for more information about a command.
```



**Note:** First, you need to run the command: ***ibmcloud pr target -n NAME_SPACE***

# Using Service API keys: Generate token

Curl command to generate OIDC token for APIKeys:

***$ curl -k -X POST --header 'Content-Type: application/x-www-form-urlencoded' --header 'Accept: application/json' -d 'grant_type=urn:ibm:params:oauth:grant-type:apikey&apikey=metering-service-apikey&response_type=cloud_iam' 'https://$MASTER_NODE_IP:8443/iam-token/oidc/token'***

*{"expiration":1520666627,"access_token":"eyJraWQiOiIyMDE3MDUxNS0wMDowMDowMCIsImFsZyI6IlJTMjU2In0.eyJyZWFsbWlkIjoiaWFtIiwic3ViX3R5cGUiOiJTZXJ2aWNlSWQiLCJpYXQiOjE1MjA1ODAyMjcsImV4cCI6MTUyMDY2NjYyNywiaXNzIjoiaHR0cHM6Ly9sb2NhbGhvc3Q6NDQzMC9vaWRjL3Rva2VuIiwiZ3JhbnRfdHlwZSI6InVybjppYm06cGFyYW1zOm9hdXRoOmdyYW50LXR5cGU6YXBpa2V5Iiwic2NvcGUiOiJvcGVuaWQiLCJjbGllbnRfaWQiOiJkZWZhdWx0In0.cJs3O2KFMQj7jM2b3p0ieem0qCeL1wxC5WAFPWBVe7jpicvjmLkww7LJyaT45o_ickH3ehoGCDVyaZZdtYmiMKr2CFdAZvCEbpVKeq2KHqsZVWae_ezjUp2aHyPh9MUjyQKmNaI2dinxqQSHZkXH4nLMrDhsL3VUYhTI786m6crhESuhndZnCJq3otKhy6xFg1woCIxp9L3gWPth2f4srS9z1d-ZXP02mtyGZJUUZJeQA84dP6OC5QjJVlE-clIlq_-xDOk4M16vHX8KSPjKhwv2F5gCV32EhZGUUc-PvsRl5SW5xKpyaRP5VGxHEbunu0aPCsA-JtL6ELbi77sagw","token_type":"Bearer","expires_in":86400}*

# Using Service API keys: Introspect token

Curl command to introspect the APIKeys OIDC token:

***$ curl -k -X POST --header 'Content-Type: application/x-www-form-urlencoded' --header 'Accept: application/json' -d 'token=$ACCCESS_TOKEN'  'https://$MASTER_NODE_IP:8443/iam-token/oidc/introspect'***

*{"exp":1520666627,"active":true,"scope":"openid","iss":"https://$MASTER_NODE_IP:8443/iam-token/oidc/token","realmId":"iam","account":{},"iat":1520580227,"client_id":"default","grant_type":"urn:ibm:params:oauth:grant-type:apikey","sub_type":"ServiceId"}*

# Resources

IBM Cloud Blog - IBM Cloud Private v2.1.0.3 Boosts Scalability and Security
https://www.ibm.com/blogs/bluemix/2018/05/ibm-cloud-private-v2103-boosts-scalability-and-security/

IBM Cloud Private Knowledge Center - Configure an LDAP
https://www.ibm.com/support/knowledgecenter/en/SSBS6K_2.1.0.3/user_management/configure_ldap.html

IBM Cloud Private Github - Test Service ID API key
https://github.ibm.com/IBMPrivateCloud/platform-api/wiki/Test-Service-ID---API-key

IBM Cloud Private Github - IAM Service On-boarding
https://github.ibm.com/IBMPrivateCloud/roadmap/blob/master/feature-specs/security/iam-onboarding.md

# Resources (continued)

IBM blueprint: Cloud Security Offerings
https://blueprint-secured.sl.bluecloud.ibm.com/b_dir/blueprint.nsf/url/AB632147?OpenDocument

IBM Cloud - Creating and working with service IDs
https://console.bluemix.net/docs/iam/serviceid.html#serviceids

Vulnerability Advisor comes to your cloud with IBM Cloud Private
https://medium.com/ibm-cloud/vulnerability-advisor-comes-to-your-cloud-with-ibm-cloud-private-38a6afeab302