Red Hat Istio Policy Design

Minuta incontro del 13 maggio 2024 sul disegno e implementazione demo delle policy di network segregation relative al traffico interno sul cluster OCP di collaudo.  
Ho aggiunto le persone presenti nell'invitation della riunione.  
  
Al fine di provare sul cluster di collaudo le istio policy di network segregation così come definite nel documento "Scenario di funzionamento Microgateway" si è provveduto ad installare un'applicazione di esempio sul cluster di collaudo che simulasse la comunicazione attraverso 3 distinti layer (namespace).  
L'ìapplicazione utilizzata è stata l'applicazione Demo di Istio [BookInfo]([https://istio.io/latest/docs/examples/bookinfo/](https://urldefense.com/v3/__https:/istio.io/latest/docs/examples/bookinfo/__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoYxzuUk8$)) adeguatamente modificata per essere distribuita in 3 diversi namespace.  
  
A screenshot of a computer

Description automatically generated  
  
Sul cluster di collaudo è stata installata nella mesh già presente  (non è stato creato un ControlPlane separato perchè 'installazione è di tipo ClusterWide -  vedi note)  
  
A seguito dell'installazione non è stato possibile raggiungere l'applicazione dall'esterno del cluster per la mancanza del VIP dedicato. In attesa che il VIP venisse creato si è generato traffico dall'interno del cluster in modo da proseguire con la verifica delle policy  
  
Di seguito le azioni intraprese:

- creati 3 namespace

  - ossm-bookinfo-fe   
  - ossm-bookinfo-middle   
  - ossm-bookinfo-be

- aggiunti i namespace alla mesh tramite applicazione della label

**oc label namespace <NOME\_NAMESPACE> istio-injection=enabled --overwrite**

- installata l'applicazione di esempio modificata nei 3 namespace

- aggiunta label per la sidecar injection nei deployment applicativi

**spec:**

**template:**

**metadata:**

**labels:**

**sidecar.istio.io/inject: 'true'**

- verificato su Kiali configurazione della mesh e il corretto traffico in assenza di policy

- applicate manualmente le policy gradualmente in modo da verificare la corretta applicazione (eg: deny in ingresso sul backend,  verificato l'impossibilità di accedere, applicata la regola di allow e verificato il ripristino del traffico)

- per semplificare il deploy delle policy inoltre è stato mostrato un helm-chart di esempio che tramite un semplice file di values permette l'applicazione delle policy di default su uno specifico namespace in un singolo pacchetto.

  L'helm chart di esempio contiene le seguenti policy:  
     - deny all incoming  
     - allow from gateway (opzionale)  
     - allow from namespace (opzionale configurabile con un elenco di namespace)

- applicate le successive policy con helm chart e appropriati file di configurazione (values)

- verificato tramite Kiali il corretto funzionamento delle policy; in particolare, in aggiunta alla verifica del corretto traffico si è testata l'impossibilità di accedere dai servizi di backend al microservizio di frontend.

- condiviso con Imola informatica l'helm chart di esempio  
  
Una volta che il VIP è stato creato si è effettuata un'ulteriore verifica tramite la URL esposta dell'applicazione di esempio verificando su Kiali il corretto flusso del traffico.  
  
**Documentazione**  
- [[Service Mesh 2.x](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-about.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuo2mFEtXQ$)]([https://docs.openshift.com/container-platform/4.14/service\_mesh/v2x/ossm-about.html](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-about.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuo2mFEtXQ$))  
- [[Istio Documentation](https://urldefense.com/v3/__https:/istio.io/v1.18/docs/__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoOSQXjPc$)]([https://istio.io/v1.18/docs/](https://urldefense.com/v3/__https:/istio.io/v1.18/docs/__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoOSQXjPc$)) - verificare le versione  
- [[Deployment Model](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-deployment-models.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoGBpiiVA$)]([https://docs.openshift.com/container-platform/4.14/service\_mesh/v2x/ossm-deployment-models.html](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-deployment-models.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoGBpiiVA$))  
- [[Sidecar Injection](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/prepare-to-deploy-applications-ossm.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuolYmNVsM$)]([https://docs.openshift.com/container-platform/4.14/service\_mesh/v2x/prepare-to-deploy-applications-ossm.html](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/prepare-to-deploy-applications-ossm.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuolYmNVsM$))  
- [[Traffic Management](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-traffic-manage.html*ossm-routing-traffic__;Iw!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoryxQl1M$)]([https://docs.openshift.com/container-platform/4.14/service\_mesh/v2x/ossm-traffic-manage.html#ossm-routing-traffic](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-traffic-manage.html*ossm-routing-traffic__;Iw!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoryxQl1M$))  
- [[Automatic Route](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-traffic-manage.html*ossm-auto-route_traffic-management__;Iw!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoxVh7bV0$)]([https://docs.openshift.com/container-platform/4.14/service\_mesh/v2x/ossm-traffic-manage.html#ossm-auto-route\_traffic-management](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-traffic-manage.html*ossm-auto-route_traffic-management__;Iw!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoxVh7bV0$))  
- [[Security](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-security.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoBXEq0Fg$)]([https://docs.openshift.com/container-platform/4.14/service\_mesh/v2x/ossm-security.html](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-security.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoBXEq0Fg$))  
  
**Repository di esempio utilizzato**  
- [[Repository](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuo4_7VbxI$)]([https://github.com/alessandrocaglio/ca-gateway-call](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuo4_7VbxI$))  
- [[Branch applicazione BookInfo modificata](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call/tree/bookinfo-layer__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoa8L8I1Y$)]([https://github.com/alessandrocaglio/ca-gateway-call/tree/bookinfo-layer](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call/tree/bookinfo-layer__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoa8L8I1Y$))  
- [[Branch policy helm chart di esempio](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call/tree/policy-helm-chart__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuobZIBH6M$)]([https://github.com/alessandrocaglio/ca-gateway-call/tree/policy-helm-chart](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call/tree/policy-helm-chart__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuobZIBH6M$))  
Alcuni file di configurazione sono stati adeguati al funzionamento in ambiente Credit Agricole

**Note**  
\* Il Service Mesh sul cluster di collaudo è stato installato in modalità *ClusterWide* il che significa che non è possibile la multi-tenancy ed è presente un solo Control Plane per tutto il cluster.

  Non si è quindi creato un nuovo control plane per effettuare i test ma utilizzato quello già installato.   
  (Rif: [[Deployment Model](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-deployment-models.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoGBpiiVA$)](<https://docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-deployment-models.html)>)

  - Proxy AutoInjection è disabilitato: Il ControlPlane attualmente installato ha l'auto-injection dell'Envoy proxy disabilitato. Per abilitare quindi l'injection sarà necessario aggiungere la label ai deploy applicativi.   
    ```  
    metadata:   
      labels:   
        [sidecar.istio.io/inject](https://urldefense.com/v3/__http:/sidecar.istio.io/inject__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoIoxgRos$): 'true'  
    ```  
   (Rif:[[Sidecar Injection](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/prepare-to-deploy-applications-ossm.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuolYmNVsM$)](<https://docs.openshift.com/container-platform/4.14/service_mesh/v2x/prepare-to-deploy-applications-ossm.html)>)

- L'attuale installazione di ServiceMesh ha abilitato la creazione automatica delle rotte attive (IOR - Istio Openshift Routing). Nonostante questa funzionalità sia supportata è stata recemente deprecata e verrà rimossa in futuro e quindi a tendere la creazione delle Route Openshift dovrà essere effettuata manualmente (direi contestualmente ai relativi Gateway/VirtualService).

  (Rif: [[Automatic Route](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-traffic-manage.html*ossm-auto-route_traffic-management__;Iw!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoxVh7bV0$)](<https://docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-traffic-manage.html#ossm-auto-route_traffic-management)>)

  - mTLS è abilitato nella mesh in modalità \*PERMISSIVE\*   
   (Rif: [[Security](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-security.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoBXEq0Fg$)]([https://docs.openshift.com/container-platform/4.14/service\_mesh/v2x/ossm-security.html](https://urldefense.com/v3/__https:/docs.openshift.com/container-platform/4.14/service_mesh/v2x/ossm-security.html__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuoBXEq0Fg$)))  
  - Il repository utilizzato è un repository personale preparato per semplificare il test delle policy. Non è un repository ufficiale Red Hat e quindi non supportato e/o certificato in alcun modo.

[- [[Repository](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuo4_7VbxI$)]([https://github.com/alessandrocaglio/ca-gateway-call](https://urldefense.com/v3/__https:/github.com/alessandrocaglio/ca-gateway-call__;!!OrxsNty6D4my!-8KQHwZh4c84L6FznzlteEKPYbDn-EXKsLk0YfSDKqedbONHn4WJN9B-sonaGOYA_Kw4H1-GT-WyUFuo4_7VbxI$))]