vcluster 使用者連接遠端主叢集指南

簡介

vcluster 允許使用者在一個底層的 Kubernetes 主叢集上建立輕量級的虛擬叢集。預設情況下，vcluster 只能透過埠轉發 (port-forwarding) 的方式在遠端叢集上進行連接。然而，為了讓 vcluster 使用者能夠直接連接到遠端主叢集，需要進行額外的網路配置和認證設定。

本指南將詳細說明如何配置 vcluster，使其使用者能夠直接連接到遠端主叢集，並涵蓋以下幾個主要方面：

1. **網路暴露方法**：介紹如何透過 Ingress、LoadBalancer 或 NodePort 服務來暴露 vcluster 的 API 伺服器。
2. **認證與授權**：說明如何為 vcluster 使用者配置 kubeconfig，並確保其具有適當的權限。
3. **最佳實踐**：提供一些建議，以確保連接的安全性和效率。

網路暴露方法

為了讓 vcluster 能夠從遠端直接訪問，需要將其 API 伺服器暴露出來。以下是幾種常見的方法：

1. 透過 LoadBalancer 服務暴露

使用 LoadBalancer 服務是最簡單直接的方法，但可能會產生額外的雲端供應商費用。這種方法會為 vcluster 建立一個外部可訪問的 IP 地址。

步驟：

1. **建立 LoadBalancer 服務定義**：

   ```
   yaml apiVersion: v1 kind: Service metadata: name: vcluster-loadbalancer namespace: <vcluster-namespace> # 替換為您的 vcluster 所在的命名空間 spec: selector: app: vcluster release: <vcluster-name> # 替換
   ```

`為您的 vcluster 名稱 ports: - name: https port: 443 targetPort: 8443 protocol: TCP type: LoadBalancer`

2. **應用服務定義**：

   `bash kubectl apply -f load-balancer.yaml`

3. **獲取外部 IP 地址**：

   `bash kubectl get svc vcluster-loadbalancer -n <vcluster-namespace>`

   您將會看到類似以下的輸出，其中 `EXTERNAL-IP` 即為 vcluster 的外部可訪問 IP：

   `NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE vcluster-loadbalancer LoadBalancer 10.68.9.239 x.x.x.x 443:32678/TCP 7m15s`

4. **更新 vcluster 配置 (TLS SAN)**：

   為了確保 TLS 憑證的有效性，需要將外部 IP 地址添加到 vcluster 的 TLS Subject Alternative Name (SAN) 中。這通常在建立 vcluster 時透過 `values.yaml` 進行配置：

   `yaml syncer: extraArgs: - --tls-san=x.x.x.x # 替換為您獲取的外部 IP 地址`

5. **建立或更新 vcluster**：

   `bash vcluster create <vcluster-name> -n <vcluster-namespace> --connect=false -f values.yaml`

6. **連接到 vcluster**：

   `bash vcluster connect <vcluster-name> -n <vcluster-namespace> --server=https://x.x.x.x # 替換為外部 IP 地址`

2. 透過 NodePort 服務暴露

NodePort 服務透過主叢集節點的 IP 地址和一個靜態埠來暴露 vcluster。這適用於自建環境或需要更精細控制網路的場景。

步驟：

1. **建立 NodePort 服務定義**：

`yaml apiVersion: v1 kind: Service metadata: name: vcluster-nodeport namespace: <vcluster-namespace> spec: selector: app: vcluster release: <vcluster-name> ports: - name: https port: 443 targetPort: 8443 protocol: TCP type: NodePort`

2. **應用服務定義**：

`bash kubectl apply -f nodeport.yaml`

3. **獲取節點 IP 和 NodePort**：

`bash kubectl get svc vcluster-nodeport -n <vcluster-namespace> kubectl get nodes -o wide`

您將會看到類似以下的輸出，其中 `PORT(S)` 顯示了 NodePort，`EXTERNAL-IP` 顯示了節點的外部 IP：

``` NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE vcluster-nodeport NodePort 10.68.9.75 443:31992/TCP 85s

NAME STATUS ROLES AGE VERSION INTERNAL-IP EXTERNAL-IP OS-IMAGE KERNEL-VERSION CONTAINER-RUNTIME gke-cluster-1-default-pool-8f0bb8bb-p6wx Ready 6d v1.20.6-gke.1000 10.156.0.14 x.x.x.x Container-Optimized OS from Google 5.4.104+ containerd://1.4.3 ```

4. **更新 vcluster 配置 (TLS SAN)**：

將所有節點的外部 IP 地址添加到 vcluster 的 TLS SAN 中：

`yaml syncer: extraArgs: - --tls-san=x.x.x.x,y.y.y.y,z.z.z.z # 替換為所有節點的外部 IP 地址`

5. **建立或更新 vcluster**：

`bash vcluster create <vcluster-name> -n <vcluster-namespace> --connect=false -f values.yaml`

6. **連接到 vcluster**：

`bash vcluster connect <vcluster-name> -n <vcluster-namespace> --server=https://<node-ip>:<node-port> # 替換為節點 IP 和 NodePort`
```

3. 透過 Ingress 暴露

Ingress 是一種更靈活且成本效益更高的方法，特別是在雲端環境中。它允許您透過單一的負載平衡器來路由多個服務的流量。

步驟：

1. **確保主叢集已安裝 Ingress Controller**：

   例如 NGINX Ingress Controller。

2. **建立 Ingress 資源定義**：

   ```
   yaml apiVersion: networking.k8s.io/v1 kind: Ingress metadata: name: vcluster-ingress namespace: <vcluster-namespace> annotations: nginx.ingress.kubernetes.io/backend-protocol: "HTTPS" # 其他 Ingress Controller 特定的註解 spec: rules: - host: vcluster.<your-domain.com> # 替換為您希望的域名 http: paths: - path: / pathType: Prefix backend: service: name: <vcluster-name> # vcluster 服務的名稱，通常與 vcluster 名稱相同 port: number: 8443 # vcluster API 伺服器的埠 tls: - hosts: - vcluster.<your-domain.com> secretName: vcluster-tls-secret # 包含 TLS 憑證的 Secret
   ```

3. **建立 TLS Secret**：

   您需要為 Ingress 配置 TLS 憑證。這通常透過 `kubectl create secret tls` 命令或 cert-manager 等工具來完成。

   ```
   bash kubectl create secret tls vcluster-tls-secret --cert=/path/to/tls.crt --key=/path/to/tls.key -n <vcluster-namespace>
   ```

4. **應用 Ingress 定義**：

   ```
   bash kubectl apply -f ingress.yaml
   ```

5. **更新 vcluster 配置 (TLS SAN)**：

   將 Ingress 的域名添加到 vcluster 的 TLS SAN 中：

   ```
   yaml syncer: extraArgs: - --tls-san=vcluster.<your-domain.com>
   ```

6. **建立或更新 vcluster**：

`bash vcluster create <vcluster-name> -n <vcluster-namespace> --connect=false -f values.yaml`

7. **連接到 vcluster**：

`bash vcluster connect <vcluster-name> -n <vcluster-namespace> --server=https://vcluster.<your-domain.com>`

認證與授權

vcluster 使用者連接到遠端主叢集後，需要正確的認證和授權才能執行操作。vcluster 會為每個虛擬叢集建立一個服務帳戶 (ServiceAccount) 和相關的 RBAC 資源。

1. 獲取 vcluster 的 kubeconfig

最常見的方式是透過 `vcluster connect` 命令來獲取 kubeconfig：

```
vcluster connect <vcluster-name> -n <vcluster-namespace> --update-current=false --print > /tmp/vcluster.kubeconfig
```

這會將 vcluster 的 kubeconfig 寫入 `/tmp/vcluster.kubeconfig` 文件。使用者可以使用此文件來設定 `KUBECONFIG` 環境變數，或將其合併到現有的 kubeconfig 中。

2. 使用 kubeconfig 連接

使用者可以透過以下方式使用獲取的 kubeconfig 連接到 vcluster：

```
export KUBECONFIG=/tmp/vcluster.kubeconfig
kubectl get ns
```

或者，將其合併到預設的 `~/.kube/config` 文件中：

```
KUBECONFIG=~/.kube/config:/tmp/vcluster.kubeconfig kubectl config view --flatten > ~/.kube/config.new
mv ~/.kube/config.new ~/.kube/config
```

3. RBAC 考量

vcluster 內部會管理其虛擬叢集中的 RBAC。對於連接到遠端主叢集的使用者，其權限範圍僅限於該 vcluster 內部。vcluster 會將虛擬叢集中的資源同步到主叢集的一個特定命名空間中，並對這些同步的資源進行命名重寫，以避免衝突。

重要提示：

- vcluster 使用者在虛擬叢集中的操作，大部分資源只存在於虛擬叢集內部，而不會直接暴露在底層主叢集。
- 只有少數與工作負載 (如 Pods) 和網路相關的資源 (如 Services) 會被同步到主叢集，因為 vcluster 本身沒有節點或網路。
- vcluster 的同步器 (syncer) 會負責將虛擬叢集中的資源狀態同步到主叢集，並確保命名空間和資源名稱的唯一性。

最佳實踐

- **安全性**：
  - 始終使用 TLS/SSL 加密連接 (HTTPS)。
  - 定期審查和更新 vcluster 的 TLS 憑證。
  - 限制對 vcluster API 伺服器的網路訪問，只允許必要的 IP 範圍或網路。
  - 對於 Ingress，考慮使用 Web Application Firewall (WAF) 來增強安全性。
- **成本考量**：
  - LoadBalancer 服務在雲端環境中可能會產生較高的費用，特別是當您有多個 vcluster 時。考慮使用 Ingress 或 NodePort 作為替代方案。
- **監控與日誌**：
  - 監控 vcluster 的運行狀況和資源使用情況。
  - 收集和分析 vcluster 的日誌，以便及時發現和解決問題。
- **版本兼容性**：
  - 確保 vcluster CLI、vcluster 版本和 Kubernetes 主叢集版本之間的兼容性。
- **自動化**：
  - 使用基礎設施即程式碼 (IaC) 工具 (如 Helm、Terraform) 來自動化 vcluster 的部署和配置，確保一致性和可重複性。

結論

透過適當的網路暴露和認證配置，vcluster 使用者可以方便地連接到遠端主叢集，並在虛擬叢集中進行操作。選擇合適的網路暴露方法取決於您的基礎設施環境、成本考量和安全需求。遵循最佳實踐將有助於確保 vcluster 環境的穩定、安全和高效運行。