Admission Control Debug

Friday, March 10, 2023 7:42 PM

// Admission Webhook debug

if we found the overall admission webhook is not being called.. we can check kube-apiserver log

```
neuvector@ubuntu2204-E:/var/log$ kubectl get pods -n kube-system
NAME                                   READY   STATUS    RESTARTS   AGE
coredns-558bd4d5db-42sp2               1/1     Running   2          69d
coredns-558bd4d5db-lv6bk               1/1     Running   2          69d
etcd-ubuntu2204-e                      1/1     Running   2          69d
kube-apiserver-ubuntu2204-e            1/1     Running   3          69d
kube-controller-manager-ubuntu2204-e   1/1     Running   2          69d
kube-proxy-5d8vw                       1/1     Running   2          69d
kube-proxy-c7wd7                       1/1     Running   3          69d
kube-proxy-jbm4g                       1/1     Running   5          69d
kube-scheduler-ubuntu2204-e            1/1     Running   2          69d
weave-net-l4lhh                        2/2     Running   5          69d
weave-net-ljdp4                        2/2     Running   8          69d
weave-net-qn4wh                        2/2     Running   8          69d
neuvector@ubuntu2204-E:/var/log$
```

```
neuvector@ubuntu2204-E:/var/log$ kubectl logs -f kube-apiserver-ubuntu2204-e -n kube-system
```

// we can see the the calling webhook related log..

```
W0118 02:15:55.506753       1 dispatcher.go:142] rejected by webhook "neuvector-validating-admission-webhook
.neuvector.svc": &errors.StatusError{ErrStatus:v1.Status{TypeMeta:v1.TypeMeta{Kind:"", APIVersion:""}, ListM
eta:v1.ListMeta{SelfLink:"", ResourceVersion:"", Continue:"", RemainingItemCount:(*int64)(nil)}, Status:"Fai
lure", Message:"admission webhook \"neuvector-validating-admission-webhook.neuvector.svc\" denied the reques
t: Creation of Kubernetes Deployment is denied.", Reason:"", Details:(*v1.StatusDetails)(nil), Code:400}}
I0118 02:15:56.249798       1 client.go:360] parsed scheme: "passthrough"
I0118 02:15:56.250047       1 passthrough.go:48] ccResolverWrapper: sending update to cc: {[{https://127.0.0
.1:2379  <nil> 0 <nil>}] <nil> <nil>}
I0118 02:15:56.250125       1 clientconn.go:948] ClientConn switching balancer to "pick_first"
```

// remember to have valid keys.go file when compile our program, otherwise k8s api-server can't call our webhook

```
I0118 02:36:11.331896       1 clientconn.go:948] ClientConn switching balancer to "pick_first"
W0118 02:36:23.944296       1 dispatcher.go:129] Failed calling webhook, failing open neuvector-validating-a
dmission-webhook.neuvector.svc: failed calling webhook "neuvector-validating-admission-webhook.neuvector.svc
": Post "https://neuvector-svc-admission-webhook.neuvector.svc:443/v1/validate/1674007391161599827-167400739
1161600263?timeout=30s": remote error: tls: handshake failure
E0118 02:36:23.944408       1 dispatcher.go:130] failed calling webhook "neuvector-validating-admission-webh
ook.neuvector.svc": Post "https://neuvector-svc-admission-webhook.neuvector.svc:443/v1/validate/167400739116
1599827-167400739116160026 3?timeout=30s": remote error: tls: handshake failure
W0118 02:36:24.101553       1 dispatcher.go:129] Failed calling webhook, failing open neuvector-validating-a
dmission-webhook.neuvector.svc: failed calling webhook "neuvector-validating-admission-webhook.neuvector.svc
": Post "https://neuvector-svc-admission-webhook.neuvector.svc:443/v1/validate/1674007391161599827-167400739
1161600263?timeout=30s": remote error: tls: handshake failure
```

```
jeff@SUSE-387793:~/go/src/github.com/neuvector/neuvector/share$ cd utils/
jeff@SUSE-387793:~/go/src/github.com/neuvector/neuvector/share/utils$ ls -l keys.go
-rw-r--r-- 1 jeff jeff 402 Jan 17 18:48 keys.go
jeff@SUSE-387793:~/go/src/github.com/neuvector/neuvector/share/utils$ cat keys.go
package utils

var passwordSymKey []byte = []byte{78, 101, 117, 86, 101, 99, 116, 111, 114, 49, 54, 45, 112, 97, 115, 115}

var licenseSymKey []byte = []byte{78, 101, 117, 86, 101, 99, 116, 111, 114, 49, 54, 45, 115, 107, 101, 121}

var cveDBEncryptKey []byte = []byte{97, 49, 98, 101, 55, 101, 99, 52, 97, 48, 48, 56, 52, 50, 55, 97, 99, 97, 53, 5
4, 102, 57, 48, 50, 48, 54, 100, 49, 53, 48, 98, 102}
jeff@SUSE-387793:~/go/src/github.com/neuvector/neuvector/share/utils$
```

// admission webhook breakpoint, stack

```
(dlv) b github.com/neuvector/neuvector/controller/rest.handlerAddAdmissionRule
(dlv) c
.........
```

```
(dlv) p confData.Config.Criteria
[]*github.com/neuvector/neuvector/controller/api.RESTAdmRuleCriterion len: 1, cap: 4, [
        *{
                Name: "labels",
                Op: "containsAny",
                Value: "applabel=nginx,mysql,busybox,envlabel=beta,prd",
                SubCriteria: []*github.com/neuvector/neuvector/controller/api.RESTAdmRuleCriterion len: 0, cap: 0, nil,
                Type: "",
                Kind: "",
                Path: "labels",
                ValueType: "",},
]


(dlv) p critValues
[]string len: 5, cap: 5, [
        "applabel=nginx",
        "mysql",
        "busybox",
        "envlabel=beta",
        "prd",
]


(dlv) p clusConf.Criteria
[]*github.com/neuvector/neuvector/share.CLUSAdmRuleCriterion len: 1, cap: 1, [
        *{
                Name: "labels",
                Op: "containsAny",
                Value: "busybox,envlabel=beta,prd,applabel=nginx,mysql",
                ValueSlice: []string len: 0, cap: 0, nil,
                SubCriteria: []*github.com/neuvector/neuvector/share.CLUSAdmRuleCriterion len: 0, cap: 0, nil,
                Type: "",
                Kind: "",
                Path: "labels",
                ValueType: "",},
]


jeff@SUSE-387793:~/go/src/github.com/neuvector/neuvector/controller$ dlv connect 10.1.45.45:12345
Type 'help' for list of commands.
(dlv) funcs MatchK8sAdmissionRules
github.com/neuvector/neuvector/controller/cache.(*CacheMethod).MatchK8sAdmissionRules
github.com/neuvector/neuvector/controller/cache.CacheMethod.MatchK8sAdmissionRules

(dlv) b github.com/neuvector/neuvector/controller/cache.(*CacheMethod).MatchK8sAdmissionRules
Breakpoint 1 set at 0x2eaf858 for github.com/neuvector/neuvector/controller/cache.(*CacheMethod).MatchK8sAdmissionRules() <autogenerated>:1

(dlv) c
> github.com/neuvector/neuvector/controller/cache.(*CacheMethod).MatchK8sAdmissionRules() <autogenerated>:1 (hits goroutine(1114):1 total:1) (PC:
0x2eaf858)
(dlv) stack
 0  0x0000000002eaf858 in github.com/neuvector/neuvector/controller/cache.(*CacheMethod).MatchK8sAdmissionRules
    at <autogenerated>:1
 1  0x0000000003062232 in github.com/neuvector/neuvector/controller/rest.walkThruContainers
    at ./rest/admwebhook.go:737
 2  0x0000000003064ed7 in github.com/neuvector/neuvector/controller/rest.(*WebhookServer).validate
    at ./rest/admwebhook.go:1100
 3  0x000000000306b550 in github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s
    at ./rest/admwebhook.go:1234
 4  0x000000000306d13a in github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveWithTimeStamps
    at ./rest/admwebhook.go:1332
 5  0x000000000306d844 in github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serve
    at ./rest/admwebhook.go:1340
 6  0x00000000032f0a1d in github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serve-fm
    at ./rest/admwebhook.go:1336
 7  0x00000000013b0d14 in net/http.HandlerFunc.ServeHTTP
    at /usr/local/go/src/net/http/server.go:2041
 8  0x00000000013b39f6 in net/http.(*ServeMux).ServeHTTP
    at /usr/local/go/src/net/http/server.go:2416
 9  0x00000000013b559f in net/http.serverHandler.ServeHTTP
    at /usr/local/go/src/net/http/server.go:2836
10  0x00000000013afcba in net/http.(*conn).serve
    at /usr/local/go/src/net/http/server.go:1924
11  0x0000000000f906c1 in runtime.goexit
    at /usr/local/go/src/runtime/asm_amd64.s:1373
(dlv) c
```

// delve debug

```
(dlv) b github.com/neuvector/neuvector/controller/rest.(*WebhookServer).validate
Breakpoint 3 set at 0x3064861 for github.com/neuvector/neuvector/controller/rest.(*WebhookServer).validate() ./rest/admwebhook.go:909
(dlv) c
> github.com/neuvector/neuvector/controller/rest.(*WebhookServer).validate() ./rest/admwebhook.go:909 (hits goroutine(835):1 total:1) (PC:
0x3064861)
   904:         }
   905:
   906:         return nil
   907: }
   908:
=> 909: func (whsvr *WebhookServer) validate(ar *admissionv1beta1.AdmissionReview, mode string, defaultAction int,
```

```
   910:         stamps *api.AdmCtlTimeStamps, forTesting bool) (*admissionv1beta1.AdmissionResponse, bool) {
   911:         req := ar.Request
   912:         var objectMeta *metav1.ObjectMeta
   913:         var podTemplateSpec *corev1.PodTemplateSpec
   914:         var admResObject *nvsysadmission.AdmResObject
(dlv) n


(dlv) list rest/admwebhook.go:909         // ** 列出這個file的行數
Showing /home/jeff/go/src/github.com/neuvector/neuvector/controller/rest/admwebhook.go:909 (PC: 0x3064861)
   904:         }
   905:
   906:         return nil
   907: }
   908:
   909: func (whsvr *WebhookServer) validate(ar *admissionv1beta1.AdmissionReview, mode string, defaultAction int,
   910:         stamps *api.AdmCtlTimeStamps, forTesting bool) (*admissionv1beta1.AdmissionResponse, bool) {
   911:         req := ar.Request
   912:         var objectMeta *metav1.ObjectMeta
   913:         var podTemplateSpec *corev1.PodTemplateSpec
   914:         var admResObject *nvsysadmission.AdmResObject



(dlv) funcs serveK8s
github.com/neuvector/neuvector/controller/rest.(*WebhookServer).crdserveK8s
github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s

(dlv) list github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s     // ** 用funcs找到要看的funcion, 然後用 list 去看
Showing /home/jeff/go/src/github.com/neuvector/neuvector/controller/rest/admwebhook.go:1206 (PC: 0x306ac7b)
  1201:                 Result:  statusResult,
  1202:         }, reqIgnored
  1203: }
  1204:
  1205: // Serve method for Kubernetes Admission Control
  1206: func (whsvr *WebhookServer) serveK8s(w http.ResponseWriter, r *http.Request, admType, category, mode string,
  1207:         defaultAction int, body []byte, stamps *api.AdmCtlTimeStamps, nvStatusReq bool) {
  1208:         var admissionResponse *admissionv1beta1.AdmissionResponse
  1209:         var ignoredReq bool
  1210:         ar := admissionv1beta1.AdmissionReview{}
  1211:         if _, _, err := deserializer.Decode(body, nil, &ar); err != nil {
(dlv)



(dlv) list github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s:29  // ** list function:number, 這裡的number 是相對於這個function
的 line#
Showing /home/jeff/go/src/github.com/neuvector/neuvector/controller/rest/admwebhook.go:1235 (PC: 0x306b57c)
  1230:                         return
  1231:                 }
  1232:
  1233:                 if admType == admission.NvAdmValidateType {
  1234:                         admissionResponse, ignoredReq = whsvr.validate(&ar, mode, defaultAction, stamps, false)
  1235:                         admissionResponse.UID = ar.Request.UID                                                  // ** we want break/trace
here.. p ar, admissionResponse
  1236:                 } else {
  1237:                         log.WithFields(log.Fields{"path": r.URL.Path}).Debug("unsupported path")
  1238:                         http.Error(w, "unsupported", http.StatusNotImplemented)
  1239:                         if !nvStatusReq {
  1240:                                 cacher.UpdateLocalAdmCtrlStats(category, nvsysadmission.ReqErrored)


(dlv) b github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s:29  // *** 找到我們感興趣的line# (相對於這個function), 可以用這個格式來設
breakpoint/trace
Breakpoint 4 set at 0x306b57c for github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s() ./rest/admwebhook.go:1235


(dlv) list github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s:30  // *** 若我們指定的那一行不是一個valid state, 會出現這種錯誤訊
息.(declare variable也不算)
Command failed: could not find statement at /home/jeff/go/src/github.com/neuvector/neuvector/controller/rest/admwebhook.go:1236, please use a line
with a statement


// when breakpoint hit
(dlv) p ar.Request.Kind
github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.GroupVersionKind {
        Group: "apps",
        Version: "v1",
        Kind: "Deployment",}
(dlv) p ar.Request.Kind.Kind
"Deployment"
(dlv) p ar.Request.Name
"nginx-deployment"
(dlv) p ar.Request.Namespace
"default"

(dlv) p admissionResponse
*github.com/neuvector/neuvector/vendor/k8s.io/api/admission/v1beta1.AdmissionResponse {
        UID: "",
        Allowed: false,
        Result: *github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.Status {
```

```
                TypeMeta: (*"github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.TypeMeta")(0xc00d878c80),
                ListMeta: (*"github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.ListMeta")(0xc00d878ca0),
                Status: "",
                Message: "Creation of Kubernetes Deployment is denied.",
                Reason: "",
                Details: *github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.StatusDetails nil,
                Code: 0,},
        Patch: []uint8 len: 0, cap: 0, nil,
        PatchType: *github.com/neuvector/neuvector/vendor/k8s.io/api/admission/v1beta1.PatchType nil,
        AuditAnnotations: map[string]string nil,
        Warnings: []string len: 0, cap: 0, nil,}
(dlv) p admissionResponse.Allowed
false
(dlv) p admissionResponse.Result
*github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.Status {
        TypeMeta: github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.TypeMeta {Kind: "", APIVersion: ""},
        ListMeta: github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.ListMeta {SelfLink: "", ResourceVersion: "", Continue:
"", RemainingItemCount: *int64 nil},
        Status: "",
        Message: "Creation of Kubernetes Deployment is denied.",
        Reason: "",
        Details: *github.com/neuvector/neuvector/vendor/k8s.io/apimachinery/pkg/apis/meta/v1.StatusDetails nil,
        Code: 0,}
(dlv) p admissionResponse.Result.Message
"Creation of Kubernetes Deployment is denied."



(dlv) t github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s:29
Tracepoint 5 set at 0x306b57c for github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s() ./rest/admwebhook.go:1235
(dlv) on 5 p admissionResponse.Allowed
(dlv) c
> goroutine(1314):
github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s(("*github.com/neuvector/neuvector/controller/rest.WebhookServer")
(0xc003580b10), net/http.ResponseWriter(*net/http.response) 0xc000c22f48, ("*net/http.Request")(0xc00e62c100), "validate", "kubernetes", "protect",
0, []uint8 len: 3218, cap: 3584, [...], ("*github.com/neuvector/neuvector/controller/api.AdmCtlTimeStamps")(0xc000c23630), false)
        admissionResponse.Allowed: false



(dlv) on 5 p admissionResponse.Result.Message
(dlv) c
> goroutine(1314):
github.com/neuvector/neuvector/controller/rest.(*WebhookServer).serveK8s(("*github.com/neuvector/neuvector/controller/rest.WebhookServer")
(0xc003580b10), net/http.ResponseWriter(*net/http.response) 0xc000c22f48, ("*net/http.Request")(0xc00e62d300), "validate", "kubernetes", "protect",
0, []uint8 len: 3218, cap: 3584, [...], ("*github.com/neuvector/neuvector/controller/api.AdmCtlTimeStamps")(0xc000c23630), false)
        admissionResponse.Allowed: false
        admissionResponse.Result.Message: "Creation of Kubernetes Deployment is denied."
```