

Suse Neuvector-策略管理範例



Suse NeuVector 是一套基於雲原生容器平台的安全防護解決方案，這次介紹基礎功能當中的策略管理。NeuVector 會自動將工作節點加入到 nodes group，而部署的工作負載也會自動建立以 nv 開頭的 group (nv.<workload name>.<namespace name>) 方便進行操作。

The screenshot shows the Suse NeuVector web interface. The top navigation bar includes the NeuVector logo, a search bar, and user information for 'admin'. The main content area is titled 'Groups' and shows a list of 47 groups. The 'nodes' group is selected. The table below lists the groups with their details.

Name	Namespace	Policy Mode	Type	Members	Network Rules	Response Rules	
containers			User Created	60	0	0	
external			Learned	0	4	0	
nodes		Discover	Learned	2	27	0	
nv.alertmanager-rancher-monitoring-alertmanager.cattle-monitoring-sys	cattle-monitoring-system	Discover	Learned	1	2	0	
nv.appdynamics-infraviz.appdynamics	appdynamics	Discover	Learned	2	1	0	
nv.appdynamics-operator.appdynamics	appdynamics	Discover	Learned	1	0	0	
nv.canal.kube-system	kube-system	Discover	Learned	2	1	0	
nv.cattle-cluster-agent.cattle-system	cattle-system	Discover	Learned	1	1	0	

NeuVector 以 Group 為單位對容器與主機進行管理，包含網路規則、進程配置文件規則、文件存取規則、響應規則等設定，並且提供三種模式：

- Discover：預設模式。自動發現並記錄容器、主機之間的網路連接，自動建立網路規則白名單，保護正常的應用網路行為。觀察容器內進程的執行狀況，建立白名單進程配置文件規則。
- Monitor：監控容器和主機的網路與進程執行情況，若發現有違反安全策略的行為將於 NeuVector 發出警告。此模式下不會自動建立新規則，但可以手動增加。
- Protect：監控容器和主機的網路與進程執行情況，若發現有違反安全策略的行為直接拒絕。

以下簡單演示，首先建立兩個簡單運行 nginx 的 Deployment

```
test-ngx-user
```

```
test-ngx-web
```

預設 Discover 模式 NeuVector 會自動建立對應的 group，而此時 Network Rules 當中還沒有任何規則。

Name	Namespace	Policy Mode	Type	Members	Network Rules	Response Rules
nv.test-ngx-user-jamie-test	jamie-test	Discover	Learned	1	0	0
nv.test-ngx-web-jamie-test	jamie-test	Discover	Learned	1	0	0

透過 Rancher Console 進到 test-ngx-user 容器中並執行 curl test-ngx-web

```
> test-ngx-user-7f4db5c5dc-t2xd1 [x]
root@test-ngx-user-7f4db5c5dc-t2xd1:~# curl test-ngx-web
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@test-ngx-user-7f4db5c5dc-t2xd1:~#
```

可以正常訪問，且因為在 Discover 模式，NeuVector 會自動新增該訪問規則

The screenshot shows the 'Groups' configuration page in NeuVector. At the top, it indicates 'Network Service Policy Mode: OFF'. Below, a table lists two groups:

Name	Namespace	Policy Mode	Type	Members	Network Rules	Response Rules
nv.test-ngx-user-jamie-test	jamie-test	Discover	Learned	1	2	0
nv.test-ngx-web-jamie-test	jamie-test	Discover	Learned	1	1	0

Below the table, the 'Network Rules' section for the selected group is visible, showing a rule with ID 10078:

ID	From	To	Applications	Ports	Action	Type	Updated at
10078	nv.test-ngx-user-jamie-test	nv.test-ngx-web-jamie-test	HTTP	any	Allow	Learned	Jan 13, 2023 17:32:09

接著將兩組 group 更改為 Monitor 模式

The screenshot shows the 'Groups' configuration page with the 'Switch Mode' button highlighted. The table below shows the groups updated to 'Monitor' mode:

Name	Namespace	Policy Mode	Type	Members	Network Rules	Response Rules
nv.test-ngx-user-jamie-test	jamie-test	Monitor	Learned	1	2	0
nv.test-ngx-web-jamie-test	jamie-test	Monitor	Learned	1	1	0

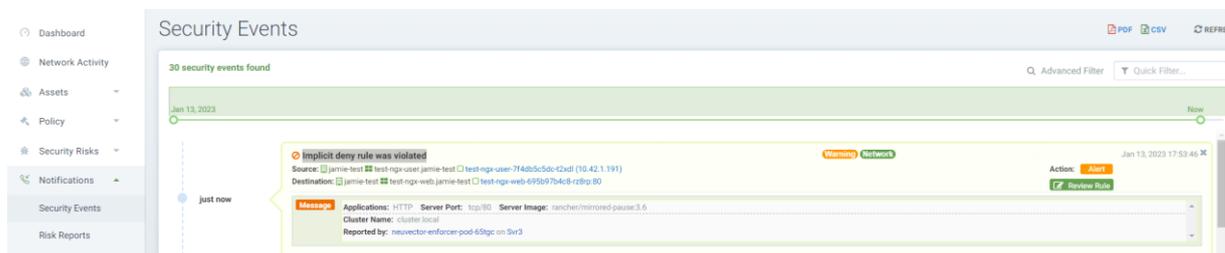
The 'Network Rules' section is also visible, showing the rule with ID 10078 highlighted in red:

ID	From	To	Applications	Ports	Action	Type	Updated at
10077	nv.test-ngx-user-jamie-test	nv.coredns.kube-system	DNS	Any	Allow	Learned	Jan 13, 2023 17:32:09
10078	nv.test-ngx-user-jamie-test	nv.test-ngx-web-jamie-test	HTTP	Any	Allow	Learned	Jan 13, 2023 17:32:09

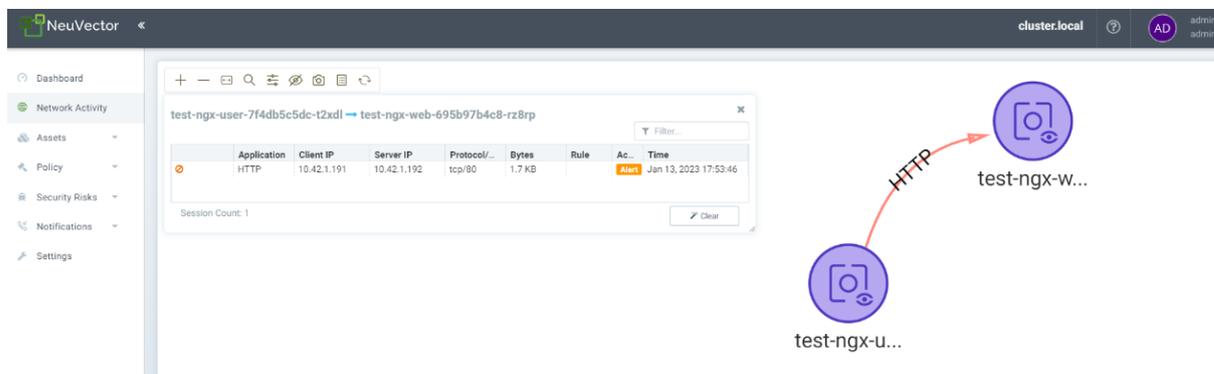
為了演示後面兩種模式，將剛剛發現訪問動作所自動新增的 Network Rule 刪除，來看
看若是違反規則的狀況

再一次進到 test-ngx-user 容器中並執行 curl test-ngx-web，一樣可以訪問，但由於將

規則移除，因此 NeuVector 通知中會記錄該警告，顯示違反規則



同時，在網路活動拓譜圖也可以觀察到該警告通知



最後，將兩組 group 更改為 Protect 模式



一樣從 test-ngx-user 容器中執行 curl test-ngx-web，看到同樣的操作但是這次卻被拒

絕

```
test-ngx-user-7f4db5c5dc-t2xd1
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
root@test-ngx-user-7f4db5c5dc-t2xd1:/#
root@test-ngx-user-7f4db5c5dc-t2xd1:/# curl test-ngx-web
bash: /usr/bin/curl: Operation not permitted
root@test-ngx-user-7f4db5c5dc-t2xd1:/#
```

以上為簡單的示範，建議的實踐方式，當部署新服務先以 Discover 模式運行一段時間，得到實際運行的網路連接與進程執行狀況。接著再用 Monitor 模式一段時間，看看有沒有額外的特殊情況，判斷是否需要新增修改規則，最終確定以後使用 Protect 模式來保護服務。

有需要諮詢協助的地方，可直接聯絡：

架構及雲端處

系統顧問 林哲名 Jamie Lin

02-27316868 分機 824

jamielin@mpinfo.com.tw