

TECHDOCS

## CNシリーズのアップグレード

---

## Contact Information

Corporate Headquarters:  
Palo Alto Networks  
3000 Tannery Way  
Santa Clara, CA 95054  
[www.paloaltonetworks.com/company/contact-support](http://www.paloaltonetworks.com/company/contact-support)

## About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal [docs.paloaltonetworks.com](http://docs.paloaltonetworks.com).
- To search for a specific topic, go to our search page [docs.paloaltonetworks.com/search.html](http://docs.paloaltonetworks.com/search.html).
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at [documentation@paloaltonetworks.com](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2021-2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at [www.paloaltonetworks.com/company/trademarks.html](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

December 13, 2021

---

# Table of Contents

<b>CN-Series ファイアウォールのアップグレード.....</b>	<b>5</b>
CNシリーズ ファイアウォールの移行.....	7
CN-Series ファイアウォールのアップグレード — ローリング更新.....	9
ローリング更新.....	9
追加の CN-MGMT StatefulSet を使用したローリング更新.....	11
新旧の PAN-CN-MGMT.yaml を比較する.....	15
CN-Series ファイアウォールのアップグレード — 再デプロイ .....	18
既存の CN-Series ファイアウォール デプロイメントを削除する.....	18
CN-Series Docker イメージを更新する.....	19
CN-Series ファイアウォールのデプロイ .....	20



# CN-Series ファイアウォールのアップグレード

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> <li>• CN-Series アップグレード</li> <li>• CN-Series デプロイメント</li> </ul>	<ul style="list-style-type: none"> <li>• CN-Series 10.1.x or above Container Images</li> <li>• PanoramaPAN-OS 10.1.x 以降のバージョンを実行している</li> </ul>

CN-MGMT ポッド (管理プレーン) と CN-NGFW ポッド (データプレーン) は、同じ PAN-OS バージョン上である必要があります。CN-Series ファイアウォール デプロイメントをアップグレードまたはダウングレードする方法は 2 つあります。どちらの方法でも、計画されたメンテナンス期間中にアップグレードまたはダウングレードをスケジュールする必要があります。

- **CNシリーズ ファイアウォールの移行**—CN シリーズを PAN-OS 10.1.x から 10.2.x、11.0.x にアップグレードできます。10.2.x から 11.0.x にアップグレードすることもできます。ただし、CN シリーズを PAN-OS 10.0.x から PAN-OS 10.1.x または 10.2.x にアップグレードすることはできません。代わりに、CN シリーズを再デプロイする必要があります。さらに、DaemonSet デプロイメントとしての CN-Series からサービスデプロイメントとしての CN-Series に直接アップグレードすることはできません。ある展開方法から別の展開方法に移動するには、CN-Series を再デプロイメントする必要があります。
- **CN-Series ファイアウォールのアップグレード—ローリング更新**—新しいバージョンを使用して、pan-cn-mgmt.yaml のイメージを変更するか、kubectl コマンドを使用して、既存の CN-MGMT StatefulSet をアップグレードしてから、CN-NGFW ポッドをアップグレードします。
- **CN-Series ファイアウォールのアップグレード (追加の CN-MGMT StatefulSet を使用したローリングアップデート)**—このバージョンを使用して、新しい pan-cn-mgmt-configmap.yaml および pan-cn-mgmt.yaml ファイルを新規にセットアップしてこれをデプロイすることにより、追加の CN-MGMT StatefulSet をクラスターにデプロイします。
- **CN-Series ファイアウォールのアップグレード—再デプロイ**—既存の CN-Series ファイアウォール デプロイメントを削除し、既存の デプロイメントを完全に置き換えます。このワークフローでは、長めのメンテナンス期間を計画する必要があります。これは、すべてのファイアウォールが同時にオフラインになり、ファイアウォール ポッドが再び稼働するまで、すべての保護されたアプリケーション トラフィック が影響を受けるためです。

追加の CN-MGMT StatefulSet メソッドを使用した再デプロイ および ローリングアップデートでは、CN-MGMT ポッドの新しいシリアル番号が作成されます。購入したサブスクリプション の **動的コンテンツアップデート** をインストールする必要があります。リリース ノートで PAN-

## CN-Series ファイアウォールのアップグレード

---

OS バージョンを参照して、必要な最小コンテンツ バージョンを確認し、そのバージョンを CN-MGMT ポッドにインストールします。

## CNシリーズファイアウォールの移行

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> <li>• CN-Series アップグレード</li> <li>• CN-Series デプロイメント</li> </ul>	<ul style="list-style-type: none"> <li>• CN-Series 10.1.x or above Container Images</li> <li>• PanoramaPAN-OS 10.1.x 以降のバージョンを実行している</li> </ul>

CNシリーズファイアウォールは、PAN-OS 10.1.xからPAN-OS 10.2.x、11.0.xまたは11.1.xにアップグレードできます。CNシリーズファイアウォールはPAN-OS 10.2.xから11.0.xまたは11.1.xにアップグレードすることもできます。ただし、PAN-OS 10.1からPAN-OS 10.2へ移行する場合、CNシリーズの直接のアップグレードパスはありません。代わりに、既存の CN-Series ファイアウォールの展開を削除してから、再デプロイメントする必要があります。

開始する前に、CN-Series YAML ファイルのバージョンが PAN-OS バージョンと互換性があることを確認します。

CN シリーズファイアウォール展開用のファイルの正しい組み合わせをダウンロードしていることを確認する必要があります。詳細については、[CN-Series ファイアウォールのイメージとファイルの互換性](#)を参照してください。

**STEP 1 |** 既存の CN-MGMT ポッドと CN-NGFW ポッドを削除します。

1. **kubectl delete -f pan-cn-mgmt.yaml**
2. **kubectl delete -f pan-cn-ngfw.yaml**

**STEP 2 |** ポッドが削除されたことを確認します。

1. **kubectl get pods -n kube-system -l app=pan-mgmt**
2. **kubectl get pods -n kube-system -l app=pan-ngfw**

**STEP 3 |** 既存の永続ボリューム クレーム (PVC) と永続ボリューム (PV) を削除する

1. **kubectl -n kube-system get pvc -l appname=pan-mgmt-sts** を使用して、pan-cn-mgmt.yaml に関連付けられたすべての PVC と PV を探します。

**pan-mgmt-sts** は、CN-MGMT ポッド用のデフォルトの appname セレクタです。別の名前を指定するように yaml を変更した場合は、一致するように appname を置き換える必要があります。EKS からのサンプル出力を以下に示します。

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
panconfig-pan-mgmt-sts-0	Bound	pvc-<id>	8Gi	RW0	gp2	15h
panconfig-pan-mgmt-sts-1	Bound	pvc-<id>	8Gi	RW0	gp2	15h
panlogs-pan-mgmt-sts-0	Bound	pvc-<id>	20Gi	RW0	gp2	15h
panlogs-pan-mgmt-sts-1	Bound	pvc-<id>	20Gi	RW0	gp2	15h
panplugincfg-pan-mgmt-sts-0	Bound	pvc-<id>	1Gi	RW0	gp2	15h
panplugincfg-pan-mgmt-sts-1	Bound	pvc-<id>	1Gi	RW0	gp2	15h
panplugins-pan-mgmt-sts-0	Bound	pvc-<id>	1Gi	RW0	gp2	15h
panplugins-pan-mgmt-sts-1	Bound	pvc-<id>	1Gi	RW0	gp2	15h
varcores-pan-mgmt-sts-0	Bound	pvc-<id>	20Gi	RW0	gp2	15h
varcores-pan-mgmt-sts-1	Bound	pvc-<id>	20Gi	RW0	gp2	15h
varlogpan-pan-mgmt-sts-0	Bound	pvc-<id>	20Gi	RW0	gp2	15h
varlogpan-pan-mgmt-sts-1	Bound	pvc-<id>	20Gi	RW0	gp2	15h



- 静的にプロビジョニングされた PV(オンプレミス デプロイメントで使用されることが多い)の場合、それを削除するには、pan-cn-pv-local.yaml ファイルと、CN-MGMT ポッドをホストしている各ノードに関するデータが格納されたディレクトリを明示的に削除する必要があります。

コマンド **rm -rf /mnt/pan-local1/\*** を使用して、pan-local 1 ~ 6 の PV を削除します。

- マネージド サービス/クラウド プラットフォームなどの動的にプロビジョニングされた PV の場合は、PVC を削除すると、PV が自動的に削除されます。

**STEP 4 |** PanoramaのKubernetesプラグインをアンインストールして古い設定を削除します。**STEP 5 |** Panorama のアップグレードを行います。**STEP 6 |** CNシリーズ用Kubernetesプラグインをインストールします。**STEP 7 |** CNシリーズファイアウォールをデプロイします。

# CN-Series ファイアウォールのアップグレード — ローリング更新

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> <li>• CN-Series アップグレード</li> <li>• CN-Series デプロイメント</li> </ul>	<ul style="list-style-type: none"> <li>• CN-Series 10.1.x or above Container Images</li> <li>• PanoramaPAN-OS 10.1.x 以降のバージョンを実行している</li> <li>• Helm 3.6 or above version client</li> </ul>

以下のオプションのいずれかを使用して、サポートされている PAN-OS バージョンへのローリング更新、アップグレード、またはダウングレードを実施します。

- [ローリング更新](#)この場合、CN-MGMT StatefulSet をアップグレードしてから、CN-NGFW ポッドをアップグレードします。
- [追加の CN-MGMT StatefulSet を使用したローリング更新](#)

このオプションを使用する場合は、「[新旧の PAN-CN-MGMT.yaml を比較する](#)」を参照して、yaml ファイルの関連セクションが更新されていることを確認してください。

開始する前に、CN-Series YAML ファイルのバージョンが PAN-OS バージョンと互換性があることを確認します。

- PAN-OS10.1.2 以降には YAML 2.0.2 が必要です
- PAN-OS10.1.0 および 10.1.1 には YAML 2.0.0 または 2.0.1 が必要です

## ローリング更新

このプロセスを使用すれば、まず CN-MGMT StatefulSet をアップグレードしてから、CN-NGFW ポッドをアップグレードすることができます。アプリケーショントラフィックの中断が最小限に抑えられます。これは、CN-MGMT StatefulSet のアップグレード中に CN-NGFW ポッドが機能し続け、CN-NGFW ポッドのローリング更新が一度に 1 つの CN-NGFW ポッドのインスタンスで発生するためです。

多数の CN-NGFW ポッドを含む大規模な Kubernetes クラスタを使用しており、短時間でアップグレードする必要がある場合は、CN-NGFW yaml を削除し、一度にすべての CN-NGFW ポッドをアップグレードするためのメンテナンス期間をスケジュールできます。

CN-MGMT のアップグレード中は、ロギングが影響を受けます。加えて、一時的なバージョンの不一致に関するメッセージが kubectl ログとシステム ログの両方で生成され、CN-NGFW ポッドと CN-MGMT ポッド間の接続が再開します。

**STEP 1 | CN-MGMT StatefulSet をアップグレードします。**

- 以下のいずれかのオプションを使用します。

- オプション 1 - pan-cn-mgmt.yaml 内でイメージ名を更新して、変更を適用します。

```
containers: - name: pan-mgmt image:<your-private-registry-image-path-new-image>
```

```
kubectl apply -f pan-cn-mgmt.yaml
```

- オプション 2 - kubectl を使用します。kubectlを使用する場合、yamlファイルを更新しないため、アップグレードに使用されるイメージを追跡する必要があります。

```
kubectl -n kube-system set image sts/pan-mgmt-sts pan-mgmt=<your-private-registry-image-path-new-image>
```

- CN-MGMT StatefulSet がデプロイされたことを確認します。

- kubectl -n kube-system get sts/pan-mgmt-sts -o wide** を使用します。
- アップグレードのステータスをチェックします。

```
kubectl exec -it pan-mgmt-sts-0 -n kube-system -- su admin
admin@pan-mgmt-sts-0> show jobs all
```

```
admin@pan-mgmt-sts-0.Basc-cluster-180>
show jobs all Enqueued Dequeued ID
PositionInQ Type Status Result Completed
-----
2020/08/25 14:11:11 14:11:11 2 AutoCom FIN OK 14:11:44
```

**STEP 2 | CN-NGFW ポッドをアップグレードします。**

- 以下のいずれかのオプションを使用します。

- オプション 1 - pan-cn-ngfw.yaml 内でイメージ名を更新して、変更を適用します。

```
containers: - name: pan-ngfw-container image:<your-private-registry-image-path-new-image>
```

```
kubectl apply -f pan-cn-ngfw.yaml
```

- オプション 2 - kubectl を使用します。kubectl を使用する場合、yaml ファイルを更新しないため、アップグレードに使用されるイメージを追跡する必要があります。
- DaemonSet デプロイメントとしての CN-Series では、次を使用します。

```
kubectl -n kube-system set image ds/pan-ngfw-ds pan-ngfw-
container=<your-private-registry-image-path-new-image>
```

- Kubernetes サービス展開としての CN-Series では、次を使用します。

```
kubectl -n kube-system set image deployment/pan-ngfw-dep
pan-ngfw-container=<your-private-registry-image-path-new-
image>
```

- アップグレードのステータスをチェックします。

**kubectl -n kube-system get ds/pan-ngfw-ds -o wide** を使用します。

Kubernetes サービス デプロイメントとしての CN-Series では、**kubectl -n kube-
system get deployment/pan-ngfw-dep -o wide** を使用します

### STEP 3 | イメージが PAN-OS バージョンに対して更新された場合にのみ必要 初期コンテナと pan-cni イメージを更新します。

- CN-MGMT ファイアウォール用の pan-cn-mgmt.yaml 内の初期コンテナ イメージを変更します。

```
initContainers: - name: pan-mgmt-init image:<your-private-
registry-image-path>
```

- pan-cni.yaml 内の PAN-CNI コンテナ イメージのイメージパスを編集します。

```
containers: name: install-pan-cni image:<your-private-
registry-image-path>
```

## 追加の CN-MGMT StatefulSet を使用したローリング更新

### STEP 1 | 作業を開始する前に。

- クラスタ内 のノードに追加の CN-MGMT StatefulSet に必要なメモリと CPU リソースが 挿っていることを確認してください。
- (静的にプロビジョニングされた PV の場合にのみ必要) 追加の CN-MGMT StatefulSet に 使用可能な PV が挿していることを確認してください。

pan-cn-pv-local.yaml によって、CN-MGMT をデプロイするために必要なディレクトリが 作成されます。

**STEP 2 |** 新しい pan-cn-mgmt-configmap.yaml をセットアップします。

上記で新しい pan-cn-mgmt.yaml に追加した値と一致するように PAN\_SERVICE\_NAME: の値を編集します。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: pan-ngfw-config
  namespace: kube-system
data:
  PAN_SERVICE_NAME: pan-mgmt-svc2
```

 *Panorama* での更新を減らすために、新しいファイル内の #Panorama 設定と # Intended License Bundle タイプの値は同じままにします。

**STEP 3 |** 新しい pan-cn-mgmt.yaml ファイルをセットアップします。

サービス名、アプリケーション、およびラベルを置き換える必要のある場所が複数あります。新旧の PAN-CN-MGMT.yaml を比較するを参照してください。

**STEP 4 |** イメージが PAN-OS バージョンに対して更新された場合にのみ必要 初期コンテナと pan-cni イメージを更新します。

CN-MGMT ファイアウォール用の pan-cn-mgmt.yaml 内の初期コンテナ イメージのイメージパス

```
initContainers: - name: pan-mgmt-init image: <your-private-registry-image-path>
```

CNI バイナリと各ノード上の CNI ネットワーク設定ファイルを含む PAN-CNI コンテナ イメージのイメージパス。

```
containers: name: install-pan-cni image: <your-private-registry-image-path>
```

**STEP 5 |** 新しい CN-MGMT yaml ファイルを適用します。

```
kubectl apply -f pan-cn-mgmt-configmap-new.yaml
```

```
kubectl apply -f pan-cn-mgmt-new.yaml
```

**STEP 6** | 新しい CN-MGMT StatefulSet がデプロイされたことを確認します。

```
kubectl -n kube-system get sts -o wide
```

NAME	READY	AGE	CONTAINERS	IMAGES
pan-mgmt-sts	2/2	16h	pan-mgmt	018147215560.dkr.ecr.ap-southeast-1.amazonaws.com/test/panos_ctnr/10.0.0/b/mp:63
pan-mgmt-sts-new	2/2	50m	pan-mgmt-new	018147215560.dkr.ecr.ap-southeast-1.amazonaws.com/test/panos_ctnr/10.0.1/b/mp:64

**STEP 7** | CN-NGFW ポッド yaml ファイルを新しいサービス名で編集します。

1. pan-cn-ngfw-configmap.yaml を更新します。

PAN\_SERVICE\_NAME を変更する場合： pan-cn-mgmt.yaml の Service name で定義した値と一致するように pan-cn-ngfw-configmap.yaml で参照されている値を変更すると、新しいイメージを使用するポッドが新しい StatefulSet に接続します。

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: pan-ngfw-config
  namespace: kube-system
data:
  PAN_SERVICE_NAME: pan-mgmt-svc2
```

2. pan-cn-ngfw-configmap.yaml をデプロイする

```
kubectl apply -f pan-cn-ngfw-configmap.yaml
```

3. pan-cn-ngfw.yaml で参照されているイメージパスを編集します。

たとえば、`kubectl set image ds/pan-cn-ngfw-ds -n kube-system pan-ngfw-container=018147215560.dkr.ecr.ap-southeast-1.amazonaws.com/test/panos_ctnr/10.0.2/b/dp:62` を使用できます。

4. ローリング更新のステータスをチェックします。

UP-TO-DATE 列に、正常に更新されたレプリカの数が表示されます。

```
kubectl get ds/pan-ngfw-ds -n kube-system -o wide
```

NAME	DESIRED	CURRENT	READY	UP-TO-DATE	AVAILABLE	NODE SELECTOR	AGE	CONTAINERS	IMAGES	SELECTOR
pan-ngfw	4	4	3	1	3	<none>	16h	pan-ngfw-container-018147215560.dkr.ecr.ap-southeast-1.amazonaws.com/test/panos_ctnr/10.0.0/b/dp:22	app=pan-ngfw	

**STEP 8 |** CN-NGFW ポッドがデプロイされたことを確認します。

```
kubectl -n kube-system get pods -l app=pan-ngfw
```

NAME	READY	STATUS	RESTARTS	AGE
pan-ngfw-ds-8b5gp	1/1	Running	0	40m
pan-ngfw-ds-h8xc6	1/1	Running	0	40m
pan-ngfw-ds-sn62b	1/1	Running	0	40m
pan-ngfw-ds-vxfqp	1/1	Running	0	40m

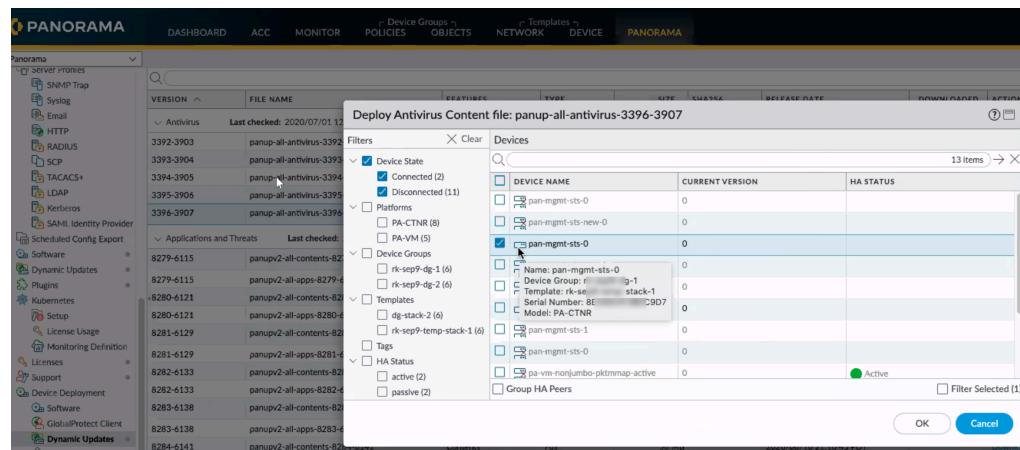
**STEP 9 |** CN-MGMT ポッドのシリアルナンバーを取得します。

```
kubectl exec -it pan-mgmt-sts-0 -n kube-system -- su admin
```

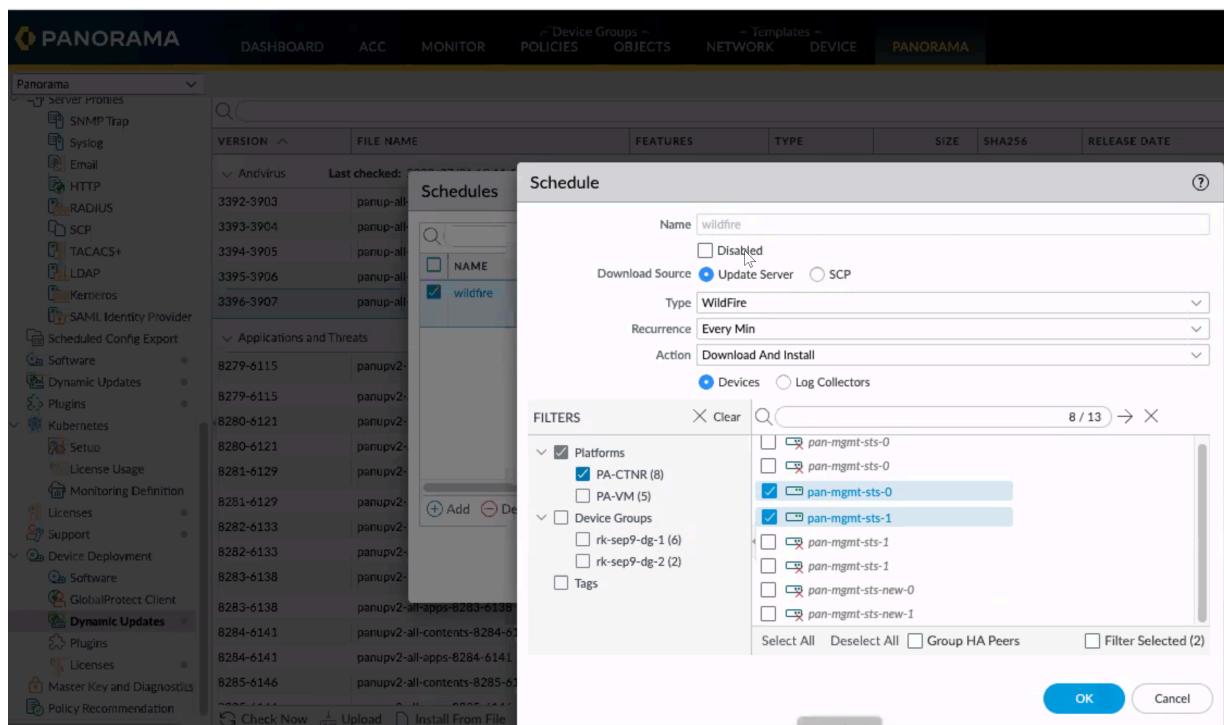
警告: デバイスは引き続きデフォルトの管理者アカウントの資格情報で設定されています。デプロイメント前にパスワードを変更してください。admin @pan-mgmt-sts-0>

## STEP 10 | 購入したサブスクリプションの動的コンテンツ更新をインストールします。

手動でインストールすることも、[スケジュール](#)をセットアップすることもできます。ダイナミック更新を行うポッドを選択する場合は、CN-MGMT ポッドのシリアルナンバーを確認してください。



または定期的なスケジュールを設定します。



## 新旧の PAN-CN-MGMT.yaml を比較する

新しい CN-MGMT StatefulSet をデプロイする場合は、yaml ファイル内のサービス名、アプリケーション、およびラベルを更新する必要のある複数の場所を確認します。

旧	新規
<pre> apiVersion: v1 kind:Service <b>metadata:</b> <b>name: pan-mgmt-svc</b> </pre>	<pre> apiVersion: v1 kind:Service <b>metadata:</b> <b>name: pan-mgmt-svc2</b> </pre>
<pre> namespace: kube-system <b>labels:</b> <b>app: pan-mgmt-svc</b> </pre>	<pre> namespace: kube-system <b>labels:</b> <b>app: pan-mgmt-svc2</b> </pre>
<pre> spec: ports: - protocol:UDP port:4500 name: ipsec <b>selector:</b> <b>appname: pan-mgmt-sts</b> </pre>	<pre> spec: ports: - protocol:UDP port:4500 name: ipsec <b>selector:</b> <b>appname: pan-mgmt-sts-new</b> </pre>
<pre> apiVersion: apps/v1 kind:StatefulSet <b>metadata:</b> <b>name: pan-mgmt-sts</b> </pre>	<pre> apiVersion: apps/v1 kind:StatefulSet <b>metadata:</b> <b>name: pan-mgmt-sts-new</b> </pre>
<pre> namespace: kube-system spec: selector: <b>matchLabels:</b> <b>appname: pan-mgmt-sts</b> <b>serviceName: pan-mgmt-svc</b> # レプリカはフォールトトレランス用で # す。Max 2 replicas supported. replicas:2 updateStrategy: type:RollingUpdate podManagementPolicy:Parallel template: </pre>	<pre> namespace: kube-system spec: selector: <b>matchLabels:</b> <b>appname: pan-mgmt-sts-new</b> <b>serviceName: pan-mgmt-svc2</b> # レプリカはフォールトトレランス用で # す。.Max 2 replicas supported. replicas:2 updateStrategy: type:RollingUpdate podManagementPolicy:Parallel template: </pre>

旧	新規
<p>metadata:</p> <p><b>labels:</b></p> <p>app: pan-mgmt</p> <p><b>appname: pan-mgmt-sts</b></p>	<p>metadata:</p> <p><b>labels:</b></p> <p>app: pan-mgmt</p> <p><b>appname: pan-mgmt-sts-new</b></p>
<p>labelSelector:</p> <p>matchExpressions:- key: "appname"</p> <p>operator:In</p> <p><b>values:</b></p> <p><b>pan-mgmt-sts</b></p>	<p>labelSelector:</p> <p>matchExpressions:- key: "appname"</p> <p>operator:In</p> <p><b>values:</b></p> <p><b>pan-mgmt-sts-new</b></p>
<p>topologyKey: "kubernetes.io/hostname"</p> <p>initContainers:</p> <ul style="list-style-type: none"> <li>- name: pan-mgmt-init</li> </ul> <p>mountPath: /var/log/pan/</p> <p>envFrom:</p> <p><b>configMapRef:</b></p> <p><b>name: pan-mgmt-config</b></p>	<p>topologyKey: "kubernetes.io/hostname"</p> <p>initContainers:</p> <ul style="list-style-type: none"> <li>- name: pan-mgmt-init</li> </ul> <p>mountPath: /var/log/pan/</p> <p>envFrom:</p> <p><b>configMapRef:</b></p> <p><b>name: pan-mgmt-new-config</b></p>
<p># sw-secret in pan-cn-ngfw.yaml and hard-coded in ipsec.conf</p> <p>value: pan-fw</p> <p><b>containers:</b></p> <p>name: pan-mgmt</p> <p><b>image:018147215560.dkr.ecr.ap-southeast-1.amazonaws.com/test/panos_ctnr/10.0.0/b/mp:63</b></p>	<p># sw-secret in pan-cn-ngfw.yaml and hard-coded in ipsec.conf</p> <p>value: pan-fw</p> <p><b>containers:</b></p> <p>name: pan-mgmt-new</p> <p><b>image:018147215560.dkr.ecr.ap-southeast-1.amazonaws.com/test/panos_ctnr/10.0.1/b/mp:64</b></p>
<p>volumes</p> <p>name: dshm</p> <p>envFrom:</p> <p><b>configMapRef:</b></p> <p><b>name: pan-mgmt-config</b></p>	<p>volumes</p> <p>name: dshm</p> <p>envFrom:</p> <p><b>configMapRef:</b></p> <p><b>name: pan-mgmt-new-config</b></p>

# CN-Series ファイアウォールのアップグレード — 再デプロイ

どこで使用できますか?	何が必要ですか?
<ul style="list-style-type: none"> <li>• CN-Series アップグレード</li> <li>• CN-Series デプロイメント</li> </ul>	<ul style="list-style-type: none"> <li>• CN-Series 10.1.x or above Container Images</li> <li>• PanoramaPAN-OS 10.1.x 以降のバージョンを実行している</li> </ul>

このオプションを使用すれば、更新した PAN-OS バージョン (サポートされている PAN-OS バージョンへのアップグレードまたはダウングレード) を使用して CN-Series ファイアウォールを新たにデプロイすることができます。このワークフローは、2つのオプションのうちの簡単な方ですが、若干のダウンタイムが必要です。

1. [既存の CN-Series ファイアウォール デプロイメントを削除する](#)
2. [CN-Series Docker イメージを更新する](#)
3. [CN-Series ファイアウォールのデプロイ](#)

開始する前に、CN-Series YAML ファイルのバージョンが PAN-OS バージョンと互換性があることを確認します。

- PAN-OS 10.1.2 以降には YAML 2.0.2 が必要です
- PAN-OS 10.1.0 および 10.1.1 には YAML 2.0.0 または 2.0.1 が必要です

## 既存の CN-Series ファイアウォール デプロイメントを削除する

**STEP 1 |** 既存の CN-MGMT ポッドと CN-NGFW ポッドを削除します。

1. `kubectl delete -f pan-cn-mgmt.yaml`
2. `kubectl delete -f pan-cn-ngfw.yaml`

**STEP 2 |** ポッドが削除されたことを確認します。

1. `kubectl get pods -n kube-system -l app=pan-mgmt`
2. `kubectl get pods -n kube-system -l app=pan-ngfw`

**STEP 3 |** 既存の永続ボリューム クレーム (PVC) と永続ボリューム (PV) を削除する

1. **kubectl -n kube-system get pvc -l appname=pan-mgmt-sts** を使用して、pan-cn-mgmt.yaml に関連付けられたすべての PVC と PV を探します。

**pan-mgmt-sts** は、CN-MGMT ポッド用のデフォルトの appname セレクタです。別の名前を指定するように yaml を変更した場合は、一致するように appname を置き換える必要があります。EKS からのサンプル出力を以下に示します。

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
panconfig-pan-mgmt-sts-0	Bound	pvc-<id>	8Gi	RW0	gp2	15h
panconfig-pan-mgmt-sts-1	Bound	pvc-<id>	8Gi	RW0	gp2	15h
panlogs-pan-mgmt-sts-0	Bound	pvc-<id>	20Gi	RW0	gp2	15h
panlogs-pan-mgmt-sts-1	Bound	pvc-<id>	20Gi	RW0	gp2	15h
panplugincfg-pan-mgmt-sts-0	Bound	pvc-<id>	1Gi	RW0	gp2	15h
panplugincfg-pan-mgmt-sts-1	Bound	pvc-<id>	1Gi	RW0	gp2	15h
panplugins-pan-mgmt-sts-0	Bound	pvc-<id>	1Gi	RW0	gp2	15h
panplugins-pan-mgmt-sts-1	Bound	pvc-<id>	1Gi	RW0	gp2	15h
varcores-pan-mgmt-sts-0	Bound	pvc-<id>	20Gi	RW0	gp2	15h
varcores-pan-mgmt-sts-1	Bound	pvc-<id>	20Gi	RW0	gp2	15h
varlogpan-pan-mgmt-sts-0	Bound	pvc-<id>	20Gi	RW0	gp2	15h
varlogpan-pan-mgmt-sts-1	Bound	pvc-<id>	20Gi	RW0	gp2	15h



- 静的にプロビジョニングされた PV(オンプレミス デプロイメントで使用されることが多い)の場合、それを削除するには、pan-cn-pv-local.yaml ファイルと、CN-MGMT ポッドをホストしている各ノードに関するデータが格納されたディレクトリを明示的に削除する必要があります。

コマンド **rm -rf /mnt/pan-local1/\*** を使用して、pan-local 1 ~ 6 の PV を削除します。

- マネージド サービス/クラウド プラットフォームなどの動的にプロビジョニングされた PV の場合は、PVC を削除すると、PV が自動的に削除されます。

## CN-Series Docker イメージを更新する

**STEP 1 |** アップグレードするバージョンの新しいイメージをコンテナ レジストリにアップロードします。

CNシリーズ デプロイメント用にイメージとファイルを取得するを参照してください。

## CN-Series ファイアウォールのアップグレード

---

**STEP 2 |** CN-MGMT yaml ファイルと CN-NGFW yaml ファイルでイメージとイメージパスを更新します。

pan-cn-ngfw.yaml 内の CN-NGFW コンテナ イメージのイメージパス

```
containers: - name: pan-ngfw-container image: <your-private-registry-image-path>
```

pan-cn-mgmt.yaml 内の CN-MGMT コンテナ イメージのイメージパス

```
CN-MGMT イメージコンテナーのイメージパス: - name: pan-mgmt image: <your-private-registry-image-path>
```

**STEP 3 |** イメージが PAN-OS バージョンに対して更新された場合にのみ必要 初期コンテナと pan-cni イメージを更新します。

CN-MGMT ファイアウォール用の pan-cn-mgmt.yaml 内の初期コンテナ イメージのイメージパス

```
initContainers: - name: pan-mgmt-init image: <your-private-registry-image-path>
```

pan-cni.yaml 内の PAN-CNI コンテナ イメージのイメージパス

```
containers: name: install-pan-cni image: <your-private-registry-image-path>
```

## CN-Series ファイアウォールのデプロイ

YAMLファイルの詳細とセットアップに関する情報については、[CNシリーズ デプロイメントの YAML ファイル内に編集可能なパラメータ](#) および [CNシリーズ デプロイメントの前提条件](#) を参照してください。

pan-cn-mgmt.yaml と pan-cn-ngfw.yaml は、CN-Series ファイアウォールを再デプロイするために必要です。他の yaml ファイルは変更したときにのみ再デプロイする必要があります。デプロイでは、pan-cni.yaml、pan-cn-mgmt.yaml、pan-cn-ngfw.yaml の順にデプロイします。

**STEP 1 |** yaml ファイルをデプロイします。

1. これらのファイルを変更した場合にのみ必要:

```
kubectl apply -f pan-cn-mgmt-configmap.yaml
kubectl apply -f pan-cn-mgmt-secret.yaml
kubectl apply -f pan-cn-mgmt-slot-cr.yaml
kubectl apply -f pan-cn-mgmt-slot-crd.yaml
kubectl apply -f pan-cn-ngfw-configmap.yaml
kubectl apply -f pan-cn-ngfw-svc.yaml
kubectl apply -f pan-cn-storage-class.yaml
kubectl apply -f pan-cni-configmap.yaml
kubectl apply -f pan-cni-serviceaccount.yaml
kubectl apply -f plugin-serviceaccount.yaml
kubectl apply -f pan-mgmt-serviceaccount.yaml
```

2. PV を静的にプロビジョニングした場合にのみ必要:

```
kubectl apply -f pan-cn-pv-local.yaml
```

3. pan-cni.yaml を変更した場合にのみ必要:

```
kubectl apply -f pan-cni.yaml
```

このコマンドは、ローリング更新をトリガーします。pan-cni daemonset が一度に 1 つのノードずつ更新されます。



cni が再起動してノードで使用可能になるまでに 30 ~ 40 秒かかります。この再起動では、実行中のアプリケーション ポッドと CN-NGFW ポッドに対する影響はありません。この期間にノード上で開始した新しいアプリケーション ポッドからのトラフィックは CN-NGFW ポッドによって保護されません。

4. **kubectl apply -f pan-cn-mgmt.yaml**
5. **kubectl apply -f pan-cn-ngfw.yaml**

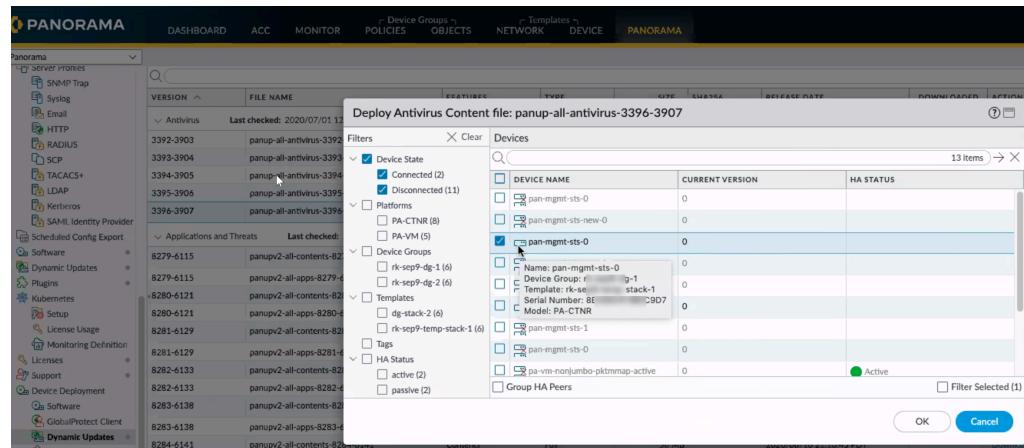
**STEP 2 |** CN-MGMT ポッドのシリアル ナンバーを取得します。

```
kubectl exec -it pan-mgmt-sts-0 -n kube-system -- su admin
```

警告: デバイスは引き続きデフォルトの管理者アカウントの資格情報で設定されています。デプロイメント前にパスワードを変更してください。admin @pan-mgmt-sts-0>

### STEP 3 | 購入したサブスクリプションの動的コンテンツ更新をインストールします。

手動でインストールすることも、[スケジュール](#)をセットアップすることもできます。ダイナミック更新を行うポッドを選択する場合は、CN-MGMT ポッドのシリアルナンバーを確認してください。



または定期的なスケジュールを設定します。

