paloalto
TECHDOCS

CNシリーズのトラブルシューティング

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
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.
- To search for a specific topic, go to our search page 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.

Copyright

Palo Alto Networks, Inc.
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. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

December 13, 2021

Table of Contents

CNシリーズ トラブルシューティング 5

MPまたはDPに接続 6

Podが以下のエラーで画像のプルに失敗します 7

MPは保留中状態のままです 8

MPがクラッシュし続ける 10

K8 MPのログに以下のエラーが表示されます 11

MPがPanoramaへの接続に失敗、またはMP CommitAllの失敗 12

CommitAllがMPで起動しない 14

DPポッドは保留中またはコンテナ作成中の状態で維持されます 16

MP:Panoramaの詳細/ステータスが表示されない 17

PanoramaがMPを管理対象デバイスとして表示していません 18

DPスロットの登録に失敗しています 20

"k8 get pods -n kube-system"を行うとMP/DP/CNIポッドが表示されません 21

セキュア アプリケーション ポッドからのトラフィックがDP/ファイアウォール経由で送信されない 22

トラフィックを処理しているDPポッドを確認する方法 25

ロギング:Panoramaがトラフィック/脅威ログを表示していません。 26

ロギング:ルール名でフィルタリングするとPanoramaにログが表示されません 27

MPがPanoramaへの再接続に失敗します 28

MPとDPはアクティブで実行中の状態ですが、IPsecはMPとDPの間で終了します 29

ImagePullBackOff 30

ns-panwネームスペースで実行されているワーカーノードからDPにログイン 31

DPポッドが**ContainerCreating**ステータスのままになり、以下のkubectlログが表示されます 32

CNv2が保護するApp pod上のリンク ステータス(vxlanを使用) 33

MPからテクニカルサポートをキャプチャ 34

HPAが動作しない 35

OpenShiftでアプリケーションへのインバウンドアクセスを制御するには？ 36

CNシリーズをアンデプロイする 37

CNでのパケット診断を有効化します 38

MPとDP間のIPSecがエラー非対称状態で失敗します 39

アプリケーション ポッドがDNS解決に失敗します(ファイアウォールの有無にかかわらず) 43

 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

CNシリーズ トラブルシューティング

どこで使用できますか?	何が必要ですか?
• CN-Seriesデプロイメント	• CN-Series 10.1.x or above Container Images • PanoramaPAN-OS 10.1.x以降のバージョンを実行している

表 **1 :** 用語の定義**:**

用語	定義
MP	CN-MGMT
DP	CN-NGFW

MPまたはDPに接続

MPまたはDPポッド名を確認するには、以下のコマンドを実行します。

kubectl get pods -n=<namespace>

MPまたはDPポッドに接続するには、以下のコマンドを実行します。

Kubectl -n kube-system exec -it <mp-pod-name> -- su admin

Kubectl -n kube-system exec -it <mp/dp-pod-name> -- bash

©2024 Palo Alto Networks, Inc.

Podが以下のエラーで画像のプルに失敗します

x509: 不明な機関によって署名された証明書 **(**主にネイティブ/オンプレミスの **k8** クラスターで見られる**)**

すべてのワーカー ノードで、プル元のイメージ リポジトリで**/etc/docker/daemon.json**を更新します。daemon.jsonファイルが存在しない場合は作成します

```
root@ctnr-debug-worker-2:~# cat /etc/docker/daemon.json { "insecure-
registries" : ["docker-panos-ctnr.af.paloaltonetworks.local",
 "panos-cntr-engtools.af.paloaltonetworks.local",
 "docker-public.af.paloaltonetworks.local", "panos-cntr-
engtools-releng.af.paloaltonetworks.local", "docker-qa-
pavm.af.paloaltonetworks.local"] } root@ctnr-debug-worker-2:~#
```

コマンド**"systemctl restart docker.service"**でDockerを再起動します。

©2024 Palo Alto Networks, Inc.

MPは保留中状態のままです

以下を確認してください。

1. 必要なリソース(ノード/メモリ/CPU)はMPポッドで使用できます。以下のコマンド出力を確認することで検証できます

   kubectl -n kube-system describe<mp-pod-name>

```
                 node.kubernetes.io/unreachable:NoExecute op=Exists for 300s
Events:
  Type     Reason            Age                  From               Message
  ----     ------            ----                 ----               -------
  Warning  FailedScheduling  101s (x551 over 13h)  default-scheduler  0/1 nodes are available: 1 Insuf
test@mks-test-181:~$
```

2. PV(PersistentVolume)は、サーバ/ストレージ/クラスタ管理者によってプロビジョニングされた、またはストレージクラスを使用して動的にプロビジョニングされたクラスタ内のストレージです。nodeと同様のクラスタ内のリソースです。PersistentVolumeClaim(PVC)は、PVから取得できるユーザによる保存要求である。

   PVCはPVにバインドされます(`kubectl -n kube-system get pvc`)。そうでない場合は、以下のコマンドを実行している古いpvcsを削除します。

```
 "kubectl -n kube-system delete pvc -l appname=pan-mgmt-sts-
<whatever>"
```

3. 必要なディレクトリ (/mnt の下の pan-local1、pan-local2、pan-local3、pan-local4、pan-local5、pan-local6) が、オンプレミス セットアップ用の少なくとも 2 つのワーカー ノードに作成されているかどうかを確認します。

   `/mnt`の下の`Pan-local1`、`Pan-local2`、`Pan-local3`、`Pan-local4`、`Pan-local5`、`Pan-local6`は、動的ボリュームプロビジョニングには必要ありません。MPが保留状態のままになる原因の1つは、AWS EKSでEBS CSIドライバが見つからないことです。EBS CSIドライバがクラスタで有効になっていることを確認し、ロールを確認し、クラスタのプロバイダを特定する必要があります。詳しくは、Amazon EKSアドオンとしてのAmazon EBS CSIドライバーの管理を参照してください。

4. エラーが"`pan-mgmt-sts-0`": pod has unbound immediate PersistentVolumeClaims"exec"**kubectl get pvcs -o wide**"と"**kubectl get pv -o wide**"の場合、どのpvcがバインドに失敗したかが分かります。

   解決策は、コマンド**kubectl -n kube-system delete pvc/<pvc-name>**を使用して古いPVCを削除するか、クリーンアップすることです。PVC、PVをすべて削除します。新しいPVをデプロイし、MPをデプロイします。

©2024 Palo Alto Networks, Inc.

5. **"k8 describe pod <mp-pod>"**が以下でエラーアウトした場合はPVが作成されていることを確認してください。作成されていない場合は、pan-cn-pv-local.yamlをデプロイします(ディレクトリが設定されているノード名を使用)。

   "ポッド**"pan-mgmt-sts-0"**の**"VolumeBinding"**フィルター プラグイン: ポッドにバインドされていないPersistentVolumeClaims

   警告FailedSchedulingがあります<unknown>ポッド**"pan-mgmt-sts-0"**の**"VolumeBinding"**フィルター プラグインを実行しているデフォルト スケジューラ: ポッドにはバインドされていないPersistentVolumeClaimsがあります

6. ```
   lnehru@lnehru-parts-vm:~/cnv1/Kubernetes/pan-cn-k8s-daemonset/eks$
    k8l pan-mgmt-sts-0
   ```

   ```
   12-22-2021 11:34:36.961697 PST INFO:PanOSバージョン10.1.3-c47
   ```

   12-22-2021 11:34:41.335521 PSTエラーの実行を開始する管理コンテナ**:pansw** の起動に失敗しました**:2**

   "pan-cn-mgmt-configmap.yaml"に必須の値がないことが問題だと考えられます。

©2024 Palo Alto Networks, Inc.
   ```

MPがクラッシュし続ける

MPルートにログインして**/var/cores**に移動し、クラッシュしているプロセスを確認します。

©2024 Palo Alto Networks, Inc.

K8 MPのログに以下のエラーが表示されます

デバイスの登録要求に失敗しました**:CSP**サーバーへの要求の送信に失敗しました

以下を確認してください。

1. "Pan-cn-mgmt-secret.yaml"は、以下の2つのフィールド以下の正しい値を持つ必要があります。CN-SERIES-AUTO-REGISTRATION-PIN-ID: "<PIN Id>"

   CN-SERIES-AUTO-REGISTRATION-PIN-VALUE:"<PIN-Value>"
2. 上記の値が正しければ、CSPからPinIDとValueの有効期限が切れていないことを確認します

©2024 Palo Alto Networks, Inc.

MPがPanoramaへの接続に失敗、またはMP CommitAllの失敗

1. MPが/ping Panorama IPに到達できることを確認します。パブリック クラウドの場合、PanoramaとK8sクラスタ間の接続を有効にするために必要なセキュリティ ポリシーが設定されていることを確認します。

   mpにログインします：

   - 1. Kubectl -n kube-system exec -it <mp-pod-name> -- su admin
     2. PanoramaのIPアドレスを取得するために"Panoramaのステータスを表示する"
     3. pingホスト<panorama-ip>
     4. pingが成功すれば、以下の検証に進みます
2. mgmt-secret.yamlで提供されるブートストラップ認証キーが Panorama に存在し、有効期限が切れていないことを確認します。
   1. bootstrap-auth-keyを検証するには、Panoramaにログインしてコマンド"request bootstrap vm-auth-key show"を実行します(このコマンドは期限切れではなく、有効である必要があります)
   2. 有効ではない場合は 、"request bootstrap vm-auth-key generate lifetime 8760"を使用して生成し、pan-mgmt-secret.yamlで更新します。すべてのyaml をアンデプロイし、PV、PVCをクリアして再デプロイします。
3. mgmt-configmap.yamlで設定された DG、TSおよびコレクター グループ(CG)のスペルが間違っていないこと、およびPanoramaで設定およびコミットされていることを確認します。
4. mgmt.yammgmt.yamlの前にpan-mgmt-configmapとsecret yamlsがデプロイされていることを確認します。mgmt.yammgmt.yamlの前にpan-mgmt-configmapとsecret yamlsがデプロイされていることを確認します。
5. "show jobs all"および"show job id"<id>のコマンドを使用してMP 上の Panorama からのcommit-all が成功したかどうかを確認し、失敗の有無を確認してPanorama の設定に必要な修正を加え、すべてをコミット/強制的に再度実行します。
6. Panorama設定が"show config pushed-shared-policy"のMPにプッシュされます
7. cmd"debug tac-login response"と入力してrootからPanorama上のconfigd.logを探し、MPシリアルナンバーで検索します。接続失敗の理由が表示されます。

   vi /var/log/pan/configd.log

   例:

```
2021-03-15 14:19:49.213 -0700 Error:
 pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4085):
 bootstrap: template stack cnv2-template-stack
 not found, serial=8CABD801686AD2021-04-15
 14:19:49.213 -0700 bootstrap: candidate cfg ch Error:
```


©2024 Palo Alto Networks, Inc.

```
pan_cfg_bootstrap_vm_auth_key_verify(pan_cfg_bootstrap_mgr.c:3822):vm_auth_k
923688689426978とvm_auth _key invalidが見つかりませんでした。
```


©2024 Palo Alto Networks, Inc.

CommitAllがMPで起動しない

CommitAllのジョブがスタック/ACTの状態かどうかPanoramaで検証します。

MPとPanoramaの間のネットワーク接続の問題が原因で発生する可能性があります。

Labでは、MP/worker-nodeとPanoramaを同じサブネットに置くことでこの問題は解決されます。

上記の問題に当たると以下のPanoramaログが見られます。

```
2023-01-19 09:13:51.788 -0800 Error:
 device_needs_bkup(pan_bkup_mgr.c:323): failed to check out /opt/
pancfg/mgmt/devices/8B8AE8CB506CF09/running-config.xml 2023-01-19
 09:13:51.938 -0800 Panorama push device-group cn-dg-12c13c51-1
 for device 8B8AE8CB506CF09 with merge-with-candidate-cfg include-
template flags set.JobId=50860.User=pano rama.Dequeue time=2023/01/19
 09:13:51. 2023-01-19 09:13:52.812 -0800 Preference list thread was
 spawned to send to device 8B8AE8CB506CF09 in group CG 2023-01-19
 09:13:52.812 -0800 Preference list thread was sent to device
 8B8AE8CB506CF09 2023-01-19 09:13:52.813 -0800 DAU2:Will clear
 all addresses on dev:8B8AE8CB506CF09.2023-01-19 09:14:35.061
 -0800 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr:Expired Request. entry:916, msgno=3
 devid=8B8AE8CB506CF09 2023-01-19 09:14:35.061 -0800
 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr:Expired Request. entry:916, msgno=6
 devid=8B8AE8CB506CF09 2023-01-19 09:14:35.061 -0800
 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr:Expired Request. entry:916, msgno=4
 devid=8B8AE8CB506CF09 2023-01-19 09:15:05.060 -0800
 Error: pan_conn_mgr_callback_expiry_async(cs_conn.c:8781):
 connmgr:Expired Request. entry:916, msgno=0
 devid=8B8AE8CB506CF09 2023-01-19 09:15:05.060 -0800 Error:
 pan_conn_mgr_callback_expiry_async(cs_conn.c:8781): connmgr:Expired
 Request. entry:916, msgno=5 devid=8B8AE8CB506CF09 2023-01-19
 09:15:05.060 -0800 copy-lcs-pref-list:Response Processor: copy
 lcs pref job received response from device 8B8AE8CB506CF09 of
 cookie 2407.現在のクッキーは2408です。残:1 2023-01-19 09:15:05.060
 -0800 copy-lcs-pref-list:レスポンスプロセッサ: copy lcs pref jobは
クッキー2408のデバイス8B8AE8CB506CF09から応答を受け取りました。現在
のクッキーは2408です。残:1 2023-01-19 09:15:05.060 -0800 Error:
 pan_async_copy_lcs_pref_list_result(pan_comp_collector.c:2761):2023-01-19
 09:15:05.060 -0800 copy-lcs-pref-list:Failed to
 receive response fro m device 8B8AE8CB506CF09.Error
 - time out sending/receiving message Error:
 pan_async_copy_lcs_pref_list_result(pan_comp_collector.c:2761):
 copy-lcs-pref-list:Failed to receive response from device
 8B8AE8CB506CF09.Error - time out sending/receiving message
 2023-01-19 09:15:08.545 -0800 connmgr: received disconnect cb
 from ms for 8B8AE8CB506CF09(1020484) 2023-01-19 09:15:08.545
 -0800 connmgr: connection entry removed. devid=8B8AE8CB506CF09
 sock=4294967295 result=0 2023-01-19 09:15:08.545 -0800 Handling
 device conn update [disconnection][activated:1] for 8B8AE8CB506CF09:
 "server: client is device" 2023-01-19 09:15:08.545 -0800 Error:
```


©2024 Palo Alto Networks, Inc.

```
 pan_bkupjobmgr_process_async_result(pan_bkup_mgr.c:208):Failed
 to receive response from device 8B8AE8CB506CF09.Error -
 failed to send message 2023-01-19 09:15:08.545 -0800 Error:
 pan_async_lcs_pref_list_result(pan_comp_collector.c:2681): lcs-pref-
list:Failed to receive response from device 8B8AE8CB506CF09.Error
 - failed to send message 2023-01-19 09:15:08.546 -0800
 Panorama HA feedback:8B8AE8CB506CF09 disconnected 2023-01-19
 09:15:08.547 -0800 connmgr: connection entry removed.
 devid=8B8AE8CB506CF09 (1020484) 2023-01-19 09:15:41.212 -0800
 Warning: _register_ext_validation(pan_cfg_mgt_handler.c:4418):
 reg: device '8B8AE8CB506CF09' not using issued
 cert.2023-01-19 09:15:41.213 -0800 Warning:
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4737):SC3: device
 '8B8AE8CB506CF09' is not SC3 capable 2023-01-19 09:15:41.213
 -0800 SVM registration.Serial:8B8AE8CB506CF09 DG:cn-dg-12c13c51-1
 TPL:cn-tmplt-stk-12c13c51-1 vm-mode:0 uuid:4b96eccd-9d66-43b1-
a3f3-2318f3e5b2fd cpuid:K8SM P:A6D64F:8410079617204080582:
 svm_id:2023-01-19 09:15:41.213 -0800 Error:
 pan_cfg_bootstrap_device_add_to_cfg(pan_cfg_bootstrap_mgr.c:4020):
 bootstrap:8B8AE8CB506CF09は既にmgdデバイスに追加されています
```


©2024 Palo Alto Networks, Inc.

DPポッドは保留中またはコンテナ作成中の状態で維持されます

以下のコマンドを実行し、それぞれのコマンドの出力に記載されているエラーを確認し、修正します

1. kubectl -n kube-system describe pod<dp-pod-name>。

   以下のコマンドの一部として以下のエラーが表示される場合は、引き続きCNIログを探し、CNIがマルチタスを使用しているかどうかを確認してください。

   ```
   MountVolume.SetUp failed for volume "pan-cni-ready" : hostPath
    type check failed: /var/log/pan-appinfo/pan-cni-ready is not a
    directory
   ```

2. Kubectl -n kube-system logs <dp-pod-name>
3. kubectl -n kube-system describe pod <cni-name-on-same-node>
4. Kubectl -n kube-system logs <cni-name-on-same-node>
5. 以下のようにkubectl CNIがログを取る場合は、各ノードでCNIが実行されていることを確認してください。(GKEクラスタでは、デフォルトCNiを実行するためにネットワーク ポリシーを有効にする必要があります):

   ```
   08-18-2022 23:55:07.397661 UTC DEBUG:PAN CNI config:
    { "name": "pan-cni", "type": "pan-cni", "log_level": "debug",
    "appinfo_dir": "/var/log/pan-appinfo", "mode": "service",
    "dpservicename": "pan-ngfw-svc", "dpservicenamespace":
    "kube-system", "firewall": [ "pan-fw" ], "interfaces":
    [ "eth0" ], "interfacesip": [ "" ], "interfacesmac": [ "" ],
    "override_mtu": "", "kubernetes": { "kubeconfig": "/etc/cni/
   net.d/ZZZ-pan-cni-kubeconfig", "cni_bin_dir": "/opt/cni/bin",
    "exclude_namespaces": [], "security_namespaces": [ "kube-
   system" ] }} 08-18-2022 23:55:07.402812 UTC DEBUG:FWサービス モードでCNIを実行中。Bypassfirewallはアプリケーション ポッドで有効化できます08-18-2022 23:55:07.454392 UTC CRITICAL:MultusをプライマリCNIとして検出(CONF file 00-multus.conf);non-MultusのCNIがプライマリCNIになるのを待機中。root@manojmaster:~/pan-cn-k8s-service/native#
   ```

   上記のエラーが表示される場合は、Multusのアンデプロイを試し、このCNIとDPsがデプロイされているワーカーノードから00-multus.confファイルを削除してください

   ```
   root@manojworker1:/etc/cni/net.d# pwd /etc/cni/net.d
    root@manojworker1:/etc/cni/net.d# rm 00-multus.conf
   ```


©2024 Palo Alto Networks, Inc.

MP:Panoramaの詳細/ステータスが表示されない

```
admin@PA-CTNR> show panorama-status admin@PA-CTNR> [root@PA-CTNR / ]
 # cat /opt/pancfg/mgmt/bootstrap/init-cfg.txt.20210527 type=static
 netmask=255.255.255.0 cgname=CG tplname=10_3_252_62-CNv2 ip-
address=10.233.99.17 default-gateway=10.233.99.1 dgname=10_3_252_62-
CNv2 panorama-server=107.21.240.64 hostname=pan-mgmt-sts-0 vm-auth-
key=158251502922307 [root@PA-CTNR / ] #
```

1. pan-cn-mgmt.yamlの後にpan-cn-mgmt-configmapがデプロイされている可能性があります
2. pan-cn-mgmt-secretデプロイメント失敗の可能性（bootstrap-auth-keyが"0"で始まるため失敗している可能性あり）→Panoramaから認証キーを削除して"0"で始まらないように再度作成してください

解決するには、MPをアンデプロイし、PVCとPVを削除し、mp-configmapを再度デプロイした後、MPもデプロイします。

HELMチャートを使用してデプロイする場合：

この問題を解決するには、HELM チャートをアンデプロイし、CNシリーズのPVC/PV を削除してから、HELM を再度デプロイします。

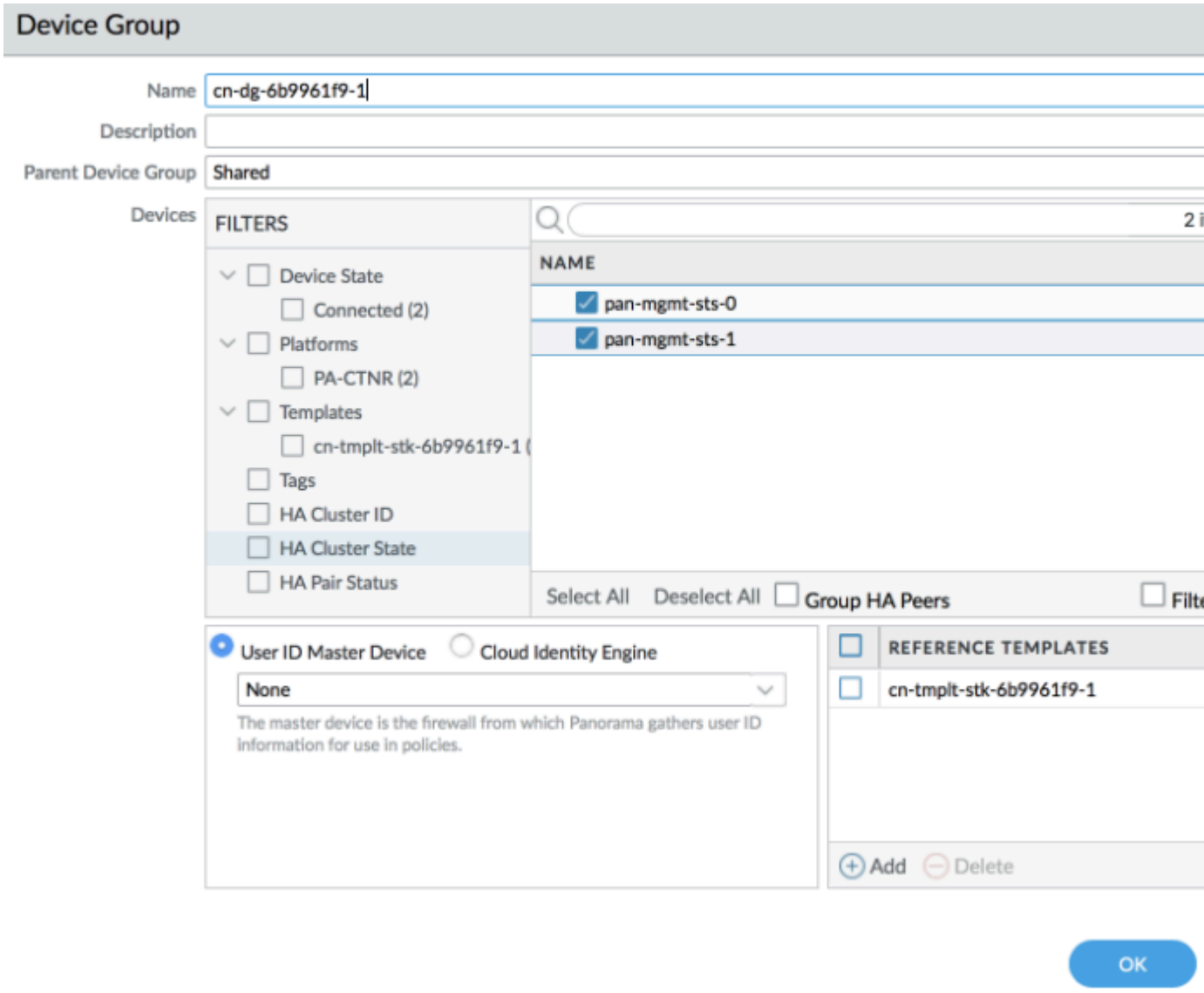
©2024 Palo Alto Networks, Inc.

PanoramaがMPを管理対象デバイスとして表示していません

1. MPとDPが同じSWバージョンであることを確認してください。同じバージョンではない場合、MP上の"K8ログがエラーログを出力します。
2. mgmt-slot-crdとmgmt-slot-cr.yamlがデプロイされている場合。
3. このDPがいずれかのMPに対してIPSecを確立している場合rootを使ってMPにログインし、コマンド"ipsec status"で確認します。
4. AutoCommitとCommitAllは、このDPが接続されているMPを既に渡しているはずです。そうでない場合は、CommitAllまたはAutoCommitが失敗した理由をMPで確認し、それに応じて修正します。上記の手順（MPがPanoramaへの接続に失敗する、またはMP CommitAllの失敗）を参照して解決してください。
5. admin@pan-mgmt-sts-0＞ debug内部インターフェースをすべて表示→インターフェース設定を表示する必要があります。表示されない場合は、テンプレート スタックがDGで参照されてい

©2024 Palo Alto Networks, Inc.

ることを確認してください。また、K8S-Network-templateにインターフェースの設定があることを確認してください。



6. DPに4Gigメモリがある場合は、ngfw.yamlファイルをチェックインしてください。
7. コマンド"masterd all status"を実行してmasterd all processが実行されている。
8. "Ps -aef"動作しているプロセスを確認します。
9. 以下のコマンドの出力を確認し、DPスロットの登録エラーがあるかどうかを確認します:

```
”kubectl get panslotconfigs -n kube-system --insecure-skip-tls-
verify -o yaml"
```


©2024 Palo Alto Networks, Inc.

DPスロットの登録に失敗しています

1. pan-cn-mgmt-slot-crおよびcrd.yamls がデプロイされていることを確認します。
2.
```
[root@rk-cl3-master-1 native-2]# k8sys get PanSlotConfig NAME AGE
 pan-mgmt-svc-2-slots 13s pan-mgmt-svc-slots 11d [root@rk-cl3-
master-1 native-2]#
```
3.
```
[root@rk-cl3-master-1 native-2 ] # k8sys get crd | grep
 pan NAME CREATED AT panslotconfigs.paloaltonetworks.com
 2022-11-10T04:18:13Z [root@rk-cl3-master-1 native-2 ] #
```

```
11-21-2022 20:54:31.783302 UTC INFO:Masterd Started 11-21-2022
 20:54:40.050008 UTC INFO:IPSec up-client event with 169.254.202.2
 11-21-2022 20:54:40.121502 UTC INFO:Calling dp slot register
 script 11-21-2022 20:54:40.323061 UTC WARNING:準備状況:準備がで
きていません。Panoramaの設定がプッシュされていません。pan_taskが実行さ
れていません。11-21-2022 20:54:40.486734 UTC INFO:Strongswanデー
モンが起動。management plane(管理プレーン - MP)に到達しようとしてい
る....11-21-2022 20:54:41.623966 UTC INFO:management plane(管理
プレーン - MP)の接続が確立されました。11-21-2022 20:54:42.700770 UTC
 ERROR:登録/再登録に失敗しました:USER 11-21-2022 20:54:42.818729
 UTC WARNING: dpスロットの登録に失敗しました。Retrying a few times
 11-21-2022 20:54:44.265372 UTC ERROR:登録/再登録に失敗しました:USER
 11-21-2022 20:54:45.759982 UTC ERROR:登録/再登録に失敗しました:USER
 11-21-2022 20:54:47.256744 UTC ERROR:登録/再登録に失敗しました:USER
 11-21-2022 20:54:48.768491 UTC ERROR:登録/再登録に失敗しました:USER
 11-21-2022 20:54:50.272969 UTC ERROR:登録/再登録に失敗しました:USER
 11-21-2022 20:54:51.390138 UTC CRITICAL:MPへの登録に失敗しました。DPを
シャットダウンします
```


©2024 Palo Alto Networks, Inc.

"k8 get pods -n kube-system"を行うとMP/DP/CNIポッドが表示されません

1. "sa.yaml"がデプロイされていないため 、"Service-account"が作成されていない可能性を確認します。
2. mpサービスがコマンド"k8 -n kube-system get svc"を使用して実行されていることを確認します。
3. "k8 -n kube-system get sts"と"k8n -n describe sts/pan-mgmt-sts"のコマンドを使用してmpステートフル セットが実行されていることを確認します→pvc/pvに問題があれば出力されます

©2024 Palo Alto Networks, Inc.

セキュア アプリケーション ポッドからのトラフィックがDP/ファイアウォール経由で送信されない

1. すべてのワーカーノードが最小5.4カーネルのバージョンを実行しているか確認します(コマンド"kubectl get nodes -o wide"を使用)

```
test@mks-test-181:~$ k8getnodes
NAME                          STATUS   ROLES    AGE   VERSION              INTERNAL-IP   EXTERNAL-IP    OS-IMAGE         KERNEL-VERSION
ip-12-12-12-23.ec2.internal   Ready    <none>   14h   v1.19.6-eks-49a6c0   12.12.12.23   3.239.70.160   Amazon Linux 2   5.4.95-42.163.amzn2.x86_64
test@mks-test-181:~$
```

2. （CNv2のみ）セキュア アプリポッドに"vxlan"インターフェースが作成され、このvxlanインターフェースを介してデフォルト ルートが作成されているかどうかを確認します。

```
root@vn-cl1-master1:~# k8getpods
NAME                          READY   STATUS    RESTARTS   AGE     IP               NODE             NOMINATED NODE   READ
lighttpd-dep-68bb6f4fbb-wwx24   1/1     Running   0          3d20h   10.233.124.128   vn-cl1-worker3   <none>           <non
wrk2-55f6f4ff85-bwrb2           1/1     Running   0          3d20h   10.233.87.141    vn-cl1-worker2   <none>           <non
root@vn-cl1-master1:~# k8 exec -it lighttpd-dep-68bb6f4fbb-wwx24 -- bash
root@lighttpd-dep-68bb6f4fbb-wwx24:/# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN mode DEFAULT group default qlen 1000
    link/ipip 0.0.0.0 brd 0.0.0.0
4: eth0@if150: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DEFAULT group default qlen 1000
    link/ether 5e:c5:45:a0:b6:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
5: vxlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/ether 5e:c5:45:a0:b6:07 brd ff:ff:ff:ff:ff:ff
root@lighttpd-dep-68bb6f4fbb-wwx24:/#
```

```
root@lighttpd-dep-68bb6f4fbb-wwx24:/# ip r
default via 169.254.1.1 dev vxlan0
10.233.20.139 dev eth0  scope link
169.254.1.1 dev vxlan0  scope link
root@lighttpd-dep-68bb6f4fbb-wwx24:/#
```

3. DP が実行中で IPSec を使用して MP に接続されているかどうか、DP がアクティブ/実行中だがIPSec が終了しているかを確認します

©2024 Palo Alto Networks, Inc.

4. DP起動後4時間経過しても認証コードがない、またはクラスタがPanoramaに接続されていないためにDPライセンスに失敗しているかを確認します-k8プラグイン

```
test2@mks-test-181:~$ k8l pan-ngfw-dep-694797597c-dcxkv
03-30-2021 16:58:19.997929 UTC INFO: DP container starting running PanOS version 10.1.0-c209.dev_s_rel
03-30-2021 16:58:20.048545 UTC INFO: Starting DP in k8s-service mode.
RTNETLINK answers: Network is unreachable
RTNETLINK answers: File exists
03-30-2021 16:58:20.645946 UTC INFO: CPU pinning is not enabled for the pan_tasks
03-30-2021 16:58:21.187358 UTC DEBUG: Using network namespace nspan-fw.
03-30-2021 16:58:21.729211 UTC DEBUG: IPsec nat port range is not specified in configmap, defaulting to port 4500.
2021-03-30 16:58:25.131 +0000 Changing python default from NONE to /etc/masterd.d/runtime/default.py
03-30-2021 16:58:25.606757 UTC INFO: Masterd Started
03-30-2021 16:58:26.646909 UTC INFO: Strongswan daemon is up. Trying to reach Management Plane..
03-30-2021 16:58:34.629870 UTC WARNING: Readiness: Not Ready. Panorama config is not pushed. pan_task is not running.
03-30-2021 17:01:33.060768 UTC INFO: IPSec up-client event with 169.254.202.2
03-30-2021 17:01:33.118831 UTC INFO: Calling dp slot register script
03-30-2021 17:01:33.624694 UTC INFO: Successfully registered with MP (slot s6). Triggering sysd daemon connect...
03-30-2021 17:01:33.902867 UTC INFO: sysd daemon connect event done
03-30-2021 17:01:34.339245 UTC INFO: Management Plane connectivity established.
03-30-2021 17:01:36.201567 UTC INFO: DP Container bringing up rest of the services.
03-30-2021 10:01:54.575489 PST WARNING: Readiness: Not Ready. Panorama config is not pushed. pan_task is running.
03-30-2021 10:02:36.993758 PST INFO: Port configuration received.
03-30-2021 10:02:38.113636 PST INFO: Phase2 commit succeeded with port config.
03-30-2021 10:02:38.572140 PST WARNING: Readiness: Ready now. Panorama config is pushed. pan_task is running.
03-30-2021 14:01:48.157911 PST CRITICAL: Failed to obtain license in predefined time.
03-30-2021 14:01:48.205252 PST CRITICAL: The system is toggling loopback state due to license fail.
test2@mks-test-181:~$
```

5. Panoramaのkubernetsプラグインの認証コードが期限切れになっていないかを確認します

   admin@Panorama> request plugins kubernetes get-license-tokens

   セキュリティ サブスクリプション:Wildfire、脅威防御、DNS、URLフィルタリング

   認証コードのタイプ:SW-NGFW Credits

   認証コード:D2962989

   有効期限: なし

   有効期限:2022年12月31日

   発行されたvCPU:50

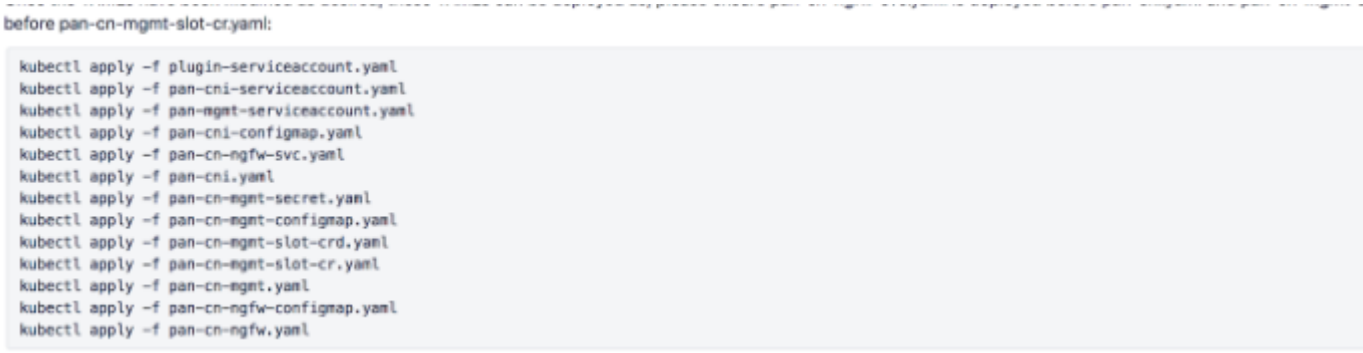
   使用済み仮想CPU:0

   発行日:2022年12月31日

   admin@Panorama-49.88>

©2024 Palo Alto Networks, Inc.

6. ngfw-svc.yamlがCNI.yamlファイルの前にデプロイされ、NGFW svcに ClusterIPが割り当てられ実行されているかどうかを確認します。


before pan-cn-mgmt-slot-cr.yaml:

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

7. /var/log/pan/pan-cni.log ([ec2-user@ip-12-12-12-184 ~]$ vi /var/log/pan-appinfo/pan-cni.log)配下のノードにログインし、CNIログを確認する。
8. アプリケーション ポッドは、CNIとngfw svcの実行後に作成する必要があります。ポッドの再起動が効果的な場合があります。
9. アプリケーション ポッドは、CNIとngfw svcの実行後に作成する必要があります。ポッドの再起動が効果的な場合があります。
10. MP podのコマンド"debug show internal interface all"を使用して、インターフェースの設定がDPにプッシュされていることを確認する
11. "show rule-hit-count vsys vsys-name vsys1 rule-base security rules all"を使用すると、どのセキュリティ ルールがヒットしているかを確認し、それに応じてセキュリティ ポリシーを変更できます。

©2024 Palo Alto Networks, Inc.

トラフィックを処理しているDPポッドを確認する方法

1. kubectl -n kube-system get pods -l app=pan-ngfw -o wide
2. kubectl -n kube-system describe pod <dp-pod-name> | grep "Container ID"
3. Panotama で、[ログの監視]に移動し、"コンテナ ID"列を追加すると、上記のコンテナ IDが表示されます。

©2024 Palo Alto Networks, Inc.

ロギング:Panoramaがトラフィック/脅威ログを表示していません。

トラブルシューティングの手順は以下のとおりです。

1. コマンド"show log traffic/threat direction equal backward"を使用して、MP上でログが生成されているかどうかを確認します。MPにログが表示されない場合は、同じMPがセキュアポッドから継続的にpingを送信しながら"show session all"を使用してトラフィックを処理しているかどうかを確認します。
2. コマンドを使ってDPがライセンスされていることを確認します:
    1. MPで"プラグインvm_series list-dp-podsを要求する"
    2. DPのK8ログがこれを確認します。
3. "debug log-receiver statistics"はDPからMPへのログ着信率を表示します。
4. "show session all"と"show session id<id>"のコマンドを実行して、ログ転送で設定した期待されるポリシーにトラフィックが到達しているかどうかを確認します。
5. "show config pushed-shared-policy"と"show running security-policy"のコマンドを実行して、設定がMPで受信されているかどうかを確認します。
6. "管理対象コレクタ"が同期していて、Panoramaで接続状態になっていることを確認します。
7. Panoramaの"マスターされたElasticsearchのステータス"→実行されているはずです。実行されていない場合は"es_restart.py -e"を実行
8. ```
   [root@cnsmokepanorama ~]# sdb cfg.es.* cfg.es.acache-update:1
    cfg.es.enable:0x0
   ```
9. es_cluster.sh health
10. Panoramaの"debug log-collector log-collection-stats show incoming-logs"
11. **pan__logquery -t traffic -i bwd -n 50**

©2024 Palo Alto Networks, Inc.
   ```

ロギング:ルール名でフィルタリングするとPanoramaにログが表示されません

PanoramaがESテンプレートの読み込みに失敗した場合に問題が発生する可能性があります。Panoramaルート モードからコマンド"es_restart.py -t"でESを再起動してみてください。新しいトラフィック/ログを送信し、ログが表示されることを確認します。

```
[root@sjc-bld-smk01-esx12-t4-pano-02 ~]# es_restart.py -t ====== /
opt/pancfg/mgmt/factory/es/templates/urlsum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/sctpsum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/iptag.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/panflex0000100004.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/sctp.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/extpcap.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/system.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/wfr.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/gtpsum.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/panflex0000100006.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/decryption.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/thsum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/globalprotect.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/hipmatch.tpl ==== ====== /
opt/pancfg/mgmt/factory/es/templates/desum.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/userid.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/panflex0000100007.tpl ==== ====== /opt/
pancfg/mgmt/factory/es/templates/trace.tpl ==== ====== /opt/pancfg/
mgmt/factory/es/templates/threat.tpl ==== ====== /opt/pancfg/mgmt/
factory/es/templates/auth.tpl ==== ====== /opt/pancfg/mgmt/factory/
es/templates/config.tpl ==== ====== /opt/pancfg/mgmt/factory/es/
templates/panflex0000100003.tpl ==== ====== /opt/pancfg/mgmt/
factory/es/templates/gtp.tpl ==== ====== /opt/pancfg/mgmt/factory/
es/templates/trsum.tpl ==== ====== /opt/pancfg/mgmt/factory/es/
templates/traffic.tpl ==== ====== /opt/pancfg/mgmt/factory/es/
templates/panflex0000100005.tpl ==== [root@sjc-bld-smk01-esx12-t4-
pano-02 ~]#
```


©2024 Palo Alto Networks, Inc.

MPがPanoramaへの再接続に失敗します

```
pan_cfg_handle_mgt_reg (pan_cfg_mgt_handler.c:5105):このデバイスまたはログ コレクタまたは wf アプライアンス (devid 892A1C93EF280D0) は管理されていません
```

上記のエラーメッセージは、以前に登録されたデバイスが、それ自体を Panorama 設定に追加するブートストラップ ワークフローを通過していないため、デバイスが再登録されていることを意味します。

これは、デバイスを以前登録して接続できていたにもかかわらず、Panoramaでその設定を保存するコミットが行われず、Panoramaが再起動して設定がクリアされ、デバイスが接続しようとしたときにPanoramaがデバイスを認識しないため、接続が切断された場合に発生する可能性があります。

Panoramaの`configd.log`の以下のログ:

```
2021-02-03 11:48:00.436 -0800 Processing lcs-register message from
 device '8B1EB1ADC72B44E' 2021-02-03 11:48:00.436 -0800 Warning:
 _get_current_cert(sc3_utils.c:84): sdb node 'cfg.ms.ak' does
 not exist.2021-02-03 11:48:04.425 -0800 logbuffer: no active
 connection to cms0 2021-02-03 11:48:24.425 -0800 logbuffer:
 no active connection to cms0 2021-02-03 11:48:44.425 -0800
 logbuffer: no active connection to cms0 2021-02-03 11:48:57.751
 -0800 Warning: sc3_register(sc3_register.c:90):SC3:無効
 - レジスタを無視します。2021-02-03 11:48:57.752 -0800 Warning:
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4645):SC3:
 device '892A1C93EF280D0' is not SC3 capable 2021-02-03
 11:48:57.752 -0800 SVM registration.Serial:892A1C93EF280D0
 DG:TPL: vm-mode:0 uuid:481a70f4-1647-426c-954a-a003ec60943f
 cpuid:K8SMP:A6D64F:84100796172040 80581: svm_id:2021-02-03
 11:48:57.752 -0800 processing a register message from
 892A1C93EF280D0 2021-02-03 11:48:57.752 -0800 Error:
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105):This device
 or log collector or wf appliance (devid 892A1C93EF280D0)
 is not managed 2021-02-03 11:49:04.426 -0800 logbuffer:
 no active connection to cms0 2021-02-03 11:49:06.015 -0800
 Warning: sc3_register(sc3_register.c:90):SC3:無効 - レ
ジスタを無視します。2021-02-03 11:49:06.015 -0800 Warning:
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:4645):SC3:
 device '8B1EB1ADC72B44E' is not SC3 capable 2021-02-03
 11:49:06.015 -0800 SVM registration.Serial:8B1EB1ADC72B44E
 DG:TPL: vm-mode:0 uuid:731de362-59ed-45a0-9fdd-7e642626f187
 cpuid:K8SMP:A6D64F:84100796172040 80581: svm_id:2021-02-03
 11:49:06.015 -0800 processing a register message from
 8B1EB1ADC72B44E 2021-02-03 11:49:06.015 -0800 Error:
 pan_cfg_handle_mgt_reg(pan_cfg_mgt_handler.c:5105):このデバイスまたはログ コレクタまたは wf アプリ
```


©2024 Palo Alto Networks, Inc.

MPとDPはアクティブで実行中の状態ですが、IPsecはMPとDPの間で終了します

MPのkubectlログを確認して、4時間後に以下のようにスロットが解放されているかを確認します。

```
(parts) root@test-virtual-machine:~# k8sys logs pan-mgmt-sts-0
 03-09-2021 01:07:36.508002 PST INFO:Management container
 starting running PanOS version 10.1.0-c182.dev_s_rel Starting
 PAN Software:03-09-2021 01:08:07.460287 PST WARNING:準備状況:準備
ができていない。データ プレーン登録用のslotdが実行されていません。 データ プ
レーン接続の ipsec が実行されていません。コマンド"dpdk-devbind"の実行を
失敗 --status [ OK ] 03-09-2021 01:09:43.043467 PST INFO:Masterd
 Started 03-09-2021 01:10:53.453639 PST WARNING:準備状況:準備完了。
データ プレーン登録用のslotdが実行中です。 データ プレーン接続のipsecが実
行されています。03-09-2021 01:10:54.558525 PST INFO:Strongswanデー
モンが起動。03-09-2021 01:10:56.286104 PST INFO:W バージョンが一
致。MP および DP ソフトウェア バージョンは両方とも10.1.0-c182.dev_s_rel
 03-09-2021 01:10:56.346162 PST INFO:uid pan-ngfw-ds-4lhhc、sw_ver
 10.1.0-c182.dev_s_rel、スロット0、dp_ip 169.254.202.2で登録を取得
します 03-09-2021 01:10:56.453298 PST INFO:uid pan-ngfw-ds-4lhhc
 169.254.202.2にslot 1を割り当て済 03-09-2021 01:10:57.131769 PST
 INFO:SW バージョンが一致。MP および DP ソフトウェア バージョンは両方と
も 10.1.0-c182.dev_s_rel03-09-2021 01:10:57.198584 PST INFO:uid
 pan-ngfw-ds-9pj2f、sw_ver 10.1.0-c182.dev_s_rel、slot 0、dp_ip
 169.254.202.3で登録を取得します 03-09-2021 01:10:57.288892 PST INFO:uid
 pan-ngfw-ds-9pj2f 169.254.202.3にslot 2を割り当て済 03-09-2021
 01:12:02.279032 PST INFO:AutoFocusライセンスをインストール中。03-09-2021
 01:12:02.362417 PST INFO:LoggingServicesライセンスのインストー
ル03-09-2021 05:13:01.521227 PST INFO:SW バージョンが一致。MPおよ
びDP ソフトウェア バージョンは両方とも 10.1.0-c182.dev_s_rel03-09-2021
 05:13:01.597810 PST INFO:スロット2、uid pan-ngfw-ds-9pj2f をForceで
解放 03-09-2021 05:13:01.694588 PST INFO:SW バージョンが一致。MP およ
び DP ソフトウェア バージョンは両方とも 10.1.0-c182.dev_s_rel 03-09-2021
 05:13:01.764245 PST INFO:スロット1、uid pan-ngfw-ds-4lhhcをForceで
解放 03-09-2021 05:13:02.100376 PST INFO:IPSec が 169.254.202.2の
ダウンクライアント イベントを取得しました 03-09-2021 05:13:02.707976 PST
 INFO:IPSECは、169.254.202.3でダウンクライアントイベントを獲得しました
```


©2024 Palo Alto Networks, Inc.

ImagePullBackOff

以下の点を確認してください。

1. リポジトリに画像がない、またはノードがリポジトリにアクセスできません
2. x509:不明な機関によって署名された証明書。上記の場合は以下を行ってください。

   プライベート リポジトリで /etc/docker/daemon.jsonのファイルを追加/修正します:

3. ```
   root@vn-cl1-master1:~# cat /etc/docker/daemon.json
    {"insecure-registries" : [ "panos-cntr-engtools-
   releng.af.paloaltonetworks.local " , "panos-cntr-
   engtools.af.paloaltonetworks.local " , "docker-cntr-
   engtools-releng.af.paloaltonetworks.local " , "docker-qa-
   pavm.af.paloaltonetworks.local " ] } root@vn-cl1-master1:~#
   ```

   イベント

   :

   ```
    Type Reason Age From Message ---- ------ ---- ---- -------
    Normal Scheduled 64s default-scheduler Successfully assigned
    kube-system/pan-cni-4jbpl to qalab-virtual-machine Normal
    Pulling 23s (x3 over 63s) kubelet Pulling image "docker-
   panos-ctnr.af.paloaltonetworks.local/pan-cni/develop/pan-
   cni-1.0.0:10_a26df862ed" Warning Failed 23s (x3 over 63s) kubelet
    Failed to pull image "docker-panos-ctnr.af.paloaltonetworks.local/
   pan-cni/develop/pan-cni-1.0.0:10_a26df862ed": rpc error: code =
    Unknown desc = Error response from daemon:https: / /docker-panos-
   ctnr.af.paloaltonetworks.local/v2 /を取得します: x509:不明な機関によって
   署名された証明書　警告失敗 23s (x3 over 63s) kubelet エラー:ErrImagePull
    Warning DNSConfigForming 8s (x7 over 63s) kubelet ネームサーバー
   の制限を超えました。ネームサーバーの一部が省略されています。適用されたネーム
   サーバーの行は以下のとおりです。8.8.8.8 8.8.4.4 2620:130:800a:14::53
    Normal BackOff 8s (x3 over 63s) kubelet Back-off pulling image
    "docker-panos-ctnr.af.paloaltonetworks.local/pan-cni/develop/pan-
   cni-1.0.0:10_a26df862ed" Warning Failed 8s (x3 over 63s) kubelet
    Error:ImagePullBackOff qalab@master-node:~/cnv2/Kubernetes/pan-cn-
   k8s-service/native$
   ```


©2024 Palo Alto Networks, Inc.
   ```

ns-panwネームスペースで実行されているワーカーノードからDPにログイン

/var/log/pan-appinfoディレクトリに移動し、コマンド**cat pan-cmdmap**を実行してログをコピーし、nspan-fwネームスペースのDPにログインします

```
root@pv-k8-vm-worker-2:/var/log/pan-appinfo# cat pan-cmdmap
 02-07-2022 17:39:54.079133 PST : kube-system/pan-ngfw-ds-ql4q9: '/
usr/bin/nsenter -t 15872 -m -p --ipc -u --net=/var/run/netns/nspan-
fw -- /bin/bash' 02-07-2022 17:43:08.976154 PST : kube-system/pan-
ngfw-ds-zbt54: '/usr/bin/nsenter -t 28308 -m -p --ipc -u --net=/var/
run/netns/nspan-fw -- /bin/bash' root@pv-k8-vm-worker-2:/var/log/
pan-appinfo# root@pv-k8-vm-worker-2:/var/log/pan-appinfo# /usr/bin/
nsenter -t 28308 -m -p --ipc -u --net=/var/run/netns/nspan-fw -- /
bin/bash [root@pan-ngfw-ds-zbt54 /]# —------>>>>>
```

DPにログインでき、マスターされたすべてのステータスをここから実行できます。

©2024 Palo Alto Networks, Inc.

DPポッドが**ContainerCreating**ステータスのままになり、以下のkubectlログが表示されます

"MountVolume.SetUp failed for volume "pan-cni-ready"

hostPathタイプのチェックに失敗しました：**/var/log/pan-appinfo/pan-cni-ready**はディレクトリではありません

```
イベント:Type Reason Age From Message ---- ------ ---- ---- -------
 Normal Scheduled 98s default-scheduler Successfully assigned kube-
system/pan-ngfw-dep-7569f69d8-j4hfp to ctnr-debug-worker-3 Warning
 FailedMount 34s (x8 over 98s) kubelet MountVolume.SetUp failed for
 volume "pan-cni-ready" : hostPath type check failed: /var/log/pan-
appinfo/pan-cni-ready is not a directory test@msatane-182:~/scripts$
```

ソリューション:

1. pan-cniポッドのkubectlログを確認する。Multusとnon-Multusを確認し、正しいyamlのデプロイを確認します。
2. Multus がデプロイされている場合は、multusをアンデプロイし、/etc/cni/net.d/ディレクトリから00-multus.conf を削除します。その後CNIとDPのアンデプロイと再デプロイが行われる

pan-cniの以下のk8ログでMultusが検出されたことを示します。そのため、上記の手順を踏む必要があります。

```
test@msatane-182:~/results/job_vm_series_72342/cn-sanity/cntr_deploy/
kube-system$ k8l pan-cni-csqt4 09-29-2021 04:07:22.495812
 UTC DEBUG:Passed CNI_CONF_NAME= 09-29-2021 04:07:22.498585
 UTC DEBUG:CNI_NETWORK_CONFIG環境変数からCNI設定テンプレートを使
用。09-29-2021 04:07:22.633416 UTC DEBUG:既存のバイナリの削除 09-29-2021
 04:07:22.731559 UTC DEBUG:Wrote PAN CNI binaries to /host/opt/
cni/bin 09-29-2021 04:07:22.734940 UTC DEBUG: /host/secondary-
bin-dir is non-writeable, skipping 09-29-2021 04:07:22.752094
 UTC DEBUG:PAN CNI config: { "name": "pan-cni", "type": "pan-
cni", "log_level": "debug", "appinfo_dir": "/var/log/pan-
appinfo", "mode": "service", "dpservicename": "pan-ngfw-svc",
 "dpservicenamespace": "kube-system", "firewall": [ "pan-fw" ],
 "interfaces": [ "eth0" ], "interfacesip": [ "" ], "interfacesmac":
 [ "" ], "override_mtu": "", "kubernetes": { "kubeconfig": "/
etc/cni/net.d/ZZZ-pan-cni-kubeconfig", "cni_bin_dir": "/opt/cni/
bin", "exclude_namespaces": [], "security_namespaces": [ "kube-
system" ] }} 09-29-2021 04:07:22.756725 UTC DEBUG:FWサービス モー
ドでCNIを実行中。Bypassfirewallはアプリケーション ポッドで有効化できま
す09-29-2021 04:07:22.796082 UTC CRITICAL:Multusをプライマリ CNIとして
検出(CONFファイル00-multus.conf);non-Multus以外のCNIがプライマリCNIになる
のを待機中。test@msatane-182:~/results/job_vm_series_72342/cn-sanity/
cntr_deploy/kube-system$
```


©2024 Palo Alto Networks, Inc.

CNv2が保護するApp pod上のリンク ステータス(vxlanを使用)

root@testapp-secure-deployment-86f9f95b5-q5nxt:/# ip link show

lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN mode DEFAULT group default qlen 1000

link/ipip 0.0.0.0 brd 0.0.0.0

eth0@if227: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1480 qdisc noqueue state UP mode DEFAULT group default qlen 1000

link/ether 26:54:8f:43:44:3f brd ff:ff:ff:ff:ff:ff link-netnsid 0

vxlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1430 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000

link/ether 26:54:8f:43:44:3f brd ff:ff:ff:ff:ff:ff

root@testapp-secure-deployment-86f9f95b5-q5nxt:/#

©2024 Palo Alto Networks, Inc.

MPからテクニカルサポートをキャプチャ

MPの場合：

1. admin@pan-mgmt-sts-0>テクニカル サポート ダンプの要求

```
Exec job enqueued with jobid 4 4 admin@pan-mgmt-sts-0> show
 jobs id 4 Enqueued Dequeued ID Type Status Result Completed
 ---------------------------------------------------------------------------
 2022/02/15 12:46:50 12:46:51 4 Exec FIN OK 12:47:36
```

2. MPルートにログインして、以下の場所に保存されているTSF名をコピーします。

   praveena@praveena:~$ kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash

   デフォルトのコンテナ "pan-mgmt" out of: pan-mgmt, pan-mgmt-init (init)

   [root@pan-mgmt-sts-0 /]#

   [root@pan-mgmt-sts-0 techsupport]# pwd

   /opt/pancfg/tmp/techsupport

   [root@pan-mgmt-sts-0 techsupport]# ls

   PA_878C48E8DDCFA5B_ts_102.0-c55_20220215_1246.tar.gz

3. 以下を使用して、TSFをMPからローカル コントローラにコピーします。

   praveena@praveena:~$ kubectl -n kube-system cp pan-mgmt-sts-0:/opt/pancfg/tmp/techsupport/PA_878C48E8DDCFA5B_ts_102.0-c55_20220215_1246.tar.gz PA_878C48E8DDCFA5B_ts_102.0-c55_20220215_1246.tar.gz

©2024 Palo Alto Networks, Inc.

HPAが動作しない

1. "k8sys get hpa"と"k8sys describe hpa"を検証する
2. モニタリング ツール(cloudwatch/GCP stackdriver/Azure App Insights)を確認して、カスタム メトリックが表示されるかどうかを確認します。
3. モニタリング ツールのカスタムメトリックが表示されない場合は、/var/log/pan/pan_vm_plugin.logにエラーがないか確認する

   test2@mks-test-181:~/cnv2/yaml-files/CNSeries_V2/eks/HPA$ k8 get pods -n custom-metrics

   NAME READY STATUS RESTARTS AGE

   k8s-cloudwatch-adapter-6647595dfd-qhbtd 1/1 Running 0 42m

   test2@mks-test-181:~/cnv2/yaml-files/CNSeries_V2/eks/HPA$ k8 logs k8s-cloudwatch-adapter-6647595dfd-qhbtd -n custom-metrics

©2024 Palo Alto Networks, Inc.

OpenShiftでアプリケーションへのインバウンドアクセスを制御するには？

アプリケーションへのインバウンドアクセスの場合:

1. お客様に、yamlファイルの注釈を使用して、haproxy/routerの保護を有効にしていただきます。これにより、haproxyに出入りするすべてのトラフィックが CN-Series を通過することが保証されます。
2. お客様に、特定のアプリケーションへのアクセスを誰に許可するかを強制するために、ソースIPでカスタムURLベースのルール(宛先)を使用していただいてください。アプリケーションのエンドポイントに対して、osecluster/paymentsなどのカスタムURLを定義する必要があります。これにより、NATを気にすることなく、これらのアプリケーションへのアクセスを許可または拒否できます。
3. お客様が OSEクラスタの前にF5などの外部ロード バランサーを使用している場合、XFFヘッダーを使用して、特定のアプリケーションへのアクセスを許可するユーザーをさらに細分化することができます。

©2024 Palo Alto Networks, Inc.

CNシリーズをアンデプロイする

以下のコマンドを実行します:

1. kubectl delete -f pan-cn-mgmt.yaml
2. kubectl delete -f pan-cn-mgmt-configmap.yaml
3. kubectl delete -f pan-cn-mgmt-secret.yaml
4. 以下のPVC を削除します:

   kubectl -n kube-system delete pvc -l appname=pan-mgmt-sts
5. kubectl delete -f . →そのディレクトリのyamlsに定義されているすべてのオブジェクトをアンデプロイします

   (この動作はすべてを破壊します!!)

©2024 Palo Alto Networks, Inc.

CNでのパケット診断を有効化します

1. アプリケーション ポッドからのトラフィックを検査する特定のDPポッドが属するMPポッドに実行します。
2. 以下のコマンドを実行します。

```
> debug dataplane packet-diag set filter match source <src>
 destination <> … > Verify the filter using “debug dataplane
 packet-diag show setting” > debug dataplane packet-diag set
 capture on > After packets are captured execute “debug dataplane
 packet-diag set capture off”
```

3. パケットがキャプチャされたら、以下のファイルを探します。

   /opt/panlogs/session/pan/filters/

©2024 Palo Alto Networks, Inc.

MPとDP間のIPSecがエラー非対称状態で失敗します

これは、以下のシナリオで発生する可能性があります。

1. MPとDPのPanOSのバージョンが異なる
2. "pan-cn-mgmt-slot-crd.yaml"と”pan-cn-mgmt-slot-cr.yaml"はデプロイされません。

```
2022-08-22 -0700 11:46:35.208 16[NET] received packet: from
 10.233.110.10[4500] to 10.233.96.7[4500] (464 bytes) 2022-08-22
 -0700 11:46:35.208 16[ENC] parsed IKE_SA_INIT request 0 [ SA KE No
 N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
 2022-08-22 -0700 11:46:35.208 16[IKE] 10.233.110.10 is initiating
 an IKE_SA 2022-08-22 -0700 11:46:35.208 16[CFG] selected
 proposal:IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/
MODP_2048 2022-08-22 -0700 11:46:35.229 16[IKE] local host is
 behind NAT, sending keep alives 2022-08-22 -0700 11:46:35.229
 16[IKE] remote host is behind NAT 2022-08-22 -0700 11:46:35.229
 16[IKE] sending cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.229 16[ENC] generating IKE_SA_INIT response
 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP)
 N(HASH_ALG) N(CHDLESS_SUP) ] 2022-08-22 -0700 11:46:35.229 16[NET]
 sending packet: from 10.233.96.7[4500] to 10.233.110.10[4500]
 (489 bytes) 2022-08-22 -0700 11:46:35.274 11[NET] received
 packet: from 10.233.110.10[4500] to 10.233.96.7[4500] (1236
 bytes) 2022-08-22 -0700 11:46:35.274 11[ENC] parsed IKE_AUTH
 request 1 [ EF(1/2) ] 2022-08-22 -0700 11:46:35.274 11[ENC]
 received fragment #1 of 2, waiting for complete IKE message
 2022-08-22 -0700 11:46:35.274 12[NET] received packet: from
 10.233.110.10[4500] to 10.233.96.7[4500] (308 bytes) 2022-08-22
 -0700 11:46:35.274 12[ENC] parsed IKE_AUTH request 1 [ EF(2/2) ]
 2022-08-22 -0700 11:46:35.274 12[ENC] received fragment #2 of
 2, reassembled fragmented IKE message (1456 bytes) 2022-08-22
 -0700 11:46:35.274 12[ENC] parsed IKE_AUTH request 1 [ IDi
 CERT N(INIT_CONTACT) CERTREQ IDr AUTH CPRQ(ADDR DNS) SA TSi TSr
 N(EAP_ONLY) N(MSG_ID_SYN_SUP) ] 2022-08-22 -0700 11:46:35.274
 12[IKE] received cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.274 12[IKE] received end entity cert "CN=pan-
fw.kube-system.svc" 2022-08-22 -0700 11:46:35.274 12[CFG] looking
 for peer configs matching 10.233.96.7[CN=pan-mgmt-svc.kube-
system.svc]...10.233.110.10[CN=pan-fw.kube-system.svc] 2022-08-22
 -0700 11:46:35.274 12[CFG] selected peer config 'to-mp' 2022-08-22
 -0700 11:46:35.274 12[CFG] using certificate "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.275 12[CFG] using trusted
 ca certificate "CN=kubernetes" 2022-08-22 -0700 11:46:35.275
 12[CFG] checking certificate status of "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.275 12[CFG] certificate
 status is not available 2022-08-22 -0700 11:46:35.275 12[CFG]
 reached self-signed root ca with a path length of 0 2022-08-22
 -0700 11:46:35.275 12[IKE] authentication of 'CN=pan-fw.kube-
system.svc' with RSA_EMSA_PKCS1_SHA2_256 successful 2022-08-22
 -0700 11:46:35.279 12[IKE] authentication of 'CN=pan-mgmt-
svc.kube-system.svc' (myself) with RSA_EMSA_PKCS1_SHA2_256
 successful 2022-08-22 -0700 11:46:35.279 12[IKE] IKE_SA to-
mp[2] established between 10.233.96.7[CN=pan-mgmt-svc.kube-
```


©2024 Palo Alto Networks, Inc.

```
system.svc]...10.233.110.10[CN=pan-fw.kube-system.svc] 2022-08-22
 -0700 11:46:35.279 12[IKE] sending end entity cert "CN=pan-
mgmt-svc.kube-system.svc" 2022-08-22 -0700 11:46:35.279 12[IKE]
 peer requested virtual IP %any 2022-08-22 -0700 11:46:35.279
 12[CFG] assigning new lease to 'CN=pan-fw.kube-system.svc'
 2022-08-22 -0700 11:46:35.279 12[IKE] assigning virtual IP
 169.254.202.2 to peer 'CN=pan-fw.kube-system.svc' 2022-08-22
 -0700 11:46:35.279 12[CFG] selected proposal:ESP:AES_GCM_8_128/
NO_EXT_SEQ 2022-08-22 -0700 11:46:35.279 12[IKE] CHILD_SA to-mp{1}
 established with SPIs 6d779dbe_i 0a178b55_o and TS 0.0.0.0/0
 === 169.254.202.2/32 2022-08-22 -0700 11:46:35.290 12[ENC]
 generating IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR)
 SA TSi TSr ] 2022-08-22 -0700 11:46:35.290 12[ENC] splitting
 IKE message (1392 bytes) into 2 fragments 2022-08-22 -0700
 11:46:35.290 12[ENC] generating IKE_AUTH response 1 [ EF(1/2) ]
 2022-08-22 -0700 11:46:35.290 12[ENC] generating IKE_AUTH response
 1 [ EF(2/2) ] 2022-08-22 -0700 11:46:35.291 12[NET] sending
 packet: from 10.233.96.7[4500] to 10.233.110.10[4500] (1236
 bytes) 2022-08-22 -0700 11:46:35.291 12[NET] sending packet:
 from 10.233.96.7[4500] to 10.233.110.10[4500] (228 bytes)
 2022-08-22 -0700 11:46:35.345 09[NET] received packet: from
 10.233.96.9[4500] to 10.233.96.7[4500] (464 bytes) 2022-08-22
 -0700 11:46:35.346 09[ENC] parsed IKE_SA_INIT request 0 [ SA KE No
 N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
 2022-08-22 -0700 11:46:35.346 09[IKE] 10.233.96.9 is initiating
 an IKE_SA 2022-08-22 -0700 11:46:35.346 09[CFG] selected
 proposal:IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/
MODP_2048 2022-08-22 -0700 11:46:35.356 09[IKE] local host is
 behind NAT, sending keep alives 2022-08-22 -0700 11:46:35.356
 09[IKE] remote host is behind NAT 2022-08-22 -0700 11:46:35.356
 09[IKE] sending cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.356 09[ENC] generating IKE_SA_INIT response
 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(FRAG_SUP)
 N(HASH_ALG) N(CHDLESS_SUP) ] 2022-08-22 -0700 11:46:35.356 09[NET]
 sending packet: from 10.233.96.7[4500] to 10.233.96.9[4500]
 (489 bytes) 2022-08-22 -0700 11:46:35.363 10[NET] received
 packet: from 10.233.96.9[4500] to 10.233.96.7[4500] (1236
 bytes) 2022-08-22 -0700 11:46:35.364 10[ENC] parsed IKE_AUTH
 request 1 [ EF(1/2) ] 2022-08-22 -0700 11:46:35.364 10[ENC]
 received fragment #1 of 2, waiting for complete IKE message
 2022-08-22 -0700 11:46:35.364 15[NET] received packet: from
 10.233.96.9[4500] to 10.233.96.7[4500] (308 bytes) 2022-08-22
 -0700 11:46:35.364 15[ENC] parsed IKE_AUTH request 1 [ EF(2/2) ]
 2022-08-22 -0700 11:46:35.364 15[ENC] received fragment #2 of
 2, reassembled fragmented IKE message (1456 bytes) 2022-08-22
 -0700 11:46:35.364 15[ENC] parsed IKE_AUTH request 1 [ IDi
 CERT N(INIT_CONTACT) CERTREQ IDr AUTH CPRQ(ADDR DNS) SA TSi TSr
 N(EAP_ONLY) N(MSG_ID_SYN_SUP) ] 2022-08-22 -0700 11:46:35.364
 15[IKE] received cert request for "CN=kubernetes" 2022-08-22
 -0700 11:46:35.364 15[IKE] received end entity cert "CN=pan-
fw.kube-system.svc" 2022-08-22 -0700 11:46:35.364 15[CFG] looking
 for peer configs matching 10.233.96.7[CN=pan-mgmt-svc.kube-
system.svc]...10.233.96.9[CN=pan-fw.kube-system.svc] 2022-08-22
 -0700 11:46:35.364 15[CFG] selected peer config 'to-mp' 2022-08-22
 -0700 11:46:35.364 15[CFG] using certificate "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.364 15[CFG] using trusted
```


©2024 Palo Alto Networks, Inc.

```
 ca certificate "CN=kubernetes" 2022-08-22 -0700 11:46:35.364
 15[CFG] checking certificate status of "CN=pan-fw.kube-
system.svc" 2022-08-22 -0700 11:46:35.364 15[CFG] certificate
 status is not available 2022-08-22 -0700 11:46:35.364 15[CFG]
 reached self-signed root ca with a path length of 0 2022-08-22
 -0700 11:46:35.364 15[IKE] authentication of 'CN=pan-fw.kube-
system.svc' with RSA_EMSA_PKCS1_SHA2_256 successful 2022-08-22
 -0700 11:46:35.366 15[IKE] authentication of 'CN=pan-mgmt-
svc.kube-system.svc' (myself) with RSA_EMSA_PKCS1_SHA2_256
 successful 2022-08-22 -0700 11:46:35.366 15[IKE] IKE_SA to-
mp[3] established between 10.233.96.7[CN=pan-mgmt-svc.kube-
system.svc]...10.233.96.9[CN=pan-fw.kube-system.svc] 2022-08-22
 -0700 11:46:35.366 15[IKE] sending end entity cert "CN=pan-
mgmt-svc.kube-system.svc" 2022-08-22 -0700 11:46:35.366 15[IKE]
 peer requested virtual IP %any 2022-08-22 -0700 11:46:35.366
 15[CFG] assigning new lease to 'CN=pan-fw.kube-system.svc'
 2022-08-22 -0700 11:46:35.366 15[IKE] assigning virtual IP
 169.254.202.3 to peer 'CN=pan-fw.kube-system.svc' 2022-08-22
 -0700 11:46:35.366 15[CFG] selected proposal:ESP:AES_GCM_8_128/
NO_EXT_SEQ 2022-08-22 -0700 11:46:35.366 15[IKE] CHILD_SA to-mp{2}
 established with SPIs a97528ab_i f6667584_o and TS 0.0.0.0/0
 === 169.254.202.3/32 2022-08-22 -0700 11:46:35.372 15[CHD]
 updown:SIOCADDRT:File exists 2022-08-22 -0700 11:46:35.373
 15[ENC] generating IKE_AUTH response 1 [ IDr CERT AUTH CPRP(ADDR)
 SA TSi TSr ] 2022-08-22 -0700 11:46:35.373 15[ENC] splitting
 IKE message (1392 bytes) into 2 fragments 2022-08-22 -0700
 11:46:35.373 15[ENC] generating IKE_AUTH response 1 [ EF(1/2) ]
 2022-08-22 -0700 11:46:35.373 15[ENC] generating IKE_AUTH
 response 1 [ EF(2/2) ] 2022-08-22 -0700 11:46:35.373 15[NET]
 sending packet: from 10.233.96.7[4500] to 10.233.96.9[4500]
 (1236 bytes) 2022-08-22 -0700 11:46:35.373 15[NET] sending
 packet: from 10.233.96.7[4500] to 10.233.96.9[4500] (228 bytes)
 2022-08-22 -0700 11:46:46.471 11[NET] received packet: from
 10.233.96.9[4500] to 10.233.96.7[4500] (80 bytes) 2022-08-22
 -0700 11:46:46.471 11[ENC] parsed INFORMATIONAL request 2
 [ D ] 2022-08-22 -0700 11:46:46.471 11[IKE] received DELETE
 for IKE_SA to-mp[3] 2022-08-22 -0700 11:46:46.471 11[IKE]
 deleting IKE_SA to-mp[3] between 10.233.96.7[CN=pan-mgmt-
svc.kube-system.svc]...10.233.96.9[CN=pan-fw.kube-system.svc]
 2022-08-22 -0700 11:46:46.471 11[IKE] unable to reestablish
 IKE_SA due to asymmetric setup 2022-08-22 -0700 11:46:46.471
 11[IKE] IKE_SA deleted 2022-08-22 -0700 11:46:46.751 11[ENC]
 generating INFORMATIONAL response 2 [ ] 2022-08-22 -0700
 11:46:46.751 11[NET] sending packet: from 10.233.96.7[4500]
 to 10.233.96.9[4500] (80 bytes) 2022-08-22 -0700 11:46:46.752
 11[CFG] lease 169.254.202.3 by 'CN=pan-fw.kube-system.svc'
 went offline 2022-08-22 -0700 11:46:47.040 12[NET] received
 packet: from 10.233.110.10[4500] to 10.233.96.7[4500] (80 bytes)
 2022-08-22 -0700 11:46:47.040 12[ENC] parsed INFORMATIONAL
 request 2 [ D ] 2022-08-22 -0700 11:46:47.040 12[IKE] received
 DELETE for IKE_SA to-mp[2] 2022-08-22 -0700 11:46:47.040 12[IKE]
 deleting IKE_SA to-mp[2] between 10.233.96.7[CN=pan-mgmt-svc.kube-
system.svc]...10.233.110.10[CN=pan-fw.kube-system.svc] 2022-08-22
 -0700 11:46:47.040 12[IKE] unable to reestablish IKE_SA due to
 asymmetric setup 2022-08-22 -0700 11:46:47.041 12[IKE] IKE_SA
 deleted
```


©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

アプリケーション ポッドがDNS解決に失敗します(ファイアウォールの有無にかかわらず)

以下を確認してください。

1. DNSポッドが実行されていることを確認します: "kubectl get pods - - namespace=kube-system -l k8s-app=kube-dns"
2. DNSサービスが起動していることを確認します: "kubectl get svc - - namespace=kube-system"
3. DNSサービスが実行されていない場合は、DNSデプロイメントをsvcとして公開するか、yamlを使用してデプロイします。
4. SVCをデプロイしたら、エンドポイントが正しく公開されていることを確認します。"kubectl get endpoints coredns --namespace=kube-system"
5. アプリケーション ポッドを再度デプロイします。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.