

CNシリーズHSFのデプロイメント

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-Series HSF	5
CN-Series HSF アーキテクチャ	6
ポッドの種類	7
相互接続リンク	8
CN-Series HSF のライセンスの取得	10
クレジットのアクティベート	10
CN-Series HSF デプロイメント プロファイルの作成	11
デプロイメントプロファイルの管理	15
CN-Series HSF システム要件	16
推奨される CN-Series システムと容量マトリックス	16
おすすめの CN-Series HSF Flavor	17
CN-Series HSF Jumbo Mode のサポート	18
CN-Series HSF をデプロイするための前提条件	
クラスタ要件	20
クラスタを準備する	20
CN-Series HSF のデプロイメント用に Panorama を準備する	27
HSF クラスタをデプロイする	
一般	33
ノード データ	34
イメージと保存	38
CN 設定	39
自動スケーリング	41
デプロイメントのさまざまな状態	44
CN-Series HSF へのトラフィック フローの設定	46
テスト ケース:レイヤー 3 BFD ベースの CN-GW 障害処理	52
CN-Series HSF の概要と監視を表示する	57
CN-Series HSF デプロイメントの検証	62
EKS 環境で KEDA を使用するカスタム メトリック ベースの HPA	64
AWS で KEDA を認証する	64
KEDA ポッドをデプロイする	65
CNシリーズHSFでのダイナミックルーティングの設定	66
CN-Series HSF:ユースケース	75
5G トラフィック テスト	75

サポートされるカスタム メトリックに基づくファイアウォールのスケ-	ール
アウト	83
テスト ケース:CN-MGMT 障害処理	84
テスト ケース:CN-NGFW 障害処理	88
テスト ケース:CN-DB の障害処理	91
CN-Series でサポートされていない機能	95



CN-Series HSF

どこで使用できますか?	何が必要ですか?
• CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

Palo Alto Networks **CN-Series Hyperscale Security Fabric** (HSF) 1.0 は、コンテナ化された次世代 ファイアウォールのクラスタであり、5G ネットワークを展開するモバイル サービス プロバイ ダー向けに高度にスケーラブルで回復力のある次世代ファイアウォール ソリューションを提供 します。

CN-Series HSF ソリューションは以下を提供します。

- コンテナ化された NGFW による超拡張性:AppID と GTP のパフォーマンスをオンデマンドで 水平方向にスケールアウトします。
- 高い可用性と回復力:予想されるスループットとセッションに基づいて動的に動作するElastic クラスタリングを提供し、ワークロード全体でのビジネス継続性とセッション復元力を保証 します。
- 外部ロードバランサーへの依存を排除:導入が簡単で、Panorama プラグインを通じて完全に調整できる DevOpsに適した環境を提供します。

CN-Series HSF ソリューションは、RedHat Openshift (オンプレミス) または AWS EKS パブリック クラウドで管理された Kubernetes 環境にデプロイできます。

CN-Series HSF アーキテクチャ

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

CN-Series HSF クラスタは、内部ネットワークで接続された CN-MGMT (管理)、CN-NGFW (デー タプレーン)、CN-GW (ゲートウェイ)、および CN-DB (データベース) ポッドのプールで構成 されます。CN-MGMT ポッドは、クラスタ管理プレーン機能を提供します。CN-NGFW ポッド は、クラスタ データ プレーン セキュリティ機能を提供します。CN-GW ポッドはクラスタへの エントリ ポイントであり、CN-NGFW ポッド間でトラフィックを分散します。CN-DB ポッド は、CN-NGFW ポッドが使用する中央クラスタ セッション キャッシュを提供します。



CN-Series HSF は、冗長性と可用性を提供する 2 つの CN-MGMT コンテナをサポートします。ただし、CN-NGFW DP からの接続を取得できるのは、2 つの CN-MGMT コンテナのうちの 1 つだけです。接続された CN-MGMT は StatefulSet サービスとして実行され、CN-NGFW がアクティブな CN-MGMT にのみ接続できるようにします。現在の CN-MGMT に障害が発生しない限り、他の CN-MGMT コンテナは CN-NGFW コンテナに接続しません。



ポッドの種類

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

CN-Series HSF には 3 種類のデータプレーン ポッドがあり、それらはすべて同じデータプレーン ポッド イメージを使用しますが、configmap オプションは異なります。CN-Series HSF は、2 つの 管理ポッドをホストします。

CN-GW ポッド - CN-GW ポッドはデータプレーン ポッドの一種で、外部ネットワーク トラフィックにアクセスし、入力トラフィックと出力トラフィックの負荷分散を管理します。外部のノードは CN-GW ポッドとその IP のみを認識し、トラフィックのすべてのデータ サブネットは multus インターフェイスを介してこれらのポッドに接続されます。CN-Series HSF 1.0 では、最小で 2 つ、最大で 4 つの CN-GW ポッドがサポートされています。CN-GW ポッドは、HSF クラス

タデプロイメント開の存続期間まで静的スケールです。たとえば、最初に2つのGW ポッドがあり、スケールアウトしたい場合、CN-NGFW ポッドは動的にスケールアウトできますが、追加の数のCN-GW ポッドを使用して HSF クラスタを再デプロイする必要があります。

CN-DB ポッド - CN-DB ポッドは、CN-NGFW ポッド全体でセッション/フローの所有権を照会で きるデータプレーン ポッドの一種です。入力スロット、ラウンドロビン、およびセッション負 荷。CN-Series HSF は 2 つの CN-DB ポッドをサポートし、セッション情報は 2 つの CN-DB ポッ ド間で複製され、2 つの CN-DB ポッドのいずれかがフローのルックアップ/バインディングで機 能します。

CN-NGFW ポッド - CN-NGFW ポッドは、C および U セッションの実際のトラフィックを処理 し、セキュリティ ポリシーを適用し、CN-NGFW ポッドの個別のスケーリングを可能にしま す。CN-Series HSF 1.0 では、最小 2 個、最大 12 個の CN-NGFW ポッドがサポートされていま す。

CN-MGMT ポッド - すべての NGFW ポッド (CN-GW、CN-DB、および CN-NGFW) は、eth0 上の IPsec を介して単一の CN-MGMT ポッドに接続されています。

相互接続リンク

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

すべての CN-GW、CN-DB、および CN-NGFW ポッドは、マルチス インターフェイスである Cluster Interconnect (CI) リンクを介して相互に接続されます。CI リンクは、クラスタ通信および クラスタ メンバー間のパケット転送用に予約されたデータ ポートです。Ethernet x/1 は、関連 するすべてのポッドの CI リンクに使用されます。CI リンクは、ある CN-NGFW から別の CN-NGFW にトラフィックを転送するためにも使用できます。

CN-GW および CN-NGFW ポッドは、マルチス インターフェイスであるトラフィック インター コネクト (TI) リンクを介して相互に接続されます。TI リンクは、クラスタ内の内部トラフィッ ク用に予約されたデータ ポートです。Ethernet x/2 は、関連するすべてのポッドの TI リンクに使 用されます。

CN-GW ポッドでは、Ethernet x/3 以降が、顧客ネットワークに接続する外部インターフェイスとして使用されます。





CN-Series HSF は、IPv4 プロトコルのみをサポートします。

オンプレミス環境の場合、CIおよび TI インターフェイスに IP アドレスを割り当てるには、DHCP サーバーまたは IPAM が必要です。AWS EKS の場合、DHCP サーバーは基盤となるインフラストラクチャの一部です。したがって、IP アドレスは、クラウド環境の CI および TI インターフェイスに自動的に割り当てられます。

CN-Series HSF のライセンスの取得

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

CN-Series ファイアウォール ライセンス割り当ては、Kubernetes plugin on Panorama によって管理 されます。CN-Series ファイアウォールは、Kubernetes 環境にデプロイされた CN-NGFW、CN-GW、CN-DB ポッドによって使用される vCPU (コア)の総数に基づいてライセンス付与されま す。これらのポッドによって使用される vCPU ごとに 1 つのトークンが消費されます。

- クレジットのアクティベート
- CN-Series HSF デプロイメント プロファイルの作成
- デプロイメントプロファイルの管理

クレジットのアクティベート

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 Helm 3.6 or above version client

組織内では、それぞれが異なる目的を持つ多くのアカウントを作成できます。アクティベーション中は、デフォルトのクレジットプールごとに1つのアカウントのみを選択できます。クレジットプールがアクティブになると、クレジット管理者ロールを付与されたユーザーは、クレジットをデプロイメントに割り当て、クレジットを他のプールに転送することもできます。

既存の CSP アカウントがあり、スーパーユーザーまたは管理者である場合、システムは自動的 にクレジット管理者ロールをプロファイルに追加します。既存のアカウントがない場合、CSP は 自動的にアカウントを作成し、クレジット管理者ロールをプロファイルに追加します。

お客様 (購入者) は、サブスクリプション、クレジット プール ID、サブスクリプションの開始日 と終了日、購入したクレジットの金額、およびデフォルトのクレジット プール (クレジットをア クティベートしたときに作成されたクレジット プール) の説明が記載された電子メールを受信し ます。



- **STEP 1** 電子メールで、[アクティベーションの開始]をクリックして、使用可能なクレジットプール を表示します。
- **STEP 2** アクティベートするクレジットプールを選択します。検索フィールドを使用して、アカウン トリストを番号または名前でフィルタリングできます。

複数のクレジットプールを購入した場合は、両方が自動的に選択されます。チェックマーク は、オンボーディングクレジットのアクティベーションリンクを表します。

認証またはサインインするように求められます。

- クレジットプールの選択を解除すると、それらのクレジットをアクティベートするには、電子メールに戻って[アクティベーションの開始]リンクをクリックする必要があるというリマインダーが表示されます。
- STEP 3 [アクティベーションの開始]を選択します。
- STEP 4 サポートアカウントを選択します(アカウント番号または名前で検索できます)。
- STEP 5 デフォルトのクレジットプールを選択します。
- STEP 6 [デポジットクレジット]を選択します。

デポジットが正常に完了したというメッセージが表示されます。

STEP 7 (オプション)これが初めてのクレジットアクティベーションである場合は、[デプロイメン トプロファイルの作成]ダイアログが表示されます。

CN-Series HSF デプロイメント プロファイルの作成

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

以下の手順を使用して、CN-Series デプロイメント プロファイルを作成します。

STEP 1 すでにクレジットプールがある場合は、アカウントにログインし、ダッシュボードからア セット > ソフトウェア NGFW クレジット > Prisma NGFW クレジット > 新規プロファイル の作成 を選択します。

クレジットプールをアクティベートしたばかりの場合は、デプロイメントプロファイルの作 成フォームが表示されます。

- 1. CN-Series ファイアウォールタイプを選択します。
- 2. PAN-OS 11.0 を選択します。
- 3. Next (次へ) をクリックします。
- **STEP 2** | CN-Series $\neg \Box \Box \neg \tau I \nu_{\circ}$
 - 1. プロファイル名。

プロファイルに名前を付けます。

2. 合計 vCPU 数。

すべてのポッド (CN-NGFW、CN-GW、CN-DB) で必要な vCPU の総数を入力します。

- ドロップダウンからセキュリティのユースケースを選択します。ドロップダウンの各セキュリティユースケースは、選択したユースケースに推奨されるいくつかの説明を自動的に選択します。[カスタム]を選択すると、デプロイメントで使用するサブスクリプションを指定できます。
- サブスクリプションの HSF を有効にするには、[サブスクリプションのカスタマイズ]で[Hyperscale Security Fabric]を選択します。
- 5. (任意) クレジットを使用して VM Panorama を有効にする—管理または専用のログ コレクタの場合。

STEP 3 [見積もりコストの計算]をクリックすると、クレジットの合計と、デプロイメント前に使用 可能なクレジットの数が表示されます。

Create Deployment	Profile	×
CN-Series		
Profile Name	CN_profile_1	
Total vCPUs (Across All CN * NGFW)	20	
Security Use Case *	Custom ×	~
Customize Subscriptions	 Threat Prevention Advanced URL Filtering DNS 	 Wildfire Intelligent Traffic Offload Hyperscale Security Fabric
Use Credits to Enable VM Panorama	 For Management As Dedicated Log Collector Protect more, save more 	
	Calculate Estimated Cost	
		Cancel Create Deployment Profile

デプロイメントプロファイルの管理

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

CN-Series デプロイメントの要件に基づいて、CN-Series デプロイメント プロファイルを編集、 複製、または削除できます。さらに、サブスクリプションを作成した後、デプロイメント プロ ファイルにサブスクリプションを追加したり、デプロイメント プロファイルからサブスクリプ ションを削除したりできます。詳細については、デプロイメント プロファイルの管理を参照し てください。

CN-Series HSF システム要件

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

- 推奨される CN-Series システムと容量マトリックス
- おすすめの CN-Series HSF Flavor
- CN-Series HSF Jumbo Mode のサポート

推奨される CN-Series システムと容量マトリックス

CN-Series HSF の推奨システム要件は次のとおりです。

次の表は、CN-Series のサイズ (小、中、大) ごとにデータを分けています。CN-Series HSFが実行 できるスループット検査は、クラスタのサイズによって異なります。

- CN-Series Small for HSF
- CN-Series Medium for HSF
- CN-Series Large for HSF

CN-Series HSF には、それぞれ2つのノードを持つ CN-Mgmt と CN-DB の2つのノードグループ が必要です。CN-GW と CN-NGFW のノード グループに必要なノード数は、スループットによっ て異なります。

Cluster Flavor		小	中	大
CN-GW	コア	24	24	24
	メモリ	16 GB	20 GB	24 GB
	帯域幅	50 Gbps	100 Gbps	100 Gbps
	Instance Type (イ ンスタンスタイ プ)	9xLarge (36vCPU、96Gi)	c5n.18xlarge	c5n.18xlarge
CN-DB	コア	8	8	12

CN-Series HSF

Cluster Flavor		/]\	中	大
	メモリ	0.64 x 12 x 最大 セッション (百 万単位) GB	0.64 x 12 x 最大 セッション (百 万単位) GB	0.64 x 10 x 10 GB
	帯域幅	10 GbE	25 GbE	25 GbE
	Instance Type (イ ンスタンスタイ プ)	c5n.4xlarge (16vCPU, 42Gi)	c5n.4xlarge	c5n.9xlarge
CN-MGMT	コア	4	12	12
	メモリ	16 GB	16 GB - 24 GB	16 GB - 24 GB
	帯域幅	10 GbE	10 GbE	10 GbE
	ディスク	56 Gi	80 Gi	80 Gi
	Instance Type (イ ンスタンスタイ プ)	c5n.4xlarge (8vCPU, 21Gi)	c5n.4xlarge また は c5d.9xlarge	c5n.4xlarge または c5d.9xlarge
CN-NGFW	コア	15	24	24 - 36
	メモリ	20 GB	16 GB - 47 GB	48 GB (32コア 以上の場合は 56 GB)
	帯域幅	25 GbE	50 GbE	50 GbE
	Instance Type (イ ンスタンスタイ プ)	c5n.4xlarge (16vCPU, 42Gi)	c5n.9xlarge	c5n.9xlarge

おすすめの CN-Series HSF Flavor

Cluster Flavor	ノード数			インター	インター
	小	中	大	フェースの総 数	フェースの最 小数
CN-GW	2	3	4	4-15	4

Cluster Flavor	ノード数			インター	インター
	小	中	大	フェースの総 数	フェースの最 小数
CN-DB	2	2	2	2	2
CN-MGMT	2	2	2	1	{{御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御御
CN-NGFW	6	8	10	3	3
DP 障害に対応 するための CN- NGFW の追加	2	2	2	-	-

CN-Series HSF Jumbo Mode のサポート

ジャンボサポートを有効にすると、Panorama は CN-MGMT 以外のすべてのインターフェイスの 最大伝送単位 (MTU) を 8744 バイトに設定します。

ジャンボモードでのシステム MTU は 9000 バイトで、MTU が指定されていない場合、インターフェイスはシステム MTU を継承します。

EKS ホストでは、*AWS EC2* インスタンスのデフォルトの*MTU* 値は 9000 です。そのため、ホスト側での設定は不要です。

ジャンボサポートを無効にすると、Panorama は CN-MGMT 以外のすべてのインターフェイスの 最大伝送単位(MTU)を 1756 バイトに設定します。 EKS 環境のジャンボ MTU 値および非ジャンボ MTU 値を Panorama MTU 値と一致させる必要があります。

モード	MTU (バイト)
ジャンボ	EKS - 9000 バイト
非ジャンボ	すべてのインターフェイスで 1756 バイト

CN-Series HSF をデプロイするための前提条件

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

CN-Series HSF を展開するための前提条件は次のとおりです。

- クラスタ要件
- クラスタを準備する
- CN-Series HSF のデプロイメント用に Panorama を準備する

クラスタ要件

ノード グループを作成および管理するために必要なアクセス許可を持つ Kubernetes クラスタが 必要です。また、CN-Series クラスタを立ち上げるために Kubernetes プラグインに必要なリソー スも必要です。

クラスタの前提条件として、以下を設定する必要があります。

• 環境に応じて、EKS または Openshift (4.10) クラスタ。VPC とサブネットを作成し、EKS クラ スタを起動するために必要な IAM ロールを設定する必要があります。

EKS クラスタの作成については、Amazon EKS クラスタの作成を参照してください。

Openshift クラスタの作成については、Openshift クラスタのインストールを参照してください。

- Kubernetes バージョン 1.22 以降。
 詳しくは、デプロイメント ツールを使用した Kubernetes のインストールを参照してください。
- Multus CNI により、Kubernetes のポッドに複数のネットワーク インターフェイスを接続できるようになります。

詳細については、Multus CNI のインストールを参照してください。

• CNシリーズのシステム要件に記載されている最小要件を持つ4つのノードグループ。

クラスタを準備する

以下を設定する必要があります

• ノード グループとノード

- ノードラベル
- サービスアカウント
- インターフェイス

ノード グループとノード

トポロジを処理し、ソリューション内のすべてのポッドに対応するには、少なくとも8つのノードが必要です。Palo Alto Networks では、それぞれ最低2つのノードを持つ4セットのノードグループを推奨しています。MPノードグループが残りの3つのノードグループと重複しないようにしてください。

DPDK を使用する場合は、DPDK ドライバーが設定された AMI が必要です。詳細について は、AWS EKS で DPDK をセットアップするを参照してください。

EKS クラスタを実行した後、Multus で CloudFormation テンプレートを使用して、ノードグルー プとノードタイプを持つ EC2 インスタンスを起動します。

	3			
lnehru@lnehru-parts-vm:~/cn-cluster_yamls/yaml	-files/pa	n-cn-k8s-	clusteri	ng/common\$ kubectl get nodes
NAME	STATUS	ROLES	AGE	VERSION
ip-10-101-201-125.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-201-204.us-west-1.compute.internal	Ready	<none></none>	3d23h	v1.22.12-eks-ba74326
ip-10-101-201-223.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-201-226.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-201-81.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-221-159.us-west-1.compute.internal	Ready	<none></none>	63d	v1.19.15-eks-9c63c4
ip-10-101-221-163.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-221-21.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-221-51.us-west-1.compute.internal	Ready	<none></none>	63d	v1.19.15-eks-9c63c4
ip-10-101-221-66.us-west-1.compute.internal	Ready	<none></none>	23d	v1.22.12-eks-ba74326
ip-10-101-221-78.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-221-90.us-west-1.compute.internal	Ready	<none></none>	23d	v1.22.12-eks-ba74326
ip-10-101-222-149.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-222-175.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-222-176.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-222-213.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
<pre>ip-10-101-222-38.us-west-1.compute.internal</pre>	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-222-6.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-222-77.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326
ip-10-101-222-96.us-west-1.compute.internal	Ready	<none></none>	24d	v1.22.12-eks-ba74326

ノードラベル

次のコマンドを使用して、すべてのノードにラベルを付けます。 kubectl label node (MP_node_name) Panw-mp=Panw-mp kubectl label node (DB_node_name) Panw-db=Panw-db kubectl label node (GW_node_nam) Panw-gw=Panw-gw kubectl label node (NGFW_node_name) Panw-ngfw=Panw-ngfw 以下は、ノード ラベルの例です。 CN-NGFW - paloalto-ngfw: networks-ngfw CN-MGMT - paloalto-mgmt: networks-mgmt

CN-GW - paloalto-gw: networks-gw

CN-DB - paloalto-db: networks-db

ノード タイプごとにキーと値のペアが提供されることが期待されます。また、主要な paloalto お よび値ネットワークのデフォルト値が推奨されます。ただし、ノード ラベルを変更することを 選択した場合は、設定で対応する変更を行う必要があります。

Internue Tradinger methods and a set of the set of the

ノードにラベルを付けたら、クラスターを起動するために必要な YAML をダウンロードします。

サービスアカウント

デプロイメントの拡張権限は、サービス アカウント yaml を使用して提供されます。サービス ア カウントを作成するには、Kubernetes クラスタの準備が整っている必要があります。

plugin-deploy-serviceaccount.yaml に対してサービス アカウント YAML を実行します。

サービス アカウントは、Panorama が Kubernetes ラベルとリソース情報を取得するためにクラ スターに対して認証するために必要な権限を有効にします。このサービス アカウントには、 デフォルトでpan-plugin-user という名前が付けられています。

2. yaml-files/clustering folder/common に移動し、以下をデプロイします。

kubectl apply -f plugin-deploy-serviceaccount.yaml

kubectl apply -f pan-mgmt-serviceaccount.yaml

kubectl -n kube-system get secrets | grep pan-plugin-user-token

シークレットを含む認証情報ファイル (例: cred.json) を作成し保存します。クラスタを監視す るための Kubernetes プラグインを設定するには、このファイルを Panorama にアップロードす る必要があります。 **3.** このサービス アカウントに関連付けられたシークレットを表示するには、以下の手順を実行します。

kubectl -n kube-system get secrets (secrets-from-above-command) -o
json >> cred.json

lnehru@lnehru-parts-vm:-/cn-cluster_yamls/yaml-files/pan-cn-k8s-clustering/common\$
Inehru@lnehru-parts-vm:-/cn-cluster_yamls/yaml-files/pan-cn-k8s-clustering/common\$ MY_TOKEN=`kubectl -n kube-system get serviceaccounts pan-plugin-user -o jsonpath='{.secre
\${0}.name}'
Inehru@lnehru-parts-vm:-/cn-cluster_yamls/yaml-files/pan-cn-k8s-clustering/common\$
Inehru@lnehru-parts-vm:-/cn-cl

4. cred.json を kubernetes プラグインにアップロードし、検証ステータスを確認します。

Image: rest Const	O PANORAMA	DASHBOARD ACC MO	Device	Groups 1 OLLECTS NET	WORK DEVICE	PANORAMA		da Cometer - 1 10	B• Q
	Panorama v								3 ()
A conduction Condu	Di Seko * Ci High Avalability	General Ucanaes Notify Group	Kabernetze Chaster						
Impact Notice Market	Config Audit	Kubernetes Cluster Definition							
Notes that is a set of the set	Managed WhitPise Applances							€iters)→×	
Marken Maar Marken Maar </td <td>Password Profiles</td> <td>HANNE</td> <td></td> <td></td> <td></td> <td></td> <td>VALID FOR MONITORING</td> <td>NAUD FOR DEPLOYMENTS</td> <td></td>	Password Profiles	HANNE					VALID FOR MONITORING	NAUD FOR DEPLOYMENTS	
Marca Data	Admin Rokes	01V-10	Kubernetes Clust	er Definition		Ø	wibble wibble wibble wibble	whole whole whole whole	
Alternational Robins Alternational	TACCES Damain		Hame				WIDDIE WOORE WOORE	WIDOE NEONE ARDOR	
 A Marine Label Region B Marine Label Region C Marine Label Region<	OS Authentication Profile		Descriptio						
Market Matheman Substantion Market Market Market Substantion Market Market Orect Oppose Market Market Market Orect Oppose Market Market Market Oppose Transme Market Market Oppose Transme Market Market Market Market Market Market Oppose Transme Market Market	Statestation Sequence								
 Schwarzer Grag Rath Schwarzer Grag Rath Chwarzer Grag Rath Chwarzer Grag Rath Chwarzer Grag Rath Checkwarzer Rath <	An Only Redebility		API server addres	API Server Accessive	e Number, Default Part is 6				
 Device Quantitie Device Qu	(A) Scheduled Carrie Push		Ter	•					
 Marager Classes Add Categor Constant Ad	Cevice Quarantine		Credential	Chick "Credentials" to a	antiques the Service-Crede	of also			
Image: Image: Ima	> CT Managed Devices								
Water Margen Other Canon Other Canon Other Other	Templates +	CAM Colere CPDDDCS							
Interpretation Inter	Device Groups +								
Image: Control Margaments Image: Control Margaments	III Managed California		Label Selector . Lab	el Filter - Ceston Ce	tificate				
Control	Contractor Droups *								
Independence Independence <td>Log Insertion Profile</td> <td></td> <td></td> <td></td> <td></td> <td>0 kem)→X</td> <td></td> <td></td> <td></td>	Log Insertion Profile					0 kem)→X			
 Server Frantise Ser	Gib Log Settings		THE MILLIN	NAMERACE	LARL MLECTOR	ARRENT			
Image: Software Image: Software <td>> Cell Server Profiles</td> <td></td> <td>End- rate of</td> <td>POPPET PROPERTY.</td> <td>1000</td> <td>11111100</td> <td></td> <td></td> <td></td>	> Cell Server Profiles		End- rate of	POPPET PROPERTY.	1000	11111100			
Substrate Projeti Projeti Projeti Projeti Substrate Sub	G Scheduled Carring Export								
Source Pagin Project Pagin Pagi	Software +								
Adm 0 Delene Adm 0	Cynamic Updates *								
Add Control Control Add Control Control Control Control Add Control Contro Control Control Control Control Contro Con	D Plagna +								
	IS see								
	A Linewar Guage								
Opplagments Image: Control of the c	Monitoring Definition								
Avans Avans <t< td=""><td>Ca Deployments</td><td></td><td>CAM O Delete</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Ca Deployments		CAM O Delete						
Image: Second	> 🔥 Asum								
Q Locationst * B Support * Call Device Displayment * Marker Key and Dispersives * * B Device Regressive Auth Ray * * Privice Recommendation	> 😯 AWS					Carcel			
Conception C	Q LICENSES *								
Monter Kay and Diagnostics + Diagnostics Autors Disconterenties Autors Disconterenties Autors Disconterenties Autors	2 Sh Device Percipament								
Device Registration Auth Key Device Recommendation	Anter Key and Diagnostics 1								
Contract Recommendation	Device Registration Auth Key								
	> B) Policy Recommendation								

Panorama での最初の検証投稿コミットの後、プラグインは定期的に検証ロジックを呼び出し、UIの検証ステータスを更新し続けます。

インターフェイス

CN-DB、CN-NGFW、および CN-GW に必要な ENI を作成する必要があります。これらのイン ターフェイスの PCI バス ID を特定します。これは、ポッドを相互接続するためのネットワーク 接続定義を作成するために使用されます。

1. クラスタの作成中に作成したキー/ユーザーを使用して、ノードに SSH 接続します。

ssh ec2-user@(node_ip) -i private_(key)

2. ethtool パッケージをインストールします。

Sudo yum install ethtool

sudo yum update -y && sudo yum install ethtool -y

3. インターフェイス名を識別します。

ifconfig

4. インターフェイスの PCI バス ID を特定して、ポッドにネットワーク接続をデプロイします。
 ethtool -i (i/f)



ここで、eth0 はノード管理インターフェイス、eth1 は CI インターフェイス、eth2 は TI、eth3 外部インターフェイス 1、eth4 外部インターフェイス 2 です。CN-MGMT のラベルが付 いたノードには、管理用の eth0 インターフェイスのみが表示されます。CN-DB の場合は eth1、CN-NGFW の場合は eth1、eth2、CN-GW の場合は eth1、eth2、および環境内で作成した 数の外部インターフェイスがあります。

net-attach-1 - 0000:00:08.0 net-attach-2 - 0000:00:09.0 netattach-def-ci-db - 0000:00:06.0 net-attach-def-ci-gw - 0000:00:06.0 net-attach-def-ci-ngfw - 0000:00:06.0 net-attach-def-ti-gw -0000:00:07.0 net-attach-def-ti-ngfw - 0000:00:07.0

デプロイメントのすべてのポッドは、同じネットワーク接続定義を使用するため、異なる ノード上にある必要があり、したがって各ポッドは同じ PCI バス ID にアクセスする必要があ ります。たとえば、net-attach が C/U ポッド CI リンクに PCI ID 6 を使用している場合、各 C/ U ポッドは、同じサブネットからの PCI ID 6 インターフェイスを持つノードに配置する必要 があります。

5. Network Attachment Definition YAML で PCI バス ID を変更します。

{ "cniVersion":"0.3.1", "type": "host-device", "pciBusID":"0000:00:07.0" }



ここでは、最初のリンク eth1 が CI として使用され、eth2 が TI として使用され、eth3 以降が 外部リンクに使用されます。

6. 前提条件の YAML ファイルを適用します。

```
kubectl apply -f pan-mgmt-serviceaccount.yaml
kubectl apply -f net-attach-def-1.yaml
kubectl apply -f net-attach-def-2.yaml
kubectl apply -f net-attach-def-ci-db.yaml
kubectl apply -f net-attach-def-ci-gw.yaml
kubectl apply -f net-attach-def-ci-ngfw.yaml
kubectl apply -f net-attach-def-ti-gw.yaml
```

Openshift で、**Kubectl apply -f ctrcfg-pidslimit.yaml**を適用します。pidlimit の詳細 については、 設定タスクを参照してください。

静的 PV を使用する場合は、CN-MGMT ポッドのラベルが付いたノードに静的 PV マウント ボ リュームを作成します。

/mnt/pan-local1, /mnt/pan-local2, /mnt/pan-local3, /mnt/pan-local4, /
mnt/pan-local5, /mnt/pan-local6

CN-Series HSF のデプロイメント用に Panorama を準備する

CN-Series HSF の設定とデプロイメントは、Panorama を介して行われます。CN-Series HSF をデ プロイする前に、次の前提条件を満たしていることを確認してください。

- STEP 1 ソフトウェア バージョン 11.0 で Panorama をデプロイし、最小のコンテンツ バージョンを インストールします。
 - 1. PAN-OS 11.0 上の最小のコンテンツ リリース バージョンは、Panorama > ダイナミック 更新に移動します。

「PAN-OS リリース ノート」を参照してください。

2. ソフトウェア バージョンについては、Panorama > ソフトウェアに移動します。

アップグレードしているリリース バージョンのモデル固有のファイルを特定し てダウンロードします。たとえば、M-Series アプライアンスを Panorama 11.0.0 にアップグレードするには、Panorama_m-11.0.0 イメージをダウンロードしま す。Panorama バーチャル アプライアンスを Panorama 10.1.0 にアップグレードするに は、Panorama_pc-11.0.0 イメージをダウンロードします。

正常にダウンロードが完了すると、ダウンロードしたイメージの [アクション] 列が [ダ ウンロード] から [インストール] に変わります。

STEP 2 | Panorama でファイアウォール ログを収集する場合は、Panorama が [Panorama モード] に なっていることを確認します。

- STEP 3 Panorama に Kubernetes プラグイン 4.0 バージョンをインストールします。Panorama アプラ イアンスが HA ペアとしてデプロイされている場合は、まずプライマリ(アクティブ)ピ アに Kubernetes プラグインをインストールする必要があります。
 - 1. Panorama Web インターフェイスにログインし、Panorama > プラグインを選択して[今 すぐチェック]をクリックし、利用できるプラグインのリストを入手します。
 - 2. [ダウンロード] を選択して、Kubernetes プラグイン 4.0 バージョンをインストールします。

プラグインのインストールが正常に完了したら、Panorama が更新され、 [**Panorama**] タブに Kubernetes プラグインが表示されます。

Panorama が HA ペアでデプロイされている場合は、手順 3 で説明した手順に従って、 セカンダリ (パッシブ) Panorama に Kubernetes プラグインをインストールします。

3. [Panorama へのコミット] をクリックします。

このコミットにより、CN シリーズ HSF で使用する K8S-CNF-Clustering-Readonly テン プレートが作成されます。Panorama にインターフェースが表示されるまでに最大1分 かかります。このテンプレートには、CN-GW、CN-DB、および CNNGFW ポッド用の 事前設定されたクラスタ相互接続 (CI) リンクと、CN-GW および CN-NGFW ポッド用 のトラフィック相互接続 (TI) リンクのネットワーク設定が含まれています。K8S-CNF-Clustering-Readonly は、30 個の論理ルーターと、論理ルーターごとに 2 つのインター フェイスを作成します。ethernet x/1 はクラスタ相互接続 (CI) リンクであり、ethernet x/2 はクラスタ相互接続 (TI) リンクです。

K8S-CNG-Clustering-Readonly テンプレートの名前を変更しないでください。

[Panorama] ダッシュボード > 一般情報で、一般情報ウィジェットを確認することもできます。

General Information		G×
Device Name		
MGT IP Address		
MGT Netmask		
MGT Default Gateway		
MGT IPv6 Address		
MGT IPv6 Link Local Address		
MGT IPv6 Default Gateway		
MGT MAC Address	0c:c4:7a:fa:13:10	
Model	M-200	
Serial #	017607000697	
System Mode	panorama	
Software Version	11.0.1-c114.dev_e_rel	
Application Version	8644-7712 (11/15/22)	
Antivirus Version	4268-4781 (11/15/22)	
Device Dictionary Version	62-361 (11/10/22)	
Time	Tue Nov 15 21:32:24 2022	
Uptime	4 days, 12:03:17	
Plugin CN Clustering plugin	clustering-1.0.0-c6	
Plugin VM-Series	vm_series-4.0.0-c12	
Plugin Cloud Connector plugin	cloudconnector-2.0.0-c1	
Plugin Kubernetes Plugin	kubernetes-4.0.0-c264.dev	
Device Certificate Status	Valid	

STEP 4 | Panorama で CN-Series HSF のライセンス クレジットを取得します。

- 1. Panorama > プラグイン > Kubernetes > セットアップ > ライセンスを選択します。
- 2. 認証コードを使用してアクティベート/更新を選択し、認証コードと必要なデータプ レーン vCPU の総数を入力します。CNシリーズの認証コードを取得するには、デプロ イメント プロファイルを作成する必要があります。

Container License			
Date Issued	Update License	(?)	
Authorization Code	Authorization Code		
Number of vCPU's	Number of vCPU's 32		
Security Subscriptions			
Authcode Type	Clear Auth Code	OK Cancel	

- CN-Series が HSF でデプロイされている場合、デプロイされたポッド (CN-NGFW、CN-GW、および CN-DB)の数が割り当てられた vCPUの数を超えた場合、さらに vCPUを追加するための 4 時間の猶予期間があります。デプロイメントプロファイルを削除するか、十分な数のポッドを削除してください。4 時間の猶予期間内に追加の vCPUを割り当てないか、ライセンスのないポッドを削除しない場合、ライセンスのないポッドが再起動し、トラフィックの乱れが発生します。ライセンスのあるの Pod は引き続きライセンスされます。
- 3. 使用可能なライセンス クレジットの数が更新されていることを確認します。

STEP 5| 親デバイス グループを作成します。

CN-Series HSF に必要なポリシーとオブジェクトを含むデバイス グループを作成する必要が あります。CN-Series HSF をデプロイするときは、このデバイス グループを参照する必要が あります。

- 1. Panorama > デバイス グループ を選択し、 [追加] をクリックします。
- 2. デバイス グループを識別するために、一意の Name (名前) と Description (内容) を 入力します。
- 3. デバイス グループの階層構造で現在作成しようとしているデバイス グループの直接の 親にあたる Parent Device Group(親デバイス グループ)(デフォルトは Shared(共 有))を選択します。
- 4. **OK**をクリックします。

デバイス グループ名は、クラスタ内の CN-MGMT ポッドにブートストラップされま す。CN-MGMT ポッドがこれらのブートストラップ パラメータを使用して Panorama に接続すると、デバイス グループがクラスタ設定のクラスタ名に関連付けられま す。Panorama 高可用性 (HA) の場合、CN-MGMT ポッドはアクティブ Panorama とパッ シブ Panorama の両方に更新を送信します。クラスタ情報は、CN-NGFW、CN-DB、お よび CN-GW ポッドがアクティブになると、自動的に入力されます。

5. コミット > コミットしてプッシュ を選択して、デバイス グループの設定を Panorama に コミットしてプッシュします。

STEP 6 変数テンプレートを作成して、トラフィック フローを有効にします。

- 1. Panorama > テンプレートに移動し、 [追加] をクリックします。
- 2. テンプレートの一意の名前を入力します。
- 3. オプションの説明を入力します。
- 4. 変数テンプレートを設定して、トラフィックフローを有効にします。
 - Cのテンプレートは、CN-Series HSF のデプロイ前またはデプロイ後に設定できます。

STEP 7| ログ コレクタを作成し、ログ コレクタ グループに追加します。

- 1. Panorama > コレクタ グループの順に選択し、コレクタ グループを追加します。
- 2. コレクタ グループの名前を入力します。
- コレクタ グループがファイアウォール ログを保持する Minimum Retention Period (最小保持期間)の日数(1~2,000)を入力します。 デフォルトでは、このフィールドは空白(コレクタ グループが無期限にログを保持する)です。
- 4. ログコレクタ (1 ~ 16 個)を Collector Group Members (コレクタ グループ メンバー) リストに Add (追加) します。

Collector Group	
General Monitoring	Device Log Forwarding Collector Log Forwarding Log Ingestion Audit
Name	FW-Cluster-CG
Log Storage	Total: 26674.87 GB,Free: 1280.39 GB
Min Retention Period (days)	[1 - 2000]
Collector Group Members	Q (2 items) >
	-cn-clustering-2(01)
	-cn-clustering-1(01: /)
	+ Add Delete
	Enable log redundancy across collectors
	Forward to an conectors in the preference ist Enable secure inter LC Communication Log collector on local panorama is using the secure client configuration from 'Panorama -> Secure Communication Settings'
	ОК Салсе
コミット > コミ クタ グループに	ットしてプッシュの順に選択し、変更を Panorama および設定したコ コミットしてプッシュします

Panorama 認証キーは、Kubernetes プラグインによって作成および管理されます。

HSF クラスタをデプロイする

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

CN-Series ファイアウォールを HSF としてデプロイするための前提条件が満たされていることを 確認したら、Kubernetes > デプロイメント に移動し、[追加]をクリックします。

HSF クラスタをデプロイするには、次のタブを設定する必要があります。

- 一般
- ノードデータ
- イメージと保存
- CN 設定
- 自動スケーリング
- 一般

[デプロイメント]ポップアップの[一般]タブ セクションに次の詳細を入力します。

- STEP 1 | CN-Series Cluster Name CN-Series HSF の名前。
- **STEP 2**| (オプション)説明— HSF クラスタを説明するテキスト文字列。
- STEP 3 Kubernetes クラスタ プラグインの[セットアップ]セクションの下に、クラスタのエン トリのリストが作成されます。作成した関連するクラスタをドロップダウンから選択しま す。





STEP 4 | CN-Series Cluster Name — CN-Series HSF の名前。

ノードデータ

[デプロイメント] ポップアップの [ノード データ] タブセクションに次の詳細を入力します。

- STEP 1 Namespace CN-Series HSF がデプロイされる既存の Kubernetes クラスタ内の名前空間。
- **STEP 2** Node Info— ノード プール ラベルは、各タイプの CN ポッドを展開するために使用されま す。ノードの可用性に基づいて、ポッド タイプごとに CPU、メモリ、および目的のポッド を指定する必要があります。ラベルとラベル値のペアは、ノードに存在するための前提条

件の値であり、ノードのラベル付けに使用されるのと同じキーと値のペアを追加する必要 があります。

1. General Namespace kube-system 2. Node Data Node Info PODS LABEL KEY LABEL VALUE CPU MEMORY (GI) DESIRED PODS 3. Image & Storage CN-MGMT PANW-MP PANW-MP 2 4 2 2 4. CN Configuration CN-OB PANW-OB PANW-OB 1 4 2 2 5. Auto-Scaling CN-GW PANW-NGFW PANW-NGFW 1 4 5 1	Deployments							(
2. Node Data Node Info PODS LABEL KEY LABEL VALUE CPU MEMORY (GI) DESIRED PODS 3. Image & Storage CN-MGMT PANW-MP PANW-MP 2 4 2 2 4. CN Configuration CN-DB PANW-DB PANW-DB 1 4 2 2 5. Auto-Scaling CN-GW PANW-GW PANW-MFW 1 4 5 Interfaces	1. General	Namespace	kube-system						
3. Image & Storage CN-MGMT PANW-MP PANW-MP 2 4 2 4. CN Configuration CN-DB PANW-DB PANW-DB 1 4 2 5. Auto-Scaling CN-MGFW PANW-GW PANW-MGFW 1 4 2 Interfaces	2. Node Data	Node Info	PODS	LABEL KEY	LABEL VALUE	CPU	MEMORY (GI)	DESIRED PODS	
4. CN Configuration 5. Auto-Scaling CN-DB PANW-DB PANW-DB 1 4 2 CN-GW PANW-GW PANW-GW 1 4 2 CN-NGFW PANW-NGFW PANW-NGFW 1 4 5	3. Image & Storage		CN-MGMT	PANW-MP	PANW-MP	2	4	2	
5. Auto-Scaling CN-GW PANW-GW PANW-GW 1 4 2 CN-NGFW PANW-NGFW PANW-NGFW 1 4 5	4. CN Configuration		CN-D8	PANW-DB	PANW-DB	1	4	2	
CN-NGFW PANW-NGFW PANW-NGFW 1 4 5	5. Auto-Scaling		CN-GW	PANW-GW	PANW-GW &	1	4	2	
Interfaces			CN-NGFW	PANW-NGFW	PANW-NGFW	1	4	5	
CN-DB CN-NGFW CN-GW ethernet-x/1 net-attach-def-ci-db		CN-DB CN-NGFW CN-GW ethernet-x/1 net-attach-def-ci-db							

STEP 3 Interfaces - CN-DB、NGFW、CN-GW ポッドのインターフェイス名を追加する必要がありま す。各インターフェイスには、特定の net-attach-def を Kubernetes クラスタに適用する必要 があります。プラグインは、デフォルトで Ethernet x/1 および Ethernet x/2 という名前を付け ます。Ethernet x/1 および Ethernet x/2 のインターフェイス名を変更する場合は、ネットワー ク接続セクションでも変更を行う必要があります。CN-GW ポッドの場合、CI および TI インターフェイスを除いて、最大 12 個のインターフェイスを追加できます。

Deployments							Ţ	0				
1. General	Namespace kube-system											
2. Node Data 3. Image & Storage 4. CN Configuration 5. Auto-Scaling	Node Info	PODS	LABEL KEY	LABEL VALUE	CPU	MEMORY (GI)	DESIRED PODS	ĩ				
		CN-MGMT	PANW-MP	PANW-MP	2	4	2	1				
		CN-DB	PANW-DB	PANW-DB	1	4	2					
		CN-GW	PANW-GW	PANW-GW	1	4	2					
		CN-NGFW	PANW-NGFW	PANW-NGFW	1	4	5					
	Interfaces CN-DB CN- ethernet-x/2 ethernet-x/2	NGFW CN 1 net-attach-de 2 net-attach-de	ef-ci-ngfw ef-ti-ngfw			ок	Cancel					

Kubernetes クラスタは、詳細がコミットされ、デプロイに有効な場合にのみ表示 されます。




1. General	Namespace	ace kube-system							
2. Node Data	Node Info	PODS	LAREL KEY	LAREL VALUE	CPU	MEMORY (GI)	DESIRED POD		
Image & Storage		CN-MGMT	PANW-MP	PANW-MP	2	4	2		
CN Configuration		CN-DB	PANW-DB	PANW-DB	1	4	2		
Auto-Scaling		CN-GW	PANW-GW	PANW-GW	1	4	2		
		CN-NGFW	PANW-NGFW	PANW-NGFW	1	4	5		
				KUREP	4 items) \rightarrow)				
	INTERFACE NAME				BERNETES NETWORK ATTACHMENT				
	ethernet-x/1	ethernet-x/1				net-attach-def-ci-gw			
	ethernet-x/2	ethemet-x/2				net-attach-def-ti-gw			
	ethernet-x/3	ethernet-x/3				net-attach-1			
	ethernet-x/4				ch-2				
	0.00								
	Add ⊖ Del Del	ete							

イメージと保存

[デプロイメント] ポップアップの [イメージと保存] タブセクションに次の詳細を入力しま す。

- STEP 1 Image 画像をローカルまたは AWS リポジトリに保存する必要があり、これは Panorama では検証できません。ただし、Kubernetes クラスタには、イメージが保存されているリポ ジトリへの接続があります。
 - 1. CN-MGMT Image:CN-MGMT ポッドをデプロイするために Kubernetes 環境がイメージ にアクセスするリポジトリからの完全な URI。
 - 2. **CN-MGMT INIT Image**:CN-MGMT ポッドに必要な 初期イメージ。
 - 3. CN-NGFW Image:CN-NGFW ポッドをデプロイするために Kubernetes 環境がイメージ にアクセスするリポジトリからの完全な URI。

- STEP 2 Storage 排他的なストレージを設定する場合は、EKS 環境の場合は [ストレージ] セクションで [動的] をクリックし、Openshift 環境の場合は [静的] または [動的] をクリックすると、プラグインがクラウド ストレージを構成します。 [静的] を選択した場合は、Storage Key Values、Worker Nodelabel Key、Worker Nodelabel Value を入力する必要があります。ストレージがマウントされている [パス] も入力する必要があります。
 - *kubernetes* 環境の名前空間に有効なデフォルト以外のストレージ クラスを追加す る必要があります。それ以外の場合、動的ストレージ オプションが選択され、 ストレージ クラス名が指定されていない場合は、名前空間に存在する既定のス トレージ クラスが選択されます。

0 items) > >					
LVALUE					
Add ODelete					
Path /mnt/					
Telemetry					
Device Certificate 🔘 Enable 🧿 Disable					
other security					

STEP 3 Certificates — これは、ライセンスなどの情報を有効または無効にするためのデバイス証明 書情報です。有効になっている場合は、PIN ID と PIN 値を指定する必要があります。

CN 設定

[デプロイメント] ポップアップの [CN 設定] タブ セクションに、次の詳細を入力します。

- STEP 1 Primary Panorama IP プラグインがインストールされている Panorama のパブリック IP アドレスとプライベート IP アドレスの値を表示します。
- STEP 2| Secondary Panorama IP プラグインがインストールされているセカンダリ Panorama (HA の場合) のパブリックおよびプライベート IP アドレスの値を表示します。
- STEP 3 Device Group 前提条件セクションで説明したように、デプロイメントを設定する前に DG を作成する必要があります。 [デバイス グループ] ドロップダウンには、現在の Panorama のすべての DG が一覧表示され、有効な DG を選択する必要があります。CN-MGMT ポッ ドは、この DG の下に登録されます。デバイス グループを作成する手順については、CN-Series HSF のデプロイメント用に Panorama を準備するの手順 5 を参照してください。
- STEP 4 Template 前提条件セクションで説明したようにデプロイメントを設定する前に、CN-GW 固有の詳細用のテンプレート (variable_template) を作成する必要があります。 [テンプレート] ドロップダウンには、現在の Panorama のすべてのテンプレートが一覧表示されます。現在のデプロイメントに適したテンプレートを選択する必要があります。HSF のデプロ イ後、このテンプレートは、CN-DB および CN-NGFW ポッドの基本構成を処理する K8S-CNF-Clustering-Readonly テンプレートとともに、プラグインによってテンプレート スタッ クに追加されます。また、CN-GW ポッドで CI および TI リンクを設定します。CN-MGMT ポッドは、テンプレート スタックから設定を取得します。変数テンプレートを作成する手順については、CN-Series HSF のデプロイメント用に Panorama を準備するの手順 6 を参照 してください。
- STEP 5 Log Collector Group (LCG) このドロップダウンには、現在の Panorama のすべてのログ コレクター グループが一覧表示され、適切な LCG を選択する必要があります。また、CN-GW ポッドの CI および TI リンクも設定します。LCG を作成する手順については、CN-Series HSF のデプロイメント用に Panorama を準備するの手順 7 を参照してください。
- **STEP 6** Jumbo Frame [Jumbo Frame]ドロップダウン リストの値 有効化、無効化、および AutoDetect。この設定は、CN-Series HSF のすべてのポッドに適用できます。
- **STEP 7** 5G Enabled これは、 [有効化] および [無効化] オプションを備えたラジオ ボタンで あり、CN-Series HSF で必要な GTP 設定を参照します。



variable_template ファイルで、テンプレートに必要な追加設定を処理する必要が あります。 STEP 8 DPDK — これは、[有効化]オプションと[無効化]オプションを備えたラジオ ボタンです。 基になるリソースが DPDK をサポートしていない場合、CN-Series HSF はデフォルトで packetmmap に設定されます。

EKS で DPDK を使用する場合は、DPDK ドライバーが設定された AMI が必要です。詳細については、AWS EKS で DPDK をセットアップするを参照してください。

Openshift で DPDK を有効にするには、ワーカー ノードでヒュージ ページを有効にする必要 があります。詳細については、hugepages の設定を参照してください。

また、ワーカー ノードで VFIO PCI ドライバーを有効にする必要があります。

```
modprobe vfio-pciecho 1 > /sys/module/vfio/parameters/
enable_unsafe_noiommu_mode
```

- STEP 9| CPU Pinning CPU ピニングを有効にするか無効にするかを選択します。
- STEP 10 | Numa Enabled NUMA のノード番号を指定します。
- **STEP 11** | **CPU Pinning Base** 転送プロセスの CPU ピニングを開始する場所から CPU 番号を指定し、 番号の小さい CPU をスキップします。

Deployments			٢
1. General 2. Node Data	Primary Panorama IP	10.55.1.20	×
3. Image & Storage	Secondary Panorama IP	10.56.1.21	~
4. CN Configuration	Device Group	demo-dg-1	~
5. Auto-Scaling	Template	demo-template-1	~
	Log Collector Group	eks_cg	v
	Jumbo Frame	enable	v
	5G Enabled	Enable O Disable	
	DPDK	Enable Disable	
	Hugepages Memory	2	
	If underlying resources of CPU Pinning	le not support dpck then CN will be defaulted to packemmap. O Enable O Disable	
	NUMA Enabled		
	CPU Pinning Base		
			OK Cancel

自動スケーリング

[デプロイメント]ポップアップの[自動スケーリング]タブセクションに次の詳細を入力します。

- Auto-Scaling は、EKS Kubernetes バージョン 1.22 を使用する EKS 環境でのみサポートされます。他の Kubernetes システムの[自動スケーリング]タブはグレー表示されています。
 - 自動スケーリングが機能するようにEKS 環境で KEDA を使用するカスタムメト リックベースの HPAをデプロイする必要があります
- STEP 1 [自動スケーリング]セクションで、[自動スケーリング メトリクス]、[スケールインしきい 値]、および[スケールアウトしきい値]を入力します。
- **STEP 2** [**OK**]をクリックして、デプロイをコミットします。

自動スケーリングでサポートされている指標は次のとおりです。

- dataplanecpuutilizationpct
- dataplanepacketbufferutilization
- pansessionactive
- pansessionutilization
- pansessionsslproxyutilization
- panthroughput
- panpacketrate
- panconnectionspersecond

	Ð
1. General Autoscaling Enable 2. Node Data Autoscaling Enable 3. Image & Storage Aws Region Isabe: System 4. CN Configuration Aws Region us-west-2 5. Auto-Scaling Autoscaling Metric Dataplanecpountlikationpct Scale In Threshold 20 Scale Out Threshold 80 Min Cn Ngfw 2 Max Cn Ngfw 4	

すべての設定の詳細を入力すると、[デプロイメント]タブに、保存されている1つの展開の 詳細が表示されます。[コミット]をクリックしてデプロイを続行します。コミットが完了する と、プラグインは[デプロイ]ボタンを表示します。[デプロイ]ボタンをクリックして、CN-Series HSF を展開します。 CN-Series HSF のデプロイメント後、クラスタはテンプレート スタック、K8S-CNF-Clustering-Readonly テンプレート、およびCN-Series HSF のデプロイメント用に Panorama を準備するのス テップ 6 で作成した変数テンプレートを備えた<cluster-name>-ts作成します。

Template Stack	(0
Name	cluster-001-ts	
Description		
	Automatically push content whe	software device (vm or container) registers to Panorama
Default VSYS	vsys1	×
Pro loss	The default virtual system template cont	guration is pushed to firewalls with a single virtual system.
Devices	FILTERS	$Q(\underline{\qquad 2 \text{ items}}) \rightarrow X$
	Platforms PA-CTNR (2) Device Groups DG-FW-Cluster-3 (2) Tags HA Cluster ID HA Cluster State cluster state	Image: Select All Deselect All Group HA Peers Filter Selected (2)
	User ID Master Device O Cic	Ud Identity Engine
	The master device is the firewall fro information for use in policies.	n which Panorama gathers user ID KBS-EI-FW- Cluster-3 KBS-EI-FW-Cluster-3
		Add Delete ↑ Move Up ↓ Move Down The Template at the top of the Stack has the highest priority in the
		presence of overlapping config

HSF デプロイメント設定中に参照したデバイス グループ (CN-Series HSF のデプロイメント用に Panorama を準備するの手順 5 で作成) と、HSF デプロイメントが CN-MGMT ポッドにブートス トラップされた後に自動的に作成されたテンプレート スタック。CN-MGMT ポッドが Panorama に接続すると、デバイス グループとテンプレート スタックが自動的に HSF 名に関連付けられま す。

CN-DB、CN-GW、および CN-NGFW ポッドの HSF 情報は、アクティブなときに自動入力され ます。これらのポッドが稼働している場合、CN-MGMT ポッドは、CI IP アドレス、ポッドの詳 細、デバイス ID、ソフトウェア バージョンなどの詳細を Panorama に送信します。

パノラマ高可用性 (HA) の場合、CN-MGMT ポッドはアクティブ Panorama とパッシブ Panorama の両方に更新を送信します。

デプロイメントのさまざまな状態

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

すべての設定の詳細を入力すると、[デプロイメント]タブに、保存されている1つの展開の詳 細が表示されます。デプロイメントには5つの段階があります。

- 1. コミットが必要
- 2. デプロイされていません
- 3. デプロイ中
- 4. 警告
- 5. 成功/失敗
- [コミット]をクリックしてデプロイを続行します。[コミット]をクリックすると、[デプロイ] ボタンが無効になり、デプロイの状態が[未デプロイ]に変わることがあります。コミットが完 了すると、[デプロイ]ボタンが有効になります。
- **2.** [デプロイ] をクリックして、CN-Series CNF のデプロイを続行します。デプロイの状態 が[デプロイ中]に変わります。この段階で、Panorama 設定が作成され、CN-GW が生成され、 プラグインが CN-Series HSF を展開するための API 呼び出しを開始します。
- **3.** リソースの可用性と設定の詳細に応じて、デプロイ中状態が警告、成功、または失敗に変わります。その後、[再デプロイ] ボタンと [デプロイ解除] ボタンが有効になります。
- [再デプロイ]をクリックして、有効になっているパラメータを変更し、[再デプロイ]をクリックする前に変更をコミットします。
- **5.** [デプロイ解除] をクリックして、このデプロイメントの一部として作成されたすべての CN-Series HSF ポッドを削除します。
- すべての CN-Series HSF ポッドを削除した後も、すべての Panorama 設定が保持されます。

🚯 PANORAMA	DASHEGARD	ACC MONITOR	POLICIES	OBJECTS NET	- Tomplates	PARADOLANA			Lomix	120 80- 0
Favorana v										6 D
Re Setur	la c									$\dim (\rightarrow \times)$
Carligh Availability	- NAME	DESCRIPTION	FURENHEIRS CUURING BANKE	EVERALITES OVERTER TYPE	PAN OF VIRSION	PRINCIPAL IN	POD INFO	EEPLOPHENT EDATAS	DEVICE GROUP	ACTON
Hanaped WielFire Custers Hanaped WielFire Appliances Password Profiles	aditive white white white white white white white white white	white white adds white white adds white white	whoir white whoir white white	white white white white white	05.764	while while while while while	urijoje odkite urijoje urijoje odkite	Fallere	while while while while while	Balleylay Undeglay
Administrations · · · · · · · · · · · · · · · · · · ·										
Authentication Profile										
Schooluled Config Push										
Device Groups										
Collector Groups Collector Groups Contribute Management										
C. Lag registion Profile Lag Settings > 2 Server Profiles										
Call Scheduled Config Doorn Call Software E Dynamic Updates										
1.0 Pupei = →										
Correct Usage										
Ca Dupleyments										
> Asire										
Licenses #										
Support =										
C Device Deployment										
Master Key and Diagnostics •										
Device Registration Auth Key										
 top Metry Recommenced on 										
	⊕ AN ⊖ Delete									
odvint Legnar Les Legin Tree	- 10/10/21 10/20/21 10	General Expire Time: #	1/54/2025 15:00:09						EE Tools Ungung	 d) paloalto

CN-Series HSF へのトラフィック フローの設定

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

アップストリーム/ダウンストリーム ルーターは、フローベースの ECMP アルゴリズムを使用 します。トラフィックが CN-GW に到達すると、対称ハッシュ アルゴリズムを使用して、トラ フィック インターコネクト (TI) リンクを介して、使用可能な CN-NGFW の1つにトラフィック を分散します。セッションに一致する両方向 (クライアントからサーバー、サーバーからクライ アント) からのトラフィックは、常に同じ CN-NGFW を通過します。CN-NGFW がトラフィック を処理すると、トラフィックを 許可する ポリシーを設定している場合、トラフィック パケット は CN-GW に返送されてサーバーに到達します。



- STEP 1 レイヤー3ルーティングに参加する論理ルータをファイアウォール上に作成します。
 - 1. ネットワーク>ルーティング> 論理ルーター に移動し、[テンプレート]ドロップダウンから変数テンプレートを選択します。
 - 2. デフォルトの仮想ルーターを選択するか、新しい論理ルーターの名前を追加します。
 - [一般]を選択し、定義済みのインターフェイスを追加します。
 論理ルーターに追加するすべてのインターフェイスを追加するには、この手順を繰り返します。
 - ethernetX/1 および ethernetX/2 インターフェイスは、それぞれ CI および TI リンク用に予約されています。ethernet1/3 と ethernet1/14の間のインター フェイスを選択します。
 - 4. **OK** をクリックします。
 - 5. 静的ルーティングのアドミニストレーティブディスタンスを設定します。範囲は 10 から 240 です。デフォルトは 10 です。

ネットワークの要件に合わせて、ルートの各タイプの管理距離を設定します。仮想ルー タに宛先が同じルートが2つ以上ある場合、仮想ルーターはアドミニストレーティブ ディスタンスを使用して、異なるルーティングプロトコルおよび静的ルートから、よ り距離が短いものを優先しつつ最適なパスを選択します。

- 6. ECMP を有効にして、転送に複数の等コストパスを活用します。
- 7. OK をクリックします。

STEP 2 トラフィック フローを有効にするようにレイヤ3インターフェイスを設定します。

CN-Series HSF のデプロイメント用に Panorama を準備するの場合、可変テンプレートを作成 した可能性があります。クラスタ ネットワークを通過するトラフィック フローを有効にする には、CN-Series HSF の負荷分散に必要なネットワークとトラフィック設定を使用して変数 テンプレートを構成する必要があります。ファイアウォールがこれらのインターフェイスで ルーティングを実行できるように、レイヤー3イーサネット インターフェイスを IPv4 アド レスで構成する必要があります。通常は次の作業を行い、インターネットおよび内部ネット ワークのインターフェイスに接続する外部インターフェイスを設定します。

Cのテンプレートは、CN-Series HSF のデプロイ前またはデプロイ後に構成できます。

このテンプレートの設定が、*Kubernetes* プラグインのインストール中に自動的に 作成された *K8S-CNF-Clustering-Readonly* テンプレートと重複しないようにして ください。

1. ネットワーク>インターフェイスに移動し、[テンプレート]ドロップダウンから変数テ ンプレートを選択します。

- 2. イーサネットインターフェイスを選択し、インターフェイスを追加します。
- 3. 1から30のスロットを選択します。
- 4. ethernet1/3 と ethernet1/14の間のインターフェイス名を入力します。
- 5. インターフェイス タイプ については、レイヤー3を選択します。
- 6. [設定] タブで、以下を行います。
 - 論理ルーターには、ステップ1で構成した論理ルーターを選択します。
 - マルチ仮想システムファイアウォールの場合、Virtual System (仮想システム) は設定中の仮想システムを選択します。
 - Security Zone (セキュリティゾーン) については、インターフェイスが属するゾーン を選択するか、New Zone (新規ゾーン) を作成します。

Ethernet Interfa	ce	(?)
Interface Name	themet1/3	
Comment		
Interface Type	ayer3	~
Netflow Profile	lone	~
Config IPv4	IPv6 SD-WAN Advanced	
Assign Interface To		
Virtual Router	None	×
Logical Router	Slot1_LR2	~
Virtual System	vsys1	~
Security Zone	untrust_ei1	×
L		



7. IPv4 タブで DHCP Client (DHCP クライアント)を選択します。

ファイアウォール インターフェイスが DHCP クライアントとして機能し、動的に割り 当てられた IP アドレスを受信します。ファイアウォールには、DHCP クライアント イ ンターフェイスから受信した設定をファイアウォールで稼働中の DHCP サーバーに配 信する機能も備えられています。詳細については、インターフェイスを DHCP クライ アントとして構成するを参照してください。

8. OK をクリックします。

Ethernet Interf	ace	?
Interface Name	ethernet1/3	
Comment		
Interface Type	Layer3	\sim
Netflow Profile	None	\sim
Config IPv4	IPv6 SD-WAN Advanced	
	Enable SD-WAN Enable Bonjour Reflector	
Туре	Static OPPoE ODHCP Client	
	🖌 Enable	
	Automatically create default route pointing to default gateway provided by server	
	Send Hostname system-hostname	\sim
Default Route Me	tric 10	

ок	Cancel)

- STEP 3| 論理ルーターのスタティック ルートを設定します。
 - 1. ネットワーク > ルーティング > 論理ルーターに移動し、 [テンプレート] ドロップダ ウンから変数テンプレートを選択します。
 - 2. 静的 > IPv4タブを選択し、 [追加] をクリックします。
 - 3. スタティックルートの Name (名前) を入力します。
 - 4. 宛先ルートとネットマスクを入力します。192.168.200.0/24 などです。
 - 5. [インターフェイス] に、パケットがネクスト ホップに移動するために使用する発信 インターフェイスを指定します。
 - 6. [ネクスト ホップ] で [**ip-address**] を選択し、内部ゲートウェイの IP アドレスを入 力します。たとえば、192.168.100.2 です。
 - 7. ルートの Admin Distance を入力して、この論理ルーターの静的ルートに設定されてい るデフォルトの管理距離を上書きします (範囲は 10 ~ 240、デフォルトは 10)。
 - 8. ルートの Metric (メトリック) を入力します (範囲は 1~65,535)。
 - BFD プロファイルを 静的ルートに適用すると、静的ルートが失敗した場合にファイア ウォールがルートを削除し、代替ルートを使用するようにします。デフォルト設定は None (なし) です。
 - 10. OK をクリックします。

Logical Router	- Static Route					?		
Name	Route-to-client	Route-to-client						
Destination	192.168.200.0/24	192.168.200.0/24						
Interface	ethernet1/3					\sim		
Next Hop	IP Address					\sim		
	192.168.100.6					\sim		
Admin Dist	[10 - 240]							
Metric	10							
BFD Profile	default					\sim		
Path Monitorin	g							
	Enabl	e						
Failur	e Condition 💿 Any		Preemptive Hold	Time (min) 2				
	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT			
	ete							

OK Cancel



どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

このテストでは、CN-GW の障害を処理するために必要な BFD 設定を評価します。BFD プロ ファイルは、アップストリーム/ダウンストリーム ルーターでの CN-GW 障害を処理します。



対称トラフィック フロー

- 入力トラフィック インターフェイスが CN-GW1の場合、出力インターフェイスを見つけるためのルート ルックアップは LR1 にあります。
 - ルート 1:宛先:クライアント サブネット、ネクスト ホップ:R1
 - ルート 2:宛先:サーバー サブネット、ネクスト ホップ:LR2

- 入力トラフィック インターフェイスが CN-GW 2 の場合、出力インターフェイスを見つけるためのルート ルックアップは LR2 にあります。
 - ルート 1:宛先:クライアント サブネット、ネクスト ホップ:R1
 - ルート 2:宛先:サーバー サブネット、ネクスト ホップ:R2

非対称トラフィック フロー

CN-Series HSF は、非対称トラフィック フローもサポートします。たとえば、クライアントから サーバーへのトラフィック マッチング セッション1は CN-GW 1 を流れ、サーバーからクライ アントへのトラフィック マッチング セッション1は CN-GW 2 を流れます。非対称トラフィック フローの場合、R1 に面するすべてのインターフェイスが同じゾーンにある必要があります。同 様に、R2 に面するすべてのインターフェイスは同じゾーンにある必要があります。

インター LR ルーティング

たとえば、入力トラフィック インターフェイスが CN-GW 1 の場合、出力インターフェイスを見 つけるためのルート ルックアップは LR1 にあります。ネクスト ホップを LR2 としてサーバー に到達するルートがある場合、CN-NGFW はトラフィックを LR2 に送信します。CN-GW 2 LR2 ルート ルックアップに基づいて、パケットがサーバーに送信されます。

- STEP 1 ネットワーク > ルーティング > ルーティング プロファイル > BFDに移動し、 [テンプレート] ドロップダウンから変数テンプレートを選択します。
 外部ルーターと論理ルーターで BFD を有効にする必要があります。
- STEP 2 「追加]をクリックして BFD プロファイルを追加します。
- **STEP 3**| 名前を入力します。
- **STEP 4**| BFDの運転 Mode (モード) を選択します。
 - Active[アクティブ] BFDがピアに対してコントロールパケットを送信開始します(デフォルト)。最低でも1つのBFDピアがアクティブに設定されている必要があります。両方がアクティブでも構いません。
 - Passive[パッシブ] BFDはピアからコントロールパケットが送られてくるまで待機し、要求に応じて応答を行います。
- STEP 5 Desired Minimum Tx Interval (ms) [目標の最低Tx間隔(ミリ秒)]を入力します。これ はBFDプロトコル(BFDと呼ぶ)にBFD制御パケットを送信させる最低間隔(ミリ秒)で あり、これにより送信間隔についてピアとネゴシエートを行います。
- STEP 6 Detection Time Multiplier [検知時間乗数]を入力します。ローカルシステムはリモートシステムから受信したDetection Time Multiplier (検知時間乗数)を同意済みのリモートシステムの送信間隔(Required Minimum Rx Interval (最低 Rx 間隔要件)および最後に受信したDesired Minimum Tx Interval (目標の最低 Tx 間隔)のうち、いずれか大きい方)で掛けることで検知時間を算出します。検知時間が過ぎるまでにBFDがピアからのBFDコントロー

ルパケットを受信しない場合、障害が発生していることを意味します。範囲は 2 ~ 50、デフォルトは 3 です。

- STEP 7 Hold Time (ms) [待機時間(ミリ秒)] を入力します。これは、リンクが確立されてからBFDがBFDコントロールパケットを送信するまでに待機する時間です(ミリ秒単位)。Hold Time (待機時間)はBFDアクティブモードのみに適用されます。BFDがHold Time [待機時間] 内にBFDコントロールパケットを受信した場合、それを無視します。範囲は0~120000、デフォルトは0です。
- STEP 8 Multihop [マルチホップ]を選択してBGPマルチホップを介したBFDを有効にします。Minimum Rx TTL [最低Rx TTL]を入力します。これは、BGPがマルチホップBFDをサポートしている場合にBFDが受け入れる(受信する)BFD制御パケット内のTime-to-Live値(ホップ数)の最低値です。(範囲は1~254。デフォルト値はありません)
- STEP 9| [OK] をクリックして、BFD プロファイルを保存します。

BFD Profile (Read Only)	()				
Name	default				
Mode	Active O Passive				
Desired Minimum Tx Interval (ms)	1000				
Desired Minimum Rx Interval (ms)	1000				
Detection Time Multiplier	3				
Hold Time (ms)	0				
Enable Multihop					
Minimum Rx TTL [1 - 254]					

ок (

Cancel

CNシリーズHSFのデプロイメント

- STEP 10 | 論理ルーターのスタティック ルートを設定します。
 - 1. ネットワーク>ルーティング>論理ルーターに移動し、 [テンプレート] ドロップダ ウンから変数テンプレートを選択します。
 - 2. 静的 > IPv4タブを選択し、 [追加] をクリックします。
 - 3. スタティックルートの Name (名前) を入力します。
 - 4. 宛先ルートとネットマスクを入力します。192.168.200.0/24 などです。
 - 5. [インターフェイス] に、パケットがネクスト ホップに移動するために使用する発信 インターフェイスを指定します。
 - 6. [ネクスト ホップ] で [**ip-address**] を選択し、内部ゲートウェイの IP アドレスを入 力します。たとえば、192.168.100.2 です。
 - 7. ルートの Admin Distance を入力して、この論理ルーターの静的ルートに設定されてい るデフォルトの管理距離を上書きします (範囲は 10 ~ 240、デフォルトは 10)。
 - 8. ルートの Metric (メトリック) を入力します (範囲は 1~65,535)。
 - 9. 前の手順で作成した BFD プロファイルを静的ルートに適用して、静的ルートが失敗した場合にファイアウォールがルートを削除し、代替ルートを使用するようにします。
 - 10. **OK** をクリックします。

BFD 設定は、CN-GW とパスの障害に対処します。次のトラフィック フロー ダイアグラムで は、クライアントとサーバー間の 2 つの SSH セッションについて考えます。セッション 1 はパ ス 1 を流れており、セッション 2 はパス 2 を流れています。CN-GW 1 またはパス 1 がダウンし ている場合、R1 と CN-GW 1、R2 と CN-GW 1 の間の BFD 設定は、R1 がパス障害を識別し、パ ス 2 を介してトラフィックを送信するのに役立ちます。R1 に面するインターフェイスは、同じ ゾーンにある必要があります。同様に、R2 に面するインターフェイスは同じゾーンにある必要 があります。

ルート 1:宛先:クライアント サブネット、ネクスト ホップは R1、メトリック 10

ルート 2:宛先:サーバー サブネット、ネクストホップは LR2、メトリック 11



CN-Series HSF の概要と監視を表示する

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

Panorama Web インターフェイスの[ファイアウォール クラスタ] タブで、CN-Series HSF の概要と 監視情報を表示できます。ファイアウォール クラスタを表示してアクセスするには、Panorama > 管理者ロール > Web UI リストからファイアウォール クラスタ > 有効にする必要があります。 詳細については、管理者ロール プロファイルを設定するを参照してください。

[ファイアウォール クラスタ]でクラスタの詳細を表示するには**Panorama** > プラグインから Clustering 1.0.0 プラグインをインストールする必要があります。

🚺 PANORAMA	DASHBOARD ACC N		Templates T TS NETWORK DEVICE	PANORAMA			<u>ش</u>	iommit 🗸 🛛 🕆 🕶 🗸			
Panorama 🗸	▼										
Syslog	Q (dustering 1.0.0							$_{18/265}$ \rightarrow \times			
Email	FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS	RELEASE NOTE URL			
The RADIUS	v Name distering										
C SCP	clustering-1.0.0-c40.main	1.0.0-c40.main	2022/06/30 16:51:43	12M	1		Install 50 Delete 50				
Kerberos	clustering-1.0.0-c42.main	1.0.0-c42.main	2022/07/06 10:58:08	12M	1		Install 50 Delete 50				
C Scheduled Config Export	clustering-1.0.0-c44.main	1.0.0-c44.main	2022/07/07 14:07:57	12M	1		Install 50 Delete 50				
Dynamic Updates O Plugins Kubernetes	clustering-1.0.0-c45.main	1.0.0-c45.main	2022/07/08 15:33:49	12M	1		Install So Delete So				

概要ビュー

過去5分間にファイアウォールによってキャプチャされた CN-Series クラスタに関する情報を表示します。更新ボタンをクリックして、最新の詳細を読み込みます。

🚯 PANORAMA	DASHBOARD A	ACC MONITOR POLI	Device Groups CIES OBJECTS	⊢ Templates NETWORK I		ма					t Commit V	°⊡ ⊞~ Q
Panorama 🗸 🗸												G 🕐
Setup High Availability Config Audit Managed WildFire Clusters Managed WildFire Papilance Config Config Clusters	Custers Summary View Monitoring											
Password Profiles												11 items \rightarrow \times
Administrators •	CLUSTER NAME	SOFTWARE VERSION	PLUGINS USED ON CLUSTER	DEVICE GROUP	TEMPLATE STACK	CLUSTER TYPE	CLUSTER STATE	MEMBERS AFFECTED	SYSTEM LOG DETAILS	SPECIFIC ERROR	CLUSTER NODE	CPU COUNT
Access Domain	∨ cluster-001	11.0.1-c114.dev_e_rel	vm_series-4.0.1 dlp-4.0.0	DG-FW-Cluster-3	cluster-001-ts	CN	ERROR	1				
Authentication Sequence	CN-MGMT-Acti	ive 11.0.1-c114.dev_e_rel	vm_series-4.0.1 dlp-4.0.0	DG-FW-Cluster-3	cluster-001-ts							
Data Redistribution	CN-MGMT	11.0.1-c114.dev_e_rel	vm_series-4.0.1 dlp-4.0.0	DG-FW-Cluster-3	cluster-001-ts							
Managed Devices	CN-NGFW-9						IMPACTED				pan-ngfw-dep- 9864d656b-dnfng	
Health •	CN-DB-10						IMPACTED				pan-db-dep- 5ddbd9d584-hnvv7	
Troubleshooting	CN-GW-2						IMPACTED				pan-gw-dep- 799f488d6-l9jzd	
Device Groups	CN-DB-5						IMPACTED				pan-db-dep- 5ddbd9d584-9h7k6	
Collector Groups	CN-GW-1						IMPACTED				pan-gw-dep- 799f488d6-nfrh9	
 Certificate Management Certificates 	CN-NGFW-6						IMPACTED				pan-ngfw-dep- 9864d656b-ltz4b	
Certificate Profile	CN-NGFW-8						ERROR				pan-ngfw-dep- 9864d656b-ztwv6	
SCEP	CN-NGFW-7						IMPACTED				pan-ngfw-dep- 9864d656b-t7nhx	

項目	詳説
クラスタ名	ファイアウォール クラスタの名前。
ソフトウェア バージョン	PAN-OSバージョン。
クラスタで使 用されるプラ グイン	クラスタで使用されるプラグインのリスト。 ① <i>CN-Series</i> のファイアウォール プラグインのみがサポートされ ています。
テンプレート スタック	クラスタに関連付けられたテンプレート スタックの名前。
デバイス グ ループ	クラスタに関連付けられたデバイス グループの名前。
Cluster State クラスタの状 態	クラスタが影響を受けるかどうかを表示します。
クラスタ タ イプ	クラスタのタイプ。 CN-Series のファイアウォール クラスタ タイプのみがサポート されています。
影響を受ける メンバー	影響を受けるクラスタ メンバーの数とその名前。
システムログ の詳細	システム イベントの詳細を表示します。
特定のエラー	クラスタ内の特定のエラーのリスト。リンクをクリックして、ログを表示で きる監視 > ログ > システムの下にあるエラーの詳細を表示します。
クラスタ ノード	ポッドの名前。
CPU 数	使用されている CPU の数。

モニタリング

	ر Device Groups مر روانده مر المساولية مر المساولية مر المساولية مردم مردم مردم مردم مردم مردم مردم مرد	روان کې او کې د م						
Panorama V Response Managed Software C High Availability	Cluster CN-series V	S (D)						
Config Audit Managed WildFire Clusters Managed WildFire Appliance Summary View	Monitoring							
Password Profiles Administrators Administrators	 Impacted 	0 ок						
**** Access Domain @E. Authentication Profile ***** ### Authentication Sequence ************************************	Clusters: 1 / 1	Clusters: 0 /1						
Data Redistribution Scheduled Config Push Device Quarantine Device Quarantine	Clusters List: cluster-001	Clusters List: '						
Summary Health								
項目	詳説							
マネージド	ファイアウォール クラスタを選	髪択します。						
ソフトウェア	ON-Seriesのファイアウォ	ール クラスタ タイプのみがサポート						
9789-	されています。							
影響を受けた	影響を受けるファイアウォール	クラスタのリスト。						
	• CN-Clusters - 影響を受ける	CN-Series ファイアウォール クラスタの数。						
	・ Clusters Impacted - 影響を受	けるクラスタのリストを表示します。						
	クリックすると、[相互接続スラ	テータス]および[クラスタ使用率]ダッシュボー						
	ドにクラスタに関する詳細情報が表示されます。							
OK	OK 影響を受けていないファイアウォール クラスタのリスト。							
	• Clusters - 影響を受けていな	い CN-Series ファイアウォール クラスタの						
	数0 の 1 日間によ 取りしてい	· · · · · · · · · · · · · · · · · · ·						
	• Clusters List - 影響を受けて	いないクラスタのリストを表示します。						
	クリックすると、[相互接続スラ	テータス]および[クラスタ使用率]ダッシュボー						
	トにクラスタに関りる評補情報	が衣小されより。						
相互接続ス	選択した時間枠のクラスタ相互接続の詳細を表示します。							
テータス	[過去5分間]を選択して、次の詳細を表示します。							
	・ Cluster Name — ファイアウ	ォール クラスタの名前。						
	• Cluster Type — クラスタのタ	マイプ。						
	$\bigcirc CN-Series OD rdrt$	ウォール クラスタ タイプのみがサポー						
	• Cluster Creation Time— クラ	マスタを作成した時刻。						

CN-Series ファイアウォール クラスタのヘルス情報を表示します。

項目	詳説							
	• Current Cluster State— クラスタが影響を受けているかどうかを表示。							
	 Current Cluster Detail— 現在のクラスタ状態のリンクをクリックして、 影響を受けるクラスタの詳細を表示します。 							
	• Cluster Interconnect Status — クラスタの相互接続性を表示します。							
	 Current Cluster Detail— 現在の相互接続ステータス リンクをクリック して、影響を受けるクラスタの詳細を表示します。 							
	• Traffic Interconnect - トラフィック相互接続のステータス。							
	• External Connection— 外部接続のステータス。							
	• Impacted Links—影響を受けるリンクの数。							
	• Management Connectivity — 管理接続の数。							
	• Impacted Cluster Member — 影響を受けるクラスタ メンバーのリスト。							
	• Time Stamp Hi-Res Uptime — アップタイムのタイム スタンプ。							
	• Time Stamp Hi-Res Downtime — ダウンタイムのタイム スタンプ。							
	他の時間枠を選択すると、次の情報のみが表示されます。							
	• クラスタ名							
	・ クラスタ タイプ							
	• クラスタ作成時間							
	• 現在のクラスタの状態							
	• クラスタ相互接続の状態							
	 トラフィック インターコネクト 							
	• 外部接続							
クラスター使 用率	ファイアウォール クラスタのスループット、メモリ、およびデータ使用率を 表示します。							
	 Cluster Name — ファイアウォール クラスタの名前。クラスタ名を展開すると、そのクラスタ内のすべてのポッドの詳細が表示されます。 							
	 Cluster Details — クラスタ名のリンクをクリックして、選択したクラス タのスループット、メモリ、およびデータ使用率の詳細を表示します。 							
	• Cluster Type — $2 \overline{7}$							
	CN-Seriesのファイアウォール クラスタ タイプのみがサポー トされています。							
	• Cluster State — クラスタの状態を表示します。							

項目	詳説
	• Cluster Throughput (gbps) — Gbps 単位でのファイアウォール クラスタス ループット。
	 CPS — 1 秒あたりの接続数。
	• Session Count (Sessions) — セッション数。
	• Average Data Plane (%) Within Health Threshold — 平均データ プレーンし きい値 (パーセント)。
	• Management Plane CPU (%) - 管理プレーンの CPU 使用率(パーセント)。
	 Management Plane Mem (%) - 管理プレーンのメモリ使用率(パーセント)。
	• Logging Rate (Log/Sec) — クラスタでログが生成されるレート。
	• DP Auto-Scale Status - データプレーンのオートスケールの詳細。

CN-Series HSF デプロイメントの検証

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

CN-Series HSFのデプロイメントは、**Panorama** > **Kubernetes**のデプロイメントセクションで検証 できます。デプロイの詳細を表示するには、[デプロイメント ステータス]の下のリンクをクリッ クします。

デプロイされたポッドとその現在のステータスは色分けされ、[デプロイメントステータス]セ クションに表示されます。失敗したポッドのデプロイメントに関するメモの下にあるリンクをク リックすると、詳細が表示されます。

Q										
	NAME	DESCR	PTION	KUBERNETES CLUSTER T	KUBERNETES CLUSTER TYPE		DEPLOY	MENT STATUS	ACTION	
	cluster-002	control	ler-10-5-84-130 OpenShift			DG-FW-Cluster-3	Success	_	Redeploy	
	cluster-001	Deployment Details					(Redeploy	
		Cluster Nan	e cluster-002						Undeploy	
		Deta	Is Deployment completed successfully	at time 11/22/2022, 05:00:	D3 UTC					
		Time Stan	p 11/22/2022, 05:00:03 UTC							
		Pods Deployed	SL POD NAME		STATUS	NOTE				
		Current State	pan-db-dep-d6fb496b-hfmlp		•		1			
			pan-db-dep-d6fb496b-jf2ms		•					
			pan-gw-dep-5cd5c87d76-4kbfk		•					
			pan-gw-dep-5cd5c87d76-przjx		•					
ł			pan-mgmt-sts-0		•					
			pan-mgmt-sts-1		•	Generate Kubernetes log				
			pan-ngfw-dep-5cd8f55848-dbhv	vh	•					
			pan-ngfw-dep-5cd8f55848-pq6k	s	•					
			pan-ngfw-dep-5cd8f55848-rsbq	n	•					
			pan-ngfw-dep-5cd8f55848-slk5l	pan-ngfw-dep-5cd8f55848-slk5l						
							Close			



Panorama CLI で次のコマンドを使用してログを生成します。

debug plugins kubernetes generate-pod-log deployment_name pod_name <value> ポッドの名前

show plugins kubernetes deployment-status

show plugins kubernetes deployment-details name

Kubernetes プラグインと CN-Series HSF 間の同期に関する問題のデバッグ

Kubernetes プラグインは、Watch API を使用して CN-Series HSF に関する情報をポッド、サービス、ノードから収集します。Watch API は、クラスタの状態が変化したときに更新を送信する通知ベースの API です。プラグインとデプロイされた CN-Series HSF が確実に同期されるように、 プラグインは通知を受信し、HPA とアップグレード/ダウングレードイベントの通知を表示します。

プラグインは次のデバッグコマンドを使用して、プラグインのステータスに基づいて特定のノー ドをデバッグします。

debug plugin kubernetes kubectl-logs pod <pod-name>

このデバッグコマンドは、コマンドで渡されたノードの kubectl describe ログを含むログファ イルを生成し、プラグイン ログ ファイルに保存します。

EKS 環境で KEDA を使用するカスタム メトリック ベー スの HPA

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

EKS 環境に HPA を実装するには、KEDA (Kubernetes ベースのEvent Driven Autoscaler)を使用す る必要があります。カスタム メトリクス ベースの HPA 実装の前提条件は次のとおりです。

- YAML からのクラスタリング用の HPA を有効にします。
 - pha-cn-mgmt-configmap.yaml ファイルに HPA パラメータが入力されていることを確認します。
 - PAN_NAMESPACE_EKS フィールドに、リージョン内の AWS アカウント全体で一意の名前 が付いていることを確認してください。これにより、同じ EKS 名前空間を持つ異なる CN クラスタのメトリクスが上書きされることが回避されます。
- CN-MGMT がメトリクスを Cloudwatch にパブリッシュします。

CN-MGMT ポッドには、Cloudwatch リソースにアクセスし、CN-NGFW メトリクスを収集 し、カスタム メトリクスを Cloudwatch に公開するために必要な権限が必要です。これは、 ノードグループの作成時に指定したノード IAM ロールに CloudWatchFullAccess ポリ シーを追加することによって行われます。

 AWS からクラスタ オートスケーラーをデプロイします。詳細については、クラスタ オート スケーラーを参照してください。

AWS で KEDA を認証する

KEDAを認証するには、keda サービス アカウントの role-arn に注釈を付けることで、IAM ロール を keda オペレーター サービス アカウントに関連付けることができます。このステップが推奨さ れるのは、ノードの IAM ロールに Cloudwatch アクセスを追加する必要なく、keda が実行されて いるノード全体ではなく、keda サービス アカウントのみが Cloudwatch にアクセスできるように するためです。

IAM ロールを keda オペレーター サービス アカウントに関連付けるには:

1. クラスタの IAM OIDC プロバイダを作成する - クラスタに IAM OIDC プロバイダを作成する 必要があるのは 1 度だけです。

- IAM ロールを作成し、サービス アカウントに必要な権限を含む IAM ポリシーをそのロール にアタッチします。このステップを実行する際は、必ず Cloudwatch アクセス ポリシーを指定 してください。
- **3.** IAM ロールをサービス アカウントに関連付ける このタスクは、AWS リソースへのアクセスが必要な各 Kubernetes サービス アカウントごとに実行します。
- **4.** AWS からクラスタ オートスケーラーをデプロイします。詳細については、クラスタ オート スケーラーを参照してください。

KEDA ポッドをデプロイする

Keda ポッドをデプロイするには、最新の keda ファイルをダウンロードします。

kubectl apply -f keda-2.7.1.yaml

プラグインは、スケーリング要件に従って提供された入力に基づいて yaml を変更して適用します。

Cloudwatch コンソールの値を確認し、ターゲットポッドがどのようにスケールインおよびス ケールアウトされるかを確認します。

CNシリーズHSFでのダイナミックルーティングの設定

どこで使用できますか?	何が必要ですか?					
 CNシリーズHSFファイアウォールのデプ	 PanoramaPAN-OS 11.1バージョン以上で動					
ロイメント	作している					

CNシリーズHyperscale Security Fabric(HSF)では、BGPおよびBGP over BFDプロトコルによ るダイナミック ルーティングが導入されました。ダイナミック ルーティングを使用すると、論 理ルータ間で使用可能なプロファイル ベースのフィルタリング リストと条件付きルートマップ を通じて、安定性、パフォーマンス、および可用性に優れたレイヤー3ルーティングを実現でき ます。これらのプロファイルは、各ダイナミック ルーティング プロトコルのルートをフィルタ リングするためのより細かい粒度を提供し、複数のプロトコル間でのルートの再配布を改善しま す。

BGPは、自律システム内で使用可能なIPプレフィックスに基づいて、データを送ることのできるパスを検索し、最適なルートを選択します。Bidirectional Forwarding Detection(BFD)の設定は、CN-GWポッドとパス障害を管理します。

ダイナミックルーティングを有効にするには、パノラマとCNシリーズHSFクラスタを設定す る必要があります。クラスタには少なくとも2つのCN-MGMT、2つのCN-NGFW、2つのCN-DB、1つのCN-GWが必要です。BGPピアリングは、CNクラスタと外部ルータの間で設定されま す。

CNシリーズHSFでは、PANOS 11.x.xでダイナミック ルーティングがサポートされ ます。PAN-OS 11.0の取得については、CNシリーズのデプロイメントのイメージと ファイルの取得を参照してください。

Panoramaでは、デバイス グループを設定し、デバイス グループを通じてHSFクラスタを管理す る必要があります。HSFクラスタを構成するには、<u>HSFクラスタのデプロイする</u>を参照してくだ さい。

HSFクラスタでBGPを設定するには、以下の手順を実行する必要があります。

- **1.** Advanced Routing(高度なルーティング)を有効にします。
- 2. 論理ルーターを設定する。
- 3. CN-GWループバック インターフェースのスタティック ルートを作成します。
- 4. 高度なルーティングエンジンでBGPを設定する。

<u>1</u>. 現在、BGPルーティングでサポートされているのはIPv4のみです。

2. ピアの作成中に、必ずループバックセッションを作成し、 [*Addressing*] タ ブの各*CN-GW*にループバック*IP*アドレスを提供していることを確認します。

- **5.** (任意) 認証、タイマー、アドレスファミリ、ダンプニング、BGP へのルート再配信、および BGPフィルタリング用のBGPルーティング プロファイルを作成します。
- **6.** (任意) アクセス リスト、プレフィクス リスト、AS Pathアクセス リスト、コミュニティ リ スト、ルート マップなど、高度なルーティング エンジンのフィルタを作成します。
- 7. [Panorama へのコミット]をクリックします。設定がパノラマにコミットされた後、BGPは 各CN-GW 設定されます。

BGPステータスを確認するには、CN-MGMTにログインし、以下のコマンドを実行します。

• show advanced-routing bgp summary

admin@pan-mgmt-sts-1.cl	uster-001> show	advanced-rout	ing bgp r	oute logi	cal-router	slot1-LR-1						
Status codes: R remove s suppre Nexthop codes: @NNN nex Origin codes: e egp, i	d, d damped, * v. ssed, i internal thop's vrf id, < igp, ? incomple	alid, r ribFa , > best, h h announce-nh- te	ilure, S istory self	stale, =	multipath,							
Logical router: slot1-L BGP table version is 10 Default local pref 100,	R-1 , local router I local AS 88	D is 88.0.0.1	, vrf ID									
Network *> 3.3.3.0/24 *> 192.168.85.0/24	Next Hop 0.0.0.0 200.0.0.1	Metric 0 0	LocPrf We 100 3 100	ight Path 2768 i 0 22 i								
Displayed 2 route(s) 2	path(s)											
Logical router: slot1-L BGP table version is 0, Default local pref 100,	R-1 local router ID local AS 88	is 88.0.0.1,	vrf ID 0									
Network	Next Hop	Metric	LocPrf We	ight Path								
Displayed 0 route(s) 0	path(s)											
admin@pan-mgmt-sts-1.cl	uster-001> show a	advanced-rout	ing route	type bgg	logical-re	outer slot1-LF	-1					
Logical Router: slot1-L	R-1											
flags: A:active, E:ecmp	, Oi:ospf intra-	area, Oo:ospf	inter-ar	ea, 01:08	pf ext 1, (02:ospf ext 2						
destination		protocol	nextho	q			distance	metric	flag	tag	age	inte
192.168.85.0/24		bgp	200.0.						AE		00:04:07	
192.168.85.0/24 et1/3 total route shown: 2		pđĐ	¥2.2.2.	222					AE		00:04:07	ethe

• show advanced-routing bgp peer status

admin@pan-mgmt-sts-1.testing> show advanced-routing bgp peer status peer-name DHCP-PEER

 • show advanced-routing bgp peer details

admin@pan-mgmt-sts-1.testir	ng> show advanced-routing bgp peer details					
Peer: DHCP-PEER						
Peer name	DHCP-PEER					
Logical router:	Slot1-LR					
Remote router ID:	11.11.11.1					
Remote AS:	65008					
Remote address:	192.168.100.109:34986					
Local address:	192.168.100.102:179					
Peer group:	DHCP-BGP					
Peer status:	Established					
Up time:	188 s					
Hold time:	90 s (configured 90)					
Keepalive interval:	30 s (configured 30)					
Connection retry timer:	15 s					
Estimated RTT:	3 ms					
Last reset time:	222 s ago					
Last reset reason:	No AFI/SAFI activated for peer					
BGP connection:	sharedNetwork					
Connection established:	2					
Connection dropped:	1					
Address family:	ipv4Unicast					
Packet queue length:	0					
Update group id:	2					
Sub group id:	2					
Prefix allowed Max:	1000 (warning-only)					
Prefix accepted:	2810					
Prefix Sent:	2920					
Prefix allowed Max warnn	ing: True					
Prefix allowed warnning	threshold: 100					
Inbound soft reconfigura	tion allowed: True					
Neighbor capabilities:						
4byteAs	advertisedAndReceived					
extendedMessage	advertisedAndReceived					
addPath	{'ipv4Unicast': {'rxAdvertisedAndReceived': True}}					
routeRefresh	advertisedAndReceivedOldNew					
enhancedRouteRefresh	advertisedAndReceived					
multiprotocolExtensions	{'ipv4Unicast': {'advertisedAndReceived': True}}					
hostName	{'advHostName': 'pan-mgmt-sts-1.testing', 'advDomainName': 'n/a', 'rcvHostName': 'vyos', 'rcvDomainName': 'n/					
gracefulRestart	advertisedAndReceived					
admin@pan-mgmt-sts-1.testi	ng>					
CN-MGMTからBFDステータスを確認するには、次のコマンドを実行します。

show advanced-routing bfd summary

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bfd summary
SESSION ID: 114
                     ethernet1/3
    Interface:
    Logical Router: Slot1-LR (id:1)
    Local IP Address: 192.168.100.104
Neighbor IP Address: 192.168.100.109
    Discriminator (local/remote): 0xb150bb9e / 0x4a1dc50a
    State:
                     up
    rState:
                     up
    Up Time:
                     0d 0h 8m 23s 670ms
                     Slot 9 - DP 0
    Agent DP:
    Errors:
                     0
```

show advanced-routing bfd details

```
admin@pan-mgmt-sts-1.testing> show advanced-routing bfd details
BFD Session ID: 114
    Version:
                    1
                   ethernet1/3
    Interface:
    Protocol:
                    BGP
    Local IP Address:
                             192.168.100.104
    Neighbor IP Address: 192.168.100.109
                             default
    BFD profile:
    State (local/remote):
                                  up / up
                   0d 0h 8m 46s 650ms
    Up Time:
    Discriminator (local/remote): 0xb150bb9e / 0x4a1dc50a
    Mode:
                    Active
    Demand Mode:
                   Disabled
    Poll Bit:
                   Disabled
    Multihop:
                    Disabled
    Multihop TTL:
                    255
    Local Diag Code:
                                    0 (No Diagnostic)
    Last Received Remote Diag Code: 0 (No Diagnostic)
    Transmit Hold Time:
                                   Oms
    Desired Min Tx Interval:
                                   1000ms
    Required Min Rx Interval:
                                   1000ms
    Received Min Rx Interval:
                                  1000ms
    Negotiated Transmit Interval: 1000ms
    Detect Multiplier:
                                   3
    Received Multiplier:
                                  3
    Detect time (exceeded):
                                  3000ms (1)
    Tx Control Packets (last):
                                  649 (861ms ago)
    Rx Control Packets (last):
                                  604 (669ms ago)
    Agent DP:
                   Slot 9 - DP 0
    Errors:
                    Θ
    Last Recieved Packet:
        Version:
        My Discriminator:
                                 0x4a1dc50a
        Your Discriminator:
                                 0xb150bb9e
        Diag Code: 0 (No Diagnostic)
        Length:
                       24
        Demand bit:
                       0
                               Poll bit:
                                               0
                               Multipoint:
        Final bit:
                       Θ
                                               Θ
        Control Plane Independent:
                                      0
        Authentication Present:
                                      Θ
        Desired Min Tx Interval:
                                     1000ms
        Required Min Rx Interval:
                                      1000ms
        Detect Multiplier:
        Required Min Echo Rx Interval: 50ms
```

CN-Series HSF:ユースケース

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

以下は、CN-Series HSF のユースケースです。

- 5G トラフィック テスト
 - N3+N4の可視性と相関ポリシーによる 5G セキュリティ
 - アプリケーション識別と脅威検査によるインバウンド/アウトバウンド保護
- サポートされるカスタム メトリックに基づくファイアウォールのスケール アウト
- テスト ケース:CN-MGMT 障害処理
- テスト ケース:CN-NGFW 障害処理
- テストケース:CN-DBの障害処理

5G トラフィック テスト

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
	• Helm 3.6 or above version client

ネットワーク エッジを保護するには、トラフィックの検査と制御 (セキュリティ要件) と、高帯 域幅、低遅延、リアルタイム アクセス (ユーザー エクスペリエンス) のバランスを取る必要があ ります。トラフィックが多数のファイアウォールで処理される場合、アプリケーションがエッ ジサイトでホストされる場合、またはネットワーク エッジが IoT データの集約ポイントである 場合、これらの問題は飛躍的に困難になります。さらに、5G ネットワークではユーザーとコン トロール プレーンが分離されているため、加入者レベルまたはデバイス レベルでセキュリティ ポリシーを適用することが困難になり、脅威に対するコンテキスト ベースの可視性が欠如しま す。N3 および N4 インターフェイスを備えたファイアウォールには、次の機能があります。

- 接続されたデバイス間の信号レベルの可視性
- PFCP と GTP-U のステートフルインスペクション

• サブスクライバー ID/機器 ID/スライス ID を GTP-U トラフィックの脆弱性と関連づけ

CN-Series HSF の 5G トラフィックのユースケースは次のとおりです。

- N3+N4 可視性と相関性ポリシーによる 5G セキュリティ
- アプリケーション識別と脅威検査によるインバウンド/アウトバウンド保護

次の図は、プライベート 5G ネットワークを使用する企業を示しています。5G のコア機能はク ラウドベースか、サービス プロバイダーの中央サイトにあります。5G アクセスと UPF 間の接続 には N3 インターフェイスを使用します。GTP-U トンネルは N3 インターフェイス上でユーザー プレーン トラフィックを伝送します。UPF とセッション管理機能 (SMF) 間の接続には、N4 イン ターフェイスを使用します。PFCP プロトコルは、N4 インターフェイス上の UDP 交換を使用し てパケット転送ルールを交換します。



この図は、ユーザー プレーン機能 (UPF) がエッジまたは MEC ロケーションにあり、5G コア機 能がクラウドベースまたはサービス プロバイダーの中央サイトにある 5G ネットワークにおける MEC を示しています。5G アクセスと UPF 間の接続は N3 インターフェイスを使用し、GTP-U ト ンネルは N3 インターフェイスを介してユーザー プレーン トラフィックを伝送します。UPF と SMF 間の接続は N4 インターフェイスを使用し、PFCP プロトコルは N4 インターフェイス経由 で UDP を使用してパケット転送ルールを交換します。



N3+N4 可視性と相関性ポリシーによる 5G セキュリティ

このテストケースでは、CNF クラスタが N3+N4 インターフェイスからのトラフィックを検査し て保護する能力を評価します。

- **STEP 1**| N3+N4 インターフェイスからのトラフィックを検査して保護するための最初のステップとして、GTP セキュリティを有効にする必要があります。
 - 1. ファイアウォール インターフェイスにログインします。
 - 2. [デバイス>セットアップ>管理>一般設定を選択し、[GTP-U セキュリティ]を選択し ます。
 - 3. **OK**をクリックします。
 - 4. 変更を **Commit** (コミット) します。
 - 5. Device > Setup > Operations を選択し、 Reboot Device を実行します。

- STEP 2 モバイル ネットワーク保護プロファイルを作成し、GTP-U 検査を有効にします。
 - オブジェクト>セキュリティプロファイル>モバイルネットワーク保護を選択します。
 - プロファイルを追加し、「5G_Mobile_Network_Protection」などの名前を入力します。
 - 3. [PFCP]タブで、ステートフル検査を有効にします。

Mobile Netwo	k Protection Profile		0
Name	5G_Mobile_Network_Protection Mobile Network Protection Profile for 5G (N4 and N	3 interfaces)	
GTP Inspection	Filtering Options GTP Tunnel Limit Ove	erbilling Protection Other Lo	og Settings
GTP-C GTP-U	5G-C PFCP		
Action Bloc	k OAlert	End User IP Address Spoofing GTP-in-GTP	block v alert v
 Rese Orde Leng Spar Unst 	er of IE th of IE e Flag in Header upported message type		GTP-U Content Inspection GTPv1-C, GTPv2-C and/or 5G-C Stateful Inspection with GTP-U Content Inspection provides IMSI and IMEI correlation with IP traffic encapsulated in GTP-U packets
			OK Cancel

- STEP 3 PFCP トラフィックに対してファイアウォールに実行させる状態チェックと、状態チェックが失敗した場合にファイアウォールに実行させるアクションを選択します。
 - 1. 使用したい状態チェックを決めてください。
 - 関連メッセージのチェック:順序が不順であるか、拒否された PFCP 関連メッセージ がないかチェックします。
 - セッションメッセージを確認 順序が間違っている、または拒否された PFCP セッション メッセージがないかどうかを確認し、すべての PFCP セッション メッセージ が既存の PFCP アソシエーションと一致することを確認し、PFCP アソシエーション が設定される前に到着した PFCP セッション メッセージを警告またはドロップしま す。
 - シーケンス番号を確認 PFCP 応答のシーケンス番号が前の PFCP 要求メッセージの シーケンス番号と一致することを確認します。

- 2. 状態チェックが失敗した場合にファイアウォールに実行させたいアクションを選択します。
 - allow トラフィックを許可し、GTP ログにログエントリを生成しないでください。
 - block トラフィックをブロックし、GTP ログに重要度の高いログ エントリを生成します。
 - alert (デフォルト) トラフィックを許可し、GTP ログに重要度の高いログエントリ を生成します。
- STEP 4 (オプション) PFCP 検査のロギングを設定します。
 - 1. ファイアウォールにログエントリを生成させるタイミングを選択します。
 - PFCPアソシエーション開始でログ
 - PFCPアソシエーション終了でログ
 - **PFCP**セッション開始でログ
 - PFCPセッション終了でログ
- STEP 5| PFCP および GTP-U メッセージのその他のログ設定を有効にする
 - 1. [その他のログ設定] タブで、ログに含める **PFCP** 許可メッセージのタイプを選択し ます。
 - これらのオプションはトラブルシューティングにのみ有効にしてください。
 - セッション確立:これらの PFCP メッセージは、GTP-U トンネルの確立を含むセッションを設定します。
 - セッション変更:これらの PFCP メッセージは、セッション ID または PDR ID が変 更された場合 (たとえば、4G から 5G ネットワークに移動した結果として)送信され

ます。これには、PFCP セッション変更要求や PFCP セッション変更応答などのメッ セージが含まれます。

 セッション削除:これらの PFCP メッセージは、関連リソースの解放を含む PFCP セッションを終了します。

Mobile Networ	k Pro	tection Profile	?
Name Description	5G_Mo Mobile Filter	bile_Network_Protection Network Protection Profile for 5G (N4 and N3 interfaces) ing Options GTP Tunnel Limit Overbilling Protection Other Log Settings	
GTP-C GTP-U	5G	-C PFCP	
Check Association Me Check Session Me	ssages	alert alert	~
Cneck Sequence N	umber	 alert ✓ Log at PFCP association start ✓ Log at PFCP association end ✓ Log at PFCP session start ✓ Log at PFCP session end 	~

OK Cancel

- STEP 6 送信元と宛先を N3 と N4 インターフェイス、アプリケーションをそれぞれ GTP-U と PFCP とする 2 つのセキュリティ ポリシーを作成します。
 - 1. ポリシー > セキュリティを選択し、セキュリティ ポリシー ルールを名前で追加または 変更します。
 - 2. [ソース] タブを選択し、ソースゾーンを追加するか、 [任意] を選択します。
 - 3. 送信元アドレスには、N3 インターフェイスの 5G 要素エンドポイントのアドレス オブ ジェクトを追加します。
 - 4. [宛先] には、N3 インターフェイスの 5G 要素エンドポイントの宛先アドレス アドレス アドレス オブジェクトを追加します。
 - 5. ユーザー プレーンなど、許可するアプリケーション (GTP-U や PFCP) を追加します。
 - 6. [アクション] タブで、許可などのアクションを選択します。
 - 7. 作成したモバイルネットワーク保護プロファイルを選択します。
 - 8. 脆弱性保護など、適用する他のプロファイルを選択します。
 - 9. [セッション開始時にログ] や [セッション終了時にログ] など、 [ログ設定] を選択 します。
 - 10. OK をクリックします。
 - 11. 同様に、N4 インターフェイス用のセキュリティポリシーをもう1つ作成します。

- STEP 7 (オプション) ソースに EDL 情報を入力して、機器 ID/加入者 ID/ネットワーク スライス ID、ベースの保護に基づいて別のセキュリティ ポリシー ルールを作成します。
 - 1. [ポリシー > セキュリティを選択し、セキュリティ ポリシー ルールを名前で追加しま す (例: 機器 ID セキュリティ)。
 - 2. [ソース] タブを選択し、ソースゾーンを追加するか、 [任意] を選択します。
 - 3. 次のいずれかの形式で1つ以上のソース機器 ID を追加します。
 - IMEI を含む 5G 永久機器識別子 (PEI)
 - IMSI (15 または 16 桁)
 - Type Allocation Code(TAC、タイプ割り当てコード)の8桁のIMEIプレフィックス
 - IMEI を指定する EDL
 - (オプション) このセキュリティ ポリシー ルールにソース サブスクライバとネットワー ク スライス名を追加して、ルールの制限を強めることができます。
 - 5. [宛先ゾーン]、[宛先アドレス]、および[宛先デバイス]を[任意]として指定します。
 - 6. アプリケーションを追加して、たとえば、ssh、ssl、radmin、telnetを許可します。
 - 7. [アクション] タブで、許可などのアクションを選択します。
 - 8. ウイルス対策、脆弱性対策、スパイウェア対策など、適用するプロファイルを選択します。
 - 9. [セッション開始時にログ] や [セッション終了時にログ] など、 [ログ設定] を選択 します。
 - 10. OK をクリックします。

期待されるテスト結果:

- 監視セクションの GTP-U ログを確認します。
- ログの詳細セクションを確認して、加入者、機器、ネットワークスライス情報を確認します。
- ルールのヒット数が増加していることを確認します。

アプリケーション識別と脅威検査によるインバウンド/アウトバウンド保護

このテストケースでは、CNF クラスタが N6 インターフェイスのインバウンド トラフィックと アウトバウンド トラフィックを検査して保護する能力を評価します。

N6 インターフェイスは、クリア テキスト トラフィックを TCP/UDP 経由でインターネットに伝送します。VM-Series ファイアウォールを N6 インターフェイスに展開することで、アプリケーションの使用状況を完全に可視化できるようになりました。ファイアウォールは、許可されたトラフィックに対する TP、Adv-URL フィルタリング、Wildfire、DNS セキュリティなどの CDSS サブスクリプションによるセキュリティを実装できます。

以下の手順は、このテストケースを実行するための概要です。個々のステップの実行の詳細については、N3+N4 可視性と相関性ポリシーによる 5G セキュリティを参照してください。

- STEP 1| 適切なゾーンとインターフェイスを備えた N6 インターフェイスのセキュリティ ポリシー を作成します。
- STEP 2 デフォルトのセキュリティ プロファイルを使用するか、URL フィルタリング、Widfire、脆弱性保護などのカスタムカテゴリを作成します。
- STEP 3 (オプション) URL カテゴリで許可された URL のカスタム プロファイルを作成します。
- STEP 4| (オプション) さまざまな基準に一致する複数のセキュリティ ポリシーを作成します。セ キュリティポリシーを作成するときに、手順 3 で作成したプロファイルを選択します。
- STEP 5| トラフィックを送信します。
- **STEP 6** 悪意のあるトラフィックをインバウンド/アウトバウンド方向に送信し、トラフィックがブロックされているかどうかを確認します。

期待される結果:

- ポリシーのヒット数が増加します。
- URL フィルタリング、トラフィック、脅威ログの該当するログを確認してください。

サポートされるカスタム メトリックに基づくファイアウォールの スケール アウト

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

このテストは、自動スケーリングで指定されたカスタムメトリック値のターゲットに基づいて、CN-Series HSF クラスタの自動スケーリング機能を検証するのに役立ちます。

- STEP 1 自動スケーリングで指定されたカスタム メトリック ターゲット値に基づいて自動スケーリ ングするために、CN-Series HSF クラスタの作成中に自動スケーリングを有効にします。詳 細については、HSF クラスタをデプロイするを参照してください。
- STEP 2 CloudWatch 名前空間を入力して、メトリクスを AWS CloudWatch にプッシュします。
- STEP 3 EKS クラスタのリージョンを入力します。
- STEP 4| プッシュ間隔を入力します。
- STEP 5| 自動スケーリングメトリックを選択します。この例では、PansessionActive を選択すること をお勧めします。

- STEP 6 スケールインのしきい値とスケールアウトのしきい値を指定します。たとえば、実行中の 2 つの NGFW ポッドがあり、ファイアウォール上のセッションの合計数が現在 1000 である 場合、クラウド ウォッチ メトリックは 500 を示します (NGFW ポッドごと)。
- STEP 7 スケールアウトのしきい値を 250 に設定すると、自動スケールによってさらに 2 つの NGFW ポッドがスピンアップされます。
- STEP 8 セッション情報を取得するには、MGMT ポッドで show session info コマンドを使用します。
- STEP 9| 自動スケーリングできる最大および最小の NGFW ポッドを指定できます。

期待される結果:NGFW ポッドは、スケールアウトのしきい値に基づいて自動スケーリングす る必要があります

テストケース:CN-MGMT 障害処理

どこで使用できますか?	何が必要ですか?
• CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

このテストでは、CN-NGMT 障害処理を評価します。

CN-Series HSF のデプロイメントに必要な CN-MGMT ポッドの最小数は、障害処理を確保する ために 2 つです。デプロイメント後、最初にアクティブになった CN-MGMT ポッドがリーダー になり、2 番目の CN-MGMT ポッドがフォロワーになります。両方の CN-MGMT ポッドの設 定は同じです。どのインスタンスでも、1 つの CN-MGMT ポッドが READY 状態になってい ます。CN-DB、CN-GW、および CN-NGFW ポッドは、Traffic Interconnect (TI) リンクを介して READY 状態の CN-MGMT ポッドに接続します。

2つの CN-MGMT ポッドは、HA アクティブ - パッシブ モードまたは HA アクティブ
 - アクティブ モードではありません。両方のポッドの設定は同じで、Panorama を使用して設定されています。

CN-MGMT ポッドの障害は、次の条件のいずれかが原因で発生します。

- ライブネスチェックが失敗する
 - slotd が ダウンしている場合、
 - ipsec または strongswan がダウンしている場合
- CN-MGMT ポッドがクラッシュして再起動する

STEP 1 Panorama CLI から、show clusters name を入力します <cluster-name>リーダーとフォロ ワーの CN-MGMT ポッドを表示します。

次の出力は、pan-mgmt-sts-1ポッドがアクティブであることを示しています。

- **STEP 2** pan-mgmt-sts-1 ポッドのクラスタ メンバーシップと、Kubernetes コントローラー CLI からの CN-DB、CN-GW、および CN-NGFW ポッドの状態を表示します。
 - kubectl get pods -n kube-system と入力して、すべてのポッドの状態を表示します。

Output:

pan-mgmt-sts-1はアクティブです。すべての CN-DB、CN-GW、および CN-NGFW ポッドは、**pan-mgmt-sts-1**に接続されています。

NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 69m pan-db-dep-6774cd774d-k49cm 1/1 Running 0 69m pan-gw-dep-d849c7df8-4sk54 1/1 Running 0 69m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 69m pan-mgmt-sts-0 0/1 Running 0 83m pan-mgmt-sts-1 1/1 Running 0 83m pan-ngfw-dep-668965d598pmmjd 1/1 Running 0 69m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 69m panngfw-dep-668965d598-s2zcc 1/1 Running 0 69m pan-ngfw-dep-668965d598-vf9l4 1/1 Running 0 69m

2. pan-mgmt-sts-1からクラスタメンバーシップを確認します。

kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash

su - admin

以下のコマンドを使用して、すべての CN-DB、CN-GW、および CN-NGFW ポッドが リーダー CN-MGMT ポッドに接続されているかどうかを確認します。

show cluster-membership show-slot-info slot all

Output:

MP leader status:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State

¹ CN-GW 192.168.23.101 192.168.24.100 UP UP UP 10 CN-DB 192.168.23.104 ::UP UP NA 2 CN-GW 192.168.23.100 192.168.24.98 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-NGFW 192.168.23.89 192.168.24.83 UP UP UP 7 CN-NGFW 192.168.23.105 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.103 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP

3. pan-mgmt-sts-0からクラスタメンバーシップを確認します。

pan-mgmt-sts-0 ポッドにアクセスします。

kubectl -n kube-system exec -it pan-mgmt-sts-0 -- bash

su - admin

次のコマンドを使用して、CN-DB、CN-GW、および CN-NGFW ポッドがフォロワー CN-MGMT ポッドに接続されているかどうかを確認します。

show cluster-membership show-slot-info slot all

Output:

メンバー情報がありません

- STEP 3 | CN-MGMT ポッドの障害処理をテストします。
 - Kubernetes コントローラー CLI から次のコマンドを入力して、リーダーの pan-mgmtsts-1 ポッドを削除します。

kubectl -n kube-system delete pod pan-mgmt-sts-1

2. Panorama CLI から、show clusters name を入力します <cluster-name>新しいリー ダーとフォロワーの CN-MGMT ポッドを表示します。

次の出力は、pan-mgmt-sts-0ポッドが現在アクティブであることを示しています。

- **STEP 4** pan-mgmt-sts-0 ポッドのクラスタ メンバーシップと、Kubernetes コントローラー CLI からの CN-DB、CN-GW、および CN-NGFW ポッドの状態を表示します。
 - kubectl get pods -n kube-system と入力して、すべてのポッドの状態を表示します。

Output:

pan-mgmt-sts-0はアクティブです。すべての CN-DB、CN-GW、および CN-NGFW ポッドは、**pan-mgmt-sts-1**に接続されています。

NAME READY STATUS RESTARTS AGE pan-db-dep-6774cd774d-gjpkr 1/1 Running 0 76m pan-db-dep-6774cd774d-k49cm 1/1 Running 0 76m pan-gw-dep-d849c7df8-4sk54 1/1 Running 0 76m pan-gw-dep-d849c7df8-ct6wk 1/1 Running 0 76m pan-mgmt-sts-0 1/1 Running 0 90m pan-mgmt-sts-1 0/1 Running 0 90m pan-ngfw-dep-668965d598pmmjd 1/1 Running 0 76m pan-ngfw-dep-668965d598-pnthb 1/1 Running 0 76m panngfw-dep-668965d598-s2zcc 1/1 Running 0 76m pan-ngfw-dep-668965d598-vf9l4 1/1 Running 0 76m

2. pan-mgmt-sts-0からクラスタメンバーシップを確認します。

Get in to the **pan-mgmt-sts-0** pod.

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

su - admin

Check if all CN-DB, CN-GW, and CN-NGFW pods are connected to the Leader CN-MGMT pod using the following command.

```
show cluster-membership show-slot-info slot all
```

Output:

3. pan-mgmt-sts-1からクラスタメンバーシップを確認します。

pan-mgmt-sts-1 ポッドにアクセスします。

kubectl -n kube-system exec -it pan-mgmt-sts-1 -- bash

su - admin

次のコマンドを使用して、CN-DB、CN-GW、および CN-NGFW ポッドがフォロワー CN-MGMT ポッドに接続されているかどうかを確認します。

```
show cluster-membership show-slot-info slot all
```

Output:

メンバー情報がありません

テスト結果:リーダー ポッド pan-mgmt-sts-1が失敗すると、フォロワー ポッド pan-mgmtsts-0 が新しいリーダーになります。この CN-MGMT 障害処理メカニズムにより、トラフィッ ク フローが中断されないことが保証されます。既存または新しいセッションへの影響はありま せん。

テストケース:CN-NGFW 障害処理

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

このテストでは、CN-NGFWの障害処理を評価します。

CN-NGFW 障害は、次の状況で発生する可能性があります。

- ノードの問題
- CN-NGFW ポッドがクラッシュして再起動する
- ノードと CN-NGFW ポッドは問題ありませんが、pan_task がクラッシュします
- CN-NGFW は、次の場合にクラスタ メンバーシップから削除されます。
 - Eth0 インターフェイスを介した IPsec モニタリングが失敗する
 - クラスタ相互接続 (CI) リンクが壊れている
 - トラフィック相互接続 (TI) リンクが壊れている

このシナリオでは、クライアントとサーバー間の SSH セッションは CN-NGFW 1 にインストー ルされます。CN-NGFW 1 がダウンした場合、別の CN-NGFW へのフェイルオーバーによって SSH セッションを維持する必要があります。

STEP 1 Panorama CLI から、show clusters name を入力します <cluster-name>CN-MGMT ポッ ドに接続されている CN-NGFW、CN-DB、および CN-GW ポッドを表示します。

Cluster: cluster-002 Creation time:2022/11/22 04:56:46 CN-MGMT pods:87F87FE94CBBB03 (active, pan-mgmt-sts-0.cluster-002, connected, In Sync) Slot-ID PodName Type Version pan-gw-dep-5cd5c87d76-przjx CN-GW 11.0.1-c156.dev e_rel 6 pan-db-dep-d6fb496b-jf2ms CN-DB 11.0.1-c156.dev e_rel 5 pan-ngfw-dep-5cd8f55848-dbhwh CN-NGFW 11.0.1-c156.dev e_rel 8 panngfw-dep-5cd8f55848-slk5l CN-NGFW 11.0.1-c156.dev_e_rel 7 pan-db-dep-d6fb496b-hfmlp CN-DB 11.0.1-c156.dev e_rel 9 pan-ngfw-dep-5cd8f55848-pq6ks CN-NGFW 11.0.1-c156.dev_e_rel 2 pangw-dep-5cd5c87d76-4kbfk CN-GW 11.0.1-c156.dev_e_rel 11 pan-ngfw-dep-5cd8f55848-rsbqn CN-NGFW 11.0.1-c156.dev_e_rel

STEP 2 コマンド show cluster-membership show-slot-info slot all を使用して、CN-MGMT ポッド an-mgmt-sts-0 のクラスタ メンバーシップの詳細を表示します。

MP リーダーのステータス:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State

1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 11 CN-NGFW 192.168.23.87 192.168.24.93 UP UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 7 CN-DB 192.168.23.102 ::UP UP NA 6

CN-DB 192.168.23.104 ::UP UP NA 5 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP

ethernetx/3 サブネットのすべてのインターフェースは、同じゾーンにある必要があります。同 様に、ethernetx/4 サブネットのすべてのインターフェースは同じゾーンにある必要がありま す。

STEP 3 show session all filter application ssh を使用して、すべての SSH セッションを表示します。

セッションごとに、クライアントからサーバーへの方向とサーバーからクライアントへの方 向の2つのフローがあります。

セッション所有者はスロット 11 です。

次のコマンド例を使用して、フィルター処理されたクラスタフローの詳細を表示できます。

show cluster-flow all filter source-port 22

Output:

```
      Slot 5
      Id

      State Type Src[Sport]/Proto Dst[Dport]
      536870940 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]

      Slot 6
      Id

      State Type Src[Sport]/Proto Dst[Dport]
      Id

      671088668 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48702]
      Id
```

show cluster-flow all filter destination-port 22

Output:

```
Slot 5

Id

State Type Src[Sport]/Proto Dst[Dport]

536870939 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]
```

Slot 6 Id State Type Src[Sport]/Proto Dst[Dport] 671088667 ACTIVE FLOW 192.168.200.100[48702]/6 192.168.250.100[22]

STEP 4 | Delete the pod on Slot 11 using the command kubectl -n kube-system delete pod pan-ngfw-dep-5cd8f55848-rsbgn.

Output:

pod "pan-ngfw-dep-5cd8f55848-rsbqn" deleted

The session owned by the CN-NGFW pod in Slot 11 is now marked as orphan.

admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session target dp changed to s6dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow id 536870939 Flow 536870939 start time :Mon Nov 21 21:30:02 2022 timeout :3600 sec source :192.168.200.100 sport :48702 dest :192.168.250.100 dport :22 proto :6 zone :1 type :FLOW state :ACTIVE ipver :4 fidx :28 cid :0 gft :0 gft ':1 predict :0 orphan :1 flag_inager :0 ager_thread :3 flags :0 flow-data : type: l7 appid:25 startlog:I endlog:1 denied:0 admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-mgmtsts-1.cluster-001> show cluster-flow id 671088667 Flow 671088667 start time :Mon Nov 21 21:30:02 2022 timeout :3600 sec source :192.168.200.100 sport :48702 dest :192.168.250.100 dport :22 proto :6 zone :1 type :FLOW state :ACTIVE ipver :4 fidx :28 cid :0 gft :1 gft' :0 predict :0 orphan :1 flag_inager :0 ager_thread :4 flags :0 flow-data : type: l7 app-id:25 startlog:1 endlog:1 denied:0

STEP 5 Access the SSH session using the command show session all filter application ssh.

ファイアウォールは、孤立したフローを処理するために、使用可能な CN-NGFW ポッドに フェイルオーバーします。新しいセッション オーナーはスロット 7 です。

ID Application State Type Flag Src[Sport]/Zone/Proto (translated IP[Port]) Vsys Dst[Dport]/Zone (translated IP[Port]) 805306374 ssh ACTIVE FLOW 192.168.200.100[48702]/untrust_ei1/6 (192.168.200.100[48702]) vsys1 192.168.250.100[22]/trust_ei2 (192.168.250.100[22]) admin@pan-mgmt-sts-1.cluster-001> show session id 805306374 Session 805306374 c2s flow: source:192.168.200.100 [untrust_ei1] dst:192.168.250.100 proto:6 sport:48702 dport:22 state:ACTIVE type:FLOW src user: unknown dst user: unknown s2c flow: source:192.168.250.100 [trust_ei2] dst:192.168.200.100 proto:6 sport:22 dport:48702 state:ACTIVE type:FLOW src user: unknown dst user: unknown Slot :7 DP :0 index(local): :6 start time :Mon Nov 21 21:43:27 2022 timeout :3600 sec time to live :3581 sec total byte count(c2s) :1350 total byte count(s2c) :1506 layer7 packet count(c2s) :17 layer7 packet count(s2c) :11 vsys : vsys1 application : ssh rule :Promoted-session service timeout override(index) :False session to be logged at end :True session in session ager:True session updated by HA peer :False layer7 processing : completed URL filtering enabled :True URL category : any session via syn-cookies :False session terminated on host :False session traverses tunnel :False session terminate tunnel :False captive portal session :False ingress interface : ethernet1/3 egress interface : ethernet1/4 session QoS rule :N/A (class 4) tracker stage l7proc : fastpath state none end-reason : unknown

クラスタフローに変更はありません。

admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s5dp0 Session target dp changed to s5dp0 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow id 536870939 Flow 536870939 start time :Mon Nov 21 21:30:02 2022 timeout :3600 sec source :192.168.200.100 sport :48702 dest :192.168.250.100 dport :22 proto :6 zone :1 type :FLOW state :ACTIVE ipver :4 fidx :12 cid :7 gft :0 gft' :1 predict :0 orphan :0 flag_inager :0 ager_thread :3 flags :0 flow-data : type: l7 appid:25 startlog:1 endlog:1 denied:0 admin@pan-mgmt-sts-1.cluster-001> set system setting target-dp s6dp0 Session target dp changed to s6dp0 admin@pan-mgmtsts-1.cluster-001> show session id 805306374 Session 805306374 Bad Key: c2s: 'c2s' Bad Key: s2c: 's2c' index(local): :6 admin@pan-mgmt-sts-1.cluster-001> show cluster-flow id 671088667 Flow 671088667 start time :Mon Nov 21 21:30:02 2022 timeout :3600 sec source :192.168.200.100 sport :48702 dest :192.168.250.100 dport :22 proto :6 zone :1 type :FLOW state :ACTIVE ipver :4 fidx :12 cid :7 gft :1 gft' :0 predict :0 orphan :0 flag_inager :0 ager_thread :4 flags :0 flow-data : type: l7 app-id:25 startlog:1 endlog:1 denied:0

Results:

既存または新しいセッションへの影響はありません。Panorama で更新されたクラスタ メンバーシップ。

テストケース:CN-DBの障害処理

どこで使用できますか?	何が必要ですか?
 CNシリーズHSFファイアウォールのデプ	 CN-Series 11.0.x or above Container Images PanoramaPAN-OS 11.0.x以降のバージョン
ロイメント	を実行している

このテストでは、CN-DB の障害処理を評価します。CN シリーズの HSF デプロイメントで推奨 される CN-DB ポッドの数は 2 です。両方の CN-DB の設定は同じです。

CN-DB1が長時間停止すると、CN-DB2が既存のセッションを処理し、新しいセッションを セットアップします。CN-DB1が再び稼働すると、既存のセッションのセッション同期、ルック アップ、ティアダウンをチェックし、新しいセッションをセットアップします。

STEP 1 コマンド show cluster-membership show-slot-info slot all を使用して、CN-MGMT ポッドのクラスタ メンバーシップの詳細を表示します。

MP リーダーのステータス:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State

1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-DB 192.168.23.104 ::UP UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP

- STEP 2 | スロット 6 の CN-DB ポッドを削除します。
 - 1. Panorama CLI からコマンド show clusters name cluster-001 を使用して、ス ロット 6 の CN-DB ポッド名を取得します。

 コントローラーの CLI からコマンド kubectl delete pod pan-dbdep-7b6f6c5458-4tvpq -n kube-system を入力して、スロット6の CN-DB ポッドを削除します。

スロット6のCN-DBポッドが削除されました。

3. コマンド show cluster-flow allを使用してクラスタ トラフィック フローを確認 します。

CN-DB ポッドを含むスロット 6 は現在 PREPARE 状態であり、CI リンクはダウンしています。

MP リーダーのステータス:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State

192.168.23.100 192.168.24.80 UP IMPACTED UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP IMPACTED UP 2 CN-GW 192.168.23.101 192.168.24.100 UP IMPACTED UP 5 CN-DB 192.168.23.102 ::UP IMPACTED NA 6 CN-DB 192.168.23.104 ::PREPARE DOWN NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP IMPACTED UP 8 CN-NGFW 192.168.23.105 192.168.24.81 UP IMPACTED UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP IMPACTED UP

STEP 3 CN-DB ポッドが再びアクティブになるまで、show cluster-membership show-slotinfo slot all と入力します。

MP リーダーのステータス:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State

1 CN-GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-DB 192.168.23.104 ::PROBE UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP

STEP 4 コマンド show cluster-flow all を使用して、クラスタ トラフィック フローを再度確認します。

Slot 5 Src[Sport]/Proto Dst[Dport] 536870953 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 536870958 ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 536870954 ACTIVE FLOW 192.168.100.6[49153]/17 192.168.100.100[3784] 536870955 ACTIVE FLOW 192.168.100.100[3784]/17 192.168.100.6[49153] 536870952 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 536870951 ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 536870960 OPENING FLOW fe80:0:0:20c:29ff:fe85:3442[133]/58 ff02:0:0:0:0:0:2[0] 536870957

ACTIVE FLOW 192.168.101.101[3784]/17 192.168.101.6[49155] 536870959 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48706] 536870950 ACTIVE FLOW 192.168.100.6[49154]/17 192.168.100.101[3784] 536870956 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784] ------ Slot 6 Id State Type Src[Sport]/Proto Dst[Dport] 671088642 ACTIVE FLOW 192.168.101.100[3784]/17 192.168.101.6[49156] 671088641 ACTIVE FLOW 192.168.200.100[48706]/6 192.168.250.100[22] 671088643 ACTIVE FLOW 192.168.100.6[49153]/17 192.168.100.100[3784] 671088645 ACTIVE FLOW 192.168.100.100[3784]/17 192.168.100.6[49153] 671088644 ACTIVE FLOW 192.168.101.6[49156]/17 192.168.101.100[3784] 671088646 ACTIVE FLOW 192.168.100.101[3784]/17 192.168.100.6[49154] 671088647 ACTIVE FLOW fe80:0:0:0:20f;fe85:342[13]/58 ff02:0:0:0:0:0:0:2[0] 671088648 ACTIVE FLOW 192.168.101.101[3784]/17 192.168.101.6[49155] 671088649 ACTIVE FLOW 192.168.250.100[22]/6 192.168.200.100[48706] 671088650 ACTIVE FLOW 192.168.100.6[49154]/17 192.168.100.101[3784] 671088651 ACTIVE FLOW 192.168.101.6[49155]/17 192.168.101.101[3784] show cluster-flow all filter count yes

----- Slot 5 ----- Number of sessions that match filter:11 ---------- Slot 6 ----- Number of sessions that match filter:11

show cluster-membership show-slot-info slot all

MP リーダーのステータス:Leader Slot-id Type CI-IP TI-IP State CI-State TI-State

GW 192.168.23.100 192.168.24.80 UP UP UP 10 CN-NGFW 192.168.23.81 192.168.24.82 UP UP UP 2 CN-GW 192.168.23.101 192.168.24.100 UP UP UP 5 CN-DB 192.168.23.102 ::UP UP NA 6 CN-DB 192.168.23.104 ::UP UP NA 7 CN-NGFW 192.168.23.103 192.168.24.86 UP UP UP 8 CN-NGFW 192.168.23.105 192.168.24.84 UP UP UP 9 CN-NGFW 192.168.23.82 192.168.24.81 UP UP UP

From Panorama CLI

show clusters name cluster-001

Cluster: cluster-001 Creation time:2022/11/22 05:11:09 CN-MGMT pods:8FF0233D36BD57D (active, pan-mgmt-sts-1.cluster-001, connected, In Sync) 8F846238B0740D2 (pan-mgmt-sts-0.cluster-001, connected, In Sync) Slot-ID PodName Type Version

dep-7b6f6c5458-5fgnr CN-DB 11.0.1-c156.dev e_rel 1 pan-gw-dep-748cdb856d-4f66g CN-GW 11.0.1-c156.dev e_rel 2 pan-gw-dep-748cdb856d-p5qdd CN-GW 11.0.1-c156.dev_e_rel 7 pan-ngfw-dep-56cdfdd656-srmdt CN-NGFW 11.0.1-c156.dev_e_rel 8 pan-ngfw-dep-56cdfdd656-hvcw2 CN-NGFW 11.0.1-c156.dev_e_rel 9 pan-ngfw-dep-56cdfdd656-

bjtmd CN-NGFW 11.0.1-c156.dev_e_rel 10 pan-ngfw-dep-56cdfdd656-6jq2f CN-NGFW 11.0.1-c156.dev_e_rel 6 pan-dbdep-7b6f6c5458-r449b CN-DB 11.0.1-c156.dev_e_rel

CN-DB の変更は、監視 > ログ > システムの下のPanorama Web インターフェイスで表示できます。

🚺 PANORAMA	DASHBOAR	D ACC	MONITOR	C Device Groups POLICIES OBJ	ECTS NETV	r Templates ¬ VORK DEVICE PANORAMA		
Panorama 🗸	Device Group	All		~				
🖌 📑 Logs	Q (subtype eq cl	ustering)						
Traffic	GENERATE TIME	ТҮРЕ	SEVERITY	EVENT	OBJECT	DESCRIPTION	DEVICE SN	DEVICE NAME
🐯 Threat	11/21 21:58:53	clustering	informational	cl-agent-node-state- change	cluster-001	Slot 6 moving to JOINED state	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
WildFire Submissions	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
HIP Match	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
😢 GlobalProtect	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
User-ID Decryption	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
GTP	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
System	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Authentication Unified	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
External Logs	11/21 21:58:53	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Threat	11/21 21:58:40	clustering	informational	cl-agent-node-state- change	cluster-001	Slot 6 moving to PROBE state	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Le System	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Config	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Automated Correlation Engine	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Correlation Objects	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
App Scope Summary	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Change Monitor	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
Threat Map	11/21 21:58:40	clustering	informational	fwcd-sync-flow	cluster-001	Slot 6 came up. Firewall clustering flows will be synchronized from slot 5 to slot 6	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
😢 Network Monitor 😤 Traffic Map	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
PDF Reports	11/21 21:58:40	clustering	informational	fwcd-config-modify	cluster-001	Firewall clustering configuration was modified	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001
User Activity Report	11/21 21:58:40	clustering	informational	fwcd-ci-ka-up	cluster-001	Keepalive is up from slot 2 to slot 6	8FF0233D36BD5	pan-mgmt-sts- 1.cluster-001

結果:

既存または新しいセッションへの影響はありません。Panorama で更新されたクラスタ メンバーシップ。

CN-Series でサポートされていない機能

PAN-OSでサポートされている次の機能は、以下で特に明記されていない限り、CN-Series では使用できません。

機能	DaemonSet	K8s サービス	CNF モード	HSF モード
認証	いいえ	いいえ	いいえ	いいえ
Cortex Data Lake へのログ	いいえ	いいえ	いいえ	いいえ
Enterprise DLP	いいえ	いいえ	いいえ	いいえ
Non-vWire インターフェー ス	いいえ	なし	あり	あり。
IoTセキュリティ	いいえ	いいえ	いいえ	いいえ
IPv6	あり。	なし	あり	いいえ
NAT	いいえ	なし	あり	いいえ
ポリシー ベース フォワー ディング	いいえ	なし	あり	いいえ
QoS	いいえ	いいえ	いいえ	いいえ
SD-WAN	いいえ	いいえ	いいえ	いいえ
User-ID	いいえ	いいえ	いいえ	いいえ
WildFire インライン ML	いいえ	いいえ	いいえ	いいえ
SaaS インライン	いいえ	いいえ	いいえ	いいえ
IPSec	いいえ	いいえ	いいえ	いいえ
Tunnel Content Inspection(トンネル コン テンツ検査)	いいえ	いいえ	いいえ	なし