

vRealize Network Insight の FAQ

VMware vRealize Network Insight 5.1

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2020 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

- 1 vRealize Network Insight FAQ ガイドの概要 4
- 2 全般 5
- 3 インストールおよび構成 8
- 4 vRealize Network Insight でのデータ ソースの追加または設定 14
- 5 マイクロセグメンテーションおよびフロー 17
- 6 クラスタリング 19
 - クラスタリング - 全般 19
 - クラスタリング - インストールと構成 21
 - クラスタリング - スケーリング 22
 - クラスタリング - 展開 24
- 7 データの管理と処理 26
- 8 IPFIX 28

vRealize Network Insight FAQ ガイ ドの概要

1

vRealize Network Insight の FAQ ガイドでは、vRealize Network Insight についてよく寄せられる質問を提供しています。

対象者

この情報は、vRealize Network Insight を使用するユーザーを対象としています。

サポート バンドルの発行方法

『vRealize Network Insight コマンドライン リファレンス ガイド』のサポート バンドルについてのセクションを参照してください。

XML API アクセス用に Palo Alto Networks Panorama の読み取り専用管理者ロールを作成する方法

XML API アクセス用の [管理者] ロールを追加するには以下の手順を実行します。

- 1 [Panorama][→][管理者ロール] を選択します。
- 2 [追加] をクリックし、管理者ロールを新規追加すると [管理者ロール プロファイル] ダイアログ ボックスが開きます。
- 3 [管理者ロール プロファイル] ダイアログボックスで次の操作を実行します。
 - a ロールに名前を指定します (例: api-only-admin)。
 - b [ロール]を[Panorama]として選択します。
 - c [Web UI] タブですべてのエントリを無効にします。
 - d [XML API] タブで [コミット] を除くすべてのエントリを有効にします。
 - e [OK] をクリックしてダイアログ ボックスを閉じると、新しい [管理者ロール] が名前のリストに表示されます。
 - f [コミット] をクリックして、変更を Panorama にコミットします。
- 4 この [管理者] ロールを管理アカウントに割り当てます。

サービスが共有されたと見なされるタイミング

次のポートは共有として構成されています。

プロトコル	ポート
DNS	53
Bootpc	68
Kerberos	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
Syslog	514
送信	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269

「証明書やキーなどのデータソース ID 情報が変更されました」というイベント/エラーがデータ ソースに表示されている場合の対処法

vRealize Network Insight が、製品に保存されている証明書とは異なる新しい証明書をデータ ソースから受信しています。vRealize Network Insight は、データ ソースによって提示された証明書を自動で受け入れます。このプロセスでは、古い証明書と新しい証明書をダウンロード可能なデータ ソース上のイベントを取得します。

vRealize Network Insight への DNS レコードのインポートの上限

DNS レコードのインポートの上限は次のとおりです。

- Infobox DNS データ ソース : 1 つのデータソースから 90 万レコードをインポートできます。

- DNS レコードの手動インポート:複数の .csv または zip ファイルとしてパッケージされたバインド ファイルを使用して DNS レコードをインポートできます。インポートできるレコードの数に制限はありませんが、アップロードには次の制限があります。
 - 1 つの zip ファイル内のファイル数 – 25
 - 1 つの zip ファイルの最大サイズ – 10 MB

インストールおよび構成

3

vRealize Network Insight のリソース要件について

リソース要件については、『vRealize Network Insight インストール ガイド』を参照してください。

vRealize Network Insight プロキシ OVA の展開中に正しくないキーを入力した場合

vRealize Network Insight プロキシ OVA の展開中は、シークレット キーが検証されません。展開は正しくないシークレット キーを使用しても完了します。ただし、ペアリングは失敗する可能性があります。vRealize Network Insight プロキシは vRealize Network Insight ユーザー インターフェイスで検出されたとおりに表示されません。

共有シークレットを修正するには、vRealize Network Insight プロキシ CLI にログインし、set-proxy-shared-secret コマンドを実行して、正しいシークレット キーを設定します。このコマンドは、古いキーを新しいキーに置き換えるため、vRealize Network Insight プラットフォームは vRealize Network Insight プロキシを検出してペアリングを実行します。

vRealize Network Insight プロキシ OVA の展開後の DNS 構成方法

vRealize Network Insight プロキシ CLI にログインし、change-network-settings コマンドを実行します。このインタラクティブ コマンドを使用すると、ユーザーに DNS を追加または変更するオプションが提供され、その後、vRealize Network Insight プロキシが新しい DNS で再構成されます。

ネットワーク パラメータのいずれかが正しく構成されていない場合は、change-network-settings コマンドを使用してネットワーク構成パラメータを変更します。

ユーザー インターフェイスから vRealize Network Insight プロキシ仮想マシンの IP アドレスを確認する方法

[設定] ページに移動し、vRealize Network Insight の [インフラストラクチャ] メニュー オプションを選択します。vRealize Network Insight プラットフォームと vRealize Network Insight プロキシ仮想マシンの両方の IP アドレスが表示されます。

vRealize Network Insight プロキシ OVA の展開後、vRealize Network Insight プロキシが 5 分以内に検出されない場合

vRealize Network Insight プロキシに `consoleuser` を使用してログインし（vRealize Network Insight コマンドライン インターフェイス ガイドを参照）、以下を確認します。

- CLI `show-connectivity-status` を使用して、vRealize Network Insight プラットフォームの vRealize Network Insight プロキシとのペアリング ステータスを確認します。
- ペアリング状態が `Passed` と表示されている場合は、新しいブラウザ ウィンドウでプラットフォームのユーザー インターフェイスを開き、ログインしてステータスを確認します。
- ペアリング状態が `Failed` と表示されている場合は、vRealize Network Insight プロキシ OVA 展開時に指定した共有シークレット キーが正しくない可能性があります。この問題を解決するには、`set-proxy-shared-secret` コマンドを使用して正しいシークレット キーを設定します。このコマンドは、古いキーを新しいキーに置き換えるため、vRealize Network Insight プラットフォームは vRealize Network Insight プロキシを検出することができます。
- `show-connectivity-status` で vRealize Network Insight プラットフォームへのネットワーク アクセスが [失敗] と表示されている場合は、`ping` コマンドを使用して vRealize Network Insight プロキシ仮想マシンから vRealize Network Insight プラットフォームにアクセスできるかどうかを確認します。
- アクセスできない場合は、`show-config` コマンドを使用して NTP、DNS、ゲートウェイなどのネットワークパラメータが正しく構成されているかどうかを確認します。
- ネットワーク パラメータのいずれかが正しく構成されていない場合は、`setup` コマンドを使用してネットワーク構成パラメータを変更します。

ログイン認証情報を忘れた場合

ユーザー インターフェイスのローカル ユーザーの場合：vRealize Network Insight ユーザー インターフェイス管理者に連絡して、認証情報をリセットしてください。

管理者の場合：vRealize Network Insight 3.4 以降の場合は、CLI `modify-password` を使用してユーザー インターフェイスの認証情報を変更できます。詳細については、CLI ガイドを参照してください。バージョン 3.4 より前の vRealize Network Insight を使用している場合は、サポートにお問い合わせください。

ログイン パスワードの変更方法

ログイン パスワードを変更するには、次の手順を実行します。

- 1 [管理者] > [設定] の順に移動し、左側のペインで [マイ プロファイル] をクリックします。
- 2 [パスワードの変更] ページで必要な情報を入力し、[保存] をクリックします。

vRealize Network Insight プロキシ仮想マシンの検出前にログイン画面が表示された場合

- この動作は、ブラウザを更新したとき、またはプロキシの検出前に URL を新しいウィンドウで開く場合に発生することがあります。
- `admin@local` ユーザー名にライセンス アクティベーション時に設定された認証情報を使用してログインします。

vRealize Network Insight による複数の vCenter Server/NSX Manager のサポート

vRealize Network Insight は、複数の vCenter Server/NSX Manager をサポートします。

インターネットアクセスが必要な vRealize Network Insight のサービスとその理由

vRealize Network Insight は、インターネット アクセスを必要とするリモート ホームの呼び出し機能をサポートします。vRealize Network Insight チームはこれらの機能またはサービスを使用することで、お客様の環境を詳細に把握し、問題のプロアクティブなトラブルシューティングまたは修復を可能にします。次のサービスにはインターネット アクセスが必要です。

- 自動更新サービス (`svc.ni.vmware.com:443`) : vRealize Network Insight はこのサービスを使用してリモートのアップグレード ホストにアクセスし、新しくリリースされたビットが使用可能になるとこれを取得し、アップデートが利用可能になるとユーザーにユーザー インターフェイス通知を表示します。このサービスはデフォルトで有効になっていますが、ユーザー インターフェイスを使用するか、または CLI で `online-upgrade` コマンドを使用して、このサービスを無効にできます。
- パフォーマンス テレメトリ サービス (`svc.ni.vmware.com:443`) : vRealize Network Insight の主要なサービスとパフォーマンスに関連する特定のメトリックが vRealize Network Insight に対して定期的に収集およびアップロードされます。サポート チームがこれらのメトリックを監視し、環境内の異常を把握することで、重要なサービスに影響する前にサポートチームが行動できるようにします。このサービスはデフォルトで無効になっていますが、CLI で `telemetry` コマンドを使用してこのサービスの有効/無効を切り替えることができます。詳細については、<https://kb.vmware.com/s/article/59242> を参照してください。
- サポート サービス (`support2.ni.vmware.com:443`) : このサービスは、認証された担当者がリモート アクセスして展開に使用できる、vRealize Network Insight サポート ホストへのリモートでセキュリティ保護されたトンネルを確立します。デフォルトでは無効になっており、ユーザー インターフェイスと「support-tunnel」CLI の両方を使用して有効/無効を切り替えることができます。

- 登録サービス (`reg.ni.vmware.com:443`) : アプライアンスをすべての外部サービスに登録するために使用します。上記のサービス間で信頼された通信を有効にします。セットアップでインターネットにアクセスすると、登録は自動的に行われます。隔離された環境では、「offline-registration」CLI を使用して実行できます（詳細については、CLI ガイドを参照してください）。これは、サポート トンネルを有効にするために必要です。

注： vRealize Network Insight プラットフォームがインターネットプロキシの背後にある場合は、次のドメイン名とポートをホワイトリストに登録します。

表 3-1.

サービス	URL	ポート
アップグレード サービス / メトリック サービス	<code>svc.ni.vmware.com</code>	443
サポート トンネル サービス	<code>support2.ni.vmware.com</code>	443
登録サービス	<code>reg.ni.vmware.com</code>	443

アプライアンスからのインターネット アクセスを無効にする方法

次のサービスは、セキュアなリモート/インターネット サービスを使用します。

- 自動更新サービス
- パフォーマンス テレメトリ サービス
- サポート サービス
- 登録サービス

これらのサービスを有効または無効にする方法については、[インターネットアクセスが必要な vRealize Network Insight のサービスとその理由](#)の FAQ を参照してください。これらのサービスのいずれかが有効になっている場合、vRealize Network Insight にはインターネットへのアクセスが必要です。

ポート集約について、そのメカニズム

ポート集約は、動的 FTP、Oracle、MS-RPC などの短期ポートフローを集約するために組み込まれています。これにより、システム内のフローの数を削減し、同じサービスで根幹である多数のフローを集約して表示できます。

実行のメカニズムは次のとおりです。

- `destination_ip` 通知の最初の 3 日間は、特定の IP アドレスの 10K のバケットで宛先ポートを集約し、その IP アドレスのポートプロファイルの作成を開始します（ターゲット IP アドレスごとにポートプロファイルを構築）。
- 3 日間が経過したら、プロファイルの作成後、ポートの密度が高くなっている（短期ポートを開くパターンが反映されている）ポート範囲の集約を開始します。範囲自体は、100、1,000、10,000 などサイズが動的になります。開いているポートの数と、指定した集約の範囲内での使用量に応じて作成されます。

注： この決定は、サーバの各 IP アドレスに対して個別に実行されます。

- これにより、大量のポートを開いているアクティビティがない場合には集約を行わずに高ポートフローを報告し、アクティビティが発生した場合には動的な集約を適用することが可能になります。
- このプロファイルは、新たに開放されたポートや、使用されなくなった古いポートを考慮して、時系列で常に更新されます。

vRealize Network Insight OVA の展開後に IP アドレス、ゲートウェイ、ネットマスクを変更する場合

vRealize Network Insight プラットフォーム/プロキシのネットワーク設定を変更するには、CLI にログインして `change-network-settings` コマンドを実行します。このインタラクティブ コマンドでは、vRealize Network Insight アプライアンスを新しい詳細を使用して再構成した後に、ユーザーに IP アドレス、ゲートウェイ、ネットマスクなどを変更するオプションが提供されます。

注：

- このタスクは、アプライアンスが最後に再起動した際に、仮想マシン コンソール セッションを使用して実行する必要があります。
- vRNI プラットフォームの IP アドレスが変更され、プロキシとペアになっている場合は、各プロキシ仮想マシンで次の CLI コマンドを実行します。

```
vrni-proxy set-platform --ip-or-fqdn <New_Platform_IP>
```

評価版ライセンスから無期限ライセンスに変更する方法

『vRealize Network Insight ユーザー ガイド』の「ライセンスの追加と変更」セクションを参照してください。

vRealize Network Insight のライセンスの特徴

表 3-2.

ライセンス名	ライセンス タイプ	機能
Enterprise	Full/Production : 無期限または期限付きのいずれかにできます。	次の機能が有効になります。 <ul style="list-style-type: none"> ■ データ プロバイダとして AWS ■ 調整可能なデータ保持ポリシー ■ Infoblox DNS データ ソース ■ 物理 IP アドレスおよび DNS マッピング ■ 分析
Advanced	Full/Production : 無期限または期限付きのいずれかにできます。	なし

注： すべてのライセンスは、CPU ソケットと CCU（同時実行ユーザー）ごとに付与されます。評価版ライセンスは、[UI] > [設定] > [バージョン情報] を介して更新されたキーを使用して更新または [本番] ライセンスに変換できます。詳細については、ユーザー ガイドを参照してください。

vRealize Network Insight の仮想マシンのバックアップを作成する方法

VMware VADP/VDP API などの仮想マシンのバックアップを作成するには、「VMware ベスト プラクティス」を参照してください。クラスタを作成または拡張する前に、バックアップを作成することをお勧めします。

vRealize Network Insight でのデータソースの追加または設定

4

IP アドレスを使用して vCenter Server を追加しているときに「要求がタイムアウトになりました」というメッセージが表示された場合の対処方法

- vRealize Network Insight プロキシ仮想マシンから vCenter Server の IP アドレスにアクセスできることを確認します。
- vRealize Network Insight プロキシ CLI にログインし、ping を送信して IP アドレスがアクセス可能であることを確認し、telnet を使用してポート 443 で vCenter Server にアクセス可能であることを確認します。
- vCenter Server にアクセスできる場合は、追加を再試行します。
- IP アドレスにアクセスできない場合は、コマンド `show-config` を使用して vRealize Network Insight プロキシ仮想マシンからゲートウェイが正しく構成されているかどうかを確認します。
- ゲートウェイが正しくない場合は、`setup` コマンドを使用して修正します。

vCenter Server の追加中に「IP アドレス/FQDN が無効です」というメッセージが表示された場合の対処方法

- vCenter Server に指定された IP アドレス/FQDN が正しいかどうかを確認します。
- `ping` コマンドを使用して vRealize Network Insight プロキシ仮想マシンから FQDN にアクセスできるかどうかを確認します。
- アクセスできない場合は、`nslookup FQDN` および `show-config` コマンドを使用して vRealize Network Insight プロキシ仮想マシンで DNS が正しく構成されていることを確認します。
- DNS が正しくない場合は、`setup` コマンドを使用して修正します。

vRealize Network Insight セキュリティと運用プラットフォームに必要な権限

vRealize Network Insight では、次の権限を持つ VMware vCenter Server の認証情報が必要となります。

- Distributed Switch : 変更

- dvPort グループ : 変更

vCenter Server のデータ ソース ページで IPFIX を有効にしている際に「ユーザーには必要な権限がありません」というエラーが表示される場合の対処方法

vRealize Network Insight では、IPFIX を有効にするために、次の権限を持つ VMware vCenter Server の認証情報が必要となります。

- Distributed Switch : 変更
- dvPort グループ : 変更

指定した VMware vCenter Server ユーザーに、vCenter Server のルート フォルダとそのすべての子エンティティ（すべてのフォルダや、すべてのデータセンターなど）に対する権限があることを確認してください。

環境からデータを取得する間隔

vRealize Network Insight プロキシは、環境から 10 分ごとにデータを取得します。

vCenter Server を追加した後、データ分析を開始するタイミング

データの分析は、vCenter Server を追加した後すぐに開始します。製品のユーザー インターフェイスでは、数分で一部のデータが表示され、完了までに 2 時間かかることがあります。

注： フロー トラフィック データは常に変化し、分析には 24 時間以上のデータが含まれます。

vRealize Network Insight OVA を削除した場合の vCenter Server の IPFIX 設定をクリーンアップ方法

- VMware vSphere Web Client を使用している場合：[ホーム] > [ネットワーク] > [VDS (VDS 名)] > [Netflow] 設定の順に移動します。コレクタ設定から vRealize Network Insight プロキシ IP アドレスを削除します。
- VMware vSphere Windows クライアントを使用している場合：[ホーム] > [インベントリ] > [ネットワーク] > [VDS (VDS 名)] > [編集] 設定の順に移動します。[Netflow] タブのコレクタ設定から vRealize Network Insight プロキシ IP アドレスを削除します。この手順は、IPFIX が有効になっている VDS でそれぞれ実行する必要があります。

vRealize Network Insight での IPFIX 設定のクリーンアップ方法

vRealize Network Insight ユーザー インターフェイスで、[設定] > [データ ソース] の順に移動し、vCenter Server を削除します。これにより、vRealize Network Insight によって実行される IPFIX の構成が削除されます。

VMware NSX Manager を vRealize Network Insight に追加した後、仮想マシン間のパスに正しいファイアウォール ルールが表示されるまでに必要な時間はどれくらいですか。

VMware NSX Manager を vRealize Network Insight に追加すると、仮想マシンとファイアウォール ルールの関係の計算が完了するまで最大 24 時間かかる可能性があります。

vRealize Network Insight に VMware vCenter を追加した後、仮想マシン間パスに PNIC が表示されないのはなぜですか。

通常、vRealize Network Insight に VMware vCenter をデータ ソースとして追加すると、vRealize Network Insight が仮想マシン間パスを計算するために約 2 時間かかります。ただし、まれに、VMware vCenter を vRealize Network Insight に追加した後に、仮想マシン間パスに PNIC が正しく表示されるまでに約 8~10 時間かかることがあります。

マイクロセグメンテーションおよびフロー

5

トラフィック分布ピンの数の意味

この割合は、フロー分析に基づくトラフィック分布の概要を示します。

表 5-1.

トラフィック	説明
East-West (EW)	グループ合計のトラフィックに対する East-West のトラフィック
スイッチング (EW の割合)	East-West トラフィックに対するスイッチングされたトラフィックの割合 (%)
ルーティング (EW の割合)	East-West トラフィックに対するルーティングされたトラフィックの割合 (%)
ホスト内 (仮想マシン間の割合)	仮想マシン間のトラフィックに対する、同じホスト上の送信元と宛先のトラフィック
仮想マシン間 (EW の割合)	East-West トラフィックに対する仮想マシン間のトラフィックの割合 (%)
インターネット	グループ合計のトラフィックに対するインターネットのトラフィック

ポートのフロー内での集約方法

ポート集約は、動的 FTP、Oracle、MS-RPC などの短期ポート フローを集約するために組み込まれています。これにより、システム内のフローの数を削減し、同じサービスで根幹である多数のフローを集約して表示できます。これを実行するメカニズムは次のとおりです。

- 最初の 3 日間で、宛先 IP アドレスを認識し、この IP アドレス上の宛先ポートを 1 万件単位のバケットに集約して、この IP アドレスのポートプロファイルの作成を開始します。
- 3 日間が経過すると、高い確度で利用できるプロファイルが作成されます。これにより、ポートの密度が高い（短期ポートを開くパターンを反映する）ポート範囲を集約します。範囲そのものは動的であり、サイズの単位は 100、1,000、10,000 となります。これは、開いたポート数と指定された集約範囲に分布に応じて、作成されます。
- これにより、ポートの一括開放アクティビティが発生していない場合でも、集約を行わずにフロー数の多いポートを報告できます。また、このようなアクティビティの発生時に動的な集約を適用することもできます。

- このプロファイルは、新たに開放されたポートや、使用されなくなった古いポートを考慮して、時系列で常に更新されます。

240.240.240.240 IP アドレスは vRealize Network Insight で何を示していますか。

240.240.240.240 は、vRealize Network Insight のブレースホルダ IP アドレスです。この IP アドレスは、特定の IP アドレスを含む、多数の IP アドレスがある場合に使用されます (5,000 件超)。このブレースホルダ IP アドレス 240.240.240.240 で受信するその他のすべてのインターネット IP アドレス (5001 番目以降) は、このサービス エンド ポイントに置き換えることができます。

これは、各インターネット クライアントを個別に記録する公開サービスでは、非常に多くのフローが発生し、システムの負荷が大きくなる可能性があるため、システム内のフローの数を制限することを目的としています。

このブレースホルダ IP アドレスで置き換えられたすべてのフローにおいては、すべてのメトリックはこの IP アドレスを使用するそれぞれのフローで集計されるため、集計レベルで統計情報が失われることはありません。

フロー ビューで報告されるフローのすべての宛先 IP アドレスは、240.240.240.240 からの送信元が、実際には多数のインターネット IP アドレス (5,000 件超) でヒットしていることが示されています。

クラスタリング

6

この章には、次のトピックが含まれています。

- クラスタリング - 全般
- クラスタリング - インストールと構成
- クラスタリング - スケーリング
- クラスタリング - 展開

クラスタリング - 全般

プロキシまたはコレクタ仮想マシンをクラスタリングできますか。

いいえ。コレクタ/プロキシ仮想マシンのクラスタリングはサポートされていません。

vRealize Network Insight では、vRealize Log Insight のようなロード バランサが必要ですか。

vRealize Network Insight クラスタリングは、スケール アウト ソリューションであり、高可用性ソリューションではありません。プライマリ プラットフォームの仮想マシン/マスター ノードで障害が発生すると、サービス全体が使用できなくなります。

リモート プロキシおよびプラットフォーム間の接続が停止した場合の動作

プラットフォームとプロキシ仮想マシン間の接続が停止した場合、プロキシ仮想マシンは、ディスク容量に応じてデータをローカルに保存します。そして、再接続するたびに送信されます。

vRealize Network Insight は vRealize Log Insight に統合されていますか。

はい。vRealize Log Insight は vRealize Network Insight 3.4 に統合されています。アラートは、Syslog に送信され、これが vRealize Log Insight となることがあります。

ノードが再起動した場合の動作

ノードが再起動すると、そのクラスタに自動的に参加し、処理は続行されます。プライマリ ノードの場合、停止している間はサービスは完全に失われます。

クラスタ内の任意のプラットフォーム ノードまたはコレクタの IP アドレスを変更する方法

クラスタでは、CLI コマンドを使用して、任意のコレクタまたはプラットフォーム ノードの IP アドレスを変更できます。

注：

- この操作を行う前に、VMware サポートにお問い合わせください。
- アプライアンスはプロセスの終了時に再起動されます。したがって、仮想マシンのコンソールで次の手順を実行する必要があります。

- コレクタの IP アドレスを変更するには、`change-network-settings` コマンドを実行します。
- プラットフォームの IP アドレスを変更するには、次の手順を実行します。
 - a `change-network-settings` コマンドを実行します。
 - b 他のすべてのプラットフォームで `update-IP-change` コマンドを実行して、新しい IP アドレスを反映させます。
 - c コレクタで `show-connectivity-status` コマンドを実行し、**Platform VM IP/URL** を検索して、このプラットフォームに関連付けられているかどうかを確認します。
 - d `vrni-proxy` を実行して、関連するコレクタに新しいプラットフォームの IP アドレスを反映させます。

ユース ケース 1: 3 ノード クラスタで、Platform2 の IP アドレスのみが変更されています。関連付けられているコレクタはありません。

- 1 Platform2 で `change-network-settings` を実行します。
- 2 Platform1 および Platform3 で `update-IP-change` を実行して、Platform2 の新しい IP アドレスを反映させます。

ユース ケース 2: 3 ノード クラスタで、Platform1 および Platform2 の IP アドレスが変更されています。CollectorA は Platform2 に、残りは Platform3 に関連付けられています。

- 1 Platform1 で `change-network-settings` を実行します。
- 2 Platform2 で `change-network-settings` を実行します。
- 3 Platform2 と Platform3 で `update-IP-change platform1-oldIP platform1-newIP` を実行します。
- 4 Platform1 と Platform3 で `update-IP-change platform2-oldIP platform2-newIP` を実行します。
- 5 CollectorA で `vrni-proxy set-platform --ip-or-fqdn platform2-newIP` を実行します。

Platform1 で必要なディスク容量

Platform1 では、一部の構成データが Platform1 のみに保存されるため、クラスタ内の他のノードに比べてより多くのディスク容量が必要となります。

いずれかのノードでディスク容量が不足した場合の動作

特定のプラットフォーム ノードのディスク容量が一定のしきい値に達すると、ユーザー インターフェイスにエラーメッセージが表示されます。vCenter Server にログインして、プラットフォーム ノードにディスク容量を追加してください。

クラスタ内でデータがレプリケートされる回数

データのレプリケーション メカニズムは、プラットフォーム ノードに配置されるコンポーネントによって異なります。

クラスタリング - インストールと構成

プラットフォーム仮想マシンはすべて、同じ L2/L3 セグメントに配置する必要がありますか。

いいえ。ただし、ノード間の遅延を縮小して、すべてのプラットフォーム ノードを共通のネットワーク上に配置することをお勧めします。これは、分散した多数のコンポーネントがノード間でデータをレプリケートすると、遅延が拡大することによってシステムのパフォーマンスや安定性の問題が発生することがあるためです。

製品内のアップグレード機能を使用してクラスタをアップグレードできますか。

オンライン アップグレードは、バージョンが 3.7 以前のクラスタではサポートされていません。3.8 以降のリリースでは、オンライン アップグレード方法を使用してクラスタをアップグレードできます。

クラスタの作成プロセスで障害が発生した場合の対処方法

クラスタの作成プロセスを開始する前に、プライマリ プラットフォームとプロキシのスナップショットを作成することをお勧めします。障害が発生した場合は、セカンダリ プラットフォーム ノードを削除し、スナップショットからプライマリ プラットフォームとプロキシ仮想マシンをリカバリします。

単一ノードの環境をクラスタに展開した場合の、既存のデータと構成への影響

すべてのデータと構成は変更なく保持されます。データは、クラスタの作成後にアクセスできます。

異なるリージョンでプラットフォーム仮想マシンを使用できますか。

いいえ。プラットフォーム ノードは同一のサイトに配置する必要があります。プロキシ サーバは、別のサイトに分散することができます。

vSAN ストレッチ クラスタ (2 つのデータセンター) でプラットフォームをホストすることはできますか。

はい。同じデータセンター内または複数のデータセンターにまたがって vSAN クラスタは、ローカル ストレージのように一定の I/O パフォーマンスを確保します。

クラスタ ノードを異なる vSAN クラスタにホストできますか。

はい。プラットフォーム クラスタの異なるノードを、別の基盤となるデータストアでホストすることができます。

プラットフォーム ノードをバックアップする必要はありますか。

はい。VMware が推奨するスナップショット/バックアップ テクノロジーを使用してバックアップを作成する必要があります。

あるリージョンのクラスタ プロキシ仮想マシンと別のリージョンにあるプラットフォーム仮想マシン クラスタ間の帯域幅を予測する方法

一部の大規模環境では、1 Mbps から 20 Mbps までの数が表示されていました。データがプラットフォーム仮想マシンに送信される前に、プロキシ仮想マシンには多くの重複排除または圧縮が発生します。

クラスタ ノード間のネットワーク トラフィック量

通常、トラフィックは、クラスタのサイズおよびデータセンター環境のタイプによって異なります。

3 ～ 5 万台の仮想マシンを持つインストールの場合：

- クラスタ間：約 50 ～ 400 Mbps
- プロキシとプラットフォーム間：約 100 Kbps ～ 15 Mbps

クラスタ内のノード間で許容される最大の遅延

プラットフォーム ノードは、同じサイト内に共存している必要があります。このような場合、遅延は最小になります。プラットフォーム ノードが vSAN ストレッチ クラスタ（2 つのデータセンター）でホストされている場合、クラスタ内またはクラスタ全体の vSAN クラスタによって、ローカル ストレージなどの一定の I/O パフォーマンスが確保されます。vRealize Network Insight など、データセンターで実行されているアプリケーションは正常に動作します。異なる基盤のデータストアにある、プラットフォーム クラスタの異なるノードをホストできます。ただし、クラスタ内のすべてのプラットフォーム仮想マシンが同じサイト内に共存していることを確認する必要があります。

リージョンのプロキシ仮想マシンと別のリージョンにあるプラットフォーム仮想マシンの間で許容される最大の遅延

設定には、別の場所に分散したプロキシを含めることができます。プロキシ仮想マシンからプラットフォーム仮想マシンへの HTTPS 接続が存在するため、約数秒ほどの長い遅延に対応できます。vRealize Network Insight はクラスタ内で最大 10 個のノード（フローありの仮想マシンは 3 万台、またはフローなしの仮想マシンは 5 万台）をサポートします。

プロキシ/プラットフォーム仮想マシンのサイズ

大規模なブリック構成の使用：インストール ガイドを参照してください。

クラスタリング - スケーリング

すでに作成されたクラスタを拡張できますか。

はい。クラスタの拡張では、最大 10 個のノードがサポートされます。

プライマリ以外のプラットフォーム仮想マシンが使用できなくなった場合の動作

内部サービスでは、プライマリ以外のノードの障害に対する回復性が制限されています。通常、ノード障害が発生すると、NI はコンピューティング能力を失います。

サポートされるロード バランシングの種類

プラットフォームへのプロキシのマッピングは固定です。任意のプロキシ仮想マシンからのデータがプラットフォーム仮想マシンに送信されると、その処理はすべてのプラットフォーム仮想マシンにまたがって内部でロード バランシングされます。

プラットフォーム クラスタを作成すると、帯域幅の使用量は増加しますか。

プロキシまたはコレクタ仮想マシンは、プライマリ仮想マシンまたはプラットフォーム仮想マシンに対してのみ通信を継続します。プラットフォーム仮想マシンのクラスタリング通信の帯域幅要件は最小限に抑えられます。したがって、帯域幅の使用量が大幅に増加することはありません。

プロキシ仮想マシンからプラットフォーム仮想マシンへデータが転送される頻度

プロキシ仮想マシンは、重複排除または圧縮データを継続的にプラットフォーム仮想マシンに送信します。

データの最適化は、プロキシ仮想マシンで実行されますか。

プロキシ仮想マシンでは、重複排除、圧縮、削減、またはバッチ処理のさまざまな手順が実行されます。プラットフォーム仮想マシンとプロキシ仮想マシン間の接続が切断されると、プロキシ仮想マシンは、ディスク容量に応じてデータをローカルに保存し、接続がリストアされるたびに送信します。

ネットワーク帯域幅の最適化は行われていますか。

はい。プロキシ仮想マシンでは、重複排除、圧縮、削減、バッチ処理のさまざまな手順が実行されます。

プロキシ サーバでクラスタリングを行うことはできますか。

いいえ。プロキシ サーバではクラスタリングを行うことはできません。

vCenter Server からプロキシ サーバへのトラフィックの送信方法

vCenter Server では、プロキシ サーバにトラフィックを送信しません。プロキシ サーバは、指定された vCenter Server に実際に接続して情報を取得します。

クラスタを展開する場合に vCenter Server から各種プロキシ サーバにトラフィックを送信する方法

実際には、プロキシが vCenter Server に接続され、情報を取得します。それぞれのプロキシは、指定された vCenter Server に接続して情報を取得します。プロキシでクラスタリングはできません。

クラスタリング - 展開

クラスタのスケール アウト後のユーザー インターフェイスへのアクセス方法

ユーザー インターフェイスへのアクセスは、Platform1 からのみに制限されます。

Platform1 の概要とこのノードの特性

クラスタの作成プロセスが開始される、プラットフォーム ノードは、[Platform1] として扱われます。ユーザー インターフェイスにアクセスできるのは、クラスタ内のノードのうち、このノードのみです。

ユーザー インターフェイスのアクセスが Platform1 に制限されている場合に、クラスタ内の他のノードからデータを取得する方法

データセンターのデータは、クラスタ内のすべてのノードにまたがって配置されます。また、ユーザー インターフェイス レイヤーが Platform1 のデータを要求すると、Platform1 ノードはすべてのノードに保存されているデータを取得し、ユーザー インターフェイスに応答を送信します。

異なるデータセンターに展開されているプラットフォーム ノードを使用してクラスタを作成する場合の注意点

クラスタ内のすべてのノード間で、データは送受信されます。したがって、遅延の問題を回避するため、同じデータセンターに展開されたプラットフォーム ノードを使用してクラスタを作成することをお勧めします。

プラットフォーム ノードをスケール アウトした場合の、既存のプラットフォームのデータ

既存のプラットフォーム ノードのデータは保持され、クラスタ内のすべてのノードに配置されます。

必要なプラットフォーム ブリックの数を決定する際に、プロキシ仮想マシンの数を考慮する必要がありますか。

いいえ。必要なブリックの数を決定する際に影響するのは、すべての vCenter Server にまたがる仮想マシン数の合計とフローのステータス（有効または無効）のみです。『vRealize Network Insight インストール ガイド』のブリック モデルの表を参照してください。

vCenter Server の数や、ルーターなどの物理デバイス数、その他のタイプのデータ ソースなどは、必要なプラットフォーム ブリックの数に影響しますか。

いいえ。必要なブリックの数を決定する際に影響するのは、すべての vCenter Server にまたがる仮想マシン数の合計とフローのステータス（有効または無効）のみです。『vRealize Network Insight インストール ガイド』のブリック モデルの表を参照してください。

vRNI では、HA を目的として 2 つのデータセンターにまたがる、分散したプラットフォーム クラスタをサポートしますか。

いいえ。プラットフォーム クラスタは、データセンターをまたがる分散をサポートしません。すべてのプラットフォーム クラスタ仮想マシンは、同じサイトに配置する必要があります。プラットフォーム クラスタは現在 HA をサポートしていません。今後対応する予定です。ディザスタ リカバリに対応する HA を目的として、2 つのサイトにまたがって SRM を使用することができます。

vRNI では、6,000 台を超える仮想マシンが配置され、フローが有効になっている単一の vCenter Server をサポートしますか。

バージョン 3.5 までの場合、vRNI プロキシでは、単一の大規模な vCenter Server で 6,000 台を超える仮想マシンを配置し、フローが有効である場合、データの収集をサポートしていません。今後対応する予定です。

Platform1 で必要なディスク容量

Platform1 では、一部の構成データが Platform1 のみに保存されるため、クラスタ内の他のノードに比べてより多くのディスク容量が必要となります。

いずれかのノードでディスク容量が不足した場合の動作

特定のプラットフォーム ノードのディスク容量が一定のしきい値に達すると、ユーザー インターフェイスにエラーメッセージが表示されます。vCenter Server にログインして、プラットフォーム ノードにディスク容量を追加してください。

クラスタ内でデータがレプリケートされる回数

データのレプリケーション メカニズムは、プラットフォーム ノードに配置されるコンポーネントによって異なります。

クラスタの動作方法

- 展開内のすべてのプロキシは、1 つのプラットフォーム (Platform1) に接続します。プラットフォームとプロキシ間の接続は、ポート 443 で https を介して行われます。そのため、Platform1 からのプロキシにはポート 443 のみが表示されます。
- Platform1 ノードは、プロキシからの要求を受信すると、ラウンド ロビン方式でクラスタ内の他のプラットフォーム ノードへ要求を分散します。
- プラットフォーム ノードは、データを正規化し、計算エンジンで処理するためにメッセージング キューに格納します。
- 計算エンジンは、データ レプリケーション メカニズムを使用して、クラスタ内のすべてのノードにデータを分散します。この方法では、クラスタ内のいずれかのノードが停止しても、データが失われることはありません (Platform1 を除く)。
- 一部の構成データは、レプリケートされていない Platform1 ノードに明示的に格納されます。これが、高可用性 (HA) ソリューションがサポートされていない理由です。

データの管理と処理

7

プラットフォームおよびプロキシ サーバ間の通信が切断したなどの境界条件における、データ処理パイプラインの動作

■ デフォルトの保持期間

30 日間です。エンタープライズ ライセンスの場合、ユーザー インターフェイスから延長することができます。
注：延長する場合は、ディスクのガイドラインに沿っていることを確認してください。

■ プロキシでのデータの処理方法

フロー データを含む、のデータをプラットフォームに送信する前に、プロキシ上のすべてのデータは SDM（自己記述メッセージ）に変換されます。すべてのデータ ソースからの構成、インベントリ、およびメトリック データがすべて含まれます。プラットフォームにアクセスできない場合、または Kafka キューへの SDM アップロードが失敗した場合、プロキシ仮想マシンのディスクに書き込まれます (/var/BLOB_STORE)。

■ プロキシでデータのパージを開始するタイミング

フロー以外のデータの場合：ディスク (BLOB_STORE) では、SDM を保存するための容量が 10 GB 割り当てられています。このストアがいっぱいになると、コレクタは古い SDM を削除し、新しい SDM をディスクに追加します。この制限に到達するペースは、すべてのデータ ソースから収集されるデータのサイズによって異なります。

フロー データの場合：/var/flows/vds/nfcapd では、raw フローを保存するための容量が 15 GB 割り当てられています。この容量が使用されると、フロー プロセッサは、古いフロー ファイルの削除を開始します。受信側の raw フローの速度（最大 2 M/分）では、ローテーションが開始するまでに 10 時間程度かかります。

■ パージ ロジックの概要

最も古い SDM が最初に削除されます。

■ 新しいデータがプロキシでの処理を停止するタイミング

サービスが適切に実行されている間は処理を停止することはありません。

■ プラットフォームとプロキシ間の接続が切断し、パージする条件を満たしていない場合、すべてのデータは再接続時にプラットフォーム上で照合されますか。

ディスクに保存されているすべてのデータがプラットフォームに送信されます。プラットフォーム上でデータが損失する条件が存在する場合をのぞき、データは完全に照合されます（詳細は以下を参照）。

■ プラットフォーム上でデータの損失が発生する条件

Kafka キューに入った SDM が 6 時間を超えると、プラットフォームは、SDM をドロップします（3 ノード クラスタの場合は 18 時間）。キューが飽和状態になっている場合でも発生します。システムに遅延が発生し、受信データ レートが高い場合に、この問題が発生する可能性があります。

■ SDM が送信される順序

最も古い SDM が最初に送信されます。バージョン 3.9 までは、既知の問題が 1 つあります。これにより、データの損失が発生する可能性があります。詳細については、VMware サポートにお問い合わせください。

■ 通信に問題がない場合、データはプロキシのディスクに保存され、プラットフォームにプッシュされますか。

通信の問題がない場合、SDM はディスクに保存されません。メモリ自体からプラットフォームに送信されます。SDM の送信中に問題が発生したことをプロキシが受信すると、ディスクにのみ保存されます。

■ 問題が発生した場合、プロキシが最後に処理されたフロー ファイルを把握する方法

フロー プロセッサは、最後に処理された nfcapd ファイルのブックマークをデータベースに保持します。

■ 問題が発生せずに処理できる SDM の最大サイズユーザーはこの制限についてどのように把握しますか。

SDM サイズには 15 MB の制限があります。バージョン 3.9 以降では、プラットフォームが大量に SDM をドロップするたびにイベントが発生します。

IPFIX の概要

IPFIX は、フロー情報をエクスポートするための IETF プロトコルです。フローは、特定のタイムスロットで転送されるパケットのセットとして定義され、5 組の値（送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、プロトコル）を共有します。フロー情報には、タイムスタンプ、パケット/バイト数、入力/出力インターフェイス、TCP フラグ、VXLAN ID、カプセル化されたフロー情報などのプロパティが含まれます。これは Netflow と呼ばれることがよくあります。ただし、IPFIX は標準の IETF プロトコルです。

どのフロー情報が VDS によってエクスポートされますか。

vSphere 環境の Distributed Switch は、IPFIX を使用してフロー情報をエクスポートするように設定できます。VDS に接続されているすべてのポート グループでフロー モニタリングを有効にします。パケットが Distributed Switch のポート X に到着し、ポート Y から送信されると、ポート Y でフロー監視が有効な場合は対応するフロー レコードが生成されます。各フロー レコードの方向は「Egress」と設定されます。

vRealize Network Insight での IPFIX の使用方法

vRealize Network Insight では、VMware VDS IPFIX を使用してネットワーク トラフィック データを収集します。すべてのセッションには 2 つのパスがあります。例：Session A ↔ C では、A→C 方向のパケットと C→A 方向のパケットがあります。セッションの完全な情報を分析するには、両方向のパケットに関する IPFIX データが必要です。次の図では、仮想マシン-A が DVPG-A との接続を介して 仮想マシン-C と通信しています。DVPG-A が提供するのは C→A パケットに関するデータのみで、DVPG-Uplink は A→C パケットに関するデータを提供します。A のトラフィックの完全な情報を取得するには、IPFIX を DVPG-A と DVPG-Uplink で有効にする必要があります。

vRealize Network Insight フロー収集のトラブルシューティング

- 1 特定の VDS およびその DVPG およびアップリンク プロパティに Netflow 監視が [有効] になっており、コレクタ IP アドレスが vRealize Network Insight コレクタのものであることを確認してください。

- 2 IPFIX Netflow パケットは、ファイアウォール（NSX、仮想、または物理）の間でドロップします。ESXi ホストと vRealize Network Insight コレクタ間のルートに存在する可能性のあるファイアウォールによって vRealize Network Insight コレクタ IP アドレス上の UDP ポート 2055 宛ての Netflow パケットが許可されていることを確認してください。
- 3 ESXi ホストは、IPFIX Netflow パケットの送信を停止します。UDP ポート 2055 にアクセスできない場合、ESXi ホストは、Netflow パケットの送信をしばらくすると停止します。これは、ファイアウォールがパケットをドロップしたことが原因で発生する可能性があります。
- 4 ネットワークのルーティングでの問題が原因、ESXi ホストが vRealize Network Insight コレクタにアクセスできません。ESXi ホストと vRealize Network Insight コレクタ間に適切なルートが存在することを確認してください。

IPFIX に関連する VMware ナレッジベースの記事

VMware ESXi 6.0 Update 1 の場合 :

[2135956](#)