

vRealize Network Insight のインストールアップグレー ド

VMware vRealize Network Insight 5.2

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

vRealize Network Insight インストール ガイドの概要	5
1 インストールの準備	6
システムの推奨事項と要件	6
権限	9
システム ポート	10
ネットワーク通信ポート	15
サポート対象の製品とバージョン	17
2 vRealize Network Insight のインストール	21
インストール ワークフロー	21
vRealize Network Insight プラットフォーム OVA の展開	23
vSphere Web Client を使用した導入	23
vSphere Windows ネイティブ クライアントを使用した展開	25
ライセンスを有効にする	26
共有シークレットの生成	27
Network Insight Collector の設定 (OVA)	27
vSphere Web Client を使用した導入	27
vSphere Windows ネイティブ クライアントを使用した展開	29
AWS での Network Insight Collector (AMI) の VMware SD-WAN 用の設定	30
既存の設定への追加コレクタの展開	32
3 評価ライセンスを使用した vRealize Network Insight へのアクセス	33
vCenter Server を追加	33
トラフィック フローの分析	34
レポートの生成	35
4 展開のスケールアップ計画	36
プラットフォーム クラスタのスケールアップ計画	36
コレクタのスケールアップ計画	37
設定のブリック サイズの増加	38
5 vRealize Network Insight のアップグレード	40
オンライン アップグレード	41
シングルクリックでのオフライン アップグレード	43
CLI によるアップグレード	46
6 vRealize Network Insight のアンインストール	48

vCenter Server で Netflow が有効な場合に Collector の IP アドレスを削除	49
NSX で Netflow が有効な場合に Collector の IP アドレスを削除	49

vRealize Network Insight インストール ガイド の概要

『vRealize Network Insight インストールガイド』は、vRealize Network Insight のインストールを担当する管理者またはスペシャリストを対象としています。

対象者

この情報は、vRealize Network Insight のインストールを担当する管理者またはスペシャリストを対象としています。記載されている情報は、仮想マシンの管理者としての経験があり、エンタープライズ管理アプリケーションおよびデータセンターの運用に詳しい方を対象としています。

インストールの準備

1

vRealize Network Insight のインストール前に、展開環境がシステム要件を満たすように準備します。

この章には、次のトピックが含まれています。

- システムの推奨事項と要件
- サポート対象の製品とバージョン

システムの推奨事項と要件

展開のパフォーマンスを最適化するには、展開の最小推奨事項に適合する必要があります。

プラットフォーム展開の推奨事項

表 1-1. プラットフォーム ブリック サイズの仕様

ブリック サイズ	必要なコア数 (2.1 GHz CPU)	必要なコア数 (2.3 GHz CPU)	必要なコア数 (2.6 GHz CPU)	RAM	ディスク
中	10	9	8	32 GB	1 TB
大	15	14	12	48 GB	1 TB
特大	20	18	16	64 GB	2 TB

注：

- 各ノードの CPU 速度と RAM の予約は、上記に指定した値の 100% である必要があります。
- セットアップをすべての仕様に一致させるには、リソース（RAM、ディスク、CPU）の追加が必要になることがあります。<https://kb.vmware.com/s/article/53550> および設定のブリック サイズの増加を参照してください。

表 1-2. クラスタ以外の展開 - 最大容量

ブリック サイズ	仮想マシン数 (1,000 台単位)	1 日あたりのフロー (100 万個単位)	合計フロー (100 万個単位)	フロー プラン (100 万個単位)
中	4,000	100 万	400 万	200 万
大	6,000	200 万	800 万	400 万

表 1-3. クラスタ以外の展開 - VMware SD-WAN の最大容量

ブリック サイズ	Edge の数 (1,000 台単位)	1日あたりのフロー (100 万個単位)	合計フロー (100 万個単位)
中	2,000	100 万	400 万
大	2,000	200 万	800 万

注：

- 仮想マシンの数には、vCenter Server 上のテンプレートも含まれます。
- 合計フローは、システムが保持期間中に保存できるフローの最大数です。
- フロー プランは、システムがセキュリティ計画を実行できるフローの合計です。

表 1-4. クラスタの展開 - 最大容量

ブリック サイズ	クラスタのサイズ	仮想マシン数 (1,000 台単位)	1日あたりのフロー (100 万個単位)	合計フロー (100 万個単位)	フロー プラン (100 万個単位)	VMware SD-WAN の Edge 数 (1,000 台単位)
大	3	1 万	200 万	800 万	400 万	4,000
特大	3	1.8 万	600 万	2,400 万	400 万	6,000
特大	5	3 万	1,000 万	4,000 万	400 万	1 万
特大	10	10 万	1,500 万	5,500 万	400 万	1 万

注：

- 仮想マシンの数には、vCenter Server 上のテンプレートも含まれます。
- クラスタのサイズは、クラスタ内のノードの合計数です。
- 合計フローは、保持期間に対するシステム内のフローの数です。
- 合計フローを決定するクエリは `count of flows in last 31 days` で、保持期間を 31 日間と仮定しています。
- フロー プランは、システムがセキュリティ計画を実行できるフローの合計です。

コレクタ展開の推奨事項

表 1-5. コレクタ ブリック サイズの仕様

ブリック サイズ	2.1 GHz CPU に必 要なコア数	2.3 GHz CPU に必 要なコア数	2.6 GHz CPU に必 要なコア数	RAM	ディスク
中	5	5	4	12 GB	200 GB
大	10	9	8	16 GB	200 GB
特大	10	9	8	24 GB	200 GB

注： 各ノードの CPU 速度と RAM の予約は、上記に指定した値の 100% である必要があります。

表 1-6. コレクタの展開 - 最大容量

コレクタ サイズ	仮想マシン数 (1,000 台単位)	1 日あたりのフロー (100 万個単位)	4 日間のフロー数 (100 万個単位)	VMware SD-WAN の Edge 数 (1,000 台単位)
中	4,000	250 万	325 万	4,000
大	1 万	500 万	650 万	6,000
特大	20,000	1,000 万	1,300 万	1 万

注：

- 仮想マシンの数には、vCenter Server 上のテンプレートも含まれます。
- 単一の展開内に複数のコレクタが含まれている場合は、プラットフォームのキャパシティに基づいてコレクタ全体の合計フローが制限されます。

その他の要件と考慮事項

- プラットフォーム ノード間の最大時間スキューは、30 秒未満である必要があります。
- NTP サービスの可用性は、システム操作にとって重要です。NTP サービスが使用できない場合は、プラットフォーム ノードまたはコレクタ ノードを再起動しないようにしてください。
- 既存のコンピューティング リソースがプラットフォーム上の他のプロセスによって完全に使用されている場合、vRealize Network Insight はクラッシュし、自動でリカバリしません。サービスがリカバリに失敗した場合は、プラットフォーム ノードを再起動します。
- プラットフォーム ノードとアップグレード サーバ間のネットワーク遅延が 500 ミリ秒より大きい場合、vRealize Network Insight のアップグレードでエラーが発生することがあります。そのため、ネットワーク遅延は 500 ミリ秒未満にする必要があります。
- 最適なパフォーマンスのために推奨されるディスク遅延は、5 ミリ秒以内です。ディスク遅延が 5 ミリ秒を超えると、システムのパフォーマンスが低下します。
- 推奨されるディスク IOPS は 7,500 です。

サポート対象 Web ブラウザ

- Google Chrome : 最新の 2 つのバージョン。
- Mozilla Firefox : 最新の 2 つのバージョン。

高可用性をサポートするための推奨事項

vSphere HA オプションをカスタマイズして、vSphere の高可用性を有効にすることができます。

- [ホスト失敗] -仮想マシンの再起動
- [ホスト隔離]-無効
- [ハートビートのないゲスト]-無効

権限

データソースに必要な権限

- IPFIX の構成と使用に必要な権限
 - 権限付きの vCenter Server 認証情報 :
 - Distributed Switch : 変更
 - dvPort グループ : 変更
 - vCenter Server の事前定義ロールには、root レベルで割り当てられた、子ロールに伝達が必要な次の権限が必要です。
 - System.Anonymous
 - System.Read
 - System.View
 - global.settings

vCenter Server でのロールの詳細については、『vSphere セキュリティ ガイド』の「ロールを使用した権限の割り当て」セクションを参照してください。

- NSX Manager データプロバイダに必要な権限
 - NSX Manager データ プロバイダには、[Enterprise] ロールが必要です。
 - セントラル CLI が有効になっている場合、NSX Manager データプロバイダには system admin の認証情報が必要です。

- メトリック収集のために Cisco スイッチで必要になるユーザー権限
 - vRealize Network Insight は、SNMP と同様に Cisco スイッチから SSH を介してメトリック データを収集することができます。Cisco スイッチの UCS プラットフォームでは、収集に SSH と API の両方を使用する必要があります。

表 1-7.

データのタイプ	ユーザー権限
構成データ	読み取り専用
メトリック データ	SNMP 読み取り専用
	SNMPv2 読み取り専用 SNMP コミュニティ
	SNMPv3 読み取り専用

システム ポート

vRealize Network Insight の受信通信に必要なポートのリストを次に示します。

プラットフォーム クラスタ設定のポート

表 1-8.

ソース	ターゲット	ポート	プロトコル	目的	センシティブ	SSL	認証
SSH クライアント	プラットフォーム	22	SSH	CLI またはホストのアクセス	なし	はい	ユーザー名 / パスワードまたは SSH キーベースの認証
クライアント Web ブラウザ および vRNI コレクタ	プラットフォーム	443	HTTPS	ユーザー インターフェイス /API アクセスおよび vRNI コレクタとの通信	はい	はい	2048 ビット RSA キーベースの SHA2 証明書（またはユーザーが構成したカスタム証明書）を使用して暗号化された SSL チャネル。このチャネルのコレクタからプラットフォームへのメッセージも、HMAC を使用して暗号化されます。

表 1-8. (続き)

ソース	ターゲット	ポート	プロトコル	目的	センシティブ	SSL	認証
プラットフォーム	プラットフォーム	2181	HTTP	他のノードにある ZooKeeper サーバ間の通信 (クラスタの場合)。メタデータ情報 (znode データ) が格納されます。	なし	なし	
プラットフォーム	プラットフォーム	2888	HTTP	ZooKeeper リーダーへの接続に使用	なし	なし	
プラットフォーム	プラットフォーム	3000	HTTP	E メール通知に使用	はい	なし	
プラットフォーム	プラットフォーム	3888	HTTP	ZooKeeper リーダーの選出に使用	はい	なし	
プラットフォーム	プラットフォーム	5432	JDBC	仮想マシン構成データとインフラストラクチャ メタデータの格納	はい	なし	
プラットフォーム	プラットフォーム	8020	TCP/RPC	他の名前ノードとデータ ノード間の通信	はい	なし	
プラットフォーム	プラットフォーム	8025	HTTP	ノード マネージャがこのポートを使用してリソース マネージャに接続	なし	なし	
プラットフォーム	プラットフォーム	8030	HTTP	リソース マネージャがタスクのスケジュール設定に使用	なし	なし	
プラットフォーム	プラットフォーム	8032	HTTP	RM のアプリケーション マネージャ インターフェイスのアドレス	なし	なし	
プラットフォーム	プラットフォーム	8033	HTTP	RM 管理インターフェイスのアドレス	なし	なし	

表 1-8. (続き)

ソース	ターゲット	ポート	プロトコル	目的	センシティブ	SSL	認証
プラットフォーム	プラットフォーム	8042	HTTP	ノード マネージャ Web アプリケーションのアドレス	なし	なし	
プラットフォーム	プラットフォーム	8080	HTTP	ユーザー インターフェイスの要求	はい	なし	
プラットフォーム	プラットフォーム	8088	HTTP	リソース マネージャ Web アプリケーションの HTTP アドレス	なし	なし	
プラットフォーム	プラットフォーム	8480	TCP/RPC	JournalNode HTTP サーバ	なし	なし	
プラットフォーム	プラットフォーム	8485	TCP/RPC	HDFS 共有編集データ ディレクトリ	なし	なし	
プラットフォーム	プラットフォーム	9090	HTTP	コレクタからの要求と、コレクタへのコマンド送信に使用	はい	はい (nginx 経由で保護)	
プラットフォーム	プラットフォーム	9092	TCP 経由のバイナリ	他のブローカーが通信しているポート	はい	なし	
プラットフォーム	プラットフォーム	9200-9300	HTTP	検索要求に使用します。ES はポートの範囲を使用して待機します。9200 が使用されている場合は、使用可能な次のポートを使用します。	はい	なし	
プラットフォーム	プラットフォーム	9300	HTTP	検索要求に使用します。ES はポートの範囲を使用して待機します。9200 が使用されている場合は、使用可能な次のポートを使用します。	はい	なし	

表 1-8. (続き)

ソース	ターゲット	ポート	プロトコル	目的	センシティブ	SSL	認証
プラットフォーム	プラットフォーム	30000:65535	TCP	他のプロセスと TCP 接続を行うために、さまざまなプロセスによって使用される短期ポート範囲	なし	なし	
プラットフォーム	プラットフォーム	60000	IPC	他の HBase プライマリおよびリージョン サーバ間の通信に使用	はい	なし	
プラットフォーム	プラットフォーム	60010	HTTP	HBase Web ユーザー インターフェイスに使用	なし	なし	
プラットフォーム	プラットフォーム	60020	IPC	HBase プライマリとリージョン サーバ間の通信	はい	なし	
プラットフォーム	プラットフォーム	4500-4510	TCP	異なるプラットフォームで実行されている Foundation DB サーバ間の通信	はい	なし	

シングル プラットフォーム設定のポート

表 1-9.

ソース	ターゲット	ポート	プロトコル	目的	センシティブ	SSL	認証
SSH クライアント	プラットフォーム	22	SSH	CLI またはホストのアクセス	なし	はい	ユーザー名 / パスワードまたは SSH キーベースの認証
クライアント Web ブラウザ および vRNI コレクタ	プラットフォーム	443	HTTPS	ユーザー インターフェイス /API アクセスおよび vRNI コレクタとの通信	はい	はい	2048 ビット RSA キーベースの SHA2 証明書（またはユーザーが構成したカスタム証明書）を使用して暗号化された SSL チャネル。このチャネルのコレクタからプラットフォームへのメッセージも、HMAC を使用して暗号化されます。

コレクタ サーバのポート

表 1-10.

ソース	ターゲット	ポート	プロトコル	目的	センシティブ	SSL	認証
SSH クライアント	コレクタ	22	SSH	CLI またはホストのアクセス	なし	はい	ユーザー名 / パスワードまたは SSH キーベースの認証
vRNI コレクタ	プラットフォーム	443	HTTPS	プラットフォームを使用するプライマリ通信チャネル	はい	はい	2048 ビット RSA キーベースの SHA2 証明書（またはユーザーが構成したカスタム証明書）を使用して暗号化された SSL チャネル。このチャネルのコレクタからプラットフォームへのメッセージも、HMAC を使用して暗号化されます。

表 1-10. (続き)

ソース	ターゲット	ポート	プロトコル	目的	センシティブ	SSL	認証
フロー転送	コレクタ	UDP 2055	NetFlow/ IPFIX	ターゲットからのフローをこのポートにプッシュ	はい	なし	
フロー転送	コレクタ	UDP 6343	sFlow	ターゲットからのフローをこのポートにプッシュ	はい	なし	
ESXi ホスト	コレクタ	1991	TCP	仮想インフラストラクチャの遅延測定値 (vNIC と物理 NIC 間の遅延、VTEP 間の遅延、TEP 間の遅延など) の収集。	なし	なし	
Dell OS10	コレクタ	50000	GRPC	Dell OS10 デバイスからのバッファ統計情報テレメトリ情報の受信	なし	なし	

ネットワーク通信ポート

次の表に、vRealize Network Insight のネットワーク通信で使用されるポートとプロトコルを示します。

ポート リストは、<https://ports.vmware.com/home/vRealize-Network-Insight> で参照することもできます。

表 1-11.

目的	接続元	接続先	ポート	プロトコル
vRealize Network Insight の仮想マシン間の通信	コレクタ	プラットフォーム <small>注： このポートはすべてのプラットフォームで有効にする必要があります。</small>	443	HTTPS
インターネット アクセスが必要なサービス	プラットフォームとコレクタ	svc.ni.vmware.com support2.ni.vmware.com reg.ni.vmware.com	443	HTTPS
構成されているその他のサービスへの通信	プラットフォーム	LDAP サーバ	389、636	LDAP および LDAPS
		SNMP サーバ	構成可能	SNMP
	プラットフォームとコレクタ	DNS サーバ	53	UDP

表 1-11. (続き)

目的	接続元	接続先	ポート	プロトコル
		Syslog サーバ	構成可能	
	ESXi ホスト	コレクタ	2055	
	ESXi ホスト	コレクタ	1991	TCP
データソースとして AWS と通信	コレクタ	AWS (* .amazonaws.com)	443	HTTPS
テレメトリ サービスとの 通信	ブラウザ	テレメトリ URL : https:// vcsa.vmware.com	433	HTTPS
データセンター内の他の データ ソースとの通信	コレクタ	Arista スイッチ	161 および 22	SNMP および SSH
		Azure	443	HTTPS
		Brocade スイッチ	161 および 22	SNMP および SSH
		Check Point ファイアウ ォール	443	HTTPS
		Cisco Nexus	161 および 22	SNMP および SSH
		Cisco UCS (統合コンピ ューティング システム)	161、22、および 443	SNMP、SSH、および HTTPS
		Cisco Catalyst スイッチ	161 および 22	SNMP および SSH
		Cisco ACI スイッチ	161	SNMP
		Cisco APIC コントロー ラ	161 および 443	HTTPS および SNMP
		Dell スイッチ	161 および 22	SNMP および SSH
		Dell OS10	50000	TCP
		VeloCloud	443、2055	HTTPS
		HP	22	SSH
		Juniper スイッチ	161 および 22	SNMP および SSH
		Palo Alto Networks	443	HTTPS
		VMware vSphere	443	HTTPS
		VMware NSX-V (すべ てのコンポーネント)	22 および 443	SSH および HTTPS
		NSX-T Manager	443	TCP
		VMware PKS API サー バ	8443 および 9021	TCP
		Kubernetes API サーバ	8443	TCP

表 1-11. (続き)

目的	接続元	接続先	ポート	プロトコル
		vRealize Log Insight	443	HTTPS
		Fortinet FortiManager	443	HTTPS

サポート対象の製品とバージョン

vRealize Network Insight はいくつかの製品およびバージョンをサポートしています。

データ ソース	バージョン / モデル	接続プロトコル	権限
Amazon Web Services (エンタープライズライセンスのみ)	該当なし	HTTPS	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Arista スイッチ	7050TX、7250QX、7050QX-32S、7280SE-72	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Azure サブスクリプション	該当なし	HTTPS	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Brocade スイッチ	VDX 6740、VDX 6940、MLX、MLXe	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Check Point ファイアウォール	Check Point R80、R80.10、R80.20、R80.30	HTTPS、SSH	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco ACI	3.2	HTTPS (APIC コントローラ) SNMP (APIC コントローラおよび ACI スイッチ)	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco ASA	OS 9.4 の X シリーズ	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco Catalyst	3000、3750、4500、6000、6500	SSH、SNMP	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Cisco Nexus	3000、5000、6000、7000、9000	SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー
Cisco UCS (統合コンピューティングシステム)	シリーズ B ブレード サーバ、シリーズ C ラック サーバ、シャーシ、ファブリック相互接続	UCS Manager : HTTPS UCS ファブリック : SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー
Dell スイッチ	FORCE10 MXL 10、FORCE10 S6000、S4048、Z9100、S4810、PowerConnect 8024、Dell OS10	SSH、SNMP	読み取り専用ユーザー 読み取り専用 SNMP ユーザー

データ ソース	バージョン / モデル	接続プロトコル	権限
Fortinet FortiManager	6.0.1	HTTPS	<p>ユーザーには次のものがが必要です。</p> <ul style="list-style-type: none"> ■ すべての ADOM およびポリシー パッケージへのアクセス権を持つ制限されたユーザー 以上のロール。 ■ コマンドライン インターフェイスから有効にされた rpc-permit read アクセス権。
F5 BIG - IP	12.1.2 以降	HTTPS、SSH、SNMP	<p>ユーザーには、ロールが 1 つ以上必要です。また、TMSH が有効になっており、すべてのパーティションにアクセスする必要があります。F5 BIG-IP は、ルーティングとロード バランシングの両方をサポートします。</p>
HP	HP Virtual Connect Manager 4.41、HP OneView 3.0	HP OneView 3.0 : HTTPS HP Virtual Connect Manager 4.41 : SSH	読み取り専用ユーザー
Huawei Cloud Engine	6800、7800、8800	SSH、SNMP	<p>読み取り専用ユーザー 読み取り専用 SNMP ユーザー</p>
Infoblox	Infoblox NIOS バージョン 8.0、8.1、8.2	HTTPS	<p>API インターフェイス アクセス権を持つ読み取り専用ユーザー DNS オブジェクト タイプの読み取り専用権限は次のとおりです。</p> <ul style="list-style-type: none"> ■ 権限タイプ - DNS ■ リソース - A レコード、DNS ゾーン、DNS ビュー
Juniper スイッチ	EX3300、QFX 51xx シリーズ (JunOS v12 & v15、QFabric なし)	Netconf、SSH、SNMP	<p>読み取り専用ユーザー 読み取り専用 SNMP ユーザー</p>
Kubernetes	<ul style="list-style-type: none"> ■ 1.12 (NSX-T 2.3.1) ■ 1.12 (NSX-T 2.3.2) ■ 1.13 (NSX-T 2.3.2) 	HTTPS	<p>ユーザーには、読み取り権限を持つクラスター管理者ロールが必要です。</p>
OpenShift	3.1.1	HTTPS	『ユーザー ガイド』の「データソースの追加」セクションを参照してください。
Palo Alto Networks	Panorama 7.0.x、7.1、8.x、9.0	HTTPS	<p>ユーザーには、XML API アクセス権限を持つ管理者ロールが必要です。詳細については、『vRealize Network Insight ユーザー ガイド』の「Palo Alto Networks」セクションを参照してください。</p>
ServiceNow	London	HTTPS	ユーザーには管理者ロールが必要です
VMware SD-WAN	VeloCloud Orchestrator および Edge バージョン 3.3.1 以降	HTTPS	<p>ユーザーには、次のいずれかの権限を持つアカウント ロールが必要です。</p> <ul style="list-style-type: none"> ■ スーパーユーザー ■ 標準管理者 ■ カスタム サポート

データ ソース	バージョン / モデル	接続プロトコル	権限
VMC on AWS - vCenter	M8 以降 注: NSX-T ベースの VMware Cloud on AWS SDDC のみがサポートされます。	HTTPS	ユーザーには次の権限が必要です。 ■ クラウド管理者: データ ソースを追加して、IPFIX を有効にします。
VMC on AWS - NSX Manager	M8 以降 注: NSX-T ベースの VMware Cloud on AWS SDDC のみがサポートされます。	HTTPS	ユーザーには次のいずれかの権限が必要です。 ■ 組織メンバー.管理者: データ ソースの追加と IPFIX の有効化。 ■ 組織メンバー.管理者.NSX Cloud 管理者: データ ソースの追加と IPFIX の有効化。 ■ 組織メンバー.VMware Cloud on AWS (すべてのロール): データ ソースの追加と IPFIX の有効化。 ■ 組織メンバー.NSX Cloud 監査者: データ ソースの追加。
VMware Identity Manager	3.3 以降	HTTPS	ユーザーには管理者ロールが必要です。
VMware PKS	サポートされているバージョン		ユーザーにはクラスタ管理者ロールの権限 - pks.clusters.admin が必要です。
VMware NSX Manager (VMware NSX-V)	サポートされているバージョン	SSH、HTTPS	『vRealize Network Insight ユーザーガイド』の「Edge データ収集」セクションを参照してください。
VMware NSX-T Manager	2.4。 その他のサポートされるバージョンについては、サポートされるバージョンを参照してください。	HTTPS	読み取り専用ユーザー
VMware vRealize Log Insight	サポートされているバージョン	HTTPS	コンテンツ バックをインストール、構成、管理する権限を持つ API ユーザー
VMware vSphere	サポートされているバージョン IPFIX の場合、VMware ESXi のバージョンは次のようになります。 ■ 5.5 Update 2 (ビルド 2068190) 以降 ■ 6.0 Update 1b (ビルド 3380124) 以降 ■ VMware VDS 5.5 以降 注: 仮想マシン間のバスを識別するには、データセンターのすべての仮想マシンに VMware Tools をインストールする必要があります。	HTTPS	読み取り専用ユーザー IPFIX の構成と使用に必要な権限 権限付きの vCenter Server 認証情報: Distributed Switch: Modify dvPort group: Modify vCenter Server の事前定義ロールには、root レベルで割り当てられた、子ロールに伝達が必要な次の権限が必要です。 System.Anonymous System.Read System.View global.settings

注：

- Cisco ASA、ACI、Catalyst、および Nexus デバイスでサポートされているオペレーティング システムは、iOS/NX-OS です。Cisco UCS の場合は、UCSM バージョンです。
 - Arista でサポートされているオペレーティング システムは、Arista EOS です。
-

vRealize Network Insight のインストール

2

vSphere Web client または vSphere Windows ネイティブ クライアントを使用して、vRealize Network Insight を展開できます。

注： vRealize Network Insight Platform OVA を正常に展開したら、指定された固定 IP アドレスが vCenter Server に設定されているかどうかを確認します。

インストール、構成、アップグレード、パッチ、構成管理、ドリフト修正、および健全性を単一の管理画面で自動化するために、vRealize Suite Lifecycle Manager を使用できます。新規ユーザーの方は、[ここをクリックして vRealize Suite Lifecycle Manager](#) をインストールしてください。クラウド管理リソースの IT 管理者はこれを使用して、価値の提供 (TTV)、信頼性、一貫性を向上させながら、ビジネス クリティカルなイニシアチブに集中することができます。

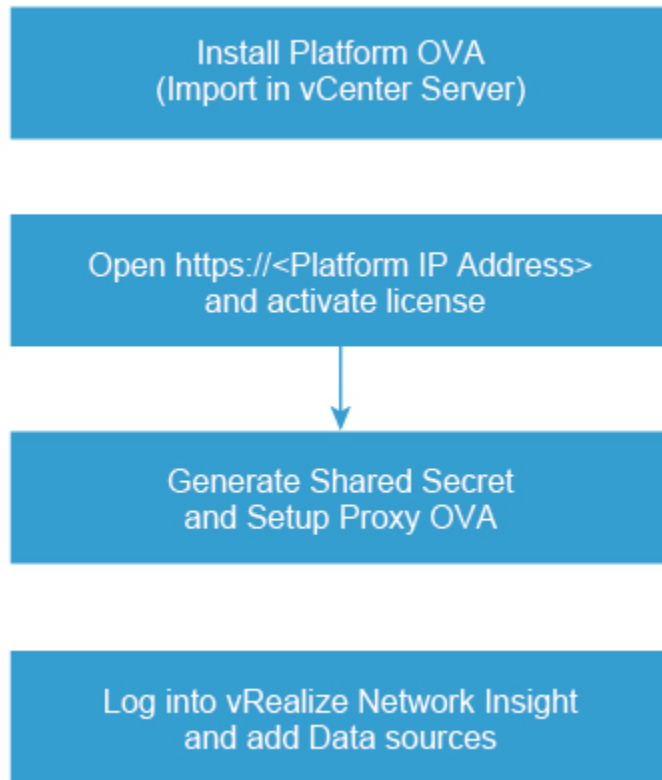
vRealize Suite Lifecycle Manager を使用して、vRealize Network Insight をインストールおよびアップグレードすることもできます。詳細については、[vRealize Suite Lifecycle Manager Installation, Upgrade, and Management Guide](#) を参照してください。

この章には、次のトピックが含まれています。

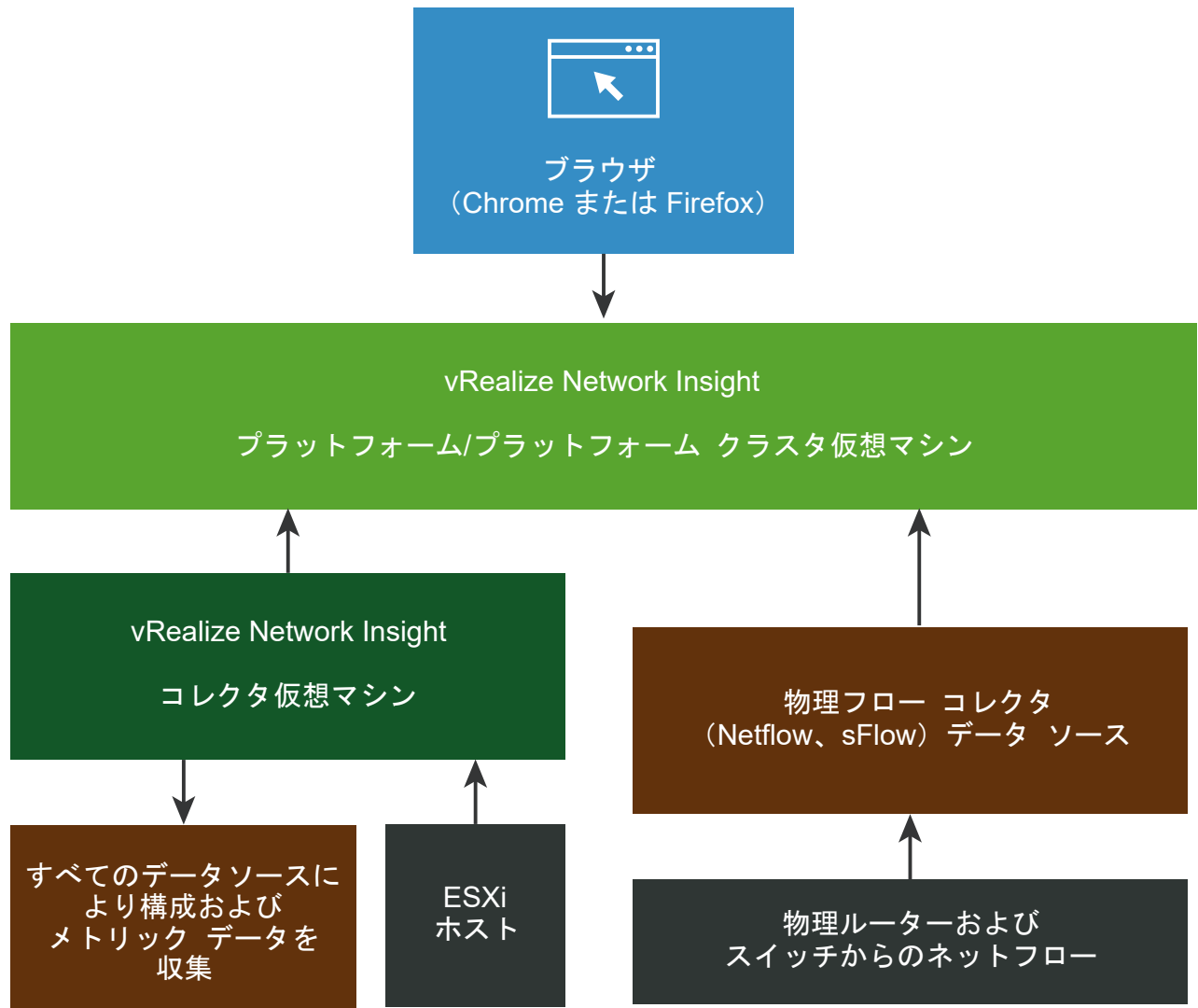
- [インストール ワークフロー](#)
- [vRealize Network Insight プラットフォーム OVA の展開](#)
- [ライセンスを有効にする](#)
- [共有シークレットの生成](#)
- [Network Insight Collector の設定 \(OVA\)](#)
- [AWS での Network Insight Collector \(AMI\) の VMware SD-WAN 用の設定](#)
- [既存の設定への追加コレクタの展開](#)

インストール ワークフロー

vRealize Network Insight をインストールするには、プラットフォーム OVA をインストールして、ライセンスを有効にし、共有シークレットを生成してコレクタ OVA を設定します。



vRealize Network Insight の概要の展開図は次のとおりです。



vRealize Network Insight プラットフォーム OVA の展開

vRealize Network Insight プラットフォーム OVA を vCenter Server にインポートできます。

注： VMC SDDC での vRealize Network Insight プラットフォーム OVA の展開はサポートされていません。

vSphere Web Client を使用した導入

vSphere Web Client を使用して、vRealize Network Insight を展開できます。

手順

- 1 アプライアンスをインストールする [データセンター] を右クリックし、[OVF テンプレートの展開] を選択します。
- 2 URL を入力して、OVA パッケージをダウンロードしてインストールするか、OVA パッケージのソースの場所を参照して選択します。

- 3 OVA 名を入力します。展開の配置先フォルダを選択してください。
- 4 展開したテンプレートを実行するホスト、クラスタまたはリソース プールを選択します。
- 5 OVF テンプレートの詳細を確認します。
- 6 エンド ユーザー使用許諾契約書を読み、[同意] をクリックします。
- 7 展開の設定を選択します。[次へ] をクリックします。
- 8 展開したテンプレートのファイルを保存する場所を選択します。仮想ディスク フォーマットとして [シン プロビジョニング] を選択します。ファイルを格納するデータストアまたはデータストア クラスタを選択します。[次へ] をクリックします。
- 9 展開した仮想マシンが使用するネットワークを選択します。
選択したネットワークは、サポートおよびアップグレードのためにアプライアンスがインターネットにアクセスできるようにする必要があります。
- 10 展開用のテンプレートをカスタマイズするには、仮想マシン コンソールを使用してアプライアンスを手動で構成する必要があります。[次へ] をクリックします。
- 11 構成の詳細を確認して、[次へ] をクリックします。
- 12 システムの推奨事項と要件を一致させるには、[設定のブリック サイズの増加](#)を参照してください。
- 13 プラットフォームがインストールされたら、仮想マシンを起動してコンソールを起動します。
- 14 画面に表示されているコンソール認証情報を使用してログインし、`setup` コマンドを実行します。
- 15 `support` ログイン用のパスワードを作成し、`consoleuser` 用のパスワードを変更します。

注：

- パスワードの長さは 6 文字以上にする必要があります。単一引用符 (') は許可されていません。
- 組織のポリシーに準拠するには、`support` と `consoleuser` のパスワードを定期的に変更する必要があります。

- 16 次の詳細を入力して、ネットワークを構成します。
 - a [IPv4 アドレス] : 2 番目の予約済み固定 IP アドレス
 - b [ネットマスク] : 上記の固定 IP アドレスのサブネット マスク
 - c [デフォルト ゲートウェイ] : ネットワークのデフォルト ゲートウェイ
 - d [DNS] : お使いの環境の DNS サーバ

注： 複数の DNS サーバの場合は、それらがスペースで区切られているようにします。

- e [ドメイン検索リスト] : DNS 参照用に追加する必要があるドメイン
- f `y` と入力して設定を保存します。

- 17 NTP サーバを入力し、仮想マシンから確実にアクセスできるようにします。NTP 時間が同期されていない場合、サービスは起動に失敗します。

注： 複数の NTP サーバの場合は、それらをカンマで確実に区切ります。

- 18 (オプション) Web プロキシを設定するには、y と入力します。
- 19 すべてのサービスが検証されます。
- 20 セットアップの要件に基づいてディスク容量を追加します。<https://kb.vmware.com/s/article/53550> を参照してください。

vSphere Windows ネイティブ クライアントを使用した展開

vSphere Windows ネイティブ クライアントを使用して、vRealize Network Insight を展開できます。

注： vRealize Network Insight 5.2 は、vSphere Windows ネイティブ クライアントを使用して、OVA の展開をサポートする最後のリリースです。5.3 リリース以降では、vSphere Web Client を引き続き使用して、vRealize Network Insight OVA を展開できます。

手順

- 1 [ファイル] - [OVF テンプレートの展開] をクリックします。
- 2 URL を入力して、インターネットから OVA パッケージをダウンロードしてインストールするか、コンピュータ上の OVA パッケージのソースの場所を参照して選択します。
- 3 [次へ] をクリックし、OVF テンプレートの詳細を確認します。
- 4 エンド ユーザー使用許諾契約書を読み、[同意] をクリックします。
- 5 展開されたテンプレートの名前と場所を指定します。[次へ] をクリックします。
- 6 [展開の設定] を選択します。
- 7 展開されたテンプレートを実行する [ホスト/クラスタ] を選択します。
- 8 このテンプレートを展開する [リソース プール] を選択します。
- 9 仮想マシン ファイルのターゲット ストレージを選択します。[次へ] をクリックします。
- 10 仮想ディスクを格納するフォーマットを指定します。仮想ディスク フォーマットとして [シン プロビジョニング] を選択します。[次へ] をクリックします。
- 11 展開されたテンプレートが使用するネットワークを指定します。ネットワークを OVA からインベントリにマッピングします。
- 12 展開用のテンプレートをカスタマイズします。オンボード ページで生成された共有シークレット キーを指定します。仮想マシン コンソールを使用してアプライアンスを手動で設定する必要があります。[次へ] をクリックします。
- 13 すべての設定データを確認します。[展開後にパワーオン] を選択します。[終了] をクリックします。
- 14 システムの推奨事項と要件を実行して、設定のブリック サイズの増加に一致させます。
- 15 コレクタ OVA がインストールされたら、仮想マシンを起動してコンソールを起動します。

16 画面に表示されているコンソール認証情報を使用してログインし、`setup` コマンドを実行します。

17 `support` ログイン用のパスワードを作成し、`consoleuser` 用のパスワードを変更します。

注：

- パスワードの長さは 6 文字以上にする必要があります。単一引用符 (') は許可されていません。
 - 組織のポリシーに準拠するには、`support` と `consoleuser` のパスワードを定期的に変更する必要があります。
-

18 次の詳細を入力して、ネットワークを構成します。

- a [IPv4 アドレス]：2 番目の予約済み固定 IP アドレス
- b [ネットマスク]：上記の固定 IP アドレスのサブネット マスク
- c [デフォルト ゲートウェイ]：ネットワークのデフォルト ゲートウェイ
- d [DNS]：お使いの環境の DNS サーバ

注： 複数の DNS サーバの場合は、それらがスペースで区切られているようにします。

e [ドメイン検索リスト]：`dns lookup` に追加する必要があるドメイン。

f `y` と入力して設定を保存します。

19 NTP サーバを入力し、仮想マシンから確実にアクセスできるようにします。NTP 時間が同期されていない場合、サービスは起動に失敗します。

注： 複数の NTP サーバの場合は、それらをカンマで確実に区切ります。

20 (オプション) Web プロキシを構成するには、`y` と入力します。

21 すべてのサービスが検証されます。

22 セットアップの要件に基づいてディスク容量を追加します。<https://kb.vmware.com/s/article/53550> を参照してください。

ライセンスを有効にする

vRealize Network Insight プラットフォーム OVA をインストールした後、Chrome Web ブラウザで `https://<vRealize Network Insight プラットフォームの IP アドレス>` を開きます。

手順

1 ようこそメールで受信したライセンス キーを入力します。

2 ユーザー名がユーザー インターフェイス管理者 (`admin@local`) の場合は、パスワードを設定します。

注： パスワードは、8 文字以上、最大 100 文字の英数字である必要があります。文字の間にスペースは使用できません。

3 [有効化] をクリックします。

- 4 ライセンスを有効にしてから、vRealize Network Insight コレクタを追加します。

共有シークレットの生成

vRealize Network Insight コレクタ仮想アプライアンスを生成してインポートすることができます。

共有シークレットを生成し、vRealize Network Insight コレクタ仮想アプライアンスをインポートします。

手順

- 1 vRealize Network Insight ユーザー インターフェイスにログインします。
- 2 [インフラストラクチャおよびサポート] を展開し、[概要と更新] をクリックします。
- 3 下にスクロールして、[プロキシ仮想マシンの追加] をクリックします。
[新しい Network Insight データ コレクタ仮想アプライアンスの追加] ダイアログが表示されます。
- 4 [コピー] をクリックして、ダイアログから共有シークレットをコピーし、[完了] をクリックします。
これは vRealize Network Insight コレクタ OVA の展開時に必要になります。

Network Insight Collector の設定 (OVA)

vCenter Server に OVA をインポートすることで、vRealize Network Insight Collector を設定することができます。

次の手順に従って、vRealize Network Insight Collector の OVA を vCenter Server にインポートします。

vSphere Web Client を使用した導入

vSphere Web Client を使用して、vRealize Network Insight コレクタ OVA をインポートできます。

手順

- 1 アプライアンスをインストールする [データセンター] を右クリックし、[OVF テンプレートの展開] を選択します。
- 2 URL を入力して、インターネットから OVA パッケージをダウンロードしてインストールするか、コンピュータにある OVA のソースの場所に移動して選択します。
- 3 展開されたテンプレートの名前と場所を指定します。[次へ] をクリックします。
- 4 展開されたテンプレートを実行するリソース（ホストまたはクラスター）を選択します。[次へ] をクリックします。
- 5 テンプレートのすべての詳細を確認します。[次へ] をクリックします。
- 6 エンド ユーザー使用許諾契約書を読み、[同意] をクリックします。[次へ] をクリックします。
- 7 展開の設定を選択します。[次へ] をクリックします。

- 8 展開されたテンプレートのファイルを保存する場所を選択します。仮想ディスクを格納するフォーマットを指定します。仮想ディスク フォーマットとして [シン プロビジョニング] を選択します。ファイルをインストールするデータストアを選択します。[次へ] をクリックします。
- 9 ソース ネットワークのターゲット ネットワークを指定します。[次へ] をクリックします。
- 10 展開用のテンプレートをカスタマイズします。ユーザー インターフェイスから生成された共有シークレットを指定します。仮想マシン コンソールを使用してアプライアンスを手動で設定する必要があります。[次へ] をクリックします。
- 11 すべての設定データを確認します。[終了] をクリックします。
- 12 コレクタ OVA がインストールされたら、仮想マシンを起動してコンソールを起動します。
- 13 画面に表示されているコンソール認証情報を使用してログインし、`setup` コマンドを実行します。
- 14 `support` ログイン用のパスワードを作成し、`consoleuser` 用のパスワードを変更します。

注：

- パスワードの長さは 6 文字以上にする必要があります。単一引用符 (') は許可されていません。
 - 組織のポリシーに準拠するには、`support` と `consoleuser` のパスワードを定期的に変更する必要があります。
-

- 15 次の詳細を入力して、ネットワークを構成します。
 - a [IPv4 アドレス]：2 番目の予約済み固定 IP アドレス
 - b [ネットマスク]：上記の固定 IP アドレスのサブネット マスク
 - c [デフォルト ゲートウェイ]：ネットワークのデフォルト ゲートウェイ
 - d [DNS]：お使いの環境の DNS サーバ

注： 複数の DNS サーバの場合は、それらがスペースで区切られているようにします。

- e [ドメイン検索リスト]：DNS 参照用に追加する必要があるドメイン
 - f `y` と入力して設定を保存します。
- 16 NTP サーバを入力し、仮想マシンから確実にアクセスできるようにします。NTP 時間が同期されていない場合、サービスは起動に失敗します。

注： 複数の NTP サーバの場合は、それらをカンマで確実に区切ります。

- 17 (オプション) Web プロキシを設定するには、次の手順を実行します。
 - a `y` と入力します。
 - b Web プロキシの詳細を入力します。
- 18 共有シークレット キーが設定されているかどうかを確認するチェックが行われます。コレクタは、対応するプラットフォームとペアになります。この処理には、数分かかる場合があります。
- 19 すべてのサービスが検証されます。

20 [完了] をクリックすると、[プロキシが検出されました。] というメッセージがオンボード ページに表示されます。ログイン画面にリダイレクトされます。

vSphere Windows ネイティブ クライアントを使用した展開

vSphere Windows ネイティブ クライアントを使用して、vRealize Network Insight コレクタ OVA をインポートできます。

注： vRealize Network Insight 5.2 は、vSphere Windows ネイティブ クライアントを使用して、OVA の展開をサポートする最後のリリースです。5.3 リリース以降では、vSphere Web Client を引き続き使用して、vRealize Network Insight OVA を展開できます。

手順

- 1 [ファイル] - [OVF テンプレートの展開] をクリックします。
- 2 URL を入力して、インターネットから OVA パッケージをダウンロードしてインストールするか、コンピュータ上の OVA パッケージのソースの場所を参照して選択します。
- 3 OVF テンプレートの詳細を確認します。[次へ] をクリックします。
- 4 エンド ユーザー使用許諾契約書を読み、[同意] をクリックします。[次へ] をクリックします。
- 5 展開されたテンプレートの名前と場所を指定します。[次へ] をクリックします。
- 6 [展開設定] を選択します。[次へ] をクリックします。
- 7 展開されたテンプレートを実行する [ホスト/クラスタ] を選択します。[次へ] をクリックします。
- 8 このテンプレートを展開する [リソース プール] を選択します。[次へ] をクリックします。
- 9 仮想マシン ファイルのターゲット ストレージを選択します。[次へ] をクリックします。
- 10 仮想ディスクを格納するフォーマットを指定します。仮想ディスク フォーマットとして [シン プロビジョニング] を選択します。[次へ] をクリックします。
- 11 展開されたテンプレートが使用するネットワークを指定します。ネットワークを OVA からインベントリにマッピングします。
- 12 展開用のテンプレートをカスタマイズします。オンボード ページで生成された共有シークレット キーを指定します。仮想マシン コンソールを使用してアプライアンスを手動で設定する必要があります。[次へ] をクリックします。
- 13 すべての設定データを確認します。[展開後にパワーオン] を選択します。[終了] をクリックします。
- 14 コレクタ OVA がインストールされたら、仮想マシンを起動してコンソールを起動します。
- 15 指定されたコンソール認証情報を使用してログインします。setup コマンドを実行します。
- 16 support ログイン用のパスワードを作成します。consoleuser のパスワードを変更します。
- 17 次の詳細を入力して、ネットワークを構成します。
 - a [IPv4 アドレス] : 2 番目の予約済み固定 IP アドレス
 - b [ネットマスク] : 上記の固定 IP アドレスのサブネット マスク

- c [デフォルト ゲートウェイ] : ネットワークのデフォルト ゲートウェイ
- d [DNS] : お使いの環境の DNS サーバ

注： 複数の DNS サーバの場合は、それらがスペースで区切られているようにします。

- e [ドメイン検索リスト] : dns lookup に追加する必要があるドメイン。
- f y と入力して設定を保存します。

- 18 NTP サーバを入力し、仮想マシンから確実にアクセスできるようにします。NTP 時間が同期されていない場合、サービスは起動に失敗します。

注： 複数の NTP サーバの場合は、それらをカンマで確実に区切ります。

- 19 (オプション) Web プロキシを構成するには、次の手順を実行します。

- a y と入力します。
- b Web プロキシの詳細を入力します。

- 20 共有シークレット キーが構成されているかどうかを確認するチェックが行われます。コレクタは、対応するプラットフォームとペアになります。この処理には、数分かかる場合があります。

- 21 すべてのサービスが検証されます。

- 22 [完了] をクリックすると、[プロキシが検出されました。] というメッセージがオンボード ページに表示されます。ログイン画面にリダイレクトされます。

AWS での Network Insight Collector (AMI) の VMware SD-WAN 用の設定

AWS 環境に Amazon Machine Image (AMI) をインポートすることで、AWS に vRealize Network Insight コレクタを設定することができます。

環境に vCenter Server がなく、クラウド環境にコレクタをデプロイする場合は、AWS にコレクタを展開することができます。

注： 現在、vRealize Network Insight では、AMI を使用した AWS へのコレクタの展開は、VMware SD-WAN に対してのみサポートされています。

EC2 インスタンスに関連する手順とタスクは、<https://docs.aws.amazon.com/efs/index.html> に記載されています。

手順

- 1 Amazon EC2 Console で VMware 提供の AMI を使用して、EC2 インスタンスを起動します。詳細については、「Amazon Elastic File System」ドキュメントの「Create Your EC2 Resources and Launch Your EC2 Instance」トピックを参照してください。

注： AWS で EC2 インスタンスを起動する際には、次の項目を選択する必要があります。

オプション	アクション
[インスタンス タイプ]	m4.xlarge (中規模ブリック)
[ネットワーク]	適切なネットワークとサブネットを選択します。
[ストレージ]	デフォルトのストレージ。
[タグ]	ユーザーのポリシーに基づきます。
[セキュリティ グループ]	ポート 443 に、0.0.0.0/0 への送信を許可します。制限付きルールの場合は、ポート 443 に NI SaaS Prod FQDN を許可します。
[キー]	適切なキーを選択します。AMI では SSH ログインが有効です。

- 2 EC2 インスタンスが実行状態の場合は、EC2 インスタンスにログインします。
- 3 指定されたコンソール認証情報を使用してログインします。setup コマンドを実行します。
- 4 support ログイン用のパスワードを作成します。consoleuser のパスワードを変更します。

注： パスワードの変更後、セットアップ CLI ではネットワーク オプションがスキップされます。

プロキシ AMI は、次の機能をサポートしていません。

- IP アドレスの変更
- IPv6
- Web プロキシの構成

- 5 NTP サーバを入力し、仮想マシンから確実にアクセスできるようにします。NTP 時間が同期されていない場合、サービスは起動に失敗します。

注： 複数の NTP サーバの場合は、それらをカンマで確実に区切ります。

- 6 共有シークレット キーが設定されているかどうかを確認するチェックが行われます。コレクタは、対応するプラットフォームとペアになります。このプロセスには数分かかることがあります。
- 7 すべてのサービスが検証されます。

次のステップ

Edge から AWS に展開したコレクタへのフロー収集を有効にします。フロー収集を有効にするには、以下を実行します。

- AWS に展開したコレクタを非 VeloCloud サイトにします。詳細については、VMware サポートにお問い合わせください。

既存の設定への追加コレクタの展開

既存の設定に追加の vRealize Network Insight コレクタを追加できます。

手順

- 1 vRealize Network Insight ユーザー インターフェイスにログインします。
- 2 [インフラストラクチャおよびサポート] を展開し、[概要と更新] をクリックします。
- 3 下にスクロールして、[プロキシ仮想マシンの追加] をクリックします。
[新しい Network Insight データ コレクタ仮想アプライアンスの追加] ダイアログが表示されます。
- 4 [コピー] をクリックして、ダイアログから共有シークレットをコピーし、[完了] をクリックします。
- 5 セクション [Network Insight Collector の設定 \(OVA\)](#) の手順 3 を実行します。

評価ライセンスを使用した vRealize Network Insight へのアクセス

3

評価ライセンスを使用すると、vRealize Network Insight は NSX 評価モードで開始します。

データ ソースを vRealize Network Insight に追加して、トラフィック フローを分析し、レポートを生成することができます。

注： 完全な製品モードに切り替えるには、右下隅にある 完全な製品評価に切り替え をクリックします。

この章には、次のトピックが含まれています。

- [vCenter Server を追加](#)
- [トラフィック フローの分析](#)
- [レポートの生成](#)

vCenter Server を追加

vCenter Servers をデータ ソースとして vRealize Network Insight に追加できます。

複数の vCenter Servers を vRealize Network Insight に追加して、データの監視を開始できます。

前提条件

- vCenter Server の事前定義ロールには、root レベルで割り当てられた、子ロールに伝達が必要な次の権限が必要です。
 - System.Anonymous
 - System.Read
 - System.View
 - Global.Settings
- IPFIX の設定と使用には、次の vCenter Server 権限が必要です。
 - Distributed Switch : 変更およびポート設定操作
 - dvPort グループ : 変更およびポリシー操作

vCenter Server でのロールの詳細については、『vSphere セキュリティ ガイド』の「ロールを使用した権限の割り当て」セクションを参照してください。

手順

- 1 [vCenter Server の追加] をクリックします。
- 2 [新しいソースの追加] をクリックし、オプションをカスタマイズします。

オプション	アクション
コレクタ仮想マシン	ドロップダウン メニューからコレクタ仮想マシンを選択します。
IP アドレス/FQDN	vCenter Server の IP アドレスまたは完全修飾ドメイン名を入力します。
ユーザー名	次の権限を持つユーザー名を入力します。 ■ [Distributed Switch] : 変更 ■ [dvPort グループ] : 変更
パスワード	vCenter Server システムにアクセスするための vRealize Network Insight ソフトウェアのパスワードを入力します。

- 3 [検証] をクリックします。

検出された仮想マシンの数が、プラットフォームまたはコレクタ ノードのキャパシティを超えている場合、検証に失敗します。プラットフォームのブリック サイズを増やすか、クラスタを作成するまでは、データ ソースを追加することはできません。

フローがある場合とない場合の各ブリック サイズの指定されたキャパシティは、次のようになります。

ブリック サイズ	仮想マシン	フローの状態
大	6 k	有効
大	10 k	無効
中	3 k	有効
中	6 k	無効

- 4 IPFIX を有効にするには、[この vCenter Server での Netflow (IPFIX)] を選択します。

IPFIX の詳細については、ユーザー ガイドの「Distributed Switch および DVPG での IPFIX 設定の有効化」のセクションを参照してください。

注： vCenter Server と VMware NSX Manager の両方で IPFIX を有効にすると、vRealize Network Insight は、関連付けられた vCenter Server で一部の DVPG で IPFIX を無効にして、フローの冗長性を自動的に検出して削除します。

- 5 高度なデータ収集ソースを vCenter Server システムに追加します。
- 6 vCenter Server システムを追加するには、[送信] をクリックします。vCenter Server システムがホーム画面に表示されます。

トラフィック フローの分析

vRealize Network Insight を使用して、データセンター内のフローを分析できます。

前提条件

フロー分析を開始する前に、データの収集を 2 時間以上行う必要があります。

手順

- 1 分析の範囲を指定します。たとえば、[クラスタ] のすべての仮想マシンのフローを分析する場合は、ドロップダウンメニューからクラスタを選択します。VLAN または VXLAN に接続されているすべての仮想マシンを交互に選択できます。
- 2 フローを分析するエンティティ名を選択します。
- 3 期間を選択し、[分析] をクリックします。

レポートの生成

フロー評価のレポートを生成できます。

前提条件

データセンター内のトラフィック フローを分析します。包括的なレポートを生成するには、分析前に 24 時間分のデータを収集します。

手順

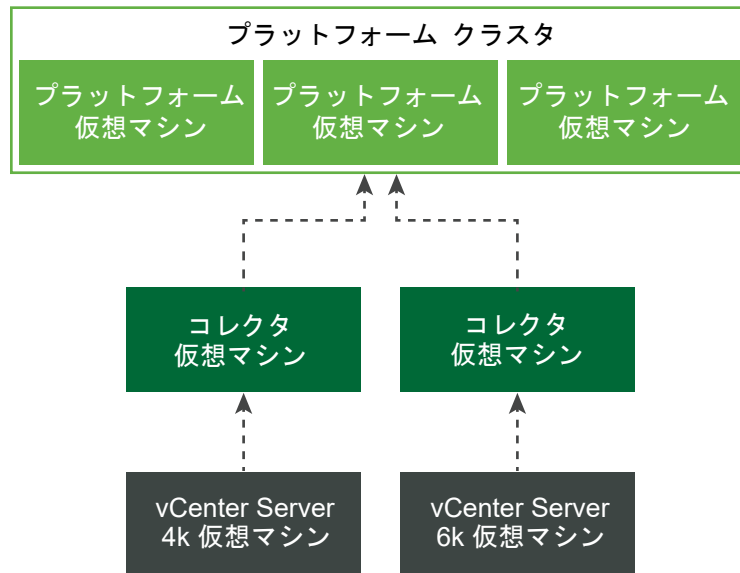
- 1 [NSX 評価モードの評価] では、[分析フロー] ページで [レポートの生成] をクリックします。
- 2 [非評価モード] では、[マイクロセグメンテーション] ページで [トラフィック ディストリビューション] > [詳細オプション] > [評価レポート] をクリックします。

展開のスケールアップ計画

4

設定内の仮想マシン数またはアクティブなフローの数が多い場合や、拡張が予想される場合は、プラットフォームまたはコレクタのサイズを拡張することができます。

プラットフォームとコレクタの分布について理解を深めるには、次のアーキテクチャを使用します。



この章には、次のトピックが含まれています。

- [プラットフォーム クラスタのスケールアップ計画](#)
- [コレクタのスケールアップ計画](#)
- [設定のブリック サイズの増加](#)

プラットフォーム クラスタのスケールアップ計画

負荷の増加に応じて、プラットフォーム クラスタをスケールアップできます。負荷に基づいて、ブリックサイズを増やすか、プラットフォーム クラスタを作成または拡張するかのいずれかの方法でスケールアップが可能です。3 つの LARGE プラットフォーム ブリックを接続して、1 つのプラットフォーム クラスタを形成することができます。プラットフォームのブリック サイズが LARGE または EXTRA LARGE の場合は、プラットフォーム クラスタを作成してスケールアップする必要があります。

プラットフォームのブリック サイズとプラットフォーム ブリックの数の決定については、[システムの推奨事項と要件](#)を参照してください。

注： プラットフォーム クラスタは、高可用性構成をサポートしていません。クラスタを最適なパフォーマンス レベルで動作させるために、すべてのプラットフォーム ノードが稼動している必要があります。

プラットフォーム クラスタのスケールアップ シナリオ

- シナリオ 1：プラットフォームで 5,000 台の仮想マシンと 150 万のアクティブ フローが実行されている場合
プラットフォームを MEDIUM から LARGE に変換します。[設定のブリック サイズの増加](#)を参照してください。
- シナリオ 2：プラットフォームで 9,000 台の仮想マシンと 200 万のアクティブ フローを持つ LARGE ノードが実行されている場合
LARGE ブリック ノードを 2 台追加して、3 ノードの LARGE ブリック クラスタに変換します。『vRealize Network Insight ユーザー ガイド』の「クラスタの拡張」を参照してください。
- シナリオ 3：プラットフォームで 1 つ以上のコレクタ、15,000 台以上の仮想マシンと 400 万のアクティブなフローを持つ 3 ノードの LARGE クラスタを実行している場合。
既存のプラットフォーム ノードを LARGE から EXTRA-LARGE に変換します。[設定のブリック サイズの増加](#)を参照してください。
- シナリオ 4：プラットフォームで 1 つ以上のコレクタ、25,000 台以上の仮想マシンと 800 万のアクティブなフローを持つ 3 ノードの EXTRA-LARGE クラスタを実行している場合。
EXTRA-LARGE ブリック ノードを 2 台追加して、5 ノードの Extra-LARGE クラスタに変換します。『vRealize Network Insight ユーザー ガイド』の「クラスタの拡張」を参照してください。

コレクタのスケールアップ計画

コレクタの容量は、ブリック サイズに基づきます。コレクタに追加できるデータソースは、コレクタ（仮想マシンおよびフロー）の容量によって異なります。

表 1-6. コレクタの展開 - 最大容量を参照してください。コレクタのブリック サイズを LARGE にすると、コレクタをさらに追加する必要があります。各コレクタを EXTRA-LARGE サイズにスケールアップできます。

サポートされているコレクタ容量に基づいて、複数のデータソースをコレクタに追加できます。ただし、複数のコレクタに同一のデータソースを追加することはできません。

コレクタのスケールアップ シナリオ

- シナリオ 1：vCenter Server 内の 2,000 台の仮想マシン。
中規模なコレクタ仮想マシンを 1 台インストールします。このコレクタに vCenter Server を追加します。[vCenter Server を追加](#)を参照してください。
- シナリオ 2：vCenter Server 1 に 1,000 台の仮想マシンがあり、vCenter Server 2 に 2,000 台の仮想マシン（すべて 1 つのデータセンターに配置）。

中規模なコレクタ仮想マシンを 1 台インストールします。このコレクタに両 vCenter Server を追加します。[vCenter Server を追加](#)を参照してください。

- シナリオ 3 : vCenter Server 1 (データセンター 1) に 1,000 台の仮想マシンがあり、vCenter Server 2 (データセンター 2) に 2,000 台の仮想マシンがあるとします。

各データセンターに中規模なコレクタ仮想マシンを 1 台インストールします。同じデータセンター内のコレクタ仮想マシンに vCenter Server 1 を追加し、そのデータセンターのコレクタ仮想マシンに vCenter Server 2 を追加します。[vCenter Server を追加](#)を参照してください。

- シナリオ 4 : 仮想マシンの数が 4,000 台を超えており、アクティブなフローが 250 万を超えている場合。
コレクタ仮想マシンを MEDIUM から LARGE に変換します。[設定のブリック サイズの増加](#)を参照してください。

- シナリオ 5 : vCenter Server 1 に 9,000 台の仮想マシンがあり、フローがない場合 (データセンター 1)。
大規模なコレクタ仮想マシンを 1 台インストールします。コレクタにこの vCenter Server を追加します。[vCenter Server を追加](#)を参照してください。

- シナリオ 6 : 仮想マシンの数が 10,000 台以下で、アクティブなフローが 500 万を超えている場合。
コレクタ仮想マシンを LARGE から EXTRA-LARGE に変換します。[設定のブリック サイズの増加](#)を参照してください。

- シナリオ 8 : 2 台の vCenter Server があり、vCenter Server 1 には 1 万個の仮想マシンと 900 万のアクティブなフローがあり、vCenter Server 2 には 1 万台の仮想マシンと 400 万のアクティブなフローがある場合。
1 つの EXTRA-LARGE と 1 つの LARGE プロキシをインストールします。vCenter Server 1 を EXTRA-LARGE プロキシに追加し、vCenter Server 2 を LARGE プロキシに追加します。

- シナリオ 9 : 1 万台の仮想マシンと 900 万のアクティブなフローを実行する 1 つの vCenter Server。
1 つの EXTRA-LARGE プロキシをインストールし、vCenter Server をプロキシに追加します。

設定のブリック サイズの増加

プラットフォームまたはコレクタ アプライアンスのブリック サイズは、MEDIUM から LARGE、または LARGE から EXTRA-LARGE に変更して要件を満たすようにできます。

手順

- ◆ 設定に関連するステップを実行します。

オプション	説明
単一ノード プラットフォームまたは新規の独立型 OVA の場合	<ul style="list-style-type: none"> a vCenter Server にログインします。 b プラットフォーム仮想マシンをシャットダウンします。 c ディスク、RAM、合計 vCPU、および対応する仮想マシンの予約を増やし、ターゲットのブリック サイズの要件を満たすようにします。詳細については、「システムの推奨事項と要件」のページを参照してください。 d プラットフォーム仮想マシンを再起動します。
クラスタ プラットフォームの場合	<ul style="list-style-type: none"> a vCenter Server にログインします。 b プラットフォーム仮想マシンを時系列順と逆にシャットダウンします。たとえば、ノード 3 からノード 1 の順にシャットダウンします。 c ディスク、RAM、合計 vCPU、および対応する予約を増やします。詳細については、「システムの推奨事項と要件」を参照してください。 d プラットフォーム仮想マシンを時系列で再起動します。たとえば、ノード 1 からノード 3 の順に再起動します。
コレクタの場合	<ul style="list-style-type: none"> a vCenter Server にログインします。 b コレクタ仮想マシンをシャットダウンします。 c ディスク、RAM、合計 vCPU、および対応する仮想マシンの予約を増やし、ターゲットのブリック サイズの要件を満たすようにします。詳細については、「システムの推奨事項と要件」のページを参照してください。 d コレクタ仮想マシンを再起動します。

vRealize Network Insight のアップグレード

5

既存の vRealize Network Insight 環境から最新バージョンにアップグレードできます。

アップグレードを行う前に、以下の点を考慮します。

- アップグレード後、vRealize Network Insight では、アップグレード操作中にパイプラインにあったデータが処理されてユーザー インターフェイスに反映されるまで 12 ～ 24 時間かかります。
- vRealize Network Insight ではロールダウンまたは製品ダウングレードはサポートされていません。アップグレードを続行する前に、バックアップを作成する必要があります。バックアップおよびリストア プロセスの詳細については、ナレッジベースの記事 <https://kb.vmware.com/s/article/55829> を参照してください。
- クラスタ環境では、platform 1 ノードでのみアップグレード操作を実行する必要があります。
- vRealize Network Insight 5.1 にアップグレードした後、ファイアウォール ルール ID の一部が VMware Cloud on AWS 1.9 API によって返される新しい ID に変更される場合があります。フローに添付されている VMware Cloud on AWS 1.8 ファイアウォール ルールがある場合は、次のようになります。
 - すべてのアクティブなフローをアップグレードすると、正しいまたは個別の VMware Cloud on AWS 1.9 ファイアウォール ルールが適用されます。
 - ファイアウォール ルールは、バージョン 1.8 から 1.9 にアップデートする前に、アクティブでない時間が 24 時間を超えているフローに存在しないルールを参照します。

注： 集中管理によるアップグレードの実行中にアップロードの失敗やユーザー インターフェイスの障害などの問題が発生した場合は、VMware サポートにお問い合わせください。

Foundation DB への移行

クラスタ内のデータストアをまたいで構成データを分散するために、vRealize Network Insight 5.1 は PostgreSQL を Foundation DB に置き換えて構成データを格納します。これにより、vRealize Network Insight では以下のことが可能になります。

- platform 1 ノードの負荷の軽減
- 単一障害点の回避
- 回復性の向上
- パフォーマンスの向上
- クラスタ ノード全体でディスクを一貫して共有

移行プロセスは以下のように自動的に開始されます。

- すべてのサービスがシャットダウンされます
- PostgreSQL から Foundation DB へのテーブルの移行が開始されます
- platform 1 のユーザー インターフェイスに動的移行の進行状況が表示されます

PostgreSQL から Foundation DB にデータを移動するのにかかる移行時間は、ディスク速度とノード数によって異なります（ノード数が多いほど、Foundation DB の書き込みスループットが向上します）。

移行プロセスを完了するのにかかる時間は、データベースのサイズによって異なります。

セットアップ サイズ	データ サイズ	ノード数	標準的な移行時間
小	20 GB ~ 40 GB	1 ノード	1 ~ 2 時間
中	60 GB ~ 100 GB	3 ノード	7 ~ 10 時間
大 (1 クラウド セットアップ)	500GB	10 ノード クラスタ	15 ~ 20 時間
特大 (Megatron)	1 TB	10 ノード クラスタ	35 ~ 40 時間

移行は、vRealize Network Insight のアップグレード プロセスの一環として実行されることに注意してください。そのため、アップグレード時間が長くなることがあります。プロセスでは時間が画面に表示されます。

vRealize Network Insight では、他のアップグレード モードも提供されています。

この章には、次のトピックが含まれています。

- [オンライン アップグレード](#)
- [シングルクリックでのオフライン アップグレード](#)
- [CLI によるアップグレード](#)

オンライン アップグレード

使用可能な vRealize Network Insight の新しいバージョンがある場合は、通知が表示されます。

前提条件

- /tmp ディレクトリに十分な容量がない場合、アップグレード手順が失敗することがあります。以下のプラットフォームおよびコレクタ サーバのディスク容量に関する要件を満たしていることを確認します。
 - /tmp - 6 GB
 - /home - 2 GB
- 次のプラットフォーム サーバのディスク容量に関する要件を満たしていることを確認します。
 - /-6 GB (Platform1 ノードのみ)
 - /var - 40 GB
- サーバからアップグレード バンドルをダウンロードするための、500 KB/秒 の最小バンド幅要件があることを確認します。ダウンロード バンド幅が十分でない場合、[インストールとサポート] 画面でエラーが発生します。

- すべてのノードがオンラインであることを確認します。いずれかのノードが非アクティブの場合、アップグレードをトリガすることはできません。
- 仮想マシンのスナップショットを作成します。
- 移行後に次の値を確認します。
 - 仮想マシンの数
 - スナップショット数が 0 を超える仮想マシン
 - ファイアウォール ルールの数
 - セキュリティ グループの数
 - NSX ファイアウォールの数

手順

- 1 アップデートが利用可能になると、[アップデートが利用可能] というメッセージ通知が表示されます。

注：

- アップデートの通知を使用できない場合は、show-connectivity-status コマンドを実行して、vRealize Network Insight のプラットフォームとコレクタ仮想マシンの両方がポート 443 で reg.ni.vmware.com に、ポート 443 で svc.ni.vmware.com に接続されていることを確認します。この接続で http proxy が必要な場合は、set-web-proxy コマンドを使用して各仮想マシンで構成します。出力にアップグレード接続ステータスが Passed として含まれていることを確認します。
 - サポート チケットを発行し、製品ユーザー インターフェイスからサービス タグを入力します。サービス タグは [設定] - [バージョン情報] に表示されます。
 - アプライアンスにログインして show-connectivity-status コマンドを実行します。各 vRealize Network Insight プラットフォームおよびコレクタ仮想マシンのコマンド出力のスクリーンショットを提供します。
-

- 2 アップデートが利用可能 というメッセージ通知で、[ビューの詳細] をクリックして、アップデートの詳細を表示します。

vRealize Network Insight のアップグレード画面が表示されます。

- 3 [続行する前に] の手順を確認し、[続行] をクリックします。

- 4 以下を確認する事前チェックが完了するまで待機します。

- ディスク容量 (移行に必要な容量を含む)
- バージョン
- NTP 同期ステータス
- バンド幅

セットアップで、移行期間を含めたアップグレード プロセスを完了するのに必要なおおよその時間を確認できます。

- 5 [今すぐインストール] をクリックします。

- 6 アップグレード プロセスが開始されると、vRealize Network Insight Upgrade の画面にアップグレード プロセスのステータスが表示されます。

注：

- ノードが非アクティブになると、アップグレード プロセスは続行されません。ノードが再びアクティブになるまで、アップグレードは再開されません。
- platform1 がここではアップグレード サーバになります。platform1 がオフラインの場合、他のノードはアップグレードされません。
- プラットフォームがアップグレードされると、コレクタのアップグレードが並行して実行されている場合でも、通常の vRealize Network Insight 処理を再開できます。アップグレード プロセスが完全に終了するまで、[インストールとサポート] 画面に「Node Version Mismatch detected」というメッセージが表示されます。

- サービスのアップグレード後、Nginx が再起動して移行プロセスが表示されます。そのため、ユーザー インターフェイスには短時間（1 ～ 2 分）アクセスできないことがあります。
- vRealize Network Insight は、Foundation データベースへのデータの移行を開始します。[データ移行のステータス] 画面には、次の項目が表示されます。
 - 全体ステータス
 - 経過時間
 - 各テーブルのステータス
 - 移行されたレコードの数

問題があった場合は、[移行ログのエクスポート] オプションを使用して、VMware サポート チームと問題の共有ができます。
- コレクタの PostgreSQL データも、アップグレード プロセスの一環として Foundation データベースに移行されます。ただし、ユーザー インターフェイスにコレクタの移行ステータスは表示されません。

- 7 移行プロセスの完了時、確認メッセージが表示されます。

すべてのプラットフォームとコレクタ ノードがアップグレードされます。

次のステップ

- vRealize Network Insight にログインし、タスクを実行します。
- 2 ～ 3 日後に、スナップショットを削除してディスク容量を確保します。

シングルクリックでのオフライン アップグレード

vRealize Network Insight は、リリース 3.7 以降の製品のシングルクリックによるオフライン アップグレードをサポートします。

前提条件

- /tmp ディレクトリに十分な容量がない場合、アップグレード手順が失敗することがあります。以下のプラットフォームおよびコレクタ サーバのディスク容量に関する要件を満たしていることを確認します。
 - /tmp - 6 GB
 - /home - 2 GB
- 次のプラットフォーム サーバのディスク容量に関する要件を満たしていることを確認します。
 - /-12 GB (Platform1 ノードのみ)
 - /var - 40 GB

注： /tmp ディレクトリに十分な容量がない場合、バンドルのアップロードと後続のアップグレード手順が失敗することがあります。

- ユーザー インターフェイスのセッション タイムアウトを回避するには、[設定] - [システム構成] - [ユーザー セッションのタイムアウト] の順に移動し、[ユーザー セッションのタイムアウト] を 2 時間以上に増やします。セッションのタイムアウト期間を変更した後は、システムに再度ログインする必要があります。
- すべてのノードがオンラインであることを確認します。いずれかのノードが非アクティブの場合、アップグレードをトリガすることはできません。
- 仮想マシンのスナップショットを作成します。
- 移行後に次の値を確認します。
 - 仮想マシンの数
 - スナップショット数が 0 を超える仮想マシン
 - ファイアウォール ルールの数
 - セキュリティ グループの数
 - NSX ファイアウォールの数

手順

- 1 必要なアップグレード バンドル ファイルを [My VMware](#) からダウンロードし、アップデート パッケージをローカル ディスクに保存します。
- 2 ダウンロードしたバンドルの MD5SUM 値が、VMware の Web サイトで指定されている MD5SUM 値と一致することを確認します。
- 3 [インストールとサポート] 画面の [ソフトウェア バージョン] で、[ここをクリック] を選択します。

- 4 [参照] をクリックしてファイルを選択し、[アップロード] をクリックします。

アップロードが完了すると、vRealize Network Insight は「バンドル アップロードの完了」というメッセージ通知を 2 ～ 3 分以内に表示し、バンドルの処理がバックグラウンドで実行されます。

注：

- パッケージのアップロードが実行されるまで、セッションが終了していないようにする必要があります。セッションが終了した場合は、アップロード プロセスを再度開始する必要があります。
 - バンドルのアップロード後、「利用可能な更新」のメッセージ通知が表示されるまで、ページを更新しないでください。
-

- 5 「利用可能な更新」のメッセージ通知で、[詳細表示] をクリックします。

vRealize Network Insight のアップグレード画面が表示されます。

- 6 [続行する前に] の手順を確認し、[続行する] をクリックします。

- 7 以下を確認する事前チェックが完了するまで待機します。

- ディスク容量 (移行に必要な容量を含む)
- バージョン
- NTP 同期ステータス
- バンドル

- 8 [今すぐインストール] をクリックします。

セットアップでアップグレード プロセスを完了するのに必要なおおよその時間を確認できます。

- 9 アップグレード プロセスが開始されると、vRealize Network Insight Upgrade の画面にアップグレード プロセスのステータスが表示されます。

注：

- ノードが非アクティブになると、アップグレード プロセスは続行されません。ノードが再びアクティブになるまで、アップグレードは再開されません。
 - platform1 がここではアップグレード サーバになります。platform1 がオフラインの場合、他のノードはアップグレードされません。
 - プラットフォームがアップグレードされると、コレクタのアップグレードが並行して実行されている場合でも、通常の vRealize Network Insight 処理を再開できます。アップグレード プロセスが完全に終了するまで、[インストールとサポート] 画面に「Node Version Mismatch detected」というメッセージが表示されます。
-
- サービスのアップグレード後、Nginx が再起動して移行プロセスが表示されます。そのため、ユーザー インターフェイスには短時間 (1 ～ 2 分) アクセスできないことがあります。
 - vRealize Network Insight は、Foundation データベースへのデータの移行を開始します。[データ移行のステータス] 画面には、次の項目が表示されます。
 - 全体ステータス

- 経過時間
- 各テーブルのステータス
- 移行されたレコードの数

問題があった場合は、[移行ログのエクスポート] オプションを使用して、VMware サポート チームと問題の共有ができます。

- コレクタの PostgreSQL データも、アップグレード プロセスの一環として Foundation データベースに移行されます。ただし、ユーザー インターフェイスにコレクタの移行ステータスは表示されません。

10 移行プロセスの完了時、確認メッセージが表示されます。

すべてのプラットフォームとコレクタ ノードがアップグレードされます。

次のステップ

- vRealize Network Insight にログインし、タスクを実行します。
- 2 ～ 3 日後に、スナップショットを削除してディスク容量を確保します。

CLI によるアップグレード

CLI によるアップグレードは、オンライン アップグレードが機能しない場合、またはシングルクリックのオフライン アップグレードが機能しない場合にのみ検討します。コレクタ仮想マシンの前にプラットフォーム仮想マシンをアップグレードする必要があります。ただし、CLI を使用してオフライン アップグレードを開始する前に、VMware のサポートに問い合わせる必要があります。

クラスタ環境では、Platform 1 (P1) ノードからのみアップグレード操作を実行する必要があります。クラスタ内の他のプラットフォーム ノードは自動的にアップグレードします。ただし、各コレクタは個別にアップグレードする必要があります。

前提条件

- /tmp ディレクトリに十分な容量がない場合、アップグレード手順が失敗することがあります。以下のプラットフォームおよびコレクタ サーバのディスク容量に関する要件を満たしていることを確認します。
 - /tmp - 6 GB
 - /home - 2 GB
 - /var - 40 GB
- すべてのノードがオンラインであることを確認します。いずれかのノードが非アクティブの場合、アップグレードをトリガすることはできません。
- 仮想マシンのスナップショットを作成します。
- 移行後に次の値を確認します。
 - 仮想マシンの数
 - スナップショット数が 0 を超える仮想マシン
 - ファイアウォール ルールの数

- セキュリティ グループの数
- NSX ファイアウォールの数

手順

- 1 必要なアップグレード バンドル ファイルを [My VMware](#) からダウンロードします。
- 2 ダウンロードしたバンドルの MD5SUM 値が、VMware の Web サイトで指定されている MD5SUM 値と一致することを確認します。
- 3 アップグレード バンドルを、vRealize Network Insight Platform 1 仮想マシンとすべてのコレクタ仮想マシンにコピーします。

- ファイルを Linux 仮想マシンから vRealize Network Insight 仮想マシンにコピーするには、コマンド `scp <filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/` を実行します。
- ファイルを Windows 仮想マシンから vRealize Network Insight 仮想マシンにコピーするには、コマンド `pscp -scp <SOURCE_PATH>\<filename>.upgrade.bundle consoleuser@<IP_Address_vRNI_VM>:~/` を実行します。

注： <https://the.earth.li/~sgtatham/putty/latest/w64/pscp.exe> の pscp ユーティリティを使用します。

- 4 CLI で `consoleuser` を使用して vRealize Network Insight Platform 1 にログインし、次のコマンドを実行します。
 - `package-installer copy --host localhost --user consoleuser --path /home/consoleuser/<filename>.upgrade.bundle`
 - `package-installer upgrade --name <filename>.upgrade.bundle`

注： 最初にプラットフォームのアップグレードを実行してから、コレクタのアップデートを開始する必要があります。

- 5 OS アップグレードの一環として、セットアップの再起動後に `package-installer upgrade` コマンドを再度実行します。

重要： SSH セッションのタイムアウト エラーが発生した場合は、再起動がすでに行われているかどうかを確認するために、`/var/log/arkin/centralized_upgrade.log` を確認する必要があります。正常に再起動していた場合、`package-installer upgrade` コマンドを再度実行する必要があります。

- 6 CLI を介して各コレクタ ノードにログインし、プラットフォームのアップグレードで使ったのと同じコマンドを使用してアップグレードを実行します。

注： すべてのコレクタを同時にアップグレードできます。

- 7 `show-version` コマンドを使用して、アップグレードしたバージョンを確認します。

vRealize Network Insight のアンインストール

6

vRealize Network Insight は vSphere Web Client からアンインストールする必要があります。

手順

- 1 vRealize Network Insight の Web ポータルにアクセスできる場合は、次の操作を行います。
 - a vRealize Network Insight の Web ポータルにログインします。
 - b [設定] - [アカウントとデータソース] の順に移動します。
 - c すべてのデータソースを無効にして削除します。

vCenter Server のデータソースを削除すると、Distributed Switch の IPFIX 設定が削除されます（構成されている場合）。同様に、NSX Manager データソースを削除すると、NSX Flow Monitor から IPFIX 設定が削除されます。
- 2 vRealize Network Insight の Web ポータルにアクセスできない場合は、次の操作を行います。
 - a vCenter Server で Netflow (IPFIX) が有効になっている場合は、VDS/DVPG IPFIX 設定から vRealize Network Insight コレクタ IP アドレスを削除します。[vCenter Server で Netflow が有効な場合に Collector の IP アドレスを削除](#)を参照してください。
 - b NSX で IPFIX が有効になっている場合は、vRealize Network Insight コレクタ IP アドレスのフロー監視設定を削除します。[NSX で Netflow が有効な場合に Collector の IP アドレスを削除](#)を参照してください。
 - c Netflow が、vRealize Network Insight Netflow Collector に Netflow を送信するように物理スイッチで設定されている場合は、スイッチで構成を変更して NetFlow 情報の送信を停止します。
- 3 特定のファイアウォール ルールまたはルーティング ルールが vRealize Network Insight 仮想マシンで出入りするトラフィックを許可または経路指定するように作成されている場合は、それらのファイアウォール / ルーティングルールを削除します。
- 4 セキュリティ上の理由により、vRealize Network Insight のデータソースの構成に使用したアクセス認証情報はクリーンアップしてください。
- 5 すべての vRealize Network Insight コレクタおよびプラットフォーム仮想マシンをシャットダウンして削除します。

vCenter Server で Netflow が有効な場合に Collector の IP アドレスを削除

vCenter Server で Netflow (IPFIX) が有効になっている場合は、この手順を使用して仮想専用サーバ (VDS)/分散仮想ポート グループ (DVPG) の IPFIX 設定から vRealize Network Insight Collector の IP アドレスを削除します。

手順

- 1 vSphere Web Client へのログイン
- 2 [ホーム] - [ネットワーク] の順に移動します。
- 3 左側のペインで、[VDS] を選択し、[設定] - [編集] の順にクリックします。
- 4 [コレクタ IP アドレス] フィールドで、vRealize Network Insight Collector の IP アドレスの詳細を削除します。
- 5 [コレクタ ポート] フィールドで、ポートの詳細を削除します。
- 6 [OK] をクリックします。

次の手順に進む前に、約 2 分間待機する必要があります。

- 7 この VDS の DVPG を選択し、[設定] - [ポリシー] - [編集] の順にクリックします。
- 8 [Netflow] フィールドで、ドロップダウン メニューから[無効] を選択します。
- 9 設定を確認して、[適用] をクリックします。

次のステップ

IPFIX が有効になっている各 VDS およびその DVPG に対して、この手順を繰り返し実行し、vRealize Network Insight Collector の IP アドレスを削除します。

NSX で Netflow が有効な場合に Collector の IP アドレスを削除

NSX で Netflow (IPFIX) が有効になっている場合は、この手順を使用して vRealize Network Insight (vRealize Network Insight) Collector の IP フローの監視設定を削除します。

手順

- 1 vSphere Web Client へのログイン
- 2 [ホーム] - [ネットワークとセキュリティ] - [ツール] - [フローの監視] - [設定] の順にクリックします。
- 3 [グローバル フロー コレクションの状態] で、[無効] をクリックします。
- 4 フロー接続を無効にするには、[IPFIX] をクリックします。
- 5 [IPFIX] タブで、[コレクタ IP] を選択し、[削除] をクリックします。
- 6 IP アドレスが残っていない場合は、[編集] をクリックして [IPFIX 設定を有効にする] チェックボックスの選択を解除します。

- 7 [保存] をクリックします。