

vRealize Log Insight スタートガイド

2022 年 5 月 24 日

vRealize Log Insight 8.0

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 © 2022 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

vRealize Log Insight スタート ガイド 4

1 vRealize Log Insight をインストールする前に 5

vRealize Log Insight でサポートされているログ ファイルおよびアーカイブの形式 5

セキュリティ要件 6

製品の互換性 6

最小要件 7

vRealize Log Insight の展開の計画 9

vRealize Log Insight 仮想アプライアンスのサイジング 11

vRealize Log Insight と vRealize Operations Manager の統合 12

2 イベントのライフサイクル 14

イベント ライフサイクルの主な特徴 15

3 vRealize Log Insight のインストール 17

vRealize Log Insight 仮想アプライアンスのデプロイ 17

新しい vRealize Log Insight 展開の開始 20

既存の展開への参加 22

4 カスタマー エクスペリエンス向上プログラム 24

vRealize Log Insight スタート ガイド

vRealize Log Insight スタート ガイドには、vRealize Log Insight 仮想アプライアンスをサイジングしてログメッセージを受信できるようにする方法など、VMware[®] vRealize™ Log Insight™ の展開および構成に関する情報が記載されています。

本書の情報は、導入を計画またはインストールするときに使用します。本書の情報は、仮想マシン テクノロジーおよびデータセンター運用に精通した、経験の豊富な Linux および Windows システムの管理者向けに記載されています。

vRealize Log Insight をインストールする前に

1

使用環境で vRealize Log Insight を使用する前に、vRealize Log Insight 仮想アプライアンスを展開し、いくつかの基本構成を適用する必要があります。

この章には、次のトピックが含まれています。

- vRealize Log Insight でサポートされているログ ファイルおよびアーカイブの形式
- セキュリティ要件
- 製品の互換性
- 最小要件
- vRealize Log Insight の展開の計画
- vRealize Log Insight 仮想アプライアンスのサイジング
- vRealize Log Insight と vRealize Operations Manager の統合

vRealize Log Insight でサポートされているログ ファイルおよびアーカイブの形式

vRealize Log Insight を使用すると、ログ データが構造化されている場合でも、されていない場合でも分析が可能です。

vRealize Log Insight では、次のソースからデータを受け入れます。

- Syslog プロトコルを使用したログ ストリームの送信をサポートするソース。
- ログ ファイルを書き込んで、vRealize Log Insight エージェントを実行できるソース。
- REST API を介して HTTP または HTTPS によりログ データを送信できるソース。API ドキュメントは https://<vRLI_host>/rest-api の vRealize Log Insight インターフェイスから利用できます。
- vRealize Log Insight によってアーカイブされた履歴データ。

vSphere ログ パーサーを使用すると、vSphere ログ バンドルを vRealize Log Insight にインポートできます。

注： vRealize Log Insight は履歴データとリアルタイム データを同時に処理できますが、インポートされたログ ファイルを処理するための vRealize Log Insight インスタンスを個別に展開することをお勧めします。

vRealize Log Insight の管理 の「[Log Insight アーカイブの vRealize Log Insight へのインポート](#)」を参照してください。

セキュリティ要件

仮想環境を外部攻撃から確実に保護するには、特定のルールを守る必要があります。

- 必ず、信頼できるネットワークに vRealize Log Insight をインストールしてください。
- 必ず、保護された場所に vRealize Log Insight サポート バンドルを保存してください。

IT 上の意思決定者、設計者、管理者など、vRealize Log Insight のセキュリティ コンポーネントに精通する必要があるユーザーは、vRealize Log Insight の管理 のセキュリティに関するトピックをお読みください。

これらのトピックは、vRealize Log Insight のセキュリティ機能についての簡潔な参考情報を提供します。トピックの内容は、製品の外部インターフェイス、ポート、認証のメカニズム、セキュリティ機能を構成および管理するためのオプションなどです。

仮想環境の保護方法については、『VMware vSphere セキュリティ ガイド』および VMware Web サイトのセキュリティ センターを参照してください。

製品の互換性

vRealize Log Insight は Syslog プロトコルおよび HTTP を介してデータを収集します。また、vCenter Server に接続してイベント、タスク、およびアラーム データを収集したり、vRealize Operations Manager と統合して通知イベントを送信し、コンテキスト内での起動を可能にしたりできます。サポート対象製品バージョンの最新アップデートについては、『VMware vRealize Log Insight リリース ノート』を参照してください。

仮想アプライアンスの展開

vRealize Log Insight 仮想アプライアンスを展開するには、vSphere を使用する必要があります。vCenter Server との接続には、必ず vSphere Client を使用してください。vRealize Log Insight 仮想アプライアンスは、vCenter Server バージョン 5.0 以降によって管理される ESX/ESXi ホスト バージョン 5.0 以降に展開する必要があります。

Syslog フィード

vRealize Log Insight は次のポートおよびプロトコルを介して Syslog データを収集および分析します。

- 514/UDP
- 514/TCP
- 1514/TCP (SSL)

vRealize Log Insight に Syslog フィードをプッシュするように、オペレーティング システム、アプリケーション、ストレージ、ファイアウォール、ネットワーク デバイスなどの環境コンポーネントを構成する必要があります。

API フィード

vRealize Log Insight 取り込み API は次のポートおよびプロトコルを介してデータを収集します。

- 9000/TCP
- 9543/TCP (SSL)

vSphere の統合

1 つ以上の vCenter Server インスタンスで発生したタスク、イベント、およびアラームのデータをプルするように、vRealize Log Insight を構成できます。vRealize Log Insight は vSphere API を使用して vCenter Server システムに接続し、データを収集します。

Syslog データを vRealize Log Insight に転送するように、ESXi ホストを構成できます。

vCenter Server および ESXi の特定のバージョンとの互換性情報については、[VMware 製品の相互運用性マトリクス](#)を参照してください。

vSphere 環境への接続の詳細については、「[vRealize Log Insight の vSphere 環境への接続](#)」を参照してください。

vRealize Operations Manager の統合

vRealize Log Insight および vRealize Operations Manager vApp または Installable は 2 つの独立した方法で統合できます。

vCenter Operations Manager のサポートされるすべてのバージョンは、通知およびコンテキストでの起動をサポートします。

- vRealize Log Insight は vRealize Operations Manager に通知イベントを送信できます。
[vRealize Operations Manager に通知イベントを送信する vRealize Log Insight の構成](#)を参照してください。
- vRealize Operations Manager のコンテキストの起動メニューに vRealize Log Insight に関連するアクションが表示されます。
[vRealize Operations Manager での vRealize Log Insight のコンテキストにおける起動の有効化](#)を参照してください。

最小要件

VMware は vRealize Log Insight を OVA ファイル形式の仮想アプライアンスとして配布しています。仮想アプライアンスを正常に実行するには、さまざまなリソースおよびアプリケーションが使用可能である必要があります。最新の要件に関する情報は、最新のリリース ノートで確認してください。

仮想ハードウェア

vRealize Log Insight 仮想アプライアンスの展開の際に、環境の取り込み要件に応じて事前に設定された構成サイズを選択できます。これはコンピューティングとディスク リソースのサイズの組み合わせとして認定されていますが、後からリソースを追加することができます。次の表に示す小規模構成は、サポート要件を満たした状態で最小リソースを使用します。極小構成も利用できますが、これはデモにのみ適しています。

取り込み要件に基づく完全なリソース要件については、[vRealize Log Insight 仮想アプライアンスのサイジング](#)を参照してください。

表 1-1. 小規模構成のための事前に設定された値

| リソース | 最小要件 |
|---------|--------|
| メモリ | 8 GB |
| vCPU | 4 |
| ストレージ領域 | 530 GB |

サポート対象ブラウザ

vRealize Log Insight Web ユーザー インターフェイスへの接続には、次のブラウザのいずれかを使用できます。これより新しいバージョンのブラウザも vRealize Log Insight で使用できますが、まだ検証されていません。

重要： ブラウザでは Cookie を有効にする必要があります。

- Mozilla Firefox 45.0 以降
- Google Chrome 51.0 以降
- Safari 9.1 以降
- Internet Explorer 11.0 以降

注：

- Internet Explorer ドキュメント モードは、[標準モード] に設定する必要があります。その他のモードはサポートされません。
- [ブラウザ モード：]互換表示はサポートされていません。
- vRealize Log Insight Web クライアントで Internet Explorer を使用するには、Windows のローカル ストレージの整合性レベルを「低」に設定する必要があります。

アカウントのパスワード

| タイプ | 要件 |
|------------|---|
| root | <p>OVA の展開時に root のパスワードを変更したり、ゲストのカスタマイズを使用したりしていなければ、vRealize Log Insight 仮想アプライアンスの root ユーザーのデフォルトの認証情報は root/blank です。vRealize Log Insight 仮想アプライアンス コンソールの初回アクセス時に、root アカウントのパスワードを変更するように求められます。</p> <p>注： root パスワードを設定するまで SSH は無効です。</p> |
| ユーザー アカウント | <p>vRealize Log Insight 3.3 以降で作成したユーザー アカウントには強力なパスワードが必要です。パスワードは 8 文字以上で、大文字、小文字、数字、特殊文字をそれぞれ 1 文字以上含む必要があります。</p> |

統合の要件

| 製品 | 要件 |
|-----------------------------|---|
| vCenter Server | vCenter Server からイベント、タスク、アラームのデータを取得するには、その vCenter Server にユーザー認証情報を一提供する必要があります。vRealize Log Insight を vCenter Server に登録または登録解除するために必要な最小ロールは、[読み取り専用]です。ロールは、vCenter Server レベルで設定し、子オブジェクトに伝達する必要があります。vCenter Server が管理する ESXi ホストを構成するには、vRealize Log Insight に追加の権限が必要です。 |
| vSphere ESXi | vRealize Log Insight との SSL 接続を確立するには、vSphere ESXi 6.0 Update 1 以降が必要です。 |
| vRealize Operations Manager | vRealize Operations Manager インスタンスで通知イベントとコンテキストでの起動機能を有効にするには、その vRealize Operations Manager インスタンスのユーザー認証情報を提供する必要があります。 |

ネットワーク ポートの要件

次のネットワーク ポートが外部アクセス可能である必要があります。

| ポート | プロトコル |
|-----------------|-------------------------------------|
| 22/TCP | SSH |
| 80/TCP | HTTP |
| 443/TCP | HTTPS |
| 514/UDP、514/TCP | Syslog |
| 1514/TCP | SSL 経由での Syslog 取り込みのみ |
| 9000/TCP | vRealize Log Insight 取り込み API |
| 9543/TCP | vRealize Log Insight 取り込み API (SSL) |

vRealize Log Insight の展開の計画

単一ノード、単一クラスタ、またはフォワーダを含むクラスタと共に vRealize Log Insight を展開できます。

注： 外部のロード バランサは、vRealize Log Insight クラスタを含め、vRealize Log Insight と一緒に使用することはできません。

vRealize Suite Lifecycle Manager によるインストール

vRealize Suite Lifecycle Manager は、スイート製品のインストール、構成、アップグレード、パッチ、構成管理、ドリフト修正、および健全性を自動化します。vRealize Log Insight によるインストールの代わりに、vRealize Suite Lifecycle Manager を介して vRealize Log Insight をインストールできます。vRealize Suite Lifecycle Manager 1.2 以降および vRealize Log Insight 4.5.1 以降を使用している必要があります。詳細については、[vRealize Suite Lifecycle Manager ドキュメント](#) を参照してください。

単一ノード

基本的な vRealize Log Insight 構成には単一ノードが含まれています。ログ ソースはアプリケーション、OS のログ、仮想マシンのログ、ホスト、vCenter Server、仮想/物理スイッチまたはルーター、ストレージ ハードウェアなどです。ログ ストリームは syslog (UDP、TCP、TCP+SSL) または CFAPI (HTTP または HTTPS を介した vRealize Log Insight ネイティブの取り込みプロトコル) を使用して、アプリケーションから直接ノードに転送されるか、syslog コンセントレータやソースにインストールされた vRealize Log Insight Agent から vRealize Log Insight ノードに転送されます。

単一ノード環境の場合、vRealize Log Insight 統合ロード バランサ (ILB) を使用し、ILB にクエリと取り込みトラフィックを送信することがベスト プラクティスです。これにより、オーバーヘッドは発生しませんし、ノードを追加して後で環境にクラスタを作成する場合に設定を簡素化できます。

ベスト プラクティスとして、本番環境では単一ノードを使用しないでください。

クラスタ

本番環境では通常、クラスタを使用する必要があります。クラスタは次の要件を満たす必要があります。

- クラスタ内のノードはすべて同じサイズで、同じデータセンター内にあります。
- クラスタで使用される ILB では、同じ L2 ネットワーク内にノードがある必要があります。
- vRealize Log Insight 仮想マシンは、VMware NSX Distributed Firewall 保護から除外する必要があります。

これは、クラスタの仮想 IP アドレスが、ロード バランシングのために Linux Virtual Server in Direct Server Return Mode (LVS-DR) を使用するためです。Direct Server Return は、すべての応答トラフィックを 1 つのクラスタ メンバーを使用してルーティングすることよりも効率的です。ただし、これは NSX Distributed Firewall にブロックされる偽装トラフィックにも似ています。

クラスタのサイジング

vRealize Log Insight の単一クラスタ構成には 3 台から 12 台のノードを含めることができ、ILB が使用されます。クラスタが正常に動作するには、最低 3 台の健全なノードが必要です。

本番環境では、そのノードが少なくとも中サイズであることが必要です。アラートを含む、多数の同時実行クエリを操作することが予想される場合は、大規模ノードの使用を検討してください。サイジングの詳細については、[vRealize Log Insight 仮想アプライアンスのサイジング](#)を参照してください。

vRealize Log Insight クラスタにおけるノードの最小数は 3 台ですが、ノードに障害が発生すると、健全なノードが 3 台に満たないクラスタは完全に機能しません。また、クラスタ内の健全なノードの数は、クラスタ ノードの合計の半分よりも多くなければなりません。たとえば、6 台のノードのクラスタがあり、3 台のノードが使用できなくなった場合、機能していないノードをクラスタから削除するまで、クラスタは完全に機能しません。クラスタ ノードを削除して再導入することはできません。

フォワーダを含むクラスタ

フォワーダを含む vRealize Log Insight クラスタの構成には、ILB を利用する 3 台から 12 台のノードからなるメイン インデックス、ストレージ、およびクエリ用のクラスタが含まれています。単一クラスタの場合と同様に、1 つのログ メッセージが、メイン クラスタ内の 1 つの場所のみに存在します。

設計を拡張するには、リモート サイトまたはリモート クラスタに複数のフォワーダ クラスタを追加します。各フォワーダ クラスタは、すべてのログ メッセージをメイン クラスタに転送するように設定されています。ユーザーはメイン クラスタに接続し、CFAPI を利用して転送パス上で圧縮を行い、復元力を高めます。トップオブブラックとして構成されたフォワーダ クラスタを構成し、ローカル保持能力を強化することができます。

冗長性のためのクロスフォワーディング

この vRealize Log Insight 展開シナリオには、拡張およびミラーリングされたフォワーダとクラスタが含まれます。2 つのメイン クラスタがインデックス作成、ストレージ、およびクエリに使用されます。各データセンターに 1 つのメイン クラスタがあります。それぞれが、専用のフォワーダ クラスタのペアを持つフロント エンドになります。すべてのトップオブブラック集計のすべてのログ ソースがフォワーダ クラスタで集中的に処理されます。両方の保持クラスタで同じログを独立してクエリすることができます。

vRealize Log Insight 統合ロード バランサ

クラスタ内のノード全体にトラフィックを適切に分散し、管理オーバーヘッドを最小限に抑えるには、すべての展開で統合ロード バランサ (ILB) を使用します。一部の vRealize Log Insight ノードが使用できなくなっても、受信する取り込みトラフィックが確実に受け入れられます。

vRealize Log Insight 仮想アプライアンスのサイジング

小規模構成の場合、vRealize Log Insight 仮想アプライアンスはデフォルトで事前設定値を使用します。

スタンドアロンの展開

展開中にログを収集する環境のニーズに合わせてアプライアンスの設定を変更することができます。

vRealize Log Insight は、環境の取り込み要件に応じて選択できるプリセットされた仮想マシン サイズを提供します。これらはコンピューティングとディスク リソースのサイズの組み合わせとして認定されていますが、後からリソースを追加することができます。小規模構成では、サポート要件を満たした状態で最小リソースを使用します。極小の構成はデモ環境にのみ適しています。

| プリセットされたサイズ | ログ取り込み速度 | 仮想 CPU | メモリ | IOPS | Syslog 接続数 (アクティブな TCP 接続) | |
|-------------|----------|--------|------|------|----------------------------|--------------|
| | | | | | | 1 秒あたりのイベント数 |
| [極小] | 6 GB/日 | 2 | 4 GB | 75 | 20 | 400 |
| [小] | 30 GB/日 | 4 | 8 GB | 500 | 100 | 2000 |
| [中] | 75 GB/日 | 8 | 16GB | 1000 | 250 | 5000 |
| [大] | 225 GB/日 | 16 | 32GB | 1500 | 750 | 15,000 |

Syslog アグリゲータを使用すると、vRealize Log Insight にイベントを送信する Syslog 接続の数を増やすことができます。ただし、1 秒間のイベントの最大数は固定されていて、Syslog アグリゲータを使用しても影響はありません。vRealize Log Insight インスタンスを Syslog アグリゲータとして使用することはできません。

サイジングは次の前提条件に基づいて行われます。

- 各仮想 CPU は 2 GHz 以上です。

- 各 ESXi ホストは 1 秒あたり最大 10 個のメッセージを送信します。平均メッセージ サイズは 170 バイト/メッセージで、これは 1 台のホストあたり 150 MB/日に相当します。

注： 大規模インストール環境では、vRealize Log Insight 仮想マシンの仮想ハードウェア バージョンをアップグレードする必要があります。vRealize Log Insight は仮想ハードウェア バージョン 7 以降をサポートしています。仮想ハードウェア バージョン 7 は最大 8 個の仮想 CPU をサポートできます。したがって、16 個の仮想 CPU をプロビジョニングする場合には、ESXi 5.x を仮想ハードウェア バージョン 8 以降にアップグレードする必要があります。仮想ハードウェアをアップグレードするには、vSphere Client を使用します。仮想ハードウェアを最新バージョンにアップグレードする場合は、VMware ナレッジ ベースの記事「[Upgrading a virtual machine to the latest hardware version](#)（最新ハードウェア バージョンへの仮想マシンのアップグレード）(1010675)」を参照してください。

クラスタの展開

vRealize Log Insight クラスタのプライマリ ノードおよびワーカー ノードには、中規模または大規模構成を使用してください。ノード数が増えると、1 秒間のイベント数も直線的に増えます。たとえば、3 台から 12 台のノードのクラスタ（クラスタには 3 台以上のノードが必要）では、12 ノード クラスタのインターネットは 1 秒あたり 180,000 イベント (EPS)、すなわち 1 日あたり 2.7 TB のイベントになります。

メモリ サイズの削減

ラップトップで [極小] バージョンのアプライアンスを使用するときに、十分なメモリが搭載されていない場合には、メモリ サイズを 2 GB に低減できます。

vRealize Log Insight のサイジング計算

ネットワークやストレージの使用率や vRealize Log Insight のサイジングに役立つツールがあります。この計算ツールはガイド目的で提供されています。多くの環境の入力はサイトに固有であるため、一部の領域では予測値を使用する場合もあります。<https://www.vmware.com/go/loginsight/calculator> を参照してください。

注： フォワードが、正規表現（たとえば `text=~"Deleting the machine"`）を含む複雑な条件または複数の条件を持つテキスト フィールドに対して定義されていると、vRealize Log Insight の全体的なパフォーマンスが低下する可能性があります。このような場合、特にクラスタの全体的な負荷が大きい場合、パフォーマンスが低下し、クラスタの各ノードにディスク ブロックが累積することがあります。

vRealize Log Insight と vRealize Operations Manager の統合

vRealize Log Insight と vRealize Operations Manager を統合するには、両方の製品で構成を行う必要があります。

手順

- 1 vRealize Log Insight Management Pack を vRealize Operations Manager にインストールします。

vRealize Log Insight Management Pack は、これら 2 つの製品の間でコンテキストでの起動機能を使用するために必要です。vRealize Log Insight Management Pack は、vRealize Operations Manager のダウンロード ファイルと一緒に、または VMware Solution Exchange の Web サイトから入手できます。

- 2 vRealize Log Insight を vRealize Operations Manager と接続するように構成します。
- 3 vRealize Log Insight アラートを vRealize Operations Manager に情報を転送するように構成します。
『vRealize Log Insight の管理』の「[vRealize Operations Manager に通知イベントを送信するための vRealize Log Insight の構成](#)」を参照してください。
- 4 vRealize Operations のコンテキストでの起動を有効にして、vRealize Log Insight のログを照会します。
『vRealize Log Insight の管理』の「[vRealize Operations Manager での vRealize Log Insight のコンテキストにおける起動の有効化](#)」を参照してください。

イベントのライフサイクル

2

vRealize Log Insight がメッセージとイベントをどのように処理するかを理解することは、vRealize Log Insight を効果的に使用するために重要です。

ログ メッセージまたはイベントのライフ サイクルには、読み取り、解析、取り込み、インデックス作成、警告、クエリ適用、アーカイブ、削除などの複数の段階があります。

イベントとメッセージは次の段階を通じて移行します。

- 1 イベントがデバイス上で生成されます (vRealize Log Insight の外部)。
- 2 以下のいずれかの方法で選択され vRealize Log Insight に送信されます。
 - 取り込み API または syslog を使用する vRealize Log Insight エージェントによって
 - Syslog を使用する、rsyslog、syslog-ng、または log4j などのサードパーティ エージェントによって
 - 取り込み API へのカスタムの書き込みによって (log4j appender など)
 - syslog へのカスタムの書き込みによって (log4j appender など)
- 3 vRealize Log Insight がイベントを受信します。
 - 統合ロード バランサ (ILB) を使用している場合は、イベントはイベントの処理を行う単一ノードに送信されます。
 - イベントが拒否される場合、クライアントは UDP 削除、プロトコルが設定された TCP、またはディスク バックアップされたキューを備えた CFAPI でイベント拒否を処理します。
 - イベントが受け付けられると、クライアントに通知されます。
- 4 イベントは vRealize Log Insight 取り込みパイプラインを通して渡され、そこから次の手順が発生します。
 - キーワード インデックスが作成または更新される。インデックスがローカル ディスク上に専用形式で格納される。
 - クラスタ イベントにマシン ラーニングが適用される。
 - イベントは、ローカル ディスク上のバケット内に、圧縮された専用形式で格納される。
- 5 イベントがクエリされる。
 - キーワードと glob のクエリは、キーワード インデックスに対して照会される。
 - 正規表現は、圧縮されたイベントに対して照会される。

- 6 イベントはバケットに移動してアーカイブされる。
 - バケットはシールされ、0.5 GB に達したときにアーカイブされる。
- 7 イベントが削除される。
 - バケットは FIFO の順で削除される。

詳細情報

詳細については、VMware Technical Publications のビデオをご覧ください。



vRealize Log Insight のログ イベントのライフ サイクル。

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_horp849x/uiConfId/50138843/)

この章には、次のトピックが含まれています。

- イベント ライフサイクルの主な特徴

イベント ライフサイクルの主な特徴

イベントが古くなると、イベントのライフサイクルではイベントの格納と管理に関して認識すべき主な特徴があります。

イベントの格納

各イベントは、単一のオンディスク バケットに格納されます。バケットを処理する場合は、次の動作と特性に注意してください。

- バケットは 0.5 GB の最大サイズに到達する場合があります。バケットが 0.5 GB に達すると、バケットはシールされ、アーカイブのためにキューに入れられます。封印されたバケットがアーカイブされると、そのバケットはアーカイブ済みとしてマーキングされます。1 つのイベントがローカルとアーカイブ内で同時に保持される場合があります。
- バケットは vRealize Log Insight ノード間でレプリケートされません。ノードを失うと、そのノード上のデータが失われます。
- すべてのバケットは /storage/core パーティションに格納されます。
- /storage/core パーティションの利用可能な容量が 3% 未満になると、vRealize Log Insight は古いバケットを削除します。削除は FIFO モデルに従います。

注： /storage/core パーティションが容量の限度に近くなるのは、予期される通常の状態です。このパーティションは vRealize Log Insight によって管理されているため、使用量が 100% に到達することはないはずです。ただし、古いバケットの削除を妨げる可能性があるため、そのパーティションにはデータを保存しないでください。

イベント管理

製品をセットアップして構成する場合、vRealize Log Insight イベントの次の特性と動作、およびイベント管理を理解しておく役に立ちます。

- イベントがローカルで削除されると、コマンドライン インターフェイスを使用してアーカイブからインポートしない限り照会できなくなります。
- マシン ラーニング クラスタ用のすべてのイベントが vRealize Log Insight から削除されると、そのクラスタは削除されます。
- vRealize Log Insight は、クラスタ内のノード全体で、すべての受信イベントを均等に再分散します。たとえば、ノードが明示的にイベントに送信された場合でも、そのイベントを受け取るべきノードではない場合があります。
- イベントのメタデータは、データベース内ではなく、単一の vRealize Log Insight ノードに専用の形式で格納されます。
- イベントはノードのローカルに存在することも、アーカイブ上に存在することもできます。

vRealize Log Insight のインストール

3

vRealize Log Insight は、vSphere 環境に展開する仮想アプライアンスとして提供されます。

vRealize Log Insight 仮想アプライアンスのサイジングを確認してから [vRealize Log Insight 仮想アプライアンスのデプロイ](#)に進んでください。単一ノードの展開の場合も、クラスタ ノードの展開の場合も、このセクションで説明する標準の OVF 展開手順に従ってください。

注: vRealize Log Insight 4.5.1 以降のリリースをインストールするには、vRealize Suite Lifecycle Manager 1.2 以降を使用します。詳細については、[vRealize Suite ドキュメント](#)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。

- [vRealize Log Insight 仮想アプライアンスのデプロイ](#)
- [新しい vRealize Log Insight 展開の開始](#)
- [既存の展開への参加](#)

vRealize Log Insight 仮想アプライアンスのデプロイ

vRealize Log Insight 仮想アプライアンスをダウンロードします。VMware は vRealize Log Insight 仮想アプライアンスを .ova ファイルとして配布しています。vSphere Client を使用して vRealize Log Insight 仮想アプライアンスを展開します。

前提条件

- vRealize Log Insight 仮想アプライアンスの .ova ファイルのコピーがあることを確認します。
- OVF テンプレートをインベントリにデプロイする権限を有することを確認します。
- 使用環境に vRealize Log Insight 仮想アプライアンスの最小要件を満たすのに必要なリソースがあることを確認します。「[最小要件](#)」を参照してください。
- 仮想アプライアンスのサイジングに関する推奨事項を読み、理解していることを確認してください。「[Log Insight 仮想アプライアンスのサイジング](#)」を参照してください。

手順

- 1 vSphere Client で、[ファイル] - [OVF テンプレートの展開] を選択します。
- 2 [OVF テンプレートの展開] ウィザードでプロンプトに従います。

- 3 [構成の選択] ページで、ログを収集する環境の規模に基づいて vRealize Log Insight 仮想アプライアンスのサイズを設定します。

本番環境の最小要件は [小] です。

vRealize Log Insight は、環境の取り込み要件に応じて選択できるプリセットされた仮想マシン サイズを提供します。これらはコンピューティングとディスク リソースのサイズの組み合わせとして認定されていますが、後からリソースを追加することができます。小規模構成では、サポート要件を満たした状態で最小リソースを使用します。極小の構成はデモ環境にのみ適しています。

| プリセットされたサイズ | ログ取り込み速度 | 仮想 CPU | メモリ | IOPS | Syslog 接続数 (アクティブな TCP 接続) | | 1 秒あたりのイベント数 |
|-------------|----------|--------|------|------|----------------------------|--|--------------|
| | | | | | | | |
| [極小] | 6 GB/日 | 2 | 4 GB | 75 | 20 | | 400 |
| [小] | 30 GB/日 | 4 | 8 GB | 500 | 100 | | 2000 |
| [中] | 75 GB/日 | 8 | 16GB | 1000 | 250 | | 5000 |
| [大] | 225 GB/日 | 16 | 32GB | 1500 | 750 | | 15,000 |

Syslog アグリゲータを使用すると、vRealize Log Insight にイベントを送信する Syslog 接続の数を増やすことができます。ただし、1 秒間のイベントの最大数は固定されていて、Syslog アグリゲータを使用しても影響はありません。vRealize Log Insight インスタンスを Syslog アグリゲータとして使用することはできません。

注： [大] を選択した場合は、展開後に vRealize Log Insight 仮想マシンの仮想ハードウェアをアップグレードする必要があります。

- 4 [ストレージの選択] ページで、ディスクのフォーマットを選択します。

- [シック プロビジョニング (Lazy Zeroed)] を選択すると、デフォルトのシック フォーマットで仮想ディスクが作成されます。仮想ディスクの作成時に、仮想ディスクに必要な容量が割り当てられます。物理デバイスに残っているデータは、仮想ディスクの作成中には消去されませんが、後で仮想アプライアンスから初めて書き込むときにオンデマンドで消去されます。
- [シック プロビジョニング (Eager Zeroed)] を選択すると、フォールトトレランスなどのクラスタリング機能をサポートする、シック仮想ディスクが作成されます。仮想ディスクに必要な容量は、作成時に割り当てられます。フラットフォーマットの場合とは異なり、物理デバイスに残っているデータは、仮想ディスクの作成時に消去されます。他のタイプのディスクに比べて、このフォーマットでディスクを作成する場合は非常に長い時間がかかることがあります。

重要： vRealize Log Insight 仮想アプライアンスのパフォーマンスおよび操作性を改善するために、可能な場合は常に仮想アプライアンスをシック プロビジョニング (Eager Zeroed) のディスクで展開します。

- [シン プロビジョニング] を選択すると、シン フォーマットでディスクが作成されます。保存されるデータの量が増えると、ディスクが拡張されます。ストレージ デバイスでディスクのシック プロビジョニングがサポートされていない場合、または vRealize Log Insight 仮想アプライアンスの未使用のディスク容量を節約する場合は、仮想アプライアンスをシン プロビジョニングのディスクで展開します。

注： vRealize Log Insight 仮想アプライアンスのディスク圧縮はサポートされていません。ディスクを圧縮すると、データの破損や消失が起きる可能性があります。

- 5 (オプション) [ネットワークの選択] ページで vRealize Log Insight 仮想アプライアンスのネットワーク パラメータを設定します。IPv4 または IPv6 プロトコルを選択できます。

IP アドレス、DNS サーバ、ゲートウェイ情報などのネットワーク設定を指定しない場合、vRealize Log Insight は DHCP を使用してこれらの設定を行います。

注意： ドメイン ネーム サーバを 3 つ以上指定しないでください。ドメイン ネーム サーバを 3 つ以上指定すると、構成されたすべてのドメイン ネーム サーバが vRealize Log Insight 仮想アプライアンスで無視されます。

コンマで区切られたリストを使用してドメイン名サーバを指定します。

- 6 (オプション) [テンプレートのカスタマイズ] ページで、DHCP を使用していない場合はネットワークのプロパティを設定します。

[アプリケーション] で、仮想マシンをデュアル スタック ネットワークで実行する場合は、[IPv6 アドレスを優先] チェック ボックスを選択します。

注意： IPv6 がネットワークでサポートされている場合でも、ピュア IPv4 を使用する場合は、[IPv6 アドレスを優先] チェック ボックスを選択しないでください。このチェック ボックスは、ネットワークで IPv6 のデュアル スタックまたはピュア スタックがサポートされている場合にのみ、選択します。

- 7 (オプション) [テンプレートのカスタマイズ] ページで [その他のプロパティ] を選択し、vRealize Log Insight 仮想アプライアンスの root パスワードを設定します。

SSH では root パスワードは必須です。このパスワードは VMware リモート コンソールで設定することもできます。

- 8 プロンプトの指示に従って、展開を完了します。

仮想アプライアンスの展開の詳細については、「vApps および仮想アプライアンスの展開に関するユーザー ガイド」を参照してください。

仮想アプライアンスをパワーオンすると、初期化プロセスが開始します。初期化プロセスが完了するまで数分かかります。プロセスが終了すると、仮想アプライアンスが再起動します。

- 9 [コンソール] タブに移動し、vRealize Log Insight 仮想アプライアンスの IP アドレスを確認します。

| IP アドレスのプリフィックス | 説明 |
|-----------------|---|
| https:// | 仮想アプライアンスの DHCP 構成が正常です。 |
| http:// | 仮想アプライアンスの DHCP 構成に失敗しました。 a vRealize Log Insight 仮想アプライアンスをパワーオフします。 b 仮想アプライアンスを右クリックし、[設定の編集] を選択します。 c 仮想アプライアンスの固定 IP アドレスを設定します。 |

次のステップ

- スタンドアロンの vRealize Log Insight 展開を構成する場合は、[新しい Log Insight 展開の構成](#)を参照してください。

vRealize Log Insight Web インターフェイスは `https://log-insight-host/` にあります。`log-insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

新しい vRealize Log Insight 展開の開始

仮想アプライアンスを展開した後、またはクラスタからワーカー ノードを取り外した後に、vRealize Log Insight Web インターフェイスに初めてアクセスする場合は、初期構成手順を実行する必要があります。

初期構成中に変更したすべての設定も、管理 Web ユーザー インターフェイスで 사용할 ことができます。

カスタマー エクスペリエンス向上プログラムに参加している場合に vRealize Log Insight が収集して VMware に送信する可能性のあるトレース データの詳細については、[4 章 カスタマー エクスペリエンス向上プログラム](#)を参照してください。

前提条件

- vSphere Client の vRealize Log Insight 仮想アプライアンスの IP アドレスを書き留めます。IP アドレスの検索方法の詳細については、[vRealize Log Insight 仮想アプライアンスのデプロイ](#)を参照してください。
- 使用しているブラウザがサポートされているかを確認するには、[最小要件](#)を参照してください。
- 有効なライセンス キーが手元にあることを確認してください。<https://my.vmware.com/> の My VMware ™ で、アカウントを通じて評価用ライセンス キーまたは永続的ライセンス キーを要求できます。
- ローカル、vCenter Server、または Active Directory の認証情報を使用して vRealize Log Insight を vRealize Operations Manager に統合する場合、これらのユーザーが vRealize Operations Manager カスタム ユーザー インターフェイスにインポートされていることを確認します。LDAP の構成方法については、[vRealize Operations Manager ドキュメント](#)を参照してください。

手順

- 1 サポート対象ブラウザを使用して、vRealize Log Insight の Web ユーザー インターフェイスに移動します。

URL 形式は `https://log_insight-host/` です。`log_insight-host` は vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名です。

初期構成ウィザードが開きます。

- 2 [新しい展開の開始] をクリックします。
- 3 管理者ユーザー用のパスワードを設定して、[保存して続行] をクリックします。
オプションとして、管理者ユーザーのメール アドレスを指定することもできます。
- 4 ライセンス キーを入力し、[ライセンス キーの追加] をクリックして、[保存して続行] をクリックします。
- 5 [一般的な構成] ページに、vRealize Log Insight からシステム通知を受信するメール アドレスを入力します。
- 6 Webhook を使用して vRealize Operations Manager またはサードパーティのアプリケーションに通知を送信する場合、[HTTP Post システム通知の送信先] テキスト ボックスにスペースで区切った URL のリストを入力します。
- 7 (オプション) カスタマー エクスペリエンス向上プログラムを終了するには、[VMware カスタマー エクスペリエンス向上プログラムに参加] オプションを選択解除します。[保存して続行] をクリックします。
- 8 [時間の構成] ページで vRealize Log Insight 仮想アプライアンスの時間の同期方法を設定し、[テスト] をクリックします。

| オプション | 説明 |
|----------------|---|
| [NTP サーバ (推奨)] | デフォルトの場合、vRealize Log Insight はパブリック NTP サーバと同期するように構成されています。ファイアウォール設定のために外部 NTP サーバにアクセスできない場合は、組織の内部 NTP サーバを使用できます。 複数の NTP サーバを区切るには、カンマを使用します。 |
| [ESX/ESXi ホスト] | 使用できる NTP サーバがない場合は、vRealize Log Insight 仮想アプライアンスの展開先の ESXi ホストと時間を同期することができます。 |

- 9 [保存して続行] をクリックします。
- 10 (オプション) 送信アラートおよびシステム通知メールを有効にするには、SMTP サーバのプロパティを指定します。
SMTP の構成が正しいことを確認するには、有効なメール アドレスを入力し、[テスト] をクリックします。
vRealize Log Insight は指定されたアドレスにテスト メールを送信します。
- 11 (オプション) カスタム SSL 証明書を提供するには、証明書ファイルを PEM 形式でクラスタにアップロードします。また、既存の証明書の詳細を表示することもできます。
システムにより、証明書がクラスタのすべてのノードのトラストストアに追加され、後で使用するために保存されます。
カスタム SSL 証明書の前提条件の詳細については、[カスタム SSL 証明書のインストール](#)を参照してください。
- 12 [保存して続行] をクリックします。

結果

vRealize Log Insight プロセスが再起動すると、vRealize Log Insight の [ダッシュボード] タブにリダイレクトされます。

次のステップ

- [管理] タブに移動します。[vSphere 統合] ページを使用して、vCenter Server インスタンスからタスク、イベント、およびアラートをプルするように vRealize Log Insight を構成し、vRealize Log Insight に Syslog フィードを送信するように ESXi ホストを構成します。
- vRealize Log Insight に永続的ライセンスを割り当てます。『vRealize Log Insight の管理』の「[Log Insight への永続的ライセンスの割り当て](#)」を参照してください。
- コンテキストでの起動を有効にするには、vRealize Operations Manager の vRealize Log Insight アダプタを構成します。『vRealize Operations Manager 構成ガイド』の「vRealize Operations Manager を使用した vRealize Log Insight の構成」を参照してください。
- vRealize Log Insight Windows エージェントをインストールして、Windows イベント チャネル、Windows ディレクトリ、およびフラット テキスト ログ ファイルからイベントを収集します。『vRealize Log Insight エージェントの操作』の [Windows エージェントのインストール](#) を参照してください。

既存の展開への参加

スタンドアロン vRealize Log Insight ノードを展開して設定した後に、新しい vRealize Log Insight インスタンスを展開し、それを既存ノードに追加して、vRealize Log Insight クラスタを形成することができます。

vRealize Log Insight は複数の仮想アプライアンス インスタンスをクラスタ化してスケール アウトできます。クラスタ化により、取り込み時のスループットを線形的にスケールアップし、クエリのパフォーマンスを高めて、取り込み時に高可用性を実現することができます。クラスタ モードの場合、vRealize Log Insight はプライマリ ノードとワーカー ノードを提供します。プライマリ ノードとワーカー ノードはいずれもデータのサブセットを処理します。プライマリ ノードはデータのあらゆるサブセットにクエリを実行して、結果を集計します。サイトのニーズをサポートするために、より多くのノードが必要になる場合があります。1つのクラスタ内で 3 台から 12 台のノードを使用できます。つまり、完全に機能するクラスタには 3 台以上の健全なノードが必要です。大規模なクラスタのノードの大多数は健全である必要があります。たとえば、6 ノード クラスタの 3 台のノードに障害が発生した場合、障害が発生したノードが削除されるまで、どのノードも完全に機能しません。

前提条件

- vSphere Client でワーカー vRealize Log Insight 仮想アプライアンスの IP アドレスを書き留めます。
- プライマリ vRealize Log Insight 仮想アプライアンスの IP アドレスまたはホスト名が判明していることを確認します。
- プライマリ vRealize Log Insight 仮想アプライアンスの管理者アカウントがあることを確認します。
- vRealize Log Insight プライマリおよびワーカー ノードのバージョンが同期されていることを確認します。古いバージョンの vRealize Log Insight ワーカーを新しいバージョンの vRealize Log Insight プライマリ ノードに追加しないでください。
- vRealize Log Insight 仮想アプライアンス上の時刻を NTP サーバと同期する必要があります。「[Log Insight 仮想アプライアンスの時刻の同期](#)」を参照してください。
- サポート対象のブラウザ バージョンの詳細については、[vRealize Log Insight リリース ノート](#) を参照してください。

手順

- 1 サポート対象ブラウザを使用して、vRealize Log Insight ワーカーの Web ユーザー インターフェイスに移動します。

URL 形式は `https://log_insight-host/` です。*log_insight-host* は vRealize Log Insight ワーカー仮想アプライアンスの IP アドレスまたはホスト名です。

初期構成ウィザードが開きます。

- 2 [既存の展開への参加] をクリックします。
- 3 vRealize Log Insight プライマリの IP アドレスまたはホスト名を入力し、[移動] をクリックします。
ワーカーは、既存の環境に参加するためのリクエストを vRealize Log Insight プライマリ ノードに送信します。
- 4 [ここをクリックして、[クラスタ管理] ページを表示します] をクリックします。
- 5 管理者としてログインします。
クラスタ ページがロードされます。
- 6 [許可] をクリックします。
ワーカー ノードが既存の展開に参加し、vRealize Log Insight がクラスタでの動作を開始します。

次のステップ

- 必要に応じて、さらにワーカー ノードを追加します。クラスタには 3 台以上のノードが必要です。

カスタマー エクスペリエンス向上プログラム

4

この製品は、VMware のカスタマー エクスペリエンス向上プログラム (CEIP) に参加しています。

CEIP を通じて収集されるデータに関する詳細と、VMware によるそのデータの使用目的については、<https://www.vmware.com/solutions/trustvmware/ceip.html> の Trust & Assurance Center に記載されています。

この製品の CEIP に参加する、または CEIP を終了するには、『vRealize Log Insight の管理』の「VMware のカスタマー エクスペリエンス プログラムに参加するまたは終了する」を参照してください。