

# vRealize Log Insight の管理

2019 年 7 月 11 日

vRealize Log Insight 4.7



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認ください。このドキュメントに関するご意見およびご感想は、[docfeedback@vmware.com](mailto:docfeedback@vmware.com) までお送りください。

VMware, Inc.  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

ヴァイエムウェア株式会社  
105-0013 東京都港区浜松町 1-30-5  
浜松町スクエア 13F  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2014-2018 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

## vRealize Log Insight の管理 7

- 1 vRealize Log Insight のアップグレード 8
  - vRealize Log Insight のアップグレード パス 8
  - vRealize Log Insight 4.7 へのアップグレード 9
  - vRealize Log Insight 4.6 へのアップグレード 10
  - vRealize Log Insight 4.5 へのアップグレード 11
  - vRealize Log Insight 4.3 へのアップグレード 12
  - vRealize Log Insight 4.0 へのアップグレード 13
  - vRealize Log Insight 3.6 へのアップグレード 14
- 2 vRealize Log Insight ユーザー アカウントの管理 16
  - ユーザー管理の概要 16
  - ロール ベースのアクセス制御 17
  - フィルタリングの使用によるユーザー アカウントの管理 17
  - vRealize Log Insight での新規ユーザー アカウントの作成 18
  - vRealize Log Insight の Active Directory グループへの VMware Identity Manager アクセスを構成する 19
  - vRealize Log Insight への Active Directory グループのインポート 20
  - クロスドメインのグループ メンバーシップを持つユーザーの認証 22
  - データ セットの定義 22
  - ロールの作成および変更 23
  - vRealize Log Insight からのユーザー アカウントまたはグループの削除 24
- 3 認証の設定 25
  - VMware Identity Manager によるユーザー認証の有効化 25
  - Active Directory を介したユーザー認証の有効化 26
    - Active Directory で使用するプロトコルの構成 27
- 4 vRealize Log Insight の構成 29
  - vRealize Log Insight 構成制限 29
  - 仮想アプライアンスの設定 30
    - vRealize Log Insight 仮想アプライアンス用の root の SSH パスワードの構成 30
    - vRealize Log Insight 仮想アプライアンスのネットワーク設定の変更 31
    - vRealize Log Insight 仮想アプライアンスのストレージ容量を増やす 32
    - vRealize Log Insight 仮想アプライアンスへのメモリおよび CPU の追加 33
  - vRealize Log Insight へのライセンスの割り当て 33
  - ログ ストレージ ポリシー 34
  - システム通知の管理 35

|   |    |
|---|----|
| システム通知  | 35 |
| vRealize Log Insight システム通知の宛先の設定                         | 39 |
| vRealize Log Insight イベント転送ターゲットの追加                       | 42 |
| SSL を使用した vRealize Log Insight イベント転送の構成                  | 45 |
| インタラクティブ分析でのイベント転送フィルタの使用                                 | 45 |
| vRealize Log Insight 仮想アプライアンスの時刻の同期                      | 46 |
| vRealize Log Insight の SMTP サーバの構成                        | 47 |
| カスタム SSL 証明書のインストール                                       | 47 |
| 自己署名証明書の生成  | 49 |
| 証明書署名要求の生成  | 50 |
| 認証局に対する署名の要求  | 51 |
| 証明書ファイルの連結  | 51 |
| 署名証明書のアップロード  | 52 |
| vRealize Log Insight サーバと Log Insight Agents 間の SSL 接続の構成 | 53 |
| vRealize Log Insight Web セッションのデフォルトのタイムアウト期間の変更          | 56 |
| アーカイブしています  | 57 |
| vRealize Log Insight でのデータ アーカイブの有効化または無効化                | 57 |
| vRealize Log Insight アーカイブ ファイルの形式                        | 58 |
| vRealize Log Insight アーカイブの vRealize Log Insight へのインポート  | 59 |
| Log Insight アーカイブの Raw テキスト ファイルまたは JSON へのエクスポート         | 60 |
| vRealize Log Insight サービスの再起動                             | 61 |
| vRealize Log Insight 仮想アプライアンスのパワーオフ                      | 61 |
| vRealize Log Insight サポート バンドルのダウンロード                     | 62 |
| VMware カスタマ エクスペリエンス改善プログラムへの参加または参加取り消し                  | 63 |
| <br>  |    |
| 5 vRealize Log Insight クラスタの管理                            | 64 |
| vRealize Log Insight クラスタへのワーカー ノードの追加                    | 64 |
| vRealize Log Insight 仮想アプライアンスのデプロイ                       | 64 |
| 既存の展開への参加   | 67 |
| vRealize Log Insight クラスタからのワーカー ノードの削除                   | 68 |
| 統合ロード バランサの操作   | 69 |
| 統合ロード バランサの有効化  | 70 |
| 本番クラスタ チェックの結果のクエリ  | 71 |
| <br>  |    |
| 6 ポートおよび外部インターフェイス  | 72 |
| <br>  |    |
| 7 vRealize Log Insight エージェントのステータスの監視                    | 76 |
| <br>  |    |
| 8 サーバからのエージェントの自動更新の有効化                                   | 78 |
| <br>  |    |
| 9 一元化されたエージェントの構成およびエージェント グループの操作                        | 79 |

- エージェント グループ構成のマージ 80
- エージェント グループの作成 80
- エージェント グループの編集 81
- Content Pack エージェント グループをエージェント グループとして追加 82
- エージェント グループの削除 82

## 10 vRealize Log Insight の監視 84

- vRealize Log Insight 仮想アプライアンスの健全性チェック 84
- ログ イベントを送信するホストの監視 85
- 非アクティブなホストについてレポートするシステム通知の構成 85

## 11 vRealize Log Insight と VMware 製品の統合 87

- vRealize Log Insight と vSphere 環境の接続 88
  - syslog サーバとしての vRealize Log Insight 89
  - vRealize Log Insight にログ イベントを転送するための ESXi ホストの構成 89
  - ログ イベントを vRealize Log Insight に転送するための ESXi ホスト構成の変更 91
  - vRealize Operations Manager の vRealize Log Insight イベント通知 92
- vCenter Server インスタンスからイベント、タスク、およびアラームをプルするための vRealize Log Insight の構成 93
- vRealize Operations Manager と vRealize Log Insight の併用 94
  - vRealize Operations Manager との統合の要件 94
  - vRealize Operations Manager に通知イベントを送信する vRealize Log Insight の構成 95
  - vRealize Operations Manager での vRealize Log Insight のコンテキストでの起動の有効化 96
  - vRealize Operations Manager での vRealize Log Insight のコンテキストでの起動の無効化 100
  - DNS 検索パスとドメイン 101
  - vRealize Log Insight アダプタの削除 102
- vRealize Log Insight の vRealize Operations Manager コンテンツ バック 103

## 12 vRealize Log Insight に関するセキュリティの考慮事項 104

- ポートおよび外部インターフェイス 104
- vRealize Log Insight 構成ファイル 107
- vRealize Log Insight のパブリック キー、証明書、およびキーストア 108
- vRealize Log Insight のライセンスおよび EULA ファイル 108
- vRealize Log Insight ログ ファイル 109
  - ユーザー監査ログ メッセージのデバッグ レベルの有効化 111
- vRealize Log Insight ユーザー アカウント 112
- vRealize Log Insight ファイアウォールに関する推奨事項 112
- セキュリティ アップデートおよびパッチ 113

## 13 バックアップ、リストア、およびディザスタ リカバリ 114

- バックアップ、リストア、およびディザスタ リカバリの概要 114
- 固定 IP アドレスおよび FQDN の使用 115

- 計画および準備 116
- ノードおよびクラスタのバックアップ 117
- Linux または Windows エージェントのバックアップ 118
- ノードおよびクラスタのリストア 118
- リストア後の構成の変更 120
  - 同じホストへのリストア 120
  - 別ホストへのリストア 120
- リストアの確認 123
- ディザスタ リカバリ 124

## 14 vRealize Log Insight のトラブルシューティング 125

- Internet Explorer で vRealize Log Insight にログインできない 125
- vRealize Log Insight のディスク領域不足 126
- アーカイブされたデータのインポートに失敗することがある 126
- vRealize Log Insight のサポート バンドルを作成するための仮想アプライアンス コンソールの使用 127
- 管理者ユーザーのパスワードのリセット 127
- root ユーザーのパスワードのリセット 128
- vRealize Operations Manager にアラートを配信できない場合 129
- Active Directory の認証情報を使用してログインできない 130
- STARTTLS オプションが有効な場合 SMTP が機能しない 130
- .pak ファイルの署名を検証できなかったためのアップグレードの失敗 131
- 内部サーバ エラーによるアップグレードの失敗 132

# vRealize Log Insight の管理

『vRealize Log Insight の管理』では、ユーザー アカウントの管理や、Log Insight Agents と他の VMware 製品との統合など、VMware vRealize™Log Insight™ の管理について説明します。また、製品セキュリティの管理と、導入環境のアップグレードに関する情報も記載されています。

記載されている情報は、Windows または Linux のシステム管理者としての経験があり、仮想マシン テクノロジー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。

# vRealize Log Insight のアップグレード

# 1

増分アップグレードパスに従って、vRealize Log Insight をバージョン 4.7 にアップグレードできます。このアップグレードには、クラスタ内のノードの自動アップグレードが含まれます。

この章には、次のトピックが含まれています。

- [vRealize Log Insight のアップグレードパス](#)
- [vRealize Log Insight 4.7 へのアップグレード](#)
- [vRealize Log Insight 4.6 へのアップグレード](#)
- [vRealize Log Insight 4.5 へのアップグレード](#)
- [vRealize Log Insight 4.3 へのアップグレード](#)
- [vRealize Log Insight 4.0 へのアップグレード](#)
- [vRealize Log Insight 3.6 へのアップグレード](#)

## vRealize Log Insight のアップグレードパス

使用するアップグレードパスは、アップグレード先の製品にどのバージョンの vRealize Log Insight がインストールされているかによって異なります。

vRealize Log Insight では増分アップグレードを行う必要があります。たとえば、バージョン 4.5 からバージョン 4.7 にアップグレードするには、4.6 アップグレードを 4.5 に適用し、4.6 から 4.7 へのアップグレードを行います。それぞれの中間リリースにアップグレードする必要があります。

また、「[VMware 製品の相互運用性マトリクス](#)」サイトの [アップグレードパス] 機能を使用して、サポートされるアップグレードパスを表示することもできます。

表 1-1. サポートされるアップグレードパス

| アップグレード元                           | アップグレード先                 | 手順  |
|------------------------------------|--------------------------|---|
| vRealize Log Insight 4.6 または 4.6.1 | vRealize Log Insight 4.7 | <a href="#">vRealize Log Insight 4.7 へのアップグレード</a> を参照してください。 |
| vRealize Log Insight 4.5           | vRealize Log Insight 4.6 | <a href="#">vRealize Log Insight 4.6 へのアップグレード</a> を参照してください。 |
| vRealize Log Insight 4.3           | vRealize Log Insight 4.5 | <a href="#">vRealize Log Insight 4.5 へのアップグレード</a> を参照してください。 |



| アップグレード元                | アップグレード先                | 手順   |
|-------------------------|-------------------------|--|
| vRealize Log Insight4.0 | vRealize Log Insight4.3 | <a href="#">vRealize Log Insight4.3 へのアップグレード</a> を参照してください。 |
| vRealize Log Insight3.6 | vRealize Log Insight4.0 | <a href="#">vRealize Log Insight4.0 へのアップグレード</a> を参照してください。 |

## vRealize Log Insight 4.7 へのアップグレード

クラスタを vRealize Log Insight 4.7 に自動的にアップグレードできます。

vRealize Log Insight のアップグレードはマスター ノードの FQDN から実行する必要があります。統合ロード バランサの IP アドレスを使用したアップグレードはサポートされていません。

アップグレード中に、マスター ノードが最初にアップグレードされ、再起動します。各クラスタ ノードが順番にアップグレードされます。ローリング アップグレードのステータスは、[管理] - [クラスタ] ページで確認できます。統合ロード バランサが構成されている場合、その IP アドレスがクラスタ ノード間で移行され、UI、API、および受信イベントの取り込みなどのクラスタ サービスは、ローリング アップグレード中も利用可能になります。低レベルの詳細が個々のノードの `upgrade.log` ファイルに書き込まれます。アップグレードが正常に完了すると、システム通知が送信されます。

アップグレード プロセス中に 1 つ以上のノードに影響する問題が発生すると、クラスタ全体が元の動作バージョンにロールバックされます。アップグレードの開始後に実行された構成の変更は一貫性がない、または有効でない場合があるため、構成はアップグレード前にキャプチャされた良好な状態に戻ります。取り込まれたイベントは失われません。進行状況は個々のノードの `rollback.log` ファイルに書き込まれます。ロールバックが終了すると、システム通知が送信されます。問題が調査されて修正されると、アップグレードを再試行できます。

アップグレードが完了すると、アップグレード前にメンテナンス モードであったノードを含む、すべてのノードが接続状態になり、オンラインになります。

### 前提条件

- バージョン 4.6.x に 4.7 のアップグレードを適用していることを確認します。サポートされるアップグレードパスの詳細については、[vRealize Log Insight のアップグレードパス](#)を参照してください。
- vRealize Log Insight 仮想アプライアンスのスナップショットまたはバックアップ コピーを作成します。
- アップグレード後のリリースに対応した vRealize Log Insight アップグレード バンドル `.pak` ファイルのコピーを取得します。
- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。
- アップグレードするノードがメンテナンス モードにある場合はメモしておきます。アップグレードが完了したら、接続状態からメンテナンス モードに戻す必要があります。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。

- 2 [管理] で、[クラスタ] をクリックします。
- 3 [PAK からアップグレード] をクリックして、.pak ファイルをアップロードします。
- 4 新しい使用許諾契約に同意して、アップグレード手順を完了します。

#### 次のステップ

マスター ノードのアップグレード プロセスが完了したら、自動で行われる残りのアップグレード プロセスを表示できます。

管理者向けに送信される E メールで、アップグレードが正常に完了したことを確認します。

アップグレードが完了すると、アップグレード前にメンテナンス モードであったノードも含めて、すべてのノードがオンラインになります。これらのノードを必要に応じてメンテナンス モードに戻します。

## vRealize Log Insight 4.6 へのアップグレード

クラスタを vRealize Log Insight 4.6 に自動的にアップグレードできます。

vRealize Log Insight のアップグレードはマスター ノードの FQDN から実行する必要があります。統合ロード バランサの IP アドレスを使用したアップグレードはサポートされていません。

アップグレード中に、マスター ノードが最初にアップグレードされ、再起動します。次に、各クラスタ ノードが順番にアップグレードされます。ローリング アップグレードの現在の状況は、[管理] - [クラスタ] ページで確認できます。統合ロード バランサが構成されている場合、その IP アドレスがクラスタ ノード間で移行され、UI、API、および受信イベントの取り込みなどのクラスタ サービスは、ローリング アップグレード中も利用可能になります。低レベルの詳細が個々のノードの `upgrade.log` ファイルに書き込まれます。アップグレードが正常に完了すると、システム通知が送信されます。


アップグレード プロセス中に 1 つ以上のノードに影響する問題が発生すると、クラスタ全体が元の動作バージョンに自動的にロールバックされます。アップグレードの開始後に実行された構成の変更は一貫性がない、または有効でない場合があるため、構成はアップグレード前にキャプチャされた良好な状態に戻ります。取り込まれたイベントは失われません。進行状況は個々のノードの `rollback.log` ファイルに書き込まれます。ロールバックが終了すると、システム通知が送信されます。問題が調査されて修正されると、アップグレードを再試行できます。

#### 前提条件

- バージョン 4.5.x に 4.6 のアップグレードを適用していることを確認します。サポートされるアップグレード パスの詳細については、[vRealize Log Insight のアップグレード パス](#)を参照してください。
- サポートされているアップグレード パスに従ってアップグレードを適用していることを確認します。[vRealize Log Insight のアップグレード パス](#)を参照してください。
- vRealize Log Insight 仮想アプライアンスのスナップショットまたはバックアップ コピーを作成します。
- アップグレード後のリリースに対応した vRealize Log Insight アップグレード バンドル .pak ファイルのコピーを取得します。
- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

- アップグレードするノードがメンテナンス モードにある場合はメモしておきます。アップグレードが完了したら、接続状態からメンテナンス モードに戻す必要があります。

#### 手順

- 1 構成ドロップダウンメニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 [PAK からアップグレード] をクリックして、.pak ファイルをアップロードします。
- 4 新しい使用許諾契約に同意して、アップグレード手順を完了します。

#### 次のステップ

マスター ノードのアップグレード プロセスが完了したら、自動で行われる残りのアップグレード プロセスを表示できます。

管理者向けに送信される E メールで、アップグレードが正常に完了したことを確認します。

アップグレードが完了すると、アップグレード前にメンテナンス モードであったノードも含めて、すべてのノードがオンラインになります。これらのノードを必要に応じてメンテナンス モードに戻します。

## vRealize Log Insight 4.5 へのアップグレード

クラスタを vRealize Log Insight 4.5 に自動的にアップグレードできます。

vRealize Log Insight のアップグレードはマスター ノードの FQDN から実行する必要があります。統合ロード バランサの IP アドレスを使用したアップグレードはサポートされていません。

アップグレード中に、マスター ノードが最初にアップグレードされ、再起動します。次に、各クラスタ ノードが順番にアップグレードされます。ローリング アップグレードの現在の状況は、[管理] - [クラスタ] ページで確認できます。統合ロード バランサが構成されている場合、その IP アドレスがクラスタ ノード間で移行され、UI、API、および受信イベントの取り込みなどのクラスタ サービスは、ローリング アップグレード中も利用可能になります。低レベルの詳細が個々のノードの `upgrade.log` ファイルに書き込まれます。アップグレードが正常に完了すると、システム通知が送信されます。


アップグレード プロセス中に 1 つ以上のノードに影響する問題が発生すると、クラスタ全体が元の動作バージョンに自動的にロールバックされます。アップグレードの開始後に実行された構成の変更は一貫性がない、または有効でない場合があるため、構成はアップグレード前にキャプチャされた良好な状態に戻ります。取り込まれたイベントは失われません。進行状況は個々のノードの `rollback.log` ファイルに書き込まれます。ロールバックが終了すると、システム通知が送信されます。問題が調査されて修正されると、アップグレードを再試行できます。

#### 前提条件

- サポートされているアップグレード パスに従ってアップグレードを適用していることを確認します。 [vRealize Log Insight のアップグレード パス](#) を参照してください。
- vRealize Log Insight 仮想アプライアンスのスナップショットまたはバックアップ コピーを作成します。
- アップグレード後のリリースに対応した vRealize Log Insight アップグレード バンドル .pak ファイルのコピーを取得します。

- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 [PAK からアップグレード] をクリックして、.pak ファイルをアップロードします。
- 4 新しい使用許諾契約に同意して、アップグレード手順を完了します。

#### 次のステップ

マスター ノードのアップグレード プロセスが完了したら、自動で行われる残りのアップグレード プロセスを表示できます。

管理者向けに送信される E メールで、アップグレードが正常に完了したことを確認します。

## vRealize Log Insight4.3 へのアップグレード

クラスタを vRealize Log Insight4.3 に自動的にアップグレードできます。

vRealize Log Insight のアップグレードはマスター ノードの FQDN から実行する必要があります。統合ロード バランサの IP アドレスを使用したアップグレードはサポートされていません。

アップグレード中に、マスター ノードが最初にアップグレードされ、再起動します。次に、各クラスタ ノードが順番にアップグレードされます。ローリング アップグレードの現在の状況は、[管理] - [クラスタ] ページで確認できます。統合ロード バランサが構成されている場合、その IP アドレスがクラスタ ノード間で移行され、UI、API、および受信イベントの取り込みなどのクラスタ サービスは、ローリング アップグレード中も利用可能になります。低レベルの詳細が個々のノードの `upgrade.log` ファイルに書き込まれます。アップグレードが正常に完了すると、システム通知が送信されます。


アップグレード プロセス中に 1 つ以上のノードに影響する問題が発生すると、クラスタ全体が元の動作バージョンに自動的にロールバックされます。アップグレードの開始後に実行された構成の変更は一貫性がない、または有効でない場合があるため、構成はアップグレード前にキャプチャされた良好な状態に戻ります。取り込まれたイベントは失われません。進行状況は個々のノードの `rollback.log` ファイルに書き込まれます。ロールバックが終了すると、システム通知が送信されます。問題が調査されて修正されると、アップグレードを再試行できます。

#### 前提条件

- サポートされているアップグレード パスに従ってアップグレードを適用していることを確認します。 [vRealize Log Insight のアップグレード パス](#)を参照してください。
- vRealize Log Insight 仮想アプライアンスのスナップショットまたはバックアップ コピーを作成します。
- アップグレード後のリリースに対応した vRealize Log Insight アップグレード バンドル .pak ファイルのコピーを取得します。

- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 [PAK からアップグレード] をクリックして、.pak ファイルをアップロードします。
- 4 新しい使用許諾契約に同意して、アップグレード手順を完了します。

#### 次のステップ

マスター ノードのアップグレード プロセスが完了したら、自動で行われる残りのアップグレード プロセスを表示できます。

管理者向けに送信される E メールで、アップグレードが正常に完了したことを確認します。

## vRealize Log Insight4.0 へのアップグレード

クラスタを vRealize Log Insight4.0 に自動的にアップグレードできます。

vRealize Log Insight のアップグレードはマスター ノードの FQDN から実行する必要があります。統合ロード バランサの IP アドレスを使用したアップグレードはサポートされていません。

アップグレード中に、マスター ノードが最初にアップグレードされ、再起動します。次に、各クラスタ ノードが順番にアップグレードされます。ローリング アップグレードの現在の状況は、[管理] - [クラスタ] ページで確認できます。統合ロード バランサが構成されている場合、その IP アドレスがクラスタ ノード間で移行され、UI、API、および受信イベントの取り込みなどのクラスタ サービスは、ローリング アップグレード中も利用可能になります。低レベルの詳細が個々のノードの `upgrade.log` ファイルに書き込まれます。アップグレードが正常に完了すると、システム通知が送信されます。


アップグレード プロセス中に 1 つ以上のノードに影響する問題が発生すると、クラスタ全体が元の動作バージョンに自動的にロールバックされます。アップグレードの開始後に実行された構成の変更は一貫性がない、または有効でない場合があるため、構成はアップグレード前にキャプチャされた良好な状態に戻ります。取り込まれたイベントは失われません。進行状況は個々のノードの `rollback.log` ファイルに書き込まれます。ロールバックが終了すると、システム通知が送信されます。問題が調査されて修正されると、アップグレードを再試行できます。

#### 前提条件

- サポートされているアップグレード パスに従ってアップグレードを適用していることを確認します。 [vRealize Log Insight のアップグレード パス](#)を参照してください。
- vRealize Log Insight 仮想アプライアンスのスナップショットまたはバックアップ コピーを作成します。
- アップグレード後のリリースに対応した vRealize Log Insight アップグレード バンドル .pak ファイルのコピーを取得します。

- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 [PAK からアップグレード] をクリックして、.pak ファイルをアップロードします。
- 4 新しい使用許諾契約に同意して、アップグレード手順を完了します。

#### 次のステップ

マスター ノードのアップグレード プロセスが完了したら、自動で行われる残りのアップグレード プロセスを表示できます。

管理者向けに送信される E メールで、アップグレードが正常に完了したことを確認します。

## vRealize Log Insight3.6 へのアップグレード

クラスタを vRealize Log Insight3.6 に自動的にアップグレードできます。

vRealize Log Insight のアップグレードはマスター ノードの FQDN から実行する必要があります。統合ロード バランサの IP アドレスを使用したアップグレードはサポートされていません。

アップグレード中に、マスター ノードが最初にアップグレードされ、再起動します。次に、各クラスタ ノードが順番にアップグレードされます。ローリング アップグレードの現在の状況は、[管理] - [クラスタ] ページで確認できます。統合ロード バランサが構成されている場合、その IP アドレスがクラスタ ノード間で移行され、UI、API、および受信イベントの取り込みなどのクラスタ サービスは、ローリング アップグレード中も利用可能になります。低レベルの詳細が個々のノードの `upgrade.log` ファイルに書き込まれます。アップグレードが正常に完了すると、システム通知が送信されます。


アップグレード プロセス中に 1 つ以上のノードに影響する問題が発生すると、クラスタ全体が元の動作バージョンに自動的にロールバックされます。アップグレードの開始後に実行された構成の変更は一貫性がない、または有効でない場合があるため、構成はアップグレード前にキャプチャされた良好な状態に戻ります。取り込まれたイベントは失われません。進行状況は個々のノードの `rollback.log` ファイルに書き込まれます。ロールバックが終了すると、システム通知が送信されます。問題が調査されて修正されると、アップグレードを再試行できます。

#### 前提条件

- サポートされているアップグレード パスに従ってアップグレードを適用していることを確認します。 [vRealize Log Insight のアップグレード パス](#)を参照してください。
- vRealize Log Insight 仮想アプライアンスのスナップショットまたはバックアップ コピーを作成します。
- アップグレード後のリリースに対応した vRealize Log Insight アップグレード バンドル .pak ファイルのコピーを取得します。

- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 [PAK からアップグレード] をクリックして、.pak ファイルをアップロードします。
- 4 新しい使用許諾契約に同意して、アップグレード手順を完了します。

#### 次のステップ

マスター ノードのアップグレード プロセスが完了したら、自動で行われる残りのアップグレード プロセスを表示できます。

管理者向けに送信される E メールで、アップグレードが正常に完了したことを確認します。



# vRealize Log Insight ユーザー アカウ ントの管理

## 2

管理者は、vRealize Log Insight Web インターフェイスにアクセス可能なユーザー アカウントとロールを作成できます。

管理情報の編集 権限を持つユーザーのみが、ユーザー アカウントを作成および編集できます。ただし、管理情報の編集 権限がない場合でも、ユーザーは自分のメールアドレスやアカウントのパスワードを変更できます。

この章には、次のトピックが含まれています。

- ユーザー管理の概要
- ロール ベースのアクセス制御
- フィルタリングの使用によるユーザー アカウントの管理
- vRealize Log Insight での新規ユーザー アカウントの作成
- vRealize Log Insight の Active Directory グループへの VMware Identity Manager アクセスを構成する
- vRealize Log Insight への Active Directory グループのインポート
- クロスドメインのグループ メンバーシップを持つユーザーの認証
- データ セットの定義
- ロールの作成および変更
- vRealize Log Insight からのユーザー アカウントまたはグループの削除

## ユーザー管理の概要

システム管理者は、ユーザー ログイン、ロールに基づくアクセス制御、権限、データ セットの組み合わせを使用して vRealize Log Insight ユーザーを管理します。ロールに基づくアクセス制御により、管理者はユーザーおよびユーザーが実行できるタスクを管理できます。

ロールは特定のタスクを実行するために必要な権限のセットです。システム管理者は、セキュリティ ポリシーの定義の一環としてロールを定義し、ユーザーに付与します。システム管理者はロール設定を更新することで特定のロールに関連付けられた権限およびタスクを変更できます。更新された設定はロールに関連付けられたすべてのユーザーに対して有効になります。

- システム管理者は、ユーザーにロールを付与することでそのユーザーがタスクを実行できるようにします。
- ユーザーがタスクを実行できないようにする場合、システム管理者はユーザーからロールを取り消します。



各ユーザーのアクセス、ロールおよび権限の管理は、ユーザー ログイン アカウント単位で行います。各ユーザーには複数のロールおよび権限が付与できます。

特定のオブジェクトの表示またはアクセス、または特定の操作の実行を行う権限が付与されていないユーザーは、それらの操作を実行できません。


## ロール ベースのアクセス制御

ロールベースのアクセス制御により、システム管理者は vRealize Log Insight へのユーザー アクセスを制御し、ユーザーがログイン後に実行できるタスクを制御できます。ロールベースのアクセス制御を実装するには、システム管理者が権限やロールをユーザー ログイン アカウントに関連付けたり取り消したりします。

|         |  |
|---------|--|
| ユーザー    | システム管理者は、ユーザーのログイン アカウントの権限やロールを付与または取り消すことによって各ユーザーのアクセスとアクションを制御できます。  |
| 権限      | 権限は vRealize Log Insight で許可されるアクションを制御します。権限は、vRealize Log Insight の特定の管理タスクまたはユーザー タスクに適用されます。たとえば、管理者の表示 権限を付与することで、ユーザーが vRealize Log Insight の管理設定を表示することを許可できます。 |
| データ セット | データ セットは一連のフィルタで構成されます。データ セットをロールに関連付けることにより、ユーザーに特定コンテンツへのアクセスを許可できます。   |
| ロール     | ロールは、ユーザーに関連付けることができる権限とデータセットの集合です。ロールは、タスクを実行するために必要なすべての権限をパッケージ化する便利な方法です。1 人のユーザーに複数のロールを関連付けることができます。  |

## フィルタリングの使用によるユーザー アカウントの管理

検索フィルタを指定することで、ユーザーまたはユーザーのセットを検索できます。

フィルタリングは、[アクセス コントロール] ページの [ユーザーおよびグループ] タブから行います。ページに移動するには、ドロップダウン メニュー アイコン  から [管理] をクリックし、[管理] メニューの [アクセス コントロール] をクリックして、[ユーザーおよびグループ] タブを選択します。

検索テキスト ボックスはページの上部付近にあり、Filter by username という語句が記されています。

検索関数は入力中に結果をフィルタリングし、入力したパターンを含むユーザー名を返します。たとえば、John\_Smith、John\_Doe、Helen\_Jonson というユーザー名がある場合、文字 J を入力すると、その文字を含むすべてのユーザー名が返されます。この例では John\_Smith、John\_Doe、および Helen\_Jonson です。引き続き文字を入力すると、そのパターンに完全に一致する検索結果に絞り込まれます。この例では、**John\_** と入力すると、John\_Smith および John\_Doe が返されます。

検索結果は、ドメイン、認証、ロール、E メール、または UPN フィールドで並べ替えることができます。また、検索結果に対して、複数ユーザーの削除などの一括操作を実行することができます。

## vRealize Log Insight での新規ユーザー アカウントの作成


スーパー管理者ロールが割り当てられたユーザーは、ユーザー アカウントを作成して vRealize Log Insight Web ユーザー インターフェイスへのアクセスを提供できます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

VMware Identity Manager または Active Directory を認証に使用するユーザー アカウントを作成する場合は、VMware Identity Manager または Active Directory のサポートを設定済みであることを確認してください。[VMware Identity Manager によるユーザー認証の有効化](#) および [Active Directory を介したユーザー認証の有効化](#) を参照してください。

### 手順

- 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- [管理] で、[アクセス コントロール] をクリックします。
- [ユーザー/ユーザーおよびグループ] をクリックします。
- [新規ユーザー] をクリックします。
- [認証] ドロップダウン メニューから、いずれかの項目を選択します。
  - デフォルトの組み込みの認証方法を使用する場合、ユーザー名とパスワードを入力します。オプションでメールアドレスを入力することもできます。[パスワード] テキスト ボックスからパスワードをコピーし、ユーザーに提供します。
  - Active Directory 認証または VMware Identity Manager 認証を使用する場合、ユーザーが所属するドメインとユーザー名を入力します。オプションでそのユーザー名のアカウントのメールアドレスを入力することができます。
- 右側の [ロール] リストから、1 つ以上の定義済みまたはカスタムのユーザー ロールを選択します。

| オプション          | 説明   |
|----------------|--|
| [ユーザー]         | ユーザーは、vRealize Log Insight のすべての機能にアクセスできます。ユーザーは、ログ イベントの表示、ログを検索およびフィルタリングするためのクエリの実行、自分のユーザー領域へのコンテンツ パックのインポート、アラート クエリの追加、自分のユーザー アカウントのパスワードやメールアドレスの変更ができます。ユーザーには、管理オプションへのアクセス権がなく、他のユーザーとのコンテンツの共有、他のユーザーのアカウントの変更、マーケットプレイスからのコンテンツ パックのインストールはできません。ただし、自分だけが見ることができるユーザー領域にコンテンツ パックをインポートできます。 |
| [ダッシュボード ユーザー] | ダッシュボード ユーザーは vRealize Log Insight の [ダッシュボード] ページのみを使用できます。   |

| オプション     | 説明  |
|-----------|---|
| [表示限定管理者] | 表示管理者ユーザーは、管理者情報を表示でき、完全なユーザー アクセス権を持ち、共有コンテナを編集できます。   |
| [スーパー管理者] | スーパー管理者ユーザーは、vRealize Log Insight の全機能にアクセスし、vRealize Log Insight を管理し、他のすべてのユーザーのアカウントを管理できます。 |

## 7 [保存] をクリックします。

- 組み込みの認証方法では、情報がローカルに保存されます。
- VMware Identity Manager による認証では、指定されたグループおよびそのドメインと VMware Identity Manager が同期しているかどうかを vRealize Log Insight が検証します。そのグループが見つからない場合、vRealize Log Insight がグループを検証できないことを伝えるダイアログ ボックスが表示されます。検証しないでグループを保存することも、キャンセルしてグループ名またはドメインを訂正することもできます。

# vRealize Log Insight の Active Directory グループへの VMware Identity Manager アクセスを構成する

VMware Identity Manager のシングル サインオン認証を介して vRealize Log Insight で Active Directory グループを使用できます。サイトでは Active Directory のサポートを有効にするための VMware Identity Manager 認証が構成され、サーバ同期が実行されている必要があります。

また、vRealize Log Insight にグループ情報をインポートする必要があります。


VMware Identity Manager ユーザーは、個々のユーザーに割り当てられたロールに加え、ユーザーが属するグループに割り当てられたロールも継承します。たとえば、管理者はグループ A を [表示管理者] のロールに割り当て、ユーザー Bob を [ユーザー] のロールに割り当てることができます。さらに、Bob をグループ A に割り当てることができます。Bob は、ログインすると、グループ ロールを継承し、[表示管理者] と [ユーザー] の両方のロールの権限を保持します。

このグループは VMware Identity Manager のローカル グループではなく、VMware Identity Manager と同期する Active Directory グループです。

## 前提条件

- UPN 属性 (userPrincipalName) が構成されていることを確認します。これは、[ID とアクセス管理] - [ユーザー属性] の VMware Identity Manager 管理者インターフェイスから構成できます。
- [管理者の編集] 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。
- vRealize Log Insight で VMware Identity Manager サポートが構成されていることを確認します。 [VMware Identity Manager によるユーザー認証の有効化](#) を参照してください。

## 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。

- 2 [管理] で、[アクセス コントロール] をクリックします。
- 3 [ユーザーおよびグループ] をクリックします。
- 4 Directory グループ テーブルにスクロールして、[新規グループ] をクリックします。
- 5 [タイプ] ドロップダウン メニューから、[VMware Identity Manager] を選択します。

VMware Identity Manager のサポートを設定するときに指定したデフォルトのドメイン名が [ドメイン] テキスト ボックスに表示されます。

- 6 ドメイン名をグループの Active Directory 名に変更します。
- 7 追加するグループの名前を入力します。
- 8 右側の [ロール] リストから、1 つ以上の定義済みまたはカスタムのユーザー ロールを選択します。

| オプション          | 説明   |
|----------------|--|
| [ユーザー]         | ユーザーは、vRealize Log Insight のすべての機能にアクセスできます。ユーザーは、ログ イベントの表示、ログを検索およびフィルタリングするためのクエリの実行、自分のユーザー領域へのコンテンツ バックのインポート、アラート クエリの追加、自分のユーザー アカウントのパスワードやメールアドレスの変更ができます。ユーザーには、管理オプションへのアクセス権がなく、他のユーザーとのコンテンツの共有、他のユーザーのアカウントの変更、マーケットプレイスからのコンテンツ バックのインストールはできません。ただし、自分だけが見ることができるユーザー領域にコンテンツ バックをインポートできます。 |
| [ダッシュボード ユーザー] | ダッシュボード ユーザーは vRealize Log Insight の [ダッシュボード] ページのみを使用できます。   |
| [表示限定管理者]      | 表示管理者ユーザーは、管理者情報を表示でき、完全なユーザー アクセス権を持ち、共有コンテンツを編集できます。   |
| [スーパー管理者]      | スーパー管理者ユーザーは、vRealize Log Insight の全機能にアクセスし、vRealize Log Insight を管理し、他のすべてのユーザーのアカウントを管理できます。  |

- 9 [保存] をクリックします。

VMware Identity Manager が指定されたグループおよびそのドメインと同期しているかどうかを vRealize Log Insight が検証します。そのグループが見つからない場合、vRealize Log Insight がグループを検証できないことを伝えるダイアログ ボックスが表示されます。検証しないでグループを保存することも、キャンセルしてグループ名またはドメインを訂正することもできます。

追加したグループに属するユーザーは、ユーザー自身の VMware Identity Manager アカウントを使用して vRealize Log Insight にログインし、ユーザーが属するグループと同じ権限レベルを持つことができます。

## vRealize Log Insight への Active Directory グループのインポート

個々のドメイン ユーザーを追加する代わりに、ドメイン グループを追加して、ユーザーが vRealize Log Insight にログインできるようにすることができます。

vRealize Log Insight で Active Directory サポートを有効にする場合、ドメイン名を構成し、ドメインに属するバインド ユーザーを指定します。vRealize Log Insight は、バインド ユーザーを使用して Active Directory ドメインへの接続を確認し、Active Directory ユーザーおよびグループの存在を確認します。


vRealize Log Insight に追加する Active Directory グループは、バインド ユーザーのドメインに属しているか、バインド ユーザーのドメインによって信頼されているドメインに属している必要があります。

Active Directory ユーザーは、個々のユーザーに割り当てられたロールに加え、ユーザーが属するグループに割り当てられたロールも継承します。たとえば、管理者はグループ A を [表示管理者] のロールに割り当て、ユーザー Bob を [ユーザー] のロールに割り当てることができます。さらに、Bob をグループ A に割り当てることができます。Bob は、ログインすると、グループ ロールを継承し、[表示管理者] と [ユーザー] の両方のロールの権限を保持します。

#### 前提条件

- [管理者の編集] 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。
- AD サポートが構成されていることを確認します。[Active Directory を介したユーザー認証の有効化](#)を参照してください。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[アクセス コントロール] をクリックします。
- 3 [ユーザーおよびグループ] をクリックします。
- 4 Directory グループで [新規グループ] をクリックします。
- 5 [タイプ] ドロップダウン メニューで [Active Directory] をクリックします。

Active Directory サポートを構成するときに指定したデフォルトのドメイン名が [ドメイン] テキスト ボックスに表示されます。デフォルト ドメインからグループを追加する場合は、ドメイン名を変更しないでください。

- 6 (オプション) デフォルト ドメインを信頼しているドメインからグループを追加する場合は、[ドメイン] テキスト ボックスに信頼するドメインの名前を入力します。
- 7 追加するグループの名前を入力します。
- 8 右側の [ロール] リストから、1 つ以上の定義済みまたはカスタムのユーザー ロールを選択します。

| オプション          | 説明   |
|----------------|--|
| [ユーザー]         | ユーザーは、vRealize Log Insight のすべての機能にアクセスできます。ユーザーは、ログインイベントの表示、ログを検索およびフィルタリングするためのクエリの実行、自分のユーザー領域へのコンテンツ バックのインポート、アラート クエリの追加、自分のユーザー アカウントのパスワードやメール アドレスの変更ができます。ユーザーには、管理オプションへのアクセス権がなく、他のユーザーとのコンテンツの共有、他のユーザーのアカウントの変更、マーケットプレイスからのコンテンツ バックのインストールはできません。ただし、自分だけが見ることができるユーザー領域にコンテンツ バックをインポートできます。 |
| [ダッシュボード ユーザー] | ダッシュボード ユーザーは vRealize Log Insight の [ダッシュボード] ページのみを使用できます。   |

| オプション     | 説明  |
|-----------|---|
| [表示限定管理者] | 表示管理者ユーザーは、管理者情報を表示でき、完全なユーザー アクセス権を持ち、共有コンテンツを編集できます。  |
| [スーパー管理者] | スーパー管理者ユーザーは、vRealize Log Insight の全機能にアクセスし、vRealize Log Insight を管理し、他のすべてのユーザーのアカウントを管理できます。 |

## 9 [保存] をクリックします。

vRealize Log Insight は、指定したドメインまたは信頼するドメインに AD グループが存在するかどうかを検証します。そのグループが見つからない場合、vRealize Log Insight がグループを検証できないことを伝えるダイアログ ボックスが表示されます。検証しないでグループを保存することも、キャンセルしてグループ名を訂正することもできます。

追加した Active Directory グループに属するユーザーは、ユーザー自身のドメイン アカウントを使用して vRealize Log Insight にログインし、ユーザーが属するグループと同じ権限レベルを持つことができます。

## クロスドメインのグループ メンバーシップを持つユーザーの認証

管理者が信頼されたドメインからのユーザーを vRealize Log Insight に対して認証する場合、2 つの方法があります。

- 各ユーザーを手動で追加する。
- グループをユーザーと同じドメインに構成してグループを追加する。

## データ セットの定義


特定のコンテンツにユーザーがアクセスできるようにデータ セットを定義できます。

データ セットにはテキストベースの制約はサポートされていません。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[アクセス コントロール] をクリックします。
- 3 [データ セット] をクリックします。
- 4 [新規データ セット] をクリックします。
- 5 [フィルタの追加] をクリックします。

- 最初のドロップダウン メニューを使用して、vRealize Log Insight 内で定義されたフィールドを選択しフィルタを実行します。

たとえば、[hostname] を選択します。

このリストには静的フィールドのみが含まれ、抽出されたフィールド、ユーザー共有フィールド、テキスト フィールド、および event\_type フィルタによって作成されたフィールドは除外されます。

**注:** 数値フィールドには文字列フィールドには含まれないその他の演算子 ([=], [>], [<], [>=], [<=]) が含まれます。これらの演算子は数値比較を実行します。これらの演算子を使用すると、文字列演算子を使用した場合とは異なる結果が得られます。たとえば、フィルタ [response\_time][=]02 は、値が 2 の [response\_time] フィールドを持つイベントに一致します。フィルタ [response\_time][contains]02 は、上記と同じ一致にはなりません。

- 2 番目のドロップダウン メニューを使用して、最初のドロップダウン メニューで選択したフィールドに適用する演算を選択します。

たとえば、[contains] を選択します。[contains] フィルタは、フル トークンに一致します。「err」という文字列を検索しても「error」を一致として検出しません。

- フィルタ ドロップダウン メニューの右にあるフィルタ ボックスに、フィルタとして使用する値を入力します。複数の値を使用できます。これらの値の演算子は OR です。

**注:** 2 番目のドロップダウン メニューで [exists] 演算子を選択した場合、ボックスは使用できません。

- (オプション) さらにフィルタを追加する場合は、[フィルタの追加] をクリックします。
- (オプション) フィルタが期待した通りに動作していることを検証するには、[インタラクティブ分析での実行] をクリックして、フィルタに一致するデータを含むインタラクティブ分析ウィンドウを開きます。
- [保存] をクリックします。

#### 次のステップ

データ セットをユーザー ロールに関連付けます。[ロールの作成および変更](#)を参照してください。

## ロールの作成および変更

カスタム ロールを作成したり、定義済みロールを変更して、特定のタスクの実行および特定のコンテンツへのアクセスをユーザーに対して許可できます。



#### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。



- 2 [管理] で、[アクセス コントロール] をクリックします。
- 3 [ロール] をクリックします。
- 4 [新規ロール] をクリックするか、  をクリックして既存のロールを編集します。  
スーパー管理者ロールおよびユーザー ロールは編集する前にクローン作成する必要があります。
- 5 [名前] および [説明] テキスト ボックスを変更します。
- 6 権限リストから 1 つ以上の権限を選択します。

| オプション     | 説明                  |
|-----------|---------------------|
| 管理者の編集    | 管理者の情報および設定を編集できます。 |
| 管理者の表示    | 管理者の情報および設定を表示できます。 |
| 共有の編集     | 共有コンテンツを編集できます。     |
| Analytics | インタラクティブ分析を使用できます。  |
| ダッシュボード   | ダッシュボードを表示できます。     |

- 7 (オプション) 右側の [データ セット] リストから、ユーザー ロールに関連付けるデータ セットを選択します。
- 8 [保存] をクリックします。

## vRealize Log Insight からのユーザー アカウントまたはグループの削除


ユーザー アカウントまたはグループを、vRealize Log Insight の管理ユーザー インターフェイスから削除できます。

ユーザー アカウントとグループは、[アクセス制御] ページの別の表にリストされています。検索フィルタを使用して、特定のユーザー アカウントを見つけることができます。グループを削除すると、そのグループに属するすべてのユーザーは、そのグループによって与えられた権限を失います。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[アクセス コントロール] をクリックします。
- 3 [ユーザーおよびグループ] をクリックします。
- 4 削除するユーザー名またはグループの横にあるチェック ボックスを選択します。
- 5 アカウントまたはグループを削除するには、[ユーザー アカウントまたはグループ] の表の上部にある [X 削除] をクリックします。



## 認証の設定

展開ではいくつかの認証方法を使用できます。

認証方法には、ローカル認証、VMware Identity Manager 認証、および Active Directory 認証が含まれます。同じ展開で複数の方法を使用することができ、ユーザーがログイン時に使用する認証のタイプを選択します。

vRealize Log Insight のダウンロード ページには、適切なバージョンの VMware Identity Manager のダウンロード リンクが含まれています。VMware Identity Manager には、次の機能が含まれています。

- Active Directory や LDAP など、既存のディレクトリに対してユーザーを認証するためのディレクトリ統合。
- シングル サインオン機能をサポートするその他の VMware 製品とのシングル サインオン統合。
- ADFS、Ping Federate など、いくつかのサードパーティ ID プロバイダとのシングル サインオン。
- RSA SecurID、Entrust などのサードパーティ製ソフトウェアとの統合による 2 要素認証。VMware Verify による 2 要素認証が含まれています。

ローカル認証は、vRealize Log Insight のコンポーネントです。ローカル認証を使用するには、ローカル ユーザーを作成してパスワードを設定し、vRealize Log Insight サーバに保存します。製品の管理者は、vRealize Log Insight および Active Directory を有効に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。

- [VMware Identity Manager によるユーザー認証の有効化](#)
- [Active Directory を介したユーザー認証の有効化](#)

### VMware Identity Manager によるユーザー認証の有効化

管理者は、vRealize Log Insight での VMware Identity Manager 認証を有効にすることができます。

VMware Identity Manager 認証を利用すると、同じ Identity Manager を使用するすべての VMware 製品でユーザーがシングル サインオンできます。


Active Directory と VMware Identity Manager サーバが同期されると、Active Directory ユーザーも VMware Identity Manager で認証できます。同期の詳細については、VMware Identity Manager のドキュメントを参照してください。

VMware Identity Manager との統合を利用できるのは、ローカル ユーザーのみです。VMware Identity Manager でテナント管理者ロールが割り当てられている Active Directory ユーザーは、vRealize Log Insight との統合を利用できる対象ではありません。

## 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

## 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] の [認証] をクリックします。
- 3 [シングル サインオンを有効にする] を選択します。
- 4 [ホスト] テキスト ボックスに、ユーザーの認証に使用する VMware Identity Manager インスタンスのホスト識別子を入力します。

たとえば、 **company-name.vmwareidentity.com** などです。

- 5 [API ポート] テキスト ボックスでは、VMware Identity Manager インスタンスとの接続に使用するポートを指定します。デフォルトは 443 です。
- 6 オプションで、VMware Identity Manager のテナントを入力します。テナントを入力する必要があるのは、VMware Identity Manager の [パスのテナント] としてテナント モードが設定されている場合のみです。
- 7 [ユーザー名] と [パスワード] のテキスト ボックスで、VMware Identity Manager ユーザー認証情報を指定します。

この情報は、VMware Identity Manager に vRealize Log Insight クライアントを作成するために、設定中に一度のみ使用されます。vRealize Log Insight のローカルには保存されません。ユーザーは、テナントに対して API コマンドを実行する権限を保有している必要があります。

- 8 [テスト接続] をクリックし、接続していることを確認します。
- 9 [URL ホストのリダイレクト] ドロップダウン メニューで、VMware Identity Manager での登録のためのリダイレクト URL で使用されるホスト名または IP アドレスを選択します。

統合ロード バランサに少なくとも 1 つの仮想 IP アドレスが定義されている場合、VMware Identity Manager は選択した仮想 IP アドレスにリダイレクトします。統合ロード バランサが定義されてない場合、代わりにマスター ノードの IP アドレスが使用されます。

- 10 VMware Identity Manager を介した Active Directory ユーザーのログインを許可するかどうかを選択します。  
VMware Identity Manager が Active Directory インスタンスと同期している場合、Active Directory ユーザー向けにこのオプションを使用できます。
- 11 [保存] をクリックします。

## Active Directory を介したユーザー認証の有効化


Active Directory を介してユーザーを認証すると、ユーザーは複数目的に共通のパスワードを使用することができ、ログイン プロセスを簡素化することができます。

子ドメインへのアクセスは Active Directory ではサポートされていません。このタイプのアクセスは VMware Identity Manager でのみサポートされています。

#### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] の [認証] をクリックします。
- 3 [Active Directory のサポートの有効化] を選択します。
- 4 [デフォルト ドメイン] テキスト ボックスにドメイン名を入力します。

たとえば、 **company-name.com** などです。

---

**注:** デフォルトのドメイン テキスト ボックスで複数のドメインを指定することはできません。指定したデフォルト ドメインが他のドメインから信頼されている場合、vRealize Log Insight はこのデフォルト ドメインおよびバインド ユーザーを使用して、信頼元のドメイン内の AD ユーザーおよびグループを検証します。子ドメインへのアクセスは Active Directory ではサポートされていません。

既にユーザーとグループが含まれている異なるドメインに切り替えると、既存のユーザーとグループに対する認証は失敗し、既存のユーザーによって保存されたデータは失われます。

---

- 5 ドメイン コントローラが地理位置情報を使用する、または、セキュリティで制限される場合、この vRealize Log Insight インスタンスに最も近いドメイン コントローラを手動で指定する必要があります。

---

**注:** ロード バランシングされた Active Directory の認証サーバはサポートされていません。

---

- 6 デフォルト ドメインに属するバインド ユーザーの認証情報を入力します。

vRealize Log Insight はデフォルト ドメインおよびバインド ユーザーを使用して、デフォルト ドメイン内、およびデフォルト ドメインを信頼しているドメイン内の AD ユーザーおよびグループを検証します。

- 7 接続タイプの値を指定します。

Active Directory の認証でこの接続を使用します。

- 8 [保存] をクリックします。

#### 次のステップ

vRealize Log Insight の現在のインスタンスにアクセスする権限を AD ユーザーおよびグループに付与します。

## Active Directory で使用するプロトコルの構成

Active Directory に接続する際に使用するプロトコルを構成できます。デフォルトでは、vRealize Log Insight が Active Directory に接続する場合、SSL LDAP を試してから、必要に応じて非 SSL LDAP を試します。

Active Directory 通信先を特定のプロトコルに限定する場合、または試行するプロトコルの順序を変更する場合は、vRealize Log Insight 仮想アプライアンスに追加の構成を適用する必要があります。

#### 前提条件

- vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。
- SSH 接続を有効にするには、TCP ポート 22 が開いていることを確認します。

#### 手順

- 1 vRealize Log Insight 仮想アプライアンスとの SSH 接続を確立し、root ユーザーとしてログインします。
- 2 次の場所へ移動します： `/storage/core/loginsight/config`
- 3 `[number]` が最も大きい最新の構成ファイルを見つけます： `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 4 最新の構成ファイルをコピーします： `/storage/core/loginsight/config/loginsight-config.xml#[number]`
- 5 `[number]` の値を増やし、次の場所に保存します： `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
- 6 ファイルを編集のために開きます。
- 7 Authentication セクションで、適用する構成に対応する行を追加します。

| オプション  | 説明                                       |
|--|--|
| <code>&lt;ad-protocols value="LDAP" /&gt;</code>       | SSL 非対応 LDAP を使用する場合専用                   |
| <code>&lt;ad-protocols value="LDAPS" /&gt;</code>      | SSL 対応 LDAP のみを使用する場合専用                  |
| <code>&lt;ad-protocols value="LDAP,LDAPS" /&gt;</code> | 最初に LDAP を使用し、次に SSL 対応 LDAP を使用する場合専用   |
| <code>&lt;ad-protocols value="LDAPS,LDAP" /&gt;</code> | 最初に LDAPS を使用し、次に SSL 非対応 LDAP を使用する場合専用 |

プロトコルを選択しない場合、vRealize Log Insight は LDAP を使用してから、SSL 対応 LDAP を使用します。

- 8 ファイルを保存して閉じます。
- 9 `service loginsight restart` コマンドを実行します。

# vRealize Log Insight の構成

vRealize Log Insight を構成およびカスタマイズしてデフォルト設定、ネットワーク設定を変更したり、ストレージリソースを調整することができます。システムの通知を構成することもできます。

この章には、次のトピックが含まれています。

- [vRealize Log Insight 構成制限](#)
- [仮想アプライアンスの設定](#)
- [vRealize Log Insight へのライセンスの割り当て](#)
- [ログストレージポリシー](#)
- [システム通知の管理](#)
- [vRealize Log Insight イベント転送ターゲットの追加](#)
- [vRealize Log Insight 仮想アプライアンスの時刻の同期](#)
- [vRealize Log Insight の SMTP サーバの構成](#)
- [カスタム SSL 証明書のインストール](#)
- [vRealize Log Insight Web セッションのデフォルトのタイムアウト期間の変更](#)
- [アーカイブしています](#)
- [vRealize Log Insight サービスの再起動](#)
- [vRealize Log Insight 仮想アプライアンスのパワーオフ](#)
- [vRealize Log Insight サポート バンドルのダウンロード](#)
- [VMware カスタム エクスペリエンス改善プログラムへの参加または参加取り消し](#)

## vRealize Log Insight 構成制限

vRealize Log Insight を構成する際には、サポートされる最大値以下にする必要があります。

表 4-1. vRealize Log Insight 構成の上限

| 項目                | 最大値            |
|-------------------|----------------|
| [ノード構成]           |                |
| CPU               | 16 vCPU        |
| メモリ               | 32 GB          |
| ストレージ デバイス (vmdk) | 2 TB - 512 バイト |

| 項目                          | 最大値   |
|-----------------------------|---|
| 指定可能な合計ストレージ                | 4 TB (+ OS ドライブ)<br>VMDK で指定可能なログ ストレージは最大 4TB で、1 台の最大サイズは 2TB です。2TB の VMDK を 2 台や 1TB の VMDK を 4 台などが可能です。最大サイズに達した場合、既存の仮想マシンにディスクを追加するのではなく、よりサイズの大きいクラスターでサイズを減らす必要があります。 |
| syslog 接続数                  | 750   |
| [クラスター構成]                   |   |
| ノード                         | 12 (マスター + 11 のワーカー)  |
| [ノードあたりの取り込み]               |   |
| 1 秒あたりのイベント数                | 15,000 eps  |
| syslog メッセージの長さ             | 10 KB (テキスト フィールド)  |
| 取り込み API HTTP POST 要求       | 16 KB (テキスト フィールド)、HTTP POST 要求あたり 4 MB   |
| [統合]                        |   |
| vRealize Operations Manager | 1   |
| vSphere vCenter Server      | ノードあたり 15   |
| Active Directory ドメイン       | 1   |
| E メール サーバ                   | 1   |
| DNS サーバ                     | 2   |
| NTP サーバ                     | 4   |
| フォワーダ                       | 10  |

## 仮想アプライアンスの設定

ストレージ、メモリ、CPU のキャパシティなど、仮想アプライアンスの設定を変更できます。

### vRealize Log Insight 仮想アプライアンス用の root の SSH パスワードの構成

仮想アプライアンスとの SSH 接続はデフォルトで無効になっています。VMware リモート コンソールから、または vRealize Log Insight 仮想アプライアンスを展開するときに、root の SSH パスワードを構成することができます。

ベスト プラクティスとして、vRealize Log Insight の .ova ファイルを展開するときに root の SSH パスワードを設定します。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。

また、VMware リモート コンソールから SSH を有効にし root のパスワードを設定することもできます。

#### 前提条件

vRealize Log Insight 仮想アプライアンスが展開され、実行していることを確認します。

#### 手順

- 1 vSphere Client インベントリで vRealize Log Insight 仮想アプライアンスをクリックし、[コンソール] タブを開きます。

- 2 スプラッシュ スクリーンで指定したキーの組み合わせを使用して、コマンド ラインに移動します。
- 3 コンソールで「**root**」と入力し、Enter を押します。パスワードを空のまま残して、Enter を押します。  
次のメッセージがコンソールに表示されます。パスワードの変更が要求されました。新しいパスワードを選択してください。
- 4 古いパスワードを空のまま残して、Enter を押します。
- 5 root ユーザーの新しいパスワードを入力し、Enter を押し、root ユーザーの新しいパスワードをもう一度入力して、Enter を押します。  
パスワードは 8 文字以上を指定する必要があります。大文字、小文字、数字、および特殊文字をそれぞれ 1 文字以上含める必要があります。同じ文字の繰り返し回数が 4 回を超えてはなりません。

次のメッセージが表示されます。パスワードが変更されました。

#### 次のステップ

root のパスワードを使用すると、vRealize Log Insight 仮想アプライアンスとの SSH 接続を確立できます。

## vRealize Log Insight 仮想アプライアンスのネットワーク設定の変更

vRealize Log Insight 仮想アプライアンスのネットワーク設定を変更するには、vSphere Client で vApp のプロパティを編集します。

vApp 構成の詳細については、<https://docs.vmware.com/jp/VMware-vSphere/index.html> を参照してください。

#### 前提条件

vApp のプロパティを編集する権限があることを確認します。

#### 手順

- 1 vRealize Log Insight 仮想アプライアンスをパワーオフします。
- 2 インベントリで vRealize Log Insight 仮想アプライアンスを右クリックし、[設定の編集] をクリックします。
- 3 [オプション] タブをクリックし、[vApp オプション] - [IP 割り当てポリシー] を選択します。
- 4 IP の割り当てオプションを選択します。

| オプション | 説明  |
|-------|---|
| 固定    | IP アドレスを手動で構成します。自動割り当てでは実行されません。   |
| 一時的   | vApp がパワーオンされると、IP アドレスは指定された範囲から、IP プールを使用して自動的に割り当てられます。アプライアンスがパワーオフされると、IP アドレスは解放されます。 |
| DHCP  | DHCP サーバを使用して IP アドレスが割り当てられます。DHCP サーバによって割り当てられたアドレスは、vApp で起動された仮想マシンの OVF 環境に表示されます。    |

- 5 (オプション) [固定] を選択した場合は、[vApp オプション] - [プロパティ] をクリックして、vRealize Log Insight vApp の IP アドレス、ネットマスク、ゲートウェイ、DNS、およびホスト名を割り当てます。

**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。

## 6 vRealize Log Insight vApp をパワーオンします。

### vRealize Log Insight 仮想アプライアンスのストレージ容量を増やす

ニーズの増加に応じて、vRealize Log Insight に割り当てるストレージリソースを増やすことができます。

ストレージ領域を増やすには、新しい仮想ディスクを vRealize Log Insight 仮想アプライアンスに追加します。必要な台数のディスクを追加できますが、指定可能なストレージの合計は最大 4 TB (+ OS ドライブ) です。合計は、2 つの 2 TB ディスクの組み合わせ、または 4 つの 1 TB ディスクの組み合わせのようにできます。 [vRealize Log Insight 構成制限](#) を参照してください。

#### 前提条件

- 環境内の仮想マシンのハードウェアを変更する権限を持ったユーザーとして vSphere Client にログインします。
- vRealize Log Insight 仮想アプライアンスを安全にシャットダウンします。 [vRealize Log Insight 仮想アプライアンスのパワーオフ](#) を参照してください。

#### 手順

- 1 vSphere Client のインベントリで vRealize Log Insight 仮想マシンを右クリックし、[設定の編集] を選択します。
- 2 [ハードウェア] タブで [追加] をクリックします。
- 3 [ハード ディスク] を選択して、[次へ] をクリックします。
- 4 [新規仮想ディスクを作成] を選択し、[次へ] をクリックします。

- a ディスク容量を入力します。

vRealize Log Insight は最大 2TB の仮想ハード ディスクをサポートします。さらに大きな容量が必要な場合は、複数の仮想ハード ディスクを追加します。

- b ディスク フォーマットを選択します。

| オプション                       | 説明  |
|-----------------------------|---|
| シック プロビジョニング (Lazy Zeroed)  | デフォルトのシック フォーマットで仮想ディスクを作成します。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。物理デバイスに常駐するデータは、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) | Fault Tolerance 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のタイプを作成します。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、物理デバイスに存在す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。<br><br>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、可能な場合は常にシックプロビジョニング (Eager Zeroed) のディスクを作成します。 |
| Thin Provision              | シン フォーマットのディスクを作成します。このフォーマットを使用してストレージ容量を節約します。  |

- c (必須) データストアを選択するには、データストアの場所を参照し、[次へ] をクリックします。



- 5 デフォルトの仮想デバイス ノードを受け入れ、[次へ] をクリックします。
- 6 情報を確認し、[終了] をクリックします。
- 7 [OK] をクリックして変更内容を保存し、ダイアログ ボックスを閉じます。

vRealize Log Insight 仮想アプライアンスをパワーオンすると、仮想マシンによって新しい仮想ディスクが検出され、デフォルトのデータ容量に自動的に追加されます。まず、仮想マシンを完全にパワーオフします。仮想アプライアンスのパワーオンの詳細については、<https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-6-pubs.html> を参照してください。

---

**注意:** 仮想アプライアンスに追加したディスクは安全に取り外すことができません。vRealize Log Insight 仮想アプライアンスからディスクを取り外すと、データが完全に損失してしまう場合があります。

---

## vRealize Log Insight 仮想アプライアンスへのメモリおよび CPU の追加

展開後に vRealize Log Insight 仮想アプライアンスに割り当てられたメモリのサイズおよび CPU 数を変更できません。

たとえば、使用環境のイベント数が増えた場合は、リソース割り当ての調整が必要になることがあります。

### 前提条件

- 環境内の仮想マシンのハードウェアを変更する権限を持ったユーザーとして vSphere Client にログインします。
- vRealize Log Insight 仮想アプライアンスを安全にシャットダウンします。 [vRealize Log Insight 仮想アプライアンスのパワーオフ](#) を参照してください。

### 手順

- 1 vSphere Client のインベントリで vRealize Log Insight 仮想マシンを右クリックし、[設定の編集] を選択します。
- 2 [ハードウェア] タブで [追加] をクリックします。
- 3 CPU 数およびメモリ サイズを必要に応じて調整します。
- 4 情報を確認し、[終了] をクリックします。
- 5 [OK] をクリックして変更内容を保存し、ダイアログ ボックスを閉じます。

vRealize Log Insight 仮想アプライアンスをパワーオンすると、仮想マシンは新しいリソースの利用を開始します。

## vRealize Log Insight へのライセンスの割り当て

vRealize Log Insight を使用するには、有効なライセンス キーと組み合わせる必要があります。

VMware の Web サイトから vRealize Log Insight をダウンロードするときに、評価ライセンスが取得されます。このライセンスの有効期間は 60 日です。評価ライセンスの有効期限が切れた後も引き続き vRealize Log Insight を使用するには、永続的ライセンスを割り当てる必要があります。

vRealize Log Insight オペレーティング システム インスタンス (OSI) ライセンス モデルは、非仮想化物理サーバまたは仮想マシン上のオペレーティング システムの単一インストールとして OSI を定義します。vRealize Log Insight の場合、OSI は、仮想化物理サーバ、ストレージアレイ、またはログ メッセージを生成できるネットワーク デバイスなど、IP アドレスによって識別される単一のシステムとすることもできます。

ホスト、サーバ、または他のソースが vRealize Log Insight へのログの送信を停止した場合、[ライセンス] 画面の OSI 数は保持期間中に変更されません。保持期間は、過去 12 か月間の OSI 数の平均として計算されるライセンスの使用状況に基づいています。


vRealize Log Insight Web ユーザー インターフェイスの [管理] セクションを使用して、vRealize Log Insight ライセンスのステータスを確認し、ライセンスを管理します。

ソリューション相互運用性の一部として、Standard、Advanced、または Enterprise エディションの VMware NSX ユーザーは、それぞれの NSX ライセンス キーを使用して vRealize Log Insight のライセンスを付与することができます。詳細については、VMware NSX のドキュメントを参照してください。

#### 前提条件

- 有効なライセンス キーは My VMware™ から取得します。
- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で [ライセンス] を選択します。
- 3 [ライセンス キー] テキスト ボックスにライセンス キーを入力して、[キーの設定] をクリックします。VMware NSX ライセンス キーがある場合は、ここに入力します。
- 4 ライセンスのステータスが [アクティブ] であること、およびライセンスのタイプと有効期限が正しいことを確認します。

## ログ ストレージ ポリシー

vRealize Log Insight 仮想アプライアンスは受信ログ用に最低 100GB のストレージを使用します。

vRealize Log Insight にインポートされたログのボリュームがストレージの上限に達すると、先に格納されたものが先に削除される方式に従い、古いログ メッセージが定期的に自動削除されます。vRealize Log Insight 仮想アプライアンスにストレージを追加して、ストレージの上限を増やすことができます。 [vRealize Log Insight 仮想アプライアンスのストレージ容量を増やす](#) を参照してください。

古いメッセージを保持するには、vRealize Log Insight のアーカイブ機能を有効にします。 [vRealize Log Insight で のデータ アーカイブの有効化または無効化](#) を参照してください。

vRealize Log Insight によって格納されたデータは変更できません。インポートされたログは、自動的に削除されない限り、削除できません。

## システム通知の管理

vRealize Log Insight には、たとえばディスク容量が枯渇しかけている場合や、古いログ ファイルが削除されようとしている場合など、vRealize Log Insight の健全性に関連するアクティビティについてのシステム通知が組み込まれています。管理者は、システム通知を送信する頻度と送信先を設定できます。

システム通知には、迅速な対応を必要とする重大な問題を通知する、応答が必要な警告を表示する、通常のシステムアクティビティを通知する、という機能があります。システム通知はアップグレード中は中断されますが、それ以外の場合は常に有効です。

管理者は、トリガされたときに通知を送信する頻度と、どのメール アドレスに送信するかを指定できます。vRealize Log Insight に関するシステム通知は、サードパーティのアプリケーションにも送信できます。

システム通知は、ユーザーによって定義されるアラート クエリとは異なります。アラート クエリの詳細については、[E メール通知を送信するためのアラート クエリを Log Insight に追加する](#)を参照してください。

## vRealize Log Insight のシステム通知

vRealize Log Insight はシステムの健全性について 2 種類の通知を提供します。1 つはすべての製品構成に適用される一般的な通知、もう 1 つはクラスタベース展開のクラスタに関連する通知です。

次の表に、vRealize Log Insight のシステム通知のリストとその説明を示します。

### 一般的なシステム通知

vRealize Log Insight は、アーカイブの障害やアラート スケジュールの遅延など、管理者の介入が必要な状態が発生すると通知を発行します。

| 通知名                    | 説明   |
|------------------------|--|
| 最も古いデータは間もなく検索できなくなります | <p>vRealize Log Insight は、検索可能なデータの予想サイズ、ストレージ容量、および現在の取り込み速度に基づいて、仮想アプライアンス ストレージから古いデータの廃止を開始します。廃止されたデータは、アーカイブが構成されている場合はアーカイブされ、アーカイブが構成されていない場合は削除されます。</p> <p>これに対処するには、ストレージを追加するか、リテンション通知のしきい値を調整します。詳細については、<a href="#">健全性通知を送信するように vRealize Log Insight を設定します</a>。を参照してください。</p> <p>vRealize Log Insight サービスが再起動されるたびに、通知が送信されます。</p>  |
| リボジトリ保持時間              | <p>保持期間は、vRealize Log Insight インスタンスのローカル ディスクにデータが保持される時間を表します。保持期間は、システムが保持できるデータ量と現在の取り込み速度によって決まります。たとえば、インデックスの作成後に 10 Gb/日のデータを受信し、容量が 300 GB の場合には、保存期間は 30 日になります。</p> <p>ストレージの制限に達すると、新しく取り込まれたデータを記録するため、古いデータが削除されます。これは、現在の取り込み速度で vRealize Log Insight が保存できる検索可能なデータの量が、仮想アプライアンス上で利用可能なストレージ容量を超えていることを通知します。</p> <p>[リテンション通知のしきい値] で設定した期間が過ぎる前にストレージが不足することがあります。ストレージを追加するか、リテンション通知のしきい値を調整します。</p> |

| 通知名  | 説明   |
|--|--|
| イベントが削除されました   | <p>vRealize Log Insight は、すべての受信ログ メッセージの取り込みに失敗しました。</p> <ul style="list-style-type: none"> <li>■ vRealize Log Insight サーバによる追跡中にいずれかの TCP メッセージがドロップした場合は、次に示す頻度でシステム通知が送信されます。 <ul style="list-style-type: none"> <li>■ 1 日に 1 回</li> <li>■ 手動か自動かを問わず、vRealize Log Insight サービスが再起動された場合</li> </ul> </li> <li>■ E メールには、前回の通知 E メールが送信された後にドロップしたメッセージの数、および vRealize Log Insight の前回の再起動以降にドロップしたメッセージの総数が記載されます。</li> </ul> <p>送信行の時間はメール クライアントで制御され、ローカル タイム ゾーンの時刻が表示されますが、Eメールの本文には UTC 時刻が表示されることに注意してください。</p> |
| インデックス バケットが破損しました   | <p>ディスク上のインデックスの一部が破損しています。インデックスが破損している場合は通常、基本となるストレージ システムに重大な問題が発生しています。インデックスの破損部分は、実行しているクエリから除外されます。破損したインデックスは新しいデータの取り込みに影響します。サービスを起動すると、vRealize Log Insight はインデックスの整合性を確認します。破損が検出された場合、vRealize Log Insight は次の頻度でシステム通知を送信します。</p> <ul style="list-style-type: none"> <li>■ 1 日に 1 回</li> <li>■ 手動か自動かを問わず、vRealize Log Insight サービスが再起動された場合</li> </ul>  |
| ディスクが不足しています   | <p>vRealize Log Insight の割り当てられたディスク容量が不足しています。ほとんどの場合、vRealize Log Insight でストレージ関連の問題が発生しています。</p>   |
| アーカイブ領域がいっぱいです   | <p>間もなく、vRealize Log Insight データをアーカイブするために使用される NFS サーバのディスクの空き容量がなくなります。</p>   |
| ディスク容量の合計サイズが変更されました   | <p>vRealize Log Insight データ ストレージのパーティションの合計サイズが減少しています。通常は、基本となるストレージ システムで重大な問題が発生しています。vRealize Log Insight はこの状況を検出すると、次の頻度でこの通知を送信します。</p> <ul style="list-style-type: none"> <li>■ ただちに</li> <li>■ 1 日に 1 回</li> </ul>   |
| アーカイブが保留されています   | <p>vRealize Log Insight は期待したとおりにデータをアーカイブできません。通常は、データ アーカイブ用に構成された NFS ストレージに問題が発生しています。</p>   |
| ライセンスが間もなく期限切れになります  | <p>vRealize Log Insight のライセンスが間もなく期限切れになります。</p>  |
| ライセンスは期限切れです   | <p>vRealize Log Insight のライセンスが期限切れになっています。</p>  |
| AD サーバに接続できません   | <p>vRealize Log Insight は構成された Active Directory サーバに接続できません。</p>   |
| High Availability の IP アドレス <IP Address> は、既に別のマシンで保持されているため引き継ぐことができません | <p>vRealize Log Insight クラスタが統合ロード バランサ (ILB) の設定済み IP アドレスを引き継ぐことができませんでした。この通知の最も一般的な理由は、同じネットワーク内の別のホストが IP アドレスを保持しているため、クラスタが IP アドレスを引き継ぐことができないことです。</p> <p>この競合は、現在その IP アドレスを保持しているホストからアドレスを解放するか、Log Insight の統合ロード バランサに、ネットワーク内で使用可能な固定 IP アドレスを構成するかのいずれかの方法で解決できます。ILB の IP アドレスを変更する場合は、新しい IP アドレスまたはこの IP アドレスに解決される FQDN/URL に宛ててログを送信するように、すべてのクライアントを必ず再構成するようにします。また、[vSphere 統合] ページで、vRealize Log Insight と統合されたすべての vCenter Server の構成を一度解除してから、再構成する必要があります。</p>                                 |

| 通知名  | 説明  |
|--|---|
| High Availability の IP アドレス <IP Address> は、ノードの障害が多すぎるため使用できません              | <p>統合ロード バランサ (ILB) の設定済み IP アドレスを使用できません。つまり、ILB IP アドレス、またはこの IP アドレスに解決される FQDN/URL を介して vRealize Log Insight クラスタにログを送信しようとするクライアントには、その IP アドレスが使用できないものとして表示します。この通知の最も一般的な理由は、vRealize Log Insight クラスタの大多数のノードが、健全でない、利用できない、またはマスターノードからアクセスできない状態であることです。また、これ以外の一般的な原因としては、NTP の時刻同期が有効になっていない場合や、構成されている各 NTP サーバの時刻に著しい誤差があることなどが挙げられます。問題が解消されたかどうかを確認するには、その IP アドレスに対して（可能な場合は）ping を実行して、そのアドレスが到達可能かどうかを確認できます。</p> <p>この問題は、クラスタ ノードの大半を健全で到達可能な状態にし、NTP の時刻同期を有効にして NTP サーバ間での誤差をなくすようにすることで解決できます。</p> |
| vRealize Log Insight ノード間での、High Availability IP アドレス [IP Address] の移行が多すぎます | <p>統合ロード バランサ (ILB) 用に構成された IP アドレスが直近の 10 分間で移行された回数が多すぎます。</p> <p>通常の操作では、IP アドレスが vRealize Log Insight クラスタ ノード間で移動されることはほとんどありません。しかし、現在の所有者ノードが再起動されたりメンテナンス モードになった場合には、IP アドレスが移動される場合があります。これ以外に、Log Insight クラスタ ノード間で時刻同期が行われていないことも理由の 1 つとして考えられます。この処理は、クラスタが適切に機能するために欠かすことができません。後者の場合は、NTP の時刻同期を有効にして NTP サーバ間での誤差をなくすようにすることで、問題を解決できます。</p>  |
| SSL 証明書エラー   | <p>Syslog ソースが SSL 経由で vRealize Log Insight への接続を開始しましたが、突然接続を終了しました。これは、syslog ソースが SSL 証明書の有効性を確認できなかったことを示している可能性があります。vRealize Log Insight が SSL を介して Syslog メッセージを受け取るためには、クライアントによって検証された証明書が必要となり、システムのクロックが同期されている必要があります。SSL 証明書またはネットワーク タイム サービスに問題が発生している可能性があります。</p> <p>SSL 証明書が Syslog ソースによって信頼されることを検証し、SSL を使用しないようにソースを再構成するか、SSL 証明書を再インストールすることができます。</p> <p><a href="#">vRealize Log Insight エージェントの SSL パラメータの構成およびカスタム SSL 証明書のインストール</a>を参照してください。</p>   |
| vCenter の収集の失敗   | <p>vRealize Log Insight は vCenter Server イベント、タスク、およびアラームを収集できません。収集の失敗の原因となったエラーを正確に特定し、収集機能が動作しているかを確認するには、<code>/storage/var/loginsight/plugins/vsphere/li-vsphere.log</code> ファイルを調べます。</p>   |
| イベントの転送イベントをドロップしました   | <p>フォワードは接続または過負荷の問題のためにイベントをドロップします。</p> <p>例：</p> <pre>Log Insight Admin Alert: Event Forwarder Events Dropped This alert is about your Log Insight installation on https://&lt;your_url&gt;  Event Forwarder Events Dropped triggered at 2016-08-02T18:41:06.972Z  Log Insight just dropped 670 events for forwarder target 'Test', reason: Pending queue is full.</pre>   |

| 通知名                 | 説明  |
|---------------------|---|
| スケジュールより遅れたアラート クエリ | vRealize Log Insight は設定された時刻にユーザー定義のアラートを実行できませんでした。遅延の理由は、1 つ以上の非効率なユーザー定義のアラート クエリがあるか、またはシステムが取り込みおよびクエリ ロード向けに適切にサイズ調整されていないためである可能性があります。 |
| 自動的に無効になったアラート      | ユーザー定義のアラートが 10 回以上実行され、その平均実行時間が 1 時間を超える場合、アラートは非効率とみなされ、その他のユーザー定義のアラートに影響するのを防ぐために無効になります。  |
| 非効率なアラート クエリ        | ユーザー定義のアラートの完了に 1 時間以上かかる場合、アラートは非効率とみなされます。  |

## クラスタのシステム通知

vRealize Log Insight は、新しいクラスタ メンバーの追加や一時的なノード通信の問題など、クラスタ トポロジの変更に関する通知を送信します。

| 送信元      | 通知名                                  | 説明   |
|----------|--------------------------------------|--|
| マスター ノード | 新しいワーカー ノードに承認が必要でした                 | ワーカー ノードがクラスタに参加するための要求を送信しています。管理者ユーザーは、要求を承認または拒否する必要があります。  |
| マスター ノード | 新しいワーカー ノードが承認されました                  | 管理者ユーザーがワーカー ノードからの vRealize Log Insight クラスタに参加するためのメンバーシップ要求を承認しました。   |
| マスター ノード | 新しいワーカー ノードが拒否されました                  | 管理者ユーザーがワーカー ノードからの vRealize Log Insight クラスタに参加するためのメンバーシップ要求を拒否しました。要求が誤って拒否された場合、管理者ユーザーはワーカー ノードから要求を再送信して、マスター ノードで承認することができます。 |
| マスター ノード | ワーカー ノードが増えたためサポートされている最大ノード数を超過しました | 新しいワーカー ノードが原因で Log Insight クラスタ内のワーカー ノードの数がサポートされている最大数を超過しました。  |
| マスター ノード | 許可されているノード数を超過し、新しいワーカー ノードが拒否されました  | 管理者ユーザーがクラスタに最大許容数を超過したノードを追加しようとして、ノードが拒否されました。   |
| マスター ノード | ワーカー ノードが切断されました                     | 以前に接続されたワーカー ノードが vRealize Log Insight クラスタから切断されました。  |
| マスター ノード | ワーカー ノードが再接続されました                    | ワーカー ノードが vRealize Log Insight クラスタに再接続されました。  |
| マスター ノード | ワーカー ノードが管理者によって失効されました              | 管理者ユーザーによってワーカー ノードのメンバーシップが失効され、そのノードが vRealize Log Insight クラスタの一部ではなくなりました。   |

| 送信元      | 通知名                             | 説明  |
|----------|---------------------------------|---|
| マスター ノード | 不明なワーカー ノードが拒否されました             | ワーカー ノードがマスターにとって不明であるため、vRealize Log Insight マスター ノードがワーカー ノードからの要求を拒否しました。ワーカーが有効なノードであり、クラスタに追加する必要がある場合は、ワーカー ノードにログインし、 <code>/storage/core/loginsight/config/</code> 内のトークン ファイルおよびユーザー構成を削除して、ワーカー ノードで <code>restart loginsight service</code> を実行します。                    |
| マスター ノード | ワーカー ノードがメンテナンス モードになりました       | ワーカー ノードがメンテナンス モードになったため、設定の変更を受信してクエリを実行するには、管理者ユーザーはワーカー ノードをメンテナンス モードから削除する必要があります。  |
| マスター ノード | ワーカー ノードがサービス状態に戻りました           | メンテナンス モードが終了し、ワーカー ノードがサービス状態に戻りました。   |
| ワーカー ノード | マスターに障害が発生したか、ワーカー ノードから切断されました | <p>通知を送信するワーカー ノードが vRealize Log Insight マスター ノードに接続できません。これは、マスター ノードに障害が発生していて、再起動が必要なことを示している可能性があります。マスター ノードに障害が発生した場合は、オンラインに戻るまでクラスタを構成できず、クエリを送信することもできません。ワーカー ノードはメッセージの取り込みを継続します。</p> <p><b>注:</b> 多数のワーカーがマスター ノードの障害を個別に検出して通知する可能性があるため、このような通知を多数受信することがあります。</p> |
| ワーカー ノード | マスターがワーカー ノードに接続しました            | 通知を送信するワーカー ノードが vRealize Log Insight マスター ノードに再接続されました。  |

## vRealize Log Insight システム通知の宛先の設定

管理者ユーザーは、システム通知がトリガされたときの vRealize Log Insight のアクションを設定できます。

重要なシステム イベントが発生すると、vRealize Log Insight はシステム通知を生成します。たとえば、ディスク容量がほとんどいっぱい、vRealize Log Insight が古いログ ファイルの削除やアーカイブを開始する必要がある場合などです。

管理者は、これらのイベントに関する E メール通知を送信するように vRealize Log Insight を構成できます。システム通知 Eメールの送信元アドレスの構成は、管理 UI の [SMTP 構成] ページにある [送信者] テキスト ボックスを使用して管理者ユーザーが行います。 [vRealize Log Insight の SMTP サーバの構成](#)を参照してください。

管理者ユーザーは、サードパーティのアプリケーションに通知を送信することもできます。 [Webhook を使用してサードパーティ製品へのシステム通知送信について](#)を参照してください。

### 健全性通知を送信するように vRealize Log Insight を設定します。

管理者は自身の健全性に関連する通知を送信するように vRealize Log Insight を構成できます。




E メール メッセージを配信できない場合、Web インターフェイスにエラーが通知されます。

#### 前提条件

- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。
- vRealize Log Insight の SMTP サーバが構成されていることを確認します。詳細については、 [vRealize Log Insight の SMTP サーバの構成](#) を参照してください。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] で、[全般] をクリックします。
- 3 [アラート] ヘッダーでシステム通知を設定します。
  - a [E メールによるシステム通知の送信先] テキスト ボックスに通知先のメール アドレスを入力します。  
複数の E メール アドレスを入力する場合は、カンマで区切ります。
  - b [リテンション通知のしきい値] チェック ボックスを選択して、通知をトリガするしきい値を設定します。  
システムが保持できるデータ量が指定された期間に不足すると、通知が送信されます。この値は、現在の取り込み速度に基づいて計算されます。
- 4 [保存] をクリックします。
- 5 [Log Insight の再起動] をクリックして変更を適用します。

### サードパーティ製品に対する vRealize Log Insight システム通知の構成


管理者は自身の健全性に関連する通知をサードパーティ アプリケーションに送信するように vRealize Log Insight を構成できます。

重要なシステム イベントが発生すると、vRealize Log Insight はこれらの通知を生成します。たとえば、ディスク容量がほぼ枯渇していて、vRealize Log Insight が古いログ ファイルの削除を開始する必要がある場合などです。

#### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] で、[全般] をクリックします。



### 3 [アラート] ヘッダーでシステム通知を設定します。

- a [HTTP Post システム通知の送信先] テキスト ボックスに通知先の URL を入力します。
- b (オプション) [容量が以下を下回ると通知を送信] チェック ボックスおよび関連するしきい値が環境に合わせて正しく構成されていることを確認します。

### 4 [保存] をクリックします。

#### 次のステップ

通知に対する Webhook 出力を操作し、shim を作成して vRealize Log Insight Webhook フォーマットをサードパーティ アプリケーションによって使用されるフォーマットにマップします。

#### Webhook を使用してサードパーティ製品へのシステム通知送信について

Webhook を使用してサードパーティ製品に vRealize Log Insight システム通知を送信することができます。

vRealize Log Insight は、Webhook を使用して HTTP POST 経由で他のアプリケーションにアラートを送信します。vRealize Log Insight は Webhook を独自のフォーマットで送信しますが、サードパーティのソリューションは受信する Webhook が専用のフォーマットであると想定します。vRealize Log Insight Webhook で送信される情報を使用するには、サードパーティ アプリケーションが vRealize Log Insight のフォーマットをネイティブでサポートするか、vRealize Log Insight のフォーマットとサードパーティによって使用されるフォーマットの間に shim を使用してマッピングを作成する必要があります。shim は、vRealize Log Insight のフォーマットを別のフォーマットに変換またはマップします。

vRealize Log Insight Webhook の実装により、リモート サーバに対して送信 HTTP 要求が実行されます。サーバは「成功」または「失敗」のいずれかを報告し、失敗の場合、vRealize Log Insight は再試行します。すべての HTTP/2xx ステータス コード応答は「成功」として扱われ、その他のすべての応答（タイムアウトおよび接続拒否を含む）は「失敗」として扱われて後で再試行されます。

メッセージ クエリにより作成されるアラート、集約クエリにより作成されるアラート、およびシステム通知には、それぞれ専用の Webhook フォーマットがあります。

HTTP 基本認証がサポートされています。認証情報は、`{{https://username:password@hostname/path}}` の形式で URL に組み込みます。

#### システム通知の Webhook フォーマット

vRealize Log Insight Webhook のフォーマットは、作成されるクエリのタイプに依存します。システム通知、ユーザー アラート メッセージ クエリ、および集約ユーザー クエリから生成されたアラートにはそれぞれ異なる Webhook フォーマットがあります。

システム通知を送信するように vRealize Log Insight を構成するには、vRealize Log Insight 管理者である必要があります。

サードパーティ プログラムにシステム通知を送信する場合は、vRealize Log Insight 情報がサードパーティ プログラムのフォーマットによって理解できるように shim を記述する必要があります。

## システム通知の Webhook フォーマット

次の例は、システム通知の vRealize Log Insight Webhook フォーマットを示します。

```
{
  "AlertName": " Admin Alert: Worker node has returned to service  (Host = 127.0.0.2)",
  "messages": [
    {
      "text": "This notification was generated from Log Insight node (Host = 127.0.0.2,
Node Identifier = a31cad22-65c2-4131-8e6c-27790892a1f9).
A worker node has returned to service after having been in maintenance mode.
The Log Insight master node reports that worker node has finished maintenance
and exited maintenance mode. The node will resume receiving configuration changes and
serving queries. The node is also now ready to start receiving incoming log messages."

      "timestamp": 1458665320514, "fields": []
    }
  ]
}
```

## vRealize Log Insight イベント転送ターゲットの追加

入力イベントを Syslog または取り込み API ターゲットに転送するように vRealize Log Insight サーバを構成できます。

フィルタされたイベントやタグ付されたイベントを vRealize Log Insight や Syslog（またはその両方）など、1 つ以上のリモート転送先に送信するには、イベント転送を使用します。イベント転送は、既存のログ収集ツール（SIEM など）のサポートや、異なるネットワーク（DMZ や WAN など）のログ収集の統合に利用できます。

イベント転送は、スタンドアロンで使用することも、クラスタ化することもできますが、リモート転送先とは分離されたインスタンスです。イベント転送用に構成されたインスタンスは、イベントをローカルに保存したり、データをクエリする際に使用します。

[転送されたイベント] ページのフィルタは、インタラクティブ分析のフィルタとは異なります。[インタラクティブ分析での実行] メニュー項目を使用してイベント フィルタの結果をプレビューする方法については、[インタラクティブ分析でのイベント転送フィルタの使用](#)を参照してください。


### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

転送先が転送されたイベント数を処理できることを確認します。転送先のクラスタが転送元インスタンスよりもかなり小さい場合には、いくつかのイベントが失われる可能性があります。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。

- 2 [管理] で、[イベント転送] をクリックします。
- 3  [新しい転送先] をクリックして次の情報を入力します。

| オプション   | 説明  |
|---------|---|
| 名前      | 新しい転送先の一意な名前。   |
| ホスト     | IP アドレスまたは完全修飾ドメイン名。<br><br><b>注意:</b> 転送ループとは、vRealize Log Insight クラスタがイベントを自分自身に転送したり、一度他のクラスタに転送して、そのクラスタから元のクラスタにイベントが再度転送される構成のことです。このようなループは、転送される各イベントのコピーを無限に作成する場合があります。vRealize Log Insight の Web インターフェイスでは、イベントを自分自身に転送するように構成することはできません。しかし vRealize Log Insight は、vRealize Log Insight クラスタ A からクラスタ B にイベントを転送し、同じイベントを B から A に再度転送するような間接的な転送ループを防ぐことはできません。転送先を作成するときは、間接的な転送ループが作成されないように注意してください。  |
| プロトコル   | <p>取り込み API または syslog。デフォルト値は取り込み API (CFAPI) です。</p> <p>イベントが取り込み API を使用して転送されるときには、イベントの元のソースが [ソース] フィールドに保持されます。イベントが Syslog を使用して転送される場合は、イベント転送元の値はなくなり、メッセージの転送元は、受信者側で vRealize Log Insight のフォワードの IP アドレスまたはホスト名として記録される場合があります。</p> <p><b>注:</b> ソース フィールドには、イベント フォワードで選択したプロトコルに応じて異なる値が含まれている可能性があります。</p> <ul style="list-style-type: none"> <li>a 取り込み API の場合、ソースは初期送信者（イベント発信者）の IP アドレスです。</li> <li>b syslog の場合、ソースはイベント転送の vRealize Log Insight インスタンス IP アドレスです。また、Syslog メッセージテキストには、初期送信者の IP アドレスを参照する <code>_li_source_path</code> が含まれています。</li> </ul> |
| SSL を使用 | <p>オプションで、取り込み API の接続を SSL によって保護することができます。リモートサーバの信頼されるルートが検証され、SSL を使用したイベント転送は、デフォルトでターゲットサーバにインストールされた自己署名証明書では機能しません。信頼されない場合は、リモートサーバの信頼されたルート証明書を転送元のキーストアにインポートします。<a href="#">SSL を使用した vRealize Log Insight イベント転送の構成</a>を参照してください。</p>  |
| タグ      | <p>オプションで、事前定義済みの値を持つタグ ペアを追加することができます。タグを使用すると、イベントをより簡単にクエリすることができます。複数のカンマ区切りのタグを追加できます。</p>   |
| 補助タグを転送 | <p>Syslog の補助タグを転送するかどうかを選択できます。</p> <p>補助タグはクラスタ自身が追加されたタグです（[vc_username]、[vc_vmname] など）。ソースから直接受信したタグと一緒に転送できます。取り込み API を使用すると、補助タグが常に転送されます。</p>  |
| 転送      | <p>Syslog の転送プロトコルを選択します。UDP または TCP を選択できます。</p>   |

#### 4 (オプション) 転送するイベントを制御するには、[フィルタの追加] をクリックします。

フィールドおよび制約を選択して、目的のイベントを定義します。静的フィールドのみをフィルタとして使用できます。フィルタを選択しない場合は、すべてのイベントが転送されます。[インタラクティブ分析での実行] をクリックして、作成しているフィルタの結果を表示できます。

| 演算子     | 説明  |
|---------|---|
| 一致する    | 指定した文字列およびワイルドカードの仕様と一致する文字列を検索します。* はゼロ文字以上、? は、ゼロまたは任意の 1 文字を意味します。プリフィックスとポストフィックスのグローピングがサポートされます。<br>たとえば、 <b>*test*</b> は <b>test123</b> や <b>my-test-run</b> などの文字列に一致します。   |
| 一致しない   | 指定した文字列およびワイルドカードの仕様と一致する文字列を除外します。* はゼロ文字以上、? は、ゼロまたは任意の 1 文字を意味します。プリフィックスとポストフィックスのグローピングがサポートされます。<br>たとえば、 <b>test*</b> は <b>test123</b> を除外しますが、 <b>mytest123</b> は除外しません。 <b>%test*</b> は <b>test123</b> を除外しませんが、 <b>xtest123</b> は除外します。 |
| 次で開始する  | 指定した文字列で開始する文字列を見つけます。<br>たとえば、 <b>test</b> は <b>test123</b> または <b>test</b> を見つけますが、 <b>my-test123</b> は見つけません。  |
| 次で開始しない | 指定した文字列で開始する文字列を除外します。<br>たとえば、 <b>test</b> は <b>test123</b> を除外しますが、 <b>my-test123</b> は除外しません。  |

#### 5 (オプション) 次の転送情報を変更するには、[詳細設定を表示] をクリックします。

| オプション      | 説明  |
|------------|---|
| ポート        | リモート ターゲットにあるイベントの送信先ポート。デフォルト値は、プロトコルに基づいて設定されます。リモート ターゲットが別のポートで待機しているのではない限り、これは変更しないでください。   |
| ディスク キャッシュ | 転送対象として構成するバッファリング イベント用に確保するためのローカル ディスク容量のサイズ。バッファリングは、リモート ターゲットを使用できない場合、または、リモート ターゲットに送信されるイベントをそのリモート ターゲットが処理できない場合に使用されます。ローカル バッファがいっぱいになっても、リモート 転送先が利用できない場合、最新のローカル イベントがドロップされます。リモート 転送先がオンラインに戻っても、リモート 転送先には転送されません。デフォルト値は 200 MB です。 |
| ワーカー数      | 同時に使用できる送信接続数。転送先に対するネットワーク遅延や 1 秒あたりの転送イベント数が多い場合は、ワーカー数に大きい値を設定します。デフォルト値は 8 です。  |

#### 6 構成を確認するには、[テスト] をクリックします。

#### 7 [保存] をクリックします。

#### 次のステップ

- [SSL を使用した vRealize Log Insight イベント転送の構成](#)。
- イベント転送先は編集または複製できます。転送先を編集してイベント転送元名を変更すると、すべての統計がリセットされます。

## SSL を使用した vRealize Log Insight イベント転送の構成

SSL を使用して、Ingestion API ターゲット経由で入カイベントを別の Log Insight サーバに転送するように vRealize Log Insight サーバを構成できます。

### 前提条件

SSL を使用したイベント転送は、デフォルトでターゲット サーバにインストールされた自己署名証明書では機能しません。[証明書署名要求の生成](#)の手順を使用して、カスタムの SSL 証明書を作成してアップロードする必要があります。[カスタム SSL 証明書のインストール](#)を参照してください。

### 手順

- 1 信頼済みルート証明書を転送インスタンスの一時ディレクトリにコピーします。たとえば、/home です。
- 2 転送インスタンスに対する SSH を設定し、次のコマンドを実行します。

```
localhost:~ # cd /usr/java/default/lib/security/
localhost:/usr/java/default/lib/security # ../../bin/keytool
-import -alias loginsight -file /home/cacert.crt -keystore cacerts
```

デフォルトのキーストア パスワードは **changeit** です。

---

**注:** Java バージョンは時間の経過とともに異なります。

---

- 3 vRealize Log Insight インスタンスを再開します。

vRealize Log Insight クラスタ環境を使用している場合は、同じ証明書が格納されているすべてのノードでこの操作を実行する必要があります。

### 次のステップ

SSL 接続を有効にします。[SSL 専用接続の強制](#)を参照してください。

## インタラクティブ分析でのイベント転送フィルタの使用

イベント フィルタで使用される演算子とインタラクティブ分析のフィルタで使用される演算子の名前には 1 対 1 の対応関係がありません。ただし、どちらの形式でも同様の結果を生成する演算子を選択することができます。

この違いは、[イベントの転送] ページから [インタラクティブ分析での実行] メニュー項目を使用する場合に重要です。たとえば、[matches]\*foo\* のイベント転送フィルタがあり、イベント フィルタ ページから [インタラクティブ分析での実行] メニュー項目を選択した場合、インタラクティブ分析のクエリはこのイベント転送フィルタが、すべての同一イベントと一致しない可能性がある [match regexp]^.\*foo.\* \$ と同一であるとみなします。

もう 1 つの例は [matches]foo で、これはインタラクティブ分析で実行するときに contains foo として扱われます。インタラクティブ分析機能はキーワード クエリも検索するので、[contains]foo は、[matches]foo と比べてより多くのイベントと一致する可能性があります。

これらの違いに対処するためにインタラクティブ分析で使用される演算子を変更することができます。

- [contains] 演算子を [matches regex] に変更します。
- イベント転送フィルタの \* を [.\*] に変更し、フィルタする文字の先頭に [.\*] を追加します。たとえば、イベントフィルタ式 [matches]\*foo\* を [matches regex].\*foo.\* に変更します。
- イベント フィルタの [does not match] 演算子の場合、正規表現の先読み値を持つ [matches regex] 演算子を使用できます。たとえば、[does not match]\*foo\* は [matches regex].\*(?foo).\* と同等です。

## vRealize Log Insight 仮想アプライアンスの時刻の同期

vRealize Log Insight 仮想アプライアンスの時刻を NTP サーバと同期するか、仮想アプライアンスが展開された ESX/ESXi ホストと同期する必要があります。


vRealize Log Insight の主要機能にとって時間は重要です。

デフォルトでは、vRealize Log Insight は事前に定義されたパブリック NTP サーバのリストと時刻を同期します。ファイアウォールによってパブリック NTP サーバへのアクセスが禁止されている場合は、会社内の NTP サーバを使用できます。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が展開された ESX/ESXi ホストと時刻を同期できます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] の[時刻] をクリックします。
- 3 [時刻の同期先] ドロップダウン メニューで時間ソースを選択します。

| オプション        | 説明  |
|--------------|---|
| NTP サーバ      | vRealize Log Insight 仮想アプライアンスの時刻を、リスト内のいずれかの NTP サーバと同期します。          |
| ESX/ESXi ホスト | vRealize Log Insight 仮想アプライアンスの時刻を仮想アプライアンスが展開された ESX/ESXi ホストと同期します。 |

- 4 (オプション) NTP サーバとの同期を選択した場合は、NTP サーバのアドレスを指定して、[テスト] をクリックします。

**注:** NTP サーバとの接続テストには、サーバあたり最大で 20 秒かかることがあります。

- 5 [保存] をクリックします。

## vRealize Log Insight の SMTP サーバの構成


vRealize Log Insight から E メール通知を送信できるように SMTP を設定できます。

vRealize Log Insight が重要なシステム イベントを検出すると、システム通知が生成されます。たとえば、仮想アプライアンスのストレージ容量が設定されたしきい値に達した場合などです。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] の[SMTP] をクリックします。
- 3 SMTP サーバ アドレスとポート番号を入力します。
- 4 SMTP サーバで暗号化接続が使用されている場合は、暗号化プロトコルを選択します。
- 5 [送信者] テキスト ボックスに、システム通知を送信するときに使用するメール アドレスを入力します。  
システム通知 E メール差出人アドレスとして [送信者] のアドレスが表示されます。このアドレスは実際のアドレスでなくてもかまいません。vRealize Log Insight の特定のインスタンスを表すアドレスを指定できます。たとえば、**loginsight@example.com** などです。
- 6 システム通知を送信するときに SMTP サーバで認証するユーザー名およびパスワードを入力します。
- 7 ターゲット E メールを入力し、[テスト メールの送信] をクリックして接続を確認します。
- 8 [保存] をクリックします。

## カスタム SSL 証明書のインストール

デフォルトでは、vRealize Log Insight は自己署名の SSL 証明書を仮想アプライアンスにインストールします。

自己署名証明書があると、vRealize Log Insight Web ユーザー インターフェイスに接続する際にセキュリティ警告が生成されます。自己署名のセキュリティ証明書を使用しない場合は、カスタム SSL 証明書をインストールします。カスタム SSL 証明書が必要な機能は、SSL を介したイベント転送のみです。ILB が有効になっているクラスタ構成がある場合は、[統合ロード バランサの有効化](#) のカスタム SSL 証明書の特定要件を参照してください。

---

**注:** vRealize Log Insight Web ユーザー インターフェイスと Log Insight Ingestion プロトコル cfapi は、認証に同じ証明書を使用します。

---

## 前提条件

- カスタム SSL 証明書が次の要件を満たしていることを確認します。
  - CommonName に、仮想 IP アドレスのマスター ノードや FQDN のワイルドカードまたは完全一致が含まれている。オプションで、その他のすべての IP アドレスと FQDN が subjectAltName としてリストされている。
  - 証明書ファイルに有効なプライベート キーと有効な証明書チェーンが含まれている。
  - プライベート キーが RSA または DSA アルゴリズムで生成されている。
  - プライベート キーがパス フレーズで暗号化されていない。
  - 証明書に他の証明書のチェーンによる署名がある場合は、インポートする証明書ファイルにその他のすべての証明書が含まれます。
  - 証明書ファイルに含まれているすべての証明書およびプライベート キーは、PEM 形式にエンコードされています。vRealize Log Insight は、DER 形式にエンコードされた証明書およびプライベートキーをサポートしていません。
  - 証明書ファイルに含まれているすべての証明書およびプライベート キーは、PEM 形式になっています。vRealize Log Insight は、PFX、PKCS12、PKCS7、またはその他の形式の証明書をサポートしていません。
- 各証明書の本体全体が次の順序で 1 つのテキスト ファイルに連結されていることを確認します。
  - a プライベート キー - *your\_domain\_name.key*
  - b プライマリ証明書 - *your\_domain\_name.crt*
  - c 中間証明書 - *DigiCertCA.crt*
  - d ルート証明書 - *TrustedRoot.crt*
- 各証明書の開始タグと終了タグが次の形式で組み込まれていることを確認します。

```

-----BEGIN PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

```



- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

## 手順

### 1 自己署名証明書の生成

OpenSSL ツールを使用して Windows または Linux 用に自己署名証明書を生成することができます。

### 2 証明書署名要求の生成

Windows 対応の OpenSSL ツールを使用して証明書署名要求を生成します。

### 3 認証局に対する署名の要求

選択した認証局に証明書署名要求を送信して、署名を要求します。

### 4 証明書ファイルの連結

お使いのキー ファイルおよび証明書ファイルを 1 つの PEM ファイルに結合します。

### 5 署名証明書のアップロード

署名済みの SSL 証明書をアップロードすることができます。

### 6 vRealize Log Insight サーバと Log Insight Agents 間の SSL 接続の構成

SSL 機能では、Log Insight Agents と vRealize Log Insight サーバ間で取り込み API の安全なフローを介した SSL のみの接続を提供できます。Log Insight Agents のさまざまな SSL パラメータを構成することもできます。

## 自己署名証明書の生成

OpenSSL ツールを使用して Windows または Linux 用に自己署名証明書を生成することができます。

### 前提条件

- <https://www.openssl.org/community/binaries.html> から OpenSSL に適したインストーラをダウンロードします。ダウンロードされた OpenSSL インストーラを使用して Windows マシンにインストールします。
- `openssl.cfg` ファイルを編集して、追加の必須パラメータを追加します。[req]セクションに `req_extensions` パラメータが定義されていることを確認します。

```
[req]
.
.
req_extensions=v3_req #
```

- たとえば、*server-01.loginsight.domain* のように、サーバのホスト名または IP アドレスの適切な Subject Alternative Name エントリを追加します。ホスト名のパターンは指定できません。

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

#### 手順

- 1 証明書ファイルを保存するフォルダ (C:\Certs\LogInsight など) を作成します。
- 2 コマンドプロンプトを開き、次のコマンドを実行します。

```
C:\Certs\LogInsight>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out server.crt -
days 3650
```

OpenSSL が国や組織、その他の証明書のプロパティの入力を求めるプロンプトを表示します。

- 3 お使いの vRealize Log Insight サーバの正確な IP アドレスまたはホスト名、あるいはロード バランシングが有効な場合は vRealize Log Insight クラスタのアドレスを入力します。

このプロパティは値の指定が必須な唯一の項目です。

*server.key* と *server.crt* の 2 つのファイルが作成されます。

- *server.key* は、新しい PEM でエンコードされたプライベート キーです。
- *server.crt* は、新しい PEM でエンコードされ、*server.key* の署名付きの証明書です。

## 証明書署名要求の生成

Windows 対応の OpenSSL ツールを使用して証明書署名要求を生成します。

#### 前提条件

- OpenSSL ツールをインストールします。OpenSSL ツールの取得方法については、<http://www.openssl.org> を参照してください。
- *openssl.cfg* ファイルを編集して、追加の必須パラメータを追加します。[req]セクションに *req\_extensions* パラメータが定義されていることを確認します。

```
[req]
.
.
req_extensions=v3_req #
```

- たとえば、*server-01.loginsight.domain* のように、サーバのホスト名または IP アドレスの適切な Subject Alternative Name エントリを追加します。ホスト名のパターンは指定できません。

```
[v3_req]
.
.
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

#### 手順

- 1 証明書ファイルを保存するフォルダ (C:\Certs\LogInsight など) を作成します。
- 2 コマンド プロンプトを開き、次のコマンドを実行してプライベート キーを生成します。

```
C:\Certs\LogInsight>openssl genrsa -out server.key 2048
```

- 3 次のコマンドを実行して証明書署名要求を作成します。

```
C:\Certs\LogInsight>openssl req -new -key server.key -out server.csr
```

**注:** このコマンドはインタラクティブに実行され、複数の質問をユーザーに尋ねます。ユーザーの回答は認証局によって照合されます。ユーザーの回答は、会社の登録に関する法的文書と一致する必要があります。

- 4 画面上の手順に従って、証明書要求に組み込まれる情報を入力します。

**重要:** [共通名] フィールドにお使いのサーバのホスト名または IP アドレスを入力します (**mail.your.domain** など)。すべてのサブドメインを含める場合は、**[\*your.domain]** と入力します。

証明書署名要求ファイル *server.csr* が生成されて、保存されます。

## 認証局に対する署名の要求

選択した認証局に証明書署名要求を送信して、署名を要求します。

#### 手順

- ◆ *server.csr* ファイルを認証局に送信します。

**注:** ファイルを PEM 形式でエンコードするよう認証局に要求します。

認証局はユーザーの要求を処理し、PEM 形式でエンコードされた *server.crt* ファイルを返信します。

## 証明書ファイルの連結

お使いのキー ファイルおよび証明書ファイルを 1 つの PEM ファイルに結合します。

#### 手順

- 1 新しい *server.pem* ファイルを作成して、テキスト エディタで開きます。

- 2 `server.key` ファイルの内容をコピーし、次の形式を使用して `server.pem` に貼り付けます。

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

- 3 認証局から受け取った `server.crt` ファイルの内容をコピーし、次の形式を使用して `server.pem` に貼り付けます。

```
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

- 4 認証局から中間証明書または連結された証明書が提供されている場合は、パブリック証明書ファイルの末尾にこれらの証明書を次の形式で追加します。


```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- 5 `server.pem` ファイルを保存します。

## 署名証明書のアップロード

署名済みの SSL 証明書をアップロードすることができます。

### 手順

- 1 構成ドロップダウンメニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] の [SSL 証明書] をクリックします。
- 3 カスタム SSL 証明書を参照して、[開く] をクリックします。
- 4 [保存] をクリックします。
- 5 vRealize Log Insight を再起動します。

### 次のステップ

vRealize Log Insight が再起動した後、ESXi からの Syslog フィードが vRealize Log Insight に引き続き受信されていることを確認します。

## vRealize Log Insight サーバと Log Insight Agents 間の SSL 接続の構成

SSL 機能では、Log Insight Agents と vRealize Log Insight サーバ間で取り込み API の安全なフローを介した SSL のみの接続を提供できます。Log Insight Agents のさまざまな SSL パラメータを構成することもできます。

vRealize Log Insight エージェントは TLSv.1.2 を使用して通信します。SSLv.3/TLSv.1.0 はセキュリティ ガイドラインに合うように無効化されています。

### 主な SSL 機能

主な SSL 機能を理解することで、Log Insight Agents を正しく構成できます。

vRealize Log Insight エージェントは、証明書を格納し、特定のサーバへの最初の接続を除くすべての接続においてその証明書を使用してサーバの ID を確認します。サーバ ID を確認できない場合、vRealize Log Insight エージェントはサーバとの接続を拒否し、適切なエラー メッセージをログに書き込みます。エージェントが受信した証明書は cert フォルダに格納されます。

- Windows の場合は、C:\ProgramData\VMware\Log Insight Agent\cert に移動します。
- Linux の場合は、/var/lib/loginsight-agent/cert に移動します。

vRealize Log Insight エージェントは、vRealize Log Insight サーバとの安全な接続を確立すると、vRealize Log Insight サーバから受信した証明書が有効であるか確認します。vRealize Log Insight エージェントはシステムによって信頼された証明書を使用します。

- Log Insight Linux Agent は /etc/pki/tls/certs/ca-bundle.crt または /etc/ssl/certs/ca-certificates.crt から信頼済み証明書を読み込みます。
- Log Insight Windows Agent はシステム ルート証明書を使用します。

vRealize Log Insight エージェントは、自己署名証明書がローカルに格納されている場合に、同一の公開キーを持つ別の有効な自己署名証明書を受信すると、その新しい証明書を受け入れます。これは、自己署名証明書が同じプライベート キー、ただし新しい有効期限などの異なる詳細を使用して、自己署名証明書が再生成された場合に発生します。そうでない場合、接続は拒否されます。

vRealize Log Insight エージェントは、自己署名証明書がローカルに格納されている場合に、有効な CA 署名付き証明書を受信すると、vRealize Log Insight エージェントは受け入れた新しい証明書をサイレントで置換します。

vRealize Log Insight エージェントは、CA 署名付き証明書の所有後に自己署名証明書を受信すると、Log Insight エージェントがその証明書を拒否します。vRealize Log Insight エージェントは、vRealize Log Insight サーバへの初回接続時にのみそのサーバから自己署名証明書を受け入れます。

vRealize Log Insight エージェントは、CA 署名付き証明書がローカルに格納されている場合に、別の信頼済み CA によって署名された有効な証明書を受信すると、その証明書を拒否します。その新しい証明書を受け入れるように vRealize Log Insight エージェントの構成オプションを変更できます。 [vRealize Log Insight エージェントの SSL パラメータの構成](#) を参照してください。

vRealize Log Insight エージェントは TLSv.1.2 を使用して通信します。SSLv.3/TLSv.1.0 はセキュリティ ガイドラインに合うように無効化されています。

## SSL 専用接続の強制


vRealize Log Insight Web ユーザー インターフェイスを使用して、サーバへの接続に SSL のみを許可するように vRealize Log Insight Agents および取り込み API を構成できます。

vRealize Log Insight API は通常、ポート 9000 の HTTP およびポート 9543 の HTTPS を介してアクセスできます。どちらのポートも、vRealize Log Insight エージェントまたはカスタムの API クライアントによって使用することができます。認証されたすべての要求には SSL が必要ですが、vRealize Log Insight エージェントの取り込みトラフィックを含む未認証の要求はどちらのポートでも実行できます。すべての API 要求で SSL 接続を使用するように強制できます。このオプションは Syslog ポート 514 のトラフィックを制限せず、vRealize Log Insight ユーザー インターフェイスには影響しません。HTTP ポート 80 の要求は HTTPS ポート 443 にリダイレクトされ続けます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] で [SSL] をクリックします。
- 3 [API サーバの SSL] の下の [SSL 接続を要求する] を選択します。
- 4 [保存] をクリックします。

vRealize Log Insight API では、サーバへの SSL 接続のみが許可されます。非 SSL 接続は拒否されます。

## vRealize Log Insight エージェントの SSL パラメータの構成

vRealize Log Insight エージェントの構成ファイルを編集して SSL 構成を変更したり、信頼済みルート証明書のパスを追加したり、エージェントが証明書を受け入れるかどうかを定義することができます。

この手順は Windows および Linux 用の vRealize Log Insight エージェントに適用されます。

### 前提条件

vRealize Log Insight Linux エージェント向け：

- root としてログインするか、または `sudo` を使用してコンソール コマンドを実行します。
- vRealize Log InsightLinux エージェントがインストールされた Linux マシンにログインし、コンソールを開き、`pgrep liagent` を実行して、vRealize Log Insight Linux エージェントがインストールされて実行中であることを確認します。

vRealize Log Insight Windows エージェント向け：

- vRealize Log InsightWindows エージェントをインストールした Windows マシンにログインし、サービス マネージャを起動して vRealize Log Insight エージェント サービスがインストールされていることを確認します。

## 手順

- 1 `liagent.ini` ファイルを含むフォルダに移動します。

| オペレーティング システム | パス  |
|---------------|---|
| Linux         | <code>/var/lib/loginsight-agent/</code>             |
| Windows       | <code>%ProgramData%\VMware\Log Insight Agent</code> |

- 2 任意のテキスト エディタで `liagent.ini` を開きます。
- 3 `liagent.ini` ファイルの `[server]` セクションに次のキーを追加します。

| キー                          | 説明   |
|-----------------------------|--|
| <code>ssl_ca_path</code>    | <p>接続ピア証明書の検証に使用される、ルート認証局の署名付き証明書のデフォルト ストレージ パスを上書きします。</p> <p><code>ssl_ca_path</code> のパスを指定すると、Linux および Windows エージェントのデフォルトがオーバーライドされます。PEM 形式の複数の証明書が連結されているファイル、または PEM 形式でフォームが <code>hash.0</code> という名前の証明書を含むディレクトリを使用できます。(X509 ユーティリティの <code>-hash</code> オプションを参照してください。)</p> <p>[Linux] : 値を指定しない場合、エージェントは <code>LI_AGENT_SSL_CA_PATH</code> 環境変数に割り当てられた値を使用します。値が存在しない場合、エージェントは信頼される証明書を <code>/etc/pki/tls/certs/ca-bundle.crt</code> ファイルまたは <code>/etc/ssl/certs/ca-certificates.crt</code> ファイルからロードしようとします。</p> <p>[Windows] : 値を指定しない場合、エージェントは <code>LI_AGENT_SSL_CA_PATH</code> 環境変数によって指定された値を使用します。値が存在しない場合、vRealize Log Insight Windows Agent は証明書を Windows ルート証明書ストアからロードします。</p> |
| <code>ssl_accept_any</code> | <p>vRealize Log Insight エージェントが証明書を受け入れるかどうかを定義します。可能な値は、<code>yes</code>、<code>1</code>、<code>no</code> または <code>0</code> です。この値を <code>yes</code> または <code>1</code> に設定すると、エージェントは、サーバからの証明書を受け入れ、データを送信するための安全な接続を確立します。デフォルト値は <code>no</code> です。</p>   |

| キー                     | 説明   |
|------------------------|--|
| ssl_accept_any_trusted | 可能な値は、yes、1、no または 0 です。vRealize Log Insight エージェントがローカルで格納された信頼済み認証局の署名付き証明書を持つ場合に、他の信頼済み認証局によって署名された別の有効な証明書を受信すると、このエージェントは構成オプションを確認します。値を yes または 1 に設定すると、エージェントは有効な新しい証明書を受け入れます。値を no または 0 に設定すると、証明書を拒否し、接続を切断します。デフォルト値は no です。   |
| ssl_cn                 | 自己署名証明書の Common Name。<br><br>デフォルト値は VMware vCenter Log Insight です。証明書 Common Name フィールドと照合してチェックするカスタム Common Name を定義できます。vRealize Log Insight エージェントは、受信した証明書の Common Name フィールドを [server] セクションの hostname キーに対して指定されたホスト名と比較します。一致しない場合、エージェントは Common Name テキストボックスを liagent.ini ファイルの ssl_cn キーと照合してチェックします。値が一致する場合、vRealize Log Insight エージェントは証明書を受け入れます。 |

**注:** SSL が無効な場合、これらのキーは無視されます。

4 liagent.ini ファイルを保存して閉じます。

#### 例：構成

SSL 構成の例を次に示します。

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

## vRealize Log Insight Web セッションのデフォルトのタイムアウト期間の変更

デフォルトでは、使用環境を常に保護するために、vRealize Log Insight Web セッションは 30 分以内に期限切れになります。このタイムアウト期間は増減できます。


タイムアウト期間は、Web UI を使用して変更できます。

#### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。



## 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] で、[全般] をクリックします。
- 3 [ブラウザ セッション] ペインで、分単位のタイムアウト値を指定します。  
値 -1 を指定すると、セッションのタイムアウトが無効になります。
- 4 [保存] をクリックします。

## アーカイブしています

ログを長期間保持する場合は、ログ データをアーカイブするように vRealize Log Insight を構成します。

### vRealize Log Insight でのデータ アーカイブの有効化または無効化

データをアーカイブすると、本来はストレージ上の制約により vRealize Log Insight 仮想アプライアンスから削除される可能性のある古いログを保持できます。vRealize Log Insight はアーカイブ データを NFS マウントに格納できます。

vRealize Log Insight は、ディスク上のログを収集し、一連の 0.5 GB のバケット内に格納します。1 つのバケットは、圧縮された複数のログ ファイルと 1 つのインデックスから構成されます。バケットには、特定の時間範囲のクエリを実行するために必要な要素がすべて格納されています。バケットのサイズが 0.5 GB を超えると、vRealize Log Insight は書き込みを停止し、そのバケット内のすべてのファイルを閉じてバケットをシールします。

データをアーカイブすると、バケットのシール時に、vRealize Log Insight が圧縮された未加工のログ ファイルをバケットから NFS マウントにコピーします。データのアーカイブが有効にされる前にシールされたバケットが、遡ってアーカイブされることはありません。

アーカイブ エクスポート内で作成されるパスは、**year/month/day/hour/bucketuuid/data.blob** 形式で、本来バケットが UTC 内で作成された時点のタイムスタンプが使用されます。

**注:** vRealize Log Insight はアーカイブに使用される NFS マウントを管理しません。NFS マウントがまもなく容量不足になる場合、または使用できない場合、システム通知が有効であれば、vRealize Log Insight から E メールが送信されます。NFS マウントに十分な空き容量がない場合、または使用不能な期間が仮想アプライアンスの保持期間を超えた場合、vRealize Log Insight は 新しいデータの取り込みを停止します。NFS マウントに十分な空き容量が確保されるか、使用可能になるか、アーカイブが無効になると、データの取り込みを再開します。


NFS を永久的にマウントしたり、`/etc/fstab` ファイルを変更しないでください。vRealize Log Insight 自身によって NFS のマウントが実行されます。

### 前提条件

- 次の要件を満たす NFS パーティションにアクセスできることを確認します。
  - NFS パーティションに、ゲスト アカウントによる読み取りおよび書き込み処理を許可する必要があります。
  - マウントで認証が必要となることがないようにしてください。
  - NFS サーバは NFS v3 をサポートする必要があります。

- Windows NFS サーバを使用している場合は、マッピングされていないユーザーの UNIX アクセス (UID/GID による) を許可します。
- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] で [アーカイブ] をクリックします。
- 3 [データ アーカイブの有効化] を選択し、ログがアーカイブされる NFS パーティションのパスを `nfs://servername<:port-number>/exportname` の形式で入力します。  
デフォルトのポート番号は 2049 です。
- 4 [テスト] をクリックし、接続を確認します。
- 5 [保存] をクリックします。

**注:** データをアーカイブすると、ストレージに制約があるため vRealize Log Insight 仮想アプライアンスから削除されていたログ イベントが保持されます。vRealize Log Insight 仮想アプライアンスから削除されて、アーカイブされたログ イベントは、検索できなくなります。アーカイブされたログを検索する場合は、このログを vRealize Log Insight インスタンスにインポートする必要があります。アーカイブされたログ ファイルのインポートの詳細については、[vRealize 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。

#### 次のステップ

vRealize Log Insight が再起動した後、ESXi からの Syslog フィードが vRealize Log Insight に引き続き受信されていることを確認します。

## vRealize Log Insight アーカイブ ファイルの形式

vRealize Log Insight アーカイブ データは所定の形式になっています。

vRealize Log Insight はアーカイブ ファイルを NFS サーバ上に保存し、アーカイブ時刻に基づいて階層ディレクトリに編成します。次に例を示します。

```
/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob
```

ここで、`/backup` は NFS の場所、`2014/08/07/16` はアーカイブ時刻、`bd234b2d-df98-44ae-991a-e0562f10a49` はバケット ID、`data.blob` はバケットのアーカイブ データです。

アーカイブ データ `data.blob` は vRealize Log Insight 内部エンコーディングを使用した圧縮ファイルです。これには、バケット内に保存されているすべてのメッセージの元のコンテンツと次のような固定フィールドが含まれています : `timestamp`、`hostname`、`source`、`appname`。

アーカイブデータは、vRealize Log Insight にインポートしたり、Raw テキストデータにエクスポートしたり、メッセージ コンテンツを抽出することができます。「[Log Insight アーカイブの Raw テキスト ファイルまたは JSON へのエクスポート](#)」および「[vRealize 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。

## vRealize Log Insight アーカイブの vRealize Log Insight へのインポート

データをアーカイブすると、本来はストレージ上の制約により vRealize Log Insight 仮想アプライアンスから削除される可能性のある古いログを保持できます。[vRealize Log Insight でのデータ アーカイブの有効化または無効化](#)を参照してください。vRealize Log Insight にアーカイブされているログをインポートするには、コマンド ラインを使用できます。

---

**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。

---

### 前提条件

- vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。
- vRealize Log Insight ログがアーカイブされている NFS サーバにアクセスするための権限があることを確認します。
- vRealize Log Insight 仮想アプライアンスに、インポートされたログ ファイルを収容できるだけの十分なディスク領域があることを確認します。

仮想アプライアンス内の `/storage/core` パーティションの最小空き領域は、インポートするアーカイブ済みログのサイズの約 10 倍である必要があります。

### 手順

- 1 vRealize Log Insight vApp との SSH 接続を確立し、root ユーザーとしてログインします。
- 2 アーカイブ済みデータが保存された NFS サーバ上の共有フォルダをマウントします。
- 3 アーカイブ済み vRealize Log Insight ログのディレクトリをインポートするには、次のコマンドを実行します。

```
/usr/lib/loginsight/application/bin/loginsight repository import Path-To-Archived-Log-Data-Folder.
```

---

**注:** アーカイブ済みデータのインポートには、インポートされるフォルダのサイズに応じて、長い時間がかかる場合があります。

---

- 4 SSH 接続を切断します。

### 次のステップ

インポートされたログ イベントは、検索、フィルタリング、分析できます。

## Log Insight アーカイブの Raw テキスト ファイルまたは JSON へのエクスポート

vRealize Log Insight アーカイブを標準の Raw テキスト ファイルまたは JSON 形式にエクスポートするには、コマンドラインを使用できます。

**注:** これは高度な手順です。コマンド構文および出力形式は、vRealize Log Insight の今後のリリースで変更され、下位互換性がなくなる可能性があります。

### 前提条件

- vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。
- vRealize Log Insight 仮想アプライアンスに、エクスポートされたファイルを収容できるだけの十分なディスク領域があることを確認します。

### 手順

- 1 vRealize Log Insight vApp との SSH 接続を確立し、root ユーザーとしてログインします。
- 2 vRealize Log Insight vApp にアーカイブ ディレクトリを作成します。

```
mkdir /archive
```

- 3 次のコマンドを実行して、アーカイブ済みデータが保存された NFS サーバ上の共有フォルダをマウントします。

```
mount -t nfs  
archive-fileshare:archive_directory_path /archive
```

- 4 vRealize Log Insight vApp の使用可能なストレージ領域を確認します。

```
df -h
```

- 5 vRealize Log Insight アーカイブを Raw テキスト ファイルにエクスポートします。

```
/usr/lib/loginsight/application/sbin/repo-exporter -d archive-file-directory output-  
file
```

次に例を示します。

```
/usr/lib/loginsight/application/sbin/repo-exporter -d /archive/2014/08/07/16/bd234b2d-  
df98-44ae-991a-e0562f10a49 /tmp/output.txt
```

- 6 vRealize Log Insight アーカイブのメッセージの内容を JSON 形式にエクスポートします。

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d archive-file-directory output-file.
```

次に例を示します。

```
/usr/lib/loginsight/application/sbin/repo-exporter -F -d /archive/2014/08/07/16/bd234b2d-  
df98-44ae-991a-e0562f10a49 /tmp/output.json
```

- 7 SSH 接続を切断します。

## vRealize Log Insight サービスの再起動


Web ユーザー インターフェイスの [管理] ページを使用すると、vRealize Log Insight を再起動できます。

**注意:** vRealize Log Insight を再起動すると、アクティブなすべてのユーザー セッションが終了します。vRealize Log Insight インスタンスのユーザーは強制的に再ログインされます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 クラスタ ノードを選択します。
- 4 [マスターの再起動] をクリックして、[再起動] をクリックします。

### 次のステップ

vRealize Log Insight が再起動した後、ESXi からの Syslog フィードが vRealize Log Insight に引き続き受信されていることを確認します。

## vRealize Log Insight 仮想アプライアンスのパワーオフ

vRealize Log Insight マスター ノードまたはワーカー ノードをパワーオフするときにデータが失われないようにするには、次の手順に厳密に従ってノードをパワーオフする必要があります。

vRealize Log Insight 仮想アプライアンスの仮想ハードウェアに変更を加える前に、このアプライアンスをパワーオフする必要があります。

vRealize Log Insight 仮想アプライアンスをパワーオフするには、vSphere Client で [パワー] - [ゲストのシャットダウン] メニュー オプションを使用するか、仮想アプライアンス コンソールを使用するか、vRealize Log Insight 仮想アプライアンスとの SSH 接続を確立してコマンドを実行します。

### 前提条件

- SSH を使用して vRealize Log Insight 仮想アプライアンスに接続する場合は、TCP ポート 22 が開いていることを確認します。
- vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。

### 手順

- 1 vRealize Log Insight vApp との SSH 接続を確立し、root ユーザーとしてログインします。
- 2 vRealize Log Insight 仮想アプライアンスをパワーオフするには、`shutdown -h now` を実行します。

### 次のステップ

これで vRealize Log Insight 仮想アプライアンスの仮想ハードウェアを安全に変更できます。

## vRealize Log Insight サポート バンドルのダウンロード

問題が発生したため vRealize Log Insight が予測どおりに動作しない場合は、ログおよび構成ファイルのコピーをサポート バンドルの形式で VMware サポート サービスに送信できます。

クラスタ全体のサポート バンドルのダウンロードが必要になるのは、VMware サポート サービスによって要求された場合のみです。バンドルは静的に作成することも（ノード上のディスク容量を使用）、ストリーミングで作成することもできます（ノード上のディスク容量を使用せず、バンドルをデフォルトで開始マシンに保存）。


サポート バンドルのストレージの場所は、サポート バンドルを取得するために使用するオプションによって異なります。

| オプション                                  | サポート バンドルの場所                        |
|--|-------------------------------------|
| API - POST appliance/vm-support-bundle | これは、ストリーミング バージョンで、ローカル ファイルはありません。 |
| API - POST appliance/support-bundle    | /tmp/ui-support/                    |
| Web ユーザー インターフェイス - 静的サポート バンドル        | /tmp/ui-support/                    |
| Web ユーザー インターフェイス - ストリーミングサポート バンドル   | これは、ストリーミング バージョンで、ローカル ファイルはありません。 |
| コマンド ライン - scripts/loginsight-support  | バンドルは、現在のディレクトリに生成されます。             |

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。

- 3 [サポート] ヘッダーで [サポート バンドルのダウンロード] をクリックします。

vRealize Log Insight システムは診断情報を収集し、データを tar 形式に圧縮してブラウザに送信します。

- 4 バンドルの作成方法を選択します。

- バンドルをローカルに作成するには、[静的サポート バンドル] を選択します。バンドルの作成には、ノード上のディスク容量を使用します。
- サポート バンドルのストリーミングをただちに開始するには、[サポート バンドルのストリーミング] を選択します。この方法はノード上のディスク容量を使用しません。

- 5 [続行] をクリックします。

- 6 [ファイルのダウンロード] ダイアログ ボックスで、[保存] をクリックします。

- 7 tarball アーカイブを保存する場所を選択し、[保存] をクリックします。

#### 次のステップ

ログ ファイルの内容を後で表示し、エラー メッセージを確認できます。問題が解決または終了したら、ディスク容量を節約するために古いサポート バンドルを削除してください。

## VMware カスタマ エクスペリエンス改善プログラムへの参加または参加取り消し


vRealize Log Insight を展開した後で VMware カスタマ エクスペリエンス改善プログラムに参加または参加取り消しを行うことができます。

vRealize Log Insight をインストールするときに、カスタマ エクスペリエンス改善プログラムに参加するかどうかを選択します。インストール後は、次の手順でプログラムへの参加または参加取り消しを行うことができます。

#### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [構成] で、[全般] をクリックします。
- 3 [カスタマ エクスペリエンス改善プログラム] ペインで、[VMware カスタマ エクスペリエンス改善プログラムに参加する] チェック ボックスをオンまたはオフにします。  
オンにすると、このプログラムが有効になり、データが `https://vmware.com` に送信されます。
- 4 [保存] をクリックします。

# vRealize Log Insight クラスタの管理

vRealize Log Insight クラスタのノードを追加、削除、またはアップグレードすることができます。

**注:** vRealize Log Insight では、WAN クラスタリングはサポートされていません。vRealize Log Insight の現在のバージョンでは、WAN クラスタリング（ジオクラスタリング、高可用性クラスタリング、またはリモート クラスタリングとも呼ばれます）はサポートされていません。クラスタ内のすべてのノードは同じレイヤ 2 の LAN に展開する必要があります。また、通信を適切に行うには、[6 章 ポートおよび外部インターフェイス](#) で説明されているポートがノード間で開かれている必要があります。

この章には、次のトピックが含まれています。

- [vRealize Log Insight クラスタへのワーカー ノードの追加](#)
- [vRealize Log Insight クラスタからのワーカー ノードの削除](#)
- [統合ロード バランサの操作](#)
- [本番クラスタ チェックの結果のクエリ](#)

## vRealize Log Insight クラスタへのワーカー ノードの追加

Log Insight 仮想アプライアンスの新しいインスタンスを展開し、既存の Log Insight マスター ノードに追加します。

### 手順

#### 1 [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。

#### 2 [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 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 [Deploy OVF Template] 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) [ネットワークのセットアップ] 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。

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 を利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。
- 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間かかります。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。<br>a vRealize Log Insight 仮想アプライアンスをパワーオフします。<br>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。<br>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。

## 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リングし、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 はマスター ノードとワーカー ノードを提供します。マスター 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。マスター 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。
- マスター 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。
- マスター 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 マスターおよびワーカー 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 マスター 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 マスターの 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 vRealize Log Insight マスター ノードに既存の環境への参加要求を送信します。
- 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。

## vRealize Log Insight クラスタからのワーカー ノードの削除

正しく機能しなくなったワーカー ノードを vRealize Log Insight クラスタから削除できます。正常に動作しているワーカー ノードはクラスタから削除しないでください。

---



**注意:** ノードを削除すると、データが失われます。ノードの削除が必要な場合は、まず、バックアップ済みであることを確認します。新しいノードの追加後 30 分間は、ノードの削除を行わないようにします。

---

## 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。


## 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 ワーカー テーブルで、目的のノードを見つけ、一時停止アイコン  をクリックして [続行] をクリックします。  
ノードはメンテナンス モードになりました。

---

**注:** メンテナンス モードのノードはログの受信を継続します。

---

- 4  をクリックしてノードを削除します。

vRealize Log Insight はクラスタからノードを削除して、E メール通知を送信します。

- 5 削除すると、ノードをスタンドアローン ノードとしてブートストラップするか、ブートストラップしてクラスタに参加させることができます。

## 統合ロード バランサの操作

vRealize Log Insight 統合ロード バランサ (ILB) は vRealize Log Insight クラスタをサポートし、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を確実に vRealize Log Insight が受け入れるようにできます。複数の仮想 IP アドレスを構成することもできます。

**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。

ベスト プラクティスは、単一ノード インスタンスを含むすべての展開に ILB を含めることです。今後必要に応じてクラスタを簡単にサポートできるように、クエリと取り込みトラフィックを ILB に送信します。ILB はクラスタ内のノード全体にトラフィックを分散し、管理オーバーヘッドを最小限に抑えます。

ILB により、一部の vRealize Log Insight ノードが使用できなくなっても、受信消費トラフィックを vRealize Log Insight が受け入れるようにできます。また、ILB は使用可能な vRealize Log Insight ノード間で受信トラフィックを均等に分散します。Web ユーザー インターフェイスと、Syslog または取り込み API を介した取り込みを使用する vRealize Log Insight クライアントは、ILB アドレスを使用して vRealize Log Insight に接続します。

ILB では、すべての vRealize Log Insight ノードが同じレイヤー 2 ネットワークにあるか（同じスイッチ内など）、相互に ARP 要求を送受信できることが求められます。ILB IP アドレスを設定して、vRealize Log Insight ノードがそれを所有し、そのトラフィックを受信できるようにする必要があります。そのためには、通常 ILB IP アドレスは、vRealize Log Insight ノードの物理アドレスと同じサブネット内に作成されます。ILB IP アドレスを構成したら、別のネットワークから ping を実行し、このアドレスに到達できることを確認してください。

今後の変更やアップグレードを簡素化するには、ILB IP アドレスを直接参照するのではなく、ILB IP アドレスに解決する FQDN を参照するようにクライアントを構成します。

## Direct Server Return の構成について

vRealize Log Insight ロード バランサは、Direct Server Return (DSR) 構成を使用します。DSR では、すべての受信トラフィックは現在のロード バランサ ノードである vRealize Log Insight ノードをパス スルーします。

vRealize Log Insight サーバから送信される戻りのトラフィックは、ロード バランサ ノードを経由する必要なくクライアントに直接戻されます。

## 複数の仮想 IP アドレス

統合ロード バランサ用に、複数の仮想 IP アドレス (vIP) を構成できます。各 vIP に対する静的タグのリストを構成し、vIP から受信した各ログ メッセージに構成済みタグで注釈を付けることもできます。

## 統合ロード バランサの有効化

vRealize Log Insight 統合ロード バランサ (ILB) を vRealize Log Insight クラスタ上で有効にする場合は、1 つまたは複数の仮想 IP アドレスを構成する必要があります。


統合ロード バランサは、1 つまたは複数の仮想 IP アドレス (vIP) をサポートします。各 vIP は、受信する取り込みトラフィックおよびクエリ トラフィックを利用可能な vRealize Log Insight ノードに分散します。ベスト プラクティスは、すべての vRealize Log Insight クライアントをノードに直接接続するのではなく vIP 経由で接続することです。

今後の変更やアップグレードを簡素化するには、ILB IP アドレスを直接参照するのではなく、ILB IP アドレスに解決する FQDN を参照するようにクライアントを構成します。vSphere と vRealize Operations の統合ならびにアラート メッセージでは、FQDN を指定した場合には FQDN が使用されます。指定しなかった場合には ILB IP アドレスが使用されます。vRealize Log Insight は、FQDN を指定の IP アドレスに解決できるようにする必要があります。これは、指定する FQDN 値が DNS で定義されたものと一致する必要があることを意味します。

### 前提条件

- すべての vRealize Log Insight ノードと、指定する統合ロード バランサーの IP アドレスが同じネットワーク上にあることを確認します。
- NSX で vRealize Log Insight を使用している場合は、NSX 論理スイッチ上で [IP 検出の有効化] オプションが無効になっていることを確認します。
- vRealize Log Insight のマスター ノードとワーカー ノードには同じ証明書がなければなりません。そうでない場合、SSL を介して接続するように構成された vRealize Log Insight エージェントは接続を拒否します。CA 署名付き証明書を vRealize Log Insight のマスター ノードとワーカー ノードにアップロードするときは、証明書の生成要求時に [共通名] を ILB FQDN (または IP アドレス) に設定します。[証明書署名要求の生成](#) を参照してください。
- 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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[クラスタ] をクリックします。
- 3 [統合ロード バランサ] セクションで、[新しい仮想 IP アドレス] を選択し、統合ロード バランシングに使用する仮想 IP (vIP) アドレスを入力します。
- 4 (オプション) 複数の仮想 IP アドレスを構成するには、[新しい仮想 IP アドレス] をクリックして IP アドレスを指定します。FQDN とタグを入力するように選択できます。
  - 各ノード上の少なくとも 1 つのネットワーク インターフェイスと vIP が使用可能 (他のマシンで使用されていない) である必要があるため、各 vIP が同じサブネット内にあるようにします。
  - タグにより、事前定義された値を使用してイベントにフィールドを追加することができるため、クエリが簡単になります。複数のカンマ区切りのタグを追加できます。vIP 経由でシステムに通知されるイベントには、すべて vIP のタグが付けられます。

- 1 つの ILB vIP に静的なタグ (key=value) のリストを構成できます。このようにすることで、vIP から受け取るそれぞれのログ メッセージに、構成済みのタグを使用して注釈が付けられます。
- 5 (オプション) FQDN でクラスタにアクセスする vRealize Log Insight ユーザを有効にするには、構成済みの ILB IP アドレスを直接参照するのではなく、FQDN をクライアントに参照させます。

将来の変更やアップグレードを簡素化するために、クライアントが ILB IP アドレスに解決する FQDN を参照するようにすることができます。クライアントが ILB IP アドレスを直接参照するのではなく、FQDN を参照するようにすることができます。

- 6 [保存] をクリックします。

統合ロード バランサーは、このサービスのリーダーとして宣言された、vRealize Log Insight クラスタ上の 1 つのノードで管理されます。現在のリーダーは、ノードの横にテキスト (ILB) で示されています。

## 本番クラスタ チェックの結果のクエリ

本番クラスタ チェック サービスは、各ノードで一連のチェックを定期的に行います。本番クラスタ チェックの最新の結果を CLI を使用して問い合わせることができます。

たとえばサービスは、クラスタが期待どおりに実行および構成されているか、または他のシステムの統合で問題が発生していないかを判定します。その他のチェック事項は以下のリストのとおりです。

- NTP が複数ホストのデプロイで構成されているか。
- Active Directory にアクセスできるか (現在構成されている場合)
- Active Directory の認証を実行できるか (現在構成されている場合)
- Active Directory ホストおよび Kerberos ホストにアクセスできるか (Active Directory が現在構成されている場合)
- システムが、サポートされていない 2 ホストのデプロイで実行しているか
- /tmp にアップグレードを実行するための十分な空き容量があるか
- /storage/core にアップグレードを実行するための十分な空き容量があるか
- localhost は /etc/hosts 内に正しく配置されているか

### 手順

- 1 コマンドラインで、vRealize Log Insight 仮想アプライアンスとの SSH 接続を確立し、root ユーザーとしてログインします。
- 2 コマンドラインで、`/usr/lib/loginsight/application/sbin/query-check-results.sh` と入力して [Enter] を押します。



## ポートおよび外部インターフェイス

vRealize Log Insight では、必要な特定のサービス、ポート、および外部インターフェイスが使用されます。

### 通信ポート

vRealize Log Insight は、このトピックにリストされた通信ポートとプロトコルを使用します。必要なポートは、ソース、ユーザー インターフェイス、クラスタ間、外部サービスのどれに対して必要なのか、あるいはファイアウォールによって安全にブロックできるのかに応じて編成されます。一部のポートは対応する統合を有効にする場合のみ使用されます。

**注:** vRealize Log Insight は、WAN クラスタリング（ジオクラスタリング、高可用性クラスタリング、リモート クラスタリングとも呼ばれます）をサポートしません。クラスタ内のすべてのノードは同じレイヤ 2 の LAN に展開する必要があります。また、通信を適切に行うには、このセクションで説明されているポートがノード間で開かれている必要があります。

vRealize Log Insight ネットワーク トラフィックには複数のソースがあります。

|                                     |   |
|-------------------------------------|---|
| <b>管理ワークステーション</b>                  | システム管理者が vRealize Log Insight 仮想アプライアンスをリモートに管理する場合に使用するマシン。  |
| <b>ユーザー ワークステーション</b>               | vRealize Log Insight ユーザーがブラウザを使用して vRealize Log Insight の Web インターフェイスにアクセスするマシン。  |
| <b>ログの送信元システム</b>                   | 分析および検索のために vRealize Log Insight にログを送信するエンドポイント。たとえば、エンドポイントには ESXi ホスト、仮想マシン、IP アドレスを持つ任意のシステムなどが含まれます。                 |
| <b>Log Insight Agents</b>           | Windows または Linux マシン上にあり、API を介してオペレーティング システムのイベントおよびログを vRealize Log Insight に送信するエージェント。                              |
| <b>vRealize Log Insight アプライアンス</b> | vRealize Log Insight サービスが配置されている任意の vRealize Log Insight 仮想アプライアンス（マスターまたはワーカー）。アプライアンスの基本オペレーティング システムは SUSE 11 SP3 です。 |

### データを送信するソースに必要なポート

vRealize Log Insight にデータを送信するソースからのネットワーク トラフィックに対して次のポートが開いている必要があります。これは、クラスタ外部からの接続とクラスタ ノード間でロード バランシングされた接続の両方に使用されます。



| ソース                         | ターゲット                        | ポート        | プロトコル   | サービスの説明                            |
|-----------------------------|------------------------------|------------|---------|------------------------------------|
| ログの送信元システム                  | vRealize Log Insight アプライアンス | 514        | TCP、UDP | 転送者の送信先として構成された送信 Syslog トラフィック    |
| ログの送信元システム                  | vRealize Log Insight アプライアンス | 1514, 6514 | TCP     | SSL を介して送信される Syslog データ           |
| vRealize Log Insight エージェント | vRealize Log Insight アプライアンス | 9000       | TCP     | Log Insight 取り込み API               |
| vRealize Log Insight エージェント | vRealize Log Insight アプライアンス | 9543       | TCP     | SSL を介して送信される Log Insight 取り込み API |

## ユーザー インターフェイスに必要なポート

vRealize Log Insight ユーザー インターフェイスを使用する必要があるネットワーク トラフィックに対して次のポートが開いている必要があります。これは、クラスタ外部の接続とクラスタ ノード間でロード バランシングされた接続の両方に使用されます。

| ソース            | ターゲット                        | ポート | プロトコル | サービスの説明               |
|----------------|------------------------------|-----|-------|-----------------------|
| 管理ワークステーション    | vRealize Log Insight アプライアンス | 22  | TCP   | SSH: Secure Shell の接続 |
| ユーザー ワークステーション | vRealize Log Insight アプライアンス | 80  | TCP   | HTTP: Web インターフェイス    |
| ユーザー ワークステーション | vRealize Log Insight アプライアンス | 443 | TCP   | HTTPS: Web インターフェイス   |

## クラスタ ノード間に必要なポート

ワーカー ノードからネットワークにアクセスする場合は、最大限のセキュリティを確保するために、vRealize Log Insight マスター ノードの次のポートのみを開くようにしてください。これらのポートは、クラスタ ノード間でロード バランシングされたソースおよびユーザー インターフェイス トラフィックに使用されるポートに追加されます。

| ソース                          | ターゲット                        | ポート                | プロトコル | サービスの説明                             |
|------------------------------|------------------------------|--------------------|-------|-------------------------------------|
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 7000               | TCP   | Cassandra のレプリケーションおよびクエリ           |
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 9042               | TCP   | ネイティブ プロトコル クライアント用の Cassandra サービス |
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 9160               | TCP   | Thrift クライアント用の Cassandra サービス      |
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 59778, 16520-16580 | TCP   | vRealize Log Insight Thrift サービス    |

## 外部サービスに必要なポート

vRealize Log Insight クラスター ノードからリモート サービスへの送信ネットワーク トラフィックに対して次のポートが開いている必要があります。

| ソース                           | ターゲット                                | ポート  | プロトコル   | サービスの説明   |
|-------------------------------|--------------------------------------|------|---------|---|
| vRealize Log Insight アプリケーション | NTP サーバ                              | 123  | UDP     | NTPD: NTP 時刻を同期します。<br><br><b>注:</b> ポートが開くのは、NTP 時刻同期を使用するように選択した場合のみです。 |
| vRealize Log Insight アプリケーション | メール サーバ                              | 25   | TCP     | SMTP: 送信アラートのメール サービス   |
| vRealize Log Insight アプリケーション | メール サーバ                              | 465  | TCP     | SMTPS: SSL を介した送信アラートのメール サービス  |
| vRealize Log Insight アプリケーション | DNS サーバ                              | 53   | TCP、UDP | DNS: 名前解決サービス   |
| vRealize Log Insight アプリケーション | AD サーバ                               | 389  | TCP、UDP | Active Directory  |
| vRealize Log Insight アプリケーション | AD サーバ                               | 636  | TCP     | SSL を介した Active Directory   |
| vRealize Log Insight アプリケーション | AD サーバ                               | 3268 | TCP     | Active Directory グローバル カタログ   |
| vRealize Log Insight アプリケーション | AD サーバ                               | 3269 | TCP     | Active Directory グローバル カタログ SSL   |
| vRealize Log Insight アプリケーション | AD サーバ                               | 88   | TCP、UDP | ケルベロス   |
| vRealize Log Insight アプリケーション | vCenter Server                       | 443  | TCP     | vCenter Server Web サービス   |
| vRealize Log Insight アプリケーション | vRealize Operations Manager アプリケーション | 443  | TCP     | vRealize Operations Web サービス  |
| vRealize Log Insight アプリケーション | サードパーティのログ マネージャ                     | 514  | TCP、UDP | syslog データ  |
| vRealize Log Insight アプリケーション | サードパーティのログ マネージャ                     | 9000 | CFAPI   | 転送者の送信先として構成された送信 Log Insight 取り込み API (CFAPI) トラフィック                     |
| vRealize Log Insight アプリケーション | サードパーティのログ マネージャ                     | 9543 | CFAPI   | 暗号化 (SSL/TLS) を使用して転送者の送信先として構成された送信 Log Insight 取り込み API (CFAPI) トラフィック  |

## ブロックすることができるポート

次のポートは開いてますが vRealize Log Insight では使用されません。これらのポートはファイアウォールによって安全にブロックすることができます。

| ターゲット                                    | ポート  | プロトコル   | サービスの説明                                   |
|--|------|---------|---|
| vRealize Log Insight アプライアンス             | 111  | TCP、UDP | RPC プログラム番号をユニバーサルアドレスに変換する RPCbind サービス。 |
| vRealize Log Insight アプライアンス Tomcat サービス | 9007 | TCP     | Tomcat サービス                               |

# vRealize Log Insight エージェントの ステータスの監視

7

vRealize Log Insight の Windows エージェントおよび Linux エージェントのステータスを監視し、運用状態に関する現在の統計情報を表示できます。

[エージェント] ページに表示されるのは、CFAPI 経由でデータを送信するように設定されたエージェントだけです。他の Syslog ソースと同様に、Syslog 経由でデータを送信するように設定されたエージェントが [ホスト] ページに表示されます。vRealize Log Insight には、最大 15,000 個のエージェントの情報を表示できます。


プロトコルを CFAPI から Syslog に変更すると、統計情報の更新が停止され、[エージェント] ページで表示されなくなってしまい、エージェントのステータスは、切断されているとして表示されます。ここで示されるデータは、30 秒おきに vRealize Log Insight エージェントから送信されています。

**注:** エージェントの設定で vRealize Log Insight サーバのホスト IP アドレスを変更すると、エージェントはページの統計をリセットします。

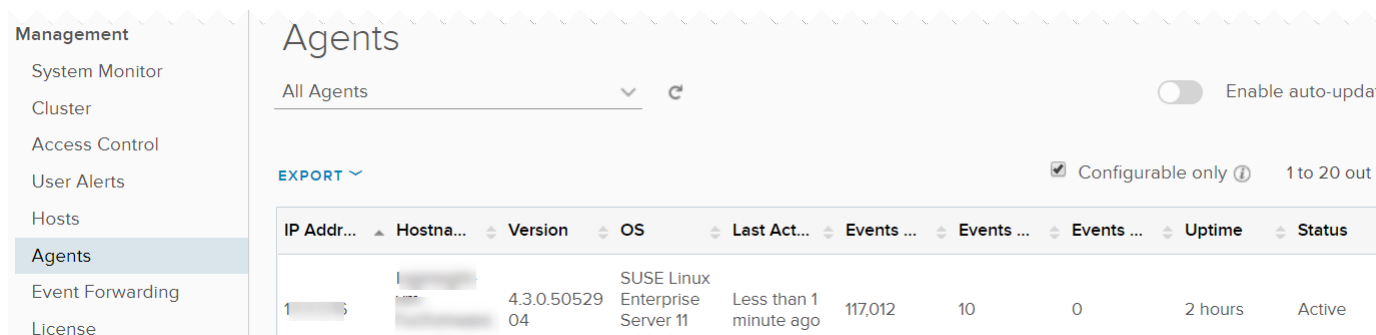
## 前提条件

表示管理者 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

## 手順

- 1 構成ドロップダウンメニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[エージェント] をクリックします。

CFAPI でデータを送信する各エージェントのステータス情報が表示されます。



| Agents                                    |            |                |                                     |                        |            |            |            |         |        |  |
|---|------------|----------------|-------------------------------------|------------------------|------------|------------|------------|---------|--------|--|
| All Agents                                |            |                |                                     |                        |            |            |            |         |        |  |
| EXPORT                                    |            |                |                                     |                        |            |            |            |         |        |  |
| Enable auto-updates                       |            |                |                                     |                        |            |            |            |         |        |  |
| Configurable only ⓘ 1 to 20 out of 15,000 |            |                |                                     |                        |            |            |            |         |        |  |
| IP Addr...                                | Hostna...  | Version        | OS                                  | Last Act...            | Events ... | Events ... | Events ... | Uptime  | Status |  |
| 10.10.10.1                                | vmware-... | 4.3.0.50529.04 | SUSE Linux Enterprise Server 11 SP3 | Less than 1 minute ago | 117,012    | 10         | 0          | 2 hours | Active |  |

### 次のステップ

[エージェント] ページの情報を使用し、インストールされた vRealize Log Insight の Windows エージェントおよび Linux エージェントの運用状態を監視できます。エージェントのホスト名をクリックして、そのホストの [インタラクティブ分析] ページに移動します。

# サーバからのエージェントの自動更新の有効化

## 8

すべてのエージェントを対象に、vRealize Log Insight サーバからの自動更新を有効にすることができます。


自動更新では、サーバに接続されているすべてのエージェントに使用可能な最新の更新を適用します。エージェントの `liagent.ini` ファイルを編集して、個々のサーバの自動更新機能を無効にすることができます。詳細については、vRealize Log Insight エージェントの操作 を参照してください。

デフォルトでは、サーバの自動更新は無効です。

### 前提条件

エージェントはアクティブ状態で、バージョン 4.3 以降である必要があります。

### 手順

- 1 構成ドロップダウンメニュー アイコン  をクリックし、[管理] を選択します。
- 2 左側のメニューで [エージェント] をクリックします。
- 3 [エージェント] のページで [すべてのエージェントの自動更新を有効にします] の切り替えコントロールをクリックします。

このサーバに接続するエージェントは、更新を利用できるようになると更新されます。

# 一元化されたエージェントの構成およびエージェント グループの操作

## 9

vRealize Log Insight サーバを使用して、アプリケーション ユーザー インターフェイス内からエージェントを構成することができます。エージェントは vRealize Log Insight サーバを定期的にポーリングし、新しい構成が使用可能かどうかを確認します。

同一構成を要求するエージェントをグループ化することができます。例えば、すべての vRealize Log Insight Windows エージェントを vRealize Log Insight Linux エージェントから分離してグループ化することができます。

[すべてのエージェント] メニューでは、コンテンツ パック内の既存のエージェント グループが自動的に一覧に表示されます。一覧中のエージェントは、インストール済みでエージェント グループを使用するコンテンツ パックに関連しています (vSphere コンテンツ パックなど)。

コンテンツ パック グループは読み取り専用です。

コンテンツ パックでは [winlog]、[filelog]、および [parser] で始まる構成セクションのみが使用されます。その他のセクションは、コンテンツ パックの一部としてエクスポートされません。コンテンツ パックでは、[winlog]、[filelog]、および [parser] の各セクションにある 1 行のコメント (; で始まる行) のみが保持されます。

ローカルおよびサーバサイドの構成のマージを含むエージェントの構成に関する情報については、『vRealize Log Insight エージェントの操作』を参照してください。

### ■ エージェント グループ構成のマージ

エージェント グループを使用すると、各エージェントを複数のグループに所属させることができます。デフォルト グループである すべてのエージェント への所属が可能で、これにより、各エージェントを一元的に構成できます。

### ■ エージェント グループの作成

同一パラメータで構成されたエージェントのグループを作成できます。

### ■ エージェント グループの編集

エージェント グループの名前を説明を編集し、フィルタの変更および設定の編集を行うことができます。

### ■ Content Pack エージェント グループをエージェント グループとして追加

コンテンツ パックの一部として定義されたエージェント グループをアクティブなグループに追加し、グループにエージェントの構成ファイルを適用することができます。

### ■ エージェント グループの削除

エージェント グループを削除し、アクティブなグループの一覧から削除することができます。

## エージェント グループ構成のマージ

エージェント グループを使用すると、各エージェントを複数のグループに所属させることができます。デフォルトグループである すべてのエージェント への所属が可能で、これにより、各エージェントを一元的に構成できます。

マージはサーバ側で実行され、その結果の構成はエージェント側の構成にマージされます。構成のマージは、次のルールに従って行われます。

- 個別のグループ構成の優先度が高く設定されており、[すべてのエージェント] のグループ設定をオーバーライドします。
- [すべてのエージェント] のグループ構成は、ローカル構成をオーバーライドします。
- 異なるグループ内に同じ名前のセクションを構成することはできませんが、[すべてのエージェント] との間では重複させることができます。ただし、個別のグループ内のセクションの方が、優先度が高くなります。

---

**注:** エージェントの消失を防止するために、エージェント構成の [hostname] および [port] パラメータをサーバから一元的に変更することはできません。

---

マージされた構成は、エージェント側の `liagent-effective.ini` ファイルに保存されます。


## エージェント グループの作成

同一パラメータで構成されたエージェントのグループを作成できます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[エージェント] をクリックします。
- 3 [すべてのエージェント] メニューで、[更新] ボタンの横にあるエージェント名フィールドのドロップダウン メニューを開き、[新規グループ] をクリックします。
- 4 エージェント グループに固有の名前と説明を入力し、[新規グループ] をクリックします。

エージェント グループが作成され、[すべてのエージェント] 一覧に表示されますが、保存されていません。



- 5 エージェント グループの 1 つまたは複数のフィルタを指定します。フィルタを作成するには、フィールド名、演算子、および値を指定します。

フィルタには、\* や ? などのワイルドカードを使用できます。たとえば、OS フィルタ `contains` を選択し、値 `windows` を指定して、構成するすべての Windows エージェントを特定することができます。

- a フィルタする次のいずれかのフィールドを選択します。

- IP アドレス
- ホスト名
- バージョン
- OS

- b ドロップダウン メニューから演算子を選択し、値を指定します。

| 演算子     | 説明  |
|---------|---|
| 一致する    | 指定した文字列およびワイルドカードの仕様と一致する文字列を検索します。* はゼロ文字以上、? は任意の 1 文字を意味します。プリフィックスとポストフィックスのグローピングがサポートされます。<br>たとえば、 <b>*test*</b> は <b>test123</b> や <b>my-test-run</b> などの文字列に一致します。   |
| 一致しない   | 指定した文字列およびワイルドカードの仕様と一致する文字列を除外します。* はゼロ文字以上、? は任意の 1 文字を意味します。プリフィックスとポストフィックスのグローピングがサポートされます。<br>たとえば、 <b>test*</b> は <b>test123</b> を除外しますが、 <b>mytest123</b> は除外しません。 <b>%test*</b> は <b>test123</b> を除外しませんが、 <b>xtest123</b> は除外します。 |
| 次で開始する  | 指定した文字列で開始する文字列を見つけます。<br>たとえば、 <b>test</b> は <b>test123</b> または <b>test</b> を見つけますが、 <b>my-test123</b> は見つけません。  |
| 次で開始しない | 指定した文字列で開始する文字列を除外します。<br>たとえば、 <b>test</b> は <b>test123</b> を除外しますが、 <b>my-test123</b> は除外しません。  |

- 6 エージェント構成エリア内でエージェント構成値を指定し、[新規グループを保存] をクリックします。

エージェントの構成は次のポーリング間隔で適用されます。

## エージェント グループの編集

エージェント グループの名前を説明を編集し、フィルタの変更および設定の編集を行うことができます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。

- 2 [管理] で、[エージェント] をクリックします。
- 3 [すべてのエージェント] メニューから、対象のエージェント グループの名前を選択し、鉛筆アイコンをクリックして編集します。
- 4 必要な変更を行います。

| 編集項目            | 操作                           |
|-----------------|------------------------------|
| [名前] または [説明]   | 必要な変更を行い [保存] をクリックします。      |
| [フィルタ] または [設定] | 必要な変更を行い [グループを保存] をクリックします。 |


## Content Pack エージェント グループをエージェント グループとして追加

コンテンツ パックの一部として定義されたエージェント グループをアクティブなグループに追加し、グループにエージェントの構成ファイルを適用することができます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[エージェント] をクリックします。
- 3 [すべてのエージェント] メニューで、使用可能なテンプレートの一覧用に変エージェント テンプレートを選択します。
- 4 [テンプレートをコピー] をクリックして Content Pack グループをアクティブなグループに追加します。
- 5 [コピー] をクリックします。
- 6 必要なフィルタを選択して [新規グループを保存] をクリックします。

Content Pack エージェント グループがアクティブなグループに追加され、指定したフィルタに従ってエージェントが構成されます。


## エージェント グループの削除

エージェント グループを削除し、アクティブなグループの一覧から削除することができます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

## 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[エージェント] をクリックします。
- 3 [すべてのエージェント] メニュー内で、グループ名の横の X アイコンをクリックして削除するエージェント グループを選択します。
- 4 [削除] をクリックします。

エージェント グループがアクティブなグループから削除されました。

# vRealize Log Insight の監視

vRealize Log Insight 仮想アプライアンスと、ログ イベントを vRealize Log Insight に送信するホストとデバイスを監視することができます。

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健全性チェック
- ログ イベントを送信するホストの監視
- 非アクティブなホストについてレポートするシステム通知の構成


## vRealize Log Insight 仮想アプライアンスの健全性チェック

vRealize Log Insight 仮想アプライアンスで使用可能なリソースおよびアクティブなクエリを確認し、vRealize Log Insight の操作に関する最新の統計情報を表示することができます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[システム モニタ] をクリックします。
- 3 vRealize Log Insight がクラスタとして実行されている場合は、[リソースの表示対象] をクリックして、監視するノードを選択します。
- 4 [システム監視] ページのボタンをクリックして、必要な情報を表示します。

| オプション       | 説明  |
|-------------|---|
| [リソース]      | vRealize Log Insight 仮想アプライアンスの CPU、メモリ、IOPS（読み書きアクティビティ）、およびストレージ使用量に関する情報を表示します。<br>右側のチャートは過去 24 時間の履歴データを表していて、5 分間隔で更新されます。左側のチャートは過去 5 分間の情報を表示していて、3 秒間隔で更新されます。 |
| [アクティブなクエリ] | vRealize Log Insight で現在アクティブになっているクエリの情報を表示します。  |
| [統計情報]      | ログ取り込みの操作および速度に関する統計情報を表示します。<br>さらに詳細な統計情報を表示するには、[統計の詳細を表示] をクリックします。   |

### 次のステップ

[システム監視] ページの情報を使用すると、vRealize Log Insight 仮想アプライアンスのリソースを管理することができます。

## ログ イベントを送信するホストの監視


vRealize Log Insight にログ イベントを送信したすべてのホストおよびデバイスのリストを表示し、それらを監視することができます。

最後にイベントが取り込まれてから 3 か月が経過するとホスト テーブルのエントリの有効期限が切れます。

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[ホスト] をクリックします。

---

**注:** vCenter Server がイベントおよびアラームを送信するように構成されていて、個々の ESXi ホストはログを送信するように構成されていない場合、[ホスト名] 列にはソースとして vCenter Server だけが表示されるのではなく、vCenter Server と個々の ESXi ホストの両方が表示されます。

---

### 次のステップ

管理者権限を持つユーザーは、ホストが非アクティブになっているときに送信されるシステム通知を設定できます。詳細については、[非アクティブなホストについてレポートするシステム通知の構成](#)を参照してください。

## 非アクティブなホストについてレポートするシステム通知の構成

vRealize Log Insight には、指定された期間どのホストが非アクティブであったかを知るために使用できる、組み込みの通知機能があります。

[ホスト] 画面から通知を有効にして、通知をトリガするしきい値を指定します。これは、すべてのホストに対して、またはホストの一部のリストに対して適用することができます。

## Hosts

☒ Inactive hosts notification.

Send alert listing hosts that are inactive for 1 days of last received event ⓘ

The query will run every 1 hour and will only alert once for the defined threshold above.


☐ Inactive hosts notification whitelist ⓘ

**SAVE** **RESET TO DEFAULTS...**

### 前提条件

管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [管理] で、[ホスト] をクリックします。

**注:** vCenter Server がイベントおよびアラームを送信するように構成されていて、個々の ESXi ホストはログを送信するように構成されていない場合、[ホスト名] 列にはソースとして vCenter Server だけが表示されるのではなく、vCenter Server と個々の ESXi ホストの両方が表示されます。

- 3 [ホスト] ページで [ホスト通知が非アクティブです] を選択して、通知がいつ、どのホストに対して送信されるかを設定するためのフォームを表示します。
- 4 ホストが非アクティブである時間がどれだけ経過したら、通知が送信されるかを指定します。

指定できる値の範囲は 10 分から、ホストの有効期間 (TTL) の最大値（デフォルトでは 3 か月）です。

例 :

Send alert listing hosts that are inactive for **8時間** of last received event.

- 5 [非アクティブなホスト通知のホワイトリスト] の設定で、どのホストを通知のための監視対象とするかを制御します。この設定が選択されていない場合、すべての非アクティブなホストについて通知が送信されます。
  - すべての非アクティブなホストについて通知が送信されるようにするには、チェック ボックスをクリアします。
  - 一部の非アクティブなホストについてのみ通知が送信されるようにするには、[非アクティブなホスト通知のホワイトリスト] を選択し、コンマ区切りのリストでホスト名を指定します。
- 6 [保存] をクリックします。

システム通知は、ホストが非アクティブである期間が指定の制限値を超える場合に、[設定 > SMTP サーバ] ページで指定したアドレスに送信されます。

# vRealize Log Insight と VMware 製品の統合

11

vRealize Log Insight を他の VMware 製品と統合して、イベントやログのデータを使用したり、仮想環境で発生するイベントの可視性を高めたりできます。

## VMware vSphere との統合

vRealize Log Insight 管理者ユーザーは、2 分間隔で vCenter Server システムに接続し、vCenter Server システムからイベント、アラーム、およびタスクのデータを収集するように vRealize Log Insight を設定することができます。さらに、vRealize Log Insight は vCenter Server を通して ESXi ホストを構成することもできます。[vRealize Log Insight と vSphere 環境の接続](#) を参照してください。

## VMware vRealize Operations Manager との統合

vRealize Log Insight と vRealize Operations Manager vApp および vRealize Operations Manager Installable を統合できます。Installable バージョンと統合するには、vRealize Operations Manager 構成に変更を加える必要があります。vRealize Log Insight と統合するための vRealize Operations Manager Installable の構成の詳細については、『Log Insight スタート ガイド』を参照してください。

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

### 通知イベント

vRealize Log Insight の管理者ユーザーは、作成したクエリに基づいて vRealize Operations Manager に通知イベントを送信するように vRealize Log Insight を設定できます。[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。

### コンテキストでの起動

コンテキストでの起動は、特定のコンテキストで URL を介して外部アプリケーションを起動できる vRealize Operations Manager の機能です。コンテキストはアクティブな UI 要素およびオブジェクト選択によって定義されます。コンテキストでの起動を使用すると、vRealize Log Insight アダプタから、カスタム ユーザー インターフェイス、および vRealize Operations Manager の vSphere ユーザー インターフェイス内の複数のビューにメニュー項目を追加できます。[vRealize Operations Manager での vRealize Log Insight のコンテキストでの起動の有効化](#) を参照してください。

---

**注:** 通知イベントはコンテキストでの起動の構成に依存しません。コンテキストでの起動機能が有効でない場合も、vRealize Log Insight から vRealize Operations Manager に通知イベントを送信できます。

---

環境が変更された場合、vRealize Log Insight 管理者ユーザーは vRealize Log Insight から vSphere システムを変更、追加、または削除できます。また、アラート通知の送信先である vRealize Operations Manager のインスタンスを変更または削除したり、vSphere システムや vRealize Operations Manager との接続に使用されるパスワードを変更したりできます。

この章には、次のトピックが含まれています。

- [vRealize Log Insight と vSphere 環境の接続](#)
- [vCenter Server インスタンスからイベント、タスク、およびアラームをプルするための vRealize Log Insight の構成](#)
- [vRealize Operations Manager と vRealize Log Insight の併用](#)
- [vRealize Log Insight の vRealize Operations Manager コンテンツ パック](#)

## vRealize Log Insight と vSphere 環境の接続

vSphere 環境からアラーム、イベント、およびタスク データを収集するように vRealize Log Insight を構成するには、vRealize Log Insight を 1 つ以上の vCenter Server システムに接続する必要があります。

vRealize Log Insight は vCenter Server インスタンス、およびそれらが管理する ESXi ホストから 2 種類のデータを収集できます。

- イベント、タスク、およびアラートは特定の意味を持つ構造化されたデータです。構成された vRealize Log Insight は、登録済みの vCenter Server インスタンスからイベント、タスク、およびアラートをプルします。
- ログには vRealize Log Insight で分析できる構造化されていないデータが含まれています。ESXi ホストまたは vCenter Server Appliance インスタンスから vRealize Log Insight に Syslog を介してログをプッシュできます。

### 前提条件

- 実現する統合レベルに応じて、ユーザーが保持しているユーザー認証情報に、vCenter Server システムおよびその ESXi ホストに必要な構成を行うための権限が含まれていることを確認してください。

| 統合レベル                | 必要な権限  |
|----------------------|--|
| イベント、タスク、およびアラームの収集  | <ul style="list-style-type: none"> <li>■ システム.表示</li> </ul> <p><b>注:</b> System.View はシステム定義の権限です。カスタム ロールを追加し、それに権限を付与しない場合、そのロールは読み取り専用ロールとして作成され、System .Anonymous、System.View、および System.Read という 3 つの System 定義権限が付与されます。</p> |
| ESXi ホストでの Syslog 構成 | <ul style="list-style-type: none"> <li>■ ホスト.構成.設定の変更</li> <li>■ ホスト.構成.ネットワーク構成</li> <li>■ ホスト.構成.詳細設定</li> <li>■ ホスト.構成.セキュリティ プロファイルおよびファイアウォール</li> </ul>  |


**注:** vCenter Server インベントリ内のトップレベル フォルダに関する権限を構成し、[子へ伝達] チェック ボックスが選択されていることを確認します。

- vCenter Server システムの IP アドレスまたはドメイン名が判明していることを確認します。



- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [統合] の [vSphere] をクリックします。
- 3 vCenter Server の IP アドレスおよび認証情報を入力して、[接続をテスト] をクリックします。  
サービス アカウント認証情報を使用することをお勧めします。
- 4 (オプション) 別の vCenter Server を登録するには、[vCenter Server を追加] をクリックして、手順 3 ~ 5 を繰り返します。

---

**注:** vCenter Server システムに重複した名前または IP アドレスを登録しないでください。vRealize Log Insight は vCenter Server の名前の重複をチェックしません。登録された vCenter Server システムのリストに重複エントリが含まれていないことを確認する必要があります。

---

- 5 [保存] をクリックします。

#### 次のステップ

- 登録した vCenter Server インスタンスからイベント、タスク、およびアラーム データの収集を開始します。  
[vCenter Server インスタンスからイベント、タスク、およびアラームをプルするための vRealize Log Insight の構成](#)を参照してください。
- vCenter Server が管理する ESXi ホストから Syslog フィードの収集を開始します。[vRealize Log Insight に ログ イベントを転送するための ESXi ホストの構成](#)を参照してください。

## syslog サーバとしての vRealize Log Insight

vRealize Log Insight には、vRealize Log Insight サービスの実行中にアクティブな状態を維持する組み込みの syslog サーバが含まれています。

syslog サーバは、ポート 514/TCP、1514/TCP、および 514/UDP で、他のホストから送信されるログ メッセージの取り込みを待機します。syslog サーバによって取り込まれたメッセージは、vRealize Log Insight Web ユーザー インターフェイスでほぼリアルタイムに検索できます。vRealize Log Insight が受け入れる syslog メッセージの最大長は 10 KB です。

## vRealize Log Insight にログ イベントを転送するための ESXi ホストの構成

ESXi ホストや vCenter Server Appliance インスタンスは vRealize Log Insight で解析可能な非構造化ログデータを生成します。

vRealize Log Insight 管理インターフェイスを使用し、登録済み vCenter Server 上の ESXi ホストを構成して Syslog データを vRealize Log Insight にプッシュします。

---

**注意:** 構成タスクをパラレルに実行すると、ターゲット ESXi ホストの Syslog 設定が正しくなくなることがあります。構成しようとしている ESXi ホストを、管理者権限を持つ別のユーザーが構成していないことを確認します。

---

vRealize Log Insight クラスタは統合ロード バランサを利用して、クラスタの個々のノード間に ESXi と vCenter Server Appliance の Syslog フィードを分散させることができます。

メッセージが vRealize Log Insight に送信される前に ESXi ホスト上で syslog メッセージをフィルタリングする方法の詳細については、『[vSphere のインストールとセットアップ]』ガイドの [ESXi の設定](#) セクションで、「ESXi ホストのログ フィルタリングの構成」のトピックを参照してください。

vCenter Server Appliance から Syslog フィードを構成する方法については、「[vRealize Log Insight にログ イベントを転送するための vCenter Server の構成](#)」を参照してください。

---

**注:** vRealize Log Insight は、ESXi ホスト バージョン 5.5 以降から Syslog データを受信できます。

---

#### 前提条件


- ESXi ホストを管理する vCenter Server がお使いの vRealize Log Insight インスタンスに登録されていることを確認します。または、ESXi ホストを登録し、単一の操作で vCenter Server を構成することができます。
- ユーザーが保持しているユーザー認証情報に、ESXi ホストで Syslog を構成するために必要な権限が含まれていることを確認します。
  - ホスト.構成.詳細設定
  - ホスト.構成.セキュリティ プロファイルおよびファイアウォール

---

**注:** vCenter Server インベントリ内のトップレベル フォルダに関する権限を構成し、[子へ伝達] チェック ボックスが選択されていることを確認します。

---

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [統合] の [vSphere] をクリックします。
- 3 Syslog フィードの受信元の ESXi ホストを管理する vCenter Server インスタンスを特定します。
- 4 [ログを Log Insight に送信するように ESXi ホストを構成します] チェック ボックスを選択します。

デフォルトでは、UDP 経由でログを送信するように、vRealize Log Insight はバージョン 5.5 以降のすべてのアクセス可能な ESXi ホストを構成します。

- 5 (オプション) デフォルトの設定値を変更するには、[詳細オプション] をクリックします。
  - すべての ESXi ホストのプロトコルを変更するには、[すべての ESXi ホストを構成する] を選択し、プロトコルを選択して [OK] をクリックします。
  - 特定の ESXi ホストのログのみを設定するか、選択した ESXi ホストのプロトコルを変更するには、次の手順を実行します。
    - a [特定の ESXi ホストを構成する] を選択します。
    - b [ホストによるフィルタ] リストから 1 つまたは複数のホストを選択します。
    - c プロトコルの値を設定します。
    - d [OK] をクリックします。

- 6 (オプション) クラスタを使用している場合は、[ターゲット] テキスト ボックスのドロップダウン メニューを開き、Syslog フィードを分散するロード バランサのホスト名または IP アドレスを選択します。
- 7 [保存] をクリックします。

## ログ イベントを vRealize Log Insight に転送するための ESXi ホスト構成の変更

ESXi ホストや vCenter Server Appliance インスタンスは vRealize Log Insight で解析可能な非構造化ログデータを生成します。

vRealize Log Insight 管理インターフェイスを使用し、登録済み vCenter Server 上の ESXi ホストを構成して Syslog データを vRealize Log Insight にプッシュします。

---

**注意:** 構成タスクをパラレルに実行すると、ターゲット ESXi ホストの Syslog 設定が正しくなくなることがあります。構成しようとしている ESXi ホストを、管理者権限を持つ別のユーザーが構成していないことを確認します。

---

初期構成が設定された後、vSphere に追加する ESXi ホストをデフォルトのプロトコルを使用して自動的に構成するオプションを有効にすることができます。

vRealize Log Insight クラスタは統合ロード バランサを利用して、クラスタの個々のノード間に ESXi と vCenter Server Appliance の Syslog フィードを分散させることができます。

構成されたメッセージが vRealize Log Insight に送信される前に ESXi ホスト上で Syslog メッセージをフィルタリングする方法の詳細については、『[vSphere のインストールとセットアップ]』ガイドの [ESXi の設定](#) セクションで、「ESXi ホストのログ フィルタリングの構成」のトピックを参照してください。

vCenter Server Appliance から Syslog フィードを構成する方法については、「[vRealize Log Insight にログ イベントを転送するための vCenter Server の構成](#)」を参照してください。

vRealize Log Insight は、ESXi ホスト バージョン 5.5 以降から Syslog データを受信できます。

### 前提条件


- ESXi ホストを管理する vCenter Server がお使いの vRealize Log Insight インスタンスに登録されていることを確認します。
- ユーザーが保持しているユーザー認証情報に、ESXi ホストで Syslog を構成するために必要な権限が含まれていることを確認します。
  - ホスト.構成.詳細設定
  - ホスト.構成.セキュリティ プロファイルおよびファイアウォール

---

**注:** vCenter Server インベントリ内のトップレベル フォルダに関する権限を構成し、[子へ伝達] チェック ボックスが選択されていることを確認します。

---

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [統合] の [vSphere] をクリックします。
- 3 [ログを Log Insight に送信するように ESXi ホストを構成します] チェック ボックスを選択します。

- 4 [詳細オプション] をクリックします。
- 5 選択された ESXi ホストのプロトコルを変更するには、次の手順を実行します。
  - a [ホストによるフィルタ] リストから 1 つまたは複数のホストを選択します。
  - b 選択されているプロトコルが目標のプロトコルであるかどうかを確認し、異なる場合は該当のプロトコルを選択します。
  - c vRealize Log Insight クラスタに追加したときに、ESXi ホストをデフォルトのプロトコルで自動的に構成する場合には、[すべての ESXi ホストを自動的に構成する] を選択します。
  - d [構成] をクリックして選択したホストの構成を開始します。ESXi のダイアログ ボックスが閉じます。
  - e メッセージ ダイアログ ボックスで、[OK] をクリックします。
  - f プロトコル設定を変更した場合は、[ESXi 構成] ダイアログ ボックスを閉じた後に、メイン ウィンドウで [保存] をクリックします。
- 6 (オプション) クラスタを使用している場合は、[vSphere 統合] ページの [ターゲット] テキスト ボックスのドロップダウン メニューを開き、ロード バランサのホスト名または IP アドレスを選択してロード バランサを指定できます。

## vRealize Operations Manager の vRealize Log Insight イベント通知

vRealize Log Insight で、作成したアラート クエリに基づいて vRealize Operations Manager にイベント通知を送信するように設定できます。

vRealize Log Insight で通知アラートを構成するには、vRealize Operations Manager で通知イベントに関連付けられたリソースを選択します。[vRealize Operations Manager に通知イベントを送信する Log Insight のアラート クエリを追加する](#)を参照してください。

以下にリストするのは、通知イベントが表示される vRealize Operations Manager のユーザー インターフェイスのセクションです。

- ホーム > [推奨] ダッシュボード > [トップ健全性アラート (子孫)] ウィジェット
- ホーム > [アラート] タブ
- 通知イベントを持つウィジェットを含むすべてのカスタム ダッシュボード

通知イベントがどこに表示されるのかの詳細については、[VMware vRealize Operations Manager のドキュメント センター](#)を参照してください。

## vRealize Log Insight にログ イベントを転送するための vCenter Server の構成

vSphere 統合は、タスクとイベントを vCenter Server から収集し、各 vCenter Server コンポーネントから低レベルの内部ログを収集しません。これらのログは vSphere コンテンツ パックによって利用されます。

vCenter Server 6.5 以降のリリースの構成は、vCenter Server Appliance 管理インターフェイスで行う必要があります。ログ イベントを vCenter Server から転送する方法については、別のマシンへの vCenter Server Appliance ログ ファイルのリダイレクトに関する vSphere のドキュメントを参照してください。

以前のバージョンの vSphere の場合、ログのルーティングに使用できる Syslog デーモンが vCenter Server Appliance に含まれていますが、vRealize Log Insight エージェントをインストールすることをお勧めします。

vRealize Log Insight エージェントのインストールについては、vRealize Log Insight エージェントの操作 を参照してください。

vSphere コンテンツ パックには vCenter Server のインストールから収集する特定のログ ファイルを定義するエージェント グループが含まれています。構成は <https://LogInsightServerFqdnOrIP/contentpack?contentPackId=com.vmware.vsphere> で確認することができます。

エージェント グループの操作の詳細については、[9 章 一元化されたエージェントの構成およびエージェント グループの操作](#)を参照してください。

vCenter Server ログ ファイルの場所については、<http://kb.vmware.com/kb/1021804> および <http://kb.vmware.com/kb/1021806> を参照してください。

## vCenter Server インスタンスからイベント、タスク、およびアラームをプルするための vRealize Log Insight の構成

イベント、タスク、およびアラートは特定の意味を持つ構造化されたデータです。1 つ以上の vCenter Server システムからアラーム、イベント、およびタスク データを収集するように vRealize Log Insight を構成できます。

管理 UI を使用して、vCenter Server システムに接続するように vRealize Log Insight を構成します。情報は vSphere Web Services API を使用して vCenter Server システムからプルされ、vRealize Log Insight Web ユーザー インターフェイスに vSphere コンテンツ パックとして表示されます。

vSphere 6.5 には、新しいネイティブの高可用性ソリューションがあります。高可用性およびロード バランサの使用の詳細については、[www.vmware.com](http://www.vmware.com) にあるホワイト ペーパー 『VMware vSphere 6.5 の新機能』を参照してください。

---

**注:** vRealize Log Insight がアラーム、イベント、およびタスクのデータをプルできるのは、vCenter Server 5.5 以降からのみです。

---

### 前提条件


システム.表示 権限を含むユーザー認証情報を保持していることを確認します。

---

**注:** vCenter Server インベントリ内のトップレベル フォルダに関する権限を構成し、[子へ伝達] チェック ボックスが選択されていることを確認します。

---

### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [統合] の [vSphere] をクリックします。
- 3 データの収集元の vCenter Server インスタンスを特定し、[vCenter Server のイベント、タスク、およびアラームを収集する] チェック ボックスを選択します。
- 4 [保存] をクリックします。

vRealize Log Insight は 2 分おきに vCenter Server に接続し、最後に成功したポーリング以降のすべての新情報を取り込みます。

### 次のステップ

- vSphere コンテンツ パックまたはカスタム クエリを使用して、vSphere イベントを分析します。
- vSphere コンテンツ パックのアラートまたはカスタム アラートを有効にします。

## vRealize Operations Manager と vRealize Log Insight の併用

### vRealize Operations Manager との統合の要件

vRealize Log Insight と vRealize Operations Manager を統合するには、vRealize Operations Manager に対して認証できるように vRealize Log Insight の認証情報を指定する必要があります。

vRealize Operations Manager は、ローカル ユーザー アカウントと複数の LDAP ソースの両方をサポートしています。

展開に vRealize Log Insight の VMware Identity Manager 統合を使用する場合、VMware Identity Manager のフォールバック URL と vRealize Operations Manager の統合先は、同じ値となっている必要があります。

#### 前提条件

統合ユーザー アカウントに、vRealize Operations Manager でオブジェクトを操作するための権限があることを確認してください。ローカルまたは Active Directory ユーザー アカウントに必要な最小権限を参照してください。

#### 手順

- ◆ ローカル ユーザー アカウントのユーザー名を決定するには：
  - a vRealize Operations Manager の Web インターフェイスから [アクセス コントロール] を選択します。
  - b 統合ユーザーを識別または作成します。[Source Type (ソース タイプ)] フィールドは [ローカル ユーザー] です。
  - c [ユーザー名] フィールドの値を書き留めます。vRealize Log Insight 管理ユーザー インターフェイスで統合を構成する場合は、このユーザー名を指定します。
- ◆ vRealize Log Insight で指定する必要がある LDAP ユーザー アカウントのユーザー名の形式を特定するには、次の手順を実行してください。
  - a vRealize Operations Manager の Web インターフェイスから [アクセス コントロール] を選択します。
  - b 統合ユーザーを識別または作成します。[ユーザー名] および [Source Type (ソース タイプ)] フィールドを書き留めます。たとえば、ソース [Active Directory - ad] からのユーザーは **integration@example.com** のように名前が付けられます。
  - c [Authentication Sources (認証ソース)] を選択します。
  - d 手順 b. の [ソース タイプ] に対応する認証ソースを特定します。[ソースの表示名] フィールドを書き留めます。たとえば、「ad」などです。
  - e vRealize Log Insight 管理ユーザー インターフェイスで入力する必要があるユーザー名は、UserName@SourceDisplayName 形式で手順 3 と手順 5 の名前の組み合わせになります。たとえば、integration@example.com@ad などです。

## ローカルまたは Active Directory ユーザー アカウントに必要な最小権限

vRealize Log Insight と vRealize Operations Manager を統合するには、vRealize Operations Manager に対して認証できるように vRealize Log Insight に認証情報を指定する必要があります。vRealize Operations Manager のオブジェクトを操作する場合、ユーザー アカウントには必要な権限があります。

コンテキストでの起動の目的でユーザーに権限を割り当てる場合、ユーザーはアラートの統合も構成できます。アラートの統合テーブルの情報をを使用して、アラートの統合の権限のみを割り当てます。

表 11-1. アラートの統合

| 操作   | 選択する権限とオブジェクト   |
|--|---|
| リストされた権限を使用してカスタム ロールを作成します。   | <ol style="list-style-type: none"> <li>1 管理 -&gt; リソース種別管理 [すべてを選択]</li> <li>2 管理 -&gt; リソース管理 [すべてを選択]</li> <li>3 管理 -&gt; Rest API <ol style="list-style-type: none"> <li>a その他すべて、読み取り、書き込み API</li> <li>b API への読み取りアクセス</li> </ol> </li> </ol> |
| 上記のロールをローカルまたは Active Directory ユーザー（新規または既存）に割り当て、割り当てるオブジェクト/オブジェクト階層を選択します。 | <ol style="list-style-type: none"> <li>1 アダプタ インスタンス -&gt; vRealizeOpsMgrAPI [すべてを選択]</li> <li>2 vSphere ホストおよびクラスタ [すべてを選択]</li> <li>3 vSphere ネットワーク [すべてを選択]</li> <li>4 vSphere ストレージ [すべてを選択]</li> </ol>  |

表 11-2. コンテキスト統合での起動

コンテキスト統合での起動を使用するには、管理者権限が必要です。アラートとコンテキストでの起動の両方を有効にしている場合は、管理者権限を持つユーザーが必要です。

| 操作                         | 選択する権限とオブジェクト   |
|----------------------------|---|
| ユーザー アカウントに管理者のロールを割り当てます。 | <p>[グループと権限の割り当て] ページの [オブジェクト] タブから：</p> <ol style="list-style-type: none"> <li>1 [ロールの選択] で、[管理者] を選択します。</li> <li>2 [このロールをユーザーに割り当てる] を選択します。</li> <li>3 [システム内のすべてのオブジェクトに対するアクセスを許可する] を選択します。</li> </ol> |

## vRealize Operations Manager に通知イベントを送信する vRealize Log Insight の構成

vRealize Operations Manager にアラート通知を送信するように vRealize Log Insight を構成できます。

vRealize Log Insight と vRealize Operations Manager vApp および vRealize Operations Manager Installable を統合できます。Installable バージョンと統合するには、vRealize Operations Manager 構成に変更を加える必要があります。vRealize Log Insight と統合するための vRealize Operations Manager Installable の構成の詳細については、『Log Insight スタート ガイド』を参照してください。

vRealize Log Insight のアラートを vRealize Operations Manager と統合すると、単一のユーザー インターフェイスで環境に関するすべての情報を表示できます。



複数の vRealize Log Insight インスタンスから通知イベントを単一の vRealize Operations Manager インスタンスに送信できます。vRealize Operations Manager インスタンスごとに 1 つの vRealize Log Insight に対してコンテキストでの起動を有効にできます。

vRealize Log Insight は vRealize Operations Manager REST API を使用して、コンテキストでの起動のアダプタを構成するためにリソースと vRealize Operations Manager の関係を作成します。

#### 前提条件


- vRealize Operations Manager で、必要な権限を持つ統合ユーザー アカウントを作成します。詳細については、[vRealize Operations Manager との統合の要件](#)を参照してください。
- ターゲット vRealize Operations Manager インスタンスの 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。
- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

---

**注:** ロード バランサが設定された vRealize Operations Manager クラスタを実行している環境では、ロード バランサが利用可能な場合、その IP アドレスを使用できます。

---

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [統合] で、[vRealize Operations Manager] を選択します。
- 3 マスター ノードまたはロード バランサーを構成する場合は、その IP アドレスまたはホスト名を入力します。vRealize Operations Manager ユーザー認証情報を使用して [接続をテスト] をクリックします。vRealize Log Insight はこの認証情報を使用して vRealize Operations Manager に通知イベントをプッシュします。設定されたユーザーが統合を機能させるために必要な最小権限を持っていることを確認してください。[ローカルまたは Active Directory ユーザー アカウントに必要な最小権限](#) を参照してください。
- 4 [vRealize Operations Manager] ペインで [アラート統合を有効にする] を選択します。
- 5 [保存] をクリックします。

#### 次のステップ

- vRealize Operations Manager ユーザー インターフェイスの関連するページで、vRealize Log Insight が送信する通知イベントを確認してください。

## vRealize Operations Manager での vRealize Log Insight のコンテキストでの起動の有効化

vRealize Log Insight に関連したメニュー項目を表示し、オブジェクト固有のクエリを使用して vRealize Log Insight を起動するように vRealize Operations Manager を構成できます。

vRealize Log Insight と vRealize Operations Manager vApp および vRealize Operations Manager Installable を統合できます。



vApp のインストールおよび Installable (Windows、Linux) と連携するには、vRealize Operations Manager の設定をさらに変更する必要があります。 [vRealize Log Insight 4.0 ドキュメント センター](#)で、vRealize Operations Manager 6.x 以降での vRealize Log Insight 管理パック (アダプタ) のインストールについてのトピックを参照してください。

vRealize Operations Manager 6.0 以降では、vRealize Log Insight 管理パックはプリインストールされています。設定を変更する必要はありません。

vRealize Operations Manager 6.5 以降では、vRealize Operations Manager Installable (Windows バージョン) は廃止されます。

---


**重要:** vRealize Operations Manager の 1 つのインスタンスがサポートするのは、vRealize Log Insight の 1 つのインスタンスに対するコンテキストでの起動のみです。vRealize Log Insight は他のインスタンスがすでに vRealize Operations Manager に登録されているかどうかを確認しないため、別のユーザーの設定がオーバーライドされる可能性があります。

---

#### 前提条件

- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。
- ターゲット vRealize Operations Manager インスタンスの 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。
- 必要なユーザー認証情報を持っていることを確認します。 [ローカルまたは Active Directory ユーザー アカウントに必要な最小権限](#) を参照してください。
- vRealize Operations Manager 6.5 以降を使用している場合、 [vRealize Operations Manager 6.5 情報センター](#) を参照して、コンテキストでの起動を有効にするための手順を使用してください。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [統合] で、[vRealize Operations Manager] を選択します。
- 3 vRealize Operations Manager マスター ノードまたはロード バランサーを構成する場合は、その IP アドレスまたは FQDN を入力し、[接続をテスト] をクリックします。

---

**注:** コンテキストでの起動機能を使う場合は、管理者権限を持つ vRealize Operations Manager ユーザーを指定する必要があります。

---

- 4 [保存] をクリックします。

vRealize Log Insight によって vRealize Operations Manager インスタンスが構成されます。この処理には数分かかることがあります。

vRealize Log Insight に関連する項目が vRealize Operations Manager のメニューに表示されます。

## 次のステップ

vRealize Operations Manager インスタンスから vRealize Log Insight クエリを起動します。 [vRealize Log Insight のコンテキストでの起動](#)を参照してください。

## vRealize Log Insight のコンテキストでの起動

vRealize Log Insight のコンテキストでの起動を有効にすると、vRealize Log Insight のリソースが vRealize Operations Manager に作成されます。

リソース識別子には vRealize Log Insight インスタンスの IP アドレスが含まれ、vRealize Operations Manager で vRealize Log Insight を開くために使用されます。

### vRealize Operations Manager 6.5 以降でのコンテキストでの起動

コンテキストでの起動を有効にする方法については、[vRealize Operations Manager 情報センター](#)を参照してください。

### vRealize Operations Manager 6.4 以前の vSphere ユーザー インターフェイスを使用したコンテキストでの起動

vRealize Log Insight に関連する、コンテキストでの起動オプションが vSphere ユーザー インターフェイスの[アクション] ドロップダウン メニューに表示されます。これらのメニュー項目を使用して vRealize Log Insight を開き、vRealize Operations Manager のオブジェクトからイベント ログを検索できます。

使用可能なコンテキストでの起動アクションは、vRealize Operations Manager インベントリで選択するオブジェクトに応じて異なります。クエリの時間範囲を 60 分に制限してからコンテキストでの起動オプションをクリックします。

表 11-3. vRealize Operations Manager ユーザー インターフェイスのオブジェクトおよび対応するコンテキストでの起動オプションとアクション

| vRealize Operations Manager で選択したオブジェクト | [アクション] ドロップダウン メニューのコンテキストでの起動オプション | vRealize Operations Manager のアクション                                     | vRealize Log Insight のアクション   |
|---|--------------------------------------|--|---|
| ワールド                                    | [vRealize Log Insight を開く]           | vRealize Log Insight を開きます。  | vRealize Log Insight に[インタラクティブ分析] タブが表示されます。                                       |
| vCenter Server                          | [vRealize Log Insight を開く]           | vRealize Log Insight を開きます。  | vRealize Log Insight に[インタラクティブ分析] タブが表示されます。                                       |
| データセンター                                 | [vRealize Log Insight でのログの検索]       | vRealize Log Insight を開き、選択したデータセンター オブジェクトにあるすべてのホスト システムのリソース名を渡します。 | vRealize Log Insight に [対話形式の分析] タブが表示され、データ センター内のホストの名前を含むイベント ログを検索するクエリが実行されます。 |
| クラスタ                                    | [vRealize Log Insight でのログの検索]       | vRealize Log Insight を開き、選択したクラスタ オブジェクトにあるすべてのホスト システムのリソース名を渡します。    | vRealize Log Insight に [対話形式の分析] タブが表示され、クラスタ内のホストの名前を含むイベント ログを検索するクエリが実行されます。     |


| vRealize Operations Manager で選択したオブジェクト | [アクション] ドロップダウン メニューのコンテキストでの起動オプション | vRealize Operations Manager のアクション                                   | vRealize Log Insight のアクション  |
|---|--------------------------------------|--|--|
| ホスト システム                                | [vRealize Log Insight でのログの検索]       | vRealize Log Insight を開き、選択したホスト オブジェクトのリソース名を渡します。                  | vRealize Log Insight に [対話形式の分析] タブが表示され、選択したホスト システムの名前を含むイベント ログを検索するクエリが実行されます。                   |
| 仮想マシン                                   | [vRealize Log Insight でのログの検索]       | vRealize Log Insight を開き、選択した仮想マシンの IP アドレスおよび関連ホスト システムのリソース名を渡します。 | vRealize Log Insight に [対話形式の分析] タブが表示され、仮想マシンの IP アドレスおよび仮想マシンが常駐するホストの名前を含むイベント ログを検索するクエリが実行されます。 |

[アラート] タブでアラートを選択し、コンテキスト内メニューから [Log Insight でのログの検索] を選択すると、アラートをトリガするまでのクエリの時間範囲が 1 時間に制限されます。たとえば、アラートを午後 2:00 にトリガした場合は、vRealize Log Insight に午後 1:00 から午後 2:00 の間に発生したすべてのログ メッセージが表示されます。これにより、アラートをトリガしたイベントを識別できます。

vRealize Operations Manager のメトリック チャートから vRealize Log Insight を開くことができます。vRealize Log Insight で実行するクエリの時間範囲は、メトリック チャートの時間範囲と一致します。

**注:** 仮想アプライアンスの時間設定が異なる場合は、vRealize Log Insight および vRealize Operations Manager のメトリック チャートに表示される時間が異なる可能性があります。

#### vRealize Operations Manager 6.4 以前のユーザー インターフェイスにおけるコンテキストでの起動

コンテキストでの起動アイコン  はユーザー インターフェイスの複数のページに表示されますが、vRealize Log Insight の通知イベントが表示される次のページからのみ vRealize Log Insight を起動できます。

- [アラート概要] ページ。
- vRealize Log Insight アラート通知の [アラート概要] ページ。
- vRealize Log Insight 通知アラートを選択しているときのダッシュボードのアラート ウィジェット。

カスタム ユーザー インターフェイスで vRealize Log Insight イベント通知を選択すると、両方のコンテキストでの起動アクションのいずれかを選択できます。

表 11-4. vRealize Operations Manager UI のコンテキストでの起動オプションとアクション

| vRealize Operations Manager のコンテキストでの起動オプション | vRealize Operations Manager のアクション                  | vRealize Log Insight のアクション  |
|--|---|--|
| [vRealize Log Insight を開く]                   | vRealize Log Insight を開きます。                         | vRealize Log Insight に [ダッシュボード] タブが表示され、vSphere Overview ダッシュボードがロードされます。 |
| [vRealize Log Insight でのログの検索]               | vRealize Log Insight を開き、イベント通知をトリガしたクエリの ID を渡します。 | vRealize Log Insight に [対話形式の分析] タブが表示され、イベント通知をトリガしたクエリが実行されます。           |

vRealize Log Insight 以外のアラートを選択すると、コンテキストでの起動メニューに [vRealize Log Insight での仮想マシン ログおよびホスト ログの検索] メニュー項目が表示されます。このメニュー項目を選択すると、vRealize Operations Manager は vRealize Log Insight を開き、アラートをトリガしたオブジェクトの識別子を渡します。vRealize Log Insight は、リソース識別子を使用して、使用可能なログ イベントで検索を実行します。

## 双方向のコンテキストでの起動

コンテキストでの起動は vRealize Log Insight から vRealize Operations Manager に対しても利用可能です。

vRealize Log Insight を vRealize Operations Manager に統合する場合、コンテキストでの起動を vRealize Log Insight イベントから実行することができます。それには、イベントの左のギア アイコンを選択し、vRealize Operations Manager で表示するオプションを選択します。

vRealize Operations Manager から vRealize Log Insight のコンテキストでの起動の詳細については、[vRealize Log Insight のコンテキストでの起動](#)を参照してください。

### 手順

- 1 vRealize Log Insight で、[インタラクティブ分析] タブに移動します。
- 2 インベントリ マッピング フィールドを含むイベントを見つけ、イベントをマウスでポイントします。
- 3 ギア アイコンをクリックし、ドロップダウン メニューから vRealize Operations Manager の [分析を開く] を選択します。

新しいブラウザ タブが開き、vRealize Log Insight に統合された vRealize Operations Manager インスタンスが表示されます。認証すると、オブジェクトが選択された vRealize Operations Manager の [環境] > [分析] セクションに移動します。

---

**注:** 同じ vRealize Operations Manager インスタンスに複数の vRealize Log Insight インスタンスが接続されるときは、コンテキストでの起動の機能は vRealize Operations Manager に統合された最後の vRealize Log Insight インスタンスでのみ使用できます。つまり、前回別の vRealize Log Insight インスタンスに統合された vRealize Operations Manager インスタンスに vRealize Log Insight インスタンスが統合されると、コンテキストでの起動の機能はオーバーライドされます。

---

## vRealize Operations Manager での vRealize Log Insight のコンテキストでの起動の無効化

vRealize Operations Manager インスタンスから vRealize Log Insight アダプタをアンインストールして、vRealize Operations Manager ユーザー インターフェイスから vRealize Log Insight に関連したメニュー項目を削除することができます。


コンテキストでの起動を無効にするには、vRealize Log Insight の管理 UI を使用します。vRealize Log Insight へのアクセス権がない場合、または vRealize Operations Manager との接続が無効になる前に vRealize Log Insight インスタンスが削除されている場合は、vRealize Log Insight を vRealize Operations Manager の管理 UI から登録解除することができます。vRealize Operations Manager 管理ポータルヘルプを参照してください。

**注意:** vRealize Operations Manager の 1 つのインスタンスがサポートするのは、vRealize Log Insight の 1 つのインスタンスに対するコンテキストでの起動のみです。無効にするインスタンスを登録した後に、vRealize Log Insight の別のインスタンスが登録されている場合は、2 番目のインスタンスによって最初の設定がオーバーライドされ、通知は送信されません。

#### 前提条件

- 管理者の編集 権限を持っているユーザーとして vRealize Log Insight Web ユーザー インターフェイスにログインしていることを確認します。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。

#### 手順

- 1 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 2 [統合] で、[vRealize Operations Manager] を選択します。
- 3 [コンテキストでの起動を有効にする] チェック ボックスの選択を解除します。
- 4 [保存] をクリックします。

vRealize Log Insight は vRealize Log Insight アダプタを削除するように vRealize Operations Manager インスタンスを構成します。この処理には数分かかることがあります。

## DNS 検索パスとドメイン

DNS 検索パスとドメインを追加して vRealize Operations Manager インベントリの一致を向上させることができます。

DNS 検索パスとドメインを追加すると、vRealize Log Insight にログ メッセージを送信するホストの IP アドレスに仮想マシン ラベルと検索ドメインが解決するときの一致を向上させることができます。たとえば、vRealize Operations Manager に `linux_01` という名前の仮想マシンがあり、ホスト 名 `linux_01.company.com` が `192.168.10.10` に解決される場合、検索ドメインを追加すると、vRealize Log Insight はそのリソースを認識して一致させることができます。

#### 手順

- 1 vRealize Log Insight 仮想アプライアンスのゲスト シャットダウンを実行します。
- 2 仮想マシンをパワーオフしたら、[設定の編集] を選択します。
- 3 [オプション] タブを選択します。
- 4 [vApp オプション] > [詳細] から、[プロパティ] をクリックします。

- 5 `vami.searchpath.VMware_vCenter_Log_Insight` および `vami.domain.VMware_vCenter_Log_Insight` キーを見つけます。

キーが存在しない場合は、作成します。

- 6 DNS 検索パスとドメインを設定します。たとえば、`ny01.acme.local` など。

- 7 仮想アプライアンスをパワーオンします。

#### 次のステップ

vRealize Log Insight が起動した後、ログインして `/etc/resolv.conf` ファイルのコンテンツを調べ、DNS 構成を検証することができます。ファイルの終わりの近くに検索とドメインのオプションが表示されます。

## vRealize Log Insight アダプタの削除

コンテキストでの起動を vRealize Operations Manager 6.2 以降のインスタンスで有効にする場合、vRealize Log Insight が vRealize Log Insight アダプタのインスタンスを vRealize Operations Manager インスタンス上に作成します。

vRealize Log Insight をアンインストールしても、vRealize Operations Manager インスタンスにアダプタのインスタンスは残ります。したがって、コンテキストでの起動のメニュー項目は引き続きアクションメニューに表示され、存在しなくなった vRealize Log Insight インスタンスを参照します。

vRealize Operations Manager でコンテキストでの起動機能を無効にするには、vRealize Operations Manager インスタンスから vRealize Log Insight アダプタを削除する必要があります。

コマンドライン ユーティリティの cURL を使用して、vRealize Operations Manager に REST コールを送信できます。

---

**注:** これらの手順は、コンテキストでの起動が有効な場合のみ実行する必要があります。

---

#### 前提条件

- システムに cURL がインストールされていることを確認します。このツールは、vRealize Operations Manager 仮想アプライアンスにプリインストールされており、IP アドレス `127.0.0.1` を使用して、このアプライアンスから手順を実行できます。
- ターゲット vRealize Operations Manager インスタンスの 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。
- 所有する vRealize Operations Manager ライセンスに応じて、管理パックの削除に必要な最小認証情報を持っていることを確認します。[ローカルまたは Active Directory ユーザー アカウントに必要な最小権限](#) を参照してください。

#### 手順

- 1 cURL で vRealize Operations Manager 仮想アプライアンスに次のクエリを実行して、vRealize Log Insight アダプタを検出します。

```
curl -k -u "admin" https://ipaddress/suite-api/api/adapterkinds/LogInsight/resourcekinds/LogInsightLogServer/resources
```

ここでは、*admin* は管理者のログイン名で、*ipaddress* は vRealize Operations Manager インスタンスの IP アドレスまたはホスト名になります。ユーザー： *admin* のパスワードを入力するように求められます。

cURL のアウトプットから識別子： `<ops:resource creationTime="{TIMESTAMP}"`

`identifier="{GUID}"` に割り当てられた GUID 値を特定します。アダプタ インスタンスを削除するコマンド内で、この GUID 値を使用できます。

- 2 次のコマンドを実行して、vRealize Log Insight アダプタを削除します。

```
curl -k -u "admin" -X DELETE https://ipaddress/suite-api/api/adapters/{GUID}
```

ここでは、*admin* は管理者のログイン名で、*ipaddress* は vRealize Operations Manager インスタンスの IP アドレスまたはホスト名になります。ユーザー： *admin* のパスワードを入力するように求められます。

vRealize Operations Manager 内のメニューから vRealize Log Insight のコンテキストでの起動項目が削除されます。コンテキストでの起動の詳細については、vRealize Log Insight の製品内ヘルプの「vRealize Log Insight コンテキストでの起動」を参照してください。

## vRealize Log Insight の vRealize Operations Manager コンテンツ パック

vRealize Log Insight の vRealize Operations Manager コンテンツ パックには、vRealize Operations Manager インスタンスからリダイレクトされたすべてのログを分析するためのダッシュボード、抽出されたフィールド、保存されたクエリ、およびアラートが含まれています。

vRealize Operations Manager コンテンツ パックを使用すると、vRealize Operations Manager インスタンスからリダイレクトされたすべてのログを分析できます。コンテンツ パックにはダッシュボード、クエリ、およびアラートが含まれていて、vRealize Operations Manager 管理者は診断およびトラブルシューティングを行うことができます。ダッシュボードは分析、ユーザー インターフェイス、アダプタなどの vRealize Operations Manager の主要コンポーネントに従ってグループ化されているため、より管理しやすくなります。vRealize Operations Manager の通知イベントや E メールを管理者に送信するためのさまざまなアラートを有効にすることができます。

[https://solutionexchange.vmware.com/store/loginsight?src=Product\\_Product\\_LogInsight\\_YES\\_US](https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US) から vRealize Operations Manager コンテンツ パックをダウンロードできます。

「[コンテンツ パックの操作](#)」を参照してください。



# vRealize Log Insight に関するセキュリティの考慮事項

# 12

vRealize Log Insight 機能を使用して、環境を攻撃から保護します。

この章には、次のトピックが含まれています。

- [ポートおよび外部インターフェイス](#)
- [vRealize Log Insight 構成ファイル](#)
- [vRealize Log Insight のパブリック キー、証明書、およびキーストア](#)
- [vRealize Log Insight のライセンスおよび EULA ファイル](#)
- [vRealize Log Insight ログ ファイル](#)
- [vRealize Log Insight ユーザー アカウント](#)
- [vRealize Log Insight ファイアウォールに関する推奨事項](#)
- [セキュリティ アップデートおよびパッチ](#)

## ポートおよび外部インターフェイス

vRealize Log Insight では、必要な特定のサービス、ポート、および外部インターフェイスが使用されます。

### 通信ポート

vRealize Log Insight は、このトピックにリストされた通信ポートとプロトコルを使用します。必要なポートは、ソース、ユーザー インターフェイス、クラスタ間、外部サービスのどれに対して必要なのか、あるいはファイアウォールによって安全にブロックできるのかに応じて編成されます。一部のポートは対応する統合を有効にする場合のみ使用されます。

---

**注:** vRealize Log Insight は、WAN クラスタリング（ジオクラスタリング、高可用性クラスタリング、リモート クラスタリングとも呼ばれます）をサポートしません。クラスタ内のすべてのノードは同じレイヤ 2 の LAN に展開する必要があります。また、通信を適切に行うには、このセクションで説明されているポートがノード間で開かれている必要があります。

---



vRealize Log Insight ネットワーク トラフィックには複数のソースがあります。

|                                     |  |
|-------------------------------------|--|
| <b>管理ワークステーション</b>                  | システム管理者が vRealize Log Insight 仮想アプライアンスをリモートに管理する場合に使用するマシン。   |
| <b>ユーザー ワークステーション</b>               | vRealize Log Insight ユーザーがブラウザを使用して vRealize Log Insight の Web インターフェイスにアクセスするマシン。   |
| <b>ログの送信元システム</b>                   | 分析および検索のために vRealize Log Insight にログを送信するエンドポイント。たとえば、エンドポイントには ESXi ホスト、仮想マシン、IP アドレスを持つ任意のシステムなどが含まれます。                  |
| <b>Log Insight Agents</b>           | Windows または Linux マシン上にあり、API を介してオペレーティング システムのイベントおよびログを vRealize Log Insight に送信するエージェント。                               |
| <b>vRealize Log Insight アプライアンス</b> | vRealize Log Insight サービスが配置されている任意の vRealize Log Insight 仮想アプライアンス (マスターまたはワーカー)。アプライアンスの基本オペレーティング システムは SUSE 11 SP3 です。 |

## データを送信するソースに必要なポート

vRealize Log Insight にデータを送信するソースからのネットワーク トラフィックに対して次のポートが開いている必要があります。これは、クラスタ外部からの接続とクラスタ ノード間でロード バランシングされた接続の両方に使用されます。

| ソース                         | ターゲット                        | ポート        | プロトコル   | サービスの説明                            |
|-----------------------------|------------------------------|------------|---------|------------------------------------|
| ログの送信元システム                  | vRealize Log Insight アプライアンス | 514        | TCP、UDP | 転送者の送信先として構成された送信 Syslog トラフィック    |
| ログの送信元システム                  | vRealize Log Insight アプライアンス | 1514, 6514 | TCP     | SSL を介して送信される Syslog データ           |
| vRealize Log Insight エージェント | vRealize Log Insight アプライアンス | 9000       | TCP     | Log Insight 取り込み API               |
| vRealize Log Insight エージェント | vRealize Log Insight アプライアンス | 9543       | TCP     | SSL を介して送信される Log Insight 取り込み API |

## ユーザー インターフェイスに必要なポート

vRealize Log Insight ユーザー インターフェイスを使用する必要があるネットワーク トラフィックに対して次のポートが開いている必要があります。これは、クラスタ外部の接続とクラスタ ノード間でロード バランシングされた接続の両方に使用されます。

| ソース            | ターゲット                        | ポート | プロトコル | サービスの説明               |
|----------------|------------------------------|-----|-------|-----------------------|
| 管理ワークステーション    | vRealize Log Insight アプライアンス | 22  | TCP   | SSH: Secure Shell の接続 |
| ユーザー ワークステーション | vRealize Log Insight アプライアンス | 80  | TCP   | HTTP: Web インターフェイス    |
| ユーザー ワークステーション | vRealize Log Insight アプライアンス | 443 | TCP   | HTTPS: Web インターフェイス   |

## クラスタ ノード間に必要なポート

ワーカー ノードからネットワークにアクセスする場合は、最大限のセキュリティを確保するために、vRealize Log Insight マスター ノードの次のポートのみを開くようにしてください。これらのポートは、クラスタ ノード間でロード バランシングされたソースおよびユーザー インターフェイス トラフィックに使用されるポートに追加されます。

| ソース                          | ターゲット                        | ポート                | プロトコル | サービスの説明                             |
|------------------------------|------------------------------|--------------------|-------|-------------------------------------|
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 7000               | TCP   | Cassandra のレプリケーションおよびクエリ           |
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 9042               | TCP   | ネイティブ プロトコル クライアント用の Cassandra サービス |
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 9160               | TCP   | Thrift クライアント用の Cassandra サービス      |
| vRealize Log Insight アプライアンス | vRealize Log Insight アプライアンス | 59778, 16520-16580 | TCP   | vRealize Log Insight Thrift サービス    |

## 外部サービスに必要なポート

vRealize Log Insight クラスタ ノードからリモート サービスへの送信ネットワーク トラフィックに対して次のポートが開いている必要があります。

| ソース                          | ターゲット    | ポート | プロトコル    | サービスの説明   |
|------------------------------|----------|-----|----------|---|
| vRealize Log Insight アプライアンス | NTP サーバ  | 123 | UDP      | NTPD: NTP 時刻を同期します。<br><br><b>注:</b> ポートが開くのは、NTP 時刻同期を使用するように選択した場合のみです。 |
| vRealize Log Insight アプライアンス | メール サーバ  | 25  | TCP      | SMTP: 送信アラートのメール サービス   |
| vRealize Log Insight アプライアンス | メール サーバ  | 465 | TCP      | SMTPS: SSL を介した送信アラートのメール サービス  |
| vRealize Log Insight アプライアンス | DNS サーバー | 53  | TCP, UDP | DNS: 名前解決サービス   |
| vRealize Log Insight アプライアンス | AD サーバ   | 389 | TCP, UDP | Active Directory  |

| ソース                          | ターゲット                               | ポート  | プロトコル   | サービスの説明  |
|------------------------------|-------------------------------------|------|---------|--|
| vRealize Log Insight アプライアンス | AD サーバ                              | 636  | TCP     | SSL を介した Active Directory  |
| vRealize Log Insight アプライアンス | AD サーバ                              | 3268 | TCP     | Active Directory グローバル カタログ  |
| vRealize Log Insight アプライアンス | AD サーバ                              | 3269 | TCP     | Active Directory グローバル カタログ SSL  |
| vRealize Log Insight アプライアンス | AD サーバ                              | 88   | TCP、UDP | ケルベロス  |
| vRealize Log Insight アプライアンス | vCenter Server                      | 443  | TCP     | vCenter Server Web サービス  |
| vRealize Log Insight アプライアンス | vRealize Operations Manager アプライアンス | 443  | TCP     | vRealize Operations Web サービス   |
| vRealize Log Insight アプライアンス | サードパーティのログ マネージャ                    | 514  | TCP、UDP | syslog データ   |
| vRealize Log Insight アプライアンス | サードパーティのログ マネージャ                    | 9000 | CFAPI   | 転送者の送信先として構成された送信 Log Insight 取り込み API (CFAPI) トラフィック                    |
| vRealize Log Insight アプライアンス | サードパーティのログ マネージャ                    | 9543 | CFAPI   | 暗号化 (SSL/TLS) を使用して転送者の送信先として構成された送信 Log Insight 取り込み API (CFAPI) トラフィック |

## ブロックすることができるポート

次のポートは開いてますが vRealize Log Insight では使用されません。これらのポートはファイアウォールによって安全にブロックすることができます。

| ターゲット                                    | ポート  | プロトコル   | サービスの説明                                    |
|--|------|---------|--|
| vRealize Log Insight アプライアンス             | 111  | TCP、UDP | RPC プログラム番号をユニバーサル アドレスに変換する RPCbind サービス。 |
| vRealize Log Insight アプライアンス Tomcat サービス | 9007 | TCP     | Tomcat サービス                                |

## vRealize Log Insight 構成ファイル

一部の構成ファイルには vRealize Log Insight のセキュリティに影響する設定が含まれています。

**注:** セキュリティ関連のすべてのリソースは、ルート アカウントからアクセスできます。このアカウントを保護することは、vRealize Log Insight のセキュリティにとって不可欠です。

表 12-1. Log Insight の構成ファイル

| ファイル  | 説明  |
|---|---|
| /usr/lib/loginsight/application/etc/loginsight-config-base.xml                  | vRealize Log Insight のデフォルトのシステム構成ファイル。           |
| /storage/core/loginsight/config/loginsight-config.xml# <i>number</i>            | (デフォルトから) 変更された vRealize Log Insight のシステム構成ファイル。 |
| /usr/lib/loginsight/application/etc/jaas.conf                                   | Active Directory との統合のための構成。                      |
| /usr/lib/loginsight/application/etc/3rd_config/server.xml                       | Apache Tomcat サーバ用のシステム構成。                        |
| /storage/var/loginsight/apache-tomcat/conf/tomcat-users.xml                     | Apache Tomcat サーバ用のシステム構成。                        |
| /usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/server.xml       | Apache Tomcat サーバ用のシステム構成。                        |
| /usr/lib/loginsight/application/3rd_party/apache-tomcat-*/conf/tomcat-users.xml | Apache Tomcat サーバ用のユーザー情報。                        |

## vRealize Log Insight のパブリック キー、証明書、およびキーストア

vRealize Log Insight のパブリック キー、証明書、およびキーストアは vRealize Log Insight 仮想アプライアンスに格納されています。

**注:** セキュリティ関連のすべてのリソースは、ルート アカウントからアクセスできます。このアカウントを保護することは、vRealize Log Insight のセキュリティにとって不可欠です。

- /usr/lib/loginsight/application/etc/public.cert
- /usr/lib/loginsight/application/etc/loginsight.pub
- /usr/lib/loginsight/application/etc/3rd\_config/keystore
- /usr/lib/loginsight/application/etc/truststore
- /usr/lib/loginsight/application/3rd\_party/apache-tomcat-\*/conf/keystore

## vRealize Log Insight のライセンスおよび EULA ファイル

エンド ユーザー使用許諾契約 (EULA) およびライセンス ファイルは vRealize Log Insight 仮想アプライアンスに格納されています。

**注:** セキュリティ関連のすべてのリソースは、ルート アカウントからアクセスできます。このアカウントを保護することは、vRealize Log Insight のセキュリティにとって不可欠です。

| ファイル  | 場所   |
|-------|--|
| ライセンス | /usr/lib/loginsight/application/etc/license/loginsight_dev.dlf |
| ライセンス | /usr/lib/loginsight/application/etc/license/loginsight_cpu.dlf |

| ファイル          | 場所   |
|---------------|--|
| ライセンス         | /usr/lib/loginsight/application/etc/license/loginsight_osi.dlf     |
| ライセンス キー ファイル | /usr/lib/loginsight/application/etc/license/loginsight_license.bak |
| エンドユーザー使用許諾契約 | /usr/lib/loginsight/application/etc/license/release/eula.txt       |

## vRealize Log Insight ログ ファイル

システム メッセージが含まれているファイルは vRealize Log Insight 仮想アプライアンスに格納されています。

次の表は、各ファイルとその目的を示します。

これらのファイルのログ ローテーションまたはログ アーカイブに関する情報については、『vRealize Log Insight エージェントの操作』の「[vRealize Log Insight エージェントによってサポートされるログのローテーション スキーム](#)」および『vRealize Log Insight の管理』の「[vRealize Log Insight でのデータ アーカイブの有効化または無効化](#)」を参照してください。

| ファイル   | 説明  |
|--|---|
| /storage/var/loginsight/alert.log                      | トリガーされたユーザー定義アラートに関する情報を追跡するために使用されます。  |
| /storage/var/loginsight/apache-tomcat/logs/*.log       | Apache Tomcat サーバのイベントを追跡するために使用されます。   |
| /storage/var/loginsight/cassandra.log                  | Apache Cassandra のクラスタ構成のストレージおよびレプリケーションを追跡するために使用されます。                                  |
| /storage/var/loginsight/plugins/vsphere/li-vsphere.log | vSphere Web Client との統合に関連したイベントを追跡するために使用されます。   |
| /storage/var/loginsight/loginsight_daemon_stdout.log   | vRealize Log Insight デモンの標準出力に使用されます。   |
| /storage/var/loginsight/phonehome.log                  | VMware に送信されるトレース データの収集が有効な場合に、この収集に関する情報を追跡するために使用されます。                                 |
| /storage/var/loginsight/pi.log                         | データベースの開始イベントまたは終了イベントを追跡するために使用されます。   |
| /storage/var/loginsight/runtime.log                    | vRealize Log Insight に関連するすべてのランタイム情報を追跡するために使用されます。                                      |
| /var/log/firstboot/stratavm.log                        | vRealize Log Insight 仮想アプライアンスの初回起動時および初回構成時に発生するイベントを追跡するために使用されます。                      |
| /storage/var/loginsight/systemalert.log                | vRealize Log Insight から送信されたシステム通知に関する情報を追跡するために使用されます。各アラートは JSON エントリとして表示されます。         |
| /storage/var/loginsight/systemalert_worker.log         | vRealize Log Insight ワーカー ノードから送信されたシステム通知に関する情報を追跡するために使用されます。各アラートは JSON エントリとして表示されます。 |
| /storage/var/loginsight/ui.log                         | vRealize Log Insight ユーザー インターフェイスに関連するイベントを追跡するために使用されます。                                |
| /storage/var/loginsight/ui_runtime.log                 | vRealize Log Insight ユーザー インターフェイスに関連するランタイム イベントを追跡するために使用されます。                          |
| /storage/var/loginsight/upgrade.log                    | vRealize Log Insight のアップグレード中に発生するイベントを追跡するために使用されます。                                    |
| /storage/var/loginsight/usage.log                      | すべてのクエリを追跡するために使用されます。  |

| ファイル   | 説明  |
|--|---|
| /storage/var/loginsight/vcenter_operations.log | vRealize Operations Manager の統合に関連するイベントを追跡するために使用されます。                                       |
| /storage/var/loginsight/watchdog_log*          | vRealize Log Insight が何らかの理由でシャットダウンしている場合に再起動を行うウォッチドッグ プロセスについて、そのランタイム イベントを追跡するために使用されます。 |
| /storage/var/loginsight/api_audit.log          | Log Insight への API 呼び出しを追跡するために使用されます。  |
| /storage/var/loginsight/pattern_matcher.log    | パターン マッチングの回数と、フィールド抽出のタイムアウトを追跡するために使用されます。  |

## セキュリティ関連のログ メッセージ

ui\_runtime.log ファイルには、ユーザー 監査ログ メッセージが次の形式で格納されています。

- [2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136 DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login success: vIDM: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]
- [2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out: vIDM: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]
- [2019-05-10 11:28:29.709+0000] ["https-jsse-nio-443-exec-9"/10.153.234.136 DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login success: Active Directory User: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]
- [2019-05-10 11:28:45.812+0000] ["https-jsse-nio-443-exec-3"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out: Active Directory User: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]
- [2019-05-10 11:29:28.330+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136 DEBUG] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login success: Local User: Name=myusername]
- [2019-05-10 11:29:47.078+0000] ["https-jsse-nio-443-exec-10"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User logged out: Local User: Name=myusername]
- [2019-05-10 11:29:23.559+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136 WARN] [com.vmware.loginsight.web.actions.misc.LoginActionBean] [User login failure: Bad username/password attempt (username: incorrectUser)]
- [2019-05-10 11:45:37.795+0000] ["https-jsse-nio-443-exec-7"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: Local User: Name=myusername]

- [2019-05-10 11:09:50.493+0000] ["https-jsse-nio-443-exec-6"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new user: VIDM: SAM=myusername, Domain=vmware.com, UPN=myusername@vmware.com]
- [2019-05-10 11:47:05.202+0000] ["https-jsse-nio-443-exec-10"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Created new group: (directoryType= VIDM, domain=vmware.com, group=vidm\_admin)]
- [2019-05-10 11:58:11.902+0000] ["https-jsse-nio-443-exec-4"/10.153.234.136 INFO] [com.vmware.loginsight.web.actions.settings.UsersActionBean] [Removed groups: [class com.vmware.loginsight.database.dao.RBACADGroupDO<vidm/vmware.com/vidm\_admin>]]

#### 注:

- 一部のログは、デバッグレベルで使用できます。各ノードでデバッグレベルを有効にする方法については、「[ユーザー監査ログメッセージのデバッグレベルの有効化](#)」を参照してください。
- vRealize Log Insight クラスタの各ノードには、独自の ui\_runtime.log ファイルが含まれています。ノードのログファイルを確認して、クラスタを監視できます。

## ユーザー監査ログメッセージのデバッグレベルの有効化

ユーザー監査ログメッセージのデバッグレベルを有効にして、ui\_runtime.log ファイルにログメッセージを含めることができます。

#### 前提条件

vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。

#### 手順

- 1 /usr/lib/loginsight/application/etc/ に移動し、テキストエディタで構成ファイル loginsight-config-base.xml を開きます。
- 2 名前が UI\_RUNTIME\_FILE のアペンドの場合、Threshold パラメータ値を DEBUG に更新します。

```
<appenders>
  <appender name="UI_RUNTIME_FILE"
    class="com.vmware.loginsight.log4j.SafeRollingFileAppender">
    <param name="Threshold" value="DEBUG"/>
  </appender>
</appenders>
```

- 3 DEBUG ログインレベルの LoginActionBean の新しいロガーを追加します。

```
<loggers>
  <logger name="com.vmware.loginsight.web.actions.misc.LoginActionBean" level="DEBUG"
    appender="UI_RUNTIME_FILE" additivity="false"/>
</loggers>
```

- 4 `loginsight-config-base.xml` ファイルを保存して閉じます。
- 5 `service loginsight restart` コマンドを実行して、変更を適用します。

## vRealize Log Insight ユーザー アカウント

vRealize Log Insight を管理するシステムおよびルート アカウントを設定する必要があります。

### vRealize Log Insight root ユーザー

vRealize Log Insight は現在 root ユーザー アカウントをサービス ユーザーとして使用しています。それ以外のユーザーは作成されません。

展開中に root パスワードのプロパティを設定しない限り、デフォルトの root パスワードは空です。vRealize Log Insight コンソールに初めてログインする場合は、root パスワードを変更する必要があります。

デフォルトの root パスワードが設定されるまで、SSH は無効です。

root パスワードは次の要件を満たす必要があります。

- 8 文字以上
- 大文字、小文字、数字、および特殊文字がそれぞれ 1 文字以上含まれている
- 同じ文字が 4 回繰り返されない

### vRealize Log Insight 管理者ユーザー

vRealize Log Insight 仮想アプライアンスを初めて起動すると、vRealize Log Insight によって Web ユーザー インターフェイスの管理者ユーザー アカウントが作成されます。

管理者のデフォルト パスワードは空です。vRealize Log Insight の初期構成中に Web ユーザー インターフェイスで管理者パスワードを変更する必要があります。

## Active Directory のサポート

vRealize Log Insight は Active Directory との統合をサポートしています。構成済みの vRealize Log Insight は、Active Directory に対してユーザーを認証または許可することができます。

[「Active Directory を介したユーザー認証の有効化」](#) を参照してください。

### デフォルト ユーザーに割り当てられた権限

vRealize Log Insight サービス ユーザーには root 権限が割り当てられています。

Web ユーザー インターフェイス管理者ユーザーには、vRealize Log Insight Web ユーザー インターフェイス限定の管理者権限が割り当てられています。

## vRealize Log Insight ファイアウォールに関する推奨事項

vRealize Log Insight で収集された機密情報を保護するには、内部ネットワークの残りの部分からファイアウォールによって保護されている管理ネットワーク セグメント上にサーバを配置します。



## 必要なポート

vRealize Log Insight にデータ送信元のソースから送られるネットワーク トラフィックに対して、次のポートを開く必要があります。

| ポート               | プロトコル  |
|-------------------|--|
| 514/UDP、514/TCP   | Syslog   |
| 1514/UDP、6514/TCP | Syslog-TLS (SSL)                               |
| 9000/TCP          | vRealize Log Insight Ingestion API             |
| 9543/TCP          | vRealize Log Insight Ingestion API - TLS (SSL) |

vRealize Log Insight UI を使用するために必要なネットワーク トラフィックに対して、次のポートを開く必要があります。

| ポート     | プロトコル |
|---------|-------|
| 80/TCP  | HTTP  |
| 443/TCP | HTTPS |

ワーカー ノードからネットワークにアクセスする場合は、セキュリティを最大にするために、vRealize Log Insight マスター ノードの次の一連のポートのみを開くようにしてください。

| ポート             | プロトコル      |
|-----------------|------------|
| 16520:16580/TCP | Thrift RPC |
| 59778/TCP       | log4j サーバ  |
| 12543/TCP       | データベース サーバ |

## セキュリティ アップデートおよびパッチ

vRealize Log Insight 仮想アプライアンスは SUSE Linux Enterprise Server 11 (x86\_64) バージョン 11、パッチ レベル 3 をゲスト OS として使用します。

VMware では、セキュリティの問題に対処するためのパッチをリリースします。

ゲスト OS にアップグレードまたはパッチを適用する前に、依存関係を考慮してください。[6 章 ポートおよび外部インターフェイス](#)を参照してください。

# バックアップ、リストア、およびディザスタ リカバリ

# 13

コストのかかるデータセンターのダウンタイムに対する保護のため、次に示すベスト プラクティスに従って、vRealize Log Insight のバックアップ、リストア、ディザスタ リカバリ操作を実行します。

この章には、次のトピックが含まれています。

- [バックアップ、リストア、およびディザスタ リカバリの概要](#)
- [固定 IP アドレスおよび FQDN の使用](#)
- [計画および準備](#)
- [ノードおよびクラスタのバックアップ](#)
- [Linux または Windows エージェントのバックアップ](#)
- [ノードおよびクラスタのリストア](#)
- [リストア後の構成の変更](#)
- [リストアの確認](#)
- [ディザスタ リカバリ](#)

## バックアップ、リストア、およびディザスタ リカバリの概要

VMware は、高可用性、データ保護、ディザスタ リカバリを実現するビジネス継続性およびディザスタ リカバリ (BCDR) ソリューションの包括的な統合ポートフォリオを提供しています。

マスター ノード、ワーカー ノードおよびフォワーダを含む vRealize Log Insight コンポーネントについては、このドキュメントのバックアップ、リストアおよびディザスタ リカバリ情報を使用してください。

- 構成、ログ データおよびカスタマイズを含むマスターおよびワーカーのクラスタ メンバーについては、[ノードおよびクラスタのバックアップ](#) を参照してください。
- Linux または Windows エージェントのローカル構成については、[Linux または Windows エージェントのバックアップ](#) を参照してください。

このドキュメントの情報は、以下のツールおよび製品には適用されません。これらのツールおよび製品に関する情報は、複数のリソースから取得する必要があります。

- バックアップ、リストア、およびディザスタ リカバリ専用のサードパーティ ツール。詳細については、ベンダーのドキュメントを参照してください。

- vSphere Data Protection、Site Recovery Manager、および Symantec NetBackup。VMware BCDR ソリューションの詳細については、<https://www.vmware.com/solutions/business-continuity-disaster-recovery-draas.html> を参照してください。
- vRealize Log Insight に統合される製品のバックアップ、リストアおよびディザスタ リカバリ機能。
  - vRealize Operations Manager
  - vSphere Web Client サーバ
  - ESXi ホスト

## 固定 IP アドレスおよび FQDN の使用

固定 IP アドレスおよび FQDN を使用して、バックアップ、リストア、およびディザスタ リカバリ操作中のリスクを回避することができます。

### vRealize Log Insight クラスタ ノードおよびロード バランサーの固定 IP アドレス

vRealize Log Insight クラスタ内のすべてのノードで固定 IP アドレスを使用している場合は、これらの IP アドレスが変更されたときに、クラスタ ノードの IP アドレスを更新する必要がありません。

vRealize Log Insight には、[VMware のナレッジベースの記事 KB2123058](#) で説明するように、各クラスタ ノード構成ファイルのすべてのノードの IP アドレスが含まれています。

vRealize Log Insight (ESXi、vSphere、vRealize Operations) と統合されたすべての製品は、syslog ターゲットとしてクラスタ マスター ノードの完全修飾ドメイン名 (FQDN) または IP アドレスを使用します。これらの製品は構成に応じて、ロード バランサの FQDN または IP アドレスを syslog ターゲットとして使用する可能性があります。固定 IP アドレスにより、複数のロケーションで syslog ターゲットの IP アドレスを継続的に更新することによるリスクを低減できます。

ロード バランサの静的 IP アドレスとオプションの仮想 IP アドレスを指定します。統合ロード バランサを構成する場合は、仮想 IP アドレスのオプションの FQDN を指定します。FQDN は、何らかの理由で IP アドレスにアクセスできない場合に使用されます。

### vRealize Log Insight クラスタ ノードおよびワーカー ノードの FQDN

vRealize Log Insight クラスタ ノード内のすべてのノードに FQDN を使用している場合、リカバリ サイトで同じ FQDN を解決できるときは、リストア後およびリカバリ時の構成変更の時間を短縮できます。

マスター ノード（使用されている場合はロード バランサ）の場合は、完全に解決可能な FQDN が必要です。そうでないと、ESXi ホストは、vRealize Log Insight またはすべてのリモート ターゲットに対する syslog メッセージの収集に失敗します。

システム通知については、vRealize Log Insight は、FQDN が使用可能な場合には IP アドレスの代わりに FQDN のホスト名を使用します。

基礎となる IP アドレスのみがバックアップ後の操作およびリストアやディザスタ リカバリ操作を変更すると、合理的に想定することができます。FQDN を使用すると、ログを vRealize Log Insight クラスタに提供するすべての外部デバイス上の syslog ターゲット アドレス（マスター ノード FQDN または内部ロード バランサ FQDN）を変更する必要がなくなります。

vRealize Log Insight のワーカー ノードからの参加要求で vRealize Log Insight のマスター ノードの FQDN が使用されることを確認します。

各ノードの構成ファイル内のマスター ノードのホスト値は、参加要求を送信する最初のワーカー ノードが使用する値に基づいています。参加要求にマスター ノードの FQDN を使用すると、ディザスタ リカバリ後のマスター ノードホスト値を手動で変更することができなくなります。このようにしないと、すべてのリストア済みクラスタ ノードの構成ファイルでマスター ノードのホスト名が更新されるまで、ワーカー ノードはマスター ノードに再参加できなくなります。

## 計画および準備

バックアップ、リストア、ディザスタ リカバリの手順を実行する前に、このトピックの計画と準備についての情報を確認してください。

バックアップ、リストア、およびディザスタ リカバリ プランに次の推奨事項を含める必要があります。

### バックアップのテスト操作

バックアップ、リストア、およびディザスタ リカバリ操作を稼働中の本番環境で実行する前に、テスト環境またはステージング環境でこれらの操作のテストを行います。

vRealize Log Insight クラスタ全体のフル バックアップを実行します。個々のファイルおよび構成をバックアップする場合は、自動手順を利用しないでください。

### 修正の確認

バックアップ、リストア、およびディザスタ リカバリ操作を実行する前に、修正が実装され、警告やエラーが対処済みであることを確認します。通常、バックアップ、リストア、およびディザスタ リカバリのツールには、これらの構成が正常に作成されたことを確認するための視覚的な検証手段とその手順が提供されています。

### バックアップのスケジュール設定

クラスタ構成によっては、初回のバックアップ操作がフル バックアップになることがあります。最初のバックアップが完了するまで期間を長めに確保するようにしてください。それ以降のバックアップは、増分バックアップまたはフル バックアップになります。2 回目以降のバックアップは、最初のバックアップ操作よりも比較的早く終了します。

### その他のドキュメントおよびツール

vRealize Log Insight のバックアップ、リストア、およびディザスタ リカバリ ツールのリソースを割り当てる場合は、次のドキュメントに従っていることを確認します。

サードパーティのバックアップ、リストア、およびディザスタ リカバリ ツールを使用する場合は、ツール固有のベストプラクティスおよび推奨事項に従っていることを確認します。

VMware 製品を使用して展開された仮想マシンでバックアップ リストア、およびディザスタ リカバリをサポートするには、専用の機能および構成を提供できる追加ツールを使用します。

## フォワーダおよびクラスタ

フォワーダには、メイン vRealize Log Insight クラスタのバックアップ リストア、およびディザスタ リカバリ手順を適用します。[ノードおよびクラスタのリストア](#)を参照してください。

顧客の要件に基づいて、1 つまたは複数の vRealize Log Insight フォワーダを配置する必要があります。また、フォワーダは、スタンドアロン ノードとしてまたはクラスタとしてインストールされることがあります。バックアップ、リストア、およびディザスタ リカバリ操作では、vRealize Log Insight フォワーダはプライマリ vRealize Log Insight クラスタ ノードに等しく、同じ方法で処理されます。

## ノードおよびクラスタのバックアップ

最善の方法は、vRealize Log Insight のノードおよびクラスタに対するスケジュールされたバックアップまたはレプリケーションを設定することです。

### 前提条件

- バックアップまたはレプリケーション操作を行う前に、ソースおよびターゲット サイトに構成上の問題が発生していないことを確認します。
- クラスタのリソース割り当てが容量いっぱいになっていないことを確認します。

取り込みとクエリ負荷がそれほど高くない構成では、バックアップおよびレプリケーションの操作中にメモリとスワップの使用量が容量のほぼ 100% に達することがあります。ライブ環境内でメモリがほぼ容量いっぱいになるため、vRealize Log Insight クラスタの使用がメモリ使用量急増の一因になっています。また、スケジュール設定されたバックアップおよびレプリケーション操作がメモリ使用量急増の大きな要因となることがあります。

場合によっては、メモリ使用率が高いために、マスター ノードが再参加する前にワーカー ノードが 1 ～ 3 分間、一時的に切断されることがあります。

- 次のいずれか、または両方を実行して、vRealize Log Insight ノードのメモリ スロットルを小さくします。
  - vRealize Log Insight の推奨構成以上になるように、追加メモリを割り当てます。
  - 繰り返し実行されるバックアップを、ピーク時以外の時間にスケジュールします。

### 手順

- 1 vRealize Log Insight サーバで使用するのと同じ手順に従って、vRealize Log Insight フォワーダの定期的なバックアップまたはレプリケーションを有効にします。
- 2 バックアップ頻度とバックアップのタイプが、使用可能なリソースと顧客固有の要件に基づいて適切に選択されていることを確認します。
- 3 リソースが問題となっていない場合、およびツールでサポートされている場合は、クラスタ ノードの同時バックアップを有効にして、バックアップ プロセスを高速化します。
- 4 すべてのノードを同時にバックアップします。

## 次のステップ

監視：バックアップの進行中に、vRealize Log Insight セットアップで、環境またはパフォーマンス上の問題が発生していないかを確認します。ほとんどのバックアップ、リストア、およびディザスタ リカバリ ツールで監視機能が提供されています。

ユーザー インターフェイスには表示されていない問題がある可能性があるため、バックアップ プロセス中に、本番システムの関連するログをすべて確認します。

## Linux または Windows エージェントのバックアップ

サーバ側のインストールおよび構成情報をバックアップすることでエージェントをバックアップします。エージェント ノードの個別のバックアップは必要ありません。

エージェントは通常、他のアプリケーションまたはサービスにも使用される Linux または Windows システム上にインストールされ、既存のバックアップ手順に含まれている場合があります。エージェント インストールとその構成全体を含むマシンの完全なファイルレベルまたはブロックレベルのバックアップを作成すれば、リカバリには十分です。エージェントは、ローカルの構成とサーバが提供する構成の両方をサポートします。

エージェントが完全に vRealize Log Insight サーバから構成され、`liagent.ini` 構成ファイルをローカルで変更しない場合は、エージェント インストールのバックアップを作成する必要はありません。代わりに、エージェントのフレッシュ インストールを実行して、サーバのバックアップを取得します。

エージェントにカスタムのローカル構成がある場合は、`liagent.ini` ファイルをバックアップし、エージェントのフレッシュ インストールと共にリストアします。エージェント ソフトウェアのインストール以上にエージェント ノードを使用していて、これらのノードでフル バックアップが必要な場合は、他の仮想マシンと同じバックアップ手順に従います。

エージェントの構成がクライアント側（エージェント上）で行われ、エージェント ノードが vRealize Log Insight エージェント ソフトウェアをインストールするためだけに使用される場合は、エージェント構成ファイルのバックアップを作成するだけで十分です。

### 前提条件

vRealize Log Insight サーバ側にエージェントの構成があることを確認します。

### 手順

- 1 `liagent.ini` ファイルをバックアップします。
- 2 リカバリされたエージェントまたは Linux や Windows マシン上のファイルを、バックアップ ファイルで置き換えます。

## ノードおよびクラスタのリストア

ノードは特定の順序でリストアする必要があります。リストアのシナリオによっては、手動による構成変更が必要になる場合があります。

リストアに使用するツールによっては、仮想マシンを同じホスト、同じデータ センター上の異なるホスト、またはターゲット リモート データセンター上の異なるホストにリストアできます。[リストア後の構成の変更](#)を参照してください。

#### 前提条件

- リストアされたノードがパワーオフ状態であることを確認します。
- クラスタを新しいサイトにリストアする前に、クラスタ インスタンスがパワーオフ状態であることを確認します。
- リカバリ サイトで同じ IP アドレスおよび FQDN を使用する場合には、スプリットブレインの動作がないことを確認します。
- プライマリ サイト上で部分的に機能しているクラスタを誤って使用しているユーザーがいないことを確認します。

#### 手順

- 1 ワーカー ノードをリストアする前に、マスター ノードをリストアします。
- 2 ワーカー ノードを任意の順番でリストアします。
- 3 (オプション) フォワーダが構成されている場合は、リストアします。

フォワーダをリストアする前に、vRealize Log Insight サーバ (クラスタ セットアップ内のマスター ノードおよびすべてのワーカー ノード) がリストアされていることを確認します。

- 4 リカバリされたすべてのエージェントをリストアします。

#### 次のステップ

- vRealize Log Insight クラスタをリストアするときに、同じ IP アドレスが使用される場合は、リストアされるすべてのノードの IP アドレスと FQDN が、対応する元の情報と関連していることを確認します。  
  
たとえば、次のシナリオの場合は失敗します。3 ノードのクラスタにノード A、B、C が含まれている場合、ノード A は IP アドレス B、ノード B は IP アドレス C、ノード C は IP アドレス A を使用してリストアされます。
  - リストアされるノードの一部のみで同じ IP アドレスが使用される場合は、これらのノードで、リストアされたすべてのイメージが元の IP アドレスに関連付けられていることを確認します。
- ほとんどのバックアップ リストア ツールおよびディザスタ リカバリ ツールには、リストア操作の進行状況を監視して障害または警告を検出するための監視ビューが用意されています。特定されたすべての問題に適切に対応します。
- サイトを完全にリストアするために、手動による構成変更が必要な場合には、[リストア後の構成の変更](#)のガイドラインに従います。
- リストアが正常に完了したら、リストアされたクラスタのスポット チェックを行います。

## リストア後の構成の変更

必要となる手動での構成変更は、バックアップ構成中に適用されたリカバリ ターゲットおよび IP カスタマイズによってきます。リストアされたサイトが完全に機能できるようになるには、1 つ以上の vRealize Log Insight ノードに構成変更を適用する必要があります。

### 同じホストへのリストア

vRealize Log Insight クラスタを同じホストにリカバリする方法は単純で、どのツールでも実行できます。

#### 前提条件

[計画および準備](#)に関する重要な情報を確認します。

#### 手順

- 1 リストア操作を開始する前に、既存のクラスタをパワーオフします。デフォルトでは、リストア後のクラスタ ノードに同じ IP アドレスおよび FQDN が使用されます。
- 2 (オプション) クラスタに新しい名前を指定します。  
リストア プロセスの際に、仮想マシンに新しい名前を付けない限り、クラスタの元のコピーはリストアされたバージョンで上書きされます。
- 3 (オプション) 可能な場合は、本番環境で使用するすべてのネットワーク、IP、および FQDN の設定が、リストアおよびリカバリされたサイトで保持されることを確認します。

#### 次のステップ

リストアが成功しサニティ チェックに合格したら、リソース節約のためと、ユーザーが誤って以前のコピーをパワーオンしてスプリットブレインの状態になることを防ぐために、以前のコピーを削除します。

### 別ホストへのリストア

異なるホストへのリストアを実行する場合、vRealize Log Insight クラスタの構成を変更する必要があります。

vRealize Log Insight 3.0 以降のリリースでは、アプライアンス コンソールからの構成ファイルの直接変更は正式にはサポートされません。Web ユーザー インターフェイスを使用してこれらの変更を行う方法については、[VMware のナレッジベースの記事 KB2123058](#) を参照してください。

これらの構成変更は、任意のバックアップ リカバリ ツールで利用できる vRealize Log Insight ビルドに固有です。

別ホストにリカバリを行う場合は、vRealize Log Insight クラスタで手動による構成変更が必要になります。リストアされた vRealize Log Insight ノードはバックアップ元の対応するノードとは異なる IP アドレスと FQDN を持つと仮定できます。

#### 前提条件

[計画および準備](#)に関する重要な情報を確認します。

#### 手順

- 1 各 vRealize Log Insight ノードに割り当てられていた、新しい IP アドレスと FQDN を一覧表示します。



## 2 VMware のナレッジベースの記事 KB2123058 で説明されている手順を実行して、マスター ノード上で次の構成変更を行います。

- a vRealize Log Insight の構成セクションで、次のような行を検索します。

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

コードに 3 つのノードが示されています。最初のノードはマスター ノードで、`<service-group name=standalone>` が示されています。残りの 2 台のノードはワーカー ノードで、`<service-group name="workernode">` が示されています。

- b マスター ノードの場合は、新たにリカバリされた環境で、リカバリ前の環境で使用されていた DNS エントリを再利用できることを確認します。
- DNS エントリを再利用できる場合は、マスター ノードの新しい IP アドレスをポイントするように DNS エントリのみを更新します。
  - DNS エントリを再利用できない場合は、マスター ノードのエントリを新しい DNS 名（新しい IP アドレスをポイントしている）に置き換えます。
  - DNS 名を割り当てられない場合は、最後のオプションとして、構成エントリを新しい IP アドレスで更新します。
- c ワーカー ノードの IP アドレスも、新しい IP アドレスを反映するように更新します。

- d 同じ構成ファイル内で、NTP、SMTP、データベース、およびアペンダのセクションを表すエントリを探します。

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>
```

- 構成済みの NTP サーバの値が新しい環境で有効でなくなった場合は、これらの値を `<ntp>...</ntp>` セクションで更新します。
  - 構成済みの SMTP サーバの値が新しい環境で有効でなくなった場合は、これらの値を `<smtp>...</smtp>` セクションで更新します。
  - オプションで、SMTP セクションの `default-sender` の値を変更します。これには任意の値を指定できますが、Eメールの送信元にするをお勧めします。
  - `<database>...</database>` セクションで、マスター ノードの FQDN または IP アドレスをポイントするように、ホストの値を変更します。
- e 同じ構成ファイルで、vRealize Log Insight ILB の構成セクションを更新します。

```
<load-balancer>
<leadership-lease-renewal-secs value="5" />
<high-availability-enabled value="true" />
<high-availability-ip value="10.158.128.165" />
<high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
<layer4-enabled value="true" />
<ui-balancing-enabled value="true" />
</load-balancer>
```

- f `<load-balancer>...</load-balancer>` セクションで、`high-availability-ip` の値が現在の設定と異なる場合は、この値を更新します。
- g ロード バランサの FQDN も更新してください。

- h [管理] ページの [クラスタ] タブを使用して Web ユーザー インターフェイスから再起動します。リストされた各ノードに対して、ホスト名または IP アドレスを選択して詳細パネルを開き、[Log Insight の再起動] をクリックします。

構成変更がすべてのクラスタ ノードに自動的に適用されます。

- i Cassandra サービスを開始するために必要な時間が確保されるよう、vRealize Log Insight サービスが開始した後に 2 分間待機してから、他のワーカー ノードをオンラインにします。

#### 次のステップ

リストア後の vRealize Log Insight ノードに、バックアップの取得元とは異なる IP アドレスと FQDN が割り当てられていることを確認します。


## リストアの確認

リストア済みの vRealize Log Insight クラスタがすべて完全に機能することを確認する必要があります。

#### 前提条件

ノードおよびクラスタの構成を確認する前に、バックアップおよびリストア プロセスが完了していることを確認します。

#### 手順

- 1 内部ロード バランサー (ILB) の IP アドレスまたは FQDN（構成されている場合）を使用して、vRealize Log Insight にログインします。
- 2 構成ドロップダウン メニュー アイコン  をクリックし、[管理] を選択します。
- 3 以下を確認します。
  - a それぞれの IP アドレスまたは FQDN を使用してすべてのクラスタ ノードに個別にアクセスできることを確認します。
  - b クラスタのページからクラスタ ノードのステータスを確認し、ILB（構成されている場合）もアクティブな状態になっていることを確認します。
  - c vSphere 統合を確認します。必要に応じて統合を再構成します。マスター ノードの IP アドレスまたは FQDN がリカバリ後に変更された場合は、再構成が必要です。
  - d vRealize Operations Manager の統合を確認し、必要に応じて再構成します。
  - e すべてのコンテンツ バックと UI 機能が適切に機能していることを確認します。
  - f vRealize Log Insight フォワーダおよびエージェントが構成されている場合は、適切に機能していることを確認します。
- 4 vRealize Log Insight のその他の主要な機能も期待される通りに機能していることを確認します。

#### 次のステップ

バックアップおよびリカバリ プランに必要な調整を行って、バックアップ、リストア、および検証操作中に特定された可能性のあるすべての問題を解決します。

## ディザスタ リカバリ

クラスタを短時間で動作状態に戻すには、適切に文書化およびテストされたリカバリ プランが不可欠です。

ディザスタ リカバリに対応するように仮想マシンを構成する場合は、レプリケーション タイプの選択が重要です。レプリケーション タイプを決定する場合は、目標復旧時点 (RPO)、目標復旧時間 (RTO)、およびコストとスケーラビリティを考慮してください。

ディザスタ リカバリのシナリオでは、プライマリ サイトが完全に停止している場合に、同じサイトにリストアできないことがあります。ただし、選択したオプションに基づいて vRealize Log Insight クラスタを完全にリストアして動作状態に戻すには、いくつかの手順を手動で行う必要があります。

vRealize Log Insight クラスタが完全にダウンし、アクセスできない状態にならない限り、クラスタを新しいサイトにリストアする前に、クラスタ インスタンスがパワーオフされていることを確認します。

停止または災害が発生した場合は、vRealize Log Insight クラスタをできるだけ早くリカバリしてください。

# vRealize Log Insight のトラブルシューティング

# 14

VMware サポート サービスに問い合わせる前に、vRealize Log Insight の管理に関連する一般的な問題を解決することができます。

この章には、次のトピックが含まれています。

- [Internet Explorer で vRealize Log Insight にログインできない](#)
- [vRealize Log Insight のディスク領域不足](#)
- [アーカイブされたデータのインポートに失敗することがある](#)
- [vRealize Log Insight のサポート バンドルを作成するための仮想アプライアンス コンソールの使用](#)
- [管理者ユーザーのパスワードのリセット](#)
- [root ユーザーのパスワードのリセット](#)
- [vRealize Operations Manager にアラートを配信できない場合](#)
- [Active Directory の認証情報を使用してログインできない](#)
- [STARTTLS オプションが有効な場合 SMTP が機能しない](#)
- [.pak ファイルの署名を検証できなかったためのアップグレードの失敗](#)
- [内部サーバ エラーによるアップグレードの失敗](#)

## Internet Explorer で vRealize Log Insight にログインできない

Internet Explorer で vRealize Log Insight の認証に失敗します。

### 問題

vRealize Log Insight Web クライアントには LocalStorage または DOM ストレージのサポートが必要ですが、現在のファイルシステムの整合性レベルでは Internet Explorer で LocalStorage を使用することはできません。コンソールとデバッガにエラー「SCRIPT5: Access is Denied」が表示されます。

### 原因

vRealize Log Insight は、LocalStorage または DOM Storage サポートにアクセスできません。Internet Explorer は、このストレージデータを CachePath パラメータで設定されたフォルダ（%USERPROFILE%\AppData\LocalLow\Microsoft\Internet Explorer\DOMstore）に保存します。このフォルダの整合性レベルが「低」以外の場合、Internet Explorer は LocalStorage を使用できません。

## 解決方法

次のコマンドを使用して、ユーザー アカウントの整合性レベルを設定できます。

```
icaccls %userprofile%\Appdata\LocalLow /t /setintegritylevel (OI)(CI)L
```

## vRealize Log Insight のディスク領域不足

サイズの小さな仮想ディスクを使用していて、アーカイブが無効になっている場合は、vRealize Log Insight マスター ノードまたはワーカー ノードのディスク領域が不足することがあります。

### 問題

1 分間に受信されるログのサイズがストレージ領域の 3% を超えると、vRealize Log Insight のディスク領域が不足します。

### 原因

通常の状況では、空き領域が 3% 未満であるかどうか 1 分おきにチェックされるため、vRealize Log Insight のディスク領域が不足することはありません。vRealize Log Insight 仮想アプライアンスの空き領域が 3% 未満に低下すると、古いデータ バケットが廃棄されます。

ただし、ディスク サイズが小さく、ログ取り込み速度が高いため、1 分以内に空き領域 (3%) がいっぱいになった場合、vRealize Log Insight はディスク領域不足になります。

アーカイブが有効であれば、vRealize Log Insight はバケットが廃棄される前にアーカイブします。古いバケットがアーカイブされて廃棄される前に空き領域がいっぱいになると、vRealize Log Insight はディスク領域不足になります。

### 解決方法

- ◆ vRealize Log Insight 仮想アプライアンスのストレージ容量を大きくします。 [vRealize Log Insight 仮想アプライアンスのストレージ容量を増やす](#) を参照してください。

## アーカイブされたデータのインポートに失敗することがある

vRealize Log Insight 仮想アプライアンスのディスク容量が不足していると、アーカイブされたデータのインポートに失敗することがある。

### 問題

vRealize Log Insight リポジトリ インポート ユーティリティは、vRealize Log Insight 仮想アプライアンスの使用可能なディスク容量をチェックしません。したがって、仮想アプライアンスのディスク容量が不足しているとアーカイブされたログのインポートは失敗することがあります。

### 解決方法

vRealize Log Insight 仮想アプライアンスのディスク容量を増やし、インポートを再度開始してください。 [vRealize Log Insight 仮想アプライアンスのストレージ容量を増やす](#) を参照してください。ただし、失敗する前に正常にインポートされた情報は重複することに注意してください。

## vRealize Log Insight のサポート バンドルを作成するための仮想アプライアンス コンソールの使用

vRealize Log Insight Web ユーザー インターフェイスにアクセスできない場合は、仮想アプライアンスのコンソールを使用することにより、または vRealize Log Insight 仮想アプライアンスとの SSH 接続を確立した後にサポート バンドルをダウンロードすることができます。

### 前提条件

- vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。
- SSH を使用して vRealize Log Insight 仮想アプライアンスに接続する場合は、TCP ポート 22 が開いていることを確認します。

### 手順

- 1 vRealize Log InsightvApp との SSH 接続を確立し、root ユーザーとしてログインします。
- 2 サポート バンドルを生成するには、`loginsight-support` を実行します。

サポート バンドルを生成して、特定の期間内に変更されたファイルのみを含めるには、`--days` 制約を指定して `loginsight-support` コマンドを実行します。たとえば、`--days=1` を実行すると、1 日以内に変更されたファイルのみが含まれます。

サポート情報が収集されて、\*.tar.gz ファイルに保存されます。このファイルには `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz` という命名規則があり、xxxxx は `loginsight-support` プロセスを実行したときに使用されたプロセス ID です。

### 次のステップ

必要に応じて VMware サポート サービスにサポート バンドルを転送します。

## 管理者ユーザーのパスワードのリセット

管理者ユーザーが Web ユーザー インターフェイスのパスワードを忘れると、アカウントにアクセスできなくなります。

### 前提条件

- vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。
- SSH 接続を有効にするには、TCP ポート 22 が開いていることを確認します。

### 問題

vRealize Log Insight の管理者ユーザーが 1 名の場合に、その管理者ユーザーがパスワードを忘れると、アプリケーションを管理できなくなります。管理者ユーザーが vRealize Log Insight の唯一のユーザーである場合は、Web ユーザー インターフェイス全体にアクセスできなくなります。

## 原因

管理者ユーザーが現在のパスワードを忘れた場合、vRealize Log Insight には、管理者ユーザーが自分のパスワードをリセットするためのユーザー インターフェイスがありません

**注:** ログイン可能な管理者ユーザーは、他の管理者ユーザーのパスワードをリセットできます。すべての管理者ユーザーのアカウントのパスワードが不明な場合に限り、管理者ユーザーのパスワードをリセットしてください。

## 解決方法

- 1 vRealize Log Insight 仮想アプライアンスとの SSH 接続を確立し、root ユーザーとしてログインします。
- 2 「li-reset-admin-passwd.sh」と入力して、[Enter] を押します。

スクリプトによって管理者ユーザーのパスワードがリセットされ、新しいパスワードが生成されて、画面に表示されます。

## 次のステップ

新しいパスワードを使用して vRealize Log Insight Web ユーザー インターフェイスにログインし、管理者ユーザーのパスワードを変更します。

# root ユーザーのパスワードのリセット

root ユーザーのパスワードを忘れると、SSH 接続を確立したり、vRealize Log Insight 仮想アプライアンスのコンソールを使用したりできなくなります。

次のような理由によって、root としてログインできない場合があります。

- デフォルトのパスワードを変更していない。デフォルトの場合、vRealize Log Insight は root ユーザーに対して空のパスワードをセットし、SSH アクセスは無効です。パスワードが設定されると、root ユーザーの SSH アクセスが有効になります。
- SSH キーを vRealize Log Insight 仮想アプライアンスのデプロイ中に設定した。SSH キーを OVF で指定した場合、パスワード認証は無効になります。設定した SSH キーでログインするか、下記の解決のための手順を参照してください。
- 間違ったパスワードを複数回入力したために、一時的にロックアウトされている。この場合、正しいパスワードを入力しても、ロックアウトの期間が過ぎるまではアクセスできません。ロックアウトが解除されるまで待機するか、仮想アプライアンスを再起動します。

## 問題

SSH 接続を確立したり、vRealize Log Insight 仮想アプライアンスのコンソールを使用したりできない場合は、管理タスクの一部を実行できなくなり、管理者ユーザーのパスワードもリセットできなくなります。

## 解決方法

- 1 vSphere Client で vRealize Log Insight 仮想アプライアンスのゲスト シャットダウンを実行します。
- 2 仮想マシンをパワーオフしたら、[設定の編集] を選択します。
- 3 [オプション] タブを選択します。



4 [vApp オプション] - [詳細] から、[プロパティ] を選択します。

5 `vm.rootpw` キーを見つけて編集します。

`vm.rootpw` キーが見つからない場合は新しいキーを追加します。

パスワード認証の代わりに SSH キーを使用している場合は、`vm.sshkey` キーを編集するか追加します。

6 パスワードを入力してください。

パスワード認証を使用していない場合は、代わりにここで SSH キーを追加することができます。

7 仮想アプライアンスをパワーオンします。

#### 次のステップ

vRealize Log Insight が起動したら root ユーザーとしてログインできることを確認します。

## vRealize Operations Manager にアラートを配信できない場合

vRealize Operations Manager にアラート イベントを送信できない場合は、vRealize Log Insight によって通知されます。問題が解決されるまで、vRealize Log Insight は 1 分ごとにアラートを送信しようとします。

#### 問題

vRealize Operations Manager にアラートを配信できなかった場合は、vRealize Log Insight ツールバーに感嘆符を含む赤い記号が表示されます。

#### 原因

接続に問題があると、vRealize Operations ManagervRealize Log Insight は vRealize Operations Manager にアラート通知を送信できません。

#### 解決方法

- ◆ 赤いアイコンをクリックしてエラー メッセージのリストを開き、下にスクロールして最新メッセージを表示します。

エラー メッセージのリストを開くか、問題が解決されると、ツールバーに赤い記号が表示されなくなります。

- ◆ vRealize Operations Manager の接続問題を解決するには、次の手順を試してください。
  - vRealize Operations Manager vApp is がシャットダウンしていないことを確認します。
  - vRealize Log Insight Web ユーザー インターフェイスの [管理] ページの [vRealize Operations Manager] セクションにある [接続をテスト] ボタンを押して、vRealize Operations Manager に接続できることを確認します。
  - vRealize Operations Manager に直接ログインして、使用している認証情報が正しいことを確認します。
  - vRealize Log Insight および vRealize Operations Manager ログ内に、接続問題に関連するメッセージがあるか確認します。
  - vRealize Operations Manager vSphere ユーザー インターフェイスでアラートが除外されていないことを確認します。

## Active Directory の認証情報を使用してログインできない

Active Directory の認証情報を使用している場合は、vRealize Log Insight Web ユーザー インターフェイスにログインできません。

### 問題

管理者がユーザーの Active Directory アカウントを vRealize Log Insight に追加した場合でも、Active Directory ドメイン ユーザーの認証情報を使用して vRealize Log Insight にログインすることはできません。

### 原因

最も一般的な原因は、パスワードの期限切れ、認証情報の間違い、接続問題、または vRealize Log Insight 仮想アプライアンスと Active Directory クロック間の非同期です。

### 解決方法

- お使いの認証情報が有効であること、パスワードの期限が切れていないこと、およびお使いの Active Directory アカウントがロックされていないことを確認してください。
- Active Directory 認証に使用するドメインを指定しなかった場合、[number] が最も大きい `/storage/core/loginsight/config/loginsight-config.xml#[number]` に、最新の vRealize Log Insight 構成でデフォルト ドメインのアカウントが格納されていることを確認してください。
- 最新の構成ファイル（[number] が最大の `/storage/core/loginsight/config/loginsight-config.xml#[number]`）を見つけます。
- また、vRealize Log Insight が Active Directory サーバに接続していることを確認します。
  - vRealize Log Insight Web ユーザー インターフェイスの [管理] ページの [認証] セクションに移動してユーザー認証情報を入力し、[接続をテスト] ボタンをクリックします。
  - vRealize Log Insight の `/storage/var/loginsight/runtime.log` 内に DNS 問題に関連したメッセージがないか確認します。
- vRealize Log Insight および Active Directory のクロックが同期していることを確認します。
  - vRealize Log Insight の `/storage/var/loginsight/runtime.log` 内にクロック スキューに関連したメッセージがないか確認します。
  - NTP サーバを使用して vRealize Log Insight と Active Directory のクロックを同期します。

## STARTTLS オプションが有効な場合 SMTP が機能しない

SMTP サーバを構成するときに STARTTLS オプションを有効にすると、テスト電子メールの送信に失敗します。この問題を解決するには、Java トラストストアに SMTP サーバの SSL 証明書を追加します。

### 前提条件

- vRealize Log Insight 仮想アプライアンスにログインするための root ユーザー認証情報があることを確認してください。

- SSH を使用して vRealize Log Insight 仮想アプライアンスに接続する場合は、TCP ポート 22 が開いていることを確認します。

#### 手順

- 1 vRealize Log Insight vApp との SSH 接続を確立し、root ユーザーとしてログインします。
- 2 SMTP サーバの SSL 証明書を vRealize Log Insight vApp にコピーします。
- 3 次のコマンドを実行します。

```
`/usr/java/latest/bin/keytool -import -alias certificate_name -file path_to_certificate -
keystore /usr/java/latest/lib/security/cacerts`
```

**注:** キーボードのチルダと同じキーにあるバッククオート記号を使用して、外側引用符が挿入されます。単一引用符は使用しないでください。

- 4 デフォルト パスワードの **changeit** を入力します。
- 5 `service loginsight restart` コマンドを実行します。

#### 次のステップ

[管理] - [Smtpt] に移動して、[テスト電子メールの送信] を使用して設定をテストします。を参照してください。

[vRealize Log Insight の SMTP サーバの構成](#)

## .pak ファイルの署名を検証できなかったためのアップグレードの失敗

vRealize Log Insight のアップグレードが、.pak ファイルの破損、ライセンスの期限切れ、またはディスク領域の不足のために失敗します。

#### 問題

vRealize Log Insight のアップグレードが失敗し、次のエラー メッセージが表示されます。アップグレードに失敗しました。アップグレードに失敗しました: PAK ファイルの署名が検証できません。

#### 原因

このエラーは次の原因で発生する場合があります。

- アップロードされたファイルが .pak ファイルではない。
- アップロードされた .pak ファイルが完全ではない。
- vRealize Log Insight のライセンスが期限切れになっている。
- vRealize Log Insight 仮想アプライアンスの root ファイル システムに十分なディスク領域がない。

#### 解決方法

- ◆ .pak ファイルをアップロードしていることを確認します。
- ◆ VMware ダウンロード サイトに対して .pak ファイルの md5sum を確認します。

- ◆ vRealize Log Insight 上で少なくとも 1 つの有効なライセンスが構成されていることを確認します。
- ◆ vRealize Log Insight 仮想アプライアンスにログインし、`df -h` を実行して使用可能なディスク領域を確認します。

---

**注:** vRealize Log Insight 仮想アプライアンスの root ファイル システム上にはファイルを置かないでください。

---

## 内部サーバ エラーによるアップグレードの失敗

接続の問題を原因とする内部システム エラーによって、vRealize Log Insight のアップグレードが失敗します。

### 問題

vRealize Log Insight のアップグレードが失敗すると、エラー メッセージ アップグレードが失敗しました。内部サーバ エラーが表示されます。

### 原因

クライアントとサーバ間で接続の問題が発生しています。たとえば、WAN 上にあるクライアントからアップグレードする場合があります。

### 解決方法

- ◆ サーバと同じ LAN 上にあるクライアントから LI をアップグレードします。