

vRealize Log Insight 8.1.1 リリース ノート

リリース ノートの概要

このリリース ノートには、次のトピックが含まれています。

- [vRealize Log Insight について](#)
- [新機能](#)
- [互換性](#)
- [制限事項](#)
- [以前のリリースからのアップグレード](#)
- [国際化のサポート](#)
- [解決した問題](#)
- [既知の問題](#)

vRealize Log Insight について

vRealize Log Insight は、VMware 環境に最適リアルタイムのアーカイブ ログ管理を提供します。機械学習ベースのインテリジェントなグループ化と高性能な検索により、物理環境、仮想環境、クラウド環境にわたり高速なトラブルシューティングが可能になります。vRealize Log Insight ではテラバイト単位でのログの分析、構造化されていないデータの構造検出、最新の Web インターフェイスを使用したエンタープライズ規模の視覚化が可能になります。

詳細については、<https://docs.vmware.com/jp/vRealize-Log-Insight/index.html> の vRealize Log Insight 製品ドキュメントを参照してください。

新機能

vRealize Log Insight 8.1.1 は、セキュリティの問題が修正されたメンテナンス リリースです。また、このリリースでは、コミュニティでサポートされているコンテンツ パックのメリットを活かすこともできます。これらのコンテンツ パックは VMware Sample Exchange からダウンロードし、vRealize Log Insight にインポートできます。

互換性

vRealize Log Insight 8.1.1 は、以下の VMware 製品およびバージョンをサポートしています。

- vRealize Log Insight は VMware vCenter Server バージョン 6.0 以降からイベント、タスク、アラームのデータを取得できます。
- vRealize Log Insight 8.1.1 は、vRealize Operations Manager バージョン 8.0.1 以降と統合できます。

ブラウザのサポート

vRealize Log Insight 8.1.1 では、以下のブラウザのバージョンがサポートされます。これより新しいバージョンのブラウザも vRealize Log Insight で使用できますが、まだ検証されていません。

- Mozilla Firefox 72.0 以降
- Google Chrome 78.0 以降
- Safari 11.1 以降
- Internet Explorer 11.0 以降

注: Internet Explorer のドキュメント モードは **標準モード** で使用する必要があります。その他のモードはサポートされません。互換表示ブラウザ モードはサポートされていません。

サポート対象のブラウザの最低解像度は、1280 X 800 ピクセルです。

重要: ブラウザでは Cookie を有効にする必要があります。

vRealize Log Insight Windows エージェントのサポート

vRealize Log Insight 8.1.1 Windows エージェントは、以下のバージョンをサポートします。

- Windows 7、Windows 8、Windows 8.1、Windows 10
- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019

vRealize Log Insight Linux エージェントのサポート

vRealize Log Insight Linux エージェントは、以下のディストリビューションとバージョンをサポートします。

- RHEL 5、RHEL 6、RHEL 7、および RHEL 8
- SUSE Enterprise Linux (SLES 11 SP3) および SLES 12 SP1
- Ubuntu 14.04 LTS、Ubuntu 16.04 LTS、および Ubuntu 18.04
- VMware Photon、バージョン 1 リビジョン 2、バージョン 2、およびバージョン 3

制限事項

vRealize Log Insight 8.1.1 には以下の制限事項があります。

全般

- vRealize Log Insight では、印字不可能な ASCII 文字は正常に処理されません。
- vRealize Log Insight は印刷をサポートしていません。ただし、ブラウザの印刷オプションは使用できます。印刷結果は使用しているブラウザによって異なることがあります。vRealize Log Insight ユーザー インターフェイスの印刷部分には Internet Explorer または Firefox の使用をお勧めします。
- ホスト テーブルでは、デバイスが、IP アドレス、ホスト名、FQDN の組み合わせなどによる、異なるフォーマットごとに重複して表示されることがあります。たとえば、foo.bar.com という名前のデバイスが foo と foo.bar.com のように表示されることがあります。
ホスト テーブルでは、Syslog RFC で定義された `hostname` フィールドが使用されます。デバイスによって Syslog プロトコル経由で送信されたイベントにホスト名がない場合、vRealize Log Insight はソースをホスト名として使用します。vRealize Log Insight は 2 つの形式が同じデバイスを指していることを判別できないため、デバイスが 2 つ以上リスト表示されることになります。
- 新しいデータ パーティションを追加したり、既存のデータ パーティションを削除したりした後、新しい構成を有効にするには、クラスタを再起動する（クラスタ ノードを 1 つずつ再起動する）必要があります。ただし、既存のデータ パーティションのルーティング フィルタ、有効化ステータス、および保持期間の変更はただちに適用されます（クラスタの再起動は必要ありません）。

vRealize Log Insight Windows および Linux エージェント

- vRealize Log Insight の Windows エージェントおよび Linux エージェントが Syslog モードで実行されていると、`hostname` フィールドと `source` フィールドの ASCII 以外の文字が正常に送信されません。

vRealize Log Insight Windows エージェント

- vRealize Log Insight Windows エージェントは 32 ビットのアプリケーションで、`C:\Windows\System32` サブディレクトリからファイルを開く要求はすべて WOW64 によって `C:\Windows\SysWOW64` にリダイレクトされます。ただし、特別なエイリアス `C:\Windows\Sysnative` を使用して vRealize Log Insight Windows エージェントが `C:\Windows\System32` から収集するように構成できます。たとえば、MS DHCP サーバのデフォルトの場所からログを収集するには、vRealize Log Insight Windows エージェントの構成ファイルの対応する場所に以下の行を追加します：`=C:\Windows\Sysnative\dhcp`。

vRealize Log Insight Linux エージェント

- オペレーティングシステムの制限事項のため、イベントを Syslog 経由で送信するように構成していると、vRealize Log Insight Linux エージェントがネットワークの停止を検出しません。
- vRealize Log Insight Linux エージェントは、フィールドまたはタグ名に含まれた英語以外 (UTF-8) の記号をサポートしません。
- vRealize Log Insight Linux エージェントは、デフォルトで隠しファイルおよび隠しディレクトリを収集します。これを回避するには、`exclude=.*` オプションを各構成セクションに追加する必要があります。オプション `exclude` では、隠しファイルの形式を表すのに glob パターン `.*` を使用します。
- ファイルへの標準出力リダイレクトを使用してログを生成すると、vRealize Log Insight エージェントはそのログ ファイル内のイベントの境界を認識できないことがあります。

vRealize Log Insight の統合

仮想マシンの IP アドレスが vRealize Operations インスタンスから認識されず、vCenter Server によって仮想マシンの **[仮想マシンのサマリ]** タブに表示されない場合は、仮想マシンに対する vRealize Log Insight と vRealize Operations のどちらの場合もコンテキストでの起動は動作しません。vmware-tools ユーティリティがないため IP アドレスを使用できない可能性があります。vmware-tools のバージョンが古い、またはサポートされていない場合、あるいは誤動作している場合も、IP アドレスが使用できないことがあります。

適切なバージョンの VMware Tools が仮想マシンにインストールされ、vCenter Server の **仮想マシンのサマリ** タブに仮想マシンの IP アドレスが表示されていることを確認します。

vRealize Log Insight の旧バージョンからのアップグレード

このバージョンの vRealize Log Insight にアップグレードする場合は次の点に注意してください。

アップグレード パス

8.1、8.0、または 4.8 から vRealize Log Insight 8.1.1 にアップグレードできます。

アップグレードに関する重要事項

- vRealize Log Insight 8.1.1 にアップグレードするには、現在 vRealize Log Insight 8.1、8.0 または 4.8 を実行している必要があります。
- 手動でアップグレードする際には、ワーカーを一度に 1 つずつアップグレードする必要があります。複数のワーカーを同時にアップグレードすると、アップグレード失敗の原因になります。マスター ノードを vRealize Log Insight 8.1.1 にアップグレードすると、無効を指定しない場合を除き、ローリング アップグレードが発生します。

- 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。
- vRealize Log Insight は 2 ノードのクラスタをサポートしていません。アップグレードを実行する前に、既存の 2 つのノードと同じバージョンの 3 つ目の vRealize Log Insight ノードを追加します。
- vRealize Log Insight アップグレード (.pak ファイル) に新しいバージョンの JRE が含まれている場合、アップグレードの実行後、ユーザーがインストールした証明書が vRealize Log Insight の設定 (イベントの転送など) に表示されなくなります。
- 統合ターゲットが SSL 接続に対して信頼されていない証明書を提供する場合、証明書がトラストストアに追加されないため、vRealize Log Insight との統合はアップグレード後に正しく機能しません。これらの統合ターゲットには、vSphere、vRealize Operations Manager、イベント フォワーダ、Active Directory、および SMTP が含まれます。回避策として、それぞれの統合構成ページで、接続をテストし、証明書の詳細がダイアログ ボックスに表示された場合は、信頼されていない SSL 証明書を受け入れます。証明書を受け入れると、トラストストアに追加されます。
- Photon OS のセキュリティ ポリシーが強化されており、Photon OS へのアップグレードが正常に完了した後に root パスワードの変更を要求される場合があります。これは、SLES の root パスワードが期限切れになっている場合にのみ発生しますが、Photon OS とは異なり、SLES OS はアップデートを強制しませんでした。
- SLES ベースの vRealize Log Insight 4.8 を最新の Photon ベースの vRealize Log Insight にアップグレードすると、カスタマイズされた sshd サービス構成 (/etc/ssh/sshd_config) がデフォルト値にリセットされます。回避策として、アップグレードの前に /etc/ssh/sshd_config 構成を保存しておき、アップグレード後に手動で再構成します。
- Photon OS には、同時 SSH 接続数に対する厳密なルールがあります。/etc/ssh/sshd_config ファイルで MaxAuthTries 値がデフォルトで 2 に設定されているため、複数の接続が存在すると、vRealize Log Insight 仮想アプライアンスへの SSH 接続が失敗し、次のメッセージが表示されることがあります。「xx.xx.xx.xxx ポート 22:2 からの切断を受信しました。認証の失敗が多すぎます」。この問題については、次のいずれかの回避策を使用できます。
 - SSH を介して接続する場合は、IdentitiesOnly=yes オプションを使用します。#ssh -o IdentitiesOnly=yes user@ip
 - ~/.ssh/config ファイルを更新して以下を追加します。Host* IdentitiesOnly yes
 - /etc/ssh/sshd_config ファイルを変更し、sshd サービスを再起動して、MaxAuthTries の値を変更します。
- vRealize Log Insight 4.8 クラスタから 8.1.1 へのアップグレードを開始する前に、各ノードのルートパーティションに十分な空き容量があることを確認します。詳細については、<https://kb.vmware.com/s/article/76282> を参照してください。
- vRealize Log Insight 4.8 から 8.1.1 へのアップグレード後、アプライアンスはデフォルトで Photon OS ではなく SLES 起動オプションになります。回避策としては、<https://kb.vmware.com/s/article/79592> の手順に従ってください。

国際化のサポート

vRealize Log Insight 8.1.1 には以下のローカライズ機能があります。

- vRealize Log Insight サーバの Web ユーザー インターフェイスは、日本語、フランス語、スペイン語、ドイツ語、簡体字中国語、繁体字中国語、韓国語にローカライズされています。
- 機械学習機能も含め、vRealize Log Insight サーバの Web ユーザー インターフェイスでは Unicode データがサポートされています。
- vRealize Log Insight エージェントは、英語以外のネイティブの Windows で動作します。

制限事項

- エージェントのインストーラおよびコンテンツ パックはローカライズされていません。vRealize Log Insight サーバの Web ユーザー インターフェイスの一部に、ローカライズされていない文字列が表示され、レイアウトの問題がある可能性があります。
- vRealize Log Insight は、ローカライズ版の vCenter Server および vRealize Operations Manager と相互運用できます。ただし、コンテンツ パックは適合する非ローカライズ版のログ メッセージに依存します。vCenter Server のイベントはデフォルトのロケールで取得されるため、米国英語 (en_US) に設定する必要があります。詳細については、<http://kb.vmware.com/kb/2121646> を参照してください。
- ASCII 文字以外のユーザー名を持つ Active Directory、vSphere および vRealize Operations Manager との統合はサポートされていません。
- イベント ログのローカライズはサポートされていません。イベント ログがサポートするエンコードは、UTF-8 と UTF-16 のみです。
- vRealize Log Insight 8.1.1 の新規デプロイには、英語版のエンド ユーザー使用許諾契約書 (EULA) のみが表示されます。

解決した問題

このリリースで解決されたセキュリティ脆弱性のリストについては、<https://kb.vmware.com/s/article/79258> を参照してください。

既知の問題

このリリースには、次の既知の問題があります。

- **Virtual Center (VC) のイベント収集が遅延する**

vRealize Log Insight サービスまたはクラスタのアップグレードを再開すると、多数の Virtual Center (VC) が統合されている場合に VC イベント収集が遅延することがあります。

回避策： イベントは、十分な時間が経過した後に自動的に復元されます。時間の長さは、使用環境によって異なります。たとえば、4 ノード クラスタ上の 80 個の VC の場合、遅延は 1 時間になります。

- **vRealize Operations の統合の削除に失敗する**

vRealize Log Insight が以前に vRealize Operations インスタンスと統合されていても、その統合に到達できなくなった場合、統合を強制的に削除することはできません。

回避策： 更新を行ってから、統合の削除を再度試みてください。

- **双方向の信頼が構成されている場合、vRealize Log Insight が信頼できる第 2 の Active Directory のユーザーとグループを認証できない**

Active Directory が別の Active Directory と双方向の信頼関係で構成されている場合、vRealize Log Insight が、信頼できる第 2 の Active Directory のユーザーおよびグループを認証できません。

回避策： 両方の Active Directory に直接統合されている vIDM を使用します。

- **一部のディレクトリからの収集は、ディレクトリがエージェントの起動または再構成イベントの前に作成された場合は実行されない**

エージェントの再構成後に新しいディレクトリが作成されている場合は、新たに作成されたディレクトリからの収集は行われません。

回避策： ディレクトリ監視を開始するには、サービスを再起動するか、liagent.ini ファイルを使用して、または [サーバ管理エージェント] ページからエージェント構成を更新します。

- **Photon OS の vRealize Log Insight エージェントには自動アップグレードがない**

Photon OS は gpg コマンドをサポートしていないため、Photon OS の vRealize Log Insight エージェントでは自動アップグレードを実行できません。

回避策： 手動でのアップグレードを実行します。

- **IPv6 を介したパブリック メール サーバの SMTP 構成が機能しないことがある**

Google や Yahoo などのパブリック E メール サービスでは、IPv6 に対してより厳格な制限ポリシーを適用している場合があるため、SMTP 構成はそれらのサービスでは機能しない可能性があります。

回避策： 会社のメール サーバなどの代替メール サーバを使用するか、専用サーバを起動します。

- **VMware Identity Manager を IPv4 を介して vRealize Log Insight と統合すると、リダイレクト URL ホストが IPv6 アドレスに変更される**

vRealize Log Insight 仮想アプライアンスをデプロイするときに IPv6 アドレスを優先するオプションを選択すると、IPv6 をサポートしていない VMware Identity Manager との統合時に、リダイレクト URL ホストのリストが IPv6 ノード アドレスで設定されます。

回避策：vRealize Log Insight と VMware Identity Manager を統合するための予備の IPv4 仮想 IP アドレスを作成します。

- **20,000 件を超えるイベントのエクスポートにデフォルトのタスク名を使用できない**

20,000 件を超えるイベントをエクスポートする場合、表示されるデフォルトのエクスポート タスク名は使用できません。

回避策：英数字でカスタムのエクスポート タスク名を指定します。

- **Internet Explorer 11.0 のレイアウトの問題**

Internet Explorer 11.0 では、[ダッシュボード] および [インタラクティブ分析] タブのヘッダーとグラフの凡例リスト表示で、ユーザー アイコンのレイアウトに問題があります。

回避策：回避策については、<https://kb.vmware.com/s/article/78592> を参照してください。