NAKIVO Backup for VMware の新機能

目次

はじめに

NAKIVO Backup & Replicationは、オールインワンのバックアップ、即時復元、ランサムウェア対策、および災害復旧機能を提供し、データ損失やサイバー脅威の影響から VMware 環境を保護します。

最新の機能と改善点

IT脅威の状況は絶えず変化しており、それに伴いデータ保護のニーズも頻繁に変化しています。　各組織がバックアップおよび災害復旧戦略を適応させられるよう、NAKIVOは、新たなデータ保護機能を導入し、既存の機能を強化するアップデートを継続的にリリースしています。

2023年1月以降、当社はVMware環境における重要データを保護するための、さまざまなバックアップおよびランサムウェア対策ツールを搭載した「NAKIVO Backup & Replication」の新バージョンを8つリリースしてきました。 以下は、バージョン11.2までの最新機能の概要です。

VMware vSphere サポートに関する最新情報

NAKIVOは、VMware　vSphereの最新バージョンへの早期対応を継続し、お客様がアップグレードのたびに保護機能を途切れることなく維持できるよう支援しています。

v11.2では、VMware vSphere 9に対する完全な保護機能を導入しました。これにより、最新バージョンのVMwareを実行している環境において、バックアップおよびリカバリ操作を継続的に実行できるようになります。

ソース側でのバックアップ暗号化

NAKIVO Backup & Replicationを使用すると、バックアップデータをネットワーク経由で保存先へ転送する前に、ソース側で暗号化することができます。

暗号化されたバックアップは、ローカルフォルダやパブリッククラウドプラットフォーム（Amazon　S3、Wasabi、Azure Blob、Backblaze B2）、S3互換のストレージ先、SMB/NFSネットワーク共有、テープ、および重複排除アプライアンスに保存できます。　バックアップデータの復号にはパスワードが必要です。また、この機能では、復号キーを紛失した場合のフェイルセーフ手段として、AWS KMSとの連携もサポートされています。

フェデレーテッドリポジトリ

フェデレーテッド・リポジトリは、大規模なデータセットを扱う大規模環境におけるパフォーマンスのボトルネックや複雑さに対処できる、拡張性が高く柔軟なバックアップリポジトリの一種です。

フェデレーテッド・リポジトリは、「メンバー」と呼ばれる複数の独立したリポジトリで構成される、拡張可能なストレージプールのように機能します。　フェデレーテッドリポジトリは、新しいメンバーを追加してより多くのデータを格納できるようにすることで、迅速かつ簡単に拡張できます。　メンバーの追加や削除には複雑な設定は不要で、わずか数回のクリックで完了します。　フェデレーテッド・リポジトリでは、構成リポジトリのいずれかが障害を起こしたり、容量が不足したりした場合でも、使用可能な別の構成リポジトリが存在する限り、バックアップおよび復旧処理は中断されることなく継続されます。

NetApp ストレージのスナップショットからのバックアップ

NAKIVOは、「ストレージスナップショット用バックアップ」機能でサポートされるストレージデバイスの一覧に、NetApp FASおよびNetApp AFFストレージアレイを追加しました。 通常のVMスナップショットではなく、ストレージスナップショットから直接VMware VMをバックアップすることで、本番環境におけるリソースやパフォーマンスへのVMバックアップ操作の影響を軽減できます。

テナント概要ダッシュボード

当社はMSPコンソールに「テナント概要ダッシュボード」を追加しました。これにより、管理対象のすべてのテナントの概要を一元的に確認できるようになりました。

この動的なダッシュボードからは、ノードの状態、利用可能なリソース、スケジュールされたアクティビティ、インベントリ情報など、お客様のデータ保護インフラに関するリアルタイムの分析情報やアラートを確認できます。 テナント一覧を並べ替えたり、フィルタリングしたり、検索したりして、必要な情報を抽出したり、未解決の問題を特定したり、一括操作を実行したりすることができます。

NEC HYDRAstor上の不変ストレージ

NAKIVO Backup & Replicationは、他の重複排除アプライアンスと同様に、NEC HYDRAstorをバックアップ先ストレージとしてサポートしています。

NEC HYDRAstor ストレージシステム上に保存されているバックアップに対して不変性を有効にすることで、ランサムウェア攻撃や誤削除、その他の望ましくない変更からバックアップを保護できるようになりました。

詳細な通知

詳細な通知はワークフロー追跡機能を強化し、バックアップおよびレプリケーションジョブの実行状況をより可視化します。 ジョブの実行中、NAKIVO Backup & Replicationは、データ転送やログの切り捨てなど、進行中の操作に関する説明を表示します。 作業の進捗状況はリアルタイムで更新されるため、作業の進行状況を随時把握することができます。

ファイルシステムのインデックス作成

ファイルシステムのインデックス作成は、グローバル検索機能の既存の機能を基盤として、VMバックアップ内のすべてのファイルおよびフォルダのインデックスを作成します。 したがって、1つまたは複数のファイルやフォルダを復元するために細粒度復元を実行する際は、「グローバル検索」機能を使用して必要な項目を素早く見つけることができ、その過程で貴重な時間を節約できます。

IT監視におけるアラームとレポート機能

IT監視のためのアラームおよびレポート機能を使用すると、特定の条件が満たされた際に発動するカスタムアラートを作成・設定できます。

アラームにはいくつかの用途があり、その中には、CPU使用率が突然通常レベルを上回る場合など、悪意のある行為を示唆する可能性のある異常な活動を事前に検知することも含まれます。 レポート機能を使用すると、インフラストラクチャ内で監視対象となっている VMware vSphere アイテムに関するさまざまな詳細情報を表示、エクスポート、およびメール送信することができます。

HPE Alletra および HPE Primera ストレージのスナップショットからのバックアップ

NAKIVOは、「ストレージスナップショットからのバックアップ」機能の対応ストレージデバイス一覧に、HPE AlletraおよびHPE Primeraを追加しました。 これらのストレージデバイスに保存されている VMware vSphere 仮想マシンを、通常の仮想マシンスナップショットではなく、ストレージスナップショットを利用することで、より効率的にバックアップすることができます。

VMware向けリアルタイムレプリケーション

VMware向けリアルタイムレプリケーションは、NAKIVO Backup & Replicationの災害復旧機能を強力に補完する機能です。

VMware vSphere仮想マシンのリアルタイムレプリカを作成し、ソース仮想マシンで発生したデータ変更に合わせて継続的に更新されるように設定できます。 ソースVMのデータ変更は、更新間隔（およびリカバリポイント目標）が最短1秒というリアルタイムで処理されるため、重要なマシンやデータの継続的な可用性が確保されます。

VMware向けリアルタイムレプリケーション：vSphere 9.0 対応

NAKIVOは、VMware向けリアルタイムレプリケーションの対象範囲をvSphere 9.0まで拡大しました。これにより、VMware環境のアップグレード時にも、レプリケーションワークフローを中断することなく維持することが可能になります。

バックアップマルウェアスキャン

「バックアップ時のマルウェアスキャン」機能は、NAKIVO Backup & Replicationのランサムウェア対策機能に追加された重要な機能です。 この機能を使用すると、復元を実行する前にバックアップをスキャンしてマルウェアやランサムウェアの有無を確認し、インフラストラクチャへの感染を防ぐことができます。

このソリューションをWindows Defender、ESET NOD32、およびSophosと連携させることで、マルウェアのスキャンを実行し、バックアップを復旧に安全に活用できるようにすることができます。 スキャン中にマルウェアが検出された場合、リカバリジョブを失敗させるか、隔離されたネットワークをリカバリ先として指定するかを選択できます。

テープからの直接復元

「テープからのダイレクトリカバリ」を使用すると、テープメディアに保存されたバックアップから、仮想マシン全体やAmazon EC2インスタンスを、お客様のインフラストラクチャに直接復元することができます。

直接復元の手法により、復旧時間と効率が向上します。 VMware vSphereに加え、サポート対象のプラットフォームには、Microsoft Hyper-V、Nutanix AHV、Amazon EC2が含まれます。また、「Physical-to-Virtual Recovery」による物理ワークロードもサポートされています。

S3互換オブジェクトストレージのサポート

NAKIVO Backup & Replicationのハイブリッドバックアップストレージ機能を拡張する「S3互換オブジェクトストレージのサポート」により、S3 APIを採用したローカルおよびクラウドベースのストレージ先へバックアップを保存できるようになります。

組織のニーズや予算に合わせて、S3互換のさまざまなストレージ先から選択できます。 さらに、S3互換のストレージに保存されたリカバリポイントに対して不変性を有効にすることで、ランサムウェアの感染、誤削除、その他の意図しない変更からデータを保護することができます。

永続的なVMエージェント

NAKIVO Backup & Replicationに「永続的なVMエージェント」機能が追加されたことで、VMware vSphere 仮想マシンに永続的なエージェントを展開し、OS の認証情報を指定することなく、ゲスト側の処理を効率化できるようになりました。

このソリューションは、パーシステントエージェントを使用して、単一のポートを介してターゲットVMと通信するため、OSの認証情報やその他の機密情報の共有を禁止するセキュリティポリシーへの準拠が確保されます。

NAKIVO BACKUP FOR VMWARE：主な機能

NAKIVO Backup & Replicationは、高速なエージェントレスバックアップ、VM の即時復旧およびきめ細かな復旧機能、多層的なランサムウェア対策を提供し、VMware 環境内のデータを確実に保護し、復旧可能な状態に保ちます。 以下は、バックアップ、災害復旧、ランサムウェア対策、セキュリティおよびコンプライアンス、ならびに管理に関する主な機能と性能の概要です。

バックアップ

- 増分バックアップ：VMware独自の変更ブロック追跡（Changed Block Tracking）技術を活用し、各バックアップジョブの実行時に変更されたデータブロックのみを処理することで、高速かつ効率的な増分バックアップを実行します。
- アプリ対応処理：さまざまなアプリ（Microsoft Exchange Server、Active Directory、SQL Serverなど）およびデータベースのバックアップデータが、トランザクションの一貫性を保ち、迅速な復旧に対応できる状態であることを保証します。

- ハイブリッドバックアップストレージ：バックアップデータおよびバックアップコピーを、ローカルフォルダ、NFS/SMBネットワーク共有、パブリッククラウドプラットフォーム（Amazon S3、Wasabi、Azure Blob、Backblaze B2）、S3互換のオブジェクトストレージ、テープ、および重複排除アプライアンスに送信することで、「3-2-1」バックアップ戦略を実践します。
- 即時確認：2つの組み込み方法のいずれかを使用して、VMware vSphere VMのバックアップおよびレプリカの即時検証を自動化し、復旧性を確保します。

ディザスタリカバリ

- VMの即時復旧：VMware vSphereのバックアップから完全なVMを直接起動し、 Flash VM Bootを使用することで、数秒以内に業務を再開できます。
- 即時細粒度復元： 個々のファイルおよびアプリケーションオブジェクトを、すべてのアクセス権限を維持したまま、わずか数回のクリックで元の場所または新しいマシンに復元します。
- 効率的なレプリケーション：レプリカを作成し、ソースVMまたは既存のバックアップから、障害発生時の可用性と業務の継続性を確保します。
- サイト復旧：自動実行シーケンスを作成し、緊急時/計画的なフェイルオーバー、フェイルバック、および災害復旧テストのために、ワンクリックで実行できます。
- クロスプラットフォーム復元：VMware vSphere 仮想マシンをMicrosoft Hyper-V 仮想マシンとして復元したり、その逆を行ったりするには、バックアップをエクスポートし、異なる仮想ディスク形式に変換することで、マルチプラットフォーム管理を効率化します。
- 物理マシンから仮想マシンへの復旧：Windows および Linux の物理マシンを、バックアップからVMware vSphere VMとして瞬時に起動し、ダウンタイムを最小限に抑えた上で、本番環境で使用するためにVMを復元します。

ランサムウェア対策

- 変更不可能なローカルストレージ：ランサムウェア対策済みのローカルリポジトリにバックアップを送信し、ランサムウェアによる暗号化やその他の望ましくない変更を防止します。
- 不変のクラウドストレージ：不変性をS3 Object Lockを通じて有効にし、パブリッククラウドストレージプラットフォーム（Amazon S3、Wasabi、Azure Blob、Backblaze B2）に保存されたバックアップデータをランサムウェア感染から保護します。
- エアギャップ方式のバックアップ：VMware vSphere 仮想マシンのバックアップコピーを、テープなどの取り外し可能なドライブにオフラインで保存することで、ランサムウェア対策の追加の防護層を確保します。

セキュリティとコンプライアンス

- 二要素認証（2FA）：セキュリティの層を追加するため、ワンタイムコードをGoogle Authenticatorで生成し、データ保護活動を確実に守ります。
- ロールベースのアクセス制御：プリセットおよびカスタムロールに、関連する権限やアクセス許可を割り当てて、VMware vSphere VMのバックアップへの不正アクセスを防止します。
- 柔軟な保持機能：VMware vSphere VMのバックアップごとに最大10,000個の復旧ポイントを保存し、毎日、毎週、毎月、毎年、または定期的な間隔でローテーションできます。
- テープへのネイティブバックアップ：VMware vSphere 仮想マシンのバックアップデータを、物理および仮想テープライブラリに直接送信し、安全に長期保存します。

管理

- Webインターフェース：使いやすいWebインターフェースから、便利なダッシュボードやステップバイステップのウィザードを活用して、すべてのバックアップおよび復旧作業を管理できます。
- カレンダーダッシュボード：過去、現在、および将来のすべてのジョブをシンプルなカレンダー形式で表示・管理できます。 VMware vSphere の仮想マシン（VM）のバックアップジョブを簡単にスケジュール設定し、スケジュールが重複するのを防ぎます。
- グローバル検索：必要なファイルやフォルダを検索して素早く見つけ出し、効率的かつ正確な復元を実現します。
- ポリシーベースのデータ保護：カスタムポリシールールを作成し、環境の拡大や変化に合わせて、データ保護ジョブ内のVMを自動的に追加または削除します。
- ジョブの連鎖：バックアップジョブとバックアップコピージョブを連携させてワークフローを自動化し、効率を高め、バックアップ管理にかかる時間を節約します。
- HTTP API 連携：NAKIVO Backup & Replicationを監視、自動化、オーケストレーションソリューションとHTTP APIを介してシームレスに連携させます。
- パフォーマンス向上ツール：データ転送速度を管理し、本番環境のリソース負荷を軽減するにはネットワークアクセラレーション、LANを使用しないデータ転送、ストレージスナップショットからのバックアップ、および帯域幅制御を活用し、バックアップウィンドウを短縮し、中核業務への影響を最小限に抑えます。
- 柔軟な導入： Windows、Linux、NAS、あるいは仮想マシン（VA）やAWS AMIとして、わずか数分でソリューションをインストールできます。
- セルフバックアップ：NAKIVO Backup & Replicationのシステム構成（ジョブ、インベントリ、ログ、設定など）を、同じ統合インターフェースからバックアップおよび復元できます。

nakivo.com | +1 408 440 5605 | 4894 Sparks Blvd., Sparks, NV USA 89436-8202