Tintri VMstore – 独自アーキテクチャがランサムウェアの被害を軽減

担当者 *DCIG*アナリスト ケン・クリッパートン

Tintri

会社名

株式会社データダイレクト・ネットワークス・ジャパン

Tintri 事業部

〒102-0081　東京都千代田区四番町6-2 東急番町ビル8F

https://tintri.co.jp/

業界

データストレージ ソリューション

Tintri VMstore

特徴

- きめ細かなデータ保護
- インテリジェントな統合分析
- VMレベルの管理

メリット

- ランサムウェアによる被害を軽減
- アプリケーションの迅速なサービス復旧

本レポートでは、ランサムウェアによる攻撃からのリカバリに役立つTintri VMstoreストレージプラットフォームに焦点を当てています。

昨今、サプライチェーンの寸断が懸念されており、実際多くのビジネスに影響を与えています。一方で、企業を混乱から守るという意味では、ランサムウェアも、経営レベルにおける最重要課題となっています。

ファイルやフォルダを誤って削除してしまったり、アップグレードがうまくいかなかったり、スクリプトにタイプミスがあったりと、データ損失やデータへのアクセス障害の最も一般的な原因は人為的なミスであると言われてきました。これには、インターネットサービスの中断も含まれます。

しかし、ここ数年は、ランサムウェアの攻撃は増加の一途をたどり、今や企業のデータに対する最大の脅威となっています。

ランサムウェアの被害を受けてしまうことも想定する

すべての企業は、あらゆるサイバー攻撃を阻止するためにあらゆる対策を講じなければなりません。そしてさらに、ランサムウェア攻撃が、サイバーセキュリティの対策を擦り抜けてくることも想定する必要があります。

1,000回の攻撃のうち999回を防ぐことができたとしても、それは失敗です。サイバー犯罪者にとっては、逆の比率になります。999回失敗しても、1回で組織のサイバー防御を突破できたら成功なのです。

> 「組織は、サイバーセキュリティの防御が失敗する可能性に備えなければならない。」

ニュースの見出しやセキュリティ企業の統計が示すように、ランサムウェアによる攻撃は、ほぼすべての企業にとって重大な脅威となっています。従って、企業やITのリーダーは、このようなサイバー攻撃の防御に失敗することを想定し、このような攻撃からリカバリするための計画を準備しておく必要があり、その中で迅速なリカバリと通常業務の再開を成功させるために、データストレージは重要な役割を果たします。

ランサムウェアで生じる最大の被害はダウンタイム

サイバー犯罪者が要求する身代金は、数百万ドルに達することもあります。このような身代金要求は確実にニュースになります。しかし、このような攻撃による最大の被害は、実際にはビジネスの中断につながるアプリケーションのダウンタイムによって発生します。

具体的には、ランサムウェアの攻撃からオペレーションをリカバリする際にかかる平均的な総費用は185万ドル[1]となります。そして、支払額そのものよりも大きい費用は、21日間にも及ぶ事業中断によって生じるビジネスの損失額（中央値）です。[2]

その上、ランサムウェアの被害にあったために、経営層の人材を失ったり、従業員を解雇したり、さらには完全にビジネス活動を閉鎖しまうことも珍しくありません。そのため、ITリーダーの約4分の1が、このような事態から会社を守ることを最優先事項としているのも不思議ではありません。

幸いなことに、VMstore には、ランサムウェアの影響を軽減する多くの技術が組み込まれています。

2021年 ランサムウェアの状況

600%	新型コロナウイルス以降の悪意のあるメールの増加 3
170,404ドル	中堅企業の平均支払額 4
185 万ドル	リカバリのための平均コスト
21日	ランサムウェアの攻撃による平均的な企業のダウンタイム

最大のコスト **ビジネスの中断**

1. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 Referenced 8/12/2021
2. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 Referenced 8/12/2021
3. https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542 Referenced 8/12/2021
4. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 Referenced 8/12/2021

インテリジェントな統合分析でランサムウェアの影響を軽減

VMstoreの特徴は、綿密なストレージ分析にあります。これらの分析は、単に管理や可視化のためだけに作られたものではありません。むしろ、これらの分析は、VMstoreの動作と適応的な自律管理機能に内在するものです。

自律的な管理機能は、もともとあらゆるアプリケーションの安定したパフォーマンスを保証するために使われており、現在では、ランサムウェア攻撃を特定し、その範囲を把握し、迅速かつ的確なリカバリを行うためにも利用されています。

VMstoreには、迅速なアプリケーションのリカバリを実現するための複数の機能が搭載されており、それらが連携して動作します。

これらの機能は以下の通りです。

- インテリジェントな分析による攻撃の特定
- 不可視なスナップショット・ポインタとメタデータ
- 非常に高度なスナップショット
- 柔軟なレプリケーション
- ポリシーに基づいたきめ細かなデータ保護とリカバリ
- プライマリーサイトまたはDRサイトでの超高速リカバリ
- ロールベースのアクセス制御

VMレベルの管理によるアプリケーションの迅速なリカバリ

VMstoreと他のストレージ製品との主な違いは、VMstoreがVMレベルで管理が行えるようにするために独自ファイルシステムを搭載していることです。そのため、「VMstore」という名称になりました。

VMレベルで管理できることの重要性は、経験豊富なストレージ管理者であればすぐにご理解いただけるものです。VMstoreの管理は、LUNの管理よりもはるかにきめ細かく、しかも時間をかけずに行うことができます。そしてTintriは、その管理方法を今ではSQLデータベースにまで拡大し、今後はコンテナにも広げていく予定です。

データ損失やサイバー攻撃からのリカバリでは、このVMレベルの管理によって、アプリケーションごとに迅速なデータの保護・リカバリをすることができます。この最大のメリットは、ITスタッフが他のデータ保護ソリューションよりも格段に早くアプリケーションをリカバリし、サービスを再開できることです。

ロールベースのアクセス制御

VMstoreのロールベースのアクセス制御（RBAC）は、ストレージシステム内で受ける攻撃の範囲を限定することができます。RBACは、ストレージインフラへのアクセス権をすべて与えるのではなく、各個人やビジネスプロセスにおいて、そのタスクを遂行するために必要な権限のみを与えます。

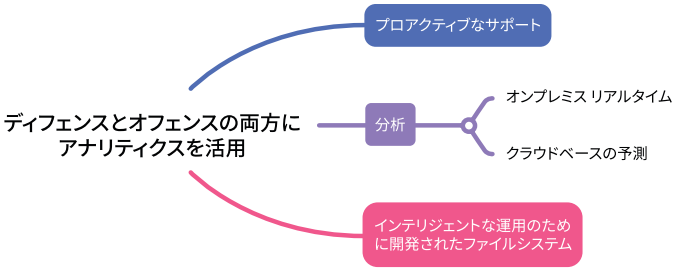
ユーザ毎に割り当て可能なロールは以下の通りです。

- 読み取り専用
- サービスアカウント
- ストレージ管理者
- スーパー管理者
- データベース管理者

これらの役割を適切に割り当てることで、日々の責任を効果的に委ねることができ、各部門の担当者が業務を遂行できるようになります。また、個々の認証情報が漏洩した場合の影響を最小限に抑えることができます。

攻撃の識別

VMstoreは、個々の仮想マシンや SQL Server データベースが使用するパフォーマンスや容量を詳細に可視化します。分析ビューは簡単に設定でき、アプリケーション間でパフォーマンスや容量の「動き」を示すことができます。また、通常のトレンドラインから外れた変化も容易に確認できます。



他のストレージシステムでは、このような詳細なレベルの可視性を提供しているものはほとんどないでしょう。Tintriのインテリジェント・インフラストラクチャへの今後の取り組みとしては、異常を検知した際にアラートを通知する機能を追加する予定です。

独自ファイルシステムの強み

VMstoreがAIOPS機能を実現するために収集するメタデータは、データとは別に保存されます。Tintri独自のファイルシステムにより、VM レベルのスナップショットは、データのポインタ情報が含まれるメタデータのみを取得し、このメタデータはランサムウェアが変更を加えることができないように保存されています。そのため、メタデータやスナップショットもランサムウェアからは見えないようになっています。

ストレージベンダーの中には、ランサムウェアに感染しにくくするための機能を自社のソリューションに追加しているところもあります。VMstoreはそうではありません。この保護機能は、VMstoreアーキテクチャ固有のものです。このようにして、設計当初から搭載されているVMstore独自のファイルシステムでランサムウェアからの攻撃を防御できるのです。

非常に高度なスナップショット技術

多くの企業のストレージシステムでは、データ保護の仕組みとしてスナップショットが使われていますが、VMstore のスナップショットは他の多くのストレージソリューションのものよりも高性能です。

ワークロードに影響を与えない高速なスナップショット：VMstoreは、高速且つワークロードに影響を与えないVMレベルのスナップショットを提供します。これらのスナップショットは、高いレベルのRPOが設定されているバックアップやレプリケーションを容易とし、アプリケーションの迅速なリカバリも可能とします。

オブジェクトレベルのスナップショット：スナップショットは、グループ単位、VMレベル、SQL Server のデータベースごとに作成できます。VMごとのスナップショットでは、各vDiskを個別に操作してクローニングやリストアも行うことができます。

このレベルの粒度でスナップショットを管理できることは、多くの日常的なオペレーションに役立ちます。特に、ランサムウェアの被害を受けた場合には、ターゲットを絞ったデータ復元を提供するのに役立ちます。

ほとんどのLUNベースの環境では、複数のVMやアプリケーションが1つのLUNを共有しています。あるアプリケーションのデータをリストアする必要がある場合、LUN全体をその同じ時点に遡ってリストアする必要があります。これにより、影響を受けたVMのみを復元する場合と比較して、より多くの時間と必要以上の影響を及ぼします。

任意の時点、さらには複数の時点に復元が可能： VMstore は保護対象のオブジェクトごとに100以上のスナップショットをサポートし、SyncVMは複数のスナップショットからのリカバリが可能です。SyncVMを使用することで、ITスタッフは複数のリカバリポイントをテストし、アプリケーションをリカバリする際に使用する最適な時点のスナップショットを決定することができます。

更には、VMstoreの容量効率の高いスナップショットは、ポインタとメタデータベースで構成されています。ランサムウェアの被害を受けた企業は、これらのスナップショットを活用して、業務が正常に戻った後にフォレンジック分析を行うことができます。

大規模環境におけるポリシーベースのデータ保護：多くのTintriの環境では、10万個以上のVM、データベース、またはコンテナの稼働をサポートしています。Tintri Global Center は、スナップショットとレプリケーションのタスクをポリシーに基づいてスケジューリングします。これにより、企業はVMを適切な

ポリシーに関連付けることで、一貫したアプリケーションレベルの保護を適用することができます。また、企業は PowerShell や REST API を使って、データ保護を動的かつ大規模に管理することができます。

コピーデータの管理を効率的に行うことで、アジリティを大幅に向上： 企業は、VMstoreのVMレベルの高速スナップショット技術を活用して、アプリケーション開発を加速することができます。SyncVM は、最小限のデータ移動で本番データを複数の開発サーバに瞬時に移行することができます。

SyncVMは、アプリケーション開発者が開発に必要な完全かつ合理的な最新のデータセットを提供するという、煩雑で時間のかかる困難な作業を解消します。また、VMstoreの自動QoSにより、開発者は他のアプリケーションへのパフォーマンスの影響を受けることなく、高速なストレージ機能を利用することができます。このように VMstore を使用することで、アプリケーションの開発プロセスから複数のオーバーヘッドコストを排除し、開発サイクルと品質を向上させることができます。

ランサムウェアからはアクセス不可：VMstore を支えるOSであるTxOSは、内部的にメタデータ用のストレージスペースを確保しています。このメタデータレポジトリは、アプリケーション、ホスト、およびクライアントからは見えません。つまり、TxOSのポインタとメタデータベースのスナップショットアーキテクチャは、ランサムウェアからは見えないことを意味しています。これは重要なことです。というのも、多くのランサムウェアの攻撃は、データ保護メカニズムを妨害し、攻撃の初期段階でバックアップを暗号化しようとするためです。

柔軟性に富んだレプリケーション

VMstoreは、RPO/RTOを1分間隔で行う非同期レプリケーションをサポートしています。VMstoreは、最大200の主要なVMに対して、1分のRPOで高頻度のスナップショットをサポートしています。標準的な間隔は、通常15分程度の頻度です。その他のレプリケーション機能には、筐体間の同期レプリケーション、1対1、1対多、多対1などがあります。これらのレプリケーションオプションは、主にディザスタリカバリとビジネスコンティニュイティを実現するためのものです。

ランサムウェア対策に最も関連するもう一つのレプリケーションオプションは、VMstoreが複数のパブリッククラウド上のS3ストレージにレプリケートする機能です。Tintriは、AWS、IBM、Wasabiのサポートを受けています。Wasabiのオプションは、Wasabiがパフォーマンスに重点を置いていることと、オブジェクトデータの使用またはエクスポートに関連する料金がないことから興味深いものです。

S3ストレージにレプリケートすることで、スナップショットをプライマリストレージとは別に保護することができます。S3ストレージにレプリケートされたスナップショットは、任意のVMstoreにリストアすることができます。

ポリシーに基づくきめ細かなデータ保護により、瞬時のリカバリを実現

VMstoreは、VMやSQLデータベース、コンテナを管理するためにゼロから設計されているため、ポリシーベースのデータ保護とリカバリを同じレベルの粒度で提供することができます。多くの企業では、ランサムウェア攻撃を受けた後に21日間のダウンタイムを経験すると言われていますが、VMstoreの場合には、数分から数時間で通常のオペレーションを再開することができます。

さらに、Tintriはリカバリを自動化するスクリプトを追加することで、アプリケーションのリカバリをさらに加速させ、その過程でのヒューマンエラーの可能性を減らすことができます。

現在のランサムウェア対策の限界

複合的な認証機能：Tintriは、前述の既存のロールベースのアクセス制御に加えて、多要素認証によるセキュリティのさらなる強化を計画しています。多要素認証（MFA）により、悪意のある者が管理者のユーザー名とパスワードを取得したとしても、VMstoreのインフラにログインすることはできません。これは、ログイン試行を認証するための追加のメカニズムを必要とするもので、多くの場合、物理的なセキュリティキーや認証アプリケーション付きのスマートフォンを必要とします。MFAはセキュリティのベストプラクティスです。

異常検知に基づくアラート機能：Tintriは、インテリジェント・インフラストラクチャの機能を拡張し、異常検知に基づくアラート機能を搭載する予定です。VMstoreは、アプリケーションごとにSLAを監視し、自動的に最適化するAIOPS機能の強固なコアセットを提供します。サイバー攻撃やランサムウェアの感染に関連する異常を検出することは、VMstoreにとってはこれらのAIOPS機能の自然な拡張であり懸念を払拭することができます。

VMstore 、ランサムウェアによる被害の軽減とリカバリに威力を発揮

ランサムウェアの攻撃は、年々洗練され・巧妙化しており、その被害は計り知れません。従って、すべての企業は、次の標的になることを想定し、それに応じた計画を立てる必要があります。これらの計画は、ランサムウェアの感染を防ぎ、影響を受けたアプリケーションを特定し、それらのアプリケーションを可能な限り迅速に通常の運用状態にリカバリすることに重点を置くべきです。

VMstoreは、エンタープライズクラスのデータ保護機能を備えており、VMレベルでの管理を可能にすることで、ランサムウェアの被害を軽減し、アプリケーションを迅速にリカバリします。

Tintriは、ランサムウェアの脅威に直面しても業務を継続という、インテリジェントなアドバンテージをお客様に提供していると言えるでしょう。

Tintriがどのようなメリットをもたらすかについては、Tintriのウェブサイト（www.tintri.co.jp）をご覧いただくか、お近くのTintriのパートナーにお問い合わせください。

DCIG について

ストレージの技術に関する情報に基づき第三者の立場からの分析を提供しています。詳細については、**www.dcig.com** をご覧ください。

DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552 dcig.com