Rubrik 検証報告書

2021年12月3日

ノックス株式会社
営業本部

目次

1．検証概要

2．検証構成

3．検証結果
　3－1．ETERNUS AX/HXシリーズ SnapDiff連携バックアップ検証
　3－2．ランサムウェア対策機能検証

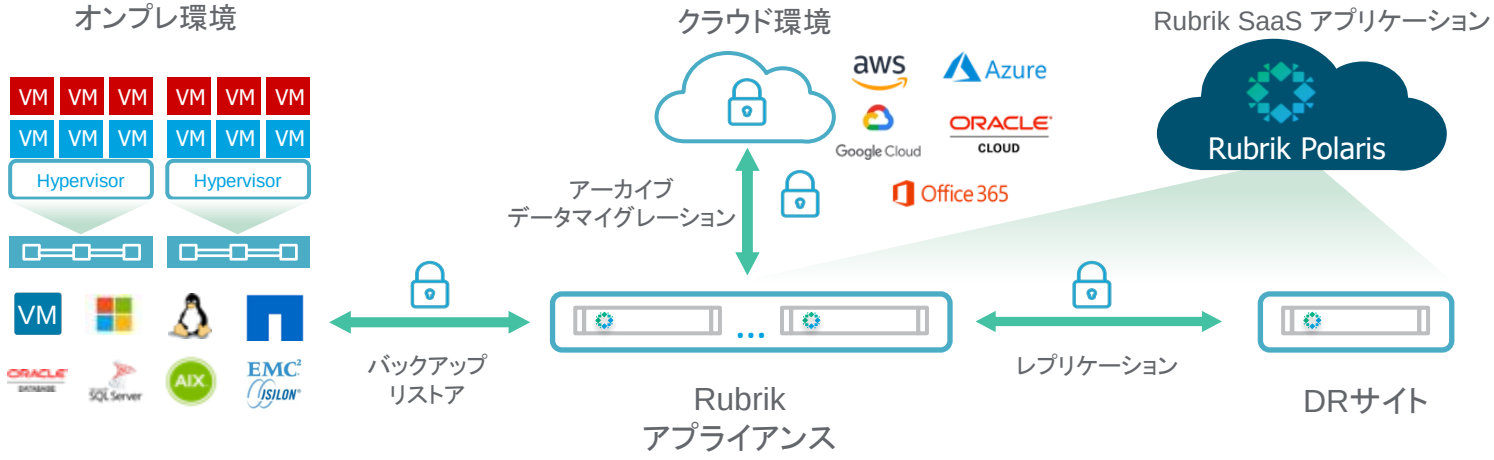
4．検証総括

1．検証概要

Rubrik①ソリューション概要

Rubrikは、これまでの複雑なバックアップ運用を大幅に改善するシンプルな操作性、
自動化運用を実現するデータ保護ソリューションです。

オンプレ環境(仮想・物理・NAS・DB)、クラウド環境(パブリッククラウド・Microsoft365)
のデータ保護に対応しており、ランサムウェアの脅威から確実にデータを守ります。

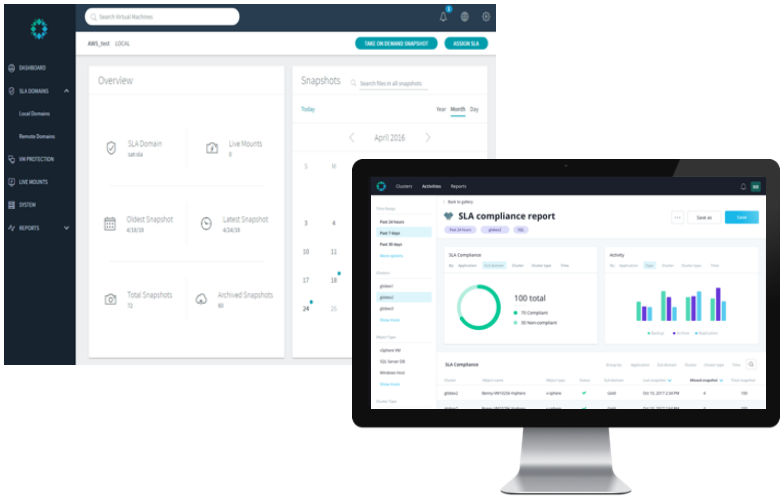


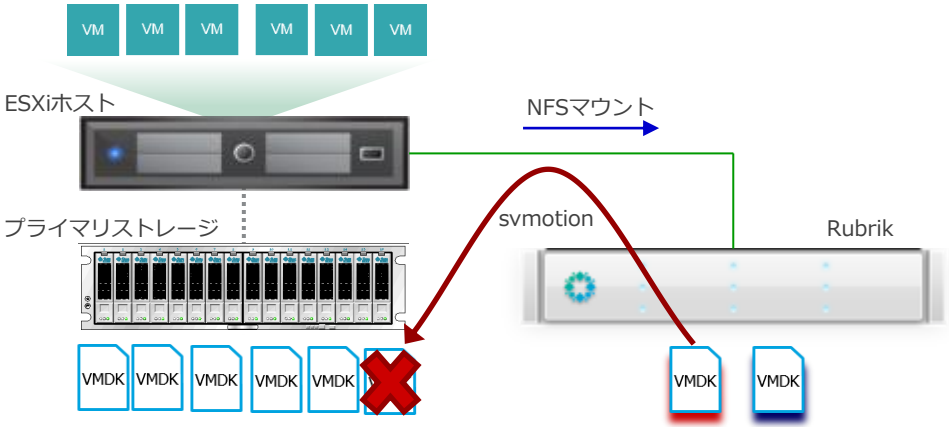
Rubrik②シンプルな操作性、自動化

スマートフォンのようなシンプルな操作性で、直感的にバックアップ・リストアが可能です。

保護対象が頻繁に増加する仮想環境では、ホスト単位・フォルダ単位・タグ単位で、
バックアップポリシー設定が出来るため、自動的に対象を追従したデータ保護を実現します。

一時的にRubrikをデータ領域とし、即時に復旧するインスタントリカバリー機能も
実装しております。



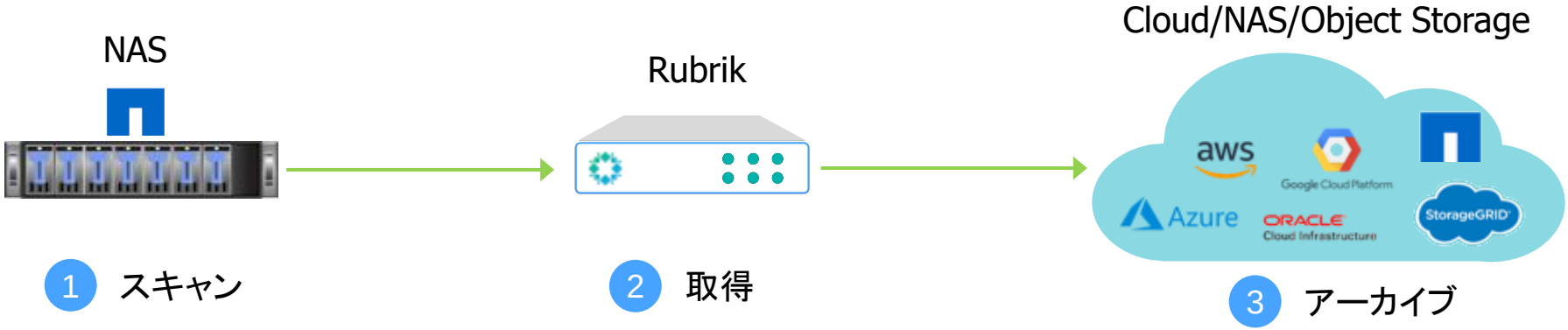


Rubrik③NASのバックアップ

NASデータのバックアップを他アーキテクチャで取得し、別環境に保管しておくことは、ランサムウェア・サイレント障害・人為的ミスに対する備えとして重要です。

RubrikはNASのバックアップ、検索、リストアにおいても、シンプル、かつ効率的に行うことが可能です。

特にNetApp社との連携を強めており、スキャンポイントでSnapDiff機能を活用できます。

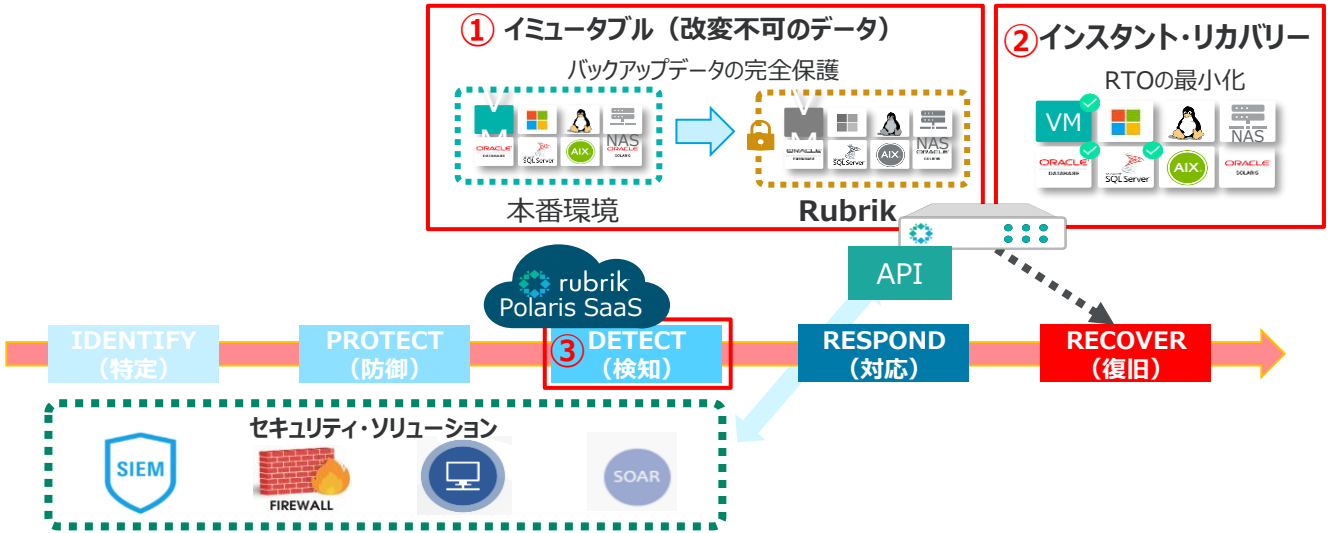


Rubrik④ランサムウェア対策

Rubrikはバックアップデータが外部からの改変を不可とするイミュータブルファイルシステムを実装しているため、本番環境がランサムウェア被害にあっても確実にデータを復旧できます。

シンプルな操作性と即時復旧が可能なインスタントリカバリーを活用することで、業務全体の迅速な復旧が可能です。

Rubrikが提供するSaaSのPolaris Radarと連携することで、ランサムウェア被害の能動的な検知や影響範囲の特定が容易になります。



検証概要

以下の機能を中心に検証を実施し、バックアップシステム、連携機能の
有用性を確認します。

- ETERNUS AX/HXシリーズ SnapDiff 連携機能
  SnapDiff APIの連携により書き換えの発生したファイルを効率的に検出し、
  大容量、数万ファイルの大規模なETERNUS AX/HX環境を効率的にバックアップ可能

- ランサムウェア対策機能
  Rubrik Polaris RadarのSaaSサービスと連携し、バックアップデータを分析することで
  ランサムウェアによる被害を検出し、警告を発信

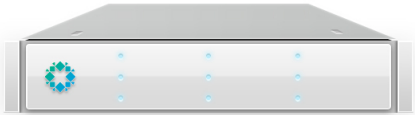
2. 検証構成

検証構成

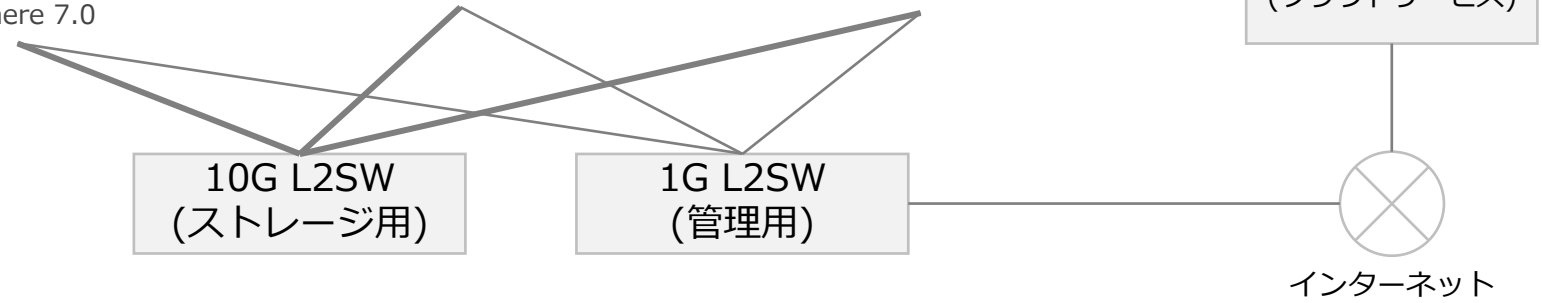
- 検証期間: 2021年9月17日～11月30日
- 検証場所: 富士通 Platform Solution Lab (蒲田)

PRIMERGY RX2540 M5
Xeon Gold 6240 x2
メモリ64GB
vSphere 7.0

ETERNUS AX2100
ONTAP 9.9.1P1
SSD 960GBx12



Rubrik r6404s
4ノード / 計40コア・メモリ256GB
SSD 400GBx4 / HDD 4TBx12

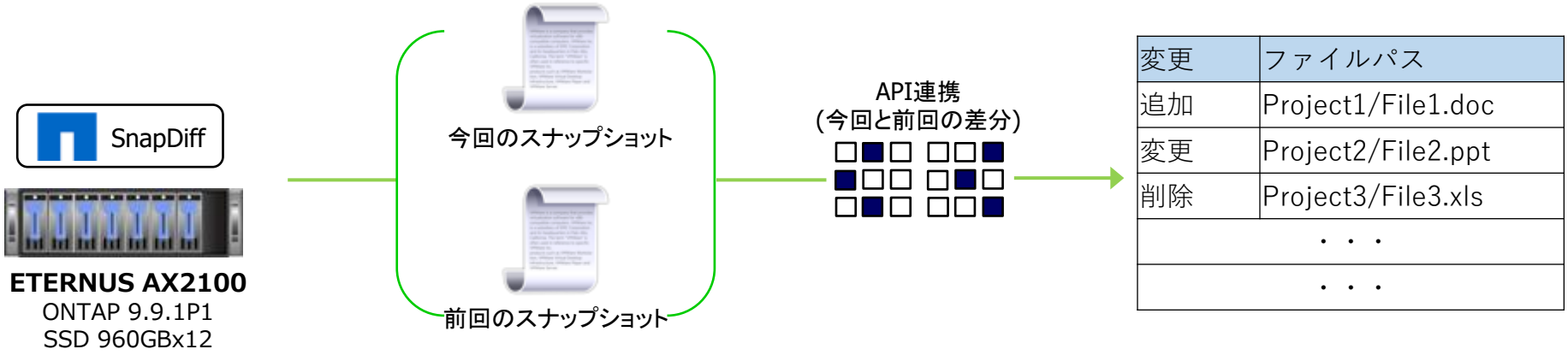


3-1. 検証結果

ETERNUS AX/HXシリーズ
SnapDiff 連携バックアップ検証

SnapDiff連携機能について

Rubrikは、NetApp社が提供するSnapDiffと連携することで、すべてのファイルのメタデータをチェックすることなく、前回のスナップショットから変更差分ファイル情報が把握できるため、スキャン時間の短縮、NASの負荷低減に繋がります。



変更	ファイルパス
追加	Project1/File1.doc
変更	Project2/File2.ppt
削除	Project3/File3.xls
・・・	
・・・	

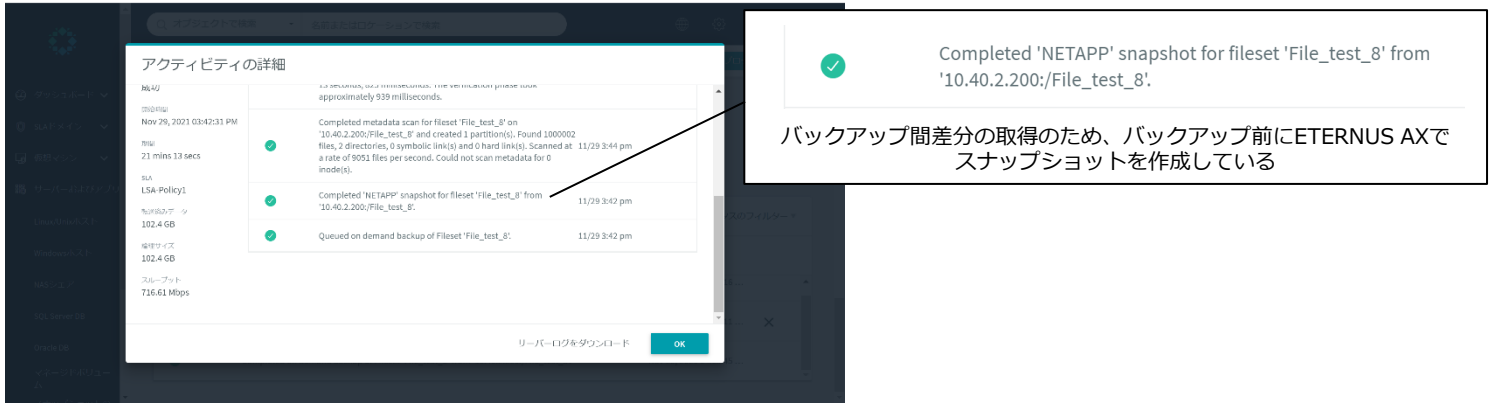
＜備考＞
・ETERNUS AX/HXシリーズは富士通株式会社によるNetApp社のOEM製品となります。
・SnapDiffは、2つのSnapshotコピー間のファイルやディレクトリの差異を迅速に識別するData ONTAPの内部エンジンです。

SnapDiff連携機能：検証内容

■検証内容

・RubrikのSnapDiff連携機能を有効にして以下の作業を行い、(1)と(2)でバックアップの所要時間と、バックアップ中のETERNUS AXの平均CPU負荷率を測定、比較しました。
（１）ETERNUS AXのNFSボリュームに10万個のファイルを作成しバックアップ取得
（２）1万個のファイルを追加で作成し再度バックアップを取得

・同様の作業をファイル100万個(追加ファイル作成10万個)でも行いました。

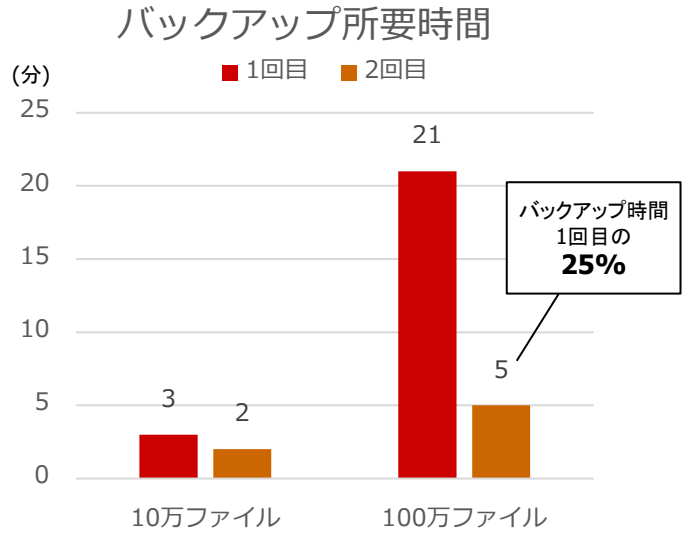


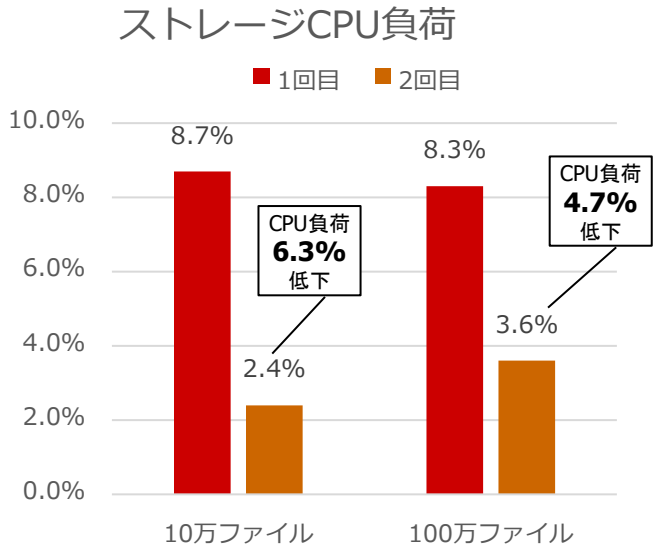
RubrikによるETERNUS AXボリュームバックアップのログ

SnapDiff連携機能：検証結果

■検証結果

SnapDiff連携機能により2回目のバックアップはETERNUS AXからRubrikへ更新されたファイルの情報が渡されることでファイルの更新チェックが不要になり、更新されたファイルのみバックアップされるため、1回目よりも所要時間が短く、ストレージのCPU負荷も下がりました。
そのため、頻繁なアクセスが発生している時間帯でもETERNUS AXのバックアップが効率的に行えると言えます。



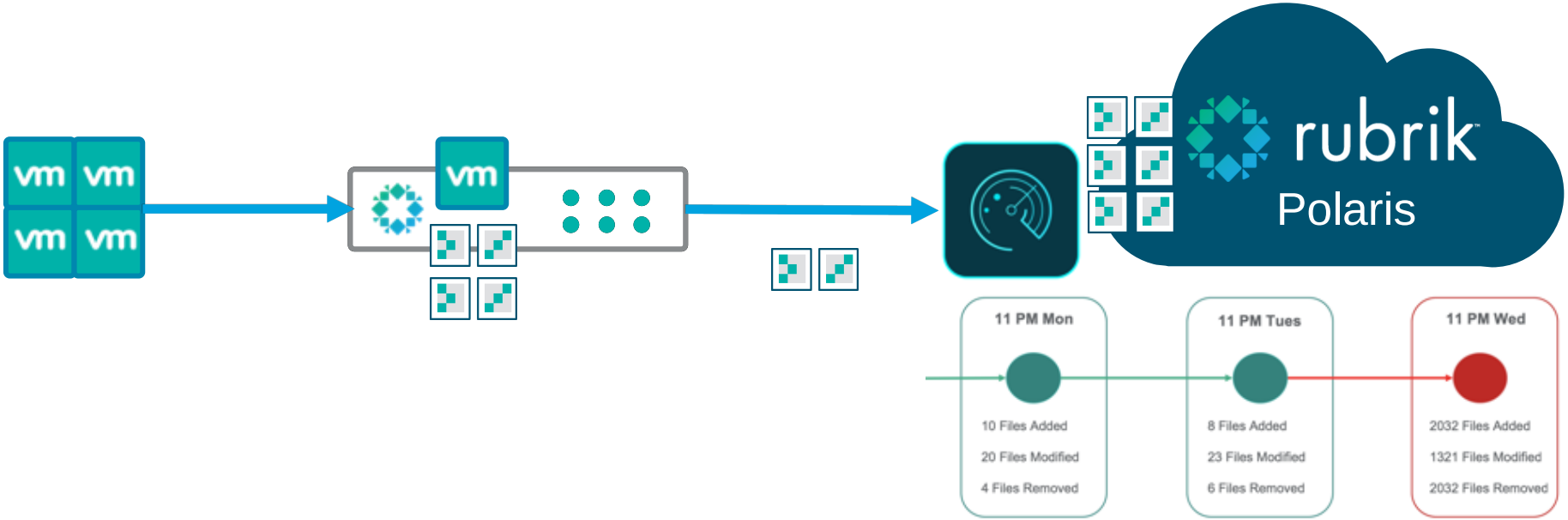


3-2. 検証結果

ランサムウェア対策機能検証

ランサムウェア対策機能 Polaris Radar

Polaris RadarはRubrikが提供するランサムウェア対策用のSaaSアプリケーション
サービスです。
アプライアンスから送られてくる日々のバックアップメタ情報をマシンラーニングで
解析します。
水面下で行われるファイルの暗号化を解析データから検知し、能動的に通知します。



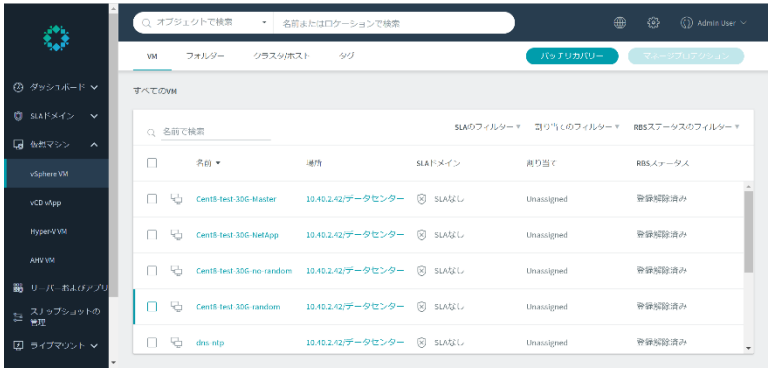
仮想マシンのバックアップ:検証内容

■検証内容

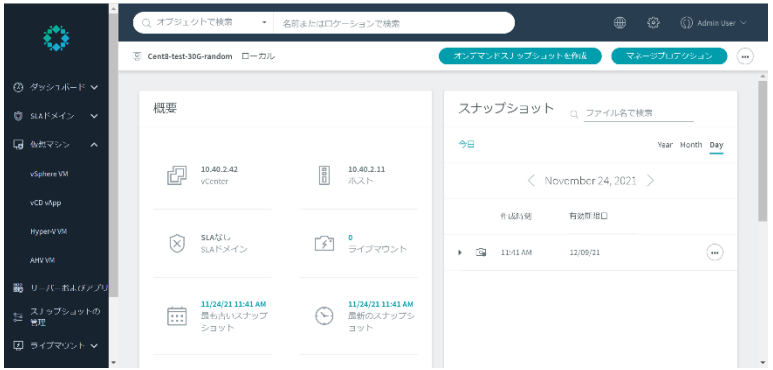
ランサムウェア対策機能 Polaris Radarはバックアップ間のファイル更新状況から通常運用時の状況を学習し、
異常な書き換えを検出することでランサムウェア被害を発見するため、導入にはシステム全体の定期的なバックアップ取得が必要となります。
そのため、多数の仮想マシンを連続でバックアップする想定で以下のバックアップ性能を検証しました。
(ストレージはPRIMERGY RX2540 M5の内蔵ストレージを使用しました)

（１）仮想マシンの連続バックアップ…仮想ディスク容量130GBの仮想マシンのバックアップを取得した後、
仮想マシン上にファイル(1GB)の追加と再バックアップをそれぞれ2回実施

（２）複数仮想マシンのバックアップ…30GBのファイルを作成した仮想マシンのバックアップを3VM同時に取得し、
同サイズの1VMバックアップの所要時間と比較



バックアップ対象仮想マシンの選択画面



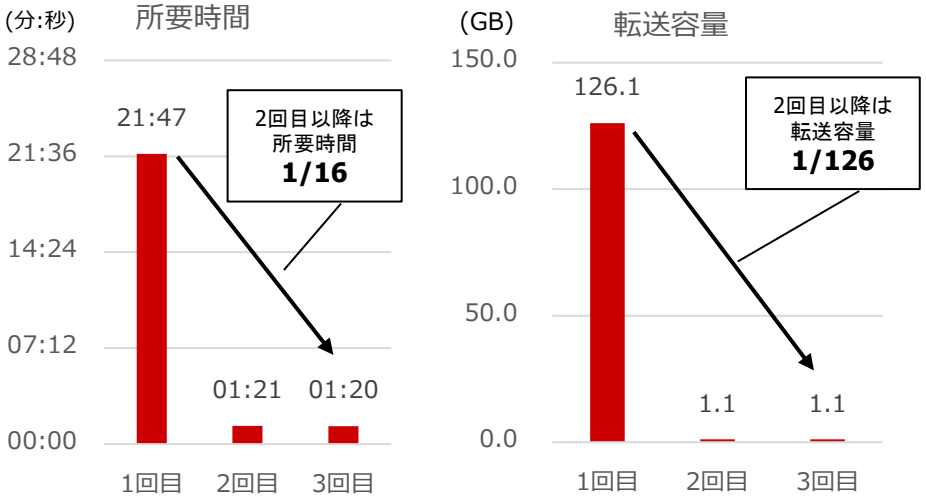
仮想マシンのバックアップ状況確認画面

仮想マシンのバックアップ:検証結果

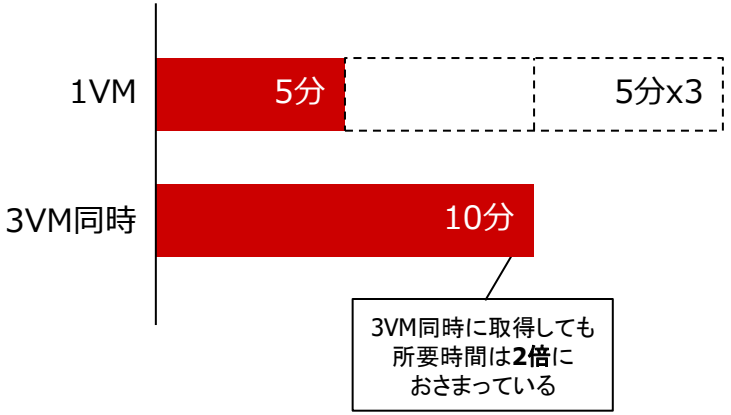
■検証結果

Rubrikにより、vSphere上の仮想マシンのバックアップが問題なく取得できました。
仮想マシンの連続バックアップは2回目以降は短時間かつ取得でき、更新されたデータのみ転送されるため、定期的なバックアップが効率よく行えることがわかりました。複数仮想マシンのバックアップは並列で行われるため、3VM同時バックアップの所要時間は1VMの3倍よりも短くなりました。
そのため、Rubrikによりシステム全体の仮想マシンのバックアップが高頻度で取得できると言えます。

仮想マシンの連続バックアップ



複数仮想マシンのバックアップ

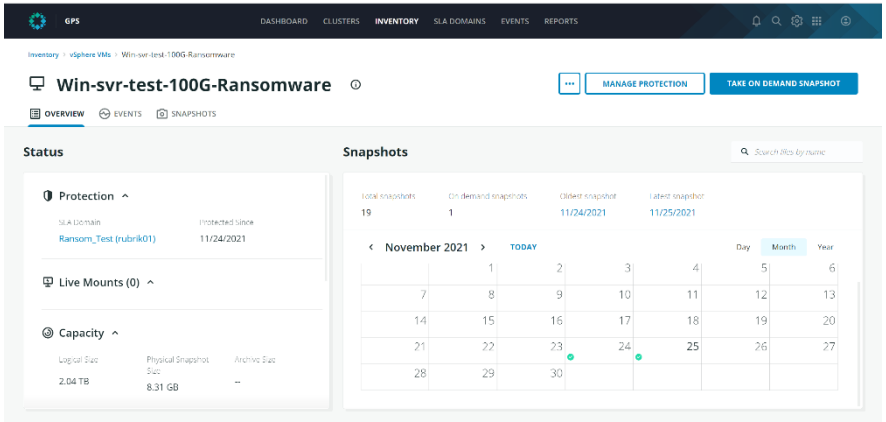


ランサムウェア被害の検出・回復:検証内容

■検証内容

仮想マシンにファイルを暗号化するランサムウェアの被害を想定し、以下の手順により被害の発生からどれくらいで検出できるか、被害にあったファイルを復元できるかを検証しました。

（１）仮想マシン上にファイルを4,999個作成
（２）仮想マシンのバックアップを50世代以上取得
（３）OS上のファイルを書き換えるツールを仮想マシンに対して実行
　※ファイルを暗号化するランサムウェア被害を想定
（４）再度バックアップを取得し、取得からランサムウェア被害が検出されるまでの時間を測定
（５）バックアップからのファイル復元を行う



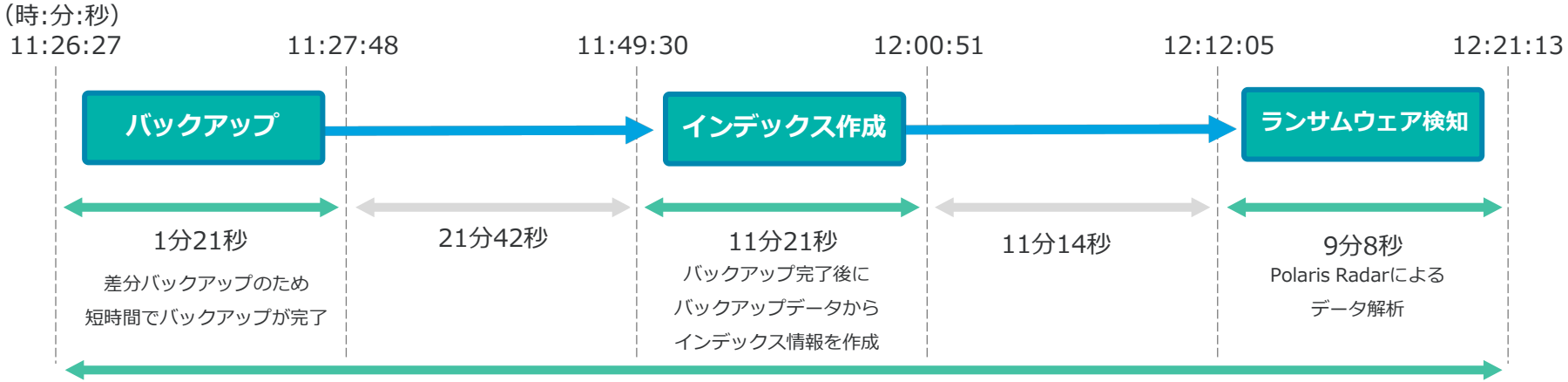
Polaris RadarのRubrik連携・スナップショット管理画面

ランサムウェア被害の検出・回復:検証結果①

■検証結果

・ランサムウェア被害の検出所要時間: 約55分
（バックアップ開始からRadarによるランサムウェア検知まで）

＜各タスクの開始時間と終了時間＞



TOTAL：54分46秒

バックアップ開始からランサムウェア検知までの合計時間

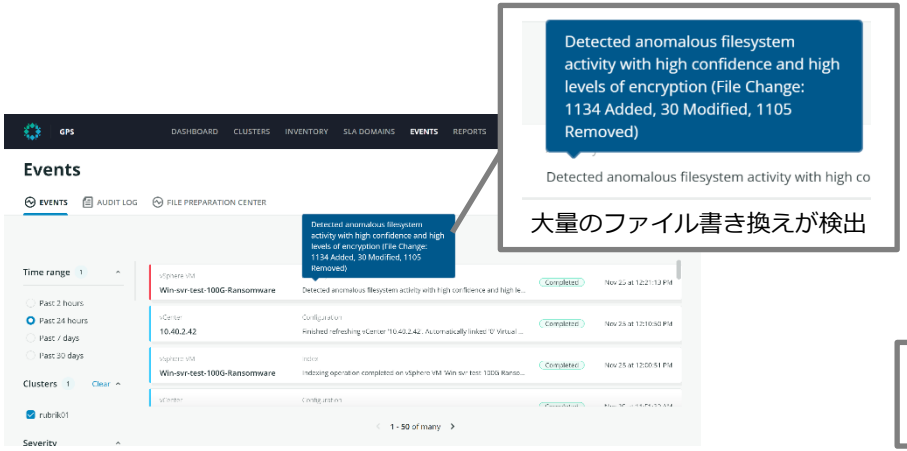
ランサムウェア被害の検出・回復:検証結果②

■検証結果

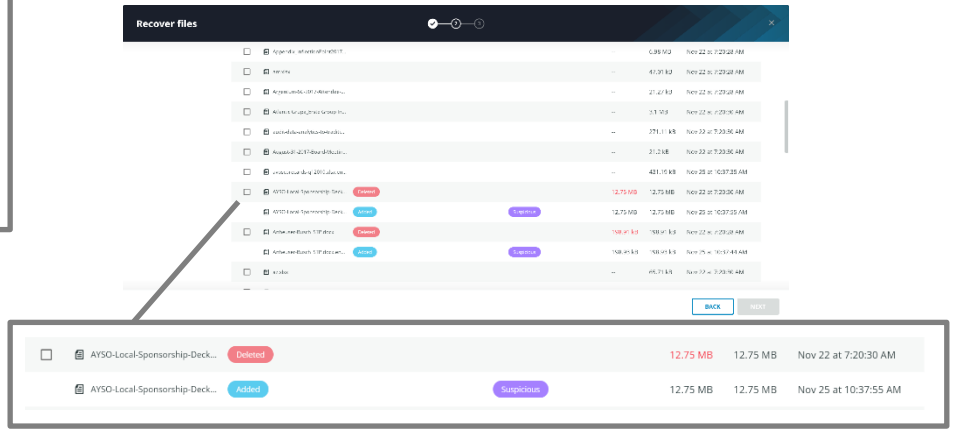
・バックアップからのファイル復元: 問題なく復元

・Polarisにより、不正なファイル書き換えが検出できることがわかりました。

・ファイルの大規模な書き換えが短時間で検出でき、書き換えられたファイルが問題なく復元できることがわかりました。また、Polaris(SaaSツール)のGUI画面でどのファイルがどのように書き換えられたかの確認と、ファイル復元も行えます。そのため、RubrikおよびPolaris Radarによりランサムウェアによる暗号化が行われても短時間で検出・復元ができるといえます。



Polaris Radarによるランサムウェア検出画面



ランサムウェアによるファイルの書き換え状況表示・ファイル回復画面

4. 検証総括

検証総括

本検証結果より、Rubrikは以下のような要望を持つお客様に
お薦めできるソリューションとなります。

- 大規模なNASファイルサーバのバックアップを行いたい
  SnapDiff 連携により効率的に大規模ファイルサーバ環境のバックアップが可能

- ランサムウェアに対する対策を行いたい
  ランサムウェア被害を即座に検知し、影響範囲の特定も容易で即時の復旧を行える
  Rubrikはランサムウェア対策のデータ保護ソリューションとして最適

- バックアップリストアでシンプルな操作運用を行いたい
  日本語対応しており直感的に操作が可能なGUIは使いやすく操作性に優れている。
  必要な情報をすぐに見つけられるシンプルなGUIにより設定変更や日々の運用、
  緊急のリストア時などでRubrikのシンプルな操作性は効率化に繋がる大きなメリット

補足:注意事項

本検証結果報告書は、検証を実施した2021年9月17日～11月30日時点での機能検証結果となります。

Rubrik社とNetApp社とのライセンス規約の更新、および変更により、 SnapDiff API機能と連携をした、バックアップのサポートが終了となります。本検証で実施したSnapDiff API機能との連携は使用が出来なくなりますが、引き続きRubrikのスキャン機能による差分情報の取得、ならびにNetApp ONTAP APIとの連携（NetAppストレージのスナップショットとの連携によるバックアップ）は可能です。NetApp ONTAP APIとは引き続き連携可能なため、共有領域の自動検索や、スナップショットと連携したオープンファイルの保護が可能となります。
また、Rubrikクラスタ内の複数ノードで連携して大容量データの分散バックアップが可能である点やNASファイルサーバから取得したバックアップデータからPolaris Radarによるランサムウェア検知が可能なため、引き続きNetAppストレージのバックアップソリューションとしてRubrikはお薦めできるソリューションとなります。
（追記：2022年6月30日）

ありがとうございました

お問い合わせ先

ノックス株式会社

営業本部

住所 ： 〒152-0023 東京都目黒区八雲2-23-13

電話 ： 03-5731-5551 / FAX ： 03-5731-5552

Email ： sales@nox.co.jp