BlueXPのランサムウェア対策を活用

BlueXP ransomware protection

NetApp
May 10, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/bluexp-ransomware-protection/rp-use-overview.html on May 10, 2024. Always check docs.netapp.com for the latest.

目次

BlueXPのランサムウェア対策を活用 1
BlueXPのランサムウェア対策を活用 1
ダッシュボードを使用してワークロードの健常性を一目で表示 1
ランサムウェア攻撃からワークロードを保護 4
検出されたランサムウェアに関するアラートに対応 11
ランサムウェア攻撃からのリカバリ（インシデントの中和後） 13

BlueXPのランサムウェア対策を活用

BlueXPのランサムウェア対策を活用

BlueXPのランサムウェア対策を使用すると、ワークロードの健常性を確認してワークロードを保護できます。

- "BlueXPのランサムウェア対策でワークロードを検出"。
- "ダッシュボードから保護とワークロードの健全性を表示"。
  - ランサムウェア対策に関する推奨事項を確認して対処
- "ワークロードを保護"：
  - ワークロードにランサムウェア対策ポリシーを割り当てる。
  - アプリケーションの保護を強化して、将来のランサムウェア攻撃を防止します。
  - 保護ポリシーを作成、変更、削除します。
- "ランサムウェア攻撃の可能性の検出に対応"。
- "攻撃からのリカバリ" （事件が中和された後）。
- "保護の設定"。

ダッシュボードを使用してワークロードの健常性を一目で表示

BlueXPランサムウェア対策ダッシュボードには、ワークロードの保護の健全性に関する情報が一目でわかるように表示されます。リスクがあるワークロードや保護されているワークロードをすばやく特定し、インシデントやリカバリの影響を受けたワークロードを特定し、保護されているストレージ容量やリスクがあるストレージ容量を確認することで保護の範囲を判断できます。

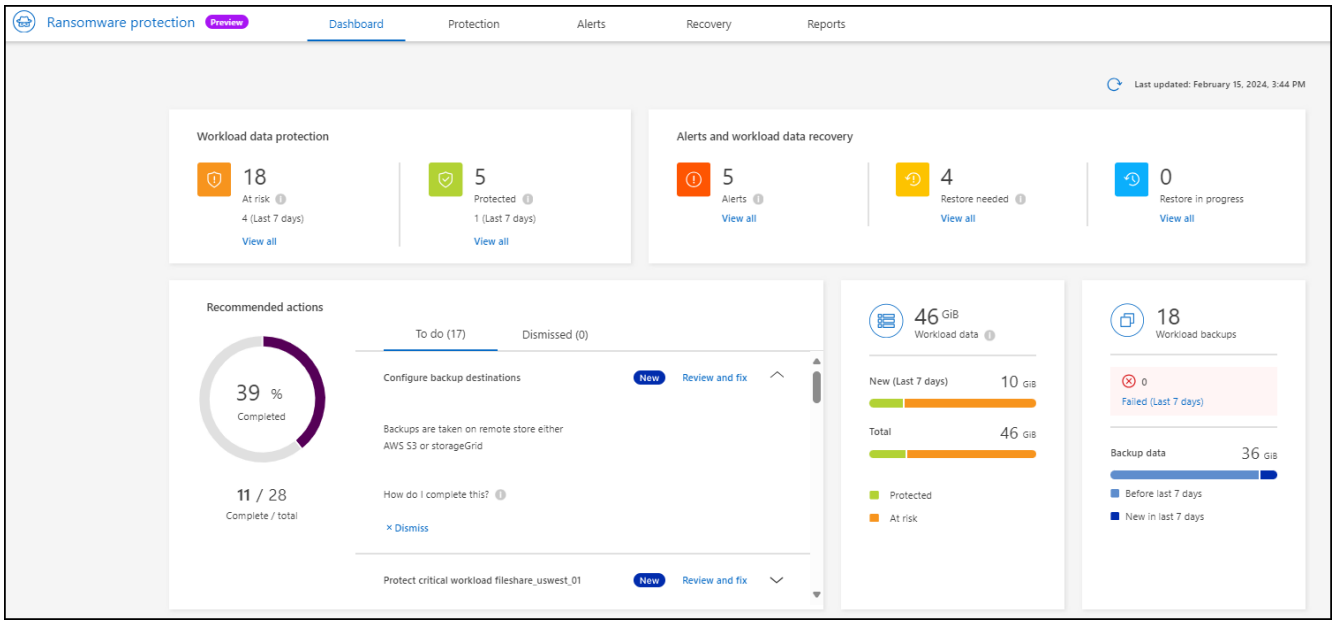
ダッシュボードを使用して、保護の推奨事項を確認して対処することもできます。

ダッシュボードを使用したワークロードの健全性の確認

手順

1. BlueXPの左側のナビゲーションで、**[保護]**>*[Ransomware protection]*を選択します。

   検出が完了すると、ワークロードのデータ保護の健常性がダッシュボードに表示されます。



2. ダッシュボードでは、各ペインで次の操作を表示および実行できます。

   - ワークロードのデータ保護：*[すべて表示]*をクリックすると、リスクがあるか保護されているすべてのワークロードが[保護]ページに表示されます。保護レベルが保護ポリシーと一致しないと、ワークロードがリスクにさらされます。を参照してください "ワークロードを保護"。
   - アラートとワークロードデータのリカバリ：*[すべて表示]*をクリックして、ワークロードに影響を与えたアクティブなインシデント、インシデントが中和された後のリカバリの準備ができているアクティブなインシデント、またはリカバリ中を参照してください "検出されたアラートへの対応"。

     インシデントは、次のいずれかの状態に分類されます。

     - 影響を受ける（[Alerts]ページに表示）
     - リカバリの準備完了（[Recovery]ページに表示）
     - リカバリ（[Recovery]ページに表示）
     - recovery failed（[Recovery]ページに表示）
     - リカバリ済み（[Recovery]ページに表示）
   - 推奨される対処方法：保護を強化するには、各推奨事項を確認し、*[確認と修正]*をクリックします。

     を参照してください "ダッシュボードで保護の推奨事項を確認する" または "ワークロードを保護"。

     最後にダッシュボードにアクセスしてから追加された推奨事項には、24時間以上[New]と表示されます。アクションは優先度順にリストされ、最も重要なものが一番上に表示されます。それぞれを確認して対処することも、却下することもできます。

アクションの総数には、却下されたアクションは含まれません。

   - ワークロードデータ:過去7日間の保護範囲の変化を監視します。
   - ワークロードバックアップ：サービスで作成され、過去7日間に失敗または正常に完了したワークロードバックアップの変更を監視します。

ダッシュボードで保護の推奨事項を確認する

BlueXPのランサムウェア対策は、ワークロードの保護を評価し、保護を強化するためのアクションを提案します。

推奨事項を確認して対処すると、推奨ステータスが[完了]に変更されます。または、後でそれに対処したい場合は、それを却下することができます。アクションを却下すると、推奨事項が却下されたアクションのリストに移動します。このリストは後で確認できます。

ここでは、サービスが提供する推奨事項のサンプルを示します。

推奨事項	説明	カイケツホウホウ
ランサムウェア対策ポリシーを追加する	ワークロードは現在保護されていません。	ワークロードにポリシーを割り当てます。 を参照してください "ランサムウェア攻撃からワークロードを保護"。
バックアップデスティネーションの設定	ワークロードには現在バックアップ先がありません。	このワークロードを保護するには、このワークロードにバックアップデスティネーションを追加してください。 を参照してください "保護の設定"。
ポリシーを強化します。	ワークロードによっては、十分な保護がない場合があります。ポリシーでワークロードの保護を強化	保持期間の延長、バックアップの追加、変更不可のバックアップの適用、疑わしいファイル拡張子のブロック、セカンダリストレージの検出などが可能になります。 を参照してください "ランサムウェア攻撃からワークロードを保護"。
重要なアプリケーションワークロードをランサムウェアから保護	[保護]ページには、保護されていないアプリケーションワークロードが（割り当てられている優先度レベルに基づいて）クリティカルまたは重要であると表示されます。	これらのワークロードにポリシーを割り当てます。 を参照してください "ランサムウェア攻撃からワークロードを保護"。
重要または重要なファイル共有ワークロードをランサムウェアから保護	[保護]ページには、ファイル共有またはデータストアタイプで保護されていない重要なワークロードが表示されます。	各ワークロードにポリシーを割り当てます。 を参照してください "ランサムウェア攻撃からワークロードを保護"。
新しいアラートの確認	新しいアラートが存在します。	新しいアラートを確認します。 を参照してください "検出されたランサムウェアに関するアラートに対応"。

手順

1. BlueXPの左側のナビゲーションで、**[保護]**>*[Ransomware protection]*を選択します。
2. [推奨される操作]ペインで推奨事項を選択し、*[確認と修正]*を選択します。
3. 後で処理を終了するには、*[却下]*を選択します。

推奨事項がTo Doリストからクリアされ、却下されたリストに表示されます。

却下された項目は、後でTo Do項目に変更できます。アイテムを完了としてマークするか、却下されたアイテムをTo Doアクションに変更すると、合計アクションが1ずつ増加します。

4. 推奨事項に対処する方法に関する情報を確認するには、* INFORMATION *アイコンを選択します。

ランサムウェア攻撃からワークロードを保護

BlueXPのランサムウェア対策を使用して次の操作を実行することで、ランサムウェア攻撃からワークロードを保護できます。

- 既存のワークロード保護を表示
- ワークロードにポリシーを割り当てます。
  - アプリケーションの保護を強化して、将来のRW攻撃を防止します。
  - 以前にrwサービスで保護されていたワークロードの保護を変更します。
- ポリシーを管理します（作成したポリシーのみ）。

BlueXPのランサムウェア対策は、検出時に各ワークロードに優先順位を割り当てます。ワークロードの優先順位は、次のSnapshotの頻度によって決まります。

- 重要：Snapshotコピーは1時間に1つ以上作成されます（非常に積極的な保護スケジュール）。
- 重要：Snapshotコピーは1時間に1回未満、1日に1回以上作成されます。
- 標準：1日に1つ以上のSnapshotコピーを作成

保護ステータス：ワークロードには、ポリシーが適用されているかどうかを示す次のいずれかの保護ステータスが表示されます。

- 保護：ポリシーが適用されます。
- リスクあり：ポリシーは適用されません。
- 進行中：ポリシーが適用されていますが、まだ完了していません。
- 失敗:ポリシーは適用されていますが、機能していません。

保護の健常性：ワークロードの保護の健常性ステータスは、次のいずれかになります。

- 正常：ワークロードで保護が有効になっており、バックアップとSnapshotコピーが完了しています。
- 実行中：バックアップまたはSnapshotコピーが実行中です。
- 失敗：バックアップまたはSnapshotコピーが正常に完了していません。
- * N/A *：ワークロードで保護が有効になっていないか、十分に機能していません。

ワークロードのランサムウェア対策を見る

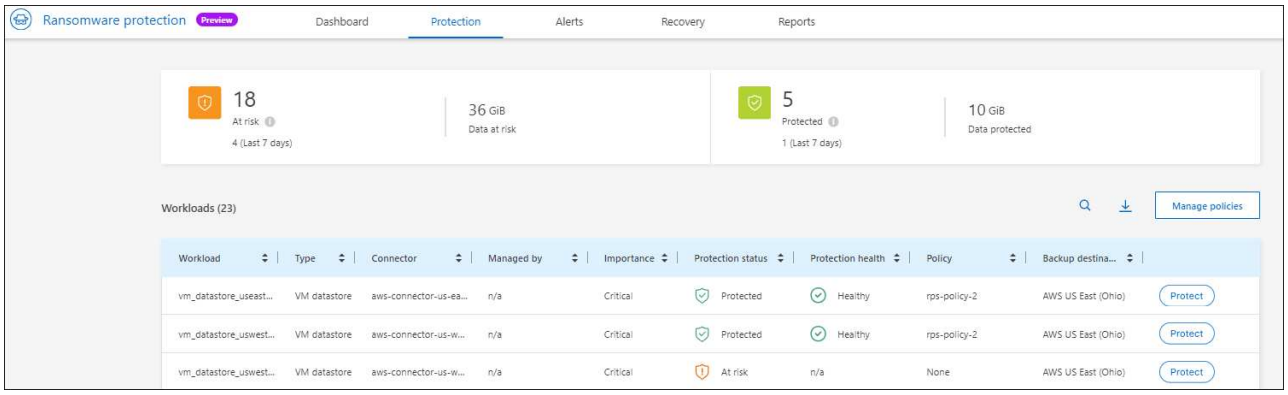
ワークロードを保護するための最初の手順の1つは、現在のワークロードとその保護ステータスを確認するこ

とです。次のタイプのワークロードが表示されます。

- VMワークロード
- ファイル共有のワークロード

手順

1. BlueXPの左側のナビゲーションで、**[保護]**>*[Ransomware protection]*を選択します。
2. 次のいずれかを実行します。
    - [ダッシュボード][データ保護]ペインで、*[すべて表示]*を選択します。
    - メニューから*[保護]*を選択します。



ページ"]

3. このページでは、ワークロードにポリシーを割り当てることができます。

ワークロードに事前定義された保護ポリシーを割り当てる

データの保護に役立つように、既存のランサムウェア対策ポリシーを1つ以上のワークロードに割り当てることができます。すでにポリシーが設定されているワークロードに別のポリシーを割り当てることもできます。

BlueXPのランサムウェア対策には、ワークロードの優先順位に合わせて次のポリシーが事前定義されています。

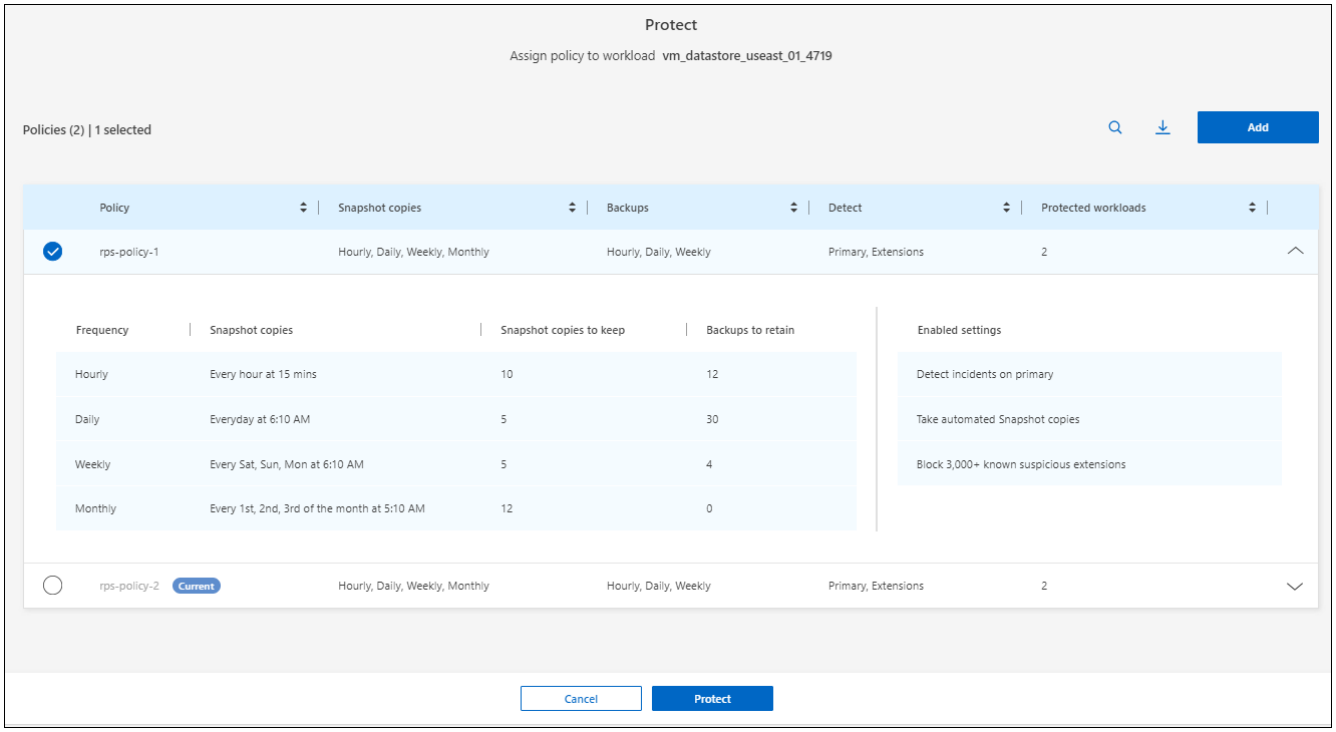
ポリシーレベル	スナップショット	頻度	保持（日数）	**Snapshot**コピー数	**Snapshot**コピーの最大総数
重要なワークロードポリシー	四半期毎時間	15分ごと	3.	288	309
	毎日	1日ごと	14	14	309
	毎週	1週間ごと	35	5.	309
	毎月	30日ごと	60ドルだ	2.	309

ポリシーレベル	スナップショット	頻度	保持（日数）	**Snapshot**コピー数	**Snapshot**コピーの最大総数
重要なワークロードポリシー	四半期毎時間	30分ごと	3.	144です	165
	毎日	1日ごと	14	14	165
	毎週	1週間ごと	35	5.	165
	毎月	30日ごと	60ドルだ	2.	165
標準ワークロードポリシー	四半期毎時間	60分ごと	3.	72です	93
	毎日	1日ごと	14	14	93
	毎週	1週間ごと	35	5.	93
	毎月	30日ごと	60ドルだ	2.	93

手順

1. BlueXPのランサムウェア対策で、次のいずれかを実行します。
   - [ダッシュボード][データ保護]ペインで、*[すべて表示]*を選択します。
   - [Dashboard Recommendation]ペインで、ポリシーの割り当てに関する推奨事項を選択し、*[Review and fix]*を選択します。
   - メニューから*[保護]*を選択します。
2. [保護]ページで、ワークロードを確認し、ワークロードの横にある*[保護]*を選択します。

   ポリシーのリストが表示されます。



3. 詳細を表示するには、ポリシーの下矢印をクリックします。
4. ワークロードに割り当てるポリシーを選択してください。
5. [保護]*を選択します。
6. [Dashboard]の推奨操作ウィンドウで、操作が[Completed]になっていることを確認します。

保護ポリシーを作成する

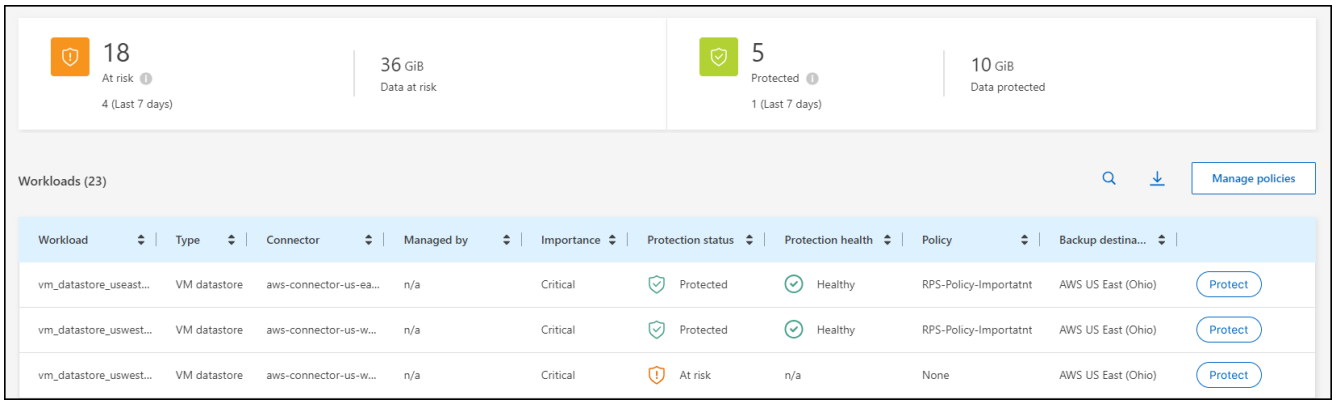
既存のポリシーがビジネスニーズを満たしていない場合は、新しい保護ポリシーを作成できます。独自のポリシーを最初から作成することも、既存のポリシーを使用して設定を変更することもできます。

プライマリストレージとセカンダリストレージを管理するポリシーを作成し、プライマリストレージとセカンダリストレージを同じまたは別の方法で扱うことができます。

ポリシーは、ポリシーを管理するとき、またはワークロードにポリシーを割り当てるプロセス中に作成できます。

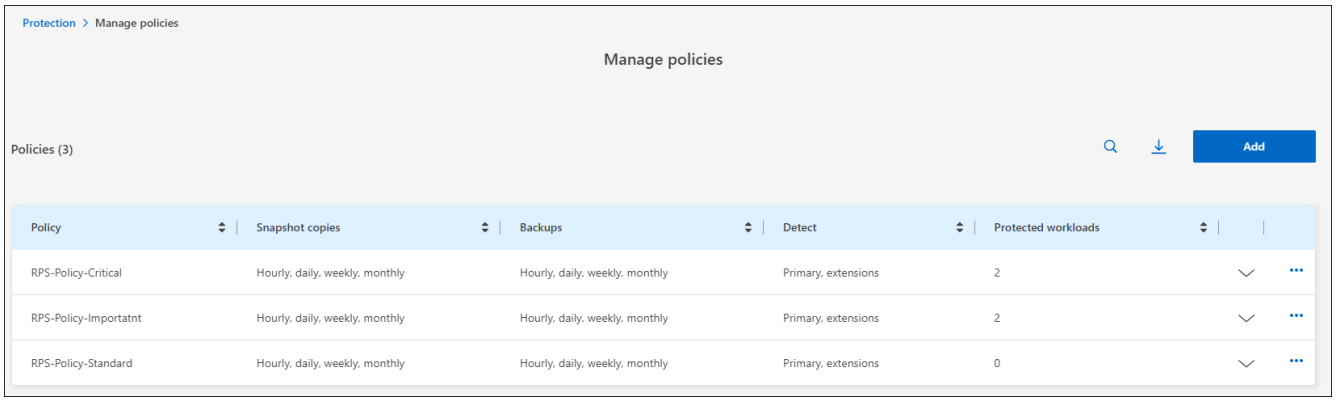
ポリシー管理時にポリシーを作成する手順

1. BlueXPのランサムウェア対策メニューから、* Protection *を選択します。



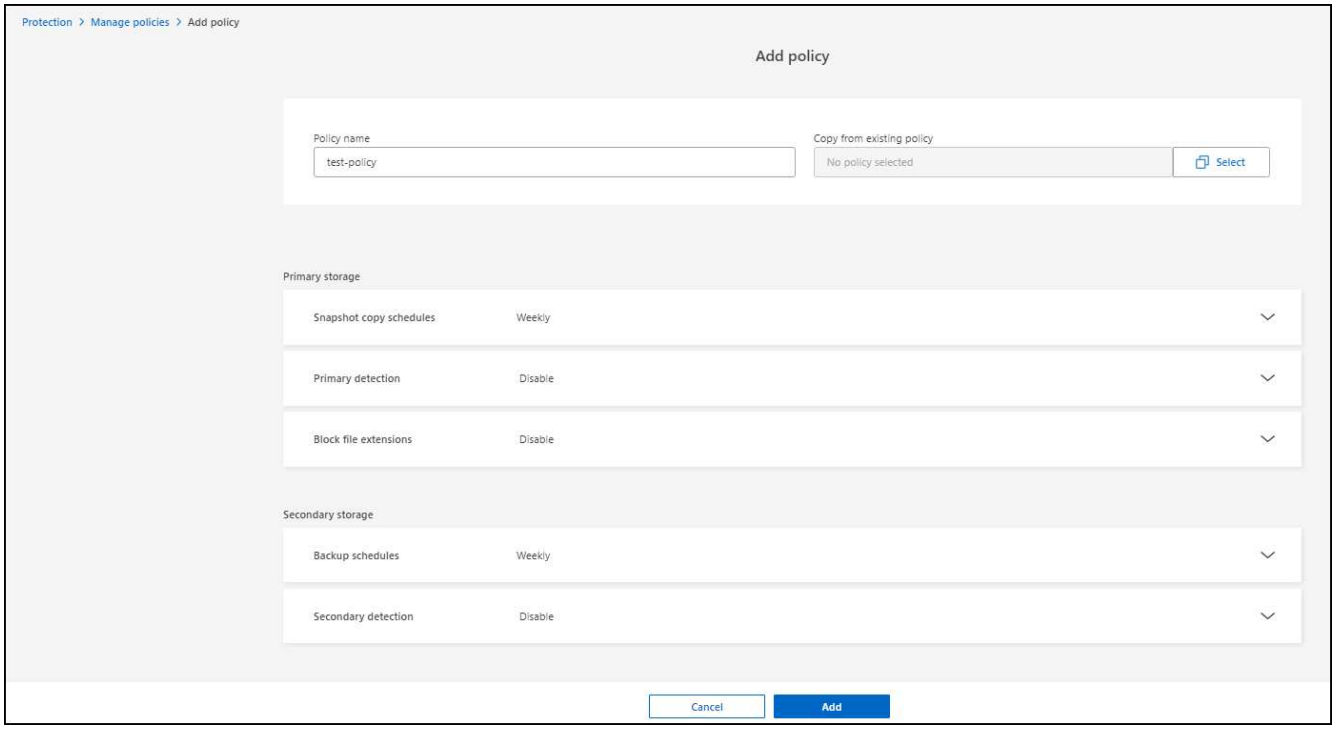
ページ"]

2. [保護]ページで、*[ポリシーの管理]*を選択します。



ページ"]

3. [ポリシーの管理]ページで、*[追加]*を選択します。



ページ"]

4. 新しいポリシー名を入力するか、既存のポリシー名を入力してコピーします。既存のポリシー名を入力した場合は、コピーするポリシーを選択します。

> 既存のポリシーをコピーして変更する場合は、一意にするために少なくとも1つの設定を変更する必要があります。

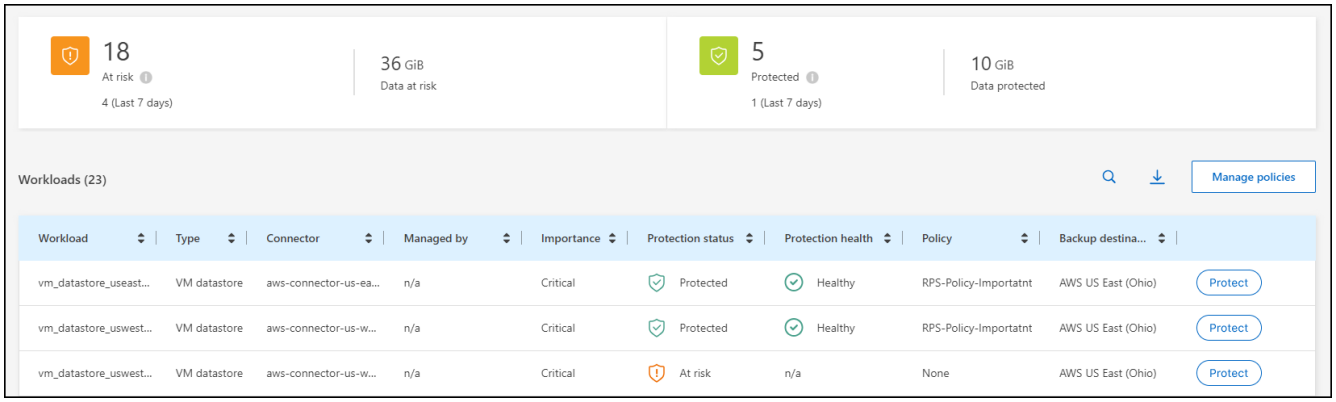
5. 各項目について、下矢印を選択します。
   - プライマリストレージ：
     - * Snapshotコピースケジュール*：スケジュールオプションと保持するSnapshotコピーの数を選択し、スケジュールを有効にする場合に選択します。
     - 一次検出：プライマリストレージ上のランサムウェアのインシデントを検出するサービスを有効にします。
     - ファイル拡張子をブロック:これを有効にすると、既知の疑わしいファイル拡張子がサービスブロックされます。プライマリ検出が有効になっている場合、サービスは自動Snapshotコピーを作成します。
   - セカンダリストレージ：
     - バックアップスケジュール:セカンダリストレージのスケジュールオプションを選択し、スケジュールを有効にします。
     - セカンダリ検出：セカンダリストレージ上のランサムウェアのインシデントを検出するサービスを有効にします。
     - バックアップをロック：セカンダリストレージ上のバックアップが一定期間変更または削除されないようにする場合に選択します。これは_不変ストレージ_とも呼ばれます。

       このオプションでは、セカンダリストレージ上のバックアップをロックするNetApp DataLockテクノロジを使用します。バックアップ・ファイルがロック（および保持）される期間をDataLockの保持期間と呼びます定義したバックアップポリシーのスケジュールと保持設定に加え、14日間のバッファに基づいて設定されます。30日未満のDataLock保持ポリシーは、最小30日に切り上げられます。

6. 「* 追加」を選択します。

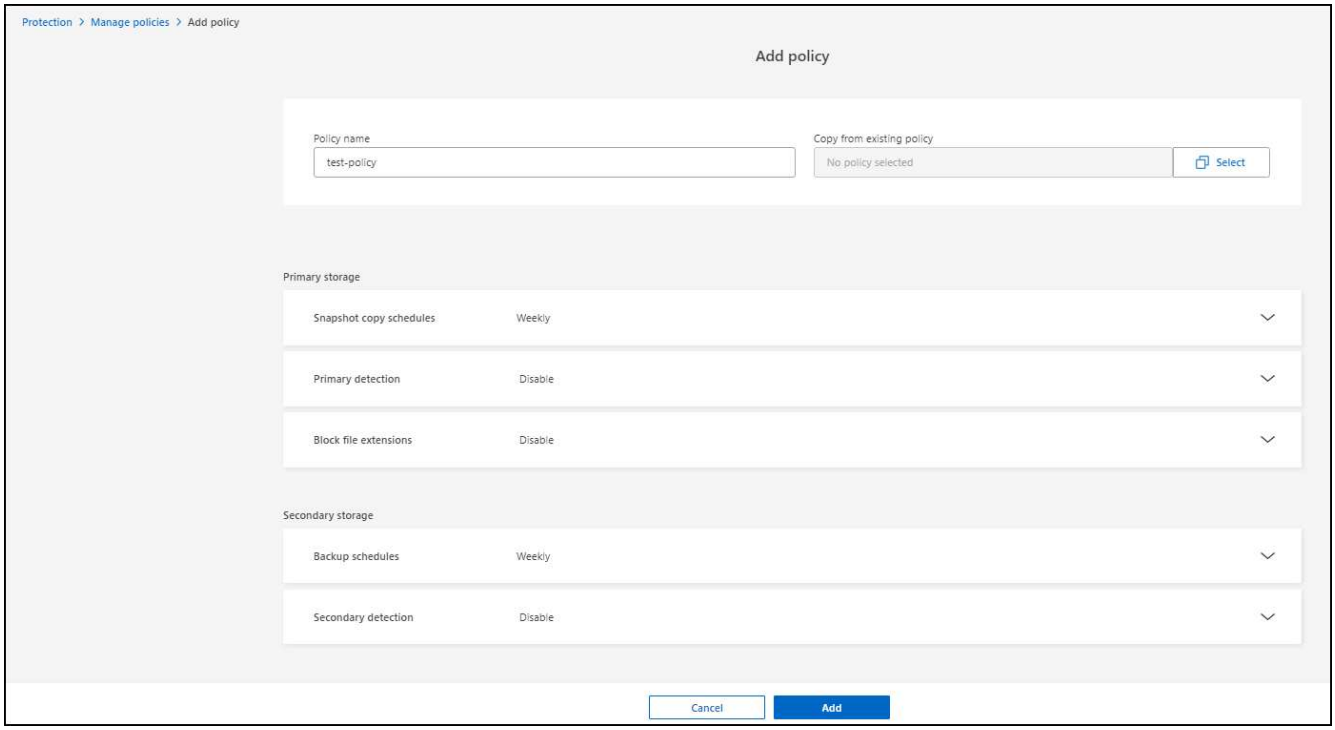
保護ポリシーの割り当て時にポリシーを作成する手順

1. BlueXPのランサムウェア対策メニューから、* Protection *を選択します。



ページ"]

2. [保護]ページで、*[保護]*を選択します。
3. [保護]ページで、*[追加]*を選択します。



ページ"]

4. [Manage policies]ページでポリシーを作成する場合と同じ手順で、プロセスを完了します。

別の保護ポリシーを割り当てる

ワークロードに別の保護ポリシーを選択できます。
保護ポリシーを変更することで、保護を強化し、将来のランサムウェア攻撃を防止できます。

手順

1. BlueXPのランサムウェア対策メニューから、* Protection *を選択します。
2. [保護]ページで、ワークロードを選択し、*[保護]*を選択します。
3. [保護]ページで、ワークロードに別のポリシーを選択します。
4. ポリシーの詳細を変更するには、右側の下矢印を選択して詳細を変更します。
5. [保存]*を選択して変更を終了します。

既存のポリシーを編集する

ポリシーの詳細を変更できるのは、ポリシーがワークロードに関連付けられていない場合だけです。

手順

1. BlueXPのランサムウェア対策メニューから、* Protection *を選択します。
2. [保護]ページで、*[ポリシーの管理]*を選択します。
3. [ポリシーの管理]ページで、変更するポリシーの*[アクション]*オプションを選択します。

4. [操作]メニューから*[ポリシーの編集]*を選択します。
5. 詳細を変更します。
6. [保存]*を選択して変更を終了します。

ポリシーを削除する

現在どのワークロードにも関連付けられていない保護ポリシーを削除できます。

手順

1. BlueXPのランサムウェア対策メニューから、* Protection *を選択します。
2. [保護]ページで、*[ポリシーの管理]*を選択します。
3. [ポリシーの管理]ページで、削除するポリシーの*[アクション]*オプションを選択します。
4. [操作]メニューから*[ポリシーの削除]*を選択します。

検出されたランサムウェアに関するアラートに対応

BlueXPのランサムウェア対策で攻撃の可能性が検出されると、BlueXPのランサムウェア対策ダッシュボードと右上のBlueXP通知にランサムウェア攻撃の可能性を示すアラートが表示されます。また、サービスはすぐにSnapshotコピーの作成を開始します。この時点で、BlueXPのランサムウェア対策*アラート*タブで潜在的なリスクを確認する必要があります。

データのリカバリを開始するには、ストレージ管理者がリカバリプロセスを開始できるように、アラートをリカバリ準備完了としてマークします。

各アラートには、ステータスが異なるボリューム上に複数のインシデントが存在する可能性があるため、すべてのインシデントを確認してください。

このサービスは、アラートが発行された原因に関する_evidence_という情報を提供します。これには、次のような情報が含まれます。

- ファイル拡張子が作成または変更された場合
- ファイルの作成が発生し、表示された割合で増加しました。
- ファイル削除が発生し、表示された割合で増加した

アラートは、次のタイプの動作に基づいています。

- 攻撃の可能性：Autonomous Ransomware Protectionが新しい拡張子を検出し、過去24時間に20回以上繰り返した場合にアラートが発生します（デフォルトの動作）。
- 警告：次の動作に基づいて警告が発生します。
  - 新しい拡張の検出はこれまでに特定されておらず、同じ動作が攻撃であると宣言するのに十分な回数繰り返されません。
  - 高エントロピーが観測される。
  - ファイルの読み取り/書き込み/名前変更/削除処理で、ベースラインを超えるアクティビティが100%急

増しました。

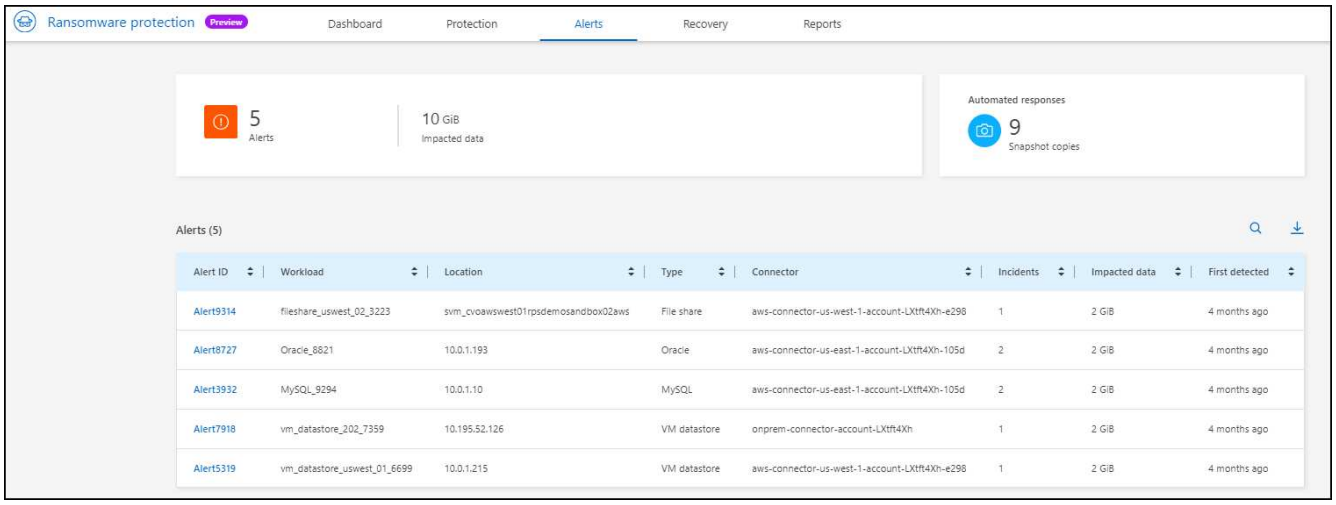
証拠は、ONTAPの自律型ランサムウェア対策の情報に基づいています。詳細については、を参照してください "Autonomous Ransomware Protection Overview"。

アラートを表示します

アラートには、BlueXPランサムウェア対策ダッシュボードまたは*[アラート]*タブからアクセスできます。

手順

1. BlueXPランサムウェア対策ダッシュボードで、[Alerts]ペインを確認します。
2. いずれかの彫像の下にある*すべて表示*を選択します。
3. アラートをクリックすると、各アラートの各ボリュームのすべてのインシデントを確認できます。
4. その他のアラートを確認するには、左上のパンくずリストにある* Alert *をクリックします。
5. [Alerts]ページでアラートを確認します。



ページ"]

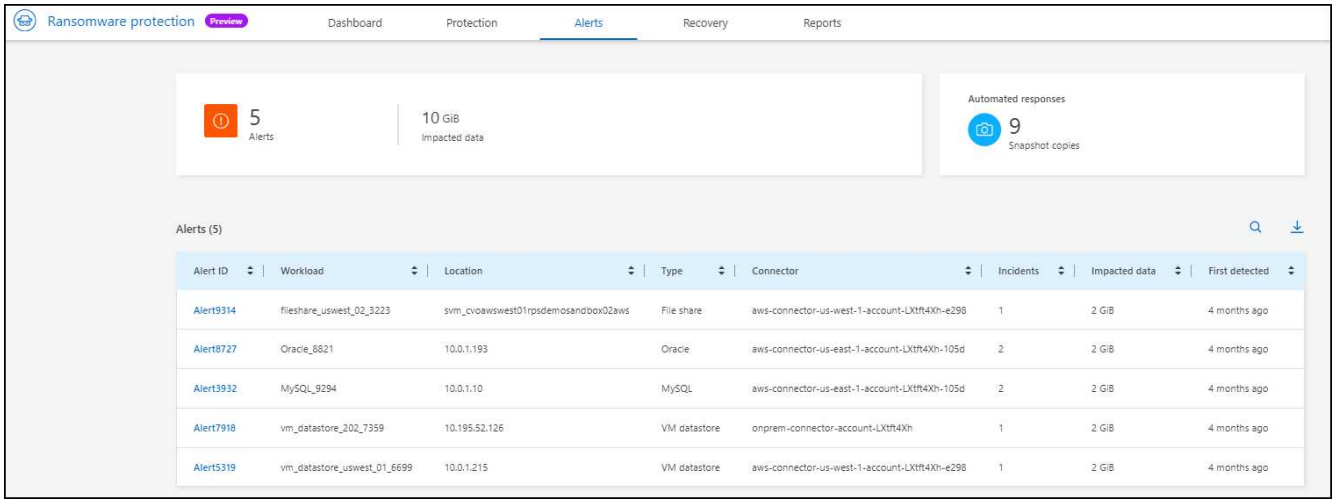
6. に進みます [ランサムウェアのインシデントをリカバリ準備完了としてマーク（インシデントが無力化された後）]。

ランサムウェアのインシデントをリカバリ準備完了としてマーク（インシデントが無力化された後）

攻撃を軽減し、ワークロードをリカバリできる状態になったら、ストレージ管理チームにデータのリカバリ準備ができていることを伝え、リカバリプロセスを開始できるようにします。

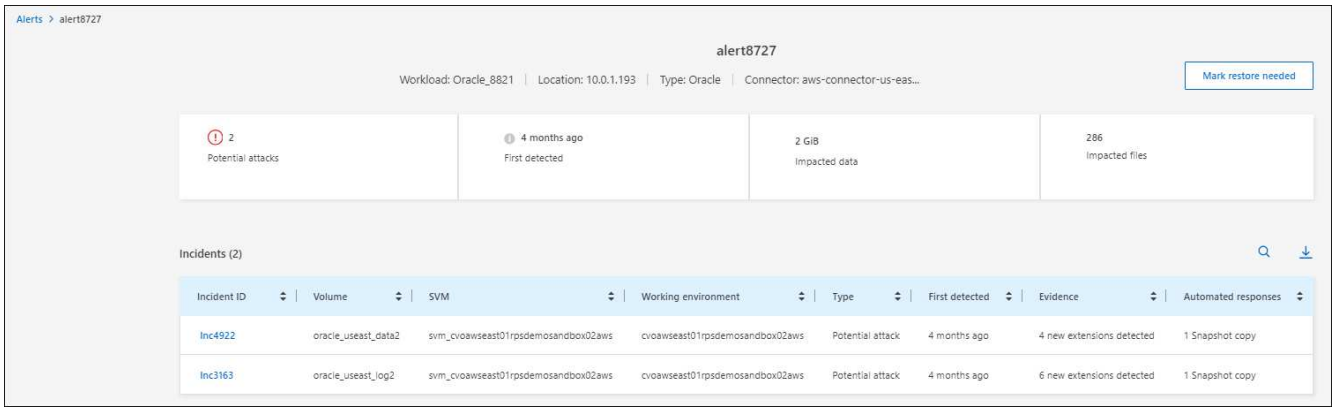
手順

1. BlueXPのランサムウェア対策メニューから、*アラート*を選択します。



ページ"]

2. [アラート]ページで、アラートを選択します。
3. アラートのインシデントを確認します。



4. インシデントをリカバリする準備ができていると判断した場合は、*[リストアが必要であることをマークする]*を選択します。
5. 操作を確認し、*[リストアが必要なマークを付ける]*を選択します。
6. ワークロードのリカバリを開始するには、メッセージで*ワークロードを選択するか、[リカバリ]*タブを選択します。

結果

アラートがリカバリ対象としてマークされると、アラートは[Alerts]タブから[Recovery]タブに移動します。

ランサムウェア攻撃からのリカバリ（インシデントの中和後）

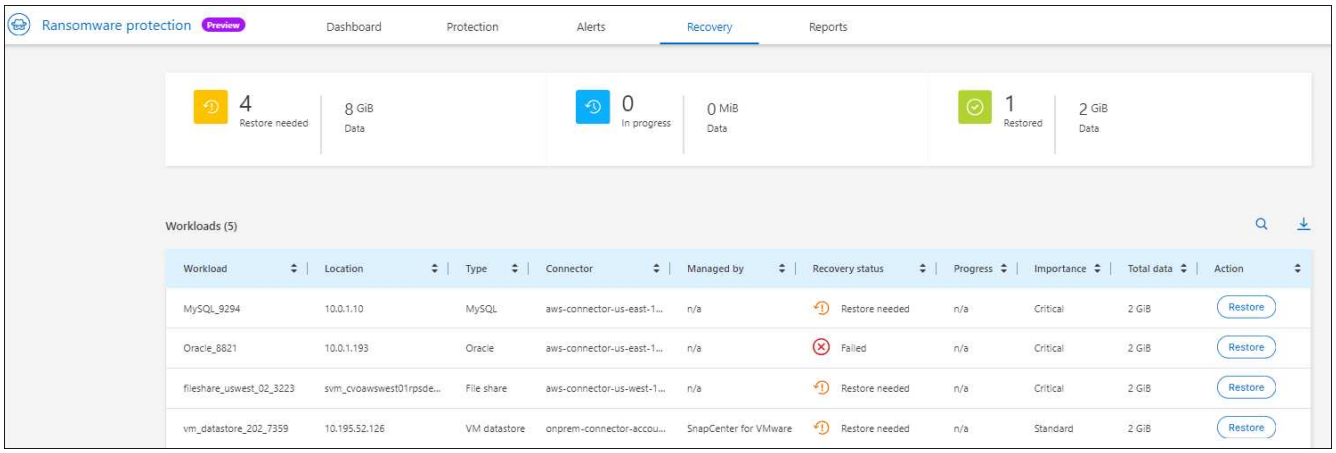
ワークロードが「Ready for recovery」とマークされると、BlueXPランサムウェア対策では、実際のRPA（Recovery Point Actual）を推奨し、クラッシュに強いリカバリのためのワークフローをオーケストレーションします。

リストアの準備が完了したワークロードを表示する

「Restore Needed」リカバリステータスのワークロードを確認します。

手順

1. 次のいずれかを実行します。
    - ダッシュボードの[Alerts]ペインで[Restore Needed]の合計を確認し、*[View All]*を選択します。
    - メニューから* Recovery *を選択します。
2. [リカバリ]*ページでワークロード情報を確認します。



ページ"]

ワークロードをリカバリする

BlueXPのランサムウェア対策を使用すると、ストレージ管理者は、推奨されるリストアポイントまたは希望するリストアポイントからワークロードをリカバリする最適な方法を判断できます。

セキュリティストレージ管理者は、さまざまなレベルでデータをリカバリできます。

- すべてのボリュームをリカバリ
- ボリュームレベルまたはファイルおよびフォルダレベルでアプリケーションをリカバリします。
- ボリュームレベル、ディレクトリレベル、またはファイル/フォルダレベルでファイル共有をリカバリします。
- データストアからVMレベルでリカバリ

このプロセスはワークロードの種類によって多少異なります。

手順

1. BlueXPのランサムウェア対策メニューから、*リカバリ*を選択します。
2. [リカバリ]*ページでワークロード情報を確認します。
3. 「Restore Needed」状態のワークロードを選択します。
4. リストアするには、*[リストア]*を選択します。
5. リストア範囲：完了するリストアのタイプを選択します。

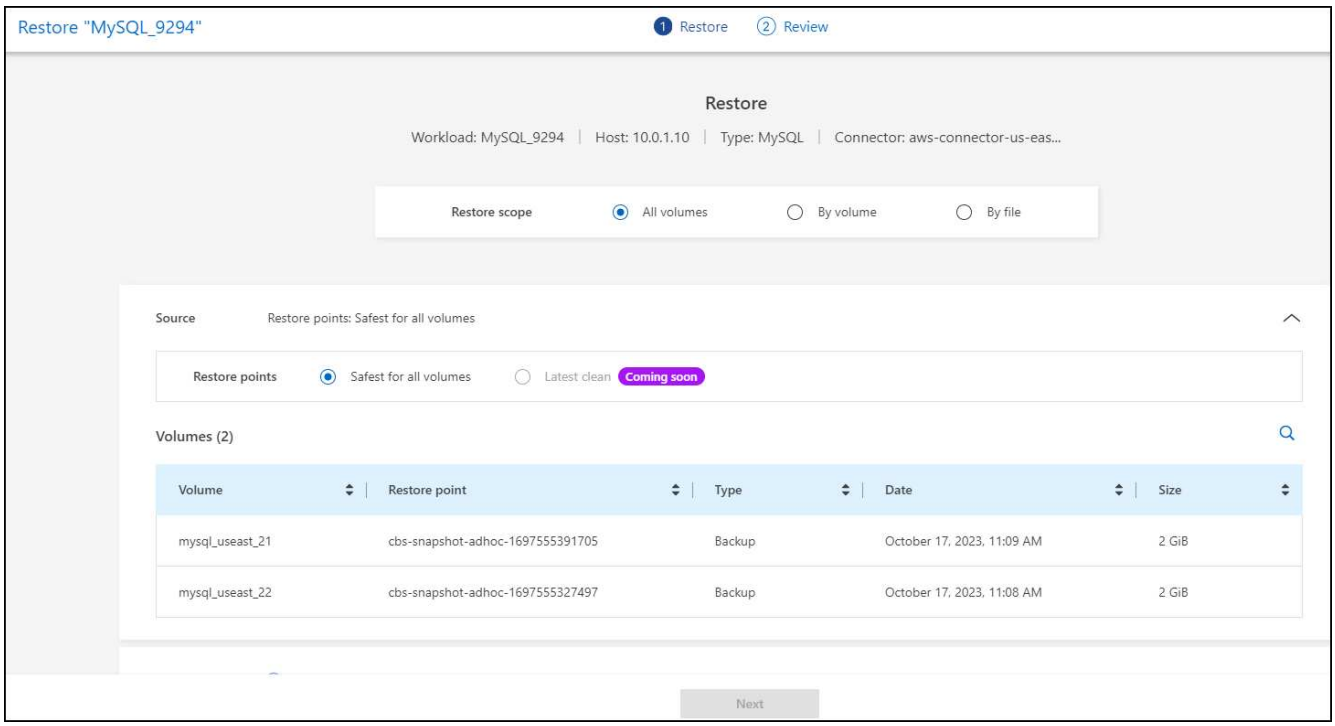
- すべてのボリューム
- ボリューム別
- ファイル別：リストアするフォルダまたは単一のファイルを指定できます。

> 最大100個のファイルまたは1つのフォルダを選択できます。

6. アプリケーション、ボリューム、ファイルのいずれを選択したかに応じて、次のいずれかの手順を実行します。

すべてのボリュームをリストア

1. [リストア]ページの[リストア]範囲で、*[すべてのボリューム]*を選択します。



2. ソース:ソースの横にある下向き矢印を選択すると、詳細が表示されます。
   a. データのリストアに使用する復元ポイントを選択します。

> BlueXPのランサムウェア対策は、インシデント発生直前の最新バックアップとして最適なリストアポイントを特定し、「すべてのボリュームで最も安全」を示します。つまり、最初に検出されたボリュームに対する最初の攻撃の前に、すべてのボリュームがコピーにリストアされます。

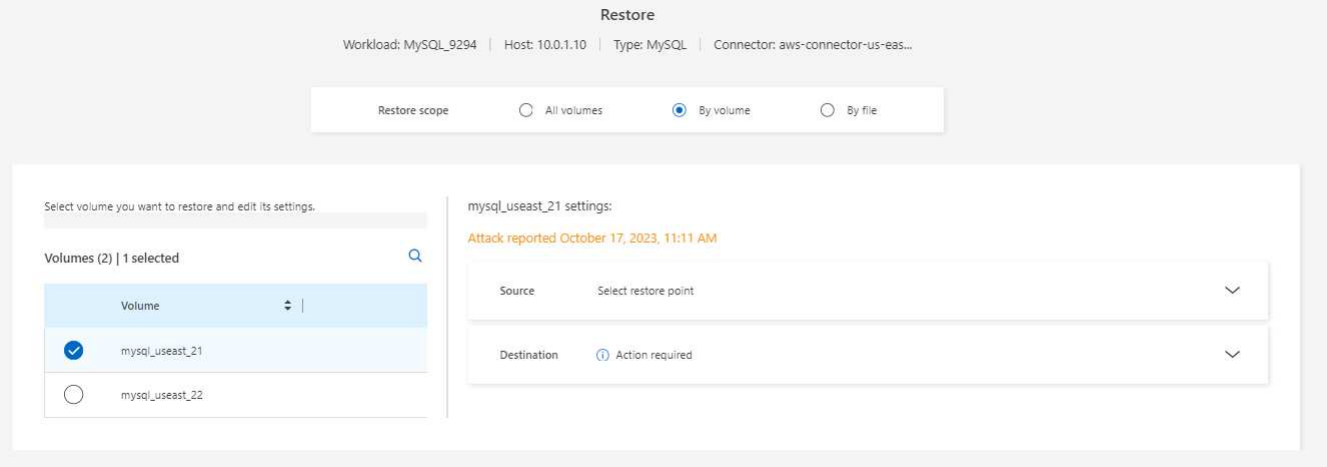
3. * Destination *：Destinationの横にある下向き矢印を選択すると、詳細が表示されます。
   a. 作業環境を選択します。
   b. Storage VMを選択します。
   c. アグリゲートを選択します。
   d. すべての新しいボリュームの先頭に付加されるボリュームプレフィックスを変更します。

新しいボリューム名は、プレフィックス+元のボリューム名+バックアップ名+バックアップ日付として表示されます。

4. [保存（ Save ）] を選択します。
5. 「 * 次へ * 」を選択します。
6. 選択内容を確認します。
7. [* Restore] を選択します。
8. トップメニューから* Recovery *を選択し、[リカバリ]ページで処理のステータスが状態間を移動するワークロードを確認します。

アプリケーションワークロードをボリュームレベルでリストア

1. [リストア]ページの[リストア対象]で、*[ボリューム別]*を選択します。



2. ボリュームのリストで、リストアするボリュームを選択します。
3. ソース:ソースの横にある下向き矢印を選択すると、詳細が表示されます。
   a. データのリストアに使用する復元ポイントを選択します。

BlueXPのランサムウェア対策は、インシデント発生直前の最新バックアップとして最適なリストアポイントを特定し、「推奨」を表示します。

4. * Destination *：Destinationの横にある下向き矢印を選択すると、詳細が表示されます。
   a. 作業環境を選択します。
   b. Storage VMを選択します。
   c. アグリゲートを選択します。
   d. 新しいボリューム名を確認します。

新しいボリューム名は、元のボリューム名+バックアップ名+バックアップ日付として表示されます。

5. [保存（ Save ）] を選択します。

6. 「 * 次へ * 」を選択します。
7. 選択内容を確認します。
8. [* Restore] を選択します。
9. トップメニューから* Recovery *を選択し、[リカバリ]ページで処理のステータスが状態間を移動するワークロードを確認します。

ファイルレベルでのアプリケーションワークロードのリストア

1. [リストア]ページの[リストア対象]で、*[ファイル別]*を選択します。
2. ボリュームのリストで、リストアするボリュームを選択します。
3. ソース:ソースの横にある下向き矢印を選択すると、詳細が表示されます。
   a. データのリストアに使用する復元ポイントを選択します。

      BlueXPのランサムウェア対策は、インシデント発生直前の最新バックアップとして最適なリストアポイントを特定し、「推奨」を表示します。

   b. 最大100個のファイルまたは1つのフォルダを選択してリストアします。
4. * Destination *：Destinationの横にある下向き矢印を選択すると、詳細が表示されます。
   a. データのリストア先として、元のソースの場所または指定可能な別の場所を選択します。

      元のファイルまたはディレクトリはリストアされたデータで上書きされますが、新しい名前を指定しないかぎり、元のファイル名とフォルダ名は変わりません。

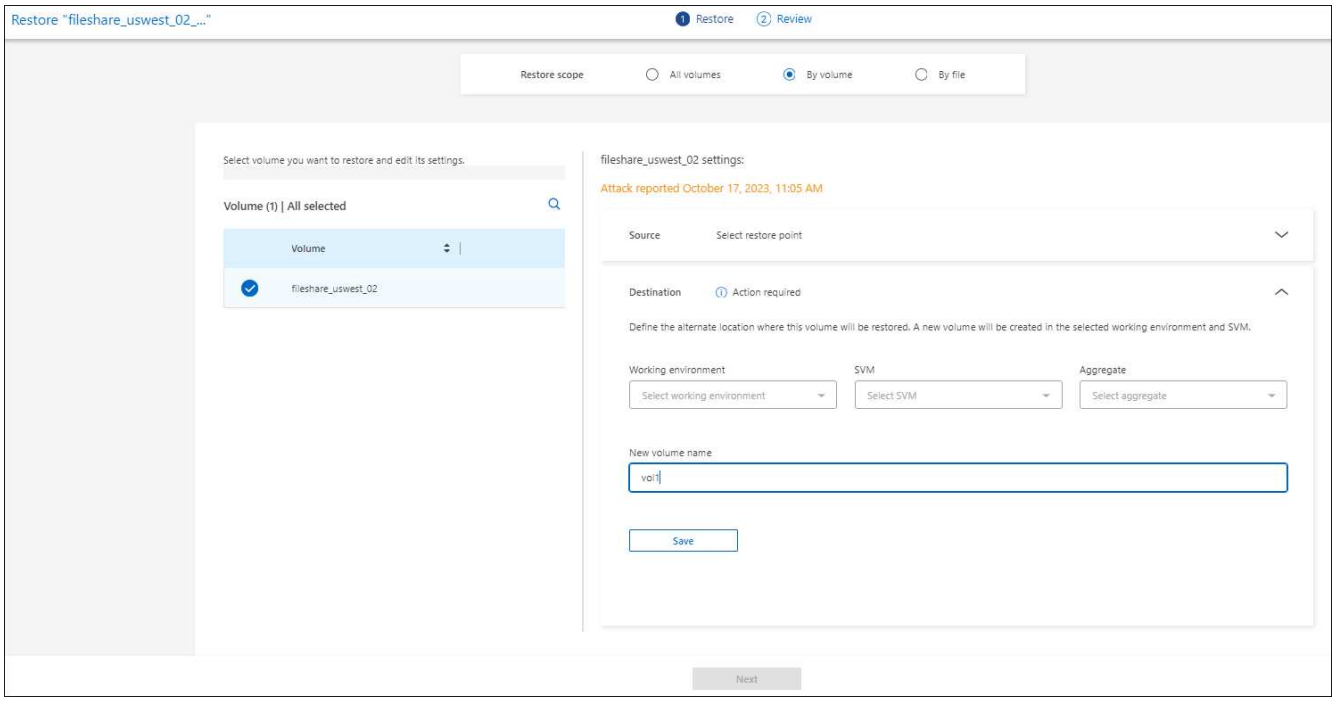
   b. 作業環境を選択します。
   c. Storage VMを選択します。
   d. 必要に応じて、パスを入力します。

      リストアのパスを指定しない場合、ファイルは最上位のディレクトリにある新しいボリュームにリストアされます。

   e. リストアされたファイルまたはディレクトリの名前を現在の場所と同じ名前にするか、別の名前にするかを選択します。
5. [保存（ Save ）] を選択します。
6. 「 * 次へ * 」を選択します。
7. 選択内容を確認します。
8. [* Restore] を選択します。
9. トップメニューから* Recovery *を選択し、[リカバリ]ページで処理のステータスが状態間を移動するワークロードを確認します。

ボリュームまたはファイルレベルでのファイル共有またはデータストアのリストア

1. リストアするファイル共有またはデータストアを選択したら、[リストア]ページの[リストア対象]で*または[ファイル別]*を選択します。



ページ"]

2. ボリュームのリストで、リストアするボリュームを選択します。
3. ソース:ソースの横にある下向き矢印を選択すると、詳細が表示されます。
   a. データのリストアに使用する復元ポイントを選択します。

> BlueXPのランサムウェア対策は、インシデント発生直前の最新バックアップとして最適なリストアポイントを特定し、「推奨」を表示します。

4. * Destination *：Destinationの横にある下向き矢印を選択すると、詳細が表示されます。
   a. データのリストア先として、元のソースの場所または指定可能な別の場所を選択します。

> 元のファイルまたはディレクトリはリストアされたデータで上書きされますが、新しい名前を指定しないかぎり、元のファイル名とフォルダ名は変わりません。

   b. 作業環境を選択します。
   c. Storage VMを選択します。
   d. 必要に応じて、パスを入力します。

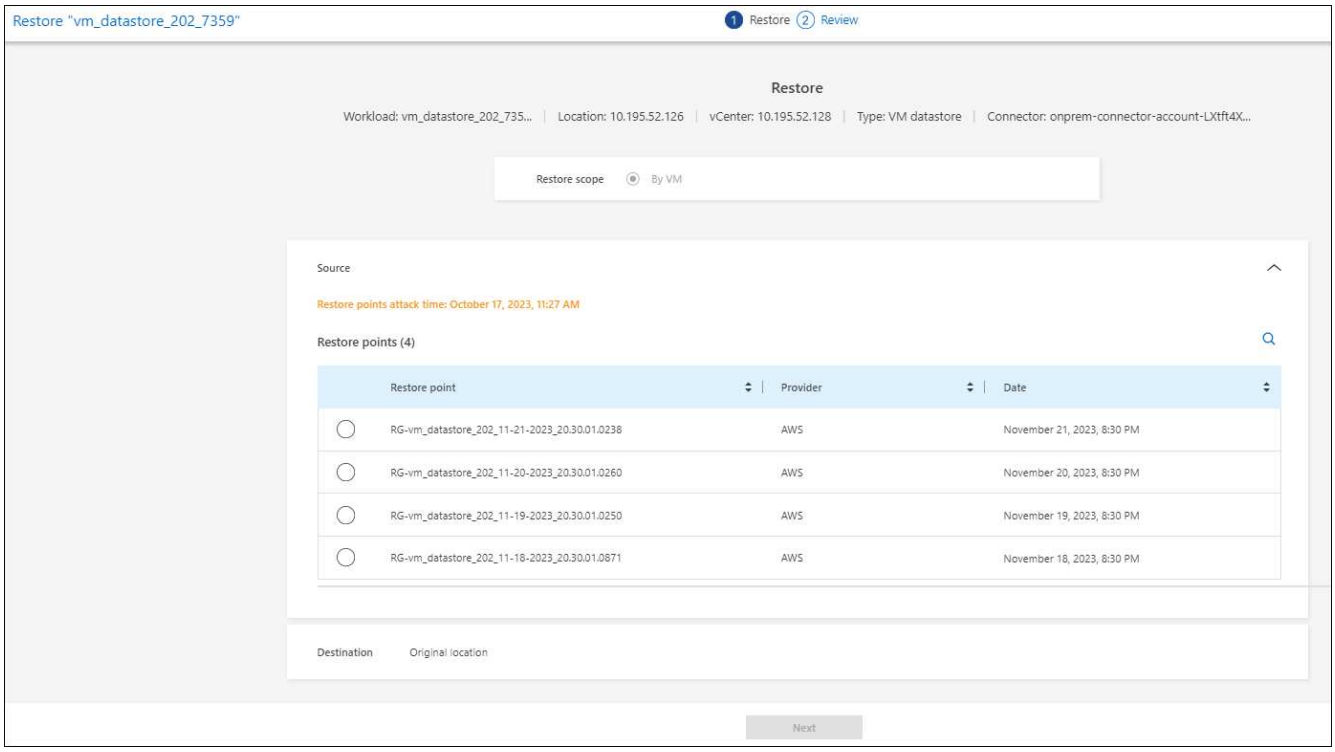
> リストアのパスを指定しない場合、ファイルは最上位のディレクトリにある新しいボリュームにリストアされます。

5. [保存（ Save ）] を選択します。
6. 選択内容を確認します。
7. [* Restore] を選択します。
8. メニューから*[リカバリ]*を選択して、処理のステータスが状態間を移動する[リカバリ]ページでワークロードを確認します。

VMレベルでの**VM**ファイル共有のリストア

リストアするVMを選択したあと、[Recovery]ページで次の手順を実行します。

1. ソース:ソースの横にある下向き矢印を選択すると、詳細が表示されます。



ページ"]

2. データのリストアに使用する復元ポイントを選択します。
3. 目的地：元の場所に移動します。
4. 「 * 次へ * 」を選択します。
5. 選択内容を確認します。
6. [* Restore] を選択します。
7. メニューから*[リカバリ]*を選択して、処理のステータスが状態間を移動する[リカバリ]ページでワークロードを確認します。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。