



ワークロードを保護

BlueXP ransomware protection

NetApp
October 07, 2024

目次

ワークロードを保護.....	1
ランサムウェア戦略でワークロードを保護.....	1

ワークロードを保護

ランサムウェア戦略で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。

- SnapCenterソフトウェアまたはSnapCenter Plug-in for VMware vSphereと連携して、ワークロードと整合性のある保護を実現します。
- ランサムウェア対策戦略を作成または管理します。この戦略には、Snapshot、バックアップ、ランサムウェア対策用に作成するポリシー（*detection policies*）が含まれます。
- ストラテジーをインポートして調整します。
- ファイル共有をグループ化すると、ワークロードを個別に保護するのではなく、簡単に保護できます。
- ランサムウェア対策戦略を削除

*保護にはどのサービスが使用されていますか？*保護ポリシーの管理には次のサービスを使用できます。これらのサービスからの保護情報は、BlueXP ransomware protectionに表示されます。

- ファイル共有、VMファイル共有のBlueXP バックアップとリカバリ
- VMデータストア用のVMware SnapCenter
- OracleおよびMySQL向けSnapCenter

保護ポリシー

変更可能な保護ポリシーに関する情報や保護戦略に含まれるポリシーのタイプを確認すると役立つことがあります。

どの保護ポリシーを変更できますか？

現在のワークロード保護に基づいて保護ポリシーを変更できます。

- * NetAppアプリケーションで保護されていないワークロード*：これらのワークロードは、SnapCenter、SnapCenter Plug-in for VMware vSphere、BlueXP のバックアップとリカバリでは管理されません。このようなワークロードでは、ONTAPやその他の製品の一部としてSnapshotが作成される場合があります。ONTAPのFPolicy保護が設定されている場合は、ONTAPを使用してFPolicyの保護を変更できます。
- * NetAppアプリケーションによる既存の保護が適用されるワークロード*：これらのワークロードには、SnapCenter、SnapCenter for VMware vSphere、またはBlueXP バックアップ/リカバリで管理されるバックアップポリシーまたはSnapshotポリシーが適用されます。
 - SnapCenter、SnapCenter for VMware、またはBlueXP のバックアップとリカバリでSnapshotポリシーやバックアップポリシーを管理している場合は、それらのアプリケーションで引き続き管理されます。BlueXP ランサムウェア対策を使用すると、これらのワークロードにランサムウェア検出ポリシーを適用することもできます。
 - ランサムウェア検出ポリシーがAutonomous Ransomware Protection（ARP）およびONTAPのFPolicyで管理されている場合、それらのワークロードは保護され、引き続きARPおよびFPolicyで管理されます。

ランサムウェア対策戦略で必要なポリシーはどれですか？

ランサムウェア対策戦略では、次のポリシーが必要です。

- ランサムウェア検出ポリシー
- スナップショットポリシー

BlueXP ランサムウェア対策戦略ではバックアップポリシーは必要ありません。

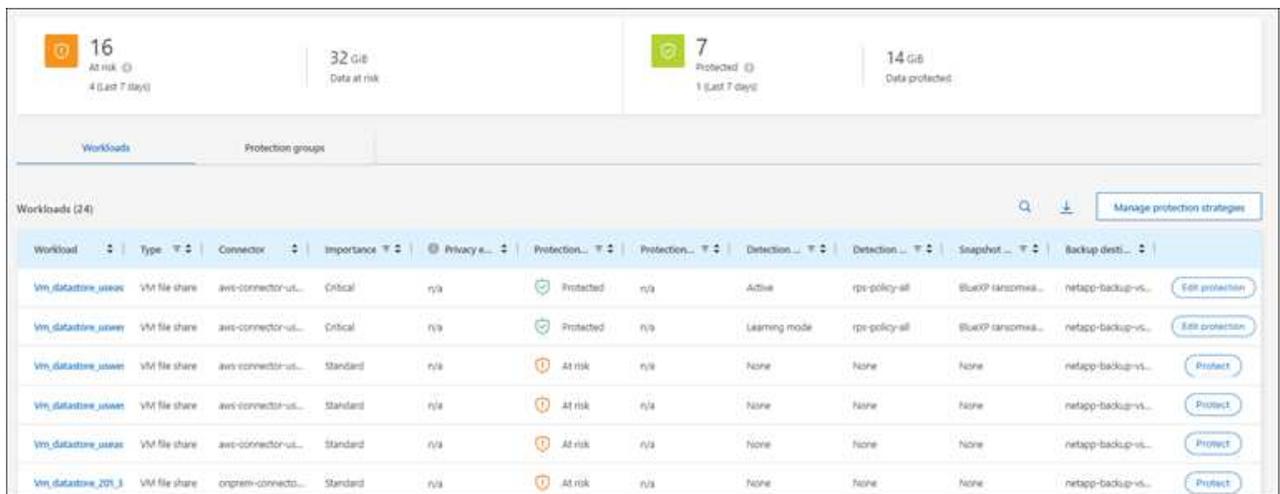
ワークロードに対するランサムウェア対策を表示する

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。

- アプリケーションワークロード
- 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。
 - ダッシュボードの**[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。



The screenshot shows the 'Workloads' page in BlueXP. At the top, there are four summary cards: 'At risk' (16 items, 4 last 7 days), 'Data at risk' (32 GiB), 'Protected' (7 items, 1 last 7 days), and 'Data protected' (14 GiB). Below these is a table with 24 workloads. The table columns include Workload, Type, Connector, Importance, Privacy, Protection, Detection, and Backup destination. The first two rows show 'Protected' status, while the remaining rows show 'At risk' status.

Workload	Type	Connector	Importance	Privacy	Protection	Detection	Snapshot	Backup dest.
Win_datastore_usaes	VM file share	aws-connector-us...	Critical	n/a	Protected	Active	BlueXP ransomwa...	netapp-backup-vs...
Win_datastore_usaes	VM file share	aws-connector-us...	Critical	n/a	Protected	Learning mode	BlueXP ransomwa...	netapp-backup-vs...
Win_datastore_usaes	VM file share	aws-connector-us...	Standard	n/a	At risk	None	None	netapp-backup-vs...
Win_datastore_usaes	VM file share	aws-connector-us...	Standard	n/a	At risk	None	None	netapp-backup-vs...
Win_datastore_usaes	VM file share	aws-connector-us...	Standard	n/a	At risk	None	None	netapp-backup-vs...
Win_datastore_201_3	VM file share	onprem-connecto...	Standard	n/a	At risk	None	None	netapp-backup-vs...

ページ]

3. このページでは、ワークロードの保護の詳細を表示および変更できます。



SnapCenterまたはBlueXPのバックアップおよびリカバリサービスですすでに保護ポリシーが設定されているワークロードについては、保護を編集することはできません。これらのワークロードに対して、BlueXPランサムウェアは自律型ランサムウェア対策やFPolicy保護（他のサービスですすでにアクティブ化されている場合）を有効にします。、およびの詳細については、を参照して "自律的なランサムウェア防御" "BlueXPのバックアップとリカバリ" "ONTAP FPolicy" ください。

[Protection]ページでの保護の詳細

[Protection]ページには、ワークロードの保護に関する次の情報が表示されます。

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。ワークロードに関連するすべてのボリュームでARPが有効になっている。
- リスクあり：ポリシーは適用されません。ワークロードでプライマリ検出ポリシーが有効になっていない場合は、Snapshotポリシーとバックアップポリシーが有効になっていても「リスク」になります。
- 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。

検出ステータス：ワークロードは、次のいずれかのランサムウェア検出ステータスを持つことができます。

- 学習中：最近、ランサムウェア検出ポリシーがワークロードに割り当てられ、サービスがワークロードをスキャンしています。
- * Active *：ランサムウェア検出保護ポリシーが割り当てられています。
- 設定なし：ランサムウェア検出保護ポリシーが割り当てられていません。
- エラー：ランサムウェア検出ポリシーが割り当てられましたが、サービスでエラーが発生しました。



BlueXP ランサムウェア対策で保護を有効にすると、ランサムウェア検出ポリシーのステータスがラーニングモードからアクティブモードに変わった後にアラート検出とレポートが開始されます。

検出ポリシー：ランサムウェア検出ポリシーの名前が割り当てられている場合は、その名前が表示されます。検出ポリシーが割り当てられていない場合は、「N/A」と表示されます。

- Snapshotポリシーとバックアップポリシー*：この列には、ワークロードに適用されているSnapshotポリシーとバックアップポリシー、およびそれらのポリシーを管理している製品またはサービスが表示されません。
- SnapCenterが管理
- SnapCenter Plug-in for VMware vSphereで管理
- BlueXPのバックアップとリカバリで管理
- Snapshotとバックアップを管理するランサムウェア対策ポリシーの名前
- なし

ワークロードの重要性

BlueXPのランサムウェア対策では、各ワークロードの分析に基づいて、検出時に各ワークロードの重要度や優先度を割り当てます。ワークロードの重要度は、次のSnapshot作成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

事前定義された検出ポリシー

次のいずれかのBlueXP ランサムウェア対策事前定義ポリシーを選択でき、ワークロードの重要性に応じて調整できます。

ポリシーレベル	スナップショット	頻度	保持（日数）	Snapshotコピーの数	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
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	30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

SnapCenterでアプリケーションまたはVMと整合性のある保護を実現

アプリケーションまたはVMと整合性のある保護を有効にすると、アプリケーションまたはVMワークロードを一貫した方法で保護し、休止状態と整合性のある状態を実現して、リカバリが必要になった場合のデータ損失を回避できます。

このプロセスでは、BlueXPのバックアップとリカバリを使用して、アプリケーション用のSnapCenterソフトウェアサーバまたはSnapCenter Plug-in for VMware vSphere for VMの登録が開始されます。

ワークロードと整合性のある保護を有効にしたら、BlueXPのランサムウェア対策で保護戦略を管理できます。保護戦略には、他の場所で管理されるSnapshotポリシーとバックアップポリシー、およびBlueXP ランサムウェア対策で管理されるランサムウェア検出ポリシーが含まれます。

BlueXPのバックアップとリカバリを使用してSnapCenterまたはSnapCenter Plug-in for VMware vSphereを登録する方法については、次の情報を参照してください。

- ["SnapCenterサーバソフトウェアの登録"](#)
- ["SnapCenter Plug-in for VMware vSphereの登録"](#)

手順

1. BlueXPのランサムウェア対策メニューから、*[ダッシュボード]*を選択します。
2. [Recommendations]ペインで、次のいずれかの推奨事項を探し、*[Review and fix]*を選択します。
 - 利用可能なSnapCenterサーバをBlueXPに登録
 - 使用可能なSnapCenter Plug-in for VMware vSphere (SCV) をBlueXPに登録
3. 表示された情報に従って、BlueXPのバックアップとリカバリを使用してSnapCenterまたはSnapCenter Plug-in for VMware vSphereホストを登録します。
4. BlueXPランサムウェア対策に戻ります。
5. BlueXPのランサムウェア対策から、ダッシュボードに移動して検出プロセスを再度開始します。
6. BlueXPのランサムウェア対策で、* Protection *を選択してProtectionページを表示します。
7. [Protection]ページの[snapshot policies]列で詳細を確認して、別の場所でポリシーが管理されていることを確認します。

ランサムウェア対策戦略を追加

ワークロードにランサムウェア対策戦略を追加できます。この方法は、Snapshotポリシーとバックアップポリシーがすでに存在するかどうかによって異なります。

- スナップショットポリシーやバックアップポリシーがない場合は、ランサムウェア対策戦略を作成。ワークロードにSnapshotポリシーやバックアップポリシーがない場合は、ランサムウェア対策戦略を作成できます。この戦略には、BlueXP ランサムウェア対策で作成する次のポリシーを含めることができます。
 - スナップショットポリシー
 - バックアップポリシー
 - ランサムウェア検出ポリシー
- *スナップショットポリシーとバックアップポリシー*がすでに設定されているワークロードに対して検出ポリシーを作成します。これらのポリシーは、他のNetApp製品またはサービスで管理されています。検出ポリシーでは、他の製品で管理されているポリシーは変更されません。

ランサムウェア対策戦略を作成する（Snapshotポリシーやバックアップポリシーがない場合）

ワークロードにSnapshotポリシーやバックアップポリシーがない場合は、ランサムウェア対策戦略を作成できます。この戦略には、BlueXP ランサムウェア対策で作成する次のポリシーを含めることができます。

- スナップショットポリシー
- バックアップポリシー
- ランサムウェア検出ポリシー

ランサムウェア対策戦略の策定手順

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。

Workload	Type	Connector	Importance	Privacy	Protection	Detection	Snapshot	Backup dest.
Vm_datastore_juwei	VM file share	aws-connector-us...	Critical	n/a	Protected	Active	BlueXP ransomwa...	netapp-backup-vs...
Vm_datastore_juwei	VM file share	aws-connector-us...	Critical	n/a	Protected	Learning mode	BlueXP ransomwa...	netapp-backup-vs...
Vm_datastore_juwei	VM file share	aws-connector-us...	Standard	n/a	At risk	None	None	netapp-backup-vs...
Vm_datastore_juwei	VM file share	aws-connector-us...	Standard	n/a	At risk	None	None	netapp-backup-vs...
Vm_datastore_juwei	VM file share	aws-connector-us...	Standard	n/a	At risk	None	None	netapp-backup-vs...
Vm_datastore_201_3	VM file share	onprem-connecto...	Standard	n/a	At risk	None	None	netapp-backup-vs...

ページ]

2. [保護]ページで、*[保護戦略の管理]*を選択します。

Ransomware protection strategy	Snapshot policy	Backup policy	Detection policy	Protected workloads
rps-strategy-critical	critical-ss-policy	critical-bu-policy	rps-policy-all	3
rps-strategy-important	important-ss-policy	important-bu-policy	rps-policy-all	1
rps-strategy-standard	standard-ss-policy	standard-bu-policy	rps-policy-all	0

3. [Ransomware protection strategy]ページで、*[Add]*を選択します。

Add ransomware protection strategy

Ransomware protection strategy name:

Copy from existing ransomware protection strategy:

Detection policy:

Snapshot policy:

Backup policy:

セクションを示す[Add strategy]ページ"]

4. 新しいストラテジー名を入力するか、既存の名前を入力してコピーします。既存の名前を入力した場合は、コピーする名前を選択して*コピー*を選択します。



既存のストラテジーをコピーして変更する場合は、元の名前に「_copy」が追加されます。一意にするには、名前と少なくとも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。

◦ 検出ポリシー：

- ポリシー:事前に設計された検出ポリシーのいずれかを選択します。
- 一次検出：ランサムウェアの検出を有効にして、ランサムウェア攻撃の可能性を検出します。
- 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、このサービスは自動スナップショットコピーを作成します。

ブロックされるファイル拡張子を変更する場合は、System Managerで編集します。

◦ * Snapshotポリシー*：

- * Snapshotポリシーのベース名*：ポリシーを選択するか*[作成]*を選択してSnapshotポリシーの名前を入力します。
- * Snapshotロック*：このオプションを有効にすると、プライマリストレージ上のSnapshotコピーがロックされ、ランサムウェア攻撃を受けてバックアップ先にたどり着いた場合でも、一定期間変更や削除ができないようになります。これは_不変ストレージ_とも呼ばれます。これにより、リストア時間が短縮されます。

Snapshotがロックされると、ボリュームの有効期限はSnapshotコピーの有効期限に設定されません。

Snapshotコピーロックは、ONTAP 9.12.1以降で使用できます。SnapLockの詳細については、["ONTAPのSnapLock"](#)。

- * Snapshot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。

◦ バックアップポリシー：

- バックアップポリシーのベース名：新しい名前を入力するか、既存の名前を選択します。
- 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。



セカンダリストレージでバックアップロックを有効にするには、*[設定]*オプションを使用してバックアップ先を設定します。詳細については、を参照してください ["セツテイノセツテイ"](#)。

6. 「* 追加」を選択します。

Snapshotポリシーとバックアップポリシーがすでに設定されているワークロードに検出ポリシーを追加する

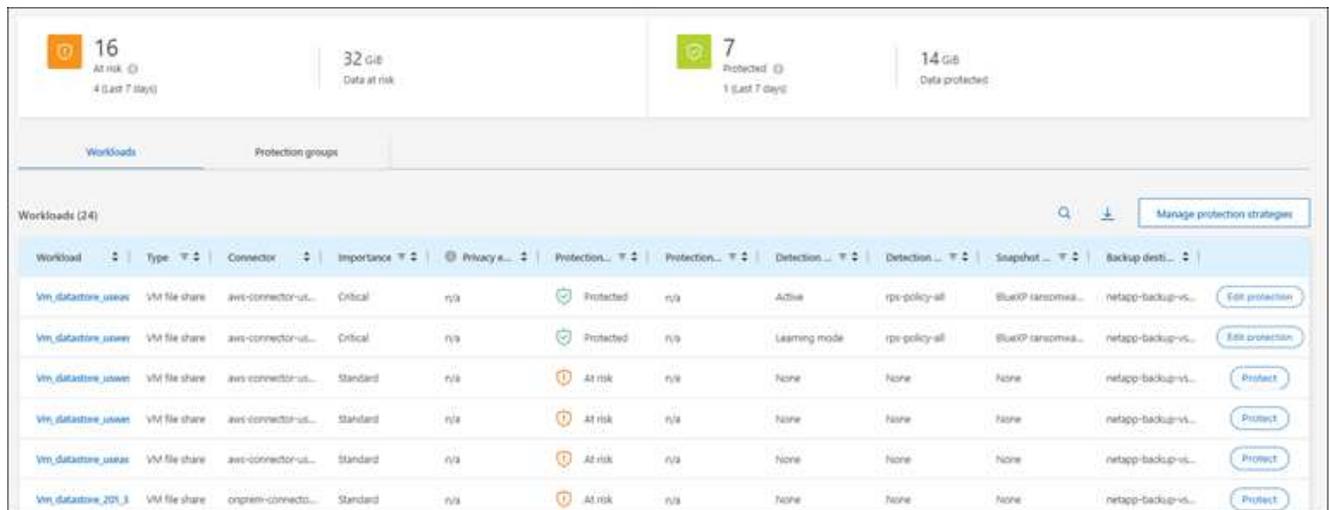
BlueXP ランサムウェア対策では、Snapshotポリシーとバックアップポリシーがすでに設定されているワークロードにランサムウェア検出ポリシーを割り当てることができます。これらのポリシーは、他のNetApp製品やサービスで管理されます。検出ポリシーでは、他の製品で管理されているポリシーは変更されません。

BlueXPのバックアップとリカバリやSnapCenterなどの他のサービスでは、次のタイプのポリシーを使用してワークロードを管理しています。

- スナップショットを管理するポリシー
- セカンダリストレージへのレプリケーションを管理するポリシー
- オブジェクトストレージへのバックアップに関するポリシー

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。



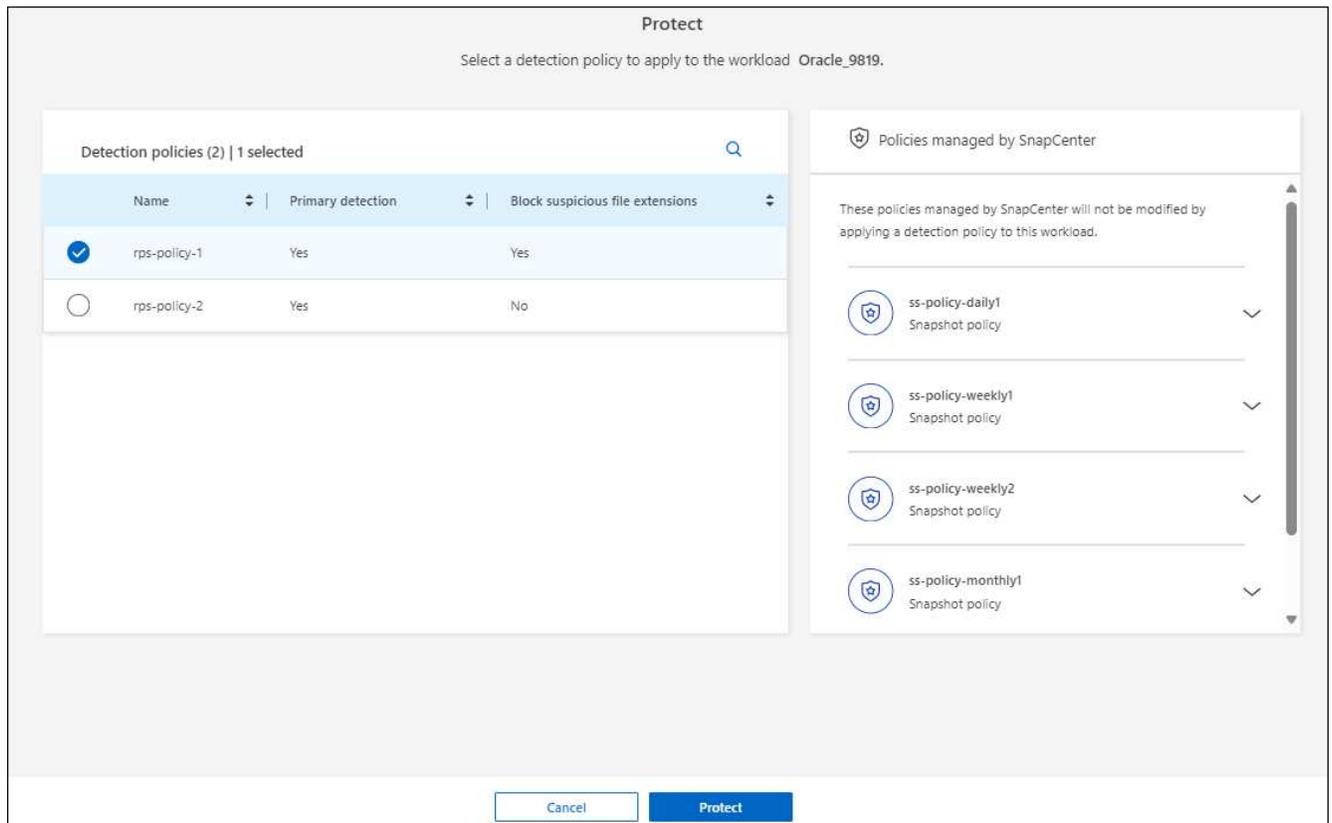
Workload	Type	Connector	Importance	Privacy	Protection	Protection	Detection	Detection	Snapshot	Backup dest.	
Win_datastore_juwei	VM file share	aws-connector-ut...	Critical	n/a	Protected	n/a	Active	rpe-policy-all	BlueXP ransomwa...	netapp-backup-vs...	Edit protection
Win_datastore_juwei	VM file share	aws-connector-ut...	Critical	n/a	Protected	n/a	Learning mode	rpe-policy-all	BlueXP ransomwa...	netapp-backup-vs...	Edit protection
Win_datastore_juwei	VM file share	aws-connector-ut...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_juwei	VM file share	aws-connector-ut...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_201_3	VM file share	ongrem-connecto...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect

ページ]

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。

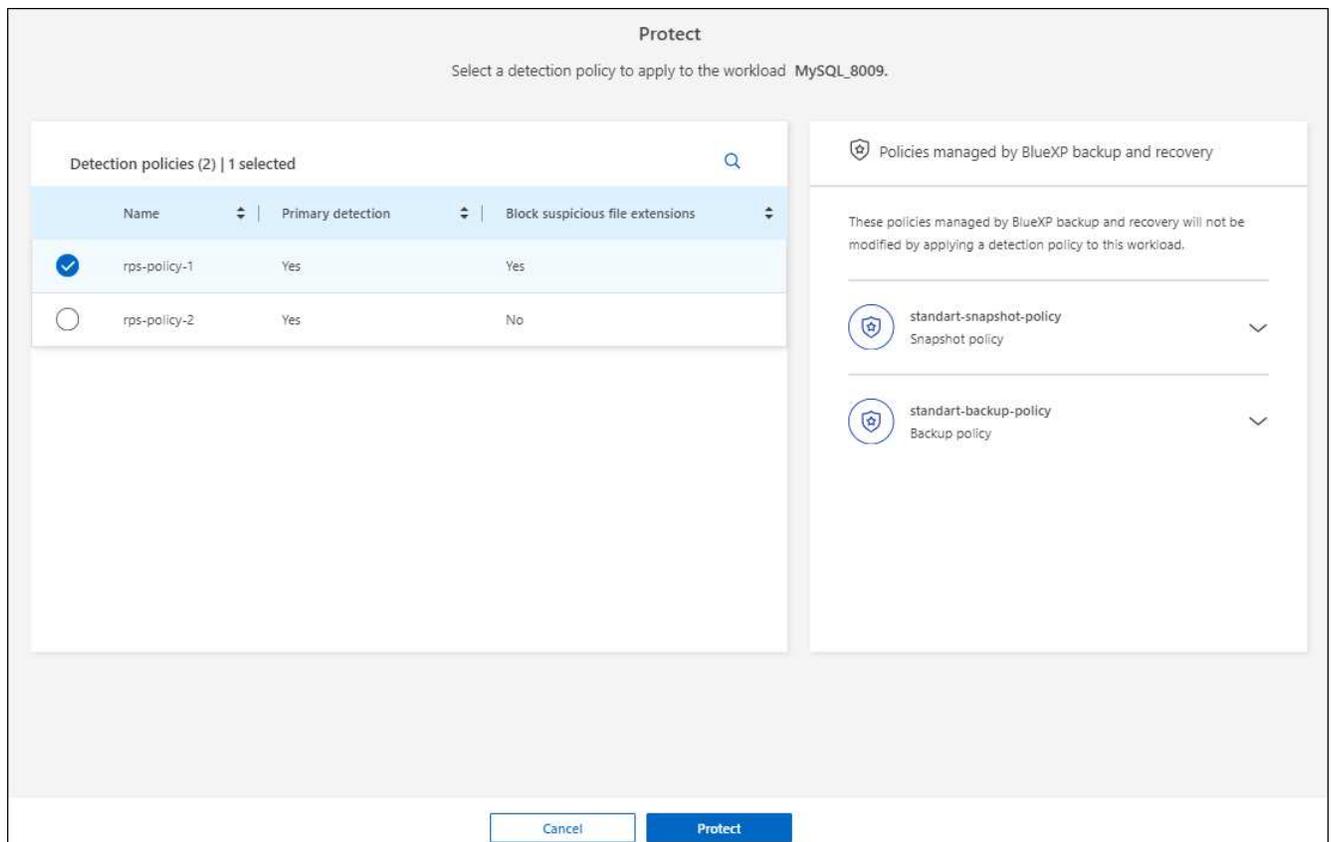
[保護]ページには、SnapCenterソフトウェア、SnapCenter for VMware vSphere、およびBlueXPのバックアップとリカバリで管理されるポリシーが表示されます。

次の例は、SnapCenterで管理されるポリシーを示しています。



ページ]

次の例は、BlueXPのバックアップとリカバリで管理されるポリシーを示しています。



ページ]

3. 他の場所で管理されているポリシーの詳細を表示するには、*下矢印*をクリックします。
4. 他の場所で管理されているスナップショットポリシーとバックアップポリシーに加えて検出ポリシーを適用するには、検出ポリシーを選択します。
5. [保護]*を選択します。
6. [Protection]ページで、[Detection policy]列を確認して、割り当てられた検出ポリシーを確認します。また、スナップショットポリシーとバックアップポリシーの列には、ポリシーを管理している製品またはサービスの名前が表示されます。

別のポリシーを割り当てる

現在の保護ポリシーを置き換える別の保護ポリシーを割り当てることができます。

手順

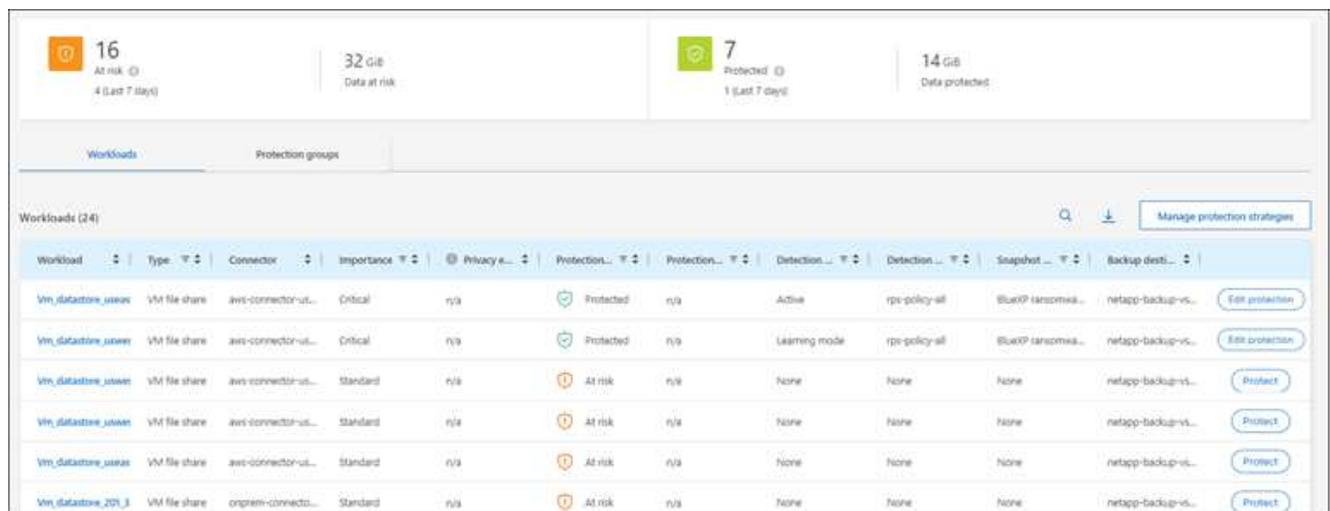
1. BlueXPのランサムウェア対策メニューから、* Protection *を選択します。
2. [保護]ページのワークロードの行で、*[保護の編集]*を選択します。
3. [Policies]ページで、割り当てるポリシーの下矢印をクリックして詳細を確認します。
4. 割り当てるポリシーを選択します。
5. [保護]*を選択して変更を終了します。

グループファイル共有による保護の強化

ファイル共有をグループ化すると、データ資産の保護が容易になります。このサービスでは、各ボリュームを個別に保護するのではなく、グループ内のすべてのボリュームを同時に保護できます。

手順

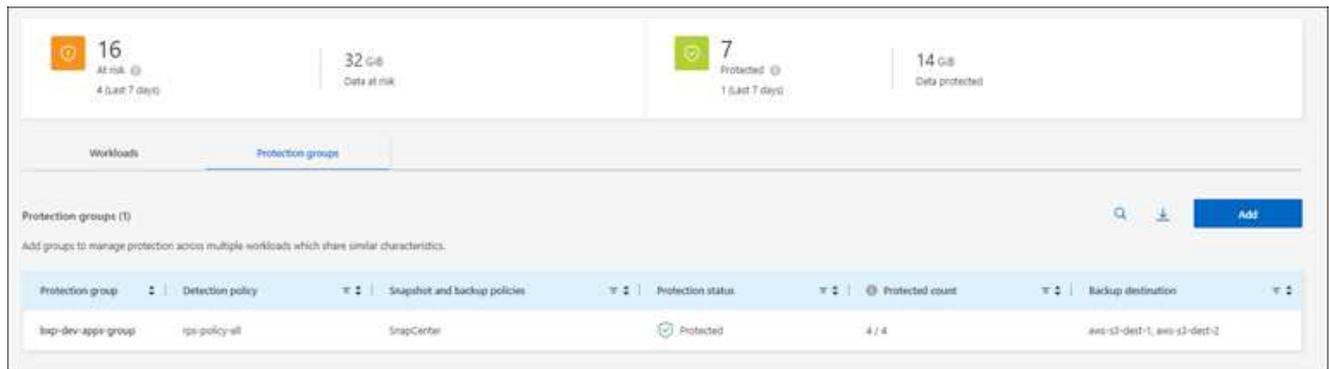
1. BlueXPのランサムウェア対策メニューから、* Protection *を選択します。



Workload	Type	Connector	Importance	Privacy	Protection	Protection	Detection	Detection	Snapshot	Backup desti...	
Win_datastore_00000	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Active	rpe-policy-all	BlueXP ransomwa...	netapp-backup-vs...	Edit protection
Win_datastore_00001	VM file share	aws-connector-us...	Critical	n/a	Protected	n/a	Learning mode	rpe-policy-all	BlueXP ransomwa...	netapp-backup-vs...	Edit protection
Win_datastore_00002	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_00003	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_00004	VM file share	aws-connector-us...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect
Win_datastore_201_3	VM file share	onprem-connecto...	Standard	n/a	At risk	n/a	None	None	None	netapp-backup-vs...	Protect

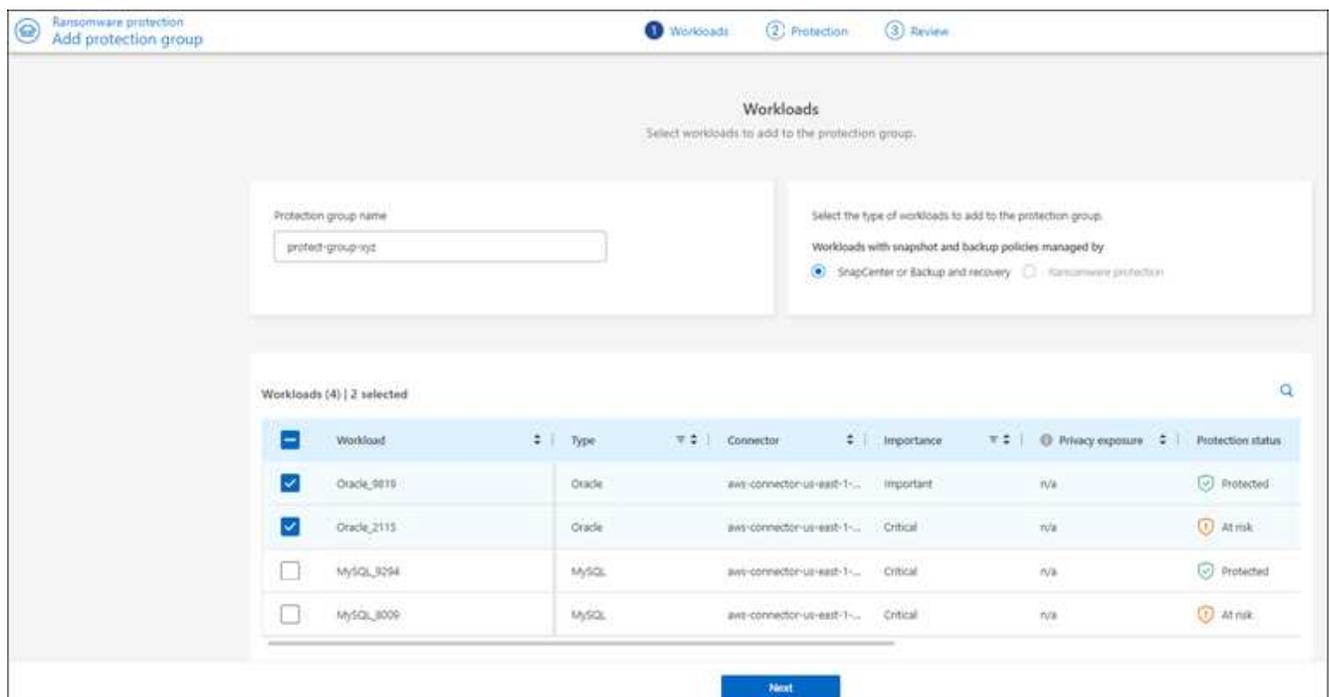
ページ"]

2. [保護]ページで、*[保護グループ]*タブを選択します。



ページ]

3. 「* 追加」を選択します。



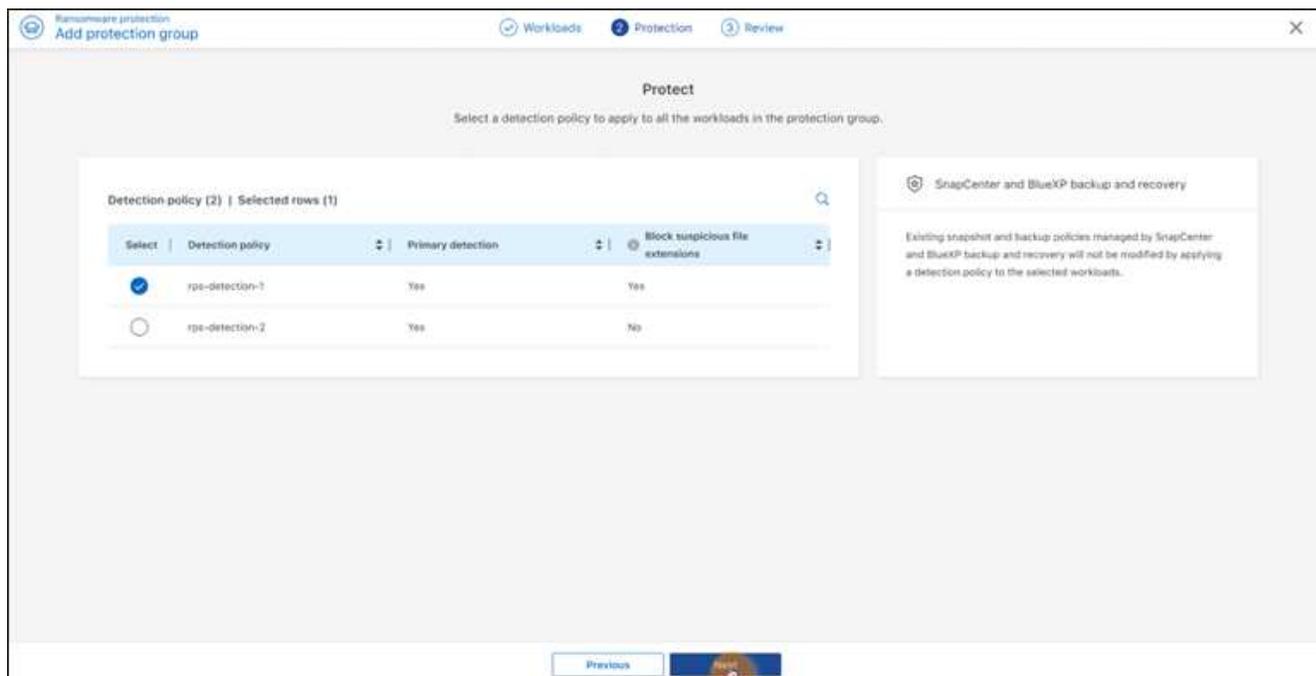
ページ]

4. 保護グループの名前を入力します。
5. 次のいずれかの手順を実行します。
 - a. 保護ポリシーがすでに設定されている場合は、次のいずれかでワークロードが管理されているかどうかに基づいてワークロードをグループ化するかどうかを選択します。
 - BlueXPのランサムウェア対策
 - SnapCenterまたはBlueXP のバックアップとリカバリ
 - b. 保護ポリシーがまだ設定されていない場合は、設定済みのランサムウェア対策戦略がページに表示されます。
 - i. 1つを選択してグループを保護し、*次へ*を選択します。
 - ii. 選択したワークロードに複数の作業環境にボリュームが含まれている場合は、複数の作業環境のバックアップ先を選択してクラウドにバックアップできるようにします。
6. グループに追加するワークロードを選択します。



ワークロードの詳細を確認するには、右にスクロールします。

7. 「* 次へ *」を選択します。



-[Policy]ページ]

8. このグループの保護を制御するポリシーを選択します。
9. 「* 次へ *」を選択します。
10. 保護グループの選択内容を確認します。
11. 「* 追加」を選択します。

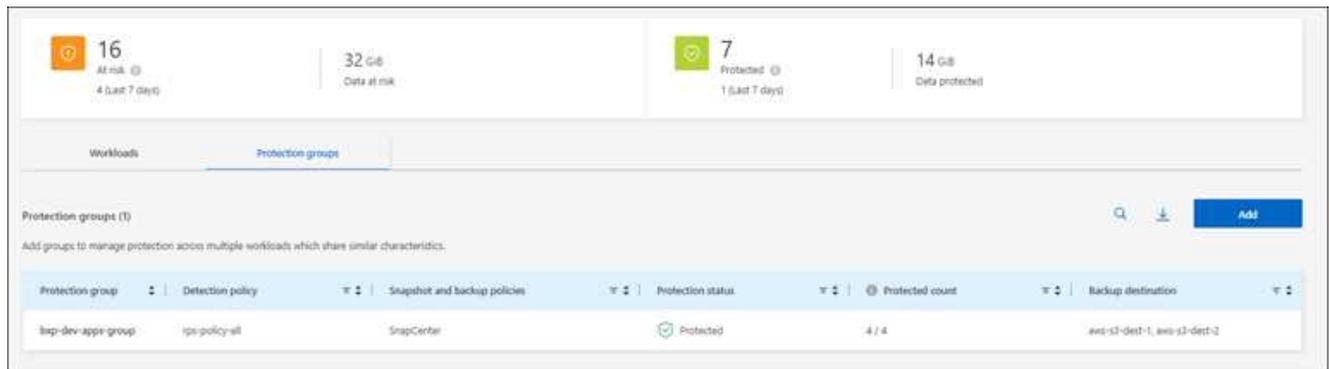
グループにワークロードを追加する

あとで既存のグループにワークロードを追加しなければならない場合があります。

BlueXP ランサムウェア対策のみで管理されるワークロードがグループに含まれている場合（SnapCenter やBlueXP のバックアップとリカバリでは管理されない）、BlueXP ランサムウェア対策のみで管理されるワークロードには別々のグループを使用し、他のサービスで管理されるワークロードには別々のグループを使用する

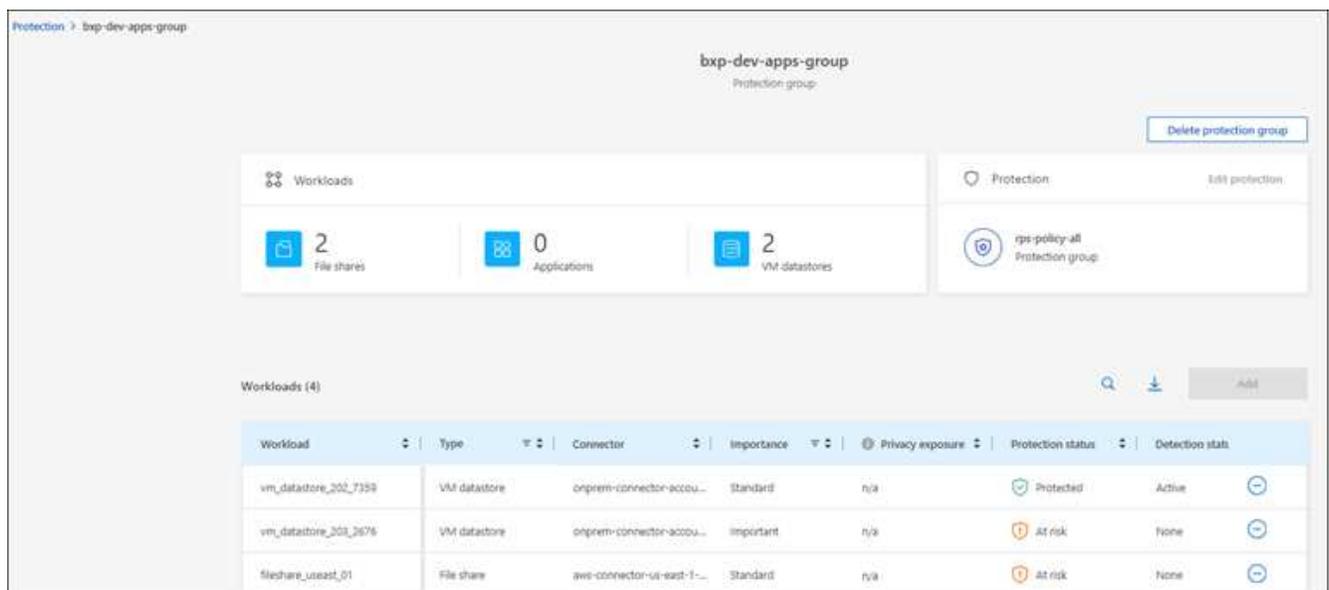
手順

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。
2. [保護]ページで、*[保護グループ]*タブを選択します。



ページ]

- ワークロードを追加するグループを選択します。



ページ]

- [選択した保護グループ]ページで、*[追加]*を選択します。

BlueXP ランサムウェア対策では、グループに含まれていないワークロードのうち、Snapshotポリシーとバックアップポリシーがグループと同じであるワークロードだけが表示されます。



ページの上部には、スナップショット、バックアップ、および検出のポリシーを保持しているサービスが表示されます。

- グループに追加するワークロードを選択します。
- [保存 (Save)]を選択します。

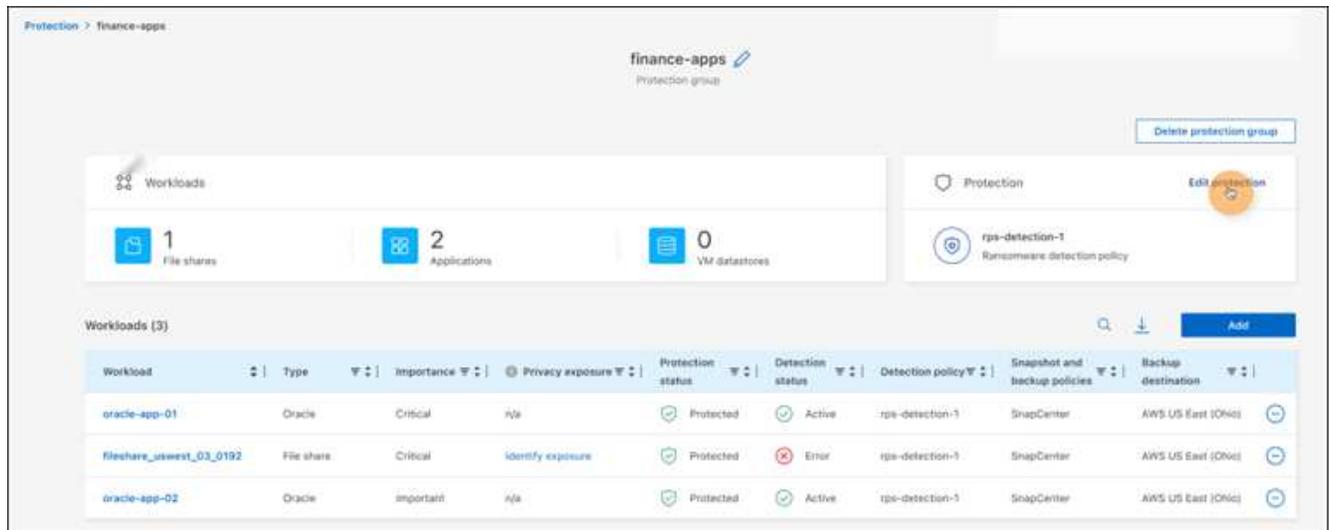
グループ保護の編集

既存のグループの検出ポリシーを変更できます。検出ポリシーがこのグループにまだ追加されていない場合は、ここで追加できます。

手順

- 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、*[保護グループ]*タブを選択します。



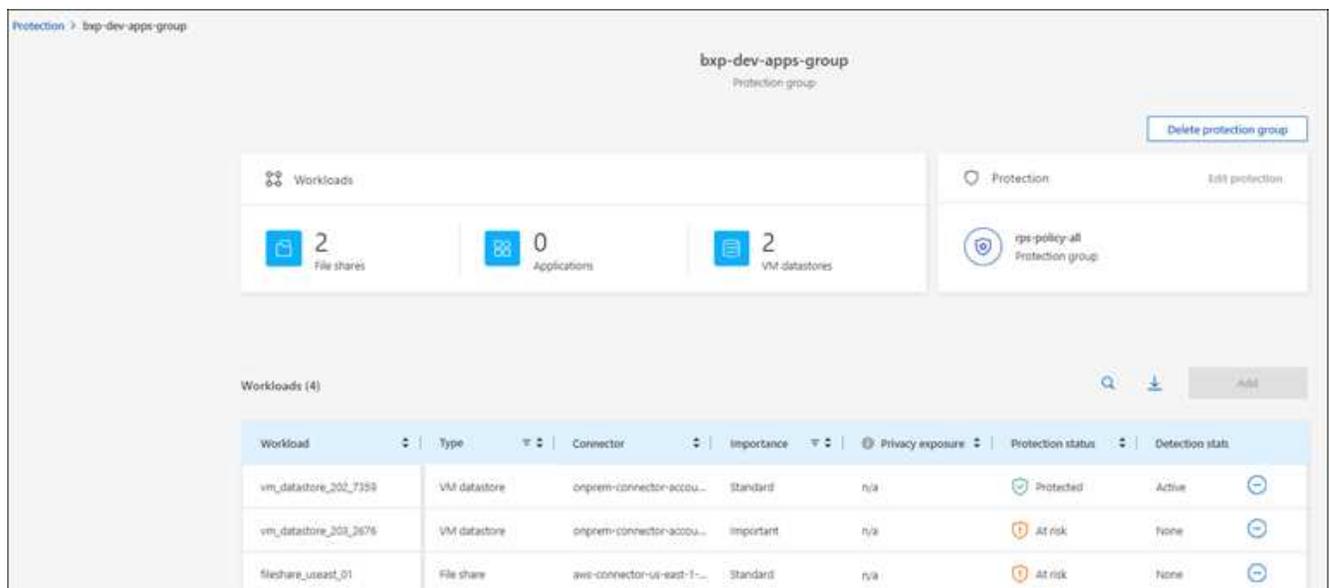
3. [保護]ペインで、*[保護の編集]*を選択します。
4. このグループに検出ポリシーを選択または追加します。

グループからワークロードを削除する

あとで既存のグループからワークロードを削除しなければならない場合があります。

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、*[保護グループ]*タブを選択します。
3. ワークロードを削除するグループを選択します。



ページ"]

4. [選択した保護グループ]ページで、グループから削除するワークロードを選択し、*[アクション]*オプションを選択し...ボタン]ます。

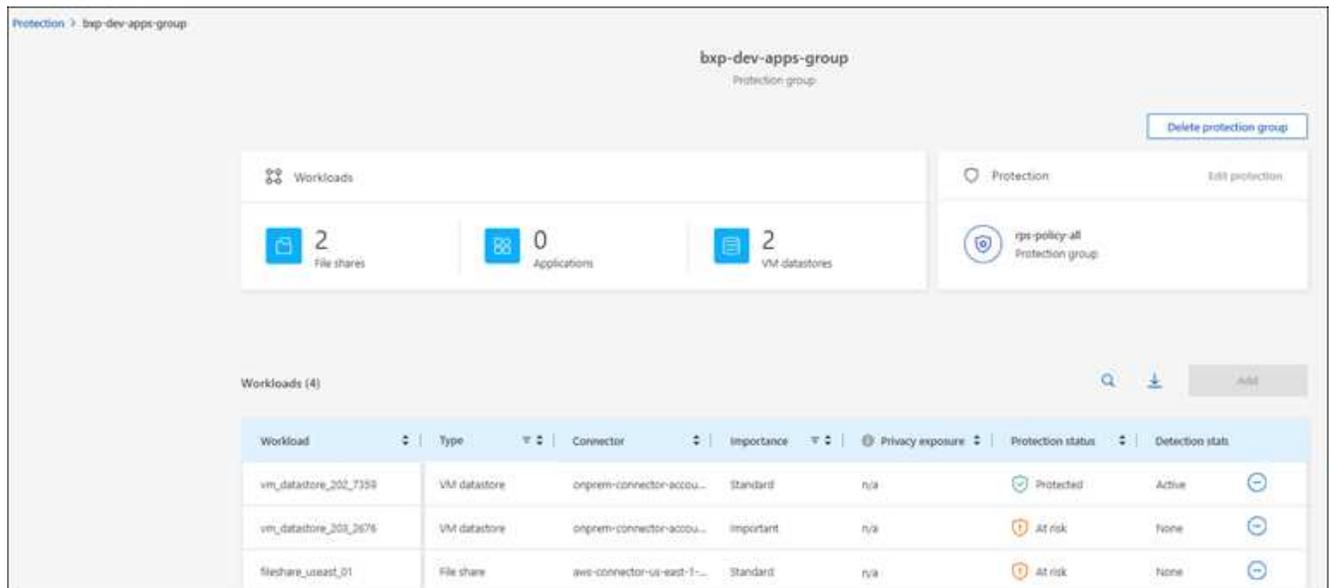
5. [操作]メニューから*[ワークロードの削除]*を選択します。
6. ワークロードを削除することを確認し、*[削除]*を選択します。

保護グループの削除

保護グループを削除すると、グループとその保護は削除されますが、個々のワークロードは削除されません。

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、*[保護グループ]*タブを選択します。
3. ワークロードを削除するグループを選択します。



ページ"]

4. [選択した保護グループ]ページの右上にある*[保護グループの削除]*を選択します。
5. グループを削除することを確認し、*[削除]*を選択します。

ランサムウェア対策戦略の管理

ランサムウェア対策は削除できます。

ランサムウェア対策戦略で保護されているワークロードを表示する

ランサムウェア対策戦略を削除する前に、その戦略で保護されているワークロードを確認することができます。

ワークロードは、戦略のリストから表示するか、特定の戦略を編集するときに表示できます。

ストラテジーのリストを表示する際の手順

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、*[保護戦略の管理]*を選択します。

[Ransomware protection strategy]ページには、戦略のリストが表示されます。

Ransomware protection strategy	Snapshot policy	Backup policy	Detection policy	Protected workloads	
rpi-strategy-critical	critical-si-policy	critical-bu-policy	rpe-policy-all	3	▼ ...
rpi-strategy-important	important-si-policy	important-bu-policy	rpe-policy-all	1	▼ ...
rpi-strategy-standard	standard-si-policy	standard-bu-policy	rpe-policy-all	0	▼ ...
RPS strategy 4	standard-si-policy-344	standard-bu-policy-344	rpe-policy-all	0	▼ ...

3. [Ransomware protection strategy]ページの[Protected workloads]列で、行の最後にある下矢印をクリックします。

ランサムウェア対策戦略を削除

現在どのワークロードにも関連付けられていない保護戦略を削除できます。

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、*[保護戦略の管理]*を選択します。
3. [ストラテジーの管理]ページで、削除するストラテジーの*[アクション]*オプションを選択し ...ボタン]ます。
4. [操作]メニューから*[ポリシーの削除]*を選択します。

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权を有し、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权については、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。