

# **Cyber Recovery Solution**

## **簡易運用ガイド**

**(PPDM 編)**

---

## 目次

はじめに.....	3
1. ポリシー作成 .....	5
2. ステータス確認(正常系).....	10
3. ステータス確認(Suspection データ検出時) .....	13
4. 攻撃ファイルの特定.....	17
5. データの復旧 .....	20
6. コピーの破棄 .....	24

## はじめに

昨今、ランサムウェアやシステムの脆弱性を利用したサイバー攻撃が増えており、それらへの対策はシステムの可用性を検討する上で欠かすことのできない観点となりつつあります。

Dell Technologies においても、お客様のビジネスを継続する上で必要なデータを保護、サイバー攻撃からシステムを迅速に復旧するためのプロダクトとして、“Cyber Recovery Solution”を提供しております。

今回は、その“Cyber Recovery Solution”について、構築後にどのような運用が必要になるのか、実際にサイバー攻撃が発生した場合に保護しているデータをどのように活用するのか、といった観点について、ご説明をさせていただきます。

## 前提条件

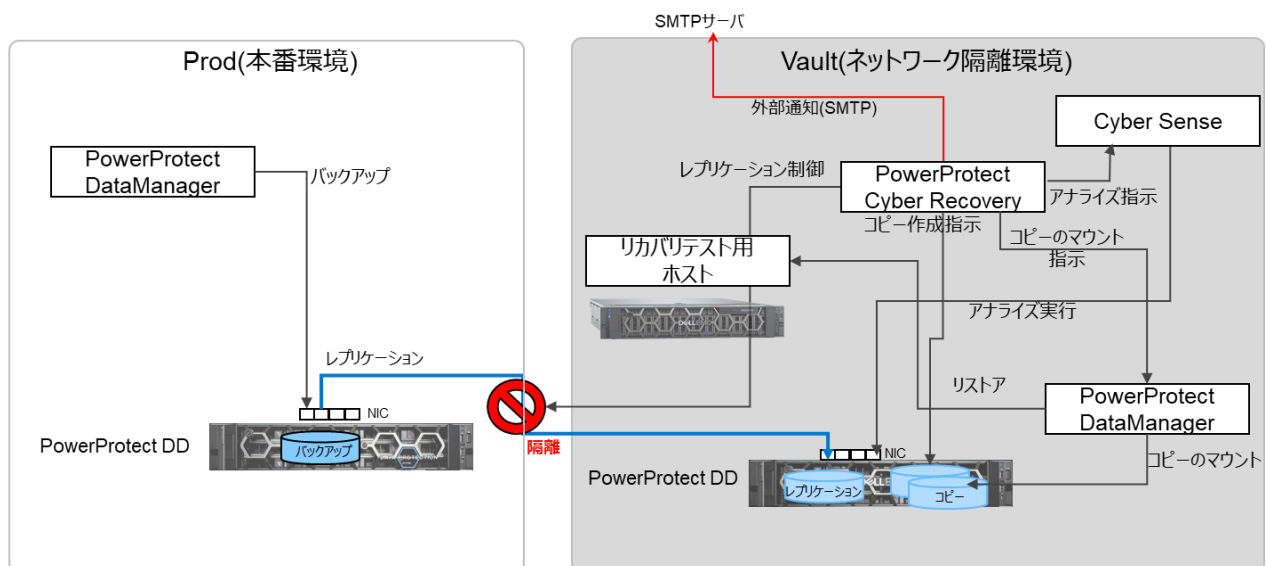
本ガイドは、PowerProtect Cyber Recovery および PowerProtectDataManager 構築後の運用手順を簡略化して説明することを目的としています。各コンポーネントの初期構築および詳細な設定項目については、別途サポートサイトのマニュアルをご参照ください。

本ガイドは PowerProtect Cyber Recovery 19.11、PowerProtectDataManager 19.11、CyberSense 7.12 の環境をベースとしたものとなります。ご利用される環境と異なる場合は適宜読み替えていただくか、マニュアルをご参照ください。

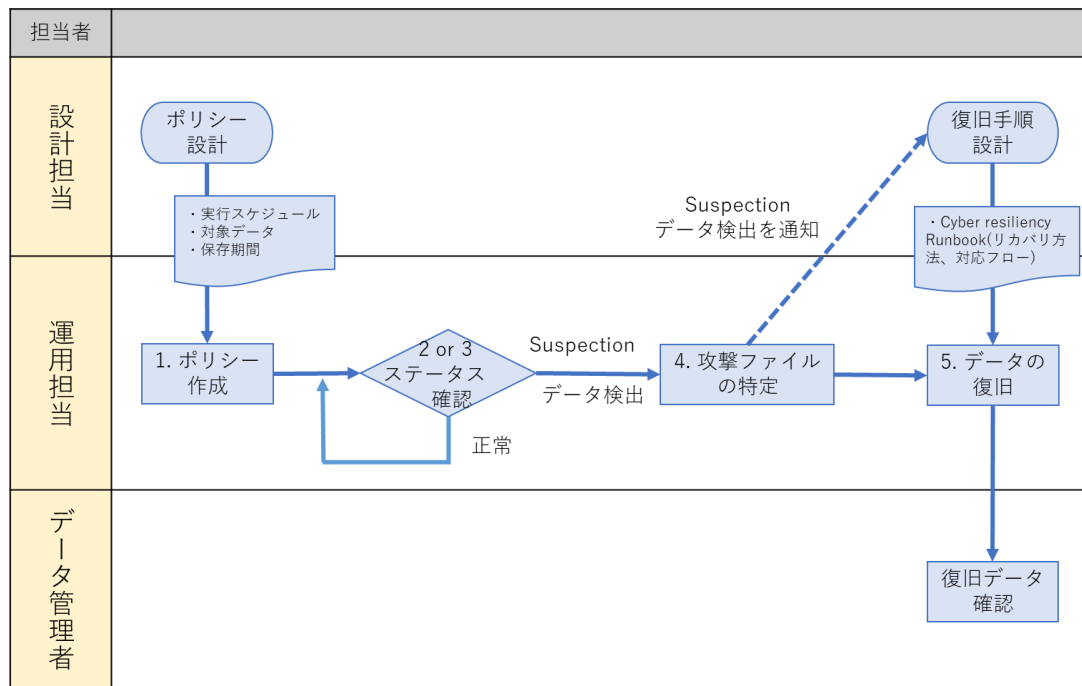
## 環境

このガイドでは、以下の環境およびフローでの運用を想定しています。

環境：



運用フロー：



- ・本ガイド 1、設計担当により特定された Vault 環境で保管すべきデータをコピーするスケジュールと保存期間をポリシー設定。
- ・本ガイド 2 もしくは 3、Vault 環境の PowerProtectDD 上のデータを対象に PowerProtectCyberRecovery がコピーの作成、データのアナライズがスケジュール実行されているか、疑わしいデータの検出状況を確認。
- ・本ガイド 4、CyberSense を利用して攻撃されたファイルを特定し、関連部門へ通知。
- ・本ガイド 5、事前に定義された CyberRecovery の Runbook、発生ケースによる対応方針に従って、リカバリテスト用ホストにデータを復元、データ管理者がチェックを実施。

事前準備

PowerProtectDataManager(PPDM)より、必要なデータのバックアップポリシーを作成しておきます。  
PowerProtectDD より、レプリケーションポリシーを作成しておきます。

## 1. ポリシー作成

本項では Prod(本番環境)の PowerProtectDD に格納されているバックアップデータを Vault(ネットワーク隔離環境)の PowerProtectDD へセキュアコピー※1 および、コピーされたデータに対して改ざんや暗号化等の不正操作の有無をアナライズするためのスケジュールポリシーの作成を実施します。

スケジュールポリシーの作成は、データ管理者によって特定された隔離対象データを新たに加える場合に行います。

※1 レプリケーション、PIT コピーの作成、コピーロックすることでデータ削除を予防する操作をまとめたものです。

- 1 ブラウザを起動し、PowerProtect CyberRecovery にアクセスします。

“管理者”アカウント、パスワードを入力し、**Log in** をクリックします。

※ブラウザの言語は English を選択しておきます。



User Name:

Password:

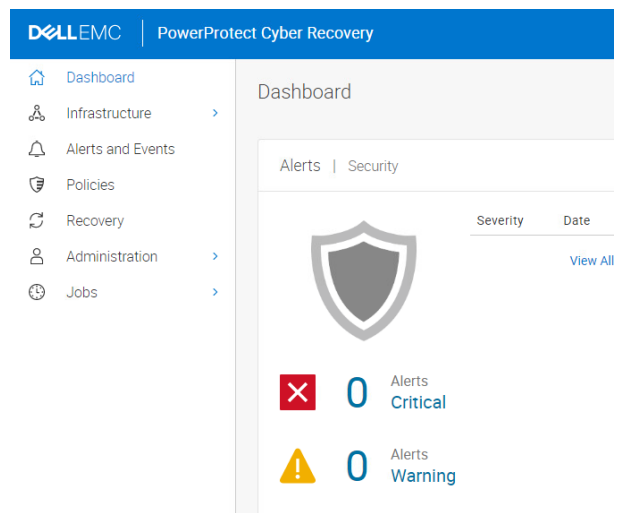
Log In

User Name:

Password:

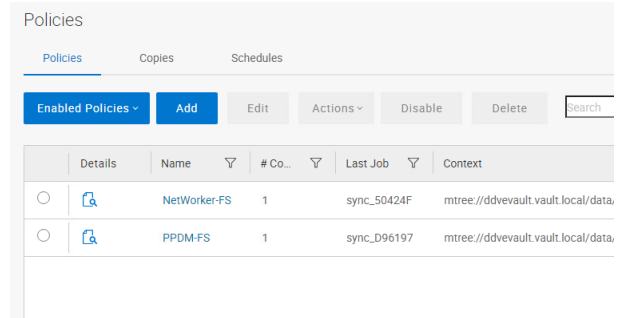
Log In

2 左側のペインから、**Policies** をクリックします。



3 **Add** をクリックし、セキュアコピーの対象とするバックアップポリシーとレプリケーションコンテキストを指定していきます。

※あらかじめ、バックアップポリシーとレプリケーションコンテキストは PPDM と PowerProtectDD 側で定義を行っておく必要があります。



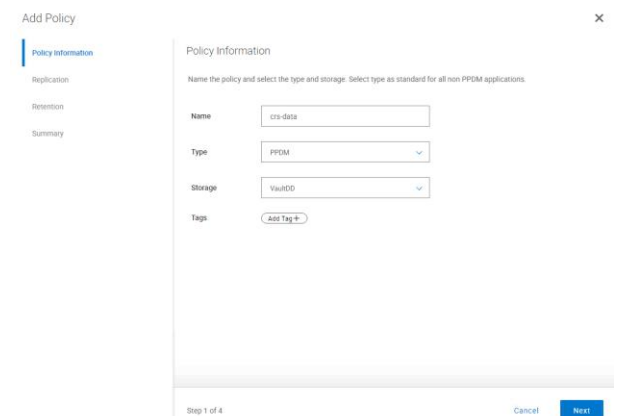
4 Policy Information を指定し、**Next** をクリックします。

Name : ポリシー名を指定します。

Type : 利用しているバックアップソフト(PPDM)を選択します。

Avamar、Networker を利用されている場合は Standard を指定します。

Storage : Vault の PowerProtectDD を選択します。



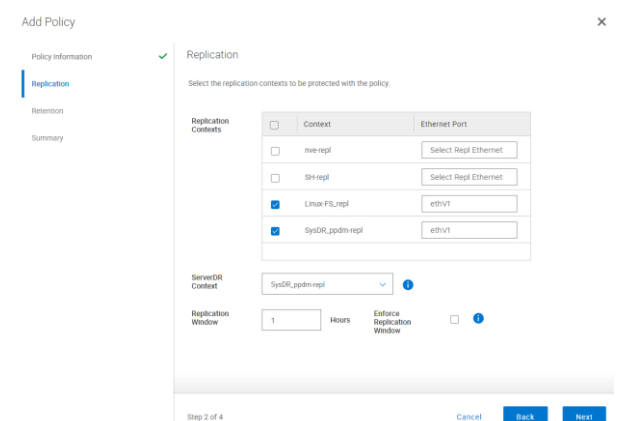
5 レプリケーションコンテキストとレプリケーションウィンドウを指定し、**Next** をクリックします。

Replication Contexts : 隔離対象のデータが含まれたレプリケーションコンテキストと PPDM の DR が含まれたレプリケーションコンテキストの 2 つ以上のコンテキストを指定します。

Ethernet Port は Prod と Vault 間の通信に利用する Vault 側の PowerProtectDD の NIC を指定します。

ServerDR Context : PPDM の DR バックアップが含まれたレプリケーションコンテキストを指定します。

Replication Window : レプリケーションの実行時間を指定



します。

Enforce Replication Window にチェックを入れることでレプリケーションウィンドウ経過後はレプリケーション中であってもセッションを切断します。

- 6 隔離データに対するロックの設定を指定し、**Next** をクリックします。

Retention Lock Type : Governance を選択します。

Enable Auto Retention Lock をチェックすることでデータに対する編集が自動的に制限されます。

Retention Lock Minimum : PIT コピーに指定できる最小値を指定します。(12 Hours ~)

Retention Lock Maximum : PIT コピーに指定できる最大値を指定します。(～1827 Days)

Retention Lock Duration : デフォルトのロック期間を指定します。

Step 3 of 4

- 7 確認し、**Finish** をクリックします。

これで隔離対象とするデータの指定が完了です。

Step 4 of 4

- 8 次にセキュアコピーの実行スケジュールを指定します。**Policies** より、**Schedules** を選択し、**Add** をクリックします。

※運用手順簡素化のため、必要なアクションを 1 スケジュールポリシーで行うものとしていますが、特定のアクションのみに絞って行う、スケジュールポリシーを定義せずにオンデマンドで行うことも可能です。

There are no schedules available

- 9 Schedule Information にて、隔離対象のデータが含まれたポリシーとスケジュール実行するアクションを指定し、**Next** をクリックします。

Schedule Name : スケジュールポリシー名を指定します。  
 Policy : 隔離対象としたいデータが含まれたポリシーを指定します。  
 Action : Secure Copy Analyze を選択します。  
 Secure Copy Analyze を選択した場合、Vault に対するレプリケーション、レプリケーションしたデータのコピー作成、コピーのロック、コピーを対象にデータ分析のアクションが行われます。  
 Retention Lock Duration : コピーの編集を制限する期間を指定します。  
 Application Host : Analyze を実行する CyberSense を指定します。

- 10 Scheduling にて、実行時間を指定し、**Next** をクリックします。

Frequency : 実行間隔を指定します。  
 Next Run Date : このスケジュールでポリシーの実行を開始する日時を選択します。

- 11 Analyze Options にて、対象データの形式を指定します。

Content Format : Backup を選択します。  
 NFS や CIFS によって、PowerProtectDD 上に書き込まれたデータをアナライズの対象とする場合は Filesystem ないしは Databases を選択します。  
 Storage Data Interface : CyberSense がアナライズのため、接続する PowerProtectDD の NIC を指定します。



12 確認し、**Finish**をクリックします。

Summary

Schedule Information

Schedule Name crs-schedule

Policy crs-data

Action securecopyanalyze

Retention Lock Duration 12 hours

Application Host CyberSense

Scheduling

Frequency 0 Days 12 Hours

Next Run Date Aug 17, 2022 3:00 AM UTC

Analyze Options

Content Format Backup

Storage Data Interface ethV0

Files/Directories to Include

Files/Directories to Exclude

Step 4 of 4 Cancel Back Finish

13 これでスケジュールポリシーの作成が完了です。  
定義したスケジュールに従って、データの管理が実行されていきます。

Policies

Enabled Schedules - Add Edit Disable Delete Search

Details	Name	Policy Name	Action Details	Frequency	Next Run
	crs-schedule	crs-data	securecopyanalyze	12 Hours	Aug 17, 2022 3:00 AM UTC

## 2. ステータス確認(正常系)

本項では、データの隔離状況の確認、分析結果の確認を実施します。

ステータス確認は日常的に行うオペレーションとなります。日常的に確認する観点をご説明させていただくことを目的としております。

アラートやステータスの出力は様々な要因により変わります。異常と感じられた場合は弊社サポートサービスにご相談ください。

- 1 ブラウザを起動し、PowerProtect CyberRecovery にアクセスします。  
“管理者”アカウント、パスワードを入力し、**Log in** をクリックします。



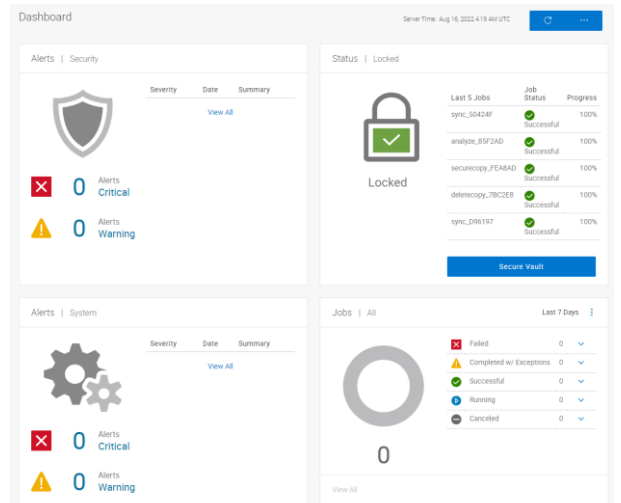
User Name:

Password:

User Name:

Password:

- 2 ダッシュボードから PowerProtectCyberRecovery のステータスを確認します。



- 3 左上の Alert | Security のタイトルでは、Vault 環境におけるエラーアクティビティが表示されます。新規に出力されたものがないことを確認します。

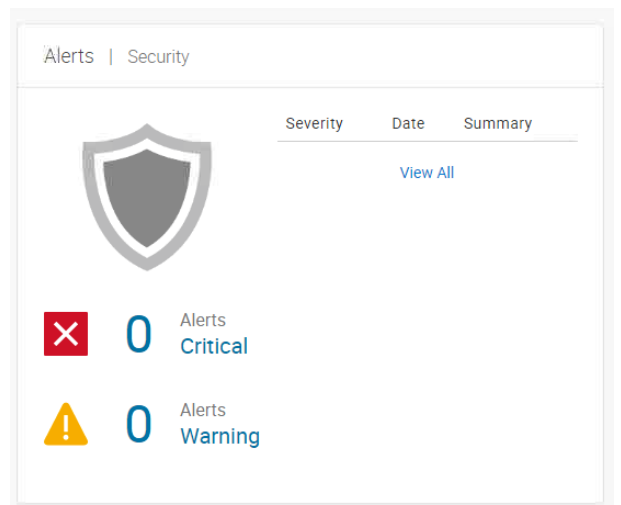
CyberSense によるデータ分析において、疑わしいデータが検出された場合 Alerts | Security にアラートが出力されています。”ステータス確認(Suspection データ検出時)”の手順に移ります。

Ex) Severity : Critical

Date : mm/dd/yyyy

Summary: Suspicious Point-in-time Copy.

**View All** をクリックすることで確認済みの過去のエラーアクティビティを確認できます。



- 4 右上の Status | Locked のタイトルでは、Vault の PowerProtectDD のステータスを確認します。

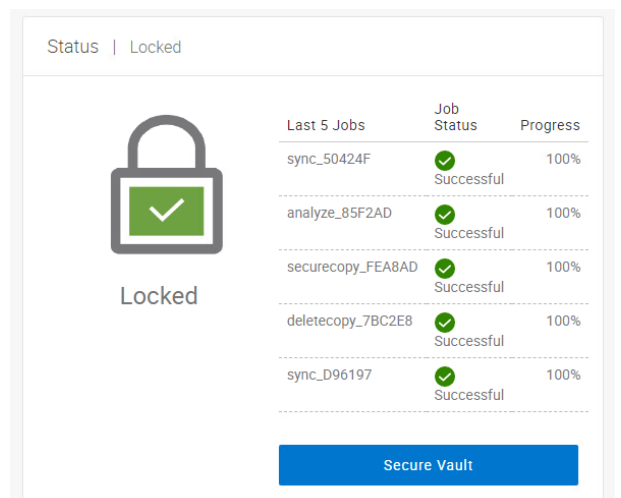
スケジュールポリシーの実行中を除き、“Locked”となっていることを確認します。

スケジュールポリシーの実行状況は左下ペインにて確認します。

各ステータス内容は以下となります。



: (Locked) レプリケーション接続が閉じられた状態です。





: (Unlocked) レプリケーション中のため、1 つ以上のレプリケーション ネットワーク接続が開かれています。



: (Secured) セキュリティ担当者または管理者が手動で接続をロックし、保護した状態です。



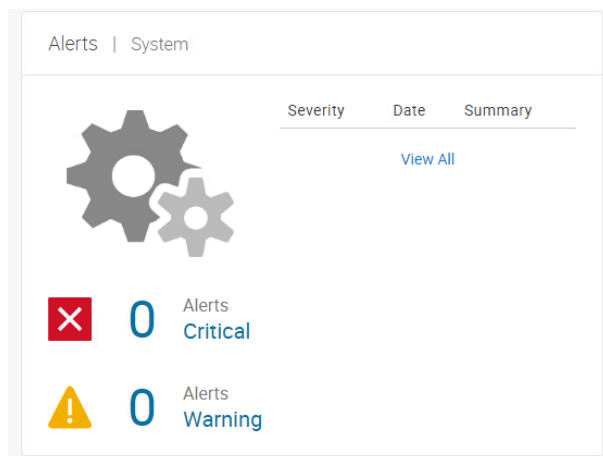
: (Degraded) 複数の PowerProtectDD のいずれかと通信できない場合。Alerts | system で通信ができない PowerProtectDD を特定します。



: (Unknown) すべての PowerProtectDD との接続ができない状態です。

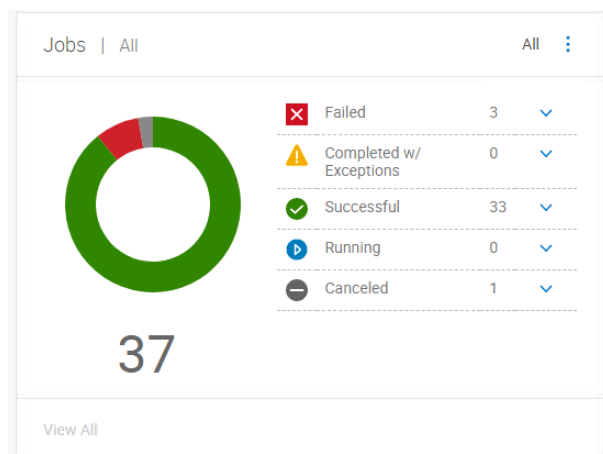
- 5 左下の Alerts | system のタイルでは、Vault 環境におけるシステムイベントが表示されます。新規に出力されたものがないことを確認します。

**View All** をクリックすることで確認済みの過去のエラーアクティビティを確認できます。



- 6 右下の Jobs ペインでは、スケジュールポリシーを含むジョブの実行状況を確認します。

Running 中のジョブが存在する、右上ペインの Status が unlocked になっている場合は を展開し、Protection をクリックし、レプリケーション(Sync)が実行中であるかを確認します。



- 7 Dashboard を確認し、アラート、ステータス、ジョブに対して、新しいアラートや想定していないステータス、前回確認時からの新しいジョブの Fail 等が無ければ、ステータスの確認は完了です。

### 3. ステータス確認(Suspection データ検出時)

前項では日常的なステータス確認をご説明させていただきましたが、本項では、CyberSense によるデータ分析において、データ改ざんが行われたと可能性の高いデータが検出された場合の対応をご説明します。

- 1 ブラウザを起動し、PowerProtect CyberRecovery にアクセスします。  
“管理者”アカウント、パスワードを入力し、**Log in** をクリックします。



User Name:

Password:

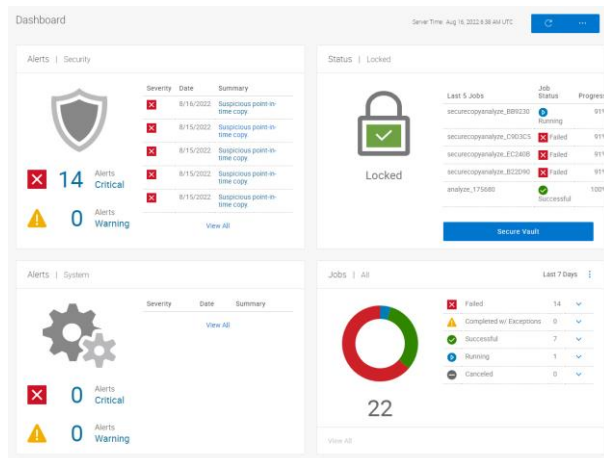
Log In

User Name:

Password:

Log In

- 2 Dashboard を確認します。



- 3 CyberSense によるデータ分析において、疑わしいデータが検出された場合 Alerts | Security にアラートが出力されます。

Ex) Severity : Critical

Date : mm/dd/yyyy

Summary: Suspicious Point-in-time Copy.

**Summary** をクリックします。

Severity	Date	Summary
Critical	8/16/2022	Suspicious point-in-time copy.
Critical	8/15/2022	Suspicious point-in-time copy.
Critical	8/15/2022	Suspicious point-in-time copy.
Critical	8/15/2022	Suspicious point-in-time copy.
Critical	8/15/2022	Suspicious point-in-time copy.

- 4 対象のアラートに絞って抽出されます。

をクリックし、詳細を確認します。

**Additional Details** に疑わしいデータが検出された PIT コピー名が記載されていますので、控えます。

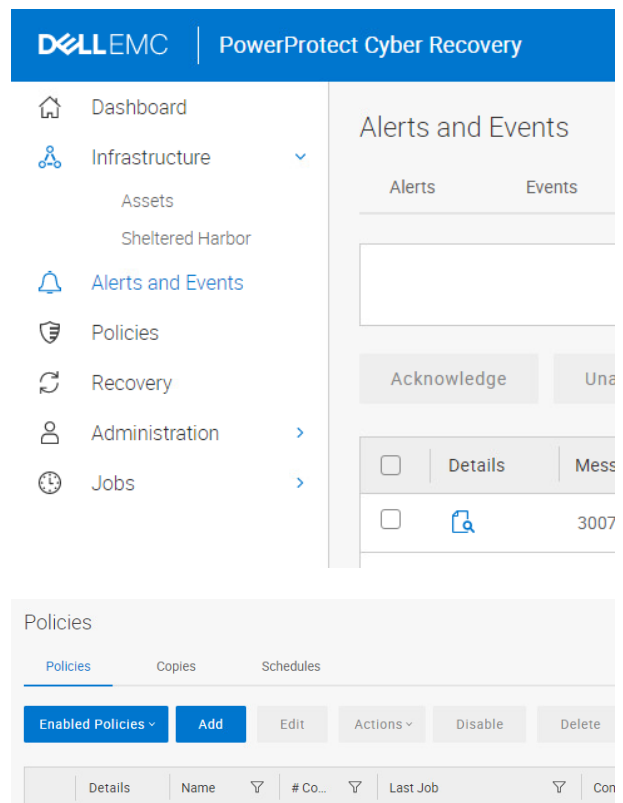
Ex) cr-copy-PPDM-FS-20220816000834

Details	Msg.	Sev.	Date	Summary	Cat.	Serv.	Acti.	Job ID
	3007	Critical	Aug 16, 2022 12:40 A.	Suspicious point-in-time	security	apps		62fae0094422f0001c92b01

### Details

Message ID	3007
Type	Alert
Category	security
Severity	Critical
Summary	Suspicious point-in-time copy.
Description	The application that performed the analysis reported a suspicious point-in-time copy.
Remedy	Investigate possible irregular activity.
Job ID	<a href="#">62fade0094422f0001c92b01</a>
Post To	SMTP
Created By	cradmin
Date	Aug 16, 2022 12:40 AM UTC
Alert ID	62fae792f37bd2000140511f
Notes	
Additional Details	Request: analyze Analysis Status: Suspicious CR copy: cr-copy-PPDM-FS-20220816000834 Job status detail: Completed LAN indexing job. No files to index. An infection was previously reported. <a href="#">... less</a>

5 **Policies** をクリックし、Copies を選びます。



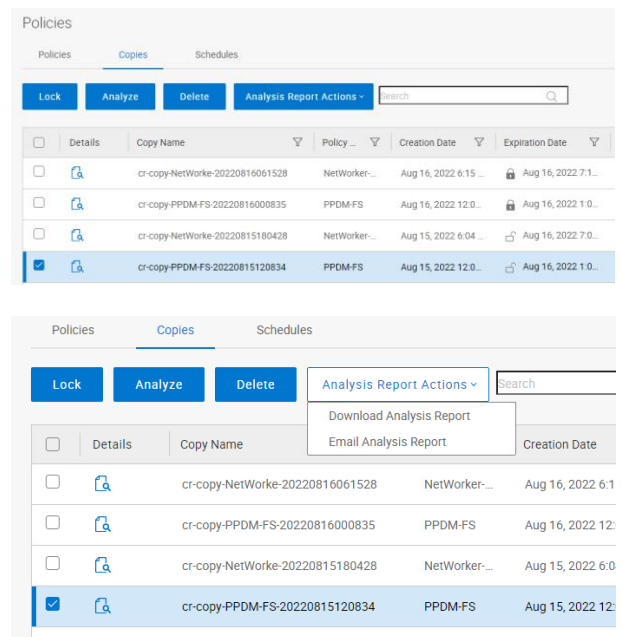
6 Alerts and Events で控えた PIT コピー名を参照し、同じ Copy Name を選択、**Analysis Report Actions** をクリックします。

**Download Analysis Report** をクリックし、分析結果のレポートファイル(csv 形式)をダウンロードします。

※SMTP サーバ設置環境では同様のファイルが以下の subject のメールに添付されています。

Ex)yyyy-mm-dd:Cybersense Report – Policy ID ; Infection Alert!

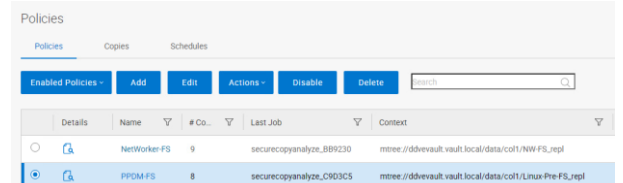
選択したコピーの元となった Policy Name を控えます。



7 **Policies** をクリックします。

控えた Policy Name を参照し、Context に含まれるバックアップデータを確認します。

※Context から PowerProtectDataManager において、バックアップ対象としていたクライアント、ファイル等を特定することを目的としていますが、不明であれば、そのまま進めてください。



8 ダウンロードしたレポートファイルを参照します。

Alert 列に数字(攻撃パターン)が入っているものが、データが改ざんされた可能性が高いものです。

ALERT	CR Job ID	CR Policy Name	Backup Server	Backupset ID	I
●	9	62862ac194422...	84e195a6d1884...	84e195a6d1884...	,
●	9	62862ac194422...	41a9c37e8ceb1...	00000006-f0b3...	,
●	9	62862ac194422...	41a9c37e8ceb1...	00000006-efb3...	,
●6	9	62862ac194422...	a17593c90e5b...	00000006-f2b3...	,
●	9	62862ac194422...	41a9c37e8ceb1...	00000006-eeb3...	,

比較的検出されるケースの多い攻撃パターンの例は下記になります。

- 1 - ファイル名/拡張子の変更を伴わない強力な暗号化
- 4 - ランサムウェア拡張子ありの強力な暗号化
- 6 - 難読化されたファイル拡張子による強力な暗号化
- 14 - データベースページの破損



## 4. 攻撃ファイルの特定

本項では、ステータス確認において、サイバー攻撃を確認した後、攻撃されたファイル、攻撃範囲の特定を実施する際の運用をご説明させていただきます。

- 1 ブラウザを起動し、CyberSense にアクセスします。  
“管理者”アカウント、パスワードを入力し、**Sign in** をクリックします。

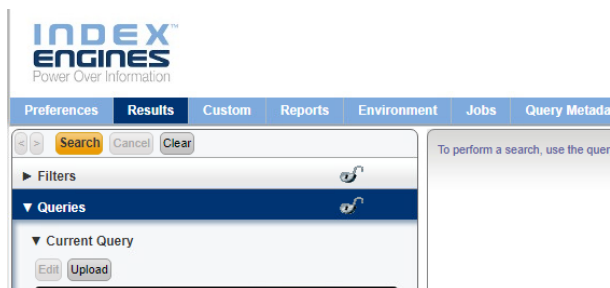


Sign In dialog box with fields for Username, Password, and Domain. The Domain dropdown is set to (engine). There is a checkbox for "Remember me on this computer" and a "Sign In" button.

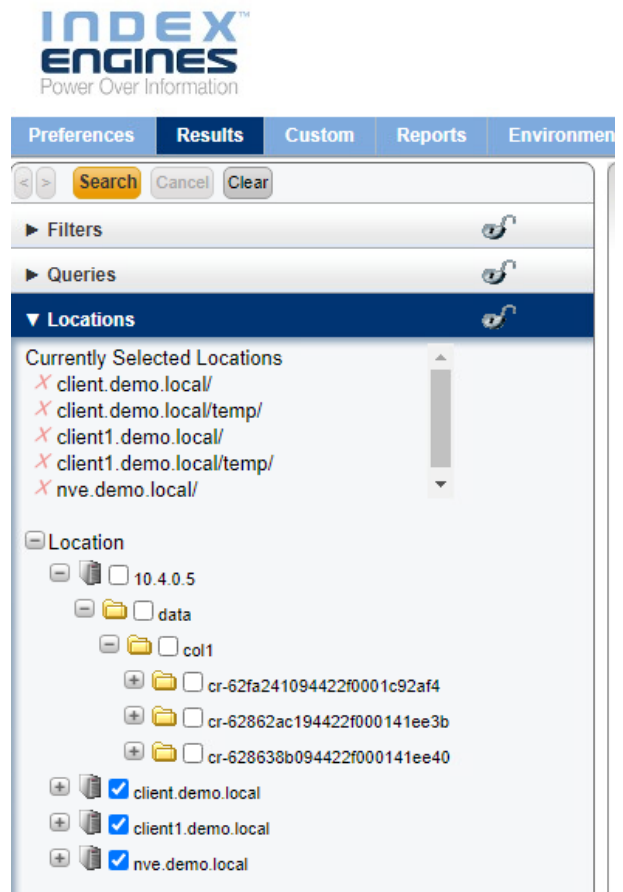
Sign In dialog box with fields filled with Username: admin, Password: \*\*\*\*\*, and Domain: (engine). There is a checkbox for "Remember me on this computer" and a "Sign In" button.

- 2 **Search** をクリックします。  
**Results** をクリックします。

Alerts Setup Manage Index **Search** Administration About Help Sign Out  
Signed In As: admin Index Name: Cyber Engine: cybersense.vault.local



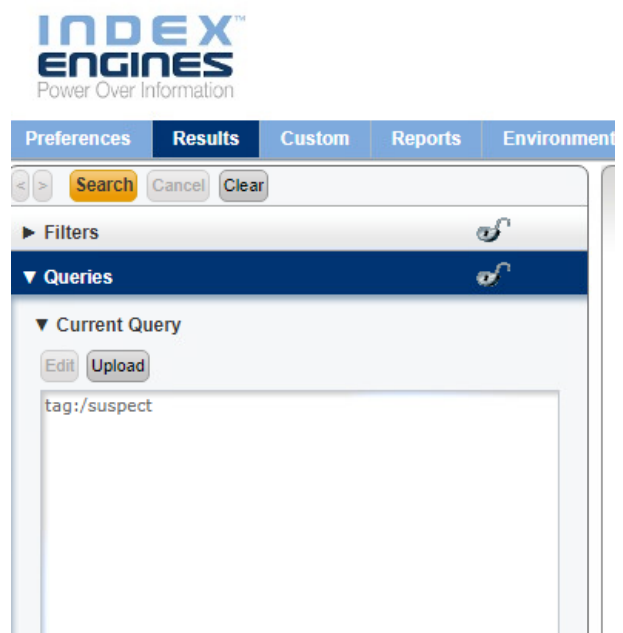
- 3 攻撃を受けた Context に含まれるバックアップデータが把握できている場合は **Locations** を展開し、対象クライアントにチェックを入れます。  
不明の場合は選択せずに進めます。



- 4 **Queries** にタグを入力します。  
tag:/suspect

入力後、**Search** をクリックします。

※tag:/suspect or tag:/previous とすることで拡張子が変更される前と合わせて、リストを出すことが可能です。



5 攻撃をされたファイルのリストが作成されます。

Name	Owner	Modified	Accessed	Size
.../pub-administration-guide-ehrus.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	3.14KB
.../pub-administration-guide-elencu.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	3.82KB
.../pub-administration-guide-elencu.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	3.38KB
.../pub-administration-guide-elencu.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	1.79KB
.../PowerScale-Orch5.0-3.0-0-security-config-guide.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	824.4KB
.../PowerScale-Orch5.0-3.0-0-ssuiprse-admin-guide.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	837.7KB
.../PowerScale-Orch5.0-3.0-0-7sh-8aws-Quile.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	154.3KB
.../PowerScale-Orch5.0-3.0-0-Support-Coman-Quile.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	238.1KB
.../PowerScale-Orch5.0-3.0-0-SP-Reference-Guide.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	1.48KB
.../HCL-0430-VFRAI-Integration_with_PowerProtect_18_3.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	2.49KB
.../HCL-0430-Protecting_Virtual_Machines_with_PowerProtect_VMDI_and_PowerProtect_Data_Manager.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	2.20KB
.../HCL-0411_18_4_Data_Protection_Suite_Versions_1.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	18.80KB
.../HCL-0411_18_3_Data_Protection_Suite_New.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	9.81KB
.../HCL-0411_18_3_Data_Protection_Suite.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	9.78KB
.../HCL-0411_18_3_Data_Protection_Suite.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	9.72KB
.../HCL-0407_OPA_2_5_MGMT_Services_Privy.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	1.80KB
.../HCL-0407_OPA_2_5_MGMT_Services_Privy.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	8.80KB
.../HCL-0407_OPA_2_5_MGMT_Services_Privy.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	8.80KB
.../Content_Archive_Archive_Webinars.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	92.9KB
.../Content_Backup-2021-03-24T07_20_46_2152.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	18.0KB
.../All_Java-2021-03-24T10_32_28_8552.pdf.rtk	Nobody@AD.NULL.Nessus	Jun-22-2022	Jun-22-2022	53.3KB
.../302-005-880-01-or-n.pdf.doc	S-1-0-1-0	Jun-22-2022	Sep-07-2021	138.5KB
.../302-005-880-01-or-n.pdf.doc	S-1-0-1-0	Jun-22-2022	Sep-07-2021	454.3KB
.../302-005-880-01-or-n.pdf.doc	S-1-0-1-0	Jun-22-2022	Sep-07-2021	101.5KB
.../302-005-880-01-or-n.pdf.doc	S-1-0-1-0	Jun-22-2022	Sep-07-2021	411.1KB
.../302-005-880-01-or-18-2-005-00000.pdf.doc	S-1-0-1-0	Jun-22-2022	Sep-07-2021	348.8KB

6 **Reports** タブをクリックします。  
**Report** ルールを Location に変更します。  
 影響範囲が出力されます。

疑わしいデータが発生した旨をユーザーに通知、利用の差し止めを連絡、データ復旧の準備をする等、事前に定義された Cyber resiliency Runbook に沿った組織ごとの対応に移ります。

影響範囲、攻撃されたデータにより、対応が異なることが想定されますので、復旧を進める前にセキュリティオペレーションセンター、もしくは相当部門に判断を仰ぎます。

INDEX ENGINES  
Power Over Information

Preferences Results Custom **Reports** Envi

Search Cancel Clear

Filters

Report: Locations Select Action

Results 1 - 2 Result Page: Previous Next 1 Results Per Page: 10 View: Responsive

Unique Locations by File Count

Rank	Locations	Nominal Size	Extraction File Size	File Count
1	client1.demo.local/temp/	12.96MB	12.96MB	24 52.17%
2	client.demo.local/temp/	80.87MB	80.87MB	22 47.83%
	Subtotal:	93.83MB	93.83MB	46 100.00%
	Total:	93.83MB	93.83MB	46

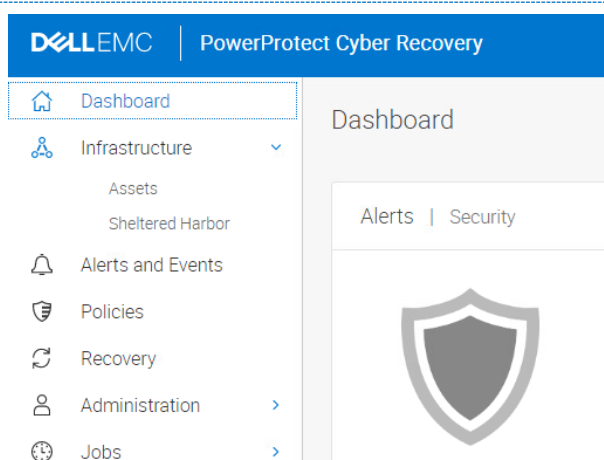
## 5. データの復旧

本項では、サイバー攻撃による被害範囲が確定した後、直前のデータを用いてデータを復旧する手順を説明します。復旧において、Prod 側のバックアップ領域および Vault 側のレプリケーション領域に対しての書き込みは発生しないため、サイバー攻撃発生時の事前確認としても行っていただくことが可能です。

- 1 ブラウザを起動し、PowerProtect CyberRecovery にアクセスします。  
“管理者”アカウント、パスワードを入力し、**Log in** をクリックします。

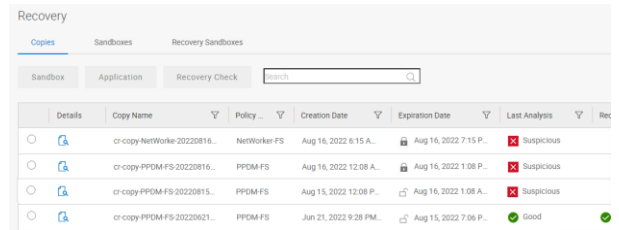


- 2 **Recovery** を選択します。  
Last Analysis が Good と表示されているものが CyberSense によるデータ分析の結果、利用可能と判断されたものです。

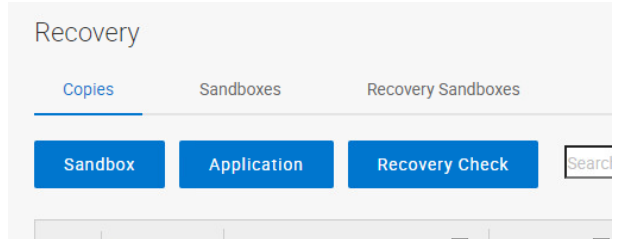


- 3 Last Analysis が Good と表示されているものが CyberSense によるデータ分析の結果、利用可能と判断されたものです。

対象の Copy を選択し、**Application** をクリックします。ApplicationHost に Vault 側の PPDM を選択し、**Apply** をクリックします。



Details	Copy Name	Policy	Creation Date	Expiration Date	Last Analysis	Rec
<input type="radio"/>	cr-copy-NetWorker-20220816...	NetWorker-FS	Aug 16, 2022 6:15 A...	Aug 16, 2022 7:15 P...	<span style="color: red;">✖</span> suspicious	
<input type="radio"/>	cr-copy-PPDM-FS-20220816...	PPDM-FS	Aug 16, 2022 12:08 A...	Aug 16, 2022 1:08 P...	<span style="color: red;">✖</span> suspicious	
<input type="radio"/>	cr-copy-PPDM-FS-20220815...	PPDM-FS	Aug 15, 2022 12:08 P...	Aug 16, 2022 1:08 A...	<span style="color: red;">✖</span> suspicious	
<input type="radio"/>	cr-copy-PPDM-FS-20220621...	PPDM-FS	Jun 21, 2022 9:28 PM...	Aug 15, 2022 7:06 P...	<span style="color: green;">✔</span> good	<input checked="" type="checkbox"/>



Recovery

Copies Sandboxes Recovery Sandboxes

Sandbox Application Recovery Check Search

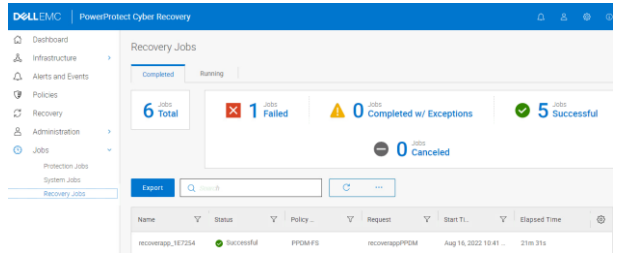
Application Recovery

Enter the details of the application recovery below.

Application Host: VaultPPDM

Cancel Apply

- 4 **Jobs** を展開し、**RecoveryJobs** をクリックします。ステータスが Successful になっていれば、PIT コピーを Vault 側の PPDM がマウントできています。 ※環境によっては数十分かかるケースがあります。進捗については **Running** タブより確認が可能です。



Dell EMC | PowerProtect Cyber Recovery

Recovery Jobs

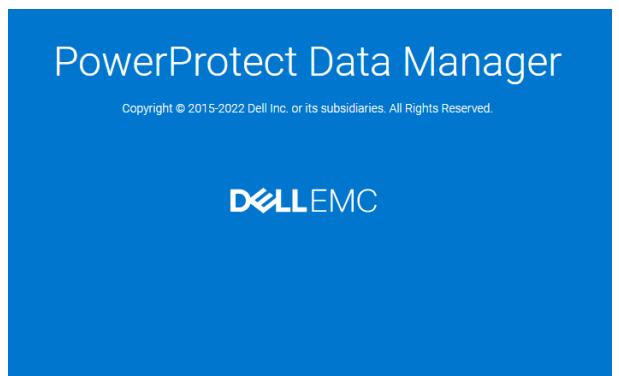
Completed Running

6 Total 1 Failed 0 Completed w/ Exceptions 5 Successful 0 Canceled

Name	Status	Policy	Request	Start TL	Elapsed Time
recoverapp_167254	Successful	PPDM-FS	recoverappPPDM	Aug 16, 2022 10:41	21m 31s

- 5 Vault 側の PPDM にログインします。PPDM は Restricted Mode で起動しています。通常と異なる点はスケジュールタスクが動作しない点です。リストアについては通常通り、実行可能です。

Vault 側のリカバリテスト用のホスト、VM リカバリ先の vCenter 等、リストア対象に合わせて追加し、必要なデータをリカバリ可能です



Username:

Password:

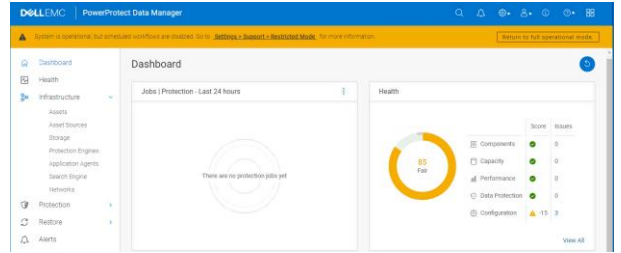
[Forgot password?](#)

Username:

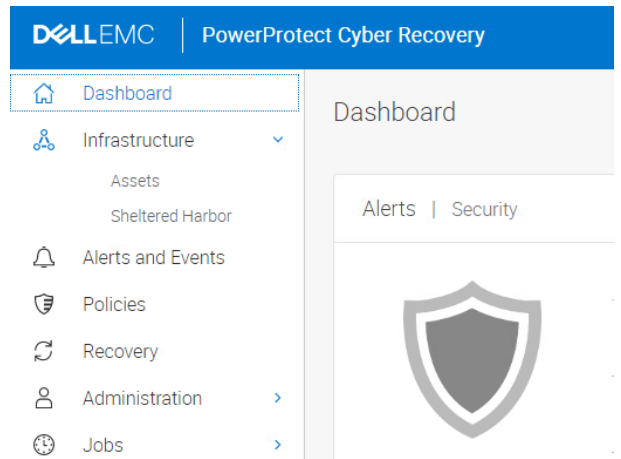
Password:

[Forgot password?](#)

**Log In**

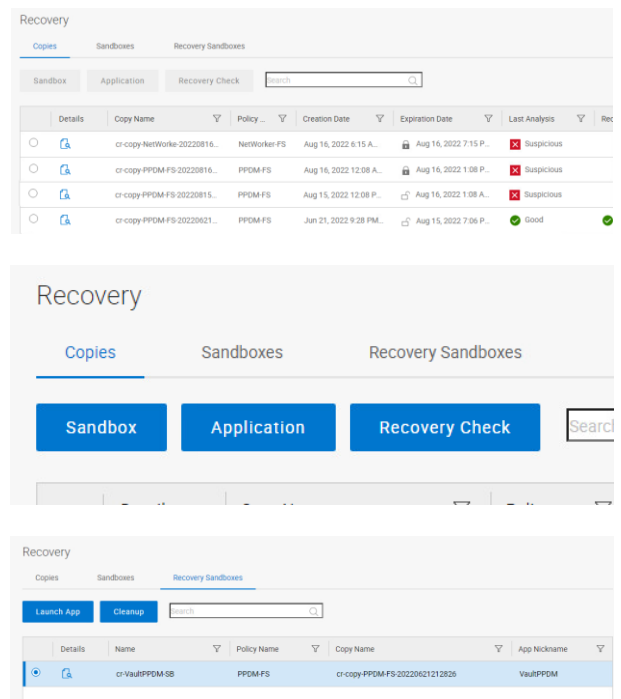


- 6 リカバリ完了後、PowerProtect CyberRecovery からコピーのマウントを解除します。  
**Recovery** を選択します。



- 7 **Recovery Sandboxes** タブを選択し、マウントしているコピーを選択、**Cleanup** をクリックします。

※この動作に伴って、コピーに対して変更が加わる、Vault側のPPDMに設定が残るといったことはありません。同じコピーを再度PPDMにマウントし、データを活用いただくことが可能です。



---

## Confirm

Are you sure you want to cleanup the selected sandbox?

Cancel

Cleanup

## 6. コピーの破棄

本項では、不要になったコピーを破棄する方法をご説明します。

コピーは PowerProtectDD の FastCopy 機能を利用しており、使用量はコピー数ではなく、世代間の差分量に比例して増えるものとなるため、比較的容易に多世代保管することが可能ですが、不要なコピーについては定期的に削除することを推奨します。

- 1 ブラウザを起動し、PowerProtect CyberRecovery にアクセスします。  
“管理者”アカウント、パスワードを入力し、**Log in** をクリックします。



User Name:

Password:

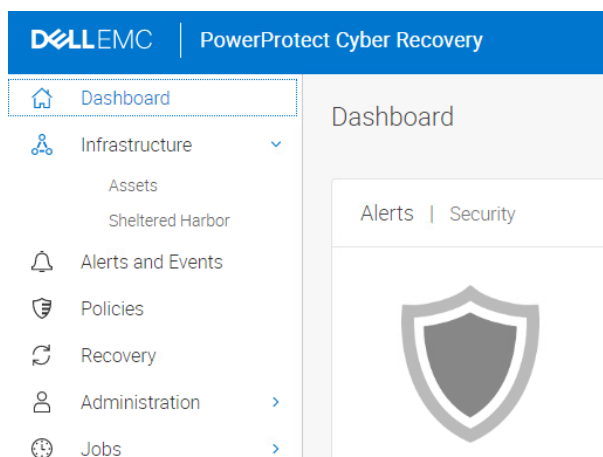
Log In

User Name:

Password:

Log In

- 2 **Policies** を選択し、**Copies** をクリックします。





- 3 Expiration Date が到来しているもののみ、削除可能です。  
削除するコピーを選択し、**Delete** をクリックします。

The screenshot displays the 'Policies' section of the console, specifically the 'Copies' tab. A table lists various policy copies with columns for 'Copy Name', 'Policy', 'Creation Date', 'Expiration Date', 'Last Analysis', and 'Recovery'. One row is selected, and a 'Delete' button is visible in the top navigation bar. Below the table, a 'Confirm' dialog asks 'Are you sure you want to delete the selected copy?' with 'Cancel' and 'Delete' buttons.

Copy Name	Policy	Creation Date	Expiration Date	Last Analysis	Recovery
cr-copy-PPDM-FS-2022081...	PPDM-FS	Aug 16, 2022 12:06 ...	Aug 17, 2022 1:06 ...	Analysis in Progress	
cr-copy-NetWorke-2022081...	NetWorker...	Aug 16, 2022 6:15 A...	Aug 16, 2022 7:15 ...	Suspicious	
cr-copy-PPDM-FS-2022081...	PPDM-FS	Aug 16, 2022 12:08 ...	Aug 16, 2022 1:08 ...	Suspicious	
cr-copy-NetWorke-2022081...	NetWorker...	Aug 15, 2022 6:04 P...	Aug 16, 2022 7:04 ...	Suspicious	
cr-copy-PPDM-FS-2022081...	PPDM-FS	Aug 15, 2022 12:08 ...	Aug 16, 2022 1:08 ...	Suspicious	
cr-copy-NVE-20220815105...	NVE	Aug 15, 2022 10:53 ...	Aug 15, 2022 11:5...	Good	
cr-copy-SH-2022081510856	SH	Aug 15, 2022 10:08 ...	No lock set		
cr-copy-NetWorke-2022081...	NetWorker...	Aug 15, 2022 6:06 A...	Aug 15, 2022 7:06 ...	Suspicious	

以上が PowerProtect CyberRecovery Solution の運用となります。

今回は GUI からステータスを確認するものとしていますが、PowerProtect CyberRecovery から外部通知を行うように構成することで、正常時のステータス確認はメール確認を行うことで代替し、GUI アクセスをする機会を減らすなども検討いただけるかと思えます。