

VERITAS™

Backup Execのランサムウェア対策

～ これがあれば一安心！～

ベリタステクノロジーズ合同会社

ランサムウェア対策の現状とベストプラクティス



セキュリティ10大脅威で、「ランサムウェアによる被害」が、今年も1位に

2022 情報セキュリティ10大脅威*

2022年 順位	情報セキュリティ脅威	2021年 順位
1	ランサムウェアによる被害	1
2	標的型攻撃による機密情報の窃取	2
3	サプライチェーンの弱点を悪用した攻撃	4
4	テレワーク等のニューノーマルな働き方を狙った攻撃	3
5	内部不正による情報漏えい	6

* 出典: 2022年IPA (情報処理推進機構) による調査結果

ランサムウェア対策のベストプラクティス



周知させる:
BE aware



セキュリティー対策:
BE ready



データ保護:
BE prepared



Backup Exec

ランサムウェア対策: Ransomware Resilience



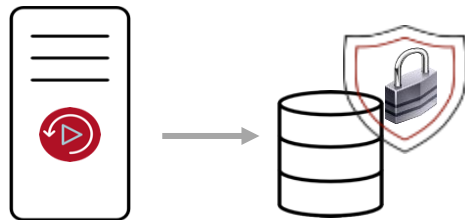
Backup ExecのRansomware Resilience



バックアップはランサムウェア対策の最後の砦！

バックアップデータも攻撃

二通りの方法でバックアップデータを保護



Backup Exec

- バックアップの保管先（ディスクストレージ）に保管しているバックアップデータはBackup Execしかアクセスできない



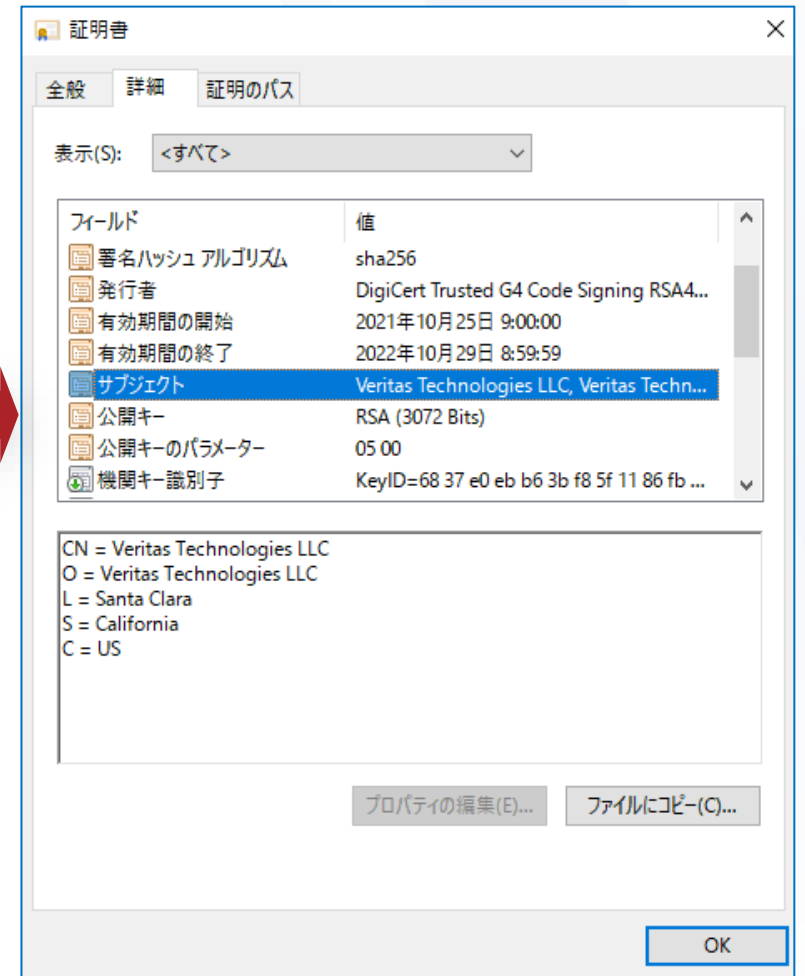
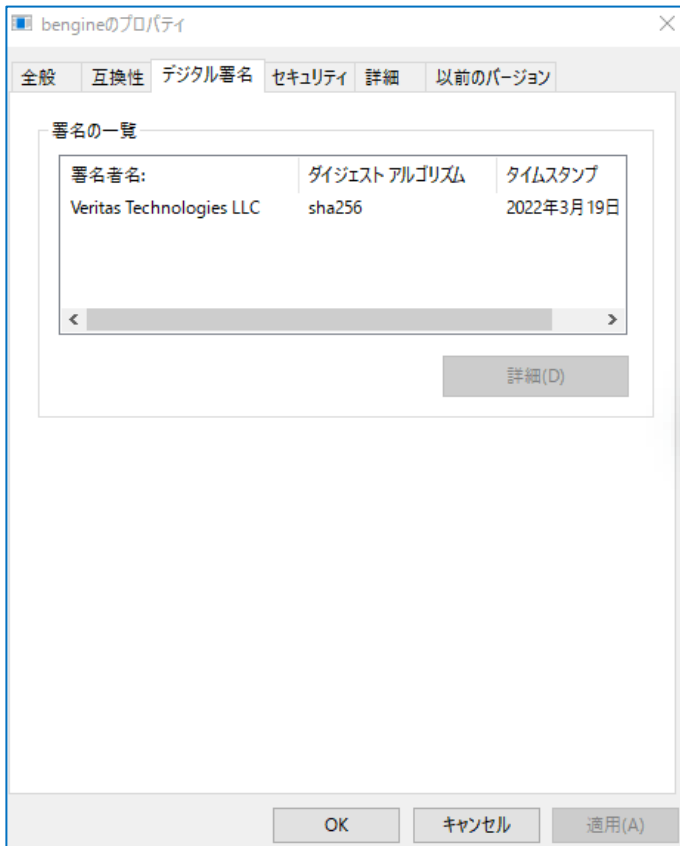
Backup Exec

- Backup Execのソフトウェアになりすましてバックアップデータへのアクセスを防ぐ

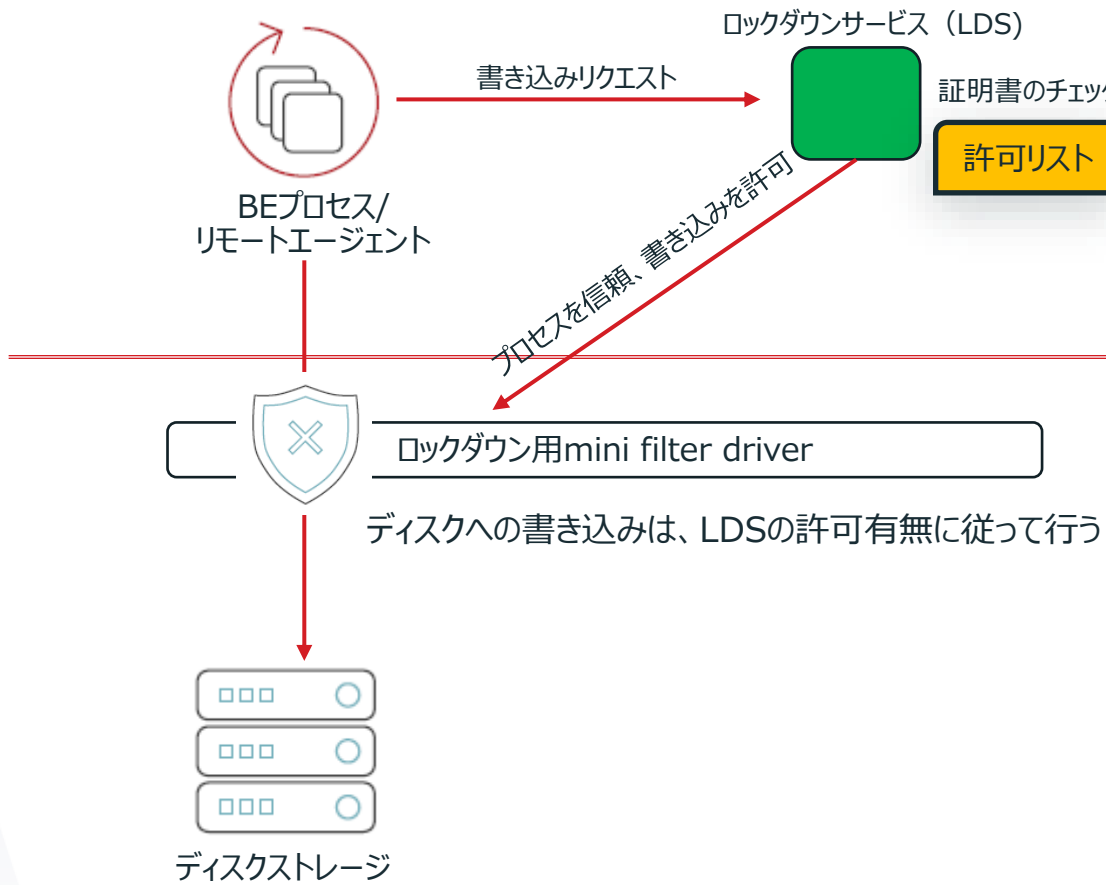
これがあれば一安心！

Authenticode

Authenticodeとは、署名されたソフトウェアの発行元を識別するMicrosoft コード署名テクノロジー

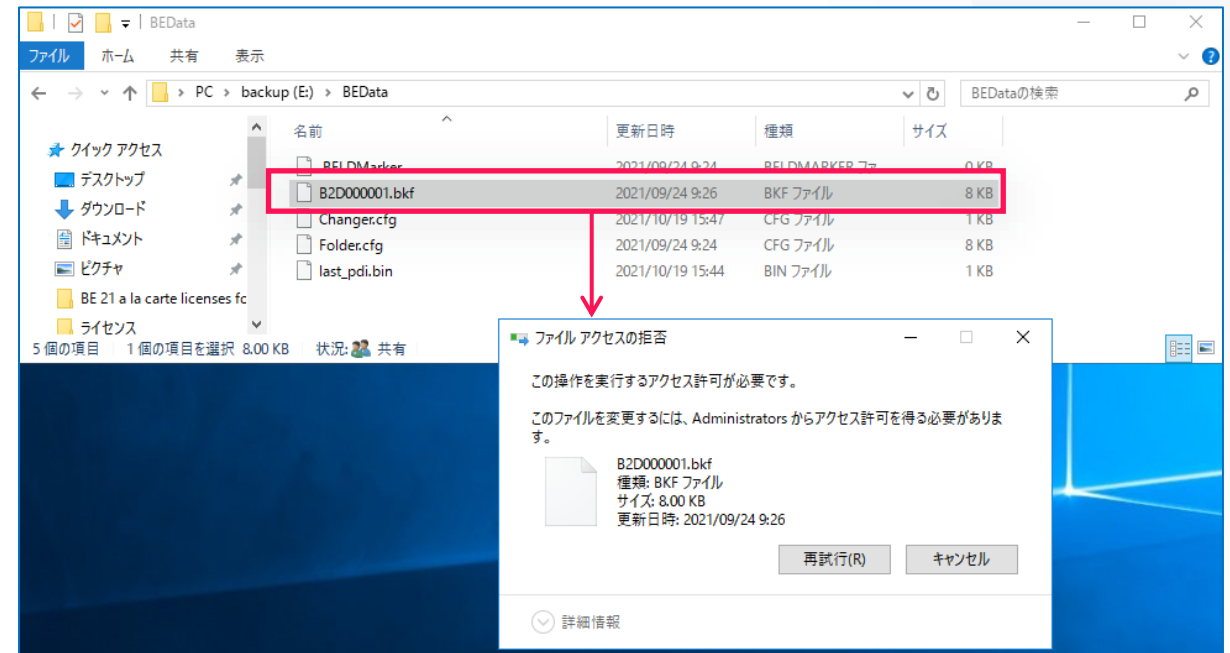
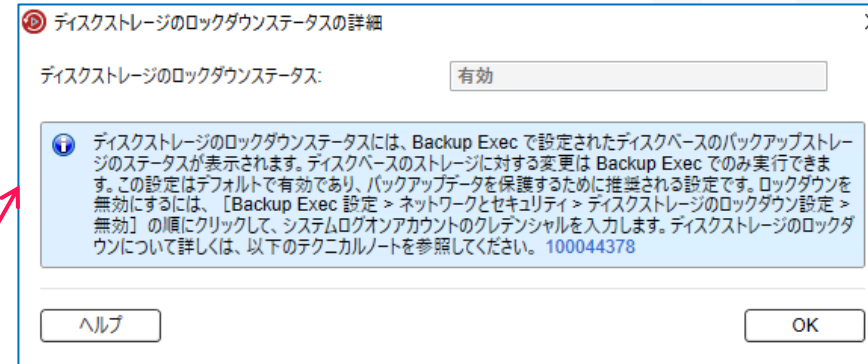
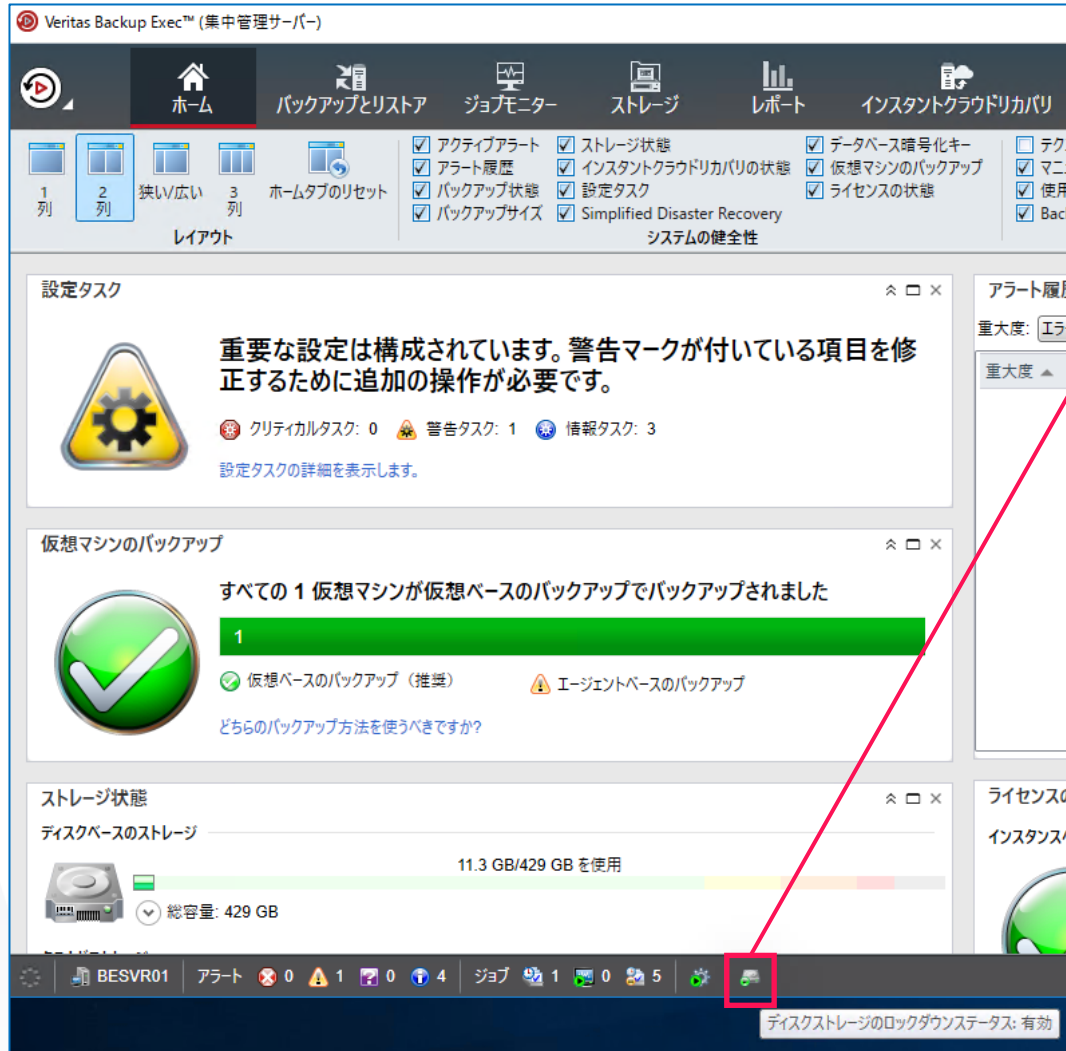


Ransomware Resilience: Backup Execのロックダウンサービス (LDS)

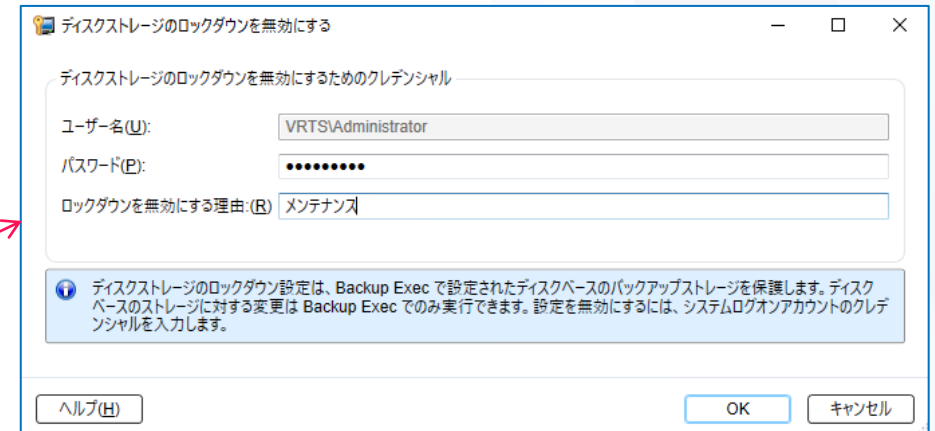
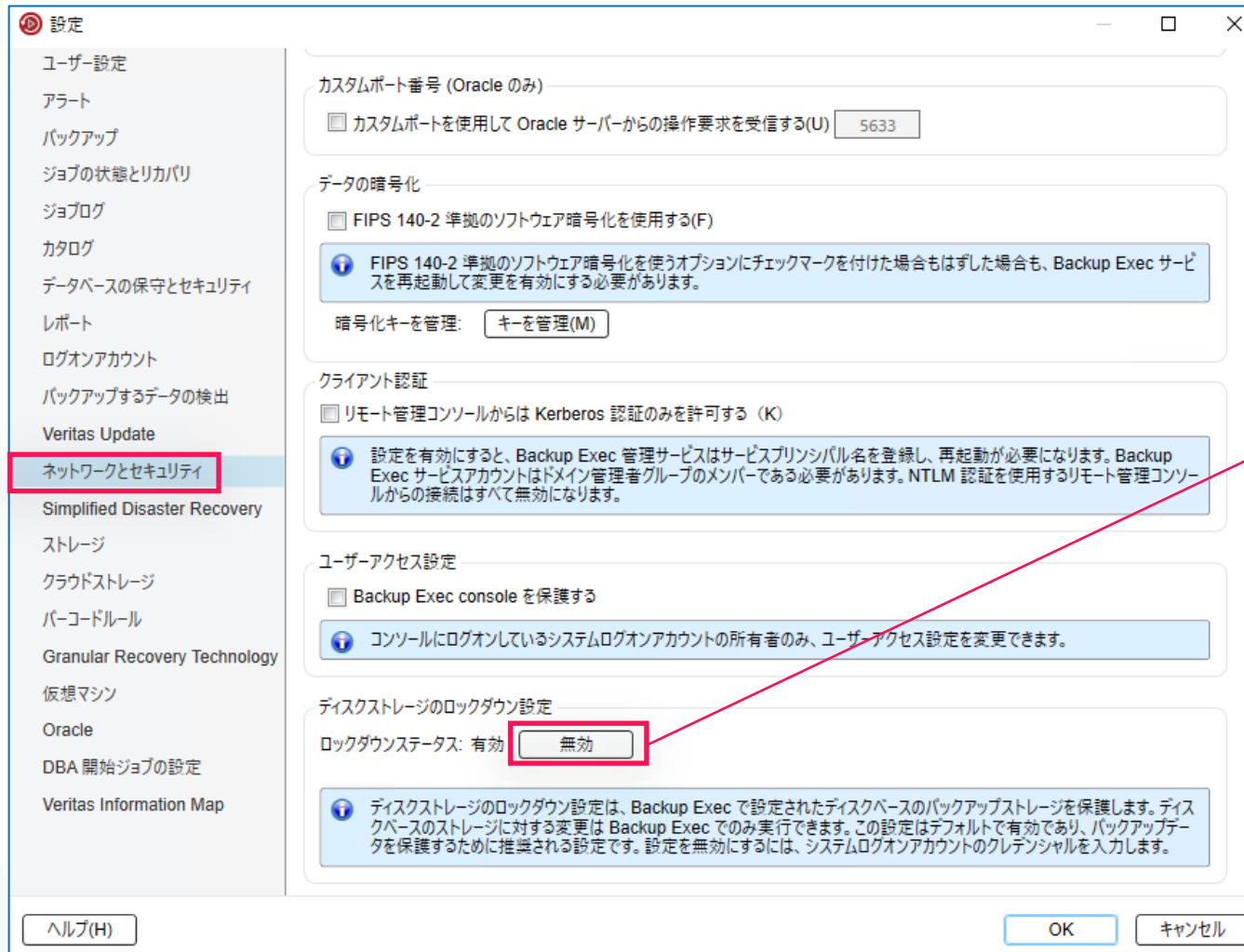


- **ロックダウン**：ディスクストレージへの不正な書き込みを保護する機能
- ディスクストレージへの書き込みは、「ロックダウン用mini filter driver」が行う
- ロックダウンサービス (LDS)が書き込みリクエストを受けたプロセスの証明書をチェック
- ベリタスの正規な証明書であれば、書き込みの許可をmini filter driverに与える
- LDSは許可リストにないプロセスからのアクセスを遮断させる
- ロックダウンに対応したストレージ
 - ネットワーク共有されたディスクストレージ
 - ローカルのディスクストレージ、重複排除ストレージ
 - RDX

Ransomware Resilience: Backup Execのロックダウンサービス (LDS)



Ransomware Resilience: Backup Execのロックダウンサービス (LDS)



ランサムウェア対策: WORM型ストレージの対応





WORMストレージ
(Write Once Read Many)

ランサムウェア対策: WORM型ストレージの対応

Write Once Read Many (WORM)に対応したストレージへのバックアップとリストアをサポート。
このリリースで対応したストレージは 2 種類 :

- Dell EMC Data Domain
- Backup Execの重複排除機能を設定したAmazon S3 (AWS)のクラウドストレージ
- さらに多くのベンダーを今後のリリースで追加する予定

WORM型ストレージで定義された保存期間に応じて、書き込み、上書き、消去、再フォーマットができない

WORM型ストレージは、ランサムウェアや誤った削除からの保護に役立つ

WORM型ストレージの対応: 前提条件

AWSの場合:

- MSDPCLDUTIL.EXEを実行して、WORM機能付きのクラウドバケットを設定する
- MSDPCLDUTILツールはBackup Execのインストールフォルダの下にある
- Backup Execのクラウド重複排除ストレージを設定
- MSDPCLDUTIL.EXEを使って設定したクラウドボリューム名と同じストレージデバイス名をBackup Exec側で設定する

Data Domainの場合:

Backup Exec サーバに Data Domain プラグイン (DDBoost)をインストールする

Backup Execの管理コンソールでストレージを設定

Backup Execで使用するMSDPCLDUTIL.EXEは、NetBackupと同じツールを使用するため、詳細についてはNetBackup Deduplication Guideの[About MSDP cloud admin command-line tool](#) の記載をご確認ください

環境変数の設定 (AWS)

- コマンドプロンプト(管理者モード) から (Backup Execのインストールディレクトリの配下で)、以下のコマンドを実行して環境変数を設定する (以下は例)

```
set MSDPC_ACCESS_KEY=xxxx  
set MSDPC_SECRET_KEY=yyyyyyyyyyyyyy  
set MSDPC_REGION=ap-northeast-1  
set MSDPC_PROVIDER=amazon
```

- Amazon S3の場合:

MSDPC_ACCESS_KEYは、IAMユーザーに関連付けられたAWSアクセスキー
MSDPC_SECRET_KEYは、アクセスキーに関連付けられた秘密鍵
MSDPC_REGIONは、バケットが作成されるまたはアクセスされるAWSのリージョン

MSDPCLDUTIL.EXEの実行

- 以下のコマンドを実行して、クラウドのイミュータブルストレージボリュームを作成
`msdpclldutil.exe create --bucket bucketname --volume volumename
--mode GOVERNANCE --min 1D --max 30D --live 2021-12-31`

注：ここで示した--min、--max、--liveの値はあくまでも例です。環境に合わせて適切に設定する。

--min = 消去されない最小値（日単位）

--max = 消去されない最大値（日単位）

- クラウドボリュームの一覧を表示するには、次のコマンドを実行
`msdpclldutil.exe list --bucket bucketname`

Backup Execの「ストレージ設定」で設定する名前は、
Volumenameと一緒にしておく

Backup ExecでAWSストレージを設定する

BESVR01 にストレージを設定

クラウドストレージデバイスに使用する名前と説明を指定してください。

名前(M):

説明(D):

クラウドストレージへの重複排除を有効にする ※

暗号化を有効にする

既存のクラウド重複排除用ストレージをインポートする

暗号化キー(Y):

[クラウド重複排除用ストレージを作成する前に、『Backup Exec 管理者ガイド』を参照するか、次のテクニカルノートを参照することもできます: technote](#)

[Amazon S3 クラウドストレージに Write Once Read Many \(WORM\) 対応のバックアップセットを作成するには、次を参照してください: technote](#)


選択した暗号化キーは、Backup Exec サーバーで作成されたすべてのクラウドの重複排除用ストレージデバイスで使用されます。データ回復には、クラウドの重複排除用ストレージで使用される暗号化キーが必要です。詳しくは、次のテクニカルノートを参照してください: 100050612

ストレージデバイスの名前は、MSDPCLDUTIL.EXEを使って設定したVolumenameと一緒にしておく

「クラウドストレージへの重複排除を有効にする」にチェックを入れる


※ 「クラウドストレージへの重複排除」を利用するには、Silver EditionまたはGold Editionのライセンスが必要です。Bronze/単体ライセンス/V-Ray Editionのライセンスには対応していません

AWSストレージデバイスのプロパティ

すべてのストレージ			
名前 ▲	状態	ストレージの種類	
 vol-be-s3-worm	オンライン	クラウド重複排除用ストレージ	OST WORM 変更不可, 削除不可

ジョブ	デバイス情報
ジョブ履歴	名前(N): vol-be-s3-worm
バックアップセット	説明(D):
アクティブアラート	状態: オンライン
プロパティ	クラウドストレージ: amazon:amazon.com
	ストレージの種類: S3
	ストレージ層: Standard
	バケットストレージコンテナ: be-worm-bucket
	Storage WORM: サポート対象
	バケットストレージコンテナのサブフォルダ: vol-be-s3-worm
	WORM 機能: 変更不可, 削除不可
	WORM の削除不可最小間隔: 1 日間
	WORM の削除不可最大間隔: 30 日間
	ホストサーバー: BESVR01
	キャッシュパス: F:\BackupExecDeduplicationStorageFolder

Data Domainのストレージデバイスのプロパティ

すべてのストレージ							
名前 ▲	状態	OST WORM	アクティブアラート	ストレージの傾向	容量	実行中とスケ...	平均スループット
 Data Domain	オンライン	変更不可, 削除不可			225 MB/117 GB を使用		

ジョブ

ジョブ履歴

バックアップセット

アクティブアラート

プロパティ

デバイス情報

名前(N): Data Domain WORM

説明(D):

状態: オンライン

ホストサーバー: 192.168.0.20

サーバーの場所: 192.168.0.20

サーバーの種類: DataDomain

Storage server WORM: サポート対象

論理ストレージユニット: ost-disk

論理ストレージユニット機能: 変更不可, 削除不可

論理ストレージユニットの削除不可最小間隔: 3 日間

論理ストレージユニットの削除不可最大間隔: 7 日間

バックアップジョブの変更

バックアップオプション

スケジュール

ストレージ

ネットワーク

通知

テスト実行

検証

Advanced Open File

Advanced Disk-based Backup

プリポストコマンド

ファイルとフォルダ

除外

このバックアップ定義のすべてのバックアップジョブのオプション:

優先度(R): 通常

完全

ストレージ(S): Data Domain WORM (116 GB の空き)

保持ロックの有効化

保持する期間(K): 2 週間


LSU の削除不可間隔

最小: 3 日間

最大: 7 日間

圧縮(P): なし

暗号化の種類(C): なし


 権限のないアクセスからデータを保護するために暗号化の使用をお勧めします。NDMP パ

「保持ロックの有効化」というチェックボックスを新設。ここにチェックを入れると、WORMストレージの保持期間が優先される（Backup Execのジョブで設定した保持期間は無視される）

保持する期間の設定は削除不可の最小値と最大値の間に設定しなければならない。設定しないと次のようなエラーが表示される



Veritas Backup Exec™

 「保持期間」の値は、LSU の削除不可間隔に設定された最小値と最大値の間にする必要があります。

OK

バックアップセットの保持について

Data Domain WORM 詳細

サーバー ▲	リソース	バックアップ時刻	バックアップ方式	ストレージ	有効期限	サイズ	保持	保持理由	検証の状態
BESVR01	C:	2021/12/06 15:46:51	スナップショット 完全	OpenStorage デバイス	期限切れ	16.9 MB		WORM 対応デバイスによって保持がロックされています	

「保持ロックの有効化」が設定されている場合

- WORMストレージ側で設定した保持期間が経過した後でないとバックアップセットの削除、変更ができない。
- WORMストレージ側の保持期間が優先される。バックアップセットを手動で削除しようとしても、WORMストレージ側でロックされていることが保持理由に表示される（画面例参照）。

「保持ロックの有効化」が設定されていない場合

- WORMストレージ側の設定、保持期間に関係なく、バックアップセットの削除が可能
- Backup Execのライフサイクル管理（DLM）に従って、保持期間経過後、バックアップセットが削除される。いつでも手動で削除することも可能。

ジョブログ

AWS

ジョブログ

1/1 ジョブログ

バックアップを 2021/12/06 16:38:04 に開始しました。
バックアップを 2021/12/06 16:38:06 に完了しました。

バックアップ セットの概略

バックアップしたファイル数 91、ディレクトリ数 2
17,490,960 バイト処理済み、所要時間 2 秒
スループット: 500 MB/分

OST イメージ「BEOST_00000006」は「2021/12/08 7:38:10」まで保持するために正常にロックされました。
Deduplication Stats:PDDO Stats (multi-threaded stream used) for (BESVR01): scanned: 20491 KB, CR sent: 655 KB, CR sent over FC: 0 KB, dedup: 96.8%, cache disabled, where dedup space saving:45.4%, compression space saving:51.4%

ジョブの完了状態

ジョブの終了日時: 2021年12月6日、16:38:13
完了状態: 成功

名前を付けて保存(A) 印刷(P) 検索(F)

ヘルプ(H) 閉じる

Data Domain

ジョブログ

1/1 ジョブログ

ストレージメディアのシーケンス番号: 1
ジョブの説明:
バックアップ方式: 完全 - ファイルをバックアップ (修正日時を使用)

バックアップを 2021/12/06 15:46:51 に開始しました。
バックアップを 2021/12/06 15:46:53 に完了しました。

バックアップ セットの概略

バックアップしたファイル数 91、ディレクトリ数 2
17,490,960 バイト処理済み、所要時間 2 秒
スループット: 500 MB/分

OST イメージ「BEOST_00000077」は「2021/12/10 6:46:54」まで保持するために正常にロックされました。

ジョブの完了状態

ジョブの終了日時: 2021年12月6日、15:46:55
完了状態: 成功

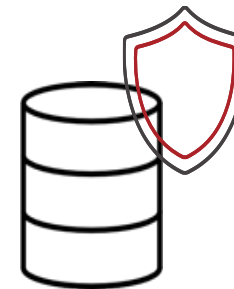
名前を付けて保存(A) 印刷(P) 検索(F)

まとめ



まとめ：Backup Execのランサムウェア対策

- バックアップは最後の砦
- 二通りの方法でバックアップデータを保護
 - 保管先バックアップデータへのアクセス制御
 - ソフトウェアのなりすまし防止
- 設定いらず、最初から有効
- 標準機能（無償、追加オプション不要）
- WORM型ストレージも効果的
- いざというときの安心感！
- **Backup Exec = ランサムウェア対策**



WORMストレージ
(Write Once Read Many)

VERITAS™

ありがとうございました