ユーザーガイド

HYCUデータ保護 for Enterprise Clouds

バージョン :4.5.0

製品リリース日 :2022年4月

資料リリース日 :2022年7月

HYCU®

法的通知

著作権情報

商標

HYCUのロゴ、名称、商標、サービスマーク、およびそれらの組み合わせは、HYCUまたはその関連会社の財産です。その他の製品名は、それぞれの商標またはサービスマーク所有者の財産であり、ここに明記します。

AcropolisおよびNutanixは、Nutanix, Inc.の米国およびその他の管轄区域における商標です。

Azure®、Microsoft®、Microsoft Edge™、およびWindows®は、Microsoft Corporationの米国およびその他の国における商標または登録商標です。

Dell Technologies、Dell、Dell EMC、およびその他の商標は、Dell Inc.またはその関連会社の登録商標です。

GCP™、Google Cloud Platform™、およびGoogle Cloud Storage™は、Google LLCの商標です。

Linux®は、米国およびその他の国におけるLinus Torvaldsの登録商標です。

Red Hat Enterprise Linuxは、米国およびその他の国におけるRed Hat, Inc.またはその関連会社の登録商標です。

VMware ESXi™、VMware Tools™、VMware vCenter Server®、VMware vSphere®、VMware vSphere® Data Protection™、およびVMware vSphere® Web Clientは、米国およびその他の管轄区域におけるVMware, Inc.またはその関連会社の商標または登録商標です。

免責事項

本資料に記載されている詳細や説明は、資料が作成された時点で正確かつ最新であると判断されています。この資料に記載されている情報は、予告なしに変更される場合があります。

HYCUはこの資料を「現状のまま」で提供し、商品性および特定の目的への適合性の黙示の保証を含む(ただしそれらに限定されない) 、明示または黙示のいかなる種類の保証も行いません。HYCUは本資料に含まれている誤記や省略については責任を負わないものとします。HYCUは、保証、契約、または他の何らかの法理論に準じているかどうかにかかわらず、本資料の使用または使用できない状態や、あるいは本資料に記載されている情報に基づいて取られたすべての措置について、たとえそれが損害を発生させる可能性があるという助言がある場合であっても、そのことに起因する直接

的、間接的、結果的、懲罰的、特別、または偶発的な損害について、一切責任を負わないものとします。この損害には、損失と利益の損害、予期される節約の損失、業務の中断、または情報の損失が含まれますが、それらに限定されません。

HYCU製品およびサービスに対する唯一の保証は、そのような製品およびサービスに付随する明示的な保証規定に記載されています。本資料のいかなる内容も、追加的な保証を制定するものと解釈すべきではありません。

注意

本資料はHYCU製品とともに提供されます。HYCUは、本資料の主題に関する著作権、特許、特許出願、商標、またはその他の知的財産権を有している場合があります。

HYCUからの書面によるライセンス契約で明示的に提供されている場合を除き、本資料の提供は、HYCU製品に関するこれらの特許、商標、著作権、またはその他の知的財産に対するライセンスをお客様に付与するものではありません。基礎となるHYCU製品の使用は、それぞれのソフトウェアライセンスおよびサポート条件に準拠します。

重要 :付属のソフトウェア製品を使用する前に、ソフトウェアライセンスとサポート条件をお読みください。

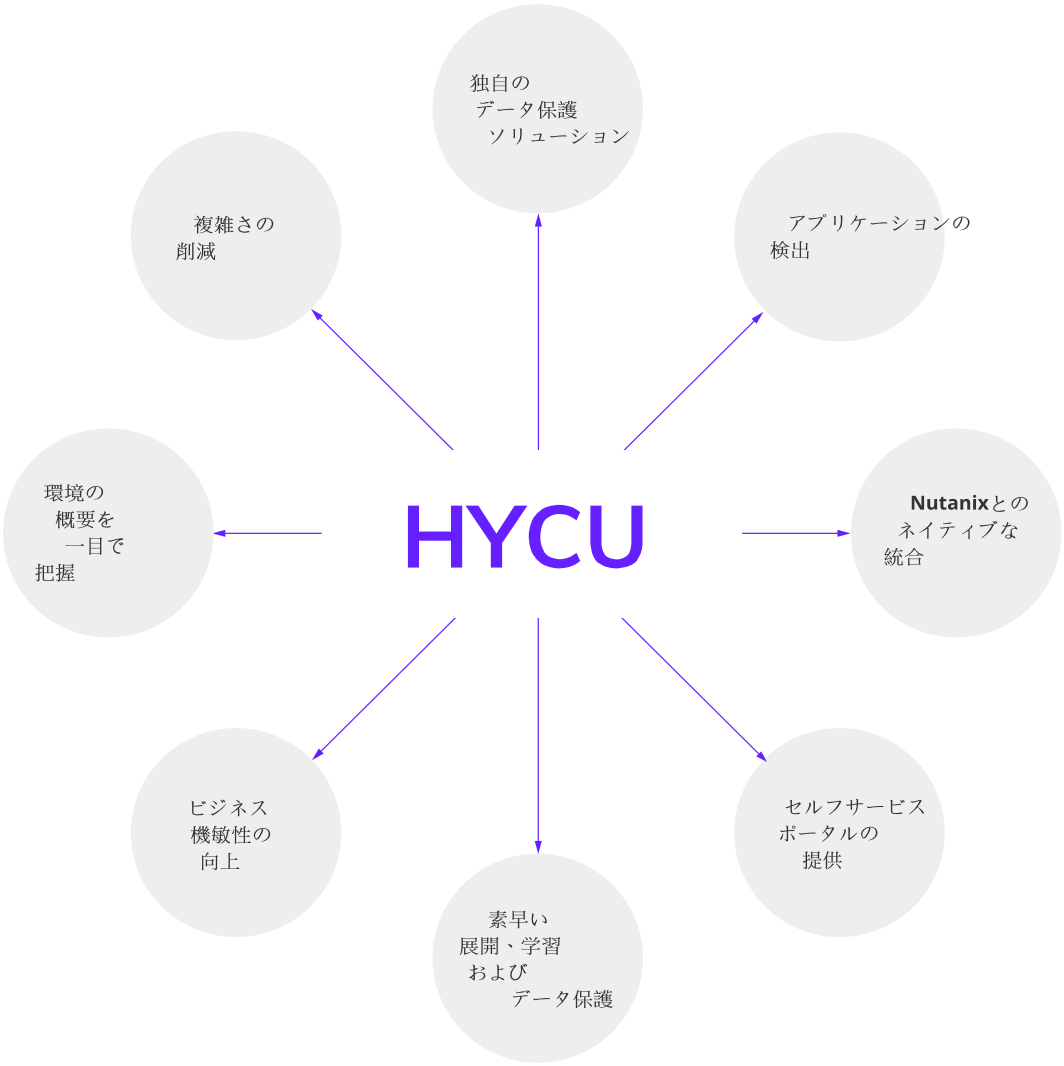
HYCU
www.hycu.com

目次

第 1章

HYCUについて

HYCU Data Protection for Enterprise Clouds(HYCU) は、Nutanix、VMware、および物理マシン環境向けの高性能なバックアップおよび復元ソリューションです。これは、Nutanixと完全に統合された初めてのデータ保護ソリューションであり、データ保護を簡単に展開して使用できるようになります。



参照 :図 1–1 :HYCUの概要

HYCUの主要な機能と利点

以下の機能により、HYCUはビジネスを変革し、完全なコンプライアンスとデータ保護を実現できるソリューションになります。

- **データ損失からの保護**

  ハイパーコンバージド環境でミッションクリティカルなアプリケーションとデータに対してネイティブで信頼性の高いデータ保護を提供すると同時に、データの整合性と容易な復元性を保証します。

- **展開の簡素化**

  HYCU仮想アプライアンスの展開は、Nutanix Prism Webコンソール(Nutanix AHVクラスターの場合) またはvSphere (Web) Client(Nutanix ESXiクラスターとvSphere環境の場合) から実行されます。●●

- **自動検出と可視性の提供**

  検出ソリューションは、仮想マシンと物理マシンに対する新たな検出と可視性を提供し、各アプリケーションが実行されている場所を特定します。

- **データを迅速に保護**

  仮想マシン、物理マシン、アプリケーション、ファイル共有、ボリュームグループ、および仮想マシンテンプレートのデータ保護は、HYCU展開後、数分で利用できます。

- **定義済みポリシーとカスタムポリシーの提供**

  HYCUに付属する定義済みポリシー(Gold、Silver、Bronze) により、データ保護の実装が簡素化されます。また、要件に合わせてカスタムポリシーを作成することも可能です。

- **RPOに基づいたバックアップ計画**

  自動バックアップスケジューリングは、目標復旧ポイント(RPO) に基づいてデータを保護します。

- **アプリケーションの検出と保護**

  アプリケーション認識機能により、アプリケーション検出、アプリケーション固有バックアップ、復元フローが提供され、アプリケーションデータ全体を確実に整合性のとれた状態でバックアップおよび復元できます。

- **ソースとターゲットの選択**

  保護対象となるソースと保存場所となるターゲットを自由に選択できます。

- **運用環境の可視化**

  HYCUダッシュボードは、潜在的な問題とボトルネックを識別して、データ保護環境のパフォーマンスを向上させるのに役立ちます。

- **Nutanixに効果的なROBOデータ保護ソリューションを提供します**

  リモートオフィス/ブランチオフィス(ROBO) のデータをデータセンターにレプリケートすることで、HYCUはレプリカから効率的なバックアップを実現し、かつ、データセンターまたは任意のリモート環境に復元できます。

- **ファイルサーバーのスケーラブルなバックアップを提供**

  ファイル共有のバックアップにかかる時間を短縮し、コンピューティングリソースを大幅に節約し、より高い頻度でバックアップを取得できるため、障害発生時のデータ損失量を低減できます。

- **バックアップをNutanixプラットフォームのサービスとして活用**

  Nutanix Mine with HYCUは、バックアップと復元をNutanixプラットフォームのネイティブサービスにすることが可能で、バックアップ専用の独立したインフラストラクチャを不要にします。

- **さまざまなインフラストラクチャにまたがるデータ保護とビジネス継続性を提供**

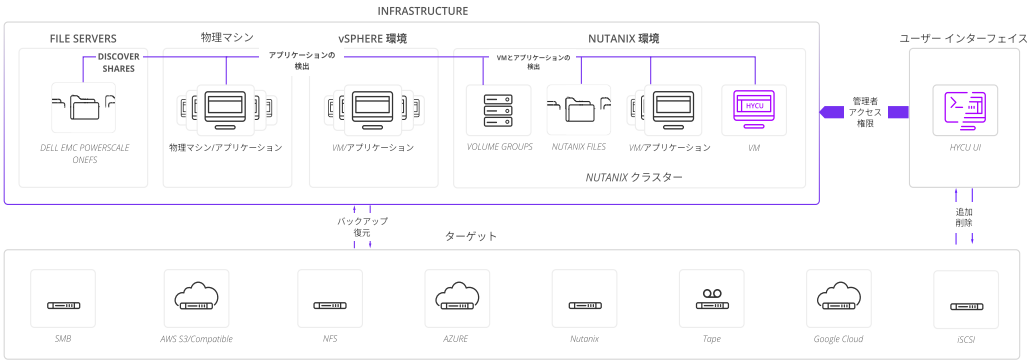
  HYCU Protégé は、スピンアップ機能を使用して、保護されたデータをオンプレミスとクラウドインフラストラクチャ(Google Cloud、グローバルAzure、またはAzure US Government環境) 間で移行や復元を実現します。災害発生時に、HYCU Protégéはクラウドへのミッションクリティカルなデータの災害復旧を提供します。

データ保護環境の概要

データ保護環境は、以下のコンポーネントで構成されます。

HYCU Backup Controller	ソースから収集されたデータの処理や、Webユーザーインターフェースに情報を表示する仮想マシン。
HYCUインターフェース	エンティティを保護し、データ保護環境を管理するためのインターフェース。HYCU Webユーザーインターフェースおよびコマンドラインインターフェース(hyCLI) として使用できます。
ターゲット	保護されたデータを保存するためにHYCUが使用する保存場所。
ソース	HYCUがデータ保護を提供する環境。Nutanixクラスター、vSphere環境、ファイルサーバー、および物理マシン。
エンティティ	ポリシーを割り当てることができ、データ保護の対象となるオブジェクト(仮想および物理マシン、アプリケーション、およびファイル共有) 。 データは常にきめ細かなレベルで保護されているため、エンティティ全体またはその一部(ディスクおよびアプリケーション項目) を復元できます。

次の図は、データ保護環境とその最も重要なコンポーネントを示しています。



参照 :図 1–2 :HYCUアーキテクチャ

HYCUデータ保護

HYCUデータ保護ソリューションを使用すると、ビジネスデータが保護されていることに信頼感を持つことができます。つまり、ビジネスデータは整合性のある状態でバックアップし保存されます。復元可能、アクセス可能であり、破損していないということが確認できます。

HYCUを使用すると、仮想マシンと物理マシン、それらで実行されているアプリケーション、ファイルサーバー上のファイル共有、Nutanixボリュームグループ、および仮想マシンテンプレートを保護できます。データ保護環境を構築後(ソースの追加やターゲットのセットアップ、および任意でポリシーの作成)、データ保護を有効にできます。最初のバックアップが正常に完了したら、データは破損や破壊が発生しても復元できます。

HYCUはアプリケーションに対応しており、仮想マシンと物理マシンに資格情報を設定すると、それらにアプリケーションがインストールされて実行されているかどうかを検出します。さらに、バージョン、検出されたアプリケーションの個々のコンポーネントがインストールされているホスト、および各ホストのロールなど、検出されたアプリケーションに関する詳細も検出します。

HYCUを展開してデータ保護環境を確立後、保護するデータの種類に応じて、次のいずれかのセクションを参照してください。

- “仮想マシンの保護” ページ71
- “アプリケーションの保護” ページ113
- “ファイル共有の保護” ページ139
- “ボリュームグループの保護” ページ146

第2章

HYCU仮想アプライアンスの展開

HYCU仮想アプライアンスは事前構成されたソフトウェアソリューションであり、データ保護を提供するNutanix AHVクラスター、Nutanix ESXiクラスター、またはvSphere環境に簡単に展開できます。

展開モード

モード	用途
HYCUバックアップコントローラー	仮想マシン(仮想マシンテンプレートを含む)、物理マシン、アプリケーション、ファイル共有、およびボリュームグループを保護します。 HYCU Backup Controllerはソースから収集したデータを処理して、Webユーザーインターフェースに表示する仮想マシンです。
HYCUインスタンス	ファイル共有を保護します。 HYCUインスタンスは、ファイルサーバーのデータ保護操作を実行するためにHYCUが使用する仮想マシンであり、HYCU Backup Controllerの負荷を取り除きます。
HYCU Manager	HYCUコントローラーを管理します。 HYCU Managerは仮想マシンとして構築し、オンプレミスおよびクラウドのデータ保護環境にあるすべてのHYCUコントローラーからデータを収集し、それらの情報をWebユーザーインターフェースに表示します。

展開タスク

タスク	説明
1. HYCUのバックアップインフラストラクチャのサイジング	"HYCUバックアップインフラストラクチャのリソースのサイジング" 次のページ
2. *ファイアウォールがネットワーク上に構成されている場合のみ。*関係する各ファイアウォールで関連するポートを開きます。	"ファイアウォール構成の調整" ページ18
3. ウイルス対策の設定をカスタマイ	"ウイルス対策構成の調整" ページ22

タスク	説明
ズします。	
4. HYCU仮想アプライアンスをソースに展開します。	"HYCUのNutanix AHVクラスターへの展開" ページ23または"HYCUのNutanix ESXiクラスターまたはvSphere環境への展開" ページ26

HYCU仮想アプライアンスを正常に展開したら、サポートされるWebブラウザーを使用して、HYCUにアクセスできます。HYCUへのログオン方法の詳細については、"HYCUへのログオン" ページ29を参照してください。

HYCUバックアップインフラストラクチャのリソースのサイジング

HYCU仮想アプライアンスを展開する前に、HYCUバックアップインフラストラクチャにより必要とされるリソースのサイジングを行い、他の関連要件が満たされていることを確認します。

- HYCU仮想マシン(HYCU Backup Controller、HYCU インスタンス、HYCU Manager) ：
  - ネットワーク接続 ：

    仮想マシン用のIPアドレスは必ず予約しておきます。
  - システム要件 ：
    - 最小要件は4個のCPUコアと4 GiBのRAMです。
    - データディスクの最小サイズはRAMの容量の少なくとも2倍であり、データディスクはOSディスクよりも大きくなります。
    - *HYCU Backup Controllerモードで展開する場合* ：データ保護環境の規模を超える想定は、システム要件に影響を与えることに注意してください。ソースのパフォーマンス、ターゲットの効率、選択されたバックアップ戦略、およびバックアップデータ圧縮はすべて、特定のリソースの要件を増やすかまたは減らす可能性があります。たとえば、バックアップデータをコピーしてアーカイブすることを予定している場合には、必要なターゲットの数は増えます。同様に、短いRPOまたは低いバックアップしきい値を指定している場合、バックアップインフラストラクチャの負荷が増え、HYCUはより多くのストレージおよびコンピューティングリソースを必要とします。以下の推奨事項を検討してください。

環境内のVMの数	システム要件				
	vCPU	コア数	メモリ	OSディスク	データディスク：
50未満	8	1	8 GiB	10 GiB	32 GiB
50 ~ 200	8	2	16 GiB	10 GiB	32 GiB

環境内のVMの数	システム要件				
	vCPU	コア数	メモリ	OSディスク	データディスク：
200 ~ 500	16	2	32 GiB	10 GiB	50 GiB
500を超える	数値は変更されることがあります。HYCUカスタマーサポートにお問い合わせください。				

- HYCU Webユーザーインターフェース：

  HYCU Webユーザーインターフェースにアクセスするために使用できるWebブラウザーのリストについては、「*HYCU互換性マトリックス*」を参照してください。

  > 注 HYCU Webユーザーインターフェースは、最低1280 × 720ピクセルの画面解像度で機能するように設計されています。

- *「HYCUバックアップコントローラー」モードでの展開の場合のみ*:ターゲット：

  保護データの保管に使用する宛先が使用可能であり、アクセス可能であることを確認します。

ファイアウォール構成の調整

展開された各HYCU仮想マシンには、必要なすべてのポートが事前に開いています。ただし、ネットワーク上にインストールされた他のファイアウォールが、特定のNutanix、vSphere、またはHYCU通信エンドポイント間のネットワークトラフィックをブロックする可能性があります。HYCUが正しく動作するには、ファイアウォールルールを調整して、以下の表にリストされているポートを開く必要があります。

ソースエンドポイントにインストールされているファイアウォールはトラフィックを発信と見るのに対して、宛先エンドポイントにインストールされているファイアウォールはトラフィックを着信と見ます。ファイアウォールが別の場所にインストールされている場合には、両方向の接続が許可されるように調整する必要があります。

目的	通信エンドポイント		宛先のポート	プロトコル
	ソース	宛先		
HYCUインターフェースの使用	HYCUインターフェースがアクセスされるシステム	HYCU Backup Controller	8443	TCP
SSHの使用によるHYCU Backup Controllerへのアクセス	HYCUインターフェースがアクセスされるシステム	HYCU Backup Controller	22	TCP
DNSサーバーの使用	HYCU Backup Controller、HYCUインスタン	DNSサーバー	53	TCP UDP

目的	通信エンドポイント		宛先のポート	プロトコル
	ソース	宛先		
	ス			
NTPサーバーの使用	HYCU Backup Controller、HYCUインスタンス	NTPサーバー	123	UDP
Linuxを実行するVMおよびその上のアプリケーションの検出	HYCU Backup Controller	VM	22[a]	TCP
Windowsを実行するVMおよびその上のアプリケーションの検出	HYCU Backup Controller	VM	5985 5986	TCP
バックアップ	HYCU Backup Controller	Nutanixコントローラー VM	3205 3260	TCP
Nutanix Files共有のバックアップおよび復元	HYCUインスタンス	Nutanix Filesサーバー	445[b] 2049[c] 9440	TCP
	HYCU Backup Controller	HYCU インスタンス	8443	
	HYCU インスタンス	HYCU Backup Controller		
PowerScale OneFS共有のバックアップおよび復元	HYCUインスタンス	PowerScale OneFS サーバー	445[b] 2049[c] 8080	TCP
	HYCU Backup Controller	HYCU インスタンス	8443	
	HYCU インスタンス	HYCU Backup Controller		
NFS v4ターゲットへのデータのバックアップ	HYCU Backup Controller、HYCUインスタンス	NFS v4サーバー	2049	TCP UDP
NFS v3ターゲットへのデータのバックアップ	HYCU Backup Controller、HYCUインスタン	NFS v3サーバー	111 2049 mountdポー	TCP UDP

目的	通信エンドポイント		宛先のポート	プロトコル
	ソース	宛先		
	ス		ト[d]	
SMBターゲットへのデータのバックアップ	HYCU Backup Controller、HYCUインスタンス	SMBサーバー	445	TCP
iSCSIターゲットへのデータのバックアップ	HYCU Backup Controller	iSCSIサーバー	3260	TCP
クラウドターゲットへのデータのバックアップ	HYCU Backup Controller、HYCUインスタンス	クラウドサーバー	443[e]	TCP
QStar NFSターゲットへのデータのアーカイブ	HYCU Backup Controller、HYCUインスタンス	QStarサーバー	111 2049 mountdポート[d] 18082[f]	TCP
QStar SMBターゲットへのデータのアーカイブ	HYCU Backup Controller、HYCUインスタンス	QStarサーバー	445 18082[f]	TCP
「Fast Restore」ポリシーオプションを有効にして作成したバックアップからの復元	HYCU Backup Controller	Nutanixコントローラー VM	3205	TCP
Windows VMへのアプリケーションまたはファイルの復元	VM	Nutanix iSCSIデータサービス	860 3260	TCP
		HYCU Backup Controller		
`flr.fast.disable`構成設定が`true`に設定された場合のWindows VMへのアプリケーションまたはファイルの復元	VM	HYCU Backup Controller	445	TCP
Linux VMへのアプリケーションまたはファイルの復	HYCU Backup Controller	VM	22	TCP

目的	通信エンドポイント		宛先のポート	プロトコル
	ソース	宛先		
元				
SMB共有へのファイルの復元	HYCU Backup Controller	SMB共有のあるシステム	445	TCP
NFS共有へのファイルの復元	HYCU Backup Controller	NFS共有のあるシステム	NFS4 :2049 NFS3 :111、mountdポート[d]	TCP
ローカルマシンへのファイルの復元	HYCUインターフェースがアクセスされるシステム	HYCU Backup Controller	8443	TCP
Nutanixクラスターまたは Nutanix Filesサーバー上のエンティティのデータ保護[i]	HYCU Backup Controller	クラスター仮想サーバー(クラスター仮想IPアドレス)	9440	TCP
		Nutanixコントローラー VM		
PowerScale OneFSクラスター上のエンティティのデータ保護	HYCU Backup Controller	クラスター仮想サーバー(クラスター仮想IPアドレス)	8080	TCP
		PowerScale OneFSノード		
Nutanixクラスターまたはボリュームグループ内にある仮想マシンのデータ保護[j]	HYCU Backup Controller	クラスター仮想サーバー(クラスター仮想IPアドレス) [g]	3205 3260	TCP
		iSCSIターゲット検出ポータル(iSCSIデータサービスIPアドレス) [h]		
vSphere環境でのエンティティのバックアップ	HYCU Backup Controller	ESXiホスト	902	TCP
		vCenterサーバー	443	
HYCUとのテレメトリデータの共有	HYCU Backup Controller	テレメトリホスト : callhome.hycu.com[k]	443	TCP
		データホスト :protege-production-bucket.s3.eu-central-		

目的	通信エンドポイント		宛先のポート	プロトコル
	ソース	宛先		
		1.amazonaws.com[l]		
LDAPサーバーの使用	HYCU Backup Controller	LDAPサーバー	LDAP :389 LDAPS :636	TCP
メール通知送信でのSMTPサーバーの使用	HYCU Backup Controller	SMTPサーバー	25[m]	TCP

[a] SSHサーバーをインストールし、SSH通信用にTCPポート22を使用するように構成する必要があります。
[b] HYCUがSMBプロトコルを使用してファイル共有にアクセスする場合のみ。
[c] HYCUがNFSプロトコルを使用してファイル共有にアクセスする場合のみ。
[d] ポート番号の詳細については、NFSサーバーの資料を参照してください。
[e] クラウドターゲットが複数のIPアドレスを使用する可能性があります。パブリッククラウドにより使用されるIP範囲の詳細については、各クラウドの資料を参照してください。
[f] これはHTTPS接続に使用される既定のポートですが、他のポートも使用できます。HTTP接続もサポートされていますが、推奨されていません。
[g] クラスター仮想IPアドレスが、HYCUのiSCSIターゲット構成で「ターゲットポータル」オプションに指定されている場合のみ。
[h] iSCSIデータサービスIPアドレスが、HYCUのiSCSIターゲット構成で「ターゲットポータル」オプションに指定されている場合のみ。
[i] HYCUはNutanix REST API v3を使用します。
[j] HYCUはNutanixボリュームにアクセスします。
[k] ホスト名はエイリアスであり、DNSサーバーから報告されたIPアドレスに解決されます。IPアドレスは静的ではなく、時間の経過とともに変更される可能性があることに注意してください。
[l] ホスト名はエイリアスで、ip-ranges(https://ip-ranges.amazonaws.com/ip-ranges.jsonで公開された) から生成され、リージョン(eu-central-1) およびサービス(S3) によってフィルタリングされたIPアドレスセットからのIPアドレスに解決されます。IPアドレスは定期的に変更されることに注意してください。
[m] SMTPサーバーは通常ポート25を使用しますが、他のポートも使用できます(たとえば、587や465など) 。

ウイルス対策構成の調整

HYCUはデータ保護環境のバックアップと復旧の目標を達成するために、ゲストオペレーティングシステムのファイルや構成にアクセスすることが必要になる場合があります。この場合、必要なバイナリプログラムやスクリプトは仮想マシン内で実行されるので、ウイルス対策プログラムがそれらの実行を妨げないことを確認する必要があります。

HYCUをデータにアクセスさせる必要がある場合のデータ保護シナリオの詳細については、“データへのアクセスの有効化” ページ79を参照してください。

考慮事項

- バイナリプログラムやスクリプトが実行されるたびに、ファイルの新しいコピーが使用されます。ファイル名の一部はUUIDであり、新しいUUIDが毎回生成されます。
- ウイルス対策プログラムがHYCUの操作を妨害している場合、Windowsシステムでは、`%ProgramData%\hycu`に保存されているHYCUファイルのうち、拡張子がないものや、次の

拡張子を持つものを除外してください。.bat、.cmd、.exe、.json、.log、.ps1、.txt、または.xml。

HYCUのNutanix AHVクラスターへの展開

HYCU仮想アプライアンスは、Nutanix Prism Webコンソールを使用して、Nutanix AHV クラスターに簡単に展開できる仮想ディスクイメージとして配布されます。

前提条件

バックアップインフラストラクチャが、"HYCUバックアップインフラストラクチャのリソースのサイジング" ページ17に説明されている要件に従ってサイズ指定されている。

考慮事項

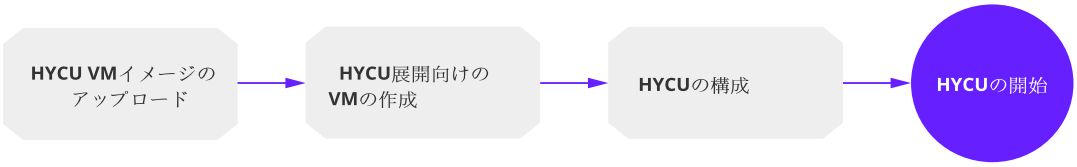
HYCUのNutanix AHVクラスターへの展開の説明は、Nutanix Mineクラスターにも適用されます。

展開タスク

HYCUをNutanix AHVクラスターに展開するときに、以下のタスクを実行する必要があります。

タスク	説明
1. HYCU仮想アプライアンスイメージをNutanix AHVクラスターにアップロード。	"HYCU仮想アプライアンスイメージのNutanix AHVクラスターへのアップロード" 下
2. HYCU展開のための仮想マシンを作成。	"Nutanix AHVクラスター上でのHYCU展開のための仮想マシンの作成" 次のページ
3. HYCUを、作成された仮想マシン上で構成します。	"仮想マシン上でのHYCUの構成" ページ25

以下のフローチャートは、HYCU展開タスクの概要を示しています。



参照 :図2-1 :展開タスクの概要

HYCU仮想アプライアンスイメージのNutanix AHVクラスターへのアップロード

手順

1. Nutanix Prism Webコンソールにログオンします。
2. メニューバーで、⚙をクリックし、「**イメージ構成**」を選択します。
3. 「イメージ構成」ダイアログボックスで、「**イメージのアップロード**」をクリックします。

4. 「イメージの作成」ダイアログボックスで、以下の情報を入力します。
   a. HYCUイメージ名を、アップロードするHYCUイメージファイルの名前に対応する形式で入力します。

      > ⚠ **重要** HYCU仮想アプライアンスイメージは、以下の形式でNutanix AHVクラスターにアップロードする必要があります。
      >
      > hycu-<*Version*>-<*Revision*>
      >
      > 例 :hycu-4.5.0-3634
      >
      > 別の形式でHYCUイメージ名を入力すると、アップグレードにはそのイメージを使用できません。

   b. *オプション :* 注釈を入力します。
   c. 「イメージのタイプ」ドロップダウンメニューから、「**ディスク**」を選択します。
   d. 「ストレージコンテナ」ドロップダウンメニューから、アップロードするイメージのストレージコンテナを選択します。
   e. 「イメージのソース」セクションから、イメージファイルの場所を指定します。
5. 「**保存**」をクリックします。
6. 画像が正常にアップロードされたら、「**閉じる**」をクリックします。

Nutanix AHVクラスター上でのHYCU展開のための仮想マシンの作成

手順

1. Nutanix Prism Webコンソールのメニューバーで、「**ホーム**」をクリックし、「**VM**」を選択します。
2. 画面の右上の「**VMの作成**」をクリックします。
3. 「VMの作成」ダイアログボックスで、以下の情報を入力します。
   a. 「全般構成」セクションで、次の手順を実行します。
      i. 仮想マシンの名前と、その説明(オプション)を入力します。
      ii. 必要に応じてタイムゾーンを設定します。
      iii. 「このVMをエージェントVMとして使用」チェックボックスのチェックは外したままにしておきます。
   b. 「詳細の計算」セクションで、仮想CPUの数と仮想CPU当たりのコアの数、およびこの仮想マシンに割り当てるメモリの量を入力します。
   c. 「ディスク」セクションで、「**新規ディスクの追加**」をクリックし、「ディスクの追加」ダイアログボックスで、以下のようにシステムディスクを指定します。
      i. 「タイプ」ドロップダウンメニューから、「**ディスク**」を選択します。
      ii. 「操作」ドロップダウンメニューから、「**イメージサービスからクローン**」を選択します。
      iii. 「バスタイプ」ドロップダウンメニューから、「**SCSI**」を選択します。
      iv. 「イメージ」ドロップダウンメニューから、アップロードしたイメージを選択します。

v. 「容量(GiB) 」フィールドでは、システムディスクの既定サイズ(10 GiB) はそのままにしておきます。

> 注 システムディスクのサイズは、必要であれば後で増やすことができます。詳細については、“Nutanix AHVクラスターでのHYCUディスクのサイズの増分” ページ268を参照してください。

vi. 「**追加**」をクリックします。

d. 「ディスク」セクションで、「**新規ディスクの追加**」をクリックし、「ディスクの追加」ダイアログボックスで、以下のようにデータディスクを指定します。

i. ストレージデバイスのタイプ、デバイスコンテンツ、およびバスタイプの既定値は、そのままにしておきます。

ii. 「ストレージコンテナ」ドロップダウンメニューから、アップロードするイメージのストレージコンテナを選択します。

iii. 「容量(GiB) 」フィールドに、32を入力します。

> 注 データディスクのサイズは、必要であれば後で増やすことができます。詳細については、“Nutanix AHVクラスターでのHYCUディスクのサイズの増分” ページ268を参照してください。

iv. 「**追加**」をクリックします。

4. 「ネットワークアダプタ(NIC) 」セクションで、「**新規NICの追加**」をクリックし、「NICの作成」ダイアログボックスで、次の手順を実行します。

a. 「VLAN名」ドロップダウンメニューから、「VLAN」を選択します。

b. 「**追加**」をクリックします。

5. 「**保存**」をクリックします。

仮想マシン上でのHYCUの構成

手順

1. Nutanix Prism Webコンソールの仮想マシンのリストから、作成したものを1つ選択し、「**電源オン**」をクリックします。
2. 仮想マシンをオンにして、「**コンソールの起動**」をクリックします。
3. 開かれた「HYCUモード選択」ダイアログボックスで、以下のいずれかの展開モードを選択します。
   - **HYCUバックアップコントローラー**
   - **HYCUインスタンス**
   - **HYCU Manager**

   展開モードの詳細については、“展開モード” ページ16を参照してください。
4. 「**OK**」に移動し、**Enter**を押します。
5. 開かれた「ネットワーク設定」ダイアログボックスで、次の手順を実行します。

a. 以下の値を入力します。

- *オプション:*仮想マシンのホスト名

  既定のホスト名は、HYCU仮想アプライアンスの展開中に自動的に生成されます。カスタムホスト名を使用する場合は、以下に注意してください。

  - *HYCU Backup ControllerまたはHYCU Managerモードを選択した場合のみ*。ホスト名の先頭は文字でなければならず、使用できるのは文字、数字、ハイフン(-) のみです。
  - *HYCUインスタンスモードを選択した場合のみ*。ホスト名の命名規則については、"HYCUインスタンスの管理" ページ220を参照してください。

- IPv4アドレス(例 :`10.1.100.1`)
- サブネットマスク(例 :`255.0.0.0`)
- 既定のゲートウェイ(例 :`10.1.1.1`)
- *オプション:*DNSサーバー(例 :`10.1.1.5`)
- *オプション:*検索ドメイン(例 :`domain.com`)

> 注ドメイン名の先頭は文字でなければならず、1つ以上のピリオドを含める必要があります。また、使用できるのは文字、数字、ハイフン(-) のみです。

b. 「**OK**」に移動し、**Enter**を押します。

HYCU構成の進行状況が表示されます。

6. *HYCUを「HYCUインスタンス」モードで展開する場合のみ*。開かれた「HYCUバックアップコントローラー」ダイアログボックスで、HYCUのアクセスに使用するHYCU Backup Controller URL、ユーザー名、およびパスワードを入力します。

> ⚠ 重要HYCU Backup Controllerホスト名をHYCUインスタンスから解決できない場合(たとえば、DNSサーバーを使用しない環境内である場合) には、必ずIPアドレスを使用します。
>
> `https://<IPAddress>:<Port>`

HYCU Backup Controller割り当ての進捗が表示されます。

7. HYCUが構成されたら、**Enter**を押して要約メッセージを確認します。

HYCUは試用ライセンスですぐに使い始めることができます。このライセンスは30日後に自動的に失効し、再利用はできません。したがって、使い始めてから30日以内に有効なライセンスを取得してください。手順については、"ライセンス" ページ222を参照してください。

HYCUのNutanix ESXiクラスターまたはvSphere環境への展開

HYCU仮想アプライアンスは、Nutanix ESXiクラスターまたはvSphere環境にvSphere (Web) Clientを使用して簡単に展開できるOPVFパッケージとして配布されます。

> ⚠ 重要 特に記述がない限り、このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

前提条件

- バックアップインフラストラクチャが、"HYCUバックアップインフラストラクチャのリソースのサイジング" ページ17に説明されている要件に従ってサイズ指定されている。
- *HYCUを「HYCUインスタンス」モードで展開する場合*: お使いのVMware vSphereバージョンが6.7 Update 3g以降の場合は、vSphere Web ClientまたはvSphere Clientを使用して展開できる。それ以外の場合は、必ずvSphere Web Clientを使用する。

考慮事項

以下は、HYCU Backup Controller時刻同期に適用されます。

- *VMware vSphereバージョン6.7および7.0の場合*: HYCU Backup Controllerは、vCenter Serverで構成されたタイムゾーンを使用します。システムのタイムゾーンと時刻同期の構成方法の詳細については、VMwareの資料を参照してください。
- *VMware vSphereバージョン6.5の場合*: タイムゾーンはUTCに設定されます。

手順

1. vSphere Web Clientにログオンします。
2. vCenter Serverを右クリックし、「**OVFテンプレートの展開...**」を選択します。「OVFテンプレートの展開」ダイアログボックスが開きます。
3. 「テンプレートの選択」セクションで、以下のようにOVFパッケージの場所を選択します。

URL	HYCU OVFパッケージのURLを指定します。
Local file	HYCU OVFパッケージのファイルシステムを参照します。 ⚠ 重要 ファイルシステムを参照するときには、`.ovf`ファイルと、OVFパッケージに関連した`.vmdk`ファイルの両方を必ず選択します。

「**次へ**」をクリックします。

4. 「名前とロケーションの選択」セクションで、HYCU仮想マシンの名前を入力し、展開する場所を指定し、「**次へ**」をクリックします。
5. 「リソースの選択」セクションで、展開されたパッケージを実行する場所を選択し、「**次へ**」をクリックします。
6. 「詳細の確認」セクションで、パッケージの詳細を確認し、「**次へ**」をクリックします。
7. 「構成の選択」セクションで、次の手順を実行します。
   a. 展開構成を選択します。
      - **HYCUバックアップコントローラー**
      - **HYCUインスタンス**

- **HYCU Manager**

展開モードの詳細については、"展開モード" ページ16を参照してください。

b. 「**次へ**」をクリックします。

8. 「ストレージの選択」セクションで、展開されたパッケージのファイルを保存する場所を選択し、「**次へ**」をクリックします。
9. 「ネットワークの選択」セクションで、既定値はそのままにして、「**次へ**」をクリックします。
10. 「テンプレートのカスタマイズ」セクションで、以下の値を入力します。
    - *オプション*:仮想マシンのホスト名

      既定のホスト名は、HYCU仮想アプライアンスの展開中に自動的に生成されます。カスタムホスト名を使用する場合は、以下に注意してください。

      - *HYCU Backup ControllerまたはHYCU Managerモードを選択した場合のみ*。ホスト名の先頭は文字でなければならず、使用できるのは文字、数字、ハイフン(-) のみです。
      - *HYCUインスタンスモードを選択した場合のみ*。ホスト名の命名規則については、"HYCUインスタンスの管理" ページ220を参照してください。
    - IPv4アドレス(例 :`10.1.100.1`)
    - サブネットマスク(例 :`255.0.0.0`)
    - 既定のゲートウェイ(例 :`10.1.1.1`)
    - *オプション*:DNSサーバー(例 :`10.1.1.5`)
    - *オプション*:検索ドメイン(例 :`domain.com`)

      > 注 ドメイン名の先頭は文字でなければならず、1つ以上のピリオドを含める必要があります。また、使用できるのは文字、数字、ハイフン(-) のみです。

    - *HYCUを「HYCUインスタンス」モードで展開する場合のみ*。
      - HYCU Backup Controller URL

        > ⚠ 重要 HYCU Backup Controllerホスト名をHYCUインスタンスから解決できない場合(たとえば、DNSサーバーを使用しない環境内である場合) には、必ずIPアドレスを使用します。
        >
        > `https://<IPAddress>:<Port>`

      - HYCU Backup Controllerユーザー
      - HYCU Backup Controllerパスワード

    「**次へ**」をクリックします。
11. 「終了可能」セクションで、データを確認し、「**終了**」をクリックします。

    > 注 仮想マシンの作成にはしばらく時間がかかる場合があります。「電源オン」オプションは、仮想マシンの作成後にのみ有効になります。

12. 仮想マシンのリストから、新しく作成した仮想マシンを右クリックし、「**電源**」>「**電源オン**」を選択してオンにします。

HYCUは試用ライセンスですぐに使い始めることができます。このライセンスは30日後に自動的に失効し、再利用はできません。したがって、使い始めてから30日以内に有効なライセンスを取得してください。手順については、"ライセンス" ページ222を参照してください。

HYCUへのログオン

HYCU仮想アプライアンスを正常に展開したら、サポートされるWebブラウザーを使用して、HYCUにアクセスできます。サポートされるWebブラウザーのリストについては、*HYCU互換性マトリックス*を参照してください。

手順

1. サポートされるブラウザーで、以下のURLを入力します。

   ```
   https://<ServerName>:8443
   ```

   この場合、<*ServerName*>はHYCUサーバーの完全修飾ドメイン名です。

   例：

   ```
   https://hycu.example.com:8443
   ```

2. ログオンページで、HYCUへのログオン方法に応じて、次のいずれかを実行します。

   - *HYCUに専用のログオン資格情報を使用することによって*。ログオン名とパスワードを入力します。

     HYCUへの初回アクセスには、既定のユーザー名(admin)とパスワード(admin)を使用できます。セキュリティ上の目的で、既定のパスワードは変更することを強くお勧めします。

   - *IDプロバイダーを使用して*。希望するIDプロバイダーをクリックし、必要に応じて資格情報を入力します。

     HYCUとIDプロバイダーを統合する方法の詳細については、"HYCUとIDプロバイダーの統合" ページ216を参照してください。

3. *アカウントで2要素認証が有効になっている場合のみ*。適切な2要素資格情報を入力します。

   - *時間ベースのワンタイムパスワード(OTP)を使用する場合*:認証アプリケーション(Google認証システムまたは互換性のあるアプリケーションなど)によって生成された、6桁の認証コードを入力します。

     アカウントで2要素認証を有効にした後の初回のログオン時に、OTPバックアップコードが表示されます。選択した認証アプリケーションで、QRコードを読み取るか、OTPバックアップコードを手動で入力し、認証アプリケーションで生成された認証符号を「認証符号」フィールドに入力します。

   - *FIDO認証システムを使用する場合*:セキュリティダイアログボックスが表示され、認証することが求められます(たとえば、キーを挿入するなど)。説明に従ってアカウントを認証します。

     アカウントに対して2要素認証を有効にした後の初回のログオン時には、セキュリティダイアログボックスが表示され、認証システム(セキュリティキーや指紋リーダーなど)をセットアップすることが求められます。手順は、選択した認証システムとオペレーティングシステムによって異な

ります。説明に従って認証システムをセットアップします。詳細については、"FIDO認証システムの管理" ページ264を参照してください。

> 注 アクセスのレベルは、ユーザー権限に応じたものになることに注意してください。詳細については、"ユーザーの管理" ページ197を参照してください。

HYCU Webユーザーインターフェースにログオンしたら、環境を構成して、HYCUコマンドラインインターフェース(hyCLI) も使用することができます。詳細については、"コマンドラインインターフェースの使用" ページ272を参照してください。

言語の設定

HYCU Webユーザーインターフェースや HYCU Managerコンソールにアクセスすると、お使いのブラウザーの言語が検出され、サポートされている言語の場合はユーザーインターフェースがその言語で表示されます。ブラウザーの言語がサポートされていない場合、ユーザーインターフェースは英語で表示されます。サポートされている言語のリストについては、*HYCU互換性マトリックス*を参照してください。

考慮事項

HYCU REST APIエクスプローラーおよびHYCUコマンドラインユーザーインターフェース(hyCLI) は英語でのみ使用可能です。

手順

- インフラストラクチャまたはセルフサービスグループの管理者は、ユーザーが使用する言語を設定できます。説明については、"ユーザーの作成" ページ201を参照してください。
- 現在ログオンしているユーザーは、使用する言語を「プロファイルの更新」オプションで設定できます。説明については、"ユーザープロファイルの更新" ページ208を参照してください。
- イベントが発生したときに送信される通知の言語を設定できます。説明については、"イベント通知の構成" ページ166を参照してください。

また、HYCU Webユーザーインターフェースや HYCU Managerコンソールへのアクセスに使用するURLにLANG属性を追加すると、ユーザーインターフェースの言語を変更できます。例：

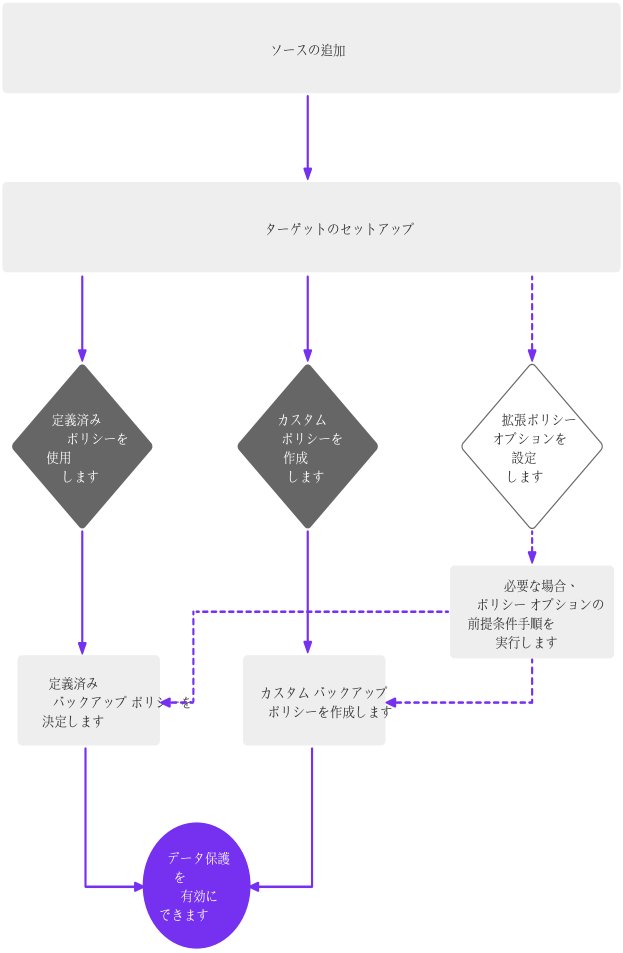
```
https://hycu.example.com:8443/#!/login?lang=JA
```

第3章

データ保護環境の確立

HYCU仮想アプライアンスを展開してHYCUにログオンしたら、データが効果的に保護されるデータ保護環境を構築する必要があります。データ保護環境の構築には、ソースの追加、ターゲットのセットアップ、および環境にカスタムポリシーが必要な場合はそれを作成することが含まれます。

次のフローチャートは、データ保護環境を確立するために実行する必要があるタスクを説明しています。



参照 :図3-1 :データ保護環境の確立

データ保護環境を確立するために必要なタスクは、インフラストラクチャグループ管理者のみが実行でき、次のとおりです。

- “ソースの追加” 下
- “ターゲットのセットアップ” ページ38

HYCUの定義済みポリシーを使用して、データ保護を有効にできます。それらのいずれも使用したくない場合は、必ず独自のポリシーを作成してください。詳細については、“ポリシーの作成” ページ60を参照してください。

データ保護環境が準備できたら、任意のビジネス要件を満たすために、いくつかの方法でデータ保護を実現できます。

> 注 データ保護環境の保護を開始する前に、HYCU Backup Controllerが保護されていることを確認します。これにより、災害時にデータ保護アクティビティを迅速に復元および再開できます。詳細については、“災害復旧の準備” ページ74を参照してください。

ソースの追加

HYCUがデータ保護を提供する環境は、保護するデータの種類に応じてHYCUに追加する1つ以上のソースで構成されます。保護する対象には、Nutanixクラスターまたはvsphere環境の仮想マシンで実行される仮想マシンまたはアプリケーション、ファイルサーバー上のファイル共有、Nutanixクラスター上のボリュームグループ、または物理マシンと物理マシンで実行されているアプリケーションなどがあります。特定のソースを追加する方法については、以下のいずれかのセクションを参照してください。

- “Nutanixクラスターの追加” 下
- “vCenter Serverの追加” ページ34
- “ファイルサーバーの追加” ページ35
- “物理マシンの追加” ページ38

> ⚠ 重要 データ保護環境の最適なパフォーマンスを実現し、復元性を確保するには、HYCU Backup Controllerが実行されているソースをHYCUに追加します。

Nutanixクラスターの追加

Nutanix環境は、HYCUがデータ保護を提供するエンティティ(アプリケーションを実行する仮想マシンとボリュームグループ) をホストする1つまたは複数のNutanixクラスターで構成されています。Nutanixクラスターをhycuに追加することは、データを保護するための最初の手順です。

前提条件

- *Nutanix ESXiクラスターの場合 :*クラスターが、Prism Webコンソールを介してvCenter Serverに登録されている。この実行方法の詳細については、Nutanixの資料を参照してください。
- *ポリシーの自動割り当てを使用する場合のみ。*ポリシーを自動的に割り当てる仮想マシンをホストするNutanix AHVクラスターが、Prism Centralに登録されている。この実行方法の詳細については、Nutanixの資料を参照してください。ポリシーの自動割り当ての詳細については、“自動ポリシー割り当てのセットアップ” ページ69を参照してください。

考慮事項

- *Nutanix ESXiクラスターの場合：*
  - 仮想マシンの管理には必ずNutanix Prism Webコンソールを使用してください。
  - Windows仮想マシンは必ず一定時間後にスリープモードにならないように構成します。そうしないと、ネットワーク設定が認識されなくなり、そのような仮想マシンはHYCUで保護できなくなります。
- リモートオフィス/ブランチオフィス(ROBO) 環境のレプリカから仮想マシンおよびボリュームグループをバックアップするには、中央サイトNutanixクラスターとブランチオフィスサイトクラスターの両方を追加する必要があります。

推奨事項

パフォーマンスを向上させるためには、iSCSIデータサービスIPアドレスをHYCUに追加しようとしているNutanixクラスターで指定することをお勧めします。これにより、データ保護操作中にNutanixロードバランシング機能が自動的に有効になり、Nutanixクラスターとストレージコンテナの過度なI/O負荷はなくなります。iSCSIデータサービスIPアドレスの指定方法の詳細については、Nutanixの資料を参照してください。

> 「ソース」ダイアログボックスへのアクセス
>
> 「ソース」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ソース**」を選択します。

手順

1. 「ソース」ダイアログボックスで、「**ハイパーバイザー**」タブをクリックし、「**＋ 新規**」をクリックします。
2. 以下のURL形式でNutanixクラスターの名前を入力します。

   `https://<ServerName>:<Port>`
3. クラスター管理権限を持つユーザーのユーザー名とパスワードを入力します。

   > ⚠ 重要 クライアント認証が有効になっているNutanixクラスターを追加する場合は、必ずローカルユーザーを指定します。
4. *HYCUを追加するNutanixクラスター上でクライアント認証が有効になっている場合のみ。*「**証明書認証を有効にする**」スイッチを使用し、信頼されたCA証明書、クライアント証明書、およびクライアント秘密鍵を参照してアップロードします。以下に注意してください。
   - サポートされる証明書ファイル形式はPKCS#1とPKCS#8です。
   - 秘密鍵は暗号化しないでください。

   > 注 Conjurを使用してHYCUのシークレットを管理する場合、ファイルを参照する代わりにシークレットを提供するのであれば、「**シークレットマネージャーから値を取得**」を有効にすることができます。シークレットの管理の詳細については、“シークレットの管理” ページ231を参照してください。

   証明書認証を有効にすることによって、HYCUがNutanixクラスターに接続することを許可します。

5. 「**次へ**」をクリックし、追加するNutanixクラスターのタイプに応じて、以下を実行します。

Nutanixクラスターのタイプ	説明
Nutanix AHVクラスター	ポリシーの自動割り当てを使用する場合、「Prism Centralの新規資格情報」ダイアログボックスで、Nutanix AHVクラスターが登録されているPrism CentralのURL、およびクラスター管理者権限を持つユーザーのユーザー名とパスワードを指定します。そうでない場合は、すべてのフィールドを空白のままにします。「**次へ**」をクリックします。 ポリシーの自動割り当ての詳細については、“自動ポリシー割り当てのセットアップ” ページ69を参照してください。
Nutanix ESXiクラスター	「vSphereの新規資格情報」ダイアログボックスで、クラスターが登録されているvCenter ServerのURLと、vCenter Serverの特定の特権を持つユーザーのユーザー名とパスワードを指定して、vSphere資格情報をNutanix ESXiクラスターに割り当てます。「**次へ**」をクリックします。 注 Nutanix ESXiクラスターを追加すると、そのタイプの横に、必要なvCenter Server許可があることを示すvcアイコンが表示されます。

6. 「概要」ダイアログボックスで、検証が正常に実行されたことを確認し、「**保存**」をクリックします。

既存のNutanixクラスターはいずれも編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。Nutanixクラスターを削除する際は、以下について考慮してください。

- 「**スナップショットの削除**」スイッチを使用すると、HYCUにより作成されたスナップショットを削除するか維持するか選べます。
- Nutanixクラスターは、依存関係がなければ削除できます。そのため、ポリシーで中央サイトクラスターとして指定されているNutanixクラスターや、検証ポリシーで指定されているストレージコンテナをホストするNutanixクラスターは、その依存関係がすべて削除されるまで削除できません。

vCenter Serverの追加

vSphere環境は、vCenter Serverによって管理されるESXiホストで構成されます。これらの各ESXiホストには、アプリケーションを実行する一連の仮想マシンが存在します。1つ以上のvCenter ServerをHYCUに追加することは、仮想マシンデータを保護するための最初のステップです。

前提条件

vCenter Serverの特定の特権を持つユーザーが指定されている。どの特権をvSphereユーザーに割り当てるべきかの詳細については、“vSphereユーザーへの特権の割り当て” ページ269を参照してください。

制限事項

vCloud DirectorまたはスタンドアロンESXiホストの追加はサポートされていません。

> 「ソース」ダイアログボックスへのアクセス
>
> 「ソース」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ソース**」を選択します。

手順

1. 「ソース」ダイアログボックスで、「**ハイパーバイザー**」タブをクリックし、「＋ **新規**」をクリックします。
2. 以下のURL形式でvCenter Serverの名前を入力します。

   `https://<vCenterServerFQDN>:<Port>`

   vCenter Serverの既定のポートは443です。

   > ⚠ **重要** 必ずHYCUがこのFQDNを解決できるような仕方でHYCU DNS設定を構成します。そのために、バックアップに含める仮想マシンが実行されているvCenter ServerおよびESXiホストに接続します。

3. vCenter Serverの特定の特権を持つユーザーのユーザー名とパスワードを入力します。
4. 「**保存**」をクリックします。

既存のvCenter Serverはいずれも編集することができます(「✎ **編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「🗑 **削除**」をクリックします)。

ファイルサーバーの追加

HYCUを使用すると、ファイルサーバー上のSMBおよびNFSファイル共有を保護できます。バックアップに含めるファイル共有をホストするファイルサーバーを1つ以上追加できます。サポートされるファイルサーバーの情報については、*HYCU互換性マトリックス*を参照してください。

ファイル共有を保護するために、データ保護環境にHYCUインスタンスが導入されています。HYCUインスタンスは、ファイルサーバーのデータ保護操作を実行するためにHYCUが使用する仮想マシンであり、HYCU Backup Controllerの負荷を軽減します。ビジネスの要件に応じて、データ保護環境に1つ以上のHYCUインスタンスを持つことができます。HYCUインスタンスの詳細については、“HYCUインスタンス” ページ37を参照してください。

前提条件

HYCUはファイルサーバーにアクセスできます。HYCUがNutanix Filesサーバーにアクセスできるようにする方法については、“HYCUのNutanix Filesサーバーへのアクセスの有効化” 次のページを参照してください。

制限事項

PowerScale OneFSサーバーを追加する場合のみ。ファイルサーバーのURLを入力する場合、ホスト名またはIPアドレスは、個々のクラスターノードのホスト名または外部IPアドレスに対応している必要があります。Smartconnect IPアドレスやホスト名を使用することは、PowerScale OneFSとセッションベース認証の制限によりサポートされていません。

> 「ソース」ダイアログボックスへのアクセス

「ソース」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ソース**」を選択します。

手順

1. 「ソース」ダイアログボックスで、「**ファイルサーバー**」タブをクリックし、「＋ **新規**」をクリックします。
2. 以下の形式で、ファイルサーバーの名前またはIPアドレスを入力します。

   `https://<FileServerHostname/IP>:<Port>`

   既定値を使用する場合、ポートの入力はオプションです。Nutanix Filesの場合は9440、PowerScale OneFSの場合は8080です。

   > ⚠ **重要** ファイルサーバーの名前を入力する場合は、必ず固有の名前にします。

3. ファイルサーバーのREST APIアクセスのために、サーバー管理権限を持つユーザーのユーザー名とパスワードを指定します。

   Nutanix Filesサーバーのこのタイプのユーザーを作成する方法については、"HYCUのNutanix Filesサーバーへのアクセスの有効化" 下を参照してください。

4. SMBファイル共有を保護する場合は、「**共有フォルダへのアクセスにはSMBプロトコルを使用する**」スイッチを使用し、「SMBバックアップ資格情報」セクションで、ファイルサーバー内のすべてのSMBファイル共有へのアクセス権があるサーバーまたはバックアップ管理者のユーザー名とパスワードを入力します。

   > 📋 **注** 資格情報を各共有に個別に割り当てることはできません。

5. NFSファイル共有を保護する予定の場合は、「**共有フォルダへのアクセスにはNFSv4プロトコルを使用する**」スイッチを使用します。
6. 「**保存**」をクリックします。

後で以下を実行できます。

- いずれかの既存のファイルサーバーを編集します。これを実行するには、ファイルサーバーを選択し、「✎ **編集**」をクリックし、必要な変更を行い、「**保存**」をクリックします。
- 不要になったファイルサーバーを次のように削除します。
  a. ファイルサーバーを選択し、「🗑 **削除**」をクリックし、以下を実行します。
     - 対応するHYCUインスタンスも削除する場合は、「**使用されていないHYCUインスタンスを削除します**」スイッチを使用します。
     - HYCUにより作成されたスナップショットを削除する場合は、「**スナップショットの削除**」スイッチを使用します。

  b. 「**はい**」をクリックします。

HYCUのNutanix Filesサーバーへのアクセスの有効化

HYCUがNutanix Filesサーバーにアクセスできるようにするには、着信REST API要求を検証するために、Nutanix Files環境を準備する必要があります。

> 📋 **注** Nutanix Prismの一部のバージョンでは、「ロールの管理」ダイアログボックスでREST APIアクセス許可を管理できます。詳細については、Nutanixの資料を参照してください。

このダイアログボックスが利用できない場合は、REST APIにアクセスするために新規ユーザーを作成します。これを実行するには、次の手順に従います。

1. Nutanixクラスターへの接続を確立します。

```
ssh @<NutanixClusterHostname>
```

2. `ncli fs list`コマンドを実行して、ファイルサーバーのUUIDをリストします。
3. 新しいユーザーを以下のように作成します。

```
ncli fs add-user uuid=<UUIDFromStep2> user=<Username>
password=<Password>
```

HYCUインスタンス

ファイル共有の保護を開始する前に、HYCU Backup Controllerには、データ保護操作を実行する少なくとも1つの接続されたHYCUインスタンスが必要です。

1つ以上のHYCUインスタンスを持つことができます。複数のHYCUインスタンスを持つことは、データ保護操作を実行するときにHYCUインスタンスがそれらの間で負荷を共有できる多数のファイル共有がある環境で特に役立ちます。複数のHYCUインスタンスに負荷を分散させる場合、HYCUは、HYCU Backup ControllerおよびファイルサーバーとHYCU Nutanixクラスター上で実行されているHYCUインスタンスに自動的に優先順位を付けます。ただし、`afs.instance.afs.cluster.priority`または`afs.instance.bc.cluster.priority`構成設定を変更することにより、負荷分散プロセスを要件に合わせて調整できます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

HYCUインスタンスを、以下のいずれかの方法で作成できます。

- HYCU仮想アプライアンスの展開および「HYCUインスタンス」モードの選択によって。詳細については、"HYCU仮想アプライアンスの展開" ページ16を参照してください。
- HYCU Webユーザーインターフェースの使用によって。詳細については、"HYCU Webユーザーインターフェースの使用によるHYCUインスタンスの作成" ページ220を参照してください。

考慮事項

- ファイルサーバーをHYCUに追加する前または後のどちらでもHYCUインスタンスを作成できます。
- 作成されたHYCUインスタンスは、対応するHYCU Backup Controllerに自動的に接続します。
- 各HYCUインスタンスは、既定では、16 GiBのRAM、1 CPU、8 CPUコア、および64 GiBのデータディスクサイズで作成されます。ただし、`afs.instance.memory.mb`、`afs.instance.cpu`、`afs.instance.cores.per.cpu`、および`afs.instance.datadisk.size.gb`構成設定を目的の値に設定することにより、これを上書きできます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。
- HYCU Backup Controllerのホスト名またはIPアドレスを変更する場合、接続されているすべてのHYCUインスタンスでも変更する必要があります。接続されている各HYCUインスタンスで、`/hycudata/opt/grizzly/config.properties`ファイル内の`catalog.master.url`構成設定を更新します。

後でHYCUインスタンスをデータ保護環境から削除することにした場合は、“HYCUインスタンスの削除” ページ221での説明に従ってそれを実行できます。

物理マシンの追加

1つ以上の物理マシンをHYCUに追加することは、物理マシンデータを保護するための最初のステップです。

> 「ソース」ダイアログボックスへのアクセス
>
> 「ソース」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ソース**」を選択します。

手順

1. 「ソース」ダイアログボックスで、「**物理マシン**」タブをクリックし、「＋ **新規**」をクリックします。
2. 物理マシンの名前を入力します。
3. 物理マシンのホスト名またはIPアドレスを入力します。
4. 「**保存**」をクリックします。

既存の物理マシンはいずれも編集することができます(「🖉 **編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「🗑 **削除**」をクリックします)。

> 注 HYCUから物理マシンを削除してから(同じ名前とIPアドレスで)再度追加する場合、この物理マシンは新しいものとして扱われるため、古い復元ポイントは使用できないことに注意してください。

ターゲットのセットアップ

ターゲットは、保護されたデータが保存される場所です。HYCUでは、次のタイプのターゲットにデータを保存できます。NFS、SMB、Nutanix、Nutanix Objects、iSCSI、AWS S3/互換、Azure、Google Cloud、およびテープ。

> 注 ファイルサーバー共有は、NFSまたはSMBのターゲットとして使用できます。ファイルサーバーをターゲットとしてのみ使用し、ソースとして使用しない予定であれば、HYCUに追加する必要はありません。

ターゲットをセットアップする方法は、さまざまなターゲットタイプに共通です。ただし、各ターゲットタイプに必要な特定の前提条件と手順があります。セットアップするターゲットに応じて、次のいずれかのセクションを参照してください。

- “NFSターゲットのセットアップ” 次のページ
- “SMBターゲットのセットアップ” ページ41
- “Nutanixターゲットのセットアップ” ページ43
- “Nutanix Objectsターゲットのセットアップ” ページ45
- “iSCSIターゲットのセットアップ” ページ47
- “AWS S3/Compatibleターゲットのセットアップ” ページ49
- “Azureターゲットのセットアップ” ページ51

- “Google Cloudターゲットのセットアップ” ページ53
- “テープターゲットのセットアップ” ページ56

NFSターゲットのセットアップ

前提条件

- サービスが構成され、HYCU Backup ControllerとHYCUインスタンスにアクセス可能である。
- データを保存するための十分な空きスペースがターゲット上にある。
- ターゲットで重複排除が有効である場合、ターゲットはHYCUバックアップ専用とする。ターゲットをHYCUバックアップ専用にすることにより、正確なストレージ使用率レポートが提供されます。
- ターゲットがWindows上にある場合は、`Everyone`のローカル許可(セキュリティ)は`Full Control`に設定されます。HYCUのみにこのシステムへのアクセスを制限する場合は、この目的でHYCU Backup Controller IPアドレスを使用します。
- *物理マシンデータを保護する場合*:ターゲットは物理マシンからアクセスできます。

制限事項

- ファイル共有のターゲット圧縮はサポートされません。
- *物理マシンデータを保護する場合*:
  - このタイプのターゲットにはLinux物理マシンのバックアップのみ保存できます。
  - ターゲットの暗号化と圧縮はサポートされません。

推奨事項

バックアップデータが保存されているターゲットには、パブリックアクセスを無効にすることを強くお勧めします。HYCUは、ターゲットに対してパブリックアクセスが有効になっているかどうかを自動的に検出し、データへのアクセスを制限するようにセキュリティ設定を調整することを促す警告メッセージを発行します。

> **「ターゲット」パネルへのアクセス**
>
> 「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. *オプション*:「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位)。ターゲットがHYCUバックアップ専用でない場合には、このフィールドは空欄にしておく必要があります。

   このフィールドを空欄にしておくと、HYCUはターゲットから利用可能なストレージ領域の量を取得します。

> 注 ターゲットで重複排除が有効である場合、ターゲットでのHYCUの必要なストレージ領域の見積もりは、ストレージメディアでの必要な実際の領域の量よりも高くなる可能性があります。したがって、そのような場合にはこのフィールドは空欄にしておくことをお勧めします。

4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。

5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

   > ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。

6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性があります。さらに、圧縮を有効にしてターゲットへの圧縮データのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。

7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

   > 注 ファイル共有データのアーカイブは既定ではターゲットから実行されるため、追加料金を回避するために、このオプションを有効にすることをお勧めします。

8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「タイプ」ドロップダウンメニューから、「**NFS**」を選択します。
10. NFSサーバー名またはIPアドレス、およびサーバーのルートからのNFS共有フォルダへのパスを入力します(たとえば、/backups/HYCU) 。
11. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

    > 注 ターゲットの暗号化を有効にする場合は、以下に注意してください。
    >
    > - それによって重複排除率が影響を受ける可能性があります(ターゲットで重複排除が有効である場合) 。
    > - 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、“暗号化キーのエクスポート” ページ215を参照してください。

12. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

SMBターゲットのセットアップ

前提条件

- サービスが構成され、HYCU Backup ControllerとHYCUインスタンスにアクセス可能である。
- データを保存するための十分な空きスペースがターゲット上にある。
- ターゲットで重複排除が有効である場合、ターゲットはHYCUバックアップ専用とする。ターゲットをHYCUバックアップ専用にすることにより、正確なストレージ使用率レポートが提供されます。
- サポートされるSMBバージョンが使用されている。サポートされるSMBのバージョンのリストについては、*HYCU互換性マトリックス*を参照してください。
- *物理マシンデータを保護する場合*:ターゲットは物理マシンからアクセスできます。

制限事項

- ファイル共有のターゲット圧縮はサポートされません。
- *物理マシンデータを保護する場合*:
  - このタイプのターゲットにはWindows物理マシンのバックアップのみ保存できます。
  - ターゲットの暗号化と圧縮はサポートされません。

推奨事項

バックアップデータが保存されているターゲットには、パブリックアクセスを無効にすることを強くお勧めします。HYCUは、ターゲットに対してパブリックアクセスが有効になっているかどうかを自動的に検出し、データへのアクセスを制限するようにセキュリティ設定を調整することを促す警告メッセージを発行します。

> 「ターゲット」パネルへのアクセス
>
> 「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. *オプション*:「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位)。ターゲットがHYCUバックアップ専用でない場合には、このフィールドは空欄にしておく必要があります。

   このフィールドを空欄にしておくと、HYCUはターゲットから利用可能なストレージ領域の量を取得します。

> 注 ターゲットで重複排除が有効である場合、ターゲットでのHYCUの必要なストレージ領域の見積もりは、ストレージメディアでの必要な実際の領域の量よりも高くなる可能性があります。したがって、そのような場合にはこのフィールドは空欄にしておくことをお勧めします。

4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。

5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

   > ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。

6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性があります。さらに、圧縮を有効にしてターゲットへの圧縮データのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。

7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

   > 注 ファイル共有データのアーカイブは既定ではターゲットから実行されるため、追加料金を回避するために、このオプションを有効にすることをお勧めします。

8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「タイプ」ドロップダウンメニューから、「**SMB**」を選択します。
10. *オプション* ドメインとユーザー資格情報を入力します。
11. SMBサーバー名またはIPアドレス、およびサーバーのルートからのSMB共有フォルダへのパスを入力します(たとえば、/backups/HYCU) 。
12. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

    > 注 ターゲットの暗号化を有効にする場合は、以下に注意してください。
    >
    > - それによって重複排除率が影響を受ける可能性があります(ターゲットで重複排除が有効である場合) 。
    > - 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、“暗号化キーのエクスポート” ページ215を参照してください。

13. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

Nutanixターゲットのセットアップ

前提条件

Nutanixターゲットが作成されるNutanixクラスターは、HYCU Backup Controllerにアクセスできる必要がある。

制限事項

- Nutanixターゲットは、ファイル共有データを保存するためには使用できません。
- 物理マシンのバックアップをこのタイプのターゲットに保存することはサポートされません。

考慮事項

- HYCUが自動的に作成し、Nutanixターゲットとして使用するNutanixクラスター上のストレージコンテナは、バックアップデータ保存の専用にする必要があります。このようなストレージコンテナの名前は先頭がHYCU-接頭語であるため、同じ接頭語を持つ独自のストレージコンテナは作成しないでください。これらのストレージコンテナは、データの復元、データの複製、およびHYCUインスタンスの作成時には宛先として使用できないことに注意してください。
- *Nutanix Mine with HYCUを採用することを予定している場合のみ*。Nutanixターゲットを追加する際に、まだ追加していない場合は、関連するNutanixクラスターをソースとしてHYCUに追加することもできます。
- *Nutanix Mine with HYCUの場合* .Nutanix Mine with HYCUダッシュボードで、NutanixターゲットはMineストレージとしてリストされます。

推奨事項

パフォーマンスを向上させるためには、Nutanixターゲットを作成するNutanixクラスターでiSCSIデータサービスIPアドレスを指定することをお勧めします。これにより、データ保護操作中にNutanixロードバランシング機能が自動的に有効になり、Nutanixクラスターとストレージコンテナの過度なI/O負荷はなくなります。iSCSIデータサービスIPアドレスの指定方法の詳細については、Nutanixの資料を参照してください。

> **「ターゲット」パネルへのアクセス**
>
> 「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。

3. *オプション*:「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位) 。

   このフィールドを空欄にしておくと、HYCUはターゲットから利用可能なストレージ領域の量を取得します。

4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。

5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

   > ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。

6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性があります。さらに、圧縮を有効にしてターゲットへの圧縮データのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。

7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。

9. 「タイプ」ドロップダウンメニューから、「**Nutanix**」を選択します

10. 以下のURL形式でNutanixクラスターの名前を入力します。

    `https://<ServerName>:<Port>`

11. クラスター管理権限を持つユーザーのユーザー名とパスワードを入力します。

    > ⚠ 重要 クライアント認証が有効になっているNutanixクラスターを追加する場合は、必ずローカルユーザーの資格情報を指定します。

12. ストレージコンテナでそれぞれのNutanixオプションを有効にして、Nutanixクラスターの有効なストレージ容量を増やす場合は、次のスイッチを1つ以上使用します。

    - **重複排除**
    - **イレージャーコーディング**
    - **ハードウェア圧縮**

    これらのオプションの詳細については、Nutanixの資料を参照してください。

13. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

> 注 ターゲットの暗号化を有効にする場合は、以下に注意してください。
> - クラスターの有効なストレージ容量を増やすことを目的としたオプションと組み合わせてターゲット暗号化を有効にしても、そのようなオプションは有効になりません。
> - 仮想マシン、アプリケーション、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、"暗号化キーのエクスポート" ページ215を参照してください。

14. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

Nutanix Objectsターゲットのセットアップ

前提条件

- サービスが構成され、アクセス可能である。
- 安全なHTTPSアクセスを提供するには、必要なCA署名付き証明書が以下のとおりインポートされていることを確認します。
  1. HYCU Backup Controller仮想マシンへのリモートセッションを開きます。

     ```
     ssh hycu@<HYCUBackupControllerIPAddress>
     ```

     要求されたら、既定のパスワードを入力します。
  2. 必要なCA署名付き証明書をインポートします。

     ```
     keytool -importcert -keystore /etc/pki/ca-
     trust/extracted/java/cacerts
     -file <CertificatePathname>
     ```

     ```
     keytool -importcert -keystore /etc/pki/cert-
     templates/cacerts.template
     -file <CertificatePathname>
     ```

制限事項

- ライフサイクルポリシーでHYCUオブジェクトとバージョンの有効期限が有効になっているターゲットへのバックアップデータの保存は、サポートされていません。
- ファイル共有のターゲット圧縮はサポートされません。
- 物理マシンのバックアップをこのタイプのターゲットに保存することはサポートされません。

考慮事項

WORMが有効なNutanix Objectsターゲットは、ターゲットのリストの  アイコンで表されます。

「ターゲット」パネルへのアクセス

「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. 「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位)。
4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。
5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

   > ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。
6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性があります。さらに、圧縮と圧縮データのアーカイブを有効にして、バックアップ、バックアップデータのコピー、およびターゲットへのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。
7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

   > 注 ファイル共有データのアーカイブは既定ではターゲットから実行されるため、追加料金を回避するために、このオプションを有効にすることをお勧めします。
8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「タイプ」ドロップダウンメニューから、「**Nutanix Objects**」を選択します
10. 以下の情報を提供します。

必須情報	注
サービスエンドポイント	HTTPまたはHTTPSプロトコルを含む、完全なサービスエンドポイン

必須情報	注
	トURLを入力する必要があります。
バケット名	バケットの名前を入力します。バケットが存在しない場合、それをHYCUが自動的に作成します。
アクセスキーID	アクセスキーIDとシークレットアクセスキーは、S3 REST APIサービスコールを認証するために使用されます。
秘密アクセスキー	

11. HYCUがパススタイルURL(`https://<ServiceEndpointURL>/<BucketName>`) を使用してバケットにアクセスする場合は、「**パススタイルアクセス**」スイッチを使用します。HYCUは、既定では仮想ホストスタイルURL(`https://<BucketName>.<ServiceEndpointURL>`) を使用します。
12. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

    > 注 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、"暗号化キーのエクスポート" ページ215を参照してください。

13. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

iSCSIターゲットのセットアップ

前提条件

- サービスが構成され、アクセス可能である。
- ターゲットがまだ初期化されていない。
- HYCU iSCSIイニシエーターの秘密は、HYCUとiSCSIサーバーの間の相互認証を有効にする場合に、iSCSIサーバー上に追加される。

制限事項

- iSCSIターゲットは、ファイル共有データを保存するためには使用できません。
- 物理マシンのバックアップをこのタイプのターゲットに保存することはサポートされません。

考慮事項

- 選択したiSCSIターゲット上に複数のボリュームが作成されている場合、HYCUはデータを保存するためにアクセスできるすべてのボリュームのディスクを使用します。
- iSCSIターゲットとして使用されるNutanixボリュームグループは、未使用のブロックを自動的に破棄します。他のタイプのiSCSIターゲットの場合、このオプションは手動で追加できます。詳細については、HYCUカスタマーサポートにお問い合わせください。

「ターゲット」パネルへのアクセス

「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. *オプション*:「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位)。

   このフィールドを空欄にしておくと、HYCUはターゲットから利用可能なストレージ領域の量を取得します。
4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。
5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

   > ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。
6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性があります。さらに、圧縮を有効にしてターゲットへの圧縮データのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。
7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。
8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「タイプ」ドロップダウンメニューから、「**iSCSI**」を選択します
10. ターゲットポータルIPアドレスとターゲット名を入力します。

    > 注 HYCU以外のソースからのデータがストレージデバイスに存在する場合、そのようなターゲットはHYCUバックアップに設定できません。
11. iSCSIサーバーがCHAP認証を必要とする場合には、CHAPセクションで、以下を実行します。

a. **CHAP**スイッチを使用してCHAP認証を有効にし、iSCSIサーバーにアクセスするユーザーアカウントのユーザー名とターゲットシークレット(セキュリティキー)を入力します。

b. iSCSIターゲットがHYCUによって認証されるようにする場合は、「**相互認証を実行**」スイッチを使用します。この場合、HYCU iSCSIイニシエーターの秘密はiSCSIサーバー上で指定される必要があります。iSCSIイニシエーターの秘密の設定の詳細については、"iSCSIイニシエーターシークレットの設定" ページ222を参照してください。

12. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

> ⚠ 重要 仮想マシン、アプリケーション、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、"暗号化キーのエクスポート" ページ215を参照してください。

13. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

AWS S3/Compatibleターゲットのセットアップ

前提条件

- サービスが構成され、アクセス可能である。
- S3バケットがAWSまたはその他サポート対象のS3互換環境で作成され、構成されている。サポート対象のS3互換クラウドストレージソリューションのリストについては、*HYCU互換性マトリックス*を参照してください。
- 以下は、指定する最低限必要なAWS S3許可です :`s3:GetObject`、`s3:GetObjectRetention`、`s3:DeleteObject`、`s3:PutObject`、`s3:ListBucket`、`s3:GetBucketAcl`、`s3:ListBucketMultipartUploads`、`s3:GetBucketLocation`、`s3:GetBucketObjectLockConfiguration`、`s3:DeleteObjectVersion`、`s3:ListBucketVersions`、および`s3:GetBucketVersioning`。
- *Amazon Virtual Private Cloud(VPC) のAWS S3ターゲットへのデータ保存を予定している場合のみ*。インターフェースVPCエンドポイントがセットアップされます。
- *S3互換ターゲットの場合* :安全なHTTPSアクセスを提供する場合は、CA証明書/チェーンをHYCUにインポートします。詳細については、"カスタム証明書のインポート" ページ235を参照してください。
- *Tencent Cloudターゲットのセットアップの場合* :サービスエンドポイントURLにバケット名が含まれていないことを確認します。たとえば、Tencent Cloudアクセスドメインが`https://testbucket-1234567890.cos.ap-chengdu.myqcloud.com`の場合、「HYCUサービスエンドポイント」フィールドに、バケット名なしでURLを入力します。

  `https://cos.ap-chengdu.myqcloud.com`

制限事項

- HYCUは、Glacierストレージクラスを使用するAWS S3ターゲットはサポートしていません。
- HYCUは現在、AWS S3 Signatureバージョン4のみをサポートしています。
- ライフサイクルポリシーでHYCUオブジェクトとバージョンの有効期限が有効になっているターゲットへのバックアップデータの保存は、サポートされていません。
- ファイル共有のターゲット圧縮はサポートされません。
- 物理マシンのバックアップをこのタイプのターゲットに保存することはサポートされません。

考慮事項

AWS S3またはCloudian S3互換ターゲットで、オブジェクトロック(WORM)が有効であるものは、ターゲットのリストではアイコンで表されます。

推奨事項

バックアップデータが保存されているターゲットには、パブリックアクセスを無効にすることを強くお勧めします。HYCUは、ターゲットに対してパブリックアクセスが有効になっているかどうかを自動的に検出し、データへのアクセスを制限するようにセキュリティ設定を調整することを促す警告メッセージを発行します。

> 「ターゲット」パネルへのアクセス
>
> 「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. 「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位)。
4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。
5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

   > ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。
6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性

があります。さらに、圧縮と圧縮データのアーカイブを有効にして、バックアップ、バックアップデータのコピー、およびターゲットへのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。

7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

   注 ファイル共有データのアーカイブは既定ではターゲットから実行されるため、追加料金を回避するために、このオプションを有効にすることをお勧めします。

8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「タイプ」ドロップダウンメニューから、「**AWS S3/Compatible**」または「**AWS Government**」を選択します。
10. サービスエンドポイントURL、バケット名、アクセスキーID、および秘密アクセスキーを入力します。アクセスキーと秘密アクセスキーは、Amazon APIサービス呼び出しの認証に使用されます。
11. HYCUがパススタイルURL(`https://s3.amazonaws.com/<BucketName>`) を使用してバケットにアクセスする場合は、「**パススタイルアクセス**」スイッチを使用します。HYCUは、既定では仮想ホストスタイルURL(`https://<BucketName>.s3.amazonaws.com`) を使用します。
12. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

    注 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、"暗号化キーのエクスポート" ページ215を参照してください。

13. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

Azureターゲットのセットアップ

前提条件

サービスが構成され、アクセス可能である。

制限事項

- ファイル共有のターゲット圧縮はサポートされません。
- 物理マシンのバックアップをこのタイプのターゲットに保存することはサポートされません。
- Blobストレージのバージョニングが有効なターゲットへのデータのバックアップはサポートされていません。

考慮事項

- *仮想マシン、アプリケーション、ボリュームグループの場合*：Azureターゲット上のデータは、ホット、クール、およびアーカイブストレージ層に保存できます。データアーカイブを復元するときに、HYCUは、Blobオブジェクトストレージの層がアーカイブストレージ層からホットストレージ層に変更されるデータリハイドレートを実行します。これを完了するには数時間かかる場合があることに注意してください。HYCUは、後でデータをアーカイブストレージ層に戻します。詳細については、"データリハイドレートの設定" ページ312を参照してください。
- *仮想マシン、アプリケーション、ボリュームグループの場合*：HYCUは、保持期間が少なくとも180日間に設定されている各データアーカイブを、次のアーカイブ同期中にAzureのクールストレージ層またはホットストレージ層からアーカイブストレージ層に自動的に移動します。アーカイブストレージ層は頻繁にアクセスされないデータを保存するために最適化されており、少なくとも180日間保存されるため、データアーカイブをアーカイブストレージ層に移動することで、HYCUによりデータは最も費用効率の高い方法で保存されることになります。
- *ファイル共有の場合*：HYCUは、ファイル共有データアーカイブをアーカイブストレージ層に自動的に移動しません。ファイル共有データをバックアップした後に、データをアーカイブストレージ層に手動で移動した場合、データを復元する前に、クールストレージ層またはホットストレージ層に戻せることも確認する必要があります。
- 不変性ポリシー(WORM)が設定されているAzureターゲットは、ターゲットのリストでは  アイコンで表されます。

推奨事項

バックアップデータが保存されているターゲットには、パブリックアクセスを無効にすることを強くお勧めします。HYCUは、ターゲットに対してパブリックアクセスが有効になっているかどうかを自動的に検出し、データへのアクセスを制限するようにセキュリティ設定を調整することを促す警告メッセージを発行します。

> **「ターゲット」パネルへのアクセス**
>
> 「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. 「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位)。
4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。
5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

> ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。

6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性があります。さらに、圧縮と圧縮データのアーカイブを有効にして、バックアップ、バックアップデータのコピー、およびターゲットへのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。

7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

   > 注 ファイル共有データのアーカイブは既定ではターゲットから実行されるため、追加料金を回避するために、このオプションを有効にすることをお勧めします。

8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「タイプ」ドロップダウンメニューから、「**AZURE**」、「**AZURE Government**」、または「**AZURE China**」を選択します。
10. ストレージアカウント名、秘密アクセスキー、およびコンテナ名を入力します。

    > 注 コンテナが存在しない場合、自動的に作成されます。

11. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

    > 注 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、"暗号化キーのエクスポート" ページ215を参照してください。

12. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

Google Cloudターゲットのセットアップ

前提条件

- Google Cloudサービスアカウントが作成済みで、HYCUに追加されている。クラウドアカウントをHYCUに追加する方法に関する説明については、"Google Cloudサービスアカウントの追加" ページ212を参照してください。

- HYCUに追加した作成済みのGoogle Cloudサービスアカウントにリンクされているプロジェクトに、Google Cloudストレージバケットが作成されている。
- サービスが構成され、アクセス可能である。
- *バケットロック(WORM)がターゲットで有効になっている場合のみ*。HYCUに追加するGoogle Cloudサービスアカウントは、Google Cloudで付与された`storage.buckets.create`および`storage.buckets.delete`許可を持っている必要があります。

制限事項

- ファイル共有のターゲット圧縮はサポートされません。
- 物理マシンのバックアップをこのタイプのターゲットに保存することはサポートされません。

考慮事項

- データを最も費用対効果の高い方法で保存するために、HYCUはデータを、ポリシーで設定された保持期間に最適なGoogle Cloudストレージクラスに保存します。したがって、そのようなデータは、バケットの既定のストレージクラスとして設定されたものとは異なるストレージクラスに保存できます。ただし、バケットの既定のストレージクラスが標準に設定されている場合、バックアップデータとバックアップデータのコピーは、常に標準のストレージクラスに保存されます。
- 保持期間が365日以上に設定されている各データアーカイブは、次回のアーカイブ同期中に、Google Cloudアーカイブストレージクラスに自動的に移動します。
- バケットロック(WORM)が有効なGoogle Cloudターゲットは、ターゲットのリストでは🔒アイコンで表されます。

推奨事項

バックアップデータが保存されているターゲットには、パブリックアクセスを無効にすることを強くお勧めします。HYCUは、ターゲットに対してパブリックアクセスが有効になっているかどうかを自動的に検出し、データへのアクセスを制限するようにセキュリティ設定を調整することを促す警告メッセージを発行します。

> **「ターゲット」パネルへのアクセス**
>
> 「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. 「容量」フィールドで、バックアップファイル用に予約する最大ストレージ領域を入力します(MiB、GiB、またはTiB単位)。
4. 「同時バックアップ数」フィールドで、同時バックアップの最大数を指定します。

   バックアップのスループットが許す限り、バックアップ時間とキューに入れられるバックアップジョブの量を減らすために、さらに多くのバックアップジョブが同時に実行されるように指定できます。

5. データアーカイブ用にこのターゲットを予約する場合は、「**アーカイブに使用**」スイッチを使用します。

   > ⚠ 重要 データのアーカイブに使用するターゲットは、データのバックアップまたはバックアップデータのコピーの保存には使用できません。

6. HYCUでバックアップデータをこのターゲットに保存する前に圧縮する場合は、「**圧縮を有効にする**」スイッチを使用します。圧縮は、バックアップデータ、バックアップデータのコピー、およびデータアーカイブに使用できます。

   > ⚠ 重要 データアーカイブ用に予約されているターゲット、特に多数の増分バックアップイメージを含むバックアップチェーンで圧縮を使用すると、HYCUのパフォーマンスが低下する可能性があります。さらに、圧縮と圧縮データのアーカイブを有効にして、バックアップ、バックアップデータのコピー、およびターゲットへのアーカイブを行うと、HYCU Backup Controllerのシステム要件が増える可能性があります。

7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

   > 注 ファイル共有データのアーカイブは既定ではターゲットから実行されるため、追加料金を回避するために、このオプションを有効にすることをお勧めします。

8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「Type」ドロップダウンメニューから、「**Google Cloud**」を選択します。
10. 「バケット名」フィールドで、バケット名を入力します。

    > 注 指定したバケットは、HYCUに追加したGoogle Cloudサービスアカウントにリンクされているプロジェクトで作成する必要があります。

11. 「クラウドアカウント」ドロップダウンメニューから、HYCUに追加したGoogle Cloudサービスアカウントを選択します。
12. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。

    > 注 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、“暗号化キーのエクスポート” ページ215を参照してください。

13. 「**保存**」をクリックします。

ターゲットはターゲットのリストに追加されます。ターゲットの管理の詳細については、"ターゲットの管理" ページ185を参照してください。

テープターゲットのセットアップ

HYCUは、QStar Archive Storage Manager (ASM)のIntegral Volumeセットで長期間保管するデータをアーカイブする際、テープを使用できます。

前提条件

- ライセンスされた容量がアーカイブデータを保存するのに十分である。
- QStarキャッシュのサイズが十分である。
- QStarにアーカイブデータを保存するための十分な空きスペースがある。

詳細については、QStarの資料を参照してください。

制限事項

- ターゲットの圧縮はサポートされていません。アーカイブデータはターゲットに保存されるまで圧縮できません。
- このタイプのターゲットから、個々のファイル、アプリケーション全体、SQL Serverデータベース、Exchange Serverデータベース、メールボックス、パブリックフォルダ、またはOracleデータベースインスタンスとテーブルスペースを復元することはサポートされていません。

考慮事項

- アーカイブデータの保存にのみテープターゲットを使用してください。
- 各Integral Volumeセットは HYCUでは個別のターゲットとして扱われます。

手順

1. 「ターゲット」パネルで、「**＋追加**」をクリックします。「ターゲットを追加」ダイアログボックスが開きます。
2. ターゲットの名前とその説明(オプション)を入力します。
3. *オプション*:「容量」フィールドで、アーカイブデータ用に予約する最大領域を入力します(MiB、GiB、またはTiB単位)。
4. 「同時バックアップ数」フィールドで、同時アーカイブジョブの最大数を指定します。データアーカイブの期間とキューに入れられるアーカイブジョブの量を減らすために、さらに多くのアーカイブジョブを同時に実行するように指定できます。

   > ⚠ **重要** QStarキャッシュのサイズが同時アーカイブ操作をサポートするのに十分であることを確認する必要があります。複数のアーカイブジョブを同時に実行するよう指定することで、HYCUバックアップコントローラーのシステム要件が増加する可能性があることに注意してください。

5. 「**アーカイブに使用**」オプションが有効であることを確認します。
6. 「**圧縮を有効にする**」オプションが無効であることを確認します。

7. *ターゲットからデータを読み取るための料金が発生する可能性がある場合のみ*。追加料金を避けるために最初に他の場所からデータの読み取りをHYCUに試行させたい場合は、「**従量性ターゲット**」スイッチを使用します。この場合、HYCUはスナップショットが利用可能であればそこから、またはこのデータを含み、追加料金が発生しない他のターゲットから、データの取得を試みます。それができない場合、データはターゲットから読み込まれます。

   > 注 ファイル共有データのアーカイブは既定ではターゲットから実行されるため、追加料金を回避するために、このオプションを有効にすることをお勧めします。

8. 「**次へ**」をクリックします。「ターゲットの詳細情報」ダイアログボックスが開きます。
9. 「タイプ」ドロップダウンメニューから、次のいずれかのテープターゲットを選択して、説明に従います。

ターゲットタイプ	説明
QStar NFS	a. HYCUが共有フォルダにアクセスしてWebサービス呼び出しをするのに使用するユーザー資格情報を入力します。 b. データをアーカイブするIntegral Volumeセットの名前を入力します。 c. Webサービス情報を入力します。既定のポートが使用され、QStarサーバーへのHTTPSアクセスが構成されている場合、QStarサーバーのホスト名を入力します。そうでない場合は、以下の形式でのQStarサーバーへのアクセスに使用されるURLを指定します。 `https://<QStarServer>:<Port>` d. *オプション*.マウントされているIntegral Volumeセットの共有フォルダへのパスを入力します。このフィールドを空にしていると、HYCUが共有フォルダへのパスの取得を試行します。 e. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。 > 注 ターゲットの暗号化を有効にする場合は、以下に注意してください。 • 圧縮率が影響を受ける可能性があります(テープ圧縮が有効になっている場合)。 • 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、"暗号化キーのエクスポート" ページ215を参照してください。
QStar SMB	a. *オプション*.共有フォルダでアクセス許可を持つアカウントが登録されているドメインを指定します。 b. HYCUが共有フォルダにアクセスしてWebサービス呼び出しをするのに使用するユーザー資格情報を入力します。

ターゲットタイプ	説明
	c. データをアーカイブするIntegral Volumeセットの名前を入力します。 d. Webサービス情報を入力します。既定のポートが使用され、QStarサーバーへのHTTPSアクセスが構成されている場合、QStarサーバーのホスト名を入力します。そうでない場合は、以下の形式でのQStarサーバーへのアクセスに使用されるURLを指定します。 `https://<QStarServer>:<Port>` e. *オプション*:マウントされているIntegral Volumeセットの共有フォルダへのパスを入力します。このフィールドを空にしていると、HYCUが共有フォルダへのパスの取得を試行します。 f. このターゲットに保存されているデータを暗号化する場合は、「**ターゲットの暗号化**」スイッチを使用します。 注 ターゲットの暗号化を有効にする場合は、以下に注意してください。 • 圧縮率が影響を受ける可能性があります(テープ圧縮が有効になっている場合)。 • 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するための暗号化ターゲットをインポートできるようにするには、暗号化キーをファイルにエクスポートし、このファイルを安全に保管します。説明については、"暗号化キーのエクスポート" ページ215を参照してください。

10. 「**保存**」をクリックします。

テープターゲットを作成すると、ターゲットのリストに追加され、∞アイコンで表示されます。

バックアップ戦略の定義

HYCUでは、自動バックアップをスケジュールして、回復ポイントと時間目標、およびバックアップ保持要件に基づいて最適なレベルのデータ保護を実現できます。バックアップは、一定の分、時間、日、週、または月が経過するごとに開始するようにスケジュールできます。

バックアップ戦略を定義するときは、環境の特定の要件を考慮に入れ、次のことを検討してください。

- 目標復旧時点(RPO)

  RPOは、データ損失が許容可能と見なされる最大期間(月、週、日、時間、または分)です。たとえば、RPOを24時間に設定するということは、業務で過去24時間のデータのみを失うのは許容できるということです。

- 目標復旧時間(RTO)

  RTOは、災害発生後のデータの復元に費やすことができる最大時間(月、週、日、時間、または分単位)です。

次の方法のうち、どの方法が要件に最も適しているかを決定します。

- 定義済みポリシーの活用

  定義済みポリシー(Gold、Silver、Bronze) のいずれかを使用することで、データ保護の実装を簡素化できます。詳細については、"定義済みポリシーの活用" 下を参照してください。

- カスタムポリシーの作成

  定義済みポリシーが要件を満たさない場合は、新しいポリシーを作成し、要件に合わせて調整できます。詳細については、"カスタムポリシーの作成" 下を参照してください。

ポリシー方法を決定したら、次のことを考慮します。

- 定義済みポリシーまたはカスタムポリシーのいずれかが環境のすべてのデータ保護目標を満たしている場合、そのようなポリシーを既定として設定できます。詳細については、"既定のポリシーの設定" ページ70を参照してください。
- 仮想マシンへのポリシーの自動割り当てをセットアップできます。詳細については、"自動ポリシー割り当てのセットアップ" ページ69を参照してください。

定義済みポリシーの活用

データ保護環境を構築するときには、データ保護を有効にする迅速かつ便利な方法を提供し、最も一般的なデータ保護シナリオをカバーする、定義済みポリシーを利用できます。

HYCUには次の定義済みポリシーが付属しています。

定義済みポリシーのタイプ	説明
Gold	データは4時間ごとにバックアップされ、4時間以内に復元されます。
Silver	データは12時間ごとにバックアップされ、12時間以内に復元されます。
Bronze	データは24時間ごとにバックアップされ、24時間以内に復元されます。

エンティティをバックアップ対象から除外する場合は、「除外」ポリシーを使用できます。

カスタムポリシーの作成

要件を定義済みのポリシーでカバーできない場合には、新しいポリシーを作成して、要件に合わせて調整できます。要件に合わせてポリシーを調整し、目的のRPO、RTO、およびターゲットを設定しながら、最適なポリシー実装のために1つ以上のポリシーオプションを有効にすることもできます。それらのポリシーオプションは以下のとおりです。

ポリシーオプション	説明
コピー	バックアップデータのコピーを作成できます。
アーカイブ	長期保管目的でデータを保存できます。
Fast restore	*Nutanixクラスターにのみ使用できます*。指定した保持期間、Nutanixクラスターにローカルスナップショットを保持することにより、仮想マシン、アプリケーション、およびボリュームグループデータを元のス

ポリシーオプション	説明
	トレージコンテナに迅速に復元できます。 このオプションを有効にすると、HYCUは保持設定に応じてNutanixクラスターに複数のスナップショットを保持します。これにより、仮想マシン、アプリケーション、ボリュームグループデータを迅速に復元し、ダウンタイムを削減できます。
Backup from replica	*Nutanixクラスターにのみ使用できます*。リモートオフィス/ブランチオフィス(ROBO) 環境のレプリカから仮想マシンおよびボリュームグループをバックアップできます。 ⚠ 重要 保護する仮想マシンとボリュームグループを含むNutanix保護ドメインに設定したスケジュール間隔が、HYCUポリシーで設定されたRPO以下であることを確認します。 Nutanixクラスター上の各スナップショットのレプリケーション保持は、HYCUポリシーで設定されたRPOに自動的に調整されることに注意してください。これにより、HYCUは変更ブロックトラッキング(CBT) 機能を使用して、最後のスナップショット以降に変更されたデータのリストを取得し、増分バックアップを実行できます。 Nutanix Prism Webコンソールを介した仮想マシンおよびボリュームグループの保護の詳細については、Nutanixの資料を参照してください。
自動割り当て	仮想マシンへのポリシーの自動割り当てをセットアップできます。これを行うには、まずNutanix PrismまたはVMware vSphereで仮想マシンにカテゴリー、またはタグ属性かカスタム属性を適用し、次にHYCUポリシーで、対応するメタデータを指定します。

ポリシーの作成

データ保護環境のすべての要件を満たすカスタムポリシーを作成できます。

前提条件

- バックアップジョブおよびバックアップコピージョブのタイムウィンドウを指定することを予定している場合は、それらが作成済みであることを確認してください。タイムウィンドウを指定することで、バックアップおよびバックアップコピージョブを開始できる時間枠を定義します。タイムウィンドウの詳細については、"タイムウィンドウの作成" ページ64を参照してください。
- 「アーカイブ」ポリシーオプションを有効にする予定の場合は、必ずデータアーカイブを事前に作成します。この実行方法の詳細については、"データアーカイブの作成" ページ67を参照してください。
- ROBO環境のレプリカから仮想マシンおよびボリュームグループをバックアップすることを予定している場合は、以下のようにします。

- 保護する必要がある仮想マシンとボリュームグループを含む保護ドメインが作成され、指定されたスケジュール間隔は、HYCUポリシーで設定されたRPO以下にする必要があります。Nutanix Prism Webコンソールを介した仮想マシンおよびボリュームグループの保護の詳細については、Nutanixの資料を参照してください。
- 中央サイトNutanixクラスターとブランチオフィスサイトクラスターの両方をHYCUに追加する必要があります。詳細については、"Nutanixクラスターの追加" ページ32を参照してください。

- 自動割り当てポリシーオプションを有効にすることを予定している場合は、"自動ポリシー割り当てのセットアップ" ページ69に記載されている情報を十分に理解しておくようにします。

「ポリシー」パネルのアクセス

「ポリシー」パネルにアクセスするには、ナビゲーションペインで、「 **ポリシー**」をクリックします。

手順

1. 「ポリシー」パネルで、「 **＋ 新規**」をクリックします。「新しいポリシー」ダイアログボックスが表示されます。
2. ポリシーの名前とその説明(オプション)を入力します。
3. 以下のいずれかのポリシーオプションをクリックして、有効なオプションのリストに追加します。
   - **バックアップ** *(必須)*
   - **コピー**
   - **アーカイブ**
   - **Fast restore**
   - **Backup from replica**
   - **自動割り当て**

   ⚠ 重要「Backup from replica」オプションと「Fast restore」オプションは、vSphere仮想マシンとアプリケーションには使用できません。
4. 「バックアップ」セクションで、以下を実行します。
   a. 「バックアップ頻度」フィールドで、RPOを設定します(月、週、日、時間、または分単位)。
   b. 「復旧時間」フィールドで、RTOを設定します(月、週、日、時間、または分単位)。
   c. 「保持期間」フィールドで、データの保持期間(月、週、または日単位)を設定します。保存期間は、復元ポイントが期限切れになる時期を定義します。期限切れのバックアップの詳細については、"バックアップの期限切れ指定" ページ252を参照してください。

      注 *AWS S3またはNutanix Objectsターゲットでオブジェクトロックを使用する場合のみ。*保持期間は、クラウドターゲットで指定されているオブジェクト保持期間とほぼ同じにすることをお勧めします。
   d. 「新しいバックアップチェーンを開始する」で、新しいバックアップチェーンを開始するタイミングを選択します。

- **バックアップのしきい値**

  最後の完全バックアップ以降のデータの変更率がこのオプションに指定した値を超えると、新しいバックアップチェーンが開始されます。既定値は25です。

- **バックアップチェーンの長さ**

  バックアップチェーン内の完全バックアップと後続の増分バックアップの数が、このオプションに指定した値を超えると、新しいバックアップチェーンが開始されます。既定値は7です。

> 注 両方のオプションを選択した場合、指定した値のいずれかを超えたときに新しいバックアップチェーンが開始されます。

e. 「ターゲット」ドロップダウンメニューから、保護されたデータの保存に使用する1つ以上のターゲットを選択します。

ターゲットを自動的に選択する場合は、必ず「**自動的に選択**」オプションを選択します。この場合、HYCU拡張スケジューラーは、RPOおよびRTOポリシー設定への準拠を保証できるターゲットのみを自動的に選択します。RPOよりも推定バックアップ時間が短く、RTOよりも推定復元時間が短いターゲットは、ターゲットのプールに追加されます。HYCU拡張スケジューラーは、各エンティティサイズ、およびターゲットのバックアップと復元のスループットとキューに基づいて、バックアップと復元の終了時間を計算し、バックアップが最速で完了するターゲットを選択します。

> 注 増分バックアップのターゲットは、選択したターゲットプール内の任意のターゲットにすることができます。バックアップチェーン内のすべてのバックアップに対して単一のターゲットを使用するには、必ずポリシーごとに単一のターゲットを選択します。

f. *バックアップウィンドウを指定する場合のみ*。「**バックアップウィンドウを使用する**」スイッチを有効にし、「バックアップウィンドウ」ドロップダウンメニューから、バックアップジョブのバックアップウィンドウを選択します。選択できるバックアップウィンドウがなく、作成したい場合には、"バックアップウィンドウの作成" ページ64を参照してください。

5. 有効にしたポリシーオプションに応じて、以下を実行します。

有効なオプション	手順
コピー	バックアップデータのコピーを作成するには、「コピー」セクションで、以下を実行します。 a. バックアップデータのコピーの保持期間(月、週、または日単位)を設定します。 b. 「ターゲット」ドロップダウンメニューから、バックアップデータのコピーの保存に使用する1つ以上のターゲットを選択します。 ターゲットを自動的に選択する場合は、必ず「**自動的に選択**」オプションを選択します。コピーターゲットは、データの安全性の理由においてバックアップターゲットとは異なる場所になります。 注 バックアップデータのコピーを保存する用途に複数のターゲッ

有効なオプション	手順
	トがあり、バックアップデータの複数のコピーが並行して作成されている場合、HYCUは、キューに入れられたバックアップとターゲットで実行中のバックアップの推定サイズに基づいて、それらのコピーをターゲット間で適切に分散させます。 c. *コピーウィンドウを指定する場合のみ*。「**コピーアップウィンドウを使用する**」スイッチを有効にし、「コピーウィンドウ」ドロップダウンメニューから、バックアップコピージョブのコピーウィンドウを選択します。選択できるコピーウィンドウがなく、作成したい場合には、"コピーウィンドウの作成" ページ65を参照してください。
アーカイブ	データをアーカイブするには、「アーカイブ」セクションの「データアーカイブ」ドロップダウンメニューから、データアーカイブを選択します。選択できるデータアーカイブがなく、作成したい場合には、"データアーカイブの作成" ページ67を参照してください。
Fast restore	*Nutanixクラスターにのみ使用できます*。高速復元ができるNutanixクラスターに複数のスナップショットを保持するには、「Fast restore」セクションで、スナップショットの保持期間(月、週、日、時間、または分)を設定します。たとえば、RPOを2日間に設定し、スナップショット保持期間を4日間に設定すると、Nutanixクラスターで2つのスナップショットを使用できます。 注 スナップショット保持期間は、RPOより短くしたり、バックアップ保持期間より長くしたりすることはできません。
Backup from replica	*Nutanixクラスターにのみ使用できます*。レプリカから仮想マシンおよびボリュームグループをバックアップするには、「Backup from replica」セクションの「中央サイトクラスター」ドロップダウンメニューから、仮想マシンおよびボリュームグループのレプリカが存在するクラスターを選択します。
自動割り当て	自動ポリシー割り当てをセットアップするには、「自動割り当て」セクションで、メタデータのキーと値を入力し、「**追加**」をクリックします。必要であれば、追加するすべてのキーと値についてこの手順を繰り返します。 ⚠ 重要 Nutanix Prismのカテゴリーに複数の値が含まれており、同じキーを異なる値でHYCUに追加したい場合、追加する値ごとにこの手順を繰り返す必要があります。

6. 「**保存**」をクリックします。

カスタムポリシーが作成され、ポリシーのリストに追加されます。ポリシーの管理の詳細については、"ポリシーの管理" ページ188を参照してください。

タイムウィンドウの作成

HYCUでは、バックアップジョブおよびバックアップコピージョブを開始できる時間枠を定義できます。タイムウィンドウを使用する場合、バックアップジョブまたはバックアップコピージョブは指定された時間内にのみ開始されるため、効率が向上し、環境の過負荷が回避されます。たとえば、バックアップジョブまたはバックアップコピージョブを非実稼働時間に実行するようにスケジュールすることで、ピーク時の負荷を減らすことができます。

定義済みのポリシーとカスタムポリシーの両方で、タイムウィンドウを使用できます。

> ⚠ 重要 タイムウィンドウを定義するときは、影響を受けるポリシーで指定されているRPOが、そのタイムウィンドウ内で達成できることを確認します。RPOが、バックアップジョブまたはバックアップコピージョブを開始できない時間枠より短い場合、結果としてエンティティはバックアップ要件に準拠しなくなります。

バックアップウィンドウとコピーウィンドウのどちらを作成するかによって、次のいずれかのセクションを参照します。

- “バックアップウィンドウの作成” 下
- “コピーウィンドウの作成” 次のページ

> 「タイムウィンドウ」ダイアログボックスへのアクセス
>
> 「タイムウィンドウ」ダイアログボックスにアクセスするには、「ポリシー」パネルで、「 **タイムウィンドウ**」をクリックします。

バックアップウィンドウの作成

手順

1. 「タイムウィンドウ」ダイアログボックスで、「 **＋ 新規**」をクリックします。「ウィンドウを選択」ダイアログボックスが表示されます。
2. 「**バックアップウィンドウ**」を選択して、「**次へ**」をクリックします。
3. バックアップウィンドウの名前と説明(オプション)を入力します。
4. 「タイムゾーン」ドロップダウンメニューで、バックアップウィンドウのタイムゾーンを指定します。表示されているタイムゾーン(ローカルタイムゾーンまたはHYCU Backup Controllerタイムゾーン)のいずれかをクリックするか、ドロップダウンメニューから選択することができます。
5. 「**完全/増分**」または「**増分のみ**」をクリックして、バックアップタイプに応じてバックアップをスケジュールします。

   > 注 「完全/増分」時間枠では、任意の完全および増分バックアップが開始されますが、「増分のみ」時間枠では、増分バックアップのみが開始されます。ただし、何らかの理由(たとえば、「コピーポリシー」オプションが有効になっている、スナップショットがない、ディスクが仮想マシンに追加されたなど)で増分バックアップを開始できない場合は、代わりに完全バックアップが開始されます。「増分のみ」時間枠も同様です。
6. 選択したバックアップタイプのバックアップの実行を開始する、曜日と時間を選択します。別のバックアップタイプのバックアップの時間枠を指定するには、別のバックアップタイプを選択してから、この

手順を繰り返します。

> ヒント クリックしてドラッグすると、追加する日と時間を含む時間枠をすばやく選択できます。

選択した時間枠が「時間枠」フィールドに表示されます。選択した時間枠を削除する場合は、その隣の「×」をクリックします。

7. 「**保存**」をクリックします。

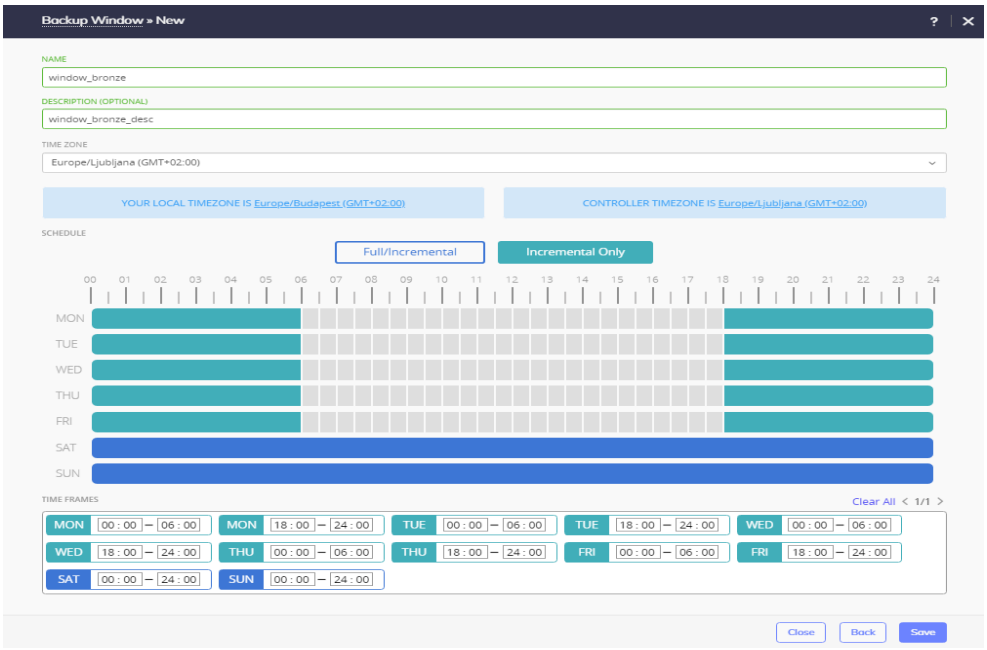
既存のバックアップウィンドウはいずれも後から編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。

バックアップウィンドウを作成したら、以下を実行できます。

- 新しいポリシーを作成するときにバックアップウィンドウを指定します。詳細については、"ポリシーの作成" ページ60を参照してください。
- バックアップウィンドウを既存のポリシーに割り当てます。これを実行するには、ポリシーを選択し、「**編集**」をクリックし、必要な変更を行います。

例

Bronzeポリシーを選択し、土曜日と日曜日に開始されるすべてのタイプのバックアップの時間枠と、平日の午後6時から午前6時の間に開始される増分のみバックアップの時間枠を指定しています。



この場合、バックアップジョブは、指定されたバックアップウィンドウ内の任意の時点で24時間ごとに開始されます(完全バックアップは週末のみに開始されます)。

コピーウィンドウの作成

手順

1. 「タイムウィンドウ」ダイアログボックスで、「**新規**」をクリックします。「ウィンドウを選択」ダイアログボックスが表示されます。

2. 「**コピーウィンドウ**」を選択して、「**次へ**」をクリックします。
3. コピーアップウィンドウの名前と説明(オプション)を入力します。
4. 「タイムゾーン」ドロップダウンメニューから、コピーウィンドウのタイムゾーンを指定します。表示されているタイムゾーン(ローカルタイムゾーンまたはHYCU Backup Controllerタイムゾーン)のいずれかをクリックするか、ドロップダウンメニューから選択することができます。
5. バックアップコピージョブの実行を開始する、曜日と時間を選択します。

   > **ヒント** クリックしてドラッグすると、追加する日と時間を含む時間枠をすばやく選択できます。

   選択した時間枠が「時間枠」フィールドに表示されます。選択した時間枠を削除する場合は、その時間枠で一時停止し、その隣に表示される「×」をクリックします。
6. 「**保存**」をクリックします。

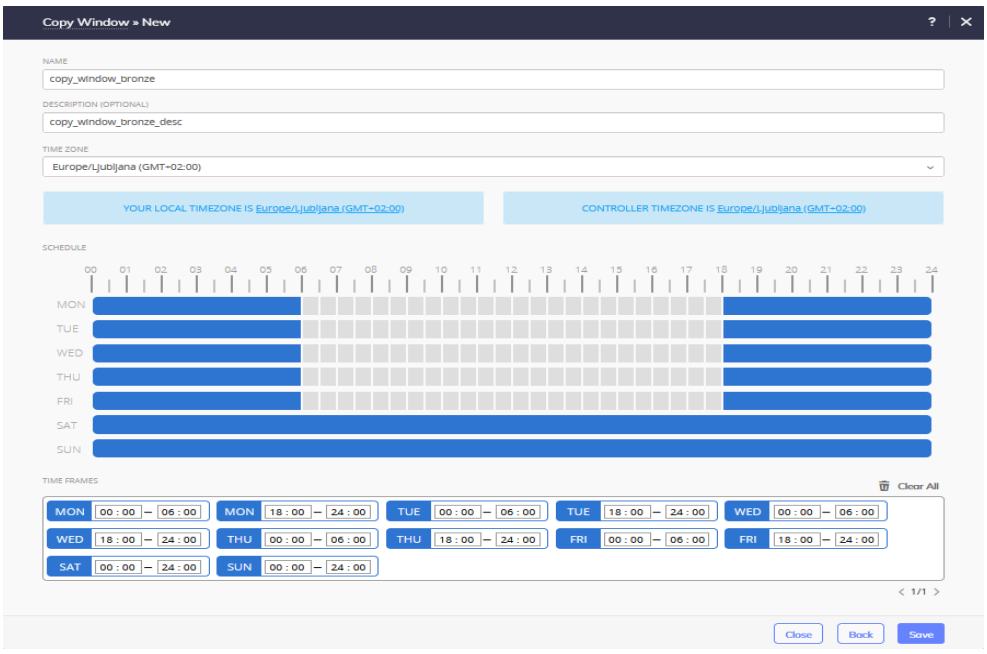
既存のコピーウィンドウはいずれも後から編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。

コピーウィンドウを作成したら、以下を実行できます。

- 新しいポリシーを作成するときにコピーウィンドウを指定します。詳細については、"ポリシーの作成" ページ60を参照してください。
- コピーウィンドウを既存のポリシーに割り当てます。これを実行するには、ポリシーを選択し、「**編集**」をクリックし、必要な変更を行います。

例

Bronzeポリシーを選択し、バックアップコピージョブを月曜日から金曜日の午後6時から午前6時まで、および土曜日から日曜日まで終日開始できる時間枠を指定しました。



この場合、バックアップコピージョブは24時間ごとに、指定した時間枠内の任意の時点で開始されます。

データアーカイブの作成

HYCUを使用すると、データのアーカイブを作成し、それを長期間保存できます。データをアーカイブすることにより、データは将来の参照用に、日時、週次、月次、または年次ベースで保存されます。データは現在のアクティビティから分離され、ローカルまたはクラウドアーカイブの安全な場所に安全な仕方で保存されます。

前提条件

- アーカイブターゲットがデータアーカイブ専用に予約されている(バックアップデータがアーカイブターゲットに保存されない)。
- *Azureアーカイブストレージ層にデータをアーカイブする場合*:データアーカイブは、Blob Storageまたは汎用v2(GPv2)アカウントでAzureに保存される。

制限事項

- *Azureアーカイブストレージ層にデータをアーカイブする場合*:汎用v1(GPv1)アカウントは、データアーカイブのアーカイブストレージ層への移動はサポートしていません。
- *データをAzureアーカイブストレージ層およびGoogle Cloudアーカイブストレージクラスにアーカイブする場合*:HYCUの以前のバージョンで作成されたデータアーカイブは、アーカイブストレージ層に移動されません。

> 「ポリシー」パネルのアクセス
>
> 「ポリシー」パネルにアクセスするには、ナビゲーションペインで、「**ポリシー**」をクリックします。

手順

1. 「ポリシー」パネルで、「**アーカイブ**」をクリックします。
2. 表示される「アーカイブ」ダイアログボックスで、「**＋ 新規**」をクリックします。
3. 表示される「新規」ダイアログボックスで、データアーカイブの名前と説明(オプション)を入力します。
4. データの日次、週次、月次、または年次のアーカイブを作成するかどうかに応じて、次の任意の優先アーカイブオプションをクリックして、有効なオプションのリストに追加します。
   - **日次**
   - **週次**
   - **月次**
   - **年次**
5. アーカイブジョブの実行を開始する時間と分を指定します。

   > ⚠ 重要 すべてのスケジュールされたアーカイブジョブは、HYCU Backup Controllerタイムゾーンに基づいて開始され、同じポリシーに指定されたタイムウィンドウの影響を受けません。
6. 選択したアーカイブオプションに応じて、データをアーカイブする間隔を指定します。

アーカイブオプション	説明
日次	a. 「繰り返し間隔」フィールドで、データのアーカイブを毎日実行する

アーカイブオプション	説明
	か、数日ごとに実行するかを指定します。 b. 平日のみデータをアーカイブする場合は、「**平日のみ適用**」スイッチを使用します。
週次	a. 「繰り返し間隔」フィールドで、データのアーカイブを毎週実行するか、数週間ごとに実行するかを指定します。 b. データをアーカイブする曜日を1つ以上選択します。 > 注 複数の日を選択した場合、アーカイブ準拠は、最新のデータアーカイブだけでなく、選択したすべての日のデータアーカイブを考慮して計算されます。
月次	a. 「繰り返し間隔」フィールドで、データのアーカイブを毎月実行するか、数か月ごとに実行するかを指定します。 b. データを、毎月の同じ日付(「毎月5日」など)にアーカイブするか、毎月の特定の日(「毎月第2金曜日」など)にアーカイブするかを選択します。
年次	a. 「繰り返し間隔」フィールドで、データのアーカイブを毎年実行するか、数年ごとに実行するかを指定します。 b. データのアーカイブを、希望する月の同じ日付(「1月5日」など)に行うか、希望する月の特定の日(「4月の第2金曜日」など)に行うかを選択します。

7. 「保持期間」フィールドで、使用する保持期間を設定します。

   > 注 新しいバックアップが実行される前にアーカイブが期限切れにならないように、保持期間はRPOよりも必ず長くします。

8. 「ターゲット」ドロップダウンメニューから、1つ以上のアーカイブターゲットを選択します。
9. 「**保存**」をクリックします。

既存のデータアーカイブはいずれも後から編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。アーカイブジョブがそのターゲットで進行中の場合には、アーカイブターゲットを変更できないことに注意してください。

データアーカイブを作成したら、以下を実行できます。

- 新しいポリシーを作成するときにデータアーカイブを指定します。詳細については、"ポリシーの作成" ページ60を参照してください。
- データアーカイブを既存のポリシーに割り当てます。これを実行するには、ポリシーを選択し、「**編集**」をクリックし、必要な変更を行います。
- データを手動でアーカイブします。詳細については、"データの手動でのアーカイブ" ページ194を参照してください。

自動ポリシー割り当てのセットアップ

自動ポリシー割り当てをセットアップすると、カテゴリー、またはタグ属性かカスタム属性が割り当てられるすべての仮想マシンに、ポリシーが自動的に割り当てられるようになります。これは特に、データ保護のアプローチで多くの場合にさまざまなポリシーの使用が求められる、複雑なデータ保護環境で役立ちます。

仮想マシンにカテゴリー、またはタグ属性かカスタム属性を割り当て、一致するメタデータを指定し、これらの値の比較で、指定された値が一致することが示された場合、対応するポリシーは、次回の仮想マシンの同期中に仮想マシンに自動的に割り当てられます。

> 注 HYCUは5分ごとに仮想マシンの自動同期を実行します。ただし、「仮想マシン」パネルの「**同期**」をクリックして、いつでも仮想マシンのリストを手動で更新することもできます。

考慮事項

- 定義済みのポリシーを仮想マシンに自動的に割り当てる場合は、カテゴリー、タグ、またはカスタム属性とメタデータの値を指定するときに、ポリシーの名前(Gold、Silver、Bronze、またはExclude)を使用できます。「除外」値を使用すると、仮想マシンがバックアップから除外されることに注意してください。
- ポリシーの自動割り当ては、すでにポリシーが割り当てられている仮想マシンには影響しません。
- 既定のポリシーが設定されていても、カテゴリー、またはタグ属性かカスタム属性が適用されている新しく検出された仮想マシンには決して割り当てられず、ポリシーの自動割り当てがセットアップされていないもののみを対象として割り当てられます。既定ポリシーの設定の詳細については、"既定のポリシーの設定" 次のページを参照してください。
- タグ属性またはカスタム属性とメタデータ値の比較で複数の一致結果が返される場合、最も低いRPOのポリシーが仮想マシンに割り当てられます。
- *Nutanix ESXiクラスターおよびvSphere環境の場合* :ポリシーの自動割り当てを設定した仮想マシンを復元すると、VMware vSphereに元のタグまたはカスタム属性が存在する場合のみ、タグまたはカスタム属性値が復元された仮想マシンで維持されます。

手順

データ保護環境に応じて、次のように自動ポリシー割り当てを設定できます。

データ保護環境	説明
Nutanix AHVクラスター	1. Nutanix Prismで仮想マシンにカテゴリーを割り当てます。説明については、Nutanixの資料を参照してください。 2. 一致するメタデータをHYCUポリシーに指定します。説明については、"ポリシーの作成" ページ60を参照してください。
Nutanix ESXiクラスターまたはvSphere環境	1. タグ属性またはカスタム属性をvSphere (Web) Clientの仮想マシンに割り当てます。説明については、VMwareの資料を参照してください。 2. 一致するメタデータをHYCUポリシーに指定します。説明については、"ポリシーの作成" ページ60を参照してください。

既定のポリシーの設定

定義済みポリシーまたはカスタムポリシーのいずれかを選択して、データ保護環境の既定のポリシーにすることができます既定のポリシーを設定すると、選択に応じて、既定のポリシーが次のエンティティ(仮想マシン、アプリケーション、ボリュームグループ、ファイル共有)に割り当てられます。

- 新しく検出されたエンティティのみ。
- 新しく検出されたエンティティと、ポリシーが割り当てられていないすべての既存エンティティの両方です。

> 「ポリシー」パネルのアクセス
>
> 「ポリシー」パネルにアクセスするには、ナビゲーションペインで、「 **ポリシー**」をクリックします。

手順

1. 「ポリシー」パネルで、既定として設定するポリシーを選択し、「 **既定に設定**」をクリックします。「既定ポリシーを設定する」ダイアログボックスが開きます。
2. 既定のポリシーを割り当てるエンティティを選択します：
   - **仮想マシン**
   - **アプリケーション**

     > ⚠ 重要 アプリケーションの既定ポリシーの設定は、仮想マシンにも既定ポリシーが設定されている場合のみ可能です。
   - **ボリュームグループ**
   - **共有フォルダ**
3. 既定のポリシーを、新しく検出されたエンティティのみに割り当てるか、新しく検出されたエンティティとポリシーが未割り当ての既存のエンティティの両方に割り当てるかによって、次のいずれかを実行します。

既定のポリシーの割り当て先...	説明
新しく検出されたエンティティのみ。	「**保存**」をクリックします。
新しく検出されたエンティティと、ポリシーが割り当てられていないすべての既存エンティティの両方です。	a. 「**ポリシーなしでエンティティに割り当て**」スイッチを有効にします。 b. 「**保存**」をクリックします。

既定のポリシーは、 アイコンによって表されます。このポリシーを既定のポリシーとして使用しないと後で決定した場合には、「 」「**既定をクリア**」をクリックします。このようにしても、割り当てられているエンティティからこのポリシーが割り当て解除されることはないことに注意してください。

第4章

仮想マシンの保護

HYCUにより、高速で信頼性の高いバックアップと復元操作で仮想マシンデータを保護できます。仮想マシンをバックアップしたら、仮想マシン全体、仮想ディスク、または個別のファイルを復元することを選択できます。

ソースとして次の環境が保護できます。

ソース	保護に使用できる項目
Nutanixクラスター	ストレージコンテナ内のボリュームグループ(論理的に関連した仮想ディスクの集合) ⚠ 重要 バックアップ時に1つ以上のボリュームグループが仮想マシンにアタッチされている場合、仮想マシンのバックアップ時にそれらもバックアップされます。そのようなボリュームグループとその詳細は、HYCUに追加されたNutanixクラスター上にある既存のすべてのボリュームグループとともに、「ボリュームグループ」パネルに表示されます。仮想マシン保護に依存していないボリュームグループのデータ保護を有効にする方法については、“ボリュームグループの保護” ページ146を参照してください。
vSphere環境	仮想マシンテンプレート(他の仮想マシンを作成するためのテンプレートとして使用される仮想マシン)

仮想マシン(HYCU Backup Controllerを含む)と物理マシンを保護するための準備手順と説明は、異なる場合があります。

仮想マシンデータを効率的に保護する方法の詳細については、以下のセクションを参照してください。

- “仮想マシン保護の計画” 下
- “仮想マシンのバックアップ” ページ85
- “仮想マシンの復元” ページ86
- “個別のファイルの復元” ページ107

仮想マシン保護の計画

バックアップを実行する前に、すべてのデータ保護環境に共通のものと、データ保護環境固有の前提条件、制限、考慮事項、および推奨事項を十分に理解してください。

- “データ保護環境の準備” 下
- “災害復旧の準備” ページ74
- “物理マシンの詳細” ページ76
- “HYCU Protégéの詳細” ページ77
- “データへのアクセスの有効化” ページ79
- “仮想マシンのバックアップ構成オプションのセットアップ” ページ82

データ保護環境の準備

前提条件

- *vSphere環境の場合*：最新バージョンのVMware Toolsが仮想マシンにインストールされている。
- *ROBO環境の場合*：バックアップする予定の仮想マシンにボリュームグループがアタッチされており、仮想マシンのバックアップ中にこれらのボリュームグループもバックアップする場合は、それらが仮想マシンと同じNutanix保護ドメインにあるようにする。
- *QStarのテープターゲットにデータをアーカイブする場合*：HYCU Backup Controller上で同時アーカイブジョブに1 GiBの追加空きメモリが使用可能である。
- *仮想マシンのバックアップを検証する予定で、カスタムスクリプトを指定する場合のみ*。
  - スクリプトは、仮想マシン上のアクセス可能なフォルダで利用でき、以下のいずれかの拡張子である必要があります。
    - Windows：`bat`、`ps1`、`cmd`
    - Linux：`sh`
  - *Linuxの場合*：割り当てられた資格情報を使用して仮想マシンでスクリプトを実行する許可を持つ必要がある。

制限事項

- ローカル固定ディスクとNutanixボリュームグループのバックアップのみがサポートされます。リモートボリューム(iSCSI、ディスクアレイ、マップされたネットワークディスクなど) がある仮想マシンをバックアップする場合、そのようなボリュームはスナップショットに含まれないため、結果としてバックアップされません。
- *Linux仮想マシンの場合*：永続的にマウントされているファイルシステムからのみファイルを復元できます。したがって、バックアップを実行する前に、必要なファイルシステムが`/etc/fstab`ファイルで指定されていることを確認します。
- *Nutanixクラスターの場合*：次のタイプの仮想マシンの保護はサポートされていません。Nutanix Controller VM、Prism Central VM、Nutanix Filesファイルサーバー VM、Nutanix Objectsノード。したがって、そのような仮想マシンは「仮想マシン」パネルに表示されません。これらのタイプの仮想マシンを保護する場合は、Nutanix販売担当員にお問い合わせください。
- *Nutanix ESXiクラスターの場合*：

- NVMeコントローラーが追加されている仮想マシンの保護はサポートされません。
- 「Backing up from replica」ポリシーオプションを有効にした場合、別のコンテナにディスクがある仮想マシンのバックアップはサポートされません。

考慮事項

- 仮想マシンのサイズが大きい(2～4 TB)大規模または中規模のデータ保護環境では、そのような仮想マシンの最初のバックアップには長い時間と多くのリソースが必要になることに注意してください。これらの仮想マシンは、同時にバックアップしないようにスケジュール調整を検討してください。大規模な仮想マシンにポリシーを割り当て、保護されるまで待ってから、他の仮想マシンの保護を続行できます。
- *vSphere環境の場合*：仮想マシンテンプレートのバックアップ中に予期しない事態が発生した場合(ネットワークの問題など)、バックアッププロセスの一部として仮想マシンに変換された仮想マシンテンプレートは、変換されたままになります。この場合、必ず仮想マシンを変換して仮想マシンテンプレートに戻します。この実行方法の詳細については、VMwareの資料を参照してください。
- *Nutanixクラスターの場合*：アーカイブは、元の場所(元の仮想マシンが実行されているクラスター、または「Backup from replica」オプションを使用している場合は中央サイトのNutanixクラスター)でスナップショットが使用可能な場合、スナップショットから実行されます。そうでない場合、アーカイブはターゲットから実行されます。
- *Nutanix ESXiクラスターの場合*：HYCUが完全バックアップを実行するために使用したスナップショットがNutanixクラスターにない場合(たとえば、HYCU保護ドメインがPrismから削除されたため)、次の仮想マシンバックアップは完全バックアップになります。
- *NearSyncで構成されている保護ドメインの場合*：保護ドメインのスナップショットは1～15分間隔で作成されますが、HYCUはスナップショットからのバックアップと復元に、1時間ごとに作成されたスナップショットのみを使用します。これは以下の環境に適用されます。
  - Nutanix ESXiクラスター
  - 「Backup from replica」オプションを使用した場合のNutanixクラスター
- *Nutanix ESXiクラスターの場合*：Nutanix ESXiクラスターのストレージコンテナがVMwareインフラストラクチャへのNFSデータストアとして提示される場合、対応するvSphereソースを使用して実行されるこのようなストレージコンテナ上の仮想ディスクの完全バックアップは、使用済みブロックだけでなく、割り当てられたディスク全体をコピーします。
- Nutanix Prism Webコンソールおよびv Sphere (Web) Clientの仮想マシンの詳細セクションに、仮想マシンに割り当てられているHYCUポリシーに関する情報を含める場合は、HYCU `config.properties`ファイルで、`hycu.policy.description`構成設定を`true`に設定します。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。
- *ROBO環境の場合*：HYCUが仮想マシンとボリュームグループのバックアップにこれらのスナップショットを使用する場合、保護ドメイン内のスナップショットの数は、構成された数よりも多くなる可能性があります。

推奨事項

- *ROBO環境の場合*:バックアップする予定の複数の仮想マシンにボリュームグループがアタッチされており、このボリュームグループもバックアップする場合は、同じNutanix保護ドメイン内の仮想マシンにのみアタッチすることをお勧めします。したがって、同じボリュームグループを同じNutanix保護ドメイン内の仮想マシンにアタッチし、同時に他の仮想マシンにアタッチすることはお勧めしません。
- *ROBO環境の仮想マシン*:そのような仮想マシン上のアプリケーションが仮想マシンの復元後に確実に実行するようにするには、それらに対してアプリケーション整合性のあるスナップショットを作成することをお勧めします。この実行方法の詳細については、Nutanixの資料を参照してください。
- *仮想マシンを異なるハイパーバイザーを持つ環境に復元は*、以下の推奨事項に従ってください。
  - *仮想マシンをNutanix ESXiクラスターまたはvSphere環境からNutanix AHVクラスターに復元する場合*:仮想マシンをバックアップする前に次の推奨事項に従って、復元後に仮想マシンが確実に起動するようにしてください。(そうでない場合は、“Nutanix ESXiクラスターまたはvSphere環境からの仮想マシンのNutanix AHVクラスターへの復元” ページ315で説明されているように、追加の手動手順を実行する必要があります)。
    - *Windows仮想マシンの場合*:Nutanix VirtIOパッケージは仮想マシン上にインストールされます。
    - *Nutanix ESXiクラスター上のLinux仮想マシンの場合*:NGTは仮想マシン上にインストールされます。
    - *vSphere環境におけるLinux仮想マシンの場合*:VirtIOドライバーはゲストOSカーネルに追加されます。
  - *Linux仮想マシンをNutanix AHVクラスターからvSphere環境に復元する場合*:

災害復旧の準備

データ保護環境の高い信頼性と復元性を実現するには、HYCU Backup Controller自体も保護する必要があります。そのようにすることで、保護されたデータの整合性と安全性を確保し、災害が発生した場合、たとえばHYCU Backup Controllerが誤って削除されたり、実行のベースとなっているクラスターノードが動作を停止したりした場合のデータ損失を防ぎます。さらに、データ保護環境にHYCUインスタンスも含まれている場合は、それらも保護する必要があります。

> ⚠ **重要** さらに安全性を高めるために、HYCU Backup Controllerの保護を、HYCU Backup Controllerをホストするソースの保護と組み合わせることをお勧めします。たとえば、Nutanix保護ドメインまたはVMware vSphereデータ保護を使用できます。詳細については、Nutanixまたは VMwareの資料を参照してください。

HYCU Backup Controllerバックアップを保存する予定のターゲットの構成パラメーターは必ずメモしておいてください。HYCU Backup Controllerを復元せずにそれらを復元する場合は、仮想マシン、アプリケーション、ファイル共有、ボリュームグループのバックアップを保存する予定のターゲットの構成パラメーターをメモしておくこともできます。災害復旧のターゲットをインポートするときには、正しい構成データを提供する必要があります。

ターゲットタイプ	インポートに必要な情報
NFS	• NFSサーバー名またはIPアドレス • 共有フォルダ
SMB	• ドメイン(使用する場合) • ユーザー名(使用する場合) • パスワード(使用する場合) • SMBサーバー名またはIPアドレス • 共有フォルダ
Nutanix	• URL • ユーザー名 • パスワード
Nutanix Objects	• サービスエンドポイント • バケット名 • アクセスキーID • 秘密アクセスキー • パススタイルアクセス
iSCSI	• ターゲットポータル • ターゲット名 • ユーザー(CHAP認証が有効な場合) • ターゲットの秘密(CHAP認証が有効な場合) • 相互認証の実行(CHAP認証が有効な場合)
AWS S3/Compatible	• サービスエンドポイント • バケット名 • アクセスキーID • 秘密アクセスキー • パススタイルアクセス
Azure	• ストレージアカウント名 • 秘密アクセスキー • ストレージコンテナ名
Google Cloud	• バケット名 • Google Cloudサービスアカウント
QStar NFS	• ユーザー名 • パスワード(使用する場合) • Integral volumeセット名 • Webサービスエンドポイント • 共有フォルダ(使用する場合)
QStar SMB	• ドメイン(使用する場合) • ユーザー名 • パスワード(使用する場合)

	• Integral volumeセット名 • Webサービスエンドポイント • 共有フォルダ(使用する場合)

考慮事項

- HYCU Backup Controllerに割り当てられるポリシー内のRPOは、データ保護環境内の他の保護されたエンティティに対してすでに設定されているRPOよりも常に低くする必要があります。
- *データ保護に複数のHYCU Backup Controllerを使用する場合のみ*。各HYCU Backup Controllerは、独自のWebユーザーインターフェース内から保護する必要があります。

物理マシンの詳細

仮想マシンデータの保護についての説明は、特に断りのない限り、物理マシンにも適用されます。

前提条件

- ファイルシステムデータへのアクセスが有効になっている。説明については、"データへのアクセスの有効化" ページ79を参照してください。
- 十分なディスク領域が、HYCUによりデータ保護の目的で以下の場所に作成された索引に使用できる。
  - Linux :`/var/opt/hycu/hycuraw`
  - Windows :`%programdata%\HYCU\hycuraw`
- *Windows物理マシンの場合：*
  - VSSサービスが有効で実行中であり、VSSライターのステータスが安定している。
  - WinRMが有効であり、`winrm quickconfig`コマンドを使用して構成されている。
  - *Windows物理マシンをNutanix AHVクラスターに複製する場合：*バックアップする前に、Nutanix VirtIOパッケージが物理マシンにインストールされていることを確認します。Nutanix VirtIOのインストールの詳細については、Nutanixの資料を参照してください。
- *Linux物理マシンの場合：*
  - SSHを介した物理マシンへのアクセスが有効である。
  - *LVMスナップショットを使用してデータをバックアップすることを予定している場合のみ(推奨方法)*。ボリュームグループでLVMスナップショットに十分な領域が使用できる。各ボリュームで10%以上の空きスペースが使用可能であることが推奨される。ただし、バックアップ中にボリュームへの書き込みが多数見込まれる場合、さらに多くの空きスペースが必要となる。詳細については、LVMの資料を参照してください。
  - ルートとして、またはパスワードなしでsudoコマンドを使用することによる、Linuxシステムへの特権アクセスが必要となる。
  - dm-snapshotカーネルモジュールがinitramfsに含まれている必要がある。モジュールを追加するには、物理マシンでrootユーザーとして次のコマンドを実行します。

    ```
    dracut -f --add-drivers dm-snapshot
    ```

- *Linux物理マシンを複製する場合*：以下のドライバーをゲストOSカーネルに追加する必要がある。
  - *Nutanix AHVクラスターに複製する場合*：Nutanix VirtIOドライバー(virtio_pci、virtio_blk、virtio_scsi、virtio_net)

    ドライバーを追加するには、ルートユーザーとして次のコマンドを実行します。

    ```
    dracut -f --add-drivers "virtio_pci virtio_blk virtio_scsi
    virtio_net"
    ```

  - *Nutanix ESXiクラスターまたはvSphere環境に複製する場合*：VMwareドライバーvmw_pvscsi

    ドライバーを追加するには、ルートユーザーとして次のコマンドを実行します。

    ```
    dracut -f --add-drivers vmw_pvscsi
    ```

制限事項

- Virtual Data Optimizer(VDO) を使用する物理マシンの保護はサポートされていません。
- *UEFIファームウェアを使用するLinux物理マシンの場合*：
  - サポートされているオペレーティングシステムの既定のブートローダーのみがサポートされます。サポートされるオペレーティングシステムのリストについては、*HYCU互換性マトリックス*を参照してください。
  - EFIシステムパーティションは、オペレーティングシステムが使用する既定の場所にマウントする必要があります(`/boot/efi`) 。

考慮事項

Linux物理マシンの場合：既定では、HYCUはデータ保護にLVMスナップショットを使用します。ただし、各ボリュームにLVMスナップショットのストレージに必要な容量を確保できない場合は、代替手段としてデバイスマッパー(DM) スナップショットを使用するようにHYCUを構成できます。詳細については、“DMスナップショットの有効化” ページ85を参照してください。

HYCU Protégéの詳細

HYCU Protégéを使用してオンプレミス環境とクラウド(Google Cloud、グローバルAzure、またはAzure US Government) 環境間で仮想マシンを移行する場合は、次の前提条件が満たされていることを確認します。

前提条件

- *仮想マシンとアプリケーションのクラウドへの移行の場合*：仮想マシンと物理マシンのバックアップ中にクラウド準備チェックが成功するように環境を構成する。
  - SSHまたはリモートデスクトップ接続を介した仮想マシンへのアクセスが有効になっていて、パブリックネットワークを使用したリモートデスクトップまたはSSH接続を許可するようにファイアウォールが構成されている。

- 移行を予定している仮想マシン、または移行を予定しているアプリケーションが実行している仮想マシンに、適切な資格情報が割り当てられています。仮想マシンへの証明書の割り当て方法に関する説明については、“データへのアクセスの有効化” 次のページを参照してください。
- *Linux仮想マシンの移行の場合：*
  - クラウドに移行する仮想マシンでDHCPが有効になっている。
  - ルートとして、またはパスワードなしでsudoコマンドを使用することによる、Linuxシステムへの特権アクセスが必要となる。
  - MACアドレスを基にした永続的なネットワークデバイス名の使用が無効になっている。この実行方法の詳細については、お使いのLinux配信ドキュメントを参照してください。
  - 以下のドライバーがinitramfsに含まれている必要がある。
    - *Google Cloudへの移行*：virtioドライバー(virtio_pci、virtio_net、およびvirtio_scsi)

      ドライバーを追加するには、仮想マシンでrootユーザーとして次のコマンドを実行します。

      ```
      dracut -f --add-drivers "virtio_pci virtio_net virtio_scsi"
      ```

      > ⚠ 重要 virtio_pciドライバーの追加は、それがモジュールとしてビルドされ、カーネルに含まれていない場合にのみ必要です。

    - *AzureまたはAzure US Governmentへの移行*：Hyper-Vドライバー(hv_vmbus、hv_storvsc、およびhv_netvs)

      ドライバーを追加するには、仮想マシンでrootユーザーとして次のコマンドを実行します。

      ```
      dracut -f --add-drivers "hv_vmbus hv_storvsc hv_netvsc"
      ```

- *Windows仮想マシンのGoogle Cloudへの移行の場合*：Nutanix VirtIOパッケージが、移行する予定の仮想マシンにインストールされている。

クラウド準備チェックステータスは、バックアップジョブレポートで確認できます。

- *Linux仮想マシンとクラウドとの間での移行の場合*：仮想マシンの`/etc/fstab`システム構成ファイルでは、ファイルシステムのデバイス識別に、デバイス名の代わりにUUID(たとえば、`UUID=8ff089c0-8e71-4320-a8e9-dbab8f18a7e5`) を使用する必要があります。
- *AzureからNutanix AHVクラスターへの仮想マシンの移行の場合*：Nutanix VirtIOパッケージは仮想マシン上にインストールされます。
- *クラウドへの災害復旧の場合*：仮想マシンの移行/DR準備完了ステータスを提供するように環境を構成します。以下が当てはまる場合、仮想マシンは移行/DR準備完了ステータスになります。
  - 現在のバックアップチェーンのすべてのバックアップは、いずれかのクラウドターゲット(Google Cloud、Azure、またはAzure US Government) に保存されます。
  - 仮想マシンのバックアップ中に、クラウド準備チェックが正常に実行されます。

「仮想マシン」パネルで仮想マシンの移行/DR準備完了ステータスを確認できます。

制限事項

Google Cloudからの仮想マシンの移行の場合：UEFIファームウェアを使用する仮想マシンは、Nutanix AHVクラスターまたはvSphere環境にのみ移行できます。そのような仮想マシンからNutanix ESXiクラスターへの移行はサポートされません。

推奨事項

- *仮想マシンとアプリケーションのクラウドへの移行の場合*：
  - *Windows仮想マシンの場合*：EMSコンソールリダイレクションをトラブルシューティング目的で有効にすることをお勧めします。有効にすることで、クラウドへの移行後に仮想マシンが起動しない場合、多くの情報を収集することが可能になります。
  - *Linux仮想マシンの場合*：シリアルコンソールリダイレクションをトラブルシューティング目的で有効にすることをお勧めします。有効にすることで、クラウドへの移行後に必要な場合、仮想マシンネットワークを構成することが可能になります。シリアルコンソールリダイレクションを有効にした仮想マシンであれば、ネットワークが機能していない場合でも、正常なクラウド準備チェックステータスを得られます。
- *UEFIファームウェアを使用するLinux物理マシンをクラウドに移行する場合*：移行後に仮想マシンが起動しない場合は、マシンを再起動します。

考慮事項

- データは以下のようにクラウドに移行されます。
  - Nutanixクラスターからデータを移行する場合、スナップショットが使用可能であれば、データはスナップショットから移行されます。そうでない場合は、ターゲットから移行されます。
  - vSphere環境からデータを移行する場合、データは常にターゲットから移行されます。
- *Windows仮想マシンの場合*：仮想マシンに複数のディスクがある場合、移行中は既定で追加ディスクがオフラインになります。移行後にディスクを手動でオンラインに戻すことができます。また、バックアップの前にPowerShellで以下のコマンドを実行して、既定設定を変更することもできます。

```
Set-StorageSetting -NewDiskPolicy OnlineAll
```

データへのアクセスの有効化

環境の復元目標で仮想マシンまたは物理マシンのファイルシステム内のデータをバックアップする必要がある場合は、HYCUがデータにアクセスできるようにする必要があります。

次のデータ保護シナリオでは、データへのアクセスが有効であることが前提条件です。

- 物理マシンを保護することを計画します。
- 仮想マシンのバックアップを検証する予定です。
- 個別のファイルを仮想マシンに復元することを計画している。
- アプリケーションを保護することを計画します。

- 仮想マシンの保護の一環として、iSCSIを使用して、仮想マシンにアタッチされているボリュームグループを保護することを計画している。
- プレ/ポストスクリプトの使用を計画します。
- HYCU Protégéを使用した仮想マシンとアプリケーションのクラウドへの移行を計画します。

前提条件

- ファイアウォールが、必要なTCPポート経由で着信ネットワークトラフィックを許可するように構成されている。
- *HTTPSを介するWinRMプロトコルのみが使用される場合*。HYCUが仮想マシンへのHTTPS for WinRM接続を使用するように構成されている必要がある。説明については、"HTTPS for WinRM接続の有効化" ページ260を参照してください。

制限事項

公開キー認証付きのSSHプロトコルを使用する場合のみ。古いPEM形式を使用してPuttyKeyGenまたはssh-keygenでキーが生成されている場合、DSAとRSAキーのみサポートされます。

考慮事項

- *Windows仮想マシンの場合*：ユーザー名を指定する際、以下のいずれかの形式を使用してください。
  - 仮想マシンがActive Directoryドメインに追加されている場合：`<Domain>\<Username>`または`<Username>@<Domain>`
  - 仮想マシンがActive Directoryドメインに追加されていない場合：`<Username>`、`.\<Username>`、または`<Hostname>\<Username>`(この場合、`<Hostname>`はCOMPUTERNAME変数の値です)。
- *ROBO環境でレプリカからバックアップする予定の仮想マシンの場合*：最新のレプリカが仮想マシンの状態を反映していることを確認します。

> **「仮想マシン」パネルへのアクセス**
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、アクセスを有効にする仮想マシンを選択します。
2. 「**資格情報**」をクリックします。「資格情報グループ」ダイアログボックスが開きます。
3. 「**新規**」をクリックします。
4. 資格情報グループの名前を入力します。
5. 「プロトコル」ドロップダウンメニューから、以下のいずれかのプロトコルオプションを選択します。

プロトコルオプション	説明
自動	仮想マシンにアクセスするプロトコルをSSHプロトコル(TCPポート22)またはWinRMプロトコル(HTTPSトランスポートとTCPポート5986、または

プロトコルオプション	説明
	HTTPトランスポートとTCPポート5985) からHYCUに自動的に選択させたいときにこのオプションを選択します。次に仮想マシンへのアクセスに必要な権限を持つユーザーアカウントのユーザー名とパスワードを入力します。 注 *Linux仮想マシンの場合* .既定でパスワード認証が使用されます。公開キー認証を使用する場合は、**SSH**プロトコルオプションを選択して、必要な変更を行います。
SSH	SSHプロトコルを使用する場合はこのオプションを選択し、次の手順を実行します。 a. 「ポート」フィールドで、SSHサーバーポート番号を入力します。 b. 「認証タイプ」ドロップダウンメニューから、使用する認証タイプを選択し、必要な情報を入力します。 • **パスワード認証** 仮想マシンへのアクセスに必要な権限を持つユーザーアカウントのユーザー名とパスワードを入力します。 • **公開キー認証** i. 「ユーザー名」フィールドで、仮想マシンへのアクセスに必要な権限を持つユーザーアカウントのユーザー名を入力します。 ii. 秘密鍵を選択します。 注 *セルフサービスのグループ管理者としてHYCUにログオンしている場合のみ*。Conjurを使用してHYCUのシークレットを管理する場合、ファイルを参照する代わりにシークレットを提供するのであれば、「**シークレットマネージャーから値を取得**」を有効にすることができます。シークレットの管理の詳細については、"シークレットの管理" ページ231を参照してください。 iii. *秘密鍵が暗号化されている場合のみ*。秘密鍵のパスフレーズを入力します。
WinRM	WinRMプロトコルを使用する場合はこのオプションを選択し、次の手順を実行します。 a. 「転送」ドロップダウンメニューから、使用するトランスポートのタイプを選択します。 b. 「ポート」フィールドで、WinRMサーバーポート番号を入力します。 c. 仮想マシンへのアクセスに必要な権限を持つユーザーアカウントのユーザー名とパスワードを入力します。

6. 「**保存**」をクリックします。
7. 「**割り当て**」をクリックします。

割り当てられた資格情報グループの名前が「仮想マシン」パネルの「資格情報グループ」列に表示されます。仮想マシンに資格情報を割り当てると、HYCUが仮想マシンおよびアプリケーション検出を実行します。また、「仮想マシン」パネルと「アプリケーション」パネルの「検出」ステータスがそれに応じて更新されます。

> **ヒント** 複数の仮想マシンで同じユーザー名とパスワードを共有する場合、複数選択を使用して同じ資格情報グループを一度に割り当てることができます。

仮想マシンから資格情報グループの割り当てを解除するには、「仮想マシン」パネルで、対象の仮想マシンを選択し、「**資格情報**」をクリックして、「**割り当て解除**」をクリックします。

既存の資格情報グループはいずれも編集することができます(資格情報グループを選択し、「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(資格情報グループを選択し、「**削除**」をクリックします)。

仮想マシンのバックアップ構成オプションのセットアップ

各仮想マシンについて、構成オプションをセットアップして、特定の仮想マシンのバックアップの範囲とフローを、データ保護環境の要件に合わせてさらに調整できます。

次の目的で、選択した仮想マシンにバックアップ構成オプションを設定できます。

目的	説明
プレ/ポストバックアップスクリプトおよびプレ/ポストスナップショットスクリプトを指定します。	"プレ/ポストバックアップスクリプトおよびプレ/ポストスナップショットスクリプトの指定" 下
仮想マシンをバックアップする際に、除外/追加するディスクまたはボリュームグループを指定します。	"バックアップでディスクを除外/追加する" 次のページ
*Linux物理マシンにのみ適用されます。*データのバックアップにLVMスナップショットではなく、DMスナップショットを使用するようにHYCUを構成します。	"DMスナップショットの有効化" ページ85

> 「仮想マシン」パネルへのアクセス
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

プレ/ポストバックアップスクリプトおよびプレ/ポストスナップショットスクリプトの指定

プレ/ポストバックアップスクリプトおよびプレ/ポストスナップショットスクリプトを使用して、バックアップの実行前またはスナップショットの作成前に必要なアクション(アプリケーションI/Oを一時停止するなど)を、バックアップの実行後またはスナップショットの作成後に必要なアクション(アプリケーションI/Oを再開するなど)を実行できます。スクリプトの指定方法の詳細については、このセクションで説明する手順に

従います。終了コードとエクスポートされた環境変数の詳細については、"プレ/ポストスクリプトの使用" ページ272を参照してください。

前提条件

- 仮想マシンのファイルシステムへのアクセスが有効である。説明については、"データへのアクセスの有効化" ページ79を参照してください。
- スクリプトは、アクセス可能なフォルダにあり、次のいずれかの拡張子である。
  - Windows :`bat`、`ps1`、`cmd`
  - Linux :`sh`
- *Linuxの場合* :割り当てられた資格情報を使用して仮想マシンでスクリプトを実行する許可がある。

手順

1. 「仮想マシン」パネルで、プレ/ポストスクリプトを指定する仮想マシンを選択し、「**構成**」を選択します。「構成」ダイアログボックスが開きます。
2. 「プレ/ポストスクリプト」タブで、選択したスイッチを使用して、プレ/ポストスナップショットスクリプトとプレ/ポストバックアップスクリプトを指定し、スクリプトのパス名を入力します。1つ以上のスイッチを有効にします。
   - **プレバックアップスクリプトの実行**
   - **プレスナップショットスクリプトの実行**
   - **ポストスナップショットスクリプトの実行**
   - **ポストバックアップスクリプトの実行**

   > 注 スクリプトのパス名フィールドに、サンプルのパス名が表示されます。必ず有効なスクリプトパス名を入力します。
3. 「**保存**」をクリックします。

バックアップでディスクを除外/追加する

既定では、仮想マシンに接続されているすべてのディスクとボリュームグループが、仮想マシンのバックアップ時にバックアップされます。ただし、特定のディスクをバックアップで除外/追加する場合は、仮想マシンのバックアップを実行する前にこれらのディスクをHYCUで選択できます。

- ディスクを除外することで、選択したディスクのみをバックアップするようにします。
- ディスクを含めることで、選択したディスクのみをバックアップするようにします。この場合、一時ディスクは自動的にバックアップから除外されます。

前提条件

バックアップで除外/追加するディスクが含まれている仮想マシンの所有者である。仮想マシンの所有権の設定方法に関する説明については、"仮想マシンの所有権の設定" ページ205を参照してください。

制限事項

- *個別のファイルの復元を予定している場合のみ*。バックアップからすべての仮想マシンディスクを除外し、仮想マシンにアタッチされたボリュームグループのみを残した場合、個々のファイルを復元することはできなくなります。
- *SQL Serverの場合*：「最適化されたSQL Server HADR保護オプション」が有効な場合、バックアップでディスクを除外/追加することはサポートされていません。
- *Exchange Serverの場合*：「最適化されたExchangeサーバーDAGの保護」オプションが有効な場合、バックアップでディスクを除外/追加することはサポートされていません。

考慮事項

- 仮想マシンのバックアップスコープを変更した後の次のバックアップは、完全バックアップになります。
- 保護されたアプリケーションがあるディスクを除外すると、アプリケーションの保護に影響を与える場合があります。
- (手動と自動どちらでも) バックアップから除外したディスクがある場合、その仮想マシンはそうしたディスクなしで、または除外したディスクを空のディスクとして作成するオプションを選択していると、空のディスクでクラウドに復元または移行されます。対応する復元ポイントのラベルは赤い丸でマークされています。詳細については、"エンティティ詳細の表示" ページ174を参照してください。
- *vSphere仮想マシンの場合*：独立ディスクやRDMディスクが仮想マシンにアタッチされている場合、バックアップからは自動的に除外されます。データの復元時またはクラウドへのデータの移行時に除外したディスクを空のディスクとして作成するオプションは、独立ディスクにのみ使用可能で、RDMディスクには使用できないことに注意してください。
- *動的ディスクがある物理マシンの場合*：動的ディスクは自動的にバックアップから除外されます。

手順

1. 「仮想マシン」パネルで、バックアップで含める/除外するディスクとボリュームグループがある仮想マシンを選択し、「**構成**」を選択します。「構成」ダイアログボックスが開きます。
2. 「除外/追加」タブで、バックアップにディスクとボリュームグループを除外するか追加するかによって、次のいずれかを実行します。

目的	説明
バックアップからディスクとボリュームグループを除外します。	a. 「**選択したvDisksを除外する**」をクリックし、バックアップから除外するディスクまたはボリュームグループを選択します。 b. 「**保存**」をクリックします。 ⚠ 重要 *vSphere環境の場合*：個々のファイルを復元する場合は、バックアップからオペレーティングシステムのディスクを除外しないようにしてください。
バックアップにディスクとボリュー	a. 「**選択したvDisksを追加する**」をクリックし、バックアップ

目的	説明
ムグループを追加します。	に追加するディスクまたはボリュームグループを選択します。 b. 「**保存**」をクリックします。

除外するディスクの選択は後で変更を加えることができます。

DMスナップショットの有効化

既定では、HYCUはLinux物理マシンデータ保護にLVMスナップショットを使用します。ただし、Linux物理マシンをDMスナップショットを使用してバックアップするように構成することもできます。

考慮事項

- データ保護にDMスナップショットを使用するようにHYCUを構成することは可能ですが、DMボリュームはサポートされていません。サポートされるボリュームの詳細については、「*HYCU互換性マトリックス*」を参照してください。
- スナップショットストレージでは、バックアップから除外された任意のボリュームまたはNFS共有でホストされるディレクトリを指定できます。
- *NFS共有をスナップショットストレージに使用することを予定している場合のみ。*システムパフォーマンスの問題を避けるため、NFSサーバーへの接続は必ず低レイテンシーかつ高スループット(10 GiBps以上)にしてください。

手順

1. 「仮想マシン」パネルで、DMスナップショットを使用してバックアップする仮想マシンを選択し、「**構成**」を選択します。「構成」ダイアログボックスが開きます。
2. 「スナップショット」タブで、「**DMスナップショットを有効にする**」スイッチを使用し、スナップショットストレージに使用するディレクトリへのパスを指定します(例 :`/mnt/nfs/snapshotdir`)。
3. 「**保存**」をクリックします。

仮想マシンのバックアップ

HYCUを使用すると、仮想マシンを高速かつ効率的な方法でバックアップできます。

> 注 仮想マシンテンプレートをバックアップする手順は、仮想マシンの場合と同じです。したがって、仮想マシンのバックアップと同じ説明に従うことができます。

前提条件

*iSCSIを使用して仮想マシンにアタッチされている物理マシンまたはボリュームグループを保護する予定の場合のみ。*資格情報は、保護する物理マシン、または保護するボリュームグループを持つ仮想マシンに割り当てられている。説明については、"データへのアクセスの有効化" ページ79を参照してください。

Nutanixクラスターの考慮事項

- 保護された仮想マシンを持つ保護ドメインをNutanix Prismを介して1つのクラスターから別のクラスターに移行する予定であり、それらの仮想マシンを保護されたままにしておきたい場合は、その両方のクラスターがHYCUに追加されていることを確認してください。移行後の次回の仮想マシンの同期では、対応する仮想マシンが、保護ドメインの移行先のクラスター上の仮想マシンのリストに追加されます。移行された仮想マシンは、移行前と同じUUIDを持ち、割り当てられたポリシーも保持します。そのような仮想マシンの次のバックアップは完全バックアップになることに注意してください。
- 仮想マシンの同期中に、仮想マシンがNutanixクラスターで見つからない場合、この仮想マシンまたはそこで実行されている検出済みアプリケーションのステータスはPENDING_REMOVALに設定されます。そのような仮想マシンとそのアプリケーションはHYCUではグレー表示され、それらに対してデータ保護を実行することはできません。2つの自動仮想マシン同期プロセスの時間間隔中に、仮想マシンがNutanixクラスターで見つかった場合、そのステータスはPROTECTED_DELETEDに変更されます。それ以外の場合、仮想マシンはHYCUから削除されます。

> 「仮想マシン」パネルへのアクセス
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、バックアップする仮想マシンを選択します。

   > ヒント「**同期**」をクリックして、仮想マシンのリストを更新できます。表示されている仮想マシンのリストを絞り込むには、"データのフィルタリング" ページ177で説明されているフィルタリングオプションを使用できます。

2. 「**ポリシー**」をクリックします。「ポリシー」ダイアログボックスが開きます。
3. 選択可能なポリシーのリストから、目的のポリシーを選択します。
4. 「**割り当て**」をクリックして、選択した仮想マシンにポリシーを割り当てます。

   > 注 選択した仮想マシンにポリシーを割り当てると、それらの上で実行されているアプリケーションにすでにポリシーが割り当てられている場合には、それらのアプリケーションにも同じポリシーが割り当てられます。この場合、仮想マシンに割り当てられたポリシーはアプリケーションに割り当てられたポリシーよりも優先され、アプリケーションに自動的に割り当てられます。

バックアップは、ポリシーに定義した値に従ってスケジュールされます。必要であれば、手動バックアップもいつでも実行できます。詳細については、"手動バックアップの実行" ページ190を参照してください。

仮想マシンの復元

HYCUを使用すると、破損した仮想マシン全体、または仮想ディスク(仮想マシンディスクや仮想マシンにアタッチされたNutanixボリュームグループ) のみを復元できます。仮想マシンのバックアップは、仮想マシンのクローンを作成することでも検証できます。

> 注 *vSphere環境の場合* .仮想マシンテンプレートを復元する手順は、仮想マシンの場合と同じです。したがって、仮想マシンの復元と同じ説明に従うことができます。

前提条件

- *テープからデータを復元する場合*: テープターゲットがデータのアーカイブに積極的に使用されている場合、モードは「読み取り専用」に設定する。ターゲットを編集する方法の詳細については、「"ターゲットの管理" ページ185」を参照してください。
- *vSphere環境の場合*: 割り当てられている必要な復元特権がある。詳細については、"vSphereユーザーへの特権の割り当て" ページ269を参照してください。
- 仮想マシンを同じソースに復元し、既存のISOイメージをその復元された仮想マシンにアタッチする場合、バックアップ時に仮想マシンにアタッチされたISOイメージが、仮想マシンの復元時刻にソースにまだ存在しており、その名前と場所が同じであることを確認する。
- *物理マシンの場合*: 少なくとも1つのNutanixクラスターまたはvCenterサーバーがHYCUに追加され、復元データの保存のためのストレージコンテナが提供されている。Nutanixクラスターを HYCUに追加する方法の詳細については、"Nutanixクラスターの追加" ページ32を参照してください。vCenterサーバーをHYCUに追加する方法の詳細については、"vCenter Serverの追加" ページ34を参照してください。

制限事項

あるソースから別のソースに仮想マシンを復元する場合、バックアップ時に仮想マシンにアタッチされたISOイメージは、復元された仮想マシンにアタッチされません。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため)がある層が含まれている場合、データを復元するかまたは仮想マシンのバックアップを検証するためにこの層を使用することはできません。
- ポリシーに指定された保持期間が経過してしまっている(復元ポイントがHYCU Webユーザーインターフェースでグレー表示になっている)仮想マシンの復元は実行できません。ただし、必要な場合、これはHYCU `config.properties`ファイル内の `restore.enabled.if.retention.is.up`構成設定を`true`に設定することで上書きできます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

復元オプション

次の復元オプションから選択できます。

復元オプション	説明
VMの復元	仮想マシンを復元できます。元の仮想マシンを、復元した仮想マシンで置き換える場合は、このオプションを選択します。説明については、"仮想マシンの復元" 次のページを参照してください。 ⚠ 重要 このオプションを使用して物理マシンを復元することはできません。

復元オプション	説明
VMのクローン	仮想マシンのクローンを作成することで、仮想マシンを復元できます。元の仮想マシンを保持する場合は、このオプションを選択します。説明については、"仮想マシンの複製" ページ91を参照してください。
VMバックアップを検証	仮想マシンのバックアップを、仮想マシンのクローンを作成することで検証できるようにします。仮想マシンに破損したバックアップがないことを確認する場合は、このオプションを選択します。説明については、"仮想マシンのバックアップの検証" ページ98を参照してください。
vDiskの復元	仮想ディスクを復元できます。元の仮想ディスクを、復元した仮想ディスクで置き換える場合は、このオプションを選択します。説明については、"仮想ディスクの復元" ページ101を参照してください。 ⚠ 重要 このオプションを使用して物理マシンのディスクを復元することはできません。
vDiskのクローン	クローンを作成することで、仮想ディスクを復元できます。元の仮想ディスクを保持する場合は、このオプションを選択します。説明については、"仮想ディスクのクローン" ページ102を参照してください。 ⚠ 重要 このオプションを使用してvSphere仮想マシンのディスクを復元することはできません。
vDiskのエクスポート	仮想ディスクをNFSまたはSMB共有に復元できます。特定のアクセス権限を持つユーザーが仮想ディスクを使用できるようにする場合、または後から仮想ディスクを使用してデータを物理マシンや、HYCUにサポートされていないあるいはソースとしてHYCUに追加されていないハイパーバイザーのある環境に復元する場合に、このオプションを選択します。説明については、"仮想ディスクのエクスポート" ページ104を参照してください。

📋 注 「VMのクローン」オプションを使用すると、異なるハイパーバイザーを使用する環境に仮想マシンを復元することもできます。異なるハイパーバイザーを持つ環境に仮想マシンを正常に復元するために考慮または実行する必要がある前提条件、制限事項、考慮事項、および追加の手順については、"異なるハイパーバイザーを持つ環境への復元" ページ314を参照してください。

仮想マシンの復元

仮想マシンを元の場所または新しい場所に復元できます。この場合、元の仮想マシンは上書きされます。

制限事項

- *Nutanix AHVクラスターの場合*：UEFIブート構成をサポートしているNutanix AHVクラスターにのみUEFIブートモードが有効になっている仮想マシンを復元できます。
- 「VMの復元」オプションを使用した物理マシンの復元はサポートされていません。

考慮事項

- *復元するボリュームグループが仮想マシンにアタッチされている場合のみ。*バックアップ時にアタッチされたのであれば、ボリュームグループを仮想マシンとともに復元することを選択できます。この場合、元のボリュームグループは削除され、復元されたボリュームグループは、バックアップ時にアタッチされた他のすべての仮想マシンと同じように、復元された仮想マシンに自動的にアタッチされます。
- 復元された仮想マシンは元のMACアドレスを保持します。
- *vSphere仮想マシンのデータを元のストレージコンテナに復元することを予定している場合のみ。*ストレージコンテナが複数のホストにマウントされており、復元時に元のホストが電源オフまたはメンテナンスモードになっている場合、データは異なるホストの同じストレージコンテナに復元されます。

> 「仮想マシン」パネルへのアクセス
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、復元する仮想マシンをクリックします。画面の下部に「詳細ビュー」が表示されます。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 「詳細ビュー」で、目的の復元ポイントを選択します。
3. 「**VMの復元**」をクリックします。
4. 「**VMの復元**」を選択し、「**次へ**」をクリックします。
5. 「全般」セクションで、次の手順を実行します。
   a. 「ストレージコンテナ」ドロップダウンメニューから、仮想マシンを復元する場所を選択します。(既定では、元のストレージコンテナが選択されます。)

      > 注仮想マシンを別のストレージコンテナに復元することを決定した場合、スナップショットからではなくターゲットから復元が実行されるため、高速復元は実行できません。

   b. 復元した仮想マシンを元の仮想マシンと同じ構成設定にする場合は、「**元のVM設定を使用**」スイッチを使用します。

      構成設定のいずれかを変更する場合は、「**元のVM設定を使用**」スイッチを無効にして、以下を実行します。

      - 「vCPU(s)」フィールドに、復元した仮想マシンの仮想CPU数を入力します。仮想CPUの最大数は1024です。
      - 「vCPUあたりのコア数」フィールドに、復元した仮想マシンの仮想CPUあたりのコア数を入力します。仮想CPUあたりの最大コア数は64です。

        > 注復元した仮想マシンのコア数の合計は、仮想CPU数に仮想CPUあたりのコア数を掛けた数となります。

- 「メモリ」フィールドで、復元した仮想マシンのメモリ量(GiBまたはMiB単位)を設定します。指定する値は整数でなければならず、4096 GiBを超えることはできません。

c. 復元した仮想マシンを復元後にオンにする場合は、「**仮想マシンの電源をオンにします**」スイッチを使用します。元の仮想マシンは自動的に削除されます。

> ⚠ 重要 *vSphere仮想マシンをvSphere環境に復元し、「仮想マシンの電源をオンにします」スイッチを無効にしている場合のみ。*仮想マシンをオンにしようとしたときに、仮想マシンが移動したものかコピーしたものか答えるよう求められた場合は、必ず「**移動しました**」と答えてください。

d. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
- **自動** :最新の状態に最速で復元できます。
- **バックアップ**
- **コピー**
- **アーカイブ**
- **スナップショット**

e. *仮想ディスクが(手動または自動で)バックアップから除外されている場合のみ* :サイズと構成が同じ空のディスクを除外したディスクとして作成し、復元した仮想マシンにアタッチしたい場合は、「**除外ディスクを空ディスクとして作成**」スイッチを使用します。

f. *仮想マシンにアタッチされているボリュームグループの場合* :仮想マシンにアタッチされているボリュームグループも復元する場合は、「**ボリュームグループの復元**」スイッチを使用します。

6. 「ネットワーク」セクションで、バックアップ時に仮想マシンに追加されたネットワークアダプタのリストを確認します(仮想マシンが接続されていたネットワークを含む) 。元のネットワークのいずれかが利用できなくなった場合は、「該当なし」が表示されます。

   元のネットワークが使用可能かどうかに応じて、以下のように続行します。

   - 元のネットワークが利用可能な場合は、既定値を変更せずに元のネットワーク設定で仮想マシンを復元するか、またはネットワーク設定を変更することができます。
   - 元のネットワークが利用できない場合は、ネットワーク設定を変更する必要があります。

ネットワーク設定の変更

元のネットワーク...	説明
使用可能	次の手順を実行できます。 • 「**＋ 新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。 • 仮想アダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、既存のネットワークアダプタを編集して、仮想マシンを別のネットワークに接続します。 • 必要なくなったネットワークアダプタの資格情報を選択し、「**削除**」をクリックして削除します。

元のネットワーク...	説明
使用不可	次の手順を実行できます。 • ネットワークアダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、影響を受けるネットワークアダプタを編集して、仮想マシンを新しいネットワークに接続します。 • 影響を受けるネットワークアダプタを選択して削除し、「**削除**」をクリックします。 • 「**新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。

> 注 仮想マシンはネットワークアダプタなしで復元できます。後で必ず仮想マシンのネットワーク設定を構成してください。

7. 「**復元**」をクリックします。

> 注 *Nutanix ESXiクラスターの場合* :仮想マシンの復元に必要な最小RAMは256 MiBであるので、それよりRAMが少ない仮想マシンは復元中に自動的に256 MiBに設定されます。

仮想マシンの複製

元の仮想マシンのクローンは、仮想マシンを元の場所または新しい場所に復元することにより作成できます。この場合、元の仮想マシンは上書きされません。

前提条件

- *新しい場所にクローンを予定している仮想マシンの場合* :仮想マシンのクローンを予定しているvSphere環境のNutanixクラスターまたはvCenterサーバーが、HYCUに追加されている。この実行方法の詳細については、"Nutanixクラスターの追加" ページ32または"vCenter Serverの追加" ページ34を参照してください。
- *Linux物理マシンの場合* :物理マシンの`/etc/fstab`システム構成ファイルでは、ファイルシステムのデバイス識別に、デバイス名の代わりにUUID(`UUID=8ff089c0-8e71-4320-a8e9-dbab8f18a7e5`など) を使用する必要があります。

制限事項

vSphere環境の場合 :復元された仮想マシンへのISOイメージのアタッチはサポートされていません。

考慮事項

- スナップショットが元の場所(元の仮想マシンが実行されていたソース) で利用可能な場合にのみ、スナップショットから復元が実行されます。スナップショットが元の場所で利用できない場合、復元のために選択した層に応じて、次のようになります。
  - スナップショットを選択した場合、復元は失敗します。
  - 「自動」を選択した場合、利用可能なターゲットがあれば、ターゲットから復元が実行されます。そうでない場合は、失敗します。

- *複製するボリュームグループが仮想マシンにアタッチされている場合のみ*。バックアップ時にアタッチされたのであれば、ボリュームグループを仮想マシンとともに復元することを選択できます。この場合、元のボリュームグループは復元されたボリュームグループとともに維持されます。ボリュームグループが他の仮想マシンにもアタッチされている場合、(仮想マシンへのアタッチ方法に応じて) 以下が適用されます。
  - 直接：ボリュームグループは、クローンされた仮想マシンのみに自動的にアタッチされます。
  - iSCSIを使用：ボリュームグループは、バックアップ時にアタッチされたすべての仮想マシンに自動的にアタッチされます。
- *Nutanix AHVクラスターで実行されている仮想マシンをNutanix ESXiクラスターに復元する場合*：仮想マシンのディスクがPCIバスにアタッチされている場合、復元後にバスタイプが自動的にSCSIに変更されます。この構成変更のため、復元は警告で終了します。
- *Nutanix ESXiクラスターで実行されているLinux仮想マシンの場合*：vSphere (Web) Clientを介して作成された仮想マシンを復元した後、仮想マシンが起動しない場合は、“vSphere環境から仮想マシンのNutanix ESXiクラスターへの復元” ページ318で説明されている手順に従ってください。
- 仮想マシンを復元した後、次の復元を実行すると、仮想ディスクの順序が元の仮想マシンの順序と異なるものとなる場合があります。
  - Nutanix AHVクラスターからNutanix ESXiクラスターまたはvSphere環境への
  - Nutanix ESXiから別のNutanix ESXiクラスターへの
  - vSphere環境からNutanix ESXiクラスターへの

  この場合は、正しいブートディスクの選択を含め、必要な調整を行います。
- *vSphere仮想マシンのデータを元のストレージコンテナに復元することを予定している場合のみ*。ストレージコンテナが複数のホストにマウントされており、復元時に元のホストが電源オフまたはメンテナンスモードになっている場合、データは異なるホストの同じストレージコンテナに復元されます。
- *仮想マシンに所有権が設定されている場合のみ*。同じ所有者は、復元された仮想マシンに自動的に割り当てられます。

推奨事項

- *Linux仮想マシンの場合*：MACアドレスを基にした永続的なネットワークデバイス名の使用は無効にすることをお勧めします。そうしないと、ネットワークの手動での構成が必要になります。永続的なネットワークデバイス名の使用を無効にする方法については、お使いのLinux配信ドキュメントを参照してください。
- *Linux物理マシンの場合*：物理マシンの元のブートローダーがバックアップ中に一時的なものに置き換わったため、復元後にブート構成を更新することをお勧めします。これを実行する方法の詳細については、物理マシンがどのようなファームウェアを使用しているかに応じて、次のいずれかのセクションを参照してください。
  - “BIOSファームウェアを使用するLinux物理マシンのブート構成の更新” ページ96
  - “UEFIファームウェアを使用するLinux物理マシンのブート構成の更新” ページ97

「仮想マシン」パネルへのアクセス

ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、復元する仮想マシンをクリックします。画面の下部に「詳細ビュー」が表示されます。

   > 注 「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 「詳細ビュー」で、目的の復元ポイントを選択します。
3. 「**VMの復元**」をクリックします。
4. 「**VMのクローン**」を選択し、「**次へ**」をクリックします。
5. 「全般」セクションで、次の手順を実行します。
   a. 「ストレージコンテナ」ドロップダウンメニューから、仮想マシンを復元する場所を選択します。

      > 注 *仮想マシンの場合* .既定では、元のストレージコンテナが選択されます。仮想マシンを別のストレージコンテナに復元する場合、次の点にご注意ください。
      > - スナップショットからではなくターゲットから復元が実行されるため、高速復元は実行できません。
      > - 選択したストレージコンテナが別のハイパーバイザーにある場合、追加の前提条件が適用されます。詳細については、"異なるハイパーバイザーを持つ環境への復元" ページ314を参照してください。

   b. 「新しいVM名」フィールドで、仮想マシンの新しい名前を指定します。
   c. 復元した仮想マシンを元の仮想マシンと同じ構成設定にする場合は、「**元のVM設定を使用**」スイッチを使用します。

      構成設定のいずれかを変更する場合は、「**元のVM設定を使用**」スイッチを無効にして、以下を実行します。

      - 「vCPU(s)」フィールドに、復元した仮想マシンの仮想CPU数を入力します。仮想CPUの最大数は1024です。
      - 「vCPUあたりのコア数」フィールドに、復元した仮想マシンの仮想CPUあたりのコア数を入力します。仮想CPUあたりの最大コア数は64です。

        > 注 復元した仮想マシンのコア数の合計は、仮想CPU数に仮想CPUあたりのコア数を掛けた数となります。

      - 「メモリ」フィールドで、復元した仮想マシンのメモリ量(GiBまたはMiB単位)を設定します。指定する値は整数でなければならず、4096 GiBを超えることはできません。

   d. 復元した仮想マシンを復元後にオンにする場合は、「**仮想マシンの電源をオンにします**」スイッチを使用します。復元した仮想マシンをオンにすると、元の仮想マシンは自動的にオフになります。

      > ⚠ 重要 以下にご注意ください。

- このオプションは、iSCSIを使用してアタッチされたボリュームグループがある仮想マシンには無効です。復元された仮想マシンをオンにする前に実行する必要がある事柄については、"仮想マシンの複製後" 次のページを参照してください。
- *vSphere仮想マシンをvSphere環境に複製し、「仮想マシンの電源をオンにします」スイッチを無効にしている場合のみ。*仮想マシンをオンにしようとしたときに、仮想マシンが移動したものかコピーしたものか答えるよう求められた場合は、必ず「**コピーしました**」と答えてください。

e. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**

f. *仮想ディスクが(手動または自動で)バックアップから除外されている場合のみ* :サイズと構成が同じ空のディスクを除外したディスクとして作成し、復元した仮想マシンにアタッチしたい場合は、「**除外ディスクを空ディスクとして作成**」スイッチを使用します。

g. *仮想マシンにアタッチされているボリュームグループの場合* :仮想マシンにアタッチされているボリュームグループも復元する場合は、「**ボリュームグループのクローン**」スイッチを使用します。

6. 「ネットワーク」セクションで、次の手順を実行します。

   a. バックアップ時に仮想マシンに追加されたネットワークアダプタのリストを確認します(仮想マシンが接続されていたネットワークを含む)。元のネットワークのいずれかが利用できなくなった場合は、「該当なし」が表示されます。

   元のネットワークが使用可能かどうかに応じて、以下のように続行します。

   - 元のネットワークが利用可能な場合は、既定値を変更せずに元のネットワーク設定で仮想マシンをクローンするか、またはネットワーク設定を変更することができます。
   - 元のネットワークが利用できない場合は、ネットワーク設定を変更する必要があります。

ネットワーク設定の変更

元のネットワーク...	説明
使用可能	次の手順を実行できます。 • 「**＋ 新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。 • 仮想アダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、既存のネットワークアダプタを編集して、仮想マシンを別のネットワークに接続します。 • 必要なくなったネットワークアダプタの資格情報を選択し、「**削除**」をクリックして削除します。

元のネットワーク...	説明
使用不可	次の手順を実行できます。 • ネットワークアダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、影響を受けるネットワークアダプタを編集して、仮想マシンを新しいネットワークに接続します。 • 影響を受けるネットワークアダプタを選択して削除し、「**削除**」をクリックします。 • 「**新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。

> 注 仮想マシンはネットワークアダプタなしでクローンできます。後で必ず仮想マシンのネットワーク設定を構成してください。

b. *仮想マシンを別のNutanixクラスターまたはvSphere環境に復元する場合のみ*。復元した仮想マシンで元のMACアドレスを維持する場合は、「**元のMACアドレスを維持**」スイッチを使用します。これは、少なくとも1つのネットワークアダプタにMACアドレスが割り当てられている場合にのみ適用されることにご注意ください。

7. 「**復元**」をクリックします。

仮想マシンの複製後

仮想マシンの複製後は、以下について考慮してください。

- クローンされた仮想マシンのネットワークアダプタに新しいMACアドレスが割り当てられている場合、ゲストオペレーティングシステムが、クローンされた仮想マシンを、選択したネットワークに接続するように適切に構成されていることを確認します。
- 仮想マシンをNutanix AHVクラスターからNutanix ESXiクラスターまたはvSphere環境に複製した後で、IDEデバイスが正しく構成されていないことにより仮想マシンが起動しない場合には、手動でIDEデバイスの構成を編集する必要があります。この実行方法の詳細については、VMwareの資料を参照してください。
- *vSphere環境の場合*：一部のオペレーティングシステム(たとえば、RHEL 7) は、ネットワーク構成を必要とする場合があります。詳細については、VMwareの資料を参照してください。
- *iSCSIを使用してボリュームグループがアタッチされている仮想マシンの場合*：元の仮想マシンと復元された仮想マシンは、復元後に同じネットワークとiSCSI構成設定を持つため、潜在的な問題を回避するために、両方の仮想マシンが同時にオンにならないようにしてください。問題を防ぐ1つの方法として、復元した仮想マシンをオンにする前にネットワークから切断し、ネットワークアダプタの交換やiSCSI設定の更新などの必要な変更を行うことができます。
- *物理マシンの場合*：
  - *Windows物理マシンをNutanix ESXiクラスターにクローンした場合のみ*。復元後に適切なゲストOSを指定してマシン構成を変更し、最新バージョンのVMware Toolsをマシンにインストールしてください。詳細については、VMwareの資料を参照してください。

- *UEFIファームウェアを使用するLinux物理マシンをNutanix AHVクラスターにクローンした場合のみ*。復元後に仮想マシンが起動しない場合は、マシンを再起動します。

BIOSファームウェアを使用するLinux物理マシンのブート構成の更新

手順

1. `/etc/default/grub`システム構成ファイルで、以下を実行します。
   a. 「`GRUB_CMDLINE_LINUX`」オプションを編集して、以下のカーネルパラメーターがある場合は削除します。
      - `rd.lvm.`(`rd.lvm=0`を除く)
      - `rd.md.`(`rd.md=0`を除く)
      - `rd.dm.`(`rd.dm=0`を除く)
      - `rd.luks.`
   b. 仮想マシンのレジュームデバイスが、元の物理マシンのレジュームデバイスUUIDと一致するように設定します。たとえば、元の物理マシンのレジュームデバイスが `resume=/dev/mapper/cl-swap`の場合、仮想マシンのレジュームデバイスは `resume=UUID=4044243b-612b-42bc-ba22-4736c4eadde6`とします。
2. *オプション*:ブートプロセスを高速化し、存在しないボリュームのマウントをスキップしたい場合は、`/etc/fstab`システム構成ファイルで、バックアップ時に警告がトリガーされたボリュームの行をすべてコメントにします。

   例
   以下の警告メッセージがトリガーされます。

   `Non LVM volumes detected: Following volumes are not backupable: /dev/sdf3:/test_mount.`

   `/etc/fstab`システム設定ファイルで、`/test_mount`マウントポイントを含む行をコメントします。
3. 以下のコマンドを実行して、GRUB構成を更新します。

   ```
   grub2-mkconfig -o /boot/grub2/grub.cfg
   ```
4. 以下のコマンドを実行して、ブートローダーをブートディスクにインストールします。

   ```
   grub2-install /dev/sdc
   ```

   > **ヒント** ブートディスクにブートパーティションが含まれます。ブートパーティションを特定するには、以下のコマンドを実行します。
   >
   > ```
   > findmnt -nT /boot -o SOURCE
   > ```
5. 仮想マシンを再起動します。

UEFIファームウェアを使用するLinux物理マシンのブート構成の更新

手順

1. *物理マシンをNutanix ESXiクラスターまたはvSphere環境にクローンした場合のみ*。仮想マシンがファームウェアセットアップモードになったら、「**ファイルからブート**」オプションを選択し、`<EFIPartition>/EFI/hycu/shimx64.efi`ファイルを指定します。詳細については、NutanixまたはVMwareの資料を参照してください。
2. `/etc/default/grub`システム構成ファイルで、以下を実行します。
   a. 「`GRUB_CMDLINE_LINUX`」オプションを編集して、以下のカーネルパラメーターがある場合は削除します。
      - `rd.lvm.`(`rd.lvm=0`を除く)
      - `rd.md.`(`rd.md=0`を除く)
      - `rd.dm.`(`rd.dm=0`を除く)
      - `rd.luks.`

   b. 仮想マシンのレジュームデバイスが、元の物理マシンのレジュームデバイスUUIDと一致するように設定します。たとえば、元の物理マシンのレジュームデバイスが `resume=/dev/mapper/cl-swap`の場合、仮想マシンのレジュームデバイスは `resume=UUID=4044243b-612b-42bc-ba22-4736c4eadde6`とします。
3. *オプション*:ブートプロセスを高速化し、存在しないボリュームのマウントをスキップしたい場合は、`/etc/fstab`システム構成ファイルで、バックアップ時に警告メッセージがトリガーされたボリュームの行をすべてコメントにします。

   例
   以下の警告メッセージがトリガーされます。

   ```
   Non LVM volumes detected: Following volumes are not backupable:
   /dev/sdf3:/test_mount.
   ```

   `/etc/fstab`システム設定ファイルで、`/test_mount`マウントポイントを含む行をコメントします。
4. 以下のコマンドを実行して、GRUB構成を更新します。
   - Red Hat Enterprise LinuxおよびOracle Linuxの場合：

     ```
     grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
     ```

   - CentOSの場合：

     ```
     grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
     ```
5. 仮想マシンを再起動します。
6. *元の物理マシンでセキュアブートが有効になっており、サードパーティのカーネルモジュールを使用する場合のみ*。サードパーティのカーネルモジュールに署名するために使用されるマシン所有者キー(MOK) を登録します。この実行方法の詳細については、それぞれのオペレーティングシステムの資料を参照してください。

7. UEFIファームウェアのセットアップで既定のブートエントリを作成します。ブートエントリは次のシステムファイルを指す必要があります。
   - Red Hat Enterprise LinuxおよびOracle Linuxの場合：

     ```
     <EFIPartition>/EFI/redhat/shimx64.efi
     ```

   - CentOSの場合：

     ```
     <EFIPartition>/EFI/centos/shimx64.efi
     ```

仮想マシンのバックアップの検証

仮想マシンのバックアップは、仮想マシンのクローンを作成することで検証できます。この場合、元の仮想マシンが上書きされたりオフになったりすることはありません。バックアップの検証を実行した後に、仮想マシンのクローンを保持するかどうかを指定することもできます。

> 注 検証ポリシーをセットアップし、検証ポリシーで定義した値に従ってバックアップ検証をスケジュールすることができます。この実行方法の詳細については、“検証ポリシーのセットアップ” ページ191を参照してください。

前提条件

- 仮想マシンをvSphere環境に複製する場合、仮想マシンに最新バージョンのVMware Toolsがインストールされている必要があります。
- *高度な検証タイプを指定することを予定している場合のみ。*
  - 資格情報を仮想マシンに割り当てる必要があります。前提条件、制限、考慮事項、説明については、“アプリケーションデータへのアクセスの有効化” ページ113を参照してください。
  - ネットワークカードを仮想マシンに追加する必要があります。

制限事項

HYCU Backup Controllerに対するバックアップ検証の実行はサポートされていません。

考慮事項

- 仮想マシンが静的IPアドレスで構成されている場合、バックアップ検証中にネットワークの競合が発生し、バックアップ検証データの信頼性が低下する可能性があります。
- *Windows仮想マシンのバックアップ検証を実行するときに、高度な検証タイプを指定することを予定している場合のみ。*ディスクエラーのチェックが失敗する場合もありますが、これは仮想マシンが破損していることを意味するものではありません。ただし、そのような仮想マシンのステータスは手動で確認することをお勧めします。
- バックアップの検証を実行した後、次のことを検討します。
  - 「仮想マシン」パネルの「検証」列で、仮想マシンのバックアップ検証ステータスを表示できます(アイコンで表される)。アイコンを一時停止することで、仮想マシンにどの検証ポリシーが割り当てられているかも確認できます(セットアップ済みの場合)。検証ポリシーのセットアップ

の詳細については、“検証ポリシーのセットアップ” ページ191を参照してください。

- 除外ポリシーは、クローンされた仮想マシンに自動的に割り当てられます。

手順

1. 「仮想マシン」パネルで、バックアップ検証を実行する仮想マシンをクリックします。画面の下部に「詳細ビュー」が表示されます。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 「詳細ビュー」で、目的の復元ポイントを選択します。
3. 「**VMの復元**」をクリックします。
4. 「**VMバックアップを検証**」を選択して、「**次へ**」をクリックします。
5. 「ストレージコンテナ」ドロップダウンメニューから、バックアップ検証を実行する仮想マシンのクローンを作成する場所を選択します。
6. 「復元元」ドロップダウンメニューから、バックアップ検証に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動**
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**

   > 注「自動」を選択した場合、バックアップ検証の階層は、既定では、バックアップ > コピー > アーカイブ > スナップショットという優先順位で選択されます。これは、HYCUが常に、バックアップ検証のために指定された順序で最初に利用可能な層を使用することを意味します。ただし、この既定の動作は、HYCU `config.properties`ファイルの `backup.validation.restore.source.priority.order`構成設定をカスタマイズして、データ保護のニーズに合わせて層の順序を調整することで、いつでも変更できます。HYCU構成設定のカスタマイズ方法の詳細については、“HYCU構成設定のカスタマイズ” ページ308を参照してください。

7. 「新しいVM名」フィールドで、クローンされた仮想マシンの名前を指定します。
8. クローンされた仮想マシンを元の仮想マシンと同じ構成設定にする場合は、「**元のVM設定を使用**」スイッチを使用します。

   構成設定のいずれかを変更する場合は、「**元のVM設定を使用**」スイッチを無効にして、以下を実行します。

   - 「vCPU(s)」フィールドに、クローンした仮想マシンの仮想CPU数を入力します。仮想CPUの最大数は1024です。
   - 「vCPUあたりのコア数」フィールドに、クローンした仮想マシンの仮想CPUあたりのコア数を入力します。仮想CPUあたりの最大コア数は64です。

     > 注 クローンした仮想マシンのコア数の合計は、仮想CPU数に仮想CPUあたりのコア数を掛けた数となります。

- 「メモリ」フィールドで、クローンした仮想マシンのメモリ量(GiBまたはMiB単位)を設定します。指定する値は整数でなければならず、4096 GiBを超えることはできません。

9. 「検証後にVMを保持」ドロップダウンメニューから、バックアップ検証の実行後に仮想マシンを保持するかどうかに応じて、次のオプションのいずれかを選択します。

オプション	説明
常に	仮想マシンは、バックアップ検証の実行後に、常に保持されます。
検証エラー時	仮想マシンは、検証時に検証エラーが発生した場合にのみ、バックアップ検証の実行後に保持されます。
決して	仮想マシンは、バックアップ検証の実行後に、自動的に削除されます。

10. 「検証タイプ」ドロップダウンメニューから、以下のいずれかのタイプを選択します。

検証タイプ	説明
基本	バックアップ検証時に、以下のタスクが行われます。 • 仮想マシンがクローンされ、オンになります。 • ゲストOSがシャットダウンします。
高度	バックアップ検証時に、以下のタスクが行われます。 • 仮想マシンがクローンされ、オンになります。 • 仮想マシン上で実行しているすべてのアプリケーションが検出されます。 • 仮想ディスクが検証され、それには仮想マシンのファイルシステムや仮想マシン上の既存のディスクの確認が含まれます。Windows仮想マシンの場合、ディスクエラーの確認も行われます。 • 指定された場合、カスタムスクリプトが実行されます。 • ゲストOSがシャットダウンします。

11. *高度な検証タイプを選択した場合のみ*。以下を実行します。

    a. バックアップ検証プロセスの一部として仮想マシン上でカスタムスクリプトを実行する場合は、「**カスタムスクリプトを実行**」スイッチを有効にし、スクリプトへの適切なパスが指定されていることを確認します。

    > 注 正常に終了した場合はスクリプトは終了コード0を返し、失敗の場合はそれ以外を返します。

    b. 「ネットワーク」セクションで、バックアップ時に仮想マシンに追加されたネットワークアダプタのリストを確認します(仮想マシンが接続されていたネットワークを含む)。元のネットワークのいずれかが利用できなくなった場合は、「該当なし」が表示されます。

    元のネットワークが使用可能かどうかに応じて、以下のように続行します。

    - 元のネットワークが利用可能な場合は、既定値を変更せずに元のネットワーク設定で仮想マシンをクローンするか、またはネットワーク設定を変更することができます。

- 元のネットワークが利用できない場合は、ネットワーク設定を変更する必要があります。

ネットワーク設定の変更

元のネットワーク...	説明
使用可能	次の手順を実行できます。 • 「＋ **新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。 • 仮想アダプタを選択し、「✎ **編集**」をクリックして優先するネットワークを選択することで、既存のネットワークアダプタを編集して、仮想マシンを別のネットワークに接続します。 • 必要なくなったネットワークアダプタの資格情報を選択し、「🗑 **削除**」をクリックして削除します。
使用不可	次の手順を実行できます。 • ネットワークアダプタを選択し、「✎ **編集**」をクリックして優先するネットワークを選択することで、影響を受けるネットワークアダプタを編集して、仮想マシンを新しいネットワークに接続します。 • 影響を受けるネットワークアダプタを選択して削除し、「🗑 **削除**」をクリックします。 • 「＋ **新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。

12. 「**検証**」をクリックします。

仮想ディスクの復元

仮想ディスクは元の場所または新しい場所に復元できます。この場合、元の仮想ディスクは上書きされます。

制限事項

「vDiskの復元」オプションを使用した物理マシンディスクの復元はサポートされていません。

考慮事項

- バックアップから除外された仮想ディスクがある場合、それらを選択して復元することはできません。対応する復元ポイントのラベルは赤い丸でマークされています。詳細については、"エンティティ詳細の表示" ページ174を参照してください。
- 元の仮想ディスクは削除され、復元された仮想ディスクは、バックアップ時にアタッチされていたすべての仮想マシンに自動的にアタッチされます。
- *仮想マシンにアタッチされているボリュームグループを復元する場合のみ*。ボリュームグループがアタッチされている仮想マシンがオフになっている必要があります。

「仮想マシン」パネルへのアクセス

ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、仮想ディスクを復元する仮想マシンをクリックします。
2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

3. 「**VMの復元**」をクリックします。
4. 「**vDiskの復元**」を選択して、「**次へ**」をクリックします。
5. 復元に選択できる仮想ディスクのリストから、復元するディスクを選択し、「**次へ**」をクリックします。

   > 重要 *仮想マシンにアタッチされているボリュームグループを復元する場合のみ*。個別のディスクは選択できず、ボリュームグループ全体のみを選択できます。

6. 「ストレージコンテナ」ドロップダウンメニューから、仮想ディスクを復元する場所を選択します。

   > 注既定では、元のストレージコンテナが選択されます。仮想ディスクを別のストレージコンテナに復元することを決定した場合、スナップショットからは復元されず、ターゲットから復元されます。したがって、高速復元は実行されません。

7. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :このタイプの復元では、最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット** *(Nutanixクラスターのみ)*
8. 「**復元**」をクリックします。

仮想ディスクのクローン

仮想ディスクを元の場所または新しい場所に復元することで、仮想ディスクのクローンを作成できます。この場合、元の仮想ディスクは上書きされません。

制限事項

「vDiskのクローン」オプションを使用したvSphere仮想マシンディスクの復元はサポートされていません。

考慮事項

- バックアップから除外されている仮想ディスクがある場合、それらを選択して復元することはできません。対応する復元ポイントのラベルは赤い丸でマークされています。詳細については、"エンティティ詳細の表示" ページ174を参照してください。
- *仮想マシンにアタッチされているボリュームグループを復元する場合のみ*。元のボリュームグループは復元されたボリュームグループと一緒に保持され、そのアタッチに関して次のことが適用されま

す。

- ボリュームグループを元の仮想マシンに復元する場合、それらはバックアップ時にアタッチされていたすべての仮想マシンにアタッチされます。
- ボリュームグループをNutanix AHVクラスターで実行されている元の仮想マシン以外の仮想マシンに復元する場合、それらは選択された仮想マシンにのみアタッチされます。ボリュームグループをNutanix ESXiクラスターで実行されている元の仮想マシン以外の仮想マシンに復元する場合、それらは復元後に手動でアタッチする必要があります。

クローンされたボリュームグループの名前の形式は、以下のとおりです。

`<OriginalVGName>-<Timestamp>`

- *仮想マシンディスクの場合：*
  - 元の仮想マシンディスクは、最初に使用可能なインターフェースインデックスとして(インターフェースタイプごとに)仮想マシンに自動的にアタッチされる、復元された仮想マシンディスクと一緒に保持されます。たとえば、`scsi.0`、`scsi.1`、および`scsi.4`仮想ディスクがすでに仮想マシンにアタッチされている場合、復元された仮想ディスクは`scsi.2`になります。
  - 元の仮想ディスクのバスタイプがIDEの場合、復元中に自動的にSCSIに変更されます。

> 「仮想マシン」パネルへのアクセス
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、仮想ディスクを復元する仮想マシンをクリックします。
2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

3. 「**VMの復元**」をクリックします。
4. 「**vDiskのクローン**」を選択して、「**次へ**」をクリックします。
5. 復元に選択できる仮想ディスクのリストから、復元するディスクを選択し、「**次へ**」をクリックします。

   > 重要 *仮想マシンにアタッチされているボリュームグループを復元する場合のみ。*個別のディスクは選択できず、ボリュームグループ全体のみを選択できます。

6. 「VM」ドロップダウンメニューから、復元された仮想ディスクをアタッチする仮想マシンを選択します。復元された仮想ディスクは、元の仮想マシン(既定の選択)または他の仮想マシンにアタッチできます。以下について考慮してください。
   - 仮想ディスクを元の仮想マシンにアタッチする場合は、それがオンになっていることを確認してください。
   - 復元されたディスクを物理マシンにアタッチすることはできません。
7. 「ストレージコンテナ」ドロップダウンメニューから、仮想ディスクを復元する場所を選択します。

   > 注 *仮想マシンの場合* 選択した仮想マシンが存在するNutanixクラスター上に作成されたストレージコンテナからのみ選択できます。

8. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :このタイプの復元では、最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット** *(Nutanixクラスターのみ)*
9. 「**復元**」をクリックします。

仮想ディスクのエクスポート

仮想ディスクをNFSまたはSMB共有に復元できます。エクスポートした仮想ディスクを使用してデータを物理マシンに復元できます。詳細については、"物理マシンへのデータの復元" 次のページを参照してください。

前提条件

仮想ディスクをSMB共有に復元する場合 SMBサーバーは、スパースファイルの作成を停止するように構成されている(`smb.conf`ファイルで`strict allocate`パラメーターが`yes`に設定されています) 。

考慮事項

バックアップから除外された仮想ディスクがある場合、それらを選択して復元することはできません。対応する復元ポイントのラベルは赤い丸でマークされています。詳細については、"エンティティ詳細の表示" ページ174を参照してください。

> 「仮想マシン」パネルへのアクセス
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、仮想ディスクを復元する仮想マシンをクリックします。
2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。
3. 「**VMの復元**」をクリックします。
4. 「**vDiskのエクスポート**」を選択して、「**次へ**」をクリックします。

   > ⚠ 重要 仮想ディスクの復元中には、この仮想マシンの追加の復元を実行したり、バックアップを期限切れにしたりすることはできません。
5. 復元に選択できる仮想ディスクのリストから、復元するディスクを選択し、「**次へ**」をクリックします。
6. 「タイプ」ドロップダウンメニューから、仮想ディスクを復元する場所を選択し、必要な情報を入力します。

- **SMB**
  a. *オプション*:ドメインとユーザー資格情報を入力します。
  b. SMBサーバー名またはIPアドレス、およびサーバーのルートからのSMB共有フォルダへのパスを入力します(たとえば、/backups/HYCU) 。
- **NFS**
  NFSサーバー名またはIPアドレス、およびサーバーのルートからのNFS共有フォルダへのパスを入力します(たとえば、/backups/HYCU) 。

7. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   • **自動** :このタイプの復元では、最新の状態に最速で復元できます。
   • **バックアップ**
   • **コピー**
   • **アーカイブ**
   • **スナップショット** *(Nutanixクラスターのみ)*
8. 「**復元**」をクリックします。

仮想ディスクのエクスポート後

仮想ディスクの復元が完了したら、それを使用してデータを物理マシンや、HYCUにサポートされていないあるいはソースとしてHYCUに追加されていないハイパーバイザーのある環境に復元することができます。

データは次の場所に復元されます。

/<SharedPath>/<VMName>/<Timestamp>/<Filename>

この場合、*<SharedPath>*は共有フォルダへのパス、*<VMName>*は仮想マシン名、*<Timestamp>*は復元の時間、*<Filename>*は仮想マシンディスクのUUIDです。

復元により作成されるファイルの種類は、復元した仮想ディスクを持つ仮想マシンがバックアップされている環境により異なります。お使いの環境にあるハイパーバイザーのタイプに応じて、選択した各ディスクに対して以下のファイルが作成されます。

ハイパーバイザー	ファイル
Nutanix AHV	*<DiskName>*(拡張子なし) 割り当てられていないスペースをゼロとして含む、ディスクのローイメージ
Nutanix ESXi	
vSphere	• *<DiskName>*-flat.vmdk ディスクのローイメージ • *<DiskName>*.vmdk *<DiskName>*-flat.vmdkを参照するVMDK記述子ファイル

物理マシンへのデータの復元

このセクションで説明する手順は、データをWindows物理マシンに復元する方法の一例です。

前提条件

- データの復元先とする物理マシンは、元のマシンと同じ数のディスクを持ち、ディスクサイズは元のサイズ以上であること。
- LinuxライブCD(Ubuntuなど) をダウンロード済みであり、データを復元する物理マシン上で起動済みであること。

考慮事項

- コマンドはすべてルートとして実行してください。
- 以下のエラーメッセージは無視してもかまいません。

  ```
  The backup GPT table is corrupt, but the primary appears OK, so that will be used.
  ```

手順

1. 宛先ディスクを特定します。

   HYCUはバックアップをディスクレベルで実行するため、データを復元する各ディスクのパスを特定する必要があります。システム上のすべてのディスクをリストするには、次のコマンドを実行します。

   ```
   fdisk -l
   ```

   以下は出力の例です。

   ```
   Disk /dev/sda: 32 GiB, 34359738368 bytes, 67108864 sectors
   Disk /dev/sdb: 5 GiB, 5368709120 bytes, 10485760 sectors
   ```

2. ディスクをエクスポートした共有をマウントします。
3. 以下のコマンドを実行して、マウントした共有上のエクスポートしたディスクへのパスを特定します。

   ```
   cd /<共有パス>/<VM名>/<タイムスタンプ>
   ```

   ```
   ls
   ```

   以下は出力の例です。

   ```
   PhysicalDisk0 PhysicalDisk1
   ```

4. 以下のコマンドを実行して、エクスポートした各ディスクを検証します。

   ```
   fdisk -l <エクスポートしたディスク名>
   ```

   例：

   ```
   fdisk -l PhysicalDisk0
   ```

   エクスポートしたディスクの情報(ディスクサイズやパーティションのリストなど) が表示されます。この情報を使用して、データの復元に適した宛先ディスクを特定します。たとえば、エクスポートしたディスクPhysicalDisk0のサイズはディスク/dev/sdaのサイズに一致します。したがって、ディスクPhysicalDisk0はディスク/dev/sdaに復元できます。

以下は出力の例です。

```
Disk PhysicalDisk0: 32 GiB, 34359738368 bytes, 67108864 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x36bab260
Device Boot Start End Sectors Size Id Type
PhysicalDisk0p1 * 2048 718847 716800 350M 7
HPFS/NTFS/exFAT
PhysicalDisk0p2 718848 67106815 66387968 31.7G 7
HPFS/NTFS/exFAT
```

5. 各ディスクに対して以下のコマンドを実行して、データを復元します。

```
dd if=<エクスポートしたディスク名> of=<宛先ディスクのパス> bs=1024 status=progress
```

例：

```
dd if=PhysicalDisk0 of=/dev/sda bs=1024k status=progress
```

以下は出力の例です。

```
33540483072 bytes (34 GB, 31 GiB) copied, 229 s, 146 MB/s
33554432+0 records in
33554432+0 records out
34359738368 bytes (34 GB, 32 GiB) copied, 229.78 s, 150 MB/s
```

6. Linuxライブ CDを取り出し、物理マシンを再起動します。

個別のファイルの復元

個別のファイルは元の仮想マシンまたは違う仮想マシン、SMBまたはNFS共有、あるいはローカルマシンに復元できます。仮想マシン全体を復元する代わりに、破損したか、何らかの理由で削除され、現在は仮想マシンに存在しない1つ以上のファイルのみを復元できます。

個々のファイルは、ターゲットまたはスナップショットから復元できます。選択した復元ポイントでスナップショットが使用可能な場合、復元は常にスナップショットから実行されます(これにより、復元プロセスが高速化します) 。そうでない場合、復元はターゲットから実行されます(これにより環境のスペースが節約されます) 。スナップショットから個々のファイルを復元したいものの、選択した仮想マシンの復元ポイントで使用可能なスナップショットがない場合は、HYCUを使用して手動で再作成できます。この実行方法の詳細については、“スナップショットの再作成” ページ195を参照してください。

プレリストア/ポストリストアスクリプトを使用して、個別のファイルの復元が実行される前と後に必要なアクションを実行できます。スクリプトの指定方法の詳細については、このセクションで説明する手順に

従います。終了コードとエクスポートされた環境変数の詳細については、“プレ/ポストスクリプトの使用” ページ272を参照してください。

前提条件

Windows仮想マシン	• NTFS、FAT、またはFAT32ファイルシステムが使用されている。 • 復元のパフォーマンスの向上のために、Microsoft iSCSIイニシエーターサービスの始動タイプが「`Disabled`」に設定されていない。 • *ファイルを仮想マシンに復元する場合：* ◦ *Windows 8および10仮想マシンの場合：*WinRMが有効であり、`winrm quickconfig`コマンドを使用して構成されている。 ◦ WinRMアクセス許可が付与され、仮想マシンのローカルAdministratorsグループのメンバーであるWindowsオペレーティングシステムユーザーアカウントが存在している。 ◦ 仮想マシンのファイルシステムへのアクセスが有効である。説明については、“データへのアクセスの有効化” ページ79を参照してください。 ◦ *プレ/ポストリストアスクリプトの場合：*スクリプトは、アクセス可能なフォルダにあり、拡張子は`bat`、`ps1`、`cmd`のいずれかです。
Linux仮想マシン	• FAT32、xfs、ext4/ext3/ext2、reiserfs、またはbtrfsファイルシステムが使用されている。 • `/etc/fstab`システム構成ファイルエントリ内の参照で、エントリが論理ボリューム(`/dev/mapper/ol-root`など) を参照しない限り、デバイス名(`/dev/sda1`など) ではなく、UUID(`UUID=8ff089c0-8e71-4320-a8e9-dbab8f18a7e5`など) を使用している。 • *ファイルを仮想マシンに復元する場合：* ◦ SSHを介した仮想マシンへのアクセスが有効である。 ◦ 仮想マシンのファイルシステムへのアクセスが有効である。説明については、“データへのアクセスの有効化” ページ79を参照してください。 ◦ *プレ/ポストリストアスクリプトの場合：*スクリプトは、アクセス可能なフォルダにあり、拡張子は`sh`です。割り当てられた資格情報を使用して仮想マシンでスクリプトを実行する許可があります。
Nutanix ESXiクラスター	• *ファイルを仮想マシンに復元する場合：*最新バージョンのVMware ToolsとNGTがクライアント仮想マシンにインストールされている。 VMware Toolsのインストールの詳細については、VMwareの資料を参照してください。NGTのインストールの詳細については、Nutanixの資料を参照してください。
vSphere環境	• 割り当てられている必要な復元特権がある。詳細については、“vSphereユーザーへの特権の割り当て” ページ269を参照してください。

制限事項

- デュアルブートシステムでの個別のファイルの復元はサポートされていません。
- テープからのデータの復元はサポートしていません。
- Linuxでは、シンボリックリンクとソフトリンクのみを元の場所に復元できます。
- 2人の異なるユーザーが同じスナップショットから同時にファイルを復元することはできません。
- *ファイルを別の仮想マシンに復元する場合*：元のシステムと同じオペレーティングシステムファミリに属する仮想マシンにのみファイルを復元できます。
- *ファイルをローカルマシンに復元する場合*：サイズが2 GiB以下のデータアーカイブのみダウンロードできます。
- すべての仮想マシンディスクをバックアップから除外し、アタッチされたボリュームグループのみを残した場合、個々のファイルを復元することはできません。
- *「ストレージレプリカ」が有効なNutanixクラスター上で実行されているWindows仮想マシンの場合*：個別ファイルの仮想マシンへの復元は、その復元がターゲットから実行される場合にのみサポートされます。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため)がある層が含まれている場合、データを復元するためにこの層を使用することはできません。
- ポリシーに指定された保持期間が経過してしまっている(復元ポイントがHYCU Webユーザーインターフェースでグレー表示になっている)仮想マシンの復元は実行できません。ただし、必要な場合、これはHYCU `config.properties`ファイル内の `restore.enabled.if.retention.is.up`構成設定を`true`に設定することで上書きできます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。
- *ファイルを仮想マシンに復元する場合*：一部のタイプのファイル(システムファイルなど)を復元できるようにするには、仮想マシンにアクセスするために指定するアカウントは、Windowsでは仮想マシンのローカルのAdministratorsグループのメンバーであり、Linuxではroot権限を持つものである必要があります。
- バックアップから除外されている仮想ディスクがある場合、それらを選択して復元することはできません。対応する復元ポイントのラベルは赤い丸でマークされています。詳細については、"エンティティ詳細の表示" ページ174を参照してください。
- *レプリカオプションからのバックアップを使用する場合*：中央またはリモートサイト(元の場所)に復元する場合、復元は常に中央サイトのスナップショットから実行されます。
- *プレ/ポストリストアスクリプトの場合*：プレ/ポストリストアスクリプトは、ファイルを仮想マシンに復元する場合のみ指定できます。

推奨事項

多数のファイルを復元する場合のみ。個別のファイルを復元する代わりに、「vDiskのクローン」オプションを使用してファイルをホストしているディスクを復元することを強くお勧めします。説明については、"仮想ディスクのクローン" ページ102を参照してください。

「仮想マシン」パネルへのアクセス

ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、復元するファイルを含む仮想マシンをクリックして、「詳細ビュー」を開きます。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。
3. 「**ファイルの復元**」をクリックします。「ファイルの復元」ダイアログボックスが開きます。
4. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**
5. 「**次へ**」をクリックします。
6. 使用可能なファイルのリストから、復元するファイルを選択し、「**次へ**」をクリックします。

   > ヒントファイルが多すぎて表示が1ページに収まらない場合、「 > 」と「 < 」をクリックしてページを移動できます。
   >
   > さらに、ファイルまたはフォルダを検索するには、「検索」フィールドに名前を入力し、**Enter**を押します。

7. 選択したファイルの復元先(同じ仮想マシン、別の仮想マシン、外部SMBまたはNFS共有、またはローカルマシン)に応じて、希望する復元オプションを選択し、「**次へ**」をクリックして、指示に従います。

復元オプション	説明
仮想マシンに復元	a. 「全般」タブで、次の手順を実行します。 i. 「仮想マシン」ドロップダウンメニューから、ファイルの復元先とする仮想マシンを選択します。ファイルは元の仮想マシンまたは違う仮想マシンに復元できます。 ii. ファイルを元の場所に復元するか、別の場所に復元するか選択します。

復元オプション	説明
	別の場所を選択する場合、その場所へのパスを次の形式で指定します。 `C:\<Path>` iii. 選択した場所にすでに同じ名前のファイルが存在した場合に、復元操作中に実行するアクションを指定します(ファイルの上書き、ファイルのスキップ、元のファイルの名前変更、または復元したファイルの名前変更)。 iv. 元のアクセス制御リストを復元する場合は、「**ACLの復元**」スイッチを使用します。 ⚠ 重要 さまざまな理由により仮想マシンにアクセスできない場合(たとえば、資格情報が割り当てられていない、検出に失敗した、オフになっている、またはソースから削除されているなど)、個別のファイルを復元するためにその仮想マシンを選択することはできません。 b. *オプション*:「**プレ/ポストスクリプト**」タブをクリックします。選択したスイッチを使用して、プレ/ポストリストアスクリプトを指定し、スクリプトのパス名を入力します。1つ以上のスイッチを有効にします。 • **プレリストアスクリプトの実行** • **ポストリストアスクリプトの実行** 📋 注 スクリプトのパス名フィールドに、サンプルのパス名が表示されます。必ず有効なスクリプトパス名を入力します。 c. 「**保存**」をクリックします。 d. 「**復元**」をクリックします。
外部共有に復元する	a. ファイル共有の場合は「**NFS**」または「**SMB**」を選択し、共有フォルダへのパスを次の形式で指定します。 `\\server\<Path>` b. *SMBの場合*: SMB共有にアクセスするためのユーザー資格情報を入力します(オプション)。 c. 選択した場所にすでに同じ名前のファイルが存在した場合に、復元操作中に実行するアクションを指定します(ファイルの上書き、ファイルのスキップ、元のファイルの名前変更、または復元したファイルの名前変更)。 d. 「**復元**」をクリックします。
ダウンロード	「**ダウンロード**」をクリックして、選択したファイルをローカルマシンに復元します。

復元オプション	説明
	⚠ 重要 ダウンロード処理が終了するまで、ページの更新やページからの移動はしないでください。

第5章

アプリケーションの保護

HYCUにより、高速で信頼性の高いバックアップと復元によりアプリケーションデータを保護できます。HYCUを仮想マシンで実行中のアプリケーションにアクセスできるようにし、必要な準備手順を完了し、アプリケーションをバックアップしたら、アプリケーション全体または特定のアプリケーション項目のみのいずれかを復元することを選択できます。

> 注 仮想マシン上にあるアプリケーションの保護についての説明は、特に断りのない限り、物理マシン上のアプリケーションにも適用されます。

アプリケーションデータを効率的に保護する方法の詳細については、以下のセクションを参照してください。

- “アプリケーションデータへのアクセスの有効化” 下
- “アプリケーション保護の計画” ページ115
- “アプリケーションのバックアップ” ページ121
- “アプリケーション全体の復元” ページ122
- “SQL Serverデータベースの復元” ページ130
- “Exchange Serverデータベース、メールボックス、およびパブリックフォルダの復元” ページ133
- “Oracleデータベースのインスタンスと表領域の復元” ページ136

アプリケーションデータへのアクセスの有効化

“データへのアクセスの有効化” ページ79で説明されているとおりに資格情報を仮想マシンに割り当てると、アプリケーション検出プロセスが自動的に開始します。

アプリケーション検出ジョブが完了すると、検出されたアプリケーションは「アプリケーション」パネルにリストされます。HYCUは仮想マシンと物理マシンでさまざまなタイプのアプリケーションをサポートします。サポートされるアプリケーションの種類については、*HYCU互換性マトリックス*を参照してください。

保護するアプリケーションの検出ステータスに応じて、以下のいずれかを実行します。

✔	HYCUは仮想マシンの資格情報でアプリケーションにアクセスすることができ、アプリケーションの保護を開始できます。説明については、“アプリケーションのバックアップ” ページ121を参照してください。 > 注 Active DirectoryとSAP HANAへのアクセスは、仮想マシンの資格情報が必ず付与されます。

⊗	仮想マシンの資格情報には適切な権限がなく、HYCUアプリケーションにアクセスできません。HYCUがアプリケーションにアクセスできるようにするには、以下のいずれかを実行します。 • 仮想マシンの資格情報を使用する場合は、仮想マシンに資格情報を再割り当てして、適切な権限が付与されるようにします。仮想マシンへの証明書の割り当て方法に関する説明については、"データへのアクセスの有効化" ページ79を参照してください。 • アプリケーション固有の資格情報を使用する場合は、このセクションで説明する手順に従います。

前提条件

Windows仮想マシン	• *Windows 8および10の場合*：WinRMが有効であり、`winrm quickconfig`コマンドを使用して構成されている。 • WinRM許可を持つWindowsユーザーアカウントが存在する。このアカウントにはアプリケーションへのアクセス権が必要であり、仮想マシンのローカルのAdministratorsグループのメンバーである必要があります。 • 仮想マシンのファイルシステムへのアクセスが有効である。説明については、"データへのアクセスの有効化" ページ79を参照してください。
Linux仮想マシン	• SSHを介した仮想マシンへのアクセスが有効である。 • 仮想マシンのファイルシステムへのアクセスが有効である。説明については、"データへのアクセスの有効化" ページ79を参照してください。
Nutanix ESXiクラスター	VMware ToolsとNGTがクライアント仮想マシンにインストールされている。 VMware Toolsのインストールの詳細については、VMwareの資料を参照してください。NGTのインストールの詳細については、Nutanixの資料を参照してください。

アプリケーション固有の前提条件

SQL Server	• アクセスは、SQL Serverフェールオーバークラスターおよび SQL Server Always On可用性グループインスタンスがあるすべての仮想マシン上で有効である必要がある。 • *SQL ServerAlways On可用性グループの場合*：可用性グループは、自動シードを使用して作成される。
Oracle	• OSユーザーには、sudo特権があり、NOPASSWDオプションが設定されている必要がある。

考慮事項

Oracleアプリケーションの場合：オペレーティングシステムがOracleデータベースユーザーの認証に使用される場合、OracleデータベースはOSユーザー資格情報でアクセスできます。これによりアプリケーショ

ンデータへのアクセスを提供する手順はスキップできます。そのような認証モードを有効にするには、Oracleデータベース管理者にお問い合わせください。

> 「アプリケーション」パネルへのアクセス
>
> 「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「アプリケーション」パネルで、保護するアプリケーションを選択します。
2. 「**構成**」をクリックします。「構成」ダイアログボックスが開きます。
3. 使用する資格情報に応じて、次のいずれかを実行します。
   - 仮想マシンの資格情報を使用する場合は、「**保存**」をクリックします。
   - アプリケーション固有の資格情報を使用する場合は、次の手順を実行します。
     a. 「**アプリケーションへのアクセス権を持つVM資格情報を使用します**」スイッチを無効にします。
     b. 必要な権限を持つユーザーアカウントの資格情報を入力して、アプリケーションにアクセスします。次の要件が満たされていることを確認します。
        - *Windows仮想マシン上で実行するアプリケーションの場合*：指定するアカウントは、仮想マシンのローカルAdministratorsグループのメンバーでなければなりません。
        - *SQL Serverの場合*：指定するアカウントには、SQL Serverアプリケーションインスタンスに対するsysadminロールが必要です。SQL Server認証を使用して接続されるSQL Serverアカウントはサポートされていません。
        - *Exchange Serverの場合*：指定するアカウントは、組織管理ロールグループのメンバーでなければならず、既定の許可が有効になっていなければなりません。
     c. 「**保存**」をクリックします。

アプリケーション検出の新しいプロセスが、変更された資格情報で、それらの資格情報が割り当てられているすべての仮想マシンに対して開始されます。これが完了すると、アプリケーションのステータスは✅になり、"アプリケーションのバックアップ" ページ121の説明に従ってアプリケーションデータの保護を続行できます。

後で「**割り当て解除**」をクリックして、仮想マシンから資格情報の割り当てを解除できます。または「**削除**」をクリックして、必要なくなった仮想マシンの資格情報を削除します。

> ⚠ 重要 仮想マシンから資格情報を割り当て解除または削除できるのは、その上で実行する検出されたアプリケーションに、割り当てられたポリシーや使用可能な復元ポイントがない場合のみです。したがって、資格情報を割り当て解除または削除する前に、必ずポリシーを割り当て解除するか、または復元ポイントを期限切れとマークします。

アプリケーション保護の計画

アプリケーションのバックアップを実行する前に、前提条件、制限、考慮事項、推奨事項、およびアプリケーション固有のオプションについて十分に理解し、環境がアプリケーションデータ保護の準備ができ

ているかどうかを判断します。

前提条件

- *vSphere環境の場合*：最新バージョンのVMware Toolsが、保護するアプリケーションが実行されている仮想マシンにインストールされている。
- *NGTがインストールされているLinux仮想マシンの場合*：スクリプト`/usr/local/sbin/pre_freeze`および`/usr/local/sbin/post_thaw`は、システムで利用可能で、rootが所有し、`0700`に設定された許可を持つ。
- *HYCU Protégéの場合*："HYCU Protégéの詳細" ページ77にリストされている仮想マシンとアプリケーションをクラウドに移行するためのすべての前提条件が満たされていることを確認する。
- *物理マシンの場合*：
  - *Windowsの場合*：
    - VSSサービスが有効で実行中であり、VSSライターのステータスが安定している。
    - WinRMが有効であり、`winrm quickconfig`コマンドを使用して構成されている。
  - *Linuxの場合*：SSHを介した物理マシンへのアクセスが有効である。
- *QStarのテープターゲットにデータをアーカイブする場合*：HYCU Backup Controller上で同時アーカイブジョブに1 GiBの追加空きメモリが使用可能である。

アプリケーション固有の前提条件

アプリケーションタイプ	前提条件
SQL Server	• データベースがNutanix環境内のローカルディスク上に存在している。 • *SQL Serverアプリケーションのある仮想マシン上にNGTがインストールされている場合のみ*。アプリケーション整合性スナップショットの撮影が無効である。詳細については、Nutanixの資料を参照してください。 • *SQL Serverデータベースをポイントインタイムで復元する場合*：データベースがオンラインであり、バックアップ中に完全復旧モデルまたは一括ログ復旧モデルに設定されている。 • *Always On可用性グループの一部であるデータベースを復元する場合*：Always On可用性グループ内のすべてのノードがHYCUによって保護されている、またはAlways On可用性グループの同期されたデータベースを持つノードのみ(保護されている場合はオンラインである必要があります) 。後者の場合、ノードがオフラインになるか、データベースが同期しなくなると、データ損失のリスクが高まります。 • *SQL Server一時ファイルのバックアップストレージとして別のディスクボリュームを使用する場合*：十分なサイズの専用ディスクが割り当てられていることを確認します。ボリュームは、SQL Serverデータベースの2つのバックアップの間に生成される一時ファイルを保存できる必要があります。 • *SQL Serverフェールオーバークラスターの場合*：

アプリケーションタイプ	前提条件
	◦ SQL Serverフェールオーバークラスターがあるすべての仮想マシンがHYCUによって検出される。 ◦ ポリシーが、アプリケーションインスタンスが実行されているすべての仮想マシンに割り当てられている。
Active Directory	• NGTがクライアント仮想マシン上にインストールされて有効になっている。この実行方法の詳細については、Nutanixの資料を参照してください。 • クライアント仮想マシンにアタッチされているボリュームグループがない。
Exchange Server	• NGTがクライアント仮想マシン上にインストールされて有効になっている。この実行方法の詳細については、Nutanixの資料を参照してください。 • クライアント仮想マシンにアタッチされているボリュームグループがない。 • すべてのデータベースがマウントされている。 • Active Directoryアプリケーションが保護されている。 Exchange Serverはすべての構成情報をActive Directoryに保存するため、必要な場合に構成に関する情報を取得できるように、Active Directoryアプリケーションも必ずバックアップします。たとえば、データベース全体を誤って削除してしまい、復元したい場合は、最初にActive Directoryアプリケーションを復元する必要があります。それからExchange Serverの復元を実行すれば、そのデータベースを復元できます。ただし、データベースのコンテンツのみが削除された場合は、Exchange Serverアプリケーションのみを復元する必要があります。
Oracle	• SSHサービスがOracleサーバーで有効になっており、着信接続用のポート22でリッスンしている。 • Oracleデータベースユーザーには SYSDBA権限がある。 • データベースはARCHIVELOGモードで実行している。 • 表領域がオンラインである。 • 2つのデータベースバックアップ間で作成された一時ファイル用に追加ディスク領域が必ず用意されている。最適な復元パフォーマンスのために、一時ファイルとデータベースファイルそれぞれに個別のディスクが指定されている。
SAP HANA	• SAP HANAセーブポイントが有効になっている。 • *複数のボリュームグループの場合 :*すべてのデータボリュームとログボリュームが、同じボリュームグループに属している。 *分散(マルチホスト) 環境の場合 :* • SAP HANAが存在するすべての仮想マシンがHYCUによって検出される。 • ポリシーが、アプリケーションインスタンスが実行されているすべての仮想マシンに割り当てられている。

制限事項

- 仮想マシンで実行されている複数のアプリケーションタイプのバックアップはサポートされていません。
- 仮想マシンで実行されている同じアプリケーションタイプの複数のインスタンスのバックアップは、SQL ServerとOracleでのみサポートされます。
- ROBO環境の仮想マシンで実行されているアプリケーションのバックアップはサポートされていません。
- *Nutanix ESXiクラスターの場合*：「Backup from replica」ポリシーオプションを有効にした場合、別のコンテナにディスクがある仮想マシンのバックアップはサポートされません。

アプリケーション固有の制限事項

アプリケーションタイプ	制限事項
SQL Server	• `tempdb`SQL Serverシステムデータベースはすべてのバックアップから除外されます。 • `master`、`model`、および`msdb`SQL Serverシステムデータベースのフルバックアップのみサポートされます。SQL Serverシステムデータベースは、インスタンス全体としてのみ復元できます。 • `master`、`model`、`msdb`、または`tempdb`SQL Serverシステムデータベースのポイントインタイム復元はできません。 • すでに使用中の場合、シングルユーザーモードに設定されているデータベースはバックアップできません。 • *Always On基本可用性グループの場合*：セカンダリレプリカでのバックアップはできません。
Active Directory	• *Nutanixクラスターの場合*：IDEディスクがある仮想マシンで実行されているアプリケーションを保護することはできません。 • ボリュームグループで実行されているアプリケーション、またはアタッチされたボリュームグループがある仮想マシンで実行されているアプリケーションのバックアップは、サポートされていません。
Exchange Server	• *Nutanixクラスターの場合*：IDEディスクがある仮想マシンで実行されているアプリケーションを保護することはできません。 • ボリュームグループで実行されているアプリケーション、またはアタッチされたボリュームグループがある仮想マシンで実行されているアプリケーションのバックアップは、サポートされていません。
Oracle	• Oracle Real Application Clusters(RAC) データベースのバックアップはサポートされません。したがって、そのようなデータベースにポリシーを割り当てることはできません。

考慮事項

- *Nutanix ESXiクラスターの場合 :*完全バックアップスナップショットがNutanixクラスターにない場合 (たとえば、HYCU保護ドメインがPrismから削除されるため) 、次のバックアップは完全バックアップになります。
- *NearSyncで構成されている保護ドメインの場合 :*保護ドメインのスナップショットは1～15分間隔で作成されますが、HYCUはスナップショットからのバックアップと復元に、1時間ごとに作成されたスナップショットのみを使用します。これは以下の環境に適用されます。
  - Nutanix ESXiクラスター
  - 「Backup from replica」オプションを使用した場合のNutanixクラスター
- *SQL Serverの場合 :*
  - *SQL Serverを新しいバージョンにアップグレードした場合のみ*。HYCUはアップグレードされたアプリケーションを新しいアプリケーションとして認識し、同時に古いアプリケーションのステータスをPROTECTED_DELETEDに変更します。したがって、アップグレードされたアプリケーションのデータ保護を確保するには、以下を実行します。
    1. アップグレードされたアプリケーションに資格情報を割り当てて、HYCUがアプリケーションにアクセスできるようにします。詳細については、“アプリケーションデータへのアクセスの有効化” ページ113を参照してください。
    2. アップグレードしたアプリケーションにポリシーを割り当てて保護します。詳細については、“アプリケーションのバックアップ” ページ121を参照してください。
  - データベースのステータスがRECOVERINGの場合、AUTO CLOSEオプションをTRUEに設定してSQL Serverデータベースのトランザクションログをバックアップすると、失敗することがあります。

推奨事項

*SQL ServerおよびOracleの場合 :*バックアップ中に生成された一時ファイルを保存するのに十分なサイズの専用ディスクを使用することをお勧めします。そうしない場合、このデータは最大のディスクまたはオペレーティングシステムのディスクボリュームに保存され、復元パフォーマンスに影響する可能性があります。

アプリケーション固有のオプション

HYCUを使用すると、アプリケーションのバックアップを開始する前に、いくつかのアプリケーション固有のオプションを設定できます。そうすることにより、それらのオプションで指定された処理が、アプリケーションバックアップの一部として自動的に実行されるようにします。

「構成」ダイアログボックスへのアクセス

「構成」ダイアログボックスにアクセスするには、次の手順に従います。

1. ナビゲーションペインで、「**アプリケーション**」をクリックします。
2. 検出されたアプリケーションのリストから、アプリケーション固有のオプションを指定するものを選択し、「**構成**」をクリックします。

次のアプリケーション固有のオプションを選択できます。

SQL Server	• SQLトランザクションログのバックアップと切り捨て*(既定では有効)*

	HYCUアプリケーションバックアップの一部として、SQL Serverトランザクションログをバックアップし、SQL Serverデータベースで自動的に切り捨てる場合は、このスイッチを使用します。この場合、HYCUを使用してSQL Serverデータベースを回復することができます。 無効の場合、HYCUはSQL Serverトランザクションログのバックアップと切り捨ては実行しません。この場合、SQL Serverデータベースを復旧するには、データの復元後にトランザクションログを手動で適用する必要があります。 • Enter path for temporary translog and metadata files *(オプション)* 指定すると、SQL Server一時ファイル(トランザクションログとメタデータファイル)のバックアップコピーがこの場所に保存されます。そうでない場合、これらのバックアップコピーは、空き容量が最も大きいディスクのルート上の.hycuフォルダに保存されます。 > 注 復元のパフォーマンスを向上させるには、一時ファイルのバックアップコピーの保存用に専用ディスクを使用することをお勧めします。 • 最適化されたSQL Server HADR保護 *Always On可用性グループの一部であるSQL ServerデータベースをホストしているWindows仮想マシンで使用可能。バックアップ優先度が最高のセカンダリレプリカでのみバックアップを実行する場合に、このオプションを有効にします。プライマリレプリカのみ使用可能な場合は、バックアップはプライマリレプリカで実行されます。* > ⚠ 重要 最適化されたSQL Server HADR保護オプションを有効にする可能性がある場合は、以下を考慮してください。 > ◦ プライマリレプリカは、セカンダリレプリカやSQL Serverインスタンスのローカルデータベースとディスクを共有すべきではない。 > ◦ バックアップ優先度が最高のセカンダリレプリカは、バックアップ優先度が低いセカンダリレプリカやSQL Serverインスタンスのローカルデータベースとディスクを共有すべきではない。
Exchange Server	• Exchange Server復元要求の優先順位 Exchange Serverでメールボックス復元の復元要求が処理される優先順位を指定します。Lowest、Lower、Low、Normal(既定)、High、Higher、Highest、Emergencyを指定できます。 • 最適化されたExchange Server DAG保護 *データベース可用性グループ(DAG)の一部であるExchange ServerデータベースをホストしているホストしているWindows物理マシンで使用可能。アクティブ化の優先順位が最高のパッシブデータベースコピー(システムディスクを含む)をホストしているディスクのみバックアップする場合に、このオプションを有効にします。パッシブデータベースコピーが使用可能でない場合、アクティブデータベースコピーがバックアップされます。*

	⚠ 重要 個別のデータベースが個別のディスクに格納されている場合のみ、最適化されたExchange Server DAG保護が有効になります。
Oracle	• Oracleアーカイブログのバックアップと切り捨て*(既定では有効)* HYCUアプリケーションバックアップの一部として、Oracleアーカイブログをバックアップし、Oracleデータベースで自動的に切り捨てる場合は、このスイッチを使用します。この場合、HYCUを使用してOracleデータベースを回復することができます。 無効の場合、HYCUはOracleアーカイブログのバックアップと切り捨ては実行しません。この場合、Oracleデータベースを復旧するには、データの復元後にトランザクションログを手動で適用する必要があります。 • 一時的なOracleファイルへのパスを入力*(オプション)* 指定した場合、Oracle一時ファイルのバックアップコピーはこの場所に保存されます。 📋 注 復元のパフォーマンスを向上させるには、一時ファイルのバックアップコピーの保存用に専用ディスクを使用することをお勧めします。

アプリケーションのバックアップ

アプリケーション対応バックアップにより、検出されたアプリケーションの整合性バックアップが可能になります。

「アプリケーション」パネルへのアクセス

「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

考慮事項

Nutanixクラスターの場合 :仮想マシンの同期中に、仮想マシンがNutanixクラスターで見つからない場合、この仮想マシンまたはそこで実行されている検出済みアプリケーションのステータスはPENDING_REMOVALに設定されます。そのような仮想マシンとそのアプリケーションはHYCUではグレー表示され、それらに対してデータ保護を実行することはできません。2つの自動仮想マシン同期プロセスの時間間隔中に、仮想マシンがNutanixクラスターで見つかった場合、そのステータスはPROTECTED_DELETEDに変更されます。それ以外の場合、仮想マシンはHYCUから削除されます。

手順

1. 「アプリケーション」パネルで、バックアップするアプリケーションを選択します。

   💡 ヒント 表示されているすべてのアプリケーションのリストを絞り込むには、"データのフィルタリング" ページ177で説明されているフィルタリングオプションを使用できます。

2. 「**ポリシー**」をクリックします。「ポリシー」ダイアログボックスが表示されます。

3. 選択可能なポリシーのリストから、目的のポリシーを選択します。
4. 「**割り当て**」をクリックして、選択したアプリケーションにポリシーを割り当てます。

> 注 選択したアプリケーションにポリシーを割り当てると、それらが実行されている仮想マシンにも同じポリシーが割り当てられます。これらの仮想マシンにすでにポリシーが割り当てられている場合、アプリケーションに割り当てられたポリシーは仮想マシンに割り当てられたポリシーよりも優先され、仮想マシンに自動的に割り当てられます。

バックアップは、ポリシーに定義した値に従ってスケジュールされます。必要であれば、アプリケーションの手動バックアップもいつでも実行できます。詳細については、“手動バックアップの実行” ページ190を参照してください。

アプリケーション全体の復元

HYCUを使用すると、アプリケーションが実行されている仮想マシンおよびアタッチされたボリュームグループを復元することにより、アプリケーション全体を元の場所または新しい場所に復元できます。

> 注 *Active Directoryの場合*：HYCUはAuthoritative Restoreは実行しません。

前提条件

- *vSphere環境の場合*：割り当てられている必要な復元特権がある。詳細については、“vSphereユーザーへの特権の割り当て” ページ269を参照してください。
- *インポートされたターゲットにバックアップが保存される、ステータスがPROTECTED_DELETEDのアプリケーションの場合*：これらのアプリケーションを検出する。詳細については、“アプリケーションデータへのアクセスの有効化” ページ113を参照してください。
- *物理マシンの場合*：少なくとも1つのNutanixクラスターまたはvCenterサーバーがHYCUに追加され、復元データの保存のためのストレージコンテナが提供されている。Nutanixクラスターを HYCUに追加する方法の詳細については、“Nutanixクラスターの追加” ページ32を参照してください。 vCenterサーバーをHYCUに追加する方法の詳細については、“vCenter Serverの追加” ページ34を参照してください。

制限事項

テープからのデータの復元はサポートしていません。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため) がある層が含まれている場合、データを復元するためにこの層を使用することはできません。
- ポリシーに指定された保持期間が経過してしまっている(復元ポイントがHYCU Webユーザーインターフェースでグレー表示になっている) アプリケーションの復元は実行できません。ただし、必要な場合、これはHYCU `config.properties`ファイル内の `restore.enabled.if.retention.is.up`構成設定を`true`に設定することで上書きできま

す。HYCU構成設定のカスタマイズ方法の詳細については、“HYCU構成設定のカスタマイズ” ページ308を参照してください。

- *SQL Serverの場合*：「SQLトランザクションログのバックアップと切り捨て」オプションを無効にした場合、SQL Serverデータベースを復旧するためにデータを復元した後、トランザクションログを手動で適用する必要があります。
- *Oracleの場合*：「Oracleアーカイブログのバックアップと切り捨て」オプションを無効にした場合、Oracleデータベースを復旧するためにデータを復元した後、アーカイブログを手動で適用する必要があります。
- *SQL ServerフェールオーバークラスターおよびSAP HANAマルチホスト環境の場合*：アタッチされたボリュームグループの最新のバックアップがある仮想マシンを必ず選択します。適切な仮想マシンを識別するには、「ジョブ」パネルを使用できます。詳細については、“HYCUジョブの管理” ページ163を参照してください。

復元オプション

次の復元オプションから選択できます。

復元オプション	説明
VMの復元	アプリケーションが実行されている仮想マシンを復元することにより、アプリケーションを復元できます。アプリケーションが実行されている元の仮想マシンを、復元した仮想マシンで置き換える場合は、このオプションを選択します。説明については、“仮想マシンの復元” 下を参照してください。 ⚠ 重要 このオプションを使用して、物理マシンで実行されているSQL ServerまたはExchange Serverアプリケーションを復元することはできません。
VMのクローン	仮想マシンのクローンを作成することで、仮想マシンを復元できます。アプリケーションが実行されている元の仮想マシンを保持する場合は、このオプションを選択します。説明については、“仮想マシンの複製” ページ126を参照してください。

仮想マシンの復元

HYCUを使用すると、アプリケーションが実行されている仮想マシンを、元の場所または新しい場所に復元することにより、アプリケーションを復元できます。この場合、元の仮想マシンは上書きされます。

⛔ 注意 アプリケーションを元の場所に復元すると、復元されたデータが元の場所のデータを上書きします。データの損失を避けるには、保護されていない可能性のあるデータ(最後に成功したバックアップから復元の間までに生成されたデータ)を必ずバックアップします。手動バックアップを開始するには、“手動バックアップの実行” ページ190を参照してください。

制限事項

「VMの復元」オプションを使用して、物理マシン上で実行されているSQL Server、Exchange ServerおよびOracleアプリケーションを復元することはサポートされていません。

考慮事項

- *復元するボリュームグループが仮想マシンにアタッチされている場合のみ。*バックアップ時にアタッチされたのであれば、ボリュームグループを仮想マシンとともに復元することを選択できます。この場合、元のボリュームグループは削除され、復元されたボリュームグループは、バックアップ時にアタッチされた他のすべての仮想マシンと同じように、復元された仮想マシンに自動的にアタッチされます。
- 復元された仮想マシンは元のMACアドレスを保持します。
- *vSphere仮想マシンのデータを元のストレージコンテナに復元することを予定している場合のみ。*ストレージコンテナが複数のホストにマウントされており、復元時に元のホストが電源オフまたはメンテナンスモードになっている場合、データは異なるホストの同じストレージコンテナに復元されます。

> **「アプリケーション」パネルへのアクセス**
>
> 「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「アプリケーション」パネルで、復元するアプリケーションをクリックして、「詳細ビュー」を開きます。

   > 注「詳細ビュー」は、アプリケーションをクリックした場合にのみ表示されます。アプリケーションの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択し、「**復元**」をクリックします。

   > 重要 選択した復元ポイントのバックアップステータスが、バックアップがクラッシュ整合性であることを示す場合、アプリケーションの復元にこの復元ポイントは使用できません。

3. 「**サーバー全体を復元**」を選択して、「**次へ**」をクリックします。
4. 「**VMの復元**」を選択し、「**次へ**」をクリックします。
5. 「全般」セクションで、次の手順を実行します。
   a. 「ストレージコンテナ」ドロップダウンメニューから、仮想マシンを復元する場所を選択します。(既定では、元のストレージコンテナが選択されます。)

      > 注 仮想マシンを別のストレージコンテナに復元することを決定した場合、スナップショットからではなくターゲットから復元が実行されるため、高速復元は実行できません。

   b. 復元した仮想マシンを元の仮想マシンと同じ構成設定にする場合は、「**元のVM設定を使用**」スイッチを使用します。

      構成設定のいずれかを変更する場合は、「**元のVM設定を使用**」スイッチを無効にして、以下を実行します。

- 「vCPU(s)」フィールドに、復元した仮想マシンの仮想CPU数を入力します。仮想CPUの最大数は1024です。
- 「vCPUあたりのコア数」フィールドに、復元した仮想マシンの仮想CPUあたりのコア数を入力します。仮想CPUあたりの最大コア数は64です。

  > 注 復元した仮想マシンのコア数の合計は、仮想CPU数に仮想CPUあたりのコア数を掛けた数となります。

- 「メモリ」フィールドで、復元した仮想マシンのメモリ量(GiBまたはMiB単位)を設定します。指定する値は整数でなければならず、4096 GiBを超えることはできません。

c. 復元した仮想マシンを復元後にオンにする場合は、「**仮想マシンの電源をオンにします**」スイッチを使用します。元の仮想マシンは自動的に削除されます。

> ⚠ 重要 *vSphere仮想マシンをvSphere環境に復元し、「仮想マシンの電源をオンにします」スイッチを無効にしている場合のみ*。仮想マシンをオンにしようとしたときに、仮想マシンが移動したものかコピーしたものか答えるよう求められた場合は、必ず「**移動しました**」と答えてください。

d. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
- **自動** :最新の状態に最速で復元できます。
- **バックアップ**
- **コピー**
- **アーカイブ**
- **スナップショット**

e. *仮想ディスクが(手動または自動で)バックアップから除外されている場合のみ* :サイズと構成が同じ空のディスクを除外したディスクとして作成し、復元した仮想マシンにアタッチしたい場合は、「**除外ディスクを空ディスクとして作成**」スイッチを使用します。

f. *仮想マシンにアタッチされているボリュームグループの場合* :仮想マシンにアタッチされているボリュームグループも復元する場合は、「**ボリュームグループの復元**」スイッチを使用します。

6. 「ネットワーク」セクションで、バックアップ時に仮想マシンに追加されたネットワークアダプタのリストを確認します(仮想マシンが接続されていたネットワークを含む)。元のネットワークのいずれかが利用できなくなった場合は、「該当なし」が表示されます。

   元のネットワークが使用可能かどうかに応じて、以下のように続行します。

   - 元のネットワークが利用可能な場合は、既定値を変更せずに元のネットワーク設定で仮想マシンを復元するか、またはネットワーク設定を変更することができます。
   - 元のネットワークが利用できない場合は、ネットワーク設定を変更する必要があります。

ネットワーク設定の変更

元のネットワーク...	説明
使用可能	次の手順を実行できます。 • 「**＋ 新規**」をクリックして新しいネットワークアダプタを追加し、優

元のネットワーク...	説明
	先するネットワークを選択します。 • 仮想アダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、既存のネットワークアダプタを編集して、仮想マシンを別のネットワークに接続します。 • 必要なくなったネットワークアダプタの資格情報を選択し、「**削除**」をクリックして削除します。
使用不可	次の手順を実行できます。 • ネットワークアダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、影響を受けるネットワークアダプタを編集して、仮想マシンを新しいネットワークに接続します。 • 影響を受けるネットワークアダプタを選択して削除し、「**削除**」をクリックします。 • 「**新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。

> 注 仮想マシンはネットワークアダプタなしで復元できます。後で必ず仮想マシンのネットワーク設定を構成してください。

7. 「**復元**」をクリックします。

> 注 *Nutanix ESXiクラスターの場合* :仮想マシンの復元に必要な最小RAMは256 MiBであるので、それよりRAMが少ない仮想マシンは復元中に自動的に256 MiBに設定されます。

復元中には、元のアプリケーションインスタンスはオフラインであり、アクセスできません。

仮想マシンの復元後

Exchange ServerまたはActive Directoryアプリケーションの復元後は、NGTを再インストールして、確実にアプリケーションデータが正常にバックアップされるようにします。

仮想マシンの複製

元の仮想マシンのクローンは、仮想マシンを元の場所または新しい場所に復元することにより作成できます。この場合、元の仮想マシンは上書きされません。

前提条件

- *新しい場所にクローンを予定している仮想マシンの場合* :仮想マシンのクローンを予定しているvSphere環境のNutanixクラスターまたはvCenterサーバーが、HYCUに追加されている。この実行方法の詳細については、“Nutanixクラスターの追加” ページ32または“vCenter Serverの追加” ページ34を参照してください。

- *Linux物理マシンの場合*：物理マシンの/etc/fstabシステム構成ファイルでは、ファイルシステムのデバイス識別に、デバイス名の代わりにUUID(UUID=8ff089c0-8e71-4320-a8e9-dbab8f18a7e5など) を使用する必要があります。

考慮事項

- スナップショットが元の場所(元の仮想マシンが実行されていたソース) で利用可能な場合にのみ、スナップショットから復元が実行されます。スナップショットが元の場所で利用できない場合、復元のために選択した層に応じて、次のようになります。
  - スナップショットを選択した場合、復元は失敗します。
  - 「自動」を選択した場合、利用可能なターゲットがあれば、ターゲットから復元が実行されます。そうでない場合は、失敗します。
- *複製するボリュームグループが仮想マシンにアタッチされている場合のみ*。バックアップ時にアタッチされたのであれば、ボリュームグループを仮想マシンとともに復元することを選択できます。この場合、元のボリュームグループは復元されたボリュームグループとともに維持されます。ボリュームグループが他の仮想マシンにもアタッチされている場合、(仮想マシンへのアタッチ方法に応じて) 以下が適用されます。
  - 直接：ボリュームグループは、クローンされた仮想マシンのみに自動的にアタッチされます。
  - iSCSIを使用：ボリュームグループは、バックアップ時にアタッチされたすべての仮想マシンに自動的にアタッチされます。
- *Nutanix AHVクラスターで実行されている仮想マシンをNutanix ESXiクラスターに復元する場合*：仮想マシンのディスクがPCIバスにアタッチされている場合、復元後にバスタイプが自動的にSCSIに変更されます。この構成変更のため、復元は警告で終了します。
- *Nutanix ESXiクラスターで実行されているLinux仮想マシンの場合*：vSphere (Web) Clientを介して作成された仮想マシンを復元した後、仮想マシンが起動しない場合は、“vSphere環境から仮想マシンのNutanix ESXiクラスターへの復元” ページ318で説明されている手順に従ってください。
- 仮想マシンを復元した後、次の復元を実行すると、仮想ディスクの順序が元の仮想マシンの順序と異なるものとなる場合があります。
  - Nutanix AHVクラスターからNutanix ESXiクラスターまたはvSphere環境への
  - Nutanix ESXiから別のNutanix ESXiクラスターへの
  - vSphere環境からNutanix ESXiクラスターへの

  この場合は、正しいブートディスクの選択を含め、必要な調整を行います。
- *vSphere仮想マシンのデータを元のストレージコンテナに復元することを予定している場合のみ*。ストレージコンテナが複数のホストにマウントされており、復元時に元のホストが電源オフまたはメンテナンスモードになっている場合、データは異なるホストの同じストレージコンテナに復元されます。
- *仮想マシンに所有権が設定されている場合のみ*。同じ所有者は、復元された仮想マシンに自動的に割り当てられます。

推奨事項

Linux仮想マシンの場合 :MACアドレスを基にした永続的なネットワークデバイス名の使用は無効にすることをお勧めします。そうしないと、ネットワークの手動での構成が必要になります。永続的なネットワークデバイス名の使用を無効にする方法については、お使いのLinux配信ドキュメントを参照してください。

> 「アプリケーション」パネルへのアクセス
>
> 「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「アプリケーション」パネルで、復元するアプリケーションをクリックして、「詳細ビュー」を開きます。

   > 注 「詳細ビュー」は、アプリケーションをクリックした場合にのみ表示されます。アプリケーションの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択し、「**復元**」をクリックします。

   > ⚠ 重要 選択した復元ポイントのバックアップステータスが、バックアップがクラッシュ整合性であることを示す場合、アプリケーションの復元にこの復元ポイントは使用できません。

3. 「**サーバー全体を復元**」を選択して、「**次へ**」をクリックします。
4. 「**VMのクローン**」を選択し、「**次へ**」をクリックします。
5. 「全般」セクションで、次の手順を実行します。
   a. 「ストレージコンテナ」ドロップダウンメニューから、仮想マシンを復元する場所を選択します。

      > 注 *仮想マシンの場合* :既定では、元のストレージコンテナが選択されます。仮想マシンを別のストレージコンテナに復元する場合、次の点にご注意ください。
      >
      > - スナップショットからではなくターゲットから復元が実行されるため、高速復元は実行できません。
      > - 選択したストレージコンテナが別のハイパーバイザーにある場合、追加の前提条件が適用されます。詳細については、"異なるハイパーバイザーを持つ環境への復元" ページ314を参照してください。

   b. 「新しいVM名」フィールドで、仮想マシンの新しい名前を指定します。
   c. 復元した仮想マシンを元の仮想マシンと同じ構成設定にする場合は、「**元のVM設定を使用**」スイッチを使用します。

      構成設定のいずれかを変更する場合は、「**元のVM設定を使用**」スイッチを無効にして、以下を実行します。

      - 「vCPU(s)」フィールドに、復元した仮想マシンの仮想CPU数を入力します。仮想CPUの最大数は1024です。
      - 「vCPUあたりのコア数」フィールドに、復元した仮想マシンの仮想CPUあたりのコア数を入力します。仮想CPUあたりの最大コア数は64です。

> 注 復元した仮想マシンのコア数の合計は、仮想CPU数に仮想CPUあたりのコア数を掛けた数となります。

- 「メモリ」フィールドで、復元した仮想マシンのメモリ量(GiBまたはMiB単位)を設定します。指定する値は整数でなければならず、4096 GiBを超えることはできません。

d. 復元した仮想マシンを復元後にオンにする場合は、「**仮想マシンの電源をオンにします**」スイッチを使用します。復元した仮想マシンをオンにすると、元の仮想マシンは自動的にオフになります。

> ⚠ 重要 以下にご注意ください。
>
> - このオプションは、iSCSIを使用してアタッチされたボリュームグループがある仮想マシンには無効です。復元された仮想マシンをオンにする前に実行する必要がある事柄については、"仮想マシンの複製後" ページ95を参照してください。
> - *vSphere仮想マシンをvSphere環境に複製し、「仮想マシンの電源をオンにします」スイッチを無効にしている場合のみ。*仮想マシンをオンにしようとしたときに、仮想マシンが移動したものかコピーしたものか答えるよう求められた場合は、必ず「**コピーしました**」と答えてください。

e. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
- **自動** :最新の状態に最速で復元できます。
- **バックアップ**
- **コピー**
- **アーカイブ**
- **スナップショット**

f. *仮想ディスクが(手動または自動で)バックアップから除外されている場合のみ* :サイズと構成が同じ空のディスクを除外したディスクとして作成し、復元した仮想マシンにアタッチしたい場合は、「**除外ディスクを空ディスクとして作成**」スイッチを使用します。

g. *仮想マシンにアタッチされているボリュームグループの場合* :仮想マシンにアタッチされているボリュームグループも復元する場合は、「**ボリュームグループのクローン**」スイッチを使用します。

6. 「ネットワーク」セクションで、次の手順を実行します。

a. バックアップ時に仮想マシンに追加されたネットワークアダプタのリストを確認します(仮想マシンが接続されていたネットワークを含む)。元のネットワークのいずれかが利用できなくなった場合は、「該当なし」が表示されます。

元のネットワークが使用可能かどうかに応じて、以下のように続行します。

- 元のネットワークが利用可能な場合は、既定値を変更せずに元のネットワーク設定で仮想マシンをクローンするか、またはネットワーク設定を変更することができます。
- 元のネットワークが利用できない場合は、ネットワーク設定を変更する必要があります。

ネットワーク設定の変更

元のネットワーク...	説明
使用可能	次の手順を実行できます。 • 「**＋ 新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。 • 仮想アダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、既存のネットワークアダプタを編集して、仮想マシンを別のネットワークに接続します。 • 必要なくなったネットワークアダプタの資格情報を選択し、「**削除**」をクリックして削除します。
使用不可	次の手順を実行できます。 • ネットワークアダプタを選択し、「**編集**」をクリックして優先するネットワークを選択することで、影響を受けるネットワークアダプタを編集して、仮想マシンを新しいネットワークに接続します。 • 影響を受けるネットワークアダプタを選択して削除し、「**削除**」をクリックします。 • 「**＋ 新規**」をクリックして新しいネットワークアダプタを追加し、優先するネットワークを選択します。

> 注 仮想マシンはネットワークアダプタなしでクローンできます。後で必ず仮想マシンのネットワーク設定を構成してください。

b. *仮想マシンを別のNutanixクラスターまたはvSphere環境に復元する場合のみ*。復元した仮想マシンで元のMACアドレスを維持する場合は、「**元のMACアドレスを維持**」スイッチを使用します。これは、少なくとも1つのネットワークアダプタにMACアドレスが割り当てられている場合にのみ適用されることにご注意ください。

7. 「**復元**」をクリックします。

復元中には、元のアプリケーションインスタンスはオフラインであり、アクセスできません。

仮想マシンの複製後に注意すべき考慮事項がいくつかあります。詳細については、"仮想マシンの複製後" ページ95を参照してください。

SQL Serverデータベースの復元

HYCUを使用すると、SQL Serverデータベースを元のまたは別のSQL Serverインスタンスに復元できます。

前提条件

- *ポイントインタイム復元の場合*：データベース復旧モデルが完全または一括ログに設定されている。

- *SQL Serverフェールオーバークラスターインスタンス全体を復元する場合*：SQL Serverサービスは、フェールオーバークラスターマネージャーを使用して停止されている。この実行方法の詳細については、SQL Serverの資料を参照してください。
- 復元のパフォーマンスの向上のために、Microsoft iSCSIイニシエーターサービスの始動タイプが「Disabled」に設定されていない。
- *物理マシンの場合*：少なくとも1つのNutanixクラスターまたはvCenterサーバーがHYCUに追加され、復元データの保存のためのストレージコンテナが提供されている。NutanixクラスターをHYCUに追加する方法の詳細については、“Nutanixクラスターの追加” ページ32を参照してください。vCenterサーバーをHYCUに追加する方法の詳細については、“vCenter Serverの追加” ページ34を参照してください。

制限事項

- 検出されたアプリケーションの復元は、NTFS、FAT、およびFAT32ファイルシステムで利用できます。
- 別のSQL Serverアプリケーションインスタンスへの SQL Serverデータベースの復元は、同じバージョン以降のアプリケーションに復元する場合にのみサポートされます。
- Always On可用性グループの一部であるデータベースは(セカンダリノードまたはプライマリノードから) プライマリノードにのみ復元できます。ただし、Always On基本可用性グループの場合は、データベースを復元できるのはプライマリノードからのみであることに注意してください。
- テープからのデータの復元はサポートしていません。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため) がある層が含まれている場合、データを復元するためにこの層を使用することはできません。
- データベースを別のSQL Serverインスタンスに復元する場合、データベースの名前は変更され、選択したターゲットの既定のSQL Serverの場所にコピーされます。
- 仮想マシンがソースから削除されたものの、利用できる有効な復元ポイントが少なくとも1つは残っている場合、その仮想マシンは保護されていると見なされます。その場合、仮想マシンまたはそこで実行されている検出されたアプリケーションのステータスは、PROTECTED_DELETEDです。このようなアプリケーションのアプリケーション項目を復元する場合、元のアプリケーションインスタンスに復元できないことに注意してください。
- ポリシーに指定された保持期間が経過してしまっている(復元ポイントがHYCU Webユーザーインターフェースでグレー表示になっている) アプリケーションの復元は実行できません。ただし、必要な場合、これはHYCU `config.properties`ファイル内の `restore.enabled.if.retention.is.up`構成設定を`true`に設定することで上書きできます。HYCU構成設定のカスタマイズ方法の詳細については、“HYCU構成設定のカスタマイズ” ページ308を参照してください。
- *SQL Serverフェールオーバークラスターの場合*：

    - 復元はアクティブなSQL Serverフェールオーバークラスターインスタンスにリダイレクトする必要があります。
    - 「既存のデータベースを上書きする」オプションは、データベースの場所がターゲット仮想マシンにも存在する場合にのみ、リダイレクトされた復元に対して有効にできます。
- *SQL Serverデータベースを別のSQL Serverインスタンスに復元する場合*：別のサーバーにありながら同じデータベースパスを持つSQL Serverインスタンスにデータベースを復元する場合のみ、「既存のデータベースを上書きする」オプションを有効にする必要があります。

> 「アプリケーション」パネルへのアクセス
>
> 「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「アプリケーション」パネルで、データベースを復元するアプリケーションをクリックして、「詳細ビュー」を開きます。「詳細ビュー」は、アプリケーションをクリックした場合にのみ表示されます。アプリケーションの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

   > 注 SQL Server Always On可用性グループを使用すると、アプリケーション項目を展開して、検出された可用性グループを表示できます。

2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   > ⚠ 重要 選択した復元ポイントのバックアップステータスが、バックアップがクラッシュ整合性であることを示す場合、データベースの復元にこの復元ポイントは使用できません。

3. 「**復元**」をクリックします。「MS SQL Serverの復元」ダイアログボックスが開きます。

   > 注 バックアップ中に「SQLトランザクションログのバックアップと切り捨て」オプションが無効であった場合、復元後にデータベースの復旧を実行する必要があることを示すプロンプトが表示されます。

4. 「**データベースを復元**」を選択し、「**次へ**」をクリックします。
5. 「ターゲットインスタンス」ドロップダウンメニューから、データベースを復元する場所を選択します。
6. *SQL Server Always On可用性グループの場合*：「宛先可用性グループ」ドロップダウンメニューから、利用可能な可用性グループの1つを選択してデータベースをこのグループに復元するか、フィールドを空のままにしてデータベースをSQL Serverに復元します。
7. 「宛先ストレージコンテナ」ドロップダウンメニューから、データベースを復元する場所を選択します。
8. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動**：最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**

9. アプリケーションインスタンス全体を復元する場合は、「**インスタンス全体**」チェックボックスを選択します。または、復元に使用できるデータベースのリストから、復元するデータベースを選択します。
10. *オプション*:データを復元するポイントインタイムを指定します。データベースは、指定された時刻の状態に復元されます。

    > 注 ポイントインタイム復元を実行するには、指定されたポイントインタイムの前に実行されたバックアップを選択し、その次のバックアップからのトランザクションログファイルを適用して、データベースインスタンスを適切な状態に戻せるようにします。

11. 「**次へ**」をクリックします。
12. 復元を実行するときに既存のデータベースを上書きする場合は、「**既存のデータベースを上書きする**」スイッチを使用します。この場合、バックアップは元の場所に復元され、すべてのデータが上書きされます。データベースを別のSQL Serverインスタンスに復元する場合、同じ名前(必ずしもコンテンツは同じでない)を持つすべてのデータベースが上書きされることに注意してください。

    それ以外の場合、同じまたは別のSQL Serverインスタンスの別の場所にデータを復元するには、データベースに付与されるデータベース接頭語、新しいデータベースファイルの場所、および新しいデータベースログの場所を指定します。

    > ⚠ 重要 インスタンス全体を復元する場合は、既存のデータベースのみを上書きできます。この場合、「既存のデータベースを上書きする」オプションは既定で有効になっており、無効にすることはできません。

13. 「**復元**」をクリックします。
14. *バックアップ中に「SQLトランザクションログのバックアップと切り捨て」オプションが無効であった場合のみです*。トランザクションログを手動で適用して、SQL Serverデータベースを復旧します。
15. *SQL Server 2012および2014 Always On可用性グループを使用している場合のみ*。SQL Server Management Studioを使用して、復元されたデータベースをAlways On可用性グループに参加させます。この実行方法の詳細については、Microsoftの資料を参照してください。

    > 注 復元されたデータベースをAlways On可用性グループに参加させたら、Always On可用性グループのバックアップを新たに実行することをお勧めします。

16. *SQL Serverフェールオーバークラスターインスタンス全体を復元する場合のみ*。フェールオーバークラスターマネージャーを使用して、SQL Serverサービスと他のすべての関連サービスを開始します。この実行方法の詳細については、SQL Serverの資料を参照してください。

Exchange Serverデータベース、メールボックス、およびパブリックフォルダの復元

HYCUを使用すると、Exchange Serverデータベース、メールボックス、およびパブリックフォルダを復元できます。Exchange Serverデータベースを復元する場合、元のメールボックスサーバーに復元するか、またはメールボックスサーバーがデータベース可用性グループ(DAG)のメンバーである場合はDAG内の別のメールボックスサーバーに復元するかを選択できます。メールボックスとパブリックフォルダを復元する場合、回復用データベースは、元のメールボックスサーバーまたはExchangeServer組織の一

部である他のメールボックスサーバーに復元できます。そこから、組織内の任意のメールボックスまたはパブリックフォルダに対して実際の復元が実行されます。

前提条件

- *パブリックフォルダを復元する場合：*パブリックフォルダが、パブリックフォルダメールボックスに存在している。存在しない場合は、バックアップ時と同じ名前を付けて、手動で再作成します。
- 復元のパフォーマンスの向上のために、Microsoft iSCSIイニシエーターサービスの始動タイプが「Disabled」に設定されていない。
- *物理マシンの場合：*少なくとも1つのNutanixクラスターまたはvCenterサーバーがHYCUに追加され、復元データの保存のためのストレージコンテナが提供されている。NutanixクラスターをHYCUに追加する方法の詳細については、"Nutanixクラスターの追加" ページ32を参照してください。vCenterサーバーをHYCUに追加する方法の詳細については、"vCenter Serverの追加" ページ34を参照してください。

制限事項

- 検出されたアプリケーションの復元は、NTFS、FAT、およびFAT32ファイルシステムで利用できます。
- hycuサブフォルダへのデータの復元(「サブフォルダに復元」オプション)は、現在、パブリックフォルダにはサポートされていません。
- テープからのデータの復元はサポートしていません。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため)がある層が含まれている場合、データを復元するためにこの層を使用することはできません。
- ポリシーに指定された保持期間が経過してしまっている(復元ポイントがHYCU Webユーザーインターフェースでグレー表示になっている)アプリケーションの復元は実行できません。ただし、必要な場合、これはHYCU `config.properties`ファイル内の`restore.enabled.if.retention.is.up`構成設定を`true`に設定することで上書きできます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

> **「アプリケーション」パネルへのアクセス**
>
> 「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「アプリケーション」パネルで、復元対象のアプリケーションをクリックして、「詳細ビュー」を開きます。

   > 注「詳細ビュー」は、アプリケーションをクリックした場合にのみ表示されます。アプリケーションの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   > ⚠ 重要 選択した復元ポイントのバックアップステータスが、バックアップがクラッシュ整合性であることを示している場合、アプリケーション項目の復元にはこの復元ポイントは使用できません。

3. 「**復元**」をクリックします。「MS Exchange Serverの復元」ダイアログボックスが表示されます。
4. 復元するアプリケーションアイテムを選択します。
   - **データベースの復元**
     a. 「宛先サーバー」ドロップダウンメニューから、データを復元するサーバーを選択します。宛先サーバーを指定する場合、それを選択できるのは、メールボックスサーバーがDAGのメンバーであり、DAG内の別のメールボックスサーバーにデータを復元する場合のみであることに注意してください。それ以外の場合は、元のメールボックスサーバーにのみ復元できます。

        > ⚠ 重要 *DAGのメンバーであるメールボックスサーバーを復元する場合*、必ずデータベースが現在アクティブになっている宛先サーバーを選択します。

     b. 「宛先ストレージコンテナ」ドロップダウンメニューから、データを復元するストレージコンテナを選択します。
     c. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
        - **自動**：最新の状態に最速で復元できます。
        - **バックアップ**
        - **コピー**
        - **アーカイブ**
        - **スナップショット**

     d. すべてのデータベースを復元する場合は、「**すべてのデータベース**」チェックボックスを選択します。または、復元に使用できるデータベースのリストから、復元するデータベースを選択します。
     e. 回復用データベースへのデータの復元を有効にする場合は、「**回復用データベースへの復元を有効にする**」スイッチを使用します。有効にした場合、回復用データベースのパスを指定します。既定は`C:\ProgramData\Hycu`です。
   - **メールボックスまたはパブリックフォルダの復元**
     a. 「回復用データベースサーバー」ドロップダウンメニューから、データを復元するメールボックスサーバーを選択します。Exchange Server組織に属するメールボックスサーバーの中から選択できます。
     b. 「ストレージコンテナ」ドロップダウンメニューから、データを復元するストレージコンテナを選択します。
     c. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
        - **自動**：最新の状態に最速で復元できます。
        - **バックアップ**

- **コピー**
- **アーカイブ**
- **スナップショット**

d. 復元に選択できるメールボックスまたはパブリックフォルダのリストから、復元するものを選択します。

> ヒント メールボックスまたはパブリックフォルダが多すぎて表示が1ページに収まらない場合、「 > 」と「 < 」をクリックしてページを移動できます。「 ⌄ 」を使用して、ページごとに表示されるメールボックスとパブリックフォルダの数を設定することもできます。
>
> メールボックスとパブリックフォルダを検索するには、「検索」フィールドに名前を入力し、**Enter**を押します。

e. 既定以外のドメインコントローラーを使用する場合は、「**既定以外のドメインコントローラーを使用する**」スイッチを有効にし、「ドメインコントローラー」フィールドに、優先するドメインコントローラーのFQDNまたはIPアドレスを入力します。

f. 「**次へ**」をクリックします。

g. データを復元する場所を選択します。

- **元のメールボックス**
- **代替メールボックス**。この場合は代替メールボックスの名前を入力します。

h. データを復元するモードを選択します。

- **元の場所に復元**

  データを元の場所に復元できます。

- **サブフォルダに復元** *(パブリックフォルダにはサポートされていません)*

  自動的に作成されるhycuサブフォルダにデータを復元できます。

i. *元の場所にデータを復元する場合* .競合する項目の最新バージョンを維持することで、潜在的なデータ競合を解決する場合は、「**競合回避**」スイッチを使用します。そうでない場合、HYCUは、既存のアイテムをバックアップのアイテムで上書きします。

j. 一時回復用データベースのパスを入力します。既定は`C:\ProgramData\Hycu`です。

5. 「**復元**」をクリックします。

Oracleデータベースのインスタンスと表領域の復元

HYCUを使用して、Oracleデータベースインスタンス全体または選択した表領域を元の場所に復元できます。

前提条件

- 元の仮想マシンで、`/etc/fstab`システム構成ファイルエントリの参照は、論理ボリューム(`/dev/mapper/ol-root`など)を参照しない限り、デバイス名(`/dev/sda1`など)ではなく、UUID(`UUID=8ff089c0-8e71-4320-a8e9-dbab8f18a7e5`など)を使用している。

- bashrcおよび.bash_profileスクリプトは、アプリケーションの検出に資格情報が使用されるユーザーの標準出力(STDOUT) または標準エラー(STDERR) に書き込まない。
- *物理マシンの場合* :少なくとも1つのNutanixクラスターまたはvCenterサーバーがHYCUに追加され、復元データの保存のためのストレージコンテナが提供されている。NutanixクラスターをHYCUに追加する方法の詳細については、“Nutanixクラスターの追加” ページ32を参照してください。 vCenterサーバーをHYCUに追加する方法の詳細については、“vCenter Serverの追加” ページ34を参照してください。

制限事項

- 表領域は、バックアップチェーンの最新の復元ポイントからのみ復元でき、ポイントインタイムに復元することはできません。
- テープからのデータの復元はサポートしていません。

考慮事項

- データベースインスタンスまたは表領域の復元を実行する場合、完全な復元またはポイントインタイム復元を実行できます。
  - 完全な復元

    HYCUは、バックアップチェーンの最新のバックアップから、データベースインスタンス全体または表領域の完全な復元を実行します。

    完全な復元を実行すると、制御ファイルとアーカイブログファイルは復元されず、既存のアーカイブログファイルのみが適用されます。制御ファイルまたは既存のアーカイブログファイルが失われた場合、完全な復元は不可能であり、ポイントインタイム復元を実行する必要があります。
  - ポイントインタイム復元

    ポイントインタイム復元を実行するには、指定されたポイントインタイムの前に実行されたバックアップを選択し、その次のバックアップからのアーカイブログファイルを適用して、データベースインスタンスをポイントインタイムに戻せるようにする必要があります。

    ポイントインタイム復元を実行すると、制御ファイル、データベースファイル、および必要なアーカイブログファイルが復元されます。

    > ⚠ 重要 ポイントインタイム復元が正常に完了すると、アーカイブログファイルはリセットされます。したがって、新しいバックアップが実行されるまで完全な復元という観点ではデータベースは保護されないため、ポイントインタイム復元を実行した直後にバックアップを実行することを強くお勧めします。
- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため) がある層が含まれている場合、データを復元するためにこの層を使用することはできません。
- ポリシーに指定された保持期間が経過してしまっている(復元ポイントがHYCU Webユーザーインターフェースでグレー表示になっている) アプリケーションの復元は実行できません。ただし、必要な場合、これはHYCU config.propertiesファイル内の restore.enabled.if.retention.is.up構成設定をtrueに設定することで上書きできま

す。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

「アプリケーション」パネルへのアクセス

「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「アプリケーション」パネルで、データベースを復元するアプリケーションをクリックして、「詳細ビュー」を開きます。

   注 「詳細ビュー」は、アプリケーションをクリックした場合にのみ表示されます。アプリケーションの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   重要 選択した復元ポイントのバックアップステータスが、バックアップがクラッシュ整合性であることを示す場合、データベースインスタンスの復元にこの復元ポイントは使用できません。

3. 「**復元**」をクリックします。「Oracleサーバーの復元」ダイアログボックスが開きます。

   注 バックアップ中に「Oracleアーカイブログのバックアップと切り捨て」オプションが無効であった場合、復元後にデータベースの復旧を実行する必要があることを示すプロンプトが表示されます。

4. 「**データベースを復元**」を選択し、「**次へ**」をクリックします。
5. 「ストレージコンテナ」ドロップダウンメニューから、データを復元するストレージコンテナを選択します。
6. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**
7. データベースインスタンス全体を復元する場合は、「**インスタンス全体**」チェックボックスを選択します。または、復元に使用できる表領域のリストから、復元する表領域を選択します。
8. *データベースインスタンス全体を復元する場合のみ。*データを復元するポイントインタイムを指定します(オプション)。データベースインスタンスは、指定された時刻の状態に復元されます。
9. 「**復元**」をクリックします。
10. *バックアップ中に「Oracleアーカイブログのバックアップと切り捨て」オプションが無効であった場合のみ。*アーカイブログを手動で適用して、Oracleデータベースを復旧します。

第6章

ファイル共有の保護

HYCUにより、高速で信頼性の高いバックアップと復元操作でファイル共有データを保護できます。ファイル共有をバックアップしたら、ファイル共有全体を復元するか、個別ファイルを復元するかを選択できます。

ファイル共有データを効率的に保護する方法の詳細については、以下のセクションを参照してください。

- "ファイル共有のバックアップ" 下
- "ファイル共有データの復元" ページ141

ファイル共有のバックアップ

ファイル共有バックアップを使用すると、並列バックアップストリームを使用してファイル共有を迅速にバックアップできます。

前提条件

- *QStarのテープターゲットにデータをアーカイブする場合*：HYCU Backup Controller上で同時アーカイブジョブに1 GiBの追加空きメモリが使用可能である。
- *PowerScale OneFS SMB共有の場合*：バックアップオペレーターは、保護する予定のすべての共有に対する完全な許可を持っている必要があります。

制限事項

- iSCSIおよびNutanixターゲットは、ファイル共有データを保護するためには使用できません。
- Nutanix Filesのレプリカからのバックアップはサポートされていません。したがって、ファイル共有に割り当てる予定のポリシーで「Backup from replica」オプションが有効になっている場合、このオプションは無視されます。
- ファイルシステム項目名にUnicode Basic Multilingual Plane(BMP) の文字のみが含まれる場合、クラウドターゲットへのファイル共有のバックアップがサポートされます。
- *NFSファイル共有の場合*：ファイル名にUTF-8ではない多言語の文字を含むファイルのバックアップ(Windowsクライアントにより作成されたファイルなど) はサポートされていません。そのため、そのようなファイルはバックアップの際スキップされます。
- *Nutanix Filesバージョン3.8.1以降の場合*：Nutanix Files保護にスマート災害復旧(DR) を使用する場合、HYCUによって、レプリケーションされたファイル共有データを保護できます。復旧ファイルサーバーをソースとしてHYCUに追加すると、対応するファイル共有をポリシーを割り当てることで

バックアップし、後で復元することもできます。レプリケーションされたファイル共有にはデータを復元できないことに注意してください。Smart DRの構成方法の詳細については、Nutanixの資料を参照してください。

考慮事項

- 増分ファイル共有バックアップの数は変更できます。その後には、`afs.reindex.interval.count`構成設定をカスタマイズすることによる完全インデックス再作成が実行されます。これにより復元時に関連ファイルを検索するプロセスを高速化できます。この実行方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。
- ファイル共有のバックアップ中に最大100個のファイルバックアップが失敗した場合、ファイル共有のバックアップステータスは「エラーで完了」です。`afs.partial.success.threshold.count`構成設定を編集すると、この値をカスタマイズできます。この実行方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。
- ファイル共有をバックアップするときに、HYCUは選択したファイル共有内にあるネストされた共有もバックアップします。ネストされた共有の個別のバックアップはサポートされないことに注意してください。
- *Nutanix Files 3.8.0の場合* .接続された共有のバックアップはサポートされます。親共有のバックアップには子共有のコンテンツが含まれないため、接続された共有は個別にバックアップする必要があることに注意してください。
- *Nutanix Filesバージョン4.0.0以降の場合* .階層化されたファイルでの共有のバックアップはサポートされます。ただし、以下について考慮してください。
  - バックアップオペレーターまたはHYCU インスタンス IPアドレスをゼロユーザーまたはクライアントとしてセットアップしてはなりません。これは、階層型ファイルのバックアップデータの破損を引き起こす可能性があるからです。
  - バックアップと復元の操作には、データ消去による追加料金が発生する場合があります。

推奨事項

ファイル共有データの保存にNFSターゲットを使用するには、ターゲットへのパブリックアクセスを有効にする必要があります。セキュリティ上の目的で、このような構成は避けることをお勧めします。

> 「共有フォルダ」パネルへのアクセス
>
> 「共有フォルダ」パネルにアクセスするには、ナビゲーションペインで、「**共有フォルダ**」をクリックします。

手順

1. 「共有フォルダ」パネルで、バックアップするファイル共有を選択します。

   > **ヒント**「**同期**」をクリックして、ファイル共有のリストを更新できます。表示されているファイル共有のリストを絞り込むには、"データのフィルタリング" ページ177で説明されているフィルタリングオプションを使用できます。

2. *特定のファイル共有フォルダをバックアップから除外する場合のみ*。「**構成**」をクリックし、開かれた「構成」ダイアログボックスで、以下を実行します。

a. 「フォルダパスを除外」フィールドに、バックアップから除外するファイル共有フォルダへのフルパス(ファイル共有のルートからのパス、たとえば/backup)を入力し、「**＋ 追加**」をクリックします。ファイル共有フォルダを追加するには、この手順を繰り返します。

> 注 バックアップから除外したすべてのファイル共有フォルダへのパスが、「フォルダパスを除外」リストに追加されます。除外リストからそれらのいずれかを削除する場合は、「**ー 削除**」をクリックします。

b. 「**保存**」をクリックします。

3. 「**ポリシー**」をクリックします。「ポリシー」ダイアログボックスが表示されます。
4. 選択可能なポリシーのリストから、目的のポリシーを選択します。
5. 「**割り当て**」をクリックして、ポリシーを選択したファイル共有に割り当てます。

ポリシーを割り当てると、バックアップは、ポリシーに従ってスケジュールされます。必要であれば、手動バックアップもいつでも実行できます。詳細については、"手動バックアップの実行" ページ190を参照してください。

> ヒント データ保護環境内に複数のHYCUインスタンスがある場合、「ジョブ」パネルで目的のバックアップジョブをクリックし、「詳細ビュー」でHYCUインスタンスのIPアドレスを確認することにより、どのHYCUインスタンスがバックアップを実行したかを確認できます。

ファイル共有データの復元

ファイル共有全体か個別のファイルを元のまたは別のファイルサーバー共有、外部のSMBまたはNFS共有、あるいはローカルマシンに復元できます。

ファイル共有データは、ターゲットまたはスナップショットから復元できます。スナップショットからのデータの復元は、`afs.restore.snapshot.enabled`構成設定が`true`(既定値は`false`)に設定されている場合のみ可能です。この場合、スナップショットが使用可能であれば、復元は常にスナップショットから実行されます。そうでない場合、復元はターゲットから実行されます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

前提条件

- *別のファイルサーバー共有にデータを復元する場合*:データの復元先にするファイル共有のあるファイルサーバーがHYCUに追加されている。この実行方法の詳細については、"ファイルサーバーの追加" ページ35を参照してください。
- *テープからデータを復元する場合*:テープターゲットがデータのアーカイブに積極的に使用されている場合、モードは「読み取り専用」に設定する。ターゲットを編集する方法の詳細については、「"ターゲットの管理" ページ185」を参照してください。

制限事項

- 代替データストリーム(ADS)の復元は、データを1つのファイルサーバーSMB共有から別のファイルサーバーSMB共有にデータを復元する場合のみサポートされます。
- *トップレベルのディレクトリに代替データストリーム(ADS)を含むNutanix Files共有を、分散ファイル共有に復元する場合のみ*。分散ファイル共有のトップレベルディレクトリへのADSの復元はサポー

トされていません。ADSは、分散ファイル共有のサブディレクトリ、または標準ファイル共有に復元できます。

- シンボリックリンクが復元されます。
  - *Nutanix Filesバージョン3.8.1よりも前の場合*：NFS共有から別のNFS共有へデータを復元する場合のみ。
  - *Nutanix Filesバージョン3.8.1以降の場合*：NFS共有から別のNFS共有に、またはSMB共有からNFS共有にデータを復元する場合のみ。
- *ファイルを外部共有に復元する場合のみ*。名前に改行を含むファイルまたはフォルダの復元は、NFS共有がUnixでセットアップされている場合のみサポートされます。
- *ファイルをローカルマシンに復元する場合のみ*：
  - ファイルは、圧縮前のファイルサイズが2 GiB以下の場合のみ復元できます。
  - ファイルの元のアクセス制御リストの復元はサポートされません。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため) がある層が含まれている場合、データを復元するためにこの層を使用することはできません。
- *ファイル共有バックアップから多数のファイルを復元する場合のみ*。HYCUインスタンスは、既定で利用可能なよりも多くのRAMを必要とする場合があります。この場合、`afs.instance.memory.mb`構成設定を使用して既定値を増やします。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。
- *ファイルをローカルマシンに復元する場合のみ*。復元されたファイルは.zipファイルでダウンロードされます。復元されたファイルの解凍について考えられる問題を回避するため、また名前に改行を含むファイルやフォルダを正しく復元できるよう、ファイルの抽出には必ず7-Zipを使用してください。
- ファイル共有復元処理中に、復元できなかったファイル数が既定値である100以上になった場合、ファイル共有復元のステータスは「警告」となります。`afs.restore.partial.success.threshold.count`構成設定をカスタマイズすることで、この既定値を編集できます。この実行方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

推奨事項

最適な復元パフォーマンスのために、外部ファイル共有ではなく、可能な限りファイルサーバー共有にデータを復元することをお勧めします。

> **「共有フォルダ」パネルへのアクセス**
>
> 「共有フォルダ」パネルにアクセスするには、ナビゲーションペインで、「**共有フォルダ**」をクリックします。

手順

1. 「共有フォルダ」パネルで、復元するファイルを含むファイル共有をクリックし、「詳細ビュー」を開きます。

   > 注「詳細ビュー」は、ファイル共有をクリックした場合にのみ表示されます。ファイル共有の名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。
3. 「**ファイルの復元**」をクリックします。「ファイルの復元」ダイアログボックスが開きます。
4. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**
5. 「**次へ**」をクリックします。
6. ファイル共有全体を復元する場合は、「フォルダ」セクションで、一番上のチェックボックス(「 」アイコンの前にあるチェックボックス)を選択します。そうでない場合は、選択可能なフォルダとファイルのリストから、復元するものを選択します。「**次へ**」をクリックします。

   > ヒントファイルが多すぎて表示が1ページに収まらない場合、「 」と「 」をクリックしてページを移動できます。「 」を使用して、ページごとに表示されるファイルの数を設定することもできます。

7. 選択したファイルの復元先(元のファイルサーバー共有、別のファイルサーバー共有、外部SMBまたはNFS共有、またはローカルマシン)に応じて、希望する復元オプションを選択し、「**次へ**」をクリックして、指示に従います。

復元オプション	説明
ファイルサーバー共有に復元	a. 「共有フォルダ」ドロップダウンメニューから、ファイルの復元先とするファイルサーバー共有を選択します。 b. ファイルを元の場所に復元するか、同じファイルサーバー共有にある別の場所に復元するか選択します。 別の場所を選択する場合、その場所へのパスを次の形式で指定します。 `/<Path>` c. 選択した場所にすでに同じ名前のファイルが存在した場合に、復元操作中に実行するアクションを指定します(ファイルの上書き、ファイルのスキップ、元のファイルの名前変更、または復元したファイルの名前変更)。

復元オプション	説明
	> ⚠ 重要 元のファイルの名前を変更する場合は、ファイルサーバー管理者でなければなりません。その他すべての操作については、ファイルサーバーかバックアップどちらの管理者でも構いません。 d. *ファイルを1つのSMB共有から別のSMB共有に復元する場合のみ。*ファイルの元のアクセス制御リストを復元する場合は、「**ACLの復元**」スイッチを有効にします。 e. 「**復元**」をクリックします。
外部共有に復元する	「共有タイプ」ドロップダウンメニューから、ファイルを復元する場所を選択し、必要な情報を入力します。 • **NFS** a. NFS共有フォルダへのパスを次の形式で入力します。 `\\server\<Path>` b. 選択した場所にすでに同じ名前のファイルが存在した場合に、復元操作中に実行するアクションを指定します(ファイルの上書き、ファイルのスキップ、元のファイルの名前変更、または復元したファイルの名前変更) 。 c. 「**復元**」をクリックします。 • **SMB** a. SMB共有フォルダへのパスを次の形式で入力します。 `\\server\<Path>` b. *オプション* .SMB共有にアクセスするためのユーザー資格情報を入力します。 c. 選択した場所にすでに同じ名前のファイルが存在した場合に、復元操作中に実行するアクションを指定します(ファイルの上書き、ファイルのスキップ、元のファイルの名前変更、または復元したファイルの名前変更) 。 d. *ファイルを1つのSMB共有から別のSMB共有に復元する場合のみ。*ファイルの元のアクセス制御リストを復元する場合は、「**ACLの復元**」スイッチを有効にします。 > ⚠ 重要「ACLの復元」スイッチを有効にする場合、ACLが宛先のSMB共有で認識されないことにより、復元したファイルにアクセスできない可能性があることに注意してください。 e. 「**復元**」をクリックします。

復元オプション	説明
ダウンロード	「**ダウンロード**」をクリックして、選択したファイルをローカルマシンに復元します。 ⚠ 重要 ダウンロード処理が終了するまで、ページの更新やページからの移動はしないでください。

第7章

ボリュームグループの保護

HYCUにより、高速で信頼性の高いバックアップと復元によりNutanixボリュームグループを保護できます。ボリュームグループをバックアップしたら、ボリュームグループ全体または個々の仮想ディスクのみを、NFSまたはSMB共有にエクスポートして復元することを選択できます。

> ⚠ 重要 バックアップ時にボリュームグループが1つ以上の仮想マシンにアタッチされている場合、それらは仮想マシンのバックアップ時に自動的にバックアップされます。詳細については、"仮想マシンの保護" ページ71を参照してください。

ボリュームグループを効率的に保護する方法の詳細については、以下のセクションを参照してください。

- "ボリュームグループのバックアップ" 下
- "ボリュームグループの復元" 次のページ

ボリュームグループのバックアップ

HYCUを使用すると、Nutanixボリュームグループを高速かつ効率的な方法でバックアップできます。

前提条件

保護したいボリュームグループが存在するNutanixクラスターが、HYCUに追加されました。説明については、"Nutanixクラスターの追加" ページ32を参照してください。

考慮事項

HYCUが自動的に作成し、データ保護目的で使用するボリュームグループは、「ボリュームグループ」パネルに表示されません。これらのボリュームグループの名前は、先頭が`NTNX-`、`hycu-vg-`、`HYCU-`になります。これと同じ接頭辞を持つ独自のボリュームグループを作成しないようしてください。

> 「ボリュームグループ」パネルのアクセス
>
> 「ボリュームグループ」パネルにアクセスするには、ナビゲーションペインで、「**ボリュームグループ**」をクリックします。

手順

1. 「ボリュームグループ」パネルで、バックアップするボリュームグループを選択します。

   > 💡 ヒント「**同期**」をクリックして、ボリュームグループのリストを更新できます。表示されているボリュームグループのリストを絞り込むには、"データのフィルタリング" ページ177で説明され

ているフィルタリングオプションを使用できます。

2. 「**ポリシー**」をクリックします。「ポリシー」ダイアログボックスが開きます。
3. 選択可能なポリシーのリストから、優先するポリシーを選択します。
4. 「**割り当て**」をクリックして、選択したボリュームグループにポリシーを割り当てます。

バックアップは、ポリシーに定義した値に従ってスケジュールされます。必要であれば、ボリュームグループの手動バックアップもいつでも実行できます。詳細については、"手動バックアップの実行" ページ190を参照してください。

ボリュームグループの復元

HYCUでは、ボリュームグループ全体、または破損した個々の仮想ディスクのみの、いずれかを復元できます。

考慮事項

選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため)がある層が含まれている場合、データを復元するためにこの層を使用することはできません。

復元オプション

次の復元オプションから選択できます。

復元オプション	説明
ボリュームグループを復元	ボリュームグループを復元できます。元のボリュームグループを、復元したボリュームグループで置き換える場合は、このオプションを選択します。説明については、"ボリュームグループの復元" 次のページを参照してください。
ボリュームグループをクローン	ボリュームグループのクローンを作成することで、仮想マシンを復元できます。元のボリュームグループを保持する場合は、このオプションを選択します。説明については、"ボリュームグループの複製" 次のページを参照してください。
vDiskのエクスポート	仮想ディスクをNFSまたはSMB共有に復元できます。特定のアクセス権限を持つユーザーが仮想ディスクを使用できるようにする場合、または後から仮想ディスクを使用してデータをHYCUにサポートされていないあるいはソースとしてHYCUに追加されていないハイパーバイザーのある環境に復元する場合に、このオプションを選択します。説明については、"仮想ディスクのエクスポート" ページ149を参照してください。

「ボリュームグループ」パネルのアクセス

「ボリュームグループ」パネルにアクセスするには、ナビゲーションペインで、「**ボリュームグループ**」をクリックします。

ボリュームグループの復元

ボリュームグループを元の場所または新しい場所に復元できます。この場合、元のボリュームグループは上書きされます。

考慮事項

ボリュームグループが1つ以上の仮想マシンにアタッチされている場合のみ。ボリュームグループがアタッチされている仮想マシンがオフになっている必要があります。

手順

1. 「ボリュームグループ」パネルで、復元するボリュームグループをクリックします。画面の下部に「詳細ビュー」が表示されます。

   > 注「詳細ビュー」は、ボリュームグループをクリックした場合にのみ表示されます。ボリュームグループの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 「詳細ビュー」で、優先する復元ポイントを選択します。
3. 「**復元**」をクリックします。
4. 「**ボリュームグループを復元**」を選択して、「**次へ**」をクリックします。
5. 「ストレージコンテナ」ドロップダウンメニューから、ボリュームグループを復元する場所を選択します。既定では、元のストレージコンテナが選択されます。
6. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**
7. *復元するボリュームグループが1つ以上の仮想マシンにアタッチされている場合のみ*。復元後にボリュームグループを仮想マシンにアタッチする場合は、「**ボリュームグループをアタッチ**」スイッチを有効にします。
8. 「**復元**」をクリックします。

ボリュームグループの複製

元のボリュームグループのクローンは、ボリュームグループを元の場所または新しい場所に復元することにより作成できます。この場合、元のボリュームグループは上書きされません。

手順

1. 「ボリュームグループ」パネルで、復元するボリュームグループをクリックします。画面の下部に「詳細ビュー」が表示されます。

   > 注「詳細ビュー」は、ボリュームグループをクリックした場合にのみ表示されます。ボリュームグループの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 「詳細ビュー」で、優先する復元ポイントを選択します。
3. 「**復元**」をクリックします。
4. 「**ボリュームグループをクローン**」を選択して、「**次へ**」をクリックします。
5. 「ストレージコンテナ」ドロップダウンメニューから、ボリュームグループを復元する場所を選択します。既定では、元のストレージコンテナが選択されます。
6. 「新しいボリュームグループ名」フィールドで、ボリュームグループの新しい名前を指定します。
7. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**
8. *復元するボリュームグループが1つ以上の仮想マシンにアタッチされている場合のみ*。復元後にボリュームグループを仮想マシンにアタッチする場合は、「**ボリュームグループをアタッチ**」スイッチを有効にします。
9. 「**復元**」をクリックします。

仮想ディスクのエクスポート

仮想ディスクをNFSまたはSMB共有に復元できます。

手順

1. 「ボリュームグループ」パネルで、仮想ディスクを復元するボリュームグループをクリックします。画面の下部に「詳細ビュー」が表示されます。

   > 注「詳細ビュー」は、ボリュームグループをクリックした場合にのみ表示されます。ボリュームグループの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

2. 「詳細ビュー」で、優先する復元ポイントを選択します。
3. 「**復元**」をクリックします。
4. 「**vDiskのエクスポート**」を選択して、「**次へ**」をクリックします。
5. 復元に選択できる仮想ディスクのリストから、復元するディスクを選択し、「**次へ**」をクリックします。
6. 「タイプ」ドロップダウンメニューから、仮想ディスクを復元する場所を選択し、必要な情報を入力します。

タイプ	説明
SMB	a. *オプション* .ドメインとユーザー資格情報を入力します。 b. SMBサーバー名またはIPアドレスを入力します。 c. サーバーのルートからのSMB共有フォルダへのパスを入力します(たとえば、/backups/HYCU) 。

タイプ	説明
NFS	a. NFSサーバー名またはIPアドレスを入力します。 b. サーバーのルートからのNFS共有フォルダへのパスを入力します(たとえば、/backups/HYCU) 。

7. 「復元元」ドロップダウンメニューから、復元に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :最新の状態に最速で復元できます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**
8. 「**復元**」をクリックします。

第8章

データ保護環境の復元

データ保護環境で災害が発生し、データが破損した、または利用できなくなった場合、HYCUではバックアップデータが保存されているターゲットをインポートすることにより、効果的にデータを復元することが可能になります。復元を実行できるのは次のとおりです。

- HYCU Backup Controllerを復元し、データの復元に使用
- 仮想マシン、アプリケーション、ファイル共有、ボリュームグループ

考慮事項

移行/DR準備完了仮想マシンとアプリケーション：HYCU Backup Controllerを使用すると、HYCU Protégéと保護されたデータをクラウドに復元できます。詳細については、"HYCU Protégé" ページ287を参照してください。

手順

1. 災害復旧の準備をします。説明については、"災害復旧の準備" 下を参照してください。
2. 災害復旧を実行します。説明については、"災害復旧の実行" ページ155を参照してください。
3. *HYCUがファイル共有保護に使用されている場合のみ*：HYCU インスタンスから復元されたHYCU Backup Controllerへの接続を再確立するか、HYCU インスタンスを再作成します。説明については、"HYCUインスタンスの再作成" ページ159を参照してください。

災害復旧の準備

前提条件

- 元のHYCU Backup Controllerのバックアップまたは復元する他のエンティティのバックアップを保存するターゲットの構成パラメーターが分かっている。詳細については、"災害復旧の準備" ページ74を参照してください。
- 復元するエンティティのバックアップデータを保存するターゲットは、復旧HYCU Backup Controllerを展開する予定のソースにアクセスできる。
- *元のHYCU Backup Controllerのバックアップが*SCSI*ターゲットに保存されている場合のみ*。iSCSIストレージデバイスは、単一のHYCU Backup Controller専用であり、HYCU以外のアプライアンスはない。
- *元のHYCU Backup Controllerまたは復元する仮想マシン、アプリケーション、ファイル共有、ボリュームグループのバックアップがGoogle Cloudターゲットに保存されている場合のみ*。Google Cloudサービスアカウントが作成済みで、HYCUに追加されている。クラウドアカウントをHYCUに追

加する方法に関する説明については、“Google Cloudサービスアカウントの追加” ページ212を参照してください。

- *元のHYCU Backup Controllerまたは復元する他のエンティティのバックアップが、ターゲット暗号化が有効になっているターゲットに保存されている場合のみ。*元のHYCU Backup Controllerから暗号化ターゲットキーをエクスポートし、暗号化キーを含むファイルが利用可能であること。

手順

タスク	説明
1. 復旧HYCU Backup Controllerを展開します。	“復旧HYCU Backup Controllerの展開” 下
2. 元のHYCU Backup Controllerのバックアップを保存するターゲットをインポートします。 インポートされたターゲットには、仮想マシン、アプリケーション、ファイル共有、ボリュームグループのバックアップが含まれる場合もあります。	“ターゲットのインポート” ページ154
3. HYCU Backup Controllerを復元する予定のソースを追加します。 仮想マシン、アプリケーション、ファイル共有、ボリュームグループも復元する場合は、それらを復元する予定のソースを追加します。	“ソースの追加” ページ32

復旧HYCU Backup Controllerの展開

手順

1. Nutanix Prism Webコンソール(Nutanix AHVクラスターの場合) またはvSphere (Web) Client (Nutanix ESXiクラスターとvSphere環境の場合) にログオンします。
2. 元のHYCU Backup Controllerまたは他のエンティティの復元に使用する復旧HYCU Backup Controllerを展開します。展開する環境に応じて、以下のいずれかを参照してください。
   - *Nutanix AHVクラスターの場合*：“HYCUのNutanix AHVクラスターへの展開” ページ23。
   - *Nutanix ESXiクラスターおよびvSphere環境の場合*：“HYCUのNutanix ESXiクラスターまたはvSphere環境への展開” ページ26。
3. *HYCU Backup Controllerの別のソースへの復元を予定している場合のみ。*HYCU Backup Controllerのクローンの作成を有効にします。これを実行するには、HYCU `config.properties`ファイルで、`clone.enabled.for.hycu.dr`構成設定を`true`に設定します。

   HYCU構成設定のカスタマイズ方法に関する説明については、“HYCU構成設定のカスタマイズ” ページ308を参照してください。

> **注意** 元のHYCU Backup Controllerがまだアクティブである間は、HYCU Backup Controllerのクローンをアクティブにしないでください。そのようにすると、データ損失が発生する可能性があります。

4. 復旧HYCU Backup ControllerのHYCU Webユーザーインターフェースにログオンします。
5. *元のHYCU Backup Controllerのバックアップまたは復元するエンティティのバックアップが、ターゲットの暗号化が有効になっているターゲットに保存されている場合のみ。*元のHYCU Backup Controllerからエクスポートした暗号化キーをインポートします。説明については、"ターゲット暗号化の構成" ページ215を参照してください。

復旧HYCU Backup Controllerの展開後

データ保護のニーズに応じて、災害復旧を実行した後、リカバリHYCU Backup Controllerを保持するか削除するかを決定できます。復旧HYCU Backup Controllerを削除すると、次に災害復旧を行うときに新しい災害復旧を展開する必要があります。

制限事項

*NutanixおよびSCSIターゲットの場合：*復旧HYCU Backup Controllerの保持はサポートされていません。このようなターゲットを災害復旧に使用する場合、毎回新しい復旧HYCU Backup Controllerを展開する必要があります。

考慮事項

復元HYCU Backup Controllerを維持することに決定した場合は、次のことを考慮してください。

- ターゲットのインポートに成功すると、復旧HYCU Backup Controllerは自動的に復旧モードになり、以下が適用されます。
  - HYCUはインポートしたターゲットを60分ごとに自動的に同期し、最新の復元ポイント(ターゲットに保存されたバックアップ)に関する情報、およびインポート可能なターゲットまたは削除されたターゲットに関する情報を取得します。

    > **注** インポートしたターゲットは、いつでも手動で同期させることもできます。これを実行するには、「ターゲット」パネルで、「**同期**」をクリックします。
  - バックアップ操作は無効です。これは、ポリシーの割り当て、手動バックアップの実行、または手動でバックアップの有効期限を切ることはできないことを意味します。
  - 電源オプションの設定は無効です。
  - 編集できるのは限られたターゲットオプションのみです。
  - ターゲットの追加は無効になります。
- ターゲット同期を成功させるには、復旧HYCU Backup ControllerはHYCUバージョン4.5.0で展開する必要があります。
- 非アクティブ化されたターゲットは、ターゲット同期から除外されます。
- 既定の自動ターゲット同期値は、データ保護のニーズに合わせて調整できます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

ターゲットのインポート

前提条件

- 元のHYCU Backup Controller(まだ存在する場合)のアクティビティは一時停止されなければならず、ジョブは実行できない。説明については、"電源オプションの設定" ページ231を参照してください。
- 復旧HYCU Backup Controllerにターゲットが存在しないか、インポートされたターゲットしか存在できない。そうでない場合、ターゲットのインポートは無効になっています。
- *iSCSIまたはNutanixターゲットをインポートする場合*:ターゲットは、電源がオンになっている他のHYCUバックアップコントローラー上でマウント解除する必要があります。

制限事項

- インポートされたターゲットへのデータのバックアップはサポートされていません。
- Blobストレージのバージョニングが有効なAzureターゲットのインポートはサポートされていません。

考慮事項

- インポートするターゲットには、復元するエンティティの完全なバックアップチェーンが含まれている必要があります。
- インポートジョブが完了するまで、HYCUを変更しないでください。

「ターゲット」パネルへのアクセス

「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

手順

1. 復旧HYCU Backup ControllerのHYCU Webユーザーインターフェースにログオンします。
2. 「ターゲット」パネルで、「**インポート**」をクリックします。「ターゲットのインポート」ダイアログボックスが開きます。
3. ドロップダウンメニューから、ターゲットのタイプを選択します。
4. 元のターゲット構成と一致するように値を指定して、「**次へ**」をクリックします。
5. 「バックアップカタログのインポート」ダイアログボックスで、バックアップをインポートするHYCU Backup Controllerの名前を選択し、「**次へ**」をクリックします。
6. 「複数のターゲット」ダイアログボックスに、選択したHYCU Backup Controllerおよび他のエンティティのバックアップデータを保存する1つ以上のターゲットが表示されます。追加のターゲットが見つかった場合は、それらを1つずつ選択して、元のターゲット構成と一致するように値を指定します。ターゲットごとに、「**検証**」をクリックして構成を確認します。

   > ⚠ 重要 アーカイブターゲットは他のターゲットから個別にインポートする必要があります。

7. 復元に必要なすべてのターゲットを検証したら、「**インポート**」をクリックします。

   > 注 リストからすべてのターゲットをインポートして、完全なバックアップチェーンを復元に使用できるようにすることをお勧めします。一部のターゲットをインポートせず、バックアップチェー

> ンが完了していない場合は、インポート手順を繰り返すことにより、欠落しているターゲットを後でインポートできます。

ターゲットのインポートが成功した後

- インポートされたターゲットが「ターゲット」パネルにリストされ、それらのモードが読み取り専用に設定されているため、これらのターゲットにバックアップデータを保存できません。
- HYCU Backup Controllerは「仮想マシン」パネルにリストされ、そのステータスはPROTECTED_DELETEDです。
- 仮想マシン、アプリケーション、ファイル共有、およびボリュームグループの復旧については、以下の点を考慮してください。
  - 元のデータ保護環境に存在するセルフサービスグループは、復旧HYCU Backup Controllerで再作成されます。再作成されたセルフサービスグループにはユーザーが含まれていません。仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元するには、ユーザーを作成し、それらを、復元する仮想マシン、ファイル共有、ボリュームグループの所有権を持つ再作成されたユーザーグループに追加する必要があります。説明については、“ユーザー環境のセットアップ” ページ200を参照してください。
  - インポートされたターゲットにバックアップが保存されている仮想マシンは、「仮想マシン」パネルにリストされ、ステータスはPROTECTED_DELETEDです。HYCU Backup Controller以外の仮想マシンを復元するには、“仮想マシンの復元” ページ86を参照してください。
  - インポートされたターゲットにバックアップが保存されているアプリケーションが「アプリケーション」パネルにリストされ、ステータスはPROTECTED_DELETEDです。アプリケーションを復元するには、“アプリケーション全体の復元” ページ122を参照してください。
  - インポートされたターゲットにバックアップが保存されているファイル共有が「共有フォルダ」パネルにリストされ、ステータスはPROTECTED_DELETEDです。ファイル共有を復元する方法は、“ファイル共有データの復元” ページ141を参照してください。
  - インポートされたターゲットにバックアップが保存されているボリュームグループが「ボリュームグループ」パネルにリストされ、ステータスはPROTECTED_DELETEDです。ボリュームグループを復元するには、“ボリュームグループの復元” ページ147を参照してください。

災害復旧の実行

次のいずれかの方法で、災害復旧を実行します。

復元対象	説明
HYCUバージョン4.0.0以降で作成された復元ポイントを使用して、HYCU Backup Controllerを元のソースに復元します。	“HYCU Backup Controllerの元のソースへの復元” 次のページ
HYCUバージョン4.0.0以降で作成された復元ポイントを使用して、HYCU Backup Controllerを別のソースに復元します。	• Nutanixクラスターで保護されているHYCU Backup ControllerをvSphere環境に復元する場合：

復元対象	説明
	"Nutanix AHVクラスターまたは Nutanix ESXiクラスターからvSphere環境への仮想マシンの復元" ページ318 • HYCU Backup Controllerを復元するときにソース環境と宛先環境の他のすべての組み合わせを使用する場合： "HYCU Backup Controllerの別のソースへの復元" 次のページ
4.0.0より前のHYCUバージョンで作成された復元ポイントを使用して、HYCU Backup Controllerを元のソースまたは別のソースに復元します。	"仮想ディスクのエクスポート" ページ104
仮想マシン	"仮想マシンの復元" ページ86
アプリケーション	"アプリケーション全体の復元" ページ122
ファイル共有	"ファイル共有データの復元" ページ141
ボリュームグループ	"ボリュームグループの復元" ページ147

HYCU Backup Controllerの元のソースへの復元

HYCU Backup Controllerの元のクラスターが破損していない場合、この手順を使用します。

前提条件

- 復旧HYCU Backup Controllerに、元のHYCU Backup Controllerのクラスターへのネットワークアクセスがあります。
- HYCU Backup Controllerの復元先に予定しているクラスターに応じて、対応するソースがHYCUに追加されている。
- *元のHYCU Backup Controllerのバックアップが SCSIまたはNutanixターゲットに保存されている場合のみ*：ターゲットを非アクティブ化して復元HYCU Backup Controllerから切り離してから、復元されたHYCU Backup Controllerの電源を入れる必要があります。

手順

1. 復旧HYCU Backup ControllerのHYCU Webユーザーインターフェースにログオンします。
2. 「仮想マシン」パネルで、HYCU Backup Controllerを選択します。
3. 画面の下部に表示される「詳細ビュー」で、最新の復元ポイントを選択します。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

4. 「**VMの復元**」をクリックします。

5. 「**VMの復元**」を選択し、「**次へ**」をクリックします。
6. 「ストレージコンテナを選択します」ドロップダウンメニューから、HYCU Backup Controllerを復元する場所を選択します。
7. 復元されたHYCU Backup Controllerが復元後に自動的にオンになるようにする場合は、「**仮想マシンの電源をオンにします**」スイッチをオンにしておきます。元のHYCU Backup Controllerがまだ存在している場合、自動的に削除されます。
8. 「**復元**」をクリックします。復元されたHYCU Backup Controllerのアクティビティは自動的に一意停止されます。
9. HYCU Webユーザーインターフェースからログアウトします。
10. *復旧HYCU Backup Controllerを保持しないと決定した場合のみ。*ソースから復旧HYCU Backup Controllerを削除します。説明については、NutanixまたはVMwareの資料を参照してください。
11. 復元されたHYCU Backup ControllerのHYCU Webユーザーインターフェースにログオンします。
12. HYCU Backup Controllerのアクティビティを再開します。説明については、"電源オプションの設定" ページ231を参照してください。
13. *Nutanix ESXiクラスターの場合 .*元のHYCU Backup Controllerが存在しない場合は、HYCU Backup Controllerに割り当てられた新しいネットワークアダプタの設定を構成します。説明については、"ネットワークの構成" ページ228を参照してください。

   > ⚠ 重要 必ずHYCU Backup Controllerの元のIPアドレスを入力します。接続を編集したら、古いネットワークアダプタを削除します。

HYCU Backup Controllerの別のソースへの復元

この手順は、元のHYCU Backup Controllerのクラスターが破損しているか動作不能である場合、またはHYCU Backup Controllerを再配置する場合に使用します。

前提条件

- 復旧HYCU Backup Controllerに、元のHYCU Backup Controllerを復元する予定のクラスターへのネットワークアクセスがある。
- HYCU Backup Controllerの復元先に予定しているクラスターに応じて、対応するソースがHYCUに追加されている。
- *元のHYCU Backup Controllerのバックアップが*SCSIまたは*Nutanixターゲットに保存されている場合のみ .*ターゲットを非アクティブ化して復元HYCU Backup Controllerから切り離してから、復元されたHYCU Backup Controllerの電源を入れる必要があります。

手順

1. *元のHYCU Backup Controllerがまだ存在している場合のみ。*元のHYCU Backup Controllerのアクティビティを一時停止します。

   > ⛔ 注意 元のHYCU Backup Controllerがまだアクティブである間は、HYCU Backup Controllerのクローンをアクティブにしないでください。この手順をスキップすると、データ損失が

発生する可能性があります。

元のHYCU Backup Controllerのアクティビティを一時停止するには、次の手順を実行します。

a. *HYCU Backup Controllerがオフになっている場合のみ*。HYCU Backup Controller(仮想マシン)をオンにします。

b. HYCU Webユーザーインターフェースにログオンします。

c. HYCU Backup Controllerのアクティビティを一時停止します。説明については、"電源オプションの設定" ページ231を参照してください。

d. 実行中のジョブが完了するのを待機します。これは、ジョブの実行ステータスでジョブリストをフィルタリングすることで確認できます。説明については、"データのフィルタリング" ページ177を参照してください。

2. *元のHYCU Backup Controllerがまだ存在している場合のみ*。以下のいずれかを実行します。

- ソースからHYCU Backup Controllerを削除します。

  Nutanix Prism Webコンソールまたはvsphere (Web) Clientで、ソースからHYCU Backup Controllerを削除します。説明については、NutanixまたはVMwareの資料を参照してください。

- HYCU Backup Controllerのアクティビティが、クローンの展開後に再開されないようにします。

3. 復旧HYCU Backup ControllerのHYCU Webユーザーインターフェースにログオンします。
4. 「仮想マシン」パネルで、元のHYCU Backup Controllerを選択します。
5. 画面の下部に表示される「詳細ビュー」で、最新の復元ポイントを選択します。

> 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

6. 「**VMの復元**」をクリックします。
7. 「**VMのクローン**」を選択し、「**次へ**」をクリックします。
8. 「ストレージコンテナを選択します」ドロップダウンメニューから、HYCU Backup Controllerを復元する場所を選択します。
9. 復元されたHYCU Backup Controllerが復元後に自動的にオンになるようにする場合は、「**仮想マシンの電源をオンにします**」スイッチをオンにしておきます。
10. 「**復元**」をクリックします。復元されたHYCU Backup Controllerのアクティビティは自動的に一意停止されます。
11. HYCU Webユーザーインターフェースからログアウトします。
12. *復旧HYCU Backup Controllerを保持しないと決定した場合のみ*。ソースから復旧HYCU Backup Controllerを削除します。説明については、NutanixまたはVMwareの資料を参照してください。
13. 復元されたHYCU Backup ControllerのHYCU Webユーザーインターフェースにログオンします。
14. HYCU Backup Controllerのアクティビティを再開します。説明については、"電源オプションの設定" ページ231を参照してください。

15. *元のHYCU Backup Controllerのネットワーク設定を使用する場合のみ*。HYCU Backup Controllerのネットワークアダプタの設定を構成します。説明については、"ネットワークの構成" ページ228を参照してください。

    > 注 必ずHYCU Backup Controllerの元のIPアドレスを入力します。

HYCUインスタンスの再作成

ファイルサーバー共有の保護にHYCUを使用している場合、データ保護環境には、HYCU Backup Controllerに接続されている少なくとも1つのHYCUインスタンスが含まれます。したがって、災害の重大度に応じて、復元されたHYCU Backup ControllerへのHYCUインスタンスの接続を再確立するか、またはHYCUインスタンスを再作成する必要があります。

影響を受けるコンポーネント	HYCUインスタンスに対する必須アクション
HYCU Backup Controller	HYCU Backup Controllerに接続されていたすべてのHYCUインスタンスの再接続
HYCUインスタンス	HYCUインスタンスの復元

前提条件

HYCU Backup Controllerの復元が完了し、HYCU Backup Controllerがオンになっている。

手順

1. HYCU Webユーザーインターフェースにログオンします。
2. 「⚙ **管理**」をクリックして、「**インスタンス**」を選択します。
3. 各HYCUインスタンスについて、その状態に応じて、以下のいずれかを実行します。
   - HYCUインスタンスはまだソース上にあります。
     a. *HYCUインスタンスがオンになっている場合のみ*。Nutanix Prism Webコンソールから、HYCUインスタンスをオフにします。
     b. Nutanix Prism Webコンソールから、HYCUインスタンスをオンにします。これによりHYCU Backup Controllerへの接続が確立され、自動的に再構成されます。
   - HYCUインスタンスは破損しているかすでに存在していません。
     a. *HYCUインスタンスの名前を維持する場合のみ*。「インスタンス」ダイアログボックスから、HYCUインスタンスのVM名、ホスト名、ソース、およびIPアドレスオプション値をメモします。
     b. *元のHYCUインスタンスがまだ存在しており、破損している場合のみ*。Nutanix Prism Webコンソールから、対応する仮想マシンをソースから削除します。
     c. *HYCUインスタンスの新しい名前を使用する場合のみ*。HYCUインスタンスをHYCU Webユーザーインターフェースから削除します。説明については、"HYCUインスタンスの管理" ページ220を参照してください。

d. 新しいHYCU インスタンスを作成します。元のHYCU インスタンスと同じソースで作成する必要はありません。説明については、“ファイルサーバーの追加” ページ35を参照してください。

> ⚠ 重要 HYCU インスタンスは、ご使用のHYCU Backup Controllerと同じHYCU 仮想アプライアンスイメージ(OVFパッケージ) から作成する必要があります。
>
> *HYCU インスタンスの名前を維持する場合のみ*。新しいHYCU インスタンスが元のHYCU インスタンスと同じ名前、ホスト名、およびネットワーク設定で構成されていることを確認します。

データ保護環境の変更により、HYCU インスタンスがもう必要ないことに気付いた場合は、それらを削除できます。説明については、“HYCUインスタンスの削除” ページ221を参照してください。

第9章

日々のタスクの実行

データ保護環境の安全で信頼できるパフォーマンスを確保するために、HYCUは日々の活動をサポートするためのさまざまなメカニズムを提供します。

目的	手順
データ保護環境の状態の概要を一目で把握し、最終的なボトルネックを特定し、データ保護環境のさまざまな箇所を検査します。	“HYCUダッシュボードの使用” 次のページ
環境で実行されているジョブを追跡し、特定のジョブステータスの分析情報を得て、ジョブレポートを生成し、現在実行中のジョブをキャンセルします。	“HYCUジョブの管理” ページ163
環境で発生しているすべてのイベントを表示します。	“HYCUイベントの管理” ページ165
イベントの発生時に通知を送信するようにHYCUを構成します。	“イベント通知の構成” ページ166
イベントおよびジョブの消去を有効にします。	“イベントおよびジョブの消去の有効化” ページ168
データ保護環境のさまざまな側面に関するレポートを取得します。	“HYCUレポートの使用” ページ169
エンティティ詳細を表示します。	“エンティティ詳細の表示” ページ174
フィルターを適用して、表示されている項目のリストを絞り込みます。	“データのフィルタリング” ページ177
任意のパネルのテーブルに表示できるデータをJSONまたはCSVファイルにエクスポートします。	“パネルのコンテンツのエクスポート” ページ184
ターゲット情報を表示、ターゲットのアクティブ化や非アクティブ化、iSCSIターゲットの容量を増やしたり、ターゲットを編集または削除したりします。	“ターゲットの管理” ページ185
ポリシー情報を表示するか、ポリシーを編集または削除します。	“ポリシーの管理” ページ188
データを手動でバックアップします。	“手動バックアップの実行” ページ190

目的	手順
検証ポリシーをセットアップし、バックアップ検証をスケジュールします。	“検証ポリシーのセットアップ” ページ191
復元ポイントを期限切れとしてマークします。	“バックアップの期限切れ指定” ページ252
データを手動でアーカイブします。	“データの手動でのアーカイブ” ページ194
スナップショットを再作成します	“スナップショットの再作成” ページ195

データ保護の効率や信頼性を低下させる可能性があるNutanix環境内での認識された問題の場合(たとえば、ストレージ、vCPU、またはメモリ使用率が超過している)、データ保護の目標をより適正に満たせるように調整を加えることができます。詳細については、“HYCU仮想マシンリソースの調整” ページ196を参照してください。

HYCUダッシュボードの使用

HYCUダッシュボードにより、環境内のデータ保護ステータスの概要を一目で確認できます。この直感的なダッシュボードにより、すべてのデータ保護アクティビティを監視し、注意が必要な箇所をすばやく特定できます。このダッシュボードは、対応するウィジェットをクリックするだけで目的のデータに簡単にアクセスできるため、日々のタスクの開始点として使用できます。

「ダッシュボード」パネルへのアクセス

「ダッシュボード」パネルにアクセスするには、ナビゲーションペインで、「**ダッシュボード**」をクリックします。

> ⚠ **重要** ユーザーロールは、表示およびアクセスを許可されるウィジェットを定義します。

以下の表は、各ウィジェットで見つけることができる情報の種類を説明しています。

ダッシュボードウィジェット	説明
仮想マシン	環境内の保護されている仮想マシンと物理マシンの割合、および保護されている、保護されていない、移行/DR対応のそれぞれの仮想マシンと物理マシンの正確な数を表示します。仮想マシンまたは物理マシンが考慮されます。 • 保護済み:少なくとも1つの有効なバックアップが利用でき、除外ポリシーが割り当てられていない場合、アプリケーションは保護されていると見なされます。 • 移行/DR準備完了:現在のバックアップチェーン内のすべてのバックアップがクラウドターゲット(Google CloudまたはAzure)の1つに保存され、最新のバックアップ中に正常なクラウド準備チェックが実行された場合。

ダッシュボードウィジェット	説明
	仮想および物理マシンの保護の詳細については、“仮想マシンのバックアップ” ページ85を参照してください。
アプリケーション	保護されたアプリケーションの割合と、保護されたアプリケーションと保護されていないアプリケーションの正確な数を表示します。少なくとも1つの有効なバックアップが利用でき、除外ポリシーが割り当てられていない場合、アプリケーションは保護されていると見なされます。アプリケーションの保護の詳細については、“アプリケーションのバックアップ” ページ121を参照してください。
HYCUコントローラー*	HYCUバックアップコントローラーがある仮想マシンに関するリソース情報を表示します(ストレージ、vCPU、およびメモリ)。これらの値のいずれかがクリティカル値に達した場合(つまり、円で示された値のいずれかが赤になった場合)の対処方法の詳細については、“HYCU仮想マシンリソースの調整” ページ196を参照してください。
バックアップ	過去7日間のバックアップジョブの成功率を示します。
ターゲット*	既存のターゲットの数、全体的な容量使用率、およびターゲットタイプごとの使用率を表示します。ターゲットのセットアップの詳細については、“ターゲットのセットアップ” ページ38を参照してください。
ポリシー	準拠しているポリシーの割合と、準拠および非準拠ポリシーの正確な数を示します。このポリシーが割り当てられているすべてのエンティティがポリシー設定に準拠している場合、ポリシーは準拠していると見なされます。ポリシーの詳細については、“バックアップ戦略の定義” ページ58を参照してください。
ジョブ	ステータス(成功、警告、失敗、進行中、待機中)に応じた過去56時間のデータ保護環境内のジョブの数を表示します。ジョブの詳細については、“HYCUジョブの管理” 下を参照してください。
イベント	ステータス(成功、警告、失敗)に応じた過去56時間のデータ保護環境内のイベントの数を表示します。イベントの詳細については、“HYCUイベントの管理” ページ165を参照してください。

* インフラストラクチャグループ管理者のみ。

HYCUジョブの管理

「ジョブ」パネルで、以下を実行できます。

- 現在実行中のプロセスを確認します。
- 完了および停止したプロセスを確認します。

- ジョブを選択したら、画面の下部に表示される「詳細ビュー」で、特定のジョブの詳細を確認します。

  > **ヒント** 特定のタスク(データのバックアップなど)の進行状況バーで一時停止することで、すでにバックアップ済みのデータの量や、進行状況時間の最終更新日など、タスクに関する追加情報を利用できます。

- *アタッチされているボリュームグループがある仮想マシンの場合* :仮想マシンにアタッチされているボリュームグループのバックアップと復元プロセスのステータスを確認します。これを行うには、アタッチされたボリュームグループがある仮想マシンのバックアップジョブまたは復元ジョブの横にある矢印をクリックします。アタッチされたボリュームグループプロセスとそのステータスのリストが展開されます。ボリュームグループプロセスは一度にすべて表示されるのではなく、ジョブが進行するにつれて1つずつ表示されることに注意してください。
- 特定のジョブに関するレポートを選択して生成し、「**レポートを見る**」をクリックします。クリップボードへのレポートをコピーするには、開かれた「ジョブレポート」ダイアログボックスで、「**クリップボードにコピー**」をクリックします。
- 現在実行中または待機中のジョブを選択してキャンセルし、「**ジョブを中止する**」をクリックします。
- ジョブの消去を有効にします。詳細については、"イベントおよびジョブの消去の有効化" ページ 168を参照してください。

考慮事項

バックアップ、バックアップコピー、またはアーカイブジョブに失敗すると、HYCUはジョブの再試行を自動的にスケジュールします。以下について考慮してください。

- バックアップジョブが失敗すると、RPO値に達するまで、それぞれの連続する再試行の時間間隔は2倍となります(たとえば、既定では最初の再試行は15分後、2回目は30分後、3回目は1時間後、のようになります)。RPO値に達すると、バックアップジョブを再試行する時間間隔は、RPOに指定されたものと同じになります。
- バックアップコピージョブが失敗すると、HYCUは失敗したジョブを15分の時間間隔で2回再試行します(既定の場合)。どちらの再試行も失敗した場合、ジョブの再試行は24時間中断されます。
- アーカイブジョブが失敗すると、HYCUは失敗したジョブを15分後に1回再試行します(既定の場合)。この再試行が失敗した場合、ジョブの再試行は12時間中断されます。

「ジョブ」パネルへのアクセス

「ジョブ」パネルにアクセスするには、ナビゲーションペインで、「**ジョブ**」をクリックします。

> **ヒント** 「**更新**」をクリックして、ジョブのリストを更新できます。

各ジョブについて次の情報を入手できます。

ジョブ情報	説明
名前	実行されたジョブの名前(たとえば、ソースの追加、ターゲットの追加、バックアップの実行など)

ジョブ情報	説明
ステータス	ジョブの現在のステータス(たとえば、キューに入っている、実行ステータスを示す進行状況バー、OK、またはエラーなど) 。
作成日時	ジョブが作成された日時。
終了日時	ジョブが終了した日時。

HYCUイベントの管理

「イベント」パネルで、以下を実行できます。

- お使いの環境で発生しているすべてのイベントを表示します。
- 選択したイベントについての詳細を確認します。
- 指定したフィルターに一致するイベントをリストします。
- イベントの発生時に通知を送信するようにHYCUを構成します。詳細については、"イベント通知の構成" 次のページを参照してください。
- イベントの消去を有効にします。詳細については、"イベントおよびジョブの消去の有効化" ページ 168を参照してください。

「イベント」パネルへのアクセス

「イベント」パネルにアクセスするには、ナビゲーションペインで、「**イベント**」をクリックします。

> ヒント「**更新**」をクリックして、イベントのリストを更新できます。

各イベントについて次の情報を入手できます。

イベント情報	説明
ステータス	イベントのステータス(成功、警告、失敗)
メッセージ	イベントの説明
カテゴリー	イベントが属するカテゴリー(たとえば、ポリシー、バックアップ、資格情報、内部イベントの場合のシステムなど) 。
タイムスタンプ	イベント作成時刻

イベントの概要やイベントの詳細を検索できる「詳細ビュー」を開くには、目的のイベントをクリックします。

> ヒント「詳細ビュー」を最小化するには、「▼ **最小化**」をクリックするか、または**スペースバー**を押します。元のサイズに戻すには、「▲ **最大化**」をクリックするか、または**スペースバー**を押します。

イベント通知の構成

HYCUは、データ保護環境で新しいイベントが発生したときに通知を送信するように構成できます。これによりデータ保護環境をより効率的に監視および管理し、必要な場合はすぐにイベントに対応することができます。メールやWebhookを通知チャネルとしてセットアップできます。

> 「通知」ダイアログボックスへのアクセス
>
> 「通知」ダイアログボックスにアクセスするには、ナビゲーションペインで「 **イベント**」をクリックし、ツールバーで「 **通知**」をクリックします。

どの通知チャネルを使用するかに応じて、次のセクションのいずれかを参照してください。

- “メール通知のセットアップ” 下
- “Webhook通知のセットアップ” 次のページ

メール通知のセットアップ

前提条件

HYCUはSMTPを使用してメール通知を送信するため、SMTPサーバーを構成する必要があります。詳細については、“SMTPサーバーの構成” ページ233を参照してください。

手順

1. 「通知」ダイアログボックスで、「**Eメール**」タブをクリックし、「 **新規**」をクリックします。
2. 「件名」フィールドで、Eメール通知の件名を入力します。
3. 「カテゴリー」ドロップダウンメニューから、イベントが属する1つ以上のカテゴリー(ポリシー、バックアップ、資格情報、システムなど) を選択します。すべてのカテゴリーを含めるには「**すべてを選択**」をクリックします。
4. 「ステータス」ドロップダウンメニューから、イベントのステータス(成功、警告、失敗) を選択します。すべてのステータスを含めるには「**すべてを選択**」をクリックします。
5. 「言語」ドロップダウンメニューから、メール通知に使用する言語を選択します。
6. 「電子メールアドレス」フィールドに、通知の送信先となる電子メールアドレスを1つ以上入力します。複数のメールアドレスを入力する場合には、それぞれを入力してから必ずスペースバーを押します。
7. 「**保存**」をクリックします。

変更内容は即時に有効となり、通知設定で指定した電子メールアドレスに電子メール通知が送信されます。

既存のメール通知の設定は後から編集することができます(「 **編集**」をクリックして必要な変更を行います) 。または不要になったものは削除できます(「 **削除**」をクリックします) 。

Webhook通知のセットアップ

手順

1. 「通知」ダイアログボックスで、「**Webhook**」タブをクリックし、「**＋ 新規**」をクリックします。
2. Webhook通知の名前とその説明(オプション)を入力します。
3. 「カテゴリー」ドロップダウンメニューから、イベントが属する1つ以上のカテゴリー(ポリシー、バックアップ、資格情報、システムなど)を選択します。すべてのカテゴリーを含めるには「**すべてを選択**」をクリックします。
4. 「ステータス」ドロップダウンメニューから、イベントのステータス(成功、警告、失敗)を選択します。すべてのステータスを含めるには「**すべてを選択**」をクリックします。
5. 「言語」ドロップダウンメニューから、Webhook通知に使用する言語を選択します。
6. 「Post URL」フィールドに、Webhook通知の送信先とするエンドポイントのURLを、次のいずれかの形式で入力します。

   ```
   https://<Host>
   https://<Host>/<Path>
   ```

   指定されたURLにHYCUが送信するデータ形式の詳細については、"Webhookデータ形式" 下を参照してください。
7. *受信側のエンドポイントが送信者のIDを必要とする場合のみ*。「認証タイプ」ドロップダウンメニューから、以下のいずれかの認証タイプを選択します。
   - 「**Basic認証**」を選択した場合は、Webhookエンドポイントに関連するユーザー名とパスワードを入力します。
   - 「**シークレットによる認証**」を選択した場合は、Webhookエンドポイントに接続するためのシークレットを入力します。
8. 「**次へ**」をクリックします。
9. *オプション* :HYCUから送信されたリクエスト本文をカスタマイズします。HYCUのフィールドリストで該当するフィールドをクリックすると、イベント変数を簡単に本文に挿入できます。

   > ⚠ 重要 本文で定義したフォーマットが、Webhook通知の送信先のプラットフォームでサポートされていることを確認します。

   Webhookリクエスト本文の形式については、"Webhookデータ形式" 下を参照してください。
10. 「**保存**」をクリックします。

変更内容は即時に有効となり、通知設定で指定したURLにWebhook通知が送信されます。

既存のWebhook通知の設定は後から編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。

Webhookデータ形式

Webhookデータ形式は、次により定義されます。

- HYCUによって送信されるHTTPリクエストヘッダー
- HYCUによって送信されるHTTPリクエスト本文
- Webhookエンドポイントにより送信され、HYCUにより受信されたHTTP応答コード

HTTPリクエストヘッダー

リクエストヘッダーは次の形式で送信されます。

```
content-type = application/json
x-hycu-signature = base64(hmac(body, secret, 'sha256'))
```

> 注 x-hycu-signatureリクエストヘッダーは、Webhookシークレットが指定されている場合のみ送信されます。

HTTPリクエスト本文

リクエスト本文は次の形式で送信されます。

```
{
"severity": "<severity-value>",
"created": "<created-value>",
"details": "<details-value>",
"category": "<category-value>",
"message": "<message-value>",
"user": "<user-value>",
"taskId": "<taskId-value>"
}
```

> 注 null値は無視されます。

HTTP応答コード

Webhook URLは、HTTPステータスコード204の応答を必ず返します。

イベントおよびジョブの消去の有効化

HYCUデータベースからのデータの消去を有効にすると、日々のビジネス操作に必要なくなったイベントやジョブ(また関連する全ジョブレポート)をHYCUが定期的に削除するように構成することができます。

前提条件

インフラストラクチャグループ管理者であること。

考慮事項

対応する復元ポイントが存在しないか期限切れの場合にのみ、バックアップ、バックアップのコピー、アーカイブに関連するジョブは削除されます。

イベントを消去するのかジョブを消去するのかに応じて、次のいずれかのパネルにアクセスします。

- 「イベント」パネルへのアクセス

  「イベント」パネルにアクセスするには、ナビゲーションペインで、「**イベント**」をクリックします。

- 「ジョブ」パネルへのアクセス

  「ジョブ」パネルにアクセスするには、ナビゲーションペインで、「**ジョブ**」をクリックします。

手順

1. 「イベント」または「ジョブ」パネルで「**パージ構成**」をクリックします。
2. 状況に応じて、「**イベントのパージを有効にする**」または「**ジョブのパージを有効にする**」スイッチを使用します。
3. データを保持する年数、月数、週数、日数を指定します。指定した値よりも古いイベントやジョブは消去されます。最大値は99年です。
4. 「**保存**」をクリックすると、指定値を基にしてHYCUデータベースの消去が開始されます。

   > ⚠ 重要 このアクションを元に戻すことはできません。削除したイベントデータやジョブデータは取得することができなくなります。

イベントやジョブの消去を有効にしても、後からいつでも消去構成を編集することや消去を無効にすることができます。

HYCUレポートの使用

HYCUレポートは、データ保護環境のリソースとジョブの視覚的なプレゼンテーションを提供します。この包括的で正確なプレゼンテーションにより、データを分析するための最適なビューが得られるので、データの保護について最善の判断を下すことができます。

レポートデータは、表またはグラフとして表示できます。レポートを視覚化するために、棒グラフ、ヒートマップ、折れ線グラフ、面グラフ、散布図などのレポートグラフタイプが使用されます。

考慮事項

ユーザーグループとユーザーロールによって、表示できるレポートデータの種類と実行できるレポートアクションが決まることに注意してください。

"レポートの開始" 次のページで説明されているレポートに精通したら、次のように続行できます。

- レポートを表示します。詳細については、"レポートの表示" ページ171を参照してください。
- レポートを生成します。詳細については、"レポートの生成" ページ172を参照してください。
- レポートをスケジュールします。詳細については、"レポートのスケジューリング" ページ173を参照してください。

  > 注 レポートをスケジュールするときは、レポートをメールで送信することも選択できます。

- レポートをエクスポートおよびインポートします。詳細については、"レポートのエクスポートおよびインポート" ページ174を参照してください。

「レポート」パネルへのアクセス

「レポート」パネルにアクセスするには、ナビゲーションペインで、「**レポート**」をクリックします。

レポートの開始

定義済みレポートを利用するか、追加のレポートを作成して、データ保護環境をよりよく理解し、潜在的な問題を特定し、パフォーマンスを向上させることができます。

定義済みレポートのリストについては、"定義済みレポート" 下を参照してください。レポートの作成方法の説明については、"レポートの作成" 次のページを参照してください。

定義済みレポート

「 🔖 」アイコンで表される定義済みレポートにより、データ転送、ジョブステータス、バックアップの数、保護されたデータの量など、データ保護環境の重要な側面に関するレポートを取得できます。これらのレポートは編集または削除できません。

定義済みレポート	説明
Entity compliance status	バックアップ要件に準拠および非準拠の仮想マシンと物理マシン、アプリケーション、および共有のリスト。
Hourly activities per policy	割り当てられたポリシーのリストと、過去24時間の各時間に実行されていた対応するジョブの数。
Hourly activities per target*	ターゲットのリストと、過去24時間の各時間に実行されていた対応するジョブの数。
Protected data	毎日計算される保護されたデータの総量。
Protected data per policy	ポリシーごとに過去24時間に保護されたデータの量。
Protected data per owner*	所有者ごとの保護されたデータの総量。
Protected data per target*	ターゲットごとの過去24時間の保護されたデータの量。
Protected data timeline per target*	ターゲットごとの保護されたデータの1日の量。
Protected VM size per target *	保護された仮想マシンと物理マシンのリスト、およびターゲット間での対応する保護されたデータの配布。
VM backup status	バックアップのステータスや期間、バックアップサイズなどの情報を含む、過去24時間に発生したバックアップのリスト。
VM backup status per target*	ターゲットと、バックアップのステータスや期間、バックアップサイズなどの情報を含む、過去24時間に発生した関連バックアップのリスト。

* インフラストラクチャグループ管理者のみが利用できます。

レポートの作成

定義済みレポートがレポート要件を満たさない場合は、新しいレポートを作成して、要件に合わせて調整できます。

前提条件

管理者ユーザーロールが割り当てられている。

新しいレポートを最初から作成するか、または既存のレポートを編集して新しいレポートとして保存するかに応じて、以下を実行します。

目的	手順
新規レポートをゼロから作成します。	1. 「レポート」パネルで、「**＋ 新規**」をクリックします。「レポート構成」ダイアログボックスが開きます。 2. レポート名とその説明(オプション)を入力します。 3. レポートのタイプを選択します。 4. 収集したデータセットに基づいて計算を実行するために使用する集計値を選択します。 5. レポートの時間範囲を指定します。定義済みの時間範囲を選択するか、「**カスタム**」を選択してからカレンダーを使用して、時間範囲の開始日と終了日を選択することができます。 6. x軸とy軸の間でレポートに含める収集データのレポートタグを配布し、収集データのレポートでの表示方法を決定します。 7. 「**保存**」をクリックします。
既存のレポートを編集して、新しいレポートとして保存します。	1. 「レポート」パネルで、レポートのリストから、編集して新しいレポートとして保存するレポートを選択し、「**✎ 編集**」をクリックします。「レポート構成」ダイアログボックスが開きます。 2. レポートの新しい名前を入力し、必要な変更を加えます。 3. 「**名前を付けて保存**」をクリックします。

作成済みレポートはいずれも後から編集することができます(「**✎ 編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**🗑 削除**」をクリックします)。「**🔖**」アイコンで表される定義済みレポートは編集または削除できません。

レポートの表示

データ保護環境の現在の状態に関するレポート、または手動あるいは自動で生成された保存済みレポートを表示できます。

目的	手順
データ保護環境の現在の状態に関するレポートを表	「レポート」パネルで、レポートのリストから、目的のレポートを選択し、それをダブルクリックするかまたは「**👁 プレビュー**」をクリックします。

目的	手順
示します。	
保存済みレポートを表示します。	1. 「レポート」パネルで、レポートのリストから、目的のレポートを選択します。 2. 画面の下部に表示される「詳細ビュー」で、目的のレポートバージョンを選択し、「**ビュー**」をダブルクリックまたはクリックします。 手動または自動でレポートを生成する方法の詳細については、"レポートの生成" 下または"レポートのスケジューリング" 次のページを参照してください。

開かれたダイアログボックスで、レポートデータを表示することに加え、以下も実行できます。

- レポートを切り替えます。
- PDF、PNG、またはCSV形式のレポートをダウンロードします。これを実行するには、「**ダウンロード**」をクリックし、使用可能な形式の1つを選択します。
- *管理者ユーザーロールが割り当てられているユーザーの場合*：データ保護環境の現在の状態に関するレポートを表示する場合、「**生成**」をクリックしてこのバージョンのレポートを保存できます。保存されたレポートは、レポートバージョンのリストに追加されます。

レポートの生成

レポートを生成すると、実際には選択したレポートの現在のバージョン(レポートバージョン)のコピーが将来の参照用に保存されます。

前提条件

管理者ユーザーロールが割り当てられている。

手順

1. 「レポート」パネルで、レポートのリストから、生成するレポートを選択します。

   > 注 選択可能などのレポートもレポート要件を満たさない場合、新しいレポートを作成できます。詳細については、"レポートの作成" 前のページを参照してください。

2. 画面の下部に表示される「詳細ビュー」で、「**＋ 生成**」をクリックします。「レポートバージョンの生成」ダイアログボックスが開きます。
3. *オプション*：レポートの説明を入力します。
4. 「**生成**」をクリックします。

> ヒント 選択したレポートのバージョンは、「**プレビュー**」、次に「**生成**」をクリックして保存することもできます。

生成されたレポートは、対応するレポートを選択したときに画面の下部に表示される「詳細ビュー」の、レポートバージョンのリストに追加されます。

後で以下を実行できます。

- 保存済みレポートを表示します。詳細については、"レポートの表示" ページ171を参照してください。
- 不要になった保存済みレポートを削除します。これを実行するには、目的のレポートバージョンを選択し、「**削除**」をクリックします。

レポートのスケジューリング

スケジューリングを使用して、毎日、毎週、または毎月の特定の時間にレポートを自動的に生成できます。これらのレポートをWebブラウザーで表示したり、メールで配信されるようにスケジュールしたりできます。

前提条件

- 管理者ユーザーロールが割り当てられている。
- *メールでレポートを送信する場合* SMTPサーバーが構成済みである。詳細については、"SMTPサーバーの構成" ページ233を参照してください。

手順

1. 「レポート」パネルで、レポートのリストから、定期的に生成するレポートを選択し、「**スケジューラー**」をクリックします。「レポートスケジューラ」ダイアログボックスが開きます。

   > 注 選択可能などのレポートもレポート要件を満たさない場合、新しいレポートを作成できます。詳細については、"レポートの作成" ページ171を参照してください。

2. 「スケジュール日」フィールドで、レポート生成を開始する日付と時刻を指定します。
3. 「間隔」ドロップダウンメニューから、レポートを生成する頻度(毎日、毎週、または毎月)を選択します。
4. メール受信者へのレポートの自動配信をスケジュールする場合は、「**送信**」スイッチを使用して、以下を実行します。
   a. 「レポート形式」ドロップダウンメニューから、レポートのファイル形式(PDF、PNG、またはCSV)を選択します。
   b. 「電子メールアドレス」フィールドで、レポートを受け取る1人以上のメール受信者を入力します。複数のメールアドレスを入力する場合には、それぞれを入力してから必ずスペースバーを押します。
5. 「**保存**」をクリックします。

> ヒント 自動的に生成されるレポートには、「レポート」パネルの「スケジュール済み」列に「✓」のマークが付いています。

後で以下を実行できます。

- スケジュールされたレポートのスケジュールオプションを編集します。これを実行するには、レポートを選択し、「**スケジューラー**」をクリックし、必要な変更を行い、「**スケジュール**」をクリックします。
- レポートを自動的に生成したくなくなった場合は、レポートのスケジュールを解除します。これを実行するには、レポートを選択し、「**スケジューラー**」をクリックし、「**スケジュールを解除**」をクリックします。

レポートのエクスポートおよびインポート

HYCUを使用すると、レポートをJSONファイルにエクスポートし、それからレポートをJSONファイルからインポートすることにより、異なるHYCUデータ保護環境間でユーザーが作成したレポートを共有できます。

> ⚠ 重要 付与されている権限により、表示や編集ができるレポートの種類が決まり、HYCUアプライアンス間でレポートをコピーする前に考慮する必要がある、レポートへのさまざまなアクセスレベルも定義されます。

レポートのエクスポート

手順

1. 「レポート」パネルで、すべてのレポートのリストから、エクスポートするレポートを選択し、「**エクスポート**」をクリックします。
2. 「**OK**」をクリックします。

選択したレポートはJSONファイルにエクスポートされ、システムのダウンロード場所に保存されます。

レポートのインポート

手順

1. 「レポート」パネルで、「**インポート**」をクリックします。「レポートのインポート」ダイアログボックスが開きます。
2. インポートするレポートのファイルシステムを参照します。
3. レポートの名前とその説明(オプション)を入力します。
4. 「**インポート**」をクリックします。

新しいレポートがレポートのリストに追加されます。

エンティティ詳細の表示

「仮想マシン」、「アプリケーション」、「共有フォルダ」、または「ボリュームグループ」パネルの「詳細ビュー」で、各仮想マシン、物理マシン、検出されたアプリケーション、ファイル共有、ボリュームグループに関する詳細を表示できます。以下の詳細が利用可能です。

概要	選択したエンティティについての詳細情報を表示します。
復元ポイント	各復元ポイントに関する以下の情報を表示できます。 • 復元ポイントが作成された日時。 • 層: ◦ BCKP バックアップ:バックアップが期限切れでない限り、既定で使用できます。 ▪ FULL 完全:完全バックアップが実行された場合に表示されま

	す。 ■ INCR増分 :増分バックアップが実行された場合に表示されます。 ◦ ARCHアーカイブ :データアーカイブが作成された場合に使用できます。アイコンを一時停止することで、データアーカイブの総数やアーカイブの有効期限を確認できます。いずれかのアーカイブジョブが失敗した場合、失敗したアーカイブジョブの数が表示されます。 ◦ COPYコピー :バックアップデータのコピーが作成された場合に使用できます。アイコンを一時停止することで、バックアップコピーの総数やバックアップコピーの有効期限を確認できます。バックアップコピージョブのいずれかが失敗した場合、失敗したバックアップコピージョブの数が表示されます。 ◦ SNAPスナップショット :高速復元を実行できるローカルスナップショットがソースに含まれている場合に使用できます。アイコンを一時停止すると、スナップショットが再作成されたかどうかとその有効期限を確認できます。 ◦ SNAP部分スナップショット :*Nutanixクラスターのみ*。高速復元を実行できるローカルスナップショットがソースに含まれている場合に使用できます。このようなスナップショットには、ディスクの部分セットのみが含まれています。アイコンを一時停止すると、スナップショットが再作成されたかどうかとその有効期限を確認できます。 仮想ディスクがバックアップから除外された場合、対応する層のラベルは赤い丸でマークされます。たとえば、FULL。 ⚠ 重要 層のいずれかが赤色になっている場合、復元には使用できません。
コンプライアンス	エンティティの次の準拠ステータスを示します。 • 成功 • 失敗 • 未定義 エンティティは、最後の正常なバックアップからの時間がHYCUポリシーで設定されたRPOよりも短く、推定復元時間がHYCUポリシーで設定されたRTOよりも短い場合、バックアップ要件に準拠していると見なされます。 それぞれのアイコンで示される準拠ステータスで一時停止することにより、バックアップに関する追加情報を使用できます。バックアップ頻度、最後に成功したバックアップからの経過時間、復元に設定した制限時間、復元に必要な推定時間を確認できます。さらに、エンティティの準拠ステータスが「失敗」の場合、このリストには準拠していない理由も記載されます。

バックアップステータス	詳細については、"エンティティのバックアップステータスの表示" 下を参照してください。
復元ステータス	エンティティの復元の進行状況を示す進行状況バーを表示します。 ヒント 進行状況バーをダブルクリックすると、「ジョブ」パネルに移動し、関連するジョブの詳細を確認できます。

ヒント 項目が多すぎて表示が1ページに収まらない場合、「 > 」と「 < 」をクリックしてページを移動できます。「 ⌄ 」を使用して、ページごとに表示される項目の数を設定することもできます。

エンティティのバックアップステータスの表示

エンティティのバックアップステータスによって、エンティティを復元できるかどうかが決まります。

制限事項

アタッチされたボリュームグループがある仮想マシンの場合、「エラーで完了」バックアップステータスは、ボリュームグループが直接アタッチされている仮想マシンでのみ有効です。

エンティティのバックアップステータス	VM、VG、またはvDisksの復元？	仮想マシンファイルの復元？	アプリケーションを復元しますか？	ファイル共有の復元？
Completed successfully	✓	✓	✓	✓
Completed with warnings	✓	✓	✓[a]	✓
Completed with errors	✓[b]	✓[c]	✓[d]	✓[e]
失敗	×	×	×	×
期限切れ	×	×	×	×
スキップ[f]	✓	✓	×	該当なし

[a] データを復元するポイントインタイムを指定することはできません。このバックアップステータスは、ディスクマッピングが失敗したか、仮想マシンにNICがないためか、またはアプリケーションの場合、少なくとも1つのデータベースログバックアップが失敗した(他のすべてのデータベースは整合状態である)ために発生する可能性があります。

[b] すべての仮想マシンのディスクファイルが正常にバックアップされたわけではないため、仮想マシンの復元は部分的です。システムディスクの1つがバックアップされていない場合は、オンにできない可能性があります。

[c] すべての仮想マシンディスクファイルが正常にバックアップされたわけではないため、個別のファイルの復元は部分的です(「ファイルの復元」ダイアログボックスに表示されるファイルのみ)。

[d] アプリケーションの復元は部分的です(それぞれの復元ダイアログボックスに表示されるデータベースのみ)。

[e] すべてのファイルが正常にバックアップされたわけではないため、ファイル共有の復元は部分的です。バックアップが失敗したファイルは、対応するサブタスクのジョブレポートにリストされます。

[f] 共有ストレージでのフェールオーバークラスターのパッシブノードのバックアップにのみ適用されます。

> 注 アイコンで示されるバックアップステータスで一時停止することにより、バックアップに関する追加情報を利用できます。バックアップタイプ、バックアップ整合性、バックアップの期間と規模、使用されたターゲット、およびバックアップUUIDを確認できます。ボリュームグループの場合、仮想マシンバックアップの一環として、およびポリシーを直接割り当てることによって、ボリュームグループがバックアップされているかどうかを確認することもできます。
>
> バックアップステータスアイコンをダブルクリックすると、「ジョブ」パネルに移動し、関連するジョブの詳細を確認できます。

データのフィルタリング

HYCUは、メインフィルターと詳細フィルターという、適用できる2タイプのフィルターを提供しています。フィルターを適用したら、フィルター条件に一致したデータのみが表示され、必要なものを簡単に見つけることができます。

メインフィルターの適用

データ保護環境の特定の側面に焦点を合わせたい場合は、メインフィルターを適用します(たとえば、「仮想マシン」パネルでデータをフィルタリングすると、目的の仮想マシンまたは担当している仮想マシンにのみ焦点を当てることができます) 。

> 注 このタイプのフィルターは、「アプリケーション」、「仮想マシン」、「ボリュームグループ」、「共有フォルダ」、「ポリシー」、「ターゲット」、「ジョブ」、「イベント」、および「セルフサービス」パネルで利用できます。

手順

1. 選択したパネルで、「**メインフィルター**」をクリックします。「メインビュー」サイドパネルが開きます。
2. フィルター条件を選択します。
3. 「**フィルターを適用**」をクリックします。

利用可能なフィルタリングオプションの詳細については、次のセクションのいずれかを参照してください。

- “「アプリケーション」パネルのフィルタリングオプション” 次のページ
- “「仮想マシン」パネルのフィルタリングオプション” ページ179
- “「ボリュームグループ」パネルのフィルタリングオプション” ページ181
- “「共有フォルダ」パネルのフィルタリングオプション” ページ182
- “「ポリシー」パネルのフィルタリングオプション” ページ183
- “「ターゲット」パネルのフィルタリングオプション” ページ183
- “「ジョブ」パネルのフィルタリングオプション” ページ183

- “「イベント」パネルのフィルタリングオプション” ページ183
- “「セルフサービス」パネルのフィルタリングオプション” ページ184

詳細フィルターの適用

選択した項目の復元およびバックアップデータに関する情報に焦点を合わせたい場合は、詳細フィルターを適用します。

> 注 このタイプのフィルターは、「アプリケーション」、「仮想マシン」、「ボリュームグループ」、および「共有フォルダ」パネルで利用できます。

手順

1. 選択したパネルのすべての項目のリストから、復元およびバックアップデータによってフィルタリングする項目を選択します。
2. 画面の下部に表示される「詳細ビュー」で、「**詳細フィルター**」をクリックします。「詳細ビュー」サイドパネルが開きます。
3. フィルター条件を選択します。
4. 「**フィルターを適用**」をクリックします。

利用可能なフィルタリングオプションの詳細については、次のセクションのいずれかを参照してください。

- “「アプリケーション」パネルのフィルタリングオプション” 下
- “「仮想マシン」パネルのフィルタリングオプション” 次のページ
- “「ボリュームグループ」パネルのフィルタリングオプション” ページ181
- “「共有フォルダ」パネルのフィルタリングオプション” ページ182

> ヒント フィルタリングされた項目が多すぎて表示が1ページに収まらない場合、「 > 」と「 < 」をクリックしてページを移動できます。「 ∨ 」を使用して、ページごとに表示されるフィルタリング結果の項目の数を設定することもできます。

「アプリケーション」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
検索	検索語句を入力します。アプリケーションの名前でフィルタリングできます。
ソース	ドロップダウンメニューから、アプリケーションが実行されている仮想マシンまたはアプリケーションが実行されている物理マシンをホストするソースを選択します。
ポリシー割り当て	いずれかのオプションを選択して、仮想マシンまたは物理マシン上で実行するアプリケーションをポリシーの割り当てによってフィルタリングします。 • **割り当て解除** • **割り当て済み**

フィルタリングオプション	実行内容
	注このオプションを選択した場合、除外ポリシーが割り当てられているアプリケーションはリストされないことに注意してください。 • **特定のポリシー**
所有者	ドロップダウンメニューから、アプリケーションが実行されている仮想マシンまたは物理マシンに割り当てられている所有者を選択します。
アプリケーションタイプ	ドロップダウンメニューから、アプリケーションタイプを選択します。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
保護	保護ステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
検出	アプリケーション検出ステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。 • **成功** :1つ以上のアプリケーションが検出されました。 • **失敗** :アプリケーションは検出されませんでした。 • **警告** :仮想マシンまたは物理マシンがオフラインであるかアクセスできないため、アプリケーション検出に失敗しました。

「詳細ビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
層	ドロップダウンメニューから、1つ以上の層を選択します。
復元ポイント日	復元ポイントの作成時刻でフィルタリングするための時刻を選択します。
バックアップステータス	バックアップステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

「仮想マシン」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
検索	検索語句を入力します。仮想マシン名または物理マシン名、HYCU UUID、またはソースUUIDでフィルタリングできます。
ソース	ドロップダウンメニューから、仮想マシンまたは物理マシンをホストするソースを選択します。

フィルタリングオプション	実行内容
資格情報グループ	ドロップダウンメニューから、仮想マシンまたは物理マシンの資格情報を選択します。
ポリシー割り当て	いずれかのオプションを選択して、仮想マシンまたは物理マシンをポリシーの割り当てによってフィルタリングします。 • **割り当て解除** • **割り当て済み** 注 このオプションを選択した場合、除外ポリシーが割り当てられている仮想マシンまたは物理マシンはリストされないことに注意してください。 • **特定のポリシー**
検証ポリシーの割り当て	いずれかのオプションを選択して、仮想マシンまたは物理マシンを検証ポリシーの割り当てによってフィルタリングします。 • **割り当て解除** • **割り当て済み** • **特定の検証ポリシー**
所有者	ドロップダウンメニューから、仮想マシンまたは物理マシンに割り当てられている所有者を選択します。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
検出	アプリケーション検出ステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。 • **成功** :1つ以上のアプリケーションが検出されました。 • **失敗** :アプリケーションは検出されませんでした。 • **警告** :仮想マシンまたは物理マシンがオフラインであるかアクセスできないため、アプリケーション検出に失敗しました。 • **未定義** :アプリケーション検出ステータスに関する情報は利用できません。
保護	保護ステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
検証ステータス	バックアップ検証ステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
ディザスタリカバリの準備完了	移行/DR準備ステータスでフィルタリングするために、このチェックボックスを選択します。

「詳細ビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
層	ドロップダウンメニューから、1つ以上の層を選択します。
復元ポイント日	復元ポイントの作成時刻でフィルタリングするための時刻を選択します。
バックアップステータス	バックアップステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

「ボリュームグループ」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、以下のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
ソース	ドロップダウンメニューから、ボリュームグループをホストするソースを選択します。
ポリシー割り当て	いずれかのオプションを選択して、ポリシー割り当てでボリュームグループをフィルタリングします。 • **割り当て解除** • **割り当て済み** 注 このオプションを選択した場合、除外ポリシーが割り当てられているボリュームグループは表示されないことに注意してください。 • **特定のポリシー**
所有者	ドロップダウンメニューから、ボリュームグループに割り当てられている所有者を選択します。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
保護	保護ステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

「詳細ビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
層	ドロップダウンメニューから、1つ以上の層を選択します。
復元ポイント日	復元ポイントの作成時刻でフィルタリングするための時刻を選択します。
バックアップステータス	バックアップステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

フィルタリングオプション	実行内容
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

「共有フォルダ」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
検索	検索語句を入力します。ファイル共有名でフィルタリングできます。
ファイルサーバー	ドロップダウンメニューから、ファイル共有をホストするファイルサーバーを選択します。
プロトコル	ドロップダウンメニューから、ファイル共有のプロトコルを選択します(SMBまたはNFS) 。
ポリシー割り当て	いずれかのオプションを選択して、ポリシー割り当てでファイル共有をフィルタリングします。 • **割り当て解除** • **割り当て済み** 注 このオプションを選択した場合、除外ポリシーが割り当てられているファイル共有はリストされないことに注意してください。 • **特定のポリシー**
所有者	ドロップダウンメニューから、ファイル共有に割り当てられている所有者を選択します。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
保護	ファイル共有の保護ステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

「詳細ビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
層	ドロップダウンメニューから、1つ以上の層を選択します。
復元ポイント日	復元ポイントの作成時刻でフィルタリングするための時刻を選択します。
バックアップステータス	バックアップステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

「ポリシー」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
検索	検索語句を入力します。ポリシーの名前でフィルタリングできます。
コンプライアンス	コンプライアンスステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。

「ターゲット」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
検索	検索語句を入力します。ターゲットの名前でフィルタリングできます。
ターゲットタイプ	ターゲットタイプでフィルタリングするために、1つ以上のチェックボックスを選択します。
健全性	ターゲットの正常性でフィルタリングするために、1つ以上のチェックボックスを選択します。

「ジョブ」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
検索	検索語句を入力します。ジョブ名またはジョブUUIDでフィルタリングできます。
ステータス	ジョブのステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
時間範囲	ジョブの検索を制限する時間範囲を指定します。定義済みの時間範囲(過去1時間、過去24時間、または先週)のいずれかを選択するか、カレンダーを使用して、表示するジョブの時間範囲の開始日時と終了日時を選択できます。

「イベント」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
メッセージ	テキスト文字列を入力して、指定された文字列があるメッセージのみが

フィルタリングオプション	実行内容
	含まれるようにリストをフィルタリングします。
カテゴリー	テキスト文字列を入力して、指定された文字列があるカテゴリーのみが含まれるようにリストをフィルタリングします。
ユーザー名	ドロップダウンメニューから、ユーザー名を選択します。
ステータス	イベントのステータスでフィルタリングするために、1つ以上のチェックボックスを選択します。
時間範囲	イベントの検索を制限する時間範囲を指定します。定義済みの時間範囲(過去1時間、過去24時間、または先週)のいずれかを選択するか、カレンダーを使用して、表示するイベントの時間範囲の開始日時と終了日時を選択できます。

「セルフサービス」パネルのフィルタリングオプション

「メインビュー」サイドパネルで、1つ以上のフィルタリングオプションを選択します。

フィルタリングオプション	実行内容
グループ名	グループ名を入力します。
ステータス	次のいずれかを選択して、グループまたはユーザーのステータス(つまり、どのグループまたはユーザーがHYCUへのログオンを許可されている/いないか)でフィルタリングします。

パネルのコンテンツのエクスポート

任意のパネルの表に表示できるデータは、JSON形式またはCSV形式のファイルにエクスポートできます。

考慮事項

特定のデータのみをエクスポートする場合は、「**メインフィルター**」をクリックし、ファイルにエクスポートするデータの種類に基づいてフィルター条件を選択し、「**フィルターを適用**」をクリックします。

手順

1. データをエクスポートするパネルにナビゲートします。
2. 「**エクスポート**」をクリックし、ドロップダウンメニューから、以下のいずれかのオプションを選択します。

オプション	説明
JSONにエクスポート(現在)	現在のテーブルページをJSONファイルにエクスポートします。

オプション	説明
JSONにエクスポート(すべて)	すべてのテーブルデータをJSONファイルにエクスポートします。
CSVにエクスポート(現在)	現在のテーブルページをCSVファイルにエクスポートします。
CSVにエクスポート(すべて)	すべてのテーブルデータをCSVファイルにエクスポートします。

ターゲットの管理

適切な許可がある場合には、ターゲット情報の表示、ターゲットプロパティの編集、ターゲットのアクティブ化/非アクティブ化、ターゲットを保護データの保存に使用しなくなったときの削除などを実行できます。

「ターゲット」パネルへのアクセス

「ターゲット」パネルにアクセスするには、ナビゲーションペインで、「**ターゲット**」をクリックします。

ターゲット情報の表示

「ターゲット」パネルのターゲットのリストで、各ターゲットについての情報を表示できます。これによりターゲットの一般ステータスの概要を知ることができます。各ターゲットについて次の情報を入手できます。

ターゲット情報	説明
名前	ターゲットの名前。
タイプ	ターゲットのタイプ(NFS、SMB、Nutanix、Nutanix Objects、iSCSI、AWS S3/Compatible、AZURE、Google Cloud、QStar NFS、またはQStar SMB)。 注 テープターゲットはアイコンで、WORMが有効なクラウドターゲットはアイコンでそれぞれ表されます。
健全性	ターゲットの正常性ステータス: • グレー:正常性テストの前の初期ターゲットステータスを示します。これは非アクティブなターゲットも示します。 • 緑:ターゲットは正常な状態で、ターゲット利用率は設定値未満です(既定は90%)。 • 黄:ターゲット利用率は設定値を超えています(既定は90%)。 • 赤:ターゲット利用率は設定値を超えています(既定は95%)。また、テストタスク後のターゲットエラー状態も示します(たとえば、I/Oエラーが発生した、ターゲットがアクセスできない、許可が拒否されたなど)。 HYCUは、バックアップデータを保存するための十分なスペースがターゲットにあるかどうかを、以下に基づいて計算します。

ターゲット情報	説明
	• *以前のバックアップがターゲットに保存されていない場合* :バックアップが完全か増分かに関係なく、仮想マシンまたは物理マシンのバックアップに含まれるすべてのディスクのプロビジョニングされたスペースの合計。 • *以前のバックアップがターゲットに保存されている場合* :増分バックアップの最後の増分バックアップのサイズ、または完全バックアップあるいは(以前の増分バックアップが存在しない場合の)増分バックアップの最後の完全バックアップのサイズ。
容量	バックアップファイル用に予約するストレージ領域量の見積もり(MiB、GiB、またはTiB単位)。
使用率	保護されたデータの保存にすでに使用されている指定されたターゲットサイズの割合。
モード	ターゲットのモード: • 読み書き:このターゲットは、データのバックアップと復元に使用できます。 • 読み取り専用:このターゲットは、データの復元にのみ使用できます。 ⚠ 重要 インポートされたターゲットで読み取り専用モードが自動的に設定され、バックアップを実行できなくなります。インポートされたターゲットのモードを変更しないようにしてください。
ステータス	ターゲットのステータス: • アクティブ:このターゲットは、データのバックアップと復元に使用できます。 • 非アクティブ:このターゲットは、データのバックアップと復元に使用できません。このステータスは、メンテナンスタスク(たとえば、新しいディスクの追加)により、ターゲットが非アクティブ化されていることを示します。 ターゲットのステータスを変更する方法の詳細については、"ターゲットのアクティブ化または非アクティブ化" 次のページを参照してください。

ターゲットの概要やターゲットの詳細を検索できる「詳細ビュー」を開くには、目的のターゲットをクリックします。

> ヒント 「詳細ビュー」を最小化するには、「▼ **最小化**」をクリックするか、または**スペースバー**を押します。元のサイズに戻すには、「▲ **最大化**」をクリックするか、または**スペースバー**を押します。

ターゲットの編集

> ⛔ 注意 ターゲットの場所を変更すると、データ損失が生じる可能性があります。したがって、新しいターゲットの場所を指定する前に、同じサーバーまたは別のサーバー上のこの新しい場所に既存のバックアップデータがすでに移動していることを確認します。

考慮事項

- HYCU Backup Controllerに割り当てられたポリシーのターゲット設定を変更する場合は、必ずターゲットの構成のメモを更新します。
- *QStarテープターゲットの場合*：Integral Volumeセットのステータスがオフラインの場合、対応するテープターゲットがHYCU内で自動的に非アクティブ化されます。Integral VolumeセットをQStarに再マウントする場合は、必ずターゲットをアクティブ化してください。この実行方法の詳細については、"ターゲットのアクティブ化または非アクティブ化" 下を参照してください。

手順

1. 「ターゲット」パネルで、編集するターゲットを選択し、「**編集**」をクリックします。「ターゲットの編集」ダイアログボックスが表示されます。
2. 選択したターゲットを必要に応じて編集します。ターゲットプロパティの詳細については、"ターゲットのセットアップ" ページ38を参照してください。

   > ⚠ 重要 NFSかSMBのサーバー名、IPアドレス、または共有フォルダへのパス、あるいはiSCSIターゲットのポータルIPアドレスを変更する場合は、"ストレージの取り外しとターゲットデータの変更" 下を参照してください。
3. 「**保存**」をクリックします。

ストレージの取り外しとターゲットデータの変更

NFSかSMBのサーバー名、IPアドレス、または共有フォルダへのパス、あるいはiSCSIターゲットのポータルIPアドレスを変更する場合は、ストレージをHYCU Backup Controllerから取り外して、必要な変更を行える状態にする必要があります。

手順

1. "ターゲットのアクティブ化または非アクティブ化" 下の説明に従って、ターゲットを非アクティブ化し、ストレージをHYCU Backup Controllerから取り外します。
2. "ターゲットの編集" 前のページの説明に従って、最初にターゲットのあるサーバーで必要な変更を行い、次にHYCU Webユーザーインターフェースでも同じ変更を行います。
3. "ターゲットのアクティブ化または非アクティブ化" 下の説明に従って、ターゲットをアクティブ化します。

ターゲットのアクティブ化または非アクティブ化

手順

1. 「ターゲット」パネルで、アクティブ化または非アクティブ化するターゲットを選択します。
2. 「**アクティブ化**」または「**非アクティブ化**」をクリックして、選択したターゲットのステータスを変更します。
3. *NFS、SMB、およびiSCSIターゲットの場合*：ターゲットを非アクティブ化してNFSかSMBのサーバー名、IPアドレス、または共有フォルダへのパス、あるいはiSCSIターゲットのポータルIPアドレスを変更する場合は、「**ストレージの取り外し**」スイッチを有効にしてください。ストレージをHYCU Backup

Controllerから取り外す方法の詳細については、“ストレージの取り外しとターゲットデータの変更” 前のページを参照してください。

4. *ターゲットの非アクティブ化の場合*：「**はい**」をクリックして、選択したターゲットの非アクティブ化を確認します。

   ターゲットを非アクティブにすると、そのターゲットはバックアップと復元の操作には使用されなくなります。

iSCSIターゲットのサイズの増分

HYCUでは、HYCU論理ボリュームを拡張することにより、iSCSIターゲットのサイズを増やすことができます。

前提条件

- iSCSIサーバー上でターゲットのサイズが増分されている。
- 選択したターゲットで進行中のバックアップまたは復元ジョブがない。
- 他のどのメンテナンスタスクも選択されたターゲット上ではまだ実行されていない(ターゲットの編集、iSCSIイニシエーターの秘密の更新、CHAP認証を有効にしたターゲットのCHAP認証セッションのリセットなど)。
- 選択したターゲットの他のサイズの増分がまだ開始されていない。

手順

1. 「ターゲット」パネルで、サイズを大きくするターゲットを選択し、「**拡張**」をクリックします。
2. 「**はい**」をクリックして、選択したターゲットのサイズを増やすことを確認します。

iSCSIターゲットのサイズの増分が正常に完了したかどうかを示すメッセージを受け取ります。

ターゲットの削除

保護されたデータが含まれていないターゲットは削除できます。ターゲットを削除すると、そのターゲットを含むバックアップまたは復元アクションは実行できなくなります。

手順

1. 「ターゲット」パネルで、削除するターゲットを選択し、「**削除**」をクリックします。

   > **注** 削除するターゲットがアーカイブに使用されている場合、指定したアーカイブターゲットを持つデータアーカイブがポリシーにより使用されてないことを確認します。

2. 「**はい**」をクリックして、選択したターゲットを削除することを確認します。

ポリシーの管理

適切な権限があれば、ポリシー情報を表示したり、ポリシーのプロパティを編集したり、データの保護に使用しなくなった場合にポリシーを削除したりできます。

> 「ポリシー」パネルのアクセス
>
> 「ポリシー」パネルにアクセスするには、ナビゲーションペインで、「**ポリシー**」をクリックします。

ポリシー情報の表示

「ポリシー」パネルのポリシーのリストで、各ポリシーについての情報を表示できます。これによりポリシーの一般ステータスの概要を知ることができます。

考慮事項

ポリシーで定義されたバックアップRPO、RTO、および保持期間の値は、日、週、月、または年に丸められて表示されますが、内部的には定義したとおりに保存され使用されます。たとえば、30日はHYCU Webユーザーインターフェースでは1か月に丸められます。

各ポリシーで以下の情報を入手できます。

ポリシー情報	説明
名前	ポリシーの名前。
コンプライアンス	ポリシーの準拠ステータス： • 成功 • 失敗 • 未定義 このポリシーが割り当てられているすべてのエンティティがポリシー設定に準拠している場合、ポリシーは準拠していると見なされます。エンティティのコンプライアンスステータスの詳細については、“エンティティ詳細の表示” ページ174を参照してください。
VM数	特定のポリシーが割り当てられている仮想マシンと物理マシンの総数。
APP Count	特定のポリシーが割り当てられているアプリケーションの総数。
説明	ポリシーの説明(バックアップジョブと復元ジョブが実行される頻度)。

ポリシーの概要やポリシーの詳細を検索できる「詳細ビュー」を開くには、目的のポリシーをクリックします。

> **ヒント** 「詳細ビュー」を最小化するには、「▼ **最小化**」をクリックするか、または**スペースバー**を押します。元のサイズに戻すには、「▲ **最大化**」をクリックするか、または**スペースバー**を押します。

ポリシーの編集

考慮事項

「コピー」オプションを有効にしたのと同様の方法でポリシーを編集する場合、このポリシーを割り当てる仮想マシンおよびボリュームグループの次のバックアップは完全バックアップになります。

手順

1. 「ポリシー」パネルで、編集するポリシーを選択し、「✎ **編集**」をクリックします。「ポリシーの編集」ダイアログボックスが表示されます。

2. 必要に応じて、選択したポリシーを編集します。ポリシープロパティの詳細については、"ポリシーの作成" ページ60を参照してください。

   > ⚠ 重要 *vSphere環境の場合*：「Backup from replica」または「Fast restore」オプションを有効にするような方法で、vSphere仮想マシンまたはアプリケーションに割り当てられているポリシーを編集することはできません。これらのオプションは、vSphere仮想マシンまたはアプリケーションには使用できません。

3. 「**保存**」をクリックします。

ポリシーの削除

考慮事項

- バックアップがスケジュールされている1つ以上のエンティティに割り当てられているポリシーは、削除できません。このようなポリシーを削除したい場合は、まずスケジュールされたバックアップを中止する必要があります。待機中ジョブの中止の詳細については、"HYCUジョブの管理" ページ163を参照してください。
- 1つ以上のエンティティに割り当てられているポリシーを削除する場合、これらのエンティティに対してそれ以上のバックアップは実行されないことに注意してください。

手順

1. 「ポリシー」パネルで、削除するポリシーを選択し、「 **削除**」をクリックします。
2. 「**はい**」をクリックして、選択したポリシーを削除することを確認します。

手動バックアップの実行

選択したエンティティにポリシーを割り当てたら、HYCUはデータを自動的にバックアップします。ただし、データはいつでも手動でバックアップできます(たとえば、テスト目的で、またはバックアップが失敗した場合など) 。

前提条件

ボリュームグループを手動でバックアップする場合のみ。ポリシーが直接ボリュームグループに割り当てられていることを確認します。ボリュームグループがアタッチされている仮想マシンのみにポリシーが割り当てられている場合、選択したボリュームグループの手動バックアップを実行することはできません。

考慮事項

手動バックアップが、ポリシーで指定されたRPOによって決定されるスケジュール済みバックアップに干渉するのを防ぐことができます。それを実行するには、`exclude.manually.run.backups.regarding.rpo`構成設定を`true`に設定します。手動バックアップを実行すると、バックアップウィンドウでスケジュールされたバックアップが開始されず、次のバックアップウィンドウまたは次の手動バックアップまでデータが保護されなくなるという可能性があるため、バックアップウィンドウを定義する場合、これは特に重要です。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

手順

1. 「仮想マシン」、「アプリケーション」、「共有フォルダ」、または「ボリュームグループ」パネルで、バックアップするエンティティを選択します。
2. 「**バックアップ**」をクリックして、選択したエンティティのバックアップを実行します。
3. 完全バックアップを実行する場合は、「**完全バックアップを実行**」スイッチを使用します。そうしない場合、HYCUはポリシーで定義された設定に基づき、フルバックアップまたは増分バックアップを実行します。
4. 「**はい**」をクリックして、手動バックアップの開始を確認します。

> ヒント ナビゲーションペインで、「**ジョブ**」をクリックして、バックアップの総合的な進捗を確認します。

検証ポリシーのセットアップ

仮想マシンのバックアップ検証を手動で行い、仮想マシンに破損したバックアップがないことを確認する代わりに、検証ポリシーをセットアップし、検証ポリシーで定義した値に従ってバックアップ検証をスケジュールすることができます。仮想マシンクローンを作成して仮想マシンのバックアップを検証する方法の詳細については、“仮想マシンのバックアップの検証” ページ98を参照してください。

> ⚠ 重要 HYCUは、バックアップ検証の実行中に、仮想マシンのクローンを自動的に作成します。

前提条件

- 仮想マシンのコピーにvSphereストレージコンテナを選択する場合は、仮想マシンに最新バージョンのVMware Toolsがインストールされている必要があります。
- *高度な検証タイプを指定することを予定している場合のみ。*
  - 資格情報を仮想マシンに割り当てる必要があります。前提条件、制限、考慮事項、説明については、“アプリケーションデータへのアクセスの有効化” ページ113を参照してください。
  - ネットワークカードを仮想マシンに追加する必要があります。

制限事項

HYCU Backup Controllerに対するバックアップ検証の実行はサポートされていません。

考慮事項

- 仮想マシンが静的IPアドレスで構成されている場合、バックアップ検証中にネットワークの競合が発生し、バックアップ検証データの信頼性が低下する可能性があります。
- *Windows仮想マシンのバックアップ検証を実行するときに、高度な検証タイプを指定することを予定している場合のみ。*ディスクエラーのチェックが失敗する場合もありますが、これは仮想マシンが破損していることを意味するものではありません。ただし、そのような仮想マシンのステータスは手動で確認することをお勧めします。
- バックアップ検証の実行後に、次のことを検討します。

- 「仮想マシン」パネルの「検証」列で、仮想マシンのバックアップ検証ステータスを表示できます(アイコンで表される)。アイコンを一時停止することで、仮想マシンにどの検証ポリシーが割り当てられているかも確認できます。
- 除外ポリシーは、クローンされた仮想マシンに自動的に割り当てられます。

「仮想マシン」パネルへのアクセス

ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、バックアップ検証を実行する1つ以上の仮想マシンを選択します。

   ヒント「**同期**」をクリックして、仮想マシンのリストを更新できます。表示されている仮想マシンのリストを絞り込むには、"データのフィルタリング" ページ177で説明されているフィルタリングオプションを使用できます。

2. 「**認証**」をクリックします。「検証ポリシー」ダイアログボックスが開きます。
3. 「**＋ 新規**」をクリックします。
4. 検証ポリシーの名前と説明(オプション)を入力します。
5. 「ストレージコンテナ」ドロップダウンメニューから、バックアップ検証を実行する仮想マシンのクローンを作成する場所を選択します。
6. 「復元元」ドロップダウンメニューから、バックアップ検証に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動**
   - **バックアップ**
   - **コピー**
   - **アーカイブ**

   注「自動」を選択した場合、バックアップ検証の階層は、既定では、バックアップ > コピー > アーカイブという優先順位で選択されます。これは、HYCUが常に、バックアップ検証のために指定された順序で最初に利用可能な層を使用することを意味します。ただし、この既定の動作は、HYCU `config.properties`ファイルの`backup.validation.restore.source.priority.order`構成設定をカスタマイズして、データ保護のニーズに合わせて層の順序を調整することで、いつでも変更できます。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

7. 「検証後にVMを保持」ドロップダウンメニューから、バックアップ検証の実行後に仮想マシンを保持するかどうかに応じて、次のオプションのいずれかを選択します。

オプション	説明
常に	仮想マシンは、バックアップ検証の実行後に、常に保持されます。
検証エラー時	仮想マシンは、検証時に検証エラーが発生した場合にのみ、バックアップ検証の実行後に保持されます。

オプション	説明
決して	仮想マシンは、バックアップ検証の実行後に、自動的に削除されます。

8. 「検証タイプ」ドロップダウンメニューから、以下のいずれかのタイプを選択します。

検証タイプ	説明
基本	バックアップ検証時に、以下のタスクが行われます。 • 仮想マシンがクローンされ、オンになります。 • ゲストOSがシャットダウンします。
高度	バックアップ検証時に、以下のタスクが行われます。 • 仮想マシンがクローンされ、オンになります。 • 仮想マシン上で実行しているすべてのアプリケーションが検出されます。 • 仮想ディスクが検証され、それには仮想マシンのファイルシステムや仮想マシン上の既存のディスクの確認が含まれます。Windows仮想マシンの場合、ディスクエラーの確認も行われます。 • 指定された場合、カスタムスクリプトが実行されます。 • ゲストOSがシャットダウンします。

9. *高度な検証タイプを選択した場合のみ*。以下を実行します。
   a. バックアップ検証プロセスの一部として仮想マシン上でカスタムスクリプトを実行する場合は、「**カスタムスクリプトを実行**」スイッチを有効にし、スクリプトへの適切なパスが指定されていることを確認します。

      > 注 正常に終了した場合はスクリプトは終了コード0を返し、失敗の場合はそれ以外を返します。

   b. 「ネットワーク」ドロップダウンメニューから、仮想マシンのネットワークを選択します。
10. 「**次へ**」をクリックします。
11. 仮想マシンのバックアップ検証を日次、週次、月次、または年次ベースで実行するかどうかに応じて、任意の優先バックアップ検証オプションをクリックして、有効なオプションのリストに追加します。
    - **日次**
    - **週次**
    - **月次**
    - **年次**
12. 選択したバックアップ検証オプションに応じて、バックアップ検証を実行する間隔を指定します。

アーカイブオプション	説明
日次	a. 「繰り返し間隔」フィールドで、バックアップ検証を毎日実行するか、数日ごとに実行するかを指定します。 b. 平日のみバックアップ検証を行う場合は、「**平日のみ適用**」スイッ

アーカイブオプション	説明
	チを使用します。
週次	a. 「繰り返し間隔」フィールドで、バックアップ検証を毎週実行するか、数週間ごとに実行するかを指定します。 b. バックアップ検証を実行する曜日を1つ以上選択します。
月次	a. 「繰り返し間隔」フィールドで、バックアップ検証を毎月実行するか、数か月ごとに実行するかを指定します。 b. バックアップ検証を、毎月の同じ日付(「毎月5日」など)にアーカイブするか、毎月の特定の日(「毎月第2金曜日」など)に実行するかを選択します。
年次	a. 「繰り返し間隔」フィールドで、バックアップ検証を毎年実行するか、数年ごとに実行するかを指定します。 b. バックアップ検証を、希望する月の同じ日付(「1月5日」など)に行うか、希望する月の特定の日(「4月の第2金曜日」など)に行うかを選択します。

13. 「**保存**」をクリックします。
14. 「**割り当て**」をクリックします。

既存の検証ポリシーはいずれも後から編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。

データの手動でのアーカイブ

HYCUは「アーカイブ」ポリシーオプションを有効にすると、データを自動的にアーカイブします。ただし、いつでも手動でデータをアーカイブできます(たとえば、特定の復元ポイントのデータをアーカイブする場合や、アーカイブジョブが失敗した場合など)。

前提条件

- 管理者、バックアップおよび復元オペレーター、またはバックアップオペレーターユーザーロールが割り当てられている。
- 割り当てられたポリシーで「アーカイブ」オプションが指定され、データアーカイブが作成されている。

考慮事項

- アーカイブの保存期間は、データをアーカイブするエンティティの復元ポイントが作成された日時から計算されます。
- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため)がある層が含まれている場合、手動でデータをアーカイブするためにこの層を使用することはできません。

アーカイブするデータのタイプに応じて、以下のいずれかのパネルにアクセスします。

- 「アプリケーション」パネルへのアクセス

  「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

- 「仮想マシン」パネルへのアクセス

  ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

- 「共有フォルダ」パネルへのアクセス

  「共有フォルダ」パネルにアクセスするには、ナビゲーションペインで、「**共有フォルダ**」をクリックします。

- 「ボリュームグループ」パネルのアクセス

  「ボリュームグループ」パネルにアクセスするには、ナビゲーションペインで、「**ボリュームグループ**」をクリックします。

手順

1. 「アプリケーション」、「仮想マシン」、「共有フォルダ」、または「ボリュームグループ」パネルで、データをアーカイブするエンティティをクリックします。
2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   > 注「詳細ビュー」は、エンティティをクリックした場合にのみ表示されます。エンティティの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

3. 「**アーカイブの実行**」をクリックします。「アーカイブの実行」ダイアログボックスが開きます。
4. 目的のアーカイブオプションを選択します。
5. 「**実行**」をクリックします。

スナップショットの再作成

(ターゲットから直接ではなく) スナップショットから個々のファイルを復元する予定であり、選択した仮想マシンの復元ポイントで使用可能なスナップショットがない場合は、手動で再作成できます。

考慮事項

選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため) がある層が含まれている場合、スナップショットを再作成するためにこの層を使用することはできません。

「仮想マシン」パネルへのアクセス

ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、再作成するスナップショットがある仮想マシンをクリックします。
2. 画面の下部に表示される「詳細ビュー」で、目的の復元ポイントを選択します。

   > 注「詳細ビュー」は、仮想マシンをクリックした場合にのみ表示されます。仮想マシンの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

3. 「**スナップショットの再作成**」をクリックします。「スナップショットの再作成」ダイアログボックスが表示されます。
4. 「ストレージコンテナ」ドロップダウンメニューから、スナップショットを再作成する場所を選択します。

   > ⚠ 重要 *vSphere環境の場合* .vVolデータストアにあるディスクから個々のファイルを復元することはサポートされていないため、使用可能なVMFSまたはNFSデータストアのみが表示されます。

5. 「復元元」ドロップダウンメニューから、スナップショットの再作成に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :スナップショットの作成を最速にできます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
6. 「**再作成**」をクリックします。

HYCU仮想マシンリソースの調整

ストレージ、vCPU、またはメモリの使用率が超過になると(つまり、これらのリソースのいずれかの使用率が90%を超えると) 、「ダッシュボード」パネルの「HYCUコントローラー」ウィジェットに円で示されている値が赤になります。HYCU仮想マシンリソースを調整するには、次の手順に従います。

1. Nutanix Prismにログオンします。Prism Webコンソールの詳細については、Nutanixの資料を参照してください。
2. メニューバーで、「**ホーム**」をクリックし、「**VM**」を選択します。
3. 「**テーブル**」タブをクリックして、「VMテーブル」ビューを表示します。
4. 仮想マシンのリストから、HYCU仮想マシンを選択し、「**電源オフアクション**」をクリックして仮想マシンをシャットダウンします。

   > ⚠ 重要 仮想マシンが完全にシャットダウンされるまで待機します。

5. 「**更新**」をクリックし、「VMの更新」ダイアログボックスで、必要に応じて構成を変更し、「**保存**」をクリックします。
6. 「**電源オン**」をクリックして仮想マシンをオンにします。

第10章

ユーザーの管理

HYCUユーザー管理システムは、許可されていないユーザーが、保護されたデータにアクセスするのを防ぐためのセキュリティメカニズムを提供します。特定の権限が付与されたユーザーのみがデータ保護環境にアクセスできます。これらのユーザーは、HYCUまたはサポートされているいずれかのIDプロバイダーによって認証できます。IDプロバイダーの詳細については、"HYCUとIDプロバイダーの統合" ページ 216を参照してください。

HYCUにログオンする各ユーザーは、いずれかのHYCUグループ(インフラストラクチャグループまたはセルフサービスグループ) に属し、ユーザーロールが割り当てられている必要があります。

HYCUグループとユーザーロールの詳細については、"HYCUグループ" 下と"ユーザーロール" 次のページ を参照してください。

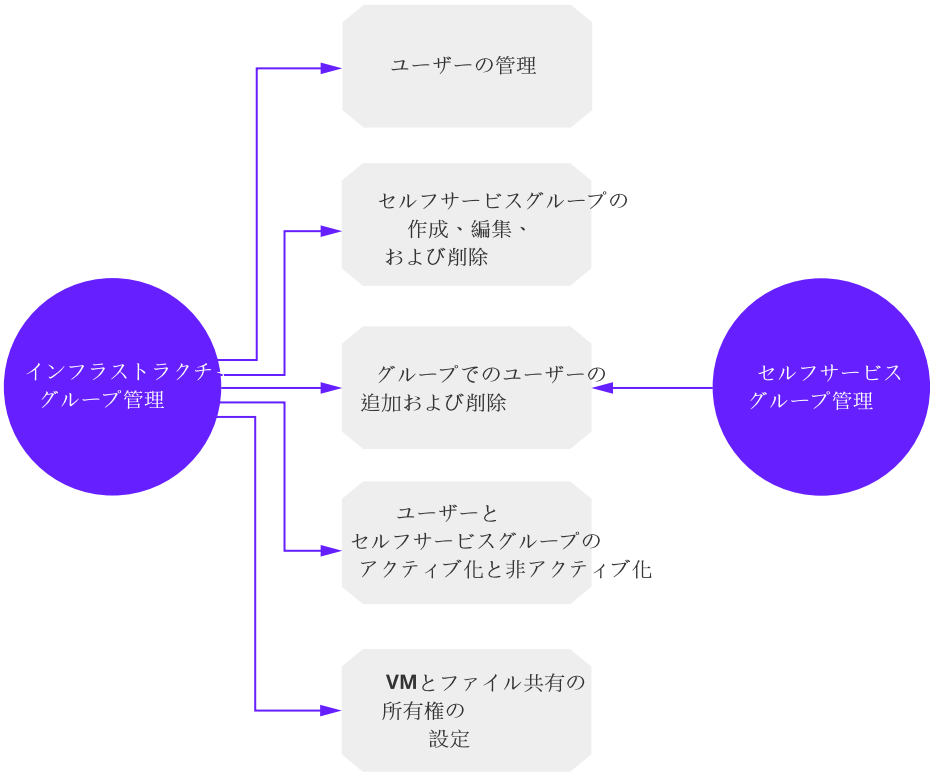
> 注 ユーザー管理の概念と手順は、仮想マシンと物理マシンの両方に適用されます。

HYCUグループ

統合されたユーザー管理エクスペリエンスのために、HYCUはユーザーが所属できる2タイプのグループを提供します。

グループ	説明
インフラストラクチャグループ	HYCU仮想アプライアンスの展開中に既定で作成され、管理者ユーザーロールが割り当てられた(🔖 で表される) 組み込みユーザーがすでに含まれています。編集、非アクティブ化、および削除はできません。 ユーザーは、インフラストラクチャグループ管理者(管理者ユーザーロールが割り当てられたインフラストラクチャグループユーザー) によってこのグループに追加できます。
セルフサービスグループ	インフラストラクチャグループ管理者が作成する必要があり、データ保護環境内の特定のエンティティセットを担当する顧客または部門を表します。 ユーザーは、インフラストラクチャグループ管理者がこのグループに追加できます。 ⚠ 重要 特定のセルフサービスグループが削除されると、そのグループによってバックアップされたすべてのデータがデータベースから削除されます。

ユーザーを管理できるのは、管理者ロールが割り当てられている場合のみ。ただし、実行できるユーザー管理アクションの範囲は、インフラストラクチャに属しているかセルフサービスグループに属しているかによって異なることに注意してください。インフラストラクチャグループ管理者は、データ保護環境全体でユーザーとグループを管理できますが、セルフサービス管理者は、所属するグループのみを管理できます。次の図は、実行できるユーザー関連アクションを示しています。



参照 :図 10-1 :インフラストラクチャおよびセルフサービスグループ管理者によって実行されるユーザー管理アクション

所属するHYCUグループと割り当てられたユーザーロールに応じて、データ保護環境内で特定のアクションのみを実行できます。ユーザーロールの詳細については、“ユーザーロール” 下を参照してください。

ユーザーロール

グループ内の各ユーザーには、ユーザーがデータ保護環境内で実行できるアクションの範囲を決定するロールが割り当てられています。つまり、データ保護環境内のデータと情報へのアクセスは、ユーザーが割り当てたロールに基づいて制限されます。ユーザーが複数のグループのメンバーである場合、ビジネス要件に応じて、そのユーザーには異なるグループ内で異なるロールを割り当てることができ、HYCUにログオンしている間にそれらのグループを切り替えることができます。

ユーザーが属するグループに応じて、ユーザーは次のアクションを実行できます。

ロール	インフラストラクチャグループ	セルフサービスグループ
管理者	• データ保護環境におけるすべての	• ポリシーを割り当てます。

ロール	インフラストラクチャグループ	セルフサービスグループ
	アクションを実行します。	• 仮想マシン、アプリケーション、ファイル共有、ボリュームグループをバックアップおよび復元します。 • バックアップの有効期限を切ります。 • 「VMバックアップを検証」オプションを使用して、仮想マシンのバックアップ検証を実行します。 • 検証ポリシーを割り当て/割り当て解除します。 • グループでユーザーを追加および削除します。 • すべてのレポート管理アクションを実行します。 • クラウドアカウントを追加、編集、および削除します。
ビューアー	• データ保護環境内のアプリケーション、仮想マシン、ファイル共有、ボリュームグループ、ポリシー、ターゲット、ジョブ、イベント、ユーザー、生成されたレポートバージョン、および「⚙ 管理」メニューから利用できる設定に関する情報を表示します。	• データ保護環境内のアプリケーション、仮想マシン、ファイル共有、ボリュームグループ、ポリシー、ジョブ、イベント、および生成されたレポートバージョンに関する情報を表示します。
バックアップオペレーター	• ビューアーと同じ情報を表示します。 • バックアップ戦略を定義します。 • セルフサービスグループが所有していない仮想マシン、ファイル共有、ボリュームグループをバックアップし、アプリケーションをバックアップします。	• ビューアーと同じ情報を表示します。 • ポリシーを割り当てます。 • 仮想マシン、アプリケーション、ファイル共有、ボリュームグループをバックアップします。
復元オペレーター	• ビューアーと同じ情報を表示します。 • セルフサービスグループが所有していない仮想マシン、ファイル共有、ボリュームグループを復元し、	• ビューアーと同じ情報を表示します。 • 仮想マシン、アプリケーション、ファイル共有、ボリュームグループを復元します。

ロール	インフラストラクチャグループ	セルフサービスグループ
	アプリケーションを復元します。 • 「VMバックアップを検証」オプションを使用して、仮想マシンのバックアップ検証を実行します。 • 検証ポリシーを割り当て/割り当て解除します。	• 「VMバックアップを検証」オプションを使用して、仮想マシンのバックアップ検証を実行します。 • 検証ポリシーを割り当て/割り当て解除します。
バックアップおよび復元オペレーター	• ビューアーと同じ情報を表示します。 • バックアップ戦略を定義します。 • セルフサービスグループが所有していない仮想マシン、ファイル共有、ボリュームグループをバックアップおよび復元し、アプリケーションをバックアップおよび復元します。 • 「VMバックアップを検証」オプションを使用して、仮想マシンのバックアップ検証を実行します。 • 検証ポリシーを割り当て/割り当て解除します。	• ビューアーと同じ情報を表示します。 • ポリシーを割り当てます。 • 仮想マシン、アプリケーション、ファイル共有、ボリュームグループをバックアップおよび復元します。 • 「VMバックアップを検証」オプションを使用して、仮想マシンのバックアップ検証を実行します。 • 検証ポリシーを割り当て/割り当て解除します。

ユーザー環境のセットアップ

ユーザーがHYCUを使用してデータ保護を開始する前に、データ保護環境内のデータにアクセスする権限をユーザーに付与する必要があります。ユーザーを作成し、ユーザーをグループに追加することで、ユーザーは定義されたデータ保護環境のみにアクセスし、割り当てられたロールで指定された一連のアクションを実行できるようになります。

タスク	実行者...	説明
1. 新しいユーザーを作成します。	インフラストラクチャグループ管理者	“ユーザーの作成” 次のページ
2. ユーザーをユーザーグループに追加します。	インフラストラクチャまたはセルフサービスグループの管理者	“ユーザーのグループへの追加” ページ203

ユーザー環境のセットアップ中に、次のタスクの1つ以上を実行することにより、ユーザーの要件に合わせて環境を調整できます。

タスク	実行者...	説明
新しいセルフサービスグループを	インフラストラクチャグループ管	“セルフサービスグループの作成”

タスク	実行者...	説明
作成します。	理者	ページ204
仮想マシン、ファイル共有、ボリュームグループの所有権を設定します。	インフラストラクチャグループ管理者	"所有権の設定" ページ205
特定のグループまたはユーザーのHYCUへのログオンを有効または無効にします。	インフラストラクチャグループ管理者	"ユーザーまたはセルフサービスグループのアクティブ化または非アクティブ化" ページ207

「セルフサービス」パネルへのアクセス

「セルフサービス」パネルにアクセスするには、ナビゲーションペインで、「**セルフサービス**」をクリックします。

ユーザーの作成

前提条件

- *2要素認証を使用する場合* :適切な認証システムをセットアップする必要があります。認証方式に応じて、次のものを使用します。
  - 時間ベースのワンタイムパスワード(OTP) 認証アプリケーション(スマートフォンのGoogle認証システム) 。
  - ハードウェアキーや指紋リーダーなどの、FIDO互換認証システム。
- *HYCUをIDプロバイダーと統合する場合* :IDプロバイダー環境では、IDプロバイダーを使用してHYCUにサインインできるようにするユーザーに対して、HYCUをアプリケーションとして割り当てる必要があります。HYCUとIDプロバイダーを統合する方法の詳細な説明については、"HYCUとIDプロバイダーの統合" ページ216を参照してください。

制限事項

Active Directoryプライマリグループ(通常はドメインユーザーグループ) をADグループとして追加することはできません。

考慮事項

Active Directoryグループのメンバーが個別のユーザーとしてリストされ、それぞれに2要素認証を有効にしたり、優先言語を設定したりできます。

手順

1. 「セルフサービス」パネルで、「**ユーザーの管理**」をクリックし、「**＋新規**」をクリックします。
2. HYCUユーザー、ADユーザー、またはIDプロバイダーユーザーを追加する場合は、ユーザー名を入力します。ADグループを追加する場合は、一般名を入力します。

> ⚠ 重要 名前を入力するときは、SAMアカウント名の制限に準拠するようにします。名前の長さは20文字を超えてはならず、次の文字を含めることができます。"/ \ [ ] : ; | = , + * ? < >
> さらに、HYCUは名前にアットマーク(@) を使用できません。
>
> 環境で必要な場合は、`ad.username.filter.regex`構成設定を編集することでこれらの制限を上書きできます。ただし、これはサポートされず、認証の問題を引き起こす可能性があります。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。

3. 「認証タイプ」ドロップダウンメニューから、以下のいずれかの認証タイプを選択し、説明に従います。

認証タイプ	説明
HYCU	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「名前」フィールドで、ユーザーの表示名を入力します。 c. *オプション*:「Eメール」フィールドには、ユーザーの電子メールアドレスを入力します。 d. 「パスワード」フィールドで、ユーザーパスワードを入力します。 > 注 最小パスワード長は6文字です。
ADユーザー	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「IDプロバイダー」ドロップダウンメニューから、ADユーザーが属するActive Directoryを選択します。
ADグループ	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「IDプロバイダー」ドロップダウンメニューから、ADグループが属するActive Directoryを選択します。
IDプロバイダーユーザー	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「IDプロバイダー」ドロップダウンメニューから、IDプロバイダーを選択します。 c. 「IDプロバイダーのユーザーID」フィールドに、IDプロバイダーのユーザーIDを入力します。 > 注 IDプロバイダーに応じて、ユーザーIDは以下のように対応します。 • *Google* :ユーザーの電子メールアドレス • *Microsoft* :オブジェクトID • *Okta* :ユーザーのプロファイルに移動するときのURLの

認証タイプ	説明
	一部 詳細については、それぞれのIDプロバイダーの資料を参照してください。

4. *HYCUユーザー、ADユーザー、またはADグループを追加する場合のみ。*ユーザーに対して2要素認証を有効にする場合は、「**2要素認証の有効化**」スイッチを使用し、次の2要素認証方式のいずれかを選択します。

   - **時間ベースのワンタイムパスワード**

     このオプションを使用すると、OTPアプリケーションによって生成された時間ベースのワンタイムパスワード(OTP) を使用できます。2要素認証が有効になった後の最初のログオン時に、ユーザーがOTPをセットアップする必要があります。

   - **FIDO**

     このオプションを選択すると、FIDOプロトコル(FIDO認証システム) に準拠する認証システムを使用できます。ユーザーはFIDO認証システムを登録する必要があります。詳細については、"FIDO認証システムの管理" ページ264を参照してください。

5. *2要素認証を有効にした場合のみ。*ユーザーが2要素認証を無効にできないようにするには、必ず「**ユーザーは2要素認証を無効にできません**」チェックボックスを選択します。このチェックボックスをクリアすると、2要素認証を無効にできます。管理者ロールが設定され、インフラストラクチャグループに属しているユーザーは、このオプションが設定されていても、2要素認証を無効できます。

   > 注 ユーザーが2要素認証を無効にした場合、管理者にはセキュリティ警告が通知されます。

6. 「**保存**」をクリックし、「**閉じる**」をクリックします。ユーザーはすべてのユーザーのリストに追加されます。

後で以下を実行できます。

- 「**編集**」をクリックして必要な変更を加えることで、既存のHYCUまたはIDプロバイダーのユーザーを編集します。組み込みユーザー、ADユーザー、およびADグループは編集できないことに注意してください。
- 特定のユーザーのHYCUへのログオンを有効または無効にします。詳細については、"ユーザーのアクティブ化または非アクティブ化" ページ207を参照してください。
- 「**削除**」をクリックして、既存のユーザーのいずれかを削除します。組み込みユーザーは削除できないことに注意してください。

ユーザーのグループへの追加

前提条件

*ユーザーをセルフサービスグループに追加する場合のみ。*セルフサービスグループが作成されている。この実行方法の詳細については、"セルフサービスグループの作成" 次のページを参照してください。

考慮事項

- ユーザーを複数のグループに追加して、そのグループ内でユーザーに異なるユーザーロールを割り当てることができます。ユーザーロールの詳細については、"ユーザーロール" ページ198を参照してください。
- ADユーザーが複数のADグループのメンバーシップに基づいて複数のユーザーロールを割り当てられている場合、ユーザーは最高の特権レベルを持つロールを取得します。ユーザーロールの優先順位は、管理者 > バックアップおよび復元オペレーター > 復元オペレーター > バックアップオペレーター > ビューアーとなっています。ただし、ADグループとは無関係にADユーザーに割り当てられたロールは、ADグループ内のロールよりも常に優先されることに注意してください。

手順

1. 「セルフサービス」パネルの「詳細ビュー」で、ユーザーを追加するグループを選択します。
2. 「**＋グループに追加**」をクリックします。「グループにユーザーを追加」ダイアログボックスが開きます。

   > 注 既定で作成されるインフラストラクチャグループ、または自分で作成する必要があるセルフサービスグループにユーザーを追加できます。

3. 「ユーザー名」フィールドで、ユーザー名を入力します。

   > ⚠ 重要 *ADユーザーおよびADグループの場合*：ユーザー名を、*user@domain*または*domain\name*のいずれかの形式で入力します。

4. 「ユーザーロール」ドロップダウンメニューから、ユーザーに割り当てるロール(「**管理者**」、「**バックアップと復元オペレーター**」、「**復元オペレーター**」、「**バックアップオペレーター**」、または「**閲覧者**」)を選択します。
5. 「**ユーザーを追加**」をクリックします。

特定のデータ保護環境のニーズに応じて、いつでもグループからユーザーを削除できます。これは、削除するユーザーを選択し、「**ー グループから削除**」をクリックして行うことができます。

セルフサービスグループの作成

手順

1. 「セルフサービス」パネルで、「**＋新しいグループ**」をクリックします。「新しいグループ」ダイアログボックスが開きます。
2. セルフサービスグループ名とその説明(オプション)を入力します。
3. 「**保存**」をクリックします。

後で以下を実行できます。

- ユーザーをグループに追加します。詳細については、"ユーザーのグループへの追加" 前のページを参照してください。
- 「**編集**」をクリックして必要な変更を加えることで、既存のセルフサービスグループを編集します。

- 特定のセルフサービスグループに属するユーザーが、グループ名とアンダースコアで始まる名前を持つポリシー(たとえば、HYCUGroup_Policy1)、およびExcludeポリシー(既にユーザーが所有者となっている仮想マシン、ファイル共有、ボリュームグループに割り当てられている他のポリシーと同様)のみを表示できるようにします。これを実行するには、HYCU `config.properties`ファイルで、`policies.group.specific.synchronized`構成設定を`true`に設定します。そのようなポリシーは、エンティティに割り当てられていない場合にのみ編集または削除できることに注意してください。HYCU構成設定のカスタマイズ方法の詳細については、"HYCU構成設定のカスタマイズ" ページ308を参照してください。
- 特定のセルフサービスグループのHYCUへのログオンを有効または無効にします。詳細については、"セルフサービスグループのアクティブ化または非アクティブ化" ページ207を参照してください。
- 「**削除**」をクリックして、既存のセルフサービスグループのいずれかを削除します。

所有権の設定

仮想マシン、ファイル共有、ボリュームグループの所有権を設定することにより、特定のグループが、割り当てられた仮想マシン、ファイル共有、ボリュームグループのみを保護できるようにします。所有者を割り当てるエンティティに応じて、次のいずれかのセクションを参照してください。

- "仮想マシンの所有権の設定" 下
- "ファイル共有の所有権の設定" 次のページ
- "ボリュームグループの所有権の設定" 次のページ

仮想マシンの所有権の設定

考慮事項

仮想マシンの所有権を変更する際、特定の所有者により保護されているデータを維持するか削除するかのどちらかを選択することができます。特定の所有者により保護されているデータを維持するよう選択した場合、その仮想マシンはHYCU内に「PROTECTED_DELETED」ステータスで維持されます。このような仮想マシンを「VMの復元」オプションで復元することは可能ですが、復元を実行する前に仮想マシンをソースから削除しておく必要があります。

> 「仮想マシン」パネルへのアクセス
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、所有者を割り当てる仮想マシンを選択し、「**所有者**」をクリックします。
2. グループのリストから、選択した仮想マシンの所有者として割り当てるグループを選択し、「**割り当て**」をクリックします。

> ⚠ 重要 仮想マシンまたはアプリケーションのバックアップジョブまたは復元ジョブが進行中の場合、またはスケジュールされたバックアップタスクがキュー内にある場合、関連する仮想マシンに新しいグループを割り当てることはできません。

特定のデータ保護環境の要件に応じて、いつでも仮想マシンから所有者を削除できます。これは、対象の仮想マシンを選択し、「**所有者**」をクリックして、次に「**割り当て解除**」をクリックして行います。

ファイル共有の所有権の設定

考慮事項

ファイル共有の所有権を変更する際、特定の所有者により保護されているデータを維持するか削除するかのどちらかを選択することができます。特定の所有者により保護されているデータを維持するよう選択した場合、そのファイル共有はHYCU内に「PROTECTED_DELETED」ステータスで維持されます。

> 「共有フォルダ」パネルへのアクセス
>
> 「共有フォルダ」パネルにアクセスするには、ナビゲーションペインで、「**共有フォルダ**」をクリックします。

手順

1. 「共有フォルダ」パネルで、所有者を割り当てるファイル共有を選択し、「**所有者**」をクリックします。
2. グループのリストから、選択したファイル共有の所有者として割り当てるグループを選択し、「**割り当て**」をクリックします。

   > ⚠ 重要 ファイル共有のバックアップジョブまたは復元ジョブがすでに進行中の場合、またはスケジュールされたバックアップタスクがキュー内にある場合、このファイル共有に新しいグループを割り当てることはできません。

特定のデータ保護環境のニーズに応じて、いつでもファイル共有から所有者を削除できます。これは、所有者を削除するファイル共有を選択し、「**所有者**」をクリックし、次に「**割り当て解除**」をクリックして行うことができます。

ボリュームグループの所有権の設定

考慮事項

ボリュームグループの所有権を変更する際、特定の所有者により保護されているデータを維持するか削除するかのどちらかを選択することができます。特定の所有者により保護されているデータを維持するよう選択した場合、そのボリュームグループはHYCU内に「PROTECTED_DELETED」ステータスで維持されます。

> 「ボリュームグループ」パネルのアクセス
>
> 「ボリュームグループ」パネルにアクセスするには、ナビゲーションペインで、「**ボリュームグループ**」をクリックします。

手順

1. 「ボリュームグループ」パネルで、所有者を割り当てるボリュームグループを選択し、「**所有者**」をクリックします。

2. グループのリストから、選択したボリュームグループの所有者として割り当てるグループを選択し、「**割り当て**」をクリックします。

> ⚠ 重要 ボリュームグループのバックアップジョブまたは復元ジョブがすでに進行中の場合、またはスケジュールされたバックアップタスクがキュー内にある場合、このボリュームグループに新しいグループを割り当てることはできません。

特定のデータ保護環境のニーズに応じて、いつでもボリュームグループから所有者を削除できます。これは、所有者を削除するボリュームグループを選択し、「**所有者**」をクリックし、次に「**割り当て解除**」をクリックして行うことができます。

ユーザーまたはセルフサービスグループのアクティブ化または非アクティブ化

ビジネスの性質に応じて、特定のユーザーまたはセルフサービスグループをアクティブ化または非アクティブ化することで、HYCUにログオンすることをいつでも有効または無効にできます。セルフサービスグループをアクティブまたは非アクティブにすることにより、特定のセルフサービスグループに属するすべてのユーザーがそのグループのメンバーとしてHYCUにログオンすることを有効または無効にできます。

ユーザーのアクティブ化または非アクティブ化

手順

1. 「セルフサービス」パネルで、「**ユーザーの管理**」をクリックします。
2. すべてのユーザーのリストから、ステータスを変更するユーザーを選択します。
3. ユーザーのステータスに応じて、以下のいずれかを実行します。
   - 選択したユーザーのステータスが非アクティブであり、それをアクティブにしたい場合には、「**アクティブ化**」をクリックします。
   - 選択したユーザーのステータスが「アクティブ」であり、それを非アクティブにする場合には、「**非アクティブ化**」をクリックします。

セルフサービスグループのアクティブ化または非アクティブ化

手順

1. 「セルフサービス」パネルで、セルフサービスグループのリストから、ステータスを変更するものを選択します。
2. セルフサービスグループのステータスに応じて、以下のいずれかを実行します。
   - 選択したセルフサービスグループのステータスが「非アクティブ」であり、それをアクティブにする場合には、「**アクティブ化**」をクリックします。
   - 選択したセルフサービスグループのステータスが「アクティブ」であり、それを非アクティブにする場合には、「**非アクティブ化**」をクリックします。

> 注 ユーザーが複数のセルフサービスグループのメンバーであり、これらのグループの少なくとも1つが「Active」ステータスになっている場合、ユーザーはそれに自動的に切り替えられます。ユー

> ザーが属する「アクティブ」ステータスのグループが複数ある場合、ユーザーは最初に作成されたグループに自動的に切り替えられます。

別のグループへの切り替え

ユーザーとして、1つ以上のグループに属し、所属するグループに関連付けられているすべての権限でHYCUにログオンできます。複数のグループのメンバーである場合には、HYCUにログオンしているときにいつでも別のグループに切り替えることができます(そのステータスが「アクティブ」である場合)。これは、所属するグループのいずれかを選択して、セッションで使用できることを意味します。

手順

1. 画面の右上にある、現在そこからHYCUにログオンしているグループをクリックします。

   参照 :図 10–1 :例として、セルフサービスグループHYCU_groupの下のユーザーHYCU_group_memberがHYCUにログオンします。

2. 所属するすべてのグループのリストから、切り替えたいグループを選択します。

   > ヒント 現在そこからHYCUにログオンしているグループには、その横に「✔」が付きます。

3. 「**切り替え**」をクリックします。

選択したグループに自動的に切り替わります。

ユーザープロファイルの更新

現在ログオンしているユーザーは、自分の名前、メールアドレス、使用する言語、認証設定を、「プロファイルの更新」オプションで設定できます。

考慮事項

管理者ロールが割り当てられているユーザーは、別のユーザーの情報を「セルフサービス」パネルで編集できます。詳細については、“ユーザーの作成” ページ201を参照してください。

> 「プロファイルの更新」ダイアログボックスへのアクセス
>
> 「プロファイルの更新」ダイアログボックスにアクセスするには、画面右上の「👤」をクリックし、「**プロファイルの更新**」を選択します。

手順

1. 「名前」フィールドで、新しい名前を指定します。
2. 「Eメール」フィールドで、自分のユーザープロファイルと関連付けるメールアドレスを入力します。
3. 「言語」ドロップダウンメニューから、使用する言語を選択します。
4. *オプション*。「**2要素認証の有効化**」を選択して、2要素認証を有効にします。2要素認証方式を選択します。

- **時間ベースのワンタイムパスワード**

  このオプションを使用すると、OTPアプリケーションによって生成された時間ベースのワンタイムパスワード(OTP) を使用できます。

- **FIDO**

  このオプションを選択すると、FIDOプロトコル(FIDO認証システム) に準拠する認証システムを使用できます。

5. 「**保存**」をクリックします。
6. *2要素認証を有効にした場合のみ*。2要素認証の初期セットアップを実行します。
   - *時間ベースのワンタイムパスワードの場合* :「2要素認証の設定」ダイアログボックスが表示されます。以下を実行します。
     a. 適切なOTPアプリケーション(スマートフォンのGoogle Authenticatorなど) で、QRコードを読み取るか、またはOTPバックアップコードを手動で入力します。
     b. 「認証符号」フィールドに、生成された6桁のコードを入力し、「**確認**」をクリックしてセットアッププロセスを完了します。

     > 注 ワンタイムパスワードをセットアップしない場合、次回のログオン時に「2要素認証の設定」ダイアログボックスが表示されます。

   - *FIDOの場合*:「FIDO認証システム」ダイアログボックスが表示されます。以下を実行します。
     a. ウィザードに従って、認証システム(セキュリティキーや指紋リーダー付きWindows Helloなど) を登録します。プロセスは、選択した認証システムのタイプとオペレーティングシステムのバージョンによって異なります。
     b. 認証システムの名前を入力し、「**登録**」をクリックします。

     > 注 少なくとも1つの認証システムの登録が完了していない場合、2要素認証を有効にした後の最初のログオン時に、認証システムを登録することが求められます。
     >
     > 後で認証システムを追加したり、既存の認証システムを取り消したりすることもできます。詳細については、“FIDO認証システムの管理” ページ264を参照してください。

第11章

管理

HYCUをデプロイしたら、「⚙ **管理**」メニューでさまざまな管理タスクを実行して、データ保護環境向けにHYCUをカスタマイズできます。

目的	手順
クラウドアカウントをHYCUに追加します。	“クラウドアカウントの追加” 次のページ
ターゲットの暗号化を構成します。	“ターゲット暗号化の構成” ページ215
HYCUをIDプロバイダーと統合します。	“HYCUとIDプロバイダーの統合” ページ216
HYCUインスタンスを管理します。	“HYCUインスタンスの管理” ページ220
iSCSIイニシエーターシークレットを設定します。	“iSCSIイニシエーターシークレットの設定” ページ222
恒久HYCUライセンスを取得します。	“ライセンス” ページ222
HYCUが予期したとおりに実行しない場合、問題をトラブルシューティングするためにログファイル設定を構成します。	“ログのセットアップ” ページ226
ネットワーク設定を変更するか、ネットワーク帯域幅の調整を有効にします。	“ネットワークの構成” ページ228
電源オプションを設定します。	“電源オプションの設定” ページ231
Conjurシークレット管理ソリューションを採用することで、資格情報(シークレット)を安全に保管、アクセス、管理できます。	“シークレットの管理” ページ231
SMTPサーバーを構成します。	“SMTPサーバーの構成” ページ233
HYCUを利用可能な新しいバージョンにアップグレードします。	“HYCUのアップグレード” ページ238
HYCU修正プログラムを適用します。	“HYCU修正プログラムの適用” ページ248
SSL証明書を構成します。	“SSL証明書の構成” ページ234
HYCUとテレメトリ診断データを共有します。	“HYCUとのテレメトリデータの共有” ページ237

何らかの理由で、データの保護にHYCUを使用する必要がなくなったと判断した場合には、システムから簡単に削除できます。詳細については、“HYCUの削除” ページ254を参照してください。

クラウドアカウントの追加

次のいずれかのデータ保護タスクを実行する前に、1つ以上のクラウドアカウントをHYCUに追加する必要があります。

- Google Cloudターゲットへのデータの保存。
- HYCUで保護されたデータのオンプレミス環境からクラウドへの移行。
- HYCU Data Protection as a Service for Google Cloud(HYCU for Google Cloud) またはHYCU Data Protection as a Service for Azure(HYCU for Azure) で保護されたデータのクラウドからオンプレミス環境への移行。
- 災害発生時のデータのクラウドへの災害復旧実行。
- HYCU ManagerでのHYCU for Google CloudおよびHYCU for Azureデータ保護環境の監視。

考慮事項

異なるインフラストラクチャ間での仮想マシンの移行、クラウドへのデータの災害復旧の実行、およびクラウドデータ保護環境の監視は、HYCU Protégéライセンスを所有している場合にのみサポートされます。

どのデータ保護タスクを実行するかに応じて、1つ以上のクラウドアカウントをHYCUに追加します。

目的	クラウドアカウント	説明
• Google Cloudターゲットにデータを保存します。 • HYCUで保護されたデータをGoogle Cloudに移行します。 • HYCU for Google Cloudで保護されたデータをオンプレミス環境に移行します。 • Google Cloudへの災害復旧を実行します。 • HYCU ManagerのHYCU for Google Cloudデータ保護環境を監視します。	Google Cloudサービスアカウント	“Google Cloudサービスアカウントの追加” 次のページ
• HYCUで保護されたデータをAzureに移行します。 • HYCU for Azureで保護されたデータをオンプレミス環境に移行します。 • Azureへのデータの災害復旧を実行します。 • HYCU ManagerのHYCU for Azureデータ	Azureサービスプリンシパル	“Azureサービスプリンシパルの追加” ページ213

目的	クラウドアカウント	説明
保護環境を監視します。		
• HYCUで保護されたデータをAzure US Governmentに移行します。 • Azure US Governmentへの災害復旧を実行します。	Azure US Governmentサービスプリンシパル	“Azure US Governmentサービスプリンシパルの追加” ページ215

Google Cloudサービスアカウントの追加

HYCUに追加するGoogle Cloudサービスアカウントのタイプは、実行するデータ保護タスクによって異なります。

> ⚠ 重要 HYCUには、必ず自分で作成した専用のサービスアカウントを追加する必要があります。

目的	追加するサービスアカウント
Google Cloudターゲットにデータを保存します。	バックアップデータを保存するバケットにアクセスできるアカウント。
HYCU for Google Cloudで保護されたデータをGoogle Cloudからオンプレミス環境に移行します。	HYCU for Google Cloudにインポートされ、インスタンスを含むプロジェクトにストレージ管理者の役割が割り当てられているアカウント。
HYCUで保護されたデータをオンプレミス環境からGoogle Cloudに移行します。	HYCU for Google Cloudにインポートされ、仮想マシンを移行するプロジェクトに割り当てられたストレージ管理者およびコンピューティング管理者のロールを持つアカウント。
災害発生時に、Google Cloudへのデータの災害復旧を実行します。	HYCU for Google Cloudにインポートされ、障害復旧を実行するプロジェクトでストレージ管理者およびコンピューティング管理者のロールが割り当てられているアカウント。
HYCU ManagerのHYCU for Google Cloudデータ保護環境を監視します。	HYCU Managerで監視する保護セットにアクセスする許可を持つアカウント。

前提条件

- サービスアカウントがGoogle Cloudで構成済みである。
- 次のAPIは、サービスアカウントが作成されたGoogle Cloudプロジェクトで有効になっている。
  - Cloud Resource Manager API
  - Compute Engine API
  - Cloud Storage API
  - Identity and Access Management API

  これらを有効にする方法の説明については、Google Cloudの資料を参照してください。

- サービスアカウントにはGoogle Cloudのロールが付与されており、それには保護されたインスタンスプロジェクトに対するコンピューティング管理者(ロール/compute.admin)、ストレージ管理者(ロール/storage.admin)、およびサービスアカウントユーザー(ロール/iam.serviceAccountUser)があります。
- サービスアカウント情報(その秘密鍵を含む)を保存する有効なJSONファイルにアクセス可能である。

> 「クラウドアカウント」ダイアログボックスへのアクセス
>
> 「クラウドアカウント」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**クラウドアカウント**」を選択します。

手順

1. 「クラウドアカウント」ダイアログボックスで、「＋ **新規**」をクリックします。「クラウドを選択」ダイアログボックスが表示されます。
2. 「**GCPサービスアカウントの追加**」を選択し、「**次へ**」をクリックします。「Google Cloud認証」ダイアログボックスが開きます。
3. サービスアカウント情報を含むJSONファイルを参照します。「サービスアカウント認証」フィールドに、ファイル名が表示されます。

   > 注 *セルフサービスのグループ管理者としてHYCUにログオンしている場合のみ*。Conjurを使用してHYCUのシークレットを管理する場合、ファイルを参照する代わりにシークレットを提供するのであれば、「**シークレットマネージャーから値を取得**」を有効にすることができます。シークレットの管理の詳細については、"シークレットの管理" ページ231を参照してください。
4. 「名前」フィールドで、アカウントサービス名を変更できます。
5. 「**アップロード**」をクリックします。

   サービスアカウントのアップロードが成功したことが通知されると、その名前が「クラウドアカウント」ダイアログに表示されます。
6. 「**閉じる**」をクリックします。

既存のクラウドアカウントはいずれも後から編集することができます(「✎ **編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「🗑 **削除**」をクリックします)。次の場合には、クラウドアカウントを削除できないことに注意してください。

- Google Cloudターゲットがこのアカウントを使用する。
- HYCU Managerで監視される保護セットがこのアカウントを使用する。

Azureサービスプリンシパルの追加

前提条件

サービスプリンシパルはAzureで作成し、HYCU for Azureに追加する必要があります。詳細については、HYCU for Azureの資料を参照してください。

> ⚠ 重要 必ず自分で作成した専用のサービスプリンシパルをHYCUに追加し、サービスの利用開始時にHYCU for Azureが自動的に作成される既定のプリンシパルは使用しないようにする必

> 要があります。

サービスプリンシパルに割り当てる必要があるロールは、実行するデータ保護タスクによって異なります。

目的	必要なロール
HYCU for Azureで保護されたデータをAzure環境からオンプレミス環境に移行します。	• サブスクリプションレベルで割り当てられたコントリビューターロール • サブスクリプション、リソースグループ、またはストレージアカウントレベルで割り当てられたストレージBlobデータコントリビューターロール
HYCUで保護されたデータをオンプレミス環境からAzureに移行します。	
災害発生時に、Azureへのデータの災害復旧を実行します。	
HYCU ManagerのHYCU for Azureデータ保護環境を監視します。	• サブスクリプションレベルで割り当てられたコントリビューターロール

> 「クラウドアカウント」ダイアログボックスへのアクセス
>
> 「クラウドアカウント」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**クラウドアカウント**」を選択します。

手順

1. 「クラウドアカウント」ダイアログボックスで、「＋ **新規**」をクリックします。「クラウドを選択」ダイアログボックスが表示されます。
2. 「**Azureサービスプリンシパルの追加**」を選択し、「**次へ**」をクリックします。「Azure認証」ダイアログボックスが表示されます。
3. 「名前」フィールドで、サービスプリンシパルの名前を入力します。
4. 「テナントID」フィールドで、テナントIDを入力します。
5. 「アプリケーションID」フィールドに、Azure Active Directoryでのアプリケーションの(HYCU for Azure) 登録のIDを入力します。
6. 「秘密鍵」フィールドに、アプリケーションIDに関連付けられているシークレットを入力します。
7. 「**保存**」をクリックします。

既存のサービスプリンシパルはいずれも後から編集できます(「✎ **編集**」をクリックして必要な変更を行います) 。または不要になったものは削除できます(「🗑 **削除**」をクリックします) 。HYCU Managerで監視されている保護セットがこのアカウントを使用している場合は、サービスプリンシパルを削除できないことに注意してください。

Azure US Governmentサービスプリンシパルの追加

前提条件

- サービスプリンシパルは、Azure US Governmentで作成する必要があります。
- サービスプリンシパルには、サブスクリプションレベルでコントリビューターロールを割り当てる必要があります。

> 「クラウドアカウント」ダイアログボックスへのアクセス
>
> 「クラウドアカウント」ダイアログボックスにアクセスするには、「⚙**管理**」をクリックし、「**クラウドアカウント**」を選択します。

手順

1. 「クラウドアカウント」ダイアログボックスで、「＋**新規**」をクリックします。「クラウドを選択」ダイアログボックスが表示されます。
2. 「**Azure US Governmentサービスプリンシパルの追加**」を選択し、「**次へ**」をクリックします。「Azure US Government認証」ダイアログボックスが表示されます。
3. 「名前」フィールドで、サービスプリンシパルの名前を入力します。
4. 「テナントID」フィールドで、テナントIDを入力します。
5. 「アプリケーションID」フィールドに、Azure Active DirectoryでのアプリケーションのHYCU登録のIDを入力します。
6. 「秘密鍵」フィールドに、アプリケーションIDに関連付けられているシークレットを入力します。
7. 「**保存**」をクリックします。

既存のサービスプリンシパルはいずれも後から編集できます(「✎ **編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「🗑 **削除**」をクリックします)。

ターゲット暗号化の構成

ターゲットのセットアップにターゲットの暗号化を有効にした場合、使用されるアルゴリズムに関する情報の表示、暗号化されたターゲットのリストの表示、暗号化キーのファイルへのエクスポート、および暗号化キーのインポートを行うことができます。

> 「暗号化」ダイアログボックスへのアクセス
>
> 「暗号化」ダイアログボックスにアクセスするには、「⚙**管理**」をクリックし、「**暗号化**」を選択します。

暗号化キーのエクスポート

手順

1. 「暗号化」ダイアログボックスで、「**エクスポート**」をクリックします。
2. エクスポートしたファイルを安全な場所に保存します。

暗号化キーのインポート

手順

1. 「暗号化」ダイアログボックスで、「**インポート**」をクリックします。
2. 「インポート」ダイアログボックスで、暗号化キーを含むファイルを参照し、「**インポート**」をクリックします。

暗号化キーが正常にインポートされたことが通知されます。

HYCUとIDプロバイダーの統合

HYCUをActive Directory IDプロバイダー、およびGoogle、Microsoft、OktaなどのOpenID Connect認証プロトコルをサポートするIDプロバイダーと統合すると、それらのIDプロバイダーを利用してHYCUに安全にサインインできるようになり、HYCU専用の資格情報を維持する必要がなくなります。

HYCUをIDプロバイダーと統合する場合、次のタスクを実行する必要があります。

タスク	説明
1. IDプロバイダーをHYCUに追加して、ユーザーを認証できるようにします。	"IDプロバイダーのHYCUへの追加" 下に説明されている手順に従います。
2. IDプロバイダーを使用してサインインできるユーザーを作成し、そのユーザーをユーザーグループに追加します。	"ユーザーの作成" ページ201と"ユーザーのグループへの追加" ページ203に説明されている手順に従います。

IDプロバイダーのHYCUへの追加

前提条件

- *OpenID Connect認証プロトコルをサポートするIDプロバイダーを追加する場合のみ*。HYCUに追加する予定のIDプロバイダー内で、HYCUがWebアプリケーションとして登録されている必要があります。HYCUを登録する場合は、次が実行済みであることを確認してください。
  - *MicrosoftをIDプロバイダーとして使用している場合のみ*。Azureでは、HYCUに、次のAzure APIへのアクセス権限を付与する必要があります。User.Readに対する権限を委譲されたMicrosoft Graph。
  - *OktaをIDプロバイダーとして使用している場合のみ*。Oktaでは、付与のタイプとして、ユーザーの代わりに行動するクライアントの下で**承認コード**を選択する必要があります。

  アプリケーションの登録方法については、それぞれのIDプロバイダーの資料を参照してください。
- *Active DirectoryでLDAPSを使用することを予定している場合のみ*。LDAPS認証がセットアップされます。詳細については、"LDAPS認証のセットアップ" ページ262を参照してください。

考慮事項

- ユーザーアカウントのセキュリティをさらに高めるために、IDプロバイダー内に多要素認証を構成することもできます。この方法については、それぞれのIDプロバイダーの資料を参照してください。
- HYCUの認証ソースとしてActive Directoryを使用する場合、証明書認証を有効にして、ユーザーがクライアント証明書またはスマートカードでHYCU Webユーザーインターフェースにログオンできるようにすることも可能です。説明については、"証明書認証の有効化" ページ219を参照してください。

> 「IDプロバイダー」ダイアログボックスへのアクセス
>
> 「IDプロバイダー」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**IDプロバイダー**」を選択します。

手順

1. 「IDプロバイダー」ダイアログボックスで、「＋ **新規**」をクリックします。新しいダイアログボックスが開きます。
2. IDプロバイダーの名前を入力します。
3. 「タイプ」ドロップダウンメニューから、次のいずれかのIDプロバイダーのタイプを選択して、説明に従います。

IDプロバイダーのタイプ	説明
Active Directory	a. 「ドメイン」フィールドで、Active DirectoryのFQDNまたはドメインエイリアス名を入力します。ADグループの使用を予定している場合、FQDNの入力は必須です。 たとえば、`mycompany.com`をFQDNとして、`mc`をエイリアスドメイン名として入力する場合、ユーザーはHYCUに`<Username>@mycompany.com`または`mc\<Username>`でログオンできます。 > 注 複数のFQDNまたはドメインエイリアス名を入力できます。この場合には、それぞれを入力してからスペースバーを押します。 b. 「プロバイダーURL」フィールドに、対応するLDAPサーバーのURLを以下のいずれかの形式で入力します。 • `ldap://<LDAPServerHostnameorIPAddress>:<Port>` LDAPプロトコルを使用する場合、既定のポートは389です。既定値を使用する場合、ポートの入力はオプションです。 • *LDAPS認証がセットアップされている場合のみ。* `ldaps://<LDAPServerHostname>:<Port>` > ⚠ 重要 LDAPサーバーのホスト名が、LDAPサーバーの証明書のサブジェクト代替名(SAN)拡張で指定されたDNSエント

IDプロバイダーのタイプ	説明
	リと一致していることを確認します。そうでない場合、LDAPサーバーへの接続が失敗します。 LDAPSプロトコルを使用する場合、既定のポートは636です。既定値を使用する場合、ポートの入力はオプションです。 注 複数のURLを入力できます。この場合には、それぞれを入力してからスペースバーを押します。 c. *証明書認証を有効にすることを予定している場合のみ*。「**サービスアカウントを使用する**」オプションを有効にし、Active Directoryへのログオンとユーザーの認証にHYCUが使用するサービスアカウントのユーザー名とパスワードを入力します。

Google	a. 「クライアントID」フィールドに、IDプロバイダーによって生成されたアプリケーションIDを入力します。
	b. 「シークレットID」に、クライアントIDに関連付けられており、IDプロバイダーによって生成されたアプリケーションシークレットを入力します。
	c. 「URIをリダイレクト」フィールドで、認証後にユーザーがリダイレクトされるURLを入力します。形式は次のとおりです。
	`https://<ServerName>:8443`
	この場合、<*ServerName*>はHYCUサーバーの完全修飾ドメイン名です。
	例：
	`https://hycu.example.com:8443`

Microsoft	a. 「クライアントID」フィールドに、IDプロバイダーによって生成されたアプリケーションIDを入力します。 b. 「シークレットID」に、クライアントIDに関連付けられており、IDプロバイダーによって生成されたアプリケーションシークレットを入力します。
Okta	a. 「クライアントID」フィールドに、IDプロバイダーによって生成されたアプリケーションIDを入力します。 b. 「シークレットID」に、クライアントIDに関連付けられており、IDプロバイダーによって生成されたアプリケーションシークレットを入力します。 c. 「発行者」フィールドに、IDプロバイダーの発行者のURLを入力します。
OpenID Connect IDプロバイダー	a. 「クライアントID」フィールドに、IDプロバイダーによって生成されたアプリケーションIDを入力します。 b. 「シークレットID」に、クライアントIDに関連付けられており、IDプロバイ

IDプロバイダーのタイプ	説明
	ダーによって生成されたアプリケーションシークレットを入力します。 c. 「発行者」フィールドに、IDプロバイダーの発行者のURLを入力します。 d. 「承認エンドポイント」フィールドに、IDプロバイダーの承認エンドポイントを入力します。 e. 「トークンエンドポイント」フィールドに、IDプロバイダーのトークンエンドポイントを入力します。 f. 「JWKSエンドポイント」フィールドに、IDプロバイダーのJSON Webキーセットエンドポイントを入力します。 g. *オプション*:「Userinfoエンドポイント」フィールドに、IDプロバイダーのUserinfoエンドポイントを入力します。 注 このフィールドを空にすると、HYCUがUserInfoエンドポイントデータを自動的に生成します。

4. 「**保存**」をクリックします。

後で以下を実行できます。

- 「**編集**」をクリックして必要な変更を加えることで、既存のIDプロバイダーに関する情報を編集します。

  注 「URIをリダイレクト」フィールドには、認証後にユーザーがリダイレクトされるURLが示されます(例 :`https://hycu.example.com:8443`)。あらかじめ入力されているホスト名は、ユーザーアクセスを認証するHYCU Backup Controllerのホスト名です。

- 「**削除**」をクリックして、既存のIDプロバイダーのいずれかを削除します。

証明書認証の有効化

証明書認証を有効にすると、Active Directoryユーザーは、パスワードを入力しなくても、クライアント証明書またはスマートカードを使用してHYCU Webインターフェースにログオンできます。

前提条件

- サービスアカウントが構成されたActive Directoryが少なくとも1つ、HYCUに追加されている。
- CA署名証明書がHYCUにインポートされている。この実行方法の詳細については、"カスタム証明書のインポート" ページ235を参照してください。

手順

1. 「IDプロバイダー」ダイアログボックスで、証明書認証を有効にする場合は、「**証明書認証を有効にする**」スイッチを使用します。
2. 「CA証明書」ドロップダウンメニューから、クライアント証明書を確認するためのCA署名付き証明書を選択します。

> ⚠ 重要 証明書認証を有効または無効にすると、HYCU Webユーザーインターフェースにログオンしている影響を受けるすべてのユーザーの接続が失われ、再度ログオンする必要があります。

HYCUインスタンスの管理

データ保護環境内のすべての既存のHYCUインスタンスは、「インスタンス」ダイアログボックスにリストされます。既存のすべてのHYCUインスタンスを表示することに加え、このダイアログボックスを使用して、新しいHYCUインスタンスを作成し、各HYCUインスタンスについての情報を表示し、HYCUインスタンスを削除することもできます。

HYCUインスタンスの詳細については、"HYCUインスタンス" ページ37を参照してください。

> 「インスタンス」ダイアログボックスへのアクセス
>
> 「インスタンス」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**インスタンス**」を選択します。

HYCU Webユーザーインターフェースの使用によるHYCUインスタンスの作成

HYCU仮想アプライアンスを「HYCUインスタンス」モードで展開して作成する代わりに、HYCU Webユーザーインターフェースを使用して、HYCUインスタンスを作成できます。

前提条件

- *Nutanix AHVクラスターでHYCUインスタンスを作成する場合*：HYCU仮想アプライアンスイメージが、Nutanixクラスター上に以下の形式で存在している。

  `hycu-<Version>-<Revision>`

  たとえば、`hycu-4.5.0-3634`。

- *HYCUインスタンスをNutanix ESXiクラスター上で作成する場合*：
  - vCenter Serverの特定の特権を持つユーザーが指定されている。どの特権をvSphereユーザーに割り当てるべきかの詳細については、"vSphereユーザーへの特権の割り当て" ページ269を参照してください。
  - HYCU OVFパッケージがvCenter Serverコンテンツライブラリにインポートされ、その形式は以下のとおりである。

    `hycu-<Version>-<Revision>`

    たとえば、`hycu-4.5.0-3634`。

手順

1. 「インスタンス」ダイアログボックスで、「＋ **新規**」をクリックします。「新規」ダイアログボックスが開きます。
2. 「全般」セクションで、HYCUインスタンスの名前を入力します。
3. 「ネットワーク設定」セクションで、以下を実行します。

a. HYCUインスタンスのホスト名を入力します。

> ⚠ 重要 作成するHYCUインスタンスごとに一意のホスト名を入力し、以下のルールに従ってください。
> - ホスト名には、アルファベット、数字、ハイフン(-) 、ピリオドのみ使用する。最大文字数は253文字で、アルファベット1文字を含める。
> - 各ホスト名セグメントの最大文字数は63。ホスト名セグメントの先頭または末尾はハイフンにできない。
> - トップレベルドメインの先頭または末尾は数字にできない。

b. 動的IPアドレスをHYCUに割り当てる場合は、「**DHCP**」スイッチを使用します。そうでない場合は、IPアドレス、ネットマスク、およびゲートウェイを指定します。

4. 「展開」セクションで、以下を実行します。

a. 「宛先」ドロップダウンメニューから、HYCUを配置するNutanixクラスターを選択します。

b. 「ネットワーク」ドロップダウンメニューから、「VLAN」を選択します。

c. 「Datastore」ドロップダウンメニューから、データストアを選択します。

> 💡 ヒント「**自動選択**」を選択すると、HYCUは使用可能なスペースが最も多いデータストアを選択します。

5. 「**保存**」をクリックします。

HYCUインスタンス情報の表示

各HYCUインスタンスに関する次の情報を表示できます。

HYCUインスタンス情報	説明
VM名	HYCUインスタンスの名前(把握している場合) 。
ホスト名	HYCUインスタンスのホスト名。
ソース	HYCUインスタンスが存在するNutanixクラスター(HYCUに追加された場合にのみ表示されます) 。
ステータス	HYCUインスタンスが実行しており、HYCU Backup Controllerと通信している場合に表示されます。
バージョン	HYCUインスタンスのバージョン(たとえば、`hycu-4.5.0-3634`) 。
IPアドレス	HYCUインスタンスに現在割り当てられているIPアドレス。

HYCUインスタンスの削除

手順

1. 「インスタンス」ダイアログボックスで、HYCUインスタンスのリストから、削除するものを選択し、「🗑 **削除**」をクリックします。

> ⚠ 重要 選択したHYCUインスタンスはHYCUとNutanixクラスターのどちらからも削除されます。

2. 「インスタンスの削除」ダイアログボックスで、選択したHYCUインスタンスを削除することを確認するために、「**はい**」をクリックします。

iSCSIイニシエーターシークレットの設定

HYCU展開中に、HYCU iSCSIクライアント(iSCSIイニシエーターと呼ばれる) は、データの保存にHYCUがiSCSIターゲットを使用できるようにセットアップされます。

相互CHAP認証をiSCSIイニシエーターとiSCSIターゲットとの間で構成する場合、iSCSIイニシエーターシークレット(セキュリティキー) を指定する必要があります。相互認証を有効にする方法の詳細については、"ターゲットのセットアップ" ページ38を参照してください。

> 「iSCSIイニシエーター」ダイアログボックスへのアクセス
>
> 「iSCSIイニシエーター」ダイアログボックスにアクセスするには、「⚙ **管理**」にクリックし、「**iSCSIイニシエーター**」を選択します。

iSCSIイニシエーターの秘密を設定するには、次の手順に従います。

1. 「iSCSIイニシエーター」ダイアログボックスに、秘密を入力します。
2. 「**保存**」をクリックします。

ライセンス

HYCU仮想アプライアンスを展開したら、HYCUは試用ライセンスですぐに使い始めることができます。このライセンスは30日後に自動的に失効し、再利用はできません。したがって、使い始めてから30日以内に有効なライセンスを取得してください。

HYCUライセンスはHYCUバックアップコントローラーにリンクされ、環境に最も適したライセンスタイプまたはライセンスタイプの組み合わせを決定できます。次のライセンスタイプが使用できます。

- 標準ライセンス
  - ソケットベースライセンス

    ライセンスは、HYCUを使用して保護する予定のすべてのソース(Nutanixクラスター、vCenterサーバー、Nutanix Files、および物理マシン) のCPUソケットの数に基づいています。
  - VMベースライセンス

    ライセンスは、HYCUを使用して保護する予定のすべてのソースおよび物理マシン上の仮想マシンの数に基づいています。
- ファイルサーバーライセンス

  これらのライセンスは、単独で使用することも、標準ライセンスと組み合わせて使用することもできます。

- ソケットベースライセンス

  ライセンス数は、HYCUを使用して保護する予定のNutanix Filesサーバーが存在するすべてのNutanixクラスター上のCPUソケットの数に基づきます。

  > ⚠ 重要 このタイプのライセンスは、Nutanix Filesについてのみ予約されています。Nutanix Filesソケットベースのライセンスをお持ちであり、PowerScale OneFSを保護したい場合は、HYCU販売担当員にお問い合わせください。

- キャパシティベースライセンス

  ライセンスは、すべての保護されたファイルサーバー共有の全体サイズ(テラバイト単位)として自動的に計算されるファイルサーバー共有のキャパシティに基づいています。

- HYCU Protégéライセンス

  このライセンスを他のライセンスと組み合わせて使用すると、異なるインフラストラクチャ間で仮想マシンを移行し、クラウドへのデータの災害復旧を実行し、HYCU for Google CloudおよびHYCU for Azureデータ保護環境を監視できます。

考慮事項

- ライセンスが有効であることを確認する場合には、HYCUはPROTECTEDまたはPROTECTED_DELETEDステータスのエンティティを含むソースのみを考慮します。
- HYCU Backup Controllerの保護にはライセンスは必要ありません。
- マネージドサービスプロバイダ(MSP)ライセンスがHYCUに適用されている場合、HYCUとのテレメトリデータの共有は既定で有効になっており、無効にはできません。
- *Nutanix Community Edition(CE)環境の場合*、HYCUライセンスは不要です。

手順

1. 必要数のHYCUライセンスを購入します。オプションの説明については、販売担当者にお問い合わせください。
2. ライセンス要求を作成します。詳細については、"ライセンス要求の作成" 下を参照してください。
3. Webライセンスポータルからライセンスを要求して取得します。詳細については、"ライセンスの要求と取得" 次のページを参照してください。
4. ライセンスをアクティベーションして、HYCUの使用を開始します。詳細については、"ライセンスのアクティベーション" ページ225を参照してください。

> 「ライセンス」ダイアログボックスへのアクセス
>
> 「ライセンス」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ライセンス**」を選択します。

ライセンス要求の作成

HYCUライセンスを取得するには、Webライセンスポータルにリクエストフォームを送信する必要があります。

前提条件

- 必要数のHYCUライセンスを購入済みで、エンタイトルメント注文番号を持っている。
- 保護するソースをデータ保護環境に追加済みである。説明については、“ソースの追加” ページ 32を参照してください。

手順

1. 「ライセンス」ダイアログボックスで、「**ダウンロードリクエスト**」をクリックします。
2. ライセンス要求ファイルを一時的な場所に保存します。

> **例**
> license.reqファイル：
>
> ```
> CN myCompany
> ND C0F90A56-3FCC-4437-A49C-EFBA9BD8FC0F
> VER V2
> PID nutanixbackup
> NRP 3
> QTY 127
> AFS 3
> AFSCAP 4
> NRPALL 12
> QTYALL 167
> HYCUVER 4.5.0-66
> HSUD 83B770D4D02B9F9D516C9FAD7027F50AEF67C1F85209735165B7C500CCB3BFDC
> NEXT NODE
> ```

ライセンスの要求と取得

ライセンス要求ファイルを作成したら、ライセンスポータルからライセンスを取得できます。

手順

1. Webライセンスポータルに以下から接続します。

   https://licensing.hycu.com/

2. ライセンスポータルのアカウントをすでに持っている場合は、「**サインイン**」をクリックし、ユーザー名とパスワードを入力し、「**ログイン**」をクリックします。そうでない場合は、アカウントを作成してから、新しく作成したユーザーアカウントでサインインします。
3. 「**ライセンスのアクティベーション**」リンクをクリックして、エンタイトルメント注文番号を入力します。「**次へ**」をクリックします。
4. 次の手順を実行します。
   a. ライセンス要求ファイルを参照し、「**ライセンスの要求**」をクリックします。
   b. 「永続ライセンスのアクティベーション」ページで、ライセンスタイプと、アクティベーションするライセンスの数を指定します。既定では、ライセンス要求ファイルからのライセンス数が提供されま

す。購入したライセンスの数を超えない別の値を指定できます。「**ライセンスのアクティベーション**」をクリックします。

数分以内に、ライセンスファイルlicense.datが添付されたメールを受信します。

> **例**
> license.datファイル：
>
> ```
> CN myCompany
> ND C0F90A56-3FCC-4437-A49C-EFBA9BD8FC0F
> VER V2
> PID nutanixbackup
> EXP 05.04.2022
> NRP 3
> AFSCAP 5
> LK
> 302C02146B7A48EE010CD1E1212E73B27DD2E58958B6C6ED021426BA2A4CCD271CC45
> 571A35129B7E8B4E46A75AD
> NEXT NODE
> ```

5. ライセンスファイルをローカルに保存します。

ライセンスのアクティベーション

HYCUライセンスのライセンス要求をWebライセンスポータルに送信すると、製品ライセンスファイルが添付されたメールを受け取ります。

手順

1. 「ライセンス」ダイアログボックスで、「**ライセンスのアップロード**」をクリックします。
2. メールで受け取ったライセンスファイルを参照し、「**アップロード**」をクリックします。

ライセンスがアクティベーションされると、ライセンスに関連する情報が更新されます。

> 注 環境が拡張する場合はいつでも新しいライセンスを追加できます。HYCU販売担当員にお問い合わせください。

ライセンスに関連する以下の情報を確認できます。

- ステータス
- ライセンスタイプ
- Backup Controller ID
- ライセンス有効期限
- マネージドサービスプロバイダ
- 保護されライセンスされた、仮想マシンと物理マシンの数
- 保護されライセンスされたソケット数
- Nutanix Filesのライセンスされたソケット数
- 保護されライセンスされたファイルサーバーのキャパシティ

ログのセットアップ

さまざまなレベルで情報を記録するようにログをセットアップして、HYCU操作全体の分析とトラブルシューティングを行い、バックアップと復元のパフォーマンスの問題を診断できます。

前提条件

ログファイルをHYCUカスタマーサポートに送信する場合：HYCUとのテレメトリデータの共有が有効である。説明については、"HYCUとのテレメトリデータの共有" ページ237を参照してください。

> 「ロギング」ダイアログボックスへのアクセス
>
> 「ロギング」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ロギング**」を選択します。

「ロギング」ダイアログボックスで、以下を実行できます。

- 「**ログを取得する**」をクリックして、既存のログファイルをダウンロードして表示します。

  ログファイルは記録されたときに指定されたレベルでダウンロードします。ログがセットアップされていない場合、ログファイルは既定の設定でダウンロードされます。変更されたログレベルは、新しいログ設定を保存した後に記録されるログファイルにのみ適用されます。

  zipファイルを抽出したら、以下の場所のログファイルを確認します。

  `/opt/grizzly/logs/`

- *HYCUとのテレメトリデータの共有が有効である場合のみ*。「**ログを送信する**」をクリックして、既存のログファイルをHYCUカスタマーサポートに送信します。

  ログファイルは記録されたときに指定されたレベルで送信します。ログがセットアップされていない場合、ログファイルは既定の設定でアップロードされます。変更されたログレベルは、新しいログ設定を保存した後に記録されるログファイルにのみ適用されます。

- ログをセットアップします。これを実行するには、次の手順に従います。
  1. 以下のログ設定に値を指定します。

ログ設定	説明
最大ログファイルサイズ (MiB)	ログファイルの最大サイズ。 既定のログファイルサイズは10 MiBで、最大ログファイルサイズは10 GiBです。
ログファイル数	ログファイルの数。 既定の数は9です。
レベル	以下のログレベルが使用できます。 ◦ `Informational`(既定):HYCUの操作に関する情報メッセージがログファイルに記録されます。 ◦ `Detailed`:すべてのアクティビティはログファイルに記録されます。
発信RESTコールレベル *(「詳細」ログレベルが選択されている場合にのみ選択可能。)*	以下のレベルが選択できます。 ◦ `Off`(既定):発信RESTコールログはログファイルには記録されません。 ◦ `Informational`:発信RESTコールに関連する操作に関する情報メッセージがログファイルに記録されます。 ◦ `Detailed`:発信RESTコールに関連するすべてのアクティビティがログファイルに記録されます。
着信RESTコールレベル *(「詳細」ログレベルが選択されている場合にのみ選択可能。)*	以下のレベルが選択できます。 ◦ `Off`(既定):着信RESTコールログはログファイルには記録されません。 ◦ `Informational`:着信RESTコールに関連する操作に関する情報メッセージがログファイルに記録されます。 ◦ `Detailed`:着信RESTコールに関連するすべてのアクティビティがログファイルに記録されます。

  2. HYCUのアップグレード後にもカスタムログ設定を同じままにしておきたい場合は、「**アップグレード後も設定を維持する**」スイッチを使用します。通常はログをトラブルシューティング目的で設定し、製品の通常使用には同じログレベルを必要としないので、このスイッチはオフになっています。
  3. 「**保存**」をクリックします。

     > 注 変更されたログレベルは、新しいログ設定を保存した後に記録されるログファイルにのみ適用されることに注意してください。

後から新しい値を指定し、「**保存**」をクリックして設定を変更したり、「**既定**」をクリックして既定値を設定したりできます。

ネットワークの構成

ネットワークを構成する際、IPアドレスおよびHYCUリスニングポート番号などのネットワーク設定を変更すること、またはネットワーク帯域幅の調整を有効にすることができます。実行内容に応じて、以下のいずれかのセクションを参照してください。

- “ネットワーク設定の変更” 下
- “ネットワーク帯域幅の制限” 次のページ

> 「ネットワーク」ダイアログボックスへのアクセス
>
> 「ネットワーク」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ネットワーク**」を選択します。

ネットワーク設定の変更

ネットワーク設定を変更することで、ネットワークをお使いの環境の要件に適した構成にすることが可能になります。

> ⚠ 重要 HYCUネットワーク設定に変更を加えると、自動的にログアウトされ、セッションが再開されます。

制限事項

同じネットワーク上の複数のネットワークアダプタはサポートされていません。

考慮事項

HYCUの展開中に指定したネットワークはメインに設定され、🔖アイコンで表されます。後でNutanix Prism WebコンソールまたはvSphere (Web) Clientを使用してHYCU Backup Controllerを複数のネットワークに接続する場合は、別のネットワークをメインネットワークとして使用できます。これを行うには、目的のネットワークにリスニングポートとSSL証明書が指定されていることを確認し、このネットワークを選択して、「🔖 **メインに設定**」をクリックします。

手順

1. 「ネットワーク」ダイアログボックスに、HYCU Backup Controllerのホスト名と、それが接続されているネットワークが表示されます。設定を変更するネットワークを選択し、「✎ **編集**」をクリックします。
2. 必要に応じて、IPアドレス、ゲートウェイ、ドメイン名、ネットマスク、DNSサーバーを変更します。
3. *HYCU Backup Controllerが複数のネットワークに接続されている場合のみ*。このネットワークを使用してHYCU Webユーザーインターフェースにアクセスする場合は、「**このポートでのリスニングを有効にする**」スイッチを使用します。

   > 📋 注 HYCUの展開中に指定したネットワークでは、このスイッチは既定で有効になっています。

4. *「このポートでのリスニングを有効にする」スイッチが有効な場合のみ*。以下を実行します。

a. 「リスニングポート」フィールドに、HYCU Webユーザーインターフェースへのアクセスに使用するポート(既定では8443)を入力します。

> ⚠ 重要 インフラストラクチャでファイアウォールが構成されている場合は、指定したポートが開いていることを確認します。

b. 「SSL証明書」ドロップダウンメニューから、このネットワークに使用するSSL証明書を選択します。適切な証明書がリストにない場合は、「**管理**」をクリックして、必要な証明書をインポートまたは生成できます。SSL証明書の生成とインポート方法に関する説明については、"SSL証明書の構成" ページ234を参照してください。

> 注 この「このポートでのリスニングを有効にする」スイッチが無効になっている場合は、このネットワークに使用するSSL証明書を指定することもできます。

5. 「**保存**」をクリックします。

ネットワーク帯域幅の制限

ネットワーク帯域幅の調整により、HYCUで使用できる帯域幅を制限できるようになります。サイトに対する帯域幅の制限を定義することで、お使いの環境にある全ネットワーク操作で十分な帯域幅を使用可能にできます。

制限事項

HYCUから発信されるトラフィックに対してのみ、ネットワーク帯域幅を制限できます。

考慮事項

- HYCU Managerではネットワーク帯域幅の調整を使用できません。
- データの復元先として予定しているストレージコンテナのIPアドレスが、帯域幅を制限するサイト内で定義されている場合、復元パフォーマンスに影響が出る可能性があります。
- クラウド、iSCSI、またはSMBターゲットが複数のIPアドレスを使用する可能性があります。サイトを定義する際、使用されているIPアドレスをすべて入力してください。パブリッククラウドにより使用されるIP範囲の詳細については、各クラウドの資料を参照してください。
- AWS IPアドレス用にネットワーク帯域幅を調整しても、テレメトリデータの共有に影響があります。ログファイルの送信に時間がかかる場合があります。
- *HYCUがファイル共有保護に使用されている場合のみ*。ネットワーク帯域幅の調整を有効にしている場合、設定した制限はHYCUインスタンスにも適用されます。

推奨事項

NFSターゲットに対してネットワーク帯域幅を調整することは推奨されません。

手順

1. 「ネットワーク」ダイアログボックスで、「**スロットリング**」タブをクリックし、「**＋ 新規**」をクリックします。「新規」ダイアログボックスが表示されます。
2. 帯域幅を制限するサイトの名前とその説明(オプション)を入力します。

3. 「帯域幅制限」フィールドで、HYCUからサイトへのデータの転送に使用できる最高速度(KiBps、MiBps、またはGiBps単位)を指定します。
4. 「IPアドレス/範囲一覧」フィールドで、帯域幅を制限するサイトのIPアドレスかIP範囲を入力します。IPアドレスまたはIP範囲は以下の形式で入力できます。
   - 単一のIPv4アドレス:192.0.2.1
   - CIDRプレフィックスが付いたIPv4サブネット:192.0.2.0/24
   - IPv4範囲:192.0.2.3 ~ 192.0.2.100
5. *オプション*:「スロットリングウィンドウ」ドロップダウンメニューから、帯域幅の制限に使用するスロットリングウィンドウを選択します。新しいスロットリングウィンドウを作成することや、「**管理**」をクリックして既存のウィンドウを編集することもできます。調整ウィンドウの作成方法の詳細については、"調整ウィンドウの作成" 下を参照してください。

   > ⚠ 重要 同じIPアドレスを持つ複数のサイトを定義する場合は、各サイトに割り当てる調整ウィンドウが重複しないように注意してください。

6. 「**保存**」をクリックします。

既存のサイトはいずれも後から編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。

調整ウィンドウの作成

HYCUでは、ネットワーク帯域幅を調整する時間枠を定義できます。調整ウィンドウを使用する場合、指定された時間内だけネットワーク帯域幅が制限されます。たとえば、ネットワーク上でのアクティビティが多い時間帯である生産のピーク時間に、ネットワーク帯域幅を制限することができます。

手順

1. 「ネットワーク」ダイアログボックスで、「**スロットリング**」タブをクリックし、「**Windows**」をクリックします。「スロットリングウィンドウ」ダイアログボックスが表示されます。
2. 「**新規**」をクリックします。「新規」ダイアログボックスが表示されます。
3. 調整ウィンドウの名前を入力します。
4. 「タイムゾーン」ドロップダウンメニューで、スロットリングウィンドウのタイムゾーンを指定します。表示されているタイムゾーン(ローカルタイムゾーンまたはHYCUバックアップコントローラータイムゾーン)のいずれかをクリックするか、ドロップダウンメニューから選択することができます。
5. ネットワーク帯域幅を制限する曜日と時間を選択します。

   > ヒント クリックしてドラッグすると、追加する日と時間を含む時間枠をすばやく選択できます。

6. 「**保存**」をクリックします。

既存のスロットリングウィンドウはいずれも後から編集することができます(「**編集**」をクリックして必要な変更を行います)。または不要になったものは削除できます(「**削除**」をクリックします)。

電源オプションの設定

HYCU Backup Controllerの電源オプションを設定して、そのアクティビティを一時停止したり再開したりできます。

「電源オプション」ダイアログボックスへのアクセス

「電源オプション」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**電源オプション**」を選択します。

電源オプション	説明
すべて一時停止	すべてのHYCU Backup Controllerアクティビティを一時停止します。 指定した時間の経過後にHYCU Backup Controllerアクティビティを自動的に再開する場合は、「以下の時間後に自動再開」フィールドで、アクティビティが再開されるまでの経過時間数(1～168)を指定します。 現在実行中のすべてのジョブは正常に完了できます。HYCU Backup Controllerが再開されると、キューにあるすべてのジョブが開始されます。アクティビティが一時停止している間は、新しいジョブを開始できません。
クリーンアップを一時停止	ターゲットのクリーンアップを一時停止し、有効になっている場合には、イベントとジョブを消去します。 スナップショットのクリーンアップは影響を受けません。
再開	HYCU Backup Controllerアクティビティを続行できます。

シークレットの管理

HYCUでは、Conjurシークレット管理ソリューションを採用することで、資格情報(シークレット)を安全に保管、アクセス、管理できます。HYCUシークレットを1つ以上のConjur構成(つまり、セキュリティルールを定義する1つ以上のポリシーのセット)としてConjurに保存すると、管理が簡単になり、確実に許可された関係者だけがそのリソースにアクセスできるようになります。

前提条件

- 1つ以上のポリシーのセットとして、Conjur環境がセットアップされ、HYCUシークレットが保存されています。説明については、Conjurの資料を参照してください。
- インフラストラクチャ管理者によって、ConjurサーバーのSSL証明書がHYCUにインポートされる必要があります。説明については、“SSL証明書の構成” ページ234を参照してください。

制限事項

- Conjurに保存する予定のHYCU資格情報は、${で始まり}で終わらない場合があります。
- HYCUユーザーはConjurを使用して管理できません。HYCUユーザーの詳細については、“ユーザーの管理” ページ197を参照してください。

考慮事項

- 混合モードが可能です。つまり、この統合の恩恵を受けられるようにするために、すべてのHYCUシークレットをConjurに保存する必要はありません。
- Conjurに保存されているシークレットを提供する場合には、HYCUでは必ず以下の構文を使用します。

  ```
  ${<PathtoSecret>}
  ```

推奨事項

Conjurでシークレットの名前を変更する予定がある場合のみ。Conjurでシークレットの名前を変更するたびに、HYCUのキャッシュをクリアすることをお勧めします。これを実行するには、「シークレット管理」ダイアログボックスで、「**キャッシュのクリア**」をクリックします。これもHYCUによって24時間ごとに自動的に実行されますが、ビジネスプロセスの継続性のために、手動で行うことをお勧めします。

> **ヒント** Conjurに保存されている値の入力をサポートするHYCU Webユーザーインターフェースのすべてのフィールドの横には、インフラストラクチャグループ構成であれば、プライベート構成であればのアイコンが表示されます。

「シークレット管理」ダイアログボックスへのアクセス

「シークレット管理」ダイアログボックスにアクセスするには、「⚙ **管理**」にクリックし、「**シークレット管理**」を選択します。

Conjur構成の追加

考慮事項

HYCUデータ保護環境ごとに、各セルフサービスグループに対して、1つのインフラストラクチャグループConjur構成と、1つのプライベートConjur構成を追加することができます。

手順

1. 「シークレット管理」ダイアログボックスで、実行するConjur構成のタイプに応じて、次のいずれかのボタンをクリックします。

Conjur構成タイプ	説明
インフラストラクチャグループ構成の追加	*インフラストラクチャグループ管理者の場合のみ利用可能です*。すべてのデータ保護タスクと管理タスクを実行する際に、Conjurに保存されているシークレットを提供できるようにします。たとえば、ソースとターゲットを追加するとき、IDプロバイダーを追加するときなどです。
プライベート構成の追加	*インフラストラクチャまたはセルフサービスグループの管理者である場合に利用可能*以下のタスクを実行する際に、Conjurに保存されているシークレットを提供できるようにします。

Conjur構成タイプ	説明
	• クラウドアカウントの追加。 • 資格情報グループを仮想マシンに割り当てます。 • Webhook通知をセットアップします。

2. 「アプライアンスURL」フィールドに、接続先のConjurサーバーのURLを入力します。
3. 「アカウント」フィールドに、Conjur環境設定時に指定したアカウントの名前を入力します。
4. 「ログイン認証」フィールドに、Conjurホストユーザー名を入力します。例：

   ```
   host/HycuPolicy/hycuBckupController
   ```

   この例では、hostはユーザーのタイプ、HycuPolicyはユーザーが属するポリシーの名前、hycuBckupControllerはユーザー名です。
5. 「認証APIキー」フィールドに、Conjurホストユーザー名に対応するAPIキーを入力します。
6. *インフラストラクチャグループ管理者である場合のみ。*一方のタイプのConjur構成を実行するときに、他方のタイプのConjur構成の実行に同じ値を使用する場合は、「**プライベート構成に同じ値を使用する**」または「**インフラストラクチャグループ構成に同じ値を使用する**」スイッチを有効にします。
7. 「**保存**」をクリックします。

Conjur構成の編集

手順

1. 「シークレット管理」ダイアログボックスで、編集するConjur構成の横にある「**編集**」をクリックします。
2. 必要に応じて、選択したConjur構成を編集します。認証ログインとAPIキー情報の編集を予定している場合は、必ず最初に「**認証の変更**」チェックボックスを選択します。

   Conjur構成プロパティの詳細については、“Conjur構成の追加” 前のページを参照してください。
3. 「**保存**」をクリックします。

Conjur構成の削除

手順

1. 「シークレット管理」ダイアログボックスで、削除するConjur構成の横にある「**削除**」をクリックします。
2. 「**はい**」をクリックして、選択したConjur構成を削除することを確認します。

SMTPサーバーの構成

HYCUがメール通知を送信できるようにする前に、HYCUが使用するSMTPサーバーを構成する必要があります。

前提条件

STARTTLSまたはSSL/TLSセキュリティモードを使用してメールトラフィックを保護する場合：有効なSSL証明書がHYCUにインポートされていること。この実行方法の詳細については、"SMTP接続の保護" ページ265を参照してください。

> 「SMTPサーバー設定」ダイアログボックスへのアクセス
>
> 「SMTPサーバー設定」ダイアログボックスにアクセスするには、「⚙ **管理**」にクリックし、「**SMTPサーバー設定**」を選択します。

手順

1. 「SMTPサーバー設定」ダイアログボックスで、以下の情報を入力します。

必須情報	説明
ユーザー名	SMTPサーバーのアカウントのユーザー名。
パスワード	SMTPサーバーのアカウントのパスワード。
表示名	メール送信者の表示名。
ホスト名またはIPアドレス	SMTPサーバーのホスト名またはIPアドレス。
ポート	使用されるポート番号(通常は25に設定)。
セキュリティモード	電子メールトラフィックを保護するために使用されるプロトコル。なし、STARTTLS、またはSSL/TLSに設定できます。
送信元メールアドレス	メール通知の送信元のメールアドレス。

2. 「**保存**」をクリックします。

メール通知を送信するようにHYCUを構成できるようになりました。この実行方法の詳細については、"メール通知のセットアップ" ページ166を参照してください。

SSL証明書の構成

データ保護環境で信頼できる安全な通信を確立するには、SSL証明書を構成する必要があります。

> 「SSL証明書」ダイアログボックスへのアクセス
>
> 「SSL証明書」ダイアログボックスで、「⚙ **管理**」をクリックし、「**SSL証明書**」を選択します。

表示される「SSL証明書」ダイアログボックスで、証明書名、証明書の共通名、証明書の有効期限、証明書のキーサイズなど、SSL証明書に関する情報を表示できます。

考慮事項

SSL証明書を作成またはインポートしたら、この証明書を指定して、HYCUネットワーク設定も必ず更新します。この実行方法の詳細については、"ネットワークの構成" ページ228を参照してください。

推奨事項

HYCU展開中に自動的に生成される自己署名証明書をCA署名証明書で置き換えることをお勧めします。

手順

自己署名証明書を作成するか、カスタム証明書をHYCUにインポートするかに応じて、次のいずれかのセクションを参照します。

- “自己署名証明書の作成” 下
- “カスタム証明書のインポート” 下

自己署名証明書の作成

手順

1. 「SSL証明書」ダイアログボックスで、「**生成**」をクリックします。「生成」ダイアログボックスが表示されます。
2. 以下の証明書関連情報を提供します。
   - 名前
   - 一般名
   - 組織
   - 組織単位
   - ロケーション
   - 国
   - キーサイズ

   > ⚠ 重要 各フィールドの最大文字数は64です。
3. 「**生成**」をクリックします。

自己署名証明書はSSL証明書のリストに追加されます。HYCUによって生成される各SSL証明書は3年間有効であり、証明書の有効性を維持する必要があることに注意してください。

カスタム証明書のインポート

前提条件

- 証明書はPKCS#7標準に準拠し、PEM形式でエンコードされている。
- すべての証明書ファイルは暗号化されていない。
- *SSLキーペアをインポートする場合* :秘密鍵と証明書を使用できる。
- *CA署名付き証明書をインポートする場合* :CA署名付き証明書またはトラストチェーン証明書が使用可能である。

考慮事項

証明書が共通名(CN)にワイルドカードを使用している場合には、「証明書のサブジェクト代替名」フィールドに、すべての可能なホスト名またはFQDN、および対応するIPアドレスが含まれていることを

確認します。そうしない場合、証明書はWebブラウザーまたはhyCLIによって無効と認識されることがあります。

手順

1. 「SSL証明書」ダイアログボックスで、「**インポート**」をクリックします。「インポート」ダイアログボックスが表示されます。
2. SSLキーペアとCA署名付き証明書のどちらをインポートするかに応じて、次のいずれかのタブをクリックして、指示に従います。

タブ	説明
SSLキーペア	a. 証明書の名前を入力します。 b. 次のファイルを参照します。 • *オプション* :CA証明書/チェーン :CA署名付き証明書またはトラストチェーン証明書を含むファイル。 • 証明書 :インポートする秘密鍵に対応する証明書を含むファイル。 • 秘密鍵 :インポートする証明書に関連付けられている秘密鍵を含むファイル。 秘密鍵は、PKCS#1またはPKCS#8形式のRSAまたはECDSAアルゴリズムで作成される必要があります。RSAアルゴリズムで作成される秘密鍵の最小キーサイズは2048ビットです。 注 Conjurを使用してHYCUのシークレットを管理する場合、ファイルを参照する代わりにシークレットを提供するのであれば、「**シークレットマネージャーから値を取得**」を有効にすることができます。シークレットの管理の詳細については、"シークレットの管理" ページ231を参照してください。 c. 「**インポート**」をクリックします。
CA証明書/チェーン	a. 証明書の名前を入力します。 b. CA署名付き証明書またはトラストチェーン証明書を含むファイルを参照します。 c. 「**インポート**」をクリックします。 d. HYCUアプリケーションサーバーを再起動します。説明については、"HYCUアプリケーションサーバーの管理" ページ259を参照してください。

自己署名証明書またはカスタム証明書の名前を変更したり(「**編集**」をクリックして必要な変更を加える)、不要になった証明書を削除したりすることもできます(「**削除**」をクリックする)。

HYCUとのテレメトリデータの共有

HYCUを設定して、テレメトリデータを収集できます。このデータは、HYCUがプロアクティブなサポートを提供し、データ保護環境の要件により適切に応えるためにパフォーマンスを向上させるのに役立ちます。

テレメトリを介して診断データを共有すると、次のようにHYCUの事前対応型のコンテキスト化サポートが可能になります。

1. syslogファイル、HYCU内部データベース(PostgreSQL) ログ、システムアクティビティ情報(sar) 、HYCUライセンス情報、および特定のインフラストラクチャに関するその他の詳細情報を含む、データ保護環境の詳細データを収集し、このデータをHYCUカスタマーサポートに送信します。

   > ⚠ 重要 HYCUはデータ保護環境から機密情報を収集しません。

2. 収集されたデータを分析し、内部レポートを生成し、最終的な問題または好ましくない傾向を特定して、問題解決時間を大幅に短縮します。
3. 最終的な問題に対処するHYCU環境に関するフィードバックを提供し、環境を調整してインフラストラクチャとパフォーマンスを改善する方法を指示します。

> 注 高度なトラブルシューティングに含める各HYCU Backup Controllerのテレメトリデータ共有を有効にする必要があります。

前提条件

有効なHYCUカスタマーサポートユーザーアカウントを持っている。

考慮事項

マネージドサービスプロバイダ(MSP) ライセンスがHYCUに適用されている場合、HYCUとのテレメトリデータの共有は既定で有効になっており、無効にはできません。

「テレメトリ」ダイアログボックスへのアクセス

「テレメトリ」ダイアログボックスにアクセスするには、「⚙ **管理**」にクリックし、「**テレメトリ**」を選択します。

手順

「テレメトリ」ダイアログボックスで、「**テレメトリデータをHYCU Inc.と共有します**」スイッチを使用してHYCUがテレメトリデータを収集できるようにし、「**保存**」をクリックします。

HYCUはデータの収集を開始し、HYCUカスタマーサポートに送信します。その後、テレメトリ診断データは1日に1回、HYCUカスタマーサポートに送信されます。「ジョブ」パネルで、収集ジョブステータスを表示できます。

テレメトリデータをHYCUと共有する必要がなくなったと後で判断した場合は、構成済みの各HYCU Backup Controllerに対して「**テレメトリデータをHYCU Inc.と共有します**」オプションを無効にします。

> 注「**テレメトリデータをHYCU Inc.と共有します**」オプションが有効になっている場合、ログファイルをHYCUカスタマーサポートに送信できます。詳細については、“ログのセットアップ” ページ226を参照してください。

HYCUのアップグレード

新しいソフトウェアリリースバージョンが入手可能になると、HYCUをアップグレードできます。

前提条件

- HYCU Backup Controllerがあるソースが HYCUに追加されている。
- HYCU Backup Controllerアクティビティが保留中である。これを実現する方法の説明については、“電源オプションの設定” ページ231を参照してください。
- 中止したくないジョブを終了している(アップグレードプロセスは現在実行中のすべてのジョブを中止します) 。
- HYCUデータディスクがHYCUシステムディスクより大きい。ディスクサイズを増やす方法の説明については、“HYCU仮想ディスクのサイズの増分” ページ268を参照してください。

考慮事項

- *Nutanixクラスターの場合* :HYCU Backup ControllerがNutanix保護ドメインの一部である場合(推奨方法) 、アップグレード後にHYCU Backup Controller仮想マシンの新しいバージョンがこの保護ドメインに含まれていることを確認します。古いHYCU Backup Controller(仮想マシン) はNutanixクラスター上に残り、<*HYCUBackupControllerName*>_version_<*OldHYCUVersion*>に名前変更されます。正常にアップグレードしたら、それを削除してNutanix保護から問題なく除去することができます。
- アップグレードされるHYCU仮想マシンのHYCU Webユーザーインターフェースにログオンしているユーザーは、プロセスの完了後にWebブラウザーでWebユーザーインターフェースページの強制リロードを実行する必要があります。
- アップグレードすると、HYCU仮想マシンの修正プログラムディレクトリから以前に追加された修正プログラムパッケージが削除されます。
- *Nutanix ESXiクラスターの場合* :Nutanix AOSのバージョンが5.11.3以降で、バージョン4.0.3からHYCUをアップグレードする場合、アップグレード後の最初のデータのバックアップはフルバックアップになることに注意してください。
- *S3互換ターゲットの場合* :HYCUのアップグレード後に、安全なHTTPSアクセスを提供する場合は、CA証明書/チェーンをHYCUにインポートします。詳細については、“カスタム証明書のインポート” ページ235を参照してください。

手順

- “Nutanix AHVクラスター上のHYCUのアップグレード” 次のページ
- “Nutanix ESXiクラスター上のHYCUのアップグレード” ページ240
- “vSphere環境でのHYCUのアップグレード” ページ244

Nutanix AHVクラスター上のHYCUのアップグレード

前提条件

- Nutanix Prism Webコンソールの「VMの更新」ダイアログボックスの「ディスク」セクションで、HYCUシステムディスクが起動デバイスとして選択されている。
- アップグレードに使用するHYCU仮想アプライアンスイメージの状態が、Nutanix Prismイメージサービスで「アクティブ」である。

詳細については、Nutanixの資料を参照してください。

考慮事項

ファイル共有保護にHYCUを使用する場合、Nutanix AHVクラスターに存在するHYCUインスタンスは、以下が当てはまる場合、HYCUアップグレードプロセス中に自動的にアップグレードされます。

- HYCUインスタンスが存在するNutanixクラスターがHYCUに追加されています。
- HYCU仮想アプライアンスイメージが、次の形式の同じNutanixクラスター上にあります。

  `hycu-<Version>-<Revision>`

  たとえば、`hycu-4.5.0-3634`。

そうでない場合は、HYCUアップグレード手順に従って、HYCUインスタンスのアップグレードを実行します。

手順

1. Nutanix Prism Webコンソールにログオンし、Nutanix AHVクラスターのアップグレードに使用するHYCU仮想アプライアンスイメージをアップロードします。
   a. ⚙をクリックし、「**イメージ構成**」を選択します。
   b. 「イメージ構成」ダイアログボックスで、「**イメージのアップロード**」をクリックします。
   c. 「イメージの作成」ダイアログボックスで、以下の情報を入力します。
      i. HYCUイメージ名を、アップロードするHYCUイメージファイルの名前に対応する形式で入力します。

      > ⚠ 重要 HYCU仮想アプライアンスイメージは、以下の形式でNutanix AHVクラスターにアップロードする必要があります。
      >
      > `hycu-<Version>-<Revision>`
      >
      > 例 :`hycu-4.5.0-3634`
      >
      > 別の形式でHYCUイメージ名を入力すると、アップグレードにはそのイメージを使用できません。

      ii. *オプション*:注釈を入力します。
      iii. 「イメージのタイプ」ドロップダウンメニューから、「**ディスク**」を選択します。
      iv. 「ストレージコンテナ」ドロップダウンメニューから、アップロードするイメージのストレージコンテナを選択します。

v. 「イメージのソース」セクションから、イメージファイルの場所を指定します。

vi. 「**保存**」をクリックします。

vii. 画像が正常にアップロードされたら、「**閉じる**」をクリックします。

2. HYCU Webユーザーインターフェースにログオンし、次の手順を実行します。
   a. 「⚙ **管理**」をクリックして、「**ソフトウェアのアップグレード**」を選択します。
   b. 「ソフトウェアのアップグレード」ダイアログボックスの「リリース」タブで、HYCUの現行バージョンと選択可能なすべてのバージョンをチェックします。
   c. 選択可能なバージョンのリストから、HYCUをアップグレードするものを選択します。

      > 注「**新しいバージョンを確認してください**」リンクをクリックして、HYCUカスタマーサポートポータルで新しいバージョンが利用可能かどうかを確認することもできます。

   d. 「**ソフトウェアのアップグレード**」をクリックし、「**はい**」をクリックして、HYCUのアップグレードを確認します。
3. *HYCUがファイル共有保護に使用されている場合のみ*。HYCUインスタンスが存在するNutanixクラスターがHYCUに追加されていないか、適切なHYCU仮想アプライアンスイメージが同じNutanixクラスターに存在していない場合、HYCUインスタンスを次のようにアップグレードします。
   a. 既存のHYCUインスタンスを削除します。この実行方法の詳細については、"HYCUインスタンスの削除" ページ221を参照してください。
   b. 新しいHYCUインスタンスを最新バージョンのHYCUで作成します。この実行方法の詳細については、"HYCU Webユーザーインターフェースの使用によるHYCUインスタンスの作成" ページ220を参照してください。

HYCUからログアウトし、Nutanix Prism Webコンソールで次のようにアップグレードの進行状況を追跡できます。

- 古いHYCU Backup Controller仮想マシンはNutanix AHVクラスター上に残り、`<HYCUBackupControllerName>_version_<OldHYCUVersion>`に名前変更されます。
- アップグレードされた新しいHYCU Backup Controller仮想マシンは、古い仮想マシンに置き換えられます。
- アップグレードされたHYCU Backup Controller仮想マシンは、自動的に電源オンになります。

アップグレードプロセスが完了したら、HYCU Webユーザーインターフェースにログオンできます。

> ⚠ 重要 HYCU Webユーザーインターフェースに再度ログオンする前に、Webブラウザーでの Webページの強制リロードを必ず実行します。

HYCUが正常にアップグレードされたことを確認したら、古いHYCU Backup Controller仮想マシンをNutanix AHVクラスターから問題なく削除することができます。

Nutanix ESXiクラスター上のHYCUのアップグレード

Nutanix ESXiクラスター上のHYCUをアップグレードするには、次のいずれかの方法を選択できます。

アップグレード方法	説明
HYCU OVFパッケージのコンテンツライブラリへのインポートによる。	"HYCU OVFパッケージのコンテンツライブラリへのインポートによるHYCUのアップグレード" 下
HYCU OVFパッケージのvCenter Serverインベントリへの展開による。	"HYCU OVFパッケージのvCenter Serverインベントリへの展開によるHYCUのアップグレード" 次のページ

HYCUがファイル共有保護に使用される場合、HYCU Backup Controllerに接続されているHYCUインスタンスもアップグレードする必要があります。詳細については、"HYCUインスタンスのアップグレード" ページ244を参照してください。

前提条件

- HYCU Backup Controllerのスナップショットが Nutanix保護ドメインを使用して作成されている。詳細については、Nutanixの資料を参照してください。
- VMware vSphereを使用して作成されたすべてのHYCUが削除されている。

考慮事項

HYCUまたはHYCUインスタンスのアップグレード後に、一部のNutanix ESXiクラスター上で、MACアドレスの競合があることを示すエラーメッセージを受け取ることがあります。このメッセージは無視してもかまいません。

HYCU OVFパッケージのコンテンツライブラリへのインポートによるHYCUのアップグレード

> ⚠ 重要 このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

手順

1. vSphere Web Clientにログオンし、次の手順を実行します。
   a. HYCU OVFパッケージをインポートするコンテンツライブラリにナビゲートします。
   b. コンテンツライブラリを右クリックし、「**アイテムのインポート**」を選択します。「ライブラリアイテムのインポート」ダイアログボックスが開きます。
   c. 「ソース」セクションで、以下のようにOVFパッケージの場所を選択します。

URL	HYCU OVFパッケージのURLを指定します。
Local file	HYCU OVFパッケージのファイルシステムを参照します。 ⚠ 重要 ファイルシステムを参照するときには、`.ovf`ファイルと、OVFパッケージに関連した`.vmdk`ファイルの両方を必ず選択します。

「**OK**」をクリックします。
   d. 「宛先」セクションで、項目の名前と説明を入力し、「**OK**」をクリックします。

> ⚠ 重要 入力する項目名がHYCU OVFパッケージ名と一致していることを確認します。たとえば、hycu-4.5.0-3634。

2. HYCU Webユーザーインターフェースにログオンし、次の手順を実行します。
   a. 「⚙ 管理」をクリックして、「**ソフトウェアのアップグレード**」を選択します。
   b. HYCUの現在のバージョンと選択可能なすべてのバージョンを調べ、選択可能なバージョンのリストから、HYCUをアップグレードするものを選択します。

      > ヒント 各バージョンの横のアイコンは、HYCUアップグレードイメージの場所、CL(コンテンツライブラリ)、またはvC(vCenter Serverインベントリ)を示します。

   c. 「**アップグレード**」をクリックし、「**はい**」をクリックして、HYCUのアップグレードを確認します。

HYCUからログアウトし、Nutanix Prism Webコンソールで次のようにアップグレードの進行状況を追跡できます。

- 古いHYCU Backup Controller仮想マシンはNutanix ESXiクラスター上に残り、<*HYCUBackupControllerName*>_version_<*OldHYCUVersion*>に名前変更されます。
- アップグレードされた新しいHYCU Backup Controller仮想マシンは、古い仮想マシンに置き換えられます。
- アップグレードされたHYCU Backup Controller仮想マシンは、自動的に電源オンになります。

アップグレードプロセスが完了したら、HYCU Webユーザーインターフェースにログオンできます。

> ⚠ 重要 HYCU Webユーザーインターフェースに再度ログオンする前に、Webブラウザーでの Webページの強制リロードを必ず実行します。

HYCUが正常にアップグレードされたことを確認したら、古いHYCU Backup Controller仮想マシンをNutanix ESXiクラスターから問題なく削除することができます。

HYCU OVFパッケージのvCenter Serverインベントリへの展開によるHYCUのアップグレード

> ⚠ 重要 このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

手順

1. vSphere Web Clientにログオンし、次の手順を実行します。
   a. vCenter Serverを右クリックし、「**OVFテンプレートの展開...**」を選択します。「OVFテンプレートの展開」ダイアログボックスが開きます。
   b. 「テンプレートの選択」セクションで、以下のようにOVFパッケージの場所を選択します。

URL	HYCU OVFパッケージのURLを指定します。
Local file	HYCU OVFパッケージのファイルシステムを参照します。 ⚠ 重要 ファイルシステムを参照するときには、.ovfファイルと、

	OVFパッケージに関連した.vmdkファイルの両方を必ず選択します。

「**次へ**」をクリックします。

c. 「名前とロケーションの選択」セクションで、HYCU Backup Controller仮想マシンの名前を入力し、展開する場所を指定し、「**次へ**」をクリックします。

> ⚠ **重要** 入力する仮想マシン名がHYCU OVFパッケージ名と一致していることを確認します。たとえば、`hycu-4.5.0-3634`。

d. 「リソースの選択」セクションで、展開されたパッケージを実行する場所を選択し、「**次へ**」をクリックします。

e. 「詳細の確認」セクションで、パッケージの詳細を確認し、「**次へ**」をクリックします。

f. 「ストレージの選択」セクションで、展開されたパッケージのファイルを保存する場所を選択し、「**次へ**」をクリックします。

g. 「ネットワークの選択」セクションで、宛先ネットワークを選択し、「**次へ**」をクリックします。

h. 「テンプレートのカスタマイズ」セクションで、以下の値を入力します。

- *オプション*.仮想マシンのホスト名

  > 注 既定のホスト名は、HYCU仮想アプライアンスの展開中に自動的に生成されます。ホスト名の先頭は文字でなければならず、使用できるのは文字、数字、ハイフン(-) のみです。

- IPv4アドレス(例 :`10.1.100.1`)
- サブネットマスク(例 :`255.0.0.0`)
- 既定のゲートウェイ(例 :`10.1.1.1`)
- *オプション*.DNSサーバー(例 :`10.1.1.5`)
- *オプション*.検索ドメイン(例 :`domain.com`)

  > 注 ドメイン名の先頭は文字でなければならず、1つ以上のピリオドを含める必要があります。また、使用できるのは文字、数字、ハイフン(-) のみです。

「**次へ**」をクリックします。

i. 「終了可能」セクションで、データを確認し、「**終了**」をクリックします。

2. HYCU Webユーザーインターフェースにログオンし、次の手順を実行します。

a. 「⚙ **管理**」をクリックして、「**ソフトウェアのアップグレード**」を選択します。

b. HYCUの現在のバージョンと選択可能なすべてのバージョンを調べ、選択可能なバージョンのリストから、HYCUをアップグレードするものを選択します。

> 💡 **ヒント** 各バージョンの横のアイコンは、HYCUアップグレードイメージの場所、CL(コンテンツライブラリ) 、またはvC(vCenter Serverインベントリ) を示します。

c. 「**アップグレード**」をクリックし、「**はい**」をクリックして、HYCUのアップグレードを確認します。

HYCUからログアウトし、Nutanix Prism Webコンソールで次のようにアップグレードの進行状況を追跡できます。

- 古いHYCU Backup Controller仮想マシンはNutanix ESXiクラスター上に残り、*<HYCUBackupControllerName>*_version_*<OldHYCUVersion>*に名前変更されます。
- アップグレードされた新しいHYCU Backup Controller仮想マシンは、古い仮想マシンに置き換えられます。
- アップグレードされたHYCU Backup Controller仮想マシンは、自動的に電源オンになります。

アップグレードプロセスが完了したら、HYCU Webユーザーインターフェースにログオンできます。

> ⚠ **重要** HYCU Webユーザーインターフェースに再度ログオンする前に、Webブラウザーでの Webページの強制リロードを必ず実行します。

HYCUが正常にアップグレードされたことを確認したら、古いHYCU Backup Controller仮想マシンを Nutanix ESXiクラスターから問題なく削除することができます。

HYCUインスタンスのアップグレード

HYCU OVFパッケージがvCenter Serverコンテンツライブラリにインポートされ、その形式が以下のとおりである場合、HYCUアップグレード後に、Nutanix ESXiクラスターにあるHYCUインスタンスのアップグレードが自動的に開始します。

`hycu-<Version>-<Revision>`

たとえば、`hycu-4.5.0-3634`。

そのようにしない場合、HYCUインスタンスは次のように手動でアップグレードします。

1. 既存のHYCUインスタンスを削除します。この実行方法の詳細については、"HYCUインスタンスの削除" ページ221を参照してください。
2. 新しいHYCUインスタンスを最新バージョンのHYCUで作成します。この実行方法の詳細については、"HYCU Webユーザーインターフェースの使用によるHYCUインスタンスの作成" ページ220を参照してください。

> 📋 **注** 既定のユーザー資格情報を変更した場合、HYCUインスタンスのアップグレード後には、既定のオペレーティングシステムユーザー資格情報(ユーザー名 :**hycu**) のみを使用できます。パスワード :**hycu/4u**
>
> 環境の要件を満たすように後で変更することができます。

vSphere環境でのHYCUのアップグレード

vSphere環境内でHYCUをアップグレードするには、次のいずれかの方法を選択できます。

アップグレード方法	説明
HYCU OVFパッケージのコンテンツライブラリへのインポートによる。	"HYCU OVFパッケージのコンテンツライブラリへのインポートによるHYCUのアップグレード" 次のページ
HYCU OVFパッケージのvCenter Serverインベントリへの展開による。	"HYCU OVFパッケージのvCenter Serverインベントリへの展開によるHYCUのアップグレード" ページ246

前提条件

- vSphereユーザーとして、必要なアップグレード特権を持っている。アップグレード特権の詳細については、“vSphereユーザーへの特権の割り当て” ページ269を参照してください。
- *HYCU OVFパッケージをコンテンツライブラリにインポートする場合* :コンテンツライブラリがvSphere (Web) Clientで作成されている。

考慮事項

- *HYCU Backup Controllerが分散スイッチに接続されているときにHYCUをアップグレードする場合* : アップグレード後は、アップグレードされたHYCU Backup Controller上で構成されたポートは、古いHYCU Backup Controller上で構成された分散スイッチポートとは異なるものになります。アップグレードされたHYCU Backup Controllerで以前と同じポートを使用する必要がある場合は、古いHYCU Backup Controllerのポートを削除してから、新しいHYCU Backup Controller設定でポート番号を変更します。この実行方法の詳細については、VMwareの資料を参照してください。
- HYCUのアップグレード後に、一部のvSphere環境で、MACアドレスの競合があることを示すエラーメッセージを受け取ることがあります。このメッセージは無視してもかまいません。
- HYCU Backup ControllerをVMware Virtual SAN (vSAN)データベースに展開することは推奨されません。ただし、そのようにしている場合、HYCUをアップグレードする前にHYCUカスタマーサポートにご連絡ください。

HYCU OVFパッケージのコンテンツライブラリへのインポートによるHYCUのアップグレード

> ⚠ 重要 このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

手順

1. vSphere Web Clientにログオンし、次の手順を実行します。
   a. HYCU OVFパッケージをインポートするコンテンツライブラリにナビゲートします。
   b. コンテンツライブラリを右クリックし、「**アイテムのインポート**」を選択します。「ライブラリアイテムのインポート」ダイアログボックスが開きます。
   c. 「ソース」セクションで、以下のようにOVFパッケージの場所を選択します。

URL	HYCU OVFパッケージのURLを指定します。
Local file	HYCU OVFパッケージのファイルシステムを参照します。 ⚠ 重要 ファイルシステムを参照するときには、`.ovf`ファイルと、OVFパッケージに関連した`.vmdk`ファイルの両方を必ず選択します。

「**OK**」をクリックします。
   d. 「宛先」セクションで、項目の名前と説明を入力し、「**OK**」をクリックします。

> ⚠ 重要 入力する項目名がHYCU OVFパッケージ名と一致していることを確認します。たとえば、hycu-4.5.0-3634。

2. HYCU Webユーザーインターフェースにログオンし、次の手順を実行します。
   a. 「⚙ 管理」をクリックして、「**ソフトウェアのアップグレード**」を選択します。
   b. 「ソフトウェアのアップグレード」ダイアログボックスで、HYCUの現行バージョンと選択可能なすべてのバージョンをチェックします。
   c. 選択可能なバージョンのリストから、HYCUをアップグレードするものを選択します。

      > 💡 ヒント 各バージョンの横のアイコンは、HYCUアップグレードイメージの場所、CL(コンテンツライブラリ)、またはvC(vCenter Serverインベントリ)を示します。

   d. 「**アップグレード**」をクリックし、「**はい**」をクリックして、HYCUのアップグレードを確認します。

HYCUからログアウトし、vSphere (Web) Clientで次のようにアップグレードの進行状況を追跡できます。

- 古いHYCU Backup Controller仮想マシンはvSphere環境に残り、*<HYCUBackupControllerName>*_version_*<OldHYCUVersion>*に名前変更されます。
- アップグレードされた新しいHYCU Backup Controller仮想マシンは、古い仮想マシンに置き換えられます。
- アップグレードされたHYCU Backup Controller仮想マシンは、自動的に電源オンになります。

アップグレードプロセスが完了したら、HYCU Webユーザーインターフェースにログオンできます。

> ⚠ 重要 HYCU Webユーザーインターフェースに再度ログオンする前に、Webブラウザーでの Webページの強制リロードを必ず実行します。

HYCUが正常にアップグレードされたことを確認したら、古いHYCU Backup Controller仮想マシンをvSphere環境から問題なく削除することができます。

HYCU OVFパッケージのvCenter Serverインベントリへの展開によるHYCUのアップグレード

> ⚠ 重要 このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

手順

1. vSphere Web Clientにログオンし、次の手順を実行します。
   a. vCenter Serverを右クリックし、「**OVFテンプレートの展開...**」を選択します。「OVFテンプレートの展開」ダイアログボックスが開きます。
   b. 「テンプレートの選択」セクションで、以下のようにOVFパッケージの場所を選択します。

URL	HYCU OVFパッケージのURLを指定します。
Local file	HYCU OVFパッケージのファイルシステムを参照します。

> ⚠ 重要 ファイルシステムを参照するときには、.ovfファイルと、OVFパッケージに関連した.vmdkファイルの両方を必ず選択します。

「**次へ**」をクリックします。

c. 「名前とロケーションの選択」セクションで、HYCU Backup Controller仮想マシンの名前を入力し、展開する場所を指定し、「**次へ**」をクリックします。

> ⚠ 重要 入力する仮想マシン名がHYCU OVFパッケージ名と一致していることを確認します。たとえば、hycu-4.5.0-3634。

d. 「リソースの選択」セクションで、展開されたパッケージを実行する場所を選択し、「**次へ**」をクリックします。

e. 「詳細の確認」セクションで、パッケージの詳細を確認し、「**次へ**」をクリックします。

f. 「ストレージの選択」セクションで、展開されたパッケージのファイルを保存する場所を選択し、「**次へ**」をクリックします。

g. 「ネットワークの選択」セクションで、宛先ネットワークを選択し、「**次へ**」をクリックします。

> ⚠ 重要 仮想NICオプションにはvSphere分散スイッチ(dvSwitch) を選択しないようにしてください。

h. 「テンプレートのカスタマイズ」セクションで、以下の値を入力します。

- *オプション* .仮想マシンのホスト名

  > 注 既定のホスト名は、HYCU仮想アプライアンスの展開中に自動的に生成されます。ホスト名の先頭は文字でなければならず、使用できるのは文字、数字、ハイフン(-) のみです。

- IPv4アドレス(例 :10.1.100.1)
- サブネットマスク(例 :255.0.0.0)
- 既定のゲートウェイ(例 :10.1.1.1)
- *オプション* .DNSサーバー(例 :10.1.1.5)
- *オプション* .検索ドメイン(例 :domain.com)

  > 注 ドメイン名の先頭は文字でなければならず、1つ以上のピリオドを含める必要があります。また、使用できるのは文字、数字、ハイフン(-) のみです。

「**次へ**」をクリックします。

i. 「終了可能」セクションで、データを確認し、「**終了**」をクリックします。

2. HYCU Webユーザーインターフェースにログオンし、次の手順を実行します。

a. 「⚙ **管理**」をクリックして、「**ソフトウェアのアップグレード**」を選択します。

b. 「ソフトウェアのアップグレード」ダイアログボックスで、HYCUの現行バージョンと選択可能なすべてのバージョンをチェックします。

c. 選択可能なバージョンのリストから、HYCUをアップグレードするものを選択します。

> ヒント 各バージョンの横のアイコンは、HYCUアップグレードイメージの場所、CL(コンテンツライブラリ)、またはvC(vCenter Serverインベントリ)を示します。

d. 「**アップグレード**」をクリックし、「**はい**」をクリックして、HYCUのアップグレードを確認します。

HYCUからログアウトし、vSphere (Web) Clientで次のようにアップグレードの進行状況を追跡できます。

- 古いHYCU Backup Controller仮想マシンはvSphere環境に残り、*<HYCUBackupControllerName>*_version_*<OldHYCUVersion>*に名前変更されます。
- アップグレードされた新しいHYCU Backup Controller仮想マシンは、古い仮想マシンに置き換えられます。
- アップグレードされたHYCU Backup Controller仮想マシンは、自動的に電源オンになります。

アップグレードプロセスが完了したら、HYCU Webユーザーインターフェースにログオンできます。

> ⚠ 重要 HYCU Webユーザーインターフェースに再度ログオンする前に、Webブラウザーでの Webページの強制リロードを必ず実行します。

HYCUが正常にアップグレードされたことを確認したら、古いHYCU Backup Controller仮想マシンをvSphere環境から問題なく削除することができます。

HYCU修正プログラムの適用

HYCUカスタマーサポートからHYCU修正プログラムを受け取ったら、現在の製品バージョンに適用できます。修正プログラムは、インストールされている互換性のある製品バージョンにのみ適用できます。たとえば、1.2.3-4567というラベルの付いた修正プログラムは製品バージョン1.2.3に適用できますが、1.2.4-5678というラベルの付いた修正プログラムは適用できません。

> 注 各HYCU修正プログラムは、問題の累積セットに対処します。

前提条件

- *修正プログラムをHYCU Backup Controllerに適用する場合* .HYCU Backup Controllerアクティビティが保留中である。この実行方法の説明については、"電源オプションの設定" ページ231を参照してください。
- 中止したくないジョブを終了している(修正プログラムアプリケーションプロセスは現在実行中のすべてのジョブを中止します)。これは、ジョブの実行ステータスでジョブリストをフィルタリングすることで確認できます。説明については、"データのフィルタリング" ページ177を参照してください。
- *修正プログラムをHYCU インスタンスに適用する場合* .同じ修正プログラムが、対応するHYCU Backup Controllerに適用されている。
- *シェルスクリプトを使用して修正プログラムを適用する場合* .修正プログラムを適用する予定のHYCU仮想マシンの管理ユーザー権限を持つ、オペレーティングシステムユーザーアカウントの資格情報が分かっている。

> ⚠ 重要 HYCUカスタマーサポートにより特に断りがない限り、すべてのHYCU仮想マシンに同じ修正プログラム(HYCU Backup Controller、HYCU インスタンス、およびHYCU Manager)を適用する必要があります。

考慮事項

- HYCU Backup Controllerに適用する修正プログラムは、HYCU インスタンスまたはHYCU Managerに自動的に適用されることはありません。
- *修正プログラムをHYCU Backup ControllerまたはHYCU Managerに適用する場合*、修正プログラムが適用されているHYCU仮想マシンのHYCU Webユーザーインターフェースにログオンしているユーザーは、プロセスの完了後にWebブラウザーでWebユーザーインターフェースページの強制リロードを実行する必要があります。

推奨事項

ホットフィックスをHYCU Backup Controllerに適用する前に、HYCU Backup Controllerをバックアップします。説明については、"仮想マシンのバックアップ" ページ85を参照してください。

HYCU修正プログラムを適用できます。

- HYCU Webユーザーインターフェースから

  HYCU Backup Controller、HYCU インスタンス、またはHYCU Managerに修正プログラムを適用する場合は、この方法を使用します。説明については、"HYCU Webユーザーインターフェースを使用した修正プログラムの適用" 下を参照してください。

- シェルスクリプトを使用

  HYCU Webユーザーインターフェースにログオンできない場合は、この方法を使用します。説明については、"シェルスクリプトを使用した修正プログラムの適用" ページ251を参照してください。

HYCU Webユーザーインターフェースを使用した修正プログラムの適用

HYCU Webユーザーインターフェースから、次の手順を使用して、任意の種類のHYCU仮想マシンに修正プログラムを適用できます。

- "修正プログラムのHYCU Backup ControllerまたはHYCU Managerへの適用" 下
- "ホットフィックスのHYCU インスタンスへの適用" 次のページ

修正プログラムのHYCU Backup ControllerまたはHYCU Managerへの適用

手順

1. HYCU Webユーザーインターフェースにログオンします。
2. 「⚙ **管理**」をクリックして、「**ソフトウェアのアップグレード**」を選択します。
3. 「Software Upgrade」ダイアログボックスで、「**Hotfixes**」タブをクリックします。
4. 「Hotfix Label」列で、目的の修正プログラムのパッケージがすでにHYCU Backup ControllerまたはHYCU Managerに追加されているかどうかを確認し、以下のいずれかを実行します。

- 修正プログラムラベルが存在しない場合には、次の手順を実行します。
  a. 「**＋ 追加**」をクリックします。
  b. 「Hotfixを追加する」ダイアログボックスで、「**参照**」をクリックします。修正プログラムパッケージ(ZIP形式) を参照して選択し、「**開く**」をクリックします。
  c. 「**Hotfixを追加する**」をクリックします。
- 修正プログラムのラベルが存在する場合、それを選択します。

> ヒント「**情報**」をクリックして、修正プログラムが解決する問題のリストを確認します。

5. 「**Hotfixを適用**」をクリックします。
6. 表示されたデジタル指紋が、HYCUカスタマーサポートから提供されたものと一致することを確認します。
7. 「**はい**」をクリックして、修正プログラムアプリケーションプロセスを開始します。HYCU Webユーザーインターフェースから自動的にログオフし、Webユーザーインターフェースのログオンページで修正プログラム適用の進行状況を追跡できます。
8. プロセスが完了したら、WebブラウザーでHYCU Webユーザーインターフェースページの強制リロードを実行します。
9. *修正プログラムをHYCU Backup Controllerに適用した場合のみ*。以下を実行します。
   a. HYCU Webユーザーインターフェースにログオンします。
   b. HYCU Backup Controllerのアクティビティを再開します。この実行方法の説明については、"電源オプションの設定" ページ231を参照してください。

修正プログラムが適用されていないときに、追加された修正プログラムパッケージを削除するには、「Hotfixes」タブの「ソフトウェアのアップグレード」ダイアログボックスで、追加された修正プログラムパッケージのリストからエントリを選択し、「**削除**」をクリックします。

ホットフィックスのHYCU インスタンスへの適用

手順

1. HYCU Webユーザーインターフェースにログオンします。
2. 「**管理**」をクリックして、「**インスタンス**」を選択します。
3. 「インスタンス」ダイアログボックスで、目的のHYCU インスタンスを選択し、「**Hotfixes**」をクリックします。
4. 「Hotfixラベル」列で、目的の修正プログラムのパッケージがすでにHYCU インスタンスに追加されているかどうかを確認し、以下のいずれかを実行します。
   - 修正プログラムラベルが存在しない場合には、次の手順を実行します。
     a. 「**＋ 追加**」をクリックします。
     b. 「Hotfixを追加する」ダイアログボックスで、「**参照**」をクリックします。修正プログラムパッケージ(ZIP形式) を参照して選択し、「**開く**」をクリックします。
     c. 「**Hotfixを追加する**」をクリックします。

> 注 HYCU インスタンスに適用される各修正プログラムは、最初に対応するHYCU Backup Controllerにアップロードされます。

- 修正プログラムのラベルが存在する場合、それを選択します。

> ヒント 「 情報 」をクリックして、修正プログラムが解決する問題のリストを確認します。

5. 「**Hotfixを適用**」をクリックします。
6. 表示されたデジタル指紋が、HYCUカスタマーサポートから提供されたものと一致することを確認します。
7. 「**はい**」をクリックして、修正プログラムアプリケーションプロセスを開始します。「インスタンス」ダイアログボックスのHYCU インスタンスステータスアイコンがグレー表示に変わり、進行中のプロセスであることを示します。

   「ジョブ」パネルで対応するジョブのステータスを確認することで、プロセスの進行状況を追跡できます。修正プログラムが適用されると、HYCU インスタンスステータスアイコンが緑色に変わります。

修正プログラムが適用されていないときに、追加された修正プログラムパッケージを削除するには、「Hotfixes」ダイアログボックスで、追加された修正プログラムパッケージのリストからエントリを選択し、「 **削除** 」をクリックします。

シェルスクリプトを使用した修正プログラムの適用

手順

1. 仮想化環境の管理に使用しているWebユーザーインターフェースにログオンし、修正プログラムを適用する予定のHYCU仮想マシンに接続します。
2. 管理者ユーザー権限があるユーザーアカウントでオペレーティングシステムにログオンします。
3. コマンドシェルを開いて、以下のコマンドを実行します。

   ```
   cd /opt/grizzly/bin/
   ```

4. 以下のコマンドを実行して、HYCU仮想マシンにすでに追加されている修正プログラムパッケージのリストを取得します。

   ```
   sudo ./HycuPatch.sh -list_patches
   ```

5. 目的の修正プログラムのラベルがリストにない場合は、次の手順に従います。
   a. 修正プログラムパッケージの内容を(ZIP形式で) 抽出します。パッケージには、メイン修正プログラムファイル、インストールの説明、およびデジタル指紋が含まれています。
   b. `/usr/bin/cksum`および`/usr/bin/md5sum`コマンドを使用して、メイン修正プログラムファイルのデジタル指紋がHYCUカスタマーサポートによって指定されたものと一致することを確認します。
   c. アーカイブされたTAR(`.tar.gz`) 形式のメイン修正プログラムファイルを、HYCU仮想マシンの次のディレクトリにコピーします。

      ```
      /hycudata/opt/grizzly/hotfixes
      ```

> **ヒント** 以下のコマンドを実行して、修正プログラムが解決する問題のリストを確認します。
>
> ```
> sudo ./HycuPatch.sh -patch_info <HotfixLabel>
> ```

6. 以下のコマンドを実行して、修正プログラムをHYCU仮想マシンに適用します。

   ```
   sudo ./HycuPatch.sh -apply_patch <HotfixLabel>
   ```

7. *修正プログラムをHYCU Backup Controllerに適用した場合のみ*。以下を実行します。
   a. HYCU Webユーザーインターフェースにログオンします。
   b. HYCU Backup Controllerのアクティビティを再開します。この実行方法の説明については、"電源オプションの設定" ページ231を参照してください。

バックアップの期限切れ指定

HYCUは、ポリシーでバックアップデータに設定された保持期間に従って、バックアップを自動的に期限切れにします。ただし、データの復元に使用したくない復元ポイント(バックアップ)がある場合は、いつでも手動で期限切れにできます。

復元ポイントは、指定されたポイントインタイムでバックアップされたデータを表します。復元ポイントには、バックアップ、コピー、スナップショット、およびアーカイブの1つ以上の層を含めることができ、それらを個別に期限切れとしてマークできます。

> **ヒント** バックアップ、コピー、スナップショット、アーカイブの有効期限は、「仮想マシン」、「アプリケーション」、「共有フォルダ」、「ボリュームグループ」パネルの「詳細ビュー」で確認できます。詳細については、"エンティティ詳細の表示" ページ174を参照してください。

考慮事項

- 最新の復元ポイントが期限切れとしてマークされている場合、次のバックアップは完全バックアップになります。
- 復元ポイントが期限切れとしてマークされると、選択された復元ポイントのステータスが失敗でない限り、同じバックアップチェーン内の以降の増分バックアップも期限切れとしてマークされます。この場合、選択された復元ポイントのみが期限切れになり、バックアップチェーン全体はそのようにはなりません。
- バックアップとコピーの層は、必ず一緒に期限切れになります。

バックアップの自動での期限切れ指定

いずれかの層が保持期間に達すると、HYCU Webユーザーインターフェースでグレー表示されます。このような層は、バックアップチェーンの最後の層が保存期間に達すると期限切れになります。つまり、このデータは、バックアップチェーン内のすべての層が期限切れになるまで、HYCUまたはターゲットから削除されません。ただし、アーカイブ層を含む復元ポイントがある場合、残りのバックアップチェーンが期限切れになっても、この復元ポイントは保持されます。さらに、この復元ポイントが増分バックアップの場合は、完全バックアップに変更されます。

考慮事項

- ポリシーの保持期間を変更しても、既存のバックアップには影響を与えません。
- HYCUでは、保護されていないエンティティ(ポリシーが割り当てられていない、またはポリシーが削除されたエンティティ) の最後のバックアップチェーンが自動的に期限切れになるのに対し、保護されているエンティティの最後のバックアップチェーンが自動的に期限切れになることはありません。

バックアップの手動での期限切れ指定

管理者は、以下のいずれかを期限切れとしてマークできます。

- 全体の復元ポイント：

  すべての層が期限切れとしてマークされていることを確認します。

- 1つ以上の層：

  期限切れにする層のみが期限切れとしてマークされていることを確認します。

考慮事項

- 期限切れ指定アクションは元に戻すことはできません。
- バックアップとコピーを期限切れとしてマークすると、関連するスナップショットがあれば、それも期限切れになります。
- *仮想マシンのバックアップの一環として、およびポリシーを直接割り当てることで、バックアップされているボリュームグループのバックアップを期限切れにする場合のみ。*バックアップを有効期限切れにする前に、そのボリュームグループがアタッチされている可能性がある仮想マシンで、そのバックアップデータが使用されていないことを確認します。

古いバックアップを期限切れにするエンティティに応じて、次のいずれかのパネルにアクセスします。

- 「仮想マシン」パネルへのアクセス

  ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

- 「アプリケーション」パネルへのアクセス

  「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

- 「共有フォルダ」パネルへのアクセス

  「共有フォルダ」パネルにアクセスするには、ナビゲーションペインで、「**共有フォルダ**」をクリックします。

- 「ボリュームグループ」パネルのアクセス

  「ボリュームグループ」パネルにアクセスするには、ナビゲーションペインで、「**ボリュームグループ**」をクリックします。

手順

1. 「仮想マシン」、「アプリケーション」、「共有フォルダ」、または「ボリュームグループ」パネルで、古いバックアップを期限切れにするエンティティを選択します。
2. 画面の下部に表示される「詳細ビュー」で、期限切れとしてマークする復元ポイントを選択します。
3. 「**有効期限を切る**」をクリックします。「有効期限を切る」ダイアログボックスが表示されます。
4. 期限切れとしてマークする層を選択します。
   - **バックアップとコピー**
   - **スナップショット**
   - **アーカイブ**

   有効期限に使用できる層は、ポリシーで設定したオプションに基づいています。すべての層を選択することにより、復元ポイント全体を期限切れとしてマークします。
5. 「**はい**」をクリックして、選択した層を期限切れとマークすることを確認します。

> 注 復元ポイント全体を期限切れとしてマークすると、バックアップステータスは期限切れ(「○」)として表示されます。これは、復元ポイントをデータの復元に使用できなくなったことを示します。

HYCUのクリーニングプロセスにより、期限切れのバックアップがターゲットから削除されます。

HYCUの削除

環境からHYCUを削除する場合、追加のクリーンアップタスクも実行する必要があります。

HYCUを削除するには、次の手順に従います。

1. HYCUにログオンし、すべてのエンティティからポリシーの割り当てを次のように解除します。
   - 仮想マシンからポリシーを割り当て解除するには、次のようにします。
     a. ナビゲーションペインで、「**仮想マシン**」をクリックします。
     b. すべての仮想マシンを選択し、「 」「**ポリシー**」をクリックします。
     c. 「**割り当て解除**」をクリックします。
     d. 「**はい**」をクリックして、選択した仮想マシンからポリシーを割り当て解除することを確認します。
   - アプリケーションからポリシーを割り当て解除するには、次のようにします。
     a. ナビゲーションペインで、「**アプリケーション**」をクリックします。
     b. すべての検出されたアプリケーションを選択し、「**ポリシー**」をクリックします。
     c. 「**割り当て解除**」をクリックします。
     d. 「**はい**」をクリックして、選択したアプリケーションからポリシーを割り当て解除することを確認します。
   - ファイル共有からポリシーを割り当て解除するには、次のようにします。

a. ナビゲーションペインで、「**共有フォルダ**」をクリックします。

b. すべてのファイル共有を選択し、「 」「**ポリシー**」をクリックします。

c. 「**割り当て解除**」をクリックします。

d. 「**はい**」をクリックして、選択したファイル共有からポリシーを割り当て解除することを確認します。

- ボリュームグループからポリシーを割り当て解除するには、次のようにします。

a. ナビゲーションペインで、「**ボリュームグループ**」をクリックします。

b. すべてのボリュームグループを選択し、「 」「**ポリシー**」をクリックします。

c. 「**割り当て解除**」をクリックします。

d. 「**はい**」をクリックして、選択したボリュームグループからポリシーを割り当て解除することを確認します。

2. *HYCUがファイル共有保護用に使用された場合のみ*。以下を実行します。

a. 既存のHYCUインスタンスを削除します。説明については、"HYCUインスタンスの削除" ページ221を参照してください。

b. HYCUによって作成されたファイルサーバースナップショットを削除します。これを実行するには、HYCU Backup Controller上で、`/opt/grizzly/bin/HycuCleanup.pl`スクリプトを次のように実行します。

```
sudo perl HycuCleanup.pl -c <FileServer> -u <Username> -p
<Password> -dnfs -all
```

この場合、*<FileServer>*はファイルサーバーの名前であり、次の形式です：`https://<ServerName>:<Port>`。

> ⚠ **重要** このコマンドを実行すると、名前が`hycu-`で始まるすべてのファイルサーバースナップショットも削除されます(大文字と小文字は区別されません)。

3. *Nutanixクラスターの場合*：HYCU Backup Controllerで、`/opt/grizzly/bin/HycuCleanup.pl`スクリプトを次のように実行します。

- HYCUによって作成された仮想マシンおよびボリュームグループのスナップショットを削除するには、次のようにします。

```
sudo perl HycuCleanup.pl -c <NutanixCluster> -u <Username> -p
<Password> -dvms -all
```

```
sudo perl HycuCleanup.pl -c <NutanixCluster> -u <Username> -p
<Password> -dvgs -all
```

これらの場合、*<NutanixCluster>*はNutanixクラスターの名前であり、次の形式です：`https://<ServerName>:<Port>`。

> ⚠ **重要** これらのコマンドを実行すると、名前がIPアドレスで始まる、Nutanix REST API v3を使用して作成されたすべてのサードパーティスナップショットも削除されます。

- HYCUによって作成されたボリュームグループを削除するには、次のようにします。

```
sudo perl HycuCleanup.pl -c <NutanixCluster> -u <Username> -p
<Password> -dvg -all
```

この場合、<*NutanixCluster*>はNutanixクラスターの名前であり、次の形式です :https://<*ServerName*>:<*Port*>。

> ⚠ 重要 このコマンドを実行すると、名前がHYCU-で始まる、Nutanix REST API v3を使用して作成されたすべてのボリュームグループも削除されます(大文字と小文字は区別されません) 。

4. ターゲットからデータを削除します。これを実行するには、各ターゲット上で、bkpctrlフォルダを削除します。
5. Nutanix Prism Webコンソールまたはvsphere (Web) Clientにログオンし、HYCU Backup Controller仮想マシンを削除します。仮想マシンを削除する方法の詳細については、NutanixまたはVMwareの資料を参照してください。

第12章

データ保護環境の調整

データ保護環境用にHYCUをカスタマイズするために「⚙ **管理**」メニューから実行する管理タスクで、通常は正常な管理を十分行うことができます。ただし、組織の要件によっては、最適なパフォーマンス、より高いセキュリティレベル、または外部アプリケーションとの相互作用、およびさらに幅広いHYCUオプションを活用するために、追加の管理タスクを実行する必要があります。

目的	手順
SSHを使用してHYCU Backup Controller仮想マシンにアクセスします。	“SSHを使用したHYCU Backup Controller仮想マシンへのアクセス” 次のページ
HTTPS for WinRM接続を有効にします。	“HTTPS for WinRM接続の有効化” ページ260
HYCU用にFIPS準拠モードを構成します。	“HYCU用のFIPSモードの構成” ページ260
LDAPS認証をセットアップします。	“LDAPS認証のセットアップ” ページ262
2要素認証をセットアップします。	“2要素認証のセットアップ” ページ262
APIキーを管理します。	“APIキーの管理” ページ263
FIDO認証システムを管理します。	“FIDO認証システムの管理” ページ264
SMTP接続を保護します。	“SMTP接続の保護” ページ265
複数のネットワークを使用するようにHYCUをセットアップします。	“複数のネットワークを使用するHYCUのセットアップ” ページ266
HYCU仮想ディスクのサイズを増やします。	“HYCU仮想ディスクのサイズの増分” ページ268
必要なバックアップ特権をvSphereユーザーに割り当てます。	“vSphereユーザーへの特権の割り当て” ページ269
HYCU REST APIを使用してタスクを自動化します。	“HYCU REST APIエクスプローラーの使用” ページ271
hyCLIを使用します。	“コマンドラインインターフェースの使用” ページ272
プレ/ポストスクリプトを使用して、バックアップと復元が実行される前と後に必要なアクションを実行します。	“プレ/ポストスクリプトの使用” ページ272

SSHを使用したHYCU Backup Controller仮想マシンへのアクセス

HYCU Webユーザーインターフェースまたはコマンドラインユーザーインターフェース(hyCLI) を使用して、HYCU Backup Controllerのほとんどの管理タスクを実行できます。SSHを使用する必要がある2つの例外は、HYCUアプリケーションサーバー(Grizzlyサーバー) またはアプライアンス全体の再起動です。

> ⚠ 重要 SSHを使用してHYCUアプリケーションサーバーまたはアプライアンス全体の再起動以外のタスクを実行することはお勧めしません。

HYCU仮想アプライアンスを展開したら、SSHを使用したHYCU Backup Controller仮想マシンへのアクセスに、以下の既定の資格情報を使用できます。

ユーザー名： **hycu**

パスワード： **hycu/4u**

既定のSSHパスワードの変更

セキュリティ上の目的で、既定のSSHパスワードは変更することを強くお勧めします。これを実行するには、次の手順に従います。

1. HYCU Backup Controller仮想マシンへのリモートセッションを開きます。

   ```
   ssh hycu@<HYCUBackupControllerIPAddress>
   ```

   要求されたら、既定のパスワードを入力します。

2. hycuユーザーの次のパスワードを変更します。

   ```
   passwd
   ```

   要求されたら、既定のパスワードを再度入力し、次に新しいパスワードを入力して確認します。

SSH公開キー認証の構成

SSH公開キーをHYCUに追加し、HYCU Backup Controllerへのアクセスに使用することで、お使いのデータ保護環境にセキュリティの層を追加し、SSHパスワード認証以上の安全性を実現できます。ファイル共有保護にHYCUを使用し、HYCU Backup ControllerにアクセスするためのSSH公開キー認証を構成している場合、HYCUインスタンスへのアクセスにも同じSSH公開キーを使用できます。新たなセキュリティを使用するため、SSHパスワード認証を無効にすることもできます。

制限事項

サポートされているSSHキーの種類はRSA、ECDSA、Ed25519です。

> 「SSHアクセス」ダイアログボックスへのアクセス
>
> 「SSH認証」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**SSH認証**」を選択します。

手順

1. 「SSH認証」ダイアログボックスで「**＋ 公開鍵を追加**」をクリックします。
2. SSH公開キーの名前とSSH公開キーを入力します。
3. 「**保存**」をクリックします。

SSH公開キーが表に追加されます。追加された各キーについて、名前、作成日、キーのフィンガープリントが表示されます。

既存のいずれかのSSH公開キーを選択し、「**削除**」をクリックして削除することもできます。

SSH公開キー認証の構成後にSSHパスワード認証を無効にするには、「**パスワード認証を許可する**」スイッチを無効にしてから「**保存**」をクリックします。

SSHアクセスの無効化

SSHアクセスはいつでも無効にできます。これを実行するには、次の手順に従います。

1. HYCU Backup Controller仮想マシンへのリモートセッションを開きます。

   ```
   ssh hycu@<HYCUBackupControllerIPAddress>
   ```

   要求されたら、hycuユーザーのパスワードを入力します。

2. SSH サービスをシャットダウンします。

   ```
   sudo systemctl stop sshd.service
   ```

   要求されたら、hycuユーザーのパスワードを入力します。

3. SSHサービスを無効にします。

   ```
   sudo systemctl disable sshd.service
   ```

   要求されたら、hycuユーザーのパスワードを入力します。

この手順を実行したら、SSH接続は無効になります。SSHを再有効化するには、各ハイパーバイザーのコンソールを介してHYCU Backup Controller仮想マシンに接続する必要があります。

HYCUアプリケーションサーバーの管理

HYCUアプリケーションサーバーを管理するには、次の手順に従います。

1. HYCU Backup Controller仮想マシンへのリモートセッションを開きます。

   ```
   ssh hycu@<HYCUBackupControllerIPAddress>
   ```

   要求されたら、hycuユーザーのパスワードを入力します。

2. HYCUアプリケーションサーバーで目的の操作を実行します。

   ```
   sudo service grizzly {start | stop | restart}
   ```

   要求されたら、hycuユーザーのパスワードを入力します。

> ⚠ 重要 PostgreSQLサーバーを再起動する予定がある場合は、PostgreSQLサーバーの再起動前にHYCUアプリケーションサーバーを停止し、再起動後に開始するようにします。

HTTPS for WinRM接続の有効化

セキュリティのレイヤーをさらに追加する場合は、仮想マシンへのHTTPS for WinRM接続を使用するようにHYCUを構成できます。

手順

HTTPS for WinRM接続を有効にする各仮想マシンに対して、以下を実行します。

1. WinRM for HTTPSを構成します。この実行方法の詳細については、Microsoftの資料を参照してください。
2. HYCUで証明書を構成します。
   - プライベート認証局によって署名された証明書でWinRMが構成されている場合、CA証明書/チェーンをHYCUにインポートします。詳細については、"カスタム証明書のインポート" ページ235を参照してください。
   - WinRMが自己署名証明書で構成されている場合、HYCU Backup Controllerへのリモートセッションを開き、以下を実行します。
     a. `add_certificate.sh`スクリプトを実行します。

        ```
        sudo /opt/grizzly/bin/add_certificate.sh <Hostname>
        ```

        この場合、*<Hostname>*はHTTPS接続を確立する仮想マシンのホスト名です。
     b. 信頼ストアにアクセスするためのパスワードを入力します。既定のパスワードは**hycu/4u**です。
     c. 証明書が有効であることと、表示された証明書情報が仮想マシン上の証明書情報と一致することを確認し、**y**を入力してから**Enter**を押して、証明書を受け入れます。そうでない場合、**n**と入力し、**Enter**を押して、証明書を拒否します。

HYCU用のFIPSモードの構成

HYCUは、暗号化モジュールのセキュリティ要件を確立するFederal Information Processing Standards(FIPS) に準拠して動作するように構成できます(暗号化アルゴリズムと暗号化キーの生成方法を使用できます) 。

ビジネスの性質に応じて、HYCUのFIPSモードは有効または無効にできます。FIPSモードが有効かどうか(既定では無効) を確認するには、HYCU Backup Controllerへのリモートセッションを開き、rootユーザーまたはsudoを使用して、次のコマンドを実行します。

```
/opt/grizzly/bin/enable_fips.sh --status
```

制限事項

FIPSモードを有効にした場合、以下のような制限が適用されます。

- SMBターゲットは、データを保存するためには使用できません。
- アプリケーションを検出できないため、保護できません。
- 個々のファイルは復元できません。
- Windows物理マシンは保護できません。

考慮事項

- *HYCUがファイル共有保護に使用されている場合のみ*。各HYCUインスタンスに対して個別に(HYCU Backup Controllerに依存せず) FIPSモードを有効にする必要があります。
- HYCUをアップグレードすると、FIPSモードが無効になります。必要な場合は、必ず再有効化してください。

HYCU用のFIPSモードの有効化

手順

HYCU Backup Controllerへのリモートセッションを開き、ルートユーザーとしてまたはsudoを使用して、次の手順を実行します。

1. HYCUアプリケーションサーバーを停止します。

   ```
   systemctl stop grizzly.service
   ```

2. FIPS準拠モードを有効にします。

   ```
   /opt/grizzly/bin/enable_fips.sh
   ```

3. HYCU Backup Controllerを再起動します。

   ```
   再起動
   ```

HYCU用のFIPSモードの無効化

手順

HYCU Backup Controllerへのリモートセッションを開き、ルートユーザーとしてまたはsudoを使用して、次の手順を実行します。

1. HYCUアプリケーションサーバーを停止します。

   ```
   systemctl stop grizzly.service
   ```

2. FIPS準拠モードを無効にします。

   ```
   /opt/grizzly/bin/enable_fips.sh -d
   ```

3. HYCU Backup Controllerを再起動します。

   ```
   再起動
   ```

LDAPS認証のセットアップ

もう1段階の保護を追加してデータの機密性を確実にするには、セキュアなユーザー認証のためにLDAP over SSL(LDAPS) を使用するようにHYCUを構成できます。この認証が機能するには、LDAPSサーバー証明書をHYCUにインポートする必要があります。

手順

1. LDAPSサーバー証明書をHYCUにインポートします。
   - プライベート認証局によって署名された証明書でSMTPサーバーが構成されている場合、CA証明書/チェーンをHYCUにインポートします。詳細については、"カスタム証明書のインポート" ページ235を参照してください。
   - SMTPサーバーが自己署名証明書で構成されている場合、HYCU Backup Controllerへのリモートセッションを開き、以下を実行します。
     a. `add_certificate.sh`スクリプトを実行します。

        ```
        sudo /opt/grizzly/bin/add_certificate.sh <Hostname> <Port>
        ```

        この場合、<*Hostname*>はLDAPSサーバーのホスト名であり、<*Port*>はLDAPSポートです(通常は636) 。
     b. キーストアパスワードを入力します。既定のパスワードは**hycu/4u**です。
     c. 証明書が有効であることと、表示された証明書情報が仮想マシン上の証明書情報と一致することを確認し、**y**を入力してから**Enter**を押して、証明書を受け入れます。そうでない場合、**n**と入力し、**Enter**を押して、証明書を拒否します。

2要素認証のセットアップ

2要素認証を使用すると、HYCUにサインインするときの追加のセキュリティ層を備えることができます。OTPアプリケーションによって生成される時間ベースワンタイムパスワード(OTP) 、およびFIDOプロトコル(FIDO認証システム) に準拠する認証システム(セキュリティキーと指紋リーダー) の2つの認証方法がサポートされています。

HYCUの2要素認証を有効にする場合、次のタスクを完了する必要があります。

タスク	説明
1. *管理者が実行します*。認証方式を選択し、必要な準備手順を実行します。	選択した認証方式に応じて、次のようにします。 • *OTPの場合：* ユーザーに説明し、ユーザーがOTPアプリケーションにアクセスできることを確認します。 • *FIDO認証システムの場合：* ◦ 認証システムが正しくセットアップされていることを確認します。手順について

タスク	説明
	は、認証システムの資料を参照してください。 ◦ DNSが正しく構成され、ホスト名が正しく解決されていることを確認します。
2. *管理者が実行します。*2要素認証を有効にするユーザーを作成または編集し、そのユーザーをユーザーグループに追加します。	"ユーザーの作成" ページ201と"ユーザーのグループへの追加" ページ203に説明されている手順に従います。
3. *ユーザーが実行します。*選択した方法に応じて、OTPの初期セットアップまたはFIDO認証システムの登録を実行します。	"HYCUへのログオン" ページ29で説明されている認証関連の手順に従います。 認証システムを追加したり、既存の認証システムを取り消したりするには、"FIDO認証システムの管理" 次のページを参照してください。

APIキーの管理

APIキーは、REST APIまたはHYCUコマンドラインユーザーインターフェース(hyCLI) の使用で2要素認証を有効にする場合に必要です。APIキーのオプションを使用して、APIキーを生成したり失効させたりできます。

考慮事項

管理者ロールが割り当てられているユーザーは、別のユーザーの情報を「セルフサービス」パネルで編集できます。詳細については、"ユーザーの作成" ページ201を参照してください。

> 「APIキー」ダイアログボックスへのアクセス
>
> 「APIキー」ダイアログボックスにアクセスするには、画面の右上にある👤をクリックして、「**APIキー**」を選択します。

APIキーの生成

手順

1. 「APIキー」ダイアログボックスで、「**＋ 新規**」をクリックします。
2. キーの名前を入力し、オプションで有効期限を設定します。有効期限を設定しない場合、キーが有効期限切れになることはありません。
3. 「**生成**」をクリックします。
4. APIキーが表示されます。キーを書き留めてその情報を安全に保管します。

> ⚠ 重要 セキュリティ上の理由から、APIキーは二度と表示されないので、必ずキーをメモしてそのメモを安全に保管してください。

> APIキーを使用するとお客様のデータにアクセスできるため、パスワードと同じように扱ってください。

「**終了**」をクリックします。

APIキーの取り消し

手順

1. 「APIキー」ダイアログボックスで、APIキーを選択し、「**取り消し**」をクリックします。
2. 「**はい**」をクリックして、キーを取り消すことを確認します。APIキーはすぐに取り消されます。

FIDO認証システムの管理

アカウントでFIDO 2要素認証方式が有効である場合は、FIDO認証システムをセットアップする必要があります。FIDO認証システムは、「FIDO認証システム」オプションを使用して追加または取り消しできます。

新規FIDO認証システムの追加

考慮事項

- インフラストラクチャグループで管理者ロールが割り当てられているユーザーは、別のユーザーの情報を「セルフサービス」パネルで編集できます。詳細については、“ユーザーの作成” ページ201を参照してください。
- HYCUにログオンするときは必ず完全修飾ドメイン名を使用し、DNSが正しく設定されていることを確認します。そうでない場合、認証は失敗することがあります。

> 「FIDO認証システム」ダイアログボックスへのアクセス
>
> 「FIDO認証システム」ダイアログボックスにアクセスするには、画面の右上にある👤をクリックして、「**FIDO認証システム**」を選択します。

手順

1. 「FIDO認証システム」ダイアログボックスで、「**＋ 新規**」をクリックします。
2. 「セキュリティのセットアップ」ウィザードが開きます。

   ウィザードの説明に従って認証システムを作成します。プロセスは、選択した認証システムのタイプとオペレーティングシステムのバージョンによって異なります。
3. 「名前」フィールドで、認証システムの名前を入力します。
4. 「**登録**」をクリックします。

FIDO認証システムの取り消し

手順

1. 「FIDO認証システム」ダイアログボックスで、取り消したい認証システムを選択して、「**取り消し**」をクリックします。
2. 「**はい**」をクリックして、認証システムを取り消すことを確認します。認証システムはすぐに取り消されます。

SMTP接続の保護

SMTP接続にSTARTTLSまたはSSL/TLSを使用する場合、SSL証明書をHYCUにインポートする必要があります。メールトラフィックを保護するために使用するプロトコルに応じて、以下のいずれかのセクションを参照してください。

- “STARTTLSセキュリティモードのSSL証明書のインポート” 下
- “SSL/TLSセキュリティモードのSSL証明書のインポート” 下

STARTTLSセキュリティモードのSSL証明書のインポート

手順

HYCU Backup Controllerへのリモートセッションを開き、次の手順を実行します。

1. `add_certificate_starttls.sh`スクリプトを実行します。

   ```
   sudo /opt/grizzly/bin/add_certificate_starttls.sh <Hostname> <Port>
   ```

   この場合、*<Hostname>*はSMTPサーバーのホスト名であり、*<Port>*は認証済みSMTP接続のポートです(587または25) 。
2. キーストアパスワードを入力します。既定のパスワードは**hycu/4u**です。
3. 証明書が有効であることと、表示された証明書情報が仮想マシン上の証明書情報と一致することを確認し、**y**を入力してから**Enter**を押して、証明書を受け入れます。そうでない場合、**n**と入力し、**Enter**を押して、証明書を拒否します。

SSL/TLSセキュリティモードのSSL証明書のインポート

手順

HYCU Backup Controllerへのリモートセッションを開き、次の手順を実行します。

1. `add_certificate.sh`スクリプトを実行します。

   ```
   sudo /opt/grizzly/bin/add_certificate.sh <Hostname> <Port>
   ```

   この場合、*<Hostname>*はSMTPサーバーのホスト名であり、*<Port>*は認証済みSMTP接続のポートです(465) 。

2. キーストアパスワードを入力します。既定のパスワードは**hycu/4u**です。
3. 証明書が有効であることと、表示された証明書情報が仮想マシン上の証明書情報と一致することを確認し、**y**を入力してから**Enter**を押して、証明書を受け入れます。そうでない場合、**n**と入力し、**Enter**を押して、証明書を拒否します。

複数のネットワークを使用するHYCUのセットアップ

マルチネットワーク環境で動作するようにHYCUをセットアップして、異なるVLANまたはネットワークセグメントに2つのネットワークアダプタを割り当てることができます。これは、HYCUとは異なるネットワークのバックアップに専用ストレージを使用している場合に特に役立ちます。例：

- HYCUは10.0.0.0/16 VLANに配置でき、ストレージボックスは192.168.0.0/24 VLANに配置できます。
- 仮想マシンネットワーク以外のネットワークからHYCU Webユーザーインターフェースにアクセスする必要があります。この場合、Webユーザーアクセス用のNICに加えて、Nutanixコントローラー仮想マシンと同じVLAN上に必ず必要なデータ転送用の専用NICを用意することをお勧めします。

> 注 *Nutanixクラスターの場合：*バックアップ時のデータトラフィックの大部分は追加のネットワークを介して行われますが、その一部は引き続き管理ネットワークを介して行われます。これは、HYCUがNutanixデータサービスIPアドレスを使用してNutanix Volumes(CVMの管理ネットワークと同じサブネット内に存在する必要がある) を通じてデータを消費するためです。
>
> この制限事項の詳細については、Nutanixの資料を参照してください。

ファイルサーバー環境の考慮事項

- メインネットワークは、HYCU Backup Controllerと追加のHYCUインスタンスの両方が相互に接続を確認して確立できるネットワークセグメントに対応する必要があります。
- 両方の仮想マシン(HYCU Backup Controllerと1つ以上の接続されたHYCUインスタンス) がファイルサーバーに接続できる必要があります。
- 各ネットワークアダプタは、異なるサブネット上にある必要があります。
- *DNSサーバーが指定されている場合のみ。*すべてのサブネット上のDNSサーバーが同じ結果を返す必要があります。
- *Nutanix ESXiクラスターの場合：*HYCUアップグレードすると、追加のすべてのネットワークアダプタのネットワーク設定が既定値に設定されます。アップグレード後にHYCUインスタンスを必ず再構成します。

複数のネットワークを使用するようにHYCUをセットアップする環境に応じて、次のいずれかの手順を実行します。

- “Nutanix AHVまたはESXiクラスターで複数のネットワークを使用するためのHYCUのセットアップ” 次のページ
- “vSphere環境内で複数のネットワークを使用するHYCUのセットアップ” 次のページ

Nutanix AHVまたはESXiクラスターで複数のネットワークを使用するためのHYCUのセットアップ

手順

1. Nutanix Prism Webコンソールにログオンし、さらにネットワークアダプタを追加します。
   a. メニューバーで、「**ホーム**」をクリックし、「**VM**」を選択します。
   b. 「**テーブル**」タブをクリックして「VMテーブル」ビューを表示し、次に仮想マシンのリストから、HYCU仮想マシンを選択します。
   c. 「**更新**」をクリックし、「ネットワークアダプタ(NIC) 」セクションにナビゲートします。
   d. 「**新規NICの追加**」をクリックし、「VLAN名」ドロップダウンメニューから、必要なVLANを選択します。
   e. 「**追加**」をクリックします。
   f. 「**保存**」をクリックします。

   詳細については、Nutanixの資料を参照してください。
2. ネットワークを構成します。これを行うには、VLANのセットアップ方法に応じて、以下のいずれかの方法を選択します。
   - VLANでIPアドレス(DHCP) 管理が有効になっている

     IPアドレスをNutanix Prism Webコンソールから直接割り当てます。
   - VLANに有効なIPアドレス(DHCP) 管理がない

     ネットワークを手動で構成します。
     a. HYCU Backup Controller仮想マシンへのリモートセッションを開きます。

        ```
        ssh hycu@<HYCUBackupControllerIPAddress>
        ```

     b. `/opt/grizzly/misc/`にある`ifcfg-mainnetwork.template`ファイルを開き、このテンプレートで提供される指示に従います。必ずルートユーザーとしてまたはsudoを使用して、指定されたコマンドを実行してください。

新しいネットワークアダプタが適正に構成されたら、別のVLAN上にあるターゲットをHYCUに追加できます。

vSphere環境内で複数のネットワークを使用するHYCUのセットアップ

> ⚠ 重要 このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

手順

1. vSphere Web Clientにログオンし、さらにネットワークアダプタを追加します。
   a. 「**VM**」タブをクリックし、ご使用のHYCU Backup Controllerにナビゲートします。
   b. HYCU Backup Controllerを右クリックし、「**設定の編集**」を選択します
   c. 「新規デバイス」ドロップダウンメニューから、「**ネットワーク**」を選択し、「**追加**」をクリックします。
   d. 「新規ネットワーク」ドロップダウンメニューから、必要なネットワークを選択します。

      ⚠ 重要 仮想NICオプションにはvSphere分散スイッチ(dvSwitch) を選択しないようにしてください。

   e. 「**OK**」をクリックします。

   詳細については、VMwareの資料を参照してください。
2. ネットワークを手動で構成します。
   a. HYCU Backup Controller仮想マシンへのリモートセッションを開きます。

      ```
      ssh hycu@<HYCUBackupControllerIPAddress>
      ```

   b. `/opt/grizzly/misc/`にある`ifcfg-mainnetwork.template`ファイルを開き、このテンプレートで提供される指示に従います。必ずルートユーザーとしてまたはsudoを使用して、指定されたコマンドを実行してください。

新しいネットワークアダプタが適正に構成されたら、別のネットワーク上にあるターゲットをHYCUに追加できます。

HYCU仮想ディスクのサイズの増分

HYCU Backup Controllerのディスク領域が不足している場合、必要に応じてHYCU仮想ディスクのサイズを増やすことができます。これを実行するには、以下のいずれかのセクションの説明に従ってください。

- “Nutanix AHVクラスターでのHYCUディスクのサイズの増分” 下
- “Nutanix ESXiクラスターまたはvSphere環境でのHYCUディスクのサイズの増分” 次のページ

Nutanix AHVクラスターでのHYCUディスクのサイズの増分

Nutanix AHVクラスターのHYCUシステムディスクやデータディスクのサイズを増やすには、次の手順を実行します。

1. Nutanix Prism Webコンソールにログオンします。
2. メニューバーで、「**ホーム**」をクリックし、「**VM**」を選択します。
3. 「**テーブル**」タブをクリックして、「VMテーブル」ビューを表示します。
4. 仮想マシンのリストから、ご使用のHYCU Backup Controllerを選択し、「**電源オフアクション**」をクリックし、「**電源オフ**」をクリックしてシャットダウンします。

   ⚠ 重要 仮想マシンが完全にシャットダウンされるまで待機します。

5. 「**更新**」をクリックし、以下を実行します。
   a. 「ディスク」セクションにナビゲートし、サイズを増分するHYCUディスクの横の「**編集**」をクリックします。
   b. 「容量(GiB) 」フィールドで、ディスクのサイズを必要に応じて増やします。
   c. *両方のHYCUディスクのサイズを増やす場合* 残りのHYCUディスクに手順aとbを繰り返します。
   d. 「**更新**」をクリックします。
6. 「**電源オン**」をクリックして、HYCU Backup Controllerをオンにします。

Nutanix ESXiクラスターまたはvSphere環境でのHYCUディスクのサイズの増分

> ⚠ 重要 このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

Nutanix ESXiクラスターまたはvSphere環境内のHYCUシステムディスクやデータディスクのサイズを増やすには、次の手順を実行します。

1. vSphere Web Clientにログオンします。
2. 「**VM**」タブをクリックし、ご使用のHYCU Backup Controllerにナビゲートします。
3. HYCU Backup Controllerを右クリックし、**「電源」>「電源オフ」**を選択してシャットダウンします。
   > ⚠ 重要 仮想マシンが完全にシャットダウンされるまで待機します。
4. HYCU Backup Controllerを右クリックし、「**設定の編集**」を選択します
5. 「仮想ハードウェア」タブで、「ハードディスク1」または「ハードディスク2」の一方または両方のフィールドに新しい値を入力して、1つまたは両方のHYCUディスクのサイズを増やし、「**OK**」をクリックします。
6. HYCU Backup Controllerを右クリックし、**「電源」>「電源オン」**を選択してオンにします。

Nutanix AHVまたはESXiクラスターでの仮想マシンの管理方法の詳細については、Nutanixの資料を参照してください。vSphere環境での仮想マシンの管理方法の詳細については、VMwareの資料を参照してください。

vSphereユーザーへの特権の割り当て

必要な特権をvSphere (Web) Clientを使用してユーザーに割り当てることができます。

> ⚠ 重要 このセクションに記載されている手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

手順

1. vSphere Web Clientに管理者としてログオンします。
2. 「**ロール**」をクリックします。
3. 「ロール」タブの情報パネルを右クリックし、「**追加**」をクリックします。
4. 新しいロールの名前を入力します(たとえば、**HYCU**) 。
5. ロールに必要な特権を選択し、「**OK**」をクリックします。

特権カテゴリー	バックアップ特権	復元特権	アップグレードおよびHYCUインスタンス作成特権
Datastore	• データストアの参照 • 低レベルファイル操作	• スペースの割り当て • 低レベルファイル操作	• スペースの割り当て • 低レベルファイル操作
Global	• メソッドの無効化 • メソッドの有効化	該当なし	該当なし
Host > Local operations	該当なし	• 仮想マシンの作成 • 仮想マシンの削除 • 仮想マシンの再構成	該当なし
Network	該当なし	• ネットワークの割り当て • 構成	• ネットワークの割り当て
Resource	該当なし	• 仮想マシンのリソースプールへの割り当て	該当なし
vApp	該当なし	• 仮想マシンの追加	• インポート
仮想マシン > 構成	• ディスク変更追跡 • 設定	すべての特権	• 既存のディスクの追加 • 新しいディスクの追加 • デバイスの追加または削除 • 設定 • ディスクの削除 • 名前変更
仮想マシン > Interaction	• 電源オン	• 質問への回答 • 電源オフ • 電源オン	• 電源オン

特権カテゴリー	バックアップ特権	復元特権	アップグレードおよびHYCUインスタンス作成特権
仮想マシン > Inventory	該当なし	• 新規作成 • 登録 • 削除 • 登録解除	• 既存から作成 • 削除
仮想マシン > Provisioning	• 読み取り専用ディスクアクセスの許可 • 仮想マシンダウンロードの許可 • *テンプレートをバックアップする場合 :*テンプレートとしてマーク • *テンプレートのバックアップの場合 :*仮想マシンとしてマーク	• ディスクアクセスの許可	• 仮想マシンのクローン
仮想マシン > Snapshot management	• スナップショットの作成 • スナップショットの削除	該当なし	該当なし
vSphereタグ付け	• vSphereタグの割り当てまたは割り当て解除	• vSphereタグの割り当てまたは割り当て解除	該当なし

詳細については、VMwareの資料を参照してください。

HYCU REST APIエクスプローラーの使用

HYCUは、外部アプリケーションがHYCU Backup Controllerと対話し、そこから情報を取得し、タスクを自動化するために使用できるREST APIを提供します。HYCUユーザーインターフェースを通じて公開されるすべての機能は、HYCU REST APIからも利用できます。HYCU REST APIエクスプローラーを使用してAPIとやり取りし、各エンドポイントの予想される入力および出力形式を表示できます。

HYCU REST APIエクスプローラーにアクセスするには、次の手順に従います。

1. 画面右上の「👤」をクリックし、「**REST APIエクスプローラー**」を選択します。HYCU REST APIエクスプローラーが開きます。
2. 機能グループのリストで、「**操作のリスト**」をクリックして、目的のグループを展開できます。APIエンドポイントのリストが表示されます。
3. エンドポイントのいずれかをクリックして、説明、パラメーター、および出力形式を表示します。フィールドに入力し、「**試行する**」をクリックして、APIを呼び出して出力データを取得できます。

コマンドラインインターフェースの使用

HYCUコマンドラインユーザーインターフェース(hyCLI) を使用して、データ保護環境を管理することもできます。hyCLIはHYCU Webユーザーインターフェースに相当する機能を提供し、特定のタスクを自動化するためのスクリプトを実装できます。

hyCLIの使用を有効にするには、次の手順を実行します。

1. `hycli.zip`パッケージをダウンロードします。これを実行するには、画面右上の「👤」をクリックし、「**hyCLIをダウンロード**」を選択します。
2. `hycli.zip`ファイルを保存して、システム上の任意の場所に抽出します。
3. 抽出されたファイルを含むフォルダをPATH環境変数に追加します。
4. *アカウントで2要素認証が有効になっている場合のみ*。APIキーを生成します。このキーは、hyCLIコマンドを実行するたびに入力する必要があります。詳細については、"APIキーの管理" ページ 263を参照してください。

> 注 hyCLIログファイルは、ユーザーのホームディレクトリ内の`.Hycu/log`にあります。抽出されたファイルを含むディレクトリ内にある`logging.properties`ファイルで、hyCLIのログ設定を変更できます。

hyCLIの詳細については、抽出されたファイルが含まれるディレクトリ内にある`README.txt`ファイルを参照してください。

hyCLI構造、コマンド、および使用法の詳細については、`hycli help`コマンドを実行してください。

プレ/ポストスクリプトの使用

プレ/ポストスクリプトを使用して、バックアップと復元が実行される前と後に必要なアクションを実行する場合、正常に終了した場合はスクリプトは終了コード0を返し、失敗の場合はそれ以外を返します。後者の場合、データ保護操作にも下記のような影響が及びます。

- 終了コードが0よりも大きい :ジョブのステータス(およびバックアップ操作の場合はバックアップのステータス) は「警告」に設定され、ジョブは続行します。
- 終了コードが0よりも小さい :ジョブのステータス(およびバックアップ操作の場合はバックアップのステータス) は「失敗」に設定されます。

スクリプトの実行中、以下の環境変数がエクスポートされます。

環境変数	説明
`HYCU_BKPCTRL_URL`	HYCU Backup Controller URL
`HYCU_BKPCTRL_UUID`	HYCU Backup Controller UUID
`HYCU_VM_UUID`	仮想マシンUUID
`HYCU_BACKUP_UUID`	バックアップUUID
`HYCU_JOB_UUID`	ジョブUUID

環境変数	説明
HYCU_TARGET_UUID	ターゲットUUID
HYCU_VM_NAME	仮想マシン名[a]
HYCU_TARGET_NAME	ターゲット名[a]
HYCU_TARGET_PATH	ターゲット上のデータへのパス
HYCU_SUCCESS	*ポストスクリプトにのみ使用できます。*データ保護操作は成功。
HYCU_PREEXEC_RETURN_CODE	*ポストスクリプトにのみ使用できます。*ポストスクリプトの終了コード。

[a] 名前にスペース文字や文字 " ' , ; & % € ( ) < > { } | ^ ` ˇ が含まれる場合、それらはエクスポートの前にアンダースコアに置き換えられます。

プレ/ポストスクリプトの指定方法の詳細については、以下のセクションを参照してください。

- “プレ/ポストバックアップスクリプトおよびプレ/ポストスナップショットスクリプトの指定” ページ82
- “個別のファイルの復元” ページ107

第13章

データ保護環境の監視

HYCU Managerは、すべてのデータ保護環境をプロアクティブに監視するために必要な可視性を提供するように設計されており、単一のコンソールから総合的なステータスを表示できます。HYCU Managerを使用すると、登録済みのすべてのHYCUコントローラーから受け取ったデータ保護情報が1か所に統合され、収集された情報に簡単にアクセスできます。この情報は、オンプレミス(HYCU) および次のクラウドデータ保護環境について表示できます。

- HYCU Data Protection as a Service for Azure(HYCU for Azure) データ保護環境
- HYCU Data Protection as a Service for Google Cloud(HYCU for Google Cloud) データ保護環境
- HYCU Protégé for Office 365データ保護環境

HYCU for AzureまたはHYCU for Google Cloudでデータを保護する方法の詳細については、HYCU for AzureまたはHYCU for Google Cloudの資料を参照してください。

HYCU Protégé for Office 365でのデータを保護する方法の詳細については、「*HYCU Protégé for Office 365クイックスタートガイド*」を参照してください。

HYCU Managerモードで HYCU仮想アプライアンスを展開したら、HYCU Managerにアクセスして、潜在的な問題を迅速に特定して対処するこの直感的なビジュアル化アプローチの利点を活かすことができます。

HYCU Managerコンソールの使用

HYCU Managerコンソールにより、担当するすべてのデータ保護環境から収集されたデータの概要を一目で把握できます。

> 「コンソール」パネルへのアクセス
>
> 「コンソール」パネルにアクセスするには、ナビゲーションペインで、「**コンソール**」をクリックします。

HYCU Managerコンソールの各ウィジェット内には、データ保護環境に関連する情報が表示されます。ただし、すべてのウィジェットがデータ保護シナリオに適用できるわけではないことに注意してください。

コンソールウィジェット	説明
仮想マシン	データ保護環境内のすべての仮想マシンの数、および保護されている仮想マシンと保護されていない仮想マシンの数。

コンソールウィジェット	説明
アプリケーション	データ保護環境内のすべてのアプリケーションの数、および保護されているアプリケーションと保護されていないアプリケーションの数。
HYCUコントローラー	データ保護環境内で使用できるおよび使用できないHYCUコントローラーの数。
バックアップ	データ保護環境内の成功したバックアップの割合、および成功したバックアップと移行/DR対応バックアップの数。HYCU Protégéを採用する予定がない場合は、移行/DR準備完了ラベルを無視しても問題ありません。現在のバックアップチェーン内のすべてのバックアップがいずれかのクラウドターゲット(AzureまたはGoogle Cloud)に保存され、最新のバックアップ中に正常なクラウド準備チェックが実行された場合、バックアップは移行/DR対応です。 バックアップの詳細については、"仮想マシンのバックアップ" ページ85を参照してください。
共有フォルダ	データ保護環境内のすべてのファイル共有の数、および保護されているファイル共有と保護されていないファイル共有の数。
ターゲット	データ保護環境内のすべてのターゲットの数、および空きターゲットと使用済みターゲットの数。
ポリシー	データ保護環境内のすべてのポリシーの数と、準拠および非準拠ポリシーの数。このポリシーが割り当てられているすべてのエンティティがポリシー設定に準拠している場合、ポリシーは準拠していると見なされます。
Office 365	データ保護環境における保護ユーザー、SharePointサイト、およびグループとチームの概要。ユーザーの場合、保護されているメール、OneDriveファイル、連絡先、カレンダーアイテム、タスクの総数も表示されます。

> ⚠ 重要 いずれかのウィジェットの値をクリックすると、「HYCUコントローラー」パネルに移動します。そこではクリックした値により並べ替えられるHYCUコントローラーのリストを表示できます。たとえば、準拠しているポリシーの数をクリックすると、HYCUコントローラーはポリシー準拠パーセントにより下降順にソートされます。

HYCUコントローラーの監視

「HYCUコントローラー」パネルを使用して、HYCUコントローラーの追加、編集、削除や、各コントローラーに関する情報を表示できます。

考慮事項

HYCU for Google Cloudデータ保護環境を監視している場合のみ。HYCUコントローラーのリストには、プロジェクトと、これらのプロジェクトが含まれている保護セットの両方が含まれています。

「HYCUコントローラー」パネルへのアクセス

「HYCUコントローラー」パネルにアクセスするには、ナビゲーションペインで、「**HYCUコントローラー**」をクリックします。

HYCUコントローラーの追加

前提条件

- *HYCU for AzureまたはHYCU for Google Cloudデータ保護環境を監視することを予定している場合のみ：*
  - クラウドアカウントがHYCUに追加されている。監視するクラウドデータ保護環境に応じて、「"Azureサービスプリンシパルの追加" ページ213」または「"Google Cloudサービスアカウントの追加" ページ212」を参照してください。
  - HYCU Protégéライセンスを持っている。詳細については、"ライセンス" ページ222を参照してください。
  - HYCU for AzureまたはHYCU for Google Cloudのアクティブなサブスクリプションがある。詳細については、HYCU for AzureまたはHYCU for Google Cloudの資料を参照してください。
  - *HYCU for Google Cloudデータ保護環境の場合*：監視する予定の保護セットに含まれるプロジェクトは、HYCU for Google Cloudをサブスクライブするときに選択されたGoogle Cloud請求先アカウントにリンクされている。詳細については、HYCU for Google Cloudの資料を参照してください。
- *HYCU Protégé for Office 365データ保護環境を監視することを予定している場合のみ*：HYCU Protégé for Office 365のアクティブなサブスクリプションがある。詳細については、「*HYCU Protégé for Office 365クイックスタートガイド*」を参照してください。

手順

1. 「HYCUコントローラー」パネルで、「**＋ 追加**」をクリックします。「新しいコントローラー」ダイアログボックスが開きます。
2. 監視するデータ保護環境に応じて、次のいずれかのオプションを選択します。

オプション	説明
オンプレミスコントローラーを追加	a. 「**次へ**」をクリックします。「オンプレミスコントローラーを追加」ダイアログボックスが開きます。 b. HYCU Backup Controllerの名前を入力します。 c. HYCU Backup ControllerのURLを入力します。 d. 使用する認証のタイプに応じて、次のいずれかを実行します。 • *Basic認証*：「**APIキー認証を使用する**」スイッチが無効になっていることを確認し、インフラストラクチャグループ管理者のユーザー名とパスワードを入力します。 • *APIキー認証*：「**APIキー認証を使用する**」スイッチを有効

	にして、APIキーを入力します。APIキーを生成する/取り消す方法については、"APIキーの管理" ページ263を参照してください。 e. 「**保存**」をクリックします。
AzureまたはGoogle Cloudコントローラーの追加	a. 「**次へ**」をクリックします。「AzureまたはGoogle Cloudコントローラーを追加」ダイアログボックスが開きます。 b. 利用可能なすべてのクラウドコントローラーのリストから、監視するHYCU for AzureまたはHYCU for Google Cloud(あるいはその両方の)保護セットを選択します。また、「検索」フィールドに名前を入力して、保護セットを検索することもできます。 ヒント「 > 」をクリックすると、使用可能な各保護セットにどのAzureリソースグループまたはGoogle Cloudプロジェクトが含まれているかを確認できます。 c. 「**追加**」をクリックします。
Office 365コントローラーの追加	a. 「**次へ**」をクリックします。「Office 365コントローラーの追加」ダイアログボックスが開きます。 b. Office 365コントローラーの名前を入力します。 c. HYCU Protégé for Office 365 Webユーザーインターフェースのurlを入力します。 d. HYCU Protégé for Office 365をサブスクライブしたときに受け取ったアクセストークンとリセラートークンを入力します。 e. 「**保存**」をクリックします。

後から既存のオンプレミスまたはOffice 365のコントローラーを編集したり(「 **編集**」をクリックして必要な変更を加える)、監視しなくなったHYCUコントローラーをHYCU Managerから削除したりできます(「 **削除**」をクリックする)。HYCU Managerを使用してHYCU for AzureまたはHYCU for Google Cloudデータ保護環境も監視する場合は、そのようなコントローラーを編集できないことに注意してください。

ヒント データ保護環境に関連するデータは、「 **同期**」をクリックして更新できます。

HYCUコントローラーに関する情報の表示

各HYCUコントローラーに関する特定の情報を表示できます。ただし、すべての情報がデータ保護シナリオに適用できるわけではないことに注意してください。

HYCUコントローラー情報	説明
名前	HYCUコントローラーの名前 オンプレミスコントローラーは、アイコンとHYCU Backup Controller

HYCUコントローラー情報	説明
	の名前で表されます。HYCU Managerを使用してクラウドデータ保護環境も監視する場合は、クラウドコントローラーを表示できます。クラウドコントローラーは次のように表されます。 • *HYCU for Azure* :アイコンとAzureサービスプリンシパルの名前およびHYCU for Azure保護セット。 • *HYCU for Google Cloud* :アイコンとGoogle Cloudサービスアカウントの名前およびHYCU for Google Cloud保護セット。 • *HYCU Protégé for Office 365* :アイコンとOffice 365コントローラーの名前。 ヒント HYCUコントローラーの名前をクリックすると、関連するWebユーザーインターフェースに移動します。
バージョン	HYCU Backup ControllerのHYCUソフトウェアリリースバージョン。
ステータス	HYCUコントローラーのステータス(アクティブまたは非アクティブ)
バックアップ	成功または失敗したバックアップの割合。
移行/DR対応仮想マシン	移行/DR準備完了仮想マシンと物理マシンの数。現在のバックアップチェーン内のすべてのバックアップがいずれかのクラウドターゲット(AzureまたはGoogle Cloud) に保存され、最新のバックアップ中に正常なクラウド準備チェックが実行された場合、仮想マシンまたは物理マシンは移行/DR対応です。
VM保護	保護されている仮想マシンと保護されていない仮想マシンの割合。
APP protection	保護されているアプリケーション保護されていないアプリケーションの割合。
Share protection	保護されているファイル共有と保護されていないファイル共有の割合。
ポリシーコンプライアンス	準拠と非準拠のポリシーの割合。
Target utilization	ターゲットの使用済みおよび空きストレージ領域の割合。

「HYCUコントローラー」パネルに表示されたデータは、JSONまたはCSV形式でファイルにエクスポートできます。この実行方法の詳細については、"パネルのコンテンツのエクスポート" ページ184を参照してください。

イベントの表示

「イベント」パネルを使用して、HYCU Managerで発生したすべてのイベントを表示し、選択したイベントについての詳細を確認し、指定したフィルターに一致するイベントをリストし、イベントが発生したとき

に電子メール通知を送信するようにHYCUを構成し、パネルの内容をJSONまたはCSV形式のファイルにエクスポートできます。

「イベント」パネルへのアクセス

「イベント」パネルにアクセスするには、ナビゲーションペインで、「**イベント**」をクリックします。

目的	手順
イベントを表示し、選択したイベントについての詳細を確認します。	"HYCUイベントの管理" ページ165
イベントにフィルターを適用します。	"データのフィルタリング" ページ177
イベントの発生時に通知を送信するようにHYCUを構成します。	"イベント通知の構成" ページ166
イベントデータをエクスポートします。	"パネルのコンテンツのエクスポート" ページ184

管理タスクの実行

HYCU Managerモードで HYCU仮想アプライアンスをデプロイしたら、「**管理**」メニューでさまざまな管理タスクを実行できます。

> 注 HYCU Managerモードでデプロイされた HYCUを管理する手順は、HYCU Backup Controllerモードでデプロイされた HYCUの場合と同じです。したがって、たいていの場合、同じ説明に従うことができます。
>
> 選択した展開モードに応じて、さまざまな管理タスクのセットを使用できることに注意してください。

目的	手順
HYCU ManagerをIDプロバイダーと統合します。	"HYCUとIDプロバイダーの統合" ページ216
クラウドデータ保護環境を監視できるように、Azureまたは Google Cloudアカウントを追加します。	"クラウドアカウントの追加" ページ211
HYCUが予期したとおりに実行しない場合、問題をトラブルシューティングするためにログファイル設定を構成します。	"ログのセットアップ" ページ226
ネットワーク設定を変更します。	"ネットワーク設定の変更" ページ228
SMTPサーバーを構成します。	"SMTPサーバーの構成" ページ233
HYCUを利用可能な新しいバージョンにアップグレードします。 ⚠ 重要 アップグレードする前に、"ソースの追加" ページ32の説明に従ってHYCU Manager仮想マシンが存在するソースが追加されていることを確認します。	"HYCUのアップグレード" ページ238

目的	手順
SSL証明書を構成します。	“SSL証明書の構成” ページ234
HYCU Managerユーザーを管理します。	“ユーザーの管理” 下

さらに、次の手順を実行できます。

- hyCLIを使用します。詳細については、“コマンドラインインターフェースの使用” ページ272を参照してください。
- HYCU REST APIエクスプローラーを使用します。詳細については、“HYCU REST APIエクスプローラーの使用” ページ271を参照してください。

ユーザーの管理

「ユーザーの管理」ダイアログボックスを使用して、特定のユーザーにHYCU Managerへのアクセス権を付与できます。ユーザーの管理には、ユーザーの作成、編集、削除、アクティブ化、または非アクティブ化が含まれます。

> 「ユーザー管理」ダイアログボックスへのアクセス
>
> 「ユーザー管理」ダイアログボックスにアクセスするには、「⚙ **管理**」メニューから、「**ユーザー管理**」を選択します。

新しいユーザーの作成

手順

1. 「ユーザー管理」ダイアログボックスで、「**＋新規**」をクリックします。
2. HYCUユーザー、ADユーザー、またはIDプロバイダーユーザーを追加する場合は、ユーザー名を入力しします。ADグループを追加する場合は、一般名を入力します。

   > ⚠ **重要** 名前を入力するときは、SAMアカウント名の制限に準拠するようにします。名前の長さは20文字を超えてはならず、次の文字を含めることができます。"/ \ [ ] : ; | = , + * ? < >
   > さらに、HYCUは名前にアットマーク(@) を使用できません。
   >
   > 環境で必要な場合は、`ad.username.filter.regex`構成設定を編集することでこれらの制限を上書きできます。ただし、これはサポートされず、認証の問題を引き起こす可能性があります。HYCU構成設定のカスタマイズ方法の詳細については、“HYCU構成設定のカスタマイズ” ページ308を参照してください。

3. 「認証タイプ」ドロップダウンメニューから、以下のいずれかの認証タイプを選択し、説明に従います。

認証タイプ	説明
HYCU	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「名前」フィールドで、ユーザーの表示名を入力します。

認証タイプ	説明
	c. *オプション*:「Eメール」フィールドには、ユーザーの電子メールアドレスを入力します。 d. 「パスワード」フィールドで、ユーザーパスワードを入力します。 注 最小パスワード長は6文字です。
ADユーザー	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「IDプロバイダー」ドロップダウンメニューから、ADユーザーが属するActive Directoryを選択します。
ADグループ	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「IDプロバイダー」ドロップダウンメニューから、ADグループが属するActive Directoryを選択します。
IDプロバイダーユーザー	a. 「言語」ドロップダウンメニューから、ユーザーが使用する言語を選択します。 b. 「IDプロバイダー」ドロップダウンメニューから、IDプロバイダーを選択します。 c. 「IDプロバイダーのユーザーID」フィールドに、IDプロバイダーのユーザーIDを入力します。 注 IDプロバイダーに応じて、ユーザーIDは以下のように対応します。 • *Google*:ユーザーの電子メールアドレス • *Microsoft*:オブジェクトID • *Okta*:ユーザーのプロファイルに移動するときのURLの一部 詳細については、それぞれのIDプロバイダーの資料を参照してください。

4. *HYCUユーザー、ADユーザー、またはADグループを追加する場合のみ*。ユーザーに対して2要素認証を有効にする場合は、「**2要素認証の有効化**」スイッチを使用し、次の2要素認証方式のいずれかを選択します。

   - **時間ベースのワンタイムパスワード**

     このオプションを使用すると、OTPアプリケーションによって生成された時間ベースのワンタイムパスワード(OTP)を使用できます。2要素認証が有効になった後の最初のログオン時に、ユーザーがOTPをセットアップする必要があります。

   - **FIDO**

このオプションを選択すると、FIDOプロトコル(FIDO認証システム) に準拠する認証システムを使用できます。ユーザーはFIDO認証システムを登録する必要があります。詳細については、“FIDO認証システムの管理” ページ264を参照してください。

5. *2要素認証を有効にした場合のみ*。ユーザーが2要素認証を無効にできないようにするには、必ず「**ユーザーは2要素認証を無効にできません**」チェックボックスを選択します。このチェックボックスをクリアすると、2要素認証を無効にできます。管理者ロールが設定され、インフラストラクチャグループに属しているユーザーは、このオプションが設定されていても、2要素認証を無効できます。

   > 注 ユーザーが2要素認証を無効にした場合、管理者にはセキュリティ警告が通知されます。

6. 「**保存**」をクリックし、「**閉じる**」をクリックします。ユーザーはすべてのユーザーのリストに追加されます。

後で以下を実行できます。

- 「**編集**」をクリックして必要な変更を加えることで、既存のHYCUまたはIDプロバイダーのユーザーを編集します。組み込みユーザー、ADユーザー、およびADグループは編集できないことに注意してください。
- 特定のユーザーのHYCUへのログオンを有効または無効にします。詳細については、“データ保護環境の監視” ページ274を参照してください。
- 「**削除**」をクリックして、既存のユーザーのいずれかを削除します。組み込みユーザーは削除できないことに注意してください。

> ⚠ 重要 *hyCLIを使用してユーザーを作成する場合*：これが自動的に行われるHYCU Managerコンソールで新しいユーザーを作成するのとは異なり、hyCLIを使用する場合は、作成したユーザーをインフラストラクチャグループに追加して、このユーザーに管理者ロールを割り当てることも必要です。

第14章

Nutanix Mine with HYCUの使用

Nutanix Mine with HYCUは唯一のハイパーコンバージドバックアップおよび復元ソリューションであり、バックアップと復元をNutanixプラットフォームのネイティブサービスとして提供し、独立したインフラストラクチャを不要にします。これによりハイパーコンバージドインフラストラクチャのシンプルさを維持したまま、すべてのデータを完全に保護することができます。

Nutanix Mine with HYCUソリューションにより、単一のペインを使用して、プロダクションインフラストラクチャとバックアップインフラストラクチャの両方を管理できます。Nutanix Mineストレージをターゲットとして導入することにより、データ保護環境を最適化できます。これにより、Nutanix Mineクラスターの有効なストレージ容量が増加し、バックアップと復元のパフォーマンスが向上します。

タスク	説明
1. HYCUをNutanix Mineプラットフォームのサービスとして登録します。	“HYCUのNutanix Prismへの登録” 下
2. Nutanix Mineストレージを保護データを保存するためのターゲットとして追加します。	“Nutanixターゲットのセットアップ” ページ43
3. 単一のペインを使用して、プロダクションインフラストラクチャとバックアップインフラストラクチャの両方を管理します。	“Nutanix Prism WebコンソールからのHYCUへのアクセス” 次のページ

HYCUのNutanix Prismへの登録

前提条件

- Nutanix Mineアプライアンスを取得している。
- HYCU Backup ControllerがNutanix Mineクラスターに存在しており、そのクラスターがHYCUにソースとして追加されている。詳細については、“HYCUのNutanix AHVクラスターへの展開” ページ23と“Nutanixクラスターの追加” ページ32を参照してください。
- *登録手順を繰り返す場合* 実行中のジョブを終了している。

考慮事項

- Nutanix AHVクラスターに適用されるすべての説明については、Nutanix Mineクラスターにも適用されます。
- Nutanix Mineクラスターに変更があったことを示す警告メッセージが表示された場合、HYCUをNutanix Prismに再度登録する必要があります。次の場合にそのようなメッセージを受け取ります。
  - HYCU Backup ControllerのIPアドレス/ホスト名またはポートが変更された。
  - Nutanix MineクラスターのAOSが新しいバージョンにアップグレードされた。
  - 新しいController VMがNutanix Mineクラスターに追加された。

> 「ソース」ダイアログボックスへのアクセス
>
> 「ソース」ダイアログボックスにアクセスするには、「⚙ **管理**」をクリックし、「**ソース**」を選択します。

手順

1. 「ソース」ダイアログボックスの「ハイパーバイザー」タブで、すべてのソースのリストから、Nutanix Mineクラスターを選択します。
2. 「◆ **Prismに登録**」をクリックします。
3. 「**はい**」をクリックして、続行を確認します。

> ⚠ 重要 HYCUのNutanix Prismへの登録はいくらか時間がかかる場合があります。この間はNutanix Prism Webコンソールは使用できません。

HYCUはNutanix Prismからいつでも登録解除できます。これを行うには、それぞれのNutanix Mineクラスターを選択し、「◆ **Prismから登録解除**」をクリックします。

Nutanix Prism Webコンソールからの HYCUへのアクセス

HYCUのNutanix Prismへの登録を有効にしたら、Nutanix Mine with HYCUダッシュボードを表示し、Nutanix Prism WebコンソールからHYCU Webユーザーインターフェースを直接起動することもできます。

手順

1. Nutanix Prism Webコンソールにログオンします。
2. 左側のドロップダウンメニューから、「**HYCU**」を選択します。Nutanix Mine with HYCUダッシュボードが表示されます。
3. 「**HYCUを起動します**」をクリックします。HYCUユーザーWebインターフェースが別のタブで開き、データ保護環境を管理できます。

Nutanix Mine with HYCUダッシュボードの表示

Nutanix Mine with HYCUダッシュボードにより、環境内のデータ保護ステータスの概要を一目で確認できます。この直感的なダッシュボードにより、すべてのデータ保護アクティビティを監視し、注意が必要な箇所をすばやく特定できます。このダッシュボードは、対応するリンクをクリックするだけで目的のデータに簡単にアクセスできるため、データ保護に関連する日々のタスクの開始点として使用できます。

以下の表は、各ウィジェットで見つけることができる情報の種類を説明しています。

ダッシュボードウィジェット	説明
VM保護ステータス	データ保護環境内で保護されている仮想マシンの割合と、保護されている仮想マシンと保護されていない仮想マシンの数。少なくとも1つの有効なバックアップが利用でき、除外ポリシーが割り当てられていない場合、仮想マシンは保護されていると見なされます。仮想および物理マシンの保護の詳細については、“仮想マシンの保護” ページ71を参照してください。
アプリ保護ステータス	データ保護環境内で保護されているアプリケーションの割合と、保護されているアプリケーションと保護されていないアプリケーションの数。少なくとも1つの有効なバックアップが利用でき、除外ポリシーが割り当てられていない場合、アプリケーションは保護されていると見なされます。アプリケーションの保護の詳細については、“アプリケーションの保護” ページ113を参照してください。
コンプライアンス	データ保護環境内の、準拠しているポリシーの割合と、準拠および非準拠ポリシーの数。このポリシーが割り当てられているすべてのエンティティがRPOおよびRTO要件に準拠している場合、ポリシーは準拠していると見なされます。ポリシーの詳細については、“バックアップ戦略の定義” ページ58を参照してください。
バックアップ	過去7日間のバックアップ成功率。
Mineストレージ	• Nutanixターゲットのリスト、またデータの保存に使用されている領域と空き領域の量、データ圧縮率、およびデータ重複除去率に関する情報。 • Nutanix ObjectsおよびS3互換ターゲットのリストと、データを保存するために使用されている領域と空き領域の量に関する情報。 ターゲットの詳細については、“ターゲットのセットアップ” ページ38を参照してください。
ターゲットの概要	データ保護環境内の(Nutanix、Nutanix Objects、およびS3互換ターゲットを除く) すべてのターゲットのリストと、データ保存領域の使用済みまたは使用可能な量に関する情報。ターゲットの詳細については、“ターゲットのセットアップ” ページ38を参照してください。
HYCUコントローラー	HYCU Backup Controllerが保護され、そのライセンスが有効かどうかに関する情報、およびHYCU Backup Controllerに関するリソース情報(ストレージ、メ

ダッシュボードウィジェット	説明
	モリ、vCPU)。リソース値のいずれかがクリティカル値に達した場合の対処方法の詳細については、"HYCU仮想マシンリソースの調整" ページ196を参照してください。
イベント	ステータス(成功、警告、失敗)に応じた過去56時間のデータ保護環境内のイベントの数。イベントの詳細については、"HYCUイベントの管理" ページ165を参照してください。
ジョブ	ステータス(成功、警告、失敗、進行中、待機中)に応じた過去56時間のデータ保護環境内のジョブの数。ジョブの詳細については、"HYCUジョブの管理" ページ163を参照してください。

ヒント ダッシュボードウィジェットは、ドラッグアンドドロップで、ダッシュボードの上部に最も重要なデータが表示されるように並べ替えることができます。

第15章

HYCU Protégé

HYCU Protégéソリューションは、さまざまなインフラストラクチャにまたがるデータ保護環境のビジネス継続性を保証します。オンプレミスとクラウドインフラストラクチャ(Google Cloud、グローバルAzure、またはAzure US Government) 間で仮想マシンを移行することにより、データの復元性を確保できます。オンプレミス環境で災害が発生した場合、HYCU Protégéはクラウドへのデータの災害復旧を提供します。

ご使用のクラウド環境に応じて、以下のいずれかのセクションを参照してください。

- “オンプレミス環境とGoogle Cloud環境全体でのデータの保護” 下
- “オンプレミス環境とAzure環境全体でのデータの保護” ページ294
- “オンプレミス環境とAzure US Government環境全体でのデータの保護” ページ302

オンプレミス環境とGoogle Cloud環境全体でのデータの保護

スピンアップ機能を使用して、保護されたデータをオンプレミス環境とGoogle Cloud環境間で移行することにより、HYCU Protégéはデータの復元力を保証します。災害発生時に、Google Cloudへのデータの災害復旧を提供します。

実行内容に応じて、以下のいずれかを参照してください。

目的	説明
オンプレミス環境とGoogle Cloud環境全体で保護されたデータを移行します。	“異なる環境間での仮想マシンの移行” 次のページ
Google Cloudへの災害復旧を実行します。	“Google Cloudへのデータの災害復旧の実行” ページ292

前提条件

- HYCU for Google Cloudのアクティブなサブスクリプションがある。説明については、HYCU for Google Cloudの資料を参照してください。
- Google Cloudサービスアカウントがhycuに追加されている。説明については、“Google Cloudサービスアカウントの追加” ページ212を参照してください。
- HYCU Protégéライセンスを持っている。説明については、“ライセンス” ページ222を参照してください。

異なる環境間での仮想マシンの移行

オンプレミス環境とGoogle Cloud環境全体で保護されたデータを移行できます。

- "クラウドへのデータの移行" 下
- "クラウドからのデータの移行" ページ290

クラウドへのデータの移行

HYCUスピンアップ機能を使用して、仮想マシンと物理マシン、およびそれらで実行されているアプリケーションをクラウドに移行できます。アプリケーションを移行すると、このアプリケーションが実行されている仮想マシン全体がクラウドに移行されることに注意してください。

> 注 仮想マシンデータの保護についての説明は、特に断りのない限り、物理マシンにも適用されます。

前提条件

移行する仮想マシンと移行するアプリケーションを含む仮想マシンは保護されており、バックアップ中にクラウド準備チェックが正常に実行される。詳細については、"HYCU Protégéの詳細" ページ77を参照してください。

制限事項

- *Nutanixクラスターの場合* ボリュームグループは移行できません。
- *vSphere環境の場合* :仮想マシンテンプレートは移行できません。

考慮事項

選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため) がある層が含まれている場合、データを移行するためにこの層を使用することはできません。

仮想マシンまたはアプリケーションデータをクラウドに移行するかどうかに応じて、次のいずれかのパネルにアクセスします。

- 「仮想マシン」パネルへのアクセス

  ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

- 「アプリケーション」パネルへのアクセス

  「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「仮想マシン」または「アプリケーション」パネルで、移行するエンティティを選択します。
2. 画面の下部に表示される「詳細ビュー」で、移行に使用する仮想マシンまたはアプリケーションの復元ポイントを選択します。

> 注「詳細ビュー」は、エンティティをクリックした場合にのみ表示されます。エンティティの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

3. 「**クラウドへのVMスピンアップ**」をクリックします。「クラウドへのVMスピンアップ」ダイアログボックスが表示されます。
4. 「**Google CloudへのVMスピンアップ**」を選択し、「**次へ**」をクリックします。「Google CloudへのVMスピンアップ」ダイアログボックスが表示されます。
5. 「クラウドアカウント」ドロップダウンメニューから、仮想マシンを移行するプロジェクトがリンクされているGoogle Cloudサービスアカウントを選択します。
6. 「プロジェクト」、「ターゲットリージョン」および「ターゲットゾーン」ドロップダウンメニューから必要な値を選択し、「**次へ**」をクリックします。「VM設定」ダイアログボックスが開きます。
7. 「スピンアップ元」ドロップダウンメニューから、移行に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
   - **自動** :クラウドへの最速でのデータの移行が保証されます。
   - **バックアップ**
   - **コピー**
   - **アーカイブ**
   - **スナップショット**
8. 「新しいVM名」フィールドで、移行された仮想マシンインスタンスの名前を入力します。

   > ⚠ 重要 移行した仮想マシンのインスタンス名が一意であることを確認します。

9. 「vCPUコア」フィールドに、移行した仮想マシンの仮想CPU数に仮想CPUあたりのコア数を掛けた数を入力します。指定できるvCPUコアの最大数は1024です。
10. 「メモリ」フィールドで、移行した仮想マシンインスタンスのメモリ量(GiB単位)を設定します。指定する値は整数でなければならず、4096を超えることはできません。既定値は、元の仮想マシンのGiB単位のメモリ量です。
11. 「仮想マシンタイプ」ドロップダウンメニューから、移行する仮想マシンインスタンスのマシンタイプを選択します。

    > 注リストには、指定された数の仮想CPUとメモリ量に一致するマシンタイプが含まれています。そのような一致が存在しない場合は、カスタムマシンタイプを選択できます。これらのマシンタイプの詳細については、Google Cloudの資料を参照してください。

12. 「ネットワークインターフェース」の下に既定のネットワークインターフェースが表示され、(選択したプロジェクトとリージョンに基づいて)どのネットワークに割り当てられているかを確認できます。必要であれば、ネットワーク設定も変更できます。

    ネットワーク設定の変更

    データ保護の要件に応じて、既定のネットワークインターフェースをそのまま使用するか、以下のいずれかを実行できます。

    - 新しいネットワークインターフェースを追加します。
      a. 「**ネットワークインターフェースの追加**」をクリックします。「ネットワークインターフェースの追加」ダイアログボックスが開きます。

b. 「ターゲット ネット ワーク」ドロップダウンメニューから、移行する仮想マシンインスタンスを追加するネットワークを選択します。選択したプロジェクトで構成されているネットワークと、クラウドアカウントがアクセスできるその他のネットワークの中から選択できます。

c. ネットワークインターフェースの外部アドレスタイプを選択し、必要に応じて、目的の外部IPアドレスリソースの名前を選択します。詳細については、HYCU for Google Cloudの資料を参照してください。

d. ネットワークインターフェースの内部アドレスタイプを選択し、必要であれば、アドレスタイプに応じて以下のいずれかを実行します。

   ◦ 「内部アドレス」フィールドに、目的のIPアドレスを入力します。

   ◦ 「内部アドレス」ドロップダウンメニューから、目的の内部IPアドレスリソースの名前を選択します。

   詳細については、HYCU for Google Cloudの資料を参照してください。

e. 「**保存**」をクリックします。

- 既存のネットワークインターフェースの別のネットワークを選択し、「**編集**」をクリックして、必要な変更を加えます。
- 既存のネットワークインターフェースを選択し、「**削除**」をクリックして削除します。

13. *仮想マシンのオペレーティングシステムがまだ検出されていない場合のみ*。仮想マシンのオペレーティングシステムを選択します。
    - **Linux**
    - **Windows**
14. *仮想ディスクが(手動または自動で)バックアップから除外されている場合のみ*.サイズと構成が同じ空のディスクを除外したディスクとして作成し、移行した仮想マシンインスタンスにアタッチする場合は、「**除外ディスクを空ディスクとして作成**」スイッチを使用します。
15. 「**スピンアップ**」をクリックします。

クラウドへの移行ジョブが開始されます。正常に完了すると、移行された仮想マシンインスタンスをHYCU for Google Cloudの「インスタンス」パネルで確認できます。詳細については、HYCU for Google Cloudの資料を参照してください。

クラウドへのデータの移行後

- 仮想マシンにGoogle Compute Engineゲスト環境をインストールします。
- *Windows仮想マシンの場合*.Windowsライセンスを再アクティブ化します。
- HYCU for Google Cloudを使用して、移行した仮想マシンの保護を有効にします。詳細については、HYCU for Google Cloudの資料を参照してください。

クラウドからのデータの移行

HYCUスピンアップ機能を使用して、クラウドから仮想マシンインスタンスを移行できます。

「仮想マシン」パネルへのアクセス

ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、「**クラウドからのVMスピンアップ**」をクリックします。「クラウドからのVMスピンアップ」ダイアログボックスが表示されます。
2. 「**Google CloudからのVMスピンアップ**」を選択し、「**次へ**」をクリックします。「Google CloudからのVMスピンアップ」ダイアログボックスが開きます。
3. 「クラウドアカウント」ドロップダウンメニューから、移行する仮想マシンインスタンスを含むプロジェクトをリンクするGoogle Cloudサービスアカウントを選択します。
4. 「プロジェクト」ドロップダウンメニューから、移行する仮想マシンインスタンスが属するGoogle Cloudプロジェクトを選択します。
5. 「仮想マシン」ドロップダウンメニューから、移行する仮想マシンインスタンスを選択します。
6. 「チェックポイント」ドロップダウンメニューから、仮想マシンインスタンスデータの移行元のチェックポイントを選択します。
7. 「**次へ**」をクリックします。「VM設定」ダイアログボックスが開きます。
8. 「ストレージコンテナ」ドロップダウンメニューから、仮想マシンインスタンスを移行する場所を選択します。
9. 「新しいVM名」フィールドで、移行する仮想マシンの名前を入力します。
10. *移行する仮想マシンインスタンスがオンプレミス環境で作成後にクラウドに移行され、それからオンプレミス環境に移行して戻す場合のみ。*移行された仮想マシンをオンプレミス環境のときと同じ仮想マシン設定にする場合は、「**元のオンプレミス設定を保持する**」オプションを有効にして、手順13に進みます。

    それ以外の場合は、「元のオンプレミス設定を保持する」オプションを無効のままにして、次の手順に進みます。
11. 移行された仮想マシンに以下の値を指定します。
    - 仮想CPUの数 :指定できる最大数は1024です。
    - 仮想CPUあたりのコアの数 :指定できる最大数は64です。
    - メモリ量(GiB単位) :指定する値は整数でなければならず、4096を超えることはできません。

    > 注 既定値は、オンプレミスまたはクラウドのいずれかの、仮想マシンが作成された環境にあった仮想マシンの値です。
12. 「ネットワークアダプタ」で、データ保護の要件に応じて、以下のいずれかを実行します。
    - 1つ以上のネットワークアダプタを追加します。
        a. 「**ネットワークアダプタを追加**」をクリックします。「新しいネットワークアダプタ」ダイアログボックスが開きます。
        b. 「ネットワーク」ドロップダウンメニューから、仮想アダプタのネットワークを選択します。
        c. 「**保存**」をクリックします。
    - 既存のネットワークアダプタを編集して、仮想マシンを別のネットワークに接続します。これを実行するには、ネットワークアダプタを選択し、「**編集**」をクリックし、必要な変更を行います。

- 既存のいずれかのネットワークアダプタを選択し、「**削除**」をクリックして削除します。既存のネットワークアダプタをすべて削除すると、仮想マシンはネットワーク接続なしで移行されます。

13. 移行した仮想マシンを移行後にオンにする場合は、「**仮想マシンの電源をオンにします**」スイッチを使用します。
14. 「**スピンアップ**」をクリックします。

クラウドからの移行ジョブが開始されます。正常に終了すると、移行された仮想マシンを「仮想マシン」パネルに表示できます。

クラウドからのデータの移行後

- 仮想マシンからGoogle Compute Engineゲスト環境を削除します。
- *Nutanix AHVクラスター上の仮想マシンの場合*：仮想マシンに最新バージョンのNGTがインストールされていることを確認します。この実行方法の詳細については、Nutanixの資料を参照してください。
- *Nutanix ESXiクラスターの仮想マシンの場合*：最新バージョンのVMware ToolsとNGTがクライアント仮想マシンにインストールされていることを確認します。この実行方法の詳細については、NutanixおよびVMwareの文書を参照してください。
- *vSphere環境の仮想マシンの場合*：最新バージョンのVMware Toolsが仮想マシンにインストールされていることを確認します。この実行方法の詳細については、VMwareの資料を参照してください。
- *Linux仮想マシンの場合*：Nutanix ESXiクラスターまたはvSphere環境の仮想マシンが起動しない場合は、コントローラータイプをSCSIからSATAに変更し、必要なSCSIドライバーをインストールしてSCSIに切り替えます。
- *Windows仮想マシンの場合*：Windowsライセンスを再アクティブ化します。
- *ネットワーク接続なしで仮想マシンを移行した場合のみ*。仮想マシンで必ずネットワーク設定を構成します。
- 移行したデータの保護を有効にします。この実行方法の詳細については、"仮想マシンの保護" ページ71および"アプリケーションの保護" ページ113を参照してください。

Google Cloudへのデータの災害復旧の実行

災害発生時に、オンプレミス環境からGoogle Cloudにデータの災害復旧を実行できます。

前提条件

- 次の許可を持つGoogleアカウントを持っている。
  - 新しいHYCU Backup Controllerを展開するGoogle Cloudプロジェクトの Google Cloud Storageバケットにアクセスする。
  - 新しいGoogle Cloudを展開するHYCU Backup Controllerプロジェクトに Google Compute Engine仮想マシンインスタンスを展開する。

    - 新しいHYCU Backup Controllerの展開を予定しているGoogle Cloudネットワークでファイアウォールルールをセットアップする。
- 移行する仮想マシンと、移行するアプリケーションがある仮想マシンは保護されており、移行/DR準備完了ステータスである。詳細については、“HYCU Protégéの詳細” ページ77を参照してください。

考慮事項

- HYCU Backup ControllerがGoogle Cloudに展開されている場合、ネットワーク設定の変更はHYCUで禁止されます。
- インポートしたターゲットが、仮想マシンを移行する予定のリージョンにあることを確認します。これにより災害復旧プロセスを、可能な限り迅速に、かつコスト効率よく行うことができます。
- HYCU Backup Controllerを展開した後に、それを災害復旧の実行に使用するためには、HYCU Backup Controllerを保持しておくと、将来の災害復旧に備えることができます。ただし、HYCUをアップグレードするたびに、新しいHYCU Backup Controllerを展開し、クラウドへのデータの災害復旧を実行できるようにする必要があります。

手順

1. HYCU for Google Cloud Webユーザーインターフェースを使用してHYCU Backup Controllerを展開します。この実行方法の詳細については、HYCU for Google Cloudの資料を参照してください。
2. Google Cloudでは、VPCネットワークペインのファイアウォールルールコンテキストで、HYCU Backup Controllerが属するサブネットワーク全体からのTCPポート8443を介した入力ネットワークトラフィックを許可する、新しいファイアウォールルールを作成します。この実行方法の詳細については、Google Cloudの資料を参照してください。
3. 次のURLを指定して、HYCUにログオンします。

   ```
   https://<IPAddress>:8443
   ```

   この場合、*<IPAddress>*は新しく展開されたHYCU Backup Controllerの外部IPアドレスです。
4. 保護された仮想マシンのバックアップデータが保存されているGoogle Cloud Storageバケットにアクセスする許可を持つGoogle Cloudサービスアカウントを追加します。この実行方法の詳細については、“Google Cloudサービスアカウントの追加” ページ212を参照してください。
5. バックアップデータを含むGoogle Cloudターゲットをインポートします。
   a. 「ターゲット」パネルで、「**インポート**」をクリックします。「ターゲットのインポート」ダイアログボックスが表示されます。
   b. 「バケット名」フィールドで、元のターゲット構成で指定されていた名前を入力します。
   c. 「クラウドアカウント」ドロップダウンリストから、インポートされたGoogle Cloudサービスアカウントを選択し、「**次へ**」をクリックします。
   d. ターゲット名をクリックして選択を確認し、「**次へ**」をクリックします。
   e. 「複数のターゲット」ダイアログボックスに、バックアップデータを格納する1つ以上のターゲットが表示されます。追加のターゲットが見つかった場合は、それらを1つずつ選択して、元のター

ゲット構成と一致するように値を指定します。ターゲットごとに、「**検証**」をクリックして構成を確認します。

f. 復元に必要なすべてのターゲットを検証したら、「**インポート**」をクリックします。

6. 仮想マシンまたはアプリケーションをクラウドに移行します。この実行方法の詳細については、"クラウドへのデータの移行" ページ288を参照してください。

オンプレミス環境とAzure環境全体でのデータの保護

HYCU Protégéはスピンアップ機能を使用して、保護されたデータをオンプレミス環境とAzure環境間で移行することにより、データの復元力を保証します。災害発生時に、オンプレミス環境で、Azureへのデータの災害復旧を提供します。

前提条件

- HYCU for Azureのアクティブなサブスクリプションがある。詳細については、HYCU for Azureの資料を参照してください。
- Azureサービスプリンシパルが HYCUに追加されている。説明については、"Azureサービスプリンシパルの追加" ページ213を参照してください。
- HYCU Protégéライセンスを持っている。詳細については、"ライセンス" ページ222を参照してください。
- Azureに専用のストレージアカウントを作成しました。このストレージアカウントは、移行する予定の仮想マシンと同じリージョンとリソースグループに属している必要があり、そのタイプはStandard汎用v2またはPremiumブロックBlobのいずれかである必要があります。

実行内容に応じて、以下のいずれかを参照してください。

目的	説明
オンプレミス環境とAzure環境全体で保護されたデータを移行します。	"異なる環境間での仮想マシンの移行" 下
Azureへのデータの災害復旧を実行します。	"Azureへのデータの災害復旧の実行" ページ300

異なる環境間での仮想マシンの移行

オンプレミス環境とAzure環境全体で保護されたデータを移行できます。

- "クラウドへのデータの移行" 下
- "クラウドからのデータの移行" ページ298

クラウドへのデータの移行

HYCUスピンアップ機能を使用して、仮想マシンと物理マシン、およびそれらで実行されているアプリケーションをAzureに移行できます。アプリケーションを移行すると、このアプリケーションが実行されてい

る仮想マシン全体がクラウドに移行されることに注意してください。

> 注 仮想マシンデータの保護についての説明は、特に断りのない限り、物理マシンにも適用されます。

前提条件

移行する仮想マシンと移行するアプリケーションを含む仮想マシンは保護されており、バックアップ中にクラウド準備チェックが正常に実行される。詳細については、"HYCU Protégéの詳細" ページ77を参照してください。

制限事項

- *Nutanixクラスターの場合* :ボリュームグループは移行できません。
- *vSphere環境の場合* :仮想マシンテンプレートは移行できません。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため)がある層が含まれている場合、データを移行するためにこの層を使用することはできません。
- データをクラウドに移行すると、移行した仮想マシンにAzure一時ディスクが自動的に割り当てられます。このディスクは管理対象ディスクではなく、短期間のデータストレージにのみ使用されます。
- *セキュアブートが有効になっている仮想マシンの場合* :Azureは現在仮想マシンのセキュアブート機能をサポートしていないため、そのような仮想マシンをクラウドに移行すると、そのマシンではセキュアブートを有効にできなくなります。

仮想マシンまたはアプリケーションデータをクラウドに移行するかどうかに応じて、次のいずれかのパネルにアクセスします。

- 「仮想マシン」パネルへのアクセス

  ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

- 「アプリケーション」パネルへのアクセス

  「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「仮想マシン」または「アプリケーション」パネルで、移行するエンティティを選択します。
2. 画面の下部に表示される「詳細ビュー」で、移行に使用する仮想マシンまたはアプリケーションの復元ポイントを選択します。

   > 注 「詳細ビュー」は、エンティティをクリックした場合にのみ表示されます。エンティティの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

3. 「**クラウドへのVMスピンアップ**」をクリックします。「クラウドへのVMスピンアップ」ダイアログボックスが表示されます。
4. 「**AzureへのVMのスピンアップ**」を選択し、「**次へ**」をクリックします。「AzureへのVMのスピンアップ」ダイアログボックスが表示されます。
5. 「サービスプリンシパル」ドロップダウンメニューから、必要なリソースにアクセスできるサービスプリンシパルを選択します。
6. 「サブスクリプション」ドロップダウンメニューから、移行する仮想マシンの適切なサブスクリプションを選択します。
7. 「リソースグループ」ドロップダウンメニューから、移行する仮想マシンのリソースグループを選択します。
8. 「ロケーション」ドロップダウンメニューから、移行する仮想マシンの地理的リージョンを選択します。
9. 「アベイラビリティゾーン」ドロップダウンメニューから、移行する仮想マシンのゾーンを選択します。

   > 注 選択した地理的リージョンと仮想マシンのサイズによって、データを移行できるゾーンが決まります。どのゾーンにもデータを移行しない場合は、「**なし**」を選択します。

10. 「ストレージアカウント」ドロップダウンメニューから、移行操作専用のストレージアカウントを選択します。
11. 「**次へ**」をクリックします。「VM設定」ダイアログボックスが開きます。
12. 「スピンアップ元」ドロップダウンメニューから、移行に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
    - **自動** :クラウドへの最速でのデータの移行が保証されます。
    - **バックアップ**
    - **コピー**
    - **アーカイブ**
    - **スナップショット**
13. 「新しいVM名」フィールドで、移行する仮想マシンの名前を入力します。
14. 「vCPUコア」フィールドに、移行する仮想マシンに割り当てられた仮想CPU数に仮想CPUあたりのコア数を掛けた数を入力します。指定できる最大数は1024です。
15. 「メモリ」フィールドで、移行する仮想マシンに割り当てるメモリの量(GiB単位)を入力します。指定する値は整数でなければならず、4096を超えることはできません。
16. 「仮想マシンタイプ」ドロップダウンメニューから、仮想マシンタイプを選択します。

    > 注 使用可能な仮想マシンタイプのリストは、指定した仮想CPUコアの数とメモリの量に基づいています。指定した値に正確に対応する仮想マシンタイプがない場合は、最も近いものが表示されます。

17. 「ネットワークインターフェース」の下で、移行された仮想マシンに追加されるネットワークインターフェースを表示できます。既定では、これは移行された仮想マシン用に選択したサブスクリプションの最初のネットワークインターフェースです。必要であれば、ネットワーク設定も変更できます。

    ネットワーク設定の変更

ネットワーク設定を変更する場合は、ネットワークインターフェースの追加、既存のネットワークインターフェースの編集、またはネットワークインターフェースの削除を行うことができます。

> 注 ネットワークインターフェースを追加する場合、同じネットワークにアタッチされているネットワークインターフェースしか追加できないことに注意してください。追加できるネットワークインターフェースの最大数は、選択した仮想マシンのタイプによって異なります。

ネットワーク設定の変更方法に応じて、次のいずれかを実行します。

- 「**ネットワークインターフェースの追加**」をクリックしてネットワークインターフェースを追加するか、編集するネットワークインターフェースの横にある「**編集**」をクリックして、次の手順に従います。
  a. *ネットワークインターフェースを追加する場合のみ*。「ネットワーク」ドロップダウンメニューから、ネットワークインターフェースのネットワークを選択します。
     > 注 使用可能なネットワークのリストには、移行された仮想マシン用に選択したリージョン内のネットワークのみが含まれます。
  b. ネットワークインターフェースを割り当てるサブネットを選択します。
  c. 「パブリックIPアドレスタイプ」フィールドで、ネットワークインターフェースのパブリックIPアドレスを選択します。次のオプションから選択できます。

オプション	説明
なし	パブリックIPアドレスは、移行された仮想マシン上のネットワークインターフェースに割り当てられません。
動的	動的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。
静的	静的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。
既存	Azureで作成した優先パブリックIPアドレスのリソースが、移行した仮想マシンのネットワークインターフェースに割り当てられます。

  d. 「プライベートIPアドレスタイプ」フィールドで、ネットワークインターフェースのプライベートIPアドレスを選択します。次のオプションから選択できます。

オプション	説明
動的	動的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。
静的	指定する静的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。

  e. 「**追加**」または「**保存**」をクリックします。
- 削除するネットワークインターフェースの横にある「**削除**」をクリックします。ネットワークインターフェースがないと仮想マシンを移行できないことに注意してください。

18. *仮想マシンのオペレーティングシステムがまだ検出されていない場合のみ*。仮想マシンのオペレーティングシステムを選択します。
    - **Linux**
    - **Windows**
19. *仮想ディスクが(手動または自動で)バックアップから除外されている場合のみ*:サイズと構成が同じ空のディスクを除外したディスクとして作成し、移行した仮想マシンにアタッチする場合は、「**除外ディスクを空ディスクとして作成**」スイッチを使用します。
20. 「**スピンアップ**」をクリックします。

クラウドへの移行ジョブが開始されます。正常に終了すると、移行された仮想マシンをHYCU for Azureの「仮想マシン」パネルに表示できます。詳細については、HYCU for Azureの資料を参照してください。

クラウドへのデータの移行後

- *Windows仮想マシンの場合*:Windowsライセンスを再アクティブ化します。
- *Linux仮想マシンの場合*:Hyper-VおよびAzure用のLinux統合サービスを仮想マシンにインストールします。詳細については、Microsoftの資料を参照してください。
- HYCU for Azureを使用して、移行した仮想マシンの保護を有効にします。この実行方法の詳細については、HYCU for Azureの資料を参照してください。

クラウドからのデータの移行

HYCUスピンアップ機能を使用して、Azureから仮想マシンを移行できます。

制限事項

Nutanixクラスターの場合:Azure Generation 2仮想マシンは、UEFI仮想マシンをサポートするクラスターにのみ移行できます。

考慮事項

クラウドからデータを移行した後、移行された仮想マシンには、Azureで自動的に割り当てられた一時ディスクは含まれません。

> 「仮想マシン」パネルへのアクセス
>
> ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

手順

1. 「仮想マシン」パネルで、「**クラウドからのVMスピンアップ**」をクリックします。「クラウドからのVMスピンアップ」ダイアログボックスが表示されます。
2. 「**AzureからのVMのスピンアップ**」を選択し、「**次へ**」をクリックします。「AzureからのVMのスピンアップ」ダイアログボックスが表示されます。
3. 「サービスプリンシパル」ドロップダウンメニューから、必要なリソースにアクセスできるサービスプリンシパルを選択します。

4. 「サブスクリプション」ドロップダウンメニューから、移行する仮想マシンが属するHYCU for Azureサブスクリプションを選択します。
5. 「リソースグループ」ドロップダウンメニューから、移行する仮想マシンが属するリソースグループを選択します。
6. 「仮想マシン」ドロップダウンメニューから、移行する仮想マシンを選択します。
7. 「チェックポイント」ドロップダウンメニューから、仮想マシンデータの移行元のチェックポイントを選択します。
8. 「ストレージアカウント」ドロップダウンメニューから、移行操作専用のストレージアカウントを選択します。
9. 「**次へ**」をクリックします。「VM設定」ダイアログボックスが表示されます。
10. 「ストレージコンテナ」ドロップダウンメニューから、仮想マシンを移行する場所を選択します。
11. 「新しいVM名」フィールドで、移行する仮想マシンの名前を入力します。
12. *移行する仮想マシンがオンプレミス環境で作成後にクラウドに移行され、それからオンプレミス環境に移行して戻す場合のみ。*仮想マシンをオンプレミス環境のときと同じ仮想マシン設定にする場合は、「**元のオンプレミス設定を保持する**」オプションを有効にして、手順15に進みます。

    それ以外の場合は、「元のオンプレミス設定を保持する」オプションを無効のままにして、次の手順に進みます。
13. 移行された仮想マシンに以下の値を指定します。
    - 仮想CPUの数 :指定できる最大数は1024です。
    - 各仮想CPUに割り当てられるコアの数 :指定できる最大数は64です。
    - メモリ量(GiB単位) :指定する値は整数でなければならず、4096を超えることはできません。

    > 注 既定値は、オンプレミスまたはクラウドのいずれかの、仮想マシンが作成された環境にあった仮想マシンの値です。
14. 「ネットワークアダプタ」で、データ保護の要件に応じて、以下のいずれかを実行します。
    - 1つ以上のネットワークアダプタを追加します。
      a. 「**ネットワークアダプタを追加**」をクリックします。「ネットワーク」ダイアログボックスが表示されます。
      b. 「ネットワーク」ドロップダウンメニューから、ネットワークアダプタの仮想ネットワークを選択します。
      c. 「**追加**」をクリックします。
    - 既存のネットワークアダプタを編集して、仮想マシンを別のネットワークに接続します。これを実行するには、ネットワークアダプタを選択し、「**編集**」をクリックし、必要な変更を行います。
    - 既存のいずれかのネットワークアダプタを選択し、「**削除**」をクリックして削除します。既存のネットワークアダプタをすべて削除すると、仮想マシンはネットワーク接続なしで移行されます。

15. 移行した仮想マシンを移行後にオンにする場合は、「**仮想マシンの電源をオンにします**」スイッチを使用します。
16. 「**スピンアップ**」をクリックします。

クラウドからの移行ジョブが開始されます。正常に終了すると、移行された仮想マシンを「仮想マシン」パネルに表示できます。

クラウドからのデータの移行後

- *Nutanix AHVクラスター上の仮想マシンの場合*：仮想マシンに最新バージョンのNGTがインストールされていることを確認します。詳細については、Nutanixの資料を参照してください。
- *Nutanix ESXiクラスターの仮想マシンの場合*：最新バージョンのVMware ToolsとNGTがクライアント仮想マシンにインストールされていることを確認します。詳細については、NutanixとVMwareの資料を参照してください。
- *vSphere環境の仮想マシンの場合*：最新バージョンのVMware Toolsが仮想マシンにインストールされていることを確認します。詳細については、VMwareの資料を参照してください。
- *Windows仮想マシンの場合*：Windowsライセンスを再アクティブ化します。
- *Linux仮想マシンの場合*：Nutanix ESXiクラスターまたはvSphere環境の仮想マシンが起動しない場合は、ディスクコントローラーをSCSIからIDEに変更してから、最新バージョンのVMware Toolsを仮想マシンにインストールします。後でディスクコントローラーをSCSIに戻すことができます。
- *ネットワーク接続なしで仮想マシンを移行した場合のみ*。仮想マシンで必ずネットワーク設定を構成します。
- 移行したデータの保護を有効にします。詳細については、"仮想マシンの保護" ページ71と"アプリケーションの保護" ページ113を参照してください。

Azureへのデータの災害復旧の実行

災害発生時に、オンプレミス環境からAzureへのデータの災害復旧を実行できます。

前提条件

移行する仮想マシンと、移行するアプリケーションがある仮想マシンは保護されており、移行/DR準備完了ステータスである。詳細については、"HYCU Protégéの詳細" ページ77を参照してください。

考慮事項

- HYCU Backup ControllerがAzureに展開されている場合、ネットワーク設定の変更はHYCUで禁止されます。
- インポートしたターゲットが、仮想マシンを移行する予定のリージョンにあることを確認します。これにより災害復旧プロセスを、可能な限り迅速に、かつコスト効率よく行うことができます。
- HYCU Backup Controllerを展開した後に、それを災害復旧の実行に使用するためには、HYCU Backup Controllerを保持しておくと、将来の災害復旧に備えることができます。ただし、HYCUをアップグレードするたびに、新しいHYCU Backup Controllerを展開し、クラウドへのデータの災害復旧を実行できるようにする必要があります。

手順

1. HYCU for Azure Webユーザーインターフェースを使用してHYCU Backup Controllerを展開します。この実行方法の詳細については、HYCU for Azureの資料を参照してください。
2. Azureで、HYCU Backup Controllerが属するサブネットワーク全体からの入力ネットワークトラフィックをTCPポート8443で許可する新しいファイアウォールルールを作成します。詳細については、Azureの資料を参照してください。
3. 以下のURLを指定してHYCU Webユーザーインターフェースにログオンします。

   ```
   https://<IPAddress>:8443
   ```

   この場合、*<IPAddress>*は新しく展開されたHYCU Backup Controllerの外部IPアドレスです。

   > ⚠ **重要** 仮想マシン作成時にAzureで指定した資格情報を使用してHYCUにログインし、Azureへのデータの災害復旧を実行することはできません。SSHを使用してHYCUにログインまたはHYCU Backup Controllerにアクセスするために使用できる資格情報の詳細については、"HYCUへのログオン" ページ29または"SSHを使用したHYCU Backup Controller仮想マシンへのアクセス" ページ258を参照してください。

4. バックアップデータが保存されているAzureターゲットをHYCUにインポートします。
   a. 「ターゲット」パネルで、「**インポート**」をクリックします。「ターゲットのインポート」ダイアログボックスが表示されます。
   b. 「タイプ」ドロップダウンメニューから、「**Azure**」を選択します
   c. 「ストレージアカウント名」フィールドに、元のターゲット構成で指定されたAzureストレージアカウント名を入力します。
   d. 「シークレットアクセスキー」フィールドに、Azureアカウントのシークレットアクセスキーを入力します。
   e. 「ストレージコンテナ名」に、ターゲットに関連付けられているストレージコンテナの名前と、バックアップデータが保存される場所を入力します。
   f. 「**次へ**」をクリックします。「バックアップカタログのインポート」ダイアログボックスが表示されます。
   g. バックアップデータをインポートするHYCU Backup Controllerを選択し、「**次へ**」をクリックします。
   h. 「複数のターゲット」ダイアログボックスで、以下のいずれかを実行します。
      - *バックアップデータが1つのターゲットに保存されている場合：*

        「**インポート**」をクリックします。
      - *バックアップデータが複数のターゲットに保存されている場合：*
        i. 各ターゲットを1つずつ選択し、元のターゲット構成と一致するように値を指定します。
        ii. ターゲットごとに、「**検証**」をクリックして構成を確認します。
        iii. 「**インポート**」をクリックします。

5. 仮想マシンまたはアプリケーションをクラウドに移行します。説明については、"クラウドへのデータの移行" ページ294を参照してください。

オンプレミス環境とAzure US Government環境全体でのデータの保護

スピンアップ機能を使用して、保護されたデータをオンプレミス環境からAzure US Governmentに移行することにより、HYCU Protégéはデータの復元性を保証します。災害発生時に、オンプレミス環境で、Azure US Governmentへのデータの災害復旧を提供します。

前提条件

- Azure US Governmentサービスプリンシパルが HYCUに追加されている。説明については、"Azure US Governmentサービスプリンシパルの追加" ページ215を参照してください。
- HYCU Protégéライセンスを持っている。詳細については、"ライセンス" ページ222を参照してください。

実行内容に応じて、以下のいずれかを参照してください。

目的	説明
保護データをオンプレミス環境からAzure US Governmentに移行します。	"仮想マシンのクラウドへの移行" 下
Azure US Governmentへの災害復旧を実行します。	"Azure US Governmentへのデータの災害復旧の実行" ページ306

仮想マシンのクラウドへの移行

HYCUスピンアップ機能を使用して、仮想マシンと物理マシン、およびそれらで実行されているアプリケーションをAzure US Governmentに移行できます。アプリケーションを移行すると、このアプリケーションが実行されている仮想マシン全体がクラウドに移行されることに注意してください。

> 注 仮想マシンデータの保護についての説明は、特に断りのない限り、物理マシンにも適用されます。

前提条件

移行する仮想マシンと移行するアプリケーションを含む仮想マシンは保護されており、バックアップ中にクラウド準備チェックが正常に実行される。詳細については、"HYCU Protégéの詳細" ページ77を参照してください。

制限事項

- *Nutanixクラスターの場合* ボリュームグループは移行できません。
- *vSphere環境の場合* 仮想マシンテンプレートは移行できません。

考慮事項

- 選択した復元ポイントに、不完全なバックアップチェーン(1つ以上のバックアップ、バックアップデータのコピー、またはデータアーカイブが存在しないか、非アクティブ化されたターゲットに保存されているため) がある層が含まれている場合、データを移行するためにこの層を使用することはできません。
- データをクラウドに移行すると、移行した仮想マシンにAzure一時ディスクが自動的に割り当てられます。このディスクは管理対象ディスクではなく、短期間のデータストレージにのみ使用されます。
- *セキュアブートが有効になっている仮想マシンの場合* :Azureは現在仮想マシンのセキュアブート機能をサポートしていないため、そのような仮想マシンをクラウドに移行すると、そのマシンではセキュアブートを有効にできなくなります。

仮想マシンまたはアプリケーションデータをクラウドに移行するかどうかに応じて、次のいずれかのパネルにアクセスします。

- 「仮想マシン」パネルへのアクセス

  ナビゲーションペインの「仮想マシン」パネルにアクセスするには、「**仮想マシン**」をクリックします。

- 「アプリケーション」パネルへのアクセス

  「アプリケーション」パネルにアクセスするには、ナビゲーションペインで、「**アプリケーション**」をクリックします。

手順

1. 「仮想マシン」または「アプリケーション」パネルで、移行するエンティティを選択します。
2. 画面の下部に表示される「詳細ビュー」で、移行に使用する仮想マシンまたはアプリケーションの復元ポイントを選択します。

   > 注「詳細ビュー」は、エンティティをクリックした場合にのみ表示されます。エンティティの名前の前のチェックボックスを選択しても、「詳細ビュー」は開きません。

3. 「**クラウドへのVMスピンアップ**」をクリックします。「クラウドへのVMスピンアップ」ダイアログボックスが表示されます。
4. 「**Azure US GovernmentへのVMのスピンアップ**」を選択し、「**次へ**」をクリックします。「Azure US GovernmentへのVMのスピンアップ」ダイアログボックスが表示されます。
5. 「サービスプリンシパル」ドロップダウンメニューから、必要なリソースにアクセスできるサービスプリンシパルを選択します。
6. 「サブスクリプション」ドロップダウンメニューから、移行する仮想マシンの適切なサブスクリプションを選択します。
7. 「リソースグループ」ドロップダウンメニューから、移行する仮想マシンのリソースグループを選択します。
8. 「ロケーション」ドロップダウンメニューから、移行する仮想マシンの地理的リージョンを選択します。
9. 「アベイラビリティゾーン」ドロップダウンメニューから、移行する仮想マシンのゾーンを選択します。

> 注 選択した地理的リージョンと仮想マシンのサイズによって、データを移行できるゾーンが決まります。どのゾーンにもデータを移行しない場合は、「**なし**」を選択します。

10. 「**次へ**」をクリックします。「VM設定」ダイアログボックスが開きます。
11. 「スピンアップ元」ドロップダウンメニューから、移行に使用する層を選択します。復元ポイントには1つ以上の層を含めることができ、その中から以下を選択できます。
    - **自動** :クラウドへの最速でのデータの移行が保証されます。
    - **バックアップ**
    - **コピー**
    - **アーカイブ**
    - **スナップショット**
12. 「新しいVM名」フィールドで、移行する仮想マシンの名前を入力します。
13. 「vCPUコア」フィールドに、移行する仮想マシンに割り当てられた仮想CPU数に仮想CPUあたりのコア数を掛けた数を入力します。指定できる最大数は1024です。
14. 「メモリ」フィールドで、移行する仮想マシンに割り当てるメモリの量(GiB単位)を入力します。指定する値は整数でなければならず、4096を超えることはできません。
15. 「仮想マシンタイプ」ドロップダウンメニューから、仮想マシンタイプを選択します。

    > 注 使用可能な仮想マシンタイプのリストは、指定した仮想CPUコアの数とメモリの量に基づいています。指定した値に正確に対応する仮想マシンタイプがない場合は、最も近いものが表示されます。

16. 「ネットワークインターフェース」の下で、移行された仮想マシンに追加されるネットワークインターフェースを表示できます。既定では、これは移行された仮想マシン用に選択したサブスクリプションの最初のネットワークインターフェースです。必要であれば、ネットワーク設定も変更できます。

    ネットワーク設定の変更

    ネットワーク設定を変更する場合は、ネットワークインターフェースの追加、既存のネットワークインターフェースの編集、またはネットワークインターフェースの削除を行うことができます。

    > 注 ネットワークインターフェースを追加する場合、同じネットワークにアタッチされているネットワークインターフェースしか追加できないことに注意してください。追加できるネットワークインターフェースの最大数は、選択した仮想マシンのタイプによって異なります。

    ネットワーク設定の変更方法に応じて、次のいずれかを実行します。

    - 「**ネットワークインターフェースの追加**」をクリックしてネットワークインターフェースを追加するか、編集するネットワークインターフェースの横にある「**編集**」をクリックして、次の手順に従います。
      a. *ネットワークインターフェースを追加する場合のみ*。「ネットワーク」ドロップダウンメニューから、ネットワークインターフェースのネットワークを選択します。

      > 注 使用可能なネットワークのリストには、移行された仮想マシン用に選択したリージョン内のネットワークのみが含まれます。

      b. ネットワークインターフェースを割り当てるサブネットを選択します。

c. 「パブリックIPアドレスタイプ」フィールドで、ネットワークインターフェースのパブリックIPアドレスを選択します。次のオプションから選択できます。

オプション	説明
なし	パブリックIPアドレスは、移行された仮想マシン上のネットワークインターフェースに割り当てられません。
動的	動的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。
静的	静的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。
既存	Azure US Governmentで作成した優先パブリックIPアドレスのリソースが、移行した仮想マシンのネットワークインターフェースに割り当てられます。

d. 「プライベートIPアドレスタイプ」フィールドで、ネットワークインターフェースのプライベートIPアドレスを選択します。次のオプションから選択できます。

オプション	説明
動的	動的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。
静的	指定する静的IPアドレスが、移行された仮想マシン上のネットワークインターフェースに割り当てられます。

e. 「**追加**」または「**保存**」をクリックします。

- 削除するネットワークインターフェースの横にある「 **削除**」をクリックします。ネットワークインターフェースがないと仮想マシンを移行できないことに注意してください。

17. *仮想マシンのオペレーティングシステムがまだ検出されていない場合のみ*。仮想マシンのオペレーティングシステムを選択します。
    - **Linux**
    - **Windows**
18. *仮想ディスクが(手動または自動で)バックアップから除外されている場合のみ*.サイズと構成が同じ空のディスクを除外したディスクとして作成し、移行した仮想マシンにアタッチする場合は、「**除外ディスクを空ディスクとして作成**」スイッチを使用します。
19. 「**スピンアップ**」をクリックします。

クラウドへの移行ジョブが開始されます。

クラウドへのデータの移行後

- *Windows仮想マシンの場合*：Windowsライセンスを再アクティブ化します。
- *Linux仮想マシンの場合*：Hyper-VおよびAzure用のLinux統合サービスを仮想マシンにインストールします。詳細については、Microsoftの資料を参照してください。

Azure US Governmentへのデータの災害復旧の実行

災害発生時に、オンプレミス環境からAzure US Governmentにデータの災害復旧を実行できます。

前提条件

- 移行する仮想マシンと、移行するアプリケーションがある仮想マシンは保護されており、移行/DR準備完了ステータスである。詳細については、"HYCU Protégéの詳細" ページ77を参照してください。
- Azure US GovernmentのHYCU仮想アプライアンスイメージがある。イメージと詳細な手順を入手するには、HYCUカスタマーサポートにお問い合わせください。

考慮事項

- HYCU Backup ControllerがAzure US Governmentに展開されている場合、ネットワーク設定の変更はHYCUで禁止されます。
- インポートしたターゲットが、仮想マシンを移行する予定のリージョンにあることを確認します。これにより災害復旧プロセスを、可能な限り迅速に、かつコスト効率よく行うことができます。
- HYCU Backup Controllerを展開した後に、それを災害復旧の実行に使用するためには、HYCU Backup Controllerを保持しておくと、将来の災害復旧に備えることができます。ただし、HYCUをアップグレードするたびに、新しいHYCU Backup Controllerを展開し、クラウドへのデータの災害復旧を実行できるようにする必要があります。

手順

1. HYCU Backup Controllerをデプロイします。
   a. Azure US Governmentで、HYCU仮想アプライアンスイメージから管理イメージを作成します。
   b. 管理対象イメージから仮想マシンを作成します。仮想マシンが、パブリックIPアドレスとサイズが32 GiBの追加ディスクで構成されていることを確認します。

   詳細については、Azureの資料を参照してください。
2. Azure US Governmentで、HYCU Backup Controllerが属するサブネットワーク全体からのTCPポート8443での入力ネットワークトラフィックを許可する新しいファイアウォールルールを作成します。詳細については、Azureの資料を参照してください。
3. 以下のURLを指定してHYCU Webユーザーインターフェースにログオンします。

   ```
   https://<IPAddress>:8443
   ```

   この場合、*<IPAddress>*は新しく展開されたHYCU Backup Controllerの外部IPアドレスです。

> ⚠ 重要 仮想マシン作成時にAzure US Governmentで指定した資格情報を使用してHYCUにログインし、Azure US Governmentへのデータの災害復旧を実行することはできません。SSHを使用してHYCUにログインまたはHYCU Backup Controllerにアクセスするために使用できる資格情報の詳細については、"HYCUへのログオン" ページ29または"SSHを使用したHYCU Backup Controller仮想マシンへのアクセス" ページ258を参照してください。

4. バックアップデータが保存されているAzure US Governmentターゲットを HYCUにインポートします。
   a. 「ターゲット」パネルで、「**インポート**」をクリックします。「ターゲットのインポート」ダイアログボックスが表示されます。
   b. 「タイプ」ドロップダウンメニューから、「**AZURE Government**」を選択します
   c. 「ストレージアカウント名」フィールドに、元のターゲット構成で指定されたAzure US Governmentストレージアカウント名を入力します。
   d. 「シークレットアクセスキー」フィールドに、Azure US Governmentアカウントのシークレットアクセスキーを入力します。
   e. 「ストレージコンテナ名」に、ターゲットに関連付けられているストレージコンテナの名前と、バックアップデータが保存される場所を入力します。
   f. 「**次へ**」をクリックします。「バックアップカタログのインポート」ダイアログボックスが表示されます。
   g. バックアップデータをインポートするHYCU Backup Controllerを選択し、「**次へ**」をクリックします。
   h. 「複数のターゲット」ダイアログボックスで、以下のいずれかを実行します。
      - *バックアップデータが1つのターゲットに保存されている場合：*

        「**インポート**」をクリックします。
      - *バックアップデータが複数のターゲットに保存されている場合：*
        i. 各ターゲットを1つずつ選択し、元のターゲット構成と一致するように値を指定します。
        ii. ターゲットごとに、「**検証**」をクリックして構成を確認します。
        iii. 「**インポート**」をクリックします。
5. 仮想マシンまたはアプリケーションをクラウドに移行します。説明については、"仮想マシンのクラウドへの移行" ページ302を参照してください。

付録A

HYCU構成設定のカスタマイズ

すべてのHYCU構成設定は、HYCU Backup Controllerの/opt/grizzlyフォルダにあるconfig.properties.templateファイル内にあります。このファイルには、使用可能なすべての構成設定とその既定値のリストが含まれています。特定のデータ保護環境の要件に合わせてこれらの構成設定を調整し、最適なパフォーマンスを提供する場合は、同じフォルダ内に新しいconfig.propertiesファイルを作成し、目的の構成設定と新しい値を指定します。

> 注 HYCUをアップグレードしても、config.propertiesファイルは保持されます。ただし、新しいHYCUバージョンで使用できる新しい構成設定については、更新されたconfig.properties.templateファイルから確認できます。

カスタマイズする構成設定に応じて、以下のいずれかのセクションを参照してください。

- “スナップショットの設定” 次のページ
- “使用率のしきい値設定” 次のページ
- “表示設定” ページ310
- “SQL Serverアプリケーション設定” ページ310
- “ジョブを中止するための設定” ページ310
- 「HTTPS for WinRMの構成設定」
- “ファイルサーバー設定” ページ311
- “データリハイドレートの設定” ページ312
- “災害復旧の設定” ページ312
- “ユーザー管理の設定” ページ313

手順

1. HYCU Backup Controller仮想マシンへのリモートセッションを開きます。

   ```
   ssh hycu@<HYCUBackupControllerIPAddress>
   ```

   要求されたら、hycuユーザーのパスワードを入力します。

   SSHを使用したHYCU Backup Controller仮想マシンへのアクセスの詳細については、“SSHを使用したHYCU Backup Controller仮想マシンへのアクセス” ページ258を参照してください。

2. 次のいずれかのテキストエディターを使用して、config.propertiesファイルにアクセスして開きます。

- Vim：

```
sudo vi /opt/grizzly/config.properties
```

- Nano：

```
sudo nano /opt/grizzly/config.properties
```

3. 必要に応じて、既存の構成設定を編集します。
4. config.propertiesファイルを保存して終了します。

構成設定への変更は、config.properties.templateファイル内のReloadClassアノテーションに基づいて適用されます。

アノテーション	説明
Job	変更は、新しいジョブが開始されるときに適用されます。
Mount	新しいターゲットがHYCUに追加されるか、既存のターゲットがアクティブ化されると、変更が適用されます。
Operation	変更は、ジョブを作成しない新しい操作が実行されるときに適用されます(たとえば、HYCU Webユーザーインターフェース、REST API、SSH、またはWinRMを使用する場合) 。
Service	HYCUアプリケーションサーバー(Grizzlyサーバー) を再起動すると、変更が適用されます。

構成設定にアノテーションがない場合は、HYCUアプリケーションサーバー(Grizzlyサーバー) を再起動することをお勧めします。そうするには、以下のコマンドを実行します。

```
sudo service grizzly restart
```

スナップショットの設定

以下の設定を使用して、イベントがトリガーされるスナップショット保持しきい値を構成できます。

設定	説明
max.snapshots.per.vm	仮想マシンごとに保持されるスナップショットの数が、指定された値を超えると、警告イベントがトリガーされます。既定値は24です。
max.snapshots.per.cluster	Nutanixクラスターごとに保持されるスナップショットの数が、指定された値を超えると、警告イベントがトリガーされます。既定値は2400です。

使用率のしきい値設定

次の設定を使用して、システムとデータディスク、およびターゲット使用率のしきい値を構成できます。

設定	説明
controller.disk.full.warning.threshold.fraction	システムまたはデータディスクのHYCU Backup Controller使用率が、指定された値を超えると、イベントがトリガーされます。既定値は0.90です。
target.utilization.threshold.red.fraction	ターゲットのHYCU Backup Controller使用率が、指定された値を超えると、そのヘルスステータスインジケータは赤になります。既定値は0.95です。
target.utilization.threshold.yellow.fraction	ターゲットのHYCU Backup Controller使用率が、指定された値を超えると、そのヘルスステータスインジケータは黄色になります。既定値は0.90です。

ターゲットの正常性ステータスの詳細については、"ターゲット情報の表示" ページ185を参照してください。

表示設定

以下の設定を使用して、表示される項目の最大数をカスタマイズできます。

設定	説明
items.per.directory.in.flr	個別のファイルを復元するときに各ディレクトリに表示されるファイルの最大数。既定値は1000です。

SQL Serverアプリケーション設定

次の設定を使用して、SQL Serverアプリケーションのバックアップをカスタマイズできます。

設定	説明
sql.translog.compress	SQL Serverアプリケーションのバックアップ中に、既定でトランザクションログの圧縮が有効になります(既定値は`true`です)。無効にする場合は、この設定値は必ず`false`にします。

ジョブを中止するための設定

次の設定を使用して、実行ステータスのジョブが自動的に中止されるタイミングを構成できます。

設定	説明
jobs.abort.deadline.minutes	ジョブが完了しなければならない時間(分単位)。既定値は1440です。

設定	説明
jobs.abort.interval.minutes	jobs.abort.deadline.minutes設定で指定されたよりも長くこのステータスになっている場合、実行ステータスのすべてのジョブが取得されて停止される時間間隔(分単位)。既定値は15です。

HTTPS for WinRMの構成設定

以下の設定を使用して、HTTPS for WinRMを構成できます。

設定	説明
winrm.https.enabled	HYCUは、仮想マシンにHTTP for WinRM接続を使用するように事前構成されています。HYCUで代わりにHTTPSを使用する場合は、この設定の値を`true`に設定してから、"HTTPS for WinRM接続の有効化" ページ260で説明されている手順を実行します。
winrm.fallback.http	*winrm.https.enabledの設定がtrueのときにHTTPSを構成する場合*:`true`に設定すると、HYCUは、証明書の問題のためにHTTPSの使用が失敗した場合に、仮想マシンへのHTTP for WinRM接続を使用します。

ファイルサーバー設定

以下の設定を使用して、ファイル共有バックアップを構成できます。

設定	説明
afs.reindex.interval.count	完全インデックス再作成が実行される増分ファイル共有バックアップの世代数。これにより、ファイル復元プロセスの応答性が向上します。既定値は5です。
afs.partial.success.threshold.count	対応するファイル共有のバックアップステータスが「エラーで完了」になるまでの、失敗したファイルバックアップの数。既定値は100です。値0はステータスを無効にします。
afs.instance.afs.cluster.priority	HYCUは内部アルゴリズムを使用して、複数のHYCUインスタンス間で負荷を分散します。ファイルサーバーと同じNutanixクラスターで実行されているHYCUインスタンスを優先し、HYCU Backup Controllerと同じNutanixクラスターで実行されているHYCUインスタンスを優先します。また、各HYCUインスタンスですでに実行されているジョブの数も考慮されます。 この設定の値を上げると、ファイルサーバーと同じ

設定	説明
	Nutanixクラスターで実行されているHYCUインスタンスの優先度が高くなります。
afs.instance.bc.cluster.priority	HYCUは内部アルゴリズムを使用して、複数のHYCUインスタンス間で負荷を分散します。ファイルサーバーと同じNutanixクラスターで実行されているHYCUインスタンスを優先し、HYCU Backup Controllerと同じNutanixクラスターで実行されているHYCUインスタンスを優先します。また、各HYCUインスタンスですでに実行されているジョブの数も考慮されます。 この設定の値を上げると、HYCU Backup Controllerと同じNutanixクラスターで実行されているHYCUインスタンスの優先度が高くなります。

データリハイドレートの設定

以下の設定を使用して、HYCUを構成してデータリハイドレートを実行できます。

設定	説明
target.azure.blob.rehydration.enable	バックアップデータまたはバックアップデータのコピーがAzureアーカイブストレージ層に保存されている場合、HYCUは復元を実行する前にデータリハイドレートを実行するように事前構成されます。リハイドレートタスク中に、データはアーカイブストレージ層から、HYCUがデータを復元できるホットストレージ層に移動します。HYCUは、後でデータをアーカイブストレージ層に戻すことはしません。既定値は`true`です。
target.azure.blob.rehydration.threads	並行してリハイドレートできるBLOBの数。既定値は20です。

災害復旧の設定

以下の設定を使用して、災害復旧の追加シナリオを有効にするか、または自動ターゲット同期を調整できます。

設定	説明
clone.enabled.for.hycu.dr	HYCUは、HYCU Backup Controller(仮想マシン自体またはその仮想ディスク)のクローンを作成しないように事前構成されています。 **注意** 元のHYCU Backup Controller

設定	説明
	がまだアクティブである間は、HYCU Backup Controllerのクローンをアクティブにしないでください。このようなアクティブ化が行われると、データ損失が発生する可能性があります。現在実行中のバックアップはすべて失敗し、そのステータスは「エラー」に設定されます。対応する復元ポイントは、HYCUのクリーニングプロセスによって自動的に削除されます。 `true`に設定すると、HYCU Backup Controllerの複製が有効になり、HYCU Webユーザーインターフェースでそれぞれの復元オプションが使用可能になります。
synchronize.target.catalog.interval.minutes	復旧HYCU Backup Controllerが復旧モードである場合、既定で60分ごとに自動ターゲット同期が実行されます。値を0に設定すると、自動ターゲット同期が無効になります。

ユーザー管理の設定

仮想マシンやファイル共有の所有権を変更する際、以下の設定を使用すると保護されたデータの削除を完全に防ぐことができます。

設定	説明
force.keep.backups.on.owner.change	`true`に設定すると(既定値は`false`)、特定の所有者に保護されているデータは決して削除されません。いずれかのHYCUインターフェースで仮想マシンとファイル共有の所有権を変更する際そのデータを削除するオプションが指定されていても削除されません。

付録B

異なるハイパーバイザーを持つ環境への復元

この付録では、異なるハイパーバイザーに基づく環境に仮想マシンを正常に復元するために考慮または実行する必要がある前提条件、制限事項、考慮事項、および追加の手順について説明します。

VMソース環境	VMターゲット環境	復元オプション	追加情報
Nutanix ESXiまたはvSphere	Nutanix AHV	VMのクローン	“Nutanix ESXiクラスターまたはvSphere環境からの仮想マシンのNutanix AHVクラスターへの復元” 次のページを参照してください。
vSphere	Nutanix ESXi	VMのクローン	“vSphere環境から仮想マシンのNutanix ESXiクラスターへの復元” ページ318を参照してください。
Nutanix AHV	Nutanix ESXi	VMのクローン	Nutanix AHVクラスター上の仮想マシンは、“仮想マシンの複製” ページ91で説明したようにNutanix ESXiクラスターに復元され、追加のアクションは不要です。
Nutanix AHVまたはNutanix ESXi	vSphere	VMのクローン	“Nutanix AHVクラスターまたはNutanix ESXiクラスターからvSphere環境への仮想マシンの復元” ページ318を参照してください。

前提条件

異なるハイパーバイザーを持つ環境に復元する予定のLinux仮想マシンの場合、仮想マシンの`/etc/fstab`システム構成ファイルでは、ファイルシステムのデバイス識別に、デバイス名の代わりにUUID(たとえば、`UUID=8ff089c0-8e71-4320-a8e9-dbab8f18a7e5`) を使用する必要があります。

考慮事項

- 選択した仮想マシンの復元中に、ゲストオペレーティングシステム(仮想マシンで実行されているゲストオペレーティングシステムと、仮想マシンの構成中に指定されたものとの間) の不一致が検出されたか、または新しい仮想マシンの作成中にメモリサイズの不一致が検出されたことを示す警告メッセージを受け取った場合には、適切なゲストオペレーティングシステムまたはメモリを指定して、復元後に仮想マシンの構成を必ず変更してください。こうすることで、復元された仮想マシンの構成を、復元前と同じものにすることができます。この実行方法の詳細については、NutanixまたはVMwareの資料を参照してください。

  仮想マシンの復元方法の詳細については、“仮想マシンの復元” ページ86を参照してください。
- *アタッチされたボリュームグループがある仮想マシンの場合* :復元後にボリュームグループを仮想マシンに再アタッチする必要があります。この実行方法の詳細については、Nutanixおよびゲストオペレーティングシステムの資料を参照してください。

Nutanix ESXiクラスターまたはvSphere環境からの仮想マシンのNutanix AHVクラスターへの復元

前提条件

Nutanix AHVクラスターがHYCUに追加されている。この実行方法の詳細については、“Nutanixクラスターの追加” ページ32を参照してください。

考慮事項

複数のディスクを持つ仮想マシンをvSphere環境からNutanix AHVクラスターに復元する場合のみ。
復元後に、追加のディスクはオフラインになります。必ずそれらをオンラインに戻してください。

推奨事項

Nutanix ESXiクラスターまたはvSphere環境の仮想マシンをNutanix AHVクラスターに復元した後に手動の手順を実行する必要がないようにするには、バックアップ前に次の推奨事項に従う必要があります。

- *Windows仮想マシンの場合* :Nutanix VirtIOパッケージは仮想マシン上にインストールされます。
- *Nutanix ESXiクラスター上のLinux仮想マシンの場合* :NGTは仮想マシン上にインストールされます。
- *vSphere環境におけるLinux仮想マシンの場合* :VirtIOドライバーはゲストOSカーネルに追加されます。

> **VirtIOドライバーの可用性を確認して必要な場合に追加する方法**
>
> インストールされているカーネルでVirtIOドライバーが使用可能であるかどうかを確認するには、ルートユーザーとして、以下のコマンドを実行します。
>
> ```
> grep -i virtio /boot/config-`uname -r`
> ```
>
> 次の出力は、VirtIOドライバーが使用可能であることを確認します。

```
CONFIG_VIRTIO_BLK=m
CONFIG_SCSI_VIRTIO=m
CONFIG_VIRTIO_NET=m
CONFIG_VIRTIO_CONSOLE=m
CONFIG_HW_RANDOM_VIRTIO=m
CONFIG_DRM_VIRTIO_GPU=m
CONFIG_VIRTIO=m
# Virtio drivers
CONFIG_VIRTIO_PCI=m
CONFIG_VIRTIO_PCI_LEGACY=y
CONFIG_VIRTIO_BALLOON=m
CONFIG_VIRTIO_INPUT=m
# CONFIG_VIRTIO_MMIO is not set
```

VirtIOドライバーがカーネルに追加されているかどうかを確認するには、ルートユーザーとして、以下のコマンドを実行します。

```
cp /boot/initramfs-`uname -r`.img /tmp/initramfs-`uname -r`.img.gz
```

```
zcat /tmp/initramfs-`uname -r`.img | cpio -it | grep virtio
```

VirtIOドライバーがカーネルに追加されると、次のような出力が表示されます。

```
97084 blocks
```

出力がブランクの場合、VirtIOドライバーはカーネルに追加されません。VirtIOドライバーをカーネルに追加するには、ルートユーザーとして、以下のコマンドを実行します。

```
dracut --add-drivers "virtio_pci virtio_blk virtio_scsi virtio_net" -f
-v
```

VirtIOドライバーがカーネルに追加されているかどうかを確認するには、ルートユーザーとして、以下のコマンドを実行します。

```
cp /boot/initramfs-`uname -r`.img /tmp/initramfs-`uname -r`.img.gz
```

```
zcat /tmp/initramfs-`uname -r`.img | cpio -it | grep virtio
```

次のような出力が表示されます。

```
usr/lib/modules/`uname -r`/kernel/drivers/scsi/virtio_scsi.ko
usr/lib/modules/`uname -r`/.x86_64/kernel/drivers/block/virtio_blk.ko
usr/lib/modules/`uname -r`/kernel/drivers/char/virtio_console.ko
usr/lib/modules/`uname -r`/kernel/drivers/net/virtio_net.ko
usr/lib/modules/`uname -r`/kernel/drivers/virtio
usr/lib/modules/`uname -r`/kernel/drivers/virtio/virtio.ko
usr/lib/modules/`uname -r`/kernel/drivers/virtio/virtio_pci.ko
usr/lib/modules/`uname -r`/kernel/drivers/virtio/virtio_ring.ko
97084 blocks
```

詳細については、Nutanixの資料を参照してください。

上記の推奨事項に従わなかった場合、仮想マシンは復元後に起動しないため、次の追加手順を実行する必要があります。

1. 復元された仮想マシンがオフになっていることを確認します。
2. 管理者またはrootユーザーとして、SSHを使用してNutanix AHVクラスターにログオンします。
3. 仮想マシンの詳細をリストします。

   ```
   acli vm.get <VMName>
   ```

4. disk_listセクションの現在のバスとインデックスの値をメモします。
5. 既存のディスクを互換バス上の新しいディスクにクローンします。

   ```
   acli vm.disk_create <VMName> bus=<BusType>
   clone_from_vmdisk=vm:<VMName>:<CurrentBus>.<CurrentIndex>
   ```

   この場合、<*VMName*>は復元された仮想マシンの名前であり、<*BusType*>はscsi、ide、またはsataであり、<*CurrentBus*>はdisk_listセクションからのバス値であり、<*CurrentIndex*>はdisk_listセクションからのインデックス値です。

   元の仮想マシンにSATAまたはSCSIディスクがある場合、それらをSATAディスクにクローンします。例：

   ```
   acli vm.disk_create test-vm bus=sata
   clone_from_vmdisk=vm:test-vm:scsi.0
   ```

   元の仮想マシンにIDEディスクがある場合は、それらをIDEディスクにクローンします。例：

   ```
   acli vm.disk_create test-vm bus=ide
   clone_from_vmdisk=vm:test-vm:ide.0
   ```

すべてのディスクに対して前の手順を実行したら、次の手順を実行します。

1. Nutanix Prism Webコンソールにログオンします。
2. メニューバーで、「**ホーム**」をクリックし、「**VM**」を選択します。
3. 「**テーブル**」タブをクリックして、「VMテーブル」ビューを表示します。
4. 仮想マシンのリストから、復元された仮想マシンを選択し、「**更新**」をクリックします。
5. ソースディスクを削除し、ブートディスクを選択して、「**保存**」をクリックします。
6. 「**電源オン**」をクリックして、復元した仮想マシンをオンにします。
7. 最新バージョンのNutanix Guest Toolsソフトウェアバンドルを仮想マシン上にインストールします。
8. *SCSIディスクを搭載していた仮想マシンに推奨します*。コントローラーをクローンしてSCSIコントローラーに戻します。

Nutanixクラスター上で仮想マシンを更新する方法については、Nutanixの資料を参照してください。

vSphere環境から仮想マシンのNutanix ESXiクラスターへの復元

vSphere環境から仮想マシンをNutanix ESXiクラスターに復元した後で仮想マシンが起動しない場合には、追加の手順を実行する必要があります。

> 注 手順を実行するインターフェースとして、vSphere Web ClientまたはvSphere Clientのどちらも使用できます。たとえば、vSphere Web Clientを使用している場合は、そのために必要な実行手順が案内されます。

手順

- 復元された仮想マシン上のコントローラーのタイプが元の仮想マシンのものと同じではない場合、以下を実行します。
  1. vSphere Web Clientにログオンします。
  2. 「**VM**」タブをクリックし、復元された仮想マシンを右クリックし、「**設定の編集**」を選択します。
  3. 「仮想ハードウェア」タブで、元の仮想マシンの設定と一致するように、コントローラー設定を変更します。
- 仮想マシンがUEFIファームウェアを使用している場合、ブートファイルを手動で選択することが必要になる場合があります。この場合は、次のようにします。
  1. vSphere Web Clientにログオンします。
  2. 「EFIブートマネージャー」メニューにアクセスし、以下を実行します。
     a. 「**セットアップの入力**」オプションを選択します。
     b. 「**ブートオプションのメンテナンスメニュー**」を選択して、ブートメンテナンスマネージャーを入力します。
     c. 「**ファイルからブート**」オプションを使用して、ブートファイルを参照します。
     d. 名前にブートパーティションを表すGPT文字列が含まれているデバイスを見つけ、**Enter**を押して開きます。
     e. 以下の場所にあるEFIブートファイルにナビゲートします。
        - Windows :`\EFI\Microsoft\Boot\bootmgrfw.efi`
        - Linux :`/EFI/<OSName>/grubx64.efi`
     f. **Enter**を押して、起動を再開します。

Nutanix AHVクラスターまたはNutanix ESXiクラスターからvSphere環境への仮想マシンの復元

考慮事項

複数のディスクを持つ仮想マシンをNutanix AHVクラスターからvSphere環境に復元する場合のみ。
復元後に、追加のディスクはオフラインになります。必ずそれらをオンラインに戻してください。

手順

1. クローンを作成して、仮想マシンを新しい場所に復元します。説明については、“仮想マシンの複製” ページ91を参照してください。
2. *Nutanix AHVクラスター上にある元の仮想マシンの場合のみ。*適切なゲストオペレーティングシステムを指定して、仮想マシンの構成を変更します。
3. *復元された仮想マシンに複数のディスクがある場合のみ。*復元された仮想マシンのハードディスクの起動順序を確認します。元の仮想マシンのものと異なる場合は、BIOSで起動順序を変更します。

フィードバックの送信

本製品またはその資料に関するご提案やコメントがあれば、以下の宛先までメールにてお送りください。

info@hycu.com

ご意見をお待ちしております。

www.hycu.com

HYCU®