NetBackup™ Self Service 構成ガイド

10.1.1

マニュアルバージョン 1

VERITAS™

NetBackup™ Self Service 構成ガイド

最終更新日: 2022-12-20

法的通知と登録商標

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、NetBackup は、Veritas Technologies LLC または関連会社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。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、Veritas 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア (「サードパーティ製プログラム」) が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このVeritas製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

https://www.veritas.com/about/legal/license-agreements

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されます。Veritas Technologies LLC からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Veritasがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サ

ポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

世界共通 (日本を除く)	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が記載されています。最新のマニュアルは、Veritasの Web サイトで入手できます。

https://sort.veritas.com/documents

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

NB.docs@veritas.com

次の Veritas コミュニティサイトでマニュアルの情報を参照したり、質問したりすることもできます。

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas SORT (Service and Operations Readiness Tools) は、特定の時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供する Web サイトです。製品によって異なりますが、SORT はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。SORT がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目次

第 1 章 Self Service ソリューションの構成 7

Self Service ソリューションの構成について 7
Self Service スケジュールされたバックアップ 8
構成のチェックリスト 8

第 2 章 NetBackup マスターサーバーの構成 10

NetBackup マスターサーバーの構成について 10
Windows NetBackup マスターサーバーとの通信の有効化 10
UNIX NetBackup マスターサーバーとの通信の有効化 11
NetBackup アプライアンスとの通信の有効化 13
REST API を使用した NetBackup マスターサーバーとの通信の有効化 13
NetBackup テンプレートポリシーの作成 15

第 3 章 Self Service の構成 18

Self Service 構成について 18
バックアップサーバーの構成 19
保護の構成 22
ストレージの構成 31
[今すぐバックアップ (Backup Now)]フォームの構成 31
テナントの構成 33
アクセス権 35
コンピュータの登録 36
ホームページの構成 41
ホームページの統合設定 41

第 4 章 Self Service のカスタマイズ 46

言語設定 46
リクエストフォームの作成またはカスタマイズ 46
テーマ 47
通知 48

第 5 章 ユーザー認証方法 49

ユーザー認証方法について 49
フォームベース認証 49
Windows 認証 50
Active Directory のインポート 50
フェデレーションシングルサインオンを使用するための Self Service の設定 51

第 6 章 トラブルシューティング 54

トラブルシューティングについて 54
トラブルシューティング情報の参照場所 56
テナントユーザーの偽装 57
リモート PowerShell から Windows マスターサーバーまでの問題 58
HTTPS 構成の問題 61

付録 A NetBackup ポリシータイプ 63

NetBackup ポリシー形式のリスト 63

付録 B ダッシュボードの信号機のステータスおよび使用状況 66

ダッシュボードの信号機のステータスと使用方法について 66
保護タイプのある資産 66
保護タイプのない資産 67
使用量と料金 67
テナントクォータの適用 68

付録 C NetBackup からのデータの同期 70

NetBackup からのデータの同期について 70

付録 D NetBackup Self Service データキャッシュプロセス 72

NetBackup Self Serviceのデータキャッシュ処理 72
NetBackup データの同期 74
今すぐバックアップ 74
保護 74
保護解除 74

付録 E 統合設定 75
統合設定について 75
NetBackup Adapter 76
NetBackup Adapter 使用方法 78
NetBackup Adapter のアクセス権 79
アクションリクエストタイプ 81
vCloud Director インポート 84
付録 F REST API 86
REST API について 86
付録 G 用語集 87
用語集 87

1

Self Service ソリューションの構成

この章では以下の項目について説明しています。

- Self Service ソリューションの構成について
- Self Service スケジュールされたバックアップ
- 構成のチェックリスト

Self Service ソリューションの構成について

NetBackup Self Service を使用すると、サービスプロバイダは複数の顧客に対し安全かつ分割された方法でセルフサービスのバックアップおよびリストアを提供できるようになります。企業環境では、事業単位およびプロジェクトチームはセルフサービスのバックアップおよびリストアを実行できます。

Self Service リストア機能は有効になっていますが、さらにオンデマンドの今すぐバックアップ機能に対しスケジュールされているセルフサービスのポリシー編集およびサポートを提供することもできます。

注意: NetBackup Self Service に入力される構成データはすべて大文字と小文字が区別されます。NetBackup で保持される関連データと一致する必要があります。

Self Service ソリューションでは、資産とその所有者のインベントリがサポートされます。

インベントリは複数の方法で入力できます。

- ソース非依存 API
- Self Service ポータル
- vCloud Director からのインポート

- NetBackup からのクラウド資産のインポート

Self Service では、多くの NetBackup ポリシータイプがサポートされています。Self Service を使用して、テナントのバックアップのニーズのすべてを管理できます。このオプションでは、テナントは独自のバックアップポリシーを作成できます。または、リストアサービスが手動で保持されるバックアップポリシーに基づいて提供されるように Self Service を構成することもできます。

Windows、UNIX、VMware など、登録された資産およびその保護形式の記録は、Self Service 内に保持されます。

テナントユーザーは、コンピュータ保護ステータスおよび使用状況を一式のダッシュボード機能を使用して管理します。テナントユーザーは、保護およびリストアへの変更を作成できます。

Self Service スケジュールされたバックアップ

保護を構成すると、ユーザーは自分のバックアップスケジュールを管理できるようになります。このオプションでは、NetBackup ポリシー構成からの抽出が提供され、ユーザーが選択できる精選された一連のバックアップスケジュールが示されます。

構成のチェックリスト

表 1-1は、初めて Self Service を構成するための推奨される一連の手順を示します。

表 1-1　構成のチェックリスト

場所	動作
サーバー	NetBackup Self Service ポータルをインストールします (『NetBackupSelf Service10.1.1 インストールガイド』を参照)
	NetBackup Self Service アダプタをインストールします (『NetBackupSelf Service10.1.1 インストールガイド』を参照)
	Windows マスターサーバーに対しリモート PowerShell を構成します
	UNIX マスターサーバーに対し SSH を構成します
ポータル	少なくとも 1 台のバックアップサーバーを作成します
	保護形式を少なくとも 1 つ作成します (必要に応じて)
NetBackup マスターサーバー	テンプレートポリシーを作成します

場所	動作
ポータル	ユーザーインターフェースを使用してテナントを作成します
	ユーザーインターフェース、API、NetBackup Import、または vCloud Director インポートを使用して資産を少なくとも 1 つ登録します
	Self Service の主な操作をそれぞれテストします (有効で、該当する場合)。 ■ 保護リクエストを送信し、コンピュータが保護された後に保護を解除します。 ■ 今すぐバックアップのリクエストを送信します。 ■ ファイルのリストアのリクエストを送信します。 ■ VM のリストアのリクエストを送信します。 ■ クラウド資産のリストアのリクエストを送信します。

2

NetBackup マスターサーバーの構成

この章では以下の項目について説明しています。

- NetBackup マスターサーバーの構成について
- Windows NetBackup マスターサーバーとの通信の有効化
- UNIX NetBackup マスターサーバーとの通信の有効化
- NetBackup アプライアンスとの通信の有効化
- REST API を使用した NetBackup マスターサーバーとの通信の有効化
- NetBackup テンプレートポリシーの作成

NetBackup マスターサーバーの構成について

Self Service では、最新の Service Pack を含む NetBackup 8.0 以上が必要です。

システムとの通信が必要な各 NetBackup マスターサーバーを、バックアップサーバーとして構成する必要があります。バックアップサーバーを管理するには、管理者ユーザーとして Self Service ポータルにログオンしてから、左側のナビゲーションを使用して[バックアップサーバー (Backup Servers)]ページに移動します。

Windows NetBackup マスターサーバーとの通信の有効化

NetBackup Self Service では、Windows NetBackup マスターサーバーとの通信に Windows PowerShell リモーティングが使用されます。Windows PowerShell はマスターサーバーにインストールされている必要があります。Windows PowerShell は通常、デ

フォルトでインストールされています。また、PowerShell リモーティングが有効になっている必要があります。詳細情報が利用可能です。

http://technet.microsoft.com/library/hh847859.aspx

Windows NetBackup マスターサーバーとの通信を有効にするには

1. NetBackup マスターサーバーにログオンします。
2. 管理者として Windows PowerShell ウィンドウを起動します。
3. `Enable-PSRemoting -Force` を実行します。
4. 必要なファイアウォールポートを開きます。

   デフォルトで、PowerShell リモーティングではポート 5985 上の HTTP、またはポート 5986 上の HTTPS が使用されます。

詳細情報が利用可能です。

http://technet.microsoft.com/en-us/magazine/ff700227.aspx

Self Service サーバーからのマスターサーバーとの通信が信頼されているドメインアカウントとの通信でない場合、認証されないことがあります。認証を有効にするには、リモートコンピュータを WinRM のローカルコンピュータの信頼されているホストのリストに追加する必要があります。これを実行するには、次のように入力します。

```
winrm set winrm/config/client '@{TrustedHosts="machine1,machine2"}'
```

必要に応じて、カンマで区切られたリストで追加のコンピュータを追加します。

最初のバックアップサーバーを作成した後の、接続のテストについての詳細を参照できます。

p.19 の「バックアップサーバーの構成」を参照してください。

UNIX NetBackup マスターサーバーとの通信の有効化

NetBackup Self Service では、UNIX NetBackup マスターサーバーとの通信に SSH (Secure Shell) が使用されます。SSH の構成は、このガイドの範囲外となります。ただし、NetBackup Self Service では、マスターサーバー上の SSH サーバーとの通信に資格情報が必要です。

- デフォルトで、SSH ではポート 22 が使用されます。
  別のポートを指定するには、サーバー名を *server_name*:*port_number* に設定します。たとえば、`MyServer:23` です。
- マスターサーバー上の SSH へのログオンに NetBackup Self Service で使用されるユーザーアカウントには、`sudo` 構成が必要です。
  - ユーザーアカウントでは `requiretty` を使用しないでください。

- ユーザーアカウントでは sudo パスワードを要求しないでください。
- sudo を使用する場合、ユーザーアカウントでは /usr/openv/netbackup/bin および /usr/openv/netbackup/bin/admincmd のすべてのコマンドが実行される必要があります。

サポートされているユーザー認証モードは次のとおりです。

- パスワード
  NetBackup Self Service ではログオン時にユーザー名とパスワードが渡されます。
- 公開鍵
  ユーザーの公開鍵は、マスターサーバー上のユーザーに対し authorized_keys に保存されます。ユーザーの秘密鍵は、OpenSSH 形式で NetBackup Self Service ポータルに保存されます。
- キーボードインタラクティブ
  NetBackup Self Service では、ユーザーのパスワードがキーボードインタラクティブ ssh セッションに送信されます。パスワードは、構成可能なパスワードプロンプトに応えて送信されます。デフォルトのパスワードプロンプトは [Password:] です。

公開鍵認証に対し、NetBackup Self Service および NetBackup マスターサーバーを構成するには

1. PuTTYgen などのキージェネレータを使用して、公開鍵と秘密鍵のペアを作成します。
2. 必要なマスターサーバーユーザーとしてマスターサーバーにログオンします
3. 公開鍵をユーザーの authorized_keys ファイルにマスターサーバーのオペレーティングシステム形式で追加します。
4. 秘密鍵をパスフレーズで暗号化された OpenSSH 形式に変換します

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,997295A8E365412F

SIKdyjX4UoDm03kprqfkCGQYc/thmNIlWYztEomjyRaMyEYlh0ZIC9Kx7XnMNnSk
...
MUxIcZW8d8fF3P4s+OLidxG03H6C/AsGLzJtpecjPQA=
-----END RSA PRIVATE KEY-----
```

5. NetBackup Self Service でバックアップサーバーを作成した場合:
   - 認証のための[公開鍵]を選択します。
   - [ユーザーアカウント]に、マスターサーバーに接続するユーザーアカウントを入力します。

- ［OpenSSH 公開鍵 (OpenSSH Private Key)］に暗号化された OpenSSH 形式の秘密鍵を貼り付けます。
- ［パスワード］と［パスワードの確認］にパスフレーズを入力します。

最初のバックアップサーバーを作成した後の、接続のテストについての詳細を参照できます。

p.19 の「バックアップサーバーの構成」を参照してください。

NetBackup アプライアンスとの通信の有効化

アプライアンスへの接続は、UNIX マスターサーバーへの接続と同様に構成されますが、キーの構成は使用できません。前に作成したユーザー名とパスワードを使用して、接続を行います。

アプライアンスでシェルメニューにログオンし、新しいユーザーを作成します。

［メインメニュー (Main_Menu)］>［管理 (Manage)］> [NetBackupCLI] > *［UserName の作成］の順*

詳しくは、『NetBackup Appliance Administrator's Guide』の「Creating NetBackup administrator user accounts (NetBackup 管理者ユーザーアカウントの作成)」を参照してください。

REST API を使用した NetBackup マスターサーバーとの通信の有効化

NetBackup Self Service は、マスターサーバーとの一部の通信に NetBackup REST API を使用できます。NetBackup サーバーはバージョン 8.1.2 以降である必要があります。

基本的な設定

REST API を使用した通信を有効にするには

1. NetBackup Self Service に管理者としてログオンし、［バックアップサーバー (Backup Servers)］ページに移動します。適切なバックアップサーバーを選択します。
2. ［REST API 接続 (REST API Connection)］セクションの詳細を入力します。

   バックグラウンドタスクがバックアップサーバーとの接続性を自動的に調査します。
3. ジョブが完了したら、ステータスアイコンをクリックして接続性の概要画面を開きます。
4. REST API が正常に接続されていることを確認します。

クレデンシャル (Credentials)

デフォルトでは、NetBackup Self Service は CLI へのアクセスに使用するのと同じクレデンシャルを使用して REST API にアクセスします。別のアカウントと RBAC セキュリティを使用する場合、少なくとも保護計画の表示、保護計画の管理、資産の表示、資産の管理、リカバリ/リストア、ジョブの表示が許可されたロールがアカウントに必要です。また、すべての資産とすべての保護計画にアクセスできるオブジェクトグループも必要です。

証明書

NetBackup REST API との通信は、HTTPS を経由します。HTTPS では、クライアントとサーバーの間に信頼関係が存在する必要があります。この場合、クライアントは、NetBackup Self Service Web サーバーまたはタスクエンジンサーバーで、サーバーは、NetBackup マスターサーバーです。信頼関係は、証明書を使用して確立されます。

証明書には、3 つのオプションがあります。

1. マスターサーバーは、信頼できる認証局から発行された証明書を使用します。

   NetBackup Self Service Web サーバーには https 接続の信頼が確立されているため、追加の処理は必要ありません。

2. マスターサーバー証明書は、プライベート認証局から発行されるか、自己署名証明書かのいずれかです。Web サーバーとタスクエンジンサーバーの信頼できる証明書ストアに、認証局の証明書を手動でインストールする必要があります。詳しくは、「「マスターサーバーから NetBackup Self Service Web サーバーまたはタスクエンジンサーバーに認証局の証明書をインストールするには」」を参照してください。

3. 証明書エラーを無視します。

   - NetBackup Self Service を管理者として開き、[バックアップサーバー (Backup Servers)] ページに移動します。
   - バックアップサーバーを選択します。[詳細設定の表示 (Show Advanced Settings)] をクリックします。REST API 接続のセクションで、[証明書エラーを無視する (Ignore Certificate Errors)] を確認して、変更を保存します。
     この選択は、問題の原因の 1 つを排除するため、REST API を最初に設定するときに適しています。ただし、REST API の接続が機能するようになったら、信頼できる証明書のみを使用するようにします。信頼できる証明書が確立されたら、[証明書エラーを無視する (Ignore Certificate Errors)] オプションをオフにします。

信頼できる認証局の証明書のインストール

マスターサーバーから NetBackup Self Service Web サーバーまたはタスクエンジンサーバーに認証局の証明書をインストールするには

1 NetBackup Self Service で次のように行います。

- ［バックアップサーバー (Backup Servers)］ページで、バックアップサーバーを選択します。ステータスアイコンをクリックして、構成の概要画面を開きます。
- ［REST の接続ステータス (REST Connection Status)］セクションで、クリックして、使用するコンピュータにマスターサーバーの証明書をダウンロードします。

2 Windows エクスプローラー上の該当する NetBackup Self Service サーバーで、次を実行します。
   - 証明書を特定し、右クリックして開きます。
   - 証明書を確認して、それが正しいことを確認します。
   - ［証明書のインストール...］をクリックします。
     - 格納場所を［ローカルコンピュータ］と選択します。
     - 証明書ストア［信頼されたルート証明機関］を参照して、［OK］を選択します。
     - ［次へ (Next)］を選択します。
     - ［完了］を選択します。
3 この処理はマスターサーバーの認証局の証明書を、NetBackup Self Service サーバーにインストールします。これで、サーバーは、マスターサーバーの証明書を信頼するようになりました。
4 NetBackup Self Service に戻り、［バックアップサーバー (Backup Servers)］ページでバックアップサーバーを選択します。［証明書エラーを無視する (Ignore Certificate Errors)］オプションにチェックマークが付いていないことを確認します。
5 接続性チェックを実行します。引き続きバックアップサーバーに接続できることを確認します。

NetBackup テンプレートポリシーの作成

NetBackup ポリシーの作成時には、多くのオプションを使用できます。『NetBackup 管理者ガイド Vol. I』には、バックアップポリシーの作成に関するすべての章が含まれています。バックアップポリシーの作成について詳しくは、そのマニュアルを参照してください。

Self Service テンプレートポリシーでは、NetBackup ポリシーオプションの一部のみ使用します。スケジュールされたポリシーの場合、Self Service に影響する項目は表 2-1で指定されている情報のみです。その他すべてのポリシーデータは、その他の NetBackup ポリシーを構成する場合と同様に構成する必要があります。表 2-1には、NetBackup ポリシーの作成画面の関連タブおよび Self Service テンプレートポリシーに必要な対応する情報が詳述されています。NetBackup ポリシーの作成方法について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

表 2-1 スケジュールされたポリシーと[今すぐバックアップ (Backup Now)]ポリシーに必要なポリシー情報

NetBackup ポリシータブ	適用可能なテンプレートポリシー	追加情報
属性	[今すぐバックアップ (Backup Now)]およびスケジュールされたバックアップ	■ ポリシーを無効化する必要があります。 ■ ストレージオプションを指定する場合、すべてのデータを正常にバックアップするために十分な大きさのものを指定してください。
スケジュール	[今すぐバックアップ (Backup Now)]のみ	■ [保持レベル (Retention Levels)]を使用する場合は、[デフォルト (Default)]という名前のスケジュールが必要です。 ■ Self Service では、NetBackup ポリシーで設定される保持値は使用されません。ポリシーの作成時は、Self Service で[デフォルト (Default)]スケジュールの保持レベルが更新されます。 ■ スケジュールを自動的に実行されるように設定しないでください。
クライアント	[今すぐバックアップ (Backup Now)]およびスケジュールされたバックアップ	■ NetBackup Self Service ではクライアント情報が追加されるため、このフィールドは空白にしておきます。

テンプレートポリシーは、ソリューションに対して特に作成する必要があるマスターサーバー上の非アクティブなポリシーです。これらは、保護レベルを使用する場合、または[今すぐバックアップ (Backup Now)]機能を提供する場合のみ必要です。

マスターサーバー上でポリシーの作成を必要とするアクションをユーザーが実行する場合、関連するテンプレートがコピーされ、テナント固有のポリシーが作成されます。ポリシーは、ユーザーのアクションに応じて変更されます。

テンプレートポリシーは、バックアップサーバーとして構成されるすべてのマスターサーバー上で作成する必要があります。これらのポリシーの命名規則では大文字と小文字が区別され、すべて非アクティブにマークされる必要があります。

ポリシータイプ

NetBackup のポリシータイプコード。たとえば、標準の場合は 0、Windows の場合は 13、VMware の場合は 40 となります。

NetBackup ポリシータイプの詳細を参照できます。

p.63 の「NetBackup ポリシー形式のリスト」を参照してください。

任意のタイプ 40 (VMware) テンプレートポリシーの場合:

- vCloud Director テンプレートポリシーの場合、[クライアント (Client)]タブの[仮想マシンの選択 (Virtual Machine Selection)]で [vCloud Director 統合の有効化 (Enable vCloud Director integration)]を指定する必要があります。

[今すぐバックアップ (Backup Now)]テンプレートポリシー

NetBackup Self Service は、[今すぐバックアップ (Backup Now)]ポリシーに対してデフォルトの NetBackup 保持レベルが使用されるように最初から構成されています。これらを NetBackup で変更する、または異なる保持レベルをユーザーに提供する場合、変更は NetBackup Self Service ポータルで行う必要があります。[今すぐバックアップ (Backup Now)]保持レベルについての詳しい情報を参照できます。

p.31 の「[今すぐバックアップ (Backup Now)]フォームの構成」を参照してください。

タイプ 40 (VMware) [今すぐバックアップ (Backup Now)]テンプレートポリシー

[今すぐバックアップ (Backup Now)]テンプレートポリシーの場合、[クライアント]タブの[VM 選択の問い合わせ結果の再利用]の値に関して考慮が必要になります。値をデフォルトの 8 時間のままにしておくと、過去 8 時間以内に作成された仮想マシンで実行される[今すぐバックアップ (Backup Now)]アクションが失敗する可能性があります。値をそれより少ない時間、または 0 時間に設定すると、操作は成功することがあります。ただし、この変更により全体のキャッシュが再構築されるため、接続している VMware システムのパフォーマンスに悪影響を与える可能性があります。この値は、システムの予測される使用状況によっては、デフォルトの 8 時間から変更を必要とする場合があります。

3

Self Service の構成

この章では以下の項目について説明しています。

- Self Service 構成について
- バックアップサーバーの構成
- 保護の構成
- ストレージの構成
- ［今すぐバックアップ (Backup Now)］フォームの構成
- テナントの構成
- アクセス権
- コンピュータの登録
- ホームページの構成

Self Service 構成について

鍵作成および構成タスクの編集は、ホームページのメインパネルから管理できます。

- バックアップサーバー
- 保護（Protection）
- テナント
- 資産

非テナント関連の管理者はこのホームページパネルを表示できます。

バックアップサーバーの構成

バックアップサーバーは、NetBackup マスターサーバーへの接続を示します。少なくとも 1 台のバックアップサーバーが機能する必要があります。

新しいバックアップサーバーは、[バックアップサーバー (Backup Servers)]ページの[バックアップサーバーの追加 (Add Backup Server)]で作成します。ドロップダウンリストを使用すると、さらに、[UNIX または Linux バックアップサーバーの追加 (Add UNIX or Linux Backup Server)]または[Windows バックアップサーバーの追加 (Add Windows Backup Server)]を選択できます。必要な詳細情報の入力を補助する、画面に表示されるヘルプも利用できます。

バックアップサーバーが作成されると、メインの[バックアップサーバー (Backup Servers)]ページに戻り、そこで接続性チェックが開始されます。[接続の確認 (Check Connectivity)]ボタンの動く歯車は、接続性チェックが開始されたことを示します。

チェックに合格すると、以降のアクションは不要になり、バックアップサーバーが使用できるようになります。チェックが不合格になった場合、赤いバツ印をクリックすると不合格の詳細が表示されます。

バックアップサーバーを作成したら、[バックアップサーバー (Backup Servers)]アクションリストから、[詳細の編集 (Edit Details)]、[接続の表示 (View Connectivity)]、[削除 (Delete)]の 3 つのアクションを使用できます。

表 3-1　バックアップサーバーの設定

項目	詳細
名前 (Name)	ユーザーに表示される名前。
サーバー名 (Server Name)	バックアップサーバーのホスト名または完全修飾ドメイン名 (FQDN) (たとえば、`netbackupserver` または `netbackupserver.example.com` など)。 代わりに、ポート番号付きでホスト名を指定できます。 UNIX システムの場合、構文は *`hostname`*`:`*`portnumber`* です。たとえば、`netbackupserver:22` の場合、22 は SSH のデフォルトのポート番号です。 Windows システムの場合、URL の構文 `http://`*`hostname`*`:`*`portnumber`*`/wsman` を使用して、ポート番号を指定します。例: `http://netbackupserver:5985/wsman` または `https://netbackupserver:5986/wsman`。

項目	詳細
バージョン (Version)	NetBackup マスターサーバーのバージョンが含まれる範囲。 8.0 - 8.1.1 8.1.2 8.2 8.3 以降
エージェントレスファイルリストアの有効化 (Enable Agentless File Restore)	バックアップサーバーが VMware エージェントレスファイルリストアをサポートするように構成されていることを示します。バックアップサーバーには、必要なすべての VxUpdate パッケージがインストールされている必要があります。このオプションが有効になっている場合、NetBackup クライアント名が設定されていない VMware 資産で自動的にエージェントレスファイルリストアが提供されます。
オンライン (Online)	バックアップサーバーがオンラインであることを示します。計画的なメンテナンスの実行中に、バックアップサーバーをオフラインにする必要がある場合があります。オフラインのバックアップサーバーでは、システムによる処理は行われず、ユーザーによるバックアップやリストアなどの操作の実行も遮断されます。
認証 (Authentication)	UNIX または Linux の場合: UNIX サーバーへの接続時の認証メカニズム。NetBackup Appliance に接続する場合は、[パスワード (Password)]を選択します。 オプションには、[パスワード (Password)]、[キーボードインタラクティブパスワード (Keyboard Interactive Password)]、または[公開キー (Public Key)]があります。 Windows の場合: CredSSP 認証は、ユーザーのクレデンシャルをローカルコンピュータからリモートコンピュータに委任します。 オプションには、[既定値 (Default)]または[CredSSP]があります。
ユーザーアカウントとパスワード (User Account and Password)	UNIX または Linux の場合: バックアップサーバーに接続するユーザー。ユーザーは、SSH を使用して接続できる必要があります。 Windows の場合: ユーザーは、リモート PowerShell に接続できる必要があります。

項目	詳細
サーバーの日付形式 (Server Date Format)/サーバーの時刻形式 (Server Time Format)	バックアップサーバーで想定される日付と時刻の形式。 ddMMyyyyHHmmss ■ dd: 01 から 31 の日付 ■ MM: 01 から 12 の月 ■ yyyy: 年を表す 4 桁の数 ■ HH: 00 から 23 の時間 ■ mm: 00 から 59 の分 ■ ss: 00 から 59 の秒 形式の例をリストから選択するか、カスタム形式を入力できます。日付と時刻形式の編集について詳しくは、次の記事を参照してください。 https://docs.microsoft.com/ja-jp/dotnet/standard/base-types/custom-date-and-time-format-strings
サーバーの時間帯 (Server Time Zone)	バックアップサーバーのタイムゾーン。
URL	バックアップサーバー API の URL。例: https://netbackupserver:1556
ドメイン名 (Domain Name)	ユーザーのドメイン名。
ドメイン形式 (Domain Type)	ユーザーのドメインタイプ。許可される値は、NIS、NIS+、NT、vx、および unixpwd です。
NetBackup フォルダ (NetBackup Folder)	NetBackup コマンドのバックアップサーバー上の物理パス。このパスは、NetBackup がデフォルトの場所にインストールされていない場合にのみ入力する必要があります。UNIX システムのデフォルト値は、/usr/openv/netbackup です。
NetBackup 一時フォルダ (NetBackup Temporary Folder)	NetBackup Self Service 一時ファイルのバックアップサーバー上の物理パス。このパスは、NetBackup がデフォルトの場所にインストールされていない場合にのみ入力する必要があります。NetBackup Self Service ユーザーは、このフォルダへの読み取りと書き込みのアクセス権を持っている必要があります。また、フォルダは NetBackup の許可リストに存在する必要があります。UNIX システムのデフォルト値は、/usr/openv/netbackup/logs/user_ops です。 Windows システムのデフォルト値は、C:¥Program Files¥Veritas¥NetBackup です。
コマンドタイムアウト (Command timeout)	CLI コマンドがタイムアウトするまでの待機時間 (分単位)。デフォルト値を使用する場合は空白のままにします。

項目	詳細
インプレースディスクリストアの有効化 (Enable In-Place Disk Restore)	NetBackup Self Service で既存の VM に VMDK をリストアできるようにします。バックアップサーバーが、nbrestorevm コマンドを使用するインプレースディスクリストアをサポートしていることを確認してください。
Usage Insights のデータの有効化 (Enable Usage Insights Data)	NetBackup Self Service がバックアップサーバーに Usage Insights のデータを送信できるようにします。
時間単位のチャンクサイズ (Chunk Size In Hours)	サポートから指示される場合にのみ、この値を変更します。NetBackup Self Service で NetBackup からのバックアップイメージが同期される場合、イメージはこのチャンクサイズのバッチで取得されます。デフォルトのチャンクサイズは 10 時間ですが、多数のバックアップアクティビティがあるビジー状態のシステムでは、少なくなる場合があります。チャンクサイズを減らすと、指定された数のイメージを取得するために NetBackup への呼び出しが多くなります。値が空の場合、デフォルトの 10 になります。
時間単位の最大バックアップ期間 (Maximum Backup Duration In Hours)	サポートから指示される場合にのみ、この値を変更します。最大バックアップ期間は、実行時間が長くなるバックアップに NetBackup Self Service が使用することが予想される最長時間を表します。同期エンジンは、この値をバッファ期間として使用して、長期間のバックアップが確実に検出されるようにします。長時間実行されるバックアップが NetBackup Self Service に同期されない場合は、この期間を延長します。値が空の場合、デフォルトの 24 になります。
プールされた接続を使用 (Use Pooled Connections) (Windows のみ)	サポートから指示される場合にのみ、この値を変更します。PowerShell 接続プールを有効にするかどうかを決定します。パフォーマンスを向上させるために、接続プールはデフォルトで有効になっています。
最小プールサイズ (Minimum Pool Size)	サポートから指示される場合にのみ、この値を変更します。PowerShell 接続プールの最小接続数。値が空の場合、デフォルトの 1 になります。
最大プールサイズ (Maximum Pool Size)	サポートから指示される場合にのみ、この値を変更します。PowerShell 接続プールの最大接続数。値が空の場合、デフォルトの 3 になります。

保護の構成

保護タイプでは、ユーザーが資産を保護できるすべての方法を定義します。ユーザーのすべての資産のバックアップ必要条件が似通っている場合、保護タイプは 1 つしか必要ありません。一部の資産に別の保護オプションを使用する場合は、各オプションに保護タイプが必要です。さまざまな保護タイプの例として、SQL サーバー、クラウドボリューム、

または仮想マシンと物理コンピュータの混合が挙げられます。原則として、サポートする各 NetBackup ポリシー形式に保護形式が必要です。

各保護タイプで、複数の管理対象、管理対象外、[今すぐバックアップ (Backup Now)] の保護レベルを定義できます。管理対象と[今すぐバックアップ (Backup Now)]の保護レベルは、資産を保護またはバックアップするときにユーザーに表示されるオプションです。これらのオプションを使用して、各種スケジュール、保持レベル、または NetBackup ポリシーで直接構成できるその他のオプションを指定できます。

管理対象と[今すぐバックアップ (Backup Now)]のそれぞれの保護レベルに、1 つ以上のポリシーを定義します。これらのポリシーは、ユーザーが選択したレベルに応じてバックアップサーバーで作成されるポリシーです。バックアップサーバーでポリシーが作成される方法と名前の指定方法を定義します。非管理の各保護レベルには、1 つ以上のポリシーを定義します。これらは、バックアップサーバーで手動で作成したポリシーです。

さらに、[今すぐバックアップ (Backup Now)]アクションの利用を有効にする保護レベルを設定できます。保護レベル内でコンピュータを保護しているポリシーを使用しているコンピュータに対しては、この[今すぐバックアップ (Backup Now)]アクションを使用します。

保護定義に変更を加えても NetBackup に自動的に適用されることはありません。この保護タイプを使用しているコンピュータには、変更は適用されません。変更を加えた結果、異なるターゲットポリシーセットになると、既存のコンピュータの保護レベルは不明になります。この変更は黒色のチェックマークで示されます。各資産またはコンテナの不明な保護レベルポリシーを削除して、修正した保護レベルを再割り当てできます。

保護タイプの作成

[保護 (Protection)]ページの[保護タイプ (Protection Types)]歯車ボタンで[追加 (Add)]を選択します。

表 3-2　　保護タイプの設定

項目	詳細
名前 (Name)	保護タイプを識別する名前。このオプションはユーザーに表示されます。
コード (Code)	この保護タイプの一意のコード。NetBackup ポリシーでは、ポリシー名にこのコードを使用します。例: *[CustomerCode]-[Code]-*[...]

保護レベルと今すぐバックアップのレベルの作成

選択した保護タイプで、関連する[保護レベルを追加 (Add Protection Level)]オプションをクリックします。[名前 (Name)]、[説明 (Description)]、[色 (Color)]の各プロパティをすべて使用してユーザーのレベルを区別します。他の設定は機能を制御します。

表 3-3　保護レベルと今すぐバックアップのレベルの設定

項目	詳細
名前 (Name)	レベル名 (ユーザー用)。
説明 (Description)	異なるレベルからユーザーが決定するときに役立つ説明。
コード (Code)	当該レベルに関連付けられた NetBackup ポリシーを作成するときに使用するコード。コードは、作成したポリシーの名前に含まれます。コードは保護タイプ内で一意にする必要があります。
色 (Color)	色は、さまざまなコンピュータに割り当てるさまざまなレベルを視覚的に区別するために、主にユーザー画面で使用します。
リクエストタイプコード (Request type code)	システムをカスタマイズする必要がなければデフォルト値 (保護レベルは DBNEWBACK、今すぐバックアップのレベルは DBBACKNOW) のままにしてください。 **メモ:** この設定は、管理対象外の保護レベルには関連せず、画面には表示されません。管理対象と[今すぐバックアップ (Backup Now)]の保護レベルの場合、[詳細設定の表示 (Show Advanced Settings)]を選択すると、このフィールドを表示できます。
表示 (Visible)	ユーザーに表示するレベルを制御します。 **メモ:** この設定は、管理対象外の保護レベルには関連せず、画面には表示されません。

ポリシーの作成

[保護レベル (Protection Level)]または[今すぐバックアップのレベル (Backup Now Level)]の詳細で、[ポリシーの追加 (Add Policy)]をクリックしてそのレベル内にポリシーを作成します。

管理保護レベルには、[スケジュール済み (Scheduled)]、[ファイル選択時にスケジュール済み (Scheduled with File Selection)]、[クラウド保護計画 (Cloud Protection Plan)]、[即時 (Immediate)]、[ファイル選択直後 (Immediate with File Selection)]のオプションが用意されています。[今すぐバックアップ (Backup Now)]の保護レベルには、[即時 (Immediate)]と[ファイル選択直後 (Immediate with File Selection)]のオプションがあります。

ファイル保護ポリシーを使うと、ターゲットコンピュータのファイルやフォルダのリストを保護できます。ファイル保護は、標準 (0) と MS-Windows (13) のポリシータイプにのみ使用

できます。[即時 (Immediate)]のポリシーは、実行中のスケジュール設定されたポリシーに追加するのではなく、新しいポリシーを使用した 1 回限りのバックアップとして実行されます。

[ポリシー (Policy)]で、そのポリシーの[コード (Code)]を設定できます。コードおよび親保護タイプの組み合わせと保護レベルのコードで作成した[ターゲットポリシー名 (Target Policy Name)]も表示できます。

表 3-4　ポリシーの設定

項目	詳細
名前 (Name)	管理にのみ使用します。ユーザーには表示されません。
コード (Code)	コードは、コードを設定するレベル内で一意である必要があります。NetBackup ポリシーでは、ポリシー名にこのコードを使用します。例: *CustomerCode*-*Code*-[...] レベル内に 1 つしかポリシーがない場合、コードは空白のままにできます。
ターゲットポリシー名 (Target Policy Name)	編集できません。このフィールドには、ユーザーが当該レベルを選択したときにバックアップサーバーで作成したターゲットポリシーの名前の例が表示されます。名前は、保護タイプ、レベル (保護レベルまたは[今すぐバックアップ (Backup Now)])、ポリシーコードの 3 つのコードから成ります。 **メモ:** この設定は、管理対象外の保護レベルには関連せず、画面には表示されません。
ポリシー名 (Policy Name)	この設定は、管理対象外の保護レベルにのみ使用されます。ポリシーは、カタログ内のどのバックアップを使用して信号機の状態を計算するのかを決定します。正確なポリシー名を指定するか、* を使用して任意のポリシーのバックアップに一致するようにします。

項目	詳細
テンプレート名 (Template Name)	ターゲットポリシーを作成するためにコピーする、バックアップサーバーに存在するテンプレートポリシーの名前。デフォルトの名前を受け入れるか、既存のテンプレートから選択するか、後で作成するテンプレート名を指定できます。 **メモ:** この設定は、管理対象外の保護レベルには関連せず、画面には表示されません。 詳細情報を参照できます。 p.15 の「NetBackup テンプレートポリシーの作成」を参照してください。
ポリシー形式 (Policy Type)	テンプレートポリシーの NetBackup ポリシー形式を指定する必要があります。 **メモ:** この設定は、管理対象外の保護レベルには関連せず、画面には表示されません。
常に保護対象と表示 (Always Show as Protected)	コンピュータの信号機ステータスの計算を回避する場合に使用します。選択すると、コンピュータは常に[保護対象 (Protected)]と表示されます。
警告 (時間) (Warning (hours))	コンピュータの信号機の状態を計算する場合に使用します。詳細情報を参照できます。 フィールドが空白のままの場合、バックアップのないコンピュータには、注意喚起のためのフラグが付きます。フィールドの値を指定した場合は、指定した時間内に適切なポリシー名を使用したバックアップが実行されないと、注意喚起のためのフラグがコンピュータに付きます。 p.66 の「ダッシュボードの信号機のステータスと使用方法について」を参照してください。
1 つのクライアントのバックアップスケジュール名 (Single Client Backup Schedule Name)	このフィールドに値を入力した場合、この[保護レベル (Protection Level)]でコンピュータが保護されると、保護レベルが[今すぐバックアップ (Backup Now)]オプションとして表示されます。このフィールドは、1 台のコンピュータのバックアップが開始されたときに使うスケジュールの名前を指定します。 **メモ:** このフィールドは、スケジュール設定されたポリシーにのみ適用されます。

項目	詳細
ストレージライフサイクルポリシー名 (Storage Lifecycle Policy Name)	[テンプレート (Template)]ポリシーをコピーするときに使うストレージライフサイクルポリシーの名前。
VM ファイルの復元 (VM File Restore)	仮想マシンのバックアップが、ファイルを復元できるようにするための情報を抽出したかどうかを判断するために、このフィールドを使用します。 このフィールドは、VMware または Hyper-V のポリシーでのみ利用可能です。

項目	詳細
クライアント選択タイプ (Client Selection Type)	このフィールドは、VMware または Hyper-V ポリシーでコンピュータを識別する方法を選択するために使用します。オプションは次のとおりです。 ■ ［クライアントベースの表示名 (Client-Based Display Name)］: クライアントリストと VM 表示名を使用します。 ■ ［クライアントベースのホスト名 (Client-Based Hostname)］: クライアントリストとホスト名、または NetBackup クライアント名を使用します。 ■ ［クエリー表示名 (Query Display Name)］: VMware または Hyper-V インテリジェントポリシーを使用し、VM 表示名を使用します。このオプションはデフォルトです。 ■ ［クエリーホスト名 (Query Hostname)］: VMware インテリジェントポリシーとホスト名、または NetBackup クライアント名を使用します。Hyper-V はこのオプションをサポートしていません。 ■ ［クエリーコンピュータ名 (SCVMM のみ) (Query Computer Name (SCVMM only))］: SCVMM コンピュータ名に、Hyper-V インテリジェントポリシーと NetBackup クライアント名を使用します。 ■ ［クエリー名 (SCVMM のみ) (Query Name (SCVMM only))］: SCVMM 名に、Hyper-V インテリジェントポリシーと VM 表示名を使用します。 vCloud Director インポートを使用した場合は、［クエリー表示名 (Query Display Name)］を使用する必要があります。このオプションにより、vApp と vDC の保護と、VM 表示名を取得するだけのインポートが可能になります。 このフィールドは、VMware または Hyper-V のポリシーでのみ利用可能です。

［今すぐバックアップ (Backup Now)］レベル内で作成したポリシーは、常に［すぐに実行 (Run Immediately)］に設定されます。［今すぐバックアップ (Backup Now)］ポリシーでは、［警告 (時間) (Warning (hours))］オプションは設定できません。管理保護レベルをユーザーが選択できるようにするには、［すぐに実行 (Run Immediately)］以外のポリシーを 1 つ以上含める必要があります。

スケジュールの上書き

コンピュータを保護するポリシーの作成時に、別の保護レベルの変更スケジュール情報が必要になる場合があります。このオプションは、バックアップサーバーで作成するテンプレートポリシーの数を減らすのに役立ちます。スケジュールの上書きにより、さまざまな変更を加えることができます。ポリシーの[スケジュールの上書きの追加 (Add Schedule Override)]を使用して、変更する各スケジュールの上書きを作成します。

表 3-5　スケジュールの上書きの設定

項目	詳細
名前 (Name)	変更するスケジュールの名前。スケジュールは、テンプレートポリシーに存在する必要があります。リストから選択するか、名前を入力できます。
間隔の上書き (Override Frequency)	このオプションを選択した場合、スケジュールを実行する間隔を設定できます。
ストレージライフサイクルポリシー名の上書き (Override Storage Lifecycle Policy Name)	このオプションを選択した場合は、このスケジュールで使用するストレージライフサイクルポリシーの名前を選択または入力します。このオプションは、[保持レベルの上書き (Override Retention Level)]と併用できません。
保持レベルの上書き (Override Retention Level)	このオプションを選択した場合、保持レベルを選択するか、保持レベルに関連付けられている番号を入力できます。このオプションは、[ストレージライフサイクルポリシー名の上書き (Override Storage Lifecycle Policy Name)]と併用できません。
バックアップ用ウィンドウの上書き (Override Backup Window)	このオプションを選択した場合、スケジュールのバックアップ用ウィンドウを設定できます。マウスを使用してグリッドでウィンドウを作成するか、詳細な設定を使用できます。値は、スケジュールに関連付けられているバックアップ用ウィンドウを完全に置き換えます。

レベル内の複数のポリシー

1 つのレベルに複数のポリシーを指定できます。たとえば、データベースとオペレーティングシステムの両方のバックアップを作成するポリシーでデータベースサーバーを保護します。

保護レベルと関連ポリシーを追加したら、[保護 (Protection)]ページの歯車アイコンで[更新 (Refresh)]リンクをクリックします。この処理を行うと、当該データが NetBackup マスターサーバーのポリシーと合致します。歯車アイコンがアニメーションになります。これはチェックがアクティブな状態を示しています。このチェックでは、システムで定義済みの

各バックアップサーバーで保護レベルに対応するテンプレートポリシーを確認します。システムは非管理保護レベルをチェックしないことに注意してください。テンプレートポリシーに問題があると、画面に強調表示されます。強調された行をクリックすると、解決する必要がある問題に関する詳細が表示されます。バックアップサーバーで問題が解決したら、更新して問題が修正されたことを確認できます。テンプレートポリシーの作成について詳しくは、以下を参照してください。

p.15 の「NetBackup テンプレートポリシーの作成」を参照してください。

クラウド保護計画の作成

[保護レベル (Protection Level)]の詳細で[ポリシーの追加 (Add Policy)]をクリックし、[クラウド保護計画 (Cloud Protection Plan)]を選択してそのレベル内に計画を作成します。

資産が保護されている場合、Self Service は[クラウド保護計画 (Cloud Protection Plan)]の詳細を使用して、NetBackup マスターサーバーに適切な保護計画を作成します。作成された保護計画は、保護タイプ、レベル、プランのコードに基づいて名前が付けられ、クラウド保護計画 UI に表示されます。

クラウド保護計画には複数のスケジュールを設定できますが、少なくとも 1 つのスケジュールが常に必要です。

Kubernetes 保護計画の作成

[保護レベル (Protection Level)]の詳細で[ポリシーの追加 (Add Policy)]をクリックし、[Kubernetes 保護計画 (Kubernetes Protection Plan)]を選択してそのレベル内に計画を作成します。

資産が保護されている場合、Self Service は[Kubernetes 保護計画 (Kubernetes Protection Plan)]の詳細を使用して、NetBackup マスターサーバーに適切な保護計画を作成します。作成された保護計画は、保護タイプ、レベル、プランのコードに基づいて名前が付けられ、Kubernetes 保護計画 UI に表示されます。Kubernetes 保護計画には複数のスケジュールを設定できますが、少なくとも 1 つのスケジュールが常に必要です。

Nutanix 保護計画の作成

[保護レベル (Protection Level)]の詳細で[ポリシーの追加 (Add Policy)]をクリックし、[Nutanix 保護計画 (Nutanix Protection Plan)]を選択してそのレベル内に計画を作成します。

資産が保護されている場合、Self Service は[Nutanix 保護計画 (Nutanix Protection Plan)]の詳細を使用して、NetBackup マスターサーバーに適切な保護計画を作成します。作成された保護計画は、保護タイプ、レベル、プランのコードに基づいて名前が付けられ、Nutanix 保護計画 UI に表示されます。Nutanix 保護計画には複数のスケジュールを設定できますが、少なくとも 1 つのスケジュールが常に必要です。

NetBackup Self Service での保護計画の作成はパラメータ化されないことに注意してください。システムは常に現在のリリースの基本計画を作成します。

ストレージの構成

この画面は、NetBackup Self Service の対応するバックアップサーバーと保護計画名からストレージ名を構成するために使用します。

[今すぐバックアップ (Backup Now)]フォームの構成

[今すぐバックアップ (Backup Now)]リクエストにより、事前定義済みのテンプレートから一時ポリシーを作成し、オンデマンドでコンピュータのバックアップを作成できます。次をサポートするリクエストを構成できます。

- ストレージライフサイクルポリシー (SLP) を持つポリシー
- バックアップ保持の設定を許可するスケジュールを持つポリシー (デフォルトの操作)

標準装備されているリクエストフォーム (リクエストタイプ) は、各バージョンのアップグレードで上書きされます。編集する前に、[今すぐバックアップ (Backup Now)]フォームのコピーを作成する必要があります。完了すると、すべての[今すぐバックアップ (Backup Now)]保護レベルを、新しいリクエストフォームのコードを参照するように更新できます。詳細情報を参照できます。

p.46 の「リクエストフォームの作成またはカスタマイズ」を参照してください。

NetBackup Self Service は一連のデフォルトの保持レベルを事前インストールします。それらは次に示すように修正できます。

デフォルトの保持レベルを修正するには

1. [管理 (Admin)]、[リクエストと承認 (Request & Approval)]、[リクエストタイプ (Request Type)]、[今すぐバックアップ (Backup Now) (DBBACKNOW)]の順に移動します。
2. [フォーム (Form)]タブをクリックしてから[バックアップ保持 (Backup Retention)]フィールドをクリックします。
3. ページの下部にある[構成 (Configuration)]タブをクリックします。
4. [項目 (Items)]フィールドに、[今すぐバックアップ (Backup Now)]リクエストフォームに入力可能な保持レベルのリストが表示されます。

ごみ箱アイコンを使用して既存のレベルを削除したり、新しいレベルを追加したりできます。[コード (Code)]は NetBackup 保持数と合致する必要があり、[説明 (Description)]が表示されます。

[今すぐバックアップ (Backup Now)]リクエストで SLP を使用するには、NetBackup Self Service フォームを次のように修正する必要があります。

SLP 用に NetBackup Self Service フォームを修正するには

1. ［管理 (Admin)］、［リクエストと承認 (Request & Approval)］、［リクエストタイプ (Request Type)］、［今すぐバックアップ (Backup Now) (DBBACKNOW)］の順に移動します。
2. ［フォーム (Form)］タブをクリックし、［バックアップ保持 (Backup Retention)］または［ストレージライフサイクルポリシー (Storage Lifecycle Policy)］ラジオボタンフィールドを選択します。このオプションは、`BackupRetentionRadio` のコードです。このフィールドはユーザーに表示されず、デフォルトが［バックアップ保持 (Backup Retention)］であることに注意してください。
3. ［構成 (Configuration)］タブをクリックし、選択した SLP でデフォルトを SLP に変更します。
4. ［リクエストタイプ (Request Type)］を保存します。

次回［今すぐバックアップ (Backup Now)］が開始されたとき、フォームによって SLP を選択するようにメッセージが表示されます。ユーザーは、コンピュータに登録されているバックアップサーバー (NetBackup マスターサーバー) にある、利用可能なすべての SLP から選択できます。

メモ: スクリプトをさらにカスタマイズすることにより、ユーザーの選択肢として表示される SLP のリストを制限することができます。
NSSINSTALLFOLDER¥NetBackupAdapterServices¥PowerShellScripts¥FlexiField¥DB-Get-StorageLifecyclePolicies を参照してください。

［今すぐバックアップ (Backup Now)］リクエストでユーザーが［SLP］または［保持 (Retentions)］のいずれかの使用を選択できるようにするには、ラジオボタンを表示する手順を実行します。

1. ［管理 (Admin)］、［リクエストと承認 (Request & Approval)］、［リクエストタイプ (Request Type)］、［今すぐバックアップ (Backup Now) (DBBACKNOW)］の順に移動します。
2. ［役割 (Roles)］タブを選択します。
3. リクエスタの役割を選択したら、［BackupRetentionRadio ラジオボタン (BackupRetentionRadio-Radio Button)］フィールドで［非表示 (Hide)］チェックボックスのチェックをはずします。
4. ［リクエストタイプ (Request Type)］を保存します。

次回［今すぐバックアップ (Backup Now)］を開始したときに、［SLP］または［保持 (Retentions)］を選択できます。

テナントの構成

テナントは組織単位で、少なくとも 1 つのテナントが存在する必要があります。テナントを作成するには、[テナント (Tenants)]ページの[テナントの追加 (Add Tenant)]ボタンを使用します。テナントの最初の (管理者レベル) ユーザーが同時に作成されます。vCloud Director インポートソースが定義されている場合、テナントのクレデンシャルを設定できます。[OK]をクリックすると、テナントレコード、関連するテナント統合設定、およびユーザーレコードがデータベースに追加されます。

テナントの詳細を編集するには、[管理 (Admin)]>[組織]>[テナント]の順に選択します。テナント作成時に設定されるテナントの [顧客コード]を[詳細]タブで表示できます。テナントに関連付けられているすべてのユーザーを [ユーザー]タブで表示できます。テナントレベルの統合設定は[統合 (Integration)]タブで利用可能です。vCloud Director のクレデンシャルと追加の vCloud Director インポートもここで設定できます。テナント管理者は、ホームページ vCloud Director インフラストラクチャツリービューノードの変更機能を使用して、更新された vCloud Director パスワードを必要に応じて続いて設定できます。テナントレベルのテーマは、[テーマ (Theme)]タブで実行できます。

API を使用してテナントを作成することもできます。テナントおよびそのユーザーの作成を自動化するための開始点として PowerShell スクリプトが提供されています。ここでは Front Office SDK を使用して、パブリック Web サービスを呼び出します。

SDK について詳しくは、ヘルプファイルが参照できます。ヘルプファイルは、NetBackup Self Service ポータルのインストール場所にあります。デフォルトで、ファイルは `C:¥Program Files¥Veritas¥Front Office 9.7¥Sdk¥` に置かれます。Microsoft 開発者は SDK を使用する必要があります。Microsoft 以外の開発者は Web サービスを直接呼び出すことができます。URL は、[管理 (Admin)]、[設定 (Settings)]、[システム構成 (System Configuration)]、[パブリック Web サービスの URL (Public Web Services URL)]、[サーバー (Server)]タブの[パブリック Web サービス (Public Web Service)]セクションにあります。Web サービスは `DirectaApi.svc` です。

注意: ポータルの[管理 (Admin)]セクション ([管理 (Admin)]>[組織 (Organization)]>[テナント (Tenant)]>[追加 (Add)]) でテナントを直接作成しないでください。この画面からテナントを作成すると、必要な Self Service データの一部が作成されません。テナントは、[テナントの追加 (Add Tenant)]フォーム ([テナント (Tenants)]ページ上) から、または API を使用して作成します。

テナントの無効化

テナントを無効化するには:

1. ［管理 (Admin)］、［組織 (Organization)］、［テナント (Tenant)］の順に移動します。
2. テナントを無効化します。

   リストページから、特定のテナント行の右側にある［無効化 (Deactivate)］リンクを使用してテナントを無効化します。または、テナントレコードの［アクティブ (Active)］のチェックボックスのチェックマークをはずして、［詳細 (Details)］タブからテナントを無効化します。

   このアクションによりテナントユーザーがログオンできなくなります。
3. すべてのコンピュータ、バックアップ、保護、および使用状況データが Self Service データベースに保持されます。
4. NetBackup のテナントのすべてのポリシーを削除します。

   ポリシーを特定するには、無効化されたテナントの顧客コードで始まるポリシーを確認します。

ユーザーの追加

追加のユーザーをテナントに追加するには、多くの方法があります。

- ［管理 (Admin)］、［組織 (Organization)］、［テナント (Tenant)］、［ユーザー (Users)］タブの順に移動し、手動でポータルを使用
- Active Directory (［ユーザー (Users)］>［Active Directory のインポート (Import Active Directory)］)。コストセンターコードは、テナントレコードのものと同じである必要があります。
- CSV を使用したベースデータのインポート (［ユーザー (Users)］>［ユーザーのインポート/エクスポート (Import / Export Users)］)。［ユーザーのインポート/エクスポート (Import / Export Users)］をクリックすると、新しいフォームが表示されます。フォームには、ユーザーをインポートするための CSV ファイルを選択するオプションがあります。現在のユーザーを CSV または Unicode テキストファイルにエクスポートするオプションもあります。コストセンターコードは、テナントレコードのものと同じである必要があります。
- API の使用

メモ: ユーザーがテナントに関連付けられると、この関連付けは変更できません。

ユーザーレコードを無効化して、システムにアクセスできないようにすることができます。フォーム認証を使用している場合、多くの基準を使用してパスワードルールを定義できます。これらのルールは、［管理 (Admin)］、［設定 (Settings)］、［システム構成 (System Configuration)］で構成できます。

Administrator アクセスプロファイルを持つテナントユーザーは、独自のユーザーレコードを管理できます。

アクセス権

デフォルトでは、すべてのユーザーはテナントに登録しているすべてのコンピュータで可能な処理すべてを実行できます。使用できる機能は、コンピュータがサポートする機能によって異なります。すべてのユーザーはテナントのデータ使用量を月ごとに表示できます。利用可能な処理は、全体、テナント単位、ユーザー単位の 3 つのレベルで制御できます。

これらのアクセス権の制御は、[NetBackup アダプタのアクセス権 (Adapter Access Rights)]セクションで[管理 (Admin)]、[設定 (Settings)]、[統合設定 (Integration Settings)]の順に選択して設定します。アクセス権には、[今すぐバックアップを許可 (Allow Backup Now)]、[マシンの保護を許可 (Allow Protect Machine)]、[ファイルのリストアを許可 (Allow Restore File)]、[VM のリストアを許可 (Allow Restore Vm)]、[マシンの保護解除を許可 (Allow Unprotect Machine)]、[使用状況レポートを許可 (Allow Usage Report)]、[ファイルリストアの登録を許可 (Allow Register for File Restore)]、[SQL のリストアを許可 (Allow Restore SQL)]、[Oracle のリストアを許可 (Allow Restore Oracle)]、[クラウド資産のリストアを許可 (Allow Restore Cloud Asset)]、[エージェントレスリストアファイルを許可 (Allow Agentless Restore File)]、[代替 VM へのエージェントレスリストアファイルを許可 (Allow Agentless Restore File To Alternate Vm)]、[バックアップの期限切れを許可 (Allow Expire Backups)]、[ディスクのリストアを許可 (Allow Restore Disks)]、[Kubernetes 名前空間のリストアを許可 (Allow Restore Kubernetes Namespace)]があります。

すべてのユーザーの処理を全体的に有効または無効にするには

1. [NetBackup アダプタのアクセス権 (Adapter Access Rights)]セクションで必要なアクセス権をクリックします。
2. [値 (Value)]フィールドで[有効 (Enabled)]または[無効 (Disabled)]を選択します。

   [テナントの上書きを許可 (Allow Tenant Override)]にチェックマークを付けていないことを確認します。

   [ユーザーの上書きを許可 (Allow User Override)]を[(許可しない)]に設定していることを確認します。
3. さまざまなテナントでさまざまな処理を実行できるようにするには、次の操作をします。
   - [NetBackup アダプタのアクセス権 (Adapter Access Rights)]セクションで必要なアクセス権をクリックします。
   - [値 (Value)]フィールドで[有効 (Enabled)]または[無効 (Disabled)]を選択します。この設定は、既存のテナントでも新しいテナントでもデフォルトの設定です。

- ［テナントの上書きを許可 (Allow Tenant Override)］にチェックマークを付けます。
- ［ユーザーの上書きを許可 (Allow User Override)］を［許可しない (None)］に設定していることを確認します。

すべてのテナントにアクセスできる、テナント以外に関連付けられた管理者のみがこの値を変更できます。

各テナントにアクセス権の値を設定するには

1. ［テナント管理 (Tenant Admin)］画面 (［管理 (Admin)］、［組織 (Organization)］、［テナント (Tenant)］、［統合 (Integration)］) で［統合 (Integration)］タブを選択します。
2. ［NetBackup アダプタのアクセス権 (Adapter Access Rights)］セクションで必要なアクセス権をクリックします。
3. ［値 (Value)］フィールドで［有効 (Enabled)］または［無効 (Disabled)］を選択します。

コンピュータの登録

使用するコンピュータは NetBackup Self Service に登録する必要があります。この要件には、NetBackup で使用するための UI および構成データの表示名が含まれます。

コンピュータの登録には、ユーザーインターフェースを使用した方法、API を使用した方法、NetBackup クラウド資産インポートを使用した方法、または vCloud Director インポートで自動的に行う方法の 4 つがあります。単一のテナントにはコンピュータの複数のソースを含めることができます。たとえば、vCloud Director からインポートされた仮想マシンと API を使用してインポートされた物理コンピュータです。

ユーザーインターフェースを使用したコンピュータの登録

コンピュータを登録するには、ホームページの［コンピュータ (Computers)］タブの［コンピュータを登録 (Register Computer)］から行います。データの完了をサポートするためにヘルプテキストを参照できます。入力中または［保存 (Save)］をクリックしたときにフィールドのデータが正しいことが検証されます。

コンピュータ登録を削除するには、［資産 (Assets)］ホームページの［資産 (Assets)］リストに移動し、［アクション (Actions)］ボタンから［登録の削除 (Remove Registration)］リンクを使用します。コンピュータ登録は編集できないため、変更が必要な場合はコンピュータ登録を削除し、再作成することをお勧めします。コンピュータ登録を再作成する場合、同じコンピュータコードを使用してください。

コンピュータ登録プロセスには、NetBackup からの保護データおよびイメージデータの自動更新が含まれます。保護データは、スケジュールまたは一回限りの今すぐバックアップタスクによって保護されている内容を示します。［資産の詳細 (Asset Details)］ページ

で[アクション (Actions)]ボタンから[NetBackup データの更新 (Refresh NetBackup Data)]をクリックすると、コンピュータの保護イメージとバックアップイメージを同期できます。通常、同期に手動介入は不要です。例外は、新しい保護ポリシーからのイメージ、または手動で作成されたイメージをすぐに表示する場合です。

API を使用したコンピュータの登録

API は、コンピュータ詳細の自動インポートまたは一括インポートに使用できます。SDK はクライアントが .NET に書き込まれるようにし、API の推奨される使用方法です。ただし、REST API は Microsoft 環境外で利用可能です。

インストールディレクトリの SDK マニュアルを参照してください。

vCloud Director インポートによる登録

vCloud 階層を vCloud Director から自動的にインポートし、コンピュータを NetBackup Self Service に登録できます。インポートは、個別のクレデンシャルを使用してテナントベースによりテナントで実行されます。

vCloud Director インポートでは、階層がインポートされる vCloud Director インスタンスを定義する必要があります。さらに、それと関連付ける NetBackup Self Service 設定を指定する必要があります。

インポートでは、インポートされる階層と関連付けられる[保護タイプ (Protection Type)]と[バックアップサーバー (Backup Server)]を指定する必要があります。

インポートではオプションで、仮想データセンター (vDC) フィルタリングを使用できます。vDC フィルタリングが有効になっている場合、フィルタの vDC のみがインポートされます。フィルタリングはテナントベースごとに発生し、vDC がインポートされるようにそれぞれをフィルタと設定する必要があります。各 vDC は単一テナントのフィルタでのみ表示される必要があります。

vDC フィルタリングが無効になっている場合、インポートクレデンシャルによって表示されるすべての vDC がインポートされます。

新しい vCloud Director インポートを作成するには、[資産のインポート (Asset Import)]の[vCloud Director]ページで[インポートの追加 (Add Import)]オプションを使用します。画面のプロンプトに従って、対応する[vCloud インポート統合設定 (vCloud Import Integration Setting)]セクションを作成します。

vCloud Director がバージョン 9.5 以降の場合は、vCloud Director システムの管理者のユーザー名とパスワードを指定する必要があります。バージョン 10.1 以前を使用している場合は、vCloud Director が管理する下位の各 vCenter Server のクレデンシャルも追加する必要があります。バージョン 10.2 以降ではクレデンシャルは必要ありません。各 vCenter Server はバージョン 6.5 以降を実行している必要があります。[vCenter クレデンシャルの管理 (Manage vCenter Credential)]、[vCenter クレデンシャルの追加 (Add vCenter Credential)]の順に選択して、各 vCenter を追加します。vCenter は URL を使用して識別されます。この URL は、vCloud Director に登録されている名前と一致する必要があります。

インポートを有効にするには、テナントレベルでログオンクレデンシャルを指定する必要があります。vCloud Director のクレデンシャルは組織に対して定義され、[全般 (General)] の[管理者ビュー (Adinistrator View)]に権限がある必要があります。単一のテナントのみが vCloud Director 組織からコンピュータをインポートできます。

新しいテナントを作成する場合、テナント作成プロセスの一部として[テナントの追加 (Add Tenant)]フォームで単一の vCloud Director システムに対するクレデンシャルの指定がサポートされます。追加のクレデンシャルは、API を使用するか、[テナント (Tenant)]管理の[統合 (Integration)]タブを使用して入力できます。最初のパスワードが設定されると、テナント管理者は vCloud Director へのアクセスに使用される vCloud Director パスワードを更新できます。テナント管理者は、コンピュータリストの root ノードのドロップダウンを使用してパスワードを更新します。

表 3-6 vCloud Director インポートで使用される統合設定

項目	詳細
vCloud Api	この値は、`https://hostname/api/` 形式の vCloud Director API の URL に設定する必要があります。
場所 (Location)	コンピュータが登録される NetBackup バックアップサーバーの名前。
オンライン (Online)	vCloud Director インスタンスがオンラインとみなされるかどうかを示します。Self Service では、オンラインでないインスタンスは使用されません。
SSL 証明書エラーを無視する (Ignore SSL Certificate Errors)	このオプションを使用すると、Self Service で SSL 証明書が有効でない vCloud Director インスタンスに接続できるようになります。
vCloud ユーザー名 (vCloud UserName)	テナントが vCloud Director API への接続に使用するユーザー名。各テナントに独自のクレデンシャルがある必要があります。*userid@vOrg* の形式にする必要があります。テナントレベルでのみ設定する必要があります。
vCloud パスワード (vCloud Password)	テナントの対応する vCloud Director パスワード。テナントレベルでのみ設定する必要があります。
保護タイプコード (Protection Type Code)	インポートされたコンピュータに適用される保護タイプ。
vDC フィルタを使用する (Use vDC Filter)	vDC フィルタリングを有効にするために設定します。

項目	詳細
vDC フィルタ (vDC Filter)	インポート時に vDC に適用されるフィルタ。このフィルタはカンマ区切りのリストで、vDC 名は大文字と小文字が区別されます。テナントレベルでのみ設定します。
表示名 (Display Name)	ユーザーに表示される名前。この名前は、ホームページのデフォルトのビューに表示されます。
メタデータを含める (Include Metadata)	インポート時にメタデータを含めるかどうかを判断します。
vCloud 管理者ユーザー名 (vCloud Admin UserName)	vCloud の管理者ユーザー (`Administrator@System` の形式)。vCloud Director 9.5 以降を使用している場合に必要です。
vCloud 管理者パスワード (vCloud Admin Password)	vCloud の管理者クレデンシャルを持つアカウントのパスワード。vCloud Director 9.5 以降を使用している場合に必要です。

メモ: vCloud Director インポートは、単一のセクションにグループ化される統合設定として Self Service に存在します。単一のセクションにより、個別の vCloud Director インポートがそれぞれ定義されます。それぞれに[追加 (Add)]機能を使用する場合、統合設定がバックグラウンドで作成されます。

これらは[統合の設定 (Integration Settings)]でのみ編集または削除できます。ただし、[統合の設定 (Integration Settings)]で直接値を編集する場合は、検証は実行されないため、注意が必要です。

vCloud Director からインポートされるコンピュータが 2 つのペインのツリービューのテナントユーザーに表示されます。コンピュータが親コンテナ内に一覧表示されます。コンピュータが vCloud からの場合、コンテナは左のペインに表示されます。下位レベルのコンテナをクリックすると、内容が右のペインに表示されます。保護はコンテナレベルまたはコンピュータレベルで適用できます。非 vCloud Director コンピュータのみが登録されている場合、これらのコンピュータは全幅リストに表示されます。

NetBackup インポートによる Kubernetes 資産の登録

Kubernetes 資産を NetBackup から自動的にインポートして Self Service に登録できます。インポートは、フィルタまたは個別のクレデンシャルを使用してテナントごとに実行されます。

資産のインポート元の NetBackup サーバーを定義する必要があります。

さらに、それと関連付ける Self Service 設定を指定する必要があります。

インポートした資産を関連付ける保護タイプとテナントを指定する必要があります。

インポートした資産を識別するには、少なくとも Kubernetes クラスタを指定する必要があります。インポートするためにすべての資産が満たす必要があるその他の一連のフィルタ基準 (1 つ以上の名前空間) も指定できます。セットアップ時に、現在のフィルタ基準の結果をプレビューできます。

NetBackup インポートによる Nutanix 資産の登録

Nutanix 資産を NetBackup から自動的にインポートして Self Service に登録できます。インポートは、テナントごとにテナントで実行されます。インポートでは、フィルタまたは個々のクレデンシャルが使用されます。

資産のインポート元の NetBackup サーバーを定義する必要があります。さらに、それと関連付ける Self Service 設定を指定する必要があります。

インポートした資産を関連付ける保護タイプとテナントを指定する必要があります。

インポートした資産を識別するには、少なくとも Nutanix Prism Central または Nutanix クラスタを指定する必要があります。インポートするためにすべての資産が満たす必要があるその他の一連のフィルタ基準も指定できます。基準には、プロジェクト名や VM 表示名 ([次で始まる (starts with)]、[次で終わる (ends with)]、または[次を含む (contains)]) などが含まれます。セットアップ時に、現在のフィルタ基準の結果をプレビューできます。

Nutanix インポートを保存する際には追加の検証があります。Self Service は、[ストレージの構成 (Configure Storage)] 画面で、選択したマスターサーバーと保護計画がストレージで構成されていることを検証します。NetBackup Self Service から NetBackup プライマリサーバーですぐに保護を作成するためにストレージ情報が必要なため、この検証が追加されました。

インポート中、NetBackup Self Service では同じ表示名の重複資産が許可されないことに注意してください。この動作は、NetBackup Self Service のすべての作業負荷のデフォルトの動作です。

NetBackup インポートによるクラウド資産の登録

クラウド資産を NetBackup から自動的にインポートして Self Service に登録できます。インポートは、個別のクレデンシャルを使用してテナントベースによりテナントで実行されます。

資産のインポート元の NetBackup サーバーを定義する必要があります。さらに、それと関連付ける Self Service 設定を指定する必要があります。

インポートした資産を関連付ける保護タイプとテナントを指定する必要があります。

インポートするクラウド資産のタイプも指定できます。

インポートごとにログオンクレデンシャルを指定する必要があります。これらのクレデンシャルは、指定されたテナントの資産のみにアクセスできる必要があります。

NetBackup インポートによる vCenter 資産の登録

vCenter 資産を NetBackup から自動的にインポートして Self Service に登録できます。インポートは、フィルタまたは個別のクレデンシャルを使用してテナントごとに実行されます。

資産のインポート元の NetBackup サーバーを定義する必要があります。

さらに、それと関連付ける Self Service 設定を指定する必要があります。

インポートした資産を関連付ける保護タイプとテナントを指定する必要があります。

インポートした資産を識別するには、少なくとも vCenter Server を指定する必要があります。インポートするためにすべての資産が満たす必要があるその他の一連のフィルタ基準も指定できます。セットアップ時に、現在のフィルタ基準の結果をプレビューできます。

または、インポートに個々のクレデンシャルを設定し、NetBackup RBAC 構成を使用してインポートする資産を判断することもできます。

ホームページの構成

ホームページにより、ユーザーは資産の現在のステータスを表示し、最低限のマウスクリックだけでアクションを開始できます。

上部のセクションには、信号機形式の状態、合計使用量のタイル、使用傾向のグラフがあります。これらの上部セクションの表示設定は、[統合設定 (Integration Settings)]で構成できます。

ホームページの統合設定

表示される統合設定は、[状態 (Status)]および[使用方法 (Usage)]パネルの表示と内容に影響します。

[管理 (Admin)]、[設定 (Settings)]、[統合設定 (Integration Settings)]または[管理 (Admin)]、[組織 (Organization)]、[テナント (Tenant)]、[統合 (Integration)]の順に選択すると、関連する統合設定が表示されます。

表 3-7 NetBackup Adapter

項目	詳細
契約領域 (TB)	使用領域の表示を拡大し、テナントレベルで管理できます。
使用状況保持期間 (月)	使用状況の傾向グラフやリストに表示しておく月数。
[信号機表示 (Show Traffic Light)]タイル	この設定は、ホームページに信号機を表示するかどうかを決定します。

項目	詳細
［合計使用量の表示 (Show Consumption Total)］タイル	この設定は、ホームページに使用量の合計を表示するかどうかを決定します。
［使用傾向の表示 (Show Consumption Trend)］タイル	この設定は、ホームページに使用傾向のグラフを表示するどうかを決定します。
クォータの適用	この設定により、テナントレベルでの領域使用量の追跡を切り替えます。［契約領域 (TB) (Contracted Space (TB))］で設定した値が各テナントに契約領域として適用されるようにします。 デフォルトでは、このオプションは無効です。クォータの適用を有効にするには、各テナントでこのオプションを有効にする必要があります。

［アクションリクエストタイプ (Action Request Type)］では、次のコンピュータ処理に関連付けられたリクエストタイプを制御します。

表 3-8 アクションリクエストタイプ (Action Request Type) (詳細カスタマイズのみ)

項目	詳細
DB マシンを保護解除	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBREMBACK です。
DB VM のリストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBRESTVM です。
ファイルの DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBRESTFILE です。
DB ファイルリストアを登録する	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBREGDNS です。
SQL の DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBRESTSQL です。
Oracle の DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBRESTORA です。
クラウド資産の DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBRESTCLD です。
ファイルのエージェントレス DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは ALFRORIG です。

項目	詳細
代替 VM へのファイルのエージェントレス DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは ALFRALT です。
ディスクの DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは VMDISKREST です。
名前空間の DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBRESTNASP です。
DB VM のリストアメッセージ	デフォルトの DB VM のリストアメッセージの上書き。
DB リストアファイルメッセージ	デフォルトの DB リストアファイルメッセージの上書き。
Nutanix VM の DB リストア	カスタマイズしたリクエストタイプのリクエストタイプコード。デフォルトは DBRESTNUVM です。このリクエストタイプは、パラメータ化なしで Nutanix VM の基本的な完全リストアをサポートします。
DB 保護解除メッセージ	デフォルトの DB 保護解除メッセージの上書き。
DB ファイルリストア登録メッセージ	デフォルトの DB ファイルリストア登録メッセージの上書き。
今すぐ DB バックアップメッセージ	デフォルトの今すぐ DB バックアップメッセージの上書き。
DB SQL のリストアメッセージ	デフォルトの DB SQL のリストアメッセージの上書き。
DB Oracle のリストアメッセージ	デフォルトの DB Oracle のリストアメッセージの上書き。
DB 保護メッセージ	デフォルトの DB 保護メッセージの上書き。
クラウド資産の DB リストアメッセージ	デフォルトのクラウド資産の DB リストアの上書き。
ファイルのエージェントレス DB リストアメッセージ	デフォルトのファイルのエージェントレス DB リストアメッセージの上書き。
代替 VM へのファイルのエージェントレス DB リストアメッセージ	デフォルトの代替 VM へのファイルのエージェントレス DB リストアメッセージの上書き。
ディスクの DB リストアメッセージ	デフォルトのディスクの DB リストアメッセージの上書き。

NetBackup Adapter のアクセス権は、すべてのユーザー、個々のテナント、または特定のユーザーが資産に対して実行できる処理を制御します。

表 3-9 NetBackup Adapter のアクセス権

項目	詳細
今すぐバックアップを許可 (Allow Backup Now)	[今すぐバックアップ (Backup Now)]オプションを表示するかどうかを決めます。
マシンの保護を許可 (Allow Protect Machine)	[コンピュータを保護 (Protect Computer)]オプションを表示するかどうかを決めます。
ファイルのリストアを許可 (Allow Restore File)	[ファイルのリストア (Restore File)]オプションを表示するかどうかを決めます。このオプションでは[フォルダのリストア (Restore Folder)]オプションも設定できます。
VM のリストアを許可 (Allow Restore Vm)	[VM のリストア (Restore Vm)]オプションを表示するかどうかを決めます。
Kubernetes 名前空間のリストアを許可 (Allow Restore Kubernetes Namespace)	[Kubernetes 名前空間のリストア (Restore Kubernetes Namespace)]オプションを表示するかどうかを決めます。
Nutanix VM のリストアを許可 (Allow Restore Nutanix VM)	[Nutanix VM のリストア (Restore Nutanix VM)]オプションを表示するかどうかを決めます。
マシンの保護解除を許可 (Allow Unprotect Machine)	[コンピュータを保護解除 (Unprotect Computer)]オプションを表示するかどうかを決めます。
使用状況レポートを許可 (Allow Usage Report)	ホームページに使用状況のレポートを表示するかどうかを制御します。
ファイルリストアの登録を許可 (Allow Register for File Restore)	[ファイルリストアを登録する (Register for File Restore)]オプションを表示するかどうかを決めます。
SQL のリストアを許可 (Allow Restore SQL)	バックアップが見つかった場合に[SQL データベースのリストア (Restore SQL Database)]オプションを表示するかどうかを決めます。
Oracle のリストアを許可 (Allow Restore Oracle)	バックアップが見つかった場合に[Oracle バックアップをリストア (Restore Oracle Backups)]オプションを表示するかどうかを決めます。
クラウド資産のリストアを許可 (Allow Restore Cloud Asset)	[クラウド資産のリストア (Restore Cloud Asset)]オプションを表示するかどうかを決めます。

項目	詳細
エージェントレスリストアファイルを許可 (Allow Agentless Restore File)	[ファイルのリストア (Restore File)]オプションを表示するかどうかを決めます。このオプションでは[フォルダのリストア (Restore Folder)]オプションも設定できます。
代替 VM へのエージェントレスリストアファイルを許可 (Allow Agentless Restore File to alternate VM)	[代替 VM へのファイルのリストア (Restore File to Alternate VM)]オプションを表示するかどうかを決めます。このオプションでは[フォルダのリストア (Restore Folder)]オプションも設定できます。
バックアップの期限切れを許可 (Allow Expire Backups)	[バックアップの期限切れ (Expire Backups)]オプションを[資産 (Asset)]の[バックアップ (Backups)]タブで利用できるかどうかを決めます。
ディスクのリストアを許可 (Allow Restore Disks)	[ディスクのリストア (Restore Disks)]オプションを表示するかどうかを決めます。

アクセス権について詳しくは、「テナントの構成」セクションで参照できます。

p.33 の「テナントの構成」を参照してください。

「NetBackup Adapter の使用方法」では、[使用方法 (Usage)]タブ内の機能を制御します。

表 3-10 NetBackup Adapter の使用方法

項目	詳細
料金タイプ (Charging Type)	料金計算の基準 (新しいバックアップ、使用容量、または基準を設定しない)。テナントレベルで管理が可能
転送済みデータの値の使用 (Use Data Transferred Values)	使用量の統計で[転送済みサイズ (Transferred Size)]または[イメージサイズ (Image Size)]のどちらを使用するかを制御します。[転送済みサイズ (Transferred Size)]の値は、アクセラレータを使用する場合などで低くできます。[転送済みサイズ (Transferred Size)]の値は、NetBackup 7.7.1 以降でのみ利用可能です。

4

Self Service のカスタマイズ

この章では以下の項目について説明しています。

- 言語設定
- リクエストフォームの作成またはカスタマイズ
- テーマ
- 通知

言語設定

ポータルでは複数の言語がサポートされていますが、NetBackup Self Service ソリューションデータは現在、いくつかの言語のサブセットでのみ利用可能です。これらの言語には、簡体字中国語、日本語、フランス語が含まれます。この設定には、日付形式を含む、言語および地域の設定が含まれます。

リクエストフォームの作成またはカスタマイズ

リクエストタイプはカスタマイズ可能ですが、通常の操作ではこのカスタマイズは不要です。標準装備になっているすべてのリクエストタイプは実装可能です。

メモ: 標準装備になっているリクエストフォームへの変更が必要な場合、まずそれをコピーしてから、そのコピーを必要に応じて編集できます。

NetBackup Self Service には、完全に事前構成されたリクエストフォーム (リクエストタイプ) が標準装備されています。これらのフォームは、バックアップオプションまたはリストアオプションがホームページダッシュボードから選択されると起動されます。追加のデータまたは統合が必要な場合、デフォルトのリクエストフォームをカスタマイズされたフォームへの関連付けで上書きできます。この上書きは、システム全体のレベルで有効になります。

カスタマイズはアップグレード時に上書きされる可能性があり、すべてのカスタマイズを再適用する必要があります。

標準装備されているリクエストフォームをリストから選択して、コピーする必要があります。フォームにアクセスするには、[管理 (Admin)]、[リクエストおよび承認 (Request and Approval)]、[リクエストタイプ (Request Type)]の順に選択します。次に、追加のリクエストフィールド、承認ステージまたはワークフローを追加すると、[リクエストタイプアクティブ (Request Type Active)]チェックボックスが有効になります。[リクエストタイプ名 (Request Type Name)]が[リクエストリスト (Request List)]での表示に適したテキストに修正されることを確認します。

メモ: 標準装備されているリクエストフィールドまたはワークフロー手順は削除しないでください。この機能は、フルフィルメント手順または承認プロセスの追加方法として利用可能です。

関連する[アクションリクエストタイプ (Action Request Type)]設定を[統合設定 (Integration Settings)]セクションから編集する必要があります。

1. [管理 (Admin)]、[設定 (Settings)]、[統合設定 (Integration Settings)]の順に選択して、設定にアクセスします。
2. 既存の値を新しい[リクエストタイプコード (Request Type Code)]と置き換え、編集します。
3. 次に、標準装備されているリクエストフォームを無効化できます。

メモ: サービスカタログ、標準装備されているリクエストタイプの完全リストは、デフォルト値へのリストアがリクエストされる場合に利用可能です。これらは、インストール場所の `MsBuild¥RequestTypes` フォルダにあります。

メモ: 交換用の[保護 (Protect)]と[今すぐバックアップ (Backup Now)]のフォームを有効にするには、それらを適切な[保護レベル (Protection Level)]にリンクします。このオプションは、管理者としてログオンすると[保護 (Protection)]ページに表示されます。

テーマ

事前に標準装備されている NetBackup Self Service テーマは調整可能です。テーマは管理領域画面で、使用される色、および多くのイメージとスタイルを編集して変更します。多くの要素が編集ページ別に編集可能です。[ページ幅 (Page Width)]は 1024 ピクセルのままにしておく必要があります。また、オンライン CSS エディタを使用して、追加のカスタマイズ編集を行うこともできます。

標準装備されているテーマをシステム幅に調整するには、[管理 (Admin)]、[設定 (Settings)]、[テーマとカスタマイズ (Theme & Customization)]の順に選択するか、個別のテナントの場合は[管理 (Admin)]、[組織 (Organization)]、[テナント (Tenant)]、[テーマ (Theme)]の順に選択します。

通知

ホームページの最上部にニュースティッカースタイルで新しい通知を表示できます。警告タイプまたは情報タイプの通知を表示できます。通知のテーマを変更したり、テナントを基準に通知をフィルタリングすることもできます。通知の公開は開始日と終了日の両方で制御できます。API はこれらの通知をサポートします。

[管理者 (Administrator)]のアクセスプロファイルを設定しているテナントでは、組織の通知を管理できます。

5

ユーザー認証方法

この章では以下の項目について説明しています。

- ユーザー認証方法について
- フォームベース認証
- Windows 認証
- Active Directory のインポート
- フェデレーションシングルサインオンを使用するための Self Service の設定

ユーザー認証方法について

NetBackup Self Service では、次の 3 種類の方法でユーザーを認証できます。

- ユーザー名とパスワードを使用するフォームベース認証。この設定は、Self Service に用意されているデフォルトの設定です。
- Windows 認証 (任意で Active Directory をインポート)。このオプションは、企業で配備する場合にのみ適しています。
- WS-Federation パッシブプロトコルによるフェデレーションシングルサインオン。

フォームベース認証

Self Service ポータルには、ログオンページでユーザー ID とパスワードを入力してアクセスします。この設定は、システムにアクセスするデフォルトの方法です。他の設定は必要ありません。

パスワードのルールは[管理 (Admin)]、[設定 (Settings)]、[システム構成 (System Configuration)]の[パスワードポリシー (Password Policies)]カテゴリの順に選択して定義できます。

Windows 認証

Windows 認証を使用するには、ユーザーのドメイン名と合致するユーザー名を使用してデータベースでユーザーを設定する必要があります。形式は、*DOMAIN_NAME¥username* または *username* にします。形式は、システム設定によって異なります。

[管理 (Admin)]、[設定 (Settings)]、[システム構成 (System Configuration)]で[ドメイン名の削除 (Remove Domain Name)]を設定します。*firstname.lastname* を使用する場合はスイッチをオンにして、*DOMAIN¥firstname.lastname* を使用する場合はスイッチをオフにします。

Windows ユーザーが 1 人でも管理領域にアクセスすると、IIS で匿名認証とフォーム認証の両方が無効になります。Windows 認証を有効にします。IIS のこの設定により、`web.config` ファイルが更新されて Self Service のアドレスが更新に従って変更されます。

IIS で Windows 認証を設定するまでは、用意されている `admin` ユーザー ID を使用しないとシステムにアクセスできません。設定後は、手動ログオンは利用できません。

メモ: Active Directory を使用してユーザーを同期する場合は、初回インポート時に少なくとも 1 人のユーザーを `Supervisor` アクセスプロファイルに関連付けます。関連付けないと、管理領域に不正アクセスされます。

メモ: この操作はシステムの初回実装時の設定にのみ実行します。ログオンプロトコルに後で変更を加える場合には適していません。履歴データに影響を与えるからです。

Active Directory のインポート

Self Service と Active Directory を同期するとメンテナンスが簡単になります。インポートはスケジュール設定したインポートタスクで管理します。このプロセスで処理の時間や頻度を指定できます。ユーザーセットに含まれていないユーザーは Self Service で無効になっているので、スケジュールはすべてのユーザーセットに反映されます。

各プロファイルの異なるソースで複数のインポートプロファイルを作成できます。各プロファイルの Self Service のアクセスプロファイル、コストセンター、ユーザーアカウントの状態を指定する必要があります。ユーザーは 0 個以上のユーザーグループに自動的に割り当てられます。ただし、ユーザーグループがすでに Self Service に存在する必要があります。Self Service のユーザー名は、[氏名 (Full Name)] (デフォルト) または [表示名 (Display Name)]から取得できます。言語は選択できます。選択しない場合はシステムベースの言語を使用します。インポートプロファイルはグループまたは組織単位で指定できます。子を含めるかどうかも指定できます。

インポートプロファイルはリストの最上部から処理されるので、必要条件に合わせて順序を変更できます。複数のプロファイルに同一のユーザーが存在する場合は、処理する最新のプロファイルの［インポートユーザーフィールド (Imported User Fields)］のみが適用されます。すべてのプロファイルのユーザーグループメンバーシップが更新されます。

［Active Directory のインポート (Active Directory Import)］内で指定するユーザーは、ドメインのルートレベルで［内容の一覧表示 (List Contents)］と［すべてのプロパティの読み込み (Read All Properties)］の権限が必要です。これらの権利は、すべての組織単位や組織グループを検索してすべてのユーザーをインポートできるようにするために必要です。

インポートするときにユーザー ID の先頭にドメイン名を追加するかどうかをシステム構成設定で制御できます。［管理 (Admin)］、［設定 (Settings)］、［システム構成 (System Configuration)］の順に選択すると、システム構成設定を参照できます。1 つ目のユーザーアカウントを作成する前に、設定値が適切であることを確認してください。これ以降は、変更を加えると新しいユーザーアカウントが作成されて既存のアカウントは無効になり、履歴要求へのアクセスに影響を与えます。SAM アカウント名を変更すると、新しい Self Service のユーザーアカウントが作成されます。

Active Directory で管理していないレコードにローカルで管理している Self Service ユーザーを作成できます。Active Directory の更新では、これらのユーザーは無視されます。

メモ: Windows 認証を使用する場合は、初回インポート時に少なくとも 1 人のユーザーを `Supervisor` アクセスプロファイルに関連付けます。関連付けないと、管理領域に不正アクセスされます。

メモ: この操作は、システムの初回実装時の設定でのみ実行します。この操作は、ユーザー管理方法に影響を与えるので、後でログオンプロトコルに変更を加える場合は適しません。

フェデレーションシングルサインオンを使用するための Self Service の設定

Self Service では、WS-Federation パッシブプロトコルによるフェデレーションシングルサインオンをサポートします。Microsoft WIF (Windows Identity Foundation) とともに実装し、クレームの転送時に SAML (Security Assertion Markup Language) トークンを使用します。ただし、SAML2 プロトコル (SAML-P) はサポート外です。

Self Service をインストールするときに、最初のログオンで admin アカウントを使用する必要があるフォーム認証で設定します。

ID プロバイダを使用して認証するには:

1. Self Service のデータベースで、ID プロバイダのユーザーに対応するユーザーを作成します。
2. Self Service の `web.config` ファイルを編集してフェデレーションシングルサインオンを有効にします。

Self Service でのユーザーの作成

Self Service でユーザーを識別するには[ユーザー ID (User ID)] を使用します。ID プロバイダでユーザーを識別するには[クレーム (Claims)]を使用します。正常に認証するには、Self Service のユーザーが ID プロバイダのいずれかのクレーム値に一致するユーザー ID を所有している必要があります。

Self Service ユーザーを見つけるときに、Self Service は[名前 (Name)]、[電子メール (Email)]、[Windows アカウント名 (Windows Account Name)]、[UPN]を調べます。通常、[名前 (Name)]と[Windows アカウント名 (Windows Account Name)]では `domain¥username` の形式を使用し、[電子メール (Email)]と[UPN]では `username@domain` の形式を使用します。

ポータルでユーザーを入力することも、Active Directory から直接まとめてインポートしたり `.csv` ファイルを使用してインポートすることもできます。

web.config を編集してフェデレーションシングルサインオンを有効にする

`web.config` ファイルを変更してフェデレーションシングルサインオンを有効にするには:

1. *`install_path`*`¥WebSite` にアクセスします。
2. 管理者としてメモ帳で `web.config` を開きます。
3. `<modules>` セクションを検索して 2 つの `IdentityModel` モジュールをコメント解除します。
4. `<authentication>` セクションを検索してモードを `None` に変更します。
5. `<wsFederation>` 要素の issuer 属性に WS-Federation Web サイトの URL を入力します。
6. `<trustedIssuers>` セクションを検索して WS-Federation サーバーのトークン署名証明書の拇印を入力します。

メモ: ファイルに隠し文字を挿入すると拇印の照合に影響を与える可能性があるので、拇印のカットアンドペーストは使用しないでください。

---

7 自己署名 SSL 証明書を使用するテストシステムでこれらの変更を加える場合は、`<certificateValidation>` 要素をコメント解除します。

8 `web.config` ファイルを保存します。

[フォーム認証 (Forms Authentication)] に切り替える必要がある場合は、`web.config` ファイルを編集して認証モードをフォーム `<authentication mode="Forms">` に設定できます。[フォーム認証 (Forms Authentication)] に切り替えると問題が解決することがあります。

Self Serviceへのログオン

フェデレーションログオン用にシステムを完全に構成していることを確認するには:

1 Internet Explorer を閉じて再び開きます。

2 Self Service の URL を入力します。

3 使用している環境でテスト証明書を使う場合は証明書エラーを 2 回容認します。

4 以前作成したユーザーの資格情報を入力します。ログオンに成功するはずです。

6

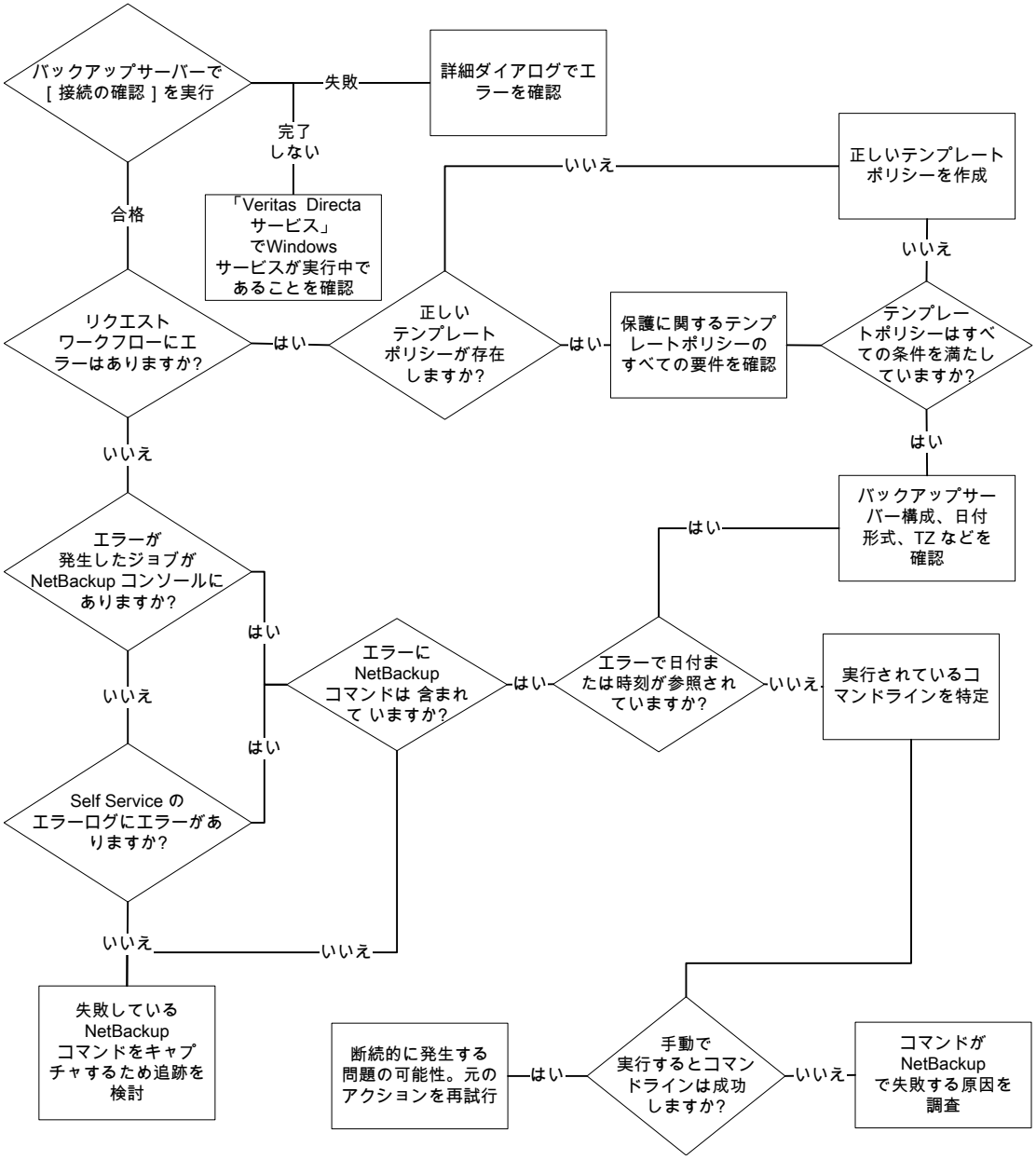
トラブルシューティング

この章では以下の項目について説明しています。

- トラブルシューティングについて
- トラブルシューティング情報の参照場所
- テナントユーザーの偽装
- リモート PowerShell から Windows マスターサーバーまでの問題
- HTTPS 構成の問題

トラブルシューティングについて

問題のトラブルシューティングの最初のステップとして、その問題が Self Service または NetBackup 自体に関するものかどうかを判断します。方向性が明確なエラーまたは障害メッセージがない限り、最善の初回のアクションは、NetBackup コンソールでアクションを手動で実行してみることです。このアクションが失敗した場合、NetBackup に問題があることを示します。NetBackup に問題が認められない場合は、続けて Self Service を診断します。


バックアップサーバーで
[接続の確認] を実行
失敗
詳細ダイアログでエラーを確認
完了しない
「Veritas Directa サービス」でWindows サービスが実行中であることを確認
合格
リクエストワークフローにエラーはありますか?
はい
正しいテンプレートポリシーが存在しますか?
いいえ
正しいテンプレートポリシーを作成
はい
保護に関するテンプレートポリシーのすべての要件を確認
テンプレートポリシーはすべての条件を満たしていますか?
いいえ
はい
バックアップサーバー構成、日付形式、TZ などを確認
はい
エラーで日付または時刻が参照されていますか?
いいえ
実行されているコマンドラインを特定
はい
エラーに NetBackup コマンドは 含まれて いますか?
はい
はい
いいえ
エラーが発生したジョブが NetBackup コンソールにありますか?
はい
Self Service のエラーログにエラーがありますか?
いいえ
いいえ
失敗している NetBackup コマンドをキャプチャするため追跡を検討
手動で実行するとコマンドラインは成功しますか?
はい
断続的に発生する問題の可能性。元のアクションを再試行
いいえ
コマンドが NetBackup で失敗する原因を調査

トラブルシューティング情報の参照場所

接続の確認

[バックアップサーバー (Backup Servers)]ページの[接続の確認 (Check Connectivity)]ボタンを使用して、システム内の各バックアップサーバーへの接続をテストします。エラーには赤いバツ印が表示され、これをクリックするとエラー情報が表示されます。

リクエストワークフロー

Self Service の一部のアクションにより、システム内でリクエストが作成されます。一番上のメニューにある[リクエスト (Requests)]アイコンから、トラブルシューティングの良い情報源となる可能性があるリクエストを見つけることができます。

表 6-1 リクエストの概略情報

マイルストーン名	詳細
フルフィルメントマイルストーン	失敗したステップは赤で、それらに対するエラーが含まれます。
リクエストマイルストーン (監査)	アクションに対する進捗状況を表示し、NetBackup ジョブ ID を提供することもできます。

Self Service エラーログと追加のアクティビティレポート

エラーログなどのさまざまなログファイルは、*install_path*¥Veritas¥NetBackupSelfService にあります。このディレクトリには、統合ログ、監査ログ、電子メールログもあります。エラーにはシステム参照が含まれている可能性があります。これを使用して特定のリクエスト、次にアクションに結び付けることができます。

失敗した NetBackup コマンドを見つける場合、テキスト /bin または ¥bin の検索を実行すると便利です。

アクティビティレポートの追加のソースは、[管理 (Admin)]ホームページの[サポート (Support)]カテゴリにあります。このカテゴリには、統合ログ、監査ログ、電子メールログへのアクセスが含まれます。[履歴 (History)]タブをフィルタし、[エラーで完了 (Completed With Errors)]の状態のタスクを表示できます。エラーのあるタスクは赤で強調表示されます。

NetBackup コマンドラインエラー

Self Service は、マスターサーバーのコマンドラインで NetBackup コマンドを実行することにより動作します。コマンド実行の問題は、Self Service のエラーに含まれます。これらのエラーを見つけることは、非常に有用です。NetBackup コマンドラインのエラーがある場合、コマンドをコピーし、それをマスターサーバーで手動で実行してください。この方法はトラブルシューティングに役立ちます。

NetBackup コンソールでエラーが発生したジョブ

特定されたジョブ ID に対して特に NetBackup アクティビティモニターでエラーを確認します。

テンプレートポリシーのチェック

テンプレートポリシーを正しく機能するように特定の方法で構成する必要があります。ポリシーテンプレートをチェックする際は、[管理 (Admin)]の[保護 (Protection)]ページを参照してください。[保護タイプ (Protection Types)]の歯車ボタンから[テンプレートポリシーのエクスポート (Export Template Policies)]をクリックして、未解決の変更の概略を生成します。

問題のある資産

[資産 (Assets)]ページで、アンバーまたは赤色の歯車によって問題のある資産が強調表示されます。

- 赤色の歯車は、同期か活動失敗のエラーが以前に発生したことを示します。
- アンバーの歯車は、同期か活動失敗のエラーが以前に発生したが、その活動が現在進行中であることを示します。

詳細のポップアップから、最後のエラーとスタックトレースを提供する[詳細 (Details)]タブを選択します。

同期エラー

MSP 管理ユーザーとしてコンピュータ詳細ポップアップに表示できます。

資産に関する正しくない詳細

資産のイメージまたは保護の詳細が正しいと考えられない場合、[アクション (Actions)]ボタンを使用して、資産に対して[NetBackup データの更新 (Refresh NetBackup Data)]を実行します。

追跡

追跡は、より詳細なレベルで問題を分析するように構成できます。この方法は、より高度なトラブルシューティング方法です。この方法はサポートなしで行わないでください。*Services Site*¥Logs および *Panels Site*¥Logs の ReadMe.txt を参照してください。

テナントユーザーの偽装

テナントユーザーを偽装して、テナントユーザーのホームページビューを表示したり、テナントユーザーのためにアクションを実行したりできます。

ホームページから、ログオンしたユーザー名にマウスを置くと、オプション[別のユーザーとして実行 (Act as another user)] が表示されます。このオプションを選択すると、ユーザーリストが表示されます。必要なテナントユーザーを選択すると、ホームページビューが表示されます。

リモート PowerShell から Windows マスターサーバーまでの問題

同時リモート PowerShell 接続制限

NetBackup マスターサーバーでは、リモート接続数が制限されています。サーバーのデフォルトは通常十分です。

使用量が大きなインストールでは、この制限を増やす必要がある場合があります。制限を超えると、次のエラーが発生する可能性があります。

```
NetBackup server name Connecting to remote server NetBackup server
name failed with the following error message : The WS-Management
service cannot process the request. The maximum number of concurrent

shells for this user has been exceeded. Close existing shells or
raise the quota for this user. For more information, see the
about_Remote_Troubleshooting Help topic.
```

制限を増やすには:

1. NetBackup マスターサーバーで、許可される接続数を決定するために表示される次の PowerShell コマンドを実行します。

   ```
   Get-Item WSMan:¥localhost¥Shell¥MaxShellsPerUser
   ```

2. NetBackup マスターサーバーで、許可される接続数を増やすために表示される次の PowerShell コマンドを実行します。

   ```
   Set-Item WSMan:¥localhost¥Shell¥MaxShellsPerUser interger_value
   ```

同時ユーザー操作の制限

この制限に達すると、次のようなエラーが表示されます。

```
RunCommand failed.
"C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd¥bpimagelist"
"-d" "03/02/2015 09:58:11" "-e" "03/02/2015 11:58:11"
"-json_compact"
Run-Process script threw exception:
Starting a command on the remote server failed with the following
error message : The WS- Management service cannot process the
```

```
request. This user is allowed a maximum number of 15 concurrent
operations, which has been exceeded. Close existing operations for
this user, or raise the quota for this user. For more information,
see the about_Remote_Troubleshooting Help topic.
```

Windows 2012 のデフォルトは 1500 です。この制限を増やすには、表示される次のコマンドを NetBackup マスターサーバーで実行します。

```
winrm set winrm/config/Service
@{MaxConcurrentOperationsPerUser="1500"}
```

PowerShell 接続プール

デフォルトで、Windows 場所では PowerShell 接続プールが使用されます。このオプションにより、NetBackup マスターサーバーで PowerShell を呼び出したときのより高いスループットが可能になります。すべての呼び出しでコンピュータでの新しい実行領域の作成および破棄が要求されないため、高いスループットが実現されます。

設定

表 6-2 PowerShell 接続プールに使用されるバックアップサーバーフィールド

名前	詳細
NetBackup 使用プール接続	PowerShell 接続プールを有効にするかどうかを決定します。パフォーマンスを向上させるために、接続プールはデフォルトで有効になっています。この値は、サポートから指示された場合にのみ変更します。
NetBackup 最小プールサイズ (Minimum Pool Size)	PowerShell 接続プールの最小接続数。値が空の場合、デフォルトの 1 になります。この値は、サポートから指示された場合にのみ変更します。
NetBackup 最大プールサイズ (Maximum Pool Size)	PowerShell 接続プールの最大接続数。値が空の場合、デフォルトの 3 になります。この値は、サポートから指示された場合にのみ変更します。

診断

診断追跡では、PowerShell 接続の作成、使用、廃棄に関する多くの情報が取得されます。

次の PowerShell スクリプトを使用して、NetBackup マスターサーバーへの接続に関する情報を検索できます。

```
$machineName = 'netbackup_master_server_machine_name'
$userName = 'user_name_-_same_as_the_location_integration_setting'
```

```
$password = '<password>'

$connectionURI = ('http://{0}:5985/wsman' -f $machineName)

$securePassword = ConvertTo-SecureString $password -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential
($userName, $securePassword)

$connections = Get-WSManInstance -ConnectionURI $connectionURI
-Credential $credential -ResourceURI shell -Enumerate #| where
{ $_.Owner -eq $userName }


if($connections.length -eq 0) { "There are no remote PowerShell
connections" }

$connections | ForEach-Object {
    # To remove the connection, uncomment the line below
    # Remove-WSManInstance -ConnectionURI $connectionURI shell
      @{ShellID=$_.ShellID}

    $_
    "Owner: {0}" -f $_.Owner
    "HostName: {0}" -f (Resolve-DnsName $_.ClientIP | select
    -expand NameHost)
    "-------------------------------------------------------"
}
```

スケジュールされているタスクの監視

Self Service では、スケジュールされているタスクの多くがバックグラウンドで実行されます。これらのスケジュールされているタスクにより外部システム間のデータが同期され、ユーザーインターフェースが可能な限り最新のものに保たれます。これらのタスクのステータスおよびタイミングは、非テナント管理者ユーザーとしてログオンすると[監視 (Monitoring)]ページの左側に表示されます。

特定のタスクの実行に問題がある場合、アクションの歯車は赤です。タスク名をクリックすると、[スケジュールされているタスクの詳細 (Scheduled Task Details)]ウィンドウが表示されます。このウィンドウにはエラーメッセージが表示され、トラブルシューティングプロセスに役立ちます。エラーを解決し、ドロップダウンの [今すぐ実行 (Run Now)]をクリックして、タスクを再試行できます。

[監視 (Monitoring)]ページの[アクティビティ (Activity)]領域に、アクションに対しキューに登録されたタスクが表示されます。このキューが 10 項目を超え、数分間にわたり変わる兆候がない場合、Self Service のメインタスクエンジンに問題がある可能性があります。

Windows サービスが実行中であることを確認し、*install_path*¥Veritas¥NetBackupSelfService にあるエラーログを確認します。[監視 (Monitoring)]ページから、使用率データの再構築を開始できます。この処理により、今月のデータと以前の月のデータの両方が更新されます。

表 6-3 バックグラウンドタスクと説明

バックグラウンドタスク	説明
System Sync	前回実行以来のすべてのバックアップサーバーからバックアップイメージをインポートします。古いバックアップイメージの有効期限を期限切れにして使用量を計算します。このタスクはスケジュールで 1 日に一度実行されます。
System Update	バックアップイメージの同期やアクティブなリクエストの更新など、システム更新を実行します。このタスクはスケジュールで 1 分に一度実行されます。
Asset Import	構成されているインポートに従って、NetBackup Import または vCloud Director からのコンピュータを同期します。このタスクはスケジュールで 1 日に一度実行されますが、手動で開始できます。

HTTPS 構成の問題

NetBackup Self Service 10.0 以降、Self Service のデフォルトの構成は HTTPS です。この変更は、セキュリティ上の理由で Veritas により行われました。

HTTPS 構成に関する問題のトラブルシューティングに役立つ手順を次に示します。

HTTPS が正しく構成されていることを確認するには:

1. インストーラが SSL 証明書を作成したことを確認します。[スタート]メニューで[インターネット インフォメーション サービス]を検索します。バインドと対応する SSL 証明書を確認できます。
2. ポート 443 のバインドが作成され、証明書がそのポートに割り当てられていることを確認します。[スタート]メニューで[インターネット インフォメーション サービス]を検索します。バインドと対応する SSL 証明書を確認できます。
3. 統合設定を検証します。[管理 (Admin)]の[統合設定 (Integration Settings)]で、すべての URL が HTTPS であることを確認します。
4. [管理 (Admin)]の[統合設定 (Integration Settings)]で、パネル URL とサービス URL に同じホスト名が使用されていることを確認します。

例:

```
https://example.com/NetbackupSelfServiceNetBackupPanels
https://example.com/NetBackupSelfServiceNetBackupServices
```

A

NetBackup ポリシータイプ

この付録では以下の項目について説明しています。

- NetBackup ポリシー形式のリスト

NetBackup ポリシー形式のリスト

表 A-1 に、NetBackup で利用可能なポリシー形式と、それらに関連付けられている ID のリストを示します。これらをポリシー形式の統合設定の作成時に使用する必要があります。

表 A-1 ポリシー形式および関連付けられている ID

ID	名前	NetBackup Self Service	バックアップ対象
0	Standard	保護; ファイルのリストア	ポリシーテンプレートで定義。ポリシーのすべてのクライアントに適用。
4	Oracle	保護 (クライアントベースのみ); データベースのリストア	クライアントに存在するスクリプトによって定義。
6	Informix-On-BAR	サポートされない	
7	Sybase	保護	クライアントに存在するスクリプトによって定義。
8	MS-SharePoint	保護	ポリシーテンプレートで定義。ポリシーのすべてのクライアントに適用。
10	NetWare	サポートされない	
11	DataTools-SQL-BackTrack	サポートされない	
12	Auspex-FastBackup	サポートされない	

ID	名前	NetBackup Self Service	バックアップ対象
13	MS-Windows	保護; ファイルのリストア	ポリシーテンプレートで定義。すべてのクライアントに適用。
14	OS/2	サポートされない	
15	MS-SQL-Server	保護 (クライアントベースのみ); データベースのリストア	クライアントに存在するスクリプトによって定義。
16	MS-Exchange-Server	保護	ポリシーテンプレートで定義。ポリシーのすべてのクライアントに適用。
17	SAP	保護	クライアントに存在するスクリプトによって定義。
18	DB2	保護	クライアントに存在するスクリプトによって定義。
19	NDMP	保護	ポリシーテンプレートで定義。ポリシーのすべてのクライアントに適用。
20	FlashBackup	保護	ポリシーテンプレートで定義。ポリシーのすべてのクライアントに適用。
21	Split-Mirror	サポートされない	
22	AFS	サポートされない	
24	DataStore	サポートされない	
25	Lotus-Notes	サポートされない	
27	OpenVMS	サポートされない	
29	FlashBackup-Windows	サポートされない	
31	BE-MS-SQL-Server	サポートされない	
32	BE-MS-Exchange-Server	サポートされない	
34	Disk Staging	サポートされない	
35	NBU-Catalog	サポートされない	
37	CMS_DB	サポートされない	
38	PureDisk Export	サポートされない	
39	Enterprise Vault	サポートされない	

ID	名前	NetBackup Self Service	バックアップ対象
40	VMware	保護 (インテリジェントポリシーまたはクライアントベース); VM のリストア; ファイルのリストア	
41	Hyper-V	保護 (インテリジェントポリシーまたはクライアントベース); VM のリストア; ファイルのリストア	
42	NBU-Search	サポートされない	
47	Nutanix AHV	保護; Nutanix VM のリストア	Nutanix VM のリストア
50	Kubernetes	保護; 名前空間と永続ボリュームのリストア	名前空間と永続ボリュームのリストア

現時点では、コンピュータをスナップショット対応ポリシーで保護できません。この問題は既知の問題です。

B

ダッシュボードの信号機のステータスおよび使用状況

この付録では以下の項目について説明しています。

- ダッシュボードの信号機のステータスと使用方法について
- 保護タイプのある資産
- 保護タイプのない資産
- 使用量と料金
- テナントクォータの適用

ダッシュボードの信号機のステータスと使用方法について

ダッシュボードのステータスを示すセクションには、既定の保護状態 (赤色、アンバー、緑色) のコンピュータ数が表示されます。この色の算出は、保護形式を設定しているコンピュータによって異なります。

使用容量は、月別の合計量として表示されます。

テナントユーザーには、テナントの合計が表示されます。サービスプロバイダには、全資産を反映する合計が表示されます。

保護タイプのある資産

ユーザーが保護タイプに設定可能な管理対象の保護レベルを選択すると、1 つ以上の NetBackup ポリシーにコンピュータが追加されます。Self Service で各ポリシーを認識するしきい値 (時間単位) が保持されます。資産を追加した既知のポリシーすべてのしき

い値を評価して、赤色、アンバー、緑色のどの状態であるかを判断します。管理対象外の保護レベルを含む保護タイプのある資産は、赤色または緑色の信号機で評価されます。信号機の色は、管理対象外の保護レベルのポリシー名に一致するバックアップの存在に依存します。

表 B-1　保護タイプを設定したコンピュータ

色	コンピュータの状態
緑色	保護レベルは適用されています。すべてのポリシーはしきい値内のバックアップです。または、ポリシーが［常に保護対象と表示 (Always show as protected)］に設定されています。
アンバー	コンピュータに保護レベルは適用されていません。
赤	保護レベルは適用されていますが、1 つ以上のポリシーにバックアップが存在しないか、最新のバックアップがしきい値外です。

メモ: NetBackup ポリシーに資産を指定していても保護レベルがわからない場合は、色の状態を判断するときにポリシーは考慮されません。

［今すぐバックアップ (Backup Now)］プロセスでのみ保護されている資産は数えられず、保護済みであるとは表示されません。

保護タイプのない資産

資産に保護タイプを設定していない場合、ステータスは常にアンバーで表示されます。

使用量と料金

［使用量 (Usage)］セクションは、使用容量の合計と月別グラフの 2 つの部分に分かれています。

使用容量は、テナントに属する有効期限内のすべてのイメージから計算されます。使用容量は、GB 単位の絶対値またはテナントの領域を減算した容量に関する絶対値として示されます。減算した領域に関する使用容量を表示すると、合計量に対する割合 (%) と絶対量の両方の値が示されます。使用容量の計算は、［転送済みデータの値の使用 (Use Data Transferred Values)］の統合設定に依存します。

料金設定

料金データは、テナントごと、保護レベルごと、またはその両方で設定できます。

［使用量 (Usage)］でバックアップの価格を計算する場合、次のルールが適用されます。

1. テナントに請求金額があり、このバックアップの保護レベルにも請求金額がある場合、その請求金額が使用される。それ以外の場合:
2. テナントにデフォルトの請求金額がある場合、このデフォルトの金額が使用される。それ以外の場合:
3. バックアップに対し、システム全体の保護レベルの請求金額がある場合、それが使用される。それ以外の場合:
4. デフォルトのシステム請求金額が使用される。

デフォルトでは、NetBackup Self Service には単一のシステム全体の請求金額として 0 米国ドルが設定されています。

テナントが保護レベルの請求金額を要求する場合は、テナント全体のコストを提供する必要があります。

料金を追加または編集するには、サービスプロバイダまたは管理者アカウントでログインし、［請求金額 (Charge Rates)］タブをクリックする必要があります。［追加 (Add)］または［編集 (Edit)］をクリックすると、システムまたはテナント全体の請求金額を設定したり、個別の保護レベルを適切な料金で上書きできます。

メモ: NetBackup Self Service 内にコンピュータのバックアップが作成されている場合、そのコンピュータに関連付けられた使用量レコードがあります。

メモ: NetBackup Self Service を認識する NetBackup ポリシーのバックアップのみが使用量に加算されます。

メモ: ［テナントの使用量 (Tenant Usage)］のデータを表示したときに報告される［CostPerGb］の図は、テナントの値を示します。システムで保護レベルの上書きを使用するように設定した場合、この［CostPerGb］は正しくありません。ただし、実際のコストは、保護レベルのコストを使用して計算されます。テナントの使用量の詳細には、そのテナントの保護レベルのデータを使用する必要があります。

テナントクォータの適用

テナントクォータの適用機能は、テナントがそれぞれの契約領域使用量の範囲内で準拠して動作するようにします。この機能により、プロバイダはテナントごとに制限を適用できます。テナントごとにこの機能を有効または無効にして、監視対象を制御できます。デフォルトでは、このオプションはすべてのテナントで無効になっています。監視するテナントごとに、この機能を有効にする必要があります。

この機能を有効にすると、Self Service はテナントアカウントからのバックアップの合計サイズを追跡します。現在のシステム同期タスクは、新しいスケジュール設定済みの計算のロックタスクと連携して使用量を追跡します。計算のロックタスクは、テナントアカウントのロックを適用または解除する前に、プライマリサーバーからのバックアップサイズを更新します。

クォータの適用を有効または無効にするには

1 クォータの適用を有効にするテナントの［NetBackup アダプタ (NetBackup Adapter)］設定セクションに移動します。

2 ［クォータの適用 (Quota Enforcement)］設定セクションを見つけます。

3 このオプションを使用して、必要に応じてクォータの適用を有効または無効にします。

システム管理者は、現在ロックアウトされているユーザーを確認できる新しいビューを利用できます。このビューから、契約領域の量を増やした後、ユーザーのロックを解除できます。

メモ: テナントが契約領域を超えてロックアウトされると、再び準拠するまで、バックアップを作成したり新しい資産を保護したりできません。ロックがリセットされるまで、ユーザーがバックアップまたは資産保護を試みると、詳細なメッセージが表示されます。

テナントのロックを解除するには:

1 左側のメニューから［テナントロックアウト (Tenant lockout)］画面を選択します。

2 ［ロックアウト (Locked Out)］オプションの選択を解除します。

3 アカウントのロックが解除されると、ユーザーは通常のバックアップと資産保護のアクティビティを再開できます。

メモ: ユーザーがロックアウトされた後に［クォータの適用 (Quota Enforcement)］オプションを無効にしても、テナントロックアウトのページからユーザーは削除されません。ユーザーはまだ使用量を超えた状態で、準拠していない可能性があります。

ユーザーのロックを正しく解除するには、［テナントロックアウト (Tenant lockout)］画面から行います。次に示すように、テナントアカウントを準拠させます。

- そのページから契約領域の量を増やし、ロックを解除します。
- 契約した領域使用量よりも少なくなるように、ユーザーにバックアップの削除を依頼します。
- その後、ユーザーのロックを解除するテナントロックアウト計算ジョブを実行します。

C

NetBackup からのデータの同期

この付録では以下の項目について説明しています。

- NetBackup からのデータの同期について

NetBackup からのデータの同期について

データを NetBackup から Self Service に同期する場合、2 つの異なるプロセスが必要です。プロセスを以下に示します。

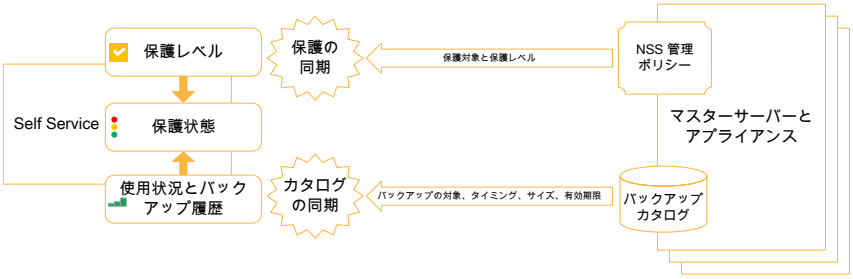


表 C-1　同期プロセスと関連詳細

同期プロセス	詳細 (Details)
同期保護	■ 保護レベルが構成されている場合にのみ同期。たとえば、ポリシーを管理する Self Service です。 ■ NetBackup 上のポリシーでクライアントコンピュータを検索します。 ■ コンピュータまたはコンテナに対し保護レベルを表示します (色が付いたチェックマークのアイコン)。 ■ Self Service では、保護要求の追加および削除により、ローカルキャッシュが最新の状態に保たれます。 ■ ［管理］パネルで手動で起動可能です。
同期カタログ	■ バックアップカタログを同期し、すべてのアクティブなイメージの詳細を Self Service に転送します。 ■ 構成可能なバッチサイズで実行される初期インストール後完全同期。 ■ 通常のタスクでは、日次増分同期によって Self Service でレコードが最新の状態に保たれます。 ■ イメージレコードは、Self Service インベントリのコンピュータと一致します。 ■ Self Service では、概略のダッシュボードに対し夜間ベースでコンピュータおよびテナントごとにイメージサイズデータがロールアップされます。 ■ 個別のコンピュータのイメージは、今すぐバックアップリクエスト完了時、または管理者が管理パネルで手動で初期化するときに再同期されます。

D

NetBackup Self Service データキャッシュプロセス

この付録では以下の項目について説明しています。

- NetBackup Self Serviceのデータキャッシュ処理
- NetBackup データの同期
- 今すぐバックアップ
- 保護
- 保護解除

NetBackup Self Serviceのデータキャッシュ処理

NetBackup アダプタは、資産、保護、バックアップイメージに関するデータをキャッシュするため、パフォーマンスが向上します。

スケジュール設定したタスクを定期的に実行してデータを最新の状態に保ちます。スケジュール設定するタスクを次に示します。

- システムの同期 (System Sync)
  - 前回の実行以降に作成されたバックアップイメージをすべてのバックアップサーバーからインポートする
  - 古いバックアップイメージを期限切れにする
  - 使用量を計算する
  - 信号機の状態を計算する
  - デフォルトで毎日午前 12 時 15 分 (UTC) に実行する
- システム更新 (System Update)

このタスクでは、NetBackup データの同期するようにフラグを付けたコンピュータを処理します。保護レベルとバックアップイメージをインポートして、信号機の状態を再計算します。デフォルトでは、毎分実行します。

- 資産のインポート (Asset Import)
  構成されているインポートに従って、vCloud Director からのコンピュータおよび NetBackup からのクラウド資産を同期します。このタスクは、デフォルトで 1 日 1 回午前 0 時 30 分 (UTC) に実行されますが、手動で開始できます。
- 計算のロックタスク
  このタスクは、クォータの適用向けにスケジュール設定されたタスクです。バックアップイメージを更新し、その時点での最新の使用量を計算します。合計に基づいて、ロックが適用または解除されます。
  このタスクは、オンデマンドで手動で実行できます。

システムの同期

- すべてのオンラインのバックアップサーバーから過去 1 日間のイメージをインポートします。前回のシステム同期時に開始したものの完了しなかったバックアップを取得するために、24 時間分重複してインポートします。
- 期限切れのイメージにフラグを付けます。
- 前回のバックアップを更新して信号機の状態を計算します。

メモ: 新しいバックアップサーバーを追加すると、システムで処理が個別にトリガされません。バックアップイメージの取得やポリシーのインポートのような新しい同期または進行中の同期にこの新しいバックアップサーバーの追加が導入されました。古いイメージは手動でしかインポートできません。[NetBackup データの更新 (Refresh NetBackup Data)] をクリックするか、または API を呼び出して古いイメージをインポートします。バックアップを設定しているすべてのコンピュータでこの処理が必要です。

統合設定

一覧表示されている統合設定は次のシステム同期に関係があります。

- 使用状況の保持期間 (月単位) (NetBackup アダプタ統合セクション)
  グラフに使用状況データと期限切れのバックアップイメージを保持する期間と月数が表示されます。この期間が終了すると、使用状況データと期限切れのイメージはシステムの同期で削除されます。

クォータの適用が有効な場合は、[統合設定 (Integration Settings)] で契約領域の量を設定する必要があります。

NetBackup データの同期

資産をインポートするときに、[NetBackup データの更新 (Refresh NetBackup Data)] をクリックするか、API で `SyncNetBackupData` を呼び出すと、資産に同期のフラグが付きます。この操作により、同期が可能であると資産がマーク付けされるので、システム更新でこの資産が選択されます。この処理は保護とイメージをインポートし、信号機の状態を再計算します。

タスクでは、5 分間に 100 台の資産をまとめて処理するか (デフォルト)、インポートが必要な資産が存在しなくなるまで処理します。一番先に追加した資産を最初に処理します。最初はすべての資産が同じ優先度ですが、[今すぐバックアップ (Backup Now)] を実行すると、これを実行した資産は高優先度にマーク付けされます。

同期に失敗すると、同期は一定期間ロックされます。ロックされても、エラーがない他の資産は処理できます。

統合設定

一覧表示される統合設定は次の NetBackup データの同期に関係があります。

- イメージのインポートのバッチ処理 (分単位) (NetBackup アダプタ統合セクション)
  同期のマークが付いたコンピュータがある場合はシステム更新で一定期間データを取得します。デフォルトでは 5 分に設定されています。
- イメージのインポートのロック待機 (分単位) (NetBackup アダプタ統合セクション)
  この値は、イメージの取得に失敗した場合にコンピュータのイメージの同期をロックする期間を定義します。デフォルトでは 60 分に設定されています。

今すぐバックアップ

[今すぐバックアップ (Backup Now)] リクエストが完了すると、コンピュータに高優先度の同期であることを示すフラグが付くので、コンピュータは可能な限り早く新しいイメージを同期します。

保護

[保護 (Protect)] リクエストが完了すると、データベースに保護レベルを追加し、信号機の状態を更新するタスクがキューに登録されます。

保護解除

[保護解除 (Unprotect)] リクエストが完了すると、データベースから保護レベルを削除し、信号機の状態を更新するタスクがキューに登録されます。

E

統合設定

この付録では以下の項目について説明しています。

- 統合設定について
- NetBackup Adapter
- NetBackup Adapter 使用方法
- NetBackup Adapter のアクセス権
- アクションリクエストタイプ
- vCloud Director インポート

統合設定について

統合設定は、値を含む名前付き設定のフレキシブルなストアです。これらは、NetBackup Self Service と NetBackup の間の統合を構成するために使用されます。個別の設定はセクション内でグループ化され、[管理 (Admin)]、[設定]、[統合設定]の順にアクセスします。このセクションには、NetBackup Self Service ソリューションに関連する統合設定の完全リストが含まれます。個別のセクションまたは設定は、マニュアル全体の該当する機能領域で参照されます。

一部の設定では[テナントの上書きを許可 (Allow Tenant Override)]が[はい]に設定されています。これらの構成は通常テナントベースごとに構成する必要があり、上位レベルの統合設定では正常に完了されません。代わりに、特定のテナントに関する詳細下で構成されます。NetBackup Adapter のアクセス権設定にもユーザー上書きのオプションがあります。アクセス権に関する詳細を参照できます。

p.35 の「アクセス権」を参照してください。

上書き設定がシステム全体の統合設定に対して自動的に作成された値から手動で変更される場合、その新しい値は無視されます。

テナントレベル統合設定のほとんどはホームページから作成されますが、[管理 (Admin)]、[組織 (Organization)]、[テナント (Tenant)]の各テナントレコードの別個のタブでも編集されます。テナント内からアクセスすると、テナントレベルで編集可能な設定のみが利用可能です。

事前に標準装備されている統合設定セクションは次のとおりです。

表 E-1　統合設定の事前設定

設定	詳細
NetBackup Adapter	このセクションでは、ソリューション全体に影響する設定が保持されます。次のセクションのうち 1 つのみがある必要があります。
NetBackup Adapter の使用方法	このセクションでは、ホームページの[使用方法 (Usage)]パネルのデータと計算が管理されます。次のセクションのうち 1 つのみがある必要があります。
NetBackup Adapter のアクセス権	このセクションでは、ソリューションで許可されるバックアップおよびリストアのアクションが決定されます。次のセクションのうち 1 つのみがある必要があります。
アクションリクエストタイプ	このセクションでは、特定の送信済みリクエストタイプの上書きがサポートされます。次のセクションのうち 1 つのみがある必要があります。

[vCloud Director インポートを追加 (Add vCloud Director Import)]フォームを完了すると生成される統合設定セクションは、次のとおりです。

表 E-2　生成される統合設定

設定	詳細
vCloud インポート *import*	このタイプのセクションには、vCloud Director インスタンスの詳細が含まれています。コンピュータはここからインポートされ、このセクションではインポートされたコンピュータと関連付けられている Self Service バックアップサーバーが決定されます。個別のテナント資格情報は、テナントに対して指定されます。複数の vCloud Director インポートセクションを指定できます。詳細情報を参照できます。 p.36 の「コンピュータの登録」を参照してください。

NetBackup Adapter

このセクションでは、ソリューション全体に影響する設定が保持されます。次のセクションのうち 1 つのみがある必要があります。

表 **E-3** NetBackup Adapter 設定

設定	テナント上書き	詳細
Report Customer Root	あり	このテナントのレポートが保存される Web サーバー上のフォルダのパス。
レポートファイル拡張子	なし	拡張子のセミコロン区切りリストを指定できます。
契約領域 (TB)	あり	使用に合意された領域の合計量 (TB)。 オプションの値。設定する場合、通常はテナントレベルで構成
クォータの適用	あり	この設定により、テナントレベルでの領域使用量の追跡を切り替えます。[契約領域 (TB) (Contracted Space (TB))] で設定した値が各テナントに契約領域として適用されるようにします。 この設定はデフォルトでは無効です。クォータの適用を有効にするには、各テナントでこのオプションを有効にする必要があります。
使用状況保持期間 (月)	なし	履歴ロールアップデータがホームページ使用状況グラフおよび表に表示するために保持される月数。
パネル URL	なし	NetBackup Adapter パネルの URL。この値は最初にインストーラによって設定されます。
サービス URL	なし	NetBackup Adapter Web サービスの URL。この値は最初にインストーラによって設定されます。
イメージインポートバッチ処理 (分)	なし	コンピュータイメージロードでは、コンピュータが同期にマークされている間の期間のイメージが取得されます。この値のデフォルトは 5 分です。
イメージインポートロック遅延 (分)	なし	この設定により、イメージ取得時にエラーが発生した場合にコンピュータに対してコンピュータ同期をロックする期間が決定されます。デフォルトは 60 分です。
使用状況電子メールの送信	なし	システム使用状況を詳細に記載する電子メールが各月の 1 日に送信されます。この電子メールの送信を希望しない場合、[いいえ (No)] に設定します。
[信号機表示 (Show Traffic Lights)] タイル	あり	この設定は、ホームページに信号機を表示するかどうかを決定します。
[合計使用量の表示 (Show Consumption Total)] タイル	あり	この設定は、ホームページに使用量の合計を表示するかどうかを決定します。

設定	テナント上書き	詳細
［使用傾向の表示 (Show Consumption Trend)］タイル	あり	この設定は、ホームページに使用傾向のグラフを表示するどうかを決定します。
［ESX ホスト選択アルゴリズム (ESX Host Selection Algorithm)］	あり	この設定には、［ランダム一致 (Random Match)］、［最良一致 (Best Match)］、［初回一致 (First Match)］の 3 つのオプションがあります。デフォルトは［ランダム一致 (Random Match)］です。このオプションは、ソースと宛先の vApp が異なる組織 vDC に存在する場合に、NetBackup Self Service が、ある vApp から別の vApp に対する VCD VM のリストアを試行したときに使用します。 この設定で許可されている値は以下のとおりです。 ランダム一致: ■ すべての利用可能なホストから ESX ホスト A をランダムに 1 つ選択します。 ■ ホスト A に、ランダムにリソースプールを選択します。 ■ ホスト A に、空き容量が最も大きいデータストアを選択します。 初回一致: ■ 1 つ目に利用可能な ESX ホスト A を選択します。 ■ ホスト A に、ランダムにリソースプールを選択します。 ■ ホスト A に、空き容量が最も大きいデータストアを選択します。 最良一致: ■ 空き容量が最も大きいデータストアに接続されている ESX ホスト A を選択します。 ■ ホスト A に、ランダムにリソースプールを選択します。 ■ ホスト A に、空き容量が最も大きいデータストアを選択します。

NetBackup Adapter 使用方法

このセクションでは、ホームページの［使用量 (Usage)］パネルのデータと計算が管理されます。次のセクションのうち 1 つのみがある必要があります。

表 E-4　アダプタの使用状況の設定

設定名	テナント上書き	詳細
料金タイプ	はい	料金が新しいバックアップまたは使用領域を表すのかどうか、または計算が行われないかどうかに関する基本パラメータ。 オプション: 新規バックアップ、使用容量、またはなし。
転送済みデータの値の使用	いいえ	使用量の統計で[転送済みサイズ (Transferred Size)]または[イメージサイズ (Image Size)]のどちらを使用するかを制御します。[転送済みサイズ (Transferred Size)]の値は、アクセラレータを使用する場合などで低くすることができます。[転送済みサイズ (Transferred Size)]の値は、NetBackup 7.7.1 以降でのみ利用可能です。

NetBackup Adapter のアクセス権

リストされているコンピュータに対しホームページから利用可能なアクションを決定します。アクションはシステム全体で、特定のテナント用、または個別のテナントユーザー用です。アクションは次のとおりです。

- 今すぐバックアップ (Backup Now)
- マシンを保護 (Protect Machine)
- ファイルのリストア (Restore File)
- VM のリストア (Restore VM)
- マシンを保護解除 (Unprotect machine)
- ファイルリストアを登録する (Register for File Restore)
- SQL のリストア (Restore SQL)
- Oracle のリストア (Restore Oracle)
- クラウド資産のリストア (Restore Cloud Asset)
- エージェントレスリストアファイル (Agentless Restore File)
- 代替 VM へのエージェントレスリストアファイル (Agentless Restore File to alternate VM)
- バックアップの期限切れ (Expire Backups)
- ディスクのリストア (Restore Disks)
- Kubernetes 名前空間のリストア (Restore Kubernetes Namespace)

このセクションでは、ホームページ[使用状況グラフ (Usage graph)]および[使用状況リスト (Usage list)]の管理も可能です。

次のセクションのうち 1 つのみがある必要があります。

表 E-5 NetBackup Adapter のアクセス権

設定名	テナント上書き	詳細
今すぐバックアップを許可 (Allow Backup Now)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
マシンの保護を許可 (Allow Protect Machine)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
ファイルのリストアを許可 (Allow Restore File)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
VM のリストアを許可 (Allow Restore Vm)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
マシンの保護解除を許可 (Allow Unprotect Machine)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
使用状況レポートを許可 (Allow Usage Report)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
ファイルリストアの登録を許可 (Allow Register for File Restore)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
SQL のリストアを許可 (Allow Restore SQL)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
Oracle のリストアを許可 (Allow Restore Oracle)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。
クラウド資産のリストアを許可 (Allow Restore Cloud Asset)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから [ユーザー用 (for user)] を選択します。この表の後の「注意」を参照してください。

設定名	テナント上書き	詳細
エージェントレスリストアファイルを許可 (Allow Agentless Restore File)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから[ユーザー用 (for user)]を選択します。この表の後の「注意」を参照してください。
代替 VM へのエージェントレスリストアファイルを許可 (Allow Agentless Restore File to alternate VM)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから[ユーザー用 (for user)]を選択します。この表の後の「注意」を参照してください。
バックアップの期限切れを許可 (Allow Expire Backups)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから[ユーザー用 (for user)]を選択します。この表の後の「注意」を参照してください。
ディスクのリストアを許可 (Allow Restore Disks)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから[ユーザー用 (for user)]を選択します。この表の後の「注意」を参照してください。
Kubernetes 名前空間のリストアを許可 (Allow Restore Kubernetes Namespace)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから[ユーザー用 (for user)]を選択します。この表の後の「注意」を参照してください。
Nutanix VM のリストアを許可 (Allow Restore Nutanix VM)	あり	この値をユーザーレベルで上書きするには、ドロップダウンから[ユーザー用 (for user)]を選択します。この表の後の「注意」を参照してください。

メモ: システム全体またはテナントレベルフラグのみを設定することをお勧めします。テナントユーザーレベルでの上書きは、システム全体設定が[有効 (enabled)]に設定されている場合にのみ考慮されます。

テナントの構成についての詳しい情報を参照できます。

p.33 の「テナントの構成」を参照してください。

アクションリクエストタイプ

このセクションでは、特定の送信済みリクエストタイプの上書きがサポートされます。次のセクションのうち 1 つのみがある必要があります。

標準装備されているリクエストタイプ詳細を変更する場合、まず標準装備されているリクエストタイプのコピーを作成します。次に、新しいリクエストタイプを必要に応じて修正しま

す。完了したら、新しいリクエストタイプを有効化し、このセクションを新しいリクエストタイプコードで更新できます。次に、標準装備されているリクエストタイプを無効化できます。

表 E-6　アクションリクエストタイプ

設定名	テナント上書き	詳細
DB VM のリストア	なし	VM のリストアダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBRESTVM です。
DB VM のリストアメッセージ	なし	このメッセージが提供される場合、VM をリストアするときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
ファイルの DB リストア	なし	ファイルのリストアダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBRESTFILE です。
DB リストアファイルメッセージ	なし	このメッセージが提供される場合、ファイルをリストアするときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
DB マシンを保護解除	なし	マシンを保護解除ダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBREMBACK です。
DB 保護解除メッセージ	なし	このメッセージが提供される場合、保護解除を指定するときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
DB ファイルリストアを登録する	なし	ファイルリストアを登録するダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBREGDNS です。
DB ファイルリストア登録メッセージ	なし	このメッセージが提供される場合、ファイルリストアの登録を選択するときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
SQL の DB リストア	なし	SQL データベースのリストアダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBRESTSQL です。

設定名	テナント上書き	詳細
DB SQL のリストアメッセージ	なし	このメッセージが提供される場合、SQL をリストアするときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
Oracle の DB リストア	なし	Oracle バックアップのリストアダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBRESTORA です。
DB Oracle のリストアメッセージ	なし	このメッセージが提供される場合、Oracle をリストアするときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
今すぐ DB バックアップメッセージ	なし	このメッセージが提供される場合、[今すぐバックアップ]が使用される時の通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
クラウド資産の DB リストア	なし	クラウド資産のリストアダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBRESTCLD です。
クラウド資産の DB リストアメッセージ	なし	このメッセージが提供される場合、クラウド資産をリストアするときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
DB 保護メッセージ	なし	このメッセージが提供される場合、保護を選択するときの通知に関して使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
ファイルのエージェントレス DB リストア	なし	[ファイルのリストア (Restore File)]ダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは ALFRORIG です。
ファイルのエージェントレス DB リストアメッセージ	なし	このメッセージが提供される場合、[ファイルのリストア (Restore File)]を使用するときの通知に使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
代替 VM へのファイルのエージェントレス DB リストア	なし	[代替 VM へのファイルのリストア (Restore File to Alternate VM)]ダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは ALFRALT です。

設定名	テナント上書き	詳細
代替 VM へのファイルのエージェントレス DB リストアメッセージ	なし	このメッセージが提供される場合、[代替 VM へのファイルのリストア (Restore File to Alternate VM)]を使用するときの通知に使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
ディスクの DB リストア	なし	[ディスクのリストア (Restore Disks)]ダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは `VMDISKREST` です。
ディスクの DB リストアメッセージ	なし	このメッセージが提供される場合、[ディスクのリストア (Restore Disks)]を使用するときの通知に使用されます。このエントリを省略した場合は、デフォルトのシステムメッセージが使用されます。この値のデフォルトは空です。
名前空間の DB リストア	なし	[Kubernetes 資産のリストア (Restore Kubernetes Asset)]ダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは `DBRESTNASP` です。
Nutanix VM の DB リストア	なし	Nutanix 資産のリストアダッシュボードオプションと関連付けられているリクエストタイプコード。デフォルトは DBRESTNUVM です。

vCloud Director インポート

この種のセクションには、特定の vCloud Director インスタンスからコンピュータをインポートして NetBackup Self Service に登録できるようにする vCloud Director インポートプロセスの詳細が記載されています。個々のクレデンシャルを使用するテナントベースでテナントにコンピュータをインポートします。vCloud Director インポートセクションは複数あります。

表 E-7

設定名	テナント上書き	詳細
vCloud Api	いいえ	この値は、`https://hostname/api/` 形式の vCloud Director API の URL に設定する必要があります。
場所 (Location)	いいえ	コンピュータが登録される NetBackup バックアップサーバーの名前。

設定名	テナント上書き	詳細
オンライン (Online)	いいえ	vCloud Director インスタンスがオンラインとみなされるかどうかを示します。Self Service では、オンラインでないインスタンスは使用されません。
SSL 証明書エラーを無視する (Ignore SSL Certificate Errors)	いいえ	このオプションを使用すると、Self Service で SSL 証明書が有効でない vCloud Director インスタンスに接続できるようになります。
vCloud ユーザー名 (vCloud username)	はい	テナントが vCloud Director API への接続に使用するユーザー名。各テナントに独自のクレデンシャルがある必要があります。`userid@vOrg` の形式にする必要があります。テナントレベルでのみ設定する必要があります。
vCloud パスワード (vCloud password)	はい	テナントの対応する vCloud Director パスワード。テナントレベルでのみ設定する必要があります。
保護タイプコード (Protection Type Code)	いいえ	インポートされたコンピュータに適用される保護タイプ。
vDC フィルタを使用する (Use vDC Filter)	いいえ	vDC フィルタリングを有効にするには、このオプションを設定します。
vDC フィルタ (vDC Filter)	いいえ	インポート時に vDC に適用されるフィルタ。このフィルタはカンマ区切りのリストで、vDC 名は大文字と小文字が区別されます。テナントレベルでのみ設定します。
表示名 (Display Name)	いいえ	エンドユーザーのホームページでデフォルトのビューに表示される名前。
メタデータを含める (Include Metadata)	はい	インポート時にメタデータを含めるかどうかを決定します。
vCloud 管理者ユーザー名 (vCloud Admin username)	いいえ	vCloud の管理者ユーザー (`Administrator@System` の形式)。
vCloud 管理者パスワード (vCloud Admin password)	いいえ	vCloud の管理者クレデンシャルを持つアカウントのパスワード。

F

REST API

この付録では以下の項目について説明しています。

- REST API について

REST API について

REST API は、コンピュータの追加、保護、リストアなど、システムに対する管理処理と操作処理の両方をサポートします。

API のマニュアルはインストールディレクトリの `SDK` フォルダに入っています。API のマニュアルは、VOX (Veritas Open Exchange) でも入手できます。URL は、`SDK` ディレクトリの `ReadMe.txt` ファイルで参照できます。これは、ポータルの[NetBackup Self Service について (About NetBackup Self Service)]ページでも見つけることができます。

API のバージョン 6 は有効化されており、ユーザーの資格情報を使ってログオンする必要があります。

G

用語集

この付録では以下の項目について説明しています。

- 用語集

用語集

表 G-1　用語集

用語	定義
資産	ソリューションが認識しているコンピュータまたはボリューム。
今すぐバックアップ	NetBackup マスターサーバーで一時ポリシーを作成し、それを即時バックアップ用にスケジュールする Self Service のユーザーアクション。テンプレートポリシーは後で削除されます。コンピュータがすでに保護され、スケジュール済みポリシー内に存在する場合、このオプションを使用して、そのポリシーを使用する即時バックアップを開始できます。
バックアップサーバー	バックアップサーバーは、NetBackup Master Server への接続を示します。バックアップサーバーは新しい UI 用語ですが、Rest API では引き続き「場所」が使用されます。
クラウドインポート	CloudPoint 資産の自動インポートを許可するコンピュータソース。
コンピュータ	ソリューションで認識される任意の物理コンピュータまたは仮想コンピュータ。
顧客コード	NetBackup Self Service のテナントを特定するために使用される一意のコード。このコードは、NetBackup のポリシー命名規則に使用されます。
イメージ同期	Self Service でコンピュータバックアップに関する情報が NetBackup から収集されるプロセス。

用語	定義
統合設定	統合設定は、Self Service ポータルで保持される値によって名前が付けられた設定のフレキシブルなストアです。すべての統合設定には、管理者ユーザーとして[管理 (Admin)]、[設定 (Settings)]、[統合設定 (Integration Settings)]からアクセスできます。統合設定がテナントレベルの例外で構成されている場合、[管理 (Admin)]、[組織 (Organization)]、[テナント (Tenant)]、[統合 (Integration)]からアクセスできます。
場所	場所は、NetBackup マスターサーバーへの接続を示します。この接続は、より一般な表現として、バックアップサーバーと呼ばれます。
マシン	ソリューションで認識される物理マシンまたは仮想マシン。
NetBackup Self Service	ソリューション全体を説明するために使用される用語。Self Service とも呼ばれます。
NetBackup Self Service Adapter	NetBackup との通信を行う Self Service システムの 2 番目の部分。
NetBackup Self Service ポータル	Self Service システムの最初の部分で、ソリューションのメインの Web サイト。
パネル	Self Service ポータルのホームページのサブ領域。ホームページウィジェットと呼ばれる場合もあります。
保護 (コンピュータ)	コンピュータを NetBackup ポリシーに追加して、定期的なバックアップをスケジュールする Self Service でのユーザーアクション。
保護レベル	保護レベルは、コンピュータに適用可能な保護のレベルを示します。保護レベルを構成することにより、ユーザーは NetBackup ポリシーに対して自分でスケジュールしたバックアップを保持できます。これは、各 NetBackup マスターサーバー上のテンプレートポリシーにマップされます。
保護タイプ	保護タイプにより、コンピュータを保護できるすべての方法が定義されます。この保護は、単一の保護レベル、または物理コンピュータと仮想コンピュータが混在する場合などは複数の保護レベルによって行うことがあります。スケジュールされた保護と 1 回限りのバックアップには、異なる保護レベルが必要になります。
NetBackup データの更新	イメージデータ、保護データ、および信号を再構築するためのコンピュータレベルの手動プロセスまたは自動プロセス。
マシンの登録	テナントのコンピュータに関する情報で Self Service システムを更新するために使用されるプロセス。
ファイル/フォルダのリストア	NetBackup でファイルまたはフォルダをリストアするジョブを作成する Self Service のユーザーアクション。

用語	定義
名前空間のリストア	NetBackup で Kubernetes 名前空間をリストアするジョブを作成する Self Service のユーザーアクション。
Nutanix VM のリストア	NetBackup で Nutanix VM をリストアするジョブを作成する Self Service のユーザーアクション。
VM のリストア	NetBackup で仮想マシンをリストアするジョブを作成する Self Service のユーザーアクション。
Self Service	ソリューション全体を説明するために使用される用語。NetBackup Self Service とも呼ばれます。
サービスカタログ	Self Service ポータルのユーザーに表示されるホームページ。[管理 (Admin)]、[サービスカタログ & 通知 (Service Catalog & Notices)]、[サービスカタログ (Service Catalog)]から編集できます。
サービスプロバイダ	Self Service システムを管理する最上位の組織を指します。
テンプレートポリシー	ユーザーに対し有効なポリシーを作成するために使用されるマスターサーバー上の無効な NetBackup ポリシー。
テナント	ユーザーの組織グループ。企業シナリオ内のビジネスユニット、またはサービスプロバイダの顧客として使用されることがあります。ユーザーはすべてテナント内にある必要があります。
管理対象外 (コンピュータ)	保護の追加クラス。コンピュータをリストアし、その健全性を監視できます。保護 (ポリシー管理) が NetBackup Self Service の外で処理されると想定します。
保護解除 (コンピュータ)	コンピュータが NetBackup ポリシーから削除される Self Service のユーザーアクション。
vCenter インポート	VMware 資産の自動インポートを許可するコンピュータソース。
vCloud Director インポート	vCloud Director からの自動インポートを許可するコンピュータソース。
Web サービス	ポータル用 API。これを使用してテナント、ユーザーなどの追加を自動化できます。DAPI と呼ばれることもあります。