NetBackup™ Web UI 管理者ガイド

リリース 10.1

VERITAS™

NetBackup™ Web UI 管理者ガイド

最終更新日: 2022-10-21

法的通知と登録商標

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

1

NetBackup の概要

この章では以下の項目について説明しています。

NetBackup について

NetBackup は、様々なプラットフォームに対して、完全かつ柔軟なデータ保護ソリューションを提供します。対象となるプラットフォームには、Windows、UNIX、Linux システムなどが含まれます。

NetBackup 管理者は、ネットワーク内のクライアントに対して、定期的またはカレンダーを基準として自動的な無人バックアップを実行するスケジュールを設定できます。バックアップを適切にスケジュールすることで、ネットワークの使用頻度が高い時間帯を避けて通信量を最適化しながら、一定期間にわたって計画的に完全なバックアップを実行できます。バックアップには、完全バックアップと増分バックアップがあります。完全バックアップは指定されたすべてのクライアントのファイルのバックアップを作成し、増分バックアップは前回のバックアップ以降に変更されたファイルのバックアップのみを作成します。

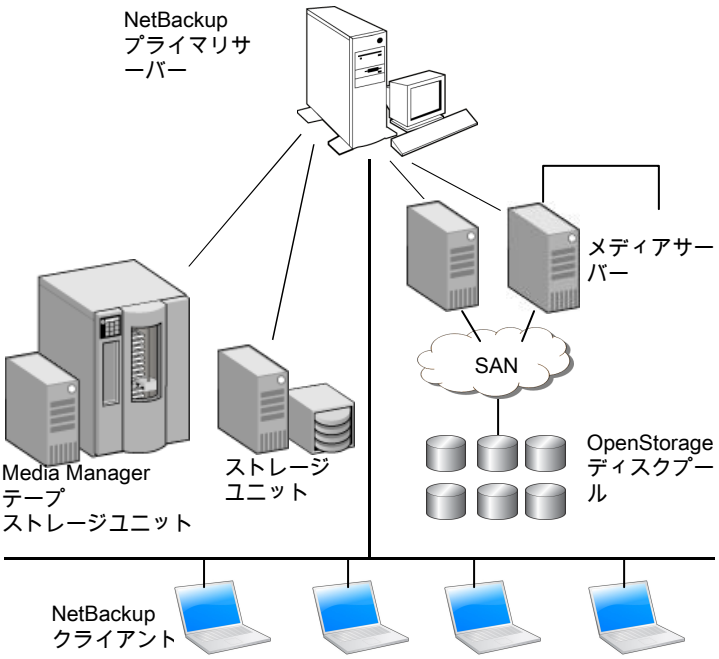
NetBackup の管理者によって許可されている場合、ユーザーは、自分のコンピュータからファイルのバックアップ、リストアまたはアーカイブを行うことができます。(アーカイブ操作では、正常にバックアップが完了すると、ファイルがローカルディスクから削除されます。)

次のように、NetBackup にはサーバーソフトウェアとクライアントソフトウェアの両方が含まれます。

- サーバーソフトウェアは、ストレージデバイスを管理するコンピュータにインストールします。
- クライアントソフトウェアは、バックアップを行うデータが存在するコンピュータにインストールします。(また、クライアントソフトウェアはサーバーにも含まれており、サーバーのバックアップを行うことができます。)

図 1-1 に NetBackup ストレージドメインの例を示します。

図 1-1　　NetBackup ストレージドメインの例



NetBackup では、次のように、複数のサーバーが連携して動作するように、1 台の NetBackup プライマリサーバーの管理下でサーバーが制御されます。

- プライマリサーバーでは、バックアップ、アーカイブおよびリストアが管理されます。また、NetBackup で使用されるメディアおよびデバイスを選択します。通常、プライマリ

サーバーには NetBackup カタログが含まれます。カタログには、NetBackup のバックアップおよび構成についての情報を含む内部データベースが含まれます。

- メディアサーバーでは、接続されているストレージデバイスを NetBackup で使用可能にすることによって、追加のストレージが提供されます。また、メディアサーバーを使用すると、ネットワークの負荷を分散させることによってパフォーマンスを向上できます。メディアサーバーは、次の用語でも呼ばれます。
  - デバイスホスト (テープデバイスが存在する場合)
  - ストレージサーバー (I/O がディスクに直接実行される場合)
  - データムーバー (OpenStorage 装置のような独立した外部ディスクデバイスへデータを送信する場合)

バックアップまたはアーカイブ中に、クライアントは、NetBackup サーバーにネットワークを介してバックアップデータを送信します。NetBackup サーバーは、バックアップポリシーで指定された形式のストレージを管理します。

ユーザーは、リストア中に、リカバリするファイルおよびディレクトリを表示して選択できます。選択したファイルおよびディレクトリは NetBackup によって検索され、クライアントのディスクにリストアされます。

NetBackup のマニュアル

サポートされている各リリースに関する NetBackup のテクニカルマニュアルの完全なリストについては、次の URL にある NetBackup のマニュアルのランディングページを参照してください。

https://www.veritas.com/docs/DOC5332

Adobe Acrobat Reader のインストールおよび使用についての責任は負いません。

NetBackup Web UI の機能

NetBackup Web ユーザーインターフェースは、次の機能を提供します。

- Chrome や Firefox などの Web ブラウザからプライマリサーバーにアクセスする機能。Web UI でサポートされるブラウザについて詳しくは、NetBackup ソフトウェア互換性リストを参照してください。
  NetBackup Web UI は、ブラウザによって動作が変わる場合があります。日付選択などの一部の機能は、一部のブラウザでは利用できないことがあります。こうした違いは、NetBackup の制限によるものではなく、ブラウザの機能によるものです。
- 重要な情報の概要を表示するダッシュボード。

- 役割ベースのアクセス制御 (RBAC) により、管理者は NetBackup へのユーザーアクセスを構成し、セキュリティ、ストレージ管理、または作業負荷の保護などのタスクを委任できます。
- NetBackup セキュリティ設定、証明書、API キー、ユーザーセッションの管理。
- NetBackup ホストのプロパティの管理。
- データ保護は、保護計画またはポリシーを通じて実現されます (現時点では、ポリシーのサポートは制限されています。今後のリリースでポリシー形式が追加される予定です)。
- 検出機能とレポート機能により、マルウェアと異常が検出され、プライマリサーバーのバックアップデータのサイズを追跡する使用状況レポートが提供されます。また、Veritas NetInsights コンソールに簡単に接続して、NetBackup ライセンスを表示および管理できます。

メモ: NetBackup Web UI は、1280x1024 以上の画面解像度で最適に表示されます。

NetBackup Web UI のアクセス制御

NetBackup では、役割ベースのアクセス制御を使用して Web UI へのアクセス権を付与します。アクセス制御は、役割を通じて実行されます。

- 役割は、ユーザーが実行できる操作と、作業負荷資産、保護計画、またはクレデンシャルに必要なアクセス権を定義します。単一のユーザーに複数の役割を設定でき、ユーザーアクセスを完全かつ柔軟にカスタマイズできます。
- RBAC は、Web UI と API でのみ利用可能です。
  NetBackup のその他のアクセス制御方法は、拡張監査 (EA) を除いて、Web UI と API ではサポートされません。

NetBackup ジョブおよびイベントの監視

NetBackup Web UI を使用すると、管理者はより簡単に NetBackup 操作とイベントを監視し、注意が必要な問題を特定できます。

- ダッシュボードに、NetBackup の操作とセキュリティ情報の概要が表示されます。この情報には、ジョブ、証明書、トークン、セキュリティイベント、マルウェア検出、異常検出、および使用状況レポートが含まれます。
  表示されるダッシュボードウィジェットは、ユーザーの RBAC の役割と権限によって異なります。
- ジョブが失敗したときに管理者が通知を受信するように電子メール通知を設定できます。NetBackup は、受信電子メールを受け取ることができる任意のチケットシステムをサポートします。

保護計画: スケジュールとストレージを一元的に構成する場所

保護計画によるデータ保護は、役割ベースのアクセス制御 (RBAC) を使用して完全に管理されます。NetBackup 管理者は、資産を表示および管理できるユーザーや、バックアップおよびリストアを実行できるユーザーを管理できます。デフォルトの作業負荷管理者の役割 (デフォルトの VMware 管理者など) では、ユーザーが保護計画、ジョブ、クレデンシャルにアクセスできます。

p.93 の「サポートされる保護計画の種類」を参照してください。

保護計画には、次の利点があります。

- 作業負荷管理者は、バックアップスケジュールや使用されているストレージを含む保護計画を作成して管理できます。この管理者は、資産を保護する保護計画を選択します。
  p.203 の「役割の権限」を参照してください。
- バックアップのスケジュールに加えて、保護計画には、レプリケーションと長期保持のスケジュールも含めることができます。
- 利用可能なストレージから選択するときに、そのストレージで利用可能な追加機能を確認できます。
- 作業負荷管理者の役割を持つユーザーは、保護計画を作成し、クレデンシャルを管理し、SLO を満たす保護計画に資産をサブスクライブし、保護状態を監視できます。

バックアップポリシー

データ保護に引き続きポリシーを使用したい管理者は NetBackup の従来のポリシーを使用できます。

p.93 の「NetBackup の従来のポリシーのサポート」を参照してください。

サーバー主導リカバリとセルフサービスリカバリ

管理者は、Web UI からサーバー主導リストアを実行できます。この形式のリストアはすべてのポリシー形式で利用可能です。

作業負荷管理者は、VM、データベース、その他の資産タイプのセルフサービスリカバリを実行できます。この形式のリカバリは、リカバリポイントで保護されている資産で使用できます。

インスタントアクセス機能をサポートする作業負荷の場合、ユーザーはスナップショットをマウントして、VM のファイルやデータベースにすぐにアクセスできます。

NetBackup 管理インターフェース

NetBackup は複数のインターフェースで管理できます。最もよい選択は、個人の好みと管理者が利用できるシステムによって異なります。

表 1-1 NetBackup 管理インターフェース

インターフェースの名前	説明
NetBackup Web ユーザーインターフェース	NetBackup Web UI (ユーザーインターフェース) を使用すると、プライマリサーバーから NetBackup のアクティビティを表示し、NetBackup 構成を管理できます。 NetBackup の Web UI を起動するには ■ ユーザーは、NetBackup RBAC でそのユーザー向けに設定された役割を持っている必要があります。 ■ Web ブラウザを開き、次の URL に移動します。https://*primaryserver*/webui/login
NetBackup 管理コンソール	[NetBackup 管理コンソール (NetBackup Administration Console)]には、役割に基づくアクセス制御を除いて、NetBackup のすべての利用可能な構成と機能が含まれます。 プライマリサーバーから、すべてのメディアサーバー上のストレージデバイスを構成および管理できます。 NetBackup には、NetBackup のサポート対象バージョンすべての管理コンソールが含まれています。管理する NetBackup サーバーと互換性があるコンソールのバージョンを選択します。 NetBackup 管理コンソールを開始するには ■ Windows の場合、[NetBackup *x.x* 管理コンソール (NetBackup x.x Administration Console)]を[スタート (Start)]メニューから選択します。 ■ UNIX の場合、`jnbSA` コマンドを実行します。 **メモ:** NetBackup 管理コンソールにログインするには、ログインクレデンシャルが接続するプライマリサーバーまたはメディアサーバーから認証されている必要があります。
文字ベースのメニューインターフェース	`tpconfig` コマンドを実行して、デバイス管理のための文字ベースのメニューインターフェースを起動します。 `termcap` か `terminfo` が定義されている任意の端末 (または端末エミュレーションウィンドウ) から `tpconfig` インターフェースを使用します。
コマンドライン	NetBackup コマンドは Windows と UNIX の両方のプラットフォームで利用可能です。NetBackup コマンドは、システムのプロンプトで入力するか、スクリプト内で使います。 NetBackup の管理者向けプログラムとコマンドはすべて、root または管理者のユーザー権限がデフォルトで必要です。

用語

次の表では、Web ユーザーインターフェースの概念と用語について説明します。

表 1-2 Web ユーザーインターフェースの用語および概念

用語	定義
管理者	NetBackup と、NetBackup Web UI を含むすべてのインターフェースに対する完全なアクセス権を持つユーザーです。root、管理者、拡張監査のすべてのユーザーは、NetBackup に対して完全なアクセス権を持ちます。NetBackup Web UI の各ガイドでは、*NetBackup 管理者*という用語は、NetBackup への完全なアクセス権を持つユーザーも指します。 *「役割」*も参照してください。
資産グループ	*「インテリジェントグループ」*を参照してください。
資産	物理クライアント、仮想マシン、データベースアプリケーションなどの保護対象データです。
今すぐバックアップ	資産のバックアップをすぐに作成します。NetBackup は、選択した保護計画を使用して資産の完全バックアップを 1 回のみ実行します。このバックアップは、スケジュールバックアップには影響しません。
従来のポリシー	NetBackup Web UI では、レガシーポリシーが資産を保護することを示します。
外部証明書	NetBackup 以外のあらゆる CA から発行されたセキュリティ証明書です。
インテリジェントグループ	指定した条件 (問い合わせ) に基づいて、NetBackup が保護対象資産を自動的に選択することを可能にします。インテリジェントグループは、本番環境の変更が含まれるように、自動的に最新の状態に維持されます。これらのグループは、資産グループとも呼ばれます。 [インテリジェント VM グループ (Intelligent VM groups)]タブまたは[インテリジェントグループ (Intelligent groups)]タブにこれらのグループが表示されます。
NetBackup 証明書	NetBackup CA から発行されたセキュリティ証明書です。
保護計画	保護計画は、バックアップを実行するタイミング、バックアップの保持期間、使用するストレージ形式を定義します。保護計画を設定したら、資産を保護計画にサブスクライブできます。
RBAC	役割ベースのアクセス制御です。役割の管理者は、RBAC で設定されている役割を通じて、NetBackup Web UI へのアクセスを委任または制限できます。 注意: RBAC で設定した役割は、NetBackup 管理コンソールへのアクセスを制御しません。

用語	定義
役割	RBAC では、ユーザーが実行できる操作と、ユーザーがアクセスできる資産やオブジェクトを定義します。たとえば、特定のデータベースのリカバリを管理する役割と、バックアップおよびリストアに必要なクレデンシャルを設定できます。
ストレージ	データのバックアップ、レプリケート、または複製 (長期保持用) 対象となるストレージです。
保護計画にサブスクライブする	保護計画にサブスクライブする資産または資産グループを選択する処理です。資産は、保護計画のスケジュールに従って保護されます。Web UI では、*サブスクライブ*を「保護の追加」とも表記します。
保護計画からサブスクライブ解除する	*サブスクライブ解除*は、保護を解除する処理、または計画から資産や資産グループを削除する処理を指します。
作業負荷	資産のタイプです。たとえば、VMware、Microsoft SQL Server、またはクラウドです。

NetBackup Web UI への初回サインイン

NetBackup のインストール後に、管理者が NetBackup Web UI に Web ブラウザからサインインして、ユーザー向けに RBAC の役割を作成する必要があります。役割は、組織のユーザーの役割に基づいて、Web UI を通じて NetBackup 環境にアクセスするためのアクセス権をユーザーに付与します。一部のユーザーは、デフォルトで Web UI にアクセスできます。

p.190 の「権限を持つユーザー」を参照してください。

root または管理者のクレデンシャルへのアクセス権がない場合は、`bpnbaz -AddRBACPrincipal` コマンドを使用して管理者ユーザーを追加できます。

NetBackup Web UI を使用して、NetBackup プライマリサーバーにサインインするには

1 Web ブラウザを開き、次の URL に移動します。

https://*primaryserver*/webui/login

primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

Web UI にアクセスできない場合、「サポートと追加の構成」を参照してください。

2 管理者のクレデンシャルを入力して、[サインイン (Sign in)]をクリックします。

ユーザーの種類	使用する形式	例
ローカルユーザー	*username*	jane_doe
Windows ユーザー	*DOMAIN¥username*	WINDOWS¥jane_doe
UNIX ユーザー	*username@domain*	john_doe@unix

3 左側で、[セキュリティ (Security)]、[RBAC]の順に選択します。

4 次のいずれかの方法で、NetBackup Web UI へのアクセス権をユーザーに付与できます。

- NetBackup へのアクセスを必要とするすべてのユーザーに役割を作成します。
- 別のユーザーに役割を作成するタスクを委任します。
  RBAC の役割を追加する権限を持つ役割を作成します。このユーザーは、NetBackup Web UI へのアクセスを必要とする、すべてのユーザー向けに役割を作成できます。

p.191 の「RBAC の構成」を参照してください。

RBAC の役割を作成する権限を 1 人以上のユーザーに委任した後は、Web UI に root または管理者アクセスは不要です。

サポートと追加の構成

Web UI へのアクセスのヘルプについては、次の情報を参照してください。

- 権限があるユーザーであることを確認します。
  p.190 の「権限を持つユーザー」を参照してください。
- Web UI でサポートされるブラウザについて詳しくは、NetBackup ソフトウェア互換性リストを参照してください。
- ポート 443 が遮断されているか使用中の場合、カスタムポートを構成して使用できます。

- Web ブラウザで外部証明書を使用する場合は、次のトピックを参照してください。
  p.133 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。
- Web UI にアクセスするためのその他のヒントを参照してください。
  p.267 の 第34章 を参照してください。

NetBackup Web UI へのサインイン

権限を持つユーザーは、NetBackup Web UI を使用して、NetBackup プライマリサーバーに Web ブラウザからサインインできます。NetBackup Web ユーザーインターフェース (Web UI) は、NetBackup 8.1.2 以降で利用可能です。このインターフェースは、プライマリサーバー上で利用可能で、そのサーバー上の NetBackup のバージョンをサポートします。NetBackup 管理コンソールで実施するように特定のバージョンを見つけて開く必要はありません。

ユーザーは、サインイン方法について NetBackup セキュリティ管理者に問い合わせる必要があります。

利用可能なサインインオプションは次のとおりです。

- 「ユーザー名とパスワードでサインインする」
- 「証明書またはスマートカードでサインインする」
- 「シングルサインオン (SSO) でサインインする」

ユーザー名とパスワードでサインインする

ユーザー名とパスワードを使用して NetBackup Web UI にサインインできます。

ユーザー名とパスワードを使用して NetBackup プライマリサーバーにサインインするには

1 Web ブラウザを開き、次の URL に移動します。

https://*primaryserver*/webui/login

primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

2 利用可能なサインイン方法に応じて、次から選択します。

- クレデンシャルを入力して、[サインイン (Sign in)]をクリックします。
- デフォルトの方法がユーザー名とパスワードによる方法でない場合は、[ユーザー名とパスワードでサインインする (Sign in with user name and password)]をクリックします。次に、クレデンシャルを入力します。

クレデンシャルの例を次に示します。

ユーザーの種類	使用する形式	例
ローカルユーザー	*username*	jane_doe
Windows ユーザー	*DOMAIN¥username*	WINDOWS¥jane_doe
UNIX ユーザー	*username*	john_doe

証明書またはスマートカードでサインインする

スマートカードまたはデジタル証明書を使用して NetBackup Web UI にサインインできます。スマートカードにないデジタル証明書を使用するには、まずブラウザの証明書マネージャに証明書をアップロードする必要があります。詳しくはブラウザのマニュアルで手順を参照するか、証明書管理者にお問い合わせください。

証明書またはスマートカードでサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*primaryserver*/webui/login

   primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

2. ［証明書またはスマートカードでサインイン (Sign in with certificate or smart card)］をクリックします。
3. ブラウザにプロンプトが表示されたら、証明書を選択します。

シングルサインオン (SSO) でサインインする

NetBackup 環境内で SAML が ID プロバイダとして設定されている場合、シングルサインオン (SSO) オプションを使用して NetBackup Web UI にサインインできます。

SSO を使用して NetBackup プライマリサーバーにサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*primaryserver*/webui/login

   primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

2. ［シングルサインオンでサインイン (Sign in with single sign-on)］をクリックします。
3. 管理者が指示する手順に従ってください。

   以降のログオンでは、NetBackup によって自動的にプライマリサーバーへのサインインが行われます。

NetBackup Web UI からのサインアウト

NetBackup は、24 時間 (ユーザーセッションで許可される最大時間) 後に Web UI からの自動サインアウトを強制的に実行します。その時間が経過すると、NetBackup は再びサインインを要求します。また、使用するサインインオプション (ユーザー名とパスワード、スマートカード、またはシングルサインオン (SSO)) を変更する場合にもサインアウトできます。

NetBackup Web UI からサインアウトするには

- 右上で、プロファイルアイコン、[サインアウト (Sign out)]の順にクリックします。

カタログリカバリウィザード、ディスクアレイホスト、ディスクプール、および NetBackup Web UI のホストプロパティのマニュアル

NetBackup Web UI には、このマニュアルに記載されていない機能が含まれています。別途明記されていない限り、次の機能について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

- カタログリカバリウィザード
- ディスクアレイホスト
- ディスクプール
  - [ディスクボリュームの更新 (Update Disk Volume)]オプション
  - OpenStorage ディスクプールの状態
- ホストプロパティ

1

監視と通知

2

NetBackup アクティビティの監視

この章では以下の項目について説明しています。

NetBackup ダッシュボード

表 2-1 NetBackup ダッシュボード

ダッシュボードウィジェット	説明
ジョブ	実行中のジョブやキューに投入済みのジョブの数、試行されたジョブや完了したジョブの状態などのジョブ情報を一覧表示します。
マルウェアの検出	イメージに対するマルウェアスキャンの結果の状態 (影響あり、影響なし、失敗、進行中、保留中など) を表示します。
異常検出	現在報告されている異常の合計数を表示します。 p.228 の「異常の表示」を参照してください。 注意: 異常数が 0 の場合は、異常が発生しなかったか、異常検出サービスが実行されていない可能性があります。

ダッシュボードウィジェット	説明
一時停止した保護アクティビティ	クライアントの一時停止中の保護アクティビティを一覧表示します。これらのアクティビティには、新しいバックアップ、複製、イメージの有効期限切れが含まれます。バックアップイメージにマルウェアを検出した場合、NetBackup は保護を一時停止します。 [自動 (Automatic)]は、NetBackup によって自動的に一時停止されるアクティビティを示します。[ユーザーによる開始 (User-initiated)]は、ユーザーが手動で一時停止したアクティビティを示します。 p.114 の「バックアップおよびその他のアクティビティの一時停止」を参照してください。
トークン	環境内の認証トークンに関する情報を表示します。
証明書	環境内の NetBackup のホスト ID ベースのセキュリティ証明書または外部証明書に関する情報を表示します。 外部証明書では、NetBackup 8.2 以降のホストに関する次の情報が表示されます。 ■ ホストの合計。ホストの合計数。ホストはオンラインになっており、NetBackup プライマリサーバーと通信できる必要があります。 ■ 不明。外部証明書が登録されていないホストの数です。 ■ 有効。外部証明書が登録されているホストの数です。 ■ 期限切れ。期限切れの外部証明書を持つホストの数です。 詳しくは、[証明書 (Certificates)]、[外部証明書 (External certificates)]の順に移動して参照してください。 p.127 の「NetBackup のセキュリティ管理と証明書について」を参照してください。
セキュリティイベント	[アクセス履歴 (Access history)]ビューには、ログオンイベントのレコードが含まれます。[監査イベント (Audit events)]ビューには、ユーザーが NetBackup プライマリサーバーで開始したイベントが含まれます。
使用状況レポート	組織内の NetBackup プライマリサーバーのバックアップデータのサイズを一覧表示します。このレポートは、容量ライセンスを追跡するために役立ちます。右上のドロップダウンリストを使用して、表示する期間とビューを選択します。サーバー名をクリックして、そのサーバーの特定の詳細を表示します。 このウィジェットでプライマリサーバーの情報を表示するために NetBackup を構成する方法について、追加の情報を参照できます。 p.231 の「プライマリサーバー上の保護データのサイズの追跡」を参照してください。

アクティビティモニター

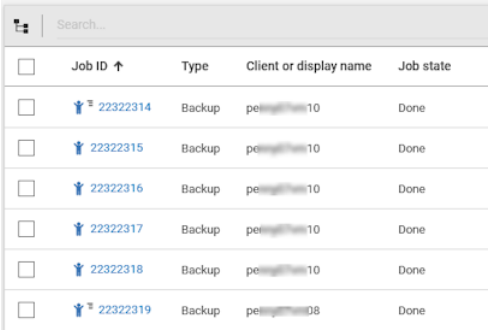
アクティビティモニターを使用して、NetBackup に関する次の側面を監視および制御できます。アクティビティモニターは、ジョブの開始、更新、完了のタイミングで更新されます。

ジョブ (Jobs)	プライマリサーバーに対して処理中または完了したジョブを表示します。[ジョブ (Jobs)] タブには、ジョブの詳細も表示されます。 p.28 の「ジョブの監視」を参照してください。
デーモン (Daemons)	プライマリサーバー上の NetBackup デーモンの状態が表示されます。環境内のメディアサーバーのデーモンを表示するには、[サーバーの変更 (Change server)]をクリックします。
プロセス (Processes)	プライマリサーバー上で実行されている NetBackup プロセスが表示されます。環境内のメディアサーバーのプロセスを表示するには、[サーバーの変更 (Change server)]をクリックします。

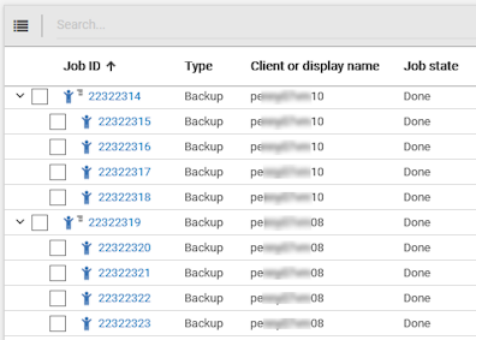
ジョブの監視

アクティビティモニターの[ジョブ (Jobs)]ノードを使用して、NetBackup 環境内のジョブを監視します。ジョブのデフォルトのビューは、すべてのジョブを非階層型でリストする一覧表示です。階層表示を使用して、親ジョブと子ジョブの階層を表示することもできます。親ジョブの役割は、要求された作業を子ジョブの形式で開始することです。

一覧表示



階層表示



ジョブに対する RBAC 権限

表示および管理できるジョブの種類は、ユーザーが持つ RBAC の役割によって異なります。たとえば、作業負荷管理者 (デフォルトの VMware 管理者の役割など) は、その作業負荷のジョブのみを表示および管理できます。一方、管理者の役割では、すべての NetBackup ジョブを表示および管理できます。

p.29 の「特定のジョブ権限に対してカスタムの RBAC の役割を必要とする作業負荷」を参照してください。

ジョブ階層の表示

ジョブへのアクセスを許可する RBAC の役割がある場合は、ジョブ階層表示にジョブのリストを表示できます。たとえば、デフォルトの VMware 管理者の役割では、階層表示に VMware ジョブを表示できます。ただし、1 つ以上の VM にのみアクセスできる場合 (資産レベルのアクセス)、ジョブ階層表示にジョブは表示されません。

p.196 の「 デフォルトの RBAC の役割」を参照してください。

特定のジョブ権限に対してカスタムの RBAC の役割を必要とする作業負荷

NetBackup Web UI では、特定の作業負荷に対して個別のジョブアクセスを提供します。この機能を使用すると、特定の作業負荷に対するジョブ権限を持つカスタムの RBAC の役割を作成できます。

これらの作業負荷には、対応するデフォルトの RBAC の役割がありません。カスタムの役割を構成するときに、[作業負荷 (Workloads)]カードの権限は、これらの作業負荷には適用されません。以下の作業負荷の種類に対して、ジョブ権限を構成できます。

BackTrack	Hyper-V	NDMP
DataStore	Informix	PureDisk Export
DB2	Lotus Notes	SAP
Enterprise Vault	SharePoint	Standard
Exchange	MS-Windows	Sybase
FlashBackup	NAS Data Protection	Vault
FlashBackup Windows	NBU Catalog	

ジョブ権限を持つカスタムの役割を作成するには

1. カスタムの RBAC の役割を作成します。
2. [資産 (Assets)]タブで作業負荷名を見つけ、作業負荷のジョブ権限を選択します。

   たとえば、Hyper-V 管理者が Hyper-V ジョブを表示できるように、カスタムの役割を作成するとします。[Hyper-V]を見つけて、必要なジョブ権限を選択します。
3. その役割に必要な追加の権限を選択します。

   例:

   - その他のグローバル権限

- 保護計画およびクレデンシャルの権限

4 その役割に割り当てるユーザーを追加します。

BigData 作業負荷に対する RBAC ジョブ権限

BigData 作業負荷 (Hadoop、HBase、MongoDB) 専用のジョブ権限を構成できません。BigData のジョブを表示および管理するには、すべての NetBackup ジョブに対する RBAC 権限を持つ役割を作成します。

ジョブ権限を構成するには

1 カスタムの RBAC の役割を作成します。

2 [権限 (Permissions)] で[割り当て (Assign)]をクリックします。

3 [グローバル (Global)]タブで NetBackup の管理を展開します。

4 [ジョブ (Jobs)]を見つけ、役割に必要なジョブ権限を選択します。

5 その役割に必要なユーザーを追加します。

ジョブの表示

NetBackup が実行する各ジョブについて、ファイルリストとジョブの状態、ログに記録されたジョブの詳細、およびジョブ階層を表示できます。

表示できるジョブは、付与されている RBAC の役割によって異なります。

p.28 の「ジョブの監視」を参照してください。

ジョブおよびジョブの詳細を表示するには

1 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。

2 表示するジョブの名前をクリックします。

3 [概要 (Overview)]タブで、ジョブに関する情報を表示します。

- [ファイルリスト (File List)]には、バックアップイメージに含まれているファイルが表示されます。
- [状態 (Status)]セクションには、ジョブに関連する状態と状態コードが表示されます。状態コード番号をクリックすると、この状態コードについてのベリタスナレッジベースの情報が表示されます。
  『NetBackup 状態コードリファレンスガイド』を参照してください。

4 [詳細 (Details)]タブをクリックして、ジョブについて記録された詳細を表示します。ドロップダウンメニューを使用して、エラーの種類によってログをフィルタできます。

p.32 の「ジョブリストのジョブの検索またはフィルタ処理」を参照してください。

5 [ジョブ階層 (Job hierarchy)]タブをクリックすると、ジョブ (親ジョブや子ジョブを含む) の完全な階層が表示されます。

p.31 の「階層表示内のジョブの表示」を参照してください。

一覧表示でのジョブの表示

アクティビティモニターの[ジョブ (Jobs)]ノードでは、一覧表示にジョブが表示されます。親ジョブと子ジョブの関係は表示されません。

一覧表示でジョブを表示するには

1 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。

2 [一覧表示 (List view)]ボタンをクリックします。

階層表示内のジョブの表示

アクティビティモニターの[ジョブ (Jobs)]ノードでは、階層表示にジョブが表示され、ジョブの完全な階層を確認できます。この表示には、最上位のジョブ (ルートジョブ) とその子ジョブ (ある場合) が含まれます。子ジョブは、下位の子ジョブの親になることができます。

階層表示内のジョブを表示するには

1 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。

2 [階層表示 (Hierarchy view)]ボタンをクリックします。

3 最上位のジョブを見つけて展開すると、子ジョブが表示されます。

ジョブ: キャンセル、一時停止、再起動、再開、削除

ジョブに対しては、そのジョブの状態に応じて特定の処理を実行できます。

ジョブを管理するには

1. 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。
2. 1 つ以上のジョブを選択します。
3. 最上位のメニューは、選択したジョブで実行できるアクションを示します。

キャンセル (Cancel)	まだ完了していないジョブは取り消すことができます。このようなジョブの状態は、[キューに投入済み (Queued)]、[キューに再投入済み (Requeued)]、[有効 (Active)]、[未完了 (incomplete)]、または[一時停止 (Suspended)]のいずれかである場合があります。 親ジョブがキャンセルされた場合、子ジョブもすべてキャンセルされます。
一時停止 (Suspend)	チェックポイントを含むバックアップジョブやリストアジョブを一時停止できます。
再起動 (Restart)	完了したジョブや、失敗したジョブ、キャンセルまたは一時停止されたジョブを再起動できます。 新しいジョブには、新しいジョブ ID が作成されます。
再開 (Resume)	一時停止されたジョブや、未完了状態のジョブを再開できます。
削除 (Delete)	完了したジョブを削除できます。親ジョブを削除すると、子ジョブもすべて削除されます。

ジョブリストのジョブの検索またはフィルタ処理

アクティビティモニターでジョブを検索したり、フィルタを作成して、表示するジョブをカスタマイズできます。

ジョブリストのジョブの検索

検索機能では、ジョブ情報 (状態コード (完全な状態コード番号)、ポリシー名、クライアント名または表示名、クライアント、ジョブ ID (完全なジョブ ID 番号)、ジョブの親 ID) を検索できます。

ジョブリストのジョブの検索

1. 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。
2. [検索 (Search)]ボックスに、検索するキーワードを入力します。たとえば、クライアント名や状態コード番号などです。

ジョブリストのフィルタ処理

ジョブリストをフィルタするには

1. 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。
2. ツールバーの[フィルタ (Filter)]アイコンをクリックします。
3. 作成したフィルタをクリックします。または、[すべてのジョブ (All jobs)]をクリックして、利用可能なすべてのジョブを表示します。

ジョブフィルタの作成

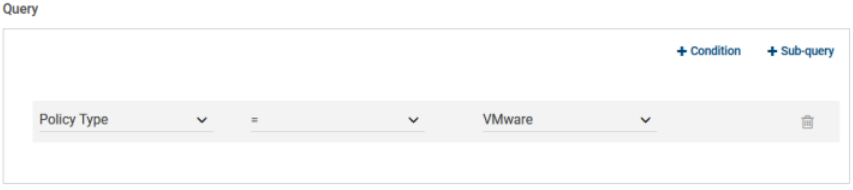
1 つ以上の問い合わせ条件に基づいて特定のフィルタを作成できます。

ジョブフィルタを作成するには

1. 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。
2. ツールバーの[フィルタ (Filter)]アイコンをクリックします。
3. フィルタがまだ作成されていない場合は、左側で[フィルタの作成 (Create filter)]をクリックします。

   それ以外の場合は、[処理 (Actions)]、[作成 (Create)]の順にクリックします。
4. フィルタの名前と、必要に応じて説明を入力します。
5. [問い合わせ (Query)]ペインで、ドロップダウンリストを使用して条件を作成します。

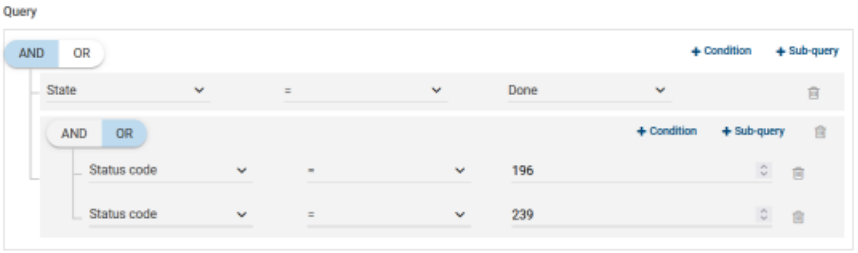
   たとえば、VMware ポリシータイプのすべてのジョブを表示するには、Policy type = VMware と入力します。



6 フィルタの条件を追加するか、条件に適用するサブクエリーを追加します。

たとえば、状態コードが 196 または 239 の完了ジョブをすべて表示するとします。次の問い合わせを作成します。

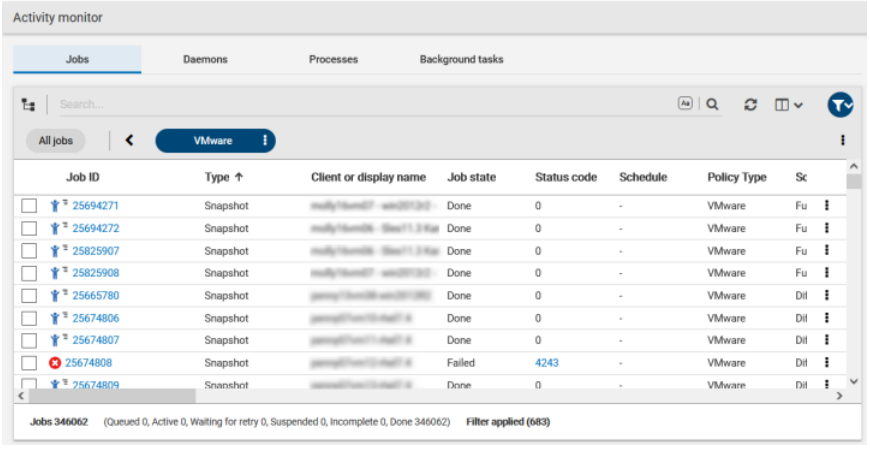
```
State = Done
AND
    (Status code = 196
    OR
    Status code = 239)
```



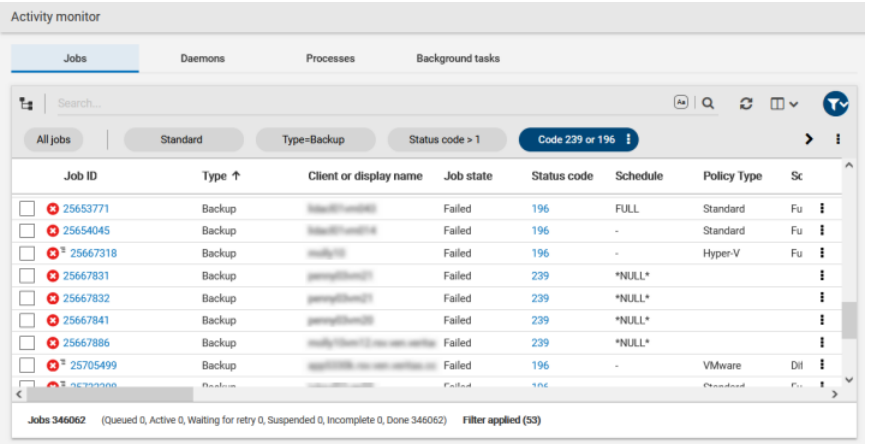
7 次のオプションのいずれかを選択します。

- この問い合わせを保存して別の問い合わせを作成するには、[保存してさらに追加 (Save and add another)]をクリックします。
- この問い合わせを保存してジョブリストに戻るには、[保存して適用 (Save and apply)]をクリックします。

例 1. VMware ポリシータイプの全ジョブの問い合わせフィルタ。



例 2. 完了し、状態コードが 196 または 239 である全ジョブの問い合わせフィルタ。



ジョブフィルタの編集または削除

ジョブフィルタの問い合わせ条件を編集したり、不要になったフィルタを削除できます。

ジョブフィルタの編集

ジョブフィルタを編集するには

1. 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。
2. ツールバーの[フィルタ (Filter)]アイコンをクリックします。
3. 削除するフィルタを見つけ、[処理 (Actions)]、[編集 (Edit)]の順にクリックします。
4. フィルタに必要な変更を加え、[保存して適用 (Save and apply)]をクリックします。

ジョブフィルタの削除

ジョブフィルタを削除するには

1. 左側で、[アクティビティモニター (Activity monitor)]をクリックします。次に、[ジョブ (Jobs)]タブをクリックします。
2. ツールバーの[フィルタ (Filter)]アイコンをクリックします。
3. コピーするフィルタを選択し、[処理 (Actions)]、[編集 (Edit)]の順にクリックします。

ジョブの表示に関するトラブルシューティング

次の原因により、ジョブの結果が表示されない場合があります。

- 検索したキーワードがどのジョブの詳細情報にも一致しない。
- 検索フィルタを適用したが、フィルタ基準に一致するジョブがない。
- 階層表示内のジョブに親ジョブはあるが、親ジョブを表示する権限がない。
  必要な RBAC の役割のアクセス権を取得するには、NetBackup のシステム管理者にお問い合わせください。
- ジョブ階層表示で開くことができるタブの数が NetBackup で制限されている。
  親ジョブを展開できず、子ジョブを表示できない場合は、開いている他のジョブのタブを閉じてください。

3

通知

この章では以下の項目について説明しています。

ジョブの通知

NetBackup のジョブには、次の種類の電子メール通知を利用できます。

- ジョブが失敗した場合の通知。NetBackup は、チケット作成のための受信電子メールサービスを使用する、チケットシステムをサポートします。
  p.37 の「ジョブエラーの電子メール通知の送信」を参照してください。
- 0 (ゼロ) 以外の状態のバックアップについてバックアップ管理者に送信される通知。
  p.40 の「失敗したバックアップについてのバックアップ管理者への通知の送信」を参照してください。
- 特定のホストのバックアップ (正常に完了したバックアップと失敗したバックアップ) についてホスト管理者に送信される通知。
  p.41 の「バックアップについてホスト管理者に通知を送信する」を参照してください。

ジョブエラーの電子メール通知の送信

ジョブでエラー発生したときに電子メール通知を送信するように NetBackup を構成できます。これにより管理者は、NetBackup のジョブの失敗を監視したり、手動でチケットを作成して問題を追跡するなどに費やす時間を削減できます。NetBackup は、受信電子メールサービスを使用してチケットを作成するチケットシステムをサポートします。

p.39 の「アラートを生成する状態コード」を参照してください。

NetBackup は、特定のジョブエラー条件、または NetBackup の状態コードに基づいてアラートを生成します。類似したアラート、またはエラーの原因が類似しているアラートは、重複としてマークされます。重複アラートの電子メール通知は、その後の 24 時間は送信

されません。通知を送信できない場合、NetBackup は 2 時間ごとに最大 3 回まで送信を再試行します。

アラートの設定に変更が加えられた場合、またはアラートを生成できない場合や電子メール通知を送信できない場合には、NetBackup がイベントを監査します。p.119 の「NetBackup の監査について」を参照してください。

前提条件

チケットシステムを使用して電子メール通知を設定する前に、次の要件を確認してください。

- チケットシステムが起動し、実行中である。
- SMTP サーバーが起動し、実行中である。
- NetBackup が送信する受信電子メールに基づいてチケット (またはインシデント) を作成するために、チケットシステムでポリシーが構成されている。

電子メール通知を設定するには

1. 右上で、[設定 (Settings)]、[電子メール通知 (Email notifications)]の順にクリックします。
2. [電子メール通知 (Email notifications)]タブにアクセスします。
3. [電子メール通知を送信する (Send Email Notification)]を選択します。
4. 受信者の電子メールアドレス、送信者の電子メールアドレス、電子メールの送信者の名前など、電子メールの情報を入力します。
5. SMTP サーバー名やポート番号などの、SMTP サーバーの詳細を入力します。

   SMTP サーバーで以前にクレデンシャルを指定した場合は、SMTP ユーザー名とパスワードを指定します。
6. [保存 (Save)]をクリックします。
7. チケットシステムにログオンして、NetBackup のアラートに基づいて生成されたチケットを表示します。

電子メール通知からの特定の状態コードの除外

特定の状態コードを除外して、これらのエラーでは電子メール通知が送信されないようにできます。

特定の状態コードを除外するには

1. 右上で、[設定 (Settings)]、[電子メール通知 (Email notifications)]の順にクリックします。
2. [状態コードを除外 (Exclude status codes)]を見つけます。

3 電子メール通知を受信しない状態コードまたは状態コードの範囲 (カンマ区切り) を入力します。

4 [保存 (Save)]をクリックします。

アラートの電子メール通知の例

アラートの電子メール通知には、プライマリサーバー、ジョブ、ポリシー、スケジュール、エラーについての情報が含まれています。ジョブの種類に基づいて、電子メールにその他の情報が含まる場合があります。たとえば、VMware ジョブのエラーの場合、vCenter Server や ESX ホストなどの詳細が電子メール通知に含まれます。

電子メール通知の例:

```
Primary Server: primary1.example.com

Client Name: client1.example.com

Job ID: 50

Job Start Time: 2018-05-17 14:43:52.0

Job End Time: 2018-05-17 15:01:27.0

Job Type: BACKUP

Parent Job ID: 49

Policy Name: Win_policy

Policy Type: WINDOWS_NT

Schedule Name: schedule1

Schedule Type: FULL

Status Code: 2074

Error Message: Disk volume is down
```

アラートを生成する状態コード

NetBackup Web UI は、VMware ジョブのエラーに対するアラートをサポートして 90 日間保持します。NetBackup は、バックアップ、スナップショット、スナップショットレプリケーション、スナップショットからのインデックス、スナップショットからのバックアップのジョブの種類に対してサポート対象の状態コードのアラートを生成します。アラートが生成される状態コードの完全なリストについては、『NetBackup 状態コードリファレンスガイド』で、アラート通知の状態コードに関する情報を参照してください。

表 3-1に、アラートが生成される条件または状態コードの一部を示します。これらのアラートは、電子メール通知を通じてチケットシステムに送信されます。

表 3-1 アラートを生成する状態コードの例

状態コード	エラーメッセージ
10	割り当てに失敗しました (allocation failed)
196	バックアップ処理時間帯でないため、クライアントバックアップが試行されませんでした (client backup was not attempted because backup window closed)
213	利用可能なストレージユニットがありません (no storage units available for use)
219	必要なストレージユニットが利用できません (the required storage unit is unavailable)
2001	利用可能なドライブがありません
2074	ディスクボリュームが停止しています (Disk Volume is Down)
2505	データベースに接続できません。
4200	操作に失敗しました: スナップショットのロックを獲得できません。
5449	スクリプトが実行を承認されていません。
7625	SSL ソケット接続に失敗しました。

失敗したバックアップについてのバックアップ管理者への通知の送信

0 (ゼロ) 以外の状態のバックアップについてバックアップ管理者に通知を送信できます。

UNIX の場合、NetBackup では、メール転送エージェント sendmail を使用して電子メール通知が送信されます。Windows の場合、NetBackup では、SMTP を使用してメッセージを転送するアプリケーションがインストールされ、通知を送信する Windows ホストで `nbmail.cmd` スクリプトが構成されている必要があります。

p.41 の「Windows ホストでの nbmail.cmd スクリプトの構成」を参照してください。

NetBackup ホストのバックアップ管理者の通知を構成するには、次のトピックを参照してください。

p.41 の「バックアップについてホスト管理者に通知を送信する」を参照してください。

失敗したバックアップについてバックアップ管理者に通知を送信するには

1. 左側で、[ホスト (Host)]、[ホストプロパティ (Host Properties)]の順に選択します。
2. ホストを選択し、[接続 (Connect)]をクリックします。
3. [プライマリサーバーの編集 (Edit primary server)]をクリックします。
4. [グローバル属性 (Global attributes)]をクリックします。

5 管理者の電子メールアドレスを入力します。(複数のアドレスはカンマで区切ります。)

6 [保存 (Save)]をクリックします。

バックアップについてホスト管理者に通知を送信する

特定のホストの正常に完了および失敗したバックアップについてホスト管理者に通知を送信できます。

UNIX の場合、NetBackup では、メール転送エージェント sendmail を使用して電子メール通知が送信されます。Windows では、SMTP でメッセージを転送するアプリケーションがインストールされている必要があります。また、通知を送信する Windows ホストで nbmail.cmd スクリプトを構成する必要があります。

p.41 の「Windows ホストでの nbmail.cmd スクリプトの構成」を参照してください。

特定のホストのバックアップの通知を送信するには

1 左側で、[ホスト (Host)]、[ホストプロパティ (Host Properties)]の順に選択します。

2 ホストを選択し、[接続 (Connect)]をクリックします。

3 [クライアントの編集 (Edit client)]をクリックします。

4 [ユニバーサル設定 (Universal settings)]をクリックします。

5 電子メール通知の送信方法を選択します。

- クライアントから電子メール通知を送信するには、[クライアントが電子メールを送信する (Client sends email)]を選択します。
- サーバーから電子メール通知を送信するには、[サーバーが電子メールを送信する (Server sends email)]を選択します。

6 ホスト管理者の電子メールアドレスを入力します。(複数のアドレスはカンマで区切ります。)

7 [保存 (Save)]をクリックします。

Windows ホストでの nbmail.cmd スクリプトの構成

バックアップについての電子メール通知を送受信する Windows ホストの場合、該当するホストで nbmail.cmd スクリプトを構成する必要があります。

Windows ホストで nbmail.cmd スクリプトを構成するには

1 nbmail.cmd のバックアップコピーを作成します。

2 プライマリサーバーで、次のスクリプトを見つけます。

install_path¥NetBackup¥bin¥goodies¥nbmail.cmd

3 該当するホストの次のディレクトリにスクリプトをコピーします。

install_path¥NetBackup¥bin¥

プライマリサーバーとメディアサーバー　次の設定を構成すると、NetBackup はサーバーから通知を送信します。

- グローバル属性の管理者の電子メールアドレス。
- [ユニバーサル設定 (Universal Settings)]の[サーバーが電子メールを送信する (Server sends email)]オプション。

クライアント　次の設定を構成すると、NetBackup はクライアントから通知を送信します。

- [ユニバーサル設定 (Universal Settings)]の[クライアントが電子メールを送信する (Client sends email)]オプション。

4 テキストエディタを使用して nbmail.cmd を開きます。

次のオプションがスクリプトで使われます。

-s　電子メールの件名の行です。

-t　電子メールの受信者を表します。

-i　電子メールのオリジネータです。メールサーバーに登録されている必要はありません。デフォルト (-i Netbackup) は、電子メールが NetBackup からのものであることを示します。

-server　電子メールを受け取り、中継するように構成されている SMTP サーバーの名前です。

-q　すべての出力を画面に表示しません。

5 行を次のように調整します。

- BLAT の実行に必要なセクションを有効にするには、5 行のそれぞれから @REM を削除します。
- SERVER_1 をメールサーバーの名前に置き換えます。次に例を示します。

```
@IF "%~4"=="" (
blat %3 -s %2 -t %1 -i Netbackup -server emailserver.company.com -q
) ELSE (
blat %3 -s %2 -t %1 -i Netbackup -server emailserver.company.com -q -attach %4
)
```

6 nbmail.cmd を保存します。

NetBackup イベント通知

NetBackup 管理者が重要なシステムイベントを認識できるように、NetBackup はシステムログを定期的に問い合わせて、イベントに関する通知を表示します。

メモ: これらの通知にはジョブイベントは含まれません。ジョブイベントについて詳しくは、アクティビティモニターのジョブの詳細を参照してください。

[通知 (Notifications)]アイコンは、Web UI の右上にあります。アイコンをクリックすると、[通知 (Notifications)]ウィンドウが開き、重要な通知のリストが一度に 10 件ずつ表示されます。数字がアイコンとともに表示される場合は、未読の重要なメッセージの数を示しています。ウィンドウを開くと、この数はリセットされます。

このウィンドウでは、すべての通知の包括的なリストを表示することもできます。各イベントには、NetBackup コンポーネントまたは外部コンポーネントのカテゴリがあり、次の重大度レベルが割り当てられます。

- エラー (Error)
- 重要 (Critical)
- 警告 (Warning)
- 情報 (Information)
- デバッグ (Debug)
- 通知 (Notice)

リストのソート、フィルタ処理、検索が可能です。包括的なリストでは、各イベントの詳細を確認することもできます。詳細には、詳細な説明と該当する拡張属性が含まれます。

NetBackup Messaging Broker (`nbmqbroker`) が実行されていない場合、NetBackup 通知は利用できません。このサービスの再起動について詳しくは、『NetBackup トラブルシューティングガイド』を参照してください。

通知の表示

通知を表示するには

1 右上にある［通知 (Notifications)］アイコンをクリックすると、重要な通知のリストが一度に 10 件ずつ表示されます。

メモ: 数字がアイコンとともに表示される場合は、未読の重要なメッセージの数を示しています。［通知 (Notifications)］ウィンドウを開くと、この数はリセットされます。

次の 10 件の通知を表示するには、［次の 10 件をロード (Load 10 more)］をクリックします。30 件の通知を表示した後、［すべて表示 (Show all)］をクリックすると、残りのメッセージが表示されます。

最新の通知を再びロードするには、［更新 (Refresh)］を使用します。

2 すべての通知を表示するには、［すべて表示 (Show all)］をクリックして、［イベント (Events)］ページを開きます。このページでは、次の操作を実行できます。

- 詳細を表示するには、イベントをクリックします。詳細には、詳細な説明と拡張属性が含まれます。
- リストを並び替えるには、［説明 (Description)］以外の列見出しをクリックします。イベントは、デフォルトでは受信日で並び替えられます。
- イベントをフィルタ処理するには、［フィルタ (Filter)］をクリックします。［重大度 (Severity)］と［時間枠 (Timeframe)］でフィルタ処理できます。
  ［フィルタ (Filters)］メニューで、フィルタ処理に使用するパラメータ値を選択し、［フィルタを適用する (Apply filters)］をクリックします。
  すべてのフィルタを解除するには、［すべて消去 (Clear All)］をクリックします。
- イベントを検索するには、［検索 (Search)］フィールドに検索文字列を入力します。［説明 (Description)］と［受信済み (Received)］を除くすべての列の値を検索できます。

Web UI での NetBackup イベント通知の変更または無効化

Web UI に表示される特定の種類の NetBackup イベント通知を無効にしたり、NetBackup プライマリサーバー上の `eventlog` ファイルを辺境して重大度と優先度を変更したりできます。

- Windows の場合:
  install_path¥var¥global¥wmc¥h2Stores¥notifications¥properties
- UNIX の場合:
  /usr/openv/var/global/wmc/h2Stores/notifications/properties

イベント通知を無効にするには

◆ 次のいずれかの形式で、eventlog.properties ファイルに DISABLE エントリを追加します。

DISABLE.*NotificationType* = true

または DISABLE.*NotificationType.Action* = true

または DISABLE.*namespace*

有効な *NotificationType* と *Action* の値については、次のトピックを参照してください。

p.46 の 表 3-2 を参照してください。

次に例を示します。

- すべてのストレージユニットイベントの通知を無効にするには:
  DISABLE.StorageUnit = true
- ストレージユニットの作成イベントの通知のみを無効にするには:
  DISABLE.StorageUnit.CREATE = true
- 名前空間を使用してストレージユニットの更新イベントの通知のみを無効にするには:
  DISABLE.eventlog.vrts.nbu.emm.storageunit.update = true

イベント通知の優先度または重大度を変更するには

◆ 次のいずれかの形式で、eventlog.properties ファイルにエントリを追加または変更します。

NotificationType.Action.priority = value

または *NotificationType.Action.severity = value*

priority の有効な値: LOW, MEDIUM, HIGH

severity の有効な値: CRITICAL, ERROR, WARNING, INFO, DEBUG

次に例を示します。

- ストレージユニットの作成イベントの優先度と重大度を設定するには:

```
StorageUnit.CREATE.priority = LOW
StorageUnit.CREATE.severity = INFO
```

メモ: 対応する処理の実行後に、ポリシー、SLP、カタログの種類のイベントが生成されるには、最大 1 分かかることがあります。

表 3-2 通知でサポートされる NetBackup イベントの種類

イベントと通知の種類の値	処理	重大度	通知メッセージの例
ポリシー `Policy` **メモ:** 可能な場合は、2 つ以上のポリシー処理の集計ポリシーイベントが作成されます。	作成 (Create)	情報	ポリシー *{Policy_Name}* が作成されました。 ポリシーのイベントを受信しました。追加の詳細情報は見つかりませんでした。
	更新 (Update)	情報または重大	ポリシー *{Policy_Name}* が有効になりました。 ポリシー *{Policy_Name}* が無効になりました。 ポリシー *{Policy_Name}* が更新されました。 クライアント *{Policy_Name}* がポリシー ${policyName} に追加されました。 クライアント *{Policy_Name}* がポリシー *{Policy_Name}* から削除されました。 スケジュール *{Policy_Name}* がポリシー *${Policy_Name}* に追加されました。 スケジュール *{Policy_Name}* がポリシー *{Policy_Name}* から削除されました。
	削除 (Delete)	重大	ポリシー *{Policy_Name}* が削除されました。
クライアント `ClientEvent`	作成 (CREATE)	情報	クライアント *{Client_Name}* が作成されました。
	削除 (DELETE)	重大	クライアント *{Client_Name}* が削除されました。
	更新 (UPDATE)	情報	クライアント *{Client_Name}* が更新されました。

イベントと通知の種類の値	処理	重大度	通知メッセージの例
ストレージユニット StorageUnit **メモ:** 追加、削除、変更など、基本的なディスクステージングスケジュール (DSSU) に変更を加えると、関連するストレージユニット通知が生成されます。これらの通知によって、ポリシー名 __DSSU_POLICY_{*Storage_Unit_Name*} を使用して、いくつかの追加のポリシー通知も生成されます。	作成 (CREATE)	情報	ストレージユニット *{Storage_Unit_Name}* が作成されました。
	削除 (DELETE)	重大	ストレージユニット *{Storage_Unit_Name}* が削除されました。
	更新 (UPDATE)	情報	ストレージユニット *{Storage_Unit_Name}* が更新されました。
ストレージユニットグループ StorageUnitGroup	作成 (CREATE)	情報	ストレージユニットグループ *{Storage_Unit_Group_Name}* が作成されました。
	削除 (DELETE)	重大	ストレージユニットグループ *{Storage_Unit_Group_Name}* が削除されました。
	更新 (UPDATE)	情報	ストレージユニットグループ *{Storage_Unit_Group_Name}* が更新されました。
	更新 (UPDATE)	情報	ストレージサービス *{Storage_Service_Name}* が更新されました。
ストレージライフサイクルポリシー SLP	作成 (Create)	情報	ストレージライフサイクルポリシーのイベントを受信しました。追加の詳細情報は見つかりませんでした。 ストレージライフサイクルポリシー *{Policy_Name}* が作成されました。
	削除 (Delete)	重大	ストレージライフサイクルポリシー *{Policy_Name}* が削除されました。 バージョン *Version_Number* のストレージライフサイクルポリシー *{Policy_Name}* が削除されました。
ストレージライフサイクルポリシーの状態変更 SlpVersionActInactEvent	更新 (UPDATE)	情報	SLP バージョン *{Version}* が変更されました。

イベントと通知の種類の値	処理	重大度	通知メッセージの例
cDOT クライアント cDOTClientEvent	作成 (CREATE)	情報	*{Cluster_Data_ONTAP_Client_Name}* は cDOT クライアントとして追加されました。
	削除 (DELETE)	重大	*{Cluster_Data_ONTAP_Client_Name}* は cDOT クライアントとして削除されました。
Isilon クライアント IsilonClientEvent	作成 (CREATE)	情報	*{Isilon_Filer_Client_Name}* が Isilon クライアントとして追加されました。
	削除 (DELETE)	重大	*{Isilon_Filer_Client_Name}* が Isilon クライアントとして削除されました。
マシン [プライマリ/メディア/クラスタ] Machine	作成 (CREATE)	情報	ホスト *{Host_Name}* が作成されました。
	削除 (DELETE)	重大	ホスト *{Host_Name}* が削除されました。
ドライブ DriveChange	作成 (CREATE)	情報	ドライブ *{Drive_Name}* がホスト *{Host_Name}* に対して作成されました。
	削除 (DELETE)	重大	ホスト *{Host_Name}* のドライブ *{Drive_Name}* が削除されました。
	更新 (UPDATE)	情報	ホスト *{Host_Name}* のドライブ *{Drive_Name}* が更新されました。 **メモ:** このような通知メッセージは、特定のホストのドライブが更新されたとき、またはドライブの状態が起動 (UP) または停止 (DOWN) に変更されたときに生成されます。
ライブラリイベント - ロボット Library	作成 (CREATE)	情報	ホスト *{Host_Name}* のライブラリ *{Library_Name}* が作成されました。
	削除 (DELETE)	重大	ホスト *{Host_Name}* のライブラリ *{Library_Name}* が削除されました。
	更新 (UPDATE)	情報	ホスト *{Host_Name}* のライブラリ *{Library_Name}* が更新されました。
メディア Media	作成 (CREATE)	情報	メディア *{Media_ID}* が作成されました。
	削除 (DELETE)	重大	メディア *{Media_ID}* が削除されました。

イベントと通知の種類の値	処理	重大度	通知メッセージの例
	更新 (UPDATE)	情報	メディア *{Media_ID}* が更新されました。
メディアグループ MediaGroup	作成 (CREATE)	情報	メディアグループ *{Media_Group_ID}* が作成されました。
	削除 (DELETE)	重大	メディアグループ *{Media_Group_ID}* が削除されました。
	更新 (UPDATE)	情報	メディアグループ *{Media_Group_ID}* が更新されました。
メディアプール MediaPool	作成 (CREATE)	情報	メディアプール *{Media_Pool_ID}* が作成されました。
	削除 (DELETE)	重大	メディアプール *{Media_Pool_ID}* が削除されました。
	更新 (UPDATE)	情報	メディアプール *{Media_Pool_ID}* が更新されました。
保持イベント RetentionEvent	更新 (UPDATE)	情報	保持レベルが変更されました。
VMware 検出 TAGSDISCOVERYEVENT	処理なし	情報	VMware タグを取得できません。
自動検出と今すぐ検出 AutoDiscoveryEvent	処理なし	情報	VMware、RHV、またはクラウドサーバーに対して自動検出処理または今すぐ検出処理が実行されると、適切な通知が生成されます。
	処理なし	重大	**メモ:** VMware、RHV、Nutanix、またはクラウドサーバーに対して自動検出処理または今すぐ検出処理が失敗すると、適切な通知が生成されます。 **メモ:** VMware、RHV、またはクラウドサーバーに対して自動検出処理または今すぐ検出処理が失敗すると、適切な通知が生成されます。
KMS 証明書の有効期限 KMSCredentialStatus	有効期限	警告	KMS サーバー *{KMS_Server_Name}*${server} との通信に使用される証明書があと *{days_to_expiration}* 日で期限切れになります。証明書が期限内に更新されないと、KMS サーバーとの通信に失敗します。

イベントと通知の種類の値	処理	重大度	通知メッセージの例
Message Broker サービスの状態 `ServiceStatus`	実行中	情報	NetBackup Messaging Broker サービスが実行中です。NetBackup の内部通知が有効になりました。
	停止	情報	NetBackup Messaging Broker サービスが停止されました。NetBackup の内部通知が無効になりました。
保護計画 `ProtectionPlan`	作成 (Create)	情報	保護計画のイベントを受信しました。 保護計画 *Protection_Plan_Name* が作成されます。 保護計画 *Protection_Plan_Name* が既存の NetBackup ポリシーから作成されます。
	更新 (Update)	情報	保護計画 *Protection_Plan_Name* が更新されます。
	削除 (Delete)	重大	保護計画 *Protection_Plan_Name* が削除されます。
保護計画のサブスクリプション `ProtectionPlanSubscription`	作成 (Create)	情報	保護計画のサブスクリプションのイベントを受信しました。 *Asset_ClassAsset_Display_Name* が、保護計画 *Protection_Plan_Name* にサブスクライブされます。
	更新 (Update)	情報	保護計画 *Protection_Plan_Name* の *Asset_ClassAsset_Display_Name* のサブスクリプションが更新されます。
	削除 (Delete)	重大	*Asset_ClassAsset_Display_Name* が、保護計画 *Protection_Plan_Name* からサブスクライブ解除されます。
カタログイメージの有効期限 `Catalog` **メモ:** 手動でイメージを期限切れにする場合も該当します。	該当なし	重大	カタログイメージのイベントを受信しました。追加の詳細情報は見つかりませんでした。 カタログイメージ *Image_Name* が変更されました。 カタログイメージ *Image_Name* が期限切れになりました。
使用状況レポート `UsageReportingEvent`	処理なし	情報またはエラー	使用状況レポートの生成が開始されました。 使用状況レポートが正常に生成されました。 使用状況レポートの生成に失敗しました。詳しくは、親ディレクトリの収集ログとレポートログを参照してください。

自動通知クリーンアップタスクの構成について

デフォルトでは、NetBackup ではイベント通知クリーンアップタスクが 4 時間ごとに実行されます。最大 10,000 件のイベントレコードがイベントデータベースで最大 3 日間保存されます。クリーンアップタスクを実行すると、NetBackup によってデータベースから古い通知が削除されます。

クリーンアップタスクの実行間隔、一度に保持されるイベントレコードの数、レコードの保持日数を変更できます。

コマンドラインから、bpsetconfig または bpgetconfig を使用して、「表 3-3」に一覧表示されているパラメータ値を変更します。これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

パラメータ値は、次の API を使用して変更することもできます。

- GET/config/hosts/{hostId}/configurations
- POST/config/hosts/{hostId}/configurations
- GET/config/hosts/{hostId}/configurations/configurationName (特定のプロパティの場合)
- PUT/config/hosts/{hostId}/configurations/configurationName
- DELETE/config/hosts/{hostId}/configurations/configurationName

これらの API について詳しくは、SORT で「NetBackup 10.1 API リファレンス」を参照してください。

表 3-3　　自動通知クリーンアップタスクの構成可能なパラメータ

パラメータと説明	最小値	デフォルト値	最大値
EVENT_LOG_NOTIFICATIONS_COUNT 保存されるレコードの最大数。その後クリーンアップ処理によって最も古いレコードが削除され、保持値が上書きされます。	1000	10000	100000
EVENT_LOG_NOTIFICATIONS_RETENTION_IN_HOURS データベースにイベントが保存される時間数。	24 (時間)	72 (時間)	168 (時間)
EVENT_LOG_NOTIFICATIONS_CLEANUP_INTERVAL_IN_HOURS イベントクリーンアップサービスが実行される間隔。	1 (時間)	4 (時間)	24 (時間)

2

ホストの構成

4

ホストプロパティの管理

この章では以下の項目について説明しています。

ホストプロパティの概要

[ホストプロパティ(Host Properties)]の構成オプションを使用することで、管理者は特定のサイトの作業環境や要件を満たすために NetBackup をカスタマイズできます。

他のクライアントまたはサーバーのプロパティを変更するには、サインインした NetBackup サーバーが、他のシステムの[サーバー (Servers)]リストに含まれている必要があります。

たとえば、NetBackup 管理コンソールを使用して *server_1* にサインインし、*client_2* の設定を変更する場合は、

一部のオプションは、NetBackup Web UI では構成できません。

client_2 の[サーバー (Servers)]リストには *server_1* が含まれる必要があります。

サーバーまたはクライアントのホストプロパティの表示または編集

[ホストプロパティ(Host Properties)]の構成オプションを使用することで、管理者は特定のサイトの作業環境や要件を満たすために NetBackup をカスタマイズできます。
NetBackup Web UI には、NetBackup プライマリサーバー、メディアサーバー、クライアントのプロパティが表示されます。

メモ: クラスタ環境では、クラスタの各ノードでホストプロパティを個別に変更する必要があります。

プライマリサーバーのホストプロパティの表示または編集

プライマリサーバーのホストプロパティを表示または編集するには

1. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。
2. 左上のリストから[プライマリサーバー (Primary server)]を選択します。
3. プライマリサーバーを選択して[接続 (Connect)]をクリックします。
4. [プライマリサーバーの編集 (Edit primary server)]をクリックします。
5. 必要な変更を加えます。次に、[保存 (Save)]をクリックします。

メディアサーバーのホストプロパティの表示または編集

メディアサーバーのホストプロパティを表示または編集するには

1. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。
2. 左上のリストから[メディアサーバー (Media server)]を選択します。
3. メディアサーバーを選択して[接続 (Connect)]をクリックします。
4. [メディアサーバーの編集 (Edit media server)]をクリックします。
5. 必要な変更を加えます。次に、[保存 (Save)]をクリックします。

クライアントのホストプロパティの表示または編集

クライアントのホストプロパティを表示または編集するには

1. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。
2. 左上のリストから[クライアントサーバー (Client server)]を選択します。
3. クライアントを選択し、[接続 (Connect)]をクリックします。
4. [クライアントの編集 (Edit client)]をクリックします。
5. 必要な変更を加えます。次に、[保存 (Save)]をクリックします。

ホストの属性のリセット

場合によっては、ホストとの通信が正常に実行できるようにするために、ホストの属性をリセットする必要があります。リセットが最も行われるのは、ホストが NetBackup の 8.0 以前のバージョンにダウングレードされた場合です。ダウングレード後は、クライアントの通信

状態が引き続きセキュアモードに設定されているため、プライマリサーバーはクライアントと通信できません。リセットすると、安全でないモードを反映するように、通信状態が更新されます。

ホストの属性をリセットする場合:

- NetBackup は、ホスト名のマッピング情報、ホストの通信状態などのホスト ID をリセットします。ホストのホスト ID、ホスト名、またはセキュリティ証明書はリセットされません。
- 接続の状態は、安全でない状態に設定されます。次にプライマリサーバーがホストと通信する際は、接続の状態が適切に更新されます。

ホストの属性をリセットするには

1. 左側で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に選択します。
2. ホストを特定し、[処理 (Actions)]、[属性のリセット (Reset attributes)]をクリックします。
3. 8.0 以前のホストと安全でない通信を行う場合に選択します。

   [グローバルセキュリティ設定 (Global Security Settings)]で、[NetBackup 8.0 以前のホストとの通信を許可する (Allow communication with 8.0 and earlier hosts)]オプションを有効にすると、NetBackup は、8.0 以前のホストと通信できます。デフォルトではこのオプションは有効です。

メモ: ホストの属性を誤ってリセットした場合は、bpcd サービスを再起動して変更を元に戻せます。それ以外の場合は、24 時間後にホスト属性が適切な値で自動的に更新されます。

5

作業負荷および NetBackup がアクセスするシステムのクレデンシャルの管理

この章では以下の項目について説明しています。

NetBackup でのクレデンシャル管理の概要

クレデンシャル管理を使用すると、NetBackup が、保護対象のシステムと作業負荷へのアクセスに使用するクレデンシャルを一元管理できます。

次の作業負荷のクレデンシャルを管理できます。

- AHV
- Cassandra
- クラウド (クラウドインスタンスの場合)

- クラウドオブジェクトストア
- Kubernetes
- Microsoft SQL Server
- MySQL Server
- Oracle
- PaaS データベース
- PostgreSQL サーバー
- SaaS

次のシステムについてもクレデンシャルを管理できます。

- コールホームプロキシサーバー
- ディスクアレイ
- 外部のキーマネージメントサービス (KMS)
- マルウェアの検出 (マルウェアスキャンホスト)
- NDMP

詳細情報

p.59 の「NetBackup コールホームプロキシ用のクレデンシャルの追加」を参照してください。

p.58 の「外部 KMS 用のクレデンシャルの追加」を参照してください。

p.61 の「ネットワークデータ管理プロトコル (NDMP) 用のクレデンシャルの追加」を参照してください。

コールホームプロキシサーバーについて詳しくは、『Veritas Usage Insights スタートガイド』参照してください。

作業負荷 (SQL Server など) のクレデンシャルの構成について詳しくは、対象の作業負荷のガイドを参照してください。

NetBackup でのクレデンシャルの追加

[クレデンシャルの管理 (Credential management)] ノードを使用して、NetBackup がシステムまたは作業負荷への接続に使用するクレデンシャルを追加できます。

- p.59 の「NetBackup コールホームプロキシ用のクレデンシャルの追加」を参照してください。
- p.58 の「外部 KMS 用のクレデンシャルの追加」を参照してください。

- p.61 の「ネットワークデータ管理プロトコル (NDMP) 用のクレデンシャルの追加」を参照してください。

SQL Server、クラウド、Kubernetes、その他の作業負荷について詳しくは、対応する作業負荷のガイドを参照してください。

NetBackup のマニュアルのポータル

外部 KMS 用のクレデンシャルの追加

この種類のクレデンシャルにより、構成した外部 KMS サーバーにアクセスできます。

外部 KMS 用のクレデンシャルを追加するには

1. 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
2. [指定したクレデンシャル (Named credentials)]タブで[追加 (Add)]をクリックし、次のプロパティを指定します。
   - クレデンシャル名 (Credential name)
   - タグ (Tag)
   - 説明 (Description) (例:「このクレデンシャルは外部 KMS へのアクセスに使用」)
3. [次へ (Next)]をクリックします。
4. [外部 KMS (External KMS)]を選択します。
5. 認証に必要なクレデンシャルの詳細を入力します。

   この詳細は、NetBackup プライマリサーバーと外部 KMS サーバー間の通信の認証に使用されます。
   - 証明書 - 証明書ファイルの内容を指定します。
   - 秘密鍵 - 秘密鍵ファイルの内容を指定します。
   - CA 証明書 - CA 証明書ファイルの内容を指定します。
   - パスフレーズ - 秘密鍵ファイルのパスフレーズを入力します。
   - CRL 確認レベル - 外部 KMS サーバー証明書の失効の確認レベルを選択します。
     CHAIN - CRL で証明書チェーンの証明書すべての失効状態が検証されます。
     DISABLE - 失効の確認を無効にします。ホストとの通信時に、CRL で証明書の失効状態は検証されません。
     LEAF - CRL でリーフ証明書の失効状態が検証されます。

   外部 KMS 構成について詳しくは、『NetBackup セキュリティと暗号化ガイド』を参照してください。
6. [次へ (Next)]をクリックします。

7 クレデンシャルへのアクセス権を付与する役割を追加します。

- ［追加 (Add)］をクリックします。
- 役割を選択します。
- 役割に付与するクレデンシャル権限を選択します。

8 ［次へ (Next)］をクリックし、プロンプトに従ってウィザードを完了します。

NetBackup コールホームプロキシ用のクレデンシャルの追加

この種類のクレデンシャルは、NetBackup Product Improvement Program と Usage Insights の両方が使用するプロキシサーバー構成を実現します。

NetBackup コールホームプロキシ用のクレデンシャルを追加するには

1 左側の［クレデンシャルの管理 (Credential management)］をクリックします。

2 ［指定したクレデンシャル (Named credentials)］タブで［追加 (Add)］をクリックし、次のプロパティを指定します。

- クレデンシャル名 (Credential name)
- タグ (Tag)
- 説明 (Description)

3 ［次へ (Next)］をクリックします。

4 ［コールホームプロキシ (Callhome proxy)］を選択します。

5 認証に必要なクレデンシャルの詳細を入力し、［次へ (Next)］をクリックします。

6 クレデンシャルへのアクセス権を付与する役割を追加します。

- ［追加 (Add)］をクリックします。
- 役割を選択します。
- 役割に付与するクレデンシャル権限を選択します。

7 ［次へ (Next)］をクリックし、プロンプトに従ってウィザードを完了します。

8 クレデンシャルを作成した後、CALLHOME_PROXY_NAME のエントリについて NetBackup の構成を更新する必要があります。CALLHOME_PROXY_NAME をクレデンシャル名に設定します。プライマリサーバーで次のコマンドを使用します。

```
echo CALLHOME_PROXY_NAME = CredentialName |bpsetconfig.exe
```

指定したクレデンシャルの編集または削除

指定したクレデンシャルのプロパティを編集したり、指定したクレデンシャルをNetBackupの[クレデンシャルの管理 (Credential management)]から削除できます。

指定したクレデンシャルの編集

指定したクレデンシャルのタグ、説明、カテゴリ、認証に関する詳細、または権限を変更したい場合はこれを編集できます。クレデンシャル名は変更できません。

指定したクレデンシャルを編集するには

1. 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
2. [指定したクレデンシャル (Named credentials)]タブで、編集するクレデンシャルを特定してクリックします。
3. 必要に応じて、[編集 (Edit)]をクリックしてクレデンシャルを更新します。
4. 変更内容を確認して[完了 (Finish)]をクリックします。
5. (該当する場合) インスタンスのエージェントレス接続を使用するクラウド作業負荷の場合は、クレデンシャルの編集後、[接続 (Connect)]ボタンをクリックしてインスタンスに再接続します。

指定したクレデンシャルの削除

NetBackup で不要になった、指定したクレデンシャルは削除できます。削除するクレデンシャルを使用する資産がある場合は、それらの資産に別のクレデンシャルを適用してください。そうしないと、それらの資産のバックアップとリストアが失敗する可能性があります。

指定したクレデンシャルを削除するには

1. 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
2. [指定したクレデンシャル (Named credentials)]タブで、削除するクレデンシャルを特定してクリックします。
3. [削除 (Delete)]をクリックします。
4. (該当する場合) 削除したクレデンシャルがプロキシのクレデンシャルの場合は、CALLHOME_PROXY_NAME エンティティを削除する必要があります。プライマリサーバーで次のコマンドを使用して、CALLHOME_PROXY_NAME エンティティを削除します。

   ```
   echo CALLHOME_PROXY_NAME |bpsetconfig.exe
   ```

ネットワークデータ管理プロトコル (NDMP) 用のクレデンシャルの追加

NetBackup がネットワークデータ管理プロトコル (NDMP) への接続に使用するクレデンシャルを追加できます。

NDMP クレデンシャルについて詳しくは、『NetBackup for NDMP 管理者ガイド』を参照してください。

NDMP クレデンシャルを追加するには

1. 左側の［クレデンシャルの管理 (Credential management)］をクリックします。
2. ［クライアントのクレデンシャル (Client credentials)］タブをクリックします。
3. ［追加 (Add)］をクリックします。
4. ［NDMP ホストの追加 (Add NDMP Host)］画面で、NDMP ホスト名を入力し、ラジオボタンからホストクレデンシャルの形式を選択します。
   - ［すべてのメディアサーバーに対してこの NDMP ホストの次のクレデンシャルを使用する (Use the following credentials for this NDMP host on all media servers)］ - このオプションは、すべてのメディアサーバーに対して同じクレデンシャルを使用します。
   - ［各メディアサーバー上のこの NDMP ホストには、個別のクレデンシャルを使用する (Use different credentials for this NDMP host on each media server)］ - このオプションを選択すると、メディアサーバーごとに一意のクレデンシャルを入力できます。各メディアサーバーのクレデンシャルを入力した後、［追加 (Add)］をクリックします。
5. ［追加 (Add)］をクリックします。

NetBackup でのネットワークデータ管理プロトコル (NDMP) クレデンシャルの編集または削除

ネットワークデータ管理プロトコル (NDMP) を使用するメディアサーバーのクレデンシャルを編集または削除できます。

NDMP クレデンシャルについて詳しくは、『NetBackup for NDMP 管理者ガイド』を参照してください。

NDMP クレデンシャルの編集

NDMP クレデンシャルを編集するには

1. 左側の［クレデンシャルの管理 (Credential management)］をクリックします。
2. ［クライアントのクレデンシャル (Client credentials)］タブをクリックします。

3 ホストを見つけます。[編集 (Edit)]をクリックします。

4 必要に応じて変更を加え、[保存 (Save)]をクリックします。

NDMP クレデンシャルの削除

NDMP クレデンシャルを削除するには

1 左側の[クレデンシャルの管理 (Credential management)]をクリックします。

2 [クライアントのクレデンシャル (Client credentials)]タブをクリックします。

3 1 つ以上のホストを選択します。次に、[削除 (Delete)]、[削除 (Delete)]の順にクリックします。

6

配備の管理

この章では以下の項目について説明しています。

NetBackup パッケージリポジトリの管理

NetBackup パッケージリポジトリは、NetBackup パッケージを一元的に追加および削除するための場所です。パッケージを使用すると、NetBackup のアップグレードや、NetBackup 環境での Emergency Engineering Binary の配備を行えます。

インターフェースで、パッケージは NetBackup のバージョン番号で整列されます。NetBackup の特定のバージョンには、複数の子パッケージ (サポート対象プラットフォームにつき 1 つ) があります。

[ホスト (Hosts)]、[配備の管理 (Deployment Management)]の順に選択し、NetBackup 環境にあるコンピュータに配備できるパッケージを確認します。このインターフェースで利用可能な処理は次のとおりです。

- 新しいパッケージを追加する。
- 既存のパッケージを削除する。

リポジトリにパッケージを追加する前に、VxUpdate 形式のパッケージを myveritas.com ライセンシングポータルからダウンロードする必要があります。ダウンロードしたパッケージをプライマリサーバーのアクセス可能な場所に配置します。パッケージのダウンロード方法について詳しくは、『NetBackup アップグレードガイド』の「リポジトリの管理」セクションを参照してください。具体的には、「Veritas NetBackup 承認済みメディアサーバーおよびクライアントパッケージのダウンロード」の手順を参照してください。

パッケージを追加するには

1 [ホスト (Hosts)]、[配備の管理 (Deployment Management)]の順に選択した後、リポジトリにすでにパッケージがあるかどうかに応じて、[パッケージを追加 (Add package)]または[追加 (Add)]を選択します。

2 ダイアログボックスで、VxUpdate パッケージが保存されている場所に移動して選択します。NetBackup で追加できるのは、プライマリサーバーのファイルシステムにあるパッケージのみです。

インターフェースには、VxUpdate パッケージのみが表示されます。ディレクトリにもファイルがある場合がありますが、VxUpdate パッケージがない場合は空として表示されます。

3 [OK]を選択して、パッケージを追加します。

追加するパッケージの数とサイズによっては、リポジトリに表示されるまでに時間がかかる場合があります。

パッケージを削除するには

1 [ホスト (Hosts)]、[配備の管理 (Deployment Management)]の順に選択し、削除するパッケージを選択します。

2 [削除 (Delete)]を選択します。

メモ: また、処理メニューから個々のパッケージを削除することもできます。

親パッケージを削除すると、その親に関連付けられているすべての子パッケージも削除されます。

サーバーパッケージを削除すると、関連付けられているクライアントパッケージも削除されます。たとえば、Windows 8.3 サーバーパッケージを削除すると、Windows 8.3 クライアントパッケージも削除されます。

ホストの更新

[ホストの更新 (Update host)]オプションを使用すると、すぐにジョブを開始して、NetBackup 環境を更新またはアップグレードできます。

[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順に選択し、1 つ以上の有効な選択を行うと、右上に[ホストの更新 (Update host)]オプションが表示されます。[ホストの更新 (Update host)]オプションの使用には、次の特定の制限が適用されます。

- 選択したすべてのコンピュータの種類が同じである必要があります。すべてのクライアントコンピュータまたはすべてのメディアサーバーを選択します。種類の異なるコンピュータを選択すると、[ホストの更新 (Update host)]オプションが消えます。

- プライマリサーバーはサポートされません。プライマリサーバーを選択すると、[ホストの更新 (Update host)]オプションが消えます。
- [ホストの更新 (Update host)]オプションを表示するには、オペレーティングシステムとバージョンの列にデータが含まれている必要があります。これらの列にデータが含まれていない場合は、ホストへの接続を試行します。

更新するコンピュータを指定した後、[ホストの更新 (Update host)]を選択すると、更新プロセスが開始されます。次の情報の入力を求められます。

- 属性 (Attributes)
  この画面で、配備するパッケージ、操作形式、並列実行ジョブの制限、Java および JRE の処理方法を指定します。
- ホスト (Hosts)
  アップグレードするホストが表示されます。この画面から、ホストを削除できます。
- セキュリティオプション (Security options) (表示された場合)
  デフォルト ([可能な場合は既存の証明書を使用します。(Use existing certificates when possible)]) を受け入れるか、環境に適したセキュリティ情報を指定します。
- 確認 (Review)
  前の画面で選択したすべてのオプションが表示されます。

[更新 (Update)]を選択すると、配備ジョブが開始されます。

配備ポリシー

[ホスト (Hosts)]、[配備の管理 (Deployment management)]の下に、[配備ポリシー (Deployment Policies)]タブが表示されるようになりました。このタブは、ポリシーの追加、編集、コピー、無効化、削除、起動に使用します。

新しいポリシーを追加するには:

1. [ホスト (Hosts)]、[配備の管理 (Deployment Management)]、[配備ポリシー (Deployment policies)]の順に移動し、[追加 (Add)]を選択します。
2. 配備ポリシーに必要な情報を入力します。

   必要な配備ポリシー情報は、更新ホスト情報に類似しています。

   p.64 の「ホストの更新」を参照してください。
3. [保存 (Save)]を選択します。

同様に、配備ポリシーを編集、コピー、無効化、または削除するには、ポリシーを選択します。その後、バナーから適切な操作を選択します。

ポリシーを手動で開始するには、目的のポリシーを選択し、メニューから[今すぐ配備 (Deploy now)]を選択します。

3

ストレージの構成

7

ストレージオプションの概要

この章では以下の項目について説明しています。

ストレージの構成について

NetBackup ですべての保護計画のストレージオプションとポリシーを設定できます。ストレージオプションは、ストレージオプションウィザードを使用して設定できます。このウィザードにアクセスするには、左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]の順にクリックします。

次のストレージオプションを設定できます。

- メディアサーバー重複排除プール (MSDP)
- イメージ共有用メディアサーバー重複排除プール (MSDP)
- AdvancedDisk
- クラウドストレージ
- OpenStorage

また、ユニバーサル共有を使用するように NetBackup を設定することもできます。

メモ: KMS (キーマネージメントサービス) を使用する場合、ストレージサーバーの設定で KMS オプションを選択するには、まず KMS を構成する必要があります。詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup Web UI にストレージサーバーの A.I.R. などのストレージ機能が正確に表示されるようにするには、メディアサーバーをアップグレードします。NetBackup 8.2 以前のメディアサーバーをアップグレードする必要がありますメディアサーバーをアップグレードした後、コマンドラインを使用してストレージサーバーを更新します。

次のコマンドを使用して、ストレージサーバーを更新します。

```
/usr/openv/netbackup/bin/admincmd/nbdevconfig -updatests
-storage_server <storage server name> -stype PureDisk
```

詳しくは、『NetBackup Deduplication ガイド』を参照してください。

8

ストレージサーバーの構成

この章では以下の項目について説明しています。

- クラウドストレージ、OpenStorage、または AdvancedDisk ストレージサーバーの作成
- メディアサーバー重複排除プール (MSDP) ストレージサーバーの作成
- イメージ共有用メディアサーバー重複排除プール (MSDP) ストレージサーバーの作成
- NetBackup Web UI からのイメージ共有の使用

クラウドストレージ、OpenStorage、または AdvancedDisk ストレージサーバーの作成

次の手順を使用して、クラウドストレージ、OpenStorage、または AdvancedDisk ストレージサーバーを作成します。

クラウドストレージサーバーの作成

クラウドストレージサーバーを作成するには、次の手順を実行します。

クラウドストレージサーバーを作成するには

1. 左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[追加 (Add)]の順にクリックします。
2. リストから[クラウドストレージ (Cloud storage)]を選択します。

3 [基本プロパティ(Basic properties)]で必要なすべての情報を入力し、[次へ(Next)]をクリックします。

フィールドをクリックして、クラウドストレージプロバイダを選択する必要があります。使用するクラウドストレージプロバイダが表示されない場合は、[検索(Search)]を使用して検索できます。

選択する[地域(Region)]情報がテーブルに表示されない場合は、[追加(Add)]を使用して必要な情報を手動で追加します。このオプションは、すべてのクラウドストレージプロバイダで表示されるわけではありません。

フィールドをクリックして、メディアサーバーを選択する必要があります。使用するメディアサーバーが表示されない場合は、[検索(Search)]を使用して検索できます。

4 [アクセス設定(Access settings)]で、選択したクラウドプロバイダに必要なアクセスの詳細を入力し、[次へ(Next)]をクリックします。

[SOCKS4]、[SOCKS5]、または[SOCKS4A]を使用する場合、[詳細(Advanced)]セクションのオプションの一部は利用できません。

5 [ストレージサーバーのオプション(Storage server options)]で、[オブジェクトのサイズ(Object size)]の調整、圧縮の有効化、またはデータの暗号化を行って、[次へ(Next)]をクリックします。

6 (オプション) [メディアサーバー(Media servers)]で、[追加(Add)]をクリックして、使用する追加のメディアサーバーを追加します。

クラウドストレージサーバーの場合、プライマリサーバーよりも古いバージョンの NetBackup がインストールされたメディアサーバーは表示されません。

追加のメディアサーバーを選択した後、または追加のメディアサーバーを選択せずに続行する場合は、[次へ(Next)]をクリックします。

7 [確認(Review)]ページで、すべてのオプションが正しいことを確認し、[保存(Save)]をクリックします。

8 (オプション) 上部の[ディスクプールの作成(Create disk pool)]をクリックします。

OpenStorage ストレージサーバーの作成

OpenStorage ストレージサーバーを作成するには、次の手順を実行します。

OpenStorage ストレージサーバーを作成するには

1 左側で[ストレージ(Storage)]、[ストレージ構成(Storage configuration)]、[追加(Add)]の順にクリックします。

2 リストから[OpenStorage]を選択します。

3 [基本プロパティ(Basic properties)]で必要なすべての情報を入力し、[次へ(Next)]をクリックします。

フィールドをクリックして、メディアサーバーを選択する必要があります。使用するメディアサーバーが表示されない場合は、[検索(Search)]を使用して検索できます。

ドロップダウンリストを使用して、正しいストレージサーバーの種類を選択します。

4 (オプション) [メディアサーバー (Media servers)]で、[追加 (Add)]をクリックして、使用する追加のメディアサーバーを追加します。

追加のメディアサーバーを選択した後、または追加のメディアサーバーを選択せずに続行する場合は、[次へ (Next)]をクリックします。

5 [確認(Review)]ページで、すべてのオプションが正しいことを確認し、[保存(Save)]をクリックします。

[保存 (Save)]をクリックすると、入力したクレデンシャルが検証されます。クレデンシャルが無効な場合は、[変更(Change)]をクリックすると、クレデンシャルに関する問題を修正できます。

6 (オプション) 上部の[ディスクプールの作成 (Create disk pool)]をクリックします。

AdvancedDisk ストレージサーバーの作成

AdvancedDisk ストレージサーバーを作成するには、次の手順を実行します。

AdvancedDisk ストレージサーバーを作成するには

1 左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[追加(Add)]の順にクリックします。

2 リストから[AdvancedDisk]を選択します。

3 メディアサーバーのリストを選択し、[ストレージサーバー名 (Storage server name)]を入力して、[選択 (Select)]をクリックします。

メディアサーバー重複排除プール (MSDP) ストレージサーバーの作成

この手順を使用して、メディアサーバー重複排除プール (MSDP) ストレージサーバーを作成します。ストレージサーバーを作成した後で、ディスクプール (ローカルストレージまたはクラウドストレージ) とストレージユニットを作成するオプションがあります。NetBackup にディスクプールとストレージユニットが存在しない場合は、作成することを推奨します。

MSDP ストレージサーバーを追加するには

1

2 左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[追加(Add)]の順にクリックします。

3 リストから[メディアサーバー重複排除プール (MSDP) (Media Server Deduplication Pool (MSDP))]を選択します。

4 [基本プロパティ (Basic properties)]で必要なすべての情報を入力し、[次へ (Next)]をクリックします。

フィールドをクリックして、メディアサーバーを選択する必要があります。使用するメディアサーバーが表示されない場合は、[検索 (Search)]を使用して検索できます。

5 [ストレージサーバーのオプション (Storage server options)]で必要なすべての情報を入力し、[次へ (Next)]をクリックします。

KMS (キーマネージメントサービス) を使用する場合、[KMS]オプションを選択するには、まず KMS を構成する必要があります。

6 (オプション) [メディアサーバー (Media servers)]で、[追加 (Add)]をクリックして、使用する追加のメディアサーバーを追加します。

追加のメディアサーバーを選択した後、または追加のメディアサーバーを選択せずに続行する場合は、[次へ (Next)]をクリックします。

7 [確認 (Review)]ページで、すべてのオプションが正しいことを確認し、[保存 (Save)]をクリックします。

MSDP ストレージサーバーの作成に失敗した場合は、画面に表示されるメッセージに従って問題を修正します。

クラウドストレージを使用するように MSDP を構成するには、次の手順 ([ボリューム (Volumes)]のドロップダウンを使用する手順) で、既存のディスクプールボリュームを選択するか、新しいボリュームを作成します。

p.77 の「ディスクプールの作成」を参照してください。

8 (オプション) 上部の[ディスクプールの作成 (Create disk pool)]をクリックします。

9 (オプション)レプリケーションを使用してクラウド論理ストレージユニットとディスクプールを作成するには、[ディスクプールを作成 (Create disk pool)]をクリックします。

ディスクプールの作成に必要な情報を入力します。

次のタブで、必要なクラウドボリュームを選択し、追加します。クラウドストレージプロバイダを選択し、ストレージプロバイダの必要な詳細情報を指定します。クレデンシャルを入力して、クラウドストレージプロバイダにアクセスし、詳細設定を定義します。

メモ: 現在、AWS S3 と Azure ストレージの API 形式がサポートされています。

メモ: サーバー側の暗号化を有効にした場合は、AWS のカスタマ管理キーを構成できます。これらのキーは、一度 NetBackup で使用されたら削除できません。各オブジェクトはアップロード中にキーで暗号化されます。AWS からキーを削除すると、NetBackup でリストアのエラーが発生します。

メモ: NetBackup Recovery Vault では、Microsoft Azure や Amazon などの複数のオプションがサポートされています。クレデンシャルについて、または利用可能なオプションについて詳しくは、Veritas NetBackup のアカウントマネージャにお問い合わせください。

環境と配備について詳しくは、Recovery Vault for NetBackup を参照してください。

詳しくは、『NetBackup クラウド管理者ガイド』および『NetBackup 重複排除ガイド』を参照してください。

p.77 の「ディスクプールの作成」を参照してください。

p.80 の「ストレージユニットの作成」を参照してください。

p.69 の「クラウドストレージ、OpenStorage、または AdvancedDisk ストレージサーバーの作成 」を参照してください。

p.95 の「保護計画の作成」を参照してください。

イメージ共有用メディアサーバー重複排除プール (MSDP) ストレージサーバーの作成

このトピックは、イメージ共有のためのクラウドリカバリサーバーの作成に使用します。クラウドリカバリサーバーについて詳しくは、『NetBackup 重複排除ガイド』の「MSDP クラウドを使用したイメージ共有について」のトピックを参照してください。

クラウドリカバリサーバーを設定するには、次の手順を実行します。

1. 左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[追加 (Add)]の順にクリックします。ストレージサーバーを削除した場合は、このページを更新します。
2. リストから[イメージ共有用メディアサーバー重複排除プール (MSDP) (Media Server Deduplication Pool (MSDP) for image sharing)]を選択します。
3. [基本プロパティ (Basic properties)]で必要なすべての情報を入力し、[次へ (Next)]をクリックします。

   フィールドをクリックして、メディアサーバーを選択する必要があります。使用するメディアサーバーが表示されない場合は、検索オプションを使用します。
4. ストレージサーバーオプションで、[暗号化オプション (Encryption options)]と[ローカルストレージの暗号化 (Encryption for local storage)]を除くすべての必要な情報を入力し、[次へ (Next)]をクリックします。

   KMS 暗号化がオンプレミス側で有効になっている場合は、クラウドリカバリサーバーを設定する前に、キーマネージメントサービス (KMS) を設定する必要があります。次に、オンプレミス側からの KMS オプションがクラウドリカバリサーバーで自動的に選択され、設定されます。
5. (オプション) メディアサーバーで、[次へ (Next)]をクリックします。クラウドリカバリサーバーはオールインワンの NetBackup サーバーであるため、追加のメディアサーバーは追加されません。
6. [確認 (Review)]ページで、すべてのオプションが正しいことを確認し、[保存 (Save)]をクリックします。

   イメージ共有を持つ MSDP の作成に失敗した場合は、画面に表示されるメッセージに従って問題を修正します。
7. 上部の[ディスクプールの作成 (Create disk pool)]をクリックします。

   別の方法: 左側で[ストレージ (Storage)]、[ディスクプール (Disk pools)]タブ、[追加 (Add)]の順にクリックします。
8. [ディスクプールオプション (Disk pool options)]で必要なすべての情報を入力し、[次へ (Next)]をクリックします。

   ストレージサーバーを選択するには、[変更 (Change)]をクリックします。
9. [ボリューム (Volume)]で、[ボリューム (Volume)]ドロップダウンを使用して新しいボリュームを追加します。選択内容に応じて必要なすべての情報を入力し、[次へ (Next)]をクリックします。

   ボリューム名は、オンプレミス側のボリューム名またはサブバケット名と同じである必要があります。

10 [レプリケーション (Replication)]で[次へ (Next)]をクリックし、プライマリサーバーを追加せずに続行します。

11 [確認 (Review)]ページで、すべての設定と情報が正しいことを確認します。[保存 (Save)]をクリックします。

p.75 の「NetBackup Web UI からのイメージ共有の使用 」を参照してください。

NetBackup Web UI からのイメージ共有の使用

NetBackup Web UI を使用して、オンプレミスの場所からクラウドにイメージを共有できます。必要に応じてクラウドリカバリサーバーを設定し、そのサーバーにイメージを共有できます。

『NetBackup 重複排除ガイド』の次のトピックの情報を使用して、クラウドリカバリサーバーを設定します。

MSDP クラウドを使用したイメージ共有について

クラウドリカバリサーバーの設定後に NetBackup Web UI から実行する手順

開始する前に、イメージのインポート、リストア、変換、AMI ID または VHD へのアクセスを行うために、Web UI で必要な権限を持っていることを確認します。

イメージのインポート

1. 左側で、[ストレージ (Storarge)]、[ストレージ設定 (Storage configuration)]、[ディスクプール (Disk pool)]の順に選択します。
2. 共有するイメージを含むボリュームプールを選択します。
3. ディスクプールのオプションで、ディスクプール名を特定し、[処理 (Actions)]、[高速インポート (Fast Import)]の順にクリックします。

   メモ: 高速インポートオプションは、イメージ共有に固有のインポート操作です。バックアップイメージは、クラウドストレージからイメージ共有に使用されるクラウドリカバリサーバーにインポートできます。高速インポートの後、イメージをリストアできます。AWS クラウドプロバイダの場合は、VM イメージを AWS AMI にも変換できます。Azure クラウドプロバイダの場合は、VM イメージを VHD に変換できます。

4. [イメージの高速インポート (Fast import images)]ページで、インポートするバックアップイメージを選択し、[インポート (Import)]をクリックします。
5. アクティビティの完了状態を[アクティビティモニター (Activity Monitor)]で確認します。

Azure での VM イメージの AWS AMI または VHD への変換

1. 左側の［VMware］、変換するインポート後の VMware イメージの順に選択します。
2. ［リカバリポイント (Recovery point)］タブで、リカバリ日を選択します。
3. リカバリポイントの日付を指定するには、必要なリカバリポイントを選択し、［処理 (Actions)］、［変換 (Convert)］の順にクリックします。
4. 変換が完了すると、AMI ID または VHD URL が生成されます。
5. AMI ID を使用して AWS 内のイメージを特定し、AWS コンソールを使用して EC2 インスタンスを起動します。または、VHD URL を使用して仮想マシンを作成します。

9

ディスクストレージの構成

この章では以下の項目について説明しています。

ディスクプールの作成

任意の種類のストレージサーバーを作成した後、ディスクプールを作成する手順を実行します。ディスクプールはいつでも作成できますが、既存のストレージサーバーが作成されている必要があります。

クラウドストレージを使用するように MSDP ストレージサーバーを設定できます。このように設定するには、ディスクプールを作成するときに既存のクラウドボリュームを選択するか、新しいクラウドボリュームを作成します。[ボリューム (Volumes)]のドロップダウンの手順を実行して、既存のクラウドボリュームを選択するか、MSDP ストレージサーバーに新しいボリュームを作成します。

[ディスクプール (Disk pools)]タブを表示すると、クラウドストレージプロバイダを使用するディスクプールの[利用可能な領域 (Available space)]列が空になっていることがあります。クラウドプロバイダがその情報の API を提供しないため、NetBackup は情報を取得できません。

ディスクプールを作成するには

1 左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[ディスクプール (Disk pools)]タブ、[追加 (Add)]の順にクリックします。

ディスクプールを作成するための別の方法として、ストレージサーバーを作成した後、画面の上部にある[ディスクプールの作成 (Create disk pool)]をクリックします。

2 [ディスクプールオプション (Disk pool options)]で必要なすべての情報を入力し、[次へ (Next)]をクリックします。

ストレージサーバーを選択するには、[変更 (Change)]をクリックします。

[I/O ストリーム数を制限 (Limit I/O streams)]をオフのままにすると、デフォルト値は[無制限 (Unlimited)]になり、パフォーマンスの問題が発生する可能性があります。

3 [ボリューム (Volume)]で、[ボリューム (Volume)]ドロップダウンを使用してボリュームを選択するか、新しいボリュームを追加します。新しいディスクプールボリュームを追加する場合は、[ボリュームの追加 (Add volume)]オプションを使用します。

メモ: サーバー側の暗号化を有効にした場合は、AWS のカスタマ管理キーを構成できます。これらのキーは、一度 NetBackup で使用されたら削除できません。各オブジェクトはアップロード中にキーで暗号化されます。AWS からキーを削除すると、NetBackup でリストアのエラーが発生します。

メモ: NetBackup Recovery Vault では、Microsoft Azure や Amazon などの複数のオプションがサポートされています。クレデンシャルについて、または利用可能なオプションについて詳しくは、Veritas NetBackup のアカウントマネージャにお問い合わせください。

選択内容に応じて必要なすべての情報を入力し、[次へ (Next)]をクリックします。

4 [レプリケーション (Replication)]で、[追加 (Add)]をクリックしてディスクプールにレプリケーションターゲットを追加します。

この手順では、信頼できるプライマリサーバーを選択または追加できます。NetBackup 認証局 (NBCA)、ECA、ECA と NBCA の両方をサポートするプライマリサーバーを追加できます。

レプリケーションは MSDP でのみサポートされます。

レプリケーションターゲットに対して入力されたすべての情報を確認し、[次へ (Next)]をクリックします。

5 [確認 (Review)]ページで、すべての設定と情報が正しいことを確認します。[完了 (Finish)]をクリックします。

ウィンドウを閉じると、ディスクプールの作成とレプリケーション構成がバックグラウンドで続行されます。クレデンシャルとレプリケーションの構成の検証に問題がある場合は、[変更 (Change)]オプションを使用して設定を調整できます。

10

ストレージユニットの構成

この章では以下の項目について説明しています。

ストレージユニットの作成

この手順を使用して、ストレージユニットを作成します。任意の種類のストレージサーバーとディスクプールを作成した後、ストレージユニットを作成する必要があります。また、ストレージサーバーとディスクプールを作成せずに新しいストレージユニットを作成する場合にも、この手順は有効です。

[ストレージユニット (Storage units)]タブを表示すると、クラウドストレージプロバイダを使用するストレージユニットの[使用領域 (Used space)]列が空になっていることがあります。クラウドプロバイダがその情報の API を提供しないため、NetBackup は情報を取得できません。

ストレージユニットを作成するには

1. 左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[ストレージユニット (Storage units)]タブ、[追加 (Add)]の順にクリックします。

   ストレージユニットを作成するための別の方法として、ディスクプールを作成した後、画面の上部にある[ストレージユニットの作成 (Create storage unit)]をクリックします。

2. リストからストレージユニットを選択し、[開始 (Start)]をクリックします。

3. [基本プロパティ(Basic properties)]で必要なすべての情報を入力し、[次へ (Next)]をクリックします。

4 [ディスクプール (Disk pool)]で、ストレージユニットで使用するディスクプールを選択し、[次へ (Next)]をクリックします。

WORM (Write Once Read Many) ストレージをサポートするディスクプールを選択すると、[WORM の有効化 (Enable WORM)]オプションが有効になります。

WORM のプロパティについて詳しくは、『NetBackup 管理者ガイド Vol. 1』の「NetBackup でのデータの変更不可と削除不可の設定」を参照してください。

[オンデマンドのみ (On demand only)]オプションはストレージユニットがオンデマンドで排他的に利用可能かどうかを指定します。このストレージユニットを使うためにポリシーまたはスケジュールを明示的に構成する必要があります。

5 [メディアサーバー (Media servers)]タブで、使用するメディアサーバーを選択し、[次へ (Next)]をクリックします。

NetBackup がメディアサーバーを自動で選択するか、ラジオボタンを使用してメディアサーバーを手動で選択できます。

6 ストレージユニットの設定を確認し、[保存 (Save)]をクリックします。

p.77 の「ディスクプールの作成」を参照してください。

p.71 の「メディアサーバー重複排除プール (MSDP) ストレージサーバーの作成」を参照してください。

p.69 の「クラウドストレージ、OpenStorage、または AdvancedDisk ストレージサーバーの作成 」を参照してください。

p.95 の「保護計画の作成」を参照してください。

11

ユニバーサル共有の構成

この章では以下の項目について説明しています。

ユニバーサル共有の作成

ユニバーサル共有は、効率的な領域である SMB (CIFS) または NFS 共有にデータを直接取り込む機能を提供します。領域の効率は、このデータを既存の NetBackup 重複排除プール (MSDP) に直接格納することで達成されます。共有をマウントしているクライアントに NetBackup ソフトウェアをインストールする必要はありません。POSIX 準拠のファイルシステムを実行し、SMB (CIFS) または NFS ネットワーク共有をマウントできるオペレーティングシステムは、すべてユニバーサル共有にデータを書き込めます。

ユニバーサル共有について詳しくは、『NetBackup 重複排除ガイド』を参照してください。

NetBackup WEB UI を使用して、次のことを実行できます。

- ユニバーサル共有の作成、変更、表示、削除、および NetBackup アプライアンス、Flex Appliance、Flex Scale、Flex WORM/非 WORM、MSDP AKS/EKS の配備、BYO (build-your-own)、BYO-In-Cloud サーバーにわたるユニバーサル共有の管理を行います。
- クォータの設定、Active Directory (AD) ユーザーおよびグループ名、ユニバーサル共有に関連するターゲットホストを変更します。

メモ: ユニバーサル共有ポリシー、前提条件、構成、クラウド LSU 制限のユニバーサル共有について詳しくは、『NetBackup 重複排除ガイド』を参照してください。

NetBackup Web UI でユニバーサル共有を作成するには

1 左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[ユニバーサル共有 (Universal Share)]、[追加 (Add)]の順にクリックします。

ストレージサーバーが存在しない場合は、MSDP ストレージサーバーを構成します。

p.71 の「メディアサーバー重複排除プール (MSDP) ストレージサーバーの作成」を参照してください。

MSDP ストレージサーバーを作成した後、[ユニバーサル共有 (Universal Share)]タブに戻り、[追加 (Add)]をクリックしてユニバーサル共有を追加します。

2 次の必須情報を入力します。

- [表示名 (Display name)]を入力します。この名前は、ユニバーサル共有パスで使用されます。
- ストレージサーバーを選択します。
- ディスクボリュームを選択します。
  検索アイコンをクリックしてボリュームリストを取得し、ディスクボリュームを選択します。デフォルトで PureDiskVolume が選択されます。
  このオプションは、クラウド機能のオブジェクトストレージを使用するユニバーサル共有が有効な場合にのみ利用可能です。詳しくは、『NetBackup 重複排除ガイド』を参照してください。
- [プロトコル (Protocol)]: NSF または SMB (CIFS) を選択します。
- 共有のマウントが許可されている[ホスト (Host)]を指定し、[リストに追加 (Add to list)]をクリックします。ホスト名、IP アドレス、短縮名または FQDN を使用して、ホストを指定できます。各共有に対して複数のホストを入力できます。

3 この時点で、残りのフィールドに値を入力するか、[保存 (Save)]をクリックしてユニバーサル共有を保存します。後で、ユニバーサル共有の詳細ページで残りのフィールドを更新できます。

- [クォータの種類 (Quota type)]: (無制限またはカスタム) を選択します。[カスタム (Custom)]を選択した場合は、クォータも、MB、GB、TB 単位で指定します。
  カスタムクォータ値は、共有に取り込まれるデータの量を制限します。クォータは、フロントエンド TB (FETB) の計算方法を使用して適用されます。これらは共有ごとに実装され、いつでも変更できます。変更を反映するために共有を再マウントする必要はありません。
  ユニバーサル共有の詳細ページから見積もりの種類または値を更新するには、[クォータ (Quota)]セクションの[編集 (Edit)]をクリックします。
- [ユーザー名 (User names)] (ローカルまたは Active Directory) と[グループ名 (Group names)] (Active Directory のみ) を指定します。指定したユーザーまたはグループのみが共有にアクセスできます。[ユーザー名 (User names)]

と[グループ名 (Group names)]は、後で既存のユニバーサル共有の詳細ページから追加および更新できます。

メモ: 現在、[ユーザー名 (User names)]と[グループ名 (Group names)]は、SMB (CIFS) プロトコルでのみサポートされます。

4 ユニバーサル共有の詳細を表示するには、[ユニバーサル共有 (Universal Share)]テーブルで、その名前をクリックします。

5 ユニバーサル共有を削除するには、1 つ以上選択し、[削除 (Delete)]をクリックするか、[処理 (Actions)]メニューで[削除 (Delete)]を選択します。

ユニバーサル共有を削除すると、共有内のすべてのデータも削除されます。この処理をやり直すことはできません。また、データ量が多い場合は時間がかかることがあります。アクティブなデータ転送はすぐに終了し、マウントされた共有はすぐに削除されます。

MS-Windows および Standard ポリシーのインスタントアクセスの使用

非構造化データ資産に対するインスタントアクセスにより、ユーザーは MS-Windows ポリシーまたは標準ポリシーによって作成されたバックアップイメージからインスタントアクセスマウントを作成できます。

MS-Windows ポリシーまたは標準ポリシーを使用してインスタントアクセスを管理するには、ユーザーに RBAC 管理者の役割が必要です。または、類似の権限を持つ役割が必要です。

NetBackup インスタントアクセス API を使用して、ローカルまたはクラウド LSU (論理ストレージユニット) からバックアップコピーに即座にアクセスできます。

クラウド LSU (論理ストレージユニット) でのインスタントアクセスの制限事項については、『NetBackup 重複排除ガイド』を参照してください。

メモ: Flex WORM ストレージでのインスタントアクセスには、次のサービスが必要です: NGINX、NFS、SAMBA、WINBIND (Active Directory が必要な場合)、SPWS、VPFS

12

ストレージ構成の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。

ストレージ構成のトラブルシューティング

次の表に、ストレージを構成する際に発生する可能性のあるいくつかの問題を示します。

表 12-1　　ストレージ構成のトラブルシューティング

エラーメッセージまたは原因	説明および推奨処置
クラウドボリュームのディスクプールを作成するときに、次のエラーが表示されます。 ディスクに空きがありません (disk is full)	回避方法: ディスクに空きがあってもエラーが表示された場合は、クラウドボリュームを作成するために利用可能な十分な領域があることを確認します。 デフォルトでは、クラウドボリュームには約 1 TB の空き容量が必要です。 クラウドボリュームのサイズを縮小するには、`/msdp/etc/puredisk/` から `contentrouter.cfg` ファイルを開き、値を変更します。値を変更した後、MSDP サービスを再起動してからクラウドボリュームを作成します。
ローカル MSDP ストレージでは、圧縮と暗号化の値が正しく表示されません。	保護計画の長期保持設定を選択するページで、ローカル MSDP ストレージに圧縮と暗号化の値が正しく表示されません。

ユニバーサル共有の構成に関する問題をトラブルシューティングする

ユニバーサル共有について詳しくは、『NetBackup 重複排除ガイド』を参照してください。

失敗したインストールまたは構成をトラブルシューティングする方法

ユニバーサル共有を構成するには、ストレージサーバーでインスタントアクセスが有効になっていることを確認します。インスタントアクセスについて詳しくは、次のマニュアルを参照してください。

- 『NetBackup Web UI VMware 管理者ガイド』
- 『NetBackup Web UI Microsoft SQL 管理者ガイド』

ストレージサーバーでインスタントアクセスが有効になっていることを確認するには

1. ストレージサーバーにログインして、次のコマンドを実行します (BYO (Build Your Own) のみ)。

   ```
   /usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
   ```

2. 前提条件の確認結果と構成結果を確認します。

   `/var/log/vps/ia_byo_precheck.log` (BYO のみ)

   `/usr/openv/pdde/vpfs/vpfs-config.log` (BYO とアプライアンス構成)

   次の例では、必要ないくつかのサービスが実行されていません。

   ```
   [root@rhelnbu06 ~]# /usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh
   Mon Apr 13 12:42:14 EDT 2020 Try to get storagepath
   Mon Apr 13 12:42:14 EDT 2020 Storage ContentRouter config path
   is
      /msdp/etc/puredisk/contentrouter.cfg
   Mon Apr 13 12:42:14 EDT 2020 Storagepath is /msdp
   Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp is
      ext2/ext3
   Mon Apr 13 12:42:14 EDT 2020 File system for partition /msdp/data

      is ext2/ext3
   Mon Apr 13 12:42:14 EDT 2020 **** Hardware Virtualization not
      supported, Instant Access browse may be slow ****
   Mon Apr 13 12:42:14 EDT 2020 **** system memory support 50 vpfs
      livemounts ****
   Mon Apr 13 12:42:14 EDT 2020 **** nginx service required by
      Instant Access is not running ****
   Mon Apr 13 12:42:14 EDT 2020 **** smb service required by
      Instant Access is not running ****
   Mon Apr 13 12:42:14 EDT 2020 **** docker service required by
      VMware Instant Access is not running ****
   ```

3. ログに示されている問題を解決します。たとえば、インスタントアクセスに必要なすべてのサービスを再起動します。

ユニバーサル共有機能を確認する方法

ストレージサーバーがユニバーサル共有機能を備えていることを確認するには

1. ストレージサービスが NetBackup 8.3 以降を実行していることを確認します。
2. ストレージサーバーにログオンして、次のコマンドを実行します。

   ```
   nbdevquery -liststs -U
   ```

   コマンドの出力に InstantAcess フラグが表示されていることを確認します。

   このフラグが表示されない場合は、前述のいずれかのガイドを参照して、ストレージサーバーでインスタントアクセスを有効にします。
3. 次のコマンドを実行します。

   ```
   nbdevconfig -getconfig -stype PureDisk -storage_server
   storage_server_name
   ```

   コマンドの出力に UNIVERSAL_SHARE_STORAGE フラグが表示されていることを確認します。

   このフラグが表示されない場合は、ストレージサーバーでユニバーサル共有を作成します。

   p.82 の「ユニバーサル共有の作成」を参照してください。

ユニバーサル共有を開始または停止する方法

ユニバーサル共有は、NetBackup サービスを使用して開始、再起動、または停止できます。

- ユニバーサル共有を開始または再起動するには、次のコマンドを使用します。

  ```
  netbackup start
  ```
- ユニバーサル共有を終了するには、次のコマンドを使用します。

  ```
  netbackup stop
  ```

NetBackup Web UI でユニバーサル共有が作成されるたびに、マウントポイントもストレージサーバーに作成されます。

次に例を示します。

```
[root@rsvlmvc01vm309 vpfs.mnt]# mount | grep vpfs
vpfsd on /mnt/vpfs type fuse.vpfsd
(rw,nosuid,nodev,relatime,user_id=0,
   group_id=0,default_permissions,allow_other)
vpfsd on /mnt/vpfs_shares/aa7e/aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e
   type fuse.vpfsd (rw,nosuid,nodev,relatime,user_id=0,group_id=0,
   default_permissions,allow_other)
```

この例では aa7e83e5-93e4-57ea-a4a8-81ddbf5f819e がユニバーサル共有の ID です。この ID は、NetBackup Web UI のユニバーサル共有の詳細ページにあります。左側で[ストレージ (Storage)]、[ストレージ構成 (Storage configuration)]、[ユニバーサル共有 (Universal Shares)]の順にクリックし、ユニバーサル共有を選択して、その詳細を表示します。

4

バックアップの構成

13

NetBackup Web UI でのバックアップの概要

この章では以下の項目について説明しています。

NetBackup Web UI でサポートされるバックアップ方式

NetBackup Web UI には、データを保護するために次の方式が用意されています。

- 保護計画。保護計画では資産を保護します。たとえば、データベースや仮想マシンなどを保護します。作業負荷管理者には、利用可能なデフォルトの RBAC 役割を通じて、保護計画へのアクセス権が付与されます。これにより、管理者は計画に資産をサブスクライブできます。
- ポリシー。ポリシーによりクライアントのデータが保護されます。一部のエージェントには、複数のクライアントに分散している資産を保護するインテリジェントポリシーもあります。

保護計画とインテリジェントポリシーは、資産管理と連携して、NetBackup 環境内の資産を自動的に検出します。

保護計画とポリシーに関する FAQ

NetBackup の従来のポリシー、保護計画、またはその両方を同時に使用して、資産を保護できます。このトピックでは、NetBackup Web UI での NetBackup の従来のポリシーについてよく寄せられる質問に回答します。

表 13-1　　従来のポリシーについてよく寄せられる質問

質問	回答
Web UI の[保護計画名 (Protected by)]列の[従来のポリシーのみ (Classic policy only)]は何を意味しますか。	資産は、現在保護計画にサブスクライブされていません。ただし、以前は保護計画にサブスクライブされていました。または、ある時点の従来のポリシーで保護対象になっていて[最終バックアップ (Last backup)]の状態になっています。資産を保護している、有効な従来のポリシーがある場合もない場合もあります (調べるには NetBackup 管理者にお問い合わせください)。
従来のポリシーの詳細はどこで見つかりますか。	従来のポリシーの詳細は、いくつかのポリシー形式の例外を除き、Web UI には表示されません。 p.93 の「NetBackup の従来のポリシーのサポート」を参照してください。
従来のポリシーを管理するにはどうすればよいですか。	一部のポリシー形式は、NetBackup Web UI で管理できます。 p.93 の「NetBackup の従来のポリシーのサポート」を参照してください。 その他の従来のポリシーについては、NetBackup 管理コンソールまたは NetBackup CLI を使用します。RBAC「管理者」役割を持つユーザーは、NetBackup API を使用してポリシーを管理および作成できます。
保護計画への資産のサブスクライブと、従来のポリシーによる資産の保護は、それぞれどのような場合に行うべきですか。	保護計画を使用すると、計画に対する資産の追加と削除、および保護対象の資産の確認を簡単に行えます。作業負荷管理者は、保護計画と資産を表示または管理できるユーザーを完全に制御できます。 ポリシーは従来のデータ保護方法を提供します。ただし、個々のポリシーまたは保護するデータに対する RBAC 制御はありません。
保護計画と従来のポリシーの両方を使用して、資産を保護できますか。	はい。Web UI には、保護計画の詳細は表示されますが、従来のポリシーの詳細は表示されません。従来のポリシーについて詳しくは、NetBackup 管理者にお問い合わせください。

質問	回答
保護計画から資産のサブスクライブが解除されて、Web UI でその資産に対して[従来のポリシーのみ (Classic policy only)]と表示された場合に、どのような対処が必要ですか。	従来のポリシーが資産を保護しているかどうかを、NetBackup 管理者に問い合わせることができます。

サポートされる保護計画の種類

Web UI は次の作業負荷の保護計画をサポートします。

- Apache Cassandra
- クラウド
- クラウドオブジェクトストア
- Kubernetes
- Microsoft SQL Server
- MySQL
- Nutanix AHV
- OpenStack
- Oracle
- PostgreSQL
- Red Hat Virtualization (RHV)
- SaaS
- VMware

NetBackup の従来のポリシーのサポート

次のポリシー形式は、NetBackup Web UI で管理できます。NetBackup 管理コンソールでは、他のポリシー形式を利用できます。

- BigData
- Cloud-Object-Store
- DB2
- Informix

- MS-Exchange-Server
- MS-SQL-Server
- MS-Windows
- NBU-Catalog
- NDMP
- Oracle
- SAP
- Standard
- Universal-Share
- VMware

14

保護計画の管理

この章では以下の項目について説明しています。

保護計画の作成

メモ: アップグレード後に、Web UI に保護計画が表示されない場合があります。変換プロセスが実行されていない可能性がありますが、アップグレードの実行から 5 分以内に実行されるはずです。

保護計画を作成する前に、すべてのストレージオプションを構成する必要があります。

p.67 の「ストレージの構成について」を参照してください。

保護計画を作成するには

1. 左側で[保護 (Protection)]、[保護計画 (Protection plans)]、[追加 (Add)]の順にクリックします。
2. [基本プロパティ (Basic properties)]で、[名前 (Name)]と[説明 (Description)]を入力し、ドロップダウンリストから[作業負荷 (Create a protection plan to protect)]を選択します。

オプションの選択:

- ポリシー名接頭辞 (Policy name prefix):
  このオプションは、ポリシー名の指定に使用します。ユーザーがこの保護計画に資産をサブスクライブする際に、NetBackup はポリシーを自動的に作成します。このとき、ポリシー名に接頭辞が付加されます。
- 継続的なデータ保護を有効にする (Enable Continuous Data Protection)
  VMware 作業負荷の場合、作業負荷に対して継続的なデータ保護を使用するには、このオプションを選択します。詳しくは『NetBackup Web UI VMware 管理者ガイド』の「継続的なデータ保護」の章を参照してください。
- PaaS 資産のみを保護 (Protect PaaS assets only)
  クラウド作業負荷の場合、スナップショットベースでない保護を使用する RDS 以外の PaaS 資産を保護計画で保護するには、このオプションを選択する必要があります。スナップショットベースの保護を使用する RDS 資産では、このオプションを選択しないでください。詳しくは、『NetBackupWeb UI クラウド管理者ガイド』の「PaaS 資産の管理」の章を参照してください。

3 [スケジュール (Schedules)]で[追加 (Add)]をクリックします。

Azure または Azure Stack の作業負荷としてクラウドを選択した場合は、『NetBackup Web UI クラウド管理者ガイド』で「クラウド作業負荷のバックアップスケジュールの構成」セクションを参照してください。

日単位、週単位、月単位のバックアップを設定してから、そのバックアップの保持とレプリケーションについて設定できます。さらに、作業負荷に応じて、[自動 (Automatic)]、[完全 (Full)]、[差分増分 (Differential incremental)]、[累積増分 (Cumulative Incremental)]、[スナップショットのみ (Snapshot only)]のバックアップスケジュールを設定できます。

AWS スナップショットレプリケーションについて詳しくは、『NetBackup Web UI クラウド管理者ガイド』の「AWS スナップショットレプリケーションの構成」を参照してください。

頻度として[毎月 (Monthly)]を選択する場合、[曜日 (Days of the week)] (グリッドビュー) または[日付 (Days of the month)] (カレンダービュー) のいずれかを選択できます。

メモ: スケジュール形式として[自動 (Automatic)]を選択すると、この保護計画のすべてのスケジュールが[自動 (Automatic)]になります。スケジュール形式として[完全 (Full)]、[差分増分 (Differential incremental)]、または[累積増分 (Cumulative Incremental)]を選択する場合、この保護計画のすべてのスケジュールをそれらのいずれかのオプションにする必要があります。

スケジュール形式として[自動 (Automatic)]を選択すると、スケジュール形式が NetBackup で自動的に設定されます。指定した頻度に基づいて、[完全 (Full)]または[差分増分 (Differential incremental)]をいつ実行するかが NetBackup で計算されます。

メモ: WORM ストレージのロック期間に特定のスケジュールの間隔が設定されている場合、保護計画の作成は VMware 作業負荷に対して機能しません。スケジュールの間隔が 1 週間未満に設定され、WORM ストレージの[ロックの最大期間 (Lock Maximum Duration)]が 1 週間未満で要求された保持期間よりも長い場合、保護計画の作成は機能しません。

WORM 対応ストレージで VMware を保護するために保護計画を使用する場合は、WORM ストレージの[ロックの最大期間 (Lock Maximum Duration)]を 1 週間より長く設定します。または、保護計画のスケジュール形式を明示的に選択します。

[属性 (Attributes)]タブで、次の操作を行います。

- [バックアップ形式 (Backup type)]、バックアップを実行する頻度、このスケジュールのバックアップを保持する期間を選択します。
  - [バックアップ形式 (Backup type)]の選択は、選択された作業負荷と、この保護計画で現在有効になっている他のバックアップスケジュールに依存します。
- (オプション) バックアップをレプリケートするには、[このバックアップをレプリケートする (Replicate this backup)]を選択します。
  - [このバックアップをレプリケートする (Replicate this backup)]オプションを使用するには、バックアップストレージが、対象の A.I.R. 環境でソースになっている必要があります。[レプリケーションターゲット (Replication target)]は、手順 4 で構成します。
  - レプリケーションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』の、NetBackup 自動イメージレプリケーションについての説明を参照してください。
- (オプション) 長期保持用ストレージにコピーを維持するには、[長期保持用にすぐにコピーを複製する (Duplicate a copy immediately to long-term retention)]をオンにします。このオプションは、一部の作業負荷では利用できません。

- NetBackup は、バックアップの完了後すぐに、長期保持用ストレージにコピーを複製します。
- 長期保持用ストレージに利用可能なスケジュールオプションは、作成した通常のバックアップスケジュールの頻度と保持レベルに基づいています。

[開始時間帯 (Start Window)]タブで、次の操作を行います。

- 画面上で設定可能なオプションを使用して、該当スケジュールの[開始曜日 (Start day)]、[開始日時 (Start time)]、[終了曜日 (End day)]、[終了日時 (End time)]を定義します。または、時間のボックス上にカーソルをドラッグして、スケジュールを作成できます。
- 右側のオプションを使用して、スケジュールを複製、削除、またはスケジュールの変更を元に戻します。

[属性 (Attributes)]タブと[開始時間帯 (Start window)]タブでオプションをすべて選択したら、[保存 (Save)]をクリックします。

[バックアップスケジュールのプレビュー (Backup schedule preview)]ウィンドウを確認して、すべてのスケジュールが正しく設定されていることを確認します。

4 [ストレージオプション (Storage options)]で、手順 3 で設定したスケジュールごとにストレージ形式を設定します。

オプションは、NetBackup で使用するように現在設定されているストレージオプションによって異なります。

保護計画では、NetBackup 8.1.2 以降のメディアサーバーがアクセスできるストレージのみを使用できます。

ストレージオプション	要件	説明
スナップショットストレージのみ (Snapshot storage only)	このオプションには、Snapshot Manager が必要です。	NetBackup 管理コンソールでスナップショット管理サーバー機能を使用して、Snapshot Manager を構成します。スナップショットのみのストレージオプションを使用する場合、他のストレージオプションは選択できません。手順 5 に進みます。
スナップショットバックアップを実行する (Perform snapshot backups)	このオプションを設定する場合は、Microsoft SQL Server が必要です。	Microsoft SQL Server の保護計画の構成手順については、『NetBackup Web UI Microsoft SQL Server 管理者ガイド』を参照してください。
バックアップストレージ (Backup storage)	このオプションには、OpenStorage が必要です。テープ、ストレージユニットグループ、および Replication Director はサポートされません。	[編集 (Edit)]をクリックして、ストレージターゲットを選択します。ストレージターゲットを選択したら、[選択したストレージの使用 (Use selected storage)]をクリックします。 NetBackup アクセラレータ機能では、使用するネットワーク帯域幅が少ないコンパクトなデータストリームを作成することで、従来のバックアップよりも保護計画を迅速に実行できます。NetBackup プライマリサーバー上のストレージサーバーで NetBackup アクセラレータがサポートされる場合、この機能は保護計画に含まれます。NetBackup アクセラレータについて詳しくは、NetBackup 管理者に問い合わせるか、『NetBackup 管理者ガイド Vol.1』または『NetBackup for VMware 管理者ガイド』を参照してください。 インスタントアクセス機能を使用すると、計画のリカバリポイントで、インスタントアクセス VM またはデータベースの作成をサポートできます。

ストレージオプション	要件	説明
レプリケーションターゲット (Replication target)	バックアップストレージは、対象の A.I.R. 環境でソースになっている必要があります。	[編集 (Edit)]をクリックして、レプリケーションターゲットプライマリサーバーを選択します。プライマリサーバーを選択し、次にストレージライフサイクルポリシーを選択します。[選択したレプリケーションターゲットを使用 (Use selected replication target)]をクリックして、ストレージオプション画面に戻ります。 クラウドの作業負荷は、レプリケーション (AIR) で MSDP と MSDP-C のストレージユニットをサポートします。 レプリケーションターゲットプライマリサーバーがリストに表示されない場合、NetBackup で追加する必要があります。レプリケーションターゲットプライマリサーバーを追加する方法について詳しくは、『NetBackup 重複排除ガイド』の「信頼できるプライマリサーバーの追加」を確認してください。
長期保持ストレージ (Long-term retention storage)	このオプションには、OpenStorage が必要です。テープ、ストレージユニットグループ、および Replication Director はサポートされません。	[編集 (Edit)]をクリックして、クラウドストレージプロバイダを選択します。クラウドプロバイダターゲットを選択したら、[選択したストレージの使用 (Use selected storage)]をクリックします。 クラウドの作業負荷は、複製のストレージユニットとして AdvancedDisk、クラウドストレージ、MSDP、および MSDP-C をサポートします。
トランザクションログのオプション (Transaction log options)	このオプションを設定する場合は、Microsoft SQL Server が必要です。	[カスタムストレージオプションを選択 (Select custom storage options)]オプションを使用する場合は、[編集 (Edit)]をクリックしてバックアップストレージを選択します。

5 [バックアップオプション (Backup options)]で、作業負荷の種類に基づいてすべてのオプションを構成します。この領域に表示されるオプションは、選択した作業負荷、スケジュール、またはストレージのオプションによって変わります。

[クラウド (Cloud)]の作業負荷の場合:

- 選択したクラウドプロバイダオプションのいずれかで[ファイルまたはフォルダの個別リカバリの有効化 (Enable granular recovery for files or folders)]を選択した場合、個別リカバリはスナップショットイメージからしか実行できないため、バックアップスケジュールを追加したときにスナップショットの保持を選択したことを確認してください。
- 選択したクラウドプロバイダオプションのいずれかで[選択したディスクをバックアップから除外 (Exclude selected disks from backups)]を選択した場合、選択したディスクはバックアップされないため、VM は完全にはリカバリされません。除外するディスクで実行中のすべてのアプリケーションが動作しない可能性があります。

メモ: ブートディスクにデータまたは関連付けられているタグがあっても、バックアップからは除外できません。

- クラウドプロバイダに Google Cloud Platform を選択した場合は、[地域別スナップショットを有効にする (Enable regional snapshot)]を選択して、地域別スナップショットを有効にしてください。
  地域別スナップショットオプションが有効になっている場合、資産が存在するのと同じ地域にスナップショットが作成されます。それ以外の場合、スナップショットは複数の地域の場所に作成されます。
- (Microsoft Azure または Azure Stack Hub クラウドプロバイダ) [スナップショットの宛先リソースグループを指定する (Specify snapshot destination resource group)]を選択して、特定のピアリソースグループにスナップショットを関連付けます。このリソースグループは、資産と同じ地域内にあります。スナップショットの宛先の構成、サブスクリプション、リソースグループを選択します。
- VMware 作業負荷の[継続的なデータ保護を有効にする (Enable Continuous data protection)]を選択した場合、リストから継続的なデータ保護ゲートウェイを選択します。[次へ (Next)]をクリックします。
- PaaS 資産を使用するクラウド作業負荷の場合、[バックアップオプション (Backup options)]タブでステージングパス を選択します。これは、RHEL メディアサーバーにある MSDP ユニバーサル共有ストレージのエクスポートパスである必要があります。

メモ: MSDP STU がクラウドストレージに作成されている場合、そのようなストレージサーバーからのユニバーサル共有は DBPaaS 保護計画に一覧表示されません。これは、ユニバーサル共有のバックアップメカニズムでは、クラウドストレージユニットからのユニバーサル共有のバックアップがサポートされないためです。

6 [アクセス権 (Permissions)]で、保護計画へのアクセス権を持つ役割を確認します。

別の役割のアクセス権をこの保護計画に付与するには、[追加 (Add)]をクリックします。表で[役割 (Role)]を選択し、[権限の選択 (Select permissions)]セクションで権限を追加または削除して役割をカスタマイズします。

7 [確認 (Review)]で保護計画の詳細が正しいことを確認し、[完了 (Finish)]をクリックします。

保護計画のカスタマイズ

保護計画を作成した後は、特定の設定のみ変更または構成できます。表 14-1 を参照してください。

表 14-1　構成および変更可能な保護計画の設定

保護計画の設定	設定が利用可能な状況		注意
	計画を編集する場合	資産をサブスクライブする場合	
ストレージオプション (Storage options)	X		
バックアップオプション (Backup options)		X	
詳細オプション (Advanced Options)		X	
スケジュール (Schedules)	X	X	バックアップ処理時間帯のみ。 SQL Server、トランザクションログの頻度、保持期間が対象。
保護対象資産 (Protected assets)		該当なし	
アクセス権 (Permissions)	X	該当なし	役割を追加可能。

保護計画の編集または削除

保護計画の編集

保護計画の[説明 (Description)]、[ストレージオプション (Storage options)]、[スケジュール (Schedules)]を変更できます。

メモ: 保護計画では、[バックアップオプション (Backup options)]と[詳細オプション (Advanced options)]の設定は編集できません。これらの設定や追加のスケジュール設定を調整する場合は、新しい保護計画を作成し、新しい計画に資産をサブスクライブする必要があります。または、資産の計画をカスタマイズできます。

p.101 の「保護計画のカスタマイズ」を参照してください。

保護計画を編集するには

1. 左側で[保護 (Protection)]、[保護計画 (Protection plans)]の順にクリックします。
2. 編集する保護計画の名前をクリックします。
3. 説明を編集するには、[説明を編集 (Edit description)]をクリックします。
4. (オプション) [ストレージオプション (Storage options)]セクションで、[編集 (Edit)]をクリックしてストレージオプションを変更します。

保護計画の削除

すべての資産を保護計画から削除しない限り、保護計画は削除できません。資産の保護を維持する場合は、現在の保護計画を削除する前に、別の保護計画をこれらの資産に追加する必要があります。

p.104 の「保護計画からの資産のサブスクライブ解除」を参照してください。

p.103 の「保護計画への資産または資産グループのサブスクライブ」を参照してください。

p.95 の「保護計画の作成」を参照してください。

保護計画を削除するには

1. 左側で[保護 (Protection)]、[保護計画 (Protection plans)]の順にクリックします。
2. 削除する保護計画のチェックボックスにチェックマークを付けます。
3. [削除 (Delete)]、[はい (Yes)]の順にクリックします。

保護計画への資産または資産グループのサブスクライブ

1 つの資産または資産のグループを、保護計画にサブスクライブできます。1 つの資産または資産のグループを、複数の保護計画にサブスクライブできます。保護計画に資産をサブスクライブする前に、保護計画を作成する必要があります。

NetBackup は、同種のクラウド資産のサブスクリプションをサポートします。保護計画に資産をサブスクライブする際、資産のクラウドプロバイダは、保護計画で定義されているクラウドプロバイダと同じである必要があります。

メモ: 資産のサブスクライブ時に、[ストレージオプション (Storage options)]または[アクセス権 (Permissions)]の設定は編集できません。[スケジュール (Schedules)]に対しては限定的に変更できます。これらの設定を調整する場合は、新しい保護計画を作成し、新しい計画に資産をサブスクライブする必要があります。または、資産の計画をカスタマイズできます。

p.101 の「保護計画のカスタマイズ」を参照してください。

保護計画に資産または資産グループをサブスクライブするには

1. 左側で[作業負荷 (Workloads)]をクリックし、作業負荷の種類をクリックします (VMware など)。
2. 資産タイプを選択します (仮想マシン、インテリジェント VM グループなど)。
3. 1 つ以上の資産を選択します。

4 [保護の追加 (Add protection)]をクリックします。

クラウド作業負荷資産または資産グループを選択した場合、手順 7 に進みます。

5 [保護計画の選択 (Choose a protection plan)]で、保護計画の名前を選択し、[次へ (Next)]をクリックします。

6 (オプション) [バックアップオプション (Backup options)]または[詳細オプション (Advanced options)]のオプションを調整します。

- スケジュール (Schedules)
  完全または増分スケジュールのバックアップの開始時間帯を変更します。
  SQL Server トランザクションログのスケジュールについては、開始時間帯、反復、保持期間を変更できます。
- バックアップオプション (Backup options)
  元の保護計画で設定されているバックアップオプションを調整します。この領域のオプションは作業負荷によって異なります。
- 詳細 (Advanced)
  元の保護計画で設定されているオプションの変更や追加を行います。

変更を行うには、次の権限が必要です。

- 属性の編集 (Edit attributes)。[バックアップオプション (Backup options)]と[詳細 (Advanced)]オプションを編集します。
- 完全および増分スケジュールの編集 (Edit full and incremental schedules)。これらのスケジュール形式の開始時間帯を編集します。
- トランザクションログのスケジュールの編集 (Edit transaction log schedules)。SQL Server トランザクションログのスケジュールの設定を編集します。

7 [保護 (Protect)]をクリックします。

保護計画からの資産のサブスクライブ解除

個別の資産または資産のグループのサブスクライブを、保護計画から解除できます。

メモ: 保護計画から資産のサブスクライブを解除するときに、Web UI で、資産に従来のポリシーが表示される可能性があります。この状況は、保護計画に資産がサブスクライブされており、その資産に対してバックアップが実行される場合に発生することがあります。資産は、有効なバックアップイメージを持ったまま、保護計画からサブスクライブ解除されます。Web UI には従来のポリシーが表示されますが、資産を保護する有効なポリシーがない場合もあります。

保護計画から 1 つの資産のサブスクライブを解除するには

1. 左側で[作業負荷 (Workloads)]をクリックし、作業負荷の種類をクリックします (VMware など)。
2. 1 つの資産タイプを選択します (仮想マシンなど)。
3. 特定の資産名をクリックします。
4. [保護の削除 (Remove protection)]をクリックし、[はい (Yes)]をクリックします。

保護計画から資産のグループのサブスクライブを解除するには

1. 左側で[作業負荷 (Workloads)]をクリックし、作業負荷の種類をクリックします (VMware など)。
2. グループ資産タイプを選択します (インテリジェント VM グループなど)。
3. 特定のグループ資産名をクリックします。
4. [保護の削除 (Remove protection)]をクリックし、[はい (Yes)]をクリックします。

保護計画の上書きの表示

保護計画の権限を設定する際に、作業負荷管理者が保護計画の対象となる資産をカスタマイズできるようにする権限を設定できます。作業負荷管理者は、資産のスケジュールとバックアップオプションの特定の領域に上書きを適用できます。

保護計画の上書きを表示するには

1. 左側で[保護 (Protection)]、[保護計画 (Protection plans)]、保護計画の名前の順にクリックします。
2. [保護対象資産 (Protected assets)]タブで、[カスタム設定 (Custom settings)]列の[適用済み (Applied)]をクリックします。
3. [スケジュール (Schedules)]と[バックアップオプション (Backup options)]タブで、元の設定と新しい設定を確認します。
   - [元 (Original)]: 保護計画を最初に作成したときの設定。
   - [新規 (New)]: その設定の保護計画に対して行われた最後の変更。

今すぐバックアップについて

今すぐバックアップを使用すると、作業負荷管理者はすぐに資産をバックアップできます。たとえば、今すぐバックアップを使って、システムの保守などのスケジュールされていないバックアップの今後のイベントの準備を行うことができます。このバックアップ形式はスケジュールバックアップには依存しないため、今後のバックアップには影響しません。その

他の NetBackup ジョブを管理および監視するのと同じ方法で、今すぐバックアップのジョブの管理と監視を行うことができます。

今すぐバックアップは、次の作業負荷でサポートされています。

- クラウドと PaaS
  NetBackup は、同種のクラウド資産のサブスクリプションをサポートします。保護計画に資産をサブスクライブする際、資産のクラウドプロバイダは、保護計画で定義されているクラウドプロバイダと同じである必要があります。
- Microsoft SQL
- Nutanix AHV
- RHV
- VMware

メモ: 今すぐバックアップを使用するには、少なくとも 1 つの保護計画をサブスクライブする権限を持っている必要があります。今すぐバックアップ操作の各実行で 1 つの資産のみを選択できます。

今すぐバックアップを使用して資産を直ちにバックアップする

資産に対する今すぐバックアップは、資産の一覧から開始できます。たとえば、仮想マシン、インテリジェントグループ、またはデータベースのリストから行えます。または、資産の詳細から今すぐバックアップを開始することもできます。この詳細には、資産がサブスクライブされているすべての保護計画が表示されます。[今すぐバックアップ (Backup now)] は、保護計画のいずれかから選択できます。

今すぐバックアップを使用して資産を直ちにバックアップするには

1. 左側で作業負荷を選択し、バックアップする資産を特定します。
2. [処理 (Actions)]、[今すぐバックアップ (Backup now)]の順に選択します。

3 バックアップの保護計画を選択します。

資産がサブスクライブされているすべての保護計画が一覧表示されます。

どの保護計画にもサブスクライブされていない資産をバックアップするには、[今すぐバックアップ (Backup now)]を選択して既存の保護計画から選択します。また、新しい保護計画を作成してから、[今すぐバックアップ (Backup now)]操作に使用することもできます。

メモ: [バックアップ形式 (Backup type)]オプションは、Microsoft SQL Server の資産に対してのみ使用できます。実行するバックアップ形式は、ドロップダウンリストから選択できます。ドロップダウンには、保護計画で利用可能なバックアップ形式のみが表示されます。

---

4 [バックアップの開始 (Start Backup)]をクリックします。

15

従来のポリシーの管理

この章では以下の項目について説明しています。

ポリシーの追加

次の手順を使用して、NetBackup Web UI でバックアップポリシーを作成します。ポリシーの例もあります。

p.109 の「ポリシーの例 - Exchange Server DAG のバックアップ」を参照してください。

p.110 の「ポリシーの例 - シャード MongoDB クラスタ」を参照してください。

ポリシーオプションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』および適切な作業負荷またはデータベースガイドを参照してください。

メモ: ポリシーを作成および管理するには、RBAC 管理者の役割または同様の権限が必要です。

新しいポリシーを追加する方法

1. 左側で[保護 (Protection)]、[ポリシー (Policies)]の順に選択します。
2. [追加 (Add)]をクリックします。
3. [属性 (Attributes)]タブで、次の操作を実行します。
   - 作成する[ポリシー形式 (Policy type)]を選択します。
   - 作成する[ポリシーストレージ (Policy storage)]を選択します。
   - その他のポリシー属性を選択または構成します。

4 [スケジュール (Schedules)]タブで、必要なすべてのスケジュールを構成します。たとえば、完全および増分スケジュールを構成します。

5 選択したポリシー形式に応じて、保護するクライアント、データベースインスタンス、または仮想マシンを追加します。この構成は[クライアント (Clients)]タブまたは[インスタンスとデータベース (Instances and databases)]タブで実行します。

- ほとんどのポリシー形式の場合、[クライアント (Clients)]タブでクライアントのリストを構成します。
- Oracle および MS-SQL-Server ポリシー形式の場合は、[インスタンスとデータベース (Instances and databases)]タブでインスタンスまたはデータベースを選択します。または、スクリプトやバッチファイルを使用する場合は、[クライアント (Clients)]タブでクライアントを選択します。

6 選択したポリシー形式に応じて、保護するファイル、データベースインスタンス、またはオブジェクトを追加します。この構成は[バックアップ対象 (Backup selections)]タブで実行します。

7 追加のタブがあるポリシー形式については、設定を完了するために必要な他のポリシーオプションを確認および選択してください。

8 [作成 (Create)]をクリックします。

ポリシーの例 - Exchange Server DAG のバックアップ

この例では、Exchange Server DAG のすべてのデータベースをバックアップするポリシーを作成する方法について説明します。

Exchange Server DAG バックアップのポリシーを追加するには

1 左側で[保護 (Protection)]、[ポリシー (Policies)]の順に選択します。

2 [追加 (Add)]をクリックします。

3 [属性 (Attributes)]タブで、次の項目を選択します。

- ポリシー形式 (Policy type): MS-Exchange-Server
- スナップショットバックアップを実行する (Perform snapshot backups): 有効にする必要があります。
- 個別リカバリを有効化する (Enable granular recovery): 任意です。データベースのバックアップから個々のメールボックスおよびパブリックフォルダオブジェクトをリストアする場合は、このオプションを有効にします。
- データベースバックアップソース (Database backup source): データベースのアクティブコピーとパッシブコピーのどちらをバックアップするかを選択します。また、選択したバックアップソースに応じて優先リストを構成します。

4 [スケジュール (Schedules)]タブで、必要なすべてのスケジュールを構成します。たとえば、完全および増分スケジュールを構成します。

名前	種類	間隔	保持
完全バックアップ	完全バックアップ	1 週間	2 週間
増分バックアップ	差分増分	1 日	2 週間

5 [クライアント (Clients)]タブで、1 つ以上の DAG 名を追加します。

クライアント名	ハードウェア	オペレーティングシステム
dag1234.domain.com	Windows-x64	Windows 2016
dag5678.domain.com	Windows-x64	Windows 2016

6 [バックアップ対象 (Backup selections)]タブで、次の指示句を追加します。

```
Microsoft Exchange Database Availability Groups:¥
```

バックアップ対象リスト

Microsoft Exchange Database Availability Groups:¥

7 [作成 (Create)]をクリックします。

ポリシーの例 - シャード MongoDB クラスタ

この例では、シャード MongoDB クラスタ内のプライマリ設定サーバーをバックアップするポリシーを作成する方法について説明します。

MongoDB クラスタバックアップのポリシーを追加するには

1 左側で[保護 (Protection)]、[ポリシー (Policies)]の順に選択します。

2 [追加 (Add)]をクリックします。

3 [属性 (Attributes)]タブで、次の項目を選択します。

- ポリシー形式 (Policy type): BigData

4 [スケジュール (Schedules)]タブで、必要なすべてのスケジュールを構成します。たとえば、完全および増分スケジュールを構成します。

名前	種類	間隔	保持
完全バックアップ	完全バックアップ	1 週間	2 週間
増分バックアップ	差分増分バックアップ	1 日	2 週間

5 [クライアント (Clients)]タブで、クライアント名を追加します。
`MongoDBNode-portnumber` の形式を使用します。

次のリストはポート 1 のプライマリ設定サーバーをバックアップします。

クライアント名	ハードウェア	オペレーティングシステム
primaryconfigserver-01	Linux	Red Hat 2.6.32

6 [バックアップ対象 (Backup selections)]タブで、アプリケーションタイプ、バックアップホストを追加し、手動で ALL_DATABASES 指示句を追加します。

バックアップ対象リスト	注意
Application_Type=mongodb	このパラメータ値では、大文字と小文字が区別されます。
mongodbhost=mongodbhost.domain.com	`Backup_Host=<FQDN_or_hostname>` の形式を使用します。バックアップホストには、NetBackup クライアントまたはメディアサーバーを指定できます。
ALL_DATABASES	

7 [作成 (Create)]をクリックします。

16

バックアップイメージの管理

この章では以下の項目について説明しています。

NetBackup カタログについて

NetBackup Web UI では、カタログユーティリティは、次の操作を実行するために使用します。

- バックアップイメージを検索して、NetBackup カタログに記録された内容でメディアの内容を検証する
- バックアップイメージを複製する
- バックアップイメージを期限切れにする
- 期限切れのバックアップイメージまたは別の NetBackup サーバーからのイメージをインポートする

これらの操作と NetBackup カタログバックアップについて詳しくは、『NetBackup 管理者ガイド、Vol. 1』を参照してください。

バックアップイメージの検索

バックアップイメージを検証、複製、またはインポートするには、まずカタログ内でそれらのイメージを見つける必要があります。

これらの処理と、NetBackup 環境での移動中のデータの暗号化 (DTE) について詳しくは、『NetBackup 管理者ガイド Vol. 1』および『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

バックアップイメージを検索するには

1. 左側の［カタログ (Catalog)］をクリックします。
2. ［処理 (Action)］リストから、次のいずれかを選択します。
   - 検証 (Verify)
   - 複製 (Duplicate)
   - フェーズ 1 インポート (Phase 1 import)
   - フェーズ 2 インポート (Phase 2 import)
3. 検索またはインポートの条件を選択します。
4. ［検索 (Search)］または［インポート (Import)］をクリックします。

検索結果

バックアップイメージを検索すると、イメージリストが画面の下部に表示されます。［列を表示または非表示 (Show or hide columns)］をクリックすると、イメージに関する追加情報が表示されます。

NetBackup Web UI には、コピー DTE モードとコピー階層 DTE モードのイメージ情報も示されます。これらの属性は、コピーまたは親コピーが安全に作成されるかどうかを示します。

17

データ保護アクティビティの一時停止

この章では以下の項目について説明しています。

バックアップおよびその他のアクティビティの一時停止

デフォルトでは、NetBackup またはそのユーザーはデータ保護アクティビティを一時停止できません。バックアップやその他のアクティビティは、スキャンによってイメージまたはリカバリポイント内でマルウェアが検出されても続行されます。データ保護アクティビティには、バックアップ、複製、レプリケーション、およびイメージの有効期限が含まれます。

。

NetBackup および権限を持つユーザーにデータ保護アクティビティの一時停止を許可できます。その後、NetBackup は、特定のクライアントのアクティビティを自動的に一時停止できます。たとえば、スキャンによって特定のクライアントのバックアップイメージまたはリカバリポイントにマルウェアが検出された場合です。スケジュールバックアップやその他の自動アクティビティに一時停止が適用されます。また、これはユーザーが開始する操作にも適用されます。

権限を持つユーザーはデータ保護アクティビティを手動で一時停止できます。これらのユーザーは、データ保護アクティビティを一時停止するために必要なセキュリティ権限を備えた RBAC の役割を持ちます。

NetBackup および権限を持つユーザーにデータ保護アクティビティの一時停止を許可する

NetBackup および権限を持つユーザーに対して、バックアップその他のアクティビティの一時停止を許可したり不許可にしたりできます。

NetBackup および権限を持つユーザーにデータ保護アクティビティの一時停止を許可するには

1. 左側で[保護 (Protection)]、[保護状態 (Protection status)]の順にクリックします。
2. [設定の編集 (Edit settings)]、[編集 (Edit)]の順にクリックします。
3. NetBackup および権限を持つユーザーにデータ保護アクティビティの一時停止を許可するかどうかを、次のように選択します。
   - 許可しない (Do not allow)。NetBackup および権限を持つユーザーは、データ保護アクティビティを一時停止できません。
   - 許可 (Allow)。NetBackup または権限を持つユーザーは、バックアップ、複製、レプリケーションを一時停止できます。必要に応じて、NetBackup またはユーザーにバックアップイメージの有効期限の一時停止を許可できます。

クライアントでのバックアップおよびその他のアクティビティの一時停止

ユーザーは、特定の日付まで、または無期限にクライアントでのバックアップやその他のアクティビティを一時停止できます。この機能は、API エンドポイント `POST/config/blocked-clients/` で利用可能です。

一時停止中のバックアップとその他の一時停止中のアクティビティの表示

データ保護アクティビティが一時停止されているクライアントまたはホストの一覧を表示できます。

一時停止されているデータ保護アクティビティを表示するには

1. 左側で[保護 (Protection)]、[保護状態 (Protection status)]の順にクリックします。
2. このページには、保護アクティビティが一時停止されているクライアントの一覧が表示されます。「自動 (Automatic)」は、NetBackup によって一時停止が自動的に適用されたことを示します。「ユーザーによる開始 (User-initiated)」は、ユーザーが手動で一時停止をクライアントに適用したことを示します。

   設定をまだ構成していない場合は、[設定の編集 (Edit settings)]をクリックします。
3. 特定のクライアントの一時停止の詳細を確認するには、そのクライアント名を見つけます。次に、[処理 (Actions)]、[一時停止の詳細を表示 (View pause details)]の順にクリックします。

データ保護アクティビティの再開

メンテナンスを実行したり、問題を解決したりした後は、クライアントで一時停止されているデータ保護アクティビティを再開できます。この処理は、[保護 (Protection)]、[保護状態 (Protection status)] ノードから実行します。

データ保護アクティビティを再開すると、クライアントでのバックアップを無効にするホストプロパティの設定も無効になります。

クライアントのデータ保護アクティビティを再開するには

1. 左側で[保護 (Protection)]、[保護状態 (Protection status)]の順にクリックします。
2. 1 つ以上のクライアントを選択し、[再開 (Resume)]をクリックします。

5

セキュリティの管理

18

セキュリティイベントと監査ログ

この章では以下の項目について説明しています。

セキュリティイベントと監査ログの表示

NetBackup は、NetBackup 環境でユーザーが開始した処理を監査して、いつ誰が何を変更したかを把握できるようにします。完全な監査レポートについては、nbauditreport コマンドを使用します。p.123 の「詳細な NetBackup 監査レポートの表示」を参照してください。

セキュリティイベントと監査ログを表示するには

1. 左側で、[セキュリティ (Security)]、[セキュリティイベント (Security events)]の順に選択します。
2. 利用可能なオプションは次のとおりです。
   - NetBackup にアクセスしたユーザーを表示するには、[アクセス履歴 (Access history)]をクリックします。
   - NetBackup で監査したイベントを表示するには、[監査イベント (Audit events)]をクリックします。これらのイベントには、セキュリティ設定の変更、証明書、バックアップイメージを閲覧またはリストアしたユーザーが含まれます。

NetBackup の監査について

新規インストールでは監査がデフォルトで有効になります。NetBackup の監査は、NetBackup プライマリサーバーで直接構成できます。

NetBackup の操作を監査すると、次の利点があります。

- NetBackup 環境の予想外の変更を調査するときに、監査記録から推測できます。
- 規制コンプライアンス。
  このレコードはサーベンスオクスリー法 (SOX) で要求されるようなガイドラインに準拠します。
- 内部の変更管理ポリシーに従う手段を提供できます。
- 問題のトラブルシューティングに NetBackup サポートが役立ちます。

NetBackup Audit Manager について

NetBackup Audit Manager (`nbaudit`) はプライマリサーバー上で実行し、監査レコードは EMM (Enterprise Media Manager) データベースに保持されます。

管理者は特に以下を調査できます。

- 処理が実行された日時
- 特定の状況で失敗した処理
- 特定のユーザーが実行した処理
- 特定のコンテンツの領域で実行された処理
- 監査の構成への変更

次の点に注意してください。

- 監査レコードでは、4096 文字を超えるエントリ(ポリシー名など) が切り捨てられます。
- 監査レコードでは、1024 文字を超えるリストアイメージ ID が切り捨てられます。

NetBackup によって監査された処理

NetBackup は、ユーザーが開始した次の処理を記録します。

アクティビティモニターの処理	任意の形式のジョブを取り消すか、中断するか、再開するか、再起動するか、削除すると、監査レコードが作成されます。
アラートと電子メール通知	アラートを生成できないか、NetBackup 構成設定に関する電子メール通知を送信できない場合。たとえば、SMTP サーバーの構成やアラートの除外状態コードのリストなどです。
異常	ユーザーが異常を誤検知として報告すると、そのユーザーの処理が監査され、ログに記録されます。

資産の処理	資産のクリーンアップ処理の一環として vCenter Server などの資産を削除すると、監査されてログに記録されます。 資産グループの作成、変更、削除や、ユーザーに許可されていない資産グループに対するすべての処理は、監査されてログに記録されます。
認証の失敗	NetBackup Web UI、NetBackup API、または拡張監査を使用する場合は、認証の失敗が監査されます。
カタログ情報	この情報には次のものが含まれます。 ■ イメージの検証および期限切れ ■ フロントエンド使用状況データを取得するために送信された要求の読み取り
証明書管理	NetBackup 証明書の作成、無効化、更新、配備、および特定の NetBackup 証明書エラー
証明書検証エラー (CVF)	SSL ハンドシェークエラー、無効化された証明書、またはホスト名の検証エラーが原因で失敗した接続試行。 SSL ハンドシェークと無効化された証明書に関する証明書検証エラー (CVF) の場合、タイムスタンプは個々の証明書の検証が失敗した日時ではなく、監査レコードがプライマリサーバーに送信された日時を示します。CVF 監査レコードには、一定期間の CVF イベントのグループが示されます。レコードの詳細には、監査期間の開始日時と終了日時、およびその期間に発生した CVF の合計数が示されます。
ディスクプールとボリュームプールの処理	ディスクプールまたはボリュームプールの追加、削除、または更新。
保留操作	保留操作の作成、変更および削除。
ホストデータベース	ホストデータベースに関連する NetBackup の操作。
ログオン試行回数	NetBackup 管理コンソール、NetBackup Web UI または NetBackup API へのログオン試行に成功または失敗した回数。
ポリシーの処理	ポリシーの属性、クライアント、スケジュール、バックアップ対象リストの追加、削除、更新。
イメージのユーザー操作のリストアおよび参照	ユーザーが実行する、イメージの内容のリストアおよび参照操作 (`bplist`) はすべて、ユーザー ID によって監査されます。
セキュリティ構成	セキュリティ構成設定に加えられた変更に関連する情報。
リストアジョブの開始	他の形式のジョブが開始されている場合、NetBackup では監査が実行されません。たとえば、バックアップジョブが開始されている場合、NetBackup では監査が実行されません。
NetBackup Audit Manager (`nbaudit`) の起動と停止。	監査機能が無効になっていても、`nbaudit` manager の起動と停止は常に監査されます。

ストレージライフサイクルポリシーの処理。	ストレージライフサイクルポリシー (SLP) の作成、変更、または削除の試行は、監査されてログに記録されます。ただし、nbstlutil コマンドを使用した、SLP のアクティブ化と一時停止は監査されません。これらの操作は、NetBackup グラフィカルユーザーインターフェースまたは API から開始する場合にのみ監査されます。
ストレージサーバーの処理	ストレージサーバーの追加、削除、または更新。
ストレージユニットの処理	ストレージユニットの追加、削除、または更新。 **メモ:** ストレージライフサイクルポリシーと関連している処理は監査されません。
トークン管理	トークンの作成、削除、クリーンアップ、および特定のトークン発行エラー。
ユーザー管理	拡張監査モードでの拡張監査ユーザーの追加と削除。
監査レコードの作成に失敗したユーザー操作	監査が有効な場合、ユーザー操作が監査レコードの作成に失敗すると、監査エラーが nbaudit ログでキャプチャされます。NetBackup 状態コード 108 が返されます (Action succeeded but auditing failed)。NetBackup は、監査が失敗しても終了状態コード 108 を返しません。

NetBackup によって監査されない処理

次の処理は監査されないため、監査レポートに表示されません。

任意の失敗した処理。	NetBackup により、失敗した処理が NetBackup のエラーログに記録されます。失敗した試行で NetBackup のシステム状態が変更されることはないので、失敗した処理は監査レポートに表示されません。
設定変更の影響。	NetBackup の構成への変更の結果は監査されません。たとえば、ポリシーの作成は監査されますが、その作成から生じるジョブは監査されません。
手動で開始されたリストアジョブの完了状態。	リストアジョブの開始は監査されますが、ジョブの完了状態は監査されません。手動で開始されたかどうかにかかわらず、他のどのジョブ形式の完了状態も監査されません。完了の状態はアクティビティモニターに表示されます。
内部的に開始された処理	NetBackup によって開始された内部処理は監査されません。たとえば、期限切れのイメージのスケジュールされた削除、定時バックアップ、または定期的なイメージデータベースのクリーンアップは監査されません。
ロールバック操作	一部の操作は、複数の手順として実行されます。たとえば、MSDP ベースのストレージサーバーの作成は、複数の手順で構成されています。成功したすべての手順が監査されます。いずれかの手順が失敗するとロールバックという結果になります。または、成功した手順を取り消す必要がある場合もあります。監査レコードはロールバック操作についての詳細を含んでいません。
ホストプロパティの処理	bpsetconfig や nbsetconfig コマンド、またはホストプロパティ内の同等のプロパティを使用して加えられた変更は監査されません。bp.conf ファイルまたはレジストリに直接加えられた変更は監査されません。

監査レポートのユーザーの ID

監査レポートは特定の処理を実行したユーザーの識別情報を示します。ユーザーの完全な ID には、ユーザー名と、認証されたユーザーに関連付けられているドメインまたはホスト名が含まれています。ユーザーの ID は、監査レポートに次のように表示されます。

- 監査イベントには、常にユーザーの完全な ID が含まれます。root ユーザーや管理者は、「root@hostname」または「administrator@hostname」として記録されます。
- NetBackup 8.1.2 以降では、イメージの参照イベントとイメージのリストアイベントには、監査イベントに常にユーザー ID が含まれます。NetBackup 8.1.1 以前では、これらのイベントは「root@hostname」または「administrator@hostname」として記録されます。
- ユーザープリンシパルの要素の順序は「`domain:username:domainType:providerId`」です。ドメイン値は Linux コンピュータには適用されません。このプラットフォームの場合、ユーザープリンシパルは `:username:domainType:providerId` です。
- クレデンシャルを必要としないすべての操作や、ユーザーにサインインを求めるすべての操作の場合、操作はユーザー ID なしで記録されます。

監査保持期間と監査レコードのカタログバックアップ

監査レコードは、保持期間に示されている期間、NetBackup データベースの一部として保持されます。監査レコードのバックアップは、NetBackup カタログバックアップの一環として作成されます。NetBackup 監査サービス (`nbaudit`) では、午前 12 時 (現地時間) に期限切れの監査レコードを 24 時間ごとに一度削除します。

デフォルトでは、監査レコードは 90 日間保持されます。監査レコードを削除しない場合は、監査保持期間の値を `0` (ゼロ) に設定します。

監査保持期間を設定するには

1. プライマリサーバーにログオンします。
2. 次のディレクトリを開きます。

   Windows の場合: *install_path*¥NetBackup¥bin¥admincmd

   UNIX の場合: /usr/openv/netbackup/bin/admincmd
3. 次のコマンドを入力します。

   ```
   nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD
   number_of_days -machinename primaryserver
   ```

   number_of_days は、監査レポート用に監査レコードを保持する期間 (日数) を示します。

   次の例では、ユーザー操作のレコードは 30 日間保持されてから削除されます。

   ```
   nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD 30
   -machinename server1
   ```

   カタログバックアップで監査レコードが抜け落ちないようにするには、カタログバックアップの間隔を -AUDIT_RETENTION_PERIOD の値以下に設定します。

詳細な NetBackup 監査レポートの表示

詳細な監査レポートを表示するには

1. プライマリサーバーにログオンします。
2. 次のコマンドを入力して、監査レポートを概略形式で表示します。

   Windows の場合: *install_path*¥NetBackup¥bin¥admincmd¥nbauditreport

   UNIX の場合: /usr/openv/netbackup/bin/admincmd¥nbauditreport

   または、次のオプションを使用してコマンドを実行します。

-sdate <"MM/DD/YY [HH:[MM[:SS]]]">	表示するレポートデータの開始日時。
-edate <"MM/DD/YY [HH:[MM[:SS]]]">	表示するレポートデータの終了日時。

-ctgy *category*	実行されたユーザー操作のカテゴリ。POLICY のようなカテゴリには、スケジュールやバックアップ対象などのいくつかのサブカテゴリが含まれることがあります。サブカテゴリに加えられた変更はすべて、プライマリカテゴリの変更としてリストされます。 -ctgy オプションについては、『NetBackup コマンドガイド』を参照してください。
-user <*username*[:*domainname*]>	監査情報を表示するユーザーの名前を指定するために使用します。
-fmt DETAIL	-fmt DETAIL オプションは監査情報の総合的なリストを表示します。たとえば、ポリシーが変更されると、属性の名前、古い値と新しい値がリストされます。このオプションには、次のサブオプションを設定できます。 ■ [-notruncate] 。レポートの詳細セクションの別々の行に、変更された属性の古い値と新しい値を表示します。 ■ [-pagewidth <NNN>] 。レポートの詳細セクションのページ幅を設定します。
-fmt PARSABLE	-fmt PARSABLE オプションは DETAIL レポートと同じセットの情報を解析可能な形式で表示します。レポートでは、監査レポートデータ間の解析トークンとしてパイプ文字 (|) を使用します。このオプションには、次のサブオプションを設定できます。 ■ [-order<DTU|DUT|TDU|TUD|UDT|UTD>]。情報を表示する順序を示します。 D (説明) T (タイムスタンプ) U (ユーザー)

3 監査レポートは次の詳細を含んでいます。

DESCRIPTION	実行された処理の詳細。
USER	処理を実行したユーザーの ID。 p.122 の「監査レポートのユーザーの ID」を参照してください。
TIMESTAMP	処理が実行された時間。

-fmt DETAIL または -fmt PARSABLE オプションを使用する場合にのみ、次の情報が表示されます。

CATEGORY	実行されたユーザー操作のカテゴリ。
ACTION	実行された処理。
REASON	処理が実行された理由。変更を加えた操作に理由が指定されている場合に表示されます。
DETAILS	すべての変更の詳細。古い値と新しい値をリストします。

監査レポートの例:

```
[root@server1 admincmd]# ./nbauditreport
TIMESTAMP            USER           DESCRIPTION
04/20/2018 11:52:43  root@server1   Policy 'test_pol_1' was saved but no changes were
detected
04/20/2018 11:52:42  root@server1   Schedule 'full' was added to Policy 'test_pol_1'
04/20/2018 11:52:41  root@server1   Policy 'test_pol_1' was saved but no changes were
detected
04/20/2018 11:52:08  root@server1   Policy 'test_pol_1' was created
04/20/2018 11:17:00  root@server1   Audit setting(s) of master server 'server1' were
modified

Audit records fetched: 5
```

システムログへの監査イベントの送信

システムログに NetBackup 監査イベントを送信できます。このタスクを実行するには、次の権限があることを確認します。

- [セキュリティ (Security)]、[セキュリティイベント (Security events)]UI の表示権限
- [NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)] UI の表示、作成、更新、削除の権限

システムログに監査イベントを送信するには

1. 左側で、[セキュリティ(Security)]、[セキュリティイベント(Security events)]の順に選択します。
2. 右上で、[監査イベント設定 (Audit event settings)]をクリックします。
3. [監査イベントをシステムログに送信する (Send the audit events to the system logs)]オプションを有効にします。
4. [監査イベントカテゴリ (Audit event categories)]ダイアログボックスで、監査イベントをシステムログに送信する監査カテゴリを選択します。

   すべての監査カテゴリの監査イベントをシステムログに送信するには、[監査イベントカテゴリ (Audit event categories)]チェックボックスにチェックマークを付けます。
5. [保存 (Save)]をクリックします。

   システムログで NetBackup 監査イベントを表示できます。例:

   Windows システムでは、[Windows イベントビューア]を使用して NetBackup 監査イベントを表示します。

   Linux システムでは、構成された場所のシステムログを表示できます。

19

セキュリティ証明書の管理

この章では以下の項目について説明しています。

NetBackup のセキュリティ管理と証明書について

NetBackup はセキュリティ証明書を使用して NetBackup ホストを認証します。これらの証明書は X.509 公開鍵のインフラストラクチャ (PKI) 標準に適合している必要があります。NetBackup 8.1、8.1.1、8.1.2 では、安全な通信を行うために NetBackup 証明書が使用されます。NetBackup 8.2 以降では、NetBackup 証明書または外部証明書を使用できます。

NetBackup 証明書はデフォルトでホストに対して発行され、NetBackup プライマリサーバーは CA として動作し、証明書失効リスト (CRL) を管理します。NetBackup 証明書の配備のセキュリティレベルにより、証明書が NetBackup ホストに配備される方法と、各ホストで CRL が更新される頻度が決定されます。ホストに新しい証明書が必要な場合 (元の証明書の期限切れまたは無効化などの場合) は、NetBackup 認証トークンを使って証明書を再発行できます。

外部証明書とは、信頼できる外部 CA が署名した証明書です。外部証明書を使うように NetBackup を構成すると、NetBackup ドメイン内のプライマリサーバー、メディアサーバー、クライアントは、外部証明書を安全な通信のために使用します。さらに、NetBackup Web サーバーもこれらの証明書を NetBackup Web UI と NetBackup ホスト間の通信に使用します。外部証明書の配備、外部証明書の更新と置換、外部 CA の CRL の管理は、NetBackup 以外で管理されます。

外部証明書について詳しくは、『NetBackup セキュリティと暗号化ガイド』を参照してください。

NetBackup 8.1 以降のホストのセキュリティ証明書

NetBackup 8.1 以降のホストは、セキュアモードでのみ相互に通信できます。NetBackup のバージョンに応じて、これらのホストには NetBackup CA が発行した証明書、またはその他の信頼できる CA が発行した証明書が必要です。制御チャネルを介した安全な通信に使用される NetBackup 証明書は、ホスト ID ベースの証明書とも呼ばれます。

NetBackup 8.0 のホストのセキュリティ証明書

NetBackup が 8.0 のホスト向けに生成したすべてのセキュリティ証明書は、ホスト名ベースの証明書と呼ばれます。これらの証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup ホスト ID とホスト ID ベースの証明書

NetBackup ドメインの各ホストには、ホスト ID または汎用固有識別子 (UUID) として参照される固有の ID が割り当てられます。ホスト ID はホストを識別するために多くの操作で使われます。NetBackup は、次のようにホスト ID を作成して管理します。

- プライマリサーバーで証明書のあるすべてのホスト ID のリストを保持します。
- ホスト ID をランダムに生成します。これらの ID は、どのハードウェアのプロパティにも関連付けられていません。
- デフォルトでは、NetBackup 8.1 以降は、NetBackup 認証局によって署名されたホスト ID ベースの証明書をホストします。
- ホスト ID はホスト名を変更しても変更されません。

場合によっては、ホストが複数のホスト ID を持つことができます。

- ホストが複数の NetBackup ドメインから証明書を取得する場合、そのホストは各 NetBackup ドメインに対応するホスト ID を複数持つことになります。
- プライマリサーバーをクラスタの一部として構成する場合、クラスタの各ノードが一意のホスト ID を受け取ります。仮想名には、追加のホスト ID が割り当てられます。たとえば、プライマリサーバークラスタが *N* 個のノードで構成される場合、そのプライマリサーバークラスタに割り当てられるホスト ID の数は *N* + 1 個になります。

NetBackup セキュリティ証明書の管理

メモ: ここに示される情報は、NetBackup 認証局 (CA) によって発行されたセキュリティ証明書に対してのみ適用されます。外部証明書の詳細を確認できます。

p.133 の「NetBackup での外部セキュリティ証明書の使用」を参照してください。

NetBackup 証明書を表示または無効化したり、NetBackup CA に関する情報を確認できます。NetBackup 証明書の管理と証明書の配備について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup 証明書の表示

NetBackup ホストに対して発行された、すべてのホスト ID ベースの NetBackup 証明書の詳細を表示できます。8.1 以降の NetBackup ホストのみでホスト ID ベースの証明書を使用できることに注意してください。[証明書 (Certificates)]リストに NetBackup 8.0 以前のホストは含まれません。

NetBackup 証明書を表示するには

1. 左側で、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
2. [NetBackup 証明書 (NetBackup certificates)]をクリックします。
3. ホストの追加証明書の詳細を表示するには、ホスト名をクリックします。

NetBackup CA 証明書の無効化

NetBackup のホスト ID ベースの証明書を無効化すると、NetBackup はそのホストの他の証明書をすべて無効化します。NetBackup はホストを信頼しなくなり、このホストは他の NetBackup ホストと通信できなくなります。

さまざまな状況下でホスト ID ベースの証明書を無効化するように選択できます。たとえば、クライアントセキュリティの危殆化を検出した場合、クライアントが廃止された場合、NetBackup がホストからアンインストールされた場合などが該当します。無効化した証明書を使ってプライマリサーバー Web サービスと通信することはできません。

セキュリティのベストプラクティスとして、NetBackup セキュリティ管理者には、アクティブではなくなったホストの証明書の明示的な無効化が推奨されます。この処理は、証明書がホストにまだ配備されているかどうかとは関係なく実行してください。

メモ: プライマリサーバーの証明書は無効化しないでください。無効化すると、NetBackup の操作が失敗する可能性があります。

NetBackup CA 証明書を無効化するには

1. 左側で、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
2. [NetBackup 証明書 (NetBackup certificates)]をクリックします。
3. 無効化する証明書に関連付けられているホストを選択します。
4. [証明書の無効化 (Revoke certificate)]、[はい (Yes)]の順にクリックします。

NetBackup 認証局の詳細と指紋の表示

プライマリサーバーの NetBackup 認証局 (CA) と安全に通信するために、ホストの管理者は、個々のホストのトラストストアに CA 証明書を追加する必要があります。プライマリサーバーの管理者は、個々のホストの管理者に CA 証明書の指紋を提供する必要があります。

NetBackup 認証局の詳細と指紋を表示するには

1. 左側で、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
2. [NetBackup 証明書 (NetBackup certificates)]をクリックします。
3. ツールバーで、[認証局 (Certificate authority)]をクリックします。
4. 指紋の情報を見つけて、[クリップボードにコピー (Copy to clipboard)]をクリックします。
5. この指紋情報をホストの管理者に提供します。

NetBackup 証明書の再発行

メモ: ここに示される情報は、NetBackup 認証局 (CA) によって発行されたセキュリティ証明書に対してのみ適用されます。外部証明書は NetBackup 以外で管理する必要があります。

ホストの NetBackup 証明書が有効でなくなることがあります。たとえば、証明書の期限が切れた場合、失効した場合、またはなくなった場合などです。再発行トークンを使用して、または使用せずに、証明書を再発行できます。

再発行トークンは、NetBackup 証明書を再発行するために使用する認証トークンの種類です。証明書を再発行すると、ホストは、元の証明書と同じホスト ID を取得します。

トークンを使用した NetBackup 証明書の再発行

ホストの NetBackup 証明書を再発行する必要がある場合、NetBackup はこの再発行を実行するためのより安全な方法を提供します。ホストの管理者が新しい証明書を取得するために使用する必要のある、認証トークンを作成できます。この再発行トークンは、元の証明書と同じホスト ID を保持します。トークンは、1 回のみ使用できます。特定のホストに関連付けられているため、このトークンは、他のホストの証明書を要求するためには使用できません。

ホストの NetBackup 証明書を再発行するには

1. 左側で、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
2. [NetBackup 証明書 (NetBackup certificates)]をクリックします。
3. ホストを選択し、[処理 (Actions)]、[再発行トークンの生成 (Generate reissue token)]の順にクリックします。

4 トークン名を入力し、トークンの有効期間を指定します。

5 [作成 (Create)]をクリックします。

6 [クリップボードにコピー (Copy to clipboard)]をクリックして、[閉じる (Close)]をクリックします。

7 ホストの管理者が新しい証明書を取得できるように、認証トークンを共有します。

トークンなしの NetBackup 証明書の再発行の許可

場合によっては、再発行トークンなしで証明書を再発行する必要があります。たとえば、BMR クライアントのリストアの場合です。[証明書の自動再発行を許可する (Allow auto reissue certificate)]オプションを使用すると、トークンがなくても証明書を再発行できます。

トークンなしの NetBackup 証明書の再発行を許可するには

1 左側で、[ホスト (Hosts)]、[ホストマッピング (Host mappings)]の順に選択します。

2 ホストを特定し、[処理 (Actions)]、[証明書の自動再発行を許可する (Allow auto reissue certificate)]、[許可 (Allow)]の順にクリックします。

[証明書の自動再発行を許可する (Allow auto reissue certificate)]オプションを設定すると、デフォルト設定では、48 時間以内はトークンなしで証明書を再発行できます。この再発行の期間が経過した後は、証明書の再発行操作に再発行トークンが必要になります。

3 トークンなしの NetBackup 証明書の再発行を許可したことを、ホストの管理者に通知します。

トークンなしで NetBackup 証明書を再発行する機能の無効化

トークンなしの NetBackup 証明書の再発行を許可した後、再発行の有効期限が切れる前に、この機能を無効にできます。デフォルトでは、この期限は 48 時間です。

トークンなしで NetBackup 証明書を再発行する機能を無効化するには

1 左側で、[ホスト (Hosts)]、[ホストマッピング (Host mappings)]の順に選択します。

2 ホストを特定し、[処理 (Actions)]、[証明書の自動再発行を無効にする (Revoke auto reissue certificate)]の順にクリックします。

NetBackup 証明書の認証トークンの管理

メモ: ここに示される情報は、NetBackup 認証局 (CA) によって発行されたセキュリティ証明書に対してのみ適用されます。外部証明書は NetBackup 以外で管理する必要があります。

NetBackup 証明書配備のセキュリティレベルによっては、ホストに新しい NetBackup 証明書を発行するために、認証トークンが必要になる場合があります。必要な場合にトークンを作成したり、再度必要になった場合に、トークンを検索してコピーしたりできます。不要になったトークンは、クリーンアップまたは削除できます。

証明書を再発行するには、ほとんどの場合、再発行トークンが必要です。再発行トークンは、ホスト ID に関連付けられています。

認証トークンの作成

NetBackup 証明書配備のセキュリティレベルに応じて、プライマリ以外の NetBackup ホストは、ホスト ID ベースの NetBackup 証明書を取得するために認証トークンを必要とする場合があります。プライマリサーバーの NetBackup 管理者はトークンを生成し、それをプライマリホスト以外のホストの管理者と共有します。その管理者は、プライマリサーバーの管理者の立ち会いなしで証明書を配備できます。

紛失、破損、または期限切れのため証明書が現時点で有効でない状態の NetBackup ホストには、認証トークンを作成しないでください。このような場合は、再発行トークンを使う必要があります。

p.130 の「NetBackup 証明書の再発行」を参照してください。

認証トークンを作成するには

1. 左側で、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。
2. 左上の[追加 (Add)]をクリックします。
3. トークンの次の情報を入力します。
   - トークン名
   - トークンを使用する最大回数
   - トークンの有効期間
4. [作成 (Create)]をクリックします。

認証トークンの値を検索してコピーするには

作成したトークンの詳細を参照し、今後使用するためにトークンの値をコピーできます。

認証トークンの値を検索してコピーするには

1. 左側で、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。
2. 詳細を表示するトークンの名前を選択します。
3. 右上で[トークンの表示 (Show Token)]、[クリップボードにコピー (Copy to clipboard)]アイコンの順にクリックします。

トークンのクリーンアップ

トークンのクリーンアップユーティリティを使用して、有効期限が切れたトークンや、許可された最大使用数に到達したトークンをトークンのデータベースから削除します。

トークンをクリーンアップするには

1. 左側で、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。
2. [クリーンアップ (Cleanup)]、[はい (Yes)]の順にクリックします。

トークンの削除

トークンは、期限切れになる前、または[最大許可使用期間 (Maximum Uses Allowed)]に達する前に削除できます。

トークンを削除するには

1. 左側で、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。
2. 削除するトークンの名前を選択します。
3. 右上の[削除 (Delete)]をクリックします。

NetBackup での外部セキュリティ証明書の使用

NetBackup 8.2 以降のバージョンでは、外部 CA が発行したセキュリティ証明書をサポートします。外部認証局の外部証明書と証明書失効リストは、NetBackup の外部で管理する必要があります。[外部証明書 (External certificates)]タブには、ドメイン内の NetBackup 8.1 以降のホストの詳細と、外部証明書を使用するかどうかが表示されます。

[証明書 (Certificates)]、[外部証明書 (External certificates)]で外部証明書情報を表示する前に、まず、外部証明書を使用するようにプライマリサーバーと NetBackup Web サーバーを構成する必要があります。

p.133 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。

詳しくは、NetBackup での外部 CA のサポートに関するビデオをご覧ください。

NetBackup Web サーバーで外部証明書を使用するための構成

デフォルトでは、NetBackup は NetBackup CA が発行したセキュリティ証明書を使用します。外部 CA が発行した証明書がある場合、安全な通信のために、それを使用するように NetBackup Web サーバーを構成できます。

メモ: Windows 証明書ストアは、NetBackup Web サーバーの証明書ソースとしてサポートされていません。

Web サーバーで外部証明書を使用するように構成するには

1. 有効な証明書、証明書の秘密鍵、信頼できる CA バンドルがあることを確認します。
2. 次のコマンドを実行します。

   ```
   configureWebServerCerts -addExternalCert -nbHost -certPath
   certificate path -privateKeyPath private key path -trustStorePath
   CA bundle path [-passphrasePath passphrase file path]
   ```

   configureWebServerCerts コマンドでは、Windows 証明書ストアのパスの使用はサポートされていません。

   コマンドラインオプションについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

   - クラスタ化されたセットアップでは、フェールオーバーを避けるために、アクティブノードで次のコマンドを実行します。

     install_path/netbackup/bin/bpclusterutil -freeze

3. NetBackup Web 管理コンソールサービスを再起動して変更を反映します。

   UNIX では、次のコマンドを実行します。

   - *install_path*/netbackup/bin/nbwmc -terminate
   - *install_path*/netbackup/bin/nbwmc start

   Windows では、[コントロールパネル]で[サービス]を使用します。

   コマンドの場所:

Windows の場合	*install_path*¥NetBackup¥wmc¥bin¥install¥
UNIX の場合	*install_path*/wmc/bin/install

   - クラスタ化されたセットアップでは、次のコマンドをアクティブノードで使用してクラスタを解凍します。

     install_path/netbackup/bin/bpclusterutil -unfreeze

4. ブラウザを使用して、証明書の警告メッセージが表示されずに NetBackup Web ユーザーインターフェースにアクセスできることを確認します。

Web サーバー用に構成された外部証明書の削除

Web サーバー用に構成された外部証明書を削除できます。NetBackup は、NetBackup CA が署名した証明書を使用して、安全な通信を行います。

Web サーバー用に構成された外部証明書を削除するには

1 次のコマンドを実行します (クラスタ化されたプライマリサーバーのセットアップでは、このコマンドをアクティブノードで実行します)。

```
configureWebServerCerts -removeExternalCert -nbHost
```

- クラスタ化されたプライマリサーバーのセットアップでは、フェールオーバーを避けるために、次のコマンドをアクティブノードで実行してクラスタを凍結します。

  install_path/netbackup/bin/bpclusterutil -freeze

2 NetBackup Web 管理コンソールサービスを再起動します。

- クラスタ化されたプライマリサーバーのセットアップでは、次のコマンドをアクティブノードで実行してクラスタを解凍します。

  install_path/netbackup/bin/bpclusterutil -unfreeze

Web サーバー用外部証明書のアップデートまたは更新

Web サーバー用に構成された外部証明書をアップデートまたは更新できます。

Web サーバー用外部証明書をアップデートまたは更新するには

1 最新の外部証明書、一致する秘密鍵、CA バンドルファイルがあることを確認します。

2 次のコマンドを実行します (クラスタ化されたセットアップでは、このコマンドをアクティブノードで実行します)。

```
configureWebServerCerts -addExternalCert -nbHost -certPath
certificate path -privateKeyPath private key path -trustStorePath
CA bundle path
```

ドメイン内の NetBackup ホストの外部証明書情報の表示

メモ: 外部証明書の情報を表示するには、外部証明書用に NetBackup を構成する必要があります。詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup ドメイン内のホストに外部証明書を追加すると、[外部証明書 (External certificates)]ダッシュボードを使用して、注意が必要なホストを追跡できます。外部証明書をサポートするには、ホストをアップグレードして外部証明書を使用して登録する必要があります。

ホストの外部証明書の情報を表示するには

1 左側で、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。

2 [外部証明書 (External certificates)]をクリックします。

ホスト情報、ホストの外部証明書の詳細に加え、次の情報が示されます。

- ［NetBackup 証明書の状態 (NetBackup certificate status)］列には、ホストに NetBackup 証明書もあるかどうかが示されます。
- ［外部証明書 (External certificate)］ダッシュボードには、NetBackup 8.1 以降のホストに関する次の情報が含まれています。
  - ホストの合計。ホストの合計数です。ホストはオンラインになっており、NetBackup プライマリサーバーと通信できる必要があります。
  - 証明書があるホスト。NetBackup プライマリサーバーで有効な外部証明書が登録されているホストの数を示します。
  - 証明書がないホスト。ホストは外部証明書をサポートしていますが、登録されていません。または、ホストを NetBackup 8.2 にアップグレードする必要があります (バージョン 8.1、8.1.1、または 8.1.2 に該当)。［NetBackup アップグレード必要数 (NetBackup upgrade required)］の合計数には、リセットされたホストや NetBackup のバージョンが不明なホストも含まれています。NetBackup 8.0 以前のホストはセキュリティ証明書を使用しないため、ここには反映されません。
  - 証明書の有効期限。期限が切れた、または期限切れ間近の外部証明書があるホストを示します。

ホストの外部証明書の詳細の表示

外部認証局によって発行された証明書の詳細を表示できます。

ホストの外部証明書の詳細を表示するには

1. 左側で、［セキュリティ (Security)］、［証明書 (Certificates)］の順に選択します。
2. ［外部証明書 (External certificates)］をクリックします。

   プライマリサーバーの外部証明書のリストが表示されます。
3. ホストの追加証明書の詳細を表示するには、ホスト名をクリックします。

20

ホストマッピングの管理

この章では以下の項目について説明しています。

- ホストのセキュリティとマッピングに関する情報の表示
- 複数のホスト名を持つホストのマッピングの承認または追加
- 複数のホスト名を持つホストのマッピングの削除

ホストのセキュリティとマッピングに関する情報の表示

[ホストマッピング (Host mappings)]の[ホスト (Hosts)]情報には、プライマリサーバー、メディアサーバー、クライアントなど、環境内の NetBackup ホストに関する詳細情報が含まれています。ホスト ID を持つホストのみがこのリストに表示されます。ホスト名には、ホストのプライマリ名とも呼ばれる、ホストの NetBackup クライアント名が反映されます。

メモ: NetBackup は、すべての動的 IP アドレス (DHCP、つまり動的ホスト構成プロトコルのホスト) を検出し、ホスト ID にこれらのアドレスを追加します。これらのマッピングは削除する必要があります。

8.0 以前の NetBackup ホストのホスト名ベースの証明書の場合は、対応するバージョンの『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup ホスト情報を表示するには

1. 左側で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に選択します。

   このホストにマップされているセキュリティ状態とその他のホスト名を確認します。

2. このホストについて詳しくは、ホストの名前をクリックします。

複数のホスト名を持つホストのマッピングの承認または追加

NetBackup ホストは、複数のホスト名を持つことができます。たとえば、プライベート名とパブリック名の両方を設定したり、短縮名と完全修飾ドメイン名 (FQDN) を設定する場合があります。NetBackup ホストが、環境内の別の NetBackup ホストと 1 つの名前を共有する場合もあります。NetBackup は、クラスタの仮想名のホスト名や完全修飾ドメイン名 (FQDN) を含む、クラスタ名も検出します。

p.140 の「クラスタの自動検出マッピングの例」を参照してください。

p.141 の「複数 NIC 環境でのクラスタ用に自動検出されたマッピングの例」を参照してください。

p.141 の「SQL Server 環境の自動検出マッピングの例」を参照してください。

ホストの NetBackup クライアント名 (つまりプライマリ名) は、証明書の配備中にそのホスト ID に自動的にマッピングされます。NetBackup ホスト間で通信が正常に行われるために、NetBackup は、すべてのホストをその別名とも自動的にマッピングします。ただし、この方法ではセキュリティが低下します。代わりに、この設定を無効にできます。その後、NetBackup が検出する個別のホスト名のマッピングを手動で承認することを選択できます。

p.149 の「NetBackup ホスト名の自動マッピングの無効化」を参照してください。

NetBackup が検出するホストマッピングの承認

NetBackup は、環境内の NetBackup ホストに関連付けられている、多くの共有名またはクラスタ名を自動的に検出します。[承認するマッピング (Mappings to approve)]タブを使用して、関連するホスト名を確認して受け入れます。[ホスト名を NetBackup ホスト ID に自動的にマッピングする (Automatically map host names to their host ID)]が有効になっている場合、[承認するマッピング (Mappings to approve)]リストには、他のホストと競合するマッピングのみが表示されます。

メモ: すべての利用可能なホスト名を、関連付けられたホスト ID にマッピングする必要があります。証明書をホストに配備する場合、ホスト名は関連付けられているホスト ID にマッピングされている必要があります。そうでない場合、NetBackup はそのホストを別のホストと見なします。NetBackup はその後、新しい証明書をホストに配備し、新しいホスト ID を発行します。

NetBackup が検出したホスト名を承認するには

1. 左側で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に選択します。
2. [承認するマッピング (Mappings to approve)]タブをクリックします。

3 ホストの名前をクリックします。

4 検出されたマッピングを使用する場合は、ホストのマッピングを確認して[承認 (Approve)]をクリックします。

ホストとのマッピングを関連付けない場合は、[拒否 (Reject)]をクリックします。

拒否されたマッピングは、NetBackup によって再度検出されるまでリストに表示されません。

5 [保存 (Save)]をクリックします。

ホストへの別のホスト名のマッピング

NetBackup ホストをそのホスト名に手動でマッピングできます。このマッピングを行うことで、NetBackup は、別の名前を使用してホストと正常に通信できます。

ホストにホスト名をマッピングするには

1 左側で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に選択します。

2 ホストを選択し、[マッピングの管理 (Manage mappings)]をクリックします。

3 [追加 (Add)]をクリックします。

4 ホスト名または IP アドレスを入力し、[保存 (Save)]をクリックします。

5 [閉じる (Close)]をクリックします。

複数の NetBackup ホストへの共有名またはクラスタ名のマッピング

複数の NetBackup ホストが 1 つのホスト名を共有する場合は、共有名またはクラスタ名のマッピングを追加します。例として、クラスタ名の場合を取り上げます。

共有名またはクラスタ名のマッピングを作成する前に、次のことに注意してください。

- NetBackup は、多数の共有名またはクラスタ名を自動的に検出します。[承認するマッピング (Mappings to approve)]タブを確認します。
- マッピングが、安全でないホストと安全なホストの間で共有されている場合、NetBackup はマッピング名が安全であると想定します。ただし、ランタイムにマッピングが安全でないホストに解決される場合、接続は失敗します。たとえば、安全なホスト (ノード 1) と安全でないホスト (ノード 2) を持つ、2 ノードクラスタがあると想定します。この場合、ノード 2 がアクティブノードである場合は、接続が失敗します。

共有名またはクラスタ名を複数の NetBackup ホストにマッピングするには

1. 左側で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に選択します。
2. [共有マッピングまたはクラスタマッピングの追加 (Add shared or cluster mappings)]をクリックします。
3. 2 つ以上の NetBackup ホストにマッピングする共有ホスト名またはクラスタ名を入力します。

   たとえば、環境内の NetBackup ホストに関連付けられているクラスタ名を入力します。
4. 右側の[追加 (Add)]をクリックします。
5. 追加する NetBackup ホストを選択して、[リストに追加 (Add to list)]をクリックします。

   たとえば、手順 3 でクラスタ名を入力した場合は、ここでクラスタ内のノードを選択します。
6. [保存 (Save)]をクリックします。

クラスタの自動検出マッピングの例

たとえば、ホスト `client01.lab04.com` と `client02.lab04.com` で構成されるクラスタの場合は、次のエントリが表示される可能性があります。各ホストについて、有効なマッピングを承認します。

ホスト	自動検出されたマッピング
client01.lab04.com	client01
client01.lab04.com	clustername
client01.lab04.com	clustername.lab04.com
client02.lab04.com	client02
client02.lab04.com	clustername
client02.lab04.com	clustername.lab04.com

有効なマッピングをすべて承認すると、次のエントリと類似するマッピングされたホストの設定が表示されます。

ホスト	マッピング済みのホスト名/IP アドレス (Mapped Host Names / IP Addresses)
client01.lab04.com	client01.lab04.com、client01、clustername、clustername.lab04.com
client02.lab04.com	client02.lab04.com、client02、clustername、clustername.lab04.com

複数 NIC 環境でのクラスタ用に自動検出されたマッピングの例

複数 NIC 環境のクラスタのバックアップには、特別なマッピングが必要です。クラスタノードの名前を、プライベートネットワーク上のクラスタの仮想名にマッピングする必要があります。

表 20-1 複数 NIC 環境のクラスタ用にマッピングされたホスト名

ホスト	マッピング済みのホスト名
Node 1 のプライベート名	プライベートネットワーク上のクラスタの仮想名
Node 2 のプライベート名	プライベートネットワーク上のクラスタの仮想名

たとえば、ホスト `client01-bk.lab04.com` と `client02-bk.lab04.com` で構成される複数 NIC 環境のクラスタの場合は、次のエントリが表示される可能性があります。各ホストについて、有効なマッピングを承認します。

ホスト	自動検出されたマッピング
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

有効なマッピングをすべて承認すると、次のエントリと類似するマッピングされたホストの設定が表示されます。

ホスト	マッピング済みのホスト名/IP アドレス (Mapped Host Names / IP Addresses)
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

SQL Server 環境の自動検出マッピングの例

表 20-2では、FCI は SQL Server フェールオーバークラスタインスタンスを意味します。WSFC は Windows Server フェールオーバークラスタを意味します。

表 20-2 SQL Server 環境用にマッピングされたホスト名の例

環境	ホスト	マッピング済みのホスト名
FCI (2 つのノードから成るクラスタ)	*Node 1* の物理名	SQL Server クラスタの仮想名
	Node 2 の物理名	SQL Server クラスタの仮想名
基本または高度可用性グループ (プライマリとセカンダリ)	プライマリ名	WSFC 名
	セカンダリ名	WSFC 名
1 つの FCI (プライマリ FCI またはセカンダリ FCI) から成る基本または高度可用性グループ	プライマリ FCI 名	WSFC 名
	セカンダリ FCI 名	WSFC 名
	Node 1 の物理名	SQL Server クラスタの仮想名
	Node 2 の物理名	SQL Server クラスタの仮想名

複数のホスト名を持つホストのマッピングの削除

NetBackup が自動的に追加したホスト名のマッピングは削除できます。または、ホストに対して手動で追加したホスト名のマッピングも対象です。マッピングを削除すると、ホストはそのマッピング名では認識されなくなることに注意してください。共有マッピングまたはクラスタマッピングを削除すると、ホストは、その共有名またはクラスタ名を使用するその他のホストと通信できなくなる場合があります。

ホストとそのマッピングに問題がある場合は、ホスト属性をリセットできます。ただし、このようにすると、ホストの通信状態などの他の属性もリセットされます。

p.54 の「ホストの属性のリセット」を参照してください。

NetBackup が検出するホスト名を削除するには

1. 左側で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に選択します。
2. 更新するホストを特定します。
3. [処理 (Actions)]、[マッピングの管理 (Manage mappings)]の順にクリックします。
4. 削除するマッピングを特定して、[削除 (Delete)]、[保存 (Save)]の順にクリックします。

21

ユーザーセッションの管理

この章では以下の項目について説明しています。

NetBackup ユーザーセッションのサインアウト

セキュリティまたはメンテナンスの目的で、1 つ以上の NetBackup ユーザーセッションをサインアウトできます。アイドル状態のユーザーセッションを自動的にサインアウトさせるように NetBackup を構成するには、次のトピックを参照してください。

p.145 の「アイドル状態のセッションがタイムアウトになるタイミングを構成する」を参照してください。

メモ: ユーザーの役割の変更は、Web UI にすぐには反映されません。変更が有効になるには、管理者がアクティブなユーザーセッションを終了する必要があります。または、ユーザーがサインアウトして、再びサインインする必要があります。

ユーザーセッションをサインアウトするには

1. 左側で[セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。
2. [有効なセッション (Active sessions)]をクリックします。

3 サインアウトするユーザーセッションを選択します。

4 [セッションを終了する (Terminate session)]をクリックします。

すべてのユーザーセッションをサインアウトするには

1 左側で[セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。

2 [有効なセッション (Active sessions)]をクリックします。

3 [すべてのセッションを終了する (Terminate all sessions)]をクリックします。

NetBackup ユーザーのロック解除

現在 NetBackup でロックされているユーザーアカウントを表示して、1 人以上のユーザーのロックを解除できます。

デフォルトでは、ユーザーのアカウントは 24 時間だけロックされたままになります。[ユーザーセッション (User sessions)]、[ユーザーアカウント設定 (User Account Settings)]、[ユーザーアカウントのロックアウト (User account lockout)]設定の順に移動して調整することで、この時間を変更できます。

p.146 の「失敗したサインインの試行の最大数を構成する」を参照してください。

ロックされたユーザーアカウントのロックを解除するには

1 左側で[セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。

2 [ユーザーを解除する (Locked users)]をクリックします。

3 ロックを解除するユーザーアカウントを選択します。

4 [ロック解除 (Unlock)]をクリックします。

ロックされたすべてのユーザーアカウントのロックを解除するには

1 左側で[セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。

2 [ユーザーを解除する (Locked users)]をクリックします。

3 [すべてのユーザーのロックを解除する (Unlock all users)]をクリックします。

アイドル状態のセッションがタイムアウトになるタイミングを構成する

ユーザーセッションがタイムアウトしてユーザーが自動的にサインアウトされるタイミングをカスタマイズできます。選択した設定は、NetBackup 管理コンソールと NetBackup Web UI に反映されます。コマンドラインからこの設定を構成するには、nbsetconfig を使用して、GUI_IDLE_TIMEOUT オプションを設定します。

アイドル状態のセッションがタイムアウトになるタイミングを構成するには

1. [セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。
2. [ユーザーアカウント設定 (User account settings)]をクリックします。
3. [セッションアイドルタイムアウト (Session idle timeout)]を有効にし、[編集 (Edit)]をクリックします。
4. 時間を分単位で選択し、[保存 (Save)]をクリックします。

   アクティブなユーザーの場合、次回ユーザーがサインインしたときに更新が適用されます。

並列ユーザーセッションの最大数の構成

この設定によって、ユーザーがアクティブにできる並列 API セッションの数が制限されます。API セッションは、NetBackup 管理コンソールの一部のアプリケーションで使用されます。

この設定は、API キーセッションや、NetBackup のバックアップ、アーカイブ、リストアインターフェースなどのその他のアプリケーションには適用されません。

コマンドラインからこの設定を構成するには、nbsetconfig を使用して、GUI_MAX_CONCURRENT_SESSIONS オプションを設定します。

並列ユーザーセッションの最大数を構成するには

1. [セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。
2. [ユーザーアカウント設定 (User account settings)]をクリックします。

3 [最大並列セッション数 (Maximum concurrent sessions)]を有効にし、[編集 (Edit)]をクリックします。

4 [ユーザーあたりの並列セッション数 (Number of concurrent sessions per user)]を選択し、[保存 (Save)]をクリックします。

[Web UI からシングルサインオン、証明書、スマートカードを使用 (Single Sign-on, Certificates, or Smart Cards through the Web UI)]オプションを使用して NetBackup 管理コンソールにサインインしている場合、ここで設定する同時ユーザーセッションには、Web UI と NetBackup 管理コンソールのユーザーセッションが含まれます。

アクティブなユーザーの場合、次回ユーザーがサインインしたときに更新が適用されます。

失敗したサインインの試行の最大数を構成する

失敗した NetBackup へのサインインの試行の最大数をカスタマイズできます。選択した設定は、NetBackup Web UI のみに適用されます。コマンドラインからこの設定を構成するには、nbsetconfig を使用して、GUI_MAX_LOGIN_ATTEMPTS と GUI_ACCOUNT_LOCKOUT_DURATION オプションを設定する必要があります。

失敗したサインインの試行の最大数を構成するには

1 [セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。

2 [ユーザーアカウント設定 (User account settings)]をクリックします。

3 [ユーザーアカウントのロックアウト (User account lockout)]を有効にし、[編集 (Edit)]をクリックします。

4 アカウントがロックされる前に許容される、サインイン試行失敗の回数を選択します。

5 一定時間の経過後にロックされたアカウントをロック解除するには、[次の経過後にロックされたアカウントをロック解除する (Unlock locked accounts after)]の分単位の時間を選択します。

6 [保存 (Save)]をクリックします。

アクティブなユーザーの場合、次回ユーザーがサインインしたときに更新が適用されます。

ユーザーがサインインするときのバナーの表示

ユーザーが NetBackup Web UI にサインインするたびに表示されるサインインバナーを構成できます。異なるバナーをプライマリサーバーに構成できます。このバナーでは、ユーザーがサインインする前に、利用規約への同意もユーザーに要求できます。

NetBackup 管理コンソールのバナーとバックアップ、アーカイブ、リストアクライアントを構成するには、『NetBackup 管理者ガイド Vol 1』を参照してください。NetBackup 管理コンソールで使用されるバナーを NetBackup Web UI に移行するには、『NetBackup コマンドリファレンスガイド』で nbmlb コマンドを参照してください。

ユーザーがサインインするときにバナーを表示するには

1. [セキュリティ (Security)]、[ユーザーセッション (User sessions)]の順に選択します。
2. [ユーザーアカウント設定 (User account settings)]をクリックします。
3. [サインインバナーの構成 (Sign-in banner configuration)]を有効にし、[編集 (Edit)]をクリックします。
4. メッセージの見出しと本文に使用するテキストを入力します。
5. ユーザーに利用規約への同意を要求する場合は、[[同意する]および[同意しない]ボタンをサインインバナーに含める (Include "Agree" and "Disagree" buttons on the sign-in banner)]を選択します。
6. [保存 (Save)]をクリックします。

   アクティブなユーザーの場合、次回ユーザーがサインインしたときに更新が適用されます。

22

プライマリサーバーのセキュリティ設定の管理

この章では以下の項目について説明しています。

安全な通信のための認証局

グローバルセキュリティ設定の[認証局 (Certificate authority)]の情報に、NetBackup ドメインがサポートする認証局の種類が示されます。この設定を確認するには、[セキュリティ (Security)]、[グローバルセキュリティ (Global security)]の順に開きます。

ドメイン内の NetBackup ホストは、次の証明書を使用できます。

- NetBackup 証明書。
  デフォルトでは、プライマリサーバーとそのクライアントに NetBackup 証明書が配備されます。
- 外部証明書。

NetBackup が外部証明書を使用するホストとのみ通信するように構成できます。ホストが 8.2 以降にアップグレードされ、外部証明書がインストールおよび登録されている必要があります。この場合、NetBackup は NetBackup 証明書を使用するホストとは通信しません。ただし、[NetBackup 8.0 以前のホストとの通信を許可する (Allow communication with 8.0 and earlier hosts)]を有効にすると、NetBackup 8.0 以前を使用するホストと通信できるようになります。

- NetBackup 証明書と外部証明書の両方。
  この構成では、NetBackup は NetBackup 証明書または外部証明書を使用するホストと通信できます。ホストにこの両方の種類の証明書がある場合、NetBackup は外部証明書を使用して通信します。

NetBackup 8.0 以前のホストとの通信の無効化

デフォルトで、NetBackup は、環境内に存在する NetBackup 8.0 以前のホストとの通信を許可します。ただし、この通信は安全ではありません。セキュリティ向上のため、すべてのホストを NetBackup の現在のバージョンにアップグレードしてこの設定を無効にします。この処置により、NetBackup ホスト間では安全な通信のみが可能になります。自動イメージレプリケーション (A.I.R) を使用する場合は、イメージレプリケーションの信頼できるプライマリサーバーを NetBackup 8.1 以降にアップグレードする必要があります。

NetBackup 8.0 以前のホストとの通信を無効化するには

1. 右上で、[セキュリティ (Security)]、[グローバルセキュリティ (Global security)]の順に選択します。
2. [NetBackup 8.0 以前のホストとの通信を許可する (Allow communication with 8.0 and earlier hosts)]をオフにします。
3. [保存 (Save)]をクリックします。

NetBackup ホスト名の自動マッピングの無効化

NetBackup ホスト間で正常に通信するために、関連するすべてのホスト名と IP アドレスをそれぞれのホスト ID にマッピングする必要があります。[ホスト名を NetBackup ホスト ID に自動的にマッピングする (Automatically map host names to their host ID)]オプションを使用して、ホスト ID をそれぞれのホスト名 (と IP アドレス) に自動的にマッピングするか、このオプションを無効化して、NetBackup セキュリティ管理者が承認する前に手動でマッピングを確認できるようにします。

NetBackup ホスト名の自動マッピングを無効化するには

1. 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順にクリックします。
2. [ホスト名を NetBackup ホスト ID に自動的にマッピングする (Automatically map host names to their host ID)]をオフにします。
3. [保存 (Save)]をクリックします。

移動中のデータの暗号化のグローバル設定を行う

NetBackup 環境内で移動中のデータの暗号化 (DTE) を構成するには、まずグローバル DTE (またはグローバル DTE モード) を設定し、次にクライアント DTE モードを設定する必要があります。

さまざまな NetBackup 操作での移動中のデータの暗号化の判断は、グローバル DTE モード、クライアント DTE モード、イメージ DTE モードに基づいて実行されます。

グローバル DTE モードでサポートされる値は次のとおりです。

- `Preferred Off` (デフォルト): 移動中のデータの暗号化が NetBackup ドメインで無効になるように指定します。この設定は、NetBackup クライアント設定によって上書きできます。
- `Preferred On`: 移動中のデータの暗号化が、NetBackup 9.1 以降のクライアントに対してのみ有効になるように指定します。
  この設定は、NetBackup クライアント設定によって上書きできます。
- `Enforced`: NetBackup クライアント設定が「自動」または「オン」の場合に移動中のデータの暗号化が適用されるように指定します。このオプションを選択すると、移動中のデータの暗号化が「オフ」に設定されている NetBackup クライアントと、9.1 より前のホストでジョブが失敗します。

メモ: デフォルトでは、9.1 クライアントの DTE モードは `Off` に設定され、10.0 以降のクライアントでは `Automatic` に設定されます。

グローバル DTE 構成に使用する RESTful API:

- GET - /security/properties
- POST - /security/properties

NetBackup Web UI を使用してグローバル DTE モードを設定または表示するには

1. 右上で、[セキュリティ (Security)]、[グローバルセキュリティ (Global security)]の順に選択します。
2. [安全な通信 (Secure Communication)]タブで、次のグローバル DTE 設定のいずれかを選択します。
   - `Preferred Off`
   - `Preferred On`
   - `Enforced`

NetBackup 証明書の配備のセキュリティレベルについて

証明書の配備のセキュリティレベルは、NetBackup CA が署名した証明書に固有です。安全な通信のために NetBackup 証明書を使用するように NetBackup Web サーバーを構成していない場合、セキュリティレベルは設定できません。

NetBackup 証明書の配備レベルによって、NetBackup CA が NetBackup ホストに証明書を発行する前に実行する確認が決定されます。また、ホストの NetBackup 証明書失効リスト (CRL) を更新する頻度も決定されます。

NetBackup 証明書はインストール時 (ホスト管理者がプライマリサーバーの指紋を確認した後) に、または `nbcertcmd` コマンドを使用してホストに配備します。お使いの NetBackup 環境のセキュリティ要件に対応する配備レベルを選択してください。

表 22-1 NetBackup 証明書の配備のセキュリティレベルに関する説明

セキュリティレベル	説明	CRL の更新
最高 (Very High)	新しい NetBackup 証明書要求ごとに認証トークンが必要です。	1 時間ごとに、ホスト上に存在する CRL が更新されます。

セキュリティレベル	説明	CRL の更新
高 (High) (デフォルト)	ホストがプライマリサーバーに認識されている場合、認証トークンは不要です。ホストが以下のエンティティで検出される場合、ホストはプライマリサーバーに認識されていると見なされます。 **1** ホストが NetBackup 構成ファイル (Windows レジストリまたは UNIX の `bp.conf` ファイル) で次のいずれかのオプションでリストされる。 ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER NetBackup の構成オプションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。 **2** `altnames` ファイル (ALTNAMESDB_PATH) にクライアント名としてホストがリストされている。 **3** ホストがプライマリサーバーの EMM データベースに表示されている。 **4** クライアントの少なくとも 1 つのカタログイメージが存在する。イメージは 6 カ月以内に作成されたものである必要があります。 **5** クライアントが少なくとも 1 つのバックアップポリシーにリストされている。 **6** クライアントがレガシークライアントである。すなわち、[クライアント属性 (Client Attributes)]ホストプロパティを使用して追加されたクライアントです。	4 時間ごとに、ホスト上に存在する CRL が更新されます。
中 (Medium)	プライマリサーバーが要求の発信元である IP アドレスにホスト名を解決できる場合、証明書は認証トークンなしで発行されます。	8 時間ごとに、ホスト上に存在する CRL が更新されます。

NetBackup 証明書配備のセキュリティレベルの選択

NetBackup は、NetBackup 証明書配備のためのいくつかのセキュリティレベルを提供します。セキュリティレベルは、NetBackup ホストに証明書を発行する前に、NetBackup

認証局 (CA) がどのようなセキュリティチェックを実行するかを決定します。また、このレベルは、NetBackup CA の証明書失効リスト (CRL) がホスト上で更新される頻度も決定します。

セキュリティレベル、NetBackup 証明書配備、NetBackup CRL について詳しくは、以下を参照してください。

- p.151 の「NetBackup 証明書の配備のセキュリティレベルについて」を参照してください。
- 『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

NetBackup 証明書配備のセキュリティレベルを選択するには

1. 上部で、[設定 (Settings)]、[グローバルセキュリティ設定 (Global security settings)] の順にクリックします。
2. [安全な通信 (Secure communication)]をクリックします。
3. [NetBackup 証明書配備のセキュリティレベル (Security level for certificate deployment)]で、セキュリティレベルを選択します。

   NetBackup 証明書を使用することを選択した場合は、インストール中、ホストの管理者がプライマリサーバーの指紋を確認した後に、ホストに配備されます。セキュリティレベルにより、ホストに認証トークンが必要かどうかが決定されます。

最高 (Very High)	NetBackup は、すべての新しい NetBackup 証明書要求に認証トークンを求めます。
高 (High) (デフォルト)	ホストがプライマリサーバーにとって既知の場合、NetBackup では認証トークンは必要ありません。つまり、NetBackup 構成ファイル、EMM データベース、バックアップポリシー、またはホストに表示されるホストはレガシークライアントです。
中 (Medium)	プライマリサーバーが要求の発信元である IP アドレスにホスト名を解決できる場合、NetBackup は認証トークンなしで NetBackup 証明書を発行します。

4. [保存 (Save)]をクリックします。

TLS セッションの再開について

NetBackup は TLS (Transport Layer Security) を使用して NetBackup ホスト間の通信を保護します。これは、デフォルトでは有効になっています。NetBackup ホスト間の新しい各 TCP 接続は、その接続を介して NetBackup がトラフィックを送信する前に、TLS ハンドシェークを実行してピア ID を確認する必要があります。

TLS セッションの再開は、オープン標準の最適化機能です。これにより、TLS クライアントとサーバーは、以前の接続中に生成されたセキュアセッションを再利用できます。セキュアセッションを再利用すると、NetBackup はフルハンドシェークの代わりに合理化されたハンドシェークを使用できます。この処理を実行すると、ホストの CPU の使用と新しい接続の確立に必要な時間の両方が削減されます。

TLS バージョン 1.2 (現在 NetBackup のバージョンで使用) では、フルハンドシェーク間のフォワードセキュリティが軽減されます。セッションの再利用による利益を得ながらこの時間帯を制限するために、NetBackup ではフル TLS ハンドシェーク間の最大間隔をグローバルに構成できます。

TLS セッションの再開のオプションを使用するには、[設定 (Settings)]、[グローバルセキュリティ (Global security)]、[安全な通信 (Secure communication)]の順に移動します。[フルハンドシェークを次の間隔で実行 (Perform full handshake every)]オプションを使用して、セキュリティレベルを次のように設定できます。

- [現在のセキュリティレベルのデフォルト (Default for current security level)] – このオプションを使用する場合、NetBackup ではセキュリティ設定のデフォルトが次のようになります。
  - 最高 - 10 分
  - 高 - 30 分
  - 中 - 60 分
- [カスタム (セキュリティレベル設定を上書き) (Custom (overrides the security level settings))] - この間隔の値は、1 分単位で 1 分から 720 分の範囲内で構成できます。

メモ: 厳格なフォワードセキュリティが必要である場合、NetBackup ではセッション再開をグローバルに無効にすることもできます。

メモ: この機能は現在 NBCA にのみ適用されます。ECA は今後のリリースでサポートされる予定です。

ディザスタリカバリのパスフレーズの設定

NetBackup は、カタログのバックアップ中にディザスタリカバリパッケージを作成し、設定したパスフレーズを使用してバックアップを暗号化します。パスフレーズの制約は、NetBackup API または CLI (`nbseccmd -setpassphraseconstraints`) を使用して変更できます。

ディザスタリカバリの設定について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

ディザスタリカバリのパスフレーズを設定するには

1 上部で、[設定 (Settings)]、[グローバルセキュリティ設定 (Global security settings)]の順にクリックします。

2 [ディザスタリカバリ (Disaster recovery)]をクリックします。

3 パスフレーズを入力して確認します。

メモ: 追加の制約を設定した場合、パスフレーズはその制約を満たす必要があります。nbseccmd コマンドまたはパスフレーズの制約 Web API を使用して、追加の制約を確認できます。

4 [保存 (Save)]をクリックします。

信頼できるプライマリサーバーについて

NetBackup ドメイン間の信頼関係によって、次の操作を実行できます。

- レプリケーションのターゲットとして特定のドメインを選択します。この種類の自動イメージレプリケーションは「対象設定された A.I.R (Targeted A.I.R)」として知られます。信頼関係がないと、NetBackup は、定義されたすべてのターゲットストレージサーバーにレプリケートします。メディアサーバー重複排除プールと PureDisk 重複排除プールをターゲットストレージにする場合、信頼関係の確立は省略できます。CloudCatalyst ストレージサーバーを使用するには、信頼関係が必要です。
- 複数のプライマリサーバーの使用状況レポートを含めます。

プライマリサーバーは、NetBackup 認証局 (CA) 証明書または外部 CA 証明書を使用できます。NetBackup は、ソースドメインとターゲットドメインで使用される CA を判断し、サーバー間の通信に使用する適切な CA を選択します。両方の CA の種類に対してターゲットプライマリサーバーが設定されている場合は、NetBackup によって使用する CA の選択を求められます。NetBackup CA を使用してリモートプライマリサーバーとの信頼を確立するには、現在のプライマリとリモートプライマリの NetBackup バージョンが 8.1 以降である必要があります。外部 CA を使用してリモートプライマリサーバーとの信頼を確立するには、現在のプライマリとリモートプライマリの NetBackup バージョンが 8.2 以降である必要があります。

表 22-2 サーバー間の信頼関係に使用する認証局 (CA) の決定

ソースプライマリサーバーの CA (1 つ以上)	ターゲットプライマリサーバーの CA (1 つ以上)	選択された認証局
NetBackup CA と外部 CA	外部 CA	外部 CA
	NetBackup CA	NetBackup CA
	外部 CA と NetBackup CA	NetBackup によって CA の選択を求められます。
NetBackup CA	外部 CA	信頼は確立されません。
	NetBackup CA	NetBackup CA
	外部 CA と NetBackup CA	NetBackup CA

信頼できるプライマリサーバーの追加

メモ: NetBackup Web UI では、バージョン 8.0 以前を使用する信頼できるプライマリの追加はサポートされていません。

NetBackup CA または外部 CA を使用するプライマリサーバー間の信頼関係を作成できます。

信頼できるプライマリサーバーを追加するには

1. NetBackup CA (認証局) を使用するサーバーの場合は、最初に各サーバーの認証トークンと指紋を取得します。
2. 上部で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。
3. [信頼できるプライマリサーバー (Trusted primary servers)]を選択します。
4. [追加 (Add)]ボタンをクリックします。
5. ウィザードに表示されるプロンプトに従います。
6. リモートプライマリサーバーでこの手順を繰り返します。

詳細情報

NetBackup での外部 CA の使用について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

信頼できるプライマリサーバーの削除

メモ: NetBackup バージョン 8.0 以前の信頼できるプライマリサーバーは、NetBackup 管理コンソールを使用して削除する必要があります。

信頼できるプライマリサーバーを削除できます。これにより、プライマリサーバー間の信頼関係が削除されます。次の点に注意してください。

- 信頼関係を必要とするレプリケーション操作はすべて失敗します。
- 信頼関係を削除した後、リモートプライマリサーバーはどの使用状況レポートにも含まれなくなります。

信頼できるプライマリサーバーを削除するには

1. ターゲットプライマリサーバーへのすべてのレプリケーションジョブが完了していることを確認します。
2. 宛先として信頼できるプライマリを使用するすべてのストレージライフサイクルポリシー (SLP) を削除します。SLP を削除する前に、ストレージに SLP を使うバックアップポリシーまたは保護計画がないことを確認します。
3. 上部で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。
4. [信頼できるプライマリサーバー (Trusted primary servers)]を選択します。
5. [操作 (Actions)]、[削除 (Remove)]の順に選択します。
6. [信頼を削除 (Remove trust)]をクリックします。
7. リモートプライマリサーバーで手順 3 から手順 6 を繰り返します。

23

アクセスキー、API キー、アクセスコードの使用

この章では以下の項目について説明しています。

アクセスキー

NetBackup アクセスキーは、API キーとアクセスコードにより NetBackup インターフェースへのアクセス権を提供します。

p.158 の「API キー」を参照してください。

p.164 の「アクセスコード」を参照してください。

API キー

NetBackup API キーは、NetBackup RESTful API に対して NetBackup ユーザーを識別する事前認証トークンです。NetBackup API で認証が必要な場合、ユーザーは API リクエストヘッダー内で API キーを使用できます。API キーは、認証済みの NetBackup ユーザー用に作成できます (グループはサポート対象外)。特定の API キーは 1 回のみ作成可能で、再作成はできません。各 API キーには、一意のキー値と API キータグが含まれます。NetBackup は、ユーザーの完全な ID を含むキーを使用して、実行される操作を監査します。

管理者および API キーのユーザーは次の処理を実行できます。

- 適切な役割または RBAC 権限を持つ管理者は、すべてのユーザーの API キーを管理できます。これらの役割とは、管理者、デフォルトのセキュリティ管理者、または API キーの RBAC 権限を持つ役割です。
- 認証された NetBackup ユーザーは、NetBackup Web UI に独自の API キーを追加して管理できます。ユーザーが Web UI にアクセスできない場合は、NetBackup API を使用してキーを追加または管理できます。

詳細情報

p.122 の「監査レポートのユーザーの ID」を参照してください。

bpnbat コマンドでの API キーの使用方法について詳しくは、『NetBackup セキュリティと暗号化ガイド』を参照してください。

API キーの追加または API キーの詳細の表示 (管理者)

API キーの管理者は、すべての NetBackup ユーザーに関連付けられているキーを管理できます。

API キーの追加

注意: 特定のユーザーに関連付けることができる API キーは、一度に 1 つだけです。ユーザーが新しい API キーを要求した場合、ユーザーまたは管理者は、そのユーザーのキーを削除する必要があります。期限切れの API キーは再発行できます。

API キーを追加するには

1. 左側で、[セキュリティ (Security)]、[アクセスキー (Access keys)]、[API キー (API keys)]の順に選択します。
2. 左側で、[追加 (Add)]をクリックします。
3. API キーを作成する[ユーザー名 (Username)]を入力します。
4. (該当する場合) API キーが SAML ユーザー用である場合、[SAML 認証 (SAML authentication)]を選択します。

   SAML ユーザー用の新しい API キーは、ユーザーが Web UI にサインインするまで無効なままです。
5. 今日の日付から API キーを有効にする期間を指定します。

   NetBackup が有効期限を計算して表示します。

6 [追加 (Add)]をクリックします。

7 API キーをコピーするには、[コピーして閉じる (Copy and close)]をクリックします。

このキーは安全な場所に保管してください。[コピーして閉じる (Copy and close)]をクリックした後は、キーを再び取得できません。アカウントの以前のキーをこの API キーで置き換える場合、新しい API キーを反映するため、スクリプトなどを更新する必要があります。

API キーの詳細の表示

API キーの管理者は、すべての NetBackup ユーザーに関連付けられている API キーの詳細を表示できます。

API キーの詳細を表示するには

1 左側で、[セキュリティ (Security)]、[アクセスキー (Access keys)]、[API キー (API keys)]の順に選択します。

2 表示する API キーを見つけます。

3 [処理 (Actions)]、[編集 (Edit)]をクリックして、キーの日付または説明を編集します。

API キーの編集、再発行、または削除 (管理者)

API キーの管理者は、API キーの詳細を編集したり、API キーを再発行または削除したりできます。

API キーの有効期限または説明の編集

メモ: SAML ユーザーの場合、SAML セッションが期限切れになった後の有効期限を API キーに選択しないようにします。セッションが期限切れになった後の日付の場合、この処理により、その API キーでセキュリティリスクが生じる可能性があります。

API キーの説明を編集したり、有効な API キーの有効期限を変更したりできます。

API キーの有効期限または説明を編集するには

1 左側で、[セキュリティ (Security)]、[アクセスキー (Access keys)]、[API キー (API keys)]の順に選択します。

2 編集する API キーを見つけます。

3 [処理 (Actions)]メニューをクリックします。次に、[編集 (Edit)]を選択します。

4 キーの現在の有効期限を確認し、必要に応じて期限を延長します。

5 必要に応じて、説明を変更します。

6 [保存 (Save)]をクリックします。

期限切れになった後の API キーの再発行

メモ: SAML ユーザーの場合、SAML セッションが期限切れになった後の有効期限を API キーに選択しないようにします。セッションが期限切れになった後の日付の場合、この処理により、その API キーでセキュリティリスクが生じる可能性があります。

API キーが期限切れになると、API キーを再発行できます。この操作によって、ユーザーに新しい API キーが作成されます。

API キーを再発行するには

1 左側で、[セキュリティ (Security)]、[アクセスキー (Access keys)]、[API キー (API keys)]の順に選択します。

2 編集する API キーを見つけます。

3 [処理 (Actions)]メニューをクリックします。次に、[再発行 (Reissue)]、[再発行 (Reissue)]の順に選択します。

API キーの削除

ユーザーのアクセス権を削除する場合や、このキーを使用する必要がなくなったときに、API キーを削除できます。キーは完全に削除され、関連付けられているユーザーは、認証でそのキーを使用できなくなります。

API キーを削除するには

1 左側で、[セキュリティ (Security)]、[アクセスキー (Access keys)]、[API キー (API keys)]の順に選択します。

2 表示する API キーを見つけます。

3 [処理 (Actions)]メニューをクリックします。次に、[削除 (Delete)]、[削除 (Delete)]の順にクリックします。

API キーの追加または自分の API キーの詳細の表示

NetBackup RESTful API を使用している場合は、NetBackup ユーザーアカウントを認証するための API キーを作成できます。

API キーの追加

NetBackup Web UI ユーザーとして、Web UI を使用して、独自の API キーの詳細を追加または表示できます。

API キーを追加するには

1. API キーが期限切れになった場合、API キーを再発行できます。

   p.163 の「期限切れになった後の API キーの再発行」を参照してください。

2. 右上で、プロファイルアイコンをクリックし、[API キーの追加 (Add API key)]をクリックします。

3. (非 SAML ユーザー) 今日の日付から API キーを有効にする期間を指定します。

   NetBackup が有効期限を計算して表示します。

4. (SAML ユーザー) NetBackup が SAML セッションからトークンを検証した後、API キーの有効期限を判断できます。

5. [追加 (Add)]をクリックします。

6. API キーをコピーするには、[コピーして閉じる (Copy and close)]をクリックします。

   このキーは安全な場所に保管してください。[コピーして閉じる (Copy and close)]をクリックした後は、キーを再び取得できません。アカウントの以前のキーをこの API キーで置き換える場合、新しい API キーを反映するため、スクリプトなどを更新する必要があります。

API キーの詳細の表示

自分の API キーの詳細を表示するには

- 右上で、プロファイルアイコンをクリックし、[API キーの詳細を表示 (View my API key details)]を選択します。

API キーの編集、再発行、または削除

自分の API キーを NetBackup Web UI から管理できます。

自分の API キーの有効期限または説明の編集 (非 SAML ユーザー)

非 SAML ユーザーは、有効な API キーの有効期限を変更できます。API キーの期限が切れたら、API キーを再発行できます。

API キーの詳細を編集するには

1. 右上で、プロファイルアイコンをクリックし、[API キーの詳細を表示 (View my API key details)]をクリックします。

   注意: API キーの有効期限が切れている場合は、[再発行 (Reissue)]をクリックしてキーを再発行できます。

   p.163 の「期限切れになった後の API キーの再発行」を参照してください。
2. [編集 (Edit)]をクリックします。
3. キーの現在の有効期限を確認し、必要に応じて期限を延長します。
4. 必要に応じて、説明を変更します。
5. [保存 (Save)]をクリックします。

期限切れになった後の API キーの再発行

API キーが期限切れになると、API キーを再発行できます。この操作によって、新しい API キーが作成されます。

API キーを再発行するには

1. 右上で、プロファイルアイコンをクリックし、[API キーの詳細を表示 (View my API key details)]をクリックします。
2. 右上で[再発行 (Reissue)]をクリックします。
3. (非 SAML ユーザー) キーの現在の有効期限を確認し、必要に応じて期限を延長します。
4. 必要に応じて、説明を変更します。
5. [再発行 (Reissue)]をクリックします。

API キーの削除

API キーは、アクセスできなくなったり、使用しなくなった場合に削除できます。API キーを削除すると、そのキーは完全に削除されます。認証または NetBackup API でそのキーを使用できなくなります。

API キーを削除するには

1. 右上で、プロファイルアイコンをクリックし、[API キーの詳細を表示 (View my API key details)]をクリックします。
2. 右上の[削除 (Delete)]をクリックします。それから[削除 (Delete)]をクリックします。

NetBackup REST API での API キーの使用

キーの作成後、ユーザーは APIリクエストヘッダーで APIキーを渡すことができます。次に例を示します。

```
curl -X GET
https://primaryservername.domain.com/netbackup/admin/jobs/5 ¥
     -H 'Accept: application/vnd.netbackup+json;version=3.0'     ¥
     -H 'Authorization: <API key value>'
```

アクセスコード

特定の NetBackup 管理者コマンド (bperror など) を実行するには、Web UI を介して認証する必要があります。コマンドラインインターフェースを使用してアクセスコードを生成し、管理者が承認したアクセス要求を取得してから、コマンドにアクセスする必要があります。

CLI アクセス用の Web UI 認証を使用すると、NetBackup 管理者は他のユーザーに関連する権限を委任できます。デフォルトでは、root 管理者または管理者のみがコマンドラインインターフェースを使用して NetBackup 操作を実行できます。Web UI の認証サポートにより、root 以外のユーザーで、セキュリティ管理者が付与した CLI アクセス権を持つユーザーは NetBackup を管理できます。NetBackup ユーザーとして登録されていなくても、RBAC ユーザー以外の役割 (オペレーティングシステム管理者など) があれば NetBackup を管理できます。CLI にアクセスするには、毎回新しいアクセスコードを生成する必要があります。

Web UI 認証を使用した CLI アクセス権の取得

CLI アクセス権を取得するには

1. 次のコマンドを実行します。

   ```
   bpnbat -login -logintype webui
   ```

   アクセスコードが生成されます。

2. (省略可能) セキュリティ管理者から承認されたコードを取得するには、次のコマンドを実行します。

   ```
   bpnbat -login -logintype webui -requestApproval
   ```

3 コマンドライン (CLI) 管理者の役割がある場合は、Web UI で、アクセスコードを使用して CLI アクセス要求を承認できます。

p.165 の「CLI アクセス要求の承認」を参照してください。

コマンドライン (CLI) 管理者の役割がない場合は、CLI アクセス要求の承認を管理者に依頼してください。

p.165 の「他のユーザーの CLI アクセス要求の承認」を参照してください。

4 CLI アクセス要求が承認されたら、コマンドラインインターフェースに移動し、必要なコマンドを実行します。

デフォルトでは、CLI アクセスのセッションは 24 時間有効です。

p.166 の「アクセス設定の編集」を参照してください。

CLI アクセス要求の承認

Web UI を使用して CLI アクセス要求を承認できます。

CLI アクセス要求を承認するには

1 右側のユーザープロファイルアイコンをクリックします。

2 [アクセス権の要求を承認する (Approve Access Request)]をクリックします。

3 CLI アクセスが必要なユーザーから受け取った CLI アクセスコードを入力し、[確認 (Review)]をクリックします。

4 アクセス要求の詳細を確認します。

5 [承認 (Approve)]をクリックします。

他のユーザーの CLI アクセス要求の承認

コマンドライン (CLI) 管理者の役割がある場合は、Web UI を使用して他のユーザーのアクセス要求を承認できます。

他のユーザーの CLI アクセス要求を承認するには

1 左側で[セキュリティ (Security)]、[アクセスキー (Access keys)]、[アクセスコード (Access codes)]の順に選択します。

2 CLI アクセスが必要なユーザーから受け取った CLI アクセスコードを入力し、[確認 (Review)]をクリックします。

3 アクセス要求の詳細を確認します。

4 コメントがある場合は入力します。

5 [承認 (Approve)]をクリックします。

アクセス設定の編集

アクセス設定を編集するには

1. 左側で[セキュリティ (Security)]、[アクセスキー (Access keys)]の順に選択します。
2. 右側で[アクセス設定 (Access settings)]を選択します。
3. [編集 (Edit)]をクリックします。
4. CLI アクセスセッションを有効にする時間を分または時間で入力します。最小値は 1 分、最大値は 24 時間です。

24

認証オプションの設定

この章では以下の項目について説明しています。

NetBackup Web UI のサインインオプション

NetBackup は、ローカルドメインユーザーおよび Active Directory (AD) ユーザーまたは LDAP ドメインユーザーの認証をサポートしています。AD および LDAP ドメイン、スマートカード、シングルサインオン (SAML を使用した SSO) では、この認証方法を使用する各プライマリサーバードメインに対して個別に構成する必要があります。

NetBackup は、次の形式のユーザー認証をサポートしています。

- ユーザー名とパスワード
- デジタル証明書またはスマートカード (CAC、PIV など)
  この認証方法はプライマリサーバーのドメインごとに 1 つの AD または LDAP ドメインのみサポートし、ローカルドメインのユーザーは使用できません。
  p.168 の「スマートカードまたはデジタル証明書によるユーザー認証の構成」を参照してください。
- SAML を使用したシングルサインオン

  次の必要条件と制限事項に注意してください。

  - SSO を使用するには、環境で SAML 2.0 に準拠した ID プロバイダが構成されている必要があります。

- 各プライマリサーバードメインでは、1 つの AD または LDAP ドメインのみサポートされます。この機能は、ローカルドメインユーザーには利用できません。
- IDP の構成には、NetBackup API または NetBackup コマンド `nbidpcmd` が必要です。
- API キーはユーザーまたはグループを認証するために使われるもので、SAML 認証されたユーザーやグループには使用できません。
- グローバルログアウトはサポートされません。

p.174 の「NetBackup の SSO (シングルサインオン) の構成」を参照してください。

スマートカードまたはデジタル証明書によるユーザー認証の構成

ユーザー検証では、スマートカードまたは証明書を AD または LDAP ドメインにマップできます。または、AD または LDAP ドメインなしでスマートカードまたは証明書のユーザー認証を構成することもできます。

p.168 の「ドメインを使用したスマートカード認証の構成」を参照してください。

p.169 の「ドメインを使用しないスマートカード認証の構成」を参照してください。

ドメインを使用したスマートカード認証の構成

ユーザー検証のために AD または LDAP ドメインにスマートカードまたは証明書をマップする場合は、NetBackup ユーザーに関連付けられている AD または LDAP ドメインを追加します。『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

メモ: スマートカードまたは証明書の認証を構成する前に、NetBackup ユーザーについて、役割に基づくアクセス制御 (RBAC) 構成を完了していることを確認してください。

p.191 の「RBAC の構成」を参照してください。

NetBackup でスマートカードまたはデジタル証明書によるユーザー認証を構成するには

1. 右上で、[設定 (Settings)]、[スマートカード認証 (Smart card authentication)]の順に選択します。
2. [スマートカード認証 (Smart card authentication)]をオンにします。
3. [ドメインの選択 (Select the domain)]オプションから必要な AD または LDAP ドメインを選択します。
4. [証明書のマッピング属性 (Certificate mapping attribute)]を選択します (一般名 (CN) またはユニバーサルプリンシパル名 (UPN))。

5 必要に応じて、[OCSP URI]に入力します。

OCSP URI を指定しない場合は、ユーザー証明書内の URI が使用されます。

6 [保存 (Save)]をクリックします。

7 [CA 証明書 (CA certificates)]の右にある[追加 (Add)]をクリックします。

8 [CA 証明書 (CA certificates)]を参照するかドラッグアンドドロップして、[追加 (Add)]をクリックします。

スマートカード認証には、信頼できる root CA 証明書または中間 CA 証明書のリストが必要です。ユーザーのデジタル証明書またはスマートカードに関連付けられている CA 証明書を追加します。

証明書ファイルの種類は .crt、.cer、.der、.pem、または PKCS #7 形式で、サイズが 64 KB 未満である必要があります。

9 [スマートカード認証 (Smart card authentication)]ページで構成情報を確認します。

10 ユーザーがスマートカードにインストールされていないデジタル証明書を使用するには、事前にブラウザの証明書マネージャに証明書をアップロードする必要があります。

詳しくはブラウザのマニュアルで手順を参照するか、証明書管理者にお問い合わせください。

11 ユーザーがサインインするときに、[証明書またはスマートカードでサインイン (Sign in with certificate or smart card)]のオプションが表示されるようになりました。

ユーザーにまだこのサインインオプションを使用させない場合は、[スマートカード認証 (Smart card authentication)]をオフにします(たとえば、ホストにすべてのユーザーの証明書がまだ構成されていない場合)。スマートカード認証を無効にした場合でも、構成した設定は保持されます。

このようなユーザーの場合、ドメイン名とドメイン形式はスマートカードです。

ドメインを使用しないスマートカード認証の構成

AD または LDAP ドメインを使用したユーザーの認証をせずに、スマートカードまたは証明書のユーザー認証を構成できます。

ユーザーがサポートされるのは、ユーザーの検証に AD または LDAP ドメインが使用されない場合のみです。ユーザーグループはサポートされません。

ドメインを使用せず、スマートカードまたはデジタル証明書を使用してユーザーを認証するように NetBackup を構成するには

1. 右上で、[設定 (Settings)]、[スマートカード認証 (Smart card authentication)]の順に選択します。
2. [スマートカード認証 (Smart card authentication)]をオンにします。
3. (該当する場合の手順) AD または LDAP ドメインが環境内で構成されている場合は、[ドメインなしで続行 (Continue without the domain)]を選択します。
4. [証明書のマッピング属性 (Certificate mapping attribute)]を選択します (一般名 (CN) またはユニバーサルプリンシパル名 (UPN))。
5. 必要に応じて、[OCSP URI]に入力します。

   OCSP URI を指定しない場合は、ユーザー証明書内の URI が使用されます。
6. [保存 (Save)]をクリックします。
7. [CA 証明書 (CA certificates)]の右にある[追加 (Add)]をクリックします。
8. [CA 証明書 (CA certificates)]を参照するかドラッグアンドドロップして、[追加 (Add)]をクリックします。
9. スマートカード認証には、信頼できるルート CA 証明書または中間 CA 証明書のリストが必要です。ユーザーのデジタル証明書またはスマートカードに関連付けられている CA 証明書を追加します。

   証明書ファイルの種類は `.crt`、`.cer`、`.der`、`.pem`、または `PKCS #7` 形式で、サイズが 64 KB 未満である必要があります。
10. [スマートカード認証 (Smart card authentication)]ページで構成情報を確認します。

    ユーザーがスマートカードにインストールされていないデジタル証明書を使用するには、事前にブラウザの証明書マネージャに証明書をアップロードする必要があります。

    詳しくはブラウザのマニュアルで手順を参照するか、証明書管理者にお問い合わせください。

    https://iase.disa.mil/pki-pke/Pages/web-browsers.aspx
11. ユーザーがサインインするときに、[証明書またはスマートカードでサインイン (Sign in with certificate or smart card)]のオプションが表示されるようになりました。

    ユーザーにまだこのサインインオプションを使用させない場合は、[スマートカード認証 (Smart card authentication)]をオフにします(たとえば、ホストにすべてのユーザーの証明書がまだ構成されていない場合)。スマートカード認証を無効にした場合でも、構成した設定は保持されます。

スマートカード認証の構成の編集

スマートカード認証の構成に変更がある場合は、構成の詳細を編集できます。

ドメインを使用したユーザー認証の構成を編集するには

1. 右上で、[設定 (Settings)]、[スマートカード認証 (Smart card authentication)]の順に選択します。
2. 次のような場合に、AD または LDAP ドメインの選択を編集できます。
   - 既存のドメインとは異なるドメインを選択する場合
   - 既存のドメインが削除されたため、新しいドメインを選択する場合
   - ドメインなしで続行する場合

   [編集 (Edit)]をクリックします。
3. ドメインを選択します。

   NetBackup 用に構成されているドメインのみがこのリストに表示されます。

   ドメインを使用するユーザーを検証しない場合は、[ドメインなしで続行 (Continue without the domain)]を選択できます。
4. [証明書のマッピング属性 (Certificate mapping attribute)]を編集します。
5. ユーザー証明書から URI の値を使用する場合は、[OCSP URI]フィールドは空のままにします。または、使用する URI を指定します。

スマートカード認証に使用される CA 証明書の追加または削除

CA 証明書の追加

スマートカード認証には、信頼できるルート CA 証明書または中間 CA 証明書のリストが必要です。ユーザーのデジタル証明書またはスマートカードに関連付けられている CA 証明書を追加します。

CA 証明書を追加するには

1. 右上で、[設定 (Settings)]、[スマートカード認証 (Smart card authentication)]の順に選択します。
2. [追加 (Add)]をクリックします。
3. [CA 証明書 (CA certificates)]を参照するか、ドラッグアンドドロップします。次に[追加 (Add)]をクリックします。

   スマートカード認証には、信頼できるルート CA 証明書または中間 CA 証明書のリストが必要です。ユーザーのデジタル証明書またはスマートカードに関連付けられている CA 証明書を追加します。

   証明書ファイルの種類は DER、PEM または PKCS #7 形式で、サイズが 1 MB 未満である必要があります。

CA 証明書の削除

スマートカード認証で使用されなくなった場合は、CA 証明書を削除できます。ユーザーが、関連付けられたデジタル証明書またはスマートカード証明書の使用を試行した場合、NetBackup にサインインできないことに注意してください。

CA 証明書を削除するには

1. 右上で、[設定 (Settings)]、[スマートカード認証 (Smart card authentication)]の順に選択します。
2. 削除する CA 証明書を選択します。
3. [削除 (Delete)]、[削除 (Delete)]の順にクリックします。

スマートカード認証を無効にするか一時的に無効にする

プライマリサーバーでスマートカード認証を使用する必要がなくなった場合は、スマートカード認証を無効にできます。または、ユーザーがスマートカードを使用できるようにする前に、その他の構成を完了する必要がある場合も同様です。

スマートカード認証を無効にするには

1. 右上で、[設定 (Settings)]、[スマートカード認証 (Smart card authentication)]の順に選択します。
2. [スマートカード認証 (Smart card authentication)]をオフにします。

   スマートカード認証を無効にした場合でも、構成した設定は保持されます。

SSO (シングルサインオン) 設定について

認証および認可情報の交換に SAML 2.0 プロトコルを使用する任意の IDP (ID プロバイダ) を使用して、SSO (シングルサインオン) を構成できます。複数の Veritas 製品で

1 つの IDP を構成できることに注意します。たとえば、同じ IDP を NetBackup と APTARE で構成できます。

次の必要条件と制限事項に注意してください。

- SSO を使用するには、環境で SAML 2.0 に準拠した ID プロバイダが構成されている必要があります。
- AD または LDAP ディレクトリサービスを使用する ID プロバイダのみがサポートされます。
- IDP の構成には、NetBackup API または NetBackup コマンド `nbidpcmd` が必要です。
- SAML ユーザーは API を使用できません。API キーはユーザーを認証するために使われるため、SAML 認証されたユーザーには使用できません。
- グローバルログアウトはサポートされません。

図 24-1 NAT 構成の例: プライベートネットワークの ID プロバイダ

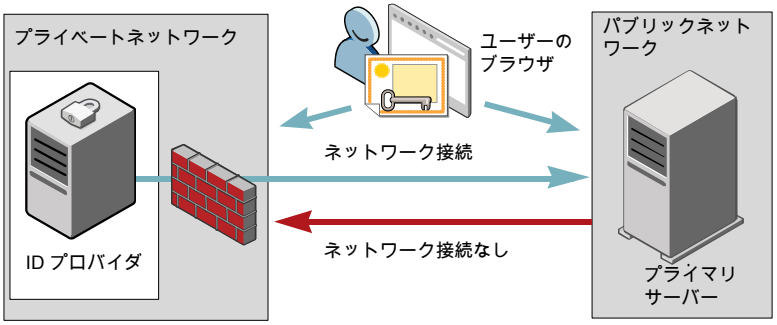


図 24-2 NAT 構成の例: プライベートネットワークのプライマリサーバー

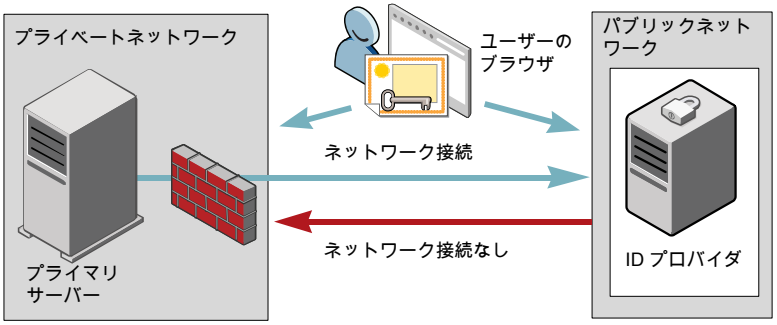


図 24-3 構成の例: 同じネットワークのプライマリサーバーと ID プロバイダ

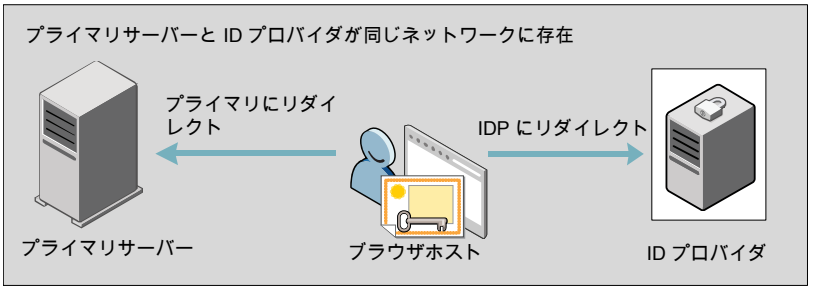
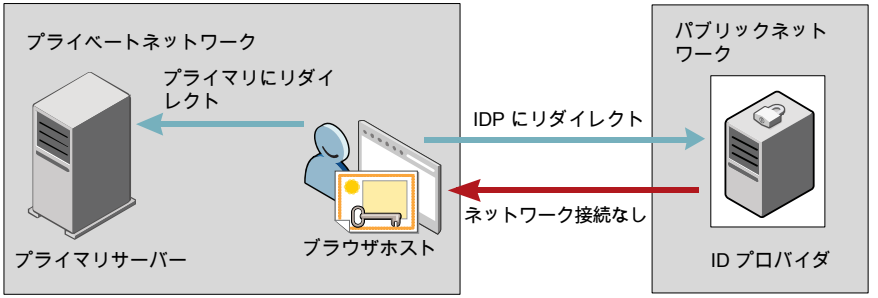


図 24-4 構成の例: プライベートネットワークのプライマリサーバーとパブリックネットワークの ID プロバイダ



NetBackup の SSO (シングルサインオン) の構成

この項では、IDP と NetBackup プライマリサーバー間で信頼を構築し、構成情報を交換する手順について説明します。手順を続行する前に、環境内で次の前提条件が満たされていることを確認します。

- IDP が、お使いの環境で設定および配備されています。
- IDP が、AD (Active Directory) またはライトウェイト ディレクトリ アクセス プロトコル (LDAP) のドメインユーザーを認証するように設定されています。

表 24-1 NetBackup のシングルサインオンを構成する手順

手順	処理	説明
1.	IDP メタデータ XML ファイルのダウンロード	IDP メタデータ XML ファイルを IDP からダウンロードして保存します。 XML ファイルに保存された SAML メタデータが、IDP と NetBackup プライマリサーバー間で構成情報を共有するために使用されます。IDP メタデータ XML ファイルは、NetBackup プライマリサーバーに IDP 構成を追加するために使用されます。
2.	NetBackup プライマリサーバーでの SAML キーストアの構成と IDP 構成の追加および有効化	p.176 の「SAML キーストアの構成」を参照してください。 p.178 の「SAML キーストアの構成と IDP 構成の追加および有効化」を参照してください。
3.	サービスプロバイダ (SP) メタデータ XML ファイルのダウンロード	NetBackup プライマリサーバーは、NetBackup 環境内の SP です。ブラウザに次の URL を入力して、NetBackup プライマリサーバーから SP メタデータ XML ファイルにアクセスします。 `https://masterserver/netbackup/sso/saml2/metadata` ここで *masterserver* には、NetBackup プライマリサーバーの IP アドレスまたはホスト名を指定します。
4.	サービスプロバイダ (SP) としての NetBackup プライマリサーバーの IDP への登録	p.180 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。
5.	必要な RBAC の役割に対する SSO を使用する SAML ユーザーと SAML グループの追加	SAML ユーザーと SAML ユーザーグループは、NetBackup プライマリサーバーで IDP が構成され、有効になっている場合にのみ RBAC で利用可能です。RBAC の役割の追加の手順については、次のトピックを参照してください。 p.193 の「役割へのユーザーの追加 (非 SAML)」を参照してください。

初回の設定後、IDP 構成を有効化、更新、無効化、または削除するかを選択できます。

p.181 の「IDP 構成の管理」を参照してください。

初期設定後、NetBackup CA SAML キーストアのアップデート、更新、または削除を選択できます。ECA SAML キーストアを構成して管理することもできます。

SAML キーストアの構成

NetBackup プライマリサーバーと IDP サーバーの間の信頼を確立するには、NetBackup プライマリサーバーに SAML キーストアを構成する必要があります。NetBackup CA を使用しているか、外部認証局 (ECA) を使用しているかに応じて、次のセクションのいずれかを参照してください。

メモ: 環境内で ECA と NetBackup CA の組み合わせを使用している場合、デフォルトでは、IDP サーバーとの信頼関係を確立するときに ECA が考慮されます。

メモ: `configureCerts.bat`、`configureCerts`、`configureSAMLECACert.bat`、`configureSAMLECACert` などのバッチファイルを使用した SAML キーストア構成と、それに対応するオプションは非推奨です。

NetBackup CA キーストアの構成

NetBackup CA を使用している場合は、NetBackup プライマリサーバー上に NetBackup CA キーストアを作成します。

NetBackup CA キーストアを作成するには

1. NetBackup プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -cCert -M master_server -f
   ```

   `-f` は省略可能です。強制更新のオプションを使用します。

NetBackup CA キーストアが作成されたら、NetBackup CA 証明書が更新されるたびに NetBackup CA キーストアを更新してください。

NetBackup CA キーストアを更新するには

1. NetBackup プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -rCert -M master_server
   ```

3 ブラウザに次の URL を入力して、NetBackup プライマリサーバーから新しい SP メタデータ XML ファイルをダウンロードします。

https://*primaryserver*/netbackup/sso/saml2/metadata

ここで、*primaryserver* は NetBackup プライマリサーバーの IP アドレスまたはホスト名です。

4 IDP に新しい SP メタデータ XML ファイルをアップロードします。

p.180 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

NetBackup CA キーストアを削除するには

1 NetBackup プライマリサーバーにルートまたは管理者としてログオンします。

2 次のコマンドを実行します。

```
nbidpcmd -dCert -M master_server
```

3 ブラウザに次の URL を入力して、NetBackup プライマリサーバーから新しい SP メタデータ XML ファイルをダウンロードします。

https://*primaryserver*/netbackup/sso/saml2/metadata

ここで、*primaryserver* は NetBackup プライマリサーバーの IP アドレスまたはホスト名です。

4 IDP に新しい SP メタデータ XML ファイルをアップロードします。

5 p.180 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

ECA キーストアの構成

ECA を使用している場合は、ECA キーストアを NetBackup プライマリサーバーにインポートします。

メモ: 環境内で ECA と NetBackup CA の組み合わせを使用している場合、デフォルトでは、IDP サーバーとの信頼関係を確立するときに ECA が考慮されます。NetBackup CA を使用するには、最初に ECA キーストアを削除する必要があります。

ECA キーストアを構成するには

1 プライマリサーバーにルートまたは管理者としてログオンします。

2 構成済みの NetBackup ECA キーストアを使用して SAML ECA キーストアを構成するか、ECA 証明書チェーンと秘密鍵を指定するかに応じて、次のコマンドを実行します。

- 構成済みの NetBackup ECA キーストアを使用するには、次のコマンドを実行します。

  ```
  nbidpcmd -cECACert -uECA existing ECA configuration [-f] [-M primary_server]
  ```

- ユーザーが指定した ECA 証明書チェーンと秘密鍵を使用するには、次のコマンドを実行します。

  ```
  nbidpcmd -cECACert -certPEM certificate chain file -privKeyPath private key file [-ksPassPath Keystore Passkey File] [-f] [-M <master_server>]
  ```

- 証明書チェーンファイル (certificate chain file) には証明書チェーンファイルのパスを指定します。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。
- 秘密鍵ファイル (private key file) には秘密鍵ファイルのパスを指定します。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。
- キーストアパスキーファイル (Keystore Passkey File) にはキーストアパスワードファイルパスを指定します。構成を実行するプライマリサーバーからこのファイルにアクセス可能である必要があります。
- プライマリサーバー (Primary server) は、SAML ECA キーストア構成を実行するプライマリサーバーのホスト名または IP アドレスです。コマンドを実行する NetBackup プライマリサーバーがデフォルトで選択されます。

ECA キーストアを削除するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. ブラウザに次の URL を入力して、NetBackup プライマリサーバーから新しい SP メタデータ XML ファイルをダウンロードします。

   https://*primaryserver*/netbackup/sso/saml2/metadata

   ここで、*primaryserver* は NetBackup プライマリサーバーの IP アドレスまたはホスト名です。
3. IDP に新しい SP メタデータ XML ファイルをアップロードします。

   p.180 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

SAML キーストアの構成と IDP 構成の追加および有効化

次の手順に進む前に、IDP メタデータ XML ファイルをダウンロードして NetBackup プライマリサーバーに保存したことを確認します。

SAML キーストアを構成し、IDP 構成を追加および有効化するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   IDP と NetBackup CA SAML キーストアの構成の場合:

   ```
   nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
   [-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
   group field] [-cCert] [-f] [-M primary server]
   ```

   または、IDP と ECA SAML キーストアの構成の場合:

   構成済みの NetBackup ECA キーストアを使用して SAML ECA キーストアを構成するか、ECA 証明書チェーンと秘密鍵を指定するかに応じて、次のコマンドを実行します。

   - NetBackup ECA 構成のキーストアを使用する:

     ```
     nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
     file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
     user group field] -cECACert -uECA existing ECA configuration
     [-f] [-M Primary Server]
     ```

   - ユーザーが指定した ECA 証明書チェーンと秘密鍵を使用する:

     ```
     nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
     file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
     user group field] -cECACert -certPEM certificate chain file
     -privKeyPath private key file [-ksPassPath KeyStore passkey
     file] [-f] [-M primary server]
     ```

   以下の説明に従って変数を置き換えます。

   - *IDP configuration name* は、IDP 構成に指定された一意の名前です。
   - *IDP XML metadata file* は、XML メタデータファイルへのパスです。これには、IDP の構成の詳細が Base64URL エンコードされた形式で含まれます。
   - `-e true | false` は、IDP 構成を有効または無効にします。IDP 構成が追加されて有効になっている必要があります。そうでない場合、ユーザーは SSO (シングルサインオン) オプションを使ってサインインできません。NetBackup プライマリサーバーに複数の IDP 構成を追加することもできますが、一度に 1 つの IDP 構成のみを有効にできます。
   - *IDP user field* および *IDP user group field* は、AD または LDAP の `userPrincipalName` および `memberOf` の属性にマッピングされる SAML 属性名です。

メモ: SAML 属性名が、それぞれ *username@domainname* および (CN=*group name*, DC=*domainname*) の形式で定義されていることを確認します。

- *primary Server* は、IDP 構成を追加または変更するプライマリサーバーのホスト名または IP アドレスです。コマンドを実行する NetBackup プライマリサーバーがデフォルトで選択されます。
- *Certificate Chain File* は証明書チェーンファイルのパスです。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。

  Private Key File は秘密鍵ファイルのパスです。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。

  KeyStore Passkey File はキーストアパスキーファイルのパスです。構成を実行するプライマリサーバーからこのファイルにアクセス可能である必要があります。

例: `nbidpcmd -ac -n veritas_configuration -mxp file.xml -t SAML2 -e true -u username -g group-name -cCert -M primary_server.abc.com`

IDP を使用した NetBackup プライマリサーバーの登録

IDP にサービスプロバイダ (SP) として NetBackup プライマリサーバーを登録する必要があります。特定の IDP に固有の順を追った手順については、次の表を参照してください。

表 24-2 NetBackup プライマリサーバーを登録するための IDP 固有の手順

IDP 名	手順へのリンク
ADFS	https://www.veritas.com/docs/100047744
Okta	https://www.veritas.com/docs/100047745
PingFederate	https://www.veritas.com/docs/100047746
Azure	https://www.veritas.com/docs/100047748
Shibboleth	https://www.veritas.com/docs/00047747

IDP を使用して SP を登録するには、通常、次の操作が含まれます。

IDP への SP メタデータ XML ファイルのアップロード

SP メタデータ XML ファイルには、SP 証明書、エンティティ ID、アサーションコンシューマーサービス URL (ACS URL)、およびログアウト URL (SingleLogoutService) が含ま

れます。SP メタデータ XML ファイルは、IDP が信頼関係を確立し、SP との間で認証と認可の情報を交換するために必要です。

AD または LDAP 属性への SAML 属性のマッピング

属性マッピングは、SSO の SAML 属性を AD または LDAP ディレクトリ内の対応する属性とマッピングするために使用されます。SAML 属性マッピングは、NetBackup プライマリサーバーに送信される SAML 応答の生成に使用されます。`userPrincipalName` にマッピングされる SAML 属性と、AD または LDAP ディレクトリ内の `memberOf` 属性を定義していることを確認します。SAML 属性は次の形式に従う必要があります。

表 24-3

対応する AD または LDAP 属性	SAML 属性形式
`userPrincipalName`	*username@domainname*
`memberOf`	(CN=*group name*, DC=*domainname*)

メモ: NetBackup プライマリサーバーに IDP の構成を追加するときに、ユーザー (`-u`) オプションとユーザーグループ (`-g`) オプションに入力する値は、AD または LDAP の `userPrincipalName` 属性および `memberOf` 属性にマッピングされている SAML 属性名と一致する必要があります。

p.178 の「SAML キーストアの構成と IDP 構成の追加および有効化」を参照してください。

IDP 構成の管理

NetBackup マスターサーバーで ID プロバイダ (IDP) の構成を管理するには、`nbidpcmd` コマンドの enable (`-e true`)、update (`-uc`)、disable (`-e false`)、および delete (`-dc`) オプションを使用します。

IDP 構成の有効化

デフォルトでは、本番環境で IDP 構成は有効になっていません。IDP を追加したときに有効にしなかった場合、`-uc -e true` オプションを使用して、IDP 構成を更新および有効化できます。

IDP 構成を有効化するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -uc -n IDP configuration name -e true
   ```

   IDP configuration name は、IDP 構成に指定された一意の名前です。

メモ: NetBackup プライマリサーバーに複数の IDP を構成することもできますが、一度に 1 つの IDP のみを有効にできます。

IDP 構成の更新

IDP 構成に関連付けられている XML メタデータファイルを更新できます。

IDP 構成内の IDP XML メタデータファイルを更新するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -uc -n IDP configuration name -mxp IDP XML metadata file
   ```

   以下の説明に従って変数を置き換えます。

   - *IDP configuration name* は、IDP 構成に指定された一意の名前です。
   - *IDP XML metadata file* は、XML メタデータファイルへのパスです。これには、IDP の構成の詳細が Base64URL エンコードされた形式で含まれます。

IDP 構成の IDP ユーザーまたは IDP ユーザーグループの値を更新する場合は、まず構成を削除する必要があります。更新後の IDP ユーザーまたは IDP ユーザーグループの値が含まれる構成を再度追加するまで、ユーザーは SSO (シングルサインオン) オプションを利用できません。

IDP 構成で IDP ユーザーまたは IDP ユーザーグループを更新するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. IDP 構成を削除します。

   ```
   nbidpcmd -dc -n IDP configuration name
   ```

   IDP configuration name は、IDP 構成に指定された一意の名前です。

3. 構成を再度追加して有効にするには、次のコマンドを実行します。

   ```
   nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
   [-t SAML2] [-e true | false] [-u IDP user] [-g IDP user group
   field] [-M Master Server
   ```

   以下の説明に従って変数を置き換えます。

- *IDP configuration name* は、IDP 構成に指定された一意の名前です。
- *IDP XML metadata file* は、XML メタデータファイルへのパスです。これには、IDP の構成の詳細が Base64URL エンコードされた形式で含まれます。
- -e true | false は、IDP 構成を有効または無効にします。IDP が利用可能で有効になっている必要があります。そうでない場合、ユーザーは SSO (シングルサインオン) オプションを使ってサインインできません。NetBackup プライマリサーバーに複数の IDP 構成を追加することもできますが、一度に 1 つの IDP 構成のみを有効にできます。
- *IDP user field* および *IDP user group field* は、AD または LDAP の userPrincipalName および memberOf の属性にマッピングされる SAML 属性の名前です。

メモ: SAML 属性名が、それぞれ *username@domainname* および (CN=*group name*, DC=*domainname*) の形式で定義されていることを確認します。

- *Master Server* は、IDP 構成を追加または変更するプライマリサーバーのホスト名または IP アドレスです。コマンドを実行する NetBackup プライマリサーバーがデフォルトで選択されます。

IDP 構成の無効化

製品環境で IDP 構成が無効化されている場合、ユーザーがサインインするときにその IDP の SSO (シングルサインオン) オプションを使用できません。

IDP 構成を無効化するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   nbidpcmd -uc -n *IDP configuration name* -e false

   IDP configuration name は、IDP 構成に指定された一意の名前です。

IDP 構成の削除

IDP 構成が削除された場合、ユーザーがサインインするときにその IDP の SSO (シングルサインオン) オプションを使用できません。

IDP 構成を削除するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   nbidpcmd -dc -n *IDP configuration name*

   IDP configuration name は、IDP 構成に指定された一意の名前です。

ビデオ: NetBackup でのシングルサインオンの設定

このビデオでは、NetBackup で SSO (シングルサインオン) を設定する方法の概要を説明します。

ビデオへのリンク

使用している IDP に応じて、IDP メタデータ XML ファイルをダウンロードして IDP で NetBackup プライマリサーバーを登録する手順を次の記事で参照してください。

- ADFS: https://www.veritas.com/docs/100047744
- Okta: https://www.veritas.com/docs/100047745
- PingFederate: https://www.veritas.com/docs/100047746
- Azure: https://www.veritas.com/docs/100047748
- Shibboleth: https://www.veritas.com/docs/100047747

NetBackup の SSO に関する詳細情報を参照できます。

p.174 の「NetBackup の SSO (シングルサインオン) の構成」を参照してください。

SSO のトラブルシューティング

このセクションでは、SSO に関連する問題をトラブルシューティングするための手順について説明します。

リダイレクトの問題

リダイレクトの問題に直面している場合は、Web サービスのログファイルのエラーメッセージを確認し、問題の原因を絞り込む必要があります。NetBackup は NetBackup Web サーバーのログと、Web サーバーアプリケーションのログを作成します。これらのログは次の場所に書き込まれます。

- UNIX の場合: `usr/openv/logs/nbwebservice`
- Windows の場合: *`install_path`*`¥NetBackup¥logs¥nbwebservice`

NetBackup Web UI が IDP のサインインページにリダイレクトしない

IDP メタデータ XML ファイルには、IDP 証明書、エンティティ ID、リダイレクト URL、ログアウト URL が含まれています。IDP XML メタデータファイルが古くなっている、または破損している場合、NetBackup Web UI が IDP のサインインページへのリダイレクトに失敗することがあります。次のメッセージが Web サービスのログに追加されます。

```
Failed to redirect to the IDP server.
```

NetBackup プライマリサーバーで最新の構成の詳細を利用できるようにするには、IDP から XML メタデータファイルの最新のコピーをダウンロードします。IDP XML メタデータファイルを使用して、NetBackup プライマリサーバーの最新の IDP 構成を追加して有効にします。p.178 の「SAML キーストアの構成と IDP 構成の追加および有効化」を参照してください。

IDP のサインインページが NetBackup Web UI にリダイレクトしない

IDP のサインインページでクレデンシャルを入力すると、NetBackup Web UI にリダイレクトするのではなく、ブラウザに[認証に失敗しました (Authentication Failed)]のエラーが表示されることがあります。Web サービスログで見つかったエラーに基づいた解決手順を、次の表で参照してください。

表 24-4

Web サービスログのエラーメッセージ	説明および推奨処置
`userPrincipalName not found in response.`	NetBackup プライマリサーバーに IDP の構成を追加するときに、ユーザー (`-u`) オプションに入力する値は、AD または LDAP の `userPrincipalName` 属性にマッピングされている SAML 属性名と一致する必要があります。詳しくは、p.178 の「SAML キーストアの構成と IDP 構成の追加および有効化」を参照してください。
`userPrincipalName is not in expected format`	IDP は、SAML ユーザーと SAML ユーザーグループの情報を含む NetBackup プライマリサーバーに SAML 応答を送信します。IDP がこの情報を正常に送信できるようにするには、IDP によって送信される `userPrincipalName` 属性の値が *username@domainname* の形式で定義されていることを確認します。 詳しくは、p.180 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

Web サービスログのエラーメッセージ	説明および推奨処置
`Authentication issue instant is too old or in the future`	このエラーは、次の理由で発生する場合があります。 ■ IDP サーバーと NetBackup プライマリサーバーの日付と時刻が同期されていません。 ■ デフォルトでは、NetBackup プライマリサーバーによって、ユーザーは 24 時間認証されたままにできます。このエラーは、IDP で 24 時間よりも長い間認証されたままにすることが許可されている場合に発生する可能性があります。このエラーを解決するには、IDP と一致するように NetBackup プライマリサーバーの SAML 認証期間を更新します。 NetBackup プライマリサーバーの `<installpath>¥var¥global¥wsl¥config¥web.conf` ファイルに新しい SAML 認証の有効期間を指定します。 たとえば、IDP の認証の有効期間が 36 時間の場合は、次のようにして、`web.conf` ファイルのエントリを更新します。 `SAML_ASSERTION_LIFETIME_IN_SECS=129600`
`Response is not success`	このエラーは、次の理由で発生する場合があります。 ■ IDP メタデータ XML ファイルに IDP 証明書が含まれています。NetBackup CA を使用している場合は、IDP 証明書が最新の NetBackup CA 証明書情報で更新されていることを確認します。詳しくは、p.176 の「SAML キーストアの構成」を参照してください。 ■ NetBackup CA のキーストアを使用している場合は、IDP で証明書失効リスト (CRL) を無効にする必要があります。

認証に関連する問題が原因でサインインできない

SSO を使用してサインインするには、必要な RBAC の役割に SAML ユーザーと SAML ユーザーグループを追加する必要があります。RBAC の役割が正しく割り当てられていない場合、NetBackup Web UI にサインインしているときに次のエラーが発生することがあります。

```
You are not authorized to access this application. Contact your
NetBackup security administrator to request RBAC permissions for the
NetBackup web user interface.
```

認証に関連する問題をトラブルシューティングするには、次の表を参照してください。

表 24-5

原因	説明および推奨処置
RBAC の役割が、SAML ユーザーおよび SAML グループに割り当てられていない	NetBackup プライマリサーバーで IDP 構成を追加して有効にした後、SSO を使用する SAML ユーザーと SAML ユーザーグループに必要な RBAC の役割が割り当てられていることを確認します。SAML ユーザーと SAML ユーザーグループは、NetBackup プライマリサーバーで IDP 構成が追加され、有効になってからのみ RBAC で利用可能です。 ユーザーの追加手順については、p.193 の「役割へのユーザーの追加 (非 SAML)」を参照してください。
RBAC の役割が、現在追加されておらず、有効になっていない IDP 構成に関連付けられている SAML ユーザーおよび SAML ユーザーグループに割り当てられている	RBAC で SAML ユーザーまたは SAML ユーザーグループを追加すると、SAML ユーザーまたは SAML ユーザーグループのエントリが、その時点で追加されて有効になっている IDP 構成と関連付けられます。 新しい IDP 構成を追加して有効にする場合は、SAML ユーザーまたは SAML ユーザーグループ用の別のエントリを追加していることも確認します。新しいエントリは、新しい IDP 構成に関連付けられます。 たとえば、ADFS IDP 構成を追加および有効化する間に、NBU_user が RBAC に追加され、必要な権限が割り当てられます。Okta IDP 構成を追加して有効にする場合は、NBU_user の新しいユーザーエントリを追加する必要があります。必要な RBAC の役割を、Okta IDP 構成に関連付けられている新しいユーザーエントリに割り当てます。 ユーザーの追加手順については、p.193 の「役割へのユーザーの追加 (非 SAML)」を参照してください。
RBAC の役割が、ローカルドメインユーザーまたは Active Directory (AD) または LDAP ドメインユーザー (SAML ユーザーと SAML ユーザーグループではなく) に割り当てられている	SAML ユーザーまたは SAML ユーザーグループのレコードは、RBAC にすでに追加されている、対応するローカルドメインユーザーまたは AD または LDAP ドメインユーザーと同様に表示されることがあります。 NetBackup プライマリサーバーで IDP 構成を追加して有効にした後、RBAC の SAML ユーザーと SAML ユーザーグループを追加し、必要な権限が割り当てられていることを確認します。SAML ユーザーと SAML ユーザーグループは、NetBackup プライマリサーバーで IDP 構成が追加され、有効になってからのみ RBAC で利用可能です。 SAML ユーザーとユーザーグループの追加手順については、p.193 の「役割へのユーザーの追加 (非 SAML)」を参照してください。

原因	説明および推奨処置
NetBackup プライマリサーバーが、IDP からユーザーグループ情報を取得できない	IDP は、SAML ユーザーと SAML ユーザーグループの情報を含む NetBackup プライマリサーバーに SAML 応答を送信します。IDP がこの情報を正常に送信できるようにするには、次のことを確認します。 ■ IDP は、AD または LDAP のドメインユーザーを認証するように構成されています。 ■ IDP によって送信される `memberOf` 属性の値は、{cn=groupname,dc=domain} のように、X.500 識別形式で指定します。 ■ NetBackup プライマリサーバーに IDP の構成を追加するときに、ユーザーグループ (`-g`) オプションに入力する値は、AD または LDAP の `memberOf` 属性にマッピングされている SAML 属性名と一致します。詳しくは、p.178 の「SAML キーストアの構成と IDP 構成の追加および有効化」を参照してください。

25

役割ベースのアクセス制御の管理

この章では以下の項目について説明しています。

RBAC の機能

NetBackup Web ユーザーインターフェースは、NetBackup 環境に役割に基づくアクセス制御を適用する機能を提供します。RBAC を使用して、現在 NetBackup へのアクセス権を持たないユーザーにアクセス権を提供します。または、現在管理者アクセス権を持っている NetBackup ユーザーに対して、組織内の役割に基づいて制限されたアクセス権を提供できます。

NetBackup 管理コンソールのアクセス制御方法と、root ユーザーおよび管理者向けのアクセス制御と監査について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

表 25-1 RBAC の機能

機能	説明
ユーザーに特定のタスクの実行を許可する役割	ユーザーを 1 つ以上のデフォルトの RBAC の役割に追加するか、ユーザーの役割に合わせてカスタムの役割を作成します。管理者の役割にユーザーを追加して、そのユーザーに完全な NetBackup 権限を付与します。 p.196 の「 デフォルトの RBAC の役割」を参照してください。
ユーザーの役割に合った NetBackup 領域および機能へのアクセス許可	RBAC ユーザーは、そのビジネスの役割において一般的なタスクを実行できますが、その他の NetBackup の領域や機能へのアクセスは制限されます。RBAC は、ユーザーが表示または管理できる資産も制御します。
RBAC イベントの監査	NetBackup は、RBAC イベントを監査します。
DR 準備完了	RBAC 設定は、NetBackup カタログで保護されています。
以前のインターフェース向けの拡張監査または認証 (auth.conf) の構成の継続利用	拡張監査はすべてのインターフェースでサポートされます。認証 (auth.conf) の構成を、NetBackup 管理コンソールと CLI を通じて引き続き使用できます。これらの以前のインターフェースを使用して、NetBackup Web UI と NetBackup API ではまだサポートされていないワークフローへのアクセスを管理できます。 auth.conf ファイルは、NetBackup Web UI または NetBackup API へのアクセスを制限しない点に注意してください。

権限を持つユーザー

次のユーザーは、NetBackup Web UI にサインインして使用する権限を持ちます。

表 25-2 NetBackup Web UI を使用する権限を持つユーザー

ユーザー	アクセス権	注意事項
root OS 管理者 拡張監査ユーザー RBAC 管理者の役割を持つユーザー	完全	OS 管理者の自動アクセス権を無効にできます。 p.195 の「OS (オペレーティングシステム) 管理者の Web UI アクセス権の無効化」を参照してください。 拡張監査について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。
nbasecadmin Appliance ユーザー appadmin Flex Appliance ユーザー	デフォルトのセキュリティ管理者の役割	この役割は、他のアプライアンスユーザーにアクセス権を付与できます。 NetBackup Appliance のデフォルトの admin ユーザーには、Web UI へのアクセス権はありません。
Web UI へのアクセス権を付与する RBAC の役割を持つユーザー	ユーザーに応じて異なる	p.191 の「RBAC の構成」を参照してください。

RBAC の構成

NetBackup Web UI の役割に基づくアクセス制御を構成するには、次の手順を実行します。

表 25-3　　役割ベースのアクセス制御を構成する手順

手順	処理	説明
1	すべての Active Directory または LDAP ドメインを構成します。	ドメインユーザーを追加する前に、NetBackup で Active Directory または LDAP ドメインを認証する必要があります。 『NetBackup セキュリティおよび暗号化ガイド』を参照してください。
2	ユーザーに必要な権限を決定します。	ユーザーが日々のタスクを実行するために必要な権限を決定します。 デフォルトの RBAC の役割を使用するか、デフォルトの役割をテンプレートとして使用して、新しい役割を作成できます。または、必要に応じて、完全なカスタム役割を作成することもできます。 p.203 の「役割の権限」を参照してください。 p.196 の「 デフォルトの RBAC の役割」を参照してください。 p.198 の「カスタムの RBAC 役割の追加」を参照してください。
3	適切な役割にユーザーを追加します。	p.193 の「役割へのユーザーの追加 (非 SAML)」を参照してください。 p.194 の「役割へのユーザーの追加 (SAML)」を参照してください。 p.194 の「役割へのスマートカードユーザーの追加 (非 SAML、AD/LDAP なし)」を参照してください。
4	OS 管理者に必要な権限を決定します。	p.195 の「OS (オペレーティングシステム) 管理者の Web UI アクセス権の無効化」を参照してください。 p.196 の「OS (オペレーティングシステム) 管理者のコマンドライン (CLI) アクセス権の無効化」を参照してください。

NetBackup RBAC を使用するための注意事項

RBAC の役割の権限を構成する場合は、次の点に注意してください。

- RBAC は、NetBackup 管理コンソールではなく、Web UI へのアクセスのみを制御します。
- 役割を作成するときに、ユーザーが Web UI にサインインして使用できるようにするために、最小数のアクセス権を確実に有効にします。個々のアクセス権が、Web UI の画面と直接的な相関を持たない場合があります。この種類のアクセス権しか付与されていないユーザーがサインインを試みると、「権限がない」ことを示すメッセージを受け取ります。

- ユーザーが役割に追加または削除された場合、ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。
- ほとんどの権限は暗黙的ではありません。
  ほとんどのケースで、[作成 (Create)]の権限では、ユーザーに[表示 (View)]権限は付与されません。[リカバリ (Recovery)]権限では、[表示 (View)]権限や、[上書き (Overwrite)]などのその他のリカバリオプションはユーザーに付与されません。
- すべての RBAC 制御された操作を NetBackup Web UI から使用できるわけではありません。これらの種類の操作は RBAC に含まれているので、役割の管理者は API ユーザーと Web UI ユーザーの役割を作成できます。
- 一部のタスクでは、複数の RBAC カテゴリの権限をユーザーに付与する必要があります。たとえば、リモートプライマリサーバーとの信頼関係を確立するには、ユーザーはリモートプライマリサーバーと信頼できるプライマリサーバーの両方に対する権限を持っている必要があります。

AD または LDAP ドメインの追加

NetBackup は、AD (Active Directory) または LDAP (ライトウェイトディレクトリアクセスプロトコル) のドメインユーザーをサポートします。RBAC の役割にドメインユーザーを追加する前に、AD または LDAP ドメインを追加する必要があります。また、ドメインでスマートカード認証を構成する前に、ドメインを追加する必要もあります。

`POST /security/domains/vxat` API または `vssat` コマンドを使用してドメインを設定できます。

`vssat` コマンドとそのオプションについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。トラブルシューティングについて詳しくは、『NetBackup セキュリティと暗号化ガイド』を参照してください。

RBAC でのユーザーの表示

RBAC に追加されているユーザーと、そのユーザーに割り当てられている役割を表示できます。[ユーザー (Users)]リストは表示専用です。役割に割り当てられているユーザーを編集するには、その役割を編集する必要があります。

RBAC でユーザーを表示するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [ユーザー (Users)]タブをクリックします。
3. [役割 (Roles)]列に、ユーザーが割り当てられている各役割が表示されます。

役割へのユーザーの追加 (非 SAML)

このトピックでは、非 SAML ユーザーまたはグループを役割に追加する方法について説明します。

非 SAML ユーザーは、ユーザー名とパスワードでサインインするか、スマートカードでサインインする方式を使用できます。

役割にユーザーを追加するには (非 SAML)

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [ロール (Roles)]タブをクリックします。
3. 役割名をクリックし、[ユーザー (Users)]タブをクリックします。
4. (該当する場合) [サインインの種類 (Sign-in type)]リストで次から選択します。
   - [デフォルトのサインイン (Default sign-in)]: ユーザー名とパスワードで NetBackup にサインインするユーザーの場合に選択します。
   - [スマートカードユーザー (Smart card user)]: スマートカードを使用して NetBackup にサインインするユーザーの場合に選択します。

   注意: [サインインの種類 (Sign-in type)]リストは、NetBackup に利用可能な IDP 構成がある場合にのみ利用可能です。
5. 追加するユーザーまたはグループの名前を入力します。

ユーザーの種類	使用する形式	例
ローカルユーザーまたはグループ	*username*	jane_doe
	groupname	admins
Windows ユーザーまたはグループ	*DOMAIN*¥*username*	WINDOWS¥jane_doe
	DOMAIN¥groupname	WINDOWS¥Admins
UNIX ユーザーまたはグループ	*username*@*domain*	john_doe@unix
	groupname@*domain*	admins@unix

6. [リストに追加 (Add to list)]をクリックします。
7. ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割へのスマートカードユーザーの追加 (非 SAML、AD/LDAP なし)

このトピックでは、スマートカードユーザーを役割に追加する方法について説明します。この場合、ユーザーは非 SAML ユーザーで、AD または LDAP ドメインの関連付けやマッピングはありません。この形式の構成では、ユーザーグループはサポートされません。

このタイプのユーザーは、スマートカードによるサインイン方法を使用します。

役割にスマートカードユーザーを追加するには (非 SAML、AD/LDAP なし)

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [ロール (Roles)]タブをクリックします。
3. 役割名をクリックし、[ユーザー (Users)]タブをクリックします。
4. (該当する場合) [サインインの種類 (Sign-in type)]リストで[スマートカードユーザー (Smart card user)]を選択します。

   メモ: [サインインの種類 (Sign-in type)]リストは、NetBackup に利用可能な IDP 構成がある場合にのみ利用できます。[サインインの種類 (Sign-in type)]リストにあるスマートカードユーザーオプションは、AD または LDAP ドメインマッピングなしでスマートカードの構成を行うときに使用できます。

5. 追加するユーザー名を入力します。

   証明書で利用可能な正確な一般名 (CN) またはユニバーサルプリンシパル名 (UPN) を指定します。
6. [リストに追加 (Add to list)]をクリックします。
7. ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割へのユーザーの追加 (SAML)

このトピックでは、SAML ユーザーまたはグループを役割に追加する方法について説明します。

SAML ユーザーは、SAML ユーザーまたは SAML グループのいずれかのサインイン方式を使用します。

役割にユーザーを追加するには (SAML)

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [ロール (Roles)]タブをクリックします。
3. 役割名をクリックし、[ユーザー (Users)]タブをクリックします。

4 [サインインの種類 (Sign-in type)]リストから、サインイン方法として[SAML ユーザー (SAML user)]または[SAML グループ (SAML group)]を選択します。

5 追加するユーザーまたはグループの名前を入力します。

たとえば、nbuadmin@my.host.com です。

6 [リストに追加 (Add to list)]をクリックします。

7 ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割からのユーザーの削除

役割を持つユーザーに対する権限を削除する場合、役割からユーザーを削除できます。

ユーザーが役割から削除された場合、ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割からユーザーを削除するには

1 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。

2 [ロール (Roles)]タブをクリックします。

3 編集する役割をクリックし、[ユーザー (Users)]タブを選択します。

4 削除するユーザーを見つけ、[処理 (Actions)]、[削除 (Remove)]、[削除 (Remove)]の順にクリックします。

OS (オペレーティングシステム) 管理者の Web UI アクセス権の無効化

デフォルトで、OS 管理者 (ユーザーまたはグループメンバー) は NetBackup Web UI にアクセスでき、RBAC の役割のメンバーである必要はありません。

OS 管理者に自動的にこのアクセス権を付与しない場合は、無効にできます。その場合、OS 管理者が Web UI にアクセスするには RBAC 管理者の役割が必要になります。

OS 管理者の Web UI アクセス制御を無効にするには

1 左側で、[セキュリティ (Security)]、[RBAC]の順に選択します。

2 右上で、[役割ベースのアクセス制御設定 (Role-based access control settings)]をクリックします。

3 [オペレーティングシステム管理者の Web UI アクセス権 (Web UI access for Operating System Administrator)]をオフにします。

OS (オペレーティングシステム) 管理者のコマンドライン (CLI) アクセス権の無効化

デフォルトで、OS 管理者 (ユーザーまたはグループメンバー) は NetBackup CLI にアクセスでき、RBAC の役割のメンバーである必要はありません。

OS 管理者に自動的にこのアクセス権を付与しない場合は、無効にできます。その場合、OS 管理者が CLI にアクセスするには、`bpnbat -login` を使用してログインする必要があります。

OS 管理者の CLI アクセス権を無効にするには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択します。
2. 右上で、[役割ベースのアクセス制御設定 (Role-based access control settings)]をクリックします。
3. [オペレーティングシステム管理者の CLI アクセス権 (CLI access for Operating System Administrator)]をオフにします。

デフォルトの RBAC の役割

NetBackup Web UI には、事前に権限や設定が構成されたデフォルトの RBAC の役割が用意されています。

表 25-4 NetBackup Web UI のデフォルトの RBAC の役割

役割名	説明
管理者	管理者の役割は、NetBackup の完全な権限を持ち、NetBackup のすべての側面を管理できます。
デフォルトの Apache Cassandra 管理者	この役割には、保護計画で Apache Cassandra 資産を管理および保護するために必要なすべての権限が付与されます。
デフォルトの AHV 管理者	この役割には、Nutanix Acropolis Hypervisor を管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。
デフォルトのクラウド管理者	この役割には、クラウド資産を管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。 PaaS 管理者には、カスタム役割に追加できる追加の権限が必要であることに注意してください。 p.202 の「PaaS 管理者のカスタムの RBAC の役割の追加」を参照してください。
デフォルトのクラウドオブジェクトストア管理者	この役割には、従来のポリシーを使用してクラウドオブジェクトの保護を管理するためのすべての権限が付与されます。

役割名	説明
デフォルトの NetBackup コマンドライン (CLI) 管理者	この役割には、NetBackup コマンドライン (CLI) を使用して NetBackup を管理するために必要なすべての権限が付与されています。この役割を使用すると、ユーザーは、root 以外のアカウントでほとんどの NetBackup コマンドを実行できます。 注意: この役割のみを持つユーザーは、Web UI にサインインできません。
デフォルトの Kubernetes 管理者	この役割には、Kubernetes を管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。この役割の権限によって、ユーザーは Kubernetes 資産のジョブを表示および管理できます。この資産タイプのすべてのジョブを表示するには、その作業負荷に対するデフォルトの役割がユーザーに割り当てられている必要があります。または、役割を作成するときに、同様のカスタム役割にオプション[選択した権限を既存および今後のすべての作業負荷資産に適用する (Apply selected permissions to all existing and future workload assets)]を適用する必要があります。
デフォルトの Microsoft SQL Server 管理者	この役割には、SQL Server データベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。この役割に加えて、NetBackup ユーザーは次の必要条件を満たす必要があります。 ■ Windows 管理者グループのメンバーである必要があります。 ■ SQL Server の「sysadmin」の役割を持っている必要があります。
デフォルトの MySQL 管理者	この役割には、MySQL インスタンスとデータベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。
デフォルトの Oracle 管理者	この役割には、Oracle データベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。
デフォルトの PostgreSQL 管理者	この役割には、PostgreSQL インスタンスとデータベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。
デフォルトの Resiliency 管理者	この役割には、Veritas Resiliency Platform (VRP) for VMware の資産を保護するためのすべての権限が付与されています。
デフォルトの RHV 管理者	この役割には、Red Hat Virtualization マシンを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。この役割によって、ユーザーは RHV 資産のジョブを表示および管理できます。 RHV 資産のすべてのジョブを表示するには、ユーザーにこの役割が必要です。または役割が作成される際、ユーザーには、[選択した権限を既存および今後のすべての RHV 資産に適用する (Apply selected permissions to all existing and future RHV assets)]オプションが適用された同様のカスタム役割が必要です。
デフォルトの SaaS 管理者	この役割には、SaaS 資産を表示および管理するためのすべての権限が付与されています。
デフォルトのセキュリティ管理者	この役割には、NetBackup セキュリティ (役割ベースのアクセス制御 (RBAC)、証明書、ホスト、ID プロバイダとドメイン、グローバルセキュリティ設定、その他の権限など) を管理する権限があります。またこの役割は、NetBackup のほとんどの領域の設定と資産 (作業負荷、ストレージ、ライセンス、その他の領域) を表示できます。

役割名	説明
デフォルトのストレージ管理者	この役割には、ディスクベースのストレージとストレージライフサイクルポリシーを構成するための権限があります。SLP 設定は管理者役割で管理されます。
デフォルトのユニバーサル共有管理者	この役割には、ポリシーとストレージサーバーを管理するための権限があります。また、Windows および標準のクライアント形式の資産と、ユニバーサル共有の資産を管理できます。
デフォルトの VMware 管理者	この役割には、VMware 仮想マシンを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。VMware 資産のすべてのジョブを表示するには、ユーザーにこの役割が必要です。または役割が作成される際、ユーザーには、[選択した権限を既存および今後のすべての VMware 資産に適用する (Apply selected permissions to all existing and future VMware assets)]オプションが適用された同様のカスタム役割が必要です。

メモ: Veritas は、今後のリリースでデフォルトの役割の RBAC 権限を更新する権限を留保します。更新された権限は、NetBackup のアップグレード時にこれらの役割のユーザーに自動的に適用されます。デフォルトの役割のコピーがある場合、これらの役割は自動的には更新されません。これらのカスタム役割にもデフォルトの役割に対する変更を適用するには、手動で変更を適用するか、カスタム役割を再作成する必要があります。

カスタムの RBAC 役割の追加

ユーザーが作業負荷資産、保護計画、またはクレデンシャルに対して持つ権限とアクセス権を手動で定義する場合は、カスタムの RBAC の役割を作成します。

メモ: Veritas は、今後のリリースでデフォルトの役割の RBAC 権限を更新する権限を留保します。更新された権限は、NetBackup のアップグレード時にこれらの役割のユーザーに自動的に適用されます。デフォルトの役割 (またはデフォルトの役割に基づくカスタム役割) のコピーは、自動的には更新されません。

カスタムの RBAC の役割を追加するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]をクリックします。
2. 作成する役割の種類を選択します。

   その種類の役割の定義済み権限と設定をすべて含んだ、デフォルトの役割のコピーを作成できます。または、[カスタム役割 (Custom role)]を選択して、役割に付与するすべて権限を手動で設定します。

3 [ロール名 (Role name)]と説明を指定します。

たとえば、特定の部署や地域のバックアップ管理者であるすべてのユーザー向けのロールであることを示す場合が考えられます。

4 [権限 (Permissions)] で[割り当て (Assign)]をクリックします。

選択する権限によって、役割に対して設定できるその他の設定が決まります。

デフォルトの役割の種類を選択すると、特定の権限が、その種類の役割に必要な場合にのみ有効になります。たとえば、デフォルトのストレージ管理者には、保護計画に対する権限は不要です。デフォルトの Microsoft SQL Server 管理者にはクレデンシャルが必要です。

- [作業負荷 (Workloads)]は、[資産 (Asset)]の権限を選択すると有効になります。
- [保護計画 (Protection plans)]は、[保護計画 (Protection plans)]の権限を選択すると有効になります。
- [クレデンシャル (Credentials)]は、[クレデンシャル (Credentials)]の権限を選択すると有効になります。

5 役割の権限を構成します。

p.203 の「役割の権限」を参照してください。

p.191 の「NetBackup RBAC を使用するための注意事項」を参照してください。

6 [ユーザー (Users)]で[割り当て (Assign)]をクリックします。

7 役割の構成が完了したら、[保存 (Save)]をクリックします。

注意: 役割の作成後、資産、保護計画、クレデンシャルの権限は、Web UI の該当するノードで直接編集する必要があります。たとえば、VMware の権限を編集するには、[作業負荷 (Workloads)]、[VMware]の順に移動し、[VMware 設定 (VMware settings)]、[権限の管理 (Manage permissions)]の順に選択します。または、VM の詳細を開き、[権限 (Permissions)]タブをクリックします。

カスタム役割の編集または削除

カスタム役割を持つユーザーに対するアクセス権を変更または削除する場合に、この役割を編集または削除できます。デフォルトの役割は編集または削除できません。デフォルトの役割に対してユーザーを追加または削除することのみ可能です。

カスタム役割の編集

メモ: カスタム役割のアクセス権を変更すると、その役割に割り当てられているすべてのユーザーに変更が影響します。

カスタム役割を編集するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [ロール (Roles)]タブで、編集するカスタム役割を特定してクリックします。
3. 役割の説明を編集するには、[名前と説明を編集する (Edit name and description)]をクリックします。
4. 役割の権限を編集します。役割について次の詳細情報を編集できます。

役割のグローバル権限	[グローバル権限 (Global permissions)]タブで、[編集 (Edit)]をクリックします。
役割のユーザー	[ユーザー (Users)]タブをクリックします。
役割のアクセス定義	[アクセス定義 (Access definitions)]タブをクリックします。

p.203 の「役割の権限」を参照してください。

p.191 の「NetBackup RBAC を使用するための注意事項」を参照してください。

5. 役割のユーザーを追加または削除するには、[ユーザー (Users)]タブをクリックします。

p.193 の「役割へのユーザーの追加 (非 SAML)」を参照してください。

p.195 の「役割からのユーザーの削除」を参照してください。

6. 資産、保護計画、クレデンシャルの権限は、Web UI の該当するノードで直接編集する必要があります。

カスタム役割の削除

メモ: 役割を削除すると、その役割に割り当てられていたすべてのユーザーが、役割で提供されていたすべてのアクセス権を失います。

カスタム役割を削除するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [ロール (Roles)]タブをクリックします。
3. 削除するカスタム役割を特定して、そのチェックボックスにチェックマークを付けます。
4. [削除 (Remove)]、[はい (Yes)]の順にクリックします。

Azure 管理対象インスタンスをリストアするためのカスタムの RBAC の役割の追加

Azure 管理対象インスタンスをリストアするには、そのインスタンスの表示権限がユーザーに付与されている必要があります。管理者および同様のユーザーは、その他のユーザーにカスタム役割とこの権限を付与できます。

Azure 管理対象インスタンスの表示権限を割り当てるには

1 管理対象インスタンスのアクセス制御 ID を取得するには、次のコマンドを入力します。

```
GET
/asset-service/workloads/cloud/assets?filter=extendedAttributes/
managedInstanceName eq 'managedInstanceName'
```

レスポンスの中から *accessControlId* フィールドを探します。このフィールドの値をメモします。

2 役割 ID を取得するには、次のコマンドを入力します。

```
GET /access-control/roles
```

レスポンスの中から *id* フィールドを探します。このフィールドの値をメモします。

3 次のように、アクセス定義を作成します。

```
POST /access-control/managed-objects/{objectId}/access-definitions
```

要求ペイロード

```
{

    "data": {
        "type": "accessDefinition",
        "attributes": {
            "propagation": "OBJECT_AND_CHILDREN"
        },
        "relationships": {
            "role": {
                "data": {
                    "id": "<roleId>",
                    "type": "accessControlRole"
                }
            },
            "operations": {
                "data": [
                    {
                        "id": "|OPERATIONS|VIEW|",
```

```
                        "type": "accessControlOperation"
                    }
                ]
            },
            "managedObject": {
                "data": {
                    "id": "<objectId>",
                    "type": "managedObject"
                }
            }
        }
    }
}
```

次の値を使用します。

- `objectId`: 手順 1 で取得した *accessControlId* の値を使用します。
- `roleId`: 手順 2 で取得した *id* の値を使用します。

メモ: 代替リストアの場合は、*operations* リストに `|OPERATIONS|ASSETS|CLOUD|RESTORE_DESTINATION|` 権限を指定します。

PaaS 管理者のカスタムの RBAC の役割の追加

PaaS 管理者には、追加のストレージ権限が必要です。デフォルトのクラウド管理者の役割をテンプレートとして使用して、カスタムの役割を作成できます。

カスタムの RBAC の役割を追加するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]をクリックします。
2. [デフォルトのクラウド管理者 (Default Cloud Administrator)]を選択します。
3. [役割名 (Role name)]と説明を指定します。

   たとえば、役割が PaaS 管理者であるすべてのユーザーを対象としていることを示すこともできます。
4. [権限 (Permissions)] で[割り当て (Assign)]をクリックします。

5 [グローバル (Global)]タブで[ストレージ (Storage)]セクションを展開します。次の権限を選択します。

ディスクプール	表示
ストレージサーバー	表示
ストレージユニバーサル共有	表示、作成

6 [割り当て (Assign)]をクリックします。

7 [ユーザー (Users)]で[割り当て (Assign)]をクリックします。次に、このカスタム役割へのアクセス権を付与する各ユーザーを追加します。

8 役割の構成が完了したら、[役割の追加 (Add role)]をクリックします。

役割の権限

役割の権限は、役割のユーザーが実行する権限を持つ操作を定義します。

個々の RBAC 権限と依存関係について詳しくは、NetBackup API のマニュアルを参照してください。

http://sort.veritas.com

表 25-5 NetBackup RBAC の役割の権限

カテゴリ	説明
グローバル	グローバル権限は、すべての資産またはオブジェクトに適用されます。 BMR - BMR の構成と管理。 NetBackup Web 管理コンソールの管理 (NetBackup Web Management Console Administration) - Veritas のサポートのガイダンスを受け、NetBackup のトラブルシューティングを行い、JVM ガーベジコレクションを実行するための診断ファイルを作成できます。 これらの操作は、NetBackup API からのみ利用可能です。JVM のチューニングオプションについて詳しくは、『NetBackup インストールガイド』、『NetBackup アップグレードガイド』を参照してください。 NetBackup の管理 - NetBackup の構成と管理。 保護 - NetBackup バックアップポリシーとストレージライフサイクルポリシー。 セキュリティ - NetBackup のセキュリティ設定。 ストレージ - バックアップストレージの設定の管理。

カテゴリ	説明
資産	1 つ以上の資産タイプを管理します。たとえば、VMware 資産です。
保護計画	保護計画を使用してバックアップを実行する方法を管理します。
クレデンシャル	NetBackup の資産とその他の機能のクレデンシャルを管理します。

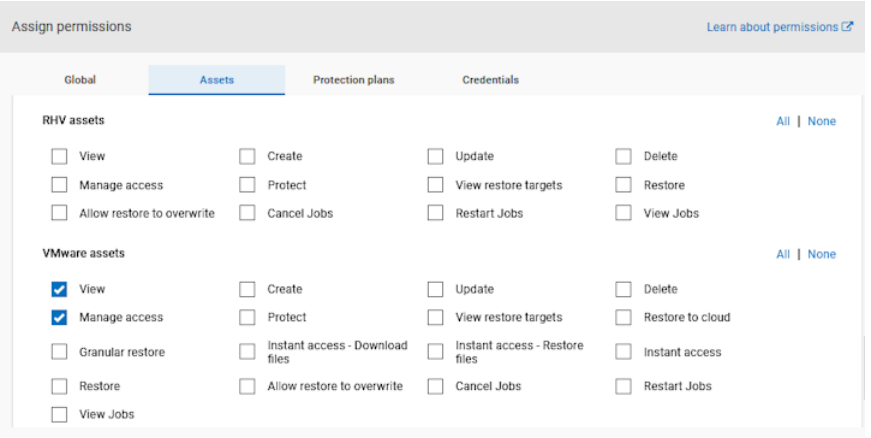
アクセスの管理権限

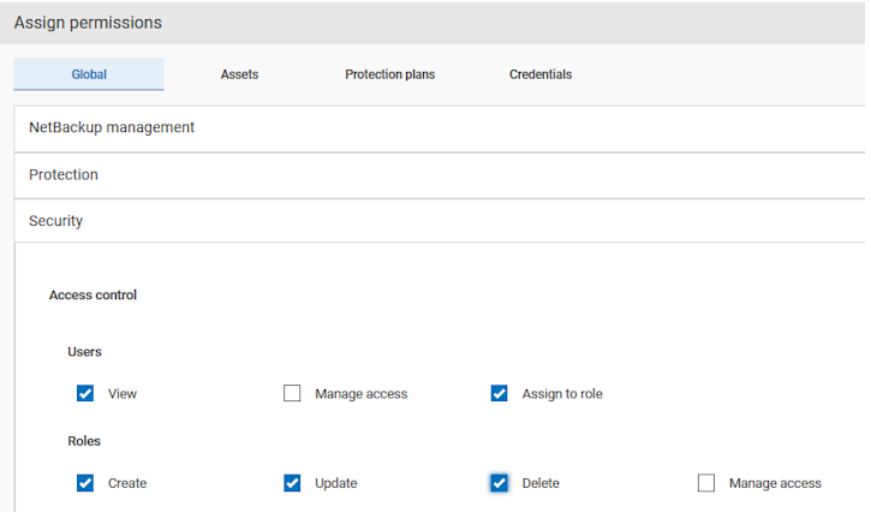
アクセス管理権限により、ユーザーは NetBackup の特定の部分にアクセスできるユーザーを管理できます。アクセスを管理するユーザーもアクセス制御権限を必要とします。この権限は、各権限のカテゴリに対して利用可能です。ただし、一部のカテゴリでは、アクセスの管理機能は NetBackup API からのみ利用可能で、NetBackup Web UI からは利用できません。

たとえば、VMware 資産に対してアクセスの管理権限を持つユーザーは、VMware 資産へのアクセス権を持つカスタム役割を追加または削除できます。このユーザーは、VMware 資産に対してカスタム役割が持つ特定の権限を追加または削除することもできます。

カスタム役割へのアクセスの管理権限の追加

デフォルトの役割に、ユーザーが必要とするアクセスの管理権限がない場合、その権限を持つカスタム役割を作成できます。また、ユーザーにユーザーと役割の権限を付与できます。これらの権限により、ユーザーを表示して役割に追加したり、役割を追加および管理したりできます。





カスタム役割のアクセス権の削除

カスタム役割の Web UI 領域へのアクセス権を削除できます。アクセスの管理権限を削除する各カテゴリに対して、[アクセスの管理 (Manage access)]権限を消去します。資産、保護計画、クレデンシャルの権限は、Web UI の該当するノードで直接編集する必要があります。

たとえば、VMware のアクセスの管理権限を削除するには、[作業負荷 (Workloads)]、[VMware]の順に移動し、[VMware 設定 (VMware settings)]、[権限の管理 (Manage permissions)]の順に選択します。または、VM の詳細を開き、[権限 (Permissions)]タブをクリックします。

アクセスの定義の表示

アクセスの定義は、RBAC の役割の一部である権限を示します。

アクセスの定義の表示

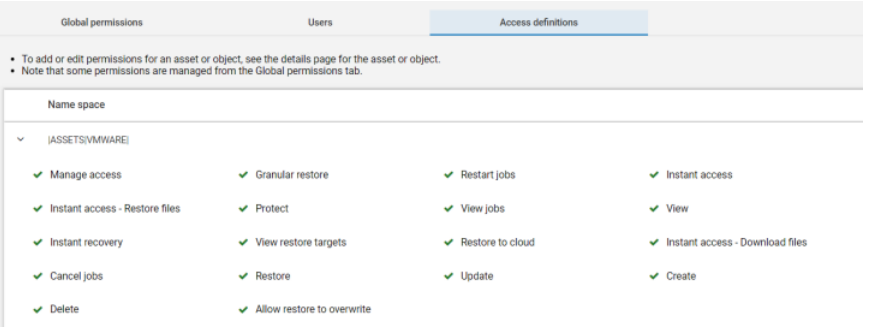
Web UI で役割のアクセスの定義を表示するには、その役割に対する表示権限が必要です。

アクセスの定義を表示するには

1. 左側で[セキュリティ (Security)]、[RBAC]の順に選択し、[役割 (Roles)]タブをクリックします。
2. 役割をクリックします。

3 [アクセス定義 (Access definitions)]タブをクリックします。

4 名前空間を展開して、その名前空間に割り当てられている権限を表示します。



アクセスの定義の削除

注意: アクセスの定義を削除する場合には注意が必要です。この処理により、その役割のユーザーの NetBackup に対する重要なアクセス権が削除される場合があります。

カスタム役割からアクセスの定義を削除できます。

アクセスの定義を表示するには

1 左側で[セキュリティ (Security)]、[RBAC]の順に選択し、[役割 (Roles)]タブをクリックします。

2 役割をクリックします。

3 [アクセス定義 (Access definitions)]タブをクリックします。

4 削除する名前空間を見つけます。

5 [操作 (Action)]、[削除 (Remove)]の順にクリックします。

6

検出とレポート

26

マルウェアの検出

この章では以下の項目について説明しています。

マルウェアの検出について

NetBackup は、サポート対象のバックアップイメージからマルウェアを検出し、マルウェアなしの最新の良好なイメージを検出します。

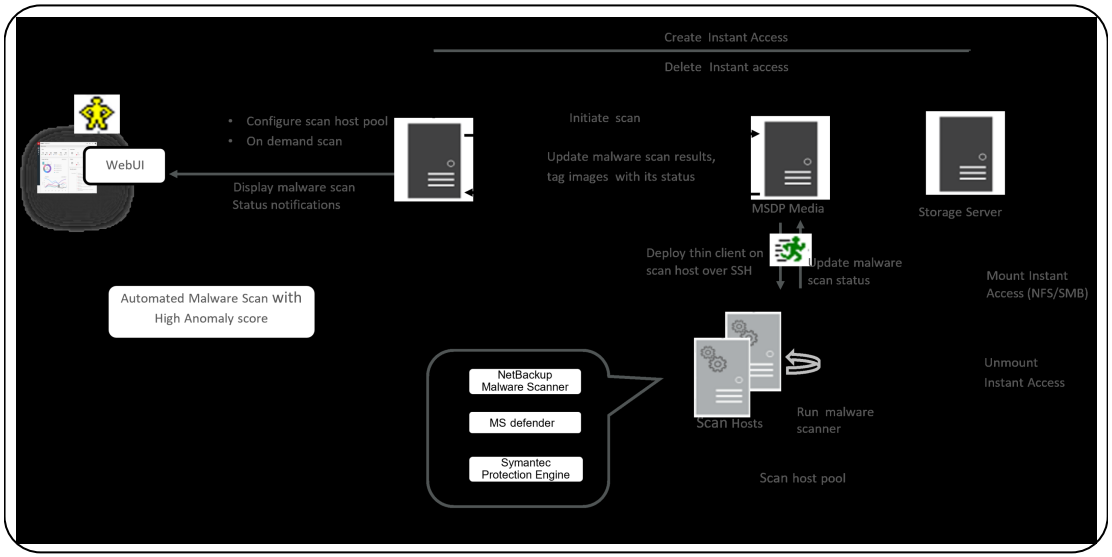
マルウェア検出には次の利点があります。

- オンデマンドスキャンでサポートされているポリシー形式のバックアップイメージを 1 つ以上選択できます。スキャンホストの事前定義済みリストを使用できます。
- スキャン中にマルウェアが検出されると、Web UI で通知が生成されます。

メモ: リカバリ中に、マルウェアの影響を受けたバックアップイメージからのリカバリを開始すると、警告メッセージが表示され、リカバリを続行するための確認が必要になります。マルウェアの影響を受けたイメージからリストアする権限を持つユーザーのみがリカバリを続行できます。

次の手順は、マルウェアのワークフローを示しています。

図 **26-1** マルウェア検出ワークフロー



1. プライマリサーバーは、指定したスキャンホストプールから利用可能なスキャンホストを識別します。スキャンホストでは、指定した時点で最大 3 件のスキャンを開始できます。

   メモ: 検証で失敗したバックアップイメージは無視されます。

2. オンデマンドスキャンのためにバックアップイメージがキューに登録されると、プライマリサーバーがストレージサーバーを識別します。スキャンホストプールで指定された構成済み共有形式のストレージサーバーに、インスタントアクセスマウントが作成されます。
3. プライマリサーバーは、利用可能な MSDP メディアサーバーを識別し、マルウェアスキャンを開始するようメディアサーバーに指示します。
4. MSDP メディアサーバーは、SSH を介してスキャンホストにシンクライアントを配備します。
5. シンクライアントは、スキャンホストにインスタントアクセスマウントをマウントします。
6. スキャンホストプールに構成されているマルウェアツールを使用してスキャンが開始されます。
7. スキャンが完了すると、スキャンホストはスキャンホストからインスタントアクセスマウントをマウント解除します。
8. SSH を介してメディアサーバーに通知されるマルウェアスキャンの状態が更新されます。スキャンログは、メディアサーバーのログディレクトリにコピーされます。
9. メディアサーバーは、プライマリサーバーに通知されるスキャン状態と感染ファイルリスト (感染ファイルが存在する場合) を更新します。
10. プライマリサーバーは、スキャン結果を更新し、インスタントアクセスを削除します。
11. マルウェアスキャン状態の通知が生成されます。

マルウェア検出では、30 日以上経過したスキャンジョブの自動クリーンアップが実行されます。

メモ: Microsoft Azure Marketplace と AWS Marketplace からマルウェアスキャナをダウンロードできます。AWS 向けと Azure 向けのマルウェアスキャナをインストール、構成、使用する方法に関する指示に従ってください。

AWS について詳しくは、以下を参照してください。

AWS Marketplace

AWS でのクラウド NetBackup マーケットプレイス配備

Microsoft Azure について詳しくは、以下を参照してください。

Azure Marketplace:

Azure クラウドでの NetBackup マーケットプレイス配備

新しいスキャンホストプールの構成

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで右上隅の[スキャナホストプールの構成 (Configure a scanner host pool)]または[マルウェア設定 (Malware settings)]をクリックし、ホストプールリストのページに移動します。

   構成について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。
3. [マルウェアスキャナホストプール (Malware scanner host pools)]ページで[追加 (Add)]をクリックし、新しいホストプールを追加します。
4. [マルウェアスキャナホストプールの追加 (Add malware scanner host pools)]ページで、[ホストプール名 (Host pool name)]、[マルウェアスキャナ (Malware scanner)]、[共有の種類 (Type of share)]などの詳細情報を入力します。
5. [ホストを保存して追加 (Save and add hosts)]をクリックします。

既存のスキャンホストの追加

この手順を使用して、同じ共有タイプの別のスキャンホストプールに同じスキャンホストを追加します。

既存のスキャンホストを構成するには

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページをクリックし、右上隅の[マルウェア設定 (Malware settings)]をクリックします。

3 [マルウェアスキャナホストプール (Malware scanner host pools)]ページで、目的のスキャンホストプールを選択し、処理メニューの[ホストの管理 (Manage hosts)]をクリックします。

4 [マルウェアスキャナホストの管理 (Manage malware scanner hosts)]ページで、[既存を追加 (Add existing)]をクリックして以前からあるホストを選択します。

メモ: リストには、すべてのスキャンホストプールのすべてのスキャンホストが含まれます。

5 [既存のマルウェアスキャナホストの追加 (Add existing malware scanner host)]ウィンドウで、目的のスキャンホストを 1 つ以上選択します。

6 [追加 (Add)]をクリックします。

クレデンシャルの管理

新しいクレデンシャルを追加

1 [クレデンシャルの管理 (Manage credentials)]ページで、[新しいクレデンシャルを追加 (Add new credentials)]を選択し、[次へ (Next)]をクリックします。

2 [クレデンシャルの管理 (Manage credentials)]ページで、クレデンシャル名、タグ、説明などの詳細情報を追加します。

3 [ホストクレデンシャル (Host credentials)]タブで、ホストのユーザー名、ホストパスワード、SSH ポート、RSA キー、共有タイプを追加します。

- MDSP メディアサーバーとホスト間の SSH 接続が動作していることを確認します。`ssh username@remote_host_name` を確実に実行するには
- - `ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa` コマンドを実行して、リモートスキャンホストの RSA キーが一覧表示されていることを確認します。
  - リモートスキャンホストの RSA キーを取得するには、Linux MSDP メディアサーバーで `ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa | awk '{print $3}' | base64 -d | sha256sum` を使用します。
    たとえば、出力は 33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef - のようになります。RSA キーは 33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef です。

メモ: コピーする際は、文字 - を RSA キーから削除してください。

4 共有の種類が SMB の場合は、次のような追加の詳細を入力します。

- Active Directory ドメイン
  これは、スキャンホストでのマウントの認証のためにストレージサーバーが参加したドメインです。
- Active Directory グループ
  これは Active Directory ドメインで利用可能なグループ名です。
- Active Directory ユーザー
  これは、選択した Active Directory グループに追加された Active Directory ユーザーです。
- パスワード

5 [保存 (Save)]をクリックします。

既存のクレデンシャルの選択

1 [クレデンシャルの管理 (Manage credentials)]ページで、[既存のクレデンシャルの選択 (Select existing credentials)]を選択し、[次へ (Next)]をクリックします。

2 [クレデンシャルの選択 (Select credentials)]タブで、目的のクレデンシャルを選択し、[保存 (Save)]をクリックします。

スキャンホストの削除

1 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。

2 [マルウェアの検出 (Malware detection)]ページをクリックし、右上隅の[マルウェアの検出設定 (Malware detection settings)]をクリックします。

3 [マルウェアスキャナホストプール (Malware scanner host pools)]ページで、目的のスキャンホストプールを選択し、処理メニューの[ホストの管理 (Manage hosts)]をクリックします。

4 目的のホストを選択し、[削除 (Remove)]をクリックします。

スキャンホストの無効化

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページをクリックし、右上隅の[マルウェアの検出設定 (Malware detection settings)]をクリックします。
3. [マルウェアスキャナホストプール (Malware scanner host pools)]ページで、目的のスキャンホストプールを選択し、処理メニューの[ホストの管理 (Manage hosts)]をクリックします。
4. 目的のホストを選択し、[無効化 (Deactivate)]をクリックします。

ポリシークライアントバックアップイメージのマルウェアスキャン

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]をクリックします。
3. [検索基準 (Search by)]オプションから、[バックアップイメージ (Backup images)]を選択します。
4. 検索条件で、以下を確認して編集します。
   - ポリシー名

     メモ: サポート対象のポリシー形式のみが一覧表示されます。

   - クライアント名

     メモ: サポート対象のポリシー形式のバックアップイメージを含むクライアントが表示されます。

   - ポリシー形式
   - バックアップ形式

     メモ: アクセラレータ機能が有効になっていない増分バックアップイメージは、VMware 作業負荷ではサポートされません。

- コピー

  メモ: 選択したコピーがインスタントアクセス可能なコピーでない場合、バックアップイメージのマルウェアスキャンはスキップされます。

- ディスクプール

  メモ: MSDP (PureDisk) ストレージ形式のディスクプールのみが表示されます。

- マルウェアスキャンの状態。
- ［バックアップの期間の選択 (Select the timeframe of backups)］で、日時の範囲を確認するか、更新します。

5 ［検索 (Search)］をクリックします。

メモ: これに基づいて検索条件を選択し、選択したスキャンホストプールにアクティブで利用可能なスキャンホストが存在することを確認します。

6 ［スキャンするバックアップの選択 (Select the backups to scan)］テーブルで、スキャンする 1 つ以上のイメージを選択します。

7 ［マルウェアスキャナホストプールの選択 (Select a malware scanner host pool)］で、適切なホストプール名を選択します。

メモ: 選択したスキャンホストプールのスキャンホストは、NFS/SMB 形式の共有が構成されている MSDP ストレージサーバーで作成されたインスタントアクセスマウントにアクセスできる必要があります。

8 ［マルウェアのスキャン (Scan for malware)］をクリックします。

メモ: マルウェアスキャナホストは、一度に 3 つのイメージのスキャンを開始できます。

9 このスキャン状態はバックアップイメージレベルであり、バックアップイメージのすべてのコピーに適用可能です。スキャンが開始されると、［マルウェアの検出 (Malware Detection)］にマルウェアスキャンの進行状況が表示され、次のフィールドが表示されます。

- 未スキャン (Not scanned)

- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

メモ: 失敗の状態を示すツールのヒントにカーソルを合わせると、スキャンが失敗した理由が表示されます。

メモ: 検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートするのは、サポート対象のポリシー形式で、インスタントアクセス機能を備えた、MSDP ストレージに格納されたバックアップイメージのみです。

- 処理中 (In progress)
- 保留中 (Pending)

メモ: 1 つ以上の処理中および保留中のジョブのマルウェアスキャンをキャンセルできます。

マルウェアスキャンの実行

マルウェアのスキャンを開始して、マルウェアを検出できます。

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]をクリックします。
3. [検索条件 (Search by)]オプションから、次のいずれかを選択します。
   - バックアップイメージ (Backup images)
     p.215 の「ポリシークライアントバックアップイメージのマルウェアスキャン」を参照してください。
   - ポリシー形式別の資産 (Assets by policy type)

     メモ: NetBackup は、マルウェアスキャンで MS-Windows ポリシー形式と標準ポリシー形式をサポートします。
   - 保護計画別の資産 (Assets by protection plans)

メモ: NetBackup はマルウェアスキャンで VMware 資産をサポートします。

4 [クライアント (Client)]または[資産 (Asset)]テーブルで、スキャンするクライアントまたは資産を選択します。

5 [次へ (Next)]をクリックします。

6 [開始日付 / 時刻 (Start date/time)]と[終了日付 / 時刻 (End date/time)]で、日時の範囲を確認または更新します。

メモ: 選択条件に従って、スキャンが最大 100 イメージまで開始されます。

7 [スキャナホストプール (Scanner host pool)]で、適切なホストプール名を選択します。

8 [マルウェアスキャンの現在の状態 (Current status of malware scan)]から、次のいずれかを選択します。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- すべて (All)

9 [マルウェアのスキャン (Scan for malware)]をクリックします。

警告: 検索には 100 個以上のイメージがあります。100 個を超えるイメージはスキャンできません。日付範囲を調整して再試行してください。

メモ: マルウェアスキャナホストは、一度に 3 つのイメージのスキャンを開始できます。

10 スキャンが開始されると、マルウェア検出のマルウェアスキャンの進行状況が表示され、次のフィールドが表示されます。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

メモ: 失敗の状態を示すツールのヒントにカーソルを合わせると、スキャンが失敗した理由が表示されます。

メモ: 検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートするのは、サポート対象のポリシー形式で、インスタントアクセス機能を備えた、MSDP ストレージに格納されたバックアップイメージのみです。

VMware 資産のマルウェアのスキャン

マルウェアをスキャンする前に、次の要件があります。

- プライマリサーバーが NetBackup 10.0.1 以降である。
- バックアップが NetBackup 10.1 以降のストレージサーバーで実行された。
- バックアップイメージが、サポート対象のポリシー形式に限り、インスタントアクセス機能を備えた MSDP ストレージに格納されている。
- スキャンホストプールがスキャンホストで構成されている。
- 前回のバックアップが正常に実行されている。
- マルウェアスキャンを実行する権限がある RBAC の役割を持っている。

VMware 資産のマルウェアをスキャンするには

1. 左側で[VMware]、[仮想マシン (Virtual machine)]の順にクリックします。
2. VM を特定してクリックします。
3. [処理 (Actions)]、[マルウェアのスキャン (Scan for malware)]を選択します。
4. [マルウェアスキャン (Malware scan)]ページで、次の操作を行います。
   - [開始日時 (Start date/time)]と[終了日時 (End date/time)]を選択して、スキャンの日付範囲を選択します。
   - [スキャナホストプール (Scanner host pool)]を選択します
   - [マルウェアスキャンの現在の状態を選択 (Select current status of malware scan)]リストから、次のいずれかを選択します。
     - 未スキャン (Not scanned)
     - 感染なし (Not infected)
     - 感染 (Infected)
     - すべて (All)

5 ［マルウェアのスキャン (Scan for malware)］をクリックします。

メモ: マルウェアスキャナホストは、一度に 3 つのイメージのスキャンを開始できます。

6 スキャンが開始されると、［マルウェアの検出 (Malware Detection)］にマルウェアスキャンの進行状況が表示され、次のフィールドが表示されます。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

メモ: 検証で失敗したバックアップイメージは無視されます。

- 処理中 (In progress)
- 保留中 (Pending)

マルウェアスキャンの状態の表示

マルウェアスキャンの状態を表示するには

◆ 左側で［検出とレポート (Detection and reporting)］、［マルウェアの検出 (Malware detection)］の順にクリックします。

次の列が表示されます。

- クライアント (Client): マルウェアが検出された NetBackup クライアントの名前。
- バックアップ時間 (Backup time): バックアップが実行された時間。
- マルウェアスキャンの状態 (Malware scan status): バックアップイメージのスキャン状態。状態には、感染、感染なし、失敗、処理中、保留中、キャンセル済み、キャンセルが進行中があります。
- スケジュール形式 (Schedule type): 関連付けられたバックアップジョブのバックアップ形式
- スキャン日 (Date of the scan): スキャンが実行された日付。
- マルウェアスキャナ (Malware scanner): スキャンに使用されたマルウェアスキャナの名前。

- スキャナホストプール (Scanner host pool): マルウェアスキャンに使用されるホストプールを示します。一括再スキャン中にスキャナホストプールが異なるか空白の場合は、新しいスキャナホストプールを選択する必要があります。
- 感染ファイル (Files infected): スキャン時に感染が確認されたファイルの数を示します。

マルウェアスキャンイメージの処理

バックアップイメージをスキャンしてマルウェア検出を行うと、[マルウェアの検出 (Malware detection)]ホームページにテーブル形式のデータが表示されます。p.220 の「マルウェアスキャンの状態の表示」を参照してください。

バックアップイメージごとに、次の簡易な構成を利用できます。

すべてのコピーを期限切れにする

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します
2. 目的のスキャン結果を表示するには、右側から[すべてのコピーを期限切れにする (Expire all copies)]を選択します。
3. 選択したバックアップイメージのすべてのコピーを期限切れにすることを確認します。

感染ファイルを表示する

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します
2. 目的のスキャン結果を表示するには、[感染ファイルを表示 (View infected files)]を選択します。

   メモ: このオプションは、感染したファイルにのみ利用できます。

3. [感染ファイル (Infected files)]テーブルで、必要に応じて目的のファイルを検索します。
4. 必要に応じて、[リストのエクスポート (Export list)]をクリックします。

   メモ: 選択したマルウェアスキャン結果の感染ファイルのリストは、`.csv` 形式でエクスポートされます。ファイル名の形式は、*`backupid`*`_infected_files_`*`timestamp`*`.csv` となります。

感染ファイルのリストをエクスポートする

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します
2. 影響を受けたマルウェアに対して、右側から[感染ファイルのリストをエクスポート (Export Infected files list)]を選択します。

メモ: .csv ファイルには、感染したファイルのバックアップ時刻と名前が含まれています。

マルウェアスキャンをキャンセルする

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します
2. 目的のクライアントの[処理 (Actions)]メニューで、[マルウェアスキャンをキャンセル]をクリックします。

メモ: マルウェアスキャンは進行中および保留中の状態からのみキャンセルできます。

3. [スキャンをキャンセル (Cancel scan)]をクリックして確定します。

メモ: 状態は[キャンセルが進行中]に変わります。

イメージの再スキャン

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します
2. 目的のクライアントの[処理 (Actions)]メニューで、[イメージの再スキャン (Rescan image)]をクリックします。
3. [再スキャン (Rescan)]をクリックして確定します。
4. 一括再スキャンで、異なるまたは空のスキャナホストプールを持つ 1 つ以上のイメージを選択する場合
   - [イメージの再スキャン (Rescan image)]をクリックします。
   - [マルウェアスキャナホストプールの選択 (Select a malware scanner host pool)]ポップアップから、新しいスキャンホストを選択します。

メモ: 新しいスキャンホストプールは、この再スキャンで選択したすべてのイメージに使用できます。

- ［再スキャン (Rescan)］をクリックして確定します。

マルウェアに感染したイメージ (ポリシーによって保護されているクライアント) からのリカバリ

デフォルトでは、リカバリ中に NetBackup はスキャンされてマルウェアのないバックアップイメージのみを表示します。

マルウェアに感染したイメージからリストアするには、管理者の役割または同等の RBAC 権限が必要です。マルウェアに感染した VMware 資産をリカバリするには、次のトピックを参照してください。

p.224 の「マルウェアに感染した VMware 資産のリカバリ」を参照してください。

マルウェアに感染したイメージ (ポリシーによって保護されているクライアント) からリカバリするには

1. 左側の［リカバリ (Recovery)］をクリックします。
2. ［標準リカバリ (Regular recovery)］で［リカバリの開始 (Start recovery)］をクリックします。
3. 次のプロパティを選択します。

ソースクライアント	バックアップを実行したクライアント。
宛先クライアント	バックアップをリストアするクライアント。
ポリシー形式	リストアするバックアップに関連付けられているポリシーの形式。
リストア形式	実行するリストア形式。利用可能なリストア形式は選択したポリシー形式によって異なります。

4. ［次へ (Next)］をクリックします。

5 [開始日時 (Start date)]と[終了日時 (End date)]を選択します。

または、[バックアップ履歴 (Backup history)]をクリックして、特定のイメージを表示して選択します。[選択 (Select)]をクリックして、選択したイメージをリカバリに追加します。

メモ: 選択した時間枠のすべてのバックアップイメージの詳細がテーブルに表示されます。イメージをフィルタ処理したり、ソートしたりできます。たとえば、マルウェアスキャンの結果、スケジュール形式、ポリシー名に基づいてフィルタ処理したり、ソートしたりできます。

---

6 マルウェアに感染したイメージをリカバリに含める場合は、[マルウェアに感染したイメージの選択を許可 (Allow the selection of images that are malware-affected)]を選択します。

7 左側で[ソースクライアント (Source client)]ディレクトリを展開します。リストアするディレクトリを選択します。または、右ペインでファイルまたはディレクトリを選択します。[次へ (Next)]をクリックします。

8 リカバリターゲットを選択します。

9 マルウェアに感染したファイルをリストアするには、[マルウェアに感染したファイルのリカバリを許可 (Allow recovery of files infected with malware)]をクリックします。クリックしない場合、NetBackup はスキャンされてマルウェアのないファイルのみをリストアします。

10 その他のリカバリオプションを選択します。続いて[次へ (Next)]をクリックします。

11 リカバリ設定を確認し、[リカバリの開始 (Start recovery)]をクリックします。

マルウェアに感染した VMware 資産のリカバリ

デフォルトでは、リカバリ中に NetBackup はスキャンされてマルウェアのないリカバリポイントのみを表示します。

マルウェアに感染したリカバリポイントからリストアするには、管理者の役割または同等の RBAC 権限が必要です。マルウェアに感染した VMware 資産をリカバリするには、次のトピックを参照してください。

p.223 の「マルウェアに感染したイメージ (ポリシーによって保護されているクライアント) からのリカバリ 」を参照してください。

マルウェアに感染した VMware 資産をリカバリするには

1 左側で[VMware]、[仮想マシン (Virtual machine)]の順にクリックします。

2 VM を見つけます。次に[操作 (Actions)]、[リカバリ (Recover)]の順にクリックします。

3 [リカバリポイント (Recovery Points)]タブでは、各リカバリポイントのマルウェアスキャンの状態が次のように表示されます。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

4 リカバリポイントを選択します。

5 [マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery of points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージを含むリカバリポイントがある場合にのみ表示されます。

メモ: マルウェアに感染したリカバリポイントからリストアするには、管理者の役割または同等の RBAC 権限が必要です。

---

6 [リカバリ (Recover)]をクリックし、リカバリの種類を選択します。次に、プロンプトに従います。

VM のリカバリについて詳しくは、『NetBackup Web UI VMware 管理者ガイド』を参照してください。

トラブルシューティング

表 26-1

エラー	説明
選択した時間範囲の感染ファイルが多すぎる。	選択した日付範囲のバックアップイメージの感染ファイルリストを表示するには、`nbmalwarescanner` を確認します。感染ファイルの数を減らすために、日付範囲またはリカバリファイルとフォルダの選択を更新します。操作を再試行します。また、次のいずれかを実行することもできます。 ■ クリーンファイルを選択的にリカバリするために使用できる[マルウェアに感染したファイルのリカバリを許可 (Allow recovery of files infected by malware)]オプションを選択します。 ■ リカバリでそのバックアップイメージをスキップします。

27

異常の検出

この章では以下の項目について説明しています。

バックアップの異常検出について

NetBackup は、バックアップメタデータの異常を検出できるようになりました。データバックアップフローの異常なジョブデータを検出できます。たとえば、ファイル数やファイルサイズが通常の数やサイズと異なる場合に検出できます。

メモ: デフォルトでは、異常検出アルゴリズムは NetBackup マスターサーバーで実行されます。異常検出プロセスによってマスターサーバーに影響がある場合は、異常を検出するようにメディアサーバーを構成できます。

次のバックアップジョブのメタデータ、属性、機能が、バックアップの異常検出中に検証されます。

- バックアップイメージのサイズ
- バックアップファイルの数
- KB 単位で転送されるデータ
- 重複排除率
- バックアップジョブの完了時間

これらのバックアップジョブ属性が通常の範囲から異常に逸脱している場合は異常と見なされ、NetBackup Web UI を使用して通知されます。

バックアップの異常検出と通知のワークフロー

バックアップの異常検出と通知のワークフローは、次のとおりです。

表 27-1 ワークフロー

手順	説明
手順 1	マスターサーバーとメディアサーバーに NetBackup ソフトウェアをインストールするか、アップグレードします。 『NetBackup インストール/アップグレードガイド』を参照してください。
手順 2	マスターサーバーでバックアップの異常検出を有効にします。 デフォルトでは、異常検出アルゴリズムは NetBackup マスターサーバーで実行されます。異常検出プロセスによってマスターサーバーに影響がある場合は、異常を検出するようにメディアサーバーを構成できます。 『NetBackup セキュリティおよび暗号化ガイド』を参照してください。
手順 3	NetBackup Web UI を使用して異常検出の設定を行います。 p.229 の「異常検出設定を行う」を参照してください。
手順 4	NetBackup Web UI を使用して異常を表示します。 p.228 の「異常の表示」を参照してください。

バックアップの異常の検出方法

たとえば、次の例を考えてみます。

ある組織では、スケジュール形式が[完全 (Full)]の特定のクライアントおよびバックアップポリシーにより、毎日約 1 GB のデータがバックアップされます。特定の日に、10 GB のデータがバックアップされました。この事例はイメージサイズの異常としてキャプチャされ、通知されました。この異常は、現在のイメージサイズ (10 GB) が通常のイメージサイズ (1 GB) をはるかに超えているために検出されます。

メタデータの大幅な逸脱は、その異常スコアに基づいて異常とされます。

異常スコアは、現在のデータが過去の類似データの観測群からどれだけ離れているかに基づいて計算されます。この例では、基準となるクラスタは 1 GB のデータバックアップです。異常の重大度は、そのスコアに基づいて判断できます。

例:

Anomaly_A の異常スコア = 7

Anomaly_B の異常スコア = 2

結論 - Anomaly_A は Anomaly_B よりも重大

NetBackup は異常検出時に、異常検出の構成の設定 (デフォルト、存在する場合は詳細設定) を考慮します。

『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

異常の表示

NetBackup は、バックアップメタデータの異常を検出できるようになりました。データバックアップフローの異常なジョブデータを検出できます。たとえば、ファイル数やファイルサイズが通常の数やサイズと異なる場合に検出できます。

p.226 の「バックアップの異常検出について」を参照してください。

メモ: 異常数が 0 の場合は、異常が発生しなかったか、異常検出サービスが実行されていない可能性があります。

異常を表示するには

1 左側で[検出とレポート (Detection and reporting)]、[異常検出 (Anomaly detection)]の順に選択します。

次の列が表示されます。

- ジョブ ID (Job ID) - 異常が検出されたジョブのジョブ ID
- クライアント名 (Client name) - 異常が検出された NetBackup クライアントの名前
- ポリシー形式 (Policy type) - 関連付けられたバックアップジョブのポリシー形式
- 数 (Count) - このジョブで検出された異常の数
- スコア (Score) - 異常の重大度。異常の重大度が大きいほどこのスコアが高くなります。
- 異常の重大度 (Anomaly severity) - このジョブについて通知された異常の重大度
- 異常の概略 (Anomaly summary) - このジョブについて通知された異常の概略
- 受信日 (Received) - 異常が通知された日付
- レビュー状態 (Review status) - 検出された異常が誤検知として報告されたか、実際の異常として報告されたか、無視できるかを示します。
- ポリシー名 (Policy name) - 関連付けられたバックアップジョブのポリシー名

- スケジュール名 (Schedule name) - 関連付けられたバックアップジョブのスケジュール名
- スケジュール形式 (Schedule type) - 関連付けられたバックアップジョブのスケジュール形式

2 行を展開すると、選択した異常の詳細が表示されます。

各異常レコードについて、その機能の現在値と、過去のデータに基づく実際の範囲が表示されます。

たとえば、次の例を考えてみます。

異常があるイメージサイズの特徴として 100 MB (通常は 350 MB、450 MB) と表示されます。この情報は、異常として報告された現在のイメージサイズが 100 MB であることを意味しています。しかし、通常のイメージサイズの範囲は、過去のデータの分析から導き出された 350 ～ 450 MB です。現在のイメージサイズと通常のイメージサイズの範囲が大幅に異なるため、NetBackup は異常として通知します。

3 異常レコードに対して次の処理を実行できます。

- 異常条件を無視できる場合は、[無視としてマーク (Mark as ignore)]をクリックします。
  異常レコードの[レビュー状態 (Review status)]は `Ignore` と表示されます。
- 異常条件に何らかの処理を実行する場合は、[異常として確認 (Confirm as anomaly)]をクリックします。
  異常レコードの[レビュー状態 (Review status)]は `Anomaly` と表示されます。
- 異常が誤検知の場合は、[誤検知として報告 (Report as false positive)]をクリックします。以後、同様の異常は表示されません。
  異常レコードの[レビュー状態 (Review status)]は `False positive` と表示されます。

異常検出設定を行う

異常検出設定を有効にすると、異常データ収集、検出サービス、イベントが有効になります。基本レベルと詳細レベルの異常検出設定を利用できます。

p.226 の「バックアップの異常検出について」を参照してください。

異常検出設定を行うには

1 左側で[検出とレポート (Detection and reporting)]、[異常検出 (Anomaly detection)]の順に選択します。

2 右上で、[異常設定 (Anomalies settings)]をクリックします。

3 右側で[編集 (Edit)]をクリックし、次のオプションのいずれかを選択して異常検出設定を行います。

- すべて無効にする (Disable all)
- 異常データの収集を有効にする (Enable anomaly data gathering)
- 異常データの収集と検出サービスを有効にする (Enable anomaly data gathering and detection service)
- 異常データの収集、検出サービス、イベントを有効にする (Enable anomaly data gathering and detection service and events)

4 [保存 (Save)]をクリックします。

5 [編集 (Edit)]をクリックして、次の基本設定を変更します。

- 異常検出の感度 (Anomaly detection sensitivity)
- データ保持の設定 (Data retention settings)
- データ収集の設定 (Data gathering settings)
- 異常プロキシサーバーの設定 (Anomaly proxy server settings)

6 [保存 (Save)]をクリックします。

7 [詳細設定 (Advanced Settings)]を選択します。

8 [クライアントの異常設定を無効にする (Disable anomaly settings for clients)]を編集します。

9 [保存 (Save)]をクリックします。

10 [機械学習でポリシー形式または特定の機能を無効にする (Disable policy type or specific features for machine learning)]を編集します。

11 [保存 (Save)]をクリックします。

28

使用状況レポートと容量ライセンス

この章では以下の項目について説明しています。

プライマリサーバー上の保護データのサイズの追跡

使用状況レポートアプリケーションには、容量ライセンス用に構成されたプライマリサーバーとそれぞれの消費の詳細が表示されます。このレポートには、次の利点があります。

- 容量ライセンスを計画する機能がある。
- NetBackup が週単位で使用状況と傾向の情報を収集してレポートできる。`nbdeployutil` ユーティリティによって、レポート用のデータの収集の実行をスケジュール化できる (デフォルトで有効)。
- Veritas NetInsights コンソールへのリンク。NetInsights コンソールツールにある Usage Insights ツールを使用すると、NetBackup カスタマは、消費パターンをほぼリアルタイムで視覚的に把握して、ライセンスの使用状況を積極的に管理できます。
- レポートは、データ保護に使用されるすべてのポリシー形式に対して実行されます。

要件

NetBackup は、次の要件が満たされていれば、使用状況レポートのデータを自動的に収集します。

- プライマリサーバーが NetBackup 8.1.2 以降である。
- 容量ライセンスを使用している。
- スケジュールされた自動レポートを使用している。容量ライセンスレポートを手動で生成する場合、NetBackup Web UI の使用状況レポートにデータは表示されません。
- 次のファイルが存在する。
  UNIX の場合: `/usr/openv/var/global/incremental/Capacity_Trend.out`
  Windows の場合:
  `install_path``¥var¥global¥incremental¥Capacity_Trend.out`
  バックアップデータが利用できない場合、[使用状況 (Usage)]タブにエラーが表示されます。また、使用状況レポートが生成されていない (ファイルが存在しない) 場合にもエラーが表示されます。
- プライマリサーバーのいずれかで、他のリモートプライマリサーバーの使用状況レポートのデータを収集する場合は、追加の構成が必要です。プライマリサーバー間に信頼関係を作成する必要があります。ローカルプライマリサーバー (`nbdeployutil` の実行を計画している場所)を、各リモートプライマリサーバー上の[サーバー (Servers)]リストに追加することも必要です。
  p.232 の「ローカルプライマリサーバーの追加」を参照してください。
  p.156 の「信頼できるプライマリサーバーの追加」を参照してください。

追加情報

- 容量ライセンス、スケジュール設定、および容量ライセンスレポートのオプションの詳細を参照できます。
  p.233 の「容量ライセンスのレポートのスケジュール設定」を参照してください。
- 『Veritas Usage Insights for NetBackup スタートガイド』。Usage Insights を使用して NetBackup の配備とライセンスを管理する方法についての詳細を説明します。このツールでは、正確なほぼリアルタイムのレポートで、バックアップされるデータの合計量を確認できます。

ローカルプライマリサーバーの追加

プライマリサーバーの使用状況レポート情報を追加しようとしても、そのサーバーがインターネットに接続されていない場合は、リモートプライマリサーバーのサーバーリストに、ローカルプライマリサーバーの名前を追加する必要があります。ローカルプライマリサーバーは、使用状況レポートツールの実行を計画している場所です。

ローカルプライマリサーバーを追加するには

1 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host Properties)]の順にクリックします。

2 ホストを選択し、[接続 (Connect)]をクリックします。

3 [プライマリサーバーの編集 (Edit primary server)]をクリックします。

4 [サーバー (Servers)]をクリックします。

5 [追加サーバー (Additional Servers)]タブで[追加 (Add)]をクリックします。

6 nbdeployutil の実行を計画しているプライマリサーバーの名前を入力します。

7 [追加 (Add)]をクリックします。

使用状況レポートに表示するライセンスタイプの選択

netbackup_deployment_insights ユーティリティを使用して使用状況レポートを生成するライセンス形式を選択できます。

一部のライセンスタイプは、プライマリサーバー上の他のタイプと一緒には構成できません。たとえば、容量ライセンスのタイプを選択した場合、従来のライセンスは選択できません。詳しくは、『NetBackup ライセンスガイド』を参照してください。

使用状況レポートに表示するライセンスタイプを選択するには

1 左側で[検出とレポート (Detection and reporting)]、[使用方法 (Usage)]の順にクリックします。

2 右上の[使用状況レポートの設定 (Usage reporting settings)]をクリックします。

プライマリサーバーのライセンス設定 (ライセンスタイプとライセンスモデルを含む) が表示されます。

3 [編集 (Edit)]をクリックします。

4 使用するライセンスタイプを選択します。次に、[保存 (Save)]をクリックします。

容量ライセンスのレポートのスケジュール設定

デフォルトでは、NetBackup は、nbdeployutil を指定のスケジュールで実行するようにトリガして、増分的にデータを収集し、ライセンスレポートを生成します。最初の実行については、構成ファイルで指定した間隔がレポートの期間として使用されます。

容量ライセンスのレポート期間は、収集データの可用性に応じて、常に過去 90 日分です。90 日分より前のデータはレポートで考慮されません。nbdeployutil が実行されるたびに、nbdeployutil の最新の実行と前回の正常な実行の間の情報が収集されます。

ライセンスレポートの場所

現在の容量ライセンスレポートは、次のディレクトリに存在します。

Windows の場合: *install_path*¥NetBackup¥var¥global¥incremental

UNIX の場合: /usr/openv/var/global/incremental

以下のファイルが含まれます。

- nbdeployutil の最新の結果について生成されたレポート。
- 増分的に収集されたデータを含むフォルダ。
- 古い生成済みのレポートを含むアーカイブフォルダ。
- nbdeployutil ログファイル。

古いレポートはアーカイブフォルダに格納されます。Veritas 90 日以上のレポートデータを保持することをお勧めします。環境の要件に応じて、データは 90 日間より長く保持できます。古いレポートは、時間の経過とともに容量の使用状況がどのように変化したのかを示すのに役立つことがあります。レポートまたはフォルダは、不要になったときに削除します。

ユースケース I: ライセンスレポートのデフォルト値の使用

デフォルトパラメータを使用する場合、nbdeployutilconfig.txt ファイルは不要です。容量ライセンスについて、nbdeployutil は次のデフォルト値を使用します。

- FREQUENCY_IN_DAYS=7
- MASTER_SERVERS=*local_server*
- PARENTDIR=*folder_name*
  Windows の場合: *install_path*¥NetBackup¥var¥global¥incremental
  UNIX の場合: /usr/openv/var/global/incremental
- PURGE_INTERVAL = 120 (日数)
- MACHINE_TYPE_REQUERY_INTERVAL = 90 (日数)

ユースケース II: ライセンスレポートのカスタム値の使用

nbdeployutilconfig.txt ファイルが存在しない場合は、次の形式を使用してファイルを作成します。

```
[NBDEPLOYUTIL_INCREMENTAL]
MASTER_SERVERS=<server_names>
FREQUENCY_IN_DAYS=7
PARENTDIR=<folder_name_with_path>
PURGE_INTERVAL=120
MACHINE_TYPE_REQUERY_INTERVAL=90
```

ライセンスレポートにカスタム値を使うには

1 nbdeployutilconfig.txt ファイルを次の場所にコピーします。

Windows の場合: *install_path*¥NetBackup¥var¥global

UNIX の場合: /usr/openv/var/global

2 nbdeployutilconfig.txt ファイルを開きます。

3 レポートを作成する頻度に合わせて FREQUENCY_IN_DAYS の値を編集します。

デフォルト (推奨)	7
最小値	1
値が 0	増分レポートが無効になり、ライセンス情報は取得されなくなります。
パラメータの削除	nbdeployutil はデフォルト値を使います。

4 MASTER_SERVERS の値を編集して、レポートに含めるプライマリサーバーのカンマ区切りのリストを含めるようにします。

メモ: Veritas Usage Insight では、プライマリサーバーが NetBackup 8.1.2 以降に配備されている必要があります。

値なし	nbdeployutil はデフォルト値を使います。
パラメータの削除	nbdeployutil はデフォルト値を使います。

次に例を示します。

- MASTER_SERVERS=newserver,oldserver
- MASTER_SERVERS=newserver,oldserver.domain.com
- MASTER_SERVERS=myserver1.somedomain.com,newserver.domain.com

5 PARENTDIR の値を編集して、データを収集して報告する場所のフルパスを含めるようにします。

値なし	nbdeployutil はデフォルト値を使います。
パラメータの削除	nbdeployutil はデフォルト値を使います。

6 PURGE_INTERVAL の値を編集して、レポートデータを削除する頻度を示す間隔 (日数) を指定します。120 日より古いデータは自動的にパージされます。

デフォルト	120
最小値	90
値なし	nbdeployutil はデフォルト値を使います。
パラメータの削除	nbdeployutil はデフォルト値を使います。

7 MACHINE_TYPE_REQUERY_INTERVAL を編集して、このマシン形式の更新のために物理クライアントをスキャンする頻度を指定します。

デフォルト	90
最小値	1
値なし	nbdeployutil はデフォルト値を使います。
パラメータの削除	nbdeployutil はデフォルト値を使います。

増分レポートのその他の構成

収集データと容量ライセンスレポートのディレクトリを変更するには

1 古い収集データとライセンスレポートが存在する場合は、該当するディレクトリ全体を新しい場所にコピーします。

2 nbdeployutilconfig.txt を編集し、PARENTDIR=*folder_name* フィールドで収集データとライセンスレポートの場所を変更します。

以前に収集されたデータを使用して容量ライセンスレポートを生成するには

1. 直前の nbdeployutil の実行によって収集されたデータを保存するために生成されたフォルダを特定し、そのフォルダを次の場所にコピーします。

   Windows の場合: *install_path*¥NetBackup¥var¥global¥incremental

   UNIX の場合: /usr/openv/var/global/incremental

2. コピーしたフォルダ内に gather_end.json ファイルを作成し、次のテキストを追加します。

   ```
   {"success":0}
   ```

   次回の増分の実行では、コピーしたフォルダ内のデータを考慮して容量ライセンスレポートが生成されます。

メモ: データの収集期間のギャップを回避するため、コピーしたフォルダ内のその他すべての収集フォルダを削除します。不足しているデータについては、時間の増分の実行で自動的に生成されます。

既存の収集データを使ってカスタムの間隔の容量ライセンスレポートを作成するには

- 90 日のデフォルトの間隔以外でレポートを作成するには、次のコマンドを入力します。

  Windows の場合:

  ```
  nbdeployutil.exe --capacity --incremental --report --inc-settings

  "install_dir¥netbackup¥var¥global¥nbdeployutilconfig.txt"
  --hoursago <custom-time-interval>
  ```

  UNIX の場合:

  ```
  nbdeployutil.exe --capacity --incremental --report --inc-settings

  "/usr/openv/var/global/nbdeployutilconfig.txt"
  --hoursago <custom-time-interval>
  ```

  --hoursago で指定する時間数は、nbdeployutilconfig.txt ファイルで指定している purge-interval 未満である必要があります。

メモ: nbdeployutil は収集データを使ってカスタムの間隔のレポートを生成します。--gather オプションを使う必要はありません。

使用状況レポートと増分レポートのエラーのトラブルシューティング

- nbdeployutil の増分実行については、通知が NetBackup Web UI に送信されます。通知の詳細情報には、実行の状態、期間、開始時刻、終了時刻が含まれます。
- nbdeployutil がデータの収集と環境についてのレポートの生成に失敗することがあります。ログを参照して、タスクが失敗したタイミングとその理由を確認してください。
- ユーティリティを手動で実行した後、nbdeployutil が bpimagelist エラー (状態コード 37) で失敗することがあります。追加サーバーのリストにプライマリサーバーが追加されていることを確認してください。
  p.232 の「ローカルプライマリサーバーの追加」を参照してください。
- Web サービスの内部通信エラーにより次のエラーが表示されることがあります。
  プライマリサーバー *SERVER_NAME* で Web API の内部エラーが発生しました。
  プライマリサーバー *SERVER_NAME* で、gather オプションを使用して nbdeployutil を再度実行してください。
- VMware または NDMP では、バックアップエージェントがデータベースにライセンス情報をポストできなかった場合、アクティビティモニターに状態コード 5930 または 26 が表示されます。詳しくは、『NetBackup 状態コードリファレンスガイド』を参照してください。

同じトラブルシューティングのポイントで、netbackup_deployment_insights を使用できます。

7

NetBackup 作業負荷と NetBackup Flex Scale

29

NetBackup SaaS Protection

この章では以下の項目について説明しています。

NetBackup for SaaS の概要

NetBackup Web UI は NetBackup SaaS Protection の資産を表示する機能を備えています。SaaS アプリケーションのデータを保護するように構成された資産は、NetBackup Web UI で自動的に検出されます。

NetBackup SaaS Protection 資産は、ハブ、StorSite、Stor、サービスなどの資産で構成されます。

次の資産に関する詳細情報が表示されます。

- ストレージサイズ
- ストレージ層の詳細
- ストレージ内のアイテム数
- WORM の詳細
- 書き込み、削除、スタブポリシーの詳細

- 次回のバックアップのスケジュール
- 前回のバックアップの状態

NetBackup Web UI では、次の操作を実行できます。

- NetBackup SaaS Protection ハブを追加する。
- ハブ内の資産を表示する。
- NetBackup SaaS Protection Web UI を起動する。
- 追加したハブを削除する。

メモ: SaaS 資産を NetBackup SaaS Protection Web UI から削除しても、削除した資産が NetBackup データベースから直ちに削除されるわけではありません。削除した資産は、NetBackup データベースに 30 日間残ります。

次の表に、NetBackup for SaaS の機能を示します。

表 29-1 NetBackup for SaaS の機能

機能	説明
NetBackup RBAC (役割ベースのアクセス制御) との統合	NetBackup Web UI は RBAC の役割を提供します。これによりユーザーは、SaaS 作業負荷内の資産を表示できます。NetBackup SaaS Protection ハブを追加したり、ハブ内の資産を表示するために、ユーザーが NetBackup 管理者である必要はありません。
NetBackup SaaS Protection 固有のクレデンシャル	NetBackup SaaS Protection のサービスアカウントは、ハブの認証に使用されます。
資産の自動検出	NetBackup は、ハブ内の StorSite、Stor、サービスを自動的に検出します。手動で検出を実行することもできます。資産の検出後は、その資産の詳細を表示できます。
クロス起動	NetBackup SaaS Protection Web UI はクロス起動できます。 SSO が構成されている場合、ユーザーは NetBackup SaaS Protection UI にリダイレクトされます。ログインのたびにクレデンシャルを入力する必要はありません。

NetBackup SaaS Protection について

NetBackup SaaS Protection は、Microsoft Azure に配備されたクラウドベースのデータ保護ソリューションです。オンプレミスアプリケーションと SaaS アプリケーションのデータを保護するために使用されます。

NetBackup SaaS Protection は、次の SaaS アプリケーションのデータを保護します。

- Box
- Exchange
- Google ドライブ
- SharePoint サイト
- OneDrive サイト
- Teams サイトおよびチャット
- Slack

NetBackup SaaS Protection は、必要な場所での一括または詳細なデータリストアをサポートします。また、最後に更新されたデータや、特定の時点でのデータのリストアもサポートします。

顧客には、テナントと呼ばれるアカウントが構成されます。必要なデータを保護するため、資産はこのテナントに対して構成されます。

詳しくは、『NetBackup SaaS Protection 管理者ガイド』を参照してください。

NetBackup SaaS Protection ハブの追加

NetBackup SaaS Protection ハブを追加し、ハブ内のすべての資産を自動検出できます。

NetBackup SaaS Protection ハブを追加するには

1. 左側で[作業負荷 (Workloads)]、[SaaS]の順にクリックします。
2. [ハブ (Hubs)]タブで、[追加 (Add)]をクリックします。
3. [NetBackup SaaS Protection ハブの追加 (Add a NetBackup SaaS Protection Hub)]ページで、ハブの名前を入力します。
   - 既存のクレデンシャルを使用するには、[既存のクレデンシャルの選択 (Select existing credential)]をクリックします。
     次のページで、必要なクレデンシャルを選択し、[選択 (Select)]をクリックします。
   - 新しいクレデンシャルを作成するには、[新しいクレデンシャルの追加 (Add a new credential)]をクリックします。
     [クレデンシャルの追加 (Add credential)]ページで、次を入力します。
     - [クレデンシャル名 (Credential name)]: クレデンシャルの名前を入力します。
     - [タグ (Tag)]: クレデンシャルに関連付けるタグを入力します。
     - [説明 (Description)]: クレデンシャルの説明を入力します。

- [ユーザー名 (Username)]: NetBackup SaaS Protection でサービスアカウントとして構成されているユーザー名を入力します。
- [パスワード (Password)]: パスワードを入力します。

4 [追加 (Add)]をクリックします。

クレデンシャルが正常に検証されると、ハブが追加され、自動検出が実行されてハブ内の利用可能な資産が検出されます。

p.174 の「NetBackup の SSO (シングルサインオン) の構成」を参照してください。

自動検出の間隔の構成

自動検出では、ハブ内の資産数がカウントされています。NetBackup Web UI は一定の間隔でハブを更新し、追加または削除された資産の最新情報を NetBackup SaaS Protection から取得します。デフォルトでは、更新の間隔は 8 時間です。

自動検出の間隔を設定するには

1 左側で[作業負荷 (Workloads)]、[SaaS]の順にクリックします。

2 右上で[SaaS 設定 (SaaS settings)]、[自動検出 (Autodiscovery)]の順にクリックします。

3 [編集 (Edit)]をクリックします。

4 NetBackup が自動検出を実行するまでの時間数を入力し、[保存 (Save)]をクリックします。

自動検出用のプロキシ構成

NetBackup SaaS Protection の SaaS アプリケーションを検出するには、プライマリサーバーを NetBackup SaaS Protection サーバーに接続する必要があります。プライマリサーバーからの直接的なインターネットトラフィックはオープンになっている必要があります。そうしないと、検出は失敗します。NetBackup SaaS Protection の資産の検出を許可するには、トラフィックを再ルーティングするようプロキシサーバーを構成します。検出プラグインは、プロキシサーバーの種類として HTTP と SOCKS をサポートします。

bpsetconfig ユーティリティを使用したプライマリサーバーのプロキシ設定を行う

bpsetconfig ユーティリティを使用してプライマリサーバーのプロキシ設定を行うには

1 プライマリサーバーでコマンドプロンプトを開きます。

2 ディレクトリを次のパスに変更します。

- Windows の場合: C:¥Program Files¥Veritas¥NetBackup¥bin¥ admincmd

- Linux の場合: /usr/openv/netbackup/bin/admincmd/

3 bpsetconfig コマンドを実行し、次のプロキシの詳細を指定します。

```
bpsetconfig> SAAS_PROXY_HOST = X.X.X.X

bpsetconfig> SAAS_PROXY_PORT = 3128

bpsetconfig> SAAS_PROXY_TYPE = HTTP

bpsetconfig> SAAS_PROXY_TUNELLING = 1
```

プロキシの構成キーは次のとおりです。

表 29-2 プロキシの構成キー

プロキシの構成キー	サポートされる値
SAAS_PROXY_TYPE	HTTP、SOCKS、SOCKS4、SOCKS4A、SOCKS5
SAAS_PROXY_HOST	プロキシホストの IP アドレスまたは FQDN
SAAS_PROXY_TUNNELING	0 または 1
SAAS_PROXY_PORT	任意の有効なポート (1 から 65535)。デフォルトのポートは 3128 です。

資産の詳細の表示

NetBackup SaaS Protection 資産は、[サービス (Services)]と[ハブ (Hubs)]という 2 つのタブに表示されます。

資産の詳細を表示するには

1 左側で[作業負荷 (Workloads)]、[SaaS]の順にクリックします。

[サービス (Services)]タブが表示されます。ハブ用に設定されたサービスが表示されます。

タブでは次の操作を実行できます。

- ハブ用に設定されたサービスを表示する。
- 必要なサービスをサービス一覧で検索する。
- サービスの状態に基づいてサービス一覧をフィルタ処理する。
- 列をソートする。
- 次のサービスの詳細を表示する。
  - サービスが構成されているアプリケーションの種類。

- 前回のバックアップと次回のスケジュールバックアップの日時。
- 書き込みポリシー、スタブポリシー、削除ポリシーに設定される条件。
- WORM の詳細。

2 [ハブ (Hubs)]タブをクリックして、ハブ、StorSite、Stor の詳細を表示します。

左のパネルを使用して、必要な資産に移動できます。[ハブ (Hubs)]タブでは次の操作を実行できます。

- ハブの一覧を表示する。
- 一覧でハブを検索する。
- 新しいハブを追加する。
- クレデンシャルを検証する。
- 列をソートする。
- [処理 (Actions)]をクリックして次を実行する。
  - クレデンシャルを編集する。
  - ハブを削除する。
  - ハブ内の資産を手動で検出する。
- 次の資産の詳細を表示する。
  - サービスの関連付けられた Stor、最後のバックアップの詳細など。
  - ハブのバージョン、ID、および状態。
  - StorSite の状態、ティアの詳細など。
  - Stor の状態、ポリシーの詳細など。
  - NetBackup SaaS Protection Web UI を起動する。NetBackup SaaS Protection Web UI は、サービス、Stor、およびハブのページからクロス起動できます。

詳しくは、『NetBackup SaaS Protection 管理者ガイド』を参照してください。

権限の構成

NetBackup Web UI を使用すると、資産のユーザーの役割にさまざまなアクセス権を割り当てることができます。たとえば、表示権限、更新権限、削除権限、管理権限などです。

p.204 の「アクセスの管理権限」を参照してください。

メモ: NetBackup の SaaS 作業負荷に対するアクセス権を持つユーザーや、NetBackup SaaS Protection に対する権限が限定的またはまったくないユーザーも、NetBackup Web UI で NetBackup SaaS Protection の資産を表示することは可能です。

SaaS 作業負荷に関する問題のトラブルシューティング

SaaS 作業負荷のログについては、次の場所を確認してください。

- PiSaaS
  - Windows の場合: <インストールパス>¥Veritas¥NetBackup¥logs¥ncfnbcs
  - UNIX の場合: <インストールパス>/openv/netbackup/logs/ncfnbcs
- bpVMUtil
  - Windows の場合: <インストールパス>¥Veritas¥NetBackup¥logs¥bpVMutil
  - UNIX の場合: <インストールパス>/openv/netbackup/logs/bpVMutil
- APIs/nbWebServices
  - Windows の場合: <インストールパス>¥Veritas¥NetBackup¥logs¥nbwebservice
  - UNIX の場合: <インストールパス>/openv/logs/nbwebservice

問題をトラブルシューティングするには、次の情報を使用します。

表 29-3 SaaS 作業負荷での問題のトラブルシューティング

問題	推奨処置
ハブ名が正しくない、またはユーザークレデンシャルが無効であることが原因で、ハブの追加に失敗した。	適切なハブ名と有効なクレデンシャルを入力します。
クレデンシャルの検証の問題により、ハブの追加に失敗した。	クレデンシャルの期限が切れていないかどうかを確認します。クレデンシャルが有効かどうかも確認してください。
権限が制限されているため、ハブの追加に失敗した。	SaaS 作業負荷に関する適切な権限をユーザーに割り当てます。 p.203 の「役割の権限」を参照してください。
権限が制限されているため、ハブの削除に失敗した。	SaaS 作業負荷に関する適切な権限をユーザーに割り当てます。 p.203 の「役割の権限」を参照してください。

問題	推奨処置
権限が制限されているため、ハブに対する検出の実行に失敗した。	SaaS 作業負荷に関する適切な権限をユーザーに割り当てます。 p.203 の「役割の権限」を参照してください。
関連付けられたコネクタを NetBackup SaaS Protection から削除しても、サービスが NetBackup から削除されない。	サービスは、コネクタを削除してから 30 日後に NetBackup から削除されます。
[NetBackup SaaS Protection の起動 (Launch NetBackup SaaS Protection)]オプションを使用しても、NSP Web UI を起動できない。NetBackup SaaS Protection Web UI の起動にはクレデンシャルが必要です。	SSO が正しく設定されているかどうかを確認してください。 SSO が正しく設定されている場合は、NetBackup SaaS Protection Web UI にアクセスするための適切な権限がユーザーにあるかどうかを確認してください。 p.174 の「NetBackup の SSO (シングルサインオン) の構成」を参照してください。
SOCKS5 形式によるポート 3128 でのプロキシホスト X.X.X.X への接続	bpsetconfig ユーティリティを使用してプライマリサーバーのプロキシ設定を行います。

30

NetBackup Flex Scale

この章では以下の項目について説明しています。

NetBackup Flex Scale の管理

Flex Scale アプライアンス管理者 (appadmin) は、NetBackup Web UI の Flex Scale インフラページから、クラスタノードとディスクを監視および管理できます。appadmin は、NetBackup Web UI のデフォルトのセキュリティ管理者の役割を持ち、NetBackup のすべてを管理することもできます。

NetBackup Flex Scale の管理について詳しくは、次のリソースを参照してください。

『NetBackup Flex Scale インストールおよび構成ガイド』

『NetBackup Flex Scale 管理者ガイド』

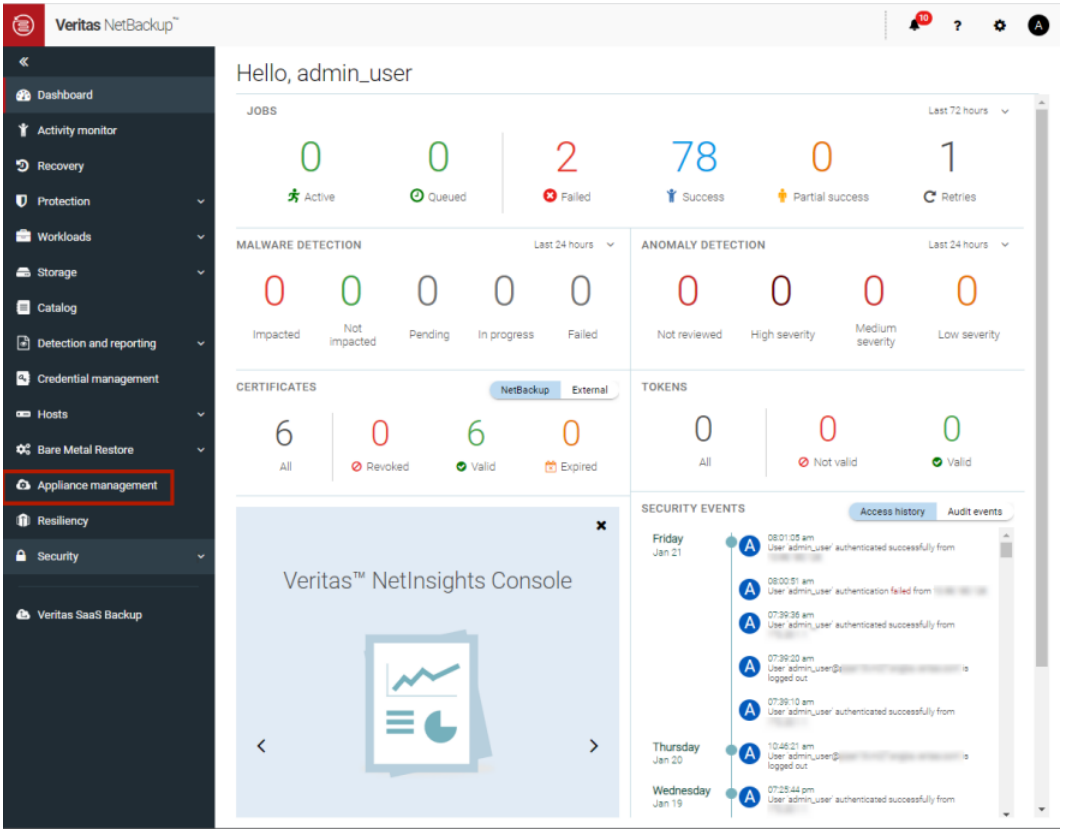
表 30-1 Flex Scale と NetBackup へのアクセス

インターフェースと URL	Flex Scale または NetBackup へのアクセス
NetBackup Web UI https://*primaryserver*/webui/login	Flex Scale を開くには、[アプライアンス管理 (Appliance management)] ノードをクリックします。この操作により、NetBackup Flex Scale インフラ管理コンソールが新しいブラウザタブで開きます。 p.249 の「NetBackup Web UI から NetBackup Flex Scale へのアクセス」を参照してください。

インターフェースと URL	Flex Scale または NetBackup へのアクセス
Flex Scale インフラ管理コンソール IPv4: https://*ManagementServerIPorFQDN*:14161/ IPv6: https://*ManagementServerIP*:14161/	NetBackup を開くには、NetBackup ノードをクリックします。この操作により、NetBackup Flex Scale UI が同じブラウザタブで起動します。Flex Scale インフラ管理コンソールに再度アクセスするには、[クラスタモニター (Cluster Monitor)]、[インフラ (Infrastructure)]の順にクリックし、[クラスタダッシュボード (Cluster Dashboard)]をクリックします。 p.251 の「Flex Scale インフラ管理コンソールから NetBackup へのアクセス」を参照してください。
Flex Scale UI https://ManagementServerIPorFQDN	Flex Scale インフラを表示するには、左側で[クラスタモニター (Cluster Monitor)]、[インフラ (Infrastructure)]の順にクリックします。 そのページから、Flex Scale UI インフラ管理コンソールを開くこともできます。右上にある[クラスタダッシュボード (Cluster Dashboard)]をクリックします。 p.251 の「Flex Scale UI からの NetBackup と Flex Scale のクラスタインフラの管理」を参照してください。

NetBackup Web UI から NetBackup Flex Scale へのアクセス

[アプライアンス管理 (Appliance management)]ノードをクリックすると、NetBackup Web UI から Flex Scale を開くことができます。



NetBackup Web UI から Flex Scale にアクセスするには

1 Web ブラウザで、NetBackup Web UI の URL を入力します。

primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

p.22 の「NetBackup Web UI へのサインイン」を参照してください。

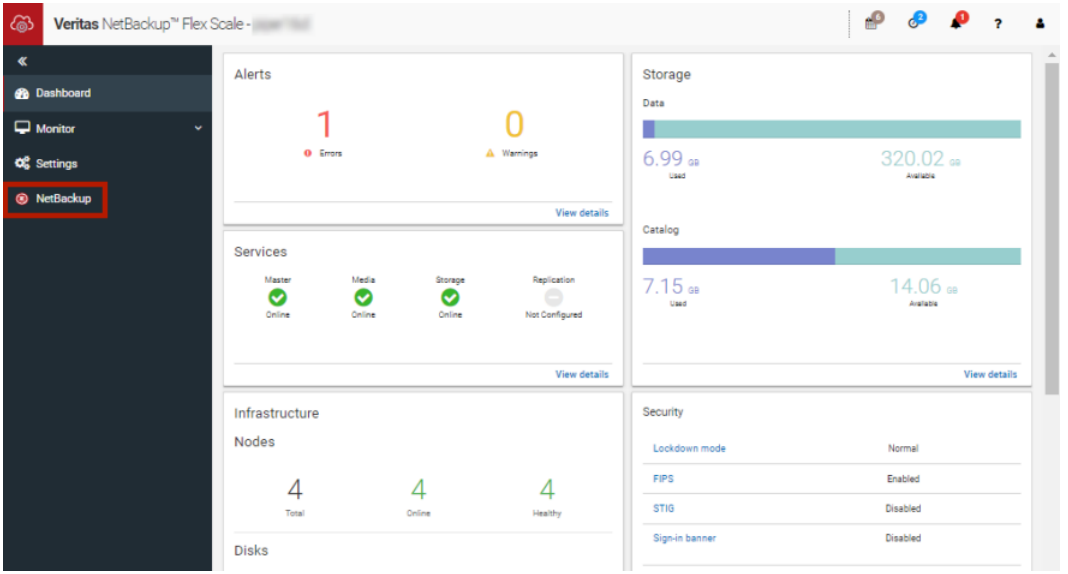
2 appadmin ユーザーのクレデンシャルを入力して、[サインイン (Sign in)]をクリックします。

3 左側の[アプライアンス管理 (Appliance management)]をクリックします。

新しいブラウザウィンドウで、NetBackup Flex Scale インフラ管理コンソールが開きます。

Flex Scale インフラ管理コンソールから NetBackup へのアクセス

［NetBackup］ノードをクリックすると、Flex Scale インフラ管理コンソールから NetBackup を開くことができます。



Flex Scale インフラ管理コンソールから NetBackup にアクセスするには

1. Web ブラウザで、Flex Scale インフラ管理コンソールの URL を入力します。

   https://*ManagementServerIPorFQDN*:14161/

   ManagementServerIP は、NetBackup Flex Scale 管理サーバーに指定したパブリック IP アドレスまたは FQDN です。

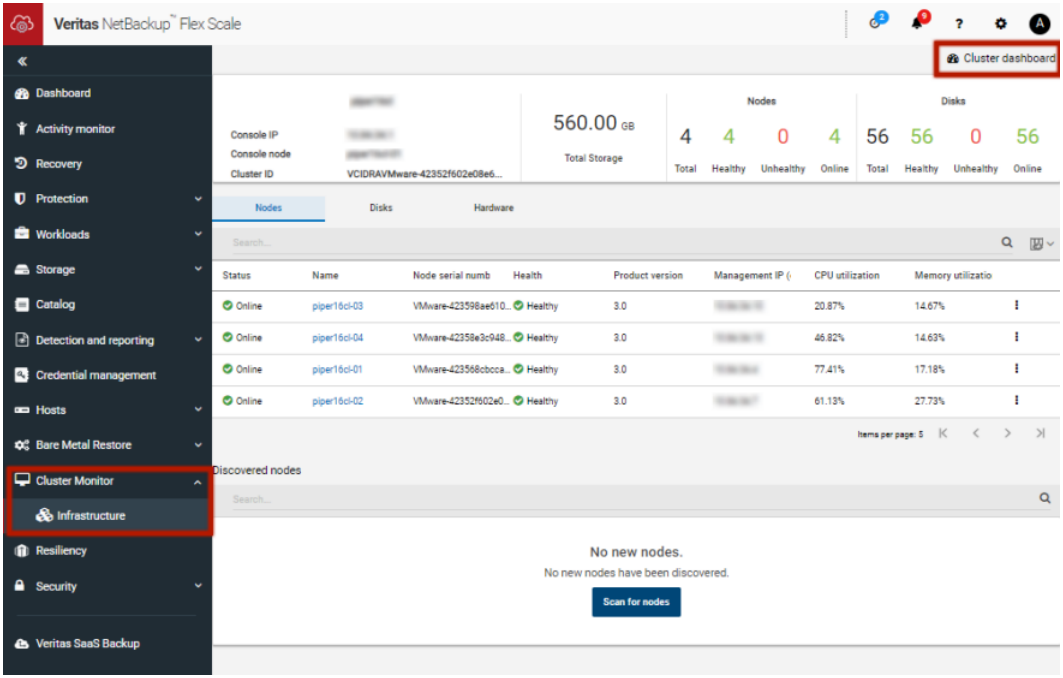
2. appadmin ユーザーのクレデンシャルを入力して、［サインイン (Sign in)］をクリックします。

3. 左側の［NetBackup］をクリックします。

   この操作により、Flex Scale Web UI が同じブラウザタブ内で起動されます。ここでは、NetBackup と Flex Scale の両方を管理できます。

Flex Scale UI からの NetBackup と Flex Scale のクラスタインフラの管理

Flex Scale UI から NetBackup と Flex Scale 両方のインフラを管理できます。



Flex Scale UI から NetBackup と Flex Scale のクラスタインフラを管理するには

1 Web ブラウザで、Flex Scale UI の URL を入力します。

https://*ManagementServerIPorFQDN*

ManagementServerIPorFQDN は、サインインする NetBackup Flex Scale サーバーのホスト名または IP アドレスです。

2 appadmin ユーザーのクレデンシャルを入力して、[サインイン (Sign in)]をクリックします。

Web UI には、NetBackup 機能と Flex Scale のインフラの両方が表示されます。

クラスタインフラを表示するには、[クラスタモニター (Cluster Monitor)]、[インフラ (Infrastructure)]の順にクリックします。

Flex Scale 管理コンソールを開くには、[インフラ (Infrastructure)]ページの右上にある [クラスタダッシュボード (Cluster Dashboard)]をクリックします。

31

NetBackup 作業負荷

この章では以下の項目について説明しています。

その他の資産タイプとクライアントの保護

NetBackup Web UI は保護計画またはポリシーのいずれかを使用して、データベース、仮想マシン、クライアントなどの資産を保護します。一部の作業負荷は、保護計画とポリシーの両方をサポートしています。バックアップとリストアの実行について詳しくは、その作業負荷またはエージェントの関連ガイドを参照してください。標準 (Standard) および MS-Windows クライアントの保護については、『NetBackup 管理者ガイド Vol. 1』を参照してください。

8

ディザスタリカバリとトラブルシューティング

32

Resiliency Platform の管理

この章では以下の項目について説明しています。

NetBackup の Resiliency Platform について

NetBackup と Veritas Resiliency Platform を統合して、ディザスタリカバリ操作を管理できます。Veritas Resiliency Platform で提供される 1 つのコンソールから、プライベート、パブリック、ハイブリッドクラウドにわたるビジネスの稼働時間をプロアクティブに保守できます。NetBackup と Resiliency Platform を統合すると、データセンター内の仮想マシンのすべての回復操作で、完全な自動化、DR 固有の情報の視覚化および監視などの機能を利用できます。

次の点に注意してください。

- 複数の Resiliency Platform を NetBackup プライマリサーバーと統合できます。
- Resiliency Platform には複数のデータセンターを作成できます。
- Resiliency Platform は、NetBackup の Veritas Resiliency Platform バージョン 3.5 以降で使用できます。
- Resiliency Platform を追加すると、資産が自動的に検出され、[仮想マシン (Virtual machines)]タブに表示されます。
- [通知 (Notifications)]セクションには、詳細な情報アラートとエラーメッセージが表示されます。

用語について

次の表では、Veritas Resiliency Platform とNetBackup 統合に関連する主なコンポーネントについて説明します。

用語	説明
Resiliency Platform	NetBackup プライマリサーバーに統合された Veritas Resiliency Platform です。Resiliency Manager は、Resiliency Domain 内で仮想マシンなどの資産を保護するために必要なサービスを提供します。作業負荷自動化サービスも提供します。
Resiliency Manager	Resiliency Domain 内で耐性機能を提供するコンポーネントです。緩やかに結び付いた複数のサービスと分散データリポジトリ、管理コンソールからなります。
IMS (Infrastructure Management Server)	データセンター内の資産インフラを検出、監視、管理するコンポーネントです。IMS は、資産インフラに関する情報を Resiliency Manager に伝送します。IMS は、仮想アプライアンスとして配備されます。必要な規模に拡大するため、複数の IMS を同じデータセンターに配備できます。
データセンター	ソースデータセンターとターゲットデータセンターが格納されている場所。各データセンターには 1 つ以上の IMS が存在します。
Resiliency Group	Resiliency Platform での管理と制御の単位です。関連する資産を Resiliency Group にまとめて、単一のエンティティとして管理および監視します。
自動仮想マシン	Resiliency Platform グループの一部であり、移行、リカバリ、リハーサルなどの処理を実行できる資産。
リカバリ準備状況	移行、リカバリ、リハーサルの各操作に基づいて測定されます。 ■ 低 (Low) - 操作が実行されていないか失敗した場合。 ■ 高 (High) - 過去 7 日間で 1 つ以上の操作が正常に実行されている場合。 ■ 中 (Medium) - リカバリの準備状況が低 (Low) または高 (High) のカテゴリに分類されてない場合。
リカバリポイント目標 (RPO)	リカバリポイントの目標は、障害発生時にリカバリできる時点です。 たとえば、重要な仮想マシンでの RPO が 4 時間である場合、VM でデータをリカバリできる最後の時点が 4 時間前であるため、4 時間分のデータが失われます。

Resiliency Platform の構成

Resiliency Platform の追加、編集、削除、更新を行うことができます。複数の Resiliency Platform を NetBackup に追加できます。

Resiliency Platform の追加

1 つ以上の Resiliency Platform を NetBackup に追加できます。Resiliency Platform を使用すると、仮想マシンを追加して保護を自動化できます。Resiliency Manager がサードパーティの証明書を使用している場合は、『NetBackup Web UI 管理者ガイド』を参照してください。

Resiliency Platform を追加するには

1. 左側の[耐性 (Resiliency)]をクリックします。
2. [Resiliency Platform]タブをクリックします。
3. [Resiliency Platform を追加 (Add Resiliency Platform)]をクリックします。
4. [Resiliency Platform を追加 (Add Resiliency Platform)]ダイアログボックスの指示を読み、[次へ (Next)]をクリックします。
5. [クレデンシャルを追加 (Add credentials)]ダイアログボックスで、次のフィールドに値を入力し、[次へ (Next)]をクリックします。
   - Resiliency Manager のホスト名または IP アドレス
   - Resiliency Platform API アクセスキー
   - NetBackup API アクセスキー
6. [データセンターと Infrastructure Management Server を追加 (Add data center and Infrastructure management server)]ダイアログボックスで、データセンターを選択します。
7. [Infrastructure Management Server]セクションで、優先サーバーを選択します。
8. [追加 (Add)]をクリックします。

   NetBackup に Resiliency Platform を追加すると、Resiliency Platform で NetBackup プライマリサーバーが自動的に構成されます。

メモ: NetBackup で FIPS モードが有効であり、それぞれの証明書をフェッチする必要がある場合は、`Resiliency Platform` **製品ドキュメント**の `NetBackup` **との統合**に関するトピックを参照してください。FIPS トラストストアで Resiliency Platform 証明書をインストールした後、Resiliency Platform を追加する必要があります。(NetBackup で FIPS モードが有効な場合にのみ実行されます)

サードパーティ CA 証明書の構成

自己署名証明書またはサードパーティの証明書を使用して、Resiliency Manager を検証できます。

以下のポイントを考慮します。

- Windows の場合、証明書をファイルパスとして指定するか、信頼できるルート認証局にサードパーティの証明書をインストールできます。
- すでに Resiliency Platform が追加されている場合に、自己署名証明書からサードパーティの証明書に切り替えるには、Resiliency Platform を編集します。

サードパーティ CA 証明書を構成するには

1. 信頼できるルート認証局の、バンドルされている証明書を持つ PKCS #7 または P7B ファイルをコピーします。このファイルは、PEM または DER でエンコードされている場合があります。
2. 信頼できるルート認証局の PEM エンコードされた証明書が連結されて含まれる CA ファイルを作成します。
3. bp.conf ファイルで、次のエントリを作成します。ここで、/certificate.pem はファイル名です。
   - ECA_TRUST_STORE_PATH = /certificate.pem
   - ECA_TRUST_STORE_PATH が参照しているパスにアクセスするための権限が `nbwebsvc` アカウントにあることを確認します。

Resiliency Platform の編集または削除

Resiliency Platform を追加した後、Resiliency Platform と NetBackup API アクセスキーを編集できます。Resiliency Manager のホスト名または IP アドレスを変更または更新することはできません。ただし、Resiliency Platform を削除して、再度 NetBackup に追加することはできます。Resiliency Platform を更新すると、Resiliency Platform で資産の検出がトリガされます。

Resiliency Platform を編集するには

1. 左側の[耐性 (Resiliency)]をクリックします。
2. [Resiliency Platform]タブをクリックします。
3. 編集する Resiliency Platform の[処理 (Actions)]メニューをクリックし、[編集 (Edit)]を選択します。
4. 更新後の [Resiliency Platform API アクセスキー (Resiliency Platform API access key)]と [NetBackup API アクセスキー (NetBackup API access key)]を入力します。
5. [次へ (Next)]をクリックします。

6 ［データセンターと Infrastructure Management Server を編集 (Edit data center and Infrastructure management server)］ダイアログボックスで、［データセンター (Data center)］を選択し、優先 Infrastructure Management Server を選択します。

7 ［保存 (Save)］をクリックします。

8 Resiliency Platform を削除するには、［処理 (Actions)］メニューから［削除 (Delete)］を選択します。

自動化済みまたは未自動化 VM の表示

Veritas Resiliency Platform の Resiliency Group に属する仮想マシンが検出されると［自動化済み (Automated)］タブに表示され、どの Resiliency Group グループにも属さない VM は［未自動化 (Not automated)］タブに表示されます。資産の状態を表示して、さまざまな処理を実行できます。VM を検索したり、フィルタを適用したりすることもできます。

次の表に、［自動化済み (Automated)］タブと［未自動化 (Not automated)］タブに表示される列を示します。

表 32-1

タブ	列	説明
■ 自動化済み (Automated) ■ 未自動化 (Not automated)	名前 (Name)	仮想マシンの名前。
■ 自動化済み (Automated)	RPO	リカバリポイントの目標は、障害発生時にリカバリできる時点です。 たとえば、重要な仮想マシンでの RPO が 4 時間である場合、VM でデータをリカバリできる最後の時点が 4 時間前であるため、4 時間分のデータが失われます。
■ 自動化済み (Automated) ■ 未自動化 (Not automated)	状態 (State)	VM がオンまたはオフかを示します。

タブ	列	説明
■ 自動化済み (Automated)	リカバリ準備状況 (Recovery readiness)	移行、リカバリ、リハーサルの各操作に基づいて測定されます。 ■ 低 (Low) - 操作が実行されていないか失敗した場合。 ■ 高 (High) - 過去 7 日間で 1 つ以上の操作が正常に実行されている場合。 ■ 中 (Medium) - リカバリの準備状況が低 (Low) または高 (High) のカテゴリに分類されてない場合。
■ 自動化済み (Automated) ■ 未自動化 (Not automated)	プラットフォーム (Platform)	VM が属するプラットフォーム。
■ 自動化済み (Automated) ■ 未自動化 (Not automated)	サーバー (Server)	VM のサーバー名。
■ 自動化済み (Automated)	保護 (Protection)	VM の保護状態。
■ 自動化済み (Automated)	Resiliency Group	VM が属する Resiliency Group の名前。
■ 未自動化 (Not automated)	リカバリの処理 (Recovery action)	Resiliency Platform を起動して、VM を Resiliency Group に追加します。

自動化された VM に対する処理を表示および実行するには

1. 左側の[耐性 (Resiliency)]をクリックします。
2. [仮想マシン (Virtual machines)]タブで、[自動化済み (Automated)]をクリックします。
3. VM についての詳細を表示するには、[名前 (Name)]列で VM をクリックします。
4. 同じ Resiliency Group に属するすべての VM を表示するには、目的の Resiliency Group をクリックします。

5 リハーサル、リストア、リカバリなどのディザスタリカバリ操作を実行するには、[Resiliency Platform を起動 (Launch Resiliency Platform)]をクリックします。

シングル署名を有効にするには、NetBackup と Veritas Resiliency Platform で同じ認証ドメインを構成する必要があります。構成しなかった場合、Veritas Resiliency Platform Web コンソールにアクセスするには、ユーザー名とパスワードを使用してログインする必要があります。

6 Resiliency Platform にログオンし、目的の処理を実行します。『Veritas Resiliency Platform ユーザーガイド』を参照してください。

自動化されていない VM に対する処理を表示および実行するには

1 左側の[耐性 (Resiliency)]をクリックします。

2 [仮想マシン (Virtual machines)]タブで、[未自動化 (Not automated)]をクリックします。

3 VM を Resiliency Group に追加するには、[リカバリ処理 (Recovery action)]列で[自動リカバリ (Automate Recovery)]をクリックします。

4 Resiliency Platform に対する目的の処理を実行します。『Veritas Resiliency Platform ユーザーガイド』を参照してください。

NetBackup と Resiliency Platform の問題のトラブルシューティング

問題をトラブルシューティングするには、次の情報を使用します。

表 32-2 問題のトラブルシューティング

問題	処理
Resiliency Platform を使用した現在の NetBackup プライマリサーバーの構成に失敗した。	Veritas Resiliency Platform の Resiliency Manager の次の場所にあるログを確認します。 ■ /var/opt/VRTSitrp/logs/copydata-service.log ■ /var/opt/VRTSitrp/logs/api-service.log
現在の NetBackup プライマリサーバーと Resiliency Platform 間で永続的な接続の確立に失敗した。	■ ログインしているユーザーがクレデンシャル名前空間の権限を持っていることを確認します。 ■ NetBackup プライマリサーバーの次の場所にあるログを確認します。 ■ NetBackup インストールディレクトリの /usr/openv/logs/nbwebservice/ ■ NetBackup Windows の C:¥Program Files¥Veritas¥NetBackup¥logs¥nbwebservice

問題	処理
Veritas Resiliency Platform の起動に失敗した	同じ認証ドメインが Veritas Resiliency Platform と NetBackup の構成に使用されていることを確認します。

33

Bare Metal Restore (BMR) の管理

この章では以下の項目について説明しています。

Bare Metal Restore (BMR) について

NetBackup BMR (Bare Metal Restore) は、NetBackup のサーバーリカバリオプションです。BMR では、サーバーのリカバリ処理が自動化され簡素化されるため、オペレーティングシステムの再インストールまたはハードウェアの構成を手動で実行する必要がなくなります。BMR は、オペレーティングシステム、システム構成、およびすべてのシステムファイルとデータファイルを次の手順でリストアします。

BMR について詳しくは、『NetBackup Bare Metal Restore 管理者ガイド』を参照してください。

NetBackup Web UI では、BMR の次の操作を実行できます。

- VM 変換用にバックアップされているクライアントを表示および管理します。
- 仮想マシン変換ウィザードを使用して BMR 対応のバックアップを仮想マシンに変換します。
- 指定した時点へのリストア構成を作成します。
- VM 変換タスクを表示および管理します。
- BMR のクライアントおよび構成を表示および管理します。
- クライアント構成と VM 変換クライアントの構成に対してリストア前操作を実行します。たとえば、リストア準備、検出準備、Dissimilar Disk Restore の操作などを実行します。

- ブートサーバーを表示および管理します。
- 共有リソースツリー、検出済み構成、Windows デバイスドライバパッケージなどのリソースを表示および管理する。
- BMR リストアタスクまたは検出タスクを表示および管理します。
- BMR のクライアントおよび構成を表示および管理します。
- クライアント構成と VM 変換クライアントの構成に対してリストア前操作を実行します。たとえば、リストア準備、検出準備、Dissimilar Disk Restore の操作などを実行します。
- ブートサーバーを表示および管理します。
- 共有リソースツリー、検出済み構成、Windows デバイスドライバパッケージなどのリソースを表示および管理する。
- BMR リストアタスクまたは検出タスクを表示および管理します。

Bare Metal Restore (BMR) 管理者のカスタム役割の追加

カスタムの RBAC の役割を追加するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]をクリックします。
2. [カスタム役割 (Custom role)]を選択して、役割に付与するすべて権限を手動で設定します。
3. [役割名 (Role name)]と説明を指定します。

   たとえば、役割が BMR 管理者であるすべてのユーザーを対象としていることを示すこともできます。
4. [グローバル (Global)]タブで、[BMR]セクションを展開し、BMR のすべての権限を選択します。

ブートサーバー	表示、削除
クライアント	表示、作成、更新、削除、リストア前
VM 変換	表示、削除、VM 変換

5. [NetBackup の管理 (NetBackup management)]セクションを展開します。
   - [NetBackup ホスト (NetBackup hosts)]グループを見つけます。
   - 次の権限を選択します。

NetBackup ホスト　　表示、更新

- ［NetBackup のバックアップイメージ (NetBackup backup images)］グループを見つけます。
- 次の権限を選択します。

NetBackup バックアップイメージ　　イメージの要求 (Image Requests)、表示 (View)

NetBackup バックアップイメージ　　表示 (View)

6 ESXi サーバーの場合、［ホストプロパティ (Host properties)］で追加の権限が必要です。

- ［グローバル (Global)］タブで［NetBackup の管理 (NetBackup management)］セクションを展開します。
- 次の権限を選択します。

アクセスホスト　　表示、作成、更新、削除

7 ［資産 (Assets)］タブで、次の権限を選択します。

VMware 資産　　表示、更新、リストアターゲットの表示

8 ［割り当て (Assign)］をクリックします。

9 ［作業負荷 (Workloads)］で［割り当て (Assign)］をクリックします。

役割にアクセス権を付与する VMware 資産を選択します。

- すべての VMware 資産と今後追加する資産へのアクセス権を役割に付与するには、［選択した権限を既存および今後のすべての VMware 資産に適用する (Apply selected permissions to all existing and future VMware assets)］を選択します。
- 個々の資産を選択するには、［選択した権限を既存および今後のすべての VMware 資産に適用する (Apply selected permissions to all existing and future VMware assets)］を選択解除し、［追加 (Add)］をクリックします。
  たとえば、データストア、データストアクラスタ、ESXi Server、ESXi クラスタ、リソースプール、vApp を 1 つ以上を選択できます。

10 すべての資産を追加したら、［割り当て (Assign)］をクリックします。

11 ［ユーザー (Users)］カードで、［割り当て (Assign)］をクリックします。次に、このカスタム役割へのアクセス権を付与する各ユーザーを追加します。

12 役割の構成が完了したら、［保存 (Save)］をクリックします。

34

NetBackup Web UI の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。

NetBackup Web UI にアクセスするためのヒント

NetBackup が正しく構成されている場合は、次の URL でプライマリサーバーにアクセスできます。

https://*primaryserver*/webui/login

プライマリサーバーの Web UI が表示されない場合は、次の手順に従って問題をトラブルシューティングします。

接続が拒否された、またはホストに接続できないというエラーがブラウザに表示される

表 34-1 Web ユーザーインターフェースが表示されない場合の解決方法

手順	処理	説明
手順 1	ネットワーク接続を確認します。	
手順 2	ファイアウォールがポート 443 で開かれていることを確認します。	次の記事を参照してください。 https://www.veritas.com/docs/100042950

手順	処理	説明
手順 3	ポート 443 が使用されている場合は、Web UI 用に別のポートを構成します。	次の記事を参照してください。 https://www.veritas.com/docs/100042950
手順 4	nbwebservice が起動していることを確認します。	詳しくは nbwebservice ログを確認してください。
手順 5	vnetd -http_api_tunnel が実行されていることを確認します。	vnetd -http_api_tunnel サービスが実行中であることを確認します。 詳しくは、vnetd -http_api_tunnel ログで OID 491 を確認してください。
手順 6	NetBackup Web サーバーの外部証明書がアクセス可能で、期限切れになっていないことを確認します。	■ Java Keytool コマンドを使用して、次のファイルを検証します。 Windows: *install_path*¥var¥global¥wsl¥credentials¥nbwebservice.jks UNIX: /usr/openv/var/global/wsl/credentials nbwebservice.jks ■ nbwebgroup に、nbwebservice.jks ファイルにアクセスするためのアクセス権があるかどうかを確認します。 ■ Veritas テクニカルサポートにお問い合わせください。

カスタムポートを使用すると Web UI にアクセスできない

- vnetd サービスを再起動します。
- 表 34-1に記載される手順に従ってください。

Web UI にアクセスしようとすると証明書の警告が表示される

NetBackup Web サーバーが、Web ブラウザによって信頼されていない CA が発行した証明書を使用している場合は、証明書の警告が表示されます(NetBackup CA が発行したデフォルトの NetBackup Web サーバーの証明書を含む)。

Web UI にアクセスするときに、ブラウザからの証明書の警告を解決するには

1. NetBackup Web サーバーで、外部証明書を構成します。

   p.133 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。

2. 問題が解決しない場合は、Veritas テクニカルサポートにお問い合わせください。

ユーザーが NetBackup Web UI への適切なアクセス権を持っていない場合

Web UI へのフルアクセスが自動的に付与されるのは、管理者、root ユーザー、または拡張監査ユーザーのみであることに注意してください。その他のユーザーは、Web UI へのアクセス権を持つように RBAC で構成する必要があります。

p.191 の「RBAC の構成」を参照してください。

ユーザーが適切なアクセス権を持っていない場合や、アクセスする必要がある作業負荷資産にアクセスできない場合は、次の操作を行います。

- ユーザーのクレデンシャルが、ユーザーの役割に指定されているユーザー名 (またはユーザー名とドメイン名) と一致していることを確認します。
- ユーザーの役割を[セキュリティ (Security)]、[RBAC]で確認します。役割の権限を変更する必要がある場合もあります。ただし、これらの種類の変更が、それらの役割に属する他のユーザーにも影響することに注意してください。
- ID プロバイダでのすべてのアカウント変更は、ユーザーの役割とは同期されません。ID プロバイダでユーザーアカウントが変更されると、そのユーザーが適切なアクセス権を持たなくなる可能性があります。既存のユーザーアカウントを削除し、新しいアカウントを再度追加するには、NetBackup セキュリティ管理者がユーザーの役割をそれぞれ編集する必要があります。
- ユーザーの役割の変更は、Web UI にすぐには反映されません。アクティブセッションを持つユーザーは、変更内容が有効になる前に、サインアウトしてもう一度サインインする必要があります。

LDAP サーバーを構成するときにユーザーまたはグループを検証できない

管理者が LDAP サーバーを構成するときは、`-d DomainName` オプションを指定する必要があります。`DomainName` には、LDAP サーバー名またはドメイン名を指定できます。`-d DomainName` に指定された名前が何であれ、これは管理者が RBAC の役割にユーザーを追加するときに使用する必要があるドメイン名です。

誤ったドメインを指定すると、「**ユーザーまたはグループを検証できません** `(Unable to validate the user or group)`」というエラーが表示されることがあります。次の項目を確認してください。

- ユーザー名とドメイン名が正しく入力されている。
- 正しいドメイン名を指定した。

指定する必要があるドメイン名は、NetBackup での LDAP サーバーの構成方法によって異なります。RBAC へのユーザーの追加については、管理者にお問い合わせください。