

NetBackup™ Web UI 管理者ガイド

リリース 9.1

VERITAS™

最終更新日: 2021-08-04

法的通知と登録商標

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、NetBackup は、Veritas Technologies LLC または関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

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

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

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

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

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

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

<https://www.veritas.com/support>

次の URL で Veritas Account の情報を管理できます。

<https://my.veritas.com>

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

世界共通 (日本を除く)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

マニュアル

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

<https://sort.veritas.com/documents>

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

第 1 章	NetBackup Web ユーザーインターフェースの概要	11
	NetBackup Web UI について	11
	用語	13
	NetBackup Web UI から NetBackup プライマリサーバーへの初回サイン イン	15
	NetBackup Web UI へのサインイン	17
	NetBackup Web UI からのサインアウト	18
第 2 章	NetBackup の監視	20
	ジョブの監視	20
	ジョブ: キャンセル、中断、再起動、再開、削除	21
	ジョブリストのジョブフィルタ	21
第 3 章	通知	23
	通知について	23
	通知の表示	24
	Web UI での NetBackup イベント通知の変更または無効化	24
	自動通知クリーンアップタスクの構成について	31
	ジョブエラーの電子メール通知の送信	32
	アラートを生成する状態コード	34
第 1 部	役割ベースのアクセス制御の管理	36
第 4 章	NetBackup の役割ベースのアクセス制御について	37
	RBAC の機能	37
	権限を持つユーザー	38
第 5 章	RBAC の役割の構成	39
	RBAC の構成	39
	NetBackup RBAC を使用するための注意事項	40

AD または LDAP ドメインの追加	40
カスタムの RBAC 役割の追加	41
カスタム役割の編集または削除	43
RBAC でのユーザーの表示	44
役割へのユーザーの追加 (非 SAML)	44
役割へのユーザーの追加 (SAML)	45
役割からのユーザーの削除	45
デフォルトの RBAC の役割	46
管理者	47
デフォルトの AHV 管理者	47
デフォルトのクラウド管理者	48
デフォルトの Kubernetes 管理者	49
デフォルトの NetBackup Kubernetes Operator サービス	49
デフォルトの RHV 管理者	50
デフォルトの Resiliency 管理者	51
デフォルトの Microsoft SQL Server 管理者	51
デフォルトのセキュリティ管理者	52
デフォルトのストレージ管理者	53
デフォルトの VMware 管理者	54

第 6 章

RBAC 権限	56
役割の権限について	56
[グローバル (Global)]> [NetBackup の管理 (NetBackup management)]	
.....	57
NetBackup Web 管理コンソールの管理	58
アクセスホスト	59
エージェントレスホスト	59
異常	60
データの分類	60
電子メール通知	60
イベントログ	61
NetBackup ホスト	62
イメージ共有	64
NetBackup バックアップイメージ	65
ジョブ	65
ライセンス	66
メディアサーバー	67
リモートプライマリサーバーの認証局	67
耐性	68
リソース制限	68
保持レベル	69

[サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]	69
クラウドプロバイダ	70
CloudPoint サーバー	72
WebSocket サーバー	73
[グローバル (Global)]> [保護 (Protection)]	74
[グローバル (Global)]> [セキュリティ (Security)]	76
アクセス制御	77
セキュリティイベント	78
証明書管理	79
ディザスタリカバリのパスフレーズ	81
ID プロバイダと SAML 証明書の構成	81
KMS (キーマネージメントサービス)	82
パスフレーズの制約	83
グローバルセキュリティ設定	83
信頼バージョン	84
API キー	84
ユーザー証明書	84
ユーザーセッションと認証	85
[グローバル (Global)]> [ストレージ (Storage)]	87
クラウドストレージ	88
ディスクプール	88
ストレージの Key Management Service	89
ストレージサーバー	89
ストレージユニット	91
テープメディア	92
レプリケーション対応のターゲットストレージサーバー	92
資産	93
AHV 資産	93
クラウド資産	95
Kubernetes 資産	97
Microsoft SQL Server 資産	98
OpenStack サーバー	100
RHV 資産	100
ユニバーサル共有	102
VMware 資産	103
Windows および標準のクライアント形式	106
保護計画	107
クレデンシャル	109
アクセスの管理	110
Web UI の領域にアクセスできる役割の削除	114
アクセスの定義の表示	115

第 2 部	セキュリティの管理	116
第 7 章	セキュリティイベントと監査ログ	117
	セキュリティイベントと監査ログの表示	117
	NetBackup の監査について	118
	監査レポートのユーザーの ID	121
	監査保持期間と監査レコードのカタログバックアップ	121
	詳細な NetBackup 監査レポートの表示	122
	システムログへの監査イベントの送信	124
第 8 章	セキュリティ証明書の管理	126
	NetBackup のセキュリティ管理と証明書について	126
	NetBackup ホスト ID とホスト ID ベースの証明書	127
	NetBackup セキュリティ証明書の管理	127
	NetBackup 証明書の再発行	129
	NetBackup 証明書の認証トークンの管理	130
	NetBackup での外部セキュリティ証明書の使用	132
	NetBackup Web サーバーで外部証明書を使用するための構成	132
	Web サーバー用に構成された外部証明書の削除	133
	Web サーバー用外部証明書のアップデートまたは更新	134
	ドメイン内の NetBackup ホストの外部証明書情報の表示	134
第 9 章	ユーザーセッションの管理	136
	NetBackup ユーザーセッションのサインアウト	136
	NetBackup ユーザーのロック解除	137
	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	138
	並列ユーザーセッションの最大数の構成	138
	失敗したサインインの試行の最大数を構成する	139
	ユーザーがサインインするときのパナーの表示	139
第 10 章	マスターサーバーのセキュリティ設定の管理	141
	安全な通信のための認証局	141
	NetBackup 8.0 以前のホストとの通信の無効化	142
	NetBackup ホスト名の自動マッピングの無効化	142
	NetBackup 証明書の配備のセキュリティレベルについて	143
	NetBackup 証明書配備のセキュリティレベルの選択	144
	ディザスタリカバリのパスフレーズの設定	145
	信頼できるプライマリサーバーについて	146
	信頼できるプライマリサーバーの追加	147

	信頼できるプライマリサーバーの削除	148
第 11 章	ユーザー用の API キーの作成と管理 (管理者)	149
	API キーについて	149
	API キーの追加または API キーの詳細の表示	150
	API キーの編集、再発行、または削除	151
第 12 章	API キーの追加と管理 (ユーザー)	153
	API キーの追加または自分の API キーの詳細の表示	153
	API キーの編集、再発行、または削除	154
	NetBackup REST API での API キーの使用	155
第 13 章	認証オプションの設定	156
	NetBackup Web UI のサインインオプション	156
	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	157
	スマートカード認証の構成の編集	158
	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	159
	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	159
	シングルサインオン (SSO) 設定について	160
	NetBackup のシングルサインオン (SSO) の構成	162
	SAML キーストアの構成	163
	SAML キーストアの構成と IDP 構成の追加および有効化	166
	IDP を使用した NetBackup プライマリサーバーの登録	167
	IDP 構成の管理	168
	ビデオ: NetBackup でのシングルサインオンの設定	171
	SSO のトラブルシューティング	171
	リダイレクトの問題	171
	認証に関連する問題が原因でサインインできない	173
第 14 章	ホストの管理	176
	NetBackup ホスト情報の表示	176
	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	177
	複数のホスト名を持つホストのマッピングの削除	181
	ホストの属性のリセット	181

第 3 部	ストレージとバックアップの管理	183
第 15 章	ストレージの構成	184
	ストレージの構成について	184
	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	185
	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	187
	ディスクプールの作成	189
	ストレージユニットの作成	190
	ユニバーサル共有の作成	191
	NetBackup Web UI からのイメージ共有の使用	193
	ストレージ構成のトラブルシューティング	194
	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	195
	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	198
第 16 章	保護計画の管理	200
	保護計画の作成	200
	保護計画の編集または削除	206
	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	207
	保護計画からの資産のサブスクライブ解除	208
	保護計画の上書きの表示	209
	今すぐバックアップについて	209
第 17 章	従来ポリシーの管理	211
	NetBackup の従来ポリシーについて	211
	NetBackup Web UI でのポリシー管理について	212
第 18 章	使用状況レポートと容量ライセンス	213
	プライマリサーバー上のバックアップデータサイズの追跡	213
	使用状況レポートのサーバーリストの構成	214
	容量ライセンスのレポートのスケジュール設定	215
	増分レポートのその他の構成	218
	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	220

第 4 部	Veritas Resiliency Platform	222
第 19 章	Resiliency Platform の管理	223
	NetBackup の Resiliency Platform について	223
	用語について	224
	Resiliency Platform の構成	225
	Resiliency Platform の追加	225
	サードパーティ CA 証明書の構成	225
	Resiliency Platform の編集または削除	226
	自動化済みまたは未自動化 VM の表示	227
	NetBackup と Resiliency Platform の問題のトラブルシューティング	229
第 5 部	クレデンシャル	230
第 20 章	クレデンシャルの管理	231
	NetBackup でのクレデンシャル管理について	231
	NetBackup でのクレデンシャルの追加	232
	クレデンシャルの編集	234
	クレデンシャルの削除	234
第 21 章	NetBackup Web UI のトラブルシューティング	236
	NetBackup Web UI にアクセスするためのヒント	236
	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	238
	vssat コマンドで AD または LDAP ドメインを追加できない	238
	AD または LDAP サーバーとの接続を確立できない	239
	ユーザークレデンシャルが有効ではない	240
	不正なユーザーベース DN、またはグループベース DN が指定され た	241
	ユーザーベース DN またはグループベース DN に同じ名前の複数の ユーザーまたはグループが存在する	242
	ユーザーまたはグループが存在しない	242
	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)	243

NetBackup Web ユーザー インターフェースの概要

この章では以下の項目について説明しています。

- [NetBackup Web UI について](#)
- [用語](#)
- [NetBackup Web UI から NetBackup プライマリサーバーへの初回サインイン](#)
- [NetBackup Web UI へのサインイン](#)
- [NetBackup Web UI からのサインアウト](#)

NetBackup Web UI について

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。

- 資産の保護は、保護計画、ジョブ管理、資産の保護状態の可視性を通じて実現します。
また、ポリシー管理は、限られた数のポリシー形式でも利用できます。
- 作業負荷管理者は、保護計画を作成し、SLO を満たす保護計画に資産をサブスクライブし、保護状態を監視し、資産のセルフサービスリカバリを実行できます。
Web UI は次の作業負荷をサポートします。
 - クラウド
 - Kubernetes
 - Microsoft SQL Server
 - Nutanix AHV
 - OpenStack
 - Oracle
 - Red Hat Virtualization (RHV)
 - VMware
- 使用状況レポートは、プライマリサーバー上のバックアップデータのサイズを追跡します。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、またはクレデンシヤ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。

- ダッシュボードには、NetBackup ジョブ、証明書、トークン、セキュリティイベント、使用状況レポートの概要が表示されます。

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、ストレージ、およびストレージオプションを一元的に構成する場所

保護計画には、次の利点があります。

- デフォルトの作業負荷管理者は、資産を保護するために使用する保護計画を選択できます。
- 必要な RBAC 権限を使用して、作業負荷管理者は、使用されているバックアップスケジュールやストレージを含む保護計画を作成して管理できます。
p.56 の「[役割の権限について](#)」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。

セルフサービスリカバリ

NetBackup Web UI を使用すると、作業負荷管理者が、その作業負荷に適用可能な VM、データベース、その他の資産形式を簡単にリカバリできるようになります。

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。

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 1-1 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。ルート、管理者、拡張監査のすべてのユーザーは、NetBackup の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が、通常は NetBackup 管理コンソールのユーザーを指します。 「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。レガシーポリシーは、NetBackup 管理コンソールで作成します。
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 管理コンソールまたは CLI 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アルを設定できます。
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 (Workload)	資産のタイプです。たとえば、VMware、RHV、AHV、またはクラウドです。

NetBackup Web UI から NetBackup プライマリサーバー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.38 の「[権限を持つユーザー](#)」を参照してください。

ルートまたは管理者のクレデンシア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	<code>username</code>	<code>jane_doe</code>
Windows ユーザー	<code>DOMAIN\username</code>	<code>WINDOWS\jane_doe</code>
UNIX ユーザー	<code>username@domain</code>	<code>john_doe@unix</code>

- 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.39 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.38 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、Web サーバー向けに外部証明書を構成するための手順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。

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。

p.38 の「権限を持つユーザー」を参照してください。

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

認可済みのユーザーのみが NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

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 クレデンシヤルを入力して、[サインイン (Sign in)]をクリックします。

次に例を示します。

ユーザーの種類	使用する形式	例
ローカルユーザー	<code>username</code>	<code>jane_doe</code>
Windows ユーザー	<code>DOMAIN#username</code>	<code>WINDOWS#jane_doe</code>
UNIX ユーザー	<code>username@domain</code>	<code>john_doe@unix</code>

証明書またはスマートカードでサインインする

権限を持つユーザーである場合は、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。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

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。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

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、プロフィールアイコン、[サインアウト (Sign out)]の順にクリックします。

NetBackup の監視

この章では以下の項目について説明しています。

- [ジョブの監視](#)
- [ジョブ: キャンセル、中断、再起動、再開、削除](#)
- [ジョブリストのジョブフィルタ](#)

ジョブの監視

[ジョブ (Jobs)]ノードを使用して、NetBackup 環境のジョブを監視し、特定のジョブの詳細を表示します。

ジョブを監視するには

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

次の操作を実行できます。

- 表示するジョブの名前をクリックします。
- ジョブのチェックボックスにチェックマークを付け、そのジョブで、ジョブの再起動などの特定のアクションを実行します。
p.21 の「[ジョブ: キャンセル、中断、再起動、再開、削除](#)」を参照してください。

- 2 表示するジョブの名前をクリックします。

[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。

- 3 [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.21 の「ジョブリストのジョブフィルタ」を参照してください。

ジョブ: キャンセル、中断、再起動、再開、削除

ジョブを管理するには

- 1 [ジョブ (Jobs)] 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)]、[待ち行列へ再投入済み (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フィルタ

特定の状態のジョブを表示するために、ジョブをフィルタできます。たとえば、実行中のジョブまたは一時停止中のジョブをすべて表示できます。

ジョブリストをフィルタするには

- 1 [ジョブ (Jobs)] をクリックします。
- 2 ジョブリストの上にある[フィルタ (Filter)] オプションをクリックします。

- 3 [フィルタ (Filter)]ウィンドウでフィルタオプションを選択すると、表示されるジョブが動的に変わります。フィルタオプションは次のとおりです。
 - すべて (All)
 - 有効 (Active)
 - 完了 (Done)
 - 失敗 (Failed)
 - 未完了 (Incomplete)
 - 部分的に成功 (Partially Successful)
 - キューへ投入済み (Queued)
 - 成功 (Successful)
 - 一時停止 (Suspended)
 - 再試行を待機中 (Waiting for Retry)
- 4 [フィルタの適用 (Apply Filters)]をクリックします。
- 5 選択した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。

通知

この章では以下の項目について説明しています。

- [通知について](#)
- [ジョブエラーの電子メール通知の送信](#)

通知について

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関い合わせて、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/opensv/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.26 の [表 3-1](#) 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 分かかります。

表 3-1 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	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	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 <code>__DSSU_POLICY_{Storage_Unit_Name}</code> 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 <code>{Storage_Unit_Name}</code> が作成されました。
	削除 (DELETE)	重大	ストレージユニット <code>{Storage_Unit_Name}</code> が削除されました。
	更新 (UPDATE)	情報	ストレージユニット <code>{Storage_Unit_Name}</code> 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 <code>{Storage_Unit_Group_Name}</code> 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 <code>{Storage_Unit_Group_Name}</code> 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 <code>{Storage_Unit_Group_Name}</code> が更新されました。
	更新 (UPDATE)	情報	ストレージサービス <code>{Storage_Service_Name}</code> 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 <code>{Policy_Name}</code> 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 <code>{Policy_Name}</code> が削除されました。 バージョン <code>Version_Number</code> のストレージライフサイクルポリシー <code>{Policy_Name}</code> 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 <code>{Version}</code> が変更されました。

イベントと通知の種類	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 メモ: 有効なクレデンシヤルを持つ VMware サーバー、RHV サーバー、Nutanix AHV、またはクラウドサーバーを追加すると、Machine Create 通知が生成されます。 無効なクレデンシヤルを持つ VMware サーバー、RHV サーバー、Nutanix AHV、またはクラウドサーバーを追加しようとする、Machine Create および Machine Delete 通知が生成されます。 エージェントレス VMware をリストアするときは、NetBackup ではファイルがリストアされる仮想マシンのクレデンシヤルが必要です。これらのクレデンシヤルは、vCenter クレデンシヤルと同様の方法でデータベースに格納されます。ホスト値として UUID を使用してこれらのクレデンシヤルがデータベースで追加、更新または削除されると、マシンタイプの通知が生成されます。	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。

イベントと通知の種類	処理	重大度	通知メッセージの例
	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。
	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。

イベントと通知の種類	処理	重大度	通知メッセージの例
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	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。
KMS 証明書の有効期限 KMSCredentialStatus	有効期限	警告	KMS サーバー <code>{KMS_Server_Name}</code> との通信に使用される証明書があと <code>{days_to_expiration}</code> 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。
メッセージブローカーサービスの状態 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 <code>Protection_Plan_Name</code> が作成されます。 保護計画 <code>Protection_Plan_Name</code> 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 <code>Protection_Plan_Name</code> が更新されます。
	削除 (Delete)	重大	保護計画 <code>Protection_Plan_Name</code> 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。 <code>Asset_ClassAsset_Display_Name</code> が、保護計画 <code>Protection_Plan_Name</code> にサブスクライブされます。
	更新 (Update)	情報	保護計画 <code>Protection_Plan_Name</code> の <code>Asset_ClassAsset_Display_Name</code> のサブスクリプションが更新されます。

イベントと通知の種類	処理	重大度	通知メッセージの例
	削除 (Delete)	重大	<i>Asset_ClassAsset_Display_Name</i> が、保護計画 <i>Protection_Plan_Name</i> 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 <i>Image_Name</i> が変更されました。 カタログイメージ <i>Image_Name</i> が期限切れになりました。

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 3-2」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 9.1 API リファレンス」を参照してください。

表 3-2 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)

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.34 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.118 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ヤ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れる場合があります。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 3-3 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 3-3 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。

状態コード	エラーメッセージ
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。

1

役割ベースのアクセス制御の 管理

- [第4章 NetBackup の役割ベースのアクセス制御について](#)
- [第5章 RBAC の役割の構成](#)
- [第6章 RBAC 権限](#)

NetBackup の役割ベースのアクセス制御について

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](#)
- [権限を持つユーザー](#)

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、ルート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 4-1 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.46 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。

機能	説明
RBAC イベントの監査	NetBackup は、RBAC イベントを監査します。
DR 準備	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 4-2 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
ルート Windows 管理者グループに属するユーザー 拡張監査ユーザー RBAC 管理者の役割を持つユーザー	完全
nbaseadmin Appliance ユーザー appadmin Flex Appliance ユーザー	NetBackup セキュリティ管理者ロールのユーザーは、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。 注意: NetBackup Appliance のデフォルトの admin ユーザーには、Web UI にアクセスする権限はありません。
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.39 の「RBAC の構成」を参照してください。

RBAC の役割の構成

この章では以下の項目について説明しています。

- [RBAC の構成](#)
- [デフォルトの RBAC の役割](#)

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 5-1 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には、NetBackup で Active Directory または LDAP ドメインを認証する必要があります。 p.40 の「 AD または LDAP ドメインの追加 」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。 p.56 の「 役割の権限について 」を参照してください。
3	ユーザーに付与する役割を選択します。	デフォルトの RBAC の役割にユーザーを直接追加するか、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.44 の「 役割へのユーザーの追加 (非 SAML) 」を参照してください。 p.45 の「 役割へのユーザーの追加 (SAML) 」を参照してください。 p.46 の「 デフォルトの RBAC の役割 」を参照してください。 p.41 の「 カスタムの RBAC 役割の追加 」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。(たとえば、NetBackup バックアップイメージは、API または NetBackup 管理コンソールからのみ表示および管理できます)。これらの種類の操作は RBAC に含まれているため、役割の管理者は、API ユーザーおよび 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 Web UI の役割ベースのアクセスは、Active Directory (AD) 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があります。

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 コマンドを使用して AD または LDAP ドメインを追加するには

- 1 ユーザーアカウント (手順 3 で -m オプションに指定) に、AD または LDAP サーバーの問い合わせに必要な権限があることを確認します。
- 2 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。

3 コマンド `vssat` を実行します。

たとえば、LDAP ドメインを追加するには次のようにします。

```
vssat addldapdomain -d nbudomain -s ldap://example.com -u  
"OU=Users,DC=example,DC=com"  
-g "OU=Groups,DC=example,DC=com" -m "CN=TestUser,OU=Users,DC=example,DC=com" -t msad
```

たとえば、AD ドメインを追加するには次のようにします。

```
vssat addldapdomain -d nbudomain -s ldap://domaincontroller.example.com  
-u "cn=Users,dc=example,dc=com" -g "cn=Users,dc=example,dc=com"  
-m "CN=TestUser,OU=Users,DC=example,DC=com" -t msad
```

`domaincontroller.example.com` の場合は、認証を完了できないことに注意してください。

4 指定した AD または LDAP ドメインが正常に追加されたことを確認します。

```
vssat validateprpl -p username -d ldap:DomainName -b  
localhost:1556:nbatd
```

`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。

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 [アクセス権 (Permissions)]カードで、[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ヤルが必要です。

 - [作業負荷 (Workloads)]カードは、[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)]カードは、[保護計画 (Protection plans)]の権限を選択すると有効になります。
 - [クレデンシヤル (Credentials)]カードは、[クレデンシヤル (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.56 の「[役割の権限について](#)」を参照してください。

p.40 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 [ユーザーの選択 (Select users)]カードで、[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、クレデンシヤルの権限は、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 [役割 (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。

役割のグローバル権限を編集するには [グローバル権限 (Global permissions)]タブで、[編集 (Edit)]をクリックします。

役割のユーザーを編集するには [ユーザー (Users)]タブをクリックします。

役割のアクセス定義を編集するには [アクセス定義 (Access definitions)]タブをクリックします。

p.56 の「[役割の権限について](#)」を参照してください。

p.40 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.44 の「[役割へのユーザーの追加 \(非 SAML\)](#)」を参照してください。

p.45 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。

- p.93 の「[資産](#)」を参照してください。
- p.107 の「[保護計画](#)」を参照してください。
- p.109 の「[クレデンシャル](#)」を参照してください。

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 [役割 (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。

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)

この手順では、役割に非 SAML ユーザーまたはグループを追加して、その役割の権限をユーザーに付与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ことでサインインできます。ユーザーが役割に追加された後、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[デフォルトのサインインまたはスマートカード (Default sign-in or smart card)]を選択します。

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	<code>username</code>	<code>jane_doe</code>
	<code>groupname</code>	<code>admins</code>
Windows ユーザーまたはグループ	<code>DOMAIN#username</code>	<code>WINDOWS#Admins</code>
	<code>DOMAIN#groupname</code>	<code>WINDOWS#jane_doe</code>
UNIX ユーザーまたはグループ	<code>username@domain</code>	<code>john_doe@unix</code>
	<code>groupname@domain</code>	<code>admins@unix</code>

- 6 [リストに追加 (Add to list)]をクリックします。

役割へのユーザーの追加 (SAML)

この手順では、役割に SAML ユーザーまたはグループを追加して、その役割の権限をユーザーに付与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。ユーザーが役割に追加された後、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。

形式	例
<code>username@domain</code>	<code>john_doe@unix</code>
<code>groupname@domain</code>	<code>admins@unix</code>

- 6 [リストに追加 (Add to list)]をクリックします。

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。

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。

- p.47 の「[管理者](#)」を参照してください。
- p.47 の「[デフォルトの AHV 管理者](#)」を参照してください。
- p.48 の「[デフォルトのクラウド管理者](#)」を参照してください。
- p.49 の「[デフォルトの Kubernetes 管理者](#)」を参照してください。
- p.49 の「[デフォルトの NetBackup Kubernetes Operator サービス](#)」を参照してください。
- p.50 の「[デフォルトの RHV 管理者](#)」を参照してください。
- p.51 の「[デフォルトの Resiliency 管理者](#)」を参照してください。
- p.51 の「[デフォルトの Microsoft SQL Server 管理者](#)」を参照してください。
- p.52 の「[デフォルトのセキュリティ管理者](#)」を参照してください。
- p.53 の「[デフォルトのストレージ管理者](#)」を参照してください。
- p.54 の「[デフォルトの VMware 管理者](#)」を参照してください。

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) のコピーがある場合、これらの役割は自動的に更新されません。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。

管理者

管理者の役割は、NetBackup のすべての側面に対する完全な NetBackup の権限を持ち、管理できます。

- グローバル RBAC 権限。
 - NetBackup の管理 - NetBackup の構成と管理。
 p.57 の「[\[グローバル \(Global\)\]](#)>[\[NetBackup の管理 \(NetBackup management\)\]](#)」を参照してください。
 - 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。
 p.74 の「[\[グローバル \(Global\)\]](#)>[\[保護 \(Protection\)\]](#)」を参照してください。
 - セキュリティ - NetBackup のセキュリティ設定。
 p.76 の「[\[グローバル \(Global\)\]](#)>[\[セキュリティ \(Security\)\]](#)」を参照してください。
 - ストレージ - バックアップストレージの設定の管理。
 p.87 の「[\[グローバル \(Global\)\]](#)>[\[ストレージ \(Storage\)\]](#)」を参照してください。
- 資産 - すべての資産タイプの管理。
 p.93 の「[資産](#)」を参照してください。
- 保護計画 - 保護計画を使用したバックアップの実行方法の管理。
 p.107 の「[保護計画](#)」を参照してください。
- 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の管理。
 p.109 の「[クレデンシャル](#)」を参照してください。

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。

表 5-2 デフォルトの AHV 管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)], [NetBackup の管理 (NetBackup management)]	
アクセスホスト	表示、作成、削除
エージェントレスホスト	表示
NetBackup ホスト	表示、更新
NetBackup バックアップイメージ	表示、内容の表示
ジョブ	表示

種類	権限
リソース制限	表示、作成、更新、削除
信頼できるプライマリサーバー	表示
[グローバル権限 (Global permissions)]、[ストレージ (Storage)]	
ストレージユニット	表示
レプリケーション対応のターゲットストレージサーバー	表示
作業負荷	
AHV 資産	完全な権限
保護計画	完全な権限
クレデンシャル	完全な権限

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。

表 5-3 デフォルトのクラウド管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]、[NetBackup の管理 (NetBackup management)]	
NetBackup バックアップイメージ	内容の表示、表示
ジョブ	表示
メディアサーバー	表示
信頼できるプライマリサーバー	表示
スナップショット管理サーバープラグイン	表示、作成、更新、アクセス管理
スナップショット管理サーバー	完全な権限
[グローバル権限 (Global permissions)]>[ストレージ (Storage)]	
ストレージユニット	表示
レプリケーション対応のターゲットストレージサーバー	表示

種類	権限
作業負荷	
クラウド資産	完全な権限
保護計画	完全な権限

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。

表 5-4 デフォルトの Kubernetes 管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]、[NetBackup の管理 (NetBackup management)]	
NetBackup ホスト	表示、更新
リソース制限	表示、作成、更新、削除
信頼できるプライマリサーバー	表示
作業負荷	
Kubernetes 資産	完全な権限
保護計画	完全な権限
クレデンシヤル	完全な権限

デフォルトの NetBackup Kubernetes Operator サービス

この役割は、Kubernetes Operator サービス (プラグイン) 用に構成された API キーのユーザーアカウントに必要な権限を提供します。

メモ: これらの権限のみを持つユーザーは、Web UI にサインインできません。

表 5-5 デフォルトの Kubernetes Operator サービスの役割に対する RBAC 権限

種類	権限
作業負荷	
Kubernetes 資産	作成、更新

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。

NetBackup 9.1 以降、この役割の権限によって、ユーザーは RHV 資産のジョブを表示および管理できます。この役割には、資産のすべてのジョブを表示するグローバル権限は含まれなくなりました。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。

p.100 の「RHV 資産」を参照してください。

表 5-6 デフォルトの RHV 管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]>[NetBackup の管理 (NetBackup management)]	
アクセスホスト	表示、作成、削除
NetBackup ホスト	表示、更新
リソース制限	表示、作成、更新、削除
信頼できるプライマリサーバー	表示
[グローバル権限 (Global permissions)]>[ストレージ (Storage)]	
ストレージユニット	表示
レプリケーション対応のターゲットストレージサーバー	表示
作業負荷	
RHV 資産	完全な権限
保護計画	完全な権限

デフォルトの Resiliency 管理者

この役割には、VMware 資産用に Veritas Resiliency Platform (VRP) を保護するためのすべての権限が付与されています。

表 5-7 デフォルトの Resiliency 管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]>[NetBackup の管理 (NetBackup management)]	
Resiliency Domain	完全な権限
クレデンシヤル	完全な権限

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。

表 5-8 デフォルトの Microsoft SQL Server 管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]、[NetBackup の管理 (NetBackup management)]	
ジョブ	表示
信頼できるプライマリサーバー	表示
[グローバル権限 (Global permissions)]>[ストレージ (Storage)]	
ストレージユニット	表示
レプリケーション対応のターゲットストレージサーバー	表示
作業負荷	
SQL Server 資産	完全な権限
保護計画	完全な権限
クレデンシヤル	完全な権限

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、その他の領域を含む) を表示できます。

表 5-9 デフォルトのセキュリティ管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]>[NetBackup の管理 (NetBackup management)]	
指定したカテゴリを除くすべてのカテゴリ	表示、アクセス管理
NetBackup ホスト	完全な権限
メディアサーバー	完全な権限
リモートプライマリサーバーの認証局	完全な権限
信頼できるプライマリサーバー	完全な権限
[グローバル権限 (Global permissions)]>[保護 (Protection)]	
すべてのカテゴリ	表示、アクセス管理
[グローバル権限 (Global permissions)]>[セキュリティ (Security)]	
指定したカテゴリを除くすべてのカテゴリ	表示、アクセス管理
アクセス制御	完全な権限
証明書の管理: NetBackup 認証局、外部証明書、NetBackup 証明書、NetBackup セキュリティトークン	完全な権限
ディザスタリカバリのパスフレーズ	完全な権限
ID プロバイダと SAML 証明書の構成	完全な権限
キーマネジメントサービス	完全な権限
パスフレーズの制約	更新 (完全な権限)
グローバルセキュリティ設定	完全な権限
ユーザーセッションと認証: API キー、ユーザー証明書、ユーザーセッション	完全な権限
[グローバル権限 (Global permissions)]>[ストレージ (Storage)]	

種類	権限
すべてのカテゴリ	表示、アクセス管理
作業負荷	
すべての作業負荷	表示、アクセス管理
保護計画	表示、アクセス管理
クレデンシヤル	表示、アクセス管理

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。

p.47 の「[管理者](#)」を参照してください。

表 5-10 デフォルトのストレージ管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]、[NetBackup の管理 (NetBackup management)]	
データの分類	表示
NetBackup ホスト	表示
メディアサーバー	表示
リモートプライマリサーバーの認証局	表示
保持レベル	表示
[サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]	表示、作成、更新、削除
[グローバル権限 (Global permissions)]、[保護 (Protection)]	
ポリシー	表示
SLP の処理時間帯	完全な権限
ストレージライフサイクルポリシー	完全な権限
[グローバル権限 (Global permissions)]>[セキュリティ (Security)]	
NetBackup セキュリティトークン	表示、作成
キーマネージメントサービス	キー、キーの詳細の表示

種類	権限
[グローバル権限 (Global permissions)]、[ストレージ (Storage)]	
クラウドストレージ	表示
ディスクプール	表示、作成、更新、削除
ストレージサーバー	表示、作成、更新、削除
ディスクボリューム	表示、作成、更新
ストレージユニット	表示、作成、更新、削除
[テープメディア (Tape media)]、[テープメディアサーバーグループ (Tape media server groups)]	表示
[テープメディア (Tape media)]、[テープメディアボリュームプール (Tape media volume pools)]	表示
レプリケーション対応のターゲットストレージサーバー	表示

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。

NetBackup 9.1 以降、この役割の権限によって、ユーザーは VMware 資産のジョブを表示および管理できます。この役割には、資産のすべてのジョブを表示するグローバル権限は含まれなくなりました。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。

p.103 の「VMware 資産」を参照してください。

表 5-11 デフォルトの VMware 管理者の役割に対する RBAC 権限

種類	権限
[グローバル権限 (Global permissions)]>[NetBackup の管理 (NetBackup management)]	
アクセスホスト	表示、作成、削除
NetBackup ホスト	表示、更新

種類	権限
継続的なデータ保護ゲートウェイ	表示、作成、削除
ホストプロパティ	表示、作成、更新
NetBackup のバックアップイメージ	表示、内容の表示
リソース制限	表示、作成、更新、削除
信頼できるプライマリサーバー	表示
[グローバル権限 (Global permissions)]>[ストレージ (Storage)]	
ストレージユニット	表示
レプリケーション対応のターゲットストレージサーバー	表示
作業負荷	
VMware 資産	トランザクションログのスケジュールの編集 (Edit transaction log schedules) を除くすべての権限。
保護計画	完全な権限

RBAC 権限

この章では以下の項目について説明しています。

- 役割の権限について
- [\[グローバル \(Global\)\]](#)> [\[NetBackup の管理 \(NetBackup management\)\]](#)
- [\[グローバル \(Global\)\]](#)> [\[保護 \(Protection\)\]](#)
- [\[グローバル \(Global\)\]](#)> [\[セキュリティ \(Security\)\]](#)
- [\[グローバル \(Global\)\]](#)> [\[ストレージ \(Storage\)\]](#)
- 資産
- 保護計画
- クレデンシヤル
- アクセスの管理

役割の権限について

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。

表 6-1 NetBackup RBAC の役割の権限

カテゴリ	説明
グローバル	<p>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。</p> <p>NetBackup の管理 - NetBackup の構成と管理。</p> <p>p.57 の「[グローバル (Global)]> [NetBackup の管理 (NetBackup management)]」を参照してください。</p> <p>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。</p> <p>p.74 の「[グローバル (Global)]> [保護 (Protection)]」を参照してください。</p> <p>セキュリティ - NetBackup のセキュリティ設定。</p> <p>p.76 の「[グローバル (Global)]> [セキュリティ (Security)]」を参照してください。</p> <p>ストレージ - バックアップストレージの設定の管理。</p> <p>p.87 の「[グローバル (Global)]> [ストレージ (Storage)]」を参照してください。</p>
資産	<p>1 つ以上の資産タイプを管理します。例: VMware 資産。</p> <p>p.93 の「資産」を参照してください。</p>
保護計画	<p>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。</p> <p>p.107 の「保護計画」を参照してください。</p>
クレデンシャル	<p>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。</p> <p>p.109 の「クレデンシャル」を参照してください。</p>

[グローバル (Global)]> [NetBackup の管理 (NetBackup management)]

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。たとえば、役割のグローバルジョブまたはホストの権限は、すべてのジョブまたはすべてのホストに適用されます (現在、ホストの権限は特定のホストに適用できません)。

NetBackup 管理では次の権限を利用できます。

p.58 の「[NetBackup Web 管理コンソールの管理](#)」を参照してください。

p.59 の「[アクセスホスト](#)」を参照してください。

p.59 の「[エージェントレスホスト](#)」を参照してください。

p.60 の「[異常](#)」を参照してください。

p.60 の「[データの分類](#)」を参照してください。

- p.60 の「[電子メール通知](#)」を参照してください。
- p.61 の「[イベントログ](#)」を参照してください。
- p.62 の「[NetBackup ホスト](#)」を参照してください。
- p.64 の「[イメージ共有](#)」を参照してください。
- p.65 の「[NetBackup バックアップイメージ](#)」を参照してください。
- p.65 の「[ジョブ](#)」を参照してください。
- p.66 の「[ライセンス](#)」を参照してください。
- p.67 の「[メディアサーバー](#)」を参照してください。
- p.67 の「[リモートプライマリサーバーの認証局](#)」を参照してください。
- p.68 の「[耐性](#)」を参照してください。
- p.68 の「[リソース制限](#)」を参照してください。
- p.69 の「[保持レベル](#)」を参照してください。
- p.69 の「[\[サーバー \(Servers\)\]、\[信頼できるプライマリサーバー \(Trusted primary servers\)\]](#)」を参照してください。
- p.70 の「[クラウドプロバイダ](#)」を参照してください。
- p.72 の「[CloudPoint サーバー](#)」を参照してください。
- p.73 の「[WebSocket サーバー](#)」を参照してください。

NetBackup Web 管理コンソールの管理

これらの権限を持つユーザーは、Veritas 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は、次のガイドを参照してください。

[NetBackup インストールガイド](#)

[NetBackup アップグレードガイド](#)

表 6-2 NetBackup Web 管理コンソールの管理のための RBAC 権限

操作	説明
ダンプの診断	スレッドダンプまたはヒープダンプを取得し、ファイルに書き込みます。プライマリサーバー上の作成されたスレッドダンプファイルのファイルパスを返します。
ガーベジコレクション	NetBackup Web サービスの JVM がガーベジコレクションを実行するように要求します。この API はプライベート API です。

アクセスホスト

アクセスホストは、NetBackup プライマリサーバーと RHV マネージャ、AHV マネージャ、または VMware サーバー間の間接通信を確立するためのチャンネルとして機能します。このホストは、バックアップ中は「バックアップホスト」、リストアを実行するときは「リカバリホスト」です。

表 6-3 アクセスホストの RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	構成されているアクセスホストを表示します。	
作成 (Create)	作業負荷のアクセスホストを追加します。	表示 (View)
更新 (Update)	アクセスホストの詳細を更新します。	表示 (View)
削除 (Delete)	作業負荷用に構成されているアクセスホストを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

エージェントレスホスト

エージェントレスホストの権限により、ユーザーは NetBackup データベースのエージェントレスホストの詳細を表示および削除できます。

表 6-4 エージェントレスホストの RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	NetBackup データベースに格納されているエージェントレスホストの詳細を表示します。	
削除 (Delete)	エージェントレスホストの詳細を削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

異常

表 6-5 異常に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	フィードバックがある異常のリストを表示します。 NetBackup Web UI で、ユーザーはシステムで報告された異常を次のように表示できます。 [通知 (Notification)]アイコン、[すべて表示 (Show all)]、[異常 (Anomalies)]タブの順にクリックします。	
更新 (Update)	ユーザーが異常を誤検知として報告できません。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

データの分類

データの分類ポリシー属性は、バックアップを保存するポリシーの分類を指定します。これらのレベルは、NetBackup 管理コンソールの[ホストプロパティ (Host Properties)]、[データの分類 (Data Classification)]から作成および編集できます。

表 6-6 データの分類に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	NetBackup ポリシー属性のデータ分類レベルを表示および選択します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

電子メール通知

これらの権限により、ユーザーは、チケットシステムで使用するために作成された電子メール通知の設定を表示および管理できます。NetBackup Web UI では、これらの設定は [設定 (Settings)]、[電子メール通知 (Email notifications)]にあります。NetBackup 管理コンソールで利用可能なその他の通知タイプ (バックアップ管理者またはホスト管理者) は、NetBackup Web UI ではまだ利用できません。

表 6-7 NetBackup 電子メール通知に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	ジョブエラーの電子メール通知の設定を表示します。	
更新 (Update)	ジョブエラーの電子メール通知の設定を更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

イベントログ

イベントログメッセージの権限により、ユーザーは外部サービスからのメッセージリソースバンドルの表示と管理を行うことができます。イベントログ通知の権限により、ユーザーは NetBackup 通知を表示して管理できます。

メモ: これらの権限のみを持つユーザーは、Web UI にサインインできません。

イベントログのメッセージ

メモ: これらの操作は、NetBackup API からのみ利用可能です。

表 6-8 イベントログメッセージに対する RBAC 権限

操作	説明
表示 (View)	外部サービスからのメッセージを表示します。(例: VRP または Picasso)
作成 (Create)	外部サービスのイベントログメッセージを作成します。
更新 (Update)	外部サービスのイベントログメッセージを更新します。
削除 (Delete)	外部サービスのイベントログメッセージを削除します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

イベントログの通知

表 6-9 イベントログ通知に対する RBAC 権限

操作	説明
表示 (View)	ツールバー、NetBackup 通知、外部サービスの通知にベルのアイコン表示します。
作成 (Create)	外部サービスのイベントログ通知を作成します。この操作は、NetBackup API からのみ利用可能です。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

NetBackup ホスト

メモ: ホストの設定が NetBackup Web UI の「[セキュリティ \(Security\)](#)」ノードの下に表示されますが、ユーザーにすべての RBAC の「[セキュリティ](#)」権限を付与しても、ユーザーに「[ホスト](#)」の権限が付与されるわけではありません。

NetBackup ホストの権限によって、ユーザーはホストとホストのマッピングを表示および管理できます。

また、NetBackup Web UI で次の設定や機能を有効にするには、少なくとも表示の権限も必要です: アクティビティモニターの「[ユーザーセッション \(User sessions\)](#)」、[プロセス \(Processes\)](#) および「[デーモン \(Daemons\)](#)」、RHV、AHV、VMware の「[ジョブ \(Jobs\)](#)」、ツールバーの通知、「[自動検出 \(Auto discovery\)](#)」設定。

表 6-10 NetBackup アクセスホストに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	プライマリサーバーの NetBackup ホストを表示します。	メディアサーバーで実行されているデーモンを表示するには: [NetBackup の管理 (NetBackup management)]>[サーバー (Server)]>[メディアサーバー (Media server)]>[表示 (View)] p.67 の「 メディアサーバー 」を参照してください。
作成 (Create)	外部認証局にホストレコードを追加します。この操作は、API からのみ利用可能です。	
更新 (Update)	証明書の自動再発行を許可または無効化します。	表示 (View)

操作	説明	その他の必要な操作
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
ホストをコメント化 (Comment hosts)	NetBackup ホストについての追加情報を提供するコメントを追加します。	表示 (View)
ホストのマッピングを削除 (Delete host mappings)	ホストマッピング、共有マッピング、またはクラスターマッピングを削除します。	表示 (View)
ホストプロパティのリセット (Reset host properties)	ホストのマッピング情報やホストの通信状態など、ホストのプロパティをリセットします。	表示 (View)
ホストのマッピングを更新 (Update host mappings)	ホストマッピング、共有マッピング、またはクラスターマッピングを追加します。自動ホストマッピングを承認または拒否します。	表示 (View)
ホストマッピングの表示 (View host mappings)	プライマリサーバーのホストのホストマッピングを表示します。この操作は API からのみ利用可能であり、Web UI ではどの機能にも不要です。	

継続的なデータ保護ゲートウェイ

NetBackup の継続的なデータ保護 (CDP) ゲートウェイの権限により、ユーザーは既存の NetBackup ホスト上の CDP 構成を表示および管理できます。

表 6-11 継続的なデータ保護ゲートウェイに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	構成済みの継続的なデータ保護ゲートウェイを表示します。	[NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[表示 (View)]
作成 (Create)	構成済みの継続的なデータ保護ゲートウェイを構成します。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[表示 (View)]
削除 (Delete)	構成済みの継続的なデータ保護ゲートウェイを削除します。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[表示 (View)]
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

ホストプロパティ

ホストプロパティの権限は、ユーザーが NetBackup ホストの設定を管理することを可能にします。これらの操作は、NetBackup API からのみ利用可能です。

表 6-12 ホストプロパティの RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	ホストの構成設定を表示します。	
作成 (Create)	ホストの構成設定を追加します。	
更新 (Update)	ホストの構成設定を更新します。	
削除 (Delete)	ホストの構成設定を削除するか、設定をデフォルト値に戻します。	
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

イメージ共有

これらの権限により、ユーザーはクラウドストレージに格納されているバックアップイメージを検索およびリストアできます。

表 6-13 イメージ共有に対する RBAC 権限

操作	説明
Amazon マシンイメージ (AMI)	
表示 (View)	アマゾンウェブサービスの Amazon マシンイメージ (AMI) を表示します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。
クラウドイメージ	
表示 (View)	共有クラウドのイメージを表示します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。
共有クラウドイメージのインポート (Import shared cloud images)	共有クラウドイメージを NetBackup カタログにインポートします。

NetBackup バックアップイメージ

メモ: 特定の資産のイメージまたはインスタントアクセスイメージからファイルとフォルダをリストアするには、NetBackup バックアップイメージに対する表示、または表示と内容の表示の権限も必要です。

p.93 の「[資産](#)」を参照してください。

イメージの有効期限の変更やコピーの管理など、NetBackup イメージの表示と管理を行います。これらの操作は、NetBackup API からのみ利用可能です。

表 6-14 NetBackup バックアップイメージに対する RBAC 権限

操作	説明
表示 (View)	バックアップイメージの属性を表示します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。
有効期限の変更 (Change expiration)	イメージカタログ内のバックアップおよびメディアカタログ内のメディアの有効期限を更新します。
コピーの管理 (Manage copies)	バックアップイメージの複製コピーを管理します。
内容の表示 (View contents)	イメージ内のファイルを含むバックアップイメージの内容を表示します。

ジョブ

メモ: アクティビティモニターでデーモンとプロセスを表示するには、NetBackup ホストと、必要に応じてメディアサーバーが必要です。

p.62 の「[NetBackup ホスト](#)」を参照してください。

ジョブの権限はグローバルであり、NetBackup Web UI で任意の NetBackup 資産のジョブを管理できます。資産の作業負荷 (RHV、Kubernetes、VMware) に対してジョブ権限が構成されます。これら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。

p.100 の「[RHV 資産](#)」を参照してください。

p.103 の「VMware 資産」を参照してください。

p.97 の「Kubernetes 資産」を参照してください。

表 6-15 ジョブに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	アクティビティモニターと NetBackup Web UI ダッシュボードにジョブを表示します。	
削除 (Delete)	任意のジョブを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「アクセスの管理」を参照してください。	表示 (View)
ジョブのキャンセル (Cancel jobs)	任意のジョブを取り消します。	表示 (View)
ジョブの再起動 (Restart jobs)	任意のジョブを再起動します。	表示 (View)
ジョブの再開 (Resume Job)	任意のジョブを再開します。	表示 (View)
ジョブの一時停止 (Suspend Job)	任意のジョブを一時停止します。	表示 (View)

ライセンス

これらの権限により、ユーザーはプライマリサーバーの傾向データ (使用状況) を表示し、Veritas Usage Insights の登録キーを表示および管理できます。

表 6-16 ライセンスに対する RBAC 権限

操作	説明
表示 (View)	単一または複数のプライマリサーバーのフロントエンドデータの使用状況を表示します。 カスタム登録キーファイルから Usage Insights の登録キーを取得します。カスタム登録キーファイルから有効な登録キー情報を取得します。 NetBackup Web UI では、傾向データはダッシュボードと使用状況ノードの使用状況ウィジェットに表示されます。
更新 (Update)	Usage Insights の既存のカスタム登録キーファイルを、登録キーと有効な登録キー情報で上書きします。カスタム登録キーファイルに有効な登録キー情報を追加します。

操作	説明
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

メディアサーバー

これらの権限により、ユーザーはプライマリサーバーとサポート対象のストレージに対して構成されたメディアサーバーを表示できます。

表 6-17 メディアサーバーに対する RBAC 権限

操作	説明
表示 (View)	構成されたメディアサーバーとメディアサーバーのストレージを表示します。この操作は、NetBackup API からのみ利用可能です。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

リモートプライマリサーバーの認証局

この権限により、ユーザーは他のドメインのリモートプライマリサーバーの CA 証明書を表示できます。

表 6-18 リモートプライマリサーバーの認証局に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	リモートプライマリサーバーの CA 証明書を表示します。	この権限は、リモートプライマリサーバーとの間で信頼関係を追加するためにも必要です。 [NetBackup の管理 (NetBackup management)]、[サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]、[表示 (View)] [NetBackup の管理 (NetBackup management)]、[サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]、[作成 (Create)] p.69 の「 [サーバー (Servers)] 、 [信頼できるプライマリサーバー (Trusted primary servers)] 」を参照してください。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

耐性

これらの権限により、ユーザーは Veritas Resiliency Platform を表示および管理できます。

表 6-19 Resiliency Domain に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	Veritas Resiliency Platform の詳細を表示します。	
作成 (Create)	Resiliency Platform を追加します。	[クレデンシヤル (Credentials)]、[表示 (View)] [クレデンシヤル (Credentials)]、[作成 (Create)]
更新 (Update)	Resiliency Platform を編集します。	表示 (View) [クレデンシヤル (Credentials)]、[表示 (View)] [クレデンシヤル (Credentials)]、[更新 (Update)]
削除 (Delete)	Resiliency Platform を削除します。	表示 (View) [クレデンシヤル (Credentials)]、[表示 (View)] [クレデンシヤル (Credentials)]、[削除 (Delete)]
検出 (Discover)	Resiliency Platform を更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

リソース制限

リソース制限により、VMware、Nutanix AHV、または RHV リソース形式で実行できる同時バックアップの数が制御されます。

リソースの制限を表示および管理するには、作業負荷と作業負荷の資産を表示する権限をユーザーに付与する必要があります。これらの設定は、Web UI または API から役割を作成するときのみ利用可能です。

表 6-20 リソース制限に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	すべての作業負荷の種類に構成されているリソース制限を表示します。	

操作	説明	その他の必要な操作
作成 (Create)	リソースの制限を追加または編集します。	表示 (View)
更新 (Update)	値をデフォルト設定にリセットします。(Web UI では、この権限によって[デフォルト設定にリセットする (Reset default settings)]ボタンが有効になります)	表示 (View)
削除 (Delete)	リソース制限の上書き設定を削除します。	表示 (View) 作成 (Create)
アクセスの管理 (Manage access)	p.110の「 アクセスの管理 」を参照してください。	表示 (View)

保持レベル

ポリシーの保持レベルによって、スケジュールに従って作成されるバックアップまたはアーカイブが NetBackup で保持される期間が決まります。この設定は、プライマリサーバーに適用されます。

メモ: これらの操作は NetBackup ポリシーを作成するときのみ利用可能です。特定のレベルを選択しない場合は、デフォルトのレベルである 2 週間が使用されます。

表 6-21 保持レベルに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	ポリシースケジュールの保持レベルを表示します。	
更新 (Update)	ポリシースケジュールの保持レベルを更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110の「 アクセスの管理 」を参照してください。	表示 (View)

[サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]

これらの権限により、ユーザーはプライマリサーバーの信頼できるプライマリサーバーを表示および管理できます。複数の NetBackup ドメイン (プライマリサーバー) 間でレプリケーション操作を実行するには、両方のプライマリサーバーに、もう一方のプライマリサーバーとの信頼関係が設定されている必要があります。

表 6-22 信頼できるプライマリサーバーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	現在のプライマリサーバーと信頼関係があるリモートプライマリサーバーを表示します。	
作成 (Create)	リモートプライマリサーバーとの信頼関係を追加します。	表示 (View) [NetBackup の管理 (NetBackup management)], [リモートプライマリサーバーの認証局 (Remote primary server certificate authority)], [表示 (View)]
更新 (Update)	リモートプライマリサーバーとの信頼関係を更新します。API のみ。	
削除 (Delete)	ターゲットプライマリサーバーとの信頼関係を削除します。	表示 (View) [NetBackup の管理 (NetBackup management)], [リモートプライマリサーバーの認証局 (Remote primary server certificate authority)], [表示 (View)]
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

クラウドプロバイダ

これらの権限により、ユーザーはクラウドプラグインを表示および管理できます。これらのプラグインには、AWS (Amazon Web Services)、Microsoft Azure、GCP (Google Cloud Platform) の各構成が含まれます。

表 6-23 クラウドプロバイダに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	構成されているクラウドプラグインを表示します。	
作成 (Create)	クラウド構成を追加します。	表示 (View)
更新 (Update)	クラウド構成を更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

表 6-24 AWS (Amazon Web Services) の構成に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	構成済みの AWS (Amazon Web Services) の構成を表示します。	
作成 (Create)	AWS 構成を追加します。	表示 (View)
更新 (Update)	AWS 構成を更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

表 6-25 Microsoft Azure Stack Hub 構成に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	Azure Stack Hub の構成を表示します。	
作成 (Create)	Azure Stack Hub の構成を追加します。	表示 (View)
更新 (Update)	Azure Stack Hub の構成を更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

表 6-26 Microsoft Azure 構成に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	Azure 構成を表示します。	
作成 (Create)	Azure 構成を追加します。	表示 (View)
更新 (Update)	Azure 構成を更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

表 6-27 GCP (Google Cloud Platform) 構成に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	GCP 構成を表示します。	
作成 (Create)	GCP 構成を追加します。	表示 (View)
更新 (Update)	GCP 構成を更新します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

CloudPoint サーバー

これらの権限により、ユーザーはプライマリサーバーの CloudPoint サーバーを表示および管理し、メディアサーバーを CloudPoint サーバーに関連付けられます。

表 6-28 CloudPoint サーバーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	CloudPoint サーバーを表示します。	
作成 (Create)	CloudPoint サーバーを追加します。	
更新 (Update)	CloudPoint サーバーを更新します。	表示 (View)
検出 (Discover)	CloudPoint サーバーの検出を手動で開始します。	表示 (View)
拡張機能の表示 (View extensions)	拡張機能を表示します。	表示 (View) 更新 (Update)
拡張機能の管理 (Manage extensions)	拡張機能を追加し、有効化または無効化します。	表示 (View) 更新 (Update) 拡張機能の表示 (View extensions)
関連メディアサーバーの更新 (Update associated media servers)	メディアサーバーを関連付けたり、CloudPoint サーバーに関連付けられているメディアサーバーを更新したりします。	表示 (View) 更新 (Update) 関連メディアサーバーの表示 (View associated media servers)

操作	説明	その他の必要な操作
関連メディアサーバーの表示 (View associated media servers)	CloudPoint サーバーに関連付けられているメディアサーバーを表示します。	表示 (View) 更新 (Update) [NetBackup の管理 (NetBackup management)], [メディアサーバー (Media server)], [表示 (View)]
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

WebSocket サーバー

これらの権限は、クラウド内のアプリケーションがファイアウォールの内側にある NetBackup プライマリサーバーと通信できるように NetBackup WebSocket サービス (NBWSS) を管理します。NBWSS は、WebSocket プロトコルを使用して、クラウド内のアプリケーションのサーバーへのセキュア接続を作成します。この接続を介して、アプリケーションは REST API を呼び出して NetBackup と対話し、NetBackup から通知を受信できます。

WebSocket サーバーの操作は、NetBackup API と NetBackup 管理コンソールからのみ可能です。

表 6-29 WebSocket サーバーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	すべての WebSocket サーバーを一覧表示します。validateHost および validateUrl API を使用して、ユーザーが WebSocket サーバーを検証できるようにします。	
作成 (Create)	WebSocket サーバーを追加します。	表示 (View)
更新 (Update)	WebSocket サーバーリストのホストの状態を更新します。	表示 (View)
削除 (Delete)	WebSocket サーバーを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

[グローバル (Global)]> [保護 (Protection)]

ポリシー

保護権限を持つユーザーは、Web UI や API を使用して、NetBackup ポリシーの処理を表示または実行できます。ポリシー形式は、MS-Windows、Standard、MS-SQL-Server、NDMP、Oracle、VMware に限定されます。

メモ: 管理者の役割を持つユーザーのみがポリシーを管理することをお勧めします。ユーザーが管理者の役割のメンバーでないと、すべてのポリシー管理操作を実行するための十分な権限をユーザーが持っていない場合があります。

表 6-30 ポリシーに対する RBAC 権限

操作	説明
表示 (View)	ポリシーを表示します。
作成 (Create)	ポリシーを作成します。
更新 (Update)	ポリシーを更新します。
削除 (Delete)	ポリシーを削除します。
手動バックアップ	ポリシーの手動バックアップを開始します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

SLP 設定

これらの権限により、ユーザーはストレージライフサイクルポリシーの保守方法と SLP ジョブの実行方法を表示およびカスタマイズできます。

表 6-31 SLP 設定に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	グローバルストレージライフサイクルポリシー (SLP) 設定を表示します。	
更新 (Update)	グローバルストレージライフサイクルポリシー (SLP) 設定を変更します。	表示 (View)

SLP の処理時間帯

これらの権限により、ユーザーはストレージライフサイクルポリシー (SLP) 操作のジョブを実行できるタイミングを表示および管理できます。

表 6-32 SLP の処理時間帯に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	設定された SLP の処理時間帯を表示します。	
作成 (Create)	SLP の処理時間帯を追加またはコピーします。	表示 (View)
更新 (Update)	SLP の処理時間帯を編集します。	表示 (View)
削除 (Delete)	SLP の処理時間帯を削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

ストレージライフサイクルポリシー

保護権限を持つユーザーは、ストレージライフサイクルポリシーの操作を表示または実行できます。

表 6-33 ストレージライフサイクルポリシーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	ストレージライフサイクルポリシーの詳細または個別のストレージライフサイクルポリシーの詳細を表示します。	
作成 (Create)	ストレージライフサイクルポリシーを追加またはコピーします。	表示 (View) p.76 の 表 6-34 を参照してください。
更新 (Update)	ストレージライフサイクルポリシーを編集します。	表示 (View) p.76 の 表 6-34 を参照してください。
削除 (Delete)	ストレージライフサイクルポリシーを削除します。	表示 (View)

操作	説明	その他の必要な操作
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

SLP に対する追加の権限

SLP を作成または更新するには、次の追加の操作が必要です。

表 6-34 ストレージライフサイクルポリシーに必要なその他の操作

RBAC カテゴリ	サブカテゴリ	操作
[グローバル権限 (Global permissions)]、[NetBackup の管理 (NetBackup management)]	データの分類 NetBackup ホスト 保持レベル	表示 (View)
[グローバル権限 (Global permissions)]、[保護 (Protection)]	ポリシー	表示 (View)
[グローバル権限 (Global permissions)]、[ストレージ (Storage)]	ストレージサーバー ディスクボリューム ストレージユニット テープメディア	表示 (View)

[グローバル (Global)]> [セキュリティ (Security)]

- p.77 の「[アクセス制御](#)」を参照してください。
- p.78 の「[セキュリティイベント](#)」を参照してください。
- p.79 の「[証明書管理](#)」を参照してください。
- p.81 の「[ディザスタリカバリのパスフレーズ](#)」を参照してください。
- p.81 の「[ID プロバイダと SAML 証明書の構成](#)」を参照してください。
- p.82 の「[KMS \(キーマネージメントサービス\)](#)」を参照してください。
- p.83 の「[パスフレーズの制約](#)」を参照してください。
- p.83 の「[グローバルセキュリティ設定](#)」を参照してください。
- p.84 の「[信頼バージョン](#)」を参照してください。
- p.84 の「[API キー](#)」を参照してください。

p.84 の「[ユーザー証明書](#)」を参照してください。

p.85 の「[ユーザーセッションと認証](#)」を参照してください。

アクセス制御

アクセス制御権限により、ユーザーは RBAC のユーザーと RBAC の役割を表示または管理できます。

メモ: NetBackup Web UI では、ユーザーを表示したり、役割のユーザーを追加または削除したりできるように、ユーザーと役割の両方に権限を持っている必要があります。

ユーザー

表 6-35 ユーザーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	API のみ。RBAC でユーザーまたはグループを表示します。 この権限は、管理者が Web UI を使用して役割を作成するときに自動的に付与されます。	該当なし
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	
役割にアクセス権を割り当てる (Assign access to role)	RBAC の役割にユーザーまたはグループを割り当てるか、削除します。	表示 (View)

役割

注意: NetBackup Web UI (または名前空間) 内の特定の RBAC カテゴリへのアクセス権を役割の管理者が付与できるようにするには、その管理者にも、それらの名前空間に対する[表示 (View)]と[アクセスの管理 (Manage access)]権限が必要です。たとえば、役割の管理者が VMware 資産 (ASSETS | VMWARE |) または親レベルの名前空間に対する[表示 (View)]および[アクセスの管理 (Manage access)]権限を付与されている場合にのみ、役割の管理者は役割を作成できます。

表 6-36 役割

操作	説明	その他の必要な操作
表示 (View)	RBAC の役割を表示します。	次の 1 つ以上の権限も必要です。 作成 (Create) 更新 (Update) 削除 (Delete)
作成 (Create)	RBAC の役割を追加します。	表示 (View)
更新 (Update)	RBAC の役割に関連する権限を編集します。 NetBackup Web UI で、管理者がアクセスの管理を持っている名前空間に対するアクセス権を管理者が付与できます。	表示 (View)
削除 (Delete)	RBAC の役割を削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	
役割にアクセス権を割り当てる (Assign access to role)	API のみ。役割が RBAC 内のオブジェクトにアクセスできるようにします。 この権限は、管理者が Web UI を使用して役割を作成するときに自動的に付与されます。	該当なし

セキュリティイベント

これらの権限により、ユーザーは、ユーザーのアクセス履歴とユーザーが開始した NetBackup に対する変更を記録する監査イベントに対するアクセスを表示および管理できます。

表 6-37 セキュリティイベント

操作	説明	その他の必要な操作
表示 (View)	プライマリサーバーのアクセス履歴と監査イベントを表示します。	

操作	説明	その他の必要な操作
表示 (View)	[監査イベント (Audit event)] の設定を管理します。これらの設定により、ユーザーは [監査イベント (Audit event)] に表示される監査イベントカテゴリを選択できます。	[NetBackup の管理 (NetBackup management)]、[ホスト (Hosts)]、[表示 (View)] [NetBackup の管理 (NetBackup management)]、[ホスト (Hosts)]、[作成 (Create)] [NetBackup の管理 (NetBackup management)]、[ホスト (Hosts)]、[更新 (Update)] [NetBackup の管理 (NetBackup management)]、[ホスト (Hosts)]、[削除 (Delete)]
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

証明書管理

証明書の管理権限により、ユーザーは NetBackup 認証局と証明書を管理し、NetBackup がどのように外部認証局を使用するかを管理できます。

NetBackup 認証局

NetBackup 認証局の権限によって、ユーザーは NetBackup ルート CA をより高いキーの強度に移行するためのプロセスを管理できます。

表 6-38 NetBackup 認証局

操作	説明
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。
CA の移行 (Migrate CA)	NetBackup ルート CA を表示して、2048 ビット以上のキー強度に移行します。
ホストの CA の移行の表示 (View hosts migrate CA)	2048 ビット以上のキー強度の NetBackup ルート CA にまだ移行されていない (保留中) NetBackup ホストを表示します。

外部証明書

外部証明書の権限により、ユーザーは、外部認証局からの証明書を NetBackup がどのように使用するかを管理できます。外部証明書の設定は、NetBackup API からのみ利用可能です。NetBackup セキュリティ API を参照してください。

メモ: NetBackup Web UI で外部証明書を表示するには、ユーザーは [NetBackup 証明書 (NetBackup 証明書)]、[表示 (View)] を持っている必要があります。

表 6-39 外部証明書に対する RBAC 権限

操作	説明
作成 (Create)	外部証明書の詳細をホストのホスト ID に関連付けます。
削除 (Delete)	外部証明書に対するホスト ID の関連付けを削除します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。
証明書のリセット (Reset certificate)	サブジェクト以外の外部証明書の値をリセットします。証明書の登録時に証明書のフィールドが再入力されます。

NetBackup 証明書

NetBackup 証明書の権限によって、ユーザーは NetBackup セキュリティ証明書を表示および管理できます。NetBackup トークンの権限は個別であることに注意してください。

表 6-40 NetBackup 証明書

操作	説明
表示 (View)	NetBackup セキュリティ証明書の詳細を表示し、NetBackup ホストが使用するすべての外部証明書を表示します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。
NetBackup セキュリティ証明書の関連付けを解除 (Dissociate NetBackup security certificates)	現在関連付けられている証明書から NetBackup ホスト名の関連付けを解除します。
無効化 (Revoke)	NetBackup セキュリティ証明書を無効にします。

NetBackup セキュリティトークン

NetBackup セキュリティトークンの権限により、ユーザーは NetBackup セキュリティトークンを表示および管理できます。NetBackup 証明書の権限は個別であることに注意してください。

表 6-41 NetBackup セキュリティトークンに対する RBAC 権限

操作	説明
表示 (View)	すべての NetBackup セキュリティトークンを表示します。
作成 (Create)	NetBackup セキュリティトークンを作成します。
削除 (Delete)	NetBackup セキュリティトークンを削除するか、期限切れのトークンをクリーンアップします。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」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

これらの権限により、ユーザーは NetBackup のディザスタリカバリ用のパスフレーズを表示および管理できます。パスフレーズの制約は、NetBackup API または CLI を使用して変更できます。

表 6-42 ディザスタリカバリのパスフレーズに対する RBAC 権限

操作	説明
表示 (View)	NetBackup Web UI に[ディザスタリカバリ (Disaster recovery)] タブを表示します。ディザスタリカバリのパスフレーズが設定されているかどうかを表示します。
作成 (Create)	ディザスタリカバリのパスフレーズを追加または変更します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

ID プロバイダと SAML 証明書の構成

これらの権限は、NetBackup 認証サービス (VxAT) ドメインと、ID プロバイダの構成 (SAML サーバーを使用した SSO (シングルサインオン) 認証) に対するアクセス制御を提供します。

メモ: VxAT および ID プロバイダの構成は、コマンドラインまたは API を使用して行う必要があります。現在、Web UI ではこの構成を行えません。

表 6-43 ID プロバイダの構成

操作	説明
表示 (View)	構成済みの VxAT ドメインを表示し、検証します。 構成されているすべての SAML ID プロバイダ設定を表示します。
作成 (Create)	VxAT を介してドメインを NetBackup に追加します。 SAML ID プロバイダの構成を追加します。
更新 (Update)	SAML ID プロバイダの構成を更新します。
削除 (Delete)	構成済みの VxAT ドメインを削除します。 SAML ID プロバイダの構成を削除します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

KMS (キーマネージメントサービス)

KMS 権限によって、ユーザーは NetBackup KMS と外部 KMS を表示、管理したり、ストレージサーバーまたはディスクボリュームの暗号化を構成したりできます。これらの操作は、NetBackup API からのみ利用可能です。

表 6-44 キーマネージメントサービス

操作	説明
表示 (View)	KMS 構成の詳細を表示します。
作成 (Create)	NetBackup で KMS 構成を追加します。
更新 (Update)	NetBackup で KMS 構成を更新します。
削除 (Delete)	NetBackup で KMS 構成を削除します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。
キーを作成 (Create key)	キー管理サーバーでキーを作成します。
KMS の詳細の検証 (Validate KMS details)	構成内のサーバーの詳細とクレデンシヤルに基づいて、NetBackup がキー管理サーバーと通信できることを確認します。
キーの詳細を表示 (View key details)	キーの詳細を表示します。

パスワードの制約

これらの権限により、ユーザーはディザスタリカバリパスワードの制約を変更できます。この操作は、NetBackup API および CLI (`nbseccmd -setpassphraseconstraints`) からのみ利用可能です。

表 6-45 パスワードの制約

操作	説明
更新 (Update)	ディザスタリカバリパスワードの制約を更新します。 ディザスタリカバリパスワードは、[設定 (Settings)]>[グローバルセキュリティ設定 (Global security settings)]>[ディザスタリカバリ (Disaster recovery)]の設定で構成されています。

グローバルセキュリティ設定

これらの権限は、NetBackup プライマリサーバーの [グローバルセキュリティ (Global security)] 設定に対するアクセス制御を管理します。

メモ: 信頼できるプライマリサーバーの権限は、[NetBackup の管理 (NetBackup management)]、[信頼できるプライマリサーバー (Trusted primary server)] の RBAC 設定にあります。

表 6-46 セキュリティプロパティ

操作	説明	その他の必要な操作
表示 (View)	NetBackup プライマリサーバーのセキュリティ設定を表示します。 メモ: この権限のみを持つユーザーは、Web UI にサインインできません。	
更新 (Update)	NetBackup プライマリサーバーのセキュリティ設定を管理します。これらの設定は、8.0 以前のホストとの通信、ホスト ID とホスト名の自動マッピング、証明書配備のセキュリティレベルに影響します。 p.141 の「安全な通信のための認証局」を参照してください。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「アクセスの管理」を参照してください。	表示 (View)

信頼バージョン

これらの権限により、ユーザーはプライマリサーバーの信頼バージョンとその詳細を表示できます。信頼バージョンは、ホストが信頼する必要があるドメインの認証局 (CA) を定義します。これらの操作は、NetBackup API からのみ利用可能です。

表 6-47 信頼バージョンに対する RBAC 権限

操作	説明
表示 (View)	トラストストアに含める必要がある CA を含む、信頼バージョンの詳細を表示します。
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

API キー

これらの権限により、ユーザーは NetBackup API キーを表示および管理できます。

表 6-48 API キーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	API キーを表示します。	
作成 (Create)	API キーを作成します。	表示 (View)
更新 (Update)	有効な API キーの有効期限を変更します。	表示 (View)
削除 (Delete)	API キーを削除します。	表示 (View)

ユーザー証明書

これらの権限により、ユーザーは、ユーザー証明書またはスマートカードでの認証を NetBackup に許可する構成を表示、管理できます。注意: スマートカード認証を構成して有効にするには、プライマリサーバーに対して認証ドメインを構成する必要があります。

表 6-49 ユーザー証明書

操作	説明	その他の必要な操作
表示 (View)	スマートカード認証の設定を表示します。	[セキュリティ (Security)]、[グローバルセキュリティ設定 (Global Security Settings)]、[更新 (Update)]

操作	説明	その他の必要な操作
作成 (Create)	外部 CA 証明書をスマートカード認証のトラストストアにアップロードします。	[セキュリティ (Security)]、[グローバルセキュリティ設定 (Global Security Settings)]、[更新 (Update)]
削除 (Delete)	外部 CA 証明書をスマートカード認証のトラストストアから削除します。	[セキュリティ (Security)]、[グローバルセキュリティ設定 (Global Security Settings)]、[更新 (Update)]
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

ユーザーセッションと認証

ユーザーセッションと認証の権限により、ユーザーは次の情報を表示および管理できません。

p.85 の「[API キー](#)」を参照してください。

p.86 の「[ユーザー証明書](#)」を参照してください。

p.86 の「[ユーザーセッション](#)」を参照してください。

API キー

これらの権限により、ユーザーは **NetBackup API キー** を表示および管理できます。

NetBackup で認証済みのユーザーは、**Web UI** を使用して自身の **API キー** を表示および管理できます。ユーザーが役割に割り当てられていない場合、ユーザーは **NetBackup API** を使用して **API** を管理できます。

表 6-50 **API キーに対する RBAC 権限**

操作	説明	その他の必要な操作
表示 (View)	API キーを表示します。	
作成 (Create)	API キーを作成します。	表示 (View)
更新 (Update)	有効な API キーの有効期限を変更します。	表示 (View)
削除 (Delete)	API キーを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

ユーザー証明書

これらの権限により、ユーザーは、ユーザー証明書またはスマートカードでの認証を NetBackup に許可する構成を表示、管理できます。注意: スマートカード認証を構成して有効にするには、プライマリサーバーに対して認証ドメインを構成する必要があります。

表 6-51 ユーザー証明書

操作	説明	その他の必要な操作
表示 (View)	スマートカード認証の設定を表示します。	[セキュリティ (Security)]、[グローバルセキュリティ設定 (Global Security Settings)]、[更新 (Update)]
作成 (Create)	外部 CA 証明書をスマートカード認証のトラストストアにアップロードします。	[セキュリティ (Security)]、[グローバルセキュリティ設定 (Global Security Settings)]、[更新 (Update)]
削除 (Delete)	外部 CA 証明書をスマートカード認証のトラストストアから削除します。	[セキュリティ (Security)]、[グローバルセキュリティ設定 (Global Security Settings)]、[更新 (Update)]
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	

ユーザーセッション

メモ: ユーザーセッションのユーザーアカウント設定を表示するには、ホストの権限も必要です。p.62 の「[NetBackup ホスト](#)」を参照してください。

これらの権限により、ユーザーはユーザーセッションとユーザーアカウントの設定を表示および管理できます。

表 6-52 ユーザーセッションに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	有効なユーザーセッションを表示します。	
更新 (Update)	ユーザーアカウントの設定でサインインパナーの構成を有効化、更新、または無効化します。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[表示 (View)]

操作	説明	その他の必要な操作
	<p>[ユーザーアカウント設定 (User account settings)]で次の設定を有効、更新、または無効にします。</p> <ul style="list-style-type: none"> ■ 最大並列セッション数 ■ ユーザーアカウントのロックアウト ■ サインインバナーの構成 	<p>更新 (Update)</p> <p>[NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[表示 (View)]</p> <p>[NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[作成 (Create)]</p> <p>[NetBackup の管理 (NetBackup management)]、[NetBackup ホスト (NetBackup hosts)]、[更新 (Update)]</p>
ユーザーセッションを閉じる (Close user session)	選択したユーザーセッションを閉じます。	表示 (View)
すべてのユーザーセッションを閉じる (Close all user sessions)	すべてのユーザーセッションを閉じます。この権限がない場合、管理者は選択したユーザーセッションのみを閉じられます。	表示 (View)
ロック解除 (Unlock)	NetBackup からロックアウトされているアカウントを持つユーザーのロックを解除します。	ロック済みを表示 (View locked)
ロック済みを表示 (View locked)	NetBackup からロックアウトされているすべてのユーザーを表示します。	
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

[グローバル (Global)]> [ストレージ (Storage)]

ストレージの権限には、次のカテゴリがあります。

- p.88 の「[クラウドストレージ](#)」を参照してください。
- p.88 の「[ディスクプール](#)」を参照してください。
- p.89 の「[ストレージの Key Management Service](#)」を参照してください。
- p.89 の「[ストレージサーバー](#)」を参照してください。
- p.91 の「[ストレージユニット](#)」を参照してください。
- p.92 の「[レプリケーション対応のターゲットストレージサーバー](#)」を参照してください。

ストレージの権限により、ユーザーはバックアップ、レプリケーション、長期保持のためのストレージを管理できます。

クラウドストレージ

これらの権限によりユーザーは、NetBackup がサポートするクラウドの「Storage as a Service」(STaaS) ベンダーの構成を表示できます。

表 6-53 クラウドストレージに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	NetBackup がサポートするクラウドストレージベンダーの構成を表示します。	
アクセスの管理 (Manage access)	API のみ。p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

ディスクプール

これらの権限により、ユーザーは、AdvancedDisk、クラウド、MSDP、OpenStorage、およびレプリケーションで使用するディスクプールを表示および管理できます。

表 6-54 ディスクプールに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	ディスクプールを表示します。	[ストレージ (Storage)]、[ストレージサーバー (Storage servers)]、[表示 (View)] [ストレージ (Storage)]、[レプリケーション対応のターゲットストレージサーバー (Replication-capable target storage servers)]、[表示 (View)]
作成 (Create)	ディスクプールを作成します。	表示 (View) [NetBackup の管理 (NetBackup management)]、[サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]、[表示 (View)] [ストレージ (Storage)]、[レプリケーション対応のターゲットストレージサーバー (Replication-capable target storage servers)]、[表示 (View)]

操作	説明	その他の必要な操作
更新 (Update)	ディスクプールの構成をインベントリし、更新します。	表示 (View) [サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]、[表示 (View)] [ストレージ (Storage)]、[レプリケーション対応のターゲットストレージサーバー (Replication-capable target storage servers)]、[表示 (View)]
削除 (Delete)	ディスクプールを削除します。	表示 (View)
アクセスの管理 (Manage access)	API のみ。p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

ストレージの Key Management Service

ストレージの Key Management Service (KMS) の権限により、ユーザーは、NetBackup KMS または外部 KMS を使用して、ストレージサーバーまたはディスクボリュームを暗号化できます。これらの操作は、NetBackup API からのみ利用可能です。

KMS に対する権限は[セキュリティ (Security)]で管理されます。p.82 の「[KMS \(キーマネジメントサービス\)](#)」を参照してください。

表 6-55 ストレージの Key Management Service に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	NetBackup で利用可能な Key Management Service を表示します。	
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

ストレージサーバー

メモ: NetBackup 8.3、9.0、9.1 では、ユニバーサル共有はメディアサーバー重複排除プール (MSDP) でのみサポートされます。

ストレージサーバーの権限により、ユーザーはストレージサーバーとユニバーサル共有を表示および管理できます。

ユニバーサル共有バックアップのインスタントアクセスマウントを表示および作成する権限は、[RBAC]>[資産 (Assets)]>[ユニバーサル共有 (Universal shares)]にあります。p.93 の「資産」を参照してください。

表 6-56 ストレージサーバーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	ストレージサーバーまたはユニバーサル共有を表示します。	クラウドストレージサーバーを表示するには: [NetBackup の管理 (NetBackup management)]、[クラウドプロバイダ (Cloud providers)]、[表示 (View)]
作成 (Create)	ストレージサーバーまたはユニバーサル共有を追加します。	表示 (View) [NetBackup の管理 (NetBackup management)]、[メディアサーバー (Media server)]、[表示 (View)] ストレージサーバーを暗号化する場合: [セキュリティ (Security)]、[キーマネージメントサービス (Key Management Services)]、[表示 (View)]
更新 (Update)	ストレージサーバーまたはユニバーサル共有の設定を編集します。	表示 (View)
削除 (Delete)	ストレージサーバーまたはユニバーサル共有を削除します。	表示 (View)
アクセスの管理 (Manage access)	API のみ。p.110 の「アクセスの管理」を参照してください。	表示 (View)

ディスクボリューム

これらの権限により、ユーザーはストレージサーバーのディスクボリュームを表示および管理できます。

表 6-57 ディスクボリュームに対する権限

操作	説明	その他の必要な操作
表示 (View)	ストレージサーバーのディスクボリュームを表示します。	[ストレージ (Storage)]、[ストレージサーバー (Storage servers)]、[表示 (View)] [ストレージ (Storage)]、[ディスクプール (Disk pools)]、[表示 (View)]
作成 (Create)	ストレージサーバーのディスクボリュームを作成します。	表示 (View) ディスクボリュームを暗号化する場合は、次の権限も必要です。 [セキュリティ (Security)]、[キーマネージメントサービス (Key Management Services)]、[表示 (View)]
更新 (Update)	ストレージサーバーのディスクボリュームの属性を変更します。	表示 (View)
アクセスの管理 (Manage access)	APIのみ。p.110の「 アクセスの管理 」を参照してください。	表示 (View)

ストレージユニット

これらの権限により、ユーザーはストレージユニットを表示および管理できます。

表 6-58 ストレージユニット

操作	説明	その他の必要な操作
表示 (View)	ストレージユニットを表示します。	表示 (View) [ストレージ (Storage)]、[ディスクプール (Disk pools)]、[表示 (View)] [ストレージ (Storage)]、[ストレージサーバー (Storage servers)]、[表示 (View)]
作成 (Create)	ストレージユニットを作成します。	表示 (View) [ストレージ (Storage)]、[ディスクプール (Disk pools)]、[表示 (View)]
更新 (Update)	ストレージユニットを変更します。	表示 (View) [ストレージ (Storage)]、[ディスクプール (Disk pools)]、[表示 (View)]

操作	説明	その他の必要な操作
削除 (Delete)	ストレージユニットを削除します。	表示 (View)
アクセスの管理 (Manage access)	API のみ。p.110 の「 アクセスの管理 」を参照してください。	

テープメディア

これらの権限により、ユーザーはテープメディアサーバーグループおよびテープメディアボリュームプールへのアクセスを表示および管理できます。

表 6-59 テープメディアサーバーグループ

操作	説明
表示 (View)	テープメディアサーバーグループを表示します。
アクセスの管理 (Manage access)	API のみ。p.110 の「 アクセスの管理 」を参照してください。

表 6-60 テープメディアボリュームプール

操作	説明
表示 (View)	テープメディアボリュームプールを表示します。
アクセスの管理 (Manage access)	API のみ。p.110 の「 アクセスの管理 」を参照してください。

レプリケーション対応のターゲットストレージサーバー

これらの権限により、ユーザーは MSDP のレプリケーション関係を表示および管理できます。

表 6-61 レプリケーション対応のターゲットストレージサーバーに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	レプリケーションに利用可能なターゲットストレージサーバーを表示します。	[サーバー (Servers)]、[信頼できるプライマリサーバー (Trusted primary servers)]、[表示 (View)]

操作	説明	その他の必要な操作
アクセスの管理 (Manage access)	API のみ。p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

資産

資産に対する権限により、管理者は次の操作を実行できます。

- ファイルシステム資産のリストアを実行する。
p.106 の「[Windows および標準のクライアント形式](#)」を参照してください。
- その他の資産タイプを表示または管理する。
p.93 の「[AHV 資産](#)」を参照してください。
p.95 の「[クラウド資産](#)」を参照してください。
p.97 の「[Kubernetes 資産](#)」を参照してください。
p.98 の「[Microsoft SQL Server 資産](#)」を参照してください。
p.100 の「[OpenStack サーバー](#)」を参照してください。
p.100 の「[RHV 資産](#)」を参照してください。
p.102 の「[ユニバーサル共有](#)」を参照してください。
p.103 の「[VMware 資産](#)」を参照してください。

AHV 資産

- p.93 の「[AHV クラスタ、VM、ストレージコンテナ](#)」を参照してください。
p.95 の「[AHV インテリジェント VM グループ](#)」を参照してください。

AHV クラスタ、VM、ストレージコンテナ

メモ: 検出、バックアップ、リストアを実行するには、AHV クラスタに対して有効なクレデンシャルが存在している必要があります。

AHV 資産の権限により、ユーザーは AHV 資産を表示、保護、リストアできます。ユーザーは、AHV バックアップからファイルとフォルダをリストアして、ファイルシステムにリストアすることもできます。

表 6-62 AHV クラスタ、VM、ストレージコンテナの権限

操作	説明	その他の必要な操作
表示 (View)	構成済みの AHV クラスタと AHV 資産を表示します。	

操作	説明	その他の必要な操作
作成 (Create)	AHV クラスタを追加します。	表示 (View)
更新 (Update)	資産の詳細を更新します。VM インテリジェントグループの内容を更新します。クレデンシャルの検証 (Validate credentials)	表示 (View)
削除 (Delete)	AHV クラスタを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
保護 (Protect)	VM を保護計画に追加するか、保護計画から削除します。	表示 (View)
リストアターゲットの表示 (View restore targets)	資産のリストア先として利用可能な宛先を表示します。	表示 (View)
個別リストア (Granular restore)	AHV 資産から個々のファイルまたはフォルダをリストアします。 この権限は、ソース VM に必要です。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[NetBackup 管理の表示 (View NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)]
リストア (Restore)	元の場所または代替の場所にリストアします。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)] ターゲットの場所での操作: リストアターゲットの表示 (View restore targets) [NetBackup の管理 (NetBackup management)]、[アクセスホスト (Access hosts)]、[表示 (View)]
リストアで上書きを許可する (Allow restore to overwrite)	資産が存在する場合は上書きします。	表示 (View) リストア (Restore)

AHV インテリジェント VM グループ

これらの権限により、ユーザーは AHV インテリジェント VM グループを表示および管理できます。

メモ: インテリジェント VM グループを作成するには、クラスタで表示権限が必要です。

表 6-63 インテリジェント VM グループの権限

操作	説明	その他の必要な操作
表示 (View)	VM インテリジェントグループを表示します。	
作成 (Create)	VM インテリジェントグループを追加します。	表示 (View) VM グループに対応する AHV クラスタでの操作: 表示 (View)
更新 (Update)	VM インテリジェントグループを更新します。	表示 (View) VM グループに対応する AHV クラスタでの操作: 表示 (View)
削除 (Delete)	VM インテリジェントグループを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	AHV インテリジェント VM グループでの操作: 表示 (View)
保護 (Protect)	VM インテリジェントグループを保護計画に追加または保護計画から削除します。	AHV インテリジェント VM グループでの操作: 表示 (View) VM グループに対応する AHV クラスタでの操作: 保護 (Protect)

クラウド資産

クラウド資産の権限により、ユーザーは CloudPoint を使用してクラウド内の作業負荷資産を表示、保護、リストアできます。

表 6-64 クラウド資産の権限

操作	説明	その他の必要な操作
表示 (View)	クラウド資産を表示します。	

操作	説明	その他の必要な操作
作成 (Create)	クラウドインテリジェントグループを追加します。	表示 (View)
更新 (Update)	クラウドインテリジェントグループの内容を更新します。	表示 (View)
削除 (Delete)	クラウドインテリジェントグループを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
個別リストア (Granular Restore)	クラウド資産から個々のファイルまたはフォルダをリストアします。	表示 (View)
保護 (Protect)	保護計画にクラウド資産を追加します。	表示 (View)
代替の場所にリストアする (Restore to alternate location)	代替場所にリストアします。 この権限は、ソース資産に必要です。	表示 (View) ターゲット資産に対して: リストアで上書きを許可する (Allow restore to overwrite) ターゲットの場所での操作: リストアターゲットの表示 (View restore targets)
リストアターゲットの表示 (View restore targets)	資産のリストア先として利用可能な宛先を表示します。 この権限は、ターゲット資産に必要です。	表示 (View)
元の場所にリストアする (Restore to original location)	クラウド資産を元の場所にリストアします。	表示 (View) ターゲットの場所での操作: リストアターゲットの表示 (View restore targets) 元の VM が存在する場合: リストアで上書きを許可する (Allow restore to overwrite)
リストアで上書きを許可する (Allow restore to overwrite)	資産が存在する場合は上書きします。	表示 (View) ターゲットの場所での操作: リストアターゲットの表示 (View restore targets)
構成の更新 (Update configuraion)	仮想マシンに対して接続または切断します。クラウド構成を追加、更新、または削除します。VM のクレデンシャルを編集します。CloudPoint からトークンを生成し、ホストのエージェントとの通信を確立します。	表示 (View)

Kubernetes 資産

Kubernetes 資産の権限により、ユーザーは Kubernetes 資産を表示、保護、リストアできます。

ジョブの権限については、次の点に注意してください。

- 特定の Kubernetes 資産に、1 つ以上のジョブ権限を付与できます。
- デフォルトの Kubernetes 管理者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。

表 6-65 Kubernetes 資産の権限

操作	説明	その他の必要な操作
表示 (View)	Kubernetes クラスタと名前空間を表示します。	
作成 (Create)	Kubernetes クラスタを追加します。クレデンシヤルを検証します。	表示 (View) [クレデンシヤル (Credentials)], [クレデンシヤルの管理 (Manage credentials)], [ビュー (View)] [クレデンシヤル (Credentials)], [クレデンシヤルの管理 (Manage credentials)], [クレデンシヤルの割り当て (Assign credentials)]
更新 (Update)	Kubernetes クラスタとそのクレデンシヤルを更新します。クレデンシヤルを検証します。	表示 (View) [クレデンシヤル (Credentials)], [クレデンシヤルの管理 (Manage credentials)], [ビュー (View)] [クレデンシヤル (Credentials)], [クレデンシヤルの管理 (Manage credentials)], [クレデンシヤルの割り当て (Assign credentials)]
削除 (Delete)	Kubernetes クラスタを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
検出 (Discover)	Kubernetes 資産を検出します。	表示 (View)
保護 (Protect)	Kubernetes 資産を保護計画に追加するか、保護計画から削除します。	表示 (View)

操作	説明	その他の必要な操作
リストア (Restore)	元の場所または代替の場所にリストアします。Kubernetes の代替の場所へのリストアは、バックアップイメージの名前空間から、同じクラスタまたは異なるクラスタ内の別の名前空間へのリストアを意味します。 メモ: リストアに異なるターゲットクラスタを選択する場合は、元のクラスタとターゲットクラスタで、Velero プラグインが使用するオブジェクトストレージが同じである必要があります。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)]
リストアターゲットの表示 (View restore targets)	資産のリストア先として利用可能な宛先を表示します。	表示 (View)
ジョブのキャンセル (Cancel jobs)	Kubernetes 資産のジョブをキャンセルします。	ジョブの表示 (View jobs)
ジョブの再起動 (Restart jobs)	Kubernetes 資産のジョブを再起動します。	ジョブの表示 (View jobs)
ジョブの表示 (View jobs)	Kubernetes 資産のジョブを表示します。	

Microsoft SQL Server 資産

Microsoft SQL Server 資産に対する権限により、ユーザーは NetBackup for SQL Server エージェントを使用して、SQL Server 資産の表示、保護、リストアを行えます。

メモ: 検出、バックアップおよびリストアを実行するには、可用性グループまたはインスタンスに対して有効なクレデンシャルが存在している必要があります。

表 6-66 SQL Server 資産の権限

操作	説明	その他の必要な操作
表示 (View)	可用性グループ、インスタンス、データベースを表示します。	
作成 (Create)	インスタンスを手動で追加します。	表示 (View)
更新 (Update)	資産の詳細を更新します。可用性レプリカまたはインスタンスのクレデンシャルを追加または更新します。	表示 (View)
削除 (Delete)	可用性レプリカまたはインスタンスを削除します。	表示 (View)

操作	説明	その他の必要な操作
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
代替の場所にリストアする (Restore to alternate location)	代替サーバーにデータベースをリストアします。この権限は、すべての SQL Server の「MOVE」操作に必要です。	表示 (View) リストア (Restore)
可用性グループの検出 (Discover availability groups)	可用性グループを手動で検出します。 検出を実行するには、有効なクレデンシヤルを可用性グループのレプリカのいずれかに追加する必要があります。	表示 (View)
データベースの検出 (Discover databases)	データベースを手動で検出します。 検出を実行するには、有効なクレデンシヤルをインスタンスに追加する必要があります。	表示 (View)
インスタントアクセス (Instant access)	インスタントアクセスデータベースを作成します。	表示 (View) リストア (Restore)
リストアで上書きを許可する (Allow restore to overwrite)	SQL Server データベースが存在する場合は上書きします。	表示 (View) リストア (Restore)
保護 (Protect)	SQL Server 資産を保護計画に追加するか、保護計画から削除します。	表示 (View)
リストア (Restore)	データベースを元の場所、別のデータベース、または別のインスタンスにリストアします。	表示 (View)
クレデンシヤルの検証 (Validate credentials)	インスタンスまたはレプリカにクレデンシヤルが追加 (割り当て) されている場合は、クレデンシヤルを検証します。 この権限は、資産に必要です。	資産には、次の権限が必要です。 表示 (View) 更新 (Update) クレデンシヤルには、次の権限が必要です。 [クレデンシヤル (Credentials)]、[表示 (View)] [クレデンシヤル (Credentials)]、[クレデンシヤルの割り当て (Assign credentials)]

OpenStack サーバー

OpenStack Horizon サーバーの権限により、ユーザーはサーバーを表示、追加、削除できます。

表 6-67 OpenStack サーバーの権限

操作	説明	その他の必要な操作
表示 (View)	OpenStack Horizon サーバーを表示します。また、管理者にクロス起動を URL に開くことを許可します。	
作成 (Create)	OpenStack Horizon サーバーを手動で追加します。	表示 (View)
更新 (Update)	TLS 設定に従って、OpenStack Horizon サーバーのポート (443/80) の詳細を更新します。	表示 (View)
削除 (Delete)	Horizon サーバーを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)

RHV 資産

RHV 資産の権限により、ユーザーは RHV 資産を表示、保護、リストアできます。

NetBackup 9.1 以降、次の更新が行われました。

- 特定の RHV 資産に、1 つ以上のジョブ権限を付与できます。
- デフォルトの RHV 管理者の役割の権限によって、ユーザーは RHV 資産のジョブを表示および管理できます。この役割には、資産のすべてのジョブを表示するグローバル権限は含まれなくなりました。

表 6-68 RHV 資産の権限

操作	説明	その他の必要な操作
表示 (View)	構成済みの RHV マネージャと RHV 資産を表示します。	
	VM インテリジェントグループを表示します。	VM グループに対応する RHV マネージャでの操作: 表示 (View)

操作	説明	その他の必要な操作
作成 (Create)	RHV マネージャを追加します。	表示 (View)
	VM インテリジェントグループを追加します。	表示 (View) VMグループに対応するRHV マネージャでの操作: 表示 (View)
更新 (Update)	資産の詳細を更新します。VM インテリジェントグループの内容を更新します。クレンジャルを検証します。	表示 (View)
	VM インテリジェントグループを更新します。	表示 (View) VMグループに対応するRHV マネージャでの操作: 表示 (View)
削除 (Delete)	RHV マネージャを削除します。	表示 (View)
	VM インテリジェントグループを削除します。	表示 (View) VMグループに対応するRHV マネージャでの操作: 表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
保護 (Protect)	VMを保護計画に追加するか、保護計画から削除します。	表示 (View)
	VM インテリジェントグループを保護計画に追加または保護計画から削除します。	VMグループに対応するRHV マネージャでの操作: 表示 (View) 保護 (Protect)
リストターゲットの表示 (View restore targets)	資産のリストア先として利用可能な宛先を表示します。	表示 (View)

操作	説明	その他の必要な操作
リストア (Restore)	元の場所または代替の場所にリストアします。	表示 (View) [NetBackup の管理 (NetBackup management)], [NetBackup のバックアップイメージ (NetBackup backup images)], [表示 (View)] ターゲットの場所での操作: リストアターゲットの表示 (View restore targets) [NetBackup の管理 (NetBackup management)], [アクセスホスト (Access hosts)], [表示 (View)]
リストアで上書きを許可する (Allow restore to overwrite)	資産が存在する場合は上書きします。	表示 (View) リストア (Restore)
ジョブのキャンセル (Cancel jobs)	RHV 資産のジョブをキャンセルします。	ジョブの表示 (View jobs)
ジョブの再起動 (Restart jobs)	RHV 資産のジョブを再起動します。	ジョブの表示 (View jobs)
ジョブの表示 (View jobs)	RHV 資産のジョブを表示します。	

ユニバーサル共有

メモ: NetBackup 8.3、9.0、9.1 では、ユニバーサル共有バックアップからリストアする機能は、NetBackup CLI または [バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)] インターフェースからのみ利用可能です。インスタントアクセスリカバリは、NetBackup API を介してのみ利用可能です。

ユニバーサル共有資産の権限により、ユーザーはユニバーサル共有の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表示および作成できます。ユニバーサル共有を作成および管理する権限は、[グローバル (Global)], [ストレージ (Storage)], [ストレージサーバー (Storage server)] に移動した先にあります。

p.87 の「[\[グローバル \(Global\)\]](#)>[\[ストレージ \(Storage\)\]](#)」を参照してください。

表 6-69 ユニバーサル共有の権限

操作	説明
インスタントアクセス (Instant access)	<p>ユニバーサル共有上のインスタントアクセスマウントポイントを表示および作成します。ユニバーサル共有からリストアします。</p> <p>注意: 役割を作成するときに、ユニバーサル共有資産に対するアクセス権をすべておよび今後のユニバーサル共有資産に適用するかどうかを選択できます。このオプションを有効にすると、役割にはすべてのマウントポイントへのアクセス権が付与されます。個々のマウントポイントにはアクセス権を付与できません。</p> <p>この権限を持つユーザーは、ユニバーサル共有に関連付けられたストレージサーバーも表示できます。</p>
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。

VMware 資産

VMware 資産の権限により、ユーザーは VMware 資産を表示、保護、リストアできます。

NetBackup 9.1 以降、次の更新が行われました。

- 特定の VMware 資産に、1 つ以上のジョブ権限を付与できます。
- デフォルトの VMware 管理者の役割の権限によって、ユーザーは VMware 資産のジョブを表示および管理できます。この役割には、資産のすべてのジョブを表示するグローバル権限は含まれなくなりました。

表 6-70 VMware 資産に対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	VM、vCenter Server、ESX ホストを表示します。	
	VM インテリジェントグループを表示します。	VM グループに対応する vCenter での操作: 表示 (View)
作成 (Create)	ESX ホストと vCenter ホストを追加します。クレンジンシャルを検証します。	表示 (View)
	VM インテリジェントグループを追加します。	表示 (View) VM グループに対応する vCenter での操作: 表示 (View)

操作	説明	その他の必要な操作
更新 (Update)	ESX ホストまたは vCenter ホストと、それらのクレデンシヤルを更新します。クレデンシヤルを検証します。	表示 (View)
	VM インテリジェントグループを更新します。	表示 (View) VM グループに対応する vCenter での操作: 表示 (View)
削除 (Delete)	ESX ホストまたは vCenter ホストを削除します。	表示 (View)
	VM インテリジェントグループを削除します。	表示 (View) VM グループに対応する vCenter での操作: 表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
保護 (Protect)	VMware 資産を保護計画に追加するか、保護計画から削除します。	表示 (View)
	VMware インテリジェントグループを保護計画に追加または保護計画から削除します。	VM グループに対応する vCenter での操作: 表示 (View) 保護 (Protect)
リストアターゲットの表示 (View restore targets)	資産のリストア先として利用可能な宛先を表示します。	表示 (View)
クラウドへのリストア (Restore to cloud)	クラウドに VM をリストアします。	表示 (View)
個別リストア (Granular Restore)	VM から個々のファイルまたはフォルダをリストアします。 この権限は、ソースおよびターゲット VM に必要です。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)] [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[内容の表示 (View contents)]

操作	説明	その他の必要な操作
インスタントアクセス - ファイルのダウンロード (Instant access - Download files)	インスタントアクセステクノロジーを使用して個々のファイルをダウンロードします。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)]
インスタントアクセス - ファイルのリストア (Instant access - Restore files)	インスタントアクセステクノロジーを使用して個々のファイルをリストアします。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)] [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[内容の表示 (View contents)]
インスタントアクセス (Instant access)	インスタントアクセス VM を作成します。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)]
リストア (Restore)	元の場所または代替の場所にリストアします。	表示 (View) [NetBackup の管理 (NetBackup management)]、[NetBackup のバックアップイメージ (NetBackup backup images)]、[表示 (View)] [NetBackup の管理 (NetBackup management)]、[アクセスホスト (Access hosts)]、[表示 (View)] ターゲットの場所での操作: リストアターゲットの表示 (View restore targets)
リストアで上書きを許可する (Allow restore to overwrite)	リストアによる既存の資産の上書きを許可します。この権限を持たないユーザーは既存の資産を別の場所にリストアする必要があります。	表示 (View) リストア (Restore)
ジョブのキャンセル (Cancel jobs)	VMware 資産のジョブをキャンセルします。	ジョブの表示 (View jobs)
ジョブの再起動 (Restart jobs)	VMware 資産のジョブを再起動します。	ジョブの表示 (View jobs)

操作	説明	その他の必要な操作
ジョブの表示 (View jobs)	VMware 資産のジョブを表示します。	

Windows および標準のクライアント形式

NetBackup 9.1 では、管理者は Windows または Standard ポリシー形式で実行されたバックアップからリストアできます。これらの権限により、管理者は AHV バックアップからファイルとフォルダをリストアすることもできます。

これらの権限は RBAC 管理者の役割に含まれますが、他のデフォルトの RBAC の役割には含まれません。ファイルシステム権限は、ファイルシステムバックアップのサーバー主導リストアを実行する管理者を対象としています。管理者以外のユーザーは対象ではありません。

メモ: [ファイルシステムのリストア (Restore file-system)] 操作を使用すると、MS-Windows または Standard ポリシーから任意の NetBackup クライアントにイメージをリストアできます。

表 6-71 すべての資産とファイルシステム資産に対する RBAC 権限

操作	説明	その他の必要な操作
アクセスの管理	p.110 の「 アクセスの管理 」を参照してください。	
クライアントを使用したファイルのリストア	<p>ファイルまたはフォルダを NetBackup クライアントにリストアします。ユーザーは次の操作を実行できます。</p> <ul style="list-style-type: none"> ■ 任意の NetBackup クライアントからリダイレクト、またはクライアントにリダイレクトする。 ■ 別のパスにファイルをリダイレクトする。 	<p>ファイルシステムバックアップのリストア</p> <p>AHV ファイルとフォルダのリストアの場合、ソース資産で次の操作を実行できます。</p> <p>ファイルとフォルダの上書き</p> <p>[資産 (Assets)]>[AHV]>[AHV クラスタ (AHV clusters)]、[VM]、および[ストレージコンテナ (storage containers)]>[表示 (View)]</p> <p>[資産 (Assets)]>[AHV]>[AHV クラスタ (AHV clusters)]、[VM]、および[ストレージコンテナ (storage containers)]>[個別リストア (Granular restore)]</p>
ファイルとフォルダの上書き	NetBackup クライアントを使用するリストアの場合、リストアで既存のファイルまたはフォルダを上書きできます。	<p>ファイルシステムバックアップのリストア</p> <p>クライアントを使用したファイルのリストア</p>

操作	説明	その他の必要な操作
ファイルシステムバックアップのリストア	MS-Windows または Standard ポリシー形式で実行されたバックアップをリカバリします。	クライアントを使用したファイルのリストア p.107 の「 ファイルシステムのバックアップに必要な追加の操作 」を参照してください。

ファイルシステムのバックアップに必要な追加の操作

ファイルシステムのバックアップからリストアするには、次の追加の操作が必要です。

表 6-72 ファイルシステムのバックアップに必要な追加の操作

RBAC カテゴリ	サブカテゴリ	操作
[グローバル権限 (Global permissions)]、 [NetBackup の管理 (NetBackup management)]	アクセスホスト データの分類 NetBackup ホスト ジョブ	表示 (View)
	NetBackup バックアップイメージ	表示 (View) 内容の表示 (View contents)
[グローバル権限 (Global permissions)]、 [保護 (Protection)]	ポリシー	表示 (View)
[グローバル権限 (Global permissions)]、 [ストレージ (Storage)]	ストレージサーバー ディスクボリューム ストレージユニット	表示 (View)

保護計画

保護計画の権限により、ユーザーは保護計画を表示して管理し、保護計画に資産を追加できます。

資産の保護

保護計画に関連付けられているストレージを表示するには、ユーザーにそのストレージに対する表示権限が付与されている必要があります。この権限は、計画に資産をサブスクライブするときにストレージを表示するために必要です。p.87 の「[\[グローバル \(Global\)\] > \[ストレージ \(Storage\)\]](#)」を参照してください。

保護計画に資産を追加するか、すぐにバックアップするために[今すぐバックアップ (Backup now)]を選択するには、ユーザーは保護計画に対して表示およびサブスクリプション権限を持っている必要があります。さらに、ユーザーには資産を表示して保護するための権限が必要です。p.93 の「[資産](#)」を参照してください。

表 6-73 保護計画の権限

操作	説明	その他の必要な操作
表示 (View)	保護計画を表示します。	
作成 (Create)	保護計画を作成します。	表示 (View) RHV、VMware、Nutanix AHV の場合: [NetBackup の管理 (NetBackup management)]、[アクセスホスト (Access hosts)]、[表示 (View)]
更新 (Update)	保護計画を編集します。	表示 (View)
削除 (Delete)	保護計画を削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
属性の編集 (Edit attributes)	保護計画の属性を編集します。編集可能な属性は、作業負荷によって異なります。	表示 (View) サブスクリプション (Subscribe)
完全および増分スケジュールの編集 (Edit full and incremental schedules)	計画に資産をサブスクリプションするユーザーが、完全または増分スケジュールのバックアップ開始時間帯を編集できるようにします。 注意: 除外される日付は Web UI で編集できません。	表示 (View) サブスクリプション (Subscribe)
トランザクションログのスケジュールの編集 (Edit transaction log schedules)	計画に資産をサブスクリプションするユーザーが、トランザクションログスケジュールの特定の設定を編集できるようにします。バックアップ開始時間帯、反復 (頻度)、保持を編集できます。 注意: 除外される日付は Web UI で編集できません。	表示 (View) サブスクリプション (Subscribe)
サブスクリプション (Subscribe)	資産が計画にサブスクリプションされることを許可します。	表示 (View)

クレデンシャル

クレデンシャル権限により、ユーザーは **NetBackup** の資産やその他の機能のクレデンシャルを表示および管理できます。クレデンシャルを表示および管理するには、ユーザーに管理者の役割か、クレデンシャルの権限を持つ別の役割が必要です。ユーザーがクレデンシャルを作成すると、そのユーザーにはそのクレデンシャルに対する完全な権限が付与されます。

p.46 の「**デフォルトの RBAC の役割**」を参照してください。

p.232 の「**NetBackup でのクレデンシャルの追加**」を参照してください。

次の作業負荷のクレデンシャルを管理できます。

- クラウド (クラウドインスタンスの場合)
- Kubernetes
- Microsoft SQL Server
- Nutanix AHV

次のクレデンシャルも管理できます。

- 外部のキーマネージメントサービス (KMS)
- コールホームプロキシサーバー
コールホームプロキシサーバーについては、『[Veritas Usage Insights スタートガイド](#)』参照してください。

クレデンシャル管理の権限

表 6-74 クレデンシャルに対する RBAC 権限

操作	説明	その他の必要な操作
表示 (View)	[クレデンシャルの管理 (Credential management)]でクレデンシャルを表示します。 注意: 役割を作成するときに[新規と既存のクレデンシャルに権限を適用します (Apply permissions to new and existing credentials)]を選択すると、その役割にはすべてのクレデンシャルを表示する権限が付与されます。	
作成 (Create)	クレデンシャル管理にクレデンシャルを追加します。	表示 (View)
更新 (Update)	クレデンシャルの詳細を更新します。	表示 (View)

操作	説明	その他の必要な操作
削除 (Delete)	クレデンシャル管理からクレデンシャルを削除します。	表示 (View)
アクセスの管理 (Manage access)	p.110 の「 アクセスの管理 」を参照してください。	表示 (View)
クレデンシャルの割り当て (Assign credentials)	資産にクレデンシャルを割り当てられるようにします。この権限はクレデンシャルに必要です。	クレデンシャルには、次の権限も必要です。 表示 (View)
		資産には、次の権限が必要です。 表示 (View) 更新 (Update)
		クレデンシャルを検証するには、次の権限が必要です。 クレデンシャルの検証 (Validate credentials)

アクセスの管理

アクセスの管理権限により、ユーザーは特定の権限カテゴリの役割と役割の権限を管理できます。たとえば、ユーザーセッションに対して表示およびアクセスの管理を持つユーザーは、ユーザーセッションと認証の設定にアクセスできる役割と、それらの役割が持つ権限を表示して管理できます。ユーザーは、選択してユーザーセッションにアクセス権を付与する役割にも表示の権限を持っている必要があります。

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（「API のみ」と記載しています）。

以下の手順を参照してください。

- [「アクセス管理権限を持つ役割の追加」](#)
- [「役割を更新してアクセス管理権限を付与する」](#)

アクセス管理権限を持つ役割の追加

新しい役割にアクセス管理権限を付与するには

- 1 左側の [RBAC] ノードを選択し、[役割 (Roles)] タブをクリックします。
- 2 [追加 (Add)] をクリックし、追加する役割の種類を選択します。
- 3 役割名を入力します。

- 4 役割にアクセス管理権限を付与する各カテゴリに対して、[アクセスの管理 (Manage access)] 権限を選択します。

たとえば、VMware 資産やクレデンシャルへのアクセスを管理できる役割を作成できます。

Assign permissions [Learn about permissions](#)

Global **Assets** Protection plans Credentials

RHV assets All | None

<input type="checkbox"/> View	<input type="checkbox"/> Create	<input type="checkbox"/> Update	<input type="checkbox"/> Delete
<input type="checkbox"/> Manage access	<input type="checkbox"/> Protect	<input type="checkbox"/> View restore targets	<input type="checkbox"/> Restore
<input type="checkbox"/> Allow restore to overwrite	<input type="checkbox"/> Cancel Jobs	<input type="checkbox"/> Restart Jobs	<input type="checkbox"/> View Jobs

VMware assets All | None

<input checked="" type="checkbox"/> View	<input type="checkbox"/> Create	<input type="checkbox"/> Update	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Manage access	<input type="checkbox"/> Protect	<input type="checkbox"/> View restore targets	<input type="checkbox"/> Restore to cloud
<input type="checkbox"/> Granular restore	<input type="checkbox"/> Instant access - Download files	<input type="checkbox"/> Instant access - Restore files	<input type="checkbox"/> Instant access
<input type="checkbox"/> Restore	<input type="checkbox"/> Allow restore to overwrite	<input type="checkbox"/> Cancel Jobs	<input type="checkbox"/> Restart Jobs
<input type="checkbox"/> View Jobs			

Assign permissions [Learn about permissions](#) ✕

Global Assets Protection plans **Credentials**

Credential management All | None

<input checked="" type="checkbox"/> View	<input type="checkbox"/> Create	<input type="checkbox"/> Update	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Manage access	<input type="checkbox"/> Assign credentials		

- 5 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。

Assign permissions

Global Assets Protection plans Credentials

NetBackup management

Protection

Security

Access control

Users

View Manage access Assign to role

Roles

Create Update Delete Manage access

役割を更新してアクセス管理権限を付与する

役割を更新してアクセス管理権限を付与するには

- 1 左側の[RBAC]ノードを選択し、[役割 (Roles)]タブをクリックします。
- 2 編集する役割をクリックします。
- 3 役割にアクセス管理権限を付与する各カテゴリに対して、[アクセスの管理 (Manage access)]権限を選択します。

次の例では、役割管理者が[アクセスホスト (Access hosts)]に対して[表示 (View)]および[アクセスの管理 (Manage access)]権限を追加しています。

Edit global permissions

Access hosts All | None

View Create Update Delete

Manage access

Agentless hosts All | None

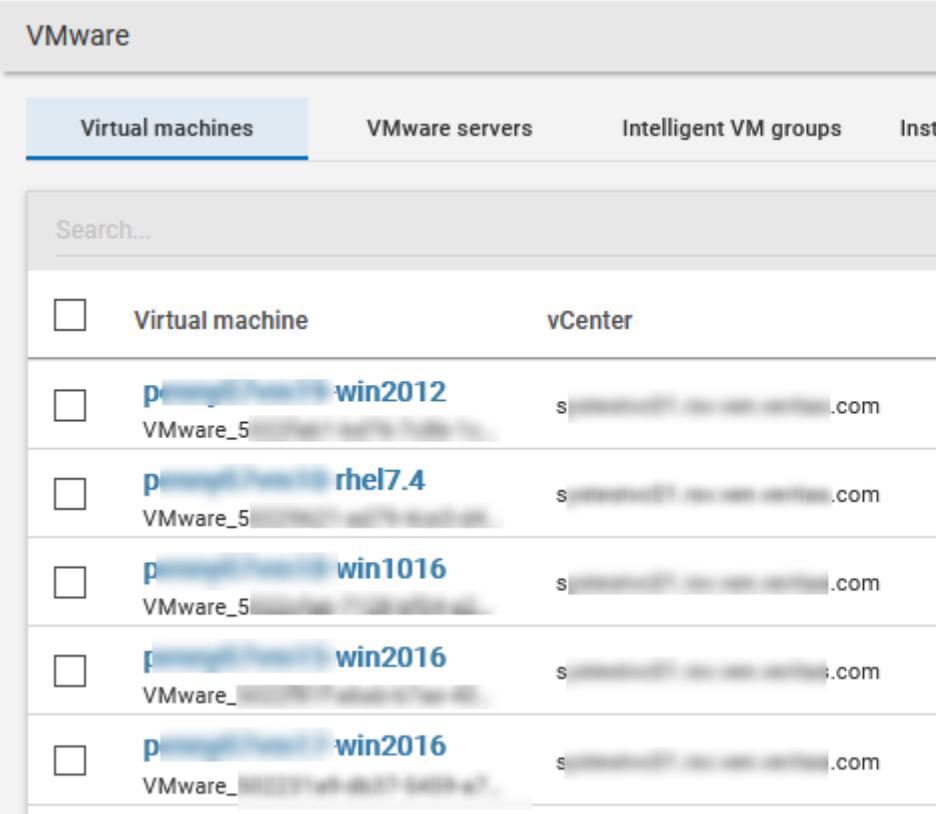
View Delete Manage access

Anomalies All | None

View Update Manage access

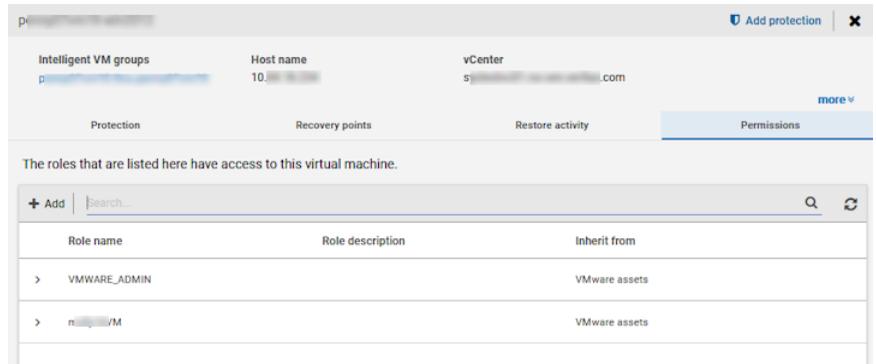
- 4 役割の作成後、資産、保護計画、クレデンシャルの権限は、Web UI の該当するノードで直接編集する必要があります。

たとえば、VMware の管理権限を役割に付与するには、[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。

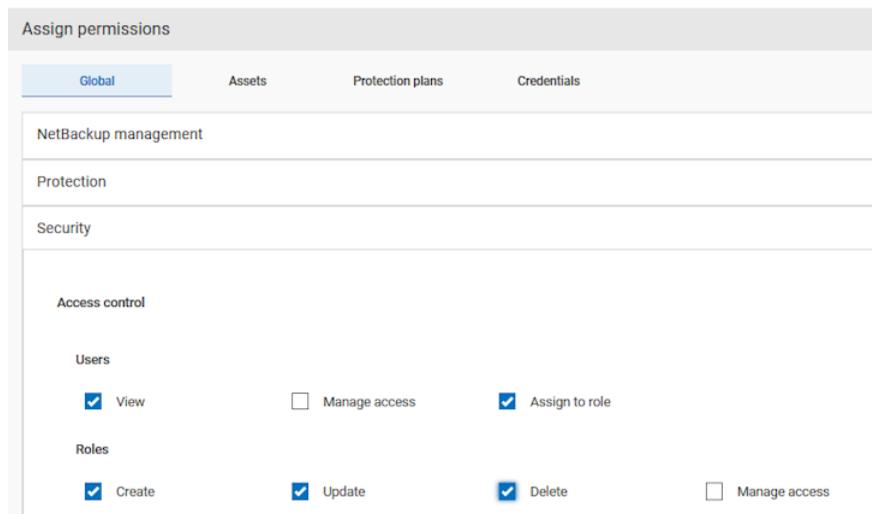


The screenshot displays the VMware management console. At the top, there are four tabs: "Virtual machines" (selected), "VMware servers", "Intelligent VM groups", and "Inst...". Below the tabs is a search bar labeled "Search...". The main content area shows a list of virtual machines with the following columns: a checkbox, the name of the virtual machine, and the vCenter it belongs to. The list contains five entries:

<input type="checkbox"/>	Virtual machine	vCenter
<input type="checkbox"/>	p-... win2012 VMware_5	s-... .com
<input type="checkbox"/>	p-... rhel7.4 VMware_5	s-... .com
<input type="checkbox"/>	p-... win1016 VMware_5	s-... .com
<input type="checkbox"/>	f-... win2016 VMware_...	s-... .com
<input type="checkbox"/>	p-... win2016 VMware_...	s-... .com



- 5 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。



Web UI の領域にアクセスできる役割の削除

Web UI の領域にアクセスできる役割を削除するには

- 1 左側の[RBAC]ノードを選択し、[役割 (Roles)]タブをクリックします。
- 2 編集する役割をクリックします。
- 3 アクセス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。

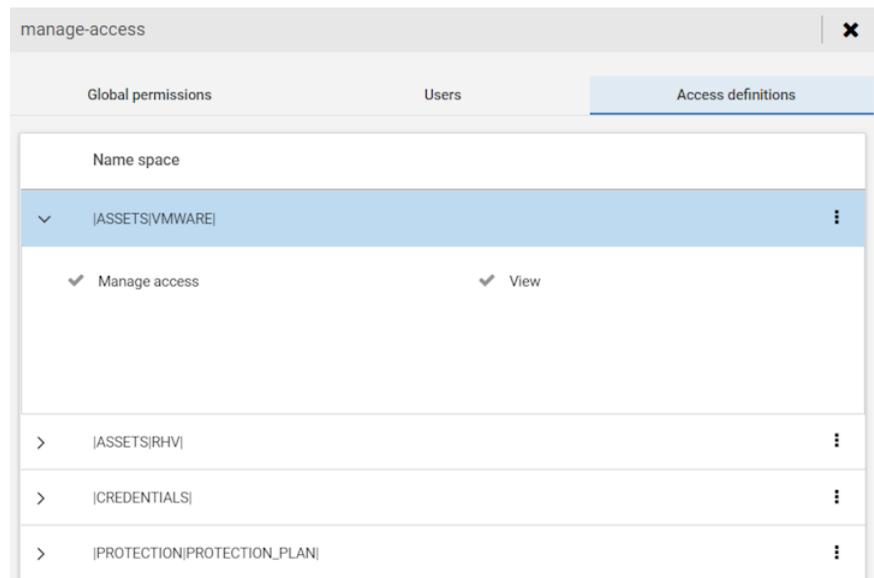
- 4 資産、保護計画、クレデンシャルの権限は、Web UI の該当するノードで直接編集する必要があります。
たとえば、VMware のアクセス管理権限を削除するには、[作業負荷 (Workloads)]、[VMware] の順に移動し、[VMware 設定 (VMware settings)]、[権限の管理 (Manage permissions)] の順に選択します。または、VM の詳細を開き、[権限 (Permissions)] タブをクリックします。
- 5 削除する役割を選択し、[処理 (Actions)]、[削除 (Remove)]、[削除 (Remove)] の順にクリックします。

アクセスの定義の表示

アクセスの管理権限は、役割に関連するアクセス定義を表示することをユーザーに許可します。ユーザーは、管理する必要がある権限のカテゴリに対して、アクセスの管理権限を持つ必要があります。たとえば、VMware または特定の VMware オブジェクトなどが該当します。

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。



セキュリティの管理

- 第7章 セキュリティイベントと監査ログ
- 第8章 セキュリティ証明書の管理
- 第9章 ユーザーセッションの管理
- 第10章 マスターサーバーのセキュリティ設定の管理
- 第11章 ユーザー用の API キーの作成と管理 (管理者)
- 第12章 API キーの追加と管理 (ユーザー)
- 第13章 認証オプションの設定
- 第14章 ホストの管理

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 の監査について](#)
- [システムログへの監査イベントの送信](#)

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.122 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 マスター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。
この記録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) はマスターサーバー上で実行し、監査記録は 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。

- 監査記録では、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。
- 監査記録では、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、監査記録が作成されます。
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	<p>資産データベース API で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。</p> <p>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。</p>
認証の失敗	<p>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。</p>
カタログ情報	<p>この情報には次のものが含まれます。</p> <ul style="list-style-type: none"> ■ 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	<p>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</p>
証明書検証エラー (CVF)	<p>SSL ハンドシェイクエラー、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。</p> <p>SSL ハンドシェイ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、監査レコードがマスター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。</p>
ディスクプールとボリュームプールの処理	<p>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。</p>
保留操作	<p>保留操作の作成、変更および削除。</p>
ホストデータベース	<p>ホストデータベースに関連する NetBackup の操作。</p>
ログオン試行回数	<p>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。</p>
ポリシーの処理	<p>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。</p>
イメージのユーザー操作のリストアおよび参照	<p>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 (bpulist) はすべて、ユーザー ID によって監査されます。</p>
セキュリティ構成	<p>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。</p>
リストアジョブの開始	<p>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。</p>
NetBackup Audit Manager (nbaudit)	<p>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。</p>

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せん。
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 管理コンソールは、監査が失敗したときに、終了状態コード 108 を返しませんが。

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ため、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 (管理コンソール) とジョブ (Web UI) 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 または nbsetconfig コマンド、[ホストプロパティ (Host Properties)]ユーティリティ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。
- 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atalog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 Catalog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 マスター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/opensv/netbackup/bin/admincmd`

- 3 次のコマンドを入力します。

```
nbermmcmd -changesetting -AUDIT_RETENTION_PERIOD  
number_of_days -machinename masterserver
```

`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。

```
nbermmcmd -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 マスター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/opensv/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` 表示するレポートデータの開始日時。

```
<"MM/DD/YY  
[HH:[MM[:SS]]]">
```

`-edate` 表示するレポートデータの終了日時。

```
<"MM/DD/YY  
[HH:[MM[:SS]]]">
```

<code>-ctgy category</code>	<p>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。</p> <p><code>-ctgy</code> 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。</p>
<code>-user</code> <code><username[:domainname]></code>	<p>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。</p>
<code>-fmt DETAIL</code>	<p><code>-fmt DETAIL</code> 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。</p> <ul style="list-style-type: none">■ <code>[-nottruncate]</code>。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。■ <code>[-pagewidth <NNN>]</code>。レポートの詳細セクションのページ幅を設定します。
<code>-fmt PARSABLE</code>	<p><code>-fmt PARSABLE</code> オプションは <code>DETAIL</code> 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 (<code> </code>) 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。</p> <ul style="list-style-type: none">■ <code>[-order<DTU DUT TUD UDT UTD>]</code>。情報を表示する順序を示します。<ul style="list-style-type: none">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.121 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。

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 ホスト ID とホスト ID ベースの証明書](#)
- [NetBackup セキュリティ証明書の管理](#)
- [NetBackup での外部セキュリティ証明書の使用](#)

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.132 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、ホストに証明書が配備されているかどうか、ホストから証明書が正常に削除されているかどうかに関係なく行う必要があります。

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名をクリックします。
- 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、これをより安全な方法で実行したい場合は、ホスト管理者が新しい証明書を取得するために使用する必要が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)]、[ホスト (Hosts)] 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、[再発行トークンの生成 (Generate reissue token)] をクリックします。

- 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

BMR クライアントリストアなどの特定のシナリオでは、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。[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、[セキュリティ (Security)]、[ホスト (Hosts)]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、[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。
- 4 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、[セキュリティ (Security)]、[ホスト (Hosts)]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、[証明書の自動再発行を無効にする (Revoke auto reissue certificate)]、[無効化 (Revoke)]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.129 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.132 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 `install_path\NetBackup\wmc\bin\install`
合

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 (クラスタ化されたマスター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
```

- クラスタ化されたマスター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。

- クラスタ化されたマスター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表示されます。
- [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。

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](#)
- [NetBackup ユーザーのロック解除](#)
- [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](#)
- [並列ユーザーセッションの最大数の構成](#)
- [失敗したサインインの試行の最大数を構成する](#)
- [ユーザーがサインインするときのパナーの表示](#)

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.138 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.139 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。

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。

マスター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](#)
- [NetBackup 8.0 以前のホストとの通信の無効化](#)
- [NetBackup ホスト名の自動マッピングの無効化](#)
- [NetBackup 証明書の配備のセキュリティレベルについて](#)
- [NetBackup 証明書配備のセキュリティレベルの選択](#)
- [ディザスタリカバリのパスフレーズの設定](#)
- [信頼できるプライマリサーバーについて](#)

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。

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 (ホスト管理者がマスター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 10-1 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)	<p>ホストがマスター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、ホストはマスターサーバーに認識されていると見なされます。</p> <ol style="list-style-type: none"> 1 ホストが NetBackup 構成ファイル (Windows レジストリまたは UNIX の <code>bp.conf</code> ファイル) で次のいずれかのオプションでリストされる。 <ul style="list-style-type: none"> ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER <p>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。</p> <ol style="list-style-type: none"> 2 <code>altnames</code> ファイル (<code>ALT NAMESDB_PATH</code>) にクライアント名としてホストがリストされている。 3 ホストがマスターサーバーの 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)	マスター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.143 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。

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 10-2 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サーバー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。

ユーザー用の API キーの作成と管理 (管理者)

この章では以下の項目について説明しています。

- [API キーについて](#)
- [API キーの追加または API キーの詳細の表示](#)
- [API キーの編集、再発行、または削除](#)

API キーについて

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、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.121 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

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)]、[API キー (API keys)]の順に選択します。
- 2 右上隅の[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)]、[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)]メニューで、[編集 (Edit)]をクリックします。

API キーの編集、再発行、または削除

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)]、[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)]、[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)]、[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 キーの追加と管理 (ユーザー)

この章では以下の項目について説明しています。

- [API キーの追加または自分の API キーの詳細の表示](#)
- [API キーの編集、再発行、または削除](#)
- [NetBackup REST API での API キーの使用](#)

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.154 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、プロフィー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、プロフィー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.154 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、プロフィー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、プロフィー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>'
```

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](#)
- [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](#)
- [シングルサインオン \(SSO\) 設定について](#)
- [NetBackup のシングルサインオン \(SSO\) の構成](#)
- [SSO のトラブルシューティング](#)

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。

- ユーザー名およびパスワード
- 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.157 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.162 の「[NetBackup のシングルサインオン \(SSO\) 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

役割に基づくアクセス制御 (RBAC) 構成の一部としてまだ完了していない場合は、証明書の認証を構成する前に、次の手順を完了していることを確認してください。

- NetBackup ユーザーに関連付けられた AD または LDAP ドメインを追加する。
 p.40 の「[AD または LDAP ドメインの追加](#)」を参照してください。
- NetBackup ユーザー用の RBAC を構成する。
 p.39 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 [ユーザー認証ドメイン (User authentication 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。
- 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。

- 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。

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。

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 [編集 (Edit)]をクリックします。
- 3 [ユーザー認証ドメイン (User authentication domain)]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。
 p.40 の「AD または LDAP ドメインの追加」を参照してください。
- 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。

シングルサインオン (SSO) 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 ID プロバイダ (IDP) 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 `nbidpccmd` 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 13-1 NAT 構成の例: プライベートネットワークの ID プロバイダ

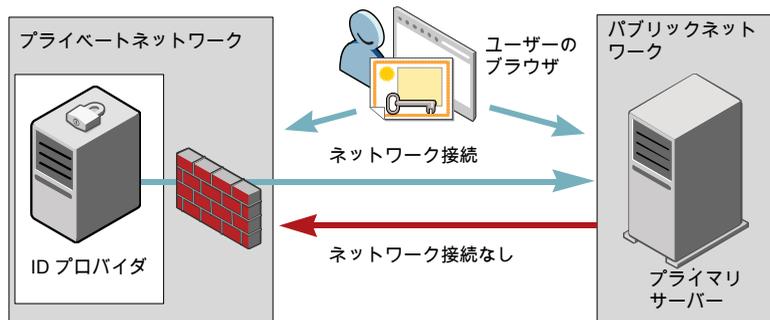


図 13-2 NAT 構成の例: プライベートネットワークのプライマリサーバー

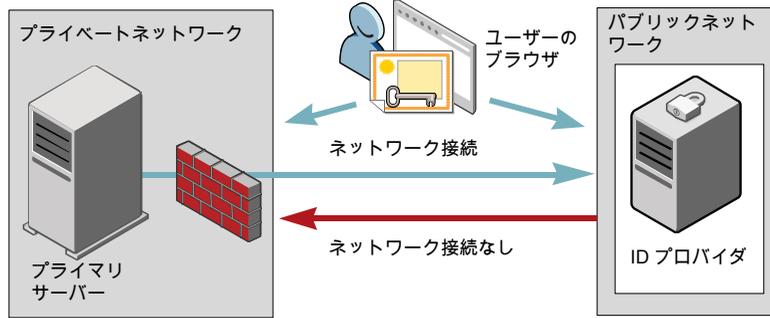
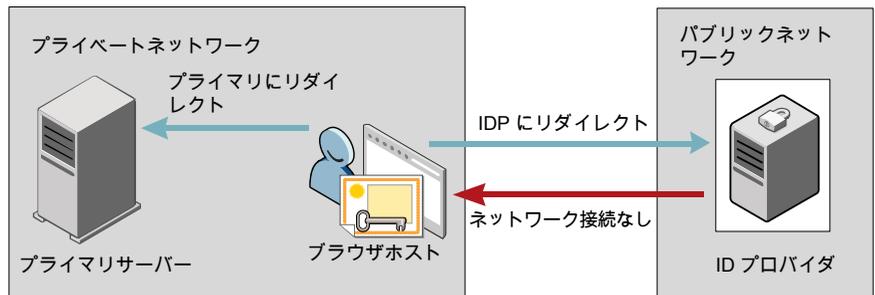


図 13-3 構成の例: 同じネットワークのプライマリサーバーと ID プロバイダ



図 13-4 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 のシングルサインオン (SSO) 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 13-1 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せん。
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.163 の「SAML キーストアの構成」を参照してください。 p.166 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。 <code>https://masterserver/netbackup/sso/saml2/metadata</code> ここで <i>masterserver</i> 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.167 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。

手順	処理	説明
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	<p>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> <p>p.44 の「役割へのユーザーの追加 (非 SAML)」を参照してください。</p>

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.168 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.167 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.167 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.167 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が含まれます。
- *-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 13-2 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 13-3

対応する AD または LDAP 属性	SAML 属性形式
userPrincipalName	<i>username@domainname</i>
memberOf	<i>(CN=group name, DC=domainname)</i>

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.166 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ならなかった場合、-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 でシングルサインオン (SSO) 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 について詳しくは、『NetBackup Web UI 管理者ガイド』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 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/opensv/logs/nbwebsservice`
- Windows の場合: `install_path¥NetBackup¥logs¥nbwebsservice`

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で最新の IDP 構成を追加して有効にします。p.166 の「[SAML キースタアの構成と 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 13-4

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
<code>userPrincipalName not found in response.</code>	NetBackup プライマリサーバーに IDP 構成を追加する際に、ユーザー (-u) オプションに入力した値が SAML 属性名と一致している必要があります。この値は、AD または LDAP の userPrincipalName 属性にマッピングされます。詳しくは、p.166 の「 SAML キースタアの構成と IDP 構成の追加および有効化 」を参照してください。
<code>userPrincipalName is not in expected format</code>	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 <code>username@domainname</code> の形式で定義されていることを確認します。 詳しくは、p.167 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
<p>Authentication issue instant is too old or in the future</p>	<p>このエラーは、次の理由で発生する場合があります。</p> <ul style="list-style-type: none"> ■ 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。 <p>NetBackup プライマリサーバーの <code><installpath>%var%global%wsl%config%web.conf</code> 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。</p> <p>SAML_ASSERTION_LIFETIME_IN_SECS=129600</p>
<p>Response is not success</p>	<p>このエラーは、次の理由で発生する場合があります。</p> <ul style="list-style-type: none"> ■ 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.163 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 13-5

原因	説明および推奨処置
<p>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</p>	<p>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。</p> <p>ユーザーの追加手順については、p.44 の「役割へのユーザーの追加 (非 SAML)」を参照してください。</p>
<p>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</p>	<p>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。</p> <p>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。</p> <p>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。</p> <p>ユーザーの追加手順については、p.44 の「役割へのユーザーの追加 (非 SAML)」を参照してください。</p>

原因	説明および推奨処置
<p>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</p>	<p>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。</p> <p>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。</p> <p>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.44 の「役割へのユーザーの追加 (非 SAML)」を参照してください。</p>
<p>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</p>	<p>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。</p> <ul style="list-style-type: none"> ■ 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.166 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。

ホストの管理

この章では以下の項目について説明しています。

- [NetBackup ホスト情報の表示](#)
- 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
- ホストの属性のリセット

NetBackup ホスト情報の表示

ホストアプリケーションには、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 (Hosts)] 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があります。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.179 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.180 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.180 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、この設定を無効にし、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.142 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。関連付けられたホスト ID にマッピングされていないホスト名を使用してホストに証明書を配備すると、NetBackup はそのホストを別のホストと認識するため、NetBackup は新しい証明書を配備し、新しいホスト ID をホストに発行します。

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 (Hosts)] 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 (Hosts)]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 (Hosts)]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
<code>client01.lab04.com</code>	<code>client01</code>
<code>client01.lab04.com</code>	<code>clustername</code>
<code>client01.lab04.com</code>	<code>clustername.lab04.com</code>
<code>client02.lab04.com</code>	<code>client02</code>
<code>client02.lab04.com</code>	<code>clustername</code>
<code>client02.lab04.com</code>	<code>clustername.lab04.com</code>

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)
<code>client01.lab04.com</code>	<code>client01.lab04.com</code> 、 <code>client01</code> 、 <code>clustername</code> 、 <code>clustername.lab04.com</code>
<code>client02.lab04.com</code>	<code>client02.lab04.com</code> 、 <code>client02</code> 、 <code>clustername</code> 、 <code>clustername.lab04.com</code>

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 環境でクラスタのバックアップを実行する場合は、プライベートネットワーク上のクラスタの仮想名にクラスタノード名をマッピングする必要があります。

表 14-1 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
<code>client01-bk.lab04.com</code>	<code>clustername-bk.lab04.com</code>
<code>client02-bk.lab04.com</code>	<code>clustername-bk.lab04.com</code>

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)
<code>client01-bk.lab04.com</code>	<code>clustername-bk.lab04.com</code>
<code>client02-bk.lab04.com</code>	<code>clustername-bk.lab04.com</code>

SQL Server 環境の自動検出マッピングの例

表 14-2 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 14-2 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

環境	ホスト	マッピング済みのホスト名
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
	<i>Node 1</i> の物理名	SQL Server クラスタの仮想名
	<i>Node 2</i> 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マッピングや、ホストに手動で追加したホスト名マッピングを削除できます。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.181 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 (Hosts)]の順に選択します。
- 2 ホストの名前を選択します。
- 3 [マッピングの管理 (Manage mappings)]をクリックします。
- 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。

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 (Hosts)]の順に選択します。
- 2 ホストを選択し、[属性のリセット (Reset attributes)]、[リセット (Reset)]の順にクリックします。
- 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: [ホスト属性をリセット (Reset Host Attributes)] オプションを誤って使用した場合は、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。

ストレージとバックアップの管理

- 第15章 ストレージの構成
- 第16章 保護計画の管理
- 第17章 従来のポリシーの管理
- 第18章 使用状況レポートと容量ライセンス

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。

- [ストレージの構成について](#)
- [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の作成](#)
- [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](#)
- [ディスクプールの作成](#)
- [ストレージユニットの作成](#)
- [ユニバーサル共有の作成](#)
- [NetBackup Web UI からのイメージ共有の使用](#)
- [ストレージ構成のトラブルシューティング](#)
- [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](#)
- [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](#)

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。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 のストレージオプションを構成できます。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。

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。ウィザードの手順に従って、AdvancedDisk、クラウ

ドストレージ、MSDP、イメージ共有用 MSDP、OpenStorage のオプションを構成できません。

メモ: KMS (キーマネジメントサービス) 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/opensv/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。

p.185 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.187 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.191 の「[ユニバーサル共有の作成](#)」を参照してください。

p.189 の「[ディスクプールの作成](#)」を参照してください。

p.190 の「[ストレージユニットの作成](#)」を参照してください。

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.189 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。クレデンシヤルを入力して、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。

詳しくは、『[NetBackup クラウド管理者ガイド](#)』および『[NetBackup Deduplication ガイド](#)』を参照してください。

p.189 の「[ディスクプールの作成](#)」を参照してください。

p.190 の「[ストレージユニットの作成](#)」を参照してください。

p.187 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.200 の「保護計画の作成」を参照してください。

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。

p.189 の「[ディスクプールの作成](#)」を参照してください。

p.190 の「[ストレージユニットの作成](#)」を参照してください。

p.185 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.200 の「[保護計画の作成](#)」を参照してください。

ディスクプールの作成

任意の種類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。
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。
- p.190 の「[ストレージユニットの作成](#)」を参照してください。
- p.185 の「[メディアサーバー重複排除ブール \(MSDP\) ストレージサーバーの作成](#)」を参照してください。
- p.187 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.200 の「[保護計画の作成](#)」を参照してください。

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.189 の「[ディスクプールの作成](#)」を参照してください。
p.185 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.187 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.200 の「[保護計画の作成](#)」を参照してください。

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 Deduplication 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。

- ユニバーサル共有を作成、変更、表示、削除し、アプライアンス間で管理し、独自の (BYO) サーバーを構築する。

メモ: NetBackup Appliance Web コンソールを使用して作成されたユニバーサル共有は、NetBackup Web UI を介して管理できません。NetBackup 8.3 以降、NetBackup Appliance でユニバーサル共有を管理するには、NetBackup Web UI を使用することをお勧めします。

- 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: ユニバーサル共有のポリシーを作成するには、NetBackup 管理コンソールを使用します。ユニバーサル共有ポリシー、前提条件、構成について詳しくは、『[NetBackup Deduplication 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.185 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。この名前は一意である必要はありません。複数のユニバーサル共有で同じ表示名を使用できます。
 - [ストレージサーバー (Storage Server)]を選択します。
 - [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。
 - [Active Directory ユーザー名 (Active Directory user names)]と[Active Directory グループ名 (Active Directory group names)]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。[Active Directory ユーザー名 (Active Directory user names)]と[Active Directory グループ名 (Active Directory 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、[Active Directory ユーザー名 (Active Directory user names)]と[Active Directory グループ名 (Active Directory 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。

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ホストを設定し、そのサーバーにイメージを共有できます。

『[NetBackup Deduplication ガイド](#)』の次のトピックの情報を使用して、クラウドリカバリホストを設定します。

MSDP クラウドを使用したイメージの共有について

クラウドリカバリホストの設定後に 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 (Storage)]、[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ホスト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。

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 15-1 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せん。 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 Deduplication 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/opensv/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/opensv/pdde/vpfs/vpfs-config.log (BYO とアプライアンス構成)
```

次の例では、必要ないいくつかのサービスが実行されていません。

```
[root@rhelnbu06 ~]# /usr/opensv/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 `InstantAccess` 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.191 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再起動する方法

ユニバーサル共有が作成されるたびに、ストレージサーバーにスクリプトも作成されます。このスクリプト (`/<msdp storage data path>/vpfs.mnt`) は、後でユニバーサル共有を再起動するために使用できます。

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-a4a8-81ddb5f819e  
  type fuse.vpfsd (rw,nosuid,nodev,relatime,user_id=0,group_id=0,  
  default_permissions,allow_other)
```

この例で、`aa7e/aa7e83e5-93e4-57ea-a4a8-81ddb5f819e` は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。

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ホストの作成に使用します。クラウドリカバリホストについて詳しくは、『[NetBackup Deduplication 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。

クラウドリカバリホストを設定するには、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、クラウドリカバリホストを設定する前に、キー管理サービス (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ホスト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。クラウドリカバリホスト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.193 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。

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](#)
- [保護計画の編集または削除](#)
- [保護計画への資産または資産グループのサブスクリプション](#)
- [保護計画からの資産のサブスクリプション解除](#)
- [保護計画の上書きの表示](#)
- [今すぐバックアップについて](#)

保護計画の作成

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、その保護計画に資産をサブスクリプションできます。また、保護計画を設定する前後に、作業負荷管理者の保護計画へのアクセス権も設定できます。アクセス権を設定するには、RBAC のロールを構成してから、これらのロールを保護計画に割り当てる必要があります。

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。OpenStorage、AdvancedDisk、クラウドストレージ、MSDP のストレージオプションは、Web UI を使用して構成できます。また、Web UI では、ディスクプールとストレージユニットも構成できます。

p.184 の「[ストレージの構成について](#)」を参照してください。

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。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
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。

- 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。

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 5 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。
 - 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 (オプション) 作業負荷として[クラウド (Cloud)]を選択し、クラウドプロバイダに Amazon AWS を選択した場合、スケジュールと保持の構成後にスナップショットレプリケーションを構成できます。クラウドスナップショットレプリケーションについては、『[NetBackup Web UI クラウド管理者ガイド](#)』を参照してください。

[追加コピー (Additional copies)]列で次の操作を行います。

- [スナップショットレプリケーションの構成 (Configure Snapshot replication)]をクリックします。
- [スナップショットレプリカの構成 (Configure snapshot replica)]ダイアログで、[追加 (Add)]をクリックします。
- [保持 (Retention)]を構成し、レプリケートしたスナップショットの[宛先 (Destination)]を選択します。

メモ: 追加のクラウドレプリケーションコピーは、保護計画ごとに 1 つだけ作成できます。

作業負荷として[クラウド (Cloud)]を選択した場合、手順 6 に進みます。

- 5 [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、CloudPoint 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、CloudPoint 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 6 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。	<p>[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。</p> <p>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。</p> <p>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。</p>

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。

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は、『NetBackup Deduplication 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。

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。

- 6 [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:

- 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。
- クラウドプロバイダに Microsoft Azure または Azure Stack Hub を選択した場合は、[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、資産が存在するのと同じ地域内の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ることができます。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。

- 7 [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。
- 8 [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。

保護計画の編集または削除

保護計画の編集

保護計画の[説明 (Description)]と[ストレージオプション (Storage options)]を変更できます。

メモ: 保護計画の作成後は、[スケジュール (Schedules)]、[保護対象資産 (Protected assets)]、[詳細 (Advanced)]オプションを編集できません。異なる保護設定を使用する場合、新しい保護計画を作成するか、計画をカスタマイズする必要があります。

p.200 の「[保護計画の作成](#)」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、別の保護計画に移動する必要があります。

p.208 の「[保護計画からの資産のサブスクリプション解除](#)」を参照してください。

p.207 の「[保護計画への資産または資産グループのサブスクリプション](#)」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 保護計画名の横にあるチェックボックスにチェックマークを付けます。
- 3 右上の[削除 (Delete)]をクリックします。次に、[はい (Yes)]をクリックします。

p.200 の「保護計画の作成」を参照してください。

保護計画への資産または資産グループのサブスクリプション

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リプションできます。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リプションできます。保護計画に資産をサブスクリプションする前に、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リプションする際、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。

保護計画に資産または資産グループをサブスクリプションするには

- 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 (Advanced)]セクション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、回復、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。

p.200 の「保護計画の作成」を参照してください。

保護計画からの資産のサブスクリプション解除

個別の資産または資産のグループのサブスクリプションを、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リプションを解除するときに、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リプションされており、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リプション解除されます。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リプションを解除するには

- 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リプションを解除するには

- 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。

p.200 の「保護計画の作成」を参照してください。

p.206 の「保護計画の編集または削除」を参照してください。

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。

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。

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。

- VMware
- RHV
- クラウド
- Microsoft SQL
- クラウド
- Nutanix AHV

メモ: 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。また、今すぐバックアップを使うために、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。

Web UI から今すぐバックアップを使うには

- 1 左側から作業負荷を選択します。
- 2 バックアップの対象となる資産を選択します。
- 3 表の上部にある[今すぐバックアップ (Backup now)]をクリックするか、資産の行の処理メニューから[今すぐバックアップ (Backup now)]を選択します。
- 4 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場合は、[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できます。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。

- 5 バックアップを開始します。

資産の詳細ページから今すぐバックアップを使うには

- ◆ 資産の詳細を表示すると、資産がサブスクライブされているすべての保護計画を表示できます。一覧表示されているいずれかの保護計画から、[今すぐバックアップ (Backup now)]を選択できます。

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場合は、[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できます。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。

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。

- [NetBackup の従来のポリシーについて](#)
- [NetBackup Web UI でのポリシー管理について](#)

NetBackup の従来のポリシーについて

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 17-1 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リブされていません。ただし、保護計画にサブスクリブされていたか、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があります (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.212 の「NetBackup Web UI でのポリシー管理について」 を参照してください。 従来のポリシーを管理するために、NetBackup 管理者は NetBackup 管理コンソールまたは NetBackup CLI を使用できます。また、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。

質問	回答
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。	NetBackup 管理者のみが従来のポリシーを作成できます。保護計画に資産をサブスクライブするのに必要な権限を持っていない場合は、作業負荷管理者が保護計画を構成できません。 NetBackup 管理者は、資産の保護に保護計画 (Web UI) を使用するか、従来のポリシー (管理コンソール) を使用するかを選択できます。
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。
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。

NetBackup Web UI でのポリシー管理について

NetBackup Web UI は保護計画を使用して、**NetBackup** 環境内の資産を保護します。ほとんどの従来のポリシーを管理するには、**NetBackup** 管理コンソールを使用する必要があります。ただし、一部のポリシー形式は、**NetBackup Web UI** でも管理できます。

- MS-Windows
- Standard
- ストレージライフサイクルポリシー (SLP)
- Oracle
- MS-SQL-Server
- NDMP
- VMware

これらのポリシーについて詳しくは、次のガイドを参照してください。

[『NetBackup 管理者ガイド Vol. 1』](#)

[『NetBackup for Oracle 管理者ガイド』](#)

[『NetBackup for Microsoft SQL Server 管理者ガイド』](#)

[『NetBackup for NDMP 管理者ガイド』](#)

[『NetBackup for VMware 管理者ガイド』](#)

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バックアップデータサイズの追跡](#)
- [使用状況レポートのサーバーリストの構成](#)
- [容量ライセンスのレポートのスケジュール設定](#)
- [増分レポートのその他の構成](#)
- [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](#)

プライマリサーバー上のバックアップデータサイズの追跡

nbdeployutil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)。詳しくは、「[容量ライセンスレポートのスケジュール設定](#)」を参照してください。
- [Usage Insights](#) へのリンク。この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。
- 次のポリシー形式のレポートを作成します。

BigData	Informix	NDMP	Sybase
MS-Exchange-Server	MS-SQL-Server	Oracle	VMware
Hyper-V	MS-Windows	Standard	Hypervisor

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 (単一または複数) 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/opensv/var/global/incremental/Capacity_Trend.out
Windows の場合:
`install_path¥var¥global¥incremental¥Capacity_Trend.out`
- 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.214 の「使用状況レポートのサーバーリストの構成」を参照してください。
p.147 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

「容量ライセンスレポートのスケジュール設定」。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説明します。

『Veritas Usage Insights 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。

使用状況レポートのサーバーリストの構成

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。

リストにサーバーを追加する方法

- 1 リモート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 NetBackup 管理コンソールの左ペインで、[NetBackup の管理 (NetBackup Management)]、[ホストプロパティ (Host Properties)] の順に展開します。
- 3 [マスターサーバー (Master Servers)] を選択します。
- 4 右ペインで、変更するプライマリサーバーをダブルクリックします。
- 5 プロパティダイアログボックスの左ペインで、[サーバー (Servers)] をクリックします。
- 6 [追加サーバー (Additional Servers)] タブを選択して [追加 (Add)] をクリックします。
- 7 [新しいサーバーエントリの追加 (Add a New Server Entry)] ダイアログボックスで、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。
- 8 [追加 (Add)] をクリックします。ダイアログボックスを開いたまま、他のエントリを追加できます。
- 9 [閉じる (Close)] 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/opensv/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/opensv/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、レポートに含めるマスター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、マスターサーバーが 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/opensv/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他の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/opensv/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せん。`--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` 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マスターサーバーが追加されていることを確認してください。

- Oracle RAC (Real Application Clusters) の場合、データのバックアップを作成するノードのサイズが報告されるため、保護データサイズが複数回報告されることがあります。

Oracle Real Application Clusters (RAC) のさまざまなノードでバックアップ操作を開始すると、容量ライセンスレポートの各行にすべてのノードが個別に表示されます。

- 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。
収集段階で Web サービスが中断されたため、正確なライセンス方式ではなくバックアップイメージヘッダーを使用して、マスターサーバー <サーバー名> のレポートが生成されています。(Report for master server SERVER_NAME is generated using the backup image header method instead of accurate licensing method because of web service interruptions during the gather phase.)

- 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。

- クラウド作業負荷のスマート測定において、スナップショットサイズの計算でエラーが発生する場合があります。

`nbDeployutil` 容量レポートが実際の使用済みサイズではなく合計ボリュームサイズをスナップショットサイズとして報告する場合があるため、クラウド作業負荷のスナップショットサイズの計算でエラーが発生する可能性があります。ログを参照して、警告メッセージを特定します。

このエラーは次の原因で発生する場合があります。

- AWS、Azure、または Azure Stack Hub プラグインの場合、スナップショットのサイズを取得するための権限が不足しています。プラグインの構成で、次の権限が追加されているかどうかを確認します。

Azure および Azure Stack Hub の場合:

```
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
```

AWS の場合:

```
"ebs:ListSnapshotBlocks",
```

- スナップショットサイズの計算に使用されるクラウド API の最大要求数の制限に達しました。
- ネットワーク接続の最大再試行回数を超過しました。

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。

4

Veritas Resiliency Platform

- [第19章 Resiliency Platform の管理](#)

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](#)
- [用語について](#)
- [Resiliency Platform の構成](#)
- [NetBackup と Resiliency Platform の問題のトラブルシューティング](#)

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。 <ul style="list-style-type: none">■ 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いない場合。
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。

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 19-1

タブ	列	説明
<ul style="list-style-type: none"> ■ 自動化済み (Automated) ■ 未自動化 (Not automated) 	名前 (Name)	仮想マシンの名前。
<ul style="list-style-type: none"> ■ 自動化済み (Automated) 	RPO	<p>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。</p> <p>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。</p>
<ul style="list-style-type: none"> ■ 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。
<ul style="list-style-type: none"> ■ 自動化済み (Automated) 	リカバリ準備状況 (Recovery readiness)	<p>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。</p> <ul style="list-style-type: none"> ■ 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いない場合。

タブ	列	説明
<ul style="list-style-type: none"> ■ 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。
<ul style="list-style-type: none"> ■ 自動化済み (Automated) ■ 未自動化 (Not automated) 	サーバー (Server)	VM のサーバー名。
<ul style="list-style-type: none"> ■ 自動化済み (Automated) 	保護 (Protection)	VM の保護状態。
<ul style="list-style-type: none"> ■ 自動化済み (Automated) 	Resiliency Group	VM が属する Resiliency Group の名前。
<ul style="list-style-type: none"> ■ 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 19-2 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。 <ul style="list-style-type: none"> ■ /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。	<ul style="list-style-type: none"> ■ 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。 <ul style="list-style-type: none"> ■ NetBackup インストールディレクトリの /usr/opensv/logs/nbwebsevice/ ■ NetBackup Windows の C:\Program Files\Veritas\NetBackup\logs\nbwebsevice
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。

クレデンシヤル

- [第20章 クレデンシヤルの管理](#)

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について](#)
- [NetBackup でのクレデンシャルの追加](#)
- [クレデンシャルの編集](#)
- [クレデンシャルの削除](#)

NetBackup でのクレデンシャル管理について

NetBackup Web ユーザーインターフェースの[クレデンシャルの管理 (Credential management)]ノードは、NetBackup を使用するクレデンシャルを一元的に管理する機能を提供します。

NetBackup では、次のシステムのクレデンシャルを作成して管理できます。

- 外部キーマネージメントサービス (KMS) サーバー
- クラウド (クラウドインスタンスの場合)
- Kubernetes
- Microsoft SQL Server
- Nutanix AHV
- NetBackup コールホームプロキシ
- ネットワークデータ管理プロトコル (NDMP)

クレデンシャルの追加は次の手順で構成されています。

- クレデンシャルの基本プロパティ (クレデンシャル名やタグなど) の追加
- クレデンシャルへのカテゴリの割り当て (例: Microsoft SQL Server または外部 KMS サーバー)。

- クレデンシャルにアクセスするために必要な権限の割り当て

NetBackup でのクレデンシャルの追加

NetBackup がさまざまなシステムに接続するために使用するクレデンシャルを追加できます。

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)]をクリックします。
- 3 次のプロパティを追加します。
 - クレデンシャル名 (例: `sqlserver_cred1`)
 - タグ (例: `sqlserver`)
 - 説明 (例: このクレデンシャルは `sqlserver` へのアクセス用)
- 4 [次へ (Next)]をクリックします。
- 5 クレデンシャルのカテゴリと、このクレデンシャルに割り当てるそれぞれのクレデンシャルの詳細を選択します。

外部 KMS

設定した外部 KMS サーバーにクレデンシャルを割り当てる場合を選択します。

外部 KMS サーバーの次の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。

Microsoft SQL Server	<p>設定した SQL Server にクレデンシャルを割り当てる場合に選択します。</p> <p>次のオプションのいずれかを使用します。</p> <ul style="list-style-type: none"> ■ クライアントのローカルで定義されているクレデンシャルを使用 (Use credentials that are defined locally on the client) ■ Microsoft SQL Server クレデンシャルの入力 (Provide Microsoft SQL Server credentials) <p>SQL Server のクレデンシャルの構成について詳しくは、『NetBackup for Microsoft SQL Server 管理者ガイド』を参照してください。</p>
クラウドインスタンス	<p>クラウドインスタンスにクレデンシャルを割り当てる場合に選択します。</p> <ul style="list-style-type: none"> ■ Linux インスタンスの場合は [Linux] オプションを選択し、[ユーザー名 (User name)] を指定します。必要に応じて [パスワード (Password)] または [SSH キー (SSH Key)] オプションを選択し、パスワードまたは SSH キーを指定します。 ■ Windows インスタンスの場合は [Windows] オプションを選択し、[ユーザー名 (User name)] と [パスワード (Password)] を指定します。必要に応じて、インスタンスの [ドメイン (Domain)] を指定します。
Kubernetes	<p>Kubernetes クラスタにクレデンシャルを割り当てる場合に選択します。</p> <p>クラスタの次の詳細を指定します。</p> <ul style="list-style-type: none"> ■ トークン - トークンを指定します。 ■ CA 証明書 - CA 証明書ファイルの内容を指定します。
AHV	<p>AHV クラスタにクレデンシャルを割り当てる場合に選択します。</p> <p>クレデンシャルの次の詳細を指定します。</p> <ul style="list-style-type: none"> ■ ユーザー名 ■ パスワード ■ ドメイン
NetBackup コールホームプロキシ	<p>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作成する場合に選択します。</p> <p>メモ: 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。マスターサーバーで次のコマンドを使用します。</p> <pre>echo CALLHOME_PROXY_NAME = CredentialName bpsetconfig.exe</pre>

6 [次へ (Next)] をクリックします。

- 7 [追加 (Add)]をクリックして、このクレデンシャルにアクセスするための特定の役割に権限を割り当てます。

p.109 の「[クレデンシャル](#)」を参照してください。

- 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。
- 9 NetBackup コールホームプロキシのクレデンシャルを構成した場合は、NetBackup の構成を更新します。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
```

クレデンシャルの編集

クレデンシャルのタグ、説明、カテゴリ、または権限を変更する場合は、クレデンシャルを編集できます。クレデンシャル名は変更できません。

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 [編集 (Edit)]をクリックします。
- 4 必要に応じてクレデンシャルを編集します。
- 5 すべての変更を確認したら、[完了 (Finish)]をクリックします。

メモ: 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、クレデンシャルの編集後、[接続 (Connect)]ボタンを使用してインスタンスを再接続する必要があります。

クレデンシャルの削除

不要になったクレデンシャルを削除できます。

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。マスター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
```

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](#)
- 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
- [vssat](#) コマンドで [AD](#) または [LDAP](#) ドメインを追加できない
- [ユーザーまたはグループを検証できません \(Unable to validate the user or group\)](#)

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 21-1 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	nbweb service が起動していることを確認します。	詳しくは nbweb service 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。	<ul style="list-style-type: none"> ■ Java Keytool コマンドを使用して、次のファイルを検証します。 Windows: <code>install_path\var\global\wsl\credentials\nbweb service.jks</code> UNIX: <code>/usr/opensv/var/global/wsl/credentials nbweb service.jks</code> ■ nbwebgroup に、nbweb service.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 21-1 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時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.132 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.39 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。

vssat コマンドで AD または LDAP ドメインを追加できない

AD または LDAP ドメインを追加した後、vssat validateprpl コマンドを使用して構成を検証したり、vssat validategroup コマンドを使用してグループを検証できます。ドメインが正常に追加されなかった場合、vssat 検証には The principal or group does not exist. と示されます。詳細は nbatd のログに書き込まれます。

AD または LDAP ユーザーの検証は、次のいずれかの理由により失敗する場合があります。

- AD または LDAP サーバーとの接続を確立できない
- 不正なユーザークレデンシャルが指定された
- 不正なユーザーベース DN、またはグループベース DN が指定された

- ユーザーベース DN またはグループベース DN に同じ名前の複数のユーザーまたはグループが存在する
- ユーザーまたはグループが存在しない

vssat 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。

AD または LDAP サーバーとの接続を確立できない

NetBackup が AD または LDAP サーバーとの接続を確立できなかった場合、nbatd ログに次のエラーが記録されます。

エラーメッセージの例:

```
(authldap.cpp) CAuthLDAP::validatePrpl - ldap_simple_bind_s()  
failed for user CN=Test User,OU=VTRSUsers,DC=VRTS,DC=com',  
error = -1, errmsg = Can't contact LDAP server,9:debugmsgs,1
```

LDAP サーバーの URL の検証が失敗する

vssat addldapdomain コマンドを使用して入力した LDAP サーバーの URL (-s オプション) は、検証テストをパスしません。

URL の検証:

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd>  
-d <debug_level> -o nettimeout=<seconds>
```

検証エラーメッセージの例:

```
ldapsearch -H ldaps://example.veritas.com:389 -D  
"CN=Test User,OU=VTRSUsers,DC=VRTS,DC=com" -w *****  
-d 5 -o nettimeout=60
```

```
TLS: can't connect: TLS error -8179:Peer's Certificate issuer  
is not recognized. ldap_sasl_bind(SIMPLE):  
Can't contact LDAP server (-1)
```

サーバー証明書の発行者が信頼できる認証局 (CA) ではない

ldaps オプションを使用すると、ldapsearch コマンドを使用して証明書発行者を検証できます。

証明書発行者の検証:

```
set env var LDAPTLS_CACERT to cacert.pem
```

```
ldapsearch -H <LDAPS_URI> -D "<admin_user_DN>" -w <passwd>  
-d <debug_level> -o nettimeout=<seconds>
```

検証メッセージの例:

```
ldapsearch -H ldaps://example.veritas.com:389 -D  
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w *****  
-d 5 -o nettimeout=60
```

```
TLS: can't connect: TLS error -8179:  
Peer's Certificate issuer is not recognized..ldap_sasl_bind(SIMPLE):
```

```
Can't contact LDAP server (-1)
```

cacert.pem ファイルのパスは次のとおりです。

Windows の場合:

```
install_path¥NetBackup¥var¥global¥vxss¥eab¥data  
¥systemprofile¥certstore¥trusted¥pluggins¥ldap¥cacert.pem
```

UNIX の場合:

```
/usr/opensv/var/global/vxss/eab/data/root/.VRTSAt/profile  
/certstore/trusted/pluggins/ldap/cacert.pem
```

LDAP サーバーのセキュリティ証明書に署名した認証局 (CA) が、nbatd トラストストアに存在しない

証明書を nbatd コマンドのトラストストアに追加するには、vssat addldapdomain コマンドの `-f` オプションを使用します。

このオプションは、次の CA 以外が証明書に署名した場合に必要です。

Certification Services Division	GeoTrust	Symantec Corporation
CyberTrust	GlobalSign	VeriSign Trust Network
DigiCert	RSA Security Inc.	

ユーザークレデンシャルが有効ではない

vssat addldapdomain を使用して LDAP ドメインを追加したときにユーザークレデンシャルが有効ではなかった場合、nbatd ログには次のエラーが記録されます。

```
CAuthLDAP::validatePrpl - ldap_simple_bind_s() failed for user  
'CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com',  
error = 49, errmsg = Invalid credentials,9:debugmsgs,1
```

次のコマンドを実行して、管理者ユーザーの DN とパスワードを検証します。

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>"  
-w <passwd> -d <debug_level> -o nettimeout=<seconds>
```

メッセージの例:

```
ldapsearch -H ldap://example.veritas.com:389 -D  
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w *****  
-d 5 -o nettimeout=60 ldap_bind: Invalid credentials (49)
```

不正なユーザーベース DN、またはグループベース DN が指定された

ユーザーベース DN (-u オプション) またはグループベース DN (-g オプション) が正しくない場合、nbatd ログには次のエラーが記録されます。

```
CAuthLDAP::validatePrpl - ldap_search_s() error = 10,  
errmsg = Referral,9:debugmsgs,1  
CAuthLDAP::validatePrpl-ldap_search_s()  
error = 34, errmsg = Invalid DN syntax,9:debugmsgs,1
```

たとえば、次のコマンドを実行します。

```
ldapsearch -H ldap://example.veritas.com:389 -D  
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w *****  
-b "OU=VRTSUsers,DC=VRTS,DC=com" "(&(cn=test user)(objectClass=user))"
```

```
ldapsearch -H ldap://example.veritas.com:389 -D  
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w *****  
-b "VRTS" "(&(cn=test user)(objectClass=user))"
```

ユーザーベース DN またはグループベース DN に同じ名前の複数のユーザーまたはグループが存在する

この問題をトラブルシューティングするには

- 1 次のエラーが nbatd ログに含まれるかどうか確認します。

```
CAuthLDAP::validateGroup - search returned '2' entries for group
name
'team_noone', even with referrals set to OFF,9:debugmsgs,1
```

- 2 ldapsearch コマンドを使用して、既存のベース DN の一致するエントリの数を検証します。

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd>
-d <debug_level> -o nettimeout=<seconds> -b <BASE_DN>
<search_filter>
```

これは、既存のユーザーベース DN とグループベース DN それぞれについて、ユーザー検索属性 (-a オプション) とグループ検索属性 (-y オプション) に一意の値がない場合に該当します。

検証メッセージの例:

```
ldapsearch -H ldap://example.veritas.com:389 -D
"CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w *****
-b "DC=VRTS,DC=com" "(&(cn=test user)(objectClass=user))"
# LDAPv3 # base <DC=VRTS,DC=com> with scope subtree # filter:
(cn=Test User) # requesting: ALL # Test User, VRTSUsers,
VRTS.com dn: CN=Test User,OU=VRTSUsers,DC=VRTS,
DC=com # Test User, RsvUsers, VRTS.com dn:
CN=Test User,OU=RsvUsers,DC=VRTS,DC=com # numEntries: 2
```

ユーザーまたはグループが存在しない

この問題をトラブルシューティングするには

- 1 次のエラーが nbatd ログに含まれるかどうか確認します。

```
CAuthLDAP::validatePrpl - user 'test user' NOT found,
9:debugmsgs,4 CAuthLDAP::validateGroup - group
'test group' NOT found, 9:debugmsgs,4
```

- 2 ユーザーまたはグループが LDAP ドメインに存在していても、vssat validateprpl または vssat validategroup のコマンドがこのエラーで失敗する場合は、次のコ

マンドを使用して、ユーザーまたはグループが現在のベース DN に存在するかどうかを検証します。

- `ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d <debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>`

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)

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。