# NetBackup Web UI セキュリティ管理者ガイド

リリース 8.1.2

VERITAS

# NetBackup Web UI セキュリティ管理者ガイド

最終更新日: 2018-10-18

マニュアルバージョン: NetBackup 8.1.2

## 法的通知と登録商標



Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

## テクニカルサポート

テクニカルサポートは世界中にサポートセンターを設けています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の Web サイトにアクセスしてください。

https://www.veritas.com/support/ja_JP.html

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

既存のサポート契約に関する質問については、次に示す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。

| | |
|---|---|
| 世界全域 (日本を除く) | CustomerCare@veritas.com |
| Japan (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 ページに最終更新日付が記載されています。最新のマニュアルは、次のベリタス 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

次のベリタスコミュニティサイトでマニュアルの情報を参照したり、質問することもできます。

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

## ベリタスの Service and Operations Readiness Tools (SORT) の表示

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

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

# 目次

1

# NetBackup 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 ユーザーインターフェースについて

NetBackup 8.1.2 に導入された新しい 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 ブラウザからマスター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。
- 重要な情報の概要を表示するダッシュボード。
- 役割に基づくアクセス制御 (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、バックアップ管理、または作業負荷の保護に関連するタスクを委任できます。
- NetBackup セキュリティ管理者は、NetBackup セキュリティ、証明書管理、RBAC を管理できます。

- バックアップ管理者は、サービスレベル目標 (SLO) を満たすために保護サービスを提供します。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。
- 作業負荷管理者は、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、仮想マシンのセルフサービスリカバリを実行できます。NetBackup 8.1.2 で、作業負荷管理者は、VMware およびクラウドの作業負荷を管理および構成できます。
- 使用状況レポートは、マスター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 Smart Meter 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。

## NetBackup Web UI のアクセス制御

NetBackup では、役割に基づく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。このアクセス制御には、ユーザーが実行できるタスクと、ユーザーが表示および管理できる資産が含まれています。アクセス制御は、アクセスルールを通じて実行されます。

- アクセスルールは、ユーザーまたはユーザーグループに、役割とオブジェクトグループを関連付けます。役割は、ユーザーが持つアクセス権を定義します。オブジェクトグループには、ユーザーがアクセスできる資産と NetBackup オブジェクトを定義します。単一のユーザーまたはグループに複数のアクセスルールを作成でき、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。
- NetBackup には、デフォルトの役割が 3 つ用意されています。ユーザーのニーズに最も適した役割を選択するか、そのユーザーの要件を満たすためのカスタムの役割を作成します。
- オブジェクトグループを使用して、資産やアプリケーションサーバーのグループを定義したり、ユーザーが表示または管理できる保護計画を示します。たとえば、特定の VMware アプリケーションサーバーを使用してオブジェクトグループを作成して、VMware 管理者向けアクセス権を付与できます。VMware 管理者が VMware 資産を保護するために選択できる特定の保護計画を、オブジェクトグループに追加することもできます。
- 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。EA を使用して構成されているユーザーは、Web UI と API に対する完全なアクセス権を持ちます。NetBackup アクセス制御 (NBAC) が有効な場合は、Web UI を使用できません。

## NetBackup ジョブおよびイベントの監視

NetBackup Web UI を使用すると、セキュリティ管理者やバックアップ管理者は、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。

- NetBackup セキュリティ管理者は、ダッシュボードを使用して、セキュリティ証明書や監査イベントの状態を参照できます。

- バックアップ管理者は、ダッシュボードを使用することで、NetBackup ジョブの状態を参照できます。ジョブが失敗したときに通知を受信するために、電子メール通知を構成することもできます。NetBackup では、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。

- 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。
- オンプレミスストレージまたはスナップショットストレージを簡単に選択できます。
- 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。たとえば、バックアップストレージ向けの NetBackup Accelerator やインスタントアクセスがあります。長期保存用には、クラウドプロバイダ、CloudCatalyst、暗号化、または圧縮があります。
- 保護計画ウィザードは、構成済みのサポート対象ストレージに基づいて、バックアップ、レプリケーション、または長期保存用ストレージを選択するために役立ちます。
- バックアップ管理者は、保護計画を作成して管理します。つまり、バックアップのスケジュールとストレージの責任を負います。
- 作業負荷管理者は、主に資産または資産グループを保護するための保護計画を選択します。ただし、バックアップ管理者は、必要に応じて保護計画に資産をサブスクライブすることもできます。

### セルフサービスリカバリ

NetBackup Web UI は、VM のリカバリを簡略化します。インスタントアクセス機能を使用して、VM のスナップショットをマウントして、そのファイルに即時アクセスすることもできます。ファイルをローカルホストにダウンロードしたり、ファイルを元の VM にリストアしたりできます。

## 用語

次の表では、新しい Web ユーザーインターフェースで導入された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 |
| --- | --- |
| アクセスルール | RBAC は、ユーザーまたはユーザーグループ、役割またはアクセス権、ユーザーまたはユーザーグループがアクセスできるオブジェクトグループを定義します。ユーザーまたはグループには、複数のアクセスルールを設定できます。 |
| 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 に対して完全なアクセス権を持ちます。NetBackup Web UI の各ガイドでは、*NetBackup 管理者*という用語は、NetBackup への完全なアクセス権を持つユーザーも指しますが、通常は NetBackup 管理コンソールのユーザーを指します。<br>「*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。 |
| 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。 |
| インテリジェントグループ | 指定した条件 (クエリー) 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。<br>VMware の場合は、[インテリジェント VM グループ (Intelligent VM groups)] タブにこれらのグループが表示されます。 |
| インスタントアクセス | NetBackup バックアップイメージから作成したインスタントアクセス VM は瞬時に利用可能になるため、ほぼゼロのリカバリ時間目標を達成できます。NetBackup は仮想マシンのスナップショットをバックアップストレージデバイスに直接マウントするため、ESXi ホストまたはクラスタはスナップショットを通常の仮想マシンとして扱えます。 |
| オブジェクトグループ | RBAC の場合、ユーザーがアクセスすることを許可された資産のコレクション、保護計画、サーバー、その他のリソースを指します。 |
| 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。 |

| 用語 | 定義 |
| --- | --- |
| RBAC | 役割に基づくアクセス制御です。管理者は、RBAC で構成されているアクセスルールを通じて、NetBackup Web UI へのアクセスを委任または制限できます。<br><br>**メモ:** RBAC で構成したルールは、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。Web UI は、NetBackup アクセス制御 (NBAC) ではサポートされておらず、NBAC が有効になっている場合は使用できません。 |
| 役割 (Role) | RBAC の場合、ユーザーが持つことができる権限を定義します。NetBackup にはシステム定義の役割が 3 つあり、ユーザーがセキュリティ、保護計画、バックアップを管理したり、作業負荷資産を管理したりすることを可能にします。 |
| 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。クラウドの作業負荷に対しては、スナップショットストレージが使用されます。 |
| サブスクライブ、保護計画に対して | 資産または資産グループを保護計画と関連付ける処理です。関連付けられた資産は、計画のスケジュールとストレージの設定に従って保護されます。Web UI では、*サブスクライブ*を「保護の構成」とも表記します。*サブスクライブ解除*は、計画から資産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 またはクラウドです。 |
| ワークフロー | NetBackup Web UI を使用して完了できるエンドツーエンドプロセスです。たとえば、NetBackup 8.1.2 で、VMware とクラウドの資産を保護およびリカバリできます。 |

# NetBackup Web UI からの NetBackup マスターサーバーへの初回サインイン

NetBackup のインストール後に、root ユーザーまたは管理者が 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 アクセスルールを作成する必要があります。(拡張監査ユーザーも管理者アクセスを持ちます。)アクセスルールは、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。「サポートと追加の構成」も参照してください。

**NetBackup Web UI を使用して、NetBackup マスター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://*masterserver*/webui/login

*masterserver* は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。

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

| ユーザーの種類 | 使用する形式 | 例 |
|---|---|---|
| ローカルユーザー | *username* | root |
| ドメインユーザー | *DOMAIN¥username* | WINDOWS¥Administrator |

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アクセスルールを作成します。
- 別のユーザーにアクセスルールを作成するタスクを委任します。
  そのユーザー用に、セキュリティ管理者の役割を使用してアクセスルールを作成します。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ルールを作成できます。

p.15 の「RBAC の構成」を参照してください。

NetBackup セキュリティ管理者として 1 人以上のユーザーに委任した後は、Web UI には root または管理者アクセスは必要ありません。

## サポートと追加の構成

- 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 がブロック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。
- サードパーティの 証明書を使用する場合は、Web サーバー向けにサードパーティの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。

# Web UI からの NetBackup マスターサーバーへのサインイン

ユーザーは、NetBackup Web UI を介して、NetBackup マスターサーバーに Web ブラウザからサインインできます。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。

ユーザーは、ルートユーザーまたは管理者であるか、NetBackup RBAC でそのユーザー向けに設定された役割を持っている必要があります。

**NetBackup Web UI を使用して、NetBackup マスター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://*masterserver*/webui/login

*masterserver* は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。

2 クレデンシャルを入力して、[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 | *username* | root |
| ドメインユーザー | *DOMAIN¥username* | WINDOWS¥Administrator |

# NetBackup ダッシュボード

NetBackup ダッシュボードでは、組織内のロールに関連する詳細情報のクイックビューを提供します。

**表 1-2** NetBackup セキュリティ管理者向けの NetBackup ダッシュボード

| ダッシュボードウィジェット | 説明 |
|---|---|
| 証明書 | 環境内にあるホストの ID ベースのセキュリティ証明書に関する情報を表示します。 |
| トークン | 環境内の認証トークンに関する情報を表示します。 |
| セキュリティイベント | [アクセス履歴 (Access history)]ビューには、ログインイベントのレコードが含まれます。[監査イベント (Audit events)]ビューには、トークン、証明書、証明書失効リスト (CRL) に関連するイベントが含まれます。 |

2

# 役割に基づくアクセス制御の管理

この章では以下の項目について説明しています。



## NetBackup の役割に基づくアクセス制御 (RBAC) について

NetBackup Web ユーザーインターフェースは、NetBackup 環境に役割に基づくアクセス制御を適用する機能を提供します。RBAC を使用して、現在 NetBackup へのアクセス権を持たないユーザーにアクセス権を提供します。または、現在管理者アクセス権を

持っている NetBackup ユーザーに対して、組織内の役割に基づいて制限されたアクセス権を提供できます。

NetBackup 管理コンソールのアクセス制御方法と、root ユーザーおよび管理者向けのアクセス制御と監査について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

**表 2-1** RBAC の機能

| 機能 | 説明 |
|---|---|
| 事前定義済みの役割またはカスタムの役割で、特定のタスクの実行をユーザーに許可 | RBAC の事前定義済みの役割は、システム管理者、バックアップ管理者、または作業負荷管理者の共通タスクを実行することをユーザーに許可します。または、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。<br>root ユーザーと管理者は、すべての NetBackup インターフェースと API で、引き続き完全なアクセス権を持ちます。 |
| ユーザーの役割に合った NetBackup 領域および機能へのアクセス許可 | RBAC ユーザーは、そのビジネスの役割において一般的なタスクを実行できますが、その他の NetBackup の領域や機能へのアクセスは制限されます。RBAC は、ユーザーが表示または管理できる資産も制御します。 |
| RBAC イベントの監査 | NetBackup は、成功した RBAC イベントを監査します。 |
| DR 準備完了 | RBAC 設定は、NetBackup カタログで保護されています。 |
| 以前のインターフェース向けの拡張監査または認証 (`auth.conf`) の構成の継続利用 | 拡張監査はすべてのインターフェースでサポートされます。認証 (`auth.conf`) の構成を、NetBackup 管理コンソールと CLI を通じて引き続き使用できます。これらの以前のインターフェースを使用して、NetBackup Web UI と NetBackup API ではまだサポートされていないワークフローへのアクセスを管理できます。<br>`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。NetBackup アクセス制御 (NBAC) が有効な場合は、Web UI を使用できません。 |

# NetBackup のデフォルトの RBAC の役割

NetBackup のデフォルトの RBAC の役割を使用すると、NetBackup のセキュリティ管理、保護計画の構成とジョブ管理、資産の保護とリカバリなどのタスクに対する委任を行えます。

## NetBackup セキュリティ管理者

NetBackup セキュリティ管理者は、NetBackup 環境で次のタスクを実行します。

- 役割に基づくアクセス制御を管理します。このユーザーは、NetBackup へのアクセスを委任できます。このタスクには、NetBackup にアクセスできるユーザー、ユーザーが持っている役割またはアクセス権、ユーザーがアクセスできる NetBackup 資産などの管理が含まれます。

- セキュリティ管理を監視します。このタスクには、NetBackup ホストと証明書の管理、グローバルセキュリティ設定の管理、セキュリティイベントの表示が含まれます。

### バックアップ管理者

バックアップ管理者は、NetBackup 環境で次のタスクを実行します。

- すべてのジョブアクティビティを管理します。すべてのジョブ操作を監視します。ジョブのキャンセル、一時停止、再開、再起動、削除ができます。
  バックアップ管理者は、特定のジョブエラーが発生したときに、チケットシステムに電子メール通知を送信するように NetBackup を構成することもできます。
- 作業負荷管理者のために保護計画を構成します。
- NetBackup マスターサーバーのバックアップデータサイズについて、使用状況レポートの詳細を表示します。

バックアップ管理者の役割またはカスタムの役割を持つユーザーのアクセス権を (オブジェクトグループを通じて) 制限できます。ただし、バックアップ管理者が表示できるジョブを制限することはできません。この役割を持つユーザーは、すべてのジョブのアクティビティを表示できます。

### 作業負荷管理者

作業負荷管理者は、NetBackup 環境で次のタスクを実行します。

- 自分が開始したジョブを管理します。
- アクセス権が付与された資産を管理します。クラウドプロバイダ、アプリケーションサーバー、資産グループを含む NetBackup 環境の資産を構成します。
- 保護状態を監視し、保護計画に資産をサブスクライブします。
- 管理する資産のリカバリを実行します。

作業負荷管理者の役割を持つユーザーのアクセス権を (オブジェクトグループを通じて) 制限できます。

# 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 2-2

| 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。<br>vssat コマンドを使用して、環境内のドメインを構成します。『NetBackup セキュリティおよび暗号化ガイド』の、NetBackup での AD ドメインまたは LDAP ドメインの追加に関するトピックを参照してください。 |
| 2 | RBAC の役割を確認します。 | NetBackup には、システム管理者、バックアップ管理者、作業負荷管理者の 3 つのデフォルトの役割があります。これらの役割のアクセス権を確認して、どの役割がユーザーに適しているかを判断します。<br>p.14 の「NetBackup のデフォルトの RBAC の役割」を参照してください。<br>必要な場合は、アクセス権のカスタムのセットを使用して、カスタムの役割を作成できます。<br>p.16 の「カスタムロールの追加」を参照してください。 |
| 3 | オブジェクトグループを追加します。 | 資産をオブジェクトグループに編成します。<br>p.20 の「オブジェクトグループの追加」を参照してください。 |
| 4 | アクセスルールを通じて、ユーザーにアクセス権を付与します。 | ユーザー、ユーザーに付与された役割、アクセスできるオブジェクトグループを含めてアクセスルールを作成します。ユーザーに複数のアクセスルールを作成できます。これは、ユーザーが複数の RBAC の役割を持ち、複数のオブジェクトグループへのアクセス権を持てることを意味します。<br>p.27 の「アクセスルールを使用したユーザーに対するアクセス権の追加」を参照してください。 |

# カスタムロールの追加

RBAC のデフォルトの NetBackup ロールではニーズが満たされない場合は、カスタムロールのアクセス権を使用してロールを構成できます。ただし、顧客のロールには特定の制限事項があることに注意してください。p.17 の「カスタムロールの制限事項」を参照してください。

### カスタムロールを追加するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択します。
2. [ロール (Roles)]タブを選択し、[追加 (Add)]をクリックします。
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 [ロールのアクセス権 (Role permissions)]で、そのロールを持つユーザーに、各アクセス権の種類に対して付与するアクセス権またはアクセスの種類を選択します。

たとえば、ユーザーに保護計画の表示を許可し、管理は許可しない場合などです。または、一部のユーザーのみに、資産のリカバリの実行を許可しながら、アプリケーションサーバーや資産グループの構成は許可しない場合があります。

「表 2-3」を参照してください。

5 [追加 (Add)]をクリックします。

## カスタムロールの制限事項

カスタムロールを作成するときは、次の点に注意してください。

- 一部のアクセス権は、デフォルトの RBAC ロールか、NetBackup API で構成されるカスタムロールでのみ利用可能になります。
  - セキュリティ管理者ロールを持つユーザーのみが、[ホスト (Hosts)]の設定を管理できます。
  - バックアップ管理者ロールを持つユーザーのみが、アラートと通知を管理し、使用状況レポートを表示できます。
  - セキュリティ管理者のロールを持つユーザーは、特定の「表示」アクセス権も持ちます。ユーザーは、このようにして資産、アプリケーションサーバー、および保護計画を見つけて、オブジェクトグループに追加できます。カスタムロールを持つユーザーがアクセスルールを作成できるようにする場合は、必ず、カスタムロールに対して適切な表示アクセス権を選択するようにします。
- 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。カスタムロールを作成するときに、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。

## カスタムロールのアクセス権

p.18 の 表 2-3 を参照してください。 に、カスタムロールに対して選択できる個々のアクセス権を説明します。

表 2-3 カスタムロールのアクセス権の説明

| アクセス権のカテゴリ | アクセス権 | アクセス権によって許可されるアクション |
|---|---|---|
| リカバリ (Recovery)<br>ユーザーが 1 つ以上の種類のリカバリを実行することを許可します。<br>ユーザーが表示およびリカバリできるのは、そのユーザーにアクセス権が付与されている資産のみであることに注意します。 | リカバリ (Recover)/リストア (Restore) | バックアップイメージのデータを、元の場所または別の場所にリストアします。 |
| | リカバリポイントの表示 (View Recovery Points) | 資産で利用可能なリカバリポイントを表示します。<br>注意: この権限のみが付与されたユーザーは、Web UI にサインインできません。 |
| | ファイルのダウンロード (Download Files) | インスタントアクセスマウントポイントから個々のファイルをダウンロードします。このアクセス権では、[リカバリポイントの表示 (View Recovery Points)]と[資産の表示 (View Assets)]も利用可能です。 |
| | インスタントアクセス (Instant Access) | インスタントアクセスのイメージを作成します。このアクセス権では、[リカバリポイントの表示 (View Recovery Points)]と[資産の表示 (View Assets)]も利用可能です。 |
| | ファイルのリストア | バックアップイメージの個々のファイルを、ESXi サーバーまたはクラスタにリストアします。このアクセス権では、[リカバリポイントの表示 (View Recovery Points)]と[資産の表示 (View Assets)]も利用可能です。 |
| 保護計画の管理<br>ユーザーが管理または選択できるのは、そのユーザーにアクセス権が付与されている保護計画のみであることに注意します。 | 保護計画の管理 (Manage Protection Plans) | 保護計画を作成、編集、または削除します。保護計画に資産をサブスクライブすることもできます。 |
| | 保護計画の表示 (View Protection Plans) | 利用可能なサブスクリプションを表示し、保護計画に資産をサブスクライブします。 |
| セキュリティ管理<br>NetBackup で、ユーザーが監査ログを表示したり、セキュリティ設定や証明書を管理することを許可します。 | 監査ログの表示 (View audit logs) | NetBackup へのサインイン、セキュリティ設定の変更、バックアップイメージの参照またはリストアを誰が行ったかを参照します。現在のユーザーのアクセス履歴も表示します。 |
| | グローバルセキュリティ設定の管理 (Manage Global Security Settings) | NetBackup でグローバルセキュリティを管理します。これらの設定は、8.0 以前のホストとの通信、ホスト名の自動マッピング、証明書配備のセキュリティレベル、ディザスタリカバリのパスフレーズに影響します。<br>注意: この権限のみが付与されたユーザーは、Web UI にサインインできません。 |
| | [管理 (Manage)]> [証明書 (Certificates)] | ホストのセキュリティ証明書を管理します。証明書の無効化、証明書の再発行を可能にする再発行トークンの作成、新しいトークンの作成の機能が含まれます。 |

| アクセス権のカテゴリ | アクセス権 | アクセス権によって許可されるアクション |
|---|---|---|
| ジョブの管理<br>ユーザーにジョブの表示や、ジョブ操作の管理を許可します。 | ジョブの管理 (Manage Jobs) | 現在のジョブまたは完了したジョブを管理します。ジョブの削除、キャンセル、再起動、一時停止の機能が含まれます。 |
| | ジョブの表示 (View Jobs) | マスターサーバーの現在のジョブまたは完了済みのジョブを表示します。 |
| 資産管理<br>資産の管理、保護計画への資産のサブスクライブ、または資産の表示をユーザーに許可します。<br>ユーザーが管理できるのは、そのユーザーにアクセス権が付与されている資産のみであることに注意します。 | Appserver と資産グループの管理 (Manage Appservers and Asset Groups) | VMware vCenter クレデンシャルを追加します。これを使用すると、NetBackup ではサーバーの追加情報を検出できるため、管理者は、vCenter 内のオブジェクトを表示して選択できます。<br>資産グループを作成および管理して、グループを保護計画にサブスクライブします。 |
| | 資産の管理 (Manage Assets) | サポート対象の作業負荷に関連付けられた資産を管理し、資産を保護計画にサブスクライブします。 |
| | 資産の表示 (View Assets) | サポート対象の作業負荷に関連付けられている資産を表示します。 |
| 役割に基づくアクセス制御<br>特定の作業負荷または資産に対して、また、特定の保護計画に対して、ユーザーに付与するアクセス権を決定するアクセスルールを、管理者が作成することを許可します。 | アクセスルールの管理 (Manage Access Rules) | アクセスルールを作成、管理、または削除します。<br>カスタムロールとオブジェクトグループを作成します。 |
| | アクセスルールの表示 (View Access Rules) | 構成されているアクセスルールを表示します。 |

# カスタムロールの編集または削除

カスタムロール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、このロールを編集または削除できます。

## カスタムロールの編集

**メモ:** ロールのアクセス権を変更すると、そのロール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。

### 役割を編集するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [ロール (Roles)]タブをクリックします。

3 編集するロールを特定してクリックします。

検索では、大文字と小文字が区別されることに注意してください。

4 左下にあるロックアイコンをクリックします。

5 ロールの詳細を編集して、[保存 (Save)]をクリックします。

### カスタムロールの削除

**メモ:** ロールを削除すると、そのロールに割り当てられていたすべてのユーザーが、ロールで提供されていたすべてのアクセス権を失います。

#### 役割を削除する方法

1 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。

2 [ロール (Roles)]タブをクリックします。

3 削除するロールを特定して、そのチェックボックスにチェックマークを付けます。

検索では、大文字と小文字が区別されることに注意してください。

4 [削除 (Remove)]、[削除 (Remove)]の順にクリックします。

# オブジェクトグループの追加

*追加すべきかどうかに迷いがあります。資産のみまたはアプリケーションサーバーのみを対象としたアクセス権をユーザーに付与すると、[VMware]タブでユーザーが表示、実行できることが変わります。(クラウドに影響があるか、ある場合はどのように影響するかについては不明です。)たとえば、アプリケーションサーバーへのアクセス権のみの場合、ユーザーは VM を参照できず、インテリジェントグループの追加や削除は行えないと思われます。*

オブジェクトグループでは、ユーザーが表示または管理できる資産、アプリケーションサーバー、または保護計画を定義できます。特定の作業負荷またはオブジェクトへのアクセス権を付与するオブジェクトグループを作成できます。たとえば、VMware 作業負荷または特定の VMware サーバーに含まれるすべてのオブジェクトへのアクセス権を付与できます。あるいは、すべての資産、アプリケーションサーバー、または保護計画へのアクセス権を付与できます。たとえば、すべての保護計画に対するアクセス権を持つバックアップ管理者は、NetBackup で任意の保護計画を管理できます。

資産またはアプリケーションサーバーのリカバリを管理または実行するには、これらのオブジェクトを含むオブジェクトグループを使用した 1 つ以上のアクセスルールがユーザーに割り当てられている必要があります。資産を管理する、または特定の保護計画に資産をサブスクライブするには、これらの計画を含むオブジェクトグループを使用した 1 つ以上のアクセスルールがユーザーに割り当てられている必要があります。

**メモ:** オブジェクトグループは、ユーザーが何を作成できるかも制限できます。たとえば、バックアップ管理者に、「finance」という単語を含む保護計画へのアクセス権を付与する 1 つのアクセスルールのみ割り当てられていると想定します。この場合、ユーザーは、「finance」という単語が含まれる保護計画のみを作成できます。

### オブジェクトグループを追加するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [オブジェクトグループ (Object groups)]タブ、[追加 (Add)]の順にクリックします。
3. オブジェクトグループの名前と説明を指定します。

   グループ内の資産の種類や、資産が存在する地域を示すキーワードを含めることができます。
4. このオブジェクトグループに追加する資産を選択します。

   次の方法で、このオブジェクトグループの資産を定義できます。

   - 特定の作業負荷内のすべての資産
   - 特定の VMware サーバーとそのすべての VM
   - 特定の VMware サーバーと、そのサーバーに対して選択した VM
   - [すべてにアクセス権を付与 (Grant access to all)]をオンにして、利用可能なすべての資産を含める

   p.22 の「オブジェクトグループの資産の選択」を参照してください。

   これらの資産へのアクセス権が付与されたユーザーは、自分に割り当てられた役割に従って、これらの資産を表示または管理できます。
5. このオブジェクトグループに追加するすべてのアプリケーションサーバーを選択します。

   次の方法で、このオブジェクトグループ用のアプリケーションサーバーを定義できます。

   - 特定の作業負荷内のすべてのアプリケーションサーバー
   - 特定のアプリケーションサーバー
   - [すべてにアクセス権を付与 (Grant access to all)]をオンにして、利用可能なすべてのアプリケーションサーバーを含める

   p.23 の「オブジェクトグループのアプリケーションサーバーの選択」を参照してください。

   これらの資産へのアクセス権が付与されたユーザーは、自分に割り当てられた役割に従って、これらのアプリケーションサーバーを表示または管理できます。
6. このオブジェクトグループに追加するすべての保護計画を選択します。

次の方法で、このオブジェクトグループ用の保護計画を定義できます。

- 特定の保護計画
- [すべてにアクセス権を付与 (Grant access to all)]をオンにして、すべての保護計画を含める

p.24 の「オブジェクトグループの保護計画の選択」を参照してください。

これらの保護計画へのアクセス権が付与されたユーザーは、自分に割り当てられた役割に従って、これらの計画を表示または管理できます。「表示」権限を持つユーザーは、オブジェクトグループの保護計画に資産をサブスクライブすることもできます。

**7** [保存 (Save)]をクリックします。

## オブジェクトグループの資産の選択

オブジェクトグループに含まれている資産をプレビューできます。p.25 の「オブジェクトグループに含まれる資産、アプリケーションサーバー、または保護計画のプレビュー」を参照してください。

**特定の作業負荷にすべての資産を含めるには**

◆ [作業負荷の追加 (Add workload)]をクリックし、含める作業負荷形式を選択します。

たとえば、すべての VMware 資産を含めるには、[VMware]を選択します。

**特定の VMware サーバーとその VM すべてを含めるには**

**1** [資産 (Assets)]の下の[作業負荷の追加 (Add workload)]をクリックし、含める作業負荷の種類を選択します。

たとえば、すべての VMware 資産を含めるには、[VMware]を選択します。

**2** [VMware サーバーの追加 (Add VMware server)]をクリックします。

**3** 含める vCenter の名前を選択します。または、vCenter 名をクリックして、サーバー、クラスタ、またはデータセンターを参照します。

**4** [保存 (Save)]をクリックします。

**特定の VMware サーバーと、そのサーバーに対して選択した VM を含めるには**

**1** [資産 (Assets)]の下の[作業負荷の追加 (Add workload)]をクリックし、含める作業負荷の種類を選択します。

たとえば、すべての VMware 資産を含めるには、[VMware]を選択します。

**2** [VMware サーバーの追加 (Add VMware server)]をクリックします。

**3** 含める vCenter の名前を選択します。または、vCenter 名をクリックして、サーバー、クラスタ、またはデータセンターを参照します。

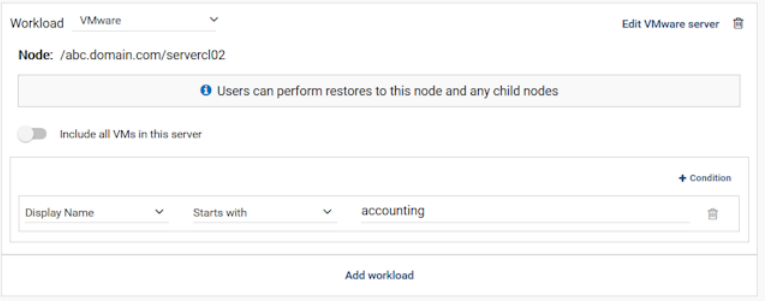
4 [保存 (Save)]をクリックします。

5 [このサーバー内のすべての VM を含める (Include all VMs in this server)]をオフにします。

6 1 つ以上の条件を定義します。条件では大文字と小文字が区別されます。

条件が複数ある場合は、オペレータ (AND または OR) を選択します。

次の例では、VMware サーバー abc.domain.com 上のクラスタ servercl02 からの、accounting で始まる表示名を持つ、VMware 作業負荷の資産がオブジェクトグループに含められます。




## オブジェクトグループのアプリケーションサーバーの選択

オブジェクトグループに含まれている資産をプレビューできます。p.25 の「オブジェクトグループに含まれる資産、アプリケーションサーバー、または保護計画のプレビュー」を参照してください。

### 特定の作業負荷内のすべてのアプリケーションサーバーを含めるには

◆ [アプリケーションサーバー (Application servers)]の下の[作業負荷の追加 (Add workload)]をクリックし、含める作業負荷の種類を選択します。

たとえば、すべての VMware アプリケーションサーバーを含めるには、[VMware]を選択します。

**特定の作業負荷内の特定のアプリケーションサーバーを含めるには**

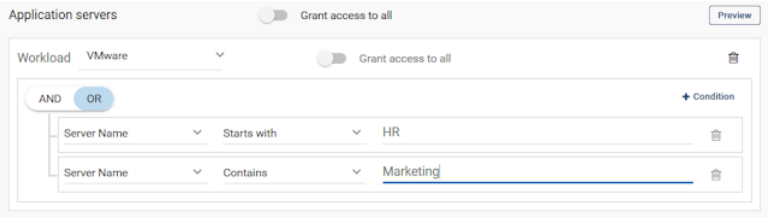
1 [アプリケーションサーバー (Application servers)]の下の[作業負荷の追加 (Add workload)]をクリックし、含める作業負荷の種類を選択します。

たとえば、すべての VMware アプリケーションサーバーを含めるには、[VMware]を選択します。

2 1 つ以上の条件を追加します。条件では大文字と小文字が区別されます。

条件が複数ある場合は、オペレータ (AND または OR) を選択します。

次の例では、名前が HR で始まるか、名前に Marketing が含まれるサーバーを持つ VMware 作業負荷のアプリケーションサーバーが、オブジェクトグループに含められます。




## オブジェクトグループの保護計画の選択

オブジェクトグループに含まれている資産をプレビューできます。p.25 の「オブジェクトグループに含まれる資産、アプリケーションサーバー、または保護計画のプレビュー」を参照してください。

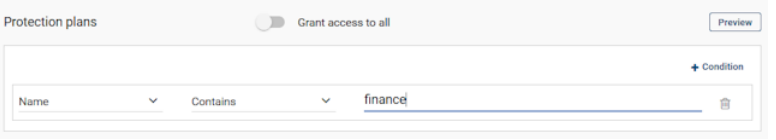
**特定の保護計画を含めるには**

1 [保護計画 (Protection plans)]の[条件の追加 (Add condition)]をクリックします。

2 条件の属性を選択します。条件では大文字と小文字が区別されます。

条件が複数ある場合は、オペレータ (AND または OR) を選択します。

次の例では、名前に finance が含まれる保護計画がオブジェクトグループに含められます。



### オブジェクトグループに含まれる資産、アプリケーションサーバー、または保護計画のプレビュー

オブジェクトグループに含まれているオブジェクトをプレビューできます。オブジェクトグループは、オブジェクトが NetBackup 環境に追加または削除されると動的に変化することに注意してください。バックアップの実行時に、バックアップ時に利用可能なオブジェクトを反映するようにオブジェクトグループがランタイムに更新されます。

**オブジェクトグループに含まれる資産、アプリケーションサーバー、または保護計画をプレビューするには**

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [オブジェクトグループ (Object Groups)]タブ、編集するオブジェクトグループの順にクリックします。
3. [資産 (Assets)]、[アプリケーションサーバー (Application Servers)]、または[保護計画 (Protection Plans)]の右側で、[プレビュー (Preview)]をクリックします。
4. NetBackup は、構成した条件を満たしているオブジェクトのリアルタイムビューを表示します。プレビューでオブジェクトをソートまたは検索できます。検索では、大文字と小文字が区別されることに注意してください。
5. プレビューが終了したら、上部にある[閉じる (Close)]アイコンを右クリックします。

## オブジェクトグループに含まれる資産、アプリケーションサーバー、または保護計画のプレビュー

オブジェクトグループにどのような資産、アプリケーションサーバー、または保護計画が関連付けられているかをプレビューできます。そのオブジェクトグループへのアクセス権を持つユーザーは、オブジェクトグループ内のそれらの項目を表示または管理できます。プレビューには、プレビューの表示時に利用可能な資産、サーバー、または計画のみが含まれます。Web UI で環境または計画に項目を追加または削除すると、オブジェクトグループは動的に変更されます。

**オブジェクトグループの資産または保護計画をプレビューするには**

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [オブジェクトグループ (Object groups)]タブをクリックします。
3. 編集するオブジェクトグループの名前をクリックします。
4. [資産 (Assets)]、[アプリケーションサーバー (Application Servers)]、または[保護計画 (Protection Plans)]の横で、[プレビュー (Preview)]をクリックします。
5. プレビューパネルを閉じます。

# オブジェクトグループの編集または削除

オブジェクトグループの資産、アプリケーションサーバー、または保護計画の変更または削除が必要な場合は、オブジェクトグループを編集または削除できます。

## オブジェクトグループの編集

**メモ:** オブジェクトグループを変更すると、そのオブジェクトグループが含まれるすべてのアクセスルール (と関連付けられているユーザー) に変更が適用されます。

### オブジェクトグループを編集するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [オブジェクトグループ (Object groups)]タブをクリックします。
3. 編集するオブジェクトグループを特定してクリックします。

   検索では、大文字と小文字が区別されることに注意してください。
4. 左下にあるロックアイコンをクリックします。
5. オブジェクトグループの名前または説明を編集します。
6. 資産、アプリケーション、サーバーまたは保護計画を編集します。
7. [保存 (Save)]をクリックします。

## オブジェクトグループの削除

**メモ:** オブジェクトグループを削除すると、そのオブジェクトグループに関連付けられているすべてのユーザーに変更が影響します。

### オブジェクトグループを削除する方法

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [オブジェクトグループ (Object groups)]タブをクリックします。
3. 削除するオブジェクトグループを特定して、そのチェックボックスにチェックマークを付けます。

   検索では、大文字と小文字が区別されることに注意してください。
4. [削除 (Remove)]、[削除 (Remove)]の順にクリックします。

# アクセスルールを使用したユーザーに対するアクセス権の追加

NetBackup Web UI で、1 つ以上のアクセスルールを通じて NetBackup へのアクセス権をユーザーに付与します。アクセスルールは、次のもので構成されます。

- ユーザーまたはユーザーグループ。これは、ローカルまたはドメインのいずれかのユーザーまたはグループである可能性があります。
- ユーザーが持つアクセス権を定義するロール。
  ロールのアクセス権は、ユーザーが実行できるアクションの種類を決定します。ユーザーが環境内で何にアクセスできるかは、オブジェクトグループによって決まります。
- ユーザーが表示または管理できる資産、アプリケーションサーバー、または保護計画を定義する、オブジェクトグループ。
  注意: セキュリティ管理者のロールを持つユーザー向けにアクセスルールを作成すると、そのユーザーは、すべてのオブジェクトまたは資産へのアクセス権を持ちます。

アクセスルールを作成する前に、次の手順を実行する必要があります。

- ドメインユーザーを追加するには、NetBackup で Active Directory または LDAP ドメインを構成する必要があります。
  `vssat` コマンドを使用して、環境内のドメインを構成します。『NetBackup セキュリティおよび暗号化ガイド』を参照してください。
  ローカルユーザーには、この認証は不要です。
- ユーザーにどの役割を付与するかを決定します。
  p.14 の「NetBackup のデフォルトの RBAC の役割」を参照してください。
- ユーザーにどの資産またはアプリケーションサーバーへのアクセス権を付与するかを決定し、適切なオブジェクトグループを選択します。または、適切なオブジェクトグループを作成します。
  p.20 の「オブジェクトグループの追加」を参照してください。
- ユーザーに付与する役割のアクセス権は、ユーザーにアクセス権が付与されるオブジェクトグループを使用してさらに制限できます。p.29 の「特定のオブジェクトまたは資産のロールアクセス権を制限する方法」を参照してください。

**ユーザーのアクセス権を追加するには**

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [アクセスルール (Access rules)]タブ、[追加 (Add)]の順にクリックします。

3 ドメインとユーザー名を入力します。このユーザーを検証するには、+ 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 | *username* | root |
| ドメインユーザー | *DOMAIN¥username* | WINDOWS¥Administrator |

4 ユーザーに割り当てるアクセス権を含む役割を選択します。

5 ユーザーにアクセス権を付与する資産が含まれるオブジェクトグループを選択します。

セキュリティ管理者の役割を持つユーザーは、すべてのオブジェクトまたは資産へのアクセス権を持つことに注意してください。その役割に利用可能な唯一の選択肢は、[すべてのオブジェクト (All objects)]です。

6 アクセスルールの説明を入力して、[保存 (Save)]をクリックします。

# ユーザーのアクセスルールの編集または削除

組織内でユーザーの役割が変わった場合や、環境内の資産に対するユーザーのアクセス権を変更する必要がある場合には、次の選択肢があります。

- ユーザーのアクセスルールを編集して、別の RBAC の役割または別のオブジェクトグループを選択します。
p.29 の「ユーザーのアクセスルールの編集」を参照してください。
- カスタムの役割を使用する場合は、RBAC の役割に対する権限を変更します。アクセス権を変更すると、その役割に関連付けられているその他すべてのユーザーに対するアクセス権も変更されることに注意してください。
p.19 の「カスタムロールの編集または削除」を参照してください。
- ユーザーが表示または管理できる資産、アプリケーションサーバー、または保護計画を決定するオブジェクトグループの設定を変更します。これらの設定を変更すると、このオブジェクトグループに関連付けられているその他のユーザーのアクセス権も変更されることに注意してください。
p.26 の「オブジェクトグループの編集または削除」を参照してください。
- ユーザーのアクセスルールを削除して、ユーザーが、アクセスルールに定義されている役割のアクセス権またはオブジェクトグループのアクセス権を持たないようにします。
p.29 の「ユーザーのアクセスルールの削除」を参照してください。
ユーザーが現在サインインしている場合は、すべてのユーザーをサインアウトするために API の `Gateway DELETE /user-sessions` を使用します。

## ユーザーのアクセスルールの編集

ユーザーに対する役割のアクセス権や、ユーザーが表示または管理できる資産、アプリケーションサーバー、または保護計画を変更する場合は、アクセスルールを編集します。アクセスルールに加えた変更は、そのユーザーのみに影響します。

**ユーザーのアクセスルールを編集するには**

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [アクセスルール (Access rules)]タブをクリックします。
3. 編集するユーザーの名前 (つまり、ユーザーに関連付けられたアクセスルール) を特定してクリックします。

   検索では、大文字と小文字が区別されることに注意してください。
4. 左下にあるロックアイコンをクリックします。
5. 別の役割またはオブジェクトグループを選択します。
6. [保存 (Save)]をクリックします。
7. 手順 3 から手順 6 を繰り返して、ユーザーのその他のアクセスルールを編集します。

## ユーザーのアクセスルールの削除

アクセスルールの役割のアクセス権とオブジェクトグループのアクセス権を無効化する場合は、ユーザーのアクセスルールを削除します。アクセスルールを削除すると、ルールに構成されているユーザーにのみ影響します。ユーザーがその他のアクセスルールから引き継いだすべてのアクセス権は引き続き保持されます。

**ユーザーのアクセスルールを削除するには**

1. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
2. [アクセスルール (Access rules)]タブをクリックします。
3. ユーザーの名前を見つけて、削除するアクセスルールにチェックマークを付けます。

   検索では、大文字と小文字が区別されることに注意してください。
4. [削除 (Remove)]、[削除 (Remove)]の順にクリックします。

# 特定のオブジェクトまたは資産のロールアクセス権を制限する方法

セキュリティ関連のアクセス権およびジョブのアクセス権は、特定のホストまたは資産に限定できません。たとえば、ジョブの表示または管理のアクセス権を持つユーザーは、すべてのジョブを表示および管理できます。バックアップ管理者に関連するその他のアクセス

権と、作業負荷管理者のアクセス権は、オブジェクトグループの基準によって制限できます。

**表 2-4　ロールのアクセス権と、オブジェクトグループを使用してアクセス権を制限する方法**

| アクセス権 | オブジェクトグループをフィルタおよび制限する方法 |
|---|---|
| リカバリ (Recover)/リストア (Restore) | VMware リカバリポイント: 表示名 VM 絶対パス<br>クラウド資産リカバリポイント: 表示名、ベンダー、構成 ID |
| リカバリポイントの表示 (View Recovery Points) | VMware リカバリポイント: 表示名 VM 絶対パス<br>クラウド資産リカバリポイント: 表示名、ベンダー、構成 ID |
| ファイルのダウンロード (Download Files) | VMware リカバリポイント: 表示名 VM 絶対パス<br>クラウド資産リカバリポイント: 表示名、ベンダー、構成 ID |
| インスタントアクセス (Instant Access) | VMware リカバリポイント: 表示名 VM 絶対パス<br>クラウド資産リカバリポイント: 表示名、ベンダー、構成 ID |
| ファイルのリストア | VMware リカバリポイント: 表示名 VM 絶対パス<br>クラウド資産リカバリポイント: 表示名、ベンダー、構成 ID |
| 保護計画の管理 (Manage Protection Plans) | 名前、説明 |
| 保護計画の表示 (View Protection Plans) | 名前、説明 |
| 監査ログの表示 (View audit logs) | すべてのログまたはログなし |
| グローバルセキュリティ設定の管理 (Manage global security settings) | すべての設定または設定なし |
| [管理 (Manage)]>[証明書 (Certificates)] | すべての証明書または証明書なし |
| ジョブの管理 (Manage Jobs) | すべてのジョブまたはジョブなし |
| ジョブの表示 (View Jobs) | すべてのジョブまたはジョブなし |
| Appserver と資産グループの管理 (Manage Appservers and Asset Groups) | ユーザーが表示できる保護計画: 名前、説明<br>アプリケーションサーバー: サーバー名、サーバー形式 |
| 資産の管理 (Manage Assets) | ユーザーが表示し、資産をサブスクライブできる保護計画: 名前、説明<br>アプリケーションサーバー: サーバー名、サーバー形式 |

| アクセス権 | オブジェクトグループをフィルタおよび制限する方法 |
| --- | --- |
| 資産の表示 (View Assets) | VMware: 表示名、VM の絶対パス<br>クラウド: 表示名、ベンダー、構成 ID |
| アクセスルールの管理 (Manage Access Rules) | すべてのオブジェクトまたはオブジェクトなし |
| アクセスルールの表示 (View Access Rules) | すべてのオブジェクトまたはオブジェクトなし |

3

# 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。



## NetBackup の監査について

監査記録は、NetBackup 環境でユーザーが開始した操作の記録です。基本的に、監査はだれが何をいつ変更したか答えるのに役立つ情報を集めます。NetBackup 操作の監査は次の領域の情報の提供に役立ちます。

| | |
|---|---|
| 概要の追跡 | お客様は NetBackup 環境の予想外の変更を調査するときに、監査記録から推測することができます。たとえば、クライアントまたはバックアップパスの付加によりバックアップ時間が大幅に増加したことが分かる場合があります。監査レポートは、ポリシーの変更に対応するためにスケジュールまたはストレージユニットの構成への調節が必要な可能性があることを示すことがあります。 |
| 規制コンプライアンス | 監査はだれが何をいつ変更したかのレコードを作成します。レコードはサーベンスオクスリー法 (SOX) で必要とされるようなガイドラインに従います。 |
| 企業の変更管理 | 内部変更の管理ポリシーを固守する必要があるお客様のために NetBackup の監査はそのようなポリシーを固守するための方式を提供します。 |
| トラブルシューティング | NetBackup の監査からの情報は NetBackup サポートがお客様のために問題をトラブルシューティングするのに役立ちます。 |

NetBackup がセキュリティイベントで監査する処理を、NetBackup Web ユーザーインターフェースまたは NetBackup 管理コンソールで表示できます。監査イベントのすべての詳細を `nbauditreport` コマンドまたは NetBackup OpsCenter で表示できます。

## NetBackup Audit Manager について

NetBackup Audit Manager (nbaudit) はマスターサーバー上で動作し、監査レコードは Enterprise Media Manager (EMM) データベースに保持されます。デフォルトでは、監査は有効にされています。

Audit Manager は監査情報に対する問い合わせおよびレポートのための機構を提供します。たとえば、管理者は、次の条件に基づいて特定の情報を検索できます。

- 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

Audit Manager は、監査レコードを作成するときに次の方法で動作します。

- 監査レコードは、エントリの詳細を最大 4096 文字に制限します。(たとえば、ポリシー名。) 残りの文字は監査データベースに格納されるときに切り捨てられます。
- 監査レコードは、リストアイメージ ID を最大 1024 文字に制限します。残りの文字は監査データベースに格納されるときに切り捨てられます。
- ロールバック操作は監査されません。
  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。

## 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。

| | |
|---|---|
| ポリシーの処理 | ポリシーの属性、クライアント、スケジュール、バックアップ対象リストの追加、削除、更新。 |
| 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、または削除すると、監査レコードが作成されます。 |
| 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。<br>**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。 |
| 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。 |
| ディスクプールとボリュームプールの処理 | ディスクプールまたはボリュームプールの追加、削除、または更新。 |

| | |
|---|---|
| カタログ情報 | この情報には次のものが含まれます。<br>■ イメージの検証および有効期限終了。<br>■ フロントエンド使用状況データに送信される要求の読み取り。 |
| 証明書管理 | 証明書の作成、取り消し、更新、配備、および特定の証明書エラー。 |
| 証明書検証エラー (CVF) | SSL ハンドシェークエラー、無効化された証明書、またはホスト名の検証エラーが原因で失敗した接続試行。 |
| 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。 |
| 保留操作 | 保留操作の作成、変更および削除。 |
| ホストデータベース | NetBackup ホストデータベース関連の操作。 |
| ログイン試行 | NetBackup 管理コンソール、NetBackup Web UI または NetBackup API への、成功または失敗したすべてのログイン試行。 |
| セキュリティ構成 | セキュリティ構成の設定に加えられた変更に関連する情報。 |
| リストアジョブの開始 | 他の形式のジョブが開始されている場合、NetBackup では監査が実行されません。たとえば、バックアップジョブが開始されている場合、NetBackup では監査が実行されません。 |
| NetBackup Audit Manager (`nbaudit`) の開始と停止。 | 監査機能が無効になっていても、`nbaudit` manager の起動と停止は常に監査されます。 |
| 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 (**処理に成功しましたが監査に失敗しました** (`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。 |
| 認証の失敗 | NetBackup Web UI、NetBackup API、または拡張監査を使用する場合は、認証の失敗が監査されます。 |

## NetBackup によって監査されない処理

次の処理は監査されないため、監査レポートに表示されません。

| | |
|---|---|
| 任意の失敗した処理。 | NetBackup により、失敗した処理が NetBackup のエラーログに記録されます。失敗した試行で NetBackup のシステム状態が変更されることはないので、失敗した処理は監査レポートに表示されません。 |
| 設定変更の影響。 | NetBackup の構成への変更の結果は監査されません。たとえば、ポリシーの作成は監査されますが、その作成から生じるジョブは監査されません。 |

| | |
|---|---|
| 手動で開始されたリストアジョブの完了状態。 | リストアジョブの開始は監査されますが、ジョブの完了状態は監査されません。手動で開始されたかどうかにかかわらず、他のどのジョブ形式の完了状態も監査されません。完了の状態はアクティビティモニター (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。 |

NetBackup は、NetBackup アクセス制御 (NBAC) が有効でないかぎり、次の処理も監査しません。ただし、NBAC が有効なときは、NetBackup Web UI を使用できません。

- `bp.conf` ファイル (UNIX の場合) またはレジストリ (Windows の場合) への変更。`bp.conf` ファイルまたはレジストリの手動変更は監査されません。
- ホストプロパティの処理。

# 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。NetBackup の監査について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』を参照してください。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。

**セキュリティイベントと監査ログを表示するには**

◆ 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。

- 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。各監査カテゴリについて、最大で 1,000 個のイベントが表示されます。

4

# ホストマッピングと証明書の管理

この章では以下の項目について説明しています。



## NetBackup のセキュリティ管理と証明書について

NetBackup は、セキュリティ証明書を使って NetBackup ホストを認証します。セキュリティ証明書は X.509 公開キーインフラストラクチャ (PKI) 標準に適合しています。マスターサーバーは、認証局 (CA) として動作し、ホストに電子証明書を発行します。NetBackup では、ホスト通信にトランスポート層セキュリティ (TLS) プロトコルを使用します。このプロトコルでは、各ホストがそのセキュリティ証明書を提示するとともに、認証局 (CA) の証明書に対してピアホストの証明書を検証する必要があります。

NetBackup 8.1 とそれ以降のホストは、セキュアモードでのみ相互に通信できます。これらのホストが通信を正常に行うには、認証局 (CA) 証明書とホスト ID ベースの証明書が必要です。

### NetBackup 8.0 以前のホストのセキュリティ証明書

NetBackup が 8.0 以前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 はシステムによってランダムに生成され、ハードウェアのどのプロパティとも関連付けられていません。ホスト ID はホスト名を変更しても変更されません。ホスト ID はホストを識別するために多くの証明書管理操作で使われます。

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。
- マスター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、マスターサーバークラスタが *N* 個のノードで構成される場合、そのマスター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。

マスターサーバーは認証局 (CA) で、証明書 (または失効した証明書) を持つすべてのホスト ID のリストを保持します。マスターサーバーは NetBackup 8.1 以降のホストにホスト ID ベースの証明書を割り当て、ホスト情報を `nbdb` データベースに格納します。

# NetBackup ホスト情報の表示

ホストアプリケーションには、マスターサーバー、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。

---

NetBackup 8.0 以前の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もあります。NetBackup は、クラスタの仮想名のホスト名や完全修飾ドメイン名 (FQDN) を含む、クラスタ名も検出します。

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.47 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。[NetBackup ホスト ID をホスト名に自動的にマッピングする (Automatically map NetBackup host ID to hostnames)]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. ホストを選択し、[共有マッピングと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。

# ホストの証明書が有効でなくなったときの証明書の再発行

ホストの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、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。

詳細情報

## トークン付きの証明書の再発行

ホストの証明書を再発行する必要があり、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. 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。
3. トークン名を入力し、トークンの有効期間を指定します。

4 [作成 (Create)]をクリックします。

5 [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。

6 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。

**トークンなしで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 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。

### トークンなしで証明書を再発行する機能の無効化

トークンなしで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 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。

## 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.42 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、マスター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に、ホスト ID をリセットします。ホスト ID、ホスト名、またはホストの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。次にマスター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。

**ホストのマッピング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、[8.0 以前のホストとの安全でない通信を有効にする (Enable insecure communication with 8.0 and earlier hosts)]オプションを有効にすると、NetBackup は、8.0 またはそれ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すことができます。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。

---

# セキュリティ証明書の管理

証明書を表示および無効化して、認証局 (CA) の情報を表示できます。証明書管理、証明書配備、および証明書管理ユーティリティについて詳しくは、『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。ホストのトークンを再発行するには、次の参照してください。

p.40 の「ホストの証明書が有効でなくなったときの証明書の再発行」を参照してください。

## 証明書の表示

ホストに発行されたすべてのホスト ID 証明書の詳細を表示できます。

**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。

   マスターサーバーの証明書のリストが表示されます。

2. 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。

## 証明書の無効化

NetBackup ホストの ID ベースの証明書を無効化するときに、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マスターサーバー Web サービスと通信することはできません。

『NetBackup セキュリティおよび暗号化ガイド』の、ホスト ID ベースの証明書の無効化に関する説明を参照してください。

セキュリティのベストプラクティスとして、ホストに証明書が配備されているかどうか、ホストから正常に削除されているかどうかに関係なく、すでにアクティブでないホストの証明書を NetBackup セキュリティ管理者が明示的に無効化することが推奨されます。

---

**メモ:** マスター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 の動作が停止する可能性があります。

---

**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. 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。
3. [証明書の無効化 (Revoke certificate)]、[はい (Yes)]の順にクリックします。

### 認証局の詳細と指紋の表示

マスターサーバーまたは認証局との間で安全に通信するために、ホストの管理者は、CA 証明書を個々のホストのトラストストアに追加する必要があります。マスター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。

**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)]、[ホスト (Hosts)]の順に選択します。
2. 上部にある[認証局を表示 (View Certificate Authority)]をクリックします。
3. 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。
4. この指紋情報をホストの管理者に提供します。

## トークンの管理

ホストの承認に必要な場合にトークンを作成し、再度必要になった場合に、トークンを検索してコピーできます。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。

証明書配備のセキュリティレベルによっては、ホストに新しい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。

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。

### トークンの作成

セキュリティレベルに応じて、マスター以外の NetBackup ホストは、ホスト ID ベースの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。マスターサーバーの NetBackup 管理者はトークンを生成し、それをマスター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、マスター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。

証明書が紛失、破損、または期限切れのため現時点で有効でない状態の証明書を持つ 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。

**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. 右上隅の[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。

## 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、将来使うためにコピーできます。

**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** 右上の［表示 (Show)］、［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** 右上隅の［削除 (Delete)］をクリックします。

5

# グローバル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。



## 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、すべてのホストを現在の NetBackup 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マスターサーバーを NetBackup 8.1 以降にアップグレードする必要があります。

OpsCenter サーバーと通信するには、安全でない通信を有効に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 以前のホストとの安全でない通信を有効にする (Enable insecure communication with NetBackup 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。[NetBackup ホスト ID をホスト名に自動的にマッピングする (Automatically map NetBackup host ID to hostnames)] 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. [NetBackup ホスト ID をホスト名に自動的にマッピングする (Automatically map NetBackup host ID to hostnames)]をオフにします。
3. [保存 (Save)]をクリックします。

# 証明書配備のセキュリティレベルの選択

NetBackup は、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、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、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、証明書配備、CRL 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。

**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 [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。

証明書は、インストール中、ホストの管理者がマスターサーバーの指紋を確認した後に、ホストに配備されます。セキュリティレベルにより、ホストに認証トークンが必要かどうかが決定されます。

| | |
|---|---|
| 最高 (Very High) | NetBackup は、すべての新しい証明書要求に認証トークンを求めます。 |
| 高 (High) (デフォルト) | ホストがマスター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。<br>『NetBackup セキュリティおよび暗号化ガイド』の、証明書配備のセキュリティレベルに関する説明を参照してください。 |
| 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、NetBackup は、認証トークンなしで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

カタログバックアップ中に、NetBackup は、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。

『NetBackup セキュリティおよび暗号化ガイド』の、ディザスタリカバリの設定に関する説明を参照してください。

**ディザスタリカバリ用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 [安全な通信 (Secure communication)]をクリックします。

3 [ディザスタリカバリ (Disaster recovery)]タブで、パスフレーズを入力して確認します。

4 [保存 (Save)]をクリックします。

6

# Web UI のトラブルシューティング

この章では以下の項目について説明しています。



## NetBackup Web UI にアクセスするためのヒント

NetBackup が正しく構成されている場合は、次の URL でマスターサーバーにアクセスできます。

https://*masterserver*/webui/login

マスターサーバーの 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 6-1** 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。<br>https://www.veritas.com/support/ja_JP/article.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。<br>https://www.veritas.com/support/ja_JP/article.100042950 |
| 手順 4 | nbwebservice が起動していることを確認します。 | 詳しくは nbwebservice ログを確認してください。 |
| 手順 5 | vnetd -http_api_tunnel が実行されていることを確認します。 | vnetd -http_api_tunnel サービスが実行されていることを確認します。<br>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 | サードパーティの証明書にアクセス可能で、期限切れになっていないことを確認します。 | java keytool コマンドを使用して nbwebservice.jks ファイルを検証します。<br>nbwebgroup に、nbwebservice.jks ファイルにアクセスするためのアクセス権があるかどうかを確認します。<br>ベリタスのテクニカルサポートに問い合わせてください。 |

## 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 6-1 のすべての手順を試します。

## Web UI にアクセスしようとすると証明書の警告が表示される

NetBackup Web サーバーが Web ブラウザによって信頼されていない CA によって発行された証明書を使用している場合、証明書の警告が表示されます。デフォルトの NetBackup Web サーバー証明書は、Web ブラウザによって信頼されていない NetBackup CA によって発行されます。

**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、サードパーティの証明書を構成します。

   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。

2. 問題が解決しない場合は、ベリタスのテクニカルサポートに問い合わせてください。

## クラスタ設定でのフェールオーバー後に証明書の警告が表示される

**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. configureTPCerts コマンドを、すべてのクラスタノードで実行します。

   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。

2. configureTPCerts コマンドを実行したら、必ず nbwmc と vnetd サービスを再起動します。

# ユーザーが NetBackup Web UI の作業負荷資産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.15 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。

- アクセスルールで指定されたユーザー名、またはユーザー名とドメイン名が、ユーザーのクレデンシャルと一致していることを確認します。
- ユーザーのアクセスルールを[セキュリティ(Security)]、[RBAC]で確認します。これらのアクセスルールに関連付けられている役割のアクセス権やオブジェクトグループの変更が必要になる場合があります。ただし、これらの種類の変更が、該当する役割またはオブジェクトグループに関連付けられてい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、ユーザーのアクセスルール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アクセスルールをそれぞれ編集する必要があります。
- ユーザーのアクセスルールの変更は、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、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。