NetBackup™ Web UI セキュリティ管理者ガイド

リリース 8.2

VERITAS™

NetBackup Web UI セキュリティ管理者ガイド

最終更新日: 2019-06-28

法的通知と登録商標

Veritas、Veritas ロゴ、NetBackupは Veritas Technologies LLC または同社の米国とその他の国における関連会社の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、サードパーティの所有物であることをベリタスが示す必要のあるサードパーティソフトウェア(「サードパーティプログラム」)が含まれている場合があります。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。このベリタス製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

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

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

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については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。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202、「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となります。業務用またはホスト対象サービスとしてベリタスによって提供されている場合でも同様です。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 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、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 のセキュリティ、証明書、RBAC、API キー、ユーザーセッション、ロックされている NetBackup ユーザーアカウントを管理できます。

- 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。Web UI は次の作業負荷をサポートします。
  - クラウド
  - Red Hat Virtualization (RHV)
  - VMware
- 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。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では、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。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。
- 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、主に資産またはインテリジェント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

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。

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 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。 「*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。
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。
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。 VMware と RHV の場合、[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。
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。
NetBackup 証明書	NetBackup CA から発行されたセキュリティ証明書。
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。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。 注意: 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。

用語	定義
役割	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する保護計画を選択する処理です。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、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 以降では、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。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。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.14 の「権限を持つユーザー」を参照してください。

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。

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 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.19 の「RBAC の構成」を参照してください。

NetBackup セキュリティ管理者を 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必要ありません。

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.14 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。
https://www.veritas.com/content/support/ja_JP/doc-viewer:21733320-136680179-0/v135179383-136680179.html
- 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 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。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」

ユーザー名とパスワ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、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。

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

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://*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. ［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。

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 1-2 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
Root ユーザー、管理者、拡張監査ユーザー	フル
nbasecadmin 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。
デフォルトまたはカスタム RBAC ロールのユーザー	ユーザーに応じて異なる

NetBackup ダッシュボード

NetBackup ダッシュボードは、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 1-3 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	環境内の NetBackup のホスト ID ベースのセキュリティ証明書または外部証明書に関する情報を表示します。 外部証明書では、NetBackup 8.2 ホストに関する次の情報が表示されます。 ■ ホストの合計。ホストの合計数です。ホストはオンラインになっており、NetBackup マスターサーバーと通信できる必要があります。 ■ 不明。外部証明書が登録されていないホストの数です。 ■ 有効。外部証明書が登録されているホストの数です。 ■ 期限切れ。期限切れの外部証明書を持つホストの数です。 詳しくは、[証明書 (Certificates)]、[外部証明書 (External certificates)]の順に移動して参照してください。 p.51 の「NetBackup のセキュリティ管理と証明書について」を参照してください。
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、ログオンイベントのレコードが含まれます。[監査イベント (Audit events)]ビューには、ユーザーが NetBackup マスターサーバーで開始したイベントが含まれます。

2

役割ベースのアクセス制御の管理

この章では以下の項目について説明しています。

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。 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。 `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。

- 役割ベースの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 のホストと証明書、グローバルセキュリティ設定、セッション、ロックされた NetBackup アカウント、API キーの管理が含まれます。この役割を持つユーザーは、セキュリティイベントも表示できます。

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。

- クラウドプロバイダ、アプリケーションサーバー、およびインテリジェントグループを構成します。
- 作業負荷管理者のために保護計画を構成します。
- 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。
  また、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 を構成できます。
- メディアサーバー重複排除プール (MSDP) と AdvancedDisk のすべてのストレージオプションを構成します。
- NetBackup とクラウドおよび OpenStorage のオプションとの連携を構成します。
- リカバリポイントを管理します。リカバリポイントのリストア、期限切れ、コピー、複製の処理を実行できます。
- 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。
- 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。 `vssat` コマンドを使用して、環境内のドメインを構成します。 p.36 の「AD または LDAP ドメインの追加」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。 p.17 の「NetBackup のデフォルトの RBAC の役割」を参照してください。 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。 p.19 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。	NetBackup 環境で資産、アプリケーションサーバー、または保護計画を編成するオブジェクトグループを作成します。オブジェクトグループにより、たとえばユーザーが表示または管理できる資産が決まります。 p.25 の「 オブジェクトグループを作成する手順」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、ユーザーがアクセスできるオブジェクトグループを含む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。 p.32 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、カスタム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。「「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。

カスタムロールのアクセス権

表 2-3 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
ジョブの管理 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。

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
資産管理 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。 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。	アプリケーションサーバーと資産グループの管理	クレデンシャルを追加すると、NetBackup は作業負荷の追加情報を検出できます。たとえば、ユーザーが VMware クレデンシャルを追加すると、NetBackup は VMware サーバーの詳細を検出します。その後、ユーザーは vCenter 内のオブジェクトを表示して選択できます。 資産グループ (または「インテリジェント」グループ) を作成して管理し、グループを保護計画にサブスクライブします。バックアップが実行されると、NetBackup はインテリジェントグループの条件を満たすすべての VM のリストを動的に作成します。たとえば、ユーザーは「Finance Department」という名前のインテリジェント VM グループを作成できます。ユーザーは、特定の文字列「finance」で始まる表示名を持つすべての VM がグループに含まれるように、条件を追加できます。
	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。
ストレージ管理 (Storage Management) ユーザーにストレージサーバーとストレージユニットの表示と管理を許可します。	ストレージの管理	ストレージサーバーとストレージユニットを作成、表示、編集、または削除します。 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。
	ストレージの表示	ストレージサーバーとストレージユニットの属性を表示します。 注意: この権限しか付与されていないユーザーは、Web UI にサインインできません。
リカバリポイントの管理 (Recovery Point Management)	リカバリポイントの有効期限の管理	資産の利用可能なリカバリポイントを期限切れにします。この機能は、現在は NetBackup API からのみ利用できます。 注意: この権限しか付与されていないユーザーは、Web UI にサインインできません。
	リカバリポイントの管理 (Manage Recovery Points)	資産の利用可能なリカバリポイントを管理します。この権限が付与されたユーザーは、リカバリポイントのリストア、コピー、複製の処理を実行でき、イメージのプライマリコピーを変更できます。これらの機能は、現在は NetBackup API からのみ利用できます。 注意: この権限しか付与されていないユーザーは、Web UI にサインインできません。

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
セキュリティ管理 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。	グローバルセキュリティ設定の管理 (Manage Global Security Settings)	NetBackup マスター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。 注意:この権限しか付与されていないユーザーは、Web UI にサインインできません。
	API キーの管理	NetBackup ユーザー用に作成された API キーを追加、編集、表示、削除します。
	証明書の管理 (Manage Certificates)	NetBackup セキュリティ証明書を管理し、ホストの外部 CA 証明書の詳細を表示します。NetBackup 証明書の場合は、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。この権限が付与されたユーザーは、ユーザーセッションの管理も可能です。
	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。
	ユーザー認証の管理 (Manage User Authentication)	スマートカードまたはデジタル証明書でユーザーを認証するための設定を管理します。この権限が付与されたユーザーは、ロックされた NetBackup ユーザーセッションの管理も可能です。
	API キーの表示 (View API Keys)	NetBackup ユーザー用に作成された API キーを表示します。NetBackup ユーザーは自身のキーを表示して管理できます。
保護計画の管理 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。
役割ベースのアクセス制御 特定の作業負荷または資産、および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。
	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。 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) 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。 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。	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。
	資産の上書き (Overwrite Asset)	資産を元の場所にリストアすることをユーザーに許可します。このアクセス権を持たないユーザーは資産を別の場所にリストアする必要があります。
	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。 注意:この権限しか付与されていないユーザーは、Web UI にサインインできません。
	ファイルのリストア (Restore Files)	バックアップイメージから個々のファイルをリストアします。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。
	リカバリ (Recover)/リストア (Restore)	バックアップイメージから別の場所にデータをリストアします。
	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。

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について

オブジェクトグループは、資産、アプリケーションサーバー、または保護計画の組み合わせを定義します。ユーザーの役割とオブジェクトグループ (ユーザーのアクセスルールを構成する) によって、オブジェクトグループ内のオブジェクトに対するユーザーのアクセス権が決まります。

特定の資産の管理またはリカバリを実行するには、それらの資産を使用した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、それらの計画を使用した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。特定のアプリケーションサーバーのクレデンシャルを管理するには、それらのサーバーを含む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。ユーザーに割り当てられた役割に応じて、ユーザーは次のタスクを実行できます。

- セキュリティ管理者には、すべてのオブジェクトグループ内のすべてのオブジェクトに対するアクセス権が割り当てられます。この役割を割り当てられたユーザーは、次の操作を実行できます。
  - すべての資産を表示する
  - すべてのアプリケーションサーバーを表示する
  - すべての保護計画を表示する
- バックアップ管理者は次のことを管理できます。
  - オブジェクトグループに含まれている保護計画
  - どの計画にオブジェクトグループ内の資産をサブスクライブするか
  - オブジェクトグループに含まれる資産のジョブ
  - オブジェクトグループ内のアプリケーションサーバーのクレデンシャル
  - 資産グループ
- 作業負荷管理者は次の操作を実行できます。
  - オブジェクトグループに含まれる保護計画を表示する
  - どの計画にオブジェクトグループ内の資産をサブスクライブするかを管理する
  - オブジェクトグループ内の資産のリカバリを実行する

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が割り当てられているとします。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作成する手順

オブジェクトグループを作成して、そのオブジェクトグループに対するアクセス権を割り当てられたユーザーが利用できる資産、アプリケーションサーバー、保護計画の組み合わせを定義します。

表 2-4 オブジェクトグループを作成する方法

手順	処理	説明
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すべての資産を構成します。	p.26 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。 ユーザーに適切な RBAC の役割またはアクセス権が割り当てられている場合、ユーザーに表示または管理を許可する資産を追加します。たとえば、作業負荷管理者に保護またはリカバリの管理を許可する資産を追加します。
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構成します。	p.28 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。 ユーザーに適切な RBAC の役割またはアクセス権が割り当てられている場合、ユーザーに管理を許可するアプリケーションサーバーを追加します。たとえば、バックアップ管理者に管理を許可するアプリケーションサーバーを追加します。
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構成します。	p.30 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。 ユーザーに適切な RBAC の役割またはアクセス権が割り当てられている場合、ユーザーに管理を許可する保護計画を追加します。たとえば、バックアップ管理者に管理を許可する保護計画を追加します。作業負荷管理者はこれらの計画を表示し、これらの計画に資産をサブスクライブできます。
7	オブジェクトグループ用に構成した資産、アプリケーションサーバー、または計画をプレビューします。	p.31 の「オブジェクトグループ内のオブジェクトのプレビュー」を参照してください。
8	[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

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。

- すべての作業負荷

- 1 つ以上の条件を満たすすべてのクラウド資産
- 特定の VMware サーバーまたは RHV マネージャとそのすべての VM
- 特定の VMware サーバーまたは RHV マネージャと 1 つ以上の条件を満たす VM

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することもできます。p.31 の「オブジェクトグループ内のオブジェクトのプレビュー」を参照してください。

すべての作業負荷

すべての作業負荷のすべての資産を含めるには

◆ [すべてにアクセス権を付与 (Grant access to all)]を選択して、すべての作業負荷で利用可能なすべての資産を含めます。

クラウド資産

1 つ以上の条件を満たすクラウド資産を含めるには

1 [資産 (Assets)]で、[作業負荷の追加 (Add workload)]をクリックし、[クラウド (Cloud)]を選択します。

2 [条件の追加 (Add condition)]をクリックし、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。

RHV 資産

特定の RHV サーバーとその VM すべてを含めるには

1 [資産 (Assets)]で、[作業負荷の追加 (Add workload)]をクリックし、[RHV]を選択します。

2 [RHV マネージャを追加 (Add RHV manager)]をクリックします。

3 含める RHV マネージャの名前を選択します。または、RHV マネージャ名をクリックして、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 デフォルトでは、[すべての VM を含める (Include all VMs)]が有効になっているため、VMware サーバーのすべての VM が含まれます。

VMware 資産

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)]で、[作業負荷の追加 (Add workload)]をクリックし、[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 デフォルトでは、[すべてのVMを含める (Include all VMs)]が有効になっているため、VMwareサーバーのすべてのVMが含まれます。

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)]で、[作業負荷の追加 (Add workload)]をクリックし、[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。

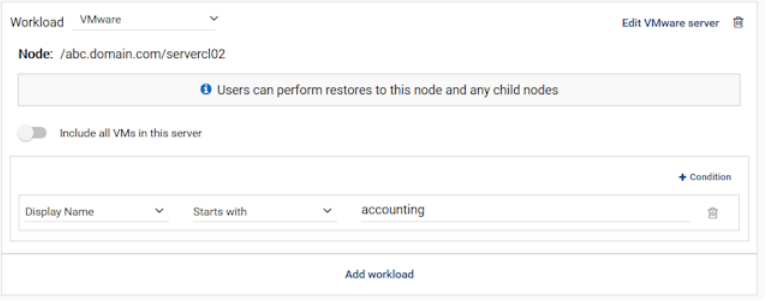
3 含めるvCenterの名前を選択します。または、vCenter名をクリックして、サーバー、クラスタ、またはデータセンターを参照します。

4 [すべての VM を含める (Include all VMs)]をオフにします。

5 [条件の追加 (Add condition)]をクリックし、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は、ユーザーが管理できるアプリケーションサーバーを定義します。アプリケーションサーバーは現在、VMware と RHV の作業負荷にのみ適用されます。

オブジェクトグループに含まれているアプリケーションサーバーをプレビューできます。

p.31 の「オブジェクトグループ内のオブジェクトのプレビュー」を参照してください。

すべて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)］で、［すべてにアクセス権を付与 (Grant access to all)］を選択します。

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を含めるには

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

  ［サーバー形式 (Server Type)］、オペレータ、作業負荷の種類を選択します。

  たとえば、［サーバー形式 (Server Type)］、［次の値に含まれる (Is In)］、［RHV］の順に選択し、すべての RHV アプリケーションサーバーを選択します。

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[条件の追加 (Add condition)]をクリックし、含める作業負荷の種類を選択します。

[サーバー形式 (Server Type)]、オペレータ、作業負荷の種類を選択します。

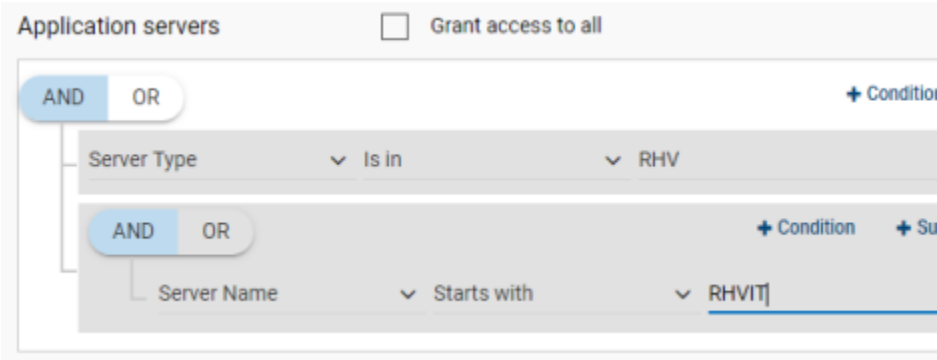
たとえば、[サーバー形式 (Server Type)]、[次の値に含まれる (Is In)]、[RHV]の順に選択し、すべての RHV アプリケーションサーバーを選択します。

2 [条件 (Condition)]をクリックし、[サーバー名 (Server Name)]に基づいて 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。

たとえば、特定の作業負荷の特定の名前で始まるアプリケーションサーバーが必要な場合があります。

3 条件が複数ある場合は、[サブクエリー (Sub-query)]オプションを使用し、オペレータ (AND または OR) を選択します。

次の例では、名前が RHVIT で始まる、RHV 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まれています。



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る保護計画によって、ユーザーが表示、追加、または管理できる計画が決まります。

オブジェクトグループに含まれる計画をプレビューできます。

p.31 の「オブジェクトグループ内のオブジェクトのプレビュー」を参照してください。

すべて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

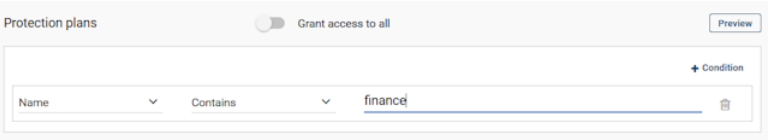
◆ [保護計画 (Protection plans)]で、[すべてにアクセス権を付与 (Grant access to all)]を選択します。

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。



メモ: この例では、ユーザーは、「finance」という単語が含まれる保護計画のみを表示、追加、または管理できます。

オブジェクトグループ内のオブジェクトのプレビュー

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。オブジェクトグループによって、環境内でユーザーが何にアクセスできるのかが決まります。
- 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 (AD) 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。p.36 の「AD または LDAP ドメインの追加」を参照してください。
  ローカルユーザーには、この構成は不要です。
- ユーザーにどの役割を付与するかを決定します。
  p.17 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.25 の「 オブジェクトグループを作成する手順」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.25 の「 オブジェクトグループを作成する手順」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.34 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。
- ユーザーにカスタムの役割が割り当てられている場合は、役割に対するアクセス権を変更します。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.24 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オブジェクトを決め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.31 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.35 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。

メモ: 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、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。NetBackup セキュリティ管理者がユーザーをサインアウトさせることもできます。

p.60 の「NetBackup ユーザーセッションのサインアウト」を参照してください。

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オブジェクトを変更する場合は、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。
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付与された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。
4. [削除 (Remove)]、[削除 (Remove)]の順にクリックします。

3

AD または LDAP ドメインの追加

この章では以下の項目について説明しています。

AD または LDAP ドメインの追加

NetBackup Web UI の NetBackup RBAC は、Active Directory (AD) または Lightweight Directory Access Protocol (LDAP) のドメインユーザーをサポートします。ドメインユーザー用のアクセスルールを追加する前に、AD または LDAP ドメインを追加する必要があります。また、ドメインでスマートカード認証を構成する前に、ドメインを追加する必要もあります。

メモ: ユーザーアカウント (`-m` オプションで指定) 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。

`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。

AD または LDAP ドメインを追加するには

1. マスター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。

```
vssat addldapdomain -d DomainName -s server_URL -u user_base_DN -g group_base_DN
-t rfc2307 | msad -m admin_user_DN
```

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
```

3. 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
```

4

セキュリティイベントと監査ログ

この章では以下の項目について説明しています。

セキュリティイベントと監査ログの表示

NetBackup は、NetBackup 環境でユーザーが開始した処理を監査して、いつ誰が何を変更したかを把握できるようにします。完全な監査レポートについては、`nbauditreport` コマンドを使用します。p.43 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。
  このレコードはサーベンスオクスリー法 (SOX) で要求されるようなガイドラインに準拠します。
- 内部の変更管理ポリシーに従う手段を提供できます。
- 問題のトラブルシューティングに NetBackup サポートが役立ちます。

NetBackup Audit Manager について

NetBackup Audit Manager (`nbaudit`) はマスターサーバー上で実行し、監査レコードは EMM (Enterprise Media Manager) データベースに保持されます。

管理者は特に以下を調査できます。

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

次の点に注意してください。

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

NetBackup によって監査された処理

NetBackup は、ユーザーが開始した次の処理を記録します。

アクティビティモニターの処理	任意の形式のジョブを取り消すか、中断するか、再開するか、再起動するか、または削除すると、監査レコードが作成されます。
アラートと電子メール通知	アラートを生成できないか、NetBackup 構成設定に関する電子メール通知を送信できない場合。たとえば、SMTP サーバーの構成やアラートの除外状態コードのリストなどです。

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

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

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。
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アイベントには、監査イベントに常にユーザー ID が含まれます。NetBackup 8.1.1 以前では、これらのイベントは「root@hostname」または「administrator@hostname」として記録されます。
- クレデンシャルを必要としないすべての操作や、ユーザーにサインインを求めるすべての操作の場合、操作はユーザー ID なしで記録されます。

監査保持期間と監査レコードのカタログバックアップ

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

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

監査保持期間を設定するには

1. 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/openv/netbackup/bin/admincmd
3. 次のコマンドを入力します。

   ```
   nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD
   number_of_days -machinename 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。

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

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

詳細な NetBackup 監査レポートの表示

nbauditreport コマンドを使用すると、NetBackup 監査イベントの詳細な情報を表示できます。

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/openv/netbackup/bin/admincmd¥nbauditreport

   または、次のオプションを使用してコマンドを実行します。

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

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

3 監査レポートは次の詳細を含んでいます。

DESCRIPTION	実行された処理の詳細。
USER	処理を実行したユーザーの ID。 p.42 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
```

5

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

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.63 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 NetBackup 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 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。

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.49 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 NetBackup 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。

6

セキュリティ証明書の管理

この章では以下の項目について説明しています。

NetBackup のセキュリティ管理と証明書について

NetBackup はセキュリティ証明書を使用して NetBackup ホストを認証します。これらの証明書は X.509 公開キー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 マスターサーバーは 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 ドメイン内のマスターサーバー、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。

- マスター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。
- 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。

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

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

NetBackup 証明書の表示

NetBackup ホストに対して発行された、すべてのホスト ID ベースの NetBackup 証明書の詳細を表示できます。NetBackup 8.1 以降の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。

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: 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

マスターサーバーの 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。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。

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 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、マスター以外の 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。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。

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.54 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. 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。

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. 右上隅の[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 は、外部 CA が発行した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。

p.57 の「ドメイン内の NetBackup ホストの外部証明書情報の表示」を参照してください。

[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マスターサーバーと NetBackup Web サーバー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。

ドメイン内の NetBackup ホストの外部証明書情報の表示

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

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

ホストの外部証明書の情報を表示するには

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

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

ホスト情報、ホストの外部証明書の詳細に加え、次の情報が示されます。

- [NetBackup 証明書の状態 (NetBackup certificate status)]列には、ホストに NetBackup 証明書もあるかどうかが示されます。
- [外部証明書 (External certificate)]ダッシュボードには、NetBackup 8.1 以降のホストに関する次の情報が含まれています。
  - ホストの合計。ホストの合計数です。ホストはオンラインになっており、NetBackup マスター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 マスター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。

マスター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。

7

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。

ユーザーがサインインするときのメッセージの表示

ユーザーが NetBackup 管理コンソール、NetBackup クライアント、または NetBackup Web UI にサインインするときに、サインインメッセージ (またはバナー) をユーザーに表示できます。異なるバナーをマスターサーバー、メディアサーバー、またはクライアントに構成できます。このメッセージでは、ユーザーがサインインする前に、利用規約への同意をユーザーに要求することもできます。

これらの設定は現在、NetBackup 管理コンソールの[ホストプロパティ (Host Properties)]、*[ホスト名 (hostname)]*、[ログインバナーの構成 (Login Banner Configuration)]で管理されています。詳しくは『NetBackup 管理者ガイド Vol. 1』を参照してください。

サインインの最大試行回数とユーザーセッションのアイドルタイムアウト設定の有効化

ユーザーセッションのタイムアウト時間と NetBackup のサインインの最大試行回数を有効化して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。

これらの設定は現在、NetBackup 管理コンソールの[ホストプロパティ (Host Properties)]、*[master_server]*、[ユーザーアカウントの設定 (User Account Settings)]で管理されています。詳しくは『NetBackup 管理者ガイド Vol. 1』を参照してください。

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。デフォルトでは、ユーザーセッションは 10 分間アイドル状態になると自動的にログアウトします。

タイムアウト設定は、NetBackup 管理コンソールの[ホストプロパティ (Host Properties)]、*[master_server]*、[ユーザーアカウントの設定 (User Account Settings)]で管理されています。詳しくは『NetBackup 管理者ガイド Vol. 1』を参照してください。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。この時間は、[アカウントロックアウト期間 (Account lockout duration)]を調整して変更できます。

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。

アカウントロックアウト設定は、NetBackup 管理コンソールの[ホストプロパティ (Host Properties)]、*[master_server]*、[ユーザーアカウントの設定 (User Account Settings)]で管理されています。詳しくは『NetBackup 管理者ガイド Vol. 1』を参照してください。ユーザーのアカウントは、[アカウントロックアウト期間 (Account lockout duration)]設定で指定された時間だけロックされたままになる点に注意してください。

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。

8

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

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、マスター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 NetBackup 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、この設定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 以前のホストとの通信を許可する (Allow 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。[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 NetBackup 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 NetBackup 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。

メモ: NAT クライアントに NetBackup 証明書を配備するときは、マスターサーバーで設定されている証明書の配備のセキュリティレベルに関係なく、認証トークンを指定する必要があります。これは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ないためです。

NetBackup の NAT に関するサポートについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

表 8-1 NetBackup 証明書の配備のセキュリティレベルに関する説明

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

セキュリティレベル	説明	CRL の更新
高 (High) (デフォルト)	ホストが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。 **1** ホストが NetBackup 構成ファイル (Windows レジストリまたは UNIX の `bp.conf` ファイル) で次のいずれかのオプションでリストされる。 ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER NetBackup の構成オプションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。 **2** `altnames` ファイル (ALTNAMESDB_PATH) にクライアント名としてホストがリストされている。 **3** ホストが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.64 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』

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 NetBackup 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 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)	ホストがマスターサーバーにとって既知の場合、NetBackup は認証トークンを必要としません。つまり、ホストは NetBackup 構成ファイル、EMM データベース、バックアップポリシーに表示されます。または、ホストはレガシークライアントです。
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、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。

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。
4. [保存 (Save)]をクリックします。

9

API キーの作成と使用

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

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。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。

表 9-1 ユーザーが Web UI と API を使用して API キーを管理および表示する方法

ユーザー	RBAC の役割またはアクセス権	API キーの作成と管理	API キーの表示	インターフェース
NetBackup セキュリティ管理者	セキュリティ管理者の役割	すべてのユーザー	すべてのユーザー	Web UI、API
NetBackup RBAC ユーザー	API キーの管理	すべてのユーザー	すべてのユーザー	Web UI、API
NetBackup RBAC ユーザー	API キーの表示	セルフ	すべてのユーザー	Web UI、API
その他の NetBackup で認証されたユーザー	RBAC の役割または API キーのアクセス権なし	セルフ	セルフ	API

詳細情報

p.42 の「監査レポートのユーザーの ID」を参照してください。

p.32 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。

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 キーの管理

NetBackup セキュリティ管理者または API キーを管理するアクセス権を持つ NetBackup ユーザーは、NetBackup Web UI を使用して、すべての NetBackup ユーザーに関連付けられているキーを追加、編集、削除、表示できます。NetBackup で認証済みのユーザーは、RBAC のアクセス権が付与されていない場合、NetBackup API を使用して自身の API キーを表示および管理できます。

p.32 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。

API キーの追加

認証済みの NetBackup ユーザー用に API キーを作成できます (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。

注: 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。ユーザーに新しい API キーが必要になった場合は、そのユーザーの有効なキーまたは期限切れのキーを削除する必要があります。

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 (User name)]を入力します。
4. 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下部に表示します。
5. [追加 (Add)]をクリックします。
6. API キーをコピーするには、[クリップボードにコピー (Copy to clipboard)]をクリックします。

   キーをユーザーに提供するまでは、安全な場所にこのキーを保存します。[閉じる (Close)]をクリックした後は、キーを再び取得することはできません。ユーザーの以前のキーをこの API キーで置き換える場合、新しい API キーを反映するには、ユーザーはスクリプトなどを更新する必要があります。
7. [閉じる (Close)]をクリックします。

API キーの編集

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、ユーザーの古いキーを削除して新しいキーを作成する必要があります。

API キーを編集するには

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. API キーを選択し、[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. [保存 (Save)]をクリックします。

API キーの削除

ユーザーにキーの使用を許可しない場合、またはキーが使用されなくなった場合は、API キーを削除できます。API キーを削除すると、そのキーは完全に削除されます。関連付けられているユーザーは、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. 左側で[セキュリティ (Security)]、[API キー (API keys)]の順に選択します。
2. API キーを選択し、[削除 (Delete)]、[削除 (Delete)]の順にクリックします。

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://masterservername.domain.com/netbackup/admin/jobs/5
 ¥
     -H 'Accept: application/vnd.netbackup+json;version=3.0'     ¥
     -H 'Authorization: <API key value>'
```

API キーの表示

NetBackup セキュリティ管理者または API キーを表示するアクセス権を持つ NetBackup ユーザーは、すべての NetBackup ユーザーに関連付けられているキーを表示できます。NetBackup で認証済みのユーザーは、RBAC のアクセス権が付与されていない場合、NetBackup API を使用して自身の API キーを表示および管理できます。

API キーを表示するには

- 左側で[セキュリティ (Security)]、[API キー (API keys)]の順に選択します。

10

スマートカード認証の構成

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

NetBackup は、デジタル証明書またはスマートカード (CAC と PIV を含む) による、Active Directory (AD) または LDAP ドメインユーザーに対する認証をサポートしています。この認証方法はマスターサーバーのドメインごとに 1 つの AD または LDAP ドメインのみサポートし、ローカルドメインのユーザーは使用できません。この認証方法を使用するそれぞれのマスターサーバードメインに対して、この構成を個別に実行する必要があります。

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.36 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.19 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.36 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

マスター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。

11

Web UI へのアクセス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 11-1 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/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。 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。 詳しくは、vnetd -http_api_tunnel ログで OID 491 を確認してください。
手順 6	NetBackup Web サーバーの外部証明書がアクセス可能で、期限切れになっていないことを確認します。	■ Java Keytool コマンドを使用して、次のファイルを検証します。 Windows: *install_path*¥var¥global¥wsl¥credentials¥nbwebservice.jks UNIX: /usr/openv/var/global/wsl/credentials nbwebservice.jks ■ nbwebgroup に、nbwebservice.jks ファイルにアクセスするためのアクセス権があるかどうかを確認します。 ■ 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 11-1の手順に従います。

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 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。
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。

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.19 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、ユーザーのアクセスルール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、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ていない場合、`vssat` の検証によって**「プリンシパルまたはグループが存在しません。**`(The principal or group does not exist.)`**」**と表示されます。詳細は `nbatd` 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=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)

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/openv/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=con" "(&(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>