NetBackup ™ セキュリティおよび暗号化ガイド

UNIX、Windows および Linux

リリース 10.3

VERITAS™

NetBackup ™ セキュリティおよび暗号化ガイド

最終更新日: 2023-12-28

法的通知と登録商標

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

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

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

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されます。Veritas Technologies Corporation 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 Corporation およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

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

Veritas Technologies Corporation
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

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

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

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

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

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

マニュアル

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

https://sort.veritas.com/documents

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

1

NetBackup での安全な通信 (最初にお読みください)

この章では以下の項目について説明しています。

NetBackup での安全な通信について

この章では、NetBackup での安全な通信に関する重要事項について説明します。安全な通信をサポートするバージョン (8.1 以降) に NetBackup をアップグレードする前に、この章をお読みになることを強くお勧めします。

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 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 ホストの認証に使用される NetBackup セキュリティ証明書は、X.509 公開鍵基盤 (PKI) 標準に適合しています。NetBackup は、次の 2 種類の証明書をサポートします。

- NetBackup CA が署名した証明書: NetBackup プライマリサーバーは、認証局 (CA) として動作し、ホストにデジタル証明書を発行します。
  p.264 の「NetBackup のセキュリティ証明書の概要」を参照してください。
- 外部 CA が署名した証明書: NetBackup 8.2 以降では、外部 CA が署名した証明書 (または外部証明書) を NetBackup ホストで設定することもできます。
  p.384 の「NetBackup での外部 CA のサポートについて」を参照してください。

NetBackup の構成に応じて、ホストには、他のホストと正常に通信するためにいずれかまたは両方の種類の証明書が必要です。

NetBackup のインストール時に、ホストに証明書を配備できます。何らかの理由でインストール時に証明書をホストに配備できない場合、ホストは他のホストと通信できません。その場合、`nbcertcmd` コマンドを使用してホストに NetBackup 証明書を手動で配備し、インストール後にホスト通信を開始します。

または、外部 CA が署名した証明書を設定できます。

NetBackup 管理コンソールの[ホスト管理 (Host Management)]と[グローバルセキュリティ設定 (Global Security Settings)]ノードで、安全な通信を設定できます。

コマンド nbhostmgmt、nbhostidentity、nbcertcmd、および nbseccmd には、証明書の配備や他のセキュリティ設定を管理するためのオプションがあります。

ご使用の環境に NetBackup 8.0 以前のホストがある場合、それらのホストとの古い通信設定も有効です。

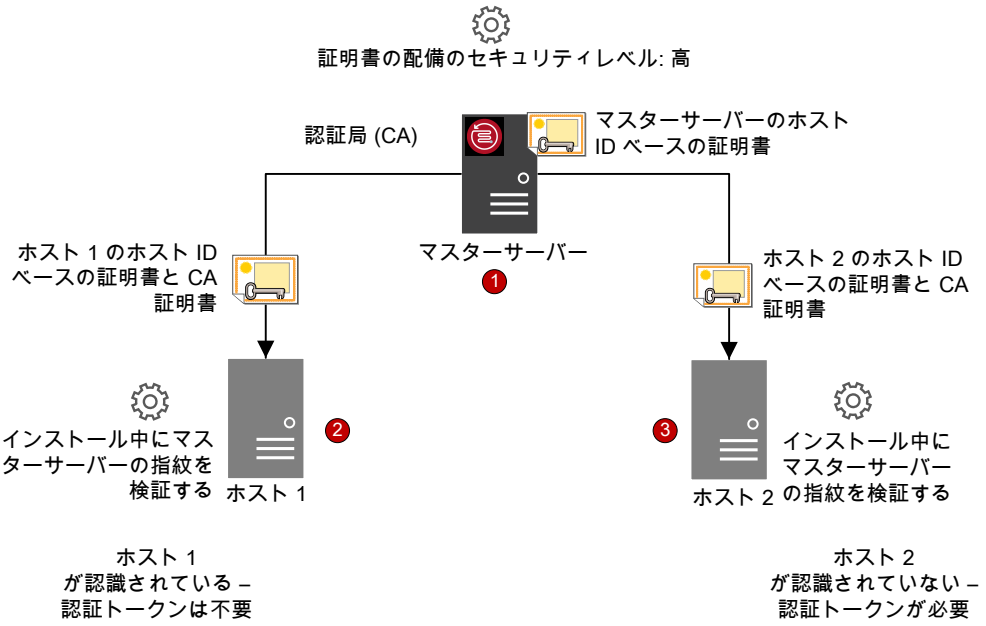
p.35 の「NetBackup 8.1 のホストが NetBackup 8.0 以前のホストと通信する方法」を参照してください。

メモ: 次のシナリオでは、ホスト名ベースの証明書が必要です。

- NetBackup アクセス制御または NBAC 対応のホストでは、ホスト名ベースの証明書が必要
- NetBackup CloudStore Service Container では、メディアサーバーにホスト名ベースの証明書のインストールが必要

インストール時に NetBackup CA が署名した証明書 (またはホスト ID ベースの証明書) を配備する方法

次の図では、インストール中に NetBackup CA が署名した証明書をホストに配備する方法を示しています。



NetBackup 証明書の配備は、次の順序で行われます。

1. NetBackup 証明書は、インストール時に NetBackup プライマリサーバーに自動的に配備されます。プライマリサーバーは NetBackup CA です。
2. NetBackup 証明書は、インストールウィザードまたはスクリプトにより利用できるようになった CA 指紋を確認した後のインストール時に、ホスト 1 に配備されます。

   プライマリサーバーの証明書配備セキュリティレベルが[高 (High)]に設定されており、ホスト 1 がプライマリサーバーに認識されているため、認証トークンは必要ありません。

メモ: プライマリサーバーの CA をホストのトラストストアに追加する前に、指紋を使用した認証が実行されます。プライマリサーバーの管理者は、CA 指紋を電子メールまたはファイルでホスト管理者に送信するか、Web サイトで公開します。

メモ: 認証トークンは、NetBackup プライマリサーバーに送信されるホストの証明書要求を承認するメカニズムとして使用されます。認証トークンは機密であり、プライマリサーバーの管理者のみが作成できます。次に、プライマリサーバーの管理者は、証明書を配備するホストの管理者に認証トークンを渡します。再発行トークンは、証明書の以前の発行先であるホスト上に証明書を再配備するために使用される、特殊な認証トークンです。

プライマリサーバーの指紋を確認せずに NetBackup のインストールを続行すると、バックアップとリストアを実行する前に手動の手順を実行することが必要になります。

https://www.veritas.com/support/en_US/article.000127129

3. NetBackup 証明書は、プライマリサーバーの指紋が確認されたら、インストール時にホスト 2 に配備されます。プライマリサーバーの証明書配備セキュリティレベルが［高 (High)］に設定されており、ホスト 2 がプライマリサーバーに認識されていないため、認証トークンが必要です。

プライマリサーバーのクラスタノードでの安全な通信の方法

クラスタのプライマリサーバーがある場合は、証明書の配備に関する次のシナリオを確認します。

- NetBackup の新規インストールの場合、アクティブノードに証明書が自動的に配備されます。すべての非アクティブノードでは、証明書を手動で配備する必要があります。
- ディザスタリカバリの場合は、アクティブノードの証明書も非アクティブノードの証明書もリカバリされません。災害後にディザスタリカバリモードで NetBackup をインストールした後、再発行トークンを使用してすべてのノードに証明書を手動で配備する必要があります。
- アップグレードの場合、アクティブノードと非アクティブノードにすでに証明書が配備されていることがあります。`nbcertcmd -listCertDetails` コマンドを使用して証明書の詳細を表示することで、クラスタノードに証明書があるかどうかを確認できます。

メモ: プライマリサーバーのクラスタノード上で NetBackup アクセス制御 (NBAC) を構成済みの場合、ホスト名ベースの証明書をすべてのノードに手動で配備する必要もあります。

クラスタのセットアップ内では、同じ仮想名が複数のクラスタノードで使用されます。そのため、仮想名をすべての関連クラスタノードにマップする必要があります。

クラスタ化されたアプリケーションのノードにインストールされた NetBackup クライアントについて

クラスタ化されたアプリケーションのノードにインストールされた NetBackup クライアントとの安全な通信については、次のシナリオを確認してください。

- 正常に通信するには、すべてのクラスタノードを同時にアップグレードする必要があります。
- フェールオーバー後のバックアップの失敗を回避するには、仮想名をすべてのクラスタノードに必ずマッピングしてください。Veritas は、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]、[承認待ちのマッピング (Mappings for approval)]タブから競合の検出を監視して、必要なマッピングを承認することをお勧めします。

アップグレード時に NetBackup 証明書をホストに配備する方法

NetBackup をアップグレードする際、NetBackup はアップグレード前に NetBackup 証明書を配備します。証明書を配備できない場合は、アップグレード処理を終了できます。アップグレードスクリプトは、使用できる既存の NetBackup 設定を保持します。

NetBackup を 8.0 から 8.1 以降にアップグレードした場合、NetBackup 証明書はホスト上にすでに存在していることがあります。そのような場合、アップグレード処理中に証明書は配備されません。

セキュリティ更新プログラムおよびソフトウェアパッチをダウンロードしてインストールするユーティリティを使用してソフトウェアがアップグレードされた場合、証明書はアップグレード処理中に配備されません。手動で証明書を配備する必要があります。

証明書配備中に認証トークンが必要である場合

このセクションの情報は NetBackup CA が署名した証明書のみに適用されます。外部 CA が署名した証明書に認証トークンは必要ありません。

セキュリティレベルの設定により、証明書の配備に認証トークンが必要かどうかが決まります。プライマリサーバーのセキュリティレベルは、必要に応じてさまざまなレベルに設定できます。 NetBackup 管理コンソールで[セキュリティ管理]>[グローバルセキュリティ設定]>[安全な通信]タブを使用します。

次の設定を利用できます。デフォルト設定は[高 (High)]です。

- [中 (Medium)] - プライマリサーバーの指紋は証明書の配備時に確認する必要があります。認証トークンは不要です。
- [高 (High)] - プライマリサーバーの指紋は証明書の配備時に確認する必要があります。ホストがプライマリサーバーに認識されている場合、認証トークンは不要です。
- [最高 (Very High)] - プライマリサーバーの指紋は証明書の配備時に確認する必要があります。認証トークンはすべてのホストに必須です。

メモ: 特定のシナリオでの証明書の配備には、クライアントが非武装ゾーンにある場合や証明書の再発行などのために、常にトークンが必要です。

p.297 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。

ホスト名 (または IP アドレス) をホスト ID にマップする理由

ホストは複数の名前で参照できます。

たとえば、複数のネットワークインターフェースの場合、またはホストが短縮名と完全修飾ドメイン名 (FQDN) の両方で参照されている場合などです。

NetBackup 8.1 以降で正常に安全な通信を行うには、関連するすべてのホスト名をそれぞれのホスト ID にマップする必要があります。ホストの NetBackup 構成のクライアント名 (つまりプライマリ名) は、証明書の配備中にそのホスト ID に自動的にマップされます。追加のホスト名は通信時に検出され、それぞれのホスト ID に自動的にマップされるか、[承認待ちのマッピング (Mappings for Approval)]リストに表示されることがあります。プライマリサーバーの[ホスト管理 (Host Management)]プロパティで、この設定を実行します。

p.269 の「ホスト ID からホスト名へのマッピングの追加」を参照してください。

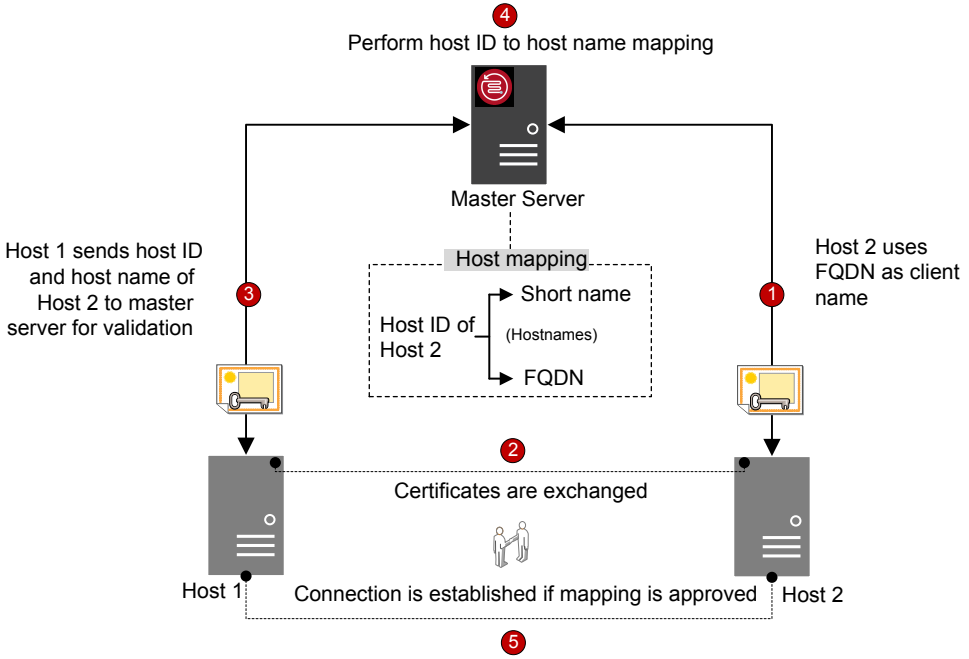
複数のホスト名がある構成の例は、次のとおりです。

- 複数のネットワークインターフェースがある場合、ホストにはパブリックとプライベートの両方のホスト名があります。
- ホストは短縮名と完全修飾ドメイン名 (FQDN) を持つことができます。
- ホストはその IP アドレスと関連付けることができます。
- クラスタ化されているファイルシステムまたはデータベースの場合、ホストはノード名とクラスタの仮想名に関連付けられます。

次の点に注意してください。

- Exchange、SharePoint、および SQL Server エージェントは、プライマリサーバーの[分散アプリケーションリストアマッピング (Distributed Application Restore Mapping)]ホストプロパティでホスト情報を構成する必要もあります。
- 高可用性環境では、SQL Server エージェントに、クラスタ名または AG ノード名を含む 2 番目のポリシーは不要になります。さらに、クラスタノードまたは AG ノードに、リダイレクトリストア用の許可を構成する必要もありません。SQL Server クラスタまたは AG の正常なバックアップとリストアでは、ホスト管理プロパティおよび分散アプリケーションリストアマッピングホストプロパティでマッピングを構成するだけで済みます。

次の図は、ホスト ID とホスト名とのマッピングプロセスを示しています。



ホスト名とホスト ID とのマッピングは、次の順序で行われます。

1. ホスト 2 の FQDN 2 は、証明書配備中にそのホスト ID にマップされます。
2. ホスト 1 は、短縮名を使用してホスト 2 への安全な接続を開始します。両方のホストは、TLS ハンドシェイクの一部として、NetBackup 証明書を交換します。
3. ホスト 1 は、ホスト ID とホスト 2 の短縮名をプライマリサーバーに検証用に送信します。
4. プライマリサーバーは、ホスト ID と短縮名をそのデータベース内から検索します。指定された短縮ホスト名がホスト 2 のホスト ID にまだマップされていないため、次のいずれかが行われます。
   - NetBackup Web UI の[ホスト ID をホスト名に自動的にマップする (Automatically map host ID to host names)]オプションが選択されており、短縮名が別のホスト ID にまだマップされていない場合、検出された短縮名はホスト 2 のホスト ID に自動的にマップされ、ホスト 1 は接続を継続するように指示されます。
   - [ホスト ID をホスト名に自動的にマップする (Automatically map host ID to host names)]オプションが選択されておらず、短縮名が別のホスト ID にすでにマップされている場合、検出されたマッピングは承認待ちリストに追加され、ホスト 1

は接続を切断するように指示されます。同じ短縮名を使用してホスト 2 への接続を正常に実行するには、その前にマッピングを手動で承認する必要があります。

5. マッピングが承認されていれば、ホスト間での接続は確立されます。マッピングが承認されていない場合、接続は切断されます。

ホスト属性またはホストの通信状態をリセットする方法

[ホスト属性をリセット (Reset Host Attributes)]オプションは、ホストのプロパティ、およびホスト名とホスト ID のマッピング情報を削除します。プライマリホスト名と NetBackup 証明書は削除されません。

ホスト属性のリセットは、次のようなシナリオの場合に便利です。

- 安全でない (または旧バージョンの) 通信を可能にするために、ホストを 8.0 以前にダウングレードした場合。
- ホスト通信の問題が発生し、ホスト情報を削除する場合。

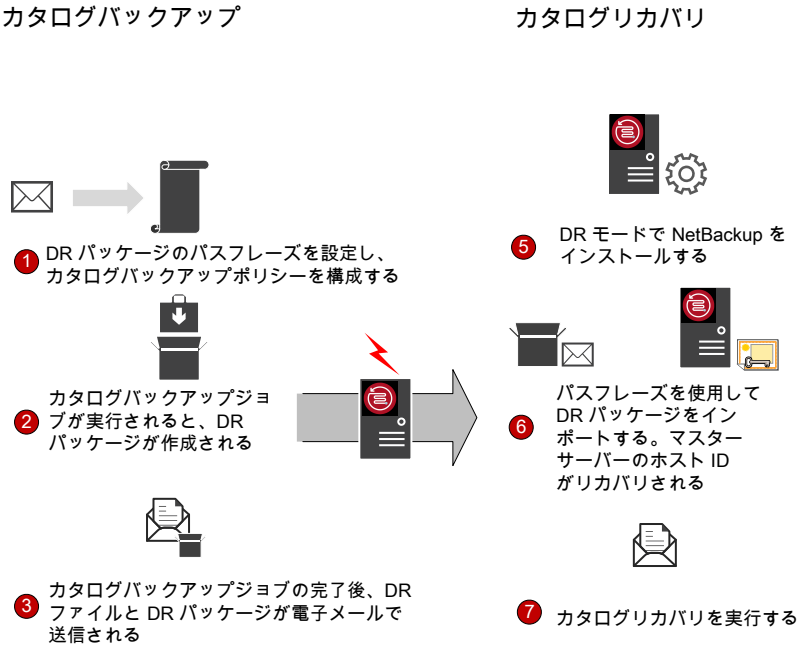
p.279 の「NetBackup ホスト属性のリセット」を参照してください。

カタログリカバリの変更点

NetBackup 8.1 以降では、災害後に NetBackup をリストアするときに、プライマリサーバーによってそのホスト ID をリカバリすることが求められます。ホスト ID には、証明書情報、セキュリティの設定、その他の情報が含まれています。

以前のホスト ID を使用すれば、プライマリサーバーは新しい NetBackup インスタンスでメディアサーバーやクライアントと通信できます。ディザスタリカバリパッケージは、プライマリサーバーのホスト ID を保持する各カタログバックアップ中に作成されます。ディザスタリカバリパッケージは、セキュリティ証明書やセキュリティの設定などの重要なデータが含まれているので、パスフレーズで暗号化されています。

次の図は、カタログリカバリのワークフローを示しています。



1. ディザスタリカバリパッケージのパスフレーズを設定し、次にカタログバックアップポリシーを構成します。カタログバックアップでは、ポリシーの実行時に構成したパスフレーズを使用します。

   パスフレーズを設定するには、NetBackup Web UI で[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に開きます。次に[ディザスタリカバリ (Disaster recovery)]をクリックします。

   `nbseccmd -setpassphraseconstraints` コマンドオプションを使用して、パスフレーズの制約を設定することもできます。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。

   コマンドを使用してパスフレーズの制約を設定しない場合、デフォルトの制約が適用されます。最小値は 8 で、最大 1024 文字です。

   パスフレーズをいつ変更しても、以前に作成されたディザスタリカバリパッケージのパスフレーズは変更されません。変更されるのは、後から作成されたディザスタリカバリパッケージのパスフレーズのみです。

   古いカタログをリカバリするには、対応するパスフレーズを使用する必要があります。

注意: カタログバックアップポリシーを構成する前に、パスフレーズを設定する必要があります。パスフレーズが設定されていない場合、カタログバックアップは失敗します。カタログバックアップポリシーを 8.1 より前のバージョンからアップグレードする場合、パスフレーズを設定するまでカタログバックアップは失敗します。

2. 各カタログバックアップ時にディザスタリカバリパッケージが作成されます。

   カタログバックアップが正常に実行された後にパスフレーズを確認するには、次のコマンドを実行します。

   ```
   nbhostidentity -testpassphrase -infile dr_package_location
   ```

3. ディザスタリカバリパッケージはディザスタリカバリファイルとともに保存され、ポリシー構成時に指定した受信者に電子メールで送信されます。
4. 災害が発生します。
5. 災害後に、NetBackup をプライマリサーバー上にディザスタリカバリモードでインストールします。この処理では、ディザスタリカバリパッケージのパスとパスフレーズを指定するように求められます。
6. 適切なパスフレーズを指定すると、プライマリサーバーのホスト ID がリカバリされます。リカバリするディザスタリカバリパッケージに対応するパスフレーズを入力する必要があります。

   パスフレーズを紛失した場合は、セキュリティ証明書をすべての NetBackup ホストに手動で配備する必要があります。

   詳しくは、次の記事を参照してください。

   http://www.veritas.com/docs/000125933
7. ホストの識別情報をリカバリしたらすぐにカタログリカバリを実行するようにします。このようにすることで、ホスト ID のリストア後に発生する可能性のある、証明書関連アクティビティに固有の情報損失を回避できます。適切なディザスタリカバリ (DR) ファイルを使用し、必要なカタログをリカバリします。

   パスフレーズは、ホスト ID (またはディザスタリカバリパッケージ) のリストア中、またはカタログリカバリ中にはリカバリされません。それは新しい NetBackup インスタンスで再設定する必要があります。

メモ: 通常の NetBackup インストール後にホスト ID をリストアする必要がある場合 (ディザスタリカバリモードが選択されていない場合)、`nbhostidentity` コマンドを使用できます。

NetBackup Appliance のホスト ID をリストアするには、通常のインストール後に `nbhostidentity` コマンドを使用する必要があります。

自動イメージレプリケーションでの変更点

安全な通信で NetBackup 自動イメージレプリケーション (A.I.R.) を使用するには、ソースとターゲットの両方のプライマリサーバーからの信頼を確立する必要があります。

ソースプライマリサーバーおよびターゲットプライマリサーバーの両方を 8.1 以降にアップグレードしたら、両方のプライマリサーバー上で信頼関係を更新する必要があります。

メモ: アップグレード後に、両方のサーバー上で信頼が再確立されていないと、新しいストレージライフサイクルポリシー (SLP) は機能しません。

信頼関係は、NetBackup Web UI または `nbseccmd -setuptrustedmaster` コマンドを使用して構成できます。

自動イメージレプリケーションの信頼できるプライマリサーバーについて詳しくは、『NetBackup 重複排除ガイド』を参照してください。

無効化された証明書を使用するホストの動作

NetBackup 証明書は、さまざまな理由でプライマリサーバー管理者により無効化される場合があります。無効化された証明書に関する情報が含まれる証明書失効リスト (CRL) はプライマリサーバーによって作成され、すべてのホストにより定期的にフェッチされます。CRL を更新する時間間隔は、プライマリサーバー上での証明書配備のセキュリティレベルによって決定されます。

ホスト間の通信中に CRL が検証されます。無効化された証明書を使用しているホストは信頼できなくなります。このようなホストとの通信は終了されます。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

NetBackup 証明書のバックアップについて

セキュリティ上の理由から、バックアップ時に NetBackup 証明書のバックアップは作成されません。NetBackup のアンインストール時に証明書は自動的に削除されます。必要に応じて、NetBackup をアンインストールする前にそれぞれの秘密鍵とともに手動でバックアップを作成します。

p.309 の「プライマリ以外のホストで NetBackup を再インストールするときのホスト ID ベースの証明書の保持」を参照してください。

プライマリサーバーに対する外部証明書の構成

信頼できる認証局 (CA) が発行した X.509 証明書を使用できます。NetBackup は、NetBackup ホストの外部証明書のソースとしてファイルベースの証明書と Windows 証明書ストアをサポートしています。PEM、DER、P7B 形式の証明書をサポートしています。

p.387 の「NetBackup ホスト通信で外部証明書を使用するワークフロー」を参照してください。

外部証明書を使用するプライマリサーバーのクラスタノードでの安全な通信の方法

クラスタプライマリサーバーで、信頼できる認証局 (CA) が発行した X.509 証明書を使用できます。

まず、NetBackup Web サーバーを構成して、外部 CA が署名した証明書の使用を NetBackup ドメインで有効にする必要があります。その後、ホストとの安全な通信に外部 CA が署名した証明書を使用するように、NetBackup のクラスタプライマリサーバーを構成できます。

p.421 の「クラスタプライマリサーバーに外部証明書を使用するワークフロー」を参照してください。

外部証明書の失効リストの仕組み

外部認証局 (CA) の証明書失効リスト (CRL) には、スケジュールされた有効期限前に外部 CA が無効化して、信頼しないようにする必要があるデジタル証明書のリストが含まれています。

p.404 の「外部 CA の証明書失効リストについて」を参照してください。

ホストがプライマリサーバーに直接接続できないときの通信の動作

非武装地帯 (DMZ) で、NetBackup クライアントがプライマリサーバーに要求 (証明書配備に対するものなど) を直接送信できない場合があります。メディアサーバー上の HTTP トンネルを使用して、クライアントホストから送信された Web サービス要求を受け入れ、それらをプライマリサーバーに転送します。HTTP トンネルの構成は自動で、設定は不要です。HTTP トンネルが機能するには、NetBackup クライアントとメディアサーバーが 8.1 以降である必要があります。

プライマリサーバーで設定されている証明書配備のセキュリティレベルに関係なく、非武装ゾーン内のホストに NetBackup CA が署名した証明書を配備するには、認証トークンが必要です。

p.340 の「非武装地帯にある NetBackup クライアントとプライマリサーバーの間の HTTP トンネルを介した通信について」を参照してください。

NetBackup 8.1 のホストが NetBackup 8.0 以前のホストと通信する方法

NetBackup 8.1 以降のホストは他の 8.1 以降のホストとセキュアモードでのみ通信できます。8.1 以降のホストが 8.0 以前のホストと通信する場合、安全でない通信を許可する必要があります。

デフォルトでは、[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)]オプションが有効になっています。このオプションは、NetBackup 管理コンソールの[セキュリティ管理 (Security Management)]>[グローバルセキュリティ設定 (Global Security Settings)]>[安全な通信 (Secure Communication)]タブで利用できます。

このオプションを無効にして安全な通信のみを許可する場合、NetBackup サービスをプライマリサーバーで再起動して安全でない通信をすべて終了し、安全な通信のみを許可する必要があります。

安全でない通信時には、NetBackup ホストはまずホスト検証のためにプライマリサーバーに接続します。プライマリサーバーは、安全でない通信が有効であるかどうかを確認します。このオプションが有効であれば、2 つのホスト間の通信は確立されます。このオプションが無効であれば、通信は切断されます。

クラウド構成でのレガシーメディアサーバーとの通信方法

[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)]オプションが無効になっている場合、CSSC_LEGACY_AUTH_ENABLED クラウド構成オプションの値に関係なく、NetBackup はクラウドストレージに使用するレガシーメディアサーバーと通信できません。

[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)]オプションは、NetBackup Web UI の[設定 (Setting)]、[グローバルセキュリティ (Global Security)]、[安全な通信 (Secure Communication)]タブで使用できます。

通信エラーのシナリオ

NetBackup 8.1 以降で生じる可能性があるホスト通信問題を解決するには、次のシナリオを確認します。

8.0 以前のホストとの通信中のエラー

安全でない通信が NetBackup で許可されていない場合、8.0 以前のホストとの通信は失敗します。8.0 以前の NetBackup ホストとの通信を正常に実行するには、以下のいずれかの方式を使用します。

- プライマリサーバーホストの NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[グローバルセキュリティ (Global security)]、[ホスト (Hosts)]、[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)]オプションの順に選択します。
- プライマリサーバーホストで次のコマンドを実行します。`nbseccmd -setsecurityconfig -insecurecommunication on`

カタログバックアップのエラー

ディザスタリカバリパッケージのパスフレーズが設定されていない場合、カタログバックアップは状態コード 2524 で失敗します。次のエラーメッセージが表示されます。

```
Catalog backup failed because the passphrase for the disaster recovery

package is not set.
```

パスフレーズを設定するには、NetBackup Web UI で[設定 (Setting)]、[グローバルセキュリティ (Global Security)]、[ディザスタリカバリ (Disaster Recovery)]タブを使用します。

NetBackup ドメイン内の他のホストに対する安全な通信のサポート

このセクションでは、NetBackup 8.1 が BMR (Bare Metal Restore) ホストとの通信をどのようにサポートするかについて説明します。

NetBackup 8.1 以降のプライマリサーバーとの通信

NetBackup 8.1 プライマリサーバーのデータを収集する前に、次のオプションが設定されていることを確認します。

- NetBackup で、安全でない通信が有効になっている。次のいずれかを確認します。
  - プライマリサーバーホスト上の NetBackup Web UI で、[グローバルセキュリティ設定 (Global security settings)]、[安全な通信 (Secure Communication)]タブの[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)]オプションが選択されている。
  - プライマリサーバーホストで、`nbseccmd -setsecurityconfig -insecurecommunication` コマンドラインオプションが「on」に設定されている。

BMR の安全な通信のサポート

NetBackup Bare Metal Restore (BMR) 8.1.1 以降のバージョンでは、NetBackup の安全な通信がサポートされます。[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、NetBackup ホストの `autoreissue` パラメータを有効にし、その後、再発行トークンを必要とせずにホスト上で証明書を配備できます。

p.281 の「証明書の自動再発行の許可または禁止」を参照してください。

BMR について詳しくは、『NetBackup Bare Metal Restore 管理者ガイド』を参照してください。

SQL Server を保護する VMware のバックアップと複数の NIC を使用する SQL Server でのバックアップの構成

特定の環境では、プライマリサーバーで[分散アプリケーションリストアマッピング (Distributed Application Restore Mapping)]ホストプロパティにホスト情報を構成する必要があります。複数の NIC を使用している場合は、そのホストプロパティ (または altnames ディレクトリ) のホストをマッピングする必要があります。VMware のバックアップについては、[VM ホスト名 (VM hostname)]ではなく[プライマリ VM 識別子 (Primary VM identifier)]を使用する場合、[プライマリ VM 識別子 (Primary VM identifier)]をそのクライアントのホスト名にマッピングする必要があります。

2

NetBackup セキュリティの強化

この章では以下の項目について説明しています。

NetBackup セキュリティおよび暗号化について

NetBackup のセキュリティと暗号化は NetBackup のプライマリサーバー、メディアサーバー、接続クライアントですべての NetBackup 操作を保護します。また、サーバーとクライアントが動作しているオペレーティングシステムも保全されます。バックアップデータは暗号化処理と Vault 処理によって保護されます。ネットワークで送信される NetBackup データは安全な専用ネットワークポートによって保護されます。

NetBackup セキュリティおよび暗号化の各レベルと実装について、次のトピックで説明します。

p.39 の「NetBackup セキュリティの実装レベル」を参照してください。

p.43 の「NetBackup アクセス制御 (NBAC)」を参照してください。

p.50 の「オペレーティングシステムのセキュリティ」を参照してください。

p.51 の「NetBackup の標準セキュリティ」を参照してください。

p.52 の「クライアント側の暗号化セキュリティ」を参照してください。

p.54 の「プライマリ、メディアサーバー、およびグラフィカルユーザーインターフェースのセキュリティ上の NBAC」を参照してください。

p.55 の「すべてに NBAC を使用したセキュリティ」を参照してください。

NetBackup セキュリティの実装レベル

NetBackup セキュリティの実装において、世界レベルは非常に広義な概念であり、エンタープライズレベルではより詳細化します。データセンターレベルではセキュリティは固有のものになります。

表 2-1は、NetBackup のセキュリティレベルをどのように実装できるかを示しています。

表 2-1 NetBackup セキュリティの実装レベル

セキュリティレベル	説明
世界レベル	Web サーバーアクセスと、発送されたり Vault に格納されたりする暗号化されたテープを指定します
企業レベル	内部ユーザーおよびセキュリティ管理者を指定します
データセンターレベル	NetBackup 操作を指定します

世界レベルのセキュリティ

世界レベルのセキュリティでは、外部ユーザーはファイアウォールで保護されている企業の Web サーバーにアクセスでき、暗号化されたテープを発送したりオフサイト Vault に

格納したりできます。世界レベルのセキュリティは企業レベルおよびデータセンターのレベルを網羅します。

図 2-1 世界レベルのセキュリティのスコープ

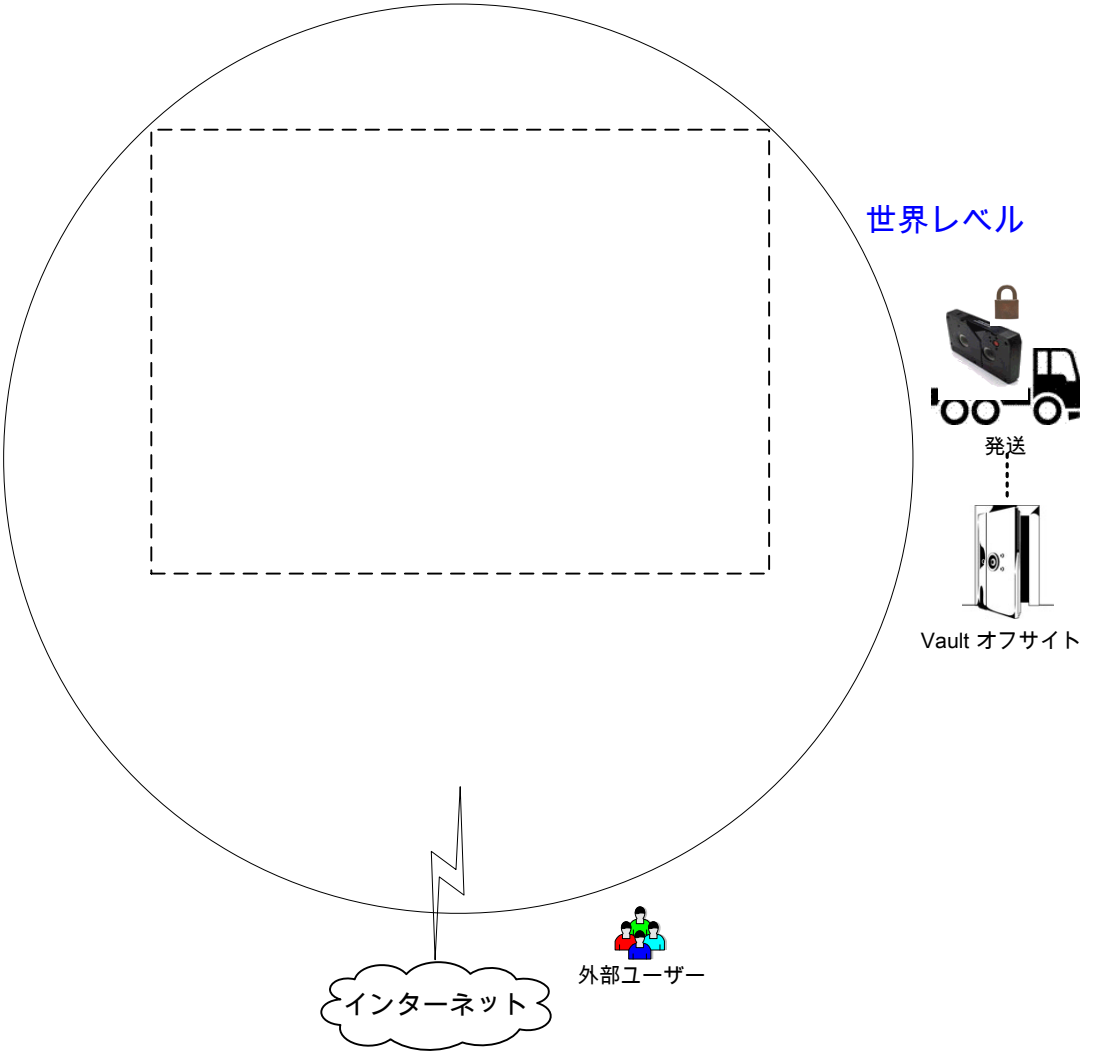


表 2-2 世界レベルのセキュリティの種類

型	説明
世界レベルの外部ユーザー	外部ユーザーはファイアウォールで保護されている Web サーバーにアクセスできます。NetBackup ポートへのアクセスは外部ファイアウォールによって遮断されるため、外部ユーザーはインターネットから NetBackup の機能にアクセスしたり、機能を使用したりすることはできません。
世界レベルのインターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。HTTP ポートを使用してファイアウォールを通過することで、インターネットから企業の Web サーバーにアクセスできます。
世界レベルの WAN	WAN (ワイドエリアネットワーク) は、セキュリティの概要の図には表示されていません。WAN は、地理的に分散している NetBackup のデータセンターをリンクするために使用される専用の高速接続です。
世界レベルのトランスポート	トランスポートトラックにより、暗号化されたクライアントテープがセキュリティ保護されたオフサイト Vault 施設に運ばれます。
世界レベルのオフサイト Vault	暗号化されたテープが現在のデータセンター以外の安全なストレージ機能で管理できることを示します。

企業レベルのセキュリティ

企業レベルのセキュリティは NetBackup セキュリティの実装のうちより目に見える部分を含んでいます。企業レベルには、内部ユーザー、セキュリティ管理者、データセンターレベルが含まれます。

図 **2-2** 企業レベルのセキュリティのスコープ

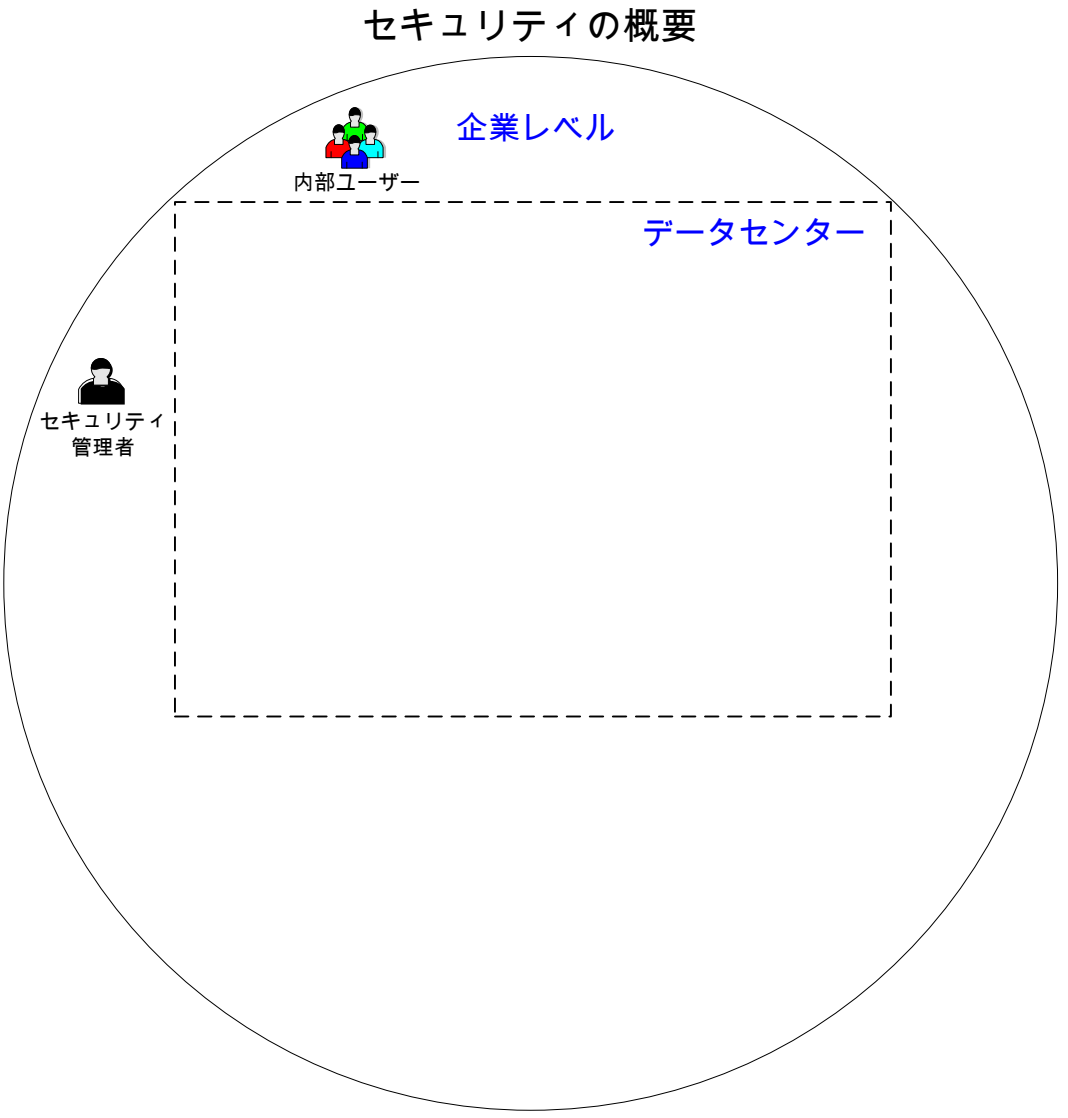


表 2-3 企業レベルのセキュリティの種類

種類	説明
内部ユーザー	データセンター内部からの NetBackup 機能へのアクセスおよび機能の使用を許可されるユーザーを示します。通常、内部ユーザーには、データベース管理者、バックアップ管理者、オペレータ、一般のシステムユーザーなどが混在しています。
セキュリティ管理者	データセンター内部から NetBackup セキュリティ機能に対してアクセスおよび管理を行う管理者権限が付与されているユーザーを示します。

データセンターレベルのセキュリティの概要

データセンターレベルのセキュリティは NetBackup セキュリティ機能の中心です。データセンターレベルのセキュリティは、ワークグループ、単一のデータセンター、または複数のデータセンターで構成される場合があります。

表 2-4 はデータセンターレベルのセキュリティ固有の展開モデルを説明します。

表 2-4 データセンターレベルのセキュリティのための展開モデル

種類	説明
ワークグループ	完全に内部で NetBackup を使用する小規模な (50 未満の) システムグループ。
単一のデータセンター	中規模から大規模な (50 を超える) ホストのグループを示し、DMZ 内のホストをバックアップできます。
複数のデータセンター	2 つ以上の地域にまたがる、中規模から大規模な (50 を超える) ホストのグループを示します。WAN によって接続できます。この構成には、バックアップ対象の DMZ 内のホストを含めることもできます。

p.39 の「NetBackup セキュリティの実装レベル」を参照してください。

NetBackup アクセス制御 (NBAC)

NetBackup アクセス制御 (NBAC) 機能は、NetBackup に NetBackup Product Authentication and Authorization を組み込んで、プライマリサーバー、メディアサーバー、およびクライアントのセキュリティを高めます。

p.39 の「NetBackup セキュリティおよび暗号化について」を参照してください。

次に、NBAC に関する重要事項を示します。

- 認証および認可は組み合わせて使用します。

- NBAC は信頼できるソースからの認証 ID を使用して、関連のあるパーティを確実に識別します。これらの ID に基づき、NetBackup 操作に対するアクセスが決定されます。NetBackup Security Services が組み込まれていることに注意してください。
- NetBackup Product Authentication and Authorization は、ルートブローカー、認証ブローカー、認可エンジンおよびグラフィカルユーザーインターフェースで構成されています。
- Oracle、Oracle Archiver、DB2、Informix、Sybase、SQL Server、SAP および EV Migrator は NBAC でサポートされません。
- NBAC はアプライアンスでサポートされません。
- NetBackup カタログバックアップは NBAC でサポートされます。

次の表は、セキュリティで使われる NetBackup コンポーネントを記述したものです。

表 2-5 セキュリティで使われる NetBackup コンポーネント

コンポーネント	説明
ルートブローカー	データセンターのインストールでは、NetBackup プライマリサーバーがルートブローカーです。別のルートブローカーを使用するためのプロビジョニングは必要ありません。ルートブローカー間の信頼を許可することをお勧めします。 ルートブローカーは認証ブローカーを認証します。ルートブローカーはクライアントを認証しません。
認証ブローカー	プライマリサーバー、メディアサーバー、GUI およびクライアントのそれぞれにクレデンシャルを設定して認証します。認証ブローカーは、コマンドプロンプトを操作するユーザーも認証します。データセンターのインストールでは、複数の認証ブローカーを配置できます。認証ブローカーをルートブローカーと組み合わせて使用することもできます。
認可エンジン	プライマリサーバーおよびメディアサーバーと通信して、認証済みユーザーの権限を決定します。これらの権限によって、指定したサーバーで利用可能な機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。データセンターのインストールには、認可エンジンが 1 つのみ必要です。認可エンジンは WAN を介して通信し、複数のデータセンター環境にある他のメディアサーバーを認可します。
グラフィカルユーザーインターフェース (GUI)	認証ブローカーからクレデンシャルを受信するリモート管理コンソールを示します。GUI は受け取ったクレデンシャルを使用して、クライアント、メディアサーバーおよびプライマリサーバーの機能へのアクセス権を取得できます。
マスターサーバー	ルートブローカー、認証ブローカー、GUI、認可エンジン、メディアサーバーおよびクライアントと通信します。
NetBackup 管理者	データセンター内部から NetBackup 機能に対してアクセスおよび管理を行う管理者権限が付与されているユーザーを示します。

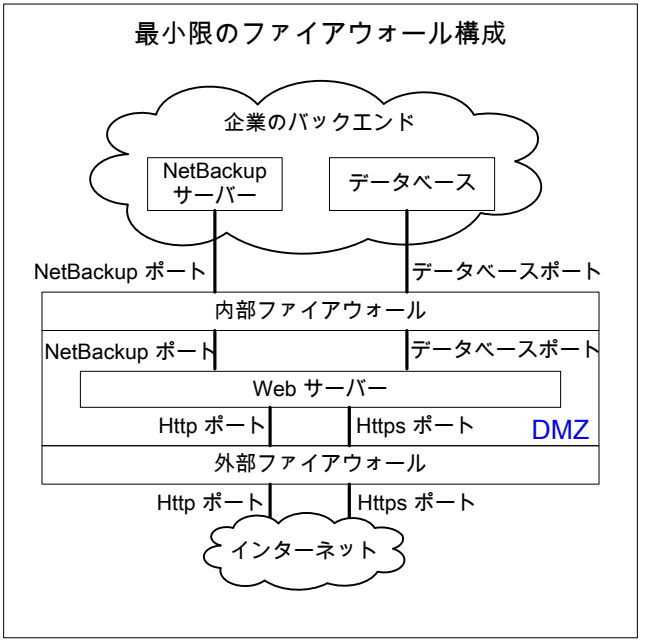
コンポーネント	説明
メディアサーバー	プライマリサーバー、ルートブローカーと認証ブローカー、認可エンジン、および 1 から 6 までのクライアントと通信します。メディアサーバーは、クライアント 5 用に、暗号化されていないデータをテープに書き込み、クライアント 6 用に、暗号化されたデータをテープに書き込みます。
クライアント	クライアント 1 から 4 までは、標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。クライアント 6 は、クライアント側で暗号化を行う形式のクライアントで、同じく DMZ に配置されています。いずれの形式のクライアントもプライマリサーバーによって管理され、クライアントのデータはメディアサーバーによってテープにバックアップされます。クライアント 5 および 6 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。
テープ	NetBackup のテープセキュリティは、次の機能を追加することによって強化できます。 ■ クライアント側の暗号化 ■ 蓄積データの暗号化 暗号化されていないデータおよび暗号化されているデータのテープはデータセンターで作成されます。1 から 5 までのクライアントの場合は、暗号化されていないテープデータが書き込まれ、データセンターのオンサイトに格納されます。クライアント 6 の場合は、暗号化されたテープが書き込まれ、ディザスタリカバリ保護に使用するためオフサイト Vault に発送されます。
暗号化	NetBackup の暗号化は、次のようにセキュリティを高めることができます。 ■ データの機密性が向上する ■ すべてのデータを効果的に暗号化することによって、物理テープの損失がそれほど重大ではなくなる ■ 最もよい危険軽減方法である 暗号化についての詳細 p.437 の「暗号化セキュリティについて考慮する際の質問」を参照してください。

コンポーネント	説明
回線上のデータセキュリティ	プライマリサーバー、メディアサーバー、クライアント間の通信およびポートを使用してファイアウォールを通過する通信と WAN を介した通信が含まれます。 ポートについて詳しくは、『NetBackup ネットワークポートリファレンスガイド』を参照してください。 NetBackup では、次の手段を使用して、回線上のデータのセキュリティを強化することができます。 ■ NetBackup アクセス制御 (NBAC) ■ 従来の NetBackup デーモンは NBAC が有効な場合に認証を使用する ■ CORBA デーモンは完全に暗号化されたチャネルを使用して機密性を確保し、データの整合性を提供する ■ ファイアウォール ■ NetBackup とそのほかの製品での未使用ポートの無効化 ■ PBX および VNETD の専用ポートを使用して NetBackup セキュリティを強化する ■ ファイアウォールを介してアクセスを監視および許可する中央ポートセット **メモ:** NetBackup 8.1 と以降のホストとの間の通信は安全です。 p.264 の「NetBackup での安全な通信について」を参照してください。

コンポーネント	説明
ファイアウォールセキュリティ	NetBackup のファイアウォールサポートはセキュリティを高めるうえで役立ちます。 ファイアウォールのセキュリティに関する重要事項を次に示します。 ■ NetBackup でファイアウォールおよび侵入検知保護を使用することをお勧めします。 ■ NetBackup の観点では、ファイアウォール保護は一般的なネットワークセキュリティに関連します。ファイアウォール保護では、窃盗犯がピッキングを試みる可能性がある「ドアロック」を減らすことに重点が置かれます。NFS、Telnet、FTP、電子メールに使用するポートのブロックを検討すると有益な場合があります。これらのポートは必ずしも NetBackup に必要ではなく、迷惑なアクセスの侵入口となる可能性があります。 ■ プライマリサーバーをできるだけ保護します ■ ファイアウォールには、次に示すように内部ファイアウォールおよび外部ファイアウォールがあります。 ■ 内部ファイアウォール - NetBackup は、DMZ 内の Web サーバークライアント 5 と暗号化クライアント 6 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、内部ファイアウォールを通過して DMZ とのデータ通信を行うことができます。HTTP ポートは外部ファイアウォールで開かれており、内部ファイアウォールを通過できません。 ■ 外部ファイアウォール - 外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
非武装地帯 (DMZ)	非武装地帯 (DMZ) は、次のようにセキュリティを高めます。 ■ DMZ は、特定のホストが使用できるポート数が高度に制御される、制限された領域です。 ■ DMZ は、外部ファイアウォールと内部ファイアウォールの間に存在します。この例での共通領域は、Web サーバーです。外部ファイアウォールでは、HTTP (標準) および HTTPS (セキュリティ保護) の Web ポートを除いたすべてのポートがブロックされます。内部ファイアウォールでは、NetBackup ポートおよびデータベースポートを除いたすべてのポートがブロックされます。DMZ を使用することで、内部の NetBackup サーバーおよびデータベース情報に外部インターネットからアクセスすることができなくなります。 DMZ は、内部ファイアウォールと外部ファイアウォールの間の Web サーバークライアント 5 および暗号化クライアント 6 に対して「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 図 2-3 に、DMZ を持つ内部ファイアウォールと外部ファイアウォールの例を示します。

次の画像は DMZ を持つ内部ファイアウォールと外部ファイアウォールの例を示します。

図 2-3 ファイアウォールおよび DMZ の例

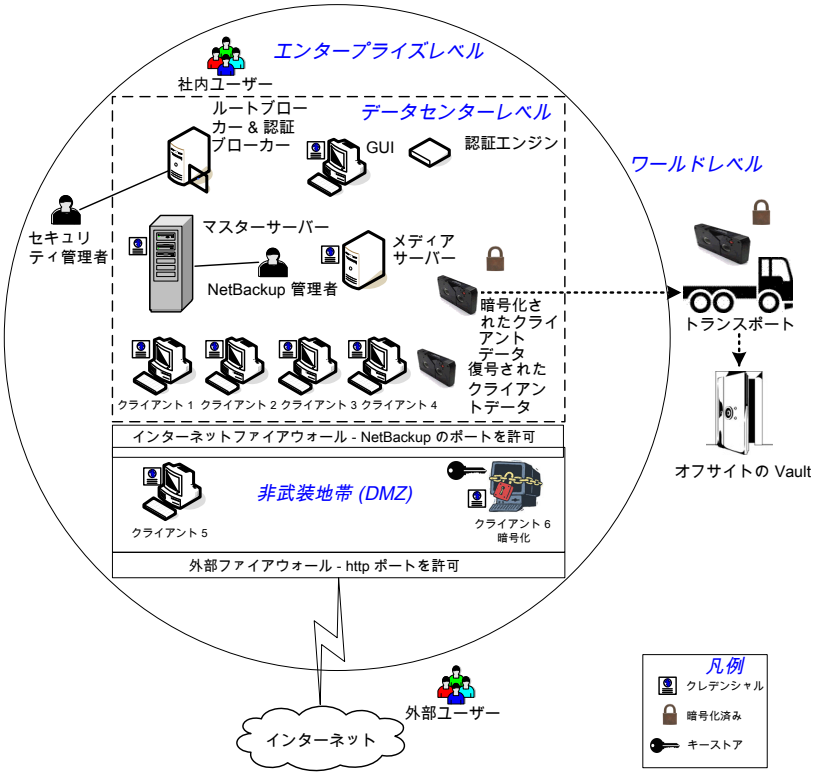


世界レベル、企業レベルおよびデータセンターレベルの統合

世界レベル、企業レベルおよびデータセンターレベルを統合したモデルは、完全に機能する標準的な NetBackup の操作が行われる領域を示します。一番外側の世界レベルでは、外部ユーザーはファイアウォールで保護されている企業の Web サーバーにアクセスすることができ、暗号化されたテープは発送されてオフサイト Vault に格納されます。その内側の企業レベルでは、内部ユーザー、セキュリティ管理者およびデータセンターレベルに関連する機能が実行されます。最も内側のデータセンターレベルでは、ワークグループ、単一のデータセンターまたは複数のデータセンターから NetBackup セキュリティの主要な機能が実行されます。

次の図に、世界レベル、企業レベルおよびデータセンターレベルの統合モデルを示します。

図 2-4 世界レベル、企業レベルおよびデータセンターレベルの統合



NetBackup セキュリティの実装形式

次の図に、NetBackup セキュリティの実装形式、特徴、複雑さのレベル、およびセキュリティの配置モデルを示します。

表 2-6 セキュリティの実装形式

セキュリティの実装形式	特徴	複雑さのレベル	セキュリティの配置モデル
p.50 の「オペレーティングシステムのセキュリティ」を参照してください。	■ オペレーティングシステムに依存 ■ システムコンポーネントに依存	システムによって異なる	ワークグループ 単一のデータセンター 複数のデータセンター

セキュリティの実装形式	特徴	複雑さのレベル	セキュリティの配置モデル
p.51 の「NetBackup の標準セキュリティ」を参照してください。	■ root または管理者として管理 ■ データは暗号化されない	低	NetBackup を使用するワークグループ 標準の NetBackup を使用する単一のデータセンター 標準的な NetBackup を使用する複数のデータセンター
p.52 の「クライアント側の暗号化セキュリティ」を参照してください。	■ データはクライアント上で暗号化される ■ 暗号化されたデータは回線を介して送信される ■ クライアントの CPU のパフォーマンスに影響を与える可能性がある ■ 鍵の保管	中	クライアント側の暗号化を使用する単一のデータセンター クライアント側の暗号化を使用する複数のデータセンター
p.54 の「プライマリ、メディアサーバー、およびグラフィカルユーザーインターフェースのセキュリティ上の NBAC」を参照してください。	■ NBAC によってプライマリサーバーおよびメディアサーバーへのアクセスに対して認可が行われる ■ プライマリサーバーおよびメディアサーバーへアクセスするシステムおよびユーザーが認証される	中	プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンター プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンター
p.55 の「すべてに NBAC を使用したセキュリティ」を参照してください。	■ NBAC によってシステム全体の認可が行われる ■ NBAC によってシステム全体の認証が行われる (サーバー、クライアント、およびユーザー)	高	すべてに NBAC を使用する単一のデータセンター すべてに NBAC を使用する複数のデータセンター

オペレーティングシステムのセキュリティ

プライマリサーバー、メディアサーバー、およびクライアントにおけるオペレーティングシステムのセキュリティは、次の対策を行うことにより強化できます。

- オペレーティングシステムのパッチをインストールする
  オペレーティングシステムのパッチには、最高レベルのシステムの整合性を維持するためにオペレーティングシステムに適用するアップグレードが含まれます。ベンダーが指定するレベルのアップグレードおよびパッチを常に適用してください。

- 安全なファイアウォール手順に従う
- 最小権限で管理を行う
- root ユーザーを制限する
- IPSEC (IP を介したセキュリティプロトコル) ハードウェアを適用する
- 外部に接続するアプリケーションの未使用ポートを無効にする
- 安全な基盤で NetBackup を実行する
- オペレーティングシステムが危険にさらされているかどうかの確認に最先端の手法を使用する
- すべてのオペレーティングシステムに同じセキュリティを実装する
- 異機種が混在する環境で、NBAC を使用して様々なシステム間での完全な相互運用性を実現する

NetBackup セキュリティの脆弱性

NetBackup の潜在的なセキュリティの脆弱性に備えて、次の保護手段を検討することをお勧めします。

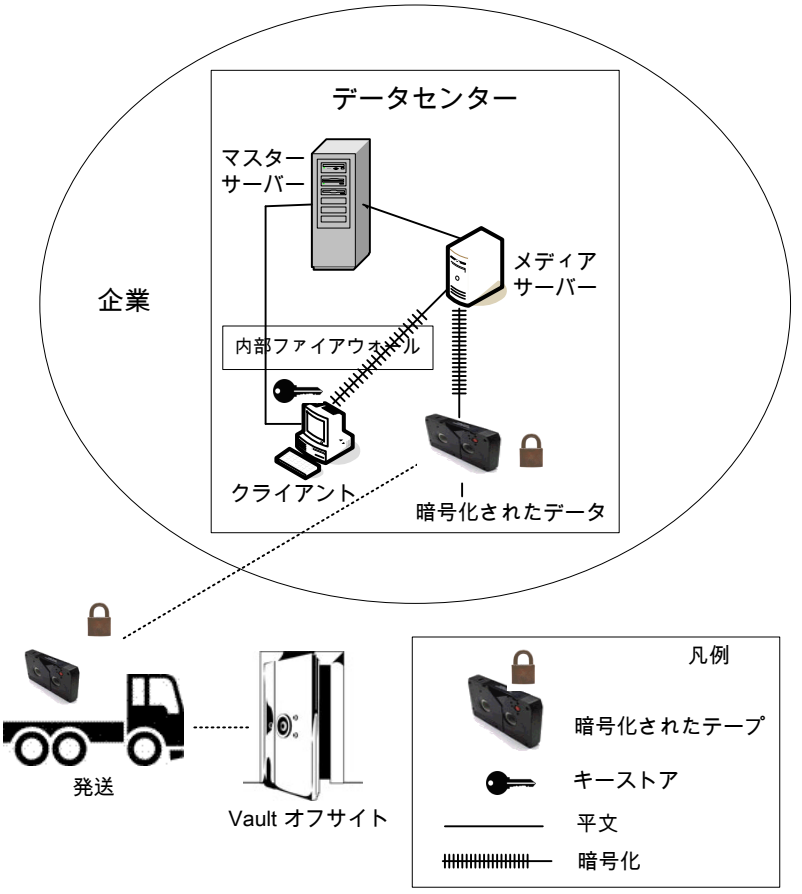
- 次に適用する NetBackup メンテナンスパッチで完全な NetBackup 更新を行う
- 累積的な NetBackup 更新を行う
- 次の Web サイトで潜在的なセキュリティの脆弱性に関する情報を参照する
  https://www.veritas.com/content/support/en_US/security.html
  https://www.veritas.com/security
- 潜在的なセキュリティの脆弱性に関して次のアドレスに電子メールで問い合わせる
  secure@veritas.com

NetBackup の標準セキュリティ

NetBackup の標準セキュリティには、オペレーティングシステムおよびデータセンターのハードウェアコンポーネントから提供されるセキュリティのみが含まれます。認可済みの NetBackup ユーザーが root または管理者として管理を行います。クライアントデータは暗号化されません。プライマリサーバー、メディアサーバー、およびクライアントはすべてローカルのエンタープライズデータセンター内で動作します。暗号化されていないデータは通常オンサイトに格納されるため、ディザスタリカバリ計画を実行できない可能性が比較的高くなります。オフサイトに送信されたデータは、傍受された場合に機密性が侵害される可能性があります。

次の画像は NetBackup の標準の構成例を示します。

図 2-5 標準的な NetBackup



クライアント側の暗号化セキュリティ

クライアント側の暗号化セキュリティを使用すると、テープ上のデータだけでなく回線を経由するデータの機密性も確保されます。この暗号化によって、組織内での回線の消極的な盗聴の危険性を軽減できます。テープをオフサイトに移動する際のデータ流出の危険性が軽減されます。暗号化鍵はクライアント上に置かれます。クライアントとメディアサーバー間の回線上のデータ通信は暗号化されます。クライアントによるデータの暗号化では、CPU に処理が集中する可能性があります。

次のバックアップポリシー形式では、クライアントの暗号化オプションの使用がサポートされます。

- AFS

- DB2
- DataStore
- DataTools-SQL-BackTrack
- Informix-On-BAR
- LOTUS_NOTES
- MS-Exchange
- MS-SharePoint
- MS-SQL-Server
- MS-Windows
- Oracle
- PureDisk-Export
- SAP
- Split-Mirror
- Standard
- Sybase

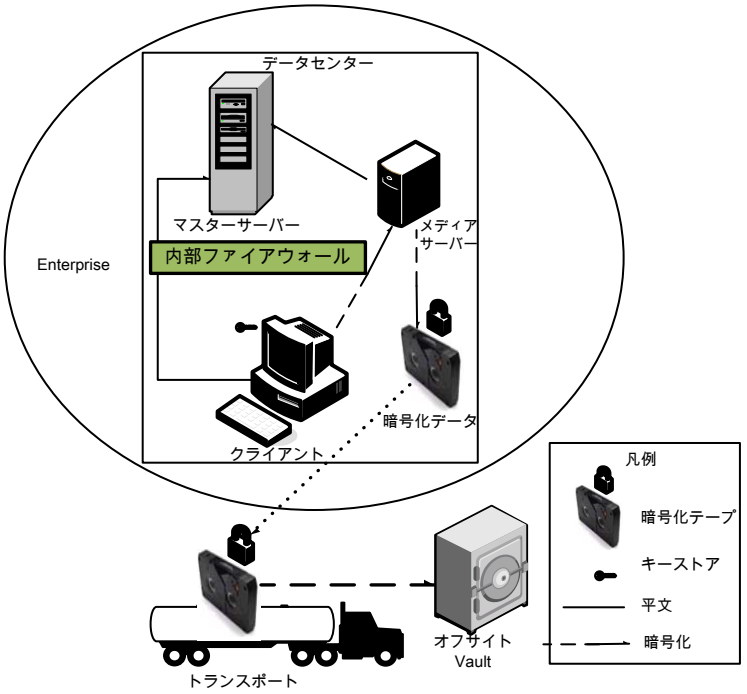
次のバックアップポリシー形式では、クライアントの暗号化オプションはサポートされません。これらのポリシー形式の場合、ポリシー属性インターフェースの暗号化のチェックボックスを選択できません。

- FlashBackup
- FlashBackup-Windows
- NDMP
- NetWare
- OS/2
- Vault

VMS と OpenVMS のクライアントはクライアントの暗号化オプションをサポートしないことに注意してください。これらのクライアントは標準のポリシー形式を使用します。

次の画像はクライアント側の暗号化の構成例を示します。

図 2-6 クライアント側の暗号化

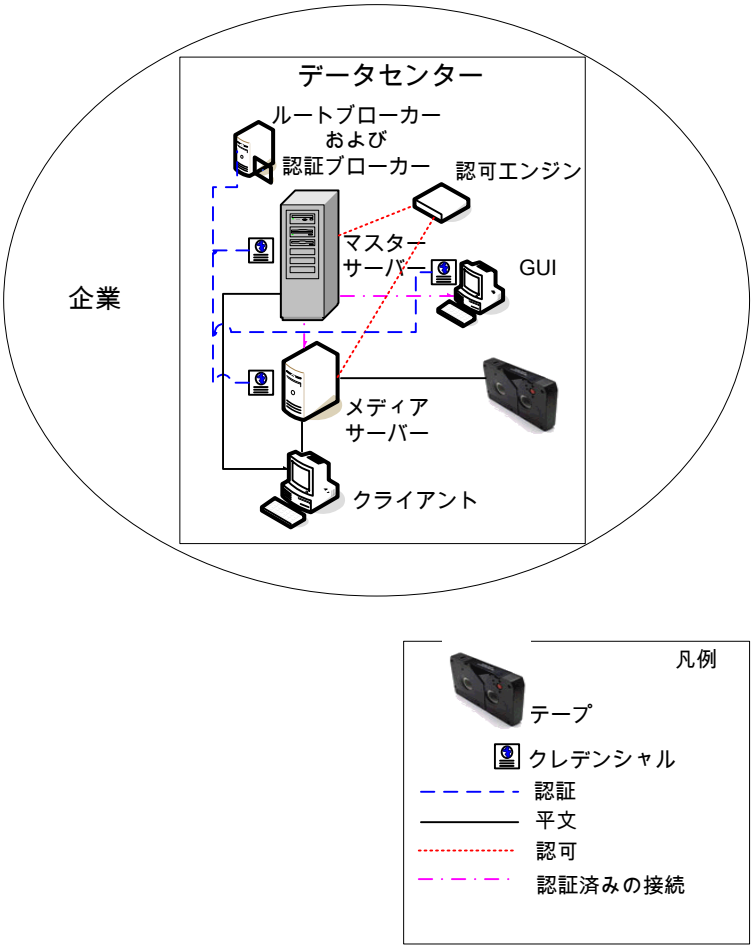


プライマリ、メディアサーバー、およびグラフィカルユーザーインターフェースのセキュリティ上の NBAC

プライマリサーバー、メディアサーバー、およびグラフィカルユーザーインターフェースセキュリティメソッド上の NBAC は認証ブローカーを使用します。ブローカーは、プライマリサーバー、メディアサーバー、およびグラフィカルユーザーインターフェースにクレデンシャルを提供します。このデータセンターの例では、プライマリサーバーおよびメディアサーバーで NetBackup アクセス制御を使用して、NetBackup の各部へのアクセスを制限しています。また、この例では、root 以外のユーザーが NetBackup を管理することもできます。NBAC はサーバーと GUI 間で使用するように設定されます。root 以外のユーザーは、オペレーティングシステムを使用して NetBackup にログオンできます。NetBackup の管理には、UNIX パスワードまたは Windows のローカルドメインを使用します。また、グローバルユーザーリポジトリ (NIS/NIS+ または Active Directory) を使って NetBackup を管理することもできます。さらに、NBAC を使用して、特定のユーザーに対して NetBackup へのアクセスレベルを制限することもできます。たとえば、日常的な操作の制御と、新しいポリシーやロボットの追加といった環境構成を分離することもできます。

次の画像に、プライマリサーバーおよびメディアサーバー構成での NBAC の例を示します。

図 2-7 プライマリサーバーおよびメディアサーバー上の NBAC



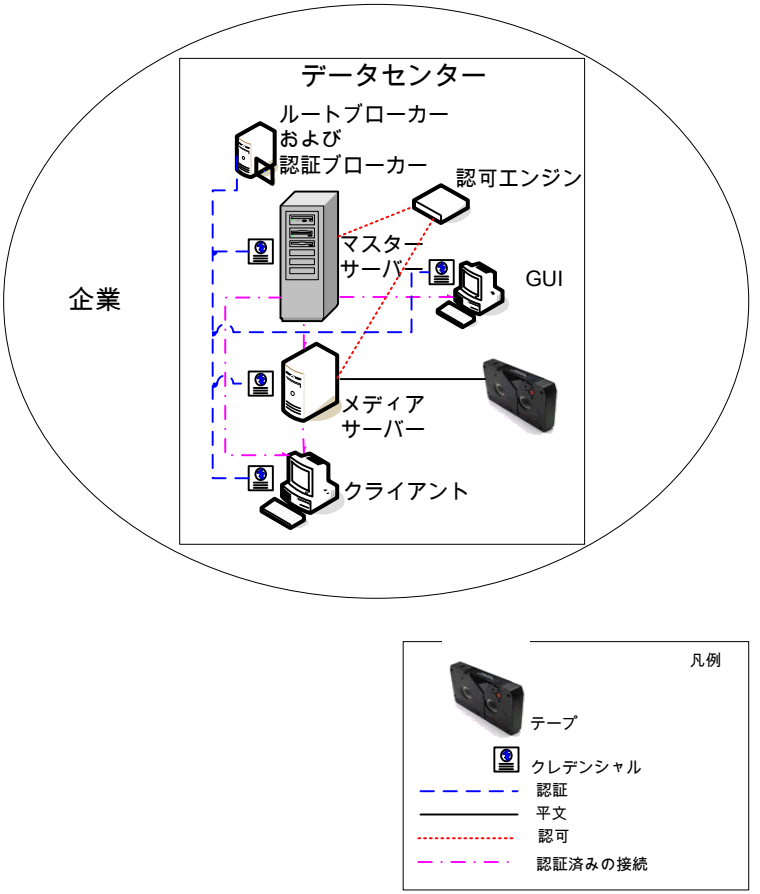
すべてに NBAC を使用したセキュリティ

すべてに NBAC を使用したセキュリティ方式では、認証ブローカーを使用して、プライマリサーバー、メディアサーバー、およびクライアントにクレデンシャルを提供します。この環境は、プライマリサーバー、メディアサーバーおよび GUI 上の NBAC モデルに非常によく似ています。主な相違点は、NetBackup 環境に含まれるすべてのホストがクレデンシャルを使用して確実に識別される点です。また、root 以外の管理者が、構成可能なア

クセスレベルに基づいて NetBackup クライアントを管理できる点も異なります。ユーザー識別情報は、Windows の Active Directory または UNIX の NIS などのグローバルリポジトリに存在する場合があります。また、識別情報は、認証ブローカーをサポートするホスト上のローカルのリポジトリ (UNIX のパスワード、Windows のローカルドメイン) に存在する場合もあります。

次の画像は NBAC の完全な構成例を示します。

図 2-8 すべてに NBAC を使用



3

セキュリティの配置モデル

この章では以下の項目について説明しています。

ワークグループ

ワークグループは、内部で NetBackup を使用する小規模な (50 未満の) システムグループです。

例のワークグループは次の項に示されています。

- p.58 の「NetBackup を使用するワークグループ」を参照してください。

単一のデータセンター

単一のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。

単一のデータセンターの例については、次の項を参照してください。

- p.62 の「標準の NetBackup を使用する単一のデータセンター」を参照してください。
- p.65 の「クライアント側の暗号化を使用する単一のデータセンター」を参照してください。
- p.67 の「プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンター」を参照してください。
- p.71 の「すべてに NBAC を使用する単一のデータセンター」を参照してください。

複数のデータセンター

複数のデータセンターには、中規模から大規模な (50 を超える) ホストのグループが含まれます。ホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。

複数のデータセンターの例については、次の項を参照してください。

- p.75 の「標準的な NetBackup を使用する複数のデータセンター」を参照してください。
- p.77 の「クライアント側の暗号化を使用する複数のデータセンター」を参照してください。
- p.82 の「プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンター」を参照してください。
- p.86 の「すべてに NBAC を使用する複数のデータセンター」を参照してください。

NetBackup を使用するワークグループ

NetBackup を使用するワークグループは、小規模な (50 未満の) システムグループです。このワークグループは NetBackup を内部で使います。通常、この構成には NIS、Active Directory などの統一されたネーミングサービスはありません。DNS、WINS のような信頼できるホストネーミングサービスを持たないこともあります。通常、この構成は大規模な企業でのテストラボや、小規模な企業の環境で使用されます。

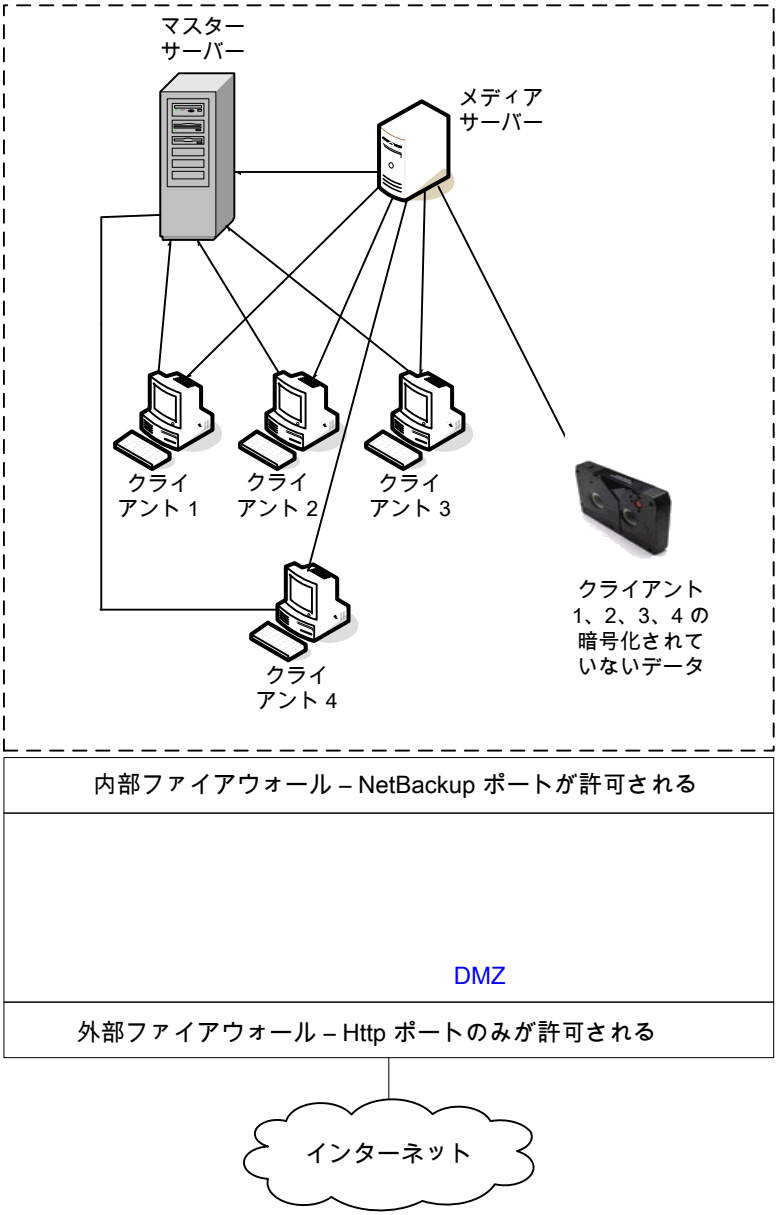
NetBackup を使用するワークグループには、次の特徴があります。

- NetBackup サーバーの数が非常に少ない

- コンピュータ環境が小規模である
- 外部に接続する装置が実装されていない

図 3-1 に、NetBackup を使用するワークグループの例を示します。

図 **3-1** NetBackup を使用するワークグループ



次の表に、ワークグループで使われる NetBackup の構成要素を示します。

表 3-1 ワークグループで使われる NetBackup の構成要素

構成要素	説明
マスターサーバー	メディアサーバーおよびクライアント 1、2、3、4 と通信します。
メディアサーバー	プライマリサーバーおよびクライアント 1、2、3、4 と通信します。メディアサーバーは、クライアント 1、2、3、4 の暗号化されていないデータのテープへの書き込みを管理します。
テープ	クライアント 1、2、3、4 の暗号化されていないバックアップデータが格納されます。
クライアント	クライアント 1、2、3、4 は、プライマリサーバーで管理される標準的な NetBackup クライアントです。これらのクライアントには、メディアサーバーによってテープにバックアップされる暗号化されていないデータが存在します。
内部ファイアウォール	NetBackup が DMZ 内のクライアントにアクセスすることを許可します。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、インターネットから内部ファイアウォールを通過できません。内部ファイアウォールは、ワークグループ配置モデルでは使用されません。この例では、内部ファイアウォールにアクセスするクライアントが存在しないため、内部ファイアウォールを通過する NetBackup ポートを開く必要はありません。 **メモ:** この例では、内部ファイアウォールの外側にクライアントは存在しません。このため、内部ファイアウォールを通過する NetBackup ポートを開く必要はありません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している NetBackup クライアントに「安全な」操作領域を提供します。DMZ で操作を行う可能性のあるクライアントには、標準的な NetBackup クライアントまたは暗号化を行う NetBackup クライアントのいずれかを使用する Web サーバー NetBackup クライアントがあります。DMZ 内のクライアントは、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバー NetBackup クライアントは、一般的な HTTP ポートを使用して、外部ファイアウォールからのインターネットへの接続を受信できます。ワークグループ配置モデル内のクライアントは、DMZ にアクセスできません。
外部ファイアウォール	外部ユーザーは、一般的に HTTP ポートを経由してインターネットから外部ファイアウォールを通過して、DMZ 内にある Web サーバー NetBackup クライアントにアクセスできます。内部ファイアウォールを通過して通信を行うクライアント向けに開かれた NetBackup ポートは、外部ファイアウォールを通過してインターネットにアクセスすることはできません。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ワークグループ配置モデル内のクライアントでは、インターネットは使用されません。 **注意:** NetBackup クライアントは、DMZ の外側に配置したり、インターネット上に直接配置したりしないでください。外部ファイアウォールを使用して、常に NetBackup ポートを外部からブロックする必要があります。

標準の NetBackup を使用する単一のデータセンター

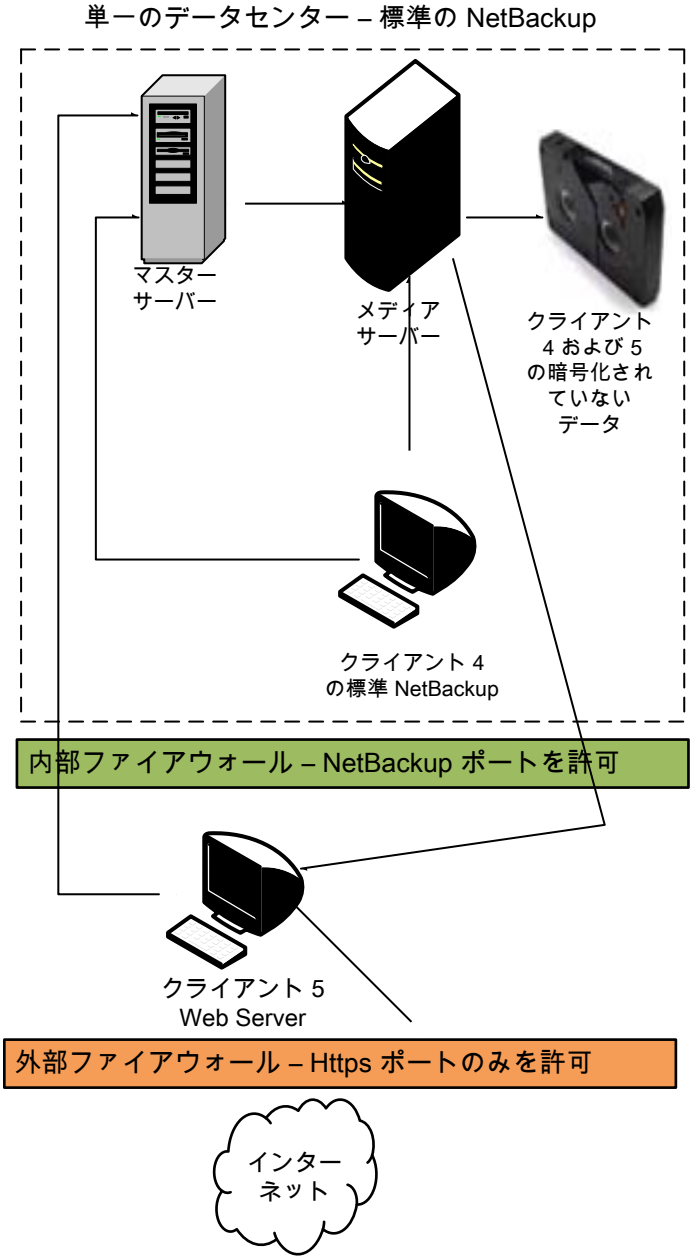
標準的な NetBackup を使用する単一のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。単一のデータセンターには、内部専用のホストと、DMZ を介してインターネットに展開するホストの両方が含まれます。通常、この構成には、ホスト向けの中央集中型ネーミングサービス (DNS、WINS など) が含まれます。また、ユーザー向けの中央集中型ネーミングサービス (NIS、Active Directory など) も含まれます。

標準の NetBackup を使用する単一のデータセンターには、次の特徴があります。

- 外部に接続するホストがある
- 通常、中央集中型ネーミングサービスが存在する
- ホスト数が 50 を超える
- 最も単純な構成で、NetBackup の一般的な知識のみが必要である
- NetBackup ユーザー用に使用される標準的な構成である
- バックアップ時に、回線上でデータの消極的な妨害が行われる危険性がほとんどない

図 3-2 に、標準の NetBackup を使用する単一のデータセンターの例を示します。

図 3-2 標準の NetBackup を使用する単一のデータセンター



次の表に、標準的なNetBackupを使用する単一のデータセンターで使われるNetBackupの構成要素を示します。

表 3-2　標準的な NetBackup を使用する単一のデータセンターにおける NetBackup の構成要素

構成要素	説明
マスターサーバー	メディアサーバー、標準的な NetBackup クライアント 4 および DMZ 内の Web サーバー NetBackup クライアント 5 と通信します。
メディアサーバー	プライマリサーバー、標準的な NetBackup クライアント 4 および DMZ 内の Web サーバー NetBackup クライアント 5 と通信します。メディアサーバーは、クライアント 4、5 の暗号化されていないデータのテープへの書き込みを管理します。
テープ	クライアント 4、5 の暗号化されていないバックアップデータが格納されます。
クライアント	クライアント 4 は標準的な NetBackup 形式であり、クライアント 5 は Web サーバー形式です。これらのクライアントはどちらもプライマリサーバーによって管理され、それらの暗号化されていないデータはメディアサーバーによってテープにバックアップされます。クライアント 4 は、データセンター内に存在します。クライアント 5 は、DMZ 内に存在します。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。照合を行うすべての NetBackup 通信は、暗号化されていない状態で回線を介して送信されることに注意してください。
内部ファイアウォール	NetBackup は、DMZ 内の Web サーバー NetBackup クライアント 5 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、インターネットから内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している NetBackup クライアント 5 Web サーバーに「安全な」操作領域を提供します。DMZ 内のクライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。
外部ファイアウォール	外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートはクライアント 5 に対して開かれており、内部ファイアウォールを通過して通信が行われます。 **注意:** NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。外部ファイアウォールでは、クライアント 5 に対する HTTP ポートだけが開かれており、インターネットに接続することができます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットを介した接続を受信できます。

クライアント側の暗号化を使用する単一のデータセンター

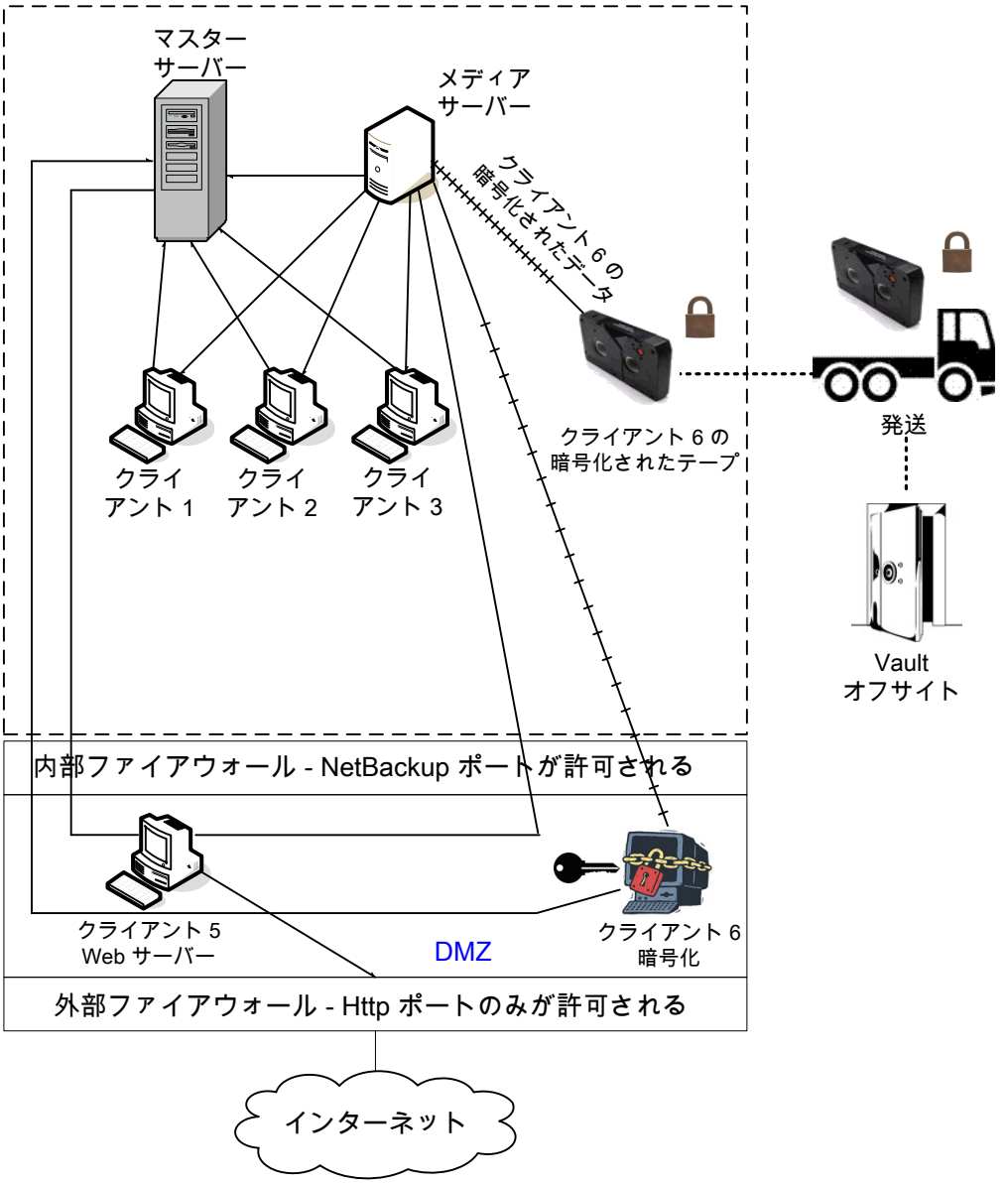
クライアント側の暗号化を使用する単一のデータセンターの例では、クライアント側の暗号化によって、テープ上のデータだけでなく回線を経由するデータの機密性も確保されます。クライアント側の暗号化によって、組織内での回線の消極的な盗聴の危険性が軽減されます。テープをオフサイトに移動する際のデータ流出の危険性が軽減されます。このデータセンターモデルでは、中規模から大規模 (50 を超える) の管理対象ホストに対応できます。データセンター内および DMZ 内のクライアントは、ホストおよびユーザー識別情報に中央集中型ネーミングサービスを使うことができます。

クライアント側の暗号化を使用する単一のデータセンターには、次の特徴があります。

- オフサイトデータの保護に役立つ
- クライアントからのデータが暗号化されるため、回線でのデータの消極的な妨害が防止される
- 鍵の管理はクライアントに分散される
- NetBackup 独自の暗号化オプションが使用される
- 暗号化処理にはクライアントの CPU が使用される
- データを戻すには鍵が必要である。鍵を失うと、データも失われます。
- オフサイトでテープをスキャンする必要がある場合または回線上での機密性が必要な場合に有効である

図 3-3 に、クライアント側の暗号化を使用する単一のデータセンターの例を示します。

図 3-3 クライアント側の暗号化を使用する単一のデータセンター



次の表に、クライアント側の暗号化を使用する単一のデータセンターで使われる NetBackup の構成要素を示します。

表 3-3 クライアント側の暗号化を使用する単一のデータセンターにおける NetBackup の構成要素

構成要素	説明
非武装地帯 (DMZ)	Web サーバークライアント 5 および暗号化クライアント 6 に対して「安全な」操作領域を提供します。これらのクライアントは、内部ファイアウォールと外部ファイアウォールの間に存在します。DMZ 内の Web サーバークライアント 5 と暗号化クライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 と暗号化クライアント 6 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。DMZ 内の暗号化クライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。
外部ファイアウォール	外部ユーザーは、Web サーバークライアント 5 および暗号化クライアント 6 にアクセスできます。これらのクライアントは HTTP ポートを経由してインターネットから DMZ 内にアクセスできます。NetBackup ポートは Web サーバークライアント 5 と暗号化クライアント 6 に対して開かれており、内部ファイアウォールを通過して通信が行われます。ただし、NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 と暗号化クライアント 6 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。外部ファイアウォールによって、クライアント 5、6 のインターネット上での双方向の通信が制限されます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンター

プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンターの例では、プライマリサーバーとメディアサーバー上で NetBackup のアクセス制御を使用します。この構成では、NetBackup へのアクセスを部分的に制限し、root 以外のユーザーが NetBackup を管理できるようになっています。NBAC はサーバーと GUI 間で実行できるように構成されます。root 以外のユーザーはオペレーティングシステム (UNIX のパスワードまたは Windows のローカルドメイン) またはグローバルユーザーリポジトリ (NIS/NIS+ または Active Directory) を使用して NetBackup にログインし、NetBackup を管理することができます。NBAC を使用して、特定のユーザーに対して NetBackup へのアクセスレベルを制限することもできます。たとえば、日常的な操作の制御と、新しいポリシーやロボットの追加といった環境構成を分離することもできます。

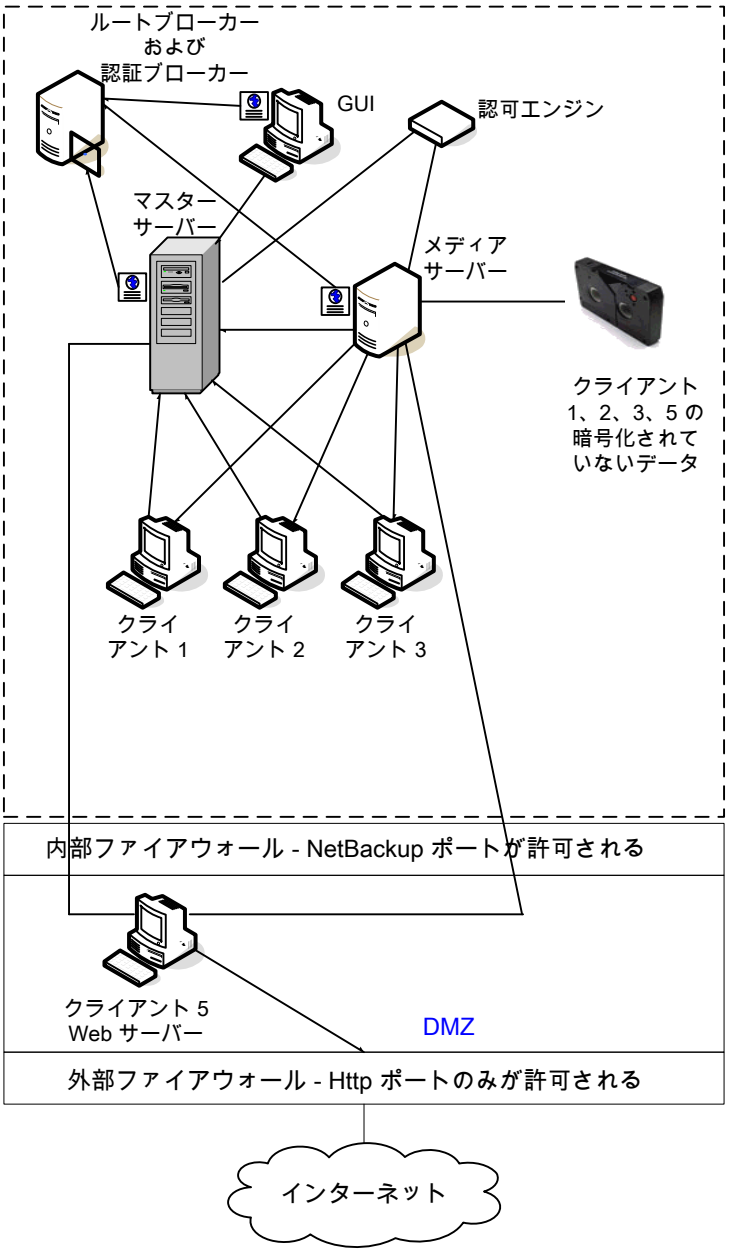
プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンターには、次の特徴があります。

- root 以外のユーザーを管理する

- Windows のユーザー ID を使用して UNIX を管理する
- UNIX アカウントを使用して Windows を管理する
- 特定のユーザーの操作を分離および制限する
- クライアントホストの root ユーザーまたは管理者はローカルクライアントのバックアップとリストアを実行できる
- 他のセキュリティ関連のオプションと組み合わせることができる
- すべてのサーバーで、適切な NetBackup バージョンが必要

図 3-4 に、プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンターの例を示します。

図 3-4 プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンター



次の表に、プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンターに使用される NetBackup の構成要素を示します。

表 3-4　プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンターにおける NetBackup の構成要素

構成要素	説明
プライマリサーバー	メディアサーバー、ルートブローカーおよび認証ブローカーと通信します。また、認可エンジン、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) とも通信します。また、プライマリサーバーは、認証ブローカーと通信して、認証ブローカーからクレデンシャルを受信します。 CLI または GUI がプライマリサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。次に、デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
メディアサーバー	プライマリサーバー、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) と通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。メディアサーバーによって、クライアント 1、2、3、5 の暗号化されていないデータのテープへの書き込みが可能になります。 CLI または GUI がメディアサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。次に、デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
GUI	このリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびプライマリサーバーの機能へのアクセス権を取得します。
ルートブローカー	認証ブローカーを認証しますが、クライアントを認証しません。この例では、ルートブローカーおよび認証ブローカーは同じコンポーネントとして示されています。
認証ブローカー	プライマリサーバー、メディアサーバーおよび GUI に対してそれぞれクレデンシャルを設定し、認証します。コマンドプロンプトが使われる場合、認証ブローカーはユーザーも認証します。
認可エンジン	プライマリサーバーおよびメディアサーバーと通信して、認証済みユーザーの権限を決定します。これらの権限によって、ユーザーが利用できる機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。必要となる認可エンジンは 1 つだけです。 **メモ:** 認可エンジンは、デーモンプロセスとしてプライマリサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	クライアント 1、2、3、5 の暗号化されていないバックアップデータが格納されます。
クライアント	クライアント 1、2、3 は標準の NetBackup 形式であり、クライアント 5 は Web サーバー形式です。どちらの形式もプライマリサーバーによって管理され、暗号化されていないデータがメディアサーバーを介してテープにバックアップされます。クライアント 1、2、3 は、データセンター内に存在します。クライアント 5 は、DMZ 内に存在します。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。

構成要素	説明
内部ファイアウォール	NetBackup は、DMZ 内の Web サーバークライアント 5 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している Web サーバークライアント 5 に「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。
外部ファイアウォール	外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートはクライアント 5 に対して開かれており、内部ファイアウォールを通過して通信が行われます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。クライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。クライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

すべてに NBAC を使用する単一のデータセンター

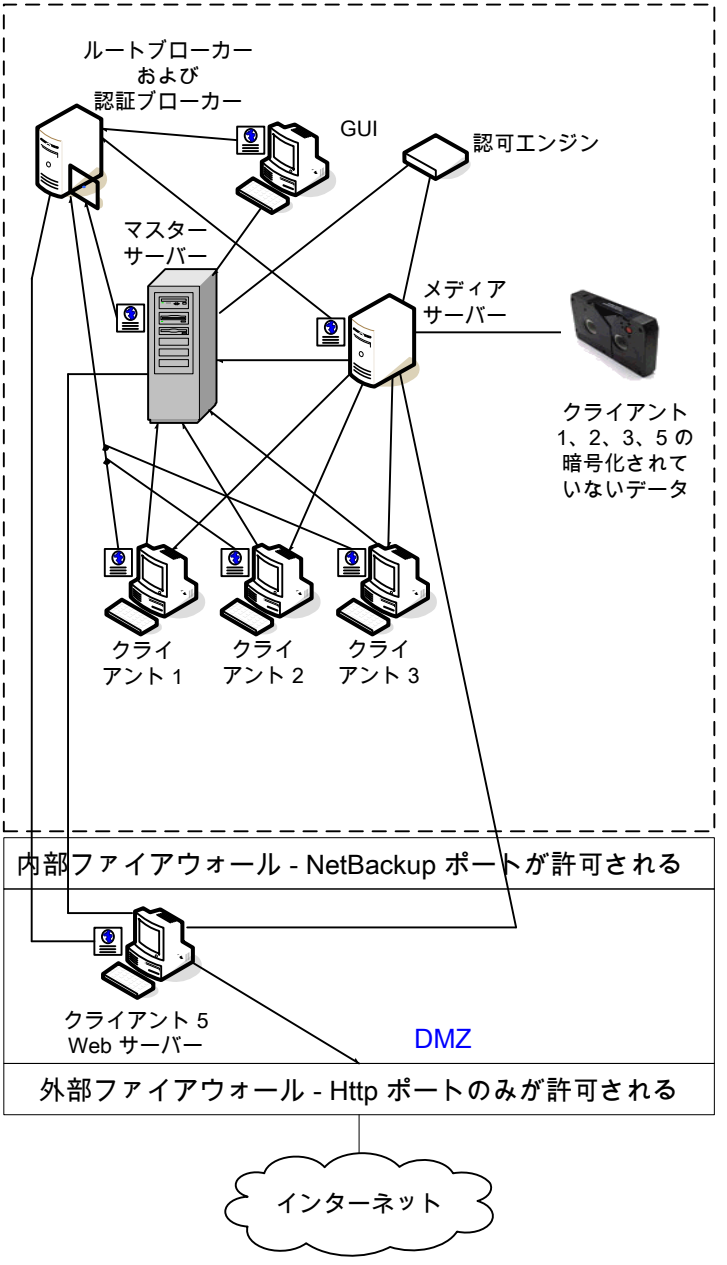
すべてに NBAC を使用する単一のデータセンターの環境は、プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンターによく似ています。主な相違点は、NetBackup 環境に含まれるすべてのホストがクレデンシャルを使用して確実に識別される点です。また、root 以外の管理者が、構成可能なアクセスレベルに基づいて NetBackup クライアントを管理できる点も異なります。ユーザー識別情報は、Windows の Active Directory または UNIX の NIS などのグローバルリポジトリに存在する場合があります。また、識別情報は、認証ブローカーをサポートするホスト上のローカルのリポジトリ (UNIX のパスワード、Windows のローカルドメイン) に存在する場合もあります。

すべてに NBAC を使用する単一のデータセンターには、次の特徴があります。

- プライマリサーバーとメディアサーバーで NBAC を使用する単一のデータセンターの場合の特徴と類似している (クライアントの root ユーザーまたは管理者についての項目は除く)
- クライアントシステムでは、ローカルバックアップとリストアを行うために root 以外または管理者以外のユーザーが設定される場合がある (デフォルト設定)
- この環境では、NetBackup に含まれるすべてのホストの信頼できる識別が容易である
- すべてのホストで、適切な NetBackup バージョンが必要

図 3-5 に、すべてに NBAC を使用する単一のデータセンターの例を示します。

図 **3-5** すべてに NBAC を使用する単一のデータセンター



次の表に、すべてに NBAC を使用する単一のデータセンターで使われる NetBackup の構成要素を示します。

表 3-5　すべてに NBAC を使用する単一のデータセンターにおける NetBackup の構成要素

構成要素	説明
プライマリサーバー	メディアサーバー、ルートブローカーおよび認証ブローカーと通信します。また、認可エンジン、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) とも通信します。プライマリサーバーは、さらに認証ブローカーと通信して、認証ブローカーからクレデンシャルを受信します。 CLI または GUI がプライマリサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
メディアサーバー	プライマリサーバー、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) と通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。メディアサーバーによって、クライアント 1、2、3、5 の暗号化されていないデータのテープへの書き込みが可能になります。 CLI または GUI がメディアサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
GUI	このリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびプライマリサーバーの機能へのアクセス権を取得します。
ルートブローカー	認証ブローカーを認証しますが、クライアントを認証しません。図 3-5 では、ルートブローカーおよび認証ブローカーは同じコンポーネントとして示されています。
認証ブローカー	プライマリサーバー、メディアサーバー、GUI、クライアントおよびユーザーに対してそれぞれクレデンシャルを設定し、認証します。
認可エンジン	プライマリサーバーおよびメディアサーバーと通信して、認証済みユーザーの権限を決定します。また、認可エンジンには、ユーザーグループおよび権限が格納されます。必要となる認可エンジンは 1 つだけです。 **メモ:** 認可エンジンは、デーモンプロセスとしてプライマリサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	クライアント 1、2、3、5 の暗号化されていないバックアップデータが格納されます。

構成要素	説明
クライアント	クライアント 1、2、3 は標準の NetBackup 形式であり、クライアント 5 は Web サーバー形式です。認証ブローカーからクレデンシャルを受信すると、クライアント 1、2、3、5 は NetBackup Product Authentication Service ドメインに認証されます。標準サーバー形式と Web サーバー形式はどちらもプライマリサーバーによって管理され、暗号化されていないデータがメディアサーバーを介してテープにバックアップされます。クライアント 1、2、3 は、データセンター内に存在します。クライアント 5 は、DMZ 内に存在します。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。
内部ファイアウォール	NetBackup は、DMZ 内の Web サーバークライアント 5 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している Web サーバークライアント 5 に「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。
外部ファイアウォール	外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートはクライアント 5 に対して開かれており、内部ファイアウォールを通過して通信が行われます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。クライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。クライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

標準的な NetBackup を使用する複数のデータセンター

標準的な NetBackup を使用する複数のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

複数のデータセンターには、内部専用のホストと、DMZ を介してインターネットに展開するホストの両方が含まれます。通常、この構成には、ホスト向けの中央集中型ネーミングサービス (DNS、WINS など) が含まれます。また、ユーザー向けの中央集中型ネーミングサービス (NIS、Active Directory など) も含まれます。

標準的な NetBackup を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- 通常、中央集中型ネーミングサービスが存在する
- ホスト数が 50 を超える
- 最も単純な構成で、NetBackup の一般的な知識のみが必要である
- バックアップ時に、回線上でデータの消極的な妨害が行われる危険性がほとんどない

次の表に、標準的な NetBackup を実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 3-6　標準的な NetBackup が実装された複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	プライマリサーバー、メディアサーバー 1、クライアント 4 の標準的な NetBackup、クライアント 4 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	メディアサーバー 2、クライアント 10 の標準的な NetBackup、クライアント 10 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN を使用することで、プライマリサーバーをメディアサーバー 2 およびクライアント 10 に接続できます。
プライマリサーバー	ロンドンにあり、ロンドンにあるメディアサーバー 1 と通信します。また、このプライマリサーバーは、WAN を介して東京にあるメディアサーバー 2 とも通信します。このプライマリサーバーは、ロンドンにある標準的な NetBackup クライアント 4 と通信し、WAN を介して東京にあるクライアント 10 と通信します。
メディアサーバー	複数のデータセンターには 2 つのメディアサーバーがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンのメディアサーバー 1 は、プライマリサーバーと、ロンドンにある標準的な NetBackup クライアント 4 とも通信します。メディアサーバー 1 は、ロンドンにあるクライアント 4 の暗号化されていないデータのテープへの書き込みを管理します。 東京のメディアサーバー 2 は、ロンドンにあるプライマリサーバーと、東京にある標準的な NetBackup クライアント 10 と通信します。メディアサーバー 2 は、東京にあるクライアント 10 の暗号化されていないデータのテープへの書き込みを管理します。
テープ	テープは、ロンドンと東京の両方のデータセンターで作成されます。ロンドンのテープには、クライアント 4 の暗号化されていないバックアップデータが格納されます。東京のテープには、クライアント 10 の暗号化されていないバックアップデータが格納されます。

構成要素	説明
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。クライアント 4 と 10 は、標準的な NetBackup 形式です。どちらのクライアントも、ロンドンにあるプライマリサーバーで管理できます。これらのクライアントの暗号化されていないデータは、メディアサーバーによってテープにバックアップされます。暗号化されていないデータは、ロンドンのクライアント 4 のテープと、東京のクライアント 10 のテープの両方に書き込まれます。クライアント 10 の照合を行うすべての NetBackup 通信は、暗号化されていない状態で回線 (WAN) を介して東京からロンドンに送信されることに注意してください。
内部ファイアウォール	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、内部ファイアウォールは使用されません。
非武装地帯 (DMZ)	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、DMZ は使用されません。
外部ファイアウォール	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、外部ファイアウォールは使用されません。
インターネット	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、インターネットは使用されません。

クライアント側の暗号化を使用する複数のデータセンター

クライアント側の暗号化オプションを使用する複数のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

この複数のデータセンターの例では、クライアント側の暗号化を利用して、テープだけでなく回線におけるデータの機密性も確保できます。この暗号化によって、組織内での回線の消極的な盗聴の危険性を軽減できます。テープをオフサイトに移動する際のデータ流出の危険性が軽減されます。このデータセンターモデルでは、中規模から大規模 (50 を超える) の管理対象ホストに対応できます。データセンター内および DMZ 内のクライアントは、ホストおよびユーザー識別情報に中央集中型ネーミングサービスを使うことができます。

クライアント側の暗号化を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- オフサイトデータの保護に役立つ
- クライアントからのデータが暗号化されるため、回線でのデータの消極的な妨害が防止される
- 鍵の管理はクライアントに分散される

- NetBackup 独自の暗号化オプションが使用される
- 暗号化処理にはクライアントの CPU が使用される
- データを戻すには鍵が必要である。鍵を失うと、データも失われます。
- オフサイトでテープをスキャンする必要がある場合または回線上での機密性が必要な場合に有効である

次の表に、クライアント側の暗号化を実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 3-7　クライアント側の暗号化を実装した複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	プライマリサーバー、メディアサーバー 1、クライアント 4、5、6 が含まれます。また、クライアント 6、7 の暗号化されたデータテープと、クライアント 4、5 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	メディアサーバー 2、クライアント 7、10、11、12 が含まれます。また、クライアント 7、12 の暗号化されたデータテープと、クライアント 10、11 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN を使用することで、ロンドンのプライマリサーバーを、東京のメディアサーバー 2 およびクライアント 7、10、11、12 に接続できます。また、WAN を使用して、ロンドンのメディアサーバー 1 を、東京のクライアント 7 に接続することもできます。
プライマリサーバー	プライマリサーバーはロンドンのデータセンターにあり、メディアサーバー 1 およびクライアント 4、5、6 と通信します。また、このプライマリサーバーは、WAN を使用して東京のメディアサーバー 2 およびクライアント 7、10、11、12 と通信します。

構成要素	説明
メディアサーバー	複数のデータセンターは 2 つのメディアサーバーを使います。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、プライマリサーバーおよびクライアント 4、5、6 と通信します。メディアサーバー 1 は、東京のクライアント 7 とも通信します。メディアサーバー 1 は、クライアント 4、5 の暗号化されていないデータをテープに書き込みます。また、クライアント 6、7 の暗号化されたデータもテープに書き込みます。クライアント 7 は東京に存在しますが、このテープバックアップはロンドンに存在することに注意してください。クライアント 6、7 の暗号化されたテープは、ロンドンのオフサイト Vault に発送されます。 東京のメディアサーバー 2 は、WAN を介してロンドンのプライマリサーバーと通信し、また、東京のクライアント 7、10、11、12 と通信します。メディアサーバー 2 は、クライアント 10、11 の暗号化されていないデータをテープに書き込みます。また、クライアント 7、12 の暗号化されたデータもテープに書き込みます。クライアント 7 は東京に存在し、ロンドンでバックアップされますが、東京でもバックアップされることに注意してください。クライアント 7、12 の暗号化されたテープは、東京のオフサイト Vault に発送されます。
クライアント側の暗号化	クライアント側の暗号化 (図には示されていない) によって、テープだけでなく回線におけるデータの機密性も確保されます。
テープ	暗号化されていないデータテープおよび暗号化されたデータテープの両方が、ロンドンと東京のデータセンターで作成されます。暗号化されたテープには、クライアント側で暗号化されたバックアップデータが格納されます。ロンドンでは、クライアント 4、5 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。クライアント 6、7 用には、暗号化されたテープが書き込まれます。暗号化されたテープは、ディザスタリカバリ保護用にロンドンのオフサイト Vault に発送されます。 東京では、クライアント 10、11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。クライアント 7、12 用には、暗号化されたテープが書き込まれます。クライアント 7 は東京に存在し、東京でバックアップされますが、ロンドンでもバックアップされることに注意してください。暗号化されたテープは、ディザスタリカバリ保護用に東京のオフサイト Vault に発送されます。 **メモ:** データを復号するには、そのデータの暗号化に使用した鍵が利用可能である必要があります。
トランスポート	複数のデータセンターは 2 つのトランスポートを使います。1 つはロンドン、もう 1 つは東京にあります。ロンドンのトランスポートトラックにより、クライアント 6、7 の暗号化されたテープは、セキュリティ保護されたロンドンのオフサイト Vault 施設に運ばれます。東京のトランスポートトラックにより、クライアント 7、12 の暗号化されたテープは、セキュリティ保護された東京のオフサイト Vault 施設に運ばれます。クライアント 7 のバックアップコピーは、ロンドンと東京の両方の Vault に格納されることに注意してください。 **メモ:** 輸送中に遠隔の場所でテープが失われた場合でも、データセンターの管理者は、データの漏洩リスクを軽減することができます。漏洩はクライアント側でのデータの暗号化の使用により軽減されます。

構成要素	説明
オフサイト Vault	複数のデータセンターは 2 つのオフサイト Vault を使います。1 つはロンドン、もう 1 つは東京にあります。どちらの Vault も、暗号化されたテープを格納する安全な施設であり、それぞれのデータセンターとは別の場所に存在します。 **メモ:** 暗号化されたテープをデータセンターから離れた場所に格納することで、ディザスタリカバリ保護が向上します。
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンの場合、クライアント 4 は標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。クライアント 6 はクライアント側で暗号化を行うクライアントで、同じく DMZ に配置されています。いずれの形式のクライアントもプライマリサーバーによって管理され、クライアントのデータはメディアサーバー 1 によってテープにバックアップされます。クライアント 5 と 6 は、NetBackup のみのポートを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 6 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。 東京の場合、クライアント 7 はクライアント側で暗号化を行うクライアントですが、DMZ の外に配置されています。クライアント 10 は、標準的な NetBackup 形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式です。クライアント 12 はクライアント側で暗号化を行うクライアントで、同じく DMZ に配置されています。すべての形式のクライアントは、ロンドンのプライマリサーバーによって管理できます。クライアント 7 のデータは、メディアサーバー 1 および 2 によってテープにバックアップされます。クライアント 10、11、12 のデータは、メディアサーバー 2 によってテープにバックアップされます。クライアント 11、12 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 12 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。
内部ファイアウォール	複数のデータセンターは 2 つの内部ファイアウォールを使います。1 つはロンドン、もう 1 つは東京にあります。ロンドンの場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 とクライアント側で暗号化を行うクライアント 6 にアクセスできます。東京の場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 11 とクライアント側で暗号化を行うクライアント 12 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。

構成要素	説明
非武装地帯 (DMZ)	複数のデータセンターは 2 つの DMZ を使います。1 つはロンドン、もう 1 つは東京にあります。ロンドンの DMZ は、Web サーバークライアント 5 およびクライアント側で暗号化を行うクライアント 6 に対して「安全な」操作領域を提供します。このクライアントは、内部ファイアウォールと外部ファイアウォールとの間に存在します。DMZ 内の Web サーバークライアント 5 およびクライアント側で暗号化を行うクライアント 6 は、NetBackup と通信できます。これらのクライアントは両方とも、指定された NetBackup ポートを使って内部ファイアウォールを通過し、通信を行います。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京の DMZ は、Web サーバークライアント 11 およびクライアント側で暗号化を行うクライアント 12 に対して「安全な」操作領域を提供します。クライアント 12 は、内部ファイアウォールと外部ファイアウォールとの間に存在します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。
外部ファイアウォール	複数のデータセンターは 2 つの外部ファイアウォールを使うことができます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。クライアント側で暗号化を行うクライアント 6 には、インターネットからはアクセスできません。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは Web サーバークライアント 11 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。クライアント側で暗号化を行うクライアント 12 には、インターネットからはアクセスできません。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンター

プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンターの例は、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

このデータセンターの例では、プライマリサーバーとメディアサーバー上で NetBackup アクセス制御を使用しています。データセンターでは、NetBackup へのアクセスを部分的に制限し、root 以外のユーザーが NetBackup を管理できるようなっています。この環境では、NBAC はサーバーと GUI 間で使用できるように構成されています。root 以外のユーザーは、オペレーティングシステム (UNIX のパスワードまたは Windows のローカルドメイン) を使って NetBackup にログインできます。また、グローバルユーザーリポジトリ (NIS/NIS+ または Active Directory) を使って NetBackup を管理することができます。さらに、NBAC を使用して、特定のユーザーに対して NetBackup へのアクセスレベルを制限することもできます。たとえば、日常的な操作の制御と、新しいポリシーやロボットの追加といった環境構成を分離することもできます。

プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- root 以外のユーザーとして管理する
- Windows のユーザー ID を使用して UNIX を管理する
- UNIX アカウントを使用して Windows を管理する
- 特定のユーザーの操作を分離および制限する
- クライアントホストの root ユーザーまたは管理者はローカルクライアントのバックアップとリストアを実行できる
- 他のセキュリティ関連のオプションと組み合わせることができる
- すべてのサーバーが NetBackup 7.7 以降である必要がある

次の表に、プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンターに使用される NetBackup の構成要素を示します。

表 3-8 プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンターで使用される NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	ロンドンのデータセンターには、ルートブローカー、認証ブローカー 1、GUI 1、認可エンジン、プライマリサーバー、メディアサーバー 1、クライアント 4、5 が含まれます。また、クライアント 4、5 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	東京のデータセンターには、認証ブローカー 2、GUI 2、メディアサーバー 2、クライアント 10、11 が含まれます。また、クライアント 10、11 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN によって、ルートブローカー/認証ブローカー 1 と認証ブローカー 2 が接続されます。さらに、ルートブローカー/認証ブローカー 1 と GUI 2/メディアサーバー 2 も接続されます。また、WAN によって、認可エンジンはメディアサーバー 2 に接続されます。プライマリサーバーは GUI 2、メディアサーバー 2、クライアント 10、11 に接続されます。
プライマリサーバー	プライマリサーバーは、ロンドンのデータセンターにあり、ルートブローカー/認証ブローカー 1 と通信します。また、GUI 1、認可エンジン、メディアサーバー 1 とも通信します。プライマリサーバーは、ロンドンのクライアント 4、5 と通信します。さらに、プライマリサーバーは、東京の GUI 2、メディアサーバー 2、クライアント 10、11 とも通信します。
メディアサーバー	この複数のデータセンターの例では、2 つのメディアサーバーがあります。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、プライマリサーバー、ルートブローカー/認証ブローカー 1、認可エンジン、クライアント 4、5 と通信します。メディアサーバー 1 は、クライアント 4、5 の暗号化されていないデータをテープに書き込みます。 東京のメディアサーバー 2 は、WAN を介してロンドンのプライマリサーバーおよび認可エンジンと通信します。また、東京の GUI 2、クライアント 10、11 とも通信します。メディアサーバー 2 は、クライアント 10、11 の暗号化されていないデータをテープに書き込みます。
GUI	この複数のデータセンターの例では、2 つの GUI があります。GUI 1 はロンドン、GUI 2 は東京にあります。これらのリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびプライマリサーバーの機能へのアクセス権を取得します。ロンドンの GUI 1 は、認証ブローカー 1 からクレデンシャルを受信します。GUI 1 には、プライマリサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。東京の GUI 2 は、認証ブローカー 2 からクレデンシャルを受信します。GUI 2 には、プライマリサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。

構成要素	説明
ルートブローカー	複数のデータセンターのインストールには、ルートブローカーが 1 つのみ必要です。ルートブローカーは、認証ブローカーと組み合わせて使用することもできます。この例では、ルートブローカーと認証ブローカーは同じコンポーネントとして示され、ロンドンのデータセンターに配置されています。ロンドンにあるルートブローカーは、ロンドンの認証ブローカー 1 と、東京の認証ブローカー 2 を認証します。ルートブローカーはクライアントを認証しません。
認証ブローカー	複数のデータセンターのインストールでは、複数の認証ブローカーを配置できます。認証ブローカーをルートブローカーと組み合わせて使用することもできます。このデータセンターのインストールでは、2 つの認証ブローカーが使用されています。認証ブローカーは、プライマリサーバー、メディアサーバーおよび GUI に対してそれぞれクレデンシャルを設定し、認証します。認証ブローカーは、コマンドプロンプトを指定するユーザーも認証します。ロンドンの認証ブローカー 1 は、プライマリサーバー、メディアサーバー 1、GUI 1 のクレデンシャルを認証します。東京とロンドンにあるすべての NetBackup サーバーとクライアントは、ロンドンの認証ブローカー 1 で認証が行われます。GUI 1 はロンドンの認証ブローカー 1 で認証が行われます。GUI 2 は東京の認証ブローカー 2 で認証が行われます。
認可エンジン	複数のデータセンターのインストールには、認可エンジンが 1 つのみ必要です。認可エンジンは、プライマリサーバーおよびメディアサーバーと通信して、認証されたユーザーの権限を決定します。これらの権限によって、ユーザーが利用できる機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。認可エンジンはロンドンに存在し、プライマリサーバー、メディアサーバー 1 と通信します。また、認可エンジンは、WAN を介して通信を行い、東京のメディアサーバー 2 へのアクセス権を認可します。 **メモ:** 認可エンジンは、デーモンプロセスとしてプライマリサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	暗号化されていないデータテープは、ロンドンのデータセンターと東京のデータセンターで生成されます。ロンドンでは、クライアント 4、5 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。東京では、クライアント 10、11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンの場合、クライアント 4 は標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもプライマリサーバーによって管理され、クライアントのデータはメディアサーバー 1 によってテープにバックアップされます。クライアント 5 は、NetBackup のみのポートを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。 東京の場合、クライアント 10 は標準的な NetBackup 形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもプライマリサーバーによって管理され、クライアントのデータはメディアサーバー 2 によってテープにバックアップされます。クライアント 11 は、NetBackup のみのポートを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 11 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。

構成要素	説明
内部ファイアウォール	この複数のデータセンターの例では、2 つの内部ファイアウォールがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンの場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 にアクセスできます。東京の場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 11 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、内部ファイアウォールを通過して DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	この複数のデータセンターの例では、2 つの DMZ があります。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 5 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 とクライアント側で暗号化を行うクライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京では、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 11 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。
外部ファイアウォール	この複数のデータセンターの例では、2 つの外部ファイアウォールがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは Web サーバークライアント 11 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

すべてに NBAC を使用する複数のデータセンター

すべてに NBAC を使用する複数のデータセンターは、中規模から大規模な (50 を超える)ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

この環境は、プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンターに非常に類似しています。主な違いは、NetBackup 環境に参加するすべてのホストがクレデンシャルを使って確実に識別され、root 以外の管理者が構成可能なアクセスレベルに基づいて NetBackup クライアントを管理できることです。ユーザー識別情報は、Windows の Active Directory または UNIX の NIS などのグローバルリポジトリに存在する場合があります。また、識別情報は、認証ブローカーをサポートするホスト上のローカルのリポジトリ (UNIX のパスワード、Windows のローカルドメイン) に存在する場合もあります。

すべてに NBAC を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- プライマリサーバーとメディアサーバーで NBAC を使用する複数のデータセンターの場合の特徴と類似している (クライアントの root ユーザーまたは管理者についての項目は除く)。この構成では、クライアントとサーバーの root 以外の管理者による管理が許可されています。
- クライアントシステムでは、ローカルバックアップとリストアを行うために root 以外または管理者以外のユーザーが設定される場合がある (デフォルト設定)
- この環境では、NetBackup に含まれるすべてのホストの信頼できる識別が容易である
- すべてのホストは NetBackup バージョン 7.7 以降である必要がある

次の表に、すべてに NBAC を実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 3-9 すべてに NBAC を実装した複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	ロンドンのデータセンターには、ルートブローカー、認証ブローカー 1、GUI 1、認可エンジン、プライマリサーバー、メディアサーバー 1、クライアント 1、5 が含まれます。また、クライアント 1、5、10 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。

構成要素	説明
東京のデータセンター	東京のデータセンターには、認証ブローカー 2、GUI 2、メディアサーバー 2、クライアント 10、11 が含まれます。また、クライアント 10、11 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN によって、ルートブローカー、認証ブローカー 1、認証ブローカー 2 が接続されます。さらに、ルートブローカー、認証ブローカー 1、GUI 2 がメディアサーバー 2 と一緒に接続されます。また、WAN によって、認可エンジンはメディアサーバー 2 に接続されます。プライマリサーバーは GUI 2、メディアサーバー 2、クライアント 10、11 に接続されます。メディアサーバー 1 はクライアント 10 に接続されます。
プライマリサーバー	プライマリサーバーは、ロンドンのデータセンターにあり、ルートブローカー/認証ブローカー 1 と通信します。また、GUI 1、認可エンジン、メディアサーバー 1 とも通信します。プライマリサーバーは、東京の GUI 2、メディアサーバー 2、クライアント 10、11 と通信します。
メディアサーバー	この複数のデータセンターの例では、2 つのメディアサーバーがあります。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、プライマリサーバー、ルートブローカー/認証ブローカー 1、認可エンジン、クライアント 1、5、10 と通信します。メディアサーバー 1 は、クライアント 1、5、10 の暗号化されていないデータをテープに書き込みます。 東京のメディアサーバー 2 は、WAN を介してロンドンのプライマリサーバー、ルートブローカー/認証ブローカー 1 および認可エンジンと通信します。また、東京の GUI 2、クライアント 10、11 とも通信します。メディアサーバー 2 は、クライアント 10、11 の暗号化されていないデータをテープに書き込みます。
GUI	この複数のデータセンターの例では、2 つの GUI があります。GUI 1 はロンドン、GUI 2 は東京にあります。これらのリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびプライマリサーバーの機能へのアクセス権を取得します。ロンドンの GUI 1 は、認証ブローカー 1 からクレデンシャルを受信します。GUI 1 には、プライマリサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。東京の GUI 2 は、認証ブローカー 2 からクレデンシャルを受信します。GUI 2 には、プライマリサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。
ルートブローカー	複数のデータセンターのインストールには、ルートブローカーが 1 つのみ必要です。ルートブローカーは、認証ブローカーと組み合わせて使用することもできます。この例では、ルートブローカーと認証ブローカーは同じコンポーネントとして示され、ロンドンのデータセンターに配置されています。ロンドンにあるルートブローカーは、ロンドンの認証ブローカー 1 と、東京の認証ブローカー 2 を認証します。ルートブローカーはクライアントを認証しません。

構成要素	説明
認証ブローカー	データセンターのインストールでは、複数の認証ブローカーを配置できます。認証ブローカーをルートブローカーと組み合わせて使用することもできます。このデータセンターのインストールでは、2 つの認証ブローカーがあります。認証ブローカーは、プライマリサーバー、メディアサーバー、GUI、クライアントに対してそれぞれクレデンシャルを設定し、認証します。認証ブローカーは、コマンドプロンプトを使用するユーザーも認証します。ロンドンの認証ブローカー 1 は、プライマリサーバー、メディアサーバー 1、GUI 1、クライアント 1、5 のクレデンシャルを認証します。東京とロンドンにあるすべての NetBackup サーバーとクライアントは、ロンドンの認証ブローカー 1 で認証が行われます。GUI 1 はロンドンの認証ブローカー 1 で認証が行われます。GUI 2 は東京の認証ブローカー 2 で認証が行われます。
認可エンジン	データセンターのインストールには、認可エンジンが 1 つのみ必要です。認可エンジンは、プライマリサーバーおよびメディアサーバーと通信して、認証されたユーザーの権限を決定します。これらの権限によって、ユーザーが利用できる機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。認可エンジンはロンドンに存在し、プライマリサーバー、メディアサーバー 1 と通信します。また、認可エンジンは、WAN を介して通信を行い、東京のメディアサーバー 2 へのアクセス権を認可します。 **メモ:** 認可エンジンは、デーモンプロセスとしてプライマリサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	暗号化されていないデータテープは、ロンドンと東京の両方のデータセンターで作成されます。ロンドンでは、クライアント 1、5、10 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。東京では、クライアント 10、11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。クライアント 10 は東京に存在し、東京でバックアップされますが、ロンドンでもバックアップされることに注意してください。
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンの場合、クライアント 1 は標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもプライマリサーバーによって管理され、クライアントのデータはメディアサーバー 1 によってテープにバックアップされます。クライアント 5 は、NetBackup のみのポートを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。 東京の場合、クライアント 10 は標準的な NetBackup 形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもプライマリサーバーによって管理され、クライアントのデータはメディアサーバー 2 によってテープにバックアップされます。クライアント 11 は、NetBackup のみのポートを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 11 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。

構成要素	説明
内部ファイアウォール	この複数のデータセンターの例では、2 つの内部ファイアウォールを設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンの場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 にアクセスできます。東京の場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 11 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、内部ファイアウォールを通過して DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	この複数のデータセンターの例では、2 つの DMZ を設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 5 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京では、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 11 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。
外部ファイアウォール	この複数のデータセンターの例では、2 つの外部ファイアウォールを設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは Web サーバークライアント 11 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

4

NetBackup 操作の監査

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

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

NetBackup の操作を監査すると、次の利点があります。

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

NetBackup Audit Manager について

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

管理者は特に以下を調査できます。

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

次の点に注意してください。

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

NetBackup によって監査された処理

NetBackup は、ユーザーが開始した次の処理を記録します。

アクティビティモニターの処理	任意の形式のジョブを取り消すか、中断するか、再開するか、再起動するか、削除すると、監査レコードが作成されます。
アラートと電子メール通知	アラートを生成できないか、NetBackup 構成設定に関する電子メール通知を送信できない場合。たとえば、SMTP サーバーの構成やアラートの除外状態コードのリストなどです。
異常	ユーザーが異常を誤検知として報告すると、そのユーザーの処理が監査され、ログに記録されます。
資産の処理	資産のクリーンアップ処理の一環として vCenter Server などの資産を削除すると、監査されてログに記録されます。 資産グループの作成、変更、削除や、ユーザーに許可されていない資産グループに対するすべての処理は、監査されてログに記録されます。
認証のエラー	NetBackup Web UI または NetBackup API を使用する場合は、認証エラーが監査されます。
カタログ情報	この情報には次のものが含まれます。 ■ イメージの検証および期限切れ ■ フロントエンド使用状況データを取得するために送信された要求の読み取り
証明書管理	NetBackup 証明書の作成、無効化、更新、配備、および特定の NetBackup 証明書エラー

証明書検証エラー (CVF)	SSL ハンドシェークエラー、無効化された証明書、またはホスト名の検証エラーが原因で失敗した接続試行。 SSL ハンドシェークと無効化された証明書に関する証明書検証エラー (CVF) の場合、タイムスタンプは個々の証明書の検証が失敗した日時ではなく、監査レコードがプライマリサーバーに送信された日時を示します。CVF 監査レコードには、一定期間の CVF イベントのグループが示されます。レコードの詳細には、監査期間の開始日時と終了日時、およびその期間に発生した CVF の合計数が示されます。
ディスクプールとボリュームプールの処理	ディスクプールまたはボリュームプールの追加、削除、または更新。
保留操作	保留操作の作成、変更および削除。
ホストデータベース	ホストデータベースに関連する NetBackup の操作。
IRE の構成および状態	IRE が許可するサブネットまたはスケジュールの追加、更新、削除。IRE 外部ネットワークは、IRE スケジュールまたは管理者によってオープンまたはクローズされます。
ログオン試行回数	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。 参照イメージ (`bplist`) 操作の監査レコードを定期的にキャッシュから NetBackup データベースに追加する間隔を設定するには、`DATAACCESS_AUDIT_INTERVAL_HOURS` 構成オプションを使用します。この構成オプションを設定すると、`bplist` 監査レコードが原因で NetBackup データベースのサイズが急激に増加することが抑制されます。 『NetBackup 管理者ガイド Vol. 1』を参照してください。 すべての `bplist` 監査レコードをキャッシュから NetBackup データベースに追加するには、プライマリサーバーで次のコマンドを実行します。 `nbcertcmd -postAudit -dataAccess`
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。
監査レコードの作成に失敗したユーザー操作	監査が有効な場合、ユーザー操作が監査レコードの作成に失敗すると、監査エラーが nbaudit ログでキャプチャされます。NetBackup 状態コード 108 が返されます (Action succeeded but auditing failed)。NetBackup は、監査が失敗しても終了状態コード 108 を返しません。

NetBackup によって監査されない処理

次の処理は監査されないため、監査レポートに表示されません。

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

現在の監査設定の表示

現在の監査の構成を表示するには、NetBackup プライマリサーバーで nbemmcmd コマンドを使用します。

現在の監査の設定を表示するには

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

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

   Linux: /usr/openv/netbackup/bin/admincmd
3. 次のコマンドを実行します。

   ```
   nbemmcmd -listsettings -machinename primaryserver
   ```

   primaryserver は対象のプライマリサーバーです。
4. 次の構成設定がリストされます。

   - AUDIT="ENABLED"
     監査がオンであることを示します。
   - AUDIT="DISABLED"
     監査がオフであることを示します。
   - AUDIT_RETENTION_PERIOD="90"
     監査が有効になっている場合に、レコードがこの期間 (日数) 保持されてから削除されることを示します。デフォルトの監査保持期間は 90 日です。0 (ゼロ) という値はレコードが削除されないことを示します。

監査イベントについて

次のセキュリティパラメーターに固有のイベントは、NetBackup Web UI で監査されます。

- 証明書 (Certificate)
- 接続 (Connection)
- ホスト (Host)
- ログイン (Login)
- セキュリティ構成 (Security Configuration)
- トークン (Token)

p.96 の「詳細な NetBackup 監査レポートの表示」を参照してください。

監査イベントの表示

[監査イベント (Audit Events)]タブには、フィルタを使用して選択した監査カテゴリに応じて NetBackup イベントが表示されます。NetBackup は、製品の使用中に発生する多数のイベントを記録します。たとえば、ホストへのセキュリティ証明書の発行、認証トークンの削除、ホスト間の接続の確立が記録されます。

監査イベントの状態を表示するには

1. NetBackup Web UI を開きます。
2. 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。
3. [監査イベント (Audit events)]タブをクリックします。
4. フィルタアイコンをクリックして、表示する監査イベントカテゴリを選択します。
5. 次の情報が表示されます。

イベント	実行された監査イベントの簡単な説明。
ユーザー	ユーザー名と、監査イベントに関連する詳細。
説明	実行された監査イベントの完全な説明。
理由	監査イベントを実行する理由 (ユーザーから提供される場合)。

6. 監査イベントの詳細を表示するには、イベントの名前をクリックします。

メモ: [接続 (Connection)]カテゴリに監査レコードが表示される場合は、必ずレコードの詳細を確認します。このカテゴリの特定のレコードでは、詳細に表示される[日付 (Date)]フィールドは、監査レコードがプライマリサーバーに送信された日付を示します。必ずしも個々のイベントが行われた日付を示すわけではありません。この種類の監査レコード (証明書検証エラー (CVF) レコードなど) は、一定期間にわたって行われているイベントのグループを表します。監査レコードの詳細には、期間の[イベント開始時間 (Beginning Event Time)]と[イベント終了時間 (Ending Event Time)]、および[イベント数 (Event Count)](その期間に行われたイベントの合計数) が記載されています。

[アクセス履歴 (Access History)]タブの監査に関連する問題のトラブルシューティング

NetBackup Web UI で、[セキュリティ (Security)]、[セキュリティイベント (Security events)]の順に開きます。[アクセス履歴 (Access History)]タブをクリックします。NetBackup には、現在のユーザーが実行したログインアクティビティについての詳細が表示されます。

必要な監査記録が[アクセス履歴 (Access History)]タブに表示されない場合は、プライマリサーバーで bprd サービスが実行中であることを確認してください。

監査保持期間と監査レコードのカタログバックアップ

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

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

監査保持期間を設定するには

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

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

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

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

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

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

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

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

詳細な NetBackup 監査レポートの表示

NetBackup Web UI を使用して、プライマリサーバーで NetBackup が監査する処理を表示できます。nbauditreport コマンドで監査イベントの詳細すべてを表示できます。

詳細な監査レポートを表示するには

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

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

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

または、次のオプションを使用してコマンドを実行します。

-sdate <"MM/DD/YY [HH:[MM[:SS]]]">	表示するレポートデータの開始日時。
-edate <"MM/DD/YY [HH:[MM[:SS]]]">	表示するレポートデータの終了日時。
-ctgy *category*	実行されたユーザー操作のカテゴリ。POLICY のようなカテゴリには、スケジュールやバックアップ対象などのいくつかのサブカテゴリが含まれることがあります。サブカテゴリに加えられた変更はすべて、プライマリカテゴリの変更としてリストされます。 -ctgy オプションについては、『NetBackup コマンドガイド』を参照してください。
-user <*username*[:*domainname*]>	監査情報を表示するユーザーの名前を指定するために使用します。
-fmt DETAIL	-fmt DETAIL オプションは監査情報の総合的なリストを表示します。たとえば、ポリシーが変更されると、属性の名前、古い値と新しい値がリストされます。このオプションには、次のサブオプションを設定できます。 ■ [-notruncate] 。レポートの詳細セクションの別々の行に、変更された属性の古い値と新しい値を表示します。 ■ [-pagewidth <NNN>] 。レポートの詳細セクションのページ幅を設定します。

-fmt PARSABLE	-fmt PARSABLE オプションは DETAIL レポートと同じセットの情報を解析可能な形式で表示します。レポートでは、監査レポートデータ間の解析トークンとしてパイプ文字 (|) を使用します。このオプションには、次のサブオプションを設定できます。 ■ [-order<DTU|DUT|TDU|TUD|UDT|UTD>]。情報を表示する順序を示します。 D (説明) T (タイムスタンプ) U (ユーザー)

3 監査レポートは次の詳細を含んでいます。

DESCRIPTION	実行された処理の詳細。
USER	処理を実行したユーザーの ID。 p.99 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
```

監査レポートのユーザーの ID

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

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

監査の無効化

デフォルトでは、NetBackup の監査は有効になっています。監査を無効にするには、次のページを参照してください。

監査を無効にするには

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

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

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

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename primaryserver
   ```

   次の例では server1 の監査がオフになります。

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename server1
   ```

監査エラーの監査アラート通知 (NetBackup 管理コンソール)

アラート通知オプションを使用して、監査可能な処理が監査レコードの作成に失敗したときに通知するかどうかを選択します。このオプションは NetBackup 管理コンソールのステータスバーに表示されます。

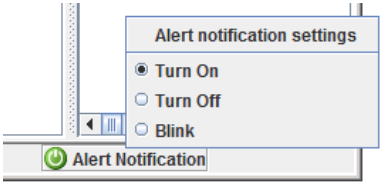


表 4-1 監査アラート通知オプション

オンにする (Turn on)	エラーを管理者に通知するポップアップメッセージが表示されます。
点滅 (Blink)	監査エラーが発生した場合、アイコンが点滅します。アイコンをクリックすると、エラーメッセージが表示されます。
オフにする (Turn off)	監査エラーが発生しても通知は表示されません。アイコンはグレー表示されます。

システムログへの監査イベントの送信

システムログに NetBackup 監査イベントを送信できます。このタスクを実行するには、NetBackup セキュリティ管理者の役割または同様の RBAC 権限が必要です。

システムログに監査イベントを送信するには

1. NetBackup Web UI を開きます。
2. 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。
3. 右上で、[セキュリティイベント設定 (Security event settings)]をクリックします。
4. [監査イベントをシステムログに送信する (Send the audit events to the system logs)]オプションを有効にします。

5 [監査イベントカテゴリの選択 (Select audit event categories)]をクリックします。次に、監査イベントをシステムログに送信する監査カテゴリを選択します。

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

6 [保存 (Save)]をクリックします。

システムログで NetBackup 監査イベントを表示できます。例:

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

Linux システムでは、構成された場所のシステムログを表示できます。

1

個人情報とアクセスの管理

5

個人情報とアクセスの管理について

この章では以下の項目について説明しています。

NetBackup のアクセス制御について

NetBackup では、次の種類のアクセス制御を提供しています。

- NetBackup 管理 Web UI (デフォルト)
  NetBackup 管理者は、NetBackup でさまざまなアプリケーションを表示できるユーザーを制御できます。root ユーザーと管理者には、NetBackup 管理 Web UI へのフルアクセス権があります。root 以外または管理者以外のユーザーは、バックアップ、アーカイブおよびリストアアプリケーションにアクセスできます。このユーザーは `auth.conf` ファイルで定義されている、追加のアプリケーションにもアクセスできます。
  アクセス制御はビューベースで、役割ベースではありません。管理者は、ユーザーが表示および管理できるアプリケーションを制御できますが、ユーザーが組織での役割に基づいて実行できるタスクを制御できません。アクセス制御は、NetBackup 管理 Web UI に制限されます。(バックアップ、アーカイブ、およびリストアクライアント、NetBackup MS SQL Client などのインターフェースは影響を受けません)。
  NetBackup 管理 Web UI でのアクセス制御について詳しくは、『NetBackup 管理者ガイド Vol.1』を参照してください。
- 役割に基づくアクセス制御 (RBAC)
  NetBackup 8.1.2 リリース以降の NetBackup Web ユーザーインターフェースでは、限られた数のセキュリティ設定と作業負荷に対して、役割に基づくアクセス制御が可能です。詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。
- NetBackup アクセス制御 (NBAC)

NBAC は、NetBackup 管理 Web UI や CLI 向けに、NetBackup で独自に提供されている役割に基づくアクセス制御です。NetBackup 環境を管理するためにアクセス制御の他のいずれかの方式を使用することが推奨されています。

NetBackup 管理コンソールと CLI のアクセス制御方法

NetBackup 管理コンソールと CLI で利用可能なアクセス制御の主な違いを次の表にまとめます。(NetBackup Web UI の RBAC 機能は、Web UI と NetBackup API に対するアクセス制御のみを提供します。) NBAC について詳しくは、8.1.2 以前のリリースの NetBackup のマニュアルを参照してください。

表 5-1

アクセスおよび監査	NetBackup 管理コンソールと auth.conf
NetBackup 管理コンソールを使用できるユーザー	root ユーザーや管理者には、管理コンソールへのフルアクセス権があります。 root 以外のユーザーまたは管理者以外のユーザーは、デフォルトでバックアップ、アーカイブ、およびリストアアプリケーションに限定されています。そうでない場合、これらのユーザーは auth.conf ファイルで定義されているアプリケーションにアクセスできます。
CLI を使用できるユーザー	root ユーザーと管理者には、CLI へのフルアクセス権があります。
ユーザーの監査方法	root または管理者として

NetBackup 管理コンソールと CLI でのアクセス制御方法の詳細を次のフローチャートにまとめます。

6

AD ドメインと LDAP ドメイン

この章では以下の項目について説明しています。

- NetBackup での AD ドメインまたは LDAP ドメインの追加
- AD または LDAP ドメイン構成の問題のトラブルシューティング
- NetBackup Authentication Service で信頼する認証局

NetBackup での AD ドメインまたは LDAP ドメインの追加

NetBackup は、AD (Active Directory) または LDAP (ライトウェイトディレクトリアクセスプロトコル) のドメインユーザーをサポートします。

AD ドメインまたは LDAP ドメインが NetBackup に追加されると、それぞれのドメインユーザーは NetBackup プライマリサーバーにログオンでき、セキュリティ管理者は、これらのドメインユーザーに RBAC (役割ベースのアクセス制御) の役割を割り当てることができます。

p.130 の「RBAC の機能」を参照してください。

次の手順では、NetBackup で既存の AD ドメインまたは LDAP ドメインを追加する方法と、NetBackup にアクセスできるようにドメインユーザーを認証する方法を説明します。

NetBackup で AD ドメインまたは LDAP ドメインを追加するには

1 次のコマンドを実行して、AD ドメインまたは LDAP ドメインを NetBackup プライマリサーバーに追加します。

```
vssat addldapdomain -d DomainName -s server_URL -u user_base_DN
-g group_base_DN [-f trusted_CA_file_name] [-tp TLS_protocol_version_to_be_disabled]
[-cs cipher_suite_list] [-t rfc2307 | msad | {-c user_object_class -a user_attribute
-q user_GID_attribute -un user_display_name_attribute -ui user_ID_attribute[:value_type]

-ud user_description_attribute -x group_object_class -y group_attribute
-z group_GID_attribute -gn group_display_name_attribute -gi
group_ID_attribute[:value_type]
-gd group_description_attribute [-k DN | UID]} [-b FLAT | BOB] -m admin_user_DN
[-w admin_user_password] [-p SUB | ONE | BASE] [-F]
```

メモ: -m オプションで指定した名前のユーザーに、AD または LDAP サーバーに問い合わせるために必要な権限があることを確認します。

LDAPS の場合、認証サービス (nbatd) で、サーバーの証明書を署名した認証局 (CA) を信頼しないときは、-f オプションを使用して、nbatd トラストストアの CA 証明書を追加します。

p.116 の「NetBackup Authentication Service で信頼する認証局」を参照してください。

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。

このコマンドラインオプションの正しい値については、AD 管理者にお問い合わせください。値は、AD の設定によって異なる場合があります。

たとえば、AD ドメインを追加する場合は次のコマンドを実行します。

```
vssat addldapdomain -d domain1 -s ldap://domain1.veritas.com -u
"CN=Users,DC=domain1,DC=veritas,DC=com" -g "CN=Users,DC=domain1,DC=veritas,DC=com" -t
msad -m
"CN=user1,CN=Users,DC=domain1,DC=veritas,DC=com" -b BOB
```

2 プライマリサーバーで vssat validateprpl コマンドを実行して、指定した AD または LDAP ドメインが正常に追加されたかどうかを確認します。

validateprpl -p *username* -d ldap:*domain_name* -b localhost:1556:nbatd

AD または LDAP ドメインを検証する場合の例を次に示します。

```
vssat validateprpl -p user1 -d ldap:domain1 -b
localhost:1556:nbatd
```

ドメイン名は、addldapdomain コマンドオプションで使用したドメイン名と一致する必要があります。

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 ドメインが追加されておらず、vssat validateprpl または vssat validategroup コマンドが失敗した場合は、問題を解決するために特定のトラブルシューティング手順を実行する必要があります。

p.107 の「AD または LDAP ドメイン構成の問題のトラブルシューティング 」を参照してください。

AD または LDAP ドメイン構成の問題のトラブルシューティング

AD または LDAP ドメインの構成を追加した後、vssat validateprpl と vssat validategroup コマンドを使用して構成を確認します。これらのコマンドは、既存の AD/LDAP ユーザーおよびグループをそれぞれ検証します。

vssat validateprpl と vssat validategroup コマンドの実行の成功は、関連付けられている AD または LDAP ドメインが正常に追加されたことを示します。

これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

コマンドが失敗した場合は、次のエラーメッセージが表示されます。

```
The principal or group does not exist.
```

AD または LDAP ドメインの検証は、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
- ユーザークレデンシャルが無効

- ユーザーベース DN またはグループベース DN が無効
- 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

AD または LDAP サーバーとの接続を確立できない

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。

```
(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
```

2 次のシナリオのいずれかが該当するかを確認し、そのシナリオに示された手順を実行します。

vssat addldapdomain で指定された LDAP サーバーの URL (-s オプション) が間違っている可能性がある

検証のために次のコマンドを実行します。

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

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される CA ではない

これは、ldaps オプションが使用されており、ldapsearch コマンドを使用して検証できる場合に該当します。

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

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

cacert.pem のファイルのパス:

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

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)
```

NetBackup Authentication Service (nbatd) は、LDAP サーバーのセキュリティ証明書に署名した認証局を信頼しません p.116 の「NetBackup Authentication Service で信頼する認証局」を参照してください。	vssat addldapdomain コマンドの -f オプションを使用して、認証サービス (nbatd) のトラストストアに CA 証明書を追加します。

LDAP サーバーに提供されている TLS 暗号スイートのリストが間違っている可能性がある

デフォルトでは、NetBackup 認証サービスは次の暗号スイートリストを使用して LDAP サーバーと通信します。

“ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:

ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA”

次のコマンドを実行して、LDAP サーバーに提供されている TLS 暗号スイートのリストを表示します。

UNIX の場合:

```
/usr/openv/netbackup/sec/at/bin/vssat listldapdomains
```

Windows の場合:

```
Install_path¥NetBackup¥sec¥at¥bin¥vssat listldapdomains
```

sslscan などの任意のユーティリティを使用して、LDAP サーバーがサポートする暗号スイートを見つけます。

次のコマンドを実行して、LDAP サーバーの要件に合わせて TLS 暗号スイートリストの値を変更します。

UNIX の場合:

```
/usr/openv/netbackup/sec/at/bin/vssregctl -s -f
/usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
-b "Security¥Authentication¥Authentication
Broker¥AtPlugins¥ldap¥ServerInfos¥LDAP_server_name" -k
"SSLCipherSuite" -t string -v LDAP_server_supported_cipher_suites
```

Windows の場合:

```
Install_path¥NetBackup¥sec¥at¥bin¥vssregctl -s -f
Install_path¥NetBackup¥var¥global¥vxss¥eab¥data¥systemprofile¥VRTSatlocal.conf
-b "Security¥Authentication¥Authentication
Broker¥AtPlugins¥ldap¥ServerInfos¥LDAP_server_name" -k
"SSLCipherSuite" -t string -v LDAP_server_supported_cipher_suites
```

例:

```
/usr/openv/netbackup/sec/at/bin/vssregctl -s -f
/usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
-b "Security¥Authentication¥Authentication
Broker¥AtPlugins¥ldap¥ServerInfos¥example.veritas.com" -k
"SSLCipherSuite" -t string -v
"DHE-RSA-AES256-SHA:AES256-GCM-SHA384"
```

LDAP サーバーで無効化された TLS プロトコルのバージョンが間違っている可能性がある

デフォルトでは、NetBackup 認証サービスは TLS 1.2 プロトコルを使用して LDAP サーバーと通信し、他のすべてのバージョンの TLS プロトコルは無効化されます。

次のコマンドを実行して、LDAP サーバーで無効化されている TLS プロトコルのバージョンを表示します。

UNIX の場合:

```
/usr/openv/netbackup/sec/at/bin/vssat listldapdomains
```

Windows の場合:

```
Install_path¥NetBackup¥sec¥at¥bin¥vssat listldapdomains
```

指定したコマンドを使用して、LDAP サーバーで無効になっている TLS プロトコルバージョンの値を変更します。指定したバージョンとそれ以前のすべてのバージョンの TLS プロトコルが無効化されます。サポートされる値は、「SSLv2」、「SSLv3」、「TLSv1」、「TLSv1.1」です。

次のコマンドを実行します。

UNIX の場合:

```
/usr/openv/netbackup/sec/at/bin/vssregctl -s -f
/usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
-b "Security¥Authentication¥Authentication
Broker¥AtPlugins¥ldap¥ServerInfos¥LDAP_server_name" -k
"DisableTLSProtocol" -t string -v
TLS_protocol_version_to_be_disabled
```

Windows の場合:

```
Install_path¥NetBackup¥sec¥at¥bin¥vssregctl -s -f
Install_path¥NetBackup¥var¥global¥vxss¥eab¥data¥systemprofile¥VRTSatlocal.conf
-b "Security¥Authentication¥Authentication
Broker¥AtPlugins¥ldap¥ServerInfos¥LDAP_server_name" -k
"DisableTLSProtocol" -t string -v
TLS_protocol_version_to_be_disabled
```

例:

```
/usr/openv/netbackup/sec/at/bin/vssregctl -s -f
/usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
-b "Security¥Authentication¥Authentication
Broker¥AtPlugins¥ldap¥ServerInfos¥example.veritas.com" -k
"DisableTLSProtocol" -t string -v "TLSv1"
```

ユーザークレデンシャルが無効

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

2 次のシナリオが該当するかを確認し、そのシナリオに示された手順を実行します。

vssat addldapdomain コマンドを使用して LDAP ドメインを追加しているときに、無効な管理ユーザーの DN またはパスワードが指定された

検証のために次のコマンドを実行します。

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

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)
```

ユーザーベース DN またはグループベース DN が無効

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

2 ログに含まれるユーザーベース DN (-u オプション) またはグループベース DN (-g オプション) の値が正しくない場合は、エラーが発生する場合があります。

検証のために次のコマンドを実行します。

例:

```
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 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。

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>
```

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>
```

NetBackup Authentication Service で信頼する認証局

NetBackup Authentication Service (nbatd) は次の認証局を信頼します:

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

7

アクセスキー

この章では以下の項目について説明しています。

アクセスキー

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

p.121 の「API キーについて」を参照してください。

p.117 の「アクセスコード」を参照してください。

アクセスコード

特定の NetBackup 管理者コマンド (`bperror` など) を実行するには、Web UI を介して認証する必要があります。コマンドラインインターフェースを使用してアクセスコードを生成し、管理者が承認したアクセス要求を取得してから、コマンドにアクセスする必要があります。

CLI アクセス用の Web UI 認証を使用すると、NetBackup 管理者は他のユーザーに関連する権限を委任できます。デフォルトでは、root 管理者または管理者のみがコマンドラインインターフェースを使用して NetBackup 操作を実行できます。Web UI の認証サポートにより、root 以外のユーザーで、セキュリティ管理者が付与した CLI アクセス権を持つユーザーは NetBackup を管理できます。NetBackup ユーザーとして登録されてい

なくても、RBAC ユーザー以外の役割 (オペレーティングシステム管理者など) があれば NetBackup を管理できます。CLI にアクセスするには、毎回新しいアクセスコードを生成する必要があります。

Web UI 認証を使用した CLI アクセスの要求

NetBackup CLI を使用して NetBackup コマンドを実行するには、ユーザーに次の要件があります。

- ユーザーにデフォルトの NetBackup CLI (コマンドライン) 管理者の RBAC の役割、または同様の権限を持つ役割も割り当てられている必要があります。
- ユーザーは CLI への一時的なアクセス権の要求を送信する必要があります。デフォルトでは、CLI アクセスのセッションは 24 時間有効です。
  ユーザーが要求のために実行するコマンドは、ユーザーが NetBackup Web UI にアクセスできるかどうかによって異なります。
  p.118 の「NetBackup Web UI へのアクセス権がある場合の CLI アクセスの要求」を参照してください。
  p.119 の「セキュリティ管理者への CLI アクセス権の要求」を参照してください。

NetBackup Web UI へのアクセス権がある場合の CLI アクセスの要求

NetBackup Web UI へのアクセス権がある場合は、Web UI で、`bpnbat` コマンドのアクセスコードを使用して CLI アクセス要求を承認できます。

CLI アクセスを要求するには

1. 次のコマンドを実行します。

   ```
   bpnbat -login -logintype webui
   ```

   アクセスコードが生成されます。
2. NetBackup Web UI を開きます。
3. 右上で、プロファイルアイコンをクリックします。
4. [アクセス権の要求を承認する (Approve access request)]をクリックします。
5. `bpnbat` コマンドの実行時に作成された CLI アクセスコードを入力します。次に、[確認 (Review)]をクリックします。
6. アクセス要求の詳細を確認します。
7. [承認 (Approve)]をクリックします。
8. 要求を承認した後、コマンドラインインターフェースを使用して目的のコマンドを実行できます。

セキュリティ管理者への CLI アクセス権の要求

NetBackup Web UI へのアクセス権がない場合は、セキュリティ管理者に CLI アクセス権の要求を送信する必要があります。デフォルトのセキュリティ管理者の役割または同様の権限の役割を持つユーザーが、要求を承認する必要があります。

セキュリティ管理者に CLI アクセス権を要求するには

1. 次のコマンドを実行します。

   ```
   bpnbat -login -logintype webui -requestApproval
   ```

   アクセスコードが生成されます。

2. セキュリティ管理者に、CLI アクセス権の要求を承認するためのアクセスコードを問い合わせます。

   p.119 の「他のユーザーの CLI アクセス要求の承認」を参照してください。

3. 要求が承認されたら、コマンドラインインターフェースを使用して目的のコマンドを実行できます。

他のユーザーの CLI アクセス要求の承認

デフォルトのセキュリティ管理者の役割または同様の権限を持つ役割が割り当てられている場合は、CLI アクセスが必要な他のユーザーの要求を承認できます。コマンドを実行するには、そのユーザーにデフォルトの NetBackup CLI (コマンドライン) 管理者の RBAC の役割、または同様の権限を持つ役割も割り当てられている必要があることに注意してください。

別のユーザーの CLI アクセス要求を承認するには

1. CLI アクセスを必要とするユーザーは、最初に次のコマンドを実行して承認を要求する必要があります。

   ```
   bpnbat -login -logintype webui -requestApproval
   ```

2. NetBackup Web UI にサインインします。
3. 左側で[セキュリティ (Security)]、[アクセスキー (Access keys)]の順に選択します。次に、[アクセスコード (Access codes)]タブをクリックします。
4. CLI アクセスが必要なユーザーから受け取った CLI アクセスコードを入力し、[確認 (Review)]をクリックします。
5. アクセス要求の詳細を確認します。
6. (オプション) コメントがある場合は入力します。
7. [承認 (Approve)]をクリックします。

コマンドラインアクセスの設定の編集

ユーザーが CLI アクセスを要求するときに CLI セッションに設定されるデフォルトの時間を構成できます。

コマンドラインアクセスの設定を編集するには

1. Web UI にサインインします。
2. 左側で[セキュリティ (Security)]、[アクセスキー (Access keys)]の順に選択します。
3. 右側で[アクセス設定 (Access settings)]を選択します。
4. [編集 (Edit)]をクリックします。
5. CLI アクセスセッションを有効にする時間を分または時間で入力します。最小値は 1 分で、最大値は 24 時間です。

8

API キー

この章では以下の項目について説明しています。

API キーについて

NetBackup は、API キーを介したユーザー認証をサポートしています。

NetBackup API キーは事前認証されたトークンで、これにより NetBackup ユーザーは NetBackup コマンド (`nbcertcmd -createToken` や `nbcertcmd -revokeCertificate`) を実行したり、NetBackup RESTful API にアクセスできます。

API キーは、パスワードとは違って長期間使用でき、期限を設定することもできます。そのため、認証が必要な自動化などの操作を、API キーを使用して長期間実行できます。

p.122 の「API キーの作成」を参照してください。

p.122 の「API キーの使用」を参照してください。

p.122 の「API キーの管理」を参照してください。

メモ: プリンシパルユーザーに対して生成された API キーは、ユーザーが非アクティブになった後、ブロックされた後、または認証システム (AD または LDAP) から削除することをお勧めします。

API キーの作成

ユーザーが所有できるのは 1 つの API キーのみです。

メモ: API キーを作成するには、「表示」の RBAC 権限が必要です。

API キーは次のいずれかの方法で作成できます。

- `netbackup/security/api-keys POST` API を使用する
  どのユーザーも `api-keys` API を使用して API キーを作成できます
- NetBackup Web UI を使用する
  Web UI または RBAC の役割を使用した API キーの作成について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

p.122 の「API キーの使用」を参照してください。

p.122 の「API キーの管理」を参照してください。

API キーの管理

各 API キーは、API キータグに関連付けられます。API キーは、次のいずれかの方法で、API キータグを使用して更新または削除できます。

- `netbackup/security/api-keys` API を使用する
  API キーは、API キータグを使用して更新または削除できます。
- NetBackup Web UI を使用する
  Web UI を使用した API キーの管理について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

p.122 の「API キーの作成」を参照してください。

p.122 の「API キーの使用」を参照してください。

API キーの使用

作成した API キーは、RESTful API へのアクセス中またはコマンドの実行中に使用できます。

p.122 の「API キーの作成」を参照してください。

NetBackup RESTful API へのアクセス中に API キーを使用する

- 他の NetBackup API にアクセスするため、API 要求ヘッダーの API キーを渡します。

NetBackup コマンドの実行中に API キーを使用する

1 次のいずれかを実行します。

- 次のコマンドを実行します。

  `bpnbat -Login -LoginType APIKEY`

  24 時間以内に認証を必要とする NetBackup コマンドは、`bpnbat -Login` を実行しなくても実行できます。

- API キーに `NETBACKUP_APIKEY` と呼ばれる新しい環境変数を設定します。

  p.123 の「NetBackup コマンドを実行するための API キーの環境変数の設定」を参照してください。

  認証を必要とする NetBackup コマンドは、API キーが有効で、環境変数が設定されている間は実行できます。

2 `nbcertcmd -createToken` などのコマンドを実行します。

NetBackup 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。

NetBackup コマンドを実行するための API キーの環境変数の設定

ユーザー認証が必要な NetBackup コマンドの実行中に API キーを使用するには、API キーを作成し、API キー用の環境変数を設定する必要があります。環境変数を設定したら、API キーが有効で、環境変数が設定されている間はコマンドを実行できます。

Windows プラットフォームでは、ユーザーコンテキストで API キーの環境変数を設定します。

API キーの環境変数の例:

`NETBACKUP_APIKEY = MasterServer1:APIKEY1`

複数の API キーを設定する場合は、プライマリサーバーと API キーのマッピングをカンマ区切りの形式で指定します。

次に例を示します。

```
NETBACKUP_APIKEY =
MasterServer1:APIKEY1,MasterServer2:APIKEY2,MasterServer3:APIKEY3
```

ファイルにマッピングを指定することもできます。ファイルには接頭辞「@」を指定する必要があります。

次に例を示します。

`NETBACKUP_APIKEY = @file_path/file_name`

ファイルの内容は、次のようになります。

`MasterServer1:APIKEY1`

MasterServer2:*APIKEY2*

MasterServer3:*APIKEY3*

p.122 の「API キーの作成」を参照してください。

9

auth.conf ファイル

この章では以下の項目について説明しています。

認可ファイル (auth.conf) の特徴

デフォルトでは、認可ファイルまたは auth.conf ファイルは、NetBackup 管理コンソールの次の機能へのアクセスを許可します。

NetBackup サーバー側	ルートユーザーに対する管理者のアプリケーションおよび機能。その他すべてのユーザーに対するユーザーバックアップ機能およびユーザーリストア機能。
NetBackup クライアント側	すべてのユーザーに対するユーザーバックアップ機能およびユーザーリストア機能。

auth.conf ファイルの場所

Windows 版 NetBackup サーバー	*install_path*¥NetBackup¥Java の auth.conf.win.template このテンプレートファイルを使用し、同じ場所で auth.conf ファイルを作成します。テンプレートファイルにはユーザーにアクセス許可を与える例があります。

UNIX 版 NetBackup サーバー	*install_path*/NetBackup/Java の auth.conf
	以下のエントリが含まれます。
	`root ADMIN=ALL JBP=ALL`
	`* ADMIN=JBP JBP=ENDUSER+BU+ARC`

auth.conf ファイルの構成

auth.conf ファイルを次のように構成します。

- auth.conf ファイルが存在する場合、そのファイルにはエントリが存在する必要があります。各ユーザーのエントリを指定するか、アスタリスク (*) を使用して、OS 管理者、RBAC 管理者を除くすべてのユーザーを示します。
  このファイル内にエントリを持たないユーザーは、すべての NetBackup アプリケーションにアクセスできません。
- アスタリスク (*) を使用して、OS 管理者、RBAC 管理者を除く任意のユーザー名を示します。
- 最初のフィールドがアスタリスクの場合、OS 管理者、RBAC 管理者を除く任意のユーザー名が受け入れられることを意味し、そのユーザーは指定されたアプリケーションを使用できます。
- 特定のユーザーのエントリを最初に記載し、その後、アスタリスク (*) を使用してすべてのエントリを記載します。
- 各エントリの最初のフィールドを使用して、アクセス権を付与または拒否するユーザー名を示します。アスタリスクを使用して、任意のユーザー名を示します。
- 残りのフィールドは、ユーザーまたは複数ユーザーに対する特定のアクセス権を指定します。アスタリスク (*) は、すべてのアプリケーションに対してすべてのユーザーを認可するためには使用できません。各ユーザー (またはすべてのユーザー) には、特定のアプリケーションキーワードが必要です。特定のユーザーに対してすべての機能を拒否する場合は、インターフェースのキーワードを提供しないようにします。次に例を示します。

  ```
  mydomain¥ray ADMIN= JBP=
  ```

- 特定の UI 機能へのアクセスが必要なユーザーグループを指定できます。
  <GRP> タグを使用して、auth.conf ファイルでユーザーグループを指定します。例:

  ```
  <GRP> domain1¥BackupAdmins ADMIN=SUM JBP=BU
  ```

  この例で、*domain1* は NetBackup ドメイン、*BackupAdmins* はユーザーグループです。*BackupAdmins* ユーザーグループのすべてのユーザーは、ストレージユニット管理 (SUM) UI ノードにアクセスし、バックアップ (BU) タスクを実行できます。

ADMIN キーワード

ユーザーがアクセスすることができるアプリケーションを指定します。ADMIN=ALL を指定すると、すべての NetBackup アプリケーション、およびそれに関連する管理者関連の機能へアクセスできます。

JBP キーワード

ユーザーがバックアップ、アーカイブおよびリストアクライアントアプリケーション (jbpSA) を使用して実行可能な機能を指定します。JBP=ALL を指定すると、管理用の機能を含む、すべてのバックアップ、アーカイブおよびリストア機能にアクセスできます。

アスタリスク (*)

最初のフィールドがアスタリスクの場合、任意のユーザー名が受け入れられることを意味し、そのユーザーは指定されたアプリケーションを使用できます。リリースバージョンの 2 行目では、最初のフィールドはアスタリスクです。アスタリスクは、NetBackup によって、バックアップ、アーカイブおよびリストアクライアントアプリケーション (jbpSA) にアクセスするすべてのユーザー名が検証されることを意味します。JBP=ENDUSER+BU+ARC を指定すると、ユーザーは、ファイルのバックアップ、アーカイブおよびリストアだけを行えます。

ユーザー認証

ログオン画面で入力するクレデンシャルは、ホストフィールドに指定するコンピュータ上で有効である必要があります。NetBackup アプリケーションサーバーは、指定されたコンピュータとの間で認証します。ユーザー名は、ファイルのバックアップ、アーカイブ、またはリストアに使用するアカウントです。jbpSA を使用してリモート管理操作またはユーザー操作を実行するには、ユーザーは、NetBackup の UNIX サーバーまたはクライアントコンピュータ上に有効なアカウントを持つ必要があります。バックアップ、アーカイブおよびリストアアプリケーション (jbpSA) では、バックアップまたはリストアするディレクトリおよびファイルを表示および選択する場合、システムファイル権限が使用されます。

そのため、そのパスワードは、そのコンピュータへのログオン時に使用したパスワードと同じである必要があります。たとえば、次の情報を使用してログオンすると想定します。

```
username = joe
password = access
```

同じユーザー名とパスワードを使用して NetBackup にログインする必要があります。

NetBackup アプリケーションサーバーには、オペレーティングシステムへのログオンに使用したユーザー名とは異なるユーザー名でログオンできます。たとえば、*joe* というユーザー名を使用してオペレーティングシステムにログオンする場合、その後にルートユーザーで jnbSA にログオンできます。

ユーザーグループのサポート

AD (Active Directory) グループは、プライマリサーバーの auth.conf ファイルでのみサポートされます。

ユーザーグループは、auth.conf ファイル内の <GRP> タグを使用して定義されます。

メモ: vssat validateprpl コマンドを実行して、auth.conf ファイルで定義したグループ名の形式を確認します。

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。

- ユーザーが複数のグループに属している場合、ユーザーのアクセス権が組み合わされます。たとえば、*user1* は *BackupAdmins* と *StorageUnitAdmins* というユーザーグループに属しています。

```
<GRP> domain1¥BackupAdmins ADMIN=SUM JBP=BU
<GRP> domain1¥StorageUnitAdmins ADMIN=CAT JBP=RAWPART
```

user1 のアクセス権は、ADMIN=SUM+CATJBP=BU+RAWPART のように組み合わされます。

- ユーザーと、ユーザーが属するユーザーグループが auth.conf ファイルに存在する場合、組み合わせたアクセス権がユーザーに割り当てられます。例: *user1* は *BackupAdmins* と *StorageUnitAdmins* というユーザーグループに属しているとします。

```
domain¥user1 ADMIN=JBP JBP=ENDUSER
<GRP> domain¥BackupAdmins ADMIN=CAT JBP=BU
<GRP> domain¥StorageUnitAdmins ADMIN=SUM JBP=RAWPART
```

user1 のアクセス権は、ADMIN=JBP+SUM+CATJBP=BU+RAWPART+ENDUSER のようになります。

- ユーザー、ユーザーグループ、またはその両方の重複したエントリが auth.conf ファイルに存在する場合、ユーザー、ユーザーグループ、またはその両方の最初のエントリが考慮され、組み合わせたアクセス権がユーザーに割り当てられます。例: *user1* が *BackupAdmins* ユーザーグループに属し、auth.conf ファイルには *BackupAdmins* ユーザーグループの 2 つのエントリが含まれているとします。

```
<GRP> domain1¥BackupAdmins ADMIN=CAT JBP=BU
<GRP> domain1¥BackupAdmins ADMIN=SUM JBP=RAWPART
```

user1 のアクセス権は、ADMIN=CATJBP=BU のようになります。

アプリケーションの状態情報

終了するときに、いくつかのアプリケーションの状態情報が、*joe* の $HOME/.java/.userPrefs/vrts ディレクトリに自動的に保存されます。(表の列の順序など)。この情報は、次回 *joe* というアカウントでオペレーティングシステムにログオンし、NetBackup アプリケーションを起動するときにリストアされます。このログオン方法では各管理者の状態情報が保存されるため、複数の管理者が存在する場合に有効です。

メモ: NetBackup では、アプリケーションの初回の終了時に、ユーザーの $HOME/.java/.userPrefs/vrts ディレクトリが作成されます。NetBackup アプリケーションだけが .java/.userPrefs/vrts ディレクトリを使用します。

10

役割に基づくアクセス制御

この章では以下の項目について説明しています。

RBAC の機能

NetBackup Web ユーザーインターフェースは、NetBackup 環境に役割に基づくアクセス制御を適用する機能を提供します。RBAC を使用して、現在 NetBackup へのアクセス権を持たないユーザーにアクセス権を提供します。または、現在管理者アクセス権を持っている NetBackup ユーザーに対して、組織内の役割に基づいて制限されたアクセス権を提供できます。

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 10-1 RBAC の機能

機能	説明
ユーザーに特定のタスクの実行を許可する役割	ユーザーを 1 つ以上のデフォルトの RBAC の役割に追加するか、ユーザーの役割に合わせてカスタムの役割を作成します。管理者の役割にユーザーを追加して、そのユーザーに完全な NetBackup 権限を付与します。 p.134 の「 デフォルトの RBAC の役割」を参照してください。
ユーザーの役割に合った NetBackup 領域および機能へのアクセス許可	RBAC ユーザーは、そのビジネスの役割において一般的なタスクを実行できますが、その他の NetBackup の領域や機能へのアクセスは制限されます。RBAC は、ユーザーが表示または管理できる資産も制御します。
RBAC イベントの監査	NetBackup は、RBAC イベントを監査します。
DR 準備完了	RBAC 設定は、NetBackup カタログで保護されています。

RBAC 設定

ユーザーの役割に基づいてアクセス制御の設定を構成できます。次の RBAC 設定を構成できます。

- オペレーティングシステム管理者の Web UI アクセス
- オペレーティングシステム管理者の CLI アクセス

OS (オペレーティングシステム) 管理者の Web UI アクセス権の無効化

デフォルトで、OS 管理者 (ユーザーまたはグループメンバー) は NetBackup Web UI にアクセスでき、RBAC の役割のメンバーである必要はありません。

OS 管理者に自動的にこのアクセス権を付与しない場合は、無効にできます。その場合、OS 管理者が Web UI にアクセスするには RBAC 管理者の役割が必要になります。

OS 管理者の Web UI アクセス制御を無効にするには

1 Web UI にサインインします。

2 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。

3 [セキュリティ制御 (Security controls)]タブで、[オペレーティングシステム管理者の Web UI アクセス権 (Web UI access for Operating System Administrator)]オプションをオフにします。

OS (オペレーティングシステム) 管理者のコマンドライン (CLI) アクセス権の無効化

デフォルトで、OS 管理者 (ユーザーまたはグループメンバー) は NetBackup CLI にアクセスでき、RBAC の役割のメンバーである必要はありません。

このオプションは、OS 管理者が NetBackup CLI を誤って実行するのを防ぎます。プライマリサーバーの OS 管理者のアクセス権を持つ悪意のあるユーザーは、この制限を回避できます。

オプションを無効にすると、OS 管理者が CLI にアクセスするには、`bpnbat -login` を使用してログインする必要があります。

OS 管理者の CLI アクセス権を無効にするには

1 Web UI にサインインします。

2 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。

3 [セキュリティ制御 (Security controls)]タブで、[オペレーティングシステム管理者の CLI アクセス権 (CLI access for Operating System Administrator)]オプションをオフにします。

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 10-2 役割ベースのアクセス制御を構成する手順

手順	処理	説明
1	すべての Active Directory または LDAP ドメインを構成します。	ドメインユーザーを追加する前に、NetBackup で Active Directory または LDAP ドメインを認証する必要があります。 『NetBackup セキュリティおよび暗号化ガイド』を参照してください。

手順	処理	説明
2	ユーザーに必要な権限を決定します。	ユーザーが日々のタスクを実行するために必要な権限を決定します。 デフォルトの RBAC の役割を使用するか、デフォルトの役割をテンプレートとして使用して、新しい役割を作成できます。または、必要に応じて、完全なカスタム役割を作成することもできます。 p.132 の「役割の権限」を参照してください。 p.134 の「 デフォルトの RBAC の役割」を参照してください。 p.139 の「カスタムの RBAC 役割の追加」を参照してください。
3	適切な役割にユーザーを追加します。	p.142 の「役割へのユーザーの追加 (非 SAML)」を参照してください。 p.144 の「役割へのユーザーの追加 (SAML)」を参照してください。 p.143 の「役割へのスマートカードユーザーの追加 (非 SAML、AD/LDAP なし)」を参照してください。
4	OS 管理者に必要な権限を決定します。	p.147 の「OS (オペレーティングシステム) 管理者の Web UI アクセス権の無効化」を参照してください。 p.146 の「OS (オペレーティングシステム) 管理者のコマンドライン (CLI) アクセス権の無効化」を参照してください。

役割の権限

役割の権限は、役割のユーザーが実行する権限を持つ操作を定義します。

個々の RBAC 権限と依存関係について詳しくは、NetBackup API のマニュアルを参照してください。

http://sort.veritas.com

表 10-3 NetBackup RBAC の役割の権限

カテゴリ	説明
グローバル	グローバル権限は、すべての資産またはオブジェクトに適用されます。 BMR - BMR の構成と管理。 NetBackup Web 管理コンソールの管理 (NetBackup Web Management Console Administration) - Veritas のサポートのガイダンスを受け、NetBackup のトラブルシューティングを行い、JVM ガーベジコレクションを実行するための診断ファイルを作成できます。 これらの操作は、NetBackup API からのみ利用可能です。JVM のチューニングオプションについて詳しくは、『NetBackup インストールガイド』、『NetBackup アップグレードガイド』を参照してください。 NetBackup の管理 - NetBackup の構成と管理。 保護 - NetBackup バックアップポリシーとストレージライフサイクルポリシー。 セキュリティ - NetBackup のセキュリティ設定。 ストレージ - バックアップストレージの設定の管理。
資産	1 つ以上の資産タイプを管理します。たとえば、VMware 資産です。
保護計画	保護計画を使用してバックアップを実行する方法を管理します。
クレデンシャル	NetBackup の資産とその他の機能のクレデンシャルを管理します。

NetBackup RBAC を使用するための注意事項

RBAC の役割の権限を構成する場合は、次の点に注意してください。

- 役割を作成するときに、ユーザーが Web UI にサインインして使用できるようにするために、最小数のアクセス権を確実に有効にします。個々のアクセス権が、Web UI の画面と直接的な相関を持たない場合があります。この種類のアクセス権しか付与されていないユーザーがサインインを試みると、「権限がない」ことを示すメッセージを受け取ります。
- ユーザーが役割に追加または削除された場合、ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。
- ほとんどの権限は暗黙的ではありません。
  ほとんどのケースで、[作成 (Create)]の権限では、ユーザーに[表示 (View)]権限は付与されません。[リカバリ (Recovery)]権限では、[表示 (View)]権限や、[上書き (Overwrite)]などのその他のリカバリオプションはユーザーに付与されません。

- すべての RBAC 制御された操作を NetBackup Web UI から使用できるわけではありません。これらの種類の操作は RBAC に含まれているので、役割の管理者は API ユーザーと Web UI ユーザーの役割を作成できます。
- 一部のタスクでは、複数の RBAC カテゴリの権限をユーザーに付与する必要があります。たとえば、リモートプライマリサーバーとの信頼関係を確立するには、ユーザーはリモートプライマリサーバーと信頼できるプライマリサーバーの両方に対する権限を持っている必要があります。

AD または LDAP ドメインの追加

NetBackup は、AD (Active Directory) または LDAP (ライトウェイトディレクトリアクセスプロトコル) のドメインユーザーをサポートします。RBAC の役割にドメインユーザーを追加する前に、AD または LDAP ドメインを追加する必要があります。また、ドメインでスマートカード認証を構成する前に、ドメインを追加する必要もあります。

`POST /security/domains/vxat` API または `vssat` コマンドを使用してドメインを設定できます。

`vssat` コマンドとそのオプションについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

デフォルトの RBAC の役割

NetBackup Web UI には、事前に権限や設定が構成されたデフォルトの RBAC の役割が用意されています。

表 10-4 NetBackup Web UI のデフォルトの RBAC の役割

役割名	説明
管理者	管理者の役割は、NetBackup の完全な権限を持ち、NetBackup のすべての側面を管理できます。
デフォルトの Apache Cassandra 管理者	この役割には、保護計画で Apache Cassandra 資産を管理および保護するために必要なすべての権限が付与されます。
デフォルトの AHV 管理者	この役割には、Nutanix Acropolis Hypervisor を管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。
デフォルトのクラウド管理者	この役割には、クラウド資産を管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。 PaaS 管理者には、カスタム役割に追加できる追加の権限が必要であることに注意してください。 p.137 の「PaaS 管理者のカスタムの RBAC の役割の追加」を参照してください。

役割名	説明
デフォルトのクラウドオブジェクトストア管理者	この役割には、従来のポリシーを使用してクラウドオブジェクトの保護を管理するためのすべての権限が付与されます。
デフォルトの IRE SLP 管理者	IRE (分離リカバリ環境) SLP (ストレージライフサイクルポリシー) 機能を管理します。
デフォルトの Kubernetes 管理者	この役割には、Kubernetes を管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。この役割の権限によって、ユーザーは Kubernetes 資産のジョブを表示および管理できます。この資産タイプのすべてのジョブを表示するには、その作業負荷に対するデフォルトの役割がユーザーに割り当てられている必要があります。または、役割を作成するときに、同様のカスタム役割にオプション[選択した権限を既存および今後のすべての作業負荷資産に適用する (Apply selected permissions to all existing and future workload assets)]を適用する必要があります。
デフォルトの Microsoft Sentinel 管理者	この役割には、Microsoft Exec のクレデンシャルを NetBackup に追加し、Microsoft Exec に NetBackup 監査イベントを送信するために必要なすべての権限が付与されます。
デフォルトの Microsoft SQL Server 管理者	この役割には、SQL Server データベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。この役割に加えて、NetBackup ユーザーは次の必要条件を満たす必要があります。 ■ Windows 管理者グループのメンバーである必要があります。 ■ SQL Server の「sysadmin」の役割を持っている必要があります。
デフォルトの MPA (マルチパーソン認証) の承認者	この役割には、MPA チケットを管理する権限があります。
デフォルトの MySQL 管理者	この役割には、MySQL インスタンスとデータベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。
デフォルトの NAS 管理者	この役割には、NAS-Data-Protection ポリシーを使用して NAS ボリュームのバックアップとリストアを実行するために必要なすべての権限が付与されています。NAS ボリュームのバックアップとリストアのすべてのジョブを表示するには、ユーザーにこの役割が必要です。または、役割の作成時に同じ権限が適用されたカスタム役割がユーザーに割り当てられている必要があります。
デフォルトの NetBackup コマンドライン (CLI) 管理者	この役割には、NetBackup コマンドライン (CLI) を使用して NetBackup を管理するために必要なすべての権限が付与されています。この役割を使用すると、ユーザーは、root 以外のアカウントでほとんどの NetBackup コマンドを実行できます。 注意: この役割のみを持つユーザーは、Web UI にサインインできません。
デフォルトの Oracle 管理者	この役割には、Oracle データベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。
デフォルトの PostgreSQL 管理者	この役割には、PostgreSQL インスタンスとデータベースを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。

役割名	説明
デフォルトの Resiliency 管理者	この役割には、Veritas Resiliency Platform (VRP) for VMware の資産を保護するためのすべての権限が付与されています。
デフォルトの RHV 管理者	この役割には、Red Hat Virtualization マシンを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。この役割によって、ユーザーは RHV 資産のジョブを表示および管理できます。 RHV 資産のすべてのジョブを表示するには、ユーザーにこの役割が必要です。または役割が作成される際、ユーザーには、[選択した権限を既存および今後のすべての RHV 資産に適用する (Apply selected permissions to all existing and future RHV assets)]オプションが適用された同様のカスタム役割が必要です。
デフォルトの SaaS 管理者	この役割には、SaaS 資産を表示および管理するためのすべての権限が付与されています。
デフォルトのセキュリティ管理者	この役割には、NetBackup セキュリティ (役割ベースのアクセス制御 (RBAC)、証明書、ホスト、ID プロバイダとドメイン、グローバルセキュリティ設定、その他の権限など) を管理する権限があります。またこの役割は、NetBackup のほとんどの領域の設定と資産 (作業負荷、ストレージ、ライセンス、その他の領域) を表示できます。
デフォルトのストレージ管理者	この役割には、ディスクベースのストレージとストレージライフサイクルポリシーを構成するための権限があります。SLP 設定は管理者役割で管理されます。
デフォルトのユニバーサル共有管理者	この役割には、ポリシーとストレージサーバーを管理するための権限があります。また、Windows および標準のクライアント形式の資産と、ユニバーサル共有の資産を管理できます。
デフォルトの Veritas Alta View 管理者	この役割には、Veritas Alta View 機能を管理するために必要なすべての権限が付与されます。
デフォルトの VMware 管理者	この役割には、VMware 仮想マシンを管理し、保護計画でそれらの資産をバックアップするために必要なすべての権限が付与されます。VMware 資産のすべてのジョブを表示するには、ユーザーにこの役割が必要です。または役割が作成される際、ユーザーには、[選択した権限を既存および今後のすべての VMware 資産に適用する (Apply selected permissions to all existing and future VMware assets)]オプションが適用された同様のカスタム役割が必要です。
NetBackup の読み取り専用オペレータ	IT Analytics オペレータ、マルチパーソン認証の承認者、およびその他の NetBackup のオペレータに、セキュリティの権限を持たない読み取り専用の権限を付与します。

メモ: Veritas は、今後のリリースでデフォルトの役割の RBAC 権限を更新する権限を留保します。更新された権限は、NetBackup のアップグレード時にこれらの役割のユーザーに自動的に適用されます。デフォルトの役割のコピーがある場合、これらの役割は自動的には更新されません。これらのカスタム役割にもデフォルトの役割に対する変更を適用するには、手動で変更を適用するか、カスタム役割を再作成する必要があります。

PaaS 管理者のカスタムの RBAC の役割の追加

PaaS 管理者には、追加のストレージ権限が必要です。デフォルトのクラウド管理者の役割をテンプレートとして使用して、カスタムの役割を作成できます。

カスタムの RBAC の役割を追加するには

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]をクリックします。
2. [デフォルトのクラウド管理者 (Default Cloud Administrator)]を選択します。
3. [役割名 (Role name)]と説明を指定します。

   たとえば、役割が PaaS 管理者であるすべてのユーザーを対象としていることを示すこともできます。
4. [権限 (Permissions)] で[割り当て (Assign)]をクリックします。
5. [グローバル (Global)]タブで[ストレージ (Storage)]セクションを展開します。次の権限を選択します。

ディスクプール	表示
ストレージサーバー	表示
ストレージユニバーサル共有	表示、作成

6. [資産 (Assets)]タブの目的のポリシー形式または作業負荷のセクションで、次の権限を選択します。
   - インスタントアクセス
   - マルウェアに感染したイメージからのリストア (マルウェアに感染したイメージからリストアするために必要)
7. [割り当て (Assign)]をクリックします。
8. [ユーザー (Users)]で[割り当て (Assign)]をクリックします。次に、このカスタム役割へのアクセス権を付与する各ユーザーを追加します。
9. 役割の構成が完了したら、[役割の追加 (Add role)]をクリックします。

Azure 管理対象インスタンスをリストアするためのカスタムの RBAC の役割の追加

Azure 管理対象インスタンスをリストアするには、そのインスタンスの表示権限がユーザーに付与されている必要があります。管理者および同様のユーザーは、その他のユーザーにカスタム役割とこの権限を付与できます。

Azure 管理対象インスタンスの表示権限を割り当てるには

1 管理対象インスタンスのアクセス制御 ID を取得するには、次のコマンドを入力します。

```
GET
/asset-service/workloads/cloud/assets?filter=extendedAttributes/
managedInstanceName eq 'managedInstanceName'
```

レスポンスの中から *accessControlId* フィールドを探します。このフィールドの値をメモします。

2 役割 ID を取得するには、次のコマンドを入力します。

```
GET /access-control/roles
```

レスポンスの中から *id* フィールドを探します。このフィールドの値をメモします。

3 次のように、アクセス定義を作成します。

```
POST /access-control/managed-objects/{objectId}/access-definitions
```

要求ペイロード

```
{

    "data": {
        "type": "accessDefinition",
        "attributes": {
            "propagation": "OBJECT_AND_CHILDREN"
        },
        "relationships": {
            "role": {
                "data": {
                    "id": "<roleId>",
                    "type": "accessControlRole"
                }
            },
            "operations": {
                "data": [
                    {
                        "id": "|OPERATIONS|VIEW|",
                        "type": "accessControlOperation"
                    }
                ]
            },
            "managedObject": {
                "data": {
```

```
                    "id": "<objectId>",
                    "type": "managedObject"
                }
            }
        }
    }
}
```

次の値を使用します。

- `objectId`: 手順 1 で取得した *accessControlId* の値を使用します。
- `roleId`: 手順 2 で取得した *id* の値を使用します。

メモ: 代替リストアの場合は、*operations* リストに `|OPERATIONS|ASSETS|CLOUD|RESTORE_DESTINATION|` 権限を指定します。

カスタムの RBAC 役割の追加

ユーザーが作業負荷資産、保護計画、またはクレデンシャルに対して持つ権限とアクセス権を手動で定義する場合は、カスタムの RBAC の役割を作成します。

メモ: Veritas は、今後のリリースでデフォルトの役割の RBAC 権限を更新する権限を留保します。更新された権限は、NetBackup のアップグレード時にこれらの役割のユーザーに自動的に適用されます。デフォルトの役割 (またはデフォルトの役割に基づくカスタム役割) のコピーは、自動的には更新されません。

カスタムの RBAC の役割を追加するには

1. NetBackup Web UI にサインインします。
2. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択して、[追加 (Add)]をクリックします。
3. 作成する役割の種類を選択します。

   その種類の役割の定義済み権限と設定をすべて含んだ、デフォルトの役割のコピーを作成できます。または、[カスタム役割 (Custom role)]を選択して、役割に付与するすべて権限を手動で設定します。
4. [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。

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

選択する権限によって、役割に対して設定できるその他の設定が決まります。

デフォルトの役割の種類を選択すると、特定の権限が、その種類の役割に必要な場合にのみ有効になります。たとえば、デフォルトのストレージ管理者には、保護計画に対する権限は不要です。デフォルトの Microsoft SQL Server 管理者にはクレデンシャルが必要です。

- [作業負荷 (Workloads)]は、[資産 (Asset)]の権限を選択すると有効になります。
- [保護計画 (Protection plans)]は、[保護計画 (Protection plans)]の権限を選択すると有効になります。
- [クレデンシャル (Credentials)]は、[クレデンシャル (Credentials)]の権限を選択すると有効になります。

6 役割の権限を構成します。

p.132 の「役割の権限」を参照してください。

p.133 の「NetBackup RBAC を使用するための注意事項」を参照してください。

7 [ユーザー (Users)]で[割り当て (Assign)]をクリックします。

8 役割の構成が完了したら、[保存 (Save)]をクリックします。

注意: 役割の作成後、資産、保護計画、クレデンシャルの権限は、Web UI の該当するノードで直接編集する必要があります。たとえば、VMware の権限を編集するには、[作業負荷 (Workloads)]、[VMware]の順に移動し、[VMware 設定 (VMware settings)]、[権限の管理 (Manage permissions)]の順に選択します。または、VM の詳細を開き、[権限 (Permissions)]タブをクリックします。

カスタム役割の編集または削除

カスタム役割を持つユーザーに対するアクセス権を変更または削除する場合に、この役割を編集または削除できます。デフォルトの役割は編集または削除できません。デフォルトの役割に対してユーザーを追加または削除することのみ可能です。

カスタム役割の編集

メモ: カスタム役割のアクセス権を変更すると、その役割に割り当てられているすべてのユーザーに変更が影響します。

カスタム役割を編集するには

1 NetBackup Web UI にサインインします。

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

3 [ロール (Roles)]タブで、編集するカスタム役割を特定してクリックします。

4 役割の説明を編集するには、[名前と説明を編集する (Edit name and description)]をクリックします。

5 役割の権限を編集します。役割について次の詳細情報を編集できます。

役割のグローバル権限	[グローバル権限 (Global permissions)]タブで、[編集 (Edit)]をクリックします。
役割のユーザー	[ユーザー (Users)]タブをクリックします。
役割のアクセス定義	[アクセス定義 (Access definitions)]タブをクリックします。

p.132 の「役割の権限」を参照してください。

p.133 の「NetBackup RBAC を使用するための注意事項」を参照してください。

6 役割のユーザーを追加または削除するには、[ユーザー (Users)]タブをクリックします。

p.142 の「役割へのユーザーの追加 (非 SAML)」を参照してください。

p.144 の「役割からのユーザーの削除」を参照してください。

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

カスタム役割の削除

メモ: 役割を削除すると、その役割に割り当てられていたすべてのユーザーが、役割で提供されていたすべてのアクセス権を失います。

カスタム役割を削除するには

1 NetBackup Web UI にサインインします。

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

3 [ロール (Roles)]タブをクリックします。

4 削除するカスタム役割を特定して、そのチェックボックスにチェックマークを付けます。

5 [削除 (Remove)]、[はい (Yes)]の順にクリックします。

RBAC でのユーザーの表示

RBAC に追加されているユーザーと、そのユーザーに割り当てられている役割を表示できます。[ユーザー (Users)]リストは表示専用です。役割に割り当てられているユーザーを編集するには、その役割を編集する必要があります。

RBAC でユーザーを表示するには

1. NetBackup Web UI にサインインします。
2. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
3. [ユーザー (Users)]タブをクリックします。
4. [役割 (Roles)]列に、ユーザーが割り当てられている各役割が表示されます。

役割へのユーザーの追加 (非 SAML)

このトピックでは、非 SAML ユーザーまたはグループを役割に追加する方法について説明します。

非 SAML ユーザーは、ユーザー名とパスワードでサインインするか、スマートカードでサインインする方式を使用できます。

役割にユーザーを追加するには (非 SAML)

1. NetBackup Web UI にサインインします。
2. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
3. [ロール (Roles)]タブをクリックします。
4. 役割名をクリックし、[ユーザー (Users)]タブをクリックします。
5. (該当する場合) [サインインの種類 (Sign-in type)]リストで次から選択します。
   - [デフォルトのサインイン (Default sign-in)]: ユーザー名とパスワードで NetBackup にサインインするユーザーの場合に選択します。
   - [スマートカードユーザー (Smart card user)]: スマートカードを使用して NetBackup にサインインするユーザーの場合に選択します。

   注意: [サインインの種類 (Sign-in type)]リストは、NetBackup に利用可能な IDP 構成がある場合にのみ利用可能です。

6 追加するユーザーまたはグループの名前を入力します。

ユーザーの種類	使用する形式	例
ローカルユーザーまたはグループ	*username*	jane_doe
	groupname	admins
Windows ユーザーまたはグループ	*DOMAIN*¥*username*	WINDOWS¥jane_doe
	DOMAIN¥groupname	WINDOWS¥Admins
UNIX ユーザーまたはグループ	*username*@*domain*	john_doe@unix
	groupname@*domain*	admins@unix

7 [リストに追加 (Add to list)]をクリックします。

8 ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割へのスマートカードユーザーの追加 (非 SAML、AD/LDAP なし)

このトピックでは、スマートカードユーザーを役割に追加する方法について説明します。この場合、ユーザーは非 SAML ユーザーで、AD または LDAP ドメインの関連付けやマッピングはありません。この形式の構成では、ユーザーグループはサポートされません。

このタイプのユーザーは、スマートカードによるサインイン方法を使用します。

役割にスマートカードユーザーを追加するには (非 SAML、AD/LDAP なし)

1 NetBackup Web UI にサインインします。

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

3 [ロール (Roles)]タブをクリックします。

4 役割名をクリックし、[ユーザー (Users)]タブをクリックします。

5 (該当する場合) [サインインの種類 (Sign-in type)]リストで[スマートカードユーザー (Smart card user)]を選択します。

メモ: [サインインの種類 (Sign-in type)]リストは、NetBackup に利用可能な IDP 構成がある場合にのみ利用できます。[サインインの種類 (Sign-in type)]リストにあるスマートカードユーザーオプションは、AD または LDAP ドメインマッピングなしでスマートカードの構成を行うときに使用できます。

---

6 追加するユーザー名を入力します。

証明書で利用可能な正確な一般名 (CN) またはユニバーサルプリンシパル名 (UPN) を指定します。

7 [リストに追加 (Add to list)]をクリックします。

8 ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割へのユーザーの追加 (SAML)

このトピックでは、SAML ユーザーまたはグループを役割に追加する方法について説明します。

SAML ユーザーは、SAML ユーザーまたは SAML グループのいずれかのサインイン方式を使用します。

役割にユーザーを追加するには (SAML)

1 NetBackup Web UI にサインインします。

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

3 [ロール (Roles)]タブをクリックします。

4 役割名をクリックし、[ユーザー (Users)]タブをクリックします。

5 [サインインの種類 (Sign-in type)]リストから、サインイン方法として[SAML ユーザー (SAML user)]または[SAML グループ (SAML group)]を選択します。

6 追加するユーザーまたはグループの名前を入力します。

たとえば、nbuadmin@my.host.com です。

IDP (ID プロバイダ) が (CN=groupname、DC=domainname) または domainname¥groupname の形式でグループ情報を返す場合は、groupname@domainname 形式を使用してグループを追加する必要があります。ただし、ドメイン名を含めずに、役割ベースのアクセス制御 (RBAC) で SAML グループを構成することもできます。IDP がドメイン情報なしでグループ名を返す場合は、これらのグループをプレーンテキストとして追加できます。SAML グループでは、電子メール形式の使用は必須ではありません。

7 [リストに追加 (Add to list)]をクリックします。

8 ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割からのユーザーの削除

役割を持つユーザーに対する権限を削除する場合、役割からユーザーを削除できます。

ユーザーが役割から削除された場合、ユーザーの権限を更新するには、ユーザーがサインアウトして再度サインインする必要があります。

役割からユーザーを削除するには

1. NetBackup Web UI にサインインします。
2. 左側で、[セキュリティ (Security)]、[RBAC]の順にクリックします。
3. [ロール (Roles)]タブをクリックします。
4. 編集する役割をクリックし、[ユーザー (Users)]タブを選択します。
5. 削除するユーザーを見つけ、[処理 (Actions)]、[削除 (Remove)]、[削除 (Remove)]の順にクリックします。

11

OS 管理者の NetBackup インターフェースアクセス

この章では以下の項目について説明しています。

OS (オペレーティングシステム) 管理者のコマンドライン (CLI) アクセス権の無効化

デフォルトで、OS 管理者 (ユーザーまたはグループメンバー) は NetBackup CLI にアクセスでき、RBAC の役割のメンバーである必要はありません。

このオプションは、OS 管理者が NetBackup CLI を誤って実行するのを防ぎます。プライマリサーバーの OS 管理者のアクセス権を持つ悪意のあるユーザーは、この制限を回避できます。

オプションを無効にすると、OS 管理者が CLI にアクセスするには、`bpnbat -login` を使用してログインする必要があります。

OS 管理者の CLI アクセス権を無効にするには

1. Web UI にサインインします。
2. 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。
3. [セキュリティ制御 (Security controls)]タブで、[オペレーティングシステム管理者の CLI アクセス権 (CLI access for Operating System Administrator)]オプションをオフにします。

OS (オペレーティングシステム) 管理者の Web UI アクセス権の無効化

デフォルトで、OS 管理者 (ユーザーまたはグループメンバー) は NetBackup Web UI にアクセスでき、RBAC の役割のメンバーである必要はありません。

OS 管理者に自動的にこのアクセス権を付与しない場合は、無効にできます。その場合、OS 管理者が Web UI にアクセスするには RBAC 管理者の役割が必要になります。

OS 管理者の Web UI アクセス制御を無効にするには

1. Web UI にサインインします。
2. 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。
3. [セキュリティ制御 (Security controls)]タブで、[オペレーティングシステム管理者の Web UI アクセス権 (Web UI access for Operating System Administrator)]オプションをオフにします。

12

スマートカードまたはデジタル証明書

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

ユーザー検証では、スマートカードまたは証明書を AD または LDAP ドメインにマップできます。または、AD または LDAP ドメインなしでスマートカードまたは証明書を構成することもできます。

p.148 の「ドメインを使用したスマートカード認証の構成」を参照してください。

p.150 の「ドメインを使用しないスマートカード認証の構成」を参照してください。

ドメインを使用したスマートカード認証の構成

AD または LDAP ドメインでスマートカードまたは証明書を使用してユーザーを認証するように NetBackup を構成できます。

次の前提条件に注意してください。

- 認証方法を追加する前に、NetBackup ユーザーに関連付けられているドメインを追加する必要があります。『NetBackup セキュリティおよび暗号化ガイド』を参照してください。
- スマートカードまたは証明書の認証を構成する前に、NetBackup ユーザーについて、役割に基づくアクセス制御 (RBAC) 構成を完了していることを確認してください。p.131 の「RBAC の構成」を参照してください。

ドメインを使用してスマートカード認証を構成するには

1. NetBackup Web UI にサインインします。
2. 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。
3. [スマートカード認証 (Smart card authentication)]をオンにします。
4. [ドメインの選択 (Select the domain)]オプションから必要な AD または LDAP ドメインを選択します。
5. [証明書のマッピング属性 (Certificate mapping attribute)]を選択します (一般名 (CN) またはユニバーサルプリンシパル名 (UPN))。
6. 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。
7. [保存 (Save)]をクリックします。
8. [CA 証明書 (CA certificates)]の右にある[追加 (Add)]をクリックします。
9. [CA 証明書 (CA certificates)]を参照するかドラッグアンドドロップして、[追加 (Add)]をクリックします。

   スマートカード認証には、信頼できる root CA 証明書または中間 CA 証明書のリストが必要です。ユーザーのデジタル証明書またはスマートカードに関連付けられている CA 証明書を追加します。

   証明書ファイルの種類は `.crt`、`.cer`、`.der`、`.pem`、または `PKCS #7` 形式で、サイズが 64 KB 未満である必要があります。
10. [スマートカード認証 (Smart card authentication)]ページで構成情報を確認します。

11 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。

12 ユーザーがサインインするときに、[証明書またはスマートカードでサインイン (Sign in with certificate or smart card)]のオプションが表示されるようになりました。

ユーザーにまだこのサインインオプションを使用させない場合は、[スマートカード認証 (Smart card authentication)]をオフにします(たとえば、ホストにすべてのユーザーの証明書がまだ構成されていない場合)。スマートカード認証を無効にした場合でも、構成した設定は保持されます。

このようなユーザーの場合、ドメイン名とドメイン形式はスマートカードです。

ドメインを使用しないスマートカード認証の構成

関連付けられた AD または LDAP ドメインを使用せずにスマートカードまたは証明書でユーザーを認証するように NetBackup を構成できます。この構成では、ユーザーのみがサポートされます。ユーザーグループはサポートされません。

ドメインを使用しないスマートカード認証を構成するには

1 NetBackup Web UI にサインインします。

2 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。

3 [スマートカード認証 (Smart card authentication)]をオンにします。

4 (該当する場合の手順) AD または LDAP ドメインが環境内で構成されている場合は、[ドメインなしで続行 (Continue without the domain)]を選択します。

5 [証明書のマッピング属性 (Certificate mapping attribute)]を選択します (一般名 (CN) またはユニバーサルプリンシパル名 (UPN))。

6 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。

7 [保存 (Save)]をクリックします。

8 [CA 証明書 (CA certificates)]の右にある[追加 (Add)]をクリックします。

9 [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。

10 スマートカード認証には、信頼できる root CA 証明書または中間 CA 証明書のリストが必要です。ユーザーのデジタル証明書またはスマートカードに関連付けられている CA 証明書を追加します。

証明書ファイルの種類は .crt、.cer、.der、.pem、または PKCS #7 形式で、サイズが 64 KB 未満である必要があります。

11 [スマートカード認証 (Smart card authentication)]ページで構成情報を確認します。

ユーザーがスマートカードにインストールされていないデジタル証明書を使用するには、事前にブラウザの証明書マネージャに証明書をアップロードする必要があります。

12 ユーザーがサインインするときに、[証明書またはスマートカードでサインイン (Sign in with certificate or smart card)]のオプションが表示されるようになりました。

ユーザーにまだこのサインインオプションを使用させない場合は、[スマートカード認証 (Smart card authentication)]をオフにします(たとえば、ホストにすべてのユーザーの証明書がまだ構成されていない場合)。スマートカード認証を無効にした場合でも、構成した設定は保持されます。

スマートカード認証の構成の編集

スマートカード認証の構成に変更がある場合は、構成の詳細を編集できます。

ドメインを使用したユーザー認証の構成を編集するには

1 NetBackup Web UI にサインインします。

2 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。

3 次のような場合に、AD または LDAP ドメインの選択を編集できます。

- 既存のドメインとは異なるドメインを選択する場合
- 既存のドメインが削除されたため、新しいドメインを選択する場合
- ドメインなしで続行する場合

[編集 (Edit)]をクリックします。

4 ドメインを選択します。

NetBackup 用に構成されているドメインのみがこのリストに表示されます。

ドメインを使用するユーザーを検証しない場合は、[ドメインなしで続行 (Continue without the domain)]を選択できます。

5 [証明書のマッピング属性 (Certificate mapping attribute)]を編集します。

6 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 NetBackup Web UI にサインインします。

2 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。

3 [追加 (Add)]をクリックします。

4 [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 NetBackup Web UI にサインインします。

2 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。

3 削除する CA 証明書を選択します。

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

スマートカード認証を無効にするか一時的に無効にする

プライマリサーバーでスマートカード認証を使用する必要がなくなった場合は、スマートカード認証を無効にできます。または、ユーザーがスマートカードを使用できるようにする前に、その他の構成を完了する必要がある場合も同様です。

スマートカード認証を無効にするには

1. NetBackup Web UI にサインインします。
2. 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。
3. [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。

13

シングルサインオン (SSO)

この章では以下の項目について説明しています。

SSO (シングルサインオン) 設定について

認証および認可情報の交換に SAML 2.0 プロトコルを使用する任意の IDP (ID プロバイダ) を使用して、SSO (シングルサインオン) を構成できます。複数の Veritas 製品で 1 つの IDP を構成できることに注意します。たとえば、同じ IDP を NetBackup と APTARE で構成できます。

次の必要条件と制限事項に注意してください。

- SSO を使用するには、環境で SAML 2.0 に準拠した ID プロバイダが構成されている必要があります。
- AD または LDAP ディレクトリサービスを使用する ID プロバイダのみがサポートされます。
- IDP の構成には、NetBackup API または NetBackup コマンド `nbidpcmd` が必要です。
- SAML ユーザーは API を使用できません。API キーはユーザーを認証するために使われるため、SAML 認証されたユーザーには使用できません。
- グローバルログアウトはサポートされません。

NetBackup の SSO (シングルサインオン) の構成

この項では、IDP と NetBackup プライマリサーバー間で信頼を構築し、構成情報を交換する手順について説明します。手順を続行する前に、環境内で次の前提条件が満たされていることを確認します。

- IDP が、お使いの環境で設定および配備されています。
- IDP が、AD (Active Directory) またはライトウェイト ディレクトリ アクセス プロトコル (LDAP) のドメインユーザーを認証するように設定されています。

表 13-1 NetBackup のシングルサインオンを構成する手順

手順	処理	説明
1.	IDP メタデータ XML ファイルのダウンロード	IDP メタデータ XML ファイルを IDP からダウンロードして保存します。 XML ファイルに保存された SAML メタデータが、IDP と NetBackup プライマリサーバー間で構成情報を共有するために使用されます。IDP メタデータ XML ファイルは、NetBackup プライマリサーバーに IDP 構成を追加するために使用されます。
2.	NetBackup プライマリサーバーでの SAML キーストアの構成と IDP 構成の追加および有効化	p.156 の「SAML キーストアの構成」を参照してください。 p.159 の「SAML キーストアの構成と IDP 構成の追加および有効化」を参照してください。
3.	サービスプロバイダ (SP) メタデータ XML ファイルのダウンロード	NetBackup プライマリサーバーは、NetBackup 環境内の SP です。ブラウザに次の URL を入力して、NetBackup プライマリサーバーから SP メタデータ XML ファイルにアクセスします。 `https://masterserver/netbackup/sso/saml2/metadata` ここで *masterserver* には、NetBackup プライマリサーバーの IP アドレスまたはホスト名を指定します。
4.	サービスプロバイダ (SP) としての NetBackup プライマリサーバーの IDP への登録	p.161 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

手順	処理	説明
5.	必要な RBAC の役割に対する SSO を使用する SAML ユーザーと SAML グループの追加	SAML ユーザーと SAML ユーザーグループは、NetBackup プライマリサーバーで IDP が構成され、有効になっている場合にのみ RBAC で利用可能です。RBAC の役割の追加の手順については、次のトピックを参照してください。 p.142 の「役割へのユーザーの追加 (非 SAML)」を参照してください。

初回の設定後、IDP 構成を有効化、更新、無効化、または削除するかを選択できます。

p.162 の「IDP 構成の管理」を参照してください。

初期設定後、NetBackup CA SAML キーストアのアップデート、更新、または削除を選択できます。ECA SAML キーストアを構成して管理することもできます。

SAML キーストアの構成

NetBackup プライマリサーバーと IDP サーバーの間の信頼を確立するには、NetBackup プライマリサーバーに SAML キーストアを構成する必要があります。NetBackup CA を使用しているか、外部認証局 (ECA) を使用しているかに応じて、次のセクションのいずれかを参照してください。

メモ: 環境内で ECA と NetBackup CA の組み合わせを使用している場合、デフォルトでは、IDP サーバーとの信頼関係を確立するときに ECA が考慮されます。

メモ: `configureCerts.bat`、`configureCerts`、`configureSAMLECACert.bat`、`configureSAMLECACert` などのバッチファイルを使用した SAML キーストア構成と、それに対応するオプションは非推奨です。

NetBackup CA キーストアの構成

NetBackup CA を使用している場合は、NetBackup プライマリサーバー上に NetBackup CA キーストアを作成します。

NetBackup CA キーストアを作成するには

1. NetBackup プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -cCert -M master_server -f
   ```

   `-f` は省略可能です。強制更新のオプションを使用します。

NetBackup CA キーストアが作成されたら、NetBackup CA 証明書が更新されるたびに NetBackup CA キーストアを更新してください。

NetBackup CA キーストアを更新するには

1. NetBackup プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -rCert -M master_server
   ```

3. ブラウザに次の URL を入力して、NetBackup プライマリサーバーから新しい SP メタデータ XML ファイルをダウンロードします。

   https://*primaryserver*/netbackup/sso/saml2/metadata

   ここで、*primaryserver* は NetBackup プライマリサーバーの IP アドレスまたはホスト名です。
4. IDP に新しい SP メタデータ XML ファイルをアップロードします。

   p.161 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

NetBackup CA キーストアを削除するには

1. NetBackup プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -dCert -M master_server
   ```

3. ブラウザに次の URL を入力して、NetBackup プライマリサーバーから新しい SP メタデータ XML ファイルをダウンロードします。

   https://*primaryserver*/netbackup/sso/saml2/metadata

   ここで、*primaryserver* は NetBackup プライマリサーバーの IP アドレスまたはホスト名です。
4. IDP に新しい SP メタデータ XML ファイルをアップロードします。
5. p.161 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

ECA キーストアの構成

ECA を使用している場合は、ECA キーストアを NetBackup プライマリサーバーにインポートします。

メモ: 環境内で ECA と NetBackup CA の組み合わせを使用している場合、デフォルトでは、IDP サーバーとの信頼関係を確立するときに ECA が考慮されます。NetBackup CA を使用するには、最初に ECA キーストアを削除する必要があります。

ECA キーストアを構成するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. 構成済みの NetBackup ECA キーストアを使用して SAML ECA キーストアを構成するか、ECA 証明書チェーンと秘密鍵を指定するかに応じて、次のコマンドを実行します。
   - 構成済みの NetBackup ECA キーストアを使用するには、次のコマンドを実行します。

     ```
     nbidpcmd -cECACert -uECA existing ECA configuration [-f] [-M primary_server]
     ```
   - ユーザーが指定した ECA 証明書チェーンと秘密鍵を使用するには、次のコマンドを実行します。

     ```
     nbidpcmd -cECACert -certPEM certificate chain file -privKeyPath private key file [-ksPassPath Keystore Passkey File] [-f] [-M <master_server>]
     ```
   - 証明書チェーンファイル (certificate chain file) には証明書チェーンファイルのパスを指定します。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。
   - 秘密鍵ファイル (private key file) には秘密鍵ファイルのパスを指定します。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。
   - キーストアパスキーファイル (Keystore Passkey File) にはキーストアパスワードファイルパスを指定します。構成を実行するプライマリサーバーからこのファイルにアクセス可能である必要があります。
   - プライマリサーバー (Primary server) は、SAML ECA キーストア構成を実行するプライマリサーバーのホスト名または IP アドレスです。コマンドを実行する NetBackup プライマリサーバーがデフォルトで選択されます。

ECA キーストアを削除するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. ブラウザに次の URL を入力して、NetBackup プライマリサーバーから新しい SP メタデータ XML ファイルをダウンロードします。

   https://*primaryserver*/netbackup/sso/saml2/metadata

   ここで、*primaryserver* は NetBackup プライマリサーバーの IP アドレスまたはホスト名です。
3. IDP に新しい SP メタデータ XML ファイルをアップロードします。

   p.161 の「IDP を使用した NetBackup プライマリサーバーの登録」を参照してください。

SAML キーストアの構成と IDP 構成の追加および有効化

次の手順に進む前に、IDP メタデータ XML ファイルをダウンロードして NetBackup プライマリサーバーに保存したことを確認します。

SAML キーストアを構成し、IDP 構成を追加および有効化するには

1. プライマリサーバーにルートまたは管理者としてログオンします。
2. 次のコマンドを実行します。

   IDP と NetBackup CA SAML キーストアの構成の場合:

   ```
   nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
   [-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
   group field] [-cCert] [-f] [-M primary server]
   ```

   または、IDP と ECA SAML キーストアの構成の場合:

   構成済みの NetBackup ECA キーストアを使用して SAML ECA キーストアを構成するか、ECA 証明書チェーンと秘密鍵を指定するかに応じて、次のコマンドを実行します。

   - NetBackup ECA 構成のキーストアを使用する:

     ```
     nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
     file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
     user group field] -cECACert -uECA existing ECA configuration
     [-f] [-M Primary Server]
     ```

   - ユーザーが指定した ECA 証明書チェーンと秘密鍵を使用する:

     ```
     nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata
     file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP
     user group field] -cECACert -certPEM certificate chain file
     -privKeyPath private key file [-ksPassPath KeyStore passkey
     file] [-f] [-M primary server]
     ```

   変数は次のように置き換えます。

   - *IDP configuration name* は、IDP 構成に指定された一意の名前です。
   - *IDP XML metadata file* は、XML メタデータファイルへのパスです。これには、IDP の構成の詳細が Base64URL エンコードされた形式で含まれます。
   - `-e true | false` は、IDP 構成を有効または無効にします。IDP 構成が追加されて有効になっている必要があります。そうでない場合、ユーザーは SSO (シングルサインオン) オプションを使ってサインインできません。NetBackup プライマリサーバーに複数の IDP 構成を追加することもできますが、一度に 1 つの IDP 構成のみを有効にできます。
   - SAML 属性名 IDP ユーザーフィールドと IDP ユーザーグループフィールドは、ID プロバイダのユーザー ID 情報とグループ情報のマッピングに使用されます。

これらのフィールドは省略可能であり、指定されない場合はデフォルトで userPrincipalName および memberOf の各 SAML 属性にマップされます。
たとえば、電子メールやグループなどの属性を使用するように ID プロバイダの属性マッピングをカスタマイズする場合、SAML 構成を構成するときに、電子メールに対して -u オプション、グループに対して -g オプションを指定する必要があります。
構成中にこれらの属性の値を指定しなかった場合は、ID プロバイダは userPrincipalName 属性と memberOf 属性に対して値が返されることを保証します。
次に例を示します。
SAML 応答が次の場合:
saml:AttributeStatement <saml:Attribute Name="userPrincipalName">
<saml:AttributeValue>username@domainname</saml:AttributeValue>
</saml:Attribute> <saml:Attribute Name="memberOf">
<saml:AttributeValue>CN=group name,
DC=domainname</saml:AttributeValue> </saml:Attribute>
</saml:AttributeStatement>
フィールド「saml:Attribute Name」に対して -u オプションと -g オプションをマッピングする必要があることを意味します。

メモ: デフォルトが userPrincipalName の -u オプションにマッピングされているフィールドに対して、SAML 属性値が *username@domainname* の形式で返されることを確認します。グループ情報を返すときにドメイン名を含める場合は、「(CN=group name, DC=domainname)」または「(domainname¥groupname)」の形式に従う必要があります。

ただし、ドメイン情報なしでプレーンテキストとしてグループ名を返す場合は、SAML RBAC グループ内のドメイン名なしでマッピングする必要があります。

- *primary Server* は、IDP 構成を追加または変更するプライマリサーバーのホスト名または IP アドレスです。コマンドを実行する NetBackup プライマリサーバーがデフォルトで選択されます。
- *Certificate Chain File* は証明書チェーンファイルのパスです。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。

  Private Key File は秘密鍵ファイルのパスです。このファイルは PEM 形式である必要があります。また、構成を実行するプライマリサーバーからアクセス可能である必要があります。

  KeyStore Passkey File はキーストアパスキーファイルのパスです。構成を実行するプライマリサーバーからこのファイルにアクセス可能である必要があります。

ID プロバイダに SAML 属性名が `userPrincipalName` と `memberOf` としてすでに構成されている場合、構成時に `-u` と `-g` オプションを指定する必要はありません。他のカスタム属性名を使用している場合は、次に示すように、`-u` と `-g` に対して名前を指定します。

例:

ID プロバイダの SAML 属性名が「email」と「groups」としてマッピングされている場合は、次のコマンドを使用して構成します。

```
nbidpcmd -ac -n veritas_configuration -mxp file.xml -t SAML2 -e
true -u email -g groups -cCert -Mprimary_server.abc.com
```

`-u` と `-g` は省略可能であり、ID プロバイダの構成によって異なります。構成時に指定したパラメータ値と同じ値を指定してください。

IDP を使用した NetBackup プライマリサーバーの登録

IDP にサービスプロバイダ (SP) として NetBackup プライマリサーバーを登録する必要があります。特定の IDP に固有の順を追った手順については、次の表を参照してください。

表 13-2 NetBackup プライマリサーバーを登録するための IDP 固有の手順

IDP 名	手順へのリンク
ADFS	https://www.veritas.com/docs/100047744
Okta	https://www.veritas.com/docs/100047745
PingFederate	https://www.veritas.com/docs/100047746
Azure	https://www.veritas.com/docs/100047748
Shibboleth	https://www.veritas.com/docs/00047747

IDP を使用して SP を登録するには、通常、次の操作が含まれます。

IDP への SP メタデータ XML ファイルのアップロード

SP メタデータ XML ファイルには、SP 証明書、エンティティ ID、アサーションコンシューマーサービス URL (ACS URL)、およびログアウト URL (SingleLogoutService) が含まれます。SP メタデータ XML ファイルは、IDP が信頼関係を確立し、SP との間で認証と認可の情報を交換するために必要です。

AD または LDAP 属性への SAML 属性のマッピング

属性マッピングは、SSO の SAML 属性を AD または LDAP ディレクトリ内の対応する属性とマッピングするために使用されます。SAML 属性マッピングは、NetBackup プライマ

リサーバーに送信される SAML 応答の生成に使用されます。userPrincipalName にマッピングされる SAML 属性と、AD または LDAP ディレクトリ内の memberOf 属性を定義していることを確認します。SAML 属性は次の形式に従う必要があります。

表 13-3

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

メモ: NetBackup プライマリサーバーに IDP の構成を追加するときに、ユーザー (-u) オプションとユーザーグループ (-g) オプションに入力する値は、AD または LDAP の userPrincipalName 属性および memberOf 属性にマッピングされている SAML 属性名と一致する必要があります。

p.159 の「SAML キーストアの構成と IDP 構成の追加および有効化」を参照してください。

IDP 構成の管理

NetBackup マスターサーバーで ID プロバイダ (IDP) の構成を管理するには、nbidpcmd コマンドの enable (-e true)、update (-uc)、disable (-e false)、および delete (-dc) オプションを使用します。

IDP 構成の有効化

デフォルトでは、本番環境で IDP 構成は有効になっていません。IDP を追加したときに有効にしなかった場合、-uc -e true オプションを使用して、IDP 構成を更新および有効化できます。

IDP 構成を有効化するには

1. プライマリサーバーに root または管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -uc -n IDP configuration name -e true
   ```

   IDP configuration name は、IDP 構成に指定された一意の名前です。

メモ: NetBackup プライマリサーバーに複数の IDP を構成することもできますが、一度に 1 つの IDP のみを有効にできます。

IDP 構成の更新

IDP 構成に関連付けられている XML メタデータファイルを更新できます。

IDP 構成内の IDP XML メタデータファイルを更新するには

1. プライマリサーバーに root または管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -uc -n IDP configuration name -mxp IDP XML metadata file
   ```

   以下の説明に従って変数を置き換えます。

   - *IDP configuration name* は、IDP 構成に指定された一意の名前です。
   - *IDP XML metadata file* は、XML メタデータファイルへのパスです。これには、IDP の構成の詳細が Base64URL エンコードされた形式で含まれます。

IDP 構成の IDP ユーザーまたは IDP ユーザーグループの値を更新する場合は、まず構成を削除する必要があります。更新後の IDP ユーザーまたは IDP ユーザーグループの値が含まれる構成を再度追加するまで、ユーザーは SSO (シングルサインオン) オプションを利用できません。

IDP 構成で IDP ユーザーまたは IDP ユーザーグループを更新するには

1. プライマリサーバーに root または管理者としてログオンします。
2. IDP 構成を削除します。

   ```
   nbidpcmd -dc -n IDP configuration name
   ```

   IDP configuration name は、IDP 構成に指定された一意の名前です。
3. 構成を再度追加して有効にするには、次のコマンドを実行します。

   ```
   nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
   [-t SAML2] [-e true | false] [-u IDP user] [-g IDP user group
   field] [-M Master Server
   ```

   以下の説明に従って変数を置き換えます。

   - *IDP configuration name* は、IDP 構成に指定された一意の名前です。
   - *IDP XML metadata file* は、XML メタデータファイルへのパスです。これには、IDP の構成の詳細が Base64URL エンコードされた形式で含まれます。
   - `-e true | false` は、IDP 構成を有効または無効にします。IDP が利用可能で有効になっている必要があります。そうでない場合、ユーザーは SSO (シングルサインオン) オプションを使ってサインインできません。NetBackup プライマリサーバーに複数の IDP 構成を追加することもできますが、一度に 1 つの IDP 構成のみを有効にできます。

- *Master Server* は、IDP 構成を追加または変更するプライマリサーバーのホスト名または IP アドレスです。コマンドを実行する NetBackup プライマリサーバーがデフォルトで選択されます。

IDP 構成の無効化

製品環境で IDP 構成が無効化されている場合、ユーザーがサインインするときにその IDP の SSO (シングルサインオン) オプションを使用できません。

IDP 構成を無効化するには

1. プライマリサーバーに root または管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -uc -n IDP configuration name -e false
   ```

   IDP configuration name は、IDP 構成に指定された一意の名前です。

IDP 構成の削除

IDP 構成が削除された場合、ユーザーがサインインするときにその IDP の SSO (シングルサインオン) オプションを使用できません。

IDP 構成を削除するには

1. プライマリサーバーに root または管理者としてログオンします。
2. 次のコマンドを実行します。

   ```
   nbidpcmd -dc -n IDP configuration name
   ```

   IDP configuration name は、IDP 構成に指定された一意の名前です。

14

NetBackup アクセス制御セキュリティ (NBAC)

この章では以下の項目について説明しています。

NetBackup アクセス制御 (NBAC) の使用について

NetBackup アクセス制御 (NBAC) は、NetBackup 向けの従来のアクセス制御方法であるため、更新されなくなりました。Web UI では、役割に基づくアクセス制御 (RBAC) を使用することをお勧めします。

NetBackup アクセス制御 (NBAC) は、プライマリサーバー、メディアサーバー、クライアントに対して使われる、役割に基づくアクセス制御です。NBAC は、次のことが必要な場合に使うことができます。

- 1 つのアプリケーションに対して複数レベルの管理者権限を使う場合。バックアップアプリケーションには、オペレータ (テープをロードおよびアンロード) を指定できます。ローカル管理者 (単一の施設内でアプリケーションを管理) も指定できます。さらに、複数のサイトの責任を負う全体的な管理者を指定し、バックアップポリシーを決定することもできます。この機能はユーザーエラーの防止にもきわめて有効です。経験の浅い管理者に対して特定の操作を制限することにより、不慮の操作ミスが防止されます。
- システム管理にシステムの root 権限が必須とならないように管理者を分離する場合。システムの管理者とアプリケーションの管理者を分離することができます。

次の表は NBAC の注意事項をリストしたものです。

表 14-1 NBAC の注意事項

注意事項または問題	説明または解決
NBAC を構成する前の前提条件	ここでは、NBAC の構成を開始する前に準備しておくと役立つ前提条件を示します。これらの項目によりインストールが簡単になります。このインストールで使う情報は次のリストのとおりです。 ■ プライマリサーバーのユーザー名またはパスワード (root 権限または管理者権限)。 ■ プライマリサーバーの名前 ■ プライマリサーバーに接続されるすべてのメディアサーバーの名前 ■ バックアップされるすべてのクライアントの名前 ■ ホスト名または IP アドレス **メモ:** ホスト名は有効な IP アドレスに解決可能であることが必要です。 ■ `ping` または `traceroute` コマンド (ホストに接続可能であることを確認するためのツールの 1 つとして使用)。これらのコマンドを使うことで、ファイアウォールやアクセスを遮断するための他の防御手段を構成していないことが確認できます。

注意事項または問題	説明または解決
プライマリサーバー、メディアサーバー、クライアントのアップグレードが必要かどうかについての判断	プライマリサーバー、メディアサーバー、クライアントのアップグレードが必要かどうかについては、次に基づいて判断します。 ■ プライマリサーバー、メディアサーバー、クライアントのアップグレードによって提供される機能がそれぞれあります。 ■ NetBackup は、上位リビジョンのプライマリサーバーおよび下位リビジョンのクライアントとメディアサーバーと連携して動作します。 ■ 機能の内容により配置される内容が決定されます。 ■ 配置は必要に応じて段階的に実行できます。
役割に関する情報	構成において役割を次のように決定します。 ■ ホストの管理者 (プライマリサーバーの root 権限は主席管理者と同等)。 ■ 開始時の役割を決定した後、必要に応じて役割を追加します。
NBAC のライセンスの要件	アクセス制御を有効にする際にライセンスは必要ありません。
NBAC と KMS の権限	通常 NBAC を使って Setupmaster コマンドを実行するとき、NetBackup 関連グループの権限 (たとえば、NBU_Admin と KMS_Admin) が作成されます。デフォルトの root と管理者ユーザーもそれらのグループに追加されます。場合によっては NetBackup がアップグレードされるときに、root と管理者レベルのユーザーが KMS グループに追加されないことがあります。解決するには、root と管理者レベルのユーザーに NBU_Admin と KMS_Admin の権限を手動で付与します。
PBX からの共有セキュリティサービスを解除する間に表示される Windows Server Failover Clustering (WSFC) のエラーメッセージ	WSFC 環境で bpnbaz -UnhookSharedSecSvcsWithPBX <virtualhostname>コマンドを実行することにより、エラーメッセージをトリガできます。ただし共有の認証と認可サービスは、PBX から正常に解除され、エラーは無視できます。
表示される可能性のあるクラスタノードエラー	クラスタ環境で bpnbaz -setupmaster コマンドをローカル管理者として実行するとき、AUTHENTICATION_DOMAIN エントリには他のクラスタノードエントリが含まれない場合があります。そのような場合、これらのエントリはホストプロパティから bp.conf ファイルに手動で追加される必要があります。
カタログリカバリは、NBAC が REQUIRED モードに設定されているとき失敗します	NetBackup は、NBAC が REQUIRED モードに設定されている場合、カタログリカバリをサポートしません。 カタログリカバリを実行するには、最初にプライマリサーバーとすべてのメディアサーバーの NBAC 設定が PROHIBITED または AUTOMATIC に構成されていることを確認する必要があります。

注意事項または問題	説明または解決
ポリシーの検証は NBAC モードでは失敗します (つまり USE_VXSS = REQUIRED の場合)	次のいずれかが実行された場合、NBAC 有効化モードでのスナップショットポリシーのバックアップ、リストア、検証は失敗する場合があります。 ■ 認証済みの原理は NBAC グループから削除されます。NBU_Users グループ ■ NBU_User グループのバックアップとリストアの権限は削除されました
bpnbaz -setupmaster コマンドはエラー「認可サービスに接続できません。」で失敗します	管理者以外のユーザーが NetBackup のセキュリティを変更しようとした場合には bpnbaz –setupmaster が失敗します。 管理者グループの一員である「管理者」ユーザーのみに NetBackup のセキュリティを修正したり NBAC を有効にする権限があります。
インストール中の認証ブローカー構成の失敗	システムの無効なドメイン名構成により認証ブローカーの構成中に失敗します。 この問題を修正するには、`bpnbaz -configureauth` コマンドを使って認証ブローカーを構成します。 `bpnbaz` 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。
以前に拡張監査が有効になっていたシステムで NBAC が有効になっていると、NetBackup の GUI エラーが発生する可能性があります。	NetBackup サーバーを拡張監査から NBAC に切り替えるときは、次のディレクトリでユーザーの名前が付いたすべてのディレクトリが削除されていることを確認してください。 Windows の場合: *`install_path`*`¥NetBackup¥logs¥user_ops` UNIX、Linux の場合: `/usr/openv/netbackup/logs/user_ops` 詳しくは、次のトピックを参照してください。 p.185 の「NBAC の問題のトラブルシューティング」を参照してください。

注意事項または問題	説明または解決
NBAC では、[ホスト名を逆引き参照 (Reverse Hostname Lookup)]オプションを[許可 (Allowed)]に設定する必要があります。	NBAC が正しく機能し、NBAC が有効なシステムとの通信を許可するには、プライマリサーバー、メディアサーバーおよびすべてのクライアントで次の操作を実行します。 ■ NetBackup 管理コンソールで、[ホストプロパティ (Host Properties)]、[ネットワーク設定 (Network Settings)]の順に移動します。 NetBackup Web UI で、[ホストプロパティ (Host Properties)]、[クライアントの編集 (Edit client)]、[ネットワーク設定 (Network settings)]の順に移動します。 ■ [ホスト名を逆引き参照 (Reverse Hostname Lookup)]オプションが[許可 (Allowed)]に設定されていることを確認します。

NetBackup のアクセス管理

NetBackup へのアクセス権は、ユーザーグループを定義して、そのグループに権限を明示的に付与することによって制御できます。ユーザーグループを構成し、権限を割り当てることができます。NetBackup 管理コンソールの[アクセス管理 (Access Management)]を選択します。

メモ: NetBackup 管理コンソールが機能するには、ユーザーがシステムにリモートでログオンする権限を所有している必要があります。

メモ: アクセス制御が構成されていないメディアサーバーは、ルート以外のユーザーまたは管理者以外のユーザーが管理することはできません。

NBAC (NetBackup アクセス制御) 構成について

メモ: NBAC は NetBackup のインストールの一部としてすでにインストールされています。NBAC の構成のみこのリリースに必要になります。

NBAC の構成手順は、非 HA 環境の NBAC 構成向けです。NetBackup は、Linux、Solaris、Windows の環境における広範な HA 環境をサポートします。NBAC の構成は次のとおりです。

- 必要に応じて、プライマリサーバーのクラスタを構築します。HA 情報については、レプリケーションとディザスタリカバリに関する『NetBackup 高可用性の環境管理者ガイド』を参照してください。クラスタに関する情報は、『NetBackup プライマリサーバーのクラスタ化管理者ガイド』を参照してください。

- 提供される手順を使用して操作に関する NBAC を構成します。
  p.170 の「NetBackup アクセス制御 (NBAC) の構成」を参照してください。

NetBackup アクセス制御 (NBAC) の構成

メモ: 認証クライアントおよび認可クライアントの手動インストールは、古いメディアサーバーとクライアントホストの場合に実行する必要があります。NetBackup には、認証クライアントと認可クライアントが組み込まれています。認証サーバーと認可サーバーはメディアサーバーとクライアントに必要ありません。

NBAC の構成手順については、次の手順を参照してください。

NetBackup アクセス制御 (NBAC) の構成

1 プライマリサーバーで NetBackup アクセス制御 (NBAC) を構成します。

p.171 の「スタンドアロンのプライマリサーバーでの NetBackup アクセス制御 (NBAC) の構成」を参照してください。

メモ: プライマリサーバーは、スタンドアロンモードまたはクラスタでの高可用性構成としてインストールできます。

2 メディアサーバーで NBAC を構成します。

p.174 の「メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成」を参照してください。

3 クライアントで NBAC を構成します。

p.176 の「クライアントでのアクセス制御のインストールおよび構成」を参照してください。

NBAC の構成の概要

この項では、bpnbaz コマンドを使って NetBackup アクセス制御 (NBAC) を構成する場合の推奨事項について説明します。このコマンドは、*install_path*/bin/admincmd ディレクトリで利用可能です。

bpnbaz ユーティリティは、プライマリサーバー、メディアサーバーおよびクライアントで NBAC を構成するために必要になります。このツールは、すべての下位リビジョンのメディアサーバーやクライアントのホストの NBAC も構成します。サービスを構成した後は、サーバーとクライアントのそれぞれにおいてサービスを再起動する必要があります。これらのコマンドの使用例や、推奨される使用方法について詳しくは、次の項を参照してください。

p.176 の「NBAC の構成コマンドの概略」を参照してください。

構成はプライマリサーバーから実行されるため、プライマリサーバー、メディアサーバー、およびクライアントの間で通信リンクが確実に動作することが必要です。前提条件を確認して、関連するすべてのメディアサーバー、クライアント、およびこれらと通信する際のアドレスをメモしてください。

p.166 の「NetBackup アクセス制御 (NBAC) の使用について」を参照してください。

トラブルシューティングの初期段階において便利な OS コマンドと NetBackup コマンドがあります。OS コマンドは `ping`、`traceroute`、`telnet` です。NetBackup コマンドは `bpclntcmd` です。これらのコマンドは、ホストが相互に通信可能であることを確認するために使用します。トラブルシューティングの情報については、次の項を参照してください。

p.187 の「NetBackup Authentication and Authorization の構成とトラブルシューティングのヒント」を参照してください。

スタンドアロンのプライマリサーバーでの NetBackup アクセス制御 (NBAC) の構成

次の手順では、単一のコンピュータにインストールされているプライマリサーバーで NetBackup アクセス制御 (NBAC) を構成する方法について記述します。プライマリサーバーには、認証サーバーおよび認可サーバーが必要です。

次の表に、NBAC 構成例のホスト名を示します。

表 14-2　　ホスト名の例

ホスト名	Windows の場合	UNIX の場合
プライマリサーバー	win_primary	unix_primary
メディアサーバー	win_media	unix_media
クライアント	win_client	unix_client

次の手順では、スタンドアロンのプライマリサーバーでの NBAC の構成方法について説明します。

メモ: プライマリサーバーで `-setupmaster` を使用して `USE_VXSS = AUTOMATIC` を設定します。`USE_VXSS = REQUIRED` がプライマリサーバーで設定されている場合にメディアサーバーで NBAC を構成しようとすると、NetBackup プライマリサーバーが `REQUIRED` モードで構成されていることを示すエラーが発生することがあります。モードを `AUTOMATIC` に変更してメディアサーバーの構成を完了してください。

スタンドアロンのプライマリサーバーでの NBAC の構成

1. すべての NetBackup プライマリサーバーのインストールまたはアップグレードを実行します。
2. `bpnbaz -setupmaster` コマンドを実行します。

   「y」を入力します。システムは構成情報を集め始めます。それから、システムは認可情報を設定し始めます。
3. `bpnbaz -setupmaster` コマンドが正常に終了したら、このコンピュータの NetBackup サービスを再起動します。
4. メディアサーバーの設定に進みます。p.174 の「メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成」を参照してください。

クラスタでの高可用性の NetBackup プライマリサーバーのインストール

クラスタで高可用性の NetBackup プライマリサーバーをインストールするには次の手順を使用できます。

NetBackup のインストールとクラスタ化

1. NetBackup プライマリサーバーをインストールするクラスタシステムを構成します。
2. クラスタのすべてのノードに NetBackup プライマリサーバーをインストールします。
3. NetBackup プライマリサーバーをクラスタ化します。

   レプリケーションとディザスタリカバリに関する HA の情報は、『NetBackup 高可用性の環境管理者ガイド』で説明されています。

   クラスタに関する情報は、『NetBackup プライマリサーバーのクラスタ化管理者ガイド』を参照してください。
4. NBAC を有効化せずに NetBackup ドメイン内で動作することを確認するために、テストバックアップを実行します。

クラスタ化されたプライマリサーバーでの NetBackup アクセス制御 (NBAC) の構成

メモ: Windows のクラスタ環境では、プライマリサーバーの設定後に、パッシブノードの AUTHENTICATION_DOMAIN エントリがアクティブノードの名前と同じである場合があります。これは許容されません。パッシブノードでのフェールオーバー後、MFC UI が (<[local machine name] > ¥[Administrator user] を使って) 起動されると、認証関連のポップアップエラーメッセージが表示されます。この問題の回避策は、プライマリサーバーの設定の実行後 (フェールオーバーの前) に、パッシブノードの AUTHENTICATION_DOMAIN にローカルノード名を認証ドメインとして追加することです。AUTHENTICATION_DOMAIN の値を更新する前に、bpgetconfig コマンドを使って現在の値を取得します。それから bpsetconfig コマンドを使って既存のドメインリストに認証ドメインとしてローカルノード名を追加します。bpsetconfig コマンドプロンプトを終了して保存するには、Ctrl + Z を押し、Enter キーを押します。

メモ: クラスタのアクティブノードで NBAC モードを REQUIRED から PROHIBITED に戻すと、クラスタがエラー状態になることがあります。この問題の回避策は次の操作を実行することです。アクティブノードで bpclusterutil -disableSvc nbatd コマンドを実行し、次に bpclusterutil -disableSvc nbazd コマンドを実行します。bpsetconfig コマンドを使って bp.conf USE_VXSS=AUTOMATIC または REQUIRED の値を PROHIBITED に変更します。アクティブノードで bpclusterutil -enableSvc nbazd コマンド、その次に bpclusterutil -enableSvc nbatd コマンドを実行して、セキュリティサービスを監視するために NBAC を REQUIRED モードに変更します。

クラスタ化されたプライマリサーバーで NetBackup アクセス制御 (NBAC) を構成するには、次の手順を実行します。

クラスタ化されたプライマリサーバーでの NetBackup アクセス制御 (NBAC) の構成

1. プライマリクラスタノードにログオンします。
2. Windows を使用している場合は、コマンドコンソールを開きます。
3. UNIX の場合は、ディレクトリを /usr/openv/netbackup/bin/admincmd に変更します。Windows の場合、ディレクトリを *install_path*¥NetBackup¥bin¥admincmd に変更します。
4. アクティブノードで bpnbaz -setupmaster を実行します。
5. プライマリサーバーの管理コンソールにログオンします。
6. NBAC の設定を確実に有効にするために、NetBackup サービスを再起動してください。

メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成

次の手順では、NetBackup 構成内のメディアサーバーで NetBackup アクセス制御 (NBAC) を構成する方法について記述します。これらの手順は、プライマリサーバーと同じ場所に配置されていないメディアサーバーに必要です。

メモ: プライマリサーバーで `-setupmedia` を使用して `USE_VXSS = AUTOMATIC` を設定します。`USE_VXSS = REQUIRED` がプライマリサーバーで設定されている場合にメディアサーバーで NBAC を構成しようとすると、NetBackup プライマリサーバーが `REQUIRED` モードで構成されていることを示すエラーが発生することがあります。モードを `AUTOMATIC` に変更してメディアサーバーの構成を完了してください。

メディアサーバーでのアクセス制御の構成

1 プライマリサーバーコンピュータにログオンします。

2 bpnbat -login コマンドを実行します。

コマンドのエラーを防ぐため、必ず bpnbat -login コマンドを実行してから bpnbaz -setupmedia コマンドを実行してください。

bpnbaz -setupmedia コマンドには、いくつかのオプションがあります。

このコマンドは、個別のホストまたは -all オプションのいずれかの拡張が指定されていないと動作しません。

p.176 の「NBAC の構成コマンドの概略」を参照してください。

最初に -dryrun オプションを使用して、構成のドライランを実行をすることをお勧めします。このオプションは、-all および単一のサーバー構成の両方に使用できます。デフォルトでは、検出されたホストのリストは SetupMedia.nbac ファイルに書き込まれます。また、-out <output file> オプションを使用して、ユーザー独自の出力ファイル名を指定することもできます。ユーザー独自の出力ファイルを使う場合、-file オプションを使って、このファイルを以降の実行に渡す必要があります。ドライランコマンドは、次のように指定します。

bpnbaz -SetupMedia -all -dryrun [-out <outfile>] または

bpnbaz -SetupMedia <media.server.com> -dryrun [-out <outfile>]。

更新するメディアサーバーがすべてログファイルにある場合、-dryrun オプションを使用します。-all コマンドを使うことにより、それらすべてを一度に実行することができます。たとえば、次のように使用できます。

bpnbaz -SetupMedia -all または

bpnbaz -SetupMedia -file <progress file>。

-all オプションを使う場合、検出されたすべてのメディアサーバーがコマンドを実行するたびに更新される点に注意してください。選択したメディアサーバーのセットに対してコマンドを実行することもできます。構成するメディアサーバーのホスト名のみをファイルに保持し、-file オプションを使用してそのファイルを渡します。この入力ファイルは、SetupMedia.nbac、または前述のドライランの際に -out オプションで与えたカスタムファイル名になります。たとえば、次のように指定できます。- bpnbaz -SetupMedia -file SetupMedia.nbac。

単一のメディアサーバーを構成する場合には、メディアサーバーのホスト名をオプションとして指定します。たとえば、以下を使用します。

bpnbaz -SetupMedia <media.server.com>。

3 コマンドが正常に終了したら、ターゲットのメディアサーバーの NetBackup サービスを再起動します。

これより、ターゲットホストで NBAC が設定されます。特定のターゲットホストの構成が完了しなかった場合には、出力ファイルを確認してください。

この手順の後、クライアントホストのアクセス制御の構成に進みます。

p.176 の「クライアントでのアクセス制御のインストールおよび構成」を参照してください。

クライアントでのアクセス制御のインストールおよび構成

次の手順では、インストールと設定のクライアントで NetBackup アクセス制御 NetBackup 構成について説明します。クライアントでは、認証クライアント ソフトウェアが必要です。

インストールおよびクライアントでのアクセス制御を構成するには、次の手順を使用します。

1 バックアップが現在実行されていないことを確認します。

2 クライアントのバックアップを設定するには、マスター サーバーで次のコマンドを実行します。

```
bpnbaz -setupClient
```

NetBackup ホットカタログバックアップへの認証データベースおよび認可データベースの追加について

オンラインホットカタログバックアップ方式を使用する NetBackup 環境の場合、NetBackup の認証データベースおよび認可データベースをカタログバックアップに含めるために追加の構成を行う必要はありません。

NBAC の構成コマンドの概略

次の表に、NBAC のクイック構成手順で使用されるコマンドの概略を示します。

コマンドの使用方法の説明では、次の表記規則を使用します。

角カッコ [ ] の中のコマンドラインの要素は、必要に応じて指定します。

垂直バーまたはパイプ (|) は、選択可能な引数の区切りを示します。たとえば、コマンドの形式が `command arg1|arg2` の場合、変数 `arg1` または `arg2` を選択できます。

表 14-3 NBAC の構成コマンドの概略

コマンド	説明
bpnbaz -GetConfiguredHosts [target.server.com [-out file] | -all [-outfile] | -file progress.file]	bpnbaz -GetConfiguredHosts コマンドは、ホストの NBAC 状態を取得するために使われます。このコマンドには、-all または target.server.com オプションが必要です。 構文は次のとおりです。 ■ *target.server.com* は、1 台のターゲットホストの名前です。たとえば、1 台のホストの NBAC 状態を確認する場合にこのオプションを使用します。 ■ -out オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は SetupMedia.nbac ファイルに書き込まれます。このオプションは、-all および単一のホスト構成オプションに使用できます。 ■ -all オプションを指定すると、すべてのポリシーが調べられ、一意のホスト名がすべて収集されます。これらのホスト名は、ポリシー内で調べられます。さらに、構成済みのメディアサーバーがすべて収集され、各ホストの NBAC 状態が ConfiguredHosts.nbac ファイルに取得されます。 ■ -file progress.file は、progress_file から読み取るホスト名を指定する場合に使われるオプションです。このオプションは、progress_file の 1 行ごとにホスト名が 1 つ記述されていることを想定しています。この CLI により、progress_file の NBAC の状態が更新されます。hostname の後に # が付加され、その後に NBAC の状態が続きます。 ■ target.server.com または -all オプションと併用する場合、ホストの状態は ConfiguredHosts.nbac ファイルに取得されます。

コマンド	説明
`bpnbaz -SetupMaster [-fsa [<domain type>:<domain name>:]<user name>]`	`bpnbaz -SetupMaster` コマンドは、NBAC を使用するためのプライマリサーバーを設定するために実行します。認可サーバーと認証ブローカーは、プライマリサーバーにインストールして実行するように想定されています。 NBU 管理者として特定の OS ユーザーをプロビジョニングするには、最初のセキュリティ管理者オプションを指定して `bpnbaz -SetupMaster -fsa` コマンドを使います。 構文は次のとおりです。 ■ `-fsa` オプションは、NBU 管理者として特定の OS ユーザーをプロビジョニングするために使われます。このオプションを使用するときに、現在の OS のユーザー識別情報に対するパスワードの入力が求められます。 ■ *domain type* は、使用しているネットワークドメインの種類です。たとえば、`bpnbaz -SetupMaster -fsa nt:ENTERPRISE:jdoe` コマンドは、NBU 管理者として Windows のエンタープライズドメインユーザー `jdoe` をプロビジョニングします。 ■ *domain name* は、使用している特定のドメインの名前です。たとえば、`bpnbaz -SetupMaster -fsa jdoe` コマンドは、現在のログオンユーザーのドメイン形式 (Windows/UNIXPWD)、ドメイン名を取得し、そのドメインの `jdoe` ユーザーをプロビジョニングします。 ■ *user name* は NBU 管理者として指定している特定の OS ユーザー名です。 **メモ:** ユーザーは、指定済みのドメインに存在するか検証されます。ログオンしている管理者または root を NBU 管理者としてプロビジョニングする既存の動作は保持されます。

コマンド	説明
`bpnbaz -SetupMedia [ media.server.com [-out file] | -all [-out file] | -file progress.file ] [-dryrun] [-disable]`	`bpnbaz -SetupMedia` コマンドは、NBU_Administrator グループのメンバーがプライマリサーバー上で実行します。このコマンドは、`bpnbaz -SetupMaster` が正常に終了するまで実行しないでください。プライマリサーバーとターゲットメディアサーバーシステム間の接続を想定します。このコマンドには、`-all` または `target.server.com` オプションが必要です。 構文は次のとおりです。 ■ *media.server.com* は単一のターゲットホストの名前です。NBAC で使用する単一の追加ホストを追加するにはこのオプションを使用します。 ■ `-out` オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は `SetupMedia.nbac` ファイルに書き込まれます。このオプションは、`-all` および単一のホスト構成オプションに使用できます。 ■ `-all` を指定すると、すべてのストレージユニットが調べられ、ストレージユニットで見つかった一意のホスト名がすべて収集されます。これらは、ソートした順序で試行できます。結果は進捗ファイルに書き込まれます。 ■ `-file` *`progress_file`* オプションは、一連のメディアサーバーホスト名を持つ入力ファイルを指定する場合に使用します。実行後、各メディアサーバーの状態は進捗ファイルで更新されます。正常に完了したホストは、以降の実行ではコメントアウトされます。このコマンドは、入力ファイルのすべてのメディアサーバーが正常に構成されるまで繰り返すことができます。 ■ `-dryrun` はメディアサーバー名のリストを生成し、ログに書き込むことができます。このオプションは media.server.com で機能しますが、`-all` オプションとともに使用することを目的にしています。 ■ `-disable` オプションは、ターゲットホストの NBAC を無効化 (USE_VXSS = PROHIBITED) できます。

コマンド	説明
`bpnbaz -SetupClient [ client.server.com [-out file] | -all [-images] [-out file] | -file progress.file ] [-dryrun] [-disable]`	`bpnbaz -SetupClient` コマンドは、クライアントの NBAC を設定するために使われます。このコマンドは、`bpnbaz -SetupMaster` コマンドが正常に終了するまで実行しないでください。`bpnbaz -SetupClient` は、プライマリサーバーから実行する必要があります。このコマンドは、プライマリサーバーとターゲットクライアントシステムが接続されていることを想定しています。このコマンドには、`-all` または `target.server.com` オプションが必要です。 構文は次のとおりです。 ■ *client.server.com* は、1 台のターゲットホストの名前です。たとえば、NBAC で使用するホストを 1 台追加する場合に、この名前が選択肢となります。 ■ `-out` オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は `SetupClient.nbac` ファイルに書き込まれます。このオプションは、`-all` および単一のホスト構成オプションに使用できます。`-out` オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は `SetupClient.nbac` ファイルに書き込まれます。このオプションは、`-all` および単一のホスト構成オプションに使用できます。 ■ `-all` オプションを指定すると、すべてのポリシーが調べられ、ポリシー内で見つかった一意のホスト名がすべて収集されます。ポリシーは、ソートした順序で試行されます。結果は進捗ファイルに書き込まれます。 ■ `-images` オプションを指定すると、一意のホスト名のイメージがすべて検索されます。大規模なカタログが存在する場合には、-dryrun オプションを追加しないかぎり、このオプションは推奨できません。このオプションは、イメージカタログ内に含まれるすべての一意のクライアントに対応します。古いカタログには、膨大な数の廃止されたホストや、新しいプライマリに移動されたホスト、名前が変更されたホストが含まれる可能性があります。到達不能なホストへの接続が試行される場合、コマンドの実行時間が長くなる可能性があります。 ■ `-dryrun` は、クライアント名のリストを生成し、それらをログに書き込むオプションです。この場合、ターゲットシステムの実際の構成は実行されません。 ■ `-disable` は、ターゲットホストの NBAC を無効化 (USE_VXSS = PROHIBITED) するオプションです。 ■ `-file progress.file` は、進捗ログに異なるファイル名を指定する場合に使われるオプションです。この CLI により、progress_file からホスト名が読み取られます。状態は、各ホスト名の横に [# separated value] とともに追加されます。正常に完了したホストは、コメントアウトされます。このコマンドは、`progress_file` のすべてのクライアントが正常に構成されるまで複数回実行することができます。

NetBackup 管理インフラストラクチャと setuptrust コマンドの統合

Veritas 製品管理サーバーは、1 つの製品の管理者が別の製品を管理するための権限を持つように通信する必要があります。この通信により、1 つの管理サーバーのアプリケー

ション処理が別のサーバーと連携して動作することが保証されます。通信を保証するための 1 つの方法は、ルートブローカーと呼ばれる共通の独立したセキュリティサーバーを使うことです。すべての管理サーバーが共通のルートブローカーを指す場合、各サーバーの権限は共通の証明書に基づきます。通信を保証するためのもう 1 つの方法は、setuptrust コマンドを使うことです。このコマンドは、2 つの管理サーバー間で信頼を確立するために使われます。このコマンドは、別の管理サーバーを信頼する必要がある管理サーバーから発行されます。セキュリティ情報は、そのホストから、信頼の確立を要求しているホストに転送されます。一方向の信頼が確立されます。双方向 (相互) の信頼の設定は、これら 2 つのサーバーのそれぞれが setuptrust コマンドを発行することにより実行されます。

setuptrust 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』で説明しています。p.181 の「setuptrust コマンドの使用」を参照してください。

setuptrust コマンドの使用

setuptrust コマンドは、信頼するブローカーに連絡し、その証明書や詳細を回線を介して取得して、提供された詳細が信頼できる場合に信頼のリポジトリに追加するために使用できます。セキュリティ管理者は、root 証明書を配布するための次のセキュリティレベルの 1 つを構成できます。

- 高セキュリティ(2): 以前に信頼できないルートがピアから取得されている (つまり、同じシグネチャの証明書がこちらのトラストストアに存在しない) 場合、ユーザーはハッシュを検証するように求められます。
- 中セキュリティ(1): 確認を求めずに、最初の認証ブローカーが信頼されます。以降の認証ブローカーを信頼しようとすると、ユーザーは、証明書が信頼済みストアに追加される前に、ハッシュを検証するように求められます。
- 低セキュリティ(0): 確認を求めずに、認証ブローカーの証明書は常に信頼されます。vssat CLI が認証サービスの 'bin' ディレクトリにあります。

setuptrust コマンドでは、次の構文を使います。

```
vssat setuptrust --broker <host[:port]> --securitylevel high [-F]
```

setuptrust コマンドでは、次の引数を使います。

重要な引数は、broker、host、port です。信頼するブローカーのホストとポートを指定します。認証の登録ポートは 2821 です。ブローカーが別のポート番号で構成されている場合は、詳細についてセキュリティ管理者にお問い合わせください。

FIPS モードで vssat コマンドを実行するには、-F (--enable_fips) オプションを使用します。デフォルトでは、FIPS モードは無効になっています。

プライマリおよびメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティの構成

プライマリサーバーまたはメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを構成するには、[NetBackup の管理 (NetBackup Management)]、[ホストプロパティ (Host Properties)]、[マスターサーバー (Master Servers)]*または*[メディアサーバー (Media Servers)]、[*server name*]、[アクセス制御 (Access Control)]の順に展開します。

[必須 (Required)]か[自動 (Automatic)]に[NetBackup Product Authentication and Authorization]を設定します。[自動 (Automatic)]は、NBAC がまだ構成されていないホストが構成内に存在する場合を考慮した設定です。他の NetBackup システムとの通信時に、使用可能な接続のうちで最もセキュリティ保護された接続の使用が、サーバーによって試行されます。[自動 (Automatic)]設定は、すべてのクライアントおよびサーバーで NBAC が構成されるまで使用する必要があります。

[自動 (Automatic)]を選択した場合、NetBackup Product Authentication and Authorization を使うために必要なコンピュータかドメインを指定できます。そうしない場合は、NetBackup Product Authentication and Authorization の使用が禁止されているコンピュータを指定できます。

[認証ドメイン (Authentication Domain)]タブ

[認証ドメイン (Authentication Domain)]タブは、次の構成を行うために使用します。

- どの認証サーバーでどの認証機構がサポートされているか
- 各ドメインで何をサポートしているか

認証するユーザーのドメインを追加します。

次の例は 6 つの認証ドメインを含んでいます。

メモ: UNIX の認証ドメインを使用する場合は、認証を行ったホストの完全修飾ドメイン名を入力します。

メモ: サポートされる認証形式は、NIS、NISPLUS、WINDOWS、vx、unixpwd です (デフォルトは unixpwd です)。

[認可サービス (Authorization Service)]タブ

メモ: このタブからは変更できません。このタブは読み取り専用です。

[アクセス制御 (Access Control)]ホストプロパティの[認可サービス (Authorization Service)]タブで、ホスト名を参照できます。この情報はすべて読み取り専用であるためグレー表示です。この画面への変更を行うことはできません。

[ネットワーク属性 (Network Attributes)]タブ

[ネットワーク属性 (Network Attributes)]タブの[アクセス制御 (Access Control)]ホストプロパティを表示します。[ネットワーク (Networks)]リストにプライマリサーバーを追加します。それから、[NetBackup Product Authentication and Authorization] を[必須 (Required)]に設定します。

NetBackup プライマリサーバーに追加した新しい NetBackup クライアントまたはメディアサーバーごとに、[アクセス制御 (Access Control)]プロパティを構成する必要があります。これらのプロパティは、それ自体とプライマリの両方で構成されます。この設定は、プライマリサーバーのホストプロパティで実行できます。

クライアントの[アクセス制御 (Access Control)]ホストプロパティダイアログボックス

ホストプロパティで NetBackup クライアントを選択します。(プライマリサーバーの NetBackup 管理コンソールで、[NetBackup の管理 (NetBackup Management)]、[ホストプロパティ (Host Properties)]、[クライアント (Clients)]を展開して*クライアントを選択*し、[アクセス制御 (Access Control)]を選択します。)

[必須 (Required)]か[自動 (Automatic)]に[NetBackup Product Authentication and Authorization]を設定します。この例では、[自動 (Automatic)]が選択されています。

クライアントの[認証ドメイン (Authentication Domain)]タブ

ホストプロパティで NetBackup クライアントを選択します。このタブを使用して、コンピュータごとに NetBackup Product Authentication and Authorization の使用を要求または禁止することができます。通信を行う両方のシステムで、設定が一致している必要があります。

[アクセス制御 (Access Control)]ホストプロパティの[認証ドメイン (Authentication Domain)]タブで、クライアントで認証に使用できるドメインのリストを追加します。[検索 (Find)]をクリックすると、利用可能な認証ドメインのリストを取得できます。それから、選択した認証ドメインのリストを作成するために[追加 (Add)]をクリックします。

クライアントの[ネットワーク属性 (Network Attributes)]タブ

[アクセス制御 (Access Control)]ホストプロパティの[ネットワーク属性 (Network Attributes)]タブで、クライアントで認証に使用できるネットワークのリストを追加します。

自動イメージレプリケーションでの NetBackup アクセス制御 (NBAC) の使用

自動イメージレプリケーションを 2 つのドメインで設定し、NetBackup アクセス制御 (NBAC) を使う場合は、ソースドメインとターゲットドメインの両方で使う必要があります。プライマリサーバーの構成は、USE_VXSS = REQUIRED または USE_VXSS = AUTOMATIC のいずれかである必要があります。(ただし設定は、ドメインのうち 1 つが REQUIRED、もう 1 つが AUTOMATIC でも構いません。

自動イメージレプリケーションは、プライマリサーバーの 1 つが NBAC を使用するように構成され、もう 1 つのプライマリサーバーでは NBAC が無効になっているプライマリサーバードメイン間ではサポートされません。つまり、1 つのプライマリサーバーの構成が USE_VXSS = AUTOMATIC または USE_VXSS = REQUIRED であり、もう 1 つのプライマリサーバーで USE_VXSS = PROHIBITED (無効) である場合です。

NBAC がプライマリサーバードメインで使用される場合、次の構成が必要です。

- ソースプライマリサーバードメイン:
  管理者は、操作用の構成を始める前に、ターゲットプライマリサーバーがアクセス権を正しく設定しているかを確かめる必要があります。
- ターゲットプライマリサーバードメイン:
  ターゲットドメインのセキュリティ管理者は、ソースドメインの管理者に正しい権限セットを与える必要があります。ソースドメイン管理者には、HostProperties、DiskPool、DevHost の各オブジェクトで参照、読み込み、設定の権限が必要です。
  ソースドメイン管理者は、3 つすべてのアクセス権を持つ既存のグループにメンバーとして追加することができます。

たとえば、次の例を考えてみます。

それぞれがプライマリサーバーを含む 2 つの NBAC ドメインの場合:

- レプリケーションソース NBAC ドメイン: *DomainA* は *Master-A* を含む
- レプリケーションターゲット NBAC ドメイン: *DomainB* は *Master-B* を含む

NBAC は両方のドメインで有効です。(NBAC が 1 つのドメインで使われる場合、もう一方のドメインでも使う必要があります。)

UserA が *Master-B* をターゲットとして自動イメージレプリケーション SLP を作成する場合、*UserA* は *Master-B* がそれを行うためのアクセス権を必要とします。

DomainB のセキュリティ管理者 (*UserB*) は、ユーザーグループ (たとえば *NB_InterDomainUsers*) を作成し、次の領域の参照、読み込み、設定権限を与える必要があります。

- HostProperties
- DiskPool

- DevHost

DomainB のセキュリティ管理者（*UserB*）は、*bpnbaz -AddUser* コマンドを使用して `DomainA¥UserA` に `bpnbaz -AddUser` を割り当てます。

アクセス管理のトラブルシューティング

アクセス管理のトラブルシューティングし、特定の処理および機能が正しく行われているかどうかを判断する方法

p.187 の「NetBackup Authentication and Authorization の構成とトラブルシューティングのヒント」を参照してください。

検証項目には次のものが含まれます。

- Windows での検証項目
  p.193 の「Windows での検証項目」を参照してください。
- UNIX での検証項目
  p.202 の「UNIX での検証項目」を参照してください。
- UNIX プライマリサーバーが存在する複合環境での検証項目
  p.210 の「UNIX プライマリサーバーが存在する複合環境での検証項目」を参照してください。
- Windows プライマリサーバーが存在する複合環境での検証項目
  p.215 の「Windows プライマリサーバーが存在する複合環境での検証項目」を参照してください。

NBAC の問題のトラブルシューティング

次の表は NBAC に関連する問題とソリューションをリストしたものです。

表 14-4 NBAC の問題

問題と原因	解決方法
ユーザー主導のバックアップまたはリストアに失敗します ユーザー主導のバックアップまたはリストアに自動モードの NBAC で失敗します。バックアップ、アーカイブおよびリストアインターフェースは、NBAC が構成されている場合、Windows インターフェースに一部のエラーを表示します。 NBAC で UNIX プライマリサーバーで NetBackup の設定が行われ、最初にインターフェースを設定せずに Windows インターフェースでこのような設定を行う場合は、バックアップまたはリストアに失敗することがあります。その他の原因として、ホームディレクトリに期限切れの証明書があることが考えられます。	設定をサポートするために Windows インターフェースを構成してください。 Active Directory のドメインからユーザーを認証するには、認証ブローカーとして機能する Microsoft Windows システムが 1 つ以上存在する必要があります。 Windows インターフェースを構成し、Active Directory の既存ユーザーを活用して、主に UNIX/Linux プラットフォーム上の NetBackup 環境を管理、操作、または使用するための手順については、TECH199281 を参照してください。 設定を正しく構成した後、`bpnbat -logout` コマンドを実行し、インターフェースを再起動する前に設定からログアウトしてください。
認証エラーが 116 で発生しました (Authentication failure with error 116) ターゲットホストで NBAC を設定する際に、`error 116-VxSS authentication` で認証が失敗します。	NBAC 認証が正しく構成され、ターゲットホストの有効で使用可能なクレデンシャルがあることを確認してください。
NBU_Operator グループの非管理ユーザーがアクセス管理の使用を試みた際にエラーが発生しました (Error when a non-admin user from the NBU_Operator group tries to use Access Management) 非管理ユーザーが NBU_Operator グループに追加されました。読み込み、表示、構成権限は、ホストプロパティの構成権限と共に割り当てられます。ただし、ユーザーがアクセス管理ユーティリティを開こうとすると、エラーが表示されます。	NBU_Operator グループのユーザーの権限は制限されています。 ユーザーがアクセス管理ユーティリティを使用するには、異なる権限が必要です。必要な権限を取得するには、NBU_Security_Admin グループにユーザーを追加してください。 ユーザーグループについての詳細 p.226 の「NetBackup のデフォルトユーザーグループ」を参照してください。
認可ファイル (auth.conf) 機能は、NBAC 対応の環境では役に立ちません。デフォルトでは、auth.confファイルは非 NBAC 環境の Java インターフェースのみでサポートされます。	NBAC 対応環境で auth.conf ファイルを機能させるには、`nbgetconfig` コマンドと `nbsetconfig` コマンドを使用して `USE_AUTH_CONF_NBAC` エントリを Windows レジストリに追加するか、または bp.conf ファイルを UNIX に追加します。エントリは次のように `YES` に設定する必要があります。 `USE_AUTH_CONF_NBAC = YES` auth.conf ファイルについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

問題と原因	解決方法
NetBackup サーバーを拡張監査から NBAC に切り替えるときのエラー NetBackup 管理コンソールは、`netbackup/logs/user_ops` にディレクトリ名としてユーザー名を持つユーザーディレクトリを作成します。拡張監査では、これらのディレクトリはルート権限を使用して実行される NetBackup プロセスによって使用されます。NBAC では、これらのディレクトリはルート権限なしで実行される NetBackup プロセスによって使用されます。 次のような場合に NetBackup GUI エラーが発生することがあります。 ■ NBAC が有効になっているときに、拡張監査が有効だったときに作成されたユーザーディレクトリがまだ存在する ■ どのユーザーにもルート権限がない エラーの例: ■ バックアップ、アーカイブ、およびリストアのインターフェースで、[タスクの進捗 (Task Progress)]タブにジョブが表示されません。 ■ VMware VM リストアの場合、リカバリ前チェックでエラー 12 がレポートされます。	**1** ユーザーが GUI を使用してログオンする各 NetBackup サーバーで、次のディレクトリにあるユーザーディレクトリを削除します。 Windows の場合: *install_path*¥NetBackup¥logs¥user_ops UNIX、Linux の場合: /usr/openv/netbackup/logs/user_ops **2** ディレクトリを削除したら、NetBackup GUI を再起動します。

NetBackup Authentication and Authorization の構成とトラブルシューティングのヒント

次の表に、NetBackup Authentication and Authorization の構成とトラブルシューティングのヒントを示します。この表示には、いくつかの既知の問題についての情報とそれを解決するためのヒントも含んでいます。

表 14-5 NetBackup Authentication and Authorization の構成とトラブルシューティングのヒント

トピック	構成のヒント
プライマリサーバー設定の検証	bpnbat -whoami を実行し、コンピュータのクレデンシャルを指定すると、ホストが登録されているドメイン、および証明書に示されているコンピュータの名前が表示されます。 bpnbat -whoami -cf "*install_path*¥netbackup¥var¥vxss¥credentials¥ primary.company.com "Name: primary.company.com Domain: NBU_Machines@primary.company.com Issued by: /CN=broker/OU=root@primary.company.com/O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@primary.company.com でない場合、対象の名前 (primary) に対して bpnbat -addmachine を実行することを検討してください。NBU_Machines ドメインとして機能するコンピュータ (primary) でこのコマンドを実行します。 次に、クレデンシャルを配置するマシン上で、bpnbat -loginmachine コマンドを実行します。
ルートクレデンシャルの設定	認証サーバーまたは認可サーバーのいずれかの設定で問題が発生し、アプリケーションでユーザーのクレデンシャルが root であるとエラー表示された場合は、root に対して $HOME 環境変数が正しく設定されていることを確認します。 次のコマンドを実行して、現在の値を検出します。 echo $HOME この値は root のホームディレクトリと一致する必要があります。このディレクトリは、通常、/etc/passwdファイルに存在します。 root に切り替える場合は、次のコマンドを実行します。 su - この場合、su とだけ入力するのではなく、root 環境変数を正しく調整する必要があります。

トピック	構成のヒント
期限切れのクレデンシャルメッセージ	クレデンシャルが期限切れであるか、不正である場合、bpnbaz または bpnbat コマンドの実行時に、次のメッセージが表示されます。 `Supplied credential is expired or incorrect. Please reauthenticate and try again.` bpnbat -Login を実行して、期限切れのクレデンシャルを更新します。
有効なデバッグログ	次のログは、NetBackup アクセス制御のデバッグを行う場合に役立ちます。 プライマリ上: admin、bpcd、bprd、bpdbm、bpjobd、bpsched クライアント上: admin、bpcd アクセス制御: nbatd、nbazd。 正しいログ記録の説明については、『NetBackup トラブルシューティングガイド』を参照してください。
クレデンシャルの格納場所	NetBackup Authentication and Authorization のクレデンシャルは次のディレクトリに格納されます。 UNIX の場合: ユーザーのクレデンシャル: $HOME/.vxss コンピュータのクレデンシャル: /usr/openv/var/vxss/credentials/ Windows の場合: <user_home_dir>¥Application Data¥VERITAS¥VSS
システム時間がアクセス制御に与える影響	クレデンシャルには、作成時間と終了時間が含まれます。コンピュータ間でシステム時間が大きく異なっていると、クレデンシャルが未来に作成されたものと見なされたり、実際よりも早く期限切れと見なされます。システム間の通信で問題が発生した場合は、システム時間の同期化を検討してください。

トピック	構成のヒント

NetBackup Authentication and Authorization のポート	NetBackup Authentication and Authorization デーモンサービスは旧バージョンのメディアサーバーとクライアントにポート 13783 番と 13722 番を使います。これらのサービスでは PBX 接続が使用されます。
	次のコマンドで、プロセスが待機していることを確認できます。
	認証:
	UNIX の場合
	`netstat -an | grep 13783`
	Windows の場合
	`netstat -a -n | find "13783"`
	認可:
	UNIX の場合
	`netstat -an | grep 13722`
	Windows の場合
	`netstat -a -n | find "13722"`

共有サービスの NetBackup の認証および認可デーモンの停止	NetBackup Authentication and Authorization Service を停止する場合は、認可を最初に停止し、その後認証を停止します。
	UNIX の場合、次のコマンドを使用します。
	認可を停止する場合、次の例に示すように、TERM シグナルを送信します。
	`# ps -fed |grep nbazd`
	`root 17018 1 4 08:47:35 ? 0:01 ./nbazd`
	`root 17019 16011 0 08:47:39 pts/2 0:00 grep nbazd`
	`# kill 17018`
	認証を停止する場合、次の例に示すように、TERM シグナルを送信します。
	`# ps -fed |grep nbatd`
	`root 16018 1 4 08:47:35 ? 0:01 ./nbatd`
	`root 16019 16011 0 08:47:39 pts/2 0:00 grep nbatd`
	`# kill 16018`
	Windows の場合
	これらのサービスは NetBackup アクティビティモニターに表示されないため、Windows の[サービス]ユーティリティを使用します。

トピック	構成のヒント
NetBackup にアクセスできない場合	アクセス制御が正しく構成されていないと、NetBackup 管理コンソールにアクセスできない場合があります。 アクセスできない場合は、vi を使って bp.conf エントリを参照するか（UNIX）、または regedit を使って次の場所の Windows レジストリを参照します（Windows）。 HKEY_LOCAL_MACHINE¥SOFTWARE¥Veritas¥NetBackup¥CurrentVersion¥config AUTHORIZATION_SERVICE、AUTHENTICATION_DOMAIN および USE_VXSS エントリが正しく設定されているかどうかを確認します。 管理者は、NetBackup アクセス制御の使用を好まない場合や認可ライブラリをインストールしていないことがあります。USE_VXSS エントリが Prohibited に設定されているか完全に削除されていることを確認します。
メディアサーバーのストレージユニットのバックアップが NBAC 環境で実行されない	NetBackup ドメインのシステム (プライマリサーバー、メディアサーバー、またはクライアント) のホスト名と bp.conf ファイルで指定するホスト名は、同じである必要があります。
nbac_cron ユーティリティの使用	nbac_cron.exe ユーティリティを使用して、cron または at ジョブを実行する際の識別情報を作成します。 nbac_cron ユーティリティについての詳細 p.221 の「nbac_cron ユーティリティについて」を参照してください。 nbac_cron.exe は、次の場所に存在します。 UNIX の場合、/opt/openv/netbackup/bin/goodies/nbac_cron Windows の場合、 *install_path*¥netbackup¥bin¥goodies¥nbac_cron.exe nbac_cron ユーティリティの使用についての詳細 p.222 の「nbac_cron ユーティリティの使用」を参照してください。
Windows でのリカバリ後の NBAC の有効化	Windows でリカバリ後に手動で NBAC を有効にするには次の手順を使います。 ■ AUTHENTICATION_DOMAIN、AUTHORIZATION_SERVICE、USE_VXSS エントリをレジストリに追加します。 ■ NetBackup Authentication and Authorization サービスのサービスの種類を AUTOMATIC に変更します。 ■ NetBackup サービスを再起動します。 ■ nbatd および nbazd サービスが実行されていることを検証します。 **メモ:** クラスタで bpclusterutil -enableSvc nbatd および bpclusterutil -enable nbazd コマンドを実行します。

トピック	構成のヒント
クラスタインストールで setupmaster が失敗する	構成ファイルが共有ディスクにあるクラスタインストールの場合には setupmaster が失敗することがある既知の問題があります。
共有セキュリティサービス (vxatd または vxazd) がプライマリサーバーとともにクラスタ化されている場合のクラスタの既知の問題	共有セキュリティサービス (vxatd または vxazd) がプライマリサーバーとともにクラスタ化されている場合にクラスタに既知の問題があります。bpnbaz -SetupMaster コマンドを実行し、セキュリティ (NBAC) を設定するときに、該当する場合は共有セキュリティサービスのサービスグループを永続的にフリーズするか、サービスをオフラインにします (ただし、共有ディスクはオンラインであることを確認します)。その後、setupmaster コマンドを実行します。
bp.conf ファイル内のすべての AUTHENTICATION_DOMAIN エントリが認証ブローカーとしてプライマリサーバー仮想名で更新される、NBAC に関するクラスタ化されたプライマリサーバーアップグレードの既知の問題	bp.conf ファイル内のすべての AUTHENTICATION_DOMAIN エントリが認証ブローカーとしてプライマリサーバー仮想名で更新される、NBAC に関するクラスタ化されたプライマリサーバーアップグレードに既知の問題があります。プライマリサーバー以外の異なる認証ブローカーを示す任意のドメインエントリがある (また、プライマリサーバーはそのドメインをサービスしない) 場合は、そのエントリは手動で bp.conf ファイルから削除される必要があります。
アクセス制御エラーと短いホスト名および長いホスト名に関する既知の問題	アクセス制御に関するエラーを含む既知の問題があります。短いホスト名と長いホスト名を解決することができ、同じ IP アドレスに解決されるかを調べてください。
ブローカーのプロファイルで ClusterName が AT の仮想名に設定されている場合の NBAC に関するクラスタアップグレードの既知の問題	ブローカーのプロファイルで ClusterName が AT の仮想名に設定されている場合の NBAC に関するクラスタアップグレードの既知の問題があります。これは組み込みのブローカーにそのまま移行されます。組み込みのブローカーはプロファイルで UseClusterNameAsBrokerName が 1 に設定されています。ブローカーのドメインマップに要求が送られると、共有 AT の仮想名をブローカー名として使用します。bpnbaz -GetDomainInfosFromAuthBroker は何も戻しません。アップグレードでは、bp.conf ファイルが NetBackup 仮想名を持つように更新されます。
エラーが発生する可能性のある bpcd の複数インスタンスの既知の問題	bpnbaz -SetupMedia コマンドで、bprd が AT_LOGINMACHINE_RQST プロトコルを使用して宛先フィールドの bpcd と通信する既知の問題があります。bpcd の新しいインスタンスが起動されます。コマンドは、完了後に char アレイを通常のポインタとして解放することを試行し、bpcd によってクライアント側にコアダンプを発生させる場合があります。この bpcd インスタンスは一時的に作成されて正常に終了するため、機能は損なわれないはずです。親 bpcd には影響しません。
共有ドライブの構成ファイルと共有 AT を使用するクラスタに関する既知の問題	共有ドライブの構成ファイルと共有 AT を使用するクラスタに関する既知の問題があります。共有サービスの解除は、この共有ドライブがアクセス可能であるノードでのみ有効になります。解除は残りのノードでは失敗します。つまり、管理を行う bpnbaz -SetupMaster を実行している間は、リモートブローカーの個々の操作が失敗します。手動でパッシブノードを構成する必要があります。各パッシブノードで bpnbaz -SetupMedia を実行します。

トピック	構成のヒント
NBAZDB をサポートするデータベースユーティリティに関する既知の問題	あるデータベースユーティリティではサポートされ、他のデータベースユーティリティではサポートされない既知の問題があります。 次のデータベースユーティリティが NBAZDB をサポートします: nbdb_backup、nbdb_move、nbdb_ping、nbdb_restore、nbdb_unload、および nbdb_admin。 dbadm ユーティリティは NBAZDB をサポートしません。

Windows での検証項目

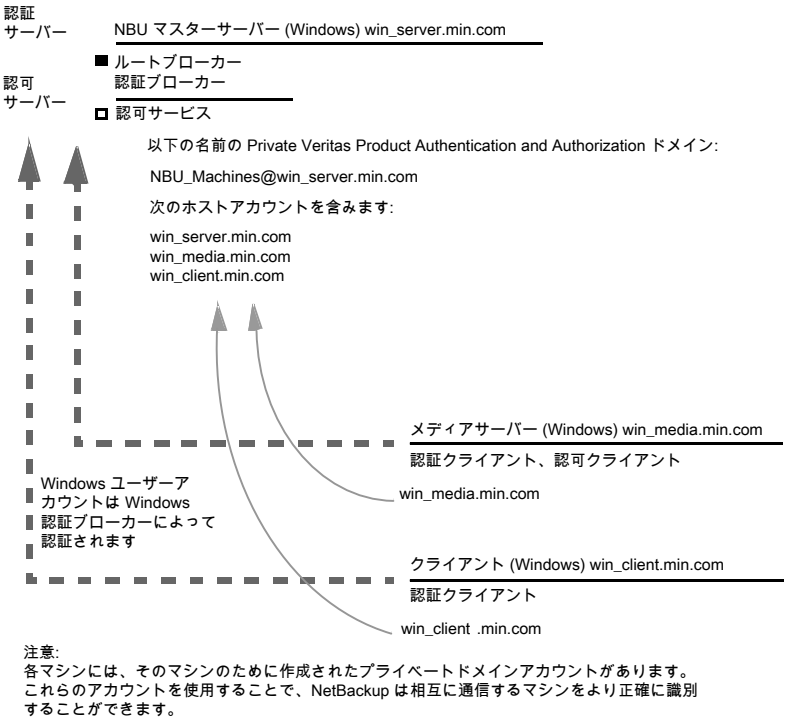
次の構成手順は、プライマリサーバー、メディアサーバーおよびクライアントでアクセス制御が正しく構成されていることを確認するのに役立ちます。

Windows での検証項目には次のものが含まれます。

- p.194 の「Windows プライマリサーバーでの検証項目」を参照してください。
- p.198 の「Windows メディアサーバーでの検証項目」を参照してください。
- p.200 の「Windows クライアントでの検証項目」を参照してください。

図 14-1 に、Windows システムだけが存在する構成の例を示します。

図 **14-1** Windows システムだけが存在する構成の例



Windows プライマリサーバーでの検証項目

この項では、次の手順について説明します。

- Windows プライマリサーバー設定を検証します。
- 認可の照合が許可されているコンピュータを検証します。
- データベースが正しく構成されていることを検証します。
- `nbatd` および `nbazd` プロセスが実行されていることを検証します。
- ホストプロパティが正しく構成されていることを検証します。

次の表に、Windows プライマリサーバーでの検証手順を示します。

表 14-6 Windows プライマリサーバーでの検証手順

手順	説明
Windows プライマリサーバー設定の検証	ホストが登録されているドメイン (プライマリ認証ブローカーが存在する場所) を判断できます。または、証明書に示されているコンピュータの名前を判別することもできます。に を指定して実行し、ホストのクレデンシャルファイルを指定します。bpnbat-whoami サーバークレデンシャルは、c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥...ディレクトリに存在します。 例: bpnbat -whoami -cf "c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_primary" Name: win_primary.company.com Domain: NBU_Machines@win_primary.company.com Issued by: /CN=broker/OU=root@win_primary.company.com/ O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@win_primary.company.com でない場合、対象の名前 (win_primary) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machinesドメインとして機能する認証ブローカーのコンピュータ (win_primary) で実行します。 次に、証明書を配置するコンピュータ (win_primary) 上で、次のコマンドを実行します。 bpnbat -loginmachine **メモ:** ユーザーのクレデンシャルの期限を判断する場合、有効期限がローカル時間ではなく GMT で表示されることに注意してください。 **メモ:** この検証の残りの手順では、コンソールウィンドウからコマンドを実行することを想定しています。また、そのウィンドウから、対象のユーザー識別情報で bpnbat -login が実行されていることを想定しています。このユーザーは、NBU_Security Admin のメンバーであると識別されます。この識別情報は、通常、セキュリティが設定された最初の識別情報です。

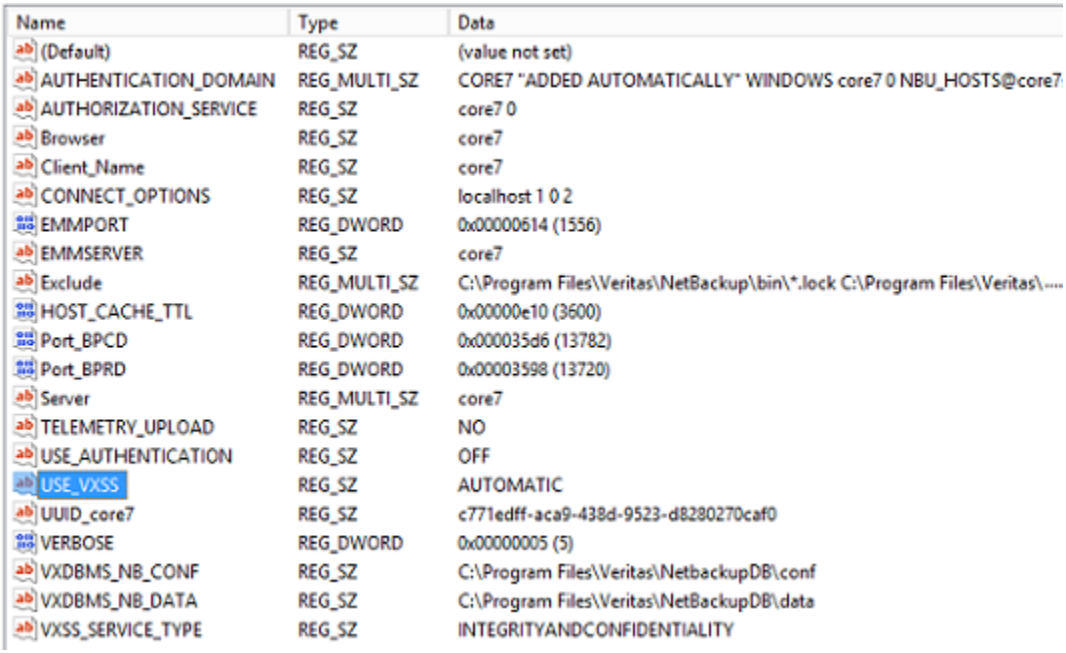
手順	説明
認証ブローカーに存在するコンピュータの検証	認証ブローカーに存在するコンピュータを検証するには、管理者グループのメンバーでログオンし、次のコマンドを実行します。 `bpnbat -ShowMachines` このコマンドを実行すると、`bpnbat -AddMachine` を実行したコンピュータが示されます。 **メモ:** ホストがリストに表示されない場合、プライマリから `bpnbat -AddMachine` を実行します。その後、対象のホストから `bpnbat -loginMachine` を実行します。

認可の照合が許可されているコンピュータの検証	認可の照合が許可されているコンピュータを検証するには、管理者グループのメンバーでログオンし、次のコマンドを実行します。
	
	`bpnbaz -ShowAuthorizers`
	
	このコマンドを実行すると、win_primary および win_media (プライマリサーバーおよびメディアサーバー) が認可を照合する権限を所有していることが示されます。両方のサーバーが、同じプライベートドメイン (ドメイン形式 vx)、NBU_Machines@win_primary.company.com に対して認証されていることに注意してください。
	
	メモ: このコマンドは、ローカル管理者または `root` ユーザーで実行します。ローカル管理者は、NBU_Security Admin ユーザーグループのメンバーである必要があります。
	
	`bpnbaz -ShowAuthorizers`
	` ==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@win_primary.company.com`
	`Name: win_primary.company.com`
	` ==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@win_primary.company.com`
	`Name: win_media.company.com`
	`Operation completed successfully.`
	
	認可済みコンピュータのリストにプライマリサーバーまたはメディアサーバーが表示されない場合、`bpnbaz -allowauthorization server_name` を実行して、表示されていないコンピュータを追加します。

手順	説明
データベースが正しく構成されていることの検証	データベースが正しく構成されていることを検証するには、bpnbaz -listgroups を実行します。 bpnbaz -listgroups NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully. グループが表示されない場合または bpnbaz -listmainobjects を実行してもデータが戻されない場合は、bpnbaz -SetupSecurity の実行が必要になる場合があります。
nbatd および nbazd プロセスが実行されていることの検証	Windows のタスクマネージャを使用して、指定したホスト上で nbatd.exe および nbazd.exe が実行されていることを確認します。必要に応じて、これらのプロセスを起動します。
ホストプロパティが正しく構成されていることの検証	[アクセス制御 (Access Control)]ホストプロパティで、[NetBackup Product Authentication and Authorization]プロパティが正しく設定されていることを検証します。この設定は、すべてのコンピュータが NetBackup Authentication and Authorization を使うかどうかによって[自動 (Automatic)]または[必須 (Required)]のいずれかにする必要があります。すべてのコンピュータで NetBackup Authentication and Authorization が使用されているわけではない場合は、[自動 (Automatic)]に設定します。 また、ホストプロパティは、次のレジストリで USE_VXSS を参照して確認することもできます。 HKEY_LOCAL_MACHINE¥SOFTWARE¥Veritas¥NetBackup¥CurrentVersion¥config. 図 14-2に、[認証 (Authentication)]ドメインタブのホストプロパティの設定例を示します。 [アクセス制御 (Access Control)]ホストプロパティで、表示された認証ドメインの綴りが正しいこと、およびドメインが適切なサーバー (有効な認証ブローカー) を示していることを確認します。すべてのドメインが Windows ベースである場合、ドメインは、認証ブローカーを実行している Windows コンピュータを示している必要があります。

次の図に、[認証 (Authentication)]ドメインタブのホストプロパティの設定を示します。

図 14-2 ホストプロパティの設定



Name	Type	Data
(Default)	REG_SZ	(value not set)
AUTHENTICATION_DOMAIN	REG_MULTI_SZ	CORE7 "ADDED AUTOMATICALLY" WINDOWS core7 0 NBU_HOSTS@core7
AUTHORIZATION_SERVICE	REG_SZ	core7 0
Browser	REG_SZ	core7
Client_Name	REG_SZ	core7
CONNECT_OPTIONS	REG_SZ	localhost 1 0 2
EMMPORT	REG_DWORD	0x00000614 (1556)
EMMSERVER	REG_SZ	core7
Exclude	REG_MULTI_SZ	C:\Program Files\Veritas\NetBackup\bin*.lock C:\Program Files\Veritas\...
HOST_CACHE_TTL	REG_DWORD	0x00000e10 (3600)
Port_BPCD	REG_DWORD	0x000035d6 (13782)
Port_BPRD	REG_DWORD	0x00003598 (13720)
Server	REG_MULTI_SZ	core7
TELEMETRY_UPLOAD	REG_SZ	NO
USE_AUTHENTICATION	REG_SZ	OFF
USE_VXSS	REG_SZ	AUTOMATIC
UUID_core7	REG_SZ	c771edff-aca9-438d-9523-d8280270caf0
VERBOSE	REG_DWORD	0x00000005 (5)
VXDBMS_NB_CONF	REG_SZ	C:\Program Files\Veritas\NetbackupDB\conf
VXDBMS_NB_DATA	REG_SZ	C:\Program Files\Veritas\NetBackupDB\data
VXSS_SERVICE_TYPE	REG_SZ	INTEGRITYANDCONFIDENTIALITY

Windows メディアサーバーでの検証項目

この項では、次の Windows メディアサーバーでの検証手順について説明します。

- メディアサーバーを検証します。
- サーバーが認可データベースにアクセスできることを検証します。
- ライブラリメッセージをロードできない場合

次の表に、Windows メディアサーバーでの検証手順を示します。

表 14-7 Windows メディアサーバーでの検証手順

手順	説明
メディアサーバーの検証	bpnbat -whoami にメディアサーバーのクレデンシャルファイルを指定する -cf を指定して実行し、メディアサーバーを認証する認証ブローカーを判断します。サーバークレデンシャルは、c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥... ディレクトリに存在します。 例: bpnbat -whoami -cf "c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@win_primary.company.com Issued by: /CN=broker/OU=root@win_primary.company.com/ O=vx Expiry Date: Oct 31 20:11:40 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@win_primary.company.com でない場合、対象の名前 (win_media) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (win_primary) で実行します。 次に、証明書を配置するコンピュータ (win_media) 上で、次のコマンドを実行します。 bpnbat -loginmachine

手順	説明
サーバーが認可データベースにアクセスできることの検証	bpnbaz -ListGroups -CredFile "*machine_credential_file*" を実行して、メディアサーバーが必要に応じて認可データベースにアクセスできることを確認します。 例: bpnbaz -ListGroups -CredFile "C:¥Program Files¥Veritas¥NetBackup¥var¥vxss¥credentials¥ win_media.company.com" NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully. このコマンドが失敗した場合、認可サーバーであるプライマリサーバー (win_primary.company.com) で bpnbaz -AllowAuthorization を実行します。
ライブラリメッセージをロードできない場合	メディアサーバーを検証します。また、メディアサーバーが適切なデータベースにアクセスできることを検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを間接的に確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合は、認証クライアントライブラリおよび認可クライアントライブラリがインストールされていることを確認します。 また、このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示することによって、認証ドメインが正しいことを検証することもできます。

Windows クライアントでの検証項目

この項では、次の Windows クライアントでの検証手順を説明します。

- クライアントのクレデンシャルを検証します。
- 認証クライアントライブラリがインストールされているを検証します。
- 正しい認証ドメインを検証します。

次の表に、Windows クライアントでの検証手順を示します。

表 14-8 Windows クライアントでの検証手順

手順	説明
クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。 例: bpnbat -whoami -cf "*install_path* ¥Netbackup¥var¥vxss¥credentials¥ win_client.company.com " Name: win_client.company.com Domain: NBU_Machines@win_primary.company.com Issued by: /CN=broker/OU=root@win_primary.company.com/ O=vx Expiry Date: Oct 31 20:11:45 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@win_primary.company.com でない場合、対象の名前 (win_client) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machinesドメインとして機能する認証ブローカーのコンピュータ (win_primary) で実行します。 次に、証明書を配置するコンピュータ(win_client)上で、コマンド bpnbat -loginmachine を実行します。
認証クライアントライブラリがインストールされていることの検証	**メモ:** クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。 bpnbat -login Authentication Broker: win_primary Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : WINDOWS Domain: ENTERPRISE Name: Smith Password:Operation completed successfully. ライブラリがインストールされていない場合は、NetBackup Authentication and Authorization のライブラリがインストールされていないことを示すメッセージが表示されます。この検証は Windows の[プログラムの追加と削除]を参照して行うこともできます。

手順	説明
正しい認証ドメインの検証	[アクセス制御 (Access Control)]ホストプロパティで、または regedit を使用して、クライアントのすべての定義済み認証ドメインが正しいことを確認します。ドメインの綴りが正しいことを確認します。各ドメインに一覧表示された認証ブローカーがそのドメイン形式に対して有効であることを確認します。

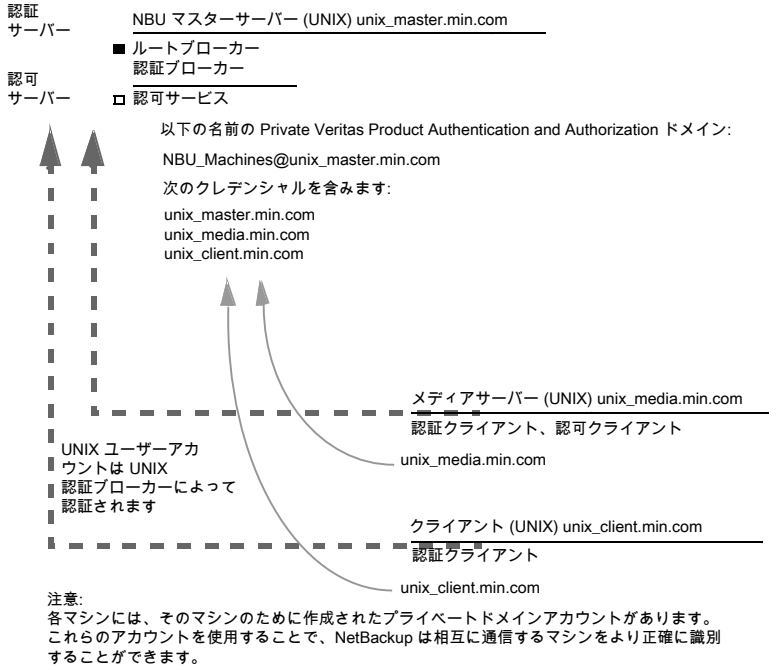
UNIX での検証項目

次の手順 (および次の図) を使用して、UNIX プライマリサーバー、メディアサーバーおよびクライアントでアクセス制御が正しく構成されていることを確認します。

- UNIX プライマリサーバーの検証
  p.203 の「UNIX プライマリサーバーの検証 」を参照してください。
- UNIX メディアサーバーの検証
  p.206 の「UNIX メディアサーバーの検証」を参照してください。
- UNIX クライアントの検証
  p.208 の「UNIX クライアントの検証」を参照してください。

次の例は UNIX システムのみを含む構成例を示したものです。

図 **14-3** UNIX システムだけが存在する構成の例



UNIX プライマリサーバーの検証

UNIX プライマリサーバーを検証するには次の手順を使います。

- UNIX プライマリサーバー設定を検証します。
- 認可の照合が許可されているコンピュータを検証します。
- データベースが正しく構成されていることを検証します。
- `nbatd` および `nbazd` プロセスが実行されていることを検証します。
- ホストプロパティが正しく構成されていることを検証します。

次の表に、UNIX プライマリサーバーの検証プロセスを示します。

表 14-9 UNIX プライマリサーバーの検証プロセス

プロセス	説明
UNIX プライマリサーバー設定の検証	ホストが登録されているドメイン (プライマリ認証ブローカーが存在する場所)、および証明書に示されているコンピュータの名前を判断します。bpnbat に -whoami およびプライマリサーバーのクレデンシャルファイルを指定する -cf を指定して実行します。サーバークレデンシャルは /usr/openv/var/vxss/credentials/ ディレクトリに存在します。 例: bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_primary.company.com Name: unix_primary.company.com Domain: NBU_Machines@unix_primary.company.com Issued by: /CN=broker/OU=root@unix_primary/O=vx Expiry Date: Oct 31 15:44:30 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@unix_primary.company.com でない場合、またはファイルが存在しない場合、対象の名前 (unix_primary) に対して bpnbat -addmachine を実行することを検討してください。NBU_Machines ドメインとして機能するコンピュータ (unix_primary) でこのコマンドを実行します。 次に、証明書を配置するコンピュータ (unix_primary) で、コマンド bpnbat -loginmachine を実行します。 **メモ:** クレデンシャルの期限が切れているかどうかを判断する場合、有効期限がローカル時間ではなく GMT で表示されることに注意してください。 **メモ:** この検証の残りの手順では、コンソールウィンドウからコマンドを実行することを想定しています。このコンソールウィンドウから、対象のユーザー識別情報で NBU_Security Admin のメンバーである識別情報を使用して bpnbat -login が実行されています。この識別情報は、通常、セキュリティが設定された最初の識別情報です。
認証ブローカーに存在するコンピュータの検証	認証ブローカーに存在するコンピュータを検証するには、管理者グループのメンバーでログオンし、次のコマンドを実行します。 bpnbat -ShowMachines 実行されているコンピュータが次のコマンドで表示されます。 bpnbat -AddMachine

プロセス	説明

認可の照合が許可されているコンピュータの検証	認可の照合を実行可能なコンピュータを検証するには、認可ブローカーで root ユーザーとしてログオンし、次のコマンドを実行します。
	
	`bpnbaz -ShowAuthorizers`
	` ==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_primary.company.com`
	`Name: unix_primary.company.com`
	
	` ==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_primary.company.com`
	`Name: unix_media.company.com`
	
	`Operation completed successfully.`
	
	このコマンドを実行すると、unix_primary および unix_media が認可を照合する権限を所有していることが示されます。両方のサーバーが、同じ vx (Veritas プライベートドメイン) ドメイン NBU_Machines@unix_primary.company.com に対して認証されていることに注意してください。
	
	認可済みコンピュータのリストにプライマリサーバーまたはメディアサーバーが表示されない場合、`bpnbaz -allowauthorization <server_name>` を実行して、表示されていないコンピュータを追加します。

データベースが正しく構成されていることの検証	データベースが正しく構成されていることを検証するには、`bpnbaz -listgroups` を実行します。
	
	`bpnbaz -listgroups`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	グループが表示されない場合または `bpnbaz -listmainobjects` を実行してもデータが戻されない場合は、`bpnbaz -SetupSecurity` を実行します。

プロセス	説明

nbatd および nbazd プロセスが実行されていることの検証	ps コマンドを実行して、指定したホスト上で nbatd および nbazd プロセスが実行されていることを確認します。必要に応じて、これらのプロセスを起動します。
	例:
	`ps -fed |grep vx`
	`root 10716 1 0 Dec 14 ? 0:02`
	`/usr/openv/netbackup/bin/private/nbatd`
	`root 10721 1 0 Dec 14 ? 4:17`
	`/usr/openv/netbackup/bin/private/nbazd`

ホストプロパティが正しく構成されていることの検証	[アクセス制御 (Access Control)]ホストプロパティで、[NetBackup Product Authentication and Authorization]プロパティが正しく設定されていることを検証します。この設定は、すべてのコンピュータが NetBackup Authentication and Authorization を使うかどうかによって[自動 (Automatic)]または[必須 (Required)]のいずれかにする必要があります。すべてのコンピュータで NetBackup Authentication and Authorization が使用されているわけではない場合は、[自動 (Automatic)]に設定します。
	[アクセス制御 (Access Control)]ホストプロパティで、リスト内の認証ドメインの綴りが正しいことを確認します。また、ドメインが適切なサーバー (有効な認証ブローカー) を示していることを確認します。すべてのドメインが UNIX ベースである場合、ドメインは、認証ブローカーを実行している UNIX マシンを示している必要があります。
	また、このプロセスは、cat を使用して bp.conf で確認することもできます。
	`cat bp.conf`
	`SERVER = unix_primary`
	`SERVER = unix_media`
	`CLIENT_NAME = unix_primary`
	`AUTHENTICATION_DOMAIN = company.com "default company NIS namespace"`
	`NIS unix_primary 0`
	`AUTHENTICATION_DOMAIN = unix_primary "unix_primary password file"`
	`PASSWD unix_primary 0`
	`AUTHORIZATION_SERVICE = unix_primary.company.com 0`
	`USE_VXSS = AUTOMATIC`
	`#`

UNIX メディアサーバーの検証

UNIX メディアサーバーを検証するには次を実行します。

- メディアサーバーを検証します。
- サーバーが認可データベースにアクセスできることを検証します。

- ライブラリメッセージをロードできないことを理解します。

次の表に、UNIX メディアサーバーの検証手順を示します。

表 14-10 UNIX メディアサーバーの検証プロセス

プロセス	説明

メディアサーバーの検証	bpnbat -whoami にメディアサーバーのクレデンシャルファイルを指定する -cf を指定して実行し、メディアサーバーを認証する認証ブローカーを判断します。サーバークレデンシャルは /usr/openv/var/vxss/credentials/ ディレクトリに存在します。
	例:
	`bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_media.company.com`
	`Name: unix_media.company.com`
	`Domain: NBU_Machines@unix_primary.company.com`
	`Issued by: /CN=broker/OU=root@unix_primary.company.com/O=vx`
	`Expiry Date: Oct 31 14:48:08 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	表示されたドメインが NBU_Machines@unix_primary.company.com でない場合、対象の名前 (unix_media) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (unix_primary) で実行します。
	次に、証明書を配置するコンピュータ (unix_primary) で、bpnbat -loginmachine を実行します。

サーバーが認可データベースにアクセスできることの検証	bpnbaz -ListGroups "machine_credential_file" を実行して、メディアサーバーが必要に応じて認可データベースにアクセスできることを確認します。
	"machine_credential_file"
	例:
	`bpnbaz -ListGroups -CredFile /usr/openv/var/vxss/credentials/unix_media.company.com`
	`NBU_User`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	このコマンドが失敗した場合、認可サーバーであるプライマリサーバー (unix_primary) で bpnbaz -AllowAuthorization を実行します。root または管理者で実行する必要があることに注意してください。

プロセス	説明
ライブラリメッセージをロードできない場合	メディアサーバーを検証します。また、メディアサーバーが適切なデータベースにアクセスできることを検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを間接的に確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合、認証および認可クライアントライブラリがインストールされていることを確認します。 また、認証ドメインが正しいことを検証することもできます。これを検証するには、このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示するか、`cat(1)ing` ファイルの内容を `bp.conf` コマンドで確認します。

UNIX クライアントの検証

次の手順が UNIX クライアントを検証するために使われます。

- UNIX クライアントのクレデンシャルを検証します。
- 認証クライアントライブラリがインストールされているを検証します。
- 正しい認証ドメインを検証します。

次の表に、UNIX クライアントの検証手順を示します。

表 14-11 UNIX クライアントの検証手順

手順	説明
UNIX クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。 例: bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_client.company.com Name: unix_client.company.com Domain: NBU_Machines@unix_primary.company.com Issued by: /CN=broker/OU=root@unix_primary.company.com/O=vx Expiry Date: Oct 31 14:49:00 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@unix_primary.company.com でない場合、対象の名前 (unix_client) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (unix_primary) で実行します。 次に、証明書を配置するコンピュータ (unix_client) 上で、コマンド bpnbat -loginmachine を実行します。
認証クライアントライブラリがインストールされていることの検証	クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。 bpnbat -login Authentication Broker: unix_primary.company.com Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd): NIS Domain: min.com Name: Smith Password: Operation completed successfully.

手順	説明

正しい認証ドメインの検証	[アクセス制御 (Access Control)]ホストプロパティで、または cat (1) を使用して、クライアントのすべての定義済み認証ドメインが正しいことを確認します。ドメインの綴りが正しいことを確認します。また、各ドメインに一覧表示された認証ブローカーがそのドメイン形式に対して有効であることを確認します。
	また、このプロセスは、cat (1) を使用して bp.conf で確認することもできます。
	`cat bp.conf`
	`SERVER = unix_primary`
	`SERVER = unix_media`
	`CLIENT_NAME = unix_primary`
	`AUTHENTICATION_DOMAIN = min.com "default company NIS namespace"`
	`NIS unix_primary 0`
	`AUTHENTICATION_DOMAIN = unix_primary.company.com "unix_primary password file" PASSWD unix_primary 0`
	`AUTHORIZATION_SERVICE = unix_primary.company.com 0`
	`USE_VXSS = AUTOMATIC`

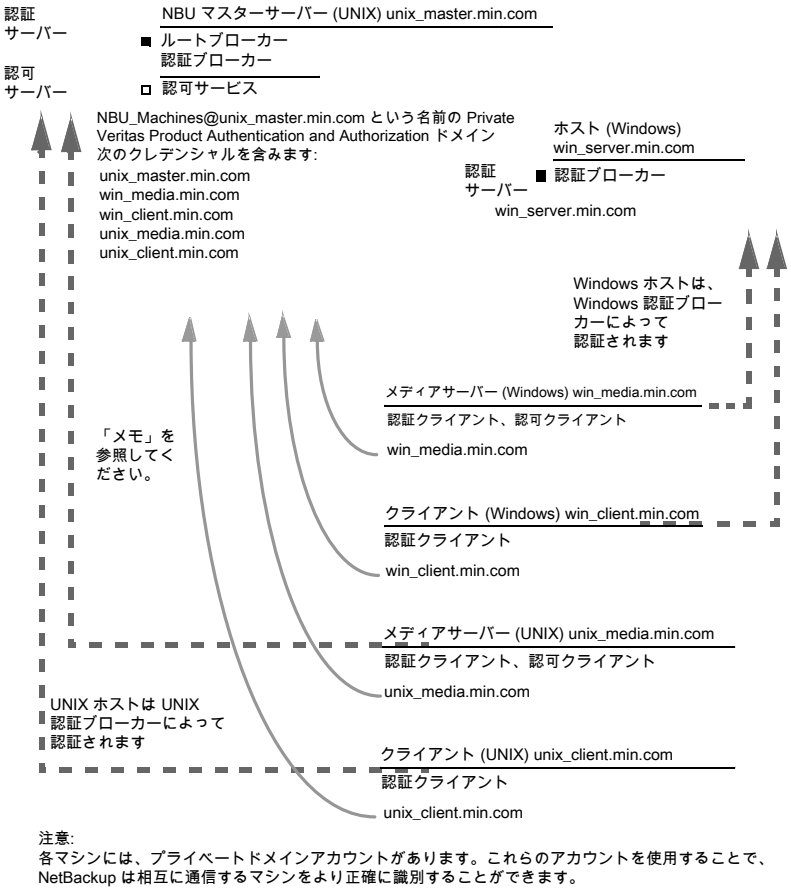
UNIX プライマリサーバーが存在する複合環境での検証項目

次の手順は、プライマリサーバー、メディアサーバーおよびクライアントが正しく構成されていることを確認するのに役立ちます。これらのマシンは、異機種間で NetBackup アクセス制御を使用する環境用に構成されている必要があります。プライマリサーバーは UNIX マシンです。

- 複合 UNIX プライマリのプライマリサーバーでの検証項目
- 複合 UNIX プライマリのメディアサーバーでの検証項目
- 複合 UNIX プライマリのクライアントでの検証項目

図 14-4 に、UNIX プライマリサーバーが存在する複合構成の例を示します。

図 **14-4** UNIX プライマリサーバーが存在する複合構成の例



複合 UNIX プライマリサーバーのプライマリサーバーでの検証項目

UNIX プライマリサーバーの検証手順については、次の項を参照してください。

p.203 の「UNIX プライマリサーバーの検証 」を参照してください。

複合 UNIX プライマリサーバーのメディアサーバーでの検証項目

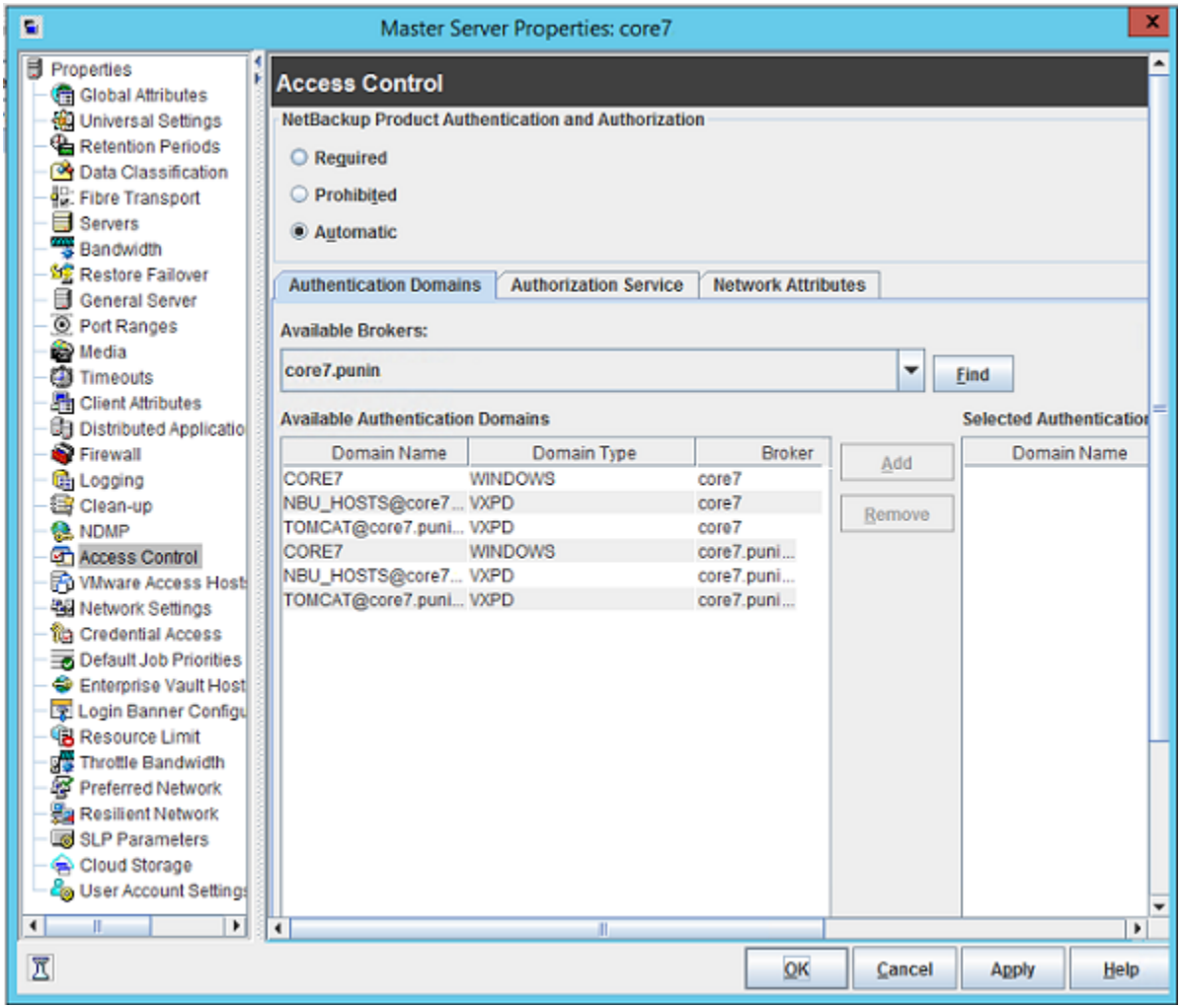
次の表に、複合 UNIX プライマリサーバーのメディアサーバーでの検証手順を示します。

表 14-12　複合 UNIX プライマリサーバーの検証手順

手順	説明
UNIX メディアサーバーの検証	UNIX メディアサーバーの検証手順については、次の項を参照してください。 p.206 の「UNIX メディアサーバーの検証」を参照してください。
Windows メディアサーバーの検証	コンピュータの証明書が、UNIX プライマリサーバー (unix_primary) に存在するルート認証ブローカーから取得されていることを確認します。 表示されない証明書がある場合、次のコマンドを実行して問題を解決します。 ■ bpnbat -addmachine ルート認証ブローカー上 (この例では、unix_primary) ■ bpnbat -loginmachine (この例では、win_media です。) 例: bpnbat -whoami -cf "*install_path* ¥Netbackup¥var¥vxss¥credentials¥ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@unix_primary.company.com Issued by: /CN=broker/OU=root@ unix_primary.company.com/O=vx Expiry Date: Oct 31 20:11:04 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.
認可の照合が許可されているメディアサーバーの検証	bpnbaz -listgroups -CredFile を実行して、メディアサーバーが認可の確認を実行できることを確認します。 例: bpnbaz -listgroups -CredFile "*install_path* ¥Netbackup¥var¥vxss¥credentials¥ win_media.company.com" NBU_User NBU_Operator NBU_Admin NBU_Security Admin Vault_Operator Operation completed successfully. メディアサーバーの認可の確認が許可されていない場合、プライマリサーバー上で、対象のメディアサーバー名に対して bpnbaz -allowauthorization を実行します。

手順	説明
ライブラリメッセージをロードできない場合	Windows メディアサーバーを検証します。また、Windows メディアサーバーで認可の確認が行えることを間接的に検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合、認証クライアントライブラリおよび認可クライアントライブラリがインストールされていることを確認します。
認証ドメインの検証	このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示することによって、認証ドメインが正しいことを検証します。 また、`regedit` (または `regedit32`) をメディアサーバー上で使用して次の場所で直接確認できます。 `HKEY_LOCAL_MACHINE¥SOFTWARE¥Veritas¥NetBackup¥CurrentVersion¥config¥AUTHENTICATION_DOMAIN`
クロスプラットフォームの認証ドメイン	複合環境では、適切なドメイン形式が正しい認証ブローカーを指していることを特に注意して確認してください。 [認証ドメイン (Authentication Domain)]タブの例は、Windows ブローカーに追加できる利用可能な Windows の認証ドメインを示します。この場合、システムが両方とも Windows ベースであるため、複合環境ではありません。Windows ドメインと UNIX ドメインの組み合わせがある場合は、ブローカーを最も有用な認証ドメインに合わせることが重要です。 プラットフォームを最も有用な認証ドメインに一致させる方法の表示については、図 14-5

図 14-5 クロスプラットフォームの認証ドメイン



複合 UNIX プライマリサーバーのクライアントでの検証項目

UNIX クライアントコンピュータを検証する手順については、次の項を参照してください。

p.208 の「UNIX クライアントの検証」を参照してください。

次の表に、Windows クライアントを検証する手順を示します。

表 14-13 Windows クライアントを検証する手順

手順	説明
Windows クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。 例: bpnbat -whoami -cf "c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_client.company.com Name: win_client.company.com Domain: NBU_Machines@unix_primary.company.com Issued by: /CN=broker/OU=root@unix_primary.company.com/ O=vx Expiry Date: Oct 31 19:50:50 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.
認証クライアントライブラリがインストールされていることの検証	クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。 例: bpnbat -login Authentication Broker: unix_primary.company.com Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : NIS Domain: min.com Name: Smith Password: Operation completed successfully.
Windows 認証ブローカーの検証	Windows 認証ブローカーが UNIX のメイン認証ブローカーとの相互信頼関係を確立していることを確認します。また、このブローカーが UNIX ブローカーをルートブローカーとして使用していることを確認します。

Windows プライマリサーバーが存在する複合環境での検証項目

次の手順は、プライマリサーバー、メディアサーバーおよびクライアントが正しく構成されていることを確認するのに役立ちます。これらのマシンは、異機種間で NetBackup アク

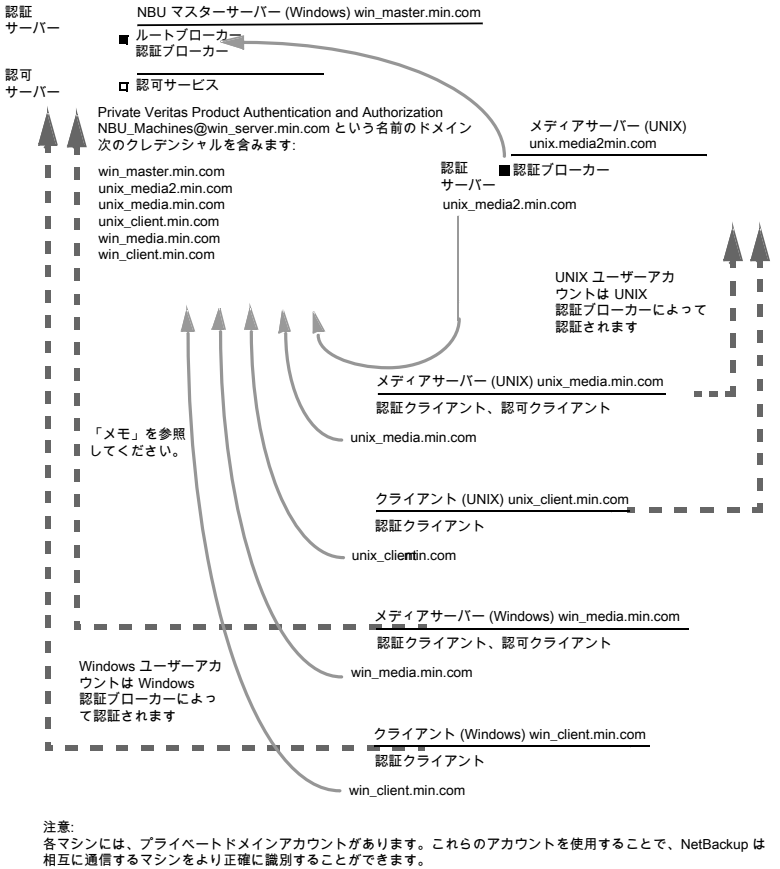
セス制御を使用する環境用に構成する必要があります。プライマリサーバーは Windows コンピュータです。

- 複合 Windows プライマリのプライマリサーバーでの検証項目
  p.217 の「複合 Windows プライマリサーバーのプライマリサーバーでの検証項目」を参照してください。
- 複合 Windows プライマリのメディアサーバーでの検証項目
  p.218 の「複合 Windows プライマリサーバーのメディアサーバーでの検証項目」を参照してください。
- 複合 Windows プライマリのクライアントでの検証項目

p.220 の「複合 Windows プライマリサーバーのクライアントでの検証項目」を参照してください。

図 14-6 に、Windows プライマリサーバーを含む構成の例を示します。

図 **14-6** Windows プライマリサーバーが存在する複合構成の例



注意:
各マシンには、プライベートドメインアカウントがあります。これらのアカウントを使用することで、NetBackup は相互に通信するマシンをより正確に識別することができます。

複合 Windows プライマリサーバーのプライマリサーバーでの検証項目

複合 Windows プライマリの検証手順については、次の項を参照してください。

p.194 の「Windows プライマリサーバーでの検証項目」を参照してください。

複合 Windows プライマリサーバーのメディアサーバーでの検証項目

次の表に、複合 Windows プライマリサーバーのメディアサーバーでの検証手順を示します。

表 14-14 複合 Windows プライマリサーバーのメディアサーバーでの検証手順

手順	説明
複合 Windows プライマリサーバーの Windows メディアサーバーでの検証	Windows メディアサーバーの検証手順については、次の項を参照してください。 p.198 の「Windows メディアサーバーでの検証項目」を参照してください。

UNIX メディアサーバーの検証	コンピュータの証明書が、Windows プライマリサーバー (win_primary) に存在するルート認証ブローカーから発行されていることを確認します。bpnbat -whoami にメディアサーバーのクレデンシャルファイルを指定する -cf を指定して実行し、メディアサーバーを認証する認証ブローカーを判断します。
	例:
	`bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_media.company.com`
	`Name: unix_media.company.comDomain: NBU_Machines@ win_primary.company.com`
	`Issued by: /CN=broker/OU=root@win_primary.company.com/ O=vx`
	`Expiry Date: Oct 31 14:48:08 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

手順	説明
サーバーが認可データベースにアクセスできることの検証	メディアサーバーが認可データベースにアクセスできることを確認するには、認可の確認を行う必要があります。bpnbaz -ListGroups -CredFile "*/usr/openv/var/vxss/credentials/<hostname>*"を実行します。 例: bpnbaz -ListGroups -CredFile¥ /usr/openv/var/vxss/credentials/unix_media.company.com NBU_Operator NBU_AdminNBU_SAN Admin NBU_UserNBU_Security Admin Vault_Operator Operation completed successfully. メディアサーバーの認可の確認が許可されていない場合、プライマリサーバー上で、対象のメディアサーバー名に対して bpnbaz -allowauthorization を実行します。
ライブラリメッセージをロードできない場合	メディアサーバーを検証します。また、メディアサーバーが適切なデータベースにアクセスできることを間接的に検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合は、認証クライアントライブラリおよび認可クライアントライブラリがインストールされていることを確認します。

手順	説明

クロスプラットフォームの認証ドメイン	また、このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示することによって、認証ドメインが正しいことを検証することもできます。または、cat(1)ing ファイルの内容を bp.conf コマンドで確認して検証することもできます。
	複合環境では、適切なドメイン形式が正しい認証ブローカーを指していることを特に注意して確認してください。
	次の例では、PASSWD ドメインおよび NIS ドメインが unix_media2.company.com (この例における UNIX 認証ブローカー) を指しています。
	`cat bp.conf`
	`SERVER = win_primary.company.com`
	`MEDIA_SERVER = unix_media.company.com`
	`MEDIA_SERVER = unix_media2.company.com`
	`CLIENT_NAME = unix_media`
	`AUTHENTICATION_DOMAIN = win_primary "win_primary domain"`
	`WINDOWS win_primary.company.com`
	`0`
	`AUTHENTICATION_DOMAIN = enterprise "enterprise domain"`
	`WINDOWS win_primary.company.com 0`
	`AUTHENTICATION_DOMAIN = unix_media2.company.com "local`
	`unix_media2 domain" PASSWD unix_media2.company.com 0`
	`AUTHENTICATION_DOMAIN = min.com "NIS domain" NIS`
	`unix_media.company.com 0`
	`AUTHORIZATION_SERVICE = win_primary.company.com 0`
	`USE_VXSS = AUTOMATIC`

複合 Windows プライマリサーバーのクライアントでの検証項目

次の表に、複合 Windows プライマリサーバーのクライアントでの検証手順を示します。

表 14-15 複合 Windows プライマリサーバーの検証手順

手順	説明
Windows クライアントのクレデンシャルの検証	Windows クライアントの検証手順については、次の項を参照してください。 p.200 の「Windows クライアントでの検証項目」を参照してください。

手順	説明
UNIX クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。 例: bpnbat -whoami -cf ¥ "/usr/openv/var/vxss/credentials/ unix_client.company.com" Name: unix_client.company.com Domain: NBU_Machines@win_primary.company.com Issued by: /CN=broker/OU=root@ win_primary.company.com/O=vx Expiry Date: Oct 31 21:16:01 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.
認証クライアントライブラリがインストールされていることの検証	クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。 bpnbat -login Authentication Broker: unix_media2.company.com Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : NIS Domain: min.com Name: Smith Password: You do not currently trust the server: unix_media.company.com, do you wish to tr ust it? (y/n): y Operation completed successfully.
UNIX 認証ブローカーの検証	UNIX の認証ブローカーが、メイン Windows 認証ブローカーとの相互信頼関係を確立していること、またはルートブローカーとして Windows ブローカーを使用していることを確認します。

nbac_cron ユーティリティについて

cron ユーティリティを使うと、NetBackup 操作をスケジュールされたジョブとして実行できます。NBAC が有効になると、これらのジョブは、必要なコマンドを実行する権限がある OS ユーザーというコンテキストで実行できます。nbac_cron.exe ユーティリティを使って、

cron ジョブまたは AT ジョブの実行に必要な資格情報を作成できます。これらの資格情報は、bpnbat ログオンを実行して取得される資格情報と比べて、より長期間有効になります。ここでは、1 年間有効になります。

このユーティリティは次の場所にあります。

```
-/opt/openv/netbackup/bin/goodies/nbac_cron
```

nbac_cron ユーティリティを設定して cron ジョブを実行する手順について詳しくは、次のトピックを参照してください。

p.222 の「nbac_cron ユーティリティの使用」を参照してください。

nbac_cron ユーティリティの使用

次の手順により、cron ジョブを実行するためのクレデンシャルを作成できます。

nbac_cron ユーティリティを使用した cron ジョブの実行

1 プライマリサーバー上で root または管理者として nbac_cron-addCron コマンドを実行します。

```
root@amp# /usr/openv/netbackup/bin/goodies/nbac_cron -AddCron

# nbac_cron -AddCron

This application will generate a Veritas private domain identity
that can be used in order to run unattended cron and/or at jobs.

User name to create account for (e.g. root, JSmith etc.): Dan

Password:*****

Password:*****

Access control group to add this account to [NBU_Admin]:

Do you with to register this account locally for root(Y/N) ? N

In order to use the account created please login as the OS
identity that will run the at or cron jobs. Then run nbac_cron
-setupcron or nbac_cron -setupat. When nbac_cron -setupcron or
nbac_cron -setupat is run the user name, password and
authentication broker will need to be supplied. Please make note
of the user name, password, and authentication broker. You may
rerun this command at a later date to change the password for an
account.

Operation completed successfully.
```

明示的に、ユーザーを追加するアクセス制御グループ (NBU_Operator、Vault_Operator など) を指定しない場合、cron ユーザー (ここでは Dan) が NBU_Admin グループに追加されます。

「Yes」を選択して、ローカルにアカウントを root として登録すると、nbac_cron -SetupCron コマンドは自動的に root として cron_user ユーザーに対して実行されます。root 以外の OS ユーザーとして cron ジョブを実行する場合は、「No」を選択して、手動で nbac_cron -SetupCron コマンドを root 以外の OS ユーザーとして実行する必要があります。

ID は Veritas プライベートドメイン内で生成されます。この ID を cron ジョブの実行に使用できます。

2 次に、cron ジョブを実行する必要がある OS ユーザーとして nbac_cron-SetupCron コマンドを実行して、この ID のクレデンシャルを取得します。

```
[dan@amp ~]$ /usr/openv/netbackup/bin/goodies/nbac_cron -SetupCron

This application will now create your cron and/or at identity.

Authentication Broker: amp.sec.punin.sen.veritas.com

Name: Dan

Password:*****

You do not currently trust the server:
amp.sec.punin.sen.veritas.com, do you wish to trust it? (Y/N): Y

Created cron and/or at account information. To use this account
in your own cron or at jobs make sure that the environment
variable VXSS_CREDENTIAL_PATH is set to
"/home/dan/.vxss/credentials.crat"

Operation completed successfully.
```

「You do not currently trust the server」メッセージは、そのブローカーをまだ信頼できていない場合、1 回だけ表示されます。

クレデンシャルは、ユーザーのホームディレクトリ user/.vxss/credentials.crat に作成されます。クレデンシャルは、生成から 1 年間有効になります。

必要に応じて、次のコマンドによりクレデンシャル情報を確認できます。

```
dan@amp~]$ /usr/openv/netbackup/bin/bpnbat -whoami -cf
~dan/.vxss/credentials.crat

Name: CronAt_dan

Domain: CronAtUsers@amp.sec.punin.sen.veritas.com

Issued by: /CN=broker/OU=amp.sec.punin.sen.veritas.com
```

```
Expiry Date: Feb 4 13:36:08 2016 GMT

Authentication method: Veritas Private Domain

Operation completed successfully.
```

期限切れになる前にクレデンシャルを更新するには、SetupCron の操作 (手順 2) を再実行する必要があります。

3 これで、独自の cron ジョブを作成できるようになりました。新しいジョブをスケジュールする前に、VXSS_CREDENTIAL_PATH パスが、作成したクレデンシャルを指していることを確認してください。

アクセス管理ユーティリティの使用

NetBackup のセキュリティ管理者ユーザーグループに割り当てられているユーザーは、NetBackup 管理コンソールの[アクセス管理 (Access Management)]ノードにアクセスできます。他のユーザーグループに割り当てられているユーザーおよび NetBackup 管理者の場合、[アクセス管理 (Access Management)]ノードを参照できます。このノードは NetBackup 管理コンソールに表示されますが、展開できません。

セキュリティ管理者以外のユーザーが[アクセス管理 (Access Management)]を選択しようとすると、エラーメッセージが表示されます。[アクセス管理 (Access Management)]固有のツールバーオプションおよびメニュー項目は、表示されません。

前の手順が正常に完了すると、デフォルトの NetBackup ユーザーグループが、NetBackup 管理コンソールの[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]ウィンドウに表示されます。

コマンドラインでグループを表示するには、認可サーバーソフトウェアがインストールされているコンピュータで、bpnbaz -ListGroups を実行します。

UNIX

bpnbaz は、/usr/openv/netbackup/bin/admincmd ディレクトリに存在します。

Windows

bpnbaz は、*Install_path*¥Veritas¥NetBackup¥bin¥admincmd ディレクトリに存在します。

(bpnbat -login を使用して、セキュリティ管理者としてログオンしておく必要があります。)

```
bpnbaz -ListGroups
 NBU_User
 NBU_Operator
 NBU_Admin
 NBU_Security Admin
 Vault_Operator
```

```
NBU_SAN Admin
NBU_KMS Admin
Operation completed successfully.
```

NetBackup のユーザーグループが表示されます。この処理によって、セキュリティ管理者がユーザーグループにアクセスできることを確認します。

NetBackup へアクセス可能なユーザーの決定について

アクセス管理ユーティリティでは、1 つのユーザーグループのみが許可されます。デフォルトでは、NBU_Security Admin ユーザーグループが NetBackup のアクセス管理に関する次の事項を定義します。

- 個々のユーザーの権限。
  p.225 の「個々のユーザー」を参照してください。
- ユーザーグループの作成。
  p.226 の「ユーザーグループ」を参照してください。

まず、ユーザーがアクセスする必要のある NetBackup リソースを決定します。リソースと関連する権限の場合

p.232 の「NetBackup ユーザーグループの特定のユーザー権限の表示」を参照してください。

セキュリティ管理者は、まず複数のユーザー間の共通点を検討し、次にそれらのユーザーが必要とする権限を付与されたユーザーグループを作成できます。一般に、ユーザーグループは、その役割 (管理者、オペレータ、エンドユーザーなど) に対応します。

次に示す 1 つ以上の条件に基づいたユーザーグループを検討してください。

- 組織内の機能に基づいた単位 (UNIX 管理など)
- NetBackup リソース (ドライブ、ポリシーなど)
- 場所 (西部、東部など)
- 個人の職務 (テープオペレータなど)

権限は、ホストごとの各ユーザーではなく、ユーザーグループ内の各ユーザーに付与されます。ユーザーは付与された権限の範囲内でのみ処理を実行できます。コンピュータ名に基づく制限はありません。

個々のユーザー

NetBackup のアクセス管理ユーティリティでは、OS で定義されている既存のユーザー、グループおよびドメインが使用されます。アクセス管理ユーティリティでは、ユーザーおよ

びパスワードのリストが保持されません。セキュリティ管理者がグループのメンバーを定義する場合は、OS の既存のユーザーをユーザーグループのメンバーとして指定します。

認証されたすべてのユーザーは、1 つ以上の認可ユーザーグループに属します。デフォルトでは、すべてのユーザーは、NBU_Users ユーザーグループに属します。

すべての認証済みユーザーは、NBU_Users ユーザーグループの暗黙的なメンバーです。他のすべてのグループには、メンバーを明示的に定義する必要があります。NetBackup セキュリティ管理者は、他のグループに手動で追加されたメンバーを削除することができます。ただし、NBU_Security Admin グループの事前定義された暗黙的なメンバーを削除することはできません。OS グループおよび OS ユーザーを認可グループに追加することもできます。

ユーザーグループ

NetBackup のアクセス管理を構成する場合、ユーザーグループに権限を割り当て、次にユーザーをユーザーグループに割り当てます。個々のユーザーに権限を直接割り当てるのではなく、グループに権限を割り当てます。

インストールが正常に行われると、NetBackup では、多くのサイトにおける NetBackup 運用の作業管理を支援するデフォルトユーザーグループが作成されます。これらのユーザーグループは、`Access Management > NBU User Groups`に表示されます。[アクセス管理 (Access Management)]の内容は NBU_Security Admin グループのメンバーだけが参照できます。

セキュリティ管理者は、デフォルトの NetBackup ユーザーグループを使うか、またはカスタムユーザーグループを作成できます。

NetBackup のデフォルトユーザーグループ

デフォルトユーザーグループで権限が付与されているユーザーは、ユーザーグループ名と直接関連しています。原則として、認可オブジェクトは、NetBackup 管理コンソールのツリーに表示されるノードと関連しています。

次の表では、NetBackup の各デフォルトユーザーグループについて説明します。

表 14-16 NetBackup のデフォルトユーザーグループ

デフォルトユーザーグループ	説明
オペレータ (NBU_Operator)	NBU_Operator ユーザーグループの主な作業は、ジョブの監視です。たとえば、NBU_Operator ユーザーグループのメンバーがジョブを監視し、問題が発生した場合は、NetBackup 管理者に通知する場合があります。その後、管理者によってその問題が解決されます。多くの場合、デフォルトでは、NBU_Operator ユーザーグループのメンバーは、より大きな問題を解決するために必要な権限を持っていません。 NBU_Operator ユーザーグループのメンバーは、テープの移動、ドライブの操作、ロボットのインベントリなどの作業を実行する権限を持ちます。
管理者 (NBU_Admin)	NBU_Admin ユーザーグループのメンバーは、任意の NetBackup 認可オブジェクトに対してアクセス、構成および操作を行うための完全な権限を持ちます。SAN 管理者の場合には、一部例外があります。つまり、メンバーは、[アクセス管理 (Access Management)]以外に管理者が利用可能なすべての権限を持ちます。ただし、このグループのメンバーは、OS に root または管理者としてログオンする必要はありません。 **メモ:** NBU_Admin ユーザーグループのメンバーは[アクセス管理 (Access Management)]の内容を参照できないため、他のユーザーグループに権限を割り当てることはできません。
SAN 管理者 (NBU_SAN Admin)	デフォルトでは、NBU_SAN Admin ユーザーグループのメンバーは、ディスクプールおよびホストプロパティの表示、読み込み、操作および構成を行うための完全な権限を持ちます。これらの権限によって、SAN 環境および NetBackup との関係を構成できます。
ユーザー (NBU_User)	NBU_User ユーザーグループは、付与された権限が最も少ない、NetBackup のデフォルトユーザーグループです。NBU_User ユーザーグループのメンバーは、ローカルホストでファイルのバックアップ、リストアおよびアーカイブだけを実行できます。NBU_User ユーザーグループのメンバーは、NetBackup のクライアントインターフェース (BAR) の機能にアクセスする権限を持ちます。
セキュリティ管理者 (NBU_Security Admin)	通常、NBU_Security Admin ユーザーグループに属するメンバーは非常に少数です。 デフォルトでは、セキュリティ管理者が所有する権限は、[アクセス管理 (Access Management)] でアクセス制御を構成する権限だけです。アクセス制御を構成する権限には、次の権限が含まれます。 ■ 管理コンソール で NetBackup[アクセス管理 (Access Management)] の内容を参照する ■ ユーザーとユーザーグループを作成、変更および削除する ■ ユーザーグループにユーザーを割り当てる ■ ユーザーグループに権限を割り当てる

デフォルトユーザーグループ	説明
Vault オペレータ (Vault_Operator)	Vault_Operator ユーザーグループは、Vault 処理で必要なオペレータ操作を実行する権限を付与されたデフォルトユーザーグループです。
KMS 管理者 (NBU_KMS Admin)	デフォルトでは、NBU_KMS Admin ユーザーグループのメンバーは、暗号化キーマネージメントプロパティの表示、読み込み、操作および構成を行うための完全な権限を持ちます。これらの権限によって、KMS 環境および NetBackup との関係を構成することができます。
追加ユーザーグループ	セキュリティ管理者 (NBU_Security Admin または同等のグループのメンバー) は、必要に応じてユーザーグループを作成できます。デフォルトユーザーグループは、選択して変更および保存することができます。今後の参照用にデフォルト設定を残しておくために、デフォルトユーザーグループをコピーして、名前を変更してから保存することをお勧めします。

ユーザーグループ作成

次の手順に従って、新しいユーザーグループを作成することができます。[アクセス管理 (Access Management)]>[処理 (Actions)]>[新しいグループ (New Group)]を展開するか、または既存のユーザーグループを選択して[アクセス管理 (Access Management)]>[処理 (Actions)]>[新しいグループにコピー (Copy to New Group)]を展開します。

新しいユーザーグループを作成する方法

次の手順に従って、新しいユーザーグループを作成することができます。

新しいユーザーグループを作成する方法

1. NBU_Security Admin ユーザーグループ (または同等のユーザーグループ) のメンバーで、[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]を展開します。
2. [処理 (Actions)]>[新しいユーザーグループにコピー (New User Group)]を選択します。[新しいユーザーグループの追加 (Add New User Group)]ダイアログボックスが表示され、[一般 (General)]タブが開きます。
3. 新しいグループの名前を[名前 (Name)]フィールドに入力し、次に[ユーザー (Users)]タブをクリックします。
4. 作成した新しいユーザーグループに割り当てる定義済みユーザーを選択します。次に[割り当て (Assign)]をクリックします。または、グループにすべての定義済みユーザーを割り当てる場合は、[すべて割り当て (Assign All)]をクリックします。[割り当て済みのユーザー (Assigned Users)]リストからユーザーを削除するには、ユーザー名を選択して[削除 (Remove)]をクリックします。
5. [アクセス権 (Permissions)]タブをクリックします。

6 [リソース (Resources)]リストおよび認可オブジェクトからリソースを選択します。次にそのオブジェクトに対する権限を選択します。

7 [OK]をクリックし、ユーザーグループおよびグループ権限を保存します。

既存のユーザーグループのコピーによる新しいユーザーグループの作成

次の手順に従って、既存のユーザーグループのコピーから新しいユーザーグループを作成することができます。

既存のユーザーグループをコピーして新しいユーザーグループを作成する方法

1 NBU_Security Admin ユーザーグループ (または同等のユーザーグループ) のメンバーで、[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]を展開します。

2 [詳細 (Details)]ペインで、既存のユーザーグループを選択します。(NetBackup 管理コンソールの左側のペイン。)

3 [処理 (Actions)]>[新しいユーザーグループにコピー (Copy to New User Group)]を選択します。選択したユーザーグループに基づいたダイアログボックスが表示され、[一般 (General)]タブが開きます。

4 新しいグループの名前を[名前 (Name)]フィールドに入力し、次に[ユーザー (Users)]タブをクリックします。

5 作成した新しいユーザーグループに割り当てる定義済みユーザーを選択します。次に[割り当て (Assign)]をクリックします。または、グループにすべての定義済みユーザーを割り当てる場合は、[すべて割り当て (Assign All)]をクリックします。[割り当て済みのユーザー (Assigned Users)]リストからユーザーを削除するには、ユーザー名を選択して[削除 (Remove)]をクリックします。

6 [アクセス権 (Permissions)]タブをクリックします。

7 [リソース (Resources)]リストのリソースおよび認可オブジェクトを選択し、次にそのオブジェクトに対する権限を選択します。

8 [OK]をクリックし、ユーザーグループおよびグループ権限を保存します。ユーザーグループの新しい名前が詳細ペインに表示されます。

ユーザーグループの名前の変更

一度 NetBackup ユーザーグループを作成すると、ユーザーグループの名前は変更できません。ユーザーグループの名前を直接変更する代わりに、ユーザーグループをコピーして新しい名前を付け、元のグループとメンバーシップが同じであることを確認してから、元の NetBackup ユーザーグループを削除します。

ユーザーグループへの新しいユーザーの追加

[新しいユーザー (New User)]をクリックして[定義されているユーザー (Defined Users)]リストにユーザーを追加します。追加したユーザーの名前が[定義されているユーザー (Defined Users)]リストに表示されます。セキュリティ管理者は、このユーザーをユーザーグループに割り当てることができます。

p.231 の「ユーザーグループへのユーザーの割り当て」を参照してください。

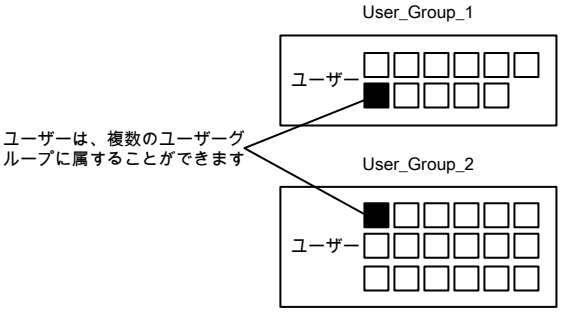
ユーザーグループおよびユーザーの定義について

NetBackup では、オペレーティングシステムの既存のユーザーが認証されます。NetBackup のパスワードとプロファイルを使用して NetBackup ユーザーを作成する必要はありません。

ユーザーは複数のユーザーグループに属することができ、属するグループのアクセス権を組み合わせた権限を持ちます。

図 14-7 に、ユーザーグループの定義を示します。

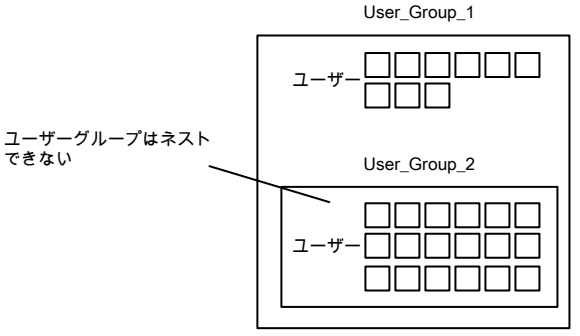
図 14-7　　ユーザーグループの定義



ユーザーは同時に複数のユーザーグループのメンバーになることができますが、NetBackup では、ユーザーグループをネストできません。たとえば、ユーザーグループのメンバーは複数のユーザーグループに属することができますが、ユーザーグループは他のユーザーグループに属することはできません。

次の図に、ユーザーグループはネストできないことを示します。

図 14-8 ユーザーグループはネストできない



新しいユーザーとしてのログオン

新しいユーザーとしてログオンするには次の手順を使うことができます。

新しいユーザーとしてログオンする方法

- [ファイル (File)]>[新しいユーザーとしてログオン (Login as New User)]を展開します (Windows)。このオプションはアクセス制御が構成されるコンピュータでのみ利用可能です。これは、最小限の権限で操作を行うという考え方を取り入れる場合に有効です。各ユーザーは、より高度な権限を持つアカウントを使用するように設定を切り替える必要があります。

ユーザーグループへのユーザーの割り当て

次の手順に従って、ユーザーをユーザーグループに割り当てることができます。ユーザーは、既存のネームスペース (NIS、Windows など) から NBU のユーザーグループに割り当てられます。この手順においては、新しいユーザーアカウントは作成されていません。

ユーザーをユーザーグループに追加する方法

1. NBU_Security Admin ユーザーグループ (または同等のユーザーグループ) のメンバーで、[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]を展開します。
2. ユーザーを追加するユーザーグループをダブルクリックします。
3. [ユーザー (Users)]タブを選択し、[ユーザーの追加 (Add User)]をクリックします。
4. ユーザー名と認証ドメインを入力します。ユーザーのドメイン形式を、[NIS]、[NIS+]、[PASSWD]、[Windows]または[Vx]から選択します。
5. ユーザーのドメイン形式を、次のいずれかから選択します。
   - NIS
     ネットワーク情報サービス

- NIS+
  ネットワーク情報サービスプラス
- PASSWD
  認証サーバー上の UNIX パスワードファイル
- Windows
  プライマリドメインコントローラまたは Active Directory
- Vx
  Veritas プライベートデータベース

6 [ユーザー形式 (User Type)]で、ユーザーが個々のユーザーか OS グループかを選択します。

7 [OK]をクリックします。名前が[割り当て済みのユーザー (Assigned Users)]リストに追加されます。

認可オブジェクトおよび権限について

通常、認可オブジェクトは、NetBackup 管理コンソールのツリーに表示されるノードと関連しています。

[認可オブジェクト (Authorization Objects)]ペインには、権限を付与することが可能な NetBackup オブジェクトが表示されます。

[「DevHost」の権限 (Permissions for "DevHost")]ペインには、選択したユーザーグループに構成されている権限のセットが表示されます。

認可オブジェクトには、次の権限セットのいずれかを付与できます。

- 参照および読み込み
- 操作
- 構成

[「DevHost」の権限 (Permissions for "DevHost")]列に小文字が表示されている場合は、権限セットのすべての権限ではなく、一部の権限を示します。権限はオブジェクトに対して付与されています。

NetBackup ユーザーグループの特定のユーザー権限の表示

各 NBU ユーザーグループに付与される権限は、認可オブジェクトの名前と関連しています。デフォルトの NBU ユーザーグループには、NBU_Operator、NBU_Admin、NBU_SAN Admin、NBU_User、NBU_Security Admin および Vault_Operator が含まれます。

リソース間の相互依存の複雑さのために、場所によってはリソースへのアクセスや単一の権限へのアクセスをマッピングすることは不可能です。アクセス確認の決定をするために評価される必要のある複数の基礎的な権限がリソース間に存在することがあります。このような権限の混在により、リソース権限とリソースアクセス間で何らかの不一致が生じる可能性があります。この潜在的な不一致は、ほとんどの場合読み込み権限に限定されます。たとえば、Security_Admin には、ポリシーの参照や表示の権限がないことがあります。ポリシーはクライアントのセキュリティの構成に必要なクライアント情報を含んでいるため、管理者はポリシーへのアクセス権が必要です。

メモ: 権限の例外がある場合があります。NBU_User、NBU_KMS_Admin、NBU_SAN Admin、Vault_Operator ユーザーは、Java GUI からホストプロパティにアクセスできません。ホストプロパティのデータをフェッチするには、ポリシーオブジェクトにも参照を作ります。この例外は、ホストプロパティにアクセスするためには、ユーザーはポリシーオブジェクトの読み込みまたは参照アクセス権が必要であることを意味します。ポリシーオブジェクトに手動で読み込みアクセス権を与えることで問題を解決します。

メモ: この件について詳しくは、ベリタステクニカルサポートの Web サイトを参照してください。

特定のユーザー権限を表示する方法

1. NetBackup 管理コンソールで、[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]を展開します。
2. [セキュリティ (Security)]ウィンドウで、NBU_Operator、NBU_Admin、NBU_SAN Admin、NBU_User、NBU_Security Admin または Vault_Operator のいずれか適切なものをダブルクリックします。
3. [NBU_Operator]ウィンドウで、[アクセス権 (Permissions)]タブを選択します。
4. [認可オブジェクト (Authorization Objects)]ペインで、必要な認可オブジェクトを選択します。[アクセス権 (Permissions)]ペインはその認可オブジェクトの権限を表示します。

権限の付与

ユーザーグループのメンバーに権限を付与するために次の手順を使うことができます。

権限をユーザーグループのメンバーに付与する方法

1. 認可オブジェクトを選択します。
2. 次に、現在選択しているユーザーグループのメンバーに付与する権限のチェックボックスにチェックマークを付けます。

新しいユーザーグループを作成するためにユーザーグループをコピーすると、権限の設定もコピーされます。

認可オブジェクト

次の表に、NetBackup 管理コンソールの［NBU_Operator］ウィンドウに表示されている順序で認可オブジェクトを示します。

また、これらの表は、次のように、NBU ユーザーグループごとに認可オブジェクトとデフォルトの権限の関係も示します。

- X は、ユーザーグループが対象の動作を実行する権限を所有していることを示します。
- 「---」は、ユーザーグループが対象の動作を実行する権限を所有していないことを示します。

メディアの認可オブジェクトの権限

次の表に、メディアの認可オブジェクトに関連する権限を示します。

表 14-17　メディアの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
操作	バーコードの更新	X	X	---	---	---	X	---
	取り出し	X	X	---	---	---	X	---
	移動	X	X	---	---	---	X	---
	割り当て	X	X	---	---	---	X	---
	割り当て解除	X	X	---	---	---	X	---
	データベースの更新	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	X	---
	削除	---	X	---	---	---	X	---
	期限切れ	---	X	---	---	---	X	---

ポリシーの認可オブジェクトの権限

次の表に、ポリシーの認可オブジェクトに関連する権限を示します。

表 14-18　ポリシーの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	---	---
読み込み	読み込み	X	X	---	---	---	---	---
操作	バックアップ (Back up)	X	X	---	---	---	---	---
構成	有効化 (Activate) 無効化 (Deactivate) 新規 削除	--- --- --- ---	X X X X	--- --- --- ---	--- --- --- ---	--- --- --- ---	--- --- --- ---	--- --- --- ---

ドライブの認可オブジェクトの権限

次の表に、ドライブの認可オブジェクトに関連する権限を示します。

表 14-19　ドライブの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	X	---	---	X	---
読み込み	読み込み	X	X	X	---	---	X	---
操作	起動	X	X	---	---	---	---	---
	停止	X	X	---	---	---	---	---
	リセット	X	X	---	---	---	---	---
	割り当て	X	---	---	---	---	---	---
	割り当て解除	X	---	---	---	---	---	---

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

レポートの認可オブジェクトの権限

次の表に、レポートの認可オブジェクトに関連する権限を示します。レポートには、アクセス権限セットだけを指定できます。構成権限セットまたは操作権限セットは指定できません。

表 14-20 レポートの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	---	X	---	---	---	X	---
読み込み	読み込み	---	X	---	---	---	X	---

NBU_Catalog の認可オブジェクトの権限

次の表に、NetBackup カタログの認可オブジェクトに関連する権限を示します。

表 14-21 NBU_Catalog の認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	---	X	---	---	---	X	---
読み込み	読み込み	---	X	---	---	---	X	---

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
操作	バックアップ (Back up)	---	X	---	---	---	---	---
	リストア	---	X	---	---	---	---	---
	検証	---	X	---	---	---	---	---
	複製	---	X	---	---	---	---	---
	インポート	---	X	---	---	---	---	---
	期限切れ	---	X	---	---	---	---	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---
	構成の読み込み	---	X	---	---	---	---	---
	構成の設定	---	X	---	---	---	---	---

ロボットの認可オブジェクトの権限

次の表に、ロボットの認可オブジェクトに関連する権限を示します。

表 14-22 ロボットの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	X	---	---	X	---
読み込み	読み込み	X	X	X	---	---	X	---
操作	インベントリ	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	X	---
	削除	---	X	---	---	---	X	--

ストレージユニットの認可オブジェクトの権限

次の表に、ストレージユニットの認可オブジェクトに関連する権限を示します。

表 14-23 ストレージユニットの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	---	---
読み込み	読み込み	X	X	---	---	---	---	---
構成	割り当て	---	X	---	---	---	---	---
	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

ディスクプールの認可オブジェクトの権限

次の表に、ディスクプールの認可オブジェクトに関連する権限を示します。

表 14-24 ディスクプールの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	X	---	---	---	---
読み込み	読み込み	X	X	X	---	---	---	---
操作	新規	---	X	X	---	---	---	---
	削除	---	X	X	---	---	---	---
	変更	---	X	X	---	---	---	---
	マウント	---	X	X	---	---	---	---
	マウント解除	---	X	X	---	---	---	---
構成	構成の読み込み	---	X	X	---	---	---	---
	構成の設定	---	---	X	---	---	---	---

バックアップおよびリストアの認可オブジェクトの権限

次の表に、バックアップおよびリストアの認可オブジェクトに関連する権限を示します。

表 14-25 バックアップおよびリストアの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	X	X	---	---	X
読み込み	読み込み	X	X	X	X	---	---	X
操作	バックアップ (Back up)	X	X	X	X	---	---	X
	リストア	X	X	X	X	---	---	X
	代替クライアント	X	X	---	---	---	---	---
	代替サーバー	X	X	---	---	---	---	---
	管理者アクセス	X	X	---	---	---	---	---
	データベースエージェント	---	---	---	---	---	---	---
	一覧表示	---	---	X	X	---	---	X

ジョブの認可オブジェクトの権限

次の表に、ジョブの認可オブジェクトに関連する権限を示します。

表 14-26 ジョブの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
操作	一時停止	X	X	---	---	---	X	---
	再開	X	X	---	---	---	X	---
	キャンセル	X	X	---	---	---	X	---
	削除	X	X	---	---	---	X	---
	再起動	X	X	---	---	---	X	---
	新規	X	X	---	---	---	X	---

サービスの認可オブジェクトの権限

次の表に、サービスの認可オブジェクトに関連する権限を示します。

表 14-27　サービスの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
操作	停止	X	X	---	---	---	---	---

読み込み権限および表示権限は[デーモン (Daemons)]タブには影響を与えません。この情報はサーバーからユーザーレベルの呼び出しを使用して取得されます。呼び出しは、プロセスタスクリストにアクセスし、すべてのユーザーに対してこの情報が表示するために使用されます。

NBU_Admin ユーザーグループのメンバーではないユーザーが、OS 管理者 (管理者または root) としてログオンしている場合:

- ユーザーは、NetBackup 管理コンソールまたはコマンドラインからサービスを再起動できます。
- ユーザーは、NetBackup 管理コンソールからサービスを停止できます。コマンドラインから停止することはできません。

NBU_Admin ユーザーグループのメンバーであるユーザーが、OS 管理者 (`root`) としてログオンしていない場合: この場合、ユーザーは NetBackup 管理コンソールまたはコマンドラインからデーモンを再起動できません。ユーザーは、次のコマンドラインからのみデーモンを再起動できます。

```
/etc/init.d/netbackup start
```

NBU_Admin ユーザーグループのメンバーであるユーザーが、OS 管理者 (管理者) としてログオンしていない場合:

- ユーザーは、NetBackup 管理コンソールまたはコマンドラインからサービスを再起動できません。
- ユーザーは、NetBackup 管理コンソールからサービスを停止できません。ただし、コマンドラインを使用してサービスを停止できます。
  (`bprdreq -terminate`、`bpdbm -terminate`、`stopltid` など)

NBU_Admin ユーザーグループのメンバーであるユーザーが、OS 管理者 (root) としてログオンしていない場合があります。この場合、ユーザーは NetBackup 管理コンソールまたはコマンドラインからデーモンを再起動できません。

ホストプロパティの認可オブジェクトの権限

次の表に、ホストプロパティの認可オブジェクトに関連する権限を示します。

表 14-28 ホストプロパティの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	X	X	X	X	X
読み込み	読み込み	X	X	X	X	X	X	X
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	--

ライセンスの認可オブジェクトの権限

次の表に、ライセンスの認可オブジェクトに関連する権限を示します。

表 14-29 ライセンスの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	X	X	X	X	X
読み込み	読み込み	X	X	X	X	X	X	X
構成	割り当て	---	X	---	---	---	---	---
	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

ボリュームグループの認可オブジェクトの権限

次の表に、ボリュームグループの認可オブジェクトに関連する権限を示します。

表 14-30 ボリュームグループの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

ボリュームプールの認可オブジェクトの権限

次の表に、ボリュームプールの認可オブジェクトに関連する権限を示します。

表 14-31 ボリュームプールの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
構成	割り当て	---	X	---	---	---	---	---
	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

デバイスホストの認可オブジェクトの権限

次の表に、デバイスホストの認可オブジェクトに関連する権限を示します。

メモ: DevHost オブジェクトは、[メディアおよびデバイスの管理 (Media and Device Management)]>[クレデンシャル (Credentials)]ノードへのアクセスを制御します。

表 14-32 デバイスホストの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	X	---	---	X	---
読み込み	読み込み	X	X	X	---	---	X	---
操作	停止	X	X	---	---	---	---	---
	同期化	X	X	---	---	---	---	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

セキュリティの認可オブジェクトの権限

次の表に、セキュリティの認可オブジェクトに関連する権限を示します。

表 14-33 セキュリティの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	---	---	---	---	X	---	---
読み込み	読み込み	---	---	---	---	X	---	---
構成	セキュリティ	---	---	---	---	X	---	---

ファットサーバーの認可オブジェクトの権限

次の表に、ファットサーバーの認可オブジェクトに関連する権限を示します。

表 14-34 ファットサーバーの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	X	---	---	---	---

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
読み込み	読み込み	X	X	X	---	---	---	---
構成	変更	---	X	X	---	---	---	---
	SAN 構成の変更	---	---	X	---	---	---	---

ファットクライアントの認可オブジェクトの権限

次の表に、ファットクライアントの認可オブジェクトに関連する権限を示します。

表 14-35 ファットクライアントの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	X	---	---	---	---
読み込み	読み込み	X	X	X	---	---	---	--
操作	検出	---	X	X	---	---	---	---
構成	変更	---	X	X	---	---	---	---

権限Vault の認可オブジェクト

次の表に、Vault の認可オブジェクトに関連する権限を示します。

表 14-36 Vault の認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	---	X	---	---	---	X	---
読み込み	読み込み	---	X	---	---	---	X	---
操作	コンテナの管理	---	X	---	---	---	X	---
	レポートの実行	---	X	---	---	---	X	---

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
構成	変更	---	X	---	---	---	---	---
	セッションの実行	---	X	---	---	---	---	---

サーバーグループの認可オブジェクトの権限

次の表に、サーバーグループの認可オブジェクトに関連する権限を示します。

表 14-37 サーバーグループの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---
	変更	---	X	---	---	---	---	---

キー管理システム (kms) グループの認可オブジェクトの権限

次の表では、キー管理システムグループの認可オブジェクトに関連する権限を示します。

表 14-38 キー管理システムグループの認可オブジェクトの権限

セット	動作	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault Operator	NBU_KMS Admin
参照	参照	---	X	---	---	---	---	X
読み込み	読み込み	---	X	---	---	---	---	X
構成	新規	---	---	---	---	---	---	X
	削除	---	---	---	---	---	---	X
	変更	---	---	---	---	---	---	X

NetBackup アクセス制御 (NBAC) のアップグレード

メモ: NBAC が有効になっている場合、NBAC は NetBackup アップグレードの一部としてアップグレードされます。NetBackup のアップグレード方法については、『NetBackup Upgrade Guide』を参照してください。アップグレードが実行されるときに現在のAT および AZ サービスが動作していることを確認してください。NetBackup がクラスタサーバーで動作している場合は、NetBackup が動作してアップグレードが実行されているアクティブノードで両方のサービスが動作していることを確認してください。

次の手順では、NetBackup アクセス制御 (NBAC) のアップグレード方法について説明します。

NetBackup アクセス制御 (NBAC) のアップグレード

1. プライマリサーバーで、NetBackup を停止します。
2. NetBackup をアップグレードします。

   メディアサーバーおよびクライアントコンピュータで、NetBackup を停止した後、NetBackup をアップグレードします。共有の認証と認可のパッケージは、メディアサーバーおよびクライアントコンピュータで使われなくなります。これらの製品が他の Veritas 製品で使用されていない場合には、これらを削除できます。

サーバーの変更を NBAC と一緒に使った場合の構成要件

NetBackup アクセス制御が使われる場合にサーバーの変更操作を実行するには、追加の構成が必要になります。

次の手順では、NBAC がすでに構成されていることを想定しています。

サーバーの変更操作をサポートするための設定: *fromServer -> toServer*

- *toServer* のホストプロパティの追加サーバーリストに、*fromServer* を追加します。
- *fromServer* と *toServer* が異なる NetBackup ドメイン (異なるプライマリサーバーのメディアサーバー) にある場合:
  - *fromServer* と *toServer* のプライマリサーバーの間で信頼を設定するために `vssat` コマンドを使用します。
  - *fromServer* のプライマリサーバーを、*toServer* のホストプロパティの追加サーバーリストに追加します。
- *fromServer* または *toServer* がメディアサーバーの場合:

- 必要に応じて、bpnbaz -ProvisionCert コマンドを使用して、セキュリティ (マシン) 証明書を配備します。

追加の設定手順

auth.conf ファイルを使う場合:

- 各サーバーの auth.conf ファイルに USER エントリを追加します。
- NBAC が有効な場合は、各サーバーで nbsetconfig を実行して、エントリ USE_AUTH_CONF_NBAC = YES を追加します。

リモート管理コンソールを使う場合:

- vssat コマンドを使用するか、少なくとも 1 度各サーバーに明示的にログオンして、各プライマリサーバーに信頼を設定します。

設定後にトラブルシューティングを行う場合は、サーバー通信を検査するために nslookup と bptestnetconn -a -s を使います。

15

多要素認証の構成

この章では以下の項目について説明しています。

多要素認証について

多要素認証は、複数の手順から成るアカウントログインプロセスで、パスワードとともに 6 桁のワンタイムパスワードを入力する必要があります。

アカウントのセキュリティを保護するために多要素認証を構成することをお勧めします。

p.249 の「ユーザーアカウントに対する多要素認証の構成」を参照してください。

NetBackup ドメインで多要素認証が適用されている場合、サインインが成功するように、すべてのユーザーが自分のユーザーアカウントに対して多要素認証を構成する必要があります。

p.250 の「ドメインで適用されている場合のユーザーアカウントに対する多要素認証の構成」を参照してください。

ユーザーアカウントに対する多要素認証の構成

セキュリティを高めるために、ユーザーアカウントに多要素認証を構成できます。最初に、ワンタイムパスワードを提供するスマートデバイスに認証アプリケーションをインストールして構成する必要があります。

NetBackup 管理者が NetBackup ドメインに多要素認証を適用した場合、サインインが成功するように、ユーザーアカウントに対して多要素認証を構成する必要があります。

p.249 の「ユーザーアカウントの多要素認証の無効化」を参照してください。

ユーザーに対して多要素認証を構成するには

1. NetBackup Web UI にサインインします。
2. 右上で、プロファイルアイコンをクリックして[多要素認証を構成 (Configure multi-factor authentication)]をクリックします。
3. [多要素認証を構成 (Configure multi-factor authentication)]画面で、[構成 (Configure)]をクリックします。
4. 次の画面で、指定された手順に従います。

   認証アプリケーションをスマートデバイスにインストールして構成します。ワンタイムパスワードが生成され、スマートデバイスに送信されます。

   サポートされている認証アプリケーション
5. 認証アプリケーションで QR コードをスキャンするか、手動でキーを入力します。
6. スマートデバイスの認証アプリケーションに表示されたワンタイムパスワードを入力してください。
7. [構成 (Configure)]をクリックします。

   次回のサインイン時に、ユーザー名とパスワードとともにワンタイムパスワードを入力する必要があります。

ユーザーアカウントの多要素認証の無効化

多要素認証が適用されている場合は、ユーザーアカウントの多要素認証を無効化できます。ただし、アカウントのセキュリティを保護するために多要素認証を構成することを強く推奨します。

p.249 の「ユーザーアカウントに対する多要素認証の構成」を参照してください。

ユーザーアカウントの多要素認証を無効化するには

1. NetBackup Web UI にサインインします。
2. 右上で、プロファイルアイコンをクリックして[多要素認証を構成 (Configure multi-factor authentication)]を選択します。

3 ユーザーアカウントに多要素認証をすでに構成している場合は、[無効化 (Disable)] オプションが表示されます。

4 [無効化 (Disable)]をクリックします。

5 ワンタイムパスワードを入力し、[確認 (Confirm)]をクリックします。

すべてのユーザーへの多要素認証の適用

NetBackup 管理者だけが、すべての NetBackup ユーザーに多要素認証を適用できます。

すべてのユーザーに多要素認証を適用するには

1 NetBackup Web UI にサインインします。

2 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。

3 [セキュリティ制御 (Security controls)]タブで、[多要素認証を適用 (Enforce multi-factor authentication)]をオンにします。

[確認 (Confirm)]をクリックして、すべての NetBackup ユーザーに多要素認証を適用します。

正常にサインインできるように、ユーザーアカウントの多要素認証を構成する必要があることをすべてのユーザーに通知します。

p.249 の「ユーザーアカウントに対する多要素認証の構成」を参照してください。

ドメインで適用されている場合のユーザーアカウントに対する多要素認証の構成

多要素認証がドメインに適用された後、ユーザーアカウント用に構成する必要があります (まだ構成していない場合)。適用後にアカウントの多要素認証を構成しない場合は、サインインできません。

適用後に多要素認証を構成するには

1 Web ブラウザを開き、次の URL に移動します。

https://*primaryserver*/webui/login

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

2 NetBackup のサインイン画面に移動します。

3 ユーザー名とパスワードを入力します。

4 [サインイン (Sign in)]をクリックします。[多要素認証を構成 (Configure multi-factor authentication)]画面が表示されます。

5 次の画面で、指定された手順に従います。

認証アプリケーションをスマートデバイスにインストールして構成します。ワンタイムパスワードが生成され、スマートデバイスに送信されます。

サポートされている認証アプリケーション

6 認証アプリケーションで QR コードをスキャンするか、手動でキーを入力します。

7 スマートデバイスの認証アプリケーションに表示されたワンタイムパスワードを入力してください。

8 [構成 (Configure)]をクリックします。

構成が正常に完了すると、サインイン画面に戻ります。

正常にサインインするために、ユーザー名、パスワード、ワンタイムパスワードを入力します。

ユーザーの多要素認証のリセット

NetBackup 管理者だけが、他の NetBackup ユーザーの多要素認証をリセットできます。

NetBackup ユーザーの多要素認証をリセットするには

1 NetBackup Web UI にサインインします。

2 右上で、[設定 (Settings)]、[グローバルセキュリティ (Global security)]の順に選択します。

3 [セキュリティ制御 (Security controls)]タブをクリックします。

4 [ユーザーの多要素認証をリセット (Reset multi-factor authentication for a user)]セクションで[リセット (Reset)]をクリックします。

5 多要素認証をリセットするユーザーを選択します。

6 [リセット (Reset)]をクリックします。

7 プロンプトが表示されたら、ワンタイムパスワードを入力し、[確認 (Confirm)]をクリックします。

16

マルチパーソン認証の構成

この章では以下の項目について説明しています。

マルチパーソン認証について

NetBackup セキュリティ管理者は、マルチパーソン認証を構成できます。NetBackup プライマリサーバーを望ましくない行為または悪意のある行為からプロアクティブに保護するために、その処理の実行が許可される前に、第 2 の認可済みユーザーが処理を承認するようにします。特定の操作に対してマルチパーソン認証を構成する場合、関連付けられた操作は、NetBackup Web UI または REST API を使用してのみ実行できます。NetBackup 管理コンソールを使用して操作を実行することはできません。

マルチパーソン認証をバイパスするために、必要な操作を実行するための承認を必要としない除外されるユーザーとして関連付けられたユーザーを追加できます。

NetBackup でマルチパーソン認証を構成するには、2 人のユーザー (1 人が要求元、もう 1 人が承認者) が必要です。

要求元は、自身のチケットの承認者になることはできません。

用語

- チケット - チケットは、重要な操作を実行するためのマルチパーソン認証要求です。
- 要求元 - 要求元は、マルチパーソン認証を必要とする重要な操作を実行するエンドユーザーです。
- 承認者 - 承認者は、チケットを承認することでマルチパーソン認証を必要とする操作を確認し、許可する個人です。
- 除外されるユーザー - 除外されるユーザーはマルチパーソン認証プロセスを通過する必要はありません。非対話型の重要な操作を実行するユーザーのみを除外できます。
  セキュリティを強化するために、除外されるユーザーを含めないことをお勧めします。

NetBackup 操作に対してマルチパーソン認証を構成するためのワークフロー

NetBackup 操作に対してマルチパーソン認証を構成するための手順の概要を次に示します。

表 16-1

手順	説明
手順 1	マルチパーソン認証が必要な重要な NetBackup 操作を特定します。 p.258 の「マルチパーソン認証が必要な NetBackup 操作」を参照してください。
手順 2	要求またはマルチパーソン認証チケットを承認できる承認者を特定します。
手順 3	承認者にデフォルトのマルチパーソン認証の承認者 RBAC の役割を割り当てます。 p.254 の「マルチパーソン認証に対する RBAC の役割と権限」を参照してください。
手順 4	NetBackup Web UI を使用してマルチパーソン認証を構成します。 p.258 の「マルチパーソン認証の構成」を参照してください。

手順	説明
手順 5	ユーザーまたは要求元が、マルチパーソン認証 (イメージの期限切れなど) を必要とする操作を実行しようとすると、チケットが生成されます。 初期状態では、チケットは保留中の状態です。
手順 6	チケットは、NetBackup Web UI のすべてのマルチパーソン認証の承認者に表示されます。この承認者は、チケット情報を確認し、チケットを承認または拒否できます。
手順 7	承認者がチケットを承認または拒否すると、要求元に通知されます。

マルチパーソン認証の構成は、管理者またはセキュリティ管理者が、マルチパーソン認証を必要とする重要な操作を有効にし、有効期限やパージ期間などのその他の設定を指定すると開始されます。

マルチパーソン認証の構成チケットが生成されます。承認者がチケットを承認すると、マルチパーソン認証の構成が有効になります。

マルチパーソン認証の初期構成

マルチパーソン認証の初回構成で、デフォルトのマルチパーソン認証の承認者の役割にユーザーを追加する必要があります。データセキュリティを強化するためにマルチパーソン認証の使用を開始するために、セキュリティ管理者は、デフォルトのマルチパーソン認証承認者の役割を持つユーザーからの追加の承認を求める、重要な事前定義済み操作に対してマルチパーソン認証を有効にする必要があります。

最初に、セキュリティ管理者はマルチパーソン認証チケットとなるマルチパーソン認証を構成する必要があります。承認者がチケットを承認すると、指定された NetBackup 操作 (イメージの有効期限切れなど) でマルチパーソン認証が必須になります。管理者またはセキュリティ管理者は、任意の時点でユーザーをデフォルトのマルチパーソン認証の承認者の役割に追加できます。

マルチパーソン認証に対する RBAC の役割と権限

マルチパーソン認証の構成では、ユーザーに次の RBAC の役割が割り当てられている必要があります。

- 管理者
- デフォルトのセキュリティ管理者
- デフォルトのマルチパーソン認証の承認者

これらの RBAC の役割を持つユーザーには、次の権限が必要です。

表 16-2

RBAC の役割	権限
管理者	マルチパーソン認証の構成を表示、更新し、他のユーザーに構成権限を委任します。 チケットを表示、更新し、他のユーザーにチケットの権限を委任します。
デフォルトのセキュリティ管理者	マルチパーソン認証の構成を表示、更新し、他のユーザーに構成権限を委任します。
デフォルトのマルチパーソン認証の承認者	チケットを表示して更新します。
デフォルトのオペレータ	すべての NetBackup エンティティを表示します。

役割に関するマルチパーソン認証プロセス

ユーザーは、要求元と承認者に同時になることができますが、自分のチケットを承認することはできません。

役割に関するマルチパーソン認証プロセスフローは次のようになります。

表 16-3

コンポーネント	説明
マルチパーソン認証チケット	マルチパーソン認証によって保護されている重要な NetBackup 操作を要求元が実行すると、特定の処理を実行する前に承認者からの承認を必要とするチケットが生成されます。 このチケットは、重要な処理が実行される前に、複数のユーザーによるレビュープロセスを確実に経るようにするために NetBackup で使用されます。 次のサンプルフローは、マルチパーソン認証が必要なイメージの有効期限切れ操作用です。 **1** 要求元は、NetBackup Web UI を使用してイメージを期限切れにします。 **2** チケットが作成されます。 **3** チケットの承認が保留されています。 **4** 承認者はチケットを確認します。 **5** 承認者は、チケットを承認または拒否します。 **6** 承認後、NetBackup によってチケットがスケジュールされ、最終的に、実行された後に[完了 (Done)]とマーク付けされます。 **7** チケットのアクティビティログ、要求、および応答の詳細は、Web UI を使用して承認者または要求元が[チケットの詳細 (Ticket details)]ページで表示できます。 **8** 有効期限を過ぎると、チケットの有効期限が切れます。そのようなチケットは、要求元によって更新されない限り承認できません。 **9** [完了 (Done)]、[拒否 (Rejected)]、[期限切れ (Expired)]、[キャンセル (Canceled)]の状態のチケットは、指定したパージ期間 (日数) に処理が実行されないとパージされます。

コンポーネント	説明
要求元の役割	**1** 要求元は、マルチパーソン認証を必要とする操作を開始するユーザーです。 **2** ユーザーが除外されるユーザーの一覧に含まれていない場合、操作のチケットが作成されます。 **3** 操作が実行される前に、承認者によるチケットの承認が必要です。 **4** 要求元が承認者、管理者、またはセキュリティ管理者でもある場合でも、要求元が自己承認することは許可されません。 **5** 作成されたチケットは、保留状態になります。 **6** 要求元は、チケットが保留状態にある場合にのみ、チケットを取り消すことができます。 **7** 有効期限を経過したチケットは期限切れの状態に移行します。 **8** 要求元のみがそのようなチケットを更新できます。マルチパーソン認証の構成設定に基づいて、更新されたチケットの新しい有効期限が計算されます。
承認者の役割	**1** 承認者は、チケットを確認し、チケットを承認する認可された個人です。 **2** 承認者はチケットの詳細を評価し、評価に基づいてチケットを承認または拒否します。 **3** 承認後、チケットの実行がスケジュールされます。 **4** 承認者になるには、ユーザーがチケットの更新、チケットの表示などの RBAC 権限を持っているか、ユーザーにデフォルトのマルチパーソン認証承認者の役割が必要です。 **5** 保留状態にあるチケットは、承認または拒否できます。
除外されるユーザー	**1** 除外されるユーザーとは、マルチパーソン認証ワークフローの適用を受けていない個人です。 **2** これにより、承認の必要性はなくなりますが、慎重に使用する必要があります。 **3** 除外されたユーザーアカウントがハッキングされた場合、マルチパーソン認証プロセスはこのユーザーによってバイパスされるため、役に立たなくなります。 **4** たとえば、アリスが除外されるユーザーとして指定され、イメージを期限切れにしようとすると (マルチパーソン認証を適用すべき操作)、イメージは、チケットの生成と追加の承認をせずに自動的に期限切れになります。

マルチパーソン認証が必要な NetBackup 操作

次の操作ではマルチパーソン認証が必要なため、次の操作にチケットが生成されます。

- マルチパーソン認証の構成
- マルチパーソン認証を必要とする操作の有効化と無効化
- 除外ユーザーの追加
- マルチパーソン認証の設定を変更すると、チケットが生成されます
- イメージを期限切れに設定
- イメージの削除

イメージの有効期限設定にマルチパーソン認証が構成されている場合でも、次の操作にはマルチパーソン認証は必要ありません。

- イメージの保持レベルの値の変更
- ポリシーと SLP の保持レベルの変更
- `nbstlutil` コマンドを使用した、不完全な SLP の取り消し:
  『NetBackup コマンドリファレンスガイド』を参照してください。

マルチパーソン認証の構成

NetBackup 操作に対するマルチパーソン認証の構成は、NetBackup Web UI からのみサポートされます。管理者またはセキュリティ管理者は、重要な NetBackup 操作に対してマルチパーソン認証を構成できます。

NetBackup 操作に対してマルチパーソン認証を構成するには

1. セキュリティ管理者アカウントを使用して NetBackup Web UI にサインインします。
2. 左ペインで、[セキュリティ (Security)]、[マルチパーソン認証 (Multi-person authorization)]の順にクリックします。
3. [マルチパーソン認証の構成 (Configure multi-person authorization)]オプションをクリックします。
4. マルチパーソン認証を構成する重要な操作を選択します。
5. マルチパーソン認証から除外されるユーザーを選択します。
6. [保存 (Save)]をクリックします。
7. [構成 (Configure)]をクリックします。

   関連付けられた操作に対してマルチパーソン認証チケットが作成されます。承認者がチケットを承認すると、操作は MPA の対象となります。

マルチパーソン認証チケットの表示

ユーザーは、自分のマルチパーソン認証チケットを表示できます。

1. NetBackup Web UI にサインインします。
2. 左ペインで、[セキュリティ (Security)]、[マルチパーソン認証 (Multi-person authorization)]の順にクリックします。マルチパーソン認証チケットのリストが表示されます。

   チケット ID をクリックすると、詳細が表示されます。

マルチパーソン認証チケットの管理

承認者の役割を持つユーザーは、マルチパーソン認証チケットを承認または拒否できます。

マルチパーソン認証チケットを管理するには

1. NetBackup Web UI にサインインします。
2. 左ペインで、[セキュリティ (Security)]、[マルチパーソン認証 (Multi-person authorization)]の順にクリックします。マルチパーソン認証チケットのリストが表示されます。
3. チケット ID をクリックすると、要求の詳細が表示されます。
4. [承認 (Approve)]または[拒否 (Reject)]をクリックします。選択した処理に基づいて、それぞれのダイアログボックスが表示されます。
5. コメントを追加し、[承認 (Approve)]または[拒否 (Reject)]をクリックします。

除外されるユーザーの追加

マルチパーソン認証プロセスから特定のユーザーを除外できます。

除外されるユーザーは通常、自動化ユーザーか、マルチパーソン認証を必要としないスクリプトです。マルチパーソン認証の構成には、除外されるユーザーが含まれないデフォルト設定があり、これが推奨されるセキュリティ設定になります。一部のユーザーアカウントを除外して、二次承認なしで重要なデータ操作を続行する必要が組織にある場合は、そのようなユーザーを除外されるユーザーのリストに追加します。

メモ: ユーザーグループは除外リストに追加できません。

除外されるユーザーを追加するには

1. NetBackup Web UI にサインインします。
2. 左ペインで、[セキュリティ (Security)]、[マルチパーソン認証 (Multi-person authorization)]の順に選択します。
3. 右上で[マルチパーソン認証の構成 (Configure multi-person authorization)]をクリックします。
4. [除外されるユーザー (Exempted users)]セクションで、[追加 (Add)]をクリックします。
5. マルチパーソン認証プロセスから除外するユーザーの名前を指定します。
6. [リストへの追加 (Add to List)]、[保存 (Save)]の順に選択します。
7. [保存 (Save)]をクリックします。

マルチパーソン認証チケットの有効期限とパージのスケジュール

有効期限は構成可能なオプションで、マルチパーソン認証チケットを保留状態にできる期間を定義します。構成した有効期限を超えて保留状態のままのチケットは、期限切れになります。

マルチパーソン認証構成の場合、有効期限は最短で 24 時間から 168 時間までで設定できます。デフォルトでは、チケットは 72 時間後に期限切れになります。

パージ期間は構成可能なオプションで、チケットがチケットデータベースに存在する期間を定義します。チケットをパージすると、データベースが急に大きくなることがなくなります。パージ期間は最短で 3 日から 30 日までで設定できます。

デフォルトでは、チケットは 72 時間後にパージされます。指定したパージ期間が経過すると、[完了 (Done)]、[期限切れ (Expired)]、[拒否済み (Rejected)]、[キャンセル (Canceled)]のチケットはすべてパージされます。

チケットの有効期限とパージをスケジュール設定するには

1. NetBackup Web UI にサインインします。
2. 左ペインで、[セキュリティ (Security)]、[マルチパーソン認証 (Multi-person authorization)]の順に選択します。
3. 右上で[マルチパーソン認証の構成 (Configure multi-person authorization)]をクリックします。
4. [スケジュール (Schedules)]セクションで、[編集 (Edit)]をクリックします。

5 [チケットの有効期限: (Expire ticket after)]オプションに有効期限 (時間) を指定します。

[次を過ぎるとチケットをパージ: (Purge ticket after)]オプションにパージ期間 (日) を指定します。

6 [保存 (Save)]をクリックします。

7 [保存 (Save)]をクリックします。

マルチパーソン認証の無効化

場合によっては、関連付けられた操作に対して一時的にマルチパーソン認証を無効にする必要がある場合があります。

関連するすべての操作でマルチパーソン認証を無効にするには、root または管理者アカウントを使用して `bpnbat -login -loginType WEB` を実行した後、次のコマンドを実行します。

```
nbseccmd -disableMPA
```

NetBackup Web UI を使用して、特定の操作に対するマルチパーソン認証を無効にできます。

特定の操作に対するマルチパーソン認証を無効にするには

1 NetBackup Web UI にサインインします。

2 左ペインで、[セキュリティ (Security)]、[マルチパーソン認証 (Multi-person authorization)]の順に選択します。

3 右上で[マルチパーソン認証の構成 (Configure multi-person authorization)]をクリックします。

4 マルチパーソン認証を構成する操作のセクションで、[編集 (Edit)]をクリックします。

5 マルチパーソン認証を無効にする操作のチェックボックスのチェックマークをはずします。

6 [保存 (Save)]をクリックします。

7 [保存 (Save)]をクリックします。

これにより、チケットが生成され、その操作名はチケットの詳細ページで[MPA の構成 (MPA Configuration)]になります。

関連する操作では、それぞれのチケットの承認後にのみ、マルチパーソン認証が無効になります。

2

移動中のデータの暗号化

17

NetBackup CA および NetBackup 証明書

この章では以下の項目について説明しています。

NetBackup のセキュリティ証明書の概要

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。セキュリティ証明書は、X.509 公開鍵基盤 (PKI) 標準に適合しています。プライマリサーバーは、認証局 (CA) として動作し、ホストにデジタル証明書を発行します。

NetBackup 8.0 より前で生成され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。NetBackup は、これらの古い証明書を新しいホスト ID ベースの証明書に置き換える移行を進めています。この移行は今後のリリースで完了し、ホスト名ベース証明書は使用されなくなる予定です。

ただし、移行はまだ完了していないため、NetBackup では一部の操作で過去のホスト名ベースの証明書が引き続き必要になります。以下の表に、ホスト名ベースの証明書が必要なさまざまな操作を示します。

メモ: すべての NetBackup 8.1 のホストで、ホスト ID ベースの証明書が必要です。

表 17-1 NetBackup 8.1 ホストでのホスト名ベースの証明書要件

操作またはコンポーネント	必要な証明書の種類
NetBackup アクセス制御 (NBAC)	NBAC が有効になっている NetBackup ホストには、ホスト名ベースの証明書が必要です。これらの証明書は NBAC を有効にすると自動的に配備されます。
クラウドストレージ	これは、バージョン 8.0 から 8.1.2 の NetBackup メディアサーバーにのみ適用されます。 NetBackup CloudStore Service Container では、メディアサーバーにホスト名ベースの証明書がインストールされている必要があります。証明書がインストールされていない場合、サービスコンテナは起動できません。 p.292 の「ホスト名ベースの証明書の配備」を参照してください。

NetBackup での安全な通信について

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 8.1 のホストが通信を行うには、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 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 ホスト間のすべての制御通信 (または制御チャネル) は、トランスポート層セキュリティ (TLS) プロトコルバージョン 1.2 と X.509 証明書を使用して保護されます。制御通信は、NetBackup ソフトウェアによるバックアップ、アーカイブおよびリストア操作の開始、制御、監視に使用されます。

データ通信は、NetBackup を使用してバックアップされるデータで構成されます。セキュリティポリシーは、バックアップ管理者に対して、NetBackup クライアントがメタデータとデータを NetBackup サーバーに送信するチャネルが安全であることを保証することを要求します。NetBackup 10.0 以降では、バックアップイメージとメタデータは安全な通信によって回線を介して暗号化されます。この機能は、データチャネルの暗号化または移動中のデータの暗号化 (DTE) と呼ばれます。

次のチャネルはデータチャネルとして分類されます。

- tar ストリーム (クライアントからメディアサーバー): これは、クライアントとメディアサーバー間で tar またはデータストリームが送信されるチャネルです。バックアップ操作の間に、メディアサーバーはクライアントからデータを受信し、ストレージに送信します (OST プラグイン経由など)。リストア時には方向が逆になります。
- tar ストリーム (メディアサーバーからメディアサーバー): このチャネルは複製中に使用されます。
- カタログ情報 (クライアントからメディアサーバー): これは、クライアントとメディアサーバー間でカタログ情報と制御コマンドが送信されるチャネルです。このチャネルを介して送信されるデータの量は、バックアップを構成するファイルとディレクトリの数に比例します。メディアサーバーは、クライアントから受信したカタログ情報をプライマリサーバーに送信します。
- カタログ情報 (メディアサーバーからプライマリサーバー): これは、メディアサーバーからプライマリサーバーにカタログ情報が送信されるチャネルです。

Web UI では、[設定 (Settings)] (右上の歯車アイコン) で安全な通信の設定を使用できます。次に、[グローバルセキュリティ (Global security)]をクリックします。

p.267 の「ホスト管理について」を参照してください。

p.269 の「ホスト ID からホスト名へのマッピングの追加」を参照してください。

p.283 の「グローバルセキュリティ設定について」を参照してください。

p.283 の「安全な通信の設定について」を参照してください。

p.288 の「ディザスタリカバリ設定について」を参照してください。

nbhostmgmt と nbhostidentity の 2 つのコマンド、および機能強化された nbcertcmd と nbseccmd では、証明書の配備とその他のセキュリティ設定を管理するオプションを指定できます。

セキュリティ管理ユーティリティについて

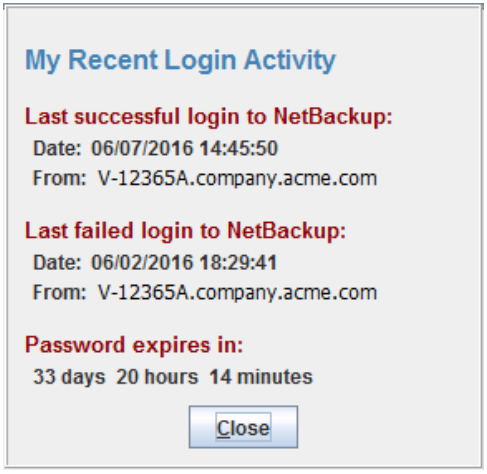
NetBackup 管理コンソールの[セキュリティ管理 (Security Management)]ノードは、NetBackup プライマリサーバーの管理者に対してのみ表示されます。

[セキュリティ管理 (Security Management)]には、ログイン処理の表示、ホスト ID ベースの証明書の管理、ドメインでの安全な通信の構成を行うユーティリティが用意されています。

- [セキュリティイベント (Security Events)]を使うと、現在の管理者のログインの詳細と、証明書、トークン、ホスト、セキュリティ構成に対して行われたユーザー始動の変更を表示できます。ホスト接続についての詳細を表示することもできます。
- [ホスト管理 (Host Management)]ノードを使って、ホスト ID のホスト名へのマッピングの追加または承認、ホストのリセット、ホストへのコメントの追加などの NetBackup ホスト操作を実行します。
  p.267 の「[ホスト (Hosts)]タブ」を参照してください。
- 表示、無効化、再発行などの証明書に固有の操作を実行するには、[証明書管理 (Certificate Management)]ノードを使います。
  p.295 の「証明書管理ユーティリティを使ったホスト ID ベースの証明書の発行と配備」を参照してください。
- [グローバルセキュリティ設定 (Global Security Settings)]ノードを使って、安全でない通信の有効化、ディザスタリカバリパッケージのパスフレーズ、証明書の配備レベルなどのセキュリティ設定を構成します。
  p.283 の「グローバルセキュリティ設定について」を参照してください。

ログイン処理について

NetBackup は、ユーザーのアクセス履歴についての情報を取得し、ユーザーのパスワードが期限切れになる時点を追跡します。この情報は、NetBackup 管理コンソールの右上隅にある[最近のログイン処理 (My Recent Login Activity)]ウィンドウに表示されます。



[最近のログイン処理 (My Recent Login Activity)]ウィンドウは、NetBackup 管理コンソールを使い始めると閉じます。

パスワードの期限切れ情報は次のシナリオでは利用できません。

- NetBackup 管理コンソールのシングルサインオン (SSO) 機能を使用してプライマリサーバーにリモートログインしている場合
- NetBackup 管理コンソールを使用して UNIX または Linux プライマリサーバーにログインしている場合

メモ: ログインとパスワード期限切れの詳細は、NetBackup 管理コンソールに初めて正常にログイン、ログアウトした後のみに表示されます。

ログインの詳細は自動的に更新されません。前回のログイン詳細についての最新情報を表示するには、NetBackup 管理コンソールからログオフして再度ログインする必要があります。

この情報は[アクセス履歴 (Access History)]タブの[セキュリティイベント (Security Events)]にも表示されます。

ホスト管理について

[セキュリティ管理 (Security Management)] > [ホスト管理 (Host Management)]ノードでは、ホスト名をそれぞれのホスト ID にマッピングすることができます。ホスト ID とホスト名間の適切なマッピングは、安全なホストの通信のために重要です。

p.264 の「NetBackup での安全な通信について」を参照してください。

p.269 の「ホスト ID からホスト名へのマッピングの追加」を参照してください。

p.279 の「NetBackup ホスト属性のリセット」を参照してください。

[ホスト (Hosts)]タブ

[ホスト (Hosts)]タブには、次の情報が示されます。

ホスト	ホストの名前。 **メモ:** [ホスト管理 (Host Management)]ノードには、ホスト ID を持つホストのみが表示されます。
マッピング済みのホスト名/IP アドレス (Mapped Host Names / IP Addresses)	選択したクライアントのホスト ID にマッピングされているホスト名または IP アドレス。 p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

バージョン	ホストにインストールされている NetBackup のバージョン。
証明書の有効期間の自動再発行を許可する	再発行トークンを要求せずにホストで証明書を再発行できる時間。 デフォルトでは、[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)]オプションの有効期間は 48 時間です。 p.281 の「証明書の自動再発行の許可または禁止」を参照してください。
オペレーティングシステム (Operating System)	ホストにインストールされているオペレーティングシステムのバージョン。
OS 形式 (OS Type)	ホストにインストールされているオペレーティングシステム の形式 (Windows または UNIX)。
CPU アーキテクチャ	ホストで使われている CPU のアーキテクチャ。
安全性 (Secure)	ホストの通信状態が安全かどうかが示されます。 ホストが 8.1 の場合、通信状態は安全であり、ホストは安全に通信できます。
コメント	ホストに対して追加したコメントまたは追加情報。
ハードウェアの説明 (Hardware Description)	ホストで使われているハードウェア。
NetBackup ホスト ID (Host ID)	ホストの一意の識別子。
NetBackup EEB (EEBs)	NetBackup EEB (Emergency Engineering Binary) がインストールされているかどうかが示されます。
サーバー (Servers)	ホストに関連付けられている追加のサーバー。
マスターサーバー	ホストに関連付けられているプライマリサーバーホスト。
発行日 (Issued On)	ホスト ID ベースの証明書がホストに発行された日付。
最終更新日時	ホスト ID ベースの証明書が更新された日付。
VxUpdate プラットフォーム (VxUpdate Platform)	ホストをアップグレードするために必要な VxUpdate パッケージを識別します。
インストール済みパッケージ (Installed Packages)	ホストにインストールされている NetBackup パッケージ。

ホスト ID からホスト名へのマッピングの追加

ホストには、ホスト名または IP アドレスが複数関連付けられている場合があります。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および 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。

通信中に NetBackup がホスト ID に関連する新しいホスト名または IP アドレスを検出することがあります。このホスト名または IP アドレスは、正常に通信するために、それぞれのホスト ID に自動または手動でマッピングできます。

[セキュリティ管理 (Security Management)]、[グローバルセキュリティ設定 (Global Security Settings)]の順に選択した[安全な通信 (Secure Communication)]タブの[ホスト ID をホスト名に自動的にマッピングする (Automatically map host ID to host names)]オプションが選択されている場合、システムによって検出されたホスト名または IP アドレスが、それぞれのホスト ID に自動的にマッピングされます。

p.287 の「ホスト ID をホスト名と IP アドレスに自動的にマッピングする」を参照してください。

重要な注意事項

ホスト ID からホスト名へのマッピングに固有の次の注意事項を確認してください。

- DHCP (Dynamic Host Configuration Protocol) ホストの場合、通信中にシステムによって動的 IP アドレスが検出され、ホスト ID からホスト名へのマッピングとして追加されることがあります。このようなマッピングは削除する必要があります。
- クラスタ設定の場合、ホスト名、仮想名の FQDN (完全修飾ドメイン名) がホスト通信中に検出されます。
- 既存のホスト 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再配備すると、新しい証明書が配備され、新しいホスト ID がホストに発行されます。これは、NetBackup により別のホストと見なされるためです。このような状況を回避するには、利用可能なすべてのホスト名を既存のホスト ID にマッピングする必要があります。
- NetBackup Snapshot Manager を NetBackup に登録すると、生成された証明書がそれらの間で交換されます。そのため、NetBackup Snapshot Manager の[ホストマッピング (Host Mapping)]には、NetBackup Snapshot Manager ホストの代わりに、NetBackup Snapshot Manager コンテナの詳細が表示されます。

特定のホスト ID を対応するホスト名または IP アドレスに手動でマッピングするには、次の手順を使用します。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

p.272 の「ホスト ID からホスト名へのマッピングの削除」を参照してください。

ホスト ID からホスト名へのマッピングを追加するには

1. NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. [ホスト (Hosts)]タブの詳細ペインで、変更するホストを右クリックします。
3. [ホストマッピングを追加または削除 (Add or Remove Host Mappings)]オプションを右クリックします。
4. [ホストマッピングを追加または削除 (Add or Remove Host Mappings)]画面に、選択したクライアントホストのホスト ID が既存のマッピングとともに表示されます。

   [追加 (Add)]をクリックします。
5. [マッピングの追加 (Add Mapping)]ダイアログボックスで、次の詳細を入力します。

マッピング名 (Mapping Name)	ホスト ID からホスト名へのマッピングを指定します。 **メモ:** ホスト ID からホスト名へのマッピングでは、大文字と小文字が区別されません。
監査理由 (Audit Reason)	このマッピングを監査目的で追加する場合の理由または追加情報を指定します。
保存 (Save)	クリックすると、追加したマッピングが保存され、同じホスト ID に対するマッピングの追加が続行されます。
キャンセル (Cancel)	クリックすると、変更を保存せずにダイアログボックスを閉じます。

コマンドラインインターフェースを使用してホスト ID からホスト名へのマッピングを追加するには

1. 次のコマンドを実行して、Web サービスのログインを認証します。

   ```
   bpnbat -login -loginType WEB
   ```
2. 次のコマンドを実行して、ホスト ID からホスト名へのマッピングを追加します。

   ```
   nbhostmgmt -add -hostid host_ID -mappingname mapping_name
   ```

[ホストマッピングを追加または削除 (Add or Remove Host Mappings)] ダイアログボックス

ホストには、ホスト名または IP アドレスが複数関連付けられている場合があります。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および 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。

[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に選択して表示される[ホスト (Hosts)]タブで、変更するホストを右クリックし、[ホストマッピ

ングを追加または削除 (Add or Remove Host Mappings)]オプションをクリックしてダイアログボックスを開きます。

システム管理者のみが NetBackup ホストの[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]プロパティにアクセスできます。

p.269 の「ホスト ID からホスト名へのマッピングの追加」を参照してください。

p.272 の「ホスト ID からホスト名へのマッピングの削除」を参照してください。

[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックスには、次のプロパティが含まれています。

NetBackup ホスト ID (Host ID)	選択したホストのホスト ID が表示されます。
マッピング済みのホスト名/IP アドレス (Mapped Host Names / IP Addresses)	クライアントホストのホスト ID にマッピングされているホスト名と IP アドレスが一覧表示されます。
自動検出済み	マッピングされたホスト名または IP アドレスが、システムによって自動的に検出されたかどうかが示されます。
作成日時	マッピングが作成された日時です。
最終更新日時	マッピングが最後に更新された日時です。
追加 (Add)	クリックすると、クライアントホストのホスト名マッピングに新しいホスト ID が追加されます。 [マッピングの追加 (Add Mapping)]ダイアログボックスが表示されます。 p.269 の「ホスト ID からホスト名へのマッピングの追加」を参照してください。
削除 (Remove)	クリックすると、クライアントホストの選択したホスト ID からホスト名へのマッピングが削除されます。 [マッピングの削除 (Remove Mapping)]ダイアログボックスが表示されます。 p.272 の「ホスト ID からホスト名へのマッピングの削除」を参照してください。 **メモ:** [マッピングの追加 (Add Mapping)]および[マッピングの削除 (Remove Mapping)]ダイアログボックスで実行する操作は、NetBackup データベースを直接更新します。
閉じる (Close)	クリックすると、[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックスが閉じます。

ヘルプ (Help)	クリックすると、ヘルプが表示されます。

ホスト ID からホスト名へのマッピングの削除

ホスト ID からホスト名へのマッピングを削除するには、次の手順を使用します。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

p.269 の「ホスト ID からホスト名へのマッピングの追加」を参照してください。

ホスト ID からホスト名へのマッピングを削除するには

1. NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. 詳細ペインの[ホスト (Hosts)]タブで、変更するクライアントホストを右クリックします。
3. [ホストマッピングを追加または削除 (Add or Remove Host Mappings)]オプションを右クリックします。
4. [ホストマッピングを追加または削除 (Add or Remove Host Mappings)]画面に、選択したクライアントホストのホスト ID が既存のマッピングとともに表示されます。
5. 削除するマッピングを選択します。
6. [削除]をクリックします。
7. 監査目的で選択したマッピングを削除する場合は、[マッピングの削除 (Remove Mapping)]ダイアログボックスで監査理由を指定します。
8. [はい (Yes)]をクリックします。

コマンドラインインターフェースを使用してホスト ID からホスト名へのマッピングを削除するには

1. 次のコマンドを実行して、Web サービスのログインを認証します。

```
bpnbat -login -loginType WEB
```

2. 次のコマンドを実行して、ホスト ID からホスト名へのマッピングを削除します。

```
nbhostmgmt -delete -hostid host_ID-mappingname mapping_name
```

[承認待ちのマッピング (Mappings for Approval)]タブ

[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に選択して表示される[承認待ちのマッピング (Mappings for Approval)]タブを使用して、承認が保留されているホスト ID からホスト名へのマッピングを表示します。

[承認待ちのマッピング (Mappings for Approval)]タブでは、次のオプションを利用できます。

ホスト	選択したホストの名前です。
自動検出されたマッピング (Auto-discovered Mapping)	通信中にホストに対して検出されたホスト ID からホスト名へのマッピングです。
競合	マッピングに競合があるかどうかが示されます。たとえば、クラスタ設定では、マッピングをホスト ID 間で共有できます。
検出日時 (Discovered On)	システムによってマッピングが検出された日時です。
NetBackup ホスト ID (Host ID)	ホストのホスト ID です。

p.273 の「自動検出されたマッピングの表示」を参照してください。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

メモ: [セキュリティ管理 (Security Management)]、[グローバルセキュリティ設定 (Global Security Settings)]の順に選択した[安全な通信 (Secure Communication)]タブの[ホスト ID をホスト名に自動的にマッピングする (Automatically map host ID to host names)]オプションが選択されている場合、[承認待ちのマッピング (Mappings for Approval)]タブには競合するマッピングのみが表示されます。

p.287 の「ホスト ID をホスト名と IP アドレスに自動的にマッピングする」を参照してください。

自動検出されたマッピングの表示

通信中に NetBackup がホスト ID に関連する新しいホスト名または IP アドレスを検出することがあります。自動的に検出されたホスト ID からホスト名へのマッピングを表示できます。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

自動検出されたホスト ID からホスト名へのマッピングを表示するには

1. NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. 詳細ペインで、[承認待ちのマッピング (Mappings for Approval)]タブをクリックします。

   p.272 の「[承認待ちのマッピング (Mappings for Approval)]タブ」を参照してください。

メモ: [セキュリティ管理 (Security Management)]、[グローバルセキュリティ設定 (Global Security Settings)]の順に選択した[安全な通信 (Secure Communication)]タブの[ホスト ID をホスト名に自動的にマッピングする (Automatically map host ID to host names)]オプションが選択されている場合、[承認待ちのマッピング (Mappings for Approval)]タブには競合するマッピングのみが表示されます。

p.287 の「ホスト ID をホスト名と IP アドレスに自動的にマッピングする」を参照してください。

[マッピングの詳細 (Mapping Details)]ダイアログボックス

[マッピングの詳細 (Mapping Details)]ダイアログボックスを使用して、保留中のホスト ID からホスト名へのマッピングを承認または拒否します。

[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に選択して表示される[承認待ちのマッピング (Mappings for Approval)]タブで、承認または拒否するホスト ID からホスト名へのマッピングを右クリックし、[マッピングの詳細 (Mapping Details)]をクリックしてダイアログボックスを開きます。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

p.275 の「ホスト ID からホスト名へのマッピングの承認」を参照してください。

p.276 の「ホスト ID からホスト名へのマッピングの拒否」を参照してください。

p.272 の「[承認待ちのマッピング (Mappings for Approval)]タブ」を参照してください。

このダイアログボックスでは、次のオプションが利用できます。

ホスト	マッピングを承認または拒否するホストの名前が表示されます。
マッピング済みのホスト名/IP アドレス (Mapped Host Names / IP Addresses)	ホストに関連付けられている既存のマッピングが一覧表示されます。

NetBackup ホスト ID (Host ID)	ホストのホスト ID が表示されます。
マッピングの競合 - ホストと共有されています (Conflict in mapping - Shared with hosts)	**メモ:** 選択したマッピングがすでに他のホストに関連付けられている場合、この情報が表示されます。 この表には、選択したマッピングが共有されているすべてのホストの情報が一覧表示されます。 たとえば、クラスタ設定では、複数のホスト ID が同一の仮想名を共有します。 ホスト ID にマッピングが追加され、同一のマッピングが別のホスト ID に対して検出された場合、[承認待ちのマッピング (Mappings for Approval)]タブに一覧表示されます。[マッピングの詳細 (Mapping Details)]ダイアログボックスを使用して、このマッピングを承認するか、拒否することができます。 ■ [ホスト (Host)]: 選択したマッピングがすでに関連付けられているホストの名前が表示されます。 ■ [NetBackup ホスト ID (NetBackup Host ID)]: 選択したマッピングがすでに関連付けられているホストのホスト ID が表示されます。 p.277 の「共有マッピングまたはクラスタマッピングのシナリオについて」を参照してください。
理由	マッピングを承認または拒否する理由を入力します。
承認 (Approve)	クリックすると、保留中のマッピングが承認されます。
拒否 (Reject)	クリックすると、保留中のマッピングが拒否されます。
閉じる (Close)	クリックすると、変更を保存せずにダイアログボックスを閉じます。
ヘルプ (Help)	クリックすると、ヘルプが表示されます。

ホスト ID からホスト名へのマッピングの承認

このセクションでは、承認を保留しているホスト ID からホスト名へのマッピングを承認するための手順について説明します。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

p.276 の「ホスト ID からホスト名へのマッピングの拒否」を参照してください。

ホスト ID からホスト名へのマッピングを承認するには

1. NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. 詳細ペインで、[承認待ちのマッピング (Mappings for Approval)]タブをクリックします。
3. 承認するマッピングを選択し、右クリックします。
4. 右クリックして表示されたオプションで、[承認 (Approve)]をクリックします。選択したマッピングが承認されます。

   または、右クリックして表示されたオプションで、[マッピングの詳細 (Mapping Details)]をクリックします。[マッピングの詳細 (Mapping Details)]ダイアログボックスを使用して、選択したマッピングを承認します。

   p.274 の「[マッピングの詳細 (Mapping Details)]ダイアログボックス」を参照してください。

ホスト ID からホスト名へのマッピングの拒否

このセクションでは、承認を保留しているホスト ID からホスト名へのマッピングを拒否するための手順について説明します。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

p.275 の「ホスト ID からホスト名へのマッピングの承認」を参照してください。

ホスト ID からホスト名へのマッピングを拒否するには

1. NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. 詳細ペインで、[承認待ちのマッピング (Mappings for Approval)]タブをクリックします。
3. 拒否するマッピングを選択し、右クリックします。
4. 右クリックして表示されたオプションで、[拒否 (Reject)]をクリックします。選択したマッピングが拒否されました。

   または、右クリックして表示されたオプションで、[マッピングの詳細 (Mapping Details)]をクリックします。[マッピングの詳細 (Mapping Details)]ダイアログボックスを使用して、選択したマッピングを拒否します。

共有マッピングとクラスタマッピングの追加

特定のシナリオでは、ホスト ID からホスト名へのマッピングがホスト ID 間で共有されます。たとえば、クラスタ設定では、仮想名はすべてのノードで共有されます。プライマリサー

バーがノードと正常に通信できるように、NetBackup 管理コンソールを使用してこれらの共有マッピングを追加する必要があります。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

共有マッピングを追加するには

1. NetBackup 管理コンソールで、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. [ホスト (Hosts)]タブの詳細ペインで、右クリックしてオプションを表示します。
3. 右クリックして表示されたオプションで、[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)]を選択します。
4. [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)]ダイアログボックスで、共有マッピング名を指定します。

   p.278 の「[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)]ダイアログボックス」を参照してください。
5. 指定した共有マッピング名を使用してマッピングするホスト ID を選択します。
6. [保存 (Save)]をクリックします。

共有マッピングまたはクラスタマッピングのシナリオについて

次のシナリオでは、ホスト ID からホスト名へのマッピングを複数のホスト間で共有できます。

- 異なるドメインの複数のホストが同一のホスト名を使用する場合
- 同一の仮想名が複数のクラスタノードによって使用されるクラスタ設定内

ただし、関連付けられたホストが同一の通信状態でない (一部が 8.0 以前で安全でない通信を行うことがあり、一部が 8.1 以降で安全な通信を行う) シナリオでは、通信が失敗することがあります。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

シナリオ 1: 異なるドメインの複数のホストが同一のホスト名を使用する場合

たとえば、次の例を考えてみます。

- Host1: abc.secure.domain1.com、バージョン: 8.1、ポリシー: P1
- Host2: abc.insecure.domain2.com、バージョン: 7.7.3、ポリシー: P2
- Host1 と Host2 は、ホスト名と同一の名前 (abc) を使用します。セキュリティ管理者が、Host2 の共有マッピングとして abc を追加します。

p.276 の「共有マッピングとクラスタマッピングの追加」を参照してください。

- 8.0 以前のホストとの安全でない通信が有効になっています。
p.286 の「8.0 以前のホストとの安全でない通信について」を参照してください。
- Host2 が別のホストとの通信を開始すると、プライマリサーバーが Host2 の通信状態 (安全ではない) を検証しますが、Host1 の通信状態 (安全) とは異なります。両方のホストが同一のホスト名を使用していて、通信状態が一致しないため、Host2 との通信が失敗します。
- 推奨: Host2 を 8.1 以降にアップグレードします。

シナリオ 2: 同一の仮想名が複数のクラスタノードによって使用されるクラスタ設定内

たとえば、次の例を考えてみます。

- Host1: abc.secure.domain1.com、アクティブクラスタノード、バージョン: 8.1
- Host2: abc.secure.domain1.com、非アクティブクラスタノード、バージョン: 8.0
- Host1 と Host2 は同一の仮想名 (abc) を使用します。セキュリティ管理者が、Host2 の共有マッピングまたはクラスタマッピングとして abc を追加します。
p.276 の「共有マッピングとクラスタマッピングの追加」を参照してください。
- 8.0 以前のホストとの安全でない通信が有効になっています。
p.286 の「8.0 以前のホストとの安全でない通信について」を参照してください。
- Host1 が Host2 にフェールオーバーします。プライマリサーバーが Host2 の通信状態 (安全ではない) を検証しますが、Host1 の通信状態 (安全) とは異なります。両方のホストの通信状態が一致しないため、Host2 との通信が失敗します。
- 推奨: Host2 を 8.1 にアップグレードします。
- 回避策: Host1 のホスト ID からホスト名へのマッピング abc を削除します。共有マッピングの場合、関連付けられたホストが同一の通信状態 (安全) でない場合、通信状態が安全でないホストの通信が失敗します。

[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)]ダイアログボックス

このオプションは、共有マッピングまたはクラスタマッピングを追加するために使用します。[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に選択して表示される[ホスト (Hosts)]タブで、[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)]をクリックしてダイアログボックスを開きます。

[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)]ダイアログボックスでは、次のオプションを利用できます。

共有マッピング名またはクラスタの仮想名 (Shared mapping name or virtual name of cluster)	複数のホスト ID で共有する必要があるマッピング名を入力します。
ホストを選択 (Select Hosts)	ボタンをクリックすると、すべてのホストが一覧表示されるので、指定したマッピング名でマッピングするホストを選択します。 [ホストを選択 (Select Hosts)]ポップアップ画面には、利用可能なすべてのホストが一覧表示されます。必要なホストを選択して、[リストへの追加 (Add to list)]をクリックします。 選択したホストが[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)]ダイアログボックスのリストに表示されます。
ホスト	指定した共有名でマッピングするホストの名前です。
NetBackup ホスト ID (Host ID)	指定した共有名でマッピングするホストのホスト ID です。
保存 (Save)	クリックすると、マッピングが保存されます。
キャンセル (Cancel)	クリックすると、変更を保存せずにダイアログボックスを閉じます。
ヘルプ (Help)	クリックすると、ヘルプが表示されます。

p.276 の「共有マッピングとクラスタマッピングの追加」を参照してください。

p.277 の「共有マッピングまたはクラスタマッピングのシナリオについて」を参照してください。

NetBackup ホスト属性のリセット

特定のシナリオでは、ホスト属性をクリーンアップまたはリセットする必要があります。たとえば、ホストをダウングレードした場合です。

このような場合、ホスト ID からホスト名へのマッピング情報や通信状態などをリセットして、通信が正常に行われるようにする必要があります。

ホスト属性をリセットする前に、次の注意事項を確認してください。

- プライマリサーバーが安全でないモードでホストと通信する場合は、ダウングレードしたホストのホスト属性をリセットする必要があります。
- ホスト属性をリセットすると、ホスト ID からホスト名へのマッピング情報や通信状態などがリセットされます。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。

- ホストの属性をリセットすると、接続の状態 (安全な状態を示すフラグ) が安全でない状態に設定されます。次回のホスト通信時は、接続の状態が適切に更新されます。
- [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。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

ホスト属性のリセットについて

NetBackup 8.1 プライマリサーバーは、すべての 8.1 ホストと安全に通信できます。ただし、8.0 以前のホストと行う通信は安全ではありません。

特定のシナリオでは、NetBackup クライアントを 8.1 から 8.0 以前のバージョンにダウングレードする必要があります。ダウングレード後は、クライアントの通信状態が引き続きセキュアモードに設定されているため、プライマリサーバーはクライアントと通信できません。ダウングレード後に、通信状態は非セキュアモードに自動的に更新されません。

ホストをリセットするには、次のいずれかのオプションを使用します。

NetBackup 管理コンソールを使用してホストをリセットするには

1. [セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. [ホスト (Hosts)]タブの詳細ペインで、リセット対象のダウングレードしたホストを右クリックして、[ホスト属性をリセット (Reset Host Attributes)]をクリックします。

メモ: ダウングレードされたホストとの安全でない通信を再開するには、[セキュリティ管理 (Security Management)]、[グローバルセキュリティ設定 (Global Security Settings)]の順に選択した[安全な通信 (Secure Communication)]タブで、[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)]オプションを選択していることを確認してください。

コマンドラインインターフェースを使用してホスト属性をリセットするには

1. 次のコマンドを実行して、Web サービスのログインを認証します。

```
bpnbat -login -loginType WEB
```

2. 次のコマンドを実行して、ホストをリセットします。

```
nbemmcmd -resethost
```

証明書の自動再発行の許可または禁止

このセクションでは、証明書の自動再発行を許可および禁止する手順について説明します。

[証明書の自動再発行を許可する (Allow Auto Reissue Certificate)]オプションを使用すると、ホストの autoreissue パラメータを有効にし、その後、再発行トークンを必要とせずにホスト上で証明書を配備できます。

p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

デフォルトでは、autoreissue パラメータが有効なのは 2,880 分 (48 時間または 2 日) です。この期間が経過するとパラメータは無効になり、証明書の再発行操作には再発行トークンが必要になります。

p.282 の「ホストに対する autoreissue パラメータの有効期間の構成」を参照してください。

autoreissue パラメータを手動で無効にするには、[証明書の自動再発行を禁止する (Disallow Auto Reissue Certificate)]オプションを使用します。

メモ: BMR (Bare Metal Restore) プロセスの実行中、autoreissue フラグが自動的に設定されます。

Bare Metal Restore について詳しくは、『NetBackup Bare Metal Restore 管理者ガイド』を参照してください。

NetBackup 管理コンソールを使用して証明書の自動再発行を許可する方法

1. [セキュリティ管理] > [ホスト管理]の順に展開します。
2. 右ペインで、証明書の自動再発行を許可するホストを選択します。
3. ホストを右クリックして、[証明書の自動再発行を許可する]オプションを選択します。

コマンドラインインターフェースを使用して証明書の自動再発行を許可する方法

1. 次のコマンドを実行して、Web サービスのログインを認証します。

```
bpnbat -login -loginType WEB
```

2. 次のコマンドを実行して autoreissue パラメータを有効にし、証明書の自動再発行を許可します。

```
nbhostmgmt -allowautoreissuecert -hostid host_ID -autoreissue 1
```

NetBackup 管理コンソールを使用して証明書の自動再発行を禁止する方法

1. [セキュリティ管理] > [ホスト管理]の順に展開します。
2. 右ペインで、証明書の自動再発行を禁止するホストを選択します。
3. ホストを右クリックして、[証明書の自動再発行を禁止する (Disallow Auto Reissue Certificate)]オプションを選択します。

コマンドラインインターフェースを使用して証明書の自動再発行を禁止する方法

1. 次のコマンドを実行して、Web サービスのログインを認証します。

   ```
   bpnbat -login -loginType WEB
   ```

2. 次のコマンドを実行して autoreissue パラメータを無効にし、証明書の自動再発行を禁止します。

   ```
   nbhostmgmt -allowautoreissuecert -hostid host_ID -autoreissue 0
   ```

ホストに対する autoreissue パラメータの有効期間の構成

ホスト ID ベースの証明書の自動再発行を許可すると、autoreissue パラメータはデフォルトで 2,880 分間 (48 時間または 2 日) 有効になります。この期間が経過するとパラメータはリセットされ、証明書の再発行操作には再発行トークンが必要になります。

証明書の自動再発行の期間、または autoreissue パラメータの TTL (time-to-live) 設定は、web.conf ファイルを更新することで構成できます。

autoreissue パラメータまたは TTL 設定の有効期間の構成方法

1. web.conf ファイルを開きます。ファイルの場所は次のとおりです。

   Windows の場合: Install_Path¥var¥global¥wsl¥config¥web.conf

   Linux の場合: /usr/openv/var/global/wsl/config/web.conf

2. autorissue パラメータの TTL 設定は分単位で構成します。次に例を示します。

   ```
   ttl.autoReissue.minutes = 1440
   ```

   メモ: autoreissue TTL 設定の有効範囲は、0 分から 43,200 分 (または 30 日) です。

   構成した TTL 値が有効な範囲内にない場合、サーバーは最後に構成された TTL 値を使用して続行します。

3. 新しい autoreissue TTL 値を有効にするには、次のいずれかを実行します。
   - NetBackup Web 管理コンソール (WMC) サービスを再起動します。
   - 次のコマンドを実行します。

Windows の場合: *Install_Path*/bin/nbhostdbcmd -reloadconfig -host

UNIX の場合: *NETBACKUP_INSTALL_DIR*¥bin¥nbhostdbcmd -reloadconfig -host

ホストのコメントの追加または削除

[コメントの追加または編集 (Add or Edit Comment)]ダイアログボックスを使用して、NetBackup ホストに関する追加情報を入力することができます。たとえば、ホストが廃止された場合、廃止された理由といつ廃止されたかを説明するコメントを追加できます。

ホストのコメントを追加または編集するには

1. [セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. [ホスト (Hosts)]タブの詳細ペインで、追加情報を入力するホストを右クリックして、[コメントの追加または編集 (Add or Edit Comment)]をクリックします。
3. [コメントの追加または編集 (Add or Edit Comment)]ダイアログボックスの[コメント (Comment)]ペインに、必要な情報またはコメントを入力します。

   [保存 (Save)]をクリックします。

ホストのコメントを削除するには

1. [NetBackup の管理 (Management)]、[セキュリティ管理 (Security Management)]、[ホスト管理 (Host Management)]の順に展開します。
2. [ホスト (Hosts)]タブの詳細ペインで、コメントを削除するホストを右クリックして、[コメントの削除 (Delete Comment)]をクリックします。

グローバルセキュリティ設定について

[セキュリティ管理 (Security Management)]、[グローバルセキュリティ設定 (Global Security Settings)]ノードでは、NetBackup での安全な通信にとって重要なことを設定できます。

p.264 の「NetBackup での安全な通信について」を参照してください。

p.288 の「ディザスタリカバリ設定について」を参照してください。

p.283 の「安全な通信の設定について」を参照してください。

安全な通信の設定について

NetBackup は、ホスト間の安全な通信を構成できる設定を提供します。

表 17-2 安全な通信の設定

設定	説明
認証局	NetBackup ドメインがサポートする認証局が表示されます。 NetBackup ドメインを有効にして次を使用するように、NetBackup Web サーバーを構成できます。 ■ NetBackup CA が署名した証明書のみ ■ 外部 CA が署名した証明書のみ ■ NetBackup CA が署名した証明書と外部 CA が署名した証明書 Web サーバー用の証明書構成には、`-configureWebServerCerts` コマンドを使用します。 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。
NetBackup 8.0 以前のホストとの安全でない通信を有効にする	NetBackup が 8.0 以前のホストと行う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。これにより、NetBackup ホスト間では安全な通信のみが可能になります。 デフォルトではこのオプションが選択されているため、NetBackup は、8.0 以前のホストも含め、既存の NetBackup 環境に存在するホストと通信できます。 また、このオプションにより、NetBackup 8.1 以降のプライマリサーバーとの通信も可能になります。 p.285 の「安全でない通信の無効化」を参照してください。 p.286 の「8.0 以前のホストとの安全でない通信について」を参照してください。 自動イメージレプリケーションを設定した場合、オプションの選択を解除する前に次のことを確認します。 イメージのレプリケーション用に指定した信頼できるプライマリサーバーが NetBackup 8.0 以降である。 詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

設定	説明
ホスト名に NetBackup ホスト ID を自動的にマッピング	ホストには、ホスト名または IP アドレスが複数関連付けられている場合があります。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および 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。 通信中に NetBackup がホスト ID に関連する新しいホスト名または IP アドレスを検出することがあります。 システムで検出されたホスト名または IP アドレスにホスト ID を自動的にマッピングする場合は、このオプションを選択します。 デフォルトでは、このオプションは選択されています。 セキュリティを強化するには、このオプションを無効にして、NetBackup 管理者がマッピングを手動で確認し、承認できるようにします。 p.287 の「ホスト ID をホスト名と IP アドレスに自動的にマッピングする」を参照してください。
証明書配備のセキュリティレベル	証明書の配備方法は、NetBackup のプライマリサーバーに構成されているセキュリティレベルに基づいて決定されます。 たとえば、セキュリティレベルが[最高 (Very High)]に設定されている場合、証明書配備には認証トークンが必要となります。 **メモ:** 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、このオプションは利用できません。 p.297 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。 p.300 の「証明書の配備のセキュリティレベルの設定」を参照してください。

安全でない通信の無効化

デフォルトでは、NetBackup は 8.0 以前のホストと通信できます。セキュリティ強化のため、すべてのホストを現在のバージョンにアップグレードし、8.0 以前のホストとの通信を無効にしてください。

p.283 の「安全な通信の設定について」を参照してください。

安全でない通信を無効にするには

1. 右ペインで、[設定 (Setting)]、[グローバルセキュリティ (Global security)]の順に選択します。
2. [グローバルセキュリティ設定 (Global security settings)]ページで、[安全な通信 (Secure Communication)]タブを選択します
3. [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)]オプションのチェックマークをはずします。
4. [保存 (Save)]をクリックします。

メモ: 安全でない通信を無効にするには、すでに確立された安全でない接続を終了させるため、サービスを再起動することをお勧めします。

8.0 以前のホストとの安全でない通信について

NetBackup は 8.0 以前のホストと安全に通信できません。

お使いの環境に NetBackup 8.0 以前のホストがある場合に、それらのホストとの安全でない通信を許可するには、NetBackup 管理コンソールの[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)]オプションを使用します。

このオプションは、[設定 (Setting)]、[グローバルセキュリティ (Global Security)]、[安全な通信 (Secure communication)]タブで利用できます。

また、このオプションにより、NetBackup 8.1 以降のプライマリサーバーとの通信も可能になります。

デフォルトでは、安全でない通信は有効になっています。ただし、セキュリティ強化のため、すべてのホストを現在のバージョンにアップグレードし、8.0 以前のホストとの通信を無効にしてください。

p.285 の「安全でない通信の無効化」を参照してください。

p.287 の「複数の NetBackup ドメインの 8.0 以前のホストとの通信について」を参照してください。

メモ: 自動イメージレプリケーションを設定した場合、安全でない通信を無効にする前に、イメージのレプリケーション用に指定した信頼できるプライマリサーバーのバージョンが NetBackup 8.0 以降であることを確認します。

p.264 の「NetBackup での安全な通信について」を参照してください。

複数の NetBackup ドメインの 8.0 以前のホストとの通信について

このセクションでは、NetBackup ホストの 1 つが複数のドメインにある場合に、[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)]オプションがホスト通信に与える影響について説明します。

次のシナリオを検討します。

- ホスト A はバージョン 8.1 であり、M1 および M2 という名前の複数の NetBackup ドメインにあります。
- ホスト B はバージョン 8.0 であり、M3 という名前の NetBackup ドメインにあります。
- [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)]オプションが、プライマリサーバー M1 で選択解除されています。これは、M1 に関連付けられているホストが 8.0 以前のホストと通信できないことを意味します。
- [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)]オプションが、プライマリサーバー M2 で選択されています。これは、M2 に関連付けられているホストが 8.0 以前のホストと通信できることを意味します。
- ホスト A の構成ファイル (UNIX の場合は `bp.conf` ファイル、Windows の場合はレジストリキー) には、プライマリサーバーリストの最初のエントリとして「M2」が含まれています。

ホスト A がホスト B との通信を開始すると、ホスト A の構成ファイルに表示される最初のプライマリサーバー (M2) の[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)]オプションのステータスが検証されます。M2 に設定されたオプションに従い、8.0 以前のホストとの通信が許可されます。そのため、ホスト A とホスト B の間の通信が成功します。

ホスト ID をホスト名と IP アドレスに自動的にマッピングする

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 ID をそれぞれのホスト名 (および IP アドレス) に自動的にマッピングするか、または NetBackup 管理者がマッピングを確認して承認できるようにするか、選ぶことができます。

p.270 の「[ホストマッピングを追加または削除 (Add or Remove Host Mappings)]ダイアログボックス」を参照してください。

メモ: セキュリティを強化するには、このオプションを無効にして、NetBackup 管理者がマッピングを手動で確認し、承認できるようにします。

ホスト ID をホスト名または IP アドレスに自動的にマッピングするには

1. 右ペインで、[設定 (Setting)]、[グローバルセキュリティ (Global security)]の順に選択します。
2. [グローバルセキュリティ設定 (Global security settings)]ページで、[安全な通信 (Secure Communication)]タブを選択します。
3. [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 host names)]オプションを選択します。
4. [保存 (Save)]をクリックします。

p.283 の「安全な通信の設定について」を参照してください。

ディザスタリカバリ設定について

セキュリティ向上のため、各カタログがバックアップされる際にディザスタリカバリパッケージが作成されます。

p.291 の「ディザスタリカバリパッケージ」を参照してください。

ディザスタリカバリパッケージは、各カタログのバックアップの際に作成され、ユーザーが設定するパスフレーズで暗号化されます。災害発生後に NetBackup をプライマリサーバーにディザスタリカバリモードでインストールする際は、この暗号化パスフレーズを入力する必要があります。

[ディザスタリカバリ (Disaster Recovery)]タブには以下のオプションが表示されます。

表 17-3　　ディザスタリカバリの設定

設定	説明
パスフレーズ	ディザスタリカバリパッケージを暗号化するパスフレーズを入力します。 ■ デフォルトでは、パスフレーズを 8 ～ 1024 文字で指定する必要があります。 `nbseccmd -setpassphraseconstraints` コマンドオプションを使用して、パスフレーズの制約を設定できます。 ■ 既存のパスフレーズと新しいパスフレーズは異なるものにする必要があります。 ■ パスフレーズでサポートされる文字は、空白、大文字 (A-Z)、小文字 (a-z)、数字 (0-9)、および特殊文字のみです。特殊文字には、~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > " が含まれます。
パスフレーズの確認	確認のため、パスフレーズを再入力します。

注意: パスフレーズにサポート対象の文字のみが含まれていることを確認します。サポートされていない文字を入力した場合、ディザスタリカバリパッケージのリストア中に問題が発生する可能性があります。パスフレーズは検証されないことがあり、ディザスタリカバリパッケージをリストアできなくなる可能性があります。

ディザスタリカバリパッケージの暗号化パスフレーズを変更する際の注意

- パスフレーズ変更以降のディザスタリカバリパッケージは、ユーザーが設定した新しいパスフレーズで暗号化されます。
- パスフレーズを変更しても、以前のディザスタリカバリのパッケージでは変更されません。新しいディザスタリカバリパッケージのみが新しいパスフレーズに関連付けられます。
- 災害発生後に NetBackup をプライマリサーバーにディザスタリカバリモードでインストールする際に入力するパスフレーズは、プライマリサーバーのホスト ID のリカバリ元であるディザスタリカバリパッケージのパスフレーズに対応している必要があります。

ディザスタリカバリパッケージを暗号化するパスフレーズの設定

ディザスタリカバリパッケージは、各カタログのバックアップの際に作成され、ユーザーが設定するパスフレーズで暗号化されます。

p.291 の「ディザスタリカバリパッケージ」を参照してください。

ディザスタリカバリパッケージの暗号化パスフレーズの設定および災害後の使用のワークフロー

災害リカバリパッケージのリストアについて理解するには、次のワークフローを確認します。

1. ディザスタリカバリパッケージの暗号化パスフレーズを設定します。
2. カタログポリシーを作成します。

   次のシナリオを検討します。

   - 以前にパスフレーズを設定したことがない場合、NetBackup で新しいカタログバックアップポリシーを構成することはできません。
   - カタログバックアップポリシーを以前のバージョンからアップグレードする場合、パスフレーズを設定するまでカタログのバックアップは失敗します。

     メモ: パスフレーズが設定されていても、カタログバックアップが失敗し、状態コード 144 が表示される場合があります。これは、パスフレーズが壊れている可能性があるためです。この問題を解決するには、パスフレーズをリセットする必要があります。

3. 災害発生後に NetBackup をプライマリサーバーにディザスタリカバリモードでインストールする際は、以前に設定した暗号化パスフレーズを入力します。インストール中、NetBackup は、このパスフレーズを使用してディザスタリカバリパッケージを復号し、プライマリサーバーの識別情報を再取得します。

注意: 災害発生後に NetBackup をプライマリサーバーにインストールする際に適切なパスフレーズを入力できない場合、NetBackup のすべてのホストにセキュリティ証明書を再配備しなくてはならなくなる場合があります。詳しくは、次の記事を参照してください。

https://www.veritas.com/content/support/en_US/article.100033743

---

4. プライマリサーバーの識別情報が再取得されると、プライマリサーバーとメディアサーバーの間で安全な通信が確立し、カタログリカバリを実行できるようになります。
5. カタログリカバリが正常に完了したら、ディザスタリカバリパッケージのパスフレーズを再度設定する必要があります。これは、パスフレーズがカタログリカバリ中にリカバリされないためです。パスフレーズを設定しないかぎり、新しい NetBackup インスタンスに構成したカタログバックアップは失敗し続けます。

パスフレーズの設定または変更

1 NetBackup Web UI を開きます。

2 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。

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

p.288 の「ディザスタリカバリ設定について」を参照してください。

4 パスフレーズを入力して確認します。

次のパスワードのルールを確認してください。

- 既存のパスフレーズと新しいパスフレーズは異なるものにする必要があります。
- デフォルトでは、パスフレーズを 8 ～ 1024 文字で指定する必要があります。`nbseccmd -setpassphraseconstraints` コマンドオプションを使用して、パスフレーズの制約を設定できます。
- パスフレーズでサポートされる文字は、空白、大文字 (A-Z)、小文字 (a-z)、数字 (0-9)、および特殊文字のみです。特殊文字には、~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > " が含まれます。

注意: サポートされていない文字を入力した場合、ディザスタリカバリパッケージのリストア中に問題が発生する可能性があります。パスフレーズは検証されないことがあり、ディザスタリカバリパッケージをリストアできなくなる可能性があります。

5 [保存 (Save)]をクリックします。パスフレーズがすでに設定されている場合、既存のパスフレーズは上書きされます

コマンドラインインターフェースを使用して、パスフレーズを設定または変更するには

1 このタスクを実行するためには、NetBackup 管理者が NetBackup Web 管理サービスにログインしている必要があります。次のコマンドを使ってログオンします。

```
bpnbat -login -loginType WEB
```

2 次のコマンドを実行して、ディザスタリカバリパッケージを暗号化するパスフレーズを設定します。

```
nbseccmd -drpkgpassphrase
```

3 パスフレーズを入力します。

パスフレーズがすでに存在する場合、既存のパスフレーズは上書きされます。

ディザスタリカバリパッケージ

セキュリティ向上のため、各カタログがバックアップされる際にディザスタリカバリパッケージが作成されます。ディザスタリカバリパッケージファイルの拡張子は `.drpkg` です。

ディザスタリカバリ (DR) パッケージには、プライマリサーバーホストの識別情報が保存されます。このパッケージは、災害発生後にプライマリサーバーの識別情報を NetBackup に再取得させるために必要です。ホストの識別情報をリカバリすると、カタログリカバリを実行できます。

ディザスタリカバリパッケージには、次の情報が含まれます。

- プライマリサーバー証明書と NetBackup 認証局 (CA) 証明書の、NetBackup CA が署名した証明書と秘密鍵
- ドメイン内のホストについての情報
- セキュリティ設定
- 外部 CA が署名した証明書
  外部 CA が署名した Windows 証明書ストアからの証明書 (該当する場合)
- 外部 CA が署名した証明書に固有の NetBackup 構成オプション
- キーマネージメントサービス (KMS) 構成

メモ: デフォルトでは、KMS 構成はカタログバックアップ時にバックアップされません。カタログバックアップ時に、KMS 構成をディザスタリカバリパッケージの一部として含めるには、KMS_CONFIG_IN_CATALOG_BKUP 構成オプションを 1 に設定します。

メモ: カタログバックアップが成功するようにディザスタリカバリパッケージのパスフレーズを設定する必要があります。

ホスト名ベースの証明書について

デフォルトでは、インストールの実行中にホスト名ベースの証明書が個別の NetBackup プライマリサーバーにプロビジョニングされます。メディアサーバーまたはクライアントでホスト名ベースの証明書をプロビジョニングするには、NetBackup 管理者がプライマリサーバー上で bpnbaz コマンドを実行して証明書を他のホストにプッシュします。

p.264 の「NetBackup のセキュリティ証明書の概要」を参照してください。

ホスト名ベースの証明書の配備

次の手順の 1 つを選択して NetBackup ホストにホスト名ベースのセキュリティ証明書を配備します。NetBackup 管理者のみが証明書を配備できます。

表 17-4　　ホスト名ベースの証明書の配備

手順	説明と手順へのリンク
クラスタ内プライマリサーバーのホスト名ベースのセキュリティ証明書の配備	この手順では、ホスト名ベースのセキュリティ証明書を NetBackup プライマリサーバークラスタ内のすべてのノードに配備します。
メディアサーバーまたはクライアントのホスト名ベースのセキュリティ証明書の配備	この手順では、IP アドレスの検証を使用してターゲットの NetBackup ホストを識別してから証明書を配備します。 この手順により、個別のホスト、すべてのメディアサーバー、またはすべてのクライアントに対するホスト名ベースの証明書を配備できます。

メモ: ホスト名ベースの証明書の配備は 1 つのホストごとに行う 1 回のみの操作です。ホスト名ベースの証明書が以前のリリースまたは修正プログラムで配備された場合は、再び配備を行う必要はありません。

クラスタ内プライマリサーバーのホスト名ベースの証明書の配備

この手順では、ホスト名ベースの証明書をすべてのクラスタノードに配備します。

ホスト名ベースの証明書を配備する前に、次のことを確認します。

- クラスタのすべてのノードにホスト ID ベースの証明書がある
- クラスタノードのすべての完全修飾ドメイン名 (FQHN) と短縮名は、それぞれのホスト ID にマッピングされます。

クラスタ内の NetBackup プライマリサーバーのホスト名ベースのセキュリティ証明書を配備する方法

1. プライマリサーバークラスタのアクティブノードで、次のコマンドを実行します:

   Windows の場合: *Install_path*¥NetBackup¥bin¥admincmd¥bpnbaz -setupat

   UNIX の場合: /usr/openv/netbackup/bin/admincmd/bpnbaz -setupat

2. プライマリサーバーのアクティブノードで NetBackup Service Layer (nbsl) サービスと、NetBackup Vault Manager (nbvault) サービスを再起動します。

メディアサーバーまたはクライアントにホスト名ベースの証明書を配備する

この手順は、同時に多数のホストにホスト名ベースのセキュリティ証明書を配備する場合に適しています。NetBackup 配備と同様に通常、この方法はネットワークが安全であることを前提とします。

メディアサーバーまたはクライアントのホスト名ベースのセキュリティ証明書を配備する方法

1. 環境に応じて、プライマリサーバーで次のコマンドを実行します。ホスト名を指定するか、すべてのメディアサーバーまたはクライアントへの配備を実行します。

   Windows の場合: *Install_path*¥NetBackup¥bin¥admincmd¥bpnbaz -ProvisionCert *host_name*|-AllMediaServers|-AllClients

   UNIX の場合: /usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert *host_name*|-AllMediaServers|-AllClients

2. メディアサーバーで NetBackup Service Layer (nbsl) サービスを再起動します。

   ターゲットホストが NetBackup クライアントの場合はどのサービスも再起動する必要はありません。

メモ: ホスト上で動的 IP を使用する場合 (DHCP) は、ホスト名と IP アドレスがプライマリサーバーで正しく一覧表示されていることを確認します。これを行うには、プライマリサーバーで次の NetBackup bpclient コマンドを実行します。

Windows の場合: *Install_path*¥NetBackup¥bin¥admincmd¥bpclient -L -All

UNIX の場合: /usr/openv/netbackup/bin/admincmd/bpclient -L -All

ホスト ID ベースの証明書について

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。プライマリサーバーが認証局 (CA) になります。マスターサーバーはホストにホスト 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。CA は、証明書 (または無効になった証明書) があるすべてのホスト ID のリストを保持します。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。

ホスト ID はシステムでランダムに生成され、ハードウェアのどのプロパティにも関連付けられません。

NetBackup が、無効化したホスト ID ベースの証明書のリストを示します。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

p.264 の「NetBackup のセキュリティ証明書の概要」を参照してください。

NetBackup 管理者は証明書の配備と無効化に関連する設定を制御できます。

ホスト ID はホスト名を変更しても変更されません。

ホストが複数の NetBackup ドメインから証明書を取得する場合、そのホストは各 NetBackup ドメインに対応するホスト ID を複数持つことになります。

プライマリサーバーをクラスタの一部として構成する場合、クラスタの各ノードが一意のホスト ID を受け取ります。仮想名には、追加のホスト ID が割り当てられます。たとえば、プライマリサーバークラスタが *N* 個のノードで構成される場合、そのプライマリサーバークラスタに割り当てられるホスト ID の数は *N* + 1 個になります。

nbcertcmd コマンドオプションの Web ログインの要件

nbcertcmd コマンドは、ホスト ID ベースの証明書に関連するすべての操作を実行するために使うことができます。ただし、一部の nbcertcmd オプションでは、ユーザーが NetBackup Web 管理サービス (nbwmc) にログインする必要があります。

- NetBackup Web 管理サービスにログインするには、次のコマンドを実行します。

  ```
  bpnbat -login -logintype WEB
  ```

  このアカウントには、NetBackup 管理者権限が必要です。
  WEB ログインの例を次に示します。

  ```
  bpnbat -login -LoginType WEB
  Authentication Broker: server.domain.com
  Authentication port [0 is default]: 0
  Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap):
  unixpwd
  Domain: server.domain.com
  Login Name: root
  ```

```
Password: ********
Operation completed successfully.
```

- bpnbat -login -logintype AT コマンドは NetBackup 認証ブローカー (nbatd) とのセッションを作成します。(NetBackup 認証ブローカーはプライマリサーバーである必要はありません。)

  メモ: nbcertcmd コマンドを実行する場合、nbatd セッションは不要です。

- WEB または AT のいずれも指定されていない場合、bpnbat -login は nbatd と nbwmc の両方のログインセッションを作成します。(この処理は、認証ブローカーがプライマリサーバーに存在する場合に実行されます)。

メモ: nbwmc サービスはプライマリサーバーでのみ実行するため、WEB ログインの認証ブローカーはプライマリサーバーです。

『コマンドリファレンスガイド』には、各 オプションで必要とされる権限の詳細が示されています。
https://www.veritas.com/content/support/en_US/article.100040135NetBackupnbcertcmd
このガイドには、bpnbat コマンドの実行についての詳細情報も記載されています。

証明書管理ユーティリティを使ったホスト ID ベースの証明書の発行と配備

ホスト ID ベースの証明書の配備のプロセスは、プライマリ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よって異なります。レベルは、[中 (Medium)]、[高 (High)]、[最高 (Very High)]のいずれかです。デフォルトのセキュリティレベルは[高 (High)]です。

ホスト ID ベースの証明書は、アップグレードまたはインストール時にプライマリサーバーに自動的に配備されます。

ホスト ID ベースの証明書は、指紋を確認した後、ホストに配備されます。認証トークンが必要かどうかは、セキュリティレベルによって異なります。

セキュリティレベルによって、認証局 (CA) が NetBackup ホストから証明書要求を受信したときに実行する検査の性質が決まります。お使いの NetBackup 環境のセキュリティ要件に応じて、証明書配備レベルを選択します。

p.297 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。

一部のシナリオでは、証明書の配備において NetBackup 管理者が管理する認証トークンを使う必要があります。NetBackup 管理者は、これらのトークンを作成して、ローカルホストで証明書の配備を行う個々のホストの管理者と共有します。証明書の配備は容易

に実行できるため、NetBackup 管理者の介入なしで複数の NetBackup ホストにわたり柔軟な配備を実施できます。

表 17-5　　それぞれの証明書配備レベルまたはシナリオにおける配備要件

証明書配備レベルまたはシナリオ	認証トークンの必要性	ホスト ID ベースの証明書の配備
[最高 (Very High)]の証明書配備レベルの設定	はい。すべての証明書要求において認証トークンが必要です。プライマリサーバー管理者はプライマリ以外のホストで使用するトークンを作成します。 p.318 の「認証トークンの作成」を参照してください。	プライマリサーバー以外のホストのホスト管理者は、プライマリサーバー管理者から認証トークンを取得して、ホスト ID ベースの証明書の配備に使用する必要があります。 p.301 の「ホスト ID ベースの証明書の配備」を参照してください。
[高 (High)] (デフォルト)の証明書配備レベルの設定	必要な場合があります。証明書は、プライマリサーバーに認識されているホストでトークンを使用せずに配備されます。 次のトピックでは、プライマリサーバーに認識される意味について説明します。 p.297 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。 ホストがプライマリサーバーに認識されていない場合は、認証トークンを使用して証明書を配備する必要があります。プライマリサーバー管理者はプライマリサーバー以外のホストで使うトークンを作成します。 p.318 の「認証トークンの作成」を参照してください。	ホスト ID ベースの証明書を配備する場合、追加の操作は不要です。 トークンが必要な場合、プライマリサーバー以外のホストのホスト管理者は、プライマリサーバー管理者からトークンを取得し、これを使用してホスト ID ベースの証明書を配備する必要があります。 p.301 の「ホスト ID ベースの証明書の配備」を参照してください。
[中 (Medium)]の証明書配備レベル設定	いいえ。証明書を要求したすべてのホストに、証明書を配備できます。 p.300 の「ホスト ID ベースの証明書の自動配備」を参照してください。 **メモ:** 要求したホスト名が証明書要求の発信元の IP と一致することをプライマリサーバーが検証できない場合、証明書が配備されないことがあります。	ホスト ID ベースの証明書を配備する場合、追加の操作は不要です。 プライマリサーバーがホスト名を検証できない場合は、トークンを使用してホスト ID ベースの証明書を配備する必要があります。 p.301 の「ホスト ID ベースの証明書の配備」を参照してください。
証明書の再発行	はい。証明書の再発行では、ほとんどの場合、再発行トークンが必要です。	p.314 の「再発行トークンの作成」を参照してください。

証明書配備レベルまたはシナリオ	認証トークンの必要性	ホスト ID ベースの証明書の配備
プライマリサーバーと直接的に通信できないホスト (この例では非武装地帯 (DMZ) の NetBackup ホスト) です。	はい。NetBackup は、ホストがプライマリサーバーと接続されているかどうかを自動的に検出できます。接続されていない場合、NetBackup はメディアサーバーの組み込み HTTP トンネルを使用して、証明書要求をプライマリサーバーにルーティングしようとします。 p.340 の「非武装地帯にある NetBackup クライアントとプライマリサーバーの間の HTTP トンネルを介した通信について」を参照してください。	p.310 の「プライマリサーバーと接続されていないクライアントでの証明書の配備」を参照してください。
NAT クライアントに対する証明書の配備と生成	はい。NAT クライアントに NetBackup 証明書を配備するときは、プライマリ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、認証トークンが必須であることを指定する必要があります。これはプライマリサーバーが、要求の発信元である IP アドレスにホスト名を解決できないためです。	NetBackup の NAT クライアントの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。

ホスト ID ベースの証明書の詳細の表示

ホスト ID ベースの各証明書の詳細は NetBackup 管理コンソールまたは nbcertcmd コマンドを使って表示できます。

NetBackup 管理 Web UI で証明書の詳細を表示するには

1. 左ペインで、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
   証明書の詳細が右ペインに表示されます。
2. ホスト名を選択し、[詳細の表示 (View details)]をクリックします。

nbcertcmd コマンドを使って証明書の詳細を表示するには

- 他のプライマリサーバーからホストに割り当てられたすべてのホスト ID を表示するには、次のコマンドを NetBackup ホストで実行します。

```
nbcertcmd -listCertDetails
```

NetBackup 証明書の配備のセキュリティレベルについて

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

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

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

メモ: NAT クライアントに NetBackup 証明書を配備するときは、プライマリ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。これはプライマリサーバーが、要求の発信元である IP アドレスにホスト名を解決できないためです。

NetBackup の NAT の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。

---

p.295 の「証明書管理ユーティリティを使ったホスト ID ベースの証明書の発行と配備」を参照してください。

p.300 の「証明書の配備のセキュリティレベルの設定」を参照してください。

表 17-6 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。 p.318 の「認証トークンの作成」を参照してください。	1 時間ごとに、ホスト上に存在する CRL が更新されます。 p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

セキュリティレベル	説明	CRL の更新
高 (High) (デフォルト)	ホストがプライマリサーバーに認識されている場合、認証トークンは不要です。ホストが以下のエンティティで検出される場合、ホストはプライマリサーバーに認識されていると見なされます。 **1** ホストが NetBackup 構成ファイル (Windows レジストリまたは UNIX の `bp.conf` ファイル) で次のいずれかのオプションでリストされる。 ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER ■ MSDP_SERVER NetBackup の構成オプションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。 **2** `altnames` ファイル (ALTNAMESDB_PATH) にクライアント名としてホストがリストされている。 **3** ホストがプライマリサーバーの EMM データベースに表示されている。 **4** クライアントの少なくとも 1 つのカタログイメージが存在する。イメージは 6 カ月以内に作成されたものである必要があります。 **5** クライアントが少なくとも 1 つのバックアップポリシーにリストされている。 **6** クライアントがレガシークライアントである。すなわち、[クライアント属性 (Client Attributes)]ホストプロパティを使用して追加されたクライアントです。 p.318 の「認証トークンの作成」を参照してください。	4 時間ごとに、ホスト上に存在する CRL が更新されます。
中 (Medium)	プライマリサーバーが要求の発信元である IP アドレスにホスト名を解決できる場合、証明書は認証トークンなしで発行されます。	8 時間ごとに、ホスト上に存在する CRL が更新されます。

証明書の配備のセキュリティレベルの設定

NetBackup Web UI または nbcertcmd コマンドを使用して、NetBackup ドメインでの証明書の配備のセキュリティレベルを設定します。

こ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。

証明書の配備レベルを構成する方法

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. [安全な通信 (Secure communication)]タブをクリックします。
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 ([最高 (Very High)]、[高 (High)] (デフォルト)、または[中 (Medium)]) を選択します。
4. [保存 (Save)]をクリックします。

コマンドラインを使って証明書の配置レベルを設定するには

1. プライマリサーバー管理者は、このタスクを実行するために NetBackup Web 管理サービスにログインしている必要があります。次のコマンドを使用してログインします。

   ```
   bpnbat -login -logintype WEB
   ```

   p.294 の「nbcertcmd コマンドオプションの Web ログインの要件」を参照してください。
2. 次のコマンドを実行し、現在のセキュリティレベルを表示します。

   ```
   nbcertcmd -getSecConfig -certDeployLevel -server
   primary_server_name
   ```
3. 次のコマンドを実行し、セキュリティレベルを変更します。

   ```
   nbcertcmd -setSecConfig -certDeployLevel 0-2 -server
   primary_server_name
   ```

   ここで、0 は[最高 (Very High)]、1 は[高 (High)] (デフォルト)、2 は[中 (Medium)]です。

nbcertcmd 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。

ホスト ID ベースの証明書の自動配備

ホスト ID ベースの証明書は、NetBackup インストールの一環として NetBackup プライマリサーバーに自動的に配備されます。

これらの証明書は、証明書配備レベルに応じて他の NetBackup ホストに配備されます (指紋の確認後)。

NetBackup プライマリサーバーの認証局 (CA) は、証明書配備レベルとプライマリサーバーのホスト情報の検証能力に応じて、証明書の要求を承認または拒否できます。

次のコマンドを使うと、NetBackup ホストに配備された証明書のリストを確認できます。

```
nbcertcmd -listCertDetails
```

証明書の要求が拒否された場合、ホスト管理者は NetBackup 管理者に対して認証トークンの生成と共有を要求して、証明書を手動で配備する必要があります。

p.318 の「認証トークンの作成」を参照してください。

p.297 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。

ホスト ID ベースの証明書の配備

証明書配備のセキュリティレベルに応じて、プライマリ以外のホストは、認証局 (プライマリサーバー) からホスト ID ベースの証明書を取得できるようになるために、認証トークンが必要になる場合があります。証明書が自動的に配備されない場合は、管理者が NetBackup コマンドを使って nbcertcmd ホストに手動で証明書を配備する必要があります。

次の項で、配備レベルと、各レベルで認証トークンが必要かどうかについて説明します。

トークンが不要の場合の配備

ホスト管理者が、認証トークンを必要とせずに、証明書をプライマリ以外のホストに配備できるセキュリティレベルでは、次の手順を実行します。

トークンが不要の場合にホスト ID ベースの証明書を生成して配備する方法

1. ホスト管理者が、プライマリサーバーが信頼できる状態を確立するためにプライマリ以外のホストで次のコマンドを実行します。

   ```
   nbcertcmd -getCACertificate
   ```

2. プライマリ以外のホストで次のコマンドを実行します。

   ```
   nbcertcmd -getCertificate
   ```

   メモ: 複数の NetBackup ドメインと通信するには、そのホストの管理者が -server オプションを使って各プライマリサーバーから証明書を要求する必要があります。

   特定のプライマリサーバーから証明書を取得するには、次のコマンドを実行します。

   ```
   nbcertcmd -getCertificate -server primary_server_name
   ```

3. 証明書がホストに配備されていることを検証するには、次のコマンドを実行します。

   ```
   nbcertcmd -listCertDetails
   ```

トークンが必要な場合の配備

CA からホスト ID ベースの証明書を配備するために認証トークンがホストで必要となるセキュリティレベルでは、次の手順を実行します。

トークンが必要な場合にホスト ID ベースの証明書を生成して配備するには

1. 操作を続行する前に、ホスト管理者が認証トークン値を CA から取得している必要があります。トークンは各環境のさまざまなセキュリティガイドラインに応じて、電子メール、ファイル、または口頭で管理者に伝えられます。
2. プライマリサーバーが信頼できる状態を確立するためにプライマリ以外のホストで次のコマンドを実行します。

   ```
   nbcertcmd -getCACertificate
   ```

3. プライマリ以外のホストで次のコマンドを実行して、メッセージが表示されたらトークンを入力します。

   ```
   nbcertcmd -getCertificate -token
   ```

   メモ: 複数の NetBackup ドメインと通信するには、そのホストの管理者が `-server` オプションを使って各プライマリサーバーから証明書を要求する必要があります。

   管理者がトークンをファイルで取得した場合、次を入力します。

   ```
   nbcertcmd -getCertificate -file authorization_token_file
   ```

4. 証明書がホストに配備されていることを検証するには、次のコマンドを実行します。

   ```
   nbcertcmd -listCertDetails
   ```

   クラスタの証明書を表示するには、`-cluster` オプションを使用します。

ホスト ID ベースの証明書の非同期的配備

ホスト ID ベースの証明書は、インストールまたはアップグレード中に、NetBackup ホストに自動的に配備されます。証明書の自動配備を正常に行うには、証明書の配備先とするホストをプライマリサーバーに接続する必要があります。

特定のシナリオで、証明書の配備時にホストとプライマリサーバーを接続する必要がない場合は、ホスト ID ベースの証明書を非同期的に作成、署名、および配備できます。

ホスト ID ベースの証明書を非同期的に配備する方法

1 このコマンドを実行できるのは、ホスト管理者のみです。

証明書の署名要求を作成します。証明書を配備するプライマリサーバーホスト以外のホストで、次のコマンドを実行します。

```
nbcertcmd -createCertRequest -requestFile request_file_name
-server primary_server_name
```

オプションで、証明書の署名要求 (CSR) ファイルを任意の NetBackup ホストにコピーすることもできます。

2 ホスト上のプライマリサーバーから署名済みの証明書を取得します。認証トークンは必須です。ホストに証明書がすでにある場合は、再発行トークンが必要です。

ホストで次のコマンドを実行します。

```
nbcertcmd -signCertificate -requestFile request_file_name
-certificateFile certificate_file_name -token
```

メモ: CSR (証明書署名要求) が生成されたときと同じかそれ以上のバージョンの NetBackup が配備されたホストでは、必ず `-signCertificate` オプションを使用してください。

---

3 手順 2 で生成された署名済み証明書をコピーし、ホストの管理者に伝えます。

4 このコマンドを実行できるのは、ホスト管理者のみです。

ホストに署名済み証明書を配備するには、クライアントで次のコマンドを実行します。

```
nbcertcmd -deployCertificate -certificateFile
certificate_file_name
```

証明書の有効期間に対するクロックスキューの意味

プライマリサーバーは、証明書を発行するときに、ホストに対する使用有効期間を決定します。プライマリサーバーは独自の時刻に基づいて証明書の有効期間を設定し、Not before と Not after の 2 つのタイムスタンプを記録します。証明書はそれらの 2 つのタイムスタンプ間の期間のみ有効です。

プライマリサーバーのクロックと証明書を受信するホストのクロックを同期することで、タイムスタンプに基づいて予期される期間、証明書が有効になります。

ホストは、そのクロックがタイムゾーンの正しい時間に設定されている限り、異なるタイムゾーンに属することができます。一般的に、ネットワークタイムプロトコル (NTP) などのサービスを使って NetBackup ドメインのすべてのホストのすべてのクロックを自動的かつ継続的に同期することが推奨されます。

クロックが同期されていない場合、その差異により次の結果が生じる場合があります。

- ホストのクロックがプライマリサーバーよりも進んでいる場合、証明書の有効期間がそのホストで予期される期間よりも短くなります。差異が極端に大きく、クロックが証明書の有効期間を超えてずれている場合は、プライマリサーバーが新しい証明書を発行した時点でその証明書が期限切れとして扱われる可能性があります。
- ホストのクロックがプライマリサーバーよりも遅れている場合、プライマリサーバーによって発行された新しい証明書がホストで利用できない場合があります。これは、ホストがその証明書がまだ有効でないと判断するためです。

プライマリサーバーのクロックとホストのクロックが同期しているかどうかを判断するには

1. ホストで次のコマンドを実行して、ホストのクロックがプライマリサーバーのクロックと同期しているかを判断します。

   ```
   nbcertcmd -checkClockSkew -server primary_server_name
   ```

2. このコマンドは次の結果を返します。

   - 両方のクロックが同期している場合、次が表示されます。

     ```
     The current host clock is in sync with the primary server.
     ```

   - 現在のホストのクロックがプライマリサーバーより遅れている場合、コマンドはその差異を秒単位で報告します。

     ```
     The current host clock is behind the primary server by 36
     seconds(s).
     ```

   - 現在のホストのクロックがプライマリサーバーより進んでいる場合、コマンドはその差異を秒単位で報告します。

     ```
     The current host clock is ahead of the primary server by 86363
     second(s).
     ```

   - このコマンドをプライマリサーバーで実行すると、チェックが省略され、次が表示されます。

     ```
     Specified server is same as the current host. Clock skew check
     is skipped.
     ```

   ホストでのクロックスキューにより証明書の有効期限に関する問題が発生する場合は、必要に応じて修正する処理を行う必要があります。

プライマリサーバー (認証局) との信頼の設定

各 NetBackup ホストは認証局 (CA) として動作する NetBackup プライマリサーバーを信頼する必要があります。信頼はホストがホスト ID ベースの証明書を要求する上で不可欠です。CA 証明書は、ドメイン内の他のホストを認証するために使用可能で、各ホストのトラストストアに格納されています。信頼を設定するときに、プライマリサーバーからの証明書の要求も行われます。

p.300 の「ホスト ID ベースの証明書の自動配備」を参照してください。

ホストのトラストストアへの CA 証明書の追加

nbcertcmd -listCACertDetails コマンドを実行して、ホストのトラストストアにある CA 証明書のリストを表示します。出力に、ホストがすでに信頼しているすべてのプライマリサーバーが表示されます。

プライマリサーバー (CA) との信頼を確立するには

1 ホスト管理者は、正当なソースを介して提供されたルート証明書の指紋を保有している必要があります。ほとんどの場合、このソースは電子メール、ファイルまたは内部 Web サイトによって指紋を提供したプライマリサーバー管理者です。次の項ではその処理について説明します。

p.306 の「認証局の指紋の検索と伝達」を参照してください。

2 NetBackup ホストから次のコマンドを実行します。

```
nbcertcmd -getCACertificate -server master_server_name
```

3 確認出力で、y を入力して続行します。

次に例を示します。

```
nbcertcmd -getCACertificate -server master1
Authenticity of root certificate cannot be established.
The SHA1 fingerprint of root certificate is B8:2B:91:E1:4E:78:D2:
25:86:4C:29:C5:92:16:00:8D:E8:2F:33:DD.
```

メモ: 表示される指紋は、ホスト管理者がプライマリサーバー管理者から受信した root 証明書の指紋と一致する必要があります。y を入力して、ホストのトラストストアに CA 証明書を追加することに合意します。

```
Are you sure you want to continue using this certificate ? (y/n):
 y
The validation of root certificate fingerprint is successful.
CA certificate stored successfully.
```

4 次に、管理者は次のタスクを実行します。

p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

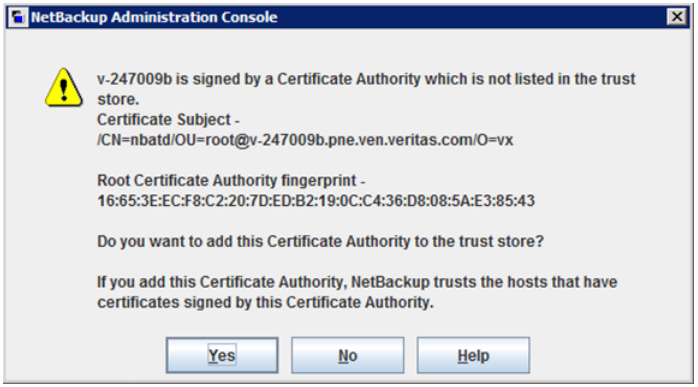
このコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

NetBackup 管理コンソールのメッセージを介した CA 証明書の追加

NetBackup 管理コンソールと[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]ユーザーインターフェースは、セキュアなチャネルを経由して NetBackup ホスト (プライマリサーバー、メディアサーバー、またはクライアント) との通信を行います。NetBackup は、NetBackup 認証局 (CA) により発行される NetBackup ホスト ID ベースまたはホスト名ベースのセキュリティ証明書を使ってこのチャネルをセキュア化します。

ユーザーが NetBackup ホスト上で 図 17-1を実行している場合に、NetBackupMessage inquiring whether to add a Certificate Authority (CA) to the trust store は NetBackup 管理コンソールに表示されます。ユーザーは、NetBackup 管理コンソールを使用してもう 1 つの NetBackup ホスト (ターゲットホスト) への接続を試みます。しかし、ターゲットホストにセキュリティ証明書を発行した CA は、コンソールが起動されたホストのトラストストアにはありません。

図 17-1 認証局 (CA) をトラストストアに追加するかどうかを照会するメッセージ



ダイアログに表示される CA の指紋を検証するには、次の項を参照してください。

p.306 の「認証局の指紋の検索と伝達」を参照してください。

このメッセージでユーザーが [はい (Yes)] を選択する場合は、コンソールが実行されているホストのトラストストアに CA が追加されます。このホストは、メッセージに示されている CA が署名した証明書を持つすべてのホストを信頼するようになります。

認証局の指紋の検索と伝達

プライマリサーバーの管理者は、ホストが CA 証明書をトラストストアに追加できるように、CA 証明書の指紋を検索して、個別のホストの管理者に伝える必要があります。

SHA-1 指紋または SHA-256 指紋の両方がサポートされます。

CA 証明書の指紋を検索するには

1 プライマリサーバーの管理者は、NetBackup Web UI またはコマンドラインを使用して指紋を検索できます。

NetBackup Web UI を使用する場合:

- [セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
- [認証局 (Certificate Authority)]をクリックします。
- 次の情報が表示されます。

サブジェクト名 (Subject name)	目的のプライマリサーバーの証明書を識別します。
開始日 (Start date)	証明書が有効化された日付。
有効期限 (Expires)	証明書の有効期限。
SHA-1 指紋 (SHA-1 fingerprint)	SHA-1 アルゴリズムを使用して計算された証明書のハッシュ値。[クリップボードにコピー (Copy to clipboard)]は、管理者が指紋をホスト管理者に伝えるのに役立ちます。
SHA-256 指紋 (SHA-256 fingerprint)	SHA-256 アルゴリズムを使用して計算された証明書のハッシュ値。[クリップボードにコピー (Copy to clipboard)]は、管理者が指紋をホスト管理者に伝えるのに役立ちます。

コマンドラインを使用する場合:

- 次のコマンドをプライマリサーバーで実行して、ルート証明書の指紋を表示します。

```
nbcertcmd -listCACertDetails
```

複数の CA 証明書が表示されている場合は、[サブジェクト名 (Subject name)]を使用します。

2 プライマリサーバーの管理者は、指紋をホスト管理者に電子メール、ファイル、または内部 Web サイトを介して伝えます。

ホスト管理者はこの指紋値を使用して、ホストが `nbcertcmd -getCACertificate` を実行するときに表示される指紋を検証します。これにより、CA 証明書の信頼性が確認されます。

vssat コマンドを使用して CA 証明書の指紋を表示する

`vssat` コマンドは CA 証明書の指紋を表示するためにも使用できます。次のオプションで `vssat` を使います。

```
vssat showcred -p nbatd
```

ただし、nbcertcmd -listCACertDetails の使用と vssat の使用には次の違いがあります。

- vssat は指紋をハッシュとして表示し、コロンをセパレータとして使用しません。
- ホストが複数の認証局を信頼する場合、nbcertcmd コマンドはすべての CA 証明書を表示します。[件名 (Subject Name)]には CA の識別情報が表示されます。

証明書の配備の強制実行または上書き

状況によって、-force オプションを nbcertcmd -getCertificate コマンドで使う必要があります。たとえば、ホストへの証明書の配備を強制実行する場合、または既存のホスト ID ベースの証明書情報を上書きして新しい証明書をフェッチする場合などです。

証明書の配備の強制実行

ホストにホスト ID ベースの証明書がすでに存在するときに、その古い証明書を新しい証明書で上書きする必要があることがあります。この操作は、プライマリサーバーが新しいサーバーに交換されたときなどに必要です。クライアントには古いサーバーに対する古い証明書が存在するため、クライアントで nbcertcmd -getCertificate コマンドを実行すると、次のエラーで失敗します。

```
Certificate already exists for the server.
```

既存のホスト ID ベースの証明書情報を上書きして新しい証明書をフェッチするには、次の手順を使います。

ホスト上で証明書の配備を強制実行するには

◆ ホスト管理者は、プライマリ以外のホストで次のコマンドを実行します。

```
nbcertcmd -getCertificate -server primary_server_name -force
```

- プライマリサーバーのセキュリティ設定に応じて、トークンも指定する必要がある可能性があります。
  p.318 の「認証トークンの作成」を参照してください。
- -cluster オプションを使って、クラスタ証明書を配備します。

既存のホスト ID ベースの証明書情報を上書きして、新しい証明書をフェッチする

ホストに証明書が発行されている場合でも、時間の経過に伴い証明書が破損したり、証明書ファイルが削除されていることがあります。

プライマリ以外のホストの管理者は、次のコマンドを実行して、証明書の状態を確認できます。

```
nbcertcmd -listCertDetails
```

- 証明書が破損している場合は、コマンドは次のエラーにより失敗します。

```
Certificate could not be read from the local certificate store.
```

- 証明書の詳細が表示されない場合は、証明書は利用できません。

既存のホスト ID ベースの証明書情報を上書きして、新しい証明書をフェッチするには、次の手順を使います。

新しいホスト ID ベースの証明書をフェッチするには

◆ ホスト管理者は、プライマリ以外のホストで次のコマンドを実行します。

```
nbcertcmd -getCertificate -force
```

- プライマリサーバーのセキュリティ設定に応じて、トークンも指定する必要がある可能性があります。
p.318 の「認証トークンの作成」を参照してください。
- `-cluster` オプションを使って、クラスタ証明書を配備します。

プライマリ以外のホストで NetBackup を再インストールするときのホスト ID ベースの証明書の保持

管理者はホストから NetBackup をアンインストールし、そのホストでクリーンインストールを実行できます。アンインストールと再インストールのプロセスを通してホストの ID を保持するには、次の手順を参照してください。

NetBackup を再インストールするときにホスト ID ベースの証明書を保持するには

1. ホストですべての NetBackup サービスを停止します。
2. 次のディレクトリのバックアップを作成します。

   Windows の場合:

   Install_path¥NetBackup¥var¥VxSS

   Install_path¥NetBackup¥var¥webtruststore

   UNIX の場合:

   /usr/openv/var/vxss

   /usr/openv/var/webtruststore
3. NetBackup クラスタサーバーを使っている場合は、次のディレクトリのバックアップも作成します。

   Shared_disk¥var¥global¥vxss

   Shared_disk¥var¥global¥webtruststore
4. ホストに NetBackup を再インストールします。
5. 手順 2 と手順 3 でバックアップを作成したデータをリストアします。

プライマリサーバーと接続されていないクライアントでの証明書の配備

NetBackup は、ホストがプライマリサーバーと接続されているかどうかを検出できます。接続されていない場合、NetBackup はメディアサーバーの組み込み HTTP トンネルを使用して、自動的にプライマリサーバーに接続要求をルーティングしようとします。

NetBackup が自動的にホストとプライマリサーバーとの接続を検出できない場合、または接続要求のルーティングに適切なメディアサーバーを見つけることができない場合は、HTTP トンネルオプションを手動で設定する必要があります。

p.340 の「非武装地帯にある NetBackup クライアントとプライマリサーバーの間の HTTP トンネルを介した通信について」を参照してください。

プライマリサーバーと接続されていないクライアントに証明書を配備する場合は、次のトピックを参照してください。

p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

メモ: 別のホスト経由で要求をルーティングすると、プライマリサーバーは証明書要求の真正性を検証できません。そのため、認証トークンが必要になります。

ホスト ID ベースの証明書の有効期限と更新について

NetBackup ホスト ID ベースの証明書は発行日から 1 年で期限切れになります。これらの証明書は期限切れの日の 180 日前に自動的に更新されます。証明書が正常に更新されるまで、証明書の更新要求が定期的に送信されます。自動更新では、更新プロセスがユーザーに対して透過的に実行されます。

メモ: ホスト ID ベースの証明書の自動更新は、構成ファイル (Windows レジストリの場合。UNIX の場合は bp.conf ファイル) の パラメータを使用して無効にできます。Ashwini - 19th Jan 2018 - ET 3938304 - DISABLE_CERT_AUTO_RENEWNetBackup

詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

更新要求は常に既存の証明書を使って認証されます。したがって、更新プロセスは、証明書の配備セキュリティレベルに関係なく、認証トークンの使用を必要としません。

次の手順に示すように、既存の証明書が期限切れになってていない場合、ホスト管理者は手動による更新要求を開始します。

ホスト ID ベースの証明書を手動で更新するには

- ホスト管理者は、プライマリ以外のホストで次のコマンドを実行します。

  ```
  nbcertcmd -renewCertificate
  ```

  - プライマリドメイン以外の NetBackup ドメインに対応する証明書は、`-server` オプションを指定することで手動で更新できます。

- NetBackup クラスタサーバーのクラスタ証明書を更新するには、-cluster オプションを使います。

証明書が期限切れになると、ホストの管理者は手動で証明書を再発行する必要があります。

p.313 の「ホスト ID ベースの証明書の再発行について」を参照してください。

メディアサーバーおよびクライアントからの重要な証明書とキーの削除

次のシナリオのクローンプロセスで、NetBackup メディアサーバーとクライアントから特定の重要な証明書とキーを削除する場合は、後続のコマンドを使用します。

- アクティブな NetBackup ホストからクローンとして作成された仮想マシンでコマンドを実行する場合
- クローン作成のために仮想マシンのゴールドイメージを作成する前にコマンドを実行する場合

```
nbcertcmd -deleteAllCertificates
```

メモ: このコマンドはメディアサーバーとクライアントでのみ許可されます。このコマンドはプライマリサーバーでは許可されません。

この操作により、以下の場所にある当該の重要情報 (証明書とキー) が削除またはシュレッドされます。

Windows の場合:

- C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥certmapinfo.json
- C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥credentials¥*<certificate>*
  例:
  C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥credentials¥6d92d4dd-ed2d-43de-adb1-bf333aa2cc3c
- C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥credentials¥keystore¥PrivKeyFile.pem (シュレッドされる)
- C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥at¥systemprofile¥certstore¥*<certificate>*
  例:
  C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥at¥systemprofile¥certstore¥9345b05e-lilycl2nb!1556!nbatd!1556.0

- C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥at¥systemprofile¥certstore¥keystore¥PrivKeyFile.pem (シュレッドされる)
- C:¥Program Files¥Veritas¥NetBackup¥var¥VxSS¥at¥systemprofile¥certstore¥keystore¥PubKeyFile.pem

UNIX の場合:

- /usr/openv/var/vxss/certmapinfo.json
- /usr/openv/var/vxss/credentials/*<certificate>*
  例:
  /usr/openv/var/vxss/credentials/
  f4f72ef3-2cfc-42a4-ab5a-65fd09e8b63e
- /usr/openv/var/vxss/credentials/keystore/PrivKeyFile.pem (シュレッドされる)
- /var/vxss/at/root/.VRTSat/profile/certstore/*<certificate>*
- /var/vxss/at/root/.VRTSat/profile/certstore/keystore/PubKeyFile.pem
- /var/vxss/at/root/.VRTSat/profile/certstore/keystore/PrivKeyFile.pem (シュレッドされる)

仮想マシンのクローンを作成する前にホストからホスト ID ベースの証明書情報を消去する

仮想マシンのクローンを作成すると、ID が盗まれる危険性が生じます。複数のホストで同一のキーペアを使うべきではありません。この手順では、ホストの各コピーが一意のキーペアと ID を取得することを確実にします。

仮想マシンのクローンの作成が一度のみの操作である場合は、それを行う前に (またはクローン作成するマシンのゴールドイメージを作成する前に) 次の手順を実行します。

クローンを作成する前にホストからホスト ID ベースの証明書を消去するには

1. ホストですべての NetBackup サービスを停止します。
2. 次の場所からすべてのファイルとディレクトリを削除します。

   Windows の場合:

   Install_path¥NetBackup¥var¥VxSS¥at¥*

   Install_path¥NetBackup¥var¥VxSS¥credentials¥*

   Install_path¥NetBackup¥var¥webtruststore¥*

   UNIX の場合:

   /usr/openv/var/vxss/at/*

   /usr/openv/var/vxss/credentials/*

   /usr/openv/var/webtruststore/*
3. 次のファイルを削除します。

   Windows の場合: *Install_path*¥NetBackup¥var¥VxSS¥certmapinfo.json

   UNIX の場合: /usr/openv/var/vxss/certmapinfo.json
4. NetBackup クラスタサーバーを使っている場合は、さらに次の手順を実行します。
5. 次の場所からすべてのファイルとディレクトリを削除します。

   Shared_disk¥var¥global¥vxss¥at¥*

   Shared_disk¥var¥global¥vxss¥credentials¥*

   Shared_disk¥var¥global¥webtruststore¥*
6. 次のファイルを削除します。

   Shared_disk¥var¥global¥vxss¥certmapinfo.json
7. 仮想マシンのクローン作成に進みます。

ホスト ID ベースの証明書の再発行について

次の場合は、証明書を再発行する必要があります。

- 証明書が無効化され、後でそのホストを信頼できると再度判断した場合
- 証明書が期限切れになった場合
- 証明書がすでに発行されているホストで NetBackup を再インストールした場合
- ホストの名前を変更した場合
- ホストの鍵ペアが変更された場合

証明書の再発行は、NetBackup プライマリサーバーにすでに登録されている既存の NetBackup ホストの ID を悪意あるユーザーに知られないようにするための 1 つの手段です。ほとんどの場合、証明書の再発行には再発行トークンが必要です。

- NetBackup ホストのホスト ID ベースの証明書の再発行は、証明書の初回の配備とは異なります。証明書を再発行するには、次の手順を使います。
  p.314 の「再発行トークンの作成」を参照してください。
- 再発行トークンを一度取得したら、証明書の再発行プロセスは認証トークンを使った手動による証明書の配備とほぼ同じです。
  p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

プライマリサーバーは、証明書の再発行要求を受信すると、該当のホストの以前の有効な証明書すべてを無効化して、必要に応じて新しい証明書を生成します。

再発行トークンの作成

プライマリ以外のホストがプライマリサーバーにすでに登録されているのにそのホスト ID ベースの証明書が有効でなくなっている場合は、ホスト ID ベースの証明書を再発行できます。たとえば、証明書は期限切れ、破棄、消失などの理由で無効になります。

再発行トークンは証明書を再発行するときに使用できるトークンです。このトークンは、元の証明書と同じホスト ID を保持する特殊なトークンです。再発行トークンは特定のホストに結び付けられるため、追加のホストの証明書を要求するためにこのトークンを使うことはできません。

再発行トークンを作成するには

1. NetBackup Web UI を開きます。
2. 左側で、[セキュリティ (Security)]、[証明書 (Certificates)]の順に選択します。
3. 再発行トークンを必要とするホストを選択します。
4. [再発行トークンの生成 (Generate Reissue Token)]をクリックします。
5. トークンの名前を入力します。
6. [次で有効 (Valid for)]オプションからトークンが有効期間の日付を選択します。
7. [理由 (Reason)]フィールドに、再発行トークンの理由を入力します。この理由は監査イベントとしてログに表示されます。
8. [生成 (Generate)]をクリックします。

9 トークンの値をコピーするには、[クリップボードにコピー (Copy to clipboard)]をクリックします。

10 プライマリホスト以外のホストの管理者にトークンの値を伝えます。トークンの伝達方法は、環境のさまざまなセキュリティ要因によって異なります。トークンは、電子メール、ファイル、または口頭で伝えられます。

プライマリ以外のホストの管理者は、トークンを配備して別のホスト ID ベースの証明書を取得します。手順について詳しくは次のトピックを参照してください。

p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

nbcertcmd コマンドを使って再発行トークンを作成するには

1 プライマリサーバー管理者は、このタスクを実行するために NetBackup Web 管理サービスにログインしている必要があります。次のコマンドを使ってログインします。

```
bpnbat -login -logintype WEB
```

p.294 の「nbcertcmd コマンドオプションの Web ログインの要件」を参照してください。

2 プライマリサーバーで次のコマンドのいずれかを実行します。

証明書を再発行する必要があるホスト名を使う場合:

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

メモ: 証明書を再発行するホストのプライマリ名を指定する必要があります。ホスト用に追加されているホスト ID からホスト名へのマッピングを指定すると、証明書を再発行することができません。

証明書を再発行する必要があるホスト ID を使う場合:

```
nbcertcmd -createToken -name token_name -reissue -hostId host_id
```

追加のパラメータを使って、有効期間と作成の理由を指定することもできます。

nbcertcmd 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。

名前を変更した NetBackup ホストの証明書を要求するための追加手順

名前を変更した NetBackup ホストの証明書を要求するには、トークンの再発行に加えて、次の手順を実行する必要があります。

ホスト名を変更した後にホストの証明書を要求するには

1. プライマリサーバーの NetBackup 管理者は、名前変更済みの NetBackup ホストの再発行トークンを生成します。
2. NetBackup Web UI を使用して、承認されたホスト ID からホスト名へのマッピングの 1 つとして新しいホスト名を追加します。

   p.269 の「ホスト ID からホスト名へのマッピングの追加」を参照してください。

   または、nbhostmgmt -add コマンドラインインターフェースオプションを使うこともできます。

   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。
3. NetBackup 管理者は、名前変更済みホストのホスト ID ベースの証明書を無効化する必要があります。

   p.326 の「ホスト ID ベースの証明書の無効化」を参照してください。

   メモ: 証明書が無効化されたホストは NetBackup Web 管理コンソールサービス (nbwmc) と通信できなくなります。再発行トークンを使って新しい証明書を取得したホストは、再び nbwmc と通信できるようになります。
4. 証明書を無効にしたら、プライマリ以外のホストの管理者は、再発行トークンを使って名前変更済みのホストの証明書を取得する必要があります。

   p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

ホストの鍵ペアの変更

鍵が危殆化した場合や漏洩した場合は、鍵ペアの変更を検討します。鍵ペアの変更を行うと、新しいホスト ID ベースとホスト名ベースの両方の証明書が生成されます。

次の手順では、ホストの鍵ペアの変更と、新しい鍵ペアを使った新しい証明書の取得について説明します。

この手順をプライマリサーバーで実行しないでください。プライマリサーバー以外のホストでのみ実行してください。

ホストの鍵ペアを変更する方法

1. NetBackup ホストの管理者は次のディレクトリのバックアップを作成します。

   Windows の場合: *Install_path*¥NetBackup¥var¥VxSS¥at¥systemprofile

   UNIX の場合: /usr/openv/var/vxss/at/root
2. NetBackup ホストの管理者はそのディレクトリをホストから削除します。

3 ホスト側で NetBackup サービスを再起動します。

4 プライマリサーバーの管理者は次の手順を実行します。

- NetBackup Web 管理サービスにログインします。
  ```
  bpnbat -login -logintype WEB
  ```
  p.294 の「nbcertcmd コマンドオプションの Web ログインの要件」を参照してください。
- ホスト ID ベースの証明書を無効化します。
  ```
  nbcertcmd -revokeCertificate -host host_name
  ```
- 鍵ペアを変更する NetBackup ホストに対して再発行トークンを生成します。
  p.314 の「再発行トークンの作成」を参照してください。
- 新しいホスト名ベースの証明書を配備します。
  ```
  bpnbaz -ProvisionCert host_name
  ```

5 NetBackup ホストの管理者は、再発行トークンを使って、更新済みの鍵ペアを含む新しいホスト ID ベースの証明書を配備します。

次のコマンドを実行して、トークンを直接入力します。

```
nbcertcmd -getCertificate -force -token
```

トークンがファイル内にある場合は、次のコマンドを実行します。

```
nbcertcmd -getCertificate -force -file /directory/token_file
```

6 ホストが複数のプライマリサーバーを持つ場合は、各プライマリサーバーについて手順 4 から始まる操作を繰り返し実行します。

7 キーを変更した NetBackup ホストで NetBackup サービスを再起動します。

ホスト ID ベースの証明書のトークン管理について

マスターサーバーの管理者は、[トークン管理 (Token Management)]ユーティリティを使って、次のタスクを実行します。

- 新規認証トークンの作成
  セキュリティレベルに応じて、プライマリ以外の NetBackup ホストは、ホスト ID ベースの証明書を取得するために認証トークンを必要とする場合があります。プライマリサーバーの NetBackup 管理者はトークンを生成し、それをプライマリホスト以外のホストの管理者と共有します。その管理者は、プライマリサーバーの管理者の立ち会いなしで証明書を配備できます。
  p.318 の「認証トークンの作成」を参照してください。
- 認証トークンの削除
  p.320 の「認証トークンの削除」を参照してください。

- 認証トークンの詳細の表示
  p.320 の「認証トークンの詳細の表示」を参照してください。
- 無効または期限切れの認証トークンのクリーンアップ
  p.321 の「期限切れの認証トークンとクリーンアップについて」を参照してください。

認証トークンの作成

証明書の配備のセキュリティ設定に応じて、NetBackup ホストは、認証局 (プライマリサーバー) からホスト 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。

p.314 の「再発行トークンの作成」を参照してください。

- セキュリティ設定が[最高 (Very High)]の場合、すべての証明書要求でトークンが必要になります。この項で説明している手順を実行します。
- セキュリティ設定が[高 (High)]の場合、プライマリサーバーにとって既知であるホストに対して証明書が自動的に配備されます。ホストがプライマリサーバーに認識されていない場合は、認証トークンを使用して証明書を配備する必要があります。この場合、この項で説明している手順を実行します。
  プライマリサーバーにとって既知の意味については、次の項を参照してください。
  p.297 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。
- セキュリティ設定が[中 (Medium)]の場合、証明書を必要とするすべてのホストに証明書が自動的に配備されるので、この手順は通常必要ありません。ただし、プライマリサーバーは証明書を要求しているホストの IP とホスト名を相互検証できる必要があります。

メモ: プライマリサーバーとの接続性がないホストに代わり証明書を要求するには、トークンが必要です。

p.310 の「プライマリサーバーと接続されていないクライアントでの証明書の配備」を参照してください。

メモ: 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 ホストの認証トークンの作成には、この手順を使用しないでください。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.313 の「ホスト ID ベースの証明書の再発行について」を参照してください。

プライマリサーバーの NetBackup 管理者は、NetBackup 管理コンソールまたはコマンドラインを使ってトークンを作成できます。

NetBackup 管理 Web UI を使用してトークンを作成するには

1 左側のペインで、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。

2 [トークン管理 (Token Management)]ページで、[クリーンアップ (Cleanup)]を選択します。

[トークンの作成 (Create Token)]ダイアログボックスが表示されます。

3 分かりやすい一意の名前をトークンに付けて入力します。このフィールドは空白にできません。

たとえば、primary_server_1 に属する複数のホストの証明書を要求するトークンを作成し、Token1_MS1 という名前を付けます。[理由 (Reason)]フィールドにトークンに関する説明を入力すると役に立ちます。

4 トークンの使用可能回数として、[最大許可使用期間 (Maximum Uses Allowed)]オプションに数を入力します。デフォルトは 1 です。1 つのホストがトークンを 1 回のみ使うことができることを示しています。

複数のホストで同一のトークンを使うには、1 から 99999 までの数値を入力します。たとえば、8 つのホストのトークンを使用するには、8 を入力します。9 つ目のホストがこのトークンを使用しようとしても成功しません。

5 [次で有効 (Valid for)]オプションを使って、無効になり使えなくなるまでのトークン使用可能期間を指定します。[次で有効 (Valid for)] 日付以後は、プライマリサーバーで別のトークンを生成する必要があります。

1 から 999 時間または 1 から 999 日間で期間を選択します。

6 トークンを作成する理由を入力することもできます。この理由は、このダイアログのその他のエントリと共に監査ログに表示されます。

7 [作成 (Create)]を選択します。

8 新しいトークンがダイアログに表示されます。[コピー (Copy)]を選択して、トークンの値をクリップボードに保存します。

9 プライマリホスト以外のホストの管理者にトークンの値を伝えます。トークンの伝達方法は、環境のさまざまなセキュリティ要因によって異なります。トークンは、電子メール、ファイル、または口頭で伝えられます。

10 プライマリ以外のホストの管理者は、トークンを使用して認証局からホスト ID ベース証明書を取得します。指示については次の手順を参照してください。

p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

nbcertcmd コマンドを使ってトークンを作成するには

◆ ホストで次のコマンドを実行します。

```
nbcertcmd -createToken -name token_name
```

次に例を示します。

```
nbcertcmd -createToken -name testtoken

Token FCBVYUTDUIELUDOE created successfully.
```

追加のパラメータを使って、最大使用数、有効期間、作成の理由を指定できます。

nbcertcmd 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。

認証トークンの削除

特定の認証トークンを削除するには、NetBackup Web UI またはコマンドラインを使います。期限切れになっていない場合や[最大許可使用期間 (Maximum Uses Allowed)]カウントに達していない場合でも、トークンを削除できます。

NetBackup 管理 Web UI を使用してトークンを削除するには

1 左側のペインで、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。

2 右ペインで、削除するトークンを選択します。

3 [削除 (Delete)]をクリックします。

4 確認ダイアログボックスで[はい (Yes)]をクリックして、トークンを削除します。

コマンドラインを使ってトークンを削除するには

◆ nbcertcmd -deleteToken コマンド (追加のパラメータを含む) を実行します。

nbcertcmd 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。

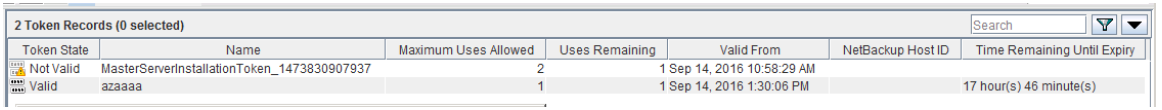
認証トークンの詳細の表示

各認証トークンの詳細は NetBackup 管理コンソールに表示するか、コマンドラインから表示できます。

NetBackup 管理 Web UI を使ってトークンの詳細を表示するには

1 左側のペインで、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。

2 [トークン管理 (Token Management)]ページに、トークンの詳細が表示されます。



nbcertcmd コマンドを使ってトークンの詳細を表示するには

- プライマリサーバーで `nbcertcmd -listToken` コマンド (追加のパラメータを含む) を実行して、トークンの詳細を表示します。

  トークンの詳細が表示されます。

期限切れの認証トークンとクリーンアップについて

認証トークンは次のいずれかの (先に発生する) 状況で、期限切れになります。

- 現在の日付と日時の組み合わせがトークンの[次で有効 (Valid For)]の値よりも後の日時である場合。
- [最大許可使用期間 (Maximum Uses Allowed)]要求にトークンを使用している場合。

期限切れの認証トークンはトークンデータベースに残りますが、証明書の配備要求を認証するために使うことはできません。

期限切れのトークンは個別に削除するか、クリーンアップ操作を使って一度にすべてを削除できます。クリーンアップ操作は、すべての期限切れのトークンをトークンデータベースから削除します。

NetBackup 管理 Web UI を使って期限切れの認証トークンをクリーンアップするには

1. 左側のペインで、[セキュリティ (Security)]、[トークン (Tokens)]の順に選択します。
2. [トークン管理 (Token Management)]ページで、[クリーンアップ (Cleanup)]を選択します。
3. [はい (Yes)]をクリックして、すべての期限切れのトークンをクリーンアップし、トークンデータベースから削除します。

コマンドラインを使ってトークンをクリーンアップするには

- すべての期限切れのトークンを削除するには、`nbcertcmd -cleanupToken` コマンドを使います。

p.320 の「認証トークンの削除」を参照してください。

ホスト ID ベースの証明書失効リストについて

NetBackup 証明書失効リスト (CRL) は、失効日前に無効化されたホスト ID ベースのデジタルセキュリティ証明書のリストです。無効化された証明書を所有するホストは、信頼されなくなります。

NetBackup 証明書失効リストは、Internet Engineering Task Force が https://www.ietf.org の RFC 5280 で公表している証明書失効リストプロファイルに準拠しています。NetBackup 認証局が CRL に署名します。NetBackup プライマリサーバーが認証局です。CRL は公開されており、安全な送信を必要としません。誰でも自由にアクセスできる CRL エンドポイントが開かれています。

すべての NetBackup ホストは、他の NetBackup ホストと通信できるように、有効なセキュリティ証明書と有効な CRL を持つ必要があります。

NetBackup が新しい CRL を生成する頻度

NetBackup プライマリサーバーは、次のように新しい CRL を生成します。

- 起動時。
- CRL が最後に生成されてから 60 分後。
- NetBackup は、5 分ごとに新しく無効化された証明書を確認します。証明書の無効化後に NetBackup で Web サーバーの更新にかかる時間は最大 5 分です。

CRL は 7 日後に期限切れになります。

NetBackup ホストが CRL を取得する頻度

NetBackup ホストがホストにインストールされている場合、NetBackup ホストが CRL を取得します。また、NetBackup ホストは、NetBackup ソフトウェアのアップグレード中に新しい CRL を取得します。

インストールまたはアップグレード後に、各ホストはホストが起動されてから一定の時間間隔で新しい CRL を要求します。(NetBackup はプル方式を使用してホストの CRL を更新します)。次の表に示すように、NetBackup プライマリサーバー証明書の配備セキュリティレベルによって時間間隔が決まります。

表 17-7 CRL 更新間隔

セキュリティレベル	CRL 更新間隔
最高 (Very High)	1 時間
高 (High)	4 時間
中 (Medium)	8 時間

p.297 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。

スケジュール設定された更新間隔の前に新しい CRL を取得できます。

p.323 の「 プライマリサーバーでの CRL の更新 」を参照してください。

p.323 の「NetBackup ホストの CRL の更新」を参照してください。

詳細情報

p.264 の「NetBackup のセキュリティ証明書の概要」を参照してください。

p.294 の「ホスト ID ベースの証明書について」を参照してください。

p.324 の「ホスト ID ベースの証明書の無効化について」を参照してください。

プライマリサーバーでの CRL の更新

プライマリサーバーで CRL を更新するには、次の手順を使用します。この手順では、NetBackup 認証局から最新の CRL を取得し、プライマリサーバーにコピーします。環境内のホストが最近無効にされた場合は、CRL がホストの無効化を反映するまで最大 5 分待ちます。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

プライマリサーバーで CRL を更新するには

1. プライマリサーバーに管理者としてログインします。

   クラスタ化されたプライマリサーバーの場合は、アクティブノードにログインします。

2. クラスタ化されたプライマリサーバーの場合は、次のコマンドを実行します。

   ```
   nbcertcmd -getCRL -cluster [-server primary_server_name]
   ```

   デフォルト以外の NetBackup ドメインから CRL を取得するには、`-server primary_server_name` オプションおよび引数を指定します。

3. 次のコマンドを実行します。

   ```
   nbcertcmd -getCRL [-server primary_server_name]
   ```

NetBackup ホストの CRL の更新

NetBackup ホストの CRL を更新するには、次の手順を使用します。この手順では、NetBackup 認証局から現在の CRL が取得され、ローカルホストにコピーされます。環境内のホストが最近無効にされた場合は、CRL がホストの無効化を反映するまで最大 5 分待ちます。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

NetBackup ホストの CRL を更新するには

1 CRL の更新が必要な NetBackup ホストで、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。

```
nbcertcmd -getCRL [-server primary_server_name]
```

デフォルト以外の NetBackup ドメインから CRL を取得するには、`-server`*primary_server_name* オプションおよび引数を指定します。

ホスト ID ベースの証明書の無効化について

NetBackup デジタルセキュリティ証明書を無効化すると、NetBackup はそのホストの他の証明書を無効化します。NetBackup はホストを信頼しなくなり、他の NetBackup ホストと通信できなくなります。

NetBackup Web UI を使って証明書を無効化する場合は、次のいずれかの理由を選択する必要があります。

変更されたアフィリエーション (Affiliation Changed)	ホストがアフィリエーションを別の NetBackup ドメインに変更した。
CA の危殆化 (CA Compromise)	認証局が危殆化した。
操作の停止 (Cessation of Operation)	ホストが NetBackup ホストではなくなった。NetBackup メディアサーバーまたはクライアントを廃止した場合など。
キーの危殆化 (Key Compromise)	証明書キーが危殆化した。
優先済み (Superseded)	新しい証明書が無効化される証明書よりも優先される。
指定されていません (Unspecified)	その他の指定されていない理由。セキュリティイベントを調査するときに一時的に権限を一時停止する場合など。

証明書を無効化した後でホストを信頼できると判断した場合は、そのホストに新しい証明書をプロビジョニングします。これは、再発行トークンを使って行います。

p.313 の「ホスト ID ベースの証明書の再発行について」を参照してください。

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

ホストの証明書を無効化した後は、NetBackup で次の操作を行うことを検討します。

- バックアップポリシーからホストを削除します。

- NetBackup メディアサーバーを無効化します。

悪質な意図を持つ人物が証明書とキーを使うことができないようにするために、NetBackup に関連がない操作についても検討する必要があります。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

ホストとプライマリサーバー間の信頼の削除

NetBackup ホストはいつでも複数の認証局 (プライマリサーバー) を信頼できます。さまざまな理由により、以前に信頼されていたプライマリサーバーから信頼を削除することが NetBackup ホスト側で必要になる場合があります。

たとえば、NetBackup クライアントを別のプライマリサーバーに移動する場合は、移動元のプライマリサーバーから信頼を削除することを推奨します。セキュリティのベストプラクティスでは、正常に機能するために必要最小限のエンティティを信頼することが推奨されます。さらに、NetBackup ホストが特定の NetBackup ドメインのホストと通信する必要がなくなった場合に、そのプライマリの CA 証明書をホストのトラストストアから削除します。

メモ: CA 証明書の削除によって、ホストが CA から取得したホスト ID ベースまたはホスト名ベースの証明書が削除されることはありません。`nbcertcmd -listCertDetails` では、引き続きホスト ID ベースの証明書が表示されます。

ホストから CA 証明書を削除すると、そのホストは CA を信頼しなくなるため、CA によって発行されたホスト ID ベースの証明書が自動的に更新されなくなります。最終的に、ホスト ID ベースの証明書は期限切れになります。

ホストとプライマリサーバー間の信頼の削除

1 プライマリ以外のホストの管理者は次のコマンドをホストで実行して、プライマリサーバーの CA 証明書の指紋を判別します。

```
nbcertcmd -listCACertDetails
```

この出力例では、ホストに 2 つのプライマリサーバーからの証明書が存在します。

```
nbcertcmd -listCACertDetails
     Subject Name : /CN=nbatd/OU=root@master1.abc.com/O=vx
       Start Date : Aug 23 14:16:44 2016 GMT
      Expiry Date : Aug 18 15:31:44 2036 GMT
 SHA1 Fingerprint : 7B:0C:00:32:96:20:36:52:92:E8:62:F3:56:
74:8B:E3:2E:4F:22:4C

     Subject Name : /CN=nbatd/OU=root@master2.xyz.com/O=vx
       Start Date : Aug 25 12:09:55 2016 GMT
      Expiry Date : Aug 20 13:24:55 2036 GMT
 SHA1 Fingerprint : 7A:C7:6E:68:71:6B:82:FD:7E:80:FC:47:F6:
8D:B2:E1:40:69:9C:8C
```

2 管理者が 2 番目のプライマリサーバーに対する信頼を削除する場合は、ホストで次のコマンドを実行します。

```
nbcertcmd -removeCACertificate -fingerprint 7A:C7:6E:68:71:
6B:82:FD:7E:80:FC:47:F6:8D:B2:E1:40:69:9C:8C
```

コロンを含む、指紋全体を含めます。

警告: このコマンドは、トラストストアから CA 証明書を削除します。トラストストアは NetBackup サービスと NetBackup Web 管理コンソールサービス (`nbwebsvc`) によって参照されます。

---

3 プライマリサーバーの NetBackup 管理コンソールで、証明書の状態が[有効(Active)]として表示されます。ただし、その証明書は自動的に更新されず、最終的に期限切れになります。NetBackup 管理者は、そのホストを NetBackup ドメインの一部として含めない場合、その証明書を無効にする必要があります。

ホスト ID ベースの証明書の無効化

NetBackup 管理者は、さまざまな状況下でホスト ID ベースの証明書の無効化を検討します。たとえば、管理者がクライアントセキュリティの危殆化を検出した場合、クライアントが廃止された場合、NetBackup がホストからアンインストールされた場合などが該当しま

す。無効化した証明書を使ってプライマリサーバー Web サービスと通信することはできません。

p.324 の「ホスト ID ベースの証明書の無効化について」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管理者が明示的に無効化することが推奨されます。

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

NetBackup 管理 Web UI を使ってホスト ID ベースの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 証明書のタブで、無効化する証明書を選択します。
3. [証明書の無効化 (Revoke Certificate)]を選択します。
4. ドロップダウンリストから理由を選択して、[はい (Yes)]をクリックします。
5. ホストの証明書を無効化した後、NetBackup で次の操作を行います。
   - バックアップポリシーからホストを削除します。
   - NetBackup メディアサーバーを無効化します。

コマンドラインを使ってホスト ID ベースの証明書を無効化するには

1. プライマリサーバー管理者は、このタスクを実行するために NetBackup Web 管理サービスにログインしている必要があります。次のコマンドを使用してログインします。

   ```
   bpnbat -login -logintype WEB
   ```

   p.294 の「nbcertcmd コマンドオプションの Web ログインの要件」を参照してください。

2. 次のコマンドのいずれかを実行して、ホスト名またはホスト ID を使って証明書を無効化します。

   ホスト名を使う無効化:

   ```
   nbcertcmd -revokeCertificate -host host_name
   ```

   メモ: 証明書を無効化するホストのプライマリ名を指定する必要があります。ホスト用に追加されているホスト ID からホスト名へのマッピングを指定すると、証明書を無効化することができません。

   ホスト ID を使う無効化:

```
nbcertcmd -revokeCertificate -hostID host_id
```

追加のパラメータを使って、無効化の理由コードとプライマリサーバーを指定できます。

3 ホストの証明書を無効化した後、NetBackup で次の操作を行います。

- バックアップポリシーからホストを削除します。
- NetBackup メディアサーバーを無効化します。

メモ: 証明書を無効化しても、その証明書はプライマリ以外のホストのローカルストアから削除されません。

NetBackup ホストの証明書の状態の確認

NetBackup CA が署名した証明書を使用する場合

NetBackup 証明書の状態が有効か無効化済みかを確認できます。これは、接続と通信の問題のトラブルシューティングに役立つことがあります。証明書の状態を確認する方法には、次の 3 つの方法があります。

ホスト自体からホスト証明書を確認する	この方法では、NetBackup `nbcertcmd` コマンドを使用します。 p.329 の「ホストからホストの証明書の状態を確認するには」を参照してください。
NetBackup サーバーからホスト証明書を確認する	この方法では、NetBackup `bptestbpcd` コマンドを使用します。 p.329 の「別のホストの証明書が失効している場合に NetBackup サーバーから確認する方法」を参照してください。
NetBackup 管理コンソールからホスト証明書を確認する	p.330 の「ホストの証明書を確認するには」を参照してください。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

ホストからホストの証明書の状態を確認するには

1 必要に応じて、NetBackup ホストで最新の証明書失効リストを取得するため、管理者として次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -getCRL [-server primary_server_name]`

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -getCRL [-server primary_server_name]`

デフォルト以外の NetBackup ドメインから CRL を取得するには、`-server`*`primary_server_name`* オプションおよび引数を指定します。

2 NetBackup ホストで、管理者として次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster] [-server primary_server_name]`

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -hostSelfCheck [-cluster] [-server primary_server_name]`

必要に応じて、次のオプションのいずれかまたは両方を使用します。

`-cluster`	仮想ホストの証明書を確認するには、NetBackup プライマリサーバークラスタのアクティブノードでこのオプションを使用します。
`-server`	デフォルト以外のプライマリサーバーから証明書を確認するには、*primary_server_name* 引数を指定してこのオプションを使用します。

3 コマンドの出力を確認します。出力は、証明書が失効しているかいないかを示します。

別のホストの証明書が失効している場合に NetBackup サーバーから確認する方法

1 NetBackup プライマリサーバーまたは NetBackup メディアサーバーで管理者として次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

Windows の場合: `install_path¥NetBackup¥bin¥bptestbpcd -host hostname -verbose`

`-host hostname` には、証明書を確認するホストを指定します。

2 コマンドの出力を確認します。指定されたホストの証明書が失効している場合、コマンド出力には `The Peer Certificate is revoked` という文字列が含まれます。コマンド出力にこの文字列が含まれていない場合、証明書は有効です。

ホストの証明書を確認するには

1 左ペインで、[セキュリティ (Security)]の[証明書 (Certificates)]を選択します。

2 証明書名をクリックして、証明書の状態を確認します。

外部 CA が署名した証明書を使用する場合

外部 CA が署名したホスト証明書の状態が有効か無効化済みかを確認できます。これは、接続と通信の問題のトラブルシューティングに役立つことがあります。

証明書の状態を確認するには、次の 2 つの方法があります。

ホスト自体からホスト証明書を確認する	p.330 の「ホスト自体からホスト証明書を確認するには」を参照してください。
NetBackup サーバーからホスト証明書を確認する	p.331 の「別のホストの証明書が失効している場合に NetBackup サーバーから確認する方法」を参照してください。

ホスト自体からホスト証明書を確認するには

1 NetBackup CRL キャッシュ内の CRL を更新します。

2 NetBackup ホストで、管理者として次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster]`

Windows の場合: `install_path¥NetBackup¥bin¥nbcertcmd -hostSelfCheck [-cluster]`

仮想名の証明書を確認するには、クラスタプライマリサーバーのアクティブノードで `-cluster` オプションを使用します。

3 コマンドの出力を確認します。出力は、証明書が無効化されているかいないかを示します。

別のホストの証明書が失効している場合に NetBackup サーバーから確認する方法

1 NetBackup プライマリサーバーまたは NetBackup メディアサーバーで管理者として次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

Windows の場合: `install_path¥NetBackup¥bin¥bptestbpcd -host hostname -verbose`

`-host hostname` には、証明書を確認するホストを指定します。

2 コマンドの出力を確認します。指定されたホストの証明書が無効化されている場合、コマンド出力には The Peer Certificate is revoked という文字列が含まれます。コマンド出力にこの文字列が含まれていない場合、証明書は有効です。

証明書を無効化した NetBackup ホストのリストの取得

無効化された証明書を持つ NetBackup ホストのリストを取得するには、次の手順を使用します。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

無効化された証明書を持つ NetBackup ホストのリストを取得するには

1 コマンドウィンドウで、次のようにプライマリサーバーの NetBackup Web 管理サービスにログオンします (ログオンアカウントには NetBackup 管理者権限が必要です)。

UNIX の場合: `/usr/openv/netbackup/bin/bpnbat -login -loginType WEB`

Windows の場合: *`install_path`*`¥NetBackup¥bin¥bpnbat -login -loginType WEB`

2 次のコマンドを実行して、失効していない証明書のリストを CRL から抽出し、結果を「`Revoked`」という単語でフィルタリングします。

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -listAllDomainCertificates | grep Revoked`

Windows の場合: *`install_path`*`¥NetBackup¥bin¥nbcertcmd -listAllDomainCertificates | findstr Revoked`

ホスト ID ベースの証明書の削除

NetBackup ホストのホスト ID ベースの証明書を手動で削除するには、このトピックを使用します。NetBackup ドメインから別の NetBackup ドメインに NetBackup ホストが移動された場合などの、特定のシナリオで証明書を削除する必要があります。このシナリオで

は、現在のホスト ID ベースの証明書を削除する必要があり、ホストに新しいプライマリサーバーである新しい認証局 (CA) によって発行された証明書が必要です。

注意: ホスト ID ベースの証明書を手動で削除すると、NetBackup の機能に悪影響を与える可能性があります。

メモ: NetBackup ソフトウェアの削除中に、ホスト ID ベースの証明書が自動的に削除されます。

NetBackup ホストからホスト ID ベースの証明書を削除するには

1 関連付けられているすべてのホスト ID ベースの証明書の詳細を表示するには、NetBackup ホストで次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -listCertDetails`

Windows の場合: *install_path*¥NetBackup¥bin¥nbcertcmd -listCertDetails

2 証明書を削除するには、ホストで次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -deleteCertificate -hostid host_ID`

Windows の場合: *install_path*¥NetBackup¥bin¥nbcertcmd -deleteCertificate -hostid *host_ID*

クラスタ設定内のアクティブノードからホスト ID ベースの証明書を削除するには

1 関連付けられているすべてのホスト ID ベースの証明書の詳細を表示するには、アクティブノードで次のコマンドを実行します。

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -listCertDetails -cluster`

Windows の場合: *install_path*¥NetBackup¥bin¥nbcertcmd -listCertDetails -cluster

2 証明書を削除するには、クラスタのアクティブノードで次のコマンドを実行します。

`nbcertcmd -deleteCertificate -hostid host_ID -cluster`

UNIX の場合: `/usr/openv/netbackup/bin/nbcertcmd -hostid host_ID -cluster]`

Windows の場合: *install_path*¥NetBackup¥bin¥nbcertcmd -hostid *host_ID* -cluster

クラスタ化されたセットアップでのホスト ID ベースの証明書配備

この項では、クラスタ化された NetBackup セットアップへのホスト名ベースとホスト ID ベースの証明書の配備についての情報を示します。

NetBackup クラスタについて詳しくは、『NetBackup プライマリサーバーのクラスタ化管理者ガイド』を参照してください。

NetBackup クラスタでのホスト ID ベースの証明書の配備について

クラスタ化された NetBackup プライマリサーバーセットアップでは、ホスト ID ベースの証明書は次のように配備されます。

- 各クラスタノードに対して 1 つの証明書。
- 仮想名に対して 1 つの証明書。証明書はクラスタの共有ディスク上にあります。

たとえば、次の例を考えてみます。

クラスタのセットアップが 4 つのノードで構成される場合、5 つのホスト ID ベースの証明書が配備されます。4 つのノードと、プライマリサーバーの仮想名に使われる共有ディスクのそれぞれに 1 つの証明書が配備されます。

メモ: NetBackup では、プライマリサーバーのみをクラスタ化できます。

NetBackup クラスタでのホスト名ベースの証明書の配備について

クラスタ化された NetBackup プライマリサーバーセットアップでは、ホスト名ベースの証明書は次のように配備されます。

- 各クラスタノードに対して 1 つの証明書。証明書は各ノードのローカルディスク上にあります。
- 各ノードに対して仮想名の 1 つの証明書。証明書は各ノードのローカルディスク上にあります。

p.292 の「ホスト名ベースの証明書の配備」を参照してください。

クラスタ化された NetBackup ホストでのホスト ID ベースの証明書の配備について

クラスタノードでの証明書配備に関する次のシナリオを確認します。

- NetBackup の新規インストールの場合、アクティブノードに証明書が自動的に配備されます。すべての非アクティブノードでは、証明書を手動で配備する必要があります。
- ディザスタリカバリの場合は、アクティブノードの証明書も非アクティブノードの証明書もリカバリされません。災害後にディザスタリカバリモードで NetBackup をインストールした後、すべてのノードに証明書を手動で配備する必要があります。
  p.339 の「ディザスタリカバリインストール後のクラスタ化されたプライマリサーバーでの証明書の生成」を参照してください。

メモ: アップグレードの場合、アクティブノードと非アクティブノードにすでに証明書が配備されていることがあります。クラスタノードに証明書が配備されているかどうかを確認できます。

p.338 の「クラスタ化された NetBackup セットアップで証明書の詳細を表示する」を参照してください。

---

p.334 の「アクティブなプライマリサーバーノードでのホスト ID ベースの証明書の配備」を参照してください。

p.334 の「非アクティブなプライマリサーバーノードでのホスト ID ベースの証明書の配備」を参照してください。

アクティブなプライマリサーバーノードでのホスト ID ベースの証明書の配備

NetBackup のインストール時に、ホスト ID ベースの証明書がアクティブなプライマリサーバーノードとその仮想名に配備されます。アクティブノードの証明書はローカルディスクに配備されます。仮想名の証明書は共有ディスクに配備されます。

非アクティブなプライマリサーバーノードでのホスト ID ベースの証明書の配備

インストール時に、非アクティブノードに証明書は配備されません。インストール後に、すべての非アクティブノードに証明書を手動で配備する必要があります。

p.334 の「クラスタノードでのホスト ID ベースの証明書の配備」を参照してください。

クラスタノードでのホスト ID ベースの証明書の配備

すべての非アクティブノードでは、証明書を手動で配備する必要があります。

場合によっては、アクティブノードにもホスト ID ベースの証明書を手動で配備する必要があります。

プライマリサーバーのクラスタノードに、ホスト ID ベースの証明書を手動で配備する方法

- プライマリサーバーのクラスタノードで次のコマンドを実行します。
  - `nbcertcmd -getCACertificate`
  - `nbcertcmd -getCertificate [-file authorization_token_file]`

  p.317 の「ホスト ID ベースの証明書のトークン管理について」を参照してください。

クラスタ化された NetBackup セットアップでホスト ID ベースの証明書を無効化する

NetBackup 管理者は、さまざまな状況下でホスト ID ベースの証明書の無効化を検討します。たとえば、管理者が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。証明書が無効化されているホストは、他のホストと通信できません。各 NetBackup ホストは、正常に通信するために有効なセキュリティ証明書と有効な証明書失効リスト (CRL) が必要です。

p.322 の「ホスト ID ベースの証明書失効リストについて」を参照してください。

NetBackup 管理者は、NetBackup ドメインの任意のホストでクラスタノードまたは仮想名の証明書を無効化できます。

証明書を無効化するときは、それが適切な証明書であることを確認します。

証明書を無効化した後に、新しいホスト ID ベースの証明書の配備が必要な場合があります。クラスタノードで再発行トークンを作成し、再発行トークンを使用して新しい証明書を配備します。

p.336 の「クラスタ化された NetBackup セットアップの再発行トークンの作成」を参照してください。

p.336 の「再発行トークンを使用して、クラスタ化された NetBackup セットアップでホスト ID ベースの証明書を配備する」を参照してください。

クラスタノードで証明書を無効化するには

1. NetBackup Web 管理サービスにログインします。

   ```
   bpnbat -login -logintype WEB
   ```

   p.294 の「nbcertcmd コマンドオプションの Web ログインの要件」を参照してください。

2. 次のコマンドを実行して、クラスタノードの証明書を無効化します。

   ```
   nbcertcmd -revokeCertificate -host host_name
   ```

   p.326 の「ホスト ID ベースの証明書の無効化」を参照してください。

仮想名の証明書を無効化するには

1 NetBackup Web 管理サービスにログインします。

```
bpnbat -login -logintype WEB
```

2 次のコマンドを実行して、仮想名のホスト ID ベースの証明書を無効化します。

```
nbcertcmd -revokeCertificate -host virtual_name
```

p.326 の「ホスト ID ベースの証明書の無効化」を参照してください。

再発行トークンを使用して、クラスタ化された NetBackup セットアップでホスト ID ベースの証明書を配備する

ホスト ID ベースの証明書を無効化した後に、再発行トークンを使って、クラスタ化された NetBackup セットアップに新しいホスト ID ベースの証明書を配備できます。

p.336 の「クラスタ化された NetBackup セットアップの再発行トークンの作成」を参照してください。

クラスタノードに新しいホスト ID ベースの証明書を配備するには

- 次のコマンドを実行して、再発行トークンを使ってクラスタノードに新しいホスト ID ベースの証明書を配備します。

```
nbcertcmd -getCertificate -file reissue_token_file -force
```

仮想マシンの新しいホスト ID ベースの証明書を配備するには

- 次のコマンドを実行して、再発行トークンを使って仮想名の新しい証明書を配備します。

```
nbcertcmd -getCertificate -file reissue_token_file_virtual -force
-cluster
```

クラスタ化された NetBackup セットアップの再発行トークンの作成

場合によっては、ホストに証明書を再発行する必要があります。たとえば、ホストの証明書が無効化された場合に、ホストに新しい証明書を再発行する必要があります。

p.336 の「再発行トークンを使用して、クラスタ化された NetBackup セットアップでホスト ID ベースの証明書を配備する」を参照してください。

新しい証明書をホストに再発行するには、再発行トークンが必要です。

p.317 の「ホスト ID ベースの証明書のトークン管理について」を参照してください。

クラスタノードの再発行トークンを作成する方法

1 次のコマンドを実行して、NetBackup Web 管理サービスにログインします。

```
bpnbat -login -logintype WEB
```

p.294 の「nbcertcmd コマンドオプションの Web ログインの要件」を参照してください。

2 次のコマンドを実行して、必要なクラスタノードの再発行トークンを作成します。

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

p.314 の「再発行トークンの作成」を参照してください。

仮想名の再発行トークンを作成する方法

1 次のコマンドを実行して、NetBackup Web 管理サービスにログインします。

```
bpnbat -login -logintype WEB
```

p.294 の「nbcertcmd コマンドオプションの Web ログインの要件」を参照してください。

2 次のコマンドを実行して、仮想名の再発行トークンを作成します。

```
nbcertcmd -createToken -name token_name_virtual -reissue -host
virtual_name
```

p.314 の「再発行トークンの作成」を参照してください。

クラスタ化された NetBackup セットアップでホスト ID ベースの証明書を更新する

クラスタノードと仮想名のホスト ID ベースの証明書は自動的に更新されます。これらの証明書は期限切れの日の 180 日前に自動的に更新されます。

必要な場合は、証明書を手動で更新することもできます。

p.310 の「ホスト ID ベースの証明書の有効期限と更新について」を参照してください。

クラスタノードの証明書を手動で更新するには

◆ ノードの証明書の更新を行うクラスタノードから次のコマンドを実行します。

```
nbcertcmd -renewCertificate
```

仮想名の証明書を手動で更新するには

◆ 仮想名の証明書の手動更新を行うアクティブノードで次のコマンドを実行します。

```
nbcertcmd -renewCertificate -cluster
```

クラスタ化された NetBackup セットアップで証明書の詳細を表示する

クラスタノードまたは仮想名の証明書の詳細を表示するには、次のコマンドを実行します。

クラスタノードの証明書の詳細を表示するには

- クラスタノードで次のコマンドを実行します。

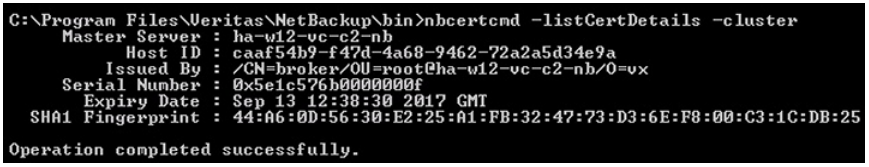
  ```
  nbcertcmd -listCertDetails
  ```

  p.297 の「ホスト ID ベースの証明書の詳細の表示」を参照してください。

仮想名の証明書の詳細を表示するには

- 仮想名の証明書の詳細を表示するアクティブノードで次のコマンドを実行します。

  ```
  nbcertcmd -listCertDetails -cluster
  ```



p.297 の「ホスト ID ベースの証明書の詳細の表示」を参照してください。

クラスタ化された NetBackup セットアップからの CA 証明書の削除

クラスタ化されたセットアップから CA (認証局) 証明書を削除するには、次のコマンドを実行します。

注意: プライマリサーバーノードから CA 証明書を削除すると、NetBackup の機能に悪影響を及ぼす場合があります。

クラスタノードから CA 証明書を削除するには

1. クラスタノードで次のコマンドを実行して、CA 証明書の指紋を表示します。

   ```
   nbcertcmd -listCACertDetails
   ```

2. 次のコマンドを実行し、適切な指紋を指定して CA 証明書を削除します。

   ```
   nbcertcmd -removeCACertificate -fingerprint fingerprint
   ```

仮想名の CA 証明書を削除するには

1. アクティブノードで次のコマンドを実行して、仮想名の CA 証明書の指紋を表示します。

   ```
   nbcertcmd -listCACertDetails -cluster
   ```

2. アクティブノードで次のコマンドを実行して、適切な指紋を指定して仮想名の CA 証明書を削除します。nbcertcmd -removeCACertificate -fingerprint *fingerprint_virtual* -cluster

ディザスタリカバリインストール後のクラスタ化されたプライマリサーバーでの証明書の生成

クラスタ化されたプライマリサーバーのディザスタリカバリが完了した後は、アクティブノードとすべての非アクティブノードで証明書を生成する必要があります。この手順は、クラスタのバックアップとリストアを成功させるために必須です。

ディザスタリカバリの後に各クラスタノードでローカル証明書を生成するインストール

1. すべての非アクティブノードをクラスタに追加します。

   クラスタのすべてのノードが現在クラスタの一部ではない場合、最初にこれらをクラスタに追加します。このプロセスについて詳しくは、オペレーティングシステムのクラスタの手順を参照してください。

   サポート対象のクラスタ技術に関する詳細情報を参照できます。『NetBackup プライマリサーバーのクラスタ化管理者ガイド』を参照してください。

2. nbcertcmd コマンドを実行し、認証局の証明書を格納します。

   UNIX の場合: /usr/openv/netbackup/bin/nbcertcmd -getCACertificate

   Windows の場合: *install_path*¥Veritas¥NetBackup¥bin¥nbcertcmd -getCACertificate

3. 以下に示す bpnbat コマンドを使用し、必要な変更を許可します。認証ブローカーを求めるメッセージが表示されたら、ローカルノード名ではなく仮想サーバー名を入力します。

   ```
   bpnbat -login -loginType WEB
   ```

4 nbcertcmd コマンドを使用して再発行トークンを作成します。*hostname* は、ローカルノード名です。コマンドを実行すると、トークン文字列値が表示されます。各クラスタノードには一意の再発行トークンが必要です。

```
nbcertcmd -createtoken -name token_name -reissue -host hostname
```

5 nbcertcmd コマンドとともに再発行トークンを使用して、ホスト証明書を格納します。このコマンドでは、トークン文字列値が求められます。nbcertcmd -createToken コマンドから入手したトークン文字列値を入力します。

```
nbcertcmd -getCertificate -token
```

詳細情報を参照できます。『Veritas NetBackup セキュリティおよび暗号化ガイド』で、プライマリサーバーノードでの証明書の配備に関するセクションを参照してください。

p.291 の「ディザスタリカバリパッケージ」を参照してください。

非武装地帯にある NetBackup クライアントとプライマリサーバーの間の HTTP トンネルを介した通信について

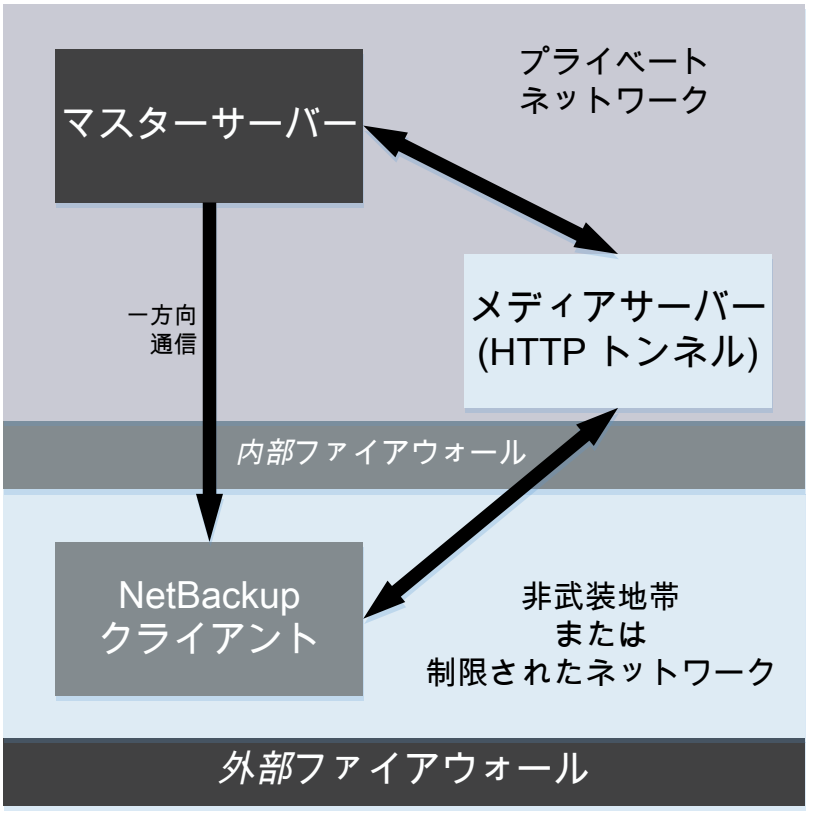
NetBackup の配備設定では、特定の Web ポートのみを介して通信が行われる非武装地帯 (DMZ) にクライアントコンピュータを置くことができます。

すべての NetBackup クライアントは、セキュリティ証明書を配備し、ピアを認証して接続を保護するために、プライマリサーバーの Web 管理サービスと通信できる必要があります。たとえば、NetBackup クライアントは、プライマリサーバーに証明書を配備するために要求を送信します。これは、NetBackup の安全な通信のために不可欠です。DMZ 設定では、クライアントは Web サービス要求をプライマリサーバーに直接送信できない場合があります。この場合、NetBackup クライアントは HTTP CONNECT プロキシ方式によって、メディアサーバー上の HTTP トンネルに接続要求と Web サービス要求を送信します。HTTP トンネルは接続要求を受け入れ、Web サービス要求をプライマリサーバーに転送します。

HTTP トンネリング機能により、DMZ の NetBackup クライアントが Web サービス要求をプライマリサーバーに送信できます。NetBackup メディアサーバーは、Web サービス要求を NetBackup クライアントからプライマリサーバーに転送する HTTP トンネルを形成します。また、Web サービス通信では SSL (Secure Socket Layer) が使用されます。

メモ: メディアサーバーのポート番号 1556 は、Web サービス要求を送信するために NetBackup クライアントからアクセスできる必要があります。

図 17-2 DMZ 設定での NetBackup クライアントとプライマリサーバーの通信



単一ドメインまたはマルチドメイン環境で、DMZ の NetBackup クライアントがプライマリサーバーへの Web サービス接続要求の送信を試みるときは、次の特定の順序に従います。

表 17-8 接続要求を送信するための順序

順序	説明
1. NetBackup クライアントが、プライマリサーバーへの接続要求の直接送信を試みます。	DMZ では、Web サービス接続要求が成功しない可能性があります。
2. 直接接続に失敗すると、クライアントは HTTP トンネリングを使用して Web サービス接続要求をプライマリサーバーに送信するようにメディアサーバーが指定されているかどうかを確認します。	

順序	説明
3. メディアサーバーが指定されていない場合、クライアントは NetBackup 構成で利用可能なメディアサーバーのリストを参照し、それらを使用して Web サービス接続要求を送信します。	NetBackup クライアントは、以前に成功した接続に基づいて自動的に更新されるメディアサーバーのリストを含む、内部キャッシュファイル (websvctunnels.cache) を保持します。このキャッシュファイルは、Windows と UNIX の両方で bp.conf ファイルと同じ場所にあります。

追加情報

- HTTP トンネル機能の構成のために、次の追加オプションを使用できます。
  - WEB_SERVER_TUNNEL_USE: このオプションを NetBackup クライアントで使用することで、HTTP トンネルを使用してデフォルトの通信の動作を構成できます。
  - WEB_SERVER_TUNNEL_ENABLE: デフォルトでは、HTTP トンネルはメディアサーバーで有効になっています。このオプションをメディアサーバーで使用して、HTTP トンネル機能を無効にすることができます。

  詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。
- NetBackup クライアント構成にドメイン内のメディアサーバーに関する情報が含まれていない場合は、プライマリサーバーで nbsetconfig コマンドを実行します。Windows クライアント上のレジストリまたは UNIX クライアント上の bp.conf ファイルには、クライアントが接続要求および Web サービス要求を送信するために選択したプライマリサーバーおよびメディアサーバーが含まれています。
- DMZ の NetBackup クライアントで nbcertcmd -getCertificate コマンドを使用すると、次のいずれかのエラーが表示される場合があります。
  - 終了状態 5955: ホスト名がプライマリサーバーに認識されていません。(EXIT STATUS 5955: The host name is not known to the primary server.)
  - 終了状態 5954: ホスト名を要求しているホストの IP アドレスに解決できませんでした。(EXIT STATUS 5954: The host name could not be resolved to the requesting host's IP address.)

  プライマリサーバーは、HTTP トンネルの IP アドレスと証明書を要求するホストの ID を照合できないため、トークンを使用してセキュリティ証明書を配備します。
- HTTP トンネルを使用して証明書要求をプライマリサーバーに送信する場合、NetBackup 監査レポートはメディアサーバーをユーザーとして一覧に表示します。

NetBackup ホストの手動での追加

特定のシナリオを除き、ホストデータベースにホストを手動で追加することはお勧めしません。たとえば、自動イメージレプリケーション (AIR) を使用して、BMR (Bare Metal Restore)

クライアントを他の NetBackupドメインにリカバリする場合は、ホストを手動で追加する必要があります。

Bare Metal Restore について詳しくは、『NetBackup Bare Metal Restore 管理者ガイド』を参照してください。

メモ: ホストを追加する前に、追加するホストエントリがホストデータベースにまだ存在していないことを確認する必要があります。

ホストの追加は、コマンドラインインターフェースを使用することによってのみ実行できます。

コマンドラインインターフェースを使用してホストデータベースのホストを追加する方法

1. 次のコマンドを実行して、プライマリサーバーで、Web サービスのログインを認証します。

   ```
   bpnbat -login -loginType WEB
   ```

2. 次のコマンドを実行して、ホストをリセットします。

   ```
   nbhostmgmt -addhost -host host name -server primary server
   ```

NetBackup CA の移行

特定のシナリオでは、既存の NetBackup 認証局 (CA) の階層を新しいものに移行することが必要になる場合があります。NetBackup は既存の NetBackup CA の移行をサポートします。この章では、NetBackup CA の移行プロセスについて説明します。

NetBackup ホストの認証に使用される NetBackup セキュリティ証明書は、X.509 公開鍵基盤 (PKI) 標準に適合しています。NetBackup プライマリサーバーは、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 は、NetBackup 認証デーモン (NBATD) を PKI プロバイダとして使用します。NBATD とそのクライアント実装は、認証に使用される RSA 秘密鍵を生成します。

NetBackup は、キー強度が 2048 ビット、3072 ビット、4096 ビット、8192 ビット、および 16384 ビットの認証局をサポートするようになりました。

メモ: NetBackup プライマリサーバーをインストールまたはアップグレードした後、デフォルトでは、キー強度が 2048 ビットの新しい root CA が配備されます。アップグレードした場合は、既存の CA を新しい CA に移行する必要があります。

表 17-9　さまざまな使用例での NetBackup CA の移行手順

使用例	説明
デフォルト (2048 ビット) 以外のキー強度の NetBackup CA が必要な場合	p.345 の「NB_KEYSIZE 環境変数を使用してインストールまたはアップグレードする前に、必要なキーの強度を設定する」を参照してください。 p.347 の「インストールまたはアップグレード後に NetBackup CA を手動で移行する」を参照してください。
NetBackup ドメイン全体を 8.3 にアップグレードした後で既存の NetBackup CA を移行する場合	p.345 の「NetBackup ドメイン全体をアップグレードするときに NetBackup CA を移行する」を参照してください。

NetBackup CA の移行プロセスは次のフェーズで構成されます。

1. NetBackup CA の移行を開始する

   メモ: 次のコマンドを実行します。

   ```
   vssat setuptrust --broker nb_master_server_name:1556:nbatd
   --securitylevel high
   ```

   これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

   vssat コマンドは次の場所に存在します。

Windows	*INSTALL_PATH*¥NetBackup¥sec¥at¥bin¥vssat
UNIX	/usr/openv/netbackup/sec/at/bin

2. 新しい NetBackup CA をアクティブ化する
3. NetBackup CA の移行を完了する
4. 古い NetBackup CA を廃止する

   メモ: 古い NetBackup CA の廃止は省略可能なクリーンアップタスクです。

詳しくは、NetBackup CA の移行に関するビデオを参照してください。

NB_KEYSIZE 環境変数を使用してインストールまたはアップグレードする前に、必要なキーの強度を設定する

NetBackup をインストールまたはアップグレードした後、デフォルトでは、キー強度が 2048 ビットの新しいルート CA が配備されます。キー強度を大きくする場合は、インストールまたはアップグレードの前に、2048 ビットより大きい値を環境変数に設定します。

2048 ビットを超えるキー強度の NetBackup CA にするには

1 NetBackup のインストールまたはアップグレードを開始する前に、プライマリサーバーの NB_KEYSIZE 環境変数を設定します。

例: NB_KEYSIZE = 4096

NB_KEYSIZE 環境変数に指定できる値は、2048、3072、4096、8192、16384 です。

メモ: プライマリサーバーで FIPS モードが有効になっている場合は、NB_KEYSIZE 環境変数の値として指定できるのは 2048 ビットと 3072 ビットのみです。

注意: 使用環境のキーサイズは慎重に選択する必要があります。大きいキーサイズを選択すると、パフォーマンスが低下する場合があります。キーサイズ 2048 は、ほとんどのユースケースにおいてセキュリティを提供します。

---

2 ホストで NetBackup をインストールまたはアップグレードします。

アップグレードの場合は、CA の移行を続行します。

p.345 の「NetBackup ドメイン全体をアップグレードするときに NetBackup CA を移行する」を参照してください。

NetBackup ドメイン全体をアップグレードするときに NetBackup CA を移行する

NetBackup 8.3 にアップグレードすると、デフォルトでは、キー強度が 2048 ビットの新しいルート CA が配備され、CA 移行プロセスが自動的に開始されます。また、インストールまたはアップグレードの前に、NB_KEYSIZE 環境変数に 2048 ビットより大きい値を設定することもできます。

p.345 の「NB_KEYSIZE 環境変数を使用してインストールまたはアップグレードする前に、必要なキーの強度を設定する」を参照してください。

メモ: クラウドストレージサーバーとして構成されている、NetBackup 8.2 より前のメディアサーバーの場合、CA 移行プロセスは開始されません。ホストと正常に通信するため、すべての NetBackup ホストが 8.3 以降にアップグレードされていることを確認してください。

NetBackup ドメインのすべてのホストが NetBackup 8.3 以降にアップグレードされたら、次の手順を使用して CA 移行プロセスを完了します。

すべてのホストが NetBackup 8.3 にアップグレードされた場合に NetBackup CA を移行するには

1. 次のコマンドを実行して、すべてのホストのトラストストアに新しい CA 証明書があることを確認します。

   ```
   nbseccmd -nbcaMigrate -hostsPendingTrustPropagation
   ```

2. コマンドから出力としてゼロ (0) ホストが返されることを確認します。

   これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

3. **警告:** 1 つ以上の NetBackup ホストが 8.2 以前のバージョンである場合、そのようなホストのバックアップはアクティブ化後に失敗します。したがって、新しい CA をアクティブ化する前に、ドメイン内のすべての NetBackup ホストが 8.3 にアップグレードされていることを確認する必要があります。

   次のコマンドを実行して、NetBackup 証明書の再発行を開始する新しい CA をアクティブ化します。

   ```
   nbseccmd -nbcaMigrate -activateNewCA
   ```

4. 次のコマンドを実行して、新しい CA が更新した証明書がすべてのホストにあることを確認します。

   ```
   nbseccmd -nbcaMigrate -hostsPendingRenewal
   ```

   コマンドから出力としてゼロ (0) ホストが返されることを確認します。

5. このホストで NetBackup Messaging Broker (nbmqbroker) サービスを再起動します。

6. CA 移行プロセスを完了するには、次のコマンドを実行します。

   ```
   nbseccmd -nbcaMigrate -completeMigration
   ```

7. NetBackup CA の移行プロセスが完了し、新しい CA が発行した証明書がホストで使用されていることを確認したら、古い NetBackup CA を安全に廃止できます。

   このクリーンアップタスクは省略可能です。

   p.349 の「非アクティブな NetBackup CA を廃止する 」を参照してください。

インストールまたはアップグレード後に NetBackup CA を手動で移行する

NetBackup の新規インストールまたはアップグレードでは、デフォルトで、キー強度が 2048 ビットの新しいルート CA が配備されます。ただし、他のキーサイズの CA を使用する場合や、インストールまたはアップグレード後に新しい CA に移動する場合は、手動で CA 移行プロセスを開始する必要があります。

p.345 の「NB_KEYSIZE 環境変数を使用してインストールまたはアップグレードする前に、必要なキーの強度を設定する」を参照してください。

インストールまたはアップグレード後に NetBackup CA を移行するには

1. CA 移行プロセスを開始するには、次のコマンドを実行します。

   ```
   nbseccmd -nbcaMigrate -initiateMigration -keysize key_value
   ```

   このコマンドにより、新しい NetBackup CA が配備されます。

   これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

2. 次のコマンドを実行して、ホストに証明書を再発行します。

   ```
   nbcertcmd -reissueCertificates
   ```

3. NetBackup Web サーバーに証明書を再発行する前に、NetBackup Web 管理コンソール (nbwmc) サービスを停止します。

4. 次のコマンドを実行して、NetBackup Web サーバーに証明書を再発行します。

   ```
   configureCerts -renew_webserver_keys
   ```

5. nbwmc サービスを起動します。

6. 次のコマンドを実行して、すべてのホストのトラストストアに新しい CA 証明書があることを確認します。

   ```
   nbseccmd -nbcaMigrate -hostsPendingTrustPropagation
   ```

7. コマンドから出力としてゼロ (0) ホストが返されることを確認します。

8. **警告:** 1 つ以上の NetBackup ホストが 8.2 以前のバージョンである場合、そのようなホストのバックアップはアクティブ化後に失敗します。したがって、新しい CA をアクティブ化する前に、ドメイン内のすべての NetBackup ホストが 8.3 にアップグレードされていることを確認する必要があります。

   次のコマンドを実行して、NetBackup 証明書の再発行を開始する新しい CA をアクティブ化します。

   ```
   nbseccmd -nbcaMigrate -activateNewCA
   ```

9 次のコマンドを実行して、新しい CA でホスト証明書を再発行します。

```
nbcertcmd -renewCertificate
```

10 次のコマンドを実行して、新しい CA が更新した証明書がすべてのホストにあることを確認します。

```
nbseccmd -nbcaMigrate -hostsPendingRenewal
```

コマンドから出力としてゼロ (0) ホストが返されることを確認します。

11 このホストで NetBackup Messaging Broker (nbmqbroker) サービスを再起動します。

12 CA 移行プロセスを完了するには、次のコマンドを実行します。

```
nbseccmd -nbcaMigrate -completeMigration
```

13 NetBackup CA の移行プロセスが完了し、新しい CA が発行した証明書がホストで使用されていることを確認したら、古い NetBackup CA を安全に廃止できます。

このクリーンアップタスクは省略可能です。

p.349 の「非アクティブな NetBackup CA を廃止する」を参照してください。

CA の移行後の新しい CA 証明書が存在しないクライアントとの通信の確立

ネットワーク上の問題など、特定のシナリオでは、NetBackup クライアントは NetBackup CA の移行中に到達できない場合があります。このようなクライアントには新しい CA 証明書がない可能性があり、そのようなクライアントとの通信が失敗することがあります。

CA の移行中にアクセスできなかった NetBackup クライアントと正常に通信するには

1 クライアントで次のコマンドを実行して、証明書を取得します。

```
nbcertcmd -getcacertificate -server master_server_name
```

2 クライアントで次のコマンドを実行して、証明書を更新します。

```
nbcertcmd -renewcertificate -server master_server_name
```

これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

ドメイン内の NetBackup CA のリストの表示

NetBackup ドメインで利用可能な NetBackup CA のリストを表示できます。

ドメイン内の NetBackup CA のリストを表示するには

◆ 次のコマンドを実行します。

```
nbseccmd -nbcaList
```

これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

特定の状態 (廃止、アクティブ、破棄など) の CA を表示する場合は、次のコマンドを実行します。

```
nbseccmd -nbcaList -state CA_state]
```

CA 移行の概略の確認

NetBackup CA 移行の概略は、さまざまな段階で確認できます。CA 移行の概略には、現在の CA 移行の状態や、証明書を発行している NetBackup CA の指紋などの情報が含まれます。

CA 移行の概略を確認するには

- 次のコマンドを実行します。

  ```
  nbseccmd -nbcaMigrate -summary
  ```

  これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

非アクティブな NetBackup CA を廃止する

NetBackup CA の移行プロセスが完了し、新しい CA が発行した証明書がホストで使用されていることを確認したら、古い NetBackup CA を安全に廃止できます。

古い NetBackup CA を廃止するには

1. 次のコマンドを実行します。

   ```
   nbseccmd -nbcaMigrate -decommissionCA -fingerprint
   certificate_fingerprint
   ```

   これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

2. NetBackup ドメインで NetBackup アクセス制御 (NBAC) が有効になっている場合、この手順は必須です。

   プライマリサーバーで NetBackup サービスを再起動します。

18

移動中のデータの暗号化 (DTE) の構成

この章では以下の項目について説明しています。

データチャネルについて

データ通信は、NetBackup を使用してバックアップされるデータで構成されます。セキュリティポリシーは、バックアップ管理者に対して、NetBackup クライアントがメタデータとデータを NetBackup サーバーに送信するチャネルが安全であることを保証することを要求します。NetBackup 10.0 以降では、データとメタデータは回線を介して暗号化されます。この機能は、データチャネルの暗号化または移動中のデータの暗号化 (DTE) と呼ばれます。

次のチャネルはデータチャネルとして分類されます。

- tar ストリーム (クライアントからメディアサーバー): このチャネルを介して、クライアントとメディアサーバー間で tar またはデータストリームが送信されます。バックアップ操作の間に、メディアサーバーはクライアントからデータを受信し、ストレージに送信します (OST プラグインなど)。リストア時には方向が逆になります。
- tar ストリーム (メディアサーバーからメディアサーバー): このチャネルは複製中に使用されます。
- カタログ情報 (クライアントからメディアサーバー): このチャネルを介して、クライアントとメディアサーバー間でカタログ情報と制御コマンドが送信されます。このチャネルを介して送信されるデータの量は、バックアップを構成するファイルとディレクトリの数に比例します。メディアサーバーは、クライアントが送信したカタログ情報をプライマリサーバーに送信します。
- カタログ情報 (メディアサーバーからプライマリサーバー): このチャネルを介して、メディアサーバーからプライマリサーバーにカタログ情報が送信されます。

メモ: NetBackup 10.3 の新規インストールの場合、移動中のデータの暗号化はデフォルトで[優先オン (Preferred On)]に設定されます。アップグレードの場合、以前の設定は保持されます。

移動中のデータの暗号化は、グローバルレベル (プライマリサーバーレベル) やクライアントレベルなどのさまざまなレベルで構成できます。

移動中のデータの暗号化のサポート

移動中のデータの暗号化は、次の NetBackup データとメタデータの操作でサポートされます。

- クライアントからメディアサーバーへのデータフロー
- メディアサーバーからクライアントへのデータフロー
- メディアサーバーからプライマリサーバーへのメタデータ転送
- 複製および合成バックアップ中のメディアサーバー間のデータフロー

移動中のデータの暗号化は、次の NetBackup の操作または通信ではサポートされません。

- OST プラグインと基盤となるストレージプロバイダ間の通信はサポートされません。次が含まれます。
  - NetBackup とクラウドストレージ間の通信
  - NetBackup とサードパーティの OST プロバイダ (DataDomain、NetApp など) 間の通信

- 移動中のデータの暗号化は、次の MSDP ワークフローではサポートされません。
  - 最適化された複製
  - AIR レプリケーション

  これら 2 つの操作では、両方のストレージサーバーで次のオプションを明示的に構成する必要があります。

  `OPTDUP_ENCRYPTION=1`

  NetBackup の DTE 構成は、2 台のストレージサーバー間のデータチャネルは制御しません。
- NetBackup と作業負荷アプリケーション (VMware、Hyper-V、Microsoft Exchange、Sharepoint、Nutanix など) 間の通信はサポートされません。
  作業負荷アプリケーションから NetBackup にデータが転送される際、NetBackup プロセスは TLS チャネルを介してそのデータを安全に転送します。
- NDMP 通信
- SAN クライアント通信
- NBFSD プロセスとの通信
  このプロセスでは、標準 NFS または CIFS プロトコルが使用されます。

移動中のデータの暗号化の構成ワークフロー

このトピックでは、NetBackup 環境内で移動中のデータの暗号化 (DTE) を実行する手順について説明します。DTE 構成は、次の 2 つの主なオプションで構成されています。

- グローバル DTE モード
- クライアント DTE モード

表 18-1 DTE 構成のワークフロー

手順の番号	手順	参照トピック
手順 1	グローバル DTE モードオプションの構成設定を確認し、DTE 要件に従ってオプションを構成する	p.353 の「移動中のデータの暗号化のグローバル設定を行う」を参照してください。
手順 2	クライアント DTE モードオプションの構成設定を確認し、DTE 要件に従ってオプションを構成する	p.354 の「クライアントの DTE モードの構成」を参照してください。

手順の番号	手順	参照トピック
手順 3	実行する NetBackup 操作と DTE の構成設定に基づいて、データの暗号化に関する決定がどのように行われるかを確認する	p.362 の「さまざまな NetBackup 操作での DTE 構成設定の動作」を参照してください。 **メモ:** 既存の DTE 構成設定の変更を計画している場合は、このトピックを確認して、NetBackup 操作にどのような影響があるかを理解する必要があります。

特定のシナリオでは、主要な DTE 構成設定とは別に次の設定が使用されます。

- メディアサーバー DTE モード
  p.358 の「メディアサーバーでの DTE モードの構成」を参照してください。
- バックアップイメージの DTE モード
  p.359 の「バックアップイメージでの DTE モードの変更」を参照してください。
  p.359 の「NetBackup サーバーの DTE_IGNORE_IMAGE_MODE」を参照してください。

移動中のデータの暗号化のグローバル設定を行う

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

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

グローバル DTE モードでサポートされる値は次のとおりです。

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

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

p.355 の「クライアントの DTE_CLIENT_MODE」を参照してください。

グローバル DTE 構成に使用する RESTful API:

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

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

1. NetBackup Web UI にサインインします。
2. 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。
3. [安全な通信 (Secure Communication)]タブで、次のグローバル DTE 設定のいずれかを選択します。
   - `Preferred Off`
   - `Preferred On`
   - `Enforced`

コマンドラインインターフェースを使用してグローバル DTE モードを設定および表示するには

1. 次のコマンドを実行して、グローバル DTE モードを設定します。

   ```
   nbseccmd -setsecurityconfig -dteglobalmode 0|1|2
   ```

   ここで、値 `0` は `Preferred Off` を表し、`1` は `Preferred On` を表し、`2` は `Enforced` を表します。
2. 次のコマンドを使用して、グローバル DTE モードに設定された値を確認します。

   ```
   nbseccmd -getsecurityconfig -dteglobalmode
   ```

クライアントの DTE モードの構成

`DTE_CLIENT_MODE` 構成オプションは、NetBackup クライアントに設定される移動中のデータの暗号化 (DTE) モードを指定します。

p.355 の「クライアントの DTE_CLIENT_MODE」を参照してください。

次のコマンドを使用して、クライアントの DTE モードを更新および表示できます。

`bpsetconfig`/`nbsetconfig` および `bpgetconfig`/`nbgetconfig`

クライアントの DTE_CLIENT_MODE

DTE_CLIENT_MODE オプションでは、NetBackup クライアントで設定されている移動中のデータの暗号化 (DTE) モードを指定します。

表 18-2 DTE_CLIENT_MODE の情報

使用方法	説明
使用する場所	NetBackup クライアント側。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 DTE_CLIENT_MODE = AUTOMATIC | ON | OFF デフォルトでは、9.1 クライアントの DTE モードは OFF に設定され、10.0 以降のクライアントでは AUTOMATIC に設定されます。 ■ この DTE_CLIENT_MODE オプションが AUTOMATIC に設定されている場合、クライアントはグローバルレベルで設定されている DTE モード (Enforced、Preferred On、または Preferred Off) に従います。 ■ このオプションが ON に設定されている場合、移動中のデータの暗号化はクライアントで有効になります。 ■ このオプションが OFF に設定されている場合、移動中のデータの暗号化はクライアントで無効になります。グローバル DTE モードが Preferred On に設定されている場合、この設定を使用してクライアントを暗号化から除外できます。 **メモ:** グローバル DTE モードが Enforced に設定されている場合、DTE_CLIENT_MODE オプションが「Off」に設定されている NetBackup クライアントと 9.1 より前のホストに対するジョブは失敗します。
同等の NetBackup Web UI プロパティ	相当するエントリは存在しません。 グローバル設定は、[設定 (Settings)]>[グローバルセキュリティ (Global security)]>[安全な通信 (Secure communication)]>[移動中のデータの暗号化 (Data-in-transit encryption)]で構成されます。

NetBackup ジョブの DTE モードの表示

グローバル DTE モードとクライアント DTE モードは主に、移動中のデータの暗号化が NetBackup 操作で行われるかどうかを決定します。NetBackup ジョブの実行時にデータが暗号化される場合、ジョブの「DTE モード」属性は On に設定されます。

NetBackup ジョブの実行時にデータが暗号化されない場合、ジョブの「DTE モード」属性は Off に設定されます。

ジョブの DTE モードを表示するための RESTful API:

- GET - /admin/jobs
- GET - /admin/jobs/{jobId}

NetBackup Web UI を使用して DTE モードを確認するには

1. NetBackup Web UI にサインインします。
2. 左側で、[アクティビティモニター (Activity Monitor)]、[ジョブ (Jobs)]の順に選択します。

   ジョブの DTE モードを決める Data-in-transit encryption 列を確認します。

コマンドラインインターフェースを使用して DTE モードを確認するには

◆ 次のコマンドを実行します。

```
bpdbjobs -dtemode Off|On
```

このコマンドは、設定されている DTE モードに基づいてジョブを一覧表示します。

NetBackup のイメージとイメージコピーに関する DTE 固有の属性の表示

グローバル DTE モードとクライアント DTE モードは主に、移動中のデータの暗号化がバックアップ操作で行われるかどうかを決定します。データがバックアップ操作中に暗号化される場合、関連付けられた NetBackup イメージの DTE モード属性は On に設定されます。

グローバル DTE モードとクライアント DTE モードに基づき、データがバックアップ中に暗号化できない場合、イメージの DTE モード属性は Off に設定されます。

p.359 の「バックアップイメージでの DTE モードの変更」を参照してください。

イメージコピーには、2 つの DTE 固有の属性があります。

コピー DTE モード	現在のイメージコピーの作成時に、セキュアなチャネルを介してデータを転送するかどうかを指定します。

コピー階層 DTE モード	現在のイメージコピーと、階層内にあるすべての親コピーの作成時に、セキュアなチャネルを介してデータを転送するかどうかを指定します。 階層内にある親コピーのいずれかが作成されたときに、データが安全でないチャネルを介して転送されると、現在のコピーの階層 DTE モードは Off に設定されます。 コピー階層 DTE モードが Off の場合、コピーは安全でないと見なされます。これは、階層内の親コピーの安全が侵害される可能性があること、および現在のコピーが安全に生成されても、侵害されたコピーからのコピーは安全でないことを示します。

メモ: データ転送に関与するメディアサーバーが 9.1 より前のバージョンの場合、イメージ DTE モードは常に Off と表示されます。データ転送に関与するメディアサーバーが 10.0 より前のバージョンの場合、コピー DTE モードとコピー階層 DTE モードは常に Off と表示されます。

イメージ属性を表示するために使用する RESTful API:

- GET - /catalog/images
- GET - /catalog/images/{backupId}

NetBackup Web UI を使用してイメージとイメージコピーの DTE 属性を表示するには

1. NetBackup Web UI にサインインします。
2. 左側で[カタログ (Catalog)]を選択します。

   バックアップイメージを検索すると、イメージのリストが画面の下部に表示されます。イメージとイメージコピーに関する DTE 固有の属性 (イメージ DTE モード、コピー DTE モード、コピー階層 DTE モード) も表示されます。

コマンドラインインターフェースを使用してイメージとイメージコピーの DTE 属性を表示するには

◆ コマンド bpimagelist、bpclimagelist、および bpimmedia を使用します。

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。

NetBackup 管理コンソールを使用してイメージの DTE 属性を表示するには

◆ NetBackup 管理コンソールで、次のレポートを参照して、イメージの DTE モード (移動中のデータの暗号化の列) を確認します。

- [NetBackup の管理 (NetBackup Management)]>[レポート (Reports)]>[メディア上のイメージ (Images on Media)]

- ［NetBackup の管理 (NetBackup Management)］>［レポート (Reports)］>［テープのレポート (Tape Reports)］>［テープ上のイメージ (Images on Tape)］
- ［NetBackup の管理 (NetBackup Management)］>［レポート (Reports)］>［ディスクのレポート (Disk Reports)］>［ディスク上のイメージ (Images on Disk)］

メディアサーバーでの DTE モードの構成

メディアサーバーの設定は、NetBackup 操作のために移動中のデータの暗号化 (DTE) をオフにする場合にのみ使用できます。

古いハードウェアが原因でメディアサーバーの速度が遅い NetBackup 構成の場合、メディアサーバー DTE モードをオフにすることでパフォーマンスの問題を回避できます。ただし、推奨されるのは、古いメディアサーバーハードウェアをアップグレードすることです。この設定は NetBackup 10.0 以降のメディアサーバーで利用可能です。

グローバル DTE 構成に使用する RESTful API:

- GET - /config/media-servers/{hostName}
- PATCH - /config/media-servers/{hostName}

メディアサーバー DTE モードを設定または表示するには

1 メディアサーバーリソースに対し、次の権限を持つ RBAC の役割があることを確認します。

- 表示
- 更新
- アクセスの管理

p.134 の「 デフォルトの RBAC の役割」を参照してください。

2 次のコマンドを実行して、メディアサーバー DTE モードを設定します。

```
nbseccmd -setsecurityconfig -dtemediamode off|on -mediaserver
media_server_name
```

3 次のコマンドを実行して、メディアサーバー DTE モードを表示します。

```
nbseccmd -getsecurityconfig -dtemediamode -mediaserver
media_server_name
```

メモ: On 9.1 メディアサーバーの場合、DTE モードの表示のみ可能で、設定はできません。

バックアップイメージでの DTE モードの変更

NetBackup の移動中のデータの暗号化 (DTE) 機能では、バックアップイメージ作成時に使用する追加のイメージ属性 (DTE モード) が導入されています。

グローバル DTE モードとクライアント DTE モードは主に、移動中のデータの暗号化が NetBackup 操作で行われるかどうかを決定します。データがバックアップ中に暗号化される場合、関連付けられた NetBackup イメージの DTE モード属性は `On` に設定されます。

グローバル DTE モードとクライアント DTE モードに基づく場合、データはバックアップ中には暗号化できず、イメージの DTE モード属性は `Off` に設定されます。

イメージに対する以降のすべての操作では、イメージ DTE モードが優先および維持されるはずです。たとえば、リストア操作や二次的操作 (複製、レプリケーション、インポートなど) などです。イメージ DTE モードがオンに設定されている場合、以降の操作では、DTE をサポートするホストのデータは常に暗号化されます。

ホストが DTE をサポートしていない場合、ジョブは失敗します。イメージ DTE モードがオフに設定されている場合、以降の操作での DTE は、その時点でのグローバル DTE モードとクライアント DTE モードに基づいて決定されます。これはデフォルトの動作です。

場合によっては、作成時に設定されたイメージ DTE モードを変更することもできます。

イメージ DTE モードの変更に使用する RESTful API:

- PATCH - /catalog/images/{backupId}

イメージ DTE モードを変更するには

◆ 次のコマンドを実行します。

```
bpimage -update -image_dtemode Off|On
```

NetBackup Web UI の[カタログ (Catalog)]ノードを使用してイメージ DTE モードを変更することもできます。

p.359 の「NetBackup サーバーの DTE_IGNORE_IMAGE_MODE」を参照してください。

p.356 の「NetBackup のイメージとイメージコピーに関する DTE 固有の属性の表示」を参照してください。

NetBackup サーバーの DTE_IGNORE_IMAGE_MODE

バックアップイメージの移動中のデータの暗号化 (DTE) モードが有効になっていても、データを暗号化しない場合は、`DTE_IGNORE_IMAGE_MODE` オプションを使用します。

`DTE_IGNORE_IMAGE_MODE` オプションはすべてのバックアップイメージに適用されます。

表 18-3 DTE_IGNORE_IMAGE_MODE の情報

使用方法	説明
使用する場所	NetBackup サーバー側
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 DTE_IGNORE_IMAGE_MODE = NEVER | ALWAYS | WHERE_UNSUPPORTED DTE_IGNORE_IMAGE_MODE オプションのデフォルト値は NEVER です。 ■ NEVER - 移動中のデータの暗号化をイメージの DTE モードに基づいて実行するように指定するには、このオプションを使用します。 ■ ALWAYS - NetBackup ホストが暗号化をサポートしているかどうかに関係なく、移動中のデータの暗号化中にイメージの DTE モードを常に無視するように指定するには、このオプションを使用します。移動中のデータの暗号化は、グローバル DTE モードとクライアント DTE モードに基づいて実行されます。 ■ WHERE_UNSUPPORTED - 環境内に 9.1 より前の NetBackup ホストがあり、DTE モードがイメージに対して有効になっている場合にこれらのホストに対するジョブでエラーが発生しないようにするには、このオプションを使用します。この構成では、移動中のデータの暗号化は、グローバルおよびクライアントの DTE モード設定に基づいて行われます。イメージの DTE モードは無視されます。
同等の NetBackup Web UI プロパティ	相当するエントリは存在しません。

メディアデバイスの選択 (MDS) とリソースの割り当て

リソースは、グローバル DTE モード、クライアント DTE モード、メディアサーバー DTE モード、およびイメージ DTE モードに基づいて割り当てられます。

MSDP やストレージユニットグループなどの動的ストレージユニットでは、DTE モードが On のメディアサーバーが推奨されます (ジョブの要件である場合)。

メモ: Snapshot Manager のバックアップおよびリカバリワークフローで、DTE が On である必要がある場合、それぞれのストレージユニット用に構成されている各メディアサーバー用に、DTE が On になるように構成されていることを確認する必要があります。

DTE モードが On のメディアサーバーがジョブで求められているにもかかわらず、そのようなメディアサーバーを利用できない場合、NetBackup は元のリソース割り当ての決定にフォールバックします。

このような場合、メディアサーバーで DTE が要求されていることを NetBackup が検出した場合、ジョブが進行し、その後のジョブの実行中 (bprd、nbjm、またはその他のデーモンや CLI など) にエラーが発生する場合があります。

次のプロセスでは、メディアデバイスの選択と DTE 検証がどのように行われるかを説明します。

1. バックアップ操作の場合は、手順 2 に直接進んでください。リストア、複製、レプリケーション、インポート、検証などのその他の操作では、ソースイメージ DTE モードが考慮されます。
   - イメージの DTE モードが ON の場合、他の DTE 構成とは関係なく、DTE が有効なメディアサーバーは ON になります。
   - イメージの DTE モードがオフの場合は、グローバル、クライアント、およびメディアサーバーの各 DTE モードを確認します。
2. グローバル DTE 設定が ENFORCED の場合は、DTE が有効なメディアサーバーが優先されます。
3. グローバル DTE 設定が PREFERRED ON または PREFERRED OFF の場合、クライアント DTE モードが考慮されます。
   - クライアント DTE モードが ON の場合 - DTE が有効なメディアサーバーが優先されます。
   - クライアント DTE モードが OFF の場合 - 利用可能な任意のメディアサーバーを選択できます。
   - クライアントの DTE モードが Automatic の場合 - グローバル DTE 設定に基づいて判断されます。これは、グローバル DTE 設定が PREFERRED OFF に設定されている場合には利用可能な任意のメディアサーバーを選択できることを意味します。そうでない場合は、DTE が有効なメディアサーバーを選択します。

リソース割り当ての際は、多くのパラメータが重要な役割を果たします。次に示すのは特別な条件です。

- クライアント名が空白の場合は、複製、レプリケーション、インポート、検証などの二次操作であることを示します。イメージ DTE モードまたはグローバル DTE モードが優先されます。

- クライアント名が空白でなくても、クライアントが 8.0 より前のバージョンであるためホストデータベースに存在しないと、クライアントは DTE をサポートしません。この場合、任意のメディアサーバーを選択できます。
- グローバルおよびクライアントの DTE 設定の後、メディアサーバーのバージョンとその DTE 設定が確認されます。
  - NetBackup 9.1 以降のメディアサーバーは、デフォルトでは DTE 対応で、DTE は有効になっています。
- DTE_IGNORE_IMAGE_MODE 設定 (イメージに基づく任意の二次操作用)
  - イメージ DTE モードが ON で、DTE_IGNORE_IMAGE_MODE オプションが適用されている場合、メディアサーバーの選択にはグローバル、クライアント、メディアサーバーの設定が使用されます。

さまざまな NetBackup 操作での DTE 構成設定の動作

このトピックでは、さまざまな NetBackup 操作に関し、必要な移動中のデータの暗号化を実現するためにどのように DTE 構成設定を変更できるかについて説明します。

DTE 構成設定を変更する前に、次の参照項目を確認してください。

以下の表は、さまざまな NetBackup 構成における特定の NetBackup ワークフローで、DTE 設定 (暗号化するかどうか) がどのように決定されるかを DTE 構成設定とともに示しています。

バックアップ

バックアップワークフローでは、データはバックアップジョブの一部としてメディアサーバーとクライアント間で転送されます。

図 18-1 バックアップのワークフロー

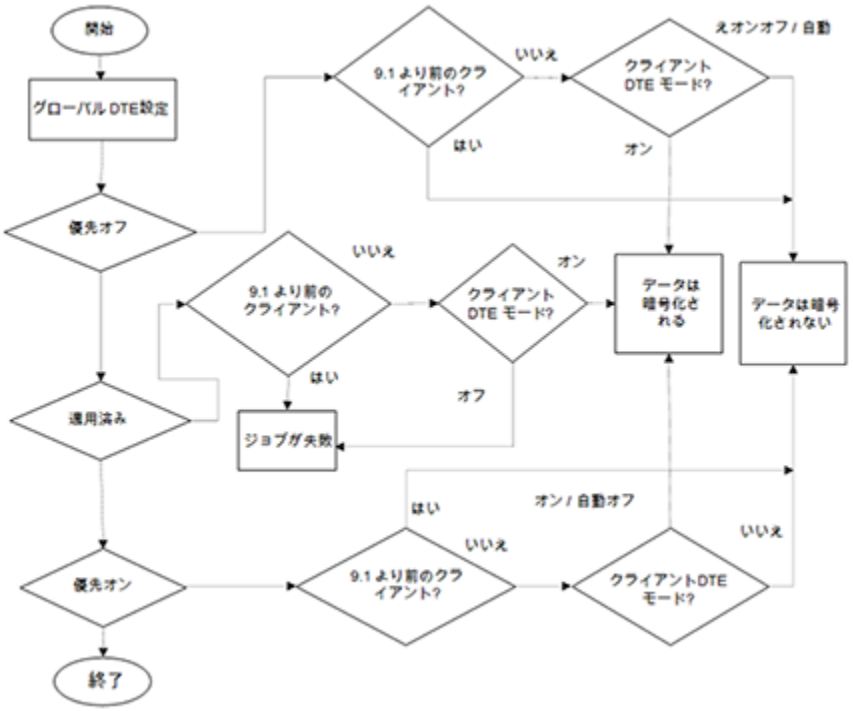


表 18-4 メディアサーバー DTE モードがオンの場合 (デフォルト)

グローバル DTE モード	NetBackup クライアント 9.1 以降の DTE モード			9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)
	オン	オフ	自動	
優先オフ	データは暗号化される	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化される	データは暗号化されない
適用済み	データは暗号化される	操作が失敗する	データは暗号化される	操作が失敗する

表 18-5 メディアサーバー DTE モードがオフの場合 (デフォルト)

グローバル DTE モード	NetBackup クライアント 9.1 以降の DTE モード			9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)
	オン	オフ	自動	
優先オフ	操作が失敗する	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	操作が失敗する	データは暗号化されない	データは暗号化されない	データは暗号化されない
適用済み	操作が失敗する	操作が失敗する	操作が失敗する	操作が失敗する

リストア

リストアワークフローには、次の 2 つの DTE シナリオがあります。

- イメージ DTE モードがオフの場合
- イメージ DTE モードがオンの場合

いずれのシナリオでも、1 つの NetBackup ジョブについてデータをクライアントでリストアするときに、1 つ以上のメディアサーバーが関与します (複数のイメージが選択されている場合)。

イメージ DTE モードがオフの場合

表 18-6 メディアサーバー DTE モードがオンの場合 (デフォルト)

グローバル DTE モード	NetBackup クライアント 9.1 以降の DTE モード			9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)
	オン	オフ	自動	
優先オフ	データは暗号化される	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化される	データは暗号化されない
適用済み	データは暗号化される	操作が失敗する	データは暗号化される	操作が失敗する

表 18-7 メディアサーバー DTE モードがオフの場合

グローバル DTE モード	NetBackup クライアント 9.1 以降の DTE モード			9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)
	オン	オフ	自動	
優先オフ	操作が失敗する	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	操作が失敗する	データは暗号化されない	データは暗号化されない	データは暗号化されない
適用済み	操作が失敗する	操作が失敗する	操作が失敗する	操作が失敗する

表 18-8 メディアサーバーが混在する場合 (9.1 と 10.0 以降) - Media1 は DTE モードがオン、Media2 は DTE モードがオフ

グローバル DTE モード	NetBackup クライアント 9.1 以降の DTE モード			9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)
	オン	オフ	自動	
優先オフ	Media1 - データは暗号化される Media2 - 操作が失敗する ジョブの状態 - 部分的に成功 ジョブ DTE モード - オン	Media1 - データは暗号化されない Media2 - データは暗号化されない	Media1 - データは暗号化されない Media2 - データは暗号化されない	Media1 - データは暗号化されない Media2 - データは暗号化されない
優先オン	Media1 - データは暗号化される Media2 - 操作が失敗する ジョブの状態 - 部分的に成功 ジョブ DTE モード - オン	Media1 - データは暗号化されない Media2 - データは暗号化されない	Media1 - データは暗号化される Media2 - データは暗号化されない ジョブ DTE モード - オフ	Media1 - データは暗号化されない Media2 - データは暗号化されない
適用済み	Media1 - データは暗号化される Media2 - 操作が失敗する ジョブの状態 - 部分的に成功 ジョブ DTE モード - オン	Media1 - 操作が失敗する Media2 - 操作が失敗する ジョブの状態 - 失敗	Media1 - データは暗号化される Media2 - 操作が失敗する ジョブの状態 - 部分的に成功 ジョブ DTE モード - オン	Media1 - 操作が失敗する Media2 - 操作が失敗する ジョブの状態 - 操作が失敗する

イメージ DTE モードがオンの場合

イメージDTEモードがオンの場合、デフォルトの動作では、9.1以降のホストについて移動中のデータの暗号化を使用してリストアが行われ、DTE をサポートしていないホストがワークフローに含まれている場合はジョブが失敗します。ただし、イメージ DTE モードを無視してもリストアできます。

プライマリサーバーに設定する DTE_IGNORE_IMAGE_MODE 構成オプションを使用してください。指定可能な値: NEVER (デフォルト) | ALWAYS | WHERE_UNSUPPORTED

表 18-9 イメージ DTE モードがオンで、メディアサーバー DTE モードがオンの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	NetBackup クライアント 9.1 以降で DTE モードがオンの場合	データは暗号化される	データは暗号化される	データは暗号化される
	NetBackup クライアント 9.1 以降で DTE モードがオフの場合	操作が失敗する	操作が失敗する	データは暗号化されない
	NetBackup クライアント 9.1 以降で DTE モードが自動の場合	データは暗号化される	データは暗号化される	データは暗号化されない
	9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)	操作が失敗する	データは暗号化されない	データは暗号化されない
優先オン	NetBackup クライアント 9.1 以降で DTE モードがオンの場合	データは暗号化される	データは暗号化される	データは暗号化される
	NetBackup クライアント 9.1 以降で DTE モードがオフの場合	操作が失敗する	操作が失敗する	データは暗号化されない
	NetBackup クライアント 9.1 以降で DTE モードが自動の場合	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)	操作が失敗する	データは暗号化されない	データは暗号化されない

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
適用済み	NetBackup クライアント 9.1 以降で DTE モードがオンの場合	データは暗号化される	データは暗号化される	データは暗号化される
	NetBackup クライアント 9.1 以降で DTE モードがオフの場合	操作が失敗する	操作が失敗する	操作が失敗する
	NetBackup クライアント 9.1 以降で DTE モードが自動の場合	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)	操作が失敗する	操作が失敗する	操作が失敗する

表 18-10 イメージ DTE モードがオンで、10.0 以降のメディアサーバーの DTE 設定がオフの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	NetBackup クライアント 9.1 以降で DTE モードがオンの場合	操作が失敗する	操作が失敗する	操作が失敗する
	NetBackup クライアント 9.1 以降で DTE モードがオフの場合	操作が失敗する	操作が失敗する	データは暗号化されない
	NetBackup クライアント 9.1 以降で DTE モードが自動の場合	操作が失敗する	操作が失敗する	データは暗号化されない
	9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)	操作が失敗する	データは暗号化されない	データは暗号化されない

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オン	NetBackup クライアント 9.1 以降で DTE モードがオンの場合	操作が失敗する	操作が失敗する	操作が失敗する
	NetBackup クライアント 9.1 以降で DTE モードがオフの場合	操作が失敗する	操作が失敗する	データは暗号化されない
	NetBackup クライアント 9.1 以降で DTE モードが自動の場合	操作が失敗する	操作が失敗する	データは暗号化されない
	9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)	操作が失敗する	データは暗号化されない	データは暗号化されない
適用済み	NetBackup クライアント 9.1 以降で DTE モードがオンの場合	操作が失敗する	操作が失敗する	操作が失敗する
	NetBackup クライアント 9.1 以降で DTE モードがオフの場合	操作が失敗する	操作が失敗する	操作が失敗する
	NetBackup クライアント 9.1 以降で DTE モードが自動の場合	操作が失敗する	操作が失敗する	操作が失敗する
	9.1 より前の NetBackup ホスト (メディアサーバーまたはクライアント)	操作が失敗する	操作が失敗する	操作が失敗する

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-7 に基づきます。

MSDP のバックアップ、リストア、最適化複製

移動中のデータの暗号化 (DTE) 機能は、バックアップとリストアのワークフロー用の MSDP ストレージサーバーに統合されました。

MSDP ディスクプールでのバックアップの場合、クライアントからメディアサーバーへのデータパスの暗号化は、NetBackup DTE 設定 (グローバル DTE モードとクライアント DTE モード) によって制御されます。

MSDP ストレージサーバーに複数の負荷分散メディアサーバーが接続されており、選択したメディアサーバーが 10.0.0.1 以降の場合、ストレージサーバーは 10.0.0.1 以降である必要があります。そうでないと、バックアップジョブは失敗します。10.0 ストレージサーバーを 10.0.0.1 にアップグレードする必要があります。負荷分散メディアサーバーが 10.0 以前の場合、DTE が優先される場合でも、データは平文で転送でき、ジョブは常に成功します。

理想的には、DTE が有効であれば、10.0.0.1 以降の負荷分散メディアサーバーとストレージサーバーを設ける必要があります。

これらの条件は、最適化複製のワークフローにも有効です。

ストレージサーバーまたは負荷分散メディアサーバーのいずれかが 10.0 より前である混在環境の場合、エンドツーエンドの暗号化を実現するには次の構成が必要です。

- DTE は、DTE 構成 (グローバル設定、メディアサーバー設定、およびクライアント設定) に基づいて NetBackup 側から有効にする必要がある
- pd.conf の ENCRYPTION フラグを使用して MSDP 側から暗号化を有効にする必要がある
  MSDP を使用した暗号化の有効化について詳しくは、『NetBackup 重複排除ガイド』を参照してください。

メモ: 移動中のデータの暗号化が NetBackup で有効になっており、`pd.conf` の `ENCRYPTION` フラグも有効になっている場合、MSDP 暗号化が NetBackup DTE より優先されます。その結果、格納データの暗号化が行われ、移動中のデータの暗号化は行われません。

Universal-Share ポリシーのバックアップ

Universal-Share ポリシー形式の場合、クライアントの選択肢となるのは、ユニバーサル共有があるストレージサーバーの名前、またはユニバーサル共有がマウントされているホストの名前です。そのため、NetBackup クライアントソフトウェアがインストールされていないホストがこのポリシー形式のクライアントになることも可能です。

この制限により、NetBackup はクライアントの DTE モードを確認できません。これは、Universal-Share ポリシーのバックアップのためにグローバルおよびメディアサーバー DTE モードを確認し、次の表に従って動作します。

表 18-11 Universal-Share ポリシーのバックアップ用の DTE

グローバル DTE モード	メディアサーバー 9.1 以降の DTE モード		9.1 より前のメディアサーバー
	オン	オフ	
優先オフ	データは暗号化されない	データは暗号化されない	データは暗号化されない

グローバル DTE モード	メディアサーバー 9.1 以降の DTE モード		9.1 より前のメディアサーバー
	オン	オフ	
優先オン	データは暗号化される	データは暗号化されない	データは暗号化されない
適用済み	データは暗号化される	操作が失敗する	操作が失敗する

カタログのバックアップとリカバリ

メディアサーバーは、カタログのバックアップおよびリカバリのワークフローに使用するプライマリサーバーと同じ NetBackup バージョンである必要があります。

次の点を確認してください。

- カタログバックアップジョブの DTE モードはファイルシステムのワークフローに似ており、DTE の判断は前述のバックアップワークフローに似ています。
- カタログバックアップジョブの DTE モードの場合:
  - 親カタログバックアップジョブには DTE モードが設定されません。
  - データベースステージングの子ジョブには DTE モードが設定されません。
  - 他の 2 つの子ジョブには、構成済みの DTE 設定に従って DTE モードが設定されます。
- カタログリカバリジョブの DTE モードの場合:
  - 最初の 2 つのジョブには、イメージ DTE モードに応じ、次の表に従って DTE モードが設定されます。
  - 最初の 2 つのジョブにより、グローバル DTE 設定とプライマリサーバーの bp.conf 値が置き換わるため、3 番目のジョブの DTE モードは、リカバリされたグローバル DTE 設定とプライマリサーバーの bp.conf 値に従って設定されます。

イメージ DTE モードがオフの場合

表 18-12 イメージ DTE モードがオフで、メディアサーバー DTE 設定がオンの場合

グローバル DTE モード	NetBackup プライマリサーバー 9.1 以降で DTE モードが次の状態の場合		
	オン	オフ	自動
優先オフ	データは暗号化される	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化される
適用済み	データは暗号化される	データは暗号化される	データは暗号化される

メモ: グローバル DTE 設定が ENFORCED に設定され、DTE_CLIENT_MODE がオフの場合、カタログリカバリの際に DTE がエラーより優先されます。

表 18-13 イメージ DTE モードがオフで、メディアサーバー DTE 設定がオフの場合

グローバル DTE モード	NetBackup プライマリサーバー 9.1 以降で DTE モードが次の状態の場合		
	オン	オフ	自動
優先オフ	データは暗号化される *	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される *	データは暗号化されない	データは暗号化されない
適用済み	データは暗号化される *	データは暗号化される *	データは暗号化される *

* は、カタログリカバリの際に DTE がエラーより優先されることを示します。クライアントの DTE モードが自動に設定されていないかぎり、メディアサーバーの DTE 設定は無視されます。

イメージ DTE モードがオンの場合

表 18-14 イメージ DTE モードがオンで、メディアサーバー DTE 設定がオンの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	DTE_CLIENT_MODE がオンのプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化される
	DTE_CLIENT_MODE がオフのプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化されない
	DTE_CLIENT_MODE が自動のプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化されない
優先オン	DTE_CLIENT_MODE がオンのプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化される
	DTE_CLIENT_MODE がオフのプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化されない
	DTE_CLIENT_MODE が自動のプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化される

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
適用済み	DTE_CLIENT_MODE がオンのプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化される
	DTE_CLIENT_MODE がオフのプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化される
	DTE_CLIENT_MODE が自動のプライマリサーバー	データは暗号化される	データは暗号化される	データは暗号化される

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-12 に基づきます。

表 18-15 イメージ DTE モードがオンで、メディアサーバー DTE 設定がオフの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	DTE_CLIENT_MODE がオンのプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化される *
	DTE_CLIENT_MODE がオフのプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化されない
	DTE_CLIENT_MODE が自動のプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化されない
優先オン	DTE_CLIENT_MODE がオンのプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化される *
	DTE_CLIENT_MODE がオフのプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化されない
	DTE_CLIENT_MODE が自動のプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化されない

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
適用済み	DTE_CLIENT_MODE がオンのプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化される *
	DTE_CLIENT_MODE がオフのプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化される
	DTE_CLIENT_MODE が自動のプライマリサーバー	データは暗号化される *	データは暗号化される *	データは暗号化される *

* は、カタログリカバリの際に DTE がエラーより優先されることを示します。クライアントの DTE モードが自動に設定されていないかぎり、メディアサーバーの DTE 設定は無視されます。

複製

複製のワークフローでは、あるストレージユニットから別のストレージユニットにバックアップコピーがコピーされるため、クライアントは関与しません。参加ホストは、ソースメディアサーバーと、同じドメインのターゲットメディアサーバーです。

表 18-16　　イメージ DTE モードがオフの場合

グローバル DTE モード	両方のメディアサーバーが 9.1 以降で DTE モードが次の状態の場合		いずれかのメディアサーバーが 9.1 より前
	オン	オフ	
優先オフ	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化されない
適用済み	データは暗号化される	操作が失敗する	操作が失敗する

表 18-17 イメージ DTE モードがオンで、メディアサーバー DTE 設定がオンの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	両方の NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化されない
	9.1 より前の NetBackup メディアサーバーがある	操作が失敗する	データは暗号化されない	データは暗号化されない
優先オン	両方の NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバーがある	操作が失敗する	データは暗号化されない	データは暗号化されない
適用済み	両方の NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバーがある	操作が失敗する	操作が失敗する	操作が失敗する

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-16 に基づきます。

表 18-18 イメージ DTE モードがオンで、10.0 以降のメディアサーバー DTE 設定がオフの場合

グローバル DTE モード	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
	NEVER	WHERE_UNSUPPORTED	ALWAYS
優先オフ	操作が失敗する	操作が失敗する	データは暗号化されない
優先オン	操作が失敗する	操作が失敗する	データは暗号化されない
適用済み	操作が失敗する	操作が失敗する	操作が失敗する

合成バックアップ

合成バックアップは、合成完全バックアップまたは合成累積型バックアップのいずれかです。合成イメージの作成に使用されるイメージは、コンポーネントイメージと呼ばれます。たとえば、合成完全バックアップのコンポーネントイメージは、前回の完全バックアップのイメージおよびその後の増分バックアップのイメージです。NetBackup の典型的なバック

アップ処理では、クライアントにアクセスしてバックアップを作成します。合成バックアップとは、クライアントを使用せずに作成されたバックアップイメージのことです。合成バックアップ処理では、クライアントを使用する代わりに、コンポーネントイメージと呼ばれる、以前に作成したバックアップイメージを使用して完全イメージまたは累積増分イメージが作成されます。合成バックアップのワークフローでは、イメージは異なるソースストレージユニットからフェッチされ、合成され、ターゲットストレージユニットにコピーされます。

関与するホストは、ソースメディアサーバーと、同じドメインのターゲットメディアサーバーです。

表 18-19 イメージで DTE モードがオフになっている場合

グローバル DTE モード	すべての NetBackup メディアサーバー 9.1 以降で DTE モードが次の状態の場合		9.1 より前の NetBackup メディアサーバーがある
	オン	オフ	
優先オフ	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化されない
適用済み	データは暗号化される	操作が失敗する	操作が失敗する

表 18-20 いずれかのイメージの DTE モードがオンで、メディアサーバー DTE 設定がオンの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	すべての NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化されない
	9.1 より前の NetBackup メディアサーバーがある	操作が失敗する	データは暗号化されない	データは暗号化されない
優先オン	すべての NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバーがある	操作が失敗する	データは暗号化されない	データは暗号化されない

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
適用済み	すべての NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバーがある	操作が失敗する	操作が失敗する	操作が失敗する

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-19 に基づきます。

表 18-21 イメージ DTE モードがオンで、10.0 以降のメディアサーバー DTE 設定がオフの場合

グローバル DTE モード	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
	NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	操作が失敗する	操作が失敗する	データは暗号化されない
優先オン	操作が失敗する	操作が失敗する	データは暗号化されない
適用済み	操作が失敗する	操作が失敗する	操作が失敗する

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-19 に基づきます。

注意:

検証

検証ワークフローでは、バックアップイメージヘッダーが読み取られ、その整合性がカタログと照合されます。したがって、クライアントは関与しません。参加ホストは、メディアサーバーと、同じドメインのプライマリサーバーです。

表 18-22 イメージ DTE モードがオフの場合

グローバル DTE モード	NetBackup メディアサーバー 9.1 以降で DTE モードが次の状態の場合		9.1 より前の NetBackup メディアサーバー
	オン	オフ	
優先オフ	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化されない
適用済み	データは暗号化される	操作が失敗する	操作が失敗する

表 18-23 イメージ DTE モードがオンで、メディアサーバー DTE 設定がオンの場合

グローバル DTE モード	NetBackup クライアント 9.1 以降の DTE モード	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	メディアサーバー 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化されない
	9.1 より前のメディアサーバー	操作が失敗する	データは暗号化されない	データは暗号化されない
優先オン	メディアサーバー 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前のメディアサーバー	操作が失敗する	データは暗号化されない	データは暗号化されない
適用済み	メディアサーバー 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前のメディアサーバー	操作が失敗する	操作が失敗する	操作が失敗する

表 18-24 イメージ DTE モードがオンで、10.0 以降のメディアサーバー DTE 設定がオフの場合

グローバル DTE モード	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
	NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	操作が失敗する	操作が失敗する	データは暗号化されない
優先オン	操作が失敗する	操作が失敗する	データは暗号化されない

グローバル DTE モード	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
	NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
適用済み	操作が失敗する	操作が失敗する	操作が失敗する

インポート

インポートワークフローでは、バックアップイメージがストレージユニットから読み取られ、NetBackup カタログが作成されます。したがって、クライアントは関与しません。参加ホストは、メディアサーバーと、同じドメインのプライマリサーバーです。

メモ: イメージに基づいて DTE 制御を保持する場合は、インポート操作を実行する前に、インポート操作に使用するメディアサーバーを NetBackup 10.0 にアップグレードする必要があります。

次の表は、フェーズ 1 のインポート、フェーズ 2 のインポート、SLP (ストレージライフサイクルポリシー) のインポートなど、すべてのインポートワークフローに適用できます。

表 18-25 イメージで DTE モードがオフになっている場合

グローバル DTE モード	メディアサーバーが 9.1 以降で DTE モードが次の状態の場合		9.1 より前のメディアサーバー
	オン	オフ	
優先オフ	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化されない
適用済み	データは暗号化される	操作が失敗する	操作が失敗する

表 18-26 イメージ DTE モードがオンで、メディアサーバー DTE 設定がオンの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	NetBackup メディアサーバー 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化されない
	9.1 より前の NetBackup メディアサーバー	データは暗号化されない	データは暗号化されない	データは暗号化されない

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オン	NetBackup メディアサーバー 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバー	データは暗号化されない	データは暗号化されない	データは暗号化されない
適用済み	NetBackup メディアサーバー 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバー	操作が失敗する	操作が失敗する	操作が失敗する

メモ: フェーズ 1 のインポートでは、9.1 以降のメディアサーバーのイメージの DTE モードを無視するようにメディアサーバーで DTE_IGNORE_IMAGE_MODE を設定する必要があります。

フェーズ 1 のインポートシナリオでは、9.1 より前の NetBackup メディアサーバーはイメージの DTE モードを認識しません。フェーズ 1 のインポートで DTE モードがオンに設定された状態でイメージが作成された場合、9.1 より前のバージョンのメディアサーバーではジョブは失敗せず、イメージ DTE モードがカタログでオフに設定されます。

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は 表 18-25 に従って行われます。

表 18-27 イメージ DTE モードがオンで、10.0 以降のメディアサーバー DTE 設定がオフの場合

グローバル DTE モード	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
	NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	操作が失敗する	操作が失敗する	データは暗号化されない
優先オン	操作が失敗する	操作が失敗する	データは暗号化されない
適用済み	操作が失敗する	操作が失敗する	操作が失敗する

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-25 に基づきます。

ターゲットドメインでの MSDP SLP のインポート

この場合、イメージはすでにターゲットディスクプールにレプリケートされているため、SLP インポートポリシーを使用してそのイメージからカタログを作成することが目的になります。この操作はターゲットドメインで行われ、クロスドメイン操作は起こらないので、ターゲットの DTE グローバル設定が関与します。

レプリケートされたイメージで DTE モードがオンの場合、他の DTE 構成に関係なく、インポート操作は DTE モードがオンの状態で実行されます。

レプリケートされたイメージで DTE モードがオフの場合、DTE モードはターゲットドメインのグローバル DTE 設定に基づいて導出され、インポートは導出された DTE モードに基づいて実行されます。

このワークフローについて考慮する必要がある、次の MSDP の制限事項を確認してください。

- MSDP ストレージサーバーに複数の負荷分散メディアサーバーが接続されており、選択したメディアサーバーが 10.0.0.1 以降の場合、ストレージサーバーは 10.0.0.1 以降である必要があります。そうでないと、バックアップジョブは失敗します。10.0 ストレージサーバーを 10.0.0.1 にアップグレードする必要があります。
  負荷分散メディアサーバーが 10.0 以前の場合、DTE が優先される場合でも、データは平文で転送でき、ジョブは常に成功します。
  理想的には、DTE が有効であれば、10.0.0.1 以降の負荷分散メディアサーバーとストレージサーバーを設ける必要があります。
- ストレージサーバーまたは負荷分散メディアサーバーのいずれかが 10.0 より前のバージョンである混在環境の場合、エンドツーエンドの暗号化を実現するには次の構成が必要です。
  - DTE は、DTE 構成設定 (グローバル、メディアサーバー、およびクライアント DTE モード) に基づいて NetBackup 側から有効にする必要がある
  - pd.conf の `ENCRYPTION` フラグを使用して MSDP 側から暗号化を有効にする必要がある

MSDP を使用した暗号化の有効化について詳しくは、『NetBackup 重複排除ガイド』を参照してください。

メモ: NetBackup で DTE をオンにしても、pd.conf の ENCRYPTION フラグが有効になっていない場合、負荷分散メディアサーバーからストレージサーバーへのデータパスは暗号化されません。ただし、ジョブ DTE モードとイメージ DTE モードはオンになることがあります。

DTE が NetBackup 側で有効になっており、暗号化が MSDP 側で有効になっている (pd.conf の `ENCRYPTION` フラグ) 場合、MSDP 暗号化が NetBackup DTE より優先されます。その結果、格納データの暗号化が行われ、移動中のデータの暗号化は行われません。

レプリケーション

MSDP ストレージサーバーをレプリケーションに使用する場合は、次の注意事項を確認する必要があります。

- 移動中のデータの暗号化 (DTE) 機能は、レプリケーションワークフローの MSDP ストレージとは統合されておらず、pd.conf の OPTDUP_ENCRYPTION フラグによって制御されます。
- ジョブ DTE モードは、イメージ DTE モードまたはソースドメインのグローバル DTE 設定に依存します。
- DTE 構成設定、およびソースドメインとターゲットドメインの OPTDUP_ENCRYPTION フラグには、正しい値を設定する必要があります。

MSDP を使用した暗号化の有効化について詳しくは、『NetBackup 重複排除ガイド』を参照してください。

表 18-28　イメージ DTE モードがオフの場合

グローバル DTE モード	メディアサーバーが 9.1 以降で DTE モードが次の状態の場合		9.1 より前のメディアサーバー
	オン	オフ	
優先オフ	データは暗号化されない	データは暗号化されない	データは暗号化されない
優先オン	データは暗号化される	データは暗号化されない	データは暗号化される
適用済み	データは暗号化される	操作が失敗する	データは暗号化される

表 18-29　イメージ DTE モードがオンで、メディアサーバー DTE 設定がオンの場合

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化されない
	9.1 より前の NetBackup メディアサーバー	データは暗号化される	データは暗号化される	データは暗号化されない
優先オン	NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバー	データは暗号化される	データは暗号化される	データは暗号化される

グローバル DTE モード	ホスト	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
		NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
適用済み	NetBackup メディアサーバーが 9.1 以降	データは暗号化される	データは暗号化される	データは暗号化される
	9.1 より前の NetBackup メディアサーバー	データは暗号化される	データは暗号化される	データは暗号化される

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-28 に基づきます。

表 18-30 イメージ DTE モードがオンで、10.0 以降のメディアサーバー DTE 設定がオフの場合

グローバル DTE モード	DTE_IGNORE_IMAGE_MODE 構成オプションの値		
	NEVER (デフォルト)	WHERE_UNSUPPORTED	ALWAYS
優先オフ	操作が失敗する	操作が失敗する	データは暗号化されない
優先オン	操作が失敗する	操作が失敗する	データは暗号化されない
適用済み	操作が失敗する	操作が失敗する	操作が失敗する

メモ: DTE_IGNORE_IMAGE_MODE が ALWAYS に設定されている場合、DTE の判断は表 - 表 18-28 に基づきます。

19

外部 CA と外部証明書

この章では以下の項目について説明しています。

- NetBackup での外部 CA のサポートについて
- NetBackup ホスト通信で外部証明書を使用するワークフロー
- 外部 CA が署名した証明書の構成オプション
- NetBackup サービスがローカルサービスアカウントのコンテキストで実行されている場合の Windows 証明書ストアの制限事項
- 外部 CA の証明書失効リストについて
- 証明書の登録について
- プライマリサーバーの登録状態の表示について
- NetBackup Web サーバーで外部証明書を使用するための構成
- 外部 CA が署名した証明書を使用するプライマリサーバーの構成
- インストール後に外部 CA が署名した証明書を使用するための NetBackup ホスト (メディアサーバー、クライアント、クラスタノード) の構成
- リモートホストの外部証明書の登録
- NetBackup ドメインがサポートする認証局の表示
- NetBackup Web UI での外部 CA が署名した証明書の表示
- ファイルベースの外部証明書の更新
- 証明書の登録を削除
- NetBackup ドメインでの NetBackup CA の無効化
- NetBackup ドメインでの NetBackup CA の有効化

NetBackup での外部 CA のサポートについて

信頼できる認証局 (CA) が発行した X.509 証明書を使用できるようになりました。

NetBackup は、NetBackup ホストの外部証明書のソースとしてファイルベースの証明書と Windows 証明書ストアをサポートしています。PEM、DER、P7B 形式の証明書をサポートしています。

メモ: NetBackup は、NetBackup Web サーバー証明書のソースとして Windows 証明書ストアをサポートしていません。

NetBackup の証明書で使用される用語について

NetBackup で使用されるセキュリティ証明書に固有の用語は、次のとおりです。

- NetBackup CA 以外の認証局 (CA) は、外部 CA と呼ばれます。
- NetBackup CA 以外の CA が発行した証明書は、外部 CA が署名した証明書、または外部証明書と呼ばれます。
- NetBackup CA が発行した証明書は、NetBackup CA が署名した証明書、または NetBackup 証明書と呼ばれます。
- 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。

ホスト証明書に関する重要な注意事項

- ホスト ID ベースの証明書は、NetBackup のインストール時にプライマリサーバーに配備されます。インストールの終了後、プライマリサーバーで外部証明書を手動で構成する必要があります。
  p.411 の「外部 CA が署名した証明書を使用するプライマリサーバーの構成」を参照してください。
- NetBackup ホスト (メディアサーバーまたはクライアント) の外部証明書は、インストールの実行中または終了後に構成できます。
  p.413 の「インストール後に外部 CA が署名した証明書を使用するための NetBackup ホスト (メディアサーバー、クライアント、クラスタノード) の構成」を参照してください。
- 相互に認証された安全な通信を可能にするため、ホスト ID ベースの証明書はすべての NetBackup 8.1 以降のホストに必要です。8.2 以降、NetBackup CA が署名し

たホスト ID ベースの証明書は、外部 CA が署名した証明書に置き換えることができます。

ホスト ID ベースの証明書に加えて、NetBackup アクセス制御 (NBAC)が有効になっているドメイン内の一部のホストに、ホスト名ベースの証明書を配備する必要がある場合があります。ホスト名ベースの証明書は、NetBackup CA によって発行されます。

p.264 の「NetBackup のセキュリティ証明書の概要」を参照してください。

外部証明書の構成の要件

- Windows プラットフォームでは、ホストの通信に外部証明書が使用されている場合、NT AUTHORITY¥SYSTEM ユーザーが、ECA_CERT_PATH に配置された証明書にアクセスできる必要があります。ECA_CERT_PATH 構成オプションは、Windows レジストリにあります。
- Windows プラットフォームでは、外部 CA パラメータ (証明書チェーン、証明書の秘密鍵、トラストストア、証明書の秘密鍵のパスフレーズファイル、CRL キャッシュ) で、汎用名前付け規則 (UNC) パス (またはネットワークパス) がサポートされていません。
- 次の要件は、NetBackup Web サーバー証明書に該当します。
  サブジェクトの別名 (SAN) が空でない場合、証明書では、プライマリサーバーが認識されるすべてのホスト名 (ドメイン内の他のホストの SERVER 構成オプションのエントリに記載されているホスト名) を証明書の SAN フィールドに含める必要があります。
- 証明書のサブジェクト名の要件:
  - サブジェクト名を空にすることはできません。
  - サブジェクト名の一般名を空にすることはできません。
  - サブジェクト名は各ホストで一意である必要があります。
  - サブジェクト名は 255 文字未満にする必要があります。
- 証明書のサブジェクトとサブジェクトの別名 (SAN) では、ASCII 7 文字のみがサポートされています。
- キー用途の目的の必要条件は次のとおりです。

  証明書に X509v3 キー用途の拡張がある場合は、次のようなキーの用途の目的が含まれている必要があります。
  - Web サーバー証明書の場合: デジタル署名またはキーの暗号化のうち少なくとも 1 つが存在する必要があります。
  - NetBackup ホスト証明書の場合: デジタル署名の目的が存在する必要があります。キーの暗号化は存在しないこともあります。
  - Web サーバーおよび NetBackup ホストの両方で使用する証明書の場合: デジタル署名の用途が存在する必要があります。キーの暗号化は存在しないこともあります。

- 証明書には、ここで指定した目的に加えて他のキー用途の目的も記載されている場合があります。これらの追加の目的は無視されます。
- X509v3 キー用途の拡張は、重要または非重要のいずれかになる場合があります。
- X509v3 キー用途の拡張を備えていない証明書は、NetBackup でも使用できます。

証明書に X509v3 拡張キー用途の拡張がある場合は、次のようなキー用途の目的が含まれている必要があります。

- Web サーバー証明書の場合: TLS Web サーバー認証。
- NetBackup ホスト証明書の場合: TLS Web サーバー認証および TLS Web クライアント認証。
- Web サーバーと NetBackup ホストの両方に使用される証明書の場合: TLS Web サーバー認証および TLS Web クライアント認証。
- 証明書には、ここで指定した目的に加えて他のキー用途の目的も記載されている場合があります。これらの追加の目的は無視されます。
- X509v3 拡張キー用途の拡張は、重要または非重要のいずれかになる場合があります。
- X509v3 拡張キー用途の拡張を備えていない証明書は、NetBackup でも使用できます。
- 証明書がこれらの要件を満たしていない場合は、証明書のプロバイダに連絡して新しい証明書を取得してください。

外部証明書の構成に使用するコマンドラインオプション

外部証明書の構成には次の固有のコマンドラインオプションを使用します。

nbcertcmd	■ -cleanupCRLCache ■ -createECACertEntry ■ -deleteECACertEntry ■ -ecaHealthCheck ■ -enrollCertificate ■ -getExternalCertDetails ■ -listEnrollmentStatus ■ -removeEnrollment ■ -updateCRLCache

configureWebServerCerts	■ -addExternalCert ■ -removeExternalCert ■ -validateExternalCert

次のコマンドラインオプションは、外部証明書と NetBackup 証明書の両方の構成に使用されます。

nbcertcmd	■ -listCertDetails: このコマンドオプションは、NetBackup CA が署名した証明書にデフォルトで適用可能です。-ECA オプションと共に使用すると、外部 CA が署名した証明書に適用できます。 ■ -listCACertDetails: このコマンドオプションは、NetBackup CA が署名した証明書にデフォルトで適用可能です。-ECA オプションと共に使用すると、外部 CA が署名した証明書に適用できます。

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。

NetBackup ホスト通信で外部証明書を使用するワークフロー

安全な通信を行うために、NetBackup で外部 CA が署名した証明書を使用するように構成するには、示された順序で次の手順を実行する必要があります。

表 19-1 NetBackup ホスト通信で外部証明書を使用するワークフロー

手順	説明
手順 1	次の項目について確認します。 ■ Web サーバー、プライマリサーバー、およびすべてのホストの外部証明書が適切な場所に配置されている。 ■ ファイルベースの証明書の場合は、外部証明書の秘密鍵ファイルが適切な場所に配置されている。 p.394 の「NetBackup サーバーとクライアントの ECA_PRIVATE_KEY_PATH」を参照してください。 秘密鍵が暗号化されている場合は、パスフレーズファイルが適切な場所に配置されている必要があります。 p.395 の「NetBackup サーバーとクライアントの ECA_KEY_PASSPHRASEFILE」を参照してください。 ■ CRL 構成オプションに基づき、CRL がホスト上の必要な場所に配置され、アクセス可能である。 p.404 の「外部 CA の証明書失効リストについて」を参照してください。

手順	説明
手順 2	プライマリサーバーに NetBackup ソフトウェアをインストール (またはプライマリサーバーをアップグレード) します。
手順 3	NetBackup Web サーバーを構成し、NetBackup ドメインで外部証明書を使用できるようにします。 p.408 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。
手順 4	NetBackup プライマリサーバーホストの外部証明書を構成します。 p.411 の「外部 CA が署名した証明書を使用するプライマリサーバーの構成」を参照してください。
手順 5	NetBackup ソフトウェアをメディアサーバーとクライアントにインストール (またはメディアサーバーとクライアントをアップグレード) します。外部証明書を使用するようにプライマリサーバーが構成されている場合、ホストの外部証明書の情報を入力するようにインストーラによって求められます。
手順 6	**メモ:** この手順は、現在の NetBackup ソフトウェアをインストールしているが、外部証明書を使用するように構成されていないホスト (メディアサーバーとクライアント) で必要です。 次の理由により、NetBackup ホストで外部証明書が構成されていない場合があります。 ■ ホストのインストールまたはアップグレード中に、外部証明書の情報を入力しなかった。 ■ ホストのインストールまたはアップグレード中に、外部証明書を使用するように NetBackup プライマリサーバーが構成されなかった。 インストール後に NetBackup ホスト (メディアサーバーまたはクライアント) の外部証明書を構成します。 p.413 の「インストール後に外部 CA が署名した証明書を使用するための NetBackup ホスト (メディアサーバー、クライアント、クラスタノード) の構成」を参照してください。

外部 CA が署名した証明書の構成オプション

NetBackup プライマリサーバー、メディアサーバー、またはクライアントで、ホストとの通信に外部 CA が署名した証明書を使用するように構成するには、NetBackup 構成ファイル (UNIX プラットフォームの `bp.conf` または Windows レジストリ) で特定の構成オプションを定義する必要があります。

必須および省略可能な構成オプションについて

■ 外部証明書の構成では、ファイルベースの証明書の場合、次の構成オプションが必須です。

- ECA_CERT_PATH
- ECA_TRUST_STORE_PATH
- ECA_PRIVATE_KEY_PATH
  外部証明書の秘密鍵が暗号化されている場合は、ECA_KEY_PASSPHRASEFILE も必須です。

- Windows 証明書ストアの場合、次の構成オプションが必須です。
  - ECA_CERT_PATH
- 省略可能なオプションは次のとおりです。
  - ECA_CRL_CHECK
    このオプションが DISABLE (または 0) に設定されていると、ECA_CRL_PATH オプションは無視され、ピアホストの証明書の失効状態が検証されません。
    このオプションが DISABLE と 0 以外の値に設定されていると、ECA_CRL_PATH に基づいて、ピアホストの証明書の失効状態が検証されます。
  - ECA_DR_BKUP_WIN_CERT_STORE
    Windows 証明書ストアの場合、カタログバックアップ中に外部証明書をバックアップするときは、このオプションを指定します。
  - ECA_CRL_PATH_SYNC_HOURS
    このオプションは、ECA_CRL_CHECK が有効で ECA_CRL_PATH が定義されているときに使用されます。
  - ECA_CRL_REFRESH_HOURS
    このオプションは、ECA_CRL_CHECK が有効だが、ECA_CRL_PATH が定義されていない (CDP が CRL ソースとして使用されている) ときに使用されます。

p.404 の「外部 CA の証明書失効リストについて」を参照してください。

NetBackup サーバーとクライアントの ECA_CERT_PATH

ECA_CERT_PATH オプションでは、ホストの外部 CA が署名した証明書のパスを指定します。このオプションは必須です。

NetBackup は、ホストの証明書に次の証明書ソースをサポートしています。

- Windows 証明書ストア

  メモ: Windows 証明書ストアは、クラスタ化されたプライマリサーバーではサポートされません。

- ファイルベースの証明書

証明書ファイルでの証明書の順序

証明書ファイルには、証明書との証明書チェーンが正しい順序で含まれている必要があります。チェーンはサーバー証明書 (リーフ証明書とも呼ばれる) から始まり、ゼロ個以上の中間証明書が続きます。チェーンには、ルート CA 証明書までのすべての中間証明書が含まれている必要がありますが、ルート CA 証明書そのものは含まれていません。チェーン内の各証明書がチェーン内の前の証明書に署名するように、チェーンが作成されます。

証明書ファイルは、次のいずれかの形式である必要があります。

- 指定された順序で証明書が含まれた、DER または PEM エンコードされた PKCS #7 または P7B ファイル
- 指定された順序で結合された PEM 証明書を持つファイル

表 19-2 ECA_CERT_PATH の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。

使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。
	これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。
	ファイルベースの証明書では、次の形式を使用します。
	`ECA_CERT_PATH = Path to the external certificate of the host`
	例: `c:¥server.pem`
	Flex Appliance アプリケーションインスタンスでこのオプションを使用する場合、パスは /mnt/nbdata/hostcert/ である必要があります。
	Windows 証明書ストアの場合は、次の形式を使用します。
	`ECA_CERT_PATH = Certificate store name¥Issuer name¥Subject name`
	複数の証明書ストアに関する選択の問い合わせをカンマ区切りの形式で指定できます。
	`ECA_CERT_PATH = Store name1¥Issuer name1¥Subject name1,Store name2¥Issuer name2¥Subject name2`
	p.391 の「ECA_CERT_PATH の Windows 証明書ストアの指定」を参照してください。

使用方法	説明
同等の NetBackup Web UI プロパティ	相当するエントリは存在しません。

ECA_CERT_PATH の Windows 証明書ストアの指定

NetBackup は、Windows ホスト上のローカルマシン証明書ストアから証明書を選択します。

Windows 証明書ストアの場合、ECA_CERT_PATH はカンマ区切りの句のリストです。

各句の形式は、「*ストア名*¥*発行者*¥*サブジェクト*」です。句の各要素には、問い合わせが含まれています。

$hostname は、ホストの完全修飾ドメイン名に置換されるキーワードです。実際のパス内に ¥ がある場合は二重引用符を使用します。たとえば、
MY¥Veritas¥"NetBackup¥$hostname" のようにします。

$shorthostname は、ホストの短縮名に置換されるキーワードです。実際のパス内に ¥ がある場合は二重引用符を使用します。たとえば、
MY¥Veritas¥"NetBackup¥$shorthostname" のようにします。

「ストア名」には、証明書が存在するストアの正確な名前が必要です。たとえば、「MY」のようにします。

「発行者」は省略可能です。このオプションを指定すると、NetBackup は、指定された部分文字列が発行者 DN に含まれる証明書を選択します。

「サブジェクト」は必須です。NetBackup は、指定された部分文字列がサブジェクト DN に含まれる証明書を選択します。

次を確認する必要があります。

- Windows 証明書ストアの信頼できるルート認証局またはサードパーティのルート認証局にルート証明書を追加します。
- 中間 CA が存在する場合、Windows 証明書ストアの中間認証局にそれらの証明書を追加します。

例: WHERE 句を使用した証明書の場所

- My¥Veritas¥$hostname, My¥ExampleCompany¥$hostname
  この場合 (証明書ストアは MY、発行者 DN に Veritas が含まれ、サブジェクト DN に $hostname が含まれる) または (証明書ストア名は MY、発行者 DN に ExampleCompany が含まれ、サブジェクト DN に $hostname が含まれる)
- MY¥Veritas¥"NetBackup¥$hostname"
  この場合、証明書ストア名は MY、発行者 DN に Veritas が含まれ、サブジェクト DN に NetBackup¥$hostname が含まれる

- MY¥¥$hostname
  この場合、証明書ストア名は MY、任意の発行者 DN、サブジェクト DN に $hostname が含まれる
- MY¥¥$shorthostname
  この場合、証明書ストア名は MY、任意の発行者 DN、サブジェクト DN に $shorthostname が含まれる
- MY¥Veritas¥NetBackup $hostname
  この場合、証明書ストア名は MY、発行者 DN に Veritas が含まれ、サブジェクト DN に NetBackup $hostname が含まれる

単語の間にスペースを指定すると、有効な文字と見なされます。

例: 無効なデータを含む証明書の場所

- MY¥¥
  サブジェクト DN には値が必要です。
- My¥$hostname
  サブジェクト DN には値が必要です。
- ¥¥$hostname
  証明書ストア名には、証明書が存在するストアの正確な値が必要です。
- MY¥CN=Veritas¥CN=$hostname
  サブジェクト DN と発行者 DN に「=」や、「CN=」などの特定のタグを含めることはできません。

NetBackup サーバーとクライアントの ECA_TRUST_STORE_PATH

ECA_TRUST_STORE_PATH オプションでは、信頼できるすべてのルート CA 証明書を含む証明書バンドルファイルへのファイルパスを指定します。

この証明書ファイルには、PEM 形式の 1 つ以上の証明書が必要です。

Windows 証明書ストアを使用する場合、ECA_TRUST_STORE_PATH オプションを指定しないでください。

トラストストアは次の形式の証明書をサポートします。

- 信頼できるルート認証局の、バンドルされている証明書を持つ PKCS #7 または P7B ファイル。このファイルは、PEM または DER でエンコードされている場合があります。
- 信頼できるルート認証局の PEM エンコードされた証明書が連結されて含まれるファイル。

このオプションは、ファイルベースの証明書で必須です。

Cloudera ディストリビューションのルート CA 証明書は、Cloudera 管理者から取得できます。Hadoop クラスタで手動 TLS 構成または自動 TLS が有効になっている場合があります。いずれの場合も、NetBackup では管理者からのルート CA 証明書が必要になります。

セキュア (SSL) クラスタの場合、Hadoop クラスタのルート CA 証明書を使用してすべてのノードの証明書を検証し、NetBackup でバックアップおよびリストアプロセスを実行できます。このルート CA 証明書は、このようなすべてのノードに対して発行された証明書のバンドルです。

自己署名 CA 環境、サードパーティ CA 環境、ローカル/中間 CA 環境の場合、`ECA_TRUST_STORE_PATH` でルート CA の証明書を構成する必要があります。たとえば、自動 TLS が有効な Cloudera 環境では、通常、`cm-auto-global_cacerts.pem` という名前のルート CA ファイルが `/var/lib/cloudera-scm-agent/agent-cert` のパスに置かれています。詳しくは、Cloudera のマニュアルを参照してください。

表 19-3 ECA_TRUST_STORE_PATH の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。 VMware、Red Hat Virtualization サーバー、Nutanix AHV に対して証明書の検証が必要な場合、NetBackup がホストの通信に使用する認証局 (NetBackup CA または外部 CA) に関係なく、NetBackup プライマリサーバーとそれぞれのアクセスホストでこのオプションを設定する必要があります。
使用方法	オプションを表示、追加、変更するには、`nbgetconfig` コマンドと `nbsetconfig` コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 `ECA_TRUST_STORE_PATH = Path to the external CA certificate` 例: `c:¥rootCA.pem` Flex Appliance アプリケーションインスタンスでこのオプションを使用する場合、パスは `/mnt/nbdata/hostcert/` である必要があります。
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_PRIVATE_KEY_PATH

ECA_PRIVATE_KEY_PATH オプションでは、ホストの外部 CA が署名した証明書の秘密鍵のファイルパスを指定します。

このオプションは、ファイルベースの証明書で必須です。

証明書の秘密鍵が暗号化されている場合は、ECA_KEY_PASSPHRASEFILE オプションを指定する必要があります。

p.395 の「NetBackup サーバーとクライアントの ECA_KEY_PASSPHRASEFILE」を参照してください。

NetBackup は、プレーンテキストまたは暗号化された PKCS #1 と PKCS #8 形式の秘密鍵をサポートします。これらは、PEM または DER でエンコードされている場合があります。ただし、PKCS #1 で暗号化されている場合は、PEM でエンコードされている必要があります。

暗号化された秘密鍵の場合、NetBackup は次の暗号化アルゴリズムをサポートしています。

- DES、3DES、AES (秘密鍵が PKCS #1 形式の場合)
- DES、3DES、AES、RC2、RC4 (秘密鍵が PKCS #8 形式の場合)

メモ: ECA_CERT_PATH オプションに Windows 証明書ストアを指定している場合、ECA_PRIVATE_KEY_PATH オプションは指定しないでください。

p.389 の「NetBackup サーバーとクライアントの ECA_CERT_PATH」を参照してください。

表 19-4 ECA_PRIVATE_KEY_PATH の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 ECA_PRIVATE_KEY_PATH = *Path to the private key of the external certificate* 例: c:¥key.pem Flex Appliance アプリケーションインスタンスでこのオプションを使用する場合、パスは /mnt/nbdata/hostcert/ である必要があります。
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_KEY_PASSPHRASEFILE

ECA_KEY_PASSPHRASEFILE オプションでは、外部証明書の秘密鍵のパスフレーズが格納されているテキストファイルのパスを指定します。

証明書の秘密鍵が暗号化されている場合にのみ、ECA_KEY_PASSPHRASEFILE オプションを指定する必要があります。

p.394 の「NetBackup サーバーとクライアントの ECA_PRIVATE_KEY_PATH」を参照してください。

メモ: Windows 証明書ストアを使用する場合、ECA_KEY_PASSPHRASEFILE オプションを指定しないでください。

p.389 の「NetBackup サーバーとクライアントの ECA_CERT_PATH」を参照してください。

メモ: MSDP ダイレクトクラウド階層化に使用される MSDP サーバーでは ECA_KEY_PASSPHRASEFILE を使用しないでください。これは MSDP ダイレクトクラウド階層化でサポートされないためです。

表 19-5 ECA_KEY_PASSPHRASEFILE の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 ECA_KEY_PASSPHRASEFILE = *Path to the passphrase file*
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_CRL_CHECK

ECA_CRL_CHECK オプションを使用すると、ホストの外部証明書の失効の確認レベルを指定できます。外部証明書の失効の確認を無効にすることもできます。確認に基づいて、ホストとの通信時に、証明書失効リスト (CRL) に対して証明書の失効状態が検証されます。

構成ファイル (UNIX または Windows レジストリの bp.conf) または CRL 配布ポイント (CDP) の ECA_CRL_PATH 構成オプションで指定されたディレクトリから CRL を使用するように選択することもできます。

p.397 の「NetBackup サーバーとクライアントの ECA_CRL_PATH」を参照してください。

表 19-6 ECA_CRL_CHECK の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 ECA_CRL_CHECK = *CRL check* 次のいずれかを指定できます。 ■ DISABLE (または 0) - 失効の確認を無効にします。ホストとの通信時に、CRL で証明書の失効状態は検証されません。 ■ LEAF (または 1) - CRL でリーフ証明書の失効状態が検証されます。これはデフォルト値です。 ■ CHAIN (または 2) - CRL で証明書チェーンの証明書すべての失効状態が検証されます。
同等の Web UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_CRL_PATH

ECA_CRL_PATH オプションは、外部認証局 (CA) の証明書失効リスト (CRL) が保存されているディレクトリのパスを指定します。

これらの CRL は、NetBackup CRL キャッシュにコピーされます。CRL キャッシュの CRL で外部証明書の失効状態が検証されます。

CRL キャッシュ内の CRL は、ECA_CRL_PATH に指定されたディレクトリにある CRL に、ECA_CRL_PATH_SYNC_HOURS オプションに基づいて定期的に更新されます。

ECA_CRL_CHECK または HADOOP_CRL_CHECK オプションが DISABLE (または 0) に設定されておらず、ECA_CRL_PATH オプションが指定されていない場合、NetBackup は CRL 配布ポイント (CDP) で指定された URL から CRL をダウンロードし、それらを使用してピアホストの証明書の失効状態を検証します。

メモ: 仮想化サーバー証明書の失効状態の検証には、VIRTUALIZATION_CRL_CHECK オプションを使用します。

Hadoop サーバー証明書の失効状態の検証には、HADOOP_CRL_CHECK オプションを使用します。

表 19-7 ECA_CRL_PATH の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。 VMware、Red Hat Virtualization サーバー、Nutanix AHV、または Hadoop に対して証明書の検証が必要な場合、NetBackup がホストの通信に使用する認証局 (NetBackup CA または外部 CA) に関係なく、NetBackup プライマリサーバーとそれぞれのアクセスホストまたはバックアップホストでこのオプションを設定する必要があります。 VMware、Red Hat Virtualization サーバー、または Hadoop に対して証明書の検証が必要な場合、NetBackup がホストの通信に使用する認証局 (NetBackup CA または外部 CA) に関係なく、NetBackup プライマリサーバーとそれぞれのアクセスホストまたはバックアップホストでこのオプションを設定する必要があります。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用して、CRL ディレクトリのパスを指定します。 `ECA_CRL_PATH = Path to the CRL directory` Flex Appliance アプリケーションインスタンスでこのオプションを使用する場合、パスは /mnt/nbdata/hostcert/crl である必要があります。
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_CRL_PATH_SYNC_HOURS

ECA_CRL_PATH_SYNC_HOURS オプションは、NetBackup CRL キャッシュの証明書失効リスト (CRL) を ECA_CRL_PATH 構成オプションに指定されているディレクトリの CRL に更新する間隔 (時間単位) を指定します。

p.397 の「NetBackup サーバーとクライアントの ECA_CRL_PATH」を参照してください。

CDP が CRL に使用されている場合、ECA_CRL_PATH_SYNC_HOURS オプションは適用されません。

デフォルトでは、キャッシュ内の CRL は 1 時間ごとに更新されます。

ホストとの通信時に、CRL キャッシュの CRL で外部証明書の失効状態が検証されます。

表 19-8 ECA_CRL_PATH_SYNC_HOURS の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 ECA_CRL_PATH_SYNC_HOURS = *Number of hours* 指定可能な最小時間数: 1 時間 指定可能な最大時間数: 720 時間 デフォルト値は 1 時間です。
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_CRL_REFRESH_HOURS

ECA_CRL_REFRESH_HOURS オプションは、ピアホスト証明書の CRL 配布ポイント (CDP) で指定した URL から CRL をダウンロードする間隔 (時間単位) を指定します。

ECA_CRL_REFRESH_HOURS オプションは、CDP を CRL に使用するときに適用されます。

p.397 の「NetBackup サーバーとクライアントの ECA_CRL_PATH」を参照してください。

指定した時間間隔が経過すると、認証局の CRL が、CDP で利用可能な URL からダウンロードされます。

デフォルトでは、24 時間ごとに CDP から CRL がダウンロードされます。

表 19-9 ECA_CRL_REFRESH_HOURS の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 ECA_CRL_REFRESH_HOURS = *Number of hours* 指定可能な最小時間数: 0 時間。CDP からの CRL が定期的にダウンロードされないことを示します。 指定可能な最大時間数: 4380 時間 このオプションのデフォルト値は 24 時間です。 **メモ:** ECA_CRL_REFRESH_HOURS オプションで設定した時間間隔とは関係なく、CRL は CRL キャッシュで期限切れまたは利用不能になると、ホストとの通信中に CDP からダウンロードされます。
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_DISABLE_AUTO_ENROLLMENT

外部 CA が署名した証明書を使用するように NetBackup が設定されている場合、そのような証明書はホストの通信中にプライマリサーバーに自動的に登録されます。そのような証明書の自動登録を無効にする場合は、ECA_DISABLE_AUTO_ENROLLMENT を「1」に設定します。

自動登録が無効になっている場合は、nbcertcmd -enrollCertificate コマンドを使用して外部証明書を手動で登録できます。

証明書をホストとの通信に使用するには、事前にプライマリサーバーに証明書を登録する必要があります。

デフォルトでは、証明書の自動登録は有効になっています。

表 19-10 ECA_DISABLE_AUTO_ENROLLMENT の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 ECA_DISABLE_AUTO_ENROLLMENT = 1
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup サーバーとクライアントの ECA_DR_BKUP_WIN_CERT_STORE

ECA_DR_BKUP_WIN_CERT_STORE オプションでは、カタログバックアップ時に Windows 証明書ストアの情報のバックアップを作成するかどうかを指定します。

デフォルトでは、カタログバックアップ時に Windows 証明書ストアの情報のバックアップが作成されます。

メモ: Windows 証明書ストアの情報をエクスポートできない場合、カタログのバックアップ中にはバックアップを作成できません。

表 19-11 ECA_DR_BKUP_WIN_CERT_STORE の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 カタログバックアップ操作で Windows 証明書ストアの情報のバックアップを作成しない場合は、次の形式を使用します。 ECA_DR_BKUP_WIN_CERT_STORE = NO
同等の UI プロパティ	相当するエントリは存在しません。

NetBackup プライマリサーバーの MANAGE_WIN_CERT_STORE_PRIVATE_KEY オプション

MANAGE_WIN_CERT_STORE_PRIVATE_KEY オプションを使用して、Windows 証明書ストアにある証明書の秘密鍵に対する権限の自動管理を無効にできます。

このオプションは、NetBackup サービスがローカルサービスアカウントのコンテキストで実行されている場合にのみ、Windows 証明書ストアに適用されます。

NetBackup サービスがローカルサービスアカウントのコンテキストで実行されている場合、サービスには Windows 証明書ストアで証明書の秘密鍵を読み取る権限が付与されている必要があります。

MANAGE_WIN_CERT_STORE_PRIVATE_KEY オプションを Automatic に設定すると、特権ユーザーアカウントのコンテキストで実行されている NetBackup サービスは、必要に応じてその他すべての NetBackup サービスに秘密鍵を読み取るためのアクセス権を付与します。

デフォルトでは、秘密鍵の権限は自動で管理されます。
MANAGE_WIN_CERT_STORE_PRIVATE_KEY オプションを Disabled に設定すると、秘密鍵の権限を手動で管理する必要があります。

メモ: MANAGE_WIN_CERT_STORE_PRIVATE_KEY オプションを Disabled に設定することはお勧めしません。

このオプションが Disabled の場合に権限を手動で更新するには、次のコマンドを実行します。

```
nbcertcmd -setWinCertPrivKeyPermissions -reason audit reason -force
```

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

表 19-12 MANAGE_WIN_CERT_STORE_PRIVATE_KEY の情報

使用方法	説明
使用する場所	NetBackup プライマリサーバー上。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 MANAGE_WIN_CERT_STORE_PRIVATE_KEY = Automatic

使用方法	説明
同等の NetBackup Web UI プロパティ	相当するエントリは存在しません。

NetBackup サービスがローカルサービスアカウントのコンテキストで実行されている場合の Windows 証明書ストアの制限事項

NetBackup サービスがローカルサービスアカウントのコンテキストで実行されている場合、サービスには秘密鍵を読み取る権限が付与されている必要があります。NetBackup は証明書の登録時に秘密鍵の権限を更新し、NetBackup サービスに秘密鍵への読み取りアクセス権を付与します。

権限を設定するには、使用する証明書の CSP (暗号サービスプロバイダ) または KSP (キーストレージプロバイダ) がセキュリティ記述子をサポートしている必要があります。

セキュリティ記述子がプロバイダによってサポートされているかどうかを確認するには、次のコマンドを実行します。

```
nbcertcmd -ecaHealthCheck -serviceUser LocalService
```

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

プロバイダでセキュリティ記述子がサポートされていない場合は、セキュリティ記述子をサポートするプロバイダを使用するか、管理者アカウントを使用して NetBackup サービスを実行する必要があります。

プロバイダを変更するには、証明書を再配備する必要があります。証明書が配備された後は、プロバイダを変更できません。セキュリティ記述子をサポートするプロバイダは、Microsoft ソフトウェアキーストレージプロバイダ、Microsoft Enhanced Cryptographic Provider v1.0、Microsoft Enhanced RSA and AES Cryptographic Provider、Microsoft Strong Cryptographic Provider などです。

PFX ファイルがある場合は、そのファイルを再インポートしてプロバイダを変更できます。

1. Windows 証明書ストアから証明書と秘密鍵を削除します。
2. `certutil` コマンドを使用して `pfx` ファイルをインポートします。

   ```
   C:¥Windows¥System32¥certutil.exe -importPfx -csp provider namepfxfile
   ```

ADCS で配備された証明書の場合、証明書テンプレートからプロバイダを変更し、証明書を再び配備できます。

構成に応じて新しい証明書を要求する際にプロバイダを選択することもできます。

管理者アカウントを使用して NetBackup サービスを実行するには、次のコマンドを実行します。

```
nbserviceusercmd.exe -changeUser
```

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

外部 CA の証明書失効リストについて

外部認証局 (CA) の証明書失効リスト (CRL) には、スケジュールされた有効期限前に外部 CA が無効化して、信頼しないようにする必要があるデジタル証明書のリストが含まれています。

NetBackup は外部 CA の CRL の PEM と DER 形式をサポートしています。

すべての CRL 発行者または外部 CA の CRL は、各ホストに存在する NetBackup CRL キャッシュに格納されています。

安全な通信中に、ECA_CRL_CHECK 構成オプションに基づき、NetBackup CRL キャッシュに存在する CRL を使用して各 NetBackup ホストがピアホストの外部証明書の失効状態を検証します。

p.396 の「NetBackup サーバーとクライアントの ECA_CRL_CHECK」を参照してください。

NetBackup CRL キャッシュは、次のいずれかの CRL ソースを使用して、必要な CRL で更新されます。

ECA_CRL_PATH 構成オプション
: CRL が存在するディレクトリパスを指定する NetBackup 構成オプション (UNIX の bp.conf ファイルまたは Windows レジストリから)。

p.398 の「NetBackup サーバーとクライアントの ECA_CRL_PATH_SYNC_HOURS」を参照してください。

p.405 の「ECA_CRL_PATH にある CRL を使用する方法」を参照してください。

CRL 配布ポイント (CDP)
: ECA_CRL_PATH を指定していない場合、NetBackup はピアホスト証明書の CDP で指定された URL から CRL をダウンロードし、NetBackup CRL キャッシュにその CRL をキャッシュします。

p.406 の「CDP URL にある CRL を使用する方法」を参照してください。

NetBackup は、CDP で指定された HTTP と HTTPS の URL からの CRL のダウンロードをサポートしています。

NetBackup CRL キャッシュには、各 CA (ルートおよび中間 CA を含む) の CRL の最新のコピーのみが含まれています。

bpclntcmd -crl_download サービスは、ECA_CRL_PATH_SYNC_HOURS または ECA_CRL_REFRESH_HOURS オプションで設定された時間の間隔にかかわらず、次のシナリオのホストの通信時に CRL キャッシュを更新します。

- CRL キャッシュ内の CRL の期限が切れたとき
- CRL が CRL ソース (ECA_CRL_PATH または CDP) で利用可能で、CRL キャッシュにない場合

メモ: bpclntcmd -crl_download サービスが CRL キャッシュ内の CRL を更新すると、次の 15 分間は、有効なダウンロードシナリオが発生したとしても、同じ CA の CRL はダウンロードされません。15 分以内に CRL を更新する必要がある場合は、bpclntcmd -crl_download サービスを終了してください。

ECA_CRL_PATH にある CRL を使用する方法

このセクションでは、ECA_CRL_PATH を NetBackup CRL キャッシュの CRL ソースとして使用する方法について説明します。

ECA_CRL_PATH にある CRL を使用するには

1. 外部 CA の CRL がディレクトリに格納され、ディレクトリのパスがホストからアクセスできることを確認します。

   Flex Appliance アプリケーションインスタンスがある場合、証明書ファイルはインスタンスの次のディレクトリに格納されている必要があります:
   /mnt/nbdata/hostcert/crl。

   ホストでの NetBackup のインストールまたはアップグレード中に、外部 CA の構成に必要な CRL の詳細を指定できます。

   インストールまたはアップグレード中に、証明書失効リスト (CRL) の次のいずれかのオプションを選択します。

   - [証明書に定義されている CRL を使用する (Use the CRL defined in the certificate)]: 追加の情報は不要です。
   - [次のパスにある CRL を使用する (Use the CRL at the following path)]: CRL のパスを入力するように求められます。
     [CRL は使用しない (Do not use a CRL)]オプションを使用する場合は、ホストの通信中に CRL を使用してピアホストの証明書は検証されません。

詳しくは、『NetBackup インストールガイド』を参照してください。

2 ECA_CRL_PATH 構成オプションの CRL ディレクトリパスを指定します。

3 ECA_CRL_CHECK 構成オプションが DISABLE 以外の値に設定されていることを確認します。

ホストとの通信時に、外部証明書の失効状態は ECA_CRL_PATH から取得した CRL を含む NetBackup CRL キャッシュを使用して検証されます。

デフォルトでは、キャッシュから取得した CRL は 1 時間ごとに更新されます。時間間隔を変更するには、ECA_CRL_PATH_SYNC_HOURS オプションを別の値に設定します。

ECA_CRL_PATH の CRL で CRL キャッシュを手動で更新するには、nbcertcmd -updateCRLCache コマンドを実行します。

CRL キャッシュから CRL を手動で削除するには、nbcertcmd -cleanupCRLCache コマンドを実行します。

CDP URL にある CRL を使用する方法

このセクションでは、CRL 配布ポイント (CDP) を NetBackup CRL キャッシュの CRL ソースとして使用する方法について説明します。

CDP から CRL を使用するには

1 ECA_CRL_PATH 構成オプションが指定されていないことを確認します。

2 ピアホストの CDP で指定されている URL にホストがアクセスできることを確認します。

3 ECA_CRL_CHECK 構成オプションが DISABLE 以外の値に設定されていることを確認します。

ホストとの通信時に、外部証明書の失効状態は CDP URL から取得した CRL を含む NetBackup CRL キャッシュを使用して検証されます。

デフォルトでは、24 時間ごとに CDP から CRL がダウンロードされ、CRL キャッシュが更新されます。時間間隔を変更するには、ECA_CRL_REFRESH_HOURS 構成オプションに別の値を設定します。

CRL キャッシュから CRL を手動で削除するには、nbcertcmd -cleanupCRLCache コマンドを実行します。

証明書の登録について

NetBackup CA の場合、証明書の配備中に、証明書がプライマリサーバーに自動登録されます。

外部 CA の場合、ECA_DISABLE_AUTO_ENROLLMENT オプションが有効であれば、ホストとの通信中に、証明書がプライマリサーバーに自動登録されます。nbcertcmd -enrollCertificate コマンドを使用して証明書を手動で登録できます。

登録した証明書はホストの通信に使用されます。

p.417 の「証明書の登録を削除」を参照してください。

外部証明書の自動登録について

初めて通信するときに、ホストの外部証明書がプライマリサーバーに自動的に登録されます。証明書の自動登録処理を無効にし、必要に応じて、nbcertcmd -enrollCertificate コマンドを使用して手動で証明書を登録できます。

p.400 の「NetBackup サーバーとクライアントの ECA_DISABLE_AUTO_ENROLLMENT」を参照してください。

通信する双方のホストで自動登録が有効で、外部証明書が構成されている場合、NetBackup は外部証明書の登録を試行します。

外部証明書は、関連付けられているプライマリサーバーに登録されます。このプライマリサーバーに関連付けられているホスト間の以降の通信には、登録された外部証明書が使用されます。

次のシナリオでは、外部証明書は自動的に登録されません。

- NAT クライアントとの通信
  NetBackup での NAT クライアントの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。
- メディアサーバー重複排除 (MSDP) のイメージレプリケーションの一部としてのメディアサーバー間の通信
- NetBackup 管理コンソールとの通信

プライマリサーバーの登録状態の表示について

外部証明書を使用するように NetBackup ホストを構成するには、必要な構成オプションを定義して、ホストの証明書を登録する必要があります。登録された証明書は、ホストと SERVER オプションに存在するプライマリサーバードメイン間の通信に使用されます。

p.411 の「外部 CA が署名した証明書を使用するプライマリサーバーの構成」を参照してください。

p.413 の「インストール後に外部 CA が署名した証明書を使用するための NetBackup ホスト (メディアサーバー、クライアント、クラスタノード) の構成」を参照してください。

nbcertcmd -listEnrollmentStatus コマンドを実行して、登録状態を表示できます。このコマンドは、ECA_CERT_PATH オプションが構成されている証明書のサブジェクト名が一致するレコードのみの一覧を表示します。

次の登録ステータスが表示されます:

- 未登録 (Not enrolled): 外部の証明書はこのプライマリサーバードメインで登録されていません。プライマリサーバーは、SERVER オプションのプライマリサーバーリストに表示されます。
- 更新対象 (To be updated): 外部証明書をこのプライマリサーバードメインに再度登録する必要があります。
- 登録済み (Enrolled): 外部の証明書はプライマリサーバーに登録されています。

p.415 の「リモートホストの外部証明書の登録」を参照してください。

NetBackup Web サーバーで外部証明書を使用するための構成

メモ: プライマリサーバーの証明書を登録する前に、次のトピックの説明に従って、必要な手順を完了していることを確認します。

p.387 の「NetBackup ホスト通信で外部証明書を使用するワークフロー」を参照してください。

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

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

Web サーバーで外部証明書を使用するように構成するには

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

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

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

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

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

  install_path/netbackup/bin/bpclusterutil -freeze

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

UNIX では、次のコマンドを実行します。

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

Windows では、[コントロールパネル]で[サービス]を使用します。

コマンドの場所:

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

UNIX の場合　*install_path*/wmc/bin/install

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

  install_path/netbackup/bin/bpclusterutil -unfreeze

4 次のように NetBackup Messaging Queue Broker (nbmqbroker) サービスを再起動します。

Windows の場合:

Windows のコントロールパネルの[サービス]アプリケーションに移動し、NetBackup Messaging Queue Broker サービスを手動で再起動します。

UNIX の場合:

次のコマンドを実行します。

```
nbmqbroker stop; nbmqbroker start
```

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

Web サーバー用外部証明書のアップデートまたは更新

Web サーバー用に構成された外部証明書をアップデートまたは更新できます。

Web サーバー用外部証明書をアップデートまたは更新するには

1. 最新の外部証明書、一致する秘密鍵、CA バンドルファイルがあることを確認します。
2. 次のコマンドを実行します (クラスタ化されたセットアップでは、このコマンドをアクティブノードで実行します)。

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

Web サーバー用に構成された外部証明書の削除

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

Web サーバー用に構成された外部証明書を削除するには

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

```
configureWebServerCerts -removeExternalCert -nbHost
```

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

     install_path/netbackup/bin/bpclusterutil -freeze

2. NetBackup Web 管理コンソールサービスを再起動します。
   - クラスタ化されたプライマリサーバーのセットアップでは、次のコマンドをアクティブノードで実行してクラスタを解凍します。

     install_path/netbackup/bin/bpclusterutil -unfreeze

3. 次のように NetBackup Messaging Queue Broker (nbmqbroker) サービスを再起動します。

   Windows の場合:

   Windows のコントロールパネルの[サービス]アプリケーションに移動し、NetBackup Messaging Queue Broker サービスを手動で再起動します。

   UNIX の場合:

   次のコマンドを実行します。

```
nbmqbroker stop; nbmqbroker start
```

外部 CA が署名した証明書を使用するプライマリサーバーの構成

NetBackup ホスト ID ベースの証明書は、インストールまたはアップグレード中にプライマリサーバーに配備されます。インストール後に、外部 CA が署名した証明書を使用するプライマリサーバーを構成できます。以下の項目が含まれます。

- 外部証明書構成オプションの定義
  p.388 の「外部 CA が署名した証明書の構成オプション」を参照してください。
- プライマリサーバーのホスト用の外部証明書の登録
  登録された証明書は、ホストと、ホストの SERVER 構成オプションに一覧表示されているプライマリサーバードメイン間の通信に使用されます。

p.416 の「NetBackup Web UI での外部 CA が署名した証明書の表示」を参照してください。

p.425 の「クラスタプライマリサーバーの外部証明書の構成」を参照してください。

重要な注意事項

- NetBackup Web サーバーを構成して、外部 CA が署名した証明書の使用が NetBackup ドメインで有効になっていることを確認します。
  p.408 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。
- NetBackup Web サーバーとプライマリサーバーの外部証明書は、同じルート認証局によって発行されている必要があります。
  この 2 つの認証局が一致しない場合は、NetBackup 管理コンソールと NetBackup Web 管理コンソールサービス (nbwmc サービス) 間の通信が失敗します。
- 外部 CA の証明書失効リスト (CRL) が必要な場所に格納されていることを確認します。
  CRL 配布ポイント (CDP) を使用している場合は、CDP で指定された URL にアクセスできることを確認します。
  p.404 の「外部 CA の証明書失効リストについて」を参照してください。
- サービスユーザー (UNIX の特権のないユーザーと Windows のローカルサービス) を使用してほとんどのデーモンまたはサービスを起動するように NetBackup プライマリサーバーが構成されている場合、サービスユーザーが次の ECA パスにアクセスできるようにする必要があります。
  - ECA_CERT_PATH
  - ECA_PRIVATE_KEY_PATH
  - ECA_TRUST_STORE_PATH
  - ECA_KEY_PASSPHRASEFILE (省略可能)

- ECA_CRL_PATH (省略可能)

p.543 の「NetBackup サービスユーザーのアカウントについて」を参照してください。

サービスユーザーにアクセス権を付与するには、次の手順を実行します。

UNIX の場合、chmod または chown コマンドを使用します。

Windows で、次のコマンドを実行します。

```
install_path¥NetBackup¥bin¥goodies¥nbserviceusercmd.exe -addAcl
ECA path -reason reason
```

外部証明書を使用するようにプライマリサーバーを構成するには

1 外部証明書に固有のパラメータで、プライマリサーバーの NetBackup 構成ファイル (UNIX の bp.conf ファイル、または Windows レジストリ) を更新します。

p.388 の「外部 CA が署名した証明書の構成オプション」を参照してください。

Windows 証明書ストアの場合	nbsetconfig コマンドを使用して次のパラメータを構成します。 ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (省略可能) ■ ECA_CRL_PATH (省略可能) ■ ECA_CRL_PATH_SYNC_HOURS (省略可能) ■ ECA_CRL_REFRESH_HOURS (省略可能) ■ ECA_DR_BKUP_WIN_CERT_STORE (省略可能)

ファイルベース証明書の場合

nbsetconfig コマンドを使用して次のパラメータを構成します。

- ECA_CERT_PATH
- ECA_PRIVATE_KEY_PATH
- ECA_TRUST_STORE_PATH
- ECA_KEY_PASSPHRASEFILE (省略可能)
- ECA_CRL_CHECK (省略可能)
- ECA_CRL_PATH (省略可能)
- ECA_CRL_PATH_SYNC_HOURS (省略可能)
- ECA_CRL_REFRESH_HOURS (省略可能)

メモ: Flex Appliance アプリケーションインスタンスがある場合、証明書ファイルはインスタンスの次のディレクトリに格納されている必要があります。

ECA_CERT_PATH、ECA_PRIVATE_KEY PATH、ECA_TRUST_STORE_PATH: `/mnt/nbdata/hostcert/`

ECA_CRL_PATH: `/mnt/nbdata/hostcert/crl`

2 プライマリサーバーで次のコマンドを実行して、SERVER オプションで定義されているプライマリサーバードメインに外部証明書を登録します。

```
nbcertcmd -enrollCertificate
```

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。

インストール後に外部 CA が署名した証明書を使用するための NetBackup ホスト (メディアサーバー、クライアント、クラスタノード) の構成

NetBackup ホスト (メディアサーバーまたはクライアント) は、インストールまたはアップグレード中に外部証明書を使用するように構成されます。インストール後に構成の実行を選択できます。

このセクションでは、外部証明書を使用するようにホストを構成する方法について説明します。

このセクションに従って、クラスタノードの外部証明書を構成できます。

p.420 の「クラスタプライマリサーバー用の外部証明書の構成について」を参照してください。

構成手順は、次のとおりです。

- 外部証明書構成オプションの定義

p.388 の「外部 CA が署名した証明書の構成オプション」を参照してください。

- 自動登録が有効になっていることの確認 (ECA_DISABLE_AUTO_ENROLLMENT が TRUE に設定されている) またはホストの外部証明書の手動登録
  p.415 の「リモートホストの外部証明書の登録」を参照してください。
  登録された証明書は、ホストと、ホストの SERVER 構成オプションに一覧表示されているプライマリサーバードメイン間の通信に使用されます。

登録した証明書はホストの通信に使用されます。

p.416 の「NetBackup Web UI での外部 CA が署名した証明書の表示」を参照してください。

重要な注意事項

- NetBackup Web サーバーを構成して、外部 CA が署名した証明書の使用が NetBackup ドメインで有効になっていることを確認します。
  p.408 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。
- 他のホストに外部証明書を登録する前に、プライマリサーバーホストに外部証明書を登録することをお勧めします。
  p.411 の「外部 CA が署名した証明書を使用するプライマリサーバーの構成」を参照してください。
- 外部 CA の証明書失効リスト (CRL) が必要な場所に格納されていることを確認します。
  CRL 配布ポイント (CDP) を使用している場合は、CDP で指定された URL にアクセスできることを確認します。
  p.404 の「外部 CA の証明書失効リストについて」を参照してください。

外部証明書を使用するようにホスト (メディアサーバーまたはクライアント) を構成するには

1 ホストで、必要な外部証明書に固有のパラメータを使用して、構成ファイル (nbcl.conf ファイルまたは Windows レジストリ) を更新します。

p.388 の「外部 CA が署名した証明書の構成オプション」を参照してください。

Windows 証明書ストアの場合	nbsetconfig コマンドを使用して次のパラメータを構成します。 ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (省略可能) ■ ECA_CRL_PATH (省略可能) ■ ECA_CRL_PATH_SYNC_HOURS (省略可能) ■ ECA_CRL_REFRESH_HOURS (省略可能) ■ ECA_DR_BKUP_WIN_CERT_STORE (省略可能)

ファイルベース証明書の場合

nbsetconfig コマンドを使用して次のパラメータを構成します。

- ECA_CERT_PATH
- ECA_PRIVATE_KEY_PATH
- ECA_TRUST_STORE_PATH
- ECA_KEY_PASSPHRASEFILE (省略可能)
- ECA_CRL_CHECK_LEVEL (省略可能)
- ECA_CRL_PATH (省略可能)
- ECA_CRL_PATH_SYNC_HOURS (省略可能)
- ECA_CRL_REFRESH_HOURS (省略可能)

メモ: Flex Appliance アプリケーションインスタンスがある場合、証明書ファイルはインスタンスの次のディレクトリに格納されている必要があります。

ECA_CERT_PATH、ECA_PRIVATE_KEY PATH、ECA_TRUST_STORE_PATH: `/mnt/nbdata/hostcert/`

ECA_CRL_PATH: `/mnt/nbdata/hostcert/crl`

2 nbgetconfig コマンドを使用して、ECA_DISABLE_AUTO_ENROLLMENT オプションが TRUE に設定されていることを確認します。これにより、自動登録が有効になっていることを確認できます。

オプションが無効になっており、証明書を手動で登録する場合は、ホストで次のコマンドを実行して、ホストの SERVER 構成オプションに定義されているプライマリサーバードメインに外部証明書を登録します。

```
nbcertcmd -enrollCertificate
```

p.407 の「プライマリサーバーの登録状態の表示について」を参照してください。

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。

リモートホストの外部証明書の登録

このセクションでは、NetBackup ホストの外部証明書をリモートで登録する方法について説明します。この手順により、セキュリティ管理者は、同じホストから複数のリモートホストの外部証明書を登録できます。

リモートホストの外部証明書を登録する (またはリモートホストで登録の同期操作を実行する) には、証明書を登録するサーバーが、リモートホストの SERVER 構成オプションに表示されていることを確認します。

リモートホストの証明書を登録するには

◆ ローカルホストで次のコマンドを実行します。

```
nbcertcmd -enrollCertificate -remoteHost remote_host_name -server
primary_server_name
```

外部証明書は、-server オプションで指定したプライマリサーバーを使用して、指定したリモートホストに登録されます。このプライマリサーバーは、リモートホストの SERVER 構成オプションに記載されている必要があります。

p.388 の「外部 CA が署名した証明書の構成オプション」を参照してください。

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。

NetBackup ドメインがサポートする認証局の表示

NetBackup 管理コンソールと NetBackup Web UI の［マスターサーバー証明書構成 (Master server certificate configuration)］オプションに、NetBackup ドメインがサポートする NetBackup CA、外部 CA、またはその両方の認証局が表示されます。

- NetBackup 管理コンソールで［セキュリティ管理 (Security Management)］、［グローバルセキュリティ設定 (Global Security Settings)］の順に展開して［安全な通信 (Secure Communication)］タブをクリックすると、サポート対象の認証局が表示されます。
- NetBackup Web UI で［グローバルセキュリティ設定 (Global Security Settings)］オプションをクリックすると、サポート対象の認証局が表示されます。

NetBackup Web UI での外部 CA が署名した証明書の表示

NetBackup Web UI の［セキュリティ (Security)］、［証明書 (Certificates)］画面を使用して、ドメイン内のホストに発行される外部証明書のリストを表示できます。

詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

ファイルベースの外部証明書の更新

このセクションでは、NetBackup サービスを再起動せずにファイルベースの外部証明書を更新する方法について説明します。

すべてのサービスが起動した状態で、証明書、秘密鍵、パスフレーズファイルを 1 つずつ置き換えると、その間に証明書と秘密鍵のペアが不一致となり通信が失敗する可能性があります。通信エラーを回避するには、ファイルの不一致が発生したときに NetBackup が使用できるファイルのコピーを作成します。

ファイルベースの外部証明書を更新するには

1. 証明書ファイルのコピーを作成し、.old 拡張子を付けた名前に変更します。

   たとえば、証明書のファイル名が cert.pem の場合、cert.pem.old という名前に変更します。

2. 秘密鍵ファイルのコピーを作成し、.old 拡張子を付けた名前に変更します。
3. 証明書の秘密鍵が暗号化されている場合は、次の手順を実行します。

   パスフレーズファイルのコピーを作成し、.old 拡張子を付けた名前に変更します。

4. 更新された証明書、秘密鍵、パスフレーズファイルで、元の証明書、秘密鍵、パスフレーズファイルを置換します。
5. 更新された証明書でホストの通信が成功したことを確認し、古い証明書ファイルを削除します。

証明書の登録を削除

ホストとの通信時に、証明書を使用しない場合は、特定のプライマリサーバーとの外部証明書の登録を削除できます。

証明書の登録を削除するには

- 次のコマンドを実行します。

  ```
  nbcertcmd -removeEnrollment -server primary_server_name
  ```

NetBackup ドメインでの NetBackup CA の無効化

このセクションでは、ドメイン内のすべてのホストがホストとの通信に外部証明書を使用するように構成されている場合、ドメインで既存の NetBackup CA のサポートを無効にする方法について説明します。

メモ: 環境に NAT クライアントがあり、NetBackup Messaging Broker (nbmqbroker) サービスが有効な場合、外部証明書のみを使用するには、NetBackup CA を無効にした後でサービスの再起動が必要になる場合があります。

NetBackup の NAT の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。

安全に通信できますが通信外部証明書を使用するように構成できないホスト (NetBackup 8.1、8.1.1、または 8.1.2) がある場合、通信エラーを回避するため、NetBackup CA 構成を無効にすることは推奨されません。

ドメイン内の NetBackup CA のサポートを無効にするには

1. ドメイン内のすべてのホストが外部証明書を使用するように構成されていることを確認します。

   p.408 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。

   p.411 の「外部 CA が署名した証明書を使用するプライマリサーバーの構成」を参照してください。

   p.413 の「インストール後に外部 CA が署名した証明書を使用するための NetBackup ホスト (メディアサーバー、クライアント、クラスタノード) の構成」を参照してください。

2. 外部証明書を使用するようにドメイン内の各ホストを構成した後、ドメイン内の各ホスト (メディアサーバーとクライアント) から NetBackup CA のサポートを削除します。

   各ホストで、次のコマンドを所定の順序で実行します。

   - `nbcertcmd -removeCACertificate -fingerPrint NetBackup CA certificate fingerprint`
   - `nbcertcmd -deleteCertificate -hostid` *`host ID of the host`*

3. プライマリサーバーから NetBackup CA サポートを削除します。

   プライマリサーバーで次のコマンドを所定の順序で実行します。

   - `nbcertcmd -removeCACertificate -fingerPrint NetBackup CA certificate fingerprint`
   - `nbcertcmd -deleteCertificate -hostid` *`host ID of the primary server`*

4. ドメイン内のすべてのホスト ID ベースの証明書を無効化します(これはオプションの手順です)。

   p.326 の「ホスト ID ベースの証明書の無効化」を参照してください。

5. Web サーバーから NetBackup CA サポートを削除します。ホストとの通信で NetBackup 証明書を必要としないことを確認します。

   Web サーバー上で次のコマンドを実行します。

   ```
   configureWebServerCerts -removeNBCert
   ```

   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。

6. NetBackup Web 管理コンソール (`nbwmc`) サービスを再起動します。

NetBackup ドメインでの NetBackup CA の有効化

このセクションでは、NetBackup ドメインで、ホストとの通信に NetBackup CA が署名した証明書 (またはホスト ID ベースの証明書) を使用できるようにする方法を説明します。

NetBackup ドメインで NetBackup CA の構成をサポートできるようにするには

1. NetBackup (ホスト ID ベース) 証明書を使用するように、NetBackup Web サーバーを構成します。
   - 次のコマンドを実行します。
     `configureWebServerCerts -addNBCert`
     p.408 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。
   - NetBackup Web 管理コンソール (`nbwmc`) サービスを再起動します。
2. プライマリサーバーで、NetBackup ホスト ID ベースの証明書を配備します。
   p.301 の「ホスト ID ベースの証明書の配備」を参照してください。
3. 各ホストで、NetBackup ホスト ID ベースの証明書を配備します。
   p.301 の「ホスト ID ベースの証明書の配備」を参照してください。

NetBackup ドメインでの外部 CA の無効化

このセクションでは、NetBackup ドメインで外部 CA を無効にする方法について説明します。

外部 CA を無効にするには

1. ドメイン内の各ホストが、NetBackup ホスト ID ベースの証明書を使用するように構成されていることを確認します。
2. ホスト上に存在する構成ファイル (UNIX の `bp.conf` または Windows レジストリ) からすべての外部証明書構成オプションを削除します。
   たとえば、`ECA_CERT_PATH` などです。
   p.422 の「仮想名の外部 CA が署名した証明書の構成オプション」を参照してください。
3. プライマリサーバーから外部 CA サポートを削除します。
   - プライマリサーバー上に存在する構成ファイル (UNIX の `bp.conf` または Windows レジストリ) からすべての外部証明書構成オプションを削除します。
     たとえば、`ECA_CERT_PATH` などです。
     p.422 の「仮想名の外部 CA が署名した証明書の構成オプション」を参照してください。

4 NetBackup データベースからすべての外部証明書エントリを削除します。

次のコマンドを実行します。

```
nbcertcmd -deleteECACertEntry -subject subject name of the certificate
```

5 Web サーバーから外部 CA サポートを削除します。

```
configureWebServerCerts -removeExternalCert
```

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。

6 次のコマンドを使用して証明書の登録を解除します。

```
nbcertcmd -removeEnrollment
```

登録済み外部証明書のサブジェクト名の変更

このセクションでは、すでに登録されているホストの外部証明書のサブジェクト名を変更する方法について説明します。

登録済みの外部証明書のサブジェクト名を変更するには

1 証明書のサブジェクト名を変更します。

2 ホストが複数のプライマリサーバードメインに参加している場合は、すべてのプライマリサーバーに対してこの手順を実行する必要があります。

次のいずれかを実行します。

- 次のコマンドを実行して、証明書を手動で登録します。
  Install_Path/bin/nbcertcmd -enrollCertificate
- 次のコマンドを実行して、既存の登録を削除します。
  Install_Path/bin/nbcertcmd -removeEnrollment

クラスタプライマリサーバー用の外部証明書の構成について

クラスタプライマリサーバーで、信頼できる認証局 (CA) が発行した X.509 証明書を使用できるようになりました。

まず、NetBackup Web サーバーを構成して、外部 CA が署名した証明書の使用を NetBackup ドメインで有効にする必要があります。

その後、ホストとの安全な通信に外部 CA が署名した証明書を使用するように、NetBackup のクラスタプライマリサーバーを構成できます。

p.421 の「クラスタプライマリサーバーに外部証明書を使用するワークフロー」を参照してください。

重要な注意事項

外部証明書を使用するように NetBackup を構成する前に、次の注意事項を確認してください。

- NetBackup 証明書またはホスト ID ベースの証明書は、NetBackup のインストール時にプライマリサーバーに配備されます。インストールの終了後、クラスタプライマリサーバーで外部証明書を手動で構成する必要があります。
- クラスタプライマリサーバーのセットアップでは、各ノードのローカルディスクに存在する各クラスタノードに対して 1 つの外部証明書を構成する必要があります。さらに、クラスタの共有ディスクに存在する仮想名に対して 1 つの証明書を構成する必要があります。
- 仮想名の外部証明書の登録に必要な NetBackup 構成オプション (たとえば、`CLUSTER_ECA_CERT_PATH`) は、`nbcl.conf` ファイルに格納されます。このファイルは共有ディスク上に存在し、各クラスタノードの外部証明書構成オプションは、`bp.conf` ファイルまたは Windows レジストリに格納されます。
- Windows 証明書ストアは、仮想名の外部証明書ソースとしてサポートされていません。クラスタノードの証明書のソースとして使用できます。
- 仮想名の個別の CRL 構成オプションはありません。ノード上の `ECA_CRL_CHECK` 構成オプションに基づき、クラスタノードの証明書失効リスト (CRL)、つまり `ECA_CRL_PATH` または CDP が、通信時にピアホストの証明書の失効状態を確認するために使用されます。したがって、プライマリサーバーの仮想名の外部証明書を使用する前に、CRL の構成オプションを設定する必要があります。
  p.404 の「外部 CA の証明書失効リストについて」を参照してください。

クラスタプライマリサーバーに外部証明書を使用するワークフロー

安全な通信を行うために、NetBackup で外部 CA が署名した証明書を使用するように構成するには、示された順序で次の手順を実行する必要があります。

表 19-13　クラスタ設定で外部証明書を使用するためのワークフロー

手順	処理
1	次の項目について確認します。 ■ 仮想名の証明書が共有ディスク上の適切な場所に配置されている。 ■ クラスタノードの外部証明書がノード上の適切な場所に配置されている。 ■ CRL 構成オプションに基づき、CRL がノード上の必要な場所に配置され、アクセス可能である。 p.404 の「外部 CA の証明書失効リストについて」を参照してください。
2	各クラスタノードで、NetBackup ソフトウェアをインストールするか、既存のソフトウェアをアップグレードします。
3	NetBackup Web サーバーを構成し、NetBackup ドメインで外部証明書を使用できるようにします。 p.408 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。
4	仮想名と各クラスタノードの外部証明書を構成します。 p.425 の「クラスタプライマリサーバーの外部証明書の構成」を参照してください。

仮想名の外部 CA が署名した証明書の構成オプション

NetBackup のクラスタプライマリサーバーで、ホストの通信に外部 CA が署名した証明書を使用するように構成するには、`nbcl.conf` ファイルで特定の構成オプションを定義する必要があります。

クラスタ化されたプライマリサーバーの CLUSTER_ECA_CERT_PATH

`CLUSTER_ECA_CERT_PATH` オプションは、クラスタ化されたプライマリサーバーに固有のオプションです。仮想名の外部 CA が署名した証明書のパスを指定します。

表 19-14　CLUSTER_ECA_CERT_PATH の情報

使用方法	説明
使用する場所	クラスタ化されたプライマリサーバー上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 `CLUSTER_ECA_CERT_PATH = Path to the certificate of the virtual identity`
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。

クラスタ化されたプライマリサーバーの CLUSTER_ECA_TRUST_STORE_PATH

CLUSTER_ECA_TRUST_STORE_PATH オプションは、クラスタ化されたプライマリサーバーに固有のオプションです。PEM 形式の信頼できるすべてのルート CA 証明書を含む証明書バンドルファイルへのファイルパスを指定します。

表 19-15 CLUSTER_ECA_TRUST_STORE_PATH の情報

使用方法	説明
使用する場所	クラスタ化されたプライマリサーバー上。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 `CLUSTER_ECA_TRUST_STORE_PATH = Path to the external CA certificate`
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。

クラスタ化されたプライマリサーバーの CLUSTER_ECA_PRIVATE_KEY_PATH

CLUSTER_ECA_PRIVATE_KEY_PATH オプションは、クラスタ化されたプライマリサーバーに固有のオプションです。仮想名の外部 CA が署名した証明書の秘密鍵のパスを指定します。

仮想名証明書の秘密鍵が暗号化されている場合は、
CLUSTER_ECA_KEY_PASSPHRASEFILE オプションを定義する必要があります。

p.424 の「クラスタ化されたプライマリサーバーの CLUSTER_ECA_KEY_PASSPHRASEFILE」を参照してください。

表 19-16 CLUSTER_ECA_PRIVATE_KEY_PATH の情報

使用方法	説明
使用する場所	クラスタ化されたプライマリサーバー上。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 CLUSTER_ECA_PRIVATE_KEY_PATH = *Path to the private key of the external certificate*
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。

クラスタ化されたプライマリサーバーの CLUSTER_ECA_KEY_PASSPHRASEFILE

CLUSTER_ECA_KEY_PASSPHRASEFILE オプションは、クラスタ化されたプライマリサーバーに固有のオプションです。仮想名証明書の秘密鍵のパスフレーズが格納されているテキストファイルのパスを指定します。

CLUSTER_ECA_KEY_PASSPHRASEFILE は省略可能です。仮想名証明書の秘密鍵が暗号化されている場合は、このオプションを定義する必要があります。

p.423 の「クラスタ化されたプライマリサーバーの CLUSTER_ECA_PRIVATE_KEY_PATH」を参照してください。

表 19-17 CLUSTER_ECA_KEY_PASSPHRASEFILE の情報

使用方法	説明
使用する場所	クラスタ化されたプライマリサーバー上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 `CLUSTER_ECA_KEY_PASSPHRASE_FILE = Path to the passphrase file`
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。

クラスタプライマリサーバーの外部証明書の構成

このセクションでは、クラスタプライマリサーバーに外部 CA が署名した証明書を構成する方法について説明します。登録した証明書はホストの通信に使用されます。

要件

- NetBackup Web サーバーを構成して、外部 CA が署名した証明書の使用が NetBackup ドメインで有効になっていることを確認します。
  p.408 の「NetBackup Web サーバーで外部証明書を使用するための構成」を参照してください。
- NetBackup Web サーバーと仮想名の外部証明書が、同じ認証局から発行されていることを確認します。
  この 2 つの認証局が一致しない場合は、NetBackup 管理コンソールと NetBackup Web 管理コンソールサービス (nbwmc サービス) 間の通信が失敗します。

外部証明書をクラスタプライマリサーバーに登録するには

1 外部証明書構成オプションで、共有ディスク上に存在する NetBackup 構成ファイル (nbcl.conf) を更新します。

p.422 の「仮想名の外部 CA が署名した証明書の構成オプション」を参照してください。

nbsetconfig コマンドを使用して、次のオプションを構成します。

- CLUSTER_ECA_CERT_PATH
- CLUSTER_ECA_TRUST_STORE_PATH
- CLUSTER_ECA_PRIVATE_KEY_PATH
- CLUSTER_ECA_KEY_PASSPHRASEFILE (省略可能)

各ノードの証明書失効リスト (CRL) 構成オプションを構成する必要があります。

p.404 の「外部 CA の証明書失効リストについて」を参照してください。

2 プライマリサーバーで次のコマンドを実行します。

```
nbcertcmd -enrollCertificate -cluster
```

登録された証明書は、アクティブノードと、ホストの SERVER 構成オプションに一覧表示されているプライマリサーバードメイン間の通信に使用されます。

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。

3 各クラスタノードで外部証明書を構成します。

p.413 の「インストール後に外部 CA が署名した証明書を使用するための NetBackup ホスト (メディアサーバー、クライアント、クラスタノード) の構成」を参照してください。

20

キーと証明書の再生成

この章では以下の項目について説明しています。

キーと証明書の再生成について

キーと証明書の一部は、NetBackup サービスを再起動するだけで再作成できます。キーまたは証明書に関連するエラーが発生した場合は、ベストプラクティスとして、NetBackup サービスを再起動し、キーまたは証明書が再作成されるかどうかを確認します。キーまたは証明書が作成されない場合は、次のセクションに記載されている手順に進みます。

NetBackup 認証ブローカーのキーと証明書の再生成

次の手順に従って、NetBackup 認証ブローカーの以下を再生成します。

- プライマリサーバーとメディアサーバーの公開鍵と秘密鍵
- メディアサーバーとクライアントの証明書

NetBackup 認証ブローカーのキーと証明書を再生成するには

1. NetBackup 認証サービスを再起動します。サービスが実行中であることを確認します。
2. 次のコマンドを実行します。

   ```
   bpnbaz -ConfigureAuth
   ```

   プロンプトに y と入力します。

   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。
3. すべての NetBackup サービスを再起動します。サービスを再起動する前に、ジョブが実行されていないことを確認します。

   サービスの再起動について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

ホスト ID のキーと証明書の再生成

プライマリサーバー、メディアサーバー、クライアントでホスト ID の公開鍵、秘密鍵、証明書を再生成するには:

- ホストの鍵ペアを変更します。
  鍵ペアの変更を行うと、新しいホスト ID ベースとホスト名ベースの両方の証明書が生成されます。
  p.316 の「ホストの鍵ペアの変更」を参照してください。

Web サービスのキーと証明書の再生成

次の手順に従って、プライマリサーバーで Web サービスの公開鍵と証明書を再生成します。

Web サービスのキーと証明書を再生成するには

1. セキュリティ証明書を生成します。次のコマンドを実行します。
   - Windows

     ```
     set WEBSVC_PASSWORD=<Password of User>
     ```

```
nbcertconfig -t -user <User Name>
```

- UNIX

```
export WEBSVC_PASSWORD=<Password of User>
nbcertconfig -t -user <User Name>
```

2 Web サービスのユーザーと Web サービスについて NetBackup 認証サービスを構成します。次のコマンドを実行します。

```
nbcertconfig -u -user <username>
```

```
nbcertconfig -m -user <username>
```

3 NetBackup 認証サービスを再起動します。

nbcertservice のキーと証明書の再生成

次の手順に従って、プライマリサーバーで nbcertservice のキーと証明書を再生成します。

nbcertservice のキーと証明書を再生成するには

1 ユーザー名を含む古いフォルダを削除します。

2 セキュリティ証明書を生成します。次のコマンドを実行します。

- Windows

```
set WEBSVC_PASSWORD=<Password of User>
nbcertconfig -u -user <User Name>
```

- UNIX

```
export WEBSVC_PASSWORD=<Password of User>
nbcertconfig -u -user <User Name>
```

tomcat のキーと証明書の再生成

次の手順に従って、プライマリサーバーで tomcat の公開鍵、秘密鍵、証明書を再生成します。

メモ: jkskey は、tomcat によって使われるキーストアを復号するキーであり、カタログバックアップの一部としてバックアップされます。再生成する必要はありません。

---

tomcat のキーと証明書を再生成するには

1 セキュリティ証明書を生成します。次のコマンドを実行します。

- Windows

```
set WEBSVC_PASSWORD=<Password of User>
nbcertconfig -t -user <User Name>
```

- UNIX

```
export WEBSVC_PASSWORD=<Password of User>
nbcertconfig -t -user <User Name>
```

2 tomcatcreds フォルダに、keystore と credentials ファイルとは別のその他のファイルを再生成します。次のコマンドを実行します。

- Windows

```
c:¥Program
Files¥Veritas¥NetBackup¥wmc¥bin¥install>configurecerts.bat
```

- UNIX

```
/usr/openv/wmc/bin/install/configurecerts
```

JWT キーの再生成

プライマリサーバーで JWT の公開鍵と秘密鍵を再生成するには:

- NetBackup Web UIを閉じ、すべての NetBackup サービスを再起動します。
  サービスの再起動について詳しくは『NetBackup 管理者ガイド Vol.1』を参照してください。

NetBackup ゲートウェイ証明書の再生成

プライマリサーバーで nbgateway 証明書を再生成するには:

- すべての NetBackup サービスを再起動します。
  サービスの再起動について詳しくは『NetBackup 管理者ガイド Vol.1』を参照してください。

Web トラストストア証明書の再生成

プライマリサーバーとメディアサーバーで Web トラストストア証明書を再生成するには、次のコマンドを実行します。

```
nbcertcmd -getCACertificate
```

プロンプトに y と入力します。

nbcertcmd 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。

VMware vCenter プラグイン証明書の再生成

次の手順に従って、プライマリサーバーで vCenter プラグイン証明書を再生成します。

VMware vCenter プラグイン証明書を再生成するには

1. 既存の証明書をリストし、既存のエントリの無効な証明書を識別します。次のコマンドを実行します。

   - Windows

     ```
     C:¥Program
     Files¥Veritas¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat
     -list
     ```

   - UNIX

     ```
     /usr/openv/wmc/bin/install/manageClientCerts -list
     ```

2. 無効な証明書を削除します。次のコマンドを実行します。

   - Windows

     ```
     C:¥Program
     Files¥Veritas¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat
     -delete
     ```

   - UNIX

     ```
     /usr/openv/wmc/bin/install/manageClientCerts -delete
     ```

3. 新しい証明書を生成します。次のコマンドを実行します。

   - Windows

     ```
     C:¥Program
     Files¥Veritas¥NetBackup¥wmc¥bin¥install¥manageClientCerts.bat
     -create <master_server_name>
     ```

   - UNIX

     ```
     /usr/openv/wmc/bin/install/manageClientCerts -create
     <master_server_name>
     ```

4. 新しく作成された証明書を vCenter プラグインに登録します。

   詳しくは『VMware vCenter の NetBackup プラグインガイド』を参照してください。

NetBackup 管理者コンソールのセッション証明書の再生成

プライマリサーバーでセッション証明書を再生成するには:

- NetBackup 管理者コンソールを閉じ、すべての NetBackup サービスを再起動します。
  サービスの再起動について詳しくは『NetBackup 管理者ガイド Vol.1』を参照してください。

NetBackup 暗号化キーファイルの再生成

NetBackup 暗号化キーファイルを再生成するには、次のコマンドを実行します。

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

パスフレーズを入力するプロンプトが表示されたら、最初に保存したパスフレーズを入力します。

キーファイルについて詳しくはp.446 の「クライアントでの暗号化鍵ファイルの作成について」を参照してください。を参照してください。

bpkeyutil を使用してこのタスクを実行するには、『NetBackup コマンドリファレンスガイド』を参照してください。

3

格納データの暗号化

21

格納データの暗号化セキュリティ

この章では以下の項目について説明しています。

格納データの暗号化に関する用語

次の表では、格納データの暗号化に関する用語について説明します。

表 21-1　　格納データの暗号化に関する用語

用語	説明
AES (Advanced Encryption Standard)	DES に代わる同期暗号化アルゴリズムを指定します。
非同期暗号化	公開鍵と秘密鍵の両方を使用する暗号化アルゴリズムが含まれます。
DES (Data Encryption Standard)	1970 年代から 1998 年までのデータ同期暗号化の一般的な規格を指定します。

用語	説明
初期化ベクター	暗号化アルゴリズムの事前準備に使われるシード値を指定します。この事前準備は、複数のデータファイルの暗号化に同じ鍵を使用する場合に現れるパターンを、分かりにくくするために行われます。これらのファイルは同じパターンで始まります。
公開鍵暗号化	非同期暗号化を使います。
同期暗号化	暗号化と復号化の両方に同じ鍵を使用する暗号化アルゴリズムが含まれます。鍵のサイズが同じ場合、同期暗号化は非同期暗号化よりも高速で安全です。

格納データの暗号化に関する注意事項

次の表では、格納データの暗号化に関する制限事項について説明します。

表 21-2　　格納データの暗号化に関する制限事項

制限事項	説明
データの暗号化によるコンピュータのパフォーマンスへの影響	データ圧縮アルゴリズムと同様、暗号化アルゴリズムでは CPU に高い負荷がかかります。コンピュータのハードウェア (専用または共有のいずれか) を追加せずにデータを圧縮すると、コンピュータと NetBackup のパフォーマンスに影響します。
データの圧縮はデータの暗号化より先に実行する必要がある	データの圧縮アルゴリズムでは、データを圧縮するためにデータのパターンが検索されます。暗号化アルゴリズムでは、データにスクランブルがかけられ、パターンが削除されます。このため、データの圧縮を行う場合はデータの暗号化手順の前に行う必要があります。
暗号化アルゴリズムの選択	多くの暗号化アルゴリズムおよび関連する鍵のサイズがあります。データの暗号化には、どれを使用すればよいでしょうか。AES (Advanced Encryption Standard) はデータの暗号化規格であり、128、192 または 256 ビットの暗号化鍵がサポートされます。
推奨される鍵のサイズ	有効な最大の鍵サイズを選択してください。通常、鍵のサイズが大きいと、鍵サイズが小さい場合よりもデータをより安全に、長期間保護できます。AES は最良の選択の 1 つです。3 つの鍵長 (128、192、256 ビット) がすべてサポートされているため、安全であると考えられています。

制限事項	説明
暗号化ソリューションの FIPS 認定	米国政府による使用には FIPS 認定が必要ですが、暗号化ソリューションを評価する唯一の条件にしないでください。 次に示す他の事項も考慮して決定する必要があります。 ■ FIPS 認定は、名前の付いた製品にのみ適用されます。さらに、製品の使用が、製品の評価時に提示される「FIPS Security Policy」文書に適合する場合にのみ適用されます。製品の将来のバージョンおよび標準外の使用については、検証の認定が適用されない可能性があります。 ■ AES のようなアルゴリズムのセキュリティ保護は、その動作の難解さによるものではありません。セキュリティ保護は、不明な暗号化鍵の推測の困難さによって行われます。何年もの精密な調査と専門家による評価によって、AES の実装は十分なものになりました。実際に、AES に対して、特定の鍵とデータセットを入力するテストが行われ、予測される出力が検証されています。 ■ データの暗号化は自動車のセキュリティによく似ています。問題の多くは鍵の消失または置き間違いに関連するもので、ロックの異常に関連する問題ではありません。 ■ 誤用によって問題が発生する可能性が高いため、暗号化製品の操作性も考慮の対象にする必要があります。 操作性の考慮事項には次のものがあります。 ■ 暗号化の製品との統合 ■ 暗号化のビジネスプロセスとの統合 ■ 暗号化鍵の適切な粒度 ■ リカバリの可能性
暗号化鍵の適切な粒度	暗号化鍵の適切な粒度は、家のセキュリティを例に使用すると最も分かりやすくなります。家の鍵が 1 つだけの場合は便利です。車庫、玄関口、裏口すべてに同じ鍵を使用して入ることができます。このセキュリティは、鍵の安全性が低下する (たとえば、鍵が盗まれる) までは効果的です。鍵の安全性が低下した場合は、この鍵を使用するすべてのロックを取り替える必要があります。極端な例では、家のすべての引き出しと戸棚に対してそれぞれの鍵を持っている人もいます。この場合、鍵を紛失しても 1 つのロックを取り替えるだけで済みます。 適切な解決方法は、これらの 2 つの例の中間にあります。ビジネスプロセスの観点から、安全性の低下した鍵または消失した鍵に対する耐性を理解する必要があります。鍵を消失した場合は、その鍵で暗号化されたすべてのデータが失われます。鍵の安全性が低下した場合は、その鍵で暗号化されたすべてのデータを復号化し、再び暗号化してセキュリティ保護する必要があります。

格納データの暗号化の宛先形式

格納データの暗号化には、次の宛先形式を利用できます。

■ クライアント側の暗号化

p.438 の「NetBackup クライアントの暗号化について」を参照してください。

- MSDP の暗号化
『NetBackup Deduplication ガイド』の「MSDP の暗号化について」を参照してください。
- テープドライブの暗号化 - NetBackup でテープの暗号化を有効にするには、ボリュームプール名の接頭辞に ENCR_ を使用する必要があります。
- クラウドの暗号化
『NetBackup クラウド管理者ガイド』の「クラウドストレージのデータ暗号化について」を参照してください。
- Advanced Disk - NetBackup で AdvancedDisk の暗号化を有効にするには、ディスクプール名の接頭辞に ENCR_ を使用する必要があります。

暗号化セキュリティについて考慮する際の質問

暗号化のセキュリティについて考慮する前に、次の質問について考えておく必要があります。

答えは、ユーザー固有の暗号化の要件によって次のように異なります。

- どのようにして最適な暗号化を選択するか。
- なぜ暗号化セキュリティを使用するのか。
- 可能性のある内部の攻撃に対してどのような保護が必要なのか。
- 可能性のある外部の攻撃に対してどのような保護が必要なのか。
- どの領域の NetBackup を暗号化セキュリティで保護するのか。
- 暗号化セキュリティの動作を示す NetBackup アーキテクチャの図を作成する必要があるか。
- どのような暗号化セキュリティの配置ユースケースを採用するか。

暗号化オプションの比較

次の NetBackup オプションは、格納データの暗号化に関するものです。

- 標準暗号化を使用した NetBackup クライアントの暗号化
- レガシー暗号化を使用した NetBackup クライアントの暗号化
- サードパーティの暗号化装置とハードウェアデバイス

次の表は利用可能な暗号化オプションとそれぞれの長所と短所を示します。

表 21-3 暗号化オプションの比較

暗号化オプション	長所	短所
クライアントの暗号化、標準暗号化 p.443 の「クライアントでの標準暗号化の構成」を参照してください。	■ 暗号化キーはクライアントコンピュータに存在し、NetBackup 管理者によって制御されない ■ NetBackup プライマリサーバーおよびメディアサーバーに影響を与えずに配置可能 ■ クライアントごとに配置可能	■ クライアントの暗号化キーは、各クライアントが一意の暗号化キーと個別の暗号化キーを持つ必要のある環境には適さない。 ■ クライアント上で実行される暗号化および圧縮は、クライアントのパフォーマンスに影響を与える可能性がある。
クライアントの暗号化、レガシー暗号化 p.450 の「クライアントでのレガシー暗号化の構成」を参照してください。	長所は、標準暗号化を使用したクライアントの暗号化と同じ。	短所は、標準暗号化を使用したクライアントの暗号化と同じ。
サードパーティの暗号化装置とハードウェアデバイス	■ ハードウェアが追加されるため、パフォーマンスへの影響がほとんど、またはまったくない。 ■ 通常、NIST FIPS 140 で認定されている。	■ NetBackup 互換性ラボでは、これらのソリューションの一部がテストされている。保証または廃棄に対するテストは行われていない。また、特定のソリューションに対するテストも行われていない。このテストでは、基本的な機能が、特定のバージョンの NetBackup での使用に対して検証されている。 ■ NetBackup 構成、操作または診断が密接に統合されていない。 ■ 装置またはデバイスごとにディザスタリカバリのシナリオが提供されている。

NetBackup クライアントの暗号化について

NetBackup クライアントの暗号化オプションは次の場合に最適です。

- クライアントが圧縮と暗号化の際の CPU 負荷を処理できる場合
- クライアントでデータの暗号化鍵の制御を保持する場合
- NetBackup と暗号化をできるだけ密接に統合する必要がある場合
- ユーザーごとに暗号化が必要な場合

暗号化セキュリティのインストール前提条件

暗号化バックアップには、NetBackup サーバーおよびクライアントのインストールに含まれる NetBackup Encryption ソフトウェアが必要です。暗号化を使うためには、有効なラ

イセンスが必要です。NetBackup のライセンスの管理について詳しくは、『NetBackup 管理者ガイド Vol. I』を参照してください。

『NetBackup 管理者ガイド Vol. 1』

NetBackup Encryption の構成が可能なプラットフォームのリストについては、『NetBackup リリースノート』を参照してください。

暗号化を使用したバックアップの実行について

次のようにして、暗号化を使用したバックアップを実行できます。

- バックアップの暗号化の選択
  p.439 の「バックアップの暗号化の選択について」を参照してください。
- 標準暗号化を使用したバックアップ処理
  p.440 の「標準暗号化を使用したバックアップ処理」を参照してください。
- レガシー暗号化を使用したバックアップ処理
  p.440 の「レガシー暗号化を使用したバックアップ処理」を参照してください。

バックアップの暗号化の選択について

バックアップを開始すると、サーバーは、バックアップを暗号化する必要があるかどうかをポリシー属性によって判別します。その後、サーバーは、クライアント上で bpcd に接続してバックアップを開始し、バックアップ要求で暗号化ポリシー属性を渡します。

クライアントは、次のようにして、暗号化ポリシー属性をクライアントの構成の CRYPT_OPTION と比較します。

- ポリシー属性が yes で、CRYPT_OPTION が REQUIRED または ALLOWED である場合、クライアントは暗号化されたバックアップを実行します。
- ポリシー属性が yes で、CRYPT_OPTION が DENIED である場合、クライアントはバックアップを実行しません。
- ポリシー属性が no で、CRYPT_OPTION が ALLOWED または DENIED である場合、クライアントは暗号化されていないバックアップを実行します。
- ポリシー属性が no で、CRYPT_OPTION が REQUIRED である場合、クライアントはバックアップを実行しません。

次の表に、それぞれの状況で実行されるバックアップ形式を示します。

表 21-4　実行されるバックアップ形式

CRYPT_OPTION	暗号化ポリシー属性あり	暗号化ポリシー属性なし
REQUIRED	暗号化する	なし
ALLOWED	暗号化する	暗号化しない

CRYPT_OPTION	暗号化ポリシー属性あり	暗号化ポリシー属性なし
DENIED	なし	暗号化しない

p.440 の「標準暗号化を使用したバックアップ処理」を参照してください。

p.441 の「NetBackup 標準暗号化を使用したリストア処理」を参照してください。

p.440 の「レガシー暗号化を使用したバックアップ処理」を参照してください。

p.442 の「NetBackup レガシー暗号化を使用したリストア処理」を参照してください。

標準暗号化を使用したバックアップ処理

標準バックアップを暗号化する場合の前提条件は、次のとおりです。

- **メモ:** NetBackup 7.5 以降のバージョンでは、暗号化ソフトウェアは、NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

  鍵ファイルが存在している必要があります。サーバーまたはクライアントから `bpkeyutil` コマンドを実行すると、鍵ファイルが作成されます。

- クライアントが含まれる NetBackup ポリシーで、暗号化属性が選択されている必要があります。

前提条件が満たされると、次のようにバックアップが実行されます。

- クライアントは、鍵ファイルから最新の鍵を取得します。

  バックアップされる各ファイルについて、次の処理が実行されます。

  - クライアントは、暗号化 `tar` ヘッダーを作成します。ヘッダーには、NetBackup によって暗号化に使用された鍵および暗号のチェックサムが含まれます。tar
  - クライアントは、CRYPT_CIPHER 構成エントリで定義された暗号を使用して、鍵で暗号化されたファイルデータを書き込みます。(デフォルトの暗号は AES-128-CFB です。)

  メモ: ファイルデータだけが暗号化されます。ファイル名および属性は暗号化されません。

- サーバー上のバックアップイメージには、バックアップが暗号化されているかどうかを示すフラグが含まれます。

レガシー暗号化を使用したバックアップ処理

レガシーバックアップを暗号化する場合の前提条件は、次のとおりです。

- 暗号化ソフトウェアには、次のように適切な DES ライブラリが含まれる必要があります。
  - 40 ビット DES 暗号化の場合、DES ライブラリは、suffix です。suffix は 、または で、クライアントプラットフォームによって異なります。libvdes40.sosldll
  - 56 ビット DES 暗号化の場合、DES ライブラリは、`libvdes56.suffix` です。suffix は `so`、`sl` または `dll` で、クライアントプラットフォームによって異なります。

  メモ: 暗号化ソフトウェアは、NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

- 鍵ファイルは、CRYPT_KEYFILE 構成オプションで指定したとおりに存在する必要があります。サーバーの場合は `bpinst` コマンド、クライアントの場合は `bpkeyfile` コマンドを実行して NetBackup パスフレーズを指定した場合に、鍵ファイルが作成されます。
- クライアントが含まれる NetBackup ポリシーで、暗号化属性を選択する必要があります。

前提条件が満たされ、バックアップが暗号化される場合に、次の操作が行われます。

- クライアントは、鍵ファイルから最新のデータを取得し、現在の時間 (バックアップ時間) と結合して DES 鍵を生成します。40 ビット DES の場合、鍵の 16 ビットは常に 0 (ゼロ) に設定されます。

  各バックアップファイルについて、次の処理が実行されます。
  - クライアントは、暗号化 `tar` ヘッダーを作成します。ヘッダーには、NetBackup によって暗号化に使用された DES のチェックサムが含まれます。tar
  - クライアントは、DES 鍵で暗号化されたファイルデータを書き込みます。ファイルデータのみが暗号化されます。ファイル名および属性は暗号化されません。
- サーバーは、クライアントからファイル名、属性およびデータを読み込んで、サーバー上のバックアップイメージにそれらを書き込みます。サーバーは、データの暗号化または復号化を行いません。サーバー上のバックアップイメージには、バックアップ時間およびバックアップが暗号化されているかどうかを示すフラグが含まれます。

NetBackup 標準暗号化を使用したリストア処理

標準暗号化が使用されたバックアップをリストアする場合の前提条件は、次のとおりです。

- 暗号化ソフトウェアは、クライアント上にコピーする必要があります。

メモ: 暗号化ソフトウェアは、NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

- 鍵ファイルが存在している必要があります。サーバーまたはクライアントから コマンドを実行すると、鍵ファイルが作成されます。bpkeyutil

リストアが実行されると、サーバーはバックアップが暗号化されているかどうかをバックアップイメージによって判別します。その後、サーバーは、クライアント上の bpcd に接続してリストアを開始します。サーバーは、リストア要求の暗号化フラグをクライアントに送信します。

バックアップが正しく実行された場合、リストアは次のように行われます。

- サーバーは、リストアされるクライアントにファイル名、属性および暗号化されたファイルデータを送信します。
- クライアントは、暗号化 tar ヘッダーを読み込むと、ヘッダーのチェックサムと鍵ファイル内の鍵のチェックサムを比較します。1 つの鍵のチェックサムがヘッダーのチェックサムと一致する場合、NetBackup では鍵を使用してファイルデータが復号化されます。ヘッダーに定義されている暗号が使用されます。
- 鍵および暗号が利用可能な場合、ファイルは復号化され、リストアされます。鍵または暗号が利用できない場合、ファイルはリストアされずに、エラーメッセージが生成されます。

NetBackup レガシー暗号化を使用したリストア処理

レガシー暗号化が使用されたバックアップをリストアする場合の前提条件は、次のとおりです。

- レガシー暗号化ソフトウェアは、クライアント上にコピーする必要があります。

メモ: 暗号化ソフトウェアは、NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

- 暗号化ソフトウェアには、40 ビット DES ライブラリが含まれる必要があります。40 ビット DES ライブラリの名前は、libvdes40.suffix です。suffix は so、sl、または dll で、クライアントプラットフォームによって異なります。
- CRYPT_STRENGTH 構成オプションが DES_56 に設定されている場合、暗号化ソフトウェアには 56 ビット DES ライブラリが含まれている必要があります。56 ビット DES ライブラリの名前は、libvdes56.suffix です。suffix は so、sl、または dll で、クライアントプラットフォームによって異なります。
- 鍵ファイルは、CRYPT_KEYFILE 構成オプションで指定したとおりに存在する必要があります。サーバーの場合は bpinst コマンド、クライアントの場合は bpkeyfile コマンドを実行して NetBackup パスフレーズを指定した場合に、鍵ファイルが作成されます。

サーバーは、バックアップが暗号化されているかどうかをバックアップイメージによって判別します。その後、サーバーは、クライアント上の bpcd に接続してリストアを開始します。サーバーは、リストア要求のバックアップイメージから暗号化フラグおよびバックアップ時間をクライアントに送信します。

前提条件が満たされると、次の操作が行われます。

- サーバーは、リストアされるクライアントにファイル名、属性および暗号化されたファイルデータを送信します。
- クライアントは、鍵ファイルのデータを取得し、バックアップ時間と結合して、1 つ以上の 40 ビット DES 鍵を生成します。56 ビット DES ライブラリが利用可能な場合、クライアントは、1 つ以上の 56 ビット DES 鍵も生成します。
- クライアントは、暗号化 tar ヘッダーを読み込むと、ヘッダーのチェックサムと DES 鍵のチェックサムを比較します。DES 鍵のチェックサムがヘッダーのチェックサムと一致する場合、NetBackup では DES 鍵を使用してファイルデータが復号化されます。

DES 鍵が利用可能な場合、ファイルは復号化され、リストアされます。DES 鍵が利用できない場合、ファイルはリストアされずに、エラーメッセージが生成されます。

クライアントでの標準暗号化の構成

このトピックでは NetBackup 標準暗号化を構成する方法について説明します。

次の構成オプションは、UNIX クライアント上の bp.conf ファイル、または Windows クライアント上のレジストリ内に存在します。

構成オプションは次のとおりです。

- CRYPT_OPTION
- CRYPT_KIND
- CRYPT_CIPHER

また、NetBackup 管理コンソールを使用して、サーバーからオプションを構成することもできます。これらのオプションは、[クライアントプロパティ (Client Properties)]ダイアログボックスの[暗号化 (Encryption)]タブに表示されます。

詳しくは『NetBackup 管理者ガイド Vol. 1』を参照してください。

標準暗号化の構成オプションの管理

次の表に、NetBackup クライアントの標準暗号化に関連する 3 つの構成オプションを示します。

これらのオプションが、クライアントに適切な値に設定されていることを確認します。

表 21-5 暗号化に関連する 3 つの構成オプション

オプション	値	説明
CRYPT_OPTION = *option*		NetBackup クライアントに、暗号化オプションを定義します。*option* に指定可能な値は、次のとおりです。
	denied|DENIED	クライアントが暗号化されたバックアップを許可しないように設定します。サーバーが暗号化されたバックアップを要求すると、エラーであると判断されます。
	allowed|ALLOWED	(デフォルト値) クライアントが暗号化されたバックアップまたは暗号化されないバックアップを許可するように指定します。
	required|REQUIRED	クライアントが暗号化されたバックアップを要求するように設定します。サーバーが暗号化されないバックアップを要求すると、エラーであると判断されます。
CRYPT_KIND = *kind*		NetBackup クライアントに、暗号化の種類を定義します。*kind* には、次のオプション値いずれかを設定できます。
	NONE	標準暗号化またはレガシー暗号化のどちらも、クライアント上では構成されません。
	STANDARD	標準の暗号に基づき、128 ビット暗号化または 256 ビット暗号化を使用するように指定します。このオプションは、標準暗号化をクライアント上で構成する場合のデフォルト値です。
	LEGACY	40 ビット DES または 56 ビット DES 暗号化のレガシー暗号化を使用するように指定します。
CRYPT_CIPHER = *cipher*		使用する暗号の形式を定義します。これは、次のオプション値のいずれかに設定できます。
	AES-128-CFB	128 ビット AES。これはデフォルト値です。
	BF-CFB	128 ビット Blowfish
	DES-EDE-CFB	2 つの鍵の Triple DES
	AES-256-CFB	256 ビット AES

NetBackup 暗号化鍵ファイルの管理

このトピックは NetBackup 暗号化鍵ファイルを管理する方法を記述します。

メモ: クラスタ内のすべてのノードで同じ鍵ファイルを使用する必要があります。

bpkeyutil コマンドを実行すると、NetBackup Encryption クライアント上に暗号を使用した暗号化鍵ファイルおよびパスフレーズが設定されます。

- Windows クライアントの場合、コマンドのフルパスは次のとおりです。

  install_path¥NetBackup¥bin¥bpkeyutil

- UNIX クライアントの場合、コマンドのフルパスは次のとおりです。

  /usr/openv/netbackup/bin/bpkeyutil

クライアントのパスフレーズを追加するためのプロンプトが表示されます。

NetBackup では、指定したパスフレーズを使用して、鍵ファイルが次のように作成されます。

- NetBackup は、次の 2 つのアルゴリズムを組み合わせて、パスフレーズから 256 ビット鍵を作成します。
  - セキュアハッシュアルゴリズム (SHA1)
  - メッセージダイジェストアルゴリズム (MD5)
- NetBackup は NetBackup の秘密鍵と 128 ビット AES アルゴリズムを使用して、鍵を暗号化します。
- この鍵は、クライアント上の鍵ファイルに格納されます。
- 実行時、NetBackup は鍵およびランダム初期化ベクターを使用して、クライアントデータを暗号化します。初期化ベクターは、バックアップイメージのヘッダーに格納されます。

以前のパスフレーズは、これらのパスフレーズを使用して暗号化されたバックアップのリストアを許可する鍵ファイルでは利用可能な状態のままです。

注意: 古いパスフレーズも含め、パスフレーズを控えておく必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

クライアントマシンの管理者に対してだけ、鍵ファイルのアクセスを可能にする必要があります。

UNIX クライアントの場合、次のことを確認する必要があります。

- 所有者が root ユーザーである。

- アクセス権モード設定が 600 である。
- ファイルは NFS マウントが可能なファイルシステムには存在しない。

サーバーからの標準暗号化の構成について

サーバーから bpkeyutil コマンドを実行して、多くの NetBackup クライアントを暗号化用に構成できます。

前提条件は次のとおりです。

- NetBackup クライアントソフトウェアは、NetBackup Encryption をサポートするプラットフォーム上で実行されている必要があります (『NetBackup リリースノート』を参照してください)。
- NetBackup クライアントは、必要な NetBackup バージョンを実行している必要があります。

クライアントでの暗号化鍵ファイルの作成について

クライアントで暗号化鍵ファイルを作成するには、次のガイドラインを使います。

- サーバーがクラスタ内にあり、暗号化クライアントでもある場合、クラスタ内のすべてのノードは同じ鍵ファイルを持つ必要があります。
- bpkeyutil コマンドを実行すると、各 NetBackup Encryption クライアント上に暗号を使用した暗号化鍵ファイルおよびパスフレーズが設定されます。
  - Windows サーバーの場合、コマンドのフルパスは次のとおりです。

    install_path¥NetBackup¥bin¥bpkeyutil

  - UNIX サーバーの場合、コマンドのフルパスは次のとおりです。

    /usr/openv/netbackup/bin/bpkeyutil

鍵ファイルの作成

各暗号化クライアントに対して、次のコマンドを実行します。

```
bpkeyutil -clients client_name
```

クライアントの鍵ファイルに追加する新しいパスフレーズを入力するプロンプトが表示されます。

複数のクライアントで同じパスフレーズを使用するよう設定するには、次のようにカンマで区切られたクライアント名のリストを指定します。

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

鍵ファイルを作成するため、NetBackup は指定したパスフレーズを使用します。

NetBackup では、指定したパスフレーズを使用して、鍵ファイルが次のように作成されます。

- NetBackup は、次の 2 つのアルゴリズムを組み合わせて、パスフレーズから 256 ビット鍵を作成します。
  - セキュアハッシュアルゴリズム (SHA1)
  - メッセージダイジェストアルゴリズム (MD5)
- NetBackup は NetBackup の秘密鍵と 128 ビット AES アルゴリズムを使用して、鍵を暗号化します。
- この鍵は、クライアント上の鍵ファイルに格納されます。
- 実行時、NetBackup は鍵およびランダム初期化ベクターを使用して、クライアントデータを暗号化します。初期化ベクターは、バックアップイメージのヘッダーに格納されます。

以前のパスフレーズは、これらのパスフレーズで暗号化されたバックアップのリストア用のファイルでは利用可能な状態のままです。

注意: 新しいパスフレーズか以前に使用されたパスフレーズかどうかにかかわらず、パスフレーズが安全で取得可能であることを確認する必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

クライアントマシンの管理者に対してだけ、鍵ファイルのアクセスを可能にする必要があります。UNIX クライアントの場合、次のことを確認する必要があります。

- 所有者が root ユーザーである。
- アクセス権モード設定が 600 である。
- ファイルは NFS マウントが可能なファイルシステムには存在しない。

鍵ファイルのリストアの推奨する実施例

暗号化されたバックアップに利用可能な鍵ファイルがない場合でも、鍵ファイルをリストアできることがあります。

鍵ファイルのパスフレーズを保護するための手作業による保存

手作業による保存は、鍵ファイルのパスフレーズを保護する最も安全な方法です。

`bpkeyutil` コマンドを使用してフレーズを追加する際に、次のように手作業による保存を実行します。

- フレーズを紙に書きます。
- 紙を封筒に入れて封印します。
- 安全な場所に封筒を保管します。

鍵ファイルを消失した場合、後で暗号化されたバックアップからリストアするには、次の手順を実行します。

- NetBackup を再インストールします。
- `bpkeyutil` コマンドを実行し、安全な場所からパスフレーズを取り出して新しい鍵ファイルを作成します。

鍵ファイルの自動バックアップ

自動バックアップはセキュリティが低い方法ですが、鍵ファイルのバックアップコピーを確実に保存できます。

この方法では、暗号化されていないポリシーを作成して、鍵ファイルをバックアップする必要があります。鍵ファイルが消失した場合、暗号化されていないバックアップから鍵ファイルをリストアできます。

この方法の問題点は、クライアントの鍵ファイルが、異なるクライアントによってリストアされることです。

鍵ファイルをクライアントへのバックアップに含める場合、鍵ファイルのパス名をクライアントのインクルードリストに追加します。

リダイレクトリストアでは、リストアを実行するために特別な構成の変更が必要です。

暗号化されたバックアップファイルの、異なるクライアントへのリストア

次に、リダイレクトリストアの手順について説明します。

暗号化されたバックアップを異なるクライアントにリストアする方法

1. サーバーは、リダイレクトリストアを実行できる必要があります。また、ユーザーはリダイレクトリストアを実行するために認証されている必要があります。

   リダイレクトリストアについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

2. 暗号化されたバックアップが作成されたときに、他のクライアントで使用されたパスフレーズを取得します。このパスフレーズがないと、ファイルをリストアすることはできません。

   両方のクライアントで同じパスフレーズが使用されている場合は、手順 5 に進んでください。

3. 現在の鍵ファイルを保存するために、鍵ファイルを移動するか、ファイル名を変更します。

4 bpkeyutil コマンドを実行して他のクライアントに一致する鍵ファイルを作成します。bpkeyutil プロセスでパスフレーズを入力するように求められたら、他のクライアントのパスフレーズを指定します。

5 他のクライアントにファイルをリストアします。

暗号化されたファイルをクライアントからリストアしたら、手順 4 で作成した鍵ファイルの名前を変更するか、ファイルを削除します。

次に、元の鍵ファイルを元の場所または元の名前に戻します。鍵ファイルを元の場所および元の名前に戻さないと、暗号化されたバックアップをリストアできない場合があります。

クライアントでの標準暗号化の直接的な構成について

次の項で説明するとおり、クライアントで直接 NetBackup Encryption を構成することもできます。

- ポリシーでの標準暗号化属性の設定
  p.449 の「ポリシーでの標準暗号化属性の設定」を参照してください。
- サーバーからのクライアントの暗号化設定の変更
  p.449 の「NetBackup サーバーからのクライアントの暗号化設定の変更」を参照してください。

ポリシーでの標準暗号化属性の設定

次のように、NetBackup ポリシーに暗号化属性を設定する必要があります。

- この属性を設定した場合、NetBackup サーバーは、ポリシーで定義された NetBackup クライアントに暗号化されたバックアップの実行を要求します。
- この属性を設定していない場合、NetBackup サーバーは、そのポリシー内で定義されている NetBackup クライアントに暗号化されたバックアップの実行を要求しません。

NetBackup 管理コンソールでポリシーの［属性 (Attributes)］タブを使用して、ポリシーの暗号化属性を設定または設定解除することができます。

ポリシーの設定について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

NetBackup サーバーからのクライアントの暗号化設定の変更

NetBackup サーバー上のクライアントに対する［暗号化 (Encryption)］ホストプロパティで、NetBackup クライアントの暗号化設定を変更することができます。

NetBackup サーバーからクライアントの暗号化設定を変更する方法

1. 左ペインで、[ホスト (Host)]、[ホストプロパティ (Host Properties)]の順に選択します。
2. 変更するクライアントの名前を選択します。[接続 (Connect)]、[クライアントの編集 (Edit client)]の順にクリックします。
3. [暗号化 (Encryption)]をクリックします。

   [暗号化 (Encryption)]ペインの設定に対応する構成オプションについては、次の項を参照してください。

   p.443 の「標準暗号化の構成オプションの管理」を参照してください。

   設定について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

クライアントでのレガシー暗号化の構成

このトピックは NetBackup レガシー暗号化の構成を説明します。

構成オプションは、UNIX クライアント上の `bp.conf` ファイル、または Windows クライアント上のレジストリ内に存在します。

オプションは次のとおりです。

- CRYPT_OPTION
- CRYPT_STRENGTH
- CRYPT_LIBPATH
- CRYPT_KEYFILE

NetBackup Web UI を使用して、サーバーからオプションを構成することもできます。これらのオプションは、[クライアントプロパティ (Client Properties)]ダイアログボックスの[暗号化 (Encryption)]タブに表示されます。

詳しくは『NetBackup 管理者ガイド Vol. 1』を参照してください。

`bpinst -LEGACY_CRYPT` コマンドに CRYPT_OPTION および CRYPT_STRENGTH オプションを設定することができます。それぞれの構成オプションと同等のオプションは、-crypt_option および -crypt_strength です。

クライアントからのレガシー暗号化の構成について

次の表は NetBackup クライアントのレガシー暗号化関連の構成オプションを含んでいます。これらのオプションが、クライアントに適切な値に設定されていることを確認します。これらのオプションは、サーバーからクライアント名に対して `bpinst -LEGACY_CRYPT` コマンドを実行して設定します。

表 21-6 レガシー暗号化構成オプション

オプション	値	説明
CRYPT_OPTION = *option*		NetBackup クライアントに、暗号化オプションを定義します。*option* に指定可能な値は、次のとおりです。
	denied|DENIED	クライアントが暗号化されたバックアップを許可しないように設定します。サーバーが暗号化されたバックアップを要求すると、エラーであると判断されます。
	allowed|ALLOWED	(デフォルト値) クライアントが暗号化されたバックアップまたは暗号化されないバックアップを許可するように指定します。
	required|REQUIRED	クライアントが暗号化されたバックアップを要求するように設定します。サーバーが暗号化されないバックアップを要求すると、エラーであると判断されます。
CRYPT_KIND = *kind*		NetBackup クライアントに、暗号化の種類を定義します。*kind* に指定可能な値は、次のとおりです。
	NONE	標準暗号化またはレガシー暗号化のどちらも、クライアント上では構成されません。
	LEGACY	レガシーの 40 ビット DES または 56 ビット DES 暗号化形式を指定します。このオプションは、レガシー暗号化形式がクライアント上で構成されている場合および標準暗号化形式が構成されていない場合のデフォルトです。
	STANDARD	128 ビット暗号化または 256 ビット暗号化のいずれかの暗号化形式を指定します。
CRYPT_STRENGTH = *strength*		NetBackup クライアントに、暗号化の強度を定義します。*strength* に指定可能な値は、次のとおりです。
	des_40|DES_40	(デフォルト値) 40 ビット DES 暗号化を指定します。
	des_56|DES_56	56 ビット DES 暗号化を指定します。
CRYPT_LIBPATH = *directory_path*		NetBackup クライアントに、暗号化ライブラリを含むディレクトリを定義します。 *install_path* は NetBackup がインストールされるディレクトリで、デフォルトでは C:¥VERITAS です。
	/usr/openv/lib/	UNIX システムでのデフォルト値。
	install_path¥NetBackup¥bin¥	Windows システムのデフォルト値

オプション	値	説明
CRYPT_KEYFILE = *file_path*		NetBackup クライアントに、暗号化鍵を含むファイルを定義します。
	/usr/openv/var/keyfile	UNIX システムでのデフォルト値。
	install_path¥NetBackup¥var¥keyfile.dat	Windows システムのデフォルト値。

レガシー暗号化鍵ファイルの管理

このトピックでは、レガシー暗号化鍵ファイルの管理について説明します。

メモ: クラスタ内のすべてのノードで同じ鍵ファイルを使用する必要があります。

暗号化バックアップおよびリストアを実行する NetBackup クライアントごとに鍵ファイルが必要です。鍵ファイルには、クライアントがバックアップを暗号化するための DES 鍵の生成に使用するデータが含まれます。

鍵ファイルを管理するには、クライアントで bpkeyfile コマンドを実行します。詳しくは、『NetBackup コマンドリファレンスガイド』で コマンドの説明を参照してください。
bpkeyfilehttps://www.veritas.com/content/support/en_US/article.100040135

鍵ファイルが存在しない場合、最初に、鍵ファイルを作成する必要があります。鍵ファイルを作成するには、サーバーからクライアント名に対して bpinst -LEGACY_CRYPT コマンドを実行して、パスフレーズを設定します。

ファイル名は、次に示すように、CRYPT_KEYFILE 構成オプションで指定したファイル名と同じであることが必要です。

- Windows クライアントの場合、デフォルトの鍵ファイル名は次のとおりです。

  install_path¥NetBackup¥var¥keyfile.dat

- UNIX クライアントの場合、デフォルトの鍵ファイル名は次のとおりです。

  /usr/openv/var/keyfile

NetBackup では、鍵ファイルのパスフレーズを使用して DES 鍵が生成され、DES 鍵を使用して鍵ファイルが暗号化されます。

通常、NetBackup アプリケーションにハードコードされている鍵ファイルのパスフレーズを使います。ただし、セキュリティを高めるため、ユーザー独自の鍵ファイルパスフレーズを使用することも可能です。

p.459 の「UNIX 版クライアントのレガシー鍵ファイルの追加によるセキュリティの向上」を参照してください。

メモ: 独自の鍵ファイルパスフレーズを使用しない場合には、新しい鍵ファイルパスフレーズを入力しないでください。代わりに、鍵ファイルの標準パスフレーズを使用して、新しい NetBackup パスフレーズを入力します。

使用する NetBackup パスフレーズを決定する必要があります。NetBackup パスフレーズは、鍵ファイルに格納するデータを生成するために使用します。そのデータは、バックアップを暗号化するための DES 鍵の生成に使用します。

鍵ファイルの標準パスフレーズで暗号化された UNIX クライアントでデフォルトの鍵ファイルを作成するには、次のようなコマンドを入力します。

```
bpkeyfile /usr/openv/var/keyfile
Enter new keyfile pass phrase: (standard keyfile pass phrase)
Re-enter new keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: **********************
Re-enter new NetBackup pass phrase: **********************
```

新しい NetBackup パスフレーズは頻繁に入力する必要があります。古いパスフレーズに関する情報は鍵ファイルに保存されています。この方法では、古いパスフレーズから生成された DES 鍵で暗号化された任意のデータをリストアすることができます。新しい NetBackup パスフレーズを入力するには、コマンドに bpkeyfile -change_netbackup_pass_phrase (または -cnpp) オプションを使用します。

Windows クライアントで、新しい NetBackup パスフレーズを入力する場合は、次の例のようなコマンドを入力します。

```
bpkeyfile.exe -cnpp install_path¥NetBackup¥var¥keyfile.dat
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: **********
Re-enter new NetBackup pass phrase: **********
```

注意: 新しいパスフレーズか以前に使用されたパスフレーズかどうかにかかわらず、パスフレーズが安全で取得可能であることを確認する必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

クライアントマシンの管理者に対してだけ、鍵ファイルのアクセスを可能にする必要があります。

UNIX クライアントの場合、次のことを確認する必要があります。

- 所有者が root ユーザーである。
- アクセス権モード設定が 600 である。
- ファイルは NFS マウントが可能なファイルシステムには存在しない。

ご使用の鍵ファイルをバックアップするかどうかを検討する必要があります。暗号化されたバックアップの場合、鍵ファイルがクライアント上にすでに存在すると、鍵ファイルのリストアだけが実行されるため、このようなバックアップは効果的ではありません。代わりに、クライアントの鍵ファイルに対して、暗号化しないバックアップを行う NetBackup ポリシーを設定することができます。このポリシーは鍵ファイルの緊急リストアが必要な場合に有効です。ただし、この方法では、クライアントの鍵ファイルが異なるクライアント上にリストアされます。

鍵ファイルのバックアップを行わない場合、鍵ファイルのパス名をクライアントのエクスクルードリストに追加します。

サーバーからのレガシー暗号化の構成について

サーバーから bpinst コマンドを実行して、多くの NetBackup クライアントを暗号化用に構成できます。

この方法の前提条件は次のとおりです。

- NetBackup クライアントソフトウェアは、NetBackup Encryption をサポートするプラットフォーム上で実行されている必要があります。
  サポートされるプラットフォームについて詳しくは、『NetBackup リリースノート UNIX、Windows および Linux』を参照してください。
- NetBackup クライアントは、必要な NetBackup バージョンを実行している必要があります。
- クラスタサーバーが NetBackup Encryption のクライアントである場合、クラスタ内のすべてのノードが同じ鍵ファイルを持っていることを確認します。

bpinst コマンドは、サーバー上の NetBackup の bin ディレクトリに次のようにロードされます。

- Windows サーバーの場合、bin ディレクトリは次のとおりです。

  install_path¥NetBackup¥bin

- UNIX サーバーの場合、bin ディレクトリは次のとおりです。

  /usr/openv/netbackup/bin

bpinst コマンドで利用可能な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』で bpinst コマンドの説明を参照してください。

bpinst の使用法の例

p.455 の「クライアントへのレガシー暗号化構成のプッシュインストールについて」を参照してください。

p.456 の「クライアントへのレガシー暗号化パスフレーズのプッシュインストールについて」を参照してください。

通常、bpinst コマンドでクライアント名を指定します。ただし、-policy_names オプションを指定した場合、代わりにポリシー名を指定する必要があります。このオプションは、指定したポリシーのすべてのクライアントに影響します。

クライアントへのレガシー暗号化構成のプッシュインストールについて

NetBackup クライアントで暗号化に関連する構成を設定するには、次に示すように bpinst コマンドで -crypt_option および -crypt_strength オプションを使用します。

- -crypt_option オプションは、クライアントが暗号化されたバックアップを拒否する (denied) か、暗号化されたバックアップを許可する (allowed) か、または暗号化されたバックアップを要求する (required) かを指定します。
- -crypt_strength オプションは、クライアントが暗号化されたバックアップに使用する DES 鍵の長さ (40 または 56) を指定します。

暗号化クライアントソフトウェアをインストールし、56 ビットの DES 鍵で暗号化されたバックアップを要求するには、サーバーから次のコマンドを実行します。

```
bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56
¥
-policy_names policy1 policy2
```

例では、コマンドが長いため UNIX の継続文字 (¥) を使用しています。40 ビットの DES 鍵で暗号化されたバックアップまたは暗号化されていないバックアップのいずれかを許可するには、次のコマンドを実行します。

```
bpinst -LEGACY_CRYPT -crypt_option allowed -crypt_strength des_40 ¥

client1 client2
```

クラスタ環境では、次の操作を実行できます。

- アクティブノードから、クライアントに構成をプッシュインストールします。
- クライアントのリストには、仮想名ではなく各ノードのホスト名を指定します。

メモ: bp.conf 内でのプライマリサーバーの USE_VXSS 設定は、AUTOMATIC に設定する必要があります。この設定は、NBAC が有効化されたプライマリから、NetBackup が前にインストールされていないホストにプッシュする場合に使用します。この設定は、NBAC で bp.conf 内のプライマリサーバー設定 USE_VXSS が有効化されていない場合にも使用します。

クライアントへのレガシー暗号化パスフレーズのプッシュインストールについて

NetBackup クライアントへパスフレーズを送信するには、bpinst コマンドの -passphrase_prompt オプションまたは -passphrase_stdin オプションを使用します。NetBackup クライアントは、パスフレーズを使用して、鍵ファイルのデータを作成または更新します。

鍵ファイルには、次に示すように、クライアントがバックアップを暗号化するための DES 鍵の生成に使用するデータが含まれます。

- -passphrase_prompt オプションを使用すると、0 文字から 62 文字のパスフレーズを入力するプロンプトが表示されます。パスフレーズを入力しても、文字は表示されません。確認のために、パスフレーズを再入力するためのプロンプトがもう一度表示されます。
- -passphrase_stdin オプションを使用すると、標準入力 (STDIN) に、0 文字から 62 文字のパスフレーズを 2 回入力する必要があります。通常、-passphrase_prompt オプションは -passphrase_stdin オプションよりセキュリティが高いのですが、シェルスクリプトで bpinst を使用する場合には -passphrase_stdin の方が便利です。

NetBackup サーバーから標準入力で、client1 という名前のクライアントへのパスフレーズを入力するには、次のようにコマンドを入力します。

```
bpinst -LEGACY_CRYPT -passphrase_stdin client1 <<EOF
This pass phase is not very secure
This pass phase is not very secure
EOF
```

NetBackup サーバーから、client2 という名前のクライアントへのパスフレーズを入力するには、次のようにコマンドを入力します。

```
bpinst -LEGACY_CRYPT -passphrase_prompt client2
Enter new NetBackup pass phrase: ********************
Re-enter new NetBackup pass phrase: ********************
```

新しいパスフレーズは頻繁に入力する必要があります。NetBackup クライアントは、鍵ファイルに古いパスフレーズの情報を保存します。古いパスフレーズから生成された DES 鍵で暗号化されたデータをリストアすることができます。

注意: 新しいパスフレーズか以前に使用されたパスフレーズかどうかにかかわらず、パスフレーズが安全で取得可能であることを確認する必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

多くのクライアントに対して、同じパスフレーズを使用するかどうかを決定する必要があります。1 回の bpinst コマンドで、各クライアントにパスフレーズを指定できるため、同じパスフレーズを使用することをお勧めします。同じパスフレーズを使用する場合、クライアント間でリダイレクトリストアを行うこともできます。

メモ: リダイレクトリストアを回避する場合、クライアントごとに別の bpinst コマンドを入力して異なるパスフレーズを指定する必要があります。

クラスタ環境の場合、次の操作を実行できます。

- アクティブノードから、クライアントに構成をプッシュインストールします。
- クライアントのリストには、仮想名ではなく各ノードのホスト名を指定します。

メモ: bp.conf 内でのプライマリサーバーの USE_VXSS 設定は、AUTOMATIC に設定する必要があります。この設定は、NBAC が有効化されたプライマリサーバーから、NetBackup が前にインストールされていないホストにプッシュする場合に使用します。この設定は、NBAC で bp.conf 内のプライマリサーバー設定 USE_VXSS が有効化されていない場合にも使用します。

別のクライアントで作成されたレガシー暗号化が使用されたバックアップのリストア

サーバーでリダイレクトリストアを実行できる場合、ユーザーはリダイレクトリストアを実行するために認証されている必要があります。

リダイレクトリストアについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

異なるクライアントで作成された、暗号化されたバックアップをリストアする方法

1. 暗号化されたバックアップが作成されたときに、他のクライアントで使用されたパスフレーズを取得します。このパスフレーズがないと、ファイルをリストアすることはできません。

   両方のクライアントで同じパスフレーズが使用されている場合は、手順 4 に進んでください。

2. 現在の鍵ファイルを保存するために、鍵ファイルを移動するか、ファイル名を変更します。

3. `bpkeyfile` コマンドを実行して他のクライアントに一致する鍵ファイルを作成します。プロセスでパスフレーズを入力するように求められたら、他のクライアントのパスフレーズを指定します。bpkeyutil

   ```
   bpkeyfile -change_key_file_pass_phrase key_file_path
   ```

   key_file_path は、クライアント上の新しい鍵ファイルのパスです。この鍵ファイルは他のクライアントの鍵ファイルと一致します。

   コマンドを入力した後、`bpkeyfile` ではクライアントのパスフレーズ (手順 1 で取得) を入力するプロンプトが表示されます。

   `bpkeyfile` 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。

4. 他のクライアントにファイルをリストアします。

   暗号化されたファイルをクライアントからリストアしたら、手順 3 で作成した鍵ファイルの名前を変更するか、ファイルを削除します。

   次に、元の鍵ファイルを元の場所または元の名前に戻します。鍵ファイルを元の場所および元の名前に戻さないと、暗号化されたバックアップをリストアできない場合があります。

ポリシーでのレガシー暗号化属性の設定について

次に示す動作に基づいて、NetBackup ポリシーに暗号化属性を設定する必要があります。

- この属性を設定した場合、NetBackup サーバーは、ポリシーで定義された NetBackup クライアントに暗号化されたバックアップの実行を要求します。
- この属性を設定していない場合、NetBackup サーバーは、そのポリシー内で定義されている NetBackup クライアントに暗号化されたバックアップの実行を要求しません。

NetBackup 管理コンソールでポリシーの[属性 (Attributes)]タブを使用して、ポリシーの暗号化属性を設定または設定解除することができます。

ポリシーの設定について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

また、bpinst コマンドを実行して、NetBackup ポリシーの暗号化属性を設定または設定解除することもできます。この方法は、複数のポリシーに対して属性を設定または設定解除する場合に便利です。

たとえば、NetBackup サーバーから、policy1 および policy2 に対して暗号化属性を設定するには、次のようにコマンドを入力します。

```
bpinst -LEGACY_CRYPT -policy_encrypt 1 -policy_names policy1 policy2
```

パラメータ 1 は暗号化属性を設定します (0 は設定を解除します)。

サーバーからのクライアントのレガシー暗号化設定の変更

NetBackup サーバー上の[クライアントプロパティ (Client Properties)]ダイアログボックスから、NetBackup クライアントの暗号化設定を変更することができます。

NetBackup サーバーからクライアントの暗号化設定を変更する方法

1. 左ペインで、[ホスト (Host)]、[ホストプロパティ (Host Properties)]の順に選択します。
2. 変更するクライアントの名前を選択して、[クライアントの編集 (Edit client)]をクリックします。
3. [プロパティ (Properties)]ペインで、[暗号化 (Encryption)]をクリックして、クライアントの暗号化設定を表示します。

   設定について詳しくは、ダイアログボックスの[ヘルプ (Help)]オプションをクリックするか、または『NetBackup 管理者ガイド Vol. 1』を参照してください。

UNIX 版クライアントのレガシー鍵ファイルの追加によるセキュリティの向上

この項は、UNIX 版 NetBackup クライアントだけに適用されます。セキュリティを強化する機能は、Windows クライアントでは利用できません。

メモ: 鍵ファイルのセキュリティを強化する機能をクラスタ内で使用しないことをお勧めします。

暗号化クライアントの鍵ファイルは、鍵ファイルのパスフレーズから生成された DES 鍵を使用して暗号化されます。デフォルトでは、鍵ファイルは、NetBackup にハードコードされている鍵ファイルの標準パスフレーズから生成された DES 鍵を使って暗号化されます。

鍵ファイルの標準パスフレーズを使用すると、暗号化されていないバックアップおよびリストアを実行するのとほぼ同じ方法で暗号化バックアップおよびリストアの自動実行が可能になります。

ただし、認証されていないユーザーがクライアントの鍵ファイルへのアクセス権を取得した場合、この方法では問題が発生する可能性があります。認証されていないユーザーはバックアップに使用する暗号化鍵を解読できるようになり、鍵ファイルを使用して、クライアントの暗号化されたバックアップをリストアできる場合があります。このような理由から、クライアントの管理者だけが鍵ファイルにアクセスできるようにする必要があります。

特別な保護用に、鍵ファイルを暗号化するための DES 鍵の生成に鍵ファイルの独自のパスフレーズを使用できます。認証されていないユーザーがこの鍵ファイルへのアクセス権を取得しても、リストアすることはより困難になります。

鍵ファイルの独自のパスフレーズを使用すると、バックアップおよびリストアは自動化されなくなります。鍵ファイルの独自のパスフレーズを使用した場合、UNIX 版 NetBackup クライアントでは、次のことが行われます。

クライアント上でバックアップまたはリストアを開始するために、NetBackup サーバーはクライアント上の bpcd デーモンに接続して、要求を作成します。

暗号化されたバックアップまたはリストアを実行するには、bpcd は鍵ファイルを復号化して読み込む必要があります。

鍵ファイルの標準パスフレーズが使用されている場合、bpcd は鍵ファイルを自動的に復号化できます。

ユーザー独自の鍵ファイルパスフレーズが使用されている場合、では自動的に鍵ファイルは復号化されません。bpcdbpcd また、デフォルトの bpcd は使用できません。p.460 の「bpcd -keyfile コマンドの実行」を参照してください。

メモ: クラスタ環境では、1 つのノードの鍵ファイルを変更した場合、すべてのノードの鍵ファイルを同じように変更する必要があります。

---

bpcd -keyfile コマンドの実行

この項では、bpcd コマンドをスタンドアロンプログラムとして実行する方法について説明します。

bpcd をスタンドアロンプログラムとして実行する方法

1 次の例のように bpkeyfile コマンドで -change_key_file_pass_phrase (または -ckfpp) オプションを使用し、鍵ファイルのパスフレーズを変更します。

```
bpkeyfile -ckfpp /usr/openv/var/keyfile
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new keyfile pass phrase: (standard keyfile pass phrase)
******
Re-enter new keyfile pass phrase: (standard keyfile pass
phrase) ******
```

Enterキーを押すと、NetBackup で鍵ファイルの標準パスフレーズが使用されます。

2 bpcd -terminate コマンドを実行して、既存の bpcd を停止します。

3 -keyfile オプションを指定して bpcd コマンドを起動します。プロンプトが表示されたら、鍵ファイルの新しいパスフレーズを入力します。

```
bpcd -keyfile
Please enter keyfile pass phrase: ******
```

bpcd はバックグラウンドで実行され、NetBackup サーバーからの要求を待ちます。

bpkeyfile コマンドに -ckfpp オプションを指定すると、鍵ファイルのパスフレーズをいつでも変更できます。新しい鍵ファイルのパスフレーズは、次に bpcd を起動したときに有効になります。

バックアップを暗号化するための DES 鍵の生成に使用する NetBackup パスフレーズを変更することもできます。bpkeyfile コマンドに -cnpp オプションを指定して、このパスフレーズをいつでも変更できます。ただし、新しい NetBackup パスフレーズは、現行の bpcd プロセスを終了して、bpcd を再起動したときに有効になることに注意してください。

UNIX クライアントでの bpcd の終了

UNIX クライアントで bpcd を終了するには、bpcd -terminate コマンドを使用します。

22

NetBackup Key Management Service

この章では以下の項目について説明しています。

FIPS 対応 KMS について

NetBackup KMS は FIPS モードに対応できるようになりました。このモードでは、作成する暗号化キーが常に FIPS 承認になります。FIPS 設定はデフォルトでは有効です。

p.464 の「FIPS (連邦情報処理標準) について」を参照してください。

新しいキーを作成すると、常に新しいキーとともに Salt が生成されます。キーのリカバリには Salt 値の指定が必須です。

たとえば、次の例を考えてみます。`hrs09to12hrs` は、NetBackup の旧バージョンを使用して作成されたキーです。

```
Key Group Name : ENCR_Monday

Supported Cipher : AES_256
```

```
Number of Keys : 8

Has Active Key : Yes

Creation Time : Wed Feb 25 22:46:32 2015

Last Modification Time: Wed Feb 25 22:46:32 2015

Description : -

Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Wed Feb 25 23:14:18 2015

Description : active
```

キー hrs09to12hrs がキーグループ ENCR_Monday から新しいキーグループ ENCR_77 に移動します。

```
C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd>nbkmsutil -modifykey
-keyname hrs09to12hrs -kgname ENCR_Monday -move_to_kgname ENCR_77

Key details are updated successfully
```

ここで、ENCR_77 キーグループのすべてのキーのリストを表示してください。新しいキー Fips77 は FIPS 承認済みになりますが、旧バージョンの NetBackup を使って作成された hrs09to12hrs は FIPS 承認済みにはなっていません。

```
C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd>nbkmsutil -listkeys
-kgname NCR_77

Key Group Name : ENCR_77 Supported

Cipher : AES_256

Number of Keys : 2

Has Active Key : Yes

Creation Time : Thu Feb 26 04:44:12 2015

Last Modification Time: Thu Feb 26 04:44:12 2015

Description : -

Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9
```

```
Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : No

Key Tag :
4590e304aa53da036a961cd198de97f24be43b212b2a1091f896e2ce3f4269a6

Key Name : Fips77

Current State : INACTIVE

Creation Time : Thu Feb 26 04:44:58 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : Yes

Salt : 53025d5710ab36ac1099194fb97bad318da596e27fdfe1f2

Number of Keys: 2
```

新しいキー `Fips77` は FIPS 承認済みになり、Salt 値も有します。

FIPS 準拠の KMS は次のプラットフォームでサポートされます。

- MS Windows Server 2012
- Linux.2.6.16 x86-64 Suse-10
- Linux.2.6.18 x86-64 RHEL-5

FIPS (連邦情報処理標準) について

FIPS (連邦情報処理標準) には米国連邦政府とカナダ政府のコンピュータシステムに対するセキュリティと相互運用性の必要条件が定義されています。FIPS 140-2 標準には暗号化モジュールのセキュリティ必要条件が明記されています。対称キー暗号化と非対称キー暗号化、メッセージ認証、ハッシュの承認済みセキュリティ機能について説明しています。

FIPS 140-2 標準とその検証プログラムについて詳しくは、http://csrc.nist.gov/groups/STM/cmvp で、米国標準技術研究所 (NIST) とカナダの通信セキュリティ機構 (CSEC) の暗号化モジュール検証プログラム Web サイトを参照してください。

NetBackup 暗号化モジュールが FIPS によって検証されました。NetBackup KMS では NetBackup 暗号化モジュールが使用され、FIPS モードで操作できるようになりました。

p.462 の「FIPS 対応 KMS について」を参照してください。

KMS のインストール

次の手順では、KMS のインストール方法について説明します。

メモ: クラウドストレージ環境での KMS 構成について詳しくは、『NetBackup クラウド管理者ガイド』を参照してください。

KMS サービスは nbkms と呼ばれます。

サービスは、データファイルが設定されるまで実行されないため、KMS を使用しない環境への影響は最小限に留められます。

KMS をインストールする方法

1. `nbkms -createemptydb` コマンドを実行します。
2. ホストマスターキー（HMK）のパスフレーズを入力します。また、Enter キーを押して、ランダムに生成されるキーを作成することもできます。
3. HMK の ID を入力します。この ID には、HMK を特定するのに使用する、わかりやすい任意の ID を指定できます。
4. キーの保護キー（KPK）のパスフレーズを入力します。
5. KPK の ID を入力します。この ID には、KPK を特定するのに使用する、わかりやすい任意の ID を指定できます。

   ID を入力して Enter キーを押すと、KMS サービスが起動します。
6. 次のように KMS サービスを起動します。

   UNIX で、次のコマンドを実行します。

   ```
   /usr/openv/netbackup/bin/nbkms
   ```

   Windows の場合は次の手順を実行します。

   ```
   Start > Run > Services.msc > Start the NetBackup Key Management Service
   ```
7. 次のように、grep コマンドを使用してサービスが起動していることを確認します。`ps -ef | grep nbkms`

8 次のコマンドを実行して、nbkms サービスを NetBackup Web サービスに登録します。

```
nbkmscmd -discovernbkms
```

9 キーグループを作成します。キーグループ名はボリュームプール名に一意に一致する必要があります。すべてのキーグループ名には接頭辞 ENCR_ が付いている必要があります。

メモ: クラウドストレージおよび PureDisk でキーマネージメントを使用する場合、キーグループ名に ENCR_ 接頭辞は必要ありません。

(クラウド以外のストレージ) キーグループを作成するには、次のコマンド構文を使用します。 `nbkmsutil -createkg -kgname ENCR_volumepoolname`

ENCR_ 接頭辞は重要です。BPTM は ENCR_ 接頭辞を含むボリュームプール要求を受け取る場合に、そのボリュームプール名を KMS に渡します。KMS はそれがボリュームプールと完全に一致するかを判別し、そのグループからバックアップ用に active キーレコードを取得します。

クラウドストレージキーグループを作成するには、次のコマンド構文を使用します。

```
nbkmsutil -createkg -kgname storage_server_name:volume_name
```

10 -createkey オプションを使用してキーレコードを作成します。

```
nbkmsutil -createkey -kgname ENCR_volumepool -keyname keyname
-activate -desc "message"
```

キー名およびキーメッセージは任意です。これらは、キーを表示するときにこのキーを特定するのに役立ちます。

-activate オプションは、prelive 状態をスキップしてこのキーを active として作成します。

11 スクリプトでパスフレーズを求められたら、パスフレーズを再入力します。

次の例では、キーグループは ENCR_pool1 と呼ばれ、キー名は Q1_2008_key です。説明部分はこのキーが 1 月、2 月、3 月用のキーであることを示します。

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q1_2008_key
-activate -desc "key for Jan, Feb, & Mar"
```

12 同じコマンドを使用して別のキーレコードを作成できます。別のキー名および説明にすると、キーレコードの区別に役立ちます。`nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q2_2008_key -activate -desc "key for Apr, May, & Jun"`

メモ: コマンド `nbkmsutil -kgname name -activate` を使用して複数のキーレコードを作成すると、最後のキーのみが active に保たれます。

13 あるキーグループ名に属するすべてのキーを表示するには、次のコマンドを使用します。

`nbkmsutil -listkeys -kgname` *keyname*

メモ: このキーが失われた場合、このキーをリカバリするには、パスフレーズ、Salt (該当する場合)、キーグループ名、キータグが必要です。この情報はすべて安全な場所に保管する必要があります。Salt、キーグループ名およびキータグは、`nbkmsutil -listkeys` コマンド実行の出力にあります。

次のコマンドと出力では、この手順の例が使用されています。

```
# nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name         : ENCR_pool1
Supported Cipher       : AES_256
Number of Keys         : 2
Has Active Key         : Yes
Creation Time          : Thu Aug  8 16:23:06 2013
Last Modification Time: Thu Aug  8 16:23:06 2013
Description            : -
 Key Tag    : 825784185f87145c368c54e919908905a45f79927cb733337a53e9b174bbe046
 Key Name               : Q2_2013_key
 Current State          : ACTIVE
 Creation Time          : Thu Aug  8 16:25:19 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description            : key for Apr, May, & Jun
 FIPS Approved Key      : No

 Key Tag    : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
 Key Name               : Q1_2013_key
 Current State          : INACTIVE
 Creation Time          : Thu Aug  8 16:25:03 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description            : key for Jan, Feb, & March
 FIPS Approved Key      : No

Number of Keys: 2
```

p.468 の「HA クラスタに使用する KMS のインストールについて」を参照してください。

p.468 の「KMS の NBAC との使用」を参照してください。

KMS の NBAC との使用

KMS の導入をサポートするために、次の変更が NBAC に加えられました。

- 新しい認可オブジェクト KMS の追加
- 新しい NetBackup ユーザーグループ NBU_KMS Admin の追加

KMS オブジェクトに対してユーザーが所有する権限によって、KMS 関連の実行可能なタスクが異なります。

表 22-1 に、各 NetBackup ユーザーグループのデフォルトの KMS 権限を示します。

表 22-1 NetBackup ユーザーグループのデフォルトの KMS 権限

セット	動作	NBU_ User	NBU_ Operator	NBU_ Admin	NBU_ Security Admin	Vault_ Operator	NBU_ SAN Admin	NBU_ KMS Admin
参照	参照	---	---	X	---	---	---	X
読み込み	読み込み	---	---	X	---	---	---	X
構成	新規	---	---	---	---	---	---	X
構成	削除	---	---	---	---	---	---	X
構成	変更	---	---	---	---	---	---	X

前述の KMS 権限に加えて、NBU_KMS 管理グループはその他の認可オブジェクトに関する次の権限も所有しています。

- BUAndRest は参照、読み取り、バックアップ、リストア、表示権限を所有
- HostProperties は参照、読み取り権限を所有
- License は参照、読み取り権限を所有

HA クラスタに使用する KMS のインストールについて

通常の NetBackup 環境では、一部のオプションパッケージのみがインストール、ライセンス付与または構成されていることがあります。このような状況では、これらのオプション製品に付随するサービスが常に有効でない場合があります。このため、これらのサービスはデフォルトでは監視されず、サービスに障害が発生しても NetBackup はフェールオーバーされません。将来、オプション製品のインストール、ライセンス取得および構成が行われると、そのサービスに障害が発生した場合に NetBackup をフェールオーバーするようにサービスを手動で構成できます。この項では、クラスタを監視するよう手動で KMS を設定する手順を説明します。

KMS サービスの監視の有効化

KMS サービスの監視を有効にし、サービスに障害が発生したときに NetBackup をフェールオーバーすることができます。

KMS サービスの監視を有効にし、サービスに障害が発生したときに NetBackup をフェールオーバーする方法

1. クラスタのアクティブノードで、コマンドプロンプトを開きます。
2. 次の場所にディレクトリを変更します。

   Windows の場合: *<NetBackup_install_path>*¥NetBackup¥bin

   UNIX の場合: /usr/openv/netbackup/bin
3. 次のコマンドを実行します。

   Windows の場合: `bpclusterutil -enableSvc "NetBackup Key Management Service"`

   UNIX の場合: `bpclusterutil -enableSvc nbkms`

KMS サービスの監視の無効化

KMS サービスの監視を無効にすることができます。

KMS サービスの監視を無効にする方法

1. クラスタのアクティブノードで、コマンドプロンプトを開きます。
2. 次の場所にディレクトリを変更します。

   Windows の場合: *<NetBackup_install_path>*¥NetBackup¥bin

   UNIX の場合: /usr/openv/netbackup/bin
3. 次のコマンドを実行します。

   Windows の場合: `bpclusterutil -disableSvc "NetBackup Key Management Service"`

   UNIX の場合: `bpclusterutil -disableSvc nbkms`

KMS の構成

KMS の構成は、キーデータベース、キーグループおよびキーレコードの作成によって行います。その後、KMS と連携するように NetBackup を構成します。

KMS を構成して初期化する方法

1. キーデータベース、ホストマスターキー (HMK) およびキーの保護キー (KPK) を作成します。
2. ボリュームプールと一致するキーグループを作成します。
3. active キーレコードを作成します。

キーデータベースの作成

空のキーデータベースを作成するには、次の手順を使用します。キーデータベースは、-createemptydb オプションを指定してサービス名を起動すると作成されます。この処理は、既存のキーデータベースの有無をチェックし、存在しないことを確認してから作成を開始します。KMS の初期化時に、2 つの保護キーを作成する必要があります。ホストマスターキー (HMK) とキーの保護キー (KPK) です。

すべての KMS キーの作成操作と同様に、これらのキーの作成に関しても次のオプションが用意されています。

- パスフレーズによって生成されたキー
- ランダムに生成されたパスフレーズ

各キーに関連付けられる論理 ID の入力を求められます。この操作が終了すると、キーデータベースおよび保護キーが作成されます。

Windows システムの場合は、これらを次のファイルで確認できます。

NetBackup_install_path¥kms¥db¥KMS_DATA.dat
NetBackup_install_path¥kms¥key¥KMS_HMKF.dat
NetBackup_install_path¥kms¥key¥KMS_HKPKF.dat

UNIX システムの場合は、これらを次のファイルで確認できます。

/usr/openv/kms/db/KMS_DATA
/usr/openv/kms/key/KMS_HMKF
/usr/openv/kms/key/KMS_HKPKF

キーデータベースを作成する方法

1. 次のコマンドを実行します。

   ```
   nbkms -createemptydb.
   ```

2. ホストマスターキーのパスフレーズを入力するか、または Enter キーを押してランダムに生成されたキーを使います。次のプロンプトでパスフレーズを再入力します。
3. HMK ID を入力します。この ID は HMK に関連付けられ、後でこの特定のキーの確認に使用できます。

4 キーの保護キーのパスフレーズを入力するか、または Enter キーを押してランダムに生成されたキーを使います。次のプロンプトでパスフレーズを再入力します。

5 KPK ID を入力します。この ID には、KPK を特定するのに使用する、わかりやすい任意の ID を指定できます。

キーグループとキーレコードについて

キーグループはキーレコードの論理コレクションで、1 つのレコードだけが active 状態になります。

キーグループの定義は、次の情報で構成されています。

- 名前
  キーグループに付ける名前。キーストア内で一意である必要があります。キーグループの名前の変更は、新しい名前がキーストア内で一意であれば可能です。
- タグ
  一意のキーグループ識別子 (変更不可)。
- 暗号
  サポートされている暗号。このキーグループに属するキーは、すべてこの暗号に基づいて作成されます (変更不可)。
- 説明
  任意の説明 (変更可能)。
- 作成時刻 (Creation Time)
  このキーグループの作成日時 (変更不可)。
- 最終変更日時
  変更可能な属性を最後に変更した日時 (変更不可)。

キーグループの作成について

暗号化を設定する最初の手順は、キーグループを作成することです。

次の例では、キーグループ `ENCR_mygroup` を作成しています。

```
nbkmsutil -createkg -kgname ENCR_mygroup
```

メモ: AdvancedDisk およびテープストレージの場合、作成するグループの名前 (たとえば、`mygroup`) に接頭辞 `ENCR_` を付けることが重要です。

キーレコードの作成について

次の手順は、active キーレコードの作成です。キーレコードは prelive 状態で作成してから、active 状態に移すことができます。または、キーレコードは active 状態で直接作成することもできます。

キーレコードは、次の重要な情報で構成されています。

- 名前
  キーに指定された名前は、KG 内で一意である必要があります。キー名の変更は、新しい名前が KG 内で一意であれば可能です。
- キータグ
  一意のキー識別子 (変更不可)。
- キーグループタグ
  このキーが属している一意のキーグループ識別子 (変更不可)。
- 状態 (State)
  キーの現在の状態 (変更可能)。
- 暗号化キー
  バックアップまたはリストアデータの暗号化または復号化に使用されるキー (変更不可)。
- 説明
  任意の説明 (変更可能)。
- 作成時刻 (Creation Time)
  作成時刻 (Creation Time)
- 最終変更日時
  キーの作成日時 (変更不可)。

キーレコードには次の状態があります。

- prelive。レコードは作成されていますが、使用されていないことを示します。
- active。レコードおよびキーが暗号化と復号化に使用されることを示します。
- inactive。レコードおよびキーを暗号化に使用できないことを示します。ただし、復号化には使用できます。
- deprecated。レコードは暗号化または復号化には使用できないことを示します。
- terminated。レコードを削除できることを示します。

キーレコードの状態の概要

キーレコードの状態には、prelive、active、inactive、deprecated および terminated があります。キーレコードの状態は、キーレコードのライフサイクルに準拠しています。いったんキーが active 状態になると (すなわち、暗号化に使用するように設定されると)、キー

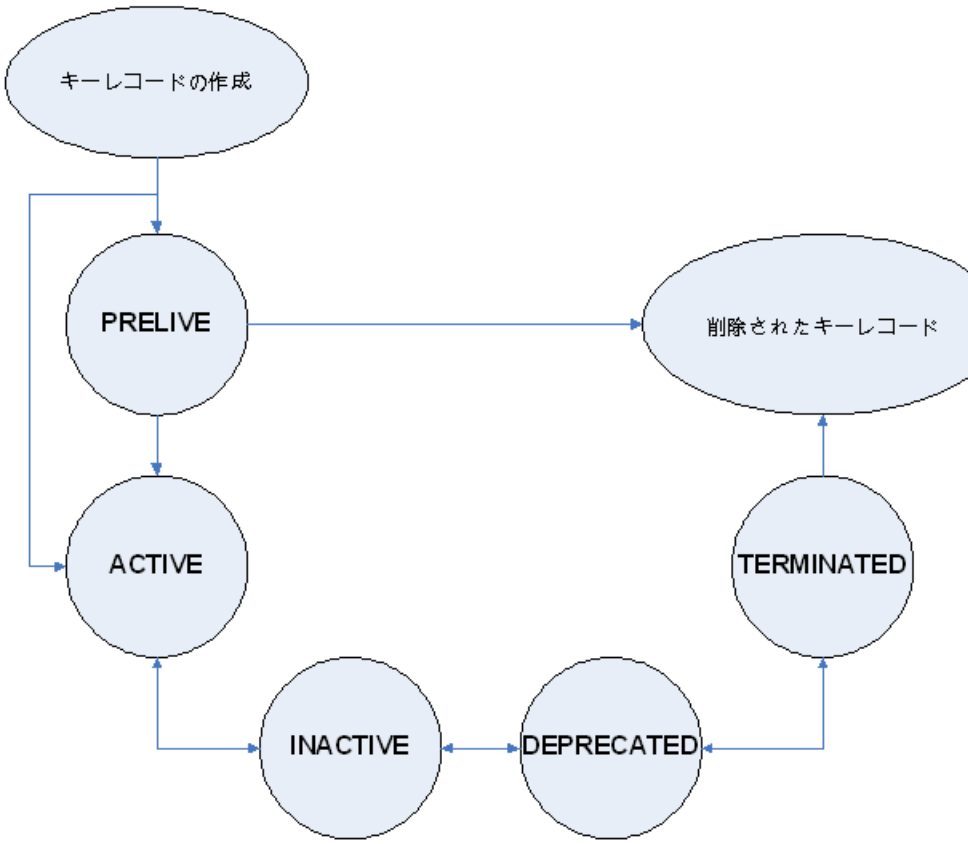
はライフサイクルを通じて、適切な順序で遷移する必要があります。適切な順序とは、ある状態からその隣接した状態に移ることです。キーは、いずれかの状態を省略して遷移することはできません。

active 状態と terminated 状態の間では、前後いずれかの方向に一度に 1 つの状態だけ遷移できます。この範囲以外の状態の場合、移行の方向は一方向のみです。削除されたキーレコードはリカバリできません（パスフレーズを使って作成されていない場合）。また、active 状態のキーを prelive 状態に戻すことはできません。

メモ: キーは、prelive 状態または active 状態のいずれかで作成できます。active キーレコードは、バックアップとリストアの両方の操作で使用できます。inactive キーは、リストア操作でのみ使用できます。deprecated キーは、使用できません。キーレコードが deprecated 状態のときに、そのキーレコードを使用してバックアップまたはリストアを実行しようとすると失敗する可能性があります。terminated 状態にあるキーレコードは、システムから削除できます。

次の図に、prelive 状態または active 状態のキーを作成する処理の流れを示します。

図 22-1 キーの作成の状態



キーレコードの状態に関する注意事項

キーレコードの状態に関して次の注意事項に従ってください。

- キーレコードの状態の遷移は明確に定義されているため、キーレコードを削除するにはこれらの状態をすべて経由する必要があります。
- キーレコードを active に設定すると、active 状態のキーレコードはそのグループに対して inactive 状態になります。1 つのグループに存在可能な active レコードは 1 つだけです。
- deprecated 状態は、キーを保存し、キーの使用を制限する場合に便利です。管理者としてキーのセキュリティが低下したと判断した場合は、そのキーをシステムから削除せずに手動でユーザーによるそのキーの使用を一時停止できます。そのキーレコードを deprecated 状態に設定すると、この deprecated キーを使用してバックアップまたはリストアを試みたユーザーにはエラーが表示されるようになります。

- キーレコードの削除は、キーを誤って削除する可能性を減らすために 2 つの手順で構成されています。まず、deprecated キーを terminated に設定する必要があります。その後、そのキーレコードを削除できます。terminated キーレコードのみを削除できます (prelive 状態のキーを除く)。
- 使用前にキーレコードを作成しておく場合には、prelive 状態を使用できます。

キーレコードの prelive 状態

prelive 状態で作成したキーは、active にすることも、削除することもできます。

prelive 状態は、次の場合に使用できます。

- KMS 管理者が、システムに影響を与えずにキーレコードの作成をテストする場合。レコードが正しく作成されたら、そのレコードを active 状態にできます。正しく作成されていなかった場合、そのレコードを削除できます。
- KMS 管理者がキーレコードを作成しておいて、そのレコードを将来のある時点で active 状態にする場合。これは、レコードを active に設定する操作を、KMS キーストアのバックアップ後（またはパスフレーズの記録後）まで延期する場合などです。または、レコードを active に設定する操作を、将来のある時点に延期する場合もあります。

  prelive 状態のキーレコードは、active にすることも、システムから削除することもできます。

キーレコードの active 状態

active キーレコードは、データの暗号化および復号化に使用できます。必要に応じて、active キーレコードを inactive にすることもできます。active 状態は、最も重要な 3 つのデータ管理状態のうちの 1 つです。他の 2 つの重要なデータ管理状態は、inactive 状態および deprecated 状態です。

キーレコードは、prelive 状態を省略して直接 active 状態で作成できます。active 状態のキーレコードは、active のままにするか、inactive に変更できます。active レコードを prelive 状態に戻すことはできません。

キーレコードの inactive 状態

inactive キーレコードは、データの復号化に使用できます。必要に応じて、inactive キーレコードを再度 active にすることも、deprecated 状態に移行させることも可能です。inactive 状態は、最も重要な 3 つのデータ管理状態のうちの 1 つです。他の 2 つの重要なデータ管理状態は、active 状態および deprecated 状態です。

inactive 状態のキーレコードは、inactive のままにするか、active または deprecated に変更できます。

キーレコードの deprecated 状態

deprecated キーレコードは、データの暗号化または復号化に使用できません。必要に応じて、deprecated 状態のキーレコードを inactive または terminated にすることが可能です。deprecated 状態は、最も重要な 3 つのデータ管理状態のうちの 1 つです。他の 2 つの重要なデータ管理状態は、active 状態および inactive 状態です。

deprecated 状態は、次の場合に使用できます。

- キーの使用を追跡または規制する必要がある場合。deprecated キーが適切な状態に変更されないかぎり、このキーの使用を試みても失敗する可能性があります。
- 今後キーが必要になることはないが、念のために terminated 状態に設定しない場合。
  deprecated 状態のキーレコードは、deprecated のままにするか、inactive または terminated に変更できます。

キーレコードの terminated 状態

terminated 状態は、deprecated 状態のキーレコードを削除する場合の 2 番目の手順、つまり安全のための手順となります。terminated キーレコードは、必要に応じて deprecated 状態に移すか、最終的に再度 active 状態まで戻すことができます。terminated キーレコードは、KMS から削除することもできます。

注意: キーを削除する前に、このキーで暗号化された有効なイメージが存在しないことを確認してください。

---

terminated 状態のキーレコードは、terminated のままにするか、deprecated に変更するかまたは物理的に削除することができます。

KMS データベースファイルのバックアップについて

KMS データベースのバックアップでは、KMS ファイルもバックアップされます。

KMS ユーティリティには、データベースファイルの静止オプション、つまり任意のユーザーによるデータファイルの変更を一時的に禁止するオプションがあります。バックアップを目的として KMS_DATA、KMS_HMKF および KMS_KPKF ファイルを別の場所にコピーする計画の場合は、静止オプションを実行することが重要です。

静止中は、NetBackup によってこれらのファイルに対する書き込みアクセスは排除され、読み込みアクセスのみが許可されます。

`nbkmsutil -quiescedb` を実行すると、静止成功に関するメッセージと、未処理のコール数を示すメッセージが戻されます。この未処理のコール数は、カウントされます。ファイルの未処理の要求数に対して、ファイルにカウントが設定されます。

静止後、そのファイルを別のディレクトリの場所にコピーすることでバックアップを実行できます。

ファイルをコピーした後、nbkmsutil -unquiescedb を使用して KMS データベースファイルの静止を解除できます。

未処理の静止要求カウントが 0 になると、KMS は KMS_DATA、KMS_HMKF、KMS_KPKF ファイルの変更が可能なコマンドを実行できるようになります。これらのファイルに対する書き込みアクセスが再び可能になります。

すべてのデータファイルのリストアによる KMS のリカバリについて

KMS_DATA、KMS_HMKF および KMS_KPKF ファイルのバックアップコピーを作成済みである場合は、これら 3 つのファイルをリストアするだけです。その後 nbkms サービスを起動すると、KMS システムが起動し、再び動作します。

KMS データファイルのみのリストアによる KMS のリカバリ

KMS データファイル kms/db/KMS_DATA のバックアップコピーは、パスフレーズを使って KMS_HMKF と KMS_KPKF ファイルを再生成することで、リストアできます。したがって、ホストマスターキーおよびキーの保護キーのパスフレーズを書き留めてある場合は、これらのファイルを再生成するコマンドを実行できます。システムからパスフレーズの入力を求められ、ここで入力したパスフレーズが元々入力してあったものと一致すると、ファイルをリセットできます。

KMS データファイルのみのリストアによって KMS をリカバリする方法

1. nbkms -resetkpk コマンドを実行します。
2. nbkms -resethmk コマンドを実行します。
3. nbkms サービスを起動します。

データ暗号化キーの再生成による KMS のリカバリ

データ暗号化キーの再生成を行うことで、完全な KMS データベースを再生成できます。目的は、新しい空の KMS データベースを作成し、個々のすべてのキーレコードを再度登録することです。

メモ: ランダムに生成されたキーは、消失した場合はリカバリできません。

データ暗号化キーの再生成によって KMS をリカバリする方法

1 次のコマンドを実行して、空の KMS データベースを作成します。

```
nbkms -createemptydb
```

同じホストマスターキーおよびキーの保護キーを使用する必要はありません。新しいキーを選択できます。

2 `nbkmsutil -recoverkey` コマンドを実行し、キーグループ、キー名およびタグを指定します。

```
nbkmsutil -recoverkey -kgname ENCR_pool1 -keyname Q1_2008_key
  -tag
d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
```

キーの作成時に `nbkmsutil -listkey` コマンドの出力の電子コピーを保持しなかった場合は、64 文字すべてを手動で入力する必要があります。

3 プロンプトで、パスフレーズを入力します。キーが NetBackup 7.7 以降を使用して生成された場合は Salt も入力します。以前に入力した元のパスフレーズと、正確に一致する必要があります。

Salt (該当する場合) は、リカバリするキーに対応する Salt と一致する必要があります。

メモ: 入力したタグがすでに KMS データベースに存在する場合は、そのキーを再作成することはできません。

---

4 リカバリしたキーがバックアップに使用するキーである場合、次のコマンドを実行してキーを active にします。

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
 -state active
```

`-recoverkey` オプションによってキーレコードは inactive 状態になり、inactive 状態で KMS データベースに登録されます。

5 このキーレコードが今後使用されない予定のものである場合は、次のコマンドを実行します。

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
-state deprecated
```

KMS データファイルのバックアップに関する問題

通常の NetBackup テープまたはカタログバックアップで KMS データファイルをバックアップする場合、問題が生じる可能性があります。

注意: KMS データファイルは、NetBackup カタログバックアップに含まれていません。

KPK、HMK およびキーファイルがカタログバックアップに含まれている場合、そのカタログバックアップテープを紛失すると、キーにアクセスするために必要なデータがすべてそのテープに含まれているため、キーストアのセキュリティが低下します。

たとえば、同じトランスポートトラックで運ばれるカタログバックアップテープとデータテープを両方一緒に紛失した場合は、重大な問題が生じる可能性があります。両方のテープを一緒に紛失した場合は、最初からこのテープを暗号化していなかったのと大差ありません。

カタログの暗号化も良いソリューションとはいえません。KPK、HMK およびキーファイルをカタログバックアップに含めて、そのカタログバックアップ自体を暗号化することは、車内に鍵を残したままロックするのと同じです。このような問題を防止するために、KMS は NetBackup の別のサービスとして確立されており、KMS ファイルは NetBackup ディレクトリとは別のディレクトリに保存されます。ただし、KMS データファイルをバックアップするためのソリューションは存在します。

KMS データベースファイルのバックアップソリューション

KMS データファイルをバックアップする最良のソリューションは、通常の NetBackup プロセス以外でバックアップするか、パスフレーズで生成された暗号化キーを使って手動で KMS を再構築することです。暗号化キーはすべてパスフレーズで生成できます。したがって、パスフレーズをすべて記録してある場合は、書き留めてある情報から KMS を手動で再作成することができます。KMS をバックアップする方法の 1 つは、別の CD、DVD または USB ドライブに KMS の情報を配置することです。

キーレコードの作成

次の手順は、パスフレーズを使って、prelive 状態を省略して active 状態のキーを作成してキーレコードを作成する方法を示します。

メモ: すでに active キーが存在するグループにキーを追加しようとすると、既存のキーは自動的に inactive 状態になります。

キーレコードと active 状態のキーを作成する方法

1 キーレコードを作成するには、次のコマンドを入力します。

```
nbkmsutil -createkey -usepphrase -kgname ENCR_mygroup -keyname
my_latest_key -activate -desc "key for Jan, Feb, March data"
```

2 パスフレーズを入力します。

主要グループからのキーのリスト

次の手順を使用して、特定のキーグループで作成したすべてのキーまたは選択したキーをリストします。

キーグループのキーのリストを作成する方法

◆ キーグループのキーのリストを作成するには、次のコマンドを入力します。

```
nbkmsutil -listkeys -kgname ENCR_mygroup
```

デフォルトでは、nbkmsutil によって詳細形式のリストが出力されます。次に、詳細形式ではないリストの出力を示します。

```
KGR ENCR_mygroup AES_256 1 Yes 134220503860000000

134220503860000000 -
KR my_latest_key Active 134220507320000000 134220507320000000
key for Jan, Feb, March data
Number of keys: 1
```

次のオプションで特定のキーグループのすべてのキーまたは特定のキーグループの特定のキーをリストできます。

```
nbkmsutil -listkeys -all | -kgname <key_group_name> [ -keyname
<key_name> | -activekey ]

[ -noverbose | -export ]
```

-all オプションですべてのキーグループのすべてのキーをリストします。キーは詳細な形式でリストに登録済みです。

-kgname オプションは指定されたキーグループからのキーをリストします。

-keyname オプションは指定されたキーグループから特定のキーをリストします。ただし、-kgname オプションと一緒に使用する必要があります。

-activekey オプションは、指定されたキーグループ名からアクティブなキーをリストします。ただし、-kgname オプションと一緒に使用する必要があります。

メモ: -activekey オプションと -keyname オプションは互いに排他的です。

-noverbose オプションは、フォーマットされた形式 (非可読形式) でキーとキーグループの詳細をリストします。デフォルトは、詳細 (verbose) リストです。

-export オプションは、key_file が必要とする出力を生成します。key_file は、nbkmsutil -export -path <key_container_path > -key_file ファイルで使用されます。別の key_file の出力を使用できます。

次のコマンドを実行して、特定のキーグループからすべてのキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name>
```

次のコマンドを実行して、特定のキーグループから特定のキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name> -keyname <key_name>
```

次のコマンドを実行して、すべてのグループからすべてのキーをリストします。

```
nbkmsutil -listkeys -all
```

次のコマンドを実行して、特定のキーグループからすべてのキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name>
```

次のコマンドを実行して、特定のキーグループからアクティブなキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name> -activekey
```

KMS と連携するための NetBackup の構成

KMS と連携するための NetBackup の構成について、次のトピックで説明します。

- NetBackup が KMS からキーレコードを取得する
  p.481 の「NetBackup および KMS のキーレコード」を参照してください。
- NetBackup で暗号化を使用するように設定する
  p.482 の「テープ暗号化を使用するように NetBackup を設定する例」を参照してください。

NetBackup および KMS のキーレコード

KMS と連携するための NetBackup の構成の最初の手順は、NetBackup でサポートされる暗号化可能なテープドライブと、必要なテープメディアをセットアップすることです。

2 番目の手順は、通常どおり NetBackup を構成することです。ただし、暗号化可能なメディアを、KMS を構成したときに作成したキーグループと同じ名前のボリュームプール内に配置する必要がある点が異なります。

メモ: AdvancedDisk とテープストレージの場合、キーマネージメント機能では、キーグループ名と NetBackup ボリュームプール名が同一で、両方の名前に接頭辞 ENCR_ が付いている必要があります。クラウドストレージと PureDisk キーグループの名前は、*storage_server_name*:*volume_name* にする必要があります。この構成方法により、NetBackup のシステム管理インフラストラクチャに大幅な変更を行わなくても、暗号化サポートが利用可能になっています。

テープ暗号化を使用するように NetBackup を設定する例

次の例では、暗号化用に作成した 2 つの NetBackup ボリュームプールを設定します (接頭辞 ENCR_ を付ける)。

次の図に示す NetBackup 管理コンソールには、KMS を使用するための適切な命名規則が適用された 2 つのボリュームプールが表示されています。

図 22-2 KMS を使用するための 2 つのボリュームプールの設定が表示された NetBackup 管理コンソール

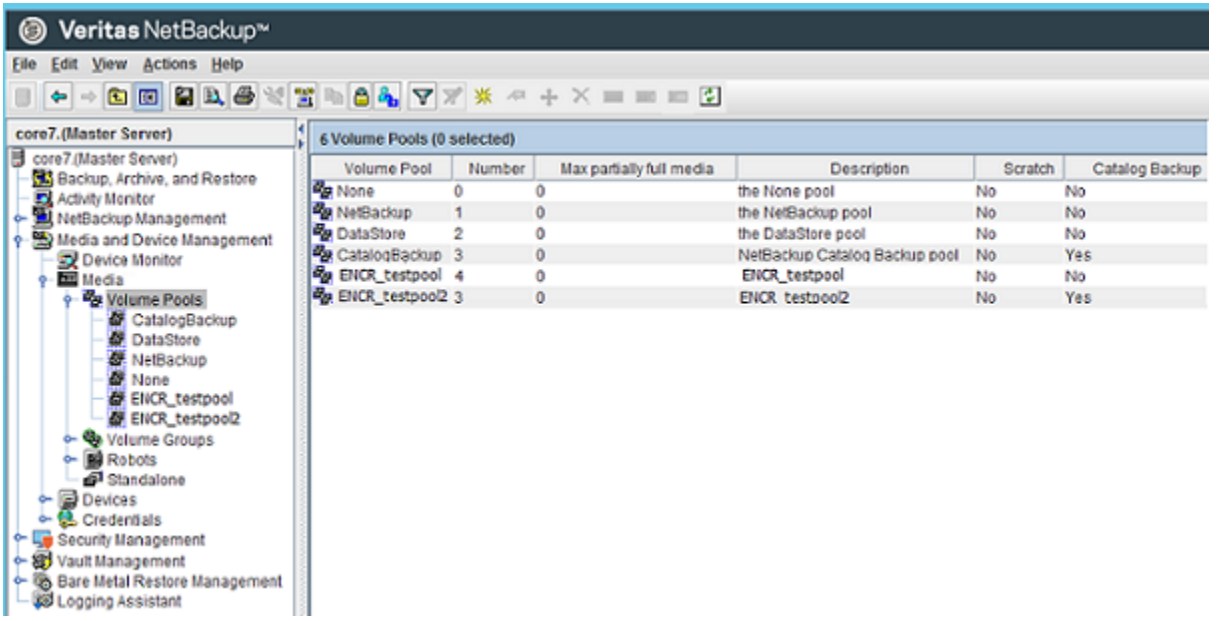
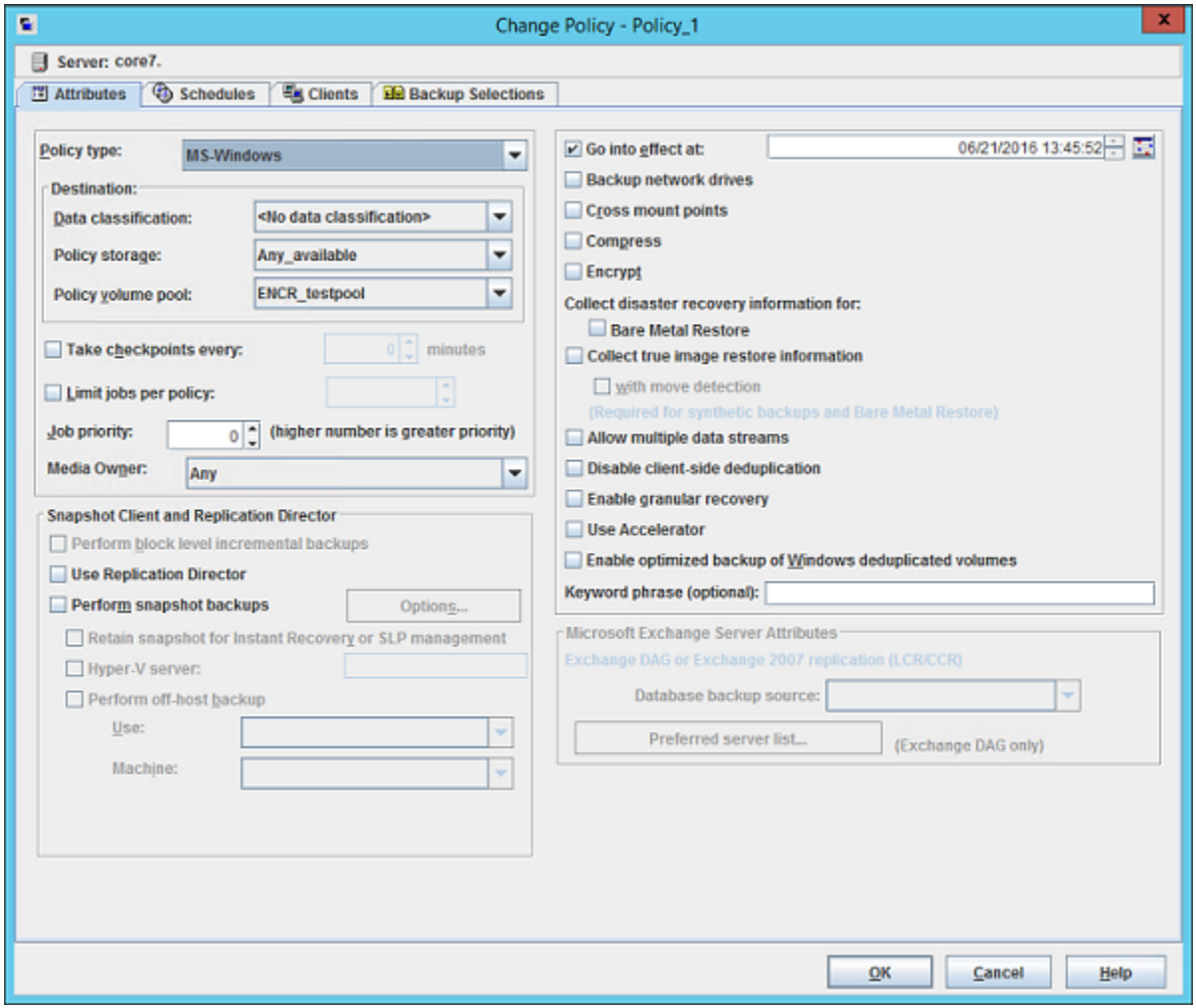


図 22-3に、ボリュームプール ENCR_testpool を使用するように構成された NetBackup ポリシーを示します。これは、以前に構成したキーグループと同じ名前です。

図 22-3 KMS のボリュームプールが表示された NetBackup の[ポリシーの変更 (Change Policy)]ダイアログボックス



NetBackup イメージが暗号化されると、キータグが記録され、イメージと関連付けられます。この情報は、NetBackup 管理コンソールのレポートで確認するか、または `bpimmedia` および `bpimagelist` コマンドの出力で確認できます。

KMS Web アプリケーションを使用した NetBackup KMS の設定

NetBackup KMS (NBKMS) を設定した場合、NetBackup はそれをキー操作には使用しません。KMS サーバーをアクティブ化するには、次のコマンドを実行します。

```
nbkmscmd -configureKMS -type NBKMS
```

暗号化への KMS の使用について

KMS は、暗号化テープバックアップの実行、暗号化テープバックアップの確認、およびキーの管理に使用できます。以降の項では、これらの各シナリオの例を示します。

- 暗号化テープバックアップの実行例
  p.484 の「暗号化テープバックアップの実行例」を参照してください。
- 暗号化バックアップの確認例
  p.485 の「暗号化バックアップの確認例」を参照してください。
- KMS 暗号化イメージのインポートについて
  p.484 の「KMS 暗号化イメージのインポートについて」を参照してください。

KMS 暗号化イメージのインポートについて

KMS 暗号化イメージのインポートは、2 フェーズの操作です。フェーズ 1 では、メディアヘッダーと各フラグメントのバックアップヘッダーが読み込まれます。このデータは暗号化されていません。ただし、バックアップヘッダーには、フラグメントファイルデータが KMS で暗号化されているかどうかが示されています。要するに、フェーズ 1 ではキーは必要ありません。

フェーズ 2 では、カタログ `.f` ファイルが再構築され、このファイルに暗号化データを読み込むように要求されます。`key-tag` (`SCSI` 用語では `KAD`) は、ハードウェアによってテープに保存されます。`NBU`/`BPTM` は、`key-tag` をドライブから読み込み、キーの照合用にこれを KMS に送信します。KMS にキーがある場合は、フェーズ 2 の処理で引き続き暗号化データが読み込まれます。KMS にキーがない場合には、KMS がキーを再作成するまでデータは読み込み可能になりません。このときにパスフレーズが重要になります。

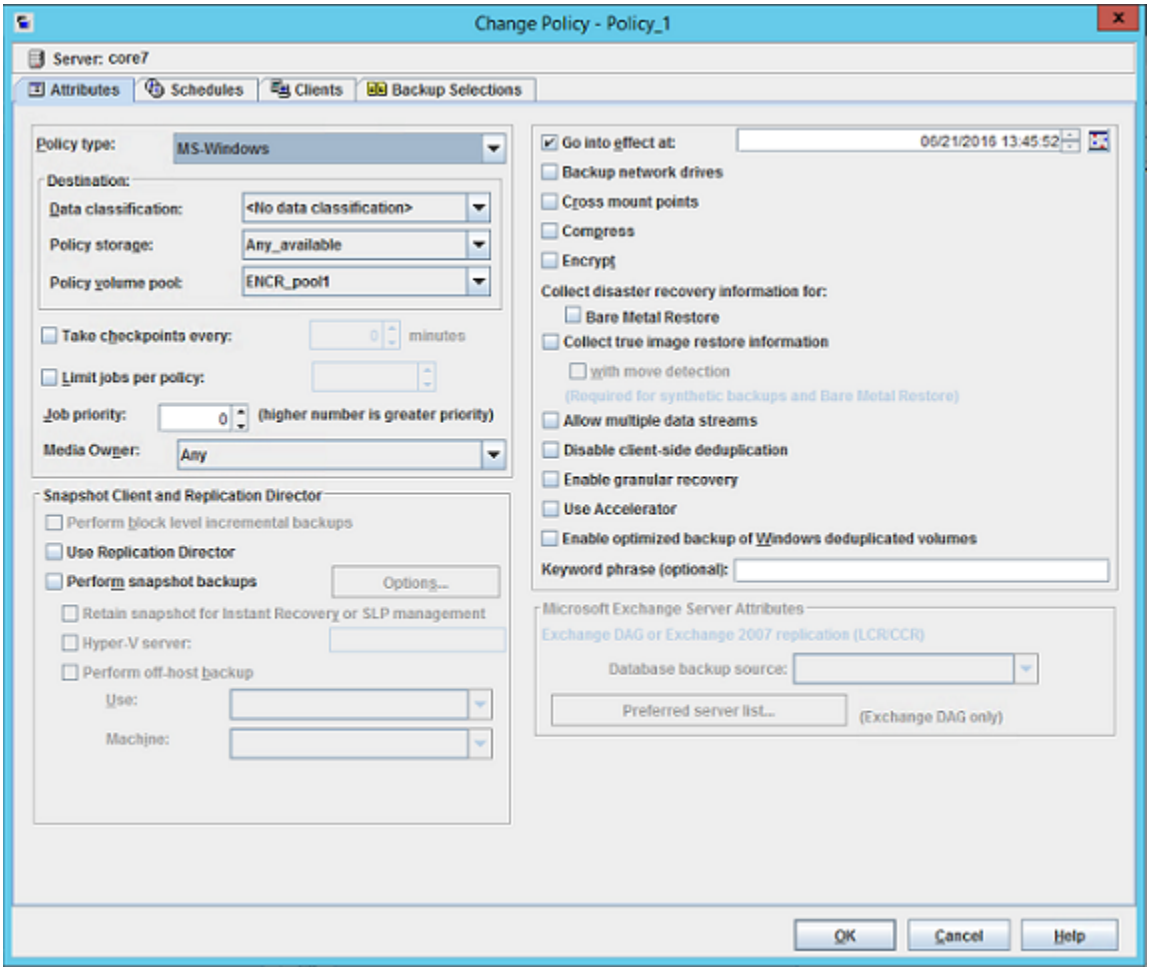
キーを破壊していない場合、これまでに使用されたすべてのキーが KMS に含まれており、任意の暗号化されたテープをインポートできます。キーストアを DR サイトに移動すれば、再作成する必要はありません。

暗号化テープバックアップの実行例

暗号化テープバックアップを実行するには、キーグループと同じ名前のボリュームプールから取得するように設定されたポリシーが必要です。

図 22-4に、ボリュームプール `ENCR_pool1` を使用するように設定した NetBackup ポリシーを示します。

図 22-4 KMS のボリュームプール ENCR_pool1 が表示された NetBackup の[ポリシーの変更 (Change Policy)]ダイアログボックス



暗号化バックアップの確認例

NetBackup による暗号化テープバックアップの実行時に[メディア上のイメージ (Images on Media)]を表示すると、レコードとともに登録される暗号化キータグが表示されます。このキータグによって、テープに書き込まれた内容が暗号化されたことがわかります。この暗号化キータグは、データの暗号化に使用されたキーを一意に識別するものです。レポートを実行してポリシー列を下まで読むと、特定のテープ上のすべての内容が暗号化されているかどうかを確認できます。

KMS データベースの要素

KMS データベースは、次の 3 つのファイルで構成されています。

- キーストアファイル (KMS_DATA)。すべてのキーグループおよびキーレコードと、一部のメタデータが含まれています。
- KPK ファイル (KMS_KPKF)。キーストアファイルに格納されるキーレコードの暗号テキスト部分の暗号化に使用される KPK が含まれています。
- HMK ファイル (KMS_HMKF)。キーストアファイルの内容全体の暗号化に使用される HMK が含まれています。キーストアファイルのヘッダーは例外です。キーストアファイルのヘッダーには、暗号化されない KPK ID および HMK ID のような一部のメタデータが含まれています。

空の KMS データベースの作成

空の KMS データベースは、コマンド nbkms -createemptydb を実行して作成できます。

このコマンドでは、次の情報の入力が求められます。

- HMK パスフレーズ(ランダムな HMK の場合は何も指定しません)
- HMK ID
- KPK パスフレーズ(ランダムな KPK の場合は何も指定しません)
- KPK ID

KMS データベースのバックアップとディザスタリカバリの手順は、次に示すように、KPK および HMK がランダムに生成された場合とパスフレーズで生成された場合で異なります。

HMK と KPK をランダムに生成した場合のリカバリ方法

1. バックアップからキーストアファイルをリストアします。
2. コマンド nbkms -info を実行して、このキーストアファイルの復号化に必要な KPK および HMK の KPK ID および HMK ID を確認します。この出力では、このキーストアファイルの HMK および KPK がランダムに生成されたことも示されているはずです。
3. セキュリティ保護されたバックアップから、この HMK ID に対応する HMK ファイルをリストアします。
4. セキュリティ保護されたバックアップから、この KPK ID に対応する KPK ファイルをリストアします。

KPK ID および HMK ID の重要性

キーストアファイルの内容を解読するには、そのジョブを実行する正しい KPK と HMK を識別することが重要です。識別は、KPK ID および HMK ID で行うことができます。これらの ID はキーストアファイルのヘッダーに暗号化されずに格納されているため、キーストアファイルにアクセスしかできない場合でも特定することができます。ディザスタリカバリの実行を可能にするために、一意の ID を選択し、ID とパスフレーズおよびファイルの関連付けを記憶しておくことが重要です。

HMK および KPK の定期的な更新について

HMK と KPK は、KMS CLI の `modifyhmk` と `modifykpk` オプションを使って定期的に更新できます。この操作では、新しいパスフレーズと ID の入力を求められ、その後 KPK/HMK が更新されます。更新のたびに、ランダムベースの KPK/HKM にするか、パスフレーズベースの KPK/HKM にするかを選択できます。

メモ: HMK および KPK の変更時には `-usepphrase` オプションを使って、今後のリカバリ時に既知のパスフレーズの使用が求められるようにすることが推奨されます。-nopphrase オプションを使った場合は、KMS で未知のランダムパスフレーズが生成され、今後の必要なリカバリが実行できなくなる可能性があります。

KMS キーストアおよび管理者キーのバックアップ

重要な KMS データファイルは、キーデータベース KMS_DATA、ホストマスターキー KMS_HMKF およびキーの保護キー KMS_HKPKF のコピーを作成することでバックアップできます。

Windows の場合、これらのファイルは次の場所にあります。

NetBackup_install_path¥kms¥kms¥db¥KMS_DATA.dat
NetBackup_install_path¥Veritas¥kms¥key¥KMS_HMKF.dat
NetBackup_install_path¥Veritas¥kms¥key¥KMS_KPKF.dat

UNIX の場合、これらのファイルは次の場所にあります。

```
/usr/openv/kms/db/KMS_DATA
/usr/openv/kms/key/KMS_HMKF
/usr/openv/kms/key/KMS_KPKF
```

コマンドラインインターフェース (CLI) コマンド

以下の項では、次のコマンドラインインターフェース (CLI) について説明します。

- CLI の使用方法のヘルプ

p.489 の「CLI の使用方法のヘルプ」を参照してください。

- 新しいキーグループの作成
p.489 の「新しいキーグループの作成」を参照してください。
- 新しいキーの作成
p.490 の「新しいキーの作成」を参照してください。
- キーグループの属性の変更
p.490 の「キーグループの属性の変更」を参照してください。
- キーの属性の変更
p.491 の「キーの属性の変更」を参照してください。
- キーグループの詳細の取得
p.491 の「キーグループの詳細の取得」を参照してください。
- キーの詳細の取得
p.492 の「キーの詳細の取得」を参照してください。
- キーグループの削除
p.492 の「キーグループの削除」を参照してください。
- キーの削除
p.493 の「キーの削除」を参照してください。
- キーのリカバリ
p.493 の「キーのリカバリ」を参照してください。
- ホストマスターキー (HMK) の変更
p.498 の「ホストマスターキー (HMK) の変更」を参照してください。
- ホストマスターキー (HMK) ID の取得
p.498 の「ホストマスターキー (HMK) ID の取得」を参照してください。
- キーの保護キー (KPK) の変更
p.498 の「キーの保護キー (KPK) の変更」を参照してください。
- キーの保護キー (KPK) ID の取得
p.498 の「キーの保護キー (KPK) ID の取得」を参照してください。
- キーストアの統計の取得
p.499 の「キーストアの統計の取得」を参照してください。
- KMS データベースの静止
p.499 の「KMS データベースの静止」を参照してください。
- KMS データベースの静止解除
p.499 の「KMS データベースの静止解除」を参照してください。

CLI の使用方法のヘルプ

CLI の使用方法のヘルプを取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

個別のオプションに関するヘルプを表示するには、nbkmsutil -help -*option* を使用します。

```
# nbkmsutil -help
nbkmsutil [ -createkg ] [ -createkey ]
[ -modifykg ] [ -modifykey ]
[ -listkgs ] [ -listkeys ]
[ -deletekg ] [ -deletekey ]
[ -modifyhmk ] [ -modifykpk ]
[ -gethmkid ] [ -getkpkid ]
[ -quiescedb ] [ -unquiescedb ]
[ -recoverkey]
[ -export ]
[ -import ]
[ -recoverkey ]
[ -ksstats ]
[ -help ]
```

新しいキーグループの作成

新しいキーグループを作成するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -createkg
nbkmsutil -createkg -kgname <key_group_name>
[ -cipher <type> ]
[ -desc <description> ]
```

メモ: デフォルトの暗号は AES_256 です。

-kgname	新しいキーグループの名前を指定します (キーストア内で一意である必要があります)。
-cipher	このキーグループでサポートされる暗号形式を指定します。

新しいキーの作成

新しいキーを作成するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -createkey
nbkmsutil -createkey [ -nopphrase ]
-keyname <key_name>
-kgname <key_group_name>
[ -activate ]
[ -desc <description> ]
```

メモ: デフォルトのキーの状態は prelive です。

-nopphrase	パスフレーズを使わずにキーを作成します。このオプションを指定しない場合は、ユーザーはパスフレーズの入力を求められます
-keyname	新しいキーの名前を指定します (このキーが属するキーグループ内で一意である必要があります)。
-kgname	新しいキーが追加される、既存のキーグループの名前を指定します。
-activate	キーの状態を active に設定します (デフォルトのキーの状態は prelive です)。

メモ: パスフレーズを使用して新しいキーを作成するときに Salt が生成されます。キーを回復する場合は、システムから salt とパスフレーズおよびキータグを入力するように求めるメッセージが表示されます。

キーグループの属性の変更

キーグループの属性を変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -modifykg
nbkmsutil -modifykg -kgname <key_group_name>
[ -name <new_name_for_the_key_group> ]
[ -desc <new_description> ]
```

-kgname	変更するキーグループの名前を指定します。
-name	キーグループの新しい名前を指定します (キーストア内で一意である必要があります)。

キーの属性の変更

キーの属性を変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -modifykey
nbkmsutil -modifykey -keyname <key_name>
-kgname <key_group_name>
[ -state <new_state> | -activate ]
[ -name <new_name_for_the_key> ]
[ -desc <new_description> ]
[ -move_to_kgname <key_group_name> ]
```

メモ: -state オプションと -activate オプションは互いに排他的です。

-keyname	変更するキーの名前を指定します。
-kgname	このキーが属するキーグループの名前を指定します。
-name	キーの新しい名前を指定します (キーグループ内で一意である必要があります)。
-state	キーの新しい状態を指定します (有効なキーの状態の遷移順序を参照してください)。
-activate	キーの状態を active に設定します。
-desc	キーに新しい説明を追加します。
-move_to_kgname	キーの移動先のキーグループの名前を指定します。

キーグループの詳細の取得

キーグループの詳細を取得するには、NetBackup KMS (Key Management Service) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
nbkmsutil -help -listkgs
nbkmsutil -listkgs [ -kgname <key_group_name> |
-cipher <type> |
-emptykgs |
-noactive ]
[ -noverbose ]
```

メモ: デフォルトでは、すべてのキーグループがリストに表示されます。オプションを指定しない場合、すべてのキーグループの詳細が戻されます。

-kgname	キーグループの名前を指定します。
-cipher	特定の暗号形式をサポートするすべてのキーグループの詳細を取得します。
-emptykgs	キーのないすべてのキーグループの詳細を取得します。
-noactive	active キーが存在しないすべてのキーグループの詳細を取得します。
-noverbose	フォーマットされたフォーム形式 (読みやすい形式ではない) で詳細を出力します。デフォルトは、詳細 (verbose) 形式です。出力は読みやすい形式で表示されます。

キーの詳細の取得

キーの詳細を取得するには、NetBackup KMS (Key Management Service) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
#nbkmsutil -help -listkeys
nbkmsutil -listkeys -all | -kgname <key_group_name>
[ -keyname <key_name> | -activekey ]
[ -noverbose | -export ]
```

-kgname	キーグループ名を指定します。キーグループに属するすべてのキーの詳細が戻されます。
-keyname	特定のキーグループに属する特定のキーの詳細を取得します。
-activekey	特定のキーグループの有効なキーの詳細を取得します。
-noverbose	フォーマットされたフォーム形式 (読みやすい形式ではない) で詳細を出力します。デフォルトは、詳細 (verbose) 形式です。出力は読みやすい形式で表示されます。
-export	key_file が必要とする出力を生成します。key_file は、nbkmsutil -export -path <key_container_path > -key_file ファイルで使用されます。出力は別の key_file に使用できます。

キーグループの削除

キーグループを削除するには、NetBackup KMS (Key Management Service) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

メモ: 空のキーグループのみを削除できます。

```
# nbkmsutil -help -deletekg
nbkmsutil -deletekg -kgname <key_group_name> -force
```

-kgname	削除するキーグループの名前を指定します。空のキーグループのみを削除できます。
-force	キーグループのすべてのキーを削除します。

空のキーグループのみを-deletekgオプションで削除できます。しかし、キーグループを空でなくても強制的に削除することもできます。強制的にキーグループを削除するには、次のコマンドを実行します。

```
# nbkmsutil -deletekg -kgname <key_group_name> -force
```

キーの削除

キーを削除するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -deletekey
nbkmsutil -deletekey -keyname <key_name>
-kgname <key_group_name>
```

メモ: prelive または terminated のいずれかの状態のキーを削除できます。

-keyname	削除するキーの名前を指定します (削除するには、キーの状態が prelive または terminated のいずれかである必要があります)。
-kgname	このキーが属するキーグループの名前を指定します。

キーのリカバリ

キーをリカバリするには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -recoverkey
nbkmsutil -recoverkey -keyname <key_name>
-kgname <key_group_name>
-tag <key_tag>
[ -desc <description> ]
```

メモ: キーの状態は inactive に設定されます。

バックアップデータの暗号化に使用したキーが失われ、そのコピーも入手できない場合、リストアが失敗することがあります。このようなキーは、元のキーの属性 (タグ、パスフレーズ、および Salt) がわかれば、リカバリ (再作成) できます。

`-keyname`	リカバリ (再作成) するキーの名前を指定します。
`-kgname`	このキーが属するキーグループの名前を指定します。
`-tag`	元のキーを識別するタグを指定します (同じタグを使用する必要があります)。

メモ: ユーザーは、正しいキーを取得するために正しいパスフレーズの入力を求められます (システムは入力されたパスフレーズの有効性を検証しません)。

メモ: キーを回復するときは必ずシステムから Salt を入力するように求めるメッセージが表示されます。salt はこのバージョンの KMS でパスフレーズ派生キー用に生成されます。旧バージョンの KMS で生成されたキーを回復するには、salt フィールドを空白のままにしてください。

KMS データベースからのキーのエクスポートと KMS データベースへのキーのインポートについて

キーのエクスポートおよびインポートにより、同じキーセットを使用する複数の NetBackup ドメインを迅速に同期化したり、キーセットをドメイン間で迅速に移動したりできます。この機能は、ディザスタリカバリにより発生する別の NetBackup ドメインでのリストアに特に役立ちます。

キーのエクスポート

`-export` コマンドにより、キーおよびキーグループをドメイン間でエクスポートできます。キーおよびキーグループのエクスポートについて重要な情報を次の一覧に示します。

- キーは必ず、所属するキーグループに基づいてエクスポートされます。
- キーとキーグループは、キーマネージメントサービス (KMS) ユーティリティ (`nbkmsutil`) が実行されるホスト上の暗号化キーコンテナ (ファイル) でエクスポートされます。キーコンテナはパスフレーズで保護されます。

  メモ: キーおよびキーグループをインポートするとき、同じパスフレーズを使用する必要があります。

- エクスポート内容の指定には、特定のキーグループを選択する方法、またはキーを選択してエクスポートする方法があります。

次のように -export コマンドを使用します。

```
nbkmsutil -export -path <secure_key_container>
[ -key_groups <key_group_name_1 ...> | -key_file <key_file_name> ]
```

デフォルトでは、キーストア全体がエクスポートされます。

-path コマンドは、安全なキーコンテナが格納される完全修飾パスを指定します。

-key_groups コマンドは、キーグループ名をスペースで区切って指定します。

-key_file コマンドは、特定形式でエクスポートするキーをリストで示すファイルパスです。

<key_group_name>/<key_name> コマンドでは、キーを選択してエクスポートできます。特定のグループのすべてのキーをエクスポートする場合は、「*」を使用できます。

```
<key_group_name>/*
```

nbkmsutil -listkeys -export コマンドを使って、このオプションに必要とされる形式で出力を生成できます。詳しくは、nbkmsutil -listkeys -export を参照してください。

キーのリスト作成の詳細:

p.480 の「主要グループからのキーのリスト」を参照してください。

メモ: -key_groups コマンドと -key_file コマンドは相互に排他的です。

次のコマンドを実行すると、キーストア全体がエクスポートされます。

```
nbkmsutil -export -path <secure_key_container>
```

次のコマンドを実行すると、選択したキーグループがエクスポートされます。

```
nbkmsutil -export -path
<secure_key_container> -key_groups
<key_group_name_1 key_group_name_2 ...>
```

次のコマンドを実行すると、選択したキーがエクスポートされます。

```
nbkmsutil -export -path
<secure_key_container> -key_file
<key_file_name>
```

エクスポート時における一般的なエラーのトラブルシューティング

キーおよびキーグループをエクスポートする場合に発生する一連のエラー。この項は、このようなエラーをトラブルシューティングするのに役立ちます。

- 指定したキーコンテナがホスト上にすでに存在していた場合、エクスポートは失敗します。
  別のキーコンテナファイルを指定してから、エクスポート操作を再度実行してください。
- 正しくないキーまたはキーグループ名を指定した場合も、エクスポートは失敗します。
  キーまたはキーグループ名を訂正し、再度エクスポートを実行してください。

キーのインポート

`-import` コマンドにより、キーおよびキーグループをドメイン間でインポートできます。キーおよびキーグループのインポートについて重要な情報を次の一覧に示します。

- キーおよびキーグループをインポートする場合、エクスポート中に作成されたキーコンテナファイルが必要です。また、エクスポート中に使われた同じパスフレーズも必要です。
- キーのインポートはアトミック操作です。操作中にエラーが発生した場合、すべての更新が元に戻されます。
- 部分的なインポートはサポートされません。
- インポート出力のプレビューが利用可能です。`-preview` コマンドを実行すると、インポート結果がプレビューされます。
- インポート操作には 2 つのモードがあります。`-preserve_kgname` コマンドを含んでいるモード、`-preserve_kgname` コマンドを含まないモードがあります。
  デフォルトでは、キーグループは次の名前形式でインポートされます。
  `< Original_Kgname_<timestamp> >`
  明示的に `<-preserve_kgname>` オプションを指定することにより、キーグループ名を保持することができます。
- 同じキータグのキーまたは同じキーのある重複キーはインポートされません。
- インポートでは、キーグループのマージをサポートしません。

ただし、`<-preserve_kgname>` コマンドを使用しなければ、キーをマージして、キーグループとしてインポートできます。`nbkmsutil -modifykey -keyname <key_name> -kgname <key_group_name>` コマンドを実行すると、現在のグループから目的のグループにキーを移動できます。

キーの移動についての詳細:

p.491 の「キーの属性の変更」を参照してください。

キーグループに同じキーまたは同じキータグを持つキーが含まれている場合、これらはインポート中無視されます。キーおよびキーグループをインポートするには、次のコマンドを実行します。

```
# nbkmsutil -import -path <secure_key_container>

[-preserve_kgname]

[ -desc <description> ]

[ -preview ]
```

-preserve_kgname コマンドは、インポート中、キーグループ名を保持します。

-desc <description> コマンドは、インポート中、キーグループと関連付けられる説明になります。

-preview コマンドは、インポート結果のプレビューを表示します。

-preserve_kgname を使用するインポート操作は次のように実行します。

```
nbkmsutil -import -path

<secure_key_container>

[-preserve_kgname]
```

-preserve_kgname とともに -import コマンドを実行すると、キーコンテナから元のキーグループ名を使ったインポートが試みられます。同じ名前のキーグループが存在すれば、インポート操作は失敗します。

-preserve_kgname なしのインポート操作は次のように実行します。

```
nbkmsutil -import -path

<secure_key_container>
```

-preserve_kgname なしで -import コマンドを実行すると、キーグループはインポートされますが、キーグループ名は、タイムスタンプなどが接尾語として使用されることにより変更されます。名前が変更されるキーグループは、必ず一意の名前になります。

インポート時における一般的なエラーのトラブルシューティング

キーおよびキーグループをインポートする場合に発生する一連のエラー。この項は、このようなエラーをトラブルシューティングするのに役立ちます。

- [-preserve_kgname] オプションでキーグループをインポートしようとしていて、そのグループが KMS にすでに存在していた場合、インポート操作全体が失敗します。既存のキーグループを削除するか、名前を変更して、または [-preserve_kgname] オプションを除外してから、インポート操作を再度実行してください。

- NetBackup KMS には、100 キーグループという制限が存在します。各グループには、30 キーという制限が存在します。100 を超えるキーグループをインポートすると、操作が失敗します。
  不要な既存のキーグループを削除して、インポート操作を再実行する必要があります。

ホストマスターキー (HMK) の変更

ホストマスターキーを変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

HMK は、キーストアの暗号化に使用します。現在の HMK を変更するには、オプションのシードまたはパスフレーズを指定する必要があります。また、その指定されたパスフレーズを連想できるような ID (HMK ID) を指定する必要もあります。パスフレーズと HMK ID は、どちらも対話形式で読み込まれます。

```
# nbkmsutil -help -modifyhmk
nbkmsutil -modifyhmk [ -nopphrase ]
```

ホストマスターキー (HMK) ID の取得

HMK ID を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。これにより、HMK ID が戻されます。

```
# nbkmsutil -help -gethmkid
nbkmsutil -gethmkid
```

キーの保護キー (KPK) ID の取得

KPK ID を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。このコマンドにより、現在の KPK ID が戻されます。

```
# nbkmsutil -help -getkpkid
nbkmsutil -getkpkid
```

キーの保護キー (KPK) の変更

キーの保護キーを変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

KPK は、KMS キーの暗号化に使用します。現在、KPK はキーストアごとに存在します。現在の KPK を変更するには、オプションのシードまたはパスフレーズを指定する必要が

あります。また、その指定されたパスフレーズを連想できるような ID（KPK ID）を指定する必要もあります。パスフレーズと KPK ID は、どちらも対話形式で読み込まれます。

```
# nbkmsutil -help -modifykpk
nbkmsutil -modifykpk [ -nopphrase ]
```

キーストアの統計の取得

キーストアの統計を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

このコマンドでは、次のキーストアの統計が戻されます。

- キーグループの総数
- キーの総数
- 未処理の静止要求

```
# nbkmsutil -help -ksstats
nbkmsutil -ksstats [ -noverbose ]
```

KMS データベースの静止

KMS データベースを静止するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

このコマンドは、KMS に静止要求を送信します。コマンドが正常に実行されると、現在の未処理の静止カウントが戻されます (複数のバックアップジョブが KMS データベースを静止させる場合があるため)。

```
# nbkmsutil -help -quiescedb
nbkmsutil -quiescedb
```

KMS データベースの静止解除

KMS データベースを静止解除するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

このコマンドは、KMS に静止解除要求を送信します。コマンドが正常に実行されると、現在の未処理の静止数が返されます。カウントが 0 (ゼロ) の場合は、KMS データベースが完全に静止解除されていることを意味します。

```
# nbkmsutil -help -unquiescedb
nbkmsutil -unquiescedb
```

キーの作成オプション

NetBackup KMS 機能を使用する場合は、必ず kms/db および kms/key ディレクトリのバックアップが作成されます。保護キーおよびキーデータベースは 2 つの別個のサブディレクトリに存在しており、バックアップコピーの作成時にこれらを容易に分けられるようになっています。

メモ: これらのファイルは、サイズが小さい点、変更頻度が低い点、およびそれ自体が暗号化される NetBackup テープには含めてはならないという点から、バックアップメディアに手動でコピーする必要があります。

メモ: このバージョンの KMS で推奨されるキーの作成方法は、常にパスフレーズからキーを作成することです。このようなキーには、保護キー (ホストマスターキーおよびキーの保護キー) と、キーレコードに関連付けられているデータ暗号化キーの両方が含まれます。キーの作成に使うパスフレーズは、リカバリで使うことができるように、記録し、保管しておくことをお勧めします。

KMS システムでランダムな暗号化キーの生成を許可するとより強力なソリューションが得られますが、この使用方法ではキーストアおよび保護キーのすべてのコピーが失われた場合または破損した場合にリカバリできなくなるため、お勧めしません。

KMS のトラブルシューティング

KMS のトラブルシューティングを開始するには、次の手順を使用します。

KMS のトラブルシューティングを開始する方法

1. 発生したエラーコードおよび説明を特定します。
2. KMS が実行されているかどうかを判別し、次の KMS データファイルが存在することを確認します。

   ```
   kms/db/KMS_DATA
   kms/key/KMS_HMKF
   kms/key/KMS_KPKF
   ```

   このファイルが存在しない場合は、KMS は構成されていないか、または構成が削除されています。ファイルが存在しない場合は、ファイルに何が発生したかを特定します。KMS が構成されていない場合、nbkms サービスは実行されません。KMS が実行されていないか、または構成されていない場合は、NetBackup 操作には影響を及ぼしません。これまでボリュームプール名に ENCR_ の接頭辞を使用していた場合は、この名前を変更する必要があります。ENCR_ は現在 NetBackup で特別な意味を持ちます。

3 KMS 構成情報を取得します。

コマンド nbkmsutil -listkgs を実行して、キーグループのリストを取得します。コマンド nbkmsutil -listkeys -kgname *key_group_name* を実行して、キーグループのすべてのキーのリストを取得します。

4 VxUL OID 286 および BPTM ログを介して、KMS ログなどの操作ログ情報を取得します。

5 ログ情報を評価します。KMS エラーは BPTM に戻されます。

6 KMS ログに記録されている KMS エラーを評価します。

バックアップが暗号化されていない問題の解決方法

テープバックアップが暗号化されていない場合、次の解決方法を検討します。

- 暗号化キータグフィールドがイメージレコードに設定されていないことを確認し、バックアップが暗号化されていないことを確認します。
- キーグループ名とボリュームプール名が完全に一致することを確認します。
- キーグループに active 状態のキーレコードがあることを確認します。

その他の KMS 以外の構成オプションでは、次の点に注目してください。

- 従来のメディア管理に関するすべての項目が適切に構成されていることを確認します。
- NetBackup ポリシーが適切なボリュームプールからテープを取得していることを確認します。
- 暗号化が可能なテープドライブで、暗号化が可能なメディアが利用可能であることを確認します。たとえば、LTO4 メディアが LTO4 テープドライブにインストールされていることを確認します。

リストアが復号化されない問題の解決方法

暗号化されたテープのリストアが復号化されていない場合は、次の解決方法を検討します。

- イメージレコードの暗号化キータグフィールドを参照して、元のバックアップイメージが最初から暗号化されていたことを確認します。
- 同じ暗号化キータグフィールドを持つキーレコードが、リストアをサポートするレコードの状態であることを確認します。これらの状態には、active 状態または inactive 状態があります。
- キーレコードが適切な状態でない場合は、キーを inactive 状態に戻します。

その他の KMS 以外の構成ソリューションのオプションを次のように検討します。

- ドライブおよびメディアが暗号化をサポートしていることを確認します。
- 読み取り中の暗号化されたメディアが、暗号化が可能なテープドライブにあることを確認します。

トラブルシューティングの例 - active キーレコードが存在しない場合のバックアップ

次の例は、active キーレコードが存在しない場合にバックアップを試行したときの結果を示します。

図 22-5 に、キーレコードのリストを示します。これらのうち 3 つのキーグループは ENCR_mygroup で、ボリュームプール名が同じです。Q2_2008_key という名前のキーグループは active でした。コマンドシーケンスの終わりでは、Q2_2008_key キーグループの状態が inactive に設定されます。

図 22-5　　キーレコードのリスト

```
fel (root) [385]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name         : ENCR_mygroup
Supported Cipher       : AES_256
Number of Keys         : 3
Has Active Key         : Yes
Creation Time          : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description            : -
  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name               : Q2_2008_key
  Current State          : Active
  Creation Time          : Sat Mar 15 11:02:46 2008
  Last Modification Time: Sat Mar 15 11:02:46 2008
  Description            : key for Apr, May, & Jun
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name               : Q1_2008_key
  Current State          : Inactive
  Creation Time          : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description            : Key for Jan, Feb, & March
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name               : test
  Current State          : Inactive
  Creation Time          : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description            : -
Number of Keys: 3
fel (root) [383]: nbkmsutil -modifykey -keyname Q2_2008_key -kgname ENCR_mygroup -state
Inactive
Key details are updated successfully
```

図 22-6に、再作成されたキーレコードのリストを示します。Q2_2008_key の状態が inactive と表示されるのがわかります。

図 22-6　active キーグループが変更された状態のキーレコードのリスト

```
fel (root) [384]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name         : ENCR_mygroup
Supported Cipher       : AES_256
Number of Keys         : 3
Has Active Key         : No
Creation Time          : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description            : -
  Key Tag     : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name               : Q1_2008_key
  Current State          : Inactive
  Creation Time          : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description            : Key for Jan, Feb, & March
  Key Tag     : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name               : test
  Current State          : Inactive
  Creation Time          : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description            : -
  Key Tag     : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name               : Q2_2008_key
  Current State          : Inactive
  Creation Time          : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 13:53:33 2008
  Description            : key for Apr, May, & Jun

Number of Keys: 3
```

active キーがない場合のバックアップへの影響を考えてみます。

図 22-7 に BPTM ログの出力を示します。BPTM ログのエラーコード 1227 内にメッセージが記録されます。

図 22-7　bptm コマンドの出力

```
14:29:16.381 [19978] <2> manage_drive_attributes: MediaPool [ENCR_mygroup], MediaLabel [MEDIA=JRO111;]
14:29:16.384 [19978] <2> manage_drive_attributes: encryption status: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decryp mode 0x0, algorithm index 0, key instance
0
14:29:16.384 [19978] <2> KMSCLIB::kmsGetKeyAndKad: Entering function....(KMSClib.cpp:583)
14:29:16.384 [19978] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:29:16.384 [19978] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:29:16.385 [19978] <2> Orb::init: Created anon service name: NB_19978_1536015948517350(Orb.cpp:600)
14:29:16.385 [19978] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_19978_1536015948517350(Orb.cpp:618)
14:29:16.385 [19978] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory ''" -ORBSvcConfDirective "static
EndpointSelectorFactory ''" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_19978_1536015948517350 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:29:16.406 [19978] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:29:16.406 [19978] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:29:16.460 [19978] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:29:16.461 [19978] <16> get_encryption_key: NBKMS failed with error status: Key group does not have an active key
(1227)
14:29:16.462 [19978] <2> send_MDS_msg: MEDIADB 1 42 JRO111 4000007 *NULL* 6 1205781805 1205782033 1206991633 0 64 2
2 1 4 0 8193 1024 0 8 0
```

[ジョブの詳細 (Job Details)]ダイアログボックスには、詳細な状態が表示されます。失敗の内容と状態の詳細を示すメッセージを確認できます。以前の診断の情報と合わせて、特定の問題を判別することや、発生した問題が何に関連しているかを特定することができます。

トラブルシューティングの例 - 不適切なキーレコード状態でのリストア

次の例は、不適切な状態のキーレコードを使用したリストアを示します。

図 22-8 は、必要なレコードが deprecated に設定されていることを示します。次にリストを示します。同じコマンドを使用して、状態が inactive から deprecated に変更されています。

図 22-8 deprecated キーグループを含むキーレコードのリスト

```
fel (root) [426]: !385
nbkmsutil -listkeys -kgname ENCR_mygroup

Key Group Name        : ENCR_mygroup
Supported Cipher      : AES_256
Number of Keys        : 3
Has Active Key        : No
Creation Time         : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description           : -

  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name              : Q1_2008_key
  Current State         : Inactive
  Creation Time         : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description           : Key for Jan, Feb, & March

  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name              : test
  Current State         : Inactive
  Creation Time         : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description           : -

  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name              : Q2_2008_key
  Current State         : Deprecated
  Creation Time         : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 14:52:59 2008
  Description           : key for Apr, May, & Jun

Number of Keys: 3
```

図 22-9 は、bptm ログの出力に 1242 エラーが戻されていることを示します。

図 22-9 1242 エラーを含む bptm ログの出力

```
14:53:48.782 [21109] <2> io_read_back_header: drive index 0, reading backup header
14:53:48.791 [21109] <2> io_position_for_read: successfully positioned JRO111 to file number 3
14:53:48.796 [21109] <2> io_position_for_read: next block encryption status: LON 0x0000000000000009, algorithm
index 1, encryption status 0x6
14:53:48.796 [21109] <2> io_position_for_read: Kad type 0x0, kad length 32 Kad
[cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d]
14:53:48.796 [21109] <2> KMSCLIB::kmsGetKeyAndKadByKeyTag: Entering function....(KMSClib.cpp:655)
14:53:48.796 [21109] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:53:48.796 [21109] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:53:48.797 [21109] <2> Orb::init: Created anon service name: NB_21109_1537488329610200(Orb.cpp:600)
14:53:48.798 [21109] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_21109_1537488329610200(Orb.cpp:618)
14:53:48.798 [21109] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory ''" -ORBSvcConfDirective "static
EndpointSelectorFactory ''" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_21109_1537488329610200 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:53:48.818 [21109] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:53:48.818 [21109] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:53:48.842 [21109] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:53:48.844 [21109] <16> get_encryption_key: NBKMS failed with error status: Operation not allowed for key record
in this state (1242)
```

23

外部のキーマネージメントサービス

この章では以下の項目について説明しています。

外部 KMS について

外部 KMS のサポートは、格納データの暗号化キーに対して、NetBackup Key Management Service (KMS) の代替機能を提供します。

テープ、クラウド、MSDP、AdvancedDisk などのストレージ構成に格納されているバックアップイメージは、外部 KMS サーバーが管理するキーを使用して暗号化できます。

NetBackup は、KMIP (Key Management Interoperability Protocol) を使用した外部 KMS との通信をサポートします。

NetBackup がサポートする KMIP のバージョンについては、NetBackup 互換性リストを参照してください。

NetBackup は、セキュリティ証明書を使用した、外部 KMS サーバーによる認証をサポートします。操作のたびに NetBackup は外部 KMS に証明書を提示し、必要な操作の実行を要求します。外部 KMS は証明書を検証し、要求された操作を実行します (ユーザーに必要な権限がある場合)。

詳しくは、NetBackup での外部 KMS のサポートに関するビデオを参照してください。

ビデオへのリンク

証明書の構成と認可

NetBackup で使用する証明書を構成する前に、外部 KMS サーバーで特定の構成を行い、キー固有の操作を実行するために必要なアクセス権を NetBackup に設定する必要があります。構成手順は、外部 KMS ソリューションによって異なる場合があります。

次の項目について確認します。

- エンティティ (ユーザー) が NetBackup プライマリサーバーを表す外部 KMS で作成されている。
- プライマリサーバーのホストに、外部 KMS サーバーが信頼する証明書がある。
- 証明書の共通名 (CN) が、プライマリサーバーを表すエンティティに関連付けられている。

外部 KMS の構成のワークフロー

外部 KMS 統合の場合は、NetBackup プライマリサーバーで集中管理されている構成が使用されます。プライマリサーバーは、外部 KMS サーバーの KMIP ポートとのアウトバウンド接続を確立する必要があります。プライマリサーバー上で、証明書クレデンシャルを使用して、外部 KMS との通信チャネルを構成します。その後、プライマリサーバーは、メディアサーバーなどの他のサーバーの代わりにすべての要求を外部 KMS サーバーに送信します。

表 23-1 KMS の構成のワークフロー

手順の番号	手順	参照トピック
手順 1	KMS クレデンシャルの検証	p.508 の「KMS クレデンシャルの検証」を参照してください。
手順 2	KMS クレデンシャルの構成	p.510 の「KMS クレデンシャルの構成」を参照してください。
手順 3	KMS の構成	p.511 の「KMS の構成」を参照してください。
手順 4	キーの作成	p.514 の「外部 KMS でのキーの作成」を参照してください。
手順 5	ストレージの設定	詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。
手順 6	ポリシーの設定	詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

KMS クレデンシャルの検証

NetBackup で誤ったクレデンシャルが設定されている場合、外部 KMS サーバーとの通信が失敗することがあります。このようなエラーを回避するために、KMS で使用するクレデンシャルを構成できるようにするために、特定の検証を実行できます。検証チェックにパスしない場合、クレデンシャルは設定できません。

次の検証は、新しいクレデンシャルを構成するか、既存のクレデンシャルを更新している間に実行されます。いずれかのチェックが失敗した場合、クレデンシャルを設定することはお勧めしません。

- 証明書のパスは有効です。
- トラストストアのパスは有効です。
- 秘密鍵のパスは有効です。
- 証明書チェーン内の証明書は読み取り可能です。
- トラストストア内の証明書は読み取り可能です。
- 秘密鍵は読み取り可能です。
- 一般名フィールドが空ではありません。
- 証明書の期限は切れていません。
- 証明書は現在有効です。

- 秘密鍵が証明書と一致しています。
- 証明書は適切な順序で並んでいます。
- ECA_CRL_PATH が設定されており、CRL の確認レベルが DISABLE 以外の場合は、次の CRL 検証チェックが実行されます。
  - CRL ディレクトリは CRL ファイルで構成されます。
  - CRL チェックレベルは有効です。
  - CRL パスは有効です。
  - 利用可能な CRL は読み取り可能です。

KMS クレデンシャルと KMS の互換性を検証するには

1 次のコマンドを実行します。

```
nbkmiputil -kmsServer kms_server_name -port port
-certPathcert_path -privateKeyPath private_key_path
-trustStorePathtrust_store_path -validate
```

この nbkmiputil コマンドは KMS サーバーへの接続を含む KMS 機能を検証します。

また、リストキー、フェッチキー、設定属性、フェッチ属性などの操作をテストします。設定属性には、KMS サーバーに対する書き込み権限が必要です。この nbkmiputil コマンドは、TLS ハンドシェークによって交換されるサーバー証明書の CA の指紋も検証します。nbkmiputil は、外部 KMS サーバーと安全に通信するために、TLS 1.2 以降のプロトコルを使用します

2 (この手順は条件付きです)。KMS ベンダーがサポート対象の KMS ベンダーとして NetBackup ハードウェア互換性リストに記載されていない場合に、ベンダーの NetBackup との互換性を確認するには、次のコマンドを使用します。

このコマンドを実行するには、外部 KMS サーバーの「書き込み」権限が必要です。このコマンドは、外部 KMS サーバーに 8 つの対称キーを作成し、互換性を確認するためにさまざまな KMIP 操作を実行します。互換性チェックの後、作成されたキーを明示的に削除する必要があります。

3 NetBackup プライマリサーバーが KMS ベンダーと互換性があり、KMIP プロトコルを使用して KMS ベンダーと通信できることを確認します。次のコマンドを実行します。

```
nbkmiputil -kmsServer kms_server_name -port port
-certPathcert_path -privateKeyPath private_key_path
-truststorepathtrust_store_path -ekmsCheckCompat
```

-ekmsCheckCompat オプションを実行して、ご利用の環境で KMS を正常に構成できるかどうかを確認することを推奨します。

このオプションを使用すると、指定した KMS サーバーに 8 個のテストキーが作成されます。その後、手動でこれらのキーを削除できます。

4 チェックが失敗した場合は、ベリタステクニカルサポートにお問い合わせください。

KMS クレデンシャルの構成

NetBackup で外部 KMS を構成するには、NetBackup が外部 KMS サーバーの認証に使用するクレデンシャルをまず構成する必要があります。この手順の一環として、証明書ベースの認証に必要な公開鍵基盤 (PKI) アーティファクトのパスを指定する必要があります。次の情報が必要です。

- 証明書ファイルのパス
- キーストアファイルパス
- トラストストアファイルのパス
- パスフレーズまたはパスフレーズファイルのパス

メモ: 外部 KMS の構成またはキーの更新後、NetBackup では、バックアップまたはリストアのワークフローで適切なキーを使用するため、時間がかかる場合があります。これは、NetBackup によるキーのキャッシュに 10 分程度 (外部 KMS の場合) 時間がかかるためです。キーを即座に使用するには、対応するメディアサーバーで次のコマンドを実行してキャッシュをクリアします。

```
bpclntcmd -clear_host_cache
```

KMS クレデンシャルを構成するには

◆ 次のコマンドを実行します。

```
nbkmscmd -configureCredential -credName credential_name -certPath
certificate_file_path -privateKeyPath private_key_file_path
-trustStorePath CA_certificate_file_path [-passphrasePath
private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN |
DISABLE] [-server master_server_name] [-description description]
```

KMS クレデンシャルの一覧表示

すべてのクレデンシャルの詳細を一覧表示するには

- 次のコマンドを実行します。

  ```
  nbkmscmd -listCredential
  ```

特定のクレデンシャルの詳細を一覧表示するには

- 次のコマンドを実行します。

```
nbkmscmd -listCredential -credName credential_name
```

KMS クレデンシャルの更新

クレデンシャルの詳細を更新するには

- 次のコマンドを実行します。

  ```
  nbkmscmd -updateCredential -credName credential_name -certPath
  certificate_file_path -privatekeyPath private_key_file_path
  -trustStorePath CA_certificate_file_path -crlCheckLevel DISABLE
  ```

KMS クレデンシャルの削除

クレデンシャルの詳細を削除するには

- 次のコマンドを実行します。

  ```
  nbkmscmd -deleteCredential -credName credential_name
  ```

KMS の構成

NetBackup KMS (NBKMS) を構成するには

- 次のコマンドを実行します。

  ```
  nbkmscmd -configureKMS -name configuration_name -type NBKMS -hmkId
  host_master_key_ID_to_identify_HMK_passphrase -kpkId
  key_protection_key_ID_to_identify_KPK_passphrase
  [-useRandomPassphrase 0 | 1] [-enabledForBackup 0 | 1] [-priority
  priority_of_KMS_server] [-server master_server_name] [-description
  description]
  ```

外部 KMS を構成するには

◆ 次のコマンドを実行します。

```
nbkmscmd -configureKMS -name configuration_name -type KMIP -port
port_to_connect_to_external_KMS_server -kmsServerName
network_name_of_external_KMS_server -credId credential_ID |
-credName credential_name [-enabledForBackup 0 | 1] [-priority
priority_of_KMS_server] [-server master_server_name] [-description
description]
```

KMS 構成の一覧表示

すべての KMS サーバーの構成の詳細を一覧表示するには

◆ 次のコマンドを実行します。

```
nbkmscmd -listKMSConfig
```

特定の KMS サーバーの構成の詳細を一覧表示するには

◆ 次のコマンドを実行します。

```
nbkmscmd -listKMSConfig -name configuration_name
```

KMS 構成の更新

KMS の優先度の更新

KMS の優先度を更新するには、次のコマンドを実行します: `nbkmscmd -updateKMSConfig -name configuration_name -priority priority`

バックアップの KMS 構成の無効化

指定した KMS からバックアップに使用されるキーを無効にするには、次のコマンドを実行します: `nbkmscmd -updateKMSConfig -name configuration_name -enabledForBackup 0`

メモ: 外部 KMS の構成またはキーの更新後、NetBackup では、バックアップまたはリストアのワークフローで適切なキーを使用するため、数分かかる場合があります。これは、NetBackup によるキーのキャッシュに 10 分程度 (外部 KMS の場合) 時間がかかるためです。キーを即座に使用するには、対応するメディアサーバーで次のコマンドを実行してキャッシュをクリアします。

```
bpclntcmd -clear_host_cache
```

KMS 構成の削除

KMS 構成を削除するには、次のコマンドを実行します: `nbkmscmd -deleteKMSConfig -name configuration_name`

NetBackup 消費用の外部 KMS でのキーの構成

NetBackup は、外部 KMS ですでに作成されているキーを使用できます。または、NetBackup を使用して外部 KMS でキーを作成できます。このために、NetBackup プライマリサーバーにキーを作成する権限を付与する必要があります。

NetBackup は、外部 KMS で作成されたキーを NetBackup での使用のために検出できます。キーの生成中にカスタム属性 `x-application` および `x-keygroup` を指定するか、これらの属性を既存のキーに関連付けて、NetBackup が使用するキーを判断できるようにします。NetBackup は、暗号化の目的でこれらの属性を持つ任意のキーを使用します。

テープボリュームプールのキーグループ名には、接頭辞 `ENCR_` を付ける必要があります。

次の例を考えてみます。テープボリュームプールを `ENCR_P1` という名前で構成します。このボリュームプール名は、このボリュームプールのバックアップイメージが暗号化されることを示します。

`x-keygroup` では大文字と小文字が区別され、ボリュームプール名と正確に一致する必要があります。

キーを設定するには

1. カスタム属性 `x-keygroup` とその値を `ENCR_P1` として使用して、外部 KMS にキーを作成します。
2. このキーが NetBackup に属していることを示すために、カスタム属性 `x-application` をその値 `NetBackup` として設定します。

3 すでに作成され、このボリュームプールの暗号化に使用されるキーについては、カスタム属性を作成できます。

4 これらの属性を設定するには、それぞれの KMS ベンダーが指定したユーザーインターフェースを使用できます。

KMS ベンダーのユーザーインターフェースでカスタム属性の追加と設定がサポートされていない場合は、nbkmiputil コマンドを使用してキーの属性を設定できます。

```
nbkmiputil -kmsServer kms_server_name -port 5696 -certPath
cert_path -privateKeyPath private_key_path -trustStorePath
caCertificatePath -setAttribute -attributeName attributeName
-attributeValue attributeVal
```

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。

外部 KMS でのキーの作成

NetBackup を使用して、外部 KMS にキーを作成できます。NetBackup には、外部 KMS でキーを作成するために必要な権限がある必要があります。

外部 KMS でキーを作成するには

◆ 次のコマンドを実行します。

```
nbkmscmd -createkey -name configuration_name -keyGroupName
keygroup_name -keyName key_name -comment comments
```

createKey コマンドを実行すると、有効な状態のキーが作成されます。外部 KMS の場合、キーグループに複数のアクティブなキーを含めることができます。NetBackup は、最新の有効なキーを使用します。このコマンドは、キーに必要なすべての属性も設定します。

メモ: 外部 KMS の構成またはキー関連の変更の更新後、NetBackup では、バックアップまたはリストアのワークフローで適切なキーを使用するため、時間がかかる場合があります。これは、NetBackup によるキーのキャッシュに 10 分程度 (外部 KMS の場合) 時間がかかるためです。キーを即座に使用するには、対応するメディアサーバーで次のコマンドを実行してキャッシュをクリアします。

```
bpclntcmd -clear_host_cache。
```

キーのリスト作成

指定された手順を使って、指定した KMS からキー ID を一覧表示します。

キー ID を一覧表示するには

- `nbkmscmd -listKeys -name configuration_name`

ストレージ構成時のキーグループ名の確認

NetBackup は、ストレージの構成時に、外部 KMS の事前構成済みキーを使用します。

キーが属性 `x-keygroup` で外部 KMS サーバーに作成され、キーグループ名に割り当てられていることを確認します。

すべてのストレージ構成で、NetBackup はキーグループ名を次のように指定します。

MSDP	キーグループ名を指定します。
クラウド	キーグループ名は *Name_of_storage_server*:*Name_of_disk_volume* です。
テープ	ボリュームプール名がキーグループ名として使用されます。 テープの場合、ボリュームプールには接頭辞として `ENCR` を付ける必要があります。
AdvancedDisk	UNIX の場合: *Name_of_storage_server*:*Name_of_disk_volume* Windows の場合: *Name_of_storage_server*

複数の KMS サーバーでの作業

NetBackup は、複数の KMS サーバーをサポートします。複数の KMS サーバーを使用して、1 台の KMS サーバーから別の KMS サーバーに移行できます。また、テープ、クラウド、MSDP などのストレージ構成ごとに個別の KMS サーバーを使用できます。

p.516 の「1 台の KMS サーバーの別の KMS サーバーへの移行」を参照してください。

p.517 の「ストレージ構成ごとの個別の KMS サーバーの使用」を参照してください。

複数の KMS サーバーを効果的に使用するには、次の KMS 構成属性を定義する必要があります。

enableForBackup　この KMS のキーをバックアップに使用するべきかどうかを指定します。デフォルト値は 1 です。

この KMS サーバーのキーをバックアップに使用しない場合は 0 を指定します。

この属性はリストアには影響しません。この KMS のキーを使用して暗号化されたバックアップイメージがある場合は、リストア時に NetBackup はこの KMS サーバーを使用して、データをリストアするためのキーをフェッチします。これらの KMS サーバーは、引き続きイメージのリストアに使用できます。したがって、KMS の構成を削除する場合は、この KMS サーバーのキーで暗号化されたイメージがないことを確認します。キーが失われた場合、そのイメージからデータはリストアできず、データが失われます。KMS サーバーの移行中に、少なくとも 1 つの KMS 構成でこのプロパティを 1 に設定する必要があります。そうしないと、すべてのバックアップが失敗します。

priority　NetBackup が暗号化または復号中にキーの確認に使用する KMS サーバーを指定します。デフォルトでは KMS サーバーの優先度は 0 に設定されます。最高値の KMS サーバーが暗号化または復号中に最初に優先されます。

バックアップまたはリストアの間に、NetBackup はキーの取得の優先度に基づいて、KMS サーバーの順序付きリストを使用します。したがって、最も優先度の高い KMS が最初に使われてキーが取得されます。複数の KMS サーバーが同じ優先度を持っている場合は、そのうちの 1 つを使用します。

NetBackup で (CLI または API を使用して) KMS を設定するときに、これらの属性の値を選択できます。これらの属性を設定するためのオプションは、`nbkmscmd` CLI 操作の `configureKMS` および `updateKMSConfig` オプションで利用可能です。

p.511 の「KMS の構成」を参照してください。

p.512 の「KMS 構成の更新」を参照してください。

1 台の KMS サーバーの別の KMS サーバーへの移行

環境内で KMS サーバーが設定されていて (NetBackup KMS - KMS1 など)、別の KMS サーバー (外部 KMS - KMS2) に移行する場合は、次の手順を実行します。

1 台の KMS サーバー (KMS1) から別の KMS サーバー (KMS2) に移行するには

1. 必要なキーを KMS2 で作成して、暗号化が有効になっているドメイン内のすべてのストレージプールについて KMS2 にキーが設定されているようにします。
2. 次のコマンドを実行して、NetBackup に KMS2 の構成を追加します。

   ```
   nbkmscmd -configureKMS -name KMS2 -type KMIP -port
   port_to_connect_to_external_KMS_server -kmsServerName
   network_name_of_external_KMS_server -credId credential_ID
   -credNamecredential_name  -enabledForBackup 1 -priority
   priority_of_KMS_server -server master_server_name -description
   description
   ```

3. 次のコマンドを実行して、KMS1 の enabledForBackup フラグを更新します。

   ```
   nbkmscmd -updatekmsconfig -name KMS1 -enabledForBackup 0
   ```

   この結果、KMS1 のキーを使用したバックアップの暗号化は行われません。キーが必須で、KMS2 に見つからない場合、NetBackup は KMS1 にフォールバックされません。
4. 既存のバックアップイメージが KMS1 を使用して暗号化されていないことを確認します。
5. NetBackup の構成から KMS1 構成を削除します。

   削除された KMS サーバー (KMS1) を使用して暗号化されたイメージがある場合、そのようなイメージからデータをリストアすることはできません。KMS サーバー (KMS1) を再構成し、データをリストアする前に、その KMS サーバーでそれぞれのキーが利用可能であることを確認します。

ストレージ構成ごとの個別の KMS サーバーの使用

ストレージ構成ごとに、異なる KMS サーバーを使用する場合があります。たとえば、テープストレージに 1 台の KMS サーバーを使用し、クラウドストレージに別のサーバーを使用できます。また、異なるテープボリュームまたは異なる MSDP ストレージサーバーに対して個別の KMS サーバーを使用することもできます。

NetBackup は、キーグループからキーを検索します。各キーグループは 1 つのストレージに関連付けられます。たとえば、暗号化が有効になっているすべてのテープボリュームには、対応するキーグループがあります。

テープとクラウドストレージに個別の KMS サーバーを使用するには

1 1 番目の KMS の構成を NetBackup に追加します (KMS1)。KMS1 の enableForBackup 属性のデフォルト値は 1 です。

2 2 番目の KMS の構成を NetBackup に追加します (KMS2)。KMS2 の enableForBackup 属性のデフォルト値は 1 です。

p.511 の「KMS の構成」を参照してください。

3 KMS1 のテープに必要なすべてのキーグループとキーを作成します。どのキーグループもクラウドストレージに対応していないことを確認します。

4 KMS2 のクラウドストレージに必要なすべてのキーグループとキーを作成します。どのキーグループもテープに対応していないことを確認します。

p.513 の「NetBackup 消費用の外部 KMS でのキーの構成」を参照してください。

p.514 の「外部 KMS でのキーの作成」を参照してください。

5 構成を検証するには、テープとクラウドストレージを使用してバックアップを実行します。

テープとクラウド形式の暗号化対応ストレージサーバーでは、異なる KMS サーバーが使用されます。バックアップの間に、NetBackup は、注文された KMS リストをフェッチし、最初の KMS サーバーでキーグループを検索し、次にもう一方の KMS サーバーで検索します。

したがって、KMS1 が KMS2 よりも優先度が高い場合は、最初に KMS1 で必要なキーが検索されます。クラウドストレージでバックアップを実行する場合でも、キー要求は最初に KMS1 で、次に KMS2 で実行されます。したがって、KMS1 にクラウドストレージに対応するキーグループがないことを確認する必要があります。

リストア時にも、優先度に基づいて利用可能な KMS サーバーでキーが検索されます。

バックアップおよびリストア時の外部 KMS の使用

バックアップ

バックアップ時の KMS ワークフロー

1 バックアップジョブを実行する場合、メディアサーバーは、キーグループ名またはディスクプール名に基づいて KMS Web サービスにキー要求を送信します。

2 外部 KMS サーバーのキーは、属性 x-keygroup を使用して作成されます。

テープボリュームプールのキーグループ名には、接頭辞 ENCR_ を付ける必要があります。

3 KMS Web サービスは外部 KMS サーバーに接続し、カスタム属性 x-keyGroup のアクティブなキーが存在するかどうかを検証します。キーが存在する場合、そのキーが取得され、メディアサーバーに返されます。

4 外部 KMS が構成されていない場合、または外部 KMS でそのようなキーを利用できない場合、Web サービスはキー参照のために nbkms にフォールバックします。

リストア

リストア時の KMS ワークフロー

1 リストア時に、メディアサーバーはキー ID または KAD (キーに関連付けられたデータ) を KMS Web サービスに送信してキーを取得します。

2 KMS Web サービスは、すべての KMS サーバーに接続し、KAD に一致する可能性のあるすべてのキーを取得します。

3 メディアサーバーはすべてのキーを使用して一致するキーを見つけ、そのキーを使用してイメージを復号します。

4 KMS が構成されていてバックアップとリストアに使用される場合、テープ、AdvancedDisk、クラウドストレージのタイプについて、ジョブの詳細で KMS 構成の詳細を確認できます。

メモ: MSDP の場合、KMS 構成の詳細はジョブの詳細に表示されません。

キーのローテーション

外部 KMS を使用すると、アクティブ状態のキーグループに 1 つ以上のキーを持つことができます。NetBackup は、データの暗号化のため、アクティブなキーから常に最新のキーを選択します。暗号化用にキーを変更する場合 (キーのローテーション) は、特定のキーグループに新しいアクティブなキーを作成します。そのキーグループに対する以降の暗号化要求には、最も新しく作成されたキーが使われます。

メモ: 外部 KMS の構成またはキーの更新後、NetBackup では、バックアップまたはリストアのワークフローで適切なキーを使用するため、時間がかかる場合があります。これは、NetBackup によるキーのキャッシュに 10 分程度 (外部 KMS の場合) 時間がかかるためです。

キーを即座に使用するには、対応するメディアサーバーで次のコマンドを実行してキャッシュをクリアします。

```
bpclntcmd -clear_host_cache
```

外部 KMS サーバーを使用してカタログバックアップを暗号化する場合のディザスタリカバリ

カタログバックアップの一部として、ディザスタリカバリ (DR) パッケージ情報を含む電子メール通知が送信されます。カタログバックアップイメージが暗号化されている場合、電子メールには KMS 情報も含まれています。カタログのリストアを実行する前に、電子メールに記載されている KMS サーバーを構成する必要があります。

外部 KMS サーバーを使用してカタログバックアップを暗号化する場合にカタログをリストアするには

1. 適切な DR パッケージを使用して NetBackup をインストールします。
2. ディザスタリカバリの電子メールには、次のように KMS 固有の情報が含まれています。

   ```
   The primary server ms1.example.veritas.com is configured to use
   the following Key Management Servers.

   KMS Server Name = kms1.example.veritas.com, KMS Server Type =
   KMIP

   KMS Server Name = kms2.example.veritas.com, KMS Server Type =
   KMIP

   KMS Server Name = ms1.example.veritas.com, KMS Server Type = NBKMS
   ```

   電子メールに一覧表示されている KMS サーバーを構成します。
3. カタログリストアを実行します。

   『NetBackup トラブルシューティングガイド』を参照してください。

KMS クレデンシャルの有効期限に関するアラート

NetBackup は、クレデンシャルマネージャサービスに格納されている証明書を使用して、KMS サーバーに接続します。この証明書の有効期限が切れている場合、ジョブは失敗します。ジョブのエラーを回避するため、クレデンシャル証明書の有効期限が近づくと送信されるように通知を構成できます。

通知の構成について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

24

安全な通信のために NetBackup で使用される暗号

この章では以下の項目について説明しています。

NetBackup で使用される暗号

このセクションでは、安全な通信のために NetBackup が使用する暗号の一覧を示します。

表 24-1 Web アクセスに NetBackup で使用される暗号

製品	ローカルアカウントのパスワードの暗号化	Web アクセス	
		接続	有効な伝送暗号
NetBackup 10.x	NetBackup では通常、ローカルアカウントは使用されません。代わりに、ローカル OS または外部 ID プロバイダ (SAML、AD、LDAP) で定義されているアカウントが使用されます。	TLSv1.2	Web サービス (ポート 443 と 1556): ECDHE_RSA_WITH_AES_128_GCM_SHA256 DHE_RSA_WITH_AES_128_GCM_SHA256 ECDHE_RSA_WITH_AES_256_GCM_SHA384 DHE_RSA_WITH_AES_256_GCM_SHA384 安全な通信 (制御とデータチャネル): ECDHE-RSA-AES256-GCM-SHA384 RabbitMQ (ポート 13781): ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384

表 24-2 認証に NetBackup で使用される暗号

製品	ローカルアカウントのパスワードの暗号化	認証サービスの接続		
		Active Directory ドメインコントローラ	LDAP 認証	暗号
NetBackup 10.2	NetBackup では通常、ローカルアカウントは使用されません。代わりに、ローカル OS または外部 ID プロバイダ (SAML、AD、LDAP) で定義されているアカウントが使用されます。	構成されている場合、NetBackup では Openldap を使用して LDAP または AD サーバーに直接接続します。LDAP と LDAPS (TLS を介した LDAP) の両方がサポートされます。	単純認証	ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSA-AES256-SHA

表 24-3 格納データの暗号化に NetBackup で使用される暗号

製品	ローカルアカウントのパスワードの暗号化	格納データの暗号化	
		ハードウェアまたはソフトウェアベースの暗号化	暗号
NetBackup 10.x	NetBackup では通常、ローカルアカウントは使用されません。代わりに、ローカル OS または外部 ID プロバイダ (SAML、AD、LDAP) で定義されているアカウントが使用されます。	テープドライブの暗号化を除くソフトウェアベース	MSDP: AES-256-CTR レガシークラウドコネクタと Advanced Disk Crypt: AES-256-CFB クライアントの暗号化 (お客様が選択): AES-128-CFB (デフォルト) BF-CFB DES-EDE-CFB AES-256-CFB テープドライブの暗号化 (ハードウェアベース): AES-256

25

NetBackup での FIPS 準拠

この章では以下の項目について説明しています。

FIPS について

FIPS (連邦情報処理標準) には米国連邦政府とカナダ政府のコンピュータシステムに対するセキュリティと相互運用性の必要条件が定義されています。FIPS 140-2 標準には暗号化モジュールのセキュリティ必要条件が明記されています。対称キー暗号化と非対称キー暗号化、メッセージ認証、ハッシュの承認済みセキュリティ機能について説明しています。FIPS 140-2 標準とその検証プログラムについて詳しくは、次の米国標準技術研究所 (NIST) とカナダの通信セキュリティ機構 (CSEC) の暗号化モジュール検証プログラム Web サイトを参照してください。

http://csrc.nist.gov/groups/STM/cmvp

NetBackup での FIPS のサポートについて

NetBackup では、FIPS モードはデフォルトで無効になっています。

FIPS 準拠モードでは、次の作業負荷がサポートされます。

- Oracle、MS-SQL、SAP HANA、DB2、VMware、Hyper-V、RHV、Nutanix、DynamicNAS、MongoDB、Hadoop、HBase、MySQL、PostgreSQL、SQLite、MariaDB、SharePoint
- Cassandra、Sybase、Informix、MS-Exchange、Enterprise Vault、BMR、ユニバーサル共有、OpenStack (クラウドベースのソリューション)

FIPS モードでは、次のオペレーティングシステムレベルのサポートが利用可能です。

- RHEL 8 で FIPS モードを有効にすると、各 RPM パッケージに SHA-256 ダイジェストが含まれていることがオペレーティングシステムで必要になります。このダイジェストを含まない RPM はインストールに失敗します。RHEL 6 または RHEL 7 プラットフォームに存在するネイティブツールチェーンを使用して構築された RPM には、SHA-256 ダイジェストが含まれていないため、FIPS モードが有効な場合に RHEL 8 へのインストールに失敗する場合があります。この問題は、NetBackup 9.1 以前のセットアップに影響します。これらのバージョンのパッケージは RHEL 7 以前の OS ネイティブツールチェーンを使用して構築されているためです。
  NetBackup 10.0 以降では、パッケージは SHA-256 ダイジェストを追加するツールチェーンを使用して構築されているため、FIPS モードが有効になっている RHEL 8 にインストールできます。

次のコンポーネント、構成、操作は FIPS モードではサポートされません。

- クライアント側の暗号化

  メモ: クライアント側の暗号化を使用してバックアップを実行するには、クライアントホストで FIPS モードを無効にする必要があります。

- NDMP バックアップ
- NetBackup 内で実行されるスクリプト (Perl、バッチ、シェル、Python)
- バイナリまたはユーティリティ: `restore_spec_utility`、`nbcallhomeproxyconfig`、`nbbsdtar`、`nbrepo`
- NBAC が有効な NetBackup ドメイン
  NetBackup ドメインで NBAC が構成されている場合は、FIPS モードを有効にしないことをお勧めします。

- MQBROKER プロセスは、Windows の NetBackup レベルの FIPS 構成をサポートしません。
- Hadoop と HBase で使用される MIT Kerberos は、FIPS 対応の OpenSSL では動作しません。Kerberos 認証を使用してバックアップを実行するには、バックアップホストで FIPS を無効にする必要があります。
- NetBackup CloudPoint は、FIPS モードで構成されている CloudPoint ホストをサポートしません。
- SharePoint は、FIPS 標準に準拠していない暗号化アルゴリズムを内部的に使用します。Windows の FIPS ポリシーは、SharePoint が使用する MD5 ハッシュアルゴリズムを遮断します。したがって、SharePoint のリストアを正常に実行するには、その操作に対する OS レベルの FIPS ポリシーを無効にする必要があります。
  SharePoint の保護では NetBackup-FIPS がサポートされることに注意してください。
  詳しくは、次の記事を参照してください。
  FIPS と SharePoint Server
  SharePoint 2016 と FIPS

前提条件

NetBackup 環境内で FIPS を構成する前に、指定した前提条件を確認します。

- NetBackup ドメインおよび NetBackup クライアントで FIPS モードを有効にする前に、次のことを確認します。
  - NetBackup プライマリサーバーとメディアサーバーが 10.0 以降である。
  - NetBackup クライアントが 8.1 以降である。
  - FIPS のサポート情報を確認済みである。
    p.525 の「NetBackup での FIPS のサポートについて」を参照してください。

メモ: FIPS モードが有効で、バックアップのターゲットがメディアサーバー重複排除プール (MSDP) である場合、システムの CPU 消費が増加する可能性があります。

- FIPS モードが有効な場合に NetBackup プロセス間でシームレスな SSL 通信を行う場合は、次のことを確認します。
  - NetBackup CA の秘密鍵が FIPS 準拠の暗号化形式 (PKCS 8) である。
  - 秘密鍵が RSA などの FIPS 準拠アルゴリズムで生成されている。
  - NetBackup CA の秘密鍵の強度が 2048 ビットまたは 3072 ビットに設定されている。
    秘密鍵の強度がサポート対象の値と一致しない場合は、CA を移行します。
    p.343 の「NetBackup CA の移行」を参照してください。

外部 CA を構成している場合は、関係するセキュリティ管理者にお問い合わせください。

p.384 の「NetBackup での外部 CA のサポートについて」を参照してください。

- 進行中の NetBackup CA 移行プロセスが完了している。

警告: 前提条件が満たされない場合、NetBackup の機能が一部動作しない可能性があります。

NetBackup でのエントロピーランダム性の指定

コンピューティングでのエントロピーとは、オペレーティングシステムまたはアプリケーションが、暗号化や、ランダムデータを必要とするその他の用途で使用するために収集するランダム性です。

この要件は Linux プラットフォームと Java ベースのプログラムまたはプロセスでのみ必要です。

どのランダム性を使用するかは、JVM 引数で指定する必要があります。指定しない場合、デフォルトでは `dev/random` が使用されます。

Java プログラムに対しては、次が JVM 引数として指定されます:

```
-DjavaDjava.security.egd=file:/dev/./random
```

`use_urandom` 構成オプションを有効にして `dev/urandom` を活用し、サービスを再起動するか、NetBackup 管理コンソールを再起動します。

p.537 の「NetBackup サーバーとクライアントの USE_URANDOM」を参照してください。

NetBackup ドメインでの FIPS モードの構成

このセクションでは、NetBackup ドメインで FIPS モードを有効にする手順について説明します。手順を続行する前に、使用環境で前提条件が満たされていることを確認してください。

p.526 の「前提条件」を参照してください。

p.525 の「NetBackup での FIPS のサポートについて」を参照してください。

インストール時の NetBackup での FIPS モードの構成

インストール時に NetBackup で FIPS モードを構成できます。次のトピックを参照してください。

1. p.528 の「インストール時の NetBackup での FIPS モードの有効化」を参照してください。

2. p.531 の「NetBackup 管理コンソールの FIPS モードの有効化」を参照してください。

インストール後の NetBackup での FIPS モードの構成

インストール後に NetBackup で FIPS モードを構成できます。次のトピックを参照してください。

メモ: 必要に応じて、すべての NetBackup ホストで必須の構成手順が実行されていることを確認します。

---

1. NetBackup ドメイン内の各ホストの FIPS モードを有効にします。

   p.528 の「インストール後の NetBackup ホストでの FIPS モードの有効化」を参照してください。

   - ホストがプライマリサーバーの場合は、次の手順を実行する必要があります。
     プライマリサーバーの `VRTSatlocal.conf` 構成ファイルを更新して、NetBackup 認証ブローカー (AT) に対して FIPS モードを有効にする必要があります。
     p.530 の「NetBackup 認証ブローカーサービスに対する FIPS モードの有効化」を参照してください。

2. NetBackup 管理コンソールに対して FIPS モードを有効化します。

   p.531 の「NetBackup 管理コンソールの FIPS モードの有効化」を参照してください。

インストール時の NetBackup での FIPS モードの有効化

NetBackup では、インストール時に FIPS モードを有効にできます。詳しくは、『NetBackup インストールガイド』を参照してください。

インストール時に NetBackup の FIPS モードを有効にした後、NetBackup 管理コンソールで FIPS モードを有効にします。

p.531 の「NetBackup 管理コンソールの FIPS モードの有効化」を参照してください。

インストール後の NetBackup ホストでの FIPS モードの有効化

このセクションでは、NetBackup ドメイン内のプライマリサーバー、メディアサーバー、またはクライアントで FIPS モードを有効にする手順について説明します。FIPS を有効にするには、各ホストで次の構成を行う必要があります。

ホストがプライマリサーバーの場合、プライマリサーバーの VRTSatlocal.conf 構成ファイルを更新して、NetBackup 認証ブローカー (AT) に対して FIPS モードを有効にします。

p.530 の「NetBackup 認証ブローカーサービスに対する FIPS モードの有効化」を参照してください。

NetBackup ホストで FIPS モードを有効にする方法

1 NetBackup 構成ファイルで NB_FIPS_MODE フラグを有効にします。

p.537 の「NetBackup サーバーとクライアントの NB_FIPS_MODE オプション」を参照してください。

2 NetBackup サービスを再起動します。

特定のデーモンまたはコマンドが FIPS モードで実行されているかどうかを確認するために、それぞれのログを確認します。ログ行は暗号化を使用するデーモンとコマンドでのみ利用できます。

例 1: nbcertcmd コマンドが FIPS モードで実行されているかどうかを確認するには

1 次のコマンドを実行します。

```
nbcertcmd -ping
```

コマンドの場所:

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

UNIX の場合: /usr/openv/netbackup/bin/nbcertcmd

2 nbcertcmd ログを確認します。

ログディレクトリの場所:

Windows の場合: *install_path*¥NetBackup¥logs¥nbcert

UNIX の場合: /usr/openv/netbackup/logs/nbcert

次のログ行があるはずです。

```
<2> nbcertcmd: ./nbcertcmd -ping ProcessContext: ProcessName:[nbcertcmd],
FipsMode:[ENABLED], Username:[root], IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

例 2: NetBackup Web Management Console が FIPS モードで実行されているかどうかを確認するには

- デフォルトでは、FIPS モードは NetBackup Web Management Console (nbwmc) サービスの実行中は無効です。FIPS モードは、NetBackup ホスト用に有効にした後、nbwmc サービスに対して有効になります。

  NetBackup プライマリサーバーホストの catalina ログファイルを調べ、nbwmc サービスが FIPS モードで動作しているかどうかを確認します。

  ログファイルの場所:

  Windows の場合:
  install_path¥NetBackup¥wmc¥webserver¥logs¥catalina-*date*.log

  UNIX の場合: /usr/openv/wmc/webserver/logs/catalina-*date*.log

  次のログ行があるはずです。

  ```
  The nbwmc service is running in FIPS approved mode
  ```

NetBackup 認証ブローカーサービスに対する FIPS モードの有効化

NetBackup 認証ブローカーサービス (nbatd) は NetBackup プライマリサーバーでのみ実行されるため、nbatd サービスに対して FIPS モードを有効にするには、プライマリサーバーで有効にする必要があります。

デフォルトでは、FIPS モードは無効になっています。

nbatd サービスの FIPS モードを有効にするには

1. プライマリサーバーで次のディレクトリを開きます。

   UNIX の場合: `/usr/openv/netbackup/sec/at/bin/`

   Windows の場合: *install_path*¥NetBackup¥sec¥at¥bin¥

2. 次のコマンドを実行します。

   UNIX の場合:
   ```
   run vssregctl -s -f
   /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
   -b "Security¥Authentication¥Client" -k FipsMode -t int -v 1
   ```

   Windows の場合:
   ```
   run vssregctl -s -f
   "install_path¥NetBackup¥var¥global¥vxss¥eab¥data¥systemprofile¥VRTSatlocal.conf"
   -b "Security¥Authentication¥Client" -k FipsMode -t int -v 1
   ```

   例:

   install_path の場所が「`"C:¥Program Files¥VERITAS"`」の場合は、Windows で次のコマンドを実行します。

   ```
   vssregctl -s -f "C:¥Program
   Files¥VERITAS¥NetBackup¥var¥global¥vxss¥eab¥data¥systemprofile¥VRTSatlocal.conf"
   -b "Security¥Authentication¥Client" -k FipsMode -t int -v 1 3
   ```

   nbatd ログを確認します。

   nbatd ログの場所:

   UNIX の場合:

   ```
   /usr/openv/logs/nbatd
   ```

   Windows の場合:

   ```
   install_path¥NetBackup¥logs¥nbatd
   ```

   次のログ行があるはずです。

   ```
   *** Trying to start Broker In FIPS mode ***

   *** Broker In FIPS mode already ***
   ```

3. NetBackup サービスを再起動します。

NetBackup 管理コンソールの FIPS モードの有効化

デフォルトでは、NetBackup 管理コンソールの FIPS モードは無効になっています。

NetBackup 管理コンソールの FIPS モードを有効にするには (ローカルホストまたはリモートホスト)

1. NetBackup 管理コンソールの構成ファイルを開きます。
   - Windows コンピュータでは、`install_path¥java¥nbj.conf` に、NetBackup 管理コンソールの構成オプションが含まれています。
   - UNIX コンピュータでは、`/usr/openv/java/nbj.conf` ファイルに、NetBackup 管理コンソールの構成オプションが含まれています。
2. 構成ファイルで `NB_FIPS_MODE` オプションを有効にします。次の形式を使用します。

   ```
   NB_FIPS_MODE = true
   ```
3. 変更を保存します。
4. NetBackup 管理コンソールを再起動します。

NetBackup 管理コンソールが FIPS モードで実行されているかどうかを確認するには

◆ NetBackup 管理コンソールのログを確認します。

ログの場所:

Windows の場合:
`install_path¥logs¥user_ops¥nbjlogs¥jbp.root.jnbSA.pid.log`

UNIX の場合:
`/usr/openv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA. pid.log`

スタンドアロンコンソールで、ディレクトリ構造を作成し、ログを確認します。

ログファイルに次のログ行が含まれる場合は、コンソールが FIPS モードで実行されることを意味します。

```
com.safelogic.cryptocomply.fips.approved_only: true
```

次のログ行があるはずです。

```
JavaPresentationLayer- FIPS mode enforced. Reconfiguring SunJSSE.

JavaPresentationLayer- Administration console is running in FIPS
 approved mode
```

メモ: この FIPS モード構成は、NetBackup KMS の FIPS モードには影響しません。デフォルトでは、NetBackup KMS は引き続き FIPS モードで動作します。

NetBackup に対する FIPS モードの無効化

NetBackup ドメインで FIPS モードを無効にするには、次の構成が必要です。

- 各 NetBackup ホストの FIPS モードを無効にします。
  p.533 の「NetBackup ホストに対する FIPS モードを無効にする」を参照してください。
- NetBackup 認証ブローカー (nbatd) サービスの FIPS モードを無効にします。
  p.534 の「NetBackup 認証ブローカー (nbatd) に対する FIPS モードを無効にする」を参照してください。
- NetBackup 管理コンソールの FIPS モードを無効にします。
  p.536 の「NetBackup 管理コンソールの FIPS モードの無効化」を参照してください。

NetBackup ホストに対する FIPS モードを無効にする

FIPS モードを無効にするには、各 NetBackup ホストで次の手順を実行します。

ホストに対する FIPS モードを無効にする方法

1. NetBackup 構成ファイルで NB_FIPS_MODE フラグを無効にします。

   p.537 の「NetBackup サーバーとクライアントの NB_FIPS_MODE オプション」を参照してください。
2. NetBackup サービスを再起動します。

特定のデーモンまたはコマンドに対して FIPS モードが無効かどうかを確認するには、それぞれのログを確認します。ログ行は暗号化を使用するデーモンとコマンドでのみ利用できます。

例 1: nbcertcmd コマンドに対して FIPS モードが無効かどうかを確認するには

1. 次のディレクトリに移動します。

   UNIX の場合: `/usr/openv/netbackup/bin`

   Windows の場合: *install_path*¥NetBackup¥bin
2. コマンド `nbcertcmd -ping` を実行します。

3 次のディレクトリにある nbcertcmd ログに移動します。

UNIX の場合: /usr/openv/netbackup/logs/nbcert

Windows の場合: *install_path*¥NetBackup¥logs¥nbcert

4 ログを確認してください。ログファイルには次のログ行が含まれているはずです。

```
ProcessContext: ProcessName:[nbcertcmd], FipsMode:[DISABLED],
Username:[root],
IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

例 2: NetBackup Web Management Console (nbwmc) サービスに対して FIPS モードが無効かどうかを確認するには

1 NetBackup サービスの FIPS モードを無効にすると、プライマリサーバーホストで実行されている nbwmc サービスの FIPS モードも無効になります。

NetBackup プライマリサーバーホストにある次のログファイルを開きます。

UNIX の場合: /usr/openv/wmc/webserver/logs/catalina-*date*.log

Windows の場合:
install_path¥NetBackup¥wmc¥webserver¥logs/catalina-*date*.log

2 ログファイルに次のログ行が含まれていることを確認します。

```
The nbwmc service is running in non-FIPS mode
```

NetBackup 認証ブローカー (nbatd) に対する FIPS モードを無効にする

NetBackup プライマリサーバーホストで実行される nbatd に対する FIPS モードを無効にするには、次の手順を実行します。

nbatd に対する FIPS モードを無効にする方法

1. プライマリサーバーで次のディレクトリを開きます。

   UNIX の場合:

   ```
   /usr/openv/netbackup/sec/at/bin/
   ```

   Windows の場合:

   ```
   install_path¥NetBackup¥sec¥at¥bin¥
   ```

2. 次のコマンドを実行します。

   UNIX の場合:

   ```
   run vssregctl -s -f
   /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
   -b "Security¥Authentication¥Client" -k FipsMode -t int -v 0
   ```

   Windows の場合

   ```
   run vssregctl -s -f
   "install_path¥NetBackup¥var¥global¥vxss¥eab¥data¥systemprofile¥VRTSatlocal.conf"
   -b "Security¥Authentication¥Client" -k FipsMode -t int -v 0
   ```

   Windows で install_path が "C:¥Program Files¥VERITAS" の場合は、次のコマンドを実行します。

   ```
   vssregctl -s -f "C:¥Program
   Files¥VERITAS¥NetBackup¥var¥global¥vxss¥eab¥data¥systemprofile¥VRTSatlocal.conf"
   -b "Security¥Authentication¥Client" -k FipsMode -t int -v 0
   ```

3. NetBackup サービスを再起動します。

nbatd サービスに対して FIPS モードが無効かどうかを確認するには

1. 次の nbatd ログに移動します。

   UNIX の場合:

   ```
   /usr/openv/logs/nbatd/
   ```

   Windows の場合:

   ```
   install_path¥NetBackup¥logs¥nbatd¥
   ```

2. ログファイルに次のログ行が含まれていることを確認します。

   ```
   Broker Not In FIPS mode
   ```

NetBackup 管理コンソールの FIPS モードの無効化

FIPS モードを無効にするには、各 NetBackup ホストで次の手順を実行します。

NetBackup 管理コンソールの FIPS モードを無効にするには (ローカルホストまたはリモートホスト)

1. NetBackup 管理コンソールの構成ファイルを開きます。

   Windows コンピュータでは、`install_path¥java¥nbj.conf` に、NetBackup 管理コンソールの構成オプションが含まれています。

   UNIX コンピュータでは、`/usr/openv/java/nbj.conf` ファイルに、NetBackup 管理コンソールの構成オプションが含まれています。

2. 構成ファイルで `NB_FIPS_MODE` オプションを無効にします。次の形式を使用します。

   NB_FIPS_MODE = false

3. 変更を保存します。

4. NetBackup 管理コンソールを再起動します。

NetBackup 管理コンソールの FIPS モードが無効かどうかを確認するには

- NetBackup 管理コンソールのログを確認します。

  ログの場所:

  UNIX の場合:
  `/usr/openv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA. pid.log`

  Windows の場合:
  `install_path¥logs¥user_ops¥nbjlogs¥jbp.root.jnbSA.pid.log`

  スタンドアロンコンソールで、ディレクトリ構造 (`C:¥Program Files¥Veritas¥NetBackup¥logs¥user_ops¥nbjlogs` など) を作成し、ログを確認します。

  ログファイルに次のログ行が含まれる場合は、コンソールに対して FIPS モードが無効であることを意味します。

  ```
  JavaPresentationLayer- Fips approved mode system property is -
  false
  JavaPresentationLayer- Administration console is running in
  non-FIPS mode
  ```

NetBackup サーバーとクライアントの NB_FIPS_MODE オプション

NB_FIPS_MODE オプションを使用して、NetBackup ドメインで FIPS モードを有効にします。

表 25-1 NB_FIPS_MODE 情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 デフォルトでは、NB_FIPS_MODE オプションは無効になっています。 このオプションを有効にするには、次の形式を使用します。 NB_FIPS_MODE = ENABLE このオプションを無効にするには、次の形式を使用します。 NB_FIPS_MODE = DISABLE
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。

NetBackup サーバーとクライアントの USE_URANDOM

コンピューティングでのエントロピーとは、オペレーティングシステムまたはアプリケーションが、暗号化や、ランダムデータを必要とするその他の用途で使用するために収集するランダム性です。

NetBackup 環境で暗号上安全なランダム出力を提供する文字型デバイスとして /dev/urandom オプションを指定するには、USE_URANDOM を有効にします。

表 25-2 USE_URANDOM の情報

使用方法	説明
使用する場所	NetBackup サーバーまたはクライアント上。

使用方法	説明
使用方法	オプションを表示、追加、変更するには、nbgetconfig コマンドと nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 USE_URANDOM オプションのデフォルト値は 0 です。USE_URANDOM オプションにデフォルト値が設定されている場合、使用される文字型デバイスは、NB_FIPS_MODE オプションの値に基づきます。NB_FIPS_MODE が有効な場合は、dev/random が使用されます。NB_FIPS_MODE が無効な場合は、dev/urandom が使用されます。 p.537 の「NetBackup サーバーとクライアントの NB_FIPS_MODE オプション」を参照してください。 USE_URANDOM オプションを有効にするには、次の形式を使用します。 USE_URANDOM = 1 USE_URANDOM が 2 に設定されている (または無効になっている) 場合は、暗号上安全なランダム出力を提供するために dev/random 文字型デバイスが使用されます。
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。

26

NetBackup Web サービスアカウント

この章では以下の項目について説明しています。

NetBackup Web サービスアカウントについて

NetBackup 8.0 より、NetBackup プライマリサーバーには、重要なバックアップ操作をサポートするための構成済み Web サーバーが含まれます。この Web サーバーは、権限が制限されているユーザーアカウント要素の下で動作します。これらのユーザーアカウント要素は、各プライマリサーバー (またはクラスタ化されたプライマリサーバーの各ノード) で使用できる必要があります。

NetBackup には、NetBackup プライマリサーバーのインストールの一環として、Web サービスのアカウント情報が必要です。

インストール前にこのアカウントを構成する方法と、インストール後にこのアカウントを変更する方法について、詳しい説明が利用できます。

Web サーバーのユーザーとグループを作成する方法については、『NetBackup インストールガイド』を参照してください。

p.540 の「Web サービスユーザーアカウントの変更」を参照してください。

メモ: セキュリティ上の理由から、Web サーバーのユーザーまたはグループに管理者権限またはスーパーユーザー権限を与えないでください。

Web サービスユーザーアカウントの変更

Web サービスユーザアカウントの変更をサポートするには、ユーティリティスクリプト wmcUtils を使用します。このユーティリティスクリプトは、Web サービスのユーザーとグループが存在するかどうかを検証しません。このユーティリティを使用する前に、Web サービスのユーザーとグループが存在し、ユーザーがグループの一部であることを確認する必要があります。Web サービスユーザーアカウントを変更するときは、次の点を考慮してください。

- 使用環境で Windows ドメインユーザーを使用している場合は、DOMAIN¥USER 形式を使用します。
- Windows プラットフォームでクラスタ環境を使用する場合、NetBackup Web サービスユーザーアカウントは DOMAIN ユーザーである必要があります。(例: AD ユーザー)
- クラスタ化されていない環境を使用する場合、NetBackup Web サービスユーザーはローカルユーザーまたはドメインユーザーにできます。
- Linux または UNIX プラットフォームでクラスタ環境を使用する場合、NetBackup Web サービスユーザーはローカルユーザーにできます。また、このグループはローカルグループにすることもできます。NetBackup Web サービスユーザーは、クラスタのすべてのノードで同じ名前と UID を持つ必要があります。同様に、グループもクラスタのすべてのノードで同じ名前と GID を持つ必要があります。クラスタ環境では、ドメインユーザー (例: NIS) を使用することを推奨します。

メモ: wmcUtils ユーティリティスクリプトを実行するために、ログオンしたユーザーを使用しないでください。*my_domain¥my_user* として環境にログインしている場合は、このアカウントを使用して NetBackup Web Management Consoleサービスを実行することはできません。NetBackup はこのシナリオをサポートしていません。

Windows 上で Web サービスユーザーアカウントを変更するには

1. コマンドプロンプトを起動します。
2. ディレクトリを *install_path*¥wmc¥bin¥install に変更します。
3. wmcUtils.bat -changeUser を実行して Web サービスユーザーを変更します。

   例: (nbwebsvc1 は Web サービスユーザーで、nbwebgrp1 は nbwebsvc1 がメンバーであるユーザーグループです)

   ```
   wmcUtils.bat -changeUser nbwebsvc1 nbwebgrp1
   ```

   wmcUtils.bat ユーティリティスクリプトについて詳しくは、wmcUtils.bat -help オプションを使用してください。
4. (該当する場合) クラスタ環境を使用する場合は、アクティブノードと非アクティブノードで wmcUtils.bat -changeUser を実行します。

5 スクリプトによりプロンプトが表示されたら、Web サービスのユーザーパスワード (例: nbwebsvc1) を入力します。

正しいパスワードが入力されると、NetBackup Web Management Consoleサービスが再開されます。正しくないパスワードを入力すると、NetBackup Web Management Consoleサービスが開始される前に[ログオン失敗 (Logon failure)]エラーが表示されます。

6 Web サービスユーザーが変更されたことを確認するには、*install_path*¥bin¥nbcertcmd.exe -ping が機能することを確認します。

メモ: wmcUtils.bat ユーティリティスクリプトの出力が nbwmc_support.log に取得されます。このログは *install_path*¥wmc¥webserver¥logs¥nbwmc_support.log にあります。

Linux または UNIX 上で Web サービスユーザーアカウントを変更するには

1 シェルを開きます。

2 ディレクトリを /usr/openv/wmc/bin/install に変更します。

3 wmcUtils -changeUser を実行して Web サービスユーザーを変更します。

例: (nbwebsvc1 は Web サービスユーザーで、nbwebgrp1 は nbwebsvc1 がメンバーであるユーザーグループです)

```
usr/openv/wmc/bin/install/wmcUtils -changeUser nbwebsvc1 nbwebgrp1
```

wmcUtils ユーティリティスクリプトについて詳しくは、wmcUtils -help オプションを使用してください。

4 (該当する場合) クラスタ環境を使用する場合は、アクティブノードと非アクティブノードで wmcUtils.bat -changeUser を実行します。

5 スクリプトによりプロンプトが表示されたら、Web サービスのユーザーパスワード (例: nbwebsvc1) を入力します。

正しいパスワードが入力されると、NetBackup Web Management Consoleサービスが再開されます。正しくないパスワードを入力すると、NetBackup Web Management Consoleサービスが開始される前に[ログオン失敗 (Logon failure)]エラーが表示されます。

6 Web サービスユーザーが変更されたことを確認するには、/usr/openv/netbackup/bin/nbcertcmd -ping が機能することを確認します。

メモ: wmcUtils ユーティリティスクリプトの出力が nbwmc_support.log に取得されます。このログは /usr/openv/wmc/webserver/logs/nbwmc_support.log にあります。

27

特権のないユーザー (サービスユーザー) アカウントでの NetBackup サービスの実行

この章では以下の項目について説明しています。

NetBackup サービスユーザーのアカウントについて

NetBackup 9.1 以降、プライマリサーバーのほとんどのサービスを特権のないユーザーが実行できます。特権のないユーザーとして実行することを強くお勧めします。特権のないユーザーは `service user` と呼ばれ、NetBackup サービスを実行することのみを目的とします。

サービスユーザーアカウントを使用する場合の重要な考慮事項

サービスユーザーアカウントで NetBackup サービスを実行する場合は、次の項目を確認してください。

- NetBackup 操作の実行にはサービスユーザーアカウントを使用しないでください。サービスユーザーアカウントは、NetBackup サービスの実行のみを目的としています。
- サービスユーザーのプライマリグループは、そのサービスユーザー専用にすることをお勧めします。
- ルートユーザーをサービスユーザーとして使用することはお勧めしません。
- nbwebsvc ユーザーはサービスユーザーとして使用しないでください。
- nbwebgrp はサービスユーザーのセカンダリグループである必要があります。
- サービスユーザーで実行できるプロセスの数は、ルートユーザーで実行するプロセスの数と同じである必要があります。
  サービスユーザーで実行できるユーザープロセスの最大数を検索するには、ulimit -u を使用します。
- サービスユーザーで開くことができるファイルの数は、ルートユーザーで開くことができるファイルの数と同じである必要があります。
  サービスユーザーで開くことができるファイルの最大数を表示するには、ulimit -Hn コマンドを使用します。
- ルートユーザーアカウント以外のサービスユーザーアカウントを使用する場合、1 回限りの変換を行う必要があります。この変換により、カタログサイズに応じてアップグレード時間が大幅に増加する場合があります。
- インストールディレクトリ以外のすべての外部パスにサービスユーザーがアクセスできる必要があります。
  p.546 の「サービスユーザーアカウントに外部パスへのアクセス権を付与する」を参照してください。
- 環境変数パスにサービスユーザーがアクセスできる必要があります。
- サービスユーザーは OS の一時ディレクトリ (通常は /tmp または /var/tmp) にアクセスできる必要があります。これは、P_tmpdir マクロで指定される場合があります。
- サービスユーザーアカウントは、パスワードなしのアカウントである場合があります。
- サービスユーザーが構成されている場合、レガシーログファイル (UNIX の場合は /user/openv/netbackup/logs、Windows の場合は C:¥Program Files¥Veritas¥NetBackup¥logs) には接頭辞 SERVICE_USER が付きます。
  例: SERVICE_USER.040921_00001.log
- サービスユーザー名は 32 文字未満で、英字のみを使用する必要があります。
- bpcd および vnetd プロセスが Oracle Admin などのアプリケーションアカウントで実行される場合、そのアカウントをサービスユーザーアカウントに変更しないでください。

サービスユーザーアカウントの構成

サービスユーザーは事前に作成する必要があり、セカンダリグループとして nbwebgrp を指定する必要があります。

UNIX でのサービスユーザーアカウントの構成

UNIX でのプライマリサーバーのインストールまたはアップグレード中に、サービスユーザーとして利用可能な新しいユーザー (可能な場合は root 以外のユーザー) を指定する新しいプロンプトが表示されます。プライマリサーバー上のほとんどのデーモンを、この新しいサービスユーザーで実行できるようになりました。

UNIX でローカルユーザーアカウントを作成するには、次のコマンドを実行します。

```
useradd -c 'NetBackup Services account' -d /usr/openv/
service_user_name
```

サービスユーザーを nbwebgrp セカンダリグループに追加するには、次のコマンドを実行します。

```
usermod -a -G nbwebgrp service_user_name
```

次の項目を確認してください。

- クラスタ環境では、すべてのクラスタノードでローカルアカウントが一貫して設定されていることを確認してください。Linux または UNIX プラットフォームでクラスタ環境を使用する場合、NetBackup サービスユーザーはローカルユーザーにできます。NetBackup サービスユーザーは、クラスタのすべてのノードで同じ名前と UID を持つ必要があります。
- クラスタ環境では、ドメインユーザー (例: NIS) を使用することをお勧めします。LDAP アカウントがサポートされており、UNIX で使用できます。
- NetBackup サービスアカウントは POSIX 準拠シェルを使用する必要があります。

Windows でのサービスユーザーアカウントの構成

Windows の場合、新規インストールではローカルサービスの組み込みアカウントが使用されます。アップグレードプロセスに変更はありません。

インストールまたはアップグレード後のサービスユーザーアカウントの変更

UNIX では、nbserviceusercmd コマンドを使用して、サービスユーザーアカウントを他のユーザーアカウントに変更できます。

Windows では、nbserviceusercmd コマンドを使用して、サービスのユーザーアカウントを管理者、ローカルシステムまたはローカルサービスに変更できます。

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。

サービスユーザーアカウントに外部パスへのアクセス権を付与する

NetBackup の外部にあるディレクトリパスとそのコンテンツに対するアクセス権がサービスユーザーアカウントに付与されていない場合、NetBackup の操作は失敗します。インストールディレクトリ以外のすべての外部パスにサービスユーザーアカウントがアクセスできる必要があります。次に例を示します。

- DR (ディザスタリカバリ) パス
- 外部 CA 証明書のパス
- 次のコマンドのパラメータとして使用される外部パス:
  - `nbdb_admin`
  - `create_nbdb`
  - `nbdb_move`
  - `nbdb_backup`
  - `nbdb_restore`
  - `nbdb_unload`
  - `cat_export`
  - `cat_import`

サービスユーザーアカウントに外部パスへのアクセス権を付与するには

1. NetBackup の操作に固有のパスがホスト上の複数のユーザー間で共有されていないことを確認します。
   - UNIX の場合、パスが次の場所に設定されていないことを確認します。
     ルート以外のユーザーの /tmp、/root またはホームディレクトリ
   - Windows の場合、パスが `C:¥users` に存在する別のユーザーアカウントのディレクトリではないことを確認します。
2. 次のコマンドを実行して、外部パスとそのコンテンツへのアクセス権をサービスユーザーアカウントに付与します。
   - UNIX の場合: `chown -R service_user_namepath`
     `chown` コマンドを実行した後、次のコマンドを使用して、指定したパスにサービスユーザーが書き込み可能かどうかを確認します。
     `su service_user_name -c "touch path/test.txt"`

- Windows の場合:
  netbackup_install_path¥NetBackup¥bin¥goodies¥nbserviceusercmd.exe -addacl *path* -reason *reason*

サービスユーザーアカウントで実行される NetBackup サービス

Windows の場合:	UNIX の場合:
NetBackup Request Daemon	bprd
NetBackup Database Manager	bpdbm
-	bpjobd
NetBackup Compatibility Service	bpcompatd
NetBackup Audit Manager	nbaudit
NetBackup Event Manager	nbevtmgr
NetBackup Enterprise Media Manager	nbemm
NetBackup Resource Broker	nbrb
NetBackup Job Manager	nbjm
NetBackup Policy Execution Manager	nbpem
NetBackup Service Layer	nbsl
NetBackup Storage Lifecycle Manager	nbstserv
NetBackup Proxy Service	nbproxy
NetBackup Indexing Manager	nbim
NetBackup Agent Request Server	nbars
NetBackup Key Management Service	nbkms
NetBackup Vault Manager	nbvault
Anomaly Detection Management Service	nbanomalymgmt

Windows の場合:

vnetd-child-proxies

- vnetd -proxy inbound_proxy -number 0
- vnetd -proxy outbound_proxy -number 0
- vnetd -proxy http_api_tunnel -number 0
- vnetd -proxy http_pbx_tunnel -number 0

メモ: 特権のあるサービスアカウント (vnetd スタンドアロンサービスが使用するユーザーアカウント) として管理者アカウントを選択した場合、vnetd 子プロキシは同じ管理者アカウントで実行されます。

UNIX の場合:

vnetd-child-proxies

- vnetd -proxy inbound_proxy -number 0
- vnetd -proxy outbound_proxy -number 0
- vnetd -proxy http_api_tunnel -number 0
- vnetd -proxy http_pbx_tunnel -number 0

28

特権のないユーザーアカウントでの NetBackup コマンドの実行

この章では以下の項目について説明しています。

- nbcmdrun ラッパーコマンドを使用した NetBackup コマンドの実行

nbcmdrun ラッパーコマンドを使用した NetBackup コマンドの実行

nbcmdrun は、NetBackup ホストで他の NetBackup コマンドを実行するために使用されるラッパーコマンドです。NetBackup ホストは、プライマリサーバー、メディアサーバー、またはクライアントにできます。

特定の NetBackup コマンドは OS (オペレーティングシステム) 管理者のみが実行できます。NetBackup RBAC (役割ベースのアクセス) システムで定義されている NetBackup 管理者の役割を持つユーザーは、これらのコマンドを実行できません。

nbcmdrun ユーティリティを使用すると、特権のない OS ユーザーが RBAC 権限に基づいてこれらのコマンドを実行できます。NetBackup のコマンドライン管理者の役割を使用すると、特権のない OS ユーザーでほとんどの NetBackup コマンドを実行できます。

nbcmdrun -listcommands を使用して、nbcmdrun がサポートするすべてのコマンドを一覧表示します。

nbcmdrun 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。

nbcmdrun のしくみ

nbcmdrun を使用して NetBackup コマンドを実行するには、nbcmdrun コマンドとサービスユーザーを NetBackup ホストで有効にする必要があります。

デフォルトでは、nbcmdrun コマンドは有効になっています。ただし、無効になっている場合は nbcmdrun を再び有効にできます。

p.551 の「nbcmdrun コマンドの再有効化」を参照してください。

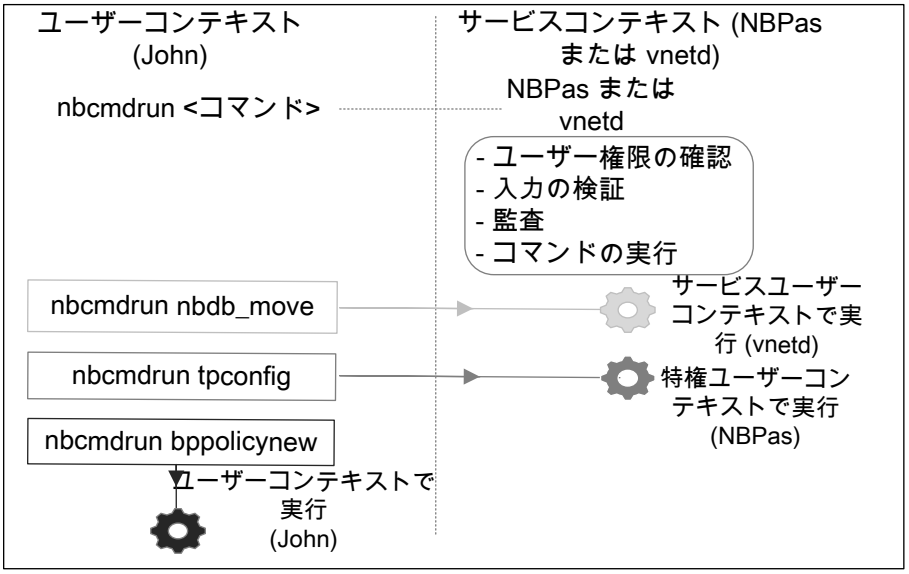
bpnbat -login -loginType web コマンドを使用して現在の NetBackupドメインで Web ログインを行う必要があります。現在の NetBackupドメインは、一般に、NetBackup 構成 (UNIX または Windows レジストリの bp.conf ファイル) 内の最初のサーバーエントリのドメインとして参照されます。

読み取りおよび書き込み権限があるディレクトリから nbcmdrun を実行する必要があります。コマンドのベース名を指定し、その後にコマンド引数を指定する必要があります。

たとえば、nbcmdrun mklogdir -create bpcd のようにします。

nbcmdrun のワークフロー

図 28-1 nbcmdrun のワークフロー図



1. nbcmdrun は入力コマンドを検証し、ユーザーの JWT (JSON Web トークン) を取得します。
2. nbcmdrun は NBPas に接続し、ユーザー JWT を NBPas に提示します。

3. NBPas はユーザー JWT、入力コマンド、および引数を検証します。サービスユーザーコンテキストまたは特権ユーザーコンテキストで入力コマンドを呼び出します。

NBpas によって実行されるコマンドは監査されます。

注意: nbcmdrun を使用して NetBackup コマンドを実行すると、特定のコマンドに指定されたパスワードが画面に表示される場合があります。

nbcmdrun コマンドの無効化

このトピックを使用して nbcmdrun コマンドを無効にします。

p.551 の「nbcmdrun コマンドの再有効化」を参照してください。

nbcmdrun コマンドを無効化するには

1 システム管理者は、ENABLE_NBCMDRUN という名前の touch ファイルをコンテンツ 0 で作成する必要があります。

メモ: ENABLE_NBCMDRUN ファイルは拡張子を付けずに作成する必要があります。

2 次のコマンドを実行します。

UNIX の場合:

```
echo 0 > /usr/openv/var/ENABLE_NBCMDRUN
```

Windows の場合:

```
echo 0 > install path¥NetBackup¥var¥ENABLE_NBCMDRUN
```

nbcmdrun コマンドの再有効化

デフォルトでは、nbcmdrun コマンドは有効になっています。

nbcmdrun コマンドを無効にして再度有効にする場合は、次の手順を実行します。

メモ: nbcmdrun コマンドを使用するには、コマンドと NetBackup サービスユーザーを NetBackup ホストで有効にする必要があります。

p.545 の「サービスユーザーアカウントの構成」を参照してください。

nbcmdrun を再度有効にするには

1. システム管理者は、ENABLE_NBCMDRUN という名前の touch ファイルをコンテンツ 1 で更新する必要があります。

   メモ: ENABLE_NBCMDRUN ファイルには拡張子がありません。

2. 次のコマンドを実行します。

   UNIX の場合:

   ```
   echo 1 > /usr/openv/var/ENABLE_NBCMDRUN
   ```

   Windows の場合:

   ```
   echo 1 > install path¥NetBackup¥var¥ENABLE_NBCMDRUN
   ```

29

NetBackup でのデータの変更不可と削除不可

この章では以下の項目について説明しています。

変更不可データと削除不可データについて

NetBackup では、WORM プロパティを使用して、データが暗号化、変更、削除されないように保護します。

WORM は、Write Once Read Many の略語です。

WORM プロパティには、バックアップイメージに対する 2 つの追加のセキュリティレベルがあります。

- 変更不可: この保護により、バックアップイメージは読み取り専用になり、バックアップ後に変更、破損、または暗号化できなくなります。
- 削除不可: このプロパティにより、バックアップイメージが期限切れになる前に削除されないように保護されます。データは悪質な削除から保護されます。

これらの WORM プロパティを構成すると、ランサムウェアなどの特定のマルウェア攻撃からデータをある程度保護できます。

NetBackup は、データが破損しないように WORM ストレージデバイスにバックアップを書き込む機能を提供します。さらに、ストレージベンダーが提供する高度なオプションを

利用して、規制やコンプライアンス要件を満たすために、バックアップをストレージプラットフォーム上で変更できないようにして保持します。

すべての NetBackup イメージコピーには有効期限があります。この期限は、スケジュールに設定されている保持レベルとバックアップジョブの開始時刻を使用して計算されます。

NetBackup イメージが WORM 対応のストレージユニットに書き込まれると、そのイメージの WORM のロック解除時間が過ぎるまでデータを変更することも削除することもできません。バックアップジョブの開始時刻から計算されるコピーの有効期限とは異なり、WORM のロック解除時間は WORM ストレージに関連付けられます。WORM のロック解除時間の値は、保持レベルと、WORM ストレージへのバックアップイメージの書き込み完了タイムスタンプを使用して計算されます。

`bpimagelist` を使用して WORM ストレージに書き込まれたイメージを表示する場合、コピーの有効期限に関連付けられたタイムスタンプは、バックアップイメージのコピーの WORM のロック解除時間より前になります。実行時間が長いバックアップや複製ジョブの場合、コピーの有効期限と WORM のロック解除時間の差が大きくなります。

通常の操作の一環として、WORM ストレージのバックアップイメージのコピーは、コピーの有効期限と WORM のロック解除時間の両方のタイムスタンプが経過するまでカタログとストレージから削除されません。WORM ストレージに書き込まれるコピーの WORM のロック解除時間は、延長のみが可能で、短縮できません。有効期限を延長するには、`bpexpdate -extend_worm_locks` コマンドを使用します。

特殊な状況では、`bpexpdate -try_expire_worm_copy` オプションを使用して NetBackup カタログから WORM 削除不可イメージの試行を強制的に実行できます。このオプションは、ストレージデバイスで WORM ロックを直接削除した後にのみ使用することをお勧めします。このオプションは、Veritasテクニカルサポートのサポートのもとで使用してください。

WORM ストレージにイメージを複製する場合は、NetBackup 10.1 で導入された `-worm_unlock_match_expiration` オプションを使用して `bpduplicate` コマンドを実行し、WORM のロック解除時間をコピーの有効期限と一致するように設定します。

このコマンドオプションを使用せずに古いバックアップイメージを WORM ストレージに複製する場合、複製したコピーの WORM のロック解除時間は、設定した保持レベルと、複製ジョブの完了時のタイムスタンプを使用して計算されます。

`bpduplicate -worm_unlock_match_expiration` コマンドオプションは SLP に基づいた複製には使用しません。SLP に基づいた複製の場合、保持期間を複製ジョブの終了時点から適用して、新しいコピーの WORM のロック解除時間が計算されます。新しいコピーの有効期限は、(コピー 1 の) バックアップ時間に適用される保持期間から計算されます。

AIR ジョブの場合、保持期間がインポートジョブの終了時点から適用され、インポートされたコピーの WORM のロック解除時間が計算されます。コピーの有効期限は、インポートジョブの開始時点から適用される保持期間によって計算されます。

bpduplicate コマンドと bpexpdate 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。

メモ: bpduplicate -worm_unlock_match_expiration および bpexpdate -extend_worm_locks コマンドオプションを使用する場合、NetBackup プライマリサーバーのクロックの精度に依存します。これは、WORM のロック解除時間がそのコピーのイメージの有効期限のタイムスタンプをミラー化するためです。

WORM のロック解除時間を元のバックアップ時間に基づいて計算する方法について詳しくは、次のナレッジベースの記事を参照してください。

Images duplicated to WORM storage have unlock time calculated from duplication date not backup date

変更不可データと削除不可データを構成するためのワークフロー

変更不可と削除不可を構成してデータを保護するには、次の手順を指定された順序で実行します。

表 29-1 変更不可データと削除不可データを構成するためのワークフロー

手順	説明
1	ストレージサーバーで、次の WORM 設定を構成します。ストレージ管理者は、NetBackup の外部でこれらの設定を構成します。 ■ [WORM 対応 (WORM capable)]: バックアップイメージの作成時に WORM プロパティを使用するようにストレージユニットおよび関連付けられたディスクプールを有効にした場合、バックアップイメージは変更不可および削除不可に設定されます。 ■ [ロックの最小時間 (Lock Minimum Time)]: バックアップイメージのデータが削除不可になる最小時間を指定します。ストレージ管理者は、NetBackup が検出した論理ストレージユニット (LSU) またはドメインボリューム (DV) でこの時間を設定します。 ■ [ロックの最大時間 (Lock Maximum Time)]: バックアップイメージのデータが削除不可になる最大時間を指定します。ストレージ管理者は、NetBackup が検出した論理ストレージユニット (LSU) またはドメインボリュームでこの時間を設定します。 OST ベンダーのプラグインのマニュアルを参照してください。
2	WORM 対応ボリュームを使用してディスクプールを構成します。
3	[WORM を使用 (Use WORM)]オプションが有効になっているストレージユニットを構成します。
4	WORM 対応ストレージユニットを使用してバックアップポリシーを構成します。

メモ: ストレージの変更またはサードパーティの OST ベンダーソフトウェアのアップグレードの場合は、ストレージサーバーとディスクプールを手動で更新する必要があります。『NetBackup アップグレードガイド』の「アップグレード後のシステム更新の完了」セクションを参照してください。

bpexpdate コマンドを使用したストレージからの変更不可イメージの削除

変更不可イメージの削除は、ロックの削除を許可するストレージが使用されている場合にのみ可能です。ロックの削除は、Flex Appliance、Flex Scale Appliance、Access Appliance の Enterprise モードまたはロックの削除をサポートするサードパーティ製のストレージデバイスを使用して実行できます。変更不可イメージを削除する際は、使用中のストレージがロックの削除を担当し、NetBackup がイメージの削除を担当します。

Flex Appliance、Flex Scale Appliance、Access Appliance を使用する場合は、コマンドラインまたは SSH セッションを使用して、イメージのロックを解除する必要があります。サードパーティ製のストレージデバイスを使用している場合は、そのベンダーのマニュアルで、ロックされたイメージを削除する手順を参照してください。

アプライアンスで変更不可イメージを削除する方法

1. アプライアンスが Enterprise モードであることを確認します。
2. NetBackup コマンドラインから、`bpimagelist` コマンドを使用してイメージ ID を見つけます。

   この手順では、次のイメージ ID の例を使用します。

   ```
   Backup ID: server123.veritas.com_1234567890
   ```

3. コマンドラインオプションまたは SSH セッションオプションを使用して、ストレージ上にあるイメージのロックを削除します。
   - Flex Appliance の場合: 次のオプションを実行するには、デフォルトの `msdpadm` ユーザーを使用する必要があります。
   - Flex Scale Appliance と Access Appliance の場合: アプライアンス管理者の役割を持つアプライアンスユーザーを使用する必要があります。

   コマンドラインオプション:
   - `/usr/openv/pdde/pdcr/bin/` ディレクトリを開きます。
   - 次のコマンドを使用して、指定したバックアップ ID のカタログデータベースを問い合わせ、変更します (例: `server123.veritas.com_1234567890`)。`-worm disable` オプションは、バックアップ ID を使用してイメージの保持ロックを無効にします。

```
sudo -u msdpsvc /usr/openv/pdde/pdcr/bin/catdbutil -worm
disable -backupid
```

SSH セッションオプション:

- WORM ストレージサーバーインスタンスへの SSH セッションを開きます。
- `retention policy disable` コマンドを使用して、指定したポリシーのカタログデータベースを問い合わせ、変更します。`policydisable` 引数は、保持ロックが設定されているイメージ保持に使用されるポリシー ID を使用してイメージの保持ロックを無効にします。

この手順のコマンドオプションについて詳しくは、『NetBackup Deduplication ガイド』を参照してください。

4 `-try_expire_worm_copy` オプションを使用して、イメージ ID を `bpexpdate` に追加します。

```
bpexpdate -d 0 backupid server123.veritas.com_1234567890
-try_expire_worm_copy -copy 1
```

5 y または n を使用して削除を確認します。

ストレージロックが削除されない場合、NetBackup は WORM ロックエラーがあることを示すエラーを返します。

p.557 の「`bpexpdate` コマンドを使用したカタログからの変更不可イメージの削除」を参照してください。

p.553 の「 変更不可データと削除不可データについて」を参照してください。

`bpexpdate` コマンドを使用したカタログからの変更不可イメージの削除

変更不可イメージを NetBackup カタログから削除し、そのイメージをストレージに残すことができます。

カタログから変更不可イメージを削除するには

1. NetBackup コマンドラインインターフェース (CLI) を開きます。
2. -try_expire_worm_copy オプションと -nodelete オプションを指定した bpexpdate コマンドを使用して、カタログからイメージを削除します。

   ```
   bpexpdate -d 0 -backupid server123.veritas.com_1234567890
    -copy 1 -try_expire_worm_copy -nodelete
   ```

   -try_expire-worm_copy オプションと -nodelete オプションを同時に使用すると、カタログからイメージが削除されるだけで、ストレージには影響しません。
3. y または n を使用して削除を確認します。

p.556 の「bpexpdate コマンドを使用したストレージからの変更不可イメージの削除」を参照してください。

p.553 の「 変更不可データと削除不可データについて」を参照してください。

30

異常検出

この章では以下の項目について説明しています。

バックアップの異常検出について

NetBackup は、バックアップメタデータの異常を検出できるようになりました。データバックアップフローの異常なジョブデータを検出できます。たとえば、ファイル数やファイルサイズが通常の数やサイズと異なる場合に検出できます。

メモ: デフォルトでは、異常検出アルゴリズムは NetBackup プライマリサーバーで実行されます。異常検出プロセスによってプライマリサーバーに影響がある場合は、異常を検出するようにメディアサーバーを構成できます。

次のバックアップジョブのメタデータ、属性、機能が、バックアップの異常検出中に検証されます。

- バックアップイメージのサイズ

- バックアップファイルの数
- KB 単位で転送されるデータ
- 重複排除率
- バックアップジョブの完了時間

これらのバックアップジョブ属性が通常の範囲から異常に逸脱している場合は異常と見なされ、NetBackup Web UI を使用して通知されます。

バックアップの異常検出と通知のワークフロー

バックアップの異常検出と通知のワークフローは、次のとおりです。

表 30-1　　ワークフロー

手順	説明
手順 1	プライマリサーバーとメディアサーバーに NetBackup ソフトウェアをインストールするか、アップグレードします。 『NetBackup インストール/アップグレードガイド』を参照してください。
手順 2	プライマリサーバーでバックアップの異常検出を有効にします。 p.561 の「プライマリサーバーでのバックアップの異常検出」を参照してください。 デフォルトでは、異常検出アルゴリズムは NetBackup プライマリサーバーで実行されます。異常検出プロセスによってプライマリサーバーに影響がある場合は、異常を検出するようにメディアサーバーを構成できます。 p.562 の「メディアサーバーでのバックアップの異常検出」を参照してください。
手順 3	NetBackup Web UI を使用して異常検出の設定を行います。 p.563 の「バックアップの異常検出の設定」を参照してください。
手順 4	NetBackup Web UI を使用して異常を表示します。 p.564 の「バックアップの異常の表示」を参照してください。

バックアップの異常の検出方法

たとえば、次の例を考えてみます。

ある組織では、スケジュール形式が[完全 (Full)]の特定のクライアントおよびバックアップポリシーにより、毎日約 1 GB のデータがバックアップされます。特定の日に、10 GB のデータがバックアップされました。この事例はイメージサイズの異常としてキャプチャされ、通知されました。この異常は、現在のイメージサイズ (10 GB) が通常のイメージサイズ (1 GB) をはるかに超えているために検出されます。

メタデータの大幅な逸脱は、その異常スコアに基づいて異常とされます。

異常スコアは、現在のデータが過去の類似データの観測群からどれだけ離れているかに基づいて計算されます。この例では、基準となるクラスタは 1 GB のデータバックアップです。異常の重大度は、そのスコアに基づいて判断できます。

例:

Anomaly_A の異常スコア = 7

Anomaly_B の異常スコア = 2

結論 - Anomaly_A は Anomaly_B よりも重大

NetBackup は異常検出時に、異常検出の構成の設定 (デフォルト、存在する場合は詳細設定) を考慮します。

プライマリサーバーでのバックアップの異常検出

このトピックでは、プライマリサーバーでバックアップの異常検出を有効にする手順について説明します。

プライマリサーバーでバックアップの異常検出を有効にするには

1. システムに NetBackup プライマリサーバーソフトウェアをインストール (またはプライマリサーバーソフトウェアをアップグレード) します。

   インストール後、次の構成がプライマリサーバーで自動的に行われます。

   - プライマリサーバーで `NetBackup Anomaly Detection Management` サービス (`nbanomalymgmt`) が再起動されます。
     異常検出サービスとアラートサービスはデフォルトでは実行されません。

     メモ: プロキシサーバーがプライマリサーバーに接続するのに 45 分以上かかると、`NetBackup Anomaly Detection Management` サービスは停止します。

2. NetBackup Web UI を使用してバックアップ異常設定を行います。NetBackup は、異常検出時にこれらの設定を考慮します。

   p.563 の「バックアップの異常検出の設定」を参照してください。

   p.560 の「バックアップの異常の検出方法」を参照してください。

   異常が検出されると、NetBackup Web UI を介して通知されます。

   p.564 の「バックアップの異常の表示」を参照してください。

メディアサーバーでのバックアップの異常検出

このトピックでは、メディアサーバーでバックアップの異常検出を有効にするワークフローと手順について説明します。

メモ: デフォルトでは、異常検出アルゴリズムは NetBackup プライマリサーバーで実行されます。異常検出プロセスによってプライマリサーバーに影響がある場合は、異常を検出するようにメディアサーバーを構成できます。

メディアサーバーでバックアップの異常検出を有効にするには

1. システムに NetBackup メディアサーバーソフトウェアをインストールします (またはメディアサーバーソフトウェアをアップグレードします)。
2. プライマリサーバーで、異常プロキシサーバーの詳細を追加します。プロキシサーバーは、異常アルゴリズムを実行するメディアサーバーにする必要があります。

   p.563 の「バックアップの異常検出の設定」を参照してください。
3. (省略可能)プライマリサーバーで以前に収集したデータを維持する場合は、次の手順を実行します。
   - Web UI を使用して、nbanomalymgmt サービスが無効になっていることを確認します。
   - メディアサーバーで nbanomalymgmt サービスが停止していることを確認します。
   - 次のディレクトリに移動します。
     Windows の場合: *Install_Path*¥NetBackup¥var¥global
     UNIX の場合: /usr/openv/var/global
     このディレクトリは、クラスタ化されたプライマリサーバー上の共有ディスクに存在します。
   - プライマリサーバーの anomaly_detection フォルダからメディアサーバーの anomaly_detection フォルダに NB_Anomaly.db、NB_Anomaly.db-shm、および NB_Anomaly-walファイルをコピーします。
     anomaly_config.conf ファイルをコピーして、自動マルウェアスキャン設定を保持できます。
   - メディアサーバーで nbanomalymgmt サービスを開始します。

4 メディアサーバーで、nbanomalymgmt サービスを手動で開始します。次のスクリプトを使用します。

```
nbanomalymgmt -start
```

5 NetBackup Web UI でバックアップ異常設定を行います。NetBackup は、異常検出時にこれらの設定を考慮します。

p.563 の「バックアップの異常検出の設定」を参照してください。

p.560 の「バックアップの異常の検出方法」を参照してください。

異常が検出されると、NetBackup Web UI で通知されます。

p.564 の「バックアップの異常の表示」を参照してください。

バックアップの異常検出の設定

異常検出を有効にすると、異常データ収集、検出サービス、イベントが有効になります。バックアップの異常検出設定は、基本レベルと詳細レベルで構成できます。

p.559 の「バックアップの異常検出について」を参照してください。

バックアップの異常検出を設定するには

1 NetBackup Web UI にサインインします。

2 左側で[検出とレポート (Detection and reporting)]、[異常検出 (Anomaly detection)]の順に選択します。

3 右上の[異常検出の設定 (Anomaly detection settings)]、[バックアップの異常検出の設定 (Backup anomaly detection settings)]の順に選択します。

4 右側で[編集 (Edit)]をクリックし、次の[異常検出 (Anomaly detection)]を構成します。

- すべて無効にする (Disable all)
- 異常データの収集を有効にする (Enable anomaly data gathering)
- 異常データの収集と検出サービスを有効にする (Enable anomaly data gathering and detection service)
- 異常データの収集、検出サービス、イベントを有効にする (Enable anomaly data gathering and detection service and events)

5 [保存 (Save)]をクリックします。

6 [編集 (Edit)]をクリックして、次の基本設定を変更します。

- 異常検出の感度 (Anomaly detection sensitivity)
- データ保持の設定 (Data retention settings)

- データ収集の設定 (Data gathering settings)
- 異常プロキシサーバーの設定 (Anomaly proxy server settings)

7 [保存 (Save)]をクリックします。

8 [詳細設定 (Advanced settings)]セクションを展開し、[編集 (Edit)]をクリックして次を設定し、[保存 (Save)]をクリックします。

- クライアントの異常設定を無効にする (Disable anomaly settings for clients)
- 機械学習でポリシー形式または特定の機能を無効にする (Disable policy type or specific features for machine learning)

バックアップの異常の表示

NetBackup は、バックアップメタデータの異常を検出できるようになりました。データバックアップフローの異常なジョブデータを検出できます。たとえば、ファイル数やファイルサイズが通常の数やサイズと異なる場合に検出できます。

p.559 の「バックアップの異常検出について」を参照してください。

メモ: 異常数が 0 の場合は、異常が発生しなかったか、異常検出サービスが実行されていない可能性があります。

バックアップの異常を表示するには

1 NetBackup Web UI にサインインします。

2 左側で[検出とレポート (Detection and reporting)]、[異常検出 (Anomaly detection)]、[バックアップの異常 (Backup anomalie)]の順に選択します。

次の列が表示されます。

- ジョブ ID (Job ID) - 異常が検出されたジョブのジョブ ID
- クライアント名 (Client name) - 異常が検出された NetBackup クライアントの名前
- ポリシー形式 (Policy type) - 関連付けられたバックアップジョブのポリシー形式
- 数 (Count) - このジョブで検出された異常の数
- スコア (Score) - 異常の重大度。異常の重大度が大きいほどこのスコアが高くなります。
- 異常の重大度 (Anomaly severity) - このジョブについて通知された異常の重大度
- 異常の概略 (Anomaly summary) - このジョブについて通知された異常の概略

- 受信日 (Received) - 異常が通知された日付
- レビュー状態 (Review status) - 検出された異常が誤検知として報告されたか、実際の異常として報告されたか、無視できるかを示します。
- ポリシー名 (Policy name) - 関連付けられたバックアップジョブのポリシー名
- スケジュール名 (Schedule name) - 関連付けられたバックアップジョブのスケジュール名
- スケジュール形式 (Schedule type) - 関連付けられたバックアップジョブのスケジュール形式

3 行を展開すると、選択した異常の詳細が表示されます。

各異常レコードについて、その機能の現在値と、過去のデータに基づく実際の範囲が表示されます。

たとえば、次の例を考えてみます。

異常があるイメージサイズの特徴として 100 MB (通常は 350 MB、450 MB) と表示されます。この情報は、異常として報告された現在のイメージサイズが 100 MB であることを意味しています。しかし、通常のイメージサイズの範囲は、過去のデータの分析から導き出された 350 ～ 450 MB です。現在のイメージサイズと通常のイメージサイズの範囲が大幅に異なるため、NetBackup は異常として通知します。

4 異常レコードに対して次の処理を実行できます。

- 異常条件を無視できる場合は、[無視としてマーク (Mark as ignore)]をクリックします。
  異常レコードの[レビュー状態 (Review status)]は `Ignore` と表示されます。
- 異常条件に何らかの処理を実行する場合は、[異常として確認 (Confirm as anomaly)]をクリックします。
  異常レコードの[レビュー状態 (Review status)]は `Anomaly` と表示されます。
- 異常が誤検知の場合は、[誤検知として報告 (Report as false positive)]をクリックします。以後、同様の異常は表示されません。
  異常レコードの[レビュー状態 (Review status)]は `False positive` と表示されます。

システムの異常検出について

NetBackup では、重要な操作中に次のようなシステムの異常を検出できます。

- 疑わしい状況下でオフラインになっている NetBackup クライアント
  「クライアントオフライン」の異常は、NetBackup ホスト上の侵害されたファイルシステムに起因するオフラインクライアントを検出する機能を追加します。異常が検出されると、NetBackup では影響を受けるクライアントに対して重要アラートが生成されます。

- NetBackup イメージの手動による異常な有効期限の終了または有効期限の変更
  「イメージの有効期限」の異常は、特権ユーザーがバックアップイメージを期限切れにする異常な試行を検出します。異常が検出されると、NetBackup は重要アラートを生成してユーザーを識別します。

p.567 の「システムの異常の表示」を参照してください。

システムの異常検出の設定

異常検出を有効にすると、異常データ収集、検出サービス、イベントが有効になります。バックアップの異常検出設定は、基本レベルと詳細レベルで構成できます。

p.565 の「システムの異常検出について」を参照してください。

バックアップの異常検出を設定するには

1. NetBackup Web UI にサインインします。
2. 左側で[検出とレポート (Detection and reporting)]、[異常検出 (Anomaly detection)]の順に選択します。
3. 右上の[異常検出の設定 (Anomaly detection settings)]、[システムの異常検出の構成 (System anomaly detection configuration)]の順に選択します。
4. [システム異常検出の構成 (System anomaly detection configuration)]画面で、次のシステム異常検出を設定します。
   - [疑わしいエラーコードがあり、オフラインのクライアントを検出する (Detect clients that are offline with suspicious error codes)]チェックボックスにチェックマークを付けると、疑わしい状況下でクライアントがオフラインであることが NetBackup で検出された場合に異常アラートが生成されます。
   - [イメージの有効期限操作の異常を検出する (Detect anomalies for image expiration operations)]チェックボックスにチェックマークを付けると、イメージの有効期限について異常なアクティビティが発生した場合に異常が生成されます。
5. 次の[ルールベースの異常検出設定 (Rules-based anomaly detection)]を設定します。

   [NetBackup 異常検出ルールを使用して異常を検出します (Detect anomalies using NetBackup anomaly detection rules)]チェックボックスにチェックマークを付けて、異常を生成する事前定義済みのルールまたは条件を一覧表示します。

   例: ストレージサーバーが Null STU に設定されている、クライアントがポリシーから削除された、またはユーザーによってトークンが削除された。

   事前定義済みの各ルールの次の詳細が表示されます。

   - ルール名 (Rule name)
   - 説明 (Description)

- 重大度 (Severity)
- バージョン (Version)
- 有効 (Enabled)

最新のルールファイルを使用する場合は、Veritas ダウンロードセンターに移動します。ルールファイル (.zip) をダウンロードし、ローカルコンピュータに保存します。

[ルールをアップロードする (Upload rules)]をクリックして、ダウンロードしたルールファイルを選択します。すべての最新のルールが、[ルールに基づく異常検出 (Rules-based anomaly detection)]セクションに一覧表示されます。

6 有効にして異常を生成するルールを選択します。

[有効化 (Enable)]をクリックします。

NetBackup は、ルール基準を満たす異常を生成します。

システムの異常の表示

NetBackup はシステムの異常を検出できます。バックアップ操作中に、NetBackup はすべてのファイル拡張子を確認し、それらをランサムウェアの拡張子リストと比較して、一致する場合は異常を生成します。異常は、特定のバックアップで検出されたランサムウェアの拡張子ごとに生成されます。デフォルトでは、この異常検出はすべてのポリシー形式で有効になっています。

システムの異常を表示するには

1 NetBackup Web UI にサインインします。

2 左側で[検出とレポート (Detection and reporting)]、[異常検出 (Anomaly detection)]、[システムの異常 (System anomalies)]の順に選択します。

次の列が表示されます。

- 異常 ID (Anomaly ID) - 異常レコードの ID
- 異常の種類 (Anomaly type) - 異常の種類
- 重大度 (Severity) - 異常の重大度
- 説明 (Description) - 異常に関する追加情報
- 検出日 (Detected on) - 異常が検出された日付
- 確認状態 (Review status) - 検出された異常が誤検知として報告されたか、実際の異常として報告されたか、無視できるかを示します。

3 行を展開すると、選択した異常の詳細が表示されます。

4 異常レコードに対して次の処理を実行できます。

- 異常条件を無視できる場合は、[無視としてマーク (Mark as ignore)]をクリックします。
- 異常状態に何らかの処理を実行する場合は、[異常として確認 (Confirm as anomaly)]をクリックします。
- 異常が誤検知の場合は、[誤検知として報告 (Report as false positive)]をクリックします。同様の異常状態は、それ以降報告されません。

自動スキャンを有効にするための異常構成

10.1 より前の NetBackup では、異常検出プロセスにより、重大度が高い異常に対して自動マルウェアスキャンをトリガできます。必要な設定を行うには、プライマリサーバーの構成ファイルを使用します。

NetBackup 10.1 以降では、異常検出プロセスにより、構成ファイルの設定に基づいた、すべての異常の自動マルウェアスキャンをトリガできます。必要な設定を行うには、異常プロキシサーバーの構成ファイルを使用します。

p.572 の「マルウェアスキャンについて」を参照してください。

p.595 の「スキャンホストの前提条件」を参照してください。

異常が検出されたイメージの自動マルウェアスキャンを有効にするには

1. プライマリサーバー上の指定した場所に anomaly_config.conf 構成ファイルを作成します。

   Windows の場合: *Install_Path*¥NetBackup¥var¥global¥anomaly_detection

   UNIX の場合: /usr/openv/var/global/anomaly_detection

2. anomaly_config.conf 構成ファイルに次の内容を追加します。

```
#Use this setting to start malware scan on anomaly detected image automatically.

[AUTOMATED_MALWARE_SCAN_SETTINGS]

ENABLE_AUTOMATED_SCAN=1

# Enable all clients. In this case pool mentioned SCAN_HOST_POOL_NAME will be used for clients not mentioned

# under batch

ENABLE_ALL_CLIENTS=1

SCAN_HOST_POOL_NAME=<scan_host_pool_name> # Default pool name

#Use specific pool for mentioned clients

NUM_CLIENTS_BATCH_SPECIFIED=2

ENABLE_SCAN_ON_SPECIFIC_CLIENT_1=client1,client2

SCAN_HOST_POOL_NAME_1=<scan_host_pool_for_batch_1>

ENABLE_SCAN_ON_SPECIFIC_CLIENT_2=client3,client4

SCAN_HOST_POOL_NAME_2=<scan_host_pool_for_batch_2>
```

3. SCAN_HOST_POOL_NAME は必須フィールドです。

   ENABLE_SCAN_ON_SPECIFIC_CLIENT_n オプションについては、完全なクライアント名を指定する必要があります。

4 すべての設定が [AUTOMATED_MALWARE_SCAN_SETTINGS] の下にあることを確認します。設定に関する次の説明を確認します。

ENABLE_AUTOMATED_SCAN=1

高スコアの異常に対してマルウェアスキャンを開始します。

ENABLE_ALL_CLIENTS=1

スキャン対象としてすべてのクライアントを有効にします。この値が 0 の場合、スキャンは次のオプションに示すクライアントでのみ実行されます。

ENABLE_SCAN_ON_SPECIFIC_CLIENT_<Batch_Number>

NUM_CLIENTS_BATCH_SPECIFIED=<batches> - このオプションは、スキャンホストプールごとにバッチ数を指定します。たとえば、ある一連のクライアントに対して特定のスキャンホストプールを使用する場合は、この設定を使用します。

5 さまざまな重大度レベルの異常について、マルウェアスキャンを自動的にトリガするには、次の手順を実行します。

- 重大度が低い異常の場合は、次のように TRIGGER_SCAN_FOR_LOW_SEVERITY オプションを設定します。

  TRIGGER_SCAN_FOR_LOW_SEVERITY=1

- 重大度が中程度の異常の場合は、次のように TRIGGER_SCAN_FOR_MEDIUM_SEVERITY オプションを設定します。

  TRIGGER_SCAN_FOR_MEDIUM_SEVERITY=1

- 指定した値以上の異常スコアについてマルウェアスキャンを自動的にトリガするには、TRIGGER_SCAN_FOR_SCORE_GREATER_THAN オプションに正の値を設定します。

  例:

  TRIGGER_SCAN_FOR_SCORE_GREATER_THAN=2.5

  指定したランサムウェアファイル拡張子で検出された異常に対してマルウェアスキャンを自動的にトリガするには、次のように TRIGGER_SCAN_FOR_RANSOMWARE_EXT_IMAGES オプションを設定します。

  TRIGGER_SCAN_FOR_RANSOMWARE_EXT_IMAGES = 1

4

マルウェアスキャン

31

概要

この章では以下の項目について説明しています。

マルウェアスキャンについて

NetBackup は、サポート対象のバックアップイメージからマルウェアを検出し、マルウェアなしの最新の良好なイメージを検出します。この機能は、Standard、MS-Windows、NAS-Data-Protection、Cloud、Universal-Share と VMware の作業負荷でサポートされます。

マルウェアスキャンには次の利点があります。

- オンデマンドスキャンでサポートされているポリシー形式のバックアップイメージを 1 つ以上選択できます。スキャンホストの事前定義済みリストを使用できます。
- スキャン中にマルウェアが検出されると、Web UI で通知が生成されます。
- スキャナからアクセスできない、またはマルウェアスキャナからエラーが発生したためにファイルがスキップされた場合、スキップされたファイルの数とリストに関する情報とともに、次の通知が生成されます。
  - 重要な重大度: バックアップイメージでマルウェアが検出され、スキャン中に一部のファイルがスキップされた場合。
  - 警告の重大度: バックアップイメージでマルウェアが検出されず、スキャン中に一部のファイルがスキップされた場合。

この情報は、[処理 (Actions)]、[スキップされたファイルのエクスポート (Export skipped files)]リストの順に選択して取得できます。

メモ: リカバリ中に、マルウェアの影響を受けたバックアップイメージからのリカバリを開始すると、警告メッセージが表示され、リカバリを続行するための確認が必要になります。マルウェアの影響を受けたイメージからリストアする権限を持つユーザーのみがリカバリを続行できます。

リカバリ前のマルウェアスキャン

- ユーザーは、Web UI からのリカバリフローの一部として、リカバリ対象として選択したファイルまたはフォルダのマルウェアスキャンをトリガし、マルウェアスキャン結果に基づいてリカバリ処理を決定できます。
- バックアップイメージのカタログエントリは、バックアップでファイルのサブセットのみがスキャンされ、リカバリ時間のスキャン後に更新されません。マルウェアがリカバリ時間スキャンの一部として検出された場合、通知が生成されます。
- リカバリ時間スキャン中に、開始日と終了日の間のすべてのイメージをスキャンしてマルウェアを検出します。バックアップイメージのマルウェアスキャンは、リカバリ用に選択されたファイルの数によっては時間がかかる場合があります。リカバリに使用するイメージのみを含むように開始日と終了日を設定することをお勧めします。
- ユーザーは同じバックアップイメージの複数のリカバリ時間スキャンをトリガできます。
- リカバリの一部としてのマルウェアスキャンでは、スキャンホストの可用性と進行中のスキャンジョブ数に基づいて、サイズが小さいバックアップの場合、最低 15 分から 20 分かかることがあります。ユーザーは [アクティビティモニター (Activity monitor)]、[ジョブ (Jobs)]の順に使用し、進行状況を追跡できます。スキャン結果は、マルウェアの検出ページに段階的に表示されます。開始日と終了日の間のバックアップイメージのリストは、マルウェアスキャンの増分バッチで選択されます。
- リカバリ時間スキャンでサポートされているポリシー形式は、Standard、MS-Windows、Universal-Share、NAS-Data-Protection です。

メモ: リカバリ時間マルウェアスキャン操作を正常に実行するには、メディアサーバーのバージョンが 10.3 である必要があります。

マルウェアスキャンのワークフロー

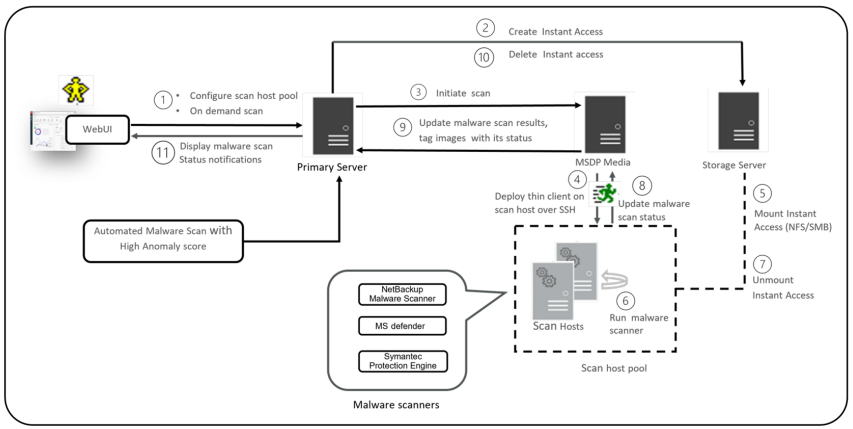
このセクションでは、次の項目に対するマルウェアスキャンのワークフローについて説明します。

- MSDP バックアップイメージ

- OST と AdvancedDisk

MSDP バックアップイメージのマルウェアスキャンのワークフロー

次の図に、MSDP バックアップイメージのマルウェアスキャンのワークフローを示します。



次の手順は、MSDP バックアップイメージのマルウェアスキャンのワークフローを示しています。

1. オンデマンドスキャンをトリガした後、プライマリサーバーはバックアップイメージを検証し、対象のバックアップイメージごとにスキャンジョブを作成し、それぞれで利用可能なスキャンホストを識別します。バックアップイメージを検証する条件の一部を次に示します。
   - バックアップイメージは、マルウェア検出でサポートされている必要があります。
   - バックアップイメージには有効なインスタントアクセスコピーが必要です。
   - オンデマンドスキャンの場合、同じバックアップイメージに対して既存のスキャンを実行中にすることはできません。DNAS の場合は、関連ストリームも考慮されます。
   - マルウェア検出では、ストレージに関連付けられたメディアサーバーはサポートされていません。
   - カタログからバックアップイメージの情報を取得できません。
2. オンデマンドスキャンのためにバックアップイメージがキューに登録されると、プライマリサーバーがストレージサーバーを識別します。スキャンホストプールで指定された構成済み共有形式のストレージサーバーに、インスタントアクセスマウントが作成されます。

メモ: 現在、プライマリサーバーは一度に 50 個のスキャンスレッドを開始します。スレッドが利用可能になると、キュー内の次のジョブが処理されます。それまでは、キューに投入されたジョブは保留中の状態になります。

NetBackup バージョン 10.3 以降、大規模なバックアップは 500K ファイルのバッチに分けてスキャンされます。各バッチは、個別のスキャンスレッドによってスキャンされます。

リカバリ時間スキャンでは、バッチごとのスキャン機能はサポートされません。

3. プライマリサーバーは、サポートされる利用可能な MSDP メディアサーバーを識別し、マルウェアスキャンを開始するようメディアサーバーに指示します。
4. MSDP メディアサーバーは、SSH を介してスキャンホストにシンクライアントを配備します。
5. シンクライアントは、スキャンホストにインスタントアクセスマウントをマウントします。
6. スキャンホストプールに構成されているマルウェアツールを使用してスキャンが開始されます。

   メディアサーバーは、スキャンホストからスキャンの進捗状況をフェッチし、プライマリサーバーを更新します。
7. スキャンが完了すると、スキャンホストはスキャンホストからインスタントアクセスマウントをマウント解除します。
8. SSH を介してメディアサーバーに通知されるマルウェアスキャンの状態が更新されます。スキャンログは、メディアサーバーのログディレクトリにコピーされます。
9. メディアサーバーは、プライマリサーバーに通知されるスキャン状態と感染ファイルリスト(感染ファイルが存在する場合)を、スキップされたファイルのリストと一緒に更新します。
10. プライマリサーバーは、スキャン結果を更新し、インスタントアクセスを削除します。
11. マルウェアスキャン状態の通知が生成されます。
12. スキャン時に更新がない場合、マルウェアスキャンはタイムアウトします。デフォルトのタイムアウト期間は 48 時間です。

マルウェア検出では、30 日以上経過した該当するスキャンジョブの自動クリーンアップが実行されます。

メモ: 感染したスキャンジョブは自動的にクリーニングされます。

p.625 の「MALWARE_DETECTION_CLEANUP_PERIOD」を参照してください。

メモ: Microsoft Azure Marketplace と AWS Marketplace からマルウェアスキャナをダウンロードできます。AWS 向けと Azure 向けのマルウェアスキャナをインストール、構成、使用する方法に関する指示に従ってください。

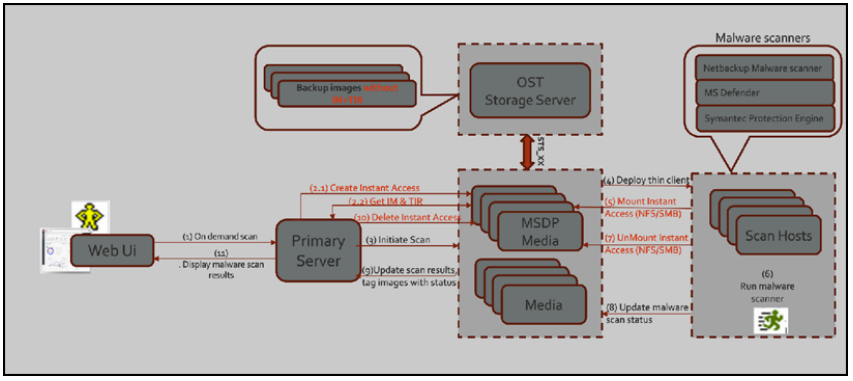
詳しくは、次を参照してください。

AWS: AWS マーケットプレイスおよび『AWS クラウドでの NetBackup マーケットプレイス配備』

Microsoft Azure: Microsoft Azure マーケットプレイスおよび Microsoft Azure マーケットプレイス

OST と AdvancedDisk のマルウェアスキャンのワークフロー

次の図に、OST と AdvancedDisk のマルウェアスキャンのワークフローを示します。



OST と AdvancedDisk のマルウェアスキャンには、次の前提条件があります。

- インスタントアクセスマウントには、SPWS、VPFSD などの MSDP コンポーネントが必要です。そのため、OST と AdvancedDisk ストレージの場合、任意のメディアサーバーを MSDP ストレージサーバーとして構成して、インスタントアクセス API を処理できるようにする必要があります。
- プライマリサーバーとメディアサーバーは、NetBackup バージョン 10.3 にアップグレードする必要があります。
- メディアサーバーは、OST または AdvancedDisk ストレージサーバーにアクセスできる必要があります。
- OST プラグインは、インスタントアクセス (MSDP コンポーネントが含まれるホスト) ホストに配備する必要があります。OST プラグインの新しいバージョンは必要ありません。
- 互換性のあるインスタントアクセスホスト (RHEL)。

- OST と AdvancedDisk STU からの同時インスタントアクセスのスロットル制限は、MSDP からのインスタントアクセスと同じです。

サポート対象の OST デバイスの完全なリストについては、NetBackup ソフトウェア互換性リストまたは NetBackup ハードウェア互換性リストを参照してください。

次の手順は、OST と AdvancedDisk のマルウェアスキャンのワークフローを示しています。

1. オンデマンドスキャン API を使用して、バックアップイメージがプライマリサーバーの作業リストテーブルに追加されます。

   プライマリサーバーは、指定したスキャンホストプールから利用可能なスキャンホストを識別します。

2. 作業リストの処理の一部として、次の操作を行います。

   (2.1) インスタントアクセス用メディアサーバーの作成:

   - バックアップイメージから、ストレージサーバーを見つけます。
   - ストレージサーバーから、適格なメディアサーバーを見つけます。
     インスタントアクセス機能を備えたメディアサーバー。
     NetBackup バージョン 10.3 以降のメディアサーバー。
   - 選択したメディアサーバーにインスタントアクセス API 要求を送信します。
   - 複数のメディアサーバーがインスタントアクセスマウント要求の対象である場合、進行中のインスタントアクセス要求の数が最小のメディアサーバーが選択されます。これにより、インスタントアクセス要求を分散し、負荷分散を実現できます。

   (2.2) IM と TIR の取得

   - 選択したメディアサーバーの、インスタントアクセス API のコンテキストで、プライマリサーバーから IM および TIR 情報をフェッチします。VPFSD によるバックアップイメージのマウントに OS が必要とするのと同じ形式で情報を格納します。
   - インスタントアクセスマウント後、IO ファイルの場合、VPFSD は OST API を使用してストレージサーバーからバックアップイメージを読み込みます。
   - `mountId`、`exportPath`、`storageserver`、`status` を使用してインスタントアクセスが実行されたイメージで、作業リストを更新します。

3. プライマリサーバーは、利用可能な MSDP メディアサーバーを識別し、マルウェアスキャンを開始するようメディアサーバーに指示します。

メモ: インスタントアクセスマウント用に選択されたメディアサーバーと、スキャンホストとの通信用に選択されるサーバーは、同じサーバーまたは異なるサーバーにすることができます。

---

4. スキャン要求を受信すると、メディアサーバーのスキャンマネージャは、SSH を使用したリモート通信を介して、シンクライアント (nbmalwareutil) を使用してスキャンホスト上のマルウェアスキャンを開始します。
5. スキャンホストの構成に応じて、メディアサーバーの NFS または SMB を使用して、スキャンホストからエクスポートをマウントします。このメディアサーバーで、バックアップイメージがインスタントアクセス API を使用してマウントされます。
6. スキャンホストプールに構成されているマルウェアツールを使用してスキャンが開始されます。

メモ: メディアサーバーの VPFSD は、STS_XXX API を使用して OST または AdvancedDisk ストレージサーバーからバックアップイメージを開き、読み込みます。

7. スキャンが完了すると、スキャンホストは、インスタントアクセス API を使用してバックアップイメージがマウントされているメディアサーバーからエクスポートパスのマウントを解除します。
8. SSH を介してメディアサーバーに通知されるマルウェアスキャンの状態が更新されます。スキャンログは、メディアサーバーのログディレクトリにコピーされます。
9. メディアサーバーは、プライマリサーバーに通知されるスキャン状態と感染ファイルリスト (感染ファイルが存在する場合) を更新します。
10. プライマリサーバーは、スキャン結果を更新し、選択したメディアへのインスタントアクセス要求を削除します。
11. マルウェアスキャン状態の通知が生成されます。

動的スキャンについて

Standard、MS-Windows、NAS-Data-Protection の作業負荷でマルウェアをスキャンするため、NetBackup 10.3 では動的スキャン機能が導入されています。この機能は、ファイルがアクセスされて読み込まれるか、ファイルのプロビジョニングにオーバーヘッドがない場合を除き、必要に応じてバックアップイメージ内のすべてのファイルをプロビジョニングします。

インスタントアクセスマウントポイントを使用する従来のスキャンと比べ、動的スキャンでは、MSDP に対するインスタントアクセスとスキャンのパフォーマンスが最適化されます (バックアップに多数のファイルが含まれる場合)。これにより、インスタントアクセスにかかる時間とスキャンのパフォーマンスが向上します。

次の表に、従来のマルウェアスキャンと動的スキャンの違いを示します。

主なスキャン手順	インスタントアクセスマウントポイントを使用した従来のマルウェアスキャン	動的スキャン
インスタントアクセスをステージングする。	tar ストリームを分析し、各ファイルのヘッダーおよびエクステントマップファイル (LMDB データベース) をビルドします。これは、バックアップに多数のファイルがあるために時間がかかります。	フラグメントから TIR (カタログデータベース) と IM (イメージメタデータ) 情報をリストアします。
インスタントアクセス共有 (NFS/SMB) がマウントされ、ユーザーがファイルを一覧表示またはアクセスしようとする。	ヘッダーファイルにアクセスし、そこから属性を読み取ります。	カタログデータベースのディレクトリに問い合わせ、このディレクトリにあるすべてのファイルとディレクトリを取得します。また、各ファイルとディレクトリの属性を出力に問い合わせることもできます。
スキャンホストがファイルを開く	LMDB データベースを開き、ロードします。	メモリ内にインデックスをビルドし、データコンテナから直接読み取ります。 ■ ファイルのエクステントを取得するには、tar ヘッダーを見つけて読み取り、内容を分析します。 ■ SO リストを取得するには (PureDisk のみ)、フラグメントの FP マップから SO リストを検索します。 ■ マッピングテーブルをビルドするには、SO リストを挿入します (PureDisk のみ)。
スキャンホストがファイルを読み取る	LMDB データベースから検索し、データコンテナから読み取ります。	ストレージサーバーがサードパーティのストレージベンダー製の場合、データは OST インターフェースを介して直接読み取られます。ストレージサーバーが PureDisk の場合、マッピングテーブルから検索され、データはデータコンテナから読み取られます。

NetBackup 10.3 は、マルウェアスキャン用に、OST ターゲットボリュームバックアップでのインスタントアクセスをサポートし、サイズの大きい ADS 情報のマルウェアスキャンをサポートします。

- MSDP ストレージの場合、動的スキャン機能は、BYO、NBA、Flex、Flex-worm、FlexScale、Azure Kubernetes Services クラスタ、Amazon Elastic Kubernetes クラスタのプラットフォームに適用されます。
- OST および AdvancedDisk ストレージの場合、動的スキャン機能は、BYO、NBA、Flex アプライアンスのプラットフォームにのみ適用されます。

マルウェアスキャンを設定する方法

表 31-1 マルウェアスキャンを設定する手順

手順の説明	リンク
プライマリサーバー、メディアサーバー、MSDP ストレージサーバーで NetBackup ソフトウェアをインストールするか、バージョン 10.0 以降にアップグレードします。	『NetBackup インストール/アップグレードガイド』
BYO 設定の場合、MSDP ストレージサーバーでインスタントアクセスを構成する必要があります。	『Veritas NetBackup™ 重複排除ガイド』にある「ユニバーサル共有の構成」セクションを参照してください
NFS や SMB などの必要な共有タイプを構成します。 注意: ■ MSDP ストレージサーバーで次の手順を実行します。 ■ NFS および SMB 設定を行います。また、NFS または SMB クライアントがスキャンホスト上に存在する必要があります。 ■ SMB 共有の場合、ストレージサーバーが Active Directory ドメインに接続または結合されていることを確認し、Active Directory ドメインの詳細と有効なユーザークレデンシャルを取得します。 ■ 共有タイプで指定したユーザーに、マウントに必要な権限があることを確認します。	『Veritas NetBackup™ 重複排除ガイド』にある「ユニバーサル共有の構成」セクションを参照してください

手順の説明	リンク
スキャンホストで、次のいずれかのマルウェアツールを構成します。 ■ NetBackup マルウェアスキャナ ■ Symantec Protection Engine ■ Microsoft Defender ウイルス対策 **メモ:** ホストユーザーが、構成済みのマルウェアツールを使用したスキャンに必要な権限を持っており、ストレージサーバーのマウントにアクセスできることを確認します。	p.595 の「スキャンホストの前提条件」を参照してください。
NetBackup Web UI で、マルウェア検出の設定を行います。	p.600 の「新しいスキャンホストプールの構成」を参照してください。

スキャンインスタンスの構成

インスタントアクセスを使用する従来のマルウェアスキャンは、vpfsd インスタンスに基づいています。NetBackup 10.2.1 は、マルウェアスキャンに別個の vpfsd インスタンスを使用しており、これは構成可能です。この構成は numOfScanInstance パラメータを使用して行います。デフォルトでは、マルウェアスキャンでは 1 つのインスタンスが使用されます。ほとんどの場合、スキャンインスタンスは適切ですが、スキャンインスタンスの数を増やすとスキャンパフォーマンスは向上します。ただし、必要な CPU とメモリも増えます。スキャンインスタンスの数は 1 から 4 まで増やすことができ、マルウェアスキャン共有をすべてのスキャンインスタンスに分散できます。

スキャンインスタンスの数を変更するには

1. 次のコマンドを使用して、メディアサーバー上の NetBackup を停止します。

   ```
   systemctl stop netbackup
   ```

   または

   ```
   /usr/openv/netbackup/bin/goodies/netbackup stop
   ```

2. スキャンインスタンスの数を次のように変更します。

   vpfsd_config.json ファイルにある numOfScanInstance パラメータの値を変更します。値は 1 から 4 の整数である必要があります。

   例:

   ```
   # grep numOfInstance /msdp/vol1/etc/puredisk/vpfsd_config.json
   "numOfScanInstance": 2、
   ```

   BYO (build-your-own): `<storage path>/etc/puredisk/vpfsd_config.json`

   NetBackup Appliance および NetBackup Flex Scale: `/msdp/data/dp1/pdvol/etc/puredisk/vpfsd_config.json`

   NetBackup Flex: `/mnt/msdp/vol0/etc/puredisk/vpfsd_config.json`

3. vpfsd インスタンスの数 (numOfInstance) を変更します。値は 2 から 16 の整数である必要があります。numOfInstance の値が numOfScanInstance より大きいことを確認します。

4. 次のコマンドを使用して、メディアサーバー上の NetBackup を起動します。

   ```
   systemctl start netbackup
   ```

   または

   ```
   /usr/openv/netbackup/bin/goodies/netbackup start
   ```

メモ: マルウェアスキャンのインスタンスは vpfsd インスタンスの一部で、マルウェアスキャン専用として予約されています。

制限事項

- 従来の NetBackup エージェントとクライアント側の暗号化、またはエージェントおよびクライアントベースの圧縮バックアップは、インスタントアクセスマウントポイントを使用したスキャンには使用できません。推奨されるのは MSDP KMS ベースの暗号化技術で、これは構成できます (『NetBackup セキュリティおよび暗号化ガイド』を参照)。
- ユーザーアーカイブバックアップと合成バックアップは、インスタントアクセスマウントポイントを使用したスキャンには利用できません。

- VMware 製品の場合: アクセラレータ機能が有効になっていない増分バックアップイメージは、VMware 作業負荷ではサポートされません。
- Windows EFS ファイルまたはフォルダは、インスタントアクセスマウントポイントを使用したスキャンには利用できません。
- (OST と AdvancedDisk の場合) 非構造化データのマルウェアスキャンのみをサポートします。詳しくは、NetBackup ソフトウェア互換性リストを参照してください。
- NetBackup は、AKS/EKS Active Directory プラットフォームで SMB 共有タイプをサポートしていません。詳しくは、『NetBackup 重複排除ガイド』を参照してください。
- 異なる NetBackup ドメインにレプリケートされた NetBackup イメージは、ターゲットドメインで再びスキャンする必要があります。ソースドメインにあるバックアップイメージのマルウェアスキャンに関する詳細な状態 (感染ファイルのリスト、使用したマルウェアスキャナ、署名情報など) は、レプリケーション中に保持されません。
- メディアサーバーと、アップグレードされたメディアサーバーにある古いバックアップイメージとの間の旧バージョンの互換性は、NetBackup バージョン 10.3 以降でのみサポートされます。このサポートは、NetBackup バージョン 10.3 で提供される、作業負荷の種類のサポートに適用されます。

32

マルウェアツール

この章では以下の項目について説明しています。

サポート対象のマルウェアツール

NetBackup では、次のマルウェア検出ツールがサポートされています。

- NetBackup マルウェアスキャナ (Avira)

  メモ: マルウェアの署名は各スキャン前に更新されます。スキャンホストがインターネットにアクセスできない場合は、次のセクションを参照してください。

  p.585 の「シグネチャ更新のためのミラーサーバーの構成」を参照してください。

  p.587 の「NetBackup マルウェアスキャナの Windows および Linux 向けの構成」を参照してください。

- Symantec Protection Engine
  p.593 の「Symantec Protection Engine の構成」を参照してください。
- Microsoft Defender ウイルス対策
  p.594 の「Microsoft Defender ウイルス対策の構成」を参照してください。

メモ: Windows スキャンホスト上の他のマルウェアスキャナツールを使用する場合、ユーザーは、マルウェアスキャンの進行中に Windows Defender のリアルタイム保護オプションを無効にする必要があります。

NetBackup マルウェアスキャナ (Avira) の構成

このセクションでは、Windows と Linux でのシグネチャの更新とマルウェアスキャナの構成について説明します。

シグネチャ更新のためのミラーサーバーの構成

NetBackup マルウェアスキャナ (Avira) ミラーサーバーは、スキャンホストがインターネットにアクセスできない場合にのみシグネチャの更新用に構成する必要があります。

ローカルミラーサーバーの作成

1. 指定されたホストに NetBackup マルウェアスキャナをインストールする必要があります。
2. NetBackup マルウェアスキャナをインストールするために使用したユーザークレデンシャルを使用してログインし、次のコマンドを実行します。

   ```
   cd $NB_MALWARE_SCANNER_PATH
   ```

   ```
   ./avupdate.bin --mirror --config=avupdate-savapilib-product.conf
   --install-dir=<update_path>
   ```

3. HTTP 経由で `<update_path>` を公開します。

   たとえば、https://<local_mirror_server>/<update_path> です。

メモ: 定期的に `./avupdate.bin --mirror` コマンドを実行して、ミラーサーバー上のシグネチャデータを最新の状態に保ちます。

シグネチャの更新時のローカルミラーサーバーの使用

1. update.sh スクリプトは、update.sh と同じ場所 ($NB_MALWARE_SCANNER_PATH) にある avupdate-savapilib-product.conf ファイルを参照します。
2. 前述のローカルミラーサーバーが提供する URL を指すように、.conf ファイルの internet-srvs エントリを更新します。

```
~/savapi-sdk-linux64/bin> cat avupdate-savapilib-product.conf
#This configuration updates the entire SAVAPI Library (binaries,
 engine, signatures)
#internet-srvs=https://oem.avira-update.com/update
internet-srvs=https://<local_mirror_server>/<update_path>
master-file=/idx/master.idx
product-file=/idx/savapi4lib-linux64-en.info.gz
install-dir=./
temp-dir=./tmp
check-product
```

3 update.sh スクリプトを実行して、更新が正しく動作していることを確認します。

avupdate.log ファイルには次のエントリが表示されます。

```
~/savapi-sdk-linux64/bin> head avupdate.log
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
 Avupdate Version: 2.6.10.36
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
 Operating System: LINUX X86_64 5.3.18-22-DEFAULT
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
 Installation Directory: .
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
 Backup Directory: ./avupdate_backup
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
 Temp Directory: ./tmp/avupdate_tmp_njoOb5
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
 Cache Modules Directory: ./idx
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:
 Proxy settings: Direct connection
18/09/2022 23:31:47 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:

Downloading
https://local_mirror_server/<update_path>/idx/master.idx
to ./tmp/avupdate_tmp_njoOb5/idx/master.idx
18/09/2022 23:31:48 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:

Downloading
https://<local_mirror_server>/<update_path>/idx/savapi4lib-linux64-en.info.gz

to ./tmp/avupdate_tmp_njoOb5/idx/savapi4lib-linux64-en.info.gz
18/09/2022 23:31:49 pndch32bl10-09 avupdate.bin[10929]: UPD: INFO:

Downloading
https://<local_mirror_server>/<update_path>/idx/xvdf.info.gz
to ./tmp/avupdate_tmp_njoOb5/idx/xvdf.info.gz
```

NetBackup マルウェアスキャナの Windows および Linux 向けの構成

メモ: NetBackup マルウェアスキャナのアップグレード前またはマスターサーバーの再起動前に、スキャンジョブがキャンセルされていることを確認します。

NetBackup マルウェアスキャナの Windows 向けの構成

NetBackup マルウェアスキャナを Windows 向けに構成するには

1. NetBackup マルウェアスキャナをベリタスダウンロードセンターからダウンロードします。
2. ダウンロードした zip ファイルを解凍します。解凍したファイルの構造は次のとおりです。

```
NBAntiMalwareClient_version number
   Readme.txt

    NBAntiMalwareClient_version number_AMD64
      savapi-sdk-win64.zip
         setup.bat
         cleanup.bat
```

3. `Readme.txt` ファイルでインストール、アップグレード、またはアンインストール処理を参照します。

   NetBackup マルウェアスキャナを Windows コンピュータにインストールまたはアップグレードするには:

   - `NBAntiMalwareClient_<`**バージョン番号**`>_AMD64` フォルダに移動して、`setup.bat` ファイルを実行します。
   - NetBackup マルウェアスキャナのインストール先を入力します。

   メモ: NetBackup マルウェアスキャナがすでにインストールされている場合、`setup.bat/setup.sh` は既存のバイナリファイルを上書きします。

   Windows コンピュータから NetBackup マルウェアスキャナをアンインストールするには:

   - `cleanup.bat` ファイルを実行します。

4 オプション設定を使用して、スキャン中のスレッド数を増やすことができます。

aviraconf.txt ファイルを更新します。次のエントリを追加します。

NumThreads = *Number of threads*

ここで、*Number of threads* はスキャンのスレッド数です。デフォルト値は CPU コアの数です。(最小値は 1、最大値は 300 です)

メモ: スキャンホストの CPU の数が 16 未満の場合、スレッド数はデフォルトで CPU の数になります。16 を超える場合、スレッド数はデフォルトで 16 個のスレッドになります。NumThreads が構成されている場合、その値によってスキャンするスレッド数が決まります。

---

5 Windows セットアップで、NetBackup マルウェアスキャナを使用したスキャンが実行されていることを検証するには、次の手順を実行します。

- ./update.bat コマンドを実行して、最新のシグネチャアップデートを取得します。
- NetBackup マルウェアスキャナがインストールされているパスに移動し、必要な scan_path と conf_path パラメータを指定して avira_lib_dir_scan.exe ファイルを実行します。

6 NetBackup マルウェアスキャナのインストールパスには、構成ファイルがあるはずです。

例:

```
avira_lib_dir_scan.exe "c:¥malwarescample" -log_path
"C:¥NBMalwareScanner.log" -conf_path
"C:¥NBMalwareScannerInstallPath¥savapi-sdk-win64¥bin¥aviraconf.txt
```

コマンドの出力が成功したことを確認します。既存のサンプルマルウェアファイルの場合、出力は感染ファイルのリストになります。それ以外の場合、出力は空になります。

7 (オプション) ログ記録レベルを上げるには、環境変数 MALWARE_LOG を使用します。

たとえば、MALWARE_LOG=2 設定は、ログ記録レベルを**警告**に設定します。

```
0 DEBUG
1 INFO
2 WARNING
3 ALERT
4 ERROR
```

Windows でのプロキシサーバーの構成

Windows でプロキシサーバーを構成するには

1 http_proxy 名と <proxy_server> の値を使用して、環境変数にプロキシサーバーエントリを追加します。

例:

```
http_proxy=http://<username>:<password>@proxy_server_ip:<port>
```

2 avupdate-savapilib-product.conf ファイルにプロキシサーバーの詳細を追加します。このファイルは、NetBackup マルウェアスキャナのインストールパスで利用可能です。

例:

```
proxy-username=<username>
proxy-password=<password_paintext>
proxy-host=<proxy_server_ip>
proxy-port=<proxy_server_port>
update-auth-type=any
receive-timeout=600000
connect-timeout=600000
```

NetBackup マルウェアスキャナの Linux 向けの構成

NetBackup マルウェアスキャナを Linux 向けに構成するには

1 NetBackup マルウェアスキャナをベリタスダウンロードセンターからダウンロードします。

2 ダウンロードした zip ファイルを解凍します。ファイルは次のような構造になっているはずです。

```
NBAntiMalwareClient_version number_LinuxR_x86
      savapi-sdk-linux64.zip
        setup.sh
        cleanup.sh

NBAntiMalwareClient_version number_LinuxS_x86 ->
NBAntiMalwareClient_version number_LinuxR_x86
      savapi-sdk-linux64.zip
        setup.sh
        cleanup.sh
```

警告: setup.sh スクリプトは Linux の bashrc ファイルを修正します。

3 Readme.txt ファイルでインストール、アップグレード、またはアンインストール処理を参照します。

Linux RHEL コンピュータで NetBackup マルウェアスキャナをインストールまたはアップグレードする場合:

- NBAntiMalwareClient_<**バージョン番号**>_LinuxR_x86 フォルダに移動して、setup.sh スクリプトを実行します。
- NetBackup マルウェアスキャナのインストール先を入力します。

Linux SUSE コンピュータで NetBackup マルウェアスキャナをインストールまたはアップグレードする場合:

- NBAntiMalwareClient_<**バージョン番号**>_LinuxS_x86 フォルダに移動して、setup.sh スクリプトを実行します。
- NetBackup マルウェアスキャナのインストール先を入力します。

メモ: Linux SUSE コンピュータでは、.bashrc ファイルがない場合は、ユーザーのホームディレクトリに空の .bashrc ファイルを作成します。

Linux コンピュータから NetBackup マルウェアスキャナをアンインストールする場合:

- cleanup.sh スクリプトを実行します。

4 Linux セットアップで、NetBackup マルウェアスキャナを使用したスキャンが実行されていることを検証するには、次の手順を実行します。

- ./update.sh スクリプトを実行して、最新のシグネチャアップデートを取得します。
- NetBackup マルウェアスキャナがインストールされているパスに移動し、必要なスキャンパスと conf_path パラメータを指定して avira_lib_dir_scan バイナリを実行します。
- NetBackup マルウェアスキャナのインストールパスには、構成ファイルがあるはずです。
  次に例を示します。

```
avira_lib_dir_scan "/root/malwareSample" -log_path
"/root/NBMalwareScanner.log" -conf_path
"/root/NBMalwareScannerInstalledPath/savapi-sdk-linux64/bin/
aviraconf.txt
```

  コマンドの出力が成功したことを確認します。既存のサンプルマルウェアファイルの場合、出力は感染ファイルのリストになります。それ以外の場合、出力は空になります。

Windows でのプロキシサーバーの構成

Linux でプロキシサーバーを構成するには

- http_proxy 名を使用して、環境変数にプロキシサーバーエントリを追加します。
  例:
  `http_proxy=http://<username>:<password>@proxy_server_ip:<port>`
  この変数は、スキャンホストの `.bashrc` ファイルに追加する必要があります。
- `avupdate-savapilib-product.conf` ファイルにプロキシサーバーの詳細を追加します。
  例:

```
proxy-username=<username>
proxy-password=<password_paintext>
proxy-host=<proxy_server_ip>
proxy-port=<proxy_server_port>
update-auth-type=any
receive-timeout=600000
connect-timeout=600000
```

- マルウェアのスキャンに正しいプロキシ設定が使用されているかどうかを、`savapi` ログで確認します。

Symantec Protection Engine の構成

Windows

Symantec Protection Engine の Windows 向けの構成

1 PATH 環境変数にコマンドラインの実行可能パスを設定します。

例: `C:¥Program Files¥Symantec¥Scan Engine¥CmdLineScanner¥C`

2 コマンドプロンプトで次のコマンドを実行し、出力を確認します。

```
ssecls -mode scan -scantype S C:¥
```

メモ: ライセンスエラーが発生した場合は、更新されたライセンスを適用します。

3 (オプション) SCAN_FILE_BUCKET_SIZE 環境変数を設定します。

例:

```
SCAN_FILE_BUCKET_SIZE = 40

If SCAN_FILE_BUCKET_SIZE not set then default
SCAN_FILE_BUCKET_SIZE is 20.
```

メモ: `ssecls` スキャナ CLI では、コマンドラインで指定した複数ファイルを一度にスキャンできます。SCAN_FILE_BUCKET_SIZE 環境変数を更新して、デフォルト値の 20 を変更できます。

Linux

Symantec Protection Engine の Linux 向けの構成

1 bashrc ファイルの LD_LIBRARY_PATH および PATH に実行可能パスを設定します。

例: LD_LIBRARY_PATH=
$LD_LIBRARY_PATH:/opt/SYMCScan/ssecls/C:/root/clientserver-2.10.97.234/bin

2 コマンドプロンプトで次のコマンドを実行し、出力を確認します。

```
ssecls -mode scan -scantype F /
```

メモ: ライセンスエラーが発生した場合は、更新されたライセンスを適用します。

3 (オプション) SCAN_FILE_BUCKET_SIZE 環境変数を設定します。

例:

```
SCAN_FILE_BUCKET_SIZE = 40

If SCAN_FILE_BUCKET_SIZE not set then default
SCAN_FILE_BUCKET_SIZE is 20.
```

Microsoft Defender ウイルス対策の構成

Microsoft Windows Defender ウイルス対策の構成

1 [コントロール パネル (Control Panel)]、[システムとセキュリティ (System and Security)]、[システム (System)]の順に移動し、[システムの詳細設定 (Advanced System)]を選択して PATH 環境変数に実行可能パスを設定します。

例: C:¥Program Files¥Windows Defender

2 コマンドプロンプトで、次のコマンドを実行します。

```
MpCmdRun -Scan -ScanType 3 -DisableRemediation -File <filepath>
check if result is proper
```

例:

```
C:¥Program Files¥Windows Defender>MpCmdRun -Scan -ScanType 3
-DisableRemediation -File "C:¥Program Files¥Windows Defender"
Scan starting...
Scan finished.
Scanning C:¥Program Files¥Windows Defender found no threats.
```

33

構成

この章では以下の項目について説明しています。

スキャンホストの前提条件

スキャンホストは、必要なマルウェアツールが構成されているホストマシンです。NetBackup と統合されると、NetBackup はスキャンホストでのスキャンを開始します。

次の前提条件を満たしていることを確認します。

- スキャンホストに必要な最小構成は、8 つの CPU と 32 GB の RAM です。
- マルウェアツールをインストールして構成する必要があります。
- スキャンホストのサポート対象オペレーティングシステムについては、ソフトウェア互換性リストを参照してください。
- スキャンホストには、NFS または SMB クライアントの共有タイプが構成されている必要があります。
- スキャンホストで NetBackup フットプリントは不要です。NetBackup クライアントまたはメディアサーバーを備えた既存のシステムもスキャンホストとして使用できます。
- スキャンホストは、SSH を介してメディアサーバーから到達可能である必要があります。

メモ: メディアサーバーからホストをスキャンするための SSH 接続が成功する必要があります。

- プラットフォームに応じて、次の手順を実行します。

  (Windows の場合)

  - OpenSSH は Windows スキャンホストで構成する必要があります。メディアサーバーからスキャンホストにアクセスできるように、OpenSSH のファイアウォールルールを作成します。

  次の点に注意してください。

  - Windows 2016 の場合は GitHub リポジトリから OpenSSH を取得し、Windows 2019 の場合は OpenSSH サーバー機能を有効にします。詳しくは、Microsoft 社のマニュアルを参照してください。
  - メディアサーバーが 10.1.1 以降に更新された場合、Microsoft Visual C/C++ 再頒布可能パッケージは追加で依存関係になります。
    Windows スキャンホストで nbmalwareutil ユーティリティを実行するには、Visual C/C++ ランタイムライブラリ DLL が必要です。ランタイム DLL は、Microsoft Visual C++ 再頒布可能パッケージの最新のサポート対象ダウンロードに関する記事から取得できます。

  (Linux の場合)

  - Linux スキャンホストのデフォルトのログインシェルは bash である必要があります。
  - NetBackup マルウェア検出ユーティリティをスキャンホストで実行するには、スキャンホストに libnsl.so.1 ライブラリをインストールします。libnsl ライブラリファイルの最新バージョン (/usr/lib64/libnsl.so.2 など) が存在する場合、/usr/lib64/libnsl.so.2 ファイルを指すソフトリンクファイル /usr/lib64/libnsl.so.1 を作成します。
    ソフトリンクファイルの作成例:

    ```
    # cd /usr/lib64 # ln -sf libnsl.so.2 libnsl.so.1
    ```

    メモ: libnsl* ライブラリファイルのインストールについてサポートを受けるには、オペレーティングシステムの管理者にお問い合わせください。

  - Windows での管理者以外のユーザーの場合: Windows スキャンホストの管理者以外のユーザーを管理者グループに追加する必要があります。
  - Linux での root 以外のユーザーの場合:
    - root 以外のユーザーを使用して ssh 接続を許可します。

たとえば、/etc/ssh/sshd_config ファイルに Allow Users root scanuser エントリを追加します。

メモ: スキャンユーザーは、システムで作成されている root 以外のユーザーです。

- マウントおよびマウント解除するユーザー権限を指定します。sodoers ファイルにユーザー権限エントリを追加します。
  たとえば、/etc/sudoers ファイルで、次のいずれかを追加します。
  - scanuser ALL=(ALL) NOPASSWD:ALL
  - scanuser ALL=(ALL) NOPASSWD:/bin/umount, /bin/mount
- スキャンホストで root 以外のユーザーを使用してマルウェアツールを構成します。

メモ: root ユーザーを使用してスキャンを実行した場合は、/tmp/malware フォルダの権限を変更して、root 以外のユーザーに書き込み権限を付与します。

メモ: 例: chmod a+rwx /tmp/malware

NFS 共有形式の Windows スキャンホストの前提条件

ID マッピングへの変更が行われた場合は、Web UI からスキャンホストのクレデンシャル検証を再実行します。

1 ローカルの passwd ファイルマッピングを有効にします。

```
C:¥Users¥Administrator> Set-NfsMappingStore -EnableUNMLookup
$True  -UNMServer localhost
C:¥Users¥Administrator> nfsadmin mapping

The following are the settings on localhost

Mapping Server Lookup       : Enabled
Mapping Server              : localhost
AD Lookup                   : Disabled
AD Domain                   :
```

2 エントリは、それぞれのファイル (ファイルの種類の形式) で次のように指定する必要があります。

C:¥Windows¥System32¥drivers¥etc¥passwd ファイル:

```
scanuser:x:1001:1001:Description:C:¥Users¥scanuser
```

C:¥Windows¥System32¥drivers¥etc¥group ファイル:

```
scangroup:x:1001:1001
```

3 次のように nfsadmin クライアントを再起動します。

```
nfsadmin client stop

nfsadmin client start
```

4 PowerShell を使用して次のコマンドを実行して、ユーザーの ID (UID/GID) マッピングを確認します。

```
Get-NfsMappedIdentity -AccountName Administrator -AccountType
User

UserIdentifier      : 0
GroupIdentifier     : 0
UserName            : Administrator
PrimaryGroup        :
SupplementaryGroups :
```

メモ: VMware とクラウドの作業負荷ポリシーのスキャンの場合、UID と GID のマッピングを 0 に設定する必要があります。

(Azure または AWS でマーケットプレイスイメージからスキャンホストが作成されている場合) 次のように、スキャンホストの root アクセスを有効にします。

- 次のコマンドを使用して、root パスワードを変更します。

  ```
  - sudo -i passwd
  ```

- /etc/ssh/sshd_config ファイルを変更して、次のようにして root ログインに対して許可を付与します。

  ```
  "PermitRootLogin yes"
  "PasswordAuthentication yes"
  ```

- 次のコマンドを使用してサービスを再起動します。

  ```
  - service sshd reload
  ```

- root ユーザーを有効にするには、/etc/cloud/cloud/cloud.cfg ファイルを次のように変更します。

  ```
  disable_root 0
  ```

マルウェアスキャンのインスタントアクセスのチューニングパラメータ

- Linux カーネルの vm.max_map_count パラメータを更新するには、次の手順を実行します。
  - /etc/sysctl.conf ファイルに、次のパラメータに値を指定して追加します。

    ```
    vm.max_map_count=262144
    ```

  - 次のコマンドを使用して、構成ファイルを再ロードします。

    ```
    root: sysctl -p
    ```

  - 次のコマンドを使用して、vm.max_map_count パラメータの新しい値が更新されたことを確認します。

    ```
    cat /proc/sys/vm/max_map_count
    ```

スキャンホストプールの構成

スキャンホストプールの前提条件

スキャンホストプールは、スキャンホストのグループです。スキャンホストの構成が完了する前に、NetBackup Web UI からスキャンホストプールの構成を実行する必要があります。

- スキャンホストプールに追加したすべてのスキャンホストには、スキャンホストプールと同じマルウェアツールが必要です。
- プールに追加されたすべてのスキャンホストには、スキャンホストプールと同じ共有タイプが必要です。
- スキャンプールにスキャンホストを追加するには、スキャンホストのクレデンシャルと RSA キーが必要です。スキャンホストの RSA キーを取得するには、p.602 の「クレデンシャルの管理」を参照してください。
- スキャンを実行する前に、スキャンホストがアクティブで、スキャンホストプールで利用可能であることを確認します。

新しいスキャンホストプールの構成

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで右上隅の[マルウェアの検出設定 (Malware detection settings)]、[マルウェアスキャナホストプール (Malware scanner host pools)]の順に選択し、ホストプールリストのページに移動します。
3. [マルウェアスキャナホストプール (Malware scanner host pools)]ページで[追加 (Add)]をクリックし、新しいホストプールを追加します。
4. [マルウェアスキャナホストプールの追加 (Add malware scanner host pools)]ページで、[ホストプール名 (Host pool name)]、[マルウェアスキャナ (Malware scanner)]、[共有の種類 (Type of share)]などの詳細情報を入力します。
5. [ホストを保存して追加 (Save and add hosts)]をクリックします。

スキャンホストプールへの新しいホストの追加

この手順を使用して、構成済みのスキャンホストプールに新しいスキャンホストを追加します。

メモ: 新しいスキャンホストを構成するにはp.595 の「スキャンホストの前提条件」を参照してください。

---

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページをクリックし、右上隅の[マルウェアの検出設定 (Malware detection settings)]をクリックします。
3. [マルウェアスキャナホストプール (Malware scanner host pools)]ページで、目的のスキャンホストプールを選択し、処理メニューの[ホストの管理 (Manage hosts)]をクリックします。

4 [マルウェアスキャナホストの管理 (Manage malware scanner hosts)]ページで、[新規追加 (Add new)]をクリックします。

5 [マルウェアスキャナホストの管理 (Add malware scanner host)]ページで、[ホスト名 (Host name)]を入力します。

6 [既存のクレデンシャルの選択 (Select existing credential)]または[新しいクレデンシャルの追加 (Add a new credential)]をクリックします。p.602 の「クレデンシャルの管理」を参照してください。

7 クレデンシャルを検証するメディアサーバーを選択します。

8 [クレデンシャルの検証 (Validate credentials)]をクリックします。検証が正常に完了したら、[保存 (Save)]をクリックしてクレデンシャルを保存します。

メモ: デフォルトでは、スキャンホストごとに 3 つの並列スキャンがサポートされており、この制限は構成可能です。スキャンプールにスキャンホストを増やすと、並列スキャンの数が増加します。

p.604 の「リソース制限の構成」を参照してください。

スキャンホストの管理

既存のスキャンホストの追加

この手順を使用して、同じ共有タイプの別のスキャンホストプールに同じスキャンホストを追加します。

既存のスキャンホストを構成するには

1 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。

2 [マルウェアの検出 (Malware detection)]ページで、右上隅の[マルウェアの検出設定 (Malware detection settings)]をクリックします。

3 [マルウェアスキャナホストプール (Malware scanner host pools)]ページで、目的のスキャンホストプールを選択し、処理メニューの[ホストの管理 (Manage hosts)]をクリックします。

4 [マルウェアスキャナホストの管理 (Manage malware scanner hosts)]ページで、[既存を追加 (Add existing)]をクリックして以前からあるホストを選択します。

メモ: リストには、すべてのスキャンホストプールのすべてのスキャンホストが含まれます。

---

5 [既存のマルウェアスキャナホストの追加 (Add existing malware scanner host)] ウィンドウで、目的のスキャンホストを 1 つ以上選択します。

6 [追加 (Add)]をクリックします。

スキャンホストの削除

1 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。

2 [マルウェアの検出 (Malware detection)]ページで、右上隅の[マルウェアの検出設定 (Malware detection settings)]をクリックします。

3 [マルウェアスキャナホストプール (Malware scanner host pools)]ページで、目的のスキャンホストプールを選択し、処理メニューの[ホストの管理 (Manage hosts)]をクリックします。

4 目的のホストを選択し、[削除 (Remove)]をクリックして、スキャンホストプールからスキャンホストを削除します。

スキャンホストの無効化

1 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。

2 [マルウェアの検出 (Malware detection)]ページで、右上隅の[マルウェアの検出設定 (Malware detection settings)]をクリックします。

3 [マルウェアスキャナホストプール (Malware scanner host pools)]ページで、目的のスキャンホストプールを選択し、処理メニューの[ホストの管理 (Manage hosts)]をクリックします。

4 目的のホストを選択し、[無効化 (Deactivate)]をクリックします。

クレデンシャルの管理

新しいクレデンシャルを追加

1 [クレデンシャルの管理 (Manage credentials)]ページで、[新しいクレデンシャルを追加 (Add new credentials)]を選択し、[次へ (Next)]をクリックします。

2 [クレデンシャルの管理 (Manage credentials)]ページで、クレデンシャル名、タグ、説明などの詳細情報を追加します。

3 [ホストクレデンシャル (Host credentials)]タブで、ホストのユーザー名、ホストパスワード、SSH ポート、RSA キー、共有タイプを追加します。

- 次のコマンドを実行して、MDSP メディアサーバーとホスト間の SSH 接続が動作していることを確認します。

```
ssh username@remote_host_name
```

- 次のコマンドを実行して、リモートスキャンホストの RSA キーが一覧表示されていることを確認します。

  ```
  ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa
  ```

- スキャンホストの RSA キーを取得するには、SSH 接続が確立された任意の Linux ホストから次のコマンドを使用して、ホストをスキャンします (これはスキャンホスト自体である可能性があります)。

  ```
  ssh-keyscan scan_host_name 2>/dev/null | grep ssh-rsa | awk
  '{print $3}' | base64 -d | sha256sum
  ```

  メモ: 次のホストキーアルゴリズムを使用して、所定の順序でスキャンするホストに接続します。

  rsa-sha2-512、rsa-sha2-256、ssh-rsa

  たとえば、出力は 33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef - のようになります。RSA キーは 33f697637ab3f0911c1d462d4bde8be3eec61a33403e8f6a88daecb415a31eef です。

  メモ: コピーする際は、- の文字を RSA キーから削除してください。

4. SMB 共有形式の場合は、次の詳細を追加で入力します。
   - Active Directory ドメイン: ストレージサーバーが接続されているドメイン (スキャンホストのマウントの認証に使用)。
   - Active Directory グループ: Active Directory ドメインのグループ名。
   - Active Directory ユーザー: 選択した Active Directory グループに追加されたユーザー。
   - パスワード
5. [保存 (Save)]をクリックします。

既存のクレデンシャルの追加

1. [クレデンシャルの管理 (Manage credentials)]ページで、[既存のクレデンシャルの選択 (Select existing credentials)]を選択し、[次へ (Next)]をクリックします。
2. [クレデンシャルの選択 (Select credentials)]タブで、目的のクレデンシャルを選択し、[保存 (Save)]をクリックします。

スキャンホストのクレデンシャルの検証

1. [マルウェアスキャナホストの追加 (Add malware scanner host)]ページでスキャンホストのクレデンシャルを指定したら、メディアサーバーを検索して選択し、[クレデンシャルの検証 (Validate credential)]ボタンを有効にします。

   メモ: 選択したメディアサーバーからスキャンホストに接続することで、SSH クレデンシャルのみが検証されます。メディアサーバーは、NetBackup バージョン 10.3 以降の Linux メディアサーバーである必要があります。

2. クレデンシャルの検証が正常に完了したら、[保存 (Save)]をクリックします。

リソース制限の構成

リソース制限を構成するには

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. 右上で[マルウェアの検出設定 (Malware detection settings)]、[リソース制限 (Resource limits)]の順に選択します。
3. [編集 (Edit)]をクリックして、リソース形式のリソース制限を編集します。
4. リソース形式にリソース制限が設定されていない場合に考慮されるグローバル制限を設定します。

   または、[追加 (Add)]をクリックしてグローバル設定を上書きします。
5. 新しいホスト名を入力し、制限を設定します。

   メモ: リソース形式のスキャンホスト: スキャンホストごとのスキャンの数。デフォルト: 3、最小: 1、最大: 10

   リソース形式のストレージサーバー: ストレージサーバーごとのスキャンの数。デフォルト: 20、最小: 1、最大: 50
6. [保存 (Save)]をクリックします。

   注意: インスタントアクセスの制限値を大きい値に設定すると、ストレージサーバーリソース(メモリ、CPU、ディスク)がマルウェアスキャンに使用されます。この値は、バックアップまたは複製操作によるストレージサーバーの既存の負荷に基づいて設定することをお勧めします。

メモ: NetBackup バージョン 10.2 以降では、MALWARE_DETECTION_JOBS_PER_SCAN_HOST 構成オプションで構成されたグローバルな並列スキャンの制限は適用されません。Web UI を使用してグローバルな並列スキャンの制限を構成します。

34

マルウェアスキャンの実行

この章では以下の項目について説明しています。

リカバリ前のマルウェアスキャンの実行

次の表に、[リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]オプションを有効または無効にした場合のシナリオを示します。

シナリオ	有効
ユーザーにマルウェアスキャンをトリガする RBAC 権限がない場合。	いいえ
プライマリコピーが、選択したいずれかのバックアップイメージのスナップショット (NAS-Data-Protection) の場合。 **メモ:** 選択した日付範囲で、ユーザーはリカバリ時間スキャンをトリガするために、プライマリコピーとしてバックアップイメージを選択する必要があります。 選択した日付範囲のイメージは、バックアップ形式である必要があります (バックアップとスナップショットの組み合わせはサポートされません)。	いいえ
スキャンホストプールが構成されていない場合。	いいえ

ファイルまたはフォルダのリカバリ前にマルウェアスキャンを実行するには

1. 左側の[リカバリ (Recovery)]をクリックします。
2. [標準リカバリ (Regular recovery)]で[リカバリの開始 (Start recovery)]をクリックします。
3. 次のプロパティを選択します。

ソースクライアント	バックアップを実行したクライアント。
宛先クライアント	バックアップをリストアするクライアント。
ポリシー形式	リストアするバックアップに関連付けられているポリシーの形式。
リストア形式	実行するリストア形式。利用可能なリストア形式は選択したポリシー形式によって異なります。

4. [次へ (Next)]をクリックします。
5. [日付の選択の使用 (Use date picker)]オプションで、[日付範囲 (Date range)]を編集します。

   または、[バックアップ履歴の使用 (Use backup history)]をクリックして、特定のイメージを表示して選択します。

   メモ: 選択した時間枠のすべてのバックアップイメージの詳細がテーブルに表示されます。マルウェアスキャンの結果、スケジュール形式、ポリシー名に基づいてイメージをフィルタ処理したり、ソートしたりできます。

   [適用 (Apply)]をクリックして日付の変更を適用するか、リカバリ用に選択したイメージを追加します。
6. リカバリ対象として選択したファイルまたはフォルダのマルウェアスキャンを実行するには、[リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]オプションを選択します。

   [リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]オプションが選択されている場合、ユーザーは最新のファイルまたはフォルダを一覧表示できます。

   メモ: [マルウェアに感染したイメージの選択を許可 (Allow the selection of images that are malware-affected)]オプションは、ユーザーが[リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]オプションを選択する場合は無効になります。

7 左側で[ソースクライアント (Source client)]ディレクトリを展開します。リストアするディレクトリを選択します。または、右ペインでファイルまたはディレクトリを選択します。[次へ (Next)]をクリックします。

8 リストア対象とリカバリオプションを選択します。

9 マルウェアに感染したファイルの[マルウェアスキャンおよびリカバリオプション (Malware scan and recover option)]から、次のいずれかのオプションを選択します。

- マルウェアに感染したファイルがある場合は、感染していない (クリーンな) ファイルのみをリカバリします (If any files are infected with malware, recover only uninfected files (clean))
- マルウェアに感染したファイルがある場合は、選択した日付範囲内でファイルの最新のクリーンコピーをリカバリします (If any files are infected with malware, recover the latest clean copy of the files within the selected date range)
- マルウェアに感染したファイルがある場合は、感染したファイルを含むすべてのファイルをリカバリします (If any files are infected with malware, recover all files, including infected files)
- マルウェアに感染したファイルがある場合は、リカバリジョブを実行しないでください (If any files are infected with malware, do not perform the recovery job)

マルウェアスキャナホストプールを選択し、[次へ (Next)]をクリックします。

10 基本プロパティ、リカバリの詳細、およびリカバリオプションを確認し、[リカバリの開始 (Start recovery)]をクリックします。

リカバリがトリガされると、アクティビティモニタージョブが作成され、ユーザーはこれをリカバリメニューで確認できます。

メモ: NAS-Data-Protection ポリシー形式の場合、マルチボリュームリストアで複数のリカバリジョブをトリガできます。ボリュームごとにジョブ ID のカンマ区切りリストが表示されます。リカバリジョブの列には 1 つのジョブ ID のみが表示されます。

マルウェアスキャンの実行

マルウェアスキャンを実行するには

1 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。

2 [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]をクリックします。

3 [検索条件 (Search by)]オプションで、次のいずれかを選択します。

- バックアップイメージ (Backup images)
- ポリシー形式別の資産 (Assets by policy type)
- 作業負荷の種類ごとの資産

メモ: NetBackup は、MSDP を使用したバックアップイメージのマルウェアスキャンに対してのみ、VMware 資産をサポートします。

スキャンのためのオプションについて詳しくは、次のオンデマンドスキャンを参照してください。

- p.611 の「バックアップイメージ」を参照してください。
- p.613 の「ポリシー形式別の資産」を参照してください。
- p.615 の「作業負荷の種類ごとの資産」を参照してください。

次の手順は、[ポリシー形式別の資産 (Assets by policy type)]と[作業負荷の種類ごとの資産 (Assets by workload type)]のスキャンに適用されます。

4 [クライアント (Client)]または[資産 (Asset)]テーブルで、スキャンするクライアントまたは資産を選択します。

5 [次へ (Next)]をクリックします。

メモ: ([検索 (Search by)]オプションで[ポリシー形式別の資産 (Assets by policy type)]が選択されている場合にのみ適用可能) 前の手順で選択したクライアントが複数のポリシー形式をサポートする場合、ユーザーはスキャンに単一のポリシー形式を選択できます。

6 [開始日付 / 時刻 (Start date/time)]と[終了日付 / 時刻 (End date/time)]で、日時の範囲を確認または更新します。

メモ: 選択基準に従って、スキャンが最大 100 イメージまで開始されます。

7 で、適切なホストプール名を選択します。Writer: Is "Select" a UI field?

8 (NAS-Data-Protection ポリシー形式にのみ適用可能) [ボリューム (Volume)]フィールドで、NAS デバイス用にバックアップするボリュームを選択します。

ボリュームレベルのフィルタ処理では、NAS-Data-Protection ボリュームバックアップの最上位ディレクトリのみをフェッチします。ボリュームレベルのフィルタ処理は、最上位ディレクトリがボリュームの場合にのみ適用されます。このような場合、ユーザーは[検索条件 (Search by)]オプションの[バックアップイメージ (Backup images)]オプションを使用して個々のバックアップイメージを選択できます。

9 [マルウェアスキャンの現在の状態 (Current status of malware scan)]から、次のいずれかを選択します。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- すべて (All)

10 [マルウェアのスキャン (Scan for malware)]をクリックします。

検索には 100 個以上のイメージがあります。100 個を超えるイメージはスキャンできません。日付範囲を調整して再試行してください。

11 スキャンが開始されると、[マルウェアのスキャン (Malware Scan)]の進捗が表示されます。状態フィールドは次のとおりです。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

メモ: 失敗の状態を示すツールのヒントにカーソルを合わせると、スキャンが失敗した理由が表示されます。

検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートされるのは、サポート対象のポリシー形式のインスタントアクセス機能を備えた、ストレージに格納されたバックアップイメージのみです。

- 保留中 (Pending)
- 処理中 (In progress)

バックアップイメージ

このセクションでは、クライアントバックアップイメージのポリシーでマルウェアをスキャンする手順について説明します。

ポリシークライアントバックアップイメージのマルウェアをスキャンするには

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]をクリックします。
3. [検索基準 (Search by)]オプションで、[バックアップイメージ (Backup images)]を選択します。
4. 検索条件で、以下を確認して編集します。
   - ポリシー名
     サポート対象のポリシー形式のみが一覧表示されます。
   - クライアント名
     サポート対象のポリシー形式のバックアップイメージを含むクライアントが表示されます。
   - ポリシー形式
   - バックアップ形式
     NetBackup アクセラレータ機能が有効になっていない増分バックアップイメージは、VMware 作業負荷ではサポートされません。
   - コピー
     選択したコピーがインスタントアクセスをサポートしない場合、バックアップイメージのマルウェアスキャンはスキップされます。
     (NAS-Data-Protection ポリシー形式の場合) [コピー (Copies)]で[コピー 2 (Copy 2)]を選択します。
   - ディスクプール
     MSDP (PureDisk)、OST (DataDomain)、AdvancedDisk ストレージ形式のディスクプールが一覧表示されます。
   - ディスク形式
     MSDP (PureDisk)、OST (DataDomain)、AdvancedDisk のディスク形式が一覧表示されます。
   - マルウェアスキャンの状態。
   - [バックアップの期間の選択 (Select the timeframe of backups)]で、日時の範囲を確認するか、更新します。

5 ［検索 (Search)］をクリックします。

検索条件を選択し、選択したスキャンホストがアクティブで利用可能であることを確認します。

6 ［スキャンするバックアップの選択 (Select the backups to scan)］テーブルで、スキャンする 1 つ以上のイメージを選択します。

7 ［マルウェアスキャナホストプールの選択 (Select a malware scanner host pool)］で、適切なホストプール名を選択します。

メモ: 選択したスキャンホストプールのスキャンホストは、NFS/SMB 共有形式で構成されているストレージサーバーで作成されたインスタントアクセスマウントにアクセスできる必要があります。

---

8 ［マルウェアのスキャン (Scan for malware)］をクリックします。

9 スキャンが開始されると、［マルウェアのスキャン (Malware Scan)］の進捗が表示されます。

状態フィールドは次のとおりです。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)
  状態にカーソルを重ねると、スキャンが失敗した理由が表示されます。

  メモ: 検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートされるのは、サポート対象のポリシー形式で、インスタントアクセス機能を備えた、ストレージに格納されたバックアップイメージのみです。

- 処理中 (In progress)
- 保留中 (Pending)

  メモ: 1 つ以上の処理中および保留中のジョブのマルウェアスキャンをキャンセルできます。

ポリシー形式別の資産

NetBackup は、マルウェアスキャンで MS-Windows、NAS-Data-Protection、および Standard のポリシー形式をサポートします。次のセクションでは、NAS-Data-Protection バックアップイメージでマルウェアをスキャンする手順について説明します。

NAS-Data-Protection

各 NAS ボリュームまたは共有は、設定された数のバックアップストリームを使用して NFS または SMB 経由で読み込まれ、バックアップされます。ボリュームあたりの最大ストリーム数によって、各ボリュームをバックアップするために作成されるバックアップストリームの数が決定されます。たとえば、10 個のボリュームを含み、ストリームの最大数が 4 であるポリシーがあるとします。このポリシーのバックアップでは、各ボリュームに対して 4 つのバックアップストリームが作成され、合計で 40 個の子バックアップストリームと 10 個の親バックアップストリームが作成されます。

メモ: スキャンの数は、スキャンを実行するために作成されたバッチの数によって異なります。マルウェア検出の UI には、親ストリームのバックアップイメージのみが表示されます。

マルチストリームバックアップについて詳しくは、『NetBackup NAS 管理者ガイド』を参照してください。

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。
2. [マルウェアの検出 (Malware detection)]ページで[マルウェアのスキャン (Scan for malware)]をクリックします。
3. [検索条件 (Search by)]オプションで、[ポリシー形式別の資産 (Assets by policy type)]を選択します。
4. [クライアント (Client)]または[資産 (Asset)]テーブルで、スキャンするクライアントまたは資産を選択します。
5. [次へ (Next)]をクリックします。

   前述の手順で選択したクライアントが複数のポリシー形式をサポートする場合、スキャンに単一のポリシー形式を選択できます。
6. [開始日付 / 時刻 (Start date/time)]と[終了日付 / 時刻 (End date/time)]で、日時の範囲を確認または更新します。

   スキャンは最大 100 個のイメージに対して開始されます。
7. で、適切なホストプール名を選択します。Writer: Is "Select" a GUI item in the UI?

8 [ボリューム (Volume)]フィールドで、NAS デバイス用にバックアップされたボリュームを選択します。

メモ: ボリュームレベルのフィルタ処理では、NAS-Data-Protection ボリュームバックアップの最上位ディレクトリのみをフェッチします。ボリュームレベルのフィルタ処理は、最上位ディレクトリがボリュームの場合にのみ適用されます。このような場合、ユーザーは[検索条件 (Search by)]オプションの[バックアップイメージ (Backup images)]オプションを使用して個々のバックアップイメージを選択できます。

---

9 [マルウェアスキャンの現在の状態 (Current status of malware scan)]から、次のいずれかを選択します。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- すべて (All)

10 [マルウェアのスキャン (Scan for malware)]をクリックします。

警告: 検索には 100 個以上のイメージがあります。100 個を超えるイメージはスキャンできません。日付範囲を調整して再試行してください。

---

11 スキャンが開始されると、[マルウェアのスキャン (Malware Scan)]の進捗が表示されます。状態フィールドは次のとおりです。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

  メモ: 状態にカーソルを重ねると、スキャンが失敗した理由が表示されます。

  検証で失敗したバックアップイメージは無視されます。マルウェアスキャンがサポートされるのは、サポート対象のポリシー形式で、インスタントアクセス機能を備えた、ストレージに格納されたバックアップイメージのみです。

- 保留中 (Pending)
- 処理中 (In progress)

マルウェアスキャンの状態に関する詳細情報を参照できます。

p.617 の「マルウェアスキャンの状態の表示」を参照してください。

メモ: NAS-Data-Protection で以前のバージョンの NetBackup 10.3 メディアサーバーで作成されたバックアップイメージの場合、[マルウェアのスキャン状態 (Malware scan status)]オプションに[すべて (All)]を選択していることを確認する必要があります。

作業負荷の種類ごとの資産

このセクションでは、VMware、ユニバーサル共有、およびクラウド VM の資産でマルウェアをスキャンする手順について説明します。

次の前提条件を満たしていることを確認します。

- バックアップが NetBackup 10.1 以降のストレージサーバーで実行された。
- バックアップイメージが、サポート対象のポリシー形式に限り、インスタントアクセス機能のみを備えた MSDP ストレージに格納されている。
- 前回のバックアップが正常に実行されている。
- マルウェアスキャンを実行する権限がある RBAC の役割を持っている。

サポート対象の資産でマルウェアをスキャンするには、次の手順を実行します。

1. 左側の[作業負荷 (Workloads)]で、サポートされている作業負荷を選択します。
2. バックアップが完了したリソース (VMware/Cloud VM、ユニバーサル共有など) を選択します。
3. [処理 (Actions)]、[マルウェアのスキャン (Scan for malware)]を選択します。
4. [マルウェアスキャン (Malware scan)]ページで、次の操作を行います。
   - [開始日時 (Start date/time)]と[終了日時 (End date/time)]を選択して、スキャンの日付範囲を選択します。
   - [スキャナホストプール (Scanner host pool)]を選択します
   - [マルウェアスキャンの現在の状態を選択 (Select current status of malware scan)]リストから、次のいずれかを選択します。
     - 未スキャン (Not scanned)
     - 感染なし (Not infected)
     - 感染 (Infected)
     - すべて (All)

5 ［マルウェアのスキャン (Scan for malware)］をクリックします。

メモ: マルウェアスキャナホストは、一度に 3 つのイメージのスキャンを開始できます。

6 スキャンが開始されると、［マルウェアの検出 (Malware Detection)］にマルウェアスキャンの進行状況が表示され、次のフィールドが表示されます。

- 未スキャン (Not scanned)
- 感染なし (Not infected)
- 感染 (Infected)
- 失敗 (Failed)

  メモ: 検証で失敗したバックアップイメージは無視されます。

- 処理中 (In progress)
- 保留中 (Pending)

35

スキャンタスクの管理

この章では以下の項目について説明しています。

マルウェアスキャンの状態の表示

マルウェアスキャンの状態を表示するには

◆ 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順にクリックします。

次の列が表示されます。

- クライアント (Client): マルウェアが検出された NetBackup クライアントの名前。
- バックアップ時間 (Backup time): バックアップが実行された時間。
- スキャンの状態 (Scan status): バックアップイメージのスキャン状態。状態には、感染、感染なし、失敗、処理中、保留中、キャンセル済み、キャンセルが進行中があります。
- 感染ファイル (Files infected): スキャン時に感染が確認されたファイルの数を示します。
- スキャンの進行状況 (Scan progress): スキャンが完了した割合を示します。
- 合計ファイル数 (Total files): バックアップイメージのカタログ (DNAS の場合はバックアップイメージのリスト) に記録されるファイルとフォルダの数を示します。リ

カバリ時スキャンの場合、[合計ファイル数 (Total files)]列には、リカバリ対象として選択されたファイル数のみが表示されます。

- 感染率 (% infected): 感染したファイルの割合を[合計ファイル数 (Total files)]と比較して表示します。

メモ: リカバリ中にスキップされたファイルは、[感染なし (Not-infected)]と見なされます。

- 経過時間 (Elapsed time): スキャン要求の受け付け (スキャンの日付) から、スキャンの完了 (スキャンの終了日) までの時間を表します。経過時間はアイドル時間、保留中の状態で費やされた時間で構成されます。エラーが発生したジョブの再開には、エラーの発生から再開操作がトリガされるまでの経過時間が含まれます。
- スキャン済みファイル (Scanned files): スキャンされるファイルの数を示します。
- スケジュール形式 (Schedule type): 関連付けられたバックアップジョブのバックアップ形式
- スキャン日 (Date of scan): スキャンが実行された日付。
- マルウェアスキャナ (Malware scanner): スキャンに使用されたマルウェアスキャナの名前。
- スキャナホストプール (Scanner host pool): マルウェアスキャンに使用されるホストプールを示します。
- マルウェアスキャナバージョン (Malware scanner version): スキャンに使用されたマルウェアスキャナのバージョン。

マルウェアスキャンイメージの処理

バックアップイメージをスキャンしてマルウェア検出を行うと、[マルウェアの検出 (Malware detection)]ホームページにテーブル形式のデータが表示されます。p.617 の「マルウェアスキャンの状態の表示」を参照してください。

バックアップイメージごとに、次の簡易な構成を利用できます。

すべてのコピーを期限切れにする

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します。
2. 目的のスキャン結果を表示するには、右側から[すべてのコピーを期限切れにする (Expire all copies)]を選択します。
3. 選択したバックアップイメージのすべてのコピーを期限切れにすることを確認します。

メモ: このオプションは、感染したスキャン結果にのみ利用できます。

感染ファイルを表示する

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します。
2. 目的のスキャン結果を表示するには、[感染ファイルを表示 (View infected files)]を選択します。

   メモ: このオプションは、感染したスキャン結果と「リカバリ」のスキャン形式にのみ利用できます。

3. [感染ファイル (Infected files)]テーブルで、必要に応じて目的のファイルを検索します。
4. 必要に応じて、[リストのエクスポート (Export list)]をクリックします。

   メモ: 選択したマルウェアスキャン結果の感染ファイルのリストは、`.csv` 形式でエクスポートされます。ファイル名の形式は、*`backupid`*`_infected_files_`*`timestamp`*`.csv` となります。

感染ファイルのリストをエクスポートする

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します。
2. 影響を受けたマルウェアに対して、右側から[感染ファイルのリストをエクスポート (Export Infected files list)]を選択します。

   メモ: `.csv` ファイルには、感染したファイルのバックアップ時刻と名前が含まれています。

マルウェアスキャンをキャンセルする

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します。
2. 目的のスキャン結果の[処理 (Actions)]メニューで、[マルウェアスキャンをキャンセル (Cancel malware scan)]をクリックします。

   メモ: マルウェアスキャンは進行中および保留中の状態からのみキャンセルできます。

3. [スキャンをキャンセル (Cancel scan)]をクリックして確定します。

   メモ: 状態は[キャンセルが進行中]に変わります。

メモ: [マルウェアスキャンをキャンセル (Cancel malware scan)]は、スキャン形式が「リカバリ」のスキャン結果ではサポートされません。

イメージの再スキャン

1. 左側で[検出とレポート (Detection and reporting)]、[マルウェアの検出 (Malware detection)]の順に選択します。
2. 目的のスキャン結果の[処理 (Actions)]メニューで、[イメージの再スキャン (Rescan image)]をクリックします。
3. [再スキャン (Rescan)]をクリックして確定します。
4. 一括再スキャンで、異なるまたは空のスキャナホストプールを持つ 1 つ以上のイメージを選択する場合、新しいスキャナホストプールを選択する必要があります。
   - [イメージの再スキャン (Rescan image)]をクリックします。
   - [マルウェアスキャナホストプールの選択 (Select a malware scanner host pool)]ポップアップから、新しいスキャンホストプールを選択します。

     メモ: 新しいスキャンホストプールは、この再スキャンで選択したすべてのイメージに使用できます。

   - [再スキャン (Rescan)]をクリックして確定します。

再スキャン (と再開) は、スキャン形式がリカバリのスキャン結果ではサポートされません。

5 エラーが発生したジョブまたはキャンセルされたジョブを再スキャンする場合、次の条件で、スキャンを最初からやり直すのではなく、エラーが発生した時点からスキャンがトリガ (再開) されます。

- [スキャン日 (Date of scan)]の値が 48 時間を超える場合、ジョブは再開されず、完全スキャンが開始されます。これは、スキャンに使用されるマルウェアシグネチャが大きく異ならないようにするためです。
- ファイル数が多い (>500k)、または DNAS の場合は複数のストリームが存在する Standard/MS-Windows バックアップイメージでサポートされます。
- 失敗したジョブに対してインスタントアクセスが成功している必要があります。
- 再開では、スキャンする最初の IA 対応コピーが識別されます。これは、最初のスキャン要求で選択されたコピーとは異なる場合があります。

再開されると、既存のスキャン結果の状態は失敗から保留に移行し、その後進行中の状態に移行します。また、エラーが発生した時点から進行状況の更新を続行できます。再スキャンが新たに実行される場合は、新しいスキャン結果が表示されます。ユーザーが完全なスキャンを実行する必要がある場合は、オンデマンドスキャンオプションを使用してトリガできます。

マルウェアに感染したイメージ (保護計画によって保護されているクライアント) からのリカバリ

マルウェアに感染したリカバリポイントからリストアするには、管理者の役割または同等の RBAC 権限が必要です。マルウェアに感染した特定のリカバリポイントをリカバリするには、次のトピックを参照してください。

p.622 の「マルウェアに感染したイメージ (ポリシーによって保護されているクライアント) からのリカバリ」を参照してください。

保護計画によって保護されているクライアントのマルウェアに感染したイメージからリカバリするには

1 左ペインで、サポート対象の作業負荷を選択します。

2 保護されているリソースを特定し、[処理 (Actions)]、[リカバリ (Recover)]の順に選択します。

3 [リカバリポイント (Recovery points)]タブでは、各リカバリポイントのマルウェアスキャンの状態が次のように表示されます。

- 未スキャン (Not scanned)
- 感染なし (Not infected)

- 感染 (Infected)

4 リカバリポイントを選択します。

5 [マルウェアに感染したリカバリポイントの選択を許可 (Allow the selection of recovery points that are malware-affected)]を選択します。このオプションは、マルウェアに感染したイメージを含むリカバリポイントがある場合にのみ表示されます。

メモ: マルウェアに感染したリカバリポイントからリストアするには、管理者の役割または同等の RBAC 権限が必要です。

---

6 [リカバリ (Recover)]をクリックし、リカバリの種類を選択します。次に、プロンプトに従います。

VM のリカバリについて詳しくは、『NetBackup Web UI VMware 管理者ガイド』を参照してください。

マルウェアに感染したイメージ (ポリシーによって保護されているクライアント) からのリカバリ

マルウェアに感染したイメージからリストアするには、管理者の役割または同等の RBAC 権限が必要です。マルウェアに感染した VMware 資産をリカバリするには、次のトピックを参照してください。

p.621 の「マルウェアに感染したイメージ (保護計画によって保護されているクライアント) からのリカバリ」を参照してください。

マルウェアに感染したイメージ (ポリシーによって保護されているクライアント) からリカバリするには

1 左側の[リカバリ (Recovery)]をクリックします。

2 [標準リカバリ (Regular recovery)]で[リカバリの開始 (Start recovery)]をクリックします。

3 次のプロパティを選択します。

ソースクライアント	バックアップを実行したクライアント。
宛先クライアント	バックアップをリストアするクライアント。
ポリシー形式	リストアするバックアップに関連付けられているポリシーの形式。
リストア形式	実行するリストア形式。利用可能なリストア形式は選択したポリシー形式によって異なります。

4 [次へ (Next)]をクリックします。

5 [開始日時 (Start date)]と[終了日時 (End date)]を選択します。

または、[バックアップ履歴 (Backup history)]をクリックして、特定のイメージを表示して選択します。[選択 (Select)]をクリックして、選択したイメージをリカバリに追加します。

メモ: 選択した時間枠のすべてのバックアップイメージの詳細がテーブルに表示されます。マルウェアスキャンの結果、スケジュール形式、ポリシー名に基づいてイメージをフィルタ処理したり、ソートしたりできます。

6 マルウェアに感染したイメージをリカバリに含める場合は、[マルウェアに感染したイメージの選択を許可 (Allow the selection of images that are malware-affected)]を選択します。

メモ: [マルウェアに感染したイメージの選択を許可 (Allow the selection of images that are malware-affected)]オプションは、ユーザーが[リカバリの前にマルウェアをスキャンする (Scan for malware before recovery)]オプションを選択する場合は無効になります。

7 左側で[ソースクライアント (Source client)]ディレクトリを展開します。リストアするディレクトリを選択します。または、右ペインでファイルまたはディレクトリを選択します。[次へ (Next)]をクリックします。

8 リカバリターゲットを選択します。

9 マルウェアに感染したファイルをリストアするには、[マルウェアに感染したファイルのリカバリを許可 (Allow recovery of files infected with malware)]をクリックします。クリックしない場合、NetBackup はスキャンされてマルウェアのないファイルのみをリストアします。

10 その他のリカバリオプションを選択します。続いて[次へ (Next)]をクリックします。

11 リカバリ設定を確認し、[リカバリの開始 (Start recovery)]をクリックします。

36

マルウェアスキャンの構成パラメータ

この章では以下の項目について説明しています。

MALWARE_SCAN_OPERATION_TIMEOUT

MALWARE_SCAN_OPERATION_TIMEOUT パラメータを使用すると、タイムアウトになる前に実行できるスキャン操作の期間を設定できます。

バックアップイメージのスキャン操作は、バックアップサイズやバックアップ内のファイル数などの要因によっては、時間がかかる場合があります。デフォルトでは、スキャン操作は 2 日後にタイムアウトします。タイムアウト値は、1 時間から 30 日までの範囲で設定できます。

表 36-1 MALWARE_SCAN_OPERATION_TIMEOUT オプションの情報

使用方法	説明
使用する場所	NetBackup メディアサーバー上で

使用方法	説明
使用方法	タイムアウト値を表示、追加、または変更するには、nbgetconfig または nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 ScanManager (nbcs) が開始される MSDP メディアサーバーで構成キーを設定します。複数の MSDP メディアサーバーの場合は、各サーバーに構成キーを設定します。 次の形式を使用します。 MALWARE_SCAN_OPERATION_TIMEOUT = 120 デフォルトでは、スキャン操作のタイムアウト値は 2,880 分 (2 日) です。サポートされる最小値は 60 分 (1 時間) で、最大値は 43,200 分 (30 日) です。
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。

MALWARE_DETECTION_CLEANUP_PERIOD

マルウェア検出では、30 日以上経過したスキャンジョブの自動クリーンアップがバッチ単位で実行され、次の状態で表示されます。

- クリーニング (Clean)
- 失敗 (Failed)
- キャンセル (Cancel)

クリーンアップは、NetBackup が起動してから 24 時間ごとに実行されます。

表 36-2　マルウェア検出クリーンアップオプション情報

使用方法	説明
使用する場所	ユーザーは、プライマリサーバーにある bp.conf ファイルの構成パラメータを変更できます。

使用方法	説明
使用方法	bp.conf ファイルで次のパラメータを設定します。 ■ クリーンアップ期間 (日数) を変更する方法: MALWARE_DETECTION_CLEANUP_PERIOD = 45 **メモ:** 値として指定できるのは日数のみです。0 より大きい整数値を指定できます。NetBackup では、6 カ月 (180 日) を超える値を設定しないことをお勧めしています。無効な値を設定した場合は、デフォルト値の 30 日が使用されます。 ■ クリーンアップ期間を無効にする方法: MALWARE_DETECTION_CLEANUP_PERIOD = 0 ■ スキャンジョブのバッチサイズを変更する方法: MALWARE_DETECTION_CLEANUP_BATCH_SIZE = 600 (バッチサイズ 600 を設定) **メモ:** バッチサイズには 1 から 5000 までの任意の値を設定できます。無効な値を設定した場合は、デフォルト値の 500 が使用されます。

NetBackup サーバーの MALWARE_DETECTION_TIMEOUT_PERIOD オプション

MALWARE_DETECTION_TIMEOUT_PERIOD パラメータを使用すると、タイムアウトになる前に実行できるスキャン操作の期間を構成できます。バックアップイメージのスキャン操作は、バックアップサイズやバックアップ内のファイル数などの要因によっては、時間がかかる場合があります。デフォルトでは、スキャン操作は 2 日後にタイムアウトします。タイムアウト値は時間単位で設定できます。

表 36-3 MALWARE_DETECTION_TIMEOUT_PERIOD オプションの情報

使用方法	説明
使用する場所	NetBackup プライマリサーバー上。
使用方法	タイムアウト値を表示、追加、または変更するには、nbgetconfig または nbsetconfig コマンドを使用します。 これらのコマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。 次の形式を使用します。 MALWARE_DETECTION_TIMEOUT_PERIOD = 72

使用方法	説明
同等の NetBackup Web UI プロパティ	ホストプロパティには、このエントリに相当するエントリは存在しません。