Veritas NetBackup™ 安全な通信のためのガイド (最初にお読みください)

VERITAS™

目次

NetBackup 安全な通信 (最初にお読みください)

この資料は、NetBackup 8.1 の安全な通信に関する重要な情報を記載しています。NetBackup 8.1 をインストールおよび配備する前にこの資料をお読みになることを強くお勧めします。

NetBackup のセキュリティ機能について詳しくは、『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。

https://www.veritas.com/content/support/en_US/doc-viewer.21733320-127424841-0.index.html

NetBackup での安全な通信について

NetBackup 8.1 のホスト同士はセキュアモードでのみ通信できます。

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 8.1 では、CA 証明書がトラストストアに追加された後に、各ホストが CA との信頼関係を確立する必要があります。さらに各 NetBackup 8.1 のホストには、正常に通信するためにホスト ID ベースの証明書も必要です。

ホスト ID ベースの証明書は、NetBackup インストール時にホスト上に配備されます。何らかの理由でインストール時に証明書をホスト上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上でホスト ID ベースの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。

NetBackup 管理コンソールの[ホスト管理]と[グローバルセキュリティ設定]ノードには、安全な通信が設定されています。

コマンド nbhostmgmt、nbhostidentity、nbcertcmd、および nbseccmd 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安全でない通信は可能です。

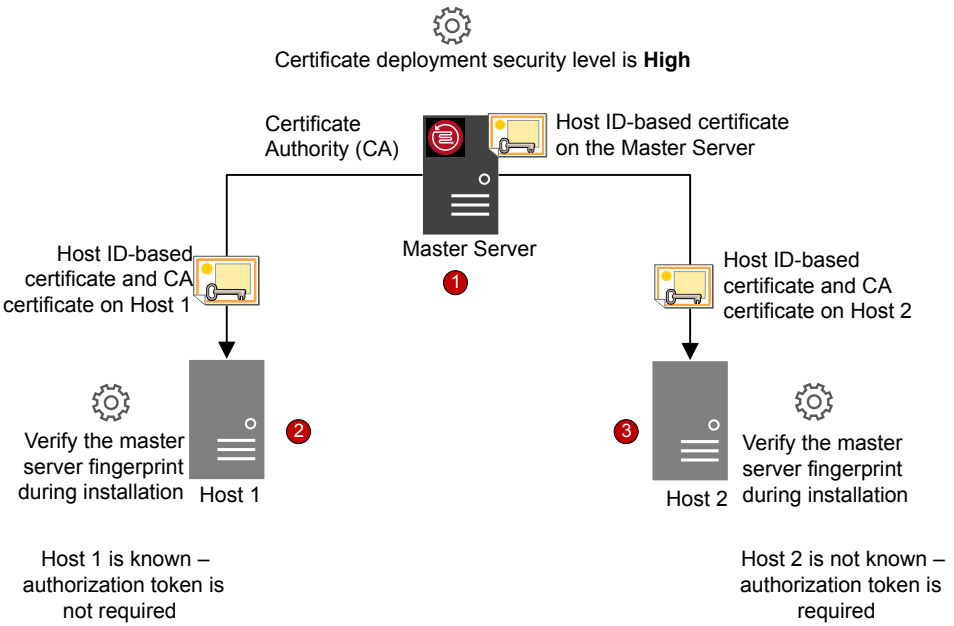
p.14 の「NetBackup 8.1 のホストが NetBackup 8.0 以前のホストと通信する方法」を参照してください。

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、ホスト名ベースの証明書が必要である。
- 拡張監査の操作で、ホストにホスト名ベースの証明書が必要である。
- NetBackup CloudStore サービスコンテナで、ホスト名ベースの証明書がメディアサーバーにインストールされている必要がある。

インストール時にホスト ID ベースの証明書を配備する方法

次の図では、インストール中に証明書をホストに配備する方法を示しています。



ホスト ID ベースの証明書の配備は、次の順序で行われます。

1. ホスト ID ベースの証明書は、インストール時に NetBackup マスターサーバーに自動的に配備されます。マスターサーバーは CA です。
2. ホスト ID ベースの証明書は、インストールウィザードまたはスクリプトにより使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。

   マスターサーバーの証明書配備セキュリティレベルが[高]に設定されており、ホスト 1 がマスターサーバーに認識されているため、認証トークンは必要はありません。

   メモ: 指紋を使用した認証は、マスターサーバーの CA をホストのトラストストアに追加する前に実行されます。マスター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、または Web サイトで公開します。

   メモ: 認証トークンは、NetBackup マスター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、マスターサーバーの管理者のみが作成できます。次にそれをマスターサーバーの管理者は、証明書を配備するホストの管理者渡します。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。

   マスター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. ホスト ID ベースの証明書は、マスター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。マスターサーバーの証明書配備セキュリティレベルが[高]に設定されており、ホスト 2 がマスター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。

アップグレード時に証明書をホストに配備する方法

NetBackup 8.1 をアップグレードする際に、NetBackup はアップグレード前にホスト ID ベースの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 にアップグレードした場合、ホスト ID ベースの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。

ソフトウェアのアップグレードのために LiveUpdate ユーティリティを使用している場合、証明書はアップグレード処理中には配備されません。証明書は手動で配備する必要があります。

マスターサーバーのクラスタノードでの安全な通信の方法

クラスタのマスター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: マスターサーバーのクラスタノード上で NetBackup アクセス制御 (NBAC) または拡張監査 (EA) 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 8.1 に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。[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推奨します。

証明書配備中に認証トークンが必要である場合

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定されます。マスター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。

次の設定を使用できます。デフォルト設定は[高]です。

- [中] - マスター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] - マスター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。ホストがマスターサーバーに認識されている場合、認証トークンは不要です。
- [最高] - マスター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要です。

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、必ずトークンが必要です。

証明書配備のセキュリティレベルについて詳しくは、『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。

https://www.veritas.com/content/support/en_US/doc-viewer21733320-127424841-0.v120724164-127424841.html

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、またはホストが短い名前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 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、または[承認待ちのマッピング]リストに表示されることがあります。マスターサーバーのホスト管理プロパティのこの構成を実行します。

ホスト ID とホスト名のマッピングついて詳しくは、『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。

https://www.veritas.com/content/support/en_US/doc-viewer21733320-127424841-0.v126691093-127424841.html

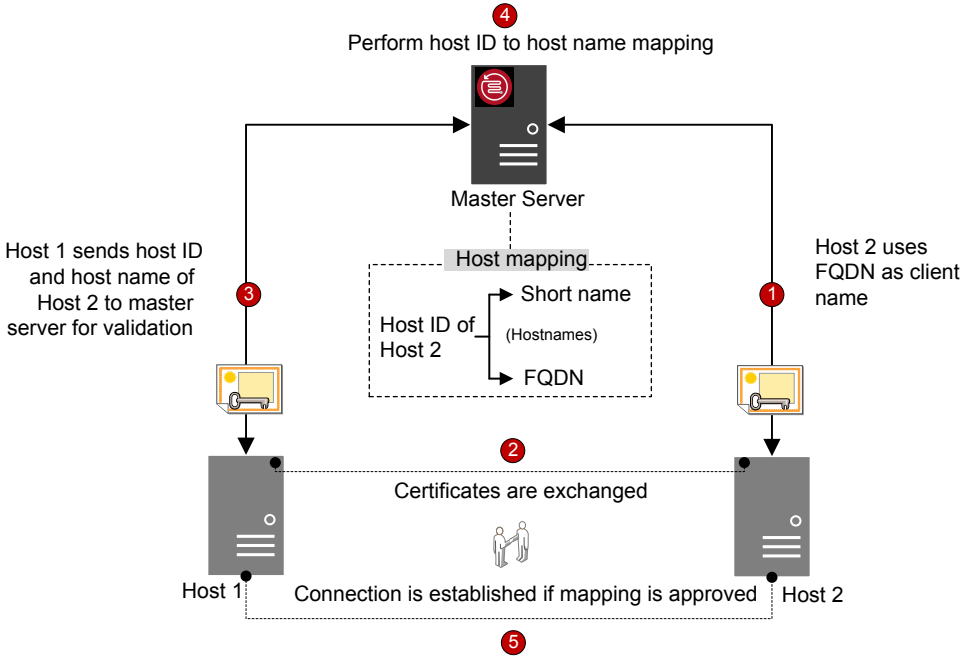
複数のホスト名がある構成の例は、次のとおりです。

- 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。
- ホストは短い名前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、マスターサーバーの分散アプリケーションリストアマッピングホストの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 エージェントは、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、リダイレクトされる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、短い名前を使用してホスト 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、ホスト ID ベースの証明書を交換します。
3. ホスト 1 は、ホスト ID とホスト 2 の短い名前をマスターサーバーに検証用に送信します。
4. マスターサーバーは、ホスト ID と短い名前をそのデータベース内から検索します。指定された短いホスト名がホスト 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 管理コンソールの[ホスト ID をホスト名に自動的にマップする]オプションが選択されており、短い名前が別のホスト ID にまだマップされていない場合、検出された短い名前はホスト 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]オプションが選択されておらず、短い名前が別のホスト 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

じ短い名前を使用してホスト 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しておく必要があります。

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。

ホストの属性またはホストの通信状態をリセットする方法

[ホストの属性をリセット]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ホスト ID ベースの証明書は削除されません。

ホストの属性をリセットすることは、次のようなシナリオの場合に便利です。

- 安全でない (またはバックレベルの) 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。

ホストの属性のリセットについて詳しくは、『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。

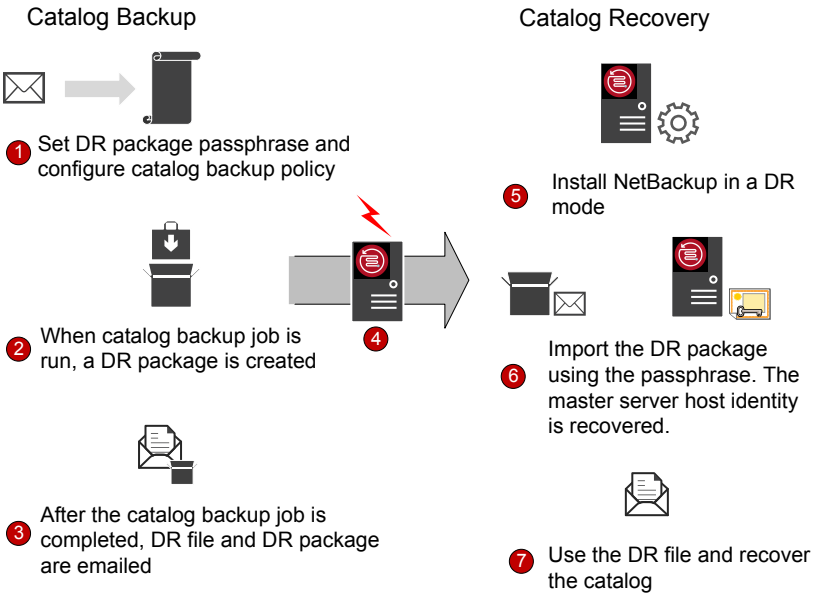
https://www.veritas.com/content/support/en_US/doc-viewer:21733320-127424841-0.v126691350-127424841.html

カタログリカバリの変更点

NetBackup 8.1 では、災害後に NetBackup をリストアするときに、マスター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、マスターサーバーは新しい 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、マスターサーバーのホスト 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 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] > [ディザスタリカバリ]タブを使用します。

   パスフレーズをいつ変更するとしても、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 をマスター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場合、マスターサーバーのホスト 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。

   https://www.veritas.com/support/ja_JP/article.000125933
7. ホスト ID のリストア後に生じた可能性がある証明書関連アクティビティに固有の情報喪失を避けるために、ホスト ID をリカバリした後にはすぐにカタログリカバリを実行する必要があります。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 アプライアンスのホスト 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

セキュア通信で 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マスターサーバーからの信頼を確立する必要があります。

ソースマスターサーバーおよびターゲットマスターサーバーの両方を 8.1 にアップグレードしてから、両方のマスターサーバー上で信頼関係を更新する必要があります。

メモ: 8.1 の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 管理コンソールまたは `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マスター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。

https://www.veritas.com/content/support/en_US/doc-viewer25074086-127355784-0.v81800250-127355784.html

失効した証明書を使用するホストの動作

ホスト ID ベースの証明書は、さまざまな理由でマスターサーバー管理者により取り消される場合があります。失効した証明書に関する情報が含まれる証明書失効リスト (CRL) はマスター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、マスター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。失効し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します。

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

https://www.veritas.com/content/support/en_US/doc-viewer21733320-127424841-0.v126192948-127424841.html

ホストがマスター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 クライアントがマスターサーバーに要求 (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、それらをマスター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。

マスター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ホスト ID ベースの証明書を配備するには、認証トークンが必要です。

DMZ 内のクライアントについて詳しくは、『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。

https://www.veritas.com/content/support/en_US/doc-viewer21733320-127424841-0.v125482382-127424841.html

セキュリティ証明書のバックアップについて

セキュリティの理由から、セキュリティ証明書はバックアップ時にはバックアップされません。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。必要な場合にはそれらを、NetBackup をアンインストールする前に手動でバックアップできます。

ホスト ID ベースの証明書の保持ついて詳しくは、『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。

https://www.veritas.com/content/support/en_US/doc-viewer21733320-127424841-0.v122201443-127424841.html

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]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]オプションは、NetBackup 管理コンソールの[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]タブで使用できます。

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 のホストは他の 8.1 ホストとセキュアモードでのみ通信できます。8.1 ホストが 8.0 以前のホストと通信する場合、または 8.1 マスターサーバーが OpsCenter 8.1 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]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]>[グローバルセキュリティ設定]>[安全な通信]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 サービスをマスターサーバーで再起動して安全でない通信はすべて終了し、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 8.1 ホストはまずホスト検証のためにマスターサーバーに接続します。マスターサーバーは、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。

通信エラーのシナリオ

NetBackup 8.1 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。

- マスターサーバーホストの NetBackup 管理コンソールで、[セキュリティ管理]>[グローバルセキュリティ]>[ホスト]>[NetBackup 8.0 以前のホストとの安全でない通信を有効にする]オプションの順に選択します。
- マスターサーバーホストで、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 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] > [ディザスタリカバリ]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

NetBackup 8.1 が OpsCenter と BMR (Bare Metal Restore) ホストとの通信をサポートする方法を調べるには、このセクションを使用します。

NetBackup 8.1 マスターサーバーと OpsCenter 8.1 サーバーとの間の通信

NetBackup 8.1 マスターサーバーから OpsCenter 8.1 サーバーを使用してデータを収集する前に、次のオプションを必ず設定します。

- OpsCenter サーバー名は、NetBackup 構成ファイル (UNIX 上では bp.conf、Windows ではレジストリキー) 内の OPS_CENTER_SERVER_NAME 構成オプションに対して追加する必要があります。
- 安全でない通信は、NetBackup では有効になっています。次のいずれかを確認します。
  - マスターサーバーホストの NetBackup 管理コンソールで、[セキュリティ管理]>[グローバルセキュリティ]>[ホスト]>[NetBackup 8.0 以前のホストとの安全でない通信を有効にする]オプションが選択されている。
  - マスターサーバーホストで、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

安全な通信を使用する場合、NetBackup Bare Metal Restore (BMR) 機能は NetBackup バージョン 8.1 ホストのリストア用にサポートされません。ただし、BMR は NetBackup 8.0 以前のホストのリストアに使用できます。8.0 以前のホストのリストアでは、8.0 以前のバージョンを含む共有リソースツリー (SRT) を使用することをお勧めします。