Veritas NetBackup™ 53xx Appliance 初期構成ガイド

リリース 4.1

VERITAS™

Veritas NetBackup™ 53xx Appliance 初期構成ガイド

最終更新日: 2021-07-19

法的通知と登録商標

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

この製品には、サードパーティの所有物であることをベリタスが示す必要のあるサードパーティソフトウェア (「サードパーティプログラム」) が含まれている場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このベリタス製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

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

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

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、この文書の供給、履行、または使用に関連して付随的または間接的に起こる損害に対して責任を負いません。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、ベリタスがオンプレミスサービスまたはホストサービスとして提供するかを問わず、必要に応じて FAR 52.227-19「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートは世界中にサポートセンターを設けています。すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供

されます。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の Web サイトにアクセスしてください。

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

次の URL でベリタスアカウントの情報を管理できます。

https://my.veritas.com

既存のサポート契約に関する質問については、次に示す地域のサポート契約管理チームに電子メールでお問い合わせてください。

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、ベリタスの Web サイトで入手できます。

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

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。

APPL.docs@veritas.com

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

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

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

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

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

目次

1

初期構成の準備

この章では以下の項目について説明しています。

アプライアンスの構成ガイドライン

新しいアプライアンスを配備するときは次の構成ガイドラインを使います。

表 1-1　　アプライアンスの構成ガイドライン

パラメータ	説明
NetBackup Appliance Web コンソールへのアクセス	NetBackup Appliance Web コンソールは、デフォルトポート 443 で HTTPS を介してのみアクセスできます。HTTP 経由のポート 80 は無効になっています。
初期構成時の接続	アプライアンスの初期構成を実行するときは、接続が切断しないように対策を採る必要があります。初期構成時に接続が切断されると、初期構成に失敗します。 次のイベントを避けるように、アプライアンスの構成に使うコンピュータを設定してください。 ■ コンピュータがスリープになる状態 ■ コンピュータがシャットダウンしたり、電源が喪失する状態 ■ コンピュータのネットワーク接続が切断される状態

パラメータ	説明
必須の名前とアドレス	構成する前に、次の情報を収集します。 ■ アプライアンスのネットワーク IP アドレス、ネットマスク、ゲートウェイ IP アドレス ■ すべてのアプライアンスのネットワーク名 ■ DNS またはホストの情報 DNS を使用する場合は、すべてのアプライアンスとプライマリサーバーのネットワーク名が DNS で解決可能であることを確認してください (FQHN、省略名)。 DNS を使用しない場合は、初期構成のときにアプライアンスに適切なホストエントリを入力していることを確かめてください。 **メモ:** ドメイン名のサフィックスはホスト名に付加され、初期構成が完了した後は変更できません。後でサフィックスを変更したり、アプライアンスを別のドメインに移動したりする必要がある場合は、最初に出荷時の設定へのリセットを実行してから、初期構成を再度実行する必要があります。 ■ NetBackup ストレージユニットの名前 アプライアンスの役割を構成するとき、ストレージ名フィールドが表示されます。デフォルト名を変更することも残すこともできます。 ストレージユニットとディスクプールのデフォルト値が以下のように NetBackup 管理コンソールに表示されます。 ■ AdvancedDisk の場合: デフォルトのストレージユニット名: stu_adv_<hostname> デフォルトのディスクプール名: dp_adv_<hostname> ■ NetBackup Deduplication の場合: デフォルトのストレージユニット名: stu_disk_<hostname> デフォルトのディスクプール名: dp_disk_<hostname> **メモ:** アプライアンスの短いホスト名は、デフォルトのストレージユニット名とディスクプール名として表示されます。
デフォルトのユーザー名とパスワード	新しい NetBackup Appliance には、次のデフォルトのログインクレデンシャルが付属しています。 ■ ユーザー名: admin ■ パスワード: P@ssw0rd ソフトウェアバージョン 4.0 以降、初期構成プロセスでは、次のユーザーアカウントのデフォルトのパスワードを変更する必要があります。 ■ admin ■ maintenance ■ sysadmin (IPMI) NetBackup Appliance Web コンソール 以降、初期構成の最初のページには、デフォルトのパスワードの変更を求めるメッセージが表示されます。NetBackup Appliance シェルメニュー 以降、役割の構成コマンドである `Main_Menu > Appliance Primary` または `Main_Menu > Appliance Media` コマンドを実行する際は、デフォルトのパスワードの変更を求めるメッセージが表示されます。

パラメータ	説明
ファイアウォールポートの使用	次のポートがプライマリサーバーとメディアサーバー間のファイアウォールで開いていることを確かめてください。 ■ 13724 (`vnetd`) ■ 13720 (`bprd`) ■ 1556 (`PBX`) NetBackup と NetBackup Appliance のファイアウォールポートについて詳しくは、ベリタスのサポート Web サイトにある次のテクニカルノートを参照してください。 https://www.veritas.com/support/en_US/article.TECH178855

パラメータ	説明
メディアサーバーの役割	NetBackup Appliance をメディアサーバーとして構成する前に、このアプライアンスで使用するプライマリサーバーを新しいアプライアンスのメディアサーバー名に更新する必要があります。プライマリサーバーが NetBackup Appliance でも従来の NetBackup プライマリサーバーでも、新しいアプライアンスメディアサーバーの名前はプライマリサーバーの[追加サーバー (Additional Servers)]リストに追加する必要があります。 新しいアプライアンスを構成する前にプライマリサーバーに新しいアプライアンスメディアサーバー名を追加すると、新しいアプライアンスで初期構成を実行するときに次のメリットがあります。 ■ メディアサーバーが NetBackup ドメインの一部になり、適切なネットワーク通信が可能になる。 ■ メディアサーバーがストレージサーバーとディスクプールエントリを作成できるようになる。 セキュリティ証明書の要件 リリース 3.2 以降では、外部認証局の証明書がサポートされています。この機能は、ホストの検証とセキュリティのために NetBackup 認証局を使用する代替手段を提供します。このアプライアンスをメディアサーバーとして構成するには、アプライアンスでセキュリティ証明書を配備して、プライマリサーバーを信頼する必要があります。 プライマリサーバーが外部 CA が発行した証明書のみを使用して稼働している場合、このアプライアンスメディアサーバーには、同じ外部 CA から発行された証明書を持つ構成が必要です。CA 証明書のプロビジョニングの場合、メディアサーバー役割の構成を続行するには、ホスト証明書、信頼済み証明書、プライベートキー、証明書ファイル、証明書失効リスト (CRL) の使用がすべて必要です。 プライマリサーバーが、外部 CA が発行した証明書と NetBackup CA が署名した証明書の両方を使用する場合は、同じ外部 CA が発行した証明書または NetBackup CA が署名した証明書を使用してこのメディアサーバーアプライアンスを構成するように選択できます。プライマリサーバーが、NetBackup CA が署名した証明書のみを使用している場合は、CA 証明書およびホスト ID ベースの証明書を、このアプライアンスで使用するプライマリサーバーから配備する必要があります。プライマリサーバーを信頼することを選択した場合、CA 証明書は自動的にダウンロードされ、配備されます。 ホスト ID ベースの証明書を配備するには ■ プライマリサーバーのセキュリティレベルが[最高 (Very High)]である場合、認証トークンを手動で入力して、ホスト ID ベースの証明書をメディアサーバーに配備する必要があります。 ■ プライマリサーバーのセキュリティレベルが[高 (High)]または[中 (Medium)]である場合、認証トークンは必要ありません。ホスト ID ベースの証明書はメディアサーバーに自動的に配備されます。 **メモ:** プライマリセキュリティレベルに関係なく、アプライアンスに対し出荷時の設定へのリセットまたは再イメージングが実行されると、アプライアンスの再構成時に再発行トークンが必要です。 セキュリティ証明書がアプライアンスメディアサーバーに配備されている場合、役割の構成中にそれらを再度配備するように要求されることはありません。 セキュリティ証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「NetBackup のセキュリティ証明書」の章を参照してください。 p.30 の「プライマリサーバーの構成によるアプライアンスのメディアサーバーとの通信」を参照してください。

パラメータ	説明
高可用性	

パラメータ	説明
	アプライアンスのリリースバージョン 3.1 以降では、高可用性 (HA) ソリューション用に 53xx シリーズのアプライアンスを配備できます。HA 構成では、計算ノードとパートナーノードとして指定されている 2 台の NetBackup 53xx アプライアンスを使用します。これらのノードは相互に接続し、さらに同じプライマリストレージシェルフの特定のチャネルに接続します。 **メモ:** Copilot 機能は、HA 設定を構成すると利用できなくなります。 **メモ:** NetBackup 5350 Appliance は、HA 設定での使用はサポートされていません。 NetBackup Appliance の HA 構成では、次のようにモデル番号、ハードウェア構成、アプライアンスソフトウェアバージョンが同一である 2 台のアプライアンスを使用する必要があります。 ■ モデル番号とハードウェア構成 両方のアプライアンスのモデル番号と I/O 構成が一致する必要があります。たとえば、構成 D の 5330 モデルのアプライアンスを 2 台使用するか、構成 D の 5340 モデルのアプライアンスを 2 台使用します。構成 D の 5330 モデルのアプライアンスを 1 台と構成 D の 5340 モデルのアプライアンスを 1 台使用することはできません。 ■ アプライアンスソフトウェアのバージョン 両方のアプライアンスで、同じソフトウェアバージョンを使用する必要があります。使用するアプライアンスのプライマリサーバーは、HA アプライアンスと同じソフトウェアバージョンを使用する必要があります。従来の (非アプライアンス) プライマリサーバーを使用する場合、アプライアンスソフトウェアバージョンに関連付けられている NetBackup ソフトウェアバージョンを使用する必要があります。たとえば、HA アプライアンスがバージョン 3.1 を使用している場合、従来の NetBackup プライマリサーバーは NetBackup バージョン 8.1 を使用する必要があります。 HA 構成は次のように設定できます。 ■ 新しいシステムのインストール 1 台の NetBackup 53xx アプライアンス (計算ノード) で初期構成を実行してから、同じノードで HA 構成を実行します。次に、もう一方のアプライアンス (パートナーノード) で初期構成を実行します。最後に、構成済みのパートナーノードを追加して、計算ノードの HA 構成を完了します。 ■ 既存のシステム 既存のコンポーネントは、次の手順で最初にアップグレードする必要があります。 プライマリサーバーの場合は、従来の NetBackup (非アプライアンス) プライマリサーバーを NetBackup リリースバージョン 8.1 以降にアップグレードする必要があります。NetBackup Appliance プライマリサーバーをアプライアンスリリースバージョン 3.1 以降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 (既存の 53xx モデル) の場合は、このアプライアンスをリリースバージョン 3.1 以降にアップグレードする必要があります。 これらのアップグレードが完了したら、既存の 53xx 計算ノードで HA 構成を設定します。次に、パートナーノードで初期構成を実行します。最後に、パートナーノードを追加して、計算ノードの HA 構成を完了します。 ■ ホスト名と IP アドレスの必要条件 HA 設定では、次の 3 つのホスト名とそれに対応する IP アドレスが必要です。 ■ 物理ノード

パラメータ	説明
	2 台の物理メディアサーバーノードにそれぞれ専用のホスト名と IP アドレスを割り当てる必要があります。各ホスト名は、同じサブネット内の対応する IP アドレスに解決する必要があります。 ■ 仮想ホスト名と IP アドレス このホスト名とそれに対応する IP アドレスは、2 台の物理ノードとこれらのノードに接続された共通ストレージから成る HA を識別する際に使用されます。仮想ホスト名と IP アドレスは、2 ノード間の HA 設定内のポインタとして動作します。たとえば、1 台のノードが正常に動作していないか、アップグレードまたはメンテナンスのために停止している場合、仮想ホスト名はまだ動作しているノードを自動的にポイントします。 HA 設定を行う前に、NetBackup 管理コンソールで、[ホスト名マッピング (Host Name Mappings)]プロパティにすべての HA ホスト名と IP アドレスを追加する必要があります。この操作は、関連付けられているプライマリサーバーで実行する必要があります。物理ノードの初期構成の前にマッピングプロパティを更新しないと、HA 設定のプロセスが失敗する可能性があります。アプライアンスのリリース 3.1.2 以降では、ホスト名マッピングでも承認が必要です。 ホスト名マッピングの追加と承認について詳しくは、『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。 HA の構成時に、最初に構成したメディアサーバーまたは既存のメディアサーバーのホスト名と IP アドレスが、HA 構成用の仮想ホスト名と IP アドレスとして自動的に昇格されます。このとき、このメディアサーバーに新しいホスト名と IP アドレスを指定する必要があります。 **メモ:** Active Directory (AD) 認証を使用する場合は、HA 構成のホスト名と IP アドレスで AD サーバーを更新するまで、HA 構成を設定しないでください。HA 構成を設定する前に、AD サーバーで、仮想ホスト名と仮想 IP アドレス、各ノードのホスト名と IP アドレスを指定する必要があります。指定しないと、AD ユーザーがシステムにアクセスする際に問題が発生する可能性があります。 NetBackup クライアントを使用して NetBackup ジョブを管理する場合、クライアントの `bp.conf` ファイルに 3 つのホスト名 (2 つのノードのホスト名と新しいホスト名) を追加します。
ディスクストレージオプションのライセンス	アプライアンスには一定期間後に期限切れになる非売品版 (NFR) ライセンスキーが付属しています。アプライアンスはこのライセンスキーがまもなく期限切れになるという警告メッセージを提供しません。したがって、アプライアンスを取り付けて構成した後はこのキーを恒久キーに変更することをお勧めします。ライセンスキーを表示し変更する方法の情報と手順については、『NetBackup Appliance 管理者ガイド』を参照してください。 NFR キーは、期限切れになる前に恒久キーと置き換えてください。

パラメータ	説明
最適化された共有の予約のストレージ	Copilot 機能を使用する予定がある場合は、初期構成時に最適化された共有の予約を作成することをお勧めします。最適化された共有の予約は、初期構成の完了後にも作成できます。たとえば、拡張ストレージシェルフを既存または稼働している 53xx アプライアンスに追加する場合です。 **メモ:** Copilot 機能は、HA 設定を構成すると利用できなくなります。 最適化された共有の予約は、次の場合のみに作成できます。 ■ 構成は NetBackup Appliance シェルメニューで行う必要があります。 ■ アプライアンスハードウェア構成は、拡張ストレージシェルフを少なくとも 1 つ含む必要があります。 ■ 拡張ストレージシェルフ上のすべてのストレージ領域は、最適化された共有の予約専用に使用される必要があります。予約の最小サイズは 114 TB です。 ■ AdvancedDisk と MSDP パーティションは、異なるシェルフに存在する必要があります。これらは、専用シェルフ上で最適化された共有の予約と共存することはできません。

NetBackup appliance MSDP クラウドアプリケーションの構成の概要

リリース 3.3.0.1 以降、MSDP クラウドアプリケーション用に NetBackup 52xx および 53xx シリーズのアプライアンスを構成できます (高可用性 (HA) の設定を含む)。

MSDP クラウドは、重複排除技術を備えたクラウドソリューションです。データは、重複排除を使用してクラウドターゲットに直接格納されます。1 台の MSDP ストレージサーバーは、ローカルストレージと複数のクラウドストレージターゲットの両方をサポートできます。アプライアンスの MSDP ストレージサーバーを構成した後、初期構成の間に、そのストレージサーバーにクラウドストレージターゲットを追加できます。その後、アプライアンスの MSDP ストレージサーバーはクラウドターゲットにデータを格納できます。

次に、MSDP クラウドアプリケーション用にアプライアンスを構成するために必要な手順の概略を示します。

- 手順 1: NetBackup Appliance Web コンソール (Web コンソール) または NetBackup Appliance シェルメニュー (シェルメニュー) を使用して、アプライアンスの初期構成を実行します。
  初期構成に Web コンソールを使用している場合は、初期構成の完了後にシェルメニューにログインし、nbasecadmin ユーザーのデフォルトのパスワードを変更する必要があります。これは手順 2 に進む前に実行してください。
  詳しくは、『NetBackup 52xx Appliance 初期構成ガイド』または『NetBackup 53xx Appliance 初期構成ガイド』を参照してください。
- 手順 2: nbasecadmin ユーザーとして NetBackup Web UI にログインし、次のように MSDP クラウドストレージを構成します。
  - ディスクプールを作成します。
  - ストレージユニットを作成します。
    詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

メモ: アプライアンスの初期構成が完了した後は、いつでも MSDP クラウドストレージを構成できます。

構成されていないアプライアンスに対するコマンドの制限

アプライアンスを管理するには、事前に構成しておく必要があります。初期構成に使うコマンドは、新しいアプライアンスまたは出荷時の設定にリセットされたアプライアンスに対してのみ実行できるコマンドです。これらのコマンドを初期構成以外に使うと、予期しない動作または望ましくない動作につながることがあります。この状況を防止するために、Veritasはアプライアンスの初期構成が完了するまで管理コマンドを使わないことをお勧めします。

構成されていないアプライアンスに対して有効なコマンドについて詳しくは、次のマニュアルを参照してください。

NetBackup Appliance 初期構成ガイド

NetBackup Appliance コマンドリファレンスガイド

IPv4-IPv6 ベースのネットワークサポートについて

NetBackup appliance はデュアルスタック IPv4-IPv6 ネットワークでサポートされ、バックアップとリストアの目的で IPv6 クライアントと通信できます。IPv6 アドレスを Appliance に割り当て、DNS を構成し、IPv6 ベースシステムを含めるようにルーティングを構成できます。

NetBackup Appliance Web コンソールまたは NetBackup Appliance シェルメニューを使って IPv4 と IPv6 のアドレス情報を入力できます。

IPv6 アドレスに関する次の注意事項を確認してください。

- 使用できるのはグローバルアドレスのみです。リンクローカルスコープまたはノードローカルスコープのアドレスは使用できません。グローバルスコープアドレスと一意のローカルアドレスは両方ともホストによってグローバルアドレスとして扱われます。
  グローバルスコープ IP アドレスは、グローバルにルーティング可能なアドレスを意味します。一意のローカルアドレスはグローバルアドレスとして扱われます。
- 同じコマンドで、IPv4 と IPv6 の両方のアドレスを使うことはできません。たとえば、`Configure 9ffe::9 255.255.255.0 1.1.1.1` は使用できません。`Configure 9ffe::46 64 9ffe::49 eth1` を使用する必要があります。
- IPv6 アドレスへの IPv4アドレスの埋め込みはサポートされていません。たとえば、9ffe::10.23.1.5 のようなアドレスを使うことはできません。
- アプライアンスのメディアサーバーの IPv6 アドレスとホスト名が利用可能な場合は、プライマリサーバーにアプライアンスのメディアサーバーを追加できます。

たとえば、プライマリサーバーにアプライアンスのメディアサーバーを追加するには、アプライアンスのメディアサーバーの IPv6 アドレスを次のように入力します。

例:

```
Main > Network > Hosts add 9ffe::45 v45 v45
```

```
Main > Settings > NetBackup AdditionalServers Add v45
```

Appliance のメディアサーバーの IPv4 アドレスを提供する必要はありません。

- 純粋な IPv6 クライアントは、NetBackup の場合と同様の方法でサポートされます。
- NIC (Network Interface Card) または結合に対して IPv4 アドレスを 1 つのみ入力できます。ただし、NIC または結合に対して複数の IPv6 アドレスを入力できます。
- `Main_Menu > Network > Hosts` コマンドは、1 つの NIC (Network Interface Card) を持つ同じホスト名への複数の IPv6 アドレスの割り当てをサポートします。ただし、このコマンドでは、1 つの NIC を持つ特定のホスト名に 1 つの IPv4 アドレスのみを割り当てることができます。
- ゲートウェイアドレスを指定せずにネットワークインターフェースの IPv6 アドレスを追加できます。
  詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

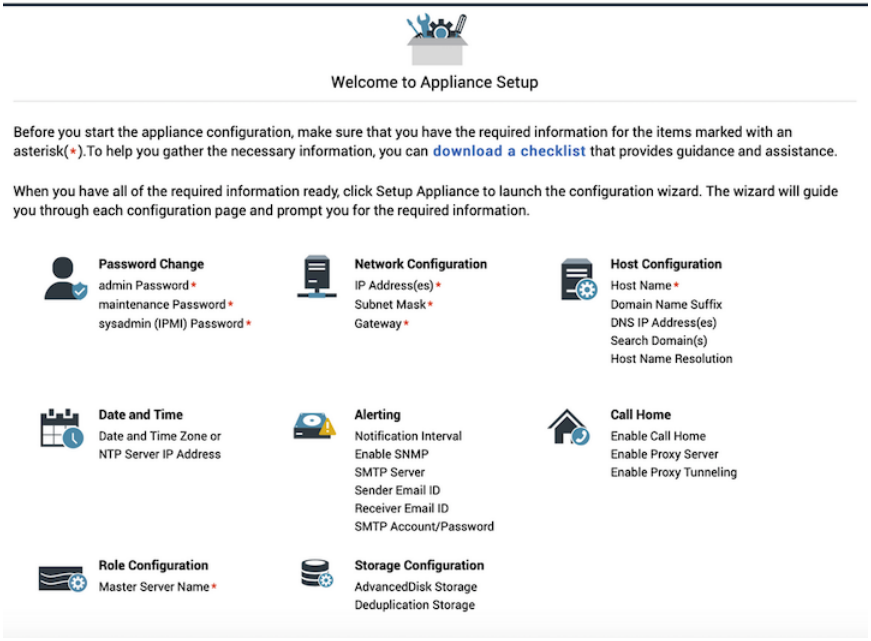
NetBackup Appliance Web コンソールの初期構成ページの概要

NetBackup Appliance Web コンソールで適切な情報を一連のページに入力して初期構成を実行できます。以下に、各ページと必要な情報の簡単な説明を示します。

アプライアンスの設定へようこそ (Welcome to Appliance Setup)

このページは、未構成のアプライアンスにログオンすると表示されます。初期構成に必要な情報の概略を示します。

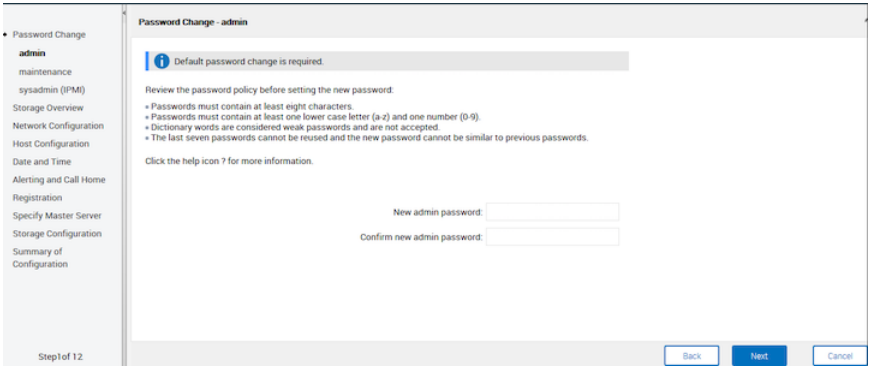
図 1-1 アプライアンスの設定へようこそ (Welcome to Appliance Setup)



パスワードの変更 (Password Change)

このページは、admin、maintenance、sysadmin (IPMI) のユーザーアカウントについて、出荷時のデフォルトのパスワードを変更するために使用します。デフォルトのパスワードをすべて変更するまで、このページから初期構成を続行することはできません。

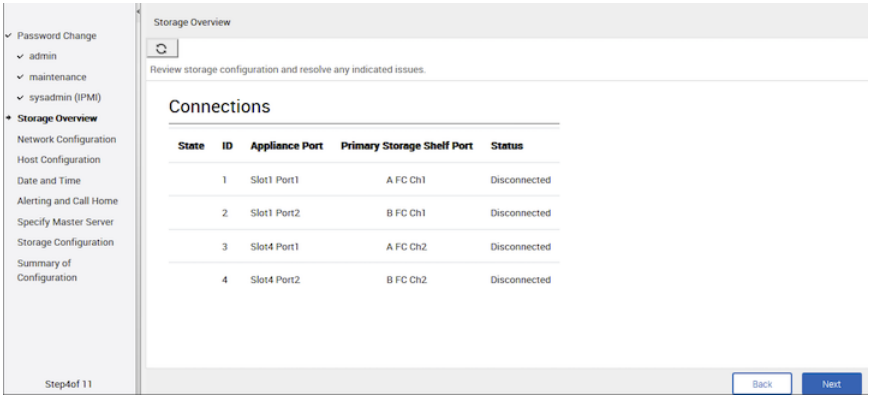
図 1-2 [パスワードの変更 (Password Change)]ページ



ストレージの概要 (Storage Overview)

このページには、システムハードウェアコンポーネントすべての現在の状態が表示されます。このページでは、アプライアンスサーバーとプライマリストレージシェルフ、または拡張ストレージシェルフ間のコンポーネントのケーブル接続の問題を特定します。ディスクドライブに問題がある場合は、この問題も特定します。

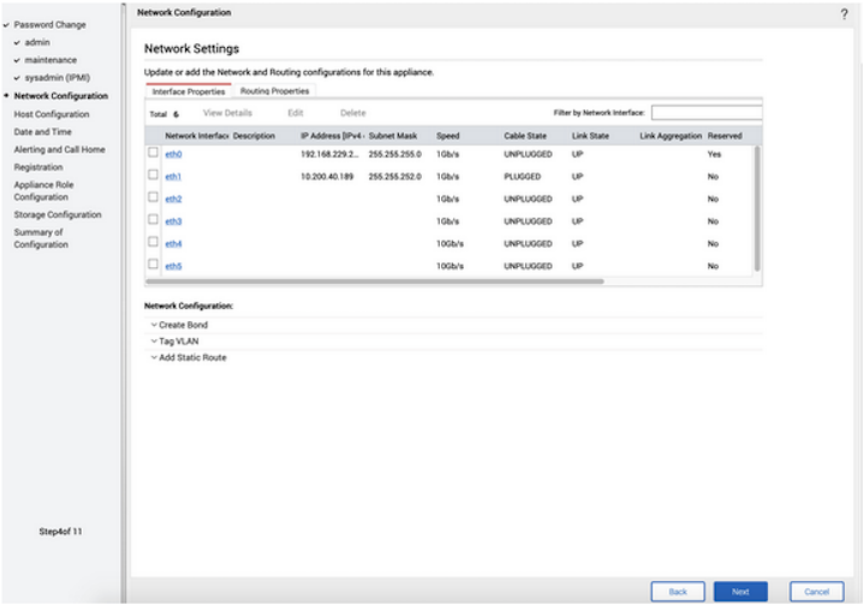
図 1-3 53xx Appliance の[ストレージの概要 (Storage Overview)]ページ



ネットワーク設定(Network Configuration)

このページでは、企業のネットワーク情報を入力します。上部のテーブルには、インターフェースとルーティングのプロパティを入力する[インターフェースプロパティ (Interface Properties)]タブと[ルーティングプロパティ (Routing Properties)]タブがあります。下部の領域には、[ボンドの作成 (Create Bond)]、[VLAN のタグ付け (Tag VLAN)]、[静的ルートの追加 (Add Static Route)]のドロップダウンタブがあります。各タブを展開してそれぞれの情報を入力します。

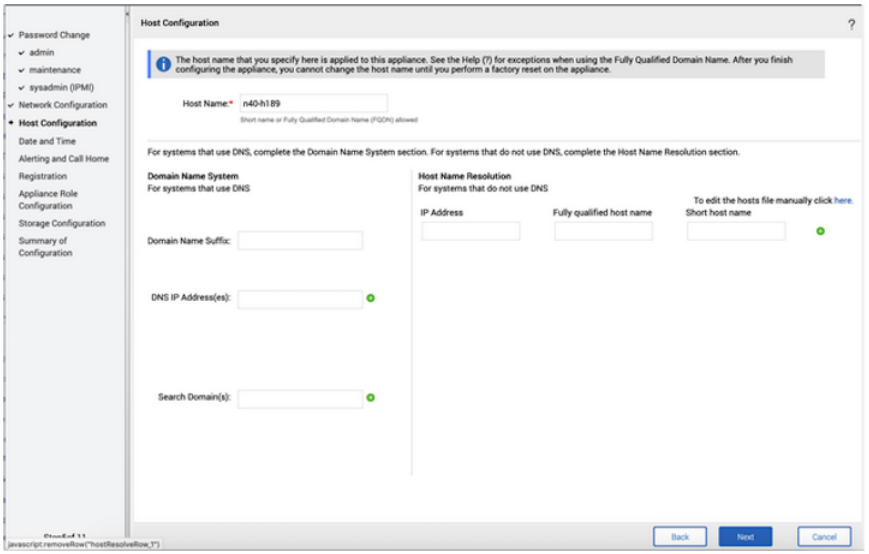
図 1-4 ［ネットワーク構成 (Network Configuration)］ページ



ホストの構成 (Host Configuration)

このページでは、アプライアンスのホスト ID を入力します。アプライアンスのホスト名 (FQDN と省略名)、IP アドレス、ドメイン名のすべてが必須です。

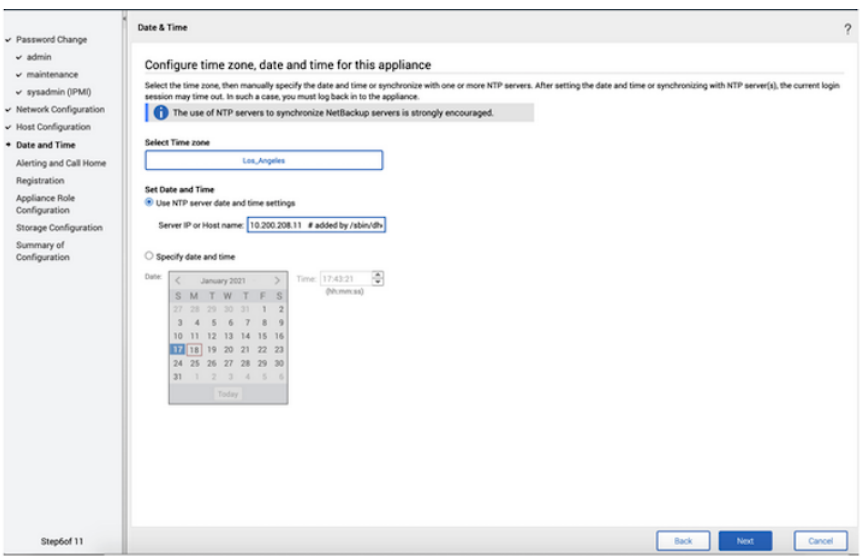
図 1-5 ［ホストの構成 (Host Configuration)］ページ



日付と時刻 (Date & Time)

このページでは、アプライアンスの設置場所の日付、時刻、およびタイムゾーンを設定します。

図 1-6 ［日付と時刻 (Date & Time)］ページ



警告とコールホーム (Alerting and Call Home)

問題を報告するために、このページでシステム警告やコールホーム機能を構成します。

図 1-7 ［警告とコールホーム (Alerting and Call Home)］ページ

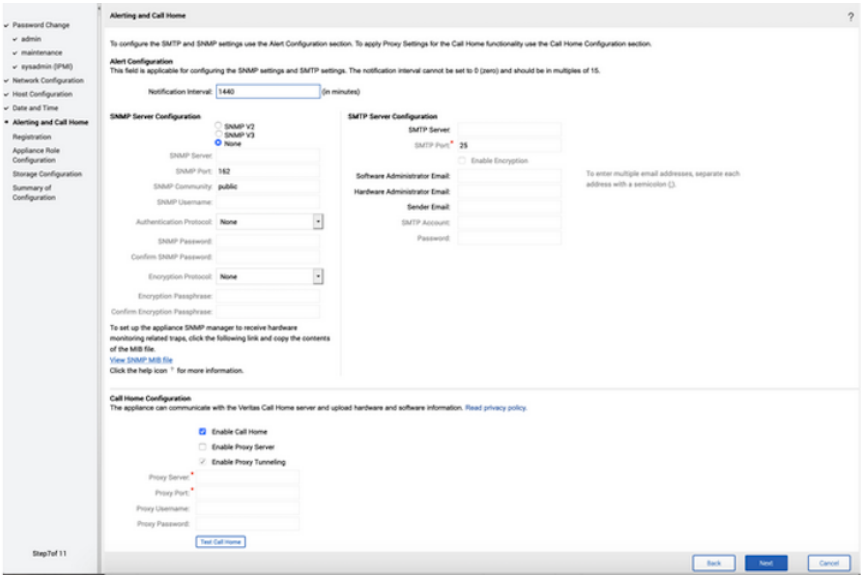
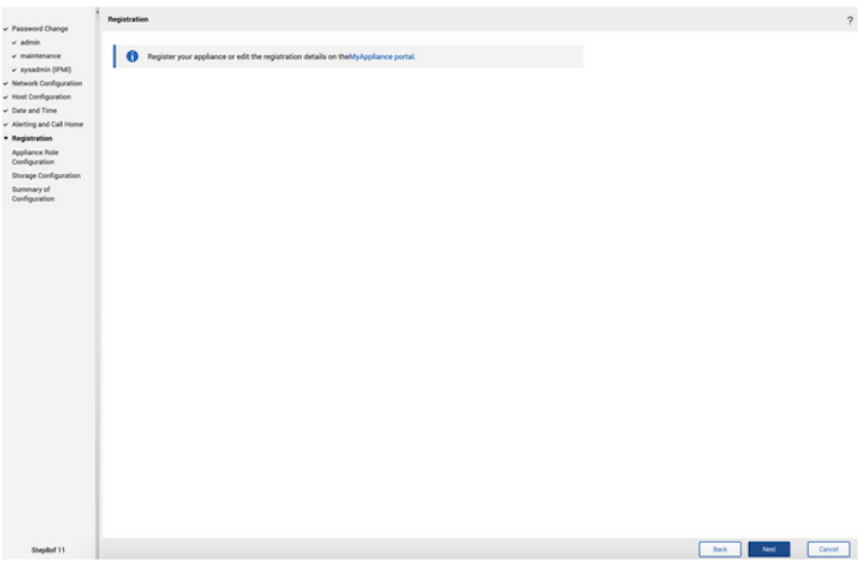


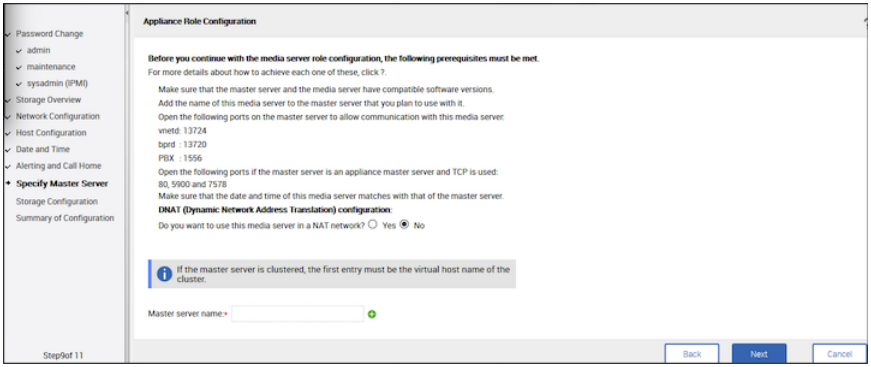
図 1-8 ［登録 (Registration)］ページ



プライマリサーバーの指定 (Specify Primary Server)

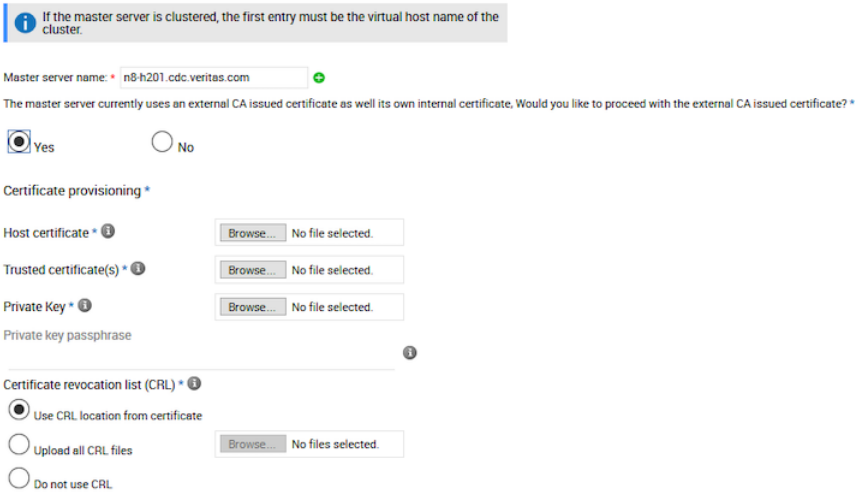
このページでは、メディアサーバーと組み合わせて使用するプライマリサーバーを指定します。プライマリサーバーを選択する前に、最初にアプライアンスメディアサーバーの名前をプライマリサーバーのサーバーリストに追加する必要があります。

図 1-9 [プライマリサーバーの指定 (Specify Primary Server)]ページ

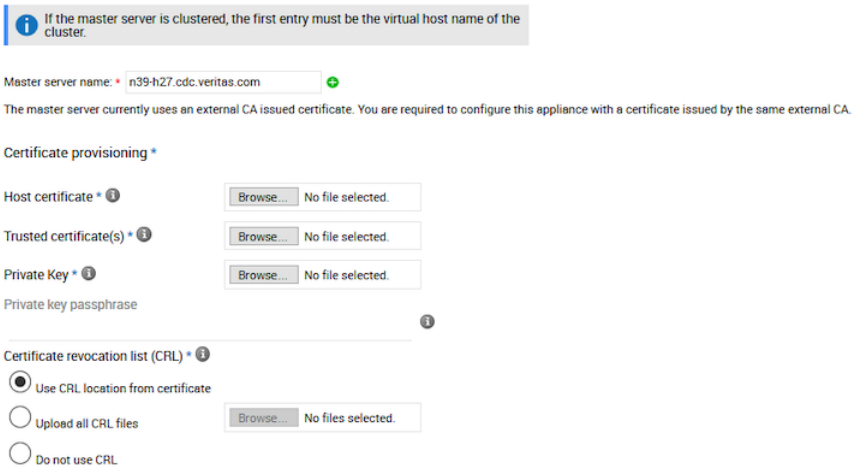


このメディアサーバーで使用するために選択したプライマリサーバー名を入力すると、次のいずれかの証明書シナリオが表示され、このアプライアンスに適切な証明書を展開できます。

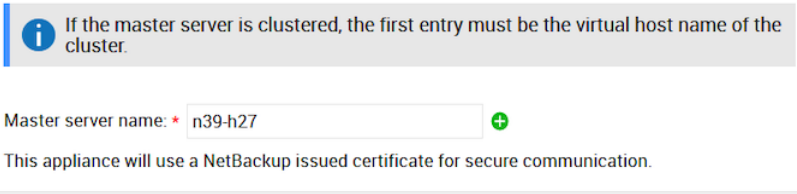
外部 CA と NetBackup 認証局を使用するプライマリサーバー:



外部 CA のみを使用するプライマリサーバー:



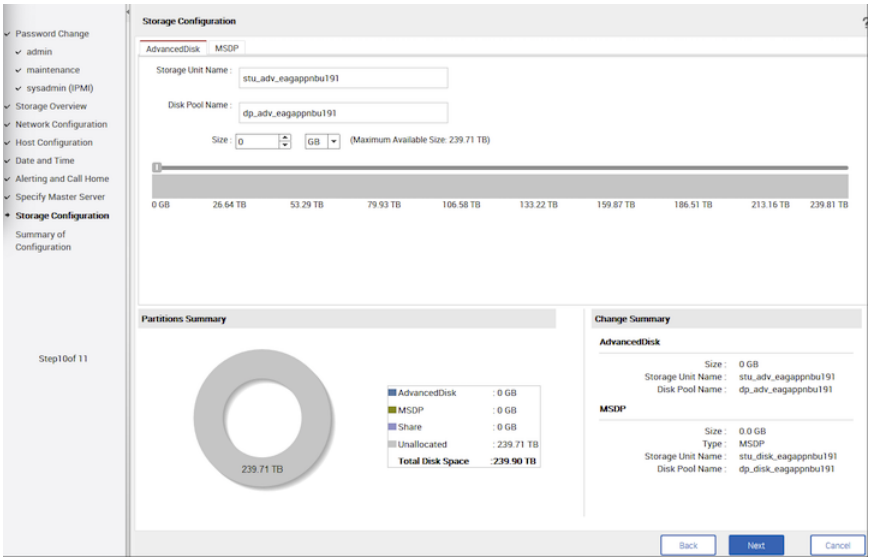
NetBackup CA のみを使用するプライマリサーバー:



[ストレージの構成 (Storage Configuration)] - [AdvancedDisk]

このページの[AdvancedDisk]タブでは、AdvancedDisk パーティションにストレージ領域を割り当て、ストレージユニットおよびディスクプールに名前を付けます。

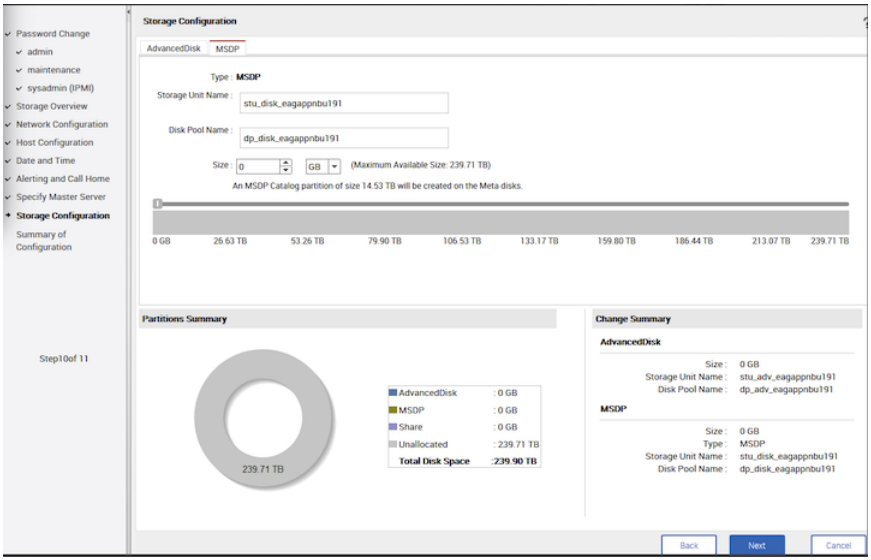
図 1-10 ［ストレージの構成 (Storage Configuration)］ページ - ［AdvancedDisk］



［ストレージの構成 (Storage Configuration)］- ［MSDP］

このページの［MSDP］タブでは、メディアサーバー重複排除プールパーティションにストレージ領域を割り当て、ストレージユニットおよびディスクプールに名前を付けます。

図 1-11 ［ストレージの構成 (Storage Configuration)］ページ - ［MSDP］



NetBackup Appliance の初期構成チェックリストについて

このガイドに記載の初期構成チェックリストは、アプライアンスの初期構成および将来の再構成の計画に役立ちます。

このチェックリストは、NetBackup Appliance Web コンソールに表示される各初期構成ページのデータ入力フィールドを記述する一連の表から成っています。

新しいアプライアンスの場合、アプライアンスを構成する前にこのチェックリストを使って初期構成の設定を記録します。アプライアンスが出荷時設定にリセットまたは再イメージ処理されている場合は、アプライアンスをもう一度構成する必要があります。チェックリストに記録された設定は、時間を節約し、アプライアンスの接続をすばやく元に戻すために役立ちます。

NetBackup Appliance の初期構成チェックリスト

このチェックリストはアプライアンスの初期構成の計画のために役立ちます。

『NetBackup Appliance の初期構成ガイド』の初期構成の手順と併せて、このチェックリストを使ってください。文書には、このチェックリストの複製も含まれます。

新しいアプライアンスで、アプライアンスの初期構成の設定を記録するために次の表を使います。アプライアンスが出荷時設定にリセットまたは再イメージ処理されている場合は、

アプライアンスをもう一度構成する必要があります。チェックリストに記録された設定は、貴重な時間を節約し、アプライアンスの接続をすばやく元に戻すために役立ちます。

このチェックリストのハードコピーまたは印刷されたバージョンを使う場合は、記入済みのチェックリストを安全な場所に置くようにします。

IPMI ポートの構成

IPMI ポートの構成は初期構成とは異なります。アプライアンスへのリモートアクセスにこのポートを使用するには、まずポートをネットワークへの接続用に構成する必要があります。次の表を使って、必要なパラメータ設定を記録します。

表 1-2 IPMI ポートの構成

パラメータ	設定
IP アドレス (IP Address)	
ネットマスク (Netmask)	
ゲートウェイ IP アドレス	

アプライアンスの初期構成

次の表は、NetBackup Appliance Web コンソールの初期構成ページに表示されるフィールドを示します。これらの表を使って、設定を記録します。

表 1-3 パスワードの変更

ユーザーアカウント	設定
admin	
maintenance	
sysadmin (IPMI)	

表 1-4 ネットワーク構成 - ボンドの作成

フィールド	設定
ネットワークインターフェース (Network Interface)	
結合モード (Bond Mode)	
IP アドレス (IP Address)	
サブネットマスク (Subnet Mask)	

表 1-5 ネットワーク構成 - VLAN のタグ付け

フィールド	設定
インターフェースの選択	
説明 (上記のインターフェースの選択フィールドについて)	
VLAN Id	
IP アドレス (IPv4 または IPv6)	
サブネットマスク (Subnet Mask)	

表 1-6 ネットワーク構成 - 静的ルートの追加

フィールド	設定
宛先 IP (Destination IP)	
宛先のサブネットマスク (Destination Subnet Mask)	
ゲートウェイ	
ネットワークインターフェース (Network Interface)	

表 1-7 ホストの構成 (Host Configuration)

フィールド	設定
ホスト名 (Host Name)	
ドメインネームシステム (DNS) ■ ドメイン名のサフィックス (Domain Name Suffix) ■ DNS の IP アドレス (DNS IP Address) ■ 検索ドメイン (Search Domain(s))	DNS: ■ _____ ■ _____ ■ _____
ホスト名解決 (Host Name Resolution) (DNS なし) ■ IP アドレス (IP address) ■ 完全修飾ホスト名 (Fully qualified host name) ■ 短いホスト名 (Short host name)	DNS なし: ■ _____ ■ _____ ■ _____

表 1-8 パスワードの変更 (Password change)

フィールド	設定
古い admin パスワード (Old admin password)	
新しい admin パスワード (New admin password)	
新しい admin パスワードの確認 (Confirm new admin password)	

表 1-9 日付と時刻の構成

フィールド	設定
タイムゾーン (Time zone)	
NTP サーバーの IP (NTP Server IP)	
日時 (Date and Time)	

表 1-10 警告の構成 (Alert configuration)

フィールド	設定
通知の間隔 (Notification Interval) (15 分間隔)	
SNMP サーバーの構成 (SNMP Server Configuration) - SNMP V2、SNMP V3、なし (デフォルト)	
SNMP サーバー (SNMP Server) (名前)	
SNMP ポート (SNMP Port)	
SNMP コミュニティ (SNMP Community) (SNMP V2 では必須、SNMP V3 ではオプション)	
SNMP ユーザー名 (SNMP Username) (SNMP V3 のみ)	
認証プロトコル (Authentication Protocol) (SNMP V3 のみ) - なし (デフォルト)、SHA256、SHA512	
SNMP パスワード (SNMP Password) (SNMP V3 のみ)	

フィールド	設定
暗号化プロトコル (Encryption Protocol) (SNMP V3 のみ) - なし (デフォルト)、AES128、AES192、AES256、AES512	
暗号化パスフレーズ (Encryption Passphrase) (SNMP V3 のみ)	
SMTP サーバー (SMTP Server)	
SMTP ポート (SMTP Port)	
ソフトウェア管理者の電子メール (Software Administrator Email)	
ハードウェア管理者の電子メール (Hardware Administrator Email)	
送信者の電子メール (Sender Email)	
SMTP アカウント (SMTP Account)	
パスワード (Password)	

表 1-11　　警告の構成

フィールド	設定
通知の間隔 (Notification Interval) (15 分間隔)	
SNMP の警告を有効にする (Enable SNMP Alert)	
SNMP サーバー (SNMP server) ([SNMP の警告を有効にする (Enable SNMP Alert)]にチェックマークを付けた場合のみ必要)	
SNMP ポート (SNMP port)	
SNMP コミュニティ (SNMP community)	
SMTP サーバー (SMTP server)	
ソフトウェア管理者の電子メール (Software administrator email address)	
ハードウェア管理者の電子メール (Hardware administrator email address)	

フィールド	設定
送信者の電子メールアドレス (Sender email address)	
SMTP アカウント (SMTP account)	
パスワード (Password)	

表 1-12 コールホームの構成

フィールド	設定
コールホームを有効にする (Enable Call Home)	
プロキシサーバーを有効化 (Enable proxy server)	
プロキシのトンネリングを有効にする (Enable proxy tunneling)	
プロキシサーバー (Proxy server) ([プロキシサーバーを有効化 (Enable proxy server)]にチェックマークを付けた場合のみ必要)	
プロキシポート (Proxy port) ([プロキシサーバーを有効化 (Enable proxy server)]にチェックマークを付けた場合のみ必要)	
プロキシのユーザー名 (Proxy user name)	
プロキシのパスワード (Proxy password)	

表 1-13 AdvancedDisk ストレージの構成

フィールド	設定
ストレージユニット名 (Storage Unit name)	
ディスクプール名	
サイズ	

表 1-14 重複排除 (MSDP) ディスクの構成

フィールド	設定
ストレージユニット名 (Storage Unit name)	
ディスクプール名	

フィールド	設定
サイズ	

最大伝送単位サイズの設定について

MTU プロパティは、イーサネットフレームの最大伝送単位のサイズを制御します。イーサネットの標準的な最大伝送単位サイズは 1500 バイトです (ヘッダーなしの場合)。サポート対象の環境では、MTU プロパティを 9,000 バイトを超えて設定できます。インターフェースにさらに大きなフレームサイズを設定することを、一般的に、ジャンボフレームを使うと言います。ジャンボフレームにより、データがネットワーク経由で送信され、場合によってはスループットが向上して CPU 使用率が減ることがあるため、断片化を減らすことができます。ジャンボフレームを活用するには、イーサネットカード、ドライバ、スイッチのすべてにおいて、ジャンボフレームをサポートする必要があります。さらに、アプライアンスへのデータ転送に使われる各サーバーインターフェースを、ジャンボフレーム用に設定する必要があります。

インターフェースの MTU プロパティを 1500 バイトより大きな値に設定した場合、特定のインターフェースのアプライアンスに接続しているすべてのシステムで、最大伝送単位サイズを同一にすることが推奨されます。こうしたシステムには、NetBackup クライアントやリモートデスクトップが含まれますが、これらに限定されません。また、MTU プロパティを設定する前に、ネットワークハードウェア、OS、ドライバのサポートをすべてのシステムで確認してください。

インターフェースの MTU プロパティは、NetBackup Appliance シェルメニューで `SetProperty` コマンドを使って設定できます。

『NetBackup Appliance コマンドリファレンスガイド』の `SetProperty` コマンドを参照してください。

2

初期構成の手順

この章では以下の項目について説明しています。

プライマリサーバーの構成によるアプライアンスのメディアサーバーとの通信

新しいアプライアンスをメディアサーバーとして構成するには、まず併用する予定のプライマリサーバーの構成を更新する必要があります。プライマリサーバーと新しいメディアサーバー間の通信を確保するには、新しいメディアサーバーホスト名をプライマリサーバー上の[追加サーバーリスト (Additional Servers List)]に追加する必要があります。

高可用性構成の場合、設定手順に使用するノードのホスト名を追加する必要があります。

次に、プライマリサーバーを構成して新しいアプライアンスのメディアサーバーと通信する手順を示します。

プライマリサーバーを構成して新しいメディアサーバーと通信する方法

1 アプライアンスをメディアサーバーの役割として構成する前に、ソフトウェアバージョンにプライマリサーバーとの互換性があることを確認します。プライマリサーバーは、

次のようにメディアサーバーと同じかそれ以降のソフトウェアバージョンを使用する必要があります。

- プライマリサーバーがソフトウェアバージョン 4.1 の NetBackup Appliance である場合、アプライアンスメディアサーバーはソフトウェアバージョン 4.1 以前を使用する必要があります。
- プライマリサーバーがソフトウェアバージョン 9.1 の従来の (非アプライアンス) NetBackup プライマリサーバーである場合、アプライアンスメディアサーバーはソフトウェアバージョン 4.1 以前を使用する必要があります。

2 プライマリサーバーに管理者としてログインし、次のようにメディアサーバー名を追加します。

アプライアンスプライマリサーバーの場合:	NetBackup Appliance Web コンソールで次の操作を実行します。 ■ ［管理 (Manage)］>［追加サーバー (Additional Servers)］>［追加 (Add)］をクリックします。 ■ ［アプライアンスのホスト名 (Appliance Hostname)］フィールドに、追加するアプライアンスのメディアサーバーの完全修飾ホスト名 (FQHN) を入力します。 ■ ［追加 (Add)］をクリックします。 アプライアンスに複数のホスト名がある場合はすべての名前を追加します。 NetBackup Appliance シェルメニューで次の操作を実行します。 ■ Main_Menu > Settings ビューで、次のコマンドを実行します。 `Settings > NetBackup AdditionalServers Add` *`media-server`* *media-server* は、まだ構成していないアプライアンスのメディアサーバーの完全修飾ホスト名 (FQHN) です。 アプライアンスに複数のホスト名がある場合はすべての名前を追加します。

従来の NetBackup プライマリサーバーの場合:

- 管理者として NetBackup 管理コンソールにログオンします。
- コンソールのメインウィンドウの左ペインで、[NetBackup の管理 (NetBackup Management)]、[ホストプロパティ (Host Properties)]、[プライマリサーバー (Primary Servers)]の順にクリックします。
- 右ペインで、プライマリサーバーのホスト名をクリックします。
- [ホストプロパティ (Host Properties)]ウィンドウの左ペインで、[サーバー (Servers)]をクリックします。
- 右ペインの[追加サーバー (Additional Servers)]セクションで、[追加 (Add)]をクリックしてアプライアンスのホスト名を入力します。アプライアンスのホスト名が最上部の[追加サーバー (Additional Servers)]セクションに表示されます。
  アプライアンスに複数のホスト名がある場合はすべての名前を追加します。
- [OK]をクリックして[プライマリサーバープロパティ (Primary Server Properties)]ウィンドウを閉じます。

3 プライマリサーバーとメディアサーバーの間にファイアウォールがある場合、プライマリサーバーの次のポートを開いてメディアサーバーとの通信を許可します。

メモ: ポート設定を変更するには管理者としてログインしている必要があります。

- `vnetd: 13724`
- `bprd: 13720`
- `PBX: 1556`
- プライマリサーバーが TCP を利用する NetBackup Appliance の場合、次のポートを開きます。
  443、5900、7578。

4 メディアサーバーの日時とプライマリサーバーの日時が一致していることを確認します。NTP サーバーを使うことも、時間を手動することもできます。

5 NAT ネットワークで新しいメディアサーバーを使用する予定がある場合は、メディアサーバーを構成する前に次のタスクを実行します。

- プライマリサーバーで DNAT 機能を有効にします。
  アプライアンスプライマリサーバーで、シェルメニューにログインし、次のコマンドを実行します。

  ```
  Main > Settings > NetBackup DNAT Enable
  ```

従来の (非アプライアンス) NetBackup プライマリサーバーについて詳しくは、『Veritas NetBackup 管理者ガイド Vol. 1』を参照してください。第 5 章とトピックタイトル「NetBackup ドメイン内の NAT ホストを有効にするワークフロー」を参照してください。

- プライマリサーバーの NetBackup サーバーリストに新しい NAT メディアサーバーの名前を追加します。
  アプライアンスプライマリサーバーで、シェルメニューにログインし、次のコマンドを実行します。
  ```
  Main > Settings > NetBackup NATServers Add
  ```
  従来の (非アプライアンス) NetBackup プライマリサーバーで、NAT サーバー名を手動で `bp.conf` レジストリファイルに追加するか、`bpsetconfig` コマンドを使用します。次のように、各サーバー名をスペースで区切って 1 行に入力する必要があります。
  NAT_SERVER_LIST = media1 media2 media3

p.33 の「NetBackup Appliance Web コンソールを使用して NetBackup 53xx シリーズのアプライアンスの初期構成を実行する」を参照してください。

NetBackup Appliance Web コンソールを使用して NetBackup 53xx シリーズのアプライアンスの初期構成を実行する

このトピックでは、新規または出荷時のデフォルト (出荷時の設定) にリセットされている NetBackup 53xx シリーズのアプライアンスを構成する方法について説明します。

この方法では、アプライアンスポート NIC1 (eth0) にノートパソコンを直接接続する必要があります。NetBackup 53xx Appliance は、メディアサーバーとしてのみ構成できます。

リリース 4.0 以降では、初期構成プロセスで、admin、maintenance、sysadmin (IPMI) ユーザーアカウントのデフォルトのパスワードを変更する必要があります。デフォルトの admin パスワードは、アプライアンスの初期ログインでのみ有効です。[パスワードの変更 (Password Change)] ページは、ようこそページの [アプライアンスを設定 (Setup Appliance)] をクリックした後に最初に表示されます。

リリース 3.2 以降では、外部認証局の証明書がサポートされています。この機能は、ホストの検証とセキュリティのために NetBackup 認証局を使用する代替手段を提供します。この手順には、これらの証明書を配備するために必要な情報が含まれています。セキュリティ証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「NetBackup の外部 CA サポート」の章を参照してください。

高可用性構成の場合、この手順を使用して 53xx Appliance (計算ノード) を構成します。その後、構成したノードを使用して高可用性設定を構成します (手順 16 を参照)。

このメディアサーバーの初期構成を実行する前に、すでに次のタスクを完了していることを確認してください。

- プライマリサーバーとメディアサーバーが互換性のあるソフトウェアのバージョンであることを検証済みであること。
- プライマリサーバー上の SERVERS リストにこのメディアサーバーのホスト名を追加済みであること。
  高可用性構成の場合、設定手順に使用するノードのホスト名が追加済みであること。
- プライマリサーバーとこのメディアサーバーの間にファイアウォールがある場合は、プライマリサーバーの該当するポートが開かれていること。
- NAT ネットワークでこのメディアサーバーを使用する場合は、必ずプライマリサーバーの DNAT 機能を有効にし、プライマリサーバーの NAT サーバーリストにこのメディアサーバー名を追加してください。

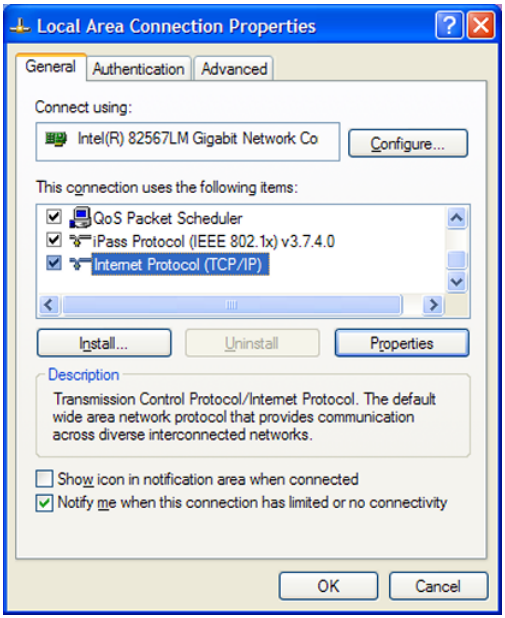
次のリンクには、上記のタスクの実施方法が指示されています。

p.30 の「プライマリサーバーの構成によるアプライアンスのメディアサーバーとの通信」を参照してください。

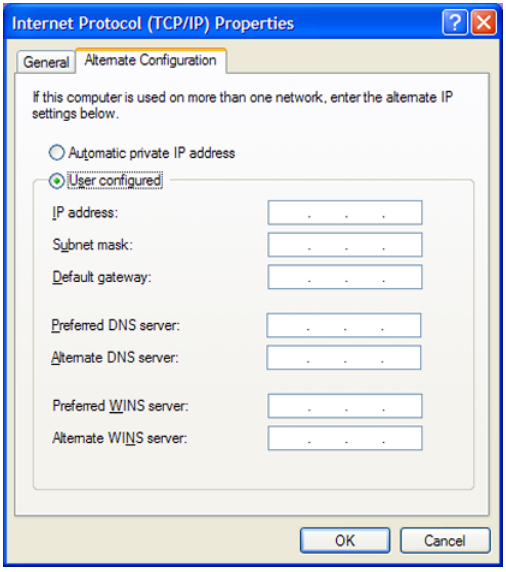
NetBackup Appliance Web コンソールを使用して NetBackup 53xx メディアサーバーアプライアンスの初期構成を実行するには

1. アプライアンスポート NIC1 にノートパソコンを接続します。次に、[ローカルエリアの接続プロパティ (Local Area Connection Properties)]ダイアログボックスに移動します。

   [全般 (General)]タブで、[インターネットプロトコル (TCP/IP) (Internet Protocol (TCP/IP))]を選択してハイライト表示し、[プロパティ (Properties)]をクリックします。



［代替の構成 (Alternate Configuration)］タブで、次のタスクを実行します。



- ［ユーザー構成 (User Configured)］をクリックします。

- ［IP アドレス (IP address)］に、192.168.229.nnn と入力します。nnn は 2 から 254 (233 を除く) の任意の数字です。
- ［サブネットマスク (Subnet mask)］に、255.255.255.0 と入力します。
- ［OK］をクリックします。

2 アプライアンスに接続したノートパソコンで Web ブラウザを開いて次の URL にアクセスします。

http://192.168.229.233

セキュリティ例外を続行することを確かめます。

3 次のようにデフォルトのクレデンシャルでアプライアンスにログオンします。

- ［ユーザー名 (User Name)］: admin
- ［パスワード (Password)］: P@ssw0rd

4 ［Appliance の設定へようこそ (Welcome to Appliance Setup)］ページで、初期構成を実行するために必要な情報の概要を確認します。

- ［構成チェックリストのダウンロード (Download Configuration Checklist)］
  事前に『NetBackup 53xx 初期構成ガイド』のチェックリストに記入していない場合は、このリンクをクリックして電子バージョンにアクセスします。構成の実行時に使えるように、最初にこのファイルを印刷し、記入しておくことをお勧めします。初期構成を完了したら、将来の参照用にこのチェックリストを安全な場所に保管します。
- ［アプライアンスを設定 (Setup Appliance)］
  構成チェックリストに記入した後、この項目をクリックして構成を開始します。

5 ［パスワードの変更 (Password Change)］ページに、出荷時のデフォルトのパスワードを置き換える新しいアプライアンスのアカウントパスワードを入力します。

新しいパスワードを設定する前に、次のパスワードポリシーを確認してください。

- パスワードは少なくとも 8 文字にする必要があります。
- パスワードには、少なくとも 1 つの小文字 (a から z) と 1 つの数字 (0 から 9) を含める必要があります。
- 辞書にある言葉は弱いパスワードと見なされて受け入れられません。
- sysadmin (IPMI) ユーザーのパスワードは、20 文字以下にする必要があります。
- 過去 7 回分のパスワードは再利用できません。以前のパスワードに類似する新しいパスワードも使えません。

次に、アカウントが表示される順序と、各パスワード変更のプロンプトを示します。

admin	新しい admin パスワード (New admin password): 新しい admin パスワードの確認 (Confirm new admin password):
maintenance	新しい maintenance パスワード (New maintenance password): 新しい maintenance パスワードの確認 (Confirm new maintenance password):
sysadmin (IPMI)	新しい sysadmin パスワード (New sysadmin password): 新しい sysadmin パスワードの確認 (Confirm new sysadmin password):

すべてのデフォルトのパスワードを変更した後、[次へ (Next)]をクリックします。

6 [ストレージの概要 (Storage Overview)]ページで、接続したハードウェアコンポーネントの状態を調べて確認します。

ダイアグラムでは、コンポーネントケーブルまたはディスクドライブに問題が存在するかどうかを示す固有のアイコンが使われます。以下では、表示される可能性のある一般的なアイコンについて説明します。

メモ: ヘルプ (?) アイコンをクリックすると、アイコンの説明の完全な一覧が表示されます。

OK

警告 (Warning)

後で解決できる問題を示します。この場合は、初期構成を続行できます。ただし、このような問題により、影響を受けるデバイスにアクセスできなくなります。アイコンをクリックして、問題の説明を参照してください。

エラー

初期構成を続行する前にすぐに解決する必要のある重要な問題を示します。アイコンをクリックして、問題の説明を参照してください。

情報

アイコンをクリックして、特定領域に関する情報を参照してください。

問題がなければ、[次へ (Next)]をクリックして初期構成を開始します。問題を解決する場合は次のガイドラインを使います。

- 問題の説明を表示するには、警告またはエラーアイコンをクリックします。
- すべてのケーブルが正しく接続され、固定されていることを確認します。
- すべてのディスクドライブが正しく設置され、固定されていることを確認します。
- すべてのユニットが電源オンであり、完全に起動していることを確認します。
- ハードウェアチェックリストの項目をすべてチェック済みであることを確認します。
- 上記の項目の確認後または変更後に[更新 (Refresh)]をクリックします。警告またはエラーアイコンが表示されなくなった場合は、問題が解決したことを示します。
  初期構成を開始する前にすべての問題を解決することをお勧めします。

メモ: 上記の項目のすべてを確認し更新してもエラー問題を解決できない場合は、そこで作業を中止してベリタスのテクニカルサポートにお問い合わせください。

---

7 [ネットワーク構成 (Network Configuration)]ページには、特定のタスクを完了するための次のタスクバーと、ネットワーク接続を構成するための関連するデータ入力フィールドがあります。

- [ボンドの作成 (Create Bond)] - 2 つ以上のネットワークインターフェース間の結合を作成するために使用します。
- [VLAN のタグ付け (Tag VLAN)] - 既存のネットワーク環境の VLAN を構成するために使用します。
- [静的ルートの追加 (Add Static Route)] - ネットワークのルート構成を追加するために使用します。

各タスクバーを展開して、関連するネットワーク構成情報を入力します。これらの機能は互いに独立しているため、表示される順序で構成する必要はありません。

メモ: NetBackup Appliance は、同じサブネットに属する 2 つの IP アドレスの構成をサポートしません。アプライアンスは Linux のオペレーティングシステムで実行され、この種類のネットワークは現在の制限事項です。作成する各結合は、異なるサブネットに属する IP アドレスを使う必要があります。

メモ: アプライアンスのホスト名がその IP アドレスに解決される場合は、IP アドレスを削除できません。

次のように、[ボンドの作成 (Create Bond)]の適切な情報を入力します。

[ボンドの作成 (Create Bond)]データ入力フィールド

- ネットワークインターフェース (Network Interface)
  ドロップダウンボックスをクリックし、ネットワーク接続に使うイーサネット NIC ポートを選択します。
- 結合モード (Bond Mode)
  ドロップダウンボックスをクリックし、結合する NIC ポートに使う結合モードを選択します。結合により、複数のネットワークインターフェースを単一の論理「結合」インターフェースに集約できます。結合されたインターフェースの動作はモードによって異なります。デフォルト結合モードは[balance-alb]です。

  ドロップダウンリストから利用可能な結合モードは以下のとおりです。
  - balance-rr
  - active-backup
  - balance-xor
  - broadcast
  - 802.3ad
  - balance-tlb
  - balance-alb

  いくつかの結合モードでは、スイッチまたはルーターでの追加構成が必要となります。結合モードを選択する際には、その点にも注意する必要があります。
  結合モードについて詳しくは、次のマニュアルを参照してください。
  http://www.kernel.org/doc/Documentation/networking/bonding.txt
  すべてのフィールドに適切なデータを入力した後に、[+]をクリックして選択したネットワークインターフェースを追加してすぐに組み込む必要があります。結合を構成するには、[結合モード (Bond Mode)]ドロップダウンボックスから複数のインターフェースを選択する必要があります。IPv6 アドレスには、[サブネットマスク (Subnet Mask)]として 64 を入力します。
- IP アドレス (IP Address)
  このアプライアンスサーバーの IP アドレスを入力します。
- サブネットマスク (Subnet Mask)
  このアプライアンスサーバーの IP アドレスを特定するネットワークアドレスを入力します。
- すべてのフィールドに適切なデータを入力した後に[+]をクリックし、結合設定を保存して追加します。

ご使用の環境で必要な場合は、次のように適切な Tag VLAN 情報を入力します。

[VLAN のタグ付け (Tag VLAN)]データ入力フィールド

- インターフェースの選択
  VLAN をタグ付けするネットワークインターフェースかデバイス名を選択します。
- 説明 (Description)
  VLAN の説明を入力します。たとえば、財務、人事管理など。
- VLAN Id
  VLAN に 1 から 4094 までの番号識別子を入力します。
- IP アドレス [IPv4 または IPv6] (IP Address [IPv4 or IPv6])
  このアプライアンスで使う IPv4 または IPv6 アドレスを入力します。
- サブネットマスク (Subnet Mask)
  IP アドレスに対応するサブネットマスク値を入力します。
- [追加 (Add)]をクリックして、タグ付けする VLANの構成情報を既存のネットワーク環境に追加します。
  タグ付けする追加の VLAN の情報を入力するには、[+]記号をクリックして行を追加します。行を削除するには、[サブネットマスク (Subnet Mask)]フィールドの横にある[-]記号をクリックします。

次のように、[静的ルートの追加 (Add Static Route)]の適切な情報を入力します。

[ルーティング構成 (Routing Configuration)]データ入力フィールド

- 宛先 IP (Destination IP)
  宛先ネットワークのネットワーク IP アドレスを入力します。アドレスは IPv4 または IPv6 のいずれかになります。グローバルスコープと一意的ローカルの IPv6 アドレスのみが許可されます。
  p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。
- 宛先のサブネットマスク (Destination Subnet Mask)
  [宛先 IP (Destination IP)]のアドレスに対応するサブネット値を入力します。
  初期構成では、変更できないデフォルト値がこのフィールドに含まれています。別のルートを構成するときは、適切な値を入力する必要があります。
- ゲートウェイ (Gateway)
  別のネットワークへの入り口として機能するネットワークポイントのアドレスを入力します。アドレスは IPv4 または IPv6 のいずれかになります。グローバルスコープと一意的ローカルの IPv6 アドレスのみが許可されます。
  p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。
- ネットワークインターフェース (Network Interface)
  ドロップダウンボックスをクリックし、ネットワーク接続に使うイーサネット NIC ポートを選択します。
- すべてのフィールドに適切なデータを入力した後に[+]をクリックし、ルーティング構成の設定を保存して追加します。

8 [ホスト構成 (Host Configuration)]ページで、次のようにホストの解決情報を入力できます。

- ［hosts ファイルを手動で編集するには、ここをクリック (To edit the hosts file manually, click here)］
  IP アドレス、完全修飾ホスト名、短いホスト名を /etc/hosts ファイルに直接追加します。［ここ (here)］をクリックして /etc/hosts ファイルを開いて編集します。
- 以下のフィールドにアプライアンスのホスト名と関連ホスト解決情報を入力します。

ホスト名 (Host Name)

このアプライアンスの完全修飾ドメイン名 (FQDN) を入力します。

このアプライアンスの短いホスト名または完全修飾ドメイン名 (FQDN) を入力します。

一部の例外を除き、ホスト名はアプライアンス構成全体に適用されます。短縮名は次の場所に常に表示されます。

- NetBackup Appliance シェルメニュープロンプト
- 重複排除プールカタログのバックアップポリシー
- デフォルトのストレージユニットおよびディスクプール名

このアプライアンスが出荷時の設定にリセットされていて、以前のバックアップイメージのいずれかをインポートする場合は、アプライアンスのホスト名が次のルールのいずれかを満たしている必要があります。

- ホスト名は出荷時の設定へのリセット前に使われるものとまったく同じである必要があります。
- FQDN にホスト名を変更する場合は、出荷時の設定へのリセットの前に使われた短い名前を含んでいる必要があります。たとえば、「myhost」が出荷時の設定へのリセットの前に使われた場合は、新しい FQDN として「myhost.domainname.com」を使います。
- 短いホスト名にホスト名を変更する場合は、出荷時の設定へのリセットの前に使われた FQDN から得られる名前にする必要があります。たとえば、「myhost.domainname.com」が出荷時の設定へのリセットの前に使用された場合は、新しい短いホスト名として「myhost」を使用します。

メモ: ドメイン名のサフィックスはホスト名に付加され、初期構成が完了した後は変更できません。後でサフィックスを変更したり、アプライアンスを別のドメインに移動したりする必要がある場合は、最初に出荷時の設定へのリセットを実行してから、初期構成を再度実行する必要があります。

DNS システムの場合:

以下の[ドメイン名システム (Domain Name System)]情報を入力します。

- ドメイン名のサフィックス (Domain Name Suffix)
  DNS サーバーのサフィックス名を入力します。
- DNS の IP アドレス (DNS IP Address(es))
  DNS サーバーの IP アドレスを入力した後、[+]アイコンをクリックしてアドレスを追加します。必要なアドレスの追加数に応じて繰り返します。
  アドレスは IPv4 または IPv6 のいずれかになります。IPv6 アドレスの場合は、グローバルスコープまたは一意のローカルアドレスのみを入力できます。
  p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。
  アドレスを削除するには、データ入力フィールド下のリストからそのアドレスを選択し、[x]アイコンをクリックします。
- 検索ドメイン (Search Domain(s))
  ご使用の環境で必要な場合、検索ドメイン名を入力し、+ アイコンをクリックして、その名前を追加します。必要な検索ドメインの追加数に応じて繰り返します。
  検索ドメインを削除するには、データ入力フィールド下のリストからその検索ドメインを選択し、[x]アイコンをクリックします。

必要な情報をすべて入力した後、[次へ (Next)]をクリックします。

DNS を使わないシステムの場合

以下の[ホスト名解決 (Host name resolution)]の情報を入力します。

- IP
  アプライアンスの IP アドレスを入力します。
  アドレスは IPv4 または IPv6 のいずれかになります。IPv6 アドレスの場合は、グローバルスコープまたは一意のローカルアドレスのみを入力できます。
  p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。
- 完全修飾ホスト名 (Fully qualified host name)
  アプライアンスの完全修飾ホスト名 (FQHN) を入力します。
- 短いホスト名 (Short host name)
  アプライアンスの短い名前を入力します。
  2 つ以上の名前を入力するには、名前の間にスペースなしでカンマを追加します。

すべてのフィールドに入力した後、[+]アイコンをクリックします。追加したエントリがフィールドの下に表示されます。

必要な情報をすべて入力した後、[次へ (Next)]をクリックします。

9 [日時 (Date & Time)]ページで、このアプライアンスの適切な日付と時刻を入力します。このメディアサーバーの日時は、関連付けられたプライマリサーバーの日時と一致する必要があります。

情報を手動で入力する以外に、NTP (Network Time Protocol) サーバーを使ってネットワーク上でアプライアンスの日時を同期することもできます。

タイムゾーン (Time zone)	アプライアンスにタイムゾーンを割り当てるには、[タイムゾーン (Time zone)]ドロップダウンボックスをクリックし、該当する地域、国、タイムゾーンを選択します。
日付と時刻の指定 (Specify date & time)	日付と時刻を手動で入力するには、このオプションを選択し、次の情報を入力します。 ■ 最初のフィールドに、mm/dd/yyyy の形式で日付を入力します。または、カレンダーのアイコンをクリックし、適切な年月日を選択します。 ■ 2 番目のフィールドに、hh:mm:ss の形式で時刻を入力します。24 時間形式 (00:00:00 - 23:59:59) で入力する必要があります。
NTP	アプライアンスを NTP サーバーと同期するには、このオプションを選択して適切な NTP [サーバーの IP (Server IP)] アドレスを入力します。

必要な情報をすべて入力した後、[次へ (Next)]をクリックします。

10 [アラートとコールホーム (Alerting and Call Home)]ページで、アプライアンスがベリタスコールホームサーバーに電子メールでアラートを送信したり、状態レポートをアップロードするための情報を入力したりします。

アラートをアップロードするようにこのサーバーを構成するには、次のように適切なアラートの構成情報を入力します。

アラートの構成 (Alert configuration)

通知の間隔 (Notification interval) (分)

サーバーがベリタスのコールホームサーバーにアラートをアップロードする間隔を入力します。Veritas15 分単位で入力する必要があります。

アラートの構成 **(Alert configuration)**

アラートの構成 (Alert configuration)

SNMP サーバーの構成 (SNMP Server Configuration)

次のオプションのいずれかを選択します。

- SNMP V2
- SNMP V3
- なし (None) (デフォルト)
  - SNMP サーバー (SNMP Server)
    このサーバーを定義する SNMP サーバーのホスト名または IP アドレスを入力します。
    IPv4 または IPv6 の IP アドレスを入力できます。IPv6 の場合は、グローバルスコープと一意のローカルアドレスのみを入力できます。
  - SNMP ポート (SNMP Port)
    このサーバーとの通信を許可する SNMP サーバーのポート番号を入力します。デフォルト値は 162 です。

    メモ: ファイアウォールで、このポートを介してアプライアンスから SNMP サーバーにアクセスできるようにする必要があります。
  - SNMP コミュニティ (SNMP Community)
    このフィールドは SNMP V2 の場合は必須、SNMP V3 の場合は省略可能です。
    警告やトラップが送信されるコミュニティ名を入力します。
    たとえば、[SNMP サーバー (SNMP server)]に入力した情報と同じ情報を入力できます。また、会社名の他、admin_group、public、private などの名前も入力できます。何も入力しない場合、デフォルト値は public です。
  - SNMP ユーザー名 (SNMP Username) (SNMP V3 のみ)
    SNMP ユーザー名を次のように入力します。
    - 最大 32 文字まで入力できます。
    - 大文字、小文字、数字の他、ピリオド、ハイフンまたはダッシュ、アンダースコアを含めることができます。
    - 空白、カンマ、特殊文字は使用できません。
  - 認証プロトコル (Authentication Protocol) (SNMP V3 のみ)
    次のように構成して、セキュリティレベルを設定します。
    - なし (None) (デフォルト)
      セキュリティレベルを認証なし、権限なし (認証無効) に設定します。パスワードと暗号化のフィールドは灰色で表示されており、必須ではありません。
    - SHA256 または SHA512
      認証のセキュリティレベルを設定します。SNMP パスワードが必要です。
  - SNMP パスワード (SNMP Password)/SNMP パスワードの確認 (Confirm SNMP Password) (SNMP V3 のみ)
    次のように、SNMP ユーザーのパスワードを入力します。
    - 8 文字以上にする必要があります。
    - 大文字、小文字、数字の他、ピリオド、ハイフンまたはダッシュ、アンダースコアを含めることができます。

アラートの構成 (Alert configuration)

- 空白、カンマ、特殊文字は使用できません。

暗号化プロトコル (Encryption Protocol) (SNMP V3 のみ)

次のように構成して、暗号化ポリシーを設定します。

- なし (None) (デフォルト)
  暗号化ポリシーを使用せず、適用もされません。パスフレーズのフィールドは灰色で表示されており、必須ではありません。
- AES128 AES192 AES256 AES512
  これらのオプションのいずれかを選択して、関連付けられている暗号化ポリシーを適用します。暗号化パスフレーズが必要です。

アラートの構成 (Alert configuration)

- 暗号化パスフレーズ (Encryption Passphrase)/暗号化パスフレーズの確認 (Confirm Encryption Passphrase)(SNMP V3 のみ)
  暗号化ポリシーを使用するように暗号化プロトコルを設定した場合は、SNMP ユーザーのパスフレーズを次のように入力します。
  - 8 文字以上にする必要があります。
  - 大文字、小文字、数字の他、ピリオド、ハイフンまたはダッシュ、アンダースコアを含めることができます。
  - 空白、カンマ、特殊文字は使用できません。

  次に、特定の SNMP 設定シナリオに必要なフィールドの概要を示します。
  - SNMP V2
    SNMP サーバー (SNMP Server)
    SNMP ポート (SNMP Port)
    SNMP コミュニティ (SNMP Community)
    これら以外のフィールドは必須ではありません。
  - SNMP V3 - 認証なし/権限なし
    SNMP サーバー (SNMP Server)
    SNMP ポート (SNMP Port)
    SNMP コミュニティ (SNMP Community) (オプション)
    認証プロトコル - なし
    これら以外のフィールドは必須ではありません。
  - SNMP V3 - 認証/権限なし
    SNMP サーバー (SNMP Server)
    SNMP ポート (SNMP Port)
    SNMP コミュニティ (SNMP Community) (オプション)
    認証プロトコル (Authentication Protocol) (SHA256、SHA512)
    SNMP パスワード (SNMP Password)/SNMP パスワードの確認 (Confirm SNMP Password)
    これら以外のフィールドは必須ではありません。
  - SNMP v3 - 認証/権限
    SNMP サーバー (SNMP Server)
    SNMP ポート (SNMP Port)
    SNMP コミュニティ (SNMP Community) (オプション)
    認証プロトコル (Authentication Protocol) (SHA256、SHA512)
    SNMP パスワード (SNMP Password)/SNMP パスワードの確認 (Confirm SNMP Password)
    暗号化プロトコル (Encryption Protocol) (AES128、AES192、AES256、AES512)
    暗号化パスフレーズ (Encryption Passphrase)/暗号化パスフレーズの確認 (Confirm Encryption Passphrase)

アラートの構成 (Alert configuration)

- SNMP の MIB ファイルを表示 (View SNMP MIB file)
  関連トラップを監視するハードウェアを受信するようにアプライアンスの SNMP マネージャを設定するには、このリンクをクリックして MIB ファイルの内容を表示します。次に、ファイルを別の場所にコピーし、その内容を使って SNMP マネージャを更新します。
  SNMP MIB ファイルは、SNMP メッセージの生成と解釈に使われるデータ辞書として機能します。SNMP を構成する場合は、SNMP トラップを解釈できるように監視ソフトウェアに MIB ファイルをインポートする必要があります。アプライアンスは SNMPv2c 形式のトラップのみを受け入れることができます。

SMTP サーバー構成 (SMTP Server Configuration)

- SMTP サーバー (SMTP Server)
  SMTP サーバーのホスト名または IP アドレスを入力します。
- SMTP ポート (SMTP Port)
  このサーバーとの通信を許可する SNMP サーバーのポート番号を入力します。デフォルトは 25 です。
- ソフトウェア管理者の電子メール (Software Administrator Email)
  ソフトウェア管理者が通知を受信するための電子メールアドレスを入力します。
- ハードウェア管理者の電子メール (Hardware Administrator Email)
  ハードウェア管理者が通知を受信するための電子メールアドレスを入力します。
- 送信者の電子メール (Sender Email)
  受信者がレポートのソースを識別できるようにこのサーバーの電子メールアドレスを入力します。
- SMTP アカウント (SMTP Account)
  SMTP サーバーのアカウント名を入力します。
- パスワード (Password)
  セキュリティを高めるには、SMTP サーバーのパスワードを入力します。

プロキシサーバーまたはベリタスコールホームサーバーに電子メールのレポートを送信するように、このサーバーを構成できます。

次のプロキシサーバーがサポートされます。

- Squid
- Apache
- TMG

メモ: プロキシ構成の NTLM 認証もサポートされます。

コールホームの場合は、次のように、[コールホームの構成 (Call Home Configuration)]の適切な情報を入力します。

[コールホームの構成 (Call Home Configuration)]データ入力フィールド

- コールホームの有効化 (Enable Call Home)
  アプライアンスがベリタスコールホームサーバーに電子メールレポートを送信するようにするには、このチェックボックスにチェックマークを付けます。
- プロキシサーバーを有効化 (Enable proxy server)
  電子メール通知にプロキシサーバーを使う場合は、このチェックボックスにチェックマークを付け、以下のプロキシ情報を入力します。
- プロキシのトンネリングを有効にする (Enable proxy Tunneling)
  プロキシトンネリングを有効にするには、このチェックボックスにチェックマークを付け、以下のプロキシ情報を入力します。
  - プロキシサーバー (Proxy server)
    サーバーの IP アドレスを入力します。
    IPv4 または IPv6 の IP アドレスを入力できます。IPv6 の場合は、グローバルスコープと一意のローカルアドレスのみを入力できます。
  - プロキシポート (Proxy port)
    このアプライアンスとの通信を許可するプロキシサーバーのポート番号を入力します。
  - プロキシのユーザー名 (Proxy username)
    プロキシサーバーのユーザー名を入力します。
  - プロキシのパスワード (Proxy password)
    プロキシサーバーのパスワードを入力します。
  - コールホームのテスト (Test Call Home)
    必要な情報をすべて入力した後、[コールホームのテスト (Test Call Home)]をクリックして、ベリタスサーバーとの通信を確認することをお勧めします。
    テストが失敗した場合は、すべての名前、IP アドレス、ポート番号が正しく入力されていることを確認してください。テストが再度失敗した場合は、ベリタスのテクニカルサポートにお問い合わせください。

必要な情報をすべて入力した後、[次へ (Next)]をクリックします。

11 [プライマリサーバーの指定 (Specify Primary Server)]ページで、次の項目に関するメッセージが表示されます。

- DNAT の構成 (DNAT configuration)
  NAT ネットワークでこのメディアサーバーを使用する予定がある場合は、プロンプトに従ってください。
- プライマリサーバー名 (Primary Server Name)
  名前と IP アドレスが 1 つしかないプライマリサーバーの場合は、プライマリサーバーのホスト名または IP アドレスを入力し、[追加 (Add)]をクリックします。
  クラスタ化されたプライマリサーバーの場合や、複数の名前と IP アドレスがあるプライマリサーバーの場合、フィールドに各ホスト名または IP アドレスを (1 回に 1 つずつ) 入力し、[追加 (Add)]をクリックします。プライマリサーバーがクラスタ化されている場合は、最初のエントリはクラスタの仮想ホスト名である必要があります。

プライマリサーバーのホスト名が FQDN の場合は、Veritasは FQDN を使用してメディアサーバーのプライマリサーバーを指定することをお勧めします。

- 証明書のプロビジョニング/証明書失効リスト (CRL)
  プライマリサーバー名の入力後、アプライアンスは、認証局 (CA) ステータスのプライマリサーバーに ping を実行し、結果を表示します。次の箇条書き項目はそれぞれ、表示される可能性のあるステータス結果を示しています。該当するステータス結果の下に表示される指示に従って、証明書の構成を完了します。

  - プライマリサーバーでは現在、外部 CA が発行した証明書が使用されています。このアプライアンスは、同じ外部 CA が発行した証明書で構成する必要があります。
    次の証明書プロビジョニング情報を入力します。
    ホスト証明書
    信頼できる証明書
    プライベートキー
    プライベートキーパスフレーズ (プライベートキーファイルが暗号化されている場合のみ必要)
    次のいずれかの CRL オプションを選択します。
    証明書から CRL を使用
    CRL ファイルのアップロード
    CRL は使用しない
    必要な情報をすべて入力した後、[次へ (Next)]をクリックします。

  - プライマリサーバーでは現在、外部 CA が発行した証明書と独自の内部証明書が使用されています。外部 CA 発行の証明書で続行しますか?
    [いいえ (No)]を選択すると、次のメッセージが表示されます。
    このアプライアンスは、セキュアな通信に NetBackup 発行の証明書を使用します。
    [はい (Yes)]を選択した場合は、次の証明書プロビジョニング情報を入力します。
    ホスト証明書
    信頼できる証明書
    プライベートキー
    プライベートキーパスフレーズ (プライベートキーファイルが暗号化されている場合のみ必要)
    次のいずれかの CRL オプションを選択します。
    証明書から CRL を使用
    CRL ファイルのアップロード
    CRL は使用しない
    必要な情報をすべて入力した後、[次へ (Next)]をクリックします。
    [証明書の検証 (Certificate Verification)]ダイアログボックスが表示されたら、[配備 (Deploy)]をクリックして CA 証明書をこのアプライアンスに配備し

ます。必要に応じてトークンを入力し、[配備 (Deploy)]をクリックして、ホスト ID ベースの証明書をこのアプライアンスに配備します。
必要な情報をすべて入力した後、[次へ (Next)]をクリックします。
[証明書の検証 (Certificate Verification)]ダイアログボックスが表示されたら、[配備 (Deploy)]をクリックして CA 証明書をこのアプライアンスに配備します。必要に応じてトークンを入力し、[配備 (Deploy)]をクリックして、ホスト ID ベースの証明書をこのアプライアンスに配備します。

- このアプライアンスは、セキュアな通信に NetBackup 発行の証明書を使用します。
これ以上の証明書の構成は必要ありません。[次へ (Next)]をクリックして続行します。

メモ: 役割の構成を完了すると、ストレージの初期化が開始します。システムのディスクドライブの数によって、ストレージの初期化が完了するまでに最長 46 時間かかることがあります。その結果、アプライアンスのバックアップと復元のパフォーマンスは、ストレージの初期化処理が完了するまで低下します。

---

12 [ストレージの構成 (Storage Configuration)]ページで、使う予定のストレージユニットとディスクプールの名前を作成し、ディスクパーティションのサイズを構成します。

AdvancedDisk 用、重複排除 (MSDP) 用、またはその両方用のストレージのパーティションを構成できます。

メモ: MSDP ストレージを構成することを選択した場合は、MSDP カタログを保護するためのポリシーが自動的に作成されます。このポリシーを見直し、アプライアンスの構成後に有効にすることを推奨します。

AdvancedDisk	次の情報を入力します。 ■ ポリシーのストレージユニット名 (Storage Unit Name) このストレージユニットを識別するために使う名前を入力します。英字、数字、特殊文字を使うことができます。名前には最大 256 文字を含めることができます。 **メモ:** 名前はマイナス (-) 文字から始めることはできません。また名前にスペースを使うこともできません。 ■ ディスクプール名 (Disk Pool Name) このディスクプールを識別するために使う名前を入力します。英字、数字、特殊文字を使うことができます。名前には最大 256 文字を含めることができます。 **メモ:** 名前はマイナス (-) 文字から始めることはできません。また名前にスペースを使うこともできません。 ■ サイズ (Size) [サイズ (Size)]フィールドに正確な数を入力してこのパーティションのサイズを設定するか、または灰色のスライドバーのボックスをクリックして目的のサイズにドラッグします。サイズは、利用可能な最大容量によって、GB 単位または TB 単位で設定できます。
重複排除ディスク (Deduplication Disk (MSDP))	次の情報を入力します。 ■ ポリシーのストレージユニット名 (Storage Unit Name) このストレージユニットを識別するために使う名前を入力します。英字、数字、特殊文字を使うことができます。名前には最大 256 文字を含めることができます。 **メモ:** 名前はマイナス (-) 文字から始めることはできません。また名前にスペースを使うこともできません。 ■ ディスクプール名 (Disk Pool Name) このディスクプールを識別するために使う名前を入力します。英字、数字、特殊文字を使うことができます。名前には最大 256 文字を含めることができます。 **メモ:** 名前はマイナス (-) 文字から始めることはできません。また名前にスペースを使うこともできません。 ■ サイズ (Size) [サイズ (Size)]フィールドに正確な数を入力してこのパーティションのサイズを設定するか、または灰色のスライドバーのボックスをクリックして目的のサイズにドラッグします。サイズは、利用可能な最大容量によって、GB 単位または TB 単位で設定できます。

必要な情報をすべて入力した後、[次へ (Next)]をクリックします。

13 [構成の進捗状況 (Configuration Progress)]ページで、アプライアンスによって構成ページからのすべてのデータ入力が適用される処理の進捗状況を監視できます。

構成が完了するまでの時間は、環境の複雑さによって決まります。

14 [構成の概略 (Summary of Configuration)]ページで、構成の結果を確認します。設定が正常に完了したことを確かめるために結果を確認します。

このページでは、発生した可能性があるエラーの特定も行います。結果にエラーが表示されている場合は、初期構成を再実行する必要がある場合もあります。

15 設定が正常に完了した後、NetBackup のサービスが開始するまで約 10 分お待ちください。その後で、完全修飾ホスト名を使ってアプライアンスに再接続し、ログインする必要があります。

16 高可用性ソリューションの場合は、パートナーノードで初期構成を実行する前に、この構成済みアプライアンス (計算ノード) で高可用性構成を設定する必要があります。高可用性構成を続行して完了するには、次のタスクを記載されている順番どおりに実行します。

p.70 の「NetBackup 53xx の高可用性設定」を参照してください。

p.78 の「NetBackup 53xx 高可用性構成のパートナーノードの初期構成を実行する」を参照してください。

p.85 の「NetBackup 53xx 高可用性構成へのパートナーノードの追加」を参照してください。

17 すべてのアプライアンスが構成され稼働したら、バックアップするクライアントソフトウェアをコンピュータにインストールする準備が完了します。

p.99 の「NetBackup appliance からクライアントへの NetBackup クライアントパッケージのダウンロード」を参照してください。

p.101 の「NFS 共有を介した NetBackup クライアントソフトウェアのインストール 」を参照してください。

18 MSDP クラウドのアプライアンスを構成する場合は、次の手順を実行します。

- 初期構成の完了後にNetBackup Appliance シェルメニューにログインし、nbasecadmin ユーザーのデフォルトのパスワードを変更します。
- nbasecadmin ユーザーとして NetBackup Web UI にログインし、次のように MSDP クラウドストレージを構成します。
  - ディスクプールを作成します。
  - ストレージユニットを作成します。
    詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

NetBackup Appliance シェルメニューを使用して NetBackup 53xx シリーズのアプライアンスの初期構成を実行する

このトピックでは、新規または出荷時のデフォルト (出荷時の設定) にリセットされている NetBackup 53xx シリーズのアプライアンスの構成方法について説明します。

この方法では、アプライアンスポート NIC1 (eth0) にノートパソコンを直接接続する必要があります。NetBackup 53xx シリーズのアプライアンスは、メディアサーバーとしてのみ構成できます。

NetBackup Appliance リリース 4.0 以降では、初期構成プロセスで、admin、maintenance、sysadmin (IPMI) ユーザーアカウントのデフォルトのパスワードを変更する必要があります。デフォルトの admin パスワードは、アプライアンスの初期ログインでのみ有効です。アプライアンスの役割を設定するために Main_Menu > Appliance コマンドを入力すると、デフォルトのパスワードの変更を求めるメッセージが表示されます。

リリース 3.2 以降では、外部認証局の証明書がサポートされています。この機能は、ホストの検証とセキュリティのために NetBackup 認証局を使用する代替手段を提供します。この手順には、これらの証明書を配備するために必要な情報が含まれています。セキュリティ証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「NetBackup の外部 CA サポート」の章を参照してください。

高可用性構成の場合、この手順を使用して、設定手順に使用するノードを設定します。このアプライアンス (計算ノード) を設定してから高可用性構成を続行および完了する方法について詳しくは、手順 17 を参照してください。

このメディアサーバーの初期構成を実行する前に、すでに次のタスクを完了していることを確認してください。

- プライマリサーバーとメディアサーバーが互換性のあるソフトウェアのバージョンであることを検証済みであること。
- プライマリサーバー上の SERVERS リストにこのメディアサーバーのホスト名を追加済みであること。
  高可用性構成の場合、設定手順に使用するノードのホスト名が追加済みであること。
- プライマリサーバーとこのメディアサーバーの間にファイアウォールがある場合は、プライマリサーバーの該当するポートが開かれていること。
- NAT ネットワークでこのメディアサーバーを使用する場合は、必ずプライマリサーバーの DNAT 機能を有効にし、プライマリサーバーの NAT サーバーリストにこのメディアサーバー名を追加してください。

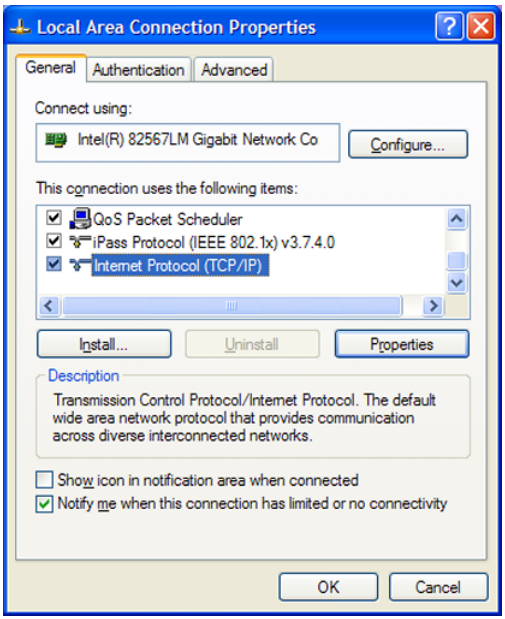
次のリンクには、上記のタスクの実施方法が指示されています。

p.30 の「プライマリサーバーの構成によるアプライアンスのメディアサーバーとの通信」を参照してください。

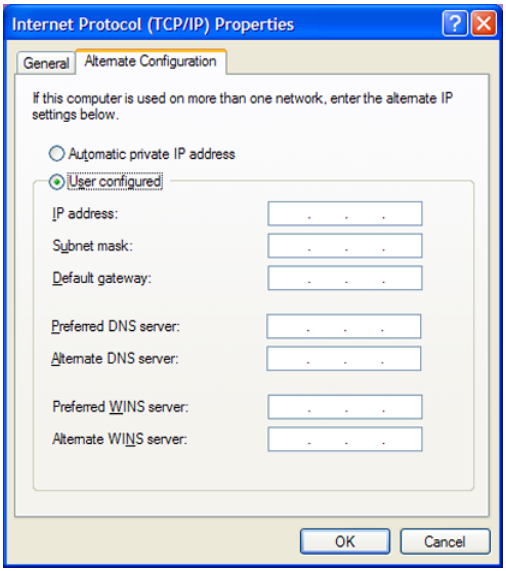
NetBackup Appliance シェルメニューを使用して NetBackup 53xx メディアサーバーアプライアンスの初期構成を実行するには

1 アプライアンスポート NIC1 にノートパソコンを接続します。次に、[ローカルエリアの接続プロパティ (Local Area Connection Properties)]ダイアログボックスに移動します。

[全般 (General)]タブで、[インターネットプロトコル (TCP/IP) (Internet Protocol (TCP/IP))]を選択してハイライト表示し、[プロパティ(Properties)]をクリックします。



[代替の構成 (Alternate Configuration)]タブで、次のタスクを実行します。



- ［ユーザー構成 (User Configured)］をクリックします。
- ［IP アドレス (IP address)］に、`192.168.229.nnn` と入力します。nnn は 2 から 254 (233 を除く) の任意の数字です。
- ［サブネットマスク (Subnet mask)］に、255.255.255.0 と入力します。
- ［OK］をクリックします。

2 アプライアンスに接続しているノートパソコンで、SSH セッションを 192.168.229.233 に開きます。

3 次のようにデフォルトのクレデンシャルでアプライアンスにログオンします。

- ［ユーザー名 (User Name)］: admin
- ［パスワード (Password)］: P@ssw0rd

ようこそメッセージがシェルメニューに表示され、［Main_Menu］ビューにプロンプトが表示されます。

メモ: 初期構成の続行には、デフォルトパスワードの変更は必須ではありません。ただし、環境のセキュリティを高めるためにパスワードを定期的に変更することをお勧めします。現在のパスワードの記録は安全な場所に保管するように徹底してください。NetBackup Appliance シェルメニューにログインしているときにパスワードを変更するには、Main_Menu ビューで `Settings > Password` と入力します。

---

4 初めて設定する前に次のコマンドを入力して、接続したハードウェアコンポーネントの状態を調べて確認します。

```
Support > Test Hardware
```

[警告 (Warning)]は後で解決できる問題を示します。この場合は、初期構成を続行できます。ただし、このような問題により、影響を受けるデバイスにアクセスできなくなります。

[エラー (Error)]は、初期構成を続行する前にすぐに解決する必要のある重要な問題を示します。

コマンド出力で問題を認識した場合には、以下の項目を調べます。

- すべてのケーブルが正しく接続され、固定されていることを確認します。
- すべてのディスクドライブが正しく設置され、固定されていることを確認します。
- すべてのユニットが電源オンであり、完全に起動していることを確認します。
- ハードウェアチェックリストの項目をすべてチェック済みであることを確認します。
- 以前の項目を検証した後、コマンドを再実行します。警告またはエラーアイコンが表示されなくなった場合は、問題が解決したことを示します。初期構成を開始する前にすべての問題を解決することをお勧めします。

メモ: 上記の項目すべてを検証してコマンドを再実行しても[エラー (Error)]の問題を解決できない場合は、そこで作業を中止してベリタスのテクニカルサポートにお問い合わせください。

---

5 Main_Menu > Network ビューで次のコマンドを入力して、アプライアンスが接続する単一ネットワークの IP アドレスを設定します。

```
Configure IPAddressNetmaskGatewayIPAddress [InterfaceNames]
```

ここで、*IPAddress* は新しい IP アドレス、*Netmask* はネットマスク、*GatewayIPAddress* はインターフェースのデフォルトゲートウェイです。`[InterfaceNames]` オプションは省略可能です。

IP Address や *Gateway IP Address* には、IPv4 または IPv6 アドレスを指定できます。グローバルスコープと一意的ローカルの IPv6 アドレスのみが許可されます。

ただし、同じコマンド内で IPv4 と IPv6 アドレスの両方は使わないでください。たとえば、`Configure 9ffe::9 255.255.255.0 1.1.1.1.` は使用できません。`Configure 9ffe::46 64 9ffe::49 eth1` を使用する必要があります。

p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。

複数のネットワークを構成する場合には、追加する各ネットワークの IP アドレスを最初に構成する必要があります。次に、追加した各ネットワークのゲートウェイアドレスを構成します。必ずデフォルトゲートウェイアドレスを最初に追加する必要があります。以下の 2 つのコマンドを使います。

各ネットワークの IP アドレスの構成	ネットワークインターフェースに対して IPv4 または IPv6 アドレスのどちらを構成するかに応じて、以下のコマンドのいずれかを使います。 ネットワークインターフェースの IPv4 アドレスを構成するには `IPv4 IPAddressNetmask [InterfaceName]` ここで、*IPAddress* は新しい IP アドレス、*Netmask* はネットマスクです。`[InterfaceName]` は省略可能です。追加する IP アドレスごとにこのコマンドを繰り返します。 ネットワークインターフェースの IPv6 アドレスを構成するには IPv6 <*IP Address*> <Prefix> [InterfaceNames] ここで、*IPAddress* は IPv6 アドレス、*Prefix* はプレフィックス長です。`[InterfaceName]` は省略可能です。

追加した各ネットワークのゲートウェイアドレスの構成	`Gateway Add GatewayIPAddress [TargetNetworkIPAddress] [Netmask] [InterfaceName]` ここで、*GatewayIPAddress* はインターフェースのゲートウェイです。*TargetNetworkIPAddress*、*Netmask*、`InterfaceName` は省略可能です。このコマンドを繰り返して、すべての宛先ネットワークにゲートウェイを追加します。 *Gateway IP Address* や *TargetNetworkIPAddress* には、IPv4 または IPv6 アドレスを指定できます。 ただし、同じコマンド内で IPv4 と IPv6 アドレスの両方は使わないでください。たとえば、`Gateway Add 9ffe::3 255.255.255.0 eth1` は使用できません。`Gateway Add 9ffe::3 6ffe:: 64 eth1` を使用する必要があります。

6 [Main_Menu] > [ネットワーク (Network)] ビューで次のコマンドを使って、アプライアンスの DNS ドメイン名を設定します。

メモ: DNS を使わない場合は、ステップ 9 に進んでください。

```
DNS Domain Name
```

ここで、*Name* はアプライアンスの新しいドメイン名です。

7 Main_Menu > Network ビューで、次のコマンドを使って DNS ネームサーバーをアプライアンス構成に追加します。

```
DNS Add NameServer IPAddress
```

ここで、*IPAddress* は DNS サーバーの IP アドレスです。

アドレスは IPv4 または IPv6 のいずれかになります。グローバルスコープと一意的ローカルの IPv6 アドレスのみが許可されます。

p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。

複数の IP アドレスを追加するには、スペースを空けずに各アドレスをカンマで区切ります。

8 Main_Menu > Network ビューで次のコマンドを使って、DNS 検索ドメインをアプライアンス構成に追加し、異なるドメインにあるホスト名をアプライアンスが解決できるようにします。

```
DNS Add SearchDomain SearchDomain
```

ここで、*SearchDomain* は検索用に追加する対象ドメインです。

9 この手順は省略可能です。ここでは、アプライアンスの hosts ファイルに、他のホストの IP アドレスを追加できます。

Main_Menu > Network ビューで次のコマンドを使って、ホストエントリをアプライアンスの hosts ファイルに追加します。

```
Hosts Add IPAddressFQHNShortName
```

ここで、*IPAddress* は IPv4 または IPv6 アドレス、*FQHN* は完全修飾ホスト名、*ShortName* は短いホスト名です。

p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。

10 Main_Menu > Network ビューで次のコマンドを使って、アプライアンスのホスト名を設定します。

```
Hostname Set Name
```

Name は、このアプライアンスの短いホスト名または完全修飾ドメイン名 (FQDN) です。

一部の例外を除き、ホスト名はアプライアンス構成全体に適用されます。短縮名は次の場所に常に表示されます。

- NetBackup Appliance シェルメニュープロンプト
- 重複排除プールカタログのバックアップポリシー
- デフォルトのストレージユニットおよびディスクプール名

このアプライアンスが出荷時の設定にリセットされていて、以前のバックアップイメージのいずれかをインポートする場合は、アプライアンスのホスト名が次のルールのいずれかを満たしている必要があります。

- ホスト名は出荷時の設定へのリセット前に使われるものとまったく同じである必要があります。
- FQDN にホスト名を変更する場合は、出荷時の設定へのリセットの前に使われた短い名前を含んでいる必要があります。たとえば、「myhost」が出荷時の設定へのリセットの前に使われた場合は、新しい FQDN として「myhost.domainname.com」を使います。
- 短いホスト名にホスト名を変更する場合は、出荷時の設定へのリセットの前に使われた FQDN から得られる名前にする必要があります。たとえば、「myhost.domainname.com」が出荷時の設定へのリセットの前に使用された場合は、新しい短いホスト名として「myhost」を使用します。

メモ: ドメイン名のサフィックスはホスト名に付加され、初期構成が完了した後は変更できません。後でサフィックスを変更したり、アプライアンスを別のドメインに移動したりする必要がある場合は、最初に出荷時の設定へのリセットを実行してから、初期構成を再度実行する必要があります。

このステップにより、NetBackup は新しいホスト名で動作するように再構成されます。この処理は、完了するまでにしばらく時間がかかることがあります。

`Hostname set` コマンドが機能するためには、少なくとも 1 つの IPv4 アドレスが必要です。たとえば、特定のホストのホスト名を v46 に設定するとします。そのためには、まず、その特定のホストが少なくとも 1 つの IPv4 アドレスを持つことを確認した後、次のコマンドを実行します。

```
Main_Menu > Network > Hostname set v46
```

11 前述のネットワーク構成設定に加え、[Main_Menu] > [ネットワーク (Network)] ビューを使って、アプライアンスの初期設定時に結合を作成して VLAN をタグ付けすることもできます。

- 2 つ以上のネットワークインターフェース間に結合を作成するには、次のコマンドを使います。

  ```
  Network > LinkAggregation Create
  ```

- 物理インターフェースまたは結合インターフェースに VLAN をタグ付けするには、次のコマンドを入力します。

  ```
  Network > VLAN Tag
  ```

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

12 [Main_Menu] > [ネットワーク (Network)] ビューで次のコマンドを使って、このアプライアンスのタイムゾーン、日付および時間を設定します。

- 次のコマンドを入力して、タイムゾーンを設定します。

  ```
  TimeZone Set
  ```

  表示されたリストから該当するタイムゾーンを選択します。

- 次のコマンドを入力して、日付と時刻を設定します。

  ```
  Date Set MonthDayHHMMSSYear
  ```

  ここで、*Month* は月の名前です。
  Day は 0 から 31 までの日付です。
  HHMMSS は 24 時間形式の時、分、秒です。フィールドはセミコロンで区切ります (HH:MM:SS)。
  Year は、1970 から 2037 までの暦年です。

13 [Main_Menu] > [設定 (Settings)] ビューで次のコマンドを使って、SMTP サーバー名とアプライアンスのエラーアラート用の電子メールアドレスを入力します。

SMTP サーバー名の入力	`Email SMTP Add smtp [acct] [pass]` ここで、*smtp* は対象 SMTP サーバーのホスト名、*acct* は SMTP サーバーに対する認証のアカウント名、*pass* は SMTP サーバーに対する認証のパスワードです。
電子メールアドレスの入力	`Email Software Add eaddr` ここで、*eaddr* はアプライアンスからのエラーアラートを受信する電子メールアドレスです。 複数アドレスを入力するには、各アドレスをセミコロンで区切ります。

14 NAT ネットワークでこのメディアサーバーを使用する予定がある場合は、アプライアンスの役割を設定する前に、関連付けられたプライマリサーバーで次のタスクを実行します。

- プライマリサーバーで DNAT 機能を有効にします。
- プライマリサーバーの NetBackup サーバーリストにこのメディアサーバーの名前を追加します。
  p.30 の「プライマリサーバーの構成によるアプライアンスのメディアサーバーとの通信」を参照してください。

15 このメディアサーバーと組み合わせて使用するプライマリサーバーを特定します。

メモ: 続行する前に、プライマリサーバーにこのメディアサーバー名が追加されていることを確認します。p.30 の「プライマリサーバーの構成によるアプライアンスのメディアサーバーとの通信」を参照してください。

[Main_Menu] > [アプライアンス (Appliance)] ビューから、次のコマンドを実行します。

```
Media PrimaryServer
```

デフォルトのパスワードを変更するため、次のプロンプトが表示されます。

```
- [Info] Default password change is required for the following
user(s): admin, maintenance, sysadmin
```

プロンプトのメッセージに従って、各ユーザーアカウントのパスワードを変更します。

新しいパスワードを設定する前に、次のパスワードポリシーを確認してください。

- パスワードは少なくとも 8 文字にする必要があります。

- パスワードには、少なくとも 1 つの小文字 (a から z) と 1 つの数字 (0 から 9) を含める必要があります。
- 辞書にある言葉は弱いパスワードと見なされて受け入れられません。
- sysadmin (IPMI) ユーザーのパスワードは、20 文字以下にする必要があります。
- 過去 7 回分のパスワードは再利用できません。以前のパスワードに類似する新しいパスワードも使えません。

メモ: 任意のユーザーアカウントに対し、無効なパスワードを 5 回連続で入力すると、アプライアンスは初期構成処理を自動的に中止します。初期構成プロセスを再び開始する必要があります。

メモ: 初期構成の完了後に STIG 機能を有効にすると、ここに入力した新しいパスワードを、STIG パスワードポリシーの要件を満たすように変更することを求められる場合があります。

PrimaryServer は、スタンドアロンのプライマリサーバー、マルチホーム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いずれかになります。それぞれのシナリオについて以下で説明します。

スタンドアロンのプライマリサーバー

この場合、1 つのプライマリサーバーホスト名になります。この名前は、アプライアンスがネットワーク上のプライマリサーバーを認識できる場合は、完全修飾名である必要はありません。コマンドの表示例を次に示します。

```
Media PrimaryServerName
```

マルチホームプライマリサーバー

この場合、プライマリサーバーに複数のホスト名が関連付けられています。ホスト名の区切り文字としてカンマを使用してください。コマンドの表示例を次に示します。

```
Media PrimaryNet1Name,PrimaryNet2Name
```

クラスタ化されたプライマリサーバー

この場合、プライマリサーバーはクラスタ内にあります。ベリタスは、クラスタ名、クラスタのアクティブノード、クラスタのパッシブノードの順で記述することをお勧めします。このリストでは、カンマを使ってノード名を区切ります。コマンドの表示例を次に示します。

```
Media PrimaryClusterName,ActiveNodeName,PassiveNodeName
```

クラスタ化されたマルチホームプライマリサーバー

この場合、プライマリサーバーはクラスタ内にあり、複数のホスト名が関連付けられています。ベリタスは、クラスタ名、クラスタのアクティブノード、クラスタのパッシブノードの順で記述することをお勧めします。このリストでは、カンマを使ってノード名を区切ります。コマンドの表示例を次に示します。

```
Media PrimaryClusterName,ActiveNodeName,
PassiveNodeName,PrimaryNet1Name,PrimaryNet2Name
```

アプライアンスの役割を設定するときに、今後問題が起こらないようにするため、関連付けられているすべてのプライマリサーバー名を指定することをお勧めします。

証明書のプロビジョニング

証明書失効リスト (CRL)

プライマリサーバー名の入力後、アプライアンスは、認証局 (CA) ステータスのプライマリサーバーに ping を実行し、結果を表示します。次の箇条書き項目はそれぞれ、表示される可能性のあるステータス結果を示しています。該当するステータス結果の下に表示される指示に従って、証明書の構成を完了します。

プライマリサーバーに有効な外部 CA が署名した証明書がある場合は、次のように表示されます。

- The primary server *<primary_server_name>* has an enabled External CA-signed certificate. Do you want to import the External CA-signed certificate for this Media server now [yes,no](yes):

  Enter を押して続行します。次のメッセージが表示されます。

  The following shares have been opened on the appliance for you to upload certificate files:

  NFS **共有** <media_server_name>:/inst/share

  CIFS **共有** ¥¥<media_server_name>¥general_share

  外部証明書の構成については、次の詳細を入力します。

  Enter the certificate file path:

  Enter the trust store file path:

  Enter the private key path:

  Enter the password for the passphrase file path or skip security configuration (default: NONE):

  CRL の使用については、次の詳細を入力します。

  Should a CRL be honored for the external certificate?

  1) Use the CRL defined in the certificate.

  2) Use the specific CRL directory.

  3) Do not use a CRL.

  q) Skip security configuration.

  CRL option: 1、2、3、または q と入力します。

  入力した外部 CA の詳細を確認します。

  Certificate file name:

  Trust store file name:

  Private key file name:

  CRL check level: (選択した CRL オプションを表示します)

  Do you want to use the above certificate files? [yes, no](yes):

  入力した情報が正しいことを確認したら、Enter を押して続行し、次のプロンプトに答えます。

  Is this correct? [yes, no](yes):

  すべての情報が正しい場合は、Enter キーを押して続行します。

  アプライアンスは ECA ヘルスチェックを実行し、各検証チェックの結果を表示します。ヘルスチェックが正常に完了すると、次のメッセージが表示されます。

  ECA health check was successful.

The external certificate has been registered successfully.

- The primary server *<primary_server_name>* currently uses an external CA issued certificate and its own internal certificate. Would you like to proceed with the external CA issued certificate? [yes,no](yes):
  [いいえ (no)]を選択すると、次のメッセージが表示されます。
  This appliance will use a NetBackup issued certificate for secure communication.
  [はい (yes)]を選択した場合は、外部証明書の構成について次の詳細を入力します。
  Enter the certificate file path:
  Enter the trust store file path:
  Enter the private key path:
  Enter the password for the passphrase file path or skip security configuration (default: NONE):
  CRL の使用については、次の詳細を入力します。
  Should a CRL be honored for the external certificate?
  1) Use the CRL defined in the certificate.
  2) Use the specific CRL directory.
  3) Do not use a CRL.
  q) Skip security configuration.
  CRL option: 1、2、3、または q と入力します。
  入力した外部 CA の詳細を確認します。
  Certificate file name:
  Trust store file name:
  Private key file name:
  CRL check level: (選択した CRL オプションを表示します)
  Do you want to use the above certificate files? [yes, no](yes):
  入力した情報が正しいことを確認したら、Enter を押して続行し、次のプロンプトに答えます。
  Is this correct? [yes, no](yes):
  すべての情報が正しい場合は、Enter キーを押して続行します。
  アプライアンスは ECA ヘルスチェックを実行し、各検証チェックの結果を表示します。ヘルスチェックが正常に完了すると、次のメッセージが表示されます。
  ECA health check was successful.
  The external certificate has been registered successfully.

- このアプライアンスは、セキュアな通信に外部証明書を使用します。
  プライマリサーバーで外部 CA が署名した証明書が無効になっている場合は、次のように表示されます。
  `The primary server <server_name> has a disabled External CA-signed certificate. Trust the certificate to continue the role configuration process.`
  `Do you trust the certificate? [yes, no], If you select yes, this appliance will continue to do storage configuration. If you select no, the role configuration will be aborted.`
- `This appliance will use a NetBackup issued certificate for secure communication.`
  これ以上の証明書の構成は必要ありません。[次へ (Next)]をクリックして続行します。

セキュリティ証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「NetBackup のセキュリティ証明書」の章を参照してください。

メモ: プライマリサーバーのホスト名が FQDN の場合は、Veritasは FQDN を使用してメディアサーバーのプライマリサーバーを指定することをお勧めします。

メモ: 役割の構成を完了すると、ストレージの初期化が開始します。システムのディスクドライブの数によってはストレージの初期化が完了するまでに最長 46 時間かかることがあります。その結果、アプライアンスのバックアップと復元のパフォーマンスは、ストレージの初期化処理が完了するまで低下します。

---

16 ストレージの初期化処理を開始すると、AdvancedDisk と重複排除 (MSDP) のパーティションについてディスクストレージのプロンプトが表示されます。

ストレージパーティションを構成するには、次を実行する必要があります。

- ストレージプールのサイズを GB または TB 単位で入力します。
  ストレージプールサイズの構成をスキップするパーティションがある場合は、サイズの入力を求められたときに 0 を入力します。ストレージプールを現在のサイズに保持するには、Enter を押します。
- ディスクプール名を入力します。
  デフォルトの名前は、AdvancedDisk の場合は *dp_adv_<hostname>*、重複排除 (MSDP) の場合は *dp_disk_<hostname>* です。デフォルト名を保持するには、Enter を押します。
- ストレージプール名を入力します。
  デフォルトの名前は、AdvancedDisk の場合は *stu_adv_<hostname>*、重複排除 (MSDP) の場合は *stu_disk_<hostname>* です。デフォルト名を保持するには、Enter を押します。

ストレージのプロンプトが次の順序で表示されます。

```
AdvancedDisk partition size in GB/TB: (1 GB)
AdvancedDisk diskpool name:
AdvancedDisk storage unit name:
MSDP partition size in GB/TB: (5 GB)
MSDP diskpool name:
MSDP storage unit name:
MSDP Catalog partition size in GB/TB:
```

ストレージパーティションの構成後、ストレージの構成の概略が次のプロンプトとともに表示されます。

```
Do you want to make changes to the storage configuration
shown above? [yes,no]:
```

変更を実行する場合は yes、現在の構成を保持する場合は no と入力します。

17 高可用性ソリューションの場合は、パートナーノードで初期構成を実行する前に、この構成済みアプライアンス (計算ノード) で高可用性構成を設定する必要があります。高可用性構成を続行して完了するには、次のタスクを記載されている順番どおりに実行します。

p.70 の「NetBackup 53xx の高可用性設定」を参照してください。

p.78 の「NetBackup 53xx 高可用性構成のパートナーノードの初期構成を実行する」を参照してください。

p.85 の「NetBackup 53xx 高可用性構成へのパートナーノードの追加」を参照してください。

18 すべてのアプライアンスが構成され稼働したら、バックアップするクライアントソフトウェアをコンピュータにインストールする準備が完了します。

p.99 の「NetBackup appliance からクライアントへの NetBackup クライアントパッケージのダウンロード」を参照してください。

p.101 の「NFS 共有を介した NetBackup クライアントソフトウェアのインストール 」を参照してください。

19 MSDP クラウドのアプライアンスを構成する場合は、nbasecadmin ユーザーとして NetBackup Web UI にログインし、次のように MSDP クラウドストレージを構成します。

- ディスクプールを作成します。
- ストレージユニットを作成します。
  詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。

NetBackup 53xx の高可用性設定

NetBackup Appliance Web コンソールまたは NetBackup Appliance シェルメニューを使用すると、高可用性 (HA) を設定できます。

メモ: Copilot 機能は、HA 設定を構成すると利用できなくなります。

メモ: NetBackup 5350 Appliance は、HA 設定での使用はサポートされていません。

HA 設定を作成する前に、次の情報を確認します。

- この手順では、最初に構成されるノードのホスト名と IP アドレスが昇格され、HA 設定用の仮想ホスト名と IP アドレスになります。この昇格では、最初のノードに新しいホスト名と新しい IP アドレスを割り当てる必要があります。HA 設定を作成する前に、まず関連付けられているプライマリサーバーの[ホスト名マッピング (Host Name Mappings)]プロパティに新しいホスト名を追加する必要があります。
- 適切な CA 証明書を最初のノードに再配備します。
  最初のノードのホスト名と IP アドレスを変更した後、必要な CA 証明書をノードに再配備する必要があります。この手順には、これらの証明書を配備するために必要な情報が含まれています。

  メモ: HA 設定中の外部 CA 配備は、NetBackup Appliance シェルメニューを介してのみサポートされます。

- NetBackup クライアントを使用して NetBackup ジョブを管理する場合、クライアントの `bp.conf` ファイルに次の情報を追加します。
  - HA 設定の仮想ホスト名
  - 最初のノードのホスト名
  - パートナーノードのホスト名
- 最初のノードの eth2 ポートと eth3 ポートでネットワークが結合されている場合は、この結合を削除します。

注意: HA 設定が完了すると、出荷時の設定にリセットするまでノードのホスト名を変更できません。

メモ: HA 用の既存の 53xx Appliance を変換している場合、HA 設定の構成が失敗し、次のエラーメッセージが報告されることがあります: [エラー] V-409-955-4011: MSDP ディスクサービスの作成に失敗しました。テクニカルノート 000127738 を参照してください。この問題が発生した場合、テクニカルノート 000127738 は参照しないでください。これは、新しい 53xx Appliance で発生した HA 設定の障害にのみ適用されるためです。代わりに、ベリタスのサポートに連絡し、担当者に 100044266 を参照するよう連絡して問題の解決に役立ててください。

NetBackup Appliance Web コンソールから HA を設定するには

メモ: 外部 CA 証明書を配備する必要がある場合は、次の手順に記載されているとおり、NetBackup Appliance シェルメニューから HA 設定を構成する必要があります。

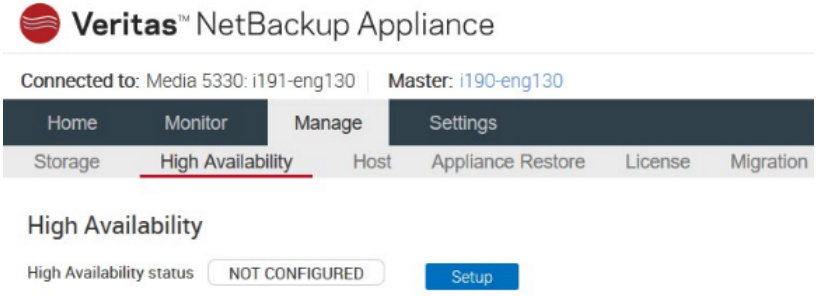
1. 関連付けられているプライマリサーバーで NetBackup 管理コンソールにログインし、[ホスト名マッピング (Host Name Mappings)]プロパティに、1 台目の構成済みノードの新しいホスト名を追加します。短縮名と完全修飾ドメイン名 (FQDN) の両方を追加する必要があります。

   詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「ホスト ID からホスト名へのマッピング」セクションを参照してください。

2. 最初の構成済みノードで、`admin` として NetBackup Appliance Web コンソールにログオンします。

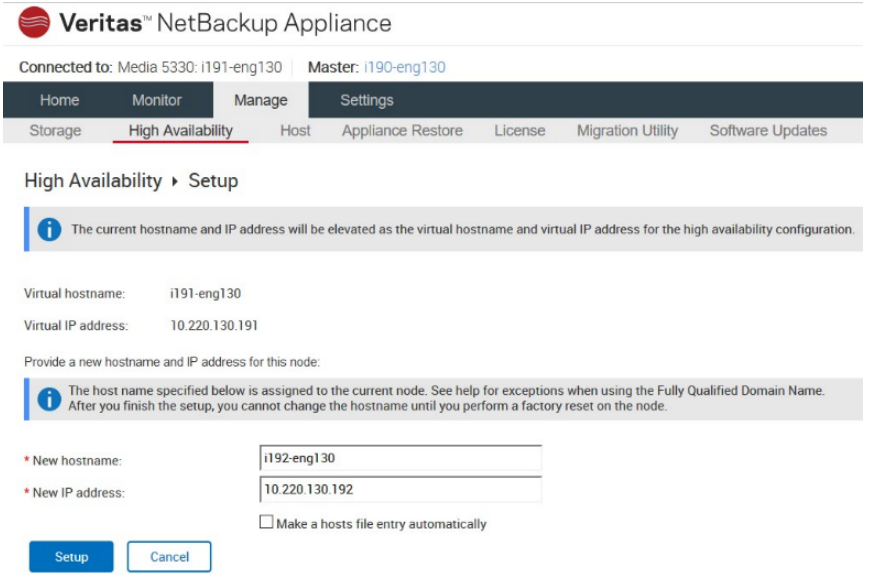
3. [Veritas NetBackup Appliance Web コンソールへようこそ (Welcome to Veritas NetBackup Appliance Web Console)]ページで、[管理 (Manage)]、[高可用性 (High Availability)]をクリックします。

4. [高可用性 (High Availability)]ページで、[設定 (Setup)]をクリックします。

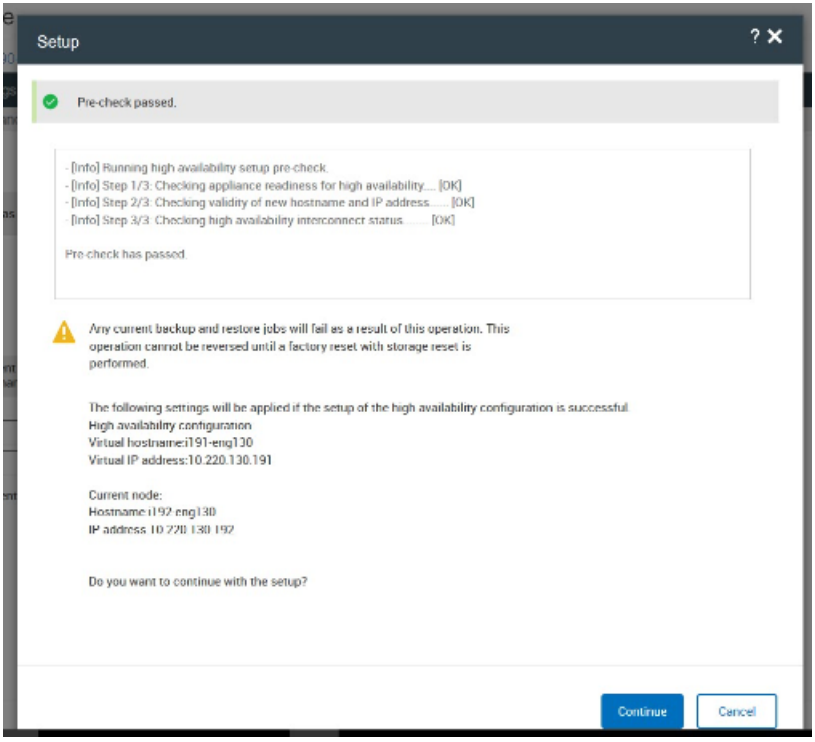


5. [高可用性 (High Availability)]、[設定 (Setup)]ページで、次の操作を実行します。

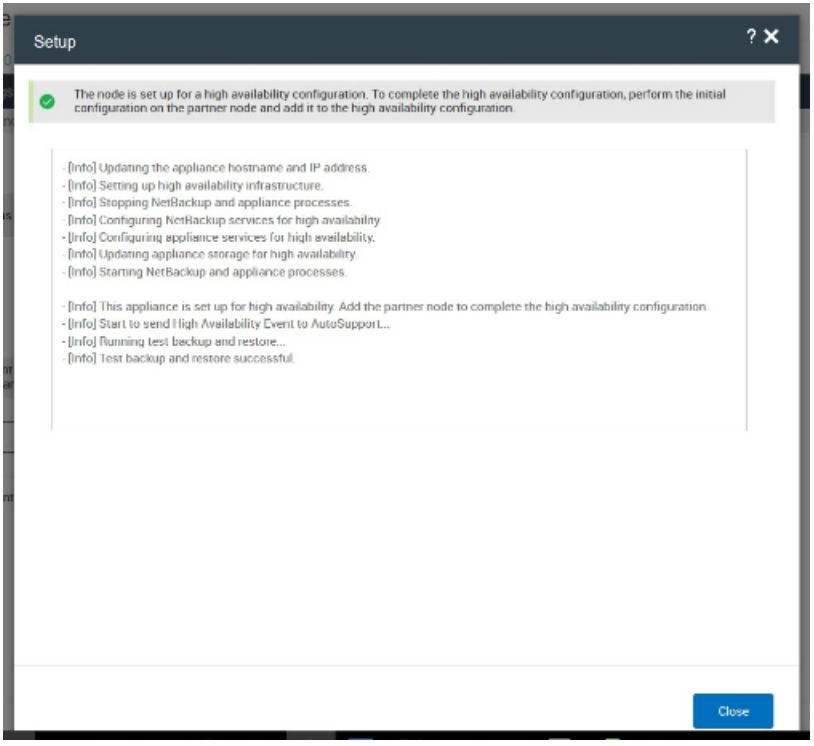
- このノードの新しいホスト名を入力します。
- このノードの新しい IP アドレスを入力します。
- 新しいホスト名と IP アドレスを /etc/hosts ファイルに追加するには、[hosts ファイルエントリを自動作成 (Make a hosts file entry automatically)]チェックボックスにチェックマークを付けます。
- [設定 (Setup)]をクリックします。



6 [設定 (Setup)]ウィンドウで事前チェックがパスしたことを示すメッセージが表示されたら、[続行 (Continue)]をクリックします。



7 [設定 (Setup)]ウィンドウが更新され、ノードが HA 用に設定されていることを示すメッセージが表示されたら、[閉じる (Close)]をクリックします。



8 ホスト名と IP アドレスを変更した後、このノードとプライマリサーバーで NetBackup サービスを再起動し、その変更と HA 設定が認識されることを確認します。

NetBackup Appliance シェルメニューを使用して NetBackup 53xx HA 構成を設定するには

1 関連付けられているプライマリサーバーで NetBackup 管理コンソールにログインし、[ホスト名マッピング (Host Name Mappings)]プロパティに、1 台目の構成済みノードの新しいホスト名を追加します。短縮名と完全修飾ドメイン名 (FQDN) の両方を追加する必要があります。

詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「ホスト ID からホスト名へのマッピング」セクションを参照してください。

2 最初の構成済みノードで、`admin` として NetBackup Appliance シェルメニューにログオンします。

3 `Main > Manage > HighAvailability` に進みます。

4 次のコマンドを使用して構成済みノードに新しいホスト名と IP アドレスを割り当てます。

```
Setup NewHostnameNewIPAddress
```

NewHostname はノードの新しいホスト名、*NewIPAddress* はノードの新しい IP アドレスを示します。

5 最初のノードのホスト名と IP アドレスを変更した後、必要な CA 証明書を再配備する必要があります。

アプライアンスは、認証局 (CA) ステータスのプライマリに ping を実行し、結果を表示します。次の箇条書き項目はそれぞれ、表示される可能性のあるステータス結果を示しています。該当するステータス結果の下に表示される指示に従って、証明書の構成を完了します。

- The primary server <*primary_server_name*> currently uses an External CA-signed certificate. You are required to configure this appliance with a certificate issued by the same external CA. Do you want to import the External CA-signed certificate for this Media server now [yes,no](yes):

  Enter を押して続行します。次のメッセージが表示されます。

  To configure the HA setup, the External CA-signed certificate must include the vip hostname and FQDN DNS information in the Subject Alternative Name.

  The following shares have been opened on the appliance for you to upload certificate files:

  NFS **共有** <media_server_name>:/inst/share

  CIFS **共有** ¥¥<media_server_name>¥general_share

  外部証明書の構成については、次の詳細を入力します。

  Enter the certificate file path:

  Enter the trust store file path:

  Enter the private key path:

  Enter the password for the passphrase file path or skip security configuration (default: NONE):

  CRL の使用については、次の詳細を入力します。

  Should a CRL be honored for the external certificate?

  1) Use the CRL defined in the certificate.

  2) Use the specific CRL directory.

  3) Do not use a CRL.

  q) Skip security configuration.

  CRL option: 1、2、3、または q と入力します。

  Verify the External CA details that you entered:

Certificate file name:

Trust store file name:

Private key file name:

CRL check level: (選択した CRL オプションを表示します)

Do you want to use the above certificate files? [yes, no](yes):

入力した情報が正しいことを確認したら、Enter を押して続行し、次のプロンプトに答えます。

Is this correct? [yes, no](yes):

すべての情報が正しい場合は、Enter キーを押して続行します。

アプライアンスは ECA ヘルスチェックを実行し、各検証チェックの結果を表示します。ヘルスチェックが正常に完了すると、次のメッセージが表示されます。

ECA health check was successful.

The external certificate has been registered successfully.

- The primary server *<primary_server_name>* currently uses an external CA issued certificate and its own internal certificate. Would you like to proceed with the external CA issued certificate? [yes,no](yes):

  [いいえ (no)]を選択すると、次のメッセージが表示されます。

  This appliance will use a NetBackup issued certificate for secure communication.

  [はい (yes)]を選択すると、次のメッセージが表示されます。

  To configure the HA setup, the External CA-signed certificate must include the vip hostname and FQDN DNS information in the Subject Alternative Name.

  The following shares have been opened on the appliance for you to upload certificate files:

  NFS **共有** <media_server_name>:/inst/share

  CIFS **共有** ¥¥<media_server_name>¥general_share

  外部証明書の構成については、次の詳細を入力します。

  Enter the certificate file path:

  Enter the trust store file path:

  Enter the private key path:

  Enter the password for the passphrase file path or skip security configuration (default: NONE):

  CRL の使用については、次の詳細を入力します。

  Should a CRL be honored for the external certificate?

  1) Use the CRL defined in the certificate.

  2) Use the specific CRL directory.

  3) Do not use a CRL.

```
q) Skip security configuration.
```

CRL option: 1、2、3、または q と入力します。

入力した外部 CA の詳細を確認します。

```
Certificate file name:
Trust store file name:
Private key file name:
CRL check level: (選択した CRL オプションを表示します)
Do you want to use the above certificate files? [yes, no](yes):
```

入力した情報が正しいことを確認したら、Enter を押して続行し、次のプロンプトに答えます。

```
Is this correct? [yes, no](yes):
```

すべての情報が正しい場合は、Enter キーを押して続行します。

アプライアンスは ECA ヘルスチェックを実行し、各検証チェックの結果を表示します。ヘルスチェックが正常に完了すると、次のメッセージが表示されます。

```
ECA health check was successful.
The external certificate has been registered successfully.
```

- `This appliance will use a NetBackup issued certificate for secure communication.`

  これ以上の証明書の構成は必要ありません。[次へ (Next)]をクリックして続行します。

6 ホスト名と IP アドレスを変更した後、このノードとプライマリサーバーで NetBackup サービスを再起動し、その変更と HA 設定が認識されることを確認します。

ノードを設定すると、ノードの新しいネットワーク情報がプライマリサーバー上の追加サーバーリストに自動的に追加されます。

次の手順

HA 設定を完了するには、次の手順を記載されている順番どおりに実行します。

- パートナーノードで初期構成を実行します。
  p.78 の「NetBackup 53xx 高可用性構成のパートナーノードの初期構成を実行する」を参照してください。
- NetBackup 管理コンソールで、高可用性構成にパートナーノードを追加して HA 設定のすべてのホスト名マッピングを承認します。
  p.85 の「NetBackup 53xx 高可用性構成へのパートナーノードの追加」を参照してください。
  すべてのホスト名マッピングを承認する必要があります。承認されないと、切り替え後に MSDP サービスがオンラインになりません。参照の手順には、ホスト名マッピングの承認方法を説明した手順が含まれています。

ホスト名マッピングについて詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「ホスト ID からホスト名へのマッピング」セクションを参照してください。

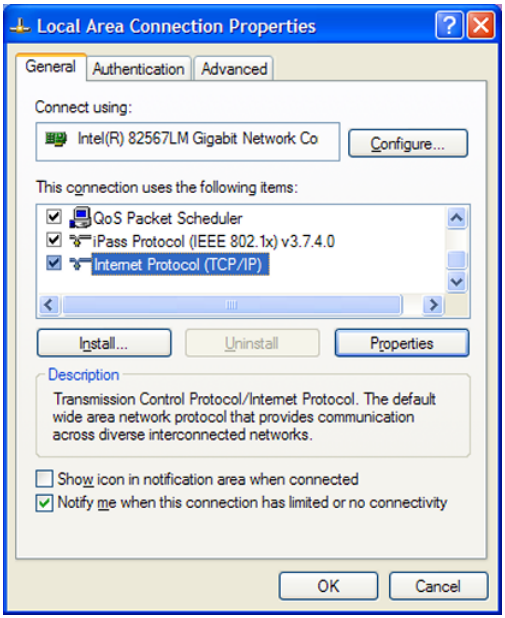
NetBackup 53xx 高可用性構成のパートナーノードの初期構成を実行する

パートナーノードは、高可用性 (HA) 構成で使用するもう一つの 53xx 計算ノードです。構成する必要があるのは、パートナーノードのネットワーク設定およびタイムゾーン情報のみです。

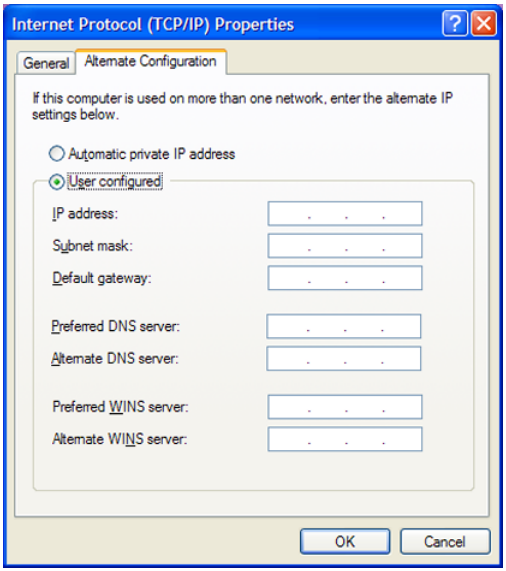
パートナーノードを構成するには

1 パートナーノードの NIC1 ポートにノートパソコンを接続します。次に、[ローカルエリアの接続プロパティ]ダイアログボックスに移動します。

[全般 (General)]タブで、[インターネットプロトコル (TCP/IP) (Internet Protocol (TCP/IP))]を選択してハイライト表示し、[プロパティ (Properties)]をクリックします。



[代替の構成 (Alternate Configuration)]タブで、次のタスクを実行します。



- ［ユーザー構成 (User Configured)］をクリックします。
- ［IP アドレス (IP address)］に、192.168.229.nnn と入力します。nnn は 2 から 254 (233 を除く) の任意の数字です。
- ［サブネットマスク (Subnet mask)］に 255.255.255.0 と入力して［OK］をクリックします。

2 パートナーノードに接続しているノートパソコンで、SSH セッションを 192.168.229.233 に開きます。

3 次のようにデフォルトのクレデンシャルでパートナーノードにログオンします。

- ［ユーザー名 (User Name)］: admin
- ［パスワード (Password)］: P@ssw0rd

ようこそメッセージがシェルメニューに表示され、［Main_Menu］ビューにプロンプトが表示されます。

メモ: 初期構成の続行には、デフォルトパスワードの変更は必須ではありません。ただし、環境のセキュリティを高めるためにパスワードを定期的に変更することをお勧めします。現在のパスワードの記録は安全な場所に保管するように徹底してください。NetBackup Appliance シェルメニューにログインしているときにパスワードを変更するには、Main_Menu ビューで `Settings > Password` と入力します。

---

4 初めて設定する前に次のコマンドを入力して、接続したハードウェアコンポーネントの状態を調べて確認します。

```
Support > Test Hardware
```

[警告 (Warning)]は後で解決できる問題を示します。この場合は、初期構成を続行できます。ただし、このような問題により、影響を受けるデバイスにアクセスできなくなります。

[エラー (Error)]は、初期構成を続行する前にすぐに解決する必要のある重要な問題を示します。

コマンド出力で問題を認識した場合には、以下の項目を調べます。

- すべてのケーブルが正しく接続され、固定されていることを確認します。
- すべてのディスクドライブが正しく設置され、固定されていることを確認します。
- すべてのユニットが電源オンであり、完全に起動していることを確認します。
- ハードウェアチェックリストの項目をすべてチェック済みであることを確認します。
- 以前の項目を検証した後、コマンドを再実行します。警告アイコンまたはエラーアイコンが表示されなくなった場合は、問題が解決したことを示します。初期構成を開始する前にすべての問題を解決することをお勧めします。

メモ: 上記の項目すべてを検証してコマンドを再実行しても[エラー (Error)]の問題を解決できない場合は、そこで作業を中止してベリタスのテクニカルサポートに問い合わせてください。

---

5 Main_Menu > Network ビューで次のコマンドを入力して、パートナーノードが接続する単一ネットワークの IP アドレスを設定します。

```
Configure IPAddressNetmaskGatewayIPAddress[[InterfaceName]]
```

ここで、*IPAddress* は新しい IP アドレス、*Netmask* はネットマスク、*GatewayIPAddress* はインターフェースのデフォルトゲートウェイです。[[InterfaceName]] オプションは省略可能です。

IPAddress または *GatewayIPAddress* には IPv4 または IPv6 アドレスを指定できます。グローバルスコープと一意的ローカルの IPv6 アドレスのみが許可されます。

ただし、同じコマンド内で IPv4 と IPv6 アドレスの両方は使わないでください。たとえば、`Configure 9ffe::9 255.255.255.0 1.1.1.1.` は使用できません。`Configure 9ffe::46 64 9ffe::49 eth1` を使用する必要があります。

p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。

複数のネットワークを構成する場合には、追加する各ネットワークの IP アドレスを最初に構成する必要があります。次に、追加した各ネットワークのゲートウェイアドレスを構成します。必ずデフォルトゲートウェイアドレスを最初に追加する必要があります。以下の 2 つのコマンドを使います。

各ネットワークの IP アドレスの構成	ネットワークインターフェースに対して IPv4 または IPv6 アドレスのどちらを構成するかに応じて、以下のコマンドのいずれかを使います。 ネットワークインターフェースの IPv4 アドレスを構成するには `IPv4 IPAddressNetmask [InterfaceName]` ここで、*IPAddress* は新しい IP アドレス、*Netmask* はネットマスクです。`[InterfaceName]` は省略可能です。追加する IP アドレスごとにこのコマンドを繰り返します。 ネットワークインターフェースの IPv6 アドレスを構成するには IPv6 <*IP Address*> <Prefix> [InterfaceNames] ここで、*IPAddress* は IPv6 アドレス、*Prefix* はプレフィックス長です。`[InterfaceName]` は省略可能です。

追加した各ネットワークのゲートウェイアドレスの構成	`Gateway Add GatewayIPAddress [TargetNetworkIPAddress] [Netmask] [InterfaceName]` ここで、*GatewayIPAddress* はインターフェースのゲートウェイです。*TargetNetworkIPAddress*、*Netmask*、`InterfaceName` は省略可能です。このコマンドを繰り返して、すべての宛先ネットワークにゲートウェイを追加します。 *Gateway IP Address* や *TargetNetworkIPAddress* には、IPv4 または IPv6 アドレスを指定できます。 ただし、同じコマンド内で IPv4 と IPv6 アドレスの両方は使わないでください。たとえば、`Gateway Add 9ffe::3 255.255.255.0 eth1` は使用できません。`Gateway Add 6ffe::3 6ffe:: 64 eth1` を使用する必要があります。

6 Main_Menu > Network ビューで次のコマンドを入力して、パートナーノードの DNS を設定します。

メモ: DNS を使わない場合は、ステップ 9 に進んでください。

```
DNS Domain Name
```

ここで、*Name* はパートナーノードのドメイン名です。

7 Main_Menu > Network ビューで次のコマンドを入力して、パートナーノードの構成に DNS ネームサーバーを追加します。

```
DNS Add NameServer IPAddress
```

ここで、*IPAddress* は DNS サーバーの IP アドレスです。

アドレスは IPv4 または IPv6 のいずれかになります。グローバルスコープと一意的ローカルの IPv6 アドレスのみが許可されます。

p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。

複数の IP アドレスを追加するには、スペースを空けずに各アドレスをカンマで区切ります。

8 Main_Menu > Network ビューで次のコマンドを使って、DNS 検索ドメインをパートナーノード構成に追加し、異なるドメインにあるホスト名をパートナーノードが解決できるようにします。

```
DNS Add SearchDomain SearchDomain
```

ここで、*SearchDomain* は検索用に追加する対象ドメインです。

9 この手順は省略可能です。hosts ファイルに他のホストの IP アドレスを追加する場合のみ続行します。それ以外の場合は、次の手順にスキップします。

Main_Menu > Network ビューで次のコマンドを入力して、ホストエントリをパートナーノードの hosts ファイルに追加します。

```
Hosts Add IPAddressFQHNShortName
```

ここで、*IPAddress* は IPv4 または IPv6 アドレス、*FQHN* は完全修飾ホスト名、*ShortName* は短いホスト名です。

p.13 の「IPv4-IPv6 ベースのネットワークサポートについて」を参照してください。

10 Main_Menu > Network ビューで次のコマンドを入力して、パートナーノードのホスト名を設定します。

```
Hostname Set Name
```

ここで、*Name* はパートナーノードの短いホスト名または完全修飾ドメイン名 (FQDN) です。

一部の例外を除き、ホスト名は構成全体に適用されます。短縮名は次の場所に常に表示されます。

- NetBackup Appliance シェルメニュープロンプト
- 重複排除プールカタログのバックアップポリシー
- デフォルトのストレージユニットおよびディスクプール名

このノードが出荷時の設定にリセットされていて、以前のバックアップイメージのいずれかをインポートする場合は、ノードのホスト名が次のルールのいずれかを満たしている必要があります。

- ホスト名は出荷時の設定へのリセット前に使われるものとまったく同じである必要があります。
- FQDN にホスト名を変更する場合は、出荷時の設定へのリセットの前に使われた短い名前を含んでいる必要があります。たとえば、「myhost」が出荷時の設定へのリセットの前に使われた場合は、新しい FQDN として「myhost.domainname.com」を使います。
- 短いホスト名にホスト名を変更する場合は、出荷時の設定へのリセットの前に使われた FQDN から得られる名前にする必要があります。たとえば、「myhost.domainname.com」が出荷時の設定へのリセットの前に使われた場合は、新しい短いホスト名として「myhost」を使います。

メモ: ホスト名は初期構成セッションの間のみ設定することができます。初期構成が正常に完了した後、パートナーノードで出荷時の設定にリセットすると初期構成を再入力できます。詳しくは、『NetBackup appliance 管理者ガイド』を参照してください。

このステップにより、NetBackup は新しいホスト名で動作するように再構成されます。この処理は、完了するまでにしばらく時間がかかることがあります。

`Hostname set` コマンドが機能するためには、少なくとも 1 つの IPv4 アドレスが必要です。たとえば、特定のホストのホスト名を v46 に設定するとします。そのためには、まず、その特定のホストが少なくとも 1 つの IPv4 アドレスを持つことを確認した後、次のコマンドを実行します。

```
Main_Menu > Network > Hostname set v46
```

11 Main_Menu > Network ビューで次のコマンドを使って、このパートナーノードのタイムゾーン、日付、および時間を設定します。

- 次のコマンドを入力して、タイムゾーンを設定します。

  ```
  TimeZone Set
  ```

  表示されたリストから該当するタイムゾーンを選択します。

- 次のコマンドを入力して、日付と時刻を設定します。

  ```
  Date Set MonthDayHHMMSSYear
  ```

  ここで、*Month* は月の名前です。
  Day は 0 から 31 までの日付です。
  HHMMSS は 24 時間形式の時、分、秒です。フィールドはセミコロンで区切ります (HH:MM:SS)。
  Year は、1970 から 2037 までの暦年です。

Veritas HA 構成の既存のノードと同じ日付と時刻を設定することを推奨します。

12 両方のノードが適切に通信し、ストレージアレイを検出できるように、パートナーノードを HA 構成に追加する前に次のタスクを実行してください。

- 次のコマンドを実行して、パートナーノードを再ブートします。

  ```
  Support > Reboot
  ```

- 最初の構成済みの計算ノードで次のコマンドを実行し、完了するまで待機します。

  ```
  Manage > Storage > Scan
  ```

- パートナーノードで次のコマンドを実行し、完了するまで待機します。

  ```
  Manage > Storage > Scan
  ```

13 HA 設定にパートナーノードを追加します。

p.85 の「NetBackup 53xx 高可用性構成へのパートナーノードの追加」を参照してください。

NetBackup 53xx 高可用性構成へのパートナーノードの追加

パートナーノードを構成したら、この手順を使用して、次のように HA 設定を完了します。

- HA 設定にパートナーノードを追加する
  NetBackup Appliance Web コンソールまたは NetBackup Appliance シェルメニューを使用してパートナーノードを追加します。
- ホスト名マッピングを承認する
  リリース 3.1.2 以降では、HA 設定を完了するため、関連付けられているプライマリサーバーの NetBackup 管理コンソールで、すべてのホスト名マッピングを承認する必要があります。マッピングが承認されないと、切り替え後に MSDP サービスがオンラインになりません。各手順の最後の手順では、マッピングを承認する方法について説明します。
- 適切な CA 証明書をパートナーノードに配備します。
  NetBackup Appliance リリース 3.2 では、外部認証局証明書のサポートを導入しました。この機能は、ホストの検証とセキュリティのために NetBackup 認証局を使用する代替手段を提供します。この手順には、これらの証明書を配備するために必要な情報が含まれています。セキュリティ証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「NetBackup の外部 CA サポート」の章を参照してください。

  メモ: パートナーノードでの外部 CA 配備は、NetBackup Appliance シェルメニューを介してのみサポートされます。

- リリース 4.0 以降では、admin、maintenance、sysadmin (IPMI) ユーザーアカウントのデフォルトのパスワードを変更する必要があります。この手順を実行する前に、パートナーノードでこれらのユーザーアカウントのパスワードが変更されていない場合、手順を示すメッセージが表示されます。

パートナーノードを追加すると、パートナーノードのネットワーク情報がプライマリサーバー上の追加サーバーリストに自動的に追加されます。HA 設定の各ノードのファームウェアと共有プライマリストレージシェルフは、同じ資産タグで自動的に接続されます。

警告: HA 設定が完了したら、2 台のノードの時刻と日付の設定は変更しないでください。

NetBackup プロセスが実行中であることの確認

パートナーノードを追加してアプライアンスの HA 設定を完了する前に、まずすべての NetBackup プロセスがプライマリサーバーと両方の HA ノードで実行されていることを確認する必要があります。

- プライマリサーバー
  プライマリサーバーがアプライアンスの場合は、アプライアンスのシェルメニューにログインし、次のコマンドを入力します。
  `Support > Processes > NetBackup Show`
  プライマリサーバーがアプライアンスでない場合は、NetBackup のコマンドラインにログインし、次のコマンドを入力します。
  `/usr/openv/netbackup/bin/goodies/netbackup show`
- メディアサーバーノード
  計算ノードと追加するパートナーノードで、アプライアンスのシェルメニューにログインし、次のコマンドを入力します。
  `Support > Processes > NetBackup Show`

プライマリサーバーまたはノードでプロセスが実行されていない場合、パートナーノードを追加できません。このエラーを防ぐには、すべての NetBackup プロセスを停止してから、次の手順で再起動する必要があります。

- NetBackup プロセスの停止
  プライマリサーバーアプライアンスと両方のアプライアンスノードで、次のコマンドを入力します。
  `Support > Processes > NetBackup Stop`
  プライマリサーバーがアプライアンスではない場合は、次のコマンドを入力します。
  `/usr/openv/netbackup/bin/goodies/netbackup stop`
  すべてのプロセスが停止したことを確認するために、次のコマンドを入力します。
  `/usr/openv/netbackup/bin/bpps -x`
  まだ実行中のプロセス (`nbftsrvr/nbfdrv64` を除く) がある場合は、stop コマンドを再入力します。
  `/usr/openv/netbackup/bin/goodies/netbackup stop`
  `nbftsrvr/nbfdrv64` プロセスを停止するには、次のコマンドを入力します。
  `/usr/openv/netbackup/bin/goodies/nbftserver stop`

  メモ: このプロセスはすぐには停止しない場合があります。コマンドの結果にプロセスが停止したと表示されるまで待機してください。

- NetBackup プロセスの再起動
  プライマリサーバーアプライアンスと両方のアプライアンスノードで、次のコマンドを入力します。
  `Support > Processes > NetBackup Start`
  プライマリサーバーがアプライアンスでない場合は、次のコマンドをこの順番で入力します。
  `/usr/openv/netbackup/bin/goodies/netbackup start`

```
/usr/openv/netbackup/bin/goodies/nbftserver start
```

パートナーノードの追加

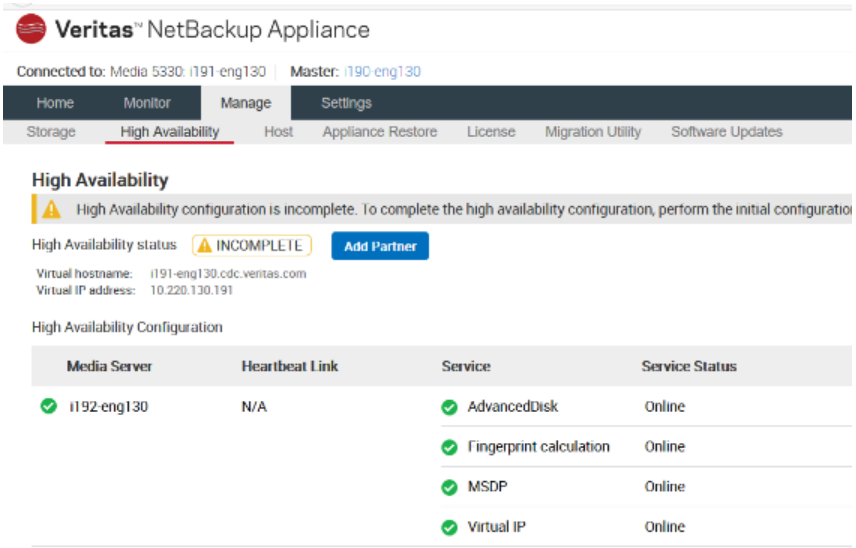
次のいずれかの手順を使用して、パートナーノードを HA 設定に追加します。

NetBackup Appliance Web コンソールを使用してパートナーノードを追加するには

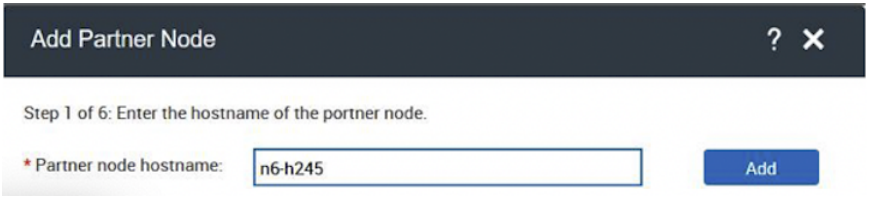
メモ: 外部 CA 証明書を配備する必要がある場合は、次の手順に記載されているとおり、NetBackup Appliance シェルメニューからパートナーノードを追加する必要があります。

---

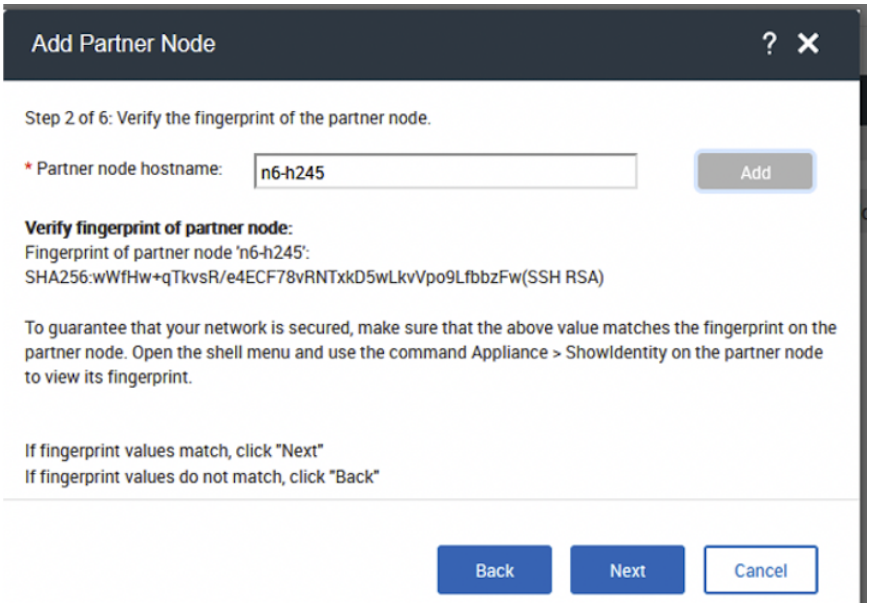
1. HA 構成の設定に使用したノードで、NetBackup Appliance Web コンソールに `admin` としてログオンします。
2. [Veritas NetBackup Appliance Web コンソールへようこそ (Welcome to Veritas NetBackup Appliance Web Console)]ページで、[管理 (Manage)]、[高可用性 (High Availability)]をクリックします。
3. [高可用性 (High Availability)]ページで、HA 構成の現在の状態が未完了と識別されます。[パートナーの追加 (Add Partner)]をクリックします。



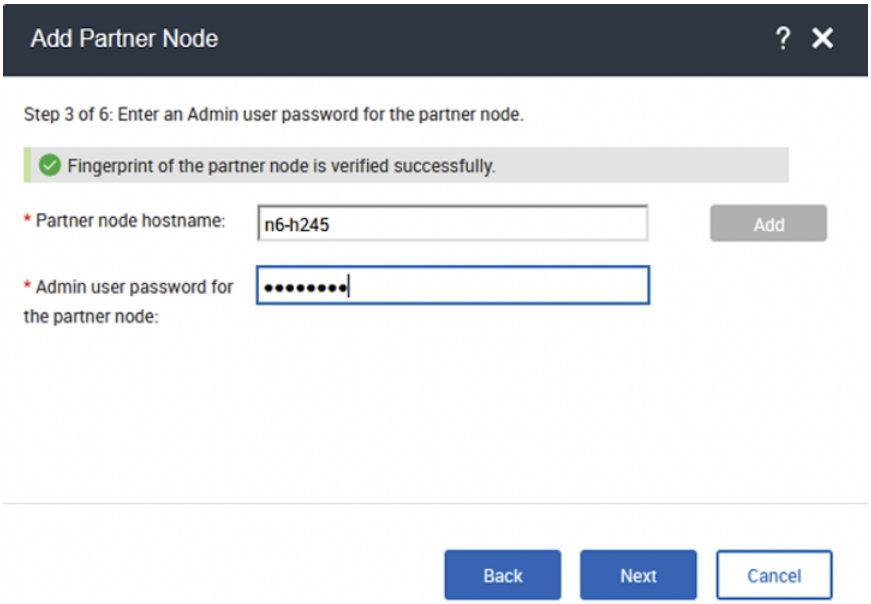
4 [パートナーノードの追加 (Add Partner Node)]ダイアログボックスで、パートナーノードの構成済みのホスト名を入力し、[追加 (Add)]をクリックします。



5 指紋値が一致した場合は、[次へ (Next)]をクリックします。

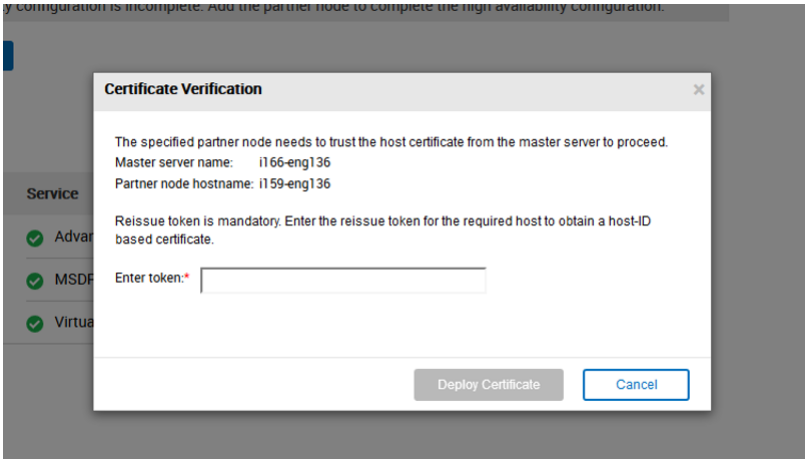


6 パートナーノードの admin ユーザーのパスワードを入力し、[次へ (Next)]をクリックします。「続行しますか? (Do you want to continue?)」というメッセージが表示されたら、[続行 (Continue)]をクリックします。



7 追加するパートナーノードに依然として admin、maintenance、sysadmin (IPMI) ユーザーアカウントのデフォルトのパスワードが含まれている場合は、パスワードの変更を求めるメッセージに従います。

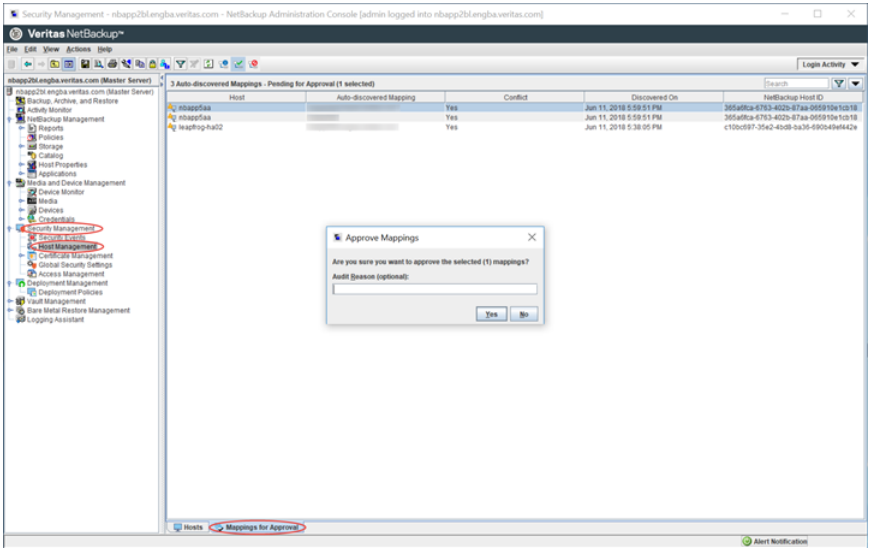
8 [証明書の検証 (Certificate Verification)]ダイアログボックスが表示される場合、認証トークンまたは再発行トークンを入力し、[証明書の配備 (Deploy Certificate)]をクリックします。



9 プロセスが成功したことを示すメッセージが表示されたら、[閉じる (Close)]をクリックします。

10 HA 設定を完了するため、関連付けられているプライマリサーバーでホスト名マッピングを承認する必要があります。

- 関連付けられているプライマリサーバーで、NetBackup 管理コンソールにログインします。
- 左ペインで[セキュリティ管理 (Security Management)]をクリックしてプロパティを展開し、[ホスト管理 (Host Management)]をクリックします。
- 右ペインの左下で、[承認のマッピング (Mappings for Approval)]をクリックします。
- 右ペインの上部で、承認が保留状態となっている任意のホストマッピングをクリックします。承認を求める[マッピングの承認 (Approve Mappings)]ダイアログボックスが表示されたら、[はい (Yes)]をクリックします。承認が保留状態となっている各ホストマッピングについて、このタスクを繰り返します。



NetBackup Appliance シェルメニューを使用してパートナーノードを追加するには

1. HA 構成を設定するノードで、NetBackup Appliance シェルメニューに `admin` としてログオンします。
2. `Main > Manage > HighAvailability` に進みます。
3. パートナーノードを追加してから、次のコマンドを入力して HA 構成を完了します。

   `AddNode` *`hostname`*

   hostname は、パートナーノードの短いホスト名または完全修飾ドメイン名 (FQDN) です。
4. 次のメッセージが表示されたら、パートナーノードで直接 SSH ECDSA 指紋をチェックしたことを確認します。

   `Do the fingerprint values match? [yes, no] (no)`

   ネットワークが安全であることを保証するには、パートナーノードの SSH ECDSA 指紋が正しいことを確認する必要があります。アプライアンスの ID を確認する方法については、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

   値が一致した場合、yes と入力します。
5. 追加するパートナーノードに依然として admin、maintenance、sysadmin (IPMI) ユーザーアカウントのデフォルトのパスワードが含まれている場合は、パスワードの変更を求めるメッセージに従います。

6 事前チェックが成功した後に、次のメッセージのいずれかが表示されたら、認証トークンまたは再発行トークンを入力して、ホスト ID ベースの証明書を信頼します。

```
Authorization token is mandatory. Enter an authorization token.
For more information about the authorization token, refer to the
NetBackup Security and Encryption Guide.

Enter token:
```

または

```
Reissue token is mandatory. Enter the reissue token for the
required host to obtain a host-ID based certificate. For more
information about the reissue token, refer to the NetBackup
Security and Encryption Guide.

Enter token:
```

セキュリティ証明書について詳しくは、『NetBackup セキュリティおよび暗号化ガイド』の「NetBackup のセキュリティ証明書」の章を参照してください。

7 次のメッセージが表示されたら、yes と入力して続行します。

```
>> Do you want to continue? [yes, no] (no)
```

アプライアンスは、認証局 (CA) ステータスのプライマリに ping を実行し、結果を表示します。次の箇条書き項目はそれぞれ、表示される可能性のあるステータス結果を示しています。該当するステータス結果の下に表示される指示に従って、証明書の構成を完了します。

- The primary server *<primary_server_name>* currently uses an External CA-signed certificate. You are required to configure this appliance with a certificate issued by the same external CA. Do you want to import the External CA-signed certificate for this Media server now [yes,no](yes):
  Enter を押して続行します。次のメッセージが表示されます。
  To configure the HA partner node, the External CA-signed certificate must include the vip hostname and FQDN DNS information in the Subject Alternative Name.
  The following shares have been opened on the appliance for you to upload certificate files:
  NFS **共有** <media_server_name>:/inst/share
  CIFS **共有** ¥¥<media_server_name>¥general_share
  外部証明書の構成については、次の詳細を入力します。
  Enter the certificate file path:
  Enter the trust store file path:
  Enter the private key path:

Enter the password for the passphrase file path or skip security configuration (default: NONE):

CRL の使用については、次の詳細を入力します。

Should a CRL be honored for the external certificate?

1) Use the CRL defined in the certificate.

2) Use the specific CRL directory.

3) Do not use a CRL.

q) Skip security configuration.

CRL option: 1、2、3、または q と入力します。

Verify the External CA details that you entered:

Certificate file name:

Trust store file name:

Private key file name:

CRL check level: (選択した CRL オプションを表示します)

Do you want to use the above certificate files? [yes, no](yes):

入力した情報が正しいことを確認したら、Enter を押して続行し、次のプロンプトに答えます。

Is this correct? [yes, no](yes):

すべての情報が正しい場合は、Enter キーを押して続行します。

アプライアンスは ECA ヘルスチェックを実行し、各検証チェックの結果を表示します。ヘルスチェックが正常に完了すると、次のメッセージが表示されます。

ECA health check was successful.

The external certificate has been registered successfully.

- The primary server *<primary_server_name>* currently uses an external CA issued certificate and its own internal certificate. Would you like to proceed with the external CA issued certificate? [yes,no](yes):

  [いいえ (no)]を選択すると、次のメッセージが表示されます。

  This appliance will use a NetBackup issued certificate for secure communication.

  [はい (yes)]を選択すると、次のメッセージが表示されます。

  To configure the HA partner node, the External CA-signed certificate must include the vip hostname and FQDN DNS information in the Subject Alternative Name.

  The following shares have been opened on the appliance for you to upload certificate files:

  NFS **共有** <media_server_name>:/inst/share

  CIFS **共有** ¥¥<media_server_name>¥general_share

  外部証明書の構成については、次の詳細を入力します。

```
Enter the certificate file path:
Enter the trust store file path:
Enter the private key path:
Enter the password for the passphrase file path or skip
security configuration (default: NONE):
```

CRL の使用については、次の詳細を入力します。

```
Should a CRL be honored for the external certificate?
1) Use the CRL defined in the certificate.
2) Use the specific CRL directory.
3) Do not use a CRL.
q) Skip security configuration.
CRL option: 1、2、3、または q と入力します。
```

入力した外部 CA の詳細を確認します。

```
Certificate file name:
Trust store file name:
Private key file name:
CRL check level: (選択した CRL オプションを表示します)
Do you want to use the above certificate files? [yes, no](yes):
```

入力した情報が正しいことを確認したら、Enter を押して続行し、次のプロンプトに答えます。

```
Is this correct? [yes, no](yes):
```

すべての情報が正しい場合は、Enter キーを押して続行します。
アプライアンスは ECA ヘルスチェックを実行し、各検証チェックの結果を表示します。ヘルスチェックが正常に完了すると、次のメッセージが表示されます。

```
ECA health check was successful.
The external certificate has been registered successfully.
```

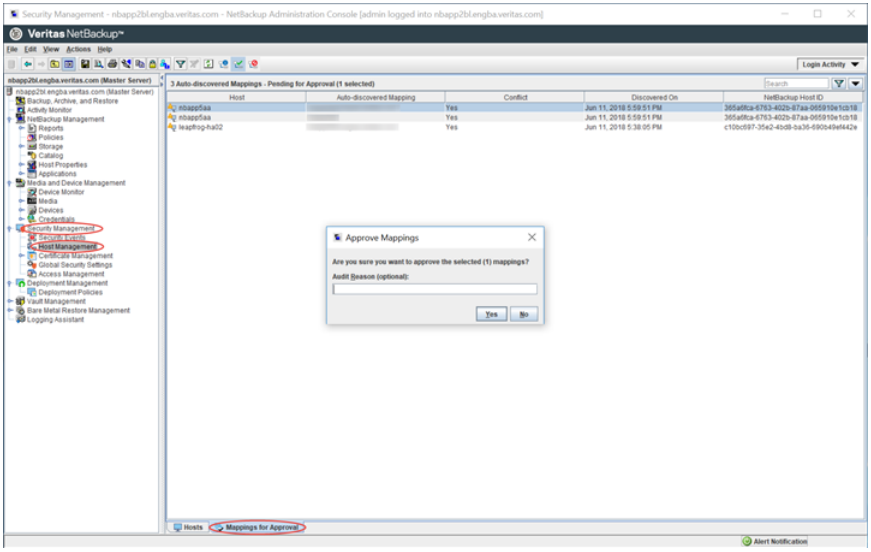
- `This appliance will use a NetBackup issued certificate for secure communication.`
  これ以上の証明書の構成は必要ありません。[次へ (Next)]をクリックして続行します。

プロセスが成功したことを示すメッセージが表示されます。

8 次のようにホスト名マッピングを承認します。

- 関連付けられているプライマリサーバーで、NetBackup 管理コンソールにログインします。
- 左ペインで[セキュリティ管理 (Security Management)]をクリックしてプロパティを展開し、[ホスト管理 (Host Management)]をクリックします。

- 右ペインの左下で、[承認のマッピング (Mappings for Approval)]をクリックします。
- 右ペインの上部で、承認が保留状態となっている任意のホストマッピングをクリックします。承認を求める[マッピングの承認 (Approve Mappings)]ダイアログボックスが表示されたら、[はい (Yes)]をクリックします。承認が保留状態となっている各ホストマッピングについて、このタスクを繰り返します。



3

構成後の手順

この章では以下の項目について説明しています。

NetBackup アプライアンスでの NIC1 (eth0) ポートの使用について

デフォルトでは、NIC1 (eth0) は出荷時に IP アドレス 192.168.229.233 に設定されます。このプライベートネットワークアドレスは、ノートパソコンと直接接続して初期構成を実行するために予約されています。NIC1 (eth0) は、通常、ネットワーク環境に接続されません。

初期構成を完了すると、バックアップデータ転送を行わない管理ネットワークに NIC1 (eth0) を接続できます。ただし、プライマリネットワークが同じ IP アドレス範囲を使用する場合は、デフォルト IP アドレスの変更が必要になることがあります。NetBackup Appliance は、NIC1 (eth0) で管理者インターフェイスのデフォルト IP アドレスと同じ範囲においてネットワーク構成を使用できません。

例えば、NIC2 (eth1) が 192.168.x.x IP アドレス範囲に設定されている場合、NIC1 (eth0) のデフォルトの IP アドレスを別の IP アドレス範囲に変更する必要があります。

初期構成を完了した後に NIC1 (eth0) の IP アドレスを変更するには、次のいずれかを実行します。

- NetBackup Appliance Web コンソールで次の操作を実行します。

アプライアンスにログインしたら、[設定 (Settings)]>[ネットワーク (Network)]>[ネットワーク設定 (Network Settings)]の順にクリックします。[ネットワーク構成 (Network Configuration)]セクションで、NIC1 (eth0) の IPv4 アドレス設定を編集します。
詳しくは、『NetBackup Appliance 管理者ガイド』を参照してください。

- NetBackup Appliance シェルメニューで次の操作を実行します。
  アプライアンスにログインしたら、`Network > IPv4`コマンドを使用して NIC1 (eth0) の IP アドレスを変更します。
  詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

メモ: アプライアンスで eth0 が構成されていない場合は、NetBackup Appliance Web コンソールからのチェックポイント操作が機能しません。この問題は、ポートの IP アドレスの構成を削除した場合にのみ発生します。この問題が発生した場合は、ポートを構成するか、NetBackup Appliance シェルメニューを使ってチェックポイントを作成するか、またはチェックポイントにロールバックします。ベストプラクティスとして、NIC1 (eth0) を使わない場合にも、IP アドレスを使って構成しておいてください。

アプライアンスのカタログバックアップポリシーの構成

バックアップ環境で新しい NetBackup Appliance の使用を開始する前に、最初の構成が完了した直後にカタログバックアップポリシーを構成することをお勧めします。次に、アプライアンスのカタログバックアップポリシーを構成する方法について説明します。

アプライアンスのカタログバックアップポリシーを構成するには

1. NetBackup 管理コンソールを起動してアプライアンスのカタログバックアップポリシーを構成する前に、次のように、最初にターゲット NFS ストレージデバイスをアプライアンスにマウントする必要があります。
   - NetBackup Appliance シェルメニューにログインして、`Manage > MountPoints` ビューに移動します。
   - 次のコマンドを実行して、NFS ストレージデバイスをアプライアンスにマウントします。
     `Mount` *`RemotePathMountPointNFS/NFSv4`*
   - `List` コマンドを実行して、NFS ストレージデバイスが正しくマウントされていることを確認します。
2. NetBackup 管理コンソールを起動し、次を実行します。
   - 左ペインで[セキュリティ管理 (Security Management)]を展開し、[セキュリティ設定 (Security Settings)]を選択します。

- [詳細 (Details)]ペインで、[ディザスタリカバリ (Disaster Recovery)]タブをクリックします。
- [パスフレーズ (Passphrase)]データ入力フィールドにパスフレーズを入力し、[パスフレーズの確認 (Confirm Passphrase)]データ入力フィールドに同じパスフレーズを入力します。

3 カタログバックアップポリシーを次のように構成します。

- 左ペインで[NetBackup の管理 (NetBackup Management)]を展開して[カタログバックアップの構成 (Configure the Catalog Backup)]をクリックし、NetBackup カタログバックアップウィザードを起動します。
- [ポリシー名 (Policy name)]を入力し、[新しいカタログバックアップポリシーの作成 (Create a new catalog backup policy)]を選択して[次へ (Next)]をクリックします。
- 目的のバックアップタイプを指定して、[次へ (Next)]をクリックします。
- バックアップの間隔とスケジュールを選択して、[次へ (Next)]をクリックします。
- [ログオン (Logon)]データ入力フィールドに、アプライアンス管理者のユーザー名を入力します。[パスワード (Password)]データ入力フィールドに、アプライアンス管理者のパスワードを入力します。

4 カタログディザスタリカバリファイルを次のように作成します。

- [カタログディザスタリカバリファイル (Catalog Disaster Recovery File)]ページで、作成した新しいマウントポイントを参照して選択します。ここに、各ディザスタリカバリイメージファイルが保存されます。イメージファイルには、ディザスタリカバリ情報が格納されます。
  イメージファイルは通常、パスフィールドに NFS 共有を指定することで、ネットワーク共有またはリムーバブルデバイスに保存されます。たとえば、`/mnt/remote/example` は、アプライアンスにマウントされた NFS 共有ポイントです。このパスが書き込み可能であることを確認するには、NFS サーバー上の次の項目が次のように設定されていることを確認してください。
- NFS サーバーで、`chmod` コマンドを使用して、共有フォルダのアクセス権の値を `777` に設定します。
- NFS サービス設定ファイル (`/etc/exports`) の共有フォルダに、読み取り/書き込み (rw) フラグを適用します。例: `/local/nfs/example 10.200.0.0/16(rw,sync,no_subtree_check)`

メモ: カタログをリカバリできるようにするため、必要に応じて、イメージファイルの場所を記録してください。

- ディザスタリカバリ情報を受信する電子メールアドレスを 1 つ以上入力し、バックアップポリシーの構成を終了します。

5 NetBackup 管理コンソールでカタログバックアップポリシーを手動で実行します。ディザスタリカバリ (DR) ファイルと .drpkg パッケージは /admin で生成され、受信者に電子メールで送信されます (電子メールが設定されている場合)。

NetBackup appliance からクライアントへの NetBackup クライアントパッケージのダウンロード

NetBackup クライアントソフトウェアは、NetBackup appliance からバックアップを作成する任意のクライアントにダウンロードできます。NetBackup Appliance Web コンソールのログオンページには、クライアントパッケージをダウンロードするための[パッケージのダウンロード (Download Packages)]セクションがあります。ログオンページにパッケージがない場合は、ベリタスダウンロードセンターからクライアントパッケージとアドオンパッケージをダウンロードできます。

メモ: 3.1.2 リリース以降、Windows クライアントアドオンは、NetBackup Appliance クライアントアドオンパッケージに含まれなくなりました。Windows クライアントアドオンをインストールまたはアップグレードする必要がある場合は、VEMS (Veritas Entitlement Management System) アカウントにログインしてダウンロードします。

パッケージは、ドロップダウンボックス内でオペレーティングシステムの種類ごとに次のように表示されます。

- すべて
- Linux
- Solaris
- AIX
- HP
- BSD
- VMware vCenter プラグイン

この手順には、ダウンロード方法以外にも、クライアント上のダウンロード済みファイルを抽出およびインストールする手順が含まれています。

NetBackup appliance からクライアントに NetBackup クライアントパッケージをダウンロードする方法

1 バックアップするクライアントにログインします。

2 ブラウザウィンドウを開き、Appliance URL を入力します。

3 ランディングページの中央の［パッケージのダウンロード (Download Packages)］セクションで、ドロップダウンボックスをクリックしてパッケージのリストを表示します。

4 選択したパッケージを右クリックして、クライアント上のダウンロード場所を指定します。

たとえば、Linux または UNIX プラットフォームでは、/tmp にパッケージをダウンロードします。

メモ: 選択後に「パッケージがありません (No packages found)」というメッセージが表示された場合、現在 Appliance にはクライアントパッケージがインストールされていません。この状況が起きる可能性が高いのは、Appliance を USB フラッシュドライブから再イメージした場合です。Appliance にクライアントパッケージをダウンロードしてインストールする場合は、『 NetBackup Appliance 管理者ガイド』を参照してください。「NetBackup Appliance Web コンソールで NetBackup Appliance を管理する」の章で、「クライアント共有を使った NetBackup Appliance へのソフトウェア更新のダウンロード」を参照してください。

---

5 パッケージを展開します。

6 クライアントソフトウェアを次のようにインストールします。

UNIX システムの場合、.install スクリプトを実行します。

7 正常にクライアントソフトウェアをインストールした後、次のように Appliance プライマリサーバーの名前をクライアントに追加する必要があります。

Windows システム

- NetBackup をクライアントにインストールした後、[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)] インターフェースを開きます。
  [スタート (Start)]>[すべてのプログラム (All Programs)]>[Veritas NetBackup]>[バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)]
- 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から、[ファイル (File)]>[NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)] の順に選択します。
- [NetBackup マシンおよびポリシー形式の指定 (Specify NetBackup Machines and Policy Type)] ダイアログで、[バックアップおよびリストアに使用するサーバー (Server to use for backups and restores)] フィールドにサーバーの名前を入力します。次に、[サーバーリストの編集 (Edit Server List)]、[OK] の順にクリックします。
- 表示されるダイアログボックスで、アプライアンスプライマリサーバーの完全修飾ホスト名を入力し、[OK] をクリックします。
- 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を閉じます。
- Windows コマンドプロンプトを開いて、NetBackup クライアントサービスを再起動します。次に、`services.msc` を押し、Enter キーを押します。

UNIX システム

- クライアントで、次の場所にナビゲートします。
  `cd /usr/openv/netbackup`
- `ls` と入力し、ディレクトリの内容を参照します。
- `bp.conf` ファイルをテキストエディタで開きます。
- アプライアンスプライマリサーバーの完全修飾ホスト名を入力します。
- 変更を保存してファイルを閉じます。

p.101 の「NFS 共有を介した NetBackup クライアントソフトウェアのインストール」を参照してください。

NFS 共有を介した NetBackup クライアントソフトウェアのインストール

すべてのアプライアンスの構成が完了したら、NFS 共有を開いて、構成済みのアプライアンスで使用する予定がある UNIX クライアントに NetBackup クライアントソフトウェアをインストールできます。

インストールの前に、アプライアンスに NetBackup クライアントソフトウェアパッケージをダウンロードして、NFS 共有 <appliance-name>:/inst/client に保存していることを確認します。

NFS 共有を介した NetBackup の UNIX クライアントソフトウェアのインストール

NFS 共有を使用して NetBackup クライアントソフトウェアを UNIX クライアントにインストールするには

1. NetBackup Appliance シェルメニューで、管理者のクレデンシャルを使用してプライマリアプライアンスにログオンします。
2. 次のコマンドを使用して、プライマリサーバーアプライアンスの追加サーバーリストにクライアントのホスト名を追加します。

   ```
   Main > Settings > NetBackup AdditionalServers Add
   ```

3. 次のコマンドを使い、NFS 共有を開きます。

   ```
   Main > Settings > Share ClientInstall Open
   ```

4. NetBackup クライアントソフトウェアをインストールする UNIX クライアントホストで、ルートとしてログオンします。
5. 次の NFS 共有をマウントします。

   <*appliance_name*>:/inst/client

6. クライアントで、NFS 共有ディレクトリ内のファイルを参照します。次のファイルまたはディレクトリが表示されます。

   - NetBackup_8.x_CLIENTS2 および/または NetBackup_8.x_CLIENTS1
   - .packages
   - clientconfig
   - quickinstall.exe
   - PC_Clnt
   - docs
   - unix-client-install

7. クライアントで、テキストエディタを使用して次のファイルを開きます。

   /inst/client/clientconfig/defaults.txt

8 ADDITIONALSERVERS エントリに、この NetBackup ドメインの 1 つ以上のメディアサーバーを追加します。ホスト名のみを使用して、メディアサーバーを指定します。複数のメディアサーバーを追加する場合は、カンマ区切りで列記します。

例:

```
PRIMARIESERVER=primary123.test.com
ADDITIONALSERVERS=media1.test.com,media2.test.come,media3.test.com
```

メモ: クライアントホストのバックアップの作成に使用されているメディアサーバーを優先します。この NetBackup ドメイン内のメディアサーバーが不明な場合は、プライマリアプライアンスで `Main > Settings > NetBackup AdditionalServers Show|ShowAll` コマンドを実行します。NetBackup 管理コンソールで、メディアサーバーを調べることもできます。

ファイルを保存して、エディタを終了します。

9 クライアントの /tmp ディレクトリに NetBackup 応答ファイル (NBInstallAnswer.conf) を作成します。

例:

```
CA_CERTIFICATE_FINGERPRINT=<fingureprint_value>
AUTHORIZATION_TOKEN=<token>
```

応答ファイルとその内容について詳しくは、『NetBackup インストールガイド』を参照してください。

10 次の情報を使って NBInstallAnswer.conf に値を指定します。

```
CA_CERTIFICATE_FINGERPRINT=<fingureprint_value>
```

例 (指紋の値は読みやすくするため折り返されています):

```
CA_CERTIFICATE_FINGERPRINT=30:A5:9A:D1:18:F0:01:E4:21:E8:0D:A0:
26:95:14:52:7C:7A:58:B1
```

お使いの NetBackup 環境のセキュリティ構成に応じて、応答ファイルに AUTHORIZATION_TOKEN オプションを追加する必要があります。

NetBackup の応答ファイルに関する追加情報を参照できます。

『NetBackup インストールガイド』を参照してください。

CA 証明書の指紋と認証トークンに関する追加情報を参照できます。

『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。

11 `unix-client-install` スクリプトを実行します。

この処理で NetBackup クライアントソフトウェアがインストールされます。

12 クライアントで次のファイルを確認します。手順 8 で `defaults.txt` ファイルに追加したメディアサーバー名が `bp.conf` ファイルに含まれていることを確認します。

```
/usr/openv/netbackup/bp.conf
```

13 アプライアンスで、次のコマンドを使い、共有ディレクトリを閉じます。

```
Main > Settings > Share ClientInstall Close
```

p.99 の「NetBackup appliance からクライアントへの NetBackup クライアントパッケージのダウンロード」を参照してください。

索引

さ

た

は

や