Veritas NetBackup™ Appliance セキュリティガイド

リリース 4.1

VERITAS™

Veritas NetBackup Appliance セキュリティガイド

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

NetBackup appliance セキュリティガイドについて

この章では以下の項目について説明しています。

NetBackup appliance セキュリティガイドについて

NetBackup Appliance は、当初からセキュリティを第一に開発されています。Linux オペレーティングシステムや中核的な NetBackup アプリケーションなどのアプライアンスの各要素は、業界標準製品および高度なセキュリティ製品の両方を使って脆弱性がテストされています。これらの評価基準により、不正にアクセスされて、結果として起きるデータの紛失や盗難を最小限にすることができます。

NetBackup Appliance のソフトウェアとハードウェアの新しい各バージョンは、リリース前に脆弱性について検証されています。見つかった問題の重大度に応じて、ベリタスは定期的なメジャーリリースまたはメンテナンスリリースでセキュリティパッチをリリースするか、修正プログラムを提供します。脅威のリスクを軽減するために、Veritas は、定期メンテナンスリリースサイクルの一部として、製品のサードパーティパッケージとモジュールを定期的に更新しています。

このガイドの目的は、NetBackup appliance 4.1 リリースに実装されているセキュリティ機能について説明することです。以下の章とサブセクションが含まれます。

NetBackup Appliance ユーザー認証

この章では、NetBackup Appliance の認証機能について説明します。以下のセクションが含まれます。

表 1-1 認証に関するセクション

セクション名	説明	リンク
NetBackup Appliance のユーザー認証について	このセクションでは、アプライアンスにアクセスできるユーザー、ユーザーアカウント、プロセスの種類について説明します。	p.14 の「NetBackup Appliance のユーザー認証について」を参照してください。
ユーザー認証の設定について	このセクションでは、アプライアンスで認証できる各種のユーザー用の設定オプションについて説明します。	p.19 の「ユーザー認証の設定について」を参照してください。
LDAP ユーザーの認証について	このセクションでは、LDAP ユーザーを登録、認証するようにアプライアンスを設定するための前提条件とプロセスについて説明します。	p.24 の「LDAP ユーザーの認証について」を参照してください。
Active Directory ユーザーの認証について	このセクションでは、Active Directory（AD）ユーザーを登録、認証するようにアプライアンスを設定するための前提条件とプロセスについて説明します。	p.25 の「Active Directory ユーザーの認証について」を参照してください。
Kerberos-NIS ユーザーの認証について	このセクションでは、Kerberos-NIS ユーザーを登録、認証するようにアプライアンスを設定するための前提条件とプロセスについて説明します。	p.29 の「Kerberos-NIS ユーザーの認証について」を参照してください。
アプライアンスのログインバナーについて	このセクションでは、ユーザーがアプライアンスで認証を試行したときに表示されるテキストバナーを設定できる、ログインバナー機能について説明します。	p.30 の「アプライアンスのログインバナーについて」を参照してください。
ユーザー名とパスワードの仕様について	このセクションでは、ユーザー名とパスワードのクレデンシャルについて説明します。	p.31 の「ユーザー名とパスワードの仕様について」を参照してください。

NetBackup Appliance ユーザーの権限の確認

この章では、NetBackup appliance にアクセスするユーザーを認可するために実装する機能について説明します。以下のセクションが含まれます。

表 1-2 認可のセクション

セクション名	説明	リンク
NetBackup Appliance でのユーザーの権限の確認について	このセクションでは、NetBackup appliance の認可のプロセスの主な特性について説明します。	p.36 の「NetBackup appliance におけるユーザー認可について」を参照してください。

セクション名	説明	リンク
NetBackup Appliance ユーザーの認可について	このセクションでは、アプライアンスユーザーの各種アクセス権限を確認するための管理オプションについて説明します。	p.38 の「NetBackup Appliance ユーザーの認可について」を参照してください。
管理者ユーザーの役割について	このセクションでは、管理者ユーザーの役割について説明します。	p.42 の「管理者ユーザーのロールについて」を参照してください。
NetBackupCLI ユーザーの役割について	このセクションでは、NetBackupCLI ユーザーの役割について説明します。	p.42 の「NetBackupCLI ユーザーロールについて」を参照してください。

NetBackup Appliance の侵入防止、侵入検知システム

この章では、以下のセクションで、NetBackup appliance の SDCS (Symantec Data Center Security: Server Advanced) の実装について説明します。

表 1-3 IPS と IDS ポリシーのセクション

セクション名	説明	リンク
NetBackup Appliance の Symantec Data Center Security について	このセクションでは、アプライアンスで実装する SDCS 機能を紹介します。	p.46 の「NetBackup appliance の Symantec Data Center Security について」を参照してください。
NetBackup Appliance の侵入防止システムについて	このセクションでは、アプライアンスの保護に使用する IPS (Intrusion Prevention System の略で侵入防止システムの意味) ポリシーについて説明します。	p.49 の「NetBackup appliance の侵入防止システムについて」を参照してください。
NetBackup Appliance の侵入検知システムについて	このセクションでは、アプライアンスの監視に使用する IDS (Intrusion Detection System の略で侵入検知システムの意味) ポリシーについて説明します。	p.49 の「NetBackup appliance の侵入検知システムについて」を参照してください。
NetBackup Appliance の SDCS イベントの見直し	このセクションでは、セキュリティレベルに基づいた SDCS イベントについて説明します。	p.50 の「NetBackup アプライアンスの SDCS イベントの見直し」を参照してください。
NetBackup Appliance でのアンマネージモードでの SDCS の実行	このセクションでは、アプライアンスでのデフォルトのセキュリティ管理について簡単に説明します。	p.53 の「NetBackup アプライアンスでのアンマネージモードでの SDCS の実行」を参照してください。

セクション名	説明	リンク
NetBackup Appliance でのマネージモードでの SDCS の実行	このセクションでは、集中管理される SDCS 環境の一部としてアプライアンスのセキュリティを管理する方法について説明します。	p.53 の「NetBackup アプライアンスでのマネージモードでの SDCS の実行」を参照してください。

NetBackup Appliance のログファイル

この章では、以下のセクションで、NetBackup appliance のログファイルとログファイルを表示するためのオプションを一覧表示します。

表 1-4　ログセクションの使用

セクション名	説明	リンク
ログファイルの使用について	この章では、NetBackup appliance に関して表示できる異なる種類のログすべての概要を提供します。	p.55 の「NetBackup appliance のログファイルについて」を参照してください。
Support コマンドの使用によるログファイルの表示	この章では、サポートコマンドを使ってログファイルを表示するための手順について説明します。	p.57 の「Support コマンドの使用によるログファイルの表示」を参照してください。
Browse コマンドを使った NetBackup Appliance のログファイルの検索	この章では、ログファイルを表示するための Browse コマンドの使い方について説明します。	p.59 の「Browse コマンドを使用した NetBackup appliance ログファイルの参照場所」を参照してください。
DataCollect コマンドを使ったデバイスログの収集	この章では、デバイスログを収集するための手順について説明します。	p.60 の「NetBackup Appliance でのデバイスログの収集」を参照してください。

NetBackup Appliance オペレーティングシステムのセキュリティ

表 1-5　オペレーティングシステムセクション

セクション名	説明	リンク
NetBackup Appliance のオペレーティングシステムのセキュリティについて	このセクションでは、全体的な NetBackup appliance のセキュリティを改善するためにオペレーティングシステムに加える、異なる更新の種類について説明します。	p.64 の「NetBackup Appliance のオペレーティングシステムのセキュリティについて」を参照してください。

セクション名	説明	リンク
NetBackup Appliance の OS の主要コンポーネント	このセクションでは、NetBackup appliance を搭載する製品とオペレーティングシステムコンポーネントを一覧表示します。	p.66 の「NetBackup appliance の OS の主要コンポーネント」を参照してください。
NetBackup Appliance の脆弱性スキャン	このセクションでは、Veritas 社がアプライアンスのセキュリティを確認するために使用するセキュリティスキャナの一部を一覧表示します。	

NetBackup Appliance のデータセキュリティ

この章では、以下のセクションで、NetBackup appliance のデータセキュリティ実装について説明します。

表 1-6 データセキュリティセクション

セクション名	説明	リンク
データセキュリティについて	このセクションでは、データセキュリティの改善のために取られる対策をリストします。	p.69 の「データセキュリティについて」を参照してください。
データ整合性について	このセクションでは、データ整合性の改善のために取られる対策をリストします。	p.70 の「データ整合性について」を参照してください。
データの分類について	このセクションでは、データ分類の改善のために取られる対策をリストします。	p.71 の「データの分類について」を参照してください。
データの暗号化について	このセクションでは、データの暗号化の改善のために取られる対策をリストします。	p.71 の「データの暗号化について」を参照してください。

NetBackup Appliance の Web セキュリティ

この章では、以下のセクションで、NetBackup appliance の Web セキュリティ実装について説明します。

表 1-7 Web セキュリティセクション

セクション名	説明	リンク
SSL 証明書について	このセクションでは、NetBackup Appliance Web コンソールの SSL 証明書の更新を一覧表示します。	p.76 の「SSL の使用について」を参照してください。

セクション名	説明	リンク
サードパーティの SSL 証明書のインストール	このセクションでは、サードパーティの SSL 証明書をインストールするための手順を一覧表示します。	p.77 の「ECA 証明書の実装について」を参照してください。

NetBackup Appliance のネットワークセキュリティ

この章では、以下のセクションで、NetBackup appliance のネットワークセキュリティ実装について説明します。

表 1-8 ネットワークセキュリティセクション

セクション名	説明	リンク
IPsec チャネル設定について	このセクションでは、NetBackup Appliance の IPsec 設定について説明します。	p.80 の「IPsec チャネル設定について」を参照してください。
NetBackup appliance ポートについて	このセクションでは、NetBackup Appliance のポート情報について説明します。	p.81 の「NetBackup appliance ポートについて」を参照してください。

NetBackup Appliance のコールホームセキュリティ

この章では、以下のセクションで、NetBackup appliance のコールホームセキュリティ実装について説明します。

表 1-9 コールホームセキュリティセクション

セクション名	説明	リンク
AutoSupport について	このセクションでは、NetBackup appliance の AutoSupport 機能について説明します。	p.86 の「AutoSupport について 」を参照してください。
コールホームについて	このセクションでは、NetBackup appliance のコールホーム機能について説明します。	p.87 の「コールホームについて」を参照してください。
SNMP について	このセクションでは、NetBackup appliance の SNMP 機能について説明します。	p.92 の「SNMP について」を参照してください。

NetBackup Appliance の IPMI セキュリティ

この章の以下のセクションでは、IPMI 設定を保護するために採用するガイドラインについて説明します。

表 1-10 IPMI セキュリティセクション

セクション名	説明	リンク
IPMI 設定の紹介	このセクションでは、IPMI と IPMI がNetBackup applianceで設定される方法について説明します。	p.94 の「IPMI 設定の紹介」を参照してください。
推奨 IPMI 設定の一覧表示	このセクションでは、安全な設定のための推奨 IPMI 設定を一覧表示します。	p.94 の「推奨される IPMI 設定」を参照してください。

対象読者

このガイドは、NetBackup appliance の保守管理業務に従事しているセキュリティ管理者、バックアップ管理者、システム管理者、IT 技術者を含むユーザーを対象としています。

メモ: 本書のタスクや手順は構成済みのアプライアンスで実行する必要があります。アプライアンスの役割を構成する前にローカルユーザーコマンドを問題なく使うことはできません。アプライアンスの役割が構成されていない場合、ユーザー権限の付与などを含むすべてのローカルユーザーコマンドが失敗します。役割を構成する前にローカルユーザーコマンドを実行すると、役割を構成した後に同じコマンドを実行しても失敗します。その他のコマンドは、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には、アプライアンスの構成が完了するまでローカルユーザーコマンドを使わないことがベストプラクティスです。

2

ユーザー認証

この章では以下の項目について説明しています。

NetBackup Appliance のユーザー認証について

NetBackup appliance は、ユーザーアカウントを使用して管理します。ローカルユーザーアカウントを作成したり、リモートディレクトリサービスに属するユーザーとユーザーグループを登録したりすることができます。各ユーザーアカウントが Appliance にアクセスするには、ユーザー名とパスワードで自己認証する必要があります。ローカルユーザーの場合には、ユーザー名とパスワードは Appliance 上で管理されます。登録済みのリモートユーザーの場合には、ユーザー名とパスワードはリモートディレクトリサービスによって管理されます。

新しいユーザーアカウントがアプライアンスにログオンしてアクセスするには、最初にそのアカウントと役割を承認する必要があります。デフォルトでは、新しいユーザーアカウントには割り当てられた役割がないので、役割が付与されるまでログオンできません。

表 2-1では、アプライアンスで利用可能なユーザーアカウントについて説明します。

表 2-1 NetBackup appliance のアカウントの種類

アカウント名	説明
admin	admin アカウントは NetBackup appliance のデフォルトの管理者ユーザーです。このアカウントは、デフォルトの管理者ユーザーにアプライアンスに対する完全なアクセスと制御を提供します。 新しいアプライアンスには、次のデフォルトのログオ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 Appliance から共有をマウントまたはマップする場合は、次の内容を記録してください。 ■ Windows: Windows CIFS 共有のマウントまたはマップは、ローカルの管理者アカウントにのみ許可されます。 ■ Linux: ルートアクセスアカウントを持つユーザーのみが NFS 共有を直接マウントする mount コマンドを実行できます。
AMSadmin	AMSadmin アカウントを使用すると、次のアプライアンスインターフェースにフルアクセスできます。 ■ Appliance Management Console ■ NetBackup Appliance Web コンソール ■ NetBackup Appliance シェルメニュー ■ NetBackup 管理コンソール このアカウントについて詳しくは、『Veritas Appliance 管理ガイド』を参照してください。
maintenance	メンテナンスアカウントは、NetBackup Appliance シェルメニューでVeritasサポートが使用します(管理者用ログオン後)。このアカウントは、メンテナンス活動または Appliance のトラブルシューティング専用として使用します。 **メモ:** このアカウントは、GRUB の変更や、STIG オプションが有効な場合のシングルユーザーモードのブートにも使用します。

アカウント名	説明
nbasecadmin	nbasecadmin アカウントは、セキュリティ管理者ユーザーが、NetBackup で役割ベースのアクセス制御 (RBAC) およびバックアップとリストア操作の管理を行うために使用します。アプライアンスのリリース 3.1.2 以降では、アプライアンスプライマリサーバーで初期構成を実行するとき、またはアプライアンスプライマリサーバーをアップグレードするときに、このユーザーが自動的に作成されます。 作成されると、このアカウントにデフォルトのアプライアンスパスワードが割り当てられます。このユーザーが NetBackup Appliance シェルメニューに初めてログインすると、アカウントのデフォルトパスワードの変更を求めるメッセージが表示されます。 **メモ:** このユーザーは、デフォルトのパスワードが変更されるまで、NetBackup Web UI にログインできません。 デフォルトのパスワードが変更されると、デフォルトでは、nbasecadmin ユーザーには次に対するアクセス権と権限が許可されます。 ■ NetBackup Web UI NetBackup Web UI へのアクセス権があると、このユーザーは他の NetBackup ユーザーのユーザー役割を設定し、NetBackup のすべてのセキュリティ設定を管理して、バックアップとリストア操作を実行できます。 nbasecadmin ユーザーは、アプライアンスのローカルユーザーや、LDAP サーバーまたは Active Directory (AD) サーバーに登録済みのユーザーに NetBackup の役割を割り当てることもできます。p.44 の「NetBackup でのユーザー権限の確認について」を参照してください。 **メモ:** ソフトウェアバージョン 3.2 以降では、nbasecadmin ユーザーにバックアップとリストアの権限を割り当てられます。以前のバージョンからアップグレードする場合は、nbasecadmin ユーザーアカウントにバックアップとリストアの権限を手動で追加する必要があります。詳しくは、『NetBackup Web UI セキュリティ管理者ガイド』を参照してください。 ■ NetBackup Appliance シェルメニュー NetBackup Appliance シェルメニューにログインして、アカウントのパスワードを変更します。アクセスは `Main > Settings > Password` ビューに制限されます。 このビューは、`nbasecadmin` ユーザーと、アプライアンスで[役割なし (No Role)]が割り当てられているすべてのアプライアンスローカルユーザーに表示されます。`nbasecadmin` ユーザーがシェルメニューにログインした場合、次のメニュー項目のみが利用可能です。 終了 (Exit) パスワード (Password) nbasecadmin ユーザーのアクセスルールを変更して、他の権限も付与できます。NetBackup Web UI にアクセスするには、ブラウザウィンドウを開き、`https://`*`appliance primary server host name`*`/webui` という URL を入力します。 RBAC および NetBackup のユーザー役割管理について詳しくは、『NetBackup Web UI セキュリティ管理者ガイド』を参照してください。

内部ユーザーにのみ利用できるアカウントを次に示します。これらのアカウントでは、NetBackup Appliance Web コンソールまたは NetBackup Appliance シェルメニューを介してシステムにアクセスすることはできません。

表 2-2 NetBackup appliance の内部アカウントの種類

アカウント名	説明
sisips	sisips アカウントは、SDCS ポリシーを実装するための内部ユーザーです。
root	root アカウントは、保守タスクを実行するためにVeritas社のサポートのみがアクセスする制限されたユーザーです。このアカウントにアクセスしようとすると、次のメッセージが表示されます。 Permission Denied !! Access to the root account requires overriding the Intrusion Security Policy.
nbcopilotxxxx	プライマリサーバーからメディアサーバーへのアクセスの認証をサポートします。
nbwebsvc	認証はサポートされません。

p.38 の「NetBackup Appliance ユーザーの認可について」を参照してください。

NetBackup アプライアンスで認証できるユーザーの種類

アプライアンスのローカルユーザーを直接追加したり、LDAP サーバー、AD（Active Directory）サーバー、または NIS サーバーのユーザーを登録したりできます。リモートユーザーを登録すると、既存のディレクトリサービスを利用してユーザー管理と認証を行うことができるので便利です。表 2-3に、NetBackup Appliance に追加できるユーザーの種類を示します。

メモ: アプライアンスの役割を構成する前にローカルユーザーコマンドを問題なく使うことはできません。アプライアンスの役割が構成されていない場合、ユーザー権限の付与などを含むすべてのローカルユーザーコマンドが失敗します。役割を構成する前にローカルユーザーコマンドを実行すると、役割を構成した後に同じコマンドを実行しても失敗します。一部のコマンドは、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には、アプライアンスの構成が完了するまでローカルユーザーコマンドを使わないことがベストプラクティスです。

表 2-3 NetBackup Appliance のユーザーの種類

ユーザーの種類	説明	注意事項
ローカル（ネーティブユーザー）	ローカルユーザーは、アプライアンスのデータベースに追加され、LDAP サーバーのような外部ディレクトリベースのサーバーに対して参照されることはありません。ユーザーを追加したら、適切なアプライアンスのアクセス権を認可したり取り消せます。	■ NetBackup Appliance Web コンソールから［設定（Settings）］>［認証（Authentication）］>［ユーザー管理（User Management）］の順に開いたページを使ってローカルユーザーを追加、削除、管理できます。 ■ NetBackup Appliance シェルメニューで `Settings > Security > Authentication > LocalUser` コマンドを使用して、ローカルユーザーを追加および削除したり、そのパスワードを変更したりできます。 ■ ローカルユーザーグループは追加できません。 ■ ローカルユーザーは、管理者、NetBackupCLI、または AMSadmin の役割を持つことができます。 **メモ:** 既存のローカルユーザーには NetBackupCLI 役割を付与できません。ただし、ローカル NetBackupCLI ユーザーを作成できます。その場合、NetBackup Appliance シェルメニューから `Manage > NetBackupCLI > Create` コマンドを実行します。
LDAP	LDAP（Lightweight Directory Access Protocol）ユーザーまたはユーザーグループが、外部 LDAP サーバー上に存在します。LDAP サーバーと通信するようにアプライアンスを構成すると、これらのユーザーとユーザーグループをアプライアンスに登録できます。ユーザーを登録（追加）したら、適切なアプライアンスのアクセス権限を認可または取り消しができます。 p.24 の「LDAP ユーザーの認証について」を参照してください。	■ NetBackup Appliance Web コンソールの［設定（Settings）］>［認証（Authentication）］>［ユーザー管理（User Management）］の順に開いたページを使って LDAP ユーザーとユーザーグループを追加、削除、管理できます。 ■ NetBackup Appliance シェルメニューで `Settings > Security > Authentication > LDAP` コマンドを使用して、LDAP ユーザーとユーザーグループを追加および削除できます。 ■ 管理者または NetBackupCLI ロールを LDAP ユーザーまたはユーザーグループに割り当てることができます。 **メモ:** NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。

ユーザーの種類	説明	注意事項
Active Directory	AD（Active Directory）ユーザーまたはユーザーグループは、外部 AD サーバー上に存在します。AD サーバーと通信するようにアプライアンスを構成すると、これらのユーザーとユーザーグループをアプライアンスに登録できます。ユーザーを登録（追加）したら、適切なアプライアンスのアクセス権限を認可または取り消しができます。 p.25 の「Active Directory ユーザーの認証について」を参照してください。	■ NetBackup Appliance Web コンソールの［設定 (Settings)］>［認証 (Authentication)］>［ユーザー管理 (User Management)］ページを使用して、AD ユーザーおよびユーザーグループを追加、削除、管理できます。 ■ NetBackup Appliance シェルメニューで `Settings > Security > Authentication > ActiveDirectory` コマンドを使用して、AD ユーザーとユーザーグループを追加および削除できます。 ■ 管理者または NetBackupCLI ロールを AD ユーザーまたはユーザーグループに割り当てることができます。 **メモ:** NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。
Kerberos-NIS	NIS（ネットワーク情報サービス）ユーザーまたはユーザーグループは、外部 NIS サーバー上に存在します。LDAP や AD の実装とは違って、NIS ドメインと通信するようにアプライアンスを構成する場合は Kerberos 認証が必要です。NIS ユーザーが登録されるようにアプライアンスを構成するには、既存の Kerberos サービスを NIS サーバーに関連付ける必要があります。 NIS サーバーや Kerberos サーバーと通信するようにアプライアンスを構成すると、NIS ユーザーとユーザーグループをアプライアンスに登録できます。ユーザーをアプライアンスに登録（追加）したら、適切なアプライアンスのアクセス権を認可または取り消しができます。 p.29 の「Kerberos-NIS ユーザーの認証について」を参照してください。	■ NetBackup Appliance Web コンソールの［設定 (Settings)］>［認証 (Authentication)］>［ユーザー管理 (User Management)］ページを使用して、NIS ユーザーおよびユーザーグループを追加、削除、管理できます。 ■ NetBackup Appliance シェルメニューで `Settings > Security > Authentication > Kerberos` コマンドを使用して AD と NIS のユーザーおよびユーザーグループを削除できます。 ■ 管理者または NetBackupCLI ロールを NIS ユーザーまたはユーザーグループに割り当てることができます。 **メモ:** NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。

新しいユーザーの構成について詳しくは、『NetBackup Appliance 管理者ガイド』を参照してください。

ユーザー認証の設定について

表 2-4では、NetBackup Appliance Web コンソールと NetBackup Appliance シェルメニューの機能を利用してアプライアンスを設定し、さまざまな種類のユーザーを認証し、アクセス権限を与える方法について説明します。

表 2-4 ユーザー認証管理

ユーザーの種類	NetBackup Appliance Web コンソール	NetBackup Appliance シェルメニュー
ローカル（ネーティブユーザー）	NetBackup Appliance Web コンソールの［設定（Settings）］>［認証（Authentication）］>［ユーザー管理（User Management）］タブを利用し、ローカルユーザーを追加します。 p.38 の「NetBackup Appliance ユーザーの認可について」を参照してください。	`Settings > Security > Authentication > LocalUser` では次のコマンドとオプションが利用可能です。 ■ `Clean` - すべてのローカルユーザーを削除します。 ■ `List` - アプライアンスに追加されているすべてのローカルユーザーの一覧を表示します。 ■ `Password` - ローカルユーザーのパスワードを変更します。 ■ `Users` - 1 人以上のローカルユーザーを追加または削除します。

ユーザーの種類	NetBackup Appliance Web コンソール	NetBackup Appliance シェルメニュー
LDAP	[設定 (Settings)] > [ユーザー ()] > [認証 (Authentication)] > [LDAP]で、次の LDAP 設定タスクを実行できます。 ■ 新しい LDAP 設定を追加します。 ■ XML ファイルから保存済みの LDAP 構成をインポートします。 ■ LDAP サーバーの構成パラメータを追加、編集、削除します。 ■ LDAP サーバーの SSL 証明書を識別し、接続します。 ■ LDAP サーバーの属性マップを追加、編集、削除します。 ■ 既存の LDAP 構成(ユーザーを含む)を XML ファイルとしてエクスポートします。このファイルをインポートし、他のアプライアンスで LDAP を構成できます。 ■ LDAP 構成を無効にして再度有効にします。 ■ LDAP サーバーの構成を解除します。 NetBackup Appliance Web コンソールの[設定 (Settings)] > [認証 (Authentication)] > [ユーザー管理 (User Management)]タブを利用し、LDAP ユーザーとユーザーグループを追加します。 p.38 の「NetBackup Appliance ユーザーの認可について」を参照してください。	Settings > Security > Authentication > LDAP では次のコマンドとオプションが利用可能です。 ■ Attribute - LDAP 構成属性を追加または削除します。 ■ Certificate - SSL 証明書を設定、表示、無効化します。 ■ ConfigParam - LDAP 構成パラメータを設定、表示、無効化します。 ■ Configure - LDAP ユーザーがアプライアンスに登録し、アプライアンスで LDAP ユーザーを認証できるようにアプライアンスを設定します。* ■ Disable - アプライアンスの LDAP ユーザー認証を無効にします。 ■ Enable - アプライアンスの LDAP ユーザー認証を有効にします。 ■ Export - 既存の LDAP 構成を XML ファイルとしてエクスポートします。 ■ Groups - 1 つ以上の LDAP ユーザーグループを追加または削除します。LDAP サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。 ■ Import - XML ファイルから LDAP 構成をインポートします。* ■ List - アプライアンスに追加されているすべての LDAP ユーザーとユーザーグループの一覧を表示します。 ■ Map - NSS マップの属性またはオブジェクトクラスを設定、削除、表示します。 ■ Show - LDAP 構成の詳細を表示します。 ■ Status - アプライアンスの LDAP 認証の状態を表示します。 ■ Unconfigure - LDAP 構成を削除します。 ■ Users - 1 人以上の LDAP ユーザーを追加または削除します。LDAP サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。

ユーザーの種類	NetBackup Appliance Web コンソール	NetBackup Appliance シェルメニュー
Active Directory	[設定 (Settings)] > [ユーザー ()] > [認証 (Authentication)] > [Active Directory]で、次の AD 設定タスクを実行できます。 ■ 新しい Active Directory 設定を行います。 ■ 既存の Active Directory 構成を構成解除します。 NetBackup Appliance Web コンソールの[設定 (Settings)] > [認証 (Authentication)] > [ユーザー管理 (User Management)]タブを利用し、Active Directory ユーザーとユーザーグループを追加します。 p.38 の「NetBackup Appliance ユーザーの認可について」を参照してください。	Settings > Security > Authentication > ActiveDirectory では次のコマンドとオプションが利用可能です。 ■ Configure - AD ユーザーがアプライアンスに登録し、アプライアンスで AD ユーザーを認証できるようにアプライアンスを設定します。 ■ Groups - 1 つ以上の AD ユーザーグループを追加または削除します。AD サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。 ■ List - アプライアンスに追加されているすべての AD ユーザーとユーザーグループの一覧を表示します。 ■ Status - アプライアンスの AD 認証の状態を表示します。 ■ Unconfigure - AD 構成を削除します。 ■ Users - 1 人以上の AD ユーザーを追加または削除します。AD サーバーにすでに存在するユーザーのみをアプライアンスに追加できます。
Kerberos-NIS	[設定 (Settings)] > [ユーザー ()] > [認証 (Authentication)] > [Kerberos-NIS]で、次の Kerberos-NIS 設定タスクを実行できます。 ■ 新しい Kerberos-NIS 設定を行います。 ■ 既存の Kerberos-NIS 構成を構成解除します。 NetBackup Appliance Web コンソールの[設定 (Settings)] > [認証 (Authentication)] > [ユーザー管理 (User Management)]タブを利用し、Kerberos-NIS ユーザーとユーザーグループを追加します。 p.38 の「NetBackup Appliance ユーザーの認可について」を参照してください。	Settings > Security > Authentication > Kerberos では次のコマンドとオプションが利用可能です。 ■ Configure - NIS ユーザーがアプライアンスに登録し、アプライアンスで NIS ユーザーを認証できるようにアプライアンスを設定します。 ■ Groups - 1 つ以上の NIS ユーザーグループを追加または削除します。NIS サーバーにすでに存在するユーザーグループのみをアプライアンスに追加できます。 ■ List - アプライアンスに追加されているすべての NIS ユーザーとユーザーグループの一覧を表示します。 ■ Status - アプライアンスの NIS と Kerberos の認証の状態を表示します。 ■ Unconfigure - NIS と Kerberos の構成を削除します。 ■ Users - 1 人以上の NIS ユーザーを追加または削除します。NIS サーバーにすでに存在するユーザーのみをアプライアンスに追加できます。

一般的なユーザー認証ガイドライン

アプライアンスでユーザーを認証する場合は次のガイドラインを使用してください。

- アプライアンス上の認証には 1 種類のリモートユーザータイプ (LDAP、Active Directory (AD)、または NIS) のみを設定できます。たとえば、アプライアンスの LDAP ユーザーを認証する場合、AD ユーザー認証に変更する前にアプライアンスの LDAP 構成を削除する必要があります。
- NetBackupCLI ロールはいつでも最大 9 ユーザーグループに割り当てることができます。
- 既存のローカルユーザーに NetBackupCLI 役割を付与することはできません。ただし、ローカル NetBackupCLI ユーザーを作成できます。その場合、NetBackup Appliance シェルメニューから `Manage > NetBackupCLI > Create` コマンドを実行します。
- 既存のアプライアンスユーザーとユーザー名、ユーザー ID、またはグループ ID が同じ場合、新しいユーザーまたはユーザーグループはそのアプライアンスに追加できません。
- アプライアンスローカルユーザーまたは NetBackupCLI ユーザーですでに使用されているユーザーグループ名またはユーザー名は使用しないでください。また、LDAP、AD、または NIS ユーザーに admin または maintenance といったアプライアンスのデフォルト名を使用しないでください。
- アプライアンスは、LDAP または NIS 構成の ID マッピングを処理しません。Veritas アプライアンスユーザーの場合に限り、1000～1999 のユーザー ID とグループ ID の範囲を予約することをお勧めします。
- アプライアンスソフトウェアバージョン 4.0 以降、ゲストユーザーと既存のローカルユーザーはユニバーサル共有の CIFS にアクセスできません。バージョン 4.0 以降にアップグレードした後、次の操作により、ユニバーサル共有の CIFS へのアクセス権をこれらのユーザーに付与できます。
  - ゲストユーザー: 新しいローカルユーザーを作成してゲストユーザーを置き換えます。
  - 既存のローカルユーザー: これらのユーザーのパスワードを変更します。
- NetBackup appliance は、パッチやインストールファイルの保存、サポートへのログのアップロード、外部サーバーへのログの転送、OST プラグインのアップロードなどの内部操作の一部に一般的な CIFS 共有を使用します。
  アプライアンスのソフトウェアバージョン 4.0 以降では、admin ユーザーを除くすべてのローカルユーザー、Active Directory ユーザー、およびユーザーグループによる一般的な CIFS 共有へのアクセスを管理する必要があります。一般的な CIFS 共有へのアクセスを管理するには、`Settings > Security > Authentication > CIFSShare` コマンドを使用します。

- ゲストユーザー: 新しいローカルユーザーを作成してゲストユーザーを置き換えます。
- 既存のローカルユーザー: これらのユーザーのパスワードを変更します。

p.14 の「NetBackup Appliance のユーザー認証について 」を参照してください。

LDAP ユーザーの認証について

NetBackup appliance は組み込みのプラガブル認証モジュール (PAM) プラグインを使って LDAP (Lightweight Directory Access Protocol) ユーザーの認証をサポートします。この機能により、LDAP ディレクトリサービスに属しているユーザーを NetBackup appliance にログオンできるように追加して認証できます。LDAP は、UNIX サービスによってインストールされるスキーマを持つ別の種類のユーザーディレクトリとして認識されます。

LDAP ユーザー認証を使うための前提条件

アプライアンスで LDAP ユーザー認証を使用するための前提条件と必要条件を以下に示します。

- LDAP スキーマは RFC 2307 または RFC 2307bis に準拠する必要があります。
- Active Directory サーバーで UNIX モードを有効にする必要があります。
- 次のファイアウォールポートを開く必要があります。
  - LDAP 389
  - LDAP OVER SSL/TLS 636
  - HTTPS 443
- LDAP サーバーが利用できること、またそれがアプライアンスに登録するユーザーとユーザーグループで設定されていることを確認します。

  メモ: ベストプラクティスとして、アプライアンスのローカルユーザーまたは NetBackupCLI ユーザーにすでに使われているグループ名またはユーザー名は使わないでください。また、LDAP ユーザーのアプライアンスのデフォルト名 admin または maintenance を使わないでください。

- アプライアンスは、LDAP 構成の ID マッピングを処理しません。Veritas アプライアンスユーザーの場合に限り、1000～1999 のユーザー ID とグループ ID の範囲を予約することをお勧めします。

LDAP ユーザー認証の構成方法

新しい LDAP ユーザーとユーザーグループをアプライアンスに登録する前に、LDAP サーバーと通信するようにアプライアンスを構成する必要があります。構成が完了すると、アプライアンスは LDAP サーバーの認証用ユーザー情報にアクセスできます。

LDAP ユーザー認証を構成するには、次のオプションのいずれかを使用します。

- NetBackup Appliance Web コンソールの［設定 (Settings)］>［認証 (Authentication)］>［LDAP］。
- NetBackup Appliance シェルメニューから `Settings > Security > Authentication > LDAP`。

LDAP ユーザー認証をアプライアンス上で構成および管理するための詳細な手順については、『NetBackup Appliance 管理者ガイド』と『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

2FA

アプライアンスリリース 3.2 以降の NetBackup Appliance では、NetBackup Web UI を使用する Active Directory (AD) または Lightweight Directory Access Protocol (LDAP) ドメインユーザーの 2 要素認証 (2FA) がサポートされます。以下、3.2 リリースの 2FA サポートについて説明します。

- nbasecadmin ユーザーまたは NetBackup 管理者の役割を持つユーザーは、NetBackup Web UI の 2FA を構成できます。
- 2FA のサポート対象は、NetBackup™ Web UI を使用する AD または LDAP ドメインユーザーのみです。現在、NetBackup Appliance シェルメニューまたは NetBackup Appliance Web コンソールを使用する場合、2FA 機能はサポートされません。
- 2FA を構成するには、アプライアンスで AD または LDAP がすでに構成されている場合でも、NetBackup のために別の AD または LDAP を構成する必要があります。2FA を有効にする方法について詳しくは、次のトピックを参照してください。
  p.27 の「スマートカードとデジタル証明書を使用した認証について」を参照してください。

Active Directory ユーザーの認証について

NetBackup appliance は組み込みのプラガブル認証モジュール (PAM) プラグインを使って、Active Directory (AD) ユーザーの認証をサポートします。この機能により、AD サービスに属しているユーザーを NetBackup appliance にログオンできるように追加して認証できます。AD は、UNIX サービスによってインストールされるスキーマを持つ別の種類のユーザーディレクトリとして認識されます。

Active Directory ユーザー認証を使うための前提条件

アプライアンスで AD ユーザー認証を使用するための前提条件と必要条件を以下に示します。

- AD サービスが利用できること、またそれがアプライアンスに登録するユーザーとユーザーグループで設定されていることを確認します。

  メモ: ベストプラクティスとして、アプライアンスのローカルユーザーまたは NetBackupCLI ユーザーにすでに使われているグループ名またはユーザー名は使わないでください。また、admin または maintenance といったアプライアンスデフォルト名を AD ユーザーに使用しないでください。

- 認可されているドメインユーザーのクレデンシャルを利用してアプライアンスで AD サーバーが構成されていることを確認します。
- AD DNS サーバーに DNS 要求を転送できる DNS サーバーを使ってアプライアンスを構成します。または、AD DNS サーバーをネームサービスデータソースとして使うようにアプライアンスを構成します。

Active Directory ユーザー認証の構成方法

新しい AD ユーザーとユーザーグループをアプライアンスに登録する前に、AD サーバーと通信するようにアプライアンスを構成する必要があります。構成が完了すると、アプライアンスは AD サーバーの認証用ユーザー情報にアクセスできます。

次の方法のいずれかを使用して AD 認証を構成します。

- NetBackup Appliance Web コンソールの［設定 (Settings)］>［認証 (Authentication)］>［Active Directory］ページ。
- NetBackup Appliance シェルメニューの `Settings > Security > Authentication > ActiveDirectory`コマンド。

AD ユーザー認証をアプライアンス上で構成および管理するための詳細な手順については、『NetBackup Appliance 管理者ガイド』と『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

2FA

アプライアンスリリース 3.2 以降の NetBackup Appliance では、NetBackup Web UI を使用する Active Directory (AD) または Lightweight Directory Access Protocol (LDAP) ドメインユーザーの 2 要素認証 (2FA) がサポートされます。以下、3.2 リリースの 2FA サポートについて説明します。

- nbasecadmin ユーザーまたは NetBackup 管理者の役割を持つユーザーは、NetBackup Web UI の 2FA を構成できます。

- 2FA のサポート対象は、NetBackup™ Web UI を使用する AD または LDAP ドメインユーザーのみです。現在、NetBackup Appliance シェルメニューまたは NetBackup Appliance Web コンソールを使用する場合、2FA 機能はサポートされません。
- 2FA を構成するには、アプライアンスで AD または LDAP がすでに構成されている場合でも、NetBackup のために別の AD または LDAP を構成する必要があります。2FA を有効にする方法について詳しくは、次のトピックを参照してください。

p.27 の「スマートカードとデジタル証明書を使用した認証について」を参照してください。

スマートカードとデジタル証明書を使用した認証について

NetBackup Web UI は、デジタル証明書またはスマートカード (CAC と PIV を含む) による、AD (Active Directory) または LDAP (Lightweight Directory Access Protocol) ドメインユーザーに対する認証をサポートしています。この認証方法はアプライアンスプライマリサーバーのドメインごとに 1 つの AD または LDAP ドメインのみサポートし、ローカルドメインのユーザーは使用できません。LDAP がアプライアンスですでに構成されている場合でも、NetBackup に LDAP を構成する必要があります。

メモ: この認証方法を使用するそれぞれのアプライアンスプライマリサーバードメインに対して、この構成を個別に実行します。

ドメインユーザーのアクセスルールを追加したり、スマートカード認証用にドメインを構成したりする前に、AD ドメインまたは LDAP ドメインを追加してください。`vssat` コマンドを使用して、AD ドメインまたは LDAP ドメインを追加します。

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

1. NetBackupCLI ユーザーとしてアプライアンスプライマリサーバーにログオンします。
2. `vssat` コマンドを実行します。

   ```
   vssat addldapdomain -d DomainName -s server_URL -u user_base_DN
   -g group_base_DN -t schema_type -m admin_user_DN
   ```

   上記のコマンドの変数を次の説明に従って置き換えます。

   - *DomainName* は、LDAP ドメインを一意に識別するシンボリック名です。
   - *server_URL* は、指定したドメインの LDAP ディレクトリサーバーの URL です。LDAP サーバーの URL は、`ldap://` または `ldaps://` で始まる必要があります。`ldaps://` で始まる場合は、指定した LDAP サーバーが SSL 接続を要求することを示します。たとえば、`ldaps://my-server.myorg.com:636` です。

- *user_base_DN* は、ユーザーコンテナの LDAP 識別名です。たとえば、ou=user,dc=mydomain,dc=myenterprise,dc=com です。
- *group_base_DN* は、グループコンテナの LDAP 識別名です。たとえば、ou=group,dc=mydomain,dc=myenterprise,dc=com です。
- *schema_type* には、使用する LDAP スキーマの種類を指定します。サポート対象のデフォルトのスキーマの種類は、rfc2307 と msad の 2 つです。
- *admin_user_DN* は、管理ユーザーまたはユーザーコンテナの検索権限を持つユーザーの DN、または UserBaseDN で指定したユーザーサブツリーを含む文字列です。匿名ユーザーを含むすべてのユーザーがユーザーコンテナを検索できる場合は、このオプションを空の文字列として構成できます。たとえば、--admin_user= です。この構成は、ユーザーコンテナの検索をすべてのユーザーに許可します。

3 vssat validateprpl を使用して、指定した AD または LDAP ドメインが正常に追加されたことを確認します。vssat コマンドと次のオプションを使用することもできます。

- vssat removeldapdomain は、認証ブローカーから LDAP ドメインを削除します。
- vssat validategroup は、指定したドメインのユーザーグループの有無を確認します。
- vssat validateprpl は、指定したドメインのユーザーの有無を確認します。

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

役割ベースのアクセス制御の構成

NetBackup に AD ドメインと LDAP ドメインを追加した後、nbasecadmin ユーザーを使用して NetBackup Web UI にログオンし、NetBackup Web UI の役割ベースのアクセス制御を構成できます。NetBackup appliance ユーザーの RBAC の構成について詳しくは、『NetBackup Web UI セキュリティ管理者ガイド』を参照してください。

スマートカードまたはデジタル証明書の認証の構成

nbasecadmin ユーザーを使用して NetBackup Web UI にログオンし、スマートカードまたはデジタル証明書の認証を構成できます。構成に必要な次の手順を実行する方法については、『NetBackup Web UI セキュリティ管理者ガイド』を参照してください。

- スマートカードまたはデジタル証明書を使用してユーザーを認証するように NetBackup Web UI を構成する。
- スマートカード認証の構成を編集する。
- スマートカード認証に使用される CA 証明書を追加する。

- スマートカード認証に使用される CA 証明書を削除する。

Kerberos-NIS ユーザーの認証について

NetBackup appliance は組み込みのプラガブル認証モジュール (PAM) プラグインを使ってネットワーク情報サービス (NIS) ユーザーの認証をサポートします。この機能により、NIS ディレクトリサービスに属しているユーザーを NetBackup appliance にログオンできるように追加して認証できます。NIS は、UNIX サービスによってインストールされるスキーマを持つ別の種類のユーザーディレクトリとして認識されます。

NIS ユーザーを認証するようにアプライアンスを構成するには、Kerberos 認証が必要です。NIS ユーザーが登録されるようにアプライアンスを設定するには、既存の Kerberos サービスを NIS ドメインに関連付ける必要があります。

NIS ユーザー認証と Kerberos を併用するための前提条件

アプライアンスで NIS ユーザー認証を使うための前提条件と必要条件を以下に示します。

- NIS ドメインが利用可能で、アプライアンスに登録するユーザーとユーザーグループが設定されていることを確認します。
- アプライアンスは、NIS 構成の ID マッピングを処理しません。Veritas アプライアンスユーザーの場合に限り、1000～1999 のユーザー ID とグループ ID の範囲を予約することをお勧めします。

  メモ: ベストプラクティスとして、アプライアンスのローカルユーザーまたは NetBackupCLI ユーザーにすでに使われているグループ名またはユーザー名は使わないでください。また、NIS ユーザーのアプライアンスのデフォルト名 admin または maintenance を使わないでください。

- Kerberos サーバーが利用可能で、NIS ドメインと通信できるように適切に構成されていることを確認します。
- Kerberos には厳しい時間要件があるため、常に NTP サーバーを利用してアプライアンス、NIS サーバー、Kerberos サーバー間の時間を同期します。

Kerberos による NIS ユーザー認証の構成方法

新しい NIS ユーザーとユーザーグループをアプライアンスに登録する前に、NIS サーバーおよび Kerberos サーバーと通信するようにアプライアンスを構成する必要があります。構成が完了すると、アプライアンスは認証のために NIS ドメインユーザー情報にアクセスできます。

Kerberos-NIS 認証を構成するには、次のいずれかの方法を使います。

- NetBackup Appliance Web コンソールの［設定 (Settings)］>［認証 (Authentication)］>［Kerberos-NIS］ページ
- NetBackup Appliance シェルメニューの `Settings > Security > Authentication > Kerberos`コマンド。

Kerberos-NIS ユーザー認証をアプライアンス上で構成および管理するための詳細な手順については、『NetBackup Appliance 管理者ガイド』と『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

アプライアンスのログインバナーについて

NetBackup appliance では、ユーザーがアプライアンスにログオンしようとすると表示されるテキストバナーを設定できます。ログインバナーを使うと、さまざまな種類のメッセージをユーザーに伝えることができます。ログインバナーの一般的な用途には、著作権、警告メッセージ、および会社方針情報の表示があります。

また、NetBackup 管理コンソールもログインバナーをサポートしています。デフォルトでは、アプライアンスのログインバナーを設定しても、NetBackup でそのバナーは使いません。ただし、アプライアンスのログインバナーの設定時に、ユーザーが NetBackup 管理コンソールにログインするときに必ずバナーが表示されるように、バナーを NetBackup に伝播できます。

表 2-5 では、ログインバナーをサポートするアプライアンスインターフェースを説明します。ログインバナーを設定すると、NetBackup Appliance シェルメニューや SSH などのバナーをサポートするアプライアンスの各インターフェースに表示されます。ただし、必要に応じて、NetBackup 管理コンソールのログインバナーのオンとオフを切り替えることができます。

表 2-5　ログインバナーをサポートするアプライアンスインターフェース

インターフェース	注意事項
NetBackup Appliance シェルメニュー	NetBackup Appliance シェルメニューにログインしようとすると、まずログインバナーが表示されます。
IPMI コンソールセッション	ユーザー名を入力すると、パスワードが要求される前に、ログインバナーが IPMI コンソールセッションで表示されます。
NetBackup Appliance Web コンソール	Web ブラウザからアプライアンスにアクセスすると、ログインバナーが表示されます。このログインバナーは、［同意 (Agree)］ボタンをクリックした場合のみ非表示にできます。

インターフェース	注意事項
NetBackup 管理コンソール (オプション)	ユーザーが NetBackup 管理コンソールを使ってアプライアンスにログインするときに、必ずログインバナーが表示されます。この機能は、NetBackup の一部である既存のログインバナー機能を使っています。詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

NetBackup Appliance シェルメニューの`Settings > Notifications > LoginBanner`を使用してログインバナーを構成します。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。

または、[設定 (Settings)] > [通知 (Notifications)] > [ログインバナー (LoginBanner)]の順に選択して NetBackup Appliance Web コンソールでログインバナーを構成します。詳しくは、『NetBackup appliance 管理者ガイド』を参照してください。

ユーザー名とパスワードの仕様について

NetBackup appliance のユーザーアカウントのユーザー名は、選択した認証システムが受け入れる形式にする必要があります。表 2-6に、ユーザーの種類ごとのユーザー名の仕様の一覧を表示します。

メモ: `Manage > NetBackupCLI > Create` コマンドを使って、NetBackupCLI ロールを持つローカルユーザーを作成します。すべてのローカルユーザーとパスワードの仕様はこれらのユーザーに適用されます。

表 2-6 ユーザー名の仕様

説明	管理者 (ローカルユーザー)	NetBackupCLI (ローカルユーザー)	登録済みのリモートユーザー
最大長	適用される制限なし	適用される制限なし	LDAP、AD、NIS ポリシーによって判断
最小長	2 文字	2 文字	LDAP、AD、NIS ポリシーによって判断
制限事項	ユーザー名の先頭に次のものを指定することはできません。 ■ 番号 ■ 特殊文字	ユーザー名の先頭に次のものを指定することはできません。 ■ 番号 ■ 特殊文字	LDAP、AD、NIS ポリシーによって判断

説明	管理者 (ローカルユーザー)	NetBackupCLI (ローカルユーザー)	登録済みのリモートユーザー
スペースの包含	ユーザー名にスペースを含めることはできません。	ユーザー名にスペースを含めることはできません。	LDAP、AD、NIS ポリシーによって判断

パスワードの仕様

NetBackup appliance パスワードポリシーはアプライアンスのセキュリティを高めるために更新されました。アプライアンスのユーザーアカウントのパスワードは、選択した認証システムが受け入れる形式にする必要があります。表 2-7は、各ユーザー形式のパスワードの仕様の一覧を表示します。

表 2-7　　パスワードの仕様

説明	管理者 (ローカルユーザー)	NetBackupCLI (ローカルユーザー)	登録済みのリモートユーザー
最大長	適用される制限なし	適用される制限なし	LDAP、AD、NIS ポリシーによって判断
最小長	パスワードは少なくとも 8 文字にする必要があります。	パスワードは少なくとも 8 文字にする必要があります。	LDAP、AD、NIS ポリシーによって判断
要件	■ 1 つの大文字 ■ 1 つの小文字 (a から z) ■ 1 つの数字 (0 から 9) ■ 辞書に記載されている単語は弱いパスワードと見なされ、受け入れられません。 ■ 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。	■ 1 つの大文字 ■ 1 つの小文字 (a から z) ■ 1 つの数字 (0 から 9) ■ 辞書に記載されている単語は弱いパスワードと見なされ、受け入れられません。 ■ 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。	LDAP、AD、NIS ポリシーによって判断
スペースの包含	パスワードにスペースを含めることはできません。	パスワードにスペースを含めることはできません。	LDAP、AD、NIS ポリシーによって判断

説明	管理者 (ローカルユーザー)	NetBackupCLI (ローカルユーザー)	登録済みのリモートユーザー
パスワードの最短期限	0 日	0 日 **メモ:** NetBackup Appliance シェルメニューの `Settings > Security > Authentication > LocalUser` コマンドを使って、ユーザーパスワード保存期間を管理できます。 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。	LDAP、AD、NIS ポリシーによって判断
パスワードの最長期限	99999 日 (期限切れになりません)	99999 日 (期限切れになりません)	LDAP、AD、NIS ポリシーによって判断
パスワード履歴	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。	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。	LDAP、AD、NIS ポリシーによって判断
パスワードの有効期限	パスワードの期限が切れませんので、適用されません	`Settings > Security > Authentication > LocalUser` コマンドを使って、NetBackupCLI ユーザーパスワードを管理します。	LDAP、AD、NIS ポリシーによって判断
パスワードロックアウト	なし	なし	LDAP、AD、NIS ポリシーによって判断
ロックアウトの期間	なし	なし	LDAP、AD、NIS ポリシーによって判断

警告: アプライアンスでは、`passwd` などのメンテナンスのアカウントパスワードはサポートされません。これらのタイプのパスワードは、システムがアップグレードされると上書きされます。メンテナンスのアカウントパスワードを変更するには NetBackup Appliance シェルメニューを使用します。

パスワード保護

NetBackup appliance では、次のパスワード保護対策を導入しています。

- SHA-512 ハッシュアルゴリズムを使用して、お客様がアクセス可能なすべてのローカルアプライアンスのユーザー (ローカルユーザー、NetBackupCLI ユーザー、管理者ユーザー、メンテナンスユーザー) のパスワードを保護します。新しいローカルアプライアンスユーザーを作成する場合、または既存のローカルアプライアンスユーザーのパスワードを変更する場合、必ず SHA-512 を使用してパスワードがハッシュ化されます。

  メモ: 2.6.1.1 より前の NetBackup Appliance ソフトウェアバージョンからアップグレードする場合、Veritasは、アップグレード後にすべてのローカルアプライアンスユーザーのパスワードを変更して、最新のデフォルトの SHA-512 ハッシュアルゴリズムを使用することをお勧めします。

- パスワード履歴は 7 に設定されているため、過去 7 個までの古いパスワードが保護され、ログに記録されます。古いパスワードを新しいパスワードとして使うことを試みると、アプライアンスはトークン操作エラーを表示します。
- 送信中のパスワードには、以下が含まれています。
  - パスワードが SSH プロトコルによって保護されている場所での SSH ログイン。
  - HTTPS 通信によってパスワードが保護されている場所での NetBackup Appliance Web コンソールログイン。

パスワードについて詳しくは、『NetBackup Appliance 管理者ガイド』を参照してください。

STIG 準拠パスワードポリシールールについて

STIG オプションを有効にすると、NetBackup Appliance に高度なセキュリティパスワードポリシーが自動的に適用され、STIG (Security Technical Implementation Guide) に準拠できます。

STIG オプションを有効にしても、デフォルトのポリシーを適用して作成した現在のユーザーパスワードはすべて引き続き有効です。ユーザーパスワードを変更する場合は、STIG 準拠ポリシールールに従う必要があります。

STIG 準拠パスワードポリシールールを次に示します。

- 最小文字数: 15
- 数字の最小文字数: 1
- 小文字の最小文字数: 1
- 大文字の最小文字数: 1

- 特殊文字の最小文字数: 1
- 同じ文字が連続する最大数: 2
- 同じクラスの文字が連続する最大数: 4
- 使用する異なる文字の最小数: 8
- 1 つのパスワードを変更するまでの最小日数: 1
- 1 つのパスワードを変更するまでの最大日数: 60
- 辞書にある言葉は無効で、使用できない
- 過去 7 回分のパスワードは再利用できない

メモ: インターフェースに表示されるパスワードポリシーは、他の言語に翻訳されません。パスワードポリシーは、日本語および中国語のインターフェースで英語で表示されます。

ログインのロックアウトの適用

STIG オプションを有効にすると、15 分以内に 3 回連続して誤ったパスワードを入力したユーザーにログインのロックアウトが適用されます。ロックアウトの状態は、7 日間続きます。ロックアウトの状態を解除するには、`Settings > Security > Authentication > AccountStatus > UnlockAccounts` コマンドを使用します。

STIG が有効なアプライアンスでのメンテナンスアカウントパスワードの変更

アプライアンスリリース 3.1.2 以降、STIG パスワード寿命ポリシーにより、次のシナリオでメンテナンスアカウントパスワードの変更が遅れます。

- STIG オプションを有効にした後の 24 時間。
- STIG が有効なアプライアンスを 3.1.2 以降にアップグレードした後の 24 時間。

これらのいずれかのイベントの 24 時間以内にメンテナンスアカウントパスワードを変更しようとすると失敗します。メンテナンスアカウントパスワードを変更するには、これらのイベントの後、少なくとも 24 時間待ちます。

p.103 の「NetBackup appliance の OS STIG の強化」を参照してください。

3

ユーザー権限の確認

この章では以下の項目について説明しています。

NetBackup appliance におけるユーザー認可について

NetBackup appliance は、ユーザーアカウントを使用して管理します。ローカルユーザーアカウントを作成したり、リモートディレクトリサービスに属するユーザーとユーザーグループを登録したりすることができます。新しいユーザーアカウントがアプライアンスにログオンしてアクセスするには、最初にそのアカウントと役割を承認する必要があります。デフォルトでは、新しいユーザーアカウントには割り当てられた役割がないので、役割が付与されるまでログオンできません。

表 3-1 NetBackup appliance のユーザー役割

役割	説明
管理者 (Administrator)	管理者役割が割り当てられているユーザーアカウントには、NetBackup appliance を管理するための管理権限が付与されます。管理者ユーザーには、NetBackup Appliance Web コンソールと NetBackup Appliance シェルメニューのすべての機能へのログオン、表示、および実行が許可されています。これらのユーザーアカウントには、アプライアンスにログオンし、NetBackup コマンドをスーパーユーザー権限で実行できる権限があります。 p.42 の「管理者ユーザーのロールについて」を参照してください。
NetBackupCLI	NetBackupCLI ロールが割り当てられているユーザーアカウントは、限定的な一連の NetBackup CLI コマンドのみを実行でき、NetBackup ソフトウェアディレクトリの範囲外にはアクセスできません。これらのユーザーがアプライアンスにログインすると、NetBackup を管理できる制限付きシェルメニューが表示されます。NetBackupCLI ユーザーには、NetBackup Appliance Web コンソールと NetBackup Appliance シェルメニューへのアクセス権はありません。 p.42 の「NetBackupCLI ユーザーロールについて」を参照してください。
AMSadmin	AMSadmin 役割が割り当てられたユーザーアカウントには、AMS でホストされている Appliance Manager にアクセスするための管理権限が付与されます。AMSadmin ユーザーは Appliance Manager ですべての機能を実行し、複数のアプライアンスを一元管理することができます。AMSadmin ユーザーは AMS の NetBackup Appliance シェルメニューにログオンすることはできません。管理者は、AMSadmin ユーザーを作成できます

次に、NetBackup appliance の認証の特徴の一部の一覧を示します。

- パスワード保護によるログインによってアプライアンスへの意図しないアクセスを防止する機能。
- 共有データへのアクセス権は、権限があるアプライアンスユーザーと NetBackup 処理のみに提供します。
- アプライアンス内に格納されているデータは、アプライアンスに対する管理者のクレデンシャルを把握している悪意のあるユーザーによる意図しない修正や削除から自身を保護することは本質的にできません。
- NetBackup Appliance シェルメニューへのネットワークアクセスは、SSH と、HTTPS を介した NetBackup Appliance Web コンソールを通してのみ許可。また、キーボー

ドとモニターをアプライアンスに直接接続し、管理者のクレデンシャルを使ってログオンすることもできます。

- FTP、Telnet、rlogin へのアクセスは、すべてのアプライアンスで無効になります。

メモ: ソフトウェアバージョン 3.1 以降では、NetBackup appliance はログイン試行を制限して、STIG 機能が有効になっている場合にのみロックアウトポリシーを適用します。詳しくは、トピック p.34 の「STIG 準拠パスワードポリシールールについて」を参照してください。を参照してください。

メモ: NetBackup Appliance リリース 3.1.2 以降、パッケージ化された Telnet が VxOS から削除され、STIG 機能が NetBackup Appliance で有効になっているときにこの機能に準拠するようになりました。APPSOL-80036 and APPSOL89038, Jay Vasa - Sangria TeamTelnet プロトコルは安全ではなく、暗号化もされていません。暗号化されていない伝送媒体を使用すると、権限のないユーザーにクレデンシャルが盗まれる可能性があります。セッションを暗号化し、セキュリティを強化する ssh パッケージが、VxOS に含まれています。

NetBackup Appliance ユーザーの認可について

表 3-2では、NetBackup Appliance Web コンソールと NetBackup Appliance シェルメニューを使用して新しいユーザーまたはユーザーグループと既存のユーザーまたはユーザーグループを認可するためのオプションについて説明します。

表 3-2 ユーザー認可管理

作業	NetBackup Appliance Web コンソール	NetBackup Appliance シェルメニュー
ユーザーの管理	次のオプションは[設定(Settings)] > [認証(Authentication)] > [User Management(ユーザー管理)]にあります。 ■ アプライアンスに追加されているすべてのユーザーを表示する。 ■ 単一のユーザーグループに属しているすべてのユーザーを展開して表示する。 ■ ローカルユーザーを追加または削除する。 ■ LDAP/AD/Kerberos-NIS ユーザーとユーザーグループを追加または削除する。	`Settings > Security > Authentication` コマンドを使用して、アプライアンスユーザーを追加、削除、表示します。 p.19 の「ユーザー認証の設定について」を参照してください。
ユーザー権限(役割)の管理	次のオプションは[設定 (Settings)] > [認証 (Authentication)] > [User Management (ユーザー管理)]にあります。 ■ ユーザーとユーザーグループの管理者役割を付与し、取り消します。 ■ ユーザーとユーザーグループの NetBackupCLI 役割を付与し、取り消します。 ■ 管理者役割を持つ登録済みユーザーグループのメンバーを同期します。	`Main > Settings > Security > Authorization` では次のコマンドとオプションが利用可能です。 ■ `Grant` アプライアンスに追加されている特定のユーザーとユーザーグループに管理者役割と NetBackupCLI 役割を与えます。 ■ `List` アプライアンスに追加されているユーザーとユーザーグループを、それに指定されている役割も含めて、すべて一覧表示します。 ■ `Revoke` アプライアンスに追加されている特定のユーザーとユーザーグループの管理者役割と NetBackupCLI 役割を取り消します。 ■ `SyncGroupMembers` 登録済みユーザーグループのメンバーを同期します。

ユーザー管理に関するメモ

- 既存のローカルユーザーに NetBackupCLI 役割を付与することはできません。ただし、ローカル NetBackupCLI ユーザーを作成できます。その場合、NetBackup Appliance シェルメニューから `Manage > NetBackupCLI > Create` コマンドを実行します。
- NetBackupCLI 役割はいつでも最大 9 個のユーザーグループに割り当てることができます。
- Active Directory (AD) のユーザーグループ名およびユーザー名で、ハイフン文字を使用できます。ハイフンは、ユーザー名またはユーザーグループ名の最初と最後の文字の間で使用される必要があります。AD のユーザー名およびユーザーグループ名の最初と最後にハイフンを使うことはできません。
- NetBackup Appliance Web コンソールからは、グループのすべてのユーザーを最大 2000 ユーザーまでリストできます。2000 を超えるユーザーが含まれるグループのユーザーすべての一覧を表示するには、NetBackup Appliance シェルメニューから `List` コマンドを使用します。

NetBackup appliance ユーザー役割権限

ユーザー役割により、システムの操作やシステム設定の変更に対してユーザーが認可されるアクセス権が決まります。このトピックで説明するユーザー役割は LDAP ユーザー、Active Directory (AD) ユーザー、NIS ユーザーに固有です。

次は、アプライアンスユーザー役割とそれに関連付けられる権限の説明です。

表 3-3　　ユーザー役割と権限

ユーザー役割	権限
NetBackupCLI	ユーザーは NetBackup CLI のみにアクセスできます。 p.42 の「NetBackupCLI ユーザーロールについて」を参照してください。
管理者 (Administrator)	ユーザーは次にアクセスできます。 ■ NetBackup Appliance Web コンソール ■ NetBackup Appliance シェルメニュー ■ NetBackup 管理コンソール p.42 の「管理者ユーザーのロールについて」を参照してください。

ユーザー役割	権限
AMSadmin	AMSadmin 役割が割り当てられたユーザーアカウントには、AMS でホストされている Appliance Management Console にアクセスするために必要な管理者権限が付与されます。AMS ユーザーは Appliance Management Console ですべての機能を実行し、複数のアプライアンスを一元管理できます。AMS ユーザーは AMS のNetBackup Appliance シェルメニューにログオンすることはできません。管理者は、AMS ユーザーを作成できます。

役割は個別ユーザーに適用できます。あるいは、複数のユーザーを含むグループに適用できます。

両方のユーザー役割に対する権限をユーザーに与えることはできません。ただし、次のシナリオでは、NetBackupCLI ユーザーには NetBackup Appliance シェルメニューへのアクセス権限も与えられます。

- NetBackupCLI 役割があるユーザーは、管理者役割が割り当てられたグループにも入ります。
- 管理者役割があるユーザーは、NetBackupCLI 役割が割り当てられたグループにも入ります。

メモ: NetBackupCLI と NetBackup Appliance シェルメニューへの権限をユーザーに与えるとき、追加の手順が必要になります。NetBackup Appliance シェルメニューにアクセスするには、NetBackup CLI から `switch2admin` コマンドを入力する必要があります。

ユーザーとユーザーグループには次のように特権を与えることができます。

- NetBackup Appliance Web コンソールから、[設定 (Settings)] > [認証 (Authentication)] > [ユーザー管理 (User Management)]ページで、[権限を付与 (Grant Permissions)]リンクをクリックします。
- NetBackup Appliance シェルメニューから、`Settings > Security > Authorization` ビューで次のコマンドを使用します。

```
Grant Administrator Group
Grant Administrator Users
Grant NetBackupCLI Group
Grant NetBackupCLI Users
Grant AMS Group
Grant AMS Users
```

p.19 の「ユーザー認証の設定について」を参照してください。

p.38 の「NetBackup Appliance ユーザーの認可について」を参照してください。

管理者ユーザーのロールについて

NetBackup appliance は、アプライアンス上のバックアップデータへの無断アクセスを回避するため、アクセス制御メカニズムを提供しています。これらのメカニズムには、アプライアンスの構成の修正、アプライアンスの監視などのための昇格システム特権を提供する管理用ユーザーアカウントが含まれます。管理者役割が割り当てられているユーザーのみに、NetBackup appliance を構成および管理する権限があります。

管理者役割は、アプライアンスの構成または拡張ディスクストレージに含まれるバックアップデータへの権限のない不適切な改変を防ぐために、権限のあるシステム管理者のみに付与する必要があります。

管理者ユーザーは SSH を通した NetBackup Appliance シェルメニューか、または HTTPS を介した NetBackup Appliance Web コンソールを使ってアプライアンスにアクセスできます。

管理者ユーザーはスーパーユーザーとして次のタスクをすべて実行できます。

- アプライアンスの初期設定の実行。
- ハードウェア、ストレージ、SDCS ログの監視。
- ストレージ構成、追加サーバー、ライセンスなどの管理。
- [日時(Date and Time)]、[ネットワーク(Network)]、[通知(Notification)]などの構成の更新。
- アプライアンスのリストア。
- アプライアンスの廃止。
- アプライアンスへのパッチ適用。
- 共有のマウントまたはマッピング。次の制限事項が適用されます。
  - Windows: Windows CIFS 共有のマウントまたはマップは、ローカルの管理者ユーザーにのみ許可されます。
  - Linux: ルートアクセスアカウントを持つユーザーのみが NFS 共有を直接マウントする mount コマンドを実行できます。
- 管理者役割が割り当てられたローカルユーザー、LDAP または Active Directory (AD) ユーザー、ユーザーグループは、NetBackup Java コンソールにアクセスできます。

NetBackupCLI ユーザーロールについて

NetBackupCLI ユーザーは、すべての NetBackup コマンドを実行したり、ログを表示したり、NetBackup タッチファイルを編集したり、NetBackup 通知スクリプトを編集したりできます。NetBackupCLI ユーザーは、スーパーユーザー権限による NetBackup コマン

ドの実行のみに制限されていて、NetBackup のソフトウェアディレクトリの範囲外にはアクセスできません。これらのユーザーがログインすると、NetBackup コマンドを実行できる制限付き Shell が表示されます。NetBackupCLI ユーザーはホームディレクトリを共有し、NetBackup Appliance Web コンソールまたは NetBackup Appliance シェルメニューにはアクセスできません。

NetBackupCLI 役割はいつでも最大 9 個のユーザーグループに割り当てることができます。ローカル NetBackupCLI ユーザーを作成するには、`Manage > NetBackupCLI > Create` コマンドを NetBackup Appliance シェルメニューから使用します。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: 既存のローカルユーザーに NetBackupCLI 役割を付与することはできません。

表 3-4に、NetBackupCLI ユーザーの権限と制限を示します。

表 3-4 アプライアンス NetBackupCLI ユーザーの権限と制限

権限	制限事項
NetBackupCLI ユーザーは、NetBackup Appliance シェルメニューを使って次の操作を実行できます。 ■ NetBackup CLI を実行して、NetBackup ディレクトリとファイルにアクセスする。 ■ `cp-nbu-notify` コマンドを使って、NetBackup 通知スクリプトを変更または作成する。 ■ 次の NetBackup コマンドを NetBackup CLI を含む次のディレクトリに対して実行します。 ■ `/usr/openv/netbackup/bin/*` ■ `/usr/openv/netbackup/bin/admincmd/*` ■ `/usr/openv/netbackup/bin/goodies/*` ■ `/usr/openv/volmgr/bin/*` ■ `/usr/openv/volmgr/bin/goodies/*` ■ `/usr/openv/pdde/pdag/bin/mtstrmd` ■ `/usr/openv/pdde/pdag/bin/pdcfg` ■ `/usr/openv/pdde/pdag/bin/pdusercfg` ■ `/usr/openv/pdde/pdconfigure/pdde` ■ `/usr/openv/pdde/pdcr/bin/*`	NetBackupCLI ユーザーには次の制限があります。 ■ NetBackupCLI ユーザーは、NetBackup ソフトウェアディレクトリの外部にはアクセスできません。 ■ エディタを使用して `bp.conf` ファイルを直接編集することはできません。`bpsetconfig` コマンドを使用して、属性を設定します。 ■ `cp-nbu-config` コマンドは、`/usr/openv/netbackup/db/config` ディレクトリ内でのみ NetBackup タッチ構成ファイルの作成と編集をサポートします。 ■ `man` または `-h` コマンドを使用して、他のコマンドのヘルプを表示することはできません。

NetBackupCLI ユーザーとして NetBackup コマンドを実行する方法

次のいずれかの方法で、NetBackupCLI ユーザーとしてコマンドを実行します。

- 制限付きシェル
- 絶対パス ["sudo"]。例: bppllist または /usr/openv/netbackup/bin/admincmd/bpplist

特別な指示句の処理を実行する方法

特別な指示句のファイルとコマンドが正しい NetBackup リストまたはパスにない場合、特別な指示句の処理は失敗することがあります。特別な指示句の処理の 1 つの例としては、代替の復元パスを指定する場合があります。

NetBackupCLI ユーザーとして NetBackup コマンドを実行して特別な指示句のファイルにアクセスする必要があるアプライアンスユーザーは、次のことを実行して正常に処理を完了する必要があります。

- NetBackup bpcd allowed list に /home/nbusers パスを追加します。
- /home/nbusers ディレクトリに特別な指示句のコマンドを追加します。

NetBackup bpcd allowed list へのエントリの追加について詳しくは、次のドキュメントの BPCD_WHITELIST_PATH 構成オプションを参照してください。

『NetBackup 管理者ガイド Vol. 1』

『NetBackup コマンドリファレンスガイド』

NetBackup でのユーザー権限の確認について

nbasecadmin アカウントを使用して、NetBackup Web UI にログインし、アプライアンスのローカルユーザーや、LDAP サーバーまたは Active Directory (AD) サーバーに登録済みのユーザーに NetBackup の役割を割り当てることができます。NetBackup の役割ベースのアクセス制御 (RBAC) で割り当てられた役割により、重要度の低い資産や機能へのアクセスを制限しながら、アプライアンスユーザーによる NetBackup での特定のタスクの実行を許可できます。RBAC および NetBackup のユーザー役割管理について詳しくは、『NetBackup Web UI セキュリティ管理者ガイド』を参照してください。

バージョン 3.1.2 または 3.2 で実行されているアプライアンスをアップグレードする場合、NetBackup RBAC によって定義されたすべての非管理者の役割はアップグレード後に失効します。NetBackup 8.3 で導入された新しい RBAC モデルを使用して、既存の RBAC 構成を再構成する必要があります。

RBAC 移行ツールを使用して、既存のバックアップ管理者とセキュリティ管理者の役割を NetBackup 8.3 RBAC モデルに移行できます。RBAC 移行ツールは次の操作を実行します。

- 既存のセキュリティ管理者の役割を、追加されたプリンシパルとともに移行する
- 既存のバックアップ管理者の役割を削除し、そのユーザーを管理者の役割に再び割り当てる

RBAC 移行ユーティリティについて詳しくは、
https://www.veritas.com/support/en_US/article.100047577 を参照してください。

現在構成されているすべての作業負荷管理者とカスタムの役割は、アップグレード後に再構成する必要があります。NetBackup 8.3 RBAC の役割ユーティリティを使用して、最新の役割の定義を追加できます。詳しくは、
https://www.veritas.com/support/en_US/article.100047660 を参照してください。

4

侵入防止、侵入検知システム

この章では以下の項目について説明しています。

NetBackup appliance の Symantec Data Center Security について

メモ: アップグレード後、アプライアンス SDCS エージェントは自動的にアンマネージモードに設定されます。アップグレード前にアプライアンスがマネージモードで動作していた場合は、アップグレードの完了後に必ずアプライアンスをマネージモードにリセットしてください。

また、SDCS 管理サーバーでアプライアンスの IPS および IDS のポリシーも更新する必要があります。アップグレード後、古いポリシーを使用する新しいソフトウェアバージョンを実行しているアプライアンスの管理はできません。新しいポリシーは、NetBackup Appliance Web コンソールの［監視 (Monitor)］>［SDCS のイベント (SDCS Events)］ページからダウンロードできます。また、IPS および IDS のポリシーに設定したカスタム規則やサポートの例外は、アップグレードした後は使用できなくなります。

Symantec Data Center Security: Server Advanced（SDCS）は、データセンターのサーバーを保護するためにシマンテック社が提供するセキュリティソリューションです。SDCS ソフトウェアはアプライアンスに含まれ、アプライアンスソフトウェアのインストール時に自動的に設定されます。SDCS はポリシーベースの保護を提供し、ホストベースの侵入防止と検出技術を使ってアプライアンスを保全します。最小の権限付与による封じ込めで、セキュリティ管理者がデータセンターの複数のアプライアンスを集中的に管理できるようにします。SDCS エージェントは起動時に実行され、カスタマイズされた NetBackup appliance の侵入防止システム (IPS) ポリシーおよび侵入検知システム (IDS) ポリシーをエンフォースします。アプライアンスの SDCS ソリューション全体で次の機能を提供します。

- Linux OS コンポーネントの強化
  OS の脆弱性によりマルウェアが基本ホストシステムの整合性を阻害しないようにするか、またはマルウェアを含めます。
- データ保護
  システム権限に関係なく、アクセスを必要とするプログラムと活動のみにアプライアンスのデータアクセスを限定します。
- アプライアンススタックの強化
  アプリケーションまた信頼されたプログラムおよびスクリプトによって変更が強固に制御されるように、アプライアンスアプリケーションのバイナリと構成の設定がロックダウンされます。
- 検出機能と監査機能の拡張
  補正制御として法規制 (PCI など) に対処する有効で完全な監査証跡を確認するために、重要なユーザーやシステムの処理の表示を拡張します。
- 集中管理モードによる操作
  ユーザーは、SDCS が管理する複数のアプライアンスや他の企業システム全体のセキュリティを統合的に表示するために集約型 SDCS マネージャを使うことができます。

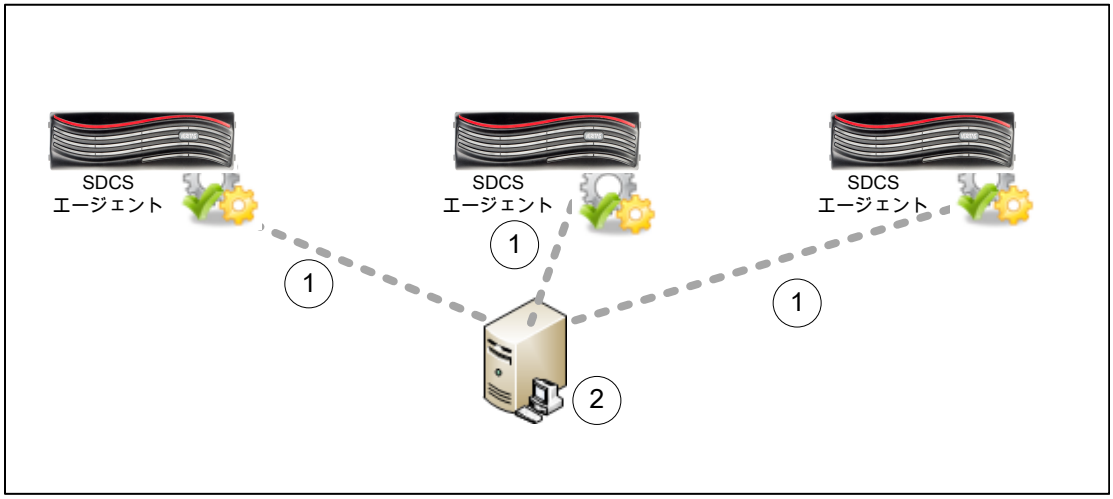
アプライアンスへの SDCS の実装は、アンマネージモードまたはマネージモードで操作できます。デフォルトでは、SDCS はアンマネージモードで動作して、ホストベースの侵入防止と検出技術を使ってアプライアンスを保全します。NetBackup アプライアンスは、SDCS サーバーに接続していないときはアンマネージモードになります。アンマネージモードでは、NetBackup Appliance Web コンソールから SDCS イベントを監視できます。ログイベントを監視するには、[監視]>[SDCS イベント]を使います。イベントは NetBackup Appliance IPS と IDS ポリシーを使って監視されます。これらのポリシーは初期構成のときに自動的に適用されます。特定のイベントをフィルタ処理して表示するには、[ログのフィルタ]をクリックします。

マネージモードでは、アプライアンスの SDCS エージェントは、アプライアンスの保護を継続し、集中管理およびログ分析のために外部 SDCS サーバーにも接続します。マネージモードでは、アプライアンスは SDCS サーバーに接続され、イベントは SDCS 管理コンソールを使って監視されます。このモードでは、1 つの SDCS サーバーを使って複数

のアプライアンスを監視できます。SDCS エージェントは、SDCS サーバーにイベントを送るのに使われる各 NetBackup アプライアンスとともに設定されます。

図 4-1は、マネージモードの SDCS を示します。

図 4-1　　マネージモードでの SDCS 実装



マネージモードを設定するには、SDCS サーバーと管理コンソールをインストールし、次にアプライアンスを SDCS サーバーに接続します。

[監視]>[SDCSイベント]から次を実行します。

- NetBackup Appliance IPS と IDS ポリシーのダウンロード
- SDCS 管理コンソールを使ってこれらのポリシーを適用
- NetBackup アプライアンスをサーバーに接続
- サーバーに接続されたすべての NetBakup アプリケーションのイベントの監視

[監視]>[SDCS イベント]>[SDCSサーバーに接続]から次を実行します。

- SDCS サーバー詳細の追加
- TBD のダウンロード
- SDCS サーバーへの接続

アプライアンスへの SDCS 実装について詳しくは、『NetBackup Appliance セキュリティガイド』を参照してください。

NetBackup appliance の侵入防止システムについて

アプライアンスの侵入防止システム (IPS) は、起動時に自動的に動作する SDCS (Symantec Data Center Security) ポリシーで構成されます。IPS ポリシーは、不要なリソースアクセスの動作がオペレーティングシステムで実行される前に事前に遮断できるインラインのポリシーです。

次のリストには、IPS ポリシー機能の一部が含まれています。

- アプライアンスの OS の処理および共通のアプリケーションのリアルタイムの厳しい制限は以下のとおりです。
  - `nscd` - DNS 要求をキャッシュして、リモート DNS ルックアップを削減します。
  - `cron`
  - `syslog-ng`
  - `klogd`
  - NFS 向けの `rpcd`
    - `rpc.idmapd`
    - `rpc.mountd`
    - `rpc.statd`
    - `rpcbind`
- SDCS エージェント自身のための自己防衛、セキュリティと SDCS の監視機能は損なわれないことを確認します。
- 特定され、信頼されているアプリケーション、ユーザー、ユーザーグループによらない限り、システムバイナリを終了します。
- アプリケーションによる `sbin` などのソフトウェアのインストール、`hosts` ファイルなどのシステム構成設定の変更の試みからシステムを保護する制限です。
- `mknod`、`modctl`、`link`、`mount` などの重要なシステムコールをアプリケーションで実行することを禁止します。
- `/advanceddisk`、`/cat`、`/disk`、`/usr/openv/kms`、`/opt/NBUAppliance/db/config/data` などのバックアップデータに権限のないユーザーやアプリケーションがアクセスすることを禁止します。

NetBackup appliance の侵入検知システムについて

アプライアンスの侵入検知システム (IDS) は、起動時に自動的に動作する SDCS (Symantec Data Center Security) ポリシーで構成されます。IDS ポリシーは、重要なシ

ステムイベントおよび重要な構成の変更を監視し、省略可能なオプションとして対象のイベントに修復操作を実行するリアルタイムポリシーです。

次のリストには、IDS ポリシーが監視するイベントの一部が含まれています。

- ユーザーログイン、ログアウト、試行時に失敗したログオン
- Sudo コマンド
- ユーザーの追加、削除、パスワード変更
- ユーザーグループの追加、削除、メンバーの変更
- システム自動起動オプションの変更
- すべてのシステムディレクトリとファイルに対する変更 (主要システムファイル、主要システム構成ファイル、インストールプログラム、共通デーモンファイルを含む)
- NetBackup のサービス開始と停止
- UNIX ルートキットファイル/ディレクトリ検出、UNIX ワームファイル/ディレクトリ検出、悪意のあるモジュールの検出、疑わしいパーミッション変更の検出などにより検出されたシステムへの攻撃
- 保守、ルートおよび NetBackupCLI ユーザーのためのシェル操作を含めた NetBackup Appliance Web コンソールおよび NetBackup Appliance シェルメニューのすべての動作の監査。

NetBackup アプライアンスの SDCS イベントの見直し

[監視]>[SCSP イベント]ページで、SDCS(Symantec Data Center Security)ログを表示できます。これらの監査ログは、アプライアンスのセキュリティ違反や異常なアクティビティを検出するのに役立ちます。監査ログのイベントには、次の詳細が含まれます。

- 時間 - ログイベントのタイムスタンプを表示します。
- ユーザー - イベントが起きた時ログオンしていたユーザーを表示します。
- 内容 - イベントと関連するリソースの説明を表示します。
- 詳細 - プロセス名、プロセス ID、操作権限、およびサンドボックスの詳細を表示します。
- 重大度 - イベントの重大度を表示します。
- 処理の実施 - イベントが許可されたか拒否されたかを表示します。

SDCS イベントが取り込まれ、表 4-1に記述されている重大度の種類を使って表されます。

表 4-1 SDCS イベントの重大度の種類

重大度の種類	説明	イベントの例

情報 (Information)	重大度が[情報 (Info)]のイベントには、通常のシステム操作についての情報が含まれます。	たとえば、次のメッセージは汎用イベントに関する基本情報を提供します。
		
		`general CLISH message`
		
		`Event source:`
		`SYSLOG PID: 30315`
		`Complete message:`
		`May 21 06:58:55`
		`nb-appliance`
		`CLISH[30315]:`
		`User admin`
		`executed Return`

通知 (Notice)	重大度が[通知 (Notice)]のイベントには、通常のシステム操作についての情報が含まれます。	イベントの実行が成功したことを確認する場合に役立つイベントが、[通知 (Notice)]として記録されます。たとえば、次のメッセージによって、ユーザーはイベントが正常に実行されたことを理解できます。
		
		`successful SUDO to root`
		`Event source: SYSLOG [sudo facility]`
		`Command: /bin/su From`
		
		`Username: AppComm To Username: root`
		`Port: unknown`

重大度の種類	説明	イベントの例
警告 (Warning)	重大度が[警告]のイベントは、SDCS によってすでに処理された予想外の活動または問題を示します。これらの警告メッセージは、ターゲットコンピュータのサービスまたはアプリケーションが適用済みのポリシーに対して不適切に機能していることを示している可能性があります。ポリシー違反を調査した後、必要に応じて、ポリシーを構成し、サービスまたはアプリケーションが特定のリソースにアクセスできるようにします。	たとえば、次のイベントはローカル IP アドレスからの着信接続のような予想外のアクティビティを特定する場合に役立ちます。 `Inbound connection allowed from <IPaddress> to local address.`

主要 (Major)	重大度が[主要 (Major)]のイベントは、[警告 (Warning)]のイベントよりも深刻な影響を示しますが、[重要 (Critical)]のイベントほど影響を与えません。	たとえば、次のイベントは認証されていないアクセスを識別するのに役立ちます。
		
		`General luser message`
		
		`Event source:SYSLOG Complete message: Feb 5 21:57 luser Unauthorized user by luser Denying access to system.`

重要 (Critical)	重大度が[重要 (Critical)]のイベントは、管理者による修正が必要になる場合があるアクティビティまたは問題を示します。	たとえば、予想外の方法でアプライアンスに影響を及ぼす可能性のある重要なイベントを特定する場合に、次のイベントが役立つことがあります。 `Group Membership for "group1" CHANGED from 'admin1' to 'admin2'`

SDCS 監査ログの取り込みについて詳しくは、『NetBackup Appliance 管理者ガイド』を参照してください。

syslog や他のアプライアンスログのようなアプライアンスのオペレーティングシステムログについて詳しくは、p.55 の「NetBackup appliance のログファイルについて」を参照してください。 の説明を参照してください。

NetBackup アプライアンスでのアンマネージモードでの SDCS の実行

アプライアンスへの Symantec Data Center Security（SDCS）の実装は、アンマネージモードまたはマネージモードで操作できます。アンマネージモードはアプライアンスを構成するデフォルトモードです。アンマネージモードの場合、アプライアンスは外部 SDCS サーバーを使わないで保護され、監査されます。アンマネージモードでも、IDS と IPS の両方のポリシーが適用され、起動時にアプライアンスが保護されます。

アンマネージモードは、アプライアンスの単独の担当者であり、主にバックアップ管理に関係する管理者にお勧めします。

SDCS イベントは、NetBackup Appliance Web コンソール（[監視 (Monitor)] > [SDCS イベント (SDCS Events)]）と NetBackup Appliance シェルメニュー (`Main_Menu > Monitor > SDCS`) から監視できます。

NetBackup アプライアンスでのマネージモードでの SDCS の実行

アプライアンスへの SDCS の実装は、アンマネージモードまたはマネージモードで操作できます。マネージモードでは、外部 SDCS サーバーを使って 1 台以上のアプライアンスの SDCS エージェントと通信し、これを管理することができます。SDCS サーバーはマネージモードで使用されているのと同じ IPS および IDS ポリシーを使用します。NetBackup Appliance Web コンソールから SDCS ポリシーをダウンロードできます。

マネージモードはセキュリティ管理者または SDCS に精通している SDCS の既存のお客様のみが使うことを推奨します。

マネージモード使用の利点:

- バックアップ管理者の役割とセキュリティ管理者の役割に応じたツールを別々に提供できます。
- 単一の SDCS サーバーとコンソールを使用して複数のアプライアンスのセキュリティの集中管理を提供します。
- ログをアーカイブし、エクスポートする機能を提供します。
- 警告の監視、報告、セットアップに使用する共通コンソールを提供します。
- データセンターの基準に合うようにシマンテック社のベースラインを基づいて IPS と IDS ポリシーを拡張します。

SDCS マネージモードでアプライアンスを構成する方法

1. SDCS コンソールを使って SDCS サーバーに接続でき、そのサーバーからアプライアンスに接続できることを確認します。

   SDCS コンソールとサーバーソフトウェアが必要な場合は、https://my.veritas.com からダウンロードできます。

2. SDCS コンソールを使ってアプライアンスから IPS ポリシーと IDS ポリシーをダウンロードしてインポートします。これらのポリシーは、NetBackup Appliance Web コンソールの［監視 (Monitor)］>［SDCS イベント (SDCS Events)］から直接ダウンロードできます。

3. アプライアンスを SDCS サーバーに接続します。NetBackup Appliance Web コンソールの［監視 (Monitor)］>［SDCS イベント (SDCS Events)］または NetBackup Appliance シェルメニューの `Monitor > SDCS` から SDCS サーバーに接続できます。

4. SDCS コンソールを使って、接続されているアプライアンスに IPS ポリシーと IDS ポリシーを適用します。

5

ログファイル

この章では以下の項目について説明しています。

NetBackup appliance のログファイルについて

ログファイルは、アプライアンスで発生する可能性がある問題の特定と解決に役立ちます。

NetBackup appliance では、ハードウェア、ソフトウェア、システム、パフォーマンス関連のデータを取得できます。ログファイルは、アプライアンス操作などの情報、未構成ボリュームまたはアレイなどの問題、温度またはバッテリに関する問題、およびその他の詳細を取得します。

表 5-1で、アプライアンスのログファイルにアクセスするために使用できる方法を説明します。

表 5-1 ログファイルの表示

開始	アクセス方法	ログの詳細
NetBackup Appliance Web コンソール	NetBackup Appliance Web コンソールの［モニター (Monitor)］>［SDCS 監査ビュー (SCSP Audit View)］画面を使用して、アプライアンスの監査ログを取得できます。p.50 の「NetBackup アプライアンスの SDCS イベントの見直し」を参照してください。	アプライアンスの監査ログ
NetBackup Appliance シェルメニュー	`Main > Support > Logs > Browse` コマンドを使用して `LOGROOT/>` プロンプトを開きます。 `ls` や `cd`コマンドを使用して、アプライアンスのログディレクトリを走査できます。 p.57 の「Support コマンドの使用によるログファイルの表示」を参照してください。	■ Appliance の構成ログ ■ Appliance のコマンドログ ■ Appliance のデバッグログ ■ NetBackup ログ、Volume Manager ログ、`openv` ディレクトリに含まれている NetBackup ログ ■ Appliance のオペレーティングシステム (OS) インストールログ ■ NetBackup 管理 Web ユーザーインターフェースログと NetBackup Web サーバーログ ■ NetBackup 52xx Appliance のデバイスログ

開始	アクセス方法	ログの詳細
NetBackup Appliance シェルメニュー	`Main > Support > Logs > VxLogView Module ModuleName` コマンドを実行して、Appliance VxUL (統合) ログにアクセスできます。`Main > Support > Share Open` コマンドを実行し、デスクトップを使用して VxUL ログのマップ、共有、コピーを行うこともできます。 p.57 の「Support コマンドの使用によるログファイルの表示」を参照してください。	Appliance 統合ログ: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace` ■ `FTMS` ■ `FTDedupTarget` ■ `TaskService` ■ `AuthService`
NetBackup Appliance シェルメニュー	`Main > Support > DataCollect` コマンドを実行して、ストレージデバイスログを収集できます。 p.60 の「NetBackup Appliance でのデバイスログの収集」を参照してください。	Appliance ストレージデバイスログ
NetBackup Java アプリケーション	NetBackup Java アプリケーションに関する問題が発生した場合、このセクションのスクリプトを使って、サポートに連絡するために必要な情報を集めることができます。	NetBackup Java アプリケーションに関するログ

Support コマンドの使用によるログファイルの表示

次のセクションを使ってログファイルの情報を表示できます。

Support > Logs > Browseコマンドを使用してログファイルを表示する方法

1. NetBackup Appliance シェルメニューで Main_Menu > Support > Logs を使用して参照モードにしたら、Browse コマンドを実行します。LOGROOT/> プロンプトが表示されます。
2. アプライアンスの利用可能なログディレクトリを表示するには、LOGROOT/> プロンプトで ls と入力します。
3. いずれかのログディレクトリで利用可能なログファイルを参照するには、cd コマンドを使用して、選択するログディレクトリにディレクトリを変更します。プロンプトが現在のディレクトリを示すように変わります。たとえば、ディレクトリを OS ディレクトリに変更した場合、プロンプトは LOGROOT/OS/> と表示されます。そのプロンプトから ls コマンドを使用すると、OS ログディレクトリの利用可能なログファイルを表示できます。
4. ファイルを表示するには、less <FILE> または tail <FILE> コマンドを使用します。ファイルは <FILE> で、ディレクトリは <DIR> でマーク付けされます。

p.59 の「Browse コマンドを使用した NetBackup appliance ログファイルの参照場所」を参照してください。

Support > Logs コマンドを使用して NetBackup appliance 統合 (VxUL) ログを表示する方法

1. Support > Logs > VXLogView コマンドを使用して、NetBackup appliance 統合 (VxUL) ログを表示できます。コマンドをシェルメニューに入力し、次のオプションのうちいずれかを使用します。
   - Logs VXLogView JobID *job_id*
     特定のジョブ ID に関するデバッグ情報の表示に使用します。
   - Logs VXLogView Minutes *minutes_ago*
     特定の時間枠に関するデバッグ情報の表示に使用します。
   - Logs VXLogView Module *module_name*
     特定のモジュールに関するデバッグ情報の表示に使用します。
2.

Main_Menu > Support > Logs コマンドを使用して、次の操作を行うこともできます。

- ベリタスのテクニカルサポートにログファイルをアップロードするVeritas
- ログレベルを設定する
- CIFS 共有と NFS 共有をエクスポートまたは削除する

メモ: NetBackup appliance VxUL ログは、cron ジョブまたはスケジュール済みタスクによってアーカイブされなくなりました。さらに、ログの再利用が有効になり、デフォルトのログファイル数が 50 に設定されました。

以上のコマンドを使用する方法について詳しくは『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

p.55 の「NetBackup appliance のログファイルについて」を参照してください。

Browse コマンドを使用した NetBackup appliance ログファイルの参照場所

表 5-2に、Support > Logs > Browse コマンドを実行するとアクセスできるログとログディレクトリの場所を示します。

表 5-2 NetBackup appliance ログファイルの場所

アプライアンスログ	ログファイルの場所
構成ログ	<DIR> APPLIANCE config_nb_factory.log
セルフテストレポート	<DIR> APPLIANCE selftest_report
ホスト変更ログ	<DIR> APPLIANCE hostchange.log
NetBackup ログ、Volume Manager ログ、openv ディレクトリに含まれている NetBackup ログ	<DIR> NBU ■ <DIR> netbackup ■ <DIR> openv ■ <DIR> volmgr
オペレーティングシステム (OS) インストールログ	<DIR> OS boot.log boot.msg boot.omsg messages
NetBackup 重複排除 (PDDE) 構成スクリプトのログ	<DIR> PD pdde-config.log
NetBackup 管理 Web ユーザーインターフェースログと NetBackup Web サーバーログ	<DIR> WEBGUI ■ <DIR> gui ■ <DIR> webserver

アプライアンスログ	ログファイルの場所
デバイスログ	`/tmp/DataCollect.zip` (ソフトウェアバージョン 3.1.2 以降) `/log/DataCollect.zip` (ソフトウェアバージョン 3.2 以降) `Main > Support > Logs > Share Open` コマンドを使用して、ローカルフォルダに `DataCollect.zip` をコピーできます。

p.55 の「NetBackup appliance のログファイルについて」を参照してください。

NetBackup Appliance でのデバイスログの収集

`Main > Support` シェルメニューから `DataCollect` コマンドを使用してデバイスのログを収集できます。これらのデバイスログをベリタスのサポートチームと共有することで、デバイス関連の問題を解決できます。Veritas

DataCollect コマンドは次のログを収集します。

- リリース情報
- ディスクパフォーマンスのログ
- コマンド出力ログ
- iSCSI ログ

メモ: iSCSI ログは /var/log/messages and /var/log/iscsiuio.log にあります。

- CPU 情報
- メモリ情報
- オペレーティングシステムのログ
- Patch ログ
- ストレージログ
- ファイルシステムログ
- Test hardware のログ
- AutoSupport ログ
- ハードウェア情報

- Sysinfo ログ

DataCollect コマンドを使ってデバイスログを収集するには

1. NetBackup Appliance シェルメニューにログオンします。
2. `Main > Support` ビューから次のコマンドを入力して、デバイスログを収集します。

   `DataCollect`

   バージョン 3.1.2 以前のアプライアンスソフトウェアの場合、デバイスログは `/tmp/DataCollect.zip` ファイル内に生成されます。

   バージョン 3.2 以降のアプライアンスソフトウェアの場合、デバイスログは `/log/DataCollect.zip` ファイル内に生成されます。
3. `Main > Support > Logs > Share Open` コマンドを使用して、`DataCollect.zip` をローカルフォルダにコピーします。
4. 問題を解決するには、Veritasのサポートチームに `DataCollect.zip` ファイルを送信します。

p.55 の「NetBackup appliance のログファイルについて」を参照してください。

ログ転送機能の概要

ログ転送機能を使用すると、外部ログ管理サーバーにアプライアンスのログを送信できます。ソフトウェアバージョン 3.0 以降では、NetBackup Appliance で syslog の転送がサポートされます。syslog は、ユーザーレベルやシステムレベルのアクティビティがイベントの形式で格納されている OS システムログのことです。この機能は、セキュリティを高めて、HIPPA、SOX、PCI などの一般的なコンプライアンスイニシアチブを実現する場合に使用します。現在サポートされているログ管理サーバーは HP ArcSight と Splunk です。

NetBackup Appliance は、Rsyslog クライアントを使用してログを転送します。HP ArcSight と Splunk 以外に、Rsyslog クライアントをサポートする他のログ管理サーバーを使用してアプライアンスから syslog を受信することもできます。Rsyslog クライアントのサポートの有無を確認するには、ログ管理サーバーのマニュアルを参照してください。

ログ送信の保護

アプライアンスからログ管理サーバーに安全にログを伝送するには、トランスポート層セキュリティ (TLS) オプションを使用します。NetBackup appliance は、現在ログ転送で TLS 匿名認証のみをサポートしています。

TLS を有効にするには、アプライアンスとログ管理サーバーのそれぞれに、次のように個別の準備が必要です。

- アプライアンスの要件
  ログ転送機能を構成して有効にするには、アプライアンスに X.509 ファイル形式で次の証明書ファイルと秘密鍵ファイルが必要になります。

- ca-server.pem
  ログ管理サーバー証明書の元であるルート CA 証明書
- nba-rsyslog.pem
  ログ管理サーバーと通信するために必要なアプライアンスの証明書。すべての中間 CA 証明書も含む
- nba-rsyslog.key
  syslog 管理サーバーと通信するために使用する証明書に対応する秘密鍵

これらのファイルは NFS 共有または CIFS 共有を使用してアプライアンスにアップロードできます。

- HP ArcSight サーバーの構成要件
  アプライアンスから暗号化されたログを受け取るには、HP ArcSight サーバーに TLS を設定して Rsyslog サーバーをセットアップする必要があります。次に、復号されたログを HP ArcSiight サーバーに転送するように Rsyslog サーバーを構成します。セットアップと構成の手順については、www.rsyslog.com の Web サイトを参照してください。
- Splunk サーバーの構成要件
  最初にこれらのサーバーで TLS を構成してから、アプライアンスでログ転送機能を構成する必要があります。TLS の適切な構成について詳しくは、Splunk のマニュアルを参照してください。

構成

この機能は、次の Main > Settings > LogFowarding コマンドオプションを使用してシェルメニューから構成する必要があります。

- LogForwarding Enable
  機能を構成します。
- LogForwarding Disable
  構成を削除して機能を無効にします。
- LogForwarding Interval
  ログの転送頻度を設定します。0 (連続)、15、30、45、または 60 分から選択します。アプライアンスで STIG を有効にすると、ログの転送間隔を手動で設定できません。
- LogForwarding Share
  必須の証明書ファイルと秘密鍵ファイルを取得するために、アプライアンスで NFS 共有または CIFS 共有を開くかまたは閉じます。共有パスは次のとおりです。
  NFS: <appliance.name>:/inst/share
  CIFS: ¥¥<appliance.name>¥general_share

メモ: アプライアンスの Web コンソールの[管理 (Manage)]>[ファイルマネージャ (File Manager)]メニューから証明書ファイルをアップロードすることもできます。

- `LogForwarding Show`
  現在の構成と状態を表示します。

`LogForwarding > Enable` コマンドを入力すると、次の表に記載されている手順に従って構成をガイドするプロンプトが表示されます。

表 5-3 `LogForwarding > Enable` **コマンドプロンプト**

プロンプト	説明
サーバー名または IP (Server name or IP)	外部ログ管理サーバーのは名前または IP アドレスを入力します。
サーバーポート	外部ログ管理サーバーの適切なポート番号を入力します。
プロトコル	UDP または TCP を選択します。
間隔(interval)	ログの転送頻度を設定します。
TLS の有効化 (Enable TLS)	ログ管理サーバーへのログ送信を保護するために TLS を選択して、有効にします。現時点では X.509 ファイル形式のみがサポートされます。 TLS を使用するには、次の証明書ファイルと秘密鍵ファイルをアプライアンスにアップロードする必要があります。 ■ `ca-server.pem` ■ `nba-rsyslog.pem` ■ `nba-rsyslog.key`

構成とコマンドについて詳しくは、次のドキュメントを参照してください。

『NetBackup Appliance 管理者ガイド』

『NetBackup Appliance コマンドリファレンスガイド』

6

オペレーティングシステムのセキュリティ

この章では以下の項目について説明しています。

NetBackup Appliance のオペレーティングシステムのセキュリティについて

NetBackup Appliance は、カスタマイズされた Linux オペレーティングシステムである VxOS (Veritas オペレーティングシステム) を使用します。NetBackup Appliance ソフトウェアの各リリースには、最新バージョンの VxOS と NetBackup ソフトウェアが含まれます。定期的なセキュリティパッチと更新に加え、VxOS には次のセキュリティ拡張機能とその他の機能が含まれています。

- 更新され、調整された RHEL (Red Hat Enterprise Linux) ベースの Linux OS プラットフォームによって、すべての必要なソフトウェアコンポーネントを互換性がある堅牢なハードウェアプラットフォームにパッケージし、インストールすることができます。
- NIST (米国標準) と RHEL からのセキュリティ基準に基づいて VxOS のセキュリティを強化します。追加のセキュリティが SDCS (Symantec Data Center Security) によって提供されます。
- Symantec Data Center Security: Server Advanced (SDCS) 侵入防止および侵入検出ソフトウェアは、各プロセスとすべてのシステムファイルを隔離し、サンドボックス化することで、VxOS を強化してバックアップデータを保護します。

- 業界に認められた脆弱性スキャナによるアプライアンスの定期スキャン。検出された脆弱性は、アプライアンスソフトウェアの定期リリースや、Emergency Engineering Binary（EEB）を使用してパッチが適用されます。セキュリティ上の脅威がリリーススケジュールの間に特定された場合、既知の解決法については Veritas サポートまでお問い合わせください。
- 未使用のサービスアカウントは削除されるか無効化されます。
- VxOS にはサービス拒否 (DoS) のような攻撃からアプライアンスを保護するための編集されたカーネルパラメータが含まれます。たとえば、`sysctl` 設定、`net.ipv4.tcp_syncookies` は、TCP SYN cookies を実装するため、`/etc/sysctl.conf` 構成ファイルに追加されました。
- 不要な runlevel サービスは無効化されました。VxOS では、runlevel を使用し、実行する必要のあるサービスを判断したり、システム上で実行する特定の作業を許可したりします。
- `FTP`、`telnet`、`rlogin (rsh)` は無効です。`ssh`、`scp`、`sftp` に限定して使用できます。

メモ: NetBackup Appliance リリース 3.1.2 以降、パッケージ化された telnet が VxOS から削除され、STIG 機能が NetBackup Appliance で有効になっているときにこの機能に準拠するようになりました。`telnet` プロトコルは安全ではなく、暗号化もされていません。暗号化されていない伝送媒体を使用すると、権限のないユーザーにクレデンシャルが盗まれる可能性があります。セッションを暗号化し、セキュリティを強化する `ssh` パッケージが、VxOS に含まれています。

- `AllowTcpForwarding no` と`X11Forwarding no` の `/etc/ssh/sshd_config` への追加で、SSH の TCP 転送は無効化されました。
- IP 転送が VxOS 上で無効にされ、TCP/IP スタックでのルーティングを許可しなくなりました。この機能により、あるサブネット上のホストがアプライアンスをルーターとして使って、別のサブネット上のホストにアクセスするのを防ぐことができます。
- NetBackup Appliance では、ネットワークインターフェース上での IP エイリアス (複数の IP アドレスの構成) は許可されません。この機能により、1 つの NIC ポート上の複数のネットワークセグメントへのアクセスを防止できます。
- UMASK 値は新しく作成されたファイルのファイル権限を判断します。新しく作成されたファイルにデフォルトでは与えられない権限を指定します。ほとんどの UNIX システムの UMASK のデフォルト値は 022 ですが、NetBackup appliance では UMASK は 077 に設定されています。
- VxOS で検出された万人書き込み可能なすべてのファイルの権限が検索されて修正されました。

- VxOS で検出されたすべての孤立した、あるいは所有者不明のファイルとディレクトリの権限が検索されて修正されました。
- ソフトウェアバージョン 3.1 以降、SMBv1 プロトコルは無効になり、SMBv2 プロトコルに置き換えられています。SMBv1 プロトコルは、WannaCry や Petya などのランサムウェア攻撃に対する脆弱性があるため、安全と見なされなくなりました。SMBv2 は、NetBackup Appliance でサポートされる最低限のプロトコルになりました。

NetBackup appliance の OS の主要コンポーネント

表 6-1に、アプライアンスのオペレーティングシステム (VxOS) の主要ソフトウェアコンポーネントの一覧を示します。

表 6-1 アプライアンスバージョン 4.0 の VxOS に含まれる主要ソフトウェアコンポーネント

ソフトウェアコンポーネント	バージョン
Red Hat Enterprise Linux (RHEL)	7.9
Veritas InfoScale	7.4.2 **メモ:** Veritas InfoScale のインストールが変更されて、アプライアンスで最大限のパフォーマンスを引き出すように調整されています。
SDCS (Symantec Data Center Security): Server 6.8 Advanced	6.8.2 (ビルド 757)
Java Runtime Environment (JRE)	11.0.11.0.9-1
Apache Tomcat	9.0.44-1
RabbitMQ	rabbitmq-server-3.8.16-1
MongoDB	4.2.11-1
Intel IPMI Utils	14.1-32

NetBackup Appliance オペレーティングシステムへのユーザーアクセスの無効化

組織のセキュリティポリシーに応じ、NetBackup appliance オペレーティングシステム (VxOS) へのユーザーアクセスを永続的に無効にできます。VxOS のセキュリティレベルを High に設定すると、VxOS へのユーザーアクセスを無効にできます。次の制限がアプライアンスに永続的に適用されるため、注意してください。

- ユーザーはメンテナンスシェルにアクセスできません。Support > Maintenance メニューはシェルメニューでは使用できません。

メモ: 問題のトラブルシューティングやオペレーティングシステム関連のタスクの管理のため、ベリタスのサポート担当者にのみ、メンテナンスシェルへのアクセス権を付与できます。p.68 の「メンテナンスシェルへのサポートのアクセスの管理」を参照してください。

- ユーザーは NetBackupCLI ユーザーを作成および削除できません。Manage > NetBackupCLI メニューはシェルメニューでは使用できません。
- ユーザーは NetBackupCLI 役割を許可または無効化できません。Authorization > Grant NetBackupCLI メニューはシェルメニューでは使用できません。
- NetBackupCLI 役割を持つユーザーは、アプライアンスにログインできません。

VxOS へのユーザーアクセスを永続的に無効にするには

1 VxOS の現在のセキュリティレベルを表示するには、次のコマンドを使用します。

```
Main_Menu > Settings > Security > SecurityLevel Show
```

VxOS は次のいずれかのセキュリティレベルで動作します。

セキュリティレベル	説明
Optimal	標準のベリタスセキュリティポリシーに従って VxOS へのアクセス権が付与されます。これはデフォルトのセキュリティ構成です。
High	すべてのユーザーの VxOS へのアクセス権が永続的に無効になります。
Maintenance	メンテナンスシェルを通じて、VxOS へのアクセス権がベリタスのサポート担当者に一時的に付与されます。メンテナンス操作が完了すると、セキュリティレベルは自動的に High に戻ります。

2 VxOS へのユーザーアクセスを永続的に無効にするには、セキュリティレベルを High に設定します。次のコマンドを使用します。

```
Main_Menu > Settings > Security > SecurityLevel High
```

メモ: セキュリティレベルを High に切り替えた後、アプライアンスの出荷時設定へのリセットを実行しないかぎり、デフォルト (Optimal) のセキュリティレベルには戻せません。

メンテナンスシェルへのサポートのアクセスの管理

VxOS のセキュリティレベルを High に設定すると、Support > Maintenance メニューのメンテナンスシェルは無効になります。ただし、問題のトラブルシューティングや OS タスクの管理を行う場合は、メンテナンスシェルを有効化してアクセスすることをベリタスのサポート担当者に対して許可できます。

Main_Menu > Support > System メニューのコマンドを使用して、メンテナンスシェルへのサポートのアクセスを管理します。詳しくは、『Veritas NetBackup Appliance コマンドリファレンスガイド』を参照してください。

表 6-2 メンテナンスシェルへのサポートのアクセスを管理するためのコマンド

コマンド	説明
Support > System > Generate-otp	このコマンドを使用して、10 桁のワンタイムパスワード (OTP) を生成します。このパスワードは 2 時間アクティブです。 OTP は、ベリタスのサポート担当者と共有できます。
Support > System > Show-otp	このコマンドを使用して現在アクティブな OTP を表示します。
Support > System > Unlock	このコマンドを使用して、ベリタスのサポート担当者がメンテナンスシェルを有効にします (Support > Maintenance)。Unlock コマンドを正常に実行してメンテナンスシェルにアクセスするため、ベリタスのサポート担当者は、アクティブな OTP に加えてカスタマケース ID とサポートパスフレーズを必要とします。 **メモ:** VxOS が一時的に Maintenance セキュリティレベルに設定されます。
Support > System > Lock	このコマンドを使用してメンテナンスシェルを無効にします。ベリタスのサポート担当者はメンテナンスシェルにアクセスできなくなり、すべてのアクティブなセッションからログアウトされます。 **メモ:** VxOS が High セキュリティレベルに戻ります。

7

データセキュリティ

この章では以下の項目について説明しています。

データセキュリティについて

NetBackup appliance は、NetBackup サーバーと同様にクライアント上のデータを保護するためにポリシーに基づいたメカニズムをサポートします。データの漏えいを回避し、保護を強化してデータセキュリティを向上させるため、次の手段が実装されています。

- リアルタイムの侵入防止メカニズムが、NetBackup appliance に格納されている機密データへのアクセスを監査するために設置されています。
- すべてのリストアをログに記録し、リアルタイムに追跡します。
- バックアップデータへのアクセスは、アプライアンスユーザーと処理に対してのみ認可されています。
- バックアップの発生時に、重複排除プール (MSDP) のすべてのバックアップデータが巡回冗長検査 (CRC) のデジタル署名 (CRC) でマーク付けされていることを NetBackup appliance が確認します。メンテナンスタスクが連続的に CRC のデジタル署名を再計算して元の署名と比較し、重複排除プールに不要な改ざんまたは破損があるかどうかを検知します。
- アプライアンスストレージへの意図しないアクセスを、アプライアンスへのログインを保護するパスワードによって回避します。
- 権限があるユーザーのみに限定される共有データと NetBackup 処理にアクセスします。

- HTTPS プロトコルとポート 443 を使って Veritas AutoSupport サーバーに接続し、コールホーム機能を使ってハードウェアとソフトウェアの情報をアップロードします。ベリタスのテクニカルサポートは、報告された問題を解決するためにこの情報を使います。この情報は 90 日間保持され、ベリタスのセキュアオペレーションセンターでパージされます。
- ある時点までシステム全体を容易にロールバックできる「チェックポイント」をサポートしています。この機能により、誤った構成を元に戻すことができます。チェックポイントは次のコンポーネントを取得します。
  - アプライアンスのオペレーティングシステム
  - アプライアンスのソフトウェア
  - NetBackup ソフトウェア
  - プライマリサーバーのテープメディアの構成
  - ネットワーク構成
  - LDAP の構成（存在する場合）
  - ファイバーチャネルの構成
  - 前回適用したパッチすべて

メモ: NetBackup カタログや KMS データベースのような重要なコンポーネントは、構成の追加が必要な場合もあります。

NetBackup appliance ソフトウェアには、HTTP (Web サービス) プロトコルを使用しない伝送やセッションのセキュリティは組み込まれていません。アプライアンスのソフトウェアが信頼できないネットワーク環境で実行されている場合、NetBackup ホスト間に IPSec のような VPN (仮想プライベートネットワーク) ソリューションを配備することをお勧めします。

データ整合性について

NetBackup appliance の重複排除プールのストレージは、正常なデータのリストアが確実に行われるように、次のデータ整合性チェックを提供しています。

重複排除プールに格納されているバックアップデータの連続的なエンドツーエンド検証

データ破損が発生する可能性のある不注意なデータ変更でも、可能な場合は、自動的に検出されて修正されます。修復不能なデータ破損の問題は、NetBackup コンソールのディスクレポート UI（[NetBackup 管理コンソール (NetBackup Administration Console)] > [レポート (Reports)] > [ディスクのレポート (Disk Reports)]）によって、ストレージ管理者に報告されます。

重複排除プールに格納されているバックアップデータの連続的な巡回冗長検査（CRC）検証

CRC 値は、重複排除プールのバックアップジョブのために作成される各オブジェクトについて計算されます。バックグラウンド処理で連続的に CRC 署名を検証することで、バックアップデータの改ざんを防ぎ、必要な場合に正常にリストアできるようにします。重複排除プールの設計では、破損が重複排除プール全体に広がらないようにするため、プールの破損していない部分からデータ破損を隔離します。

データの分類について

データの分類は、一連のバックアップ要件を表します。データの分類を使用すると、さまざまな要件でデータのバックアップを簡単に構成できるようになります。たとえば、ゴールドの分類のバックアップはゴールドのデータの分類のストレージライフサイクルポリシーに移動する必要があります。NetBackup appliance は、NetBackup と同じデータの分類の属性をサポートします。

NetBackup データの分類の属性は、バックアップを格納するストレージライフサイクルポリシーの分類を指定します。たとえば、ゴールド分類のバックアップはゴールドデータ分類のストレージユニットに送信する必要があります。

NetBackup は次のデフォルトのデータの分類を提供します。

- プラチナ
- ゴールド
- シルバー
- ブロンズ

この属性は省略可能で、バックアップがストレージライフサイクルポリシーへ書き込まれる場合のみ適用されます。リストに［データの分類なし (No data classification)］が表示される場合、ポリシーは［ポリシーストレージ (Policy storage)］リストに表示されるストレージ選択を使います。データの分類を選択しているポリシーでは、作成されるすべてのイメージは分類 ID でタグ付けされます。

データの暗号化について

NetBackup appliance は、次の暗号化の方式を提供し、格納中と送信中の両方のデータを保護します。

- セキュアトンネルを使って暗号化形式でデータを転送します。これらの構成はクライアント側の暗号化や複製によっても行うことができます。これらのオプションを使わない場合、データがアプライアンスから送信された後は、送信中のデータを保護するためにネットワークインフラストラクチャが使われます。

- NetBackup appliance バージョン 3.0 (NetBackup バージョン 8.0) より、MSDP は AES 暗号化を提供します。暗号化された MSDP を使う環境では、新たな受信データは 128 ビット (デフォルト) または 256 ビットの AES を使って暗号化されます。詳しくは、次の NetBackup のマニュアルを参照してください。
  『Veritas NetBackup Deduplication ガイド』
  『Veritas NetBackup セキュリティおよび暗号化ガイド』
- NetBackup Enterprise Server 7.1 に統合されている NetBackup キーマネージメントサービス (KMS) を使った暗号化をサポートします。p.72 の「KMS サポート」を参照してください。

KMS サポート

NetBackup appliance は、NetBackup Enterprise Server 7.1 に統合されている NetBackup キーマネージメントサービス (KMS) を使った暗号化をサポートします。KMS は、プライマリサーバーアプライアンスとメディアサーバーアプライアンスでサポートされます。データ暗号化キーを再生成することは、アプライアンスのプライマリサーバーで KMS をリカバリする場合にサポートされている唯一の方法です。

次に、KMS の主な機能について説明します。

- 追加のライセンスは必要ありません。
- プライマリサーバーベースの対称キーマネージメントサービスです。
- テープデバイスがそれか別の NetBackup appliance に接続されているプライマリサーバーとして管理できます。
- T10 基準 (LTO4 や LTO5 など) に準拠しているテープドライブの対称暗号化キーを管理します。
- ボリュームプールベースのテープ暗号化を使うように設計されています。
- 組み込みのハードウェア暗号化機能のあるテープハードウェアによって使うことができます。
- NetBackup CLI 管理者が NetBackup Appliance シェルメニューまたは KMS コマンドラインインターフェース (CLI) を使って管理できます。

KMS で使われるキーについて

KMS はパスコードからキーを生成するか、キーを自動生成します。表 7-1は、キーの情報を保持する KMS と関連付けられているファイルの一覧を示します。

表 7-1 KMS ファイル

KMS ファイル	説明	場所
キーファイルまたはキーデータベース	このファイルにはデータ暗号化キーが含まれるので、KMS にとって重要です。	/usr/openv/kms/db/KMS_DATA.dat
ホストのプライマリキー	このファイルには、AES 256 を使って KMS_DATA.dat キーファイルを暗号化して保護する暗号化キーが含まれます。	/usr/openv/kms/key/KMS_HMKF.dat
キーの保護キー (Key Protection Key)	この暗号化キーは、AES 256 を使って KMS_DATA.dat キーファイルの個別のレコードを暗号化して保護します。現時点では、すべてのレコードを暗号化するために同じ保護キーが使われています。	/usr/openv/kms/key/KMS_KPKF.dat

KMS の構成

アプライアンスプライマリサーバーで KMS を構成するには、NetBackupCLI ユーザーとしてログインする必要があります。

続行する前に、KMS を構成して有効にするために必要な RBAC 権限が NetBaclupCLI ユーザーに割り当てられていることを確認します。nbasecadmin などの NetBackup 管理者アカウントを使用して NetBackup Web UI にログインし、NetBackupCLI ユーザーにデフォルトのセキュリティ管理者役割を割り当てます。

役割ベースのアクセス制御の管理手順については、『NetBackup Web UI 管理者ガイド』を参照してください。

メモ: 必要に応じて、新しい NetBackupCLI ユーザーを作成して、KMS を構成および有効化できます。NetBackupCLI ユーザーの役割について詳しくは、p.42 の「NetBackupCLI ユーザーロールについて」を参照してください。を参照してください。

以下に、アプライアンスで KMS を構成して有効にする方法について説明します。

アプライアンスで KMS を構成して有効にするには

1 NetBackupCLI ユーザーとしてアプライアンスプライマリサーバーにログインします。

2 次のように nbkms コマンドを使用して空のデータベースを作成します。

```
[nbcli@myappliance~]# nbkms -createemptydb
```

3 nbkms を起動します。次に例を示します。

```
[nbcli@myappliance~]# nbkms
```

4 キーグループを作成します。次に例を示します。

```
[nbcli@myappliance~]# nbkmsutil -createkg -kgname KMSKeyGroupName
```

5 アクティブなキーを作成します。次に例を示します。

```
[nbcli@myappliance~]# nbkmsutil -createkey -kgname KMSKeyGroupName
-keyname KMS KeyName
```

MSDP に対する KMS 暗号化の有効化

KMS が構成されてプライマリサーバーで実行されると、プライマリサーバーに関連付けられているすべてのメディアサーバー上の MSDP に対して KMS 暗号化を有効にできます。

続行する前に、KMS を構成して有効にするために必要な RBAC 権限が NetBaclupCLI ユーザーに割り当てられていることを確認します。nbasecadmin などの NetBackup 管理者アカウントを使用して NetBackup Web UI にログインし、NetBackupCLI ユーザーにデフォルトのセキュリティ管理者役割を割り当てます。

役割ベースのアクセス制御の管理手順については、『NetBackup Web UI 管理者ガイド』を参照してください。

メモ: 必要に応じて、新しい NetBackupCLI ユーザーを作成して、KMS を構成および有効化できます。NetBackupCLI ユーザーの役割について詳しくは、p.42 の「NetBackupCLI ユーザーロールについて」を参照してください。を参照してください。

以下に、アプライアンスで MSDP に対して KMS 暗号化を有効にする方法について説明します。

MSDP に対して KMS 暗号化を有効にするには

1 NetBackup CLI ユーザーとしてアプライアンスメディアサーバーにログインします。

2 次のオプションを以下の順序で変更します。

- nbcli@myappliance:~> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSType --value=0
- nbcli@myappliance:~> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSServerName --value=<*primary server hostname*>

- nbcli@myappliance:~> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KMSKeyGroupName --value=msdp
- nbcli@myappliance:~> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KeyName --value=<*KMS KeyName*>
- nbcli@myappliance:~> pdcfg
  --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=KMSOptions --option=KMSEnable --value=true
- pdcfg --write=
  /msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg
  --section=ContentRouter --option=ServerOptions
  --value=verify_so_references,fast,encrypt
  この手順をプライマリサーバーに関連付けられているすべてのメディアサーバーで繰り返します。

3 NetBackup Web アプリケーションにログオンして、システムで自分自身を識別します。次のコマンドを実行します。

```
bpnbat -login -loginType WEB

Authentication Broker: ApplianceHostname

Authentication Port: 0

Authentication Type: unixpwd

LoginName: Username

Password: Password
```

4 KMS が NetBackup Web サービスに登録されていることを確認します。

```
nbkmscmd -discoverNbkms
```

5 次のコマンドを使用して、NetBackup サービスを停止して再起動します。

- bp.kill_all
- bp.start_all

6 メディアサーバーで MSDP に対して KMS 暗号化が有効になっていることを確認するには、サーバーでバックアップジョブを実行してから、次のコマンドを実行します。

```
crcontrol --getmode
```

8

Web セキュリティ

この章では以下の項目について説明しています。

SSL の使用について

SSL (Secure Socket Layer) プロトコルは、アプライアンスの Web サーバーと Web コンソール、およびその他のローカルサーバー間の接続を暗号化します。この接続の種類では、盗聴、データ改ざん、メッセージの偽造という問題を発生させることなく情報を安全に転送できます。アプライアンスの Web サーバーで SSL を有効にするには、アプライアンスホストを識別する SSL 証明書が必要です。

SSL 証明書により、アプライアンスと LDAP、HTTP プロキシ、Syslog などのさまざまな外部サーバー間の通信もセキュリティで保護できます。

自己署名証明書

アプライアンスは、クライアントとホストの検証に自己署名証明書を使用します。内部 CA が発行したホスト証明書は、役割の構成時にプライマリサーバーとメディアサーバーに配備されます。自己署名証明書は、SHA256 アルゴリズムでハッシュ化され、RSA 暗号化を使用して署名された 2048 ビット RSA 公開鍵を使用して生成されます。セキュリティで保護された通信で、アプライアンスは TLS バージョン 1.2 以降のプロトコルのみを使用します。

ECA 証明書

NetBackup appliance では、外部認証局 (ECA) によって発行されたホスト証明書もサポートされます。内部 CA の代わりに ECA を使用したホスト検証とセキュリティにより、組織の標準を満たすことができます。

NetBackup appliance で使用される各種の外部証明書については、次の表を参照してください。

表 8-1 ECA 証明書の種類

証明書の種類	説明
ホスト証明書	アプライアンスのホスト証明書は、X.509 または PKCS#7 標準に基づいています。証明書は、DER (バイナリ) または PEM (テキスト) 形式でエンコードされます。長さ 2048 ビット以上の RSA パブリックキーとプライベートキーを使用することをお勧めします。 **メモ:** 証明書拡張の SubjectAlternativeName に、アプライアンスに到達するすべてのアプライアンスのホスト名と IP アドレスが含まれていることを確認します。完全修飾ホスト名と短縮名を含めます。
ホストのプライベートキー (ホスト証明書に対応)	アプライアンスのホストのプライベートキーは、PKCS#8 標準に従い、PEM 形式でエンコードされている必要があります。
(オプション) 中間 CA 証明書	中間 CA 証明書は、アプライアンスホスト証明書からルート CA 証明書への証明書チェーンを構成する証明書です。これらの証明書は、ホスト証明書がルート CA 以外の CA によって発行されている場合にのみ必要です。
ルート CA 証明書	これには、アプライアンス証明書チェーンとそのピアのルート CA 証明書が含まれます。アプライアンスが異なる CA の証明書を持つホストと通信する必要がある場合は、cacerts.pem という名前のファイルで、これらの中間 CA 証明書とルート CA 証明書をすべて準備する必要があります。

ECA 証明書の実装について

NetBackup appliance の Web サービスでは、PKCS#12 標準を使用し、証明書ファイルを X.509 (.pem または .cer) 形式にする必要があります。証明書ファイルが .der、.DER または .p7b 形式の場合、NetBackup appliance はファイルを受け入れ可能な形式に自動的に変換します。

証明書の要件

証明書のインポート中にエラーを防ぐには、外部証明書ファイルが次の要件を満たしていることを確認します。

- 証明書ファイルが .pem ファイル形式であり、"-----BEGIN CERTIFICATE-----"で始まっている 。
- 証明書ファイルの証明書の SAN (サブジェクトの別名) フィールドにホスト名と FQDN が含まれている。証明書を HA 環境で使用する場合、SAN フィールドには VIP、ホスト名、FQDN が含まれている必要がある。
- サブジェクト名フィールドと一般名フィールドが空ではない。
- サブジェクトフィールドが各ホストで一意である。

- サブジェクトフィールドに含まれる文字が最大 255 文字である。
- サーバーとクライアントの認証属性が証明書に設定されている。
- 証明書のサブジェクトフィールドおよび SAN フィールドで ASCII 7 文字のみが使用されている。
- プライベートキーファイルが PKCS#8 PEM 形式で、`-----BEGIN ENCRYPTED PRIVATE KEY-----` または `-----BEGIN PRIVATE KEY-----` で始まっている。

証明書署名要求 (CSR)

省略可能ですが、`Settings > Security > Certificate > CertificateSigningRequest > Create` コマンドを使用して CSR を生成できます。CSR の内容をコマンドラインから ECA ポータルにコピーして、必要な外部証明書ファイルを取得します。

ECA の登録

バージョン 4.1 以降、`Settings > Security > Certificate > Import` コマンドを使用して NetBackup appliance と NetBackup の両方に ECA を登録できます。

ホスト証明書、ホストのプライベートキー、トラストストアをインポートして、ECA を NetBackup と NetBackup appliance に登録するには、次の手順を実行します。NetBackup 層と NetBackup appliance 層の両方で同じホスト証明書、ホストのプライベートキー、トラストストアを使用します。

1. 管理者ユーザーとしてアプライアンスにログインします。
2. NetBackup Appliance シェルメニューから `Settings > Security > Certificate > Import` コマンドを実行します。これで次の NFS および CFS 共有の場所にアクセスできます。
   - NFS: `/inst/share`
   - CFS: `¥¥<ApplianceName>¥general_share`
3. 証明書ファイル、トラストストアファイル、プライベートキーファイルを共有の場所のいずれかにアップロードし、ファイルへのパスを入力します。
4. 証明書失効リスト (CRL) へのアクセス方法を選択します。CRL は、ECA によって失効され、信頼すべきではない外部証明書の一覧で構成されています。次のオプションのいずれかを選択します。
   - 証明書ファイルに指定されている CRL の場所を使用する。
   - ローカルネットワークの CRL ファイル (`.crl`) の場所を指定します。
   - CRL を使用しない。
5. アプライアンスに登録する証明書ファイルの場所を確認します。

Copilot のサポート

外部証明書を使用して配備されたアプライアンスで Copilot 機能を使用する前に、次のことを確認してください。

- アプライアンスの証明書ファイル (/etc/vxos-ssl/servers/certs/) が、プライマリサーバーの証明書ファイル (/usr/openv/var/global/appliance_certificates/) と同じである。
- アプライアンスの証明書ファイル (/etc/vxos-ssl/servers/certs/) に *<FQDN_hostname>*-self.cert.pem という形式の名前が付いている。

関連付けられている各アプライアンスで、次のコマンドを実行します。

```
rm /etc/vxos-ssl/servers/certs/<FQDN_hostname>-self.cert.pem

cp /etc/vxos-ssl/servers/certs/server.pem
/etc/vxos-ssl/servers/certs/<FQDN_hostname>-self.cert.pem

tpconfig -delete -nb_appliance <Short_hostname>

/opt/NBUAppliance/scripts/copilot_users.pl --add
```

9

ネットワークセキュリティ

この章では以下の項目について説明しています。

IPsec チャネル設定について

NetBackup appliance は、IPsec チャネルを使用して、2 つのアプライアンス間の通信を保護します。これは、送信中のデータの保護に役立ちます。NetBackup プライマリサーバーのような NetBackup appliance と非アプライアンス間の他のすべての通信は非 IPsec です。

IPsec セキュリティは IP レベルで動作し、2 つのアプライアンス間の IP トラフィックのセキュリティ保護を許可します。デバイス証明書はプライマリアプライアンスやメディアアプライアンスにプロビジョニングされ、これらの証明書は IPsec チャネルの構成で有効になります。これはプライマリサーバーとメディアサーバーの安全な対話を有効にします。使用されるデバイス証明書は DigiCert CA によって発行される x509 証明書です。

アプライアンスは IPsec チャネルを確立する前に次の検証チェックを実行します。

- x509 証明書を使用して証明書の権限を検証します。
- デバイス証明書が IP に対応しているかどうかを検証します。
- 通信の両方向のセキュリティアソシエーションを検証し、更新します。

アプライアンスはデバイスの証明書が認識された後に検出されます。この後にのみ、IPsec チャネルは構成され、有効になります。

IPsec 構成の管理

NetBackup Appliance シェルメニューの `Main > Network > Security` コマンドを使用して、2 つのアプライアンス間の IPSec チャネルを構成できます。IPsec チャネル構成

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。

表 9-1 IPsec コマンド

コマンド	説明
`Network > Security > Configure`	このコマンドを使用して、任意の 2 アプライアンス間の IPsec を構成できます。
`Network > Security > Delete`	このコマンドを使用して、ローカルシステム上にあるリモートアプライアンスリストの IPsec ポリシーを削除できます。
`Network > Security > Export`	このコマンドを使って IPsec クレデンシャルをエクスポートします。 **メモ:** IPsec クレデンシャルは再イメージング処理中に削除されます。クレデンシャルはアプライアンスごとに一意であり、元の工場出荷時イメージの一部として含まれています。IPsec クレデンシャルは、アプライアンスの再イメージングに使われる USB ドライブには含まれていません。
`Network > Security > Import`	このコマンドを使用して IPsec クレデンシャルをインポートします。
`Network > Security > Provision`	このコマンドを使用して、ローカルシステム上にあるリモートアプライアンスリストの IPsec ポリシーをプロビジョニングします。
`Network > Security (IPsec) > Refresh`	このコマンドを使って IPsec の構成を再ロードします。
`Network > Security > Show`	ローカルホスト (アプライアンス) または指定されたアプライアンスの IPsec ポリシーを表示します。
`Network > Security > Unconfigure`	このコマンドを使用して、任意の 2 アプライアンス間の IPsec を構成解除します。

NetBackup appliance ポートについて

NetBackup ソフトウェアによって使用されるポートに加えて、NetBackup Appliance はインバンドとアウトオブバンドの両方の管理にも対応します。アウトオブバンド管理は、別のネットワーク接続、リモート管理モジュール (RMM)、およびインテリジェントプラットフォーム管理インターフェース (IPMI) を使用して行われます。必要に応じてファイアウォールを介してこれらのポートを開くことで、リモートのノートパソコンや KVM (キーボード、ビデオモニタ、マウス) から管理サービスへのアクセスを許可します。

初期構成の前後にデフォルトで開かれているアプライアンスポートのリストについては、次のトピックを参照してください。

p.83 の「NetBackup Appliance ファイアウォールについて」を参照してください。

メモ: NetBackup Appliance Web コンソールは、デフォルトポート 443 で HTTPS を介してのみ利用可能です。Web コンソールにログインするには、`https://<appliance-name>` を使用します。appliance-name はアプライアンスの完全修飾ドメイン名 (FQDN) で、IP アドレスになる場合もあります。

表 9-2に、Appliance のアウトバウンドポートを示します。これらのポートは、対象サーバーへの警告や通知の送信を許可します。

表 9-2　　アウトバウンドポート

ポート	サービス	説明
443	HTTPS	ベリタス社へのコールホーム通知 SDCS 証明書のダウンロード
161	SNMP ポーリング	Appliance の更新のダウンロード
162**	SNMP	Appliance の更新のダウンロード
22	SFTP	ベリタスへのログのアップロード
25	SMTP	電子メール警告
389	LDAP	
636	LDAPS	
514	rsyslog	ログ転送

** このポート番号は、リモートサーバーと一致するように、Appliance 構成内で変更できます。

メモ: リモート管理モジュール (RMM) ポートの一覧については、次のトピックを参照してください。

p.97 の「RMM ポート」を参照してください。

適用可能なすべてのポートの一覧は、『NetBackup ネットワークポートリファレンスガイド』で参照できます。

NetBackup Appliance ファイアウォールについて

NetBackup Appliance のリリース 3.1.2 以降、ファイアウォールポリシーによってアプライアンスに追加のネットワークセキュリティが提供されます。この機能は、ファイアウォールのデフォルトゾーンを「trusted」から「public」に変更します。最大のセキュリティを提供するため、次の操作中は特定の受信接続が自動的に開かれ、他の接続は自動的に遮断されます。

- 初期構成
- 役割の構成 (初期構成の一部)
- ノードの追加またはノードの削除 (高可用性構成)
- アップグレード

例外ルールにより、プライマリサーバーとメディアサーバー間の接続が上記の操作中に開いたままになり、不要なポートが遮断されたままになります。

次の表に、初期構成の前後にアプライアンスで開いているポートを示します。

表 9-3 は、アプライアンスの初期構成が完了する前にデフォルトで開いている NetBackup Appliance ポートを示しています。

表 9-3 出荷時のデフォルトで開いている NetBackup Appliance ポート (アプライアンスの初期構成前)

ポート	プロトコル	使用方法
22	TCP	SSH
111	TCP/UDP	Sunrpc、Portmapper
137	UDP	NetBIOS ネームサービス (Samba)
138	UDP	NetBIOS データグラムサービス (Samba)
139	TCP	NetBIOS セッションサービス (Samba)
162	TCP/UDP	SNMP
443	TCP	HTTPS
445	TCP	Samba
867	TCP	NFS マウント
2049	TCP/UDP	NFS
20048	UDP	mountd

ポート	プロトコル	使用方法
27017	TCP/UDP	Mongo **メモ:** このポートは、高可用性 (HA) 設定を完了するためにパートナーノードを追加する、または HA 設定からノードを削除するときにのみ開かれます。ノードが追加または削除した後、ポートは閉じられます。

表 9-4 は、アプライアンスの初期構成が完了した後にデフォルトで開いている NetBackup ポートを示します。

表 9-4 NetBackup Appliance で開いている NetBackup ポート (アプライアンスの初期構成後)

1025-5000	TCP	Veritas NDMP、`SERVER_PORT_WINDOW`
1556	TCP	Veritas PBX
5637	TCP/UDP	NetBackup Cloud Storage Server 構成、クラウドへの重複排除
7394	TCP	Veritas Granular Restore Technology (GRT)
8443	TCP	NetBackup VMware
10000	TCP/UDP	Veritas NDMP Agent
10082	TCP/UDP	MSDP、Deduplication Engine (`spoold`)、HA、移行
10102	TCP/UDP	MSDP、Deduplication Manager (`spad`)、HA、移行
13701-13723	TCP	Veritas Granular Restore Technology (GRT)
13720	TCP	271 個のメディアの役割の構成をサポート
13724	TCP	`vnetd`
13781	TCP	RabbitMQ
13782	TCP	Veritas `vnet_async`

アプライアンスで開いている NetBackup ポートの同期または表示

次のコマンドが追加され、アプライアンスで現在開いている NetBackup ポートを同期したり表示できるようになりました。

```
Main > Settings > Security > Ports > ModifyNBUPortRange
```

このコマンドの使用については、次の点に注意してください。

- このコマンドを実行するには、プライマリサーバーまたはメディアサーバーの役割でアプライアンスが構成されている必要があります。
- このコマンドを実行する前に、NetBackup Java コンソールでまず SERVER_PORT_WINDOW コマンドを使用して、開いている NetBackup ポートを変更する必要があります。次に、このコマンドを実行して、開いている NetBackup ポートとアプライアンスポートを同期します。

メモ: ModifyNBUPortRange コマンドでは、デフォルトの NetBackup VMware ポートの割り当てである 8443 を変更できません。VMware 製品では、アプライアンスと NetBackup の両方に対してポート 8443 をデフォルトで使用する必要があります。

```
Main > Settings > Security > Ports > Show
```

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

10

コールホームセキュリティ

この章では以下の項目について説明しています。

AutoSupport について

AutoSupport 機能を使うと、Veritasサポート Web サイトでアプライアンスと連絡先の詳細を登録できます。Veritas のサポートは、報告された問題を解決するためにこの情報を使います。この情報によって、Veritas は停止時間を最小化し、サポートにプロアクティブなアプローチを提供することが可能になります。

アプライアンスの登録と登録情報の編集を行う場所を https://netInsights.veritas.com ポータルにまとめました。

サポートインフラは、Veritas のサポートが次の方法でサポートできるように設計されています。

- プロアクティブな監視により、Veritas は自動的にケースを作成し、問題を解決し、リスクを伴う可能性のあるアプライアンスの部品を発送します。
- Veritas内の AutoSupport インフラは、アプライアンスからのコールホームデータを分析します。この分析はハードウェア障害に対してプロアクティブなテクニカルサポートを提供するため、バックアップ管理者がサポートケースを開始する必要性が減少します。
- AutoSupport 機能により、Veritas のサポートは、お客様がアプライアンスを構成して使う方法と、機能強化のメリットが最もあるところを把握できるようになります。
- アプライアンスの状態とアラート通知を送受信します。
- コールホームを使ってハードウェアとソフトウェアの状態を受信します。

- 問題に対してより多くの洞察を提供し、既存の問題の結果としてさらに発生する可能性のある問題を特定します。
- コールホームデータからのレポートを表示して、ハードウェア障害のパターンを分析し、使用状況の傾向を確認します。アプライアンスは 30 分ごとに健全性データを送信します。

データセキュリティ基準

アプライアンスからベリタスに伝送するすべてのデータは、業界標準の高度な暗号化方式を使用して伝送されます。クライアントとサーバー間で送信するすべての AutoSupport データと、クライアント内のさまざまなコンポーネント間のデータ通信に、以下のデータセキュリティ基準を適用します。

- RSA 2048 ビットキー (サーバー認証用)
- AES 128/256 ビットキー (データ暗号化用)
- SHA1、SHA2 (256/384 ビット) ハッシュ (メッセージ認証用)

コールホームについて

アプライアンスでは、Veritas AutoSupport コールホームサーバーに接続し、ハードウェアとソフトウェアの情報をアップロードできます。Veritas ベリタスのサポートは、報告された問題を解決するためにこの情報を使います。アプライアンスは HTTPS プロトコルとポート 443 を使って、Veritas AutoSupport サーバーに接続します。アプライアンスのこの機能をコールホームと呼びます。この機能はデフォルトで有効です。

AutoSupport は、コールホームが収集するデータを使用してアプライアンスをプロアクティブに監視します。コールホームが有効になっている場合、アプライアンスは 24 時間のデフォルトの間隔で情報またはデータを Veritas AutoSupport サーバーにアップロードします。

アプライアンスに問題があると判断した場合は、Veritasサポートにお問い合わせください。テクニカルサポート技術者は、アプライアンスのシリアル番号を使用してコールホームデータから状態を評価します。

NetBackup Appliance Web コンソールからアプライアンスのシリアル番号を取得するには、[監視 (Monitor)]、[ハードウェア (Hardware)]、[健全性の詳細 (Health details)] ページに移動します。シェルメニューを使ってアプライアンスのシリアル番号を確認するには、`Monitor > Hardware` コマンドを使います。`Monitor > Hardware` コマンドについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

[設定 (Settings)]>[通知 (Notification)]メニューを使って、NetBackup Appliance Web コンソールからコールホームを構成します。[警告の構成 (Alert Configuration)]をクリックし、[コールホームの構成 (Call Home Configuration)]ペインで詳細を入力します。

表 10-1では、本機能が有効または無効な場合、障害がどのように報告されるかを説明します。

表 10-1　　コールホームが有効または無効な場合の処理

監視状態	障害ルーチン
コールホーム有効時	障害が発生すると、以下の警告シーケンスが発生します。 ■ アプライアンスは、すべての監視されているハードウェアとソフトウェアの情報を Veritas AutoSupport サーバーにアップロードします。表の後に続くリストにすべての関連情報が含まれます。 ■ アプライアンスは、設定した電子メールアドレス宛てに次の 3 種類の電子メールアラートを生成します。 　■ エラーが検出されたときに電子メールでエラーを通知するエラーメッセージ。 　■ エラーが解決されると障害について通知する電子メールの解決メッセージ。 　■ 直近の 24 時間以内に発生した現在未解決のすべてのエラーを要約した、電子メール別の 24 時間の概略。 ■ アプライアンスは SNMP トラップも生成します。
コールホーム無効時	データを Veritas AutoSupport サーバーに送信しません。システムは Veritas にエラーを報告しないので問題をより早く解決できます。

次のリストは分析のために Veritas AutoSupport サーバーに監視され、送信されるすべての情報を含んでいます。

- CPU
- ディスク
- ファン (Fan)
- 電源
- RAID グループ
- 温度
- アダプタ
- PCI
- ファイバーチャネル HBA
- ネットワークカード
- パーティション情報

- MSDP 統計
- ストレージの接続
- ストレージの状態
- 52xx ストレージシェルフ - ディスク、ファン、電源、温度の状態
- 53xx プライマリストレージシェルフ - ディスク、ファン、電源、温度、バッテリバックアップ装置 (BBU)、コントローラ、ボリューム、ボリュームグループの状態
- 53xx 拡張ストレージシェルフ - ディスク、ファン、電源、温度の状態
- NetBackup appliance ソフトウェアのバージョン
- NetBackup エラーデータベースログエントリのバージョン
- アプライアンスモデル
- アプライアンスの構成
- ファームウェアのバージョン
- アプライアンス、ストレージ、およびハードウェアコンポーネントのシリアル番号

p.89 の「NetBackup Appliance シェルメニューからのコールホームの構成」を参照してください。

p.86 の「AutoSupport について 」を参照してください。

NetBackup Appliance シェルメニューからのコールホームの構成

[設定 (Settings)]>[通知 (Notification)]ページから、コールホームの詳細を構成できます。

NetBackup Appliance シェルメニューから、次のコールホームの設定を構成できます。

- 「アプライアンスシェルメニューからのコールホームの有効化と無効化」
- 「NetBackup Appliance シェルメニューからのコールホームプロキシサーバーの構成」
- `Settings > Alerts > CallHome > Test` コマンドの実行によってコールホームが正しく動作しているかどうかのテスト

`Main > Settings > Alerts > CallHome` コマンドについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

警告を引き起こすハードウェア問題のリストについては、次のトピックを参照してください。

p.87 の「コールホームについて」を参照してください。

アプライアンスシェルメニューからのコールホームの有効化と無効化

アプライアンスシェルメニューからコールホームを有効または無効にできます。コールホームはデフォルトでは有効です。

メモ: コールホームが適切に機能するように、アプライアンスを登録する必要があります。Veritas NetInsights コンソールのリリースに伴い、マイアプライアンスポータルはサポートされなくなり、廃止されます。アプライアンスの登録は、Veritas Account Manager のクレデンシャルを使用して、NetInsights ポータル (https://netInsights.veritas.com) にサインインして実行する必要があります。詳しくは、『Veritas Appliance AutoSupport リファレンスガイド』と『Veritas Netinsights コンソールユーザーガイド』を参照してください。

シェルメニューからコールホームを有効または無効にするには

1. シェルメニューにログオンします。
2. コールホームを有効にするには、`Main > Settings > Alerts > CallHome Enable` コマンドを実行します。
3. コールホームを無効にするには、`Main > Settings > Alerts > CallHome Disable` コマンドを実行します。

NetBackup appliance の `Main > Settings > Alerts > CallHome` コマンドについて詳しくは、『NetBackup Appliance コマンドリファレンスガイド』を参照してください。

NetBackup Appliance シェルメニューからのコールホームプロキシサーバーの構成

必要に応じて、コールホームのためのプロキシサーバーを構成できます。アプライアンス環境と外部インターネットアクセス間にプロキシサーバーが存在する場合、アプライアンスのプロキシ設定を有効にする必要があります。プロキシ設定には、プロキシサーバーとポートの両方が含まれています。プロキシサーバーは、ベリタスの AutoSupport サーバーからの https 接続を受け入れる必要があります。Veritasデフォルトでは、このオプションは無効になっています。

NetBackup Appliance シェルメニューからコールホームプロキシサーバーを構成する方法

1. NetBackup Appliance シェルメニューにログオンします。
2. プロキシ設定を有効にするには、`Main > Settings > Alerts > CallHome Proxy Enable` コマンドを実行します。
3. プロキシサーバーを追加するには、`Main > Settings > Alerts > CallHome Proxy Add` コマンドを実行します。

- プロキシサーバーの名前を入力するように求められます。プロキシサーバーの名前はプロキシサーバーの TCP/IP アドレスまたは完全修飾ドメイン名です。デフォルトでは、プロキシサーバーとの通信に HTTP プロトコルを使用します。

  メモ: HTTPS プロトコルを使用する場合は、プロキシサーバー名の前に https:// を入力します。プロキシサーバーと正常に通信するには、`Settings > Security > Certificate > AddCACertificate` コマンドを実行し、プロキシサーバーが使用する最新の CA 証明書を追加します。

- プロキシサーバーの名前を入力した後、プロキシサーバーのポート番号を入力するように求められます。
- さらに、次の質問に答える必要があります。

  ```
  Do you want to set credentials for proxy server? (yes/no)
  ```

- *yes* と答えると、プロキシサーバーのユーザー名を入力するように求められます。
- ユーザー名を入力した後、ユーザーのパスワードを入力するように求められます。必要な情報を入力すると、次のメッセージが表示されます。

  ```
  Successfully set proxy server
  ```

4 プロキシ設定を無効にするには、`Main > Settings > Alerts > CallHome Proxy Disable` コマンドを実行します。

さらに、NetBackup Appliance シェルメニューを使って、アプライアンスのプロキシサーバートンネリングの有効と無効を切り替えることもできます。これには、`Main > Settings > CallHome Proxy EnableTunnel` コマンドと `Main > Settings > Alerts > CallHome Proxy DisableTunnel` コマンドを実行します。プロキシサーバーのトンネリングを有効にすると、信頼できないネットワークを経由する際に安全なパスを使用できます。

コールホームワークフローの理解

このセクションでは、アプライアンスから Veritas AutoSupport サーバーにデータをアップロードするためにコールホームが使うメカニズムについて説明します。

コールホームは、Veritas AutoSupport サーバーとのすべての通信で HTTPS (暗号化された安全なプロトコル) とポート番号 443 を使用します。コールホームが正しく働くには、アプライアンスがインターネットに直接またはプロキシサーバーを経由してアクセスし、Veritas AutoSupport サーバーに到達する必要があります。アプライアンスをプロアクティブに監視するメカニズムである AutoSupport は、コールホームのデータを使って、アプライアンスで発生する可能性のある問題を分析して解決します。

アプライアンスはすべての通信を開始します。アプライアンスのプロキシやファイアウォールで、443/TCP TLS アウトバウンドソケットを使用してサイト `https://api.appliance.veritas.com` に接続できることを確認してください。

アプライアンスのコールホーム機能は以下のワークフローを使って、AutoSupport サーバーと通信します。

- `https://api.appliance.veritas.com` のポートに 24 時間ごとにアクセスします。
- `https://api.appliance.veritas.com` に対してセルフテスト操作を実行します。
- アプライアンスでエラー状態が発生した場合は、現在のログと過去 3 日間のすべてのログが収集されます。
- 次に、ログは詳しい分析とサポートのために Veritas AutoSupport サーバーにアップロードされます。これらのエラーログはアプライアンスでも格納されます。`/log/upload/<date>` フォルダからこれらのログにアクセスできます。
- エラー状態が 3 日後も発生した場合は、ログが再アップロードされます。

p.87 の「コールホームについて」を参照してください。

p.86 の「AutoSupport について 」を参照してください。

SNMP について

Simple Network Management Protocol (SNMP) は、ネットワークデバイス間の管理情報の交換を支援するアプリケーション層プロトコルです。構成に応じて、伝送制御プロトコル (TCP) またはユーザーデータグラムプロトコル (UDP) を使います。ネットワーク管理者は、SNMP を使用して、ネットワークパフォーマンスの管理、ネットワーク上の問題の検出と解決、およびネットワークの拡張計画を実行できます。

SNMP はマネージャモデルとエージェントモデルに基づいています。このモデルはマネージャ、エージェント、管理情報データベース、管理対象オブジェクト、ネットワークプロトコルで構成されています。

マネージャは、ネットワーク管理者と管理システム間のインターフェースを提供します。エージェントは、マネージャと管理対象の物理デバイス間のインターフェースを提供します。

マネージャとエージェントは、Management Information Base (MIB) および比較的少ないコマンドセットを使用して情報を交換します。MIB は、状態や説明といった個々の変数を枝の葉として表現するツリー構造で構成されています。数値タグにより表現されるオブジェクト識別子 (OID) によって、MIB および SNMP メッセージの各変数が一意に識別されます。

バージョン 3.1 以降の NetBackup appliance では、SNMP V2 がサポートされます。

ソフトウェアバージョン 4.0 以降では SNMP V3 もサポートされます。

Management Information Base (MIB) について

SNMP の各要素は、それぞれ独自の特性を備えた特定のオブジェクトを管理します。各オブジェクトと特性には、一意のオブジェクト識別子 (OID) が関連付けられています。各 OID は、小数点によって区切られた数字 (1.3.6.1.4.1.48328.1 など) で構成されています。

これらの OID はツリーを形成します。MIB は、読み取り可能なラベルと、オブジェクトに関連するさまざまなパラメータを持つ各 OID に関連付けられています。MIB は、SNMP メッセージの生成や解読に使用するデータ辞書として機能します。この情報は MIB ファイルとして保存されます。

Web コンソールの［設定 (Settings)］、［通知 (Notification)］、［アラートの構成 (Alert Configuration)］ページから、SNMP の MIB ファイルの詳細を確認できます。ハードウェア監視関連のトラップ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、［SNMP サーバーの構成 (SNMP Server Configuration)］ページの［SNMP の MIB ファイルを表示 (View SNMP MIB file)］をクリックします。

アプライアンスシェルメニューで `Settings > Alerts > SNMP ShowMIB` コマンドを使用して SNMP の MIB ファイルを表示することもできます。

11

リモート管理モジュール (RMM) セキュリティ

この章では以下の項目について説明しています。

IPMI 設定の紹介

アプライアンス用にインテリジェントプラットフォーム管理インターフェース (IPMI) サブシステムを構成できます。IPMI サブシステムは、予想外の停電によって接続済みのシステムが終了する場合に役立ちます。このサブシステムはオペレーティングシステムとは関係なく動作し、アプライアンスの背面パネルにあるリモート管理ポートを使って接続できます。

IPMI サブシステムとベリタスリモート管理ツールは、BIOS 設定を使って構成できます。ベリタスリモート管理ツールには、リモート管理ポートを使うためのインターフェースがあります。これにより、アプライアンスの監視と管理をリモートから実行することができます。

推奨される IPMI 設定

このセクションでは、安全な IPMI 構成を確認するために推奨される IPMI 設定の一覧を示します。

ユーザー (Users)

IPMI ユーザーを作成する場合は、次の推奨事項を使用します。

- Null ユーザー名またはパスワードでアカウントを作成しないでください。
- 管理ユーザーの数を 1 人に制限します。
- 匿名ユーザーを無効にします。
- CVE-2013-4786 の脆弱性を緩和するには
  - オフライン辞書攻撃および総当り攻撃を防止するには強いパスワードを使用します。推奨されるパスワードの長さは 16 ~ 20 文字です。
  - できるだけ早期にデフォルトのユーザーパスワード (`sysadmin`) を変更します。
  - アクセス制御リスト (ACL) または隔離ネットワークを使って IPMI インターフェースへのアクセスを制限します。
  - IPMI プロトコル (CVE-2013-4786) に関連するセキュリティリスクを軽減するために、使用していない場合は IPMI プロトコルポート (623) をオフにしておきます。詳しくは、https://nvd.nist.gov/vuln/detail/CVE-2013-4786 を参照してください。

ログイン (Login)

IPMI ユーザーにログイン設定を適用する場合は、次の推奨事項を使用します。

表 11-1　　ログインセキュリティ設定

設定	推奨される値
ログイン試行に失敗しました	3
ユーザーのロックアウト時間（最短）	60 秒
強制 HTTPS	はい (Yes) IPMI 接続が常に HTTPS を使用して行われるように[強制 HTTPS (Force HTTPS)]を有効にします。
Web セッションタイムアウト	1800

KCS ポリシー制御モード

BIOS バージョン 2.01.0010 以降を使用して更新された NetBackup Appliance モデル 5250、5340、5350 の場合、IPMI コンソールにログインすると次のメッセージが表示されます。

```
KCS Policy Control Mode is Allow All.
This setting is intended for BMC provisioning and is
considered insecure for deployment.
```

KCS ポリシー設定は、オペレーティングシステムレベルでの IPMI コマンドの帯域内アクセスのみに影響するため、このメッセージは無視しても問題ありません。これらのコマンドには、root レベルのユーザーのみがアクセスできます。このデフォルトのポリシー設定は、以前のベリタス製品リリースのものと一致します。

LDAP 設定

ベリタスは OpenLDAP で LDAP 認証を有効にすることをお勧めします。IPMI サブシステムは Active Directory と互換性がありません。

SSL アップロード

新規またはカスタム SSL 証明書をインポートすることを推奨します。

リモートセッション

表 11-2 リモートセッションのセキュリティ設定

設定	推奨値
KVM 暗号化	Stunnel **メモ:** BMC ファームウェア 01.51.11142 の KVM 暗号化から、AES および RC4 アルゴリズムのサポートが削除されました。
メディア暗号化	有効

また、HTML5 を介した iKVM を使用して、アプライアンスのシェルメニューにログインすることもできます。

メモ: HTML5 オプションは、ファームウェア (BIOS) バージョン 00.01.0016 以降がインストールされているアプライアンスでのみ利用できます。

暗号化の推奨事項

IPMI ユーザーの認証なしの処理またはアクティビティを防止するには、特定の暗号化を無効にする必要があります。詳しい説明が必要な場合は、テクニカルサポートに連絡して、担当者に記事番号 000127964 について問い合わせます。

イーサネット接続設定

IPMI 専用のイーサネット接続を使用し、物理サーバー接続を共有しないようにします。

- 固定 IP を使用してください。
- DHCP を使用しないでください。

RMM ポート

次のポートは、リモート管理モジュールを構成すると表示されます。

表 11-3 RMM ポート

ポート	サービス	説明	5240 のデフォルトの状態	5340、5250、5350 のデフォルトの状態
80	HTTP	アウトオブバンド管理 (ISM+ または RM*)	無効	無効
443	HTTP	アウトオブバンド管理 (ISM+ または RM*)	有効	有効
5120	RMM	ISO および CD-ROM のリダイレクト	有効	無効
5124	RMM (セキュリティで保護)	CD-ROM	無効	有効
22 または 66	SSH	CLI アクセス	無効	無効
(UDP) 623	IPMI over LAN	アウトオブバンド管理 (ISM+ または RM*)	無効	無効
5340、5250、5350 固有のポート				
5900	KVM	CLI アクセス、ISO および CD-ROM のリダイレクト	該当なし	無効
5902	KVM (セキュリティで保護)	CLI アクセス、ISO および CD-ROM のリダイレクト	該当なし	有効
623	RMM	フロッピーリダイレクト	該当なし	無効
627	RMM (セキュリティで保護)	フロッピーリダイレクト	該当なし	有効
5240 固有のポート				
7578	KVM	CLI アクセス	有効	該当なし

ポート	サービス	説明	5240 のデフォルトの状態	5340、5250、5350 のデフォルトの状態
7582	KVM (セキュリティで保護)	CLI アクセス	無効	該当なし
5123	RMM	フロッピーリダイレクト	有効	該当なし
5127	RMM (セキュリティで保護)	USB またはフロッピー	無効	該当なし

+ NetBackup 統合型ストレージマネージャ

*ベリタスリモート管理 – リモートコンソール

メモ: ポート 7578、5120、5123 は非暗号化モード用です。ポート 7582、5124、5127 は暗号化モード用です。

リモート管理モジュールでの SSH の有効化

インストール時に、ポート 20 (ssh) がリモート管理モジュールの IPMI に対して自動的に遮断されます。次の手順に従って、SSH を有効にします。

リモート管理モジュールで SSH を有効にするには

1. ベリタスリモート管理モジュールにログインします。
2. [構成 (Configuration)]タブの左ペインで、[セキュリティ設定 (Security Settings)]を選択します。
3. [オプションのネットワークサービス (Opional Network Services)]で、[SSH]の隣の[有効化 (Enable)]チェックボックスにチェックマークを付けます。
4. [保存 (Save)]をクリックします。

デフォルトの IPMI SSL 証明書の置換

IPMI Web インターフェースにアクセスするために使うデフォルトの IPMI SSL 証明書を信頼できる内部または外部の認証局 (PEM 形式)、または自己署名証明書により署名された証明書に置換することを推奨します。次の手順で、Linux コンピュータで最小限の自己署名証明書を作成して IPMI Web インターフェースにインポートできます。

Linux コンピュータに最小限の自己署名証明書を作成して IPMI Web インターフェースにインポートするには、次の操作をします。

1 次のコマンドを実行して ipmi.key と呼ばれるプライベートキーを生成します。

```
$ openssl genrsa -out ipmi.key 2048

Generating RSA private key, 2048 bit long modulus

.....+++

 .+++

 e is 65537 (0x10001)
```

2 各フィールドに適切な値を入力して次のように、ipmi.key を使って ipmi.csr という証明書の署名要求を生成します。

メモ: ブラウザに余分な警告が表示されないようにするには、CN を IPMI インターフェースの完全修飾ドメイン名に設定します。入力するのは識別名 (DN) と呼ばれる名前です。

```
$ openssl req -new -key ipmi.key -out ipmi.csr
```

次のガイドラインを参照して、証明書要求に入れる情報を入力します。

国名 (2 文字のコード) [AU]:	国の名前を入力します。たとえば、US。
都道府県名 (省略しない) [Some-State]:	都道府県の名前を入力します。たとえば、OR。
地域名 (たとえば、市区町村) []:	地域名を入力します。たとえば、Springfield。
組織名 (たとえば、会社) [Internet Widgits Pty Ltd]:	組織の名前を入力します。たとえば Veritas です。
組織単位名 (たとえば、部署) []:	組織単位の名前を入力します。
共通名 (たとえば、自社名) []:	hostname.your.company と入力します。
電子メールアドレス []:	電子メールアドレスを入力します。たとえば、email@your.company 。
チャレンジパスワード []:	適切なチャレンジパスワード (証明書要求と共に送信する追加属性) を入力します。
会社名 (省略可能) []:	適切な会社名 (証明書要求と共に送信する追加属性) を入力します (省略可能)。

メモ: フィールドを空白のままにするには「.」と入力します。

3 ipmi.key で ipmi.csr に署名し、次のように 1 年間有効な ipmi.crt と呼ばれる証明書を作成します。

```
$ openssl x509 -req -in ipmi.csr

-out ipmi.crt -signkey ipmi.key

-days 365

 Signature ok

 subject=/C=US/ST=OR/L=Springfield

/O=Veritas/OU=Your OU/

CN=hostname.your.company/

emailAddress=email@your.company


Getting Private key
```

4 ipmi.crt と ipmi.key を連結して ipmi.pem と呼ばれる証明書を PEM 形式で作成します。

```
$ cat ipmi.crt ipmi.key > ipmi.pem
```

5 アプライアンスの IPMI Web インターフェースにアクセスできるホストに ipmi.pem をコピーします。

6 ベリタスリモート管理 (IPMI Web インターフェース) にログインします。

7 [設定 (Settings)] > [SSL]をクリックします。

アプライアンスに[SSL のアップロード (SSL Upload)]ページが表示されます。

8 証明書をインポートするには[SSL のアップロード (SSL Upload)]ページで[ファイルを選択 (Choose File)]をクリックします。

9 ipmi.pem を選択して[アップロード (Upload)]をクリックします。

10 SSL 証明書がすでに存在することを示す警告が表示されることがあります。続行するには[OK]をクリックします。

11 キーをインポートするには、再び[ファイルを選択 (Choose File)]をクリックします(このボタンの隣には[新しいプライバシーキー (New Privacy Key)]があります)。

12 ipmi.pem を選択して[アップロード (Upload)]をクリックします。

13 証明書とキーを正常にアップロードしたことを示す確認メッセージが表示されたら、[OK]をクリックして Web サービスを再起動します。

14 ベリタスリモート管理インターフェース (IPMI Web インターフェース) を閉じてから再び開いて、新しい証明書が存在していることを確認します。

12

STIG と FIPS への準拠

この章では以下の項目について説明しています。

NetBackup appliance の OS STIG の強化

セキュリティ技術導入ガイド (STIG) では、情報システムとソフトウェアのセキュリティを向上するための技術ガイドを提供し、悪質なコンピュータ攻撃を防ぎます。この種のセキュリティは、強化とも呼ばれます。

ソフトウェアバージョン 3.1 以降、セキュリティの向上のため、OS STIG 強化ルールを有効にすることができます。これらのルールは、DISA (国防情報システム局) からの次のプロファイルに基づいています。

Red Hat Enterprise Linux 7 Server V1R4 用の STIG

これらのルールを有効にするには、次のコマンドを使用します。

`Main_Menu > Settings > Security > Stig Enable` の後に、メンテナンスパスワードを入力します。

STIG の有効化については、次の注意点があります。

- オプションが有効になっていると、強制的に適用されるルールのリストが表示されます。コマンド出力にも、強制的には適用されないすべてのルールの例外が表示されます。
- このコマンドでは、個々のルールの制御は許可されません。
- 高可用性 (HA) 設定のアプライアンス (ノード) の場合、切り替え後に正しく作動するように、各ノードでこの機能を手動で有効にする必要があります。
- オプションを有効にすると、関連付けられたルールを無効にするには、出荷時設定へのリセットが必要です。

- LDAP (Lightweight Directory Access Protocol) を設定する場合は、このオプションを有効にする前に、TLS (Transport Layer Security) を使用するように設定することをお勧めします。

メモ: STIG 機能が有効になっているアプライアンスをアップグレードするか、このアプライアンスに EEB をインストールする必要がある場合、午前 4 時から午前 4 時半の間には計画しないでください。このベストプラクティスに従うと、AIDE データベースと監視対象ファイルの自動アップデートの中断を防ぐことができます。自動アップデートが中断されると、アプライアンスで複数の警告メッセージが生成される可能性があります。

4.1 リリース以降、すべての STIG ルールの一覧がベリタスのサポートサイトに別々のマニュアルで掲載されるようになりました。現在、OS とアプリケーションセキュリティの STIG 用に 2 つのチェックリストが利用可能です。これらのマニュアルの入手方法については、ベリタスダウンロードセンターの［最新リリース (Latest releases)］ページに移動して［NetBackup Appliance OS］に移動し、［詳細はこちら (Learn more)］をクリックします。

NetBackup appliance における FIPS 140-2 への準拠

FIPS (連邦情報処理標準) には米国連邦政府とカナダ政府のコンピュータシステムに対するセキュリティと相互運用性の必要条件が定義されています。米国国立標準技術研究所 (NIST) は、暗号化モジュールの検証に関する必要条件と標準をまとめた FIPS 140 文書シリーズを発行しています。FIPS 140-2 標準には、暗号化モジュールのセキュリティ要件が指定されており、ハードウェアとソフトウェアの両方のコンポーネントに適用されます。対称キー暗号化と非対称キー暗号化、メッセージ認証、ハッシュの承認済みセキュリティ機能についても説明されています。

メモ: FIPS 140-2 標準とその検証プログラムについて詳しくは、次のリンクにアクセスしてください。

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

---

Java の FIPS 検証

NetBackup appliance 4.1 以降、すべての Java ベースのサービスで FIPS 140-2 標準がデフォルトで有効になっています。FIPS 検証は、SafeLogic 社の CryptoComply モジュールを使用して実行されます。

MSDP および VxOS の FIPS 検証

NetBackup appliance リリース 3.1.2 以降では、MSDP および VxOS で FIPS 140-2 標準を有効にできます。MSDP および VxOS で使用される NetBackup 暗号化モジュールは、FIPS によって検証されています。

VxOS で FIPS を有効にすると、sshd は FIPS 認定済みの次の暗号を使用します。

- aes128-ctr
- aes192-ctr
- aes256-ctr

VxOS の FIPS を有効にした後、古い SSH クライアントが Appliance へのアクセスを拒否する場合があります。リストされた暗号を SSH クライアントがサポートしていることを確認し、必要に応じて最新バージョンにアップグレードしてください。デフォルトの暗号設定は通常 FIPS 準拠ではないため、SSH クライアント構成でそれらを手動で選択することが必要になる場合があります。

NetBackup MSDP と VxOS 用の FIPS 140-2 標準は、次のコマンドを使用して有効にできます。

- Main Menu > Settings > Security > FIPS Enable MSDP の後に、メンテナンスパスワードを入力します。
  MSDP オプションを有効または無効にすると、その時点で進行中のすべてのジョブが終了し、NetBackup サービスが再起動します。ベストプラクティスとしては、最初にすべてのジョブを手動で停止してから、この機能を有効または無効にすることをお勧めします。

  メモ: NetBackup appliance の以前のバージョンからアップグレードした場合は、FIPS 準拠アルゴリズムを使用するように既存のデータを変換した後にのみ MSDP を有効にしてください。データ変換の現在の状態を確認するには、crcontrol --dataconvertstate コマンドを使用します。状態が[終了 (Finished)]に設定される前に MSDP を有効にすると、データ復元エラーが発生する可能性があります。

- Main Menu > Settings > Security > FIPS Enable VxOS の後に、メンテナンスパスワードを入力します。
  VxOS オプションを有効または無効にすると、アプライアンスが再起動し、ログイン中のすべてのユーザーがセッションから切断されます。ベストプラクティスとしては、この機能を有効または無効にする前に、すべてのユーザーに事前に通知を送ることをお勧めします。
- Main Menu > Settings > Security > FIPS Enable All の後に、メンテナンスパスワードを入力します。

All オプションを有効または無効にすると、アプライアンスが再起動し、ログイン中のすべてのユーザーがセッションから切断されます。ベストプラクティスとしては、この機能を有効または無効にする前に、すべてのユーザーに事前に通知を送ることをお勧めします。

メモ: NetBackup Appliance の高可用性 (HA) 設定では、HA 設定の構成が完了した後にのみ、両方のノードで FIPS 機能を有効にすることができます。FIPS 構成は両方のノードで同じである必要があります。HA 設定が完了する前にどちらかのノードで FIPS が有効になっている場合は、HA 設定を完了する前に、そのノードで FIPS を無効にする必要があります。

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

A

セキュリティのリリース内容

この付録では以下の項目について説明しています。

NetBackup Appliance のセキュリティリリース内容

次のリストには、解決された既知のセキュリティの問題およびこのリリースの NetBackup Appliance に含まれている既知の問題が掲載されています。

バージョン 4.1 の一般的なリリース内容

アプライアンスソフトウェアは RHEL 7.9 カーネルを使用しています。次のセキュリティ脆弱性に対処するパッケージとライブラリの一部が更新されました。

- RHSA-2021:1452
- CVE-2021-27219
- CVE-2016-4658
- CVE-2020-25648
- CVE-2021-22112
- CVE-2017-18640
- CVE-2020-13956
- CVE-2021-20328
- CVE-2021-21345
- CVE-2021-21346
- CVE-2021-21350
- CVE-2021-21344
- CVE-2021-21347

- CVE-2021-21351
- CVE-2021-21342
- CVE-2021-21349
- CVE-2021-21343
- CVE-2021-21341
- CVE-2021-21348
- CVE-2021-23358
- CVE-2021-27568
- CVE-2021-20277
- CVE-2021-26937
- CVE-2014-2524

索引