VERITAS

NetBackup セキュリティ搭載の Flex アプライアンス

Veritas Flex アプライアンスは、バックアップデータを防御し、ソフトウェアとハードウェアでリカバリするための改ざん不可能な包括的ストレージソリューションです。このホワイトペーパーでは、Veritas NetBackup™ ソリューション搭載の Flex アプライアンスの侵入検知および防止、OS 強化、マルチテナントセキュリティ機能について説明します。

ベリタスホワイトペーパー | 2020 年 10 月

目次

はじめに

概要

銀行、テクノロジー、小売店、政府機関へのサイバー攻撃に関する事件が注目を集めている中、各企業は壊滅的な侵害を受け、次の被害者となるような事態を避けなければなりません。今日、セキュリティ脅威はあらゆる企業にとって懸念事項です。ランサムウェア攻撃、ハードウェア障害、偶発的または意図的なデータ破壊のいずれの場合も、データ損失インシデントが顧客に壊滅的な影響を及ぼす可能性があります。

Veritas Flex アプライアンスなら、俊敏性、回復力、拡張性、シンプルさを備えた Veritas NetBackup™ データ保護を実現します。Flex アプライアンスは、セキュリティが強化された Linux (SELinux) を使用して侵入防止および侵入検知、OS の強化を実現します。NetBackup ソフトウェアと Flex アプライアンスは、バックアップデータを防御し、ソフトウェアとハードウェアでリカバリするための改ざん不可能な包括的ストレージソリューションです。

説明範囲

このドキュメントでは、Flex アプライアンスでの SELinux IDS/IPS、OS の強化、マルチテナント機能について技術的な詳細を提供することを目的としています。

侵入検知および侵入防止システム

企業は、顧客のデータを悪質な攻撃や破壊から保護する必要があります。データ損失を防止するため、ネットワークおよびシステム監視で整合性と安全性を保証する必要があります。インシデントの発生時に、管理者とセキュリティチームがリアルタイムで脅威に対応できるようにするためのアラートが必要です。

ベリタスは、セキュリティを第一の目的として Flex アプライアンスを開発しました。Linux オペレーティングシステムや NetBackup のコアアプリケーションなどのアプライアンスの各要素については、業界標準のセキュリティ製品と高度なセキュリティ製品の両方で脆弱性に関するテストが実施されています。このような対策により、不正アクセスのリスク、またその結果としてのデータの損失や窃盗が最小限に抑えられるのです。Flex アプライアンスでは、Red Hat でサポートされている組み込みの SELinux を使用して役割、プラットフォーム、サービス、アプリケーションを保護します。

IDS と IPS の概要

侵入検知システム (IDS) は、システムおよびネットワークアクティビティで不正なエントリや悪質なアクティビティを分析して、システムを攻撃、誤使用、侵害から守ります。IDS では、ネットワークアクティビティとシステム設定で脆弱性を監視および監査し、データ整合性の分析が可能です。IDS には管理コンソールとセンサーが含まれています。コンソールは管理およびレポートのためのものであり、センサーはホストまたはネットワークをリアルタイムで監視するエージェントです。IDS には、以前に検知された攻撃のパターンを表す攻撃シグネチャのデータベースがあり、

ホストベースの IDS とネットワークベースの IDS の 2 種類の一般的な IDS があります。ホストベースの IDS では、各ホストに検知システムを導入する必要があり、ネットワークベースの IDS では、パケットが単一デバイスに送り込まれ、そこから特定のホストへ送信されます。

侵入防止システムシステム (IPS) は、ファイアウォールを強化し、危険なコンテンツを選定するための分析層を構築しています。IPS はネットワークをアクティブに分析し、ネットワークに入るすべてのトラフィックフローで必要とされるアクションを自動的に実行します。IPS は侵入を検知すると、トラフィックをブロックし、標的に到達しないようにします。こうしたアクションには、悪質なパケットの削除、送信元アドレスへのトラフィックのブロック、接続のリセットなどがあります。

Flex アプライアンスの IPS/IDS ソリューション全体に、以下のような機能があります。

- 強化された Linux OS コンポーネント
- 基盤となるホストシステムの整合性が、OS の脆弱性によって損なわれないようにするためのマルウェア防止または封じ込め
- システム権限に関係なく、アプライアンスデータアクセスをアクセスが必要なプログラムやアクティビティのみに厳密に制限するデータ保護
- 強化されたアプライアンススタック
- アプリケーションまたは信頼できるプログラムとスクリプトによって変更を厳密に制御する、ロックされたアプライアンスアプリケーションバイナリと構成設定
- 拡張された検知および監査機能
- 重要なユーザーまたはシステムアクションの可視性の向上により、コンプライアンス規制 (PCI など) に対応する有効かつ完全な補完制御としての監査証跡

Symantec Data Center Security

Veritas NetBackup アプライアンスは、Symantec Data Center Security (SDCS) を使用してデータセンター内のサーバーを保護します。SDCS ソフトウェアはアプライアンスに含まれており、アプライアンスソフトウェアのインストール中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および侵入検知テクノロジーを使用してアプライアンスを保護します。最小権限の封じ込めアプローチを使用しているため、セキュリティ管理者がデータセンター内の複数のアプライアンスを一元管理できます。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 アプライアンス IPS および IDS ポリシーを適用します。SDCS は、中央の SDCS マネージャを使用して、複数のアプライアンスおよび SDCS が管理するその他のエンタープライズシステム全体のセキュリティを統合して表示します。

SELinux 搭載の Flex アプライアンス

Flex Appliance 2 0 OS には、データのセキュリティを確保するための複数の機能が含まれています。アプライアンスの各要素については、業界標準のセキュリティ製品と高度なセキュリティ製品の両方を使用して脆弱性に関するテストが実施されています。こうした対策により、不正アクセスのリスク、またその結果としてのデータの損失や窃盗が最小限に抑えられます。(SDCS と SELinux 搭載の Flex アプライアンスの比較については、表 1 を参照してください)

Flex 2 0 OS のセキュリティ機能は次のとおりです。

- SELinux を含む OS セキュリティの強化
- 追加のアクセス制限を設定し、指定された保持期間中のデータ削除をブロックする、ロックダウンモードと WORM ストレージサポート
- パスワードポリシーの強化:
  - デフォルトパスワードをシステム上でアクティブなままにしないための初回設定時の強制的なパスワード変更
  - セキュリティ技術導入ガイド (STIG) を検証用に使用するオプションを含む、独自のパスワードポリシーの設定機能
  - ログインに 3 度失敗したホスト管理者のアカウントを 15 分間ロックする、Flex アプライアンスシェルでの追加のパスワード保護
- 非アクティブな状態が 10 分続いた場合に Flex アプライアンスコンソールと Flex アプライアンスシェルからユーザーを自動的にサインアウトするセッションタイムアウト

SELinux の概要

SELinux は、Linux カーネルに組み込まれ、ブート時にロードされる Linux セキュリティモジュール (LSM) です。SELinux は管理者が制御するセキュリティポリシーによって駆動され、システム上のアプリケーション、プロセス、ファイルのアクセス制御を定義します。アプリケーションまたはプロセス (サブジェクトと呼ばれます) がファイルなどのオブジェクトへのアクセスを要求すると、サブジェクトとオブジェクト用の権限がキャッシュされているアクセスベクトルキャッシュ (AVC) を使ってチェックします。図 1 に、サブジェクトがオブジェクトへのアクセスを取得する方法を示します。

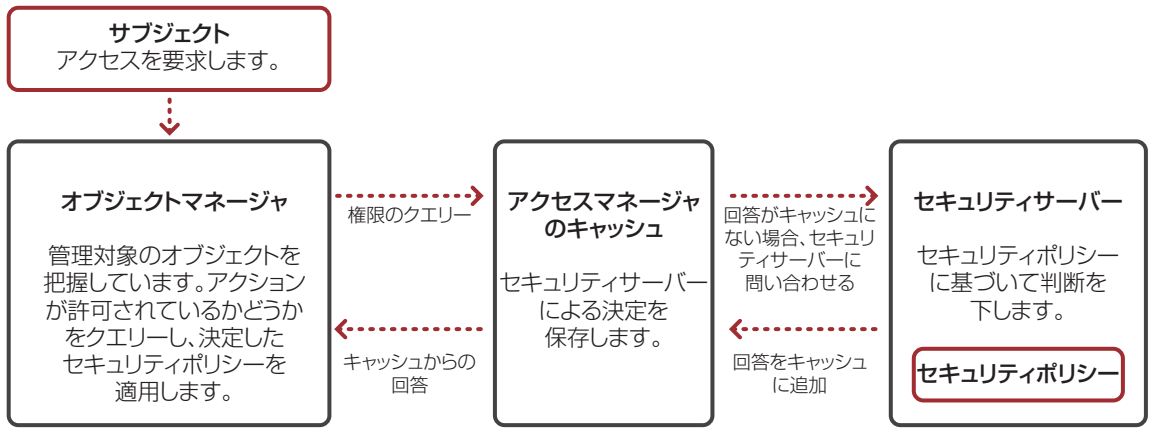

図 1. SELinux でサブジェクトがオブジェクトへのアクセスを取得する方法の概要。

SELinux は、ホストファイルシステムに対するコンテナ攻撃をコンテナ分離で防止するために使用されます。標準の Linux セキュリティモデルでは、スーパーユーザー「root」がすべてのセキュリティキャッシュを迂回できます (ユーザーが実行可能ファイルの所有者の権限を使って実行可能ファイルを実行するための setuid ビットの使用の可能性を含みます)。これにより、システムでセキュリティの問題が発生する可能性があります。SELinux はラベリングシステムであり、システム上の各オブジェクト (すべてのファイル、ディレクトリ、ソケットファイル、symlink、共有メモリ、セマフォまたは fifo ファイル)、およびすべてのサブジェクト (実行中のプロセスまたは Linux ユーザーエンティティ) を SELinux ラベル付きで表示します。

RBAC

役割ベースのアクセス制御 (RBAC) とは、企業内の役割に基づいてユーザーに権限を割り当てる概念のことです。Flex アプライアンスは、SELinux RBAC を使用してユーザーを承認し、OS の強化を実現します。ユーザー権限は、権利を取得するための役割を通じて付与されます。Flex アプライアンスログインアカウントは SELinux ユーザーにマップされます。図 2 は、Flex アカウントのホスト管理者、root ユーザー、および任意のユーザーのアカウントが staff_r 役割と gesut_r 役割を持つ SELinux ユーザー staff_u と guest_u にマップされることを示しています。

注意:

- Flex root アカウントとカスタマイズされたアカウントは、SELinux ユーザー guest_u に降格されます。
- SELinux ユーザーには 1 つまたは複数の役割が許可されます。これにより、特定のユーザーが持つことができる役割が制限されます。
- 役割は、権限にマップされ、1 つまたは複数のアプリケーションに対する特定のドメインおよび実行時権限を許可されます。

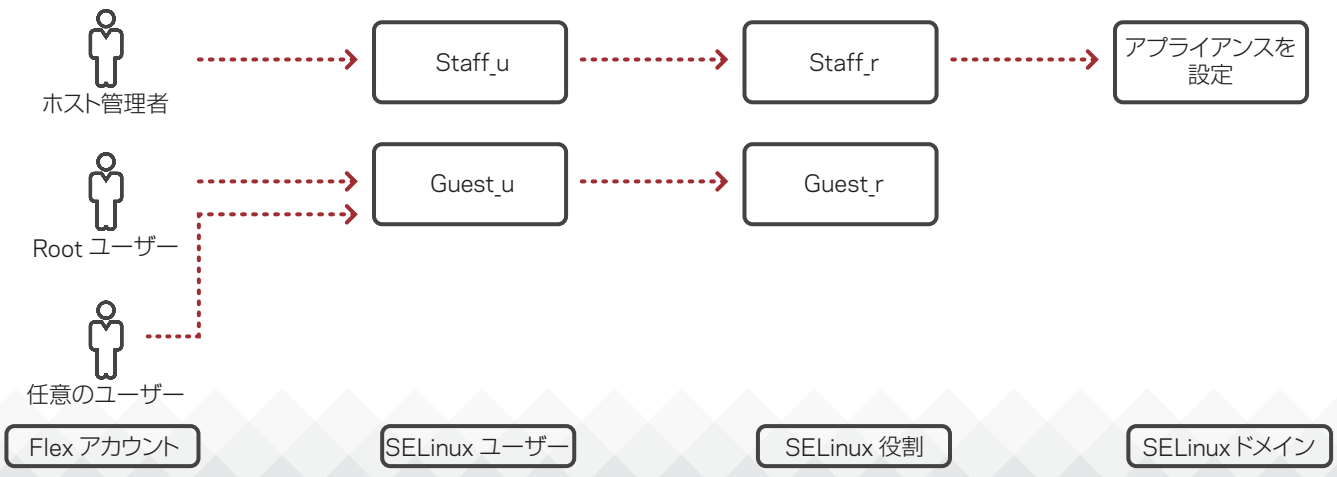

図 2. Flex アプライアンスが RBAC を使用してアカウントを SELinux ユーザーにマップする方法の概要。

プラットフォーム

Flex アプライアンスプラットフォームを保護するために、ワーカーサービスは root 以外のユーザーによって実行されます。Flex アプライアンスは、設定時にインフラ証明書を適用します。アプリケーションログは、インストール中の変更を追跡します。また、Flex アプライアンスは、Veritas InfoScale™ デバイスモジュールと統合して、シェルの基本 InfoScale 管理の昇格を可能にします。

サービスとアプリケーション

SELinux マルチカテゴリセキュリティ (MCS) により、ユーザーはファイルにカテゴリをラベル付けして、任意アクセス制御 (DAC) および Type Enforcement (TE) ロジックをさらに強制することができます。

Flex アプリケーションでは、排他的なデータアクセスを実現するために、アプリケーションとサービスはコンテナ化され、MCS をオンにして実行されます。Docker エンジンは、一意のカテゴリペア (CI、C2) を割り当て、コンテナ間の分離を実現します。Flex アプライアンスでは、各コンテナへの排他的アクセスのために、セキュリティコンテキストが組み込まれた専用ファイルシステムが表示されます。

証明書とログファイルに関しては、いくつかの設計上の考慮事項があります。

- 証明書については、ファイル共有を許可するために MCS が無効になっています。
- ログは /log/containers/service-name にアクセスします。
- MCS ポリシーはログのローテーションを許可します。
- コンテナサービスにはログファイルへのアクセスが許可されます。

	NetBackup アプライアンス SDCS	Flex アプライアンス SELinux
強化された Linux OS 導入	ポリシーにルールのセットが含まれ、各ルールにサブジェクト、リソースパス、アクセスルールが含まれます。	すべてのプロセスとファイルはラベリングされます。SELinux ポリシールールは、プロセスとファイル間の対話方法、およびプロセス間の対話方法を定義します。アクセスは、SELinux ポリシールールによって明確に許可されている場合のみ許可されます。
コンテナ保護	非推奨。	優れたサポート、Red Hat からの統合、高い柔軟性。
一元管理モード運用	利用可能	将来的に Syslog 転送で利用可能になる予定です。
統合とサポータビリティ	詳細度が低く、統合は不十分。	詳細な実行時オプション、開発者と管理者が使いやすい。
OS 保護	ユーザーは OS とポリシーを理解する必要があります。	Red Hat がデフォルトで OS ポリシーを提供します。
公共機関要件 STIG	非推奨。	STIG DISA プロファイルによる推奨アプローチとしての SELinux。
ベンダー	サードパーティ	カーネルに組み込まれた Red Hat サポート。
昇格	IPS は無効化されます。	IPS は無効化されません。

表 1. SDCS と Flex アプライアンス SELinux の比較

FLEX アプライアンスの改ざん不可能なストレージ

NetBackup ソフトウェアと Flex アプライアンスは、バックアップデータを防御し、ソフトウェアとハードウェアでリカバリするための改ざん不可能な包括的ストレージソリューションです。改ざんおよび消去不可能なデータは決められた期間内は変更できず、冗長性が不十分な場合にデータをサイバー犯罪者の侵入、内部の脅威、ランダムなディスク障害から保護します。これらのインスタンスに保存されるデータは、以下のセキュリティ対策によって保護されます。

- **改ざん防止**—バックアップイメージを読み取り専用として、バックアップ後に変更、破壊、または暗号化できないようにします。
- **消去防止**—バックアップイメージが期限切れになる前に削除されないよう保護します。データは悪質な削除から保護されます。

ロックダウンモード

NetBackup 8.3 マスターサーバーは、ストレージユニットと通信して、改ざん防止および消去防止機能と WORM (Write Once, Read Many) の最小および最大保持期間の設定を収集します。次に、マスターサーバーは、ストレージユニットで改ざん防止制御を設定し、WORM 保持期間ポリシーを適用します。NetBackup ソフトウェアは、改ざん防止ロックを視覚的に示してバックアップイメージを管理し、WORM 保持期間後に (コマンドラインインターフェース (CLI) 経由で) イメージを削除し、カタログに対するリーガルホールドを履行します。

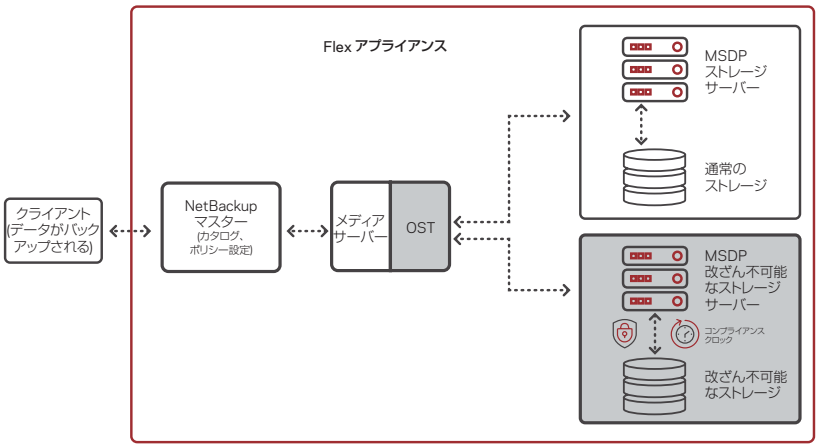

図 3. Flex アプライアンスが改ざん不可能なストレージを使用してデータを保護する方法の概要。

Flex アプライアンスは、改ざん不可能なストレージサーバーを実行して、WORM 機能、保持ロック、ランサムウェアとマルウェア脅威に対するプラットフォーム強化を実施します。コンプライアンスクロックは保持期間に使用され、OS 時間に依存しません。Flex アプライアンスには、Enterprise と Compliance の 2 つのロックダウン改ざん防止モードがあります。アプライアンスのロックダウンモードはいつでも有効化できます。Compliance-mode または Enterprise-mode MSDP ストレージコンテナを選択できますが、混在させることはできません。(図 3 を参照してください。) 表 2 に、Enterprise mode と Compliance mode の違いを示します。

	Enterprise Mode	Compliance Mode
WORM ストレージインスタンス作成	WORM ストレージインスタンスを作成できます。	WORM ストレージインスタンスを作成できます。
WORM ストレージインスタンス削除	管理者は、改ざん不可能なデータがない場合、WORM ストレージインスタンスを削除できます。ただし、改ざん不可能なデータが存在する場合は、デフォルトの管理者ユーザーのみが削除できます。	管理者は、改ざん不可能なデータがない場合、WORM ストレージインスタンスを削除できます。改ざん不可能なデータがある場合は、誰も WORM ストレージインスタンスを削除できません。
ロック削除	Flex アプライアンス MSDP ソリューションでの Enterprise ロックの削除は、2 ステップのプロセスです。 1 ストレージの「セキュリティ管理者」が保持期間を削除します (既存のストレージ管理者には権限がありません)。 2 NetBackup 管理者がカタログ経由でイメージ削除を要求します。	該当なし
セキュリティレベル変更	Enterprise mode から通常モードに変更するには、最初にすべての WORM ストレージインスタンスを削除する必要があります。	Enterprise mode または通常モードに降格するには、最初に WORM ストレージインスタンス上のすべてのデータを期限切れにしてからインスタンスを削除する必要があります。

表 2: Enterprise Mode と Compliance Mode の比較

MSDP 改ざん不可能なストレージサーバーの作成時に、最小および最大保持期間の設定が求められます。最小保持期間は、ストレージユニット内で WORM ファイルを保持できる最短期間です。最大保持期間は、WORM へのコミット時にファイルに設定できる最長の保持期間です (図 4 を参照してください)。保持期間の設定は CLI 経由で変更できます。

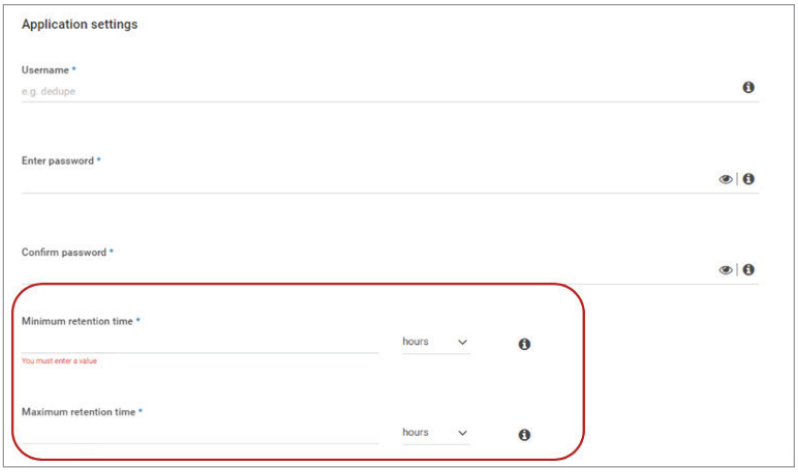

図 4. MSDP 改ざん不可能なストレージサーバーの作成時の最小および最大保持期間の設定。

NetBackup および Flex アプライアンスの改ざん防止ソリューションでは、Cohasset 社の不変性評価を提供します (Compliance mode の場合)。

- 証券取引委員会 (SEC) の 17 CFR § 240 17a-4(f)
- 金融業規制機構 (FINRA) 規則 4511(c)
- 商品先物取引委員会 (CFTC) の規制 17 CFR § 1 31(c)-(d)

改ざん不可能なストレージサーバーの保護

Flex アプライアンスでは、アプライアンス OS および MSDP コンテナへの root アカウントアクセスが排除されます。ホスト管理者アカウントのみがコンピューティングノードにログインできます。アカウントポリシーは、昇格したユーザーに特定の管理コマンド、シェルへのアクセス、Web UI 操作を許可するために使用されます。

以下のリストで、ファームウェアセキュリティの強化について説明します。

- ブート
  - 「単一ユーザー」モード/「レスキューモード」ブートオプションを削除
  - GRUB (GNU GRand Unified Bootloader) メニューの編集を無効化
- ストレージ
  - ストレージリセットなし (工場出荷設定リセット/イメージ復元は可能)
  - ストレージアレイをロックダウン

OS の強化

Flex アプライアンスでは、SELinux を使用してプラットフォームおよびホスト型アプリケーションを強化し、改ざん不可能なストレージへの不正アクセスを防止します。SELinux には、強制と許可の 2 つのモードがあります。Flex アプライアンスでは、強制モードで SELinux を有効にすると、ポリシールールを設定できます。

- Root ユーザーアカウント権限は縮小され、ほぼなくなります。ホスト管理者アカウントのみがコンピューティングノードのログインできます。
- Flex アプライアンスでは、昇格時にも IPS が有効のままになり、ユーザーは昇格しても権限の大半を保持し続けます。
- すべての Flex シェルおよび Web UI 操作を許可するためのポリシー。
- 昇格したユーザーに特定の追加管理コマンドを許可するためのポリシー。
- プラットフォーム証明書、トークン、ログ、コンプライアンスクロックデバイスのファイルラベリング。
- 各インスタンスおよびインフラサービスをストレージへの排他的アクセスによって制限します。
- インスタンスが systemd および NFS サービスを実行し、FUSE デバイスにアクセスし、NFS/CIFS 共有をマウントできるようにするためのポリシー。

セキュリティ技術導入ガイド

セキュリティ技術導入ガイド (STIG) は、ネットワーク、サーバー、コンピュータ、論理設計内のセキュリティプロトコルを標準化して全体的なセキュリティを高めるためのサイバーセキュリティ手法です。Flex アプライアンスは、STIG テンプレートを使用して、国防情報システム局 (DISA) プロファイルによるセキュリティ要件に対応します。

Flex アプライアンスは、以下によって STIG による OS の強化を実装しました。

- OS コマンドやシステム呼び出しなどの低レベルの操作に対する監査の有効化。
- Ctrl-Alt-Delete リブートの無効化。
- SSH root ログインの無効化。
- ホスト管理者アカウントの最大 10 の同時ログインセッション。
- インタラクティブ/ログインセッションの 10 分でのアイドルタイムアウト
- 15 分以内に Flex アプライアンスシェルでログインに 3 回連続で失敗した場合の 15 分間のアカウントロックアウト。
- パスワードポリシーの要件を強制するための Web UI オプション。各アプライアンスノードへ自動的に適用されます。

FLEX アプライアンスのマルチテナントアーキテクチャ

Flex アプライアンスは、NetBackup と密接に統合し、ベリタスアプリケーション向けの共通プラットフォームを提供してお客様の環境を簡素化します。複数の NetBackup および CloudCatalyst 設置対象 (ドメイン) を単一の Flex アプライアンスで統合し、データセンターのコストと複雑さを大幅に軽減することができます。(図 5 を参照してください。)

Docker コンテナソフトウェアは、Linux ベースの OS であるベリタスの最適化オペレーティングシステム (VxOS) で直接実行されます。VxOS は、Flex アプライアンスカーネル、ランタイムライブラリ、コンテナエンジンを備えています。Flex アプライアンスは、コンテナ分離とセキュリティテクノロジーを使用して、単一アプライアンスで NetBackup のインスタンスを複数使用する場合にユーザーの分離を維持します。NetBackup サービスユーザーは、VxOS に組み込まれたカーネル機能とネットワークおよびデータセグメント化の間で、互いにファイアウォールで効果的に保護されます。このマルチテナントアーキテクチャにより、複数の NetBackup ドメインをこの共通プラットフォームで実行できるため、NetBackup 環境が簡素化されます。

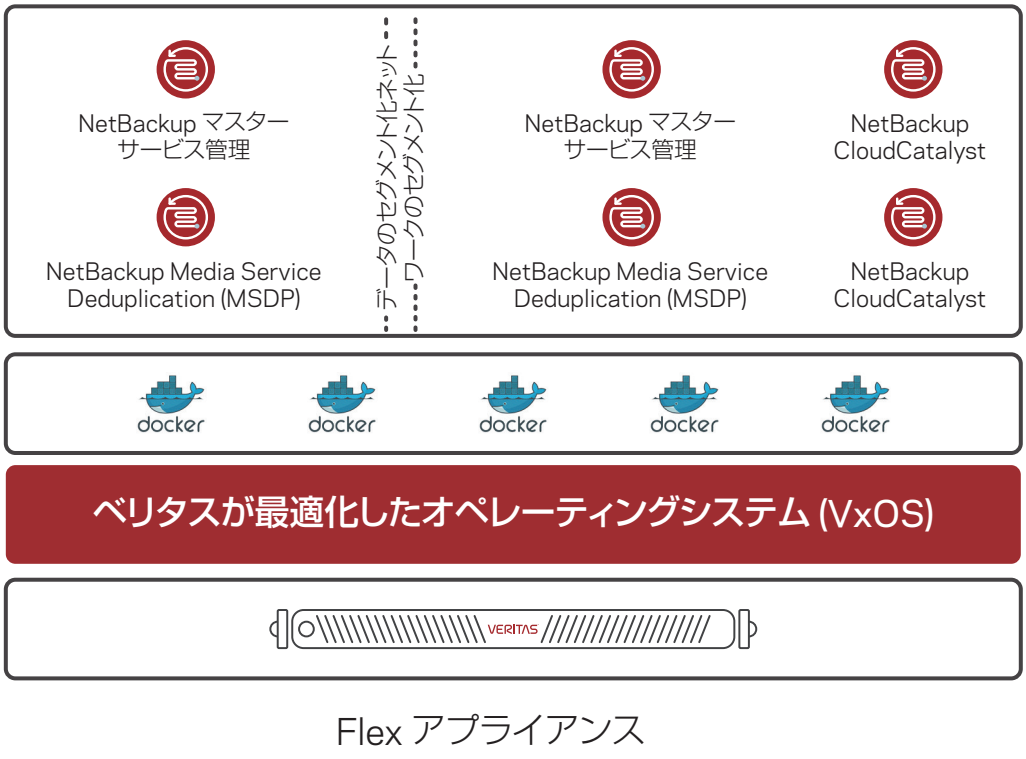

図 5. 複数の NetBackup および CloudCatalyst 設置対象 (ドメイン) の単一の Flex アプライアンスでの統合

参照情報

- Flex アプライアンスポータル:
  https://sort veritas com/DocPortal/pdf/130821112-136840843-1
- NetBackup 製品ドキュメント:
  https://sort veritas com/documents/doc_details/nbu/8 2/Windows%20and%20UNIX/Documentation
- SELinux とは:
  https://www redhat com/ja/topics/linux/what-is-selinux
- 管理者ガイド:
  https://access redhat com/documentation/ja-jp/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index
- コンテナ用の MCS:
  https://www redhat com/en/blog/why-you-should-be-using-multi-category-security-your-linux-containers
- Crash コース:
  https://www slideshare net/ffri/mr201406-a-re-introduction-to-se-linux

ベリタスについて

Veritas Technologies はデータの可用性および保護のグローバルリーダーです。複雑化したIT環境においてデータ管理の簡素化を実現するために、Fortune Global 500 の 87% を含む、先進企業 50,000 社以上が、ベリタスのソリューションを導入しています。ベリタスのエンタープライズ・データサービス・プラットフォームは、お客様のデータ活用を推進するため、データ保護とデータリカバリのオーケストレーションを実現して、ビジネスに不可欠なアプリケーションの可用性を常に確保し、複雑化するデータ規制対応に必要なインサイトを提供します。ベリタスのソリューションは信頼性とスケーラビリティに優れ、500 以上のデータソースと 60 のクラウドを含む 150 以上のストレージ環境に対応しています。ベリタステクノロジーズ合同会社は、Veritas Technologies の日本法人です。

ベリタステクノロジーズ合同会社
〒107-0052 東京都港区赤坂 1-11-44
赤坂インターシティ 4 階
www.veritas.com/ja/jp

各国オフィスとお問い合わせ先については、
弊社の Web サイトを参照してください。
www.veritas.com/ja/jp/company/contact

V1108 10/20