Oracle® ZFS Storage Appliance セキュリティーガイド、Release OS8.8.0

Part No: E97750-01
2018 年 11 月

Part No: E97750-01

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWeb サイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) か、聴覚に障害のあるお客様は (http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。

目次

Oracle ZFS Storage Appliance セキュリティーガイド

このガイドでは、セキュアなシステムを作成し、チーム全体で特定のセキュリティー目標を理解するのに必要なセキュリティー上の考慮事項について調査、検討、および強調します。アプライアンスを構成する前にこのガイドを参照して、利用可能なセキュリティー機能を活用し、必要なセキュリティーレベルを作成することをお勧めします。

このガイドをリファレンスとして使用すると、Oracle ZFS Storage Appliance のさまざまな特長および機能に関するセキュリティー上の考慮事項の詳細情報を見つけることができます。アプライアンスの構成手順については、『Oracle ZFS Storage Appliance 管理ガイド』を参照してください。

以降のセクションでは、Oracle ZFS Storage Appliance のセキュリティー機能および推奨事項について説明します。

- **最初のステップ** - アプライアンスの初期インストール時のログインセキュリティーと、システムの物理的セキュリティーに関する推奨事項について説明します。
- **管理モデル** - BUI および CLI を使ったリモートアクセス、BUI および CLI へのアクセスの制限、システムパッチ適用モデル、遅延更新、および構成のバックアップについて説明します。
- **アプライアンスユーザー** - アプライアンスを管理できる管理ロールと、ユーザー承認の管理について説明します。
- **アクセス制御リスト** - ファイルおよびディレクトリへのアクセスを許可または拒否するメカニズムについて説明します。
- **データサービス** - アプライアンスによってサポートされるデータサービスと、各種のデータサービスによって提供されるセキュリティーについて説明します。
- **ディレクトリサービス** - アプライアンス上で構成できるディレクトリサービスと、それらのセキュリティー上の問題について説明します。
- **システム設定** - フォンホーム、サービスタグ、Kerberos、SMTP、SNMP、syslog、システム ID、ディスクスクラブ、破棄の防止といったシステム設定について説明します。
- **セキュリティーログ** - セキュリティーに関連するログタイプについて説明します。

最初のステップ

このセクションでは、アプライアンスの初期インストール時のログインセキュリティーと、システムの物理的セキュリティーに関する推奨事項について説明します。

初期インストール

Oracle ZFS Storage Appliance は、アプライアンスソフトウェアが事前にインストールされた状態で提供されます。ソフトウェアをインストールする必要はなく、メディアは提供されません。

初期インストールは、デフォルトのアカウント名とパスワードで実行され、インストール後にデフォルトの root パスワードを変更する必要があります。Oracle ZFS Storage Appliance を出荷時のデフォルトにリセットすると、アプライアンスとサービスプロセッサの両方の root パスワードもデフォルトにリセットされます。

Oracle ZFS Storage Appliance の初期インストール時には、システムサービスプロセッサに関連付けられたデフォルトのアカウント名とパスワードがあります。このデフォルトアカウントによって、システム管理者のアプライアンスへの最初のアクセスが可能になります。管理者はその後、初期インストールの手順を実行する必要があります。必要な手順の 1 つは、新しいアプライアンス管理パスワードを設定することです。これにより、サービスプロセッサのデフォルトパスワードも同じ値にリセットされます。

物理的セキュリティー

システムへのアクセスを制御するには、コンピュータ環境の物理的なセキュリティーを管理する必要があります。たとえば、システムにログインしたままこれを放置することは不正アクセスを招く原因になります。コンピュータの周辺環境やコンピュータハードウェアは、不正アクセスから常に物理的に保護される必要があります。

Oracle ZFS Storage Appliance は、セキュリティー保護のための手段 (鍵、ロック、ツール、バッジなど) によりアクセスが制御されること、およびアクセスを許可された人物が、守る必要のある制限や注意事項の理由について説明を受けていることを想定しています。

管理モデル

このセクションでは、Oracle ZFS Storage Appliance の管理モデルのセキュリティーについて説明します。

リモート管理アクセス

このセクションでは、Oracle ZFS Storage Appliance のリモートアクセスセキュリティーについて説明します。

ブラウザユーザーインタフェース

ブラウザユーザーインタフェース (BUI) は、アプライアンスの一般的な管理に使用されます。BUI サービスの画面を使用すると、リモートアクセスのサービスや設定を表示および変更できます。

管理は、HTTP セキュア (HTTPS) ブラウザセッションを介して行われます。HTTPS セッションは、初期インストール時に Oracle ZFS Storage Appliance システムごとに一意に生成される自己署名付き証明書を使って暗号化されます。HTTPS セッションでは、デフォルトセッションタイムアウトは 15 分で、ユーザーによる定義が可能です。BUI に接続するために使用する SSL/TLS プロトコルおよび暗号を HTTPS サービスページから設定できます。

コマンド行インタフェース

コマンド行インタフェース (CLI) を使用すると、BUI で実行できるのと同じ管理アクションのほとんどを実行できます。

セキュアシェル (SSH) を使用すると、ユーザーは CLI への Secure Sockets Layer (SSL) 接続を介して Oracle ZFS Storage Appliance にログインできます。SSH は、日単位のログや analytics 統計を取り出すためなど、リモートホストから自動スクリプトを実行する手段として使用することもできます。CLI に接続するために使用する暗号および MAC を SSH サービスページから設定できます。

制限されたユーザー承認

管理アクセスは、root ユーザー、関連する権限で定義されたローカル管理者、および LDAP (Lightweight Directory Access Protocol) やネットワーク情報サービス (NIS) などの ID サーバーを通じて承認されたユーザーに制限されます。

また、アプライアンスでは Kerberos を使用して、BUI、CLI、および RESTful API を使用した管理ログインおよび NFS、HTTP、FTP、SFTP、SSH などのサービスへのアクセスに対してユーザーを認証できます。15 ページの「NFS 認証および暗号化オプション」に記載されているように、Kerberos は NFS プロトコルを使用する個々のシェアのセキュリティーを設定するためにも使用できます。

Oracle ZFS Storage Appliance RESTful API

Oracle ZFS Storage Appliance RESTful API を使用すると、Oracle ZFS Storage Appliance を管理できます。RESTful アーキテクチャーは、クライアントを構成せずに標準のハブ、ルーター、およびその他のネットワークシステムを介してサービスを透過的にリダイレクトする階層化されたクライアントサーバーモデルに基づいています。

Oracle ZFS Storage Appliance RESTful API では、BUI や CLI と同じ認証資格が使用されます。外部クライアントからのすべての要求は、アプライアンスの資格を使用して個別に認証され、ポート 215 上の HTTPS 接続を介して実行されます。RESTful API は、ユーザー定義可能なデフォルトのタイムアウトが 15 分である HTTPS セッションをサポートします。

RESTful API を使った Oracle ZFS Storage Appliance の管理については、『Oracle ZFS Storage Appliance RESTful アプリケーションプログラミングインタフェース (API) ガイド』 を参照してください。

システムの更新

最新のセキュリティー改善を利用するため、システムソフトウェアを最新に保つことをお勧めします。

システム更新は、システムソフトウェアのバイナリ全体の置換として適用されます。更新の前に、実行中のシステムプールのスナップショットが取得されます。これにより、管理者は必要に応じて前のバージョンにロールバックできます。

遅延更新

遅延更新は、システム更新の機能またはその一部ですが、システム更新の実行時にはアクティブにされません。管理者は、遅延更新を適用するかどうか、また適用するタイミングを決定します。システム更新時に適用されなかった更新は、その後のシステム更新時に引き続き利用できます。遅延更新の適用を選択する際、適用する更新を個別に選択することはできず、更新をすべて適用するか、一切適用しないかを選択できます。更新を適用したあとで、以前のシステムソフトウェアバージョンにロールバックすることはできません。

サポートバンドル

システムがフォンホームサポートに登録されている場合、メジャーな障害が発生すると、システムステータスが My Oracle Support に送信され、そこでエンジニアリングサポート担当者が調査を行い、サポートバンドルの作成が可能になります。My Oracle

Support に送信されるシステムステータス情報には、ユーザーデータは含まれず、構成情報だけが送信されます。

構成のバックアップ

システム構成をローカルに保存しておき、あとで復元できます。これらのバックアップには、ユーザーデータは含まれず、構成設定だけが保存されます。

アプライアンスのユーザー

Oracle ZFS Storage Appliance のユーザーには、2 つのタイプがあります。

- **データサービスユーザー** – ネットワークファイルシステム (NFS)、サーバーメッセージブロック (SMB)、ファイバチャネル、iSCSI (Internet Small Computer System Interface)、ハイパーテキスト転送プロトコル (HTTP)、ファイル転送プロトコル (FTP) などのサポートされているプロトコルを使用してファイルおよびブロックリソースにアクセスするクライアント。
- **管理ユーザー** - アプライアンス上で構成およびサービスを管理するユーザー。

このセクションは、管理ユーザーにのみ適用されます。

管理ユーザーのロール

管理者には、カスタムロールを割り当てることで権限を付与できます。ロールは、管理者に割り当てることのできる権限のコレクションです。承認レベルの異なるさまざまな管理者およびオペレータのロールを作成することもできます。スタッフメンバーには、不要な権限を割り当てずに、必要に応じて適切なロールを割り当てます。

シェアのフルアクセス管理者パスワードを使用する (たとえば、root パスワードをすべてのユーザーに割り当てる) よりも、ロールを使用した方がセキュアです。ロールにより、ユーザーは定義済みの承認セットに制限されます。さらに、ユーザーロールは監査ログ内で個別のユーザー名でトレース可能です。デフォルトでは、最小限の承認が含まれる「基本管理」というロールが存在します。

管理ユーザーは、次のものになることができます。

- **ローカルユーザー** - すべてのアカウント情報が Oracle ZFS Storage Appliance に保存されます。
- **ディレクトリユーザー** – 既存の NIS または LDAP アカウントが使用され、追加の承認設定がアプライアンスに保存されます。アプライアンスへのアクセス権限を既存の NIS/LDAP ユーザーに明示的に付与する必要があります。これらのユーザー

は、アプライアンスにログインしてアプライアンスを管理できるようになります。デフォルトではアクセス権限は付与されません。

管理スコープ

承認を使用すると、ユーザーはシェアの作成、アプライアンスのリブート、システムソフトウェアの更新などの特定のタスクを実行できます。承認のグループはスコープと呼ばれます。各スコープは、承認の数を制限するオプションのフィルタセットを保持できます。たとえば、すべてのサービスを再起動する承認の代わりに、フィルタを使用すると HTTP サービスだけを再起動できます。

アクセス制御リスト

Oracle ZFS Storage Appliance は、アクセス制御リスト (ACL) を使用してファイルアクセス制御を提供します。ACL は、特定のファイルまたはディレクトリへのアクセスを許可または拒否するメカニズムです。

Oracle ZFS Storage Appliance で提供される ACL モデルは、Windows ACL セマンティクスから派生した NFSv4 ACL モデルに基いています。これは、ファイルおよびディレクトリへのきめ細かなアクセスを提供する高機能な ACL モデルです。ストレージアプライアンス内のすべてのファイルおよびディレクトリは ACL を保持し、SMB と NFS のアクセス制御決定すべてで同じアルゴリズムが使用され、ファイルおよびディレクトリへのアクセスを許可または拒否するユーザーが決定されます。

ACL は、1 つ以上のアクセス制御エントリ (ACE) で構成されます。各 ACE には、ACE が付与または拒否するアクセス権、ACE の適用先ユーザー、および使用される継承レベルフラグのエントリが含まれます。

ACL の継承

NFSv4 ACL を使用すると、新たに作成されたファイルやディレクトリで ACE を個別に継承できます。ACE の継承は、初期構成時に管理者が ACL に設定する複数の継承レベルフラグによって制御されます。

ACL アクセスの決定

NFSv4 ACL は順序に依存しており、上から順に処理されます。いったんアクセス権が付与されたら、後続の ACE を取り除くことはできません。いったんアクセス権が拒否されたら、後続の ACE を許可することはできません。

SMB シェアレベル ACL

SMB シェアレベル ACL は、シェア内のファイルまたはディレクトリ ACL と組み合わされた ACL で、ファイルの有効なアクセス権を決定します。シェアレベル ACL は、ファイル ACL の上に別のアクセス制御レイヤーを提供して、より洗練されたアクセス制御構成を実現します。シェアレベル ACL は、ファイルシステムのエクスポート時に SMB プロトコルを使用して設定されます。ファイルシステムが SMB プロトコルを使用してエクスポートされない場合は、シェアレベル ACL を設定しても何も効果はありません。デフォルトでは、シェアレベル ACL はすべてのユーザーに完全な制御を許可します。

ZFS ACL プロパティー

ACL の動作および継承プロパティーは、NFS クライアントにのみ適用されます。SMB クライアントは、厳密な Windows セマンティクスを使用し、ZFS プロパティーよりも優先されます。異なるのは、NFS は POSIX セマンティクスを使用し、SMB クライアントは使用しない点です。プロパティーは、主に POSIX と互換性があります。

データサービス

次の表に、各データサービスの説明と使用されるポートを示します。

表 1 データサービス

サービス	説明	使用されるポート
NFS	NFSv3 および NFSv4 プロトコル経由でのファイルシステムアクセス	111 および 2049
iSCSI	iSCSI プロトコル経由での LUN アクセス	3260 および 3205
SMB	SMB プロトコル経由でのファイルシステムアクセス	SMB-over-NetBIOS 139 SMB-over-TCP 445 NetBIOS データグラム 138 NetBIOS ネームサービス 137
ウイルススキャン	ファイルシステムのウイルススキャン	
FTP	FTP プロトコル経由でのファイルシステムアクセス	21
HTTP	HTTP プロトコル経由でのファイルシステムアクセス	80
HTTPS	セキュアな受信接続用	443

サービス	説明	使用されるポート
NDMP	NDMP ホストサービス	10000
リモートレプリケーション	リモートレプリケーション	216 および 217
暗号化	ファイルシステムと LUN の透過的な暗号化	
シャドウ移行	シャドウデータ移行	
SFTP	SFTP プロトコル経由でのファイルシステムアクセス	218
TFTP	TFTP プロトコル経由でのファイルシステムアクセス	
ストレージエリアネットワーク	ストレージエリアネットワークのターゲットグループとイニシエータグループ	

最小限必要なポート

ネットワーク上のセキュリティーを提供するため、ファイアウォールを作成できます。ポート番号は、ファイアウォールの作成に使われ、ホストとサービスを指定して、ネットワーク上でトランザクションを一意に識別します。

次のリストに、ファイアウォールの作成に必要な最低限のポートを示します。

インバウンドポート

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

HTTP ファイル共有が使用されている場合 (通常は使用されない) の追加のインバウンドポート:

- tcp/443 (SSL WEB)
- tcp/80 (WEB)

アウトバウンドポート

- tcp/80 (WEB)

注記 - レプリケーションの場合、可能なかぎり GRE (Generic Routing Encapsulation) トンネルを使用します。これにより、トラフィックがバックエンドインタフェースで実行し、トラフィックを遅くする可能性のあるファイアウォールを回避できます。NFS コアで GRE トンネルを使用できない場合、フロントエンドインタフェース経由でレプリケーションを実行する必要があります。この場合、ポート 216 およびポート 217 も開いている必要があります。

NFS 認証および暗号化オプション

アプライアンスの機能によって Kerberos を使用して、管理ログインおよびサービスへのアクセスに対してユーザーを認証できるほか、Kerberos は NFS プロトコルを使用する個々のシェアのセキュリティーを設定するためにも使用できます。

NFS シェアは、デフォルトでは AUTH_SYS RPC 認証を使って割り当てられます。これらが Kerberos セキュリティーを使用してシェアされるように構成することもできます。AUTH_SYS 認証を使用すると、クライアントの UNIX ユーザー ID (UID) とグループ ID (GID) が NFS サーバーによってネットワーク上で認証なしで渡されます。この認証メカニズムは、クライアント上で root アクセスを持つユーザーであればだれでも簡単に破ることができるため、利用可能なほかのセキュリティーモードのいずれかを使用するのが最善です。

追加のアクセス制御をシェアベースで指定して、特定のホスト、DNS ドメイン、またはネットワークのシェアへのアクセスを許可または禁止できます。

セキュリティーモード

セキュリティーモードは、シェアベースで設定します。次のリストでは、利用可能な Kerberos セキュリティー設定について説明します。

- **krb5** - Kerberos V5 によるエンドユーザー認証
- **krb5i** - krb5 に完全性保護を加えたもの (データパケットに改ざんがないことが保証される)
- **krb5p** - krb5i にプライバシ保護を加えたもの (データパケットに改ざんがないことと暗号化されていることが保証される)

複数の Kerberos タイプの組み合わせをセキュリティーモード設定でも指定できます。組み合わせのセキュリティーモードにより、クライアントは一覧表示されている任意の Kerberos タイプでマウントできます。

Kerberos のタイプ

- **sys** - システム認証
- **krb5** - Kerberos v5 のみで、クライアントはこのタイプを使用してマウントする必要があります
- **krb5:krb5i** - Kerberos v5 に完全性を加えたもので、クライアントは一覧表示されている任意のタイプを使用してマウントできます
- **krb5i** - Kerberos v5 完全性のみで、クライアントはこのタイプを使用してマウントする必要があります
- **krb5:krb5i:krb5p** - Kerberos v5 に完全性またはプライバシを加えたもので、クライアントは一覧表示されている任意のタイプを使用してマウントできます

- **krb5p** - Kerberos v5 プライバシのみで、クライアントはこのタイプを使用してマウントする必要があります

iSCSI データサービス

Oracle ZFS Storage Appliance 上で LUN を構成すると、そのボリュームを iSCSI ターゲットにエクスポートできます。iSCSI サービスでは、iSCSI イニシエータが iSCSI プロトコルを使用してターゲットにアクセスできます。

このサービスは、iSNS プロトコルを使用した検出、管理、および構成をサポートします。iSCSI サービスは、チャレンジハンドシェイク認証プロトコル (CHAP) を使用して単方向 (ターゲットがイニシエータを認証する) および双方向 (ターゲットとイニシエータが相互に認証する) の両方の認証をサポートします。また、このサービスは RADIUS (Remote Authentication Dial-In User Service) データベースでの CHAP 認証データ管理もサポートします。

システムでは、2 つの独立したステップで、最初に認証を実行し、次に承認を実行します。ローカルイニシエータに CHAP 名と CHAP シークレットが指定されている場合は、システムによって認証が行われます。ローカルイニシエータに CHAP プロパティーが指定されていない場合は、認証が行われないため、すべてのイニシエータが承認の対象となります。

iSCSI サービスでは、イニシエータグループ内で使用できるイニシエータのグローバルリストを指定できます。iSCSI および CHAP 認証を使用する場合、RADIUS を iSCSI プロトコルとして使用して、選択した RADIUS サーバーにすべての CHAP 認証を持ち越すことができます。

RADIUS のサポート

RADIUS は、ストレージノードに代わって、集中管理されたサーバーを使用して CHAP 認証を実行するためのシステムです。iSCSI および CHAP 認証を使用する場合、iSCSI プロトコルに RADIUS を選択して iSCSI と iSCSI Extensions for RDMA (iSER) の両方を適用し、選択した RADIUS サーバーにすべての CHAP 認証を送信できます。

Oracle ZFS Storage Appliance が RADIUS を使用して CHAP 認証を実行できるようにするには、次の情報が一致する必要があります。

- アプライアンスは、RADIUS サーバーのアドレスと、この RADIUS サーバーと通信するときに使用するシークレットを指定する必要があります。
- RADIUS サーバーは、(たとえばクライアントファイル内の) エントリで、アプライアンスのアドレスおよび上記と同じシークレットを指定する必要があります。
- RADIUS サーバーは、(たとえばユーザーファイル内の) エントリで、イニシエータごとに CHAP 名および対応する CHAP シークレットを指定する必要があります。

- イニシエータが CHAP 名として自身の IQN 名を使用する場合 (推奨構成)、アプライアンスでは、イニシエータボックスごとに個別イニシエータエントリは必要ありません。RADIUS サーバーは、すべての認証手順を実行できます。
- イニシエータが個別の CHAP 名を使用する場合は、アプライアンスに、IQN 名から CHAP 名へのマッピングを指定する、そのイニシエータのためのイニシエータエントリが存在する必要があります。このイニシエータエントリで、そのイニシエータの CHAP シークレットを指定する必要はありません。

SMB データサービス

SMB プロトコルは、Common Internet File System (CIFS) とも呼ばれ、Microsoft Windows ネットワーク上のファイルへの共有アクセスを主に提供します。さらに、認証も提供します。

次の SMB オプションには、セキュリティー上の意味があります。

- **リストを共有する匿名アクセスを制限** - このオプションでは、クライアントがシェアリストを受信する前に SMB を使用して認証を行う必要があります。このオプションが無効な場合、匿名クライアントはシェアリストにアクセスできます。このオプションは、デフォルトでは無効になっています。
- **SMB 署名が有効** - このオプションにより、SMB 署名機能を使用した SMB クライアントとの相互運用性が有効になります。このオプションを有効にすると、署名されたパケットの署名が検証済みになります。このオプションを無効にすると、無署名のパケットが署名の検証なしで受け入れられます。このオプションは、デフォルトでは無効になっています。
- **SMB 署名が必要** - SMB 署名が必要な場合に、このオプションを使用できます。このオプションを有効にすると、すべての SMB パケットを署名する必要があり、署名しない場合には拒否されます。SMB 署名をサポートしないクライアントは、サーバーに接続できません。このオプションは、デフォルトではオフになっています。
- **アクセスベースの列挙を有効化** - このオプションを設定すると、クライアントの資格に基づいてディレクトリエントリがフィルタ処理されます。クライアントがファイルまたはディレクトリに対するアクセス権を持っていない場合、クライアントに返されるエントリのリストでそのファイルは省略されます。このオプションは、デフォルトでは無効になっています。

Active Directory ドメインモードの認証

ドメインモードでは、ユーザーが Microsoft Active Directory (AD) で定義されます。SMB クライアントは、Kerberos または NTLM 認証を使用して Oracle ZFS Storage Appliance に接続できます。

同じドメインまたは信頼できるドメイン内の Windows クライアントは、ユーザーが Oracle ZFS Storage Appliance の完全修飾ホスト名を使用して接続する場合は Kerberos 認証を使用し、それ以外の場合は NTLM 認証を使用します。

SMB クライアントが NTLM 認証を使用してアプライアンスに接続する場合、ユーザーの資格が AD ドメインコントローラに転送されて認証が行われます。これはパススルー認証と呼ばれます。

NTLM 認証を制限する Windows セキュリティーポリシーが定義されている場合、Windows クライアントは完全修飾ホスト名を使用してアプライアンスに接続する必要があります。詳細は、Microsoft Developer Network のこの記事を参照してください。

http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx

認証後に、ユーザーの SMB セッションに「セキュリティーコンテキスト」が確立されます。セキュリティーコンテキストで表されるユーザーは、一意のセキュリティー記述子 (SID) を保持します。SID は、ファイルの所有権を示し、ファイルアクセス権限の決定に使用されます。

ワークグループモードの認証

ワークグループモードでは、ユーザーが Oracle ZFS Storage Appliance 上でローカルに定義されます。SMB クライアントがワークグループモードのアプライアンスに接続すると、そのユーザーのユーザー名とパスワードのハッシュを使用してローカルでユーザーが認証されます。

アプライアンスがワークグループモードになっているときは、認証に使われるプロトコルの指定に LAN Manager (LM) 互換性レベルが使用されます。

次のリストに、各 LM 互換性レベルでの Oracle ZFS Storage Appliance の動作を示します。

- レベル 2: LM、NTLM、および NTLMv2 認証を受け入れる
- レベル 3: LM、NTLM、および NTLMv2 認証を受け入れる
- レベル 4: NTLM および NTLMv2 認証を受け入れる
- レベル 5: NTLMv2 認証のみを受け入れる

ワークグループユーザーの認証に成功すると、セキュリティーコンテキストが確立されます。マシンの SID とユーザーの UID の組み合わせを使って、アプライアンスで定義されたユーザー用に一意の SID が作成されます。すべてのローカルユーザーは、UNIX ユーザーとして定義されます。

ローカルグループと権限

ローカルグループは、追加の権限が付与されるドメインユーザーのグループです。Administrators は、ファイルの所有権を変更するためのファイルアクセス権を必要としません。Backup Operators は、ファイルのバックアップと復元のためのファイルアクセス制御を必要としません。

Microsoft 管理コンソールを使用した管理操作

適切なユーザーだけが管理操作にアクセスできるようにするため、Microsoft 管理コンソール (MMC) を使用してリモートで実行される操作に対してアクセス制限が設けられています。

次のリストに、ユーザーおよび許可される操作を示します。

- **通常ユーザー** - シェアの一覧表示。
- **Administrators グループのメンバー** - 開いているファイルと閉じているファイルの一覧表示、ユーザーの接続の切断、サービスとイベントログの表示。Administrators グループのメンバーは、シェアレベル ACL の設定や変更も可能です。

ウイルススキャン

ウイルススキャンサービスは、ファイルシステムレベルでウイルスをスキャンします。いずれかのプロトコルからファイルがアクセスされると、ウイルススキャンサービスは最初にそのファイルをスキャンし、ウイルスが見つかった場合はファイルのアクセス拒否と隔離を行います。スキャンは、Oracle ZFS Storage Appliance が接続する外部のエンジンにより実行されます。外部エンジンは、アプライアンスソフトウェアには含まれません。

最新のウイルス定義でスキャンされたファイルは、次の変更が行われるまで再スキャンされません。ウイルススキャンは、ウイルスを取り込みやすい SMB クライアントに対して主に行われます。NFS クライアントもウイルススキャンを使用できますが、NFS プロトコルの動作方法のために、SMB クライアントの場合ほど迅速にウイルスが検出されない可能性があります。

タイミング攻撃用の遅延エンジン

SMB は、タイミング攻撃を防ぐための遅延エンジンを実装していません。これは、Oracle Solaris 暗号化フレームワークに依存しています。

ネットワーク上のデータ暗号化

SMB サービスで使用される SMB プロトコルのバージョン 1 では、ネットワーク上でのデータ暗号化はサポートされていません。

FTP データサービス

FTP では、FTP クライアントからファイルシステムへのアクセスが許可されます。FTP サービスでは匿名ログインは許可されず、ユーザーは構成されたネームサービスを使って認証を行う必要があります。

FTP では、次のセキュリティー設定がサポートされます。これらの設定は、FTP プロトコルアクセスが有効なすべてのファイルシステムで共有されます。

- **SSL/TLS を有効化** - SSL/TLS 暗号化 FTP 接続を許可し、FTP トランザクションの暗号化を保証します。これは、デフォルトでは無効になっています。FTP サーバーは、自己署名付きセキュリティー証明書または顧客提供証明書を使用します。
- **SSL/TLS バージョンおよび暗号化** - FTP 接続のための SSL/TLS プロトコルバージョンおよび暗号化。デフォルトは TLSv1.1、TLSv1.2、およびそれに関連付けられた暗号化です。セキュリティー上の懸念があるため TLSv1.0 はデフォルトでは有効になっていませんが、下位互換性のために有効にできます。BUI では、使用可能な暗号化のリストは、選択されたバージョンによって異なります。選択された一部の SSL/TLS プロトコルバージョンまたは暗号化、あるいはその両方がサポートされなくなった場合は、ソフトウェアのアップグレード後に削除されます。サービスが使用不可にならないようにするために、特に必要になるか、または Oracle サポートから指示されないかぎり、デフォルト設定を維持してください。
- **root ログインを許可** - root ユーザーの FTP ログインを許可します。これはデフォルトでオフになっています。FTP 認証では平文が使用され、ネットワークスニッフィング攻撃のセキュリティーリスクが発生するためです。
- **許容可能なログイン試行の最大数** - ログイン試行の失敗回数。その回数を超えると、FTP 接続が切断されるため、ユーザーは再接続して再度試す必要があります。デフォルトは 3 です。
- **ロギングレベル** - ログの詳細レベル。

FTP では、次のログがサポートされます。

- **proftpd** - FTP イベント (成功および失敗したログイン試行を含む)
- **proftpd_xfer** - ファイル転送ログ
- **proftpd_tls** - SSL/TLS 暗号化に関連する FTP イベント

HTTP データサービス

HTTP では、HTTP プロトコル、HTTPS プロトコル、および HTTP 拡張の Web based Distributed Authoring and Versioning (WebDAV) を使用してファイルシステムにアクセスできます。このサービスにより、クライアントは Web ブラウザを介してシェアファイルシステムにアクセスすることも、ローカルファイルシステムとして (クライアントソフトウェアでサポートされている場合) シェアファイルシステムにアクセスすることもできます。

HTTPS サーバーは、自己署名付きセキュリティー証明書または顧客提供証明書を使用します。顧客提供証明書を取得するには、証明書署名リクエスト (CSR) を生成し、認証局 (CA) に送信して署名を求める必要があります。署名付き証明書が CA から返されると、アプライアンス上にインストールできます。証明書がルート以外の CA によって署名された場合、次のレベルまたは上位レベルの CA からも証明書を取得する必要があります。証明書管理の詳細は、『*Oracle ZFS Storage Appliance* 管理ガイド』を参照してください。

次のプロパティーを使用できます。

- **クライアントログインが必要** - シェアアクセスが許可されるためにはクライアントの認証が必要です。クライアントで作成されるファイルにはその所有権が割り当てられます。これを設定しない場合、作成されるファイルは HTTP サービスがユーザー「nobody」を使って所有します。
- **プロトコル** - サポートするアクセス方法 (HTTP、HTTPS、または両方) を選択します。
- **HTTP ポート (受信接続用)** - HTTP ポート、デフォルトはポート 80 です。
- **HTTPS ポート (セキュアな受信接続用)** - HTTPS ポート、デフォルトポートは 443 です。
- **SSL/TLS バージョンおよび暗号化** - HTTP 接続のための SSL/TLS プロトコルバージョンおよび暗号化。デフォルトは TLSv1.1、TLSv1.2、およびそれに関連付けられた暗号化です。セキュリティー上の懸念があるため TLSv1.0 はデフォルトでは有効になっていませんが、下位互換性のために有効にできます。BUI では、使用可能な暗号化のリストは、選択されたバージョンによって異なります。選択された一部の SSL/TLS プロトコルバージョンまたは暗号化、あるいはその両方がサポートされなくなった場合は、ソフトウェアのアップグレード後に削除されます。サービスが使用不可にならないようにするために、特に必要になるか、または Oracle サポートから指示されないかぎり、デフォルト設定を維持してください。

「クライアントログインが必要」が有効になっている場合、Oracle ZFS Storage Appliance はローカルユーザー、NIS ユーザー、または LDAP ユーザーに有効な認証資格を提供しないクライアントへのアクセスを拒否します。Active Directory 認証はサポートされていません。基本的な HTTP 認証だけがサポートされています。HTTPS を使用していなければ、ユーザー名とパスワードは暗号化されていない状態で送信されます。その方法はすべての環境にとって適切ではない可能性があります。「クライア

ントログインが必要」が無効になっている場合、アプライアンスは資格を認証しようとしません。

認証の有無にかかわらず、作成されたファイルやディレクトリでアクセス権は非表示になりません。新たに作成されたファイルは、全員が読み取りおよび書き込み権限を持っています。新たに作成されたディレクトリは、全員が読み取り、書き込み、および実行権限を持っています。

NDMP データサービス

NDMP (Network Data Management Protocol) を使用すると、Oracle ZFS Storage Appliance はデータ管理アプリケーション (DMA) と呼ばれるリモート NDMP クライアントで制御される NDMP ベースのバックアップおよび復元操作に参加できます。NDMP を使用すると、アプライアンスユーザーデータ (たとえば、アプライアンスで管理者が作成したシェアに格納されているデータ) を、テープドライブなどのローカル接続されたデバイスとリモートシステムの両方にバックアップおよび復元できます。ローカル接続されたデバイスは、DMA を使用してバックアップおよび復元することもできます。

リモートレプリケーションデータサービス

Oracle ZFS Storage Appliance リモートレプリケーションを使用すると、プロジェクトおよびシェアのレプリケーションが容易になります。このサービスを使用すると、特定のアプライアンスにデータをレプリケートしたアプライアンスを表示したり、特定のアプライアンスがレプリケーション先として使用できるアプライアンスを制御したりできます。

このサービスを有効にすると、アプライアンスはほかのアプライアンスからレプリケーション更新を受信し、その構成されたアクションに従ってローカルのプロジェクトおよびシェアに対してレプリケーション更新を送信します。このサービスを無効にすると、受信されるレプリケーション更新が失敗し、ローカルのプロジェクトおよびシェアはレプリケートされません。

アプライアンスのリモートレプリケーションターゲットを構成するには、リモートアプライアンスの root パスワードが必要です。これらのターゲットを使用して、アプライアンスによる通信を可能にするレプリケーションピア接続を設定します。

ターゲットの作成時に、root パスワードを使ってリクエストの信頼性を確認したり、以降の通信でアプライアンスの識別に使用するセキュリティー鍵の生成や交換を実行したりします。

生成された鍵は、アプライアンス構成の一部として永続的に保存されます。root パスワードが永続的に保存されたり、暗号化せずに転送されたりすることはありません。

この最初の ID のやり取りを含むすべてのアプライアンス通信は、SSL で保護されています。

Oracle ZFS Storage Appliance のオフラインレプリケーション機能により、帯域幅に制限のあるネットワーク上で大量のデータセットをレプリケートするときに時間、リソース、および潜在的なデータエラーが減少します。オフラインレプリケーションは、レプリケーションストリームを NFS サーバー上のファイルにエクスポートします。このファイルはリモートターゲットサイトに物理的に移動したり、オプションで出荷用に外部媒体へコピーしたりできます。ターゲットサイトでは、管理者がレプリケーションストリームを含むファイルをターゲットアプライアンスにインポートします。

エクスポートされたレプリケーションストリームへのアクセスを制限するには、ソースおよびターゲットアプライアンスの IP アドレスのみに NFS シェアを公開します。データを暗号化するには、NFS サーバー上の NFS シェアに対するディスク上の暗号化を有効にします。詳細は、NFS サーバーのドキュメントを参照してください。エクスポートされたレプリケーションストリームがアプライアンスによって暗号化されることはありません。

データ暗号化の操作

注記 - 暗号化は特定のモデルでライセンス付与された機能です。詳細は、「オラクル社のソフトウェアライセンス契約書 (「SLA」) およびハードウェアシステムと組み込みのソフトウェアオプションの権利書」およびソフトウェアリリースのライセンス情報ユーザーマニュアルを参照してください。

Oracle ZFS Storage Appliance は、個々のシェア (ファイルシステムおよび LUN) やプロジェクトの内部で作成されたシェアに対する透過的なデータ暗号化を提供します。ソフトウェアリリース OS8.8.0 以降では、ストレージプールの作成時に、すべてのプロジェクトおよび受信レプリケーションストリームで暗号化を要求するようにプールを設定できます。プロジェクトの暗号化を有効にするようにプールが設定されている場合、シェアはデフォルトでプールの暗号化設定を継承します。アプライアンスの初期設定時や出荷時リセット後の再構成時には、キーストアが構成されていないので、プールの暗号化プロパティーは設定できません。

暗号化鍵の管理

アプライアンスには、組み込みのローカルキーストアと Oracle Key Manager (OKM) システムに接続する機能が含まれています。各暗号化プロジェクトまたはシェアでは、ローカルキーストアまたは OKM キーストアからのラッピング鍵が必要とされます。データ暗号化鍵はストレージアプライアンスによって管理され、ローカルまたは OKM キーストアからのラッピング鍵によって暗号化された状態で永続的に保存されます。

包括的な鍵管理システム (KMS) である OKM は、企業の間で急速にニーズが高まっているストレージベースのデータ暗号化に対応するものです。この機能はオープンな標準に準拠するように設計されており、広範囲に分散した異機種混在ストレージインフラストラクチャーにおける暗号鍵を集中管理するためのキャパシティー、スケーラビリティー、相互運用性を提供します。

OKM はストレージ鍵管理における特有の課題を解決します。

- **長期間の鍵保持** – OKM ではアーカイブデータをいつでも使用できるようになります。データのライフサイクルが終了するまで OKM が暗号化鍵を安全に保持します。
- **相互運用性** – OKM は、単一のストレージ鍵管理システム下で、メインフレームやオープンシステムに接続されたさまざまなストレージデバイスをサポートするための相互運用性を提供します。
- **高可用性** – アプライアンスが同じ場所にある場合でも世界中に分散している場合でも、アクティブな N ノードクラスタリング、動的な負荷分散、および自動化されたフェイルオーバーを使用する高可用性を提供します。
- **大容量** – 大量のストレージデバイスと、さらに多くのストレージ鍵を管理します。クラスタ化されたアプライアンス 1 つで、数千ものストレージデバイスと数百万ものストレージ鍵を対象にした鍵管理サービスを提供できます。
- **柔軟な鍵構成** - OKM クラスタごとに、鍵を自動で生成したり、ローカルキーストアまたは OKM キーストアに対して個別に作成したりできます。セキュリティー管理者は、キーストアと組み合わせたときに、特定のラッピング鍵をプロジェクトまたはシェアと関連付ける鍵名を提供します。

鍵の管理

非アクティブの状態の OKM 鍵を使用するシェアおよびプロジェクトはアクセス可能なままになります。OKM 鍵を使用されないようにするには、OKM 管理者はこの鍵を明示的に削除する必要があります。

暗号化されたシェアおよびプロジェクトを確実にアクセス可能にするには、アプライアンス構成およびローカルキーストアの鍵の値をバックアップします。鍵が使用不可能になった場合、その鍵を使用するシェアまたはプロジェクトはアクセスできなくなります。プロジェクトの鍵が使用できない場合、新しいシェアをそのプロジクトに作成できなくなります。

鍵は次のような場合に使用不可能になります。

- 鍵の削除
- 暗号化をサポートしていないリリースへのロールバック
- 鍵が構成されていないリリースへのロールバック
- 出荷時リセット
- OKM サーバーを使用できない

暗号化鍵のライフサイクル

暗号化鍵のライフサイクルは、データサービスをオフラインにせずに任意の時点で鍵を変更できるため柔軟性が高くなっています。

キーストアから鍵を削除すると、その鍵を使用しているすべてのシェアがアンマウントされるため、それらのデータにアクセスできなくなります。OKM キーストア内の鍵のバックアップは、OKM バックアップサービスを使用して実行する必要があります。ローカルキーストア内の鍵はシステム構成バックアップの一環としてバックアップされます。ローカルキーストアの場合は、鍵を値で指定して作成し外部システムに委託することもできるので、鍵ごとのバックアップまたは復元機能も実現できます。

シャドウ移行データサービス

シャドウ移行は、外部または内部ソースからのデータの自動移行を可能にするとともに、バックグラウンドの自動移行を制御します。このサービスが有効か無効かに関係なく、データは帯域内リクエストに合わせて同期的に移行されます。このサービスの主な目的は、バックグラウンド移行専用のスレッドの数を調整できるようにすることです。

NFS ソース上の NFS マウントは、Oracle ZFS Storage Appliance ユーザーの管理下にありません。シャドウ移行マウントはセキュアになりません。そのため、サーバーで Kerberos または類似のリクエストを予期している場合、ソースマウントは拒否されます。

SFTP データサービス

SSH ファイル転送プロトコル (SFTP) では、SFTP クライアントからファイルシステムにアクセスできます。匿名ログインは許可されないため、ユーザーは構成済みのネームサービスを使用して認証を行う必要があります。

SFTP 鍵の作成時に、有効なユーザー割り当てをユーザープロパティーに含める必要があります。SFTP 鍵はユーザー別にグループ化され、SFTP でユーザー名を使用して認証されます。

注記 - セキュリティーを確保するため、ユーザープロパティーを含まない既存の SFTP 鍵は、認証されるとしても再作成してください。

SFTP では、次のセキュリティー設定がサポートされます。これらの設定は、SFTP プロトコルアクセスが有効なすべてのファイルシステムで共有されます。

- **暗号化** - SFTP 接続のための暗号化。
- **MAC** - SFTP 接続のためのメッセージ認証コード (MAC)。

TFTP データサービス

簡易ファイル転送プロトコル (TFTP) は、ファイル転送のための簡易プロトコルです。軽量で簡単に実装できるように設計されていますが、FTP のセキュリティー機能の大部分は省略されています。TFTP は、リモートサーバーとの間でファイルのみを読み書きします。ディレクトリを表示することはできず、現時点ではユーザー認証もありません。

ストレージエリアネットワーク

ストレージエリアネットワーク (SAN) では、ターゲットグループとイニシエータグループによって、論理ユニット番号 (LUN) を使って関連付けることができるターゲットのセットとイニシエータのセットを定義します。ターゲットグループに関連付けられた LUN は、それらのグループのターゲットからのみアクセスできます。イニシエータグループに関連付けられた LUN は、それらのグループのイニシエータからのみアクセスできます。イニシエータグループおよびターゲットグループを LUN に適用するのは、LUN の作成時です。少なくとも 1 つのターゲットグループと 1 つのイニシエータグループを定義しないかぎり、LUN の作成は成功しません。

iSCSI/iSER イニシエータアクセスでのみ選択可能なチャレンジハンドシェイク認証プロトコル (CHAP) の認証を除き、実行される認証はありません。

注記 - デフォルトのイニシエータグループを使用すると、不要な LUN イニシエータや競合する LUN イニシエータが発生する可能性があります。

ディレクトリサービス

このセクションでは、アプライアンス上で構成できるディレクトリサービスと、それらのセキュリティー上の問題について説明します。

ネットワーク情報サービス

ネットワーク情報サービス (NIS) は、ディレクトリの集中管理用のネームサービスです。Oracle ZFS Storage Appliance は、ユーザーおよびグループの NIS クライアントとして機能します。これにより、NIS ユーザーは FTP や HTTP/WebDAV にログインできるようになります。アプライアンス管理用の権限を NIS ユーザーに付与することもできます。アプライアンスでは NIS 情報に独自の権限設定を付加します。

Lightweight Directory Access Protocol

Oracle ZFS Storage Appliance は、Lightweight Directory Access Protocol (LDAP) を使用して管理ユーザーと一部のデータサービスユーザー (FTP、HTTP) の両方を認証します。アプライアンスでは、LDAP over SSL セキュリティーがサポートされています。LDAP は、ユーザーやグループに関する情報の取得に使用されるほかに、次の方法で使用されます。

- ユーザーやグループの名前の受け入れや表示用のユーザーインタフェースを提供する。
- 名前を使用する NFSv4 などのデータプロトコルのために、名前とユーザーおよびグループとのマッピングを行います。
- アクセス制御で使用するグループメンバーシップを定義します。
- オプションで、管理およびデータアクセス認証で使用される認証データを伝送します。

LDAP 接続は、認証メカニズムとして使用できます。たとえば、ユーザーが Oracle ZFS Storage Appliance に対して認証を試みる場合、アプライアンスは、認証を検証するためのメカニズムとして、そのユーザーとして LDAP サーバーに認証を試みることができます。

LDAP 接続のセキュリティーについては、さまざまな制御が存在します。

- アプライアンスからサーバーへの認証:
  - アプライアンスは匿名である
  - アプライアンスは、認証にユーザーの Kerberos 資格を使用する
  - アプライアンスは、認証に指定された「プロキシ」ユーザーおよびパスワードを使用する
- サーバーからアプライアンスへの認証 (適正なサーバーの接続が保証される):
  - セキュアでない
  - サーバーは Kerberos を使用して認証される
  - サーバーは TLS 証明書を使用して認証される

Kerberos または TLS を使用する場合、LDAP 接続経由で送信されるデータは暗号化されますが、それ以外の場合は暗号化されません。TLS を使用する場合、構成時の最初の接続はセキュアではありません。サーバーの証明書は、その時点で収集されて、あとで本番接続の認証に使用されます。

認証局証明書をインポートして、複数の LDAP サーバーの認証に使用することはできません。特定の LDAP サーバーの証明書を手動でインポートすることもできません。

raw TLS (LDAPS) だけがサポートされています。セキュアでない LDAP 接続上で開始され、その後セキュアな接続に切り替えられる STARTTLS 接続は、サポートされていません。クライアント証明書の必要な LDAP サーバーは、サポートされていません。

アイデンティティーマッピング

クライアントは、SMB または NFS を使用して Oracle ZFS Storage Appliance 上のファイルリソースにアクセスでき、それぞれ一意のユーザー識別子を持ちます。SMB/Windows ユーザーはセキュリティー記述子 (SID) を保持し、UNIX/Linux ユーザーはユーザー ID (UID) を保持します。ユーザーは、グループ SID (Windows ユーザーの場合) またはグループ ID (GID) (UNIX/Linux ユーザーの場合) で識別されるグループのメンバーになることもできます。

両方のプロトコルを使用してファイルリソースにアクセスする環境で望ましいのは、ID の等価性を確立することであり、その場合には、たとえば UNIX ユーザーは Active Directory ユーザーと同等になります。これは、アプライアンスでファイルリソースへのアクセス権を特定する上で重要です。

Active Directory、LDAP、NIS などのディレクトリサービスを含む、異なるタイプのアイデンティティーマッピングが存在します。使用するディレクトリサービスのセキュリティー面でのベストプラクティスに、注意深く従ってください。

UNIX 用 ID 管理

Microsoft では、UNIX 用 ID 管理 (IDMU) と呼ばれる機能を提供しています。このソフトウェアは Windows Server 2003 で使用でき、Windows Server 2003 R2 以降にバンドルされています。これは、かつてアンバンドル形式の Services For Unix と呼ばれていた機能の一部です。

IDMU の主な使用目的は、Windows を NIS/NFS サーバーとしてサポートすることです。IDMU を使用すると、管理者は多数の UNIX 関連パラメータ (UID、GID、ログインシェル、ホームディレクトリ、およびグループ関連の類似パラメータ) を指定できます。これらのパラメータは、AD で RFC 2307 に類似した (ただし同じではない) スキーマを介して使用できます。また、NIS サービスでも使用できます。

IDMU マッピングモードを使用すると、アイデンティティーマッピングサービスはこれらの UNIX 属性を使用して Windows ID と UNIX ID のマッピングを確立します。この方法はディレクトリベースのマッピングに非常によく似ていますが、アイデンティティーマッピングサービスはカスタムスキーマを許可するのではなく、IDMU ソフトウェアによって作成されたプロパティースキーマをクエリー検索する点が異なります。この方法を使用すると、ほかのディレクトリベースのマッピングは使用できなくなります。

ディレクトリベースのマッピング

ディレクトリベースのマッピングでは、ID が相手方プラットフォームの同等の ID にどのようにマップされるかについての情報を LDAP または Active Directory オブジェク

トの注釈として付ける必要があります。オブジェクトに関連付けられるこれらの追加属性を構成する必要があります。

名前ベースのマッピング

名前ベースのマッピングには、ID を名前でマップするためのさまざまな規則を作成することも含まれます。これらの規則は、Windows ID と UNIX ID との等価性を確立します。

一時的なマッピング

名前ベースのマッピング規則が特定のユーザーに適用されない場合、拒否マッピングによってブロックされないかぎり、そのユーザーには一時的なマッピングを通じて一時的な資格が付与されます。一時的な UNIX 名を持つ Windows ユーザーがシステム上にファイルを作成すると、SMB を使用してそのファイルにアクセスする Windows クライアントは、ファイルがその Windows ID によって所有されていると認識します。しかし、NFS クライアントは「nobody」によって所有されていると認識します。

システム設定

以降のセクションでは、利用可能なシステムセキュリティー設定について説明します。

フォンホーム

フォンホームサービスは、Oracle ZFS Storage Appliance 登録とフォンホームリモートサポートサービスの管理に使用されます。このメッセージではユーザーデータやメタデータは送信されません。

登録によって、使用している Oracle ZFS Storage Appliance が Oracle のインベントリポータルと結び付けられ、Oracle 機器を管理できるようになります。登録はフォンホームサービスを使用するための前提条件です。

フォンホームサービスは、Oracle サポートと通信して、次の機能を提供します。

- **障害報告** - システムは自動サービス応答に関するアクティブな問題を Oracle に報告します。障害の性質によっては、サポートケースが開かれることがあります。
- **ハートビート** - システムが起動し動作中であることを示すために日単位のハートビートメッセージが Oracle に送信されます。Oracle サポートでは、アクティブに

なっているシステムの 1 つが長期間にわたってハートビートの送信に失敗すると、アカウントの技術担当者に通知することがあります。

- **システム構成** - 現在のソフトウェアとハードウェアのバージョンと構成、およびストレージ構成を説明する定期メッセージが Oracle に送信されます。

サービスタグ

サービスタグを使用すると、次のようなデータを Oracle ZFS Storage Appliance に問い合わせることができるため、製品のインベントリ処理やサポートが容易になります。

- システムのシリアル番号
- システムタイプ
- ソフトウェアのバージョン番号

サービスタグは Oracle サポートに登録できます。これにより、Oracle 機器を簡単に追跡したり、保守呼び出しを円滑に行なったりすることができます。サービスタグはデフォルトで有効になっています。

Kerberos サービス

Kerberos サービスは、アプライアンスの管理ログインのための認証機能を提供するほか、Kerberos 環境と一緒に使用した場合は NFS、HTTP、FTP、SFTP、SSH などのサービスへのアクセスを提供します。アプライアンスユーザーは、これらのサービスで Kerberos 認証を使うには、同じ名前で Kerberos 主体を持つ必要があります。15 ページの「NFS 認証および暗号化オプション」に記載されているように、Kerberos は NFS プロトコルを使用する個々のシェアのセキュリティーを設定するためにも使用できます。

Kerberos と Active Directory は個別のレルムと鍵を持つため、両方を同時に有効にできます。どちらもアクティブな場合、Kerberos のレルムがデフォルトです。Active Directory のみがアクティブな場合、そのレルムがデフォルトです。

Simple Mail Transport Protocol

Simple Mail Transport Protocol (SMTP) は、通常、構成されたアラートに対応して、Oracle ZFS Storage Appliance で生成されたすべてのメールを送信します。SMTP では外部メールを受け付けません。アプライアンス自体によって自動的に生成されたメールのみを送信します。

デフォルトでは、SMTP サービスは DNS (MX レコード) を使用してメールの送信先を判断します。DNS がアプライアンスのドメイン用に構成されていない場合、または送

信メールの宛先ドメインに DNS MX レコードが正しく構成されていない場合は、送信メールサーバーを介してすべてのメールを転送するようにアプライアンスを構成できます。

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) は、Oracle ZFS Storage Appliance 上の 2 つの機能を提供します。つまり、SNMP によってアプライアンスのステータス情報を提供する機能と、SNMP トラップを送信するようにアラートを構成する機能です。このサービスが有効になっている場合は、SNMP バージョン 1、v2c、および v3 を使用できます。アプライアンスは、最大 128 個の物理および論理ネットワークインタフェースをサポートします。

Syslog メッセージ

syslog メッセージは、Oracle ZFS Storage Appliance から 1 つ以上のリモートシステムに転送される小さなイベントメッセージです。syslog は、2 つのアプライアンス機能を提供します。

- syslog メッセージを 1 つ以上のリモートシステムに送信するようにアラートを構成できます。
- アプライアンス上の syslog 対応のサービスでは、その syslog メッセージがリモートシステムに転送されます。

syslog は、RFC 3164 で説明されている classic 出力形式を使用するように構成することも、RFC 5424 で説明されている、より新しいバージョン管理された出力形式を使用するように構成することもできます。syslog メッセージは UDP データグラムで転送されます。そのため、ネットワークによってドロップされやすかったり、送信側のシステムのメモリーが少ない場合やネットワークが輻輳している場合にまったく送信されないことがあったりします。従って、管理者はネットワーク内に複雑な不具合のあるシナリオでは一部のメッセージが欠けていたり、ドロップされていることを想定するようにしてください。

このメッセージには、次の要素が含まれます。

- このメッセージを発行したシステムコンポーネントの種類を記述する facility
- このメッセージに関連付けられた状態の重要度を記述する severity
- 関連付けられたイベントの時間を UTC で記述する timestamp
- アプライアンスの正規名を記述する hostname
- このメッセージを発行したシステムコンポーネントの名前を記述する tag
- イベントそのものを記述する message

システム ID

このサービスでは、システムの名前と場所を構成できます。Oracle ZFS Storage Appliance システムを別のネットワークの場所に移動したり、ほかの目的で使用したりする場合は、システムの名前と場所の変更が必要になることがあります。

ディスクスクラブ

Oracle ZFS Storage Appliance がディスク上の破損データを検出して修正できるように、ディスクスクラブを定期的に実行してください。ディスクスクラブは、アイドル期間中にディスクを読み取って、頻繁にアクセスされないセクター内の修復不可能な読み取りエラーを検出するバックグラウンドプロセスです。この種の潜在的なセクターエラーを適時検出することは、データ損失を減らす上で重要です。

破棄の防止

破棄の防止機能を有効にすると、シェアやプロジェクトを破棄できなくなります。これには、従属クローンを介したシェアの破棄、プロジェクト内のシェアの破棄、およびレプリケーションパッケージの破棄も含まれます。ただし、レプリケーションの更新を介して破棄されるシェアは、このプロパティーに影響されません。レプリケーションのソースになっている Oracle ZFS Storage Appliance システム上のシェアが破棄される場合、このプロパティーが設定されていても、ターゲット上の対応するシェアは破棄されます。

シェアを破棄するには、別の手順としてこのプロパティーをまず明示的にオフにする必要があります。このプロパティーはデフォルトでオフになっています。

セキュリティーログ

このセクションでは、セキュリティー関連のロギング機能について説明します。

監査ログ

監査ログには、BUI および CLI へのログインとログアウトなどのユーザーアクティビティーイベント、および管理アクションが記録されます。次の表に、BUI で表示される監査ログエントリの例を示します。

表 2 監査ログレコード

時間	ユーザー	ホスト	サマリー	セッションの注釈
2018-10-12 05:20:24	root	galaxy	ftp サービスが無効	
2018-10-12 03:17:05	root	galaxy	ユーザーがログイン	
2018-10-11 22:38:56	root	galaxy	ブラウザセッションがタイムアウト	
2018-10-11 21:13:35	root	<console>	ftp サービスが有効	

フォンホームのログ

フォンホームが使用されている場合、このログには Oracle サポートとの通信イベントが表示されます。次の表に、BUI に表示されるフォンホームエントリの例を示します。

表 3 フォンホームのログレコード

時間	説明	結果
2018-10-12 05:24:09	「cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz」ファイルが Oracle サポートにアップロードされました	OK

詳細情報

Oracle ZFS Storage Appliance の詳細な製品情報は、次の場所で検索できます。

https://docs.oracle.com/en/storage/

BUI を使用して Oracle ZFS Storage Appliance を構成している場合は、各画面の右上にある「ヘルプ」リンクをクリックして、その画面のヘルプを表示できます。