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

ORACLE

# Oracle ZFS Storage Appliance セキュリティーの概要

このガイドでは、セキュアなストレージシステムを作成し、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して、Oracle ZFS Storage Appliance (ZFSSA) 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 System 管理ガイドを参照してください。

以降のセクションでは、ZFSSA のセキュリティー機能について説明します。

- **初期インストール** - 管理アクセスの設定方法、root アカウントの確立方法、および ZFSSA の出荷時リセットの影響について説明します。
- **物理的なセキュリティー** - ZFSSA の物理的なセキュリティー環境について説明します。
- **管理モデル** - CLI と BUI、システムパッチモデル、遅延更新、サポートバンドル、および構成バックアップへのアクセス制限について説明します。
- **ZFSSA ユーザー** - ZFSSA を管理可能な管理ロール、および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 (ACL)** - ファイルやディレクトリへのアクセスを許可または拒否可能なメカニズムについて説明します。
- **ストレージエリアネットワーク (SAN)** - 論理ユニット番号 (LUN) と関連するイニシエータグループ、およびイニシエータ認証オプションとデフォルトについて説明します。
- **データサービス** - ZFSSA によりサポートされるデータサービス、および異なるデータサービスで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** - ZFSSA で構成可能なディレクトリサービス、およびそのセキュリティーへの影響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、SMTP、SNMP、Syslog、システム ID、ディスクスクラブ、および破棄の防止といったシステム設定について説明します。
- **リモート管理アクセス** - BUI および CLI 経由でのリモートアクセスについて説明します。
- **ログ** - セキュリティー関連のログ形式について説明します。

# 初期インストール

ZFSSA は、ZFSSA ソフトウェアがプリ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。ZFSSA が出荷時のデフォルトにリセットされると、root パスワードも ZFSSA とサービスプロセッサの両方でデフォルトにリセットされます。

ZFSSA の初期インストール中に、システムの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存在します。システム管理者は、このデフォルトアカウントを使用して ZFSSA に初回アクセスを実行し、そこでシステムの初期インストール手順を実行する必要があります。必須手順の

1 つは新規 ZFSSA 管理パスワードの設定で、これによりデフォルトのサービスプロセッサパスワードも同じ値にリセットされます。

# 物理的なセキュリティー

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。

ZFSSA は、セキュリティ保護のための手段 (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、ZFSSA 管理モデルのセキュリティーについて説明します。

## 制限付きアクセス (CLI および BUI)

ブラウザユーザーインタフェース (BUI) およびコマンドラインインタフェース (CLI) への管理アクセスは、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) などのアイデンティティーサーバーを通じて承認されたユーザーに制限されます。

管理は、SSL (Secure Sockets Layer) コマンドラインログインまたは HTTP セキュア (HTTPS) ブラウザセッション経由で行われます。HTTPS セッションは、初期インストール時に ZFSSA 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。

## システムの更新

システムの更新は、システムソフトウェアのバイナリ全体を交換して適用されます。更新する前に、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、管理者が必要に応じて以前のバージョンにロールバックすることが可能になります。

## 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、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。更新を適用したら、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。

## ZFSSA ユーザー

2 種類の ZFSSA ユーザーが存在します。

- **データサービスユーザー** – NFS、SMB、ファイバチャネル、iSCSI、http、FTP などのサポートされ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** - ZFSSA 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。ロールとは、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 ZFSSA 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 ZFSSA に保存されます。これにより、既存の NIS/LDAP ユーザーはログインして ZFSSA を管理できるようになりますが、デフォルトでは既存の NIS/LDAP ユーザーは ZFSSA にログインすることはできません。ZFSSA へのアクセスを明示的に許可する必要があります。

### 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、ZFSSA 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、この承認で HTTP サービスだけを再起動できます。

# アクセス制御リスト (ACL)

ZFSSA 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。アクセス制御リストは、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。

ZFSSA 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豊富な ACL モデルです。ストレージ ZFSSA 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 ACE (アクセス制御エントリ) で構成されます。各 ACE には、ACE の適用先ユーザーおよび使用される継承フラグレベルといった、ACE が付与または拒否するアクセス権のエントリが含まれます。

## ACL 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、初期設定時に管理者が ACL に設定する複数の継承レベルフラグにより制御されます。

## 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 共有レベル 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、シェアレベルの 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。

# ストレージエリアネットワーク (SAN)

SAN では、ターゲットおよびイニシエータグループは、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および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限り、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ーク認証プロトコル (CHAP) の認証を除き、実行される認証はありません。

**注**: デフォルトイニシエータグループを使用すると、LUN が意図しない、または競合するイニシエータに公開されることがあります。

# データサービス

**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 |
| 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 |
| 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 |
| 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 |
| SRP | SRP プロトコル経由でのブロックアクセス | |
| TFTP | TFTP プロトコル経由でのファイルシステムアクセス | |
| 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 | |

**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: 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 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

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 uid および gid は NFS サーバーにより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

ZFSSA で LUN を構成すると、iSCSI (Internet Small Computer System Interface) ターゲットを介してそのボリュームをエクスポートできます。iSCSI サービスでは、iSCSI イニシエータは 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、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、RADIUS 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、2 番目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

Remote Authentication Dial-In User Service (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。

ZFSSA 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。

- ZFSSA 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、ZFSSA 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)、ZFSSA 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、ZFSSA 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。

## サーバーメッセージブロック (SMB)

SMB プロトコル (Common Internet File System (CIFS) とも呼ばれる) は、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。これは、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。デフォルトでは、このオプションは無効です。
- **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。デフォルトでは、このオプションは無効です。
- **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。デフォルトでは、このオプションは無効です。

### Active Directory (AD) ドメインモードの認証

ドメインモードでは、ユーザーは Active Directory 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 ZFSSA に接続できます。

ユーザーが完全修飾 ZFSSA ホスト名を使用して接続する場合、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 Kerberos 認証を使用するか、そうでなければ 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 ZFSSA 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 ZFSSA に接続する必要があります。詳細は、MSDN の記事 http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx を参照してください。

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、ユーザーは ZFSSA 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で ZFSSA に接続する場合、そのユーザーのユーザー名とパスワードハッシュを使用してユーザーがローカルで認証されます。

ZFSSA がワークグループモードにある場合、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。

次のリストは、各 LM 互換性レベルでの ZFSSA 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、ZFSSA 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

ローカルグループとは、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 (MMC) 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に、MMC を使用してリモートで実行される操作に対していくつかのアクセス制限が設けられています。

次のリストは、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 - シェアのリスト
- Administrators グループのメンバー - 開いているファイルのリストとファイルのクローズ、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。
- Administrators グループのメンバー - 開いているファイルのリストとファイルのクローズ、ユーザーの接続の切断、サービスとイベントログの表示。

## 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、ZFSSA 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、ZFSSA 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、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。

## ファイル転送プロトコル (FTP)

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。
- 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 認証は平文で行われ、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をもたらすからです。
- 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

## ハイパーテキスト転送プロトコル (HTTP)

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。これにより、クライアントは Web ブラウザ経由で、またはクライアントソフトウェアが対応している場合にはローカルファイルシステムとして、共有ファイルシステムにアクセスできます。HTTPS サーバーは、自己署名付きセキュリティー証明書を使用します。

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。

「クライアントログインが必要」を有効にした場合、ZFSSA 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」が無効な場合、ZFSSA は認証を試みません。

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。

## Network Data Management Protocol (NDMP)

NDMP を使用すると、ZFSSA 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、ZFSSA ユーザーデータ (たとえば、ZFSSA 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

ZFSSA 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、この ZFSSA にデータをレプリケートした ZFSSA を表示したり、この ZFSSA がレプリケートできる ZFSSA を構成したりできます。

このサービスを有効にすると、ZFSSA はほかの ZFSSA 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。

ZFSSA 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 ZFSSA 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、ZFSSA 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 ZFSSA 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、ZFSSA 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ることは決してありません。root パスワードが平文で転送されることは決してありません。この最初の ID のやり取りを含むすべての ZFSSA 通信は、SSL で保護されています。

## シャドウ移行

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 ソース上での NFS マウントを、ZFSSA ユーザーが制御することはできません。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。

### SSH File Transfer Protocol (SFTP)

SFTP では、SFTP 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。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:** 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。

### Trivial File Transfer Protocol (TFTP)

TFTP は、ファイル転送用の単純なプロトコルです。TFTP は、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。

## ディレクトリサービス

### ネットワーク情報サービス (NIS)

NIS は、ディレクトリの集中管理用のネームサービスです。ZFSSA はユーザーとグループに対して NIS クライアントとして動作可能であるため、NIS ユーザーは FTP および HTTP/WebDAV にログインできます。ZFSSA 管理用の権限を NIS ユーザーに付与することもできます。ZFSSA では NIS 情報に独自の権限設定を付加します。

### Lightweight Directory Access Protocol (LDAP)

ZFSSA は、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。LDAP over SSL セキュリティーは、ZFSSA で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で、ユーザーおよびグループとの間で名前をマッピングする。
- 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する。
- オプションで、管理およびデータアクセス認証で使用する認証データを伝送する。

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 ZFSSA に対して認証を試みる場合、ZFSSA 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):
  1. セキュアでない
  2. サーバーは Kerberos を使用して認証される
  3. 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 ZFSSA 上のファイルリソースにアクセスでき、それぞれが一意のユーザー識別子を保持します。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、ZFSSA 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 ID 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。

## IDMU

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 RFC2307 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

特定のユーザーに適用される名前ベースのマッピング規則がない場合、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、ZFSSA 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します。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 ZFSSA 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 サポートと通信を行なって、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 ZFSSA に問い合わせることができるため、製品のインベントリ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。

## SMTP

SMTP サービスは、通常、構成した警告に対応して、ZFSSA 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。ZFSSA 自体で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 ZFSSA 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 ZFSSA を構成できます。

## Simple Network Management Protocol (SNMP)

SNMP は、ZFSSA で 2 つの機能を提供します。SNMP が提供可能な ZFSSA ステータス情報、および SNMP トラップを送信するように構成可能なアラートです。SNMP バージョン 1 と 2c の両方を使用できます。

## Syslog

Syslog メッセージは、ZFSSA 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 ZFSSA 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警告を構成できます。
- ZFSSA 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。したがって、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の構成します。ZFSSA 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、これらの変更が必要になることがあります。

### ディスクスクラブ

ZFSSA 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 ZFSSA 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。

## リモート管理アクセス

このセクションでは、ZFSSA リモートアクセスの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 (BUI)

BUI サービスの画面を使用して、リモートアクセスのサービスや設定を表示および変更します。

### Secure Shell (SSH)

SSH を使用すると、ユーザーはコマンドラインインタフェース (CLI) 経由で ZFSSA にログインして、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。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。

# 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

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。次の表では、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 |
|---|---|---|---|---|
| 2009-10-12 05:20:24 | root | galaxy | ftp サービスが無効 | |
| 2009-10-12 03:17:05 | root | galaxy | ユーザーがログイン | |
| 2009-10-11 22:38:56 | root | galaxy | ブラウザセッションがタイムアウト | |
| 2009-10-11 21:13:35 | root | <console> | ftp サービスが有効 | |

## フォンホーム

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。次の表は、BUI で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 |
|---|---|---|
| 2009-10-12 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

各 ZFSSA ブラウザユーザーインタフェース (BUI) ページで、各ページの左上にある「ヘルプ」ボタンをクリックして、コンテキスト固有のオンラインヘルプを検索できます。

Oracle ZFS Storage アプライアンスの詳細な製品情報は、次の場所で検索できます。

www.oracle.com/us/products/servers-storage/storage/nas/overview

# ドキュメントマッピング

下の表を使用して、ZFSSA のサービス、構成、その他の機能ごとの詳細なドキュメントを参照してください。BUI を使用して ZFSSA 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。

**表 4** サービス

| サービス | ドキュメントの場所 |
|---|---|
| Active Directory | サービス:Active_Directory |
| アイデンティティーマッピング | サービス:アイデンティティーマッピング |
| DNS | サービス:DNS |
| 動的ルーティング | サービス:動的ルーティング |
| IPMP | サービス:IPMP |
| NTP | サービス:NTP |
| フォンホーム | サービス:フォンホーム |
| サービスタグ | サービス:サービスタグ |
| SMTP | サービス:SMTP |
| SNMP | サービス:SNMP |
| Syslog | サービス:Syslog |
| システム ID | サービス:システム ID |
| SSH | サービス:SSH |

**表 5** 構成

| 構成 | ドキュメントの場所 |
|---|---|
| SAN | 構成:SAN |
| SAN:FC | 構成:SAN:FC |
| SAN:iSCSI | 構成:SAN:iSCSI |
| SAN:SRP | 構成:SAN:SRP |
| クラスタ | 構成:クラスタ |
| ユーザー | 構成:ユーザー |
| 設定 | 構成:設定 |
| 警告 | 構成:警告 |
| ストレージ | 構成:ストレージ |

**表 6** ストレージ

| ストレージ | ドキュメントの場所 |
|---|---|
| シェア | シェア |
| 概念 | シェア:概念 |

| ストレージ | ドキュメントの場所 |
| --- | --- |
| シャドウ移行 | シェア:シャドウ移行 |
| スペース管理 | シェア:スペース管理 |
| ファイルシステムの名前空間 | シェア:ファイルシステムの名前空間 |
| シェア | シェア:シェア |
| 一般 | シェア:シェア:一般 |
| プロトコル | シェア:シェア:プロトコル |
| アクセス | シェア:シェア:アクセス |
| スナップショット | シェア:シェア:スナップショット |
| プロジェクト | シェア:プロジェクト |
| プロジェクト:一般 | シェア:プロジェクト:一般 |
| プロジェクト:プロトコル | シェア:プロジェクト:プロトコル |
| プロジェクト:レプリケーション | シェア:プロジェクト:レプリケーション |
| スキーマ | シェア:スキーマ |

ORACLE