Sun StorEdge™ 5310 NAS Appliance および Gateway システム 管理マニュアル

Sun Microsystems, Inc.
www.sun.com

Part No. 819-5230-10
2006 年 2 月, Revision A

コメントの送付: http://www.sun.com/hwdocs/feedback

原典: *Sun StorEdge 5310 NAS Appliance and Gateway System Administration Guide*
Part No: 819-3238-11
Revision A

目次

図目次

表目次

はじめに

『Sun StorEdge 5310 NAS Appliance および Gateway システム管理マニュアル』は、Sun StorEdge™ 5310 NAS Appliance、Sun StorEdge™ 5310 Cluster、および Sun StorEdge™ 5310 NAS Gateway システムの管理者およびユーザーを対象としたマニュアルをまとめたものです。このマニュアルでは、Web Administrator ソフトウェアを使用してシステムを設定および監視する方法について説明します。また、『Sun StorEdge 5310 NAS Appliance および Gateway システムご使用の手引き』では説明していないコマンド行インタフェース (CLI) の使用方法およびシステムハードウェアの詳細についても説明します。

お読みになる前に

このマニュアルを読む前に、『Sun StorEdge 5310 NAS Appliance および Gateway システムご使用の手引き』の説明に従って、システムの設置および構成を完了しておいてください。

マニュアルの構成

このマニュアルでは、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムの管理方法および使用方法について説明します。

第 1 章では、Web Administrator ソフトウェアの機能の概要を説明します。

第 2 章では、基本的なネットワークおよびファイルシステムの構成について説明します。

第 3 章では、RAID (Redundant Array of Independent Disks) システムの設定について説明します。

第 4 章では、管理機能について説明します。

第 5 章では、ポートの設定について説明します。

第 6 章では、命名規則について説明します。

第 7 章では、セキュリティーの設定について説明します。

第 8 章では、共有、割り当て、およびエクスポートについて説明します。

第 9 章では、ライセンス追加可能なソフトウェアオプションについて説明します。

第 10 章では、監視機能について説明します。

第 11 章では、保守機能について説明します。

付録 A では、コンソールを使用してシステムタスクを実行する手順について説明します。

付録 B では、表示される可能性のあるエラーメッセージについて説明します。

付録 C では、Compliance Archiving Software API について詳細に説明します。

付録 D では、システムハードウェアについて詳細に説明します。

付録 E では、診断電子メールの送信方法について説明します。

書体と記号について

書体または記号*	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	% **su** Password:
AaBbCc123	コマンド行の可変部分。実際の名前や値と置き換えてください。	rm *filename* と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	% **grep '^#define ** **XV_VERSION_STRING'**

* 使用しているブラウザにより、これらの設定と異なって表示される場合があります。

関連マニュアル

オンラインのマニュアルは、次の URL で参照できます。

`http://www.sun.com/hwdocs/Network_Storage_Solutions/nas`

用途	タイトル	Part No.	形式	場所
設置	『Sun StorEdge 5210 および 5310 NAS Appliance および Gateway システムご使用にあたって』	819-3093-*nn*	PDF	オンライン
設置	『Sun StorEdge 5310 NAS Appliance および Gateway システムご使用の手引き』	819-5225-*nn*	PDF HTML	オンライン オンライン
NAS Appliance の設置 (Gateway 以外)	『Sun StorEdge 5310 NAS の設定』	819-3098-*nn*	印刷物 PDF	出荷用キット オンライン
Gateway	『Sun StorEdge 5310 NAS Gateway システム』ポスター	819-5253-*nn*	印刷物 PDF	出荷用キット オンライン

マニュアル、サポート、およびトレーニング

URL	説明
http://jp.sun.com/documentation/	PDF と HTML マニュアルをダウンロードする、印刷マニュアルを注文する
http://jp.sun.com/support/	テクニカルサポートを受ける、パッチをダウンロードする
http://jp.sun.com/training/	Sun のコースについて情報を入手する

Sun 以外の Web サイト

このマニュアルで紹介する Sun 以外の Web サイトが使用可能かどうかについては、Sun は責任を負いません。このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、広告、製品、またはその他の資料についても、Sun は保証しておらず、法的責任を負いません。また、このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、商品、サービスの使用や、それらへの依存に関連して発生した実際の損害や損失、またはその申し立てについても、Sun は一切の責任を負いません。

コメントをお寄せください

マニュアルの品質改善のため、お客様からのご意見およびご要望をお待ちしております。コメントは下記よりお送りください。

http://www.sun.com/hwdocs/feedback

ご意見をお寄せいただく際には、下記のタイトルと Part No. を記載してください。

『Sun StorEdge 5310 NAS Appliance および Gateway システム管理マニュアル』、Part No. 819-5230-10

第1章

概要

Sun StorEdge 5310 NAS Appliance の Web Administrator は、Sun の革新的な Sun StorEdge 5310 NAS Appliance システムの、セキュリティーの設定およびネットワークの構成と、管理作業の実行を容易にするグラフィカルユーザーインタフェース (GUI) です。

注 – このマニュアルで説明するソフトウェアのほとんどの機能は、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムのすべての構成に適用されます。その場合は「システム」という一般的な用語を使用します。機能がいずれかの構成に限定される場合は、その構成の名前を具体的に示します。

Web Administrator 内のナビゲート

Web Administrator では、GUI の一連のメニューおよびタブ画面、またはパネルを使用してシステムパラメータを構成できます。タブ画面および設定の詳細は、このあとの章で説明します。

GUI の使用法

Web Administrator のメインウィンドウでは、システムのイベントやサービスをナビゲート、設定、および表示することができます。このウィンドウに表示される内容は、使用するハードウェアの構成に応じて異なります。

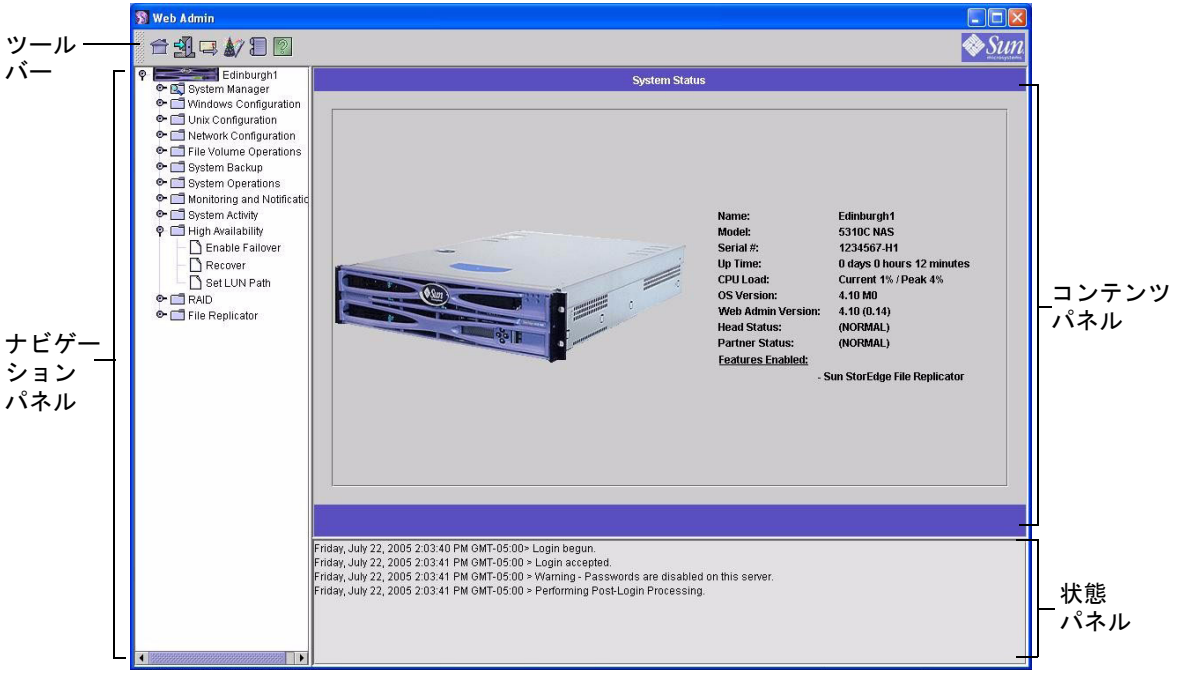


図 1-1　　メインウィンドウ

ツールバー

Web Administrator ウィンドウの上部にあるツールバーを使用すると、ホーム状態画面の表示、ログアウト、診断電子メールの送信、構成ウィザードの実行、システムログの表示、およびヘルプページの表示を行うことができます。

図 1-2　　ツールバー

表 1-1 に、ツールバーのアイコンを示します。

表 1-1　ツールバー上のアイコン

ボタン	名前	動作
	Home	ホームシステム状態画面の表示
	Log out	ログアウト
	Email	診断電子メールの送信
	Wizard	構成ウィザードの実行
	System log	システムログの表示
	Help	ヘルプの表示

ナビゲーションパネル

このパネルを使用すると、Web Administrator 内をナビゲートできます。ナビゲーションパネルからは、構成、設定、および管理に関するすべての機能にアクセスできます。

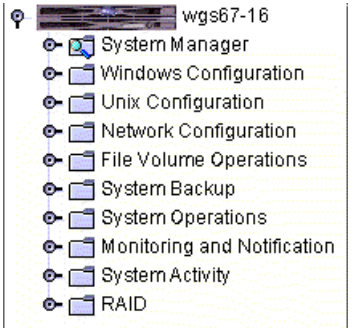
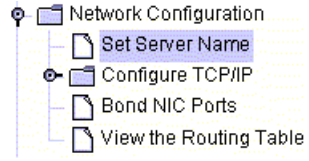


図 1-3　ナビゲーションパネル

フォルダを開くには、フォルダの横の 記号をクリックするか、またはフォルダをダブルクリックします。記号の向きが に変わります。たとえば、Network Configuration をクリックすると、次の図のようになります。



フォルダを閉じるには、 記号をクリックして の向きに戻します。

フォルダの記号

Web Administrator のフォルダはすべて記号で表されます。

表 1-2 に、フォルダの記号を示します。

表 1-2 フォルダの記号

記号	説明
	ファイルボリューム
	規制適合対応のファイルボリューム (赤いタブ付きのフォルダ)
	共有ファイルボリューム
	エクスポートされたファイルボリューム
	共有およびエクスポートされたファイルボリューム
	ミラー化されたファイルボリューム
	規制適合対応のミラー
	セグメント

その他のボタン

Web Administrator の一部の画面には、その他のボタンが表示されます。

表 1-3 に、追加のボタンを示します。

表 1-3　その他のボタン

ボタン	名前	動作
	Add	項目の追加
	Up	選択された項目の上への移動
	Down	選択された項目の下への移動
	Trash	選択された項目の削除
	Edit	選択された項目の編集

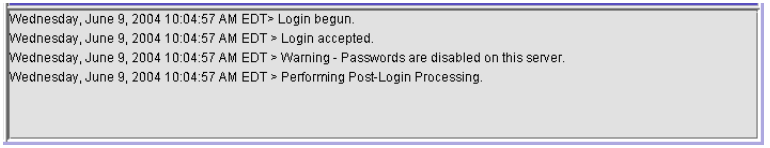
コンテンツパネル

このパネルには、システムの一般的な情報が表示されます。

システムの状態の詳細は、139 ページの「システム状態の表示」を参照してください。

状態パネル

Web Administrator ウィンドウの下部にある状態パネルには、最後のログイン以降に発生したすべてのイベントが表示されます。このパネルでは、変更が保存されたかどうか、またはシステムコマンドが正常に実行されたかどうかを確認できます。エラーおよび警告も、このパネルに表示されます。



注 – 状態パネルには、システムの日付と時刻ではなく、Web Administrator ソフトウェアが動作しているクライアントマシンの日付と時刻が表示されます。

ヘルプの使用法

ヘルプ画面は、Web Administrator の各タブ画面からアクセスできます。ヘルプ画面では、対応する画面内の用語、フィールド、チェックボックス、オプションボタン (ラジオボタン)、およびアクションボタンに関する詳細情報が提供されます。

Web Administrator のトピックに対応するヘルプ画面を表示するには、ツールバー上の「Help」ボタンをクリックしてください。現在表示されているコンテンツパネルに対応するヘルプウィンドウが、Web Administrator 画面の横に表示されます。

構成ウィザードの実行

構成ウィザードは、はじめてログインするときに自動的に実行されます。このウィザードは、表示された指示に従ってユーザーが処理を進めると、システムの初期設定を行えるように設計されています。このウィザードを使用すると、システムとネットワーク間の通信を確立するために必要なすべての手順を完了できます。このウィザードを完了したあとで、ファイルシステムの設定およびユーザーアクセスの構成を行う必要があります。

構成ウィザードで可能な構成タイプ

構成ウィザードでは、いくつかのオプションが提供されます。これらのオプションの一部は、システム自体によって自動的に決定されます。その他のオプションは、実行するネットワーク環境に基づいてユーザーが決定します。このマニュアルでは、可能な構成の一部のみについて説明します。この節では、構成ウィザードの概要と、このウィザードで選択できる構成タイプについて説明します。

また、システムの機能に応じて異なる機能もあります。これらの相違点については、このマニュアル内の対応する箇所で説明します。

ウィザードで選択できる主要な構成には、3 つのタイプがあります。これらの 3 つの構成タイプは、実行するネットワーク環境に基づいて選択する必要があります。3 つの構成タイプを次に示します。

- UNIX only − このタイプを選択すると、システムを UNIX® のみで構成されたネットワークで動作するように構成できます。このタイプの構成では、Windows に関連するすべての機能がスキップされます。
- Windows only − このタイプを選択すると、システムを Windows のみで構成されたネットワークで動作するように構成できます。このタイプの構成では、UNIX に関連するすべての機能がスキップされます。
- Both UNIX and Windows − このタイプを選択すると、システムを Windows および UNIX の機能が混在するネットワーク環境で動作するように構成できます。このタイプの構成では、すべての機能が設定されます。

使用するネットワーク環境に適切な構成タイプを選択します。

▼ ウィザードを起動する

1. **構成ウィザードを実行するには、ツールバー上の「Wizard」ボタンをクリックします。**

   このウィザードの最初のページが表示されます。

2. **「Next」をクリックして次の手順に進みます。**

   その後、ウィザードの指示に従って、次の手順を実行します。詳細は、第 2 章「ネットワークの初期構成」を参照してください。

   1. サーバー名および連絡先情報を設定します
   2. ネットワークアダプタを構成します
   3. デフォルトのゲートウェイを設定します
   4. ドメインおよびワークグループを構成し (Windows 環境および混在環境の場合)、ADS を使用可能にして構成します (Windows 環境および混在環境の場合)
   5. WINS を構成します (Windows 環境および混在環境の場合)
   6. DNS を設定します

   注 – DHCP を使用してシステムを起動した場合は、DNS サーバーのアドレスが正しいことを確認してください。アドレスが正しくない場合は、再起動およびフェイルオーバーでの遅延が発生しないように、「Configure DNS」チェックボックスの選択を解除してください。

   ---

   7. ネットワーク情報サービス (NIS) を設定します (UNIX 環境および混在環境の場合)
   8. ネットワーク情報サービスプラス (NIS+) を設定します (UNIX 環境および混在環境の場合)
   9. ネームサービスを構成します (UNIX 環境および混在環境の場合)
   10. 電子メール通知を設定します
   11. 遠隔ロギングおよびローカルロギングを設定します
   12. 言語を割り当てます

3. **設定を確認します**

   ウィザードによって設定が保存されます。設定が変更できなかった場合はユーザーに通知されます。

構成ウィザードを実行しない場合は、第 2 章「ネットワークの初期構成」を参照してください。第 2 章では、ナビゲーションパネルを使用して同じ順序で同じ機能を設定する方法について説明します。

次に実行する作業

この時点で、システムが起動し動作するようになりました。また、Web Administrator の基本的な操作方法について説明しました。次に、ファイルシステムを設定し、ユーザーアクセスを構成する必要があります。

ファイルシステムの設定では、必要に応じて LUN、パーティション、ファイルボリューム、およびセグメントを設定します。これらの概念については、35 ページの「ファイルシステムの概念」を参照してください。

ファイルシステムの構成が完了したら、ユーザーアクセス権限およびその他のシステム管理機能を設定する必要があります。基本的な管理機能については、第 4 章「システムの管理」で説明します。機能の説明、動作方法、適用する状況とその理由、設定に関する特別なルールなどの特定の項目については、索引を参照してください。

第2章

ネットワークの初期構成

この章では、使用しているシステムでネットワーク通信を構成する方法について説明します。ネットワーク通信およびサービスの構成後、ファイルシステム、ユーザーアクセス権、その他の機能、および購入したオプションを構成する必要があります。

この章では、構成ウィザードと同じ順序で説明します。ただし、ここで説明されていない機能の設定が必要になる場合もあります。この章で説明されていない特定の機能を設定する場合は、索引を参照して詳細を確認してください。

この章の内容は、次のとおりです。

サーバー名の設定

ネットワーク上でサーバーを識別するために使用される、サーバー名を設定する必要があります。

▼ サーバー名を設定する

1. **ナビゲーションパネルで、「Network Configuration」>「Set Server Name」を選択します。**
2. **「Server Name」ボックスにサーバー名を入力します。**

   この名前によって、システム、または高可用性 (HA) のためのサーバー 2 台による構成ではそのサーバー装置が、ネットワーク上で識別されます。サーバー名には、英数字 (a ～ z、A ～ Z、0 ～ 9)、「-」(ダッシュ)、「_」(下線)、および「.」(ピリオド) を指定できます。

   注 – サーバー名には、数字または記号ではなく、英字 (a ～ z または A ～ Z) から始まる文字列を指定する必要があります。たとえば、「Astro2」や「Saturn_05」は適切なサーバー名ですが、「5Saturn」や「_Astro2」は使用できません。

   ---

3. **企業名や、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムの管理者の連絡先情報など、企業の連絡先情報を入力します。**

   システムは、すべての診断電子メールメッセージにこの情報を含めて送信します。診断電子メールメッセージの詳細は、付録 E を参照してください。

4. **「Apply」をクリックして設定を保存します。**

LUN パスの設定

論理ユニット番号 (LUN) パスは、LUN のファイルボリュームにアクセスするサーバーとコントローラ、およびそのアクセス方法を指定します。すべてのファイルボリュームには、一次パスと代替パスの 2 つの LUN パスがあります。一方のパスに障害が発生すると、システムは自動的にもう一方の使用可能な LUN パスを使用して目的のファイルボリュームにアクセスします。LUN パスの数とそれらの実装は、システムのモデルおよび構成によって異なります。Sun StorEdge 5310 Cluster システム

では、一次パスおよび代替パスの両方に障害が発生すると、サーバー (本体) が本体のフェイルオーバー (18 ページの「本体のフェイルオーバーの使用可能への切り替え」を参照) を実行します。

LUN パスは「Set LUN Path」パネルで参照および編集できます (16 ページの「LUN パスの設定」を参照)。

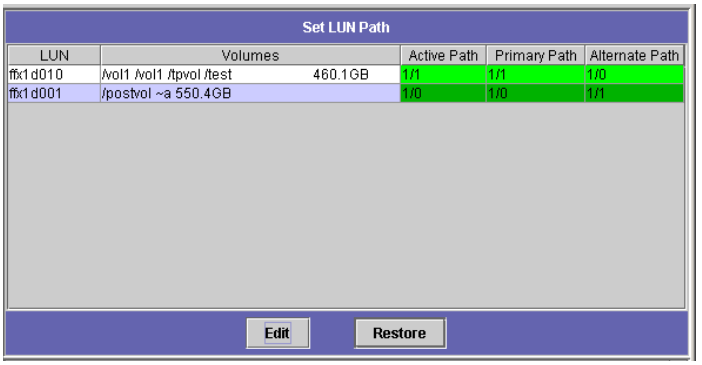


図 2-1　「Set LUN Path」パネルに表示された LUN パス

次の表に、各列の説明を示します。

表 2-1　「Set LUN Path」パネルの列

列	内容
LUN	システムで使用可能な LUN。
Volumes	ファイルボリューム名。LUN には複数のファイルボリュームが存在する場合もあります。
Active Path	現在アクティブな LUN パス。「1/1」は、コントローラ 1 が現在動作中であることを意味します。これ以外のパスについては、次のように判断してください。 最初の番号は、1 から始まる HBA の番号を示します。 2 つめの番号は、コントローラの SCSI (ターゲット) を示します。 たとえば、1/1 は HBA 1 と SCSI コントローラターゲット 1 を示します。
Primary Path	システムが起動時に選択する、第一 LUN パス。また、このパスは、LUN パスの復元先のパスにもなります。一次パスが指定されていない場合、システムは最初に使用可能なパスを使用します。
Alternate Path	一次パスに障害が発生した場合に使用されるパス。

サーバー 1 台構成のシステムの LUN パス

次の図に、サーバー 1 台構成のシステムの標準的なハードウェア構成を示します。

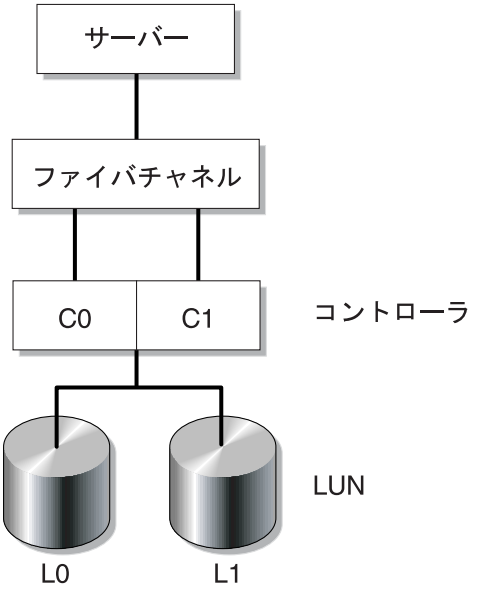


図 2-2　　サーバー 1 台によるシステム構成

LUN0 のファイルボリュームへの一次 LUN パスは C0-L0 で、代替パスは C1-L0 です。LUN1 のファイルボリュームへの一次 LUN パスは C1-L1 で、代替パスは C0-L1 です。この図に示すように、システムは次の LUN パスを持つことになります。

表 2-2　　サーバー 1 台構成のシステムの LUN パス

パス	LUN0	LUN1
一次	C0-L0	C1-L1
代替	C1-L0	C0-L1

各 LUN には、コントローラ 0 (C0) またはコントローラ 1 (C1) のいずれかを介してアクセスできます。

サーバー 2 台構成のシステムの LUN パス

次の図に、Sun StorEdge 5310 Cluster システムの標準的なハードウェア構成を示します。

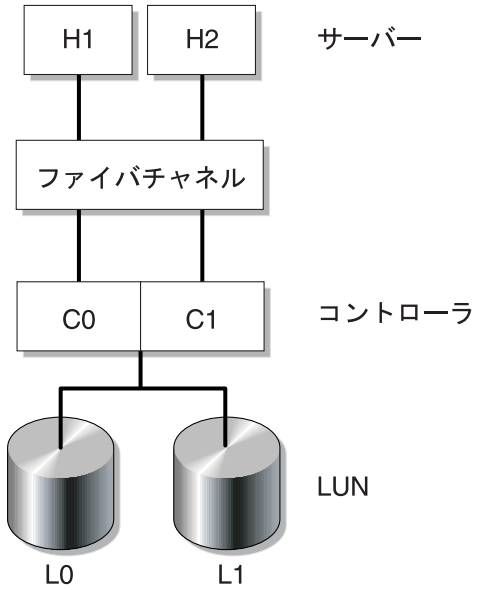


図 2-3　サーバー 2 台によるシステム構成

本体 1 の一次 LUN パスは C0-L0 で、代替パスは C0-L1 です。本体 2 の一次 LUN パスは C1-L0 で、代替パスは C1-L1 です。この図に示すように、システムは次の LUN パスを持つことになります。

表 2-3　サーバー 2 台構成のシステムの LUN パス

本体 1	LUN	LUN0	LUN1
	パス	C0-L0	C0-L1
本体 2	LUN	LUN0	LUN1
	パス	C1-L0	C1-L1

通常、ファイルボリュームへのアクセスは、そのファイルボリュームが属する LUN に指定された一次 LUN パスを介して行われます。クラスタ構成では、一次パスおよび代替パスに障害が発生すると、本体がフェイルオーバーを実行します (18 ページの「本体のフェイルオーバーの使用可能への切り替え」を参照)。

LUN パスの設定

LUN パスを設定して、現在アクティブな LUN パスを指定します。現在アクティブな LUN パスは、一次パスまたは代替パスのどちらでもかまいません。最適なパフォーマンスを実現するには、一次パスをアクティブなパスに設定することをお勧めします。LUN にファイルシステムが存在しない場合にのみ、LUN を割り当て直すことができます。Sun StorEdge 5310 Cluster システムでは、LUN を「所有する」サーバーのみが、その LUN をもう 1 台のサーバーに割り当てることができます。

注 – Sun StorEdge 5310 Cluster システムでは、最初にシステムを起動するときに、すべての LUN が 1 台のサーバー (H1) に割り当てられます。LUN を均等に振り分けるために、サーバー H1 を使用して、一部の LUN をサーバー H2 に割り当て直す必要があります。

アクティブなパスを設定するには、「Set LUN Path」パネルを使用します。Sun StorEdge 5310 Cluster システムでは、どちらのサーバーからも、未割り当てのパスを設定することができます。

▼ LUN パスを設定する

1. **ナビゲーションパネルで、「High Availability」>「Set LUN Path」を選択します。**

注 – 「Set LUN Path」パネルには、最初に、LUN パスが割り当てられていない LUN が何度も表示されることがあります。これは、複数のパスを介した複数のコントローラがそれらの存在を通知するためです。いったん LUN パスが割り当てられると、現在のパスの LUN が一度だけ表示されます。

---

2. **LUN を選択し、「Edit」をクリックします。**
3. **「Primary Path」プルダウンメニューから目的のコントローラを選択します。**

   たとえば、ドロップダウンリストのオプション「1/0」を選択すると、選択した LUN にコントローラ 0 (C0) が割り当てられます。オプション値「X/Y」の「X」値は、0 または 1 のいずれかです。「1」はコントローラが動作中であることを表し、「0」は動作していないことを表します。

   LUN の割り当てを、2 つの使用可能なパスに均等に振り分けてください。たとえば、1 つめと 3 つめの LUN を 1/0 に、2 つめと 4 つめの LUN を 1/1 に振り分けます。

4. **「Apply」をクリックします。**

▼ LUN パスを復元する

LUN の現在アクティブなパスが、一次パスではない場合があります。「Set LUN Path」パネルの「Restore」オプションを使用すると、現在アクティブな LUN パスを一次 LUN パスに復元できます。

注 – LUN パスを復元しても、データは回復されません。これは障害回復のための機能ではありません。

---

1. ナビゲーションパネルで、「High Availability」>「Set LUN Path」を選択します。
2. LUN を選択して、「Restore」をクリックします。

フェイルオーバーの使用可能への切り替え

注 – フェイルオーバーの使用可能への切り替えは、Sun StorEdge 5310 Cluster システムでのみ有効です。

Sun StorEdge 5310 Cluster システムは、「本体」とも呼ばれる一対のアクティブ/アクティブ・サーバーで構成されます。これらのサーバーは、RAID コントローラおよび複数の異なるネットワークへのアクセスを共有します。RAID コントローラは、ファイバコントローラを介して各サーバーに接続されます。2 台のサーバーの最初の NIC が専用のハートビートケーブルで接続されるため、サーバーは互いの健全性状態を監視できます。

正常に動作している間は、各サーバーが独立して LUN のサブセットを管理します。1 台のサーバーにハードウェア障害が発生してデータパスが使用不可になると、障害が発生したサーバーによってそれまで管理されていた IP アドレスおよび LUN の所有権は、動作中のサーバーに自動的に引き継がれます。RAID ボリュームの所有権とネットワークインタフェースのアドレス指定を含む、障害が発生したサーバーのすべての動作は、動作中のサーバーに引き継がれます。これは、「本体のフェイルオーバー」と呼ばれます。

クラスタのフェイルオーバー後、NFS/UDP を使用するクライアントの動作はただちに引き継がれますが、NFS/TCP の場合は再接続が必要です。この再接続は、NFS の再試行で透過的に実行されます。また、CIFS も再接続を必要としますが、別のアプリケーションによって、透過的な再接続、ユーザーへの通知、または続行前のユーザー確認の要求が行われる場合があります。

障害が発生した本体が修復されてオンラインになると、「フェイルバック」と呼ばれる回復処理を開始できます。「High Availability」>「Recover」を選択して「Recover」パネルを表示し、どの LUN をどの本体によって管理するかを決めます。

本体のフェイルオーバーの使用可能への切り替え

1 台の本体に障害が発生すると、フェイルオーバーにより、障害が発生した本体によってそれまで管理されていた IP アドレスおよび LUN の所有権が一時的に動作中の本体に引き継がれます。

注 – 本体のフェイルオーバーを使用可能にすると、DHCP が自動的に使用不可になります。

▼ フェイルオーバーを使用可能にする

1. ナビゲーションパネルで、「High Availability」>「Enable Failover」を選択します。
2. 「Automatic Failover」チェックボックスをクリックします。
3. 「Enable Link Failover」チェックボックスを選択します。

   リンクのフェイルオーバーを使用可能にすると、「Primary」の役割が割り当てられているいずれかのネットワークインタフェースに障害が発生したときに、本体のフェイルオーバーが必ず実行されます。このタイプの障害は「リンク停止」状態と呼ばれます。パートナー本体のネットワークリンクが切断されていると、フェイルオーバーを実行する本体は、パートナー本体がネットワークリンクを再構築したあとで、指定された時間が経過するまで待機する必要があります。

4. 次の項目を入力します。
   - Down Timeout − 1 台の本体のネットワークリンクの信頼性が低下し、そのパートナー本体のネットワークリンクが健全である場合に、本体がフェイルオーバーを実行するまで待機する時間を秒単位で指定します。
   - Restore Timeout − フェイルオーバーが行われるように、パートナー本体の一次リンクの確立を待機する時間を秒単位で指定します。「Restore Timeout」は、リンク停止によって開始されたフェイルオーバーが、パートナー本体の一次リンクが切断されているために中止された場合にのみ使用されます。
5. 「Apply」をクリックして設定を保存します。
6. 本体を両方とも再起動します。

フェイルバックの開始

コントローラのフェイルオーバーは、RAID コントローラに障害が発生すると自動的に実行されます。障害の発生したコントローラに管理されていた LUN は、動作中のコントローラによって一時的に管理されます。

注 – コントローラのフェイルオーバーは、デフォルトで使用可能に設定されています。これを使用不可に切り替えることはできません。

障害の発生した本体または RAID コントローラがオンラインになったときには、本体またはコントローラのフェイルオーバー後に、Sun StorEdge 5310 NAS Appliance または Sun StorEdge 5310 Cluster システムの回復 (フェイルバック) を手動で開始する必要があります。

障害の発生によりフェイルオーバーを実行したサーバーは、完全に機能する状態になると、元のファイルボリュームの所有権を「取り戻す」ことができます。

たとえば、障害が発生した H1 にボリューム A が割り当てられており、フェイルオーバー中に H2 がボリューム A の所有権を引き継いだとします。サーバー H1 が完全に機能する状態に戻ると、ボリューム A の所有権をサーバー H2 から取り戻すことができます。

注意 – 回復を実行する前に、障害の発生したサーバーが完全に動作可能であることを確認してください。

▼ 回復を開始する

1. **ナビゲーションパネルで、「High Availability」>「Recover」を選択して、「Recover」パネルを表示します。**

2. **本体を回復する場合は、RAID のリストから回復する RAID セットを選択します。**
   - 「Head 1」リストには、サーバー H1 の LUN マッピングが表示されます。
   - 「Head 2」(パートナー) リストには、パートナーサーバー H2 の LUN マッピングが表示されます。

3. **コントローラを回復する場合は、RAID のリストから回復する RAID セットを選択します。**
   - 「Controller 0」リストには、コントローラ 0 の LUN マッピングが表示されます。
   - 「Controller 1」(パートナー) リストには、コントローラ 1 の LUN マッピングが表示されます。

4. 「Recover」をクリックします。

   サーバーは、LUN マッピングを再調整して、画面に表示された構成を反映します。

ネットワークポートの構成

「Configure Network Adapters」パネルで、DHCP を使用可能にするか、各ネットワークポートの IP アドレス、ネットマスク、ブロードキャスト、およびネットワークインタフェースカード (NIC) ポートの役割を指定できます。また、各 NIC ポートのエイリアス IP アドレスも追加できます。

注 – Sun StorEdge 5310 Cluster の NIC ポートには、それぞれ役割が割り当てられている必要があります。

---

2 つ以上のポートを結合してポート結合を作成できます。ポート結合では、個々の構成ポートより広い帯域幅を利用できます。ネットワークポートの結合の詳細は、71 ページの「ポート結合」を参照してください。

Sun StorEdge 5310 NAS Appliance のポートの位置

Sun StorEdge 5310 NAS Appliance では、ポートのタイプおよびサーバー上の物理的な位置と論理的な位置に基づいて、事前定義された順序でポートが識別されます。『Sun StorEdge 5310 NAS Appliance および Gateway システムご使用の手引き』を参照して、構成するネットワークポートの位置を確認してください。さまざまなシステム構成が存在しますが、マニュアルで示されているものは一例です。

ネットワークインタフェースカード (NIC) とポートの関係については、『Sun StorEdge 5310 NAS Appliance および Gateway システムご使用の手引き』でも説明しています。

▼ ネットワークアダプタを構成する

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」を選択します。

2. **ネットワークで IP アドレスの割り当てに DHCP サーバーを使用している場合に、これを使用可能にするには、「Enable DHCP」チェックボックスを選択します。**

   DHCP を使用可能にすると、システムは DHCP サーバーから IP アドレスを動的に取得できます。静的 IP アドレスおよびネットマスクを手動で入力する場合、このチェックボックスの選択を解除します。DHCP を使用可能にしない場合、集約されたポートの構成ポートのネットマスクは使用不可のままです。集約されたポートの作成および設定については、71 ページの「ポート結合」を参照してください。

注 – Sun StorEdge 5310 Cluster システムでは、本体のフェイルオーバーが使用可能に設定されている場合、DHCP は使用できません。代わりに、ポートに静的 IP アドレスを割り当て、フェイルオーバーの際に一貫性が保たれるようにする必要があります。

---

3. **「Adapter」リストから、構成するポートを選択します。**

   作成済みポート結合にエイリアス IP アドレスを追加する場合、このリストから該当するポート結合を選択します。ポート結合の作成については、71 ページの「ポート結合」を参照してください。個々のポートは「PORT*x*」、ポート結合は「BOND*x*」というラベルで示されます。

   ポート結合の作成後、個々のポートにはエイリアス IP アドレスを追加できません。ポート結合にのみエイリアス IP アドレスを追加できます。

4. **選択したポートまたはポート結合の IP アドレスを入力します。**

5. **選択したポートまたはポート結合のネットマスクを入力します。**

   ネットマスクによって、IP アドレス内のネットワークアドレスを特定する部分と、ホストアドレスを特定する部分が識別されます。

   読み取り専用の「Broadcast」フィールドは、IP アドレスおよびネットマスクを入力すると自動的に設定されます。ブロードキャストアドレスは、ブロードキャストメッセージをサブネットに送信する際に使用される IP アドレスです。

6. 各ポートに対して、次のいずれかの役割を選択します。

役割	説明
Primary	このポートの役割は、アクティブなネットワークポートであることを示します。
Independent	このポートの役割は、バックアップなど、データの提供以外の目的に使用されるアクティブなネットワークポートであることを示します。
Mirror	このポートの役割は、ファイルボリュームをミラー化するために、このサーバーをほかのサーバーに接続するポートであることを示します。
Private–Sun StorEdge 5310 Cluster only	Private ポートは、もう 1 台の本体の状態を定期的に監視するハートビートの専用ネットワークリンクに予約されています。Private ポートは各本体に 1 つのみです。

注 – 1 つ以上のポートに、一次ポートの役割を割り当てる必要があります。

ポートの役割の詳細は、69 ページの「ポートの位置」を参照してください。

7. 選択したポートにエイリアス IP アドレスを追加するには、「IP-Aliases」フィールドにそのアドレスを入力し、「Add」ボタンをクリックして「IP-Aliases」リストに追加します。

   本体 1 台構成のシステムではインタフェースごとに最大 9 つ、本体 2 台構成のシステムでは最大 4 つのエイリアスを設定できます。リストからエイリアスを削除するには、対象のエイリアスを選択して「Trash」ボタンをクリックします。変更は、「Apply」をクリックすると保存されます。

8. 「Adapter」リスト内のすべてのポートに対して、手順 3 ～ 7 を繰り返します。
9. 「Apply」をクリックして、変更内容を保存します。

デフォルトゲートウェイアドレスの設定

デフォルトゲートウェイアドレスは、ほかのサブネットへの接続にデフォルトで使用される、ローカルサブネット上のゲートウェイまたはルーターの IP アドレスです。ゲートウェイまたはルーターは、遠隔の宛先にデータを送信するデバイスです。システムには、デフォルトゲートウェイのアドレスを指定する必要があります。

▼ デフォルトゲートウェイのアドレスを指定する

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Set Gateway Address」を選択します。
2. 「Gateway」テキストボックスにゲートウェイアドレスを入力します。
3. 「Apply」をクリックして設定を保存します。

ネームサービス

この節では、Windows のセキュリティー機能である WINS、DNS、NIS、NIS+ の設定、およびネームサービスの構成について説明します。

ネームサービスの詳細は、第 6 章の、77 ページの「Active Directory サービスおよび認証」を参照してください。

Windows のセキュリティーの構成

ドメイン、ワークグループ、または Active Directory サービス (ADS) の構成は、Windows の機能です。実行中のネットワークが UNIX のみで構成されている場合、Windows ドメインや Windows ワークグループを構成する必要はありません。

Windows ワークグループ、NT ドメインのセキュリティー、または ADS を使用可能にするには、「Configure Domains and Workgroups」パネルを使用します。デフォルトでは、システムは Windows ワークグループモードで「workgroup」というワークグループ名で構成されます。

▼ Windows のセキュリティーを構成する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Domains and Workgroups」を選択します。
2. Windows ドメインのセキュリティーを使用可能にするには、「Domain」オプションを選択します。

   このオプションを選択すると、指定したドメイン上にこのサーバー用のアカウントが作成されます。指定したドメインにサーバーを追加する権限を持つユーザーアカウントを指定する必要があります。

   a. 「Domain」フィールドにドメイン名を入力します。

      この名前は、NetBIOS の 15 文字の制限に準拠している必要があります。

b. 「User Name」フィールドおよび「Password」フィールドに、ドメイン管理者ユーザーの名前およびパスワードをそれぞれ入力します。

ユーザー名は 16 文字以内で指定する必要があります。

3. Windows ワークグループのセキュリティーを使用可能にするには、「Workgroup」オプションを選択し、「Name」フィールドにワークグループの名前を入力します。

ワークグループの名前は、NetBIOS の 15 文字の制限に準拠している必要があります。

4. 任意で、Sun StorEdge 5310 NAS Appliance システムの説明を「Comments」フィールドに入力します。

5. ADS を使用可能にするには、「Enable ADS」チェックボックスをクリックします。

ADS の詳細は、78 ページの「Active Directory サービス」を参照してください。

注 – ADS を使用可能にする前に、システムの時刻と ADS Windows ドメインコントローラの時刻の誤差が 5 分以内であることを確認してください。時刻を確認するには、ナビゲーションパネルから「System Operations」>「Set Time and Date」を選択します。

---

a. 「Domain」フィールドに、ADS が動作している Windows ドメインを入力します。

システムがこのドメインに属している必要があります。

b. 「User Name」フィールドに、管理権限を持つ Windows ユーザーの名前を入力します。

このユーザーは、ドメイン管理者か、ドメイン管理者グループのメンバーである必要があります。ADS クライアントでは、このユーザーによるセキュリティー保護された ADS の更新が検証されます。

注 – このフィールドにドメイン管理者名を入力しても ADS の更新が行われない場合は、ドメインコントローラでドメイン管理者パスワードを変更する必要があります。パスワードの変更は、管理者ユーザーのみが行う必要があります。また、同じパスワードを再使用することもできます。詳細は、Microsoft のサポートサービスの Web サイトで「文書番号 Q248808」を参照してください。

---

c. 「Password」フィールドに、Windows 管理者ユーザーのパスワードを入力します。

d. 「Container」フィールドに、LDAP (Lightweight Directory Access Protocol) の DN (識別名) 記法で Windows 管理者ユーザーの ADS のパスを入力します。

詳細は、78 ページの「Active Directory サービス」を参照してください。

注 – パスには、ドメイン名を含めないでください。

e. ADS ドメインがサイトを使用する場合は、「Site」フィールドに適切なサイト名を入力します。サイトを使用しない場合は、「Site」フィールドは空白のままにしてください。サイト名を指定すると、ドメインコントローラを選択したときにこのサイトが含められるようになります。

f. 「Kerberos Realm Info」セクションに、ADS の識別に使用されるレルム名を入力します。

通常、これは ADS ドメインまたは DNS ドメインです。「Apply」をクリックすると、入力した値がすべて大文字に変換されます。

g. 「Server」フィールドに、Kerberos Key Distribution Center (KDC) サーバーのホスト名を入力します。

通常、これは ADS ドメインのプライマリドメインコントローラのホスト名です。システムが DNS を介して KDC サーバーを検索できる場合は、このフィールドは空白のままでかまいません。

6. 「Apply」をクリックして設定を保存します。

セキュリティーモードをワークグループと NT ドメイン間で切り替えると、「Apply」をクリックしたときにサーバーが自動的に再起動されます。

WINS の設定

Windows インターネットネームサービス (Windows Internet Name Service、WINS) は Windows の機能です。実行中のネットワークが UNIX のみで構成されている場合、WINS を設定する必要はありません。

▼ WINS を設定する

1. ナビゲーションパネルで、「Windows Configuration」>「Set Up WINS」を選択します。
2. WINS を使用可能にするには、「Enable WINS」チェックボックスをクリックします。

このボックスを選択すると、システムが WINS クライアントに設定されます。

3. プライマリ WINS サーバーの IP アドレスを所定のフィールドに入力します。

プライマリ WINS サーバーは、NetBIOS の名前解決で最初に照会されるサーバーです。

4. セカンダリ WINS サーバーの IP アドレスを所定のフィールドに入力します。

   プライマリ WINS サーバーが応答しない場合、システムによってセカンダリ WINS サーバーが照会されます。

5. 「Scope」フィールドに NetBIOS の適用範囲識別子を入力します (任意)。

   適用範囲を定義すると、このコンピュータと同じ適用範囲が設定されていないすべてのシステムとの通信ができなくなります。このため、この設定には注意が必要です。適用範囲は、大規模な Windows ワークグループを小規模なグループに分割する場合に役立ちます。適用範囲を使用する場合、NetBIOS またはドメインの命名規則に従って、適用範囲 ID を 16 文字以内で設定する必要があります。

6. 「Apply」をクリックして設定を保存します。

DNS の設定

ドメインネームシステム (DNS) は、ホスト名を Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムの IP アドレスに解決する際に使用されます。

注 – 動的 DNS を使用しないで DNS を使用する場合は、使用している DNS データベースにサーバーのホスト名および IP アドレスを追加してください。動的 DNS を使用する場合は、DNS データベースを手動で更新する必要はありません。詳細は、DNS のマニュアルを参照してください。

▼ DNS を設定する

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Set Up DNS」を選択します。
2. 「Enable DNS」チェックボックスを選択します。
3. DNS サーバーのドメイン名を入力します。
4. ネットワークで使用可能にする DNS サーバーの IP アドレスを入力し、「Add」ボタンをクリックして、このサーバーを「Server List」に追加します。

   追加する各 DNS サーバーに対して、この手順を繰り返します。このリストには、DNS サーバーを 2 台まで追加できます。

   システムでは、ドメインの名前解決の際に、サーバーリストの一番上にある DNS サーバーが最初に照会されます。そのサーバーで要求が解決されない場合、リスト内の次のサーバーが照会されます。

5. リスト内の DNS サーバーの検索順序を変更するには、移動するサーバーをクリックし、「Up」ボタンまたは「Down」ボタンをクリックします。

   リストからサーバーを削除するには、サーバーの IP アドレスを選択し、「Trash」ボタンをクリックします。

6. 「Enable Dynamic DNS」チェックボックスを選択し、動的 DNS クライアントによって Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムが DNS のネームスペースに追加されるようにします。

   使用する DNS サーバーで動的更新が許可されていない場合は、このオプションを使用可能にしないでください。また、23 ページの「Windows のセキュリティーの構成」で説明した Kerberos レルムおよび KDC サーバーを構成する必要もあります。DNS サーバーでセキュリティー保護されていない動的更新が許可されている場合に、このチェックボックスを選択して動的 DNS を使用可能にすると、セキュリティー保護されていない動的更新が自動的に実行されます。

7. セキュリティー保護された動的 DNS 更新を使用可能にするには、次の情報を入力します。この情報は、セキュリティー保護されていない更新には不要です。

   a. 「DynDNS User Name」フィールドに、動的 DNS 更新の実行権限を持つ Windows ユーザーの名前を入力します。

      このユーザーのアカウントは、23 ページの「Windows のセキュリティーの構成」に記載されている「Configure Domains and Workgroups」パネルで指定した ADS ドメインおよび Kerberos レルム内に存在する必要があります。

注 – このフィールドにドメイン管理者名を入力しても ADS の更新が行われない場合は、ドメイン管理者は、ドメインコントローラでパスワードを変更する必要があります。パスワードの変更は、管理者ユーザーのみが行う必要があります。また、同じパスワードを再使用することもできます。詳細は、Microsoft のサポートサービスの Web サイトで「文書番号 Q248808」を参照してください。

---

   b. 「DynDNS Password」に DynDNS ユーザーのパスワードを入力します。

      このフィールドを更新する場合、パスワード全体を削除してから新しいパスワードを入力します。

8. 「Apply」をクリックして設定を保存します。

NIS の設定

ネットワーク情報サービス (NIS) は UNIX の機能です。実行中のネットワークが Windows のみで構成されている場合、NIS を設定する必要はありません。

「Set Up NIS」パネルを使用して、NIS を使用可能にし、ドメイン名およびサーバーの IP アドレスを指定します。

▼ NIS を設定する

1. ナビゲーションパネルで、「UNIX Configuration」>「Set Up NIS」を選択します。
2. 「Enable NIS」チェックボックスを選択します。

   NIS を使用可能にすると、NIS データベースからホスト、ユーザー、およびグループの情報をインポートするようにシステムが構成されます。
3. 「Domain Name」フィールドに、NIS サービス用に使用するドメインの名前を入力します。

   domain.com などの、DNS の命名規則を使用してください。
4. 「Server」フィールドに IP アドレスまたは NIS サーバーの名前を入力します。

   これは、データベースのインポート元のサーバーです。

   サーバーの IP アドレスが不明な場合、「Server」フィールドは空白のままにしておいてください。ただし、「Server」フィールドを空白にする場合は、「Use Broadcast」チェックボックスを選択する必要があります。「Use Broadcast」を選択すると、NIS サーバーの適切な IP アドレスが自動的に取得されます。
5. NIS 情報の更新間隔を分単位で入力します。デフォルトの設定は 5 分です。
6. NIS サーバーの IP アドレスを自動的に取得するには、「Use Broadcast」チェックボックスを選択します。
7. NIS サーバーからシステムにホスト情報をダウンロードするには、「Update Hosts」チェックボックスを選択します。
8. NIS サーバーからシステムにユーザー情報をダウンロードするには、「Update Users」チェックボックスを選択します。
9. NIS サーバーからシステムにグループ情報をダウンロードするには、「Update Groups」チェックボックスを選択します。
10. NIS サーバーからシステムにネットグループ情報をダウンロードするには、「Update Netgroups」チェックボックスを選択します。
11. 「Apply」をクリックして、変更内容を保存します。

NIS+ の設定

ネットワーク情報サービスプラス (NIS+) は UNIX の機能です。実行中のネットワークが Windows のみで構成されている場合、NIS+ を設定する必要はありません。

注 – NIS+ と NIS には関連性はありません。NIS+ のコマンドおよび構造は、NIS とは異なります。

▼ NIS+ を設定する

1. NIS+ 環境で Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムを正常に動作させるには、NIS+ サーバー上のホストの資格ファイルにそれを追加する必要があります。使用する NIS+ サーバーで次の手順を実行します。

   a. スーパーユーザーでログインします。

   b. 次のコマンドを入力します。

      nisaddcred -p unix.SERVER@DOMAIN -P SERVER.DOMAIN. des

      SERVER には Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムの名前を、DOMAIN には Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムが所属する NIS+ ドメインの名前を指定します。

注 – -P 引数のあとに指定する場合にかぎり、ドメイン名の末尾にはピリオドを追加する必要があります。

      たとえば、Sun StorEdge 5310 NAS Appliance の名前が SS1 で、NIS+ ドメインが sun.com である場合は、次のように入力してください。

      nisaddcred -p unix.ss1@sun.com -P ss1.sun.com. des

   c. プロンプトで、パスワードを入力します。

      このパスワードは、この手順の後半で NIS+ を使用するようにシステムを構成するときにも使用します。パスワードを入力します。

2. 遠隔クライアントから Web ブラウザウィンドウを開いてシステムに接続し、Web Administrator にログインします。

3. ナビゲーションパネルで、「UNIX Configuration」>「Set Up NIS+」を選択します。

4. 「Enable NIS+」チェックボックスを選択します。

5. 「Home Domain Server」フィールドに、NIS+ のホームドメインサーバーの IP アドレスを入力します。

   ホームドメインサーバーの IP アドレスが不明な場合、このフィールドを空白のままにして、「Use Broadcast」チェックボックスを選択してください。このオプションを選択すると、システムによってホームドメインサーバーの適切な IP アドレスが自動的に取得されます。

6. 「NIS+ Domain」フィールドに NIS+ のホームドメインを入力します。

注 – NIS+ ドメイン名の末尾には「.」(ピリオド) を付ける必要があります。

---

7. NIS+ サーバーの、セキュリティー保護された RPC パスワードを入力します。

   これは、29 ページの手順 1c で設定したパスワードです。

8. 「Search Path」に、コロンで区切ったドメインのリストを入力します。

   検索パスには、NIS+ での情報検索時に検索されるドメインを指定します。ホームドメインとその親のみを検索する場合、このフィールドは空白のままにします。

   たとえば、NIS+ ドメインが **`eng.sun.com.`** で検索パスが空白の場合、システムの名前解決では、最初に **`eng.sun.com.`**、次に **`sun.com.`** が検索されます。これに対して、検索パスに **`sun.com.`** を指定した場合は、システムの名前解決では **`sun.com`** のドメインのみが検索されます。

9. ホームドメインサーバーの IP アドレスが不明な場合は、「Use Broadcast」チェックボックスを選択します (手順 5 を参照)。

10. 「Apply」をクリックして設定を保存します。

ネームサービスの構成

ネームサービス (NS) の検索順序によって、照会を解決するためにネームサービスを検索する順序が制御されます。これらのネームサービスには、LDAP、NIS、NIS+、DNS、ローカルネームサービスなどがあります。名前解決にこれらのサービスを使用するには、選択したサービスを使用可能にする必要があります。

▼ ユーザー、グループ、ネットグループ、およびホストの検索順序を設定する

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure Name Services」を選択します。

2. 「Users Order」タブで、ユーザーの検索順序を選択します。

   a. 「Services Not Selected」ボックスから、ユーザーの検索に使用するサービスを選択します。

   b. 「>」ボタンをクリックして、選択したサービスを「Services Selected」ボックスに移動します。

   c. ユーザーの検索に使用する各サービスに対して、この手順を繰り返します。

   d. ユーザーの検索からサービスを削除するには、該当するサービスを選択して「<」ボタンをクリックします。

e. 「Services Selected」ボックス内のサービスの検索順序を変更するには、各サービスを選択します。

f. 「Up」ボタンおよび「Down」ボタンをクリックして、選択したサービスを上下に移動します。リストの最上位にあるサービスが、ユーザーの検索で最初に使用されます。

3. 手順 2 の説明に従って、「Groups Order」タブでグループの検索に使用するサービスを選択します。

4. 手順 2 の説明に従って、「Netgroup Order」タブでネットグループの検索に使用するサービスを選択します。

5. 手順 2 の説明に従って、「Hosts Order」タブでホストの検索に使用するサービスを選択します。

6. 「Apply」をクリックして、変更内容を保存します。

電子メール通知の設定

この画面では、SMTP (メール転送プロトコル) サーバー名および電子メール通知の受信者を設定します。システムでエラーが検出されると、システムによって電子メールメッセージが送信されます。

名前解決を確実に実行するには、「Configure Hosts」パネルで SMTP サーバーホスト名を設定する (89 ページの「ホストの構成」を参照) か、DNS を設定する (26 ページの「DNS の設定」を参照) 必要があります。

▼ SMTP を設定して電子メールメッセージを受信者に送信する

1. ナビゲーションパネルで、「Monitoring and Notification」>「Set Up Email Notification」を選択します。

2. 通知の送信先の SMTP サーバーの名前を入力します。

3. 「Email Address」ボックスに、システムエラーを自動的に通知する宛先となる担当者の電子メールアドレスを入力します。

4. この受信者に送信する電子メールのタイプを指定します。「Notification」または「Diagnostics」、あるいはその両方をチェックします。

5. 「Add」ボタンをクリックして、新しい受信者を受信者のリストに追加します。すべての受信者に対して手順 1 ～手順 4 を繰り返します。電子メールアドレスは 4 つまで入力できます。

   リストから受信者を削除するには、該当するアドレスを選択し、「Trash」ボタンをクリックしてください。

6. 「Notification Level」を選択します。
   - 「Errors and Warnings」チェックボックスを選択すると、受信者にすべての警告およびエラーが通知されます。
   - 「Errors Only」を選択すると、電子メール受信者にエラーが通知され、警告は通知されません。
   - 「None」を選択すると、通知は使用不可になります。

7. 「Apply」をクリックして設定を保存します。

ロギングの設定

遠隔ロギングを使用可能にすると、システムによって、システムログの指定サーバーへの送信またはローカルアーカイブへの保存、あるいはその両方が実行されます。指定サーバーは、`syslogd` が動作している UNIX サーバーである必要があります。ロギングホストをドメイン名で指定する場合は、遠隔ロギングを使用可能にする前に、システム上で DNS 設定を構成する必要があります。

注意 – システムの停止時にログが消去されないようにするには、遠隔ロギングを使用可能にするか、ローカルディスク上にログファイルを作成する必要があります。そうしない場合は、システムによって、起動中に揮発性メモリー内に一時ログファイルが作成されます。この一次ログファイルは、初期起動中に発生するエラーを保持して、あとで表示するには役立ちますが、電源障害発生時またはシステムの再起動時には保持されません。

▼ 遠隔ロギングおよびローカルロギングを設定する

1. ナビゲーションパネルで、「Monitoring and Notification」>「View System Events」>「Set Up Logging」を選択します。
2. 「Enable Remote Syslogd」ボックスを選択します。
3. DNS 設定が構成されている場合は、「Server」フィールドに DNS ホスト名を入力します。DNS 設定が構成されていない場合は、IP アドレスを入力します。これは、システムログの送信先になります。

4. 「Facility」で適切な機能を選択します。

   機能は、メッセージを生成するアプリケーションまたはシステムコンポーネントを示します。syslogd サーバーに送信されるすべてのメッセージには、この機能の値が指定されます。「Set Up Remote Logging」パネルで選択できる機能の値は次のとおりです。

機能	説明
Kern	カーネルによって生成されるメッセージ。ユーザープロセスでは生成されないメッセージです。
User	ランダムユーザープロセスによって生成されるメッセージ。機能を指定しない場合は、この機能識別子がデフォルトで指定されます。
Mail	メールシステム。
Daemon	システムデーモンまたはネットワークデーモン。
Auth	ログインなどの認証システム。
Syslog	syslogd によって内部的に生成されるメッセージ。
Local0 ～ Local7	ローカルでの使用のために予約済み。

5. イベントのタイプにチェックマークを付けて、ログに記録するシステムイベントのタイプを選択します (142 ページの「システムイベント」を参照)。
6. ローカルログファイルを維持するには、「Enable Local Log」オプションを選択します。
7. 「Log File」フィールドに、ログファイルのパス (ログファイルを格納するシステム上のディレクトリ) およびファイル名を入力します。
8. 「Archives」フィールドに、アーカイブファイルの最大数を入力します。

   指定可能な範囲は 1 ～ 9 です。
9. 「Size」フィールドに、各アーカイブファイルの最大ファイルサイズを K バイト単位で入力します。

   指定可能な範囲は 1000K ～ 999,999K バイトです。
10. 「Apply」をクリックして設定を保存します。

言語の割り当て

このシステムのオペレーティングシステムでは Unicode がサポートされているため、NFS および CIFS に対してローカル言語を設定できます。通常、言語の割り当ては、システムの初期設定時のウィザードで行います。ただし、あとで言語を再設定する必要があれば、手動で設定できます。

▼ 言語を割り当てる

1. ナビゲーションパネルで、「System Operations」>「Assign Language」を選択します。
2. プルダウンメニューに表示される言語から、ローカル言語を選択します。
3. 「Apply」をクリックして、変更内容を保存します。

構成情報のバックアップ

システムの構成が完了したら、システム障害に備えて構成情報をバックアップしておくことをお勧めします。構成情報のバックアップについては、196 ページの「構成のバックアップ」を参照してください。

次に実行する作業

この時点で、システムがネットワークと完全に通信可能な状態になっています。ただし、ユーザーがデータの格納を開始する前に、ファイルシステムおよびユーザーアクセス権限を設定する必要があります。次の章 (35 ページの「ファイルシステムの設定と管理」) では、ファイルシステムの設定について説明します。

割り当て、共有、エクスポート、またはその他のアクセス制御の設定については、101 ページの「共有、割り当て、およびエクスポート」を参照してください。

特定の機能を設定する必要がある場合は、索引を参照して詳細を確認してください。

第3章

ファイルシステムの設定と管理

この章では、Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster のファイルシステムの概念、設定、および管理方法について説明します。

この章の内容は、次のとおりです

ファイルシステムの概念

以降の節では、NAS ストレージで使用するいくつかの基本的なファイルシステムの概念および属性の定義について説明します。

RAID

RAID (Redundant Array of Independent Disks) システムでは、アレイコントローラを介してデータを複数のドライブに分散できます。これによって、パフォーマンスおよびデータの安全性が大幅に向上し、回復の可能性も高くなります。RAID の基本概念は、小さい物理ドライブをグループ化し、非常に大きい単一のドライブとしてネットワーク上に表示することです。コンピュータユーザーからは、RAID は 1 台のドライブのように見えます。システム管理者には、RAID の物理コンポーネントはドライブのグループとして表示されますが、RAID 自体を単一の装置として管理できます。

RAID 構成には、さまざまな種類があります。Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster では、RAID 5 のみをサポートしています。Sun StorEdge 5310 Gateway システムでは、RAID 1、RAID 0+1、および RAID 5 をサポートしています。

RAID 0 (未サポート)

RAID 0 は、RAID の開発目的である冗長性を備えていません。ただし、ドライブのパフォーマンスを大幅に向上することができます。RAID 0 では、「ストライプ化」という概念を採用しています。ストライプ化とは、データをストライプに分割することです。1 つのストライプが 1 台めのドライブに書き込まれ、次のストライプは 2 台めのドライブに書き込まれ、これ以降も同様に書き込まれます。ストライプ化の主な利点は、アレイ内のすべてのドライブが読み取りおよび書き込みを同時に処理できることです。同時アクセスによって読み取りと書き込みの両方が非常に速くなります。

ただし、RAID 0 には冗長性がないため、1 台のドライブに障害が発生するとアレイ全体のすべてのデータが失われる可能性があります。RAID 0 は、パフォーマンスを最優先とし、データ損失の重要性が低い場合にもっとも適しています。

RAID 1 (Sun StorEdge 5310 Gateway システムのみ)

RAID 1 アレイの主要概念は、ドライブの「ミラー化」です。ミラー化によって、同じ容量のストレージを提供するために必要なドライブ数は 2 倍になりますが、ドライブの最新のバックアップを提供できます。ミラー化されたドライブは常にオンラインになっているため、一次ドライブに障害が発生した場合には、非常に迅速にミラー化ドライブにアクセスできます。各一次ドライブは、同じサイズの 2 台めのドライブによってミラー化されます。すべての書き込みは複製され、RAID 1 アレイの両方のメンバーに同時に書き込まれます。RAID 1 は、優れた高可用性を提供します。RAID 1 は、データのセキュリティー保護と完全性が不可欠であり、パフォーマンスはそれほど重要でない場合にもっとも役立ちます。

RAID 0+1 (Sun StorEdge 5310 Gateway システムのみ)

RAID 0+1 は、ストライプ化とミラー化の 2 つの RAID 概念を組み合わせることによって、パフォーマンスと高可用性の両方を向上させます。ミラー化ドライブのペアが、RAID 0 アレイに組み込まれます。すべての書き込みは複製され、両方のミラー化ドライブに同時に書き込まれます。RAID 0 のストライプ化によってアレイ全体のパフォーマンスが向上する一方で、RAID 1 のドライブのミラー化によって個々のドライブの優れた高可用性が提供されます。RAID 0+1 は、パフォーマンスよりセキュリティーが重視される一方で、パフォーマンスも重要である環境に適しています。

RAID 5

RAID 5 は、アレイ全体のドライブの数を倍増させることなく、ストライプ化によるパフォーマンスの向上と、ミラー化による冗長性の両方を実現するアレイです。

RAID 5 では、ストライプ化および「パリティー」情報を使用します。パリティー情報とは、格納される情報のビットを組み合わせて作成される少量のデータで、このデータから残りの情報を抽出できます。つまり、パリティー情報とは、元のデータの一部が失われた場合でも、残りのデータとパリティーデータを組み合わせることで完全な元のデータを再生成できるように、元のデータを繰り返したものです。パリティー情報は、特定のドライブに格納されるのではありません。ストライプセット内の異なるドライブを使用して、RAID 5 セットのさまざまな領域がパリティー保護されます。

RAID 5 アレイでは、パリティー情報がストライプの 1 つとしてストライプ配列に含まれます。アレイ内の 1 台のドライブで障害が発生すると、それ以外の使用可能なドライブ内のパリティー情報と元のデータの残りの部分によって、障害が発生したドライブから失われた情報が再構築されます。このように、RAID 5 アレイは、ミラーによる高可用性とストライプによるパフォーマンスの向上を兼ね備えた非常に高度な RAID タイプです。パリティー情報用の余分な領域は少量で済むため、ソリューションにコストがかからないことも利点の 1 つです。

各アレイのドライブが構成されている最初の格納装置 (ファイバチャネルアレイの場合は 5300 RAID EU、SATA アレイの場合は空の 5300 RAID EU に接続されている最初の EU S) には、6 台のドライブ (5+1) で構成される RAID 5 グループが 2 つと、グローバルホットスペアが 2 つ含まれます。それ以降のすべての EU F または EU S 格納装置には、7 台のドライブ (6+1) で構成される RAID 5 グループが 1 つまたは 2 つ含まれ、合計で 7 台または 14 台のドライブが構成されます。

注意 – RAID サブシステムで重大な障害が発生しているときに、システムソフトウェアまたは RAID ファームウェアを更新して、新しいボリュームを作成したり既存のボリュームを再構築したりしないでください。

LUN

論理ユニット番号 (LUN) は、物理デバイスまたは仮想デバイスの論理表記を識別するための番号です。Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster の RAID セットと LUN の間には、1 対 1 の対応関係があります。ただし、システムは LUN を独立エンティティーとして管理し、単一のストレージボリュームとして処理します。

LUN をこのように取り扱うことで、Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster でのファイルシステムの構築プロセスは大幅に簡略化されます。RAID セットの領域へのアクセスは、ドライブの物理的な境界とは無関係に LUN を介して行われます。

ストレージリソースの管理は LUN を介して実施し、RAID セット自体を直接管理することはほとんどありません。RAID セットおよび LUN の設定の手順およびその詳細は、39 ページの「RAID セットおよび LUN の作成」を参照してください。

パーティション

パーティションは LUN 上のセクションで、LUN 内で使用可能な総領域を分割する方法を提供します。Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster のオペレーティングシステムは、1 つの LUN につき最大 31 個のパーティションをサポートします。

LUN の作成時、使用可能なすべての領域は最初のパーティションに配置され、それ以外のパーティションは空になります。パーティション内の領域を使用するには、ファイルボリュームを作成する必要があります。各パーティションに作成できるファイルボリュームは 1 つのみですが、1 つのファイルボリュームを複数のパーティションにスパン化することができます。ファイルボリュームを作成すると、パーティションのサイズは自動的にファイルボリュームのサイズに合わせて調整されます。LUN 上のそれ以外の領域は、自動的に次のパーティションに割り当てられます。オペレーティングシステムがサポートするすべてのファイルボリュームを作成したあとは、LUN 上の残りの領域にはアクセスできなくなります。

セグメント (39 ページの「セグメント」を参照) を配置することで、ファイルボリュームのサイズを増やすことができます。セグメントは、実際には、特殊な性質を持つ別のファイルボリュームです。既存のボリュームにセグメントを追加すると、そのセグメントはボリュームから分離できなくなります。ユーザーからはボリュームに領域が追加されただけのように見えます。このシステムの柔軟性によって、ユーザーの作業を妨げることなくファイルボリュームを作成し、必要に応じて拡張できます。複数のボリュームにユーザーのデータを分散させる必要もありません。

システム管理者がドライブおよび LUN を追加しても、ユーザーからはボリューム内に領域が追加されたようにしか見えません。

ファイルボリューム

情報の格納に使用できる領域を定義するものです。使用可能な領域を持つパーティションから作成されます。パーティション内の使用可能なすべての領域がボリュームに割り当てられていない場合、残りの領域は自動的に次のパーティションに割り当てられます。新しいファイルボリュームのサイズは 255G バイトに制限されます。これを超えるサイズのファイルボリュームを作成するには、最大 63 個のセグメント (「39 ページの「セグメント」」を参照) を作成して元のファイルボリュームに配置します。

ユーザー側では、ファイルボリュームとその内部のディレクトリ構造が重要です。ファイルボリュームの空き領域が少なくなった場合、管理者はセグメントを追加して、ファイルボリューム内の使用可能な領域を増やすことができます。物理的には、ドライブのみでなく拡張ユニットも追加できます。ただし、物理的にはユーザー側に表示されません。ユーザーには、ボリューム内にストレージ領域が追加されたようにしか見えません。

セグメント

セグメントは、ファイルボリュームと同じように作成されたストレージ領域の「ボリューム」です。既存のファイルボリュームにいつでも配置できます。セグメントを配置すると、元のファイルボリュームの総容量が増加します。各セグメントは個別に作成してファイルボリュームに配置する必要があります。ファイルボリュームに配置したあとで、セグメントをボリュームから分離することはできません。

通常、セグメントは必要に応じて作成され、ボリュームの空き容量が少なくなるとボリュームに配置されます。セグメントの配置による領域の追加の主な利点は、新しいドライブや、新しいアレイにもセグメントを作成できることです。セグメントを元のファイルボリュームに配置すると、物理的なストレージが異なる場所にあることはユーザーからは見えません。このため、ネットワークを停止することなく、必要なときに領域を追加して、データストレージの再構成や、より大きなファイルボリュームの作成を行うことができます。

ファイルシステムの作成

Sun StorEdge 5310 Gateway システムを構成する場合は、ストレージシステム構成ツールを使用して、ホットスペアドライブおよび LUN を作成します。詳細は、使用しているゲートウェイに接続したストレージシステムに付属のマニュアルを参照してください。

Sun StorEdge 5310 NAS Appliance または Cluster システムを構成する場合は、39 ページの「RAID セットおよび LUN の作成」および 44 ページの「ホットスペアとしてのドライブの指定」の節を参照してください。

RAID セットおよび LUN の作成

Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster では、RAID セットの作成と定義が、LUN の定義に統合されています (35 ページの「ファイルシステムの概念」を参照)。つまり、この 2 つのオブジェクトを同時に作成することに

なります。Sun StorEdge 5310 NAS Appliance および Cluster システムでは、RAID セットの基本構造を選択して LUN を定義することができ、通常は RAID セットの定義に関して必要である多くの作業が自動化されています。

注意 – Sun StorEdge 5310 Cluster ユーザーのみ: サーバーは、それぞれが所有している LUN を管理しています。LUN を追加する前に、フェイルオーバーが使用可能に設定され、構成されていることを確認してください。詳細は、17 ページの「フェイルオーバーの使用可能への切り替え」を参照してください。

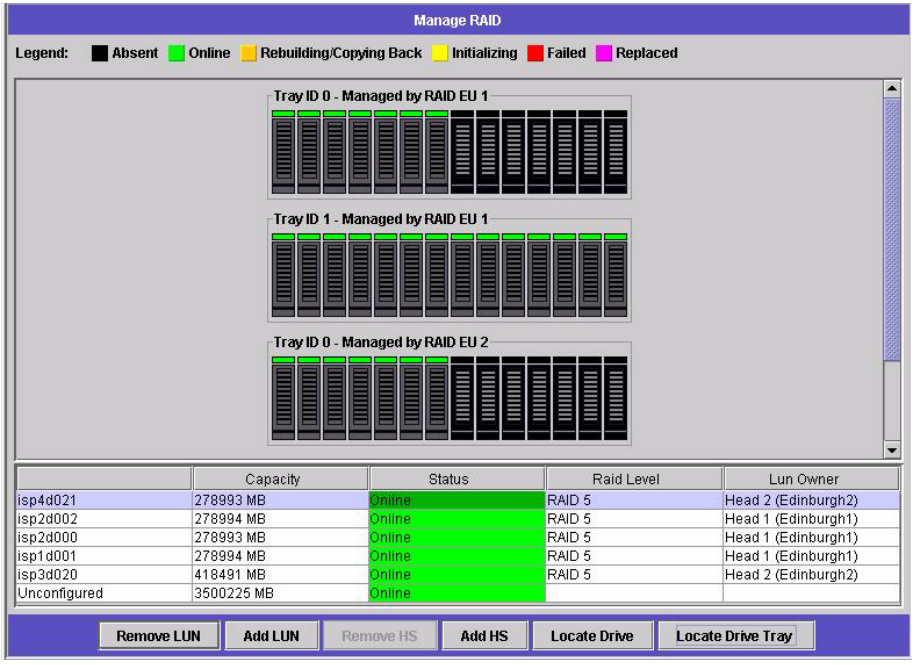
Sun StorEdge 5310 NAS Appliance および Cluster システムでは、パーティションの定義も自動化されています。パーティションは、LUN の作成時に自動的に定義されます。初期状態では、Sun StorEdge 5310 NAS Appliance および Cluster システムには、割り当て済みの 2 台のホットスペアドライブと、2 つ以上のデフォルトの LUN が存在します。

Sun StorEdge 5310 NAS Appliance および Cluster システムでは、RAID セットと LUN が同時に作成されるようになっており、どちらの構築プロセスも簡略化されています。

LUN を追加する際は、LUN を作成する前に LUN 内のディスクにホットスペアなどの別の機能を割り当てていないことを確認してください。別の LUN に割り当てられているドライブ、またはホットスペアとして割り当てられているドライブを、新しい LUN に含めることはできません。

▼ 新しい LUN を追加する

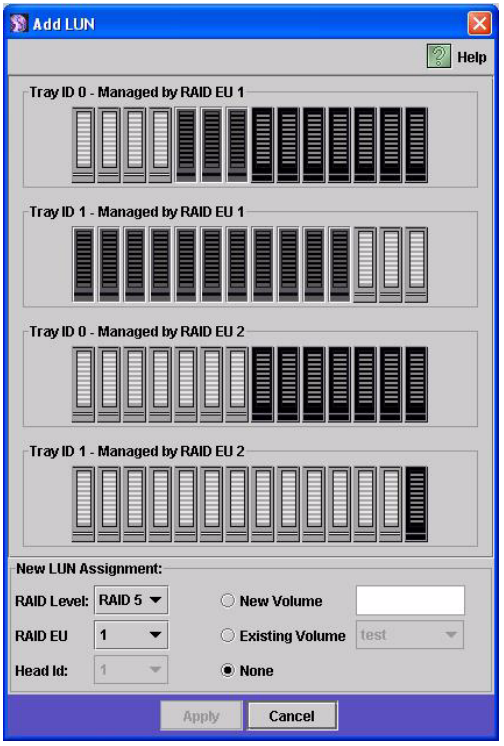
1. ナビゲーションパネルで、「RAID」>「Manage RAID」を選択します。
   「Manage RAID」パネルが表示されます。



注 – ドライブまたはドライブトレーの位置を確認するには、「Locate Drive」または「Locate Drive Tray」ボタンをクリックします。この操作によって、ドライブまたはドライブトレーの LCD インジケータが点滅します。

---

2. 「Add LUN」をクリックします。
   「Add LUN」ウィンドウが表示されます。



3. 「RAID EU」プルダウンメニューから、LUN を追加するコントローラの番号を選択します。

4. 各ドライブのイメージをクリックして、この LUN に含めるドライブを選択します。

3 つ以上のドライブを選択する必要があります。ドライブのイメージには、各ドライブの状態が示されます。

表 3-1　「Add LUN」ダイアログボックスのドライブの状態インジケータ

ドライブ	意味
	このスロットのドライブは、LUN メンバーシップに使用できます。
	このスロットのドライブは、LUN メンバーシップにすでに選択されています。
	このスロットにドライブは存在しません。

5. 次のボリュームオプションのいずれかを選択します。

オプション	説明
New Volume	このオプションは、この LUN に新しいボリュームを作成する場合に選択します。ボリュームの作成には LUN 全体が使用されます。所定のフィールドに新しいボリュームの名前を入力してください。
Existing Volume	このオプションは、この LUN を使用して既存のボリュームにディスク領域を追加 (セグメントを作成および配置) する場合に選択します。次に、プルダウンメニューから拡張するボリュームを選択します。
None	このオプションは、名前を割り当てずに新しい LUN を作成する場合に選択します。

6. 「Apply」をクリックして、新しい LUN を追加します。

システムでの LUN の追加には数時間かかります。

ホットスペアとしてのドライブの指定

Sun StorEdge 5310 Appliance または Cluster システムでは、ドライブをホットスペアとして構成できます。

▼ ドライブをホットスペアとして指定する

1. ナビゲーションパネルで、「RAID」>「Manage RAID」を選択します。
2. 画面下部の「Add HS」ボタンをクリックします。
3. ドライブのイメージをクリックして、必要なドライブを選択します。

   ホットスペアとして使用するディスクの容量が、このサーバーのすべての LUN でもっとも容量の大きいディスクと同じか、それよりも大きいことを確認してください。

   ドライブのイメージには、各ドライブの状態が示されます。

表 3-2　「Add Hot Spare」のドライブの状態のイメージ

ドライブ	意味
	このスロットのドライブは、ホットスペアとして使用できます。
	このスロットのドライブは、ホットスペアとしてすでに選択されています。
	このスロットにドライブは存在しません。

4. 「Apply」をクリックして新しいホットスペアを追加します。

ファイルボリュームまたはセグメントの作成

新しいファイルボリュームのサイズは 255G バイトに制限されます。これを超えるサイズのファイルボリュームを作成するには、最大 63 個のセグメントを一次ボリュームに追加します。255G バイトを超えるファイルボリュームを作成する場合は、1 つの一次ボリュームと、最大 63 個のセグメントを作成します。作成したセグメントを一次ボリュームに配置して、サイズを増やします。

ファイルボリュームまたはセグメントは、「Create File Volume」パネルまたは System Manager を使用して作成できます。

▼ 「Create File Volume」パネルを使用してファイルボリュームまたはセグメントを作成する

1. ナビゲーションパネルで、「File Volume Operations」>「Create File Volumes」を選択します。
2. 動作中のシステムに最近新しいディスクを追加して、まだ再起動を行なっていない場合は、「Scan For New Disks」ボタンをクリックします。
3. 「LUN」ボックスで、一次ファイルボリュームを作成する LUN をクリックします。

   「Partition」プルダウンメニュー内のファイルボリュームのパーティション番号は、ファイルボリュームを作成すると自動的に増分されます。
4. 「Name」フィールドに、新しいボリューム名またはセグメント名を入力します。

   有効な文字は、英数字 (a ～ z、A ～ Z、0 ～ 9) です。英字 (a ～ z、A ～ Z) から始まる 12 文字以内の名前を指定する必要があります。
5. プルダウンメニューをクリックして、ファイルボリュームのサイズの単位を選択します。単位は「MB」(M バイト) または「GB」(G バイト) のいずれかです。
6. ファイルボリュームのサイズを整数で入力します。

   使用可能な総容量が、このフィールドの直下に表示されています。
7. ファイルボリュームの種類 (「Primary」または「Segment」) を選択します。
8. Compliance Archiving Software がインストールされている場合に、規制適合対応のボリュームを作成するには、「Compliance」セクションで「Enable」をクリックします。次に、必要な規制適合の実施の種類を指定します。

- 「Mandatory Enforcement」(必須実施) を選択した場合、デフォルトの保持期間は永続的になります。この設定は、管理操作によって変更することができません。

注意 – いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

- 「Advisory Enforcement」(推奨実施) を選択した場合、デフォルトの保持期間は 0 日です。この設定は、管理操作によって変更できます。

注 – 保持期間の期限が切れる前に、保持期間の短縮および保持ファイルの削除を実行する場合は、承認されたホストからスーパーユーザーが行う必要があります。詳細は、220 ページの「承認されたホストの管理」を参照してください。

詳細は、132 ページの「Compliance Archiving Software」を参照してください。

9. 「Apply」をクリックして新しいファイルボリュームまたはセグメントを作成します。

▼ System Manager を使用してファイルボリュームまたはセグメントを作成する

1. ナビゲーションパネルで「System Manager」を右クリックします。
2. ポップアップメニューから「Create Volume」または「Create Segment」を選択して、目的のダイアログボックスを開きます。
3. 「LUN」ボックスで、一次ファイルボリュームを作成する LUN をクリックします。

   「Partition」ドロップダウンリスト内のファイルボリュームのパーティション番号は、ファイルボリュームを作成すると自動的に増分されます。
4. 「Name」フィールドに、新しいボリューム名またはセグメント名を入力します。

   有効な文字は、英数字 (a ～ z、A ～ Z、0 ～ 9) です。英字 (a ～ z、A ～ Z) から始まる 12 文字以内の名前を指定する必要があります。
5. プルダウンメニューをクリックして、ファイルボリュームのサイズの単位を選択します。単位は「MB」(M バイト) または「GB」(G バイト) のいずれかです。
6. ファイルボリュームのサイズを整数で入力します。

   使用可能な総容量が、このフィールドの直下に表示されています。
7. ファイルボリュームの種類 (「Primary」または「Segment」) を選択します。

8. **Compliance Archiving Software がインストールされている場合に、規制適合対応のボリュームを作成するには、「Compliance」セクションで「Enable」をクリックします。次に、必要な規制適合の実施の種類を指定します。**

   - 「Mandatory Enforcement」(必須実施) を選択した場合、デフォルトの保持期間は永続的になります。この設定は、管理操作によって変更することができません。

注意 – いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

   - 「Advisory Enforcement」(推奨実施) を選択した場合、デフォルトの保持期間は 0 日です。この設定は、管理操作によって変更できます。

注 – 保持期間の期限が切れる前に、保持期間の短縮および保持ファイルの削除を実行する場合は、承認されたホストからスーパーユーザーが行う必要があります。詳細は、220 ページの「承認されたホストの管理」を参照してください。

詳細は、132 ページの「Compliance Archiving Software」を参照してください。

9. **「Apply」をクリックして新しいファイルボリュームまたはセグメントを作成します。**

一次ファイルボリュームへのセグメントの配置

一次ファイルボリュームにセグメントを配置すると、ボリュームのサイズが大きくなります。セグメントはボリュームに永続的に関連付けられ、削除はできません。セグメントをボリュームに配置するには、事前にセグメントを作成しておく必要があります。詳細は、45 ページの「ファイルボリュームまたはセグメントの作成」を参照してください。

注 – 一次ファイルボリュームに配置したセグメントは、元に戻せません。

ファイルボリューム自体のサイズは 255G バイトに制限されていますが、どの LUN からも最大 63 個のセグメントをファイルボリュームに配置することができます。各セグメントは 8M ～ 255G バイトに指定できます。

セグメントは、「Attach Segments」パネルまたは System Manager を使用して配置できます。

注 – 必須実施の規制適合対応のボリュームは、削除できません。必須実施の規制適合対応のボリュームにセグメントを追加すると、そのセグメントが使用する領域は削除または再利用できなくなります。

▼ 「Attach Segments」パネルを使用してセグメントを配置する

1. 「File Volume Operations」>「Attach Segments」をクリックして、「Attach Segments」パネルを表示します。
2. 「Existing Volumes」ボックスから、対象のボリュームをクリックして選択します。
3. 「Available Segments」ボックスから、対象のセグメントをクリックして選択します。
4. 「Apply」をクリックして配置します。

▼ System Manager を使用してセグメントを配置する

1. ナビゲーションパネルで「System Manager」をクリックし、既存のボリュームを表示します。
2. 対象のファイルボリュームを右クリックしてポップアップメニューを表示し、「Attach Segments」を選択します。
3. 対象のセグメントをクリックして選択します。
   一度に配置できるセグメントは、1 つのみです。
4. 「Apply」をクリックして選択したセグメントを配置します。
5. 手順 3 ～ 4 を繰り返して、必要なセグメントを配置します。

LUN の再構築

LUN 内のいずれかのドライブに障害が発生すると、そのドライブの LED がオレンジ色に点灯して、新しいドライブとの交換が必要であることを示します。

注 – LUN の再構築は、Sun StorEdge 5310 NAS Gateway システムの構成には適用されません。

ホットスペアドライブを使用できる場合、障害の発生したドライブに関連付けられている RAID セットは、そのホットスペアを使用して再構築されます。再構築処理中は、再構築に関連するすべてのドライブの LED が緑色で点滅し、これらのドライブを取り外すことはできません。同様の再構築は、障害の発生したドライブの交換時に新しいドライブを RAID セット内に挿入し、ホットスペアがスタンバイモードに戻ったときにも実行されます。再構築が完了するには数時間かかる場合があります。

システムにホットスペアが指定されていない場合は、障害が発生したドライブを取り外し、同一またはそれより大きい容量の別のドライブと交換する必要があります。障害の発生したドライブの交換方法については、付録 D を参照してください。

障害が発生したドライブの交換後、RAID コントローラが自動的に LUN を再構築します。ディスク容量によって異なりますが、LUN の再構築には数時間かかる場合があります。LUN の再構築中、LUN ドライブの LED はオレンジ色に点滅します。

ファイルボリュームおよびセグメントの管理

ファイルシステムの管理には、次のような作業があります。

- 49 ページの「ファイルボリュームのプロパティーの編集」
- 51 ページの「ファイルボリュームの削除」
- 52 ページの「ボリュームパーティションの表示」

ファイルボリュームのプロパティーの編集

「Edit Properties」パネルを使用すると、ファイルボリュームのプロパティーを変更できます。

注 – 規制適合対応のボリュームが必須実施に設定されている場合は、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードを実行できません。

▼ ボリュームの名前変更、チェックポイントの使用可能への切り替え、割り当ての使用可能への切り替え、または規制適合プロパティーの編集を実行する

1. ナビゲーションパネルで、「File Volume Operations」>「Edit Properties」を選択します。

2. 「Volumes」リストから変更するボリュームの名前を選択します。

3. 「New Name」フィールドに、必要に応じてボリュームの新しい名前を入力します。

   有効な文字は、英数字 (a ～ z、A ～ Z、0 ～ 9) です。英字 (a ～ z、A ～ Z) から始まる 12 文字以内の名前を指定する必要があります。

4. このボリュームに対して、次のいずれかまたは両方のオプションを選択します。

オプション	説明
Enable Checkpoints	このチェックボックスを選択すると、ファイルボリュームのチェックポイントが作成されます。チェックポイントは、ファイルボリュームの作成時にデフォルトで使用可能に設定されています。
Enable Quotas	このチェックボックスを選択すると、選択したボリュームの割り当てが使用可能になります。割り当ては、ファイルボリュームの作成時にデフォルトで使用不可に設定されています。
Enable Attic	このチェックボックスを選択すると、各ボリュームのルートにある `.attic$` ディレクトリに、削除したファイルが一時的に保存されます。このオプションはデフォルトで使用可能に設定されています。 ビジー状態のファイルシステム上でまれに、削除処理が終了する前に `.attic$` ディレクトリがいっぱいになり、結果として空き領域が不足してパフォーマンスが低下することがあります。このような場合は、このチェックボックスの選択を解除して、`.attic$` ディレクトリを使用不可にすることをお勧めします。

5. ボリュームが規制適合対応である場合、規制適合対応のレベルに応じて「Compliance Archiving Software」セクションにいくつかのオプションが表示されます。

注意 – 必須実施の規制適合対象のボリュームの場合、デフォルトの保持期間は「永続的」です。推奨実施の規制適合対応のボリュームの場合、デフォルトの保持期間は 0 日です。デフォルトの保持期間に別の値を設定する場合は、ボリュームの使用を開始する前に新しい保持期間を指定する必要があります。

注意 – いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

詳細は、132 ページの「Compliance Archiving Software」を参照してください。

オプション	説明
Mandatory Enforcement	ボリュームが推奨実施の規制適合対応である場合、このオプションを選択して必須実施に変更できます。
Advisory Enforcement	ボリュームが必須実施の規制適合対応である場合は設定を変更できないため、このオプションは使用できません。
Permanent Retention	デフォルト。データを永続的に保持しない場合は、ボリュームを使用する前に「Retain for *nn* Days」オプションを選択する必要があります。 このオプションを選択すると、このボリュームのデータは永続的に保持されます。
Retain for *nn* Days	データの保持日数を指定するには、このオプションを選択してドロップダウンメニューを使用します。 ボリュームが推奨実施の規制適合対応である場合は、保持期間を短縮または延長することができます。 ボリュームが必須実施の規制適合対応である場合は、保持期間の延長のみが可能です。

6. 「Apply」をクリックして、変更内容を保存します。

ファイルボリュームの削除

ファイルの削除後でもボリュームの空き領域が変わらない場合、その原因はチェックポイント機能または attic の有効化機能である可能性があります。attic の有効化については、51 ページを参照してください。

チェックポイントは、定義された特定の時間内、削除および変更されたデータを格納することで、データの安全性を維持することを目的としたデータの回復を可能にします。これは、チェックポイントが期限切れにならないかぎり、データがディスクから削除されないことを意味します。有効期限は最大 2 週間ですが、手動チェックポイントによって時間が無期限に設定されている場合は例外です。

データを削除してディスク領域を解放する場合は、チェックポイントを削除するか、使用不可に切り替える必要があります。チェックポイントの削除方法については、166 ページの「チェックポイントを削除する」を参照してください。

注 – 必須実施の規制適合対応のボリュームは削除できません。また、オフラインのボリュームも削除できません。

▼ ファイルボリュームまたはセグメントを削除する

1. ナビゲーションパネルで、「File Volume Operations」>「Delete File Volumes」を選択します。
2. 削除するファイルボリュームまたはセグメントを選択します。
3. 「Apply」をクリックします。

ボリュームパーティションの表示

「View Volume Partitions」パネルには、Sun StorEdge 5310 NAS Appliance または Cluster 用に定義された LUN が読み取り専用で表示されます。

▼ ボリュームパーティションを表示する

1. ナビゲーションパネルで、「File Volume Operations」>「View Volume Partitions」を選択します。
2. 「Volumes」リストで、パーティションを表示するファイルボリュームを選択します。

   選択したボリュームに関する次の情報が表示されます。

フィールド	説明
LUN	選択したファイルボリュームのすべての LUN の一覧が示されます。
Partition	選択したファイルボリュームのパーティションが表示されます。
Use	パーティションの使用率が表示されます。
Type	パーティションタイプが sfs2 (一次) または sfs2ext (セグメント) のいずれかで表示されます。
Free	パーティションの未使用領域の容量が表示されます。
Capacity	パーティションの合計サイズが表示されます。
Requests	パーティションに対して処理された要求の合計数が表示されます。
Active	パーティションに対して未処理のアクティブな要求が表示されます。

iSCSI 構成

ホストアプリケーションから Sun StorEdge 5310 Appliance へのデータ移送に iSCSI (Internet Small Computer Systems Interface) プロトコルを使用するよう、システムを構成できます。iSCSI は、SCSI コマンド、データ、およびステータスを TCP/IP ネットワークを介して移送します。iSCSI を使用可能にすると、ホストアプリケーションはデータを Sun StorEdge 5310 Appliance に保存できるようになります。

iSCSI 環境での Sun StorEdge 5310 NAS Appliance は、iSCSI イニシエータクライアントの iSCSI ターゲットとして動作します。iSCSI イニシエータおよびターゲットは、それぞれ一意で永続的な識別子を持ちます。この iSCSI イニシエータ識別子は、ホストの iSCSI ソフトウェアによって生成されます。iSCSI ターゲットは、EUI (Enterprise Unique Identifier) および IQN (iSCSI Qualified Name) の両方の識別子をサポートします。

iSCSI ターゲットの構成

iSCSI ターゲットに接続してアクセスするように iSCSI ターゲットを構成するには、次の手順を実行する必要があります。

- iSCSI イニシエータクライアントの構成 (iSCSI イニシエータソフトウェアに付属のマニュアルを参照)
- ターゲットへのアクセスを iSCSI イニシエータに許可するためのアクセスリストの作成
- LUN の作成と、iSCSI イニシエータへの LUN アクセスの割り当て
- iSCSI ターゲットおよびイニシエータの検出方法の構成

Sun StorEdge 5310 NAS Appliance に実装されている iSCSI ターゲットは、IETF (Internet Engineering Task Force) が策定した iSCSI RFC 3720 に基づいています。サポートするプロトコルの機能には、ヘッダーのダイジェスト、イニシエータのチャレンジハンドシェーク認証プロトコル (CHAP)、エラー回復レベル 0 などがあります。

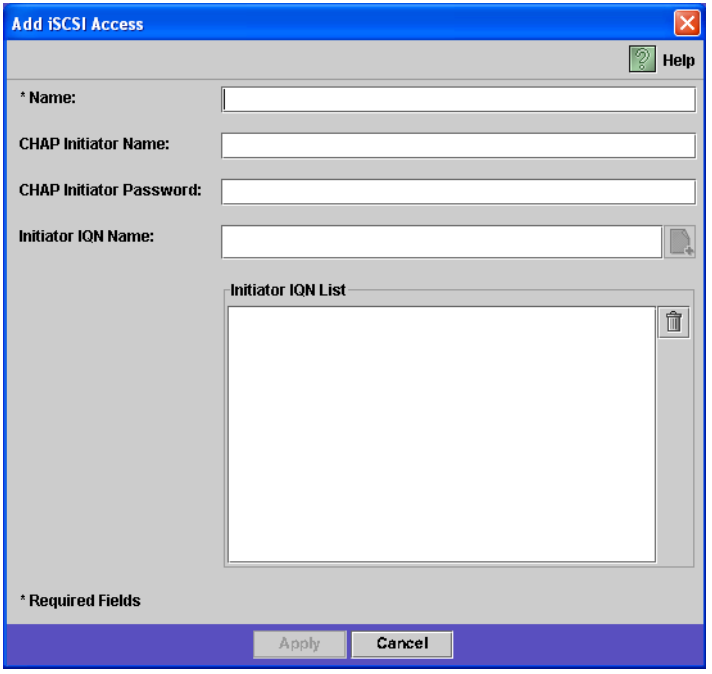
iSCSI イニシエータのアクセスの構成

iSCSI アクセスリストを作成することで、LUN にアクセスできる iSCSI イニシエータを定義できます。アクセスリストには、1 つ以上の iSCSI イニシエータ、および必要に応じて 1 つの CHAP イニシエータとパスワードを登録できます。CHAP を使用すると、承認された iSCSI イニシエータから送信されたデータであることが保証されます。

注意 – 複数の iSCSI イニシエータから同じ iSCSI ターゲット LUN にアクセスするように構成できます。ただし、iSCSI クライアントサーバー上で動作しているアプリケーション (クラスタまたはデータベース) で同期アクセスを実現して、データ破壊を回避する必要があります。

▼ iSCSI アクセスリストを作成する

1. ナビゲーションパネルで、「iSCSI Configuration」>「Configure Access List」を選択します。
2. アクセスリストを作成するには、「Add」をクリックします。
   「Add iSCSI LUN」ダイアログボックスが表示されます。



3. 次の情報を入力します。

フィールド	説明
Name	アクセスリストの名前を入力します。名前は 1 文字以上で、英数字 (a ～ z、A ～ Z、0 ～ 9)、ピリオド (.)、ハイフン (-)、またはコロン (:) を指定できます。たとえば、`iscsiwinxp` は有効なアクセスリスト名です。
CHAP Initiator Name	iSCSI イニシエータソフトウェアで構成されている CHAP イニシエータの完全な名前を入力します。Windows iSCSI クライアントのデフォルトの CHAP イニシエータ名の例を、次に示します。 `iqn.1991-05.com.microsoft:iscsi-winxp` このフィールドを空白にすると、CHAP 承認は不要になります。詳細は、iSCSI イニシエータのマニュアルを参照してください。
CHAP Initiator Password	CHAP イニシエータの名前を入力した場合は、CHAP イニシエータのパスワードを入力します。
Initiator IQN Name	イニシエータの IQN 名を入力し、「Add」ボタンをクリックしてイニシエータをリストに追加します。このフィールドを空白にすると、すべてのイニシエータがターゲットにアクセスできるようになります。 名前は 1 文字以上で、英数字 (a ～ z、A ～ Z、0 ～ 9)、ピリオド (.)、ハイフン (-)、またはコロン (:) を指定できます。 リストからイニシエータ IQN を削除するには、その名前を選択して「Trash」ボタンをクリックします。

4. 「Apply」をクリックして設定を保存します。

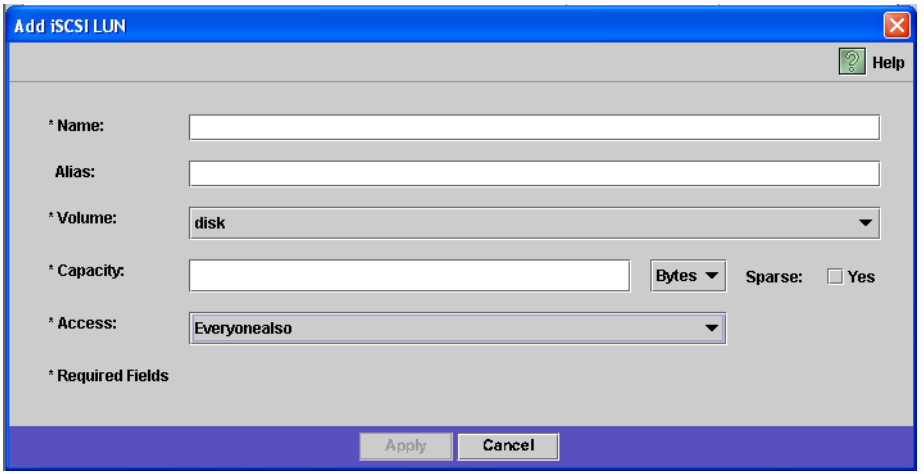
iSCSI アクセスリストを編集するには、iSCSI アクセスリスト名のいずれかをダブルクリックするか、またはアクセスリスト名を選択して「Edit」をクリックします。テキストフィールドを変更し、「Apply」をクリックして設定を保存します。

▼ iSCSI LUN を作成する

1. ナビゲーションパネルで、「iSCSI Configuration」>「Configure iSCSI LUN」を選択します。

2. iSCSI LUN をリストに追加するには、「Add」をクリックします。

「Add iSCSI LUN」ダイアログボックスが表示されます。



3. iSCSI LUN に関する次の情報を入力します。

フィールド	説明
Name	iSCSI LUN の名前を入力します。名前は 1 文字以上で、英数字 (a ～ z、A ～ Z、0 ～ 9)、ピリオド (.)、ハイフン (-)、またはコロン (:) を指定できます。 入力したターゲット名の前には、次に示す命名規則に従って、完全な IQN 名が付与されます。 `iqn.1986-03.com.sun:01:mac-address.timestamp.`*user-specified-name* たとえば、名前 `lun1` を入力する場合、iSCSI ターゲットの LUN の完全な名前は次のようになります。 `iqn.1986-03.com.sun:01:`*`mac-address.timestamp`*`.lun1` 注: timestamp は、1970 年 1 月 1 日以降の秒数を表す 16 進数です。
Alias	任意。ターゲットに関する簡単な説明を入力します。
Volume	iSCSI LUN を作成するボリュームの名前を選択します。

フィールド	説明
Capacity	LUN の最大サイズをバイト、K バイト、M バイト、または G バイト単位で指定します。
Sparse	スパース LUN を作成する場合は「Yes」チェックボックスを選択します。スパース LUN では、ファイルサイズ属性は指定された容量に設定されますが、ディスクブロックはデータがディスクに書き込まれるまで割り当てられません。詳細は、57 ページの「iSCSI のスパース LUN について」を参照してください。 スパースでない LUN を作成する場合は、作成する LUN の容量に基づいてディスクブロックが割り当てられます。スパースでない iSCSI LUN を作成するときは、ファイルシステムのメタデータ用にボリュームに約 10% の追加領域を用意します。たとえば、100G バイトの iSCSI LUN でスパースでない LUN を作成するには、110G バイトのボリュームに作成してください。 スパース LUN とスパースでない LUN のどちらを使用するかの決定方法の詳細は、57 ページの「iSCSI のスパース LUN について」を参照してください。
Access	ドロップダウンリストから、この LUN 用のアクセスリスト (事前に作成したもの) を選択します。

4. 「Apply」をクリックして設定を保存します。

iSCSI のスパース LUN について

一般に、十分なストレージを使用できる場合は、スパースでない LUN を使用することをお勧めします。

iSCSI のスパース LUN は、必ずしもすべての状況で便利であるとはかぎりません。スパース LUN を作成する場合、ディスク容量は使用するまで割り当てられません。スパース LUN は、容量を使い果たすことのない LUN をいくつか作成する予定である場合に便利です。たとえば、100G バイトの iSCSI LUN が 5 つあり、それぞれが容量の 55% のみを使用する予定である場合は、5*100*.55=275G バイトに予備として 50G バイトを追加した、325G バイトの容量を維持できるボリュームに、これらの LUN をすべて作成できます。

このモデルでは、実際のボリュームの使用量を監視し、容量が不足する前にボリュームに追加領域を割り当てることができます。iSCSI LUN が、利用可能な LUN サイズの大部分を使用する予定である場合は、スパース LUN オプションを使用しないでください。オペレーティング環境によってはスパース LUN の容量不足の状況が正常に処理されないため、システムの最適な動作を維持するには、容量不足を回避する必要があります。

iSCSI ターゲットの検出方法

次のいずれかの方法を使用して、iSCSI イニシエータが iSCSI ターゲットを検出する方法を構成できます。

- 静的構成 – iSCSI ターゲットの名前および IP アドレスを iSCSI イニシエータホストに手動で追加します。詳細は、iSCSI イニシエータソフトウェアに付属のマニュアルを参照してください。
- SendTargets 要求 – iSCSI ターゲットのポータルの IP アドレスまたは DNS 名を iSCSI イニシエータ構成に追加します。イニシエータは SendTargets 要求を発行して、指定されたターゲットポータルでアクセス可能な iSCSI ターゲットのリストを検出します。詳細は、iSCSI イニシエータソフトウェアに付属のマニュアルを参照してください。
- Internet Storage Name Service (iSNS) サーバー – iSNS サーバーを設定して、iSCSI イニシエータと iSCSI ターゲットの検出を自動化します。iSNS サーバーは、iSCSI イニシエータによる iSCSI ターゲットの存在、位置、および構成の検出を可能にします。iSNS クライアントはオプションの機能で、次の節で説明するように、Web Administrator の GUI を使用して構成できます。

iSNS サーバーの構成

iSNS サーバーを使用可能にするには、iSNS サーバーの IP アドレスまたはドメインネームサービス (DNS) 名を指定します。iSNS クライアントは、Microsoft iSNS Server 3.0 などの、任意の標準 iSNS サーバー実装とともに使用します。

詳細は、使用している iSNS サーバーのマニュアル、および iSCSI イニシエータのマニュアルを参照してください。

▼ iSNS サーバーを指定する

1. ナビゲーションパネルで、「iSCSI Configuration」>「Configure iSNS Server」を選択します。
2. iSNS サーバーの IP アドレスまたは DNS 名を入力し、「Apply」をクリックします。

   「iSNS Server」フィールドに別の IP アドレスまたは DNS 名を入力し、「Apply」をクリックして、iSNS サーバーの名前を変更することもできます。

次に実行する作業

この時点で、ファイルシステムと iSCSI ターゲットが設定され、使用する準備が整いました。次に、アクセス権限、割り当て、および必要なディレクトリ構造を設定する必要があります。これらの管理機能については、第 4 章以降を参照してください。

リソース管理に必要な監視機能については、第 10 章を参照してください。バックアップ、復元などの保守機能については、第 11 章を参照してください。

第4章

システムの管理

この章では、システム管理のいくつかの基本機能について説明します。これらの機能は、主にシステムの初期設定中にのみ使用されますが、必要に応じて、システムを再設定する場合にも使用できます。

システム管理機能には、次のものがあります。

管理者パスワードの設定

デフォルトでは、システム管理者のパスワードは設定されていません。必要に応じてパスワードを設定できます。

▼ 管理者パスワードを設定する

1. ナビゲーションパネルで、「System Operations」>「Set Administrator Password」を選択します。
2. 古いパスワードがある場合は、そのパスワードを「Old」パスワードフィールドに入力します。

   古いパスワードがない場合は、このフィールドを空白のままにします。
3. 新しいパスワードを「New」パスワードフィールドに入力します。

   パスワードは 1 ～ 21 文字で指定する必要があります。文字の種類には制限はありません。

4. 新しいパスワードをもう一度「Confirm」パスワードフィールドに入力します。

   パスワードを使用不可にするには、「New」パスワードフィールドおよび「Confirm」パスワードフィールドを空白のままにします。

5. 「Apply」をクリックして、変更内容を保存します。

日付および時刻の制御

ファイル管理を制御するには、システムの日付および時刻の制御が不可欠です。この節では、正確な日付および時刻の維持に使用できる機能について説明します。

時刻同期を使用するか、または時刻を手動で設定することができます。

注 – 日付および時刻をはじめて設定する際、システムの「固定クロック」も初期化されます。このクロックは、ライセンス管理ソフトウェアおよび Compliance Archiving Software で使用され、時間に依存する動作を制御します。

注意 – 固定クロックは一度初期化されると再設定できません。したがって、システムを構成する際は、日付および時刻を正確に設定してください。

時刻同期

システムは、時間情報プロトコル (NTP) および RDATE 時間プロトコルの 2 種類の時刻同期をサポートします。NTP サーバーまたは RDATE サーバーのいずれかの時刻と同期をとるように、システムを構成できます。

- NTP は、無線、衛星受信機、モデムなどの基準時刻にコンピュータの時計を同期化するインターネットプロトコルです。一般的な NTP 構成には、複数台の冗長サーバーおよび各種ネットワークパスが使用できるため、高い精度と信頼性を実現できます。
- RDATE 時間プロトコルは、サイトに影響を受けない日付および時刻を提供します。RDATE を使用すると、ネットワーク上の別のマシンから時刻を取得できます。通常、RDATE サーバーは UNIX システム上に存在し、システムの時刻を RDATE サーバーの時刻に同期化できます。

「手動同期」と呼ばれる 3 つめの方法では、時刻同期が使用不可になります。この方法では、システム管理者がシステムの時刻を設定するため、ネットワーク上のほかのノードとの同期化は行われません。

時刻同期の設定

「Set Up Time Synchronization」パネルで、いずれかの方法の時刻同期を設定できます。

▼ 時刻同期を設定する

1. ナビゲーションパネルで、「System Operations」>「Set Up Time Synchronization」を選択します。
2. 次の 3 つのオプションのいずれかを選択します。
   - Manual Synchronization − NTP または RDATE 時刻同期のどちらも使用しない場合は、このオプションを選択します。
   - NTP Synchronization − NTP 同期を使用し、ネットワーク上に 1 台以上の NTP サーバーがある場合は、このオプションボタンを選択して次の項目を入力します。
     - Enable Server 1 − NTP サーバーを使用可能にするには、「Enable Server 1」チェックボックスを選択し、対応するフィールドに情報を入力します。必要であれば、2 台めの NTP サーバーにも同じ操作を実行します。NTP サーバーは 2 台まで構成できます。
     - Enable Server 2 − 2 台めつまり代替の NTP サーバーを使用可能にするには、「Enable Server 2」チェックボックスを選択し、対応するフィールドに情報を入力します。NTP サーバーは 2 台まで構成できます。
     - NTP Server − システムがポーリングによって現在の時刻を取得する NTP サーバーの名前または IP アドレスを入力します。
     - Auth Type − システムは認証をサポートするため、鍵と鍵識別子を使用して、サーバーが認識および承認されていることを確認します。メッセージを認証するには、NTP サーバーとシステムとの間で鍵と鍵識別子を一致させる必要があります。使用する認証タイプとして「None」(認証構造を使用しない) または「Symmetric Key」のいずれかを選択します。
     - Key ID − 前述のフィールドで「Symmetric Key」を認証構造として選択した場合、この NTP サーバーの鍵識別子を入力します。この値の有効範囲は 1 ～ 65534 です。
     - Min Poll Rate − NTP メッセージの最小ポーリング間隔を入力します。この値が 2 乗されてポーリング間隔の最小秒数となります。たとえば 4 を入力すると、ポーリングイベントが 16 秒以上の間隔で発生します。このフィールドの有効範囲は 4 ～ 17 です。
     - Max Poll Rate − NTP メッセージの最大ポーリング間隔を入力します。この値が 2 乗されてポーリング間隔の最大秒数となります。たとえば 4 を入力すると、ポーリングイベントが 16 秒以下の間隔で発生します。このフィールドの有効範囲は 4 ～ 17 ですが、最小ポーリング間隔よりも大きい値に設定する必要があります。

- Enable Broadcast Client ー このチェックボックスを選択すると、すべてのインタフェースで受信されたサーバーのブロードキャストメッセージにシステムが応答するようになります。この機能は、サーバーとの時刻同期を必要とする多数のクライアントを持つ NTP サーバーが 1 台または数台存在する構成で使用します。
- Require Broadcast Server Authentication ー このチェックボックスを選択すると、システムにメッセージをブロードキャストしたサーバーが認識および承認されていることを NTP クライアントが確認します。

- RDATE Synchronization ー RDATE サーバーおよび許容範囲を設定するには、このチェックボックスを選択して次の項目を入力します。
  - RDATE Server ー RDATE サーバーの名前または IP アドレスを入力します。
  - Tolerance ー RDATE サーバーから受信する時刻の最大許容範囲を 0 ～ 3600 の範囲の秒数で入力します。システムの時刻と RDATE サーバーの時刻との誤差 (+ または -) がこの秒数より小さい場合は、システムの時刻が RDATE サーバーの時刻に同期化されます。誤差がこの秒数より大きい場合は、システムの時刻が RDATE サーバーの時刻に自動的に同期化されることはありません。このような誤差の確認は、毎日午後 11 時 45 分に実行されます。

3. 「Apply」をクリックして、変更内容を保存します。

日付および時刻の手動設定

時刻同期を使用しない場合は、日付と時刻を手動で設定できます。

▼ 日付と時刻を手動で設定する

1. ナビゲーションパネルで、「System Operations」>「Set Time and Date」を選択します。
2. カレンダの左上にあるプルダウンメニューから適切な年を選択します。
3. カレンダの右上にあるプルダウンメニューから適切な月を選択します。
4. カレンダ内の適切な日をクリックします。
5. 時計の左上にあるドロップダウンリストボックスから適切な時間を選択します。値の範囲は、0 ～ 23 (午前 0 時～午後 11 時) です。
6. 時計の右上にあるプルダウンメニューから適切な分 (0 ～ 59) を選択します。
7. 画面下部のプルダウンメニューから適切なタイムゾーンを選択します。

   適切なタイムゾーンを選択すると、システムで夏時間の設定が自動的に調整できるようになります。
8. 「Apply」をクリックして、日付および時刻の設定を保存します。

注 – システムに日付および時刻をはじめて設定する場合は、この手順によって固定クロックも同じ日付および時刻に設定されます。固定クロックは一度しか設定できないため、必ず日付および時刻を正確に設定してください。

ウイルス対策ソフトウェアの使用

ウイルス対策保護機能は、ネットワーク上にインストールした「スキャンエンジン」への Internet Content Adaptation Protocol (ICAP) 接続を介して利用できます。Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムでウイルス対策保護機能を使用可能にすると、システムはネットワーク上で使用しているウイルス対策エンジンのクライアントになります。

注 – システムでウイルスからの保護を構成する場合は、1 つ以上のスキャンエンジンを常に動作させておく必要があります。スキャンエンジンが動作していないと Windows クライアントからのアクセスが拒否される可能性があります。

▼ ウイルス対策保護機能を使用可能にする

1. ナビゲーションパネルで、「Configure Anti Virus」を選択します。
2. 「Enable Anti Virus」チェックボックスを選択します。

注 – ウイルス対策のスキャンを一時的に使用不可にする必要がある場合は、「Scanning Suspended」オプションを使用します。「Enable Anti Virus」チェックボックスの選択は解除しないでください。

3. スキャンモードを選択します。

スキャンモード	説明
Scanning Suspended	このオプションを選択すると、ウイルス対策保護機能が一時的に停止されます。 注: このオプションを選択した場合、ウイルス対策保護機能は無効になります。
Scan after Modify	このオプションを選択すると、ファイルの変更後にスキャンが実行されます。 このオプションは、パフォーマンスとウイルス保護の完全性の妥協点を提供するもので、読み取りアクセスは高速ですが、ウイルスからの保護は、ファイルが変更された時点でのみ最新のウイルス定義が適用された状態になります。その後、そのファイルにアクセスした時点では、ウイルス定義が変更された可能性が考慮されません。
Scan all Access	このオプションを選択すると、システムのどのようなアクセスのあとにもスキャンが実行されます。 このオプションでは、ウイルスからの保護がほぼ完全に実施され、最新のウイルス定義でスキャン済みのデータへのアクセスだけが許可されます。

4. 使用するスキャンエンジンの TCP/IP アドレスを指定します。
5. ICAP サーバーが接続を待機する TCP/IP のポート番号を指定します。通常はポート 1344 を使用します。
6. システムがスキャンエンジンに振り分ける、並行ファイルスキャン操作の最大数を指定します。通常は 2 を設定します。

7. 各スキャンの対象に含めるものと除外するものを、表示されたリストからそれぞれ選択して指定します。

指定	説明	形式
File Types Included	すべてを対象とする場合は、空白にします。対象を絞る場合は、スキャンの対象とする各ファイルタイプの拡張子を選択します。	3 文字以下。ワイルドカードマッチング用に ? を使用できます。
File Types Excluded	スキャンの対象外とする各ファイルタイプの拡張子を選択します。	3 文字以下。ワイルドカードマッチング用に ? を使用できます。
Exempt Clients	スキャンから除外する各クライアントの名前または IP アドレス。	
Exempt Groups	スキャンから除外する Windows/NT または Windows Active Directory の各グループ (UNIX グループ以外) の名前。	空白文字を含めることができます。
Exempt Shares	スキャンから除外する各共通インターネットファイルシステム (CIFS) 共有の名前。 注: 管理共有 (x$) は常にスキャンから除外されます。	

リストに新しい項目を追加するには、ボックスにその項目を入力して「Add」をクリックします。

リストから項目を削除するには、その項目を選択して「Remove」をクリックします。

8. 「Apply」をクリックして設定を保存します。

注 – すでにメモリ内に読み込まれているファイルは、スキャンの対象になりません。ウイルスのスキャンを完全に有効にするには、システムを再起動することをお勧めします。

ウイルスのスキャン

正常な動作中でも、ウイルスのスキャン時に (特に「Scan all Access」オプションが選択されている場合に)、CIFS クライアントで短い遅延が生じる場合があります。

ウイルスが検出されると、システムログに感染ファイルの名前、ウイルスの名前、および感染ファイルに対する処置を記録するエントリが追加されます。ほとんどの場合、処置は感染ファイルの「隔離」となり、その CIFS クライアントへのアクセスが拒否されるようになります。隔離ファイルは、感染ファイルが格納されているファイルシステムのルートの `/quarantine` ディレクトリで確認できます。`/quarantine`

ディレクトリ内での名前の衝突を避けるために、ファイルには「内部番号」に基づく名前が付けられます。*NNNNNN*.vir は感染ファイルへの「ハードリンク」で、*NNNNNN*.log は感染ファイルの元の名前と検出された感染の詳細が記載されたテキストファイルです。

注 – デフォルトでは、管理者 (または UNIX スーパーユーザー) のみが /quarantine ディレクトリの内容を参照できます。

感染 (隔離) ファイルから回復するもっとも簡単な方法は、そのファイルを削除することです。

▼ 隔離ファイルを削除する

1. **システムログまたは隔離ディレクトリの *NNNNNN*.log ファイルのいずれかでファイルの元の名前を確認し、まだ存在する場合はそのファイルを削除します。**
2. **隔離ディレクトリで感染ファイルに対応する *NNNNNN*.vir および *NNNNNN*.log の 2 つのファイルを探し、これらを削除します。**

第5章

システムポートの管理

この章では、ネットワークポートおよびエイリアス IP アドレスについて説明します。2 つ以上のポートを結合してポート結合を作成できます。ポート結合では、個々の構成ポートより広い帯域幅を利用できます。

この章の内容は、次のとおりです。

ポートの位置

Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムでは、ポートのタイプおよびサーバー上の物理的な位置と論理的な位置に基づいて、事前定義された順序でポートが識別されます。『Sun StorEdge 5310 NAS Appliance および Gateway システムご使用の手引き』を参照して、システムのポートの位置を確認してください。

各ポートには役割を割り当てる必要があります。割り当て可能な役割は、次のとおりです。

- Primary – このポートの役割は、アクティブなネットワークポートであることを示します。1 つ以上のポートに、一次ポートの役割を割り当てる必要があります。一次ポートは、フェイルオーバー処理が統合される部分です。ポートにこの役割を割り当てると、パートナーサーバー (サーバー H2) は、一次ポートに割り当てられた IP アドレスを、オフラインのバックアップ用エイリアス IP アドレスとして保持します。パートナーサーバーにエイリアス IP アドレスを指定すると、その逆の状態になります。パートナーサーバーの IP アドレスがバックアップ用エイリアス IP アドレスとして主サーバー (サーバー H1) に保持されます。フェイルオー

バーが発生すると、健全なサーバーはパートナーサーバーのエイリアス IP アドレスを使用可能にします。これによって、障害が発生したサーバーが依然として動作中であるかのように、ネットワークアクセスを継続できます。

注 – 各サーバーで、1 つ以上のポートに一次ポートの役割を割り当てる必要があります。

- Independent – このポートの役割は、バックアップなど、データの提供以外の目的に使用されるアクティブなネットワークポートであることを示します。Sun StorEdge 5310 Cluster システムでは、このポートはフェイルオーバー処理に組み込まれません。Independent ポートは、通常、遠隔バックアップに使用されます。Independent ポートを結合 (集約) したり、エイリアス IP アドレスをこのポートに追加したりすることはできません。この役割を割り当てるポートの数に制限はありませんが、1 台の本体に 1 つだけ割り当てることをお勧めします。
- Mirror – このポートの役割は、ファイルボリュームをミラー化するために、このサーバーをほかのサーバーに接続するポートであることを示します。ミラー化するソースサーバーおよびターゲットサーバーの両方で、同じポートを使用してください。ミラー化の詳細は、120 ページの「Sun StorEdge File Replicator」を参照してください。
- Private (Sun StorEdge 5310 Cluster のみ) – このポートは、もう 1 台の本体の状態を定期的に監視するハートビートの専用ポートに予約されています。

エイリアス IP アドレスの概要

IP エイリアス設定は、単一ポートに複数の IP アドレスを割り当てるネットワーク機能です。選択したポートに割り当てられたすべての IP エイリアスは、同一の物理ネットワーク上に存在し、選択したポートに最初に指定されたプライマリ IP アドレスと同一の「ネットマスク」および「ブロードキャストアドレス」を共有する必要があります。

サーバー (本体) 1 台構成のユーザーは、各ポートのプライマリ IP アドレスに最大 9 つのエイリアス IP アドレスを追加できます。そのため、2 つのポートを持つ単一のネットワークインタフェースカード (NIC) では、最大 20 個の IP アドレスを使用できます。

Sun StorEdge 5310 Cluster システムでは、IP エイリアス設定はフェイルオーバー処理に不可欠な要素です。本体 2 台構成のシステムでは、各ポートのプライマリ IP アドレスに、最大 4 つのエイリアス IP アドレスを追加できます。残り 5 つの IP エイリアスは、パートナーサーバーの一次ポートおよびミラーポートのプライマリ IP アドレスおよびエイリアス IP アドレスをバックアップするために予約されています。本体のフェイルオーバーが発生すると、健全なサーバーはこれらの予約済みのバック

アップ IP アドレスを使用可能にします。これによって、最小限の中断でネットワークアクセスを継続できます。本体のフェイルオーバーの詳細は、18 ページの「本体のフェイルオーバーの使用可能への切り替え」を参照してください。

サーバー 2 台構成のシステムでは、Primary の役割を割り当てられたポートにのみエイリアス IP アドレスを追加できます。ポートの役割のオプションについては、69 ページの「ポートの位置」を参照してください。

注 – Primary の役割と、プライマリ IP アドレスを混同しないでください。Primary の役割は、Sun StorEdge 5310 Cluster システムでポートがどのように機能するかを示す割り当てのことです。プライマリ IP アドレスは、選択したポートに割り当てられる最初のアドレスのことです。Web Administrator では、プライマリ IP アドレスは、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」パネルに表示されます。画面下部でポートの役割を選択できます。

ポート結合

ポート結合には、ポート集約結合および高可用性結合の 2 種類があります。ポート集約結合では、2 つ以上の隣接するポートを結合することで、以前よりも高速のポートや帯域幅の広いポートが作成されます。高可用性結合では、2 つ以上のポートを結合することで、NIC ポートのフェイルオーバーサービスまたはバックアップポートが提供されます。

注 – Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムは、802.3ad 仕様のサブセットである EtherChannel 結合をサポートしています。ポート結合を設定する前に、使用しているスイッチのマニュアルで EtherChannel 結合の詳細を確認してください。

システムでは、結合の種類にかかわらず、最大 4 つのポート結合を設定できます。各結合に設定できる最大ポート数は 6 つです。

ポート集約結合

ポート集約結合 (「チャネル結合」、「集約」、または「トランキング」とも呼ばれる) では、隣接するポートを結合してネットワーク入出力を拡大します。これによって、帯域幅の狭い 2 つ以上のチャネルから、帯域幅の広い単一ネットワークチャネルを形成できます。

集約結合には、2 つ以上の使用可能なポートが必要です。これらのポートのインタフェースタイプは、Fast Ethernet と Fast Ethernet のように、同じである必要があります。また、同一のサブネットに接続され、同一ネットワークスイッチの隣接するポートに接続されている必要もあります。

注 – チャネル結合用に構成されているポートに接続するスイッチは、IEEE 802.3ad のリンク集約をサポートしている必要があります。この機能の構成に関する詳細は、使用する LAN スイッチのマニュアルを参照してください。

高可用性結合

高可用性 (HA) ポート結合は、ポートのフェイルオーバー機能をシステムに提供します。2 つ以上の使用可能なポートが結合されているため、一次ポートに障害が発生した場合には、高可用性結合に含まれる二次ポートが自動的に作業を引き継ぎます。これによってサービスを中断せずに継続できます。

高可用性ポート結合には、2 つ以上の使用可能なポートが必要です。ただし、これらのポートのインタフェースカードタイプが同じである必要はありません。また、隣接するポートに接続されている必要もありません。

注 – 高可用性結合にはすべての種類のスイッチを使用できます。ただし、スイッチは同一のサブネットに接続されている必要があります。

サーバー 1 台構成のシステムのポート結合

この節では、サーバー 1 台構成のシステムでポートを結合する方法について説明します。

ポートは構成後に結合できます。ただし、エイリアス IP アドレスおよび元の構成の一部が変更される場合があります。ポート結合を作成したら、20 ページの「ネットワークポートの構成」に戻ってポート結合を構成します。2 つ以上のポートの結合後、個々のポートには IP エイリアスを追加できません。ポート結合にのみ IP エイリアスを追加できます。

▼ サーバー 1 台構成のシステムのポートを結合する

1. ナビゲーションパネルで、「Network Configuration」>「Bond NIC Ports」を選択します。
2. 「Create」をクリックします。

3. 「Port Aggregation」または「High Availability」をクリックして、作成する結合の種類を指定します。

4. 「Available NIC Ports」ボックスで、結合する使用可能なポートを 2 つ以上クリックして選択し、「>」をクリックして「NIC Ports in This Bond」リストに追加します。

   手順 3 で「Port Aggregation」を選択した場合、選択するポートのインタフェースタイプは同じである必要があります。また、隣接するポートに接続されているポートを選択する必要があります。

   このリストからポートを削除するには、該当するポートを選択して「<」をクリックします。

5. 「IP Address」、「Subnet Mask」、および「Broadcast Address」の各フィールドに必要な情報を入力します。

   デフォルトでは、これらのフィールドには「NIC Ports in This Bond」ボックスの最上位に表示される一次ポートの情報が設定されます。

6. 「Apply」をクリックして、ポート結合の処理を完了します。Web Administrator によって、自動再起動の確認を求めるプロンプトが表示されます。

   再起動後には、結合されたポートからすべてのエイリアス IP アドレスが削除されています。

   エイリアス IP アドレスをポート結合に追加する方法については、20 ページの「ネットワークアダプタを構成する」を参照してください。

Sun StorEdge 5310 Cluster システムのポート結合

本体 2 台構成のシステムでポートを結合する場合は、1 台のサーバーに対してのみ次の手順を実行する必要があります。1 つのポート結合に含まれるすべてのポートの種類は、Fast Ethernet と Fast Ethernet のように、同じである必要があります。また、同一のサブネットに接続され、同一のネットワークスイッチの隣接するポートに接続されている必要もあります。各ポートの結合後、システムはただちに自動的に再起動します。

ポートは構成後に結合できます。ただし、エイリアス IP アドレスおよび元の構成の一部が変更される場合があります。ポート結合を作成したら、20 ページの「ネットワークポートの構成」に戻ってポート結合を構成します。

サーバー 2 台構成のポート結合の詳細は、75 ページの「サーバー 2 台構成のポート結合例」を参照してください。

注 – ポート結合には、Primary の役割が割り当てられたポートのみを使用できます。ポートの役割の詳細は、69 ページの「ポートの位置」を参照してください。

▼ サーバー 2 台構成のシステムのポートを結合する

1. ナビゲーションパネルで、「Network Configuration」>「Bond NIC Ports」を選択します。
2. 「Create」をクリックします。
3. 「Available NIC Ports」リストから結合するポートを選択します。リストには、ポート結合に含まれていないすべてのポートが表示されます。

   ダイアログボックスには、リストの最初のポートの「IP Address」、「Subnet Mask」、および「Broadcast Address」フィールドが表示されます。
4. ポートを選択し、「>」をクリックして「NIC Ports in This Bond」リストにポートを追加します。

   このリストからポートを削除するには、目的のポートを選択して「<」をクリックします。

   2 つ以上のポートをリストに追加する必要があります。結合したすべてのポートは、同一のサブネット上にある必要があります。

   「Apply」をクリックしてサーバーを再起動すると、パートナーサーバーの対応するポートも自動的に結合されます。たとえば、サーバー H1 のポート 2 と 3 を結合すると、サーバー H2 のポート 2 と 3 も結合されます。
5. 「Apply」をクリックしてポート結合の処理を完了し、システムを再起動します。

   システムは自動的に Bond ID を新しいポート結合に割り当てます。ポート結合の IP アドレスは、結合に最初に追加されたポートのアドレスと同じです。
6. エイリアス IP アドレスをポート結合に追加する方法については、20 ページの「ネットワークアダプタを構成する」を参照してください。

   2 つ以上のポートの結合後、個々のポートには IP エイリアスを追加できません。ポート結合にのみ IP エイリアスを追加できます。

サーバー 2 台構成のポート結合例

図 5-1 に、2 つの異なるサブネットに接続された Sun StorEdge 5310 Cluster システムの例を示します。可能な組み合わせをすべて示すために、この例では、それぞれの本体が 1 つのハートビートポートと 4 つの追加ポートを備えています。各サーバーのハートビートポートを除くすべてのポートには、Primary の役割が設定されています。

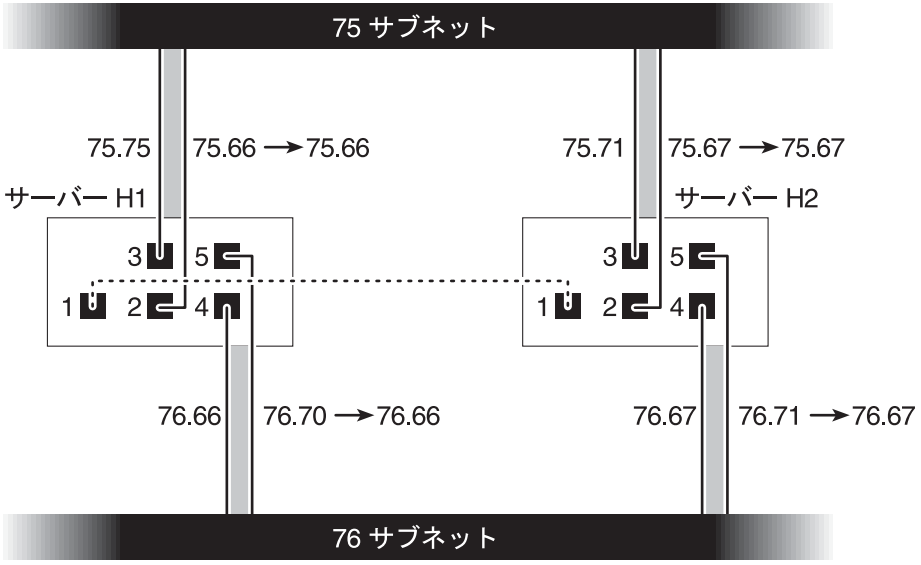


図 5-1　　サーバー 2 台構成のポート結合

ポート 2 とポート 3 を結合し、ポート 4 とポート 5 を結合した場合の IP 構成を、表 5-1 に示します。

表 5-1 サーバー 2 台構成のポート結合の例

本体	結合するポート		ポート結合		
	名前	プライマリ IP アドレス	名前	プライマリ IP アドレス	バックアップ IP アドレス
1	ポート 2	192.1xx.75.66	結合 1	192.1xx.75.66	192.1xx.75.67
	ポート 3	192.1xx.75.70			
	ポート 4	192.1xx.76.66	結合 2	192.1xx.76.66	192.1xx.76.67
	ポート 5	192.1xx.76.70			
2	ポート 2	192.1xx.75.67	結合 1	192.1xx.75.67	192.1xx.75.66
	ポート 3	192.1xx.75.71			
	ポート 4	192.1xx.76.67	結合 2	192.1xx.76.67	192.1xx.76.66
	ポート 5	192.1xx.76.71			

サーバー H1 の各ポートのプライマリ IP アドレスは、サーバー H2 の対応するポートのバックアップ IP アドレスです。また、その逆も同様です。

本体のフェイルオーバーが発生すると、正常なサーバーが障害の発生したサーバーの IP アドレスを使用可能にします。ポート結合のプライマリ IP アドレスには、エイリアス IP アドレスを追加できます。追加された IP アドレスはフェイルオーバー処理に組み込まれます。IP エイリアスの詳細は、70 ページの「エイリアス IP アドレスの概要」を参照してください。

第6章

Active Directory サービスおよび認証

この章では、Active Directory サービス (ADS) の詳細、LDAP (Lightweight Directory Access Protocol) の設定、およびネームサービスの検索順序の変更方法について説明します。その他のネームサービスの設定手順については、23 ページの「ネームサービス」を参照してください。

この章の内容は、次のとおりです。

サポートされているネームサービス

このシステムでは、Windows ネットワークおよび UNIX ネットワーク向けのさまざまなネームサービスをサポートします。これらのネームサービスを次に示します。

- ADS − Active Directory サービス (ADS) は、ドメインネームシステム (DNS) と統合された Windows 2000 のネームサービスです。DNS の詳細は、26 ページの「DNS の設定」を参照してください。ADS はドメインコントローラ上でのみ動作します。ADS は、データを格納および提供するほかに、許可されていないアクセスからネットワークオブジェクトを保護し、1 つのドメインコントローラに障害が発生した場合でもデータが失われないように、ネットワーク全体のオブジェクトを複製します。ADS を使用可能にして設定を行うと、システムは ADS の更新を自動的に実行するようになります。詳細は、78 ページの「Active Directory サービス」を参照してください。
- LDAP − LDAP (Lightweight Directory Access Protocol) は、認証を使用可能にする UNIX のサービスです。

- WINS − Windows インターネットネームサービス (WINS) サーバーは、ネットワーク上のコンピュータがほかの NetBIOS デバイスをすばやく効率的に検索できるように、NetBIOS 名を IP アドレスに解決します。WINS サーバーは、UNIX 環境の DNS サーバーと同様の機能を Windows 環境で実行します。詳細は、25 ページの「WINS の設定」を参照してください。
- DNS − ドメインネームシステム (DNS) は、ドメイン名をシステムの IP アドレスに解決します。このサービスを使用すると、サーバーの IP アドレスまたはサーバー名のいずれかでサーバーを識別できます。詳細は、26 ページの「DNS の設定」を参照してください。
- NIS − ネットワーク情報サービス (NIS) は、NIS データベースをインポートするようにシステムを構成します。NIS は、ユーザーグループやホスト情報に基づいてリソースへのアクセスを管理します。詳細は、27 ページの「NIS の設定」を参照してください。
- NIS+ − ネットワーク情報サービスプラス (NIS+) は、NIS に代わるサービスとして設計されました。NIS+ は NIS クライアントを部分的にサポートしていますが、NIS で解決できなかった問題に対処することを中心に設計されています。主に、NIS+ では資格情報の設定および NIS 機能への安全なアクセスが可能になりました。詳細は、28 ページの「NIS+ の設定」を参照してください。

Active Directory サービス

システムを Windows 2000 Active Directory 環境にシームレスに統合するために、ネットワーク上に必要なものを次に示します。

- Windows 2000 サーバーのドメインコントローラ
- Active Directory が統合された DNS サーバー。動的 DNS 機能を使用する場合には動的更新が可能なこのサーバーを使用することをお勧めしますが、ADS の使用には必要ありません。

ADS の設定後、特定の共有が ADS ディレクトリに公開されるように ADS を設定できます。これを実行するには、SMB 共有を作成または更新し、公開する各共有に対して共有コンテナを指定します。

ADS の設定では、次の作業を実行します。

1. ADS の使用可能への切り替え
2. ネームサービスの検索順序の確認
3. DNS が使用可能になっており、ADS をサポートするように構成されていることの確認
4. ADS での共有の公開

▼ ADS を使用可能にする

1. ナビゲーションパネルで、「System Operations」>「Set Time and Date」を選択します。
2. システムの時刻と ADS Windows 2000 ドメインコントローラの時刻の誤差が 5 分以内であることを確認します。
3. 「Apply」をクリックして、変更内容を保存します。

注 – 日付および時刻を再設定すると、時間に関連するほとんどの処理で使用されるシステムクロックが変更されます。ライセンス管理ソフトウェアおよび Compliance Archiving Software に使用される固定クロックは変更されません。

---

4. ナビゲーションパネルで、「Windows Configuration」>「Configure Domains and Workgroups」を選択します。
5. 「Enable ADS」チェックボックスを選択します。
6. 「Domain」に、ADS が動作している Windows 2000 ドメインを入力します。

   システムがこのドメインに属している必要があります。
7. 「User Name」フィールドに、管理権限を持つ Windows 2000 ユーザーの名前を入力します。

   このユーザーは、ドメイン管理者か、ドメイン管理者グループのメンバーである必要があります。ADS クライアントでは、このユーザーによるセキュリティー保護された ADS の更新が検証されます。

注 – このフィールドにドメイン管理者名を入力しても ADS の更新が行われない場合は、ドメインコントローラでドメイン管理者パスワードを変更する必要があります。パスワードの変更は、管理者ユーザーのみが行う必要があります。また、同じパスワードを再使用することもできます。詳細は、Microsoft のサポートサービスの Web サイトで「文書番号 Q248808」を参照してください。

---

8. 「Password」フィールドに、Windows 2000 管理者ユーザーのパスワードを入力します。

9. 「Container」フィールドに、LDAP (Lightweight Directory Access Protocol) の DN (識別名) 記法で Windows 2000 管理者ユーザーの ADS のパスを入力します。

   ユーザーなどのオブジェクトは、「コンテナ」オブジェクトの各レベルを示す階層的なパスの形式で、Active Directory ドメイン内に格納されます。ユーザーの cn (共通名) フォルダまたは ou (組織単位) フォルダの名前をパスとして入力します。

   たとえば、ユーザーが「accounting」という親フォルダ内の「users」フォルダに存在する場合は、次のように入力します。

   `ou=users,ou=accounting`

   パスには、ドメイン名を含めないでください。

10. ローカル ADS サイトの名前が ADS ドメインと異なる場合は、「Site」フィールドにローカル ADS サイトの名前を入力します。

    通常、このフィールドは空白のままです。

11. 「Kerberos Realm Info」セクションに、ADS の識別に使用されるレルム名を入力します。

12. 通常、これは ADS ドメインまたは DNS ドメインです。「Apply」をクリックすると、入力した値がすべて大文字に変換されます。

13. 「Server」フィールドに、Kerberos KDC サーバーのホスト名を入力します。

    通常、KDC サーバー名は ADS ドメインのメインドメインコントローラのホスト名です。システムが DNS を介して KDC サーバーを検索できる場合は、このフィールドは空白のままでかまいません。

14. 「Apply」をクリックして、変更内容を保存および適用します。

▼ ネームサービスの検索順序を確認する

1. 「UNIX Configuration」>「Configure Name Services」を選択します。
2. DNS のネームサービスの検索順序が使用可能になっており、優先順位が適切に設定されていることを確認します。

   a. 「Hosts Order」タブを選択します。右側のボックスの「Services Selected」リストに DNS サービスが表示されていることを確認します。表示されていない場合は、DNS サービスを選択して「>」ボタンをクリックします。

   b. 「Up」ボタンおよび「Down」ボタンを使用して、選択したサービスの走査順序を変更します。

3. 「Apply」をクリックして、変更内容を保存します。

▼ DNS 構成を確認する

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Set Up DNS」を選択します。
2. DNS が使用可能になっていない場合は、「Enable DNS」チェックボックスを選択します。
3. ドメイン名が入力されていない場合は、「DNS Domain Name」に DNS のドメイン名を入力します。

   この名前は ADS ドメインと一致する必要があります。
4. 「Server」フィールドにシステムで使用する DNS サーバーの IP アドレスを入力し、「Add」ボタンをクリックしてサーバーのアドレスを「DNS Server List」に追加します。

   このリストには、サーバーを 2 台まで追加できます。
5. 「Enable Dynamic DNS」チェックボックスを選択します。

   動的 DNS を使用可能にしない場合は、ホスト名および IP アドレスを手動で追加する必要があります。
6. 「DynDNS User Name」フィールドに、セキュリティー保護された動的 DNS の更新の実行に必要な管理権限を持つ Windows 2000 ユーザーの名前を入力します。

   DNS サーバーでセキュリティー保護されていない更新が許可されている場合は、このフィールドを空白のままにして保護されていない更新を実行できます。
7. 「DynDNS Password」フィールドに、動的 DNS ユーザーのパスワードを入力します。
8. 「Apply」をクリックして、変更内容を保存します。

   動的 DNS が使用可能になっている場合、システムはすぐに自身のホスト名および IP アドレスを使用して DNS を更新します。

▼ ADS で共有を公開する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 「Add」をクリックします。
3. 「Share Name」に共有の名前を入力します。
4. (任意) 共有についての説明を「Comment」に入力します。

   60 文字以内の英数字で入力できます。

5. プルダウンボックスから共有するボリュームを選択します。
6. (任意)「Directory」フィールドに、選択したボリューム上の、共有する既存ディレクトリを入力します。

注 – ディレクトリを指定しない場合は、ルートレベルの共有が作成されます。

---

7. 「Container」フィールドに、共有が公開される ADS ディレクトリ内の場所を入力します。

   「Container」フィールドによって、ADS コンテナが識別されます。共有を公開する ADS の場所を、LDAP の DN 記法で入力します。詳細は、80 ページの手順 9 を参照してください。

8. 「Apply」をクリックして、指定したコンテナに共有を追加します。

注 – コンテナ内で共有を公開するために指定したコンテナは、すでに存在している必要があります。システムによって ADS ツリーにコンテナオブジェクトが作成されることはありません。

▼ ADS 共有コンテナを更新する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 更新する共有を選択します。
3. 「Edit」をクリックして、「Edit Share」ダイアログボックスを表示します。
4. 新しい共有コンテナを入力します。
5. 「Apply」をクリックします。

   システムによって共有コンテナが更新されます。

▼ ADS から共有を削除する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. ADS から削除する共有を選択します。
3. 「Edit」をクリックして、「Edit Share」ダイアログボックスを表示します。

4. 「Container」フィールドから共有コンテナを削除します。
5. 「Apply」をクリックします。

LDAP の設定

LDAP を使用するには、LDAP サーバーが動作している必要があります。

▼ LDAP サービスを使用可能にする

1. ナビゲーションパネルで、「UNIX Configuration」>「Set Up NSSLDAP」を選択します。
2. LDAP を使用可能にするには、「Enable NSSLDAP」チェックボックスを選択します。
3. 「Domain」フィールドに、foo.com などの LDAP サーバーのドメイン名を入力します。
4. 「Password」フィールドに、LDAP サーバーで設定されたパスワードを入力します。
5. 「Server」フィールドに、LDAP サーバーの IP アドレスを入力します。
6. 「Proxy」フィールドに、サーバーの設定に応じて、プロキシドメインを入力します。
7. 「Apply」をクリックして設定を保存します。

ネームサービスの検索順序の変更

ネームサービス (NS) の検索順序によって、システムが照会を解決するためにネームサービスを検索する順序が制御されます。これらのネームサービスには、LDAP、NIS、NIS+、DNS、ローカルネームサービスなどがあります。名前解決にこれらのサービスを使用するには、選択したサービスを使用可能にする必要があります。

▼ ユーザー、グループ、ネットグループ、およびホストの検索順序を設定する

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure Name Services」を選択します。
2. 「Users Order」タブをクリックして、ユーザーの検索順序を選択します。
   a. 「Services Not Selected」ボックスからサービスを選択します。
   b. 「>」をクリックして、選択したサービスを「Services Selected」ボックスに移動します。
      ユーザーの検索からサービスを削除するには、サービスを選択して「<」をクリックします。
   c. 「Services Selected」ボックス内の検索サービスの順序を調整するには、各サービスを選択し、「Up」または「Down」ボタンをクリックして上下に移動します。
      リストの最上位にあるサービスが、ユーザーの検索で最初に使用されます。
3. 手順 2 の説明に従って、「Groups Order」タブをクリックしてグループの検索に使用するサービスを選択します。
4. 手順 2 の説明に従って、「Netgroup Order」タブをクリックしてネットグループの検索に使用するサービスを選択します。
5. 手順 2 の説明に従って、「Hosts Order」タブをクリックしてホストの検索に使用するサービスを選択します。
6. 「Apply」をクリックして、変更内容を保存します。

第7章

グループ、ホスト、およびファイルディレクトリのセキュリティー

この章では、ローカルグループ、ホスト、ユーザー、およびグループのマッピングと、ファイルディレクトリのセキュリティーに関するさまざまな設定について説明します。

Windows のセキュリティーの構成については、23 ページの「Windows のセキュリティーの構成」を参照してください。

この章の内容は、次のとおりです。

ローカルグループ

Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムの組み込みローカルグループの要件は、Windows システムのローカルグループの要件とは異なります。ユーザーは NAS 装置にローカルでログインすることはできません。すべてのユーザーはネットワークを介して接続し、ドメインコントローラを使用して認証されるため、ユーザーやゲストなどのローカルグループは必要ありません。

注 – ローカルグループは、CIFS ネットワークにのみ適用されます。

ローカルグループは、主に、リソースの管理およびバックアップ関連の操作の実行に使用します。ローカルグループは、管理者 (Administrators)、パワーユーザー (Power Users)、およびバックアップオペレータ (Backup Operators) の 3 つです。

- **管理者** (Administrators) ー このグループのメンバーは、システム上のすべてのファイルおよびディレクトリを管理できます。
- **パワーユーザー** (Power Users) ー このグループのメンバーには、システム上のファイルおよびディレクトリの所有権が割り当てられ、ファイルをバックアップおよび復元できます。
- **バックアップオペレータ** (Backup Operators) ー このグループのメンバーは、ファイルのセキュリティーを無視して、ファイルをバックアップおよび復元できます。

このシステムでは、認証済みユーザー (Authenticated Users) およびネットワーク (Network) という組み込みグループもサポートされています。すべてのログインユーザーは、自動的に、内部的に管理されるこれらの組み込みグループの両方のメンバーになります。有効な一次ユーザーまたは承認ドメインユーザーを、任意の組み込みローカルグループのメンバーとして追加できます。

ローカルグループの権限の構成

権限は、システム全体に作業の分担を割り当てるための安全なメカニズムを提供します。各権限には、システム管理者によってユーザーまたはグループに割り当てられる明確な役割が設定されています。Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムでは、ローカルのユーザーが存在しないため、権限はグループにのみ割り当てられます。

セキュリティー記述子を使用したオブジェクト単位の許可として割り当てられるアクセス権とは異なり、権限はオブジェクトには依存しません。権限は、オブジェクト単位のアクセス制御リストを無視して、権限の所有者に対して割り当てられた役割の実行を許可します。たとえば、バックアップオペレータグループのメンバーは、通常のセキュリティーチェックを無視して、通常はアクセス権のないファイルをバックアップおよび復元します。

アクセス権と権限との違いについて、次の定義を使用して説明します。

- アクセス権は、ユーザーまたはグループに対して明示的に付与または禁止されます。アクセス権は、オブジェクト単位で随意アクセス制御リスト (DACL) に許可として割り当てられます。
- 権限は、事前に定義された操作を実行する能力をグループのメンバーに暗黙的に付与する、システム全体での役割です。権限は、オブジェクトレベルのアクセス権より優先され、これを無視します。

表 7-1 に、サポートされる権限を示します。これらの権限のいずれかを任意の組み込みグループに割り当てることができます。任意のドメインユーザーを組み込みグループのメンバーにすることができるため、これらの権限を任意のドメインユーザーに割り当てることができます。

表 7-1　サポートされる権限

権限	説明
ファイルおよびディレクトリのバックアップ	ユーザーに対して、ターゲットのファイルおよびフォルダの読み取りアクセス権を必要とせずに、バックアップの実行を許可します。
ファイルおよびディレクトリの復元	ユーザーに対して、ターゲットのファイルおよびフォルダの書き込みアクセス権を必要とせずに、ファイルの復元を許可します。
ファイルおよびフォルダの所有	ユーザーに対して、所有アクセス権を必要とせずに、オブジェクトの所有を許可します。所有権は、所有者がオブジェクトに割り当てることのできる値にのみ設定できます。

表 7-2 に、ローカルの組み込みグループに割り当てられたデフォルトの権限を示します。ローカルの管理者グループのメンバーは任意のファイルまたはフォルダを所有でき、バックアップオペレータグループのメンバーはバックアップおよび復元操作を実行できます。

表 7-2　デフォルトのグループ権限

グループ	デフォルトの権限
管理者 (Administrators)	所有
バックアップオペレータ (Backup Operators)	バックアップおよび復元
パワーユーザー (Power Users)	なし

所有権の割り当て

デフォルトでは、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムがメンバーとして属するドメインの管理者グループは、ローカルの管理者グループのメンバーになっています。そのため、ドメイン管理者で構成されるドメインの管理者グループのメンバーがファイルやフォルダを作成または所有すると、所有権はローカルの管理者グループに割り当てられます。システムをドメイン間で移動させる場合、新しいドメインの管理者グループのメンバーはローカルの管理者グループが所有するオブジェクトにアクセスできるため、最大の移植性が保証されます。

前述の所有権の割り当て規則は、ローカルの管理者グループのメンバーである一般ユーザーにも適用されます。ローカルの管理者グループのメンバーがオブジェクトを作成または所有すると、そのメンバーではなくローカルの管理者グループに所有権が割り当てられます。

Windows システムでは、ドメイン管理者に割り当てられたローカルの管理者グループのメンバーシップが取り消されている場合があります。このような場合、ドメインの管理者グループのメンバーは、一般ユーザーとして扱われます。Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムでは、常にドメイン管理者にローカルの管理者グループのメンバーシップが割り当てられます。ただし、ドメイン管理者がこのグループのメンバーとして一覧に表示されることはないため、このメンバーシップを取り消すことはできません。ローカルユーザーが存在せず、ローカルの Windows 管理者が存在しないために、ドメインの管理者グループが Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムを管理する必要があります。

グループメンバーの追加および削除と権限の構成

「Configure Groups」パネルでは、3 つのローカルグループのいずれかに任意のドメインユーザーを追加できます。

▼ グループのメンバーを追加または削除する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Groups」を選択します。

   選択したグループの既存のメンバーが「Group Members」ボックスに表示されます。

2. グループを追加するには、次の手順に従います。

   a. 「Add Group」をクリックします。

   b. 「Group」フィールドにグループの名前を入力します。

   c. 「Comment」フィールドに、グループに関する説明またはコメントを入力します。

   d. 「Apply」をクリックして、変更内容を保存します。

3. グループを削除するには、次の手順に従います。

   a. 削除するグループを選択します。

   b. 「Remove Group」をクリックします。

   c. 「Apply」をクリックして、変更内容を保存します。

4. グループメンバーを追加または削除するには、次の手順に従います。

   a. メンバーを追加または削除するグループを強調表示します。

      選択したグループの既存のメンバーが「Group Members」ボックスに表示されます。

b. 「Group Members」ボックスで、追加または削除するメンバーを強調表示して、「Add」または「Delete」アイコンをクリックします。

c. 「Apply」をクリックして、変更内容を保存します。

権限の構成

管理者は、「Configure Privileges」パネルを使用してグループの権限の表示、付与、および取り消しを実行できます。

▼ NT 権限を構成する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Groups」を選択します。
2. 「Groups」ボックスで、権限を割り当てるグループを選択します。

ホストの構成

「Set Up Hosts」パネルでは、システムホストファイルのエントリを追加、編集、または削除できます。ホスト名、ホストの IP アドレス、ホストが承認されているかどうかなど、ホストの最新情報が表形式で表示されます。

注意 – ホストに承認 (Trusted) の状態を割り当てる場合には注意が必要です。承認されたホストはファイルシステムにスーパーユーザーでアクセスできるため、そのファイルシステム内のすべてのファイルおよびディレクトリに対して読み取りおよび書き込みアクセスが可能です。

ホストの追加および編集

「Set Up Hosts」パネルでは、ホスト情報を参照および編集して、ホストを承認するかどうかを指定できます。NFS クライアントが「承認されたホスト」として定義されており、ファイルへのアクセス権に関係なくすべてのファイルにアクセスできる場合、そのクライアントのスーパーユーザーには、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムに対するスーパーユーザー権限が付与されます。

▼ ホストを手動で追加する

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Set Up Hosts」を選択します。
2. 「Add」をクリックします。
3. 「Host Name」にホスト名を入力します。

   これは、システム上でホストが認識される名前です。ホスト名には、英数字 (a ～ z、A ～ Z、0 ～ 9)、「-」(ダッシュ)、および「.」(ピリオド) のみを指定できます。先頭の文字は、英字 (a ～ z または A ～ Z のみ) にする必要があります。
4. 新しいホストの IP アドレスを入力します。
5. 必要に応じて、「Trusted」チェックボックスを選択して、ホストに承認 (Trusted) の状態を割り当てます。

   承認されたホストは、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムにスーパーユーザーでアクセスできます。
6. 「Apply」をクリックして、変更内容を保存します。

▼ ホスト情報を編集する

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Set Up Hosts」を選択します。
2. 情報を編集するホストを選択して、「Edit」をクリックします。
3. 必要に応じて次の情報を変更します。
   - Host Name ー システム上でホストが認識される名前です。英字の大文字または小文字、数字、ピリオド (.)、またはハイフン (-) のみを使用します。先頭の文字は、英字にする必要があります。
   - IP Address ー ホストの IP アドレスです。
   - Trusted ー ホストに承認された状態を割り当てるために選択するチェックボックスです。ホストに承認された状態を割り当てる場合には注意が必要です。
4. 「Apply」をクリックして、変更内容を保存します。

▼ 特定のホストのホストマッピングを削除する

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Set Up Hosts」を選択します。
2. ホストのリストでエントリをクリックして、削除するホストを選択します。
3. 「Remove」をクリックします。
4. 「Apply」をクリックします。

ユーザーおよびグループの資格のマッピング

Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムサーバーは、マルチプロトコル環境に存在し、Windows システムと UNIX システムとの間でデータを共有するための統合モデルを提供するように設計されています。Windows システムと UNIX システムの両方からのファイルへの同時アクセスは可能ですが、Windows 環境と UNIX 環境の両方に存在するユーザーを定義するための業界標準のメカニズムは存在しません。いずれかの環境を使用してオブジェクトを作成できますが、それぞれの環境ではアクセス制御の意味に大きな違いがあります。この節では、資格のマッピングについて説明します。ユーザーまたはグループの資格のマッピングと、システム内のセキュリティー保護可能なオブジェクトとの間の相互作用の詳細は、218 ページの「マッピングおよびセキュリティー保護が可能なオブジェクト」を参照してください。

資格のマッピングでは、ローカルの構成ファイルまたは NIS データベースで定義された UNIX のユーザーまたはグループと、Windows SAM データベースで定義された Windows ドメインのユーザーまたはグループとの間に、対応関係が確立されます。ユーザーおよびグループのマッピングは、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システム上に資格の対応関係を確立し、いずれかの環境を使用した共通のアクセスを提供するためのメカニズムです。

UNIX のユーザーおよびグループ

UNIX のユーザーおよびグループは、ローカルの構成ファイル (passwd および group) または NIS データベースで定義されています。各ユーザーおよびグループは、それぞれ UID または GID と呼ばれる 32 ビットの識別子を使用して識別されます。ほとんどの UNIX システムでは 16 ビットの識別子を使用しますが、16 ビットの数値範囲による制限をなくすため、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムでは 32 ビットに拡張されています。UID または GID は、1 つの UNIX ドメイン内のユーザーまたはグループを一意に識別しますが、複数のドメインにわたって一意性を提供するメカニズムはありません。通常、値 0 はスーパーユーザーまたはスーパーユーザーグループに適用されます。スーパーユーザーには、管理作業を実行するために、ほぼ無制限のアクセス権が付与されます。

Windows のユーザーおよびグループ

Windows ユーザーおよびグループは、セキュリティーアカウントマネージャー (SAM) データベースで定義されています。各ユーザーおよびグループは、セキュリティー識別子 (SID) で識別されます。SID は可変長の構造を持ち、ローカルドメイン内でも、存在する可能性のあるすべての Windows ドメイン全体でも、ユーザーまたはグループを一意に識別します。

SID の形式は、次のとおりです。

```
typedef struct _SID_IDENTIFIER_AUTHORITY {
    BYTE Value[6];
} SID_IDENTIFIER_AUTHORITY;
typedef struct _SID {
    BYTE Revision;
    BYTE SubAuthorityCount;
    SID_IDENTIFIER_AUTHORITY IdentifierAuthority;
    DWORD SubAuthority[ANYSIZE_ARRAY];
} SID;
```

SID 構造内のフィールドは、表 7-3 に示すように解釈できます。

表 7-3 SID 内のフィールド

フィールド	値
Revision	SID のバージョン。現在のバージョン値は 1 です。
SubAuthorityCount	SID 内の副権限のエントリの数。1 つの SID には、副権限のエントリを最大 15 個含めることができます。
IdentifierAuthority	SID の発行元サブシステムを識別する 6 バイトの配列。
SubAuthority	適切なセキュリティーオブジェクト (ドメイン、ユーザー、グループ、またはエイリアス) を一意に識別する、副権限の 32 ビットの配列。ドメイン SID は、すべての権限ドメインの中でドメインを一意に識別します。ユーザー、グループ、またはエイリアスの SID は、適切な相対識別子 (RID) が追加されたドメイン SID です。RID は、32 ビットの識別子で、UNIX の UID または GID に類似しています。

わかりやすくするために、SID は、通常、S-1–5-32-500 という形式の文字列として表されます。この SID には、バージョン番号として 1、識別子発行元として 5、副権限として 32 および 500 の 2 つの値が含まれています。値 500 は RID です。

すべての Windows ドメインは一意の SID を持ち、すべての Windows ワークステーションおよび Windows サーバーは、ホスト名と同じ名前のローカルドメインです。したがって、すべての Windows ワークステーションおよび Windows サーバーは一

意の SID を持ちます。複数のマシンにまたがる Windows ドメインは、プライマリドメインコントローラ (PDC) から管理します。PDC は、ドメインのユーザーおよびグループを一元管理する機能を提供し、ドメイン全体に対して一意の SID を定義します。したがって、ユーザー SID のドメインの部分によって、ドメインのユーザーとローカルのワークステーションユーザーとを区別することができます。

Windows ドメインモデルと統合するために、各 Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムでも、そのローカルドメインを定義する SID が生成されます。この SID は 4 つの副権限を作成するアルゴリズムを使用して生成されます。最初の副権限の値は 4 で、一意ではない権限を表します。ほかの 3 つの副権限は、一意性を確実に実現するために、現在の時刻とシステムのいずれかの MAC3 アドレスを含めるアルゴリズムによって生成されます。このドメイン SID に UNIX の UID または GID を追加することによって、この SID は、ローカルユーザーおよび NIS ユーザーの両方を表すために使用されるようになります。この SID は、ローカル SAM データベースと同等のデータベースに保存されます。

資格のマッピング

ユーザーおよびグループのマッピングを定義すると、ユーザーは、UNIX システムと Windows システムのどちらからも自身のファイルに確実にアクセスできるようになります。この節では、ユーザーおよびグループのマッピングの自動生成に使用されるアルゴリズム、およびログイン処理中に適用されるポリシーについて説明します。UNIX のユーザーおよびグループを Windows のユーザーおよびグループにマッピングする際のマッピング規則は、システムポリシー設定を介して指定され、具体的なマッピングは、システムポリシーデータベースに格納されます。

各ユーザーマッピングは、特定の UID を持つ UNIX ユーザーを、特定の RID を持つ特定のドメイン内の Windows ユーザーに割り当てる方法を示します。同様に、各グループマッピングは、特定の GID を持つ UNIX グループを、特定の RID を持つ特定のドメイン内の Windows グループに割り当てる方法を示します。

マッピングの形式は、次のとおりです。

```
<UNIX-username>:<UID>:<Windows-username>:<NTDOMAIN>:<RID>
```

```
<UNIX-groupname>:<GID>:<Windows-groupname>:<NTDOMAIN>:<RID>
```

ローカルユーザーおよびローカルグループは、ローカルの `passwd` および `group` ファイルに定義されています。これらのファイルは、次に示すように、標準の UNIX 形式で定義されます。

```
<username>:<password>:<UID>:<GID>:<comment>:<home directory>:<shell>
```

```
<groupname>:<password>:<GID>:<comma-separated-list-of-usernames>
```

ユーザーマッピング

ユーザーマッピングは、UNIX ユーザーと Windows ユーザーとの間に対応関係を作成するために使用され、この関係では両方の資格セットがシステムで同等の権限を持つとみなされます。このマッピングメカニズムでは完全に双方向のマッピングがサポートされていますが、システムへの NFS アクセスに関して UNIX ユーザーを Windows ユーザーにマッピングする必要はありません。これは、UNIX ドメインを基本のマッピングドメインとして使用するというポリシー決定があるためです。

Windows ユーザーがシステムにログインするたびに、マッピングファイルが確認されて、そのユーザーの UNIX での資格が決定されます。Windows ユーザーの UNIX UID を確認するために、ユーザーマップが確認され、そのユーザーの Windows ドメイン名および Windows ユーザー名に一致するものが検索されます。一致するものが見つかると、一致したエントリから UNIX UID が取得されます。一致するものがない場合、そのユーザーの UNIX UID は、ユーザーマッピングポリシーの設定に従って決定されます。

ユーザーマッピングポリシーの設定

ユーザーマッピングポリシーには、次に示す 4 つの設定があります。

- `MAP_NONE` は、Windows ユーザーと UNIX ユーザーの間に事前定義されたマッピングがないことを示します。新しい一意の UNIX UID が Windows ユーザーに割り当てられます。現在構成されている passwd データベースおよびユーザーマップファイルを検索して新しい UID を選択するため、この UID の一意性は検証済みです。通常、新しい UID には、検索で見つかった最大値よりも 1 つ大きい値が使用されます。passwd データベースが、ローカルの NAS passwd ファイルおよび NIS passwd ファイル (NIS が使用可能な場合) を含む場合があります。この場合、Windows ユーザーを既存の UNIX ユーザーにマッピングするには、マッピングエントリを手動で変更する必要があります。
- `MAP_ID` は、Windows ユーザーの RID が UNIX UID になることを示します。`passwd` データベースは検索されません。
- `MAP_USERNAME` は、Windows ユーザーのユーザー名を `passwd` データベースで検索することを示します。Windows ユーザー名と UNIX ユーザー名が一致する場合、一致したエントリから UNIX UID が取得されます。一致しない場合は、`MAP_NONE` で説明したメカニズムに従って、一意の UNIX UID が生成されます。
- `MAP_FULLNAME` は、Windows ユーザーの Windows フルネームを passwd データベースで検索することを示します。各パスワードエントリの UNIX コメントのフィールドを使用して一致するものを検索します。passwd データベースのコメントフィールドのフルネームのエントリだけが、Windows フルネームと比較されます。一致するものが見つかると、一致したエントリの UNIX UID が使用されます。一致しない場合は、`MAP_NONE` メカニズムと同様に、一意の UNIX UID が生成されます。

Windows ユーザーの適切なグループの資格は、グループマッピングのアルゴリズムを使用して取得されます。詳細は、95 ページの「グループマッピング」を参照してください。

ユーザーマッピングポリシーの例

次の例は、Windows ユーザー HOMEBASE\johnm を UNIX ユーザー john に対応付け、Windows ユーザー HOMEBASE\alanw を UNIX ユーザー amw に対応付けるユーザーマップです。

```
john:638:johnm:HOMEBASE:1031
amw:735:alanw:HOMEBASE:1001
```

グループマッピング

グループマッピングは、UNIX グループと Windows グループとの間に対応関係を作成するために使用されます。Windows ユーザーに対する適切な UNIX GID を決定するには、グループマップでユーザーの Windows ドメイン名と Windows プライマリグループ名を検索します。一致するものが見つかると、そのマップエントリによって Windows ユーザーのグループが割り当てられる UNIX GID が定義されます。グループマップ内に一致するものがない場合、グループマップポリシーの設定に従って UNIX GID が決定され、グループマップに新しいエントリが作成されます。ただし、`MAP_UNIXGID` ポリシーは例外です。

グループマッピングポリシーの設定

グループマッピングポリシーには、次に示す 4 つの設定があります。

- `MAP_NONE` は、Windows グループと UNIX グループの間に事前設定されたマッピングがないことを示します。新しい一意の UNIX GID がグループに割り当てられます。現在構成されている group データベースおよびグループマップファイルを検索して、見つかった最大値よりも 1 つ大きい値である GID を選択するため、この GID の一意性は検証済みです。group データベースが、ローカルの NAS グループファイルおよび NIS グループファイル (NIS が使用可能な場合) から構成される場合があります。この場合、Windows グループを既存の UNIX グループにマッピングするには、マッピングエントリを手動で変更する必要があります。
- `MAP_ID` は、ユーザーのアクセストークンで検出された Windows ユーザーのグループ RID が UNIX GID になることを示します。
- `MAP_GROUPNAME` は、Windows ユーザーのグループ名を group データベースで検索することを示します。一致するものが見つかると、一致したエントリから UNIX GID が取得されます。一致しない場合は、一意の UNIX GID が生成されます。

- MAP_UNIXGID は、Windows ユーザーの UNIX グループが、ユーザーマッピング操作中に取得された passwd エントリの一次 GID フィールドで決定されることを示します。

  この場合、group.map ファイルは照会されません。GID を決定できない場合は、UNIX の nobody グループ GID (60001) が使用されます。

最後の手順は、ユーザーが所属する UNIX グループのリストを決定することです。ユーザーマッピング処理の場合と同様に、group データベースで UNIX ユーザー名が検索されます。その UNIX ユーザー名が含まれている各グループの GID が、グループリストのそのユーザーの資格内に追加されます。

グループマッピングポリシーの例

次の例は、HOMEBASE\Domain Admins グループを UNIX の wheel グループに対応付け、HOMEBASE\Domain Users グループを UNIX の users グループに対応付けるグループマップです。

```
wheel:800:Domain Admins:HOMEBASE:1005
users:100:Domain Users:HOMEBASE:513
```

システムのデフォルトのマッピング規則は、ユーザーとグループのどちらに対しても MAP_NONE です。

```
map.users=MAP_NONE
map.groups=MAP_NONE
```

ユーザーマッピング規則とグループマッピング規則を同一にする必要はありません。実際に使用される可能性のあるマッピング構成の例を、次に示します。この例のユーザーマッピング規則は MAP_USERNAME で、グループマッピング規則は MAP_ID です。

```
map.users=MAP_USERNAME
map.groups=MAP_ID
```

組み込みの資格のマッピング

UNIX のスーパーユーザー識別子の 0 (UID または GID) は、常にローカルの管理者グループにマップされます。ローカルの管理者グループの SID は、S-1-5-32-544 という組み込み (定義済み) の Windows SID です。このマッピングは、ドメイン管理者が作成したファイルに対して Windows が割り当てる所有権に一致しています。このようなファイルの所有権は、常に組み込みのローカルの管理者グループに割り当てられるため、ドメインの独立性が保たれます。つまり、システムが Windows ドメイン間で移動された場合でも、これらのファイルにアクセスできなくなることを防ぎます。

この SID は、Windows の権限表示ボックスには HOSTNAME\Administrators と表示されます。HOSTNAME は、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムのホスト名になります。

▼ マッピングポリシーを定義する

1. ナビゲーションパネルで、「Windows Configuration」>「Manage SMB/CIFS Mapping」>「Configure Mapping Policy」を選択します。
2. 「Windows <--> UNIX User Mapping Choice」セクションで、次に示すユーザーマッピング設定のいずれかを選択します。
   - Default Mapping − Windows ユーザーと UNIX ユーザーの間に事前定義されたマッピング規則が存在しない場合には、このオプションを選択します。新しいユーザーには、システムによって新しく生成された一意の ID が割り当てられます。
   - Map by User Name − システムが同一のユーザー名を持つ UNIX ユーザーと Windows ユーザーをマッピングし、同じユーザーが両方の環境から Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムにアクセスできるようにするには、このオプションを選択します。
   - Map by Full Name − 同一のフルネームを持つ UNIX ユーザーと Windows ユーザーをマッピングするには、このオプションを選択します。
3. 「Windows <--> UNIX Group Mapping Choice」セクションで、次に示すグループマッピングの設定のいずれかを選択します。
   - Default Mapping − Windows グループと UNIX グループの間に事前定義されたマッピング規則が存在しない場合には、このオプションを選択します。新しいグループには、システムによって新しく生成された一意の ID が割り当てられます。
   - Map by Group Name − 同一のグループ名を持つ UNIX グループと Windows グループをマッピングするには、このオプションを選択します。
   - Map to Primary Group − 構成済みの `passwd` ファイルのプライマリグループフィールドの NFS グループにマッピングするには、このオプションを選択します。
4. 「Apply」をクリックして、変更内容を保存します。

ユーザーまたはグループの資格のマッピングと、システム内のセキュリティー保護可能なオブジェクトとの間の相互作用の詳細は、218 ページの「マッピングおよびセキュリティー保護が可能なオブジェクト」を参照してください。

▼ Windows のグループおよびユーザーを UNIX のグループおよびユーザーにマッピングする

1. ナビゲーションパネルで、「Windows Configuration」>「Manage SMB/CIFS Mapping」>「Configure Maps」を選択します。
2. 「Add」をクリックします。
3. 「NT User」ボックスで、次の情報を入力します。
   - Account − マッピングするユーザーまたはグループの NT アカウント名を入力します。
   - RID − NT ドメイン内で NT ユーザーまたはグループを一意に識別する相対識別子を入力します。
4. 「UNIX User」ボックスで、次の情報を入力します。
   - Name − 指定した NT ユーザーまたはグループをマッピングする UNIX ユーザーまたはグループの名前を入力します。
   - ID − UNIX ドメイン内で UNIX ユーザーまたはグループを一意に識別する識別子を入力します。
5. 「Apply」をクリックして、変更内容を保存します。

ユーザーまたはグループの資格のマッピングと、システム内のセキュリティー保護可能なオブジェクトとの間の相互作用の詳細は、218 ページの「マッピングおよびセキュリティー保護が可能なオブジェクト」を参照してください。

ファイルディレクトリのセキュリティーの設定

ファイルディレクトリのセキュリティーを設定するには、次の 2 つの方法があります。

- 99 ページの「ワークグループモードでのファイルディレクトリのセキュリティーの設定」
- 99 ページの「ドメインモードでのファイルディレクトリのセキュリティーの設定」

ワークグループモードでのファイルディレクトリのセキュリティーの設定

ワークグループ/セキュリティー保護された共有モードでは、Web Administrator を使用してすべてのセキュリティーが共有自体に設定されます。これは、共有レベルセキュリティーと呼ばれます。

ワークグループモードでは、システムはクライアント上で認証が実行されないことを前提として、共有接続が要求されるたびに、パスワードを使用したアクセス権の確認を明示的に求めます。

共有を追加する際の共有レベルセキュリティーの設定については、103 ページの「新しい SMB 共有を追加する」を参照してください。共有を編集する際の共有レベルセキュリティーの設定については、105 ページの「既存の SMB 共有を編集する」を参照してください。

ドメインモードでのファイルディレクトリのセキュリティーの設定

Windows 2000 または Windows XP からのアクセス権のみを管理できます。

注 – システムがドメインモードで構成されている場合、オブジェクトアクセス権の設定は、標準の Windows ドメインコントローラでのオブジェクトアクセス権と同様に処理されます。サーバーを検索してドライブを割り当てて、共有のアクセス権を設定および管理するには、適切な方法がいくつかあります。ここでは、この処理の一例を示します。

注 – Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムは、ファイルおよびディレクトリのセキュリティーのみをサポートしており、共有にセキュリティーを設定すると、配下のディレクトリにそのセキュリティーの割り当てが渡されます。

▼ セキュリティーを設定する

1. Windows エクスプローラを起動します。
2. 「ツール」>「ネットワークドライブの割り当て」をクリックします。
3. 「ネットワークドライブの割り当て」ダイアログボックスで、「ドライブ」プルダウンメニューからドライブ文字を選択します。

4. Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムを検索して選択します。
5. 「OK」をクリックします。
6. Windows エクスプローラウィンドウで、ユーザーレベルのアクセス権を定義するシステム共有を右クリックします。
7. プルダウンメニューから「プロパティ」を選択します。
8. 「プロパティ」ダイアログボックスで「セキュリティ」タブを選択します。
9. 「アクセス権」ボタンをクリックします。
10. 必要なアクセス権を設定します。

    アクセス権の設定については、Windows のマニュアルを参照してください。
11. 「OK」をクリックします。

第8章

共有、割り当て、およびエクスポート

この章では、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システム上のファイルおよびボリュームへのユーザーアクセスを制御するさまざまな方法について説明します。

この章の内容は、次のとおりです。

共有

共通インターネットファイルシステム (CIFS) は、Microsoft のサーバーメッセージブロック (SMB) プロトコルの拡張バージョンです。SMB/CIFS を使用すると、Windows 環境のクライアントシステムから Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システム上のファイルにアクセスできます。

共有リソース (共有) とは、ネットワーク上にいる Windows クライアントがアクセス可能なサーバー上のローカルリソースです。共有は通常、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システム上では、ファイルシステムボリューム、またはボリューム内のディレクトリツリーとして存在します。各共有は、ネットワーク上で名前によって識別されます。ネットワーク上のクライアントに対しては、共有はサーバー上の完全なボリュームとして表示され、共有のルートのすぐ上のローカルディレクトリのパスは表示されません。

注 – 共有およびその他のディレクトリは、独立したエンティティーです。共有を削除しても、配下のディレクトリには影響しません。

共有は、通常、ネットワークファイルサーバー上のホームディレクトリにネットワークアクセス権を付与するために使用します。各ユーザーは、ファイルボリューム内のホームディレクトリに割り当てられます。

共有には、「静的」SMB/CIFS 共有と「自動ホーム」SMB/CIFS 共有の 2 種類があります。静的共有は、ユーザーがサーバーに接続しているかどうかに関係なく定義されている永続的な共有です。自動ホーム共有は、ユーザーがシステムにログインすると作成され、ログアウトすると削除される、一時的な共有です。

ユーザーがシステムを参照すると、静的に定義された共有と、接続中のユーザーに対する自動ホーム共有だけが表示されます。

静的共有

静的共有を作成すると、自身のホームディレクトリをクライアントワークステーションのネットワークドライブとして割り当てることができます。たとえば、vol1 というボリュームに、home という名前のホームディレクトリ、および bob と sally というユーザーのサブディレクトリを含めることができます。共有の定義は、次のとおりです。

表 8-1　共有のパスの例

共有の名前	ディレクトリのパス
bob	/vol1/home/bob
sally	/vol1/home/sally

システムへのアクセス権を持つ各 Windows ユーザーに対して静的ホームディレクトリの共有を定義および保持することが難しい場合は、自動ホーム機能を使用できます。詳細は、108 ページの「自動ホーム共有」を参照してください。

静的共有の構成

「Configure Shares」パネルを使用して、静的 SMB 共有を追加、表示、および更新します。

「Configure Shares」パネルの上部の表には、すべての既存の SMB 共有に関する情報が表示されます。この情報には、共有の名前、共有化されたディレクトリ、コンテナ名、およびデスクトップデータベースの呼び出しのほかに、Windows ワークグループのみに関する情報 (ユーザー、グループ、umask、およびパスワードの情報) が含まれます。

注 – ボリュームまたはディレクトリを共有するには、ボリュームまたはディレクトリが存在している必要があります。

デフォルトでは、各ボリュームのルートに隠し共有が作成され、ドメイン管理者のみがアクセスできます。通常、これらの共有は、データの移行およびディレクトリ構造の作成を行うために管理者が使用します。共有名は「Configure Shares」画面で確認できます。ユーザーの共有はこの手順のあと作成されます。これはボリュームのルートの下でディレクトリを共有するとセキュリティー管理が容易になるためです。

静的共有の作成

共有を作成する前に、ファイルボリュームを作成する必要があります。詳細は、45 ページの「ファイルボリュームまたはセグメントの作成」を参照してください。

▼ 新しい SMB 共有を追加する

1. **ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。**
2. **「Add」をクリックします。**
3. **「Share Name」フィールドに、追加する共有の名前を入力します。**

   これは、ネットワーク上でユーザーが確認できる名前です。この名前は 15 文字以内で入力する必要があります。次の文字は無効です。

   = | : ; \ “ ? < > * /
4. **(任意) 共有についての説明を「Comment」に入力します。**

   60 文字以内の英数字で入力できます。
5. **「Mac Extensions」セクションで「Desktop DB Calls」チェックボックスを選択すると、Macintosh デスクトップデータベースにアクセスして情報を設定できます。**

   これによって、Macintosh クライアントのファイルへのアクセスが高速化し、Macintosh 以外のクライアントによる Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システム上の Macintosh ファイルへのアクセスが可能になります。
6. **「Volume Name」プルダウンメニューに表示された選択可能なボリュームのリストから、共有するボリュームを選択します。**
7. **「Directory」フィールドに既存のディレクトリを入力します。**

   このフィールドではディレクトリを作成できません。ディレクトリの名前は大文字と小文字が区別されます。

注 – 「Directory」フィールドは、空白のままにしないでください。

8. **(任意)「Container」フィールドに、共有を公開する ADS コンテナを指定します。**

   「Set Up ADS」パネルで ADS が使用可能になっていると、このフィールドを使用できます。ただし、ADS が使用可能になっている場合でも、ADS コンテナを必ず指定する必要はありません。

9. **コンテナを指定するには、LDAP の DN 記法で共有の ADS パスを入力します。**

   詳細は、81 ページの「ADS で共有を公開する」を参照してください。

10. **「User ID」、「Group ID」、および「Password」が使用可能な場合は、これらを入力します。**

    「User ID」、「Group ID」、および「Password」フィールドは、NT ドメインモードではなく Windows ワークグループモードを使用可能にしている場合にのみ使用できます。Windows のセキュリティーモデルを使用可能にする方法については、23 ページの「Windows のセキュリティーの構成」を参照してください。

    Windows ワークグループは、共有レベルセキュリティーを使用します。この画面に表示されるユーザー ID (UID)、グループ ID (GID)、およびパスワードの各フィールドは、Windows ワークグループのユーザーが Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムファイルの所有およびアクセスを行うための唯一のセキュリティー手段となります。つまり、ディレクトリに対する権限は、ユーザーではなく、共有の定義によって判断されます。システムは、クライントが認証を実行しないことを前提として、共有接続が要求されるたびに、パスワードを使用したアクセス権の確認を明示的に求めます。

    同一のディレクトリに対して、UID、GID、およびパスワードが異なる複数の共有を作成できます。その後、各ユーザーに対して特定の共有のパスワードを発行できます。割り当てを使用して、ファイルボリュームの容量またはファイルの数について個々のユーザーおよびグループに対する制限値を管理することもできます。割り当ての詳細は、109 ページの「割り当ての管理」を参照してください。

注意 – User ID ー この共有を使用して特定のディレクトリにアクセスするユーザーの UID を入力します。このフィールドのデフォルト値は 0 (ゼロ) です。これは、UNIX のスーパーユーザーの値です。ただし、この値を割り当てる場合には注意が必要です。Windows ワークグループモードでは、このフィールドに 0 を入力すると、共有内のすべてのファイルおよびディレクトリに対するセキュリティーがすべて使用不可になります。

- R/W Password ー この共有に指定したディレクトリに対する読み取り/書き込みアクセス権のある Windows ワークグループのユーザーのパスワードを入力します。
- Confirm R/W Password ー 確認のために、読み取り/書き込みパスワードを再入力します。
- R/O Password ー 共有に対する読み取り専用アクセス権のある Windows ワークグループのユーザーのパスワードを入力します。

- Confirm R/O Password ー 確認のために、読み取り専用パスワードを再入力します。

11. この共有にファイル生成マスクを適用する場合、「Umask」フィールドにマスクを入力します。

    umask は、共有モードで作成されるファイルおよびディレクトリのセキュリティーポリシーを定義します。これによって、ファイルの作成時に使用不可になるアクセス権ビットが指定されます。

    umask は 8 進数で定義されます。8 進数は 3 バイトで構成されるため、UNIX ファイルのアクセス権の表記に簡単にマッピングできます。umask は、DOS 読み取り専用属性を除いて、標準の UNIX 規則を使用して適用されます。ファイルの作成時に DOS 読み取り専用属性を設定している場合、umask の適用後にすべての書き込みビットがファイルのアクセス権から削除されます。

    次の表に、DOS 読み取り専用属性の影響を含む、アクセス権への umask の適用例を示します。

表 8-2　アクセス権への umask の適用例

umask	新規ディレクトリのアクセス権		新規ファイルのアクセス権	
	DOS 読み取り/書き込み	DOS 読み取り専用	DOS 読み取り/書き込み	DOS 読み取り専用
000	777 (rwxrwxrwx)	555 (r-xr-xr-x)	666 (rw-rw-rw)	444 (r--r--r--)
777	000 (---------)	000 (---------)	000 (---------)	000 (---------)
022	755 (rwxr-xr-x)	555 (r-xr-xr-x)	644 (rw-r--r--)	444 (r--r--r--)
002	775 (rwxrwxr-x)	555 (r-xr-xr-x)	664 (rw-rw-r--)	444 (r--r--r--)

12. 「Apply」をクリックして、変更内容を保存します。

▼ 既存の SMB 共有を編集する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 更新する共有を選択します。
3. 「Edit」をクリックします。
4. 「Old Share Name」フィールドには、共有の現在の名前が表示されます。この名前を変更するには、「Share Name」フィールドに新しい名前を入力します。

    次の文字は共有の名前には使用できません。

    = | : ; \ " ? < > * /

5. 「Comment」フィールドで、共有についての説明を変更できます。60 文字以内の英数字で入力できます。

6. 「Mac Extensions」セクションで「Desktop DB Calls」チェックボックスを選択すると、システムから Macintosh デスクトップデータベースにアクセスして情報を設定できます。

   これによって、Macintosh クライアントのファイルへのアクセスが高速化し、Macintosh 以外のクライアントによる Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システム上の Macintosh ファイルへのアクセスが可能になります。

7. 共有のパスを変更するには、「Path」フィールドに既存のディレクトリの名前を入力します。

   このフィールドではディレクトリを作成できません。ディレクトリの名前は大文字と小文字が区別されます。

8. 必要に応じて、新しいコンテナを入力します。

   「Container」フィールドには、共有を公開する ADS コンテナを指定します。「Set Up ADS」パネルで ADS が使用可能になっている場合にのみ、このフィールドを使用できます。LDAP の DN 記法で共有の ADS パスを入力します。詳細は、79 ページの「ADS を使用可能にする」を参照してください。

9. 「User ID」、「Group ID」、および「Password」が使用可能な場合は、これらを入力します。

   これらのフィールドの詳細は、104 ページの手順 10 を参照してください。

10. 「静的共有の作成」の節で「Umask」フィールドに指定した規則を使用して、umask の設定を変更できます (詳細は、105 ページの手順 11 を参照)。

11. 「Apply」をクリックして、変更内容を保存します。

▼ SMB/CIFS 共有を削除する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 共有の表から削除する共有を選択します。
3. 「Remove」をクリックします。
4. 「Yes」をクリックして、共有を削除します。

SMB/CIFS クライアントの構成

セキュリティーおよびネットワークの設定を構成すると、ローカルネットワーク上のマスターブラウザで自動的に登録され、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムが SMB/CIFS クライアントに対して表示されるようになります。

クライアントは、次のいずれかの方法で接続します。

Windows 98、XP、および Windows NT 4.0

ユーザーは、Windows エクスプローラを使用してネットワークドライブを割り当てるか、「Network Neighborhood」ウィンドウで Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムのアイコンをクリックすることによって接続します。

ユーザーがネットワークドライブを割り当てる場合は、¥¥computer_name¥share_name のようにコンピュータの名前と共有の名前で構成された Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムの汎用命名規則 (UNC) パスが必要です。「Network Neighborhood」を使用して接続する場合は、ネットワーク上で Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムを識別するために使用されるシステム名が必要です。

Windows 2000、XP、および 2003

ADS がインストールされていない場合、ユーザーは Windows エクスプローラを使用してネットワークドライブを割り当てるか、「My Network Places」ウィンドウで Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムのアイコンをクリックすることによって接続します。

ユーザーがネットワークドライブを割り当てる場合は、¥¥computer_name¥share_name のようにコンピュータの名前と共有の名前で構成された Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムの UNC パスが必要です。「Network Neighborhood」を使用して接続する場合は、ネットワーク上で Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムを識別するために使用されるシステム名が必要です。

ADS がインストールされている場合は、ADS に公開されている Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムの共有をクリックすることによって接続できます。

DOS

net use コマンドを入力して、コマンド行でドライブ文字に共有を割り当てる必要があります。¥¥computer_name¥share_name のようにコンピュータの名前と共有の名前で構成された Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、または Sun StorEdge 5310 Gateway システムの UNC パスが必要です。

自動ホーム共有

SMB/CIFS 自動ホーム共有機能を使用すると、システムにアクセスする各 Windows ユーザーに対してホームディレクトリの共有を定義および保持するための管理作業が不要になります。ユーザーがログインするとシステムによって自動ホーム共有が作成され、ログアウトすると削除されます。これによって、ユーザーアカウントを保持するために必要な管理作業が減少し、サーバーリソースの効率が向上します。

自動ホーム機能を構成するには、この機能を使用可能にして、自動ホームパスを指定します。自動ホームパスとは、ディレクトリ共有のベースディレクトリのパスです。たとえば、ユーザーのホームディレクトリが `/vol1/home/sally` の場合、自動ホームパスは `/vol1/home` です。一時的な共有の名前は sally になります。ユーザーのホームディレクトリの名前は、ユーザーのログイン名と同じである必要があります。

ユーザーがログインすると、サーバーはユーザーの名前と一致するサブディレクトリを確認します。一致するサブディレクトリが検出され、その共有が存在しない場合、一時的な共有が追加されます。ユーザーがログアウトすると、サーバーはその共有を削除します。

動作していない状態が 15 分間続くと、Windows クライアントによってユーザーが自動的にログアウトされる場合があります。その結果、公開済みの共有のリストに自動ホーム共有が表示されなくなります。これは、CIFS プロトコルの通常の動作です。ユーザーがサーバー名をクリックするか、エクスプローラウィンドウなどでシステムへのアクセスを試みると、共有が自動的に再表示されます。

注 – システムが再起動すると、すべての自動ホーム共有が削除されます。

自動ホーム共有は自動的に作成および削除されるため、この機能を使用可能にすることによってほとんどの構成が行われます。

▼ 自動ホーム共有を使用可能にする

1. **ナビゲーションパネルで、「Windows Configuration」>「Configure Autohome」を選択します。**
2. **「Enable Autohome」チェックボックスを選択します。**
3. **「Autohome Path」を入力します。**

   パスの詳細は、108 ページの「自動ホーム共有」を参照してください。
4. **「ADS Container」を入力します。**

   詳細は、78 ページの「Active Directory サービス」を参照してください。
5. **「Apply」をクリックして、変更内容を保存します。**

割り当ての管理

「Manage Quotas」パネルでは、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムのファイルボリュームおよびディレクトリに対する割り当てを管理できます。ユーザーおよびグループの割り当ては、ユーザーまたはグループが使用可能なディスク容量、およびユーザーまたはグループがボリュームに書き込み可能なファイルの数を決定します。ディレクトリツリー割り当ては、特定のディレクトリで使用可能な容量か、そのディレクトリに書き込み可能なファイルの数、あるいはその両方を決定します。

ユーザーおよびグループに対する容量およびファイル数の制限値の設定については、109 ページの「ユーザーおよびグループの割り当ての構成」を参照してください。特定のディレクトリに対する容量およびファイル数の制限値の設定については、112 ページの「ディレクトリツリー割り当ての構成」を参照してください。

ユーザーおよびグループの割り当ての構成

「Configure User and Group Quotas」パネルでは、NT および UNIX のユーザーやグループに対するボリュームの割り当てを管理できます。このパネルには、選択したボリュームに対するスーパーユーザー、デフォルトのユーザー、および個別のユーザー、またはこれらのユーザーのグループへの割り当てが表示されます。デフォルトのユーザーおよびデフォルトのグループの設定は、個別の割り当てが設定されていないすべてのユーザーおよびグループに使用される設定です。

強い制限値および弱い制限値

「強い制限値」とは、ユーザーまたはグループが使用可能な絶対最大容量です。

「弱い制限値」は、強い制限値以下の値に設定されており、この制限値に達すると 7 日間の猶予期間に入ります。この猶予期間が過ぎると、ユーザーまたはグループは、使用済みの領域が弱い制限値より小さくなるまでボリュームへの書き込みを行うことができなくなります。

強い制限値は、弱い制限値以上の値に設定する必要があります。ディスク容量で設定する場合、最大値は約 2T バイトです。ファイル数で設定する場合、強い制限値の最大値は 40 億個です。

「スーパーユーザー」および「スーパーユーザーグループ」は、容量またはファイル数の強い制限値や弱い制限値が適用されないように自動的に設定されます。また、これらに割り当てを定義することはできません。

▼ ファイルボリュームに対して割り当てを使用可能にする

1. ナビゲーションパネルで、「File Volume Operations」>「Edit Properties」を選択します。
2. 「Volume Name」プルダウンメニューから、割り当てを使用可能にするファイルボリュームを選択します。
3. 「Enable Quotas」ボックスにチェックマークが付いていることを確認します。付いていない場合、このボックスを選択します。
4. 「Apply」をクリックします。

▼ ユーザーまたはグループの割り当てを追加する

1. ナビゲーションパネルで、「File Volume Operations」>「Manage Quotas」>「Configure User and Group Quotas」を選択します。
2. ユーザーの割り当てを構成する場合は、「Users」をクリックします。グループの割り当てを構成する場合は、「Groups」をクリックします。
3. 「Volume」ドロップダウンリストから、割り当てを追加するファイルボリュームの名前を選択します。

   この画面の表には、選択したファイルボリュームに対するスーパーユーザー、デフォルトのユーザー、および個別のユーザー、またはこれらのユーザーのグループへの割り当てが表示されます。
4. ユーザーまたはグループの割り当てを追加するには、「Add」をクリックします。
5. 適切なオプションボタンをクリックして、指定したユーザーまたはグループが UNIX 環境と NT 環境のどちらに属しているかを選択します。
6. 適切なユーザー名またはグループ名を選択します。NT ユーザーまたは NT グループの場合には、「Domain」でドメイン名もあわせて選択します。
7. 選択したユーザーまたはグループのディスク容量の制限値を設定します。

   次の 3 つのオプションから選択します。

   - Default ー 強い制限値および弱い制限値をデフォルトのユーザーまたはグループと同じ値に設定するには、このオプションを選択します。
   - No Limit ー ユーザーまたはグループに割り当てられる容量を無制限にするには、このオプションを選択します。
   - Custom ー 特定の制限値を設定するには、このオプションを選択します。割り当てを「K バイト」、「M バイト」、または「G バイト」のどの単位で表示するかを選択します。次に、ユーザーまたはグループに割り当てる容量の弱い制限値および強い制限値を「Soft」および「Hard」に入力します。

注 – ユーザーの割り当てを定義する場合、強い制限値と弱い制限値の両方を設定する必要があります。

8. **ユーザーまたはグループがファイルボリュームに書き込むことができるファイル数の制限値を設定します。次の 3 つのオプションから選択します。**
   - Default – 強い制限値および弱い制限値をデフォルトのユーザーまたはグループと同じ値に設定するには、このオプションを選択します。
   - No Limit – ユーザーまたはグループがファイルボリュームに書き込むことができるファイル数を無制限にするには、このオプションを選択します。
   - Custom – ファイル数に特定の制限値を設定するには、このオプションを選択します。次に、ファイル数の弱い制限値および強い制限値を「Soft」および「Hard」に入力します。
9. **「Apply」をクリックして、変更内容を保存します。**

▼ ユーザーまたはグループの割り当てを編集する

1. **ナビゲーションパネルで、「File Volume Operations」>「Manage Quotas」>「Configure User and Group Quotas」を選択します。**
2. **ユーザーの割り当てを編集するには、「Users」をクリックします。グループの割り当てを編集するには、「Groups」をクリックします。**
3. **「Volume」ドロップダウンリストから、割り当てを編集するファイルボリュームの名前を選択します。**

   この画面の表には、ファイルボリュームに対するスーパーユーザー、デフォルトのユーザー、および個別のユーザー、またはこれらのユーザーのグループへの割り当てが表示されます。
4. **割り当てを編集するユーザーまたはグループを選択して、「Edit」をクリックします。**
5. **選択したユーザーまたはグループのディスク容量の制限値を編集します。**

   次の 3 つのオプションから選択します。
   - Default – 強い制限値および弱い制限値をデフォルトのユーザーまたはグループと同じ値に設定するには、このオプションを選択します。
   - No Limit – ユーザーまたはグループに割り当てられる容量を無制限にするには、このオプションを選択します。
   - Custom – 特定の制限値を設定するには、このオプションを選択します。割り当てを「K バイト」、「M バイト」、または「G バイト」のどの単位で報告するかを選択します。次に、ユーザーまたはグループに割り当てる容量の弱い制限値および強い制限値を「Soft」および「Hard」に入力します。
6. **ユーザーまたはグループがファイルボリュームに書き込むことができるファイル数の制限値を編集します。次の 3 つのオプションから選択します。**

- Default ー 強い制限値および弱い制限値をデフォルトのユーザーまたはグループと同じ値に設定するには、このオプションを選択します。
- No Limit ー ユーザーまたはグループがファイルボリュームに書き込むことができるファイル数を無制限にするには、このオプションを選択します。
- Custom ー ファイル数に特定の制限値を設定するには、このオプションを選択します。次に、ファイル数の弱い制限値および強い制限値を「Soft」および「Hard」に入力します。

7. 「Apply」をクリックして、変更内容を保存します。

ユーザーまたはグループの割り当ての削除

スーパーユーザーおよびデフォルトのユーザー、またはこれらのユーザーのグループへの割り当ては、削除できません。個別のユーザーまたはグループへの割り当ては、ディスク容量およびファイル数のデフォルト値に設定することによって削除できます。

▼ 割り当てを削除する

1. ナビゲーションパネルで、「File Volume Operations」>「Manage Quotas」>「Configure User and Group Quotas」を選択します。
2. 「Configure User and Group Quotas」パネルで、ユーザーの割り当てを削除するには「Users」を、グループの割り当てを削除するには「Groups」を選択します。
3. 削除する割り当てを表から選択して、「Edit」をクリックします。
4. 「Edit Quota Setting」ダイアログボックスで、「Disk Space Limits」と「File Limits」の両方のセクションで「Default」オプションをクリックします。
5. 「Apply」をクリックして、割り当ての設定を削除します。

ディレクトリツリー割り当ての構成

「Configure Directory Tree Quotas」(DTQ) パネルでは、ファイルシステムの特定のディレクトリに対する割り当てを管理できます。ディレクトリツリー割り当ては、ディレクトリで使用可能なディスク容量およびこのディレクトリに書き込み可能なファイル数を決定します。このパネルで作成したディレクトリにのみ割り当てを構成できます。以前に作成した既存のディレクトリに割り当てを構成することはできません。

▼ DTQ を使用してディレクトリツリーを作成する

1. ナビゲーションパネルで、「File Volume Operations」>「Manage Quotas」>「Configure Directory Tree Quotas」を選択します。

2. プルダウンメニューから、ディレクトリツリー割り当てを構成するファイルボリュームを選択します。
3. 「Add」をクリックします。
4. 「DTQ Name」フィールドに、このディレクトリツリー割り当てを識別する名前を入力します。
5. 「DirName」フィールドに、新しいディレクトリの名前を入力します。
6. 「Path」フィールドの下に、選択したファイルボリュームのディレクトリツリー構造を示すボックスが表示されます。

   フォルダの内容を表示するには、フォルダの横の記号をクリックするか、フォルダのアイコンをダブルクリックします。次に、作成する新しいディレクトリを含めるディレクトリを選択します。「Path」フィールドにディレクトリのフルパスが表示されるまで続けます。
7. 「Disk Space Limits」セクションで、「No Limit」または「Custom」のいずれかを選択して、ディレクトリのディスク容量の制限値を指定します。
   - 「No Limit」を選択すると、ディレクトリのディスク容量を無制限にすることができます。
   - 「Custom」を選択すると、ディレクトリで使用可能なディスク容量の最大値を定義できます。
8. 割り当てを M バイトまたは G バイトのどちらの単位で報告するかを選択して、「Max Value」フィールドにディスク容量の制限値を入力します。

   「Custom」の値に 0 (ゼロ) を設定すると、「No Limit」を選択した場合と同様に処理されます。
9. 「File Limits」フィールドで、「No Limit」または「Custom」のいずれかを選択して、このディレクトリに書き込み可能なファイルの最大数を指定します。
   - 「No Limit」を選択すると、このディレクトリに書き込み可能なファイル数を無制限にすることができます。
   - 「Custom」を選択すると、ファイルの最大数を割り当てることができます。そのあと、「Max Value」フィールドにファイル数の制限値を入力します。
10. 「Apply」をクリックして、割り当てを追加します。

▼ 既存のディレクトリツリー割り当てを編集する

1. ナビゲーションパネルで、「File Volume Operations」>「Manage Quotas」>「Configure Directory Tree Quotas」を選択します。
2. 編集する割り当てを表から選択して、「Edit」をクリックします。

3. 「DTQ Name」フィールドで、このディレクトリツリー割り当てを識別する名前を編集します。

   「Path」は読み取り専用のフィールドで、ディレクトリのパスを示します。

4. 「Disk Space Limits」セクションで、「No Limit」または「Custom」のいずれかを選択して、ディレクトリのディスク容量の制限を指定します。
   - 「No Limit」を選択すると、ディレクトリで使用できるディスク容量の使用量を無制限にすることができます。
   - 「Custom」を選択すると、ディスク容量の最大値を割り当てることができます。

5. 割り当てを M バイトまたは G バイトのどちらの単位で報告するかを選択して、「Max Value」フィールドにディスク容量の制限値を入力します。

   「Custom」の値に 0 (ゼロ) を設定すると、「No Limit」を選択した場合と同様に処理されます。

6. 「File Limits」セクションで、「No Limit」または「Custom」のいずれかを選択して、このディレクトリに書き込み可能なファイルの最大数を指定します。
   - 「No Limit」を選択すると、このディレクトリに書き込み可能なファイル数は無制限になります。
   - 「Custom」を選択すると、ファイルの最大数を割り当てることができます。

7. 「Max Value」フィールドにファイル数の制限値を入力します。

8. 「Apply」をクリックして、変更内容を保存します。

注 – ディレクトリツリー割り当て (DTQ) が設定されたディレクトリを移動したり、名前を変更したりすると、DTQ のパスの指定はシステムによって自動的に更新されます。

▼ ディレクトリツリー割り当てを削除する

1. ナビゲーションパネルで、「File Volume Operations」>「Manage Quotas」>「Configure Directory Tree Quotas」を選択します。

2. 削除する割り当てを表から選択します。

3. 「Delete」をクリックして、割り当ての設定を削除します。

   ディレクトリツリー割り当て (DTQ) を削除すると、割り当ての設定が削除されます。ただし、ディレクトリ自体やディレクトリ内のファイルは削除されません。

注 – DTQ が設定されたディレクトリを削除すると、ディレクトリと DTQ 設定の両方が削除されます。

NFS エクスポートの設定

ネットワークファイルシステム (NFS) エクスポートを使用すると、UNIX (および Linux) ユーザーのアクセス権限を指定できます。「Configuring Exports」パネルの表には、各エクスポートのアクセス可能なディレクトリ、ホスト名、およびアクセスレベル (読み取り/書き込みまたは読み取り専用) など、現在の NFS エクスポートの情報が表示されます。

「@」で始まるホスト名は、ホストのグループを示します。たとえば、ホスト名が「@general」の場合にはすべてのホストが含まれ、ホスト名が「@trusted」の場合にはすべての承認されたホストが含まれます。承認されたホストについては、89 ページの「ホストの構成」を参照してください。

エクスポートは、特定の UNIX ホストにアクセス権限を指定すると作成されます。

▼ エクスポートを作成する

1. **ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Configure Exports」を選択します。**

   このパネルの表には、現在のエクスポートの情報が表示されます。エクスポートを作成していない場合、この部分は空白になります。

2. **「Add」ボタンをクリックして、エクスポートを追加します。**

3. **「Volume」ボックスで、UNIX NFS ホストにアクセス権を付与するボリュームを選択します。**

4. **「Path」ボックスで、UNIX NFS ホストにアクセス権を付与するディレクトリを指定します。**

   このフィールドを空白のままにすると、ボリューム全体が選択されます。

5. **「Access」セクションで、選択したボリュームに対する、読み取り/書き込み、読み取り専用、またはアクセス不可のどの権限をホストに付与するかを指定します。**

6. **「Hosts」セクションで、NFS エクスポートを定義する 1 つ以上のホストを選択します。**

   次のいずれかを選択します。

   - Host Netgroups ー ネットグループを選択するには、このオプションボタンを選択します。プルダウンメニューから、このエクスポートを定義するネットグループを選択します。

- Host Group – ホストグループを選択するには、このオプションボタンを選択します。プルダウンメニューから、すべてのホストを示す「general」、すべての承認されたホストを示す「trusted」、またはユーザー定義のホストグループを選択します。
- Known Host – 「Set Up Hosts」パネルを使用して追加したホストにエクスポートを割り当てるには、このオプションを選択します。プルダウンメニューから、このエクスポートを定義するホストを選択します。
- Other Host:「Set Up Hosts」パネルを使用して追加していない個々のホストにエクスポートを割り当てるには、このオプションを選択して、ホストの名前を入力します。

7. 「Map Root User」セクションで、スーパーユーザーのユーザー ID をマッピングする方法を選択します。

   次のいずれかを選択します。

   - Anonymous user – スーパーユーザーのユーザー ID を匿名ユーザーのユーザー ID にマッピングするには、このオプションボタンを選択します。
   - Root User – スーパーユーザーのユーザー ID をスーパーユーザーのユーザー ID (UID=0) にマッピングするには、このオプションボタンを選択します。
   - Map to UID – 特定のユーザー ID を割り当てるには、このオプションを選択してユーザー ID を入力します。

8. 「Apply」をクリックして、エクスポートを保存します。
9. 「Configure Exports」パネルで、作成したエクスポートについて、正しいパス、ホスト、およびアクセス権が表示されていることを確認します。

▼ エクスポートを編集する

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Configure Exports」を選択します。
2. 変更するエクスポートを選択して、「Edit」ボタンをクリックします。
3. アクセス権を変更するには、「Read/Write」、「Read/Only」、または「No Access」をクリックします。

   「Hosts」セクションは読み取り専用です。

4. 「Apply」をクリックして、変更内容を保存します。
5. 「Configure Exports」パネルで、編集したエクスポートについて、正しいパス、ホスト、およびアクセス権が表示されていることを確認します。

エクスポートの削除

NFS エクスポートを削除するには、「Configure Exports」パネルでエクスポートをクリックして、「Trash」ボタンをクリックします。

第9章

システムのオプション

この章では、Sun StorEdge 5310 NAS Appliance システム用に購入できるオプションを起動する方法について説明します。また、次に示すオプションの詳細も、この章で説明します。

- Sun StorEdge File Replicator。データを 1 つのボリュームから異なる Sun StorEdge 5310 NAS Appliance 上のミラー化されたボリュームへ複製できます。通常、トランザクション指向のシステムで使用されます。
- Compliance Archiving Software。データの保持および保護を目的とする規制適合アーカイブ機能のガイドラインにボリュームを準拠させることができます。

この章の内容は、次のとおりです。

システムのオプションの起動

システムのオプションを起動するには、「Activate Options」パネルで起動キーを入力する必要があります。オプションを購入した場合は、ご購入先に起動キーをお問い合わせください。

▼ オプションを起動する

1. ナビゲーションパネルで、「System Operations」>「Activate Options」を選択し、「Add」をクリックしてライセンスを追加します。
2. 「Add License」ダイアログボックスで、「Module」にご購入先から提供されたモジュールの名前 (たとえば **`Sun StorEdge File Replicator`**) を入力します。

3. 「Origination」にご購入先から提供された開始日を YYYYMMDD の形式で入力します。

   これは、時刻が 0000:00 になるとライセンスが有効になる日付を示します。この日付を 00000000 に指定すると、ライセンスはすぐに有効になります。

4. 「Expiration」にご購入先から提供された有効期限を YYYYMMDD の形式で入力します。

   これは、時刻が 2359:59 になるとライセンスが期限切れになる日付を示します。この日付を 00000000 に設定すると、ライセンスは期限切れになりません。

注 – 規制適合のライセンスが期限切れになるか、削除された場合、規制適合規則はシステムに保持されますが、規制適合対応のボリュームは作成できなくなります。Compliance Archiving Software の詳細は、132 ページの「Compliance Archiving Software」を参照してください。

---

5. 「Key」にご購入先から提供されたライセンスキーを入力します。

6. 「Apply」をクリックして、オプションを起動します。

   Sun StorEdge File Replicator の場合は、ミラー化されたサーバー上で追加手順を実行する必要があります。詳細は、124 ページの「Sun StorEdge File Replicator を遠隔サーバーで起動する」を参照してください。

7. 日付と時刻をまだ設定していない場合は、正確な日付、時刻、およびタイムゾーン情報を入力します。

   これによって、システム時間および固定クロックが設定されます。固定クロックは、ライセンス管理ソフトウェアおよび Compliance Archiving Software で、高い精度を必要とする、時間に基づく処理に使用されます。

注 – 固定クロックは一度しか設定できません。必ず正確に設定してください。

---

8. 新しい日付と時刻が正しいことを確認します。

   新しい日付と時刻が正しい場合は、「Yes」をクリックします。正しくない場合は、「No」をクリックして正しい日付と時刻を設定します。

Sun StorEdge File Replicator

Sun StorEdge File Replicator ソフトウェアを使用すると、2 台のサーバーで完全な複製データを保持できます。

Sun StorEdge 5310 NAS Appliance のミラー化

ミラー化を使用すると、1 台の Sun StorEdge NAS システムの一部またはすべてのファイルボリュームを、別の Sun StorEdge NAS システム上に複製できます。ソースサーバーは「アクティブサーバー」と呼ばれ、ターゲットサーバーは「ミラーサーバー」と呼ばれます。

アクティブサーバーに障害が発生した場合、ミラーサーバー上でミラー化を切断し、ミラーサーバー上でミラー化されたファイルボリュームをプロモートして (ユーザーが使用できるように) します。

使用されるミラー化の方法は、非同期トランザクション指向のミラー化です。ミラー化は、大容量の「ミラーバッファー」を使用して実行され、ファイルシステムのトランザクションはミラーシステムへの転送の待ち行列に入れられます。つまり、ミラーサーバーでの処理はアクティブサーバーでの処理よりわずかに遅れて実行されます。ミラー化はトランザクション指向であるため、ネットワークの中断やシステム障害の発生時にも、ミラーファイルシステムの完全性が保証されます。

ミラー化の準備

ミラー化を行う前に、次の点を確認してください。

- ミラー化には 2 台の Sun StorEdge NAS サーバーが必要です。サーバーのモデルは任意で、異なるモデルを使用できます。
- ミラーサーバーには、ミラー化するファイルボリュームと同じか、それより大きいストレージ領域が必要です。
- アクティブサーバーとミラーサーバーとの間には、十分な処理能力を持つ、継続的に使用可能な信頼性の高いネットワーク接続が存在している必要があります。これらの 2 つのサーバーを接続するインタフェースには、100M ビット Ethernet または 1000M ビット Ethernet を使用できます。スイッチまたはルーターを介してサーバーを接続することもできます。サーバーをルーターに接続する場合、静的ルートを設定して、ミラー化データが専用ルートを使用して送信されるようにしてください。サーバーをスイッチに接続する場合は、各サーバーに仮想 LAN (VLAN) を作成して、ネットワークトラフィックを分離します。
- 両方のサーバーにインストールされているオペレーティングシステムのバージョンが同じである必要があります。
- ミラー化するアクティブファイルボリュームは、1G バイト以上である必要があります。

注 – いったんファイルボリュームをミラー化すると、元のファイルボリュームの名前を変更できなくなります。

クラスタ構成の File Replicator の要件および制限事項

次に、Sun StorEdge 5310 Cluster でのミラー化の要件および制限事項の一覧を示します。

- クラスタ構成の両方のサーバーで、Sun StorEdge File Replicator ライセンスを使用可能にすることをお勧めします。
- ミラー化は、サーバー H1 からまたはサーバー H1 に対してのみ確立してください。同一クラスタのサーバー H1 からサーバー H2 に対してミラーを作成しないでください。
- ミラー管理操作を実行するには、クラスタ内のサーバーが両方とも NORMAL 状態である必要があります。ミラー管理操作には、新しいミラーの作成、役割の変更、プロモート、切断などがあります。
- クラスタがフェイルオーバーモードの場合 (つまり、1 台のサーバーが ALONE 状態で、もう 1 台のサーバーが QUIET 状態の場合) であるか、または縮退状態である場合は、ミラー管理操作を実行しないでください。ミラー管理操作を実行する前に、クラスタを NORMAL 状態にすることをお勧めします。
- クラスタ構成でフェイルオーバーが行われた場合でも、既存のミラーによるミラー化は続行されます。また、フェイルオーバー後にクラスタが復元されるときにも、既存のミラーによるミラー化は続行されます。

アクティブシステムおよびミラーシステムの構成

システムの構成時に、ミラー化するサーバーを相互に接続するポートの役割を指定します (122 ページの「専用ネットワークポートを構成する」を参照)。次に、Web Administrator インタフェースを使用して、アクティブシステムおよびミラーシステム上でミラー化を構成します (123 ページの「ミラー化されたファイルボリュームの構成」を参照)。それぞれのシステムは個別に構成します。

▼ 専用ネットワークポートを構成する

1. アクティブサーバーのナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」を選択します。
2. ローカルのネットワークまたはサブネットに接続されたポートに IP アドレスおよび「Primary」という役割を割り当てていない場合、これらを割り当てます。

   アクティブシステムおよびミラーシステムのポートは、異なるローカルサブネット上に存在することができます。TCP/IP の設定の詳細は、20 ページの「ネットワークポートの構成」を参照してください。

3. **アクティブシステムとミラーシステムとのミラー接続に使用するポートに IP アドレスを割り当てます。**

注 – 主インタフェースを含むサブネットをミラー化に使用しないでください。

ミラー化のトラフィックを処理するための分離ネットワークが作成されている場合は、192.1xx.x.x など、専用で使用するために予約された範囲のアドレスを使用してください。たとえば、アクティブシステムのミラーリンクインタフェースを 192.1xx.1.1 に割り当て、ミラーシステムのミラーリンクインタフェースを 192.1xx.1.2 に割り当てます。

4. **アクティブサーバーとミラーサーバーとの接続に使用するポートの「Role」フィールドで、「Mirror」を選択します。**

5. **アクティブシステムおよびミラーシステムのミラーインタフェースが同じサブネット上で接続されていない場合は、コマンド行インタフェースを使用して、これらのシステム間に静的ルートを設定する必要があります。**

   これによって、サーバーは、ローカルのインタフェースに直接接続されていないネットワーク上で相互に通信できます。この処理の実行については、202 ページの「ルートの管理」を参照してください。

6. **「Apply」をクリックして、変更内容を保存します。**

ミラー化されたファイルボリュームの構成

ミラー化は、ボリューム単位で実行されます。一部またはすべてのボリュームをミラー化するように選択できます。

注 – ミラー化できるのは 1G バイト以上のファイルボリュームのみです。いったんファイルボリュームをミラー化すると、ミラー接続が保持されている間は、元のファイルボリュームの名前を変更できません。

ミラーの初期同期中に、アクティブサーバーからミラー化されているファイルボリュームに対して入出力動作を行うことはできません。

ミラーバッファー

ミラーバッファーには、ミラーサーバーへのファイルシステムの書き込みトランザクションの転送中に、これらのトランザクションが格納されます。アクティブサーバー上のファイルボリュームの空き領域は、ミラーバッファーの割り当てサイズを設定することによって減少します。

ミラーバッファーのサイズはさまざまな要因によって異なりますが、100M バイト以上である必要があります。また、ミラーバッファーは、特定のファイルボリュームの残りの空き容量の半分以下である必要があります。

通常は、ミラー化するファイルボリュームの約 10% のサイズのミラーバッファーを作成することをお勧めします。このサイズは、ファイルボリュームのサイズではなく、ファイルボリュームに書き込まれる情報のサイズによって判断する必要があります。概して、ミラーバッファーのサイズは、ファイルボリュームへの書き込みの頻度に正比例し、2 台のサーバー間のネットワーク速度に反比例します。

ファイルボリュームへの書き込み操作の頻度が高く、2 台のミラーサーバー間のネットワーク接続の速度が遅い場合は、ミラー化するファイルボリュームの約 25 ～ 30% のサイズのミラーバッファーを作成することをお勧めします。

ミラーバッファーのサイズは、動的に増やすことはできません。ミラーバッファーのサイズを増やすには、既存のミラーを切断し、新しいミラーバッファーサイズでミラーを再度作成する必要があります。

▼ Sun StorEdge File Replicator を遠隔サーバーで起動する

Sun StorEdge File Replicator オプションを起動したあと (119 ページの「システムのオプションの起動」を参照)、ミラー化するファイルボリュームが含まれる遠隔サーバー上でもこのオプションを起動する必要があります。

1. ミラー化するファイルボリュームが含まれるサーバーの Web Administrator にログインします。
2. 「Add License」ダイアログボックスで、「Module」にご購入先から提供されたモジュールの名前 (**`Sun StorEdge File Replicator`**) を入力します。
3. 「Origination」にご購入先から提供された開始日を YYYYMMDD の形式で入力します。

   これは、時刻が 0000:00 になるとライセンスが有効になる日付を示します。この日付を 00000000 に指定すると、ライセンスはすぐに有効になります。
4. 「Expiration」にご購入先から提供された有効期限を YYYYMMDD の形式で入力します。

   これは、時刻が 2359:59 になるとライセンスが期限切れになる日付を示します。この日付を 00000000 に設定すると、ライセンスは期限切れになりません。
5. 「Key」にご購入先から提供されたライセンスキーを入力します。
6. 「Apply」をクリックして、Sun StorEdge File Replicator を起動します。

▼ ファイルボリュームを追加する

1. ナビゲーションパネルで、「File Replicator」>「Manage Mirrors」を選択します。
2. 「Add」をクリックします。

3. 「Volume」プルダウンメニューから、ミラー化するファイルボリュームを選択します。

   ミラー化するファイルボリュームは、1G バイト以上である必要があります。

4. 「Mirror Host」フィールドにミラーサーバーの識別できる名前を入力します。

5. 「IP Address」に、ミラーシステムの IP アドレスを入力します。

   ここには、ミラーシステム上のミラー化 NIC に対して選択した IP アドレスを入力します。

6. 任意で、「Alternate IP Address」に代替 IP アドレスを入力します。

   最初の IP アドレスが使用不可になると、サーバーはこの代替 IP アドレスを使用してミラーを保持します。

7. ミラーサーバーへのアクセスに管理パスワードが必要な場合は、「Password」フィールドに管理パスワードを入力します。

   管理パスワードを設定しない場合、このフィールドは空白のままにします。必ずパスワードを使用してサーバーを保護してください。

8. 「Mirror Buffer」にミラーバッファーのサイズを M バイト単位で入力します。

   アクティブサーバー上のファイルボリュームの空き領域は、ミラーバッファーの割り当てサイズを設定することによって減少します。

9. ミラーの作成中にアクティブサーバー上のソースファイルボリュームに対する入出力動作が発生しないことを確認してから、「Apply」をクリックしてミラーを作成します。

   ミラー作成処理が開始されます。「Manage Mirrors」パネルでミラーが「In Sync」の状態になると、ミラー化されたファイルボリュームが読み取り専用でマウントされます。いったんミラーの状態が「In Sync」になると、入出力動作を再開できます。

   既存のミラーの代替 IP アドレスまたはミラーサーバーの管理者パスワードは、編集が可能です。

▼ ミラーを編集する

1. ナビゲーションパネルで、「File Replicator」>「Manage Mirrors」を選択します。

2. 編集するミラーを表から選択します。

3. 「Edit」をクリックします。

   ファイルボリューム名およびミラーホストは、読み取り専用のフィールドです。

4. ミラー接続に使用する IP アドレスを編集して、次のフィールドで代替 IP アドレスを編集します。

5. **必要に応じて、ミラーホストサーバーへのアクセスに必要な新しい管理パスワードを入力します。**

   管理パスワードを設定しない場合は、「Password」フィールドを空白のままにします。

6. **「Apply」をクリックして、変更内容を保存します。**

▼ 破損したミラーを修正する

ミラーが破損した場合は、次の手順を実行します。ミラーの破損は、2 台のサーバー間の接続がしばらくの間停止していた場合や、ミラーバッファーが非常に小さく、マスターボリュームへの書き込みが多い場合に発生します。

1. **2 台のサーバー間に、より高速のネットワーク接続を確立します。**
2. **ミラーが In Sync 状態になるまで、マスターファイルシステムへのすべての入出力動作を休止します。**
3. **nbd ボリュームを切断およびプロモートしたあと、CIFS または NFS クライアントのいずれかから、ターゲットファイルシステムを読み取り専用でミラーサーバーにマウントします。**

   このファイルシステムは、バックアップ処理または任意の読み取り専用処理で使用されます。

   ミラー化機能にチェックポイントを組み合わせることもできます。アクティブサーバーにチェックポイントが作成されていると、そのチェックポイントもミラーサーバーにミラー化されます。これを使用して、スケジュール設定されたバックアップを実行したり、ほかのユーザーおよびアプリケーションが読み取り専用でチェックポイントにアクセスしたりすることができます。

警告しきい値の設定

「File Replicator」から「Set Threshold Alert」パネルを表示して、すべてのミラー化されたファイルボリュームにしきい値警告を設定できます。しきい値警告とは、ミラーバッファーの使用率に応じて指定した受信者に送信される警告です。

ミラーバッファーには、ミラーサーバーへのファイルシステムの書き込みトランザクションの転送中に、これらのトランザクションが格納されます。アクティブサーバーへの書き込み操作が増加したり、ネットワークリンクが切断されたりすると、ミラーサーバーへの書き込みトランザクションの代わりに、ミラーバッファーへのバックアップが行われる場合があります。この処理によってミラーバッファーが制限を超えた場合、ミラーが破損し、ミラーが再確立されるまでアクティブサーバーとミラー

サーバー間でトランザクションが発生しなくなります。通信が完全に復元されると、システムは自動的にミラーの再同期処理を開始して、ミラー化されたファイルボリュームの同期をとります。

この状況を回避するため、ミラーバッファーの使用率が特定のしきい値に達すると、システムは電子メール通知、システムログファイル、SNMP トラップ、および LCD パネルを使用して、自動的に警告を送信します。

▼ しきい値警告を設定する

1. ナビゲーションパネルで、「File Replicator」>「Set Threshold Alert」を選択します。
2. 「Mirroring Buffer Threshold 1」を選択します。

   これは、最初の警告が送信されるミラーバッファーの使用率です。デフォルト値は 70% です。これは、ミラーバッファーの使用率が 70% に達すると、自動的に警告が送信されることを意味します。
3. 「Mirroring Buffer Threshold 2」を選択します。

   これは、2 番めの警告が送信されるミラーバッファーの使用率です。デフォルト値は 80% です。
4. 「Mirroring Buffer Threshold 3」を選択します。

   これは、3 番めの警告が送信されるミラーバッファーの使用率です。デフォルト値は 90% です。
5. 「Alert Reset Interval (Hours)」を選択します。

   これは、その時間内に状態が再発生してもシステムが警告を再送信せずに待機する時間を示します。

   たとえば、「Mirroring Buffer Threshold 1」を 10% に設定し、「Alert Reset Interval」を 2 時間に設定すると、ミラーバッファーの使用率が 10% に達したときに最初の警告が送信されます。システムは、その後 2 時間はしきい値 1 警告を再送信しません。2 時間が経過してもミラーバッファーの使用率が 10% を超えていて、しきい値 2 または 3 は超えていない場合、しきい値 1 警告が再送信されます。

   このフィールドのデフォルト値は 24 時間です。
6. 「Apply」をクリックして、変更内容を保存します。

ミラーサーバー間の接続の切断

たとえば、アクティブサーバー上のファイルボリュームが使用できない場合に、ミラーサーバー上のファイルボリュームをプロモートするには、まず、ミラー接続を切断する必要があります。ミラー接続の切断は、次の手順で説明するとおり、ミラー

サーバー上ではなくアクティブサーバー上で行います。ただし、アクティブサーバーが停止し、このサーバーにアクセスして接続を切断できない場合、代わりにミラーサーバーからミラー接続を切断できます。

▼ ミラー接続を切断する

1. アクティブサーバーのナビゲーションパネルで、「File Replicator」>「Manage Mirrors」を選択します。
2. 表からミラーを選択して、「Break」をクリックします。

   ミラー接続の切断を確認するプロンプトが表示されます。ミラー接続を切断すると、そのミラー接続はこのパネルのミラーの表に表示されなくなります。ファイルボリュームをプロモートするには、ミラーサーバー上で「Manage Mirrors」パネルにアクセスする必要があります。詳細は、128 ページの「ミラー化されたファイルボリュームのプロモート」を参照してください。

ミラー化されたファイルボリュームのプロモート

ミラーサーバーは、アクティブサーバーに障害が発生した場合に、ミラー化されたファイルボリュームの高可用性を実現します。ミラー化されたファイルボリュームをネットワークユーザーが使用できるようにするには、ファイルボリュームを「プロモート」する必要があります。まず、ミラー接続を切断し、次に、ミラー化されたファイルボリュームをプロモートして、アクセス権を設定する必要があります。ミラー接続を切断して、ミラー化されたファイルボリュームをプロモートすると、元のファイルボリュームとミラー化されたファイルボリュームは完全に独立した状態になります。

注意 – 厳格な規制適合対応のボリュームのミラーはプロモートできません。

厳格な規制適合対応のミラーボリュームに一時的にアクセスする必要がある場合は、そのボリュームをプロモートせずに読み取り専用のファイルシステムとしてエクスポートできます。

ミラーサーバー上のファイルボリュームをプロモートするには、まずミラー接続を切断する必要があります。詳細は、127 ページの「ミラーサーバー間の接続の切断」を参照してください。

▼ ミラーサーバー上のファイルボリュームをプロモートする

1. ミラーサーバーのナビゲーションパネルで、「File Replicator」>「Manage Mirrors」を選択します。
2. 「Promote」をクリックします。

3. 「Promote Volume」ダイアログボックスで、プロモートするボリュームを選択し、「Apply」をクリックします。

この処理が完了するまでには数分かかる場合があります。ミラー化されたファイルボリュームをプロモートするには、ある時点でそのボリュームが「In Sync」の状態になっている必要があります。プロモートが正常に終了したときにミラー化されたファイルボリュームの同期がとれていない場合、そのボリュームは読み取り専用ボリュームとしてマウントされます。ボリュームへの書き込みを許可する前に、`fsck` コマンドを実行して必要な修復を行います。

ミラー接続を切断すると、システムによってファイルシステムチェックが実行されます。このチェック時にエラーが検出されると、ファイルボリュームのプロモート処理に要する時間が長くなる場合があります。プロモート処理中にミラーの同期がとれていない場合、データの完全性は保証されません。

ファイルボリュームをプロモートしたあとで、アクセス権を再構成する必要があります。SMB 共有の情報は自動的に継承されますが、NFS ファイルボリュームへのアクセスおよび NFS エクスポートはこのファイルボリューム用に再構成する必要があります。NFS エクスポートの設定の詳細は、115 ページの「NFS エクスポートの設定」を参照してください。

ミラー接続の再確立

ここでは、アクティブサーバーに障害が発生してミラーサーバー上のファイルボリュームをプロモートしたあとに、ミラー接続を再確立する方法について説明します。プロモートしたファイルボリュームが最新のバージョンになり、アクティブシステム上の古いファイルボリュームから完全に独立して機能します。ミラー接続を再確立するには、最新のファイルボリュームをアクティブサーバーにミラー化し、そのファイルボリュームをミラーサーバーにミラー化して元の状態に戻す必要があります。

注 – ミラー化されたファイルボリュームをプロモートしていない場合、次の手順を実行しないでください。アクティブシステムがオンラインに戻ると、ミラーが自動的に「In Sync」の状態に戻されます。

次の例では、「サーバー 1」がアクティブサーバー、「サーバー 2」がミラーサーバーです。

▼ ミラー接続を再確立する

1. **サーバー 1 上でミラーが切断されていることを確認します。**

詳細は、130 ページの「アクティブサーバーでミラー接続を切断する」を参照してください。

2. サーバー 1 上の古いファイルボリュームを削除します。

   詳細は、130 ページの「サーバー 1 上の古いファイルボリュームを削除する」を参照してください。

3. サーバー 2 の最新のファイルボリュームをサーバー 1 にミラー化します。詳細は、130 ページの「サーバー 2 からサーバー 1 へ最新ボリュームをミラー化する」を参照してください。

4. サーバー 2 の役割を変更します。

   詳細は、131 ページの「ボリュームの役割の変更」を参照してください。

   この時点で、サーバー 1 が再度アクティブになり、サーバー 2 はミラー化のターゲットになります。

▼ アクティブサーバーでミラー接続を切断する

1. Web ブラウザのウィンドウを開き、サーバー 1 にアクセスします。
2. ナビゲーションパネルで、「File Replicator」>「Manage Mirrors」を選択します。
3. 切断するミラー接続を選択します。
4. 「Break」をクリックします。

▼ サーバー 1 上の古いファイルボリュームを削除する

1. サーバー 1 のナビゲーションパネルで、「File Volume Operations」>「Delete File Volumes」を選択します。
2. ミラー化されていたファイルボリュームを選択します。

   ミラーサーバー上のファイルボリュームがプロモートされて最新バージョンになっているため、アクティブサーバー上の古いファイルボリュームを削除する必要があります。

注意 – 次の手順を実行する前に、アクティブサーバー上の古いソースファイルボリュームを削除してください。また、事前にミラーサーバー上の最新のファイルボリュームを確認し、このファイルボリュームをプロモートします。

3. 「Apply」をクリックして、古いファイルボリュームを削除します。

▼ サーバー 2 からサーバー 1 へ最新ボリュームをミラー化する

1. Web ブラウザのウィンドウを開き、サーバー 2 にアクセスします。
2. ナビゲーションパネルで、「File Replicator」>「Manage Mirrors」を選択します。
3. 「Add」をクリックします。

4. 「Volume」プルダウンメニューから、ミラー化するファイルボリュームを選択します。
5. 「Mirror Host」フィールドにサーバー 1 のミラー化の名前を入力します。
6. ミラー接続に使用するサーバー 1 のポートの IP アドレスを入力します。
7. 「Alternate IP Address」に代替 IP アドレスを入力します。
8. サーバー 1 へのアクセスに管理パスワードが必要な場合、「Password」フィールドに管理パスワードを入力します。

   管理パスワードを設定しない場合、このフィールドは空白のままにします。
9. 「Mirror Buffer」にミラーバッファーのサイズを入力します。

   ミラーバッファーの詳細は、121 ページの「Sun StorEdge 5310 NAS Appliance のミラー化」を参照してください。

   ミラー同期中は、サーバー 2 上のソースファイルボリュームに対する入出力動作を行わないでください。
10. 「Apply」をクリックして、ミラーを作成します。

    ミラー作成処理が開始されます。ミラーが「In Sync」の状態になると、サーバー 1 とサーバー 2 の両方にファイルボリュームの同一のコピーが存在するようになります。
11. サーバー 1 の「Manage Mirrors」パネルで、プロモートしたファイルボリュームを選択して、「Change Roles」をクリックします。

    詳細は、131 ページの「ボリュームの役割の変更」を参照してください。

    元のミラー接続が再確立されました。

ボリュームの役割の変更

管理者は、アクティブボリュームとミラーボリュームとの間で役割を切り替えることができます。ボリュームの役割を変更すると、アクティブボリュームをミラーボリュームとして機能させるか、ミラーボリュームをアクティブボリュームとして機能させることができます。ただし、各ボリュームの元の構成は変更されません。役割の変更は、障害回復のための機能ではありません。

注 – 役割を変更するボリュームは、In Sync 率 100% の状態である必要があります。

役割の変更は、アクティブサーバーまたはミラーサーバーの「Manage Mirror」パネルで実行できます。

▼ 役割を変更する

1. ナビゲーションパネルで「File Replicator」>「Manage Mirrors」をクリックします。
2. 「Volume」列でボリュームを選択します。
3. 「Change Roles」をクリックします。
4. メッセージを確認して、「Yes」をクリックします。

Compliance Archiving Software

Compliance Archiving Software は、情報の保持および保護に関するビジネス上の運用および規制適合規則への企業の対応を支援します。このような記録の保持および保護に関する規則およびフレームワークには、米国証券取引委員会 (SEC) 規制 17 CFR (240.17a-4 (17a-4))、米国企業改革法 (Sarbanes-Oxley Act)、新 BIS 規制 (BASEL II)、およびデータ保護とプライバシに関する多くの指示があります。

Compliance Archiving Software は、情報管理の規制適合および企業のコンテンツ管理に精通している専門家と協議し基礎から設計されているため、電子ストレージ媒体の保持および保護に関するもっとも厳しい要件への対応に役立ちます。Compliance Archiving Software では、規制適合規則に従って WORM (Write Once, Read Many) ファイルが使用されます。

Compliance Archiving の使用可能への切り替え

Compliance Archiving Software は、「推奨実施」と呼ばれる比較的厳しくない形式と、「必須実施」と呼ばれる厳しい形式の両方で使用できます。

Compliance Archiving Software を起動すると (119 ページの「システムのオプションの起動」を参照)、ボリュームの作成時に、規制適合を推奨実施または必須実施のどちらで使用可能にするかを選択できます。

注 – Sun StorEdge 5310 Gateway システムの構成では、推奨実施の規制適合はサポートされていますが、必須実施はサポートされていません。

注 – Compliance Archiving Software を適切に動作させるには、Sun StorEdge 5310 NAS Appliance または Sun StorEdge 5310 Cluster システムのハードウェアが物理的に正しく構成されている必要があります。つまり、Sun StorEdge 5300 RAID EU コントローラアレイはプライベートファイバチャネルを使用して NAS 本体およびすべての Sun StorEdge 5300 EU の拡張格納装置に接続し、その他のデバイスまたはネットワークには決して接続しないでください。

注 – できるかぎり強力なデータ保持方針を実現するには、使用している Sun StorEdge 5310 NAS Appliance または Sun StorEdge 5310 Cluster システムに物理的なセキュリティーも追加することをお勧めします。ソフトウェア制御によるデータ保持よりも、物理的な保護手段を使用してシステムのハードウェアへのアクセスを制御する方が強力です。

注意 – Compliance Archiving Software によって実施される、さまざまなデータ保持規則を認識しないアプリケーションおよびユーザーが使用するボリュームでは、規制適合アーカイブ機能を決して使用可能にしないでください。

Compliance Archiving Software を使用すると、管理者は、作成するすべての新しいボリュームに対して規制適合アーカイブ機能を使用可能にできます。ただし、これはボリュームをはじめて作成する場合だけです。45 ページの「「Create File Volume」パネルを使用してファイルボリュームまたはセグメントを作成する」に示す手順に従って、規制適合対応のボリュームを作成してください。

必須実施の規制適合

必須実施の規制適合では、次に示すように、データの保護、保持、およびプライバシに関する指示が遵守されます。

- 必須実施の規制適合対応ボリュームを破棄することはできません。
- 保持期間が期限切れになるまで、WORM ファイルを破棄することはできません。
- ボリュームの保持期間は短縮または延長できますが、WORM ファイルの保持期間は延長することしかできません。
- チェックポイントから WORM ファイルを復元することはできません。

注意 – いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

推奨実施の規制適合

必須実施の規制適合とは対照的に、推奨実施の規制適合では次の操作が可能です。

- 承認された管理者は、規制適合対応の WORM ファイルおよび規制適合対応のボリュームを、監査対象の削除機能を使用して破棄できます。

注 – ボリュームを削除する前に、そのボリューム内の監査ログを別のファイルシステムにコピーして保管しておく必要があります。保管しない場合、監査ログは失われます。

- 承認された管理者は、保持期間を短縮および延長できます。
- 承認された管理者は、監査対象の削除機能を使用してチェックポイントから WORM ファイルを復元できます。
- 出荷時のデフォルトの保持期間は 0 日ですが、変更できます。

注 – 保持期間の期限が切れる前に、保持期間の短縮および保持ファイルの削除を実行する場合は、承認されたホストからスーパーユーザーがこの操作を行う必要があります。詳細は、220 ページの「承認されたホストの管理」を参照してください。

推奨実施の規制適合対応ボリュームを必須実施にアップグレードすると、そのボリュームのデフォルトの保持期間は永続的になります。この変更は、「Edit Properties」パネルで実行できます。

注 – 推奨実施の規制適合対応ボリュームのアップグレードは、ゲートウェイ構成ではサポートされません。

規制適合の監査

規制適合の監査では、適切な権限の有無にかかわらず、データの編集または削除が試行されると、これをテキストベースのログに記録します。この監査を使用可能にするには、Data Retention Audit Service (DRAS) API を使用します。この API には、次の機能があります。

- 保持ファイルに対する変更および試行された変更の報告
- 監査可能なイベントを記録するロギングメカニズム
- システムの存続期間にわたる、監査ログの保護および保持
- 見やすい形式にまとめられた監査ログ情報と、標準のシステムアクセスプロトコルを介した監査ログへのセキュリティー保護されたアクセス

監査可能なイベントのセットは、次のとおりです。

- ファイルの保持
- 保持ファイルの保持期間の延長
- 保持ファイルへのリンクの解除 (削除) 要求
- 保持ファイルへの書き込み要求
- 保持ファイルの名前の変更要求
- ディレクトリの削除要求
- ディレクトリの名前の変更要求

ファイルサイズの制限

規制適合対応ボリュームでは、ボリュームでの監査可能な操作をログに確実に記録できる容量の空き領域が予約されます。規制適合対応ボリュームの空き領域がこの制限を下回ると、監査可能な操作を実行できなくなります。操作と監査の両方を実行するために必要な領域が不足していることを示すメッセージがログに記録され、システムで電子メールが構成されている場合は警告メールが送信されます。

監査ログ

各規制適合対応ボリュームの監査ログは、ボリュームのルートディレクトリに保存されます。

監査ログのレコードはテキストベースで、NFS や CIFS などのネットワークプロトコルを介してアクセスできます。Windows 2000 または Windows XP が動作しているクライアントでログの内容を表示するには、共有のパスに `.audit$` ディレクトリが含まれている必要があります。共有の作成の詳細は、101 ページの「共有」を参照してください。

表 9-1 に、監査ログの形式を示します。

表 9-1 監査ログの形式

フィールド	長さ	説明
Version	7	Data Retention Audit Service のバージョン番号
Serial Number	11	一意のシーケンス番号
Length	5	監査レコードの長さ
Timestamp	21	イベントが発生した日付と時刻
TID	11	イベントが実行されたスレッドのスレッド ID
Volume ID	11	監査が実行されたボリュームのボリューム ID
Protocol	9	操作の要求に使用されたネットワークプロトコル

表 9-1　監査ログの形式 (続き)

フィールド	長さ	説明
Inode	11	ファイルのファイルシステムの i ノード番号
Client IP Address	16	操作を要求したクライアントの IP アドレス
Server IP Address	16	クライアントの要求を受信した IP アドレス
UID	11	ユーザーの資格
GID	11	一次グループの資格
Operation	8	監査イベント
Status	可変	操作の結果
Domain	可変	ユーザーが属する Windows ドメイン (取得可能な場合)
File/Directory Name	可変	操作の実行対象のファイルまたはディレクトリの名前 (取得可能な場合)
Path/Extra Data	可変	監査からの追加情報 (取得可能な場合)

その他の規制適合アーカイブ機能

Compliance Archiving Software の機能およびプログラミングインタフェースの技術的な概要については、付録 C を参照してください。

規制適合アーカイブ機能の設定の変更については、244 ページの「Compliance Archiving Software の構成」を参照してください。

第 10 章

システムの監視

この章では、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムの監視機能について説明します。システム監視は保守機能と密接に関連しています。ここで説明する多くの監視機能で表示される問題への対処については、ほかの章を参照してください。監視機能では、管理アクティビティーまたは保守アクティビティーの完了や状態も表示されます。

この章の内容は、次のとおりです。

SNMP (ネットワーク管理プロトコル) の監視

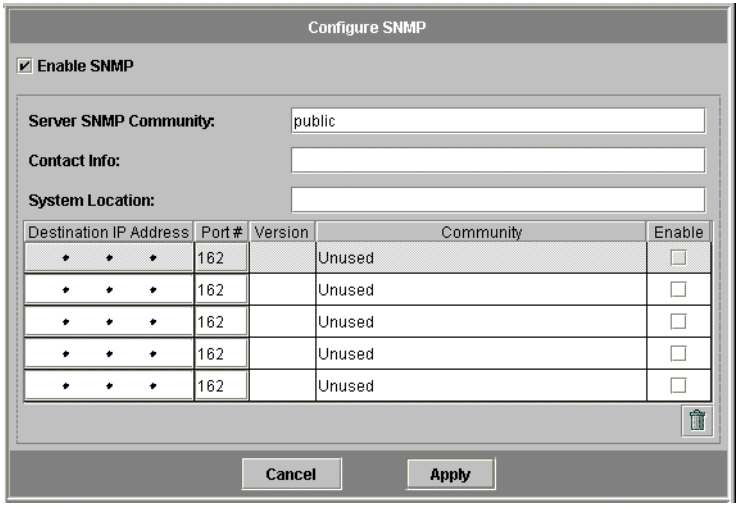
SNMP 通信を使用可能にすることによって、SNMP 監視を実行できます。Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムでは、SNMP 監視のみをサポートしています。SNMP 管理はサポートしていません。

メッセージ情報ブロック (MIB) を解釈するには、MIB ファイルが必要です。MIB ファイルは、イメージとともに *boot_directory*/www/data/mib ディレクトリにインストールされています。たとえば、`/cvol/nf1/www/data/mib` ディレクトリを使用します。

MIB ファイルは、`http://sunsolve.sun.com` からダウンロードすることもできます。これらのファイルの使用方法については、ネットワーク管理アプリケーションのマニュアルを参照してください。

▼ SNMP を設定する

1. ナビゲーションパネルで、「Monitoring and Notification」>「Configure SNMP」を選択します。



2. 「Enable SNMP」チェックボックスを選択して、SNMP を使用可能にします。

3. 「Server SNMP Community」フィールドに、Sun StorEdge 5310 NAS Appliance が属する SNMP コミュニティーを入力します。
4. 「Contact Info」フィールドに、このシステムの管理者名を入力します。
5. 「System Location」フィールドに、ネットワーク上の場所を入力します。

   物理的な場所または論理的な場所のいずれでもかまいません。
6. 新しいターゲットアドレスを追加する場合は、SNMP 表の空白の行に次の情報を入力します。
   - Destination IP Address − システムエラーの発生時に、SNMP トラップ先として指定するサーバーの TCP/IP アドレスを入力します。
   - Port # − システムによってトラップが送信されるポートを入力します。デフォルトのポートは「162」です。
   - Version − プルダウンメニューから SNMP のバージョン (1 または 2) を選択します。
   - Community − トラップ先のコミュニティー文字列を入力します。
   - Enable − このターゲットアドレスをトラップ先として使用可能にする場合は、この列のチェックボックスを選択します。
7. ターゲットアドレスを削除する場合は、削除する行を選択して「Trash」ボタンをクリックします。
8. 「Apply」をクリックして、変更内容を保存します。

システム状態の表示

Web Administrator にはじめてアクセスすると、基本的なシステム状態が表示されます。状態画面はモデルの機能および物理的特徴に基づいて表示されるため、モデルによって異なります。

この画面に表示される情報は、ご購入先に連絡する際に役立ちます。この情報によって障害が発生した場所を特定できる場合もあります。

▼ システム状態を表示する

ツールバーの「Home」ボタンをクリックします。

この画面には、表 10-1 に示すデータが読み取り専用で表示されます。

表 10-1　システム状態の表示

項目	表示
Name	サーバー名
Model	システムモデル
Serial #	システムの一意のシリアル番号
Up Time	システムの電源が最後に投入された時点からの経過時間
CPU Load	プロセッサの現在の負荷および最大負荷
OS Version	サーバーのオペレーティングシステムのバージョン
Web Admin Version	システムの Web Administrator のバージョン
Head Status	サーバー H1 の状態 (Cluster のみ): NORMAL、QUIET、ALONE
Partner Status	サーバー H2 の状態 (Cluster のみ): NORMAL、QUIET、ALONE
Features Enabled	システムで使用可能なすべてのオプション機能

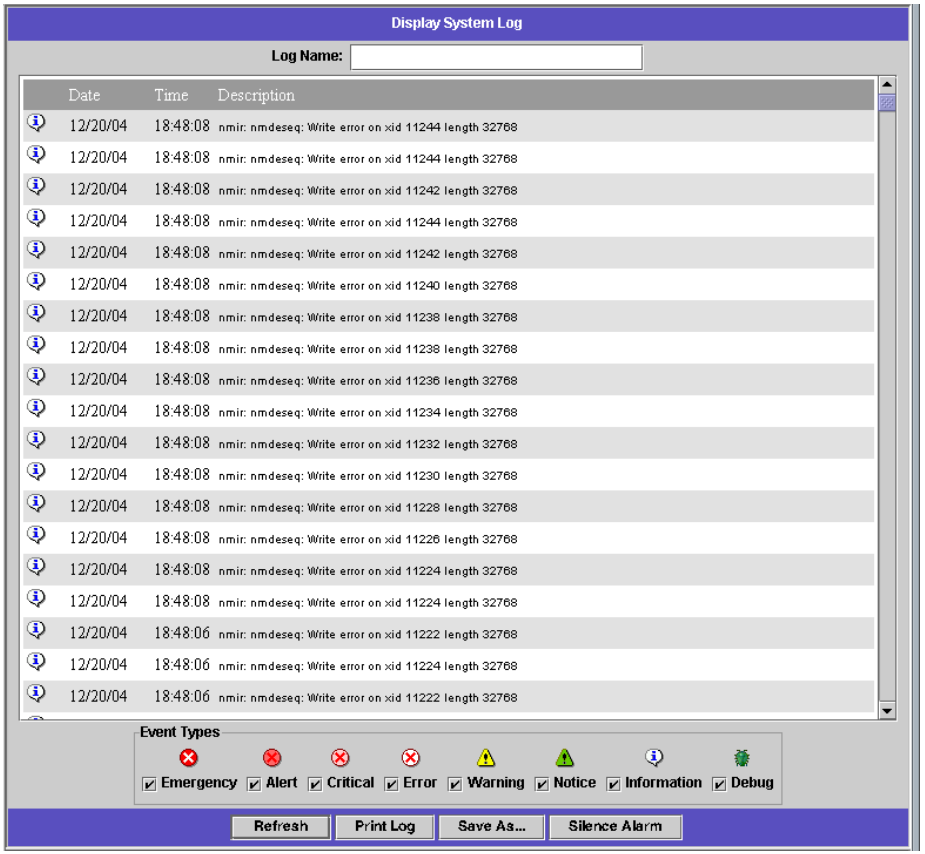
システムログ

システムログには、すべてのシステムイベントの基本情報が表示されます。このログに表示される情報は、発生したエラーおよびその日時を判断する際に重要です。

注意 – システムの停止時にログが消去されないようにするには、遠隔ロギングを使用可能にするか、ローカルディスク上にログファイルを作成する必要があります。システムをはじめて起動するときに、揮発性メモリー内に一時ログファイルが作成され、初期起動中に発生するすべてのエラーが記録されます。

「Display System Log」パネルには、すべてのシステムイベント、警告、エラー、およびそれらの発生日時が表示されます。このパネルには、最新のシステムイベントが自動的に表示され、スクロールバーを使用することで以前のイベントを表示できます。

注 – ドライブ構成の変更 (ドライブの削除、挿入など) は、イベントログに反映されるまでに最大 30 秒かかります。そのため、この時間内に複数の変更を行うと、一部のイベントが報告されない場合があります。



▼ システムログを表示する

1. ナビゲーションパネルで、「Monitoring and Notification」>「View System Events」>「Display System Log」を選択します。
2. 「Event Types」で、表示するすべてのイベントタイプにチェックします。
   詳細は、142 ページの「システムイベント」を参照してください。
3. 「Refresh」をクリックします。

注 – システムログに「Unowned SFS2」ボリュームに関するエラーメッセージが記録された場合は、技術サポートに問い合わせてください。

システムイベント

システムログには、8 つのタイプのシステムイベントが記録されます。各イベントは、表 10-2 に示すアイコンで表されます。

表 10-2　システムイベントのアイコン

	Emergency – 緊急メッセージ。このメッセージは一部のユーザーに送信されます。優先順位が緊急のメッセージは、確認用に別のファイルに記録されます。
	Alert – ただちに対処する必要がある重要メッセージ。このメッセージはすべてのユーザーに送信されます。
	Critical – ハードウェアの問題など、エラーには分類されない重大メッセージ。優先順位が重大以上のメッセージはシステムコンソールに送信されます。
	Error – ディスク書き込みの失敗など、エラーの状態を示すメッセージ。
	Warning – 回復可能な異常に関するメッセージ。
	Notice – 重要な情報メッセージ。優先順位指定のないメッセージは、この優先順位のメッセージに割り当てられます。
	Information – 情報メッセージ。このメッセージはシステムの分析に役立ちます。
	Debug – デバッグに関するメッセージ。

システム監査

システム監査機能は、特定のシステムイベントのレコードをログファイルに格納することによって、システム管理者による監査を可能にします。監査は `syslog` とは異なるもので、システム監査トレールは、ローカルシステム上のバイナリファイルへ書き込まれます。

システム監査は、システム管理者が使用可能に設定し、監査トレール用ストレージボリュームとして構成されたファイルボリュームを使用する必要があります。監査は、Web Administrator、オペレータメニュー、または CLI コマンドによって、使用可能に設定し構成できます。

監査の構成

監査に使用するボリュームを指定する必要があります。監査ボリュームには、システムボリューム以外のボリュームを割り当てることができます。システムには、指定したボリュームを監査目的のみに使用するように強制する機能はありませんが、監査に使用するボリュームを汎用的なストレージとして使用するべきではありません。

監査ログファイルの最大サイズにはデフォルト値が設定されていますが、この値はユーザーが変更できます。現在の監査ログのサイズがこの値に近くなると (差が約 1K バイト以内になると)、そのログファイルは閉じられて新しいログファイルが作成されます。

▼ システム監査を設定する

1. ナビゲーションパネルで、「Monitoring and Notification」>「Enable System Auditing」を選択します。
2. システム監査を使用可能にするには、「Enable System Auditing」チェックボックスを選択します。
3. システム監査ログを格納するボリュームを選択します。

   システムボリューム以外のボリュームを指定できます。専用の監査ボリュームを作成するようにしてください。詳細は、45 ページの「「Create File Volume」パネルを使用してファイルボリュームまたはセグメントを作成する」を参照してください。

4. 1M ～ 1024M バイトの範囲で、監査ログファイルの最大サイズを入力します。

   ログファイルは、0M バイトから指定した最大サイズまで大きくなります。ファイルが最大サイズに達すると、新しい監査ログファイルが作成されます。既存の監査ログファイルは削除されません。ボリュームがしきい値である 90 % に達すると、警告が送信されてログファイルへの書き込みができなくなります。

5. 「Apply」をクリックして設定を保存します。

監査ログファイル

監査ログファイルは、日付およびタイムスタンプと、システムのホスト名を使用した形式になります。現在のログファイルは、*YYYYMMDDhhmmss*`.not_terminated.hostname` の形式になります。

タイムスタンプは、GMT 形式です。たとえば、現在のログファイルが Sun StorEdge 5310 NAS Appliance ホスト (`testhost`) で 2005 年 10 月 21 日午後 1 時 15 分 (GMT) に開始されたとすると、そのファイルは `20051021131500.not_terminated.testhost` になります。

いったんログファイルが閉じられると、そのファイル名は、同じタイムスタンプ形式で変換されます。たとえば、前述の例のログファイルが 2005 年 10 月 30 日午後 7 時 35 分 (GMT) に最大サイズに達した場合、ファイル名は `20051021131500.20051030193500.testhost` と変換されます。

監査ログファイルには、特殊な属性があります。アクセス権がゼロであることに加え、削除できない不変のファイルとしてマークが付けられているため、削除、名前の変更、またはシステム以外からの書き込みが防止されます。これらの属性は、管理者が `chattr` コマンドを使用して削除できます。

注 – 現在、監査ログの読み取りまたは削除に使用する GUI はサポートされていません。

監査対象イベント

監査されるのは少数のイベントに限られます。システムの起動、停止、ディスクパーティションの作成と削除、およびボリュームの作成と削除です。

これらのイベントは設定できません。

監査ログの読み取り

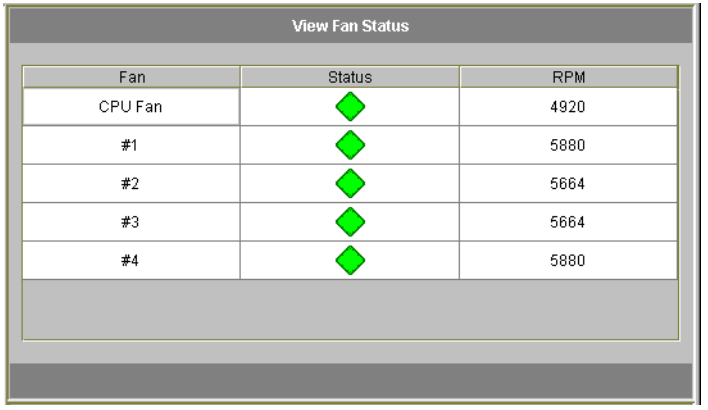
監査ログはバイナリ形式で格納されるため、`praudit` コマンドを使用して読み取る必要があります。`praudit` コマンドによって、監査ログのバイナリ情報が読みやすいテキストに変換されます。

環境状態

システムファン、温度、電源装置、および使用電圧に関する情報を表示できます。

▼ ファンの状態を表示する

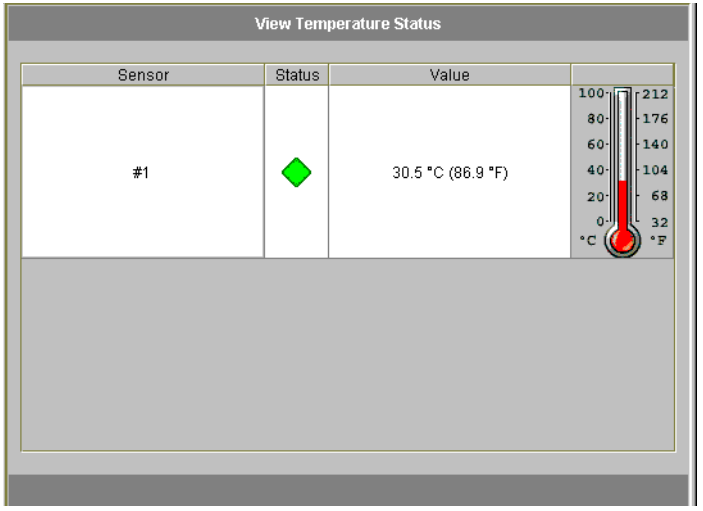
- Sun StorEdge 5310 NAS Appliance の本体装置のすべてのファンの動作状態および 1 分あたりの回転数 (RPM) を表示するには、ナビゲーションパネルで「Monitoring and Notification」>「View Environmental Status」>「View Fan Status」を選択します。



画面には各ファンの現在の状態が表示されます。「Status」列の緑色のひし形は、ファンの RPM が正常であることを示します。赤いひし形は RPM が許容範囲を超えていることを示します。すべてのファンの RPM が 1800 を下回るか、ファンに障害が発生した場合、指定した受信者に電子メールが送信されます。電子メールによる通知の設定については、31 ページの「電子メール通知の設定」を参照してください。

▼ 温度状態を表示する

- 温度状態を表示するには、ナビゲーションパネルで「Monitoring and Notification」>「View Environmental Status」>「View Temperature Status」を選択します。

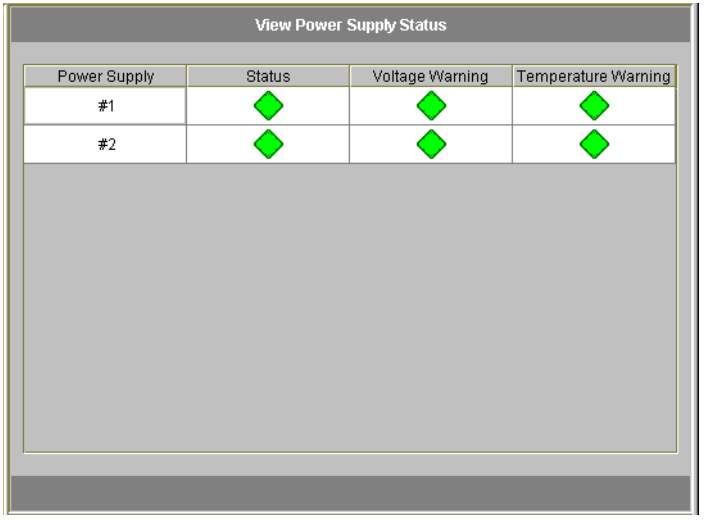


この画面には、本体装置のセンサーの温度が表示されます。「Status」列の緑色のひし形は、装置が正常な温度範囲で動作していることを示します。赤いひし形は温度が許容範囲を超えていることを示します。温度が 55℃ (131ºF) を超えると、指定した受信者に電子メールメッセージが送信されます。電子メールによる通知の設定については、31 ページの「電子メール通知の設定」を参照してください。

注 – 温度のしきい値は変更できません。

▼ 電源装置の状態を表示する

- 電源装置の状態を表示するには、ナビゲーションパネルで「Monitoring and Notification」>「View Environmental Status」>「View Power Supply Status」を選択します。

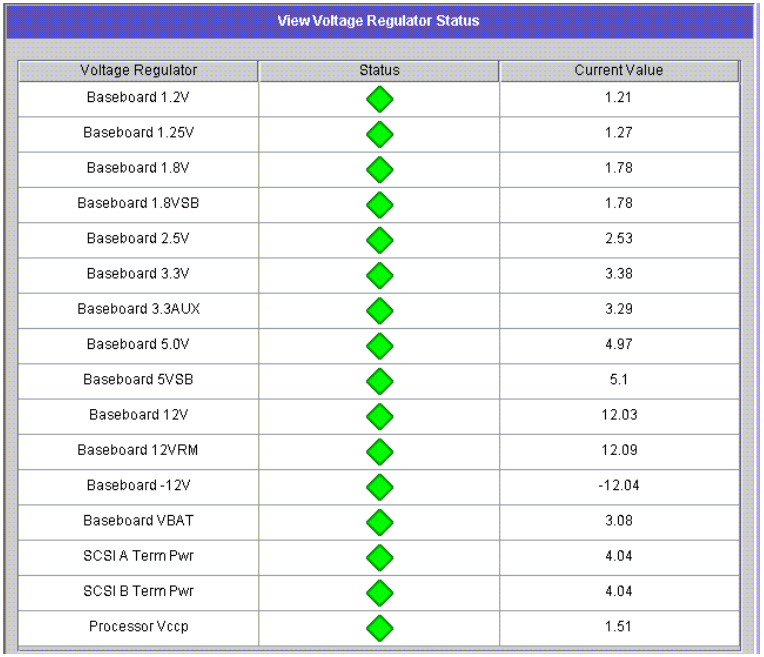


パネルには、電源装置の状態を示す 3 つの列があります。「Status」列には、電源装置が正常に機能しているかどうかが表示されます。「Voltage Warning」列および「Temperature Warning」列には、電圧および温度が許容レベルであるかどうかが表示されます。

これらの列の緑色のひし形は、電圧または温度レベルが正常であることを示します。赤いひし形は、電圧または温度が許容範囲を超えていることを示します。この場合、指定した受信者に電子メールによる通知が行われます。電子メールによる通知の詳細は、31 ページの「電子メール通知の設定」を参照してください。

▼ 電圧状態を表示する

- 現在の電圧値を表示するには、ナビゲーションパネルで「Monitoring and Notification」>「View Environmental Status」>「View Voltage Regulator Status」を選択します。



各電圧の許容範囲については、表 10-3 を参照してください。

表 10-3　　電圧の許容範囲

電圧値	許容範囲
ベースボード 1.2V	1.133V ～ 1.250V
ベースボード 1.25V	1.074V ～ 1.406V
ベースボード 1.8V	1.700V ～ 1.875V
ベースボード 1.8VSB (スタンバイ)	1.700V ～ 1.875V
ベースボード 2.5V	2.285V ～ 2.683V
ベースボード 3.3V	3.096V ～ 3.388V
ベースボード 3.3AUX	3.147V ～ 3.451V

表 10-3　電圧の許容範囲 (続き)

ベースボード 5.0V	4.784V ～ 5.226V
ベースボード 5VSB (スタンバイ)	4.781V ～ 5.156V
ベースボード 12V	11.50V ～ 12.56V
ベースボード 12VRM	11.72V ～ 12.80V
ベースボード –12V	–12.62V ～ –10.97V
ベースボード VBAT	2.859V ～ 3.421V
SCSI A 終端電源	4.455V ～ 5.01V
SCSI B 終端電源	4.455V ～ 5.01V
プロセッサ Vccp	1.116V ～ 1.884V

使用状況

ファイルボリュームの使用状況、ネットワークの動作状態、システムの動作状態、およびネットワークポートを表示できます。

▼ ファイルボリュームの使用量を表示する

- システムのファイルボリュームの使用中の領域および空き領域を表示するには、ナビゲーションパネルで「Monitoring and Notification」を選択します。次に「View File Volume Usage」を選択すると、ファイルボリュームの容量および使用量が表示されます。

  ファイルボリュームの使用量が 95% を超えると、指定した受信者に電子メールが送信されます。

▼ ネットワークの動作状態を表示する

- すべての Sun StorEdge 5310 NAS Appliance クライアントの 1 秒あたりの入出力要求数を表示するには、ナビゲーションパネルから「System Activity」>「View Networking Activity」を選択します。

▼ システムの動作状態を表示する

Sun StorEdge 5310 NAS Appliance は、ストレージシステム全体の複数のデバイスの動作状態および負荷を監視します。監視されているデバイスの名前および数は、ハードウェア構成によって異なります。

- **システムデバイスの入出力要求を表示するには、ナビゲーションパネルで「System Activity」>「View System Activity」を選択します。**

表 10-4 に、システムデバイスおよびネットワークデバイスの一覧を示します。

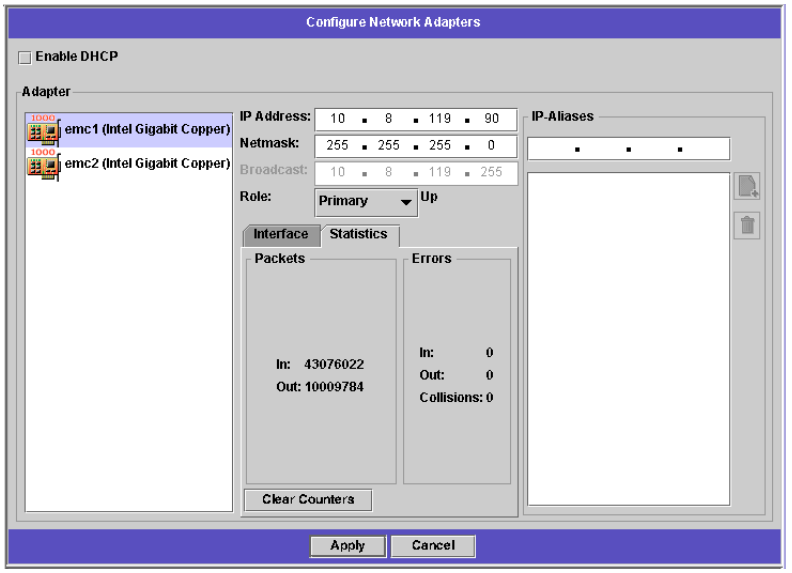
表 10-4 システムデバイスおよびネットワークデバイス

デバイスコード	デバイス
CPU	Sun StorEdge 5310 NAS Appliance の中央処理装置 (CPU)
Memory	Sun StorEdge 5310 NAS Appliance システムのランダムアクセスメモリー (RAM)
Port Aggregation *x*	ポート結合 *x*
Controller *x*	RAID コントローラ *x*
dac010*xx*	論理ユニット番号 (LUN) *xx*
PORT*x*	ポート *x*
Host Adapter *x*	SCSI ホストアダプタ *x* (テープバックアップデバイス用)

▼ ネットワーク (ポート) 統計情報を表示する

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」を選択します。

   ネットワーク統計情報の画面が表示されます。



2. 「Adapter」リストからポートを選択します。

   「Interface」タブに次の情報が表示されます。

   - Description ― 選択したポートの説明。
   - H/W Address ― 一意のハードウェア (H/W) アドレスまたはメディアアクセス制御 (MAC) アドレス (16 進数)。このネットワークカードとネットワーク上のほかのカードを区別するためにネットワークソフトウェアで使用されます。このアドレスは、出荷時にネットワークカード上で符号化されています。
   - Speed ― ネットワーク上のデータ転送速度 (M ビット/秒)。
   - MTU ― 選択したアダプタの現在の MTU (最大転送単位)。MTU は物理媒体上で送信できるフレームの最大長です。MTU の最大値はデフォルトの 1500 です。最小値には 552 を使用します。

     TCP の最大セグメントサイズは、IP の最大データグラムサイズから 40 を引いた値です。デフォルトでは、IP の最大データグラムサイズは 576、TCP の最大セグメントサイズは 536 です。

3. 「Statistics」タブをクリックして、選択したポートに関する次の入出力情報を表示します。

   - Packets In/Out ― このポートの入出力 (送受信) パケット数。

- Errors In/Out ― このポートの入出力エラー数。
- Collisions ― このポートの転送衝突数。

ネットワークルートの表示

「View the Routing Table」パネルでは、ネットワークおよびホストにパケットが送信されるルートを確認できます。これらのルートは、宛先ネットワークおよびルートエントリへの参照で構成されます。

ルーティングの概要

ルートには、「ネットワークルート」と「ホストルート」の 2 種類があります。ネットワークルートは、特定のネットワーク上のホストへのパケット送信に使用されます。ホストルートは頻繁には使用されません。このルートは、既知のネットワークではなく、ほかのホストまたはゲートウェイにのみ接続されているホストへのパケット送信に使用されます。

ルーティングテーブルに表示されるルートフラグの例を次に示します。

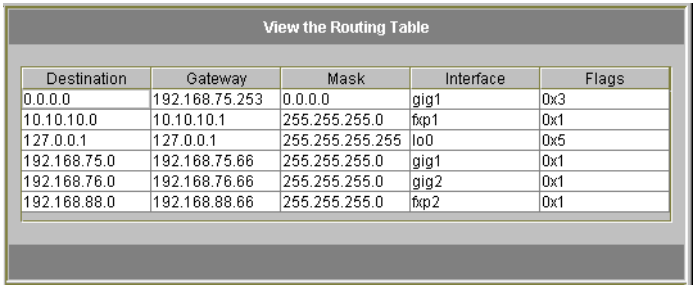
- 0x1 ― ルートは使用可能です。
- 0x2 ― 宛先はゲートウェイです。
- 0x4 ― 宛先はホストエントリです。
- 0x8 ― ホストまたはネットワークに到達できません。
- 0x10 ― 宛先が動的に作成されました。
- 0x20 ― 宛先が動的に変更されました。

フラグには、個々のフラグの合計を示すものもあります。たとえば、「0x3」は「0x1」と「0x2」の合計で、ルートが使用可能であることと宛先がゲートウェイであることを表しています。

▼ ルートを表示する

ローカルネットワーク内のすべてのルートの状態を表示するには、ナビゲーションパネルで「Network Configuration」>「View the Routing Table」を選択します。

「View the Routing Table」パネルが表示されます。



この画面には、各ネットワークルートに関する次の情報が表示されます。

- Destination − ルートの宛先 IP アドレス。ネットワークまたはホストのいずれかを指します。デフォルトのルートが 1 つ (0.0.0.0 指定)、ループバックルートが 1 つ (127.0.0.1 指定)、ネットワークルートが 1 つ以上、およびホストルートが 1 つ以上存在するようにしてください。
- Gateway − パケットが宛先に送信される際のゲートウェイアドレス。
- Mask − 宛先ネットワークのネットマスク。
- Interface − ネットワーク上のパケット送信に使用されるインタフェースタイプ。
- Flags − ルートの状態を表すフラグ。状態フラグは 16 進数で表されます。詳細は、152 ページの「ルーティングの概要」を参照してください。

システムコンポーネントの監視

無停電電源装置 (UPS)、コントローラ、およびミラーの状態を監視できます。

UPS 監視

UPS を持つ装置を設置した場合は、UPS を監視することができます。

注 – UPS を監視するには、Sun StorEdge 5310 NAS Appliance システムに UPS を接続しておく必要があります。UPS が接続されていないと、監視システムは UPS 障害を通知します。Sun StorEdge 5310 NAS Appliance では UPS 監視のみをサポートしており、UPS 管理はサポートしていません。UPS の使用方法の詳細は、『Sun StorEdge 5310 NAS Appliance および Gateway システムご使用の手引き』を参照してください。

UPS 監視機能

UPS 監視では、次の場合に通知が行われます。

- **電源障害** − 電源障害が発生し、システムがバッテリの電力で動作しています。
- **電源の復旧** − 電源が復旧しました。
- **バッテリ低下** − バッテリの電力が低下しています。
- **バッテリ充電完了** − UPS のバッテリが正常レベルまで充電されました。
- **バッテリ交換** − UPS のバッテリに異常が検出されたため、交換が必要です。
- **UPS アラーム** − UPS の周辺温度または湿度が正常なしきい値の範囲外であることが検出されました。
- **UPS 障害** − システムが UPS と通信できません。

バッテリ充電完了以外のすべてのエラーは、エラー通知電子メール、SNMP サーバー、LCD パネル、およびシステムログによって通知されます。バッテリ充電完了は、電子メール、SNMP サーバー、およびシステムログでのみ通知されます。LCD パネルには表示されません。

▼ UPS 監視を使用可能にする

1. ナビゲーションパネルで、「Monitoring and Notification」>「Enable UPS Monitoring」を選択します。
2. 「Enable UPS monitoring」を選択します。
3. 「Apply」をクリックして、変更内容を保存します。

コントローラ情報の表示

「View Controller Information」パネルには、コントローラのベンダー、モデル、およびファームウェアリリースが読み取り専用で表示されます。

▼ コントローラのベンダー、モデル、およびファームウェアリリースを表示する

ナビゲーションパネルから、「RAID」>「View Controller Information」を選択します。

ミラー化の状態の表示

Sun StorEdge 5310 NAS Appliance では、ミラー化されたファイルボリュームのさまざまなネットワーク統計情報が保持されます。ミラー化された各ファイルボリュームに関するこれらの統計情報は、アクティブサーバーおよびミラーサーバー上で確認できます。

▼ ミラーの統計情報を表示する

1. ナビゲーションパネルから、「File Replicator」>「View Mirror Statistics」を選択します。

2. 「Select Volume」リストから、目的のファイルボリュームを選択します。

   ミラー化されたファイルボリュームに関する次の情報が表示されます。

   - Status − ミラーの状態が表示されるフィールド。表示される状態の定義については、156 ページの「**ミラーの状態**」を参照してください。
   - Incoming Transactions – 選択したファイルボリュームに関する次の統計情報が表示されるセクション。
     - Average − アクティブサーバーに送信される 1 秒あたりの平均トランザクション数。
     - Minimum − アクティブサーバーに送信された 1 秒あたりの最小トランザクション数。トランザクション数が最小になった日時が右側に表示されます。
     - Maximum − アクティブサーバーに送信された 1 秒あたりの最大トランザクション数。トランザクション数が最大になった日時が右側に表示されます。
   - Outgoing Transactions − 選択したファイルボリュームに関する次の統計情報が表示されるセクション。
     - Average − アクティブサーバーからミラーサーバーに送信される 1 秒あたりの平均トランザクション数。
     - Minimum − アクティブサーバーからミラーサーバーに送信された 1 秒あたりの最小トランザクション数。トランザクション数が最小になった日時が右側に表示されます。
     - Maximum − アクティブサーバーからミラーサーバーに送信された 1 秒あたりの最大トランザクション数。トランザクション数が最大になった日時が右側に表示されます。
   - Mirror Buffer − ミラーバッファーに関する次の情報が表示されるセクション。
     - Size − バッファーに保持できる最大トランザクション数。
     - Free − ミラーバッファー内に残っているトランザクション数。
     - Utilization − ミラーバッファー内で使用されるトランザクションの割合。
     - Fill Rate − ミラーバッファーの流入速度 (1 秒あたりのトランザクション)。流入速度が 0 より大きい場合は、すべてのネットワーク接続が正常に機能していることを確認する必要があります。この場合、アクティブシステムへのトランザクションの送信速度がミラーシステムへの送信速度を上回っているため、バッファーがいっぱいになります。
   - Network Statistics − ミラーバッファーに関する次のネットワーク統計情報が表示されるセクション。
     - Host − ミラーバッファーのホスト名および接続状態。
     - Link − ミラーバッファーの状態、特性、およびその他の接続の統計情報。
     - Request Control Blocks − 送信された制御ブロック数、送信されたバイトの合計数、平均サイズ、および平均速度。
     - Transfer Rate − 転送の平均速度、最大速度、および最大速度での転送が行われた日時。
     - Response Time − 平均応答時間、最大応答時間、および応答時間が最大となった日時。

ミラーの状態

ミラーの状態は「Manage Mirrors」パネルに表示されます。ミラーの状態には、次のようなものがあります。

- New − 新しいミラーを作成しています。
- Creating mirror log − ミラーバッファーを初期化しています。
- Connecting to host − アクティブサーバーは遠隔ミラーサーバーに接続しています。
- Creating extent − ミラーサーバーでディスクパーティションを作成しています。
- Ready − システムの準備が完了して、ほかのシステムの準備完了を待機しています。
- Down − ネットワーク接続が切断されています。
- Cracked − ミラーが破損しています。
- Syncing Volume − ミラーサーバーがファイルボリュームと同期をとっています。
- In Sync − ミラーは同期がとれています。
- Out of Sync − ミラーは同期がとれていません。
- Error − エラーが発生しました。

バックアップジョブの状態の表示

ログ、ジョブの状態、テープの状態などの、バックアップジョブに関する情報を表示できます。

▼ バックアップログを表示する

ナビゲーションパネルから、「System Backup」>「Manage Backup Jobs」>「View Backup Log」を選択します。

バックアップログには、システムバックアップ処理で発生したイベントの全リストが表示されます。ログには各イベントの発生日時および説明も含まれます。以前のバックアップイベントを表示する場合は、上にスクロールしてください。

ファイルの合計サイズは画面上部に表示されます。「Refresh」をクリックすると、ログファイルの表示が更新されます。

▼ ジョブの状態を表示する

ナビゲーションパネルで、「System Backup」>「Manage Backup Jobs」>「View Backup Status」を選択します。

画面には、最新のバックアップ、復元、およびクリーニング処理が表示されます。

バックアップ処理または復元処理の実行中は、「Abort Job」ボタンが使用可能になります。実行中の処理を停止する場合は、このボタンをクリックし、状態パネルでジョブが取り消されたことを確認します。ジョブが実際に取り消されるまでには数分かかります。

▼ テープの状態を表示する

1. ナビゲーションパネルで、「System Backup」>「Manage Backup Jobs」>「View Tape Status」を選択します。
2. 表示するテープ情報を選択します。
   - 特定のテープに関する情報を表示するには、「Choose Tape Slot」オプションを選択します。次に、表示するテープに対応するスロットをリストから選択します。

     この画面では、スロット番号は 1 から開始されます。ただし、テープバックアップデバイスによって、スロット番号が異なる場合があります。テープデバイスのスロット番号が 0 (ゼロ) から開始されている場合は、この画面でスロット 1 を選択すると、テープデバイスのスロット 0 に関する情報が表示されます。
   - テープデバイス内のすべてのテープに関する情報を表示するには、「All Slots」を選択します。

     システムでテープ情報が取得され、画面下部の領域に表示されるまでに、スロットあたり 1 ～ 2 分を要します。「All Slots」を選択すると、情報の取得にかかる時間がたいへん長くなります。バックアップ、復元、またはヘッドクリーニング処理の実行中は、テープデバイスでスロット情報を取得できません。
3. 「Apply」をクリックして、テープの検出を開始します。

注 – バックアップ、復元、またはヘッドクリーニング処理の実行中は、このデータを表示できません。

第 11 章

システムの保守

この章では、システムの保守機能について説明します。

この章の内容は、次のとおりです。

遠隔アクセスオプションの設定

システムのセキュリティー機能を使用して、遠隔アクセスオプションを設定できます。システムへの遠隔アクセスに使用するネットワークサービスを使用可能または使用不可に設定できます。セキュリティー保護されたモードでシステムを実行して安全性を最大限に高めたり、Telnet、遠隔ログイン、リモートシェルなどの特定の遠隔アクセス機能を使用可能にしたりすることができます。

セキュリティー保護されたサービスは、HTTP 上で SSL (Secure Sockets Layer) を使用する Secure Web Admin、および Secure Shell (ssh) です。

▼ 遠隔アクセスセキュリティーを設定する

1. ナビゲーションパネルで、「System Operations」>「Set Remote Access」を選択します。
2. 安全性を最大限に高めるには、「Secure Mode」チェックボックスを選択します。「Secure Mode」では、該当するチェックボックスを選択して Secure Web Admin および Secure Shell のみを使用可能にできます。
3. 「Secure Mode」を選択しない場合は、次のうちから使用可能にするサービスのチェックボックスを選択します。
   - Web Admin
   - Telnet
   - Remote Login
   - Remote Shell
4. 「Apply」をクリックします。
5. 「Secure Mode」を選択した場合、サーバーを再起動して設定を有効にする必要があります。詳細は、162 ページの「サーバーの停止」を参照してください。

FTP アクセスの構成

ファイル転送プロトコル (FTP) は、クライアントとサーバー間でファイルをコピーするために使用されるインターネットプロトコルです。FTP では、サーバーへのアクセスを要求する各クライアントを、ユーザー名およびパスワードで識別する必要があります。

次の 3 つのタイプのユーザーを設定できます。

- **管理者** − admin というユーザー名を持ち、GUI クライアントと同じパスワードを使用します。

  管理者は、システム上のすべてのボリューム、ディレクトリ、およびファイルにスーパーユーザーでアクセスできます。管理者のホームディレクトリは、「/」記号と定義されます。

- **ユーザー** − ローカルのパスワードファイルまたは遠隔 NIS、NIS+、または LDAP ネームサーバーに指定されているユーザー名およびパスワードを持ちます。

  ユーザーは、自身のホームディレクトリに含まれるすべてのディレクトリおよびファイルへのアクセス権を持ちます。ホームディレクトリは、ユーザーのアカウント情報の一部として定義され、ネームサービスによって取得されます。

- **ゲスト** – 「ftp」というユーザー名または「anonymous」というエイリアスを使用してログインします。パスワードが要求されますが、認証されません。すべてのゲストユーザーは、ftp ユーザーのホームディレクトリに含まれるすべてのディレクトリおよびファイルへのアクセス権を持ちます。

注 – ゲストユーザーは、ファイルの名前の変更、上書き、または削除を行うことができません。また、ディレクトリの作成または削除、および既存のファイルまたはディレクトリのアクセス権の変更を行うこともできません。

▼ FTP ユーザーを設定する

1. ナビゲーションパネルで、「UNIX Configuration」>「Set Up FTP」を選択します。
2. 「Enable FTP」チェックボックスを選択します。
3. 該当するチェックボックスをクリックして、FTP アクセスのタイプを選択します。
   - 「Allow Guest Access」を選択すると、匿名ユーザーによる FTP サーバーへのアクセスが可能になります。
   - 「Allow User Access」を選択すると、すべてのユーザーによる FTP サーバーへのアクセスが可能になります。これには、admin ユーザーまたはスーパーユーザーは含まれません。

注 – ローカルのパスワードファイル、または遠隔 NIS、NIS+、LDAP ネームサーバーに、ユーザー名およびパスワードが指定されている必要があります。

   - 「Allow Admin Access」を選択すると、管理パスワードでの、FTP サーバーへのスーパーユーザーとしてのアクセスが可能になります。管理パスワードの使用には注意が必要です。

注 – スーパーユーザーとは、UID が 0 に設定されているユーザー、および Sun StorEdge 5310 NAS Appliance の特別なユーザーである admin を示します。

---

4. ロギングを使用可能にするには、「Enable Logging」チェックボックスを選択して、ログファイル名を指定します。
5. 「Apply」をクリックして設定を保存します。

サーバーの停止

「Shut Down the Server」パネルを使用して、サーバーを停止または再起動できます。Telnet を使用したシステムの停止方法については、238 ページの「システムを停止する」を参照してください。

▼ サーバーを停止または再起動する

1. ナビゲーションパネルで、「System Operations」>「Shut Down the Server」を選択します。
2. 次のいずれかのオプションを選択します。
   - None − サーバーを停止しません。
   - Halt Both Heads − クラスタ構成のサーバーを両方とも停止します。再起動するには、サーバーに手動で電源を入れる必要があります。
   - Reboot Both Heads − クラスタ構成のサーバーを両方とも停止して再起動します。
   - Reboot Previous Version − サーバーを停止して、以前にロードされたバージョンのソフトウェアを使用して再起動します。たとえば、ソフトウェアのアップグレード時に問題が発生した場合に、このオプションを使用します。このオプションを使用すると、アップグレード前に最後に使用したソフトウェアでサーバーを再起動できます。

注意 – 「Reboot Previous Version」オプションを選択する前に、技術サポートに確認してください。

   - Halt This Head − 現在ログオンしているサーバーを停止します。もう一方のサーバーはオンラインのままです。再起動するには、サーバーに手動で電源を入れる必要があります。
   - Reboot This Head − 現在ログオンしているサーバーを停止して再起動します。もう一方のサーバーはオンラインのままです。
3. 「Apply」をクリックします。

ファイルのチェックポイント

チェックポイント (「整合点」または「c 点」とも呼ばれる) は、一次ファイルボリュームの読み取り専用の仮想コピーです。ファイルボリュームに対する読み取り / 書き込み操作は引き続き行われますが、チェックポイントの作成時に存在したデータをすべて使用することができます。チェックポイントを使用して、誤って変更または削除したファイルを取得したり、バックアップの一貫性を確保したりします。

注 – チェックポイントはファイルボリュームの仮想コピーで、そのボリュームと物理的に同一の場所に格納されます。オンラインバックアップではありません。ファイルボリュームが失われると、チェックポイントもすべて失われます。

ファイルのチェックポイントを使用するには、チェックポイントを使用可能にして個々のチェックポイントを作成するか、またはチェックポイントのスケジュールを設定します。

ファイルのチェックポイントの作成

チェックポイントのスケジュールを設定するか、即時にチェックポイントを作成するかを選択できます。定期的なチェックポイントスケジュールの設定方法については、164 ページの「ファイルのチェックポイントのスケジュール設定」を参照してください。

「Manage Checkpoints」パネルで、チェックポイントを即時に作成したり、既存のチェックポイントの名前の変更および削除を実行したりすることができます。事前に設定した日時に作成されるようにスケジュール設定されたチェックポイントとは異なり、この画面でいつでもチェックポイントを即時に作成できます。

▼ 新しいチェックポイントを手動で作成する

1. **ナビゲーションパネルで、「File Volume Operations」>「Edit Properties」を選択します。**
2. **「Volume Name」プルダウンメニューから、チェックポイントを作成するボリュームを選択します。**
3. **「Enable Checkpoints」ボックスにチェックマークが表示されていることを確認します。**

   表示されていない場合は、ボックスを選択して「Apply」をクリックします。
4. **ナビゲーションパネルで、「File Volume Operations」>「Configure Checkpoints」>「Manage Checkpoints」を選択します。**

5. 新しいチェックポイントを作成するには、「Create」をクリックします。
6. 「Volume Name」プルダウンメニューから、チェックポイントを作成するボリュームを選択します。
7. 次のいずれかのチェックポイントオプションを選択します。
   - Auto Delete － 「Keep Days」および「Keep Hours」で指定した期間を経過すると、チェックポイントが自動的に削除されます。このオプションでは、チェックポイントの名前がシステムによって自動的に割り当てられます。このオプションを選択する場合、チェックポイントが保持される日数および時間を選択します。
   - Backup － このオプションでは、チェックポイントのデフォルトの名前が「Backup」になります。チェックポイントは、Sun StorEdge 5310 NAS Appliance ファイルシステムのローカルバックアップに使用されます。特定の期間が経過しても、チェックポイントは自動的には削除されません。
   - Manual － チェックポイントに「Backup」以外の名前を指定する場合は、このオプションを選択します。「Name」フィールドに名前を入力します。特定の期間が経過しても、チェックポイントは自動的には削除されません。
8. 「Apply」をクリックして、チェックポイントを作成します。

ファイルのチェックポイントのスケジュール設定

「Schedule Checkpoints」パネルには現在のチェックポイントスケジュールが表示され、スケジュール設定されたチェックポイントを追加、編集、および削除できます。この画面には、スケジュール設定された各チェックポイントのファイルボリューム名、説明、設定日時、およびチェックポイントが保持される期間が表示されます。「Keep」の期間は、日数と時間で表示されます。

スケジュールの行を追加すると、要求した日時のチェックポイントがシステムで自動的に設定されます。

ボリュームごとに、最大 5 つのチェックポイントのスケジュールを設定できます。1 つのスケジュールに複数のチェックポイントを指定できます。

複数のチェックポイントの例を次に示します。

			Days	Hours AM	Hours PM	Keep	
	Enabled	Description	SMTWTFS	M1234567890E	M1234567890E	Days	+ Hours
1.	Y	MTWTF5am5pm	-*****-	-----*------	-----*------	1	0
2.	Y	SunWed1pm	*--*---	----------	-*----------	0	12
3.	Y	MWFmidnight	-*-*-*-	*----------	----------	0	3
4.	Y	Weekend	*-----*	*-----*-----	*-----*-----	0	6
5.	Y	FriEvery2hrs	-----*-	*-*-*-*-*-*-	*-*-*-*-*-*-	0	2

▼ チェックポイントをスケジュールに追加する

1. ファイルボリュームのチェックポイントを使用可能にします。

   a. ナビゲーションパネルで、「File Volume Operations」>「Edit Properties」を選択します。

   b. 「Volume Name」プルダウンメニューから、チェックポイントを追加するボリュームを選択します。

   c. 「Enable Checkpoints」ボックスにチェックマークが表示されていることを確認します。

   表示されていない場合は、ボックスを選択して「Apply」をクリックします。

2. ナビゲーションパネルで、「File Volume Operations」>「Configure Checkpoints」>「Schedule Checkpoints」を選択します。

3. スケジュールにチェックポイントを追加するには、「Add」をクリックします。

4. チェックポイントをスケジュール設定するファイルボリュームを選択します。

5. 「Description」にチェックポイントの説明を入力します。

   これは必須フィールドです。たとえば、「毎週」、「毎日」など、チェックポイントの間隔を入力します。

6. 「Keep Days + Hours」ドロップダウンリストから、チェックポイントを保持する日数および時間を選択します。

7. 「Days」リストから、チェックポイントを作成する曜日を選択します。

   このリストから複数の曜日を選択するには、Ctrl キーを押しながら追加の曜日をマウスでクリックします。

8. 「AM Hours」リストから、チェックポイントを作成する時間 (午前) を選択します。

   このリストから複数の項目を選択するには、Ctrl キーを押しながら追加の項目をマウスでクリックします。

9. 「PM Hours」リストから、チェックポイントを作成する時間 (午後または夜) を選択します。

   このリストから複数の項目を選択するには、Ctrl キーを押しながら追加の項目をマウスでクリックします。

10. 「Apply」をクリックして、変更内容を保存します。

▼ 既存のチェックポイントスケジュールを編集する

1. ナビゲーションパネルで、「File Volume Operations」>「Configure Checkpoints」>「Schedule Checkpoints」を選択します。

2. 編集するスケジュールの行を選択し、「Edit」をクリックします。

3. この画面に表示される情報は「Add Checkpoint Schedule」ダイアログボックスの情報と同じですが、ボリューム名は変更できません。

4. 関連する情報を編集します。

   詳細は、165 ページの「チェックポイントをスケジュールに追加する」を参照してください。

5. 「Apply」をクリックして、変更内容を保存します。

▼ スケジュールの行を削除する

1. ナビゲーションパネルで、「File Volume Operations」>「Configure Checkpoints」>「Schedule Checkpoints」を選択します。

2. 削除するスケジュールの行をクリックして選択し、「Remove」をクリックします。

▼ チェックポイントの名前を変更する

1. ナビゲーションパネルで、「File Volume Operations」>「Configure Checkpoints」>「Manage Checkpoints」を選択します。

2. 名前を変更するチェックポイントを選択し、「Rename」をクリックします。

   「Volume Name」および「Old Name」フィールドは読み取り専用です。

3. 「New Name」にチェックポイントの新しい名前を入力します。

注意 – 「Auto Delete」を指定したチェックポイントの名前を通常の名前に変更すると、そのチェックポイントには自動削除が実行されなくなります。

4. 「Apply」をクリックして、変更内容を保存します。

▼ チェックポイントを削除する

1. ナビゲーションパネルで、「File Volume Operations」>「Configure Checkpoints」>「Manage Checkpoints」を選択します。

2. 削除するチェックポイントを選択し、「Remove」をクリックします。

ファイルのチェックポイントの共有

ユーザーはチェックポイントを共有して、チェックポイント作成時のデータにアクセスできます。

▼ ファイルのチェックポイントを共有する

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 「Add」をクリックします。
3. 「Share Name」ボックスに、チェックポイントの新しい共有名を入力します。
   共有名は、ネットワークからチェックポイントにアクセスするために使用されます。
4. 「Mac Extensions」オプションは、デフォルトで選択されています。
5. 「Volume Name」プルダウンメニューボックスをクリックし、リストからチェックポイントボリュームを選択します。
   チェックポイントボリュームには、.chkpnt 拡張子が付いています。
6. 「Directory」フィールドは、空白のままでかまいません。
7. ADS が使用可能で構成済みの場合は、「Container」テキストボックスに ADS コンテキストを入力します。
8. システムが NT ドメインモード用に構成されている場合、次のフィールドおよびオプションはグレー表示されます。グレー表示されていない場合は、次のように入力します。
   a. 「User」ボックスに 0 と入力します。
   b. 「Group」ボックスに 0 と入力します。
   c. 「R/W Password」および「R/O Password」ボックスは、空白のままにしておきます。
      チェックポイントボリュームは読み取り専用です。
9. 「Apply」をクリックします。
   「Configure Shares」パネルに、新しいチェックポイントが共有チェックポイントとして表示されていることを確認します。

ファイルのチェックポイントへのアクセス

ユーザーはチェックポイントにアクセスして、チェックポイント作成時のデータにアクセスできます。

▼ チェックポイントにアクセスする

1. ネットワークステーションを使用して、Windows の「スタート」メニューをクリックします。

2. 「ファイル名を指定して実行」を選択します。
3. 「ファイル名を指定して実行」ダイアログボックスで、Sun StorEdge 5310 NAS Appliance サーバーの IP アドレスおよびチェックポイントの共有名を入力します。
   たとえば、「`\\xxx.xxx.xxx.xxx\sharename`」と入力します。
4. 「OK」をクリックします。

バックアップおよび復元

Sun StorEdge 5310 NAS Appliance システムでは、NDMP ネットワークバックアップがサポートされています。

NDMP の設定

NDMP (Network Data Management Protocol) は、ネットワークベースのバックアップ用のオープンなプロトコルです。NDMP アーキテクチャーによって、NDMP 準拠のバックアップ管理アプリケーションを使用して、ネットワーク接続ストレージデバイスをバックアップできます。

注 – バックアップ管理アプリケーションは、コンソール管理者がコマンド行インタフェースで使用するユーザー名「administrator」とそのパスワードでログオンするように構成することをお勧めします。

注 – NDMP を使用してバックアップを実行するボリュームでは、チェックポイントを使用可能にしておく必要があります。詳細は、163 ページの「ファイルのチェックポイントの作成」を参照してください。

▼ NDMP を設定する

1. ナビゲーションパネルで、「System Backup」>「Set Up NDMP」を選択します。
2. バックアップテープドライブへのデータ転送に使用する「NDMP NIC」を選択します。

3. 各ポートのゲートウェイアドレスが表示されます。

   NDMP バックアップテープデバイスが別のネットワークに存在する場合は、適切なゲートウェイに接続するポートを選択する必要があります。

4. 「Apply」をクリックします。

CATIA V4/V5 の文字変換

Sun StorEdge 5310 NAS Appliance および Gateway システムは、Dessault Systemes 社が開発した CATIA V4/V5 製品と相互運用できます。

CATIA V4 は UNIX のみに対応する製品ですが、CATIA V5 は UNIX および Windows の両方のプラットフォームで使用できます。CATIA V4 では、ファイル名に Windows では使用できない文字を使用する可能性があります。CATIA ユーザーが V4 から V5 に移行する際、V4 のファイル名に Windows では使用できない文字が含まれていると、Windows から V4 のファイルにアクセスできなくなる場合があります。そのため、CATIA V4/V5 では文字変換オプションを提供することにより、UNIX/Windows の相互運用性を維持しています。

表 11-1 に、変換表を示します。

表 11-1 CATIA 文字変換表

CATIA V4 の UNIX 文字	CATIA V5 の Windows 文字	CATIA V5 の文字の説明
曲線的な開き二重引用符 (表示不可)	¨	ウムラウト
*	¤	通貨記号
/	ø	ローマ字の小文字 O とスラッシュ
:	÷	除算記号
<	«	左角引用符
>	»	右角引用符
?	¿	逆疑問符
\	ÿ	ローマ字の小文字 Y とウムラウト
|	破線垂直バー (表示不可)	破線垂直バー

CATIA V4/V5 の相互運用性サポートは、デフォルトで使用不可になっています。この機能は、CLI を介して手動で使用可能にするか、システム起動後自動的に使用可能にすることができます。

▼ CLI を使用して CATIA を使用可能にする

- CLI コマンドの `load catia` を実行します。この方法を使用する場合は、システムを再起動するたびに CATIA サポートを使用可能にする必要があります。

▼ 再起動時に自動的に CATIA を使用可能にする

1. `/dvol/etc/inetload.ncf` を編集して、ファイル内に新しい行を挿入し `catia` という語を追加します。
2. 次の 2 つの CLI コマンドを実行して `inetload` サービスを再開します。

```
unload inetload
load inetload
```

CATIA V4/V5 サポートが正常に使用可能になると、次のようなエントリがシステムログに表示されます。

```
07/25/05 01:42:16 I catia: $Revision: 1.1.4.1
```

ヘッドクリーニングの実行

最後に実行したヘッドクリーニングに関する情報を表示するか、ローカルテープデバイスの次のヘッドクリーニングを設定することができます。

▼ ヘッドクリーニングを実行する

1. ナビゲーションパネルで、「System Backup」>「Assign Cleaning Slot」を選択します。

2. **このヘッドクリーニング用のクリーニングテープが挿入されているスロット番号を選択します。**

   この画面では、スロット番号は 1 から開始されます。ただし、テープバックアップデバイスによって、スロット番号が異なる場合があります。テープデバイスのスロット番号が 0 (ゼロ) から開始されている場合は、この画面でスロット 1 を選択すると、テープデバイスのスロット 0 に関する情報が表示されます。

3. **「Cleaning Count」にクリーニング回数を割り当てて、クリーニングテープがヘッドクリーニングに使用される回数を記録します。**

   クリーニングテープは、10 回使用したら破棄してください。この項目の値は、ヘッドクリーニングを実行するたびに増加します。

4. **ヘッドクリーニングをすぐに実行するには、「Run Immediately」チェックボックスを選択し、スロット番号およびクリーニング回数を指定してテープクリーニングを開始します。**

5. **「Apply」をクリックして、変更内容を保存します。「Run Immediately」チェックボックスを選択した場合は、この時点でクリーニングが開始されます。**

Sun StorEdge 5310 NAS Appliance ソフトウェアの更新

使用するシステム構成用の適切な更新ファイルを取得するには、ご購入先にお問い合わせください。ファイルを入手したら、「Update Software」パネルを使用して Sun StorEdge 5310 NAS Appliance ソフトウェアを更新します。

注意 – RAID サブシステムで重大な障害が発生しているときに、システムソフトウェアまたは RAID ファームウェアを更新して、新しいボリュームを作成したり既存のボリュームを再構築したりしないでください。

▼ ソフトウェアを更新する

次の手順では、更新処理の完了後にシステムを再起動する必要があります。システムを再起動するにはすべての入出力を停止する必要があるため、ソフトウェアの更新は計画した保守期間内に実施してください。

注 – クラスタ構成では、クラスタ内の両方のサーバーでこの手順を実行してください。

1. **ナビゲーションパネルで、「System Operations」>「Update Software」を選択します。**
2. **「Update Software」パネルで、更新ファイルが格納されている場所へのパスを入力します。**

   パスを検索する必要がある場合は、「Browse」をクリックします。
3. **「Update」をクリックして処理を開始します。**
4. **更新処理が完了したら、「Yes」をクリックしてシステムを再起動するか、「No」をクリックして再起動せずに操作を続行します。**

   更新内容は、システムを再起動すると有効になります。

アレイおよびドライブのファームウェアバージョンのアップグレード

この節では、アレイおよびドライブの現在のファームウェアバージョンの確認方法と、ファームウェアのアップグレード方法について説明します。この節では、次の事項について説明します。

- 172 ページの「ファームウェアのアップグレードの必要性の確認」
- 173 ページの「アレイファームウェアおよびドライブファームウェアのアップグレード (再起動が必要)」
- 175 ページの「アレイファームウェアのアップグレード (再起動は不要)」
- 179 ページの「ドライブファームウェアのアップグレード (再起動が必要)」

ファームウェアのアップグレードの必要性の確認

ファームウェアのアップグレードを開始する前に、各アレイコンポーネントの現在のファームウェアバージョンを確認して、アップグレードが必要かどうかを判断します。

`raidctl profile` コマンドを使用すると、RAID コントローラ装置、拡張ユニット、コントローラ NVSRAM、およびドライブの現在のファームウェアバージョンをそれぞれ取得し記録できます。詳細は、181 ページの「`raidctl` コマンドの出力の取得」を参照してください。

アレイファームウェアおよびドライブファームウェアのアップグレード (再起動が必要)

この手順を実行して、RAID アレイファームウェアおよびドライブファームウェアをアップグレードします。この手順では、NAS サーバーを再起動する必要があります。

NAS サーバーの再起動ができず、アレイファームウェアのみをアップグレードする必要がある場合は、175 ページの「アレイファームウェアのアップグレード (再起動は不要)」を参照してください。

ファームウェアのアップグレードを完了するために必要な時間は、使用する構成によって異なります。たとえば、単一の NAS サーバーに 2 台の RAID コントローラ、1 台のファイバチャネル (FC) 拡張ユニット、および 1 台のシリアル ATA (Serial Advanced Technology Attachment、SATA) 拡張ユニットが取り付けられている場合、アップグレードおよび再起動に必要な時間は約 50 分です。表 11-3 を参照して、使用する構成をアップグレードするために必要な時間を確認してください。

注 – ドライブファームウェアのアップグレードでは、常に NAS サーバーを再起動する必要があります。

注 – すでに現在のファームウェアファイルと同じファームウェアバージョンになっているドライブも含めて、ドライブ種別ごとにすべてのドライブがアップグレードされます。

注意 – ドライブに障害が発生し再構築状態にある場合は、この手順を実行しないでください。この情報は、システムログまたは Web Administrator の「RAID」ページで参照できます。

この手順を開始する前に、NAS サーバーのソフトウェア version 4.10 Build 18 以降がインストールされていることを確認してください。それより前のバージョンのオペレーティングシステム (OS) がインストールされている NAS サーバーでは、アレイおよびドライブファームウェアのアップグレードを行わないでください。

1. `www.sunsolve.sun.com` から最新のパッチをダウンロードし、ファイルを解凍します。
2. パッチの `readme` ファイルを参照して、パッチに関連付けられているファームウェアバージョンを確認します。

3. NAS クライアントから、FTP を使用可能にします。

   GUI を使用して FTP を使用可能にする方法については、160 ページの「FTP アクセスの構成」を参照してください。CLI を使用する場合は、235 ページの「FTP アクセスの構成」を参照してください。

4. パッチのダウンロード先のディレクトリに移動します。

5. FTP を使用して NAS サーバーに接続し、admin ユーザーでログインします。

6. `bin` と入力してバイナリモードへ移行します。

7. `ftp` プロンプトで次のコマンドを実行して、`/cvol` 上に各ディレクトリを作成します。

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctlr
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
mkdir /cvol/firmware/2882/drive
```

8. ファームウェアを格納するために作成したディレクトリに移動し、`put` コマンドを使用してファームウェアファイル (表 11-2 を参照) をコピーします。

   たとえば、RAID コントローラのファームウェアを読み込むには、次のコマンドを実行します。

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

9. 同じ手順を続けて、各ファームウェアファイルを適切なディレクトリに読み込みます。

   表 11-2 に、各コンポーネントのディレクトリおよびファームウェアファイルの例を示します。

表 11-2　コンポーネントのファームウェアディレクトリおよびファイル

コンポーネント	ディレクトリ	ファイル名の例
RAID コントローラ	`/cvol/firmware/2882/ctlr`	`SNAP_288X_06120910.dlp`
RAID コントローラ NVSRAM	`/cvol/firmware/2882/nvsram`	`N2882-612843-503.dlp`
FC 拡張ユニット (EU)	`/cvol/firmware/2882/jbod`	`esm9631.s3r`
SATA EU	`/cvol/firmware/2882/jbod`	`esm9722.dl`
ドライブの種類:		

表 11-2　コンポーネントのファームウェアディレクトリおよびファイル (続き)

コンポーネント	ディレクトリ	ファイル名の例
Seagate ST314680	/cvol/firmware/2882/drive	D_ST314680FSUN146G_0407.dlp
Seagate 10K	/cvol/firmware/2882/drive	D_ST314670FSUN146G_055A.dlp
Hitachi 400GB HDS724040KLSA80	/cvol/firmware/2882/drive	D_HDS7240SBSUN400G_AC7A.dlp
Fujitsu MAT3300F 300GB	/cvol/firmware/2882/drive	D_MAT3300FSUN300G_1203.dlp
Seagate 10K 300GB	/cvol/firmware/2882/drive	D_ST330000FSUN300G_055A.dlp

10. FTP セッションからログアウトします。
11. Telnet を使用して NAS サーバーに接続し、admin 権限を持つユーザーアカウントでログインします。
12. システムを再起動します。クラスタ構成では、両方のサーバーを再起動します。

    表 11-3 に、各コンポーネントのファームウェアをアップグレードするために必要なおおよその時間を示します。

    表 11-3　ファームウェアのアップグレード時間

コンポーネント	アップグレードを完了するために要する時間
RAID コントローラ	再起動時間 + 15 分
RAID コントローラ NVSRAM	再起動時間 + 5 分
FC EU または SATA EU	再起動時間 + 5 分
ドライブ	再起動時間 + ドライブごとに 1.5 分

13. 次のコマンドを実行して、新しいファームウェアが読み込まれていることを確認します。

    raidctl get type=lsi target=profile ctlr=0

    システムログで障害を確認することもできます。

アレイファームウェアのアップグレード (再起動は不要)

この手順では、NAS サーバーを再起動することなく、RAID アレイファームウェアをアップグレードします。

この手順を開始する前に、次の事項に注意してください。

- NAS サーバーソフトウェア version 4.10 Build 18 以降がインストールされている必要があります。それより前のバージョンの OS がインストールされている NAS サーバーでは、ファームウェアのアップグレードを行わないでください。
- この手順は、入出力動作が制限されている状態で実行することをお勧めします。この手順の実行中、コントローラは入出力を休止します。

注意 – ドライブに障害が発生し、再構築状態にある場合は、この手順を実行しないでください。この情報はシステムログで参照できます。

1. www.sunsolve.sun.com から最新のパッチをダウンロードし、ファイルを解凍します。
2. パッチの readme ファイルを参照して、パッチに関連付けられているファームウェアバージョンを確認します。
3. パッチのダウンロード先のディレクトリに移動します。
4. NAS クライアントから、FTP を使用可能にします。

   GUI を使用して FTP を使用可能にする方法については、160 ページの「FTP アクセスの構成」を参照してください。CLI を使用する場合は、235 ページの「FTP アクセスの構成」を参照してください。
5. FTP を使用して NAS サーバーに接続し、admin 権限を持つユーザーアカウントでログインします。
6. bin と入力してバイナリモードへ移行します。
7. ftp プロンプトで次のコマンドを実行して、/cvol 上に各ディレクトリを作成します。

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctlr
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
```

8. ファームウェアを格納するために作成したディレクトリに移動し、put コマンドを使用してファームウェアファイル (表 11-4 を参照) をコピーします。

   たとえば、RAID コントローラのファームウェアを読み込むには、次のコマンドを実行します。

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

9. **同じ手順を続けて、各ファームウェアファイルを適切なディレクトリに読み込みます。**

   表 11-4 に、各コンポーネントのディレクトリおよびファームウェアファイルの例を示します。

   表 11-4　コンポーネントのファームウェアディレクトリおよびファイル

コンポーネント	ディレクトリ	ファイル名の例
RAID コントローラ	/cvol/firmware/2882/ctlr	SNAP_288X_06120910.dlp
RAID コントローラ NVSRAM	/cvol/firmware/2882/nvsram	N2882-612843-503.dlp
FC EU	/cvol/firmware/2882/jbod	esm9631.s3r
SATA EU	/cvol/firmware/2882/jbod	esm9722.dl

10. **FTP セッションからログアウトします。**

11. **Telnet を使用して NAS サーバーに接続し、admin 権限を持つユーザーアカウントでログインします。**

12. **raidctl download コマンドを使用して、各ファイルを目的のディレクトリに読み込みます。**

    たとえば、コントローラファームウェアを ctlr ディレクトリからコントローラ 0 および 1 に読み込むには、次のコマンドを実行します。

    raidctl download type=lsi target=ctlr ctlr=0

    このコマンドにより、ファームウェアファイルが両方のコントローラへダウンロードされ、ディレクトリからファイルが削除されます。

    注 – raidctl download コマンドを実行すると、各コマンドの呼び出し後にファームウェアファイルが削除されます。そのため、コントローラ装置、コントローラ NVSRAM、拡張ユニット、ドライブの各コンポーネントをアップグレードしたあと、ファームウェアファイルを再度コピーする必要があります。

    jbod ディレクトリにあるファームウェアを拡張格納装置 0 にダウンロードするには、次のコマンドを実行します。

    raidctl download type=lsi target=jbod ctlr=0

13. **Telnet セッションで、各ダウンロードの進行状況を監視します。**

各アップグレードを完了するために必要なおおよその時間は、次のとおりです。

コンポーネント	コンポーネントあたりの時間 (分)
RAID コントローラ EU	15 分
RAID コントローラ NVSRAM	5 分
FC EU または SATA EU	5 分

注 – アップグレードが完了すると、5 分以内に `telnet` のカーソルに戻ります。カーソルが表示されるまで、待機してください。

14. **次のコンポーネントの作業に進む前に、システムログでダウンロードが完了していることを確認します。**

    システムログの出力例を次に示します。

```
Ctrl-

Firmware Download  90% complete
Firmware Download  95% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
nvsram-

raidctl download type=lsi target=nvsram ctlr=0
Flashing C0 NVSRAM: /cvol/nf2/../firmware/2882/nvsram/n2882-
61.dlp (48068)
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
ESM-
```

```
>> raidctl download type=lsi target=jbod ctlr=0 tray=1

Flashing C0 JBOD 1 with
/cvol/nf1/../firmware/2882/jbod/esm9631.s3r (663604)
Firmware Download  20% complete
Firmware Download  30% complete
Firmware Download  50% complete
Firmware Download  60% complete
Firmware Download  90% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
Drive-
10/26/05 10:57:42 I Firmware Download  20% complete
10/26/05 10:57:46 I Firmware Download  30% complete
10/26/05 10:57:50 I Firmware Download  40% complete
10/26/05 10:57:54 I Firmware Download  50% complete
10/26/05 10:57:58 I Firmware Download  60% complete
10/26/05 10:58:03 I Firmware Download  70% complete
10/26/05 10:58:08 I Firmware Download  80% complete
10/26/05 10:58:13 I Firmware Download  90% complete
10/26/05 10:58:18 I Bytes Downloaded: 628224 (2454 256 chunks),
imageSize=62804
                    8
10/26/05 10:59:01 I Flashed OK - drive in tray 2 slot 12
10/26/05 10:59:01 I Downloaded firmware version 0407 to 27 drives
```

ドライブファームウェアのアップグレード (再起動が必要)

ドライブファームウェアのみをアップグレードするには、この手順を実行してください。この手順では、NAS サーバーを再起動する必要があります。

注 – ドライブファームウェアのアップグレードでは、常に NAS サーバーを再起動する必要があります。

注 – すでに現在のファームウェアファイルと同じファームウェアバージョンになっているドライブも含めて、ドライブ種別ごとにすべてのドライブがアップグレードされます。

ファームウェアのアップグレードを完了するために必要な時間は、設置されているドライブの数と、NAS サーバーの再起動に必要な時間によって異なります。表 11-3 を参照して、使用する構成をアップグレードするために必要な時間を確認してください。

注意 – ドライブに障害が発生し、再構築状態にある場合は、この手順を実行しないでください。この情報はシステムログで参照できます。

ドライブファームウェアをアップグレードする前に、NAS サーバーソフトウェア 4.10 Build 18 以降がインストールされていることを確認してください。それより前のバージョンの OS がインストールされている NAS サーバーでは、ファームウェアのアップグレードを行わないでください。

1. `www.sunsolve.sun.com` から最新のパッチをダウンロードし、ファイルを解凍します。
2. パッチの `readme` ファイルを参照して、パッチに関連付けられているファームウェアバージョンを確認します。
3. パッチのダウンロード先のディレクトリに移動します。
4. NAS クライアントから、FTP を使用可能にします。

   GUI を使用して FTP を使用可能にする方法については、160 ページの「FTP アクセスの構成」を参照してください。CLI を使用する場合は、235 ページの「FTP アクセスの構成」を参照してください。
5. FTP を使用して NAS サーバーに接続し、`admin` ユーザーでログインします。
6. `bin` と入力してバイナリモードへ移行します。
7. `ftp` プロンプトで次のコマンドを発行して、`/cvol` 上に次のディレクトリを作成します。

   `mkdir /cvol/firmware/2882/drive`
8. ドライブファームウェアを格納するために作成したディレクトリに移動し、`put` コマンドを使用してドライブファームウェアファイル (表 11-2 を参照) をコピーします。

   たとえば、Seagate ST314680 ドライブのファームウェアを読み込むには、次のコマンドを実行します。

   `cd /cvol/firmware/2882/drive`

   `put D_ST314680FSUN146G_0407.dlp`

9. FTP セッションからログアウトします。
10. Telnet を使用して NAS サーバーに接続し、admin ユーザーでログインします。
11. システムを再起動します。クラスタ構成では、両方のサーバーを再起動します。

    アップグレードを完了するために必要なおおよその時間は、再起動に要する時間にドライブあたり 1.5 分を加えた時間です。
12. 次のコマンドを実行して、新しいファームウェアが読み込まれていることを確認します。

    raidctl get type=lsi target=profile ctlr=0

    システムログで障害を確認することもできます。

raidctl コマンドの出力の取得

raidctl profile コマンドを使用すると、RAID コントローラ装置、拡張ユニット、コントローラ NVSRAM、およびドライブの、それぞれの現在のファームウェアバージョンを確認できます。この節では、次の手順について説明します。

- 181 ページの「Solaris クライアントから raidctl コマンドの出力を取得する」
- 191 ページの「Windows クライアントから raidctl の出力を取得する」

▼ Solaris クライアントから raidctl コマンドの出力を取得する

1. Solaris クライアントから、script コマンドとファイル名を入力します。次に例を示します。

    > **script raidctl**
2. Telnet を使用して NAS サーバーに接続します。
3. 次の raidctl コマンドを入力して出力を収集します。

    raidctl get type=lsi target=profile ctlr=0
4. exit と入力して Telnet セッションを終了します。
5. ふたたび exit と入力して、raidctl という名前のファイルを閉じます。

次にコマンドの出力例を示します。コマンドと、その結果として出力されたファームウェアバージョンは、太字で示します。

```
telnet 10.8.1xx.x2
Trying 10.8.1xx.x2...
Connected to 10.8.1xx.x2.
Escape character is '^]'.
connect to (? for list) ? [menu] admin
password for admin access ? *********
5310 > raidctl get type=lsi target=profile ctlr=0

SUMMARY---------------------------------
Number of controllers: 2
Number of volume groups: 4
Total number of volumes (includes an access volume): 5 of 1024 used
   Number of standard volumes: 4
   Number of access volumes: 1
Number of drives: 28
Supported drive types: Fibre (28)
Total hot spare drives: 2
   Standby: 2
   In use: 0
Access volume: LUN 31
Default host type: Sun_SE5xxx (Host type index 0)
Current configuration
   Firmware version: PkgInfo 06.12.09.10
   NVSRAM version: N2882-612843-503
Pending configuration
```

```
CONTROLLERS ---------------------------------
Number of controllers: 2

Controller in Tray 0, Slot B
   Status: Online
   Current Configuration
      Firmware version: 06.12.09.10
         Appware version: 06.12.09.10
         Bootware version: 06.12.09.10
      NVSRAM version: N2882-612843-503
   Pending Configuration
      Firmware version: None
         Appware version: None
         Bootware version: None
      NVSRAM version: None
      Transferred on: None
   Board ID: 2882
   Product ID: CSM100_R_FC
   Product revision: 0612
   Serial number: 1T44155753
   Date of manufacture: Sat Oct 16 00:00:00 2004
   Cache/processor size (MB): 896/128
   Date/Time: Thu Nov  2 19:15:49 2006
   Associated Volumes (* = Perferred Owner):
      lun4* (LUN 3)
Ethernet port: 1
      Mac address: 00.A0.B8.16.C7.A7
      Host name: gei
      Network configuration: Static
      IP address: 192.168.128.106
      Subnet mask: 255.255.255.0
      Gateway: 192.168.128.105
      Remote login: Enabled
   Drive interface: Fibre
      Channel: 2
      Current ID: 124/0x7C
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:02:00:A0:B8:16:C7:A7
      World-wide node name: 20:00:00:A0:B8:16:C7:A7
      Part type: HPFC-5400      revision 6
```

```
 Drive interface: Fibre
      Channel: 2
      Current ID: 124/0x7C
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:02:00:A0:B8:16:C7:A7
      World-wide node name: 20:00:00:A0:B8:16:C7:A7
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 2
      Current ID: 255/0x3
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
      World-wide port name: 20:07:00:A0:B8:16:C6:FB
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 2
      Current ID: 255/0x3
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
      World-wide port name: 20:07:00:A0:B8:16:C6:FB
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6

Controller in Tray 0, Slot A
   Status: Online
   Current Configuration
      Firmware version: 06.12.09.10
         Appware version: 06.12.09.10
         Bootware version: 06.12.09.10
      NVSRAM version: N2882-612843-503
   Pending Configuration
      Firmware version: None
         Appware version: None
         Bootware version: None
      NVSRAM version: None
      Transferred on: None
```

```
 Board ID: 2882
   Product ID: CSM100_R_FC
   Product revision: 0612
   Serial number: 1T44155741
   Date of manufacture: Sun Oct 10 00:00:00 2004
   Cache/processor size (MB): 896/128
   Date/Time: Thu Nov  2 19:15:45 2006
   Associated Volumes (* = Perferred Owner):
lun1* (LUN 0), lun2* (LUN 1), lun3* (LUN 2)
   Ethernet port: 1
      Mac address: 00.A0.B8.16.C6.F9
      Host name: gei
      Network configuration: Static
      IP address: 192.168.128.105
      Subnet mask: 255.255.255.0
      Gateway: 192.168.128.105
      Remote login: Enabled
   Drive interface: Fibre
      Channel: 1
      Current ID: 125/0x7D
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:01:00:A0:B8:16:C6:F9
      World-wide node name: 20:00:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
Drive interface: Fibre
      Channel: 1
      Current ID: 125/0x7D
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:01:00:A0:B8:16:C6:F9
      World-wide node name: 20:00:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
Host interface: Fibre
      Channel: 1
      Current ID: 255/0x0
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
```

```
 Link status: Down
      Topology: Unknown
      World-wide port name: 20:06:00:A0:B8:16:C6:FA
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 1
      Current ID: 255/0x0
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
World-wide port name: 20:06:00:A0:B8:16:C6:FA
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6

VOLUME GROUPS-------------------------
   Number of volume groups: 4
   Volume group 1 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun1 (681 GB)
      Associated drives (in piece order):
      Drive at Tray 0, Slot 7
      Drive at Tray 0, Slot 6
      Drive at Tray 0, Slot 5
      Drive at Tray 0, Slot 4
      Drive at Tray 0, Slot 3
      Drive at Tray 0, Slot 8
Volume group 2 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun2 (681 GB)
      Associated drives (in piece order):
      Drive at Tray 0, Slot 14
      Drive at Tray 0, Slot 13
      Drive at Tray 0, Slot 12
      Drive at Tray 0, Slot 11
      Drive at Tray 0, Slot 10
      Drive at Tray 0, Slot 9
```

```
 Volume group 3 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun3 (817 GB)
      Associated drives (in piece order):
      Drive at Tray 11, Slot 5
      Drive at Tray 11, Slot 4
      Drive at Tray 11, Slot 3
      Drive at Tray 11, Slot 2
      Drive at Tray 11, Slot 1
      Drive at Tray 11, Slot 7
      Drive at Tray 11, Slot 6
   Volume group 4 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun4 (817 GB)
      Associated drives (in piece order):
      Drive at Tray 11, Slot 13
Drive at Tray 11, Slot 12
      Drive at Tray 11, Slot 11
      Drive at Tray 11, Slot 10
      Drive at Tray 11, Slot 9
      Drive at Tray 11, Slot 8
      Drive at Tray 11, Slot 14

STANDARD VOLUMES----------------------------

SUMMARY
   Number of standard volumes: 4
   NAME    STATUS    CAPACITY  RAID LEVEL  VOLUME GROUP
   lun1    Optimal   681   GB    5            1
   lun2    Optimal   681   GB    5            2
   lun3    Optimal   817   GB    5            3
   lun4    Optimal   817   GB    5            4
```

```
DETAILS

   Volume name: lun1
      Volume ID: 60:0A:0B:80:00:16:C6:F9:00:00:23:B4:43:4B:53:3A
      Subsystem ID (SSID): 0
      Status: Optimal
      Action: 1
      Tray loss protection: No
      Preferred owner: Controller in slot A
      Current owner: Controller in slot B
      Capacity: 681 GB
      RAID level: 5
      Segment size: 64 KB
      Associated volume group: 1
      Read cache: Enabled
      Write cache: Enabled
      Flush write cache after (in seconds): 8
      Cache read ahead multiplier: 1
      Enable background media scan: Enabled
      Media scan with redundancy check: Disabled
DRIVES------------------------------

SUMMARY

   Number of drives: 28
      Supported drive types: Fiber (28)
   BASIC:
CURRENT    PRODUCT      FIRMWARE
   TRAY,SLOT  STATUS  CAPACITY   DATA RATE     ID          REV
      0,1     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,7     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,6     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,5     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,4     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,3     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,2     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,14    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,13    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,12    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,11    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,10    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,9     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,8     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
```

```
 11,5     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,4     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,3     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,2     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,1     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,13    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,12    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,11    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,10    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,9     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,8     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,7     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,6     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,14    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307

   HOT SPARE COVERAGE:

      The following volume groups are not protected:

      Total hot spare drives: 2
         Standby: 2
         In use: 0

   DETAILS:

      Drive at Tray 0, Slot 1 (HotSpare)
         Available: 0
         Drive path redundancy: OK
         Status: Optimal
         Raw capacity: 136 GB
         Usable capacity: 136 GB
         Product ID: ST314680FSUN146G
         Firmware version: 0307
         Serial number: 3HY90HWJ00007510RKKV
Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:BA:3E
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: None
         Available: No
```

```
 Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:CA:12
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: 3
         Available: No

      Drive at Tray 11, Slot 1
         Drive path redundancy: OK
         Status: Optimal
         Raw capacity: 136 GB
         Usable capacity: 136 GB
         Product ID: ST314680FSUN146G
         Firmware version: 0307
         Serial number: 3HY90JEW00007511BDPL
         Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:C8:8B
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: 3
         Available: No
Drive Tray 1 Overall Component Information
      Tray technology: Fibre Channel
      Minihub datarate mismatch: 0
      Part number: PN 54062390150
      Serial number: SN 0447AWF011
      Vendor: VN SUN
      Date of manufacture: Mon Nov  1 00:00:00 2004
      Tray path redundancy: OK
      Tray ID: 11
Tray ID Conflict: 0
      Tray ID Mismatch: 0
      Tray ESM Version Mismatch: 0
      Fan canister: Optimal
      Fan canister: Optimal
      Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A6847502330F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
```

```
 Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A6847502330F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
      Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A68475023N0F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
      Temperature: Optimal
Temperature: Optimal
      Esm card
         Status: Optimal
         Firmware version: 9631
         Maximum data rate: 2 Gbps
         Current data rate: 2 Gbps
         Location: A (left canister)
         Working channel: -1
         Product ID: CSM100_E_FC_S
         Part number: PN 37532180150
         Serial number: SN 1T44462572
         Vendor: SUN
         FRU type: FT SBOD_CEM
         Date of manufacture: Fri Oct  1 00:00:00 2004
      Esm card
         Status: Optimal
         Firmware version: 9631
         Maximum data rate: 2 Gbps
         Current data rate: 2 Gbps
         Location: B (right canister)
         Working channel: -1
```

▼ Windows クライアントから raidctl の出力を取得する

1. 「スタート」>「ファイル名を指定して実行」をクリックして、cmd と入力します。「OK」をクリックします。
2. ウィンドウの上部を右クリックして、「プロパティ」を選択します。
   「プロパティ」ダイアログボックスが表示されます。
3. 「画面バッファのサイズ」の「高さ」を 3000 に変更します。
4. 「オプション」タブをクリックして、「挿入モード」の選択を解除します。

5. Telnet を使用して NAS サーバーに接続し、次の `raidctl` コマンドを入力して出力を収集します。

   `raidctl get type=lsi target=profile ctlr=0`

6. 任意のテキストエディタを使用して、ファイルにテキストをコピーします。次に例を示します。

   a. 出力されたテキストを選択し、Ctrl-C を押してデータをコピーします。

   b. 「スタート」>「プログラム」>「アクセサリ」>「ワードパッド」をクリックして、ワードパッドを開きます。

   c. ウィンドウの内部をクリックし、Ctrl-V を押してテキストを貼り付けます。

   d. ファイルを保存します。

7. 保存したファイルを開いて、各コンポーネントの現在のファームウェアバージョンを検索します。

付録A

コンソール管理

Web Administrator の代わりにコンソールを使用して、Sun StorEdge 5310 NAS Appliance、Sun StorEdge 5310 Cluster、および Sun StorEdge 5310 Gateway システムを管理できます。使用しているアプリケーションに米国規格協会 (ANSI) 互換の端末エミュレータがあれば、Telnet、Secure Shell (SSH)、RLogin などのさまざまなプロトコルを使用して管理者コンソールに接続できます。この付録では、Windows ですぐに使用可能な Telnet プロトコルを使用します。

注 – コマンド行インタフェースにアクセスするために、遠隔アクセスセキュリティーの設定変更が必要になる場合があります。遠隔アクセスの詳細は、160 ページの「遠隔アクセスセキュリティーを設定する」を参照してください。

この付録の内容は、次のとおりです。

管理者コンソールへのアクセス

この例では、Windows Telnet プロトコルを使用します。ただし、ANSI 互換の端末エミュレータがあれば、別のプロトコルを使用することもできます。

▼ Windows Telnet にアクセスする

1. デスクトップのタスクバーから「スタート」をクリックします。
2. 「ファイル名を指定して実行」を選択します。
3. 「ファイル名を指定して実行」ウィンドウで `cmd` と入力して、「OK」をクリックします。
4. コマンドプロンプトで `telnet` *ipaddress* (*ipaddress* はサーバーの IP アドレス) と入力して、Enter キーを押します。
5. 管理アクセスがパスワードで保護されている場合は、パスワードを入力します。

   接続すると、Telnet の画面に次のコマンド行プロンプトが表示されます。

   ```
   connect to (? for list) ?[menu]
   ```

   この時点で、直接メインメニューに移動するか、コマンド行インタフェース (CLI) にアクセスして特定のコマンドを実行することができます。

   メインメニューにアクセスするには、Enter キーを押します。

▼ コマンド行インタフェースにアクセスする

1. 接続プロンプトで `admin` と入力して、Enter キーを押します。
2. 管理パスワードを入力して、Enter キーを押します。

   コマンド行プロンプトが表示されます。コマンドを入力するか、`menu` を選択してコンソールのメインメニューにアクセスできます。

注意 – 予期しない結果を回避するため、コマンドは注意して使用してください。

コマンド行に戻るには、メインメニューで Esc キーを押します。

コンソールメニューの概要

この節では、システムの設定および保持に使用する Telnet 画面の構成要素について説明します。

基本的なガイドライン

コンソールの使用に関するいくつかの基本的なガイドラインを次に示します。

- メニューを選択するには、項目に関連付けられた数字または文字を押します。たとえば、「1. Activity Monitor」画面を選択する場合は、1 を押します。
- 各画面の下部のボックスには、実行可能な作業、および処理を実行するために選択する必要がある文字が表示されます。
- リストをスクロールして表示するには、スペースキーを使用します。

キーの説明

画面のフィールドを編集するのに使用するキーを、次の表に示します。

表 A-1　画面で使用できるキー

キー	説明
Backspace、Delete、Ctrl+H	前の文字を削除します
Ctrl+U	フィールド全体を削除します
Enter、Ctrl+M、Ctrl+J、Ctrl+I、Tab	入力を完了して、カーソルを次のフィールドに進めます
Esc	変更せずに画面を終了します

フィールドの値を変更しない場合は、Enter キーを押してください。情報が変更されることなく、カーソルが次のフィールドに移動します。

メインメニューの表示

メインメニューは、次のセクションで構成されます。

- Operations − 任意の数字を押して、対応するサーバー操作を実行します。
- Configurations − 任意の文字を押して、対応するサーバー構成コマンドを実行します。
- Access Control − 任意の文字を押して、対応するメニュー項目へのアクセス方法を設定します。
- Extensions − 任意の文字を押して、対応する拡張機能を選択します。拡張機能のリストをスクロールして表示するには、スペースキーを使用します。

▼ メニューを使用する

1. 対応する文字または数字を押して、メニュー項目を選択します。
2. 拡張機能 (Extension) リストのほかのオプションを表示するには、スペースキーを押します。

構成のバックアップ

システムを構成したら、構成のバックアップを作成することをお勧めします。

注意 – システムは構成情報の冗長コピーを保存しますが、システム障害に備えてバックアップコピーを作成する必要があります。

▼ 構成情報をバックアップする

クラスタ構成では、次の手順を 1 台のサーバー上でのみ実行してください。構成はサーバー間で自動的に同期化されるため、サーバーごとに構成のバックアップを作成する必要はありません。

1. 194 ページの「コマンド行インタフェースにアクセスする」の手順を実行します。

注意 – 予期しない結果を回避するため、コマンドは注意して使用してください。

2. コマンド行で `load unixtools` と入力します。

3. `cp r v /dvol/etc` *backup-path* と入力します。*backup-path* は、構成ファイルのバックアップ先となるディレクトリの場所を示すフルパスで、ボリューム名を含みます。既存の空のディレクトリを指定する必要があります。

   この操作により、`/dvol/etc` ディレクトリに格納されているすべての構成情報が、指定した場所にコピーされます。

システムの管理

コンソール管理機能を使用して、システム管理作業を行うことができます。

▼ TCP/IP を構成する

1. 「Configuration」メニューから「Host Name & Network」を選択します。
2. 「1. Edit fields」を選択します。
3. サーバーのホスト名を入力して、Enter キーを押します。
4. 最大転送単位 (MTU) を入力するか、Enter キーを押してデフォルトを保持します。
5. サーバーの IP アドレスを入力して、Enter キーを押します。
6. ネットワークの IP サブネットマスクを入力して、Enter キーを押します。
7. ネットワークの IP ブロードキャストを入力して、Enter キーを押します。
8. 「1. Setup」を選択してエイリアス IP アドレスを設定し、Enter キーを押します。
9. ほかのすべてのポートについて手順 3 ～手順 8 を繰り返します。次の処理に進むには、Enter キーを押します。

   注 – ほかのポートが存在する場合は、スペースキーを使用して画面を下にスクロールします。

10. ゲートウェイアドレスを入力して、Enter キーを押します。
11. 「7. Save changes」を選択します。

▼ 管理者パスワードを変更する

1. 「Access Control」メニューから「Admin Access」を選択します。
2. 「Y. Yes」を選択してパスワードの保護を使用可能にするか、「N. No」を選択して使用不可にします。

注 – 必ずパスワードを使用してシステムを保護してください。

---

3. 「Yes」を選択した場合は、プロンプトに応じて次の手順を実行します。

   a. 管理アクセス用のパスワードを入力し、確認のためもう一度入力します。

   b. 「7. Save changes」を選択して、新しいパスワードを使用可能にします。

日付および時刻の制御

「Timezone, Time, Date」メニューオプションを使用して、システムのタイムゾーン、時刻、および日付の設定を変更します。メインボードのリアルタイムクロックは、現地時間に設定されています。

注 – システムに日付および時刻をはじめて設定する際、システムの固定クロックも初期化されます。このクロックは、ライセンス管理ソフトウェアおよび Compliance Archiving Software で使用され、時間に依存する動作を制御します。

注意 – 固定クロックは一度初期化されると再設定できません。したがって、システムを構成する際は、日付および時刻を正確に設定してください。

▼ タイムゾーン、時刻、および日付を設定する

1. 「Configuration」メニューから「Timezone, Time, Date」を選択します。
2. 適切なタイムゾーンを選択して、Enter キーを押します。
3. 夏時間に「Y」または「N」を選択します。
4. 新しい日付を入力して、Enter キーを押します。

   形式は YYYYMMDD で、YYYY は年、MM は月、DD は日を示します。たとえば、`20051001` は、2005 年 10 月 1 日を表します。

5. 現在の時刻を入力して、Enter キーを押します。

   システムは 24 時間時計を使用します。

6. 「7. Save changes」を選択します。

時刻同期の設定

時間情報プロトコル (NTP) または RDATE サーバーのいずれかの時刻と同期をとるように、システムを構成できます。

NTP は、基準時刻のソースに接続し、コンピュータの時計を同期化するためのインターネットプロトコルです。一般的な NTP 構成には、複数台の冗長サーバーおよび各種ネットワークパスが使用できるため、高い精度と信頼性を実現できます。

RDATE サーバーは、通常 UNIX システム上に存在し、システムサーバーの時刻を RDATE サーバーの時刻に同期化できます。

▼ NTP を設定する

1. 「Extensions」メニューから、「NTP Configuration」を選択します。
2. 「1. Edit fields」を選択して、NTP の設定を行います。
3. 「Y. Yes」を選択して、NTP を使用可能にします。
4. 構成する NTP サーバーのそれぞれに対して次の手順を実行します。

   NTP サーバーは 2 台まで構成できます。

   a. 「Y. Yes」を選択して、1 台めの NTP サーバーを使用可能にします。

   b. Sun StorEdge 5310 NAS Appliance がポーリングによって現在の時刻を取得する NTP サーバーの名前または IP アドレスを入力して、Enter キーを押します。

   c. 使用する認証タイプに「0. none」または「1. symmetric-key」を選択します。

      対称鍵による認証を使用すると、Sun StorEdge 5310 NAS Appliance は、鍵と鍵識別子を使用して NTP サーバーが認識および承認されていることを確認します。メッセージを認証するには、NTP サーバーと Sun StorEdge 5310 NAS Appliance との間で鍵および鍵識別子を一致させる必要があります。

   d. 前述のフィールドで対称鍵を認証構造として選択した場合は、この NTP サーバーに使用される鍵ファイルの非公開鍵に関連付けられた鍵識別子を入力します。

      この値の有効範囲は 1 ～ 65534 です。

5. 「Min. Polling Interval」フィールドに、NTP メッセージの最小ポーリング間隔を入力します。

   この値が 2 乗されてポーリング間隔の最小秒数となります。たとえば 4 を入力すると、ポーリング間隔は 16 秒になります。このフィールドの有効範囲は 4 ～ 17 です。

6. 「Max. Polling Interval」フィールドに、NTP メッセージの最大ポーリング間隔を入力します。

   この値が 2 乗されてポーリング間隔の最大秒数となります。たとえば 4 を入力すると、ポーリング間隔は 16 秒になります。このフィールドの有効範囲は 4 ～ 17 ですが、最小ポーリング間隔よりも大きい値に設定する必要があります。

7. 「Broadcast Client Enabled」フィールドで、「Y. Yes」を選択します。これによって、すべてのインタフェースで受信されたサーバーのブロードキャストメッセージに Sun StorEdge 5310 NAS Appliance が応答できるようになります。

8. 「Require Server authentication」フィールドで、「Y. Yes」を選択します。これによって、ブロードキャストクライアントによるサーバーの認証が行われます。

   認証を使用していない NTP サーバーは許可されません。

9. 「7. Save changes」を選択します。

▼ RDATE サーバーおよび許容範囲を設定する

1. 「Extensions」メニューから「RDATE time update」を選択します。
2. 「1. Edit fields」を選択します。
3. RDATE サーバーの名前または IP アドレスを入力して、Enter キーを押します。
4. 許容範囲を入力して、Enter キーを押します。

   Sun StorEdge 5310 NAS Appliance システムの時刻と RDATE サーバーの時刻との誤差がこの秒数より小さい場合 (+ または –) は、Sun StorEdge 5310 NAS Appliance システムの時刻が RDATE サーバーの時刻に同期化されます。このような誤差の確認は、毎日午後 11 時 45 分に実行されます。

5. 「7. Save changes」を選択します。

ウイルス対策保護機能の設定

ネットワーク上でウイルス対策スキャンエンジンを実行している場合は、システムにウイルス対策保護機能を構成できます。ウイルス対策保護機能の詳細は、65 ページの「ウイルス対策ソフトウェアの使用」を参照してください。

▼ ウイルス対策保護機能を使用可能にする

1. 「Extensions」メニューから、「Anti-Virus Configuration」を選択します。
2. 「1. Edit fields」を選択します。
3. 「AVA Enable」フィールドで「Yes」を指定して、ウイルス対策保護機能を使用可能にします。

4. 「Scan mode」フィールドでスキャンモードを選択します。

   スキャンモードオプションの詳細は、65 ページの「ウイルス対策保護機能を使用可能にする」を参照してください。

5. 使用するスキャンエンジンの TCP/IP アドレスを指定します。

6. ICAP サーバーが接続を待機する TCP/IP のポート番号を指定します。通常はポート 1344 を使用します。

7. システムがスキャンエンジンに振り分ける、並行ファイルスキャン操作の最大数を指定します。通常は 2 を設定します。

8. スキャンの対象または対象外にするファイルの種類と、除外するクライアント、グループ、または共有を指定します。

指定	説明	形式
File Types Included	スキャンの対象にするファイルの種類の拡張子。すべてを対象とする場合は、空白にします。	3 文字以内で、コンマで区切って指定します。ワイルドカードマッチング用に ? を使用できます。
File Types Excluded	スキャンの対象外にするファイルの種類の拡張子。	3 文字以内で、コンマで区切って指定します。ワイルドカードマッチング用に ? を使用できます。
Exempt Clients	スキャンから除外する各クライアントの名前および IP アドレス。	コンマで区切って指定します。
Exempt Groups	スキャンから除外する Windows/NT または Windows Active Directory の各グループ (UNIX グループ以外) の名前。	空白文字を含めることができ、コンマで区切って指定します。
Exempt Shares	スキャンから除外する各 CIFS 共有の名前。 注: 管理共有 (X$) は常にスキャンから除外されます。	コンマで区切って指定します。

9. 「7. Save changes」を選択します。

言語の選択

NFS および CIFS で使用する言語を指定できます。

▼ 言語を選択する

1. 「Extensions」メニューから「Language Selection」を選択します。

2. 使用する言語を入力して、Enter キーを押します。

   サポートされる言語は、画面の上部に表示されます。

ルートの管理

ルーティングテーブルには、指定した宛先へのネットワークパケットの送信に使用されるネットワークパスのリストが含まれます。各ルートのエントリは、宛先のアドレスおよびパスで構成されます。宛先には、ネットワークまたはホストのいずれかを指定できます。パスは、宛先へのパケットの送信に使用されるゲートウェイデバイスを示します。

▼ ローカルネットワークの静的ルートを管理する

1. 「Configuration」メニューから「Host Name & Network」を選択します。
2. 「2. Manage Routes」を選択します。
3. 「1. Add route」を選択して、「1. Edit」を選択します。
4. ルートのタイプに、ホスト、ネットワーク、ゲートウェイを経由したホスト、ゲートウェイを経由したネットワークのいずれかを選択します。
5. 宛先の IP アドレスを入力して、Enter キーを押します。
6. Sun StorEdge 5310 NAS Appliance を宛先に接続するために使用されるパスまたはゲートウェイアドレスを入力して、Enter キーを押します。

   ゲートウェイデバイスは、Sun StorEdge 5310 NAS Appliance と同じサブネットに接続している必要があります。
7. 「7. Save changes」を選択します。

ネームサービス

コンソールインタフェースで使用可能なネームサービスおよび機能は、GUI で使用可能なネームサービスおよび機能とは異なります。

DNS、syslogd、およびローカルロギングの設定

DNS は、ドメイン名を IP アドレスに変換する階層的なネームシステムです。syslogd は、遠隔ロギングをサポートするユーティリティーです。ネットワーク上に Sun StorEdge 5310 NAS Appliance のシステムログを受信できる syslogd ユーティリティーを持つ UNIX システムがある場合にのみ、遠隔ロギングを使用可能にできます。これらの機能はすべて同じ画面上で設定します。

syslogd ユーティリティーを設定すると、選択したサーバーにすべてのログメッセージが送信されます。これによって、すべてのサーバーからのログメッセージのレコードを、1 つのシステムに集中させることができます。

▼ DNS、動的 DNS、syslogd、およびローカルロギングを設定する

1. 「Configuration」メニューから「DNS & SYSLOGD」を選択します。
2. 「1. Edit fields」を選択します。
3. 「Y. Yes」を選択して、ドメインネームサービス (DNS) を使用可能にします。
4. 名前解決で最初に照会される DNS サーバーの IP アドレスを入力して、Enter キーを押します。
5. 名前解決で 2 番めに照会されるサーバーの IP アドレスを入力して、Enter キーを押します。

   セカンダリ DNS サーバーが存在しない場合は、このフィールドは空白のままにします。
6. DNS サーバーのドメイン名を入力して、Enter キーを押します。
7. システムが各 DNS サーバーに対して DNS 照会を試行する最大回数を入力して、Enter キーを押します。
8. 各 DNS サーバーに照会を試行する間隔を秒単位で入力して、Enter キーを押します。
9. 遠隔ロギングを使用可能にするには「Y. Yes」を選択します。ネットワーク上に syslogd サーバーが存在しない場合は「N. No」を選択して、手順 15 に進みます。

   この機能を使用すると、Sun StorEdge 5310 NAS Appliance は、遠隔 SYSLOGD サーバーにログメッセージを送信できます。
10. syslogd サーバーの名前または IP アドレスを入力して、Enter キーを押します。
11. 適切な機能を選択して、Enter キーを押します。機能は、メッセージの生成元のアプリケーションまたはシステムコンポーネントを示します。選択できる機能を次に示します。

- Kern − カーネルによって生成されるメッセージ。ユーザープロセスでは生成されないメッセージです。
- User − ランダムユーザープロセスによって生成されるメッセージ。機能を指定しない場合は、この機能識別子がデフォルトで指定されます。
- Mail − メールシステム。
- Daemon − システムデーモンまたはネットワークデーモン。
- Auth − ログインなどの認証システム。
- Syslog − syslogd によって内部的に生成されるメッセージ。
- Local0 ～ Local7 − ローカルでの使用のために予約済み。

12. Sun StorEdge 5310 NAS Appliance ログに含めるシステムイベントタイプを選択します。

    a. 適切なイベントタイプを選択します。

    b. 「Y. Yes」を選択して、そのタイプのイベントが報告されるようにします。イベントタイプには、次の種類があります。

    - Emerg − 緊急メッセージ。このメッセージは一部のユーザーに送信されます。優先順位が緊急のメッセージは、確認用に別のファイルに記録できます。
    - Alert − ただちに対処する必要がある重要メッセージ。このメッセージはすべてのユーザーに送信されます。
    - Crit − ハードウェアの問題など、エラーには分類されない重大メッセージ。優先順位が重大以上のメッセージはシステムコンソールに送信されます。
    - Err − ディスク書き込みの失敗など、エラーの状態を示すメッセージ。
    - Warning − 回復可能な異常に関するメッセージ。
    - Notice − 重要な情報メッセージ。優先順位指定のないメッセージは、この優先順位のメッセージに割り当てられます。
    - Info − 情報メッセージ。このメッセージはシステムの分析に役立ちます。
    - Debug − デバッグに関するメッセージ。

    c. Enter キーを押して、次のイベントタイプに移動します。

13. 「Y. Yes」を選択して、動的 DNS 更新を使用可能にします。

    動的 DNS 更新を使用すると、セキュリティー保護されていない動的更新が起動時に実行されます。

14. セキュリティー保護された更新を可能にするには、Windows ユーザーの名前を入力し動的 DNS クライアントがこの名前によって更新を検証できるようにして、Enter キーを押します。

    このユーザーには管理権限が必要です。

15. 動的 DNS ユーザーのパスワードを入力して、Enter キーを押します。

16. 「Y. Yes」を選択して、ローカルロギングを使用可能にします。

17. 「Log File」フィールドに、ログファイルのパス (ディレクトリ) およびファイル名を入力します。
18. 「Archives」フィールドに、アーカイブファイルの最大数を入力します。
    指定可能な範囲は 1 ～ 9 です。
19. 「Archives」フィールドに、各アーカイブファイルの最大ファイルサイズを K バイト単位で入力します。
    指定可能な範囲は 1000K ～ 999,999K バイトです。
20. 「7. Save changes」を選択します。

NIS および NIS+ の設定

注 – ネットワーク情報サービス (NIS) を設定すると、サーバーでマスターファイルの変更が定期的に確認されます。変更されたファイルは NIS サーバーからローカルファイルにコピーされます。「Enable」フィールドを使用すると、設定情報を失うことなく NIS 更新を使用不可にできるため、再度使用可能にするときまで設定情報を保持できます。

▼ NIS または NIS+ を使用可能にする

1. 「Configuration」メニューから「NIS & NIS+」を選択します。
2. 「1. Edit fields」を選択します。
3. 「Y. Yes」を選択して、Sun StorEdge 5310 NAS Appliance による NIS サーバーを使用したホスト、ユーザー、およびグループのファイルの定期的な更新を使用可能にします。
4. NIS ドメイン名を入力して、Enter キーを押します。
5. NIS サーバーの名前または IP アドレスを入力して、Enter キーを押します。
6. 「Y. Yes」を選択して、NIS サーバーによるホストのファイルの更新を使用可能にします。
7. 「Y. Yes」を選択して、NIS サーバーによるユーザーのファイルの更新を使用可能にします。
8. 「Y. Yes」を選択して、NIS サーバーによるグループのファイルの更新を使用可能にします。
9. 「Y. Yes」を選択して、NIS サーバーによるネットグループのファイルの更新を使用可能にします。

10. NIS 更新の間隔を 0 ～ 9 分の範囲で入力して、Enter キーを押します。
11. 「Y. Yes」を選択して、Sun StorEdge 5310 NAS Appliance に対して NIS+ を使用可能にします。
12. NIS+ ホームドメインサーバーのアドレスを入力して、Enter キーを押します。
13. NIS+ ホームドメイン名を入力して、Enter キーを押します。
14. NIS+ サーバーの、セキュリティー保護された RPC パスワードを入力します。Enter キーを押します。
15. コロンで区切ったドメインのリストの形式で検索パスを入力します。ホームドメインとその親のみを検索する場合、このフィールドは空白のままにします。Enter キーを押します。
16. 「7. Save changes」を選択します。

ネームサービスの検索順序の設定

ユーザー、グループ、およびホストの検索機能で最初に使用されるサービスを選択できます。

▼ 検索順序を設定する

1. 「Configuration」メニューから「Lookup orders」を選択します。
2. 「1. Edit fields」を選択します。
3. ユーザー情報を解決する順序 (NIS または NIS+ のいずれか) を選択して、Enter キーを押します。
4. グループ情報を解決する順序 (NIS または NIS+ のいずれか) を選択して、Enter キーを押します。
5. ホスト情報を解決する 1 ～ 4 番めのサービスを選択して、Enter キーを押します。
6. 「7. Save changes」を選択します。

サーバーファイルシステムの管理

コンソールでは、いくつかの手順を実行して、サーバーファイルシステム (SFS) ボリュームを管理できます。一般的な手順を次に示します。

- ドライブ文字の構成

- 新しいディスクボリュームの構成
- ディスクパーティションの名前の変更
- ディスクボリュームの削除
- 割り当ておよびチェックポイントの使用可能および使用不可への切り替え

ドライブ文字の構成

ドライブ文字は、サーバーメッセージブロック (SMB)/CIFS を使用して共有可能なファイルボリュームに自動的に割り当てられます。`\cvol` にのみ割り当てることができるドライブ `C:` を除き、コンソールを使用してドライブ文字の割り当てを手動で行うことができます。

使用できるドライブ文字がなくなる場合もあり、その際は次のログメッセージが表示されます。

```
No drive letter available
```

このメッセージは情報提供のみを目的としています。ファイルシステムは作成されますが、ドライブ文字を割り当てるには、現在ほかのファイルシステムに使用されているドライブ文字を割り当て直す必要があります。

▼ ファイルボリュームへのドライブ文字の再割り当てを手動で行う

1. 「Configuration」メニューから「Drive Letters」を選択します。
2. 変更するドライブ文字を入力して、Enter キーを押します。
3. ドライブ文字に新たに割り当てるファイルボリューム名を入力して、Enter キーを押します。

   ドライブ文字には既存のファイルボリュームのみを割り当てることができます。
4. Esc キーを押して、この画面を終了します。

▼ 新しいディスクボリュームを作成する

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 構成するドライブの文字を入力します。
3. 「1. Edit」を選択します。

4. 「1. Create partition」を選択します。
5. ドライブのパーティションタイプを選択するか、Enter キーを押してデフォルトを受け入れます。たとえば、`sfs2` (一次ボリューム) または `sfs2ext` (セグメント) などです。
6. ディスクボリュームラベルを入力して、Enter キーを押します。

   このボリュームで規制適合アーカイブ機能を使用可能にするかどうかを尋ねるメッセージが表示されます。
7. Compliance Archiving Software のライセンスがあり、規制適合対応のボリュームを作成する場合は、Y を押します。

注 – Sun StorEdge 5310 Gateway システムの構成では、推奨実施はサポートされていますが必須実施はサポートされていません。

注意 – いったんボリュームに対して必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

---

8. Enter キーを押してデフォルトのサイズを選択するか、ディスクボリュームのサイズを M バイト単位で入力して Enter キーを押します。
9. 「7. Proceed with create」を選択します。

   「`Initialization OK`」および「`Mount OK`」というメッセージが表示されるまで待機し、Esc キーを押して「Configure Disk」メニューに戻ります。
10. 新しいファイルボリュームの作成が終了したら、メインメニューが表示されるまで Esc キーを押します。

▼ パーティションの名前を変更する

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 名前を変更するドライブの文字を入力します。
3. 「1. Edit」を選択します。
4. 「3. Rename」を選択します。
5. パーティションの新しい名前を入力して、Enter キーを押します。

注 – 厳格な規制適合対応のボリュームは、名前を変更できません。

▼ 拡張セグメントを追加する

拡張セグメントを追加するには、まずそのボリューム上に `sfs2ext` パーティションを作成する必要があります。

注 – `sfs` ファイルボリュームに拡張ボリュームを配置したあと、これを切り離すことはできません。これは取り消し不可能な操作です。拡張ボリュームを切り離すには、`sfs` ファイルボリュームを削除する必要があります。

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 構成するドライブの文字を入力します。

注 – ディスクドライブ (ディスクボリューム) の数が 26 個を超えている場合は、スペースキーを押して探します。

3. 変更するパーティションの横に表示されている数字を入力します。
4. 「5. Segments」を選択します。
5. 「1. Add an extension segment」を選択します。
6. 拡張ドライブの横に表示されている文字を選択します。
7. 「7. Proceed」を選択します。

▼ ディスクボリュームを削除する

注 – 必須実施の規制適合対応のボリュームは、削除できません。

注意 – ボリュームを削除すると、ボリューム内のすべてのデータが失われます。

▼ ディスクボリュームを削除する

1. 「Configuration」メニューから「Disks & Volumes」を選択します。

2. 構成するドライブの文字を入力します。

注 – ディスクドライブ (ディスクボリューム) の数が 26 個を超えている場合は、スペースキーを押して探します。

---

3. 「1. Edit」を選択します。
4. 「8. Delete」を選択します。
5. ディスクボリューム名を入力して、Enter キーを押します。
6. 「7. Proceed with delete」を選択します。「`Delete OK`」および「`Delpart OK`」というメッセージが表示されるまで待機します。
7. Esc キーを押して「Configure Disk」メニューに戻ります。
8. メインメニューが表示されるまで Esc キーを押します。

共有および割り当ての管理

コンソールを使用して、共有および割り当てを管理できます。

SMB/CIFS 共有の設定

CIFS は、SMB プロトコルを使用する Windows のファイル共有サービスです。CIFS は、Windows クライアントシステムが Sun StorEdge 5310 NAS Appliance 上のファイルにアクセスするためのメカニズムを提供します。

▼ 共有を設定する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「A. Domain Configuration」を選択します。
3. 「Domain」フィールドにワークグループまたはドメインの名前を入力します。
4. 必要に応じて、ドメインの適用範囲を定義します。
5. Sun StorEdge 5310 NAS Appliance サーバーの説明を入力します。
6. 必要に応じて、プライマリおよびセカンダリの WINS サーバーの IP アドレスを入力します。

7. 「Keep Alive」パラメータを割り当てます。

   これは、アクティブでない接続をシステムが切断するまでの秒数です。

8. セキュリティーモードに「Secure Share Level」または「NT Domain Auto UID」を割り当てます。

9. 「NT Domain Auto UID」モードを使用する場合は、管理者ユーザーの名前およびパスワードを入力します。

10. 「7. Save changes」を選択します。

    「Secure Share Level」および「NT Domain Auto UID」間でセキュリティーモードを変更した場合、Sun StorEdge 5310 NAS Appliance が再起動します。

自動ホーム SMB/CIFS 共有の設定

自動ホーム共有は、ユーザーがシステムにログインすると作成され、ログアウトすると削除される、一時的な共有です。

自動ホーム共有機能では、次に定義する状態および自動ホームパスの 2 つの構成パラメータが必要になります。

- 状態パラメータは、自動ホーム共有機能を使用可能にするか使用不可にするかを決定します。この機能の現在の状態は、環境変数 `smb.autohome.enable` によって保持されます。必ず yes または no を指定してください。
- 自動ホームパスパラメータは、一時的な共有のベースディレクトリのパスを定義します。これは、`smb.autohome.path` 環境変数によって定義されます。たとえば、ユーザーのホームディレクトリが `/vol1/home/john` である場合、自動ホームパスは `/vol1/home` に設定します。一時的な共有の名前は、`john` になります。ユーザーのホームディレクトリの名前は、ユーザーのログイン名と同じである必要があります。

この機能が使用不可である場合、自動ホームパスパラメータは無効となり評価されません。

この機能が使用可能で、パスの文字列の長さが 0 である場合には、構成は無視されます。この機能が使用可能で、パスの文字列の長さが 0 でない場合は、パスが評価されます。自動ホームパスパラメータが既存のディレクトリパスを示していないと、システムログに情報メッセージが書き込まれます。たとえば、`/vol1/home` をベースパスに指定した場合は、次のようなログメッセージが書き込まれます。

```
SMB autohome: /vol1/home: no such directory
```

このログメッセージはシステム管理者に状況を通知するためのもので、構成は有効なままになります。システムは正常に動作しますが、自動ホーム共有は作成されません。そのあと指定したディレクトリパスが作成されると、その時点で、必要に応じて自動ホーム共有が追加および削除されます。

▼ 自動ホーム共有を使用可能にする

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「F. Autohome Setup」を選択します。
3. 「1. Edit fields」を選択します。
4. 「Y. Yes」を選択して、自動ホーム共有を使用可能にします。
5. 自動ホームパスを入力します。

   自動ホームパスとは、共有のベースディレクトリのパスです。たとえば、ユーザーのホームディレクトリが `/usr/home/john` である場合、自動ホームパスは `/usr/home` に設定します。一時的な共有の名前は `john` になります。システムでは、ユーザーのホームディレクトリの名前は、ユーザーのログイン名と同じであると見なされます。
6. 「7. Save changes」を選択します。

▼ 共有を定義する

SMB/CIFS の設定が終了したあと、SMB/CIFS 共有を定義する必要があります。Windows ユーザーは、共有を使用して Sun StorEdge 5310 NAS Appliance 上のディレクトリにアクセスできます。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「E. Shares」を選択します。
3. 「8. Add a share」を選択します。
4. 共有名を入力します。
5. ボリューム/ディレクトリの形式で、ディレクトリのパスを入力します。
6. 必要に応じて、このディレクトリに関するコメントを入力します。
7. システムがワークグループモードで構成されている場合は、次の手順を実行します。

   a. 「Password Protection」のプルダウンメニューで、「Yes」または「No」を選択します。

      これを使用可能に設定すると、読み取り/書き込みまたは読み取り専用のいずれかを選択するオプションが表示されます。

   b. ユーザー ID、グループ ID、および umask を入力します。
8. 「7. Save changes」を選択します。

▼ 共有を編集する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「E. Shares」を選択します。
3. 編集する共有に対応する文字を入力します。
4. 「1. Edit fields」を選択します。
5. 新しい共有名、ディレクトリ、コメント、パスワード情報、ユーザー ID、およびグループ ID を入力します。
6. 前節の 212 ページの「共有を定義する」の手順 7 の説明に従って、ADS コンテナを入力します。
7. 「7. Save changes」を選択します。

▼ 共有を削除する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「E. Shares」を選択します。
3. 削除する共有に対応する文字を入力します。
4. 「8. Delete」を選択します。

Active Directory サービスの設定

この画面で Active Directory サービスを使用可能にして設定を行うと、Sun StorEdge 5310 NAS Appliance は自動的に ADS 更新を実行します。

▼ ADS サービスを使用可能にする

1. 「Extensions」メニューから「ADS Setup」を選択します。
2. 「1. Edit fields」を選択します。
3. 「Y. Yes」を選択して、ADS クライアントによる ADS への Sun StorEdge 5310 NAS Appliance 共有の公開を許可します。
4. ADS が動作している Windows ドメインを入力します。
   Sun StorEdge 5310 NAS Appliance もこのドメインに属している必要があります。

5. 管理権限のある Windows ユーザーの名前を入力します。

   ADS クライアントでは、このユーザーによるセキュリティー保護された ADS の更新が検証されます。

6. Windows の管理者ユーザーのパスワードを入力します。

7. 「User Container」フィールドに、Windows の管理者ユーザーの ADS パスを LDAP の DN 記法で入力します。

   詳細は、79 ページの「ADS を使用可能にする」を参照してください。

8. 「Site」フィールドにローカル ADS サイト名を入力します。

9. ADS の識別に使用される Kerberos レルム名を大文字で入力します。

   通常、これは ADS ドメインになります。

10. Kerberos 鍵配布センター (KDC) サーバーのホスト名を入力します。

    通常、これは ADS ドメインのメインドメインコントローラのホスト名です。ADS クライアントまたは動的 DNS クライアントが DNS を介して KDC サーバーを検索できる場合は、このフィールドを空白のままにします。

11. 「7. Save changes」を選択します。

割り当てを使用可能および使用不可にする方法

割り当ては、それぞれのユーザーおよびグループが使用するディスク領域の量を追跡および制限します。割り当ての追跡機能をオンまたはオフにすることができます。この機能は、割り当ての使用可能または使用不可への切り替えのみを行うことができます。割り当ての制限の設定は行いません。

注 – 割り当ての初期化には数分かかります。その間、ボリュームはロックされ、ユーザーが使用することはできません。

▼ 割り当てを使用可能または使用不可にする

1. 「Configuration」メニューから「Disks & Volumes」を選択します。

2. 割り当てを使用可能にするドライブを選択します。

3. 「1. Edit」を選択します。

4. 「4. Quotas on/off」を選択します。

5. 「1. Turn quotas on」または「8. Turn quotas off」を選択します。

セキュリティー

グループと資格のマッピングを設定することで、セキュリティー保護を確実に実施できます。

ユーザーグループの構成

組み込みローカルグループの要件は、Windows NT システムのローカルグループの要件とは異なります。ユーザーグループの詳細は、85 ページの「ローカルグループ」を参照してください。

▼ グループを追加する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 「8. Add a Group」を選択して、ローカルグループを追加します。
4. グループの名前を入力して、Enter キーを押します。
5. 必要に応じて、グループの説明を入力し、Enter キーを押します。
6. 「7. Save changes」を選択して、新しいグループを保存します。

▼ グループにメンバーを追加する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 変更するグループの文字を押します。
4. 「2. Members」を押して、グループのメンバーシップを変更します。
5. 「8. Add」を押して、メンバーを追加します。
6. 「ドメイン\ユーザー名」の形式でドメインおよびユーザー名を入力します。

   ドメインとは、ユーザー名を認証できるドメインです。たとえば、`BENCHLAB\john` と入力した場合は、`john` というユーザーを認証できるドメイン `BENCHLAB` を指定したことになります。
7. Enter キーを押します。
8. 「7. Save changes」を押して、新しいメンバーを保存します。

▼ グループからメンバーを削除する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 変更するグループの文字を押します。
4. 「2. Members」を押して、グループのメンバーシップを変更します。
5. 削除するグループメンバーに対応する文字を押します。
6. プロンプトが表示されたら「Y」を押します。

グループ権限

ユーザーグループの権限の詳細は、86 ページの「ローカルグループの権限の構成」を参照してください。

▼ ローカルグループの権限を変更する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 変更するグループの文字を押します。
4. 「3. Privileges」を押して、グループメンバーの権限を変更します。
5. 追加または削除する権限の文字を押します。
6. 「7. Save changes」を押して、変更内容を保存します。

ユーザーマップとグループマップ

ユーザーおよびグループの資格の詳細は、91 ページの「ユーザーおよびグループの資格のマッピング」を参照してください。

▼ ユーザーマップを追加する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。

2. 「C. User Mapping」を選択します。
3. 「8. Add a map」を押します。
4. 「Account」フィールドに、UNIX ユーザーにマッピングする NT ユーザーのドメインおよび名前を入力します。
   「ドメイン\ユーザー名」の形式を使用します。
5. 「Name」フィールドに、NT ユーザーにマッピングする UNIX ユーザーの名前を入力します。
6. 「7. Save changes」を押します。

▼ ユーザーマップを編集する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「C. User Mapping」を選択します。
3. 編集するマップの文字を押します。
4. 「1. Edit Fields」を押します。
5. 変更内容を入力して、Enter キーを押します。
6. 「7. Save changes」を押します。

▼ ユーザーマップを削除する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「C. User Mapping」を選択します。
3. 削除するユーザーマップの文字を押します。
4. 「8. Delete」を押します。

▼ グループマップを追加する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「D. Group Mapping」を選択します。
3. 「8. Add a map」を押します。
4. 「Account」フィールドに、UNIX グループにマッピングする NT グループのドメインおよび名前を入力します。「ドメイン\ユーザー名」の形式を使用します。

5. 「Name」フィールドに、NT グループにマッピングする UNIX グループの名前を入力します。
6. 「7. Save changes」を押します。

▼ グループマップを編集する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「D. Group Mapping」を選択します。
3. 編集するグループマップの文字を押します。
4. 「1. Edit Fields」を押します。
5. 変更内容を入力して、Enter キーを押します。
6. 「7. Save changes」を押します。

▼ グループマップを削除する

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「D. Group Mapping」を選択します。
3. 削除するグループマップの文字を押します。
4. 「8. Delete」を押します。

マッピングおよびセキュリティー保護が可能なオブジェクト

この節では、ユーザーまたはグループの資格のマッピングと、ファイルシステムに含まれるファイルやディレクトリなどの、セキュリティー保護が可能なシステム内のオブジェクトとの間の相互作用について詳細に説明します。

システム上のオブジェクトは、そのセキュリティー属性が設定されたドメインに応じて分類されます。NFS プロトコルを使用して作成されたオブジェクトは UNIX のセキュリティー属性のみを保持するため、UNIX オブジェクトとして分類されます。SMB プロトコルを使用して作成されたオブジェクトは UNIX および Windows の両方のセキュリティー属性を保持しますが、Windows オブジェクトとして分類されます。セキュリティー属性の変更に伴うドメイン間の移行をオブジェクトに許可することも可能ですが、一方向の移行のみを許可するようにポリシーで定められています。SMB を使用してセキュリティー属性を変更すると、UNIX オブジェクトは Windows オブジェクトになります。デフォルトでは、NFS を使用して Windows オブジェクトのセキュリティー属性を変更することはできません。これは、Windows セキュリティーがセキュリティー記述子に基づいて設定されており、UNIX のセキュリティー

属性では必ずしも正確に表すことができないためです。Windows オブジェクトから UNIX オブジェクトへの変更を許可すると、オブジェクトを保護するアクセス制御を弱める可能性があります。

NFS を介して Windows オブジェクトの属性を変更するメカニズムには、chsmb コマンドと acl.overwrite.allowed 環境変数の 2 つがあります。

acl.overwrite.allowed が存在しないか no に設定されている場合は、デフォルトの動作が適用されるため、NFS を介して Windows オブジェクトの属性を変更することはできません。

acl.overwrite.allowed 環境変数が yes に設定されていると、標準的な UNIX のアクセス規則に従って、chown、chgrp、chmod などの UNIX コマンドが許可されます。NFS を使用して Windows オブジェクトの属性を変更すると、Windows セキュリティー記述子は削除され、オブジェクトは UNIX オブジェクトになります。

chsmb コマンドを使用すると、単一の Windows セキュリティー記述子、または 1 つのボリューム内の Windows セキュリティー記述子データベース全体を削除できます。chsmb コマンドを個別のファイルまたはディレクトリに適用するには、そのオブジェクトに対する絶対パスを指定する必要があります。chsmb では再帰的な処理が実行されないため、このコマンドをディレクトリに適用した場合、ディレクトリに含まれるサブディレクトリやファイルは影響を受けません。chsmb コマンドの使用例を次に示します。

/vol1/shared/bin/file.doc 上のセキュリティー記述子を削除して UNIX のアクセス権に戻すには、次のコマンドを使用します。

```
chsmb /vol1/shared/bin/file.doc
```

/vol1 上のすべてのセキュリティー記述子を削除し、すべてのファイルをそれぞれの UNIX のアクセス権に戻すには、次のコマンドを使用します。

```
chsmb /vol1
```

chsmb コマンドはファイルのセキュリティーに影響を及ぼすため、このコマンドを使用する際は特に注意してください。ボリュームが指定されると、chsmb コマンドは処理を実行する前に警告を出し、確認のプロンプトを表示します。

Windows ユーザーが Windows オブジェクトにアクセスする際は、マッピングは実行されません。同様に、UNIX ユーザーが UNIX オブジェクトにアクセスする際にも、マッピングは実行されません。これらはネイティブなアクセス状況と見なされます。また、Windows オブジェクトには Windows および UNIX の両方のセキュリティー属性が含まれるため、UNIX ユーザーが Windows オブジェクトにアクセスする際は、ネイティブなアクセス状況ではありませんが、マッピングを必要としません。これは、独立した中立のマッピングを作成するのではなく、1 つのドメインをデフォルトのマッピングとして選択する設計であることの直接的な利点です。したがって、マッピングが必要になるのは、Windows ユーザーが UNIX オブジェクトにアクセスする場合のみです。Windows ユーザーが UNIX オブジェクトにアクセスする場合は、オブジェクトの UNIX セキュリティー属性が Windows ドメインにマッピングされ、Windows のセキュリティーポリシーが適用されます。

ホストリストの構成

コンソールを使用して、ホスト情報を設定できます。

▼ ホストを追加する

1. 「Configuration」メニューから「Hosts」を選択します。
2. 新しいホスト名を入力して、Enter キーを押します。
   システムによって、そのホスト名がまだ使用されていないことが確認されます。
3. Enter キーを押して、ホストを追加します。
4. 新しいホストの IP アドレスを入力します。
5. 「7. Save changes」を選択します。

▼ 既存のホストを編集する

1. 「Configuration」メニューから「Hosts」を選択します。
2. 編集するホストの名前を入力して、Enter キーを押します。
3. 「1. Edit」を選択します。
4. 新しいホストの名前または IP アドレスを入力します。
5. 「7. Save changes」を選択します。

▼ ホストを削除する

1. 「Configuration」メニューから「Hosts」を選択します。
2. 削除するホストの名前を入力して、Enter キーを押します。
3. 「8. Delete」を選択します。

承認されたホストの管理

「Trusted Hosts」メニューオプションを使用して、すべてのリソースへの無制限のアクセス権を持つホストを管理します。

▼ 承認されたホストを指定する

1. 「Access Control」メニューから「Trusted Hosts」を選択します。
2. ホスト名を入力して、Enter キーを押します。

注 – ユーザーが承認されたホストを追加するには、そのホストがホストリストまたは NIS に存在する必要があります。

システムによって、そのホストの名前が承認されたホストとしてまだ指定されていないことが確認されます。すでに承認されたホストとして存在する場合は、ホストの情報が表示されます。ホストが承認されていない場合は、警告が表示されます。

3. 「7. Add to list」を選択します。

   新しく承認されたホストが追加され、画面の上部に名前が表示されます。

▼ 承認されたホストを削除する

1. 「Access Control」メニューから「Trusted Hosts」を選択します。
2. 削除する承認されたホストの名前を入力して、Enter キーを押します。
3. 「8. Delete」を選択します。

   承認されたホストがリストから削除されます。

ボリュームアクセスの管理

変更内容を保存すると、クライアントによる既存の NFS マウントが更新され、新しいパラメータが反映されます。

cvol ボリュームに対しては、読み取りおよび書き込みを含むすべてのアクセスを禁止してください。

注 – 承認されたホストには、ボリュームのアクセス権の設定にかかわらず、ファイルボリュームの読み取り/書き込みアクセス権が自動的に付与されます。

▼ NFS クライアントのボリュームアクセスを管理する

1. 「Access Control」メニューから「Volume Access」を選択します。
2. アクセス権を変更するボリュームに対応する文字を入力します。
3. 割り当てるアクセスのタイプ (読み取り/書き込み、読み取り専用、またはアクセス不可) に対応する番号を入力します。

注 – 承認リストに含まれるホストは、ボリュームアクセスパラメータの設定にかかわらず、読み取り/書き込みアクセスを許可されます。

4. 「7. Save changes」を選択します。

コンソールのロックおよびロック解除

コンソールの不正な使用を防ぐため、コンソールを使用して、ほとんどのメインメニューオプションを使用可能または使用不可に切り替えることができます。コンソールを保護するには、管理パスワードを設定する必要があります。

▼ コンソールをロックする

1. 「Operations」メニューから「Lock Console」を選択します。
2. 管理パスワードを入力します。
3. 「Y (Yes)」を選択します。

▼ コンソールのロックを解除する

1. メインメニューから「Unlock Console」を選択します。
2. 管理パスワードを入力します。
3. 「Y (Yes)」を選択します。

ファイルボリュームのミラー化

この節では、Sun StorEdge 5310 NAS Appliance のアクティブシステムから、Sun StorEdge 5310 NAS Appliance のミラーシステムへ、ファイルボリュームをミラー化する方法について説明します。ミラー化の詳細は、第 9 章を参照してください。

注 – Sun StorEdge 5310 Cluster でファイルの複製機能を使用する際、クラスタが縮退状態にある場合には役割の変更などのミラー化処理を実行しないでください。

アクティブサーバーおよびミラーサーバーの構成

アクティブサーバーおよびミラーサーバー上でプライマリ IP アドレスを構成し、Sun StorEdge 5310 NAS Appliance のミラーサーバーを相互に接続するポートの役割を指定したあとで、コンソールインタフェースを使用してアクティブサーバーおよびミラーサーバーのミラー化を構成できます。

▼ 新しいアクティブサーバーに新しいミラーサーバーを構成する

1. 「Configuration」メニューから「Host Names and Network」を選択します。
2. 「1. Edit Fields」を選択します。
3. ローカルネットワークまたはサブネットに接続するポートを構成していない場合は、ポートを構成します。

   コンソールを使用した TCP/IP の設定の詳細は、197 ページの「TCP/IP を構成する」を参照してください。ポートの構成の詳細は、第 5 章を参照してください。
4. アクティブシステムとミラーシステムとの接続に使用するポートにサーバー名および IP アドレスを割り当てます。
5. アクティブサーバーとミラーサーバーとの接続に使用するポートの「Role」フィールドで、「Mirror」を選択します。
6. 「Save」を選択して変更を保存し、メインメニューに戻ります。
7. DNS サービスおよび NIS/NIS+ サービスが使用可能である場合はこれを設定し、ネームサービスの検索順序を設定します。

   ネームサービスの設定の詳細は、202 ページの「ネームサービス」を参照してください。
8. Telnet ウィンドウを開いてミラーシステムにアクセスし、手順 1 ～手順 6 を繰り返します。

   これで、アクティブシステムおよびミラーシステムのネットワーク接続が構成されました。続けて次の節を参照してください。

▼ 既存のアクティブサーバーに新しいミラーサーバーを構成する

1. アクティブサーバー上で、「Configuration」メニューから「Host Names and Network」を選択します。
2. 「1. Edit Fields」を選択します。
3. アクティブシステムとミラーシステムとの接続に使用するポートに、サーバー名と IP アドレスを割り当てます。
4. アクティブサーバーとミラーサーバーとの接続に使用するポートの「Role」フィールドで、「Mirror」を選択します。
5. Telnet ウィンドウを開いてミラーシステムにアクセスし、手順 1 ～手順 4 を繰り返します。

6. アクティブサーバーの Telnet ウィンドウで、次のコマンド行が表示されるまで Esc キーを押します。

   ```
   connect to (? for list) ?[menu]
   ```

7. 管理者としてログインして次のように入力します。

   ping *xxx.xxx.xx.xx*

   xxx.xxx.xx.xx は、ミラーサーバーの IP アドレスです。

8. ミラーサーバー上で手順 7 を繰り返し、アクティブサーバーの IP アドレスを入力します。

これで、アクティブシステムおよびミラーシステムのネットワーク接続が構成されました。次に進んで、ミラー化するファイルボリュームを構成してください。

ファイルボリュームの構成

ミラー化は、ボリューム単位で実行されます。使用しているボリュームの一部またはすべてをミラー化できます。

注 – いったんファイルボリュームをミラー化すると、ミラー接続が保持されている間は、元のファイルボリュームの名前を変更できません。ミラー化できるのは、1G バイト以上のファイルボリュームのみです。

▼ ミラー化するファイルボリュームを設定する

次の手順は、まずアクティブシステムで実行し、次にミラーシステムで実行してください。

1. ほかのボリュームを作成する前に、小さい (たとえば 32M バイトの) ファイルボリュームを `SYS` という名前で作成します。

   アクティブシステム上にすでにファイルボリュームがある場合は、この手順は任意です。

2. 「Configuration」メニューから「Disks and Volumes」を選択します。
3. 新しいファイルボリュームを作成するドライブを選択します。
4. 「Create & init partition」を選択します。次に「1. sfs2」を選択します。
5. 名前に「SYS」と入力し、サイズには M バイト単位で 64 と入力します。

   この操作によって、`/etc` ディレクトリおよびそれに含まれる Sun StorEdge 5310 NAS Appliance の構成ファイルが、強制的に `SYS` ボリューム内に格納されます。

   ミラーシステムには、これ以外のファイルボリュームを作成しないでください。

▼ ファイルボリュームをミラー化する

1. Telnet を使用してアクティブシステムに接続し、メインメニューを表示します。
2. 「Operations」メニューから「Licenses」を選択し、「Mirroring」に対応する文字を選択します。
3. ご購入先から提供された起動キーを正確に入力します。
4. メインメニューが表示されるまで、Esc キーを押します。
5. 「Extensions」メニューから、「Mirrors」を選択します。
6. 「Add mirror」を選択して新しいミラーを作成します。
7. ミラー化するファイルボリュームに対応する文字を入力して、ファイルボリュームを選択します。

   ファイルボリュームは、1G バイト以上である必要があります。
8. ミラーシステムのホスト名を入力します。
9. 必要に応じてプライベート IP アドレスを入力します。

   これは、ミラーサーバーとのミラー接続に使用される IP アドレスです。
10. 「Alt IP Address」フィールドに代替 IP アドレスを入力します。
11. ミラーサーバーへのアクセスに管理パスワードが必要な場合は、「Remote admin password」フィールドに管理パスワードを入力します。
12. トランザクションバッファーの予約サイズを入力して、Enter キーを押します。
13. 「7. Proceed」を選択して、ミラー化されたファイルボリュームを追加します。

    ミラーボリュームがアクティブボリュームと「in sync」の状態になると、ミラーボリュームが読み取り専用でマウントされます。

    注 – ミラーの初期同期中に、アクティブサーバーに対して入出力動作を行うことはできません。

    ミラーの作成中および作成後は、システムに「Mirror Creation」画面が表示されます。
14. ミラー状態を確認するには、「A」を選択します。
15. 代替 IP アドレスまたは管理者パスワードを編集するには、「1. Edit」を選択します。

警告しきい値の設定

トランザクションバッファーとして予約した領域がいっぱいになり制限を超えると、ミラーは「破損」します。この画面では、警告が送信される使用率を設定できます。デフォルトの使用率は、70、80、および 90% です。

▼ 警告が送信される使用率のしきい値を設定する

1. アクティブシステム上で、「Extensions」メニューから「Mirrors」を選択します。
2. 「3. Threshold Config」を選択します。
3. 「1. Edit」を選択して、この画面に表示される使用率を編集します。
4. 設定する使用率を入力します。
5. 「Alert Silent Period」フィールドで、システムが同じしきい値警告をふたたび送信するまで待機する時間数を入力します。
6. 「7. Proceed」を選択します。

ミラー化されたファイルボリュームのプロモート

アクティブシステムに障害が発生した場合に、ミラーシステムは高可用性を提供します。ミラー化されたファイルボリュームをネットワークユーザーが使用できるようにするには、ファイルボリュームをプロモートします。まず、アクティブファイルボリュームとミラー化されたファイルボリュームとの間のアクティブミラー接続を切断して、ミラーを切り離す必要があります。次に、ボリュームをプロモートし、ミラー化されたファイルボリュームのアクセス権を設定します。いったんミラーを切断してミラー化されたファイルボリュームをプロモートすると、2 つのファイルボリュームは完全に独立した状態になります。

▼ ミラーシステムでファイルボリュームをプロモートする

1. ミラーシステム上で「Configuration」メニューから「Disks & Volumes」を選択し、ファイルボリュームの状態を表示します。

   ミラー化されたファイルボリュームの名前の後ろにアスタリスク (*) が表示され、そのファイルボリュームが現在ミラー化されていることを示します。

注 – ミラーシステムからミラー化されたファイルボリュームを切断するのは、アクティブシステムが使用できない場合にかぎります。アクティブシステムが使用可能な場合にファイルボリュームをプロモートするには、ミラーシステムからではなく、アクティブシステムからミラーを切断してください。

---

2. 「Extensions」メニューから、「Mirrors」を選択します。
3. 切断するミラー化されたファイルボリュームに対応する文字を選択します。
4. 「8. Break」を選択します。
5. 切断を確認するプロンプトが表示されたら、「Y. Yes」を選択して次に進みます。
6. Esc キーを押して、「Mirrors」のメイン画面に戻ります。
7. 「Extensions」メニューから、「Mirrors」を選択します。
8. 「1. Promote Volume」を選択します。
9. プロモートするファイルボリュームに対応する文字を選択します。
10. 「7. Proceed」を選択して、ファイルボリュームをプロモートします。

    この処理が完了するまでに数分かかる場合があります。ミラー化されたファイルボリュームをプロモートするには、少なくとも一度はそのボリュームが「In Sync」の状態になっている必要があります。
11. ファイルボリュームのプロモートが完了したら、Esc キーを押してメインメニューに戻ります。
12. (任意) NFS ファイルボリュームアクセスを構成するには、「Access Control」メニューから「Volume Access」を選択します。
13. ファイルボリュームに対応する文字を選択して、ファイルボリュームにアクセス権を設定します。
14. 「Read/write」、「Read only」、または「None」のいずれかを選択します。
15. 「7. Save changes」を選択して次に進みます。

    ボリュームがプロモートされました。ミラーを再確立するには、次の節の、227 ページの「ミラーの再確立」を参照してください。

ミラーの再確立

ここでは、アクティブサーバーに障害が発生してミラーサーバー上のファイルボリュームをプロモートしたときに、ミラーを再確立する方法について説明します。プロモートしたファイルボリュームが最新のバージョンになり、アクティブシステム上の古いファイルボリュームから完全に独立して機能します。ミラーを再確立するには、最新のファイルボリュームをアクティブサーバーにミラー化し、そのファイルボリュームをミラーサーバーにミラー化して元の状態に戻す必要があります。

注 – ミラー化されたファイルボリュームをプロモートしていない場合は、次の手順を実行しないでください。アクティブシステムがオンラインに戻ると、ミラーが自動的に「In Sync」の状態に戻されます。

次の例では、サーバー 1 がアクティブサーバー、サーバー 2 がミラーサーバーです。

ミラーを再確立するには、次の手順を実行します。

1. サーバー 1 でミラーを切断
2. サーバー 1 から古いファイルボリュームを削除
3. サーバー 2 の最新のファイルボリュームをサーバー 1 にミラー化
4. 役割の変更。サーバー 1 をふたたびアクティブにしてサーバー 2 をミラーサーバーに変更。

アクティブサーバーは、オンラインになるときにミラーの再確立を試みる場合があります。そのため、サーバー 1 でミラーを切断する必要があります。

▼ サーバー 1 でミラーを切断する

1. サーバー 1 で、「Extensions」メニューから「Mirrors」を選択します。
2. ミラー化されたファイルボリュームに対応する文字を選択します。
3. 「8. Break」を選択します。
4. 「Y. Yes」を選択してミラーの切断を確定します。

▼ サーバー 1 から古いファイルボリュームを削除する

1. Esc キーを押して、メインメニューに戻ります。
2. 「Configuration」メニューから「Disks & Volumes」を選択します。
3. ミラー化されたファイルボリュームに対応する数字を選択します。

注意 – 次の手順を実行する前に、削除しようとしているのはサーバー 1 の古いファイルボリュームであることを確認してください。また、サーバー 2 の最新のファイルボリュームを確認し、最初にプロモートしておいてください。

4. 「8. Delete」を選択します。
5. 古いファイルボリュームのファイル名を入力します。
6. 「7. Proceed with delete」を選択して、古いファイルボリュームを削除します。

▼ サーバー 2 の最新のファイルボリュームをサーバー 1 にミラー化する

1. サーバー 2 で、「Extensions」メニューから「Mirrors」を選択します。
2. 「8. Add mirror」を選択します。
3. ミラー化するファイルボリュームに対応する文字を選択します。
4. サーバー 1 のプライベートホスト名を入力します。
5. プライベート IP アドレスを入力し、必要に応じて管理者パスワードを入力します。
6. トランザクションバッファーの予約サイズを入力します。

   詳細は、225 ページの「ファイルボリュームをミラー化する」を参照してください。
7. 「7. Proceed」を選択します。
8. ミラーの作成中、ミラー化された新しいファイルボリュームに対応する文字を選択します。

   ミラーが「In Sync」の状態になると、サーバー 1 とサーバー 2 の両方にファイルボリュームの同一のコピーが存在するようになります。続けて次の節を参照してください。

▼ 役割を変更する

注 – 役割を変更する前に、ボリュームが In sync 率 100% の状態であることを確認してください。

---

1. メインメニューから、サーバー 1 の「Mirror」オプションを選択します。
2. 該当する文字を押して、対象のボリュームを選択します。

   たとえば、「A」を押して `cvol1` ファイルボリュームを選択します。
3. 「Mirror Status」メニューから、「Change Role」オプションを選択します。
4. 「Yes」を選択して確定します。

監視

コンソールを使用して監視機能を実行できます。

SNMP の構成

「SNMP」メニューでは、遠隔の SNMP (ネットワーク管理プロトコル) モニターにメッセージを送信し、コミュニティー文字列、連絡先情報、および SNMP モニターの場所を変更できます。

▼ SNMP を構成する

1. 「Extensions」メニューから「SNMP Configuration」を選択します。

   デフォルトのコミュニティー名は public です。任意の名前を入力できます。

2. トラップ先を追加、編集、または削除するには「1-5. Edit a Trap Destination」、コミュニティー文字列を編集するには「6. Edit Community」、連絡先情報を編集するには「7. Edit Contact」、遠隔 SNMP モニターの場所を編集するには「8. Edit Location」を選択します。

3. 「Y. Yes」を選択して、変更内容を保存します。

電子メール通知の構成

システムに問題が発生すると、Sun StorEdge 5310 NAS Appliance は特定の受信者に電子メールメッセージを送信します。

注 – 電子メール通知が正しく機能するように DNS を構成する必要があります。

▼ 電子メール通知を構成する

1. 「Extensions」メニューから、「EMAIL Configuration」を選択します。

2. 「1. Edit fields」を選択します。

3. 各フィールドに必要な情報を入力します。フィールド間を移動するには Enter キーを押します。

   - SMTP Server − すべてのメールが送信されるメールサーバー。ホストファイルまたは DOS サーバーに、このサーバー名が含まれている必要があります。

注 – IP アドレスまたは名前を使用できます。名前の場合は、DNS サーバーが解釈処理できる名前を使用する必要があります。

   - Recipient 1 ～ 4 − 問題の発生時に自動的に通知が送信される 4 人の受信者の電子メールアドレス。

- Notification Level ― 電子メールを使用して受信者に通知が送信される問題のレベル。次のいずれかを選択します。
  - Errors ― エラーの発生時にのみ通知が送信されます。
  - Errors and warnings ― エラーおよび優先順位が低い警告の発生時に通知が送信されます。
  - None ― 通知は送信されません。

4. 現在の構成を保存するには、「7. Save changes」を選択します。
5. Esc キーを押して、メインメニューに戻ります。

システム情報の表示

コンソールにシステム情報を表示できます。

▼ サーバーの状態を表示する

1. 「Operations」メニューから「Activity Monitor」を選択します。

   アクティビティーモニターの画面には、次の情報が表示されます。
   - Volume ― 最初の 22 個のファイルボリューム
   - Use% ― ボリューム上の使用済み領域
   - Reqs ― 直前の 10 秒間にボリュームに対して処理された要求の数
   - Device ― デバイス名
   - Load ― CPU の負荷 (%)
   - Peak ― 直前の 10 分間の 1 秒あたりの最大使用率
   - Client ― ユーザーの名前またはアドレス
   - Reqs ― 直前の 10 秒間にボリュームに対して処理された要求の数

2. Esc キーを押して、メインメニューに戻ります。

▼ システムログを表示する

- 「Operations」メニューから「Show Log」を選択します。

  ログには、次の 2 種類のエントリが表示されます。
  - **システム起動時のログエントリ** ― デバイスの構成、ボリューム、およびその他の関連情報。
  - **通常動作時のログエントリ** ― デバイスのエラー、セキュリティーの違反、およびルーティングの状態に関するその他の情報。リリース番号とソフトウェアのシリアル番号が最後に表示されます。

▼ ポート結合を表示する

1. 「Configuration」メニューから「Host Name & Network」を選択します。
2. 次のページにスクロールするには、スペースキーを押します。

   「bond1」列には、最初のポート結合が表示されます。この列に表示されている入出力情報は、結合した 2 つのポートの入出力情報の合計を示します。

▼ チェックポイント分析を表示する

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 構成するドライブに対応する文字を入力します。
3. 「Change/Delete ボリューム名」を選択します。
4. 「6. Checkpoints」を選択します。
5. 「3. Analysis」を選択します。分析をスクロールして表示するには、スペースキーを使用します。
6. 「0. End Analysis」を選択して、この画面を終了します。

▼ ミラー化されたファイルボリュームの状態を表示する

1. アクティブシステム上で、「Extensions」メニューから「Mirrors」を選択します。
2. ミラー化されたファイルボリュームを選択します。

   状態画面は、次の 3 つのセクションに分かれています。

   - 最初の行には、ファイルボリューム名、ミラーの状態、進捗インジケータ、状態メッセージなどのミラー状態に関連する情報が表示されます。ミラーの状態には、次の 10 種類があります。
     - ERR − エラーが発生しました。
     - NEW − 新しいミラーを作成しています。
     - INIT − ミラーバッファーを初期化しています。
     - MKPT − ミラーシステムでディスクパーティションを作成しています。
     - RDY − システムの準備が完了して、ほかのシステムの準備完了を待機しています。
     - DOWN − ネットワークリンクは使用できません。
     - CRK − ミラーが破損しています。
     - RPL − 複製段階が実行されています。
     - OOS – ミラーは同期がとれていません。
     - SYNC – ミラーは同期がとれています。

     進捗インジケータによって、各状態の動作の進捗率が示されます。また、状態メッセージにも、ミラーの状態を示す短いテキストメッセージが表示されます。

- 2 番めの行には、トランザクションバッファーの予約領域の状況が表示されます。ここに表示されるのは、バッファーが保持できるトランザクションの最大数、次のトランザクション ID、同期トランザクション ID、本体トランザクション ID、およびアクティブシステムとミラーシステム間の同期状態を示す In Sync 率のインジケータです。

  アクティブシステムでは、次の情報が表示されます。

  - next xid (次のトランザクション ID) は、ファイルシステムの次のトランザクションを示します。
  - sync xid (同期トランザクション ID) は、ミラーシステムに最後に転送されたトランザクションを示します。
  - head xid (本体トランザクション ID) は、ミラーシステムで最後に確認されたトランザクションを示します。
  - In Sync 率のインジケータが 100% になると、ミラーシステムはアクティブシステムを完全にコピーしたことになります。In Sync 率のインジケータが 0% を示す場合は、ミラーが破損しており、アクティブサーバーは自動的にブロック単位の再同期処理を実行します。ミラーの状態が「Out Of Sync」の間、ミラーボリュームは揮発性になります。

  ミラーシステムでは、次の情報が表示されます。

  - next xid (次のトランザクション ID) は、アクティブシステムから予想される次のトランザクションを示します。
  - sync xid (同期トランザクション ID) は、ディスクへの書き込みが予定されていた、最後のトランザクションを示します。
  - head xid (本体トランザクション ID) は、ディスクで最後に確認されたトランザクションを示します。
  - In Sync 率のインジケータが 100% になると、すべてのミラートランザクションがディスクに書き込まれたことになり、ミラーシステムのボリュームはアクティブシステムのボリュームの完全なコピーになります。

3. 代替 IP アドレスまたは管理者パスワードを編集するには、「1. Edit」を選択します。

4. フィールドを編集してから「7. Proceed」を選択し、変更を保存します。

5. ミラー化されたファイルボリュームのネットワーク統計情報を参照するには、「2. Statistics」を選択します。

   画面には、アクティブファイルボリュームに送信されるトランザクション数 (IN) や、アクティブシステムからミラー化されたファイルボリュームに送信されるトランザクション数 (OUT) などの、アクティブシステムの統計情報が表示されます。画面には、それぞれの 1 秒あたりトランザクション数 (t/s) の、平均値、最小値、および最大値が表示されます。

   システムは、流入速度とともに、トランザクションバッファーの予約領域 (Buffer) の残量を示します。流入速度が 0 より大きい場合は、すべてのネットワーク接続が正常に機能していることを確認する必要があります。この場合、アクティブシステムへの

トランザクションの送信速度がミラーシステムへの送信速度を上回っているため、バッファーがいっぱいになります。バッファーが制限を越えると、ミラーは「破損」します。

▼ ミラー化されたすべてのファイルボリュームのネットワーク統計情報を表示する

1. アクティブシステム上で、「Extensions」メニューから「Mirrors」を選択します。
2. 「2. Network Statistics」を選択します。

   画面には、送信された要求制御ブロック (RCB) の合計数、1 秒あたりの送信 RCB 数、および RCB の平均サイズと、平均応答時間および転送速度が表示されます。
3. 「1. Reset」を選択し、この画面を再起動します。

システムの保守

一部のシステム保守および設定機能は、コンソールからのみ実行できます。次の節では、このような機能について説明します。

- 235 ページの「FTP アクセスの構成」
- 236 ページの「RAID コントローラの管理」
- 238 ページの「ファイルシステムのマウント」

次の節では、コンソール管理機能と Web Adminstrator から実行できる、その他の作業について説明します。

- 238 ページの「システムの停止」
- 238 ページの「フェイルオーバーの管理」
- 240 ページの「LUN パスの構成」
- 243 ページの「ファイルのチェックポイントのスケジュール設定」
- 244 ページの「バックアップの構成」
- 244 ページの「Compliance Archiving Software の構成」
- 245 ページの「システム監査の構成」

FTP アクセスの構成

ファイル転送プロトコル (FTP) は、クライアントとサーバー間でファイルをコピーするために使用されるインターネットプロトコルです。FTP では、サーバーへのアクセスを要求する各クライアントを、ユーザー名およびパスワードで識別する必要があります。

次の 3 つのタイプのユーザーを設定できます。

- **管理者** − admin というユーザー名を持ち、GUI クライアントと同じパスワードを使用します。

  管理者は、システム上のすべてのボリューム、ディレクトリ、およびファイルにスーパーユーザーでアクセスできます。管理者のホームディレクトリは「/」と定義されます。

- **ユーザー** − ローカルのパスワードファイルか、遠隔の NIS または NIS+ ネームサーバーに指定されているユーザー名およびパスワードを持ちます。

  ユーザーは、自身のホームディレクトリに含まれるすべてのディレクトリおよびファイルへのアクセス権を持ちます。ホームディレクトリは、ユーザーのアカウント情報の一部として定義され、ネームサービスによって取得されます。

- **ゲスト** − ユーザー名 ftp またはそのエイリアス anonymous でログインします。パスワードが要求されますが、認証されません。すべてのゲストユーザーは、ftp ユーザーのホームディレクトリに含まれるすべてのディレクトリおよびファイルへのアクセス権を持ちます。

注 – ゲストユーザーは、ファイルの名前の変更、上書き、または削除を行うことができません。また、ディレクトリの作成または削除、および既存のファイルまたはディレクトリのアクセス権の変更を行うこともできません。

▼ FTP アクセスを設定する

1. 「Extensions」メニューから「FTP Configuration」を選択します。
2. 「1. Edit Fields」を選択します。
3. FTP を使用可能にするには「Y. Yes」、使用不可にするには「N. No」を選択します。

   FTP サービスを使用可能に設定すると、FTP サーバーは受信した接続要求を受け入れます。

4. 「Allow guest access」で、「Yes」を選択して匿名ユーザーによる FTP サーバーへのアクセスを許可するか、「No」を選択して禁止します。
5. 「Allow user access」で、「Yes」を選択してすべてのユーザーによる FTP サーバーへのアクセスを許可するか、「No」を選択して禁止します。

   これには、admin ユーザーまたはスーパーユーザーは含まれません。

注 – ローカルのパスワードファイルか、または遠隔 NIS/NIS+ ネームサーバーに、ユーザー名およびパスワードが指定されている必要があります。

6. 「Allow admin access」で、「Yes」を選択して Sun StorEdge 5310 NAS Appliance の管理パスワードでの、スーパーユーザーとしてのアクセスを許可するか、「No」を選択してアクセスを禁止します。管理パスワードの使用には注意が必要です。

注 – スーパーユーザーとは、ユーザー ID (UID) が 0 に設定されているユーザー、および Sun StorEdge 5310 NAS Appliance の特別なユーザーである `admin` を示します。

7. 「Enable logging」で、「Yes」を選択してログを使用可能にするか、「No」を選択して使用不可にします。
8. ログを使用可能にする場合は、「Log filename」にログファイル名を指定します。
9. 「7. Save changes」を選択します。

RAID コントローラの管理

`raidctl` コマンドを使用すると、CLI から RAID コントローラを管理できます。

いずれの `raidctl` コマンドを使用する場合でも、194 ページの「コマンド行インタフェースにアクセスする」の手順を実行してください。

注意 – 予期しない結果を回避するため、コマンドは注意して使用してください。

▼ サブコマンドでヘルプを表示する

1. コマンド行で **`raidctl help`** と入力します。

▼ LED を制御する

- トレーのすべての LED を点滅させるには、次のコマンドを入力します。
  `raidctl locate type=lsi target=tray ctlr=0..`*`n`* `tray=0..`*`n`*
- 指定したドライブの LED を点滅させるには、次のコマンドを入力します。
  `raidctl locate type=lsi target=drive ctlr=0..`*`n`* `tray=0..`*`n`* `slot=1..`*`n`*

- 指定したコントローラの LED の点滅を止めるには、次のコマンドを入力します。

  raidctl locate type=lsi action=stop ctlr=0..*n*

▼ イベントおよび構成情報を取得する

- 指定したコントローラのすべてのイベントを取得するには、次のコマンドを入力します。

  raidctl get type=lsi target=events ctlr=0..*n*

  すべてのイベントのログが /cvol/log/2882ae.log ファイルに書き込まれます。ファイルがすでに存在する場合は、そのファイルを上書きするか、新しいファイル名を指定するか、または操作をキャンセルするかを確認するプロンプトが表示されます。

- 指定したコントローラの重大イベントを取得するには、次のコマンドを入力します。

  raidctl get type=lsi target=events ctlr=0..*n* etype=critical

  重大イベントのログが /cvol/log/2882ce.log ファイルに書き込まれます。ファイルがすでに存在する場合は、そのファイルを上書きするか、新しいファイル名を指定するか、または操作をキャンセルするかを確認するプロンプトが表示されます。

- 指定したコントローラの構成情報を取得するには、次のコマンドを入力します。

  raidctl get type=lsi target=profile ctlr=0..*n*

▼ コントローラの時刻とバッテリの有効期限を設定する

- 指定したコントローラのバッテリの有効期限をリセットするには、次のコマンドを入力します。

  raidctl set type=lsi target=battery-age ctlr=0..*n*

- コントローラの時刻をサーバーの時刻と同期化するには、次のコマンドを使用します。

  raidctl set type=lsi target=ctlr_time-age ctlr=0..*n*

▼ ファームウェアをダウンロードする

raidctl download コマンドを使用して、ファームウェアをダウンロードします。

注 – ファームウェアのアップグレード手順の詳細は、第 11 章を参照してください。

ファイルシステムのマウント

再起動を連続して複数回行うと、1 つ以上のファイルシステムのマウントが解除されることがあります。ファイルシステムをマウントするには、次のコマンドを実行します。

```
mount -f volume_name
```

システムの停止

Sun StorEdge 5310 NAS Appliance システムは連続稼動できるように設計されていますが、システムを停止する必要がある場合は、必ず Web Administrator、コンソール、または LCD パネルで停止してください。

▼ システムを停止する

1. 「Operations」メニューから「Shutdown」を選択します。
2. 該当する文字を入力して、必要なオプションを選択します。
   - R. Reboot − システムを再起動するには「R」と入力します。
   - H. Halt − システムを停止するには「H」と入力します。
   - P. Boot Previous Version 4.x.xx.xxx − 使用可能な以前のバージョンの OS を使用してシステムを再起動するには「P」と入力します。このオプションは、複数のバージョンの OS がインストールされているシステム上で使用できます。
   - ESC − 操作を取り消してメインメニューに戻るには、Esc キーを押します。

再起動、停止、または以前のバージョンの OS を使用した起動を選択すると、ディスクへのすべての遅延書き込みが完了したあとで、サーバーが再起動または停止します。

フェイルオーバーの管理

2 つの RAID コントローラまたは本体のうちのいずれかの信頼性が低下し、その制御下にあるすべての LUN を安定しているコントローラまたは本体に移行する必要がある場合に、フェイルオーバーが発生します。フェイルオーバーメニューでは、回復可能な RAID エラーが発生したときのディスクリソースを管理します。

▼ フェイルオーバーを構成する

1. 「Extensions」メニューから「Failover/Move LUNs」を選択します。

   フェイルオーバーはデフォルトで構成されており、使用不可に切り替えることはできません。

2. 「3. Edit Failover」が使用可能な場合は、このオプションを選択します。

注 – Sun StorEdge 5310 NAS Appliance の本体 1 台構成のシステムでは、コントローラのフェイルオーバーを使用可能または使用不可に切り替えることはできません。

---

3. 「Y. Yes」を選択して、本体またはコントローラのフェイルオーバーを使用可能にします。

4. Sun StorEdge 5310 Cluster を使用している場合、または Sun StorEdge 5310 Gateway システムの 2 台のサーバーをクラスタ構成で使用している場合は、次の手順を実行します。

   a. 「Y. Yes」を選択して、リンクのフェイルオーバーを使用可能にします。

      リンクのフェイルオーバーでは、一次リンクに障害が発生すると、代替ネットワークリンクがアクティブになります。

   b. 1 つのネットワークリンクで信頼性が低下した場合に、リンクのフェイルオーバーが実行されるまでの時間を秒単位で入力します。

   c. 信頼性が低下したリンクが修復または再接続される場合に、リンクが復元されるまでの時間を秒単位で入力します。

5. Sun StorEdge 5310 Cluster および Sun StorEdge 5310 Gateway システムのクラスタ構成を使用している場合のみ、「2. Modify Lun Owner」を選択してアダプタごとの LUN 所有権を変更します。

   ここで指定する値によって、復元処理が実行される際に使用される構成が決まります。

   a. 各アダプタが所有する LUN を入力します。

   b. 空白文字を 1 つ入れて数字を区切ります (例: `0 2 8 10`)。

   c. Enter キーを押します。

6. 「Y. Yes」を選択して、変更内容を保存します。

▼ システムを復元して、フェイルバックを開始する

1. 障害の発生したコンポーネントを交換または修復して、オンラインになっていることを確認します。

2. 「Extensions」メニューから「Failover/Move LUNs」を選択します。
3. 「1. Restore」を選択します。
4. 「Y. Yes」を選択して、復元処理を続けます。

LUN パスの構成

論理ユニット番号 (LUN) パス、および LUN パスの設定で使用する GUI の詳細は、12 ページの「LUN パスの設定」を参照してください。

▼ LUN パスを設定または編集する

1. 「Extensions」メニューで、「LUN Ownership」オプションが表示されるまでスペースキーを押し、「LUN Ownership」オプションを選択します。

   「LUN Ownership」画面に、パスの変更が可能なすべての LUN が表示されます。LUN にファイルシステムが存在しない場合にのみ、LUN を割り当て直すことができます。Sun StorEdge 5310 Cluster または Sun StorEdge 5310 Gateway システムのクラスタ構成では、LUN を「所有する」本体のみが、その LUN をもう 1 台の本体に割り当て直すことができます。

注 – Sun StorEdge 5310 Cluster または Sun StorEdge 5310 Gateway システムのクラスタ構成では、システムをはじめて開始するときに、すべての LUN が 1 つの本体 (本体 1) に割り当てられます。LUN を均等に振り分けるために、本体 1 を使用して、一部の LUN を本体 2 に割り当て直す必要があります。

注 – 「LUN Ownership」画面には、最初に、LUN パスが割り当てられていない LUN が何度も表示されることがあります。これは、複数のパスを介した複数のコントローラがそれらの存在を通知するためです。いったん LUN パスが割り当てられると、現在のパスの LUN が一度だけ表示されます。

---

2. 選択するパスの左側に表示されている文字を入力して、LUN パスを選択します。
3. 「1. Edit」を選択して、LUN パスを編集します。

   「Configure LUN Path」画面では、LUN に使用できるすべてのパスが表示されます。現在アクティブな LUN パスには、「Active」と表示されます。LUN に一次パスが設定されている場合は、「PRIMARY」と表示されます。

4. 変更する LUN パスの番号を入力して Enter キーを押します。

   LUN の割り当てを、2 つの使用可能なパスに均等に振り分けます。たとえば、1 つめと 3 つめの LUN をパス 1 に、2 つめと 4 つめの LUN をパス 2 に振り分けます。

5. 「Y. Yes」を選択して、変更内容を保存します。

Gateway システムでの LUN のマッピング解除および再マッピング手順

Sun StorEdge 5310 NAS Gateway システムに割り当てられた LUN のマッピングを解除するには、次の手順を実行します。将来このデータにアクセスする必要が生じた場合は、LUN の再マッピングを実行することもできます。

マッピング解除および再マッピング手順の概要を次に示します。

1. LUN のマッピング解除
   a. マッピングを解除する LUN 上のボリュームのマウントを解除します。
   b. SAN 管理ホストソフトウェアを使用して、LUN のマッピングを解除します。
   c. Gateway システムの LUN を再走査します。
2. LUN の再マッピング
   a. SAN 管理ホストソフトウェアを使用して、LUN の再マッピングを実行します。
   b. Gateway システムの LUN を再走査します。
   c. アクセスするボリュームをふたたびマウントします。

以降の手順では、例として Sun StorEdge 6130 アレイを使用します。

▼ LUN のマッピングを解除する

1. Gateway システムでボリュームのマウントを解除します。
   a. Telnet を使用して NAS Gateway システムに接続します。
   b. 最初のプロンプトで `admin` と入力し、CLI を開始します。
   c. `mount` と入力して、マッピングを解除する LUN 上にマウントされているボリュームを一覧表示します。「Origin」列には、それらのボリュームを含む raw デバイスの名前が表示されます。マウントを解除するボリュームの名前 (左端の列に表示) を書き留めます。
   d. `umount` コマンドを使用して、マッピングを解除する LUN 上のすべてのボリュームのマウントを解除します。`mount` と入力して、その LUN に属するボリュームがマウントされていないことを確認します。
2. Sun StorEdge 6130 管理ホストを使用して、バックエンドアレイから LUN のマッピングを解除します。

a. ブラウザを開いて `https://`*hostname*`:6789` にアクセスし、管理ソフトウェアにログインします。

b. 「Sun StorEdge 6130 Configuration Service」をクリックします。

c. マッピングを解除する LUN を含むアレイをクリックします。

d. マッピングを解除する LUN の名前をクリックします。

e. 「Unmap」ボタンをクリックします。

f. ポップアップウィンドウで「OK」をクリックし、LUN の削除を確定します。

3. Gateway システムを再走査します。

a. マッピングを解除する LUN を確認します。

b. Telnet を使用して NAS Gateway システムに接続します。

c. 最初のプロンプトで `menu` と入力し、キャラクタベースのメニューインタフェースを開始します。

d. 文字 `d` を入力して、「Disks and Volumes」メニューを表示します。

e. 「Disks and Volumes」メニューで `9` と入力して、新しいディスク (LUN) を走査します。「Scanning for new disks, please wait...」というメッセージの表示が消えるまで待機します。

▼ LUN を再マッピングする

1. Sun StorEdge 6130 管理ホストから、LUN の再マッピングをバックエンドアレイで実行します。

a. ブラウザを開いて `https://<hostname>:6789` にアクセスし、管理ソフトウェアにログインします。

b. 「Sun StorEdge 6130 Configuration Service」をクリックします。

c. 再マッピングを実行する LUN を含むアレイをクリックします。

d. 再マッピングを実行する LUN の名前の横にあるボックスを選択します。

e. 「Map」ボタンを押します。

「Map Volumes」ウィンドウが表示されます。

f. LUN を割り当てるホストを選択します。

2. Gateway システムで、LUN を再走査します。

a. Telnet を使用して Gateway システムに接続します。

b. 最初のプロンプトで `menu` と入力し、キャラクタベースのメニューインタフェースを開始します。

c. 文字 `d` を入力して、「Disks and Volumes」メニューを表示します。

d. 「Disks and Volumes」メニューで `9` を入力して、新しいディスク (LUN) を走査します。「Scanning for new disks, please wait...」というメッセージの表示が消えるまで待機します。

3. Gateway システムで、ボリュームをふたたびマウントします。

a. Telnet を使用して Gateway システムに接続します。

b. 最初のプロンプトで `admin` と入力し、CLI を開始します。

c. 再マッピングした LUN 上にあるすべてのボリュームをマウントします。

d. `mount` と入力して、すべてのボリュームが再マッピングされたことを確認します。

ファイルのチェックポイントのスケジュール設定

チェックポイントは、一次ファイルボリュームの読み取り専用の仮想コピーです。チェックポイントの詳細は、163 ページの「ファイルのチェックポイント」を参照してください。

▼ チェックポイントのスケジュールを設定する

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. チェックポイントをスケジュール設定するドライブを選択します。

注 – ドライブ (ディスクボリューム) の数が 26 個を超える場合は、スペースキーを押して探します。

---

3. 「1. Edit」を選択します。
4. 「6. Checkpoints」を選択します。
5. Enter キーを押してフィールド間を移動し、画面の下部に表示されるプロンプトに従います。
6. すべてのチェックポイント情報を入力したら、「7. Save changes」を選択します。

バックアップの構成

システムボリュームをバックアップするには、まずバックアップジョブを追加し、次にそれをスケジュール設定するか、実行する必要があります。手順を開始する前に、バックアップデバイスがオンラインになっていることを確認してください。

注 – NDMP (Network Data Management Protocol) によってバックアップされるボリュームでは、チェックポイントが使用可能になっている必要があります。詳細は、163 ページの「ファイルのチェックポイントの作成」を参照してください。

▼ NDMP を設定する

1. 「Extensions」メニューから「NDMP Setup」を選択します。
2. **バックアップテープドライブへのデータ転送に使用するネットワークインタフェースカード (NIC) のポートを選択して、Enter キーを押します。**

   このフィールドの下に、使用可能なすべてのポートが表示されます。
3. **NDMP ログおよびデータファイルの保存に使用する 2G バイト以上のスペアボリュームのパス (`/vol_ndmp` など) を選択します。**

   バックアップがスケジュール設定されているボリュームではなく、別のファイルボリュームを使用することをお勧めします。
4. **変更を保存します。**

Compliance Archiving Software の構成

Compliance Archiving Software オプションを購入し、起動して使用可能にした場合 (119 ページの「オプションを起動する」を参照)、CLI を使用して追加設定を構築できます。

注 – Sun StorEdge 5310 Gateway システムの構成では、推奨実施はサポートされていますが、必須実施はサポートされていません。

注意 – 予期しない結果を回避するため、コマンドは注意して使用してください。

▼ デフォルトの保持期間を変更する

1. **194 ページの「コマンド行インタフェースにアクセスする」の手順を実行します。**

2. コマンド行で **fsctl compliance** *volume* **drt** *time* と入力します。

   volume にはデフォルトの保持時間を設定するボリューム名を指定し、*time* にはデフォルトの保持期間を秒単位で指定します。

   デフォルトの保持期間を「永続的」に設定するには、最大許容値である 2147483647 を使用します。

CIFS 規制適合の使用可能への切り替え

Compliance Archiving Software の初期構成では、NFS クライアントからのデータ保持要求のみがサポートされます。この機能への CIFS からのアクセスは、コマンド行インタフェースを使用して使用可能にすることができます。

注意 – 予期しない結果を回避するため、コマンドは注意して使用してください。

▼ Windows クライアントが規制適合アーカイブ機能を使用する

1. 194 ページの「コマンド行インタフェースにアクセスする」の手順を実行します。
2. コマンド行で、次のように入力します。

   fsctl compliance wte on

システム監査の構成

システム監査は、特定のシステムイベントの監査のために、システムイベントのレコードをログファイルに保存するサービスです。システム監査の詳細は、143 ページの「システム監査」を参照してください。

▼ システム監査を構成する

1. 「Extensions」メニューから「System Audit Configuration」を選択します。
2. 「1. Edit fields」を選択します。
3. 監査を使用可能にして、監査ログのパスとログファイルの最大サイズを指定します。
4. 「7. Save changes」を選択します。

付録B

Sun StorEdge 5310 NAS Appliance エラーメッセージ

この付録では、システムエラー発生時に電子メール、SNMP 通知、LCD パネル、およびシステムログによって管理者に通知されるエラーメッセージについて説明します。Sun StorEdge 5310 NAS Appliance の監視スレッド SysMon で、RAID デバイス、UPS、ファイルシステム、本体装置、格納装置のサブシステム、および環境変数の状態が監視されます。監視およびエラーメッセージは、モデルおよび構成によって異なります。

この付録の表では、エントリのない列は削除されています。

SysMon エラー通知の概要

Sun StorEdge 5310 NAS Appliance の監視スレッド `SysMon` では、サブシステムのエラーによって生成されたイベントが取得されます。次に、電子メールの送信、SNMP サーバーへの通知、LCD パネルでのエラーの表示、またはシステムログへのエラーメッセージの書き込みが適切に実行されます。これらの処理のいくつかが同時に実行される場合もあります。電子メール通知およびシステムログには、イベントの発生時刻も示されます。

Sun StorEdge 5310 NAS Appliance エラーメッセージ

この節では、Sun StorEdge 5310 NAS Appliance の UPS、RAID デバイス、ファイルシステム使用量、および IPMI に関するエラーメッセージを示します。

UPS サブシステムエラー

表 B-1 に、UPS のエラー状態を示します。

表 B-1　UPS エラーメッセージ

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
電源障害	**AC Power Failure:** AC power failure.System is running on UPS battery. Action: Restore system power. Severity = Error	EnvUpsOn Battery	U20 on battery	UPS: AC power failure.System is running on UPS battery.
電源の復旧	**AC power restored:** AC power restored.System is running on AC power. Severity = Notice	EnvUpsOff Battery	U21 power restored	UPS: AC power restored.
バッテリ低下	**UPS battery low:** UPS battery is low.The system will shut down if AC power is not restored soon. Action: Restore AC power as soon as possible. Severity = Critical	EnvUpsLow Battery	U22 low battery	UPS: Low battery condition.
バッテリ充電完了	**UPS battery recharged:** The UPS battery has been recharged. Severity = Notice	EnvUps Normal Battery	U22 battery normal	UPS: Battery recharged to normal condition.
バッテリ交換	**Replace UPS Battery:** The UPS battery is faulty. Action: Replace the battery. Severity = Notice	EnvUps Replace Battery	U23 battery fault	UPS: Battery requires replacement.
UPS アラーム (周辺温度または湿度が正常なしきい値の範囲外)	**UPS abnormal temperature/humidity:** Abnormal temperature/humidity detected in the system. Action: 1. Check UPS unit installation, OR 2. Contact technical support. Severity = Error	EnvUps Abnormal	U24 abnormal ambient	UPS: Abnormal temperature and/or humidity detected.

表 B-1　UPS エラーメッセージ (続き)

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
ライトバックキャッシュが使用不可	**Controller Cache Disabled:** Either AC power or UPS is not charged completely. Action: 1 - If AC power has failed, restore system power.2 - If after a long time UPS is not charged completely, check UPS. Severity = Warning		Cache Disabled	write-back cache for ctrl *x* disabled
ライトバックキャッシュが使用可能	**Controller Cache Enabled:** System AC power and UPS are reliable again.Write-back cache is enabled. Severity = Notice		Cache Enabled	write-back cache for ctrl *n* enabled
UPS の停止	**UPS shutdown:** The system is being shut down because there is no AC power and the UPS battery is depleted. Severity = Critical			!UPS: Shutting down
UPS 障害	**UPS failure:** Communication with the UPS unit has failed. Action: 1. Check the serial cable connecting the UPS unit to one of the CPU enclosures, OR 2. Check the UPS unit and replace if necessary. Severity = Critical	EnvUpsFail	U25 UPS failure	UPS: Communication failure.

ファイルシステムエラー

ファイルシステムのエラーメッセージは、ファイルシステム使用量が定義されたしきい値を超えた場合に生成されます。使用量のデフォルトのしきい値は 95% です。

表 B-2 ファイルシステムエラー

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
ファイルシステムの空き領域不足	File system full: File system <name> is *xx*% full. Action: 1. Delete any unused or temporary files, OR 2. Extend the partition by using an unused partition, OR 3. Add additional disk drives and extend the partition after creating a new partition. (Severity=Error)	PartitionFull	F40 FileSystemName full	File system <name> usage capacity is *xx*%.

RAID サブシステムエラー

表 B-3 に、Sun StorEdge 5310 NAS Appliance のイベントおよびエラーメッセージを示します。

表 B-3 RAID エラーメッセージ

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
LUN 障害	RAID LUN failure: RAID LUN *N* failed and was taken offline.Slot *n* is offline. Action: Replace bad drives and restore data from backup. Severity = Error	RaidLunFail	R10 Lun failure	RAID LUN *N* failed and was taken offline. Slot *n* is offline. (Severity=Error)
ディスク障害	Disk drive failure: Disk drive failure.Failed drives are: Slot no., Vendor, Product ID, Size Severity = Error	RaidDiskFail	R11 Drive failure	Disk drive failure. Failed drives are: Slot#, Vendor, Product ID, Size (Severity=Error)

表 B-3　RAID エラーメッセージ (続き)

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
コントローラ障害	RAID controller failure: RAID controller *N* has failed. Action: Contact technical support. Severity = Error	RaidController Fail	R12 Ctlr failure	RAID controller *N* failed.

IPMI イベント

Sun StorEdge 5310 NAS Appliance は、環境システムの監視と、電源装置および温度の異常に関するメッセージの送信を実行する IPMI ボードを搭載しています。

注 – デバイスの場所については、付録 D を参照してください。

表 B-4 に、Sun StorEdge 5310 NAS Appliance の IPMI エラーメッセージを示します。

表 B-4　IPMI のエラーメッセージ

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
ファンエラー	Fan Failure: Blower fan *xx* has failed. Fan speed = xx RPM. Action: The fan must be replaced as soon as possible. If the temperature begins to rise, the situation could become critical. Severity = Error	envFanFail trap	P11 Fan *xx* failed	Blower fan *xx* has failed!
電源モジュールの障害	Power supply failure: The power supply unit xx has failed. Action: The power supply unit must be replaced as soon as possible. Severity = Error	envPowerFail trap	P12 Power *xx* failed	Power supply unit *xx* has failed.
電源モジュールの温度	Power supply temperature critical: The power supply unit *xx* is overheating. Action: Replace the power supply to avoid any permanent damage. Severity = Critical	envPowerTemp Critical trap	P22 Power *xx* overheated	Power supply unit *xx* is overheating.

表 B-4　IPMI のエラーメッセージ (続き)

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
温度エラー	Temperature critical: Temperature in the system is critical. It is xxx Degrees Celsius. Action: 1. Check for any fan failures, OR 2. Check for blockage of the ventilation, OR 3. Move the system to a cooler place. Severity = Error	envTemperatue Error trap	P51 Temp error	The temperature is critical.
主電源コードの障害	Power cord failure: The primary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error	envPrimary PowerFail trap	P31 Fail PWR cord 1	The primary power cord has failed.
副電源コードの障害	Power cord failure: The secondary power cord has failed or been disconnected. Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord. Severity = Error	envSecondary PowerFail trap	P32 Fail PWR cord 2	The secondary power cord has failed.

付録C

Compliance Archiving Software API

ライセンスキーを使用して「Compliance Archiving Software」と呼ばれるソフトウェア拡張機能を有効にすると、Sun StorEdge 5310 NAS Appliance 製品で規制適合対応のデータストレージがサポートされるようになります。

Compliance Archiving Software は、「必須実施」と呼ばれる厳しい形式、および「推奨実施」と呼ばれる「必須実施」よりは厳しくない形式で使用できます。Compliance Archiving Software の概要は、132 ページの「Compliance Archiving Software」を参照してください。

この付録では、必須実施の Compliance Archiving Software の機能およびプログラミングインタフェースの技術的な概要について説明します。

注 – Compliance Archiving Software を適切に動作させるには、Sun StorEdge 5310 NAS Appliance システムのハードウェアが物理的に正しく構成されている必要があります。つまり、Sun StorEdge 5300 RAID EU コントローラアレイはプライベートファイバチャネルを使用して NAS 本体およびすべての Sun StorEdge 5300 EU の拡張格納装置に接続し、その他のデバイスまたはネットワークには決して接続しないでください。

注 – できるかぎり強力なデータ保持方針を実現するには、使用している Sun StorEdge 5310 NAS Appliance システムに物理的なセキュリティーも追加することをお勧めします。ソフトウェア制御によるデータ保持よりも、物理的な保護手段を使用してシステムのハードウェアへのアクセスを制御する方が強力です。

規制適合機能

Compliance Archiving Software は、ファイルの精度、完全性、および保持をストレージレベルで保証します。この機能は、主に次の 3 つの機能で構成されます。

- WORM (Write-Once、Read-Many) ファイル
- ファイル別保持期間
- 管理ロックダウン

WORM ファイル

WORM ファイルは、NFS や CIFS プロトコルによって提供される従来のファイルアクセスの定義よりも強力なアクセス制御を実現します。アプリケーションによってファイルが WORM に指定されると、そのファイルは永続的に不変となります。操作を試みるクライアントまたはユーザーの識別情報または特権にかかわらず、WORM ファイルの変更、拡張、または名前の変更はできません。また、WORM ファイルは、次に説明するファイルの保持規則に準拠している場合にのみ削除できます。

注 – これらのファイルは、再書き込みおよび消去ができないストレージを指す業界用語に合わせて「WORM」と呼んでいますが、「常時読み取り専用」と呼ぶ方がより的確です。Sun StorEdge 5310 NAS Appliance では、ファイルが WORM ファイルに変換されるまでは、ファイルの書き込み方法または内容を変更できる回数に制限はありません。

ファイル別保持期間

Compliance Archiving Software では、WORM ファイルごとに保持期間が関連付けられます。WORM ファイルは保持期間が期限切れになるまで削除できません。保持期間は延長できますが、短縮することはできません。保持期間が期限切れになったファイルには、新しい保持期間を割り当てることができます。

管理ロックダウン

WORM ファイルおよび保持期間の保持および保護を確実に保証するため、規制適合対応のファイルシステムボリュームでは、ファイルボリュームの削除、編集などの特定のシステム管理機能が使用不可になるか、または制限されます。これらの制限は、ファイルの保持を避けるために使用されるシステムの管理機能 (ファイルボリュームの削除など) に影響します。

規制適合機能の使用

Compliance Archiving Software の機能は、既存のクライアントのオペレーティングシステムおよびアプリケーションとの互換性を維持するため、Sun StorEdge 5310 NAS Appliance がサポートする既存のファイルアクセスプロトコル (NFS および CIFS) の拡張機能として実装されています。つまり、Sun StorEdge 5310 NAS Appliance は、既存のファイル属性を多重定義して、ファイルの WORM 状態および保持期間の終了を示します。これにより、標準のクライアント API およびユーティリティーを使用してメタデータフィールドを設定および参照できるため、既存の文書およびレコード管理アプリケーションの移植が容易になります。

規制適合対応のボリューム

ボリュームは、作成時に規制適合対応に指定する必要があります。既存のボリュームを規制適合対応のボリュームに変換することはできません。1 台の Sun StorEdge 5310 NAS Appliance には複数のボリュームを構成できますが、一部のボリュームのみが規制適合対応になります。

Compliance Archiving Software によって実施される、さまざまなデータ保持の定義を認識しないアプリケーションおよびユーザーが使用するボリュームでは、規制適合アーカイブ機能を使用可能にしないでください。

WORM ファイル

WORM ファイルは、変更または更新できません。いったん WORM ファイルになると、削除されるまで読み取り専用となります。

WORM ファイルの作成

Compliance Archiving Software は、WORM トリガーを使用して通常のファイルを WORM ファイルに変換します。クライアントのアプリケーションまたはユーザーがファイル上でトリガー動作を実行すると、Compliance Archiving Software は、ターゲットファイルが WORM ファイルに変換される必要があると解釈します。

UNIX クライアントの WORM トリガーでは、ファイルのアクセスモードが 4000 に設定されます。クライアントアプリケーションまたはユーザーは、chmod コマンドまたはシステムコールを使用してこの WORM トリガーを起動できます。この要求を受信すると、Compliance Archiving Software は、次の処理を実行して、ターゲットファイルを WORM ファイルに変換します。

- setuid ビットの設定
- ファイルに設定されているすべての書き込みビットのクリア
- ファイル上のすべての読み取りアクセスビットの維持

注 – 実行可能ファイルは WORM ファイルに変換できません。Windows クライアントで作成されたファイルでは、これは、ファイルに実行権を付与するアクセス制御エントリ (ACE) がアクセス制御リスト (ACL) に存在する場合、そのファイルを WORM ファイルに変換できないことを意味します。

次の例では、アクセスモードが 640 のファイルを WORM ファイルに変換します。WORM トリガーが実行されると、ファイルのアクセスモードは 4440 になります。

```
$ ls -l testfile
-rw-r-----   1 smith    staff      12139 Dec  2 13:18 testfile
$ chmod 4000 testfile
$ ls -l testfile
-r-Sr-----   1 smith    staff      12139 Dec  2 13:18 testfile
```

この WORM トリガーは既存のアプリケーションによって使用される可能性が低い操作であるため、Compliance Archiving Software によって使用されます。

Windows クライアントの WORM トリガーでは、読み取り専用ビットおよびシステムビットの両方がファイルに設定されます。WORM トリガーによってファイルの読み取り専用ビットは設定されますが、システムビットは変更されません。

WORM ファイルに変換されたファイルは、元に戻すことはできません。Windows クライアントからは、読み取り専用ビットのクリア、およびシステムビットの変更ができません。UNIX クライアントからは、setuid ビットのクリア、およびファイルのアクセスモードへの実行権または書き込み権の追加ができません。

これらの WORM 設定は、規制適合対応のボリュームによって CIFS と NFS 間で変換されます。たとえば、Windows クライアントで作成された WORM ファイルを UNIX クライアントが参照すると、WORM のアクセスモードは前述のようになります。

WORM ファイルの動作

WORM ファイルは変更、上書き、または拡張できません。クライアントユーザーの識別情報およびアクセス権にかかわらず、WORM ファイルへの書き込みはすべて失敗してエラーが返されます。

WORM ファイルの所有者や管理権限を持つユーザー、およびスーパーユーザー権限を持つユーザーでさえ、WORM ファイルを変更できません。WORM ファイルの名前を変更したり、WORM ファイルを WORM ではない通常のファイルに戻したりすることはできません。

WORM ファイルのメタデータ

Compliance Archiving Software では、クライアントデータの保有、保護、記述、または名前付けを行うメタデータを変更できません。表 C-1 に示すように、オペレーティングシステムに応じて、一部の限られたメタデータフィールドのみを変更できます。

表 C-1　変更可能または変更不可能な WORM ファイルのメタデータ

オペレーティングシステム	変更可	変更不可
UNIX	• 読み取りアクセス権ビットの設定またはクリア • ファイルおよびグループの所有者の変更	• 書き込みビットおよび実行ビットの使用可能への切り替え • setuid ビットのクリア • サイズまたは変更時刻 (mtime) の変更
Windows	• 読み取りアクセス権ビットの設定またはクリア • アーカイブビットの変更 • アクセス制御リストの作成および変更 (ただし、ACL の設定にかかわらず、WORM ファイルは変更できない)	• 読み取り専用ビット、システムビット、および隠しビットの変更 • サイズまたは変更時刻 (mtime) の変更

ネームスペースの制限

Compliance Archiving Software では、WORM ファイルの名前を変更できません。ディレクトリが空でない場合は、ディレクトリの名前も変更できません。この規則によって、WORM ファイルが存続するかぎり、ファイルのフルパス名が変更されないことが保証されます。

警告

UNIX クライアントがファイルモードを 4000 (WORM トリガーの呼び出し) に設定すると、ファイルのアクセスモードは通常 4000 にはなりません。これは、chmod コマンドおよびシステムコールの標準の定義に違反します。その結果、多くの Linux ディストリビューションで使用される GNU バージョンの chmod(1) コマンドを使用して WORM トリガーを発行すると、警告メッセージが生成されます。このメッセージは無視できます。

ファイル保持期間

WORM ファイルにはそれぞれ保持期間が設定されており、保持期間中はファイルを削除できません。保持期間は、保持期間の終了時点を表すタイムスタンプを使用して指定されます。この保持期間は、クライアントのアプリケーションまたはユーザーが明示的に設定できます。保持期間がクライアントによって指定されていない場合、Compliance Archiving Software は、ボリュームの作成時に指定されたデフォルトの保持期間を使用します。保持期間が終了する前に WORM ファイルを削除しようとしても失敗します。ただし、保持期間が期限切れになると、いつでもファイルを削除できます。

注 – 保持期間は、ファイルを削除する機能にのみ適用されます。保持期間が期限切れになっているかどうかにかかわらず、WORM ファイルは変更できません。

保持タイムスタンプの設定

Compliance Archiving System の保持タイムスタンプは、WORM ファイルのアクセス時刻 (atime) 属性に格納されます。クライアントは、通常、ファイルを読み取り専用に変更する前に atime 属性を設定します。ファイルが WORM ファイルになると、そのファイルの atime の値が秒単位で切り捨てられ、保持タイムスタンプが決まります。

atime 属性が過去の時刻を表す場合は、ファイルシステムのデフォルト保持期間が現在の時刻に追加されて保持タイムスタンプが計算されます。

永続保持

クライアントのアプリケーションまたはユーザーは、ファイルを永続的に保持するように指定できます。永続保持を指定するには、32 ビットの符号付き整数で設定可能な最大値をファイルの atime に設定します。この値 (0x7fffffff) は、2,147,483,647 に相当します。UNIX システムでは、この値は、limits.h ヘッダーファイルで INT_MAX として定義され、タイムスタンプ 03:14:07 GMT, Jan 19, 2038 に変換されます。

保持期間の変更

保持期間は、延長できます。また、保持期間が期限切れになったファイルに新しい保持期間を設定することもできます。保持期間を変更するには、WORM ファイルの atime 属性を再設定します。新しい値が古い保持タイムスタンプよりも新しい場合、変更は許可されます。

アクセス時刻の無視

Compliance Archiving Software では、アクセス時刻 (atime) 属性を使用して保持タイムスタンプを格納します。そのため、ファイルが WORM ファイルであるかどうかに関係なく、標準的なファイルシステム操作の影響によってこの属性が更新されることはありません。

ファイル状態の確認

クライアントのアプリケーションおよびユーザーは、標準ツールおよび API を使用してファイルのメタデータを読み取り、ファイルの保持状態を確認できます。たとえば UNIX クライアントの場合、ファイル属性は `stat(2)` システムコールを介して読み取ったり、`ls` コマンドで表示したりできます。(`ls -lu` コマンドを実行すると、ファイルの一覧がアクセス権および atime のタイムスタンプと一緒に表示されます。

UNIX システムコールの動作

UNIX クライアントのアプリケーションは、ローカルのシステムコールインタフェースを介して Compliance Archiving Software にアクセスします。これらのコールで呼び出されたクライアント NFS 実装によって、システムコールは標準の NFS プロトコル要求に変換されます。規制適合対応のファイルシステムの動作は標準の NAS ファイルシステムの動作と異なるため、クライアントシステムコールの動作もそれに応じて異なります。

この節では、標準 UNIX システムコールのなかで、規制適合対応の Sun StorEdge 5310 NAS Appliance 共有に対してクライアントが実行すると動作が異なるものについて説明します。この節に記載されていないシステムコールは通常どおり動作します。

Sun StorEdge 5310 NAS Appliance のインタフェースは、NFS および CIFS ファイルアクセスプロトコルです。したがって、この節では、標準のプロトコル要求に対応する Sun StorEdge 5310 NAS Appliance の規制適合に関する動作、およびシステム

コールから NFS 要求へのマッピングの両方について説明します。これらのコールの動作は Solaris オペレーティングシステムクライアントで確認済みです。また、ほかの UNIX クライアントでも同じように動作します。

access(2)

amode 引数に W_OK ビットを指定した access(2) のコールなど、WORM ファイルの書き込み権を確認しようとすると、失敗してエラー (EPERM) が返されます。

chmod(2)、fchmod(2)

ターゲットファイルが WORM ファイルではなく通常のファイルで、実行権ビットが設定されていない場合、新しいアクセス権が 4000 (S_ISUID) に設定されると、そのターゲットファイルは WORM ファイルになります。この場合、ターゲットファイルは、ファイルのアクセスモードの既存の読み取りビットに setuid ビットを追加して計算された新しいアクセスモードを受け取ります。具体的に説明すると、古いアクセスモードが oldmode の場合、WORM トリガーを受け取ったあとのファイルの新しいアクセスモードは次のように計算されます。

```
newmode = S_ISUID | (oldmode & 0444)
```

実行可能ファイルは WORM ファイルに変換できません。WORM トリガー (モード 4000) を 1 つ以上の実行権ビットが指定されたファイルに適用すると、失敗してエラー (EACCES) が返されます。

WORM ファイルの読み取りアクセスビットは、設定またはクリアできます。WORM ファイルの書き込み権または実行権の追加、setgid ビット (S_ISGID) または sticky ビット (S_ISVTX) の設定、あるいは WORM ファイルの setuid ビットのクリアを試みると、失敗してエラー (EPERM) が返されます。

chown(2)、fchown(2)

これらのコールは、WORM ファイルでも WORM ではないファイルでも同じように動作します。

link(2)

クライアントは、WORM ファイルへの新しいハードリンクを作成できます。WORM ファイルへのハードリンクは、ファイルの保持期間が期限切れになるまで削除できません。詳細は、261 ページの unlink(2) を参照してください。

read(2)、readv(2)

クライアントは、WORM ファイルを読み取ることができます。保持タイムスタンプは atime 属性に格納されているため、WORM ファイルへの読み取りアクセスを反映してこの値が更新されることはありません。

rename(2)

WORM ファイル、または規制適合対応のファイルシステム上の空ではないディレクトリの名前を変更しようとすると、失敗してエラー (EPERM) が返されます。

stat(2)、fstat(2)

これらのコールを使用して通常のファイルに関する情報を取得すると、返される stat 構造体には規制適合に関する値が含まれます。st_mode フィールドには、通常どおり、ファイルのモードとアクセス権が含まれます。WORM ファイルには setuid ビットが設定されていますが、書き込みビットまたは実行ビットは設定されていません。st_atime フィールドには、ファイルの保持期間の終了を示すタイムスタンプが含まれます。この値が limits.h で定義される INT_MAX と同じ場合、ファイルは永続的に保持されます。

unlink(2)

Sun StorEdge 5310 NAS Appliance の固定クロックが示す現在の時間がファイルの atime 属性に格納されている日付 (保持タイムスタンプ) を過ぎている場合にのみ、WORM ファイルのリンクを解除できます。この条件が満たされない場合、unlink(2) は失敗してエラー (EPERM) が返されます。

utime(2)、utimes(2)

これらのコールは、ファイルのアクセス時刻 (atime) 属性および変更時刻 (mtime) 属性を設定するために使用します。WORM 以外のファイルに対して使用すると通常どおり動作し、ファイルが WORM に変換される前に保持タイムスタンプを指定するための手段を提供します。

これらのコールを WORM ファイルに対して呼び出すと、ファイルの保持期間を延長したり、保持期限が切れたファイルに新しい保持期間を割り当てたりすることができます。新しい atime 値がファイルの既存の atime 値よりも大きい場合 (atime 値よりあとの時刻を示している場合) は、WORM ファイルに対するこれらのコールは成功

します。新しい atime 値が現在の atime 値と同じか小さい場合は、これらのコールは失敗してエラー (EPERM) が返されます。WORM ファイルに対して使用した場合、mtime 引数は無視されます。

write(2)、writev(2)

WORM ファイルへの書き込みは、すべて失敗してエラー (EPERM) が返されます。

Windows クライアントの動作

WORM ファイルの作成

Windows では、WORM ファイルでない通常のファイルから WORM ファイルへの変換は、ファイルに読み取り専用ビットとシステムビットの両方を設定することによってのみ可能です。この WORM トリガーによって、ファイルの読み取り専用ビットは設定されますが、ファイルのシステムビットの状態は変更されません。

WORM ファイルに変換されたファイルは、元に戻すことはできません。Windows クライアントからは、読み取り専用ビットのクリア、およびシステムビットの変更はできません。

WORM ファイルのメタデータの制限

Windows クライアントは、WORM ファイルのアーカイブビットを変更できますが、読み取り専用ビット、隠しビット、またはシステムビットは変更できません。Windows クライアントは WORM ファイルの ACL を変更できますが、WORM ファイルの ACL の書き込み権はすべて無視されます。ACL のアクセス権にかかわらず、WORM ファイルのデータを変更しようとすると失敗します。

保持期間の設定

UNIX クライアントと同様、Windows クライアントは、ファイルのアクセス時刻 (atime) 属性に保持タイムスタンプを格納して保持期間を設定します。

Windows クライアントに対する警告

読み取り専用ビットに関する注意事項

規制適合対応のボリュームは、WORM ファイルの特殊な動作を認識する Windows のアプリケーションおよびユーザーのみが使用する必要があります。ファイルのコピーを行う標準的な多くの Windows ユーティリティーでは、ファイルに対して読み取り専用ビットおよびシステムビットが指定されます。これらのツールを使用して規制適合対応ボリュームに WORM ファイルのコピーを作成すると、読み取り専用ビットおよびシステムビットが設定されるため、作成されたファイルが WORM ファイルになる可能性があります。

ウイルス対策ソフトウェア

多くのウイルスチェックプログラムは、検査するファイルのアクセス時刻を保持しようとします。通常、このようなプログラムは、ウイルスチェックの前にファイルの atime を読み取り、ウイルスチェックが終わると atime を走査前の値に再設定します。これによって、ほかのアプリケーションがファイルの保持期間を設定しているときに、同時にウイルスチェックプログラムがファイルを走査すると、競合状態が発生する可能性があります。その結果、ファイルに誤った保持期間が設定される場合があります。

この問題を回避する簡単な方法は、ウイルスチェックプログラムを規制適合対応のファイルシステム上で実行しないか、または WORM ファイルを作成するアプリケーションと同時に実行しないことです。

カスタムアプリケーションでは、短いデフォルト保持期間を使用し、WORM トリガーの適用後にファイルの実際の保持期間を設定することによって、この問題を回避することもできます。

その他の API

Compliance Archiving Software には、Java、Perl、C++ など、ほかにも多くの API を介してアクセスできます。これらのすべての言語は、NFS または CIFS を介してマウントされる共有にアクセスするために、基本となる同一のシステムコールに依存します。

付録 D

Sun StorEdge 5310 NAS Appliance コンポーネント

この付録では、Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster サーバー (本体) のハードウェア、Sun StorEdge 5300 RAID EU コントローラ格納装置、および Sun StorEdge 5300 EU 拡張格納装置のいくつかのコンポーネントについて説明します。

注意 – 認定された保守作業員のみが、装置のカバーを取り外し、内部コンポーネントを扱うことを承認されています。

この付録の内容は、次のとおりです。

サーバーの電源装置

システムの電源装置は、すべてのコンポーネントに電源を供給します。すべての装置に対応する電源装置システムは、電圧を 100 ～ 240 ボルト、50 ～ 60 Hz に自動的に適合させる自動検知デバイスです。

サーバーの電源装置システムは、1 + 1 構成の 2 つの冗長なホットスワップ対応モジュールで構成されています。各モジュールは、500 W の負荷を維持することができます。システムが適切に動作するには 1 台以上の電源装置が必要ですが、電源の冗長性を得るには 2 台の電源装置が必要です。

電源装置モジュールの背面にある赤い LED は、電源コードが外れていることを示します。

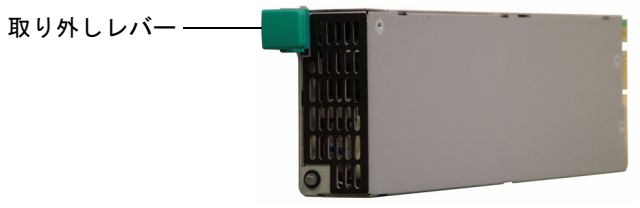


図 D-1　　電源装置

電源装置には、次の機能があります。

- 500 W の出力
- LED 状態インジケータ
- 複数の速度に対応できる内部冷却ファン
- 組み込み型負荷分散機能
- 組み込み型過負荷保護機能
- 差し込み/引き出し用の一体型のハンドル

サーバーのフロントパネルのボタン

電源ボタン – システムの電源のオンとオフを切り替えるモーメンタリスイッチ (APCI 準拠) です。

注意 – システムを停止する場合は、電源ボタンを使用しないでください。必ず、162 ページの「サーバーの停止」に示す適切な電源切断手順を実行してください。不適切な切断手順を実行すると、データが失われる可能性があります。

システム ID ボタン – このボタンを押すと、システムの正面および背面にある青色の LED が点灯し、ラック内での装置の位置確認が簡単になります。

リセットボタン – システムをリセットできるボタンです。

注意 – システムをリセットする場合は、リセットボタンを使用しないでください。必ず、適切な電源切断手順を実行してください。

状態 LED インジケータ

フロントパネルの状態 LED インジケータは、システムの現在の活動状態を示します。

表 D-1 LED 状態インジケータ

電源 LED	LED の緑色の連続点灯は、システムに電源が入っていることを示します。 オレンジ色の点灯は、いずれかの電源コードが外れていることを示します。 点灯していない場合は、システムの電源が入っていないことを示します。
組み込み型 NIC 1 LED	緑色の LED は、組み込み型の NIC ポート 1 を介してネットワーク活動が発生していることを示します。
組み込み型 NIC 2 LED	緑色の LED は、組み込み型の NIC ポート 2 を介してネットワーク活動が発生していることを示します。
ハードドライブ状態 LED	• 適用されません。
システム状態 LED	• LED の緑色の連続点灯は、システムが正常に動作していることを示します。 • LED の緑色の点滅は、システムが縮退モードで動作していることを示します。 • LED のオレンジ色の連続点灯は、システムが危険な状態か、回復不能な状態であることを示します。 • LED のオレンジ色の点滅は、システムが危険な状態でないことを示します。 • 赤色の点灯は、いずれかの電源コードが外れていることを示します。 • 電源 LED が緑色に点灯しており、この LED が点灯していない場合は、システムが停止していることを示します。
システム ID LED	• LED の青色の連続点灯は、ID ボタンが押されたことを示します。 • 点灯していない場合は、ID ボタンが押されていないことを示します。

サーバーの背面パネル

サーバーの背面パネルにある各種ポートおよびコネクタを次に示します。

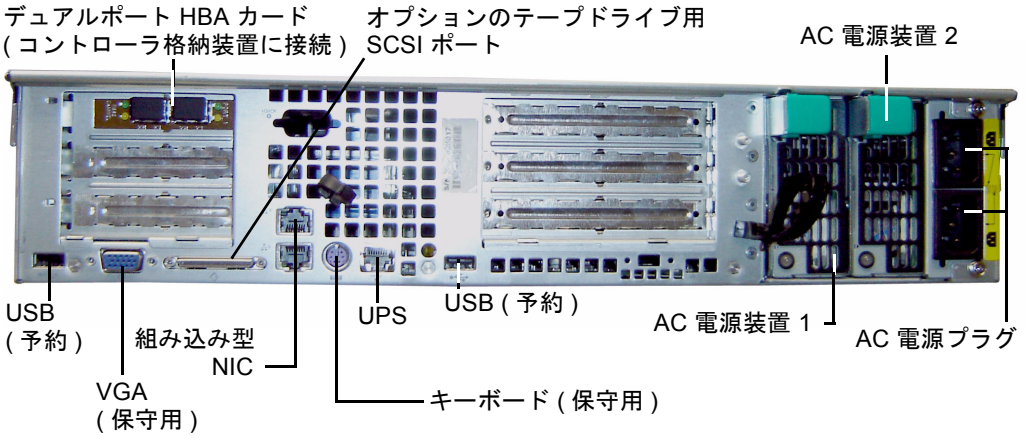


図 D-2　　1 枚の HBA カードを装備した背面パネル

注 – フロントパネルおよび背面パネルにある VGA ポートは使用しないでください。これらのコネクタは、Sun の技術サポート作業員が使用するために予約されています。

注 – 2 台のコントローラ格納装置に接続する Sun StorEdge 5310 NAS Appliance の背面パネルには、2 枚のデュアルポート HBA カードが装備されています。

直接接続のテープライブラリ

ローカルテープバックアップ用ドライブは、サーバーの背面パネルの左下にある SCSI ポートに接続できます。

注 – サポートされているテープデバイスのリストに、使用するテープドライブが含まれていることを確認してください。サポートされているテープデバイスの最新情報については、ご購入先にお問い合わせください。

テープライブラリの SCSI ID は、テープドライブより小さい値である必要があります。たとえば、ライブラリ ID を **0** に設定する場合は、ドライブ ID を **5** などの矛盾のない値に設定します。

使用するテープドライブシステムの詳細は、システムに付属するマニュアルを参照してください。

Sun StorEdge 5300 RAID EU コントローラ格納装置および Sun StorEdge 5300 EU 拡張格納装置のコンポーネント

コントローラ格納装置と拡張格納装置は、Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster システムにストレージを提供します。

Sun StorEdge 5300 RAID EU コントローラ格納装置は、ファイバチャネル拡張格納装置 (EU F) または SATA 拡張格納装置 (EU S) とともに使用できます。

注意 – 拡張格納装置を追加するか取り外すには、システムを停止する必要があります。

ファイバチャネルコントローラ格納装置のフロントパネル側には、14 台のホットスワップ対応のハードドライブが、6 台のドライブによる RAID 5 グループが 2 つと、グローバルホットスペアが 2 台という構成で取り付けられています。各ドライブの未フォーマット時の容量は 146G バイトで、使用可能な容量は 133G バイトです。格納装置で使用可能な容量は、合計で 1.3T バイトになります。

300G バイトの FC ドライブの RAID 構成には、6 台のドライブ (5+1) で構成される RAID 5 グループが 1 つと、7 台のドライブ (6+1) で構成される RAID 5 グループが 1 つ、およびグローバルホットスペアが 1 台含まれます。

SATA システムで使用するコントローラ格納装置は、ハードドライブがない状態で出荷されます。代わりに、SATA ドライブはすべて EU S 拡張格納装置に取り付けられています。

注意 – コントローラ格納装置内またはアレイ内で、ファイバチャネルディスクドライブと SATA ディスクドライブを混在させないでください。

注 – デュアルアレイ構成の場合、一方のアレイにファイバチャネルディスクドライブを取り付け (コントローラ格納装置および拡張格納装置内)、もう一方のアレイに SATA ディスクドライブを取り付ける (拡張格納装置内のみ) ことができます。

拡張格納装置を使用すると、システムのストレージ容量を拡張できます。各 EU F 拡張格納装置のフロントパネル側には、14 台のホットスワップ対応のファイバチャネルハードドライブが、7 台のドライブによる RAID 5 グループが 2 つという構成で取り付けられています。各ドライブの未フォーマット時の容量は 146G バイトで、使用可能な容量は 133G バイトです。1 台の EU F 拡張格納装置で使用可能な容量は、合計で 1.6T バイトになります。

1 台めの EU S 拡張格納装置のフロントパネル側には、14 台のホットスワップ対応の SATA ドライブが、6 台のドライブによる RAID 5 グループが 2 つと 2 台のグローバルホットスペアという構成で取り付けられています。各 SATA ドライブの未フォーマット時の容量は 400G バイトで、使用可能な容量は 360G バイトです。1 台めの EU S 拡張格納装置で使用可能な容量は、合計で 3.6T バイトになります。

2 台め以降の EU S 拡張格納装置には、14 台のホットスワップ対応の SATA ハードドライブが、7 台のドライブによる RAID 5 グループが 2 つという構成で取り付けられています。約 4.4T バイトの使用可能な容量が追加されます。

注意 – 拡張格納装置内で、ファイバチャネルディスクドライブと SATA ディスクドライブを混在させないでください。

FC 拡張ユニットと SATA 拡張ユニットの混在

シリアル ATA (Serial Advanced Technology Attachment、SATA) とファイバチャネルが混在する拡張ユニット (EU) 構成は、現在、次の条件でサポートされています。

- それぞれの EU は、ファイバチャネルドライブのみ、または SATA ドライブのみで構成される必要があります。1 つの EU 内で複数の種類のドライブを混在させることはできません。
- EU に SATA ドライブが含まれていても、RAID EU にはファイバチャネルドライブを含めることができます。RAID EU に SATA ドライブを含めることはできません。
- SATA およびファイバチャネルの両方に対して、アレイで使用しているものと同じ容量の固有のホットスペアが 1 台必要です。
- LUN に、SATA ドライブおよびファイバチャネルドライブの両方を含めることはできません。

ドライブシャトル

注意 – Sun StorEdge 5310 NAS Appliance および Sun StorEdge 5310 Cluster では、Sun が提供するファイバチャネルドライブのみが動作します。最新のサポート情報については、ご購入先にお問い合わせください。

ドライブは、それぞれのドライブシャトルに入っています。拡張格納装置、コントローラ格納装置、または Sun StorEdge 5310 NAS Appliance や Cluster を停止することなく、ドライブシャトルを個別に交換することができます。

注意 – 拡張格納装置内、コントローラ格納装置内、またはアレイ内で、ファイバチャネルディスクドライブと SATA ディスクドライブを混在させないでください。

注意 – ホットスワップできるのは、一度に 1 台のドライブシャトルのみです。RAID サブシステムで必要な再構築作業が完了していることを確認してから、次のドライブシャトルを取り外してください。

注意 – RAID サブシステムが危険な状態である場合や、新しい RAID セットを作成したり既存の RAID セットを再構築したりする場合には、システムソフトウェアまたは RAID ファームウェアを更新しないでください。

▼ ドライブまたは格納装置の位置を確認する

1. Web Administrator のナビゲーションパネルで、「RAID」>「Manage RAID」を選択します。
2. 「Locate Drive」または「Locate Drive Tray」ボタンをクリックします。この操作によって、ドライブまたは格納装置の LCD インジケータが点滅します。

図 D-3　　ファイバチャネルドライブシャトル

▼ 交換するドライブを確認する

ディスクドライブに障害が発生した場合、ディスクを特定するにはログエントリが役立ちます。システムログおよび診断レポートのどちらの場合も、同じ方法でディスクの場所を解釈できます。次にログエントリの例を示します。

```
Controller 0  enclosure 0  row 0  column 6
```

このようなログエントリを解釈するには、次の事項に注意してください。

- チャネルおよびターゲットの番号はすべて無視してください。
- コントローラ番号は、0 から始まります。たとえば、1 番めのアレイ (RAID EU) のコントローラは 0 (スロット A) および 1 (スロット B) で、2 番めのアレイのコントローラは 2 および 3 です。
- 格納装置の番号は 0 から始まり、属するアレイに対しての番号となります。たとえば、1 番めのアレイに 2 台の格納装置がある場合は、格納装置 0 および 1 として識別されます。
- Sun StorEdge 5310 Cluster の場合、行番号は常に 0 になります。
- 列番号は 0 から始まり、格納装置のスロット番号を示します。

したがって、この例は、1 番めのアレイにある 1 番めの格納装置のスロット 7 を示していると解釈できます。

注 – 1 番めのアレイと 2 番めのアレイを特定する標準的な方法はありません。通常、1 番めの HBA ポートは 1 番めのアレイ、2 番めの HBA ポートは 2 番めのアレイなどのように接続されます。

電源装置

コントローラ格納装置および拡張格納装置は、同じ電源装置モジュールを使用します。

電源装置モジュール

コントローラ格納装置

電源装置モジュール　　電源装置モジュール

拡張格納装置

電源装置モジュール　　電源装置モジュール

図 D-4　　電源装置モジュール

付録E

診断電子メールメッセージの送信

診断電子メール機能を使用して、Sun の技術サポートチームまたはその他の任意の受信者に電子メールメッセージを送信できます。診断電子メールメッセージには、Sun StorEdge 5310 NAS Appliance のシステム構成、ディスクサブシステム、ファイルシステム、ネットワーク構成、SMB 共有、バックアップや復元処理に関する情報、`/etc` ディレクトリ情報、システムログ、環境データ、および管理者情報が含まれます。

送信されるすべての診断電子メールメッセージには、発生した問題にかかわらず、これらのすべての情報が含まれます。

クラスタ構成では、クラスタ内の各サーバーに診断電子メールを設定する必要があります。

診断電子メールを設定するには、次の手順に従います。

1. **画面上部のツールバー上の  ボタンを選択します。**

   「Diagnostic Email」ウィンドウが表示されます。

2. **「Problem Description」フィールドに問題の詳細を入力します。**

   これは必須エントリで、256 文字まで入力できます。

3. **1 つ以上の電子メール受信者の「Diagnostics」チェックボックスが選択されていることを確認します。**

   受信者を追加または変更する必要がある場合は、31 ページの「電子メール通知の設定」の手順を参照してください。

4. **「Send」をクリックしてメッセージを送信します。**

索引

F

G

I

K

L

M

N

P

R

S

T

U

W

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

ね

は

ひ

ふ

へ

ほ

ま

み

ろ

わ