

**Hitachi NAS Platform, powered by
BlueArc®**

File Services Administration Guide

対象製品

Hitachi NAS Platform 10.2

輸出時の注意

本製品を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

なお、ご不明な場合は、弊社担当営業にお問い合わせください。

商標類

Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

発行

2013 年 8 月（第 1 版）K6603830

著作権

All Rights Reserved. Copyright (C) 2013, Hitachi, Ltd.

目次

はじめに.....	7
表記.....	8
関連資料.....	8
1. ファイルサービス.....	9
1.1 ファイルシステムの特徴.....	10
1.1.1 ファイルシステム形式.....	10
1.1.2 ファイルシステムの階層.....	11
(1) 階層ファイルシステムとスナップショット.....	12
1.1.3 ファイルシステムのブロックサイズ.....	12
1.1.4 リードキャッシュ.....	12
1.1.5 WORM ファイルシステム.....	13
(1) WORM の特性.....	13
1.2 ファイルシステム性能の管理.....	13
1.2.1 PFST 機能を使う.....	13
(1) PFST クラスを有効にする.....	14
(2) PFST クラスを無効にする.....	14
(3) PFST クラスを作成する.....	14
(4) PFST クラスを削除する.....	14
(5) PFST クラスを変更する.....	14
1.2.2 ファイルシステムを作成する.....	14
1.2.3 ファイルシステムを削除する.....	22
1.2.4 ファイルシステムをフォーマットする.....	23
1.2.5 ファイルシステムをマウントする.....	24
(1) ファイルシステムをアンマウントする.....	25
1.2.6 使用可能なファイルシステムを表示する.....	25
1.2.7 ファイルシステムの詳細設定を表示する.....	27
1.2.8 ファイルシステムのスペース使用を制御する.....	31
(1) ファイルシステムの負荷を監視する.....	32
(2) ファイルシステムのサイズを拡張する.....	32
(3) シンプロビジョニングファイルシステム.....	33
(4) ファイルシステムの拡張を管理する.....	34
(5) ファイルシステムの自動拡張を有効または無効にする.....	36
(6) ファイルシステムの自動拡張の制限を管理する.....	36
(7) ファイルシステムを手動で拡張する.....	38
1.2.9 仮想ボリューム.....	39
1.2.10 使用量 Quota を管理する.....	40
(1) ファイルシステムのユーザー Quota 及びグループ Quota のデフォルトを設定するには.....	41
(2) ファイルシステムの Quota を追加する.....	42
(3) ファイルシステムの Quota を変更する.....	44

(4) ファイルシステムの Quota を削除する.....	44
1.2.11 ファイルシステムを移動する.....	44
(1) ファイルシステムの再配置.....	45
1.2.12 ファイルシステムでシステムロックを使用する.....	46
(1) ファイルシステムのシステムロックを有効または無効にする.....	46
1.2.13 ファイルシステムをリカバリーする.....	47
(1) ファイルシステムをリカバリーする.....	49
1.3 WORM ファイルシステムを使用する.....	51
1.3.1 保持期限を指定する.....	51
1.3.2 ファイルに WORM のマークを付ける.....	51
1.4 仮想ボリュームを管理する.....	52
1.4.1 仮想ボリュームを追加する.....	53
1.4.2 仮想ボリュームを変更する.....	55
1.4.3 仮想ボリュームを削除する.....	55
1.4.4 仮想ボリュームの Quota を管理する.....	56
(1) 仮想ボリューム Quota を表示または変更する.....	56
(2) ユーザー／グループのデフォルトを設定する.....	58
(3) Quota を追加する.....	59
(4) Quota を削除する.....	61
(5) 全仮想ボリュームの Quota をエクスポートする.....	61
(6) 特定の仮想ボリュームの Quota をエクスポートする.....	62
2. ファイルシステムのセキュリティを管理する.....	63
2.1 セキュリティ設定を表示する.....	64
2.2 NFS セキュリティ及び Kerberos.....	65
2.2.1 セキュアな NFS を設定する.....	65
2.3 混合セキュリティモード.....	65
2.3.1 UNIX セキュリティモード.....	67
2.3.2 セキュリティモードを変更する.....	67
(1) ファイルシステムのセキュリティモードを変更する.....	67
(2) 仮想ボリュームのセキュリティモードを変更する.....	67
(3) 混合モード操作.....	68
(4) 混合モードでのファイルロック.....	71
(5) 便宜的ロック (Oplocks)	71
(6) 排他ロックとバッチロック.....	72
(7) レベル II ロック.....	73
(8) NFSv4 のユーザー名及びグループ名.....	73
(9) ユーザー及びグループのマッピングを構成する.....	73
(10) NFS ユーザー及び NFS グループのマッピングを管理する.....	74
(11) ユーザーマッピングまたはグループマッピングを、ファイルからインポートする.....	78
(12) NIS サーバまたは LDAP サーバから、ユーザーまたはグループをインポートする.....	81
3. ファイルのクローンを作成する.....	83
3.1 ファイルのクローンを作成する.....	84
3.1.1 ファイルのクローンを使用する.....	84
3.2 リードキャッシュ.....	85
3.2.1 ファイルシステムアクセスプロトコル.....	85
3.2.2 サポートされている CIFS のバージョン.....	85
3.2.3 CIFS Unicode サポート.....	86
3.2.4 サポートされる NFS バージョン.....	86
(1) NFSv2/3 及び NIS Unicode サポート.....	86
3.2.5 FTP プロトコルサポート.....	87
3.2.6 Unicode サポート.....	87
(1) FTP Unicode サポート.....	87

(2) ファイルサービスを有効または無効にする.....	87
4. リソースを NFS クライアントと共有する.....	89
4.1 リソースを NFS クライアントと共有する.....	90
4.1.1 NFS プロトコルサポートを有効にする.....	90
(1) 前提条件.....	90
(2) サポートされるクライアント及びプロトコル.....	90
(3) NFS 統計.....	90
4.2 NFS 共有を構成する.....	90
4.2.1 NFSv4 疑似ファイルシステム.....	91
4.2.2 Kerberos 設定.....	91
4.2.3 NFS 共有を追加する.....	92
(1) IP アドレスのエクスポート修飾子.....	95
(2) (IP アドレスの代わりに) 名前でクライアントを指定する.....	96
4.2.4 NFS 共有のプロパティを表示する.....	96
4.2.5 NFS 共有をバックアップ及び復元する.....	98
4.3 rquotad サービスについて.....	99
4.3.1 rquotad サービスの設定.....	100
4.3.2 制限モードでの運用.....	100
4.3.3 マッチングモードでの運用.....	100
5. Windows アクセスに CIFS を使用する.....	103
5.1 Windows アクセスに CIFS を使用する.....	104
5.1.1 CIFS プロトコルサポート.....	104
(1) 前提条件.....	104
(2) サポートされるクライアント.....	104
(3) ドメインコントローラーとの連携.....	104
(4) 動的 DNS.....	104
5.1.2 ファイルを以前のバージョンに復元する.....	105
5.1.3 CIFS セキュリティを構成する.....	105
(1) Active Directory (AD) に参加する.....	106
(2) CIFS サーバ名を削除する.....	109
(3) NetBIOS を使用する.....	109
5.1.4 ローカルグループを構成する.....	110
(1) ローカルグループまたはローカルグループメンバーを追加する.....	111
(2) ローカルグループまたはローカルグループメンバーを削除する.....	112
5.1.5 CIFS 共有を構成する.....	114
(1) CIFS 共有を追加する.....	114
(2) CIFS 共有のプロパティを表示及び変更する.....	119
(3) 修飾子を使用して、共有へのアクセスを制御する.....	120
(4) アクセス許可を使用して、共有へのアクセスを制御する.....	120
(5) CIFS 共有のアクセス許可を追加または変更する.....	121
(6) オフラインファイルアクセスモード.....	123
(7) CIFS 共有を変更または削除する.....	123
(8) CIFS 共有をバックアップ及び復元する.....	124
5.1.6 Windows サーバ管理を使用する.....	125
5.1.7 Computer Management ツールを使用する.....	125
6. FTP を使ってファイルを転送する.....	129
6.1 FTP を使ってファイルを転送する.....	130
6.1.1 FTP の優先順位を設定する.....	130
(1) FTP の優先順位を設定するには.....	130
6.1.2 FTP ユーザーを構成する.....	131
(1) FTP ユーザーをセットアップする.....	131

(2) FTP ユーザーをインポートする.....	132
(3) FTP ユーザーを表示及び変更する.....	133
6.1.3 セキュアプロキシ FTPS サービスを使う.....	134
(1) FTPS API コマンド.....	134
(2) FTPS サービスの構成.....	134
(3) コマンド形式.....	134
(4) 診断.....	135
6.1.4 FTP 統計.....	135
6.1.5 FTP 監査ロギングをセットアップする.....	135
(1) FTP 監査ロギングを構成する.....	136
7. iSCSI を介したブロックレベルアクセス.....	139
7.1 iSCSI を介したブロックレベルアクセス.....	140
7.1.1 iSCSI サポート.....	140
(1) iSCSI MPIO.....	141
(2) iSCSI アクセス統計.....	141
(3) 前提条件.....	141
(4) サポートされている iSCSI イニシエーター.....	141
(5) オフロードエンジン.....	142
7.1.2 iSCSI を構成する.....	142
(1) iSNS を構成する.....	142
(2) iSNS サーバを作成及び削除する.....	142
7.1.3 iSCSI 論理ユニットを構成する.....	143
(1) iSCSI 論理ユニットをセットアップする.....	143
(2) iSCSI 論理ユニットを管理する.....	145
7.1.4 iSCSI ターゲットを設定する.....	150
(1) iSCSI ターゲットのプロパティを表示する.....	150
(2) iSCSI ターゲットを追加する.....	151
(3) iSCSI ターゲットへの LU を追加する.....	153
(4) iSCSI ターゲットのプロパティを変更する.....	154
(5) iSCSI ターゲットを削除する.....	155
7.1.5 iSCSI のセキュリティを設定する (相互認証)	156
(1) HNAS に相互認証を設定する.....	156
(2) Microsoft iSCSI イニシエーターに相互認証を設定する.....	157
(3) HNAS の相互認証設定を変更する.....	159
7.1.6 iSCSI ストレージにアクセスする.....	160
(1) iSNS を使用して iSCSI ターゲットを検出する.....	160
(2) ターゲットポータルを使用して iSCSI ターゲットを検出する.....	161
(3) 使用可能な iSCSI ターゲットにアクセスする.....	163
(4) 実行中の接続を検証する.....	164
(5) 実行中の接続を終了する.....	165
(6) Computer Manager を使用して iSCSI ストレージを設定する.....	167



はじめに




- 表記
- 関連資料

表記

このマニュアルでは下記の表記を使用しています。

用語	意味
LITERAL	コマンド、ファイル、ルーチン、パス名、シグナル、メッセージ、及びプログラム言語構成などの文字情報を固定スペースフォントで表します。
<i>Replaceable</i>	変数や定義など可変値をイタリック文字で表します。またマニュアル名もイタリック文字で表します。
[と]	コマンドや指示文の任意入力値を括弧内に示します。
...	前述の要素が繰り返し可能なことを表します。
GUI 要素	ウィンドウ、スクリーン、ダイアログボックス、メニュー、ツールバー、アイコン、ボタン、ボックス、フィールド、及びリストなど GUI 要素名を示します。

このマニュアルでは下記の表記を使用しています。このマニュアルを読み進む前に、下記のアイコンとそれらの意味を確認してください。

アイコン	意味	説明
	参考(tip)	タスクを完了するのに役立つ補足情報を示します。
	重要(note)	システムのインストールや運用を効率よく行う上で有用な情報を示します。
	注意(Caution)	データや機器に破損の恐れがある場合に注意を促します。要求条件を理解するまで決して次のステップへ進まないでください。

関連資料

- *System Access Guide*
システム管理者が Web Manager (GUI) や Command Line Interface (CLI) でシステムにアクセスする手順と、システム管理者向けの参考資料などを提供します。(PDF)
- *G2 Hardware Reference*
Hitachi NAS PlatformTM, powered by BlueArc[®] ハードウェアの概要と、問題の解決方法、障害コンポーネントの交換方法について説明します。(PDF)
- *Command Line Reference*
コマンドをコマンドプロンプトで入力してシステムを管理する方法について説明します。(HTML)
- *Release Notes*
システムソフトウェアの最新情報と、製品添付情報への訂正及び追加情報を提供します。

ファイルサービス

- 1.1 ファイルシステムの特徴
- 1.2 ファイルシステム性能の管理
- 1.3 WORM ファイルシステムを使用する
- 1.4 仮想ボリュームを管理する

1.1 ファイルシステムの特徴

ファイルシステムは、Hitachi NAS Platform のメインのストレージコンポーネントです。HNAS の他の全ての機能は、直接または間接的に、ファイルシステムをサポートします。

ファイルシステムには次のような属性があります。

- **WFS-1 または WFS-2 のファイルシステム形式**
WFS-1 はオリジナルのファイルシステム形式です。WFS-2 は、Hitachi NAS Platform のデフォルトのファイルシステム形式です。詳細については、「1.1.1 ファイルシステム形式」を参照してください。
- **ファイルシステム階層**
ファイルシステムのデータは、性能特性の異なるストレージシステム上に格納できるので、ファイルシステムメタデータを一つの階層に格納し、実際のユーザーデータ（ファイルシステムの内容）を別の階層に格納できます。詳細については、「1.1.2 ファイルシステムの階層」を参照してください。
- **最大サイズ 256TB**
これは、ストレージの使用可能なチャンクの数とサイズのみに依存します。
- **容量、割り当て、性能を制御・監視する機能**
 - **Quota** は、クライアント別のストレージ割り当てを制御します。
 - **グラフ**は、トラフィック及び利用状況を表示します。
 - **仮想ボリューム**は、ファイルシステムを個別のストレージ領域に分割します。これは、クライアントからは独立したファイルシステムに見えます。
 - **ポリシーベースのデータ移動**。これは **Data Migrator** の機能で、ポリシーによってストレージの再割り当てルーチンを制御し、一部のデータは高性能なストレージデバイスに置いておき、他のデータは低性能で安価なストレージデバイスに移行します。ポリシーは、ユーザーが定義したさまざまな条件に基づいて、どのデータを移動するかを決定します。

1.1.1 ファイルシステム形式

WFS-2 ファイルシステム形式は、WFS-1 形式 (Hitachi High-performance NAS Platform によってサポートされるオリジナルファイルシステム) に代わるファイルシステム形式です。WFS-2 ファイルシステム形式は、Series 3000 の Hitachi High-performance NAS Platform 以降のハードウェアプラットフォーム (Hitachi NAS Platform を含む) でのみサポートされることに注意してください。

WFS-2 でフォーマットされたファイルシステムには、WFS-1 を使用してフォーマットされたファイルシステムに比べて、いくつかの改良点があります。次のような利点があります。

- 特定のチェックポイントまでのファイルシステムのロールバックが高速です。
- チャーンレート (churn rate) の高いファイルシステムで一定レベルの性能を達成するために必要なディスクが少なく済みます。チャーンレートが高いファイルシステムとは、ファイル/ディレクトリの新規作成、ファイル/ディレクトリの削除、ファイル内容の変更など、ファイルシステムオブジェクトの変更を頻繁に行うファイルシステムです。
- WFS-2 を使用してフォーマットされた階層ファイルシステムは、定義されたサイズ制限まで、または使用可能な容量がある限り、必要に応じてどちらの階層も拡張できます。
- **書き込み可能クローン機能**。ファイルを高速コピーするメカニズムを提供します。「クローン」とは、オリジナル (マスター) ファイルの書き込み可能なスナップショットであり、マスターファイルが変更されない限り、追加のストレージ空間を使用せず、変更された場合は、変更され

たデータブロックのみが複製されます。「3.1 ファイルのクローンを作成する」を参照してください。



重要 デフォルトでは、WFS-2 がハードウェアプラットフォームによってサポートされる場合、新しいファイルシステムは WFS-2 形式を使用してフォーマットされます（詳細については、「1.2.2 ファイルシステムを作成する」と「1.2.4 ファイルシステムをフォーマットする」を参照してください）。

1.1.2 ファイルシステムの階層

ファイルシステムは、一般にファイルとディレクトリで構成されます。ファイルとディレクトリに関するデータ（と、その他多くの属性）が保持されます。この情報がメタデータです。ファイルシステム内のデータ（ユーザーデータとメタデータ）は、ストレージシステムのストレージメディアに格納されます。

ストレージシステムによって、性能の点でも価格の点でも特性が異なります。ストレージシステムは、性能によって「階層」に分類され、管理者が組織内のストレージリソースを管理するために使用されます。ストレージ階層と各階層を形成する技術の詳細については、『*Storage Subsystem Administration Guide*』を参照してください。

異なる階層（現時点では 2 階層までのサポート）のストレージを使用して、ストレージプールを作成できます。このようなストレージプールは、階層ストレージプールと呼ばれます。階層ストレージプールの詳細については、『*Storage Subsystem Administration Guide*』を参照してください。ファイルシステムデータ（メタデータとユーザーデータ）は、一つの階層または複数の階層に格納されます。ファイルシステムデータが複数の階層上のストレージシステムに格納される場合、ファイルシステムは階層ファイルシステムと呼ばれます。

階層ファイルシステムでは、メタデータはストレージの中で最も性能の高い階層に格納され、ユーザーデータは、低い性能の階層に格納されます。階層ファイルシステムには、次のような利点があります。

- 性能の向上
性能の高い階層にメタデータを格納することで、メタデータとユーザーデータを同じ性能の低い階層に格納するよりも、システム性能が向上します。これは、メタデータはユーザーデータより頻繁にアクセスされるので、より性能の高いストレージに格納することで、全体的な性能が向上するためです。
- ストレージのコスト削減
より性能の高いストレージ（通常、性能が低いストレージより高価）にメタデータを格納し、性能の低い（安価な）ストレージにユーザーデータを格納することで、コストを軽減できます。これは一般的に、メタデータは比較的少量のストレージしか消費しないのに対して、ユーザーデータは大量のストレージを消費するためです。性能の高いストレージはメタデータの保持にのみ使用されるので、メタデータとユーザーデータの両方が性能の高いストレージにある場合よりも、高価なストレージの数は少なく済みます。また、ユーザーデータは性能の低いストレージで保持することができ、メタデータとユーザーデータの両方を性能の低いストレージに保持するよりも高い性能が得られるため、ストレージを頻繁に新しくする必要がなくなります（また、新しくする際に、古いストレージを別の用途に再利用できる可能性もあります）。



重要 階層ファイルシステムは、WFS-2 ファイルシステム形式を使用してフォーマットしてください。ファイルシステム形式の詳細については、「1.1.1 ファイルシステム形式」を参照してください。

階層ファイルシステムには、次のような特性があります。

- データの分離を提供しながら、単一のファイルシステムビューを維持します。この分離によって、ファイルシステムはファイルシステムのメタデータ（システム性能に不可欠）を非常に高性能なデバイスに格納できると同時に、ユーザーデータを安価で低性能なストレージシステムに格納できます。

- ストレージの複数階層の使用は、アプリケーションやクライアントにとっては完全にトランスペアレントです。環境の微調整や労力は不要です。全てのファイルシステム機能(スナップショット、レプリケーション、Quota、クラスタネームスペース、仮想ボリュームなど)が使えます。
- マウント、アンマウント、共有、エクスポートなど、階層ファイルシステムのファイルシステム管理操作は、非階層ファイルシステムの場合と同じです。
- ファイルシステムブロックサイズ (4KB または 32KB) は、ストレージの全ての階層にわたって保持されます。
- クロスボリュームリンクはメタデータとして扱われます。

(1) 階層ファイルシステムとスナップショット

スナップショットは、変更されたブロックを所定の位置に保存します。階層ファイルシステムでは、これは、メタデータのスナップショットは Tier 0 (高価なストレージ階層) に保存されることを意味します。スペースは、スナップショットが削除されたときに最終的にリクレームされます。

スナップショットは、通常、ディスク容量のごく一部しか消費しませんが、メタデータのスナップショットは、より多くの割合を消費することがあります。ファイルシステムで高価なストレージ階層が容量不足になった場合、メタデータはファイルシステム内の別の場所に割り当てられます。

1.1.3 ファイルシステムのブロックサイズ

ファイルシステムのブロックサイズは、性能、ストレージサイズ、及びストレージの効率に影響します。

- ブロックサイズが 32KB のファイルシステムは、大きなファイルを転送する場合、高いスループットを提供します。しかし、小さな I/O 操作を大量に行う場合には、ブロックサイズが 32KB のファイルシステムよりも、ブロックサイズが 4KB のファイルシステムの方が性能が高くなります。
- ファイルシステムが比較的小さなファイルを大量に含む場合は、4KB のファイルシステムブロックサイズの方が容量を有効利用できます。

例えば 42KB のファイルを保存する場合、以下のようになります。

- ブロックサイズが 32KB のファイルシステムでは、42KB のファイルは二つの 32KB ブロックを占有するので、合計 64KB が使用されます ($2 \times 32\text{KB} = 64\text{KB}$)。
- ブロックサイズが 4 KB のファイルシステムでは、42KB のファイルは 11 の 4 KB ブロックを占有するので、合計 44 KB が使用されます ($11 \times 4\text{KB} = 44\text{KB}$)。
- この例では、32KB ブロックサイズでは 22KB の容量が無駄になるのに対して、4KB ブロックサイズでは 2KB の容量しか無駄になりません。

同じストレージプール内に複数のファイルシステムを構成する利点の一つは、4KB ブロックサイズを必要とするアプリケーションと 32KB ブロックサイズを必要とするアプリケーションとがストレージを共有できることです。

1.1.4 リードキャッシュ

リードキャッシュは特殊な読み取り専用ファイルシステムであり、個々のファイルのコピーをローカルファイルシステムの外に格納して、HNAS がファイルのキャッシュコピーを持てるようにします。NFS v3 クライアントがリードキャッシュ内のファイルに対する読み取り要求を送信すると、HNAS はリードキャッシュ内のコピーから読み取り要求に応えることができます。リードキャッシュは CIFS クライアントには利点がなく、リードキャッシュには特殊な特性と制限があります。リードキャッシュについては、『*Server and Cluster Administration Guide*』を参照してください。

1.1.5 WORM ファイルシステム

HNAS は、Write Once Read Many (WORM) ファイルシステムをサポートします。WORM ファイルシステムは、企業の重要データを変更不能な状態で特定の期間だけ保存するために広く使用されています。



重要 WORM ファイルシステムを使用するには、ライセンスが必要です。WORM ライセンスの購入方法については、お問い合わせ先にご相談ください。

HNAS は、「strict」と「non-strict」の2種類の WORM ファイルシステムをサポートします。

- strict WORM ファイルシステムは、削除や再フォーマットができないため、厳密なコンプライアンス対策を展開する準備ができてから使用してください。
- non-strict WORM ファイルシステムは、再フォーマットが可能なため、テスト目的に限って使用してください。non-strict WORM ファイルシステムを削除する必要がある場合は、まず、WORM 以外のファイルシステムとして再フォーマットすることが必要です。



注意 WORM ファイルシステムは、企業のデータ保持ポリシーが政府の規制を順守していることを確実にするために、法を順守する目的でファイルシステムを使用する必要がある場合にのみ作成してください。

(1) WORM の特性

WORM ファイルシステムには、通常のファイルシステムにはない非常に重要ないくつかの特性があります。

- WORM としてマークされると変更できません。ネットワーククライアントは他のファイルにアクセスするときと同じように WORM ファイルシステム上のファイルにアクセスできます。ただし、ファイルが WORM としてマークされると、ファイルは読み取り専用になり、その他のアクセスは制限されます。WORM ファイルは、変更、名前の変更、または削除することはできず、権限や所有権を変更することもできません。このような制限は、所有者、ドメイン管理者、root など全てのユーザーに適用されます。
- 一度 WORM になると、常に WORM となります。WORM としてマークされたファイルは、保持期限が過ぎるまで WORM ファイルのままです。これに対して、WORM としてマークされていないファイルは、通常のファイルと同様にアクセスでき、使用できます。
- WORM ファイルシステムを拡張して、ストレージを追加することはできますが、使用済みスペースをリクレイムしたり、WORM ファイルシステムを削除したりすることはできません。

1.2 ファイルシステム性能の管理

per-file system throttling(PFST)コマンドを使用して、ファイルシステムの性能を管理することができます。PFSTにより、特定のファイルシステムに対してリソース使用の上限を設定することができます。サーバーリソースの過剰使用を防ぎます。全ての PFST コマンドは、クラスタ全体に有効となります。

1.2.1 PFST 機能を使う

PFST 機能を使用するには、Dev User アクセス権が必要です。PFST 機能では、以下の操作が実行できます。

- PFST を有効または無効にする。
- Quota やキューに入った操作の数など、PFST プロパティを一覧表示する。
- PFST クラスを作成、削除、及び変更する。

- ・ PFST クラスにファイルシステムのマッピングを保持する。

(1) PFST クラスを有効にする

PFST bossock fiber quota を有効にするには、以下の CLI コマンドを使用します。

```
per-fs-throttle-class-enable
```

詳細については、CommandLine Reference Guide を参照してください。

(2) PFST クラスを無効にする

PFST bossock fiber quota を無効にするには、以下の CLI コマンドを使用します。

```
per-fs-throttle-class-disable
```

詳細については、CommandLine Reference Guide を参照してください。

(3) PFST クラスを作成する

PFST クラスを作成するには、以下の CLI コマンドを使用します。

```
per-fs-throttle-class-create
```

詳細については、CommandLine Reference Guide を参照してください。

(4) PFST クラスを削除する

PFST クラスを削除するには、以下の CLI コマンドを使用します。

```
per-fs-throttle-class-delete
```

詳細については、CommandLine Reference Guide を参照してください。

(5) PFST クラスを変更する

PFST クラスを変更するには、以下の CLI コマンドを使用します。

```
per-fs-throttle-class-set
```

詳細については、CommandLine Reference Guide を参照してください。

1.2.2 ファイルシステムを作成する

この手順は、既存のストレージプール内に新しいファイルシステムまたはリードキャッシュを作成します。ファイルシステムまたはリードキャッシュを作成するには、ストレージプールが必要です。



重要 Dynamic Write Balancing が有効でない場合、またはシステムが Dynamic Write Balancing をサポートしない場合、最適なパフォーマンスを得るには、ストレージプールを拡張するとき、できるだけ多くのディスクドライブを使用して、SD をできるだけ大きく取ってください。Dynamic Write Balancing の詳細については、『Storage Subsystem Administration Guide』を参照してください。

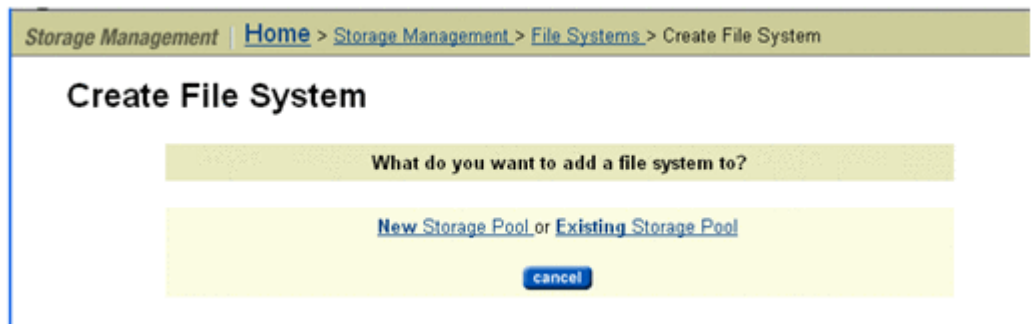
ファイルシステムを作成するには

1. [Create] 画面に移動します。

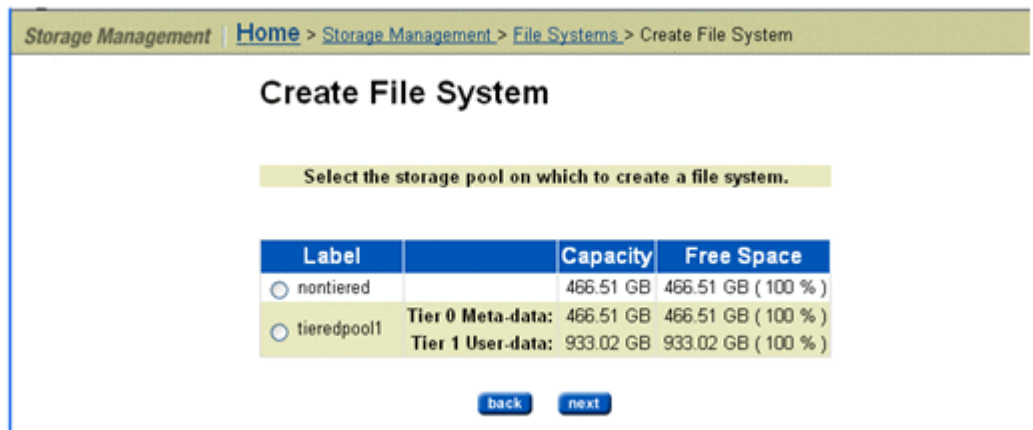
ファイルシステムを作成するには、[Home] 画面に移動します。[Storage Management] セクションの [File Systems] を選択して、[File Systems] 画面を表示し、[create] をクリックして、[Create] 画面を表示します。



2. ファイルシステムまたはリードキャッシュを選択します。
 - 通常のファイルシステム（リードキャッシュではないファイルシステム）を追加するには、[File System] をクリックして、次のステップへ進みます。
 - リードキャッシュを追加するには、[Read Cache] をクリックします。リードキャッシュの作成の詳細については、『*Storage Subsystem Administration Guide*』を参照してください。
 - ファイルシステムを作成せずに [File Systems] 画面に戻るには、[Cancel] をクリックします。
3. 新規または既存のストレージプールの場所を指定します。
 [Create File System] 画面で、新しい（これから作成する）ストレージプールを使用するか、既存のストレージプールを使用するかを指定します。



- ファイルシステムまたはリードキャッシュ用の新しいストレージプールを作成するには、[New Storage Pool] をクリックして、[Storage Pool Wizard] を起動します。Storage Pool Wizard の詳細については、『*Storage Subsystem Administration Guide*』を参照してください。
- 既存のストレージプールにファイルシステムまたはリードキャッシュを追加するには、[Existing Storage Pool] をクリックして、[Create File System] 画面を表示します。



ファイルシステムを作成するストレージプールを選択して、[next] をクリックします。

4. 通常のファイルシステムを作成します。



注意 このステップは、通常のファイルシステムの作成を選択した場合のステップです。リードキャッシュを作成するには、このステップをスキップして、次のステップへ進んでください。

通常のファイルシステム用の [Create File System] 画面で、要求された情報を入力します。

- 非階層ストレージプールを選択した場合は、非階層ファイルシステムを作成します。

[Create File System] 画面は、次のようになります。

- 階層ストレージプールを選択した場合は、階層ファイルシステムを作成します。

[Create File System] 画面は、次のようになります。

Create File System on ttestt1

Storage Pool: ttestt1
 Free Capacity: 2.28 TB
 Tier 0 Meta-data: 1.82 TB
 Tier 1 User-data: 466.51 GB
 Guideline Chunk Size: 7.32 GB

Size Limit: GB (This will be the confining size for Tier 1 User-data)
 Rounded Size Limit: 0.00 Bytes [Rounded up to nearest chunk](#)

Auto-Expansion: Enabled Create a small file system and allow it to automatically expand to the Size Limit.
 Disabled Create the file system to the full size specified by the Size Limit. The file system will not grow automatically.

Initial Capacity: 7.32 GB [Rounded to nearest chunk](#)

Label:

Assign to EVS:

WORM:

WFS Version:

Object Replication Target:

Block Size: 32 KB Provides higher throughput when transferring large files
 4 KB More efficient space utilization with lots of relatively smaller files

次の表では、この画面のフィールドについて説明し、通常のファイルシステムに関する注意事項も示します。

項目/フィールド	説明	通常のファイルシステムの設定
Storage Pool	ファイルシステムが作成されるストレージプールの名前です。	(表示のみ)
Free Capacity	ファイルシステムまたはリードキャッシュが使用できるストレージプールの使用可能な容量です。	(表示のみ)
Tier 0 Meta-data and Tier 1 User-data	ストレージプールのメタデータ階層 (Tier 0) とユーザーデータ階層 (Tier 1) のサイズです。	(表示のみ) 注：この情報は階層ファイルシステムにのみ該当するもので、非階層ファイルシステムでは表示されません。
Guideline Chunk Size	選択したストレージプールで使用されるチャンクのサイズです。	(表示のみ)
Size Limit	自動拡張を有効にした場合 <ul style="list-style-type: none"> 非階層ファイルシステムの場合、ファイルシステムを拡張できる最大サイズです。 階層ファイルシステムの場合、ファイルシステムのユーザーデータ階層 (Tier 1) を拡張できる最大サイズです。 	ファイルシステムのサイズ制限を入力します。このフィールドで、自動拡張によってファイルシステムまたはユーザーデータ階層が拡張される最大サイズを定義します。ファイルシステムを作成した後は、[File System Details] 画面で、この値を変更できます。この制限は、CLI から実行する手動の

項目／フィールド	説明	通常のファイルシステムの設定
	自動拡張を無効にした場合は、新しいファイルシステムの作成時の容量を指定します。ファイルシステムが作成されると、この量のスペースがファイルシステムにただちに割り当てられます。これは、現在未使用のスペースがこのファイルシステムのために予約され、他の用途には使用できなくなることを意味します	ファイルシステム拡張には適用されません。
Rounded Size Limit	定義されたサイズ制限と、ストレージプールについて定義されたチャンクサイズに基づく、おおよそのサイズ制限です。詳細については、[Rounded to nearest chunk] をクリックしてください。指定したサイズがチャンクサイズの倍数でなかった場合、チャンクサイズ単位で切り捨てます。	この設定はシステムによって自動的に計算されますが、変更が可能です。
Auto-Expansion	これらのラジオボタンを使用して、自動拡張を有効または無効にします。つまり、このファイルシステムまたはユーザーデータ階層（階層ファイルシステムの場合）の拡張を許可または制限します。 注：ファイルシステムの自動拡張の管理については、「1.2.8 (4) ファイルシステムの拡張を管理する」を参照してください。	ファイルシステムを自動拡張しないように設定することができます。スペースがファイルシステムに割り当てられると、スペースを回復することはできません。そのため、ファイルシステムのサイズを縮小することはできません。拡張時、ファイルシステムはストレージプールのチャンクサイズを拡張の単位として使用します。自動的に拡張するように構成されたファイルシステムは、約 80% が使用済みになると拡張します。ファイルシステムは、CLI を使用して手動で拡張できます。ファイルシステムの拡張時、ファイルサービスは中断されず、ファイルシステムをアンマウントする必要はありません。
Initial Capacity	ファイルシステムまたは階層ファイルシステムのユーザーデータ階層の初期容量。自動拡張が発生すると、ファイルシステムは上記で指定された [Size Limit] まで拡張されます。	ファイルシステム／ユーザーデータ階層の初期サイズを設定します。
Label	ファイルシステムを参照する名前を入力します。ファイルシステムには、そこに含まれるデータを表す名前を付けてください。また、システムを移動する必要が生じた場合に備えて、サイト全体で一貫したファイルシステム名を付けるようにしてください。	ファイルシステムの名前は、大文字と小文字が区別されませんが、表示上は大文字と小文字が区別されます（名前は入力されたとおりの大文字と小文字の組み合わせで表示されます）。また、ファイルシステムの名前には、スペースと特殊文字（"&'*/;:<>?¥ ）を含むことはできません。

項目/フィールド	説明	通常のファイルシステムの設定
		ファイルシステムの名前は、HNAS で一意であることが必要です。また、ファイルシステムにストレージプールと同じ名前を付けることはできません。
Assign to EVS	ファイルシステムが割り当てられる EVS を選択します。	EVS ドロップダウンリストから、ファイルシステムを割り当てる EVS を選択します。
WORM	保持制御を有効にするために使用します。詳細については、「1.3 WORM ファイルシステムを使用する」を参照してください。	ファイルシステムが通常のファイルシステムか WORM ファイルシステムかを選択します。ファイルシステムが規制の順守のために使用される場合を除き、[Not WORM] を選択してください。
WFS Version	ファイルシステム形式を指定するために使用します。 WFS-2 ファイルシステム形式は、WFS-1 形式 (Hitachi High-performance NAS Platform に よってサポートされるオリジナルファイルシステム) に代わるファイルシステム形式です。WFS-2 ファイルシステムは、Series 3000 の Hitachi High-performance NAS Platform 以降のハードウェアプラットフォーム (Hitachi NAS Platform を含む) でのみサポートされます。 詳細については、「1.1.1 ファイルシステム形式」を参照してください。	HNAS によってサポートされるときは、WFS-2 がデフォルトのファイルシステム形式です。新しいファイルシステムのファイルシステム形式を選択します。 注：ファイルシステムがいったんフォーマットされてしまうと、ファイルシステムをフォーマットせずにファイルシステム形式を変更することはできません。ファイルシステムをフォーマットすると、ファイルシステム内の全てのデータが消去されます。
Object Replication Target	ファイルシステムをオブジェクトレプリケーションの複製先にする場合は、このチェックボックスをオンにします。このチェックボックスをオンにすると、ファイルシステムは共有とエクスポートができるようにフォーマットされます。	
Block Size	ファイルシステムの最適なブロックサイズを構成するために使用します。詳細については、「1.1.3 ファイルシステムのブロックサイズ」を参照してください。	ファイルシステムのブロックサイズを選択します。

終了したら、構成を確認して、[OK] をクリックします。通常のファイルシステムが作成されます。



重要 ファイルシステムを使用するには、まず、フォーマットして、マウントする必要があります。Web Manager を使用してファイルシステムを作成する場合、ファイルシステムは自動的にフォーマットされません。デフォルトでは、WFS-2 がハードウェアプラットフォームによってサポートされるときには、新しいファイルシステムは WFS-2 形式を使用してフォーマットされます (詳細については、「1.2.2 ファイルシステムを作成する」と「1.2.4 ファイルシステムをフォーマットする」を参照してください)。ファイルシステムのマウントについては、「1.2.5 ファイルシステムをマウントする」を参照してください。

5. リードキャッシュを作成します。



注意 このステップは、リードキャッシュの作成を選択した場合のステップです。通常のファイルシステムを作成するには、前のステップを参照してください。

リードキャッシュ用の [Create Read Cache] 画面で、要求された情報を入力します。

- 非階層ストレージプールを選択した場合は、非階層リードキャッシュを作成します。
[Create Read Cache] 画面は次のようになります。

The screenshot shows the 'Create Read Cache on nontiered1' dialog box. At the top, the breadcrumb path is 'Storage Management | Home > Storage Management > File Systems > Create Read Cache'. The title is 'Create Read Cache on nontiered1'. The main content area is yellow and contains the following information:

- Storage Pool: nontiered1
- Free Capacity: 466.51 GB
- Guideline Chunk Size: 5.00 GB
- Size: [] GB (dropdown)
- Rounded Size: 0.00 Bytes (input field) with a link 'Rounded up to nearest chunk' and a small icon.
- Label: [] (input field)
- Assign to EVS: evs01 (dropdown)
- WFS Version: WFS-2 (dropdown)
- Block Size: 32 KB Provides higher throughput when transferring large files; 4 KB More efficient space utilization with lots of relatively smaller files.

At the bottom, there are 'OK' and 'cancel' buttons. At the very bottom, there is a footer with 'Home | About | Sign Out'.

- 階層ストレージプールを選択した場合は、階層リードキャッシュを作成します。
[Create Read Cache] 画面は次のようになります。

The screenshot shows the 'Create Read Cache on tieredpool1' dialog box. At the top, the breadcrumb path is 'Storage Management | Home > Storage Management > File Systems > Create Read Cache'. The title is 'Create Read Cache on tieredpool1'. The main content area is yellow and contains the following information:

- Storage Pool: tieredpool1
- Free Capacity: 922.99 GB
- Tier 0 Meta-data: 461.50 GB
- Tier 1 User-data: 461.50 GB
- Guideline Chunk Size: 5.00 GB
- Size: [] GB (dropdown) with a note '(This will be the confining size for Tier 1 User-data)'
- Rounded Size: 0.00 Bytes (input field) with a link 'Rounded up to nearest chunk' and a small icon.
- Label: [] (input field)
- Assign to EVS: evs01 (dropdown)
- WFS Version: WFS-2 (dropdown)
- Block Size: 32 KB Provides higher throughput when transferring large files; 4 KB More efficient space utilization with lots of relatively smaller files.

At the bottom, there are 'OK' and 'cancel' buttons.

次の表では、この画面のフィールドについて説明し、リードキャッシュに関する注意事項も示します。

項目/フィールド	説明	リードキャッシュの設定
Storage Pool	リードキャッシュが作成されるストレージプールの名前です。	(表示のみ)
Free Capacity	ファイルシステムまたはリードキャッシュが使用できるストレージプールの使用可能な容量です。	(表示のみ)
Tier 0 Meta-data and Tier 1 User-data	ストレージプールのメタデータ階層 (Tier 0) とユーザーデータ階層 (Tier 1) のサイズです。	(表示のみ) 注：この情報は階層ファイルシステムにのみ該当するもので、非階層ファイルシステムでは表示されません。
Guideline Chunk Size	選択したストレージプールで 사용되는チャンクのサイズです。	(表示のみ)
Size	作成されるリードキャッシュのサイズです。	リードキャッシュのサイズを入力します。 <ul style="list-style-type: none"> 非階層リードキャッシュの場合、リードキャッシュの合計サイズを定義します。 階層リードキャッシュの場合、リードキャッシュのユーザーデータ階層のサイズを定義します。 リードキャッシュが作成された後は、[File System Details] 画面でサイズの値を変更できます。
Rounded Size	これは、定義されたサイズ制限と、ストレージプールについて定義されたチャンクサイズに基づいて、ファイルのおおよそのサイズ制限を示します。詳細については、[Rounded to nearest chunk] をクリックします。	この設定は、システムによって自動的に計算されますが、変更ができません。
Label	リードキャッシュを参照する名前を入力します。 注：ファイルシステムまたはリードキャッシュの名前では、大文字と小文字は区別されず、スペースまたは特殊文字を使用することはできません。	[Label] テキストボックスに、新しいリードキャッシュの名前を入力します。 リードキャッシュの名前は、大文字と小文字が区別されませんが、表示上は大文字と小文字が区別されます (名前は入力されたとおりの大文字と小文字の組み合わせで表示されます)。また、リードキャッシュの名前には、スペースと特殊文字 ("&'*/;:<>?¥) を含むことはできません。 リードキャッシュに通常のファイルシステムまたはストレージプールと同じ名前を付けることはできません。
Assign to EVS	リードキャッシュが割り当てられる EVS を選択します。リードキャッシュは、クラスタノードへの優先マッピングを持つ EVS に割り当ててください。	EVS ドロップダウンリストから、リードキャッシュを割り当てる EVS を選択します。

項目/フィールド	説明	リードキャッシュの設定
WFS Version	<p>ファイルシステム形式を指定するために使用します。</p> <p>WFS-2 ファイルシステム形式は、WFS-1 形式 (Hitachi High-performance NAS Platform によってサポートされるオリジナルファイルシステム) に代わるファイルシステム形式です。WFS-2 ファイルシステムは、Series 3000 の Hitachi High-performance NAS Platform 以降のハードウェアプラットフォーム (Hitachi NAS Platform を含む) でのみサポートされます。</p> <p>詳細については、「1.1.1 ファイルシステム形式」を参照してください。</p>	<p>サポートされるときには、WFS-2 がデフォルトのファイルシステム形式です。新しいファイルシステムのファイルシステム形式を選択します。</p> <p>注：ファイルシステムがいったんフォーマットされてしまうと、ファイルシステムをフォーマットせずにファイルシステム形式を変更することはできません。ファイルシステムをフォーマットすると、ファイルシステム内の全てのデータが消去されます。</p>
Block Size	<p>リードキャッシュの最適なブロックサイズを構成するために使用します。詳細については、「1.1.3 ファイルシステムのブロックサイズ」を参照してください。</p>	<p>ファイルシステムのブロックサイズを選択します。</p>

終了したら、構成を確認して、[OK] をクリックします。リードキャッシュが作成され、[File System Details] 画面が表示されます。



注意 一つのクラスタノードに作成するリードキャッシュは一つだけにしてください。複数のリードキャッシュを作成しても、一つしか使用されません。



重要 リードキャッシュを使用するには、まず、フォーマットして、マウントする必要があります。Web Manager を使用してリードキャッシュを作成する場合、リードキャッシュは自動的にフォーマットされません。リードキャッシュのマウントについては、「1.2.5 ファイルシステムをマウントする」を参照してください。

1.2.3 ファイルシステムを削除する

ファイルシステムは、Strict WORM ファイルシステムでない限り、いつでも削除できます。ファイルシステムが削除されると、未使用スペースはストレージプールに戻されます。



注意 削除したファイルシステムを元に戻すことはできません。



重要 ファイルシステムを削除するには、ユーザーは「Global Admin」または「Storage Admin」でなければならない、Advanced Mode が有効になっていることが必要です。詳細については、『User Administration Guide』を参照してください。

ファイルシステムを削除するには

1. ファイルシステムを選択します。

[Home] 画面で、[Storage Management] セクションの [File Systems] をクリックして、ファイルシステムの一覧を表示します。削除するファイルシステムの [details] をクリックします。
2. ファイルシステムを削除します。
 - a. アンマウントします。

ファイルシステムがマウントされている場合は、[unmount] をクリックします。確認ダイアログで [OK] をクリックします。

- b. 削除します。

[Actions] セクションの [delete] をクリックします。次に、確認ダイアログの [OK] をクリックします。

1.2.4 ファイルシステムをフォーマットする

ファイルシステムをフォーマットすると、クライアントがデータストレージとして使用できるようになります。Web UI から作成されるファイルシステムは、自動的にフォーマットされ、マウントされます。したがって、この手順はほとんど使用されることはありません。



注意 この手順を使用する際は、次の点に注意してください。

- ファイルシステム内の既存のデータは失われます。
- ユーザーは「Global Admin」または「Storage Admin」で、Advanced Mode が有効であることが必要です。詳細については、『*User Administration Guide*』を参照してください。
- この手順では、ファイルシステムが既にマウントされていることを前提としています。詳細については、『1.2.5 ファイルシステムをマウントする』を参照してください。

既存のファイルシステムをフォーマットするには

1. ファイルシステムを選択します。

[Home] 画面で、[Storage Management] セクションの [File Systems] をクリックして、ファイルシステムの一覧を表示します。

2. ファイルシステムをアンマウントします。

ファイルシステムがマウントされている場合は、次のようにしてアンマウントします。

- [Label] 列からファイルシステムを選択します。
- [Actions] セクションの [unmount] をクリックします。
- 確認ダイアログで [OK] をクリックします。

3. [Format File System] 画面に移動します。

フォーマットするファイルシステムの [details] をクリックします。[format] をクリックして、[Format File System] 画面を表示します。

4. ファイルシステムを WORM としてフォーマットするかどうかを指定します。

ファイルシステムを WORM (Write Once Read Many) ファイルシステムとしてフォーマットするか、通常のファイルシステムとしてフォーマットするかを指定します。値は、次のいずれかです。

- Not WORM

WORM ファイルシステムではないファイルシステムで、再フォーマットできます。

- Strict WORM
再フォーマットできない WORM ファイルシステムです。
- Non-strict WORM
再フォーマットできる WORM ファイルシステムです。

WORM ファイルシステムの詳細については、「[1.1.5 WORM ファイルシステム](#)」を参照してください。

5. ファイルシステムの WFS バージョンとブロックサイズを選択します。
 - [WFS Version] ドロップダウンリストを使用して、ファイルシステムの形式として WFS-2 を選択します。ファイルシステム形式の詳細については、「[1.1.1 ファイルシステム形式](#)」を参照してください。



重要 階層ファイルシステムは、WFS-2 ファイルシステム形式を使用してフォーマットしてください。ファイルシステム形式の詳細については、「[1.1.1 ファイルシステム形式](#)」を参照してください。

- ラジオボタンを使用して、ファイルシステムのブロックサイズとして 32KB または 4KB を選択します。ブロックサイズと、ブロックサイズがファイルシステムの性能に与える影響の詳細については、「[1.1.3 ファイルシステムのブロックサイズ](#)」を参照してください。
6. ファイルシステムを、オブジェクトレプリケーションの複製先にするかどうかを指定します。

ファイルシステムを、オブジェクトレプリケーションの複製先にする場合は、[Object Replication Target] チェックボックスをオンにします。ファイルシステムをオブジェクトレプリケーションの複製先にしない場合は、[Object Replication Target] チェックボックスがオフになっているか確認してください。

ファイルシステムを複製先にするためには、オブジェクトレプリケーションの複製先としてフォーマットされていることが必要です。このチェックボックスをオンにすると、ファイルシステムは共有とエクスポートができるようにフォーマットされます。
 7. ファイルシステムをフォーマットします。

[OK] をクリックして次へ進むか、[cancel] をクリックして [File System Details] 画面に戻ります。

1.2.5 ファイルシステムをマウントする

この手順を使用して、ファイルシステムを手動でマウントします。フォーマット済みファイルシステムをマウントすることによって、共有またはエクスポートが可能になり、ネットワーククライアントがアクセスできるようになります。この手順は、次のような状況でファイルシステムの自動マウントが失敗したときに使用することもできます。

- HNAS がシャットダウンしたときに、ファイルシステムがマウントされていなかった。
- CLI により、自動マウントが無効にされていた。
- ストレージシステムの障害により、HNAS が再起動した。

ファイルシステムをマウントするには

1. ファイルシステムを選択します。

[Home] 画面で、[Storage Management] セクションの [File Systems] をクリックして、ファイルシステムの一覧を表示します。マウントするファイルシステムの名前の横にあるチェックボックスをオンにします。
2. ファイルシステムをマウントします。

ファイルシステムがアンマウントされている場合は、[mount] をクリックします。

(1) ファイルシステムをアンマウントする

ファイルシステムをサービスから削除する必要があるときは、アンマウントします。クライアント側から見ると、単に表示されなくなるだけです。これは、ファイルシステムに損傷を与えず、ファイルシステム内のデータにも影響を与えません。



重要 HNAS のシャットダウンや再起動の前にファイルシステムをアンマウントする必要はありません。HNAS のシャットダウンまたは再起動時にマウントされていたファイルシステムは、HNAS の再起動時に自動的にマウントされます。

- ファイルシステムを選択します。
[Home] 画面で、[Storage Management] セクションの [File Systems] をクリックして、ファイルシステムの一覧を表示します。アンマウントするファイルシステムの名前の横にあるチェックボックスをオンにします。
- ファイルシステムをアンマウントします。
ファイルシステムがマウントされている場合は、[unmount] をクリックします。
確認ダイアログで [OK] をクリックします。

1.2.6 使用可能なファイルシステムを表示する

使用可能なファイルシステムを表示するには、[Storage Management] 画面に移動し、[File Systems] をクリックして、[File Systems] 画面を表示します。

▼ Label	Total	Used (%)	Used	Free	Storage Pool	Status	EVS	
<input type="checkbox"/> 244_fs1	4.75 GB	47%	2.22 GB	2.53 GB	244_r5_pool	Mounted	EVS01	details
<input type="checkbox"/> 3sd_spanfs1	29.75 GB	9%	2.56 GB	27.19 GB	3sd_span	Mounted	EVS01	details
<input type="checkbox"/> 5sd_spanfs1	29.75 GB	9%	2.63 GB	27.12 GB	5sd_span	Mounted	EVS01	details
<input checked="" type="checkbox"/> 5sd_spanfs2	29.75 GB	9%	2.60 GB	27.15 GB	5sd_span	Mounted	EVS01	details
<input type="checkbox"/> 7sd_spanfs1	29.75 GB	8%	2.48 GB	27.27 GB	7sd_span	Mounted	evs02	details
<input type="checkbox"/> 7sd_spanfs2	29.75 GB	8%	2.33 GB	27.42 GB	7sd_span	Mounted	evs02	details
<input type="checkbox"/> 7sd_spanfs3	29.75 GB	9%	2.66 GB	27.09 GB	7sd_span	Mounted	evs02	details
<input type="checkbox"/> bidirect_span_fs1	39.75 GB	5%	2.16 GB	37.59 GB	bidirect_span	Mounted	EVS01	details

Check All | Clear All

Actions: [mount](#) [unmount](#) | [create](#) [Download File Systems](#)

Shortcuts: [System Drives](#) [Quotas by File System](#) [Storage Pools](#) [Active Tasks](#)

Home | About | Sign Out

次の表では、この画面の項目について説明します。

項目/フィールド	説明
Label	ファイルシステムの名前です。作成時に割り当てられ、エクスポートの作成やスナップショットの作成など、特定の操作を実行するときにファイルシステムを識別するために使用されます。
Total	ファイルシステムのサイズ (GB) です。
Used	使用済みスペースの量 (GB) です。
Free	使用可能なスペースの量 (GB) です。
Storage Pool	ファイルシステムのあるストレージプールの名前です。
Status	Checking

項目/フィールド	説明
	<p>ファイルシステムはチェック中です。このチェックの際、チェックの各フェーズのおおよその完了率が表示されます（他のフェーズより時間のかかるフェーズもあります。また、完了率は現在のフェーズの完了率であり、手順全体の完了率ではありません）。</p> <p>Failing ファイルシステムに障害があり、チェック、修復、またはリカバリー中です。</p> <p>Fixing ファイルシステムは修理中です。修理中、修理の各フェーズのおおよその完了率が表示されます（他のフェーズより時間のかかるフェーズもあります。また、完了率は現在のフェーズの完了率であり、手順全体の完了率ではありません）。</p> <p>Formatting ファイルシステムはフォーマット中です。</p> <p>Initializing System Drive System Drive の初期化中です。</p> <p>Mounted ファイルシステムはマウントされ、使用可能です。</p> <p>Mounted as Readonly ファイルシステムはマウントされましたが、読み取り専用モードです。</p> <p>Mounting ファイルシステムはマウント中であり、使用可能です。</p> <p>Not Assigned to EVS ファイルシステムは EVS に割り当てられていません。</p> <p>Not Available for Mounting ファイルシステムは使用できません。ファイルシステムが割り当てられた EVS を有効にして、ファイルシステムが「hidden」としてマークされていないか確認してください。</p> <p>Not Mounted ファイルシステムはマウントされていません。</p> <p>Not Mounted (System Drive initialization status unknown) ファイルシステムはマウントされておらず、SD 初期化ステータスは不明です。</p> <p>Not Mounted (System Drive is not initialized) ファイルシステムはマウントされておらず、SD 初期化ステータスはわかっていますが、SD の初期化が完了していません。</p> <p>Syslocked ファイルシステムは syslock されています。Syslocked モードの詳細については、「1.2.12 ファイルシステムでシステムロックを使用する」を参照してください。</p>
EVS	ファイルシステムが割り当てられている EVS です。
mount	ファイルシステムをマウントするには、アンマウントされているファイルシステムを選択して、[mount] をクリックします。
unmount	ファイルシステムをアンマウントするには、マウントされているファイルシステムを選択して、[unmount] をクリックします。

次の [Usage Alerts] 条件が適用されます。

- [Usage Alerts] がファイルシステム全体で有効になっている場合、Warning limit を超えるとスライドバーが黄色になり、Severe limit を超えると琥珀色になります。
- [Usage Alerts] が有効でない場合、容量の 85% に達するとスライドバーが黄色になり、ファイルシステムが満杯になると琥珀色になります。

[Actions] では、次のアクションを使用できます。

- [Download File Systems] をクリックすると、一覧表示されているファイルシステムに関する情報をスプレッドシートでダウンロードできます。

- ・ [System Drives] をクリックすると、[System Drives] 画面が表示されます。
- ・ [Quotas by File System] をクリックすると、「1.4.4 (2) ユーザー／グループのデフォルトを設定する」で説明する [Quotas by File System] 画面が表示されます。
- ・ [Storage Pools] をクリックすると、HNAS 上のストレージプールの一覧が表示されます。
- ・ [Active Tasks] をクリックすると、アクティブなタスクに関する情報を示す [Active Tasks] 画面が表示されます。



重要 HNAS は、シャットダウン時にマウントされていたファイルシステムを記憶して、システム起動時にそれらを自動的にマウントします。

1.2.7 ファイルシステムの詳細設定を表示する

[File Systems] 画面でファイルシステムを選択して、[details] をクリックすると、[File System Details] 画面が表示されます。

Storage Management | Home > Storage Management > File Systems > File System Details

File System Details

Settings/Status

Label: [rename](#)

Capacity

4% Total Used Space
Capacity: 65.63 GB
Free: 63.32 GB (96%)
Total Used: 2.31 GB (4%)

Live File System: 2.31 GB (4%)
Snapshots: 0 Bytes (0%)

Tier 0 Meta-data

0% Total Used Space
Capacity: 32.85 GB
Free: 32.70 GB (100%)
Total Used: 147.25 MB (0%)

Confine Auto-Expansion to: GB [apply](#)
Auto-expansion is not confined

Tier 1 User-data

7% Total Used Space
Capacity: 32.80 GB
Free: 30.61 GB (93%)
Total Used: 2.19 GB (7%)

Confine Auto-Expansion to: GB [apply](#)
Auto-expansion is not confined

Legend: ■ Live File System ■ Snapshots ■ Usage Warning ■ Usage Severe

Configuration

Status: Mounted
Syslock: disabled [enable](#)
Object Replication Target: disabled
Transfer Access Points During Object Replication: enabled [disable](#)
EVS: G5-evs2 (Online)
Security Mode: Mixed (Windows and Unix) (Inherited)
WORM: Not WORM
Block Size: 4 KB
Read Cache: No
WFS Version: WFS-2

Usage Thresholds

File System Usage			
	Live File System	Snapshots	Entire File System
Current:	4 %	0 %	4 %
Warning:	90 %	90 %	95 %
Severe:	97 %	97 %	97 %

Do not allow the live file system to expand above its Severe limit [apply](#)

Associations

Storage Pool: [G5_Doc_Pool_01](#)

Capacity: 9.82 TB
Free: 9.75 TB (99 %)
Used: 65.65 GB (1 %)

Related File Systems:
None

Check / Fix

Status: File System is not being checked or fixed.
Scope: Entire File System Directory Tree [browse...](#)
[check](#) [cancel](#) [Active Tasks](#)

Actions: [mount](#) [unmount](#) [format](#) [delete](#) [expand](#)

Shortcuts: [Data Migration Paths](#) [File System Versions](#)

Home | About | Sign Out

次の表では、この画面のフィールドについて説明します。

項目／フィールド	説明
Settings/Status	
Label	<p>ファイルシステムの名前です。作成時に割り当てられ、エクスポートの作成やスナップショットの作成など、特定の操作を実行するときにファイルシステムを識別するために使用されます。</p> <p>ファイルシステムの名前を変更するには、[Label] ボックスに新しい名前を入力して、[rename] をクリックします。</p> <p>ファイルシステムには、そこに含まれるデータを表す名前を付けてください。</p> <p>ファイルシステムの名前を付けるときは、次のルールに従う必要があります。</p> <ul style="list-style-type: none"> • ファイルシステムの名前は、大文字と小文字が区別されず、スペースと特殊文字 ("&'*/;:<>?¥) を含むことはできません。 • ファイルシステムの名前は、HNAS で一意であることが必要です。 • ファイルシステムにストレージプールと同じ名前を付けることはできません。 • サイト全体で一意なファイルシステム名を付けることを推奨します。
Capacity	<p>このエリアには、ファイルシステムのスペース割り当てと使用量に関する情報が表示されます。階層ファイルシステムの場合は、メタデータ階層とユーザーデータ階層の両方に関する情報が表示されます。非階層ファイルシステムの場合は、ファイルシステムの合計サイズが表示されます。</p> <ul style="list-style-type: none"> • % Total Used Space ファイルシステムに割り当てられた合計スペースのうち、使用済みスペースの割合です。この合計には、データとスナップショット（ある場合）が反映されます。 • Capacity フォーマット済みスペースの合計容量（未使用スペース+使用済みスペース）です。 • Free ファイルシステムの未使用のスペースの合計容量（GB）です。合計に占める割合も表示されます。 • Total Used ファイルシステムの使用済みスペースの合計容量（GB）です。合計に占める割合も表示されます。 • Live File System ファイルシステムのデータによって使用されているスペースの合計（GB）です。合計に占める割合も表示されます。 • Snapshots ファイルシステムのスナップショットによって使用されているスペースの合計（GB）です。合計に占める割合も表示されます。
Tier 0 Meta-data/Tier 1 User-data	<p>注：これらのエリアは、階層ファイルシステムの場合のみ表示されます。</p> <p>これらのエリアには、ファイルシステムを形成する階層のスペース割り当てと使用量に関する情報が表示されます。[Tier 0 Meta-data] セクションには、メタデータ階層に関する情報が表示されます。[Tier 1 User-data] セクションには、ユーザーデータ階層に関する情報が表示されます。</p> <ul style="list-style-type: none"> • % Total Used Space ファイルシステムに割り当てられた合計スペースのうち、使用済みスペースの割合です。この合計には、データとスナップショット（ある場合）が反映されます。 • Capacity フォーマット済みスペースの合計容量（未使用スペース+使用済みスペース）です。 • Free ファイルシステムの未使用のスペースの合計容量（GB）です。合計に占める割合も表示されます。 • Total Used ファイルシステムの使用済みスペースの合計容量（GB）です。合計に占める割合も表示されます。 • Confine Auto-Expansion to

項目/フィールド	説明
	階層の最大容量を示します (メタデータ/ユーザーデータとスナップショットを含みます)。階層に最初に割り当てられたストレージが使用されると、階層はこの制限まで自動拡張されます。 自動拡張制限を変更した場合は、[apply] をクリックして、変更を有効にする必要があります。
Configuration	
Status	ファイルシステムの現在のステータスです。ファイルシステムがマウントされているか、アンマウントされているかを示します。
Syslock	ファイルシステムが Syslocked モード (システムロックが有効) か、Syslocked モードではない (システムロックが無効) かを示します。 ファイルシステムのシステムロックが有効なときには、NDMP はファイルシステムへのフルアクセスを持ち、バックアップまたはレプリケーション時にファイルシステムに書き込むことができますが、ファイルサービスプロトコル (NFS, CIFS, FTP, 及び iSCSI) を使用しているクライアントに対しては、ファイルシステムは読み取り専用モードです。 ファイルシステムのシステムロックを有効または無効にするには、[enable] または [disable] をクリックします。リードキャッシュの詳細を表示しているときには、システムロックの [enable] 及び [disable] ボタンは使用できません。
Object Replication Target	ファイルシステムがオブジェクトレプリケーションの複製先としてフォーマットされているかどうかを示します。ファイルシステムを複製先にするためには、オブジェクトレプリケーションの複製先としてフォーマットされていることが必要です。
Transfer Access Points During Object Replication	オブジェクトレプリケーション時のアクセスポイントの転送許可が、ファイルシステムで有効になっているかどうかを示します。無効になっているときは、[enable] をクリックすると、ファイルシステムがオブジェクトレプリケーション時にアクセスポイントを転送できるようにできます。有効になっているときは、[disable] をクリックすると、オブジェクトレプリケーション時のアクセスポイントの転送を禁止できます。
EVS	ファイルシステムが割り当てられている EVS です。ファイルシステムが EVS に割り当てられていない場合、ファイルシステムを割り当てることができる EVS の一覧が表示されます。
Security Mode	ファイルシステムに定義されているファイルシステムセキュリティポリシーが表示されます。
WORM	このファイルシステムが Write Once Read Many ファイルシステムか、通常のファイルシステムかを示します。値は、次のいずれかです。 <ul style="list-style-type: none"> Strict WORM 再フォーマットできない WORM ファイルシステムです。 Non-strict WORM 再フォーマットできる WORM ファイルシステムです。 Not WORM WORM ファイルシステムではないファイルシステムで、再フォーマットできません。 WORM ファイルシステムの詳細については、「1.1.5 WORM ファイルシステム」を参照してください。
Block Size	ファイルシステムのブロックサイズです。32KB または 4KB のいずれかになります。ファイルシステムがフォーマットされる時に定義されます。
Read Cache	このファイルシステムがリードキャッシュ ([Yes]) か、通常のファイルシステム ([No]) かを示します。
WFS Version	このファイルシステムが WFS-1 ファイルシステムとしてフォーマットされているか、WFS-2 ファイルシステムとしてフォーマットされているかを示します。WFS ファイルシステムの詳細については、「1.1.1 ファイルシステム形式」を参照してください。
Auto-Expansion	

項目/フィールド	説明
Confine Auto-Expansion to	<p>注: このセクションは、非階層ファイルシステムの場合のみ表示されます。階層ファイルシステムの場合、この情報は上記の [Tier 0 Meta-data] 及び [Tier 1 User-data] セクションに組み込まれています。</p> <p>階層の最大容量を示します (メタデータ/ユーザーデータとスナップショットを含みます)。階層に最初に割り当てられたストレージが使用されると、階層はこの制限まで自動拡張されます。</p> <p>自動拡張制限を変更した場合は、[apply] をクリックして、変更を有効にする必要があります。</p>
Usage Thresholds	
File System Usage	<p>ファイルシステムに割り当てられたスペースに対する割合で表示されます。しきい値に達すると、イベントが記録され、Quota 設定に応じてメールが送信されます。このエリアには、次のそれぞれについて、現在の使用量に関する情報が表示されます。</p> <ul style="list-style-type: none"> ライブファイルシステム (データ) ファイルシステムのスナップショット ライブファイルシステムのデータとスナップショットの合計 <p>エディットボックスを使用して、Warning 及び Severe しきい値を指定できます。</p> <ul style="list-style-type: none"> [Warning] しきい値は、高い使用量だが危機的ではないレベルを示す値を設定してください。 [Severe] しきい値は、使用量が危機的レベルであり、容量の不足が差し迫った状況であることを示すように設定してください。 <p>次の全部またはいずれかについて、[Warning] と [Severe] の両方のしきい値を定義できます。</p> <ul style="list-style-type: none"> ライブファイルシステム (データ) ファイルシステムのスナップショット ライブファイルシステムとスナップショットの合計 <p>ライブファイルシステムが [Severe] しきい値設定を超えて拡張されて、スナップショットが失われないようにするには、[Do not allow the live file system to expand aboved its Severe limit] チェックボックスをオンにします。</p>
Associations	
Storage Pool	<p>ファイルシステムまたはリードキャッシュが作成されたストレージプールの名前です。</p> <p>このエリアには、次の情報も表示されます。</p> <ul style="list-style-type: none"> Capacity ストレージプールに割り当てられた合計スペースです。 Free ストレージプールの未使用スペースの合計 (MB, GB, または TB) です。合計に占める割合も表示されます。 Used ストレージプールの使用済みスペースの合計 (MB, GB, または TB) です。合計に占める割合も表示されます。
Related File Systems	<p>関連するファイルシステムの名前が表示されます。関連するファイルシステムは、次のいずれかです。</p> <ul style="list-style-type: none"> マイグレーションまたはレプリケーション操作において、このファイルシステムが移行先または複製先だった場合、その移行元または複製元 マイグレーションまたはレプリケーション操作において、このファイルシステムが移行元または複製元だった場合、その移行先または複製先 <p>関連ファイルシステムがある場合、最後に正常完了した操作 (マイグレーションまたはレプリケーション) の日付が表示されます。</p>
Check/Fix	
Status	<p>ファイルシステムが最後にチェックされた日時を示し、前回の再起動後のステータスを表示します。ファイルシステムのステータスメッセージは、次のいずれかです。</p> <ul style="list-style-type: none"> File system is not being checked or fixed. Checking. Fixing.

項目/フィールド	説明
	<p>[Scope] 設定と [browse] 及び [check] ボタンを使用して、ファイルシステム全体またはファイルシステムの一部のチェックを開始できます。</p> <p>一つ以上のチェックが進行中の場合は、[Active Tasks] をクリックすると、アクティブなタスクの詳細を示す [Active Tasks] 画面が表示されます。</p> <p>[cancel] をクリックすると、進行中のチェックが中止されます。</p>
Scope	<p>[Scope] コントロールでは、[Entire File System] ラジオボタンまたは [Directory Tree] ラジオボタンのいずれかを選択することによって、チェックの範囲を設定できます。</p> <p>ファイルシステム全体をチェックするには、[Entire File System] ラジオボタンを選択します。</p> <p>ファイルシステムの一部をチェックするには、[Directory Tree] ラジオボタンを選択してから、[browse] ボタンを使用して、チェックする箇所を指定します。</p> <p>範囲を設定したら、[check] をクリックします。チェックが開始されます。</p>

1.2.8 ファイルシステムのスペース使用を制御する

HNAS は、ファイルシステム上のスペース割り当てを監視して、事前設定のしきい値に達したときに、アラートをトリガーできます。必要に応じて、しきい値に達した場合、ユーザーがファイルを作成しないようにすることもできます。または、オンライン時にファイルシステムを手動、または自動で拡張できます。

以下の二つのアクティビティがシステムスペースを消費します。

- ライブファイルシステム
 ユーザーがファイルを追加したときや既存のファイルのサイズを増やしたときに消費されるスペースを指します。
- スナップショット
 特定の時点でのファイルシステムの一貫したイメージを指します。スナップショットはライブファイルシステムの完全なコピーではなく、スナップショットのサイズはライブファイルシステムに応じて変化します。ライブファイルシステムがスペースを使用するほど、スナップショットが使用するスペースも増えますが、ライブファイルシステム内のデータが変更されたときは、スナップショットはほとんどスペースを必要としません。



重要 ライブファイルシステムからファイルを削除すると、スナップショットが占有するスペースが増えることがあります。実際には、削除操作をしてもディスクスペースはリクレイムされません。スナップショットによって占有されていたスペースをリクレイムするための唯一確実な方法は、最も古いスナップショットから削除することです。

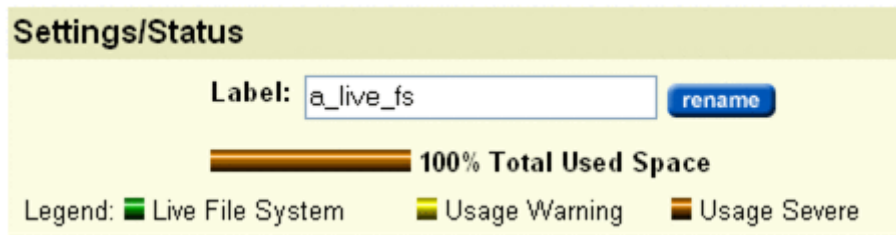
HNAS は、次のものによって占有されるスペースを追跡します。

- ライブファイルシステム内のユーザーデータ
- ファイルシステムメタデータ (HNAS がユーザーデータファイルの管理に使用するデータ)
- スナップショット
- ファイルシステム全体

これらのスライスのそれぞれについて、Warning しきい値と Severe しきい値の両方を構成することができます。これらはシステムごとに異なりますが、次の設定はほとんどの場合に有効です。

	Warning	Severe
ライブファイルシステム	70%	90%
スナップショット	20%	25%
ファイルシステム全体	90%	95%

ボリュームによって占有されるストレージスペースが **Warning** しきい値を超えると、**Warning** イベントがイベントログに記録されます。ファイルシステム全体の **Warning** しきい値に達すると、ディスク使用率を示すスペースバーが黄色になります。



スペースが **Severe** しきい値に達すると、**Severe** イベントがイベントログに記録され、対応するアラートが生成されます。ファイルシステム全体の **Severe** しきい値に達すると、ディスク使用率を示すスペースバーが琥珀色になります。

ファイルシステムの自動拡張が無効な場合、**Severe** しきい値を超えるライブファイルシステムの拡張を防止でき、スナップショットに使用できるスペースを確保できます。ライブファイルシステムを **Severe** しきい値として定義された使用可能スペースの割合に制限するには、[File System Details] 画面の [Do not allow the live file system to expand aboved its Severe limit] チェックボックスをオンにします。[File System Details] 画面の詳細については、「[1.2.7 ファイルシステムの詳細設定を表示する](#)」を参照してください。



重要 スペースまたはライブファイルシステム内のファイル数の追跡と制御、ユーザーとグループの **Quota** の構成、または仮想ボリュームの作成については、「[1.2.10 使用量 Quota を管理する](#)」と「[1.2.9 仮想ボリューム](#)」を参照してください。

(1) ファイルシステムの負荷を監視する

HNAS の性能は、1 秒間に実行した操作の数 (ops/sec) で測ることができます。Web Manager から、ops/sec の数をグラフで確認できます。これらの統計の表示またはダウンロードの詳細については、『*Server and Cluster Administration Guide*』を参照してください。

(2) ファイルシステムのサイズを拡張する

ファイルシステムに割り当てられるストレージの量を拡張するには、二つの方法があります。

- 手動拡張
- 自動拡張



重要 ファイルシステムに割り当てられたストレージは、そのファイルシステム専用になります。つまり、ファイルシステムが拡張されると、サイズを縮小することはできません。ファイルシステム内の未使用のスペースをリクレイムして、別のファイルシステムに割り当てたり、削除したりすることはできません。ストレージスペースをリクレイムするには、ファイルシステムを別のストレージに再配置するか（「[1.2.11 ファイルシステムを移動する](#)」を参照）、削除する必要があります。

ファイルシステムに割り当てられるストレージの量を（手動または自動で）増加するとき、ファイルシステムをオフラインにする必要はありません。ファイルシステム拡張の管理の詳細については、「[\(4\) ファイルシステムの拡張を管理する](#)」を参照してください。

ファイルシステムの手動拡張

ファイルシステムを手動で拡張すると、ファイルシステム（または階層ファイルシステムの階層）にストレージ容量をただちに追加できます。ファイルシステムの新しいサイズを指定すると、ストレージがただちに割り当てられます。ファイルシステムまたは階層の最大サイズが指定され、ファイルシステムサイズを、ファイルシステムが作成されたストレージプールがサポートする最大サイズに設定できます。手動ファイルシステム拡張の詳細については、「[\(7\) ファイルシステムを手動で拡張する](#)」を参照してください。

ファイルシステムの自動拡張

ファイルシステムの自動拡張では、ファイルシステムは、ファイルシステムの容量制限値または最大ファイルシステムサイズに達しない限り、必要に応じてストレージのチャンクを追加することによって拡張されます。階層ファイルシステムの場合、自動拡張はファイルシステムの一つの階層に個別に、または全ての階層に適用できるので、一つの階層だけを拡張することができます。

自動拡張を有効にすると、ファイルシステム（または階層）が割り当てられた容量の約 80% に達したときに、一つ以上の追加チャンクが割り当てられます（チャンクについては、『*Storage Subsystem Administration Guide*』を参照してください）。ファイルシステムの最大サイズを指定でき、または、ファイルシステムサイズを、ファイルシステムが作成されたストレージプールがサポートする最大サイズまで拡張可能として設定できます。ファイルシステムの自動拡張の詳細については、「(4) ファイルシステムの拡張を管理する」を参照してください。

(3) シンプロビジョニングファイルシステム

シンプロビジョニングは、ファイルシステムの空き容量の計算と報告の方法を制御する手段です。管理者はシンプロビジョニングを使用して、ストレージの使用を最適化し、経費削減と同時に、全てのユーザーのニーズに対応できるだけのストレージを確保できるような方法で、リソース取得のプランを立てることができます。

シンプロビジョニングによって、HNAS に接続されたストレージのオーバーサブスクリプションが可能で、使用可能なストレージがファイルシステムに完全に割り当てられない限り、オーバーサブスクリプションがストレージシステムのユーザーに気付かれることはありません。



重要 シンプロビジョニングが有効な場合、ストレージがオーバーサブスクリプションされると、クライアントが書き込み操作を試みて、ストレージスペースが不足していた場合、空きスペースの量に対するクエリーにより、そのスペースがまだ使用可能であることが示された場合でも、クライアントはスペース不足エラーを受け取ります。ストレージがオーバーサブスクリプションされた場合、HNAS の管理者は、この状況が起きないようにすることが必要です。HNAS は、この状況の発生を防止できません。この状況を解決するには、HNAS の管理者は、シンプロビジョニングを無効にするか、ストレージを追加することが必要です。

シンプロビジョニングが有効な場合、HNAS は、ファイルシステムに実際に割り当てられたストレージの量に基づいて空きスペースの量を報告するのではなく、ファイルシステムの拡張制限（構成された最大容量）に基づいて、ファイルシステムの空きスペースの量を報告します。ファイルシステムは指定された制限（拡張制限）まで自動的に拡張できるので、ファイルシステムが作成されるときに全てのストレージが割り当てられるのではなく、必要に応じて追加のストレージがファイルシステムに割り当てられます。ファイルシステムの自動拡張についての詳細は、「(2) ファイルシステムのサイズを拡張する」を参照してください。

例えば、ファイルシステムの拡張制限が 20TB であり、8TB が割り当て済みで、既に 6TB が使用されているとします。シンプロビジョニングが有効な場合、HNAS は、ストレージプールにある実際に使用可能な空きスペースの量に関係なく、システムには 14TB の空きスペースがあると報告します（ストレージプールの詳細については、『*Storage Subsystem Administration Guide*』を参照してください）。シンプロビジョニングが無効な場合、HNAS は、ファイルシステムには 2TB の空きスペースがあると報告します。

デフォルトでは、シンプロビジョニングは、既存のファイルシステムも新しく作成されるファイルシステムも無効に設定されます。シンプロビジョニングを有効または無効にするには、`filesystem-thin` コマンドを使用します（現時点では、Web Manager GUI によってシンプロビジョニングを有効または無効にする方法はありません）。

シンプロビジョニングは、ファイルシステム単位で作用し、`span-list --filesystems` 及び `filesystem-list` コマンドによって報告される容量には影響を与えません。また、Web Manager (GUI) は、実際のファイルシステムサイズを表示します。これにより、管理者は、正しく容量を計画することができます。

有効にした場合、シンプロビジョニング情報は、次の CLI コマンドによって返されます。

- cifs-share list
- df
- filesystem-limits
- filesystem-list -v
- fs-stat
- nfs-export list
- query

CLI コマンドの詳細については、『*Command Line Reference*』を参照してください。

シンプロビジョニングが有効であり、ストレージプールについてファイルシステムの自動拡張を無効にした場合、そのストレージプール内の各ファイルシステムについて報告される空き容量は、シンプロビジョニングが有効になっていなかった場合と同じです。これは、報告される空き容量が、ファイルシステムの現在の使用量と、そのファイルシステムに現在割り当てられている全てのストレージプールチャンク内のスペースの量の差に等しいことを意味します。ストレージプール内のファイルシステムについてファイルシステムの自動拡張を再び有効にした場合、空き容量は、ファイルシステムの現在の使用量と拡張制限との差として報告されます（拡張制限が指定されていた場合）。ファイルシステムの自動拡張の詳細については、「[\(2\) ファイルシステムのサイズを拡張する](#)」を参照してください。



重要 シンプロビジョニングが有効であり、全てのファイルシステムのファイルシステム拡張制限の合計が、HNAS に接続されているストレージの量を超えた場合、ストレージがオーバーサブスクリプションされたことを示す警告が発行されます。このような警告が発行されるのは、実際のストレージ容量が不足していて、全てのファイルシステムをそれぞれの拡張制限まで拡張できないためです。

(4) ファイルシステムの拡張を管理する

ファイルシステムの拡張管理のストラテジーを要約すると、次のようになります。

- 自動拡張は有効で、制限なし
 ファイルシステムは、サイズ制限を定義して作成され、ファイルシステムが作成される時には、実際にはそのスペースの一部だけが割り当てられます。ファイルシステムは、ファイルシステムをホストしているストレージプールが満杯になるまで（自動拡張は制限なし）、自動的に拡張されます（自動拡張が有効）。ただし、ファイルシステム拡張によって、ファイルシステムがファイルシステム内の最大許容チャンク数を超えない場合に限りです。
- 自動拡張は有効で、制限付き
 ファイルシステムは、サイズ制限を定義して作成され、ファイルシステムが作成される時には、実際にはそのスペースの一部だけが割り当てられます。ファイルシステムは、定義されたサイズ制限まで（自動拡張は制限付き）、自動的に拡張されます（自動拡張が有効）。ただし、使用可能なスペースがストレージプールにあり、ファイルシステム拡張によって、ファイルシステムがファイルシステム内の最大許容チャンク数を超えない場合に限りです。
- 自動拡張は無効
 ファイルシステムは指定されたサイズの全量で作成され、自動拡張は許されません（自動拡張は無効）。



重要 ファイルシステムのサイズを縮小することはできません。

次の表では、この三つのストラテジーについて説明します。

ファイルシステムの種類	自動拡張が有効	自動拡張が無効
非階層	<p>自動拡張が制限されない場合、サイズ制限は無視されます。ファイルシステムは、ストレージプールが満杯になるまで、拡張されます。</p> <p>自動拡張が制限付きの場合、サイズ制限によって、ファイルシステムの拡張が許される最大サイズが定義されます。</p> <p>ファイルシステムが作成される時、最初に一定量のスペースが割り当てられ（初期容量）、ファイルシステムはサイズ制限まで自動的に拡張されます。ファイルシステムが現在割り当てられているスペースの約 80%を使用すると、サイズ制限まで自動的に拡張されます。この拡張は、[guideline chunk size]（システムによって計算されます）で指定された増分単位で行われます。システムを手動で拡張して、ファイルシステムのサイズ制限を増やすことができます。</p>	<p>サイズ制限は、ファイルシステムにただちに割り当てられるスペースの量を定義します。</p> <p>ファイルシステムが作成される時には、[size limit] によって指定された全量が割り当てられます。</p> <p>システムを手動で拡張して、ファイルシステムのサイズ制限を増やすことができます。</p>
階層	<p>自動拡張が制限されない場合、サイズ制限は、定義されても無視されます。ファイルシステム階層は、ストレージプールが満杯になるまで拡張されます。</p> <p>自動拡張が制限付きの場合、サイズ制限によって、ファイルシステムの階層の拡張が許される最大サイズが定義されます。</p> <p>ファイルシステムが作成される時、ユーザーデータ階層には最初に一定量のスペースが割り当てられ（初期容量）、ユーザーデータ階層はサイズ制限まで自動的に拡張されます。ユーザーデータ階層が現在割り当てられているスペースの約 80%を使用すると、サイズ制限まで自動的に拡張されます。この拡張は、[guideline chunk size]（システムによって計算されます）で指定された増分単位で行われます。</p> <p>いずれの階層も手動で拡張して、ファイルシステムのサイズ制限を増やすことができます。</p>	<p>サイズ制限は、ユーザーデータ階層にただちに割り当てられるスペースの量を定義します。</p> <p>ファイルシステムが作成される時には、ユーザーデータ階層には、[size limit] によって指定された全量が割り当てられます。</p> <p>いずれの階層も手動で拡張して、ファイルシステムのサイズ制限を増やすことができます。</p>

デフォルト設定では、ファイルシステムの自動拡張は有効になっています。次に示す条件が存在する場合、自動拡張が有効であれば、ファイルシステムはサービスを停止することなく拡張できます。

- ファイルシステムの容量制限値に達していない（制限付き自動拡張を持つファイルシステムに限る）
ファイルシステムの拡張が、制限付き自動拡張の制限値を超えない。
- 使用可能なスペース
使用可能な未使用のスペースとチャンクがストレージプールに十分に残っている。
- チャンク制限
ファイルシステム拡張によって、ファイルシステムがファイルシステム内の最大許容チャンク数を超えない。
- サポートされるファイルシステムの最大サイズ
ファイルシステム拡張によって、ファイルシステムがサポートされる最大ファイルシステムサイズを超えない。

自動拡張が有効か無効かにかかわらず、非階層ファイルシステムのサイズ、または階層ファイルシステムの階層のサイズを制限できます。必要な場合は、非階層ファイルシステムのファイルシステムまたは階層ファイルシステムの階層を手動で拡張できます。



重要 ファイルシステムの自動拡張は、特定のストレージプールの全てのファイルシステムについて有効または無効にできません。ストレージプールの自動拡張が有効なときには、ファイルシステムの自動拡張はデフォルトで有効ですが、個々のファイルシステムについて無効にした場合は、再び有効にできません。ストレージプールのファイルシステム自動拡張が無効なときには、有効にすることはできません（ファイルシステムを手動で拡張する必要があります）。

(5) ファイルシステムの自動拡張を有効または無効にする

ストレージプールについてファイルシステムの自動拡張を有効または無効にする場合、ストレージプール内の一つのファイルシステムの設定を変更することはできません。ストレージプール内の全てのファイルシステムについて、ファイルシステム自動拡張を有効または無効にする必要があります。ストレージプール内の全てのファイルシステムについてファイルシステム自動拡張を有効にするには、「[ファイルシステムの自動拡張を制限する](#)」を参照してください。

ファイルシステム自動拡張が無効なとき、ファイルシステムの拡張が必要になったときには、ファイルシステムを手動で拡張する必要があります。ファイルシステムを手動で拡張するには、「[\(7\) ファイルシステムを手動で拡張する](#)」を参照してください。

ストレージプール内のファイルシステムの自動拡張は、ストレージプールレベルで有効または無効にされます。

- ストレージプールのファイルシステム自動拡張が有効なときには、ストレージプール内のファイルシステムの自動拡張を許可するか、指定したサイズ制限までに限定できます。ファイルシステム自動拡張は、各ファイルシステムについて個別に有効または無効にされます。
- ストレージプールのファイルシステム自動拡張が無効なときには、ストレージプール内のファイルシステムの自動拡張はできません。自動拡張が可能なように、ストレージプール内の個別のファイルシステムの設定を変更することはできません。

ファイルシステム自動拡張が無効な場合（ストレージプールレベルで、または個別のファイルシステムについて）、ファイルシステムの拡張が必要になったときは、ファイルシステムを手動で拡張する必要があります。

ファイルシステムを手動で拡張するには、「[\(7\) ファイルシステムを手動で拡張する](#)」を参照してください。ストレージプール内のファイルシステムについて自動拡張を有効または無効にするには、「[ファイルシステムの自動拡張を制限する](#)」を参照してください。

(6) ファイルシステムの自動拡張の制限を管理する

ファイルシステムの自動拡張を有効にすると、次のことができます。

- 非階層ファイルシステムまたは階層ファイルシステムの階層の最大サイズを制限できます。
- 非階層ファイルシステムまたは階層ファイルシステムの階層の最大サイズの制限を解除できます。

制限付き及び制限なしファイルシステム拡張の詳細については、「[\(4\) ファイルシステムの拡張を管理する](#)」を参照してください。ファイルシステムの制限設定の変更は、ファイルシステムをサービスから削除せずに行うことができます。

ファイルシステムの自動拡張を制限する

非階層ファイルシステムまたは階層ファイルシステムのユーザーデータ階層の最大サイズを制限するには

1. [File Systems] 画面に移動します。

[Home] 画面で, [Storage Management] セクションの [File Systems] をクリックして, [File Systems] 画面を表示します。ファイルシステムの一覧が表示されます。

2. 制限設定を変更するファイルシステムを選択します。
自動拡張を再び有効にするファイルシステムの [details] をクリックして, [File System Details] 画面を表示します。[File System Details] 画面の詳細については、「[1.2.7 ファイルシステムの詳細設定を表示する](#)」を参照してください。
3. 自動拡張の制限設定を定義します。
階層ファイルシステムの場合, 階層が特定のサイズを超えないようにするには, 次のようにします。
 - a. [Capacity] セクションを見つけます。
 - b. 制限する階層のそれぞれについて, 制限を追加します。
[Confine Auto-Expansion to] フィールドで, 階層のサイズ制限を指定します。
非階層ファイルシステムの場合, ファイルシステムが特定のサイズを超えないようにするには, 次のようにします。
 - a. [Auto-Expansion] セクションを見つけます。
 - b. 制限を追加します。
[Confine Auto-Expansion to] フィールドで, ファイルシステムのサイズ制限を指定します。
4. 変更を適用します。
設定が正しいことを確認し, [apply] をクリックして, 変更を保存します。

ファイルシステムの自動拡張の制限を解除する

非階層ファイルシステムまたは階層ファイルシステムの最大サイズの制限を削除するには

1. [File Systems] 画面に移動します。
[Home] 画面で, [Storage Management] セクションの [File Systems] をクリックして, [File Systems] 画面を表示します。ファイルシステムの一覧が表示されます。
2. 制限設定を変更するファイルシステムを選択します。
自動拡張を再び有効にするファイルシステムの [details] をクリックして, [File System Details] 画面を表示します。[File System Details] 画面の詳細については、「[1.2.7 ファイルシステムの詳細設定を表示する](#)」を参照してください。
3. 自動拡張の制限設定を削除します。
階層ファイルシステムの場合, 階層が特定のサイズに制限されないようにするには, 次のようにします。
 - a. [Capacity] セクションを見つけます。
 - b. 制限を削除する階層のそれぞれについて, 制限を削除します。
[Confine Auto-Expansion to] フィールドで, 階層について以前に定義したサイズ制限を削除します。
非階層ファイルシステムの場合, ファイルシステムが特定のサイズに制限されないようにするには, 次のようにします。
 - a. [Auto-Expansion] セクションを見つけます。
 - b. 制限を削除します。
4. 変更を適用します。
設定が正しいことを確認し, [apply] をクリックして, 変更を保存します。

(7) ファイルシステムを手動で拡張する

ファイルシステムの手動拡張は、Web Manager と CLI によってサポートされます。

ファイルシステムを手動で拡張するには

1. [File Systems] 画面に移動します。
[Home] 画面で、[Storage Management] セクションの [File Systems] をクリックして、[File Systems] 画面を表示します。ファイルシステムの一覧が表示されます。
2. 制限設定を変更するファイルシステムを選択します。
自動拡張を再び有効にするファイルシステムの [details] をクリックして、[File System Details] 画面を表示します。[File System Details] 画面の詳細については、「[1.2.7 ファイルシステムの詳細設定を表示する](#)」を参照してください。
3. [Expand File System] 画面に移動します。
[expand] をクリックして、[Expand File System] 画面を表示します。
 - 非階層ファイルシステムの場合、[Expand File System] 画面は次のようになります。

Storage Management | [Home](#) > [Storage Management](#) > [File Systems](#) > [File System](#) > Expand File System

Expand File System

Storage Pool: SP01
Free Capacity: 5.47 TB
Guideline Chunk Size: 25.21 GB

File System Label: test_manual
Current File System Capacity: 25.19 GB
New Capacity: GB [Rounded to nearest chunk](#)

[Home](#) | [About](#) | [Sign Out](#)

- 階層ファイルシステムの場合、[Expand File System] 画面は次のようになります。

Storage Management | [Home](#) > [Storage Management](#) > [File Systems](#) > [File System](#) > Expand File System

Expand File System

Storage Pool: SP02
Free Capacity: 2.10 TB
Guideline Chunk Size: 5 GB

File System Label: test_manual
Current File System Capacity: 9.97 GB

Expand Tier 0 Meta-data
Current Tier 0 Capacity: 4.99 GB
New Capacity: GB [Rounded to nearest chunk](#)

Expand Tier 1 User-data
Current Tier 1 Capacity: 4.99 GB
New Capacity: GB [Rounded to nearest chunk](#)

[Home](#) | [About](#) | [Sign Out](#)

4. 新しい容量を指定します。

[New Capacity] エディットボックスで、ファイルシステムの新しい容量を指定し、ドロップダウンリストを使用して、MB、GB、またはTBを選択します。

- 非階層ファイルシステムの場合、[New Capacity] フィールドで、ファイルシステムの新しい容量を指定し、ドロップダウンリストを使用して、MB、GB、またはTBを選択します。
- 階層ファイルシステムの場合、拡張する階層を選択し、[New Capacity] フィールドで、ファイルシステムの新しい容量を指定し、ドロップダウンリストを使用して、MB、GB、またはTBを選択します。



重要 1回の拡張操作で一つの階層を拡張できます。両方の階層を拡張するには、手動拡張を2回行う必要があります。

5. プロセスを開始します。

[OK] をクリックして、ファイルシステムまたは階層を拡張します。または、変更せずに [File System Details] 画面に戻るには、[cancel] をクリックします。



重要 スペースは常に、ファイルシステムを含んでいるストレージプールが作成されたときに設定されたチャンクサイズの倍数で割り当てられるので、ファイルシステムの最終的なサイズは、要求したものよりもわずかに大きくなる場合があります。

ファイルシステムの手動拡張は、CLI でもサポートされます。このプロセスの詳細については、CLI で `man filesystem-expand` を実行してください。

1.2.9 仮想ボリューム

ファイルシステムを、仮想ボリュームと呼ばれる、ストレージの個別の領域に分割することができます。クライアント側からは、仮想ボリュームは通常のファイルシステムに見えます。仮想ボリュームは、プロジェクト、ユーザー、またはグループ用のディレクトリを割り当てて制御するための簡単な手段となります。仮想ボリューム内の容量とファイル数は、**Quota** を使用して制御できます。



重要 このセクションでは、「ユーザー」と「グループ」という用語は、NFS または CIFS ユーザーとグループを指します。

仮想ボリュームには次のような特性があります。

- 名前
仮想ボリュームを識別する名前です。これは、しばしば、仮想ボリュームのルートディレクトリにある CIFS 共有または NFS 共有と同じです。
- ファイルシステム
仮想ボリュームが作成されるファイルシステム。
- パス
仮想ボリュームのルートディレクトリ。
- メール連絡先
仮想ボリュームのアクティビティに関する情報とアラートが送信されるメールアドレスのリスト。リストを使用して、個々のユーザーにメールを送信することもできます。
- ファイルの移動
仮想ボリュームへ、または仮想ボリュームからファイルを移動できます。
- ディレクトリの移動
仮想ボリュームへ、または仮想ボリュームからディレクトリを移動すると、クロスボリュームリンクエラーが返されますが、ほとんどの CIFS または NFS クライアントは、このエラーを抑制

して、代わりに、ディレクトリを移動先の場所へコピーしてから、元のディレクトリを削除します。

- ファイルのリンク（ハードリンク）
異なる仮想ボリューム間でファイルをリンクすることはできません。

仮想ボリュームと Quota に関する重要な情報

HNAS は、仮想ボリュームのルートディレクトリとそのサブディレクトリの全てを自己完結型ファイルシステムとして扱います。仮想ボリュームはスペースの使用量とファイル数を追跡して、ファイルシステム使用量を監視する手段となります。この追跡によって、ディスクスペース使用量と合計ファイル数に Quota を課することができます。

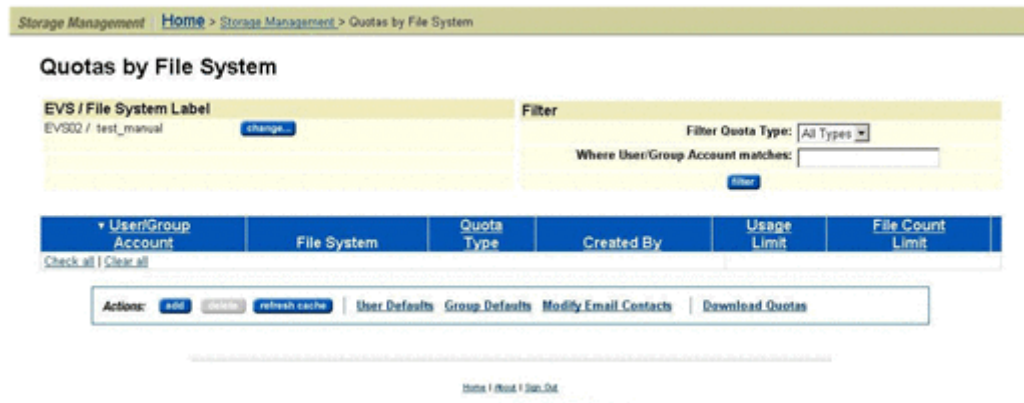
Quota は、仮想ボリューム全体、個々のユーザー、及びユーザーグループに対して設定できます。デフォルトのユーザー及びグループ Quota を定義でき、明示的なユーザーまたはグループ Quota がない場合は、デフォルトの Quota が適用されます。

Quota のしきい値に対する仮想ボリュームステータスの測定には、次の注意事項が適用されます。

- メタデータとスナップショットファイル
ファイルシステムのメタデータもスナップショットファイルも、Quota 制限の対象にはなりません。
- シンボリックリンクの計算
複数のハードリンクが指しているファイルは、Quota 計算に一度だけ含まれます。シンボリックリンクは、リンク先のファイルのサイズではなく、仮想ボリュームへのシンボリックリンクファイルのサイズを追加します。

1.2.10 使用量 Quota を管理する

使用量 Quota を表示するには、[Storage Management] 画面に移動して [Quotas by File System] をクリックし、以下の画面を表示します。



この画面には、選択したファイルシステムの使用量 Quota が一覧表示されます。

- 任意の列で昇順または降順に並べ替えるには、列のヘッダーをクリックします。
- さまざまな Quota を表示するには、[change...] をクリックして、別のファイルシステムを選択します。

次の表では、この画面のフィールドについて説明します。

項目	説明
EVS/File System Label	選択された EVS 及びファイルシステムの名前です。別のファイルシステムを選択するには、[change...] をクリックします。

項目	説明
Filter	この画面に表示されている Quota または仮想ボリュームの数を減らすために定義できます。指定したフィルター基準に基づいて Quota を一覧表示するには、[filter] をクリックします。
User/Group Account	Quota 名は、以下で構成されている場合があります。 <ul style="list-style-type: none"> CIFS ドメインと、ユーザー名またはグループ名 例：bb¥Smith, bb¥my_group (この場合、「bb」がドメイン、「Smith」がユーザー、「my_group」がグループ。) NFS ユーザーまたはグループ 例：richardb, finance (この場合、「richardb」が NFS ユーザーで、「finance」が NFS グループ。) 名前には、「0」のこともあります (Quota が、仮想ボリュームのルートで、ディレクトリの所有者に対して作成された場合)。
File System	Quota が適用されるファイルシステムです。
Quota Type	ファイルシステムのアクティビティの種類です。使用可能な値は、User, Group, または Virtual Volume です。仮想ボリュームは、仮想ボリューム全体でアクティビティを開始する任意のユーザーに適用されます。各仮想ボリュームには、このターゲットの種類を持つ Quota が一つしか存在しない場合があります。
Created By	Quota の作成方法です。使用可能な値は、Automatically Created (Quota デフォルトを使って作成)、または User Defined (特定の Quota に対して、Quota を一意に設定) です。
Usage Limit	Quota のターゲットが所有するファイルシステム内で、全ファイルの合計サイズに設定されている総合限度です。
File Count Limit	Quota のターゲットが所有するファイルシステム内で、ファイルの合計数に設定されている総合限度です。
Actions	[details] を使って、選択された Quota の詳細を編集できます。 [add] をクリックすると、Quota を追加できます。 Quota (または選択した複数の Quota) を削除するには、チェックボックスをオンにして、[delete] をクリックします。 [Delete All Quotas] で、仮想ボリュームの現在の Quota 全てを削除します。 [refresh cache] で、SMU のキャッシュを消去し、関連オブジェクトを使って再作成します。(これは、ブラウザの更新ボタンをクリックして、キャッシュを消去せずに最近の更新を取得することとは異なります。) [User Defaults] で、ユーザーデフォルトを設定、編集、またはリセットできます。 [Group Defaults] で、グループデフォルトを設定、編集、またはリセットできます。 [Modify Email Contacts] で、Quota に達した場合に通知を受け取る連絡先のリストを編集できます。 [Download Quotas] (ファイルシステムの Quota 以外) : この仮想ボリュームの Quota は、.csv ファイルとしてダウンロードできます。

(1) ファイルシステムのユーザー Quota 及びグループ Quota のデフォルトを設定するには

[Quotas by File System] 画面で [User Defaults] (または [Group Defaults]) をクリックして、[User File System Quota Defaults] (または [Group File System Quota Defaults]) 画面を表示します (下の図は、[User Defaults] 画面です)。

Storage Management Home > Storage Management > Quotas by File System > User File System Quota Defaults

User File System Quota Defaults

EVS / File System: EVSD01 / vol0 [change...](#)

Usage	File Count
Limit: <input type="text"/> GB	Limit: <input type="text"/>
Hard Limit: <input checked="" type="checkbox"/>	Hard Limit: <input checked="" type="checkbox"/>
Warning: <input type="text"/> %	Warning: <input type="text"/> %
Severe: <input type="text"/> %	Severe: <input type="text"/> %

Log Quota Events in the managed server's EventLog

[OK](#) [clear defaults](#) [cancel](#)



重要 [Group File System Quota Defaults] 画面は、[User File System Quota Defaults] 画面と同様ですが、チェックボックス [Automatically create quotas for Domain Users] が追加されています。このチェックボックスをオンにすることで、「Domain Users」グループのデフォルト Quota を作成できます。デフォルトで、各 NT ユーザーは、「Domain Users」グループに属しています。そのため、このオプションを有効にすると、全ての NT ユーザーを効率よく Quota に含めることができます。ただし、各ユーザーのプライマリグループが既に明示的に設定されている場合を除きます。

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS/File System	ユーザーファイルシステムの Quota が適用される、EVS 及びファイルシステムです。
Usage	このセクションには、使用量に関する現在の Quota 設定が表示されます。
Limit	使用可能な空き容量を、バイト単位 (KB, MB, GB, または TB) で示します。
Hard Limit	選択した場合、[Limit] フィールドで指定した空き容量を超過できません。
Warning	[Limit] フィールドに指定した空き容量の割合になった時点で、[Warning] アラートが発信されます。
Severe	[Limit] フィールドに指定した空き容量の割合になった時点で、[Severe] アラートが発信されます。
File Count	このセクションには、ファイル数に関する現在の Quota 設定が表示されます。
Limit	この Quota に対して有効にする最大ファイル数を入力します。
Hard Limit	選択した場合、[Limit] フィールドで指定したファイル数を超過できません。
Warning	[Limit] フィールドに指定したファイル数の割合になった時点で、[Warning] アラートが発信されます。
Severe	[Limit] フィールドに指定したファイル数の割合になった時点で、[Severe] アラートが発信されます。
Log Quota Events in the managed server's Event Log	このチェックボックスをオンにすると、Quota イベントがノードのイベントログに記録されるようになります。



重要 フィールドが 0 (または空欄) になっている場合、その入力は「未設定」とみなされます。

全ての必須フィールドに入力し終わったら、[OK] をクリックします。



重要 ユーザーデフォルトを消去して、ファイルシステムに、その他の Quota デフォルトが作成されないようにするには、[clear defaults] をクリックします。これで、既存の「Automatically Created」のユーザー Quota が、「User Defined」のユーザー Quota に変換されます。

(2) ファイルシステムの Quota を追加する

[Quotas by File System] 画面で [add] をクリックして、[Add File System Quota] 画面を表示します。

Add File System Quota

EVS / File System: EVS02 / test_manual [change...](#)

Quota Type: User User Account i.e. domain/user (CIFS) or user (NFS)
 Group Group Account i.e. domain/group (CIFS) or group (NFS)

Usage	File Count
Limit: <input type="text"/> GB	Limit: <input type="text"/>
Hard Limit: <input type="checkbox"/>	Hard Limit: <input type="checkbox"/>
Warning: <input type="text"/> 75 %	Warning: <input type="text"/> 75 %
Severe: <input type="text"/> 85 %	Severe: <input type="text"/> 85 %

Log Quota Events in the managed server's Event Log

[OK](#) [cancel](#)

[Home](#) | [About](#) | [Sign Out](#)

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS/File System	Quota が適用されるファイルシステムです。
Quota Type	仮想ボリュームのアクティビティのソースの種類です。使用可能な値は、User、Group、及び Virtual Volume です。 仮想ボリュームは、仮想ボリューム全体でアクティビティを開始する任意のユーザーに適用されます。各仮想ボリュームには、このターゲットの種類を持つ Quota が一つしか存在しない場合があります。
User/Group Account	Quota 名は、以下で構成されている場合があります。 <ul style="list-style-type: none"> CIFS ドメインと、ユーザー名またはグループ名 例：bb¥Smith, bb¥my_group (この場合、「bb」がドメイン、「Smith」がユーザー、「my_group」がグループです。) NFS ユーザーまたはグループ 例：richardb, finance などです (この場合、「richardb」が NFS ユーザーで、「finance」が NFS グループです。) 名前前は、空欄または「0」にできます。空欄は仮想ボリュームの Quota の場合、「0」は仮想ボリュームのルートでディレクトリの所有者に対して作成された場合です。
Usage	
Limit	使用可能な空き容量を、バイト単位 (KB, MB, GB, または TB) で示します。
Hard Limit	選択すると、[Limit] フィールドで指定した空き容量を超過できません。
Warning	[Limit] フィールドに指定した空き容量の割合になった時点で、[Warning] アラートが発信されます。
Severe	[Limit] フィールドに指定した空き容量の割合になった時点で、[Severe] アラートが発信されます。
File Count	
Limit	この Quota に対して有効にする最大ファイル数を入力します。
Hard Limit	選択した場合、[Limit] フィールドで指定したファイル数を超過できません。
Warning	[Limit] フィールドに指定したファイル数になった時点で、[Warning] アラートが発信されるようになります。
Severe	[Limit] フィールドに指定したファイル数になった時点で、[Severe] アラートが発信されるようになります。
Log Quota Events in the managed server's Event Log	このチェックボックスをオンにすると、Quota イベントがノードのイベントログに記録されるようになります。



重要 フィールドが 0 (または空欄) になっている場合、その入力は「未設定」とみなされます。

全ての必須フィールドに入力したら、[OK] をクリックします。

(3) ファイルシステムの Quota を変更する

[Quotas by File System] 画面で、変更する Quota の [details] をクリックします。

この画面の詳細も、前の画面と同じです。追加されているチェックボックス [Automatically create quotas for Domain Users] を使用して、「Domain Users」グループのデフォルトの Quota を作成できます。デフォルトで、各 NT ユーザーは「Domain Users」グループに属しています。そのため、このオプションを有効にすると、全ての NT ユーザーを効率よく Quota に含めることができます。ただし、各ユーザーのプライマリグループが既に明確に設定されている場合を除きます。全ての必須フィールドに入力したら、[OK] をクリックします。

(4) ファイルシステムの Quota を削除する

[Quotas by File System] 画面で Quota を選択し、[delete] をクリックします。

1.2.11 ファイルシステムを移動する

性能の向上や負荷の分散のため、データを別のストレージリソースに移動するため、ネットワークトポロジーの変更に対応するため、またはその他の理由で、(一つまたは複数の) ファイルシステムの移動が必要になることがあります。

ファイルシステムを移動するには、基本的に二つの方法があります。

- ファイルシステムの再配置

ファイルシステムの再配置は、ファイルシステムをホストする EVS (Virtual Server) を変更しますが、ファイルシステムデータは移動しません。ファイルシステムを別の EVS に移動すると、ファイルシステムへのアクセスに使用される IP アドレスが変更され、そのファイルシステムの CIFS 共有と NFS 共有も変更されます。ファイルシステム再配置を使用してファイルシステムを再配置する方法については、『*Replication and Disaster Recovery Administration Guide*』を参照してください。

再配置されるファイルシステムが CNS 内からリンクされていて、クライアントが CIFS 共有または NFS 共有を使用して CNS にアクセスする場合、ネットワーククライアントの構成を変更せずに再配置を実行できます。この場合、クライアントは、再配置後も、再配置が開始される前と同じ IP アドレスと CIFS 共有/NFS 共有名でファイルシステムにアクセスできます。CNS の詳細については、『*Server and Cluster Administration Guide*』を参照してください。



注意 ファイルシステムが CNS にあるかどうかにかかわらず、ファイルシステムを再配置すると、CIFS と HNAS の通信は中断されます。Windows クライアントがファイルシステムへのアクセスを必要とする場合、ファイルシステムの再配置は、CIFS アクセスを中断できる時間帯にスケジュールしてください。

- プライマリアクセスの転送

プライマリアクセスの転送は、ファイルシステムの一部 (またはファイルシステム全体) からデータをコピーして、そのデータのアクセスポイントを再配置する (データとメタデータをコピーする) レプリケーションベースの方法です。プライマリアクセスの転送によるダウンタイムはほとんどなく、再配置プロセスの大部分の時間、ファイルシステムはライブであり、ファイル読み取り要求を処理し続けます。再配置プロセス中の短時間、アクセスは読み取り専用で制限されます。プライマリアクセスの転送を使用したファイルシステムの再配置の詳細については、『*Replication and Disaster Recovery Administration Guide*』を参照してください。

ファイルシステムを再配置するために使用する方法は、移動する対象とファイルシステムの再配置の目的に、ある程度、依存します。

- ファイルシステムのアクセスポイントは移動させたいが、実際のデータは移動させたくない場合、ファイルシステム再配置を使用するのが最適の方法です。
- ファイルシステムのデータとアクセスポイントを移動する場合には、プライマリアクセスの転送が最適の方法です。

(1) ファイルシステムの再配置

ファイルシステムを共有またはエクスポートするには、まず、ファイルシステムを **Virtual Server (EVS)** に関連付けて、ネットワーククライアントからアクセスできるようにする必要があります。ファイルシステムと **EVS** との関連付けは、ファイルシステムが作成される時に確立されます。時間の経過と共に、ストレージリソースの使用パターンや要件が変化して、ファイルシステムを別の **EVS** に再配置した方がよくなる場合があります。



重要 リードキャッシュを再配置することはできません。

クラスタノード上の **EVS** によってホストされるファイルシステムは、次の場所へ再配置できます。

- 同じクラスタノード上の **EVS**
- 同じクラスタ内の別のノード上の **EVS**

しかし、次の場所へ再配置することはできません。

- 別のクラスタのノード上の **EVS**

一般に、ファイルシステム再配置は、クラスタノード上の **EVS** から同じクラスタ内の別のノード上の **EVS** へファイルシステムを移動して、クラスタノード間の負荷を均衡させることにより、スループットを高めるために使用されます。

ファイルシステム再配置は、次の操作を実行します。

- 選択された **EVS** にファイルシステムを再び関連付けます。
- ファイルシステムの明示的 **CIFS** 共有を新しい **EVS** に転送します。
- ファイルシステムの明示的 **NFS** 共有を新しい **EVS** に転送します。
- **FTP** ユーザーを新しい **EVS** に移行します。
- ファイルシステムに関連付けられているスナップショットルールを新しい **EVS** に移行します。
- **iSCSI** 論理ユニット及びターゲットを移行します。

ファイルシステム再配置では、指定されたファイルシステムだけでなく、それ以上のものを再配置しなければならない場合があります。ファイルシステムがデータ移行パスに含まれている場合、データ移行元のファイルシステムと移行先のファイルシステムの両方が再配置されます。データ移行パスの移行先は、複数の移行元ファイルシステムの移行先にできます。データ移行先が再配置される場合、関連付けられた全ての移行元ファイルシステムも再配置されます。

複数のファイルシステムを再配置する必要がある場合、移動しなければならない追加のファイルシステムを示す確認ダイアログが表示されます。再配置を実行する前に、明示的に確認する必要があります。

ファイルシステム再配置は、次のような状況でネットワーククライアントがファイルシステムにアクセスする方法に影響を与えます。

- ファイルシステムは **CNS** ツリーからリンクされますが、**CNS** のコンテキストの外部で共有またはエクスポートされます。
- クラスタは **CNS** を使用しません。

上記の場合、共有とエクスポートへのアクセスは変更されます。再配置後に共有及びエクスポートにアクセスするためには、新しい EVS の IP アドレスを使用して、ファイルサービスにアクセスします。

iSCSI 論理ユニット (LU) を含むファイルシステムを再配置すると、接続されたイニシエーターへのサービスは中断され、再配置の完了後に、移行先にアクセスするための IP アドレスの手動再構成が必要になります。LU を含むファイルシステムの再配置が必要な場合、次のステップを実行する必要があります。

- ・ 再配置されるファイルシステム上の LU に接続している iSCSI イニシエーターを切断します。
- ・ iSCSI 論理ユニットをアンマウントします。
- ・ ファイルシステムを通常どおりに再配置します。この手順については、『*Replication and Disaster Recovery Administration Guide*』で詳しく説明しています。
- ・ 新しい移行先を iSCSI イニシエーターに再接続します。移行先は、新しい EVS に対応する新しい名前参照されます。



重要 移行先の全ての iSCSI 論理ユニットは、同じ EVS によってホストされるファイルシステムに関連付ける必要があります。

1.2.12 ファイルシステムでシステムロックを使用する

システムロックモードは、再配置とプライマリアクセスの転送の操作時にファイルシステムを保護します。四つの重要な区別が適用されます。

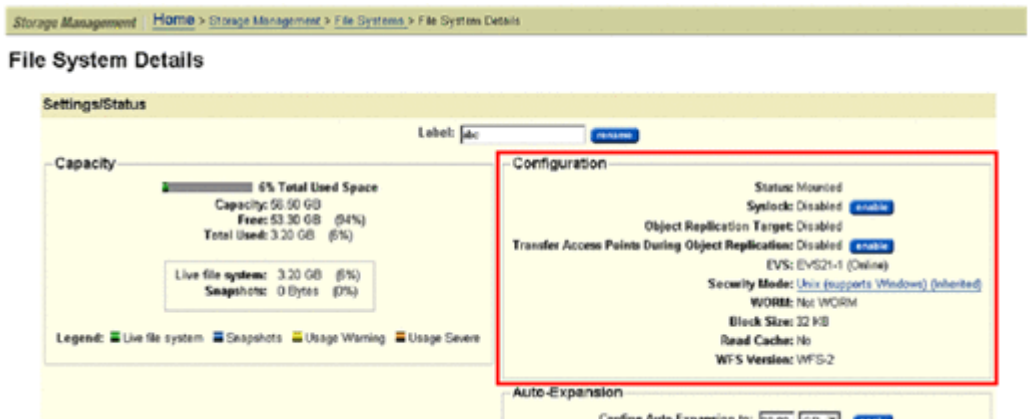
- ・ NDMP (Network Data Management Protocol) 対ファイルサービスプロトコル
ファイルシステムのシステムロックが有効なとき
 - NDMP は、バックアップ、レプリケーション、及びプライマリアクセスの転送時はフルアクセス (書き込みアクセスを含む) を持ちます。
 - ファイルサービスプロトコル (NFS, CIFS, FTP, 及び iSCSI) を使用しているクライアントにとっては、ファイルシステムは読み取り専用モードのままです。
- ・ システムロック対読み取り専用
 - ファイルシステムが Syslock されているときでも、NDMP はそのファイルシステムに対するフルアクセスを持ち、書き込むことができます。
 - ファイルシステムが読み取り専用としてマウントされているとき、NDMP は (他の全てのプロトコルと同様に) そのファイルシステムへの読み取り専用アクセスしか持たず、書き込むことはできません。ファイルシステムが完全に変更されないままであることを確実にするには、読み取り専用としてマウントしてください。
- ・ レプリケーション対プライマリアクセスの転送
 - レプリケーション操作時、複製先のファイルシステムはシステムロックモードになります。
 - プライマリアクセスの転送操作時、転送元ファイルシステムと転送先ファイルシステムの両方がシステムロックモードになります。
- ・ リードキャッシュの例外
リードキャッシュをシステムロックモードにすることはできません。

(1) ファイルシステムのシステムロックを有効または無効にする

ファイルシステムのシステムロックを有効または無効にするには

1. [File System Details] 画面に移動します。

[Home] 画面で [Storage Management] をクリックし、[File Systems] リンクをクリックして、[File Systems] 画面を表示します。次に、ファイルシステムを選択して、[details] をクリックし、[File System Details] 画面を表示します。



2. システムロックを有効または無効にします。

赤い枠で囲まれたセクションの [Syslock] フィールドで、[enable] または [disable] ボタンを選択します。

ファイルシステムがシステムロックモードのときには、[Status] が [Syslocked] に変わり、[Syslock] が [Enabled] に変わり、[enable] ボタンは [disable] になります。

ファイルシステムのシステムロックが有効などときには、NDMP はファイルシステムへのフルアクセスを持ち、バックアップまたはレプリケーション時にファイルシステムに書き込むことができますが、ファイルサービスプロトコル (NFS, CIFS, FTP, 及び iSCSI) を使用しているクライアントに対しては、ファイルシステムは読み取り専用モードです。

リードキャッシュの詳細を表示しているときには、システムロックの [enable] 及び [disable] ボタンは使用できません。

1.2.13 ファイルシステムをリカバリーする

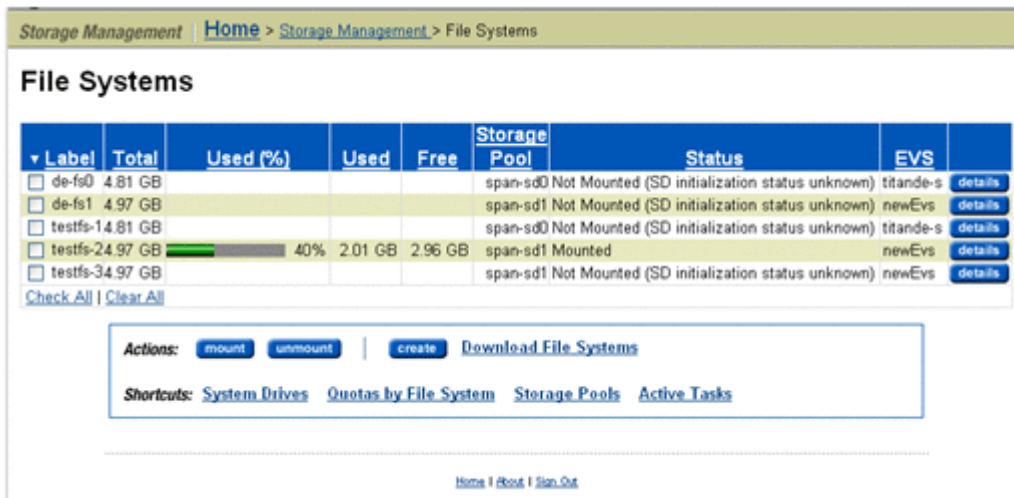
何らかのシステム障害の後、ファイルシステムをマウントする前にリカバリーが必要なことがあります。必要な場合、そのようなリカバリーは、ファイルシステムをマウントしたときに自動的行われます。リカバリーを実行すると、ファイルシステムは最後のチェックポイントにロールバックされ、NVRAM 内のデータが再生されます。

ごくまれに、システム障害後にファイルシステムをマウントするとき、ファイルシステムをリカバリーするには、自動のリカバリー手順では不十分なことがあります。そのような場合、ファイルシステムを強制的にマウントする必要があります。これにより、NVRAM のデータは、ファイルシステムをマウントする前に廃棄されます。

ファイルシステムをリカバリーするには

1. [File Systems] 画面に移動します。

[Storage Management] 画面で [File Systems] をクリックして、[File Systems] 画面を表示します。

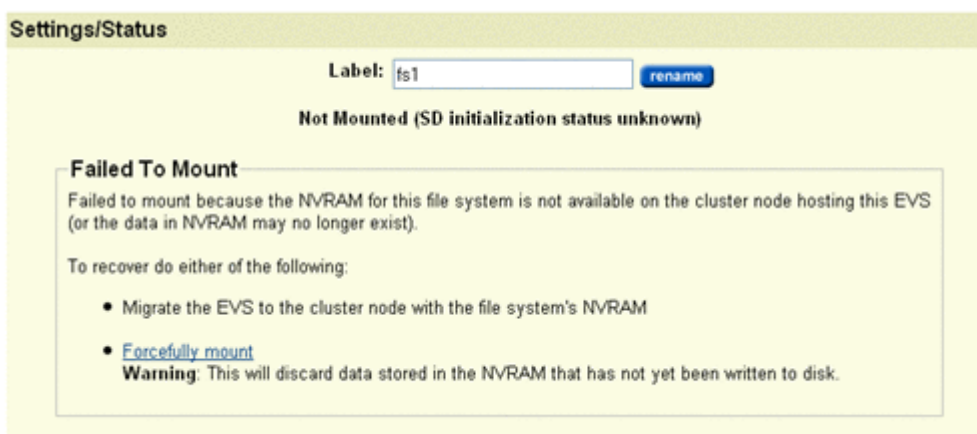


2. ファイルシステムをマウントします。

[Status] 列に「Not Mounted」と表示されている場合は、[mount] をクリックして、ファイルシステムのマウントを試みます。

必要に応じて、自動リカバリープロセスが自動的に呼び出されます。自動リカバリーが失敗した場合、ファイルシステムはマウントされず、[File Systems] 画面が再び表示されて、ファイルシステムがマウントされなかったことを示します。

3. マウントが失敗したファイルシステムについては、[File System Details] 画面に移動します。マウントが失敗したファイルシステムについては、[details] をクリックして、[File System Details] 画面を表示します。[Settings/Status] エリアに、そのファイルシステムの名前の他、マウントが失敗した理由（わかる場合）と、[Forcefully mount] オプションのリンクなどファイルシステムをリカバリーするためのヒントが表示されます。



4. リカバリーを開始します。

システムの構成と、マウントが失敗した理由によって、いくつかのリカバリーオプションがあります。

- 割り当てた EVS を別のクラスタノードに移行してから、ファイルシステムのマウントを試みることができます。これは、クラスタ内の別のノードに、最後のチェックポイント後のファイルシステムへの書き込みトランザクションを再生するために必要な NVRAM 内の現在使用可能なデータがある場合に必要になることがあります。EVS は、失敗したノードの NVRAM をミラーするクラスタノードに移行してください。NVRAM ミラーリングの詳細については『*System Administration Overview*』を参照してください。EVS のマイグレーションの詳細については、『*Server and Cluster Administration Guide*』を参照してください。

- 最初のリカバリーの試みが失敗した場合は、[Forcefully mount] リンクをクリックしてください。これは、NVRAM の内容を再生せずに、ファイルシステムのリカバリーを実行します。



注意 [Forcefully mount] オプションを使用すると、NVRAM のデータ（既にクライアントに確認応答された可能性があるデータ）が破棄されます。NVRAM のデータの破棄は、NVRAM の全ての書き込み操作（まだディスクにコミットされていない書き込み操作）が失われることを意味します。その場合、クライアントは、書き込み要求を再送信する必要があります。[Forcefully mount] オプションは、お問い合わせ先から推奨された場合にのみ使用してください。

(1) ファイルシステムをリカバリーする

ストレージシステムの障害後、ファイルシステムのリカバリーが必要になることがあります。WFS-2 ファイルシステムは、WFS-1 システムよりも、ストレージシステム障害後のファイルシステムの復旧力が高いです。WFS-2 を使用してフォーマットされたファイルシステムは、冗長なメタデータ構造が基盤になっているため、チェックポイントまたはスナップショットから復元できます。WFS-1 を使用してフォーマットされたファイルシステムは、冗長なメタデータ構造を持たないため、チェックポイントまたはスナップショットから復元できません。

チェックポイントからファイルシステムを復元する（WFS-2 のみ）

イベント（RAID コントローラーのクラッシュ、ストレージシステムコンポーネントの障害、停電など）によるファイルシステムの破損は、しばしば、イベントの発生時前後に変更中だったオブジェクトに影響を与えます。

WFS-2 は、一つのファイルシステムに対して複数のチェックポイントを保存します。デフォルトでは、WFS-2 ファイルシステムは、最大 128 のチェックポイントを維持するように構成されます。サポートされる最大チェックポイント数は 1,024 です。保存されるチェックポイントの数は、ファイルシステムのフォーマット時に構成できますが、設定後にチェックポイント数を変更することはできません。

チェックポイントが完了すると、以前のチェックポイントに使用されていたストレージがただちに解放されるのではなく、WFS-2 は複数の古いチェックポイントを維持します。新しいチェックポイントが完了するたびに、最も古いチェックポイントが上書きされます。これは、ディスク上に複数のチェックポイントがあり、それぞれが完全かつ内部的に一貫した、特定時点でのファイルシステムのビューであることを意味します。必要な場合は、これらのいずれかのチェックポイントにファイルシステムを復元できます。

ファイルシステムが破損した場合、ディスク上に十分なチェックポイントがあれば、破損の原因となったイベントより前のチェックポイントへロールバックして、破損していないチェックポイントを使用してファイルシステムを復元することができます。そのイベントがファイルシステムがオフラインになる数分前に発生した場合でも、復元できる場合があります。

ファイルシステムを前のチェックポイントに復元するには、`fs-checkpoint-health` 及び `fs-checkpoint-select` コマンドを使用します。これらのコマンドの詳細については、『*Command Line Reference*』を参照してください。

次のことに注意してください。

- ・ チェックポイントを使用してファイルシステムを復元した場合、復元されるチェックポイントより前に作成されたスナップショットは影響を受けませんが、他のファイルシステムの更新と同様に、そのチェックポイント後に取られたスナップショットは失われます。
- ・ あるチェックポイントに復元した後、さらに古いチェックポイントに再び復元することができ、ファイルシステムが変更されていなかった場合は、より最近のチェックポイントに再び復元できます。したがって、例えば、ファイルシステムを読み取り専用モードでマウントしてから、ファイルシステムを通常（読み取り／書き込み）モードで再マウントするか、別のチェックポイントに復元するかを決めることができます。



注意 復元したファイルシステムを通常 (読み取り/書き込み) モードでマウントした場合、それより後のチェックポイントに復元することはできません。

スナップショットからファイルシステムをリカバリーする (WFS-2 のみ)

ライブファイルシステムが破損しても、良好なスナップショットが存在する可能性があります。その場合、ライブファイルシステムの修復でダウンタイムを発生させるより、データの一部が失われたとしても、このスナップショットからファイルシステムをリカバリーした方がよいかもかもしれません。スナップショットからファイルシステムをリカバリーすると、ファイルシステムはスナップショットが作成された時点の状態に復元されます。

スナップショットからファイルシステムをリカバリーすると、ファイルシステムをスナップショットが作成された時点の状態にロールバックできます。

スナップショットからのファイルシステムのリカバリーはライセンスが必要な機能であり、クラスタ上に有効な FSRFS ライセンスが必要です。



重要 スナップショットからファイルシステムをリカバリーできるのは、そのスナップショットが作成されてから、少なくとも構成された数のファイルシステムチェックポイントが維持されている場合に限られます。例えば、ファイルシステムが 128 (デフォルト) のチェックポイントを維持するように構成されていた場合、スナップショット後に少なくとも 128 のチェックポイントが作成された後でのみ、スナップショットからファイルシステムをリカバリーできます。スナップショット後に作成されたチェックポイントの数が構成された数より少ない場合は、より古いスナップショットからリカバリーするか、チェックポイントからファイルシステムをリカバリーできます (『[チェックポイントからファイルシステムを復元する \(WFS-2 のみ\)](#)』を参照してください)。

次のファイルシステムロールバックに関する注意事項が適用されます。

- ファイルシステムのロールバックは、ライブファイルシステムが破損した場合でも実行できます。
- ロールバック後は、全てのスナップショットが失われます。
- ファイルシステムのリカバリーにはごく短い時間しかかからなかったとしても、以前のスナップショットが全て破棄されるまで、新しいスナップショットを作成することはできません。新しいスナップショットを作成できるようになるまでの時間は、ファイルシステム内のファイル数ではなく、ファイルシステムのサイズに依存します。



重要 ファイルシステムをスナップショットからリカバリーして、読み取り/書き込みモードでマウントすると、再度リカバリーしたり、別のスナップショットまたはチェックポイントへもう一度リカバリーしたりすることはできません。

スナップショットからファイルシステムをロールバックするには、`snapshot-recover-fs` コマンドを使用します。このコマンドの詳細については、『[Command Line Reference](#)』を参照してください。

ファイルシステムの自動リカバリー (WFS-1 及び WFS-2)

ファイルシステムリカバリーのための CLI は、WFS-2 ファイルシステムに対応しています。fixfs ユーティリティは、WFS-1 及び WFS-2 ファイルシステム用の主要なファイルシステムリカバリーツールですが、お問い合わせ先の担当者の監督下でのみ使用してください。その他のツールとして、現在の全てのスナップショットを kill する `kill-snapshots` コマンドも使用できます (このコマンドの詳細については、『[Command Line Reference](#)』を参照してください)。

fixfs は、オーファンリカバリーなどを実行して、重要でない一定量のメタデータを修復できます。fixfs では、数分以上かかるステージでは進捗状況を報告して、修復を中止するオプションを提供します。進捗状況の報告は、ステージまたは操作単位であり、例えば、7 ステージのうちの 3 ステージが完了したことが報告されます。一部の操作では、fixfs は、操作完了までの推計時間も表示します。

fixfs がファイルシステムを修復するために使用するストラテジーを要約すると、次のようになります。

- fixfs は、ファイルシステムが破損した場合に使用される唯一のリカバリーツールです。さまざまなコマンドラインスイッチによって fixfs のデフォルトの動作を変更できますが、必要なスイッチは、しばしば、実行中または前回の実行の終了時に fixfs によって提案されます。
- 可能な場合、fixfs は、どんな状態のファイルシステムでも実行します（はじめにファイルシステムのリカバリーを実行する必要がないので、破損のためにリカバリーを完了できない場合に何が起これるのかを心配する必要もありません）。可能でない場合（例えば、ファイルシステムが既にマウントされている場合や、「failed」または「requires expansion」としてマークされている場合）、fixfs は実行しません。fixfs が実行しない場合には、実行するために必要な操作が明確に表示されます。
- デフォルトでは、fixfs は、失われたか破損したオブジェクトのみを変更します。
- デフォルトでは、fixfs は、ファイルシステムをマウントできる状態にするだけです。
- スナップショットは不要とみなされて、削除されます。

1.3 WORM ファイルシステムを使用する

ファイルシステムは、作成時に WORM に指定されています。WORM ファイルを作成する場合は、保持ポリシーをテストするために、厳密でない（non-strict）WORM ファイルシステムから始めます。その後、コンプライアンスソリューションを展開する準備が整ったら、厳密な（strict）WORM ファイルシステムを作成します。詳細については、「1.2.2 ファイルシステムを作成する」を参照してください。



重要 WORM 以外の既存ファイルシステムは、WORM ファイルシステムとして再フォーマットできます。種類の異なるファイルシステムを使うためには、ファイルシステムの再フォーマットを、CLI で行う必要があります。このプロセスの詳細については、`man format` を実行してください。

1.3.1 保持期限を指定する

ファイルに WORM のマークを付ける前に、ファイルの保持期限を指定します。保持期限を設定するには、ファイルの「last access time」を将来の特定日時に設定します。「last access time」は、Unix の `touch` コマンドを使ってセットできます。以下は、その例です。

```
touch -a -t YYYYMMDDhhmm ./filename
```

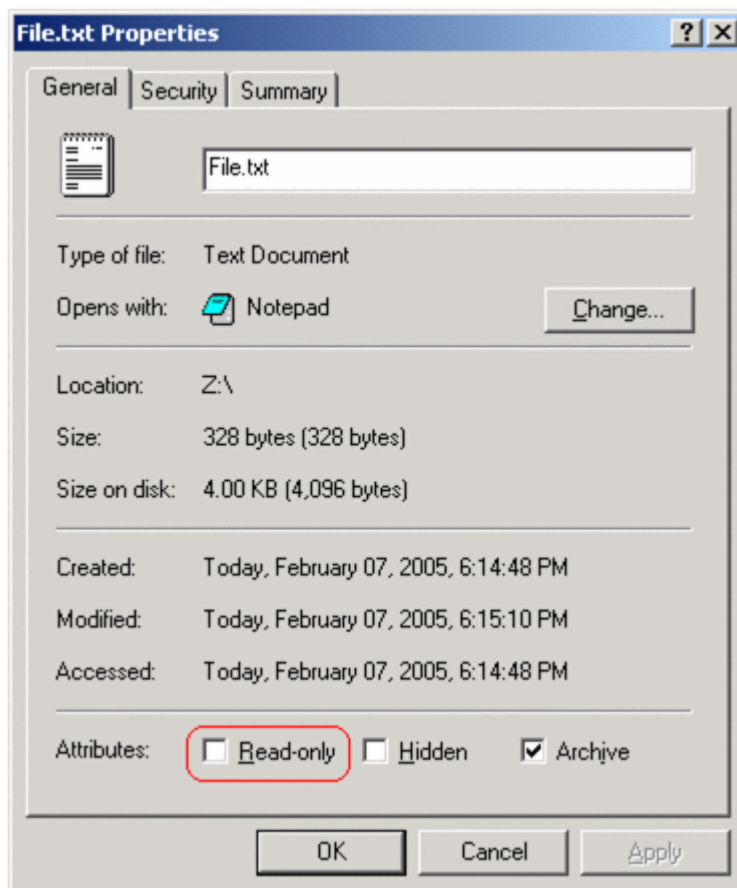
保持期限の日時を現在の時刻以前にすると、有効期限切れにならなくなります。

ファイルを WORM にすると、ファイルが保持期限に達するまで、そのファイルのアクセス許可を変更できなくなります。WORM ファイルが保持期限に達すると、ファイルに書き込み権限を付与することが可能になります。ファイルに書き込み権限を付与することで、ファイル削除が可能となりますが、ファイル内容の変更はできないままです。

1.3.2 ファイルに WORM のマークを付ける

保持期限を設定した時点で、ファイルに WORM のマークを付けることができます。ファイルに WORM のマークを付けるには、以下のとおりファイルのアクセス許可を [read-only] に設定します。

- Unix クライアントから、書き込み属性権限を削除します。
- Windows クライアントから、ファイルのプロパティ経由で、ファイルを [read-only] としてマークします。



1.4 仮想ボリュームを管理する

ファイルシステムは、仮想ボリュームと呼ばれる分離ストレージエリアに分割できます。クライアント側からすると、仮想ボリュームは通常のファイルシステムのように見えます。仮想ボリュームには、プロジェクト、ユーザー、またはグループのディレクトリの割り当てや管理を行う簡単な方法が用意されています。仮想ボリューム内のファイルの容量と数は、Quota を使って管理できます。

仮想ボリュームを表示するには、[Storage Management] 画面に移動して [Virtual Volumes & Quotas] をクリックし、[Virtual Volumes & Quotas] 画面を表示します。



ここには、選択されたファイルシステムの仮想ボリュームが記載されています。

- 任意の列で昇順または降順に並べ替えるには、列のヘッダーをクリックします。
- 別の仮想ボリュームを表示するには、[change...] をクリックして、別のファイルシステムを選択します。

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS/File System Label	選択された EVS 及びファイルシステムの名前です。
Filter	この画面に表示されている Quota または仮想ボリュームの数を減らすために定義します。名前またはパスに基づいて設定できます。
Name	仮想ボリュームの名前です。
File System	ファイルシステムの名前です。
Contact	仮想ボリュームのアクティビティに関する情報やアラートを受け取る、連絡先メールアドレスです。 注：表示されるのは、最初の連絡先メールアドレスのみです。連絡先全てを表示したり、別途仮想ボリュームを変更したりするには、[details] をクリックします。
Path	仮想ボリュームが作成されたディレクトリです。
Usage	仮想ボリュームのデータ量です。

[Actions] では、以下のアクションを使用できます。

- [details] をクリックして、選択された仮想ボリュームの [Virtual Volume] 画面を表示します。
- [add] をクリックすると、[Add Virtual Volume] 画面を表示します。詳細は「1.4.1 仮想ボリュームを追加する」を参照してください。
- [delete] をクリックすると、選択した仮想ボリュームを削除します。詳細は「1.4.3 仮想ボリュームを削除する」を参照してください。

[Shortcut] では、以下のショートカットを使用できます。

- [View Quotas] をクリックして、選択された仮想ボリュームの [Quotas] 画面を表示します。
- [Download All Quotas] をクリックして、CSV (カンマ区切り) ファイルをダウンロードします。この CSV ファイルには、全ての仮想ボリュームの構成済み Quota が列挙されています。保存される Quota 情報は、Quota Type, Created By, Usage, Usage Limit, Usage Hard Limit, Usage Reset (%), Usage Warning (%), Usage Severe (%), File Count, File Count Limit, File Count Hard Limit, File Count Reset (%), File Count Warning (%), File Count Severe (%)などです。

1.4.1 仮想ボリュームを追加する

仮想ボリュームを追加するには

1. [add Virtual Volume] 画面に移動します。

[Virtual Volumes & Quotas] 画面で [add] をクリックして、[Add Virtual Volume] 画面を表示します。

2. 要求された情報を入力します。

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS/File System	この仮想ボリュームを追加する、EVS やファイルシステムです。仮想ボリュームを別の EVS/ファイルシステムに追加する場合は、[change...] をクリックして、EVS/ファイルシステムを選択します。
Virtual Volume Name	この名前には、最大 128 文字まで入力できます。 以下の文字はサポートしていません。 ?*=[] ; : / , < > ¥ 「A\$」という名前は Windows イベントビューアー用なので、使用できません。
Create a CIFS Share with the same name as the Virtual Volume Create a NFS Export with the same name as the Virtual Volume	仮想ボリュームと同名の共有やエクスポートがない場合は、このチェックボックスをオンにし、共有やエクスポートを確実に作成します。これは、CIFS または NFS 経由で仮想ボリュームにアクセスできるという利便性を考慮しているものにすぎません。 注：CIFS 共有または NFS 共有の名称は、80 文字を超えてはなりません。「A\$」は、Windows イベントビューアー用なので、CIFS 共有の名称に使用できません。
Allow exports to overlap	エクスポートを重複すると、セキュリティホールの抜け穴が明らかになる可能性があります。状態をテストして、セキュリティホールが発見されると、エクスポートの作成が拒否されることがあります。このチェックボックスを選択して、このテストを行わないようにすると、重複する NFS 共有を作成できます。
Path	ファイルシステムのディレクトリは、仮想ボリュームの「ルート」になります。例えば、/company/sales などです。このパスの全てのサブディレクトリは、仮想ボリュームの一部になります。以下のことに注意してください。 <ul style="list-style-type: none"> 固定パスです。 いったん作成したパスは、変更できません。 ファイルシステムのルートを扱うことはできません。 ファイルシステムのルート (/) で、仮想ボリュームを作成することはできません。仮想ボリュームは、ファイルシステムのディレクトリに適用されます。 空のホストファイルシステムディレクトリが必要です。 仮想ボリュームを作成して割り当てられる先は、空のディレクトリのみです。仮想ボリュームを、データを含むディレクトリに作成するには、まず、そのディレクトリの外にデータを移動させて、ディレクトリを空にします。仮想ボリュームを作成して、そのディレクトリに割り当てると、データを戻せます。 [Create path if it does not exist] : [Create path if it does not exist] のチェックがオンになっていると、[Path] フィールドに入力されたパスを作成します。
Email Contacts	仮想ボリューム使用量についての情報を受け取るための、メール連絡先です。各メールアドレスをボックスに入力し、[Add] をクリックすると、リストにそのアドレスが追加されます。アドレスを誤って入力した場合は、リストからそのアドレスを選択して [X] をクリックし、削除します。必要であれば、複数のメールアドレスを選択できます。 しきい値アラートのメール通知を設定するには、定義したしきい値に達した時にメール通知を随時受信する、明示的なメール受信者 (例: admin@company.com) を指定します。 ユーザーの Quota に達した時に、影響を受けるユーザーアカウント全てにメールを送信するには、*マークで始まるメールアドレスを、メール連絡先リスト (例: *@company.com) に追加します。 メールリストは、最大 512 文字に制限されています。 注：仮想ボリューム用に指定するメール連絡先がない場合は、HNAS が、Quota 警告イベントを生成します。メールアラートに加えてイベントを生成するには、

項目/フィールド	説明
	HNAS の Command Line Interface にアクセスして、 <code>quota-event --on</code> コマンドを発行します。

3. 設定を保存します。

設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。



重要 その後、[Virtual Volume] リスト画面で [details] をクリックすると、仮想ボリュームを変更できます。

1.4.2 仮想ボリュームを変更する

仮想ボリュームを変更するには

1. [Virtual Volumes & Quotas] 画面に移動します。

[Storage Management] 画面で [Virtual Volumes & Quotas] をクリックして、[Virtual Volumes & Quotas] 画面を表示します。



2. 設定を変更します。

仮想ボリュームの [details] をクリックして、設定を変更します。

3. 設定を保存します。

設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

1.4.3 仮想ボリュームを削除する

仮想ボリュームを削除するには

1. [Virtual Volumes & Quotas] 画面に移動します。

[Storage Management] 画面で [Virtual Volumes & Quotas] をクリックして、[Virtual Volumes & Quotas] 画面を表示します。

2. 仮想ボリュームを選択します。

仮想ボリュームを一つ選択するか、または [Check All] で全ての仮想ボリュームを選択します。



重要 仮想ボリュームを削除できるのは、ディレクトリが空の場合だけです。データが入っているディレクトリに割り当てられている仮想ボリュームを削除するには、まずデータを削除してから、仮想ボリュームを削除します。

3. 削除します。

[delete] をクリックすると、このアクションが確かに必要かどうか確認を求める警告が表示されます。仮想ボリュームの削除を続行するには、[OK] をクリックします。

1.4.4 仮想ボリュームの Quota を管理する

各仮想ボリュームに対して、以下の3種類の Quota が維持されます。

- 明示的ユーザー／グループの Quota
個々のユーザーまたはグループに制限を設けるために、一意なしきい値を定義することによって明示的に作成する Quota です。
- デフォルトユーザー／グループの Quota
明示的な Quota を持たないユーザー及びグループに、自動的に設定される Quota です。Quota デフォルト (しきい値) を定義することによって設定され、仮想ボリュームでファイルが作成または変更されるときに自動的にこの Quota が適用されます。
仮想ボリュームのデフォルトの Quota は、ファイルシステムに定義されているデフォルトの Quota と同じように動作します。ユーザーの (またはグループの) Quota デフォルトは、ユーザー (またはグループ) が初めて仮想ボリュームにファイルを保存するとき、そのユーザー (またはグループ) 向けの Quota を作成するために使用されるしきい値のセットです。
最初は、デフォルトの Quota は設定されていません。ユーザーが仮想ボリュームにファイルを作成しても、いずれかのしきい値にゼロ以外が設定されるまで、Quota は自動作成されません。少なくとも一つのしきい値がゼロ以外に設定されたとき、仮想ボリュームのルートディレクトリの所有者に対して、ユーザー Quota またはグループ Quota が (必要に応じて) 作成されます。
- 仮想ボリュームの Quota
仮想ボリュームの Quota は、仮想ボリュームの特定のディレクトリ内で使用されるスペースを監視します。どのユーザーやグループが操作を開始したかには関係なく、仮想ボリューム内での全ての操作を制限するしきい値を定義するために、明示的に Quota を作成できます。



重要 Quota は、全てのファイルの数と合計サイズを追跡します。特定のしきい値で、仮想ボリュームに関連する連絡先リストにメールアラートが発信されます。さらに、オプションとして、Quota しきい値超過イベントが記録されます。ユーザーまたはグループが設定された制限を超える操作は、[Hard Limit] を設定することによって禁止できます。

使用量制限及びファイル数制限が併用されている場合、両方とも有効となります。それぞれの制限値が個別に管理されます。

(1) 仮想ボリューム Quota を表示または変更する

仮想ボリューム Quota を表示または変更するには

1. [Quotas] 画面に移動します。

[Storage Management] 画面で、[Virtual Volumes & Quotas] を選択します。次に、Quota を確認する仮想ボリュームを選択して、[View Quotas] をクリックし、[Quotas] 画面を表示します。

User/Group Account	Quota Type	Created By	Usage Limit	File Count Limit
root	User	Automatically Created	1.00 GB	50
root	User	Automatically Created	1.00 GB	50
root	Group	Automatically Created	1.00 GB	50

2. フィルタリングして、一つの Quota または複数の Quota を表示します。

[Quotas] 画面に表示される Quota は、20 件のみです。Quota リストの次の画面に進むには、リストの上部と下部にあるリンクを使用します。リンク上にマウスを重ねると、リンクの使用について説明する画面ヒント (screen tips) が表示されます。

[Quotas] 画面の内容について、以下の表で説明します。

セクション	説明
Virtual Volume	Quota を適用する仮想ボリュームを特定します。 <ul style="list-style-type: none"> EVS/File System 仮想ボリュームが存在する EVS 及びファイルシステムです。 Virtual Volume Name 仮想ボリュームの名前です。 Path 仮想ボリュームが作成されたディレクトリです。
Filter	仮想ボリュームには、ユーザー/グループの Quota を多数存在させることができるため、HNAS には、リストをフィルタリングする方法が用意されています。 <ul style="list-style-type: none"> [Filter Quota Type] [All Types] (デフォルト), [Users], [Groups], または [Virtual Volume] から選択できます。 [where User/Group Account matches] このフィールドに、一致させる名前を入力します。ワイルドカード文字 (*) を使えます。 [filter] をクリックして、下のリストに表示される Quota を限定し、上で定めたフィルター基準に一致させます。
User/Group Account (別称: ターゲット)	Quota 名は、以下で構成されている場合があります。 <ul style="list-style-type: none"> CIFS ドメインと、ユーザー名またはグループ名 例: bb¥Smith, bb¥my_group (この場合、「bb」がドメイン、「Smith」がユーザー、「my_group」がグループです。) NFS ユーザーまたはグループ 例: richardb, finance (この場合、「richardb」が NFS ユーザーで、「finance」が NFS グループです。) 名前には、空欄または「0」にできます。空欄は仮想ボリュームの Quota の場合、「0」は仮想ボリュームのルートディレクトリの所有者に対して作成された場合です。
Quota Type	仮想ボリュームアクティビティのソースの種類です。使用可能な値は、User, Group, または Virtual Volume です。仮想ボリュームは、仮想ボリューム全体でアクティビティを開始する任意のユーザーに適用されます。各仮想ボリュームには、このターゲットの種類を持つ Quota が一つしか存在しない場合があります。
Created By	Quota の作成方法です。使用可能な値は、[Automatically Created] (Quota デフォルトを使って作成), または [User Defined] (特定の Quota に対して、Quota を一意に設定) です。
Usage Limit	Quota のターゲットが所有する、仮想ボリューム内のファイルの合計サイズに対する制限です。
File Count Limit	Quota のターゲットが所有する、仮想ボリューム内のファイルの合計数に対する制限です。

3. 必要に応じて、設定を変更します。

[Actions] では、以下のアクションを使用できます。

- 新しい Quota を追加するには、[add] をクリックします。
「(3) Quota を追加する」の説明を参照してください。
- 選択した Quota を削除するには、[delete] をクリックします。

- SMU のキャッシュを消去し、関連オブジェクトを使って再作成するには、[refresh cache] をクリックします。(これは、ブラウザの更新ボタンをクリックして、キャッシュを消去せずに最近の更新を取得することとは異なります。)

[Shortcuts] では、以下のショートカットを利用できます。

- [User Defaults] をクリックして、[User Quota Defaults] 画面に移動します。この画面で、ユーザーのデフォルトを設定または変更できます。
- [Group Defaults] をクリックして、[Group Quota Defaults] 画面に移動します。この画面で、グループのデフォルトを設定または変更できます。
- [Download Quotas for this Virtual Volume] をクリックして、CSV (カンマ区切り) ファイルをダウンロードします。この CSV ファイルには、仮想ボリュームの利用可能な全ての Quota 情報が含まれています。

(2) ユーザー／グループのデフォルトを設定する

ユーザー／グループのデフォルトを設定するには、以下の操作を行います。この手順は、[User Default] 画面の例です。[Automatically create quotas for Domain Users] チェックボックス以外は、[Group Default] 画面と同じです。このオプションを使って、グループの「Domain Users」のデフォルト Quota を作成できます。デフォルトで、各 NT ユーザーは「Domain Users」グループに属しています。各ユーザーのプライマリグループが既に明示的に設定されている場合を除き、Quota に全ての NT ユーザーが含まれます。

1. [User Quota Defaults] 画面に移動します。

[Quotas] 画面で [User Defaults] をクリックして、[User Quota Defaults] 画面を表示します。

[User Quota Defaults] 画面には、EVS／ファイルシステム及び仮想ボリューム名がデフォルトとして表示されます。

2. 要求された情報を入力します。

フィールドが 0 (または空欄) になっている場合、その入力は「未設定」とみなされます。例えば、[File Count Limit] が 0 なら、作成される Quota はファイル数に制限を課さないということです。[Warning] 及び [Severe] のしきい値も、未設定とみなされます。



重要 ユーザーの Quota デフォルトを消去するには、[Clear Defaults] をクリックします。これにより、仮想ボリュームに、ユーザー Quota デフォルトが追加作成されないようにします。また、既存の「Automatically Created」ユーザーの Quota を「User Defined」ユーザーの Quota に変換します。

次の表では、この画面のフィールドについて説明します。

項目／フィールド	説明
EVS/File System	ユーザー Quota が適用される、EVS 及びファイルシステムです。
Virtual Volume Name	デフォルトを使って作成したユーザー Quota を割り当てる、仮想ボリュームの名前です。
Usage	

項目/フィールド	説明
Limit	使用可能な空き容量を、バイト単位 (Bytes, KB, MB, GB, TB, PB, EB) で入力します。
Hard Limit	選択した場合、[Limit] フィールドで指定した空き容量を超過できません。
Warning	[Limit] フィールドに指定した空き容量の割合になった時点で、[Warning] アラートが発信されます。
Severe	[Limit] フィールドに指定した空き容量の割合になった時点で、[Severe] アラートが発信されます。
File Count	
Limit	仮想ボリュームで許可する最大ファイル数を入力します。
Hard Limit	選択した場合、[Limit] フィールドで指定したファイル数を超過できません。
Warning	[Limit] フィールドに指定したファイル数の割合になった時点で、[Warning] アラートが発信されます。
Severe	[Limit] フィールドに指定したファイル数の割合になった時点で、[Severe] アラートが発信されます。
Log Quota Events in the managed server's Event Log	このチェックボックスをオンにすると、全てのユーザーまたは全てのグループのデフォルトが設定されます。ノードのイベントログに、Quota イベントを記録するためです。

3. 設定を保存します。

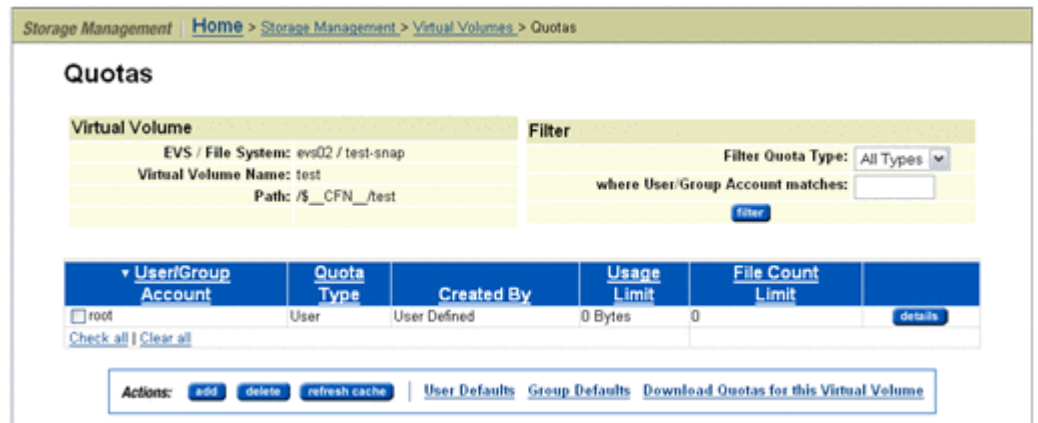
設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

(3) Quota を追加する

Quota を追加するには

1. [Quotas] 画面に移動します。

[Storage Management] 画面で [Virtual Volumes & Quotas] を選択し、Quota を追加する仮想ボリュームを選択して、[View Quotas] をクリックし、[Quotas] 画面を表示します。



2. [Add Quota] 画面に移動します。

[Quotas] 画面で、[add] をクリックします。

Add Quota

EVS / File System: evs-1 / fs01
Virtual Volume Name: vv01

Quota Type: User Group Virtual Volume

User Account i.e. domain/user (CIFS) or user (NFS):
Group Account i.e. domain/group (CIFS) or group (NFS):

Usage

Limit: 00

Hard Limit:

Warnings: 75 %

Severe: 95 %

File Count

Limit:

Hard Limit:

Warnings: 75 %

Severe: 95 %

Log Quota Events in the managed server's Event Log

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS/File System	Quota を追加する仮想ボリュームをホストしている、EVS 及びファイルシステムの名前です。
Virtual Volume Name	Quota を追加する仮想ボリュームの名前です。
Quota Type	仮想ボリュームアクティビティのソースの種類です。使用可能な値は、User、Group、または Virtual Volume です。
User Account Group Account	[User Account] 及び [Group Account] の名前は、以下で構成されています。 <ul style="list-style-type: none"> CIFS ドメインと、ユーザー名またはグループ名 例: bb¥Smith, bb¥my_group (この場合、「bb」がドメイン、「Smith」がユーザー、「my_group」がグループ。) NFS ユーザーまたはグループ 例: richardb, finance (この場合、「richardb」が NFS ユーザーで、「finance」が NFS グループ。) 「Quota Type」に「Virtual Volume」が選択されている場合は、Quota 名を指定できません。
Usage	
Limit	使用可能な空き容量を、バイト単位 (Bytes, KB, MB, GB, TB, PB, EB) で入力します。
Hard Limit	選択すると、[Limit] フィールドで指定した空き容量を超過できません。
Warning	[Limit] フィールドに、空き容量の割合を指定して入力します。その割合になった時点で、[Warning] アラートが発信されます。
Severe	[Limit] フィールドに、空き容量の割合を指定して入力します。その割合になった時点で、[Severe] アラートが発信されます。
File Count	
Limit	この Quota に対して有効にする最大ファイル数を入力します。
Hard Limit	選択した場合、[Limit] フィールドで指定したファイル数を超過できません。
Warning	[Limit] フィールドに、ファイル数の割合を指定して入力します。その割合になった時点で、[Warning] アラートが発信されます。

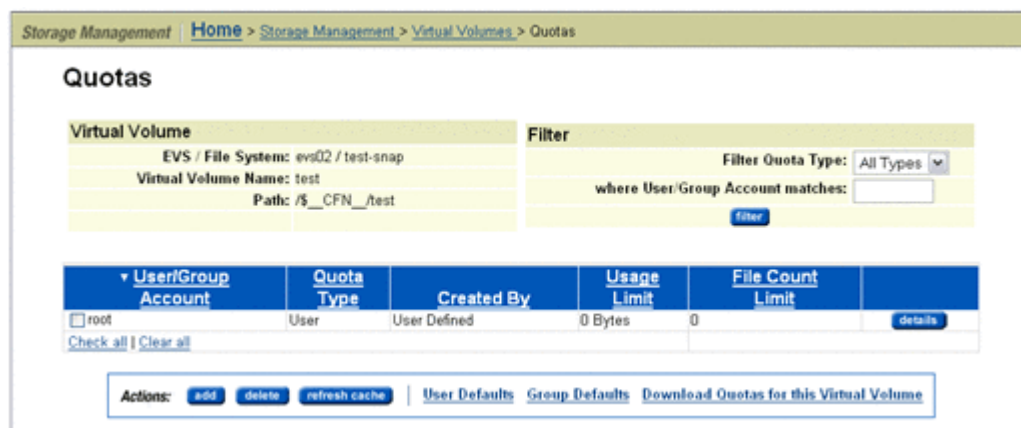
項目/フィールド	説明
Severe	[Limit] フィールドに、ファイル数の割合を指定して入力します。その割合になった時点で、[Severe] アラートが発信されます。
Log Quota Events in the managed server's Event Log	このチェックボックスをオンにすると、この Quota に起因するイベントが、サーバイベントログに記録されます。

- Quota を追加するには、要求された情報を入力します。
フィールドが 0 (または空欄) になっている場合、その入力は「未設定」とみなされます。例えば、[File Count Limit] が 0 なら、作成される Quota はファイル数に制限を課さないということです。[Warning] 及び [Severe] のしきい値も、未設定とみなされます。
- 変更を保存します。
追加または削除を確認したら、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

(4) Quota を削除する

Quota を削除するには

- [Quotas] 画面に移動します。
[Storage Management] 画面で、[Virtual Volumes & Quotas] を選択します。次に Quota を削除する仮想ボリュームを選択して、[View Quotas] をクリックし、[Quotas] 画面を表示します。



- 削除する Quota を選択します。
削除する Quota のチェックボックスをオンにします。
- 選択した Quota を削除するには、[delete] をクリックします。

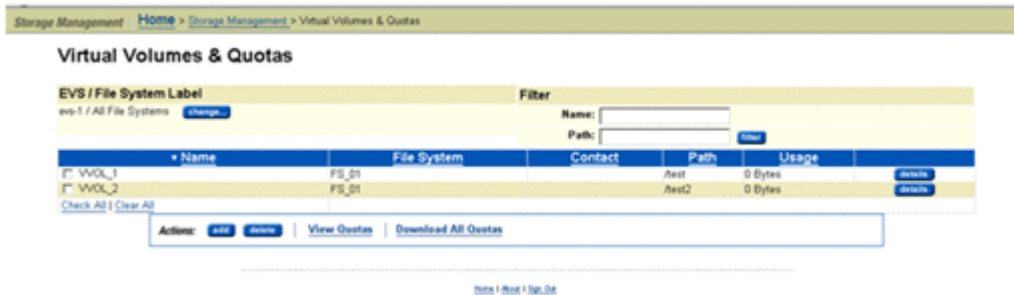


重要 明示的な Quota を削除すると、仮想ボリュームのルートディレクトリ所有者のデフォルト Quota が、Quota リストに自動的に再表示されます。

(5) 全仮想ボリュームの Quota をエクスポートする

全仮想ボリュームの Quota をエクスポートするには

- [Virtual Volumes & Quotas] 画面に移動します。
[Storage Management] 画面で [Virtual Volumes & Quotas] を選択して、[Virtual Volumes & Quotas] 画面を表示します。



2. エクスポートを起動します。

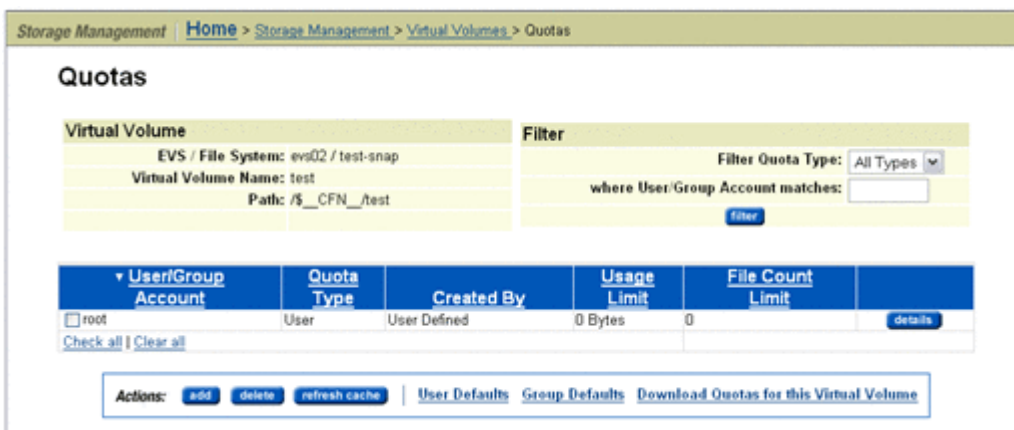
[Download All Quotas] をクリックします。CSV（カンマ区切り）ファイルとして、Quota 情報を保存することを許可するダイアログボックスが表示されます。また、Quota 情報は、アプリケーションに表示させることもできます。

(6) 特定の仮想ボリュームの Quota をエクスポートする

特定の仮想ボリュームの Quota をエクスポートするには

1. [Quotas] 画面に移動します。

[Storage Management] 画面で [Virtual Volumes & Quotas] を選択し、[Virtual Volumes & Quotas] 画面を表示します。次に、仮想ボリュームを選択して、[View Quotas] をクリックし、[Quotas] 画面を表示します。



2. エクスポートを起動します。

[Download Quotas for this Virtual Volume] をクリックします。CSV（カンマ区切り）ファイルとして、Quota 情報を保存することを許可するダイアログボックスが表示されます。また、Quota 情報は、アプリケーションに表示させることもできます。

ファイルシステムのセキュリティを管理する

セキュリティモードは、クラスタごと、ファイルシステムごと、または仮想ボリュームごとに構成できます。セキュリティモードを、システム全体ではなく前述したクラスタ、ファイルシステム、仮想ボリュームなどの階層ごとに選択することで、システムセキュリティ管理の粒度と利便性を向上させることができます。

- [2.1 セキュリティ設定を表示する](#)
- [2.2 NFS セキュリティ及び Kerberos](#)
- [2.3 混合セキュリティモード](#)

2.1 セキュリティ設定を表示する

2.2 NFS セキュリティ及び Kerberos

2.2.1

2.3 混合セキュリティモード

HNAS の混合セキュリティモードは、Windows と UNIX の両方のセキュリティ定義をサポートしています。セキュリティは、ファイル（ディレクトリ）を作成したユーザー、または直近でファイル（ディレクトリ）の所有権を持っていたユーザーに基づいて、ファイル（ディレクトリ）ごとにセットアップされます。Windows ユーザーの場合、セキュリティ定義のデフォルトは CIFS になり、Windows セキュリティルールの対象です。同様に、UNIX ユーザーの場合、セキュリティ定義のデフォルトは NFS になり、UNIX セキュリティルールの対象です。

ネイティブ CIFS ファイルへの CIFS アクセス

CIFS クライアントが、ネイティブ CIFS ファイルにアクセスしようとする（Windows セキュリティルールを適用すると）、HNAS が、ファイルのセキュリティ情報とユーザー情報を照らし合わせて確認し、操作を許容するかどうかを判断します。

- ユーザーセキュリティ
この情報は、アクセストークンに含まれており、ユーザーセキュリティ識別子 (SID)、プライマリグループ SID、及びその他の SID で構成されています。HNAS は、ドメインコントローラーからトークンを受け取り、ユーザーセッションが終わるまでキャッシュします。
- ファイルセキュリティ
この情報は、ファイルセキュリティ記述子に含まれており、所有者 SID、グループ SID、及びアクセス制御リスト (ACL) で構成されています。ACL には、アクセス条件を指定する複数のアクセス制御エントリ (ACE) が含まれます。

ACE エントリは、`cacls` と呼ばれるコマンドセットを使って、修正または削除できます。このコマンドセットには、`cacls-add`、`cacls-del`、`cacls-fields`、`cacls-mask-in`、`cacls-mask-out`、及び `cacls-set` が含まれます。

これらのコマンドの詳細については、『*Command Line Reference*』を参照してください。

ネイティブ NFS ファイルへの NFS アクセス

NFS クライアントが、ネイティブ NFS ファイルに（UNIX セキュリティルールを適用して）アクセスしようとする、HNAS が、ファイルのセキュリティ情報とユーザー情報を照らし合わせて UNIX 証明書を確認し、操作を許容するかどうかを判断します。ファイルセキュリティ情報は、ユーザー ID、グループ ID、及び読み取り・書き込み・実行の権限で構成されています。

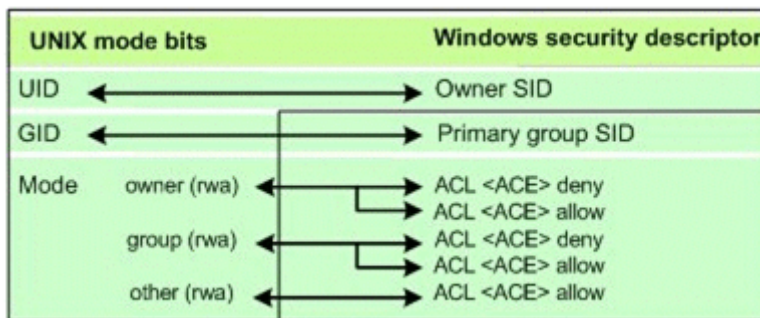
ネイティブ以外のファイルへのクライアントアクセス

CIFS クライアントは、UNIX セキュリティルールが記録されているファイルにアクセスできます。NFS クライアントは、Windows セキュリティルールが記録されているファイルにアクセスできます。HNAS は、NFS のユーザー ID 及びグループ ID と、Windows のそれらと同等の情報を関連付けるマッピングテーブルを使用してこの機能をサポートします。例えば、CIFS クライアントが UNIX のセキュリティ情報だけを持ったファイルにアクセスしようとする、HNAS が、マッピングテーブルを参照し対応する CIFS のユーザー名を対応する NFS のユーザー ID に自動的にマップします。

- HNAS は、ユーザーのセキュリティ情報を UNIX 形式から Windows 形式、またはその逆に自動変換し、それをセッション継続中キャッシュします。

UNIX 証明書	マッピングテーブル	Windows アクセストークン
UID	ユーザーマッピングテーブル	ユーザー SID
GID	グループマッピングテーブル	プライマリグループ SID
その他グループ	グループマッピングテーブル	その他グループ

- システムは、ファイルセキュリティ属性を Windows 形式から UNIX 形式に自動変換し、その結果をファイルメタデータに保存します。その結果、それ以降ファイルは CIFS クライアントと NFS クライアントの両方に対してネイティブになります。UNIX ファイルも Windows 形式に変換されますが、結果はファイルメタデータに保存されません。



- ユーザーがファイルのセキュリティ属性に加える変更は、Windows と UNIX に等しく適用されます。

つまり、CIFS クライアントが、UNIX セキュリティルールだけを持ったファイルにアクセスしようとする、HNAS が CIFS ユーザー名を NFS ユーザー ID にマップし、ユーザーのアクセストークンを UNIX 証明書に変換します。次に、この証明書を、ファイルのセキュリティ属性に照らしてチェックし、この操作が許容できるものかどうかを判断します。

同様に、NFS クライアントが Windows セキュリティ情報だけを持ったファイルにアクセスしようとする、HNAS が NFS ユーザー名を CIFS ユーザー ID にマップし、ユーザーの UNIX 証明書を Windows アクセストークンに変換します。次に、このトークンを、ファイルセキュリティ属性に照らしてチェックします。

2.3.1 UNIX セキュリティモード

HNAS が UNIX セキュリティモードで構成されている場合、この HNAS は、CIFS クライアント及び NFS クライアントの UNIX セキュリティをサポートします。ただし、全てのセキュリティ設定が、Unix ファイル属性で保存されます。その結果、NFS クライアントは常にネイティブモードでファイルにアクセスすることになり、CIFS クライアントは、常にネイティブ以外のモードでファイルにアクセスすることになります。両モードの操作についての詳細は、「2.3.2 (3) 混合モード操作」を参照してください。



重要 UNIX セキュリティモードでは、NFS ユーザーは、ファイルにアクセスするために、Windows ドメインコントローラー (DC) の有無に依存する必要はありません。結果として、DC 障害の可能性から完全に切り離されます。

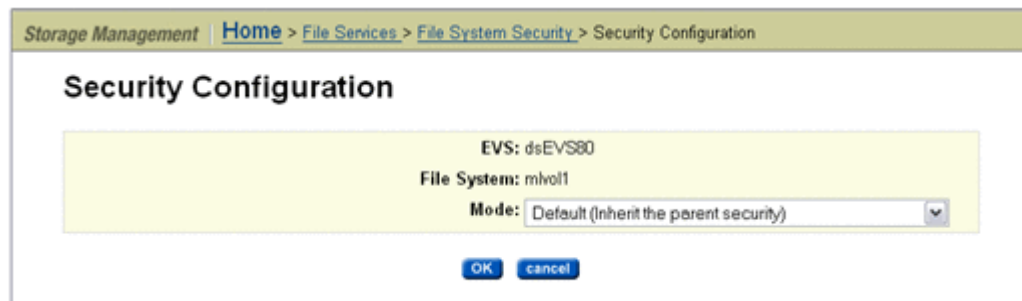
2.3.2 セキュリティモードを変更する

(1) ファイルシステムのセキュリティモードを変更する

デフォルトでは、ファイルシステムは、親 EVS のセキュリティモードを引き継ぎます。例えば、親 EVS が Unix セキュリティモードのとき、子ファイルシステムは、そのセキュリティモードを引き継ぎます。

ファイルシステムを変更して、別のセキュリティモードを使用するには

1. [File System Security] 画面へ移動します。
[File Services] 画面で [File System Security] をクリックして、[File System Security] 画面を表示します。
2. [Security Configuration] 画面を表示するには、[details] リンクをクリックします。
[File System Security] 画面で、表示されている EVS が正しいかどうか、フィルターが適切に設定され、必要なファイルシステムが表示されているかどうかを確認してください。[Security Configuration] 画面を表示するには、[details] ボタンをクリックします。



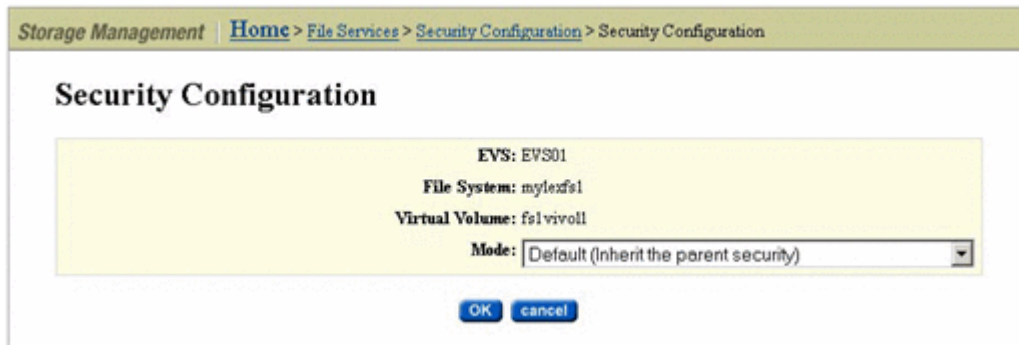
3. セキュリティモードを選択します。
ドロップダウンメニューから、セキュリティモードを選択します。選択するには [OK]、キャンセルするには [cancel] をクリックします。

(2) 仮想ボリュームのセキュリティモードを変更する

デフォルトでは、仮想ボリュームは、親ファイルシステムのセキュリティモードを引き継ぎます。例えば、親ファイルシステムが Unix セキュリティモードのとき、子仮想ボリュームは、そのセキュリティモードを引き継ぎます。

1. [File System Security] 画面へ移動します。
[File Services] 画面で [File System Security] をクリックして、[File System Security] 画面を表示します。
2. [Security Configuration] 画面を表示するには、[details] リンクをクリックします。

[File System Security] 画面で、表示されている EVS が正しいかどうか、フィルターが適切に設定され、必要な仮想ボリュームが表示されているかどうかを確認してください。[Security Configuration] 画面を表示するには、[details] ボタンをクリックします。



次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS	ファイルシステムをホストしている Virtual Server です。
File System	仮想ボリュームの親ファイルシステムです。
Virtual Volume	セキュリティモードを変更する、仮想ボリュームです。
Mode	ドロップダウンリストを使って、仮想ボリュームのセキュリティモードを選択します。

3. セキュリティモードを選択します。

ドロップダウンメニューから、セキュリティモードを選択します。選択するには [OK], キャンセルするには [cancel] をクリックします。

(3) 混合モード操作

HNAS を使用して、ネットワーククライアントは、Windows クライアントと UNIX クライアントの共有ストレージプールを共有できます。これを、「混合モード操作」といいます。HNAS は、できるだけシームレスにこの操作を行います。この二つのプロトコルは大きく違うため、混合モード操作には、いくつか課題があります。この課題については、以下の「ファイル名表現」セクション及び「シンボリックリンク」セクションで扱っています。

ファイル名表現

ファイル名の長さは、最大 255 文字までです。

ファイル名には、Unicode 文字を含めることができます。Windows NT 4.0, Windows 2000, Windows 2003, Windows XP の各クライアントには、Unicode 全部を使用できますが、Windows 9x と NFS の各クライアントは、拡張 ASCII の Latin-1 バージョンのみをサポートします。

ファイル名の大文字と小文字を区別することが、NFS クライアントと FTP クライアントには重要ですが、CIFS クライアントには重要ではありません。

シンボリックリンク

シンボリックリンク（シムリンク）は、以下のためによく使用されます。

- ファイルシステムの異なる部分を結合するため
- Windows 環境のショートカットと似た利便性があるため
- クラスタ外のデータにアクセスするため

例えば、シムリンクは、別の HNAS や、ファイルサーバ上にあるデータを指すことができます。

シムリンクには、以下の二つの種類があります。

- シムリンク自体に関連するパスを含む、相対シムリンク
例えば、「../dst」は相対シムリンクです。
- (HNAS のファイルシステムのルートに関連するのではなく) シムリンクを作成した NFS クライアントのファイルシステムのルートに関連するパスを含む、絶対シムリンク
例えば、「/mnt/datadir/dst」は絶対シムリンクです。

NFS 経由でファイルシステムにアクセスするときは、HNAS がシムリンクを完全サポートします。NFS/UNIX クライアントは、シンボリックリンクのマークの付いたファイルには、クライアントが読み込んで、別のファイルやディレクトリへの間接的な参照と解釈できるテキストパス名が含まれているとみなします。どのクライアントもシムリンクをたどることはできますが、ターゲットファイル (ディレクトリ) へのアクセスには権限が必要です。

一方で、CIFS クライアントは、シムリンクとマークの付いたファイルを追跡できません。そのため、HNAS が、HNAS 側シムリンク追跡能力を備えています。CIFS クライアントまたは FTP クライアントが HNAS 側シムリンクにアクセスすると、HNAS がリンクからパスを読み取り、自動的に追跡を試みます。

- 相対シムリンクは、追跡できます。HNAS が、リンク自体からパスを追跡できるためです。
- 一方で、絶対リンクに関しては、リンクを作成した NFS クライアント上にあるファイルシステムのルートに、HNAS がアクセスできないため、リンクを自動的に追跡できません。
この問題を克服するために、HNAS はグローバルシムリンクを備えています。グローバルシムリンクを使用して、CIFS クライアントは絶対シムリンクを追跡できます。
 - 絶対シムリンクがシムリンクと同じ CIFS 共有内のファイルまたはディレクトリを参照している場合、HNAS はシムリンクを (CIFS クライアントに代わって) 内部的に追跡します。
 - 絶対シムリンクがシムリンクと異なる CIFS 共有のオブジェクトを参照している場合、CIFS クライアントは Microsoft の DFS メカニズムを介してリンク先にリダイレクトされます。



重要 Microsoft の DFS メカニズムは、ディレクトリ (ファイルではない) へのリダイレクトのみサポートします。このため、異なる CIFS 共有のファイルを参照する絶対シムリンクは、CIFS クライアントで正しく処理されません。

リンク先は、このリンクと同じファイルシステム上、サーバファーム内の別のファイルシステム上、またはリモート CIFS サーバ上とすることができます。グローバルシムリンクと絶対シムリンクを関連付けるために、HNAS は、絶対シムリンクパスとグローバルシムリンクパスの間の変換テーブルを維持します。



重要 CIFS2 (SMB2) クライアントは、Hitachi High-performance NAS Platform™ 経由でアクセスするストレージ上のファイルへのシムリンク (相対または絶対) を追跡できません。

HNAS 側シムリンクにアクセスするとき、CIFS クライアントは、NFS に対して完全に有効にされている一部のシムリンクを追跡できません。ストレージシステムが、CIFS クライアントに代わってシムリンクを追跡し、シムリンクの代わりにファイルへのリンクを提示するためです。この場合、Samba の動作に合わせて、HNAS が、シムリンクの存在を CIFS/FTP クライアントから完全に隠します。デフォルトで、共有範囲外 (別のファイルシステムなど) を指しているシムリンクは、追跡されません。

グローバルシムリンクを使用して、クラスター外のデータへのリンクを設定できます。NFS クライアントは、グローバルシムリンクを直接追跡できます。CIFS クライアントは、HNAS が維持する変換テーブルを使用して、リンク先へアクセスできます。グローバルシムリンクは通常、リンク先としてディレクトリを指定します。ファイルを対象としたリンクは同一共有内のみ対応しています。グローバルシムリンクは、スラッシュ文字 (/) で始まります。

クライアントがグローバルシmlinkを検出すると、以下の状態になります。

- NFS クライアントに対しては、HNAS は、グローバルシmlinkのコンテンツを返し、クライアントがリンク先までリンクを追跡できるようにします。つまり、NFS クライアントのマウントポイント及び NFS 共有は、正確にセットアップされている必要があります。
- CIFS クライアントに対しては、HNAS がクライアントに、ローカル EVS 変換テーブルからのシmlink参照をリクエストさせます。CIFS クライアントが参照をリクエストした時点で、HNAS がリンク先サーバ名、共有名、CIFS クライアントへのパスを返し、CIFS クライアントがリンク先にアクセスできるようになります。



注意 シmlinkのリンク先ディレクトリに注意してください。CIFS クライアントがグローバルシmlinkのパスを追跡した時点で、長期間、そのシmlinkの別の参照を HNAS に問い合わせられなくなります。シmlinkは、クライアントが追跡するシmlinkを毎回参照するわけではないため、リンク先ディレクトリが変更または削除されると、CIFS クライアントが誤ったリンク先への接続を試みようとする場合があります。場合により、クライアントがエラーを報告します。

グローバルシmlinkと CIFS の併用には、性能に不利な条件があります。そのため、グローバルシmlinkはデフォルトで無効になっています。ただし、[Add Share] 画面（共有作成時）、または [CIFS Share Details] 画面（共有作成後）の [Follow Global Symbolic Links] チェックボックスをオンすると、有効にできます。

シmlink変換テーブルは、EVS ごとに保持されます。そのため、以下のような動作となります。

- シmlink変換テーブルは、EVS と共に移行されます。EVS が移行されると、シmlink変換テーブル全てが EVS と共に移行されます。
- シmlink変換テーブルは、EVS から複製されません。ある EVS から別の EVS にデータを複製するとき、グローバルシmlinkのマッピング情報は自動的に再配置されないため、データコピー先 EVS の変換テーブルで再作成する必要があります。
- シmlink変換テーブルは、ファイルシステムと共に移動しません。ファイルシステムが、ある EVS から別の EVS に移動する場合、グローバルシmlinkのマッピング情報は自動的に再配置されないため、手動調整が必要です。ただし、CNS ツリーに関連するシmlinkは、調整不要なので除外します。
- シmlink変換テーブルは、CNS に関連するシmlinkに無関係です。EVS が移行される場合、CNS に関連するシmlinkを調整する必要はありません。クライアントがシンボリックリンクを追跡する場合は、最初に CNS ツリーを参照します。次に、パスが CNS リンクと交差したときに、実際のファイルシステムを参照します。

シmlink変換テーブルは、以下の CLI コマンドを介して管理されます。

```
global-symlink-add
```

```
global-symlink-del
```

```
global-symlink-delall
```

```
global-symlink-list
```

グローバルシmlinkの管理に使用する CLI コマンドについては、『*Command Line Reference*』を参照してください。

混合モード操作及び LDAP サーバ

HNAS は、ファイルシステムの混合モードアクセスをサポートします。一貫したセキュリティとアクセスを確保するために、ファイルシステムのアクセス許可と所有者の間にマッピングが必要なためです。NIS/LDAP サービスを使用すると、HNAS はローカルアカウントを作成する代わりに、ネットワーク上の既存の NIS/LDAP サービスに基づいて、ユーザー及びアクセス許可を検索し、マッピングできます。

既存の LDAP サービスでは、HNAS がユーザー及びアクセス許可を検索してマッピングできるようにするために、通常、以下のうち一つの方法を使用します。

- RFC 2307 スキーマ

RFC 2307 は、LDAP サーバのユーザー及びグループのマッピング情報の保管と検索の標準的な規約を定義します。ユーザーのサイトで RFC 2307 スキーマを使用し、混合モード操作と LDAP サービスの両方をサポートするように、HNAS を設定する場合、ユーザーは、既に RFC 2307 スキーマをディレクトリにロードし、ユーザーオブジェクトを適切にプロビジョニングしているとみなされます。

- Services for Unix (SFU) スキーマ

SFU (Services for Unix) を設定する場合、Active Directory (AD) ドメインの各アカウントに対して、NIS 参加を明示的に有効にする必要があります。Active Directory ユーザー及びコンピューターユーティリティのユーザーアカウントプロパティの UNIX 属性タブにある個別アカウントに対して、NIS 参加を有効にできます。

HNAS を混合モード操作及び LDAP サービスの両方をサポートするよう設定するときに、最適性能を確保するために、最も最適化された構成には、HNAS が問い合わせる属性に対する、LDAP サービスのインデックス作成を含みます。

クエリーへの最速の応答を確保するには、LDAP サーバ上に、検索する属性のために、完全一致インデックスを構成しなければなりません。ネットワーク上にある LDAP サーバは、少なくとも以下の属性をインデックス化することが必要です。

オブジェクトの記述内容	RFC 2307 クラス	Services for Unix クラス	Map to NIS クラス
ユーザーアカウントの説明	posixAccount	ユーザー	posixAccount
グループ識別子の説明	posixGroup	グループ	posixGroup

属性の目的	RFC 2307 属性	Services for Unix 属性	Map to NIS 属性
ユーザー ID/ログイン名	uid	sAMAccountName	memberUid
ユーザー ID 番号	uidNumber	msSFU30UidNumber	uidNumber
グループ名	cn	cn	memberNisNetgroup
グループ ID 番号	gidNumber	msSFU30GidNumber	gidNumber

RFC 2307 属性または Services for Unix 属性が、LDAP サーバにあらかじめインデックス化されているかどうかは、ディレクトリサービスの提供者によって異なります。

インデックス作成の性能を追跡するには、LDAP クエリーの応答時間を監視できる `ldap-stats` コマンドを使用できます。統計データを収集できるように、最初に、HNAS がユーザー参照を問題なく完了させる必要があります。一方で、どの属性をインデックス化するかを、短時間で判断できるようにしなくてはなりません。

(4) 混合モードでのファイルロック

CIFS クライアントは、ファイルへの読み取りまたは書き込みを行う場合に、CIFS クライアントと NFS クライアントの両方が外したロックを考慮します。反対に、NFS クライアントは、CIFS クライアントが外したロックのみ考慮します。したがって、NFS クライアントは、ネットワークロックマネージャー (NLM) プロトコルを用いる既存の NFS ロックをチェックします。HNAS は、監視対象及び監視対象外の NFS ファイルロックの両方をサポートします。

(5) 便宜的ロック (Oplocks)

Oplock は、マイクロソフトネットワーク (CIFS) 環境で使用される性能エンハンス技術です。ファイルの全部または一部をローカルでキャッシュすることによって、アプリケーションによるファイルアクセスを迅速化したり、ネットワークトラフィックを最小限に抑えたりできます。デー

タがクライアントに保存されているため、HNAS に関与することなく、読み書き操作をローカルで行えます。

HNAS は、以下の三つの便宜的ロックをサポートします。

- 排他ロック

排他ロックは、単一クライアントがファイルの読み取り・書き込みの両方をキャッシュできるようにします。便宜的ロックを所有するクライアントは、ファイルにアクセスする唯一のクライアントなので、ファイルの全部または一部をローカルで読み込んだり、変更したりできます。クライアントは、ファイルを閉じて便宜的ロックを解除するまで、変更を HNAS に送信する必要はありません。

- バッチロック

バッチロックは、便宜的排他ロックの場合と同様に、単一クライアントがファイルの読み取り・書き込みの両方をキャッシュできるようにします。さらに、クライアントは、ファイルを閉じた後もキャッシュされた情報を保存できます。また、ファイルの開閉操作も、ローカルで行えます。クライアントは、便宜的ロックを解除するまで、変更を HNAS に送信する必要はありません。

- レベル II ロック

便宜的レベル II ロックは、複数のクライアントがファイルを読み取りのみキャッシュできるようにします。便宜的ロックを所有しているクライアントは、キャッシュされたローカル情報や先読みされたローカル情報のファイルデータ及び属性を読み込みます。特定のクライアントがファイルに変更を加えると、全ての便宜的ロックが解除されます。

便宜的ロックを扱うとき、HNAS は、CIFS 仕様に従って動作します。Windows 環境でも、CIFS クライアントと NFS クライアントの混合でも、HNAS は、データの整合性を守ったままで、アプリケーションがローカルキャッシュを利用できるようにします。

(6) 排他ロックとバッチロック

排他ロックとバッチロックは、CIFS クライアントがファイルを開いたときに得られる、排他的（読み書き／全て拒否）ファイルロックです。HNAS は、他のアプリケーションがその時点でファイルにアクセスしていない場合に限り、この便宜的ロックを許可します。

クライアントがファイルの排他ロックまたはバッチロックを所有している場合、クライアントは、ファイルの一部または全部をローカルでキャッシュできます。クライアントがファイルに加える変更も、ローカルでキャッシュされます。クライアントが便宜的ロックを解除するまで、変更を HNAS に書き込む必要はありません。排他ロックの場合、クライアントが便宜的ロックを解除するよう HNAS がリクエストするとき、またはクライアントがファイルを閉じるときに、クライアントは便宜的ロックを解除します。バッチロックの場合、ファイルを閉じた後も、クライアントは情報（変更を含む）をローカルに保存できます。クライアントが排他ロックまたはバッチロックをファイルにかけている間、HNAS は、他のクライアントがファイルにアクセスしないことを保証します。

クライアントが、排他ロックまたはバッチロックがかけられているファイルへのアクセスをリクエストすると、HNAS は、便宜的ロックを使用しているクライアントに、ロックを解除するよう求めます。その後、クライアントが HNAS に変更を書き込み、便宜的ロックを解除します。この操作が完了した時点で、HNAS は、2 番目のクライアントに、ファイルへのアクセスを許可します。これは、2 番目のクライアントのネットワークプロトコルの種類にかかわらず行われます。

CIFS クライアントが排他的ロックまたはバッチロックを使えるファイルの便宜的ロックをリクエストする場合、HNAS は既存の便宜的ロックを解除し、その代わりにレベル II の便宜的ロックを両クライアントに許可します。

(7) レベル II ロック

レベル II ロックは、CIFS クライアントがファイルを開いたときに得られる、非排他的（読み取り専用／書き込み拒否）ファイルロックです。HNAS は、その時点でファイルにアクセスしている他の全てのアプリケーションもレベル II ロックを持っている場合に限り、この便宜的ロックを許可します。

- 他のクライアントが排他的ロックまたはバッチロックを所有している場合は、新しいクライアントが便宜的ロックの許可を受ける前に、HNAS は、そのロックを解除し、レベル II ロックに変換します。
- クライアントがファイルのレベル II ロックを所有している場合、クライアントは、ファイルの一部または全部をローカルでキャッシュできます。便宜的ロックを所有しているクライアントは、HNAS に関与することなく、ファイルデータ及び属性をローカル情報から読み込むことができます。また、他のクライアントがファイルに書き込めないことを保証します。
- クライアントが、レベル II ロックをかけているファイルに書き込む場合、HNAS は、この便宜的ロックを使っているクライアントにロックを解除するよう求め、その後、2 番目のクライアントに書き込みを許可します。これには、2 番目のクライアントのネットワークプロトコルを問いません。

(8) NFSv4 のユーザー名及びグループ名

NFSv4 では、ユーザー及びグループは、`user@dns_domain` 及び `group@dns_domain` という形式の UTF-8 文字列で識別されます。HNAS は、以下のユニバーサルなユーザー／グループ識別子をサポートしています。

OWNER@	ファイルの所有者。
GROUP@	ファイルのグループ。
EVERYONE@	全員。
NETWORK@	ネットワーク経由のアクセス。
ANONYMOUS@	認証なしのアクセス。
AUTHENTICATED@	認証ユーザー。

(9) ユーザー及びグループのマッピングを構成する

HNAS が混合セキュリティモードまたは UNIX セキュリティモードのどちらかで動作している場合、HNAS は、UNIX と Windows のユーザー及びグループの間のマッピングを作成します。例えば、「John Doe」というユーザーが「jdoe」という UNIX ユーザーアカウントと、「johnd」という Windows ユーザーアカウントを持っているとします。これら二つのユーザーアカウントは、ユーザーマッピングを設定することによって同等になります。さらに、HNAS は、同等のユーザー（グループ）名を、両方の環境に対して同一とみなします。例えば、「janed」というユーザーの明示的なマッピングが検出されない場合、HNAS は、「janed」という UNIX ユーザーアカウントは、同名の Windows ユーザーアカウントと同一であるとみなします。

HNAS 上でユーザー及びグループのマッピングを設定するときは、以下の二つの手順に従います。

- 各 NFS ユーザー（グループ）の名前と ID を指定します。
Windows ユーザーまたはグループには、このステップは不要です。HNAS が必要な情報全てを、ドメインコントローラー（DC）から取得するためです。
- NFS ユーザー（グループ）の名前を、Windows NT ユーザー（グループ）名にマップします。

(10) NFS ユーザー及び NFS グループのマッピングを管理する

UNIX ユーザーが作成したファイルに Windows がアクセスすること（または Windows ユーザーが作成したファイルに UNIX がアクセスすること）が許可されるのは、UNIX の名前または Windows の名前が同一ユーザーと認識された場合です。ただし、NFS クライアントは、証明書として、数値の UNIX ユーザー ID (UID) 及び UNIX グループ ID (GID) を持つ NFS サーバに、NFS 動作を提示します。HNAS は、UNIX から Windows への名前のマッピングを確認する前に、UID 及び GID を UNIX ユーザー（グループ）の名前にマップする必要があります。

HNAS は、以下の方法を使用して、数値の UNIX UID または GID から、UNIX ユーザー（グループ）名へのマップを実行します。

- HNAS が、特別な構成ステップのいないネットワーク情報サービス (NIS) を使用するように構成されている場合、HNAS は、ユーザー（グループ）名及び ID を、NIS サーバから自動的に取り込みます。
- NFS ユーザー名及びグループ名は、手動で追加できます。
ユーザー（グループ）マッピングの手動での追加については、「[NFS ユーザーマッピングを手動で指定する](#)」及び「[NFS グループマッピングを手動で指定する](#)」を参照してください。
- NFS ユーザー（グループ）名は、ファイルをインポートすることによって追加できます。
例えば、ユーザー名と UID のマッピングを HNAS に提示するために、UNIX `/etc/passwd` ファイルをインポートできます。また、グループ名と GID のマッピングを HNAS に提示するために、`/etc/groups` ファイルもインポートします。ファイルからのユーザー（グループ）マッピングのインポートについては、「[\(11\) ユーザーマッピングまたはグループマッピングを、ファイルからインポートする](#)」を参照してください。
- 数値 ID と名前のマッピングが既に設定されている場合、NIS サーバまたは LDAP サーバから直接インポートできます。UID が HNAS に提示されるたびに、UID は、マッピングを確認するために、NIS サーバに NIS リクエストを発行します。このマッピングのキャッシュは、設定した期間、HNAS に残せます。ユーザーまたはグループの ID と名前のバインディングのキャッシュは、NFS ユーザー（グループ）リストに「Transient」として表示されます。NIS サーバまたは LDAP サーバからのユーザー（グループ）マッピングのインポートについては、「[\(12\) NIS サーバまたは LDAP サーバから、ユーザーまたはグループをインポートする](#)」を参照してください。



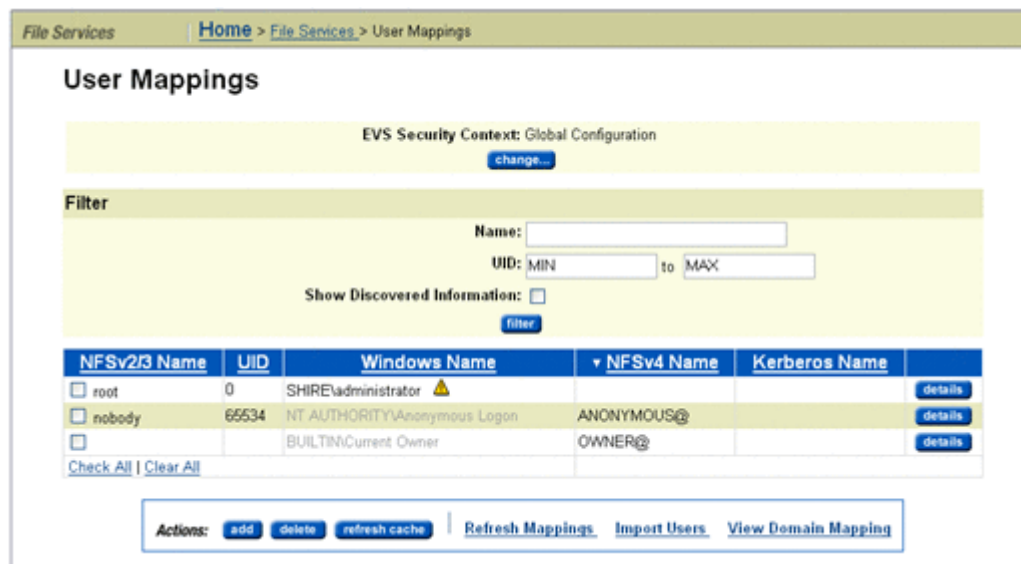
重要 Windows ユーザーがファイルを作成し、UNIX ユーザー（グループ）マッピングに失敗した場合、HNAS は UID または GID を 0 (root) に設定します。これまでのリリースでは、HNAS は、UID または GID を 0 (root) または 65534 (nobody) に設定します。

NFS ユーザーマッピングを手動で指定する

各々の UNIX ユーザー名及び数値 UID、及び対応する Windows ユーザー名及びドメイン名は、手動で入力できます。手動設定したユーザーは、NFS ユーザーリストに「permanent」として表示されます。

NFS 名を手動で指定するには

1. [User Mappings] 画面に移動します。
[File Services] 画面で [User Mappings] をクリックして、次の画面を表示します。



この画面のフィールドについて、以下の表で説明します。

項目／フィールド	説明
EVS Security Context	現在選択されている EVS セキュリティコンテキストが表示されます。別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。別の EVS セキュリティコンテキストを選択すると、マッピングが適用される EVS が変更されます。
Filter	以下の基準を使って、ユーザーマッピングのリストをフィルタリングします。 <ul style="list-style-type: none"> ・ [Name] は、NFSv2/v3、NFSv4 のユーザー名または Windows ユーザー名に適用されます。 ・ [UID] は、表示する UID 値の範囲、または表示する最少／最大 UID 値を指定するために使用できます。 ・ NIS サーバ、LDAP サーバ、またはドメインコントローラーから取得された情報のみを表示するには、[Show Discovered Information] チェックボックスをオンにします。
NFSv2/3 Name	UNIX 環境で設定されるユーザー名です。
UID	UNIX 環境で設定されるユーザー ID です。
Windows User name	Windows 環境で設定されるユーザー名です。
NFSv4 Name	NFSv4 ユーザー名を表示します。詳細については、「(8) NFSv4 のユーザー名及びグループ名」を参照してください。
Kerberos Name	ユーザーの Kerberos プリンシパル (user@realm 形式) を表示します。

2. 必要に応じて、EVS セキュリティコンテキストを変更します。

[EVS Security Context] には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面を使ってマッピングに加えられる変更は、現在選択されている EVS セキュリティコンテキストのみに適用されます。

- EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えます。
- EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のマッピングを変更するには、それらの設定がグローバルセキュリティコンテキストによって使用され

る設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。

別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。

3. ユーザーマッピングを作成、変更または削除します。
 - ユーザーマッピングを変更するには
ユーザーマッピングを変更するには、[details] をクリックして、[NFSv2/3 Name], [UID], [Windows Name], [NFSv4 Name], または [Kerberos Name] フィールドを編集して、[OK] をクリックします。
[Stored] チェックボックスをオンにし、Virtual Server が使用するセキュリティコンテキストの一部として、マッピング情報をローカルに保存します。フィールドを空欄にしたまま [Stored] チェックボックスをオンにすると、HNAS は、NIS サーバ、LDAP サーバ、またはドメインコントローラーからの情報取得を試みません。[Stored] チェックボックスがオンになっていない場合、HNAS は、このマッピングに関して NIS サーバ、LDAP サーバ、またはドメインコントローラーから取得した情報によって処理をします。
 - ユーザーマッピングを削除するには
ユーザーマッピングを削除するには、削除するユーザーマッピングの [NFSv2/3 Name] の横にあるチェックボックスをオンにしてから、[delete] をクリックします。
 - ユーザーマッピングを作成するには
NFS ユーザーのセットアップには、以下のステップが必要です。
 - a. [add] をクリックして、[Add User Mapping] 画面を表示します。
 - b. マップするユーザー情報を指定します ([NFSv2/3 Name], [UID], [Windows Name], [NFSv4 Name], または [Kerberos Name])。
 - c. [Stored] チェックボックスをオンにし、Virtual Server が使用するセキュリティコンテキストの一部として、マッピング情報をローカルに保存します。フィールドを空欄にしたまま [Stored] チェックボックスをオンにすると、HNAS は、NIS サーバ、LDAP サーバ、またはドメインコントローラーからの情報取得を試みません。[Stored] チェックボックスがオンになっていない場合、HNAS は、このマッピングに関して NIS サーバ、LDAP サーバ、またはドメインコントローラーから取得した情報によって処理をします。
 - d. [OK] をクリックします。
4. SMU のキャッシュをリフレッシュします。
SMU のキャッシュを消去し、関連オブジェクトを使って再作成するには、[refresh cache] をクリックします。これは、ブラウザの更新ボタンをクリックして、キャッシュを消去せずに最近の更新を取得することとは異なります。

NFS グループマッピングを手動で指定する

各々の UNIX グループ名及び数値 GID、及び対応する Windows グループ名及びドメイン名は、手動で入力できます。手動設定したグループは、NFS グループリストに「permanent」として表示されます。

NFS グループ名を手動で指定するには

1. [Group Mappings] 画面に移動します。
[File Services] 画面で [Group Mappings] をクリックして、次の画面を表示します。

File Services | Home > File Services > Group Mappings

Group Mappings

EVS Security Context: Global Configuration [change...](#)

Filter

Name:

GID: MIN to MAX

Show Discovered Information:

[filter](#)

<input type="checkbox"/>	NFSv2/3 Name	GID	Windows Name	NFSv4 Name	details
<input type="checkbox"/>			BUILTIN\Current Owner	OWNER@	details
<input type="checkbox"/>			NT AUTHORITY\Authenticated Users	AUTHENTICATED@	details
<input type="checkbox"/>			Everyone	EVERYONE@	details
<input type="checkbox"/>			BUILTIN\Current Group	GROUP@	details
<input type="checkbox"/>			NT AUTHORITY\NETWORK	NETWORK@	details
<input type="checkbox"/>			NT AUTHORITY\BATCH	BATCH@	details
<input type="checkbox"/>			NT AUTHORITY\INTERACTIVE	INTERACTIVE@	details
<input type="checkbox"/>			NT AUTHORITY\SERVICE	SERVICE@	details
<input type="checkbox"/>			Null		details
<input type="checkbox"/>	nogroup	65534	NT AUTHORITY\Anonymous Logon	ANONYMOUS@	details
<input type="checkbox"/>	root	0			details

[Check All](#) | [Clear All](#)

Actions: [add](#) [delete](#) [refresh cache](#) | [Refresh Mappings](#) [Import Groups](#) [View Domain Mapping](#)

次の表では、この画面のフィールドについて説明します。

項目／フィールド	説明
EVS Security Context	現在選択されている EVS セキュリティコンテキストが表示されます。特定のセキュリティコンテキスト（セキュア EVS が使用する個別セキュリティコンテキスト、またはグローバル構成のどちらか）に、マッピングが追加されます。別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。別の EVS セキュリティコンテキストを選択すると、マッピングが適用される EVS が変更されます。
Filter	以下に基づいて、グループマッピングリストをフィルタリングします。 <ul style="list-style-type: none"> ・ [Name] は、名前フィールド全てに適用されます。 ・ [GID] は、表示する GID 値の範囲、または表示する最少／最大 GID 値を指定するために使用できます。 ・ NIS サーバ、LDAP サーバ、またはドメインコントローラーから取得された情報のみを表示するには、[Show Discovered Information] チェックボックスをオンにします。
NFSv2/3 Name	UNIX 環境で設定される NFS グループ名を表示します。
GID	アカウントの出所（通常はドメイン）やアカウント名など、Windows グループアカウントに関する情報を表示します。
Windows name	アカウントの出所（通常はドメイン）やアカウント名など、Windows グループアカウントに関する情報を表示します。
NFSv4 Name	NFSv4 グループ名を表示します。

2. 必要に応じて、EVS セキュリティコンテキストを変更します。

[EVS Security Context] には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面を使ってマッピングに加えられる変更は、現在選択されている EVS セキュリティコンテキストのみに適用されます。

- EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えません。

- EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のマッピングを変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。

別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。

3. グループマッピングを作成、変更または削除します。

- グループマッピングを変更するには
グループマッピングを変更するには、[details] をクリックして、[NFSv2/3 Name], [GID], [Windows Name], または [NFSv4 Name] フィールドを編集して、[OK] をクリックします。

[Stored] チェックボックスをオンにし、Virtual Server が使用するセキュリティコンテキストの一部として、マッピング情報をローカルに保存します。フィールドを空欄にしたまま [Stored] チェックボックスをオンにすると、HNAS は、NIS サーバ、LDAP サーバ、またはドメインコントローラーからの情報取得を試みません。[Stored] チェックボックスがオンになっていない場合、HNAS は、このマッピングに関して NIS サーバ、LDAP サーバ、またはドメインコントローラーから取得した情報によって処理をします。

- グループマッピングを削除するには
グループマッピングを削除するには、削除するグループマッピングの [NFSv2/3 Name] の横にあるチェックボックスをオンにしてから、[delete] をクリックします。

- グループマッピングを作成するには

NFS グループマッピングのセットアップには、以下のステップが必要です。

- [add] をクリックして、[Add Group Mapping] 画面を表示します。
- マップするグループ情報を指定します ([NFSv2/3 Name], [GID], [Windows Name], または [NFSv4 Name])。
- [Stored] チェックボックスをオンにし、Virtual Server が使用するセキュリティコンテキストの一部として、マッピング情報をローカルに保存します。フィールドを空欄にしたまま [Stored] チェックボックスをオンにすると、HNAS は、NIS サーバ、LDAP サーバ、またはドメインコントローラーからの情報取得を試みません。[Stored] チェックボックスがオンになっていない場合、HNAS は、このマッピングに関して NIS サーバ、LDAP サーバ、またはドメインコントローラーから取得した情報によって処理をします。
- マッピングを保存するには、[OK] をクリックします。

4. SMU のキャッシュをリフレッシュします。

SMU のキャッシュを消去し、関連オブジェクトを使って再作成するには、[refresh cache] をクリックします。これは、ブラウザの更新ボタンをクリックして、キャッシュを消去せずに最近の更新を取得することとは異なります。

(11) ユーザーマッピングまたはグループマッピングを、ファイルからインポートする

ユーザーまたはグループの詳細情報は、ファイルからインポートすることによって設定できます。

このセクションでは、インポートする NFSv2/3 データ及びマッピングを指定します。NFSv4 ユーザー/グループ名は、Unix UID/GID と関連付けられる UNIX 名とは異なります。ただし、多くの環境では、NFSv4 ドメインを加えることによって、ユーザー/グループの NFSv4 名を UNIX 名から派生させることができます。HNAS は、Web Manager の [Domain Mappings] 画面上で指定する設定に基づいて、または CLI の domain-mappings-add コマンドを介して、この変換を自動実行できます。([Domain Mappings] 画面を表示するには、[File Services] 画面へ移動し、[User

Mappings] または [Group Mappings] をクリックしてから、[View Domain Mapping] リンクを選択します。domain-mappings-add コマンドの詳細については、『*Command Line Reference*』を参照してください。)

ユーザー名と UID のマッピングを HNAS に提示するために、UNIX `/etc/passwd` ファイルをインポートできます。グループ名と GID のマッピングを HNAS に提示するために、`/etc/groups` ファイルもインポートします。

HNAS は、暗号化されたパスワードやユーザーのホームディレクトリなど、`passwd` ファイルのその他のフィールドを無視します。`/etc/passwd` ファイルからインポートすることによって設定されたユーザーまたはグループは、[User Mappings] 画面または [Group Mappings] 画面の該当するリストに表示されます。

以下三つの形式から一つを選び、ファイル全体にわたって一貫して使用します。

- NFSv2/3 ユーザー/グループデータのみ

ユーザーデータのソースとして、`/etc/passwd` などの UNIX パスワードファイルを使用できます。

ネットワーク情報サービス (NIS) を使う場合、ファイルを作成するには、以下のコマンドを使用します。

```
ypcat passwd > /tmp/x.pwd
```

結果として生じるファイルは、以下の形式です。

```
john:x:544:511:John Brown:/home/john:/bin/bash
keith:x:545:517:Keith Black:/home/keith:/bin/bash
miles:x:546:504:Miles Pink:/home/miles:/bin/bash
carla:x:548:504:Carla Blue:/home/carla:/bin/bash
```

- NFSv2/3 から Windows へのユーザー/グループマッピングのみ

以下の形式のエントリを持つファイルを作成します。

```
UNIXuser="NT User", "NT Domain"
```

以下の構文ルールを使用します。

- NT ドメインはオプション。
- NFS ユーザー名には、スペースを含めない。
- NT 名はクォーテーションマークで囲む。
- ドメイン名が省略される場合、サーバドメインが代わりになる。空のドメインが必要な場合、下記のように指定することが必要。

```
users="Everyone", ""
```

この場合、「Everyone」ユーザーは、空のドメイン名を持つ唯一の共通アカウントです。

- NFSv2/3 ユーザー/グループデータ及び NFSv2/3 から Windows へのユーザーマッピングの両方

以下の形式で、エントリを持つファイルを作成します。

```
UNIXuser:UNIXid="NT User", "NT Domain"
```

NFS 名及び NT 名のルールは、NFSv2/3 から Windows へのユーザーマッピングのルールと同じです。

結果として生じるファイルは、以下の形式のエントリが含まれます。

```
john:544="john", "Domain1"
keith:545="keith", "Domain1"
miles:546="miles", "Domain1"
carla:548="carla", "Domain1"
```

ファイルをインポートすることによって、NFS ユーザー/グループマッピングを指定するには

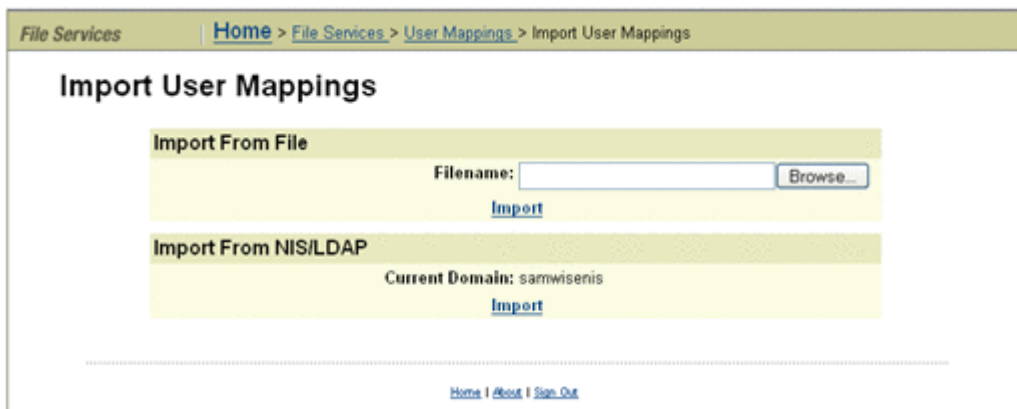
1. [User Mappings] 画面または [Group Mappings] 画面に移動します。
[File Services] 画面で [User Mappings] をクリックして [User Mappings] 画面を表示するか、または [Group Mappings] をクリックして [Group Mappings] 画面を表示します。

2. 必要に応じて、EVS セキュリティコンテキストを変更します。
[EVS Security Context] には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面を使ってマッピングに加えられる変更は、現在選択されている EVS セキュリティコンテキストのみに適用されます。

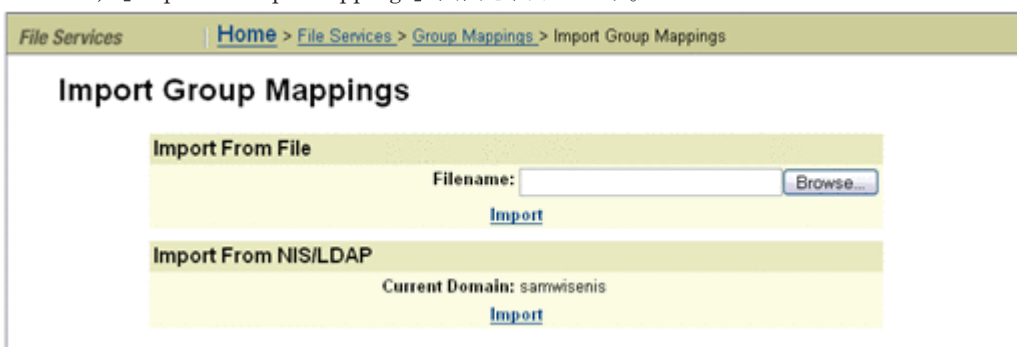
- EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えます。
- EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のマッピングを変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。

別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。

3. [Import User Mappings] 画面または [Import Group Mappings] 画面に移動します。
 - ユーザーをインポートするには、[User Mappings] 画面で [Import Users] をクリックして、[Import User Mappings] 画面を表示します。



- グループをインポートするには、[Group Mappings] 画面で [Import Groups] をクリックして、[Import Groups Mappings] 画面を表示します。



4. インポートするユーザー/グループマッピングを含んでいるファイルを指定します。
[Filename] フィールドにファイル名を入力するか、またはファイルの場所を見つけるには、[Browse] をクリックします。ファイルのユーザー/グループ名が、既に NFS リストに存在している場合、Web Manager はそれらを無視して、エラーまたはユーザーが重複したという警告を表示します。

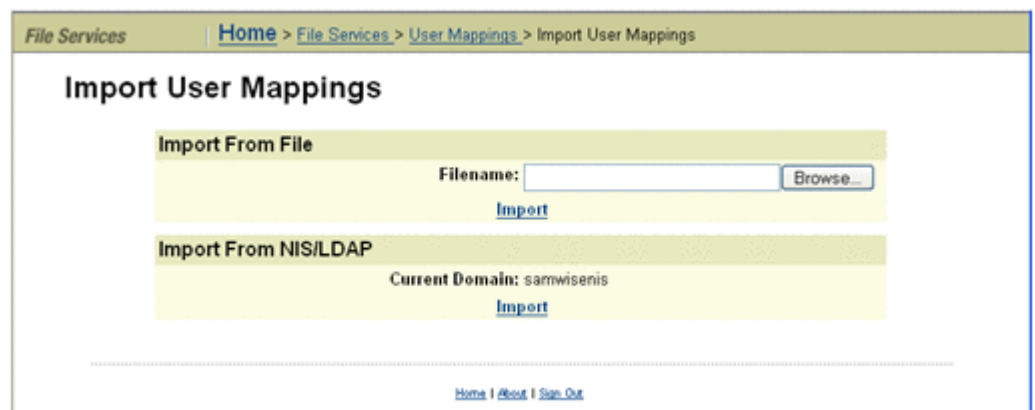
5. インポートします。
[Import] をクリックします。

(12) NIS サーバまたは LDAP サーバから、ユーザーまたはグループをインポートする

管理者は、NIS サーバまたは LDAP サーバから、ユーザーまたはグループの詳細情報をインポートできます。

NIS サーバまたは LDAP サーバから、NFS ユーザー／グループのマッピングをインポートするには

1. [User Mappings] 画面または [Group Mappings] 画面に移動します。
[File Services] 画面で [User Mappings] をクリックして [User Mappings] 画面を表示するか、または [Group Mappings] をクリックして [Group Mappings] 画面を表示します。
2. 必要に応じて、EVS セキュリティコンテキストを変更します。
[EVS Security Context] には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面を使ってマッピングに加ええられる変更は、現在選択されている EVS セキュリティコンテキストのみに適用されます。
 - EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えます。
 - EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のマッピングを変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。
3. [Import User Mappings] 画面または [Import Group Mappings] 画面に移動します。
 - ユーザーをインポートするには、[User Mappings] 画面で [Import Users] をクリックして、[Import User Mappings] 画面を表示します。



- グループをインポートするには、[Group Mappings] 画面で [Import Groups] をクリックして、[Import Groups Mappings] 画面を表示します。

File Services | [Home](#) > [File Services](#) > [Group Mappings](#) > Import Group Mappings

Import Group Mappings

Import From File

Filename:

[Import](#)

Import From NIS/LDAP

Current Domain: samwisenis

[Import](#)

4. ユーザー／グループのマッピングをインポートします。

[Import] をクリックします。[Current Domain] に表示される NIS サーバまたは LDAP サーバが接続され、マッピングをインポートします。

現在のドメインを変更するには、[NIS/LDAP Configuration] 画面に移動して [modify] をクリックし、ドメインを変更します。

ファイルのクローンを作成する

- 3.1 ファイルのクローンを作成する
- 3.2 リードキャッシュ

3.1 ファイルのクローンを作成する

WFS-2 ファイルシステムの機能を引き出すために、ファイルクローン機能は、ファイルの迅速なコピーを可能にします。これは、ソースファイルとそのコピー（「クローン」）のデータに時間が経過しても大きな差異が生じないような場合には、スペース的に効率的です。この機能は、大きなマスターファイルの、ライブ時間が長く、ほとんど変化しないコピーが必要な状況を対象としています（例えば、仮想デスクトップのために、OS ディスクイメージの多数のコピーを展開する場合など）。

ファイルのクローンが作成されると、マスターファイルのスナップショットが作成され、その時点でのソースファイルのイメージを保存します。スナップショットはファイルのスナップショットにすぎず、HNAS によってのみアクセス可能であり、読み取り専用です。このスナップショットにより、ソースファイルとクローンが共通のデータブロックを共有できます。マスターファイルの追加のクローンが作成された場合、必要に応じて、新しいスナップショットが作成されます。

クローンの最大数は、使用可能なソースによります。関連するクローンのデータの差異が大きい場合には、ファイルのクローンはスペース効率的ではありません。一部のクローンのライブ時間が短く、他のクローンのライブ時間が長い場合、クローン間で共有されたデータブロックは、全ての関連クローンとソース（マスター）ファイルが削除されない限り解放されないため、ファイルクローンの全体的なスペース効率は低下します。

ファイルクローン機能を有効にするには、FileClone ライセンスが必要です。



重要 ファイルクローン機能は、WFS-2 を使用してフォーマットされたファイルシステム内のファイルについてのみサポートされます。WFS-1 ファイルシステム内のファイルのクローンはサポートされません。また、ファイルクローン機能は、全ての Hitachi NAS Platform モデルでサポートされます。



重要 この機能が使用されると、特定のダウングレード制限が適用されます。ファイルクローンをサポートしないリリースにダウングレードした場合、ファイルクローン機能が使用されていたファイルシステムをマウントできなくなります。ファイルクローンを使用するときのダウングレード制限の詳細については、お問い合わせ先にお尋ねください。

3.1.1 ファイルのクローンを使用する

現時点では、Web Manager はファイルクローン機能のサポートを含んでいません。この機能を使用するには、CLI コマンドを使用する必要があります。ファイルクローン機能の構成と使用の詳細については、次の CLI の man 画面を参照してください。

- `file-clone`
ファイルクローン機能のメカニズムについて説明します。
- `file-clone-create`
新しいファイルを作成し、そのデータストリームをソースファイルのデータストリームのクローンにします。
- `file-clone-stat`
クローンオブジェクト、具体的には、クローンオブジェクトが依存するスナップショットファイルオブジェクトのハンドルに関する統計を表示します。
- `file-clone-report-block-sharing`
クローンとその先祖である各スナップショットファイルオブジェクトの間で共有されているブロック数を報告します。
- `file-clone-declone`
クローンされたファイルとスナップショットオブジェクトの依存関係を削除して、クローンを通常のファイルに変換します。
- `file-clone-stat-snapshot-file`
スナップショットファイルオブジェクトに関する統計を表示します。

3.2 リードキャッシュ

リードキャッシュは特殊な読み取り専用ファイルシステムであり、個々のファイルのコピーをローカルファイルシステムの外に格納して、HNAS がファイルのキャッシュコピーを持てるようにします。NFS v3 クライアントがリードキャッシュ内のファイルに対する読み取り要求を送信すると、HNAS はリードキャッシュ内のコピーから読み取り要求に応えることができます。リードキャッシュは CIFS クライアントには利点がなく、リードキャッシュには特殊な特性と制限があります。リードキャッシュについては、『*Server and Cluster Administration Guide*』を参照してください。

3.2.1 ファイルシステムアクセスプロトコル

HNAS は、クライアントファイルアクセス用の CIFS、NFS、及び FTP プロトコルと、ストレージへのブロックレベルアクセス用 iSCSI をサポートしています。サポート対象の全てのプロトコルは、有効または無効にできます。

HNAS によって、NFS、CIFS、FTP ユーザーが同一ファイル領域にアクセスできるようになります。その一方で、iSCSI 論理ユニット (LU) はファイルシステム上に存在しますが、HNAS のファイルサービス (CIFS または NFS など) を介して、iSCSI ターゲット上にあるフォルダやファイルにアクセスすることはできません。

FTP を除いて、これらのプロトコルには、アクティベーション用ライセンスキーが必要です。



重要 HNAS がプロトコル間の相違を解決する方法についての詳細は、「2.3 混合セキュリティモード」を参照してください。

3.2.2 サポートされている CIFS のバージョン

HNAS は、CIFS (SMB) バージョン 1 及び 2 をサポートしています。SMB バージョン 2 (SMB2) サポートは、Windows Vista 及び Windows Server 2008 のオペレーションシステムを実行するコンピューターとの互換性を維持するために用意されています。SMB2 サポートは、デフォルトでは無効です。有効にされた場合、SMB2 サポートは EVS ごとであり、このサポートは、クラスタ全体ではありません。つまり、SMB2 サポートは、クライアントが CIFS バージョン 2 プロトコルを使用して接続する必要がある各 EVS 上で、明確に有効にする必要があります。



重要 SMB2 サポートは、プロトコルのファイルサーバの部分に限定されます。クライアントとして動作する場合 (ドメインコントローラーとウイルススキャナーを接続する場合など)、HNAS が使用するのは、SMB バージョン 1 クライアント実装のみです。

SMB2 サポートを有効にするには、CLI の `cifs-smb2-enable` コマンドを使用します。有効にした時点で、EVS は、プロトコルのバージョン 1 またはバージョン 2 を経由して接続する CIFS クライアントをサポートします。



重要 SMB2 サポートを有効にするには、有効な CIFS ライセンスが必要です。ライセンスキーの詳細については、『*Server and Cluster Administration Guide*』を参照してください。

SMB2 サポートが有効になっている場合、確立される CIFS 接続の種類は、クライアントがサポートを通知する接続の種類に基づきます。CIFS バージョン 2 接続を確立するのは、CIFS バージョン 2 サポートを通知するクライアントのみです。バージョン 2 接続を指定せずに CIFS 接続を要求するクライアントは、CIFS バージョン 1 接続を確立します。



重要 SMB2 サポートを HNAS 上で有効にした後、CIFS バージョン 2 をサポートする一部クライアントは、再起動されるまで、CIFS バージョン 1 接続を使って接続し続ける場合があります。この状態は、一部クライアントが接続タイプをキャッシュし、接続のたびに接続タイプのネゴシエーションを実行しないことによります。この方法で動作するクライアントは、再起動されるまで、CIFS バージョン 1 を使って接続し続けます。

SMB2 サポートを無効にするには、CLI の `cifs-smb2-disable` コマンドを使用します。SMB2 サポートが無効の場合は、CIFS バージョン 1 接続のみ確立できます。クライアントが、CIFS バ

ジョン 2 接続をサポートしていることを通知した場合、HNAS は CIFS バージョン 1 接続を確立します。

CIFS バージョン 1 及び 2 クライアント接続の統計情報は保存され、[CIFS Statistics] 画面で表示できます。(詳細については、『*Server and Cluster Administration Guide*』を参照してください)。



重要 CIFS 署名は、アウトバウンド (HNAS からドメインコントローラーへ) 接続のみサポートします (これは、CIFS バージョン 1 または CIFS バージョン 2 使用時に適用されます)。

3.2.3 CIFS Unicode サポート

クライアント/デバイスと通信するために CIFS プロトコルを使用する場合、HNAS は、UCS - 2 文字エンコードをサポートします。

3.2.4 サポートされる NFS バージョン

HNAS は、NFS バージョン 3 及び 4 をサポートします。バージョン 3 では、TCP と UDP の両方をサポートしますが、バージョン 4 がサポートするのは TCP のみです。デフォルトで、サポート対象の最大バージョンは、バージョン 3 です。HNAS は、デフォルトでバージョン 3 を使用します。サポート対象の最大バージョンを NFSv4 に変更するには、CLI の `nfs-max-supported-version` コマンドを使用します。サポート対象の最大バージョンを 4 に設定することにより、HNAS が、NFS バージョン 3、及び 4 をサポートできるようになります。

(1) NFSv2/3 及び NIS Unicode サポート

クライアント/デバイスや NIS サーバと通信するために NFSv2/3 を使用する場合、デフォルトの文字セットは、ISO 8859-1 (Latin-1) です。この文字セットは、NFS クライアント及び NIS サーバいずれとの通信にも十分でないことがあります (中国語、日本語、韓国語など、Latin-1 以外の文字が必要なときなど)。そのため、NFS クライアントや NIS サーバと通信する場合には、管理者が、`protocol-character-set` コマンドを使って、使用する文字セットを指定できます。`protocol-character-set` コマンドは、以下を送受信するときに使用する文字セットを指定します。

- NFS クライアントとの送受信のためのファイル及びディレクトリ名
- NIS サーバとの送受信のためのユーザー名及びグループ

全ての NFS クライアントや全ての NIS サーバとの通信には、同一文字セットを使用します。HNAS が、NFS クライアントや NIS サーバによって文字セットを使い分けて通信するように指定することはできません。

文字セットを変更する

NFS クライアントや NIS サーバと通信するとき、HNAS は、デフォルトで ISO 8859-1 (Latin-1) 文字セットを使用します。NIS サーバと NFS クライアントが別の文字セットを使用するときは、管理者は、NFS クライアントが使用する文字セット、及び NIS サーバが使用する文字セットを指定する必要があります。

管理者は、`protocol-character-set` コマンドを使って、NFS クライアントや NIS サーバと通信する場合の文字セットを指定できます。`protocol-character-set` コマンドの詳細については、『*Command Line Reference*』を参照してください。



重要 `protocol-character-set` コマンドが発行された時点ですぐに、指定された文字セットが実際に使用されます。HNAS を再起動する必要はありません。

3.2.5 FTP プロトコルサポート

HNAS は、FTP サーバのファイルサービス機能を実装しています。HNAS に用意されているのは、以下のために必要なファイルサービス機能です。

- ファイル操作
- ディレクトリ操作
- ファイルアクセス制御（例：アクセス許可）

前提条件

システムへの FTP アクセスを許可する前に、FTP サービスを有効にする必要があります。このプロトコルに、ライセンスキーは必要ありません。

FTP 統計

HNAS の FTP 統計（10 秒のタイムスライス）は、前回の再起動から、または統計データが前回リセットされた時点からのアクティビティについて利用できます。

3.2.6 Unicode サポート

HNAS は、仮想サーバ用のファイル、ディレクトリ、移行パス、CIFS 共有、NFS 共有、ユーザー名、グループ名、ログエントリ、マウントポイントなどに関するメタデータを保存し、HNAS がサービスを行うファイルシステム及びネームスペースを保存します。

他のネットワークデバイスと相互作用する場合、HNAS によって送受信されるメタデータは、相手のネットワークデバイスがサポートしている文字セットでエンコードする必要があります。通常、CIFS（Windows）プロトコルを使うクライアント/デバイスは、データを UCS - 2 文字セットでエンコードし、NFS プロトコルを使うクライアント/デバイスは、データを UTF - 8 文字セットでエンコードします。



重要 HNAS に接続されているストレージシステムのデータが、HNAS がその時点で使用している文字セットによって、何らかの影響を受けることはありません。

(1) FTP Unicode サポート

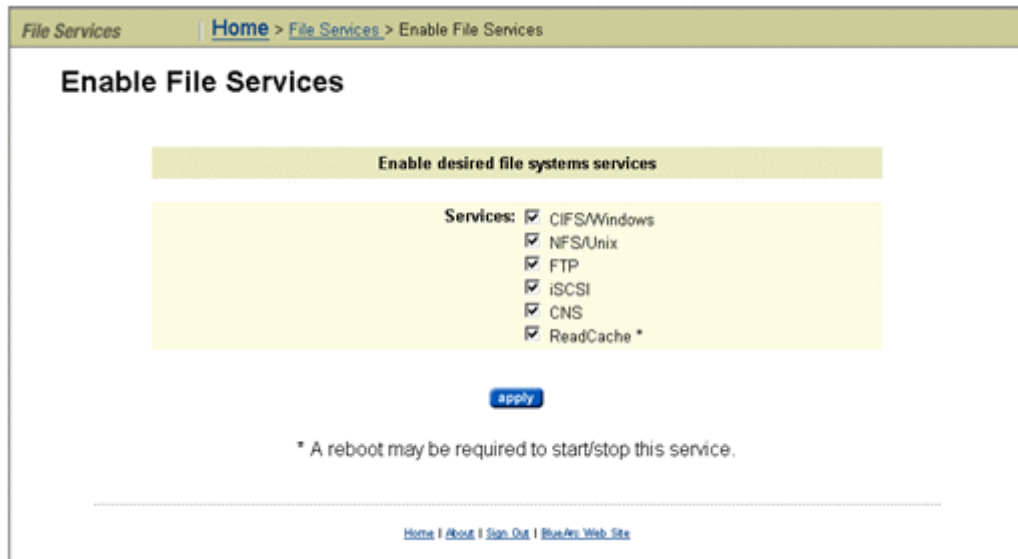
クライアント/デバイスと通信するために FTP プロトコルを使用する場合、HNAS は、ユーザー名、パスワード、及びファイル/ディレクトリ名に対して、UTF - 8 文字エンコードをサポートします。

(2) ファイルサービスを有効または無効にする

[Enable File Services] 画面を使用して、システムに必要なファイルサービスを有効または無効にします。

ファイルサービスを有効にするには

1. [Enable File Services] 画面に移動します。
[Home] 画面で [File Services] をクリックします。次に [Enable File Services] をクリックして、[Enable File Services] 画面を表示します。



2. 以下のサービスを一つ以上選択/選択解除します。

- CIFS/Windows
- NFS/Unix
- FTP
- iSCSI
- CNS
- ReadCache



重要 FTP を除いて、これらのサービスには、サービスを有効にするための、有効なライセンスが必要です。ライセンスの取得については、『*Server and Cluster Administration Guide*』を参照してください。

3. 構成を保存する

保存するには、[apply] をクリックします。

[ReadCache] が選択または選択解除された場合、再起動が必要になることがあります。その場合は、画面上の指示に従って、HNAS を再起動してください。

リソースを NFS クライアントと共有する

- 4.1 リソースを NFS クライアントと共有する
- 4.2 NFS 共有を構成する
- 4.3 rquotad サービスについて

4.1 リソースを NFS クライアントと共有する

大半の UNIX ネットワークの基本コンポーネントであるネットワークファイルシステム (NFS) プロトコルは、PC 及び UNIX ワークステーションに、お互いのファイルへのトランスペアレントなアクセスを提供します。このセクションでは、NFS 共有のセットアップ方法について記載し、また、NFS 統計データ、サポートされるクライアント、及び前提条件について説明します。

HNAS は、NFS サーバのファイルサービス機能を実装しています。備えているのは、以下などの標準的なファイルサービス機能です。

- エクスポート操作
- ファイル操作 (読み取り, 書き込み, リンク, 作成など)
- ディレクトリ操作 (mkdir, readdir, lookup など)
- バイトの範囲のファイルロック
- ファイルアクセス制御 (アクセス許可)
- ファイル及びディレクトリの属性 (サイズ, アクセス時間など)
- ハードリンク及びシンボリック (ソフト) リンク

4.1.1 NFS プロトコルサポートを有効にする

(1) 前提条件

NFS がシステムにアクセスできるようにするには

- NFS ライセンスキーを入力します。
- NFS サービスを有効にします。

(2) サポートされるクライアント及びプロトコル

HNAS は、NFS バージョン 3、またはバージョン 4 の各標準に準拠する全てのクライアントをサポートします。NFS バージョン 3 のサポートには、TCP と UDP の両方を含みますが、NFS バージョン 4 のサポートが含むのは TCP のみです。HNAS は、以下の UNIX プロトコルもサポートします。

プロトコル	サポートバージョン
NFS	3
Port Mapper	2
Mount	1 及び 3
Network Lock Manager (NLM)	1, 3, 及び 4
Network Status Monitor (NSM)	1

(3) NFS 統計

HNAS の NFS 統計 (10 秒のタイムスライス) は、前回の再起動から、または統計データが前回リセットされた時点からのアクティビティについて利用できます。

4.2 NFS 共有を構成する

NFS 共有は、マウントされたファイルシステム上で構成されます。NFS 共有は手動で構成できません。また、エクスポートの詳細設定は、ファイルからインポートできます (詳細については、

『*Snapshot Administration Guide*』を参照してください)。NFS 共有は、手動で、または、詳細設定をファイルからインポートすることによって構成できます。

4.2.1 NFSv4 疑似ファイルシステム

NFSv4 は、疑似ファイルシステム概念を採用し、エクスポートをディレクトリであるように見せます。NFSv4 クライアントは、NFSv2/3 のように NFS 共有に直接接続しません。その代わりに、全てのクライアントを、疑似ファイルシステムのルートに接続します。これが仮想ディレクトリです。疑似ファイルシステムは NFS 共有から自動で生成され、エクスポートの変更・削除時に自動的に保持されます。ユーザーは、全てのファイルシステムを単一の疑似ファイルシステムに表示するかどうかを選択できます。

HNAS は、特定の接点、ネームスペースから、多数のファイルシステムのビューを作成します。これらのビューは、EVS ごとにもまたはクラスタ全体で利用できます。

疑似ファイルシステムの例

「numbers」という名前の付いた EVS に、「/one」と「/two」の二つのエクスポートがあります。クライアントが、エクスポート「/one」にアクセスする場合、エクスポートをマウントするには、以下の二つの方法があります。

```
mount -t nfs4 numbers:/ /mnt
```

これは、疑似ファイルシステムを /mnt にマウントする方法です。

```
mount -t nfs4 numbers:/one /mnt
```

これは、エクスポート「/one」を /mnt にマウントする方法です。

一つ目の方法は NFSv4 でのみサポートされています。二つ目の方法は、バージョン 2, 3, 及び 4 でサポートされています。一つ目の方法では、クライアントは、`cd /mnt/one` コマンドを使って「/one」のエクスポートに、`cd /mnt/two` コマンドを使って「/two」のエクスポートにアクセスできます。

4.2.2 Kerberos 設定

4.2.3 NFS 共有を追加する

NFS 共有を追加するには

1. [Add Export] 画面に移動します。
[File Services] 画面で [NFS Exports] を選択し, [add] をクリックして, [Add Export] 画面を表示します。

Add Export

2. エクスポートを追加します。

[Add Export] 画面のフィールドについて、以下の表で説明します。

項目/フィールド	説明
EVS/File System	現在選択されている EVS 及びファイルシステムです。NFS 共有のリンク先となります。NFS 共有を、別の EVS またはファイルシステム（またはファイルシステムへの CNS リンク）に追加するには、[change...] をクリックします。
Export Name	エクスポートの名前です。
Path	エクスポートのソースディレクトリへのパスです（大文字と小文字を区別します）。パスの場所を見つけるには、[browse] をクリックします。
Path Options	<ul style="list-style-type: none"> • [Create path if it does not exist] : [Create path if it does not exist] のチェックがオンになっていると、[Path] フィールドに入力されたパスを作成します (EVS/File System に CNS を選択した場合、当チェックボックスは表示されません)。 • [Allow this export path to overlap other exports] : チェックがオンになっていると (デフォルト設定)、ネスト化した NFS 共有が許可されます。 <p>これを使用するのは、ファイルシステムのルートディレクトリをエクスポートして、1 ユーザーグループのみ (管理者など) が利用できるようにする場合です。その後、さらに、ルートディレクトリのサブディレクトリにエクスポートして、多様なユーザーグループが各サブディレクトリを利用できるようにします。</p>
Show snapshots	<p>以下を選択し、NFS 共有からスナップショットにアクセスできるようにします。</p> <ul style="list-style-type: none"> • [Show and Allow Access] は、スナップショットへのアクセスを表示し、許可します。 • [Hide and Allow Access] は、スナップショットを隠しますが、隠されたスナップショットへのアクセスを許可します。 • [Hide and Disable Access] は、スナップショットを隠し、アクセスも許可しません。 <p>この変更が NFS クライアントで有効になるには、全ての NFS クライアントがエクスポートをアンマウントしてから再マウントするか、または管理</p>

項目／フィールド	説明	
	<p>者が、エクスポートのルートディレクトリ内から「touch .」を実行する必要があります。</p>	
Local Read Cache	<p>このエクスポートが指すファイルシステムのファイルまたはクロスファイルシステムリンクをキャッシュできるようにするには、以下のいずれかを選択します。</p> <ul style="list-style-type: none"> • [Cache all files] : エクスポートのファイルシステムにある、ファイル及びクロスファイルシステムリンクをキャッシュできます。クロスファイルシステムリンクは、リモートファイルシステムのデータファイルを指すローカルリンクです。リモートファイルシステムは、リモートサーバ上でもストレージデバイス上でもかまいません。 • [Cache cross-file system links] : クロスファイルシステムリンクのみキャッシュできます。 • ファイル及びクロスファイルシステムリンクのキャッシュの読み取りを許可しないためには、デフォルトで選択されている [Do not cache files] を変更しないでください。 <p>NFSv4 クライアントでは、ローカルリードキャッシュをサポートしていません (EVS/File System に CNS を選択した場合、当項目は表示されません)。</p> <p>リードキャッシュの詳細については、『<i>Server and Cluster Administration Guide</i>』を参照してください。</p>	
Transfer to Object Replication Target	<p>ファイルシステムがスナップショットからリカバリーされる場合、最後の手順の一つとして、選択されたファイルシステムのバージョンを示すスナップショットで検出された NFS 共有をインポートします。転送可能なマークの付いた NFS 共有に限り、インポートされます。ドロップダウンリストを使用して、次のうち一つを指定します。</p> <ul style="list-style-type: none"> • [Enable] : NFS 共有は、リカバリーされたファイルシステムに転送されます。 • [Disable] : NFS 共有は、リカバリーされたファイルシステムに転送されません。 • [Use FS Default] (デフォルト) : ターゲットのファイルシステムがオンラインになっている場合に、[Transfer Access Points During Object Replication] がファイルシステムで有効になっていれば、NFS 共有が転送されます (EVS/File System に CNS を選択した場合、当項目は表示されません)。 	
Access Configuration	<p>NFS 共有へのアクセスが許可されるクライアントの IP アドレス、ホスト名、または NIS ネットグループです (最大 5957 文字まで)。システムがネームサーバと連携するようにセットアップされている場合、クライアントが属する NIS ネットグループを入力できます。または、クライアントの IP アドレスではなく、コンピューター名を入力できます (大文字と小文字は区別しません)。また、オプション (sec=<mode>) を使用して、NFS セキュリティの種類も指定できます。構文については、「(1) IP アドレスのエクスポート修飾子」で説明します。</p> <p>アクセス構成の設定についての詳細については、「(1) IP アドレスのエクスポート修飾子」、「(2) (IP アドレスの代わりに) 名前前でクライアントを指定する」、「2.2 NFS セキュリティ及び Kerberos」を参照してください。</p>	
	入力内容	意味
	空欄またはアスタリスク (*)	全てのクライアントが、エクスポートにアクセスできます。
	固有のアドレスまたは名前。 例 : 10.168.20.2, client.dept.company.com	指定された名前またはアドレスを持つクライアントに限り、エクスポートにアクセスできます。
Classless Inter-Domain Routing (CIDR) 表記を使用した、アドレスの範囲。	この範囲内のアドレスを持つクライアントが、エクスポートにアクセスできます。	

項目/フィールド	説明	
	例：10.168.1.0/16	
	ワイルドカードを使用した、部分的アドレスまたは部分的な名前。 例：10.168.*.*、*.company.com	一致する名前またはアドレスを持つクライアントが、エクスポートにアクセスできます。

3. 設定を保存します。

設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

(1) IP アドレスのエクスポート修飾子

NFS 共有にアクセスするクライアントを指定するときに、IP アドレスに加えることのできる修飾子について、以下の表で説明します。

修飾子	説明
read_write, readwrite, rw	読み取り/書き込みアクセスを許可します。デフォルトの設定です。
read_only, readonly, ro	読み取り専用アクセスを許可します。
root_squash, rootsquash	0 (ゼロ) のユーザー ID 及びグループ ID を、匿名ユーザーまたはグループにマップします。デフォルトの設定です。
no_root_squash, norootsquash	ルート強制割り当てをオフにします。
all_squash, allsquash	全てのユーザー ID 及びグループ ID を、匿名のユーザーまたはグループにマップします。
no_all_squash, noallsquash	全ての強制割り当てをオフにします。デフォルトの設定です。
secure	1,024 番未満の IP ポートからリクエストが発行されるように要求します。こうしたポートにアクセスできるのは、通常、クライアントマシンの管理者にかぎられています。オフにするには、[insecure] オプションを選択します。
insecure	[secure] オプションをオフにします。デフォルトの設定です。
anon_uid, anonuid	匿名ユーザー ID を明示的に設定します。
anon_gid, anongid	匿名グループ ID を明示的に設定します。
noaccess, no_access	指定クライアントがエクスポートにアクセスすることを拒否します。
(sec=<mode>)	NFS セキュリティの種類を指定できます。<mode>は、許可されたセキュリティの種類のコロン区切りのリストです (sys:krb5:krb5i:krb5p)。

以下は、いくつかの例です。

- 10.1.2.38 (ro)
10.1.2.38 という IP アドレスを持っているクライアントに、読み取り専用アクセスを許可します。
- 10.1.2.0/24 (ro)
10.1.2.0~10.1.2.255 の範囲内の IP アドレスを持っているクライアント全てに、読み取り専用アクセスを許可します。
- yourcompanydept (ro)
NIS グループ「yourcompanydept」の全員に、読み取り専用アクセスを許可します。
- *.mycompany.com(ro, anonuid=20)

「mycompany.com」で終わるコンピューター名を持っているクライアント全てに、読み取り専用アクセスを許可します。強制的に割り当てられた全てのリクエストは、ユーザー ID20 から生じる場合と同様に扱います。

- 10.1.*.* (readonly, allsquash, anonuid=10, anongid=10)
一致するクライアント全てに、読み取り専用アクセスを許可します。全てのリクエストが、ユーザー ID10, グループ ID10 と明示的に設定されている匿名ユーザーに強制的に割り当てられません。
- エントリの指定順序は重要です。以下に例を示します。
*(ro)
10.1.2.38 (rw)
1行目では、全てのクライアントに読み取り専用アクセスを許可していますが、2行目では、指定クライアントに読み取り/書き込みアクセスを許可しています。ただし、1行目は全てのクライアントに一致するため、2行目は冗長です。書き込みアクセスを 10.1.2.38 に許可するために、この2行の順序を入れ替える必要があります。
- 10.1.1.*(sec=sys),10.1.2.*(sec=krb5:krb5i:krb5p),*(sec=krb5p)
 - 10.1.1.*サブネットのクライアントは、sys 認証を使用します。
 - 10.1.2.*サブネットのクライアントは、krb5, krb5i, または krb5p を使用します。
 - その他全てのクライアントは、krb5p を使用します。



重要 性能を向上させるには、エクスポートにアクセスできるクライアントを指定するときに、ホスト名または NIS ネットグループを指定するより先に、IP アドレスまたは IP アドレスの範囲（ワイルドカードを使用しているものを含む）を指定することを推奨します。

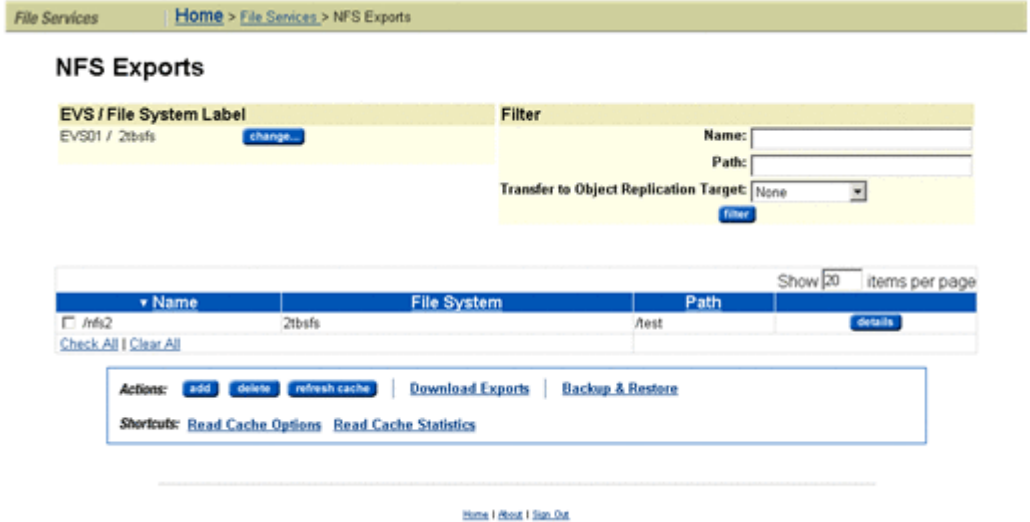
(2) (IP アドレスの代わりに) 名前でクライアントを指定する

- 完全修飾ドメイン名が必要です。必ず、クライアントの完全修飾ドメイン名を指定してください。例えば、「aclient」と指定するだけでなく、「aclient.dept.mycompany.com」と指定します。
- ワイルドカードを先頭に置くことができます。部分的な名前を指定するために、単一のワイルドカードを名前の最初に使うことができます。
- エクスポートオプションを変更するには、再マウントが必要です。クライアントが NFS 共有をマウントするときには、特定のクライアントに、どのエクスポートオプションを適用するかを判断します。その後、クライアントの IP アドレスから別のコンピューター名への解決を行う DNS, WINS, または NIS に変更を加えた場合は、クライアントがエクスポートをアンマウントしてから再マウントしたときに、マウントされたエクスポートに対してのみ適用されます。
- ネームサーバの順序は重要です。クライアントのマウントリクエストに対してエクスポートオプションを適用する場合、IP アドレスを解決するためにシステムが DNS, WINS, 及び NIS 情報を適用する順序に影響される場合があります。クライアント名を解決できる名前の順序の最初のサービスが、名前を供給し、かつエクスポートの構成オプションを検索します。

4.2.4 NFS 共有のプロパティを表示する

NFS 共有のプロパティを表示するには

1. [NFS Exports] 画面に移動します。
[File Services] 画面で [NFS Exports] をクリックして、以下の画面を表示します。



[NFS Exports] 画面のフィールドについては、以下の表で説明します。

項目/フィールド	説明
EVS/File System Label	NFS 共有が割り当てられる EVS 及びファイルシステムの名前です。別の EVS またはファイルシステムの NFS 共有を表示するには、[change...] をクリックします。
Filter	テーブルを名前、パス、[Transfer to Object Replication Target] の設定値でフィルタリングできます (EVS/File System に CNS を選択した場合、当項目は表示されません)。 [filter] をクリックして、NFS 共有のテーブルを表示します。
Name	NFS 共有の名前です。
File System	NFS 共有が割り当てられるファイルシステム (またはファイルシステムへの CNS リンク) の名前です。
Path	NFS 共有先のパスとディレクトリです。
Details	[details] をクリックして、[NFS Export Details] 画面を表示すると、NFS 共有についての詳細情報を表示できます。
Actions	
add	NFS 共有を追加するには、ファイルシステムを選択して、[add] をクリックします。
delete	NFS 共有を削除するには、NFS 共有を選択して [delete] をクリックします。
refresh cache	SMU のキャッシュを消去し、その後、関連オブジェクトを使って再作成します。これは、ブラウザの更新ボタンをクリックして、キャッシュを消去せずに最近の更新を取得することとは異なります。
Download Exports	選択した EVS 及びファイルシステム上にある、全ての構成済み NFS 共有のリストをカンマ区切り (.csv) ファイルでダウンロードするには、[Download Exports] をクリックします。ダウンロードファイルを使用して、NFS 共有を復元することはできませんので注意してください (NFS 共有は、NFS 共有バックアップファイルから復元する必要があります)。別のファイルシステムからエクスポートリストをダウンロードするには、[change...] をクリックします。
Backup & Restore	[NFS Export Backup & Restore] 画面を表示します (詳細については、「4.2.5 NFS 共有をバックアップ及び復元する」を参照してください)。

2. [NFS Export Details] 画面に移動します。

[NFS Exports] 画面で、エクスポートを選択して [details] をクリックします。

File Services | [Home](#) > [File Services](#) > [NFS Exports](#) > NFS Export Details

NFS Export Details

File System: G1_Tar_02 [change...](#)

Export Name: /exptestrep

Path: / [browse...](#)

Path Options

These options only apply when 'path' or 'file system' values are changed.

Create path if it does not exist. (See online help for security implications).

Allow this export path to overlap other exports.

Show snapshots: Show and Allow Access ▾

Local Read Cache: Do not cache files ▾

Transfer to Object Replication Target: Use FS Default ▾ (The File System Default: Enabled)

Access Configuration:

(Enter IP-based values first, if possible)

[OK](#) [cancel](#)

[Home](#) | [About](#) | [Sign Out](#)

3. 必要に応じて、エクスポートの設定を変更します。
[NFS Export Details] 画面の項目とフィールドの説明については、「4.2.3 NFS 共有を追加する」を参照してください。
4. 変更を保存します。
設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

4.2.5 NFS 共有をバックアップ及び復元する

NFS 共有をバックアップするときは

- バックアップ範囲
全ての EVS 上にある、全ての NFS 共有をバックアップします (CNS ツリー上にある NFS 共有は除きます)。
- バックアップ形式
NFS 共有バックアップファイルは、.txt ファイルとして保存されます。

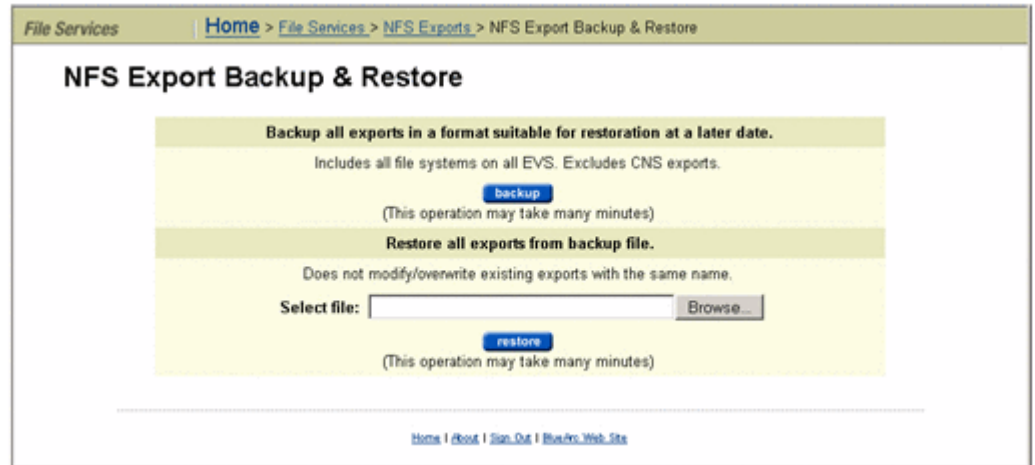
バックアップファイルから NFS 共有を復元するときは

- 復元操作により、現在存在している同名のエクスポートが変更されたり上書きされたりすることはありません。
- 上記の場合を除き、選択されたバックアップファイルの全てのエクスポートが復元されます。

NFS 共有をバックアップまたは復元する

NFS 共有をバックアップまたは復元するには

1. [NFS Export Backup & Restore] 画面に移動します。
[File Services] 画面で [NFS Exports] を選択し、[Backup & Restore] をクリックして、[NFS Export Backup & Restore] 画面を表示します。



2. バックアップまたは復元を実行します。

- バックアップするには：

[backup] をクリックします。ブラウザで、バックアップファイルの名前と場所を指定し、[OK/Save] をクリックします（表示されるボタンと、バックアップファイルを保存する方法は、使用しているブラウザによって異なります）。

バックアップファイル名が提案されますが、カスタマイズできます。提案されたファイル名が使用している構文は、NFS_EXPORTS_日付_時間.txt です。以下は、適切な構文の例です。

NFS_EXPORTS_Aug_4_2006_11_09_22_AM.txt

- 復元するには：

[restore] をクリックします。ブラウザで、復元する特定のエクスポートのバックアップテキストファイル（NFS_EXPORTS_日_時間.txt）を選択し、[Open] をクリックします。

[NFS Export Backup & Restore] 画面に選択したファイルの名前と場所が表示されたら、[restore] をクリックします。

NFS 共有を削除する



注意 エクスポートを削除するときは注意してください！ エクスポート削除の手順を実行する前に、そのエクスポートに、ユーザーがアクセス中でないかどうかを確認してください。ユーザーがアクセス中のエクスポートを削除すると、NFS セッションは終了し、保存されていないデータが失われる可能性があります。ストレージシャーシを交換するときには、関連付けられている全てのエクスポートを削除してください。その後、シャーシの交換品が利用できるようになったら、新しいシステムドライブに新しいエクスポートを追加します。

4.3 rquotad サービスについて

rquotad プロトコルは、HNAS のサービスとして実装されています。読み取り専用プロトコルとして機能し、ユーザー Quota 及びグループ Quota に関する情報の報告にのみ関与します。Quota は、Web Manager の [Storage Management] セクション経由で作成、削除、または変更できます。

Unix/Linux NFS クライアントは、quota コマンドを発行し、ID に基づいて、ユーザーまたはグループの Quota 使用量に関する情報を取得します。取得したレポートには、ブロック数、ファイル数、ならびにブロック数とファイル数の Quota 制限などの情報が含まれます（コマンドで起動するオプションに基づきます）。実装方法はクライアントのオペレーティングシステムによって異なるため、正確な構文については、クライアントの [man] 画面を参照してください。

HNAS は、rquotad 経由で [Hard Limit] の Quota 情報のみを報告します。以下の 3 種類の Quota 制限を定義できます。

- ・ 仮想ボリューム内で、個人やグループのスペースや、ファイル数を制限するための、ユーザー Quota 及びグループ Quota
- ・ ファイルシステム全体で、個人やグループのスペースや、ファイル数を制限するための、ユーザー Quota 及びグループ Quota
- ・ 仮想ボリューム単位で、スペースやファイル数を制限するための、仮想ボリューム Quota



重要 rquotad が報告するのは、明示的に定義された Quota 及び自動的に作成された（デフォルト）Quota の Quota 使用量情報です。デフォルト Quota 情報の報告は、明示的な Quota が定義されていない場合に行われま

4.3.1 rquotad サービスの設定

以下のいずれかの方法を使用して、Quota 情報の報告を行うよう、rquotad サービスを設定できます。

- ・ 制限モード

rquotad サービスは、クライアント側の quota コマンドが指定したユーザーまたはグループについて、最も制限の多い Quota の Quota 情報を報告します。

- ・ マッチングモード

rquotad サービスは、クライアント側の quota コマンドが指定したユーザーまたはグループについて、クライアント側の quota コマンドが定義するパラメーターに一致する第 1Quota の Quota 情報を報告します。



重要 rquotad サービスが無効になっている場合は、全てのリクエストが、エラーコード「EPERM」で拒否されます。

4.3.2 制限モードでの運用

制限モードでは、rquotad サービスは、最初に超えた Quota のしきい値を選びます。それにより、ユーザーは、データ量が [Hard Limit] に達する前に、この Quota で安全に記録できるデータ量を判断できるようになります。これは、HNAS の rquotad に対するデフォルト構成オプションです。



重要 制限モードオプションは、最も制限の厳しい使用量 Quota と、最も制限の厳しいファイル数 Quota を組み合わせて、Quota 情報を返します。以下は、その例です。

容量 10K 及びファイル数 100 を追加できるユーザー Quota と、容量 100K 及びファイル数 10 を追加できる仮想ボリューム Quota がある場合、rquotad は、容量 10K 及びファイル数 10 を追加できるという情報を返します。同様に、容量 10K のユーザー Quota のうち 5K が使用されており、容量 100K の仮想ボリューム Quota のうち 99K が使用されている場合、rquotad は、1K のデータを追加できるという情報を返します。

この二つのオプション間の変更を行うために、コンソールコマンド rquota が用意されています。Quota 情報へのアクセスの無効化も、このコマンドで行えます。rquotad の設定方法については、『*Command Line Reference*』を参照してください。

4.3.3 マッチングモードでの運用

マッチングモードの場合、rquotad サービスは、特定の順序に従って、該当する Quota 情報の一致を検出します。

- ・ rquotad がユーザーの Quota 情報を返す場合、仮想ボリューム内でのユーザー Quota が存在していれば、この仮想ボリューム内でのユーザー Quota を返します。

- 上記が存在しない場合、ファイルシステムでのユーザー Quota が存在していれば、rquotad は、このファイルシステムでのユーザー Quota を参照します。
- ファイルシステムでのユーザー Quota が存在していない場合、rquotad は、仮想ボリューム Quota を参照します。

このように、rquotad は、特定のユーザーまたはグループの Quota が検出されるまでチェックを続けます。一致する Quota が最初に検出された時点で、rquotad は検索を中止して、Quota 情報を返します。

ユーザーに対して、仮想ボリューム内またはファイルシステムでの Quota を定義しておらず、仮想ボリューム Quota が容量 100K 及びファイル数 10 を全ユーザーに許可している場合、rquotad は、ユーザーの Quota は容量 100K 及びファイル数 10 であるという情報を返します。同様に、ユーザーに対して、容量 200K 及びファイル数 20 の仮想ボリューム内での Quota と、容量 400K 及びファイル数 40 のファイルシステムでの Quota が指定されている場合は、rquotad は、容量 200K 及びファイル数 20 を追加できるという、最初の Quota のみに関する情報を返します。

Windows アクセスに CIFS を使用する

- 5.1 Windows アクセスに CIFS を使用する

5.1 Windows アクセスに CIFS を使用する

Windows ネットワークは、クライアントと HNAS との間のファイル共有のために、共通インターネットファイルシステム (CIFS) プロトコルを使用します。

5.1.1 CIFS プロトコルサポート

HNAS は、Windows 2003、及び Windows 2008 サーバのファイルサービス機能をエミュレートします。クライアントは、HNAS と Windows サーバとの差異を意識せずにアクセスすることができます。HNAS は、以下をはじめとする通常のファイルサービス機能の全てを備えています。

- 共有操作 (追加, 一覧表示, 削除など)
- ファイル操作 (読み取り, 書き込み, 作成, 削除, 移動, コピーなど)
- ファイルのロック及びバイト範囲のロック
- 標準 Windows ACL を用いたファイルアクセス制御
- ファイル及びディレクトリの属性 (読み取り専用, アーカイブなど)
- ユーザーホームディレクトリの自動作成

(1) 前提条件

HNAS への CIFS アクセスを有効にするには

- CIFS ライセンスキーを入力します。
- CIFS サービスを有効にします。
- HNAS を構成します。

CIFS ネットワークで使用されるセキュリティモデルに応じて、以下の方法のいずれかを使って HNAS を構成します。

セキュリティモデル	クライアント認証	構成方法
Windows 2003, 及び 2008 Active Directory	Kerberos	Active Directory に参加する

(2) サポートされるクライアント

HNAS は、CIFS (SMB) バージョン 1 及び 2 に準拠しているプラットフォーム及びクライアントをサポートします。

(3) ドメインコントローラーとの連携

HNAS は、Windows ドメインコントローラーに依存して、ユーザーを認証し、ユーザー情報 (グループメンバーシップなど) を取得します。HNAS は、安定性の最も高い、最速のドメインコントローラーを自動的に検出し、接続します。操作条件が徐々に変化する場合がありますため、HNAS は 10 分ごとに「最善」のドメインコントローラーを選択します。

デフォルトでは、Active Directory でクライアントを認証するときに、HNAS は、ドメインコントローラーによって維持されている時間を使用して、自動的に時刻を合わせます。

(4) 動的 DNS

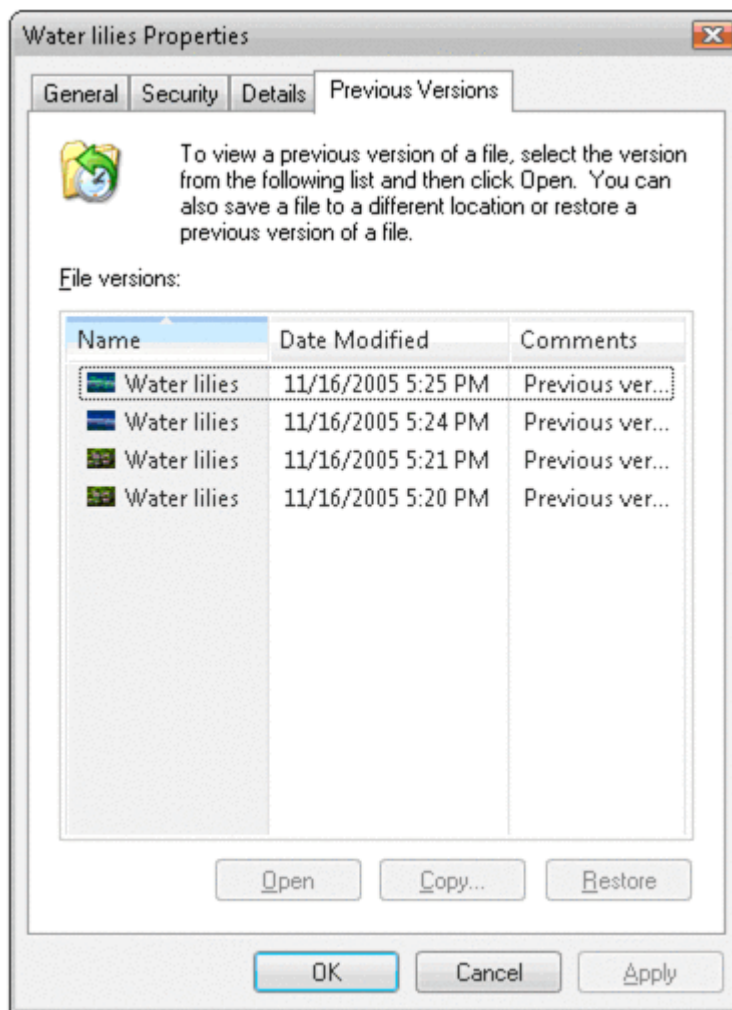
HNAS は、DNS 及び DDNS をサポートします。詳細については、『*Network Administration Guide*』を参照してください。

CIFS 統計

HNAS の CIFS 統計（10 秒のタイムスライス）は、前回の再起動から、または統計データが前回リセットされた時点からのアクティビティについて利用できます。

5.1.2 ファイルを以前のバージョンに復元する

CIFS クライアントは、あるファイル/ディレクトリを含んでいるスナップショットが存在する限り、共有に保存されているそのファイルの以前のバージョンにアクセスできます。以前のバージョンをスナップショットから入手できるファイル及びフォルダの [Properties] 画面には、[Previous Versions] タブが表示されます。このタブには、入手できる前バージョンと、その前バージョンに対応する時間のリストが表示されます。



このタブでは、一覧表示された以前のバージョンにアクセスし、復元することができます。

5.1.3 CIFS セキュリティを構成する

HNAS は、既存のドメインにシームレスに統合し、既存ドメインユーザーアカウントに対する全ての認証を実行して、アクセス制御を簡略化します。



重要 ドメインまたは信頼されたドメイン内で作成されたアカウントに限り、HNAS にアクセスできます。

ユーザーが共有へアクセスしようとする時、HNAS は、ユーザがその共有にアクセスする適切な権限を持っているか確認します。このレベルでアクセスが許可されたら、標準的なファイルアクセス許可、及びディレクトリアクセス許可が適用されます。

HNAS は特定のドメインで動作し、オプションとして Active Directory に参加できます。また、ユーザーの証明書の妥当性を確認するため、そのドメインのドメインコントローラー (DC) と連携します。HNAS は、Active Directory に対する Kerberos ベースの認証を、(pre-Windows 2000 プロトコルを使用して) サポートします。このドメインに属しているユーザーの他、HNAS は、信頼されたドメインのメンバーが、CIFS 経由で接続できるようにします。

HNAS は、DC が認証したドメイン管理者に、管理者特権を自動的に付与します。さらに、選択されたグループ (またはユーザー) に対するバックアップオペレーター特権を含めて、ローカル管理特権を割り当てることができます。

CIFS 名を割り当てる

HNAS は CIFS 名をドメインコントローラーに登録します。Windows クライアントは、ドメインコントローラーに登録された CIFS 名を用いて HNAS にアクセスします。従来の Windows サーバでは、ホスト名は一つしか持てませんが、複数の Windows サーバを HNAS に統合する状況に対応するために、HNAS は複数の CIFS 名を構成することができます。

Windows ネットワーク上で CIFS 名を独立した 1 台の Windows サーバであるかのように見せるために、HNAS は CIFS 名ごとに以下を実行します。

- Computer Management 管理ツールによる管理を許可する。
- NetBIOS が有効の場合、各 CIFS 名をドメインマスターブラウザに登録して、[マイネットワーク] で各 CIFS 名が一意のサーバとして表示されるようにする。
- 適切なホスト名解決を行うために、各 CIFS 名を DDNS または WINS に登録する。
- EVS ごとに最大 256 件までの CIFS 名をサポートする。

(1) Active Directory (AD) に参加する

Active Directory に参加するには、CIFS サーバ名を追加する必要があります。設定されたそれぞれの CIFS 名について、対応するコンピューターアカウントが Active Directory に存在することが必要です。コンピューターアカウントは、「Active Directory Users and Computers」ツールを使用して、任意のフォルダにあらかじめ作成できます。コンピューターアカウントが存在しない場合には、CIFS 名がサーバ構成に追加されたときに、HNAS は対応するコンピューターアカウントを [Computers] フォルダに追加します。



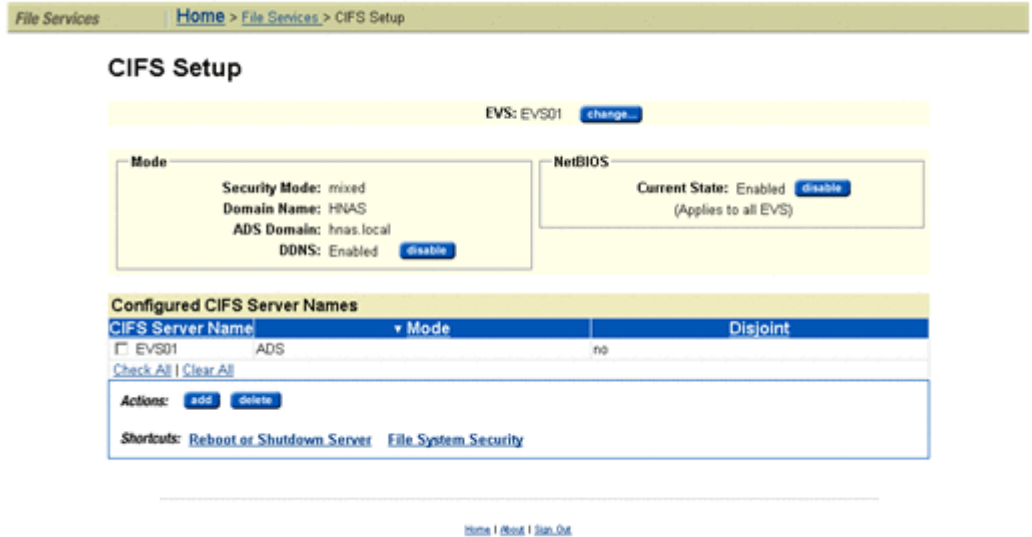
重要 セキュリティのため、Microsoft AD と参加するコンピューターとの時刻のずれは 5 分以内にする必要があります。AD への参加を試みる前に、HNAS の時刻が適切に設定され、ドメインと同期されていることを確認してください。



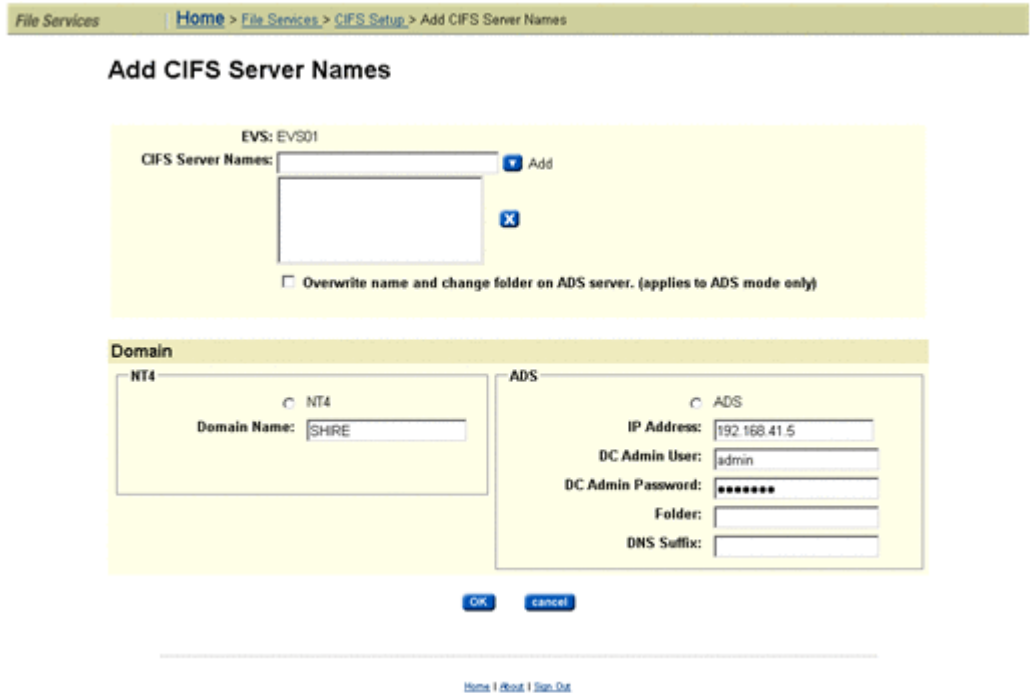
重要 HNAS を Microsoft Windows 2008 の AD に追加するには、その HNAS 上で NetBIOS を無効にする必要があります。AD に参加した後は、NetBIOS を有効にできます。ただし、NetBIOS は Windows 2008 では推奨されていません。

Active Directory に参加するには

1. [CIFS Setup] 画面に移動します。
[File Services] 画面で、[CIFS Setup] をクリックして [CIFS Setup] 画面を表示します。



2. Virtual Server (EVS) を選択します。
[change...] をクリックし、[Select an EVS] 画面で EVS を選択します。
3. [Add CIFS Server Names] 画面に移動します。
[CIFS Setup] 画面で、[add] をクリックして [Add CIFS Server Names] 画面を表示します。



次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
CIFS Server Names	CIFS クライアントが HNAS 上のファイルサービスにアクセスするのに使用するコンピューター名です。ADS ドメインでは、CIFS サーバ名の最大文字数は 63 文字です。NT4 ドメインでは、CIFS サーバ名の最大文字数は 15 文字です。
Overwrite name and change folder on ADS server	このチェックボックスをオンにすると、ADS サーバで名前が上書きされ、フォルダが変更されます (ADS モードのみ有効)。
Domain	CIFS サーバが NT4 ドメインと ADS ドメインのどちらに属するかを設定します。そのドメインに属するために必要な設定も同時にできます。

項目/フィールド	説明
NT4	CIFS サーバを NT4 ドメインに属するように設定するには、[NT4] ラジオボタンを選択します。
Domain Name	CIFS サーバを追加する NT4 ドメインの名前です。
ADS	CIFS サーバを ADS ドメインに属するように設定するには、[ADS] ラジオボタンを選択します。
IP Address	CIFS サーバが参加する Active Directory のドメインコントローラーの IP アドレスです。
DC Admin User	ドメイン管理者グループメンバーのユーザーアカウントです。この特権は、Active Directory にコンピューターアカウントを作成するために必要です。 注：信頼されたドメインからユーザーアカウントを指定する場合、ユーザーアカウントは、「administrator@ADdomain.mycompany.com」という Kerberos 形式で入力する必要があります。「ADdomain¥administrator」ではありません。
DC Admin Password	ドメイン管理者ユーザーのパスワードです。
Folder	コンピューターアカウントを作成する、Active Directory のフォルダです。デフォルトでは、コンピューターアカウントは [Computers] フォルダに作成されます。
DNS Suffix	Active Directory ドメインのプライマリ DNS サフィックス以外の DNS サフィックスを設定する必要がある場合に限り、このオプションを使用します。(例えば、結合が解除されたドメインがある場合に設定します。)

4. CIFS サーバ名を指定します。

CIFS サーバを追加するには、[CIFS Server Names] フィールドに CIFS サーバ名を指定します。

5. [ADS] ラジオボタンを選択します。

[Domain] エリアで、[ADS] ラジオボタンを選択します。

ADS ドメインに参加するときは、CIFS サーバ名を追加する必要があります。設定されたそれぞれの CIFS 名について、対応するコンピューターアカウントが Active Directory に存在することが必要です。コンピューターアカウントは、「Active Directory Users and Computers」ツールを使用して、任意のフォルダにあらかじめ作成できます。コンピューターアカウントが存在しない場合には、CIFS 名がサーバ構成に追加されたときに、HNAS は対応するコンピューターアカウントを [Computers] フォルダに追加します。



重要 セキュリティのため、Microsoft AD と参加するコンピューターとの時刻のずれは 5 分以内にする必要があります。AD への参加を試みる前に、HNAS の時刻が適切に設定され、ドメインと同期されていることを確認してください。

6. ADS ドメインを設定します。

ADS ドメインエリアに、追加する CIFS サーバのための ADS ドメインの設定を入力します。

a. ADS ドメインの DC の IP アドレスを指定します。

[IP Address] フィールドで、Active Directory のドメインコントローラーの IP アドレスを指定します。

b. DC 管理者ユーザー名を指定します。

[DC Admin User] フィールドに、ドメイン管理者グループのメンバーであるユーザーアカウントを指定します。この特権は、Active Directory にコンピューターアカウントを作成するために必要です。



重要 信頼されたドメインからユーザーアカウントを指定する場合、ユーザーアカウントは、「administrator@ADdomain.mycompany.com」という Kerberos 形式で入力する必要があります。「ADdomain¥administrator」ではありません。

c. DC 管理者ユーザー名と関連付けられているパスワードを指定します。

[DC Admin Password] フィールドに、上で指定した DC 管理者ユーザー名と関連付けられているパスワードを指定します。

- d. コンピューターアカウントフォルダを指定します。

[Folder] フィールドに、コンピューターアカウントを作成する Active Directory のフォルダのフォルダ名を指定します。デフォルトでは、コンピューターアカウントは、[Computers] フォルダに作成されます。

7. 構成を保存します。

[OK] をクリックして、構成を保存します。または、[cancel] をクリックして、[CIFS Setup] 画面に戻ります。

(2) CIFS サーバ名を削除する

設定された CIFS サーバ名のリストから CIFS サーバ名を削除すると、その CIFS サーバ名をサーバ構成から削除できます。ADS CIFS 名が削除されると、Active Directory 上にある対応するコンピューターアカウントも削除されます。NT 4 ドメインのコンピューターアカウントは、Server Manager から手動で削除する必要があります。



注意 CIFS 名を削除するときは注意してください！

Windows クライアントからの接続をサポートするには、HNAS 上に、少なくとも一つの CIFS 名を構成する必要があります。したがって、設定された最後の CIFS 名が削除されると、Windows クライアントが、CIFS で HNAS にアクセスできなくなります。



重要 CIFS サーバ名を削除しても、DNS エントリの登録は自動的に解除されません。そのため管理者は、CIFS サーバ名のエントリを DNS から手動で削除してください。

(3) NetBIOS を使用する

NetBIOS を有効にすると、HNAS 上の NetBIOS 及び WINS を許可します。HNAS が、旧バージョンの Windows コンピューターと NetBIOS 名で通信するためには、この設定が必要です。デフォルトでは、HNAS は NetBIOS を使用するよう構成されます。

NetBIOS を無効にすると、以下のようないくつかの利点があります。

- SMB トラフィックの転送を簡易化します。
- 名前解決の手段として、WINS 及び NetBIOS のブロードキャストをしなくなるためネットワークの負担が軽減します。
- ファイル共有のために、DNS による名前解決を一般的に使用します。

CIFS 名を削除する (NetBIOS を無効にする)



注意 NetBIOS は、安定した DNS インフラストラクチャーがある場合に限り、無効にしてください。NetBIOS を無効にする前に、そのネットワーク接続で NetBIOS、WINS、または従来の NetBT 型アプリケーションを使用する必要がないことを確認してください。無効にしてしまうと、クライアントは、DNS を介して名前ではか HNAS に接続できなくなります。NetBIOS を無効にすることで、Windows の旧バージョンのユーザーに接続性の問題が発生する可能性があります。

HNAS が、Windows 2000 以降のバージョンの Windows を実行するコンピューターとしか通信しない場合、NetBIOS の無効化によるクライアントへの影響はなく、性能上の利点が生じることがあります。これは、CIFS 名及び IP アドレスの動的な DNS 登録が、安定した接続性を確保する簡単な方法であるためです。

NetBIOS を無効にするには、[File Services] 画面に移動し、[CIFS Setup] をクリックして、[CIFS Setup] 画面を表示します。

CIFS Setup

EVS: EVS01 [change...](#)

Mode

Security Mode: mixed

Domain Name: HNAS

ADS Domain: hnas.local

DDNS: Enabled [disable](#)

NetBIOS

Current State: Enabled [disable](#)

(Applies to all EVS)

Configured CIFS Server Names

CIFS Server Name	Mode	Disjoint
<input type="checkbox"/> EVS01	ADS	no

[Check All](#) | [Clear All](#)

Actions: [add](#) [delete](#)

Shortcuts: [Reboot or Shutdown Server](#) [File System Security](#)

[Home](#) | [Back](#) | [Sign Out](#)

[NetBIOS] メニューの [disable] をクリックして、NetBIOS を無効にします。メッセージが表示されたら、クラスタを再起動してください。

5.1.4 ローカルグループを構成する

Windows セキュリティドメインでは、ユーザー及びグループは、ネットワーク上のユーザー（例：vsmith）及びユーザーグループ（例：software）を識別します。ユーザーが定義するネットワークグループ名（例：software, finance, test など）とは別に、Windows は、各自が構成されたサーバへのアクセスに関するさまざまな特権とレベルを各々備えている多数の組み込みグループ、または「ローカル」グループをサポートします。

こうしたグループは、Windows コンピューターごとに存在します。これらのグループは、ネットワークグループではなく、各コンピューターのローカルグループです。例えば、jamesg というユーザーは、あるコンピューター上で管理者特権を与えられているけれども、別のコンピューター上では管理者特権を与えられていないというケースもあります。HNAS も同様に、管理者は、ユーザーをローカルグループに追加できますが、現在有効なのは、以下の四つのグループのみです。

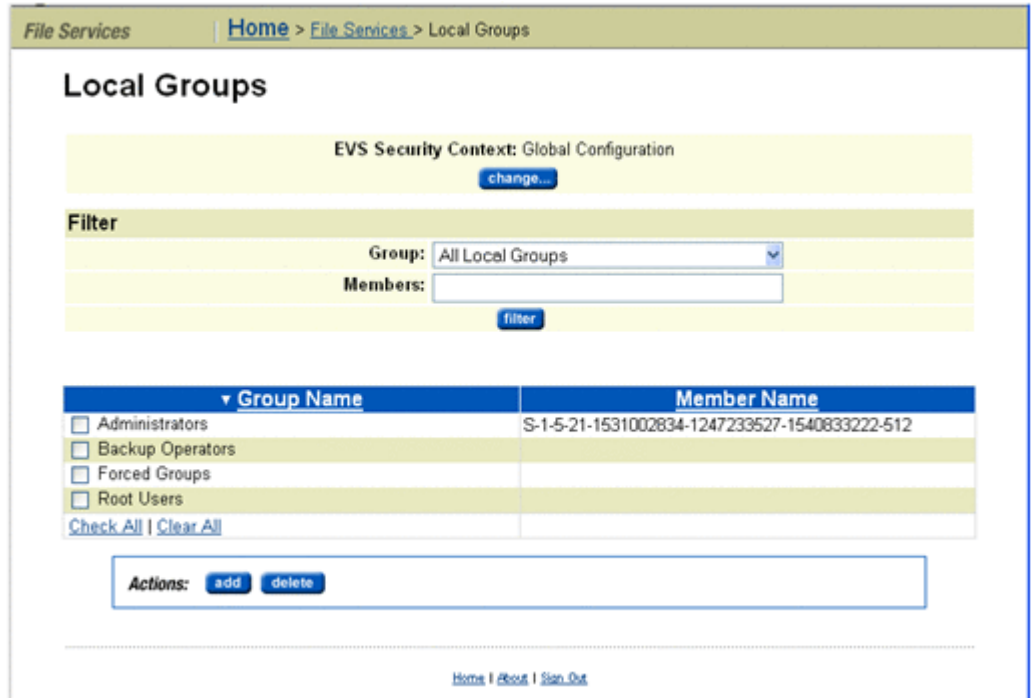
- **Root**
ユーザーがローカル Root グループのメンバーである場合、ユーザーは、全てのセキュリティチェックを回避し、ファイルシステムの全てのファイルの所有権を得ることができます。
- **Administrators**
ユーザーがローカル Administrators グループのメンバーである場合、ユーザーは、ファイルシステムの全てのファイルの所有権を得ることができます。
- **Backup Operators**
ユーザーが、ローカル Backup Operators グループのメンバーである場合、ユーザーは、全てのセキュリティチェックを回避できますが、ファイルシステムのファイルの所有権を得ることはできません。ファイルシステムの全てのセキュリティチェックを回避する特権は、Backup Exec を実行するアカウントまたはウィルススキャンを実行するアカウントに必要です。ただし、Backup Operators グループの一部であるウィルススキャンサーバは、ファイルシステムの全てのファイルの所有権を得ることができます。
- **Forced Groups**
ユーザーがローカル Forced Groups グループのメンバーである場合、ユーザーがファイルを作成すると、そのユーザーが定義されたプライマリグループは上書きされ、ファイル作成者名にはそのユーザーのユーザーアカウントが使用されます。

(1) ローカルグループまたはローカルグループメンバーを追加する

ローカルグループを追加するには

1. [Local Groups] 画面に移動します。

[File Services] 画面で [Local Groups] をクリックして、[Local Groups] 画面を表示します。



2. 必要に応じて、EVS セキュリティコンテキストを変更します。

[EVS Security Context] には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面で行ったローカルグループの変更は、現在選択されている EVS セキュリティコンテキストにのみ適用されます。

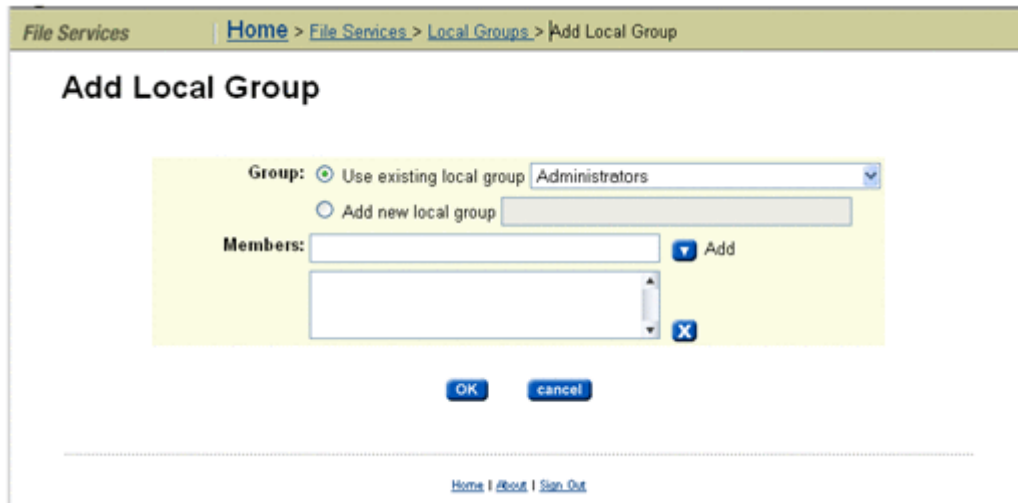
- EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えます。
- EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のローカルグループを変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。

別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。

3. 新しいローカルグループまたはメンバーを追加します。

- a. [Add a Local Group] 画面に移動します。

[add] をクリックして、[Add a Local Group] 画面を表示します。



- b. 新しいグループの名前を入力するか、またはユーザーを追加するグループを選択します。
- 新しいローカルグループを追加するには、[Add new local group] ラジオボタンを選択し、フィールドに新しいローカルグループの名前を入力します。
 - ユーザーを既存のローカルグループに追加するには、[Use existing local group] ラジオボタンを選択し、ドロップダウンメニューから既存のローカルグループを選択してください。
- c. グループメンバーを指定します。
- ローカルグループに追加するユーザーの名前を [Members] フィールドに入力し、下矢印をクリックして、ユーザーをメンバーシップリストに追加します。このステップを必要なだけ繰り返して、複数のメンバーを同時に追加できます。
- メンバーシップリストから名前を削除するには、削除する名前を選択して、[x] をクリックします。
- d. 新しいローカルグループ/グループメンバーを保存します。
- [OK] をクリックして、新しいローカルグループ/グループメンバーを保存します。

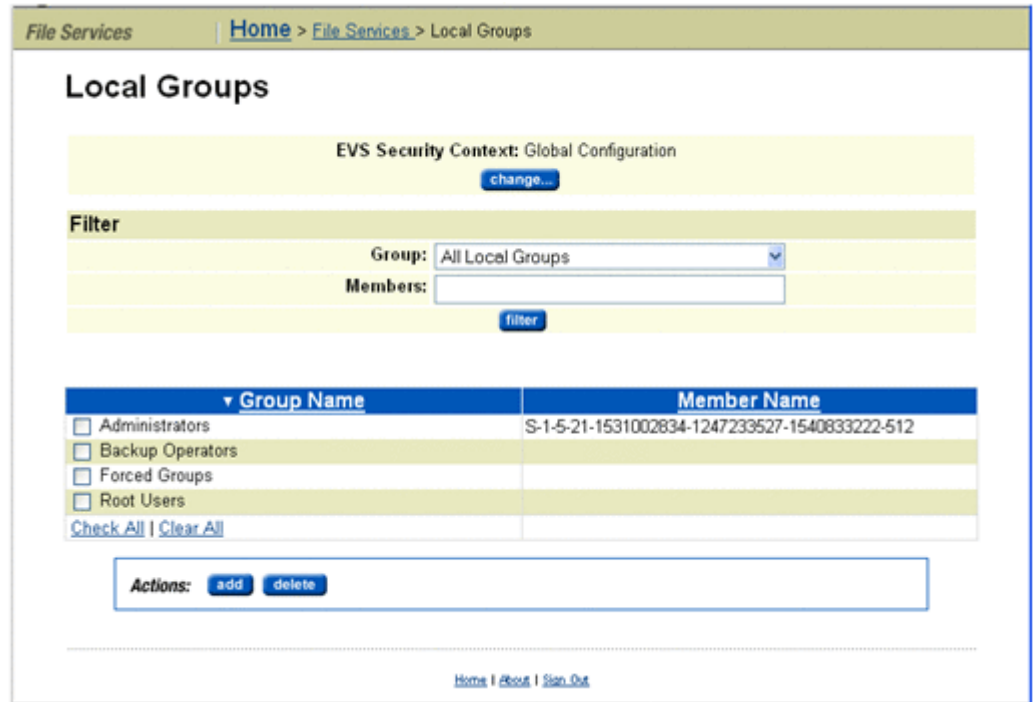


重要 グループ名はいったん作成されると、変更できません。グループ名を変更するには、グループを削除してから新しいグループを作成し、新しいグループにメンバーを追加する必要があります。

(2) ローカルグループまたはローカルグループメンバーを削除する

ローカルグループを削除するには

1. [Local Groups] 画面に移動します。
[File Services] 画面で [Local Groups] をクリックして、[Local Groups] 画面を表示します。



2. 必要に応じて、EVS セキュリティコンテキストを変更します。

[EVS Security Context] には、現在選択されている EVS セキュリティコンテキストが表示されます。この画面で行ったローカルグループの変更は、現在選択されている EVS セキュリティコンテキストにのみ適用されます。

- EVS がグローバル構成を使用している場合、グローバル構成設定の変更は EVS に影響を与えます。
- EVS が個別セキュリティコンテキストを使用している場合、グローバル構成設定の変更は EVS に影響を与えません。個別セキュリティコンテキストを使用している EVS のローカルグループを変更するには、それらの設定がグローバルセキュリティコンテキストによって使用される設定と同じ場合でも、その EVS の個別セキュリティコンテキストを選択して変更する必要があります。

別の EVS セキュリティコンテキストを選択したり、グローバル構成を選択したりするには、[change...] をクリックします。

3. グループの全てのメンバーを削除します。



重要 ローカルグループの削除は、2段階プロセスです。グループ自体を削除する前に、グループの全てのメンバーを削除する必要があります。

- a. 削除するグループメンバーを選択します。
削除するグループの各メンバーの横にあるチェックボックスを全てオンにします。
- b. 選択したグループメンバーを削除します。
[delete] をクリックして、選択したグループメンバーを削除します。
確認のダイアログが表示されます。[OK] をクリックしてユーザーを削除し、[Local Groups] 画面に戻ります。または、[Cancel] をクリックして、ユーザーを削除せずに [Local Groups] 画面に戻ります。
4. ローカルグループを削除します。
 - a. 削除するグループを選択します。
削除する全てのグループの横にあるチェックボックスをオンにします。
 - b. グループを削除します。

[delete] をクリックして、選択したグループを削除します。

確認のダイアログが表示されます。[OK] をクリックしてグループを削除し、[Local Groups] 画面に戻ります。または、[Cancel] をクリックして、グループを削除せずに [Local Groups] 画面に戻ります。

5.1.5 CIFS 共有を構成する

CIFS 共有は、マウントされたボリューム上にセットアップできます。HNAS は、1,000 を超える共有をサポートできます。ただし、共有割り当ての正確な制限は、HNAS の構成によって異なります。

(1) CIFS 共有を追加する

CIFS 共有を追加または削除するには

1. [CIFS Shares] 画面に移動します。

[File Services] 画面で [CIFS Shares] をクリックして、以下の画面を表示します。



次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
Cluster Name Space/ CNS Label または EVS/File System Label	共有が表示される、現在選択されているコンテキスト（クラスタネームスペースコンテキストまたは EVS ローカルコンテキストのどちらか）の名前です。 <ul style="list-style-type: none">クラスタネームスペースコンテキストが表示されている場合、CNS ツリーにリンクしている共有が一覧表示されます。これらの共有にアクセスするユーザーは、CNS ツリーが指すディレクトリ及びその下にあるディレクトリにアクセスできます。ローカル EVS コンテキスト及びファイルシステム名が表示されている場合、リストには、選択された EVS のファイルシステムの共有が表示されません。 表示されているコンテキストを変更するには、[change...] をクリックします。
Filter	共有名、パス、[Transfer to Object Replication Target] の設定値に基づいて、フィルターを定義し、画面に表示される共有リストを制限できます。
Name	CIFS 共有の名前です。
Comment	CIFS 共有に関連する追加情報です。この情報は、共有名と共に頻繁にクライアントに表示されます。
File System/Name Space	共有が配置されるファイルシステムまたは CNS リンクの名前です。

項目/フィールド	説明
Path	CIFS 共有が指すディレクトリです。共有にアクセスするユーザーは、このディレクトリ及びディレクトリツリーでこのディレクトリの下にあるディレクトリにアクセスできます。

[Actions] では、次のアクションを使用できます。

- CIFS 共有の詳細情報を表示するには、[details] をクリックします。
- CIFS 共有を追加し、次のステップに進むには、[add] をクリックします。
- 選択した CIFS 共有を削除するには、[delete] をクリックします。
- SMU のキャッシュを消去し、関連オブジェクトを使って再作成するには、[refresh cache] をクリックします。これは、ブラウザの更新ボタンをクリックして、キャッシュを消去せずに最近の更新を取得することとは異なります。

[Shortcut] では、以下のショートカットも使用できます。

- 選択された EVS 及びファイルシステム上にある構成済み CIFS 共有のリストをカンマ区切り (.csv) ファイルでダウンロードするには、[Download Shares] をクリックします。ダウンロードされたファイルを使用して、CIFS 共有を復元することはできませんので注意してください (CIFS 共有は、CIFS 共有バックアップファイルから復元する必要があります)。別のファイルシステムから共有リストをダウンロードするには、[change...] をクリックします。
- [CIFS Shares Backup & Restore] 画面を表示するには、[Backup & Restore] をクリックします。詳細については、「(8) CIFS 共有をバックアップ及び復元する」を参照してください。

2. CIFS 共有を追加します。

既に [add] をクリックして、[Add Share] 画面を表示しています。

The screenshot shows the 'Add Share' configuration page. The breadcrumb navigation is 'Home > File Services > CIFS Shares > Add Share'. The main title is 'Add Share'. The page is divided into several sections:

- EVS / File System:** evs1 / G1_Tar_02 (with a 'change' link).
- Share Name:** Text input field.
- Comment:** Text input field.
- Path:** Text input field with a 'browse...' button. Below it is a checkbox 'Create path if it does not exist. (See online help for this option.)' which is checked.
- Max Users:** Text input field with 'unlimited' entered.
- Show Snapshots:** Dropdown menu with 'Show and Allow Access' selected.
- Cache Options:** Dropdown menu with 'Manual local caching for documents' selected.
- Transfer to Object Replication Target:** Dropdown menu with 'Use FS Default' selected. Below it is the text '(The File System Default: Enabled)'. Below this is an 'Access Configuration' section with a large empty text area and the instruction '(Enter IP-based values first, if possible)'.
- Share Permissions:** A list box containing 'Everyone'. Below it is a 'Type' dropdown with 'Well Known Group' selected. There are 'Allow' and 'Deny' checkboxes. Under 'Allow', 'Full Control' (checked), 'Change' (checked), and 'Read' (checked) are listed.
- User Home Directory Mapping:** 'Mode' dropdown with 'Off' selected. Below it is the instruction 'Choose "ADS" mode to use the home directory path value provided by Active Directory.' Below that is a 'Path' text input field with a 'browse...' button. Below the path field is the text '(Relative to Share path)'.

At the bottom of the form are 'OK' and 'cancel' buttons. At the very bottom of the page are links for 'Home | About | Sign Out'.

要求された情報を入力します。次の表で、この画面のフィールドについて説明します。

項目/フィールド	説明
Cluster Name Space/ CNS Label または EVS/File System	共有が表示される、現在選択されているコンテキスト（クラスタネームスペース コンテキストまたは EVS ローカルコンテキストのどちらか）の名前です。 <ul style="list-style-type: none"> クラスタネームスペースコンテキストが表示されている場合、CNS ツリーに リンクしている共有が一覧表示されます。これらの共有にアクセスする ユーザーは、CNS ツリーが指すディレクトリ及びその下にあるディレクトリ にアクセスできます。 ローカル EVS コンテキスト及びファイルシステム名が表示されている場 合、リストには、選択された EVS のファイルシステムの共有が表示されま す。 表示されているコンテキストを変更するには、[change...] をクリックします。
Share Name	CIFS 共有の名前です。
Comment	CIFS 共有に関する追加情報を入力します。この情報は、共有名と共にクライア ントに表示されます。
Path	CIFS 共有が指すディレクトリです。共有にアクセスするユーザーは、このディ レクトリ、及びディレクトリツリーでこのディレクトリの下にあるディレクトリ にアクセスできます。ディレクトリを検索するには、[browse] をクリックしま す。 まだパスが存在していない場合は、[Create path if it does not exist] チェック ボックスをオンにして、パスを作成します。 注：[browse] ボタンは、パスが、ネームスペースではなくファイルシステムに 作成されている場合に限り表示されます。
Max Users	CIFS 共有に関連付けることのできるユーザーの最大数です。デフォルトは無制 限です。
Show Snapshots	この共有からスナップショットにアクセスできるようにするには、このチェック ボックスをオンにします。 <ul style="list-style-type: none"> [Show and Allow Access] は、スナップショットへのアクセスを表示し、許 可します。 [Hide and Allow Access] は、スナップショットを隠しますが、隠されたス ナップショットへのアクセスを許可します。 [Hide and Disable Access] は、スナップショットを隠し、アクセスも許可 しません。 この設定に対する変更は、CIFS クライアントが、フォルダビューを更新したと きに有効になります。
Cache Options	<ul style="list-style-type: none"> [Manual local caching for documents]：手動モードでは、ユーザーは、オ フラインクアクセスに必要な個別ファイルを指定できます。この操作は、オン ラインかオフラインかを問わず、ユーザーが指定されたファイルにアクセス できることを保証します。 [Automatic local caching for documents]：この自動モードは、共有全体の、 実行ファイル以外の全てのファイルに適用されます。ユーザーが、この共有 の実行ファイル以外のファイルにアクセスするときに、ユーザーが、オフラ インアクセスできるようにします。この操作は、ユーザーが実行ファイル以 外の全てのファイルにアクセスできることを保証しません。少なくとも一度 使用されたことのあるファイルしか、キャッシュされないためです。「自動」 は、プログラムにも定義できます。 [Automatic local caching for programs]：この自動モードは、共有全体の、 全ての実行ファイルに適用されます。この共有の実行ファイルにユーザー がアクセスするときに、オフラインアクセスできるようにします。この操作 は、ユーザーが全ての実行ファイルにアクセスできることを保証しません。 少なくとも一度使用されたことのあるファイルしか、キャッシュされないた めです。「自動」は、ドキュメントにも定義できます。 [Local caching disabled]：ファイルやフォルダのキャッシュは発生しま せん。 注：HNAS は、オフラインファイルアクセスをサポートしています。これによ り、Windows 2000 以降のクライアントは、ネットワーク/ファイル共有からよ く使用されるファイルを、キャッシュできるようになります。オフラインファイ

項目/フィールド	説明										
	ルを使用するには、クライアントのコンピューターが Windows 2000 以降を実行している必要があります。										
Transfer to Object Replication Target	<p>ファイルシステムがスナップショットからリカバリーされる場合、最後の手順の一つとして、選択されたファイルシステムのバージョンを示すスナップショットで検出された CIFS 共有をインポートします。転送可能なマークの付いた CIFS 共有に限り、インポートされます。</p> <p>ドロップダウンリストを使用して、以下のうち一つを指定します。</p> <ul style="list-style-type: none"> • [Enable] : CIFS 共有は、リカバリーされたファイルシステムに転送されません。 • [Disable] : CIFS 共有は、リカバリーされたファイルシステムに転送されません。 • [Use FS Default] (デフォルト) : ターゲットのファイルシステムがオンラインになっている場合に、[Transfer Access Points During Object Replication] がファイルシステムで有効になっていれば、CIFS 共有が転送されます。 										
Access Configuration	<p>共有にアクセスできるクライアントの IP アドレスです (このフィールドには、最大 2,000 文字まで入力できます)。アクセス構成の設定についての詳細は、「(3) 修飾子を使用して、共有へのアクセスを制御する」を参照してください。</p> <table border="1"> <thead> <tr> <th>入力内容</th> <th>意味</th> </tr> </thead> <tbody> <tr> <td>空欄またはアスタリスク (*)</td> <td>全クライアントが共有にアクセスできます。</td> </tr> <tr> <td>固有アドレス。 例 : 10.168.20.2</td> <td>指定された IP アドレスを持つクライアントに限り、共有にアクセスできます。</td> </tr> <tr> <td>CIDR 表記を使用した、アドレスの範囲。 例 : 10.168.20.0/16</td> <td>この範囲内のアドレスを持つクライアントが、エクスポートにアクセスできます。</td> </tr> <tr> <td>ワイルドカードを使用した、部分的アドレス。 例 : 10.168.*.*</td> <td>アドレスが一致するクライアントが、共有にアクセスできます。</td> </tr> </tbody> </table>	入力内容	意味	空欄またはアスタリスク (*)	全クライアントが共有にアクセスできます。	固有アドレス。 例 : 10.168.20.2	指定された IP アドレスを持つクライアントに限り、共有にアクセスできます。	CIDR 表記を使用した、アドレスの範囲。 例 : 10.168.20.0/16	この範囲内のアドレスを持つクライアントが、エクスポートにアクセスできます。	ワイルドカードを使用した、部分的アドレス。 例 : 10.168.*.*	アドレスが一致するクライアントが、共有にアクセスできます。
入力内容	意味										
空欄またはアスタリスク (*)	全クライアントが共有にアクセスできます。										
固有アドレス。 例 : 10.168.20.2	指定された IP アドレスを持つクライアントに限り、共有にアクセスできます。										
CIDR 表記を使用した、アドレスの範囲。 例 : 10.168.20.0/16	この範囲内のアドレスを持つクライアントが、エクスポートにアクセスできます。										
ワイルドカードを使用した、部分的アドレス。 例 : 10.168.*.*	アドレスが一致するクライアントが、共有にアクセスできます。										
Follow Symbolic Links	<p>この共有に対するシムリンクの追跡を有効にするには、このチェックボックスをオンにします。</p> <p>注 : CIFS2 (SMB2) クライアントは、Hitachi High-performance NAS Platform™ 経由でアクセスするストレージ上のファイルへのシムリンク (相対または絶対) を追跡できません。</p>										
Follow Global Symbolic Links	<p>このチェックボックスをオンにすると、この共有について、CIFS クライアントが Microsoft の DFS メカニズム経由でグローバル (絶対) シムリンクを追跡できるようになります。シンボリックリンクの詳細については、「シンボリックリンク」を参照してください。</p>										
Force Filename to be Lowercase	<p>この共有で生成される全てのファイル名を小文字にするよう強制するには、このチェックボックスをオンにします。これは、UNIX アプリケーションの相互運用に便利です。</p>										
Enable ABE	<p>この共有に対する ABE (アクセスベースの列挙) を有効にするには、チェックボックスをオンにします。</p> <p>デフォルトで、ABE は、共有に対して無効であり、HNAS でも無効です。共有に対して ABE を有効にする前に、ABE が、HNAS に対して有効かどうかを確認する必要があります (ABE サポートを有効にする CLI コマンドは、<code>fsm set disable-ABE-support false</code> です)。</p> <p>有効にすると、ABE は、CIFS 共有の内容をフィルタリングします。ユーザーが「FileReadData」権または「FileListDirectory」権を持っているファイル及びディレクトリに限り、そのユーザーに表示されます (ディレクトリリストに戻される、ワイルドカード削除の対象にされるなど)。ABE を有効にすると、CIFS の性能が低下する可能性があります。</p>										

項目/フィールド	説明
Enable Virus Scanning	<p>グローバル構成または共有が指すファイルシステムをホストする EVS でウイルススキャンを設定して有効にした場合、その後、共有が作成されるときには、ウイルススキャンはデフォルトで有効です。グローバル構成または共有が指すファイルシステムをホストする EVS でウイルススキャンを有効にしていない場合、その後、共有が作成されるときには、ウイルススキャンはデフォルトで無効です。ただし、EVS ごとに有効にできます。</p> <p>ウイルススキャンは、EVS ごと、またはグローバル構成コンテキストを使って、いる全ての EVS にセットアップされます。ただし、ノードごとのセットアップはできません。</p> <p>特定の共有に対するウイルススキャンを無効にするには、このチェックボックスをオフにします。</p>
Share Permissions	
Share Permissions List	<p>デフォルトで、CIFS 共有が作成されると、グループ「Everyone」が [Share Permissions] リストに追加されます。共有アクセス許可の変更については、「(5) CIFS 共有のアクセス許可を追加または変更する」を参照してください。</p>
User Home Directory Mapping	
Mode	<p>ユーザーごとのホームディレクトリの作成方法を指定するために使用します。ドロップダウンリストを使って、以下のいずれかを選択できます。</p> <ul style="list-style-type: none"> • [Off]: この共有のホームディレクトリ機能を無効にします。ユーザーに対して、この共有のホームディレクトリを自動作成しません。これがデフォルトです。 • [ADS]: 各ユーザーに対して、Active Directory サーバからのホームディレクトリ情報に基づいて、ユーザーホームディレクトリを作成します。[ADS] を選択する場合は、[Path] を指定しません。 • [User]: ユーザーの Windows ユーザー名を小文字に変換することによって、ユーザーのホームディレクトリを作成します。(ユーザーの Window ドメイン名は、あったとしても無視されます。) 例えば、「DOMAIN¥John Smith」というユーザーのホームディレクトリは、「john_smith」になります。 • [DomainAndUser]: ユーザーの Windows ドメイン名に由来するディレクトリを作成することによって、ユーザーのホームディレクトリを作成します。その後、ユーザーの Windows ドメイン名を小文字に変換し、その名前前でサブディレクトリを作成します。例えば、「DOMAIN¥John Smith」というユーザーのホームディレクトリは、「domain¥john_smith」になります。 • [Unix]: ユーザーの UNIX ユーザー名を小文字に変換することによって、ユーザーのホームディレクトリを作成します。
Path	<p>共有ルートに関連する、ユーザーごとのホームディレクトリを、先頭に「¥」を入れずに作成します。このフィールドを空欄のままにすると、ユーザーのホームディレクトリが、共通ルートに直接作成されます。</p> <p>デフォルトで、ホームディレクトリを使って構成できるのは、ファイルシステムごとに共有一つのみです。cifs-home-directory コマンドを使用して、この制限を緩和できます。その場合は、矛盾するホームディレクトリを構成しないよう、細心の注意が必要です。</p> <p>例えば、「¥home1」というパスを使っている共有と、「¥home2」というパスを使っている共有は、どのようなホームディレクトリパスが構成されても矛盾しません。その一方で、「¥」というパスとデフォルトのホームディレクトリパスを使っている共有は、「¥dir」というパスとデフォルトのホームディレクトリパスを使う共有と矛盾します。</p> <p>既存ディレクトリに進むには、[browse] をクリックします。</p>

3. 設定を保存します。

設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

(2) CIFS 共有のプロパティを表示及び変更する

共有を変更する前に、その共有の [CIFS Shares Details] 画面を開き、共有ユーザー数が「0」であることを確認します。



注意 他のユーザーがアクセス中の共有を変更または削除すると、CIFS セッションが終了し、保存されていないデータが失われる可能性があります。



重要 ストレージを交換して、新しいファイルシステムの場所を指すために共有を変更する必要がある場合は、「ファイルシステムのレプリケーション」と「プライマリアクセスの転送」の各機能を使って、ファイルシステムを移動し、共有を自動で変更します。これらの各機能の詳細については、『*Replication and Disaster Recovery Administration Guide*』を参照してください。

CIFS 共有のプロパティを表示及び変更するには

1. [CIFS Shares] 画面に移動します。

[File Services] 画面で [CIFS Shares] をクリックして、以下の画面を表示します。

The screenshot shows the 'CIFS Shares' management page. At the top, there's a breadcrumb trail: 'Home > File Services > CIFS Shares'. Below that, the page title is 'CIFS Shares'. There are two main sections: 'EVS / File System Label' (EVS01 / All File Systems) and a 'Filter' section. The filter section has input fields for 'Name', 'Path', and a dropdown for 'Transfer to Object Replication Target' (set to 'None'). Below the filter is a table with columns: Name, Comment, File System, Path, and a 'details' button. The table contains one row: 'C\$' with comment 'Default share' and file system 'Unknown'. Below the table are action buttons: 'add', 'delete', 'refresh cache', 'Download Shares', and 'Backup & Restore'. At the bottom, there are links for 'Home', 'About', and 'Sign Out'.

2. 詳細を表示し、(必要に応じて) CIFS 共有を変更します。

CIFS 共有の [details] をクリックして、[CIFS Share Details] 画面を表示します。

The screenshot shows the 'CIFS Share Details' configuration page. At the top, there's a breadcrumb trail: 'Home > File Services > CIFS Shares > CIFS Share Details'. Below that, the page title is 'CIFS Share Details'. The page is divided into several sections: 'File System' (G1_Tar_02), 'Share Name' (testrep012), 'Comment', 'Number of Share Users' (0), 'Path', 'Max Users' (unlimited), 'Show Snapshots' (Show and Allow Access), 'Cache Options' (Manual local caching for documents), 'Transfer to Object Replication Target' (Use FS Default), 'Access Configuration', 'Share Permissions' (Everyone), and 'User Home Directory Mapping' (Mode: Off). There are also checkboxes for 'Follow Symbolic Links', 'Follow Global Symbolic Links', 'Force Filename to be Lowercase', 'Enable ABE', and 'Enable Virus Scanning'. At the bottom, there are 'OK' and 'cancel' buttons. At the very bottom, there are links for 'Home', 'About', and 'Sign Out'.

この画面のフィールドの説明については、「(1) CIFS 共有を追加する」を参照してください。共有アクセス許可の変更については、「(4) アクセス許可を使用して、共有へのアクセスを制御する」を参照してください。

この画面のフィールドを、必要に応じて変更します。

3. 設定を変更します。

設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

(3) 修飾子を使用して、共有へのアクセスを制御する

CIFS 共有にアクセスできるクライアントを指定するために、修飾子を IP アドレスに追加できます。

修飾子	説明
read_write, readwrite, rw	読み取り/書き込みアクセスを許可します。デフォルトの設定です。
read_only, readonly, ro	特定クライアントの読み取り専用アクセスを、CIFS 共有に許可します。
no_access, noaccess	指定クライアントが CIFS 共有にアクセスすることを拒否します。

CIFS 共有の修飾子の例を、以下に記載します。

- 10.1.2.38(ro)
10.1.2.38 という IP アドレスを持っているクライアントに、読み取り専用アクセスを許可します。
- 10.1.2.0/24(ro)
10.1.2.0~10.1.2.255 の範囲内の IP アドレスを持っているクライアント全てに、読み取り専用アクセスを許可します。
- 10.1.*.*(readonly)
IP アドレスが 10.1 で始まる全てのクライアントに、読み取り専用アクセスを許可します。

エントリが指定される順序は、重要です。以下は、その例です。

* (ro)

10.1.2.38 (noaccess)

この場合、1 行目で読み取り専用アクセスを全てのクライアントに許可し、2 行目で指定したクライアントへのアクセスを拒否しています。ただし、1 行目は全てのクライアントに一致するため、2 行目は冗長です。10.1.2.38 に対するアクセスを確実に拒否するために、この 2 行の順序を入れ替える必要があります。

(4) アクセス許可を使用して、共有へのアクセスを制御する

共有へのアクセスは、共有レベルとファイルレベルのアクセス許可を組み合わせることにより、制限されます。これらのアクセス許可は、ユーザーが共有ディレクトリの内容を表示、変更できる範囲を決定します。ユーザーが共有へのアクセスをリクエストすると、最初に、共有レベルのアクセス許可がチェックされます。共有へのアクセスが認められると、ファイルレベルのアクセス許可がチェックされます。

共有レベルのアクセス許可が、ファイルレベルのアクセス許可と異なる場合、以下の表で説明しているとおり、より制限の強いアクセス許可が適用されます。この表では、[a]=「アクセス許可」、[d]=「拒否」を表しています。

アクティビティ	読み取り (Read)	変更 (Change)	完全 (Full Control)
ファイルとサブディレクトリの名前を表示する	a	a	a
共有ディレクトリのサブディレクトリを変更する	a	a	a
ファイルのデータを表示する	a	a	a
アプリケーションを実行する	a	a	a
ファイルとサブディレクトリを追加する	d	a	a
ファイルのデータを変更する	d	a	a
ファイルとサブディレクトリを削除する	d	a	a
ファイルまたはサブディレクトリのアクセス許可を変更する	d	d	a
ファイルまたはサブディレクトリの所有権を取得する	d	d	a

共有へのアクセスを構成するときに実行できるのは、以下の状態のユーザーまたはグループの追加のみです。

- ・ ドメインコントローラーが認識しているユーザーまたはグループ
- ・ ネットワーク上の HNAS が確認しているユーザーまたはグループ

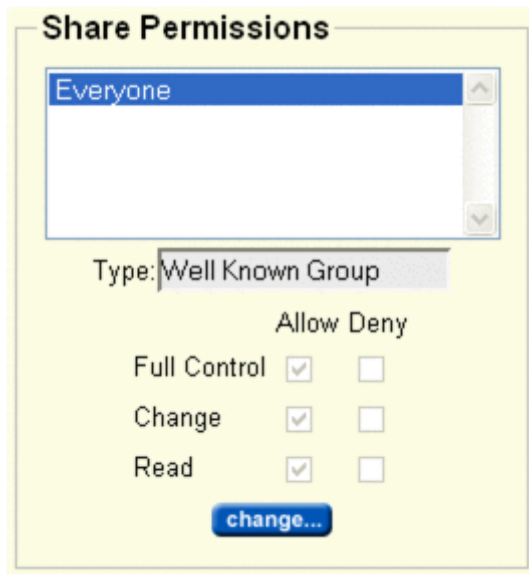


重要 ユーザーが、共有へのアクセス権を与えられている場合で、さまざまなアクセスレベルを持つグループのメンバーである場合は、より制限の緩いアクセス許可が適用されます。例えば、あるユーザーが、共有の読み取りアクセス権を与えられており、さらに、同一の共有への変更アクセス権を持つグループに属している場合、そのユーザーは、共有に対する変更アクセス権を持つこととなります。変更アクセス権は、読み取りアクセス権よりも、制限が緩いためです。

(5) CIFS 共有のアクセス許可を追加または変更する

CIFS 共有のアクセス許可を追加または変更するには

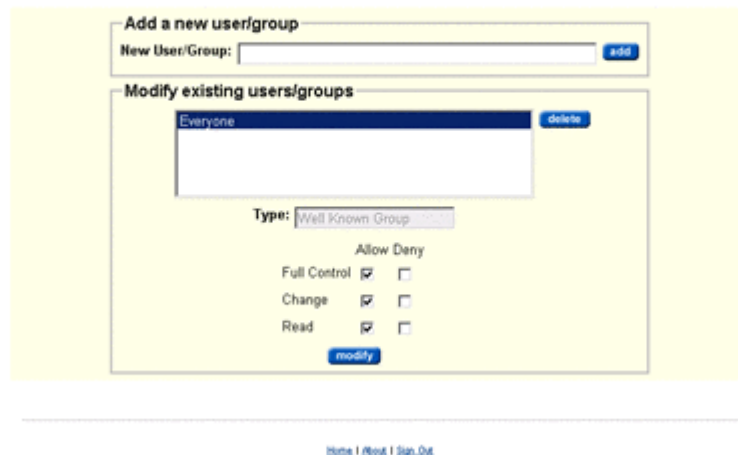
1. [CIFS Shares] 画面に移動します。
[File Services] 画面で [CIFS Shares] をクリックして、[CIFS Shares] 画面を表示します。
2. [CIFS Shares Details] 画面に移動します。
アクセス許可を追加または変更する共有を選択して、[details] をクリックします。
3. [CIFS Share Permissions] 画面に移動します。
[CIFS Share Details] 画面の [Share Permissions] エリアで、[change...] をクリックします。



[CIFS Share Permissions] 画面が表示されます。

File Services | Home > File Services > CIFS Shares > CIFS Shares Details > CIFS Share Permissions

CIFS Share Permissions for fs1_shr



4. 新規ユーザー／グループを追加するか、または既存ユーザー／グループを選択します。
 - 新規ユーザーまたはグループを追加するには
 - a. 新規ユーザーまたはグループの名前を、[New User/Group] フィールドに入力します。
 - b. [New User/Group] フィールドの右にある [add] ボタンをクリックして、新規ユーザー／グループを、ユーザー／グループリストに追加します。
[Type] フィールドに、追加されるユーザー／グループが属することになるセキュリティグループの、標準化された識別子が表示されます。この値は、追加されるユーザー／グループの既知のセキュリティ識別子に基づいて、自動設定されます。
 - c. ユーザー／グループリストのユーザー／グループ名をクリックして、新規ユーザー／グループを選択します。
 - 既存ユーザー／グループを選択するには、ユーザー／グループリストのユーザー／グループ名をクリックします。
5. 選択したユーザー／グループのアクセス許可を設定します。

ユーザー／グループのアクセス許可を設定するには、上記ガイドラインに従って、[Allow] または [Deny] のチェックボックスをオンにします。(「(4) アクセス許可を使用して、共有へのアクセスを制御する」の表を参照してください。)

(6) オフラインファイルアクセスモード

HNAS は、オフラインファイルアクセスをサポートしています。これにより、ネットワーククライアントは、ネットワーク／ファイル共有からよく使用されるファイルを、キャッシュできるようになります。オフラインファイルを使用するには、クライアントのコンピューターが Windows 2000 以降を実行している必要があります。共有キャッシュモードは、3 種類です (全 3 種のキャッシュモードをサポートしています)。

- キャッシュなし
ファイルやフォルダのキャッシュは発生しません。
- 手動
オフラインアクセスに必要な、個別ファイルのユーザー指定を許可します。この操作は、オンラインかオフラインかを問わず、指定されたファイルにユーザーがアクセスできることを保証します。
- 自動
共有全体に適用されます。ユーザーが、この共有のファイルにアクセスすると、そのユーザーは、そのファイルにオフラインアクセスできるようになります。この操作は、ユーザーが指定されたファイルにアクセスできることを保証しません。少なくとも一度使用されたことのあるファイルしか、キャッシュされないためです。ドキュメントやプログラムに対して、自動モードを定義できます。

(7) CIFS 共有を変更または削除する

共有を変更または削除する前に、その共有の [CIFS Shares Details] 画面を開き、共有ユーザー数が「0」であることを確認します。



注意 他のユーザーがアクセス中の共有を変更または削除すると、CIFS セッションが終了し、保存されていないデータが失われる可能性があります。

CIFS 共有を削除するには

1. [CIFS Shares] 画面に移動します。

[File Services] 画面で [CIFS Shares] をクリックして、以下の画面を表示します。

File Services | Home > File Services > CIFS Shares

CIFS Shares

EVS / File System Label
EVS01 / All File Systems [change...](#)

Filter

Name:
Path:
Transfer to Object Replication Target: [filter](#)

Name	Comment	File System	Path
C\$	Default share	Unknown	A

[Check All](#) | [Clear All](#)

Actions: [add](#) [delete](#) [refresh cache](#) | [Download Shares](#) | [Backup & Restore](#)

Home | About | Sign Out

2. 削除する共有を選択します。
削除する各共有の名前の横にあるチェックボックスをオンにします。
3. 選択した CIFS 共有を削除します。
[delete] をクリックして、選択した共有を削除します。

(8) CIFS 共有をバックアップ及び復元する

CIFS 共有をバックアップ及び復元するときは

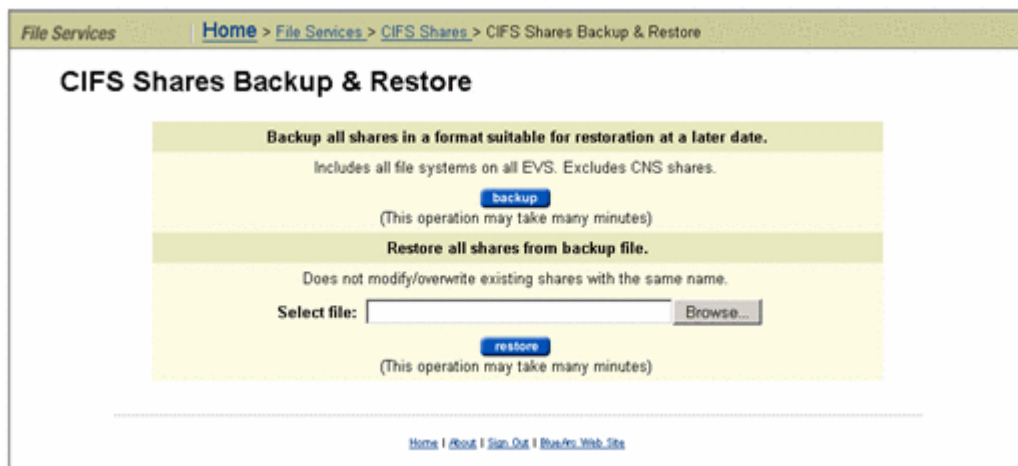
- 全ての EVS 上にある、全ての CIFS 共有をバックアップします (CNS ツリー上にある CIFS 共有は除きます)。
- CIFS 共有バックアップファイルは、.txt ファイルとして保存されます。バックアップファイルには、ファイルシステム名、共有名の他、パス存在の確認、スナップショットの表示、シンボリックリンクの追跡、ファイル名の小文字強制、ウイルススキャン、キャッシュオプション、最大ユーザー数の設定など、共有に関するほとんどの情報が含まれます。

CIFS 共有をバックアップファイルから復元するときは

- 復元操作により、現在存在している同名の共有が変更されたり上書きされたりすることはありません。
- 上記の場合を除き、選択されたバックアップファイルの全ての共有が復元されます。

CIFS 共有をバックアップまたは復元するには

1. [CIFS Shares Backup & Restore] 画面に移動します。
[File Services] 画面で [CIFS Shares] を選択し、[Backup & Restore] をクリックして、[CIFS Shares Backup & Restore] 画面を表示します。



2. バックアップまたは復元を実行します。
 - バックアップするには
[backup] をクリックします。ブラウザで、バックアップファイルの名前と場所を指定し、[OK/Save] をクリックします (表示されるボタンと、バックアップファイルを保存するために使う方法は、使用しているブラウザによって異なります)。
バックアップファイル名が提案されますが、カスタマイズできます。提案されたファイル名が使用している構文は、CIFS_SHARES_日付_時間.txt です。以下は、適切な構文の例です。
CIFS_SHARES_Aug_4_2006_11_09_22_AM.txt
 - 復元するには

[restore]をクリックします。ブラウザで、復元する特定の共有のバックアップテキストファイル (CIFS_SHARES_日付_時間.txt) を選択し、[Open]をクリックします。[CIFS Export Backup & Restore] 画面に、選択したファイルの名前と場所が表示されたら、[Restore] をクリックします。

5.1.6 Windows サーバ管理を使用する

Windows 2000 以降で利用できる Computer Management MMC ツールを使うと、以下などの共有管理タスクを、リモートコンピュータから実行できます。

- 現在システムに接続しているユーザーの一覧表示
- 共有の作成
- システム上の全ての共有、共有に接続しているユーザーの一覧表示
- システムまたは特定の共有に接続しているユーザーのうちの 1 人、または全てのユーザーの切断
- 現在開いている共有リソースのうち、一つまたは全ての終了
- イベントログの表示



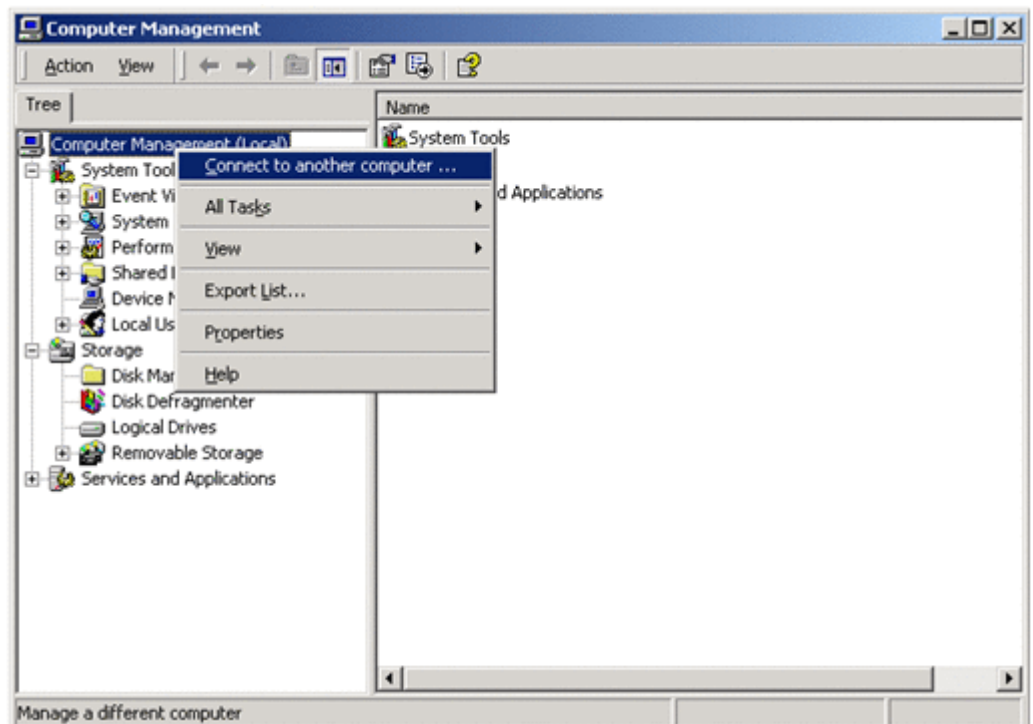
重要 Windows の旧バージョンでは、Server Manager に、このツールに相当するツールが用意されています。

5.1.7 Computer Management ツールを使用する

Computer Management ツールを使用するには

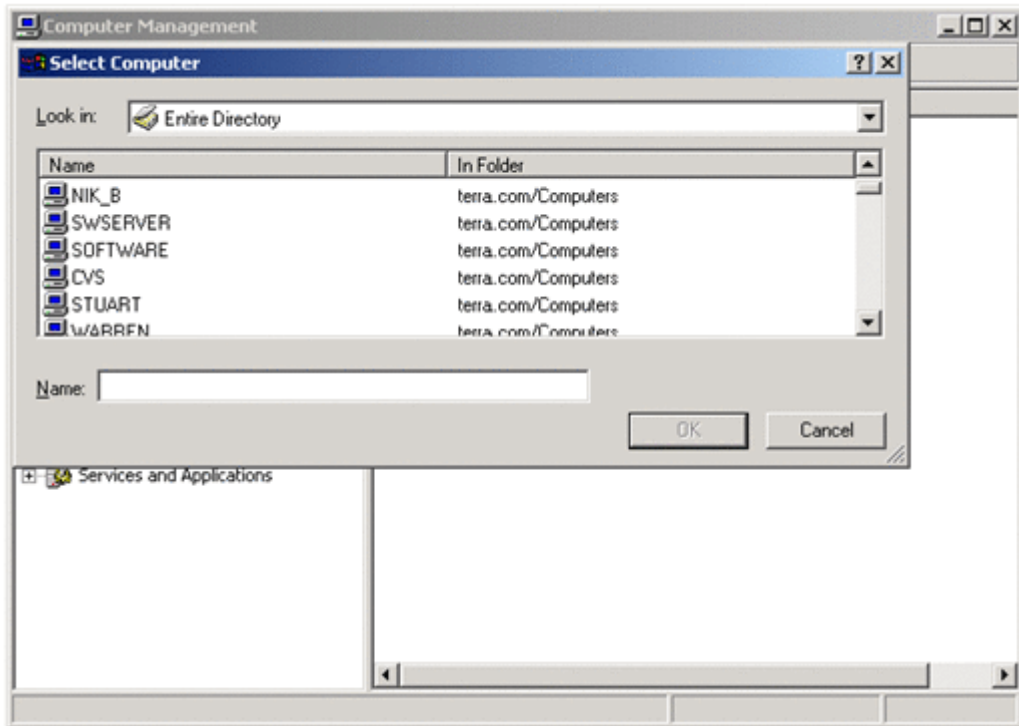
1. Computer Management ツールを開きます。

Windows インターフェースでは、[Administrative Services] から [Computer Management] を選択します。次に [Computer Management (Local)] を右クリックして、コンテキストメニューを表示し、[Connect to another computer] を選択します。



2. 必要に応じて、ドメインを指定し、続いて名前を選択します。

[Look in] ドロップダウンフィールドから、ドメインを選択します。



次に、HNAS 上のファイルサービスに使用する名前または IP アドレスを選択して、[OK] をクリックします。

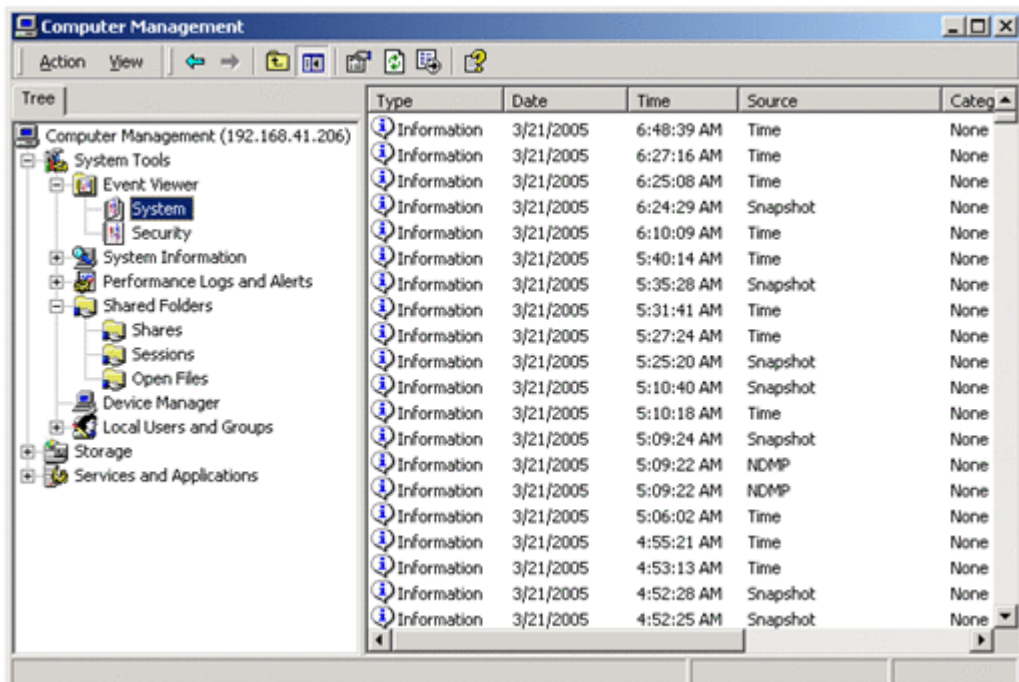


重要 管理 EVS (Admin EVS) を指定しないでください。

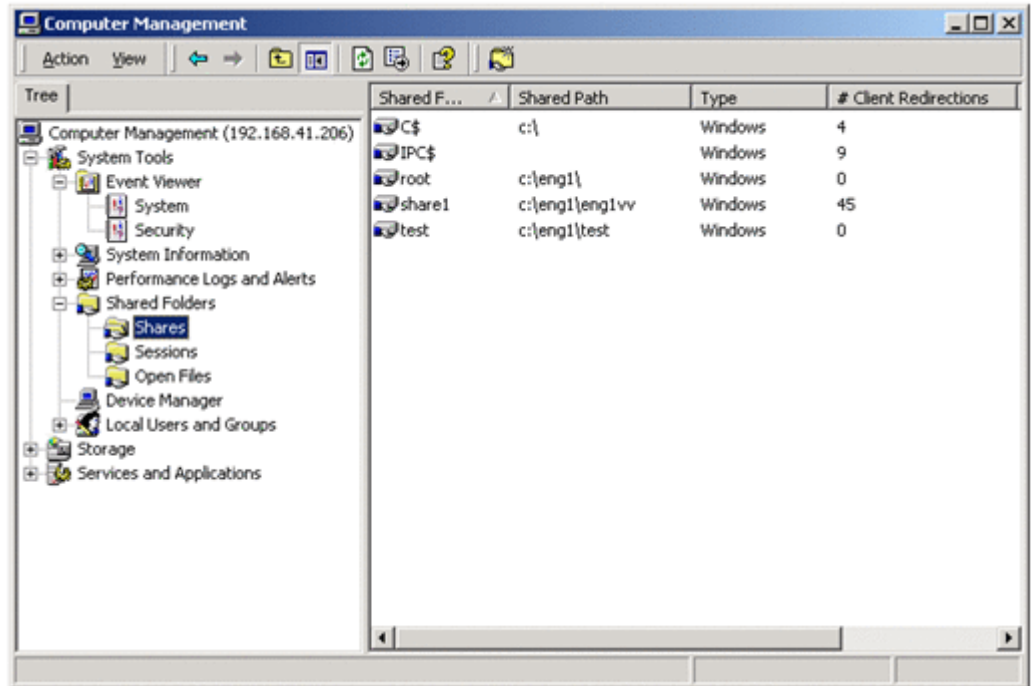
3. 入手できる情報を表示します。

入手できるのは、以下の情報です。

◦ HNAS のイベントログを表示するには、[Event Viewer] をクリックします。



以下は、イベントログウィンドウです。



- 全ての共有を一覧表示するには、[Shares] をクリックします。ユーザーの一部または全てを、特定の共有から切断できます。
 - システムに現在接続している全てのユーザーを一覧表示するには、[Sessions] をクリックします。ユーザーの一部または全てを切断できます。
- 全ての共有オープンリソースを一覧表示するには、[Open Files] をクリックします。共有リソースの一部または全てを終了できます。

FTP を使ってファイルを転送する

- 6.1 FTP を使ってファイルを転送する

6.1 FTP を使ってファイルを転送する

このセクションでは、ファイル転送プロトコル (FTP) をセットアップする方法を説明します。FTP クライアントを使っているユーザーは、HNAS 上のファイルやディレクトリにアクセスできるようになります。

6.1.1 FTP の優先順位を設定する

FTP セットアップのプロセスの一部として、FTP ユーザーのパスワード認証サービスを選択します。また、アクティブでない FTP セッションを終了させるために使う、タイムアウトを設定する必要があります。

(1) FTP の優先順位を設定するには

1. [FTP Configuration] 画面に移動します。

[File Services] 画面で [FTP Configuration] をクリックして、以下の画面を表示します。

The screenshot shows the 'FTP Configuration' page. It has a breadcrumb 'Home > File Services > FTP Configuration'. The main content area is titled 'FTP Configuration' and contains three sections: 'Password Authentication Services' with 'NT' checked and 'NIS' unchecked; 'Session Timeout' with a text input field set to '15 minutes'; and 'Anonymous User Permissions' with 'ReadOnly' unchecked. An 'apply' button is located at the bottom center.

2. [Password Authentication Service], [Session Timeout], [Anonymous User Permissions] の選択をします。

- [Password Authentication Service]

FTP ユーザーを認証するために使います。[NT] または [NIS] を選択します。

設定されたセキュリティモードによって、使用するパスワード認証サービスが決定されます。セキュリティモードの詳細については、「[2.3.2 セキュリティモードを変更する](#)」を参照してください。

UNIX セキュリティモード、または混合セキュリティモードで操作する場合は、NT と NIS の両方のパスワード認証がサポートされます。両方のサービスを有効にすると、FTP ユーザーは、まず、構成済みの NT ドメインに照らして認証されます。認証に失敗すると、HNAS は、構成済みの NIS ドメインに照らして、ユーザー認証を試みます。

- [Session Timeout]

FTP セッションの自動終了までの、アクティブでない状態の経過分数です。値は、15 分以上にする必要があります。

- [Anonymous User Permissions]

匿名リクエストに対して、読み取り書き込みを許可するかどうかを指定します。読み取り書き込み許可がデフォルトですが、[ReadOnly] チェックボックスをオンにして、匿名リクエストを読み取り専用で制限できます。

3. 設定を保存します。

設定を確認してから、[apply] をクリックして保存します。

6.1.2 FTP ユーザーを構成する

FTP ユーザーは手動でセットアップできます。または、ユーザーの詳細情報をファイルからインポートできます。

(1) FTP ユーザーをセットアップする

FTP ユーザーをセットアップするには

1. [FTP Users] 画面に移動します。
[File Services] 画面で [FTP Users] をクリックして、以下の画面を表示します。

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS / File System Label	このフィールドには、画面に一覧表示されている FTP ユーザーが構成された、EVS 及びファイルシステムが表示されます。別のファイルシステムを選択するには、[change...] ボタンをクリックします。
Filter	[filter] ボタンを使用して、ユーザーの [Name] または [Path] に基づいて、ユーザーをフィルタリングできます。
Name	この列には、既存の FTP ユーザーが表示されます。最大 500 ユーザーまで一覧表示できます。ただし、この FTP ユーザーリストに表示されるのは、1 画面につき最大 20 ユーザーです。ユーザー表示を制御するには、[filter] 基準を使用します。
File System	この列には、ユーザーの最初のパスを含んでいるファイルシステムの名前が表示されます。
Path	選択した FTP ユーザーが、FTP でログインしたときに開始するディレクトリのパスです。
details	[FTP User Details] 画面を開きます。この画面では、選択したユーザーに関する特定の詳細情報を変更できます。
add	[Add User] 画面を開きます。この画面では、新規ユーザーをセットアップできます。
delete	選択したユーザーを削除します。ユーザーを選択するには、ユーザーの [Name] の横にあるチェックボックスをオンにします。
Import Users	[Import FTP Users] 画面を開きます。この画面では、新規ユーザーを、ファイルからインポートしてセットアップできます。FTP ユーザーのインポートについての詳細は、「(2) FTP ユーザーをインポートする」を参照してください。

2. FTP ユーザーを追加します。
[add] をクリックして、[Add User] 画面を表示します。

The screenshot shows the 'Add User' dialog box. At the top, it says 'File Services' and 'Home > File Services > FTP Users > Add User'. The main title is 'Add User'. Below that, there's a section for 'EVS / File System: dsEVS03 / dsFS03' with a 'change...' button. Then, there are input fields for 'User Name:' and 'Initial Directory for the user:' with a 'browse...' button. Below these is a 'Path Options' section with a note: 'These options only apply when 'path' or 'file system' values are changed.' There is a checked checkbox for 'Create path if it does not exist. (See online help for security implications)'. At the bottom, there are 'OK' and 'cancel' buttons.

適切な情報を入力します。

- [EVS / File System] フィールドには、選択したファイルシステムが表示されます。ファイルシステムを変更するには、[change...] ボタンをクリックして、[Select a File System] 画面を開きます。
- [User Name] フィールドには、ユーザーがログインするために使用する名前を入力します。最初のディレクトリへの匿名ログインを許可するには、ユーザー名を、「anonymous」または「ftp」と指定します。
ユーザーがログインに使う必要のある名前が、NT ドメイン名なのか、UNIX ユーザー名なのかは、利用するパスワード認証サービスが判断します。
- [Initial Directory for the user] フィールドには、ユーザーが FTP でログインしたときの最初のディレクトリへのパスを入力します。まだパスが存在しない場合は、[Create path if it does not exist] チェックボックスをオンにして、パスを自動作成します。



重要 自動作成されるディレクトリは、ルートユーザー及びグループ (UID:0/GID:0) によって所有され、全てのユーザーがアクセスできます (つまり、アクセス許可は rwxrwxrwx に設定されます)。そのようなディレクトリは CIFS または NFS を介して作成するか、このオプションを使用して作成した後、必要なアクセス許可を明示的に付与することを推奨します。

3. 変更を保存します。

設定を確認してから、[OK] をクリックして設定を保存し、[FTP Users] 画面に戻ります。新規ユーザーは、この画面のテーブルに追加されます。

(2) FTP ユーザーをインポートする

FTP ユーザーをインポートするには

1. [FTP Users] 画面に移動します。

[File Services] 画面で [FTP Users] をクリックして、[FTP Users] 画面を表示します。次に [Import Users] リンクをクリックして、[Import FTP Users] 画面を表示します。

The screenshot shows the 'Import Ftp Users' dialog box. At the top, it says 'File Services' and 'Home > File Services > Ftp Users > Import Ftp Users'. The main title is 'Import Ftp Users'. Below that, there's a section for 'Import From File' with a 'Filename:' input field and a 'Browse...' button. At the bottom, there is an 'Import' button.

2. インポートファイルの場所を見つけます。

[Filename] フィールドに、ユーザーの詳細情報を含んでいるファイル名を入力します。または、[Browse] をクリックして、ファイル名を検索します。

インポートファイルのユーザー詳細情報には、以下の構文が含まれています。

```
user_name file_system initial_directory
```

入力ごとに、少なくとも一つのスペースで区切る必要があります。user_name または initial_directory がスペースを含む場合は、入力を二重引用符で囲む必要があります。以下は、その例です。

```
carla Sales /Sales/Documents
miles Sales "/Sales/Sales Presentations"
john Marketing /Marketing
```

最初のディレクトリが存在するかどうか不明の場合は、ファイルの別の行に ENSURE_PATH_EXISTS というオプションを指定することによって、最初のディレクトリを自動作成できます。以下は、その例です。

```
ENSURE_PATH_EXISTS true
carla Sales /Sales/Documents
miles Sales "/Sales/Sales Presentations"
ENSURE_PATH_EXISTS false
john Marketing /Marketing
```

一つ目の ENSURE_PATH_EXISTS オプションのインスタンスでは、true 属性によって、このオプションはオンになります。このオプションは、「false」という属性を使う二つ目のオプションのインスタンスでオフになるまで、一つ目のインスタンスの後に続く二つの入力に適用されます。最初のディレクトリを自動作成できるように、ENSURE_PATH_EXISTS オプションのデフォルトは、「true」です。

ファイルにコメントを挿入するには、コメントの前に番号記号 (#) を付けます。



重要 自動作成されるディレクトリは、ルートユーザー及びグループ (UID:0/GID:0) によって所有され、全てのユーザーがアクセスできます (つまり、アクセス許可は rwxrwxrwx に設定されます)。そのようなディレクトリは CIFS または NFS を介して作成するか、このオプションを使用して作成した後、必要なアクセス許可を明示的に付与することが推奨されます。

3. ファイルをインポートします。
[Import] をクリックします。

(3) FTP ユーザーを表示及び変更する

FTP ユーザーを表示及び変更するには

1. [FTP Users] 画面に移動します。

[File Services] 画面で [FTP Users] をクリックして、[FTP Users] 画面を表示します。次に [details] をクリックして、[FTP User Details] 画面を表示します。

The screenshot shows a web-based interface for managing FTP users. The title bar reads 'File Services | Home > File Services > FTP Users > FTP User Details'. The main content area is titled 'FTP User Details'. It contains a form with the following elements: 'File System: No File System Selected' with a 'change...' button; 'User Name: ftptest-0001'; 'Initial Directory for the user: /optest/0001' with a 'browse...' button; and a 'Path Options' section with a checked checkbox for 'Create path if it does not exist. (See online help for security implications)'. At the bottom are 'OK' and 'cancel' buttons.

2. 必要に応じて、設定を変更します。
 - [File System] フィールドで、[change...] をクリックして、別のファイルシステムを選択できます。
 - [Initial Directory for the user] フィールドで、別のディレクトリへのパスを入力することによって、ディレクトリを変更できます。[browse] ボタンをクリックすると、必要なディ

レクトリを探せます。このディレクトリは、FTP でログイン後に、ユーザーが開始する場所です。

- まだパスが存在しない場合は、[Path Options] ボックスの [Create path if it does not exist] チェックボックスをオンにして、パスを自動作成できます。



重要 自動作成されるディレクトリは、ルートユーザー及びグループ (UID:0/GID:0) によって所有され、全てのユーザーがアクセスできます (つまり、アクセス許可は `rw-rw-rw-` に設定されます)。そのようなディレクトリは CIFS または NFS を介して作成するか、このオプションを使用して作成した後、必要なアクセス許可を明示的に付与することが推奨されます。

3. プロセスを開始します。

FTP ユーザーの設定を変更するには、設定を確認してから、[OK] をクリックします。

6.1.3 セキュアプロキシ FTPS サービスを使う

セキュアプロキシ FTPS サービス (FTP with support for TLS) により、FTP クライアントから HNAS 上のファイルやディレクトリにセキュアにアクセスできます。

FTPS サービスは、独立した Linux ベースの機器で動作し、NFS を使用して HNAS ファイルシステムにアクセスします。HNAS FTP サービスのように、FTPS サービスは FTP ユーザー名と Unix/NT ユーザー名のダイレクトマッピングを前提とします。

FTPS サービスは、ユーザー認証と Unix 証明書取得をサポートします。API コマンドにより、ネットワークユーザーを認証して、証明書をレポートできます。

FTPS サービスを以下に示します。

- ユーザーがアクセスする EVS で使用されるディレクトリサービス (NIS/AD) に対して、FTP ユーザーを認証する。
- FTP ユーザーの HNAS 証明書を Unix 証明書にマップする。
- ユーザーに代わって HNAS にアクセスするとき、FTP ユーザーのマップされた Unix 証明書を使用する。

(1) FTPS API コマンド

CLI コマンドの `user-authenticate` は、ユーザー名とパスワードの NT または NIS 認証を実行して、ユーザーの Unix 証明書をレポートします。

(2) FTPS サービスの構成

NT 認証を介して Unix 証明書に取得されるマッピング証明書を使用するには、以下の構成が必要です。

- ドメイン、またはユーザーとグループのマッピング (CLI コマンドの `domain-mappings-add`, `user-mappings-add`, `group-mappings-add` を参照してください。)
- ユーザーとプライマリグループのマッピング (`primary-group-`, `localgroup` を参照してください。)

(3) コマンド形式

```
user-authenticate [--no-nt-auth] | [--no-nis-auth]] [--base64-args] [--json] [--report-unix-credentials] [--interactive] <user-name>
[<password>]
```

コマンドの説明

`--no-nt-auth, --no-nis-auth`

これらのコマンドは、認証を NT または NIS のどちらかに制限することができます。

`--base64-args`

`<user-name>` と `<password>` フィールドが base64 エンコードされていることを示します。

`--json`

JSON フォーマット出力を使用します。

`--report-unix-credentials`

ユーザーのマッピングされた Unix 証明書を `stdout` に出力します (認証が成功した場合)。

`--interactive`

パスワードを対話式で入力することを許可します (テスト、トラブルシューティング、一般使用のため)。

`<user-name>`

ユーザー名 (必須)。

`<password>`

パスワード (`--interactive` を指定した場合を除いて、必須)。

(4) 診断

認証失敗: コマンドは、認証に失敗したユーザー名と試みられた認証タイプをログに取得します。

このロギングは、ユーザー名ごとに出力量を制御する必要があります (例えば、`IdenticalMessagePacer` を使用して)。

性能: 以下の性能アキュムレーターは、PIR によって加えられてレポートされます。

- 経過時間性能アキュムレーター
- NT 認証時間性能アキュムレーター
- NIS 認証時間性能アキュムレーター
- 成功/失敗カウンター

6.1.4 FTP 統計

HNAS の FTP 統計 (10 秒のタイムスライス) は、前回の再起動から、または統計データが前回リセットされた時点からのアクティビティについて利用できます。

6.1.5 FTP 監査ロギングをセットアップする

FTP は、ユーザーアクティビティを追跡するために、監査ログを生成します。ユーザーが以下のアクションを行うたびに、システムはイベントを記録します。

- ログインまたはログアウト
- ファイル名変更またはファイル削除
- ファイルの取得、追加、保存
- ディレクトリの作成または削除

システムは、セッションのタイムアウトが発生したときも記録します。

各ログファイルは、各 FTP イベントにつき 1 行記述する、タブ区切りテキストファイルです。イベント発生日時を記録する他、システムは、クライアントのユーザー名と IP アドレス、実行されたコマンドについての説明を記録します。最新ログファイルの名前は「ftp.log」となり、古いファイルの名前は「ftpn.log」となります（n の値が大きいほど、古いファイルです）。

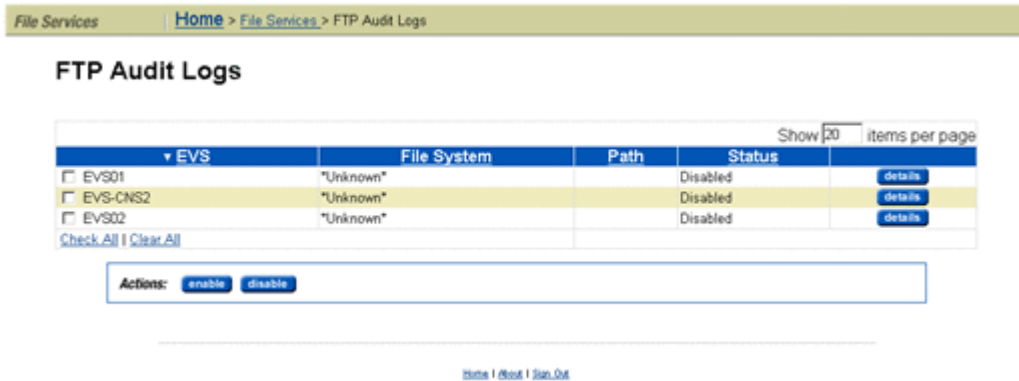
(1) FTP 監査ロギングを構成する

FTP 監査ロギング構成を表示及び変更するには

1. [FTP Audit Logs] 画面に移動します。

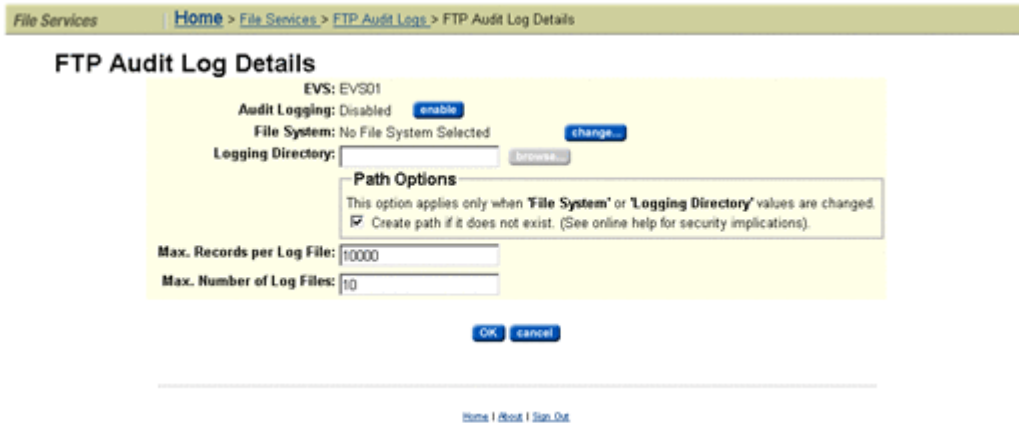
[File Services] 画面で [FTP Audit Logs] をクリックして、以下の画面を表示します。

EVS 一覧が表示されます。



2. FTP 監査ロギング構成を表示または変更する EVS を選択します。

FTP 監査ロギング構成を表示または変更するには、[details] をクリックして、[FTP Audit Log Details] 画面を表示します。



3. 必要に応じて、設定の表示や変更を行います。

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS	[EVS] フィールドで、ログファイルの EVS を指定します。
Audit Logging	[enable] または [disable] ボタンをクリックすると、FTP 監査ロギングが有効または無効になります。
File System	ログファイルを保存するファイルシステムです。変更するには、[change...] ボタンをクリックします。
Logging Directory	ログファイルを保存するように指定したファイルシステム上にあるディレクトリです。

項目／フィールド	説明
Path options	このチェックボックスをオンにすると、[Logging Directory] がない場合に自動作成されます。 注：自動作成されるディレクトリは、ルートユーザー及びグループ (UID:0/GID:0) によって所有され、全てのユーザーがアクセスできます（つまり、アクセス許可は rwxrwxrwx に設定されます）。そのようなディレクトリは CIFS または NFS を介して作成するか、このオプションを使用して作成した後、必要なアクセス許可を明示的に付与することが推奨されます。
Max. Records per Log File	各ログファイルに保存するレコードの最大数です。最適な性能を得るために、小さいファイルをたくさん作成するのではなく、大きなファイルを少数作成してください。
Max. Number of Log Files	保存するログファイルの最大数です。HNAS は、この制限に達すると、新しいログファイルを作成するたびに、最も古いログファイルを削除します。

4. 設定を保存します。

設定を確認し、[OK] をクリックして保存します。キャンセルするには、[cancel] をクリックします。

iSCSI を介したブロックレベルアクセス

- 7.1 iSCSI を介したブロックレベルアクセス

7.1 iSCSI を介したブロックレベルアクセス

HNAS は、iSCSI をサポートしています。Internet Small Computer System Interface (iSCSI) プロトコルが、要求アプリケーションと iSCSI ターゲットデバイス間のブロックレベルのデータ転送を有効にします。Microsoft iSCSI Software イニシエーター (バージョン 1.06 以降) を使用して、Windows サーバは、iSCSI ターゲットを、ローカルに接続したハードディスクとして表示します。Windows は、iSCSI ターゲット上にファイルシステムを作成し、ローカルディスクにあるのと同じように、データの読み取りと書き込みを実行します。Microsoft Exchange、Microsoft SQL Server などの Windows サーバアプリケーションは、iSCSI ターゲットをデータレポジトリとして使用して動作できます。

iSCSI サーバの導入に対しては、マイクロソフトの Designed for Windows Server™ 2003 認定を取得しています。Designed for Windows Server™ 2003 ロゴは、Microsoft Windows Server 2003 オペレーティングシステムによって質の高いコンピューティング体験をもたらす製品を、顧客が識別できるようにするためのものです。

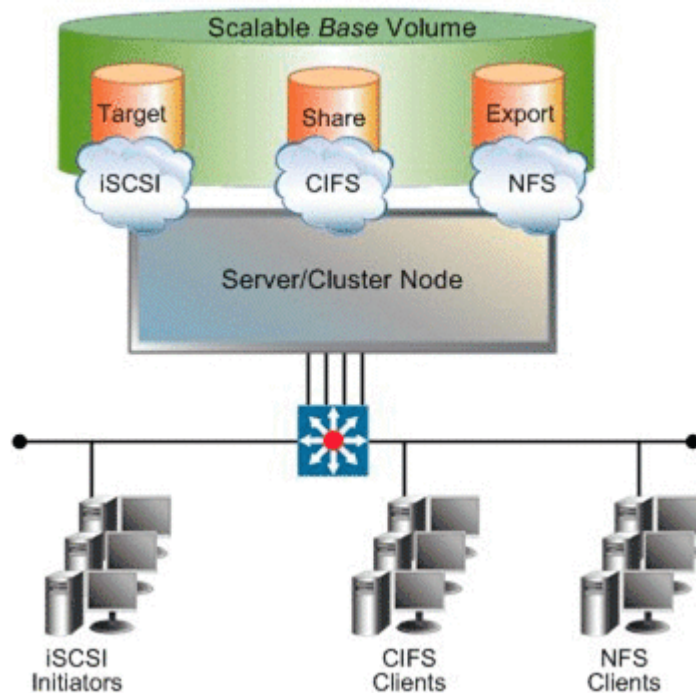


7.1.1 iSCSI サポート

HNAS 上の iSCSI ストレージを使用するには、一つ以上の iSCSI 論理ユニット (LU) を定義する必要があります。iSCSI 論理ユニットは、iSCSI ターゲットを介してアクセスされる、SCSI ストレージブロックです。iSCSI ターゲットは、iSNS データベースまたはターゲットポータルを介して検出できます。iSCSI ターゲットが検出されると、Windows サーバ上で実行中のイニシエーターが、ターゲットを介して、「ローカルディスク」として LU にアクセスできます。セキュリティメカニズムを使用して、iSCSI ターゲットへの不正アクセスを防止できます。

HNAS 上では、iSCSI 論理ユニットは、ファイルシステムにある通常ファイルにすぎません。結果として、iSCSI は、NVRAM ログイン、スナップショット、Quota といった、HNAS が備えているファイルシステム管理機能の恩恵を受けています。

iSCSI 論理ユニットの内容は、Windows サーバで管理されます。HNAS が、生データを含むファイルとして LU を表示する場合、Windows は、各 iSCSI ターゲットを論理ディスクとして表示し、ファイルシステムボリュームとして (通常は、NTFS を使用して) 管理します。その結果、iSCSI 論理ユニット内の個別ファイルには、Windows サーバからのみアクセスできます。スナップショットなどの HNAS のサービスは、NTFS ボリューム全体でのみ動作します。個別ファイル上では動作しません。



(1) iSCSI MPIO

iSCSI MPIO（マルチパス入出力）は、冗長パスを使用して、クライアントと iSCSI ストレージの間に、複数の論理「パス」を作成します。一つ以上のコンポーネントが障害に陥り、パスの失敗を招く場合、マルチパス論理は代替パスを使用して、アプリケーションがデータにアクセスできるようにします。

例えば、複数のイーサネット接続を使用しているクライアントは、論理パスを使用して、HNAS 上の iSCSI ターゲットに対するマルチパス接続を確立できます。冗長パスにより、特定のパスが失敗した場合でも、iSCSI セッションを中断せずに継続させることができます。iSCSI MPIO 接続は負荷分散通信にも使用でき、性能を高めることができます。

オフロードエンジンを使用する場合は、Microsoft マルチパス及び負荷分散に対応しているどうかを確認してください。

iSCSI MPIO は、Microsoft iSCSI イニシエーター 2.0 でサポートされています。

(2) iSCSI アクセス統計

この統計は、前回の HNAS 起動以降、または統計データリセット以降の、iSCSI アクティビティを監視するために使用できます。この統計データは、10 秒ごとに更新されます。

(3) 前提条件

iSCSI 機能を有効にするには

- iSCSI ライセンスキーを入力します。
- iSCSI サービスを有効にします。

(4) サポートされている iSCSI イニシエーター

HNAS が現在サポートしているのは、以下の iSCSI イニシエーターです。

- Microsoft iSCSI イニシエーター、バージョン 1.06 以降
- Microsoft iSCSI イニシエーター、バージョン 2.05 (MPIO サポート提供)

- Linux iSCSI イニシエーター, バージョン 3.4.2, 3.6.2, 3.6.3, 及び 4.0.188.13 (SourceForge 上の Linux iSCSI プロジェクトから利用可能)
- Solaris 10 U2 (64 ビット) ネイティブイニシエーター, iscsiadm v1.0
- Macintosh (OS X 10.4 Tiger) ATTO Xtend SAN v3.10
- Open iSCSI, バージョン 2.0.865



重要 その他の iSCSI イニシエーターや, 上記イニシエーターの各バージョンも, HNAS で機能する場合がありますが, テストは実施していません。サポートされている iSCSI イニシエーターの最新リストについては, お問い合わせ先に確認してください。

(5) オフロードエンジン

HNAS は現在, Microsoft iSCSI イニシエーター (バージョン 1.06) 以降と共に使用する場合, Alacritech SES1001T 及び SES1001F のオフロードエンジンをサポートしています。サポートされているオフロードエンジンの最新リストについては, お問い合わせ先に確認してください。

7.1.2 iSCSI を構成する

HNAS 上で iSCSI を構成するには, 以下の情報を指定する必要があります。

- iSNS サーバ
- iSCSI 論理ユニット
- iSCSI ターゲット (iSCSI ドメインを含む)
- iSCSI イニシエーター (相互認証を使用する場合)

(1) iSNS を構成する

インターネット記憶域名前サービス (iSNS : Internet Storage Name Service) は, iSCSI イニシエーター及び iSCSI ターゲットのネットワークデータベースです。構成する場合, HNAS は, ターゲットリストを iSNS に追加できます。それにより, イニシエーターは, ネットワーク上にあるターゲットを簡単に検出できるようになります。

iSNS サーバリストは, [iSNS Servers] 画面で管理できます。HNAS は, 以下のイベントが発生すると, iSCSI ターゲットを iSNS データベースに登録します。

- 最初の iSNS サーバの追加
- iSCSI ターゲットの追加または削除
- iSCSI サービスの開始
- iSCSI ドメインの変更
- EVS の IP アドレスの追加または削除

(2) iSNS サーバを作成及び削除する

iSNS サーバを作成及び削除するには

1. [iSNS Servers] 画面に移動します。
[File Services] 画面で [iSNS Servers] をクリックして, [iSNS Servers] 画面を表示します。



2. 必要に応じて、EVS を変更します。
表示されている EVS の名前は、iSNS サーバの追加先の EVS を示しています。
別の EVS を選択するには、[change...] をクリックします。
3. iSNS サーバを追加または削除します。
 - iSNS サーバを追加するには、[add] をクリックして、[Add iSNS Server] 画面を表示します。



次に、iSNS サーバの IP アドレスとポート番号（デフォルトのポート番号は、3205 です）を入力して、[OK] をクリックします。

- iSNS サーバを削除するには、削除する iSNS サーバを選択して（削除する iSNS サーバの IP アドレスの横にあるチェックボックスをオンにして）、[delete] をクリックします。



重要 Microsoft iSNS サーバの最新バージョンをダウンロードするには、<http://www.microsoft.com> にアクセスしてください。

7.1.3 iSCSI 論理ユニットを構成する

(1) iSCSI 論理ユニットをセットアップする

iSCSI 論理ユニット (LU) は、ローカルに接続したハードディスクとして、iSCSI イニシエーターがアクセスできるストレージブロックです。LU は、サーバファイルシステム上のファイルとして保存されます。サーバファイルシステム上で設定されている他のデータセットと同様に、iSCSI 論理ユニットは、仮想ボリュームや Quota など、HNAS のサイズ管理ツールを使用して、サイズにバインドできます。LU は、特定の初期サイズで作成されますが、ニーズに応じて、徐々に拡張できます。

LU を作成し、iSCSI ドメイン名を設定した後、iSCSI ターゲットを作成して、LU にアクセスできるようにする必要があります。iSCSI ターゲットごとに、最大 32 の LU を構成できます。

論理ユニットの管理

iSCSI 論理ユニットは、HNAS のファイルシステムの一つの中にあるファイルです。このようなファイルは、iSCSI 論理ユニットとして識別するために、「.iscsi」という拡張子を持つ必要があります。ただし、この拡張子を除いて、ファイルが確かに LU であるかどうかを判断する方法はありません。



重要 全ての iSCSI 論理ユニットを、/iscsi/などの既知のディレクトリ内に配置することを推奨します。こうすることで、既知の場所の LU に、単一のレポジトリが用意されます。

論理ユニットのセキュリティ

LU はファイルなので、CIFS や NFS といった、他のプロトコルでアクセスできます。そのため、修正、名前変更、削除や、ファイルに影響を及ぼすその他の方法を実行できる悪意あるユーザーに対して、LU は脆弱です。



注意 迷惑アクセスを防ぐために、LU ファイル、LU の属するディレクトリ、またはその両方に、十分なセキュリティを設定することを推奨します。

論理ユニットへの同時アクセス

HNAS に iSCSI を実装することで、複数のイニシエーターが単一の LU にアクセスできるようになります。このことは、ファイルシステムへの同時アクセスをサポートする、またはファイルシステムへの同時アクセスに依存する、アプリケーションやオペレーティングシステムに不可欠です。しかし、その一方で、クライアントが、他のクライアントがファイルシステムにアクセスしていることに気付かない場合に、同時アクセスが、クライアントマシンに害を及ぼす可能性があります。例えば、以下のような場合です。

- 同一ファイルが、同時に、別個で更新される場合

シナリオ

2 台の独立した Microsoft Windows クライアントが、NTFS ファイルシステムを含む同一 LU に接続できる。

結果

同時に、かつ別個にデータ、メタデータ、システムファイルを変更できる場合、相反するディスク更新によって、ファイルシステムが即座に破損する。

- 同時アクセスして、パーティションを分割する場合

シナリオ

一つの LU に、区別できる二つの NTFS パーティションが含まれている。パーティションの一つは、第 1 パーティションにのみ接続できる Microsoft Windows クライアント、もう一つは、第 2 パーティションにのみ接続できる Microsoft Windows クライアントを持っている。

結果

Microsoft iSCSI クライアントが、LU 上で検出した各パーティションのマウントを試みるため、NTFS パーティションをマウントしている Microsoft Windows クライアントが、全てのパーティション上のシステムファイルを更新する。その結果、2 台のクライアントが LU 内の別個のパーティションにアクセス中にもかかわらず、両クライアントが、両方のパーティション上でシステムファイルを更新する。それにより、システムファイル更新が相反し、一方または両方のクライアントが失敗する原因となる。

論理ユニットのスナップショットを取る

iSCSI 論理ユニットのデータは、アクセスするクライアントによって完全に制御されます。HNAS は、ファイルシステムや LU 内に含まれるデータを決して解読できません。そのため、HNAS は、

iSCSI 論理ユニット内に保持されているデータが一貫した状態かどうかを把握しません。これにより、LU スナップショットを取るときに、潜在的な問題が生じます。

例えば、クライアントがファイルを作成するときには、ファイル名をホストディレクトリに挿入する必要もあります。これは、操作を完了するには、複数の書き込みが必要だということです。ファイルオブジェクト作成後、名前がディレクトリに挿入される前に、HNAS がスナップショットを作成すると、スナップショットに含まれているファイルシステムの整合性が取れなくなります。別のクライアントが、万が一ファイルシステムのスナップショットのコピーを表示すれば、ディレクトリで名前のないファイルオブジェクトを見ることになるはずですが、この例は、スナップショットの整合性欠如に関して、起こり得るシナリオの一つを提示しているにすぎません。



注意 iSCSI 論理ユニットのスナップショットを作成する前に、全てのアプリケーションを既知の状態にすることを推奨します。例えば、データベースは休止させてください。スナップショットを作成する LU から iSCSI イニシエーターを切断することも、推奨します。こうすることで、全ての保留中の書き込みが、スナップショットを作成する前に LU に送信されるようになります。

ボリュームフルの状態

以下の二つの例が示すとおり、iSCSI 論理ユニットが原因で、ボリュームフルの状態が生じてしまう可能性があります。

- 直接接続されたディスク。クライアントが、直接接続されたディスクを使用すると、利用できる空き容量を監視できます。パーティションに空き容量がない場合、クライアントは、ボリュームフルの状態を返します。このようにして、クライアントは、操作の途中で起こる、ディスク領域不足によるファイルシステムの破損を予防できます。
- iSCSI 論理ユニット。バックグラウンドを経由して、スナップショットが有効な iSCSI 論理ユニット上で、古いデータが上書きせずに保存されます。そのため、LU の領域への上書きは、ノードが、余分なディスク領域を割り当てることとなります。その際、クライアントのパーティション内で余計なディスク領域は使用されませんが、LU 内のパーティションに空き容量があっても、ボリュームフルの状態が発生します。このシナリオでは、クライアントが、操作途中でボリュームフルの状態を受け取ることがあります。これはファイルシステムの破損の原因となります。この破損は修復可能ですが、こうした状況は回避してください。



注意 全ての iSCSI 論理ユニット及びスナップショットを含めるために、十分なディスク領域をノードに割り当てることと、ディスクの空き容量を慎重に監視することを推奨します。

(2) iSCSI 論理ユニットを管理する

iSCSI 論理ユニットのプロパティを表示する

iSCSI 論理ユニットのプロパティを表示するには、[File Services] 画面に移動し、[iSCSI Logical Units] をクリックして、[iSCSI Logical Units] 画面を表示します。

iSCSI Logical Units

EVS / File System Label

EVS01 / All File Systems

[change](#)

Alias	File System:Path	Size	Status	
<input type="checkbox"/> iSCSI-TEST	FS02:/iscsi1.iscsi	100 MB	Unmounted	details
<input type="checkbox"/> test4	FS02:/doctest/testfile04.iscsi	2 MB	Unmounted	details
<input type="checkbox"/> testey	FS02:/#_CFN_.iscsi	10 MB	Unmounted	details

[Check All](#) | [Clear All](#)Actions: [mount](#) [unmount](#) [delete](#) | [add](#)Shortcuts: [iSCSI Targets](#) [iSCSI Initiator Authentication](#)[Home](#) | [About](#) | [Sign Out](#)

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS/File System Label	LUが存在するか、またはLUを作成できる、EVS及びファイルシステムを選択します。
Alias	LUの名前です。
File System:Path	LUのファイルシステムとパスです。 注：LUは、サーバファイルシステム上で、通常ファイルと同じように表示されます。
Size	LUのサイズです。 注：LUの最大サイズは、2TBです。この制限は、SCSIプロトコルが課しているものです。
Status	LUのステータスを示します。通常は、LUがマウントされているかどうかを表示します。 注：LUが非同期的に作成されている場合、ステータスには [Unmounted] と表示されます。その後、作成が完了すれば、[Mounted] と表示されます。

iSCSI 論理ユニットを追加する

1. [Add iSCSI Logical Unit] 画面に移動します。

[File Services] 画面で、[iSCSI Logical Units] を選択した後、[add] をクリックして [Add iSCSI Logical Unit] 画面を表示します。

Add iSCSI Logical Unit

2. 必要に応じて、EVS やファイルシステムを変更します。
表示される EVS 名は、LU の追加先となる EVS 及びファイルシステムを示します。別の EVS またはファイルシステムを選択するには、[change...] をクリックします。
3. 論理ユニットの別名を指定します。
[Alias] フィールドで、LU の名前を入力します。
4. ファイルへのパスが既に存在する場合は、論理ユニットへのパスを指定します。
既に存在する LU のパスを入力するときには、完了までに複数のステップがあります。
 - a. ファイルを選択します。
[browse] をクリックすると、LU のファイルを選択できるダイアログが表示されます。また、[browse] ボタンを使わずに、ファイルのパス名（拡張子を含む）を入力することもできます。
 - b. [File Already Exists] ラジオボタンを選択します。
 - c. 必要に応じて、コメントを追加します。
[Comment] フィールドを使って、LU に関する説明を提供できます。
 - d. 論理ユニット定義を保存します。
[OK] をクリックして、LU を追加します。
5. ファイルへのパスがまだ存在しない場合は、論理ユニットへのパスを作成します。
LU 用として新規ファイルを作成するときには、完了までに複数のステップがあります。
 - a. ファイルのパスを選択します。
[browse] をクリックすると、LU のファイルのディレクトリを選択できるダイアログが表示されます。ファイルとディレクトリの名前を指定する必要があります。ファイルに、拡張子は必要ありません。「.iscsi」が自動的に追加されます。また、[browse] ボタンを使わずに、ファイル名とパス（拡張子を含む）を入力することもできます。
 - b. [Create File] ラジオボタンを選択します。
 - c. 論理ユニットのサイズを指定します。
[Size] フィールドとドロップダウンリストを使用して、LU ファイルのサイズを指定します。
 - d. [Create path to file if it does not exist] チェックボックスをオンにします。
 - e. 必要に応じて、コメントを追加します。

[Comment] フィールドを使って、LU に関する説明を提供できます。

f. 論理ユニットの定義を保存します。

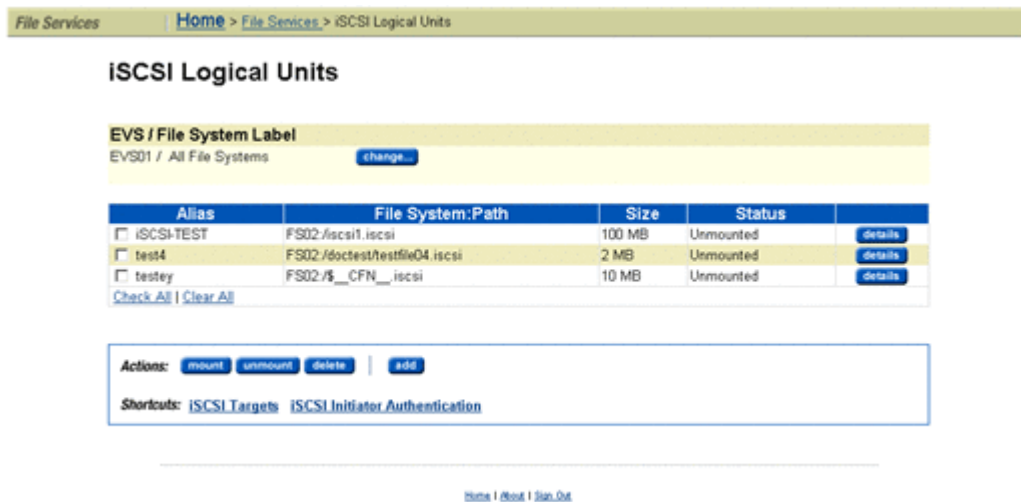
[OK] をクリックして、LU を追加します。

iSCSI 論理ユニットを変更または削除する

iSCSI 論理ユニットを変更または削除するには

1. [iSCSI Logical Units] 画面に移動します。

[File Services] 画面で、[iSCSI Logical Units] をクリックして、[iSCSI Logical Units] 画面を表示します。



2. 必要に応じて、EVS やファイルシステムを変更します。

表示される EVS 名は、LU が存在する EVS 及びファイルシステムを示します。別の EVS またはファイルシステムを選択するには、[change...] をクリックします。

3. 変更または削除する論理ユニットを選択します。

変更または削除する LU の横にあるチェックボックスをオンにします。

4. 変更または削除します。

- iSCSI 論理ユニットを削除するには、LU を選択して、[delete] をクリックします。[Confirm Delete] ポップアップウィンドウに、[Delete] オプションが表示されます。LU を削除するには、選択して [OK] をクリックします。LU を削除せずにポップアップウィンドウを閉じるには、[cancel] をクリックします。

- iSCSI 論理ユニットを変更するには

[details] をクリックして、[iSCSI Logical Unit Details] 画面を表示します。

iSCSI Logical Unit Details for test4

次の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS/File System	LU をホストしている、EVS 及びファイルシステムを表示します。
Status	LU がマウントされているか、アンマウントされているかを示します。基盤となるファイルシステムをマウントしたままの状態、LU のマウントやアンマウントを実行できます。 LU がマウントされていないとき、[mount] をクリックすると、LU がマウントされます。LU がマウントされているとき、[unmount] をクリックすると、LU がアンマウントされます。 [Create .iscsi file during this mount if it does not exist] チェックボックスをオンにすると、マウントしている間、.iscsi ファイルが存在しない場合はファイルを作成します。
Alias	LU の名前です。この名前は変更できます。
Path to File	LU ファイルへの完全なファイルシステムパスです。 注：LU は、サーバファイルシステム上で、通常ファイルと同じように表示されます。
Size	LU のサイズです。 注：LU の最大サイズは、2TB です。この制限は、SCSI プロトコルが課しているものです。

- 論理ユニットのプロパティを変更します。
必要に応じて、LU の設定を変更します。
- 設定を保存します。
設定を確認し、[OK] をクリックして変更を保存します。キャンセルするには、[cancel] をクリックします。

iSCSI 論理ユニットをバックアップする

ターゲットを介して LU に接続されているクライアントに限り、LU に含まれている個別のファイル及びディレクトリにアクセスして、バックアップできます。LU は、サーバファイルシステムの通常ファイルとしてバックアップします。



注意 HNAS から iSCSI 論理ユニットをバックアップする場合は、iSCSI イニシエーターを確実に切断します。または、スナップショットからバックアップを作成します。

iSCSI 論理ユニットをバックアップするには

1. ターゲットから、iSCSI イニシエーターを切断します。
2. iSCSI 論理ユニットをアンマウントします。
iSCSI 論理ユニットをアンマウントするには、以下の CLI コマンドが使用できます。

```
iscsi-lu unmount <名前>
```


この場合、<名前>は iSCSI 論理ユニット名です。
3. スナップショットまたはバックアップデバイスに、論理ユニットをバックアップします。
安全のため、iSCSI 論理ユニットを、スナップショットか、別のバックアップデバイスにバックアップしてください。このプロセスの詳細については、「[論理ユニットのスナップショットを取る](#)」を参照してください。
4. 論理ユニットをマウントします。
iSCSI 論理ユニットをマウントするには、以下の CLI コマンドが使用できます。

```
iscsi-lu mount <名前>
```


この場合、<名前>は iSCSI 論理ユニット名です。
5. iSCSI イニシエーターを使って、iSCSI ターゲットに再接続します。
6. 必要に応じて、ディスクを再スキャンします。
LU をクライアントに再表示するために、Windows Computer Manager 再スキャンディスクを使用することが必要な場合があります。このプロセスの詳細については、「[7.1.6 \(6\) Computer Manager を使用して iSCSI ストレージを設定する](#)」を参照してください。

iSCSI 論理ユニットを復元する

LU のデータの一貫性を確保するために、スナップショットまたはバックアップからのデータの復元が必要となる場合があります。iSCSI 論理ユニットを復元するには、以下のステップを実行します。

iSCSI 論理ユニットを復元するには

1. ターゲットから、iSCSI イニシエーターを切断します。
2. iSCSI 論理ユニットをアンマウントします。
CLI コマンド `iscsi-lu unmount <名前>` を使用します。この場合、<名前>は LU 名です。
3. スナップショットまたはバックアップから、論理ユニットを復元します。
4. iSCSI 論理ユニットをマウントします。
CLI コマンド `iscsi-lu mount <名前>` を使用します。この場合、<名前>は LU 名です。
5. iSCSI イニシエーターを使って、ターゲットに再接続します。
6. 必要に応じて、Computer Management でディスクを再スキャンします。
「[7.1.6 \(6\) Computer Manager を使用して iSCSI ストレージを設定する](#)」を参照してください。

7.1.4 iSCSI ターゲットを設定する

iSCSI ターゲットは、iSCSI イニシエーターにアクセス可能なストレージ構成要素です。iSCSI イニシエーター側では、それぞれの iSCSI ターゲットはネットワーク上でアクセス可能な別個のストレージデバイスとして表示されます。HNAS では、EVS 1 台につき最大 32 個の iSCSI ターゲット、ターゲット 1 個につき最大 32 件の iSCSI セッションをサポートしています。

(1) iSCSI ターゲットのプロパティを表示する

[File Services] 画面で、[iSCSI Targets] をクリックします。[iSCSI Targets] 画面が表示されます。



下の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS	ターゲットをホストする EVS を選択します。 別の EVS を選択するには [change...] をクリックします。
EVS iSCSI Domain	iSCSI ドメインを表示します。iSCSI ドメインは、iSCSI ターゲットに固有の修飾名を作成するときに使用する DNS ドメインです。
Alias	ターゲットの名前を識別します。
Comment	ターゲットに関連する追加情報を示します。
Globally Unique Name	ターゲットの名前を示します。HNAS によって自動的に生成される、全世界で一意的な名前です。

(2) iSCSI ターゲットを追加する

iSCSI ターゲットを追加するには

1. [Add iSCSI Target] 画面に移動します。
[File Services] 画面で [iSCSI Targets] を選択し、[add] をクリックすると、[Add iSCSI Target] 画面が表示されます。

Add iSCSI Target

下の表では、この画面のフィールドについて説明します。

項目/フィールド	説明
EVS	LU が存在する EVS を選択します。別の EVS に切り替えるには [change...] をクリックします。
EVS iSCSI Domain	iSCSI ドメインを表示します。iSCSI ドメインは、iSCSI ターゲットに固有の修飾名を作成するときに使用する DNS ドメインです。
Alias	iSCSI ターゲットの名前を識別します。
Comment	iSCSI ターゲットに関する追加情報を示します。
Enable Authentication	iSCSI ターゲットの認証を有効にします。デフォルトでは、このチェックボックスはオンになっています。チェックボックスをオンにすると認証が有効に、オフにすると無効になります。 認証が無効の場合、イニシエーターはターゲットの秘密鍵を知らなくてもターゲットとその LU への接続を許可されます。
Secret	不正アクセスからターゲットを保護するために使用するパスワードを示します。ターゲットに接続する際、イニシエーターが自動的にこのパスワードを認証します。秘密鍵は 12 文字以上 16 文字以下で設定してください。1~255 文字で設定することもできますが、12 文字未満や 17 文字以上の秘密鍵の場合、一部の iSCSI イニシエーターで拒否されることがあります。
Access Configuration	アクセス設定のパラメーターを入力します。構文については、下の [Access Configuration] に関する表を参照してください。
Available Logical Unit Name	iSCSI ターゲットに割り当て可能な LU のリストです。EVS 上の全ての LU がリストに含まれます。一部の LU は既に他のターゲットに割り当てられている場合があります。
Selected Logical Unit Number - Logical Unit Name	iSCSI ターゲットの一部として選択されている LU のリストです。
Logical Unit Number	LU に割り当てられている番号 (LUN) を示します。0~255 の範囲で論理ユニット番号を入力し、[OK] をクリックします。

2. iSCSI ターゲットに関する情報を入力します。
 - a. 必要な情報を指定します。

[iSCSI Domain], [Alias], [Available LUs] 及び [Logical Unit Number] は必須で、その他のフィールドはオプションです。

- b. 必要に応じて、ターゲットの [Comment] や [Secret], [Access Configuration] を指定します。

次の表では、[Access Configuration] フィールドの構文について説明します。

入力内容	意味
空白または*	全てのクライアントがターゲットにアクセスできます。
特定のアドレスまたは名前を示します。例：10.168.20.2, client.dept.company.com 特定のホストへのアクセスを拒否するには、no_access または noaccess 修飾子を使用します。例えば「10.1.2.38 (no_access)」と入力すると、10.1.2.38 という IP アドレスのホストへのアクセスを拒否します。	指定された名前またはアドレスのクライアントのみがターゲットにアクセスできます。
一部にワイルドカードを使用したアドレスや名前を示します。例：10.168.*.*, *.company.com 特定のホストへのアクセスを拒否するには、no_access または noaccess 修飾子を使用します。例えば「10.1.2.38 (no_access)」と入力すると、10.1.2.38 という IP アドレスのホストへのアクセスを拒否します。	名前やアドレスが一致するクライアントがターゲットにアクセスできます。

3. 設定を保存します。

設定内容を確認し、保存するには [OK], 保存せずに終了するには [cancel] をクリックします。

(3) iSCSI ターゲットへの LU を追加する

iSCSI ターゲットに LU を追加するには

1. [iSCSI Target Details] 画面に移動します。

[File Services] 画面で [iSCSI Targets] をクリックして [iSCSI Targets] 画面を表示し、[details] をクリックして、変更する iSCSI ターゲットの [iSCSI Target Details] 画面を表示します。

iSCSI Target Details for firstTarget

The screenshot shows the 'iSCSI Target Details for firstTarget' configuration page. It includes the following sections:

- EVS: EVS01**
 - EVS iSCSI Domain: www.night.com
 - Alias: firstTarget
 - Regenerate GUN
 - Comment: no comment
- Authentication**
 - Enable Authentication
 - Secret: [text input]
- Access Configuration**
 - [List box]
 - (Enter IP-based values first, if possible)
- Logical Unit selection**
 - Available**
 - Logical Unit Number: [text input]
 - Logical Unit Name: test4, testey
 - Selected**
 - Logical Unit Number - Logical Unit Name: 1 - iSCSI-TEST

Buttons: OK, cancel

Footer: Home | About | Sign Out

2. iSCSI 論理ユニットを追加します。

[Available Logical Units] リストから LU を選択し、[Logical Unit Number] フィールドで 0 ~255 の間の数字を指定して、右矢印をクリックして LU を [Selected Logical Units] リストに移動します。



重要 選択した LU が他のターゲットに割り当て済みでないことを確認してください。

3. 変更内容を保存します。

設定内容を確認し、保存するには [OK]、保存せずに終了するには [cancel] をクリックします。

(4) iSCSI ターゲットのプロパティを変更する

iSCSI ターゲットのプロパティを変更するには

1. [iSCSI Target Details] 画面に移動します。

[File Services] 画面で [iSCSI Targets] をクリックして [iSCSI Targets] 画面を表示し、[details] をクリックして、変更する iSCSI ターゲットの [iSCSI Target Details] 画面を表示します。

iSCSI Target Details for firstTarget

The screenshot shows the 'iSCSI Target Details for firstTarget' configuration page. It includes the following sections:

- EVS: EVS01**
 - EVS iSCSI Domain: www.right.com
 - Alias: firstTarget
 - Regenerate GUN
 - Comment: no comment
- Authentication**
 - Enable Authentication
 - Secret: [text input]
- Access Configuration**
 - [text area]
 - (Enter IP-based values first, if possible)
- Logical Unit selection**
 - Available**
 - Logical Unit Number: [text input]
 - Logical Unit Name: test4, testey
 - Selected**
 - Logical Unit Number - Logical Unit Name: 1 - iSCSI-TEST

Buttons: OK, cancel

Footer: Home | Logout | Sign Out

2. iSCSI ターゲットを変更します。

[iSCSI Domain], [Alias], [Available LUs] 及び [Logical Unit Number] は必須です。必要に応じて、ターゲットの [Comment] や [Secret], [Access Configuration] を指定できます。この画面の項目やフィールドの詳細については、「(2) iSCSI ターゲットを追加する」を参照してください。



重要 iSCSI ドメインはいったん設定すると変更できません。ただし、後から同じ EVS 内に別の iSCSI ドメインで新しく iSCSI ターゲットを指定した場合は、上書きまたは置き換えられます。最後に指定した iSCSI ドメインが、EVS 内で前に追加された全ての iSCSI ターゲットに設定されている全ての iSCSI ドメインに優先します。

3. 設定を保存します。

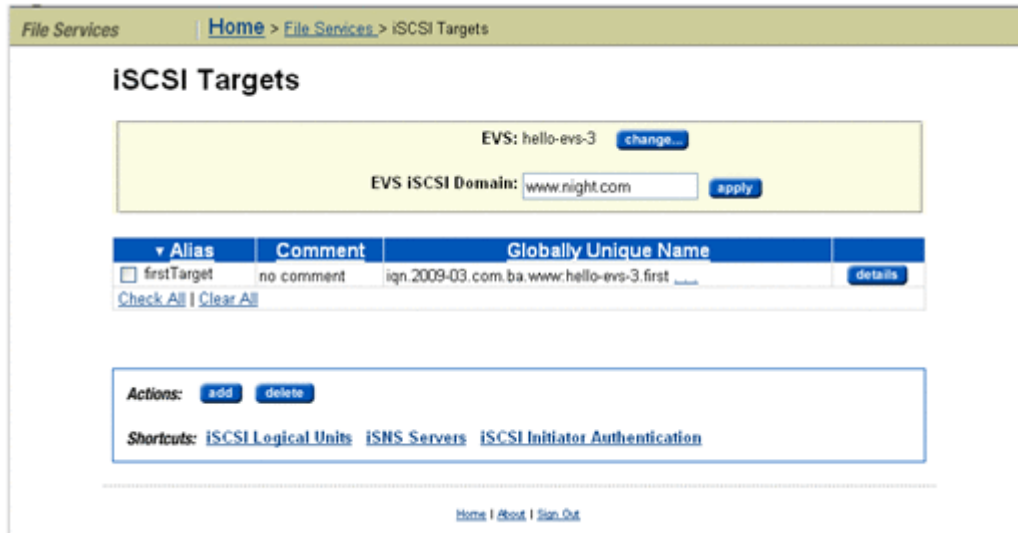
設定内容を確認した後、保存するには [OK], 保存せずに終了するには [cancel] をクリックします。

(5) iSCSI ターゲットを削除する

iSCSI ターゲットを削除するには

1. [iSCSI Targets] 画面に移動します。

[File Services] 画面で、[iSCSI Targets] をクリックします。[iSCSI Targets] 画面が表示されます。



2. iSCSI ターゲットを削除します。

[Alias] の横のチェックボックスをオンにすると表示されるリストからターゲットを選択し、[delete] をクリックします。確認ダイアログが表示されます。iSCSI ターゲットを削除するには [OK] を、ターゲットを削除せずに [iSCSI Targets] 画面に戻るには [cancel] をクリックします。

7.1.5 iSCSI のセキュリティを設定する（相互認証）

HNAS では、Challenge Handshake Authentication Protocol (CHAP) を使用して iSCSI イニシエーターを認証します。CHAP を使用するには、イニシエーターとターゲットが「共有秘密鍵」を知っている必要があります。HNAS 上のターゲットに対するイニシエーターによる認証に加えイニシエーターに対する HNAS による認証を行う必要がある相互認証もサポートされます。

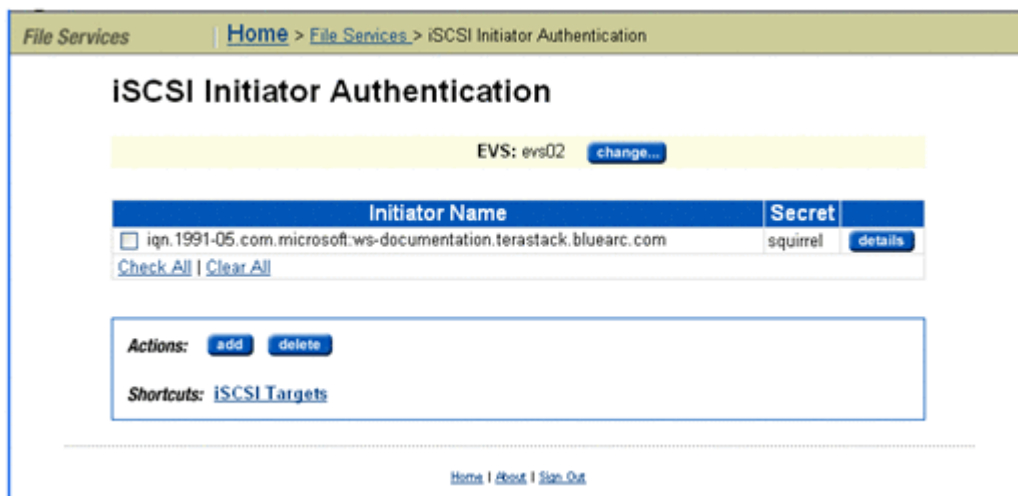
相互認証のプロセスを簡単にするには、認証に使用できるイニシエーターのリストとそのイニシエーターそれぞれの共有秘密鍵を HNAS が保持している必要があります。

(1) HNAS に相互認証を設定する

HNAS に相互認証を設定するには

1. [iSCSI Initiator Authentication] 画面に移動します。

[File Services] 画面で、[iSCSI Initiator Authentication] をクリックします。[iSCSI Initiator Authentication] 画面が表示されます。



この画面には、選択された EVS で現在指定されている全ての iSCSI イニシエーターが一覧表示されます。下の表では、この画面のフィールドについて説明します。

項目／フィールド	説明
EVS	イニシエーター認証の設定先の EVS を選択します。 別の EVS を選択するには [change...] をクリックします。
Initiator Name	地球上に唯一の名前でイニシエーターを識別します。
Secret	不正アクセスからイニシエーターを保護するために使用するパスワードを示します。秘密鍵は 1~255 文字でも設定できますが、12~17 文字で設定してください。

2. iSCSI イニシエーターを追加します。

a. [Add iSCSI Initiator] 画面に移動します。

[add] をクリックすると、[Add iSCSI Initiator] 画面が表示されます。

b. イニシエーター名を指定します。

イニシエーター名を入力します。この名前は、Microsoft iSCSI イニシエーターの [Initiator Node Name Change] ダイアログに表示されるものと同じです。

c. 秘密鍵を指定します。

[Secret] にイニシエーターの秘密鍵を入力します。これは、iSCSI イニシエーターの [Chap Secret Setup] ダイアログに入力する秘密鍵と同じです。

d. 設定を保存します。

設定内容を確認した後、保存するには [OK]、保存せずに終了するには [cancel] をクリックします。

(2) Microsoft iSCSI イニシエーターに相互認証を設定する

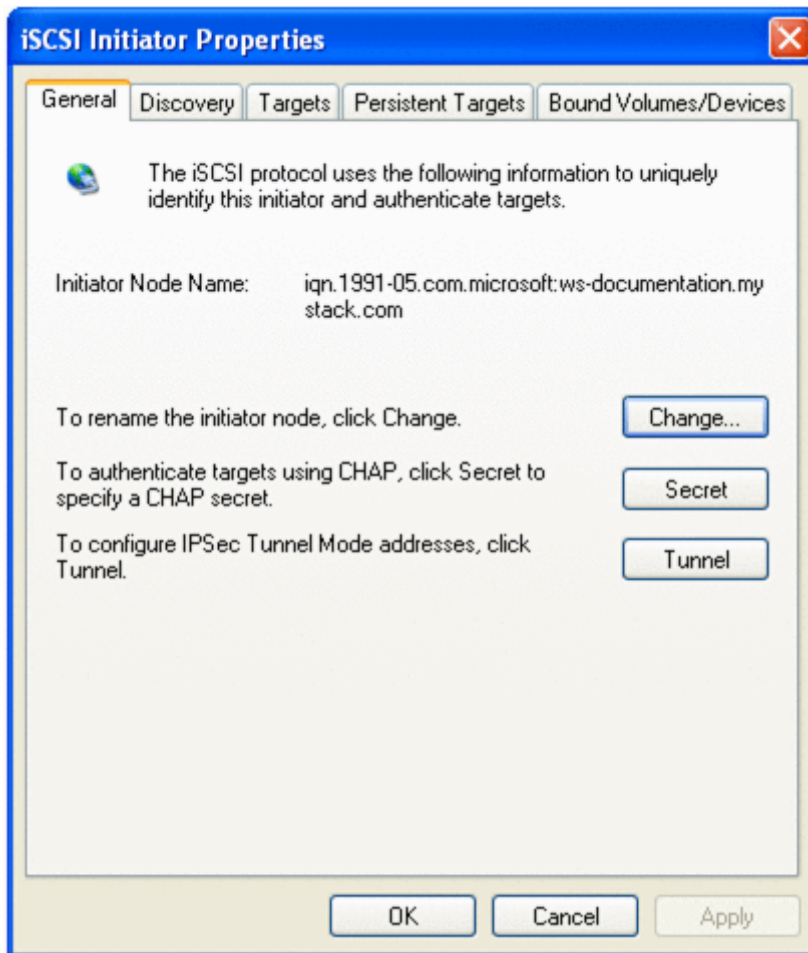


重要 Microsoft iSCSI Software イニシエーターの最新バージョンを入手するには、<http://www.microsoft.com/> にアクセスしてください。

相互認証のために Microsoft iSCSI イニシエーターを設定するには

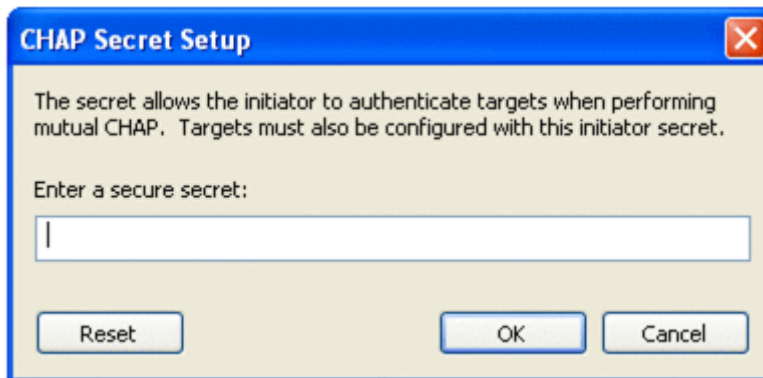
1. [iSCSI Initiator Properties] ウィンドウを開きます。

Microsoft iSCSI イニシエーターを起動し、[iSCSI Initiator Properties] ウィンドウを開きます。[General] タブが表示されます。



2. 秘密鍵を入力します。

[Secret] ボタンをクリックすると、[CHAP Secret Setup] ダイアログが表示されます。



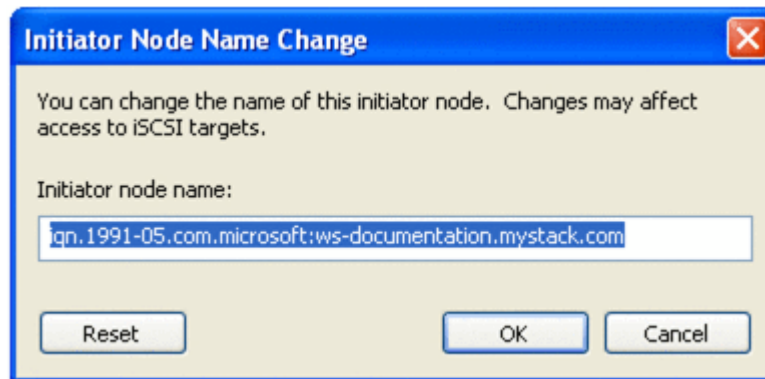
このフィールドに、相互 CHAP を実行する際にターゲットがイニシエーターと認証を行うための秘密鍵を入力して、[OK] をクリックします。



重要 イニシエーターと HNAS の認証に使用される共有秘密鍵は、ターゲットの設定時に指定した秘密鍵とは異なるものにしてください。

3. 必要に応じて、イニシエーターのノード名を変更します。

イニシエーターのノード名を変更するには、[Change...] ボタンをクリックして [Initiator Node Name Change] ダイアログを表示します。



このフィールドで、名前を変更して [OK] をクリックします。



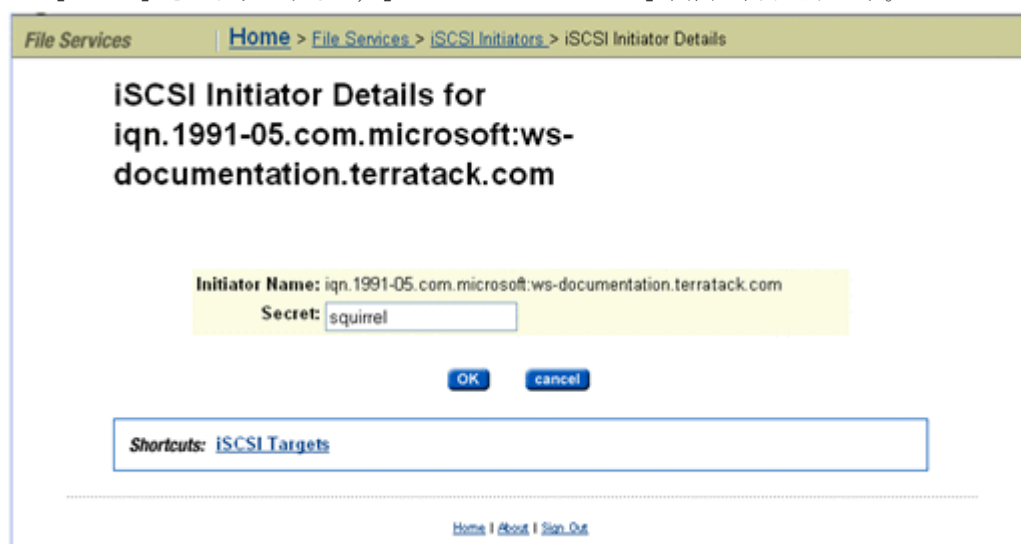
重要 イニシエーターのノード名は、[iSCSI Initiator Authentication] 画面 ([File Services] の下にあり
ます) の [Initiator Name] に使用する名前にしてください。

4. 変更内容を保存します。
設定内容を確認した後、保存するには [OK]、保存せずに終了するには [Cancel] をクリック
します。

(3) HNAS の相互認証設定を変更する

HNAS の相互認証の設定を変更するには、イニシエーターの秘密鍵を変更します。ただし、イニシ
エーターの名前は変更できません。

1. [iSCSI Initiator Authentication] 画面に移動します。
[File Services] 画面で、[iSCSI Initiator Authentication] をクリックします。[iSCSI Initiator
Authentication] 画面が表示されます。
2. 必要に応じて、イニシエーターの秘密鍵を変更します。
必要な場合は、次の方法でイニシエーターの秘密鍵を変更します。
 - a. [iSCSI Initiator Details] 画面に移動します。
[details] をクリックすると、[iSCSI Initiator Details] 画面が表示されます。



- b. 新しい秘密鍵を入力します。
[Secret] フィールドに、イニシエーターの新しい秘密鍵を入力します。秘密鍵は 1~255 文
字でも設定できますが、12~17 文字で設定してください。
- c. 設定を保存します。

設定内容を確認した後、保存するには [OK]、保存せずに終了するには [cancel] をクリックします。

- 必要に応じて、iSCSI イニシエーターを削除します。

イニシエーターとその秘密鍵を削除するには、[Initiator Name] フィールドのイニシエーター名の横にあるチェックボックスをオンにして [delete] をクリックします。確認ダイアログが表示されます。iSCSI イニシエーターを削除するには [OK] を、イニシエーターを削除せずに [iSCSI Targets] 画面に戻るには [cancel] をクリックします。

7.1.6 iSCSI ストレージにアクセスする

iSCSI の LU には、Microsoft iSCSI イニシエーターを使用して LU のターゲットからアクセスできます。iSNS 経由で検出されたかターゲットポータル経由で検出されたかにかかわらず、全ての使用可能な iSCSI ターゲットが、使用可能なターゲットとしてイニシエーターに表示されます。



注意 ダイナミックディスクに注意してください！—Microsoft では現在、iSCSI の LU 上でのベーシックディスクの作成のみをサポートしています。データの整合性を保つため、ダイナミックディスクは作成しないでください。詳細については、『*Microsoft iSCSI Initiator ユーザーガイド*』を参照してください。

基本となるボリュームが、HNAS によってマウントされた読み取り専用ボリュームである場合、または別の LU のスナップショットコピーである場合、iSCSI の LU も読み取り専用になります。そして LU が読み取り専用であれば、その LU に含まれるファイルシステムも読み取り専用になります。そのような読み取り専用のファイルシステムにアクセスするクライアントは、ファイルのデータやメタデータ、システムファイルを含め、ファイルシステムのいかなる部分も変更することはできません。

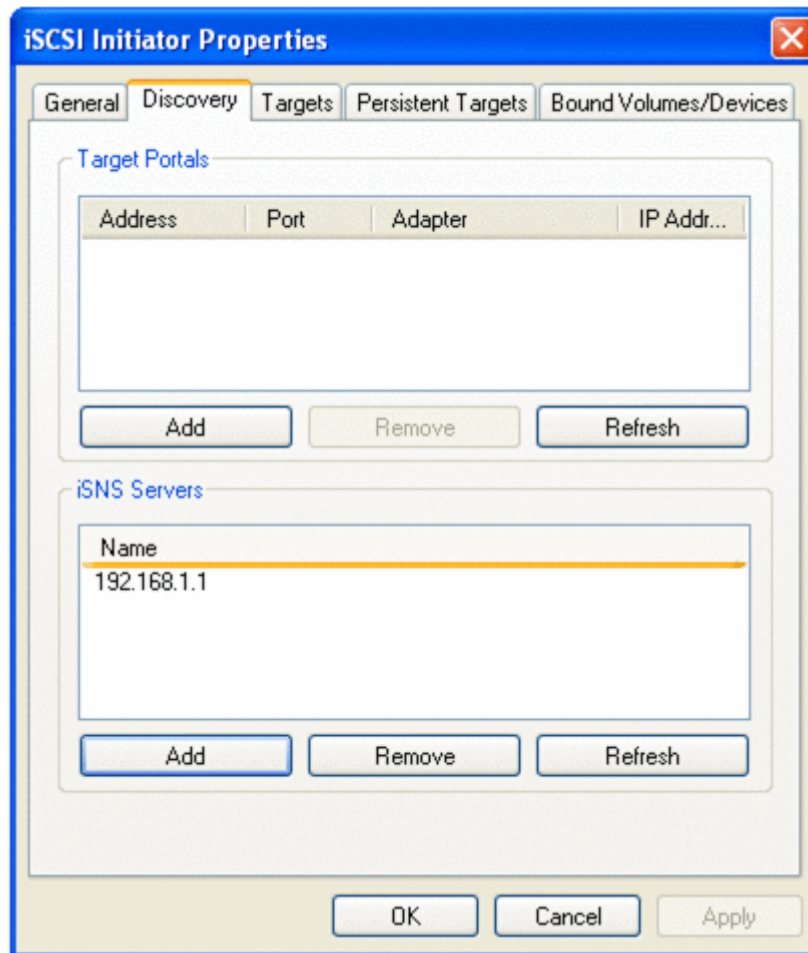
読み取り専用の FAT や FAT32 ファイルシステムをマウントすることは可能ですが、Microsoft Windows 2000 クライアントで読み取り専用の NTFS ファイルシステムをマウントすることはできません。Microsoft Windows 2003 クライアントでは、読み取り専用の FAT、FAT32 及び NTFS ファイルシステムをマウントできます。したがって、Microsoft Windows クライアントで iSCSI を介して読み取り専用の NTFS ファイルシステムにアクセスする必要がある場合は、Microsoft Windows 2003 を使用する必要があります。

(1) iSNS を使用して iSCSI ターゲットを検出する

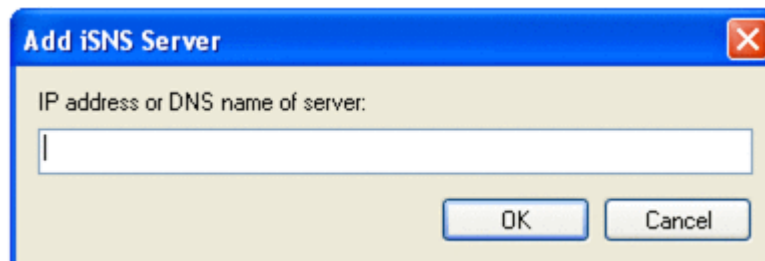
ネットワーク上で iSCSI ターゲットを検出するには、iSNS を使用するのがもっとも簡単な方法です。ネットワークが iSNS サーバで構成されている場合は、iSNS を使用するように Microsoft iSCSI イニシエーターを設定します。

iSNS サーバを追加するには

- [iSNS Servers] タブを開きます。
[Microsoft iSCSI Initiator] で、[Discovery] タブをクリックします。



2. iSNS サーバを追加します。
 タブの [iSNS Servers] セクションで [Add] ボタンをクリックすると、[Add iSNS Server] ダイアログが表示されます。



iSNS サーバの IP アドレスか DNS 名を入力して、[OK] をクリックします。



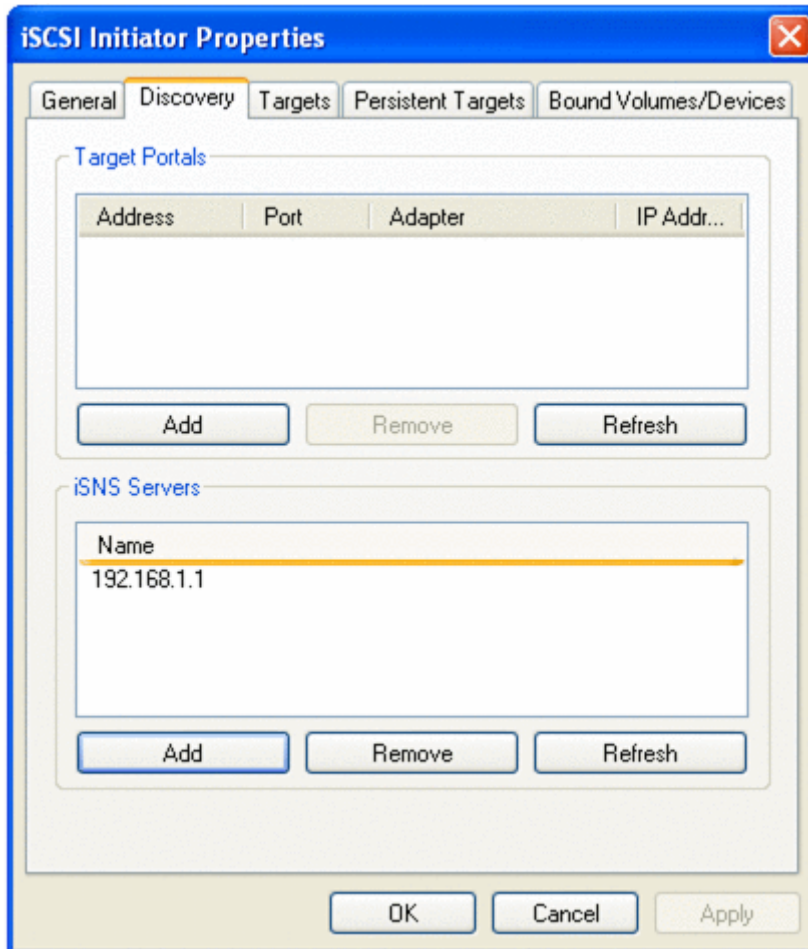
重要 iSNS サーバを追加すると、iSNS に登録されている全ての使用可能な iSCSI ターゲットが、使用可能なターゲットとして表示されます。

3. 変更内容を保存します。
 設定内容を確認した後、保存するには [OK]、保存せずに終了するには [Cancel] をクリックします。

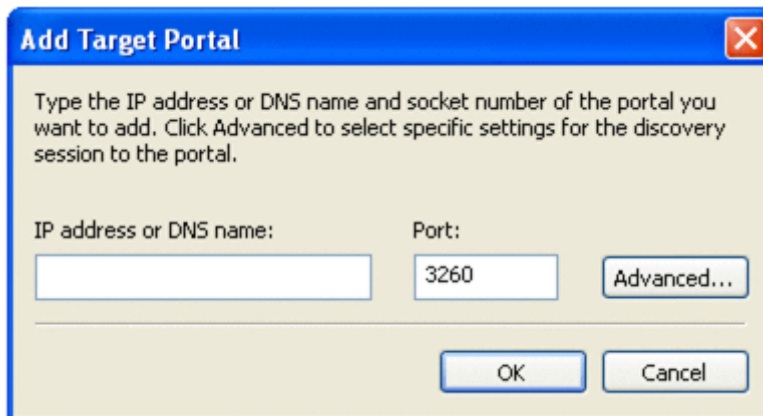
(2) ターゲットポータルを使用して iSCSI ターゲットを検出する

ネットワーク上に iSNS サーバが存在しない場合は、ターゲットポータルを使用して iSCSI ターゲットを検出できます。ターゲットポータルのリストに HNAS の EVS IP を追加して、その HNAS か EVS に関連付けられたターゲットを検出します。

1. [Target Portals] タブを開きます。
[Microsoft iSCSI Initiator] で, [Discovery] タブをクリックします。



2. ターゲットポータルを追加します。
タブの [Target Portals] セクションで [Add] ボタンをクリックすると, [Add Target Portal] ダイアログが表示されます。



HNAS のファイルサービス IP アドレスを入力します。

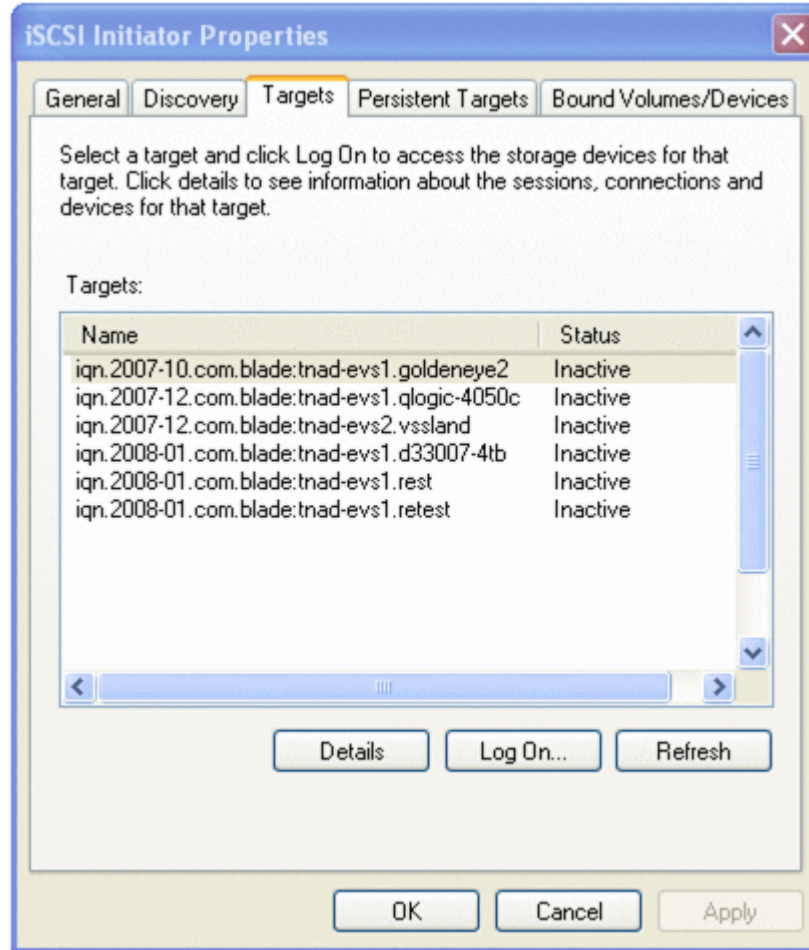
3. 変更内容を保存します。
設定内容を確認した後, 保存するには [OK], 保存せずに終了するには [Cancel] をクリックします。

(3) 使用可能な iSCSI ターゲットにアクセスする

使用可能な iSCSI ターゲットにアクセスするには

1. [Targets] タブを開きます。

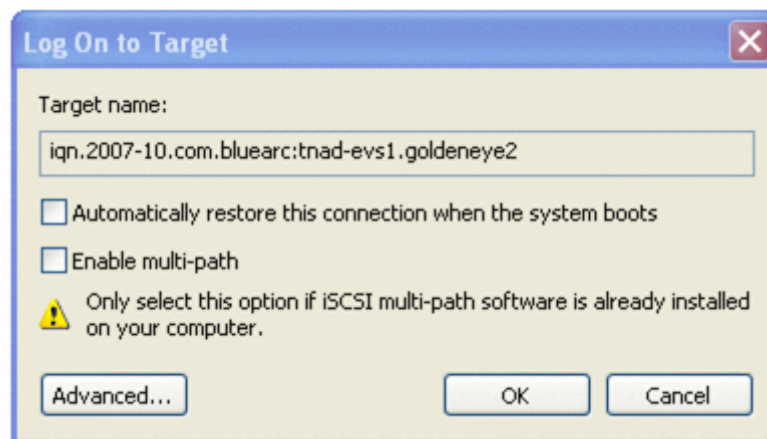
[Microsoft iSCSI Initiator] で、[Targets] タブをクリックします。



2. いずれかの使用可能なターゲットにログオンします。

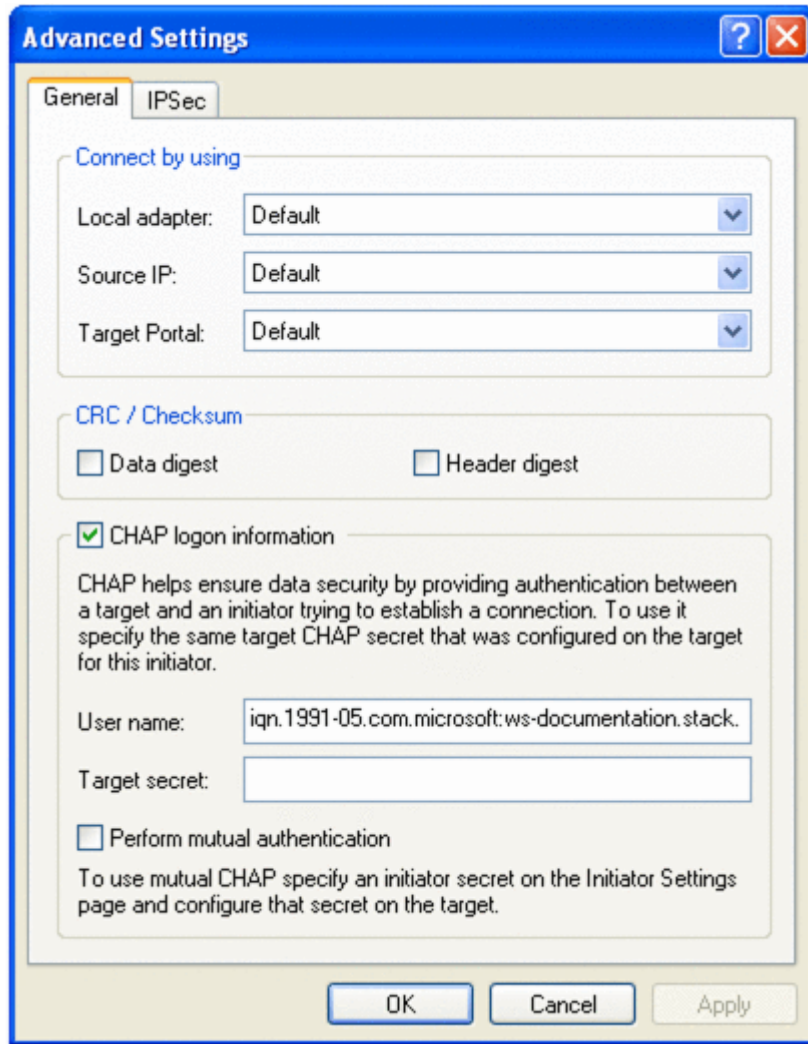
ログオンするごとに、次の iSCSI セッションが開始します。

- ターゲットを選択し、[Log On] ボタンをクリックすると、[Log On to Target] ダイアログが表示されます。



重要 実行可能な iSCSI セッションはターゲットごとに最大 32 件です。

- ターゲットで認証が有効になっている場合は、[Advanced] をクリックすると、[Advanced Settings] ダイアログの [General] タブが開きます。

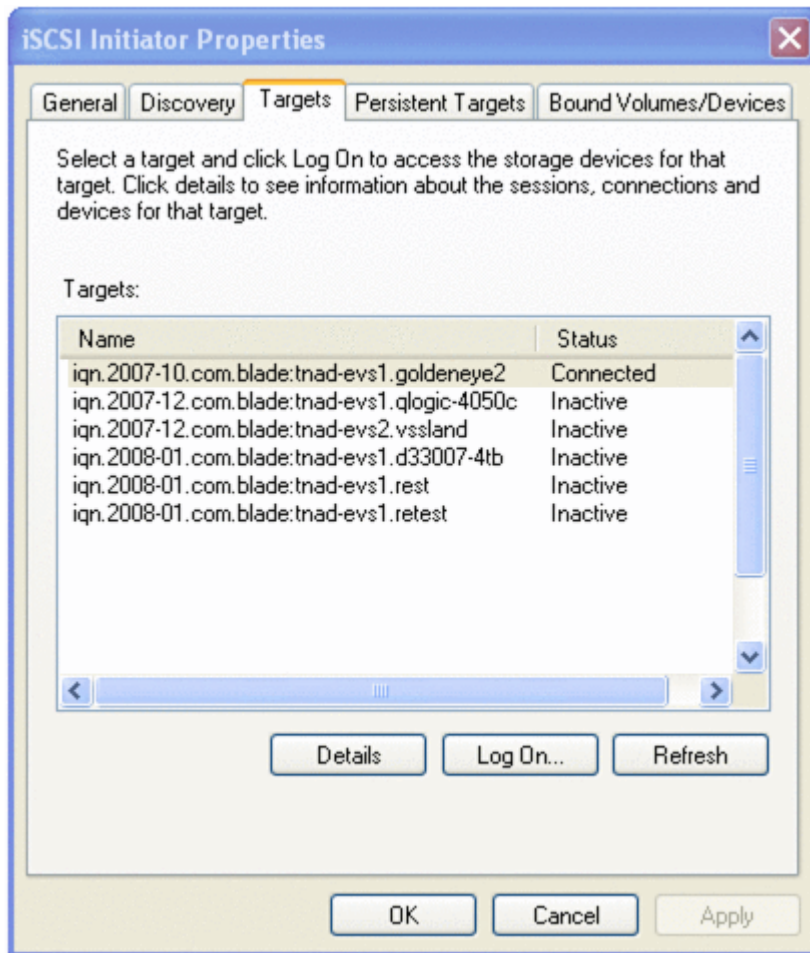


[CHAP logon information] チェックボックスをオンにして、ターゲットの秘密鍵 (iSCSI ターゲットの作成時に設定したパスワード) を入力します。また、相互認証が設定されている場合は [Perform mutual authentication] チェックボックスをオンにして、[OK] をクリックします。

- 必要に応じて、マルチパスを設定します。
マルチパスが Microsoft iSCSI イニシエーターでサポートされていて、ターゲットに対してマルチパスを使用する場合は、[Enable Multi-Path] チェックボックスをオンにします。
ターゲットへのマルチパスを作成するには、そのターゲットに対して別のセッションを後から開始する必要があります。詳しくは「7.1.1 (1) iSCSI MPIO」を参照してください。
- 接続を確立します。
[Log On] ダイアログで、[OK] をクリックして保存するか、[Cancel] をクリックして設定を破棄します。

(4) 実行中の接続を検証する

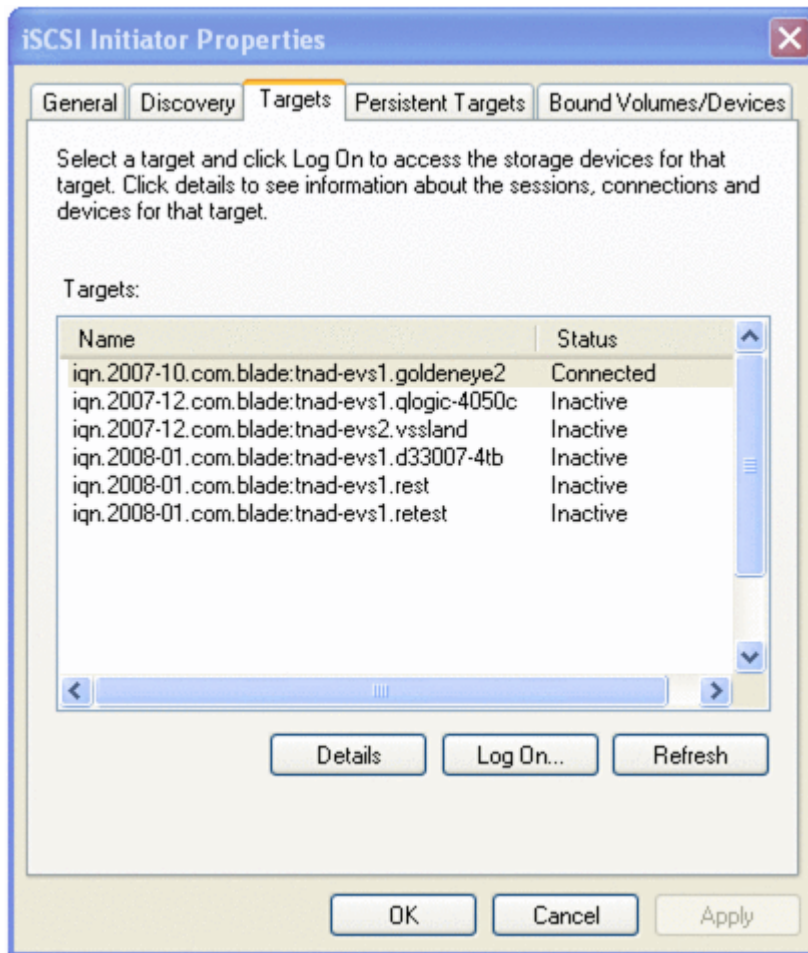
接続が確立されたら、[Targets] タブをクリックして、新しく確立された接続に関する詳細情報を確認します。



ターゲットの [Status] 列に [Connected] と表示されている必要があります。

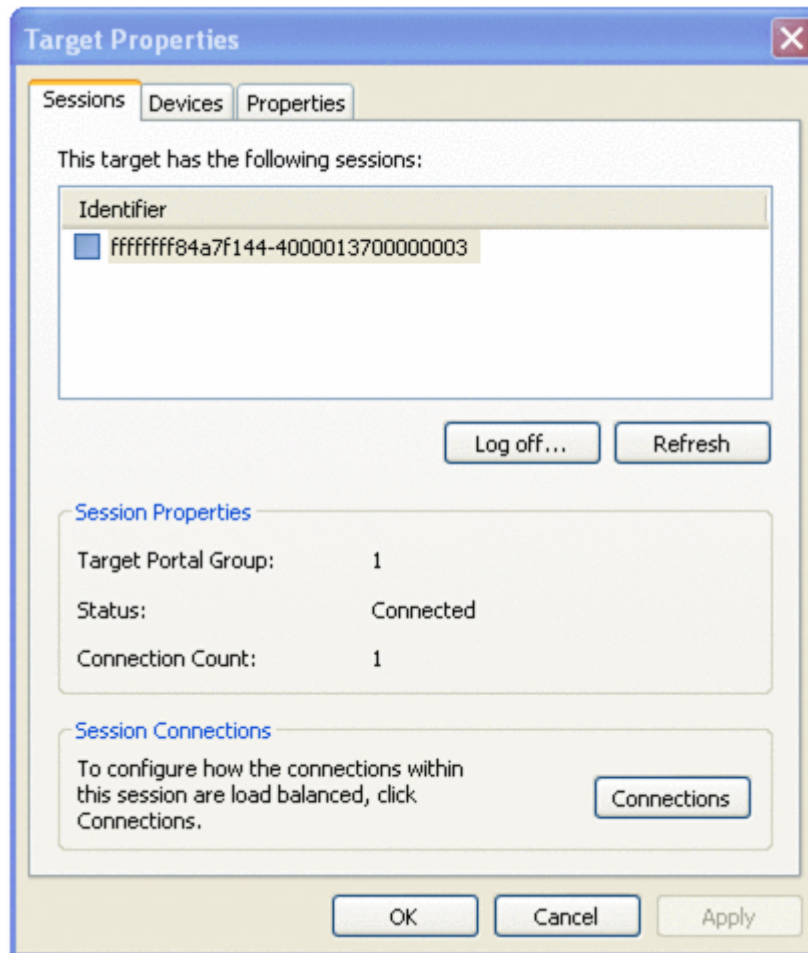
(5) 実行中の接続を終了する

接続がいったん確立すると、[Targets] タブにその接続の状態が表示されます。



接続を終了するには

1. 終了する接続を選択します。
2. [Target Properties] ダイアログを表示します。
[Details] ボタンをクリックすると、[Target Properties] ダイアログが表示されます。



3. 終了する接続を選択します。
セッション識別名のリストで、終了するセッションの識別名を選択します。
4. 接続を終了します。
[Log off...] ボタンをクリックしてセッションを終了します。デバイスを使用しているアプリケーションが存在しなければ、イニシエーターが iSCSI セッションを閉じようとしています。

(6) Computer Manager を使用して iSCSI ストレージを設定する

iSCSI の「ローカルディスク」は、Windows Disk Management ツールを使用して設定する必要があります。Microsoft では、次のことを推奨しています。

- LU の容量が 2TB 以下の場合、ベーシックディスクとして設定してください。
- LU の容量が 2TB を超える場合は、GPT ディスクとして設定してください。

いったんディスクを設定したら、Windows Disk Management ツールを使用してディスク上にパーティションを作成したりフォーマットしたりします。Windows Disk Management ツールの使用方法について詳しくは、お使いの Windows コンピューターのオペレーティングシステムのオンラインヘルプを参照してください。

