共有 Web ホスティングシステムの改善

針木剛 (京都大学情報部)
hariki@media.kyoto-u.ac.jp

1 はじめに

現在京都大学では汎用コンピュータシステムにおいて，公開 Web サイトなどの情報サービスを構築したいという学内の部局や研究室向けにホスティングサービスを提供している．

具体的にはコンテンツのファイルを置くだけで Web サイト運用可能な共有 Web ホスティングのサービスと OS の管理者権限を使い自由にシステムを構築できる VPS(Virtual Private Server) のサービスの 2 種類を提供しており，利用者は自身の利用ニーズに合わせて選択し利用することができる．

本発表では前者の共有 Web ホスティングサービスを提供するシステムの性能向上とセキュリティの強化のために具体的に行った作業について報告する．

2 サービス内容

共有 Web ホスティングサービスは複数の利用者でシステムを共有し利用してもらうサービスである．Web サービスを提供するためのサーバ OS は Linux でディストリビューションは RedHatEenterpriseLinux(以下 RHEL とする) を用いている．RHEL5 系と RHEL6 系の 2 つのサーバ環境を提供しており表 1 に各種ソフトウェアのバージョン一覧を示す．

表 1: Web サーバのソフトウェアとバージョン

	RHEL5	RHEL6
Apache-HTTPD	2.2.3	2.2.15
PHP	5.1.6	5.3.3
Perl	5.8.8	5.10.1
Ruby	1.8.5	1.8.7
Python	2.4.3	2.6.6

利用者は全学認証 ID を使い，FTPS で準備したコンテンツファイルをホームディレクトリの Web 公開領域へアップロード [1] する．HTML や CSS などの静的コンテンツに加え CGI や SSI による表 1 にあるプログラミング言語を使った動的コンテンツもサポートする．その中で PHP に関しては Apache-HTTPD のモジュール機能を用いて CGI などに比べ高速な動作環境で提供している．

Web アクセスログはホームディレクトリ領域に保存され利用者のみ閲覧可能な ACL(Access Control List) が設定されおり統計やエラーの確認などが可能である．

また Web サービス以外に MySQL と PostgreSQL が動作するデータベースサービスやメール転送サービス，動画配信サービスも提供している．

3 システム構成

3.1 変更前のシステム構成

改善変更前のシステムの構成を図 1 に示す．

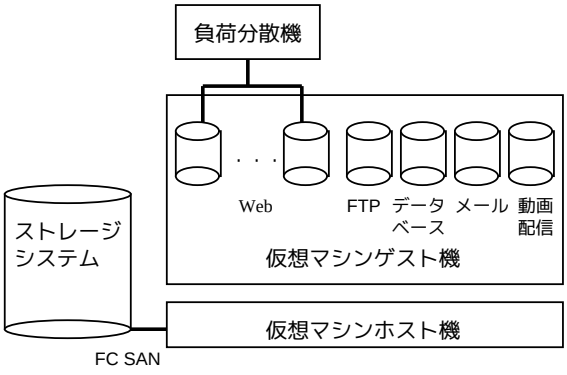

図 1: 変更前のシステムの構成

ストレージシステムはベンダ提供のアプライアンス機を利用しており，ファイバチャネルの SAN として仮想マシンホスト機に接続している．

当該ホスト機上で Web サーバ，FTP サーバ，データベースサーバ，メール転送サーバ，動画配信サーバをすべて仮想マシンゲスト機として構築している．

Web サーバは複数台で運用し Web アクセスは負荷分散アプライアンス機により分散し，ま

た分散先の Web サーバを随時監視してダウンしたサーバを外すことでシステムの可用性を高めている.

次にホームディレクトリ領域の共有に関する構成を図 2 に示す.

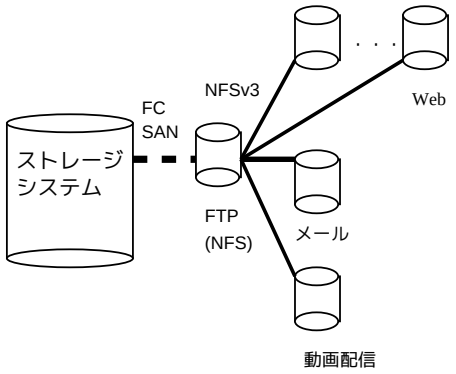

図 2: 変更前のホーム共有構成

FTP サーバが NFS サーバとなり利用者のホームディレクトリを他の全てのサーバがマウントして共有している.

3.2 変更後の新システムの構成

変更した新システムの構成を図 3 に示す.

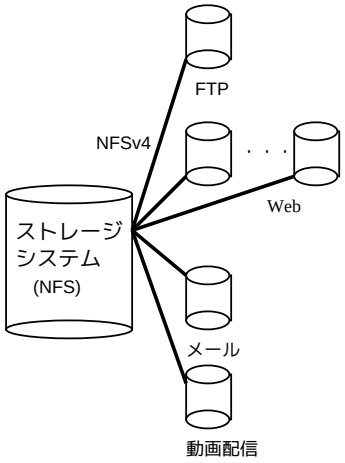

図 3: 新システム構成

ストレージシステムを NFS サーバとしても機能させて各サーバがホームディレクトリ領域をマウントして共有できるようにした.

これにより Linux の NFS サーバを経由せず直接アクセスすることが可能となり接続時のオーバヘッド削減による性能向上が期待できる. また単一障害点の一つである Linux の NFS サーバを排除することができ信頼性の向上が実現できる.

4 システム移行作業

4.1 ファイルシステム移行の制約と問題点

新システム構成のようにストレージシステムを NFS サーバで利用する場合, ベンダに確認したところ下記の制約が存在した.

1. ストレージシステムが POSIX の ACL をサポートしていないため, 対応している NFSv4 の ACL を使わなければいけない. NFSv4 クライアントは RHEL であればバージョン 6.4 以降が必要で, それ以前にはファイル操作のバグが存在する.
2. ファイル名やディレクトリ名は ASCII または UTF-8 でなければならない.

1 に関して, RHEL5 系の環境で動作しているホストを RHEL6 系に移行する際には表 1 にあるようなバージョン変更に伴う動的コンテンツの動作確認が必要になる.

移行作業前の 2013 年 9 月時点で全体の約 400 件のうち約 300 件のホストが RHEL5 系のサーバで動作しており, 全件を漏れなく確認するためにはブラウザの手動操作と目視ではなくクローラなどによる自動テストが必要になる.

また 2 に関して移行前は FTP サーバでのアップロード時の文字コード制限がなかったため, クライアント固有の文字コードのまま保存されており, マルチバイトのファイル名では Windows クライアントからのアップロードと思われる CP932 のものが多く確認された.

これらのファイル名の文字コードを適宜変換する作業が必要でありそれは実質ファイル名を強制的に変えることになるため, こちらもクローラなどによる Web 閲覧時のリンク切れ動作確認が必要になる.

4.2 ファイルシステム移行作業

4.1 の問題点を考慮して下記のような作業を計画した.

1. FTP サーバでアップロード時の文字コードを UTF-8 に強制指定する設定を追加する.
2. ストレージシステムに新たな利用者ホームディレクトリ領域を作成して FTP サーバがこれを NFSv4 でマウントする.

3. FTP サーバ上で旧領域から新領域への複製を毎晩バッチ処理で行う．このときにファイル名がマルチバイトであった場合は文字コードを UTF-8 に変換して保存する．複製終了後に NFSv4 の ACL も設定する．

4. 図 4 にあるように新規で RHEL6.4 の Web ホスティングサーバを構築して新ホームディレクトリ領域を NFSv4 でマウントし，従来の RHEL6.4 で旧ホームディレクトリをマウントしたサーバと平行運用とする．この後 1 ホストずつクローラで確認し，問題なければ負荷分散機の振り先変更で移行する．

5. 最後に RHEL5 の Web ホスティングサーバから同様にクローラで確認しながら新 RHEL6.4 へ移行する．
こちらはバージョンアップによる影響は大きいと考え，クローラの動作確認に加え動的コンテンツ利用者に対し個別に動作確認の協力を依頼した．

2013 年 10 月現在 5 の作業中であり 2 つのホームディレクトリ領域を平行運用しているが，残りの未移行ホスト約 140 件の移行が済み次第 RHEL5 の Web ホスティングサーバを停止し旧ホームディレクトリ領域を削除する方針で適宜作業をすすめている．

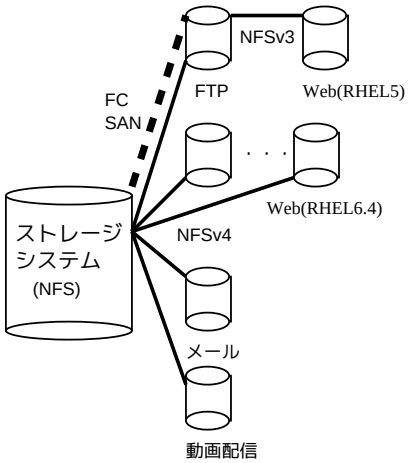

図 4: 移行中のシステム構成

4.3 動作確認テストクローラの問題点

移行作業時に必要となるクローラは Web ホスティングサーバのネットワーク外からトップのコンテンツからリンク先をたどりファイルに保存し，新旧両者から取得したコンテンツの差分で確認する仕組みとした．概ねうまく動作したが下記の問題点があった．

- アクセス制限コンテンツが確認不可
- リンクされていないコンテンツが確認不可
- 更新タイミングでの差分検出
- アクセスする度に違うトークンが埋め込まれたコンテンツの差分検出

アクセス制限は仕方がないが他の項目は改善の余地があると考えられる．今後もシステム移行の際に利用できるツールであるので問題点を改善してテストの精度を高めたい．

5 ファイルシステム性能測定結果

5.1 測定方法

変更前の構成と新しい構成でファイルシステムの性能比較を行った．
表 2 に NFS サーバの違いを示す．

表 2: NFS サーバの違い

	旧構成	新構成
OS	Linux-2.6.32	ONTAP[2]
ファイルシステム	ext3	WAFL[3]

NFS クライアントは実際に利用している Web ホスティングサーバを利用した．

5.2 測定結果

測定は下記の方法で行った．

- RHEL6.4 にバンドルされた dd コマンド (バージョン 8.4) を用いた．
- 読み込みは当該ディレクトリに存在するファイルを/dev/null に出力した時間を測定した．その際に Linux のメモリキャッシュを測定しないよう測定前には再マウントを行った．
- 書み込みは/dev/zero を当該ディレクトリに書き込んだ時間を測定した．
- dd コマンドのブロックサイズは NFS オプションの rsize と wsize に合わせた．

- ファイルサイズは写真などを想定した10MBとして測定した.

3回測定を行った平均値の結果を表3に示す.

表 3: ファイルシステム性能の比較

[MB/sec]

	旧構成	新構成
読み込み	91.9	101.2
書き込み	57.7	77.9

読み込みに関しては約1.1倍，書き込みに関しては約1.3倍新構成が優れた結果となった.

6 セキュリティ関連の変更

6.1 変更前の設定と問題点

共有Webホスティングサービスにおいてサービス利用者が作成したコンテンツが他のサービス利用者から閲覧や編集できないよう分離することは，運用していく上で非常に重要な要素である．まず変更前の運用方法を下記に述べる.

- SSHやTelnetでのログインは不可であり，FTPSでは自身のホームディレクトリが最上位となっているため他者のホームディレクトリにはアクセスできない.
- CGIやSSIはApache-HTTPDのsuEXEC機能を使い，当該ファイルオーナの権限で実行される．他者に閲覧されたくないファイルなどはPOSIXの権限の許可を適切に設定する必要がある.
- PHPはApache-HTTPDのmod_phpで動作するため「apache」という共通のUIDで実行される．ただし各々のVirtualHostディレクティブ内でopen_basedirを自身の公開領域と/tmpのみに設定することで，スクリプト内で他者のホームディレクトリへのアクセスを禁止している.

問題点としてPHPや静的コンテンツファイルには「apache」という共通UIDからの閲覧権限が必要だが，そのためには全UIDからの閲覧権限を設定する必要があった．データベース接続パスワードなどが記載された閲覧制限すべきファイルに関しては，利用者自身と「apache」のみ閲覧可能となるディレクトリも別途準備したが，アナウンス不足により利用されてこなかった.

6.2 新構成移行時の対策

4.2で行った移行作業時に全ての利用者のホームディレクトリに表4のNFSv4のACLを追加設定した.

表 4: 各ディレクトリに追加したACL

UID	利用者	apache	他者
ホーム	閲覧編集	閲覧	不可
公開	閲覧編集	閲覧	不可
公開以下デフォルト	閲覧編集	閲覧編集	不可

コンテンツ上位のディレクトリを制限することで，コンテンツ自身も他者からの閲覧や編集を禁止する設定となった．また公開領域のデフォルトACLにより，公開領域以下にアップロードしたファイルには自動で利用者自身と「apache」のみ閲覧編集可能なACLが付与される設定となった.

7 まとめ

共有Webホスティングサービスを行うシステムにおいて下記の改善を行った.

- NFSサーバの変更や構成変更によりファイル読み込み性能向上を図ることができた
- 構成変更により単一障害点であるLinuxサーバを排除することができた
- ACL設定追加でよりセキュアな環境での提供が可能になった

参考文献

[1] 平成22年度熊本大学総合技術研究会「統合認証基盤を用いたWebホスティングサービスの認証システム構築」○針木剛，赤坂浩一，古村隆明，永井靖浩

[2] ONTAP(OS), ウィキペディア, http://ja.wikipedia.org/wiki/ONTAP_%28OS%29

[3] WAFLによるディスクアクセスの高速化, 富士通, http://storage-system.fujitsu.com/jp/products/nwdiskarray/feature/hard040/