VMwareイメージを利用した構築

VMwareイメージを利用した構築

NIIが提供する“OSからshibboleth(IdP)までインストールされた”システムを利用する方式です。貴学では、貴学のサーバにVMware Serverをインストールし、その上にこのシステムイメージを稼動することで利用できます。

本ページでの記述およびVMイメージは古いものです。Shibboleth IdPの最新版は3.1.1であり、VMwareのソフトウェアも現在はサポートが切れております。Shibboleth IdPをインストールする方法での構築をご検討ください。

1. 前提条件
2. VMwareServerをインストールする
3. VMイメージをダウンロードする
4. VMwareServerにVMイメージを登録し、起動する
5. ゲストOSにログインする
6. IPアドレス、ホスト名を変更する
7. 時刻同期を設定、確認する
8. セキュリティを設定、確認する
9. サーバをリブートする

---

1. 前提条件

（１）NIIで動作検証した環境

・ホストOS：CentOS 5.3
・VMwareServer：VMware-server-2.0.1-156745.i386.rpm

※64bit版OSの場合は、VMwareServer: VMware-server-2.0.1-156745.x86_64.rpmをご使用ください。

（２）配布するVMイメージの初期情報

■VMwareServerでの設定

・ゲストOS：「LINUX」ー「Other Linux 2.6.x kernel」

・ネットワーク接続：ブリッジ

・ディスクサイズ：４GB

・メモリサイズ：２５６MB

■(ゲスト)OSでの設定

・(ゲスト)OS：CentOS 5.3（Apache HTTP Server 2.2.3-22）

・rootパスワード：passwd

・ホスト名：upki-test-idpvm.nii.ac.jp

・ｉｐアドレス：192.168.0.1

・インストールソフトウェア：

開発	開発ツール (オプションパッケージは全て無し)
	開発ライブラリ(オプションパッケージは全て無し)
サーバ	Webサーバー (オプションパッケージはHTTPのみ)
	ネットワークサーバー(オプションパッケージは LDAP Serverのみ)
ベースシステム	ベースのみチェック(オプションはデフォルト)
X Window	なし

・追加インストール

SUN JDK 1.6、Apache Tomcat 6.0、openldap-2.3.43-3

・Firewall Configuration：

Security Level	Disabled
SELinux	Disabled

・認証設定：デフォルト(MD5,Shaddow)

・サービス設定： ip6tables, iptables 停止。その他はデフォルト。

■LDAPの初期設定

・suffix： o=Test Organization, dc=ac, c=JP

・rootdn： cn=olmgr, o=Test Organization, dc=ac, c=JP

・rootpw： csildap

・初期構成

属性	ユーザ１	ユーザ２	ユーザ３
uid	test001	test002	test003
userPasswd	test001	test002	test003
mail	test001_email@nii.ac.jp	test002_email@nii.ac.jp	test003_email@nii.ac.jp
sn	test001_sn	test002_sn	test003_sn
sn;lang-ja	テスト001_sn	テスト002_sn	テスト003_sn
o	Test Organization	Test Organization	Test Organization
ou	Test Unit1	Test Unit2	Test Unit3
ou;lang-ja	テスト001_学部1	テスト002_学部2	テスト003_学部3
givenName	test001_givenname	test002_givenname	test003_givenname
givenName;lang-ja	テスト001_givenname	テスト002_givenname	テスト003_givenname
displayName	test001_displayname	test002_displayname	test003_displayname
displayName;lang-ja	テスト001_displayname	テスト002_displayname	テスト003_displayname
eduPersonAffiliation	faculty	student	staff

■shibbolethインストールディレクトリ

/opt/shibboleth-idp

---

2. VMwareServerをインストールする

※ VMware Serverはすでに EOLを迎えておりますので、可能なら他の仮想化ソフトウェアをお使いください。

■ダウンロードURL

https://my.vmware.com/jp/web/vmware/info/slug/infrastructure_operations_management/vmware_server/2_0

■ダウンロードプロダクト

NIIでの動作検証環境では、以下のプロダクトをダウンロードし、インストールしました。

・VMware Server for Linux （VMware Server本体）

■インストール手順

http://www.vmware.com/jp/pdf/server_admin_manual.pdf

貴学の環境によっては、gcc、kernel-devel、kernel-headers、libXtstの追加インストールが必要となる場合があります。

インストールにはシリアルナンバーの入力を要します。
シリアルナンバーの取得は、以下のURLでアカウント登録をしてください。

http://register.vmware.com/content/registration.html

---

3. VMイメージをダウンロードする

■ダウンロードURL

本サイトの「技術ガイド」ー「IdP構築関連ファイル」からダウンロードしてください。

---

4. VMwareServerにVMイメージを登録し、起動する

①当該サーバのホストOS上の「/var/lib/vmware/Virtual Machines」配下でダウンロードしたVMイメージを格納し、解凍します。

```
# cd /var/lib/vmware/"Virtual Machines"
# ls
upkishibIdPv2.0.tar.gz
# tar -zxvf upkishibIdPv2.0.tar.gz
```

②upkishibIdPディレクトリが作成され、その配下には以下の５つのファイルが作成されたことを確認します。

```
# ls /var/lib/vmware/"Virtual Machines"
upkishibIdPv2.0.tar.gz   upkishibIdPv2.0
# ls /var/lib/vmware/"Virtual Machines"/upkishibIdPv2.0
upkishibIdP.vmx  upkishibIdP.vmdk  upkishibIdP.flat.vmdk   upkishibIdP.vmsd  nvram
```

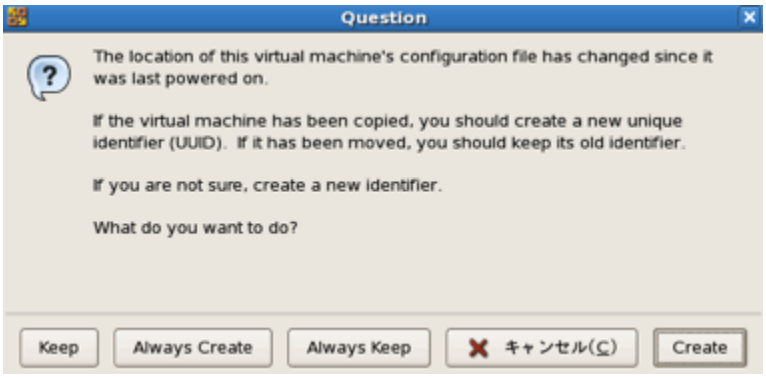
③upkishibIdP.vmxの権限を変更します。

```
# chmod 754 /var/lib/vmware/"Virtual Machines"/upkishibIdPv2.0/upkishibIdP.vmx
```

④ホストOSのX Windowから「VMwareServer Console」を起動し、menuバーより
「File」ー「Open」を選択し
「/var/lib/vmware/" Virtual Machines" /upkishibIdPv1.0/upkishibIdP.vmx」を指定します。

⑤「Power on this Virtual machine」をクリックします。

⑥次のようなダイアログが表示されるので、「Create」を選択します。



※仮想マシンを移動またはコピーした後に初めて仮想マシンをパワーオンすると、新しいUUID を生成するか聞いています。「Create」を選択することにより、MACアドレスが新たに生成されます。

⑦IdPがインストールされたゲストOS（CentOS5.3）が起動します。

---

5. ゲストOSにログインする

■rootの初期パスワードはpasswdです。

■ログイン後、パスワードを変更してください。

```
# passwd
```

---

6. IPアドレス、ホスト名を変更する

■配布時は以下のように初期設定されていますので、貴学の環境に基づき変更してください。

・IPアドレス：192.168.0.1

・ホスト名：upki-test-idpvm.nii.ac.jp

■変更箇所は以下の通りです。

①/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
ONBOOT=yes
IPADDR=192.168.0.1  ←ipアドレス
NETMASK=255.255.255.0  ←サブネットマスク
GATEWAY=192.168.0.254  ←ゲートウェイ
NETWORK=192.168.0.0  ←ネットワークアドレス
（中略）
```

②/etc/sysconfig/network

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=upki-test-idpvm.nii.ac.jp  ←ホスト名
```

③/etc/resolv.conf

```
search nii.ac.jp  ←ローカルドメイン名
nameserver 192.168.0.2  ←ネームサーバ
```

④/etc/httpd/conf/httpd.conf

```
 (中略)
ServerName upki-test-idpvm.nii.ac.jp:80  ←ホスト名
 (中略)
```

⑤/etc/httpd/conf.d/ssl.conf

```
 (中略)
ServerName upki-test-idpvm.nii.ac.jp:443  ←ホスト名
 (中略)
<VirtualHost _default_:443>
 (中略)
ProxyPass /idp/ ajp://localhost:8009/idp/    ←記述されているか確認
 (中略)
</VirtualHost>
```

⑥/opt/shibboleth-idp/metadata/idp-metadata.xml

```
 (中略)

   <EntityDescriptor entityID="https://upki-test-idpvm.nii.ac.jp/idp/shibboleth">  ←ホスト名  <IDPSSODescriptor
protocolSupportEnumeration="urn:mace:shibboleth:1.0 urn:oasis:names:tc:SAML:2.0:protocol"> <KeyDescriptor> <ds:KeyInfo>  (中略)

     <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="https://upki-test-idpvm.nii.ac.jp/idp
/profile/Shibboleth/SSO" /> ←ホスト名

      <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://upki-test-idpvm.nii.ac.jp/idp
/profile/SAML2/POST/SSO" /> ←ホスト名

      <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://upki-test-idpvm.nii.ac.jp/id
p/profile/SAML2/Redirect/SSO" /> ←ホスト名

  (中略)

     <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding" Location="https://upki-test-idpvm.nii.ac.jp:8443
/idp/profile/SAML1/SOAP/AttributeQuery"/> ←ホスト名

      <AttributeService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://upki-test-idpvm.nii.ac.jp:8443/idp
/profile/SAML2/SOAP/AttributeQuery"/> ←ホスト名
```

⑦/opt/shibboleth-idp/conf/relying-party.xml

```
 (中略)
   <AnonymousRelyingParty provider="https://upki-test-idpvm.nii.ac.jp/idp/shibboleth" />  ←ホスト名
   <DefaultRelyingParty provider="https://upki-test-idpvm.nii.ac.jp/idp/shibboleth"  ←ホスト名
                        defaultSigningCredentialRef="IdPCredential">
```

■新しいホスト名とIPアドレスをDNSに登録してください。

---

7. 時刻同期を設定、確認する

■ntpサービスを用い、貴学環境のntpサーバと時刻同期をしてください。
Shibbolethでは、通信するサーバ間の時刻のずれが約５分を越えるとエラーになります。

■VMwareServerのゲストOSでは、システムクロックが著しくずれますが、ハードウェアクロックのずれは少ないので、NIIでの検証では、以下の設定を施し安定稼動させています。

【設定例】

```
# crontab -l
*/3 * * * * /sbin/clock --hctosys  ←３分毎にclockコマンドでシステムクロックをハードウェアクロックに合わせる
*/3 * * * * /usr/sbin/ntpdate (ntpサーバ) > /dev/null && /sbin/clock --systohc > /dev/null  ←毎時10分にntpdate コマンドでntpサーバと同期し、ハードウェアクロックも合わせる
```

---

8. セキュリティを設定、確認する

貴学のセキュリティポリシーに準拠し、サーバのセキュリティの設定・確認をしてください。

---

9. サーバをリブートする

```
# reboot
```

お使いの環境によっては、極稀にサーバ起動時にtomcatサービスで”failed”が表示される場合があります。これは依存するサービスの起動に待ちが発生するためで、”failed”が表示されてもリトライされて正常起動するケースが多いです。

”failed”の場合でも以降の設定および接続テストを実施し、それでもエラーとなる場合はヘルプデスク（gakunin-help (at) nii.ac.jp）へ連絡してください。

設定および確認が完了したら，サイト情報等の設定および接続テストを行って下さい.