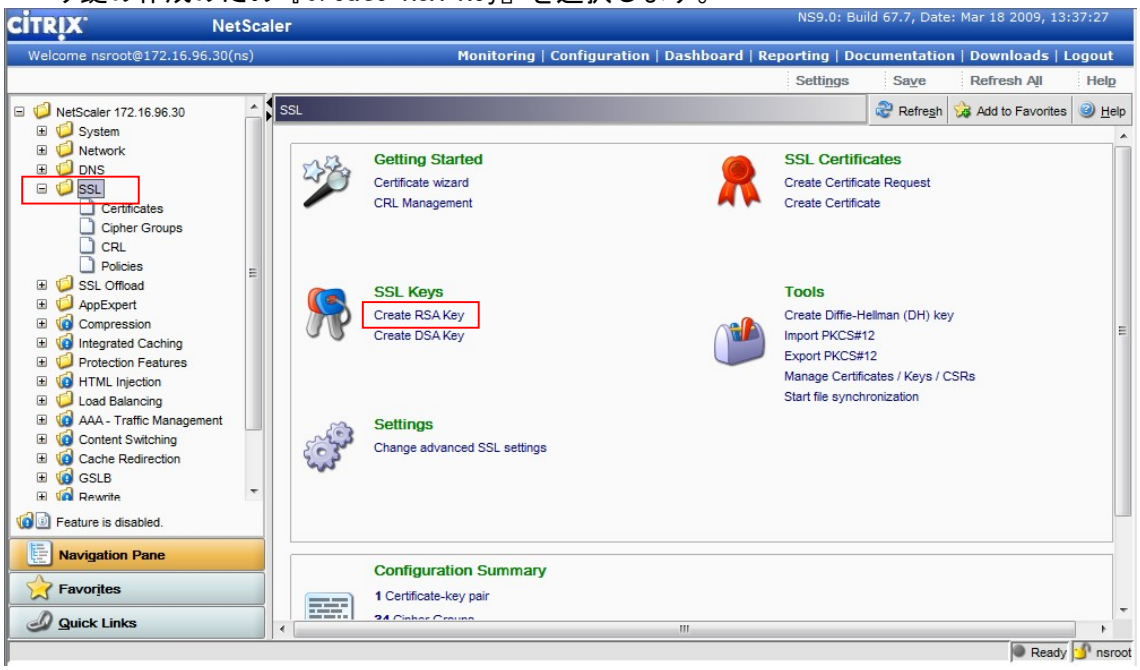
マクニカネットワークス株式会社
Citrix サポートチーム

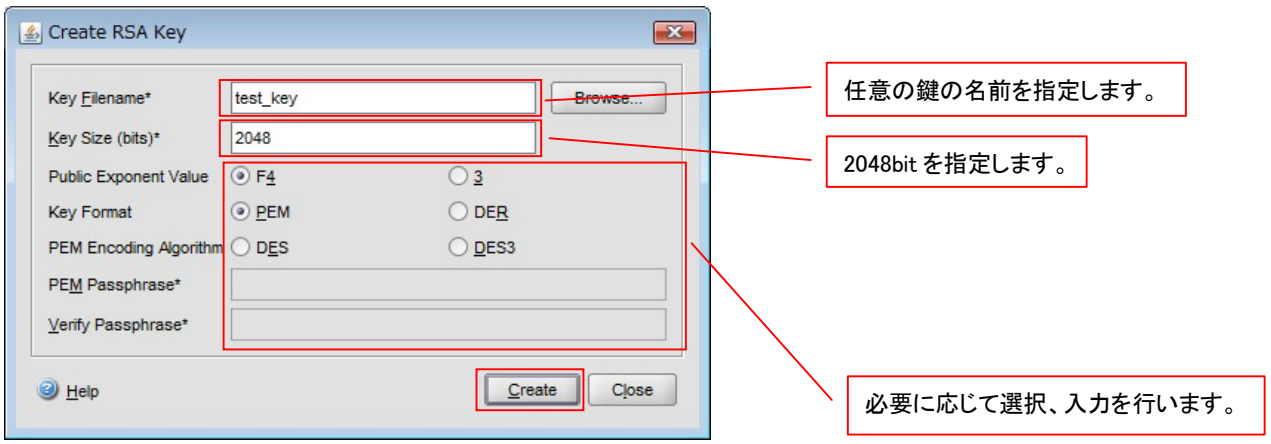
Citrix NetScaler サーバ証明書設定手順書

① 鍵ペア及び CSR の作成

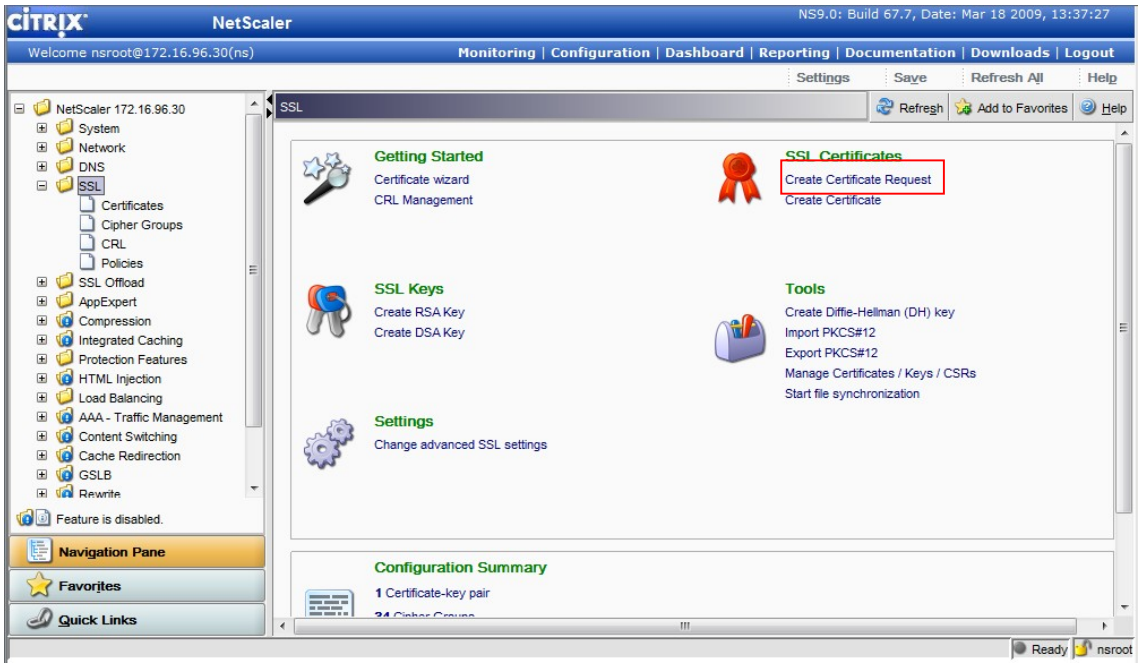
1. NetScaler に WebUI よりログインし、SSL を画面左より選択します。選択後、画面右より鍵の作成のため『Create RSA Key』を選択します。



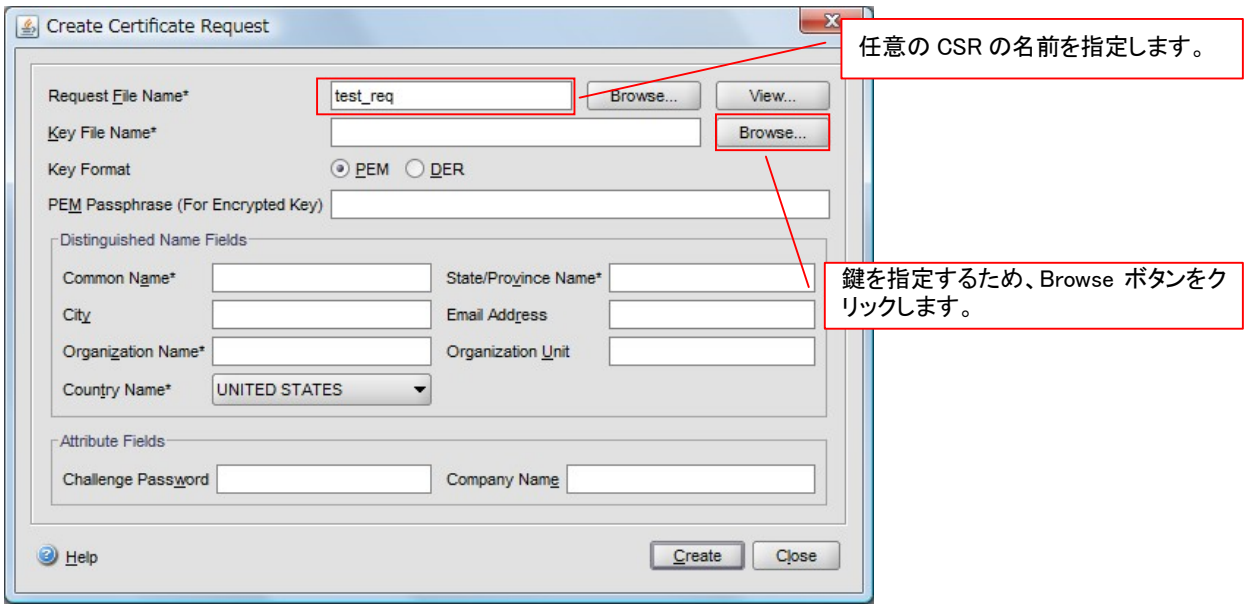
2. 鍵の作成画面にて鍵の名前やサイズを設定し、Create ボタンをクリックします。



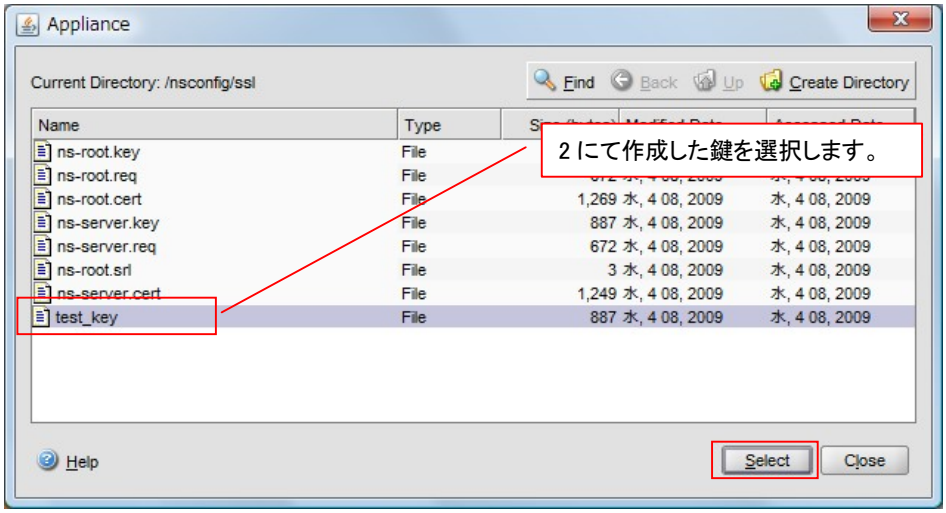
3. 再度画面左より SSL を選択します。(Ver8.0 及び 8.1 の場合は画面左より SSL→CA Tools を選択)
選択後、画面右より CSR 作成のため『Create Certificate Request』を選択します。



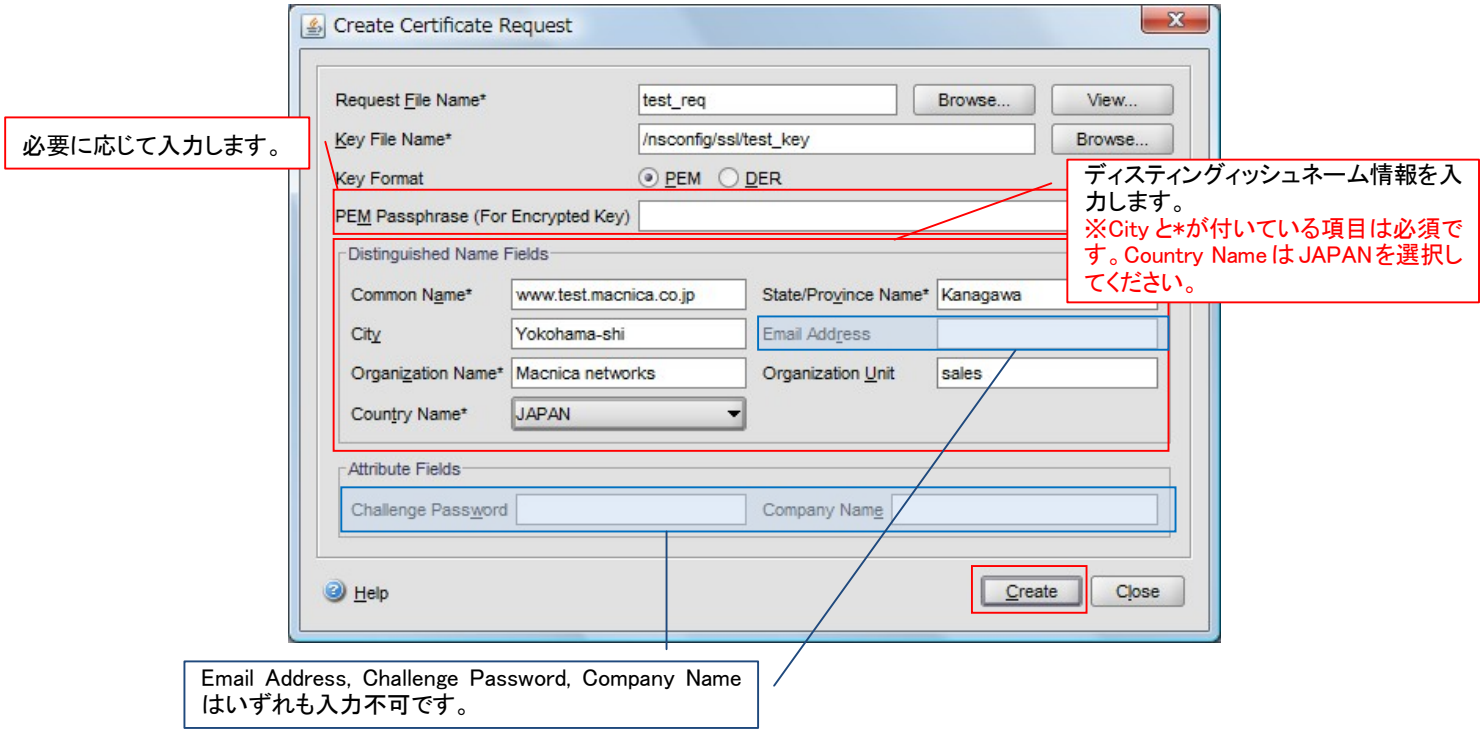
4. CSR の名前を入力し、Browse ボタンをクリックして鍵を指定します。



5. 鍵の選択画面にて 2 にて作成した鍵を選択し、Select ボタンをクリックします。

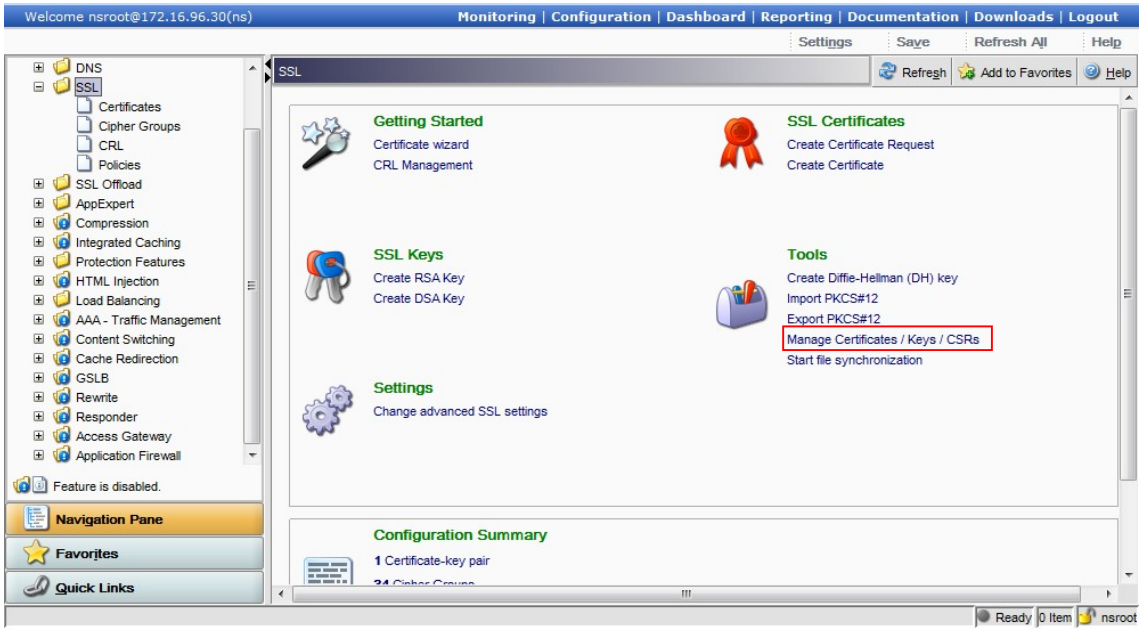


6. ディスティングィッシュネーム情報などを入力し、Create ボタンをクリックします。
*が付いている項目は、入力が必須です。

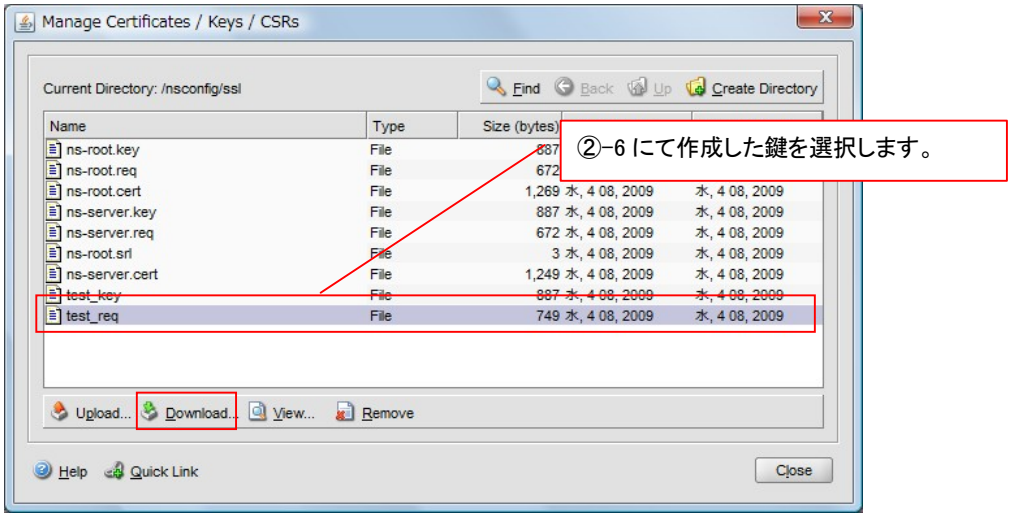


② CSR のエクスポート

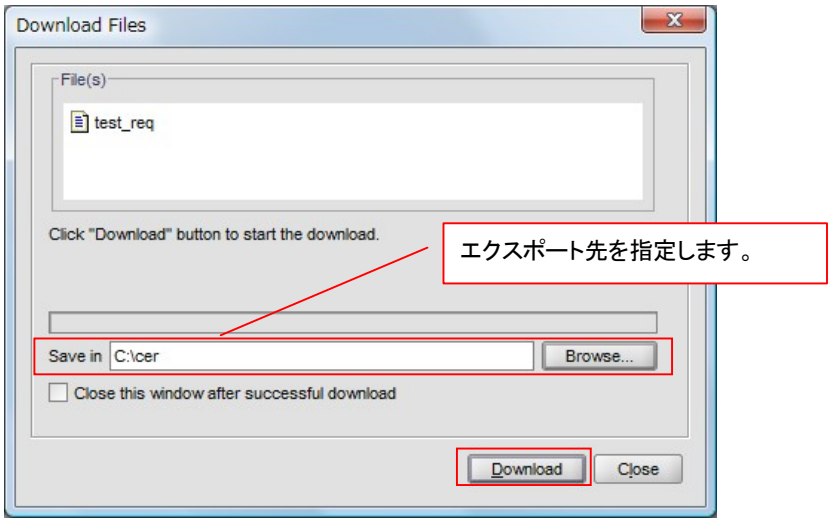
1. 画面左より SSL を選択します。
   選択後、CSR をエクスポートするため画面右より Manage Certificates/Keys/CSRs を選択します。



2. 選択画面にて①－6 にて作成した CSR を選択し、Download ボタンをクリックします。



3. CSR のエクスポート先の指定画面にて、管理端末のどこにエクスポートするのかを指定し、Download ボタンをクリックします。



4. エクスポートした CSR ファイルをテキスト等で開き中身を確認します。
下記のようなファイルであることを確認します。

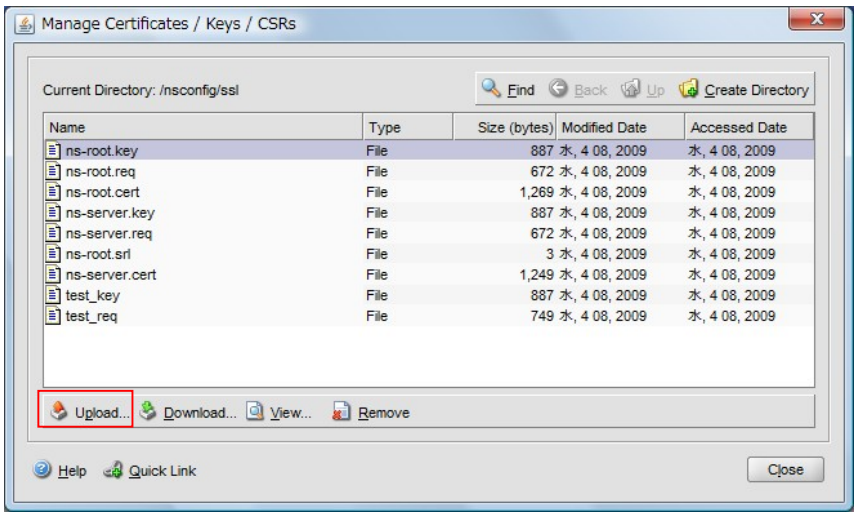
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB6zCCAVQCAQAwgaoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTEV
MBMGA1UEBxMMWW9rb2hhbWEtc2hpMRkwFwYDVQQKExBNYWNuaWNhIG5ldHdvcmtz
MQ4wDAYDVQQLEwVzYWxlczEfMB0GA1UEAxMWd3d3LnRlc3QubWFjbmljYS5jby5q
cDElMCMGCSqGSIb3DQEJARYWdGVzdGFkZHJlc0BtYWNuaWNhLm5ldDCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0L+9WU4wJMCxwkgjbs39NeOpH+tzy6gJrgfx
ITfp6CreMcaEYsFYVjptHZ7Axi4Jo4jGszcWt+hQxgXVb/V94XfMCLy2rlqPSc9B
JCcAseM3mooB+j4p8BR9p3cGkYWXXzYZRd+vv9gqJPTreaN9ow8vWdBSxKXaHoem
jiM82UcCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBABIfxtV8SkPOZAZObcryWZ48
3RQQiCgdNwKcfnBFvOcNgHugNAQIw7fgwRHsPCM3pYIZX1o6QF5wsAT4cFDzFivB
UBug6GOBA3rGPUnEH+eZUjzpG97vB3xEKez5uy21QTVtyU+5xqLnx4PDsMgArstC
gaHvgI5SYV5Dfat1ZK4o
-----END NEW CERTIFICATE REQUEST-----
[EOF]
```

5. エクスポートした CSR を証明書発行機関に送付し、証明書を作成してもらいます。

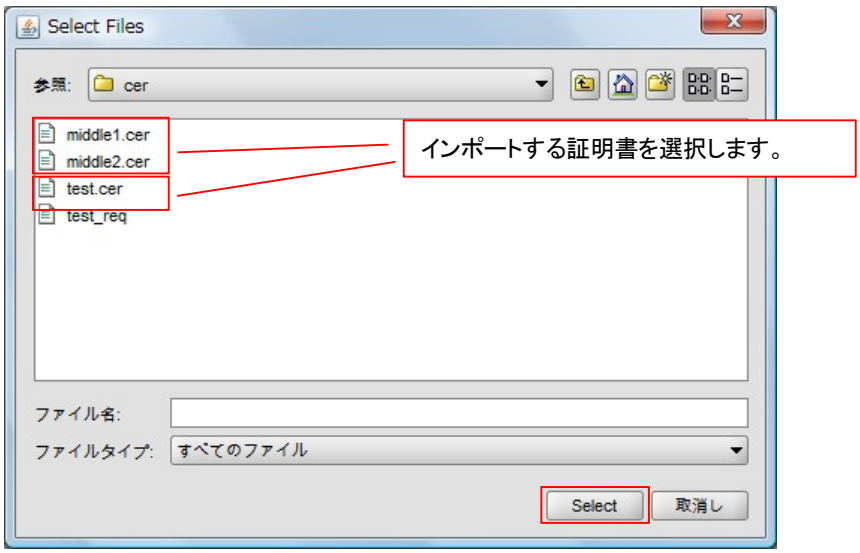
6. CSR をもとに、証明書発行機関より証明書が発行されます。

③ 証明書のインポート

1. 証明書を NetScaler に取り込むため WebUI よりログインし、SSL を画面左より選択します。選択後、画面右より Manage Certificates/Keys/CSRs を選択し、Upload ボタンをクリックします。

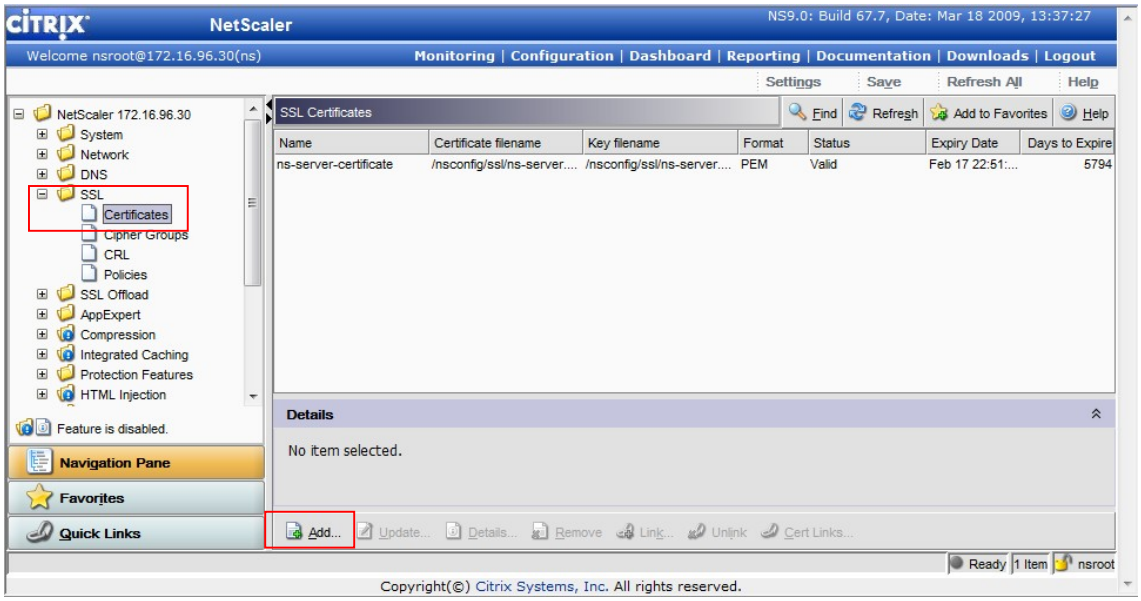


2. インポートするファイルを選択し、Slect ボタンをクリックします。
本例ではサーバ証明書 1 枚、中間証明書 2 枚をインポートしています。

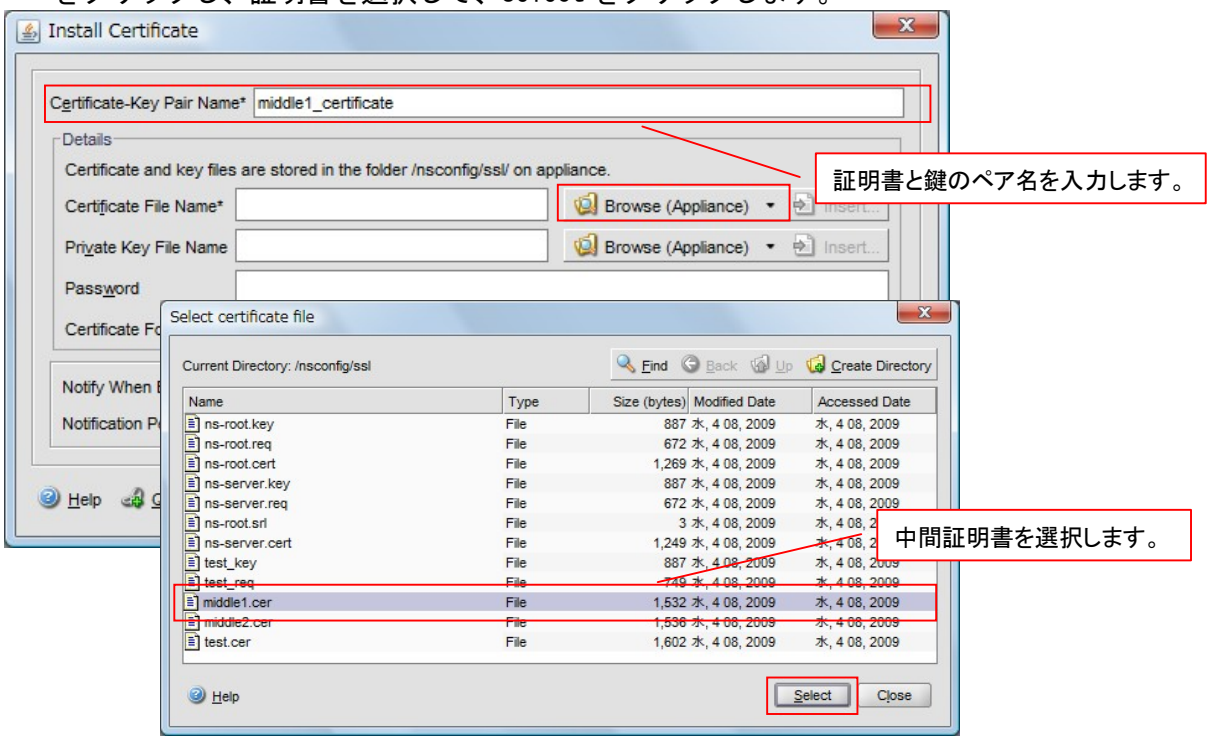


④　証明書の設定と、Vserver との紐付け

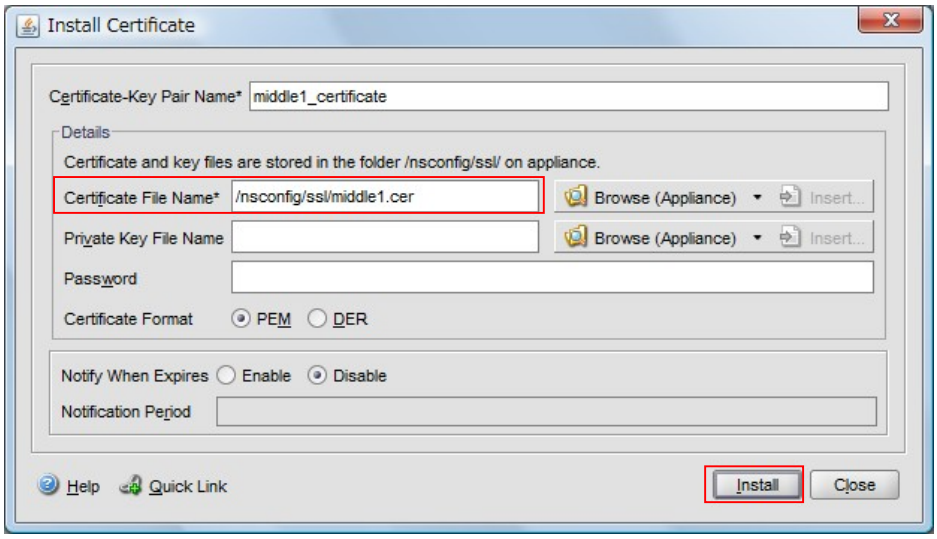
1. 画面左より SSL → Certificates を選択します。
   選択後、証明書を設定するため画面下の Add ボタンをクリックします。



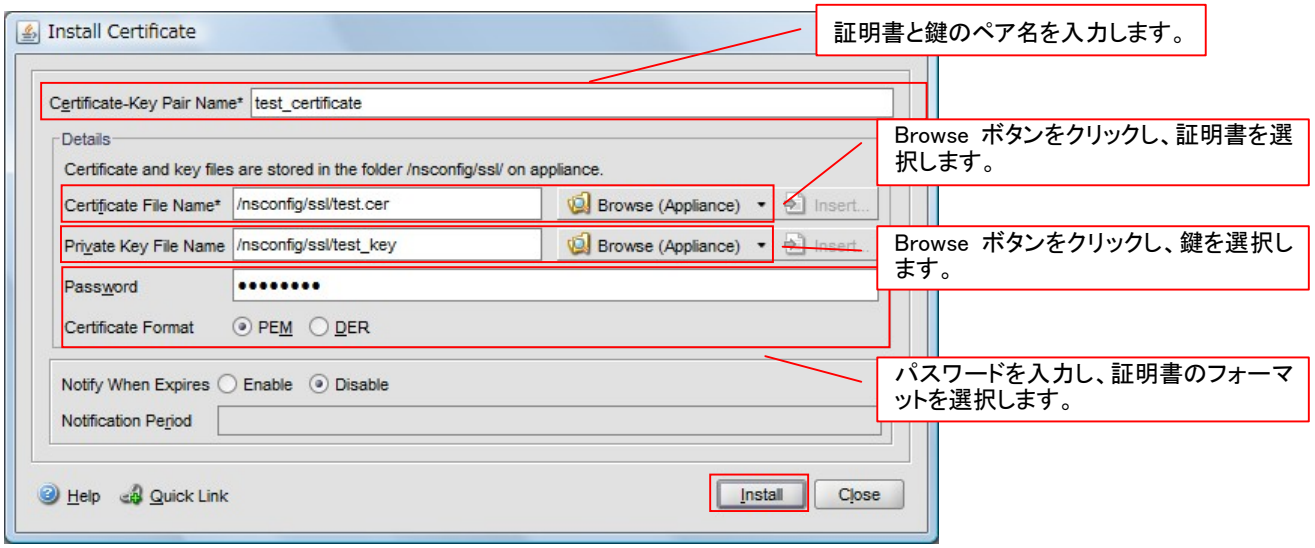
2. 中間証明書を設定するため、証明書と鍵のペア名を入力します。その後、Browse ボタンをクリックし、証明書を選択して、Select をクリックします。



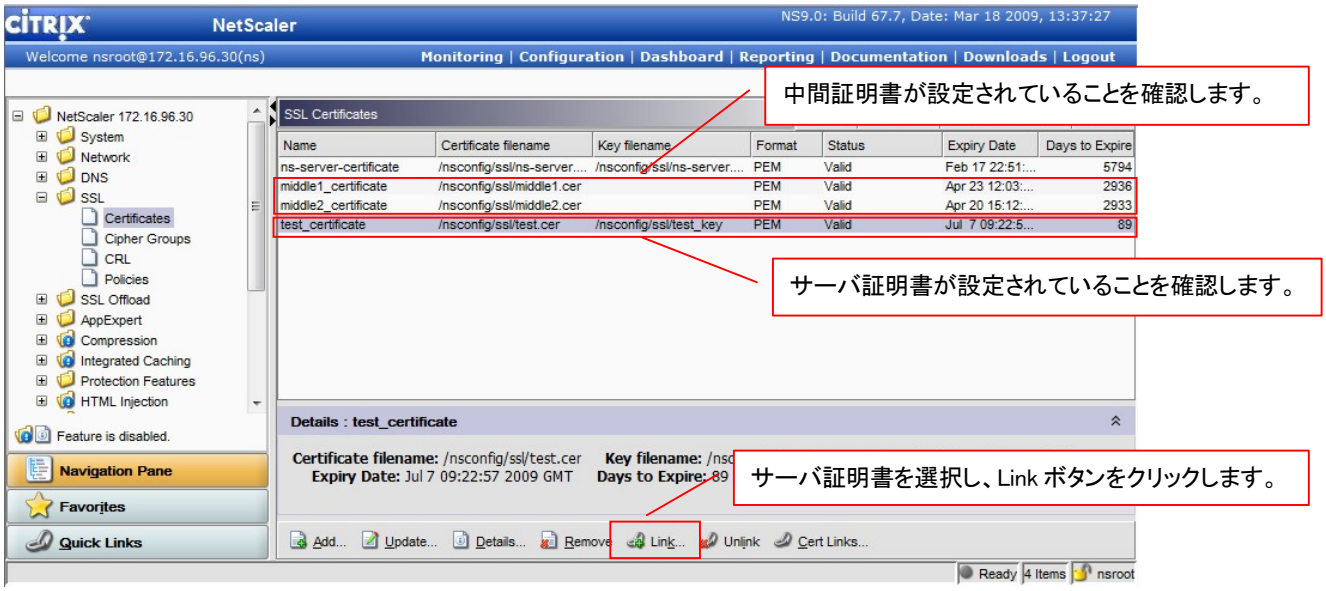
3. 選択した証明書が表示されていることを確認して、Install ボタンをクリックします。
中間証明書の場合、鍵の設定は必要ありません。
本例では中間証明書を2つ使用しますので、もう一方の中間証明書も同様に設定します。



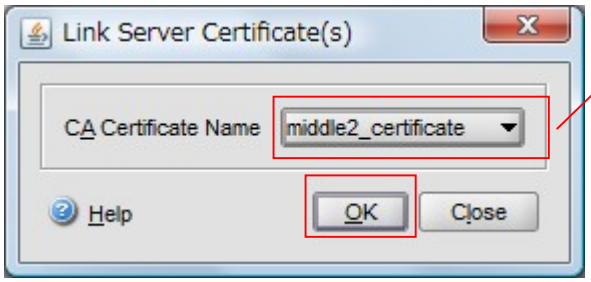
4. サーバ証明書を設定するため、証明書と鍵のペア名を入力します。その後、Browse ボタンをクリックし、証明書と鍵と選択して、必要項目を入力し Install ボタンをクリックします。
本例では、②-6 にて証明書発行機関より発行された証明書と、①-2 にて作成した鍵のペアを設定しています。



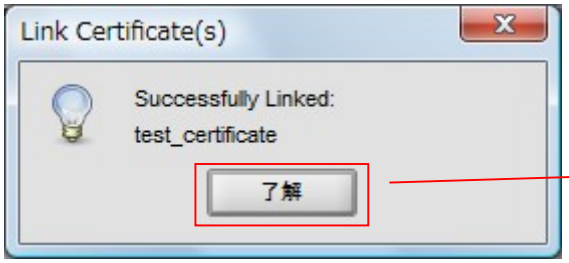
5. 中間証明書とサーバ証明書が設定されていることを確認します。その後、サーバ証明書と中間証明書を紐付けるため、サーバ証明書を選択して、画面下の Link ボタンをクリックします。



6. 中間証明書の選択画面になりますので、対象の証明書を選択し、OK ボタンをクリックします。

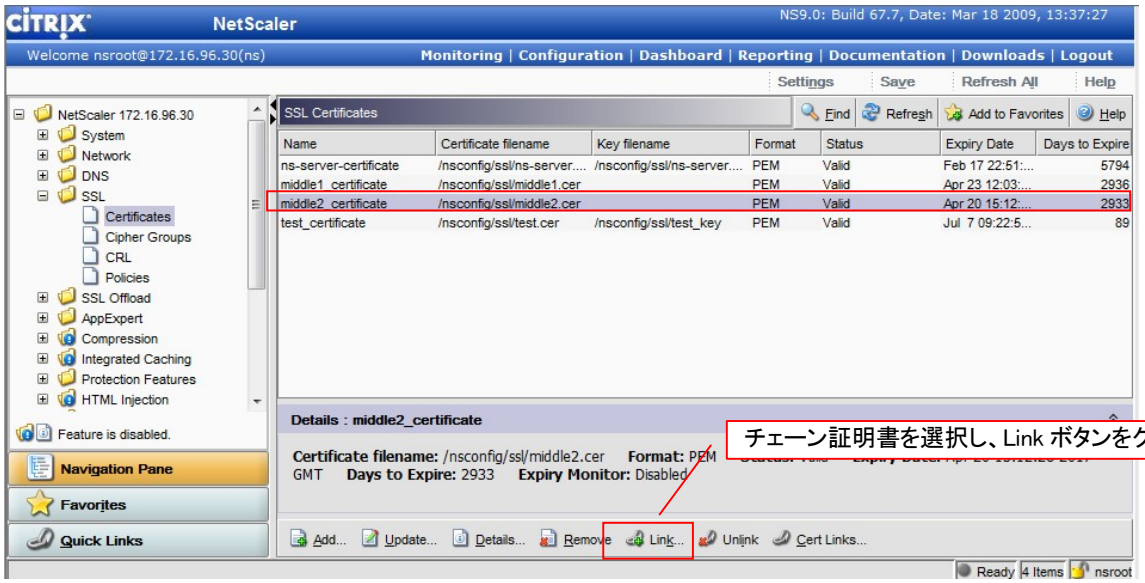


プルダウンより対象の中間証明書を選択します。
本例ではサーバ証明書『tes_certigicate』と中間証明書『middle1_certificate』のチェーン証明書である『middle2_certificate』と『tes_certigicate』を紐付けています。

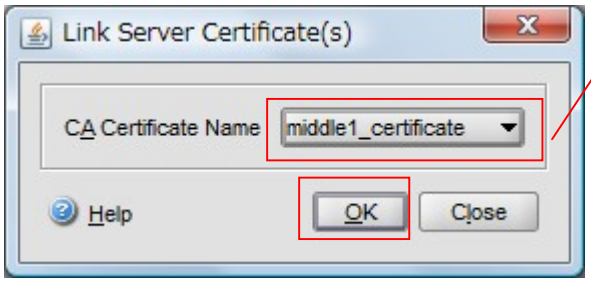


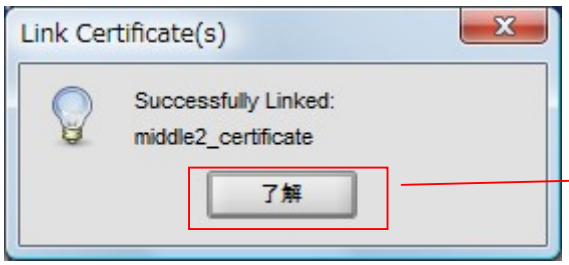
設定の確認画面が表示されますので、『了解』ボタンをクリックします。

7. チェーン証明書と中間証明書を紐付けるため、チェーン証明書を選択して、画面下の Link ボタンをクリックします。

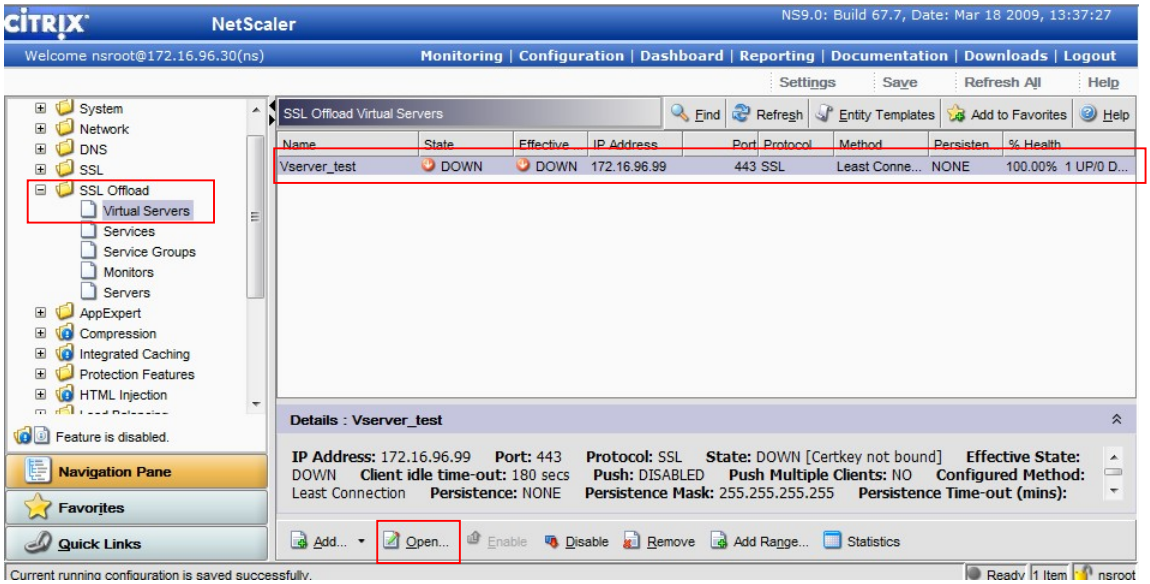


8. 中間証明書の選択画面になりますので、対象の証明書を選択し、OK ボタンをクリックします。

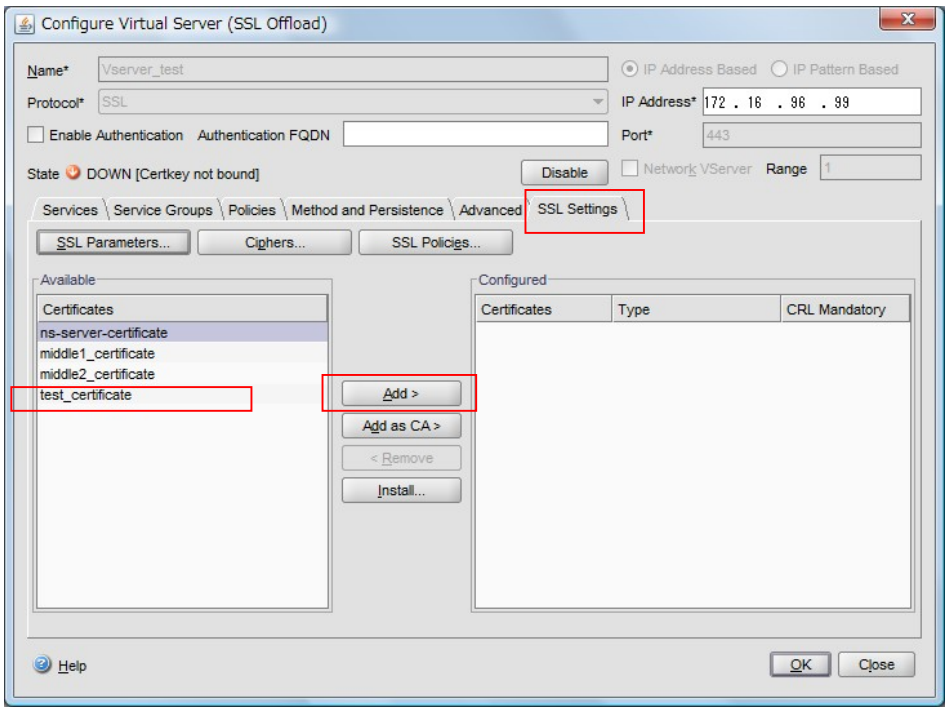




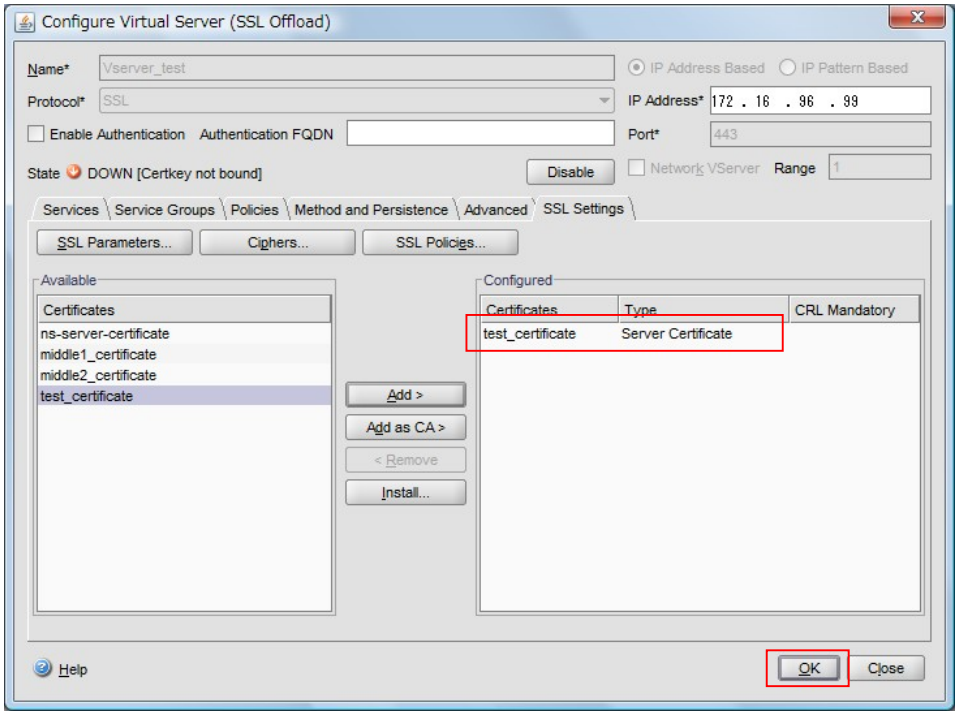
9. Vserve に、設定したサーバ証明書と鍵のペアを紐付けるため、画面右より SSL → Virtual Servers を選択します。その後対象の Vserver を選択し、Open ボタンをクリックします。(証明書の紐付け以外の Vserve の設定は、すべて正常に終了していることを前提としています。)



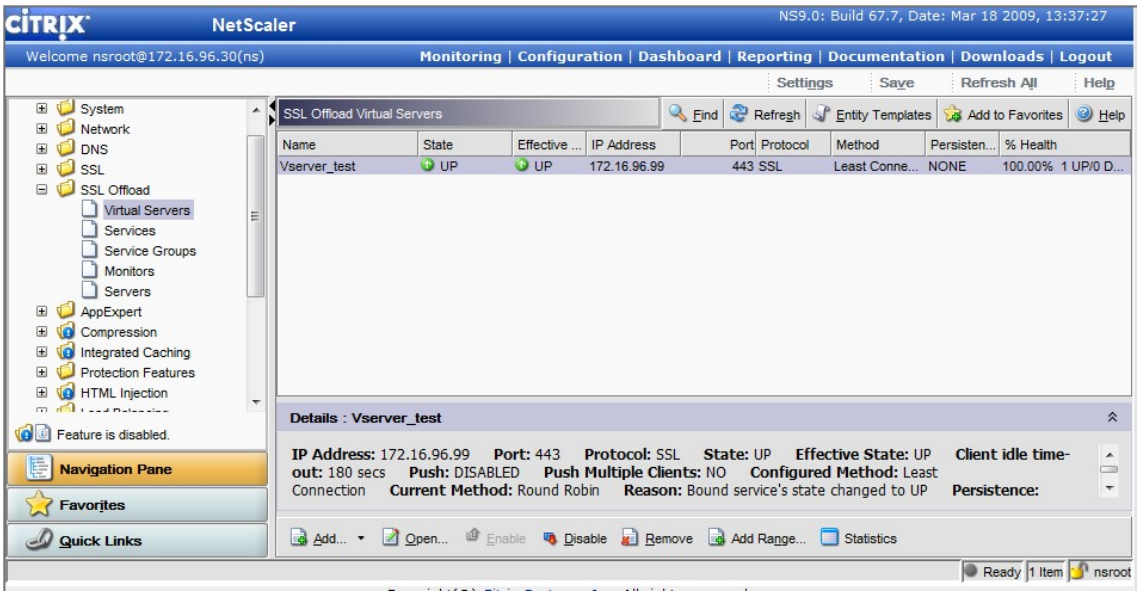
10. SSL Settings タブにて、対象のサーバ証明書と鍵のペアを選択し、Add ボタンをクリックします。



11. 選択した証明書が、画面右に表示されていることを確認し、OK ボタンをクリックします。

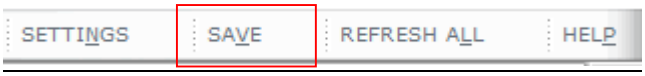


12. 証明書が正常に Vserver と紐付けられている場合、State が UP になっているので、確認します。



13.　動作確認をして作業完了です。

※　設定を保存する場合は、設定画面の右上の『SAVE』ボタンをクリックする必要がありますのでご注意ください。



最後に

以上