



北京四通管理软件技术有限公司  
Beijing Stone Software Technology Co., Ltd



## PoC标准化实施指南

### 基础环境

#### 07 NetScaler基本安装及配置

版本：v1.0

目 录

修正历史 ..... 2

第 1 章 基本过程..... 3

    1.1 安装配置环境..... 4

第 2 章 基础环境准备——DNS 解析配置..... 5

第 3 章 StoreFront 结合 NetScaler 配置.....10

第 4 章 NetScaler 配置 .....16

    4.1 NetScaler VPX 虚拟机导入 .....16

    4.2 NetScaler 基础配置 .....23

    4.3 NetScaler 服务器证书申请及安装 .....28

        4.3.1 NetScaler 服务器证书申请 .....28

        4.3.2 NetScaler 服务器证书安装 .....37

    4.4 NetScaler Gateway 配置向导 .....39

    4.5 使用 IOS 设备第一次登录失败 .....44

    4.6 访问验证及 NetScaler Gateway 登录首页风格优化.....46

    4.7 常见问题及排错.....49

        4.7.1 注意事项： .....49

        4.7.2 常见错误： .....50

产品版本 .....52

修正历史

修正	改变说明	更新者	日期
V1.0	新建	陈余南、李申君、 孙凌、杨华	2014年7月11日

## 第1章 基本过程

本章节介绍了通过 NetScaler 实现 ICA Proxy 的基本过程。其包括了：

- 基础环境准备——DNS 解析配置
- StoreFront 结合 NetScaler 配置
- NetScaler 配置
  - VPX 虚机导入
  - NetScaler 服务器证书申请
  - NetScaler Gateway 配置向导
  - 访问验证

本章节开始前，请确认 《PoC 手册 - 1 基础环境 - Lab 06 StoreFront 配置 v1.0》环境均已完成。并且确认有有效的测试 NetScaler License 文件供此测试使用。

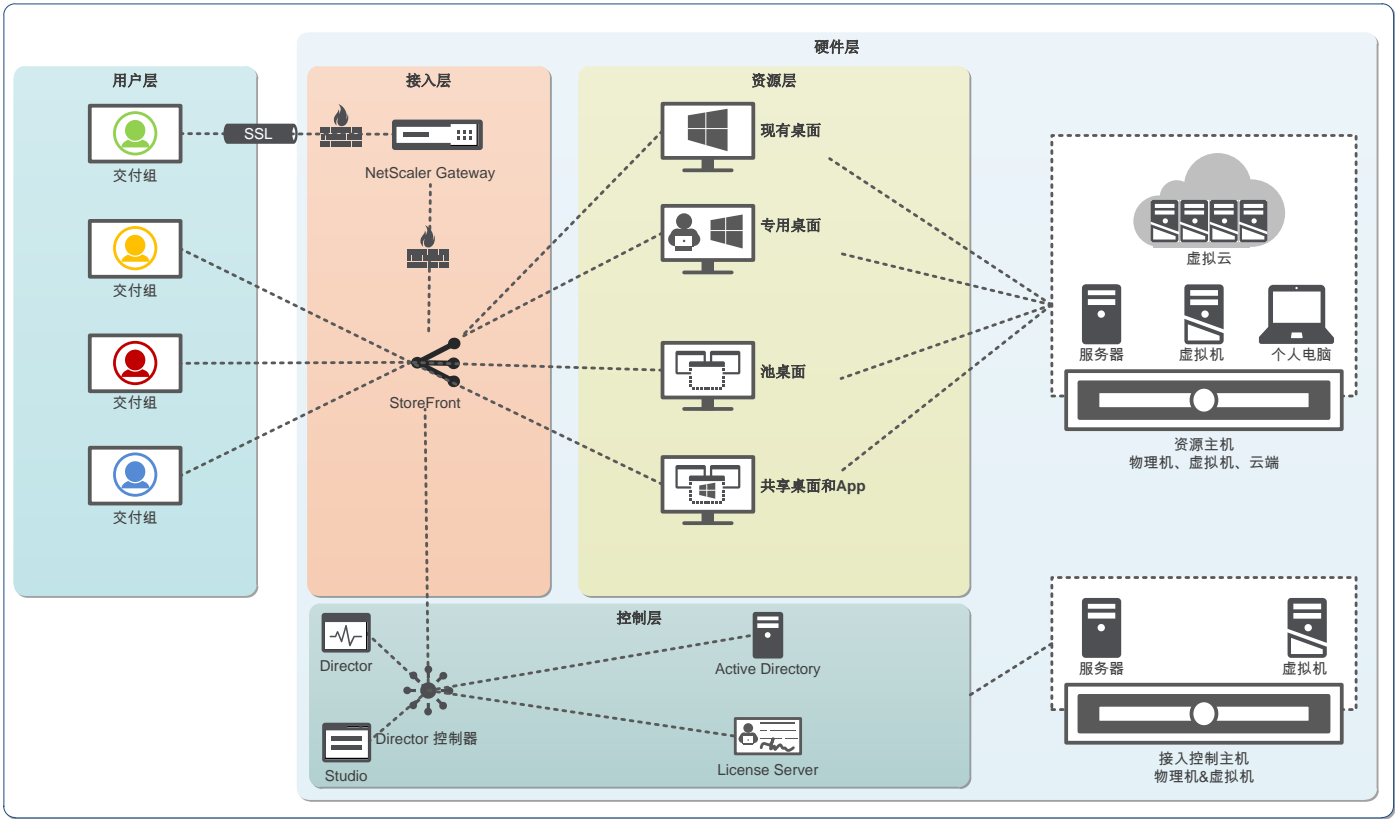
### 术语

NSIP，是 NetScaler 的管理 IP，用于对 NetScaler 本身进行一般的系统配置和管理访问的 IP 地址。

VIP，提供给客户端直接访问的 IP 地址，实际测试环境中需要将 VIP 443 端口，映射到公网。

SNIP，SNIP 用于 NetScaler 本身访问后端服务器使用。因为 NetScaler 的工作模式通常是部署在服务器群的前面，做为客户端和后端服务器之间的透明 TCP 代理，这个操作模式称为"请求交换技术"，是 NetScaler 功能的核心。当 NetScaler 做为 TCP 代理的时候，它会把客户机发过来的请求切断，然后自己建立一个 TCP 连接到后端的应用服务器，当后端应用服务器处理完毕以后再返回给 NetScaler，然后 NetScaler 再返回结果给用户。这个过程中，NetScaler 会使用 SNIP 做为向后端应用服务器请求的源地址。

1.1 安装配置环境



通过 NetScaler 实现 ica proxy 有多种实现方式，本 PoC 只作为 PoC Runbook 使用，考虑到简化部署：

- 使用 NetScaler Gateway 做身份认证
- NetScaler 对外只有一个 IP 地址即 NetScaler Gateway 的 Virtual Server IP（VIP）

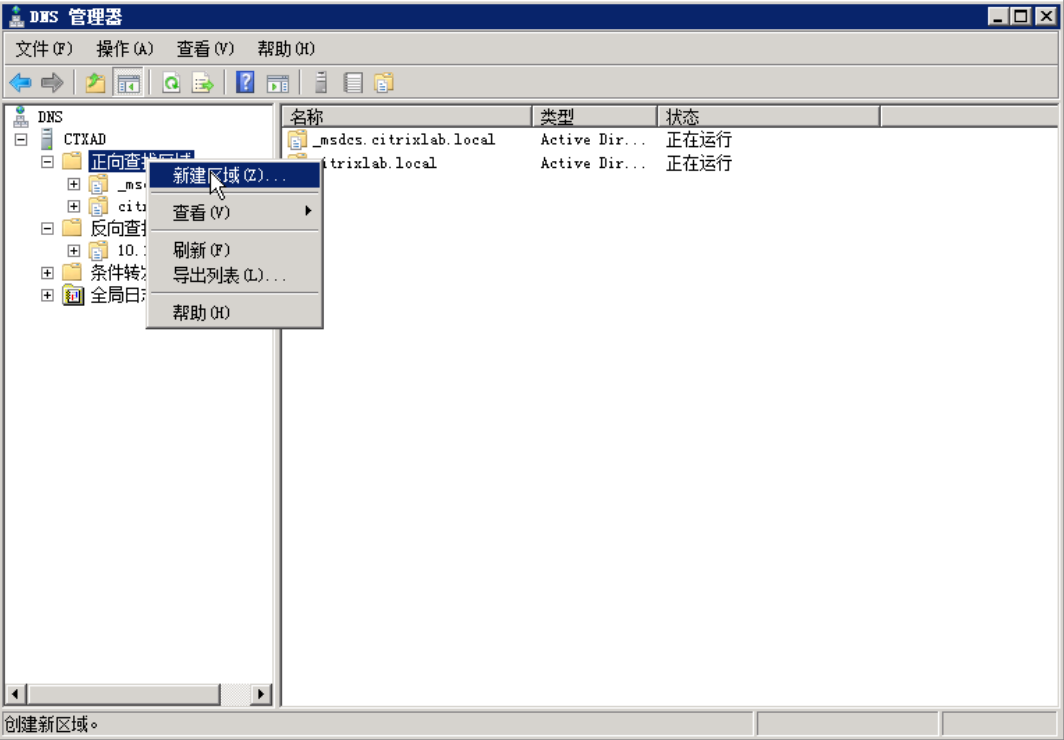
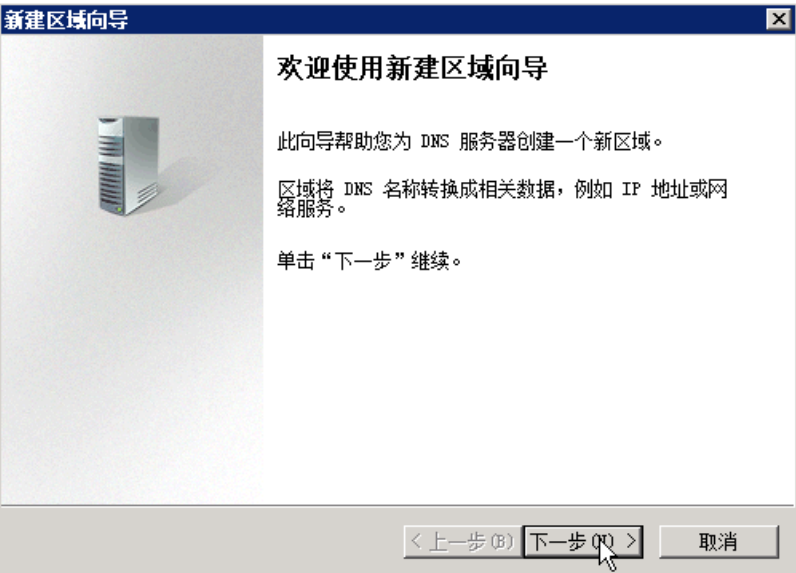
当用户请求 Web 站点时，NetScaler Gateway Virtual Server 将把请求转给 StoreFront。

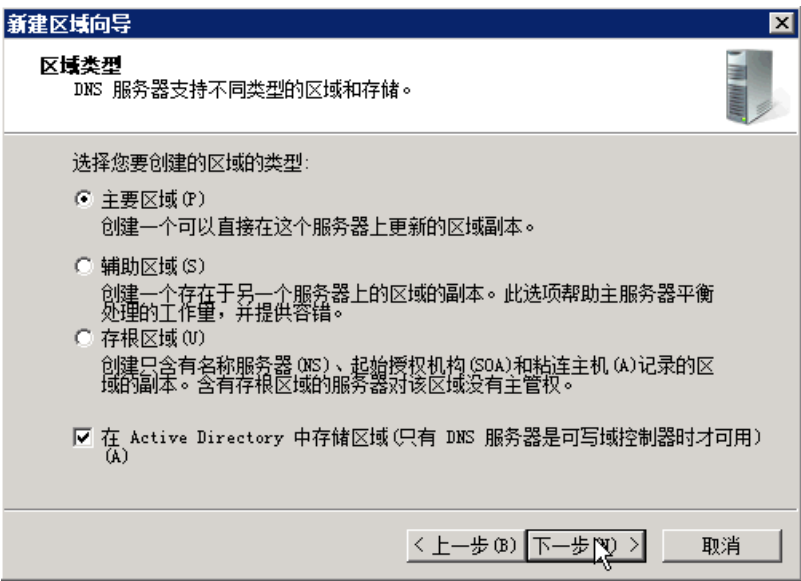
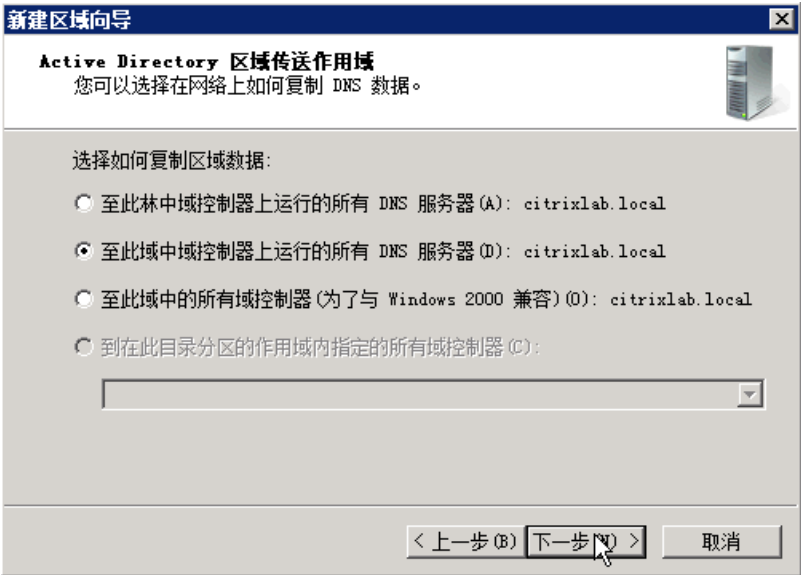
本 PoC 为了简化起见，内外网地址都使用 192.168.10.0/24，但必须要明白，当 NetScaler Gateway 被放置在 DMZ 的时候，VIP 是 ICA 请求从公网接入的唯一入口。

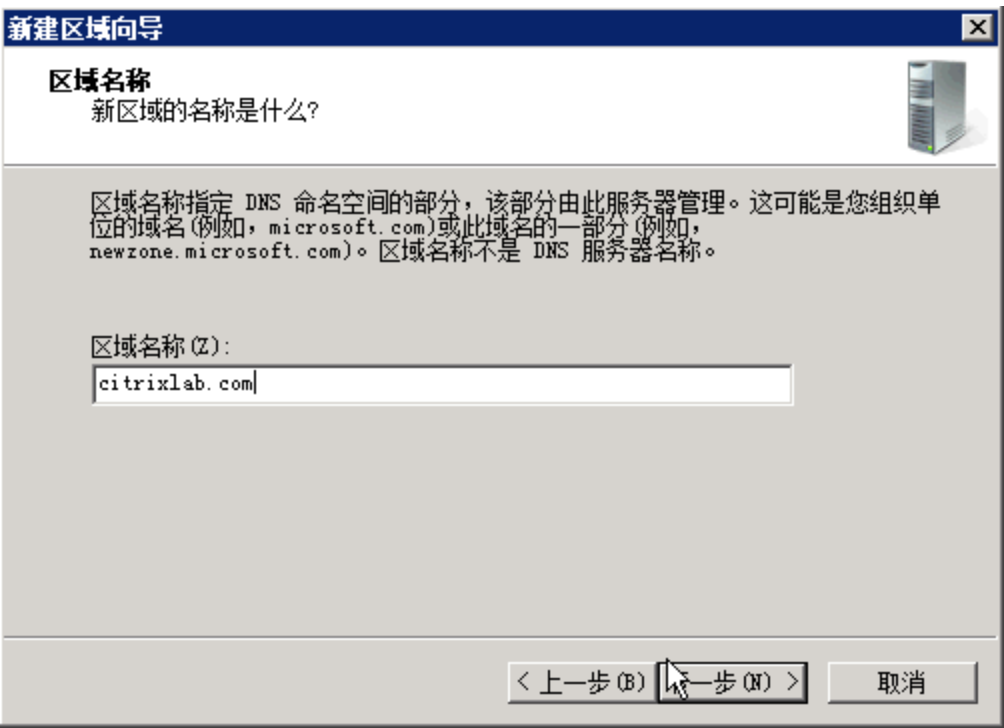
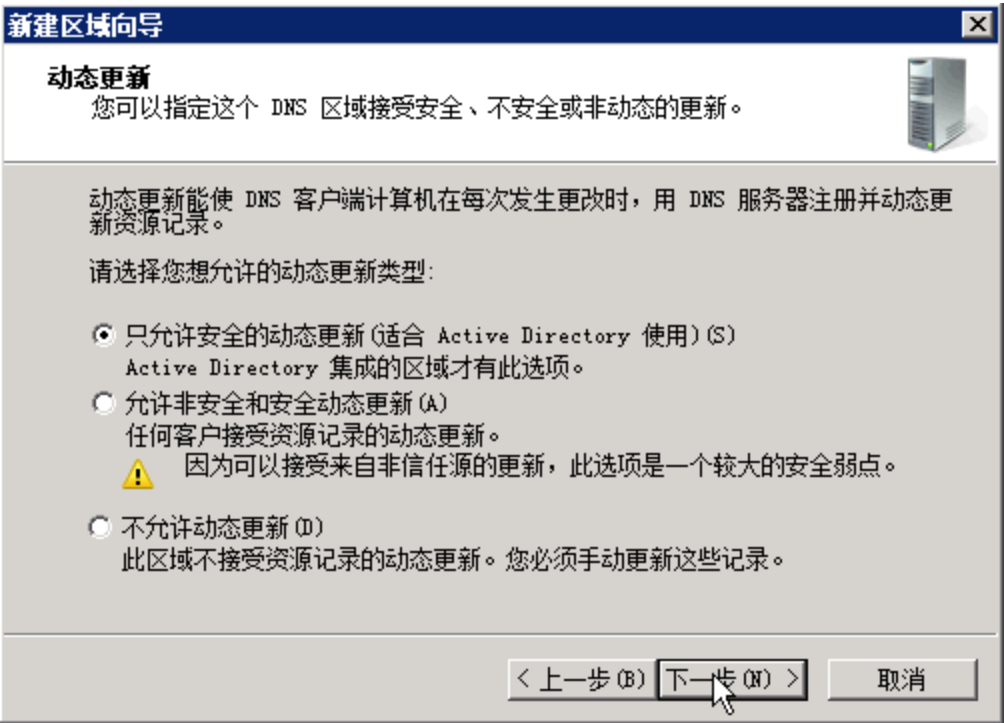
NetScaler 规划，版本：Netscaler 10.1 build 126.12nc

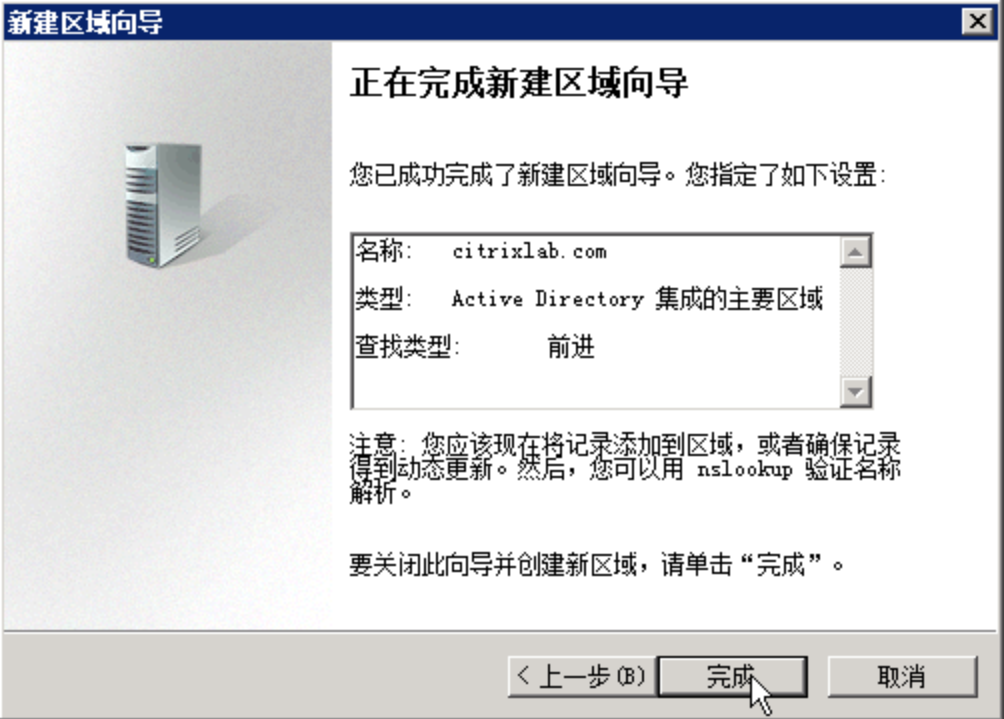
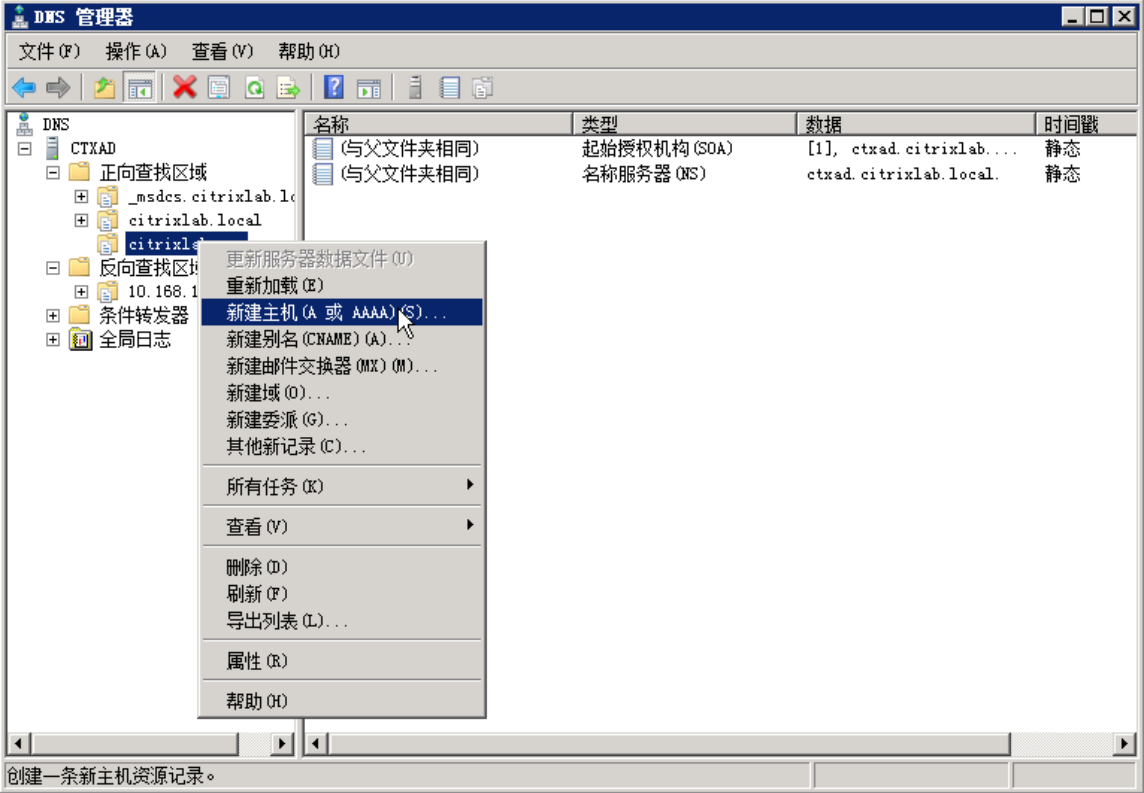
No		IP Address	FQDN
1	VPX IP（NSIP）	192.168.10.145	
2	Subnet IP(SNIP)	192.168.10.146	
3	NetScaler Gateway virtual server IP（VIP）	192.168.10.147	www.citrixlab.local

第2章 基础环境准备——DNS 解析配置

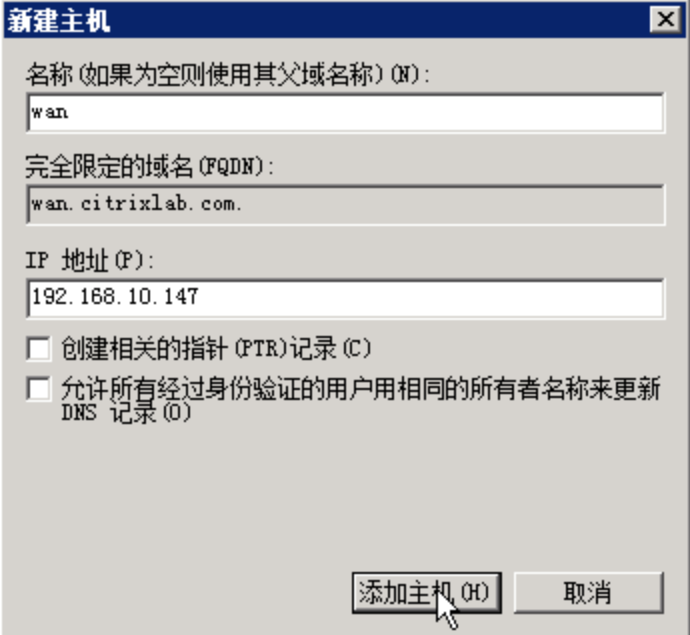

步骤	操作									
1.	<p>配置 DNS 解析(实际测试中必须使用公网域名和对应公网 IP)</p> <p>如果有公网域名和 IP 后，可跳过以下步骤。</p> <p>本次 POC 在 AD 上的 DNS 来做解析</p> <p>在开始，管理工具，DNS 管理器中右键 “正向查找区域”，点击 “新建区域”。</p>  <p>The screenshot shows the DNS Manager console with a tree view on the left containing 'CTXTAD', '正向查找区域', '反向查找区域', '10.10.10.10', '条件转发', and '全局记录'. A right-click context menu is open over '正向查找区域', with options: '新建区域(N)...', '查看(V)', '刷新(F)', '导出列表(L)...', and '帮助(H)'. The main pane shows a table of zones:</p> <table><tr><th>名称</th><th>类型</th><th>状态</th></tr><tr><td>_msdcs.citrixlab.local</td><td>Active Dir...</td><td>正在运行</td></tr><tr><td>citrixlab.local</td><td>Active Dir...</td><td>正在运行</td></tr></table> <p>At the bottom of the console, the text '创建新区域。' is visible.</p>	名称	类型	状态	_msdcs.citrixlab.local	Active Dir...	正在运行	citrixlab.local	Active Dir...	正在运行
名称	类型	状态								
_msdcs.citrixlab.local	Active Dir...	正在运行								
citrixlab.local	Active Dir...	正在运行								
2.	<p>点击 “下一步”</p>  <p>The screenshot shows the '新建区域向导' (New Zone Wizard) window. It has a title bar with a close button. The main area contains a server icon, the text '欢迎使用新建区域向导' (Welcome to the New Zone Wizard), and instructions: '此向导帮助您为 DNS 服务器创建一个新区域。' (This wizard helps you create a new zone for the DNS server.), '区域将 DNS 名称转换成相关数据，例如 IP 地址或网络服务。' (The zone converts DNS names into related data, such as IP addresses or network services.), and '单击“下一步”继续。' (Click 'Next' to continue.). At the bottom, there are three buttons: '&lt; 上一步(B)' (disabled), '下一步(N) &gt;' (active, with a mouse cursor), and '取消' (disabled).</p>									

步骤	操作
3.	<p>选择“主要区域”，点击“下一步”。</p> 
4.	<p>选择“至此域中域控制器上运行的所有 DNS 服务器 (D): citrixlab.local”，点击“下一步”</p> 

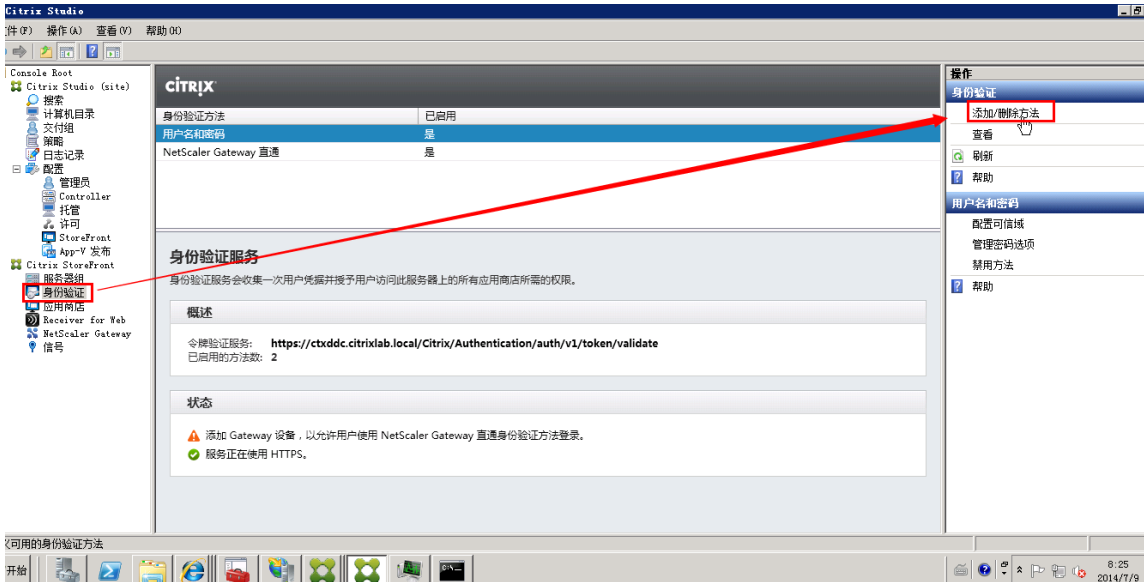
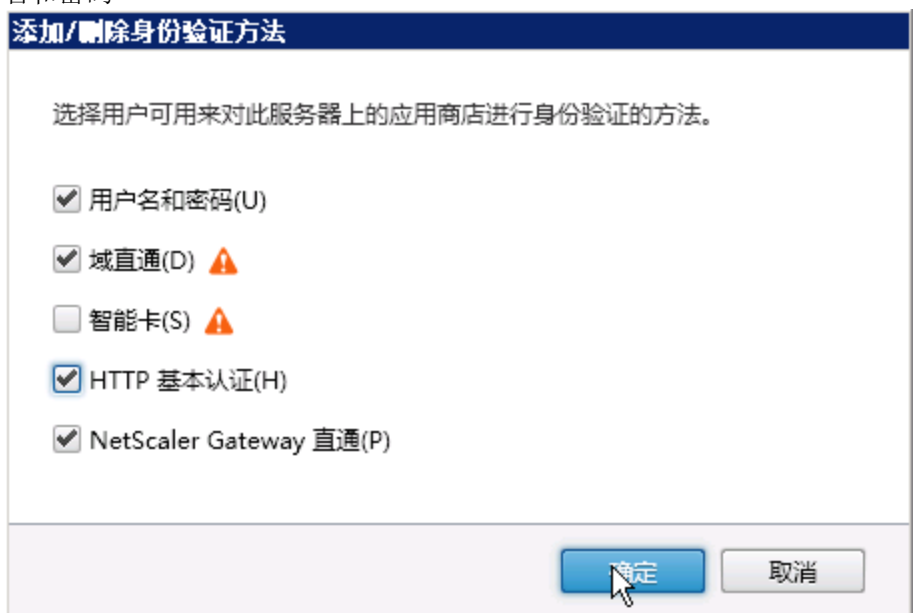
步骤	操作
5.	<p>输入 citrixlab.com, 点击“下一步”</p> 
6.	<p>选择“只允许安全的动态更新”，点击“下一步”。</p> 

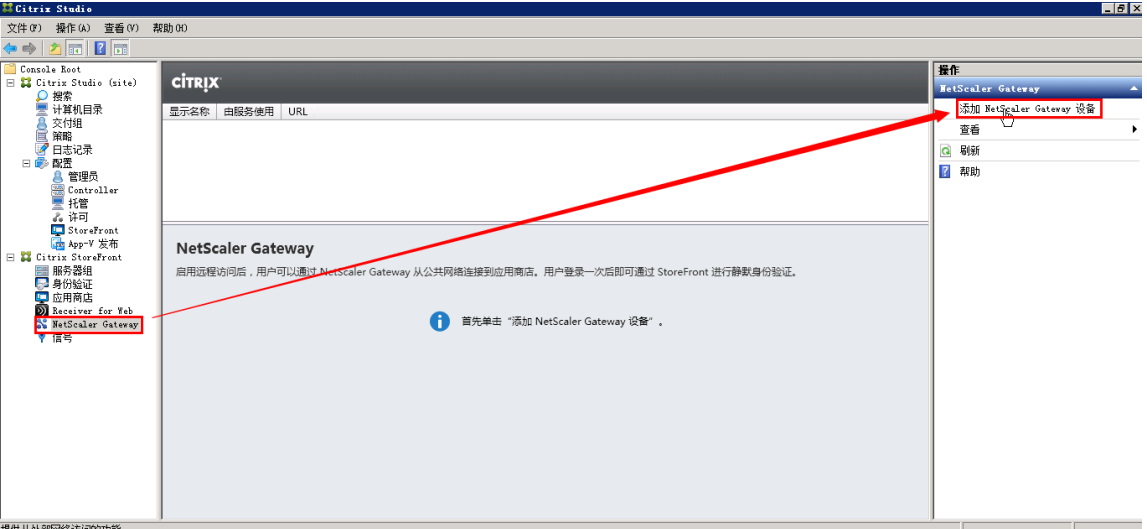

步骤	操作
7.	<p>点击“完成”。</p> 
8.	<p>右键“citrixlab.com”，点击“新建主机（A 或 AAAA）”。</p> 

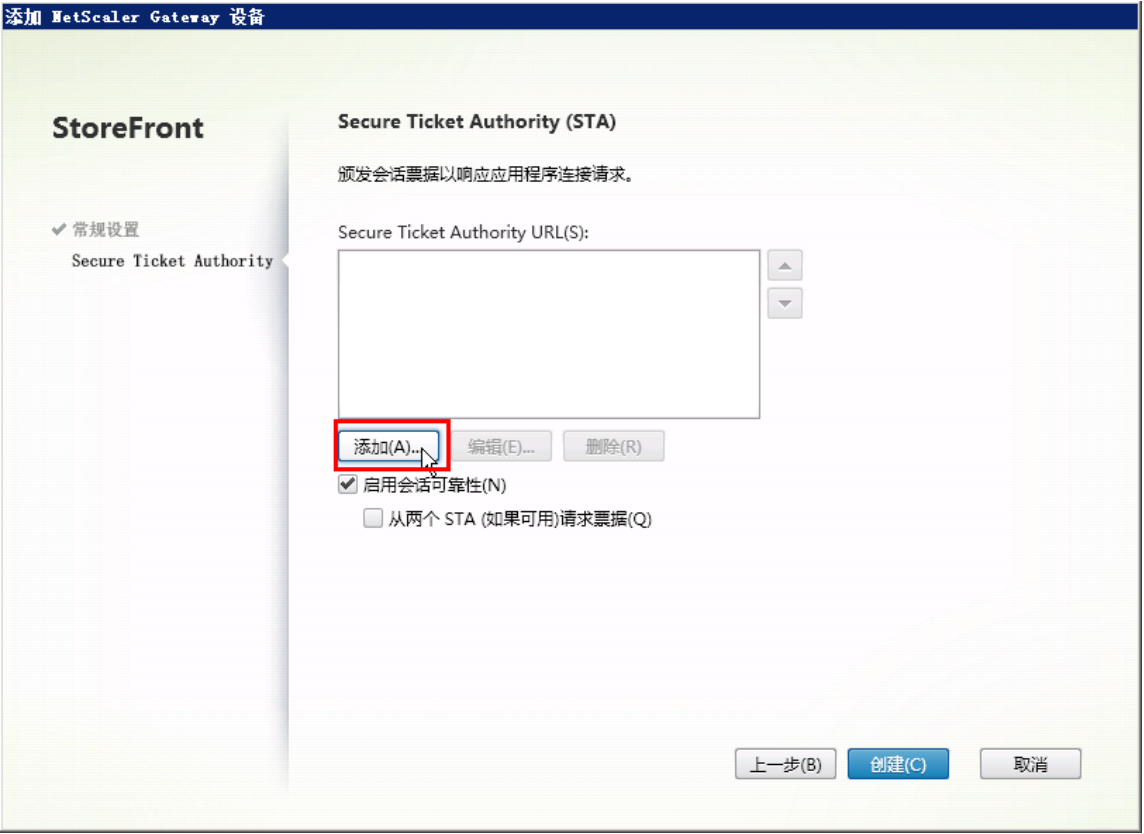
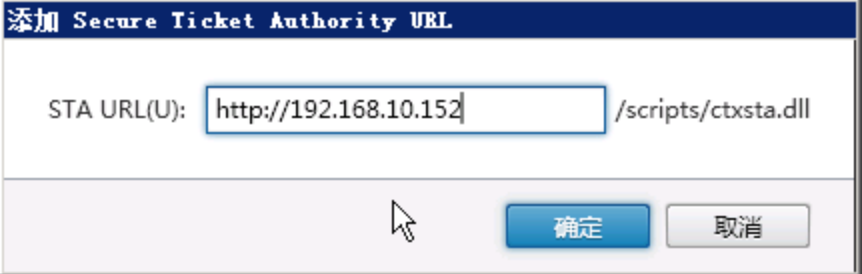


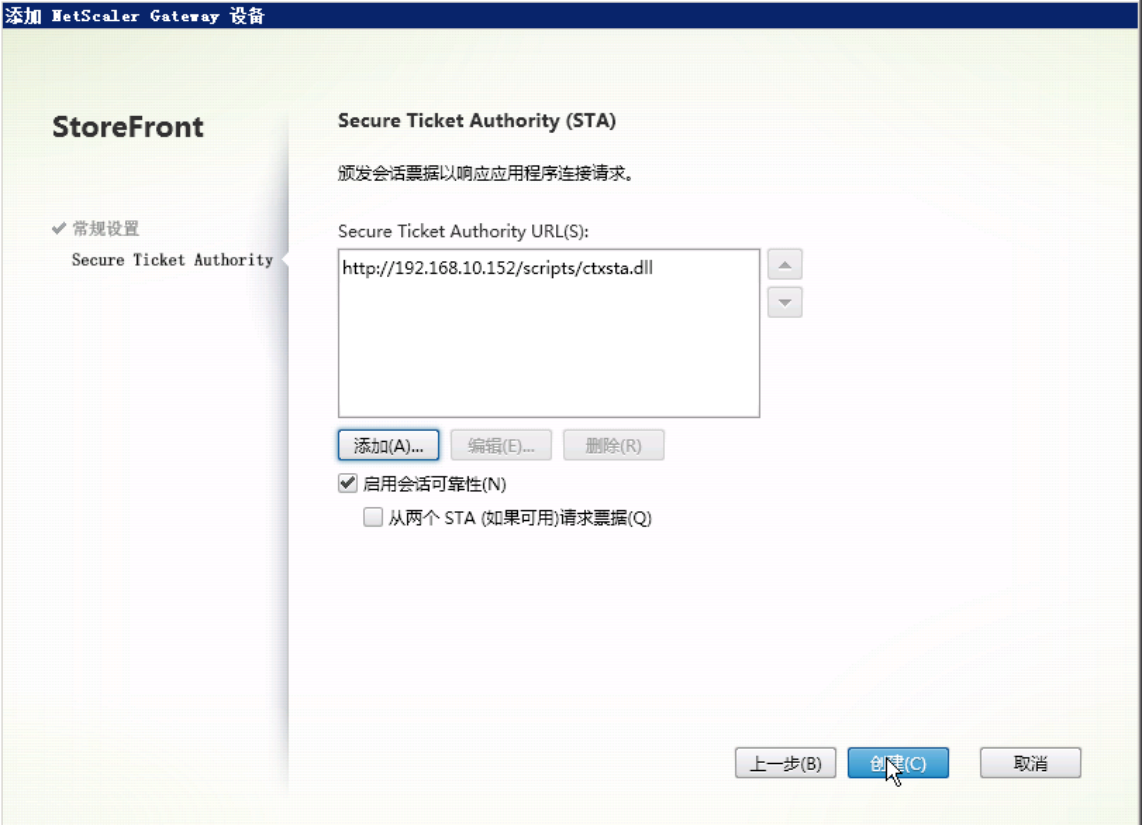

步骤	操作
9.	<p>输入以下内容            名称: wan            IP 地址: 192.168.10.147            点击“添加主机”            本次 POC 中使用 wan.citrixlab.com 模拟公网域名</p> 
10.	<p>在客户端和 CTXDDC 服务器上打开 CMD 命令行，输入: ping wan.citrixlab.com            查看该地址是否能被正确解析。</p> 

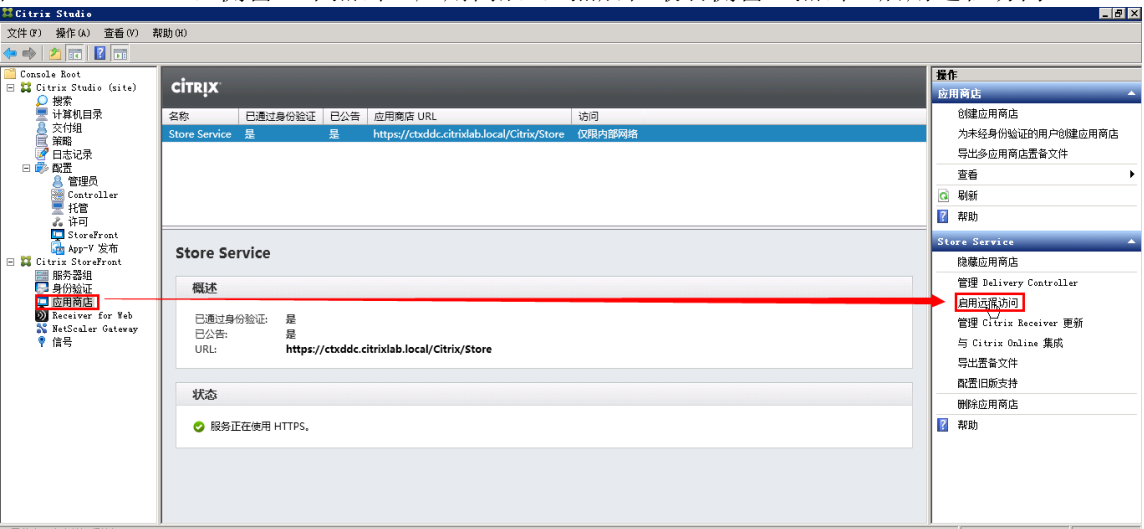

## 第3章 StoreFront 结合 NetScaler 配置

步骤	操作
1.	<p>使用 ctxadmin 账号登录 CTXDDC 服务器，打开 Citrix Studio，在左侧窗口点击“身份验证”，然后在最右侧窗口点击“添加/删除方法”。</p> 
2.	<p>将“域直通”，“NetScaler Gateway 直通”，“HTTP 基本认证”勾选上，并保留默认的“用户名和密码”</p> 

步骤	操作
3.	<p>在 Citrix Studio 左侧窗口中点击“NetScaler Gateway”，然后在最右侧窗口点击“添加 NetScaler Gateway 设备”</p> 
4.	<p>在常规设置中输入以下内容</p> <p>显示名称: NetScaler Gateway</p> <p>NetScaler Gateway URL: <a href="https://wan.citrixlab.com">https://wan.citrixlab.com</a></p> <p>版本: 10.0 (Build 69.4) 或更高</p> <p>登录类型: 域</p> <p>回调 URL: <a href="https://wan.citrixlab.com">https://wan.citrixlab.com</a></p> <p>在子网 IP 地址中这里, 可以直接放空, 不填入 SNIP 地址</p> 

步骤	操作
5.	<p>点击“添加”</p>  <p>The screenshot shows the 'Add NetScaler Gateway Device' wizard. On the left, under 'StoreFront', there is a 'Secure Ticket Authority' section with a '常规设置' (General Settings) sub-section. The main area is titled 'Secure Ticket Authority (STA)' and contains the text '颁发会话票据以响应应用程序连接请求。' (Issue session tickets in response to application connection requests). Below this is a text box for 'Secure Ticket Authority URL(S):'. At the bottom of this section, there are three buttons: '添加(A)...' (Add), '编辑(E)...' (Edit), and '删除(R)' (Delete). The '添加(A)...' button is highlighted with a red rectangular box. Below the buttons are two checkboxes: '启用会话可靠性(N)' (Enable session reliability) which is checked, and '从两个 STA (如果可用)请求票据(Q)' (Request tickets from two STAs if available) which is unchecked. At the bottom right of the wizard are three buttons: '上一步(B)' (Previous), '创建(C)' (Create), and '取消' (Cancel).</p>
6.	<p>输入 <a href="http://192.168.10.152">http://192.168.10.152</a>，点击“确定”。 192.168.10.152 是 CTXDDC 的地址</p>  <p>The screenshot shows a dialog box titled '添加 Secure Ticket Authority URL' (Add Secure Ticket Authority URL). It contains a text field labeled 'STA URL(U):' with the value 'http://192.168.10.152' entered. To the right of the text field, the path '/scripts/ctxsta.dll' is displayed. At the bottom of the dialog are two buttons: '确定' (OK) and '取消' (Cancel). A mouse cursor is pointing at the '确定' button.</p>

步骤	操作
7.	<p>点击“创建”</p> 
8.	<p>点击“完成”</p> 







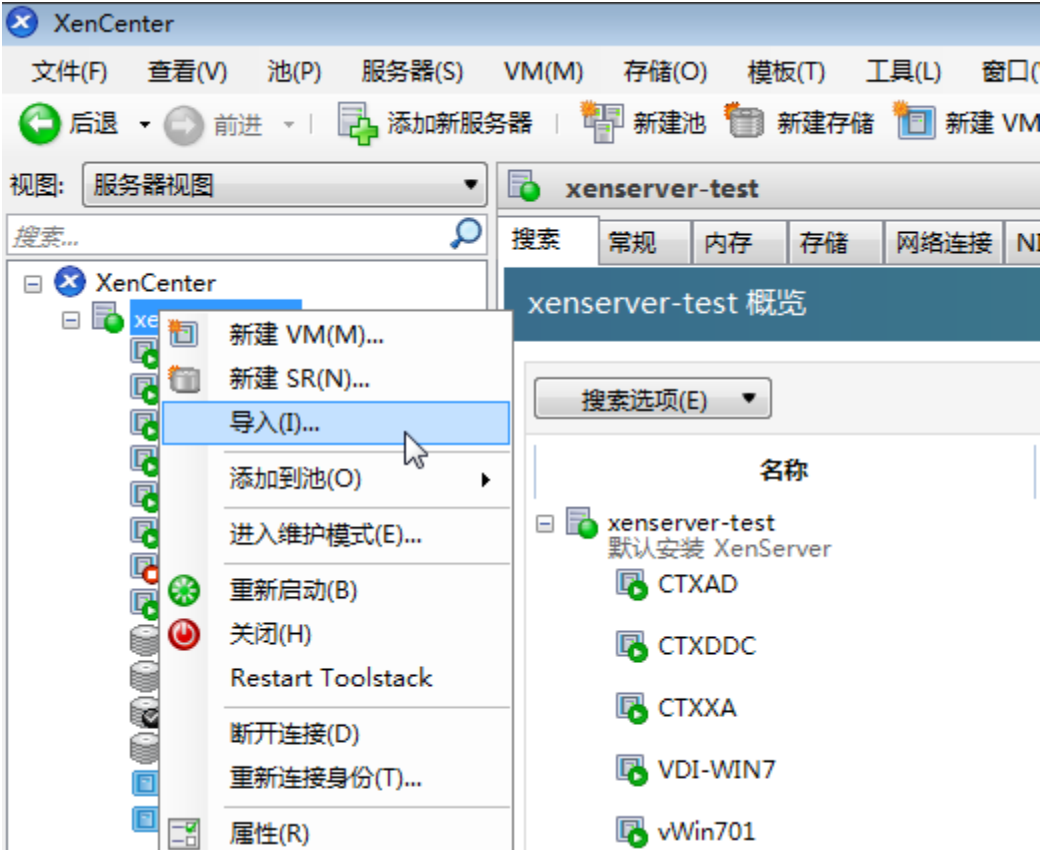
步骤	操作
9.	<p>在 Citrix Studio 左侧窗口中点击“应用商店”，然后在最右侧窗口点击“启用远程访问”</p> 
10.	<p>勾选 NetScaler Gateway，点击“确定”</p> 

步骤	操作
11.	<p>完成在 StoreFront 上的配置。</p>  <p>The screenshot shows the Citrix Studio console. On the left is a tree view with 'Citrix Studio (site)' expanded, showing 'StoreFront' and 'App-V 发布'. The main pane displays the 'Store Service' configuration for 'Store Service'. It includes a table with columns: 名称 (Name), 已通过身份验证 (Authenticated), 已公告 (Published), 应用商店 URL (Store URL), and 访问 (Access). The row shows 'Store Service' is authenticated and published, with URL 'https://ctxddc.citrixlab.local/Citrix/Store' and access '内部和外部网络' (Internal and external network). Below this is a 'Store Service' summary section with '概述' (Overview) and '状态' (Status). The status shows '服务正在使用 HTTPS' (Service is using HTTPS) with a green checkmark. On the right is a '操作' (Actions) pane with '应用商店' (Store) and 'Store Service' sections, listing actions like '创建应用商店' (Create Store), '删除应用商店' (Delete Store), and '管理 Delivery Controller' (Manage Delivery Controller).</p>

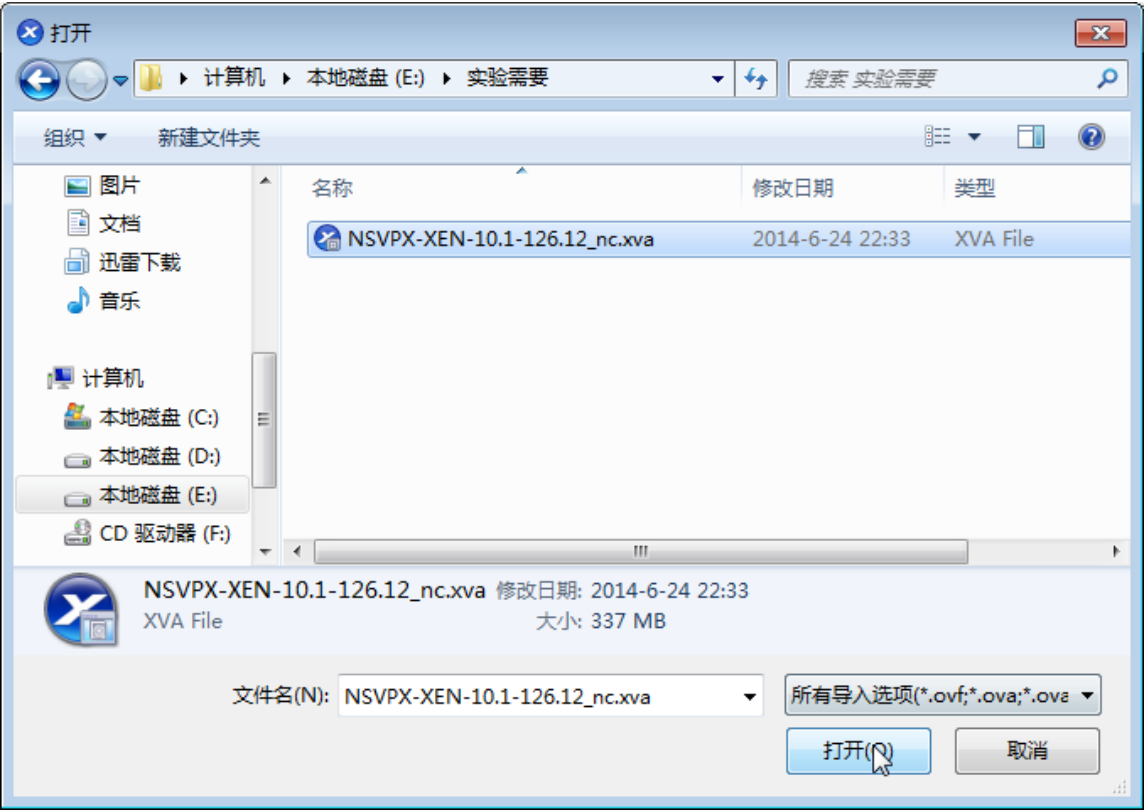
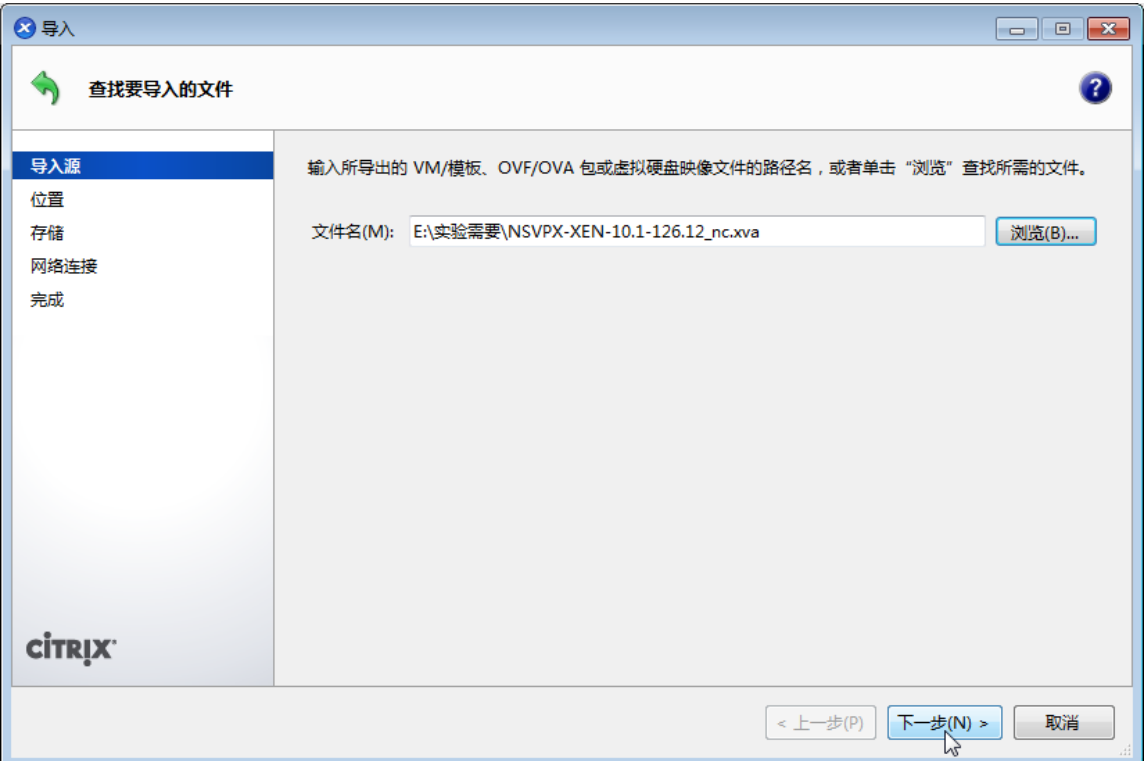
第4章 NetScaler 配置

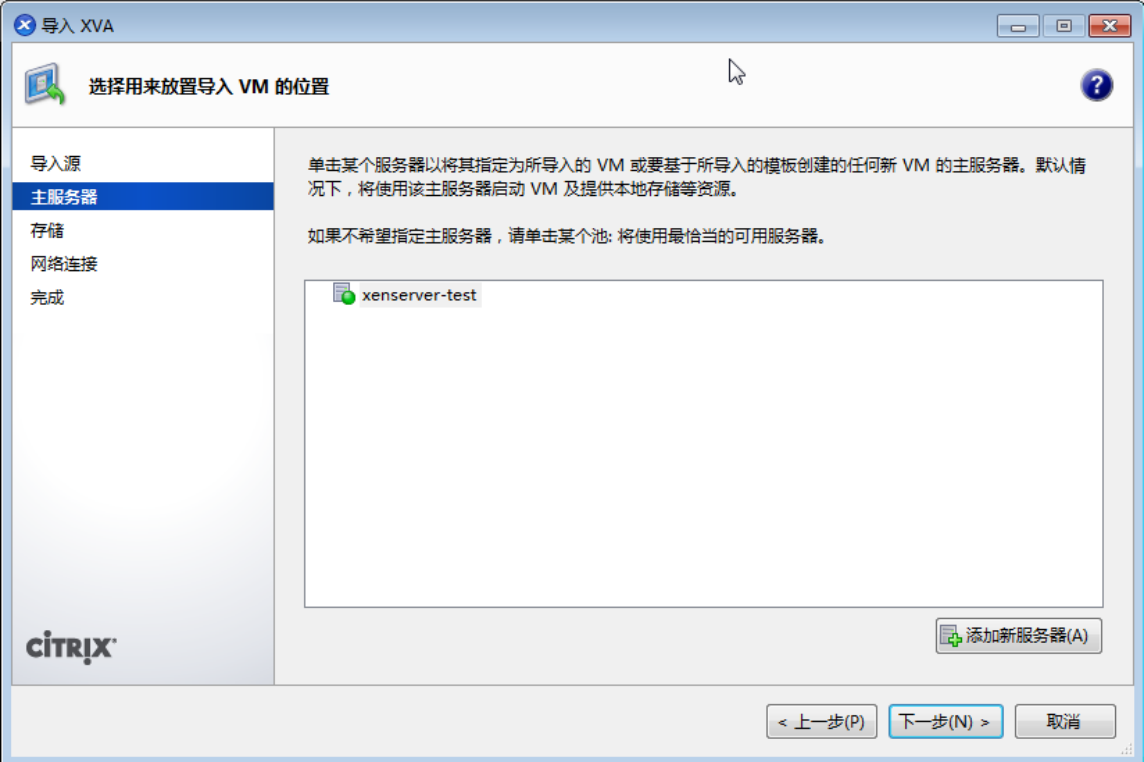
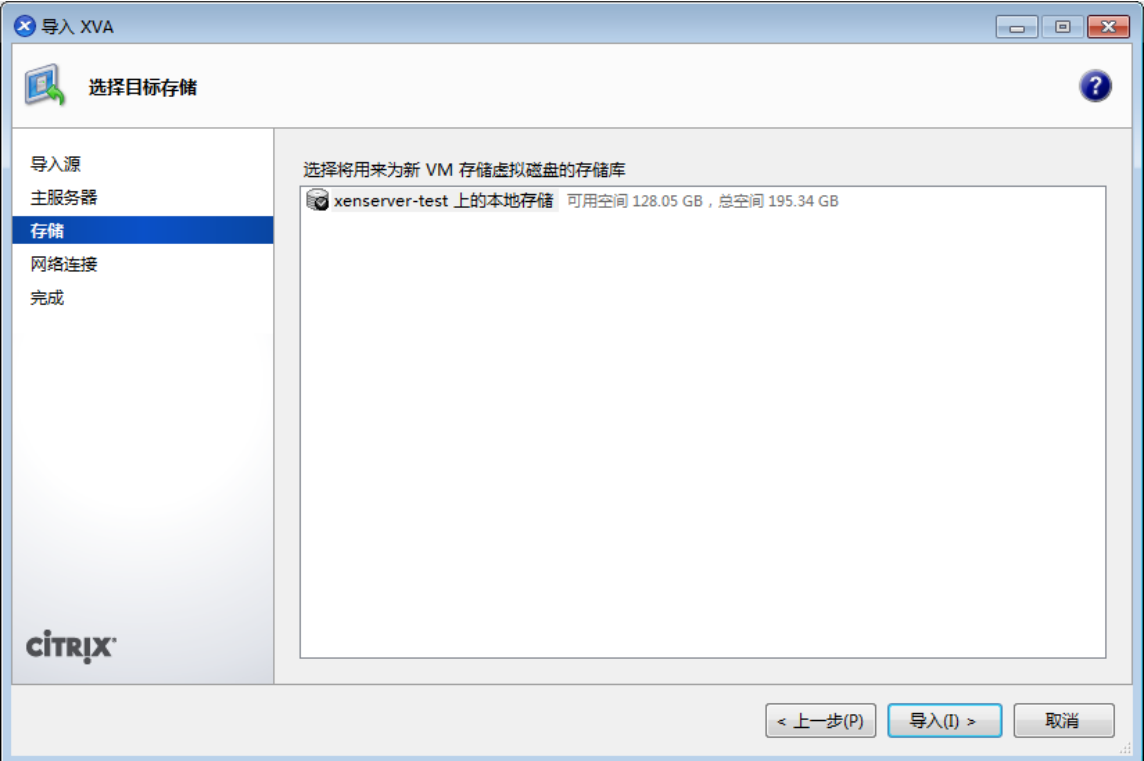
4.1 NetScaler VPX 虚拟机导入

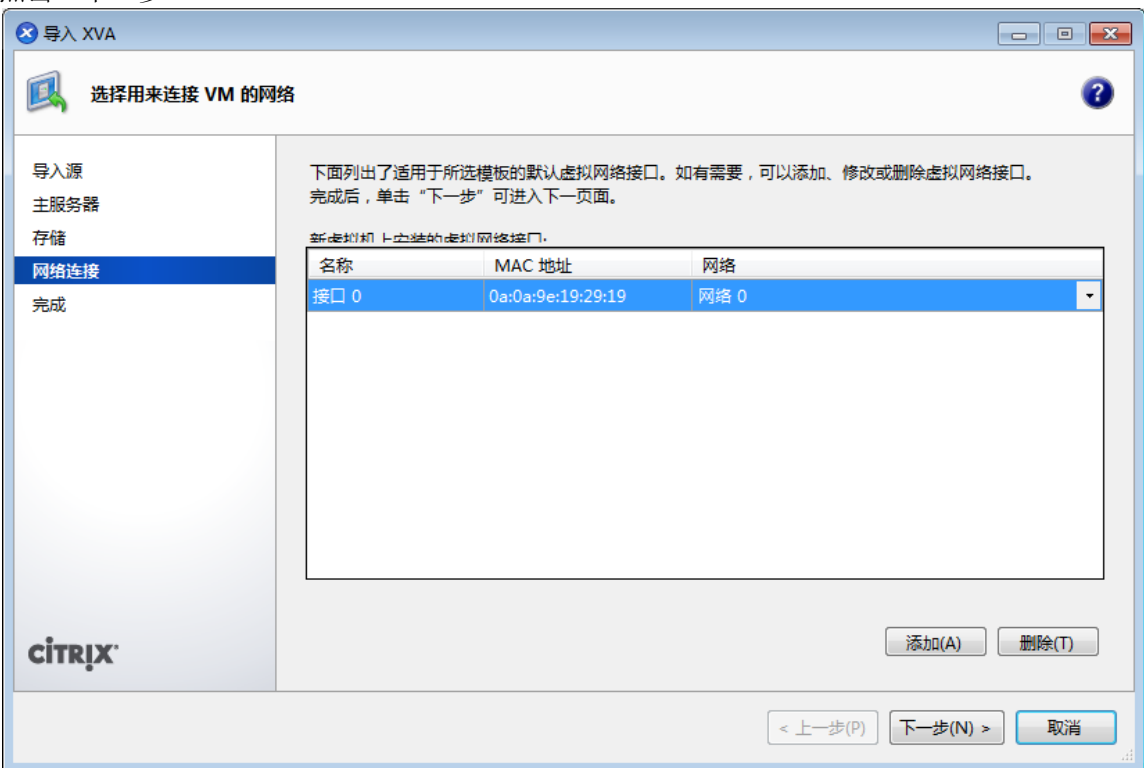
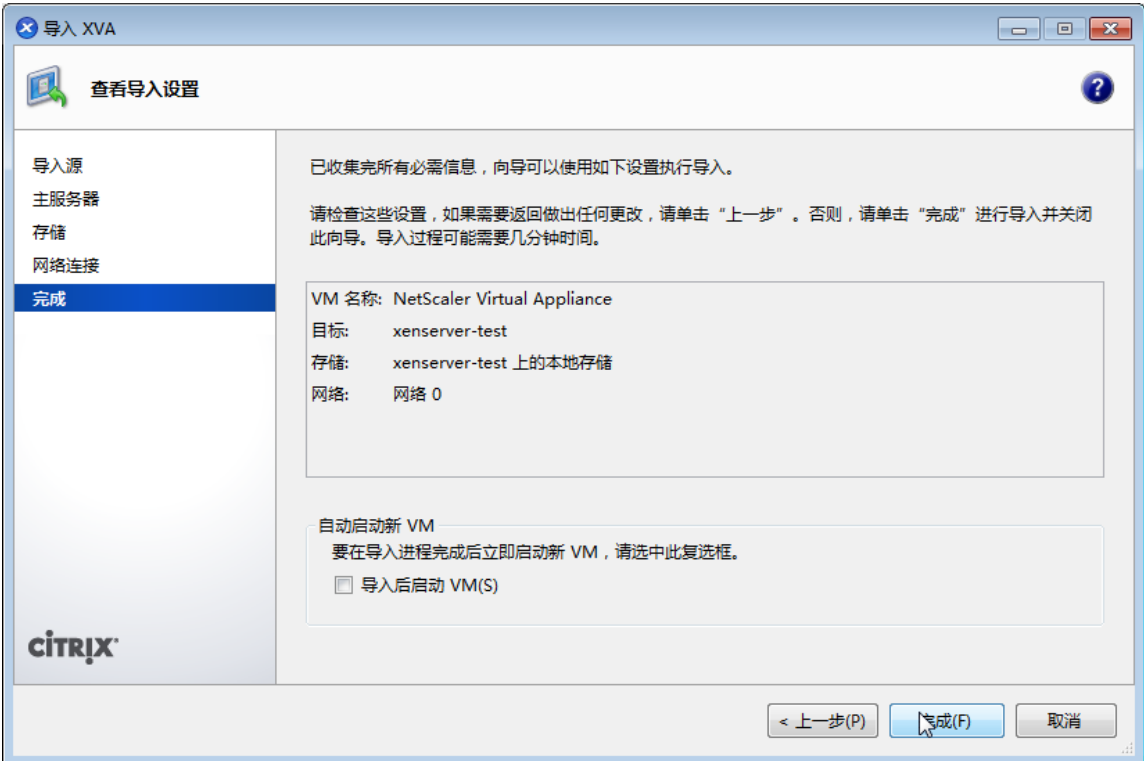
测试环节一般使用 NetScaler VPX 来进行，生产环境一般推荐使用 NetScaler MPX/SDX 硬件平台。NetScaler VPX 这次 XenServer，vSphere，Hyper-V，KVM4 个主流的虚拟化平台。

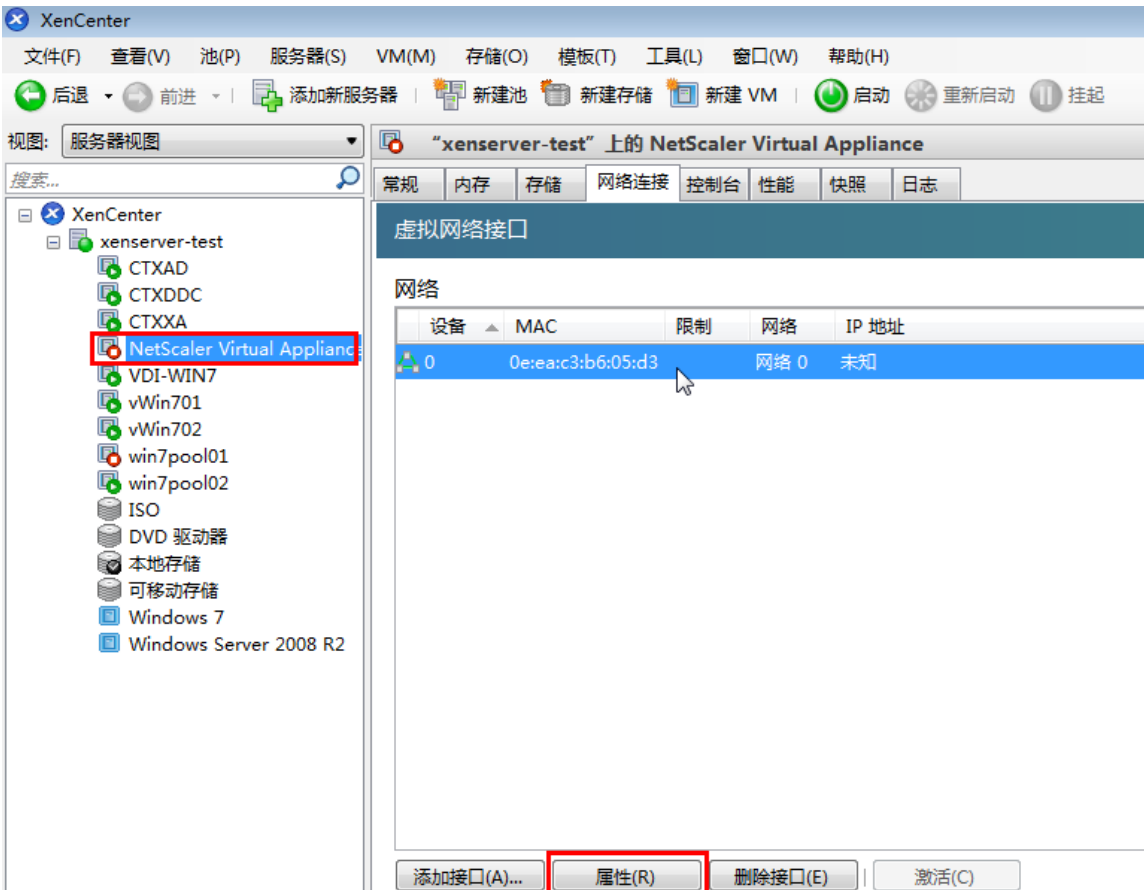

步骤	操作												
1.	<p>下载 NerScaler VPX 10.1 介质以及许可证文件。</p> <table> <tr> <th>名称</th><th>修改日期</th><th>类型</th><th>大小</th></tr> <tr> <td> 00155dcb1e07.lic</td><td>2014-7-9 17:04</td><td>LIC 文件</td><td>3 KB</td></tr> <tr> <td> NSVPX-XEN-10.1-126.12_nc.xva</td><td>2014-6-24 22:33</td><td>XVA File</td><td>345,625 KB</td></tr> </table>	名称	修改日期	类型	大小	 00155dcb1e07.lic	2014-7-9 17:04	LIC 文件	3 KB	 NSVPX-XEN-10.1-126.12_nc.xva	2014-6-24 22:33	XVA File	345,625 KB
名称	修改日期	类型	大小										
 00155dcb1e07.lic	2014-7-9 17:04	LIC 文件	3 KB										
 NSVPX-XEN-10.1-126.12_nc.xva	2014-6-24 22:33	XVA File	345,625 KB										
2.	<p>在 XenCenter 左边窗口中右键 “xenserver-test”，选择 “导入”。</p> 												

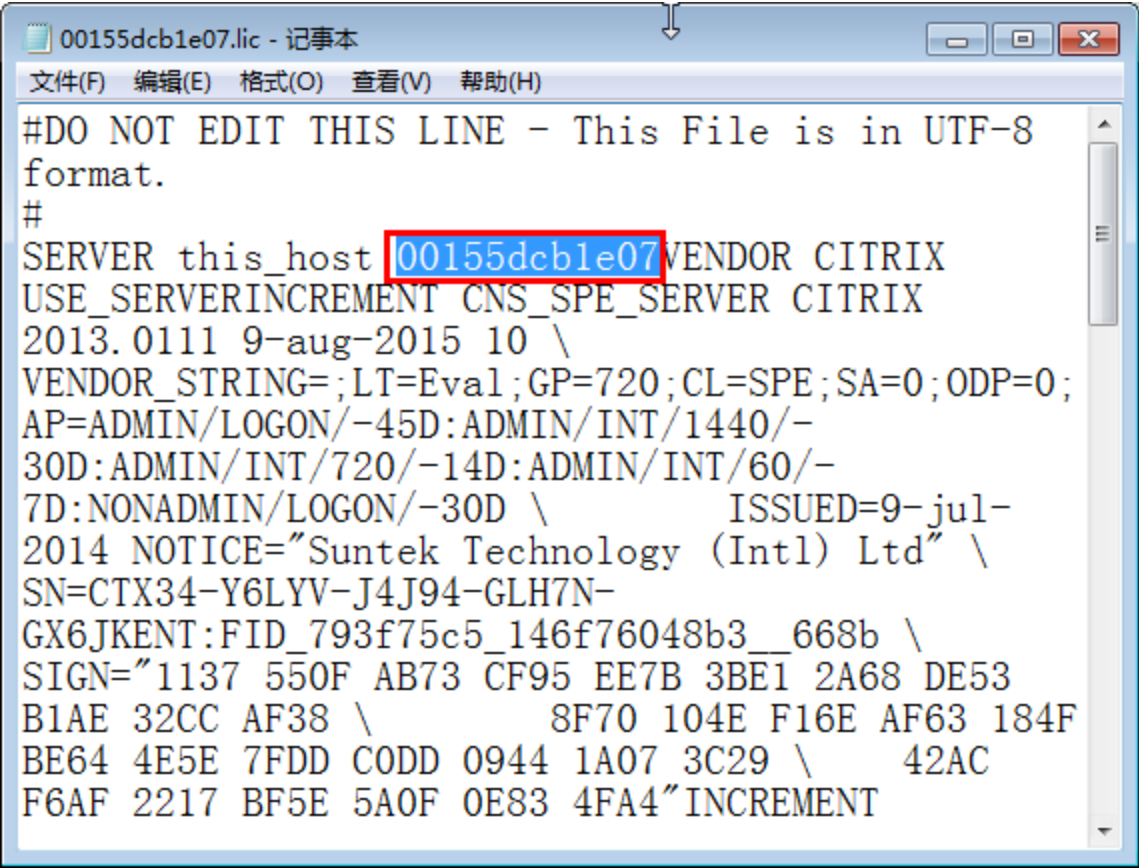



步骤	操作
3.	<p>浏览到你存放 NS VPX 模板的文件夹，选中“NSVPX-XEN-10.1-126.12_nc.”，点击“打开”。</p> 
4.	<p>点击“下一步”</p> 

步骤	操作
5.	<p>点击“下一步”</p> 
6.	<p>点击“导入”</p> 

步骤	操作
7.	<div>点击“下一步”</div> <div></div>
8.	<div>点击“完成”，不要勾选导入后启动 VM (S)</div> <div></div>

步骤	操作										
9.	<p>导入完成后，在 XenCenter 中确认导入的 NetScaler 虚拟机处于关机状态，选择“网络连接”选项卡，点击属性。</p>  <p>The screenshot shows the XenCenter application window. On the left, the 'xenserver-test' server is expanded, and the 'NetScaler Virtual Appliance' is selected and highlighted with a red box. The main pane shows the 'Network Connections' tab for this VM. A table lists the network interfaces:</p> <table><thead><tr><th>设备</th><th>MAC</th><th>限制</th><th>网络</th><th>IP 地址</th></tr></thead><tbody><tr><td>0</td><td>0e:ea:c3:b6:05:d3</td><td></td><td>网络 0</td><td>未知</td></tr></tbody></table> <p>At the bottom of the network connections pane, the '属性(R)' (Properties) button is highlighted with a red box.</p>	设备	MAC	限制	网络	IP 地址	0	0e:ea:c3:b6:05:d3		网络 0	未知
设备	MAC	限制	网络	IP 地址							
0	0e:ea:c3:b6:05:d3		网络 0	未知							
10.	<p>使用记事本打开 NetScaler 许可证文件。</p>  <p>The screenshot shows a file explorer window with the file 'NSVPX-XEN-10.1-126.12_nc.xva' selected. An '打开方式' (Open With) dialog box is open, prompting the user to choose a program to open the file. The dialog lists recommended programs:</p> <ul style="list-style-type: none"><li>Internet Explorer (Microsoft Corporation)</li><li>记事本 (Microsoft Corporation) - This option is highlighted.</li><li>腾讯QQ (Tencent)</li><li>写字板 (Microsoft Corporation)</li></ul> <p>At the bottom of the dialog, there is a checkbox for '始终使用选择的程序打开这种文件(A)' (Always use the selected program to open this type of file) and a '浏览(B)...' (Browse...) button. The '确定' (OK) and '取消' (Cancel) buttons are at the bottom right.</p>										

步骤	操作
11.	<p>将文件中从“SERVER this_host”后面到“VENDOR CITRIX”之间的内容记录下来。本例为了方便测试直接修改 MAC 地址，正常情况请联系贵公司所属总代协调测试 lic</p>  <pre> 00155dcb1e07.lic - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)  #DO NOT EDIT THIS LINE - This File is in UTF-8 format. # SERVER this_host 00155dcb1e07 VENDOR CITRIX USE_SERVERINCREMENT CNS_SPE_SERVER CITRIX 2013.0111 9-aug-2015 10 \ VENDOR_STRING=;LT=Eval;GP=720;CL=SPE;SA=0;ODP=0; AP=ADMIN/LOGON/-45D:ADMIN/INT/1440/- 30D:ADMIN/INT/720/-14D:ADMIN/INT/60/- 7D:NONADMIN/LOGON/-30D \          ISSUED=9-jul- 2014 NOTICE="Suntek Technology (Intl) Ltd" \ SN=CTX34-Y6LYV-J4J94-GLH7N- GX6JKENT:FID_793f75c5_146f76048b3_668b \ SIGN="1137 550F AB73 CF95 EE7B 3BE1 2A68 DE53 B1AE 32CC AF38 \          8F70 104E F16E AF63 184F BE64 4E5E 7FDD C0DD 0944 1A07 3C29 \          42AC F6AF 2217 BF5E 5A0F 0E83 4FA4"INCREMENT           </pre>
12.	<p>在之前打开的虚拟接口属性中选择“使用此 MAC 地址”，将之前记录的内容修改成 MAC 地址格式。此处输入 00:15:5d:cb:1e:07</p>  <p>虚拟接口属性</p> <p>为此虚拟接口选择网络和 MAC 地址。也可以定义 QoS 限制(可选)。</p> <p>网络(N): 网络 0</p> <p>MAC 地址:</p> <p><input type="radio"/> 自动生成 MAC 地址(G)</p> <p><input checked="" type="radio"/> 使用此 MAC 地址(U): 00:15:5d:cb:1e:07</p> <p>QoS 设置:</p> <p><input type="checkbox"/> 启用此项目的 QoS 限制(Q): <input type="text"/> KB/秒</p> <p>确定 取消</p>

步骤

操作

13.

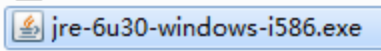
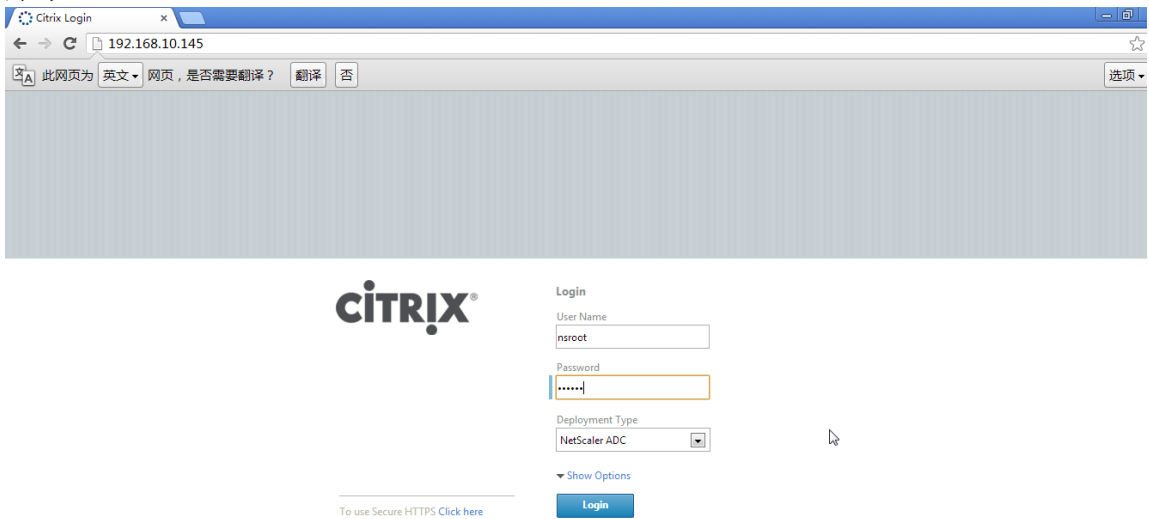
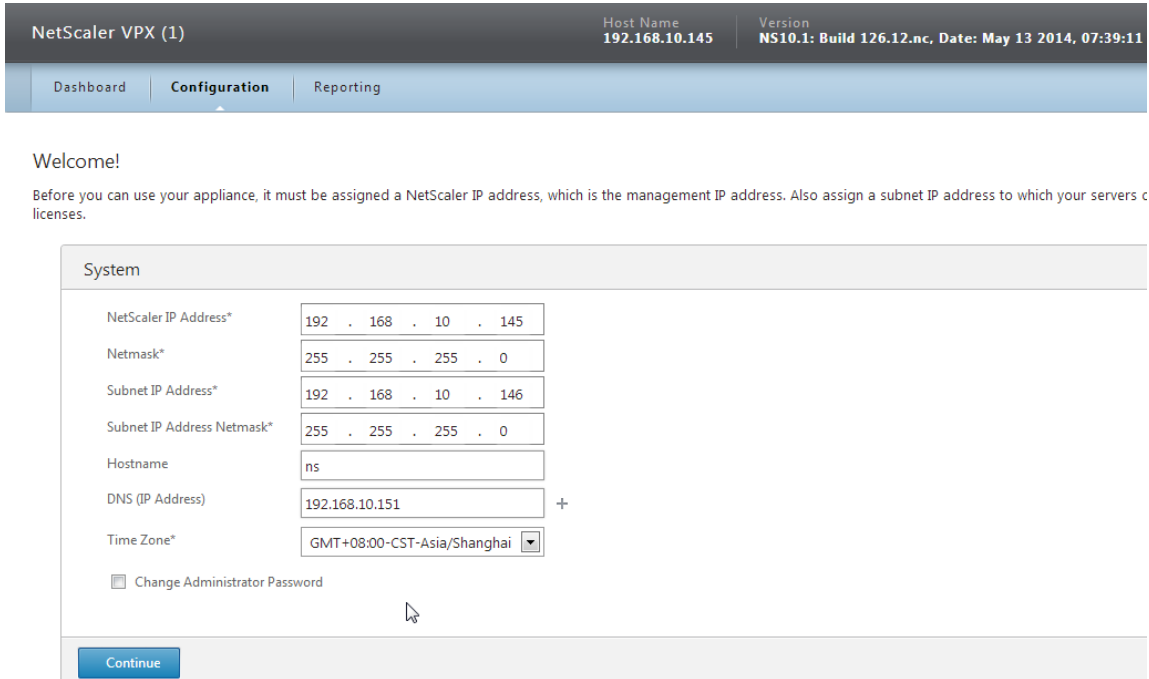
修改完成后，启动 NetScaler VPX。

The screenshot shows the XenCenter application window. On the left, a tree view displays the 'xenserver-test' pool containing several VMs, including 'NetScaler Virtual Appliance'. A right-click context menu is open over this VM, with the '启动' (Start) option highlighted. The main pane on the right shows the configuration for the selected VM, including tabs for '常规' (General), '内存' (Memory), '存储' (Storage), '网络连接' (Network), '控制台' (Console), and '性能' (Performance). The '网络连接' (Network) tab is active, showing a table of virtual network interfaces.

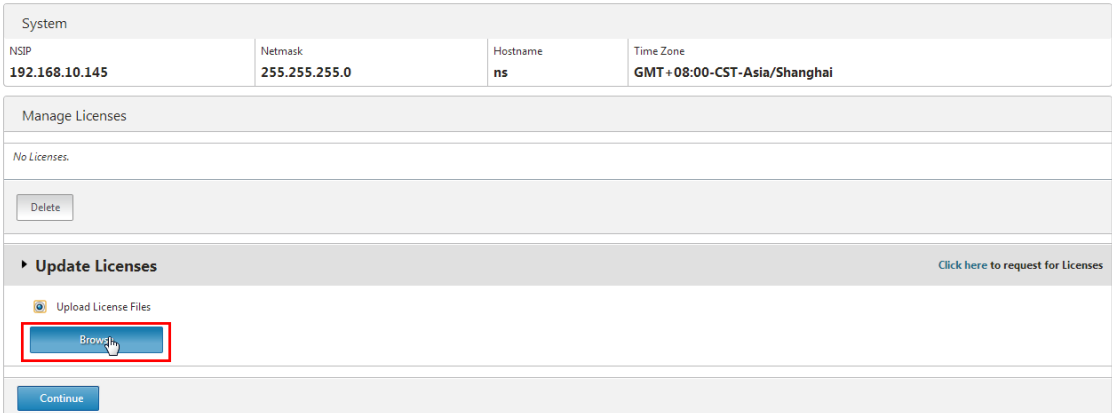
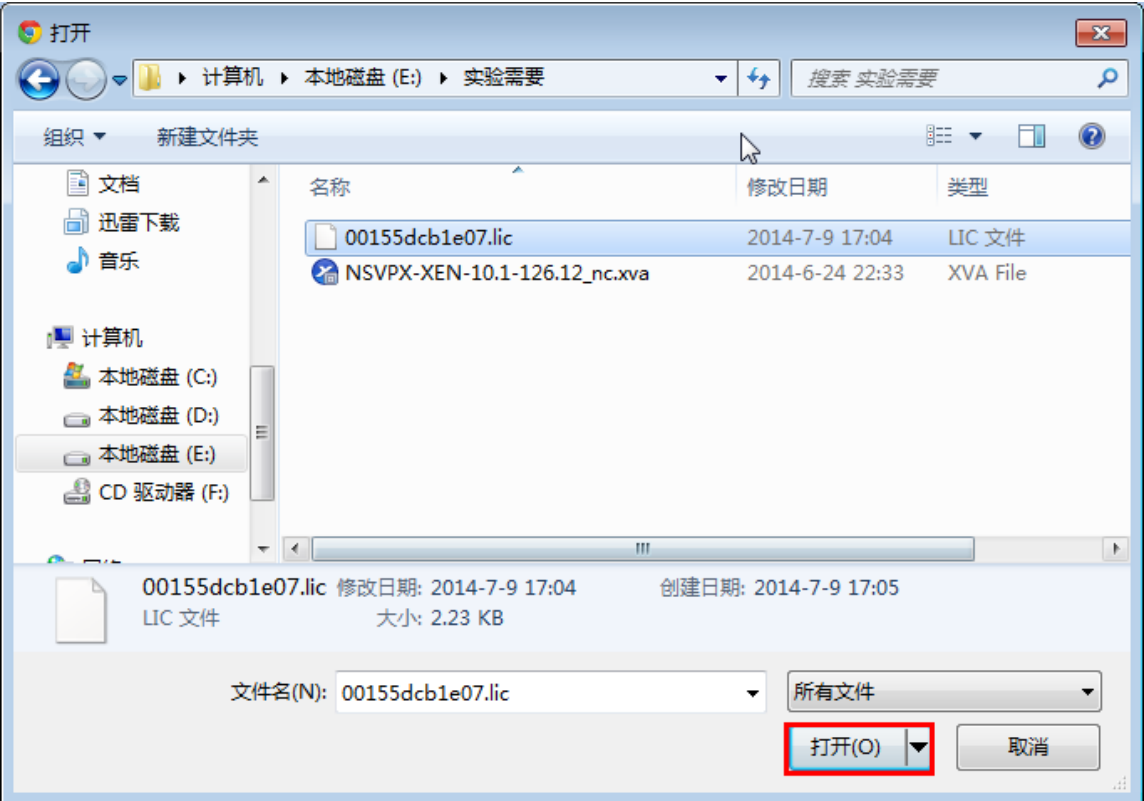
设备	MAC	限制	网络
	00:15:5d:cb:1e:07		网络 0

## 4.2 NetScaler 基础配置

步骤	操作
1.	<p>启动完成后，进入控制台，配置 NetScaler 管理 IP</p> <p>NetScaler's IPv4 address: 192.168.10.145</p> <p>Netmask: 255.255.255.0</p> <p>Gateway IPv4 address: 192.168.10.254</p> <pre> Your identification has been saved in /nsconfig/ssh/ssh_host_rsa_key. Your public key has been saved in /nsconfig/ssh/ssh_host_rsa_key.pub. The key fingerprint is: 86:70:0e:a5:48:73:98:ec:5b:d1:8e:24:d9:e3:07:47 root@ns . Creating ssh2 DSA host key: Generating public/private dsa key pair. Your identification has been saved in /nsconfig/ssh/ssh_host_dsa_key. Your public key has been saved in /nsconfig/ssh/ssh_host_dsa_key.pub. The key fingerprint is: 8f:a2:16:48:25:6b:ca:9c:73:91:7f:9b:42:c2:ba:b0 root@ns . machdep.cpu_idle_hlt: 0 -&gt; 1 Start daemons: syslogd Jul  9 09:19:51 &lt;kern.info&gt; ns syslogd: kernel boot file is /flash/ns-10.1-126.12 inetd cron httpd monit sshd .  !There is no ns.conf in the /nsconfig!  Start Netscaler software tput: no terminal type specified and no TERM environmental variable. Enter NetScaler's IPv4 address []: 192.168.10.145 Enter Netmask []: 255.255.255.0 Enter Gateway IPv4 address []: 192.168.10.254 </pre>
2.	<p>输入 4，保存设置。</p> <pre> !There is no ns.conf in the /nsconfig!  Start Netscaler software tput: no terminal type specified and no TERM environmental variable. Enter NetScaler's IPv4 address []: 192.168.10.145 Enter Netmask []: 255.255.255.0 Enter Gateway IPv4 address []: 192.168.10.254  ----- Netscaler Virtual Appliance Initial Network Address Configuration. This menu allows you to set and modify the initial IPv4 network addresses. The current value is displayed in brackets ([]). Selecting the listed number allows the address to be changed.  After the network changes are saved, you may either login as nsroot and use the Netscaler command line interface, or use a web browser to http://192.168.10.145 to complete or change the Netscaler configuration. -----  1. NetScaler's IPv4 address [192.168.10.145] 2. Netmask [255.255.255.0] 3. Gateway IPv4 address [192.168.10.254] 4. Save and quit Select item (1-4) [4]: 4 </pre>

步骤	操作
3.	<p>在浏览器中输入 NetScaler 管理地址，打开登录页面，输入用户名密码登录。 备注：使用浏览器管理必须提前安装好 JRE，推荐 JRE1.6</p> <p></p> <p>用户名：nsroot 密码：nsroot</p> 
4.	<p>在欢迎页面中的初始化配置向导中输入以下内容：</p> <p>NetScaler IP Address: 192.168.10.145 Netmask: 255.255.255.0 Subnet IP Address: 192.168.10.146 Subnet IP Address Netmask: 255.255.255.0 Hostname: ns DNS:192.168.10.151 #AD 域控的 IP 地址 TimeZone 选择 “GMT +08:00-CST-Asia/Shanghai” 点击 “Continue”</p> 

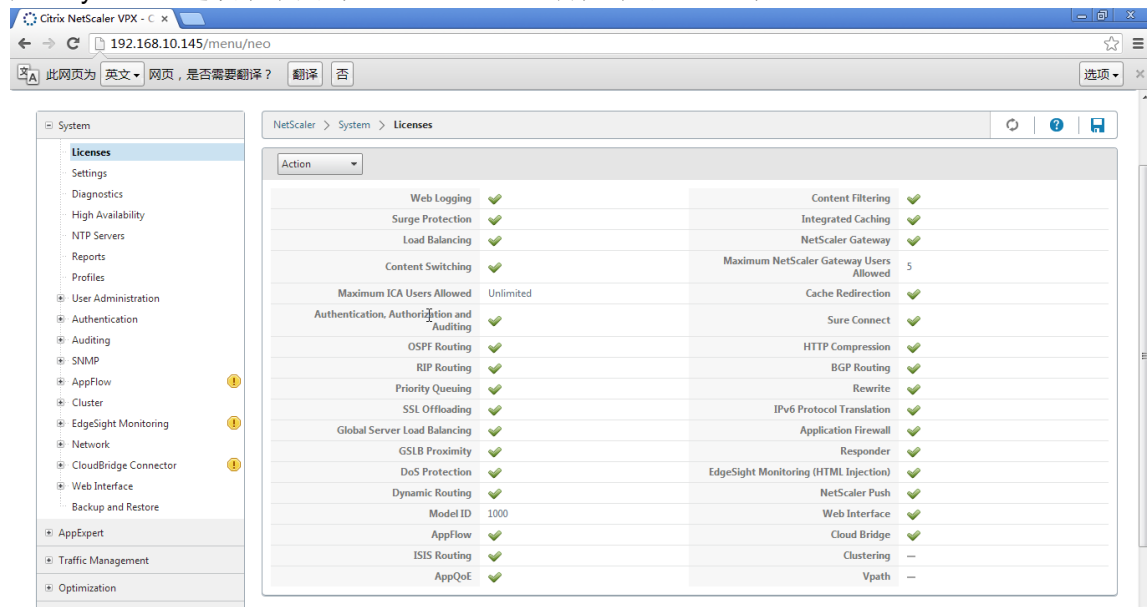


步骤	操作
5.	<p>点击 “Browse”</p> <p>Welcome!</p> <p>Before you can use your appliance, it must be assigned a NetScaler IP address, which is the management IP address. Also assign a subnet IP address to which your servers can connect, and allocate or upload your licenses.</p>  <p>The screenshot shows the NetScaler configuration interface. Under the 'Manage Licenses' section, there is a 'No Licenses' message and a 'Delete' button. Below that, the 'Update Licenses' section is expanded, showing an 'Upload License Files' option with a 'Browse...' button highlighted by a red rectangle. A 'Continue' button is also visible at the bottom of the section.</p>
6.	<p>浏览到保存许可证文件的文件夹中，选择许可证文件，点击 “打开”</p>  <p>The screenshot shows a Windows File Explorer window titled '打开' (Open). The address bar shows the path '计算机 &gt; 本地磁盘 (E:) &gt; 实验需要'. The left sidebar shows the '本地磁盘 (E:)' selected. The main pane displays a list of files: '00155dcb1e07.lic' (LIC 文件, 2.23 KB) and 'NSVPX-XEN-10.1-126.12_nc.xva' (XVA File). The '00155dcb1e07.lic' file is selected. At the bottom, the '文件名(N):' field contains '00155dcb1e07.lic', and the '打开(O)' button is highlighted with a red rectangle.</p>

步骤	操作								
7.	<div>点击 “Continue”</div> <div><p>Welcome!</p><p>Before you can use your appliance, it must be assigned a NetScaler IP address, which is the management IP address. Also assign a subnet IP address to which your server licenses.</p><div><div>System</div><table><tr><td>NSIP</td><td>Netmask</td><td>Hostname</td><td>Time Zone</td></tr><tr><td>192.168.10.145</td><td>255.255.255.0</td><td>ns</td><td>GMT +08:00-CST-Asia/Shanghai</td></tr></table></div><div><div>Manage Licenses</div><div><div><input type="checkbox"/> 00155dcb1e07.lic</div><div>Delete</div></div><div><div>► Update Licenses</div><div><div> Upload License Files</div><div>Browse</div></div></div><div>Continue</div></div></div>	NSIP	Netmask	Hostname	Time Zone	192.168.10.145	255.255.255.0	ns	GMT +08:00-CST-Asia/Shanghai
NSIP	Netmask	Hostname	Time Zone						
192.168.10.145	255.255.255.0	ns	GMT +08:00-CST-Asia/Shanghai						
8.	<div>点击 “Done”，重启 NetScaler</div> <div><div><div>NetScaler VPX (1000)</div><div>Host Name 192.168.10.145</div><div>Version NS10.1: Build 126.12.nc, Date: May 13 2014, 07:39:11</div><div>User nsroot</div><div>Logout</div><div>CITRIX®</div></div><div><div>Dashboard</div><div>Configuration</div><div>Reporting</div><div>Documentation</div><div>Downloads</div><div>⚙</div></div><div><p>Welcome!</p><p>Before you can use your appliance, it must be assigned a NetScaler IP address, which is the management IP address. Also assign a subnet IP address to which your servers can connect, and allocate or upload your licenses.</p><div><div>System</div><table><tr><td>NSIP</td><td>Netmask</td><td>Hostname</td><td>Time Zone</td></tr><tr><td>192.168.10.145</td><td>255.255.255.0</td><td>ns</td><td>GMT +08:00-CST-Asia/Shanghai</td></tr></table></div><div><div>Manage Licenses</div><div><div><input type="checkbox"/> 00155dcb1e07.lic</div><div>Delete</div></div></div><div>Done</div></div></div>	NSIP	Netmask	Hostname	Time Zone	192.168.10.145	255.255.255.0	ns	GMT +08:00-CST-Asia/Shanghai
NSIP	Netmask	Hostname	Time Zone						
192.168.10.145	255.255.255.0	ns	GMT +08:00-CST-Asia/Shanghai						

步骤 操作

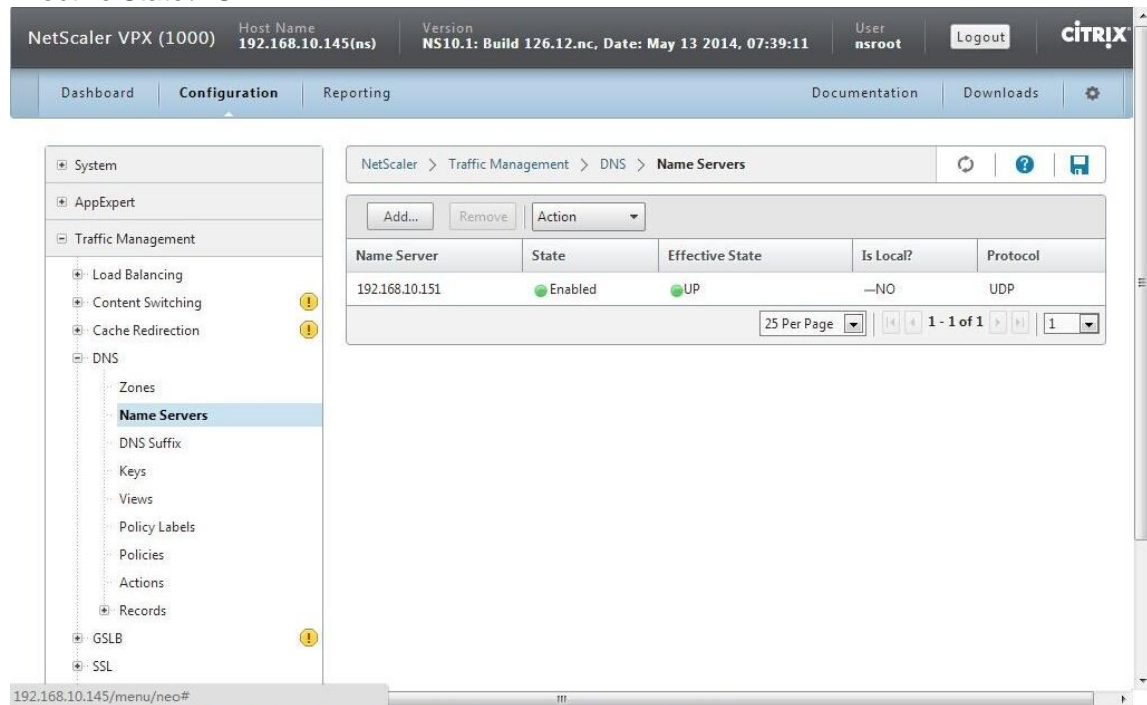
9. 重启后再次登录 NetScaler  
在“System”选项卡中点击“Licenses”，确认许可证已生效。



10. 在“Traffic Management”选项卡中选择“DNS” -> “Name Servers”。在右侧的窗口中确认 DNS 服务器状态正常。

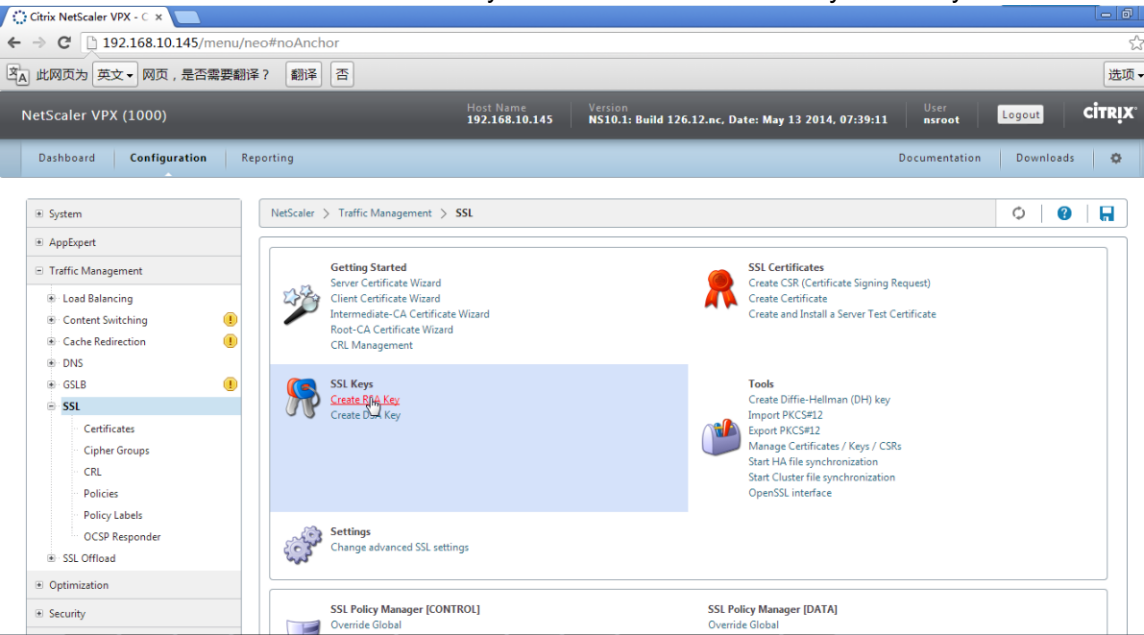
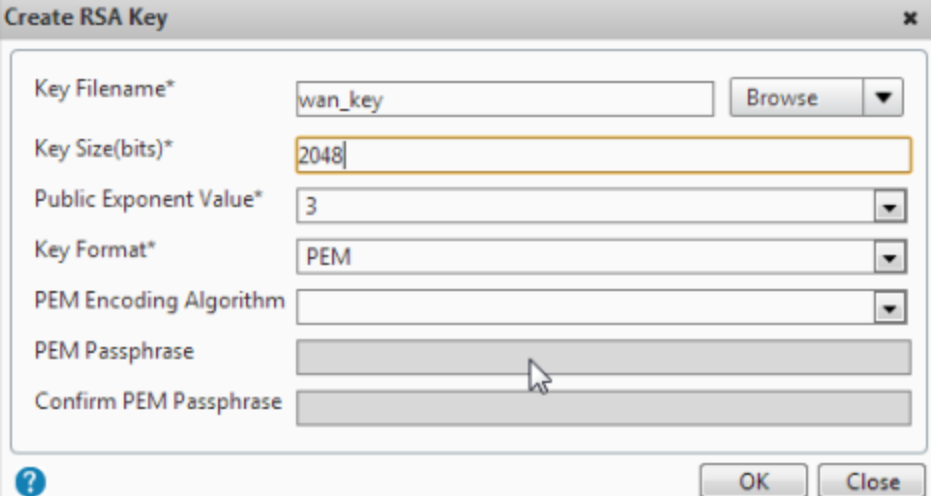
State: Enabled

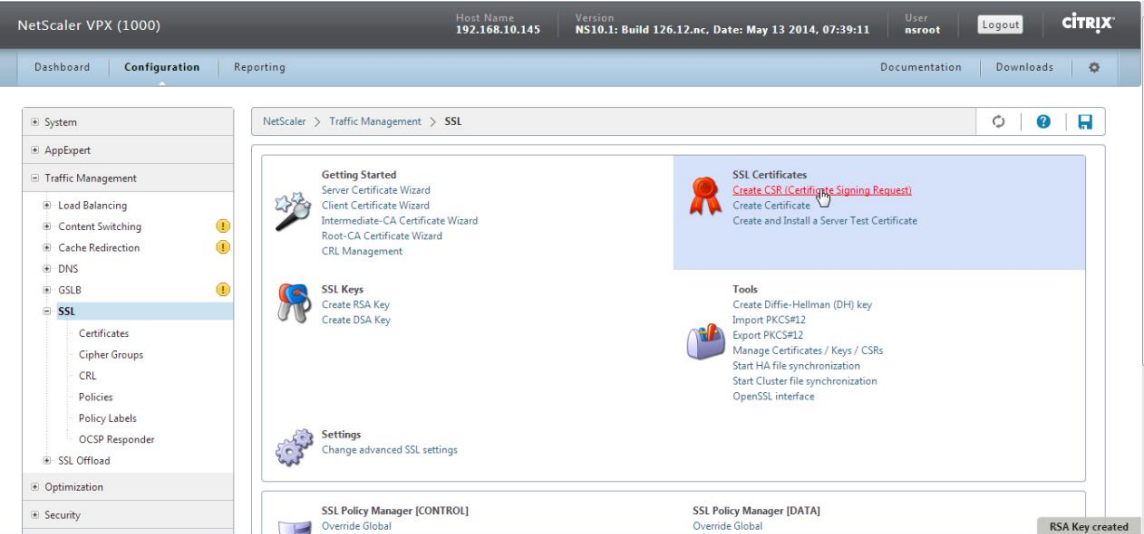
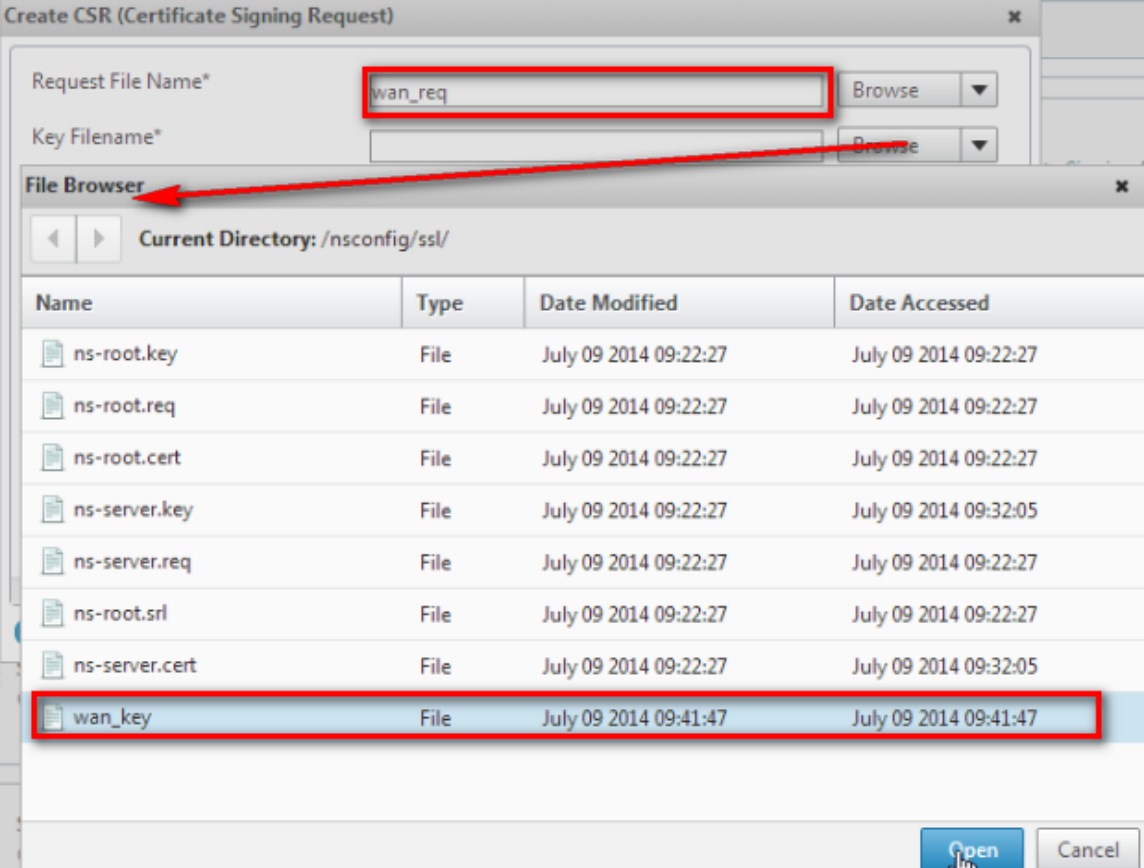
Effective State: UP

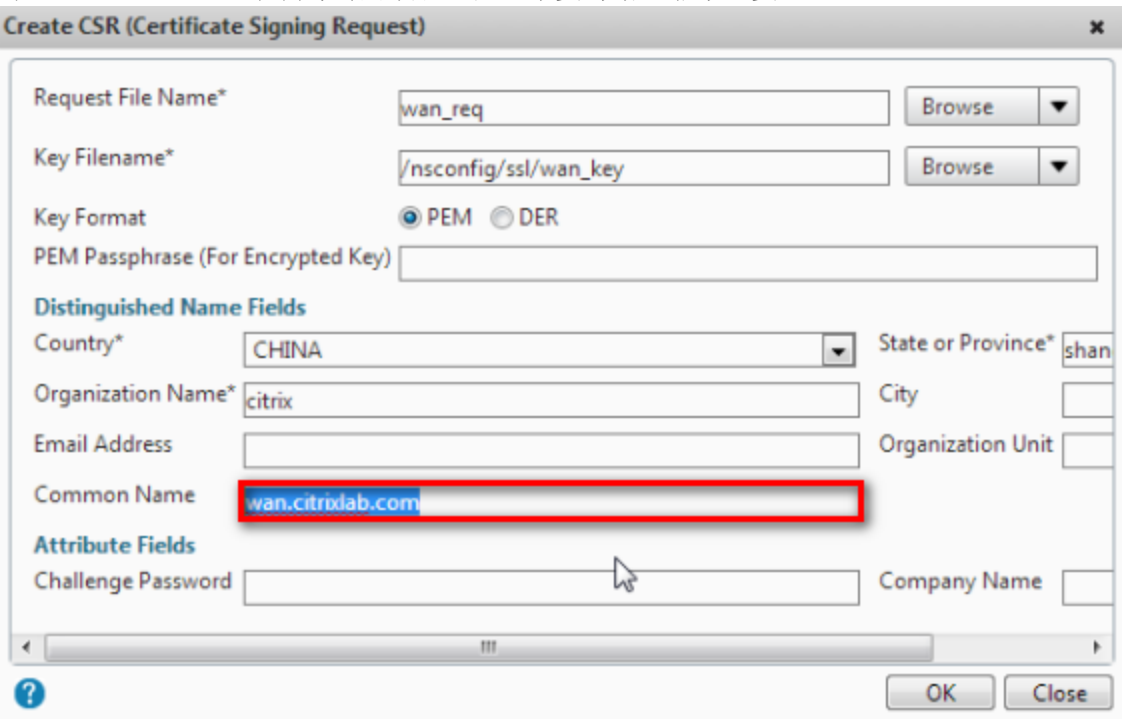
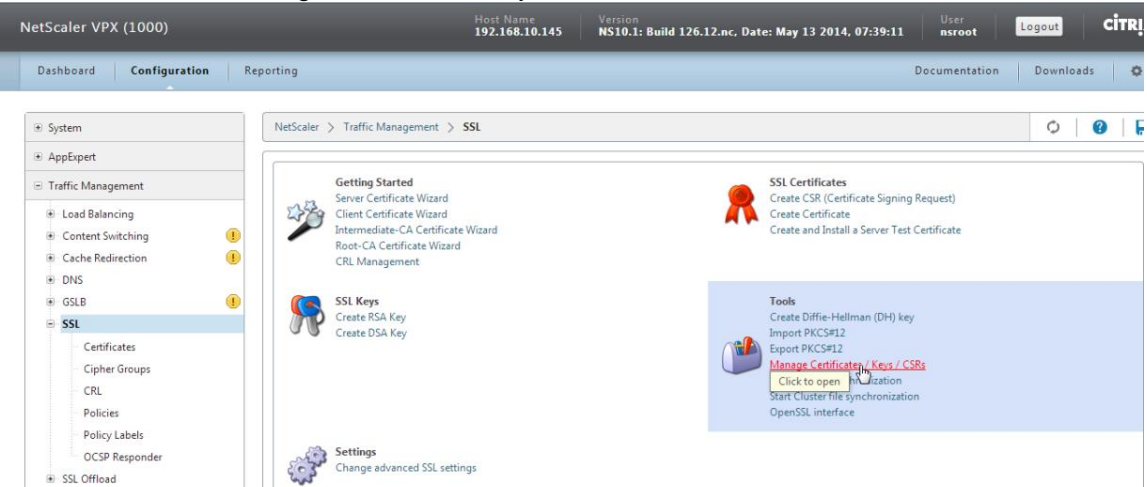


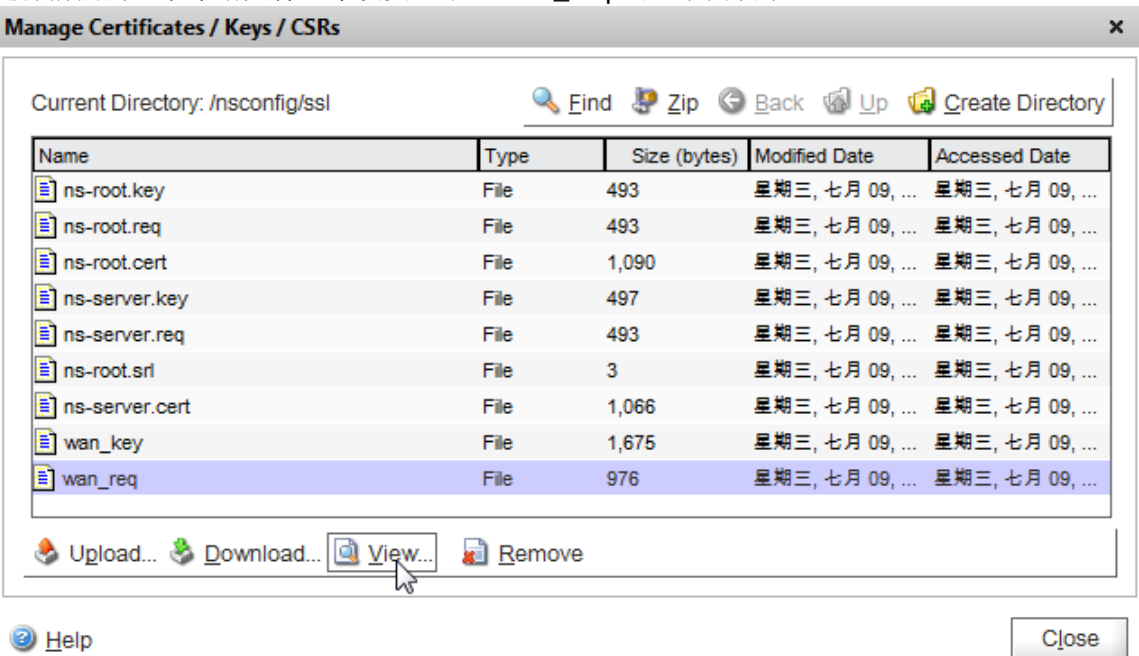

## 4.3 NetScaler 服务器证书申请及安装


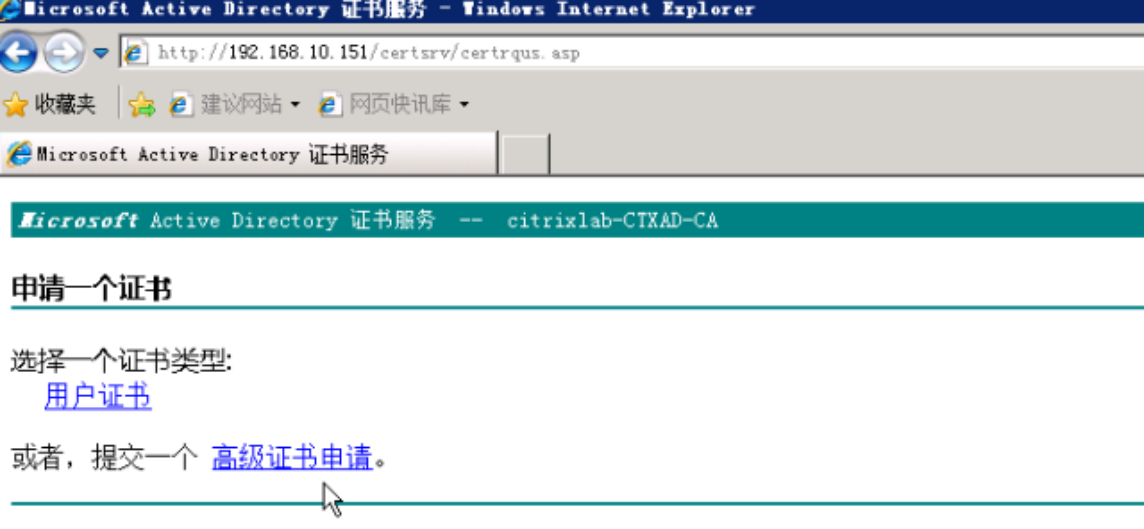
### 4.3.1 NetScaler 服务器证书申请

步骤	操作
1.	<p>在 VPX 上，进入 SSL 界面，在 SSL Keys 下，点击“Create RSA key”申请 Key</p> 
2.	<p>输入证书名，本次实验输入证书名为 wan_key，然后输入 Key 的大小：2048，点击“OK”</p> 

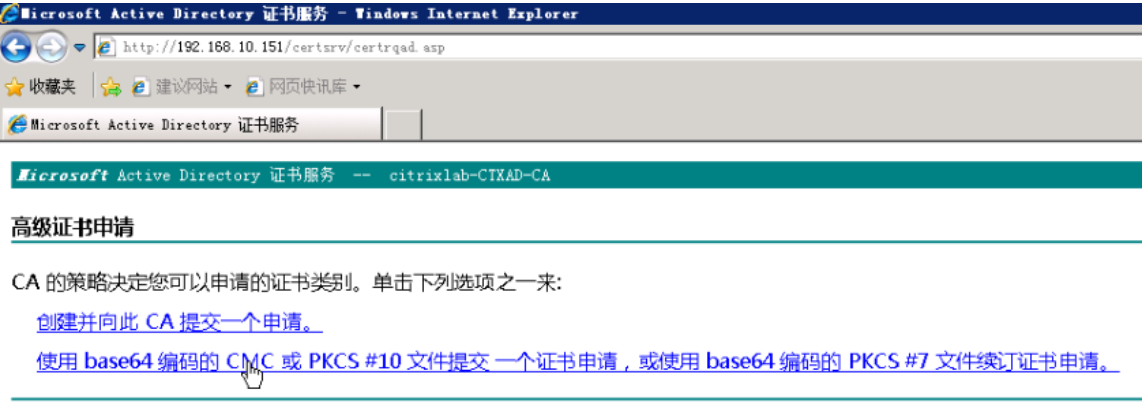

步骤	操作
3.	<p>点击 SSL Certificates 下的“Create CSR (Certificate Signing Request)”申请证书</p> 
4.	<p>输入相应的 Request File Name, 本次 POC 输入“wan_req”, 在 Key Filename 中, 点击“browse”, 在显示的文件列表中选中我们前面申请的 key 文件, 本次实验中对的是 wan_key, 并点击 open</p> 

步骤	操作
5.	<p>在 Common Name 中填写公网域名，注意不要写错（非常重要）</p> 
6.	<p>在 Tools 中，选择 Manage Certificates/Keys/CSRs</p> 

步骤	操作
7.	<p>选择前面的证书申请文件，本次实验中是 wan_req，点击下方的“View”</p>  <p>Help Close</p>
8.	<p>全选所有内容，复制</p>  <p>Help Save Close</p>

步骤	操作
9.	<p>如果能申请三方机构的受信任证书, 请将前序生成的 request file 提交给三方购买证书证书。本例中, 直接使用 AD 的 CA 来签发一张自信任证书。</p> <p>在浏览器中, 打开证书服务器地址 <a href="http://192.168.10.151/certsrv/">http://192.168.10.151/certsrv/</a>, 点击“申请证书”。</p> <p>注意, 必须使用域管理员登录才能申请证书。</p> 
10.	<p>点击“高级证书申请”</p> 



步骤	操作
11.	<p>选择“使用 base64 编码的 CMC 或 PKCS#10 文件提交一个证书申请，或使用 base64 编码的 PKCS#7 文件续订证书申请”</p> 
12.	<p>在“保存的申请”中，将前面复制的申请文件内容粘贴进来，在“证书模板”中选择“Web 服务器”，点击“提交”</p> 

步骤	操作
13.	<p>选择“Base 64 编码”，点击“下载证书”</p> 
14.	<p>选择一个保存的证书名，本次实验保存为 wan</p> 

步骤

操作

15. 点击 “Upload...” 上传证书

The screenshot shows a web-based interface titled "Manage Certificates / Keys / CSRs". At the top, it indicates the "Current Directory: /nsconfig/ssl". Below this is a table listing files in the directory. The file "wan\_req" is selected, highlighted in blue. At the bottom of the window, there are buttons for "Upload...", "Download...", "View...", and "Remove". A mouse cursor is pointing at the "Upload..." button. The interface also includes a search bar, navigation buttons (Find, Zip, Back, Up, Create Directory), and a "Help" button.

Name	Type	Size (bytes)	Modified Date	Accessed Date
ns-root.key	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.req	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.cert	File	1,090	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.key	File	497	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.req	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.srl	File	3	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.cert	File	1,066	星期三, 七月 09, ...	星期三, 七月 09, ...
wan_key	File	1,675	星期三, 七月 09, ...	星期三, 七月 09, ...
wan_req	File	976	星期三, 七月 09, ...	星期三, 七月 09, ...

16. 选择刚才生成的证书文件，本次实验生成的证书文件为 wan.cer，点击 “Select”

The screenshot shows a "Select Files" dialog box. The "Look in" dropdown is set to "Desktop". The file list contains several files, with "wan.cer" selected and highlighted in blue. At the bottom of the dialog, there are buttons for "Select" and "取消" (Cancel). A mouse cursor is pointing at the "Select" button. The dialog also includes a search bar and a "File name" field.

File Name	File Type
SF HA IB.docx	File
wan.cer	File
WIFI共享精灵.lnk	File
XenApp and XenDesktop 7.5 (Visio 2013).vssx	File
xenapp-ie.vbs	File
XXX软件列表.xls	File
【工作】职场电子邮件礼仪.pdf	File

步骤

操作

17. 可以看到，证书文件已经上传成功

The screenshot shows a web interface titled "Manage Certificates / Keys / CSRs". The current directory is "/nsconfig/ssl". At the top, there are navigation buttons: Find, Zip, Back, Up, and Create Directory. Below this is a table with columns: Name, Type, Size (bytes), Modified Date, and Accessed Date. The file "wan.cer" is highlighted in blue. Below the table are buttons for Upload, Download, View, and Remove. At the bottom left is a Help button, and at the bottom right is a Close button.

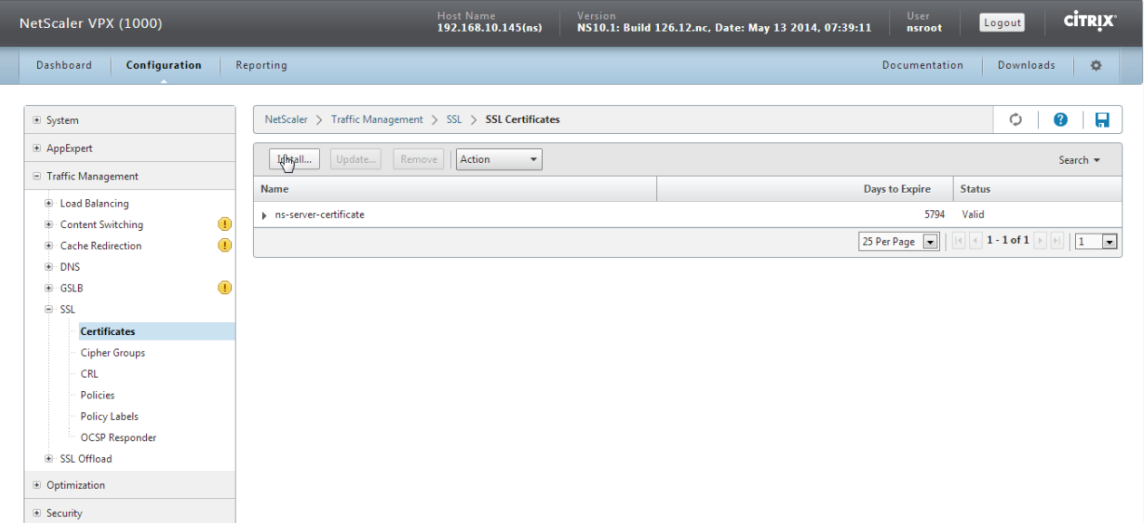
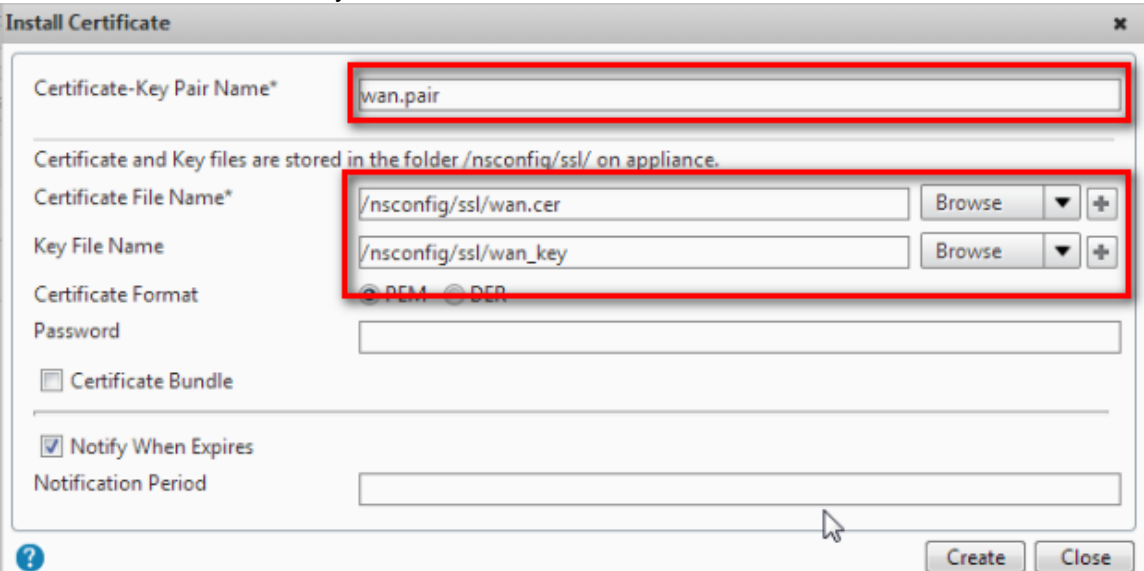
Name	Type	Size (bytes)	Modified Date	Accessed Date
ns-root.key	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.req	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.cert	File	1,090	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.key	File	497	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.req	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.srl	File	3	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.cert	File	1,066	星期三, 七月 09, ...	星期三, 七月 09, ...
wan_key	File	1,675	星期三, 七月 09, ...	星期三, 七月 09, ...
wan_req	File	976	星期三, 七月 09, ...	星期三, 七月 09, ...
wan.cer	File	1,930	星期三, 七月 09, ...	星期三, 七月 09, ...

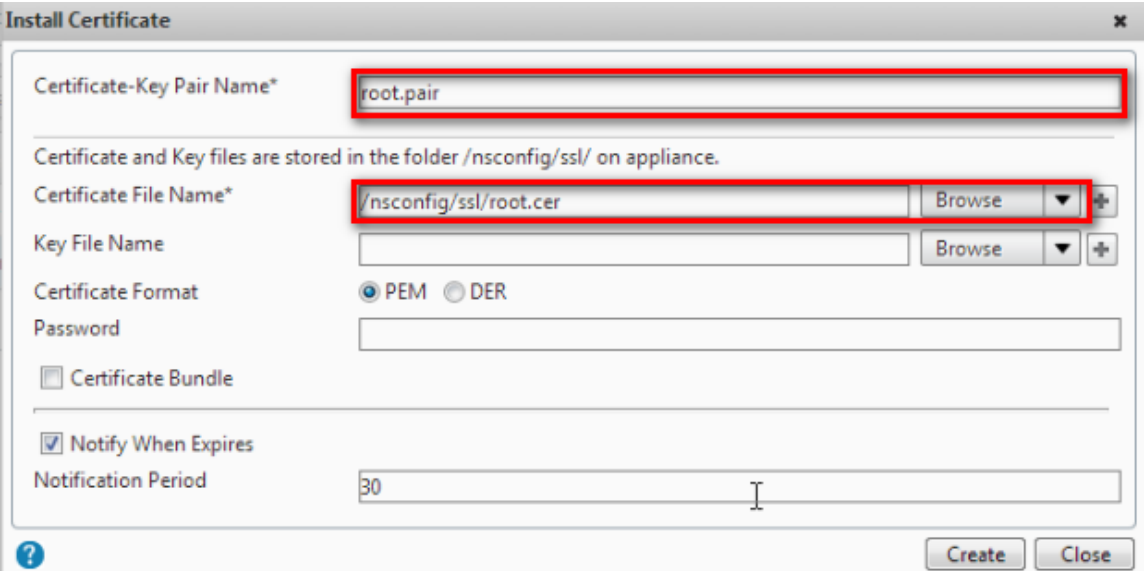
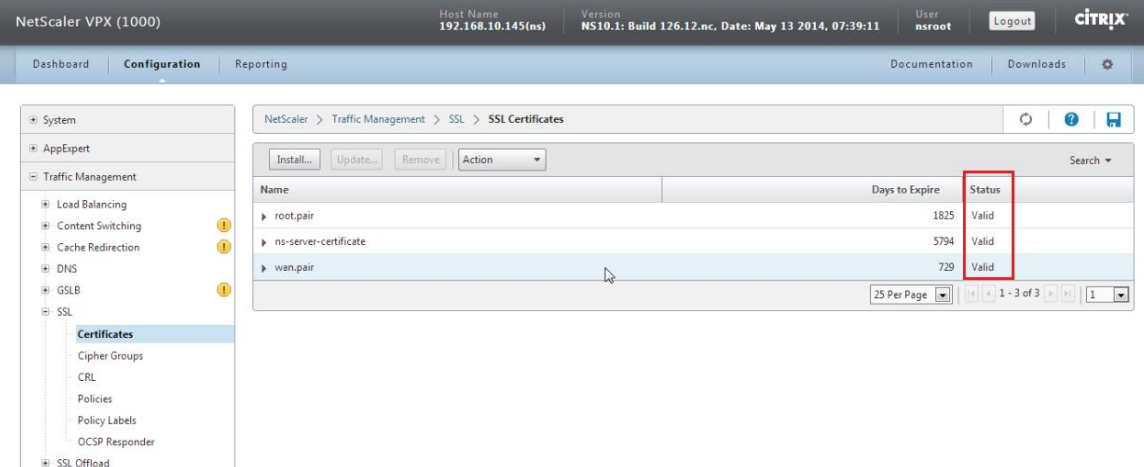
18. 同时将此 AD 的根证书 root.cer 也上传到 VPX，确保 NetScaler 与 StoreFront 通信时证书的相互信任。完成后点击 close

The screenshot shows the same web interface as step 17. The file "root.cer" is now highlighted in blue. The "View" button is now labeled "root.cer".

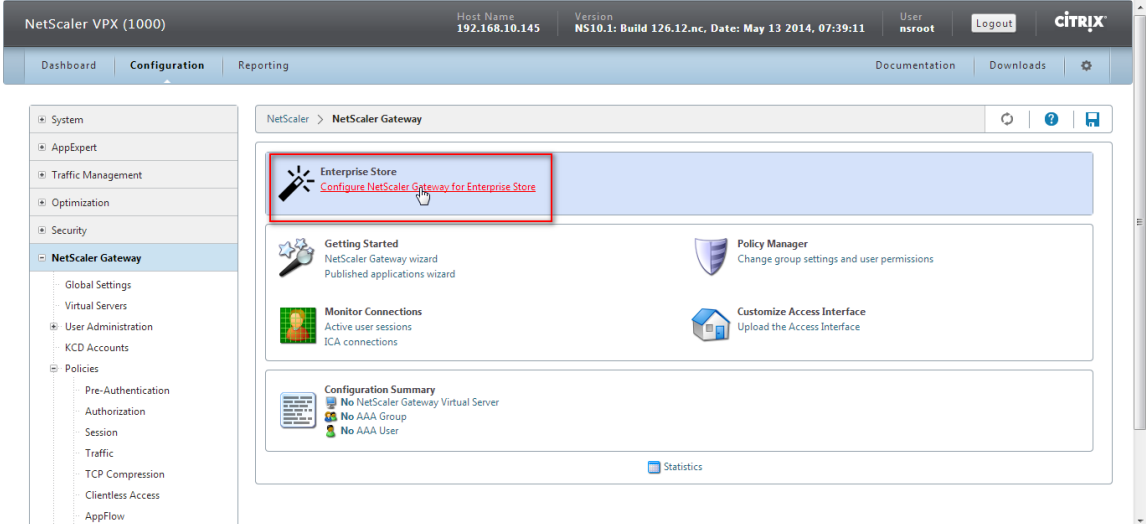
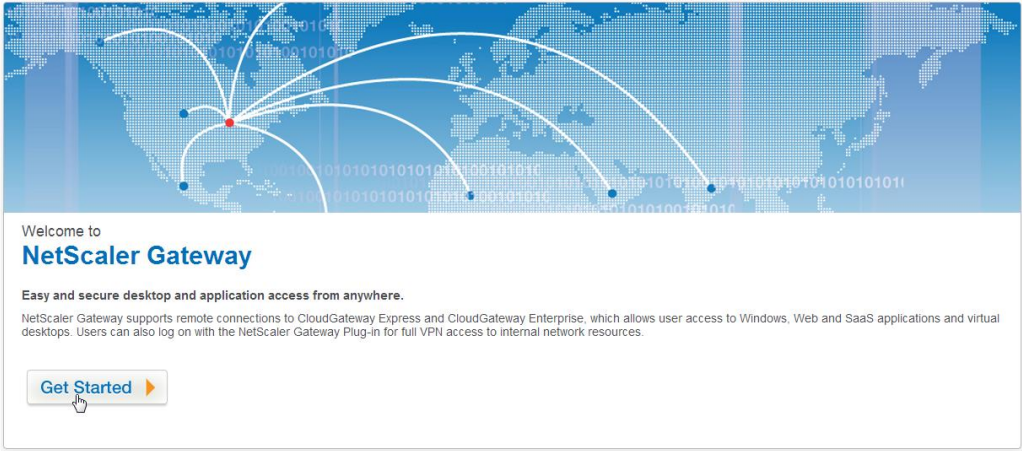
Name	Type	Size (bytes)	Modified Date	Accessed Date
ns-root.req	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.cert	File	1,090	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.key	File	497	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.req	File	493	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-root.srl	File	3	星期三, 七月 09, ...	星期三, 七月 09, ...
ns-server.cert	File	1,066	星期三, 七月 09, ...	星期三, 七月 09, ...
wan_key	File	1,675	星期三, 七月 09, ...	星期三, 七月 09, ...
wan_req	File	976	星期三, 七月 09, ...	星期三, 七月 09, ...
wan.cer	File	1,930	星期三, 七月 09, ...	星期三, 七月 09, ...
root.cer	File	1,286	星期三, 七月 09, ...	星期三, 七月 09, ...

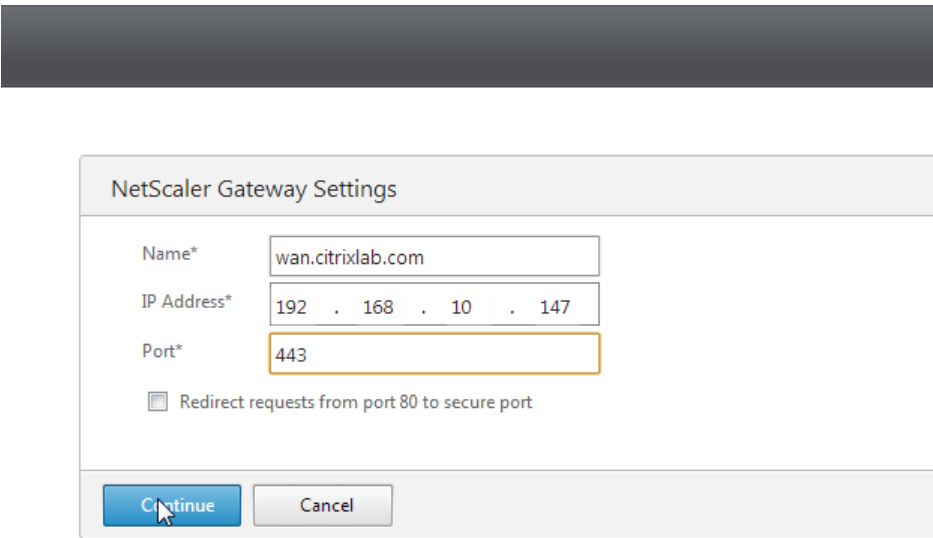
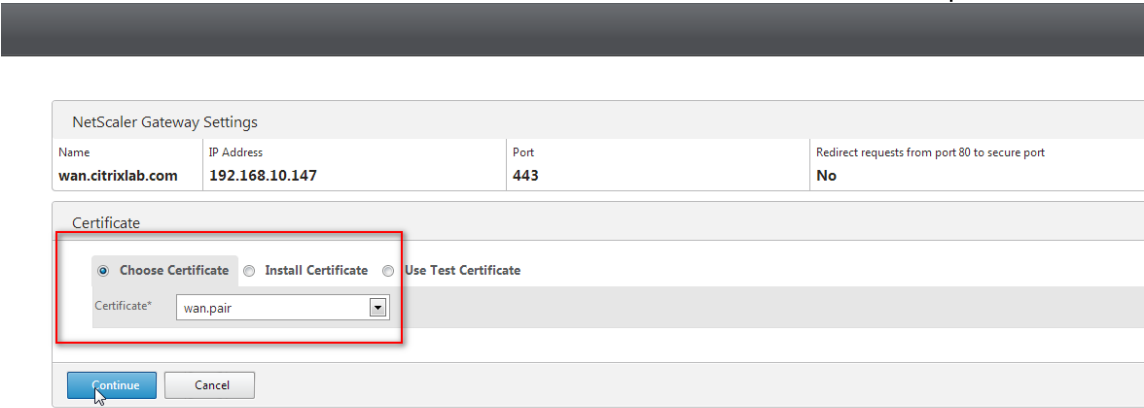
### 4.3.2 NetScaler 服务器证书安装

步骤	操作
1.	<p>在 SSL, Certificates 中, 点击"Install..."</p> 
2.	<p>在 Certificate-Key Pair Name*中, 填写一个证书匹配名, 本次实验匹配名为 wan.pair, 在 Certificate File Name*和 Key File Name, 选择"Brower", 选择相对应的文件位置</p> 

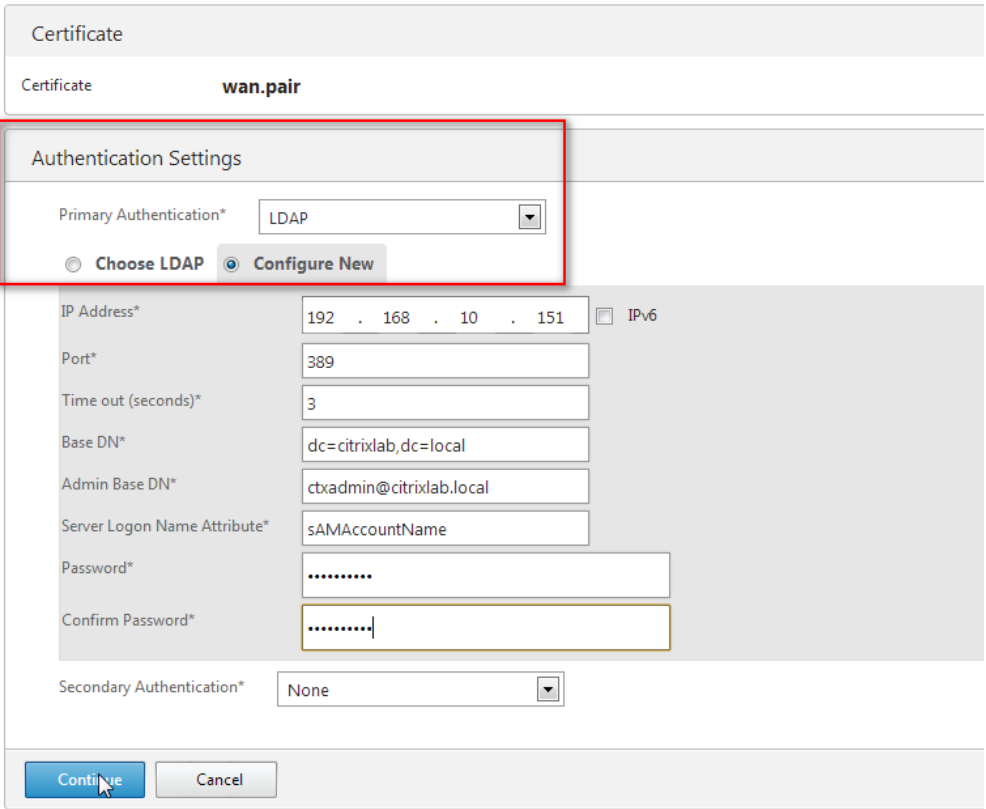
步骤	操作
3.	<p>同样方法安装根证书，输入证书匹配名，和选择证书文件名 注意，root 证书不需要选择 Key File Name</p> 
4.	<p>在 SSL-Certificates 中，可以看到前面添加的两个证书的匹配名已经罗列其中，Status 下面状态为 Valid, 说明证书已经生效</p> 

## 4.4 NetScaler Gateway 配置向导

步骤	操作
1.	<p>打开 NetScaler Gateway，点击右边的“Enterprise Store，Configure NetScaler Gateway for Enterprise Store”</p> 
2.	<p>点击 Get Started</p> 

步骤	操作
3.	<p>在 NetScaler Gateway Settings 中输入以下信息，continue</p> <p>Name: wan.citrixlab.com</p> <p>IP Address: 192.168.10.147      #NetScaler VIP 的地址</p> <p>Port: 443</p> 
4.	<p>点击 Choose Certificate，在 Certificate 下拉菜单中，选择导入的证书，wan.pair，continue</p> 



步骤	操作
5.	<p>Authentication Settings 设置:            Primary Authentication: LDAP            点击 Configure New            Configure New 设置            IP Address: 192.168.10.151      #AD 域控地址            Port: 389            Time out: 3            Base DN: dc=citrixlab,dc=local            Admin Base DN: <a href="#">ctxadmin@citrixlab.local</a>            Server Logon Name Attribute: sAMAccountName            Password: *****      #ctxadmin 的密码            检查无误后, 点击 continue</p> 

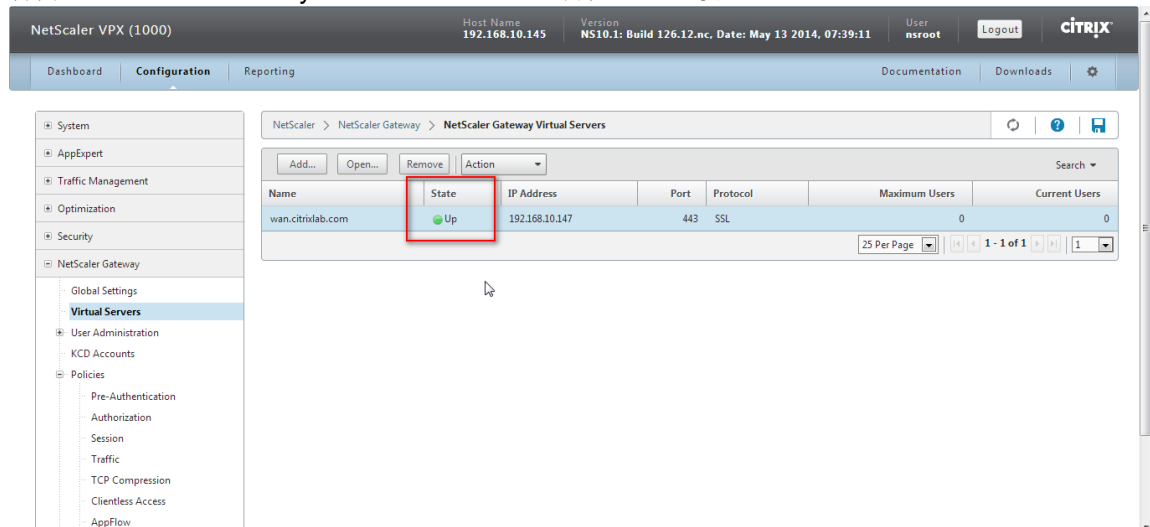
步骤	操作
6.	<div><div>Enterprise Store Settings 设置: 选择 XenApp/XenDesktop Deployment Type: 下拉菜单中选择 StoreFront StoreFrontFQDN: CTXDDC.citrixlab.local #注意必须填写完整 Use HTTPS: 勾选 #注意必须填写完整 Receiver for Web Path: /Citrix/StoreWeb #填写域名 Single Sign-on Domain: citrixlab #填写 CTXDDC 的 IP 地址 STA URL: <a href="http://192.168.10.152">http://192.168.10.152</a> 检查无误后, 点 done 请确保 StoreFront 服务器启用 https 服务, 参考 《PoC 手册 - 1 基础环境 - Lab 06 StoreFront 配置 v1.0》第 2 章 StorFront HTTPS 配置</div><div><div>Certificate</div><div>Certificate wan.pair</div><div>Authentication Settings</div><div>Primary Authentication - LDAP 192.168.10.151_LDAP_pol</div><div><div>Enterprise Store Settings</div><div><div>XenMobile XenApp / XenDesktop</div><div>Deployment Type* StoreFront</div><div>StoreFront FQDN* CTXDDC.citrixlab.local</div><div><input checked="" type="checkbox"/> Use HTTPS</div><div>Receiver for Web Path* /Citrix/StoreWeb</div><div>Single Sign-on Domain* citrixlab</div><div>STA URL* http://192.168.10.152</div></div><div><div>Done</div><div>Cancel</div></div></div></div></div>

步骤

操作

7.

打开 NetScaler Gateway, Virtual Servers, 确认 State 状态是 UP



NetScaler VPX (1000) Host Name: 192.168.10.145 Version: NS10.1: Build 126.12.nc, Date: May 13 2014, 07:39:11 User: nsroot Logout

Dashboard Configuration Reporting Documentation Downloads

System AppExpert Traffic Management Optimization Security NetScaler Gateway

Global Settings Virtual Servers User Administration KCD Accounts Policies Pre-Authentication Authorization Session Traffic TCP Compression Clientless Access AppFlow

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

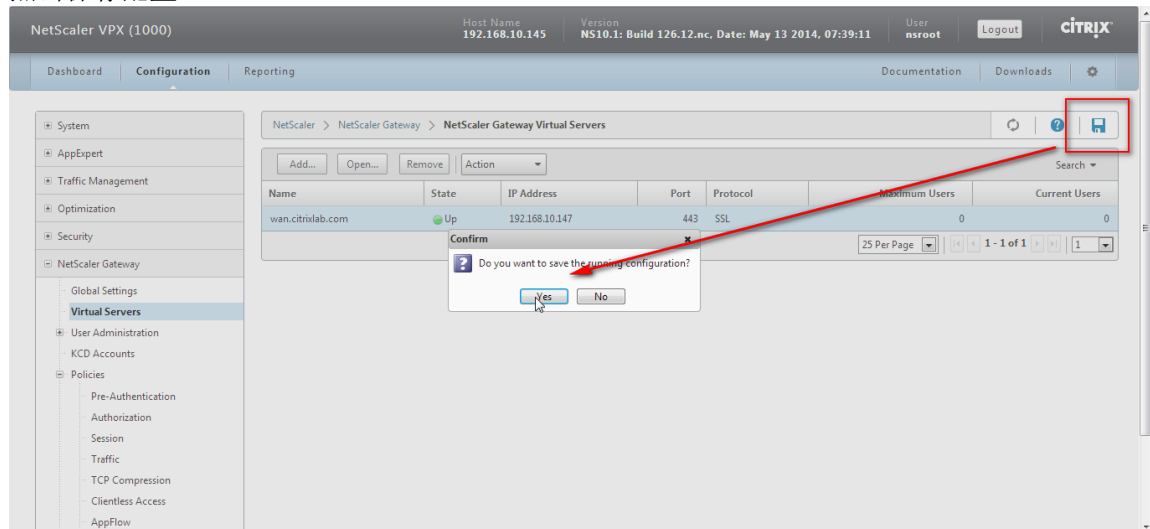
Add... Open... Remove Action Search

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
wan.citrixlab.com	Up	192.168.10.147	443	SSL	0	0

25 Per Page 1 - 1 of 1 1

8.

点击保存配置



NetScaler VPX (1000) Host Name: 192.168.10.145 Version: NS10.1: Build 126.12.nc, Date: May 13 2014, 07:39:11 User: nsroot Logout

Dashboard Configuration Reporting Documentation Downloads

System AppExpert Traffic Management Optimization Security NetScaler Gateway

Global Settings Virtual Servers User Administration KCD Accounts Policies Pre-Authentication Authorization Session Traffic TCP Compression Clientless Access AppFlow

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Add... Open... Remove Action Search

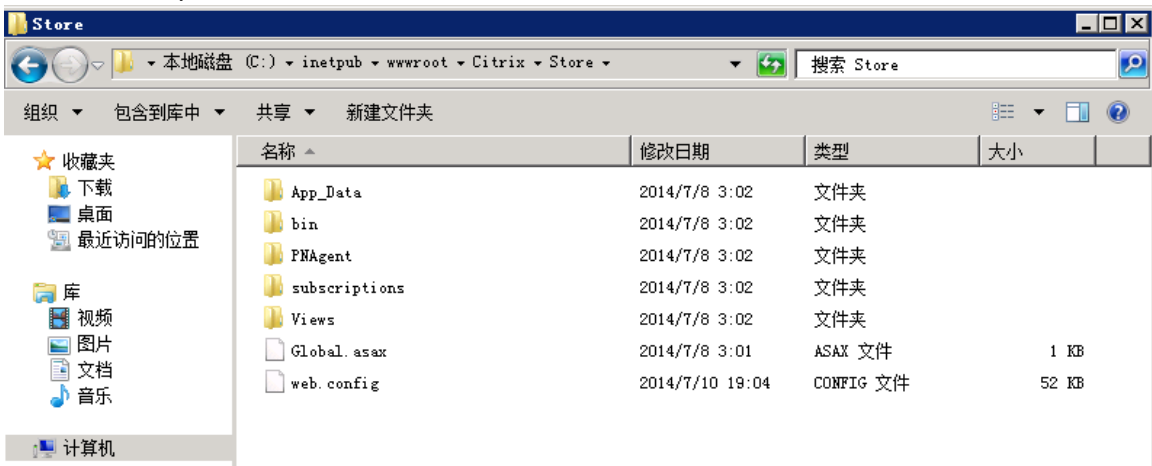
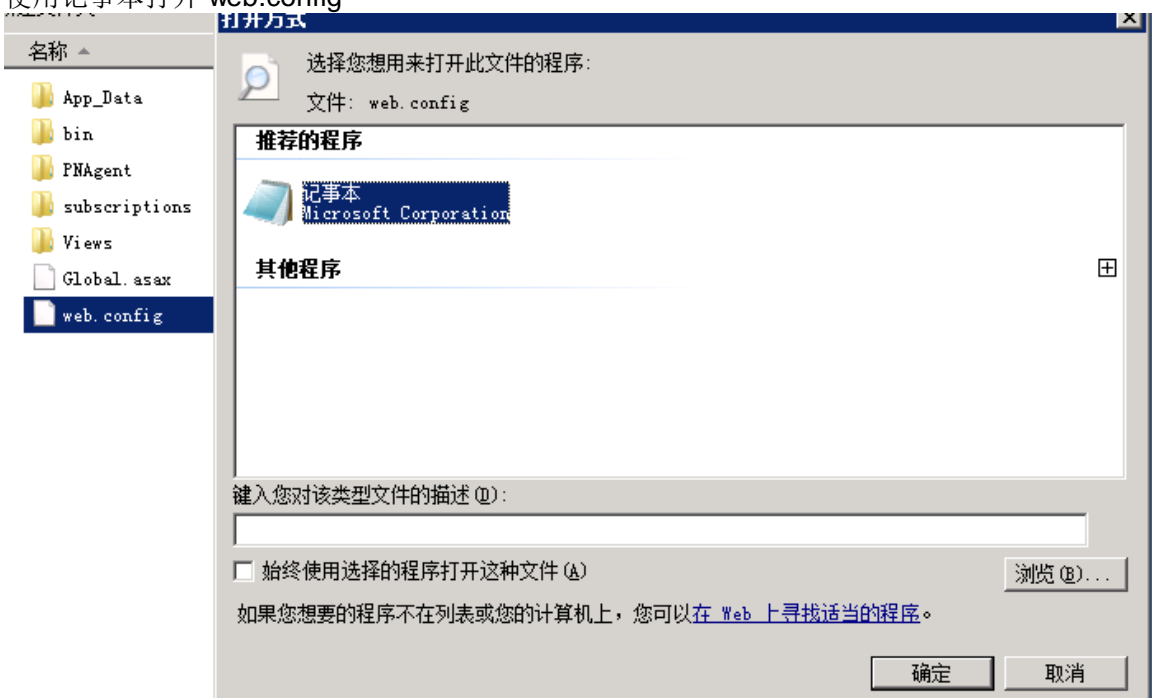
Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
wan.citrixlab.com	Up	192.168.10.147	443	SSL	0	0

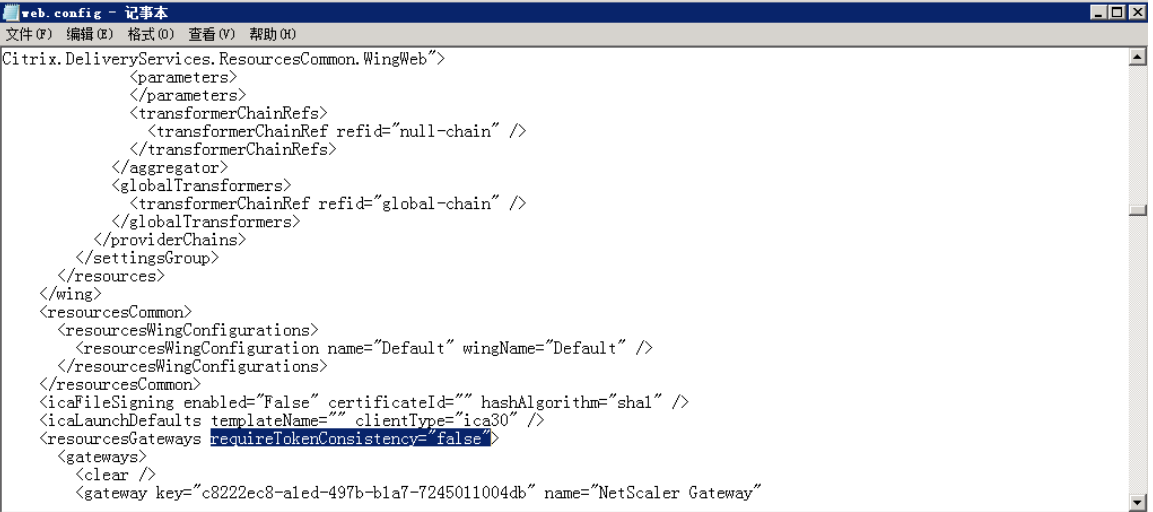
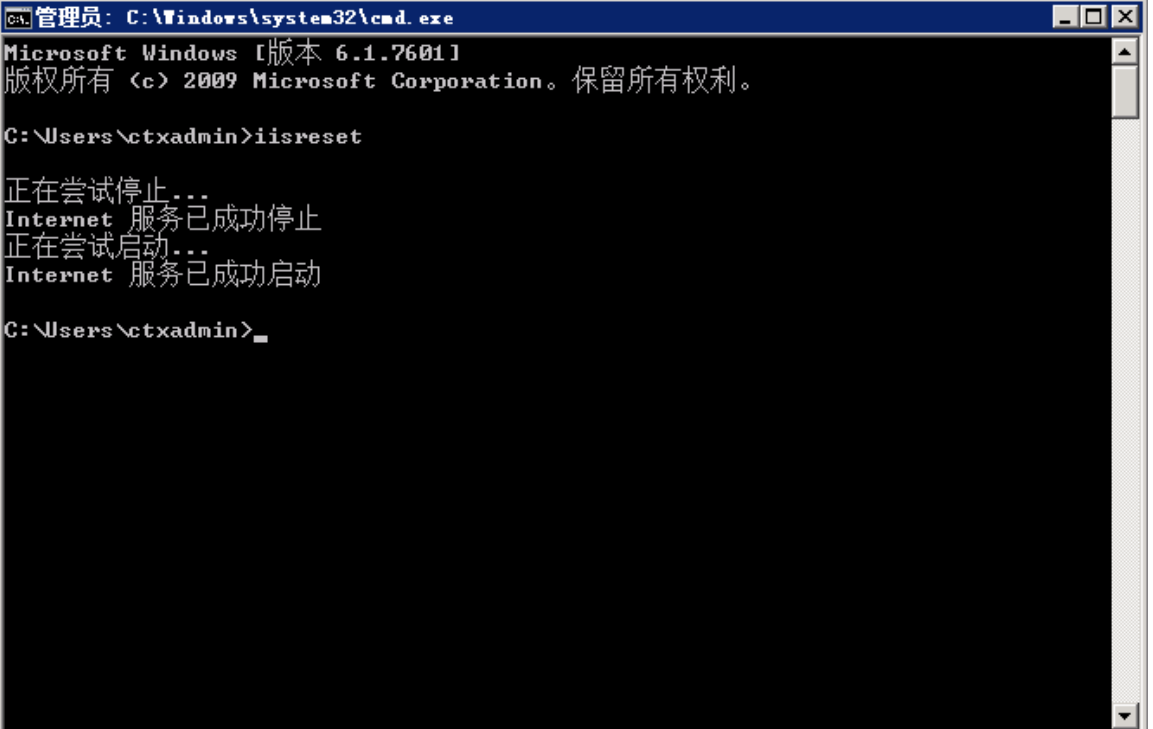
25 Per Page 1 - 1 of 1 1

Confirm Do you want to save the running configuration? Yes No

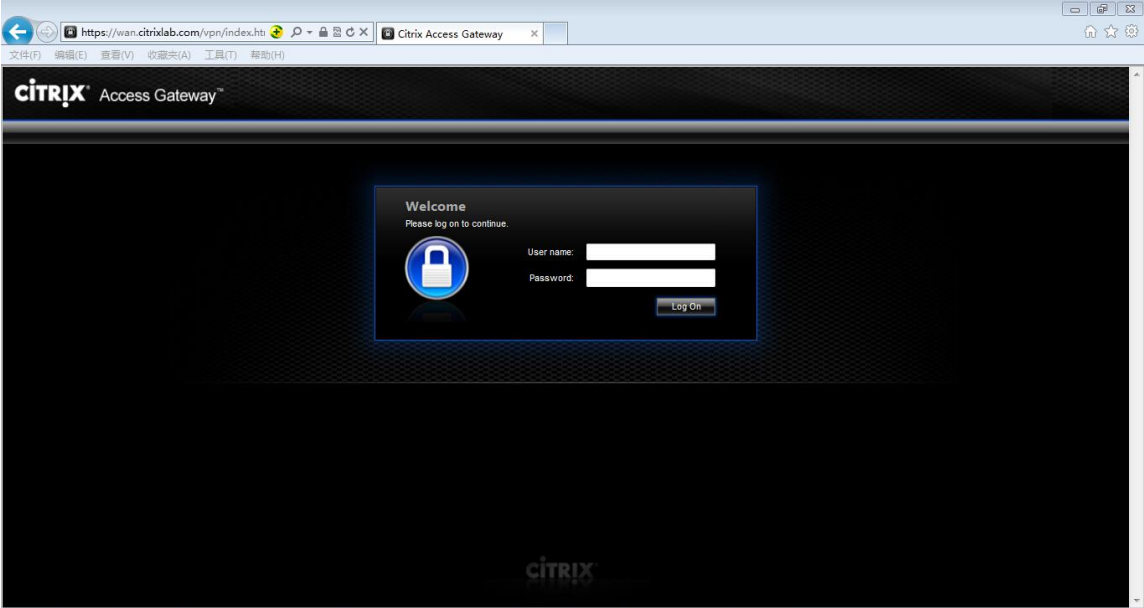
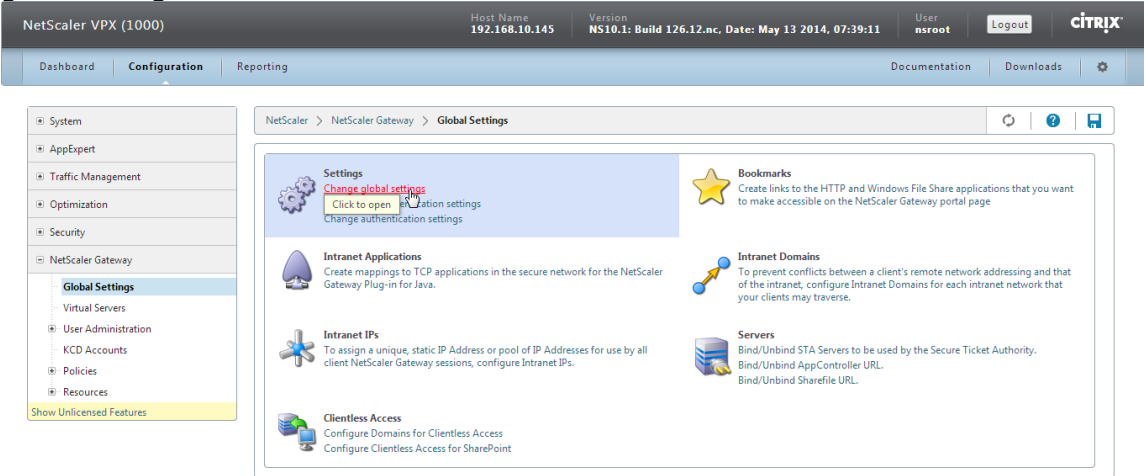
## 4.5 使用 IOS 设备第一次登录失败

使用 IOS 设备，第一登录 NetScaler 提示登录失败，需要再次登录才能成功，解决方法如下：

步骤	操作
1.	<p>使用 ctxadmin 登录 StoreFront 服务器 导航到 C:\inetpub\wwwroot\Citrix\Store</p> 
2.	<p>使用记事本打开 web.config</p> 

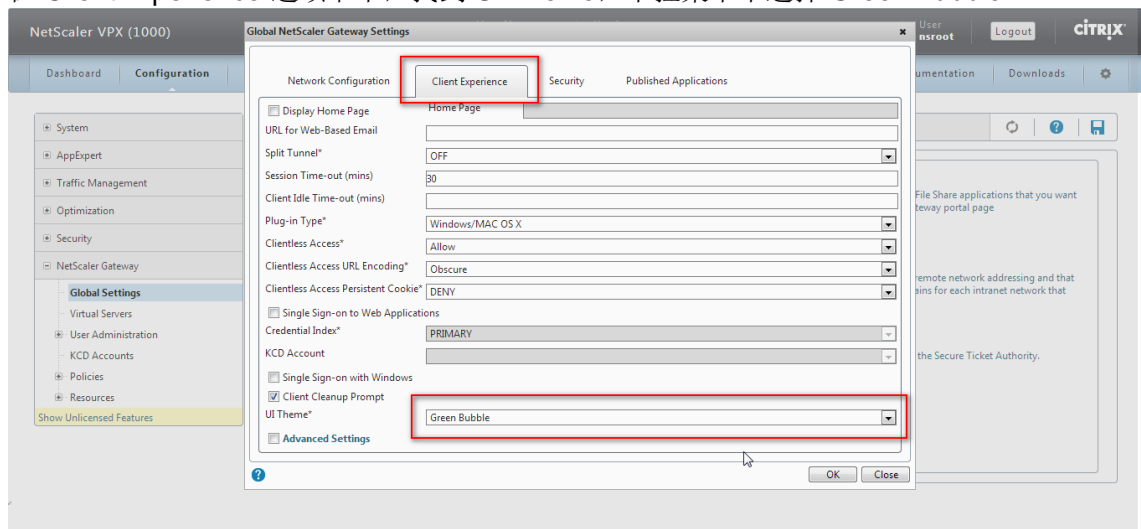
步骤	操作
3.	<p>查找 requireTokenConsistency, 将 True 修改为 false。</p>  <pre> web.config - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) Citrix.DeliveryServices.ResourcesCommon.WingWeb"&gt;   &lt;parameters&gt;   &lt;/parameters&gt;   &lt;transformerChainRefs&gt;     &lt;transformerChainRef refid="null-chain" /&gt;   &lt;/transformerChainRefs&gt;   &lt;/aggregator&gt;   &lt;globalTransformers&gt;     &lt;transformerChainRef refid="global-chain" /&gt;   &lt;/globalTransformers&gt;   &lt;/providerChains&gt;   &lt;/settingsGroup&gt; &lt;/resources&gt; &lt;/wing&gt; &lt;resourcesCommon&gt;   &lt;resourcesWingConfigurations&gt;     &lt;resourcesWingConfiguration name="Default" wingName="Default" /&gt;   &lt;/resourcesWingConfigurations&gt; &lt;/resourcesCommon&gt; &lt;icaFileSigning enabled="False" certificateId="" hashAlgorithm="sha1" /&gt; &lt;icaLaunchDefaults templateName="" clientType="ica30" /&gt; &lt;resourcesGateways requireTokenConsistency='false'&gt;   &lt;gateways&gt;     &lt;clear /&gt;     &lt;gateway key="c8222ec8-a1ed-497b-b1a7-7245011004db" name="NetScaler Gateway" </pre>
4.	<p>使用 iisreset 命令重启 IIS 服务</p>  <pre> 管理员: C:\Windows\system32\cmd.exe Microsoft Windows [版本 6.1.7601] 版权所有 (c) 2009 Microsoft Corporation。保留所有权利。  C:\Users\ctxadmin&gt;iisreset  正在尝试停止... Internet 服务已成功停止 正在尝试启动... Internet 服务已成功启动  C:\Users\ctxadmin&gt;_ </pre>

## 4.6 访问验证及 NetScaler Gateway 登录首页风格优化

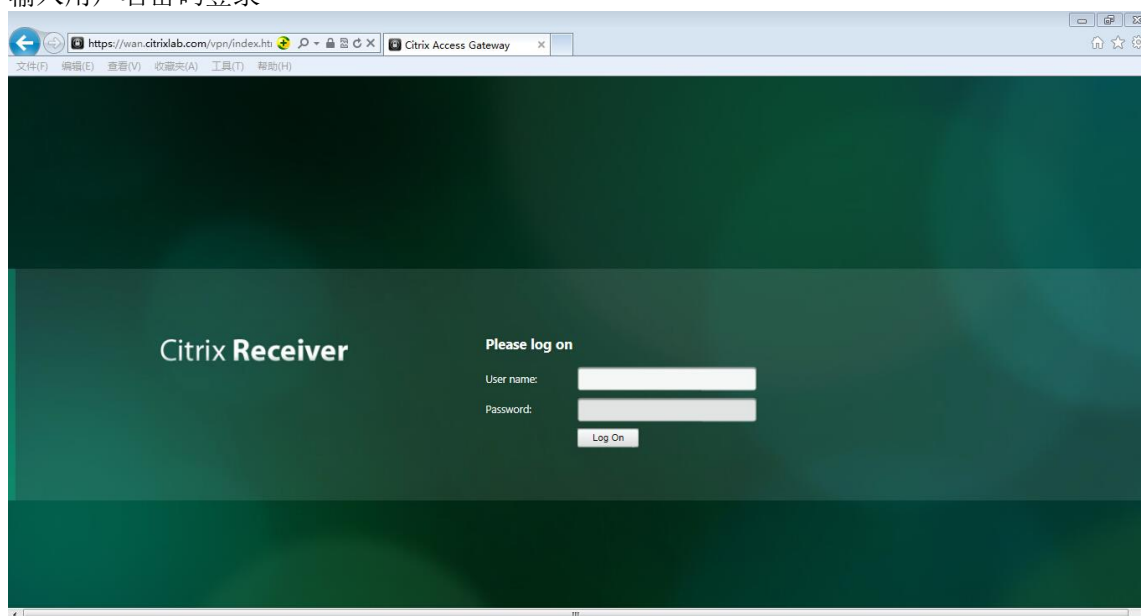
步骤	操作
5.	<p>使用浏览器，输入 <a href="https://wan.citrixlab.com">https://wan.citrixlab.com</a> 访问 NetScaler Gateway。首页面风格如下图所示。可以对其做更改。</p> 
6.	<p>回到 NetScaler 配置页面，在 NetScaler Gateway，Global Settings 右边找到并点击 Change global settings</p> 

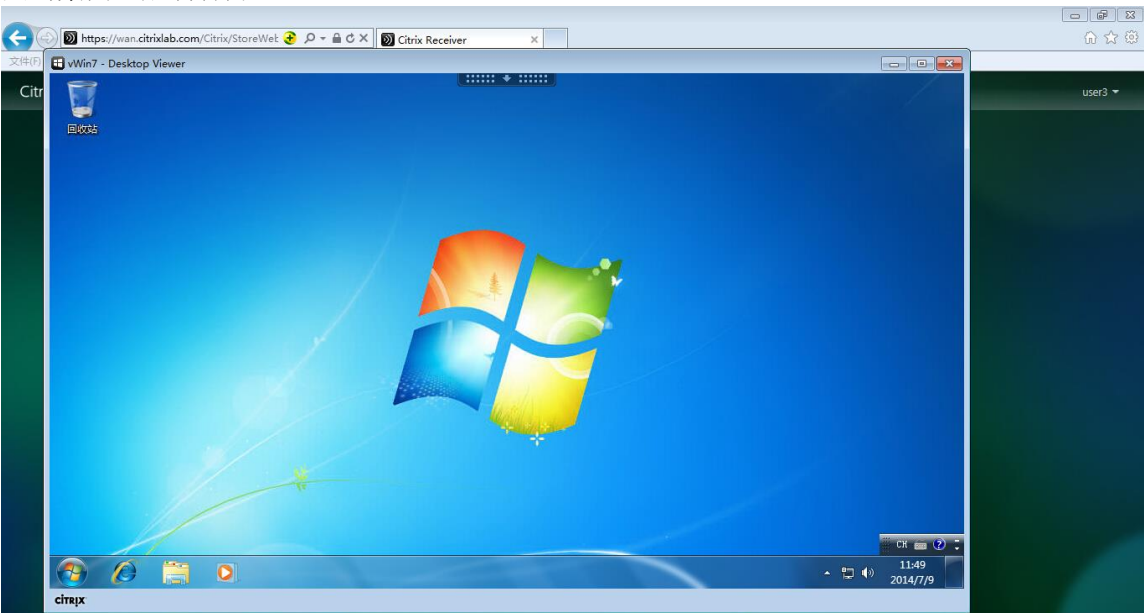
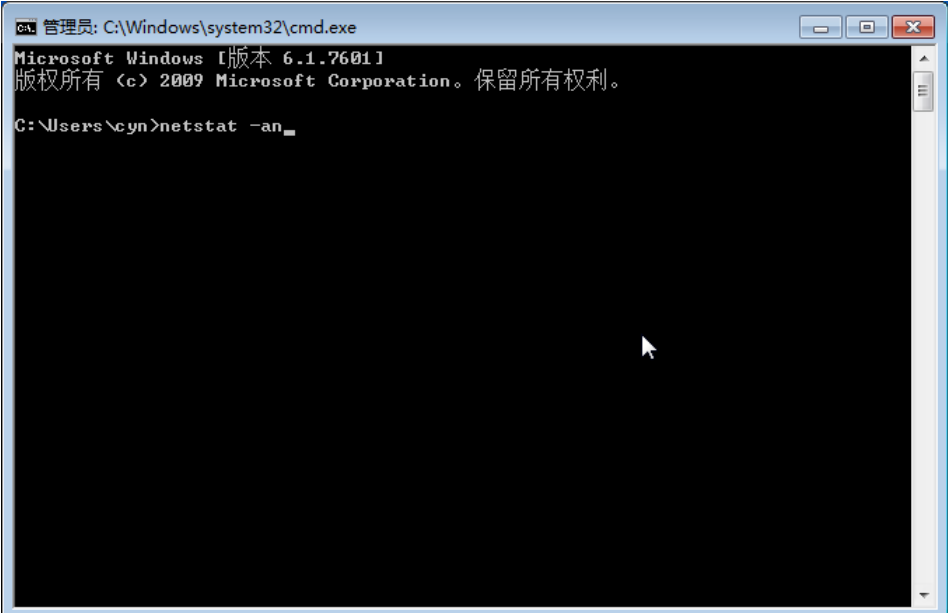
步骤 操作

7. 在 Client Experience 选项卡中，找到 UI Theme，下拉菜单中选择 Green Bubble

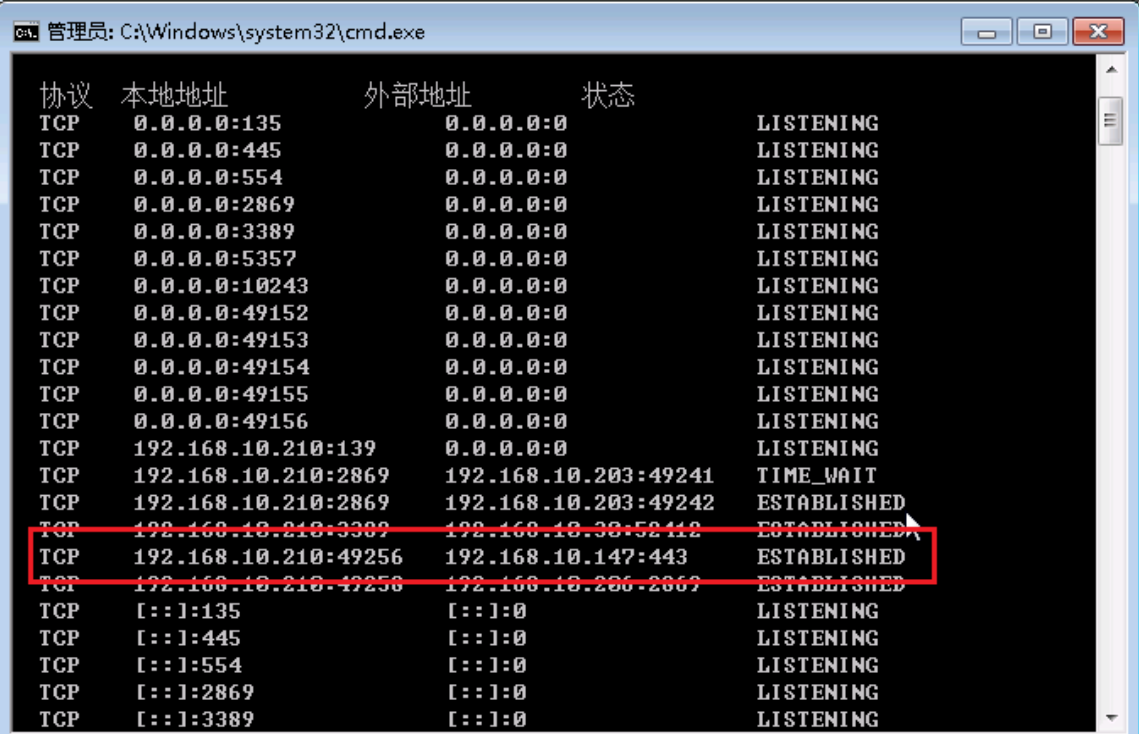


8. 再次登录 <https://wan.citrixlab.com>，登录界面风格已经修改。  
输入用户名密码登录



步骤	操作
9.	<p>点击桌面，成功打开</p> 
10.	<p>为了进一步验证当前的连接是使用 SSL 连接，打开命令行窗口，并输入 netstat -an</p> 



步骤	操作
11.	<p>可以注意到，我们和 NetScaler Gateway 的 VIP 地址之间，使用的是 SSL 连接</p>  <pre> 协议 本地地址          外部地址          状态 TCP    0.0.0.0:135        0.0.0.0:0         LISTENING TCP    0.0.0.0:445        0.0.0.0:0         LISTENING TCP    0.0.0.0:554        0.0.0.0:0         LISTENING TCP    0.0.0.0:2869       0.0.0.0:0         LISTENING TCP    0.0.0.0:3389       0.0.0.0:0         LISTENING TCP    0.0.0.0:5357       0.0.0.0:0         LISTENING TCP    0.0.0.0:10243      0.0.0.0:0         LISTENING TCP    0.0.0.0:49152      0.0.0.0:0         LISTENING TCP    0.0.0.0:49153      0.0.0.0:0         LISTENING TCP    0.0.0.0:49154      0.0.0.0:0         LISTENING TCP    0.0.0.0:49155      0.0.0.0:0         LISTENING TCP    0.0.0.0:49156      0.0.0.0:0         LISTENING TCP    192.168.10.210:139 0.0.0.0:0         LISTENING TCP    192.168.10.210:2869 192.168.10.203:49241 TIME_WAIT TCP    192.168.10.210:2869 192.168.10.203:49242 ESTABLISHED TCP    192.168.10.210:3389 192.168.10.30:52442 ESTABLISHED TCP    192.168.10.210:49256 192.168.10.147:443 ESTABLISHED TCP    192.168.10.210:49256 192.168.10.206:2869 ESTABLISHED TCP    [::]:135           [::]:0            LISTENING TCP    [::]:445           [::]:0            LISTENING TCP    [::]:554           [::]:0            LISTENING TCP    [::]:2869          [::]:0            LISTENING TCP    [::]:3389          [::]:0            LISTENING </pre>

至此，NetScaler 配置完成。

## 4.7 常见问题及排错

前面已经介绍了 NetScaler 与 StoreFront 的集成配置，实际上这样的配置完成了两个产品的整合。不过在整个配置的过程中，仍然会有些小的注意事项，还有一些简易的排错手段。

### 4.7.1 注意事项：

- 1， 相比较于过去的 Access Gateway 与 Web Interface 集成，认证部分是既可以通过 Web Interface 来完成也可以通过 NetScaler 完成。但 StoreFront 与 NetScaler 集成，认证必须在 NetScaler 上完成。
- 2， 因此，NetScaler 与 AD 的 DC 之间的相对应的端口 389/3268 必须开通，以保证认证顺利完成。
- 3， 与过去需要手动一条条在 NetScaler 上配置 VIP/profile/session 等各种策略不同，现在使用 wizard 方式要简单很多。不过这种方式只适合所谓的新手，因为其默认策略只有 2 条，如果需要更复杂策略的则还是需要手动添加完成。
- 4， NetScaler 发布的时候，一定需要一张证书并关联在对应的 VIP 上。
- 5， 如果前端有多台 NetScaler，如部署 GSLB，在 StoreFront 上配置 NetScaler Gateway 时，SNIP 请直接设空。如果此处设定 SNIP 反而有可能出问题。

- 6, 此设定只适用于 NetScaler 与 StoreFront 集成为 XenDesktop 服务, 如果您的环境中还有 XenMobile 的组件, 需要手动创建 profile/session policy。或者在发布时选择 App Controller。
- 7, 请确认 NetScaler 与 StoreFront 之间相互名称解析正确, 证书相互信任。

#### 4.7.2 常见错误:

##### 1. Cannot complete your request/无法完成您的请求

在 NetScaler 与 StoreFront 集成配置中, 这个报错是最容易遇到的。导致这个问题的原因有很多, 可能有以下几种:

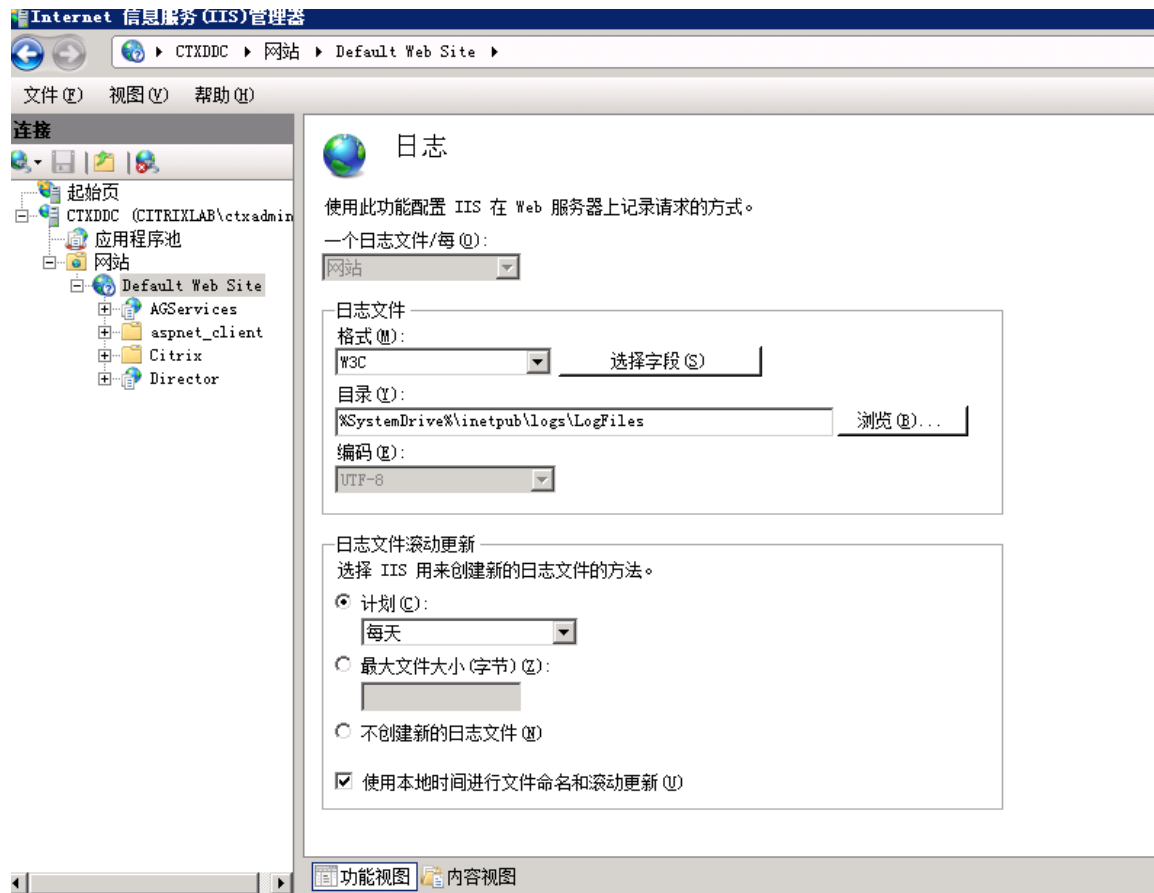
- a. 在 StoreFront 上设定的域认证的名称与在 NetScaler 上设定的 Single sign on 的单点登录所设定的短域名不一致。
  - b. Callback 中所设定的 FQDN, 在 StoreFront 上不能正常解析。
  - c. NetScaler 不能正确解析你所设定的 StoreFront 的 FQDN。
  - d. NetScaler 和 StoreFront/DDC 之间通信的问题。
  - e. 确认各服务都正常启动。
2. 使用 iOS 设备, 第一次登陆失败, 退出 receiver 后再重新登陆正常。
    - a. 在 StoreFront 主机上, 定位到 c:\inetpub\wwwroot\Citrix\<your store name>\
    - b. 用文本编辑器编辑 web.config (修改前请先拷贝一份此文件作为备份)
    - c. 查找 requireTokenConsistency, 将 True 修改为 false。
    - d. 在命令行, 输入 iisreset, 重启 IIS 引擎。

#### 排错工具:

1. 事件日志为 StoreFront 排错的时候, 除了查看 Windows 本身的 App/Sys 事件日志之外, 还有一个 Citrix Delivery Service 事件类别可以使用。里面会较为详细记录各种信息, 尤其在排错一般登陆问题, 如 “Cannot complete the request” 问题时非常有用。



2. IIS log 只要请求能够发送到 StoreFront 上，则一定会在 IIS 上留下记录。使用 Excel 打开目录下的最新日志，通过排序可以分析出一些有价值的信息。



产品版本

产品	版本
XenDesktop	7.5
XenApp	7.5
XenServer	6.2 SP1
NetScaler	10.1