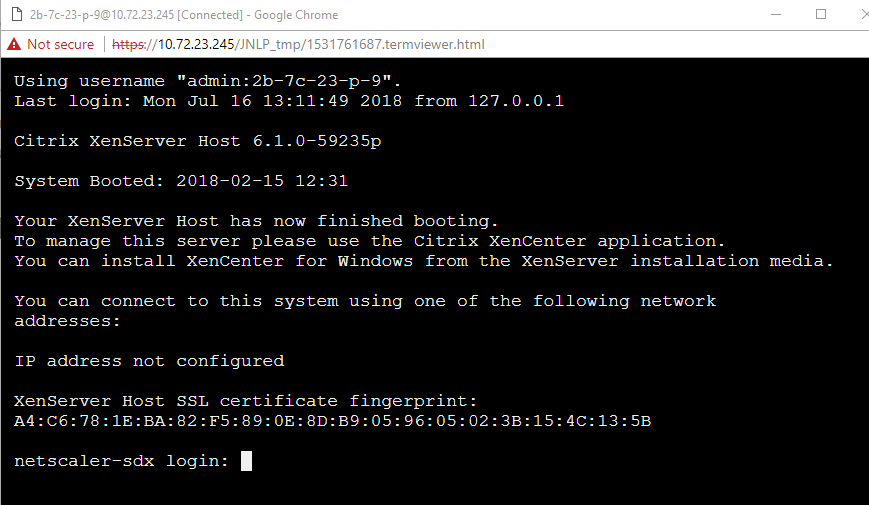
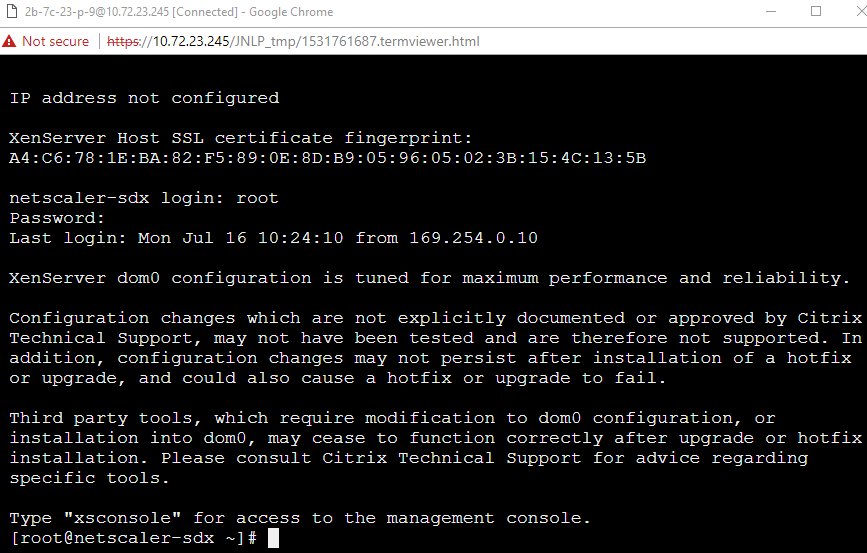
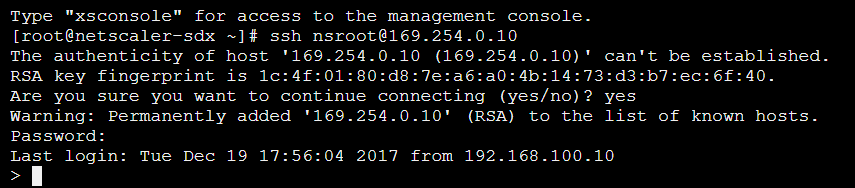
Initial Network Config



Default Password: root/nsroot

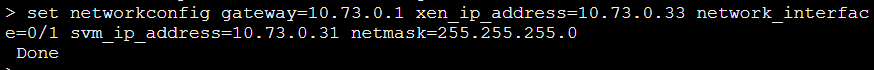


At the prompt, type: ssh nsroot@169.254.0.10 When prompted for the password, type nsroot



At the shell prompt, type:

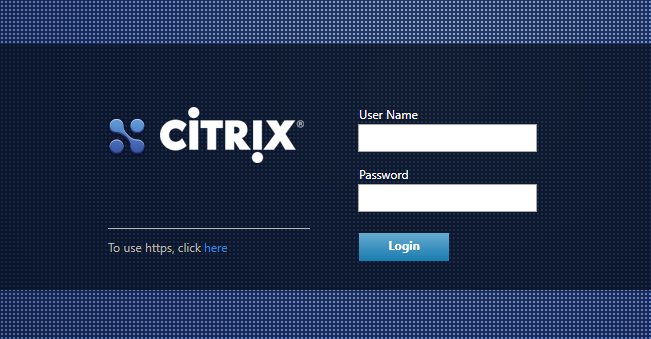
set networkconfig gateway=<ipaddress> xen\_ip\_address=<ipaddress> network\_interface=<string> svm\_ip\_address=<ipaddress> netmask=<ipaddress>



Firmware Upgrade

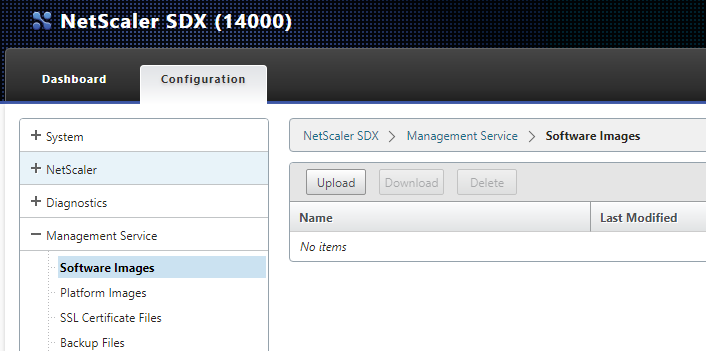
http://{svm\_ip\_address}

nsroot/nsroot



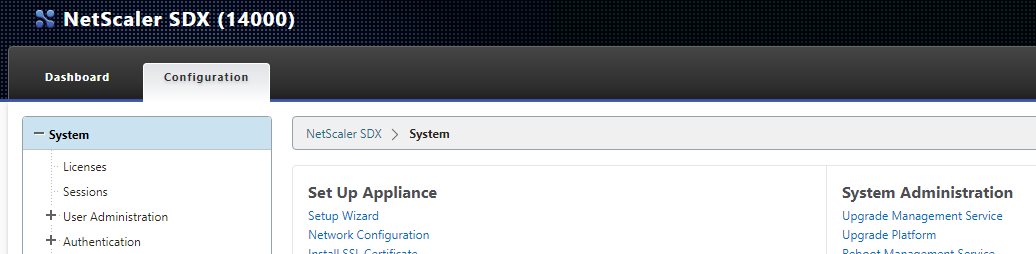
Configuration…Management Service…Software Images

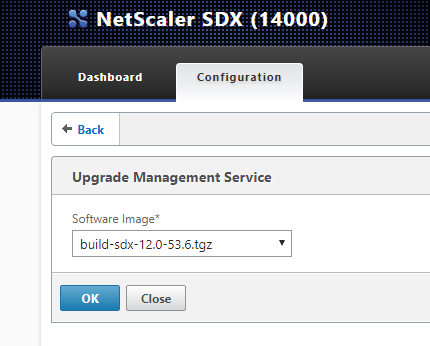
Upload

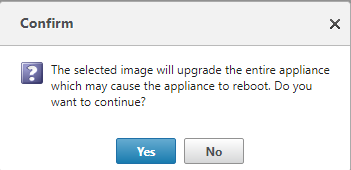


[\\aqrcapital.com\shares\FS001\Citrix\Citrix\SDX-12.0-53.6\build-sdx-12.0-53.6.tgz](file:///\\aqrcapital.com\shares\FS001\Citrix\Citrix\SDX-12.0-53.6\build-sdx-12.0-53.6.tgz)

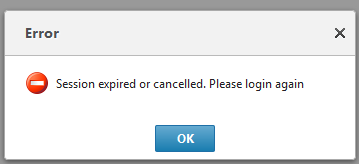
Upgrade by clicking System…System Administration…Upgrade Management Service



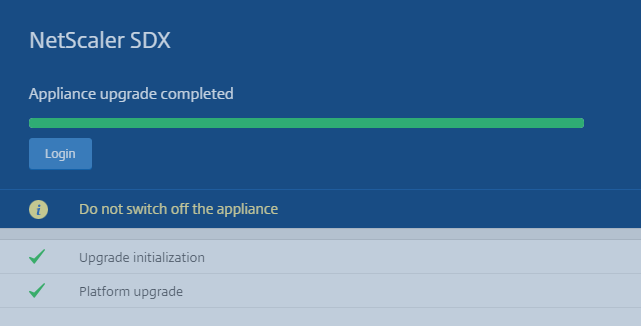




This will take a long time. Do not freak out. After a while, reloading the page will show a progress bar…



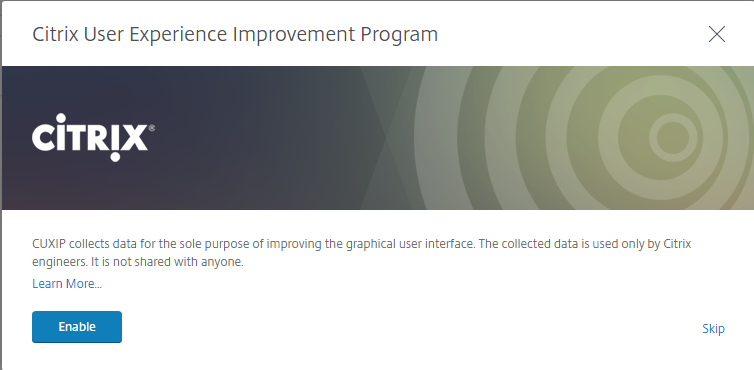




Change Default Password

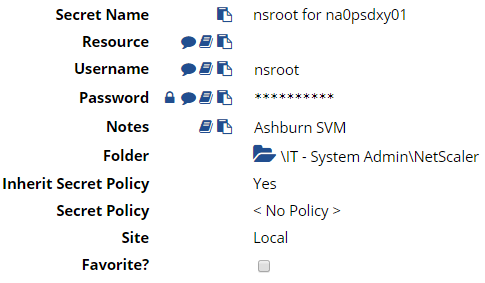
Login

Skip the User Experience Setup



Reset nsroot password

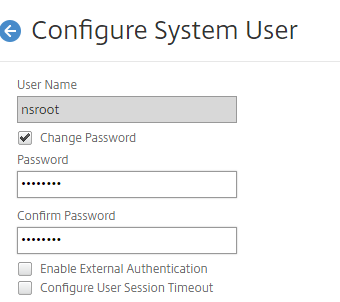
Add PIM Entry



System…User Administration…Users

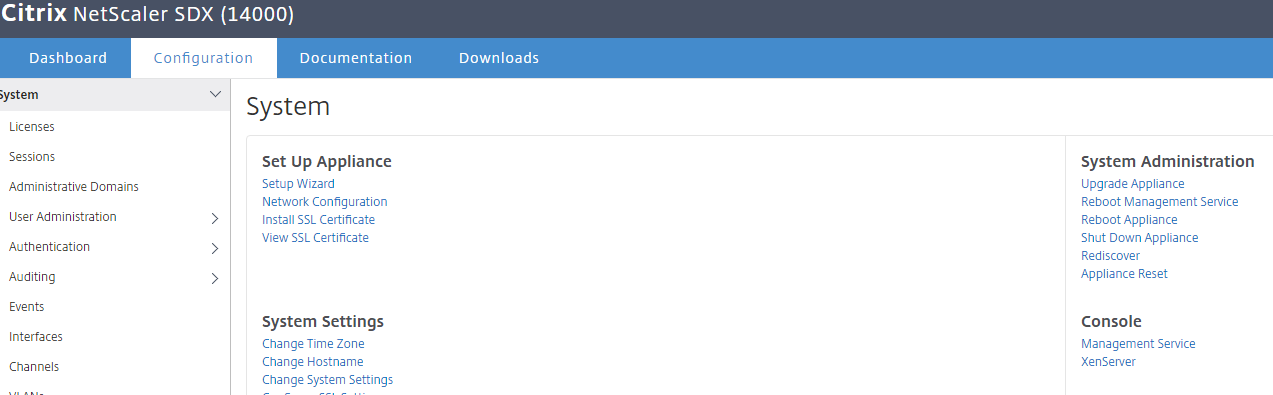
\*\*\* NOTE: This also changes the “root” password for XenServer \*\*\*

Edit nsroot, change password

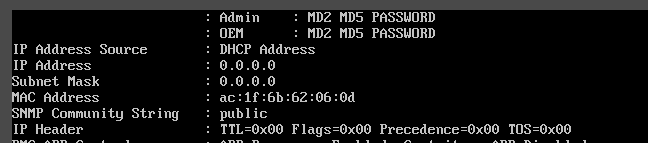


Configure LOM

System…Console…XenServer



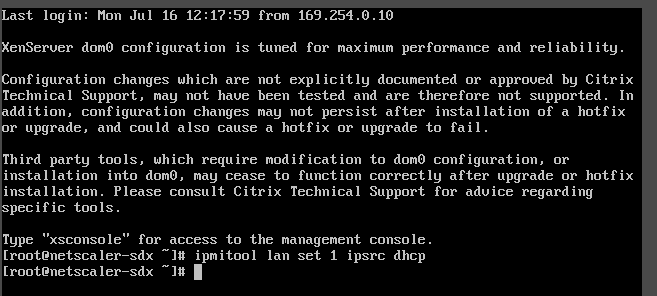
Ipmitool lan print 1 and get the MAC Address



Add Fixed Address in InfoBlox for the MAC address.

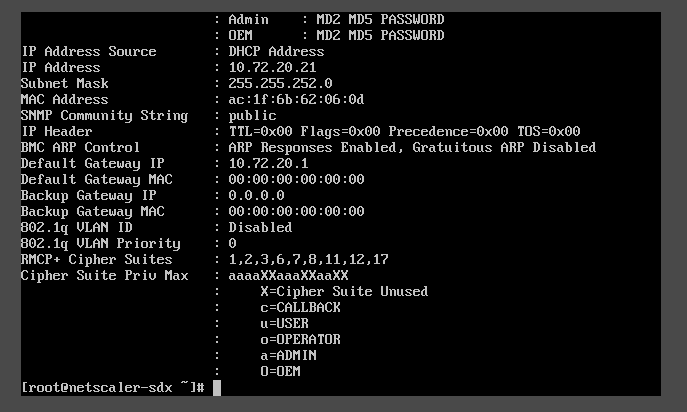
Ipmitool lan set 1 ipsrc dhcp

Ipmitool mc reset warm



Ipmitool lan print 1

Verify DHCP address

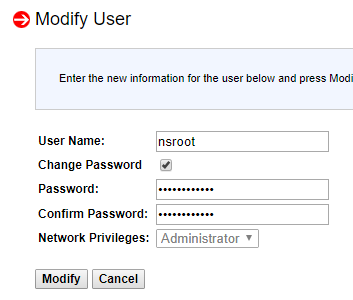


Connect to LOM via browser nsroot/nsroot

Add Entry in PIM

Configuration…Users…nsroot…Modify User

Change LOM password



If setting a static IP address, use: ipmitool lan set 1 ipaddr IP\_Address

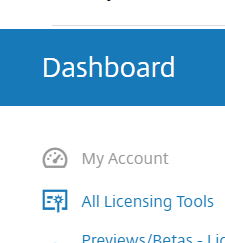
Ipmitool lan set 1 netmask netmask\_address

Ipmitool lan set 1 defgw ipaddr gateway\_server

Licensing

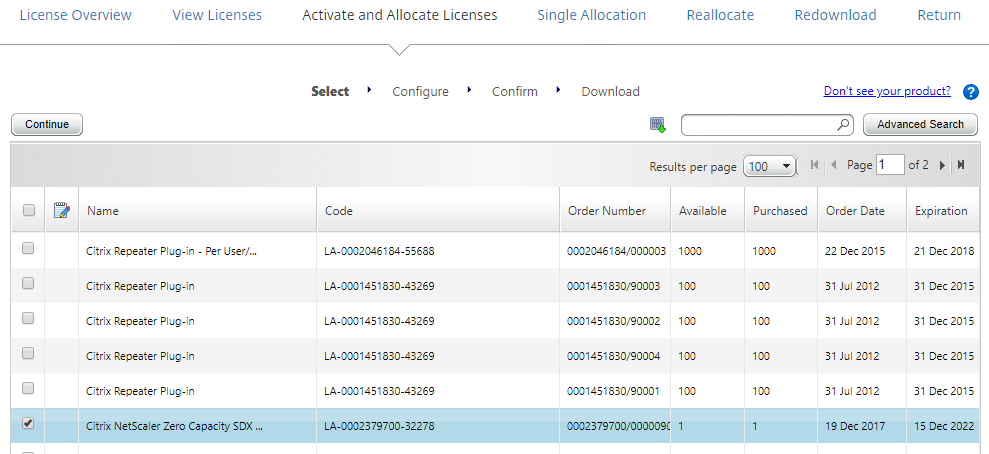
Login to [www.citrix.com](http://www.citrix.com)

All Licensing Tools



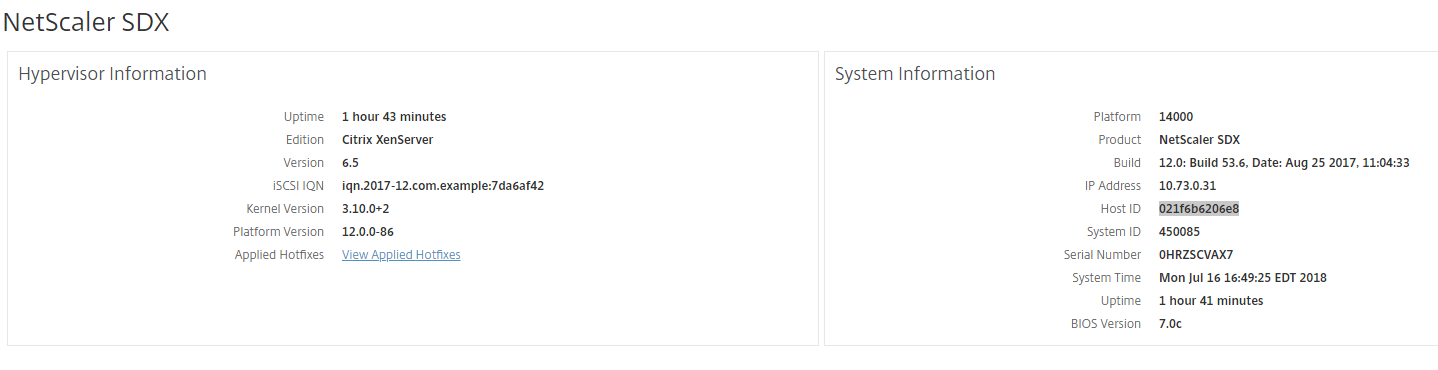
Activate and Allocate Licenses

Find Citrix NetScaler Zero Capacity SDX Z License and Select it

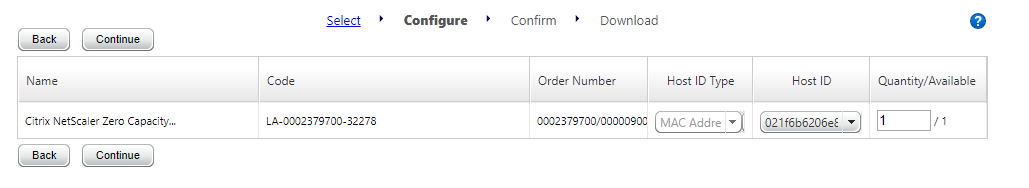


Click Continue

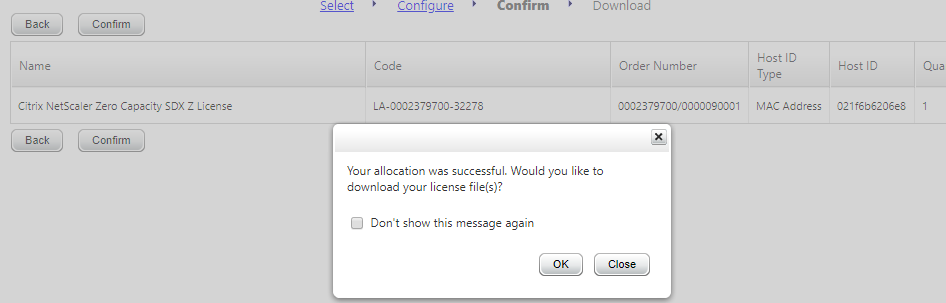
From the SDX System Information page, select and copy the Host ID



Paste it in the Host ID field on the Citrix License page



Confirm and Download the license file.

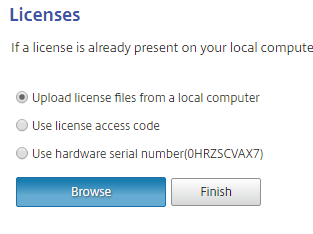


Save the file in:

[\\aqrcapital.com\shares\FS001\Citrix\Citrix\licenses\SDX-Zero](file:///\\aqrcapital.com\shares\FS001\Citrix\Citrix\licenses\SDX-Zero)

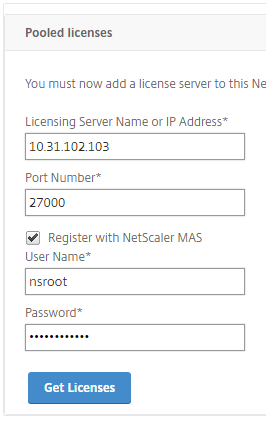
As the SDX hostname-mac address.lic (ie: na0psdxy01-021f6b6206e8.lic)

On the SDX, System…Licenses…Upload license files from a local computer

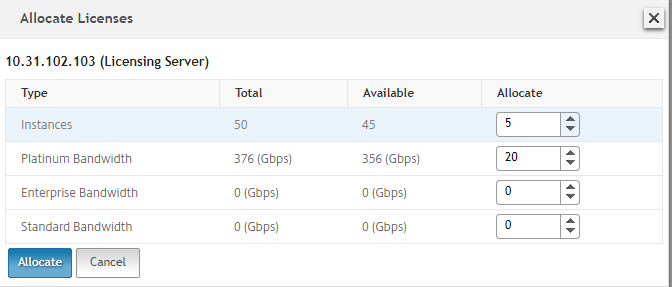


Click Finish.

Enter the NMAS information using the nsroot password in PIM for nt0pctxmas01\nsroot



Allocate licenses as appropriate



Apply Licenses. Verify Licenses Applied Successfully

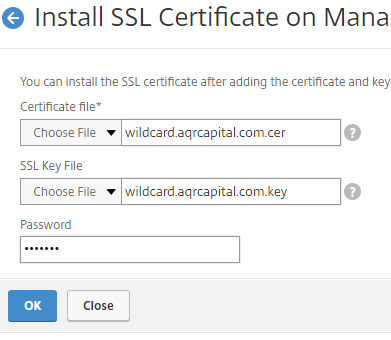


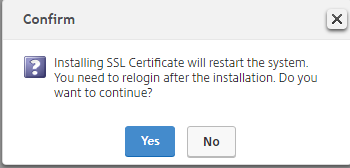
SSL Certificate

System…Set Up Appliance…Install SSL Certificate

[\\aqrcapital.com\shares\FS001\Citrix\Citrix\SSL\AQRCapital\_Wildcard\](file:///\\aqrcapital.com\shares\FS001\Citrix\Citrix\SSL\AQRCapital_Wildcard\)

Password: PIM secret: wildcard.aqrcapital.com



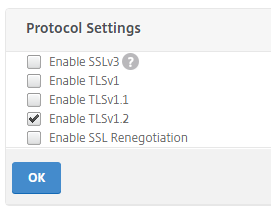


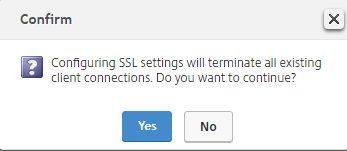
SSL Configuration

System…System Settings…Configure SSL Settings

Edit Settings… Protocol Settings

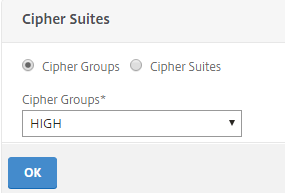
Enable TLSv1.2 ONLY

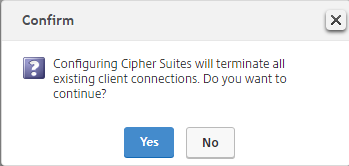




Edit Settings…Cipher Suites

Cipher Groups...HIGH

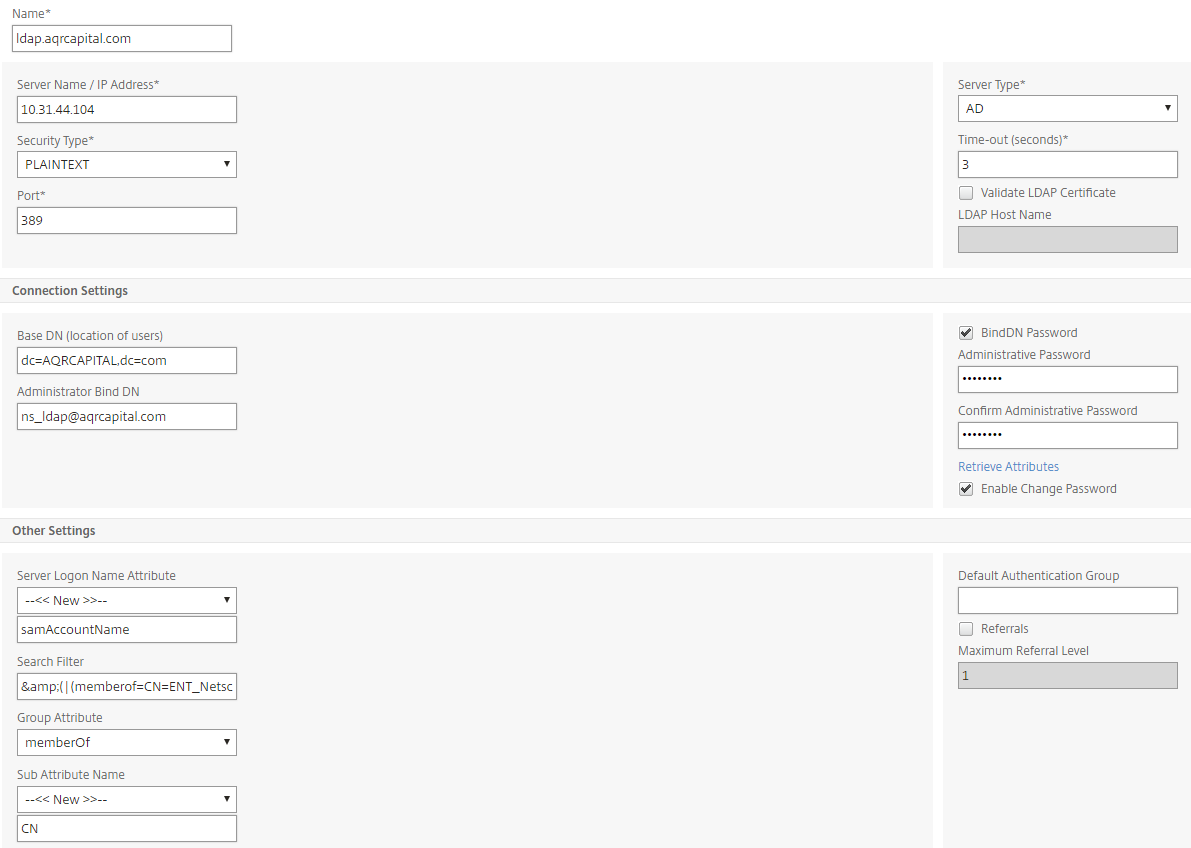




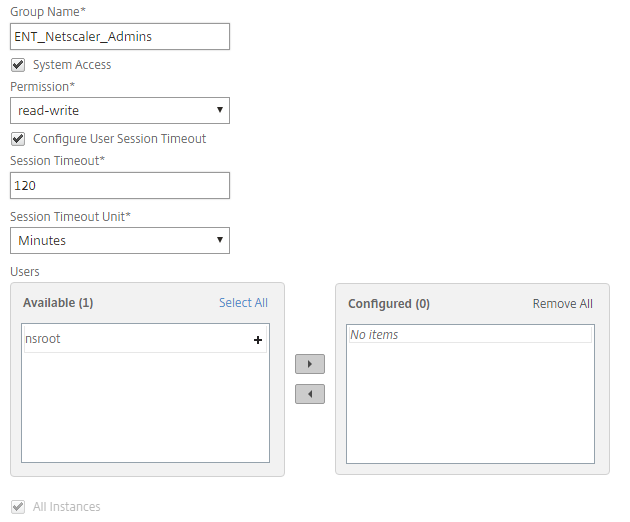
Enable LDAP Authentication

System…Authentication…LDAP…Add

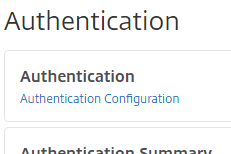
Use Bind Password from PIM: Netscaler LDAP bind account



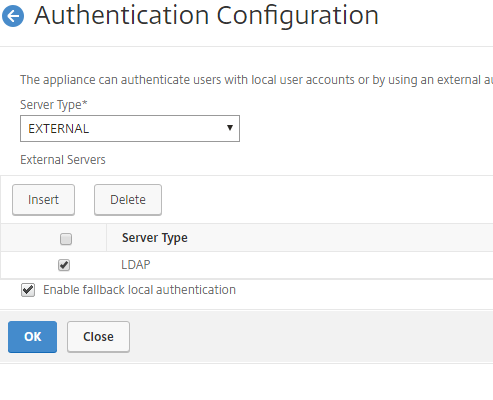
System…User Administration…Groups…Add



System…Authentication…Authentication Configuration



Change to EXTERNAL and Insert LDAP



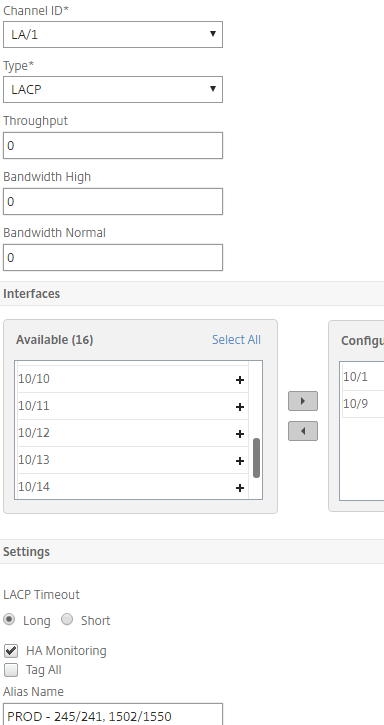
LACP Channels

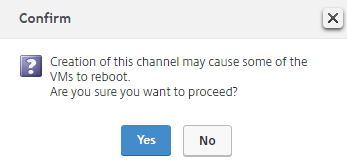
System…Channels…Add

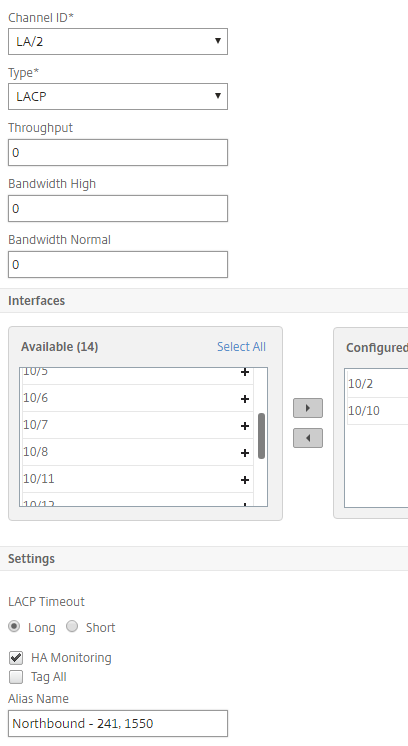
LA/1 – 10/1 and 10/9 – VLAN 245 (Southbound - DMZv2), VLAN 241 (Northbound - DMZv2) – PROD

VLAN 1502 (Southbound – DMZv3), VLAN 1550 (Northbound – DMZv3) – PROD

LA/2 – 10/2 and 10/10 – VLAN 1513 (Southbound), VLAN 1556 (Northbound) – STG



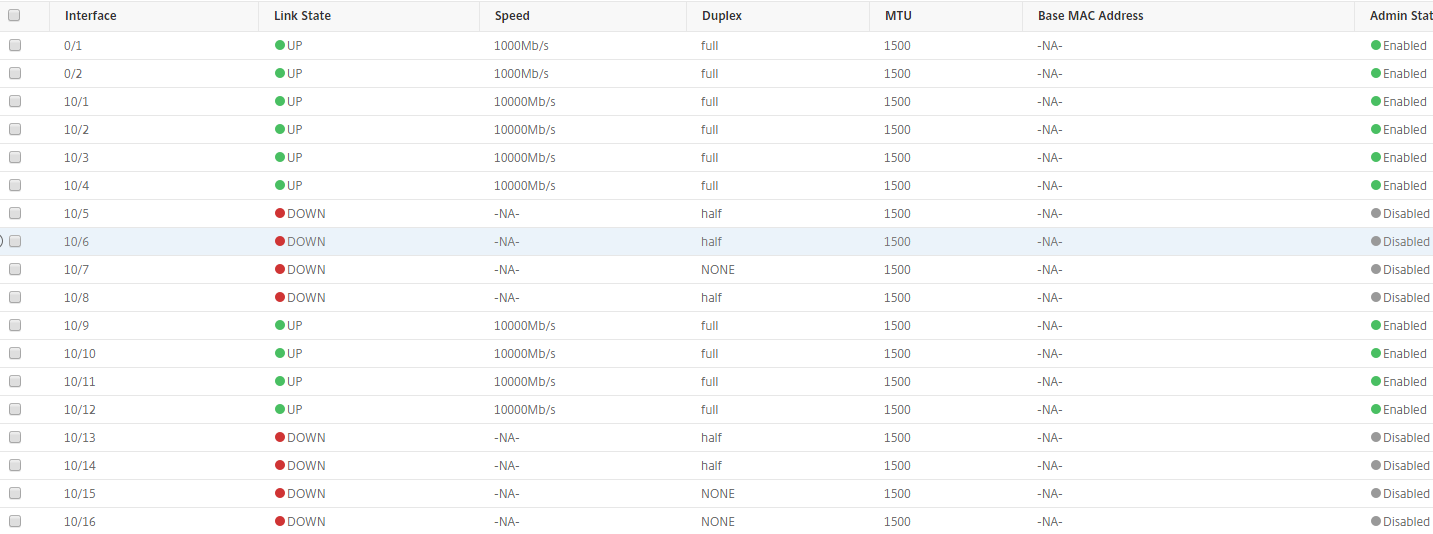




Disable Unused Interfaces

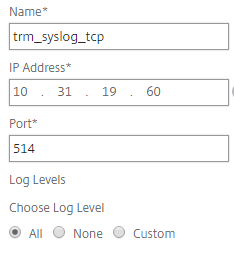
System…Interfaces

Disable each Down Interface



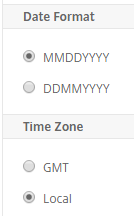
SYSLOG Configuration

System…Auditing…Syslog Servers…Add



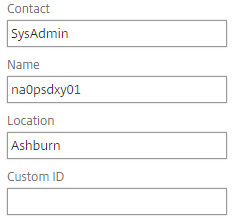
Syslog Parameters

Change Time Zone to Local



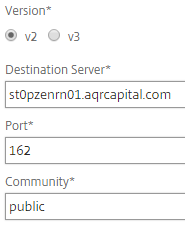
SNMP Configuration

System…SNMP…Settings…Configure SNMP MIB



System…SNMP...Trap Destinations…Add

Zenoss:

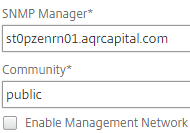


NMAS:



System…SNMP...Managers…Add

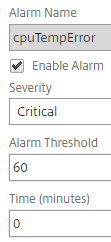
Add st0pzenrn01.aqrcapital.com through st0pzenrn04.aqrcapital.com



System…SNMP...Users…Add



System...Alarms



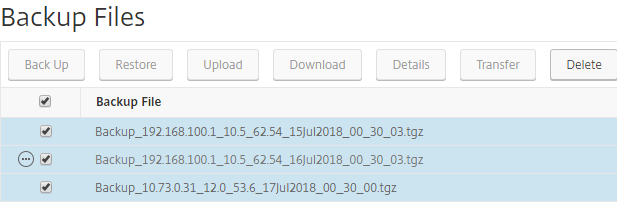
Set the following Alarms as Critical:

* cpuTempError
* cpuTempNormal
* cpuUsageHigh
* cpuUsageNormal
* diskUtilizationHigh
* diskUtilizationNormal
* fanSpeedError
* fanSpeedNormal
* interfaceDown
* interfaceUp
* ipmiStateError
* ipmiStateNormal
* logicalDriveFailed
* loginFailure
* memoryUsageHigh
* memoryUsageNormal
* networkConfigChanged
* physicalDriveFailed
* powerSupplyFailed
* powerSupplyNormal
* systemTempError
* systemTempNormal
* voltageError
* voltageNormal

Backup Configuration

Management Service…Backup Files

Delete default backups



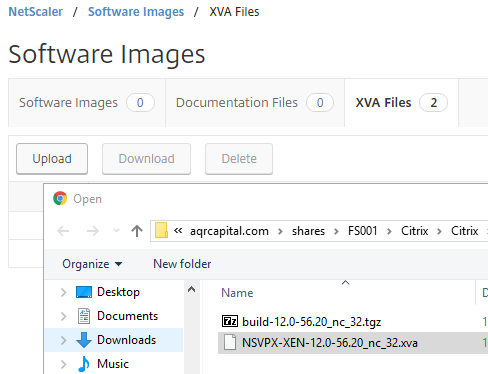
Make a New Backup File.

Upload NetScaler XVA Firmware

NetScaler…Software Images...XVA Files…Upload

Browse to the XVA file (downloaded from Citrix Site).

Note: This is downloaded as a .tgz file, extract the .xva file from the TAR file and use this for uploading to the SDX

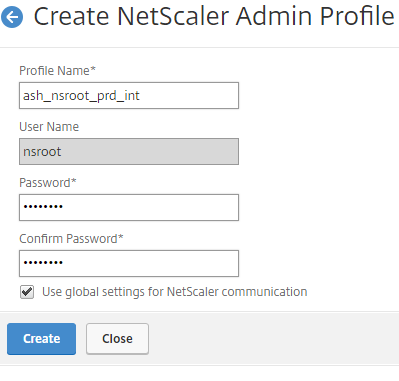


Create VPX Admin Profile

NetScaler…Admin Profiles…Add

Use the naming convention: site\_nsroot\_environment\_int/ext

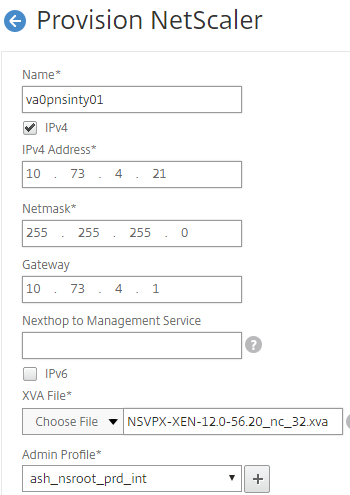
Record the password in PIM



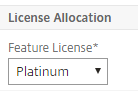
Create VPX Instance

NetScaler…Instances…Add

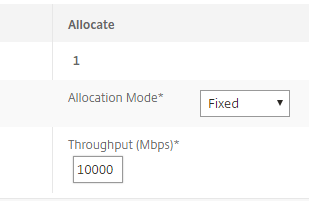
Name/IP Address/XVA Firmware/Profile:



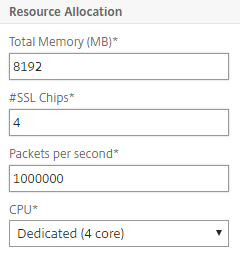
License:



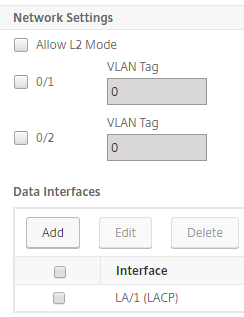
Bandwidth Throughput (Prod):



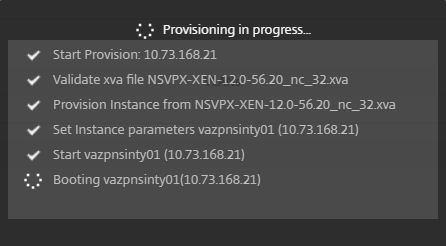
Resources (Prod):



Network:



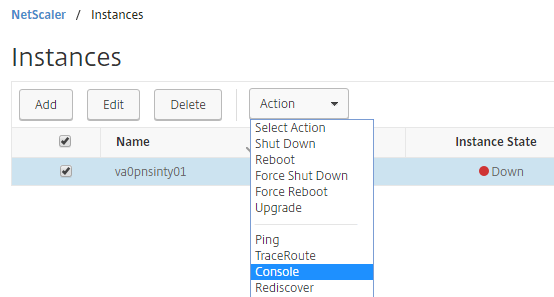
Click Done

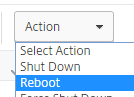


Note: This will take several minutes, and will ultimately time out – this is because the VPX Instance is not on the proper VLAN for administration. This will be adjusted in the next steps. Watch for the line stating “Booting…”. After 10 minutes, you may refresh the page and return to the Instances page.

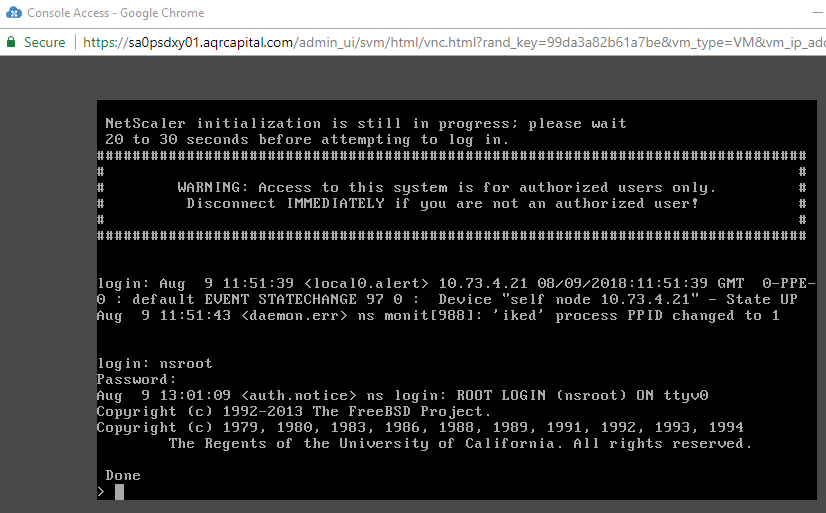
Configure VPX VLAN

NetScaler…Instances…Console



Note: If no response, reboot the instance once.  

Login using the nsroot account set up in PIM



Enter the following commands:

add vlan xxx

Use the appropriate VLAN ID

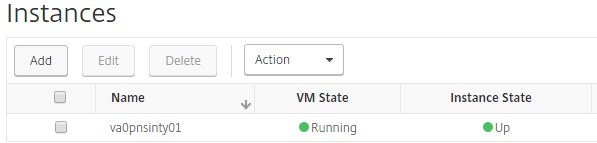
bind vlan xxx -ifnum LA/y -tagged

Use the appropriate Link Aggregate Channel

save config

Use ping to check communication to the gateway.

Verify that the SDX shows the instance as Running/Up



Basic VPX Configuration

As a pre-requisite, you need WinSCP and the WinSCP PowerShell Wrapper installed.

* Install WinSCP
* Open Admin PowerShell Command Line and run “Install-Module -Name WinSCP“

Go/aqrgit to retrieve the NetScaler\_basic\_setup.ps1 script

Open a PowerShell Command Window

Execute the NetScaler\_basic\_setup.ps1 script

Provide the following information:

* NSIP
* SNIP
* NetMask
* Host Name
* Credentials (nsroot from PIM as defined above)

After the script completes, there will be a file called H:\{hostname}-initial.txt. Review the contents of this file for any errors.

Login to the GUI of the NetScaler using LDAP credentials to verify.