Infoblox

DEPLOYMENT GUIDE

Enabling and Configuring Content filtering without Multi-Service Proxy (MSP)

Table of Contents

What is Subscriber Policy Enforcement and Parental Control?

NIOS 8.3 onwards, Infoblox introduced a new product line known as Subscriber Services. It encompasses multiple features, namely Subscriber Insight, Subscriber Policy Enforcement, and Parental Control. Subscriber Policy Enforcement and Parental Control enable Infoblox customers to have granular control of DNS responses at the client level. Policies pertaining to DNS resolution can be created for individual clients or networks. These policies essentially notify Infoblox NIOS whether a client (or clients from a subnet) query should be allowed/blocked/redirected to query certain domains.

Subscriber Policy Enforcement and Parental Control feature can be leveraged by Service Providers to license it out to their customers, more commonly referred to as subscribers.

How is Parental Control different from Subscriber Policy Enforcement?

Both, Parental Control and Subscriber Policy Enforcement can only be used after activating the subscriber services functionality in the Infoblox grid. However, there are still some underlying differences between them.

Subscriber Policy Enforcement	Parental Control
The Subscriber Secure policy (SSP) decides the DNS response a subscriber should get for a DNS query based on pre-configured Response Policy Zones (RPZs) in NIOS.	The Parental Control policy (PCP) decides the DNS response a subscriber should get for a DNS query based on the Content Categorization database.

More about Parental control

Parental Control enables parents and guardians to monitor and control the internet browsing of their kids and dependents. Once enabled, Parental Control downloads the content categorization database to restrict access to prohibited websites. DNS requests are then evaluated against these categories and a pre-defined action is taken.

The Content Categorization database has 128 categories assigning websites to categories such as alcohol, gambling, pornography, etc. Parents or guardians can create various policies by which access can be blocked to these age-restricted sites.

What is IB-FLEX?

IB-FLEX is an Infoblox virtual platform that is scalable based on the resources that you allocate to the virtual machine. NIOS automatically detects the capacity of the virtual machine and scales it to the appropriate platform after you provision the IB-FLEX member.

Points to remember

- You must first install the Grid license on a non-IB-FLEX appliance that is designated as the Grid Master to allow members to join the Grid, even if you have already installed a Flex Grid Activation license.
    - This license does not affect a non-IB-FLEX Grid Master.
    - An IB-FLEX appliance designated as a member does not require any license, neither Grid nor vNIOS while joining the Grid.
    - When you register an IB-FLEX member, the appliance checks for the Grid (enterprise) license and changes it to a non-IB-FLEX member.
    - For an IB-FLEX appliance, it checks for a Flex Grid Activation Grid-wide license before node registration.
- FLEX members can join the Grid through the MGMT interface when Software ADP is enabled.
- You can configure an IB-FLEX appliance to function as a Grid Master or a member.
- To enable reporting for a Grid member that is running Software ADP, you must configure the MGMT interface.

- A non IB-FLEX appliance designated as a member requires either a Grid and/or vNIOS/NIOS licenses installed to join the Grid.
- Similarly, for a reporting appliance to join the Grid, you must install a Grid and/or vNIOS/NIOS licenses. You cannot assign pool licenses to an IB-FLEX appliance. IB-FLEX supports HA for appliances that are running Software ADP.
- Infoblox supports elastic scaling on IB-FLEX members that use the Flex Grid Activation Grid-wide license.
- It also supports pre-provisioning for Software ADP on the supported platforms. You must add the new IB-FLEX model to the list of supported pre-provisioning hardware types so that you can select it during the member pre-provisioning.
- To pre-provision a non-IB-FLEX Grid member, you must have valid pool licenses and pre-provisioned those members in the Grid.

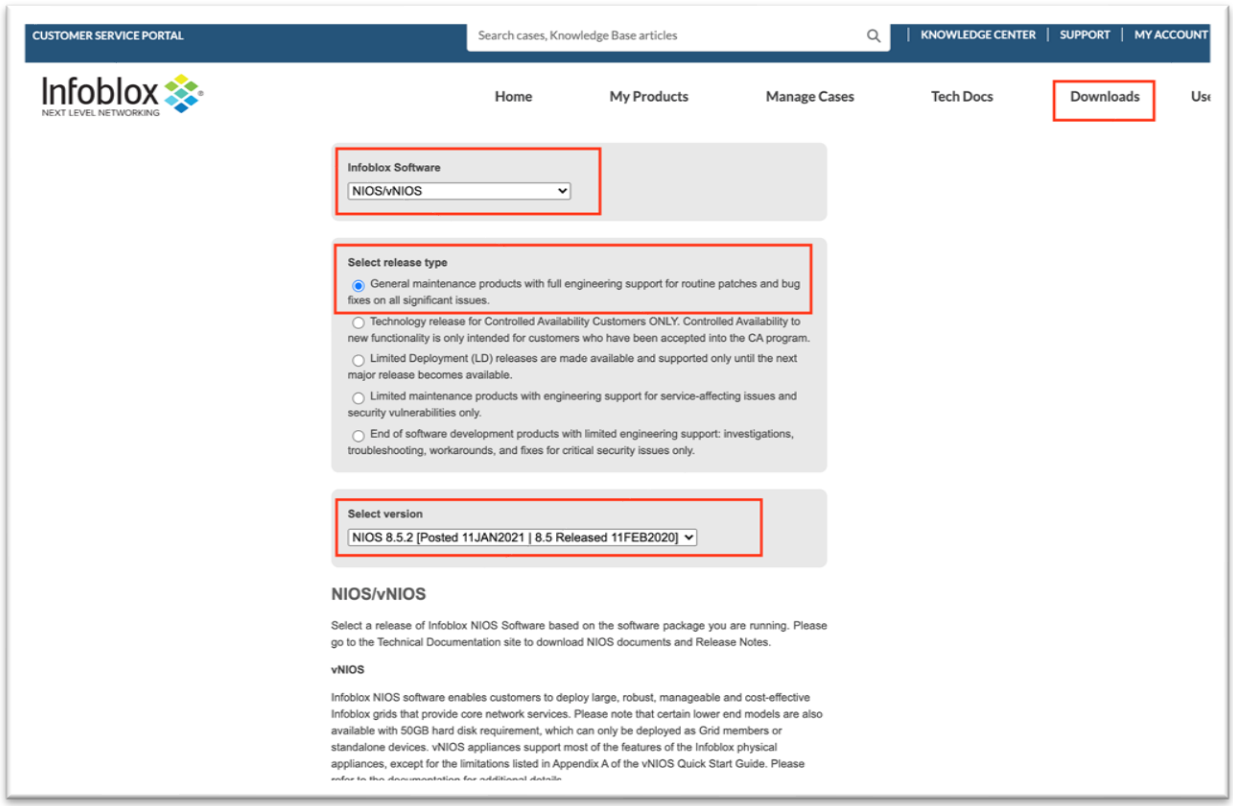
Configuring Infoblox Grid

Pre-requisites for Grid Environment

1. VMware vSphere environment
   The Infoblox vNIOS on VMware software can run on ESX or ESXi servers that have DAS (Direct Attached Storage), or iSCSI (Internet Small Computer System Interface) or FC (Fibre Channel) SAN (Storage Area Network) attached.
   You can install the vNIOS software package on a host with VMware ESX or ESXi 6.7, 6.5.x, 6.0.x, 5.5.x, 5.1.x, or 5.0.x installed, and then configure it as a virtual appliance.
   vSphere vMotion is also supported. You can migrate vNIOS virtual appliances from one ESX or ESXi server to another without any service outages. The migration preserves the hardware IDs and licenses of the vNIOS virtual appliances.
   VMware Tools is automatically installed for each vNIOS virtual appliance. Infoblox supports the control functions in VMware Tools. For example, through the vSphere client, you can shut down the virtual appliance. You can deploy certain vNIOS virtual appliances with different hard disk capacities.
   Some vNIOS appliances are not supported as Grid Masters or Grid Master Candidates. For more information about vNIOS on VMware, refer to the Infoblox Installation Guide for vNIOS Software on VMware.
2. Grid Master (deployed on VMware with Flex activation license)
3. DDI images (.ova for VMware). Images can be downloaded from https://support.infoblox.com
4. Reporting server deployed and added to the grid.

Downloading the required images (For VMware)
IB-FLEX images can be downloaded from the Infoblox Support Portal.

1. Navigate to the Downloads tab
2. Select Infoblox Software as NIOS
3. Under Select version, select NIOS 8.5.2
4. Scroll down and expand vNIOS for VMware


CUSTOMER SERVICE PORTAL
Search cases, Knowledge Base articles
KNOWLEDGE CENTER | SUPPORT | MY ACCOUNT
Infoblox
NEXT LEVEL NETWORKING
Home
My Products
Manage Cases
Tech Docs
Downloads
Infoblox Software
NIOS/vNIOS
Select release type
General maintenance products with full engineering support for routine patches and bug fixes on all significant issues.
Technology release for Controlled Availability Customers ONLY. Controlled Availability to new functionality is only intended for customers who have been accepted into the CA program.
Limited Deployment (LD) releases are made available and supported only until the next major release becomes available.
Limited maintenance products with engineering support for service-affecting issues and security vulnerabilities only.
End of software development products with limited engineering support: investigations, troubleshooting, workarounds, and fixes for critical security issues only.
Select version
NIOS 8.5.2 [Posted 11JAN2021 | 8.5 Released 11FEB2020]
NIOS/vNIOS
Select a release of Infoblox NIOS Software based on the software package you are running. Please go to the Technical Documentation site to download NIOS documents and Release Notes.
vNIOS
Infoblox NIOS software enables customers to deploy large, robust, manageable and cost-effective Infoblox grids that provide core network services. Please note that certain lower end models are also available with 50GB hard disk requirement, which can only be deployed as Grid members or standalone devices. vNIOS appliances support most of the features of the Infoblox physical appliances, except for the limitations listed in Appendix A of the vNIOS Quick Start Guide. Please

NIOS 8.5.x is not supported on the following appliances: IB-250, IB-250-A, IB-500, IB-550, IB-550-A, IB-1000, IB-1050, IB-1050-A, IB-1550, IB-1550-A, IB-1552, IB-1552-A, IB-1852-A, IB-2000, IB-2000-A, IB-VM-250, IB-VM-550, IB-VM-1050, IB-VM-1550, IB-VM-1850, IB-VM-2000, and Trinzic Reporting TR-2000 and TR2000-A series appliances. You cannot upgrade to NIOS 8.5 on these appliances. See Upgrade Guidelines in this document for additional upgrade information.

▸ **NIOS**

▾ **vNIOS for VMware**

The Infoblox vNIOS on VMware software can run on ESX or ESXi servers that have DAS (Direct Attached Storage), or iSCSI (Internet Small Computer System Interface) or FC (Fibre Channel) SAN (Storage Area Network) attached. You can install the vNIOS software package on a host with VMware ESX or ESXi 6.7, 6.5.x, 6.0.x, 5.5.x, 5.1.x, or 5.0.x installed, and then configure it as a virtual appliance.

The vNIOS and vDiscovery resizable images give you the option to define the allocated amount of storage for vNIOS and vDiscovery. This optimizes the resource footprint during situations in which the standard image is not adequate starting at 68GB. You must use the resizeable image only if explicitly recommended by Infoblox Professional Services or System Engineering.

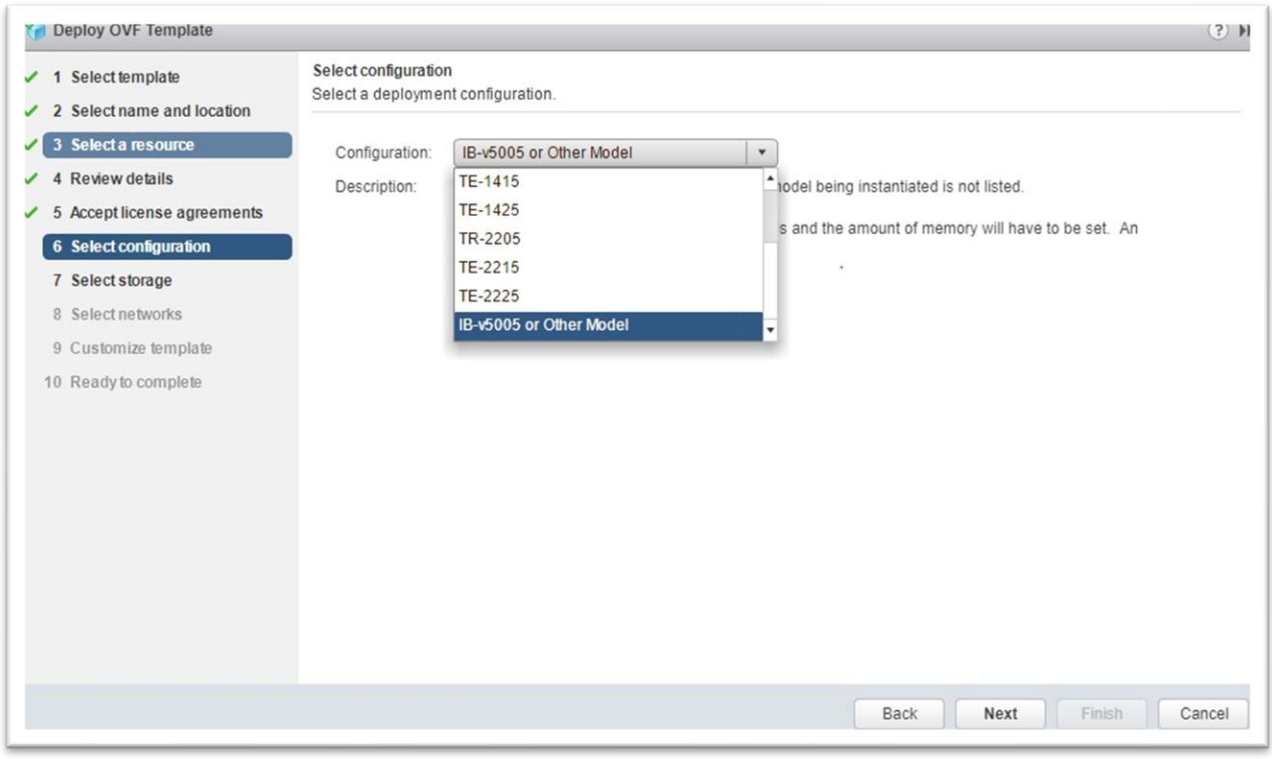
Grid Role	An Open Virtual Appliance (or Application) (.ova) single file distribution package	Link to Download Images
Member, Grid Master, Reporting	**DDI:v815, v825, v1415, v1425, v2215, v2225, v4015, v4025, Flex, Reporting: v805, v1405, v2205, v5005 and CP: v805, v1405, v2205**	**Download Image**
Resizable of Member, Grid Master, Reporting	**DDI:v815, v825, v1415, v1425, v2215, v2225, v4015, v4025, Flex, Reporting: v805, v1405, v2205, v5005 and CP: v805, v1405, v2205**	**Resizable Download Image**
Discovery	**Discovery: ND-v805, ND-v1405, ND-v2205, ND-v4005**	**Download Image**
Resizable of Discovery	**Discovery: ND-v805, ND-v1405, ND-v2205, ND-v4005**	**Resizable Download Image**

Installing IB-FLEX on VMware

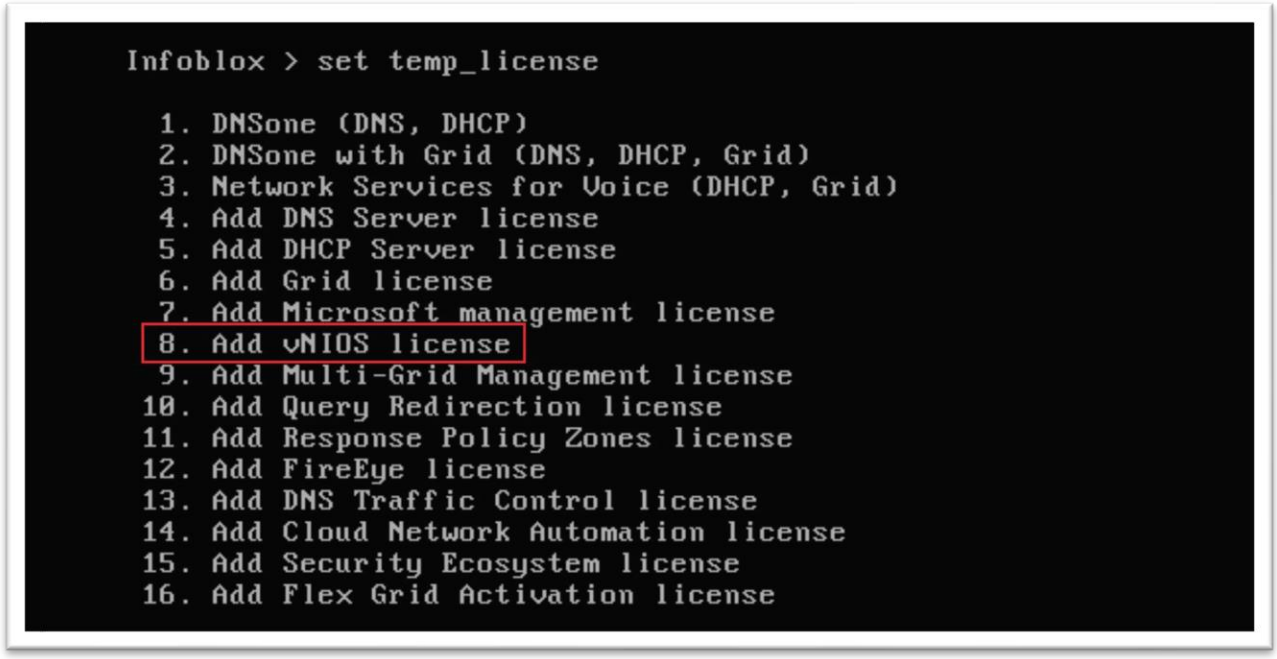
This section walks you through installing and managing IB-FLEX appliances on VMware Lorem simply dummy text of the printing and typesetting industry

Deploying Grid Master

1. Deploy the NIOS OVF template downloaded from the Infoblox Support site.
2. During the OVF deployment, please select the IB-Appliance model.
   In this example we have used IB-v825 as the Grid Master model.



3. Type **set temp_license** and enter **8** to assign vNIOS license.



```
Select license (1-17) or q to quit: 4

 1. IB-V805
 2. CP-V805
 3. IB-V815
 4. IB-V825
 5. IB-V1405
 6. CP-V1405
 7. IB-V1415
 8. IB-V1425
 9. IB-V2205
10. CP-V2205
11. IB-V2215
12. IB-V2225
13. IB-V4005
14. IB-V4015
15. IB-V4025
16. IB-V5005

Enter a number corresponding to a NIOS model (1 - 16) or q to quit: 5
```

4. Set the networking using **set network** command and configure it as Grid Master

```
Infoblox > set network
NOTICE: All HA configuration is performed from the GUI.  This interface is
        used only to configure a standalone node or to join a Grid.
Enter IP address: 10.10.10.2
Enter netmask [Default: 255.255.255.0]:
Enter gateway address [Default: 10.10.10.1]:
Enter VLAN tag [Default: Untagged]:
Configure IPv6 network settings? (y or n): n
Become grid member? (y or n): n

 New Network Settings:
  IPv4 address:         10.10.10.2
  IPv4 Netmask:         255.255.255.0
  IPv4 Gateway address: 10.10.10.1
  IPv4 VLAN tag:        Untagged

 Old IPv4 Network Settings:
  IPv4 address:         192.168.1.2
  IPv4 Netmask:         255.255.255.0
  IPv4 Gateway address: 192.168.1.1
  IPv4 VLAN tag:        Untagged
        Is this correct? (y or n): y
```

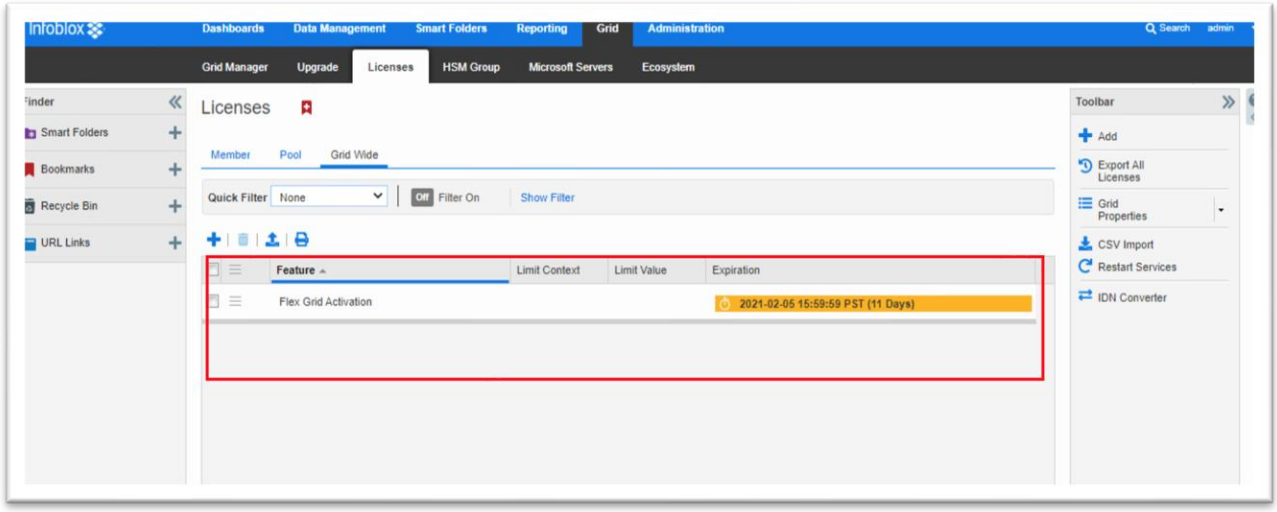
5. Navigate to the licensing option again by typing **set temp_license** .
   Type **17** to activate Flex Grid Activation License.

```
Infoblox > set temp_license

 1. DNSone (DNS, DHCP)
 2. DNSone with Grid (DNS, DHCP, Grid)
 3. Network Services for Voice (DHCP, Grid)
 4. Add NIOS License
 5. Add DNS Server license
 6. Add DHCP Server license
 7. Add Grid license
 8. Add Microsoft management license
 9. Add Multi-Grid Management license
10. Add Query Redirection license
11. Add Response Policy Zones license
12. Add FireEye license
13. Add DNS Traffic Control license
14. Add Cloud Network Automation license
15. Add Security Ecosystem license
16. Add Threat Analytics license
17. Add Flex Grid Activation license

Select license (1-17) or q to quit: 17
```

6. You will get following prompt. Type **y** for yes and hit enter.

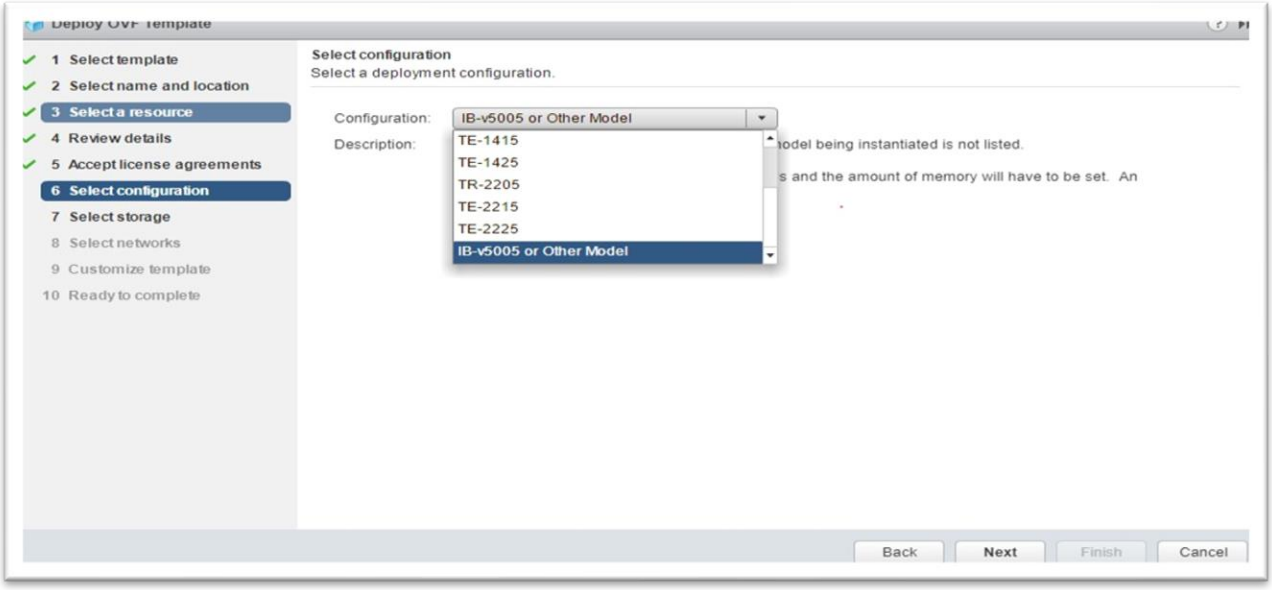
```
Select license (1-17) or q to quit: 17

The Flex Grid Activation license will be effective only if there is an IB-FLEX m
ember in the Grid . Adding license(s) will restart IB-FLEX members, if any, in t
he Grid.


Are you sure you want to proceed? (y or n): y_
```

7. To verify the Flex Grid Activation license, login to the Grid GUI and navigate to **Grid→ Licenses → Grid Wide**

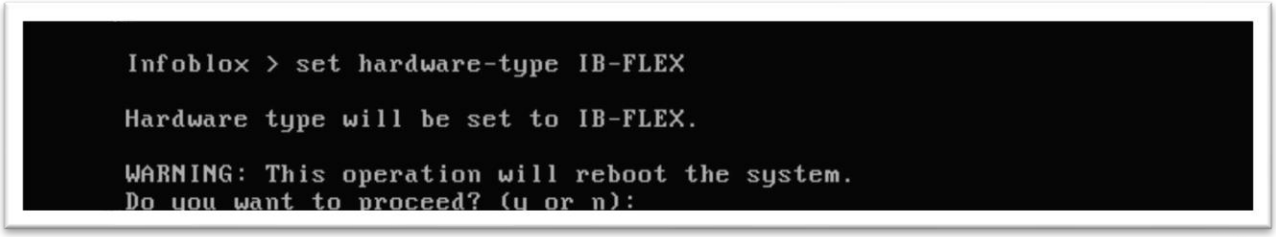


Adding an IB-FLEX member to the Grid

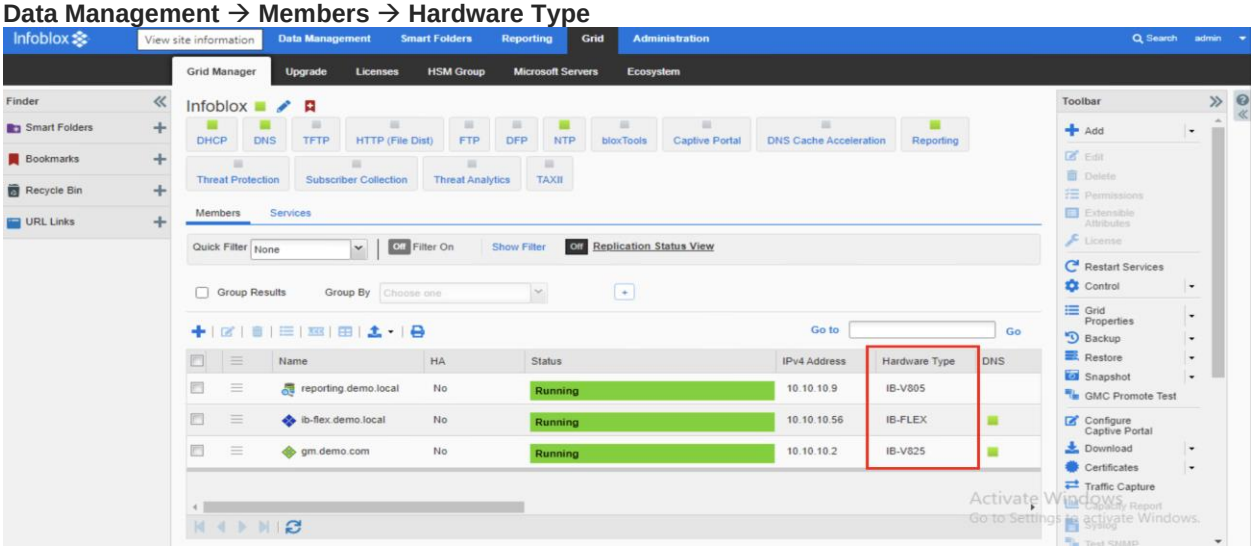
1. Deploy a NIOS instance from the previously downloaded NIOS OVF template.
2. During the deployment, select the desired NIOS model.



3. After NIOS VM boots up, log in at the command prompt and type **set hardware-type IB-FLEX**



4. After reboot set the networking and add the NIOS to the grid using **set network** command.
5. You can verify the IB-FLEX member type in the grid by navigating to **Grid→ Grid Manager → Data Management → Members → Hardware Type**



6. IB-FLEX license can also be verified by using **show hardware-type** command.

```
Infoblox > show hardware-type
Member hardware type: IB-FLEX
Infoblox > _
```

Enabling and configuring Parental Control

This deployment guide assumes that you have an Infoblox grid with a Grid-master, an IB-FLEX member running DNS service and a reporting appliance already deployed. For deploying reporting server, refer to following link.

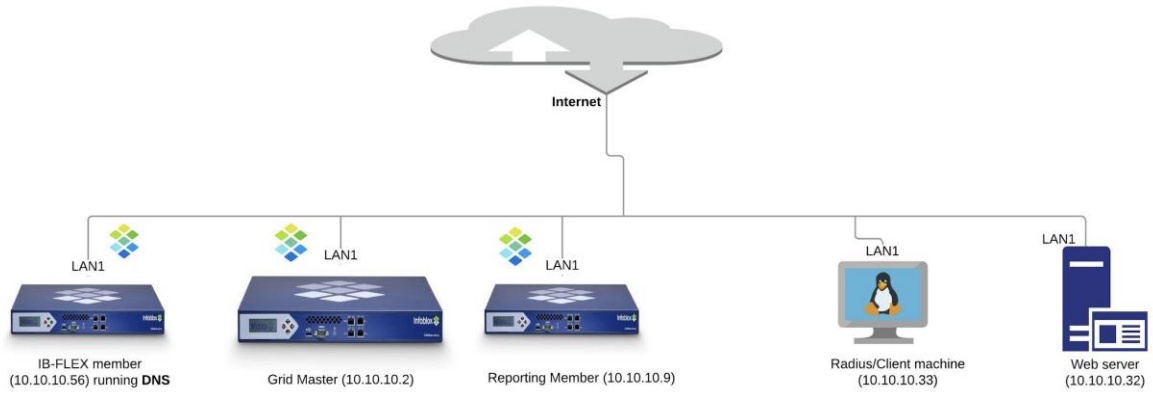
Pre-requisites to enable Parental Control

- Grid-master must have internet access.
- Content Categorization database credentials.
- Grid must be configured with a DNS resolver that can resolve public URLs.
- Grid DNS resolver must be configured with the loopback.
- DNS members must be configured with RPZ logging.

Lab Architecture

The following diagram depicts an example deployment of Parental Control.

- Grid master, member, and reporting appliance are connected over LAN1 network.
- We have a web server (ubuntu based machine) hosting blocking page and a client machine (ubuntu-desktop based machine) running Infoblox radius server, also connected to the same network (LAN1).
    - Client machine serves dual purpose. It is used to initiate the radius messages and is also used to test the parental control functionality.
- Both webserver and client-machine have internet access.



The Workflow

1. Client machine sends the radius messages to the Infoblox DNS server which acts as a Radius Collector.
2. Once the Infoblox DNS server receives the radius message containing information about a subscriber id and the corresponding parental control policy, it updates its subscriber cache.

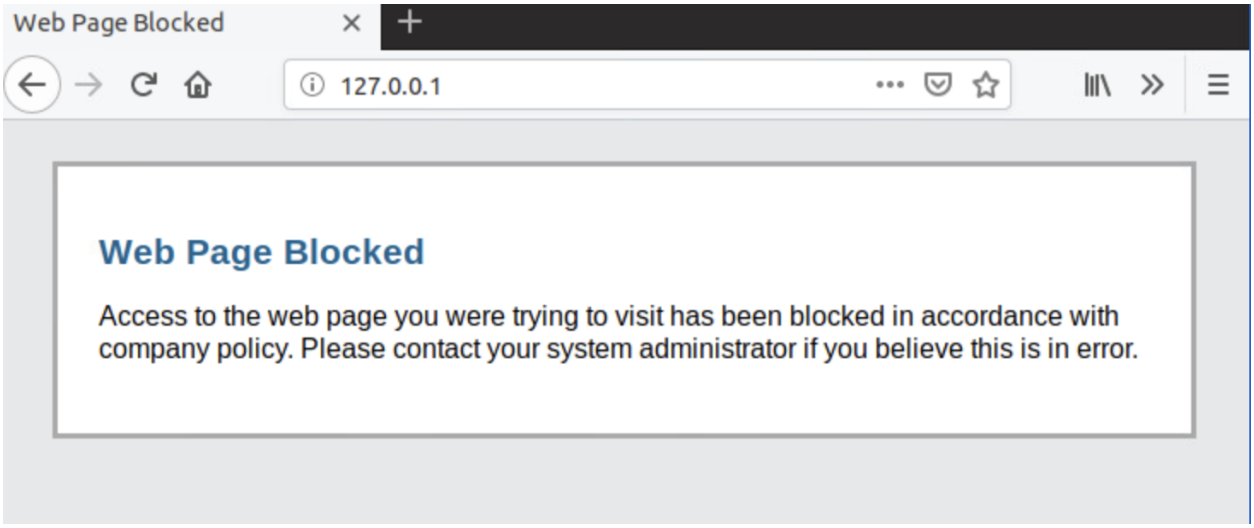
3. DNS queries are evaluated against this cache and in case subscriber is trying to access a restricted site, access is blocked, and blocking page is presented.
4. These violations are captured by the reporting appliance, which displays a detailed report about the time of violation, accessed website and the subscriber ID.

Preparing Webserver to host and render Blocking page

1. Login to the web server (ubuntu based machine) as a root user.
2. Execute **`apt-get update`** command to update the package list.
3. Execute **`apt-get install apache2`** to install a webserver.
4. Download the blocking page html file by executing **`git clone https://github.com/infobloxopen/parental_control.git`** . This git clone command will create a directory → **`parental_control`** .
5. Navigate to the **`parental_control`** directory using the command **cd** **`parental_control`** . You should see following files using the command **ls**:

    - dictionary.infoblox
    - **freeradius-server-3.0.9.tar**
    - **index.html**
    - rad_msg.txt

6. Move this index.html file to **`/var/www/html`** location by executing **`mv index.html /var/www/html/`**
7. Restart the web server by executing **`/etc/init.d/apache2 restart`** command.
8. Verify if the blocking page is working by typing the loopback IP on the Web Server Browser:



Installing Infoblox Radius client

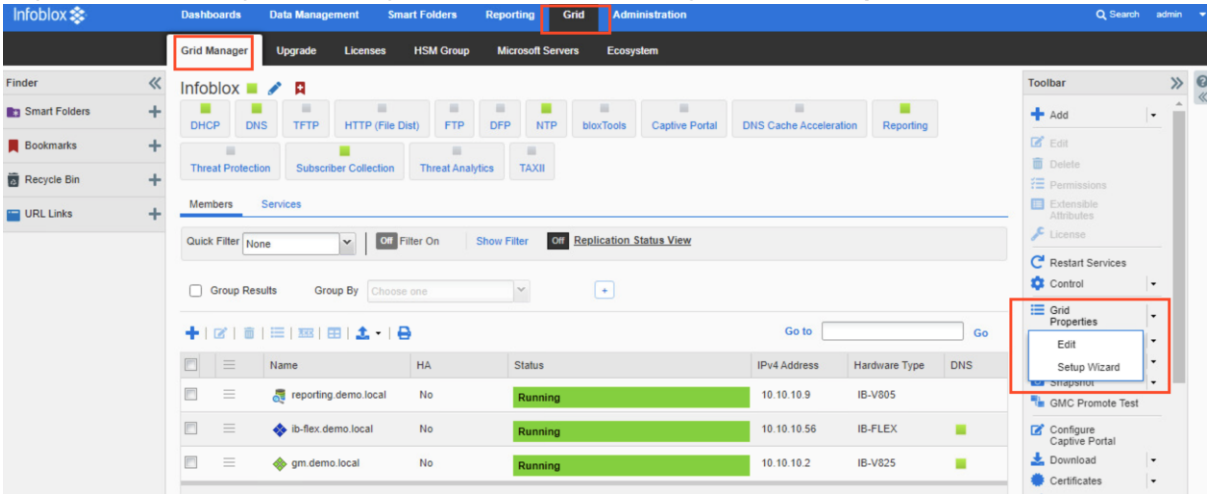
1. Login to the client machine (ubuntu desktop-based machine) as a root user.
2. Run **`apt-get update`** command to update the package list.
3. Create a folder and name it as **`infoblox-radius`**. Navigate to this folder by running **`cd`** command.

4. Download talloc library tar file by executing **wget https://www.samba.org/ftp/talloc/talloc-2.1.0.tar.gz**
5. Untar the talloc library by executing **tar -xvf talloc-2.1.0.tar.gz**
6. Change directory and navigate to the talloc library folder by running **cd talloc-2.1.0**
7. Run **./configure** to initiate the dependency test.
    a. (Please ensure that the machine has build-essential installed, if it's not then use this command to do that **apt-get install build-essential**)
8. Run **make** command to start the build process.
9. Run **make install** command to finalize the installation.
10. Come out of the talloc-2.1.0 folder by running **cd ..** command.
11. Run **git clone https://github.com/infobloxopen/parental_control.git** to download the infoblox radius server packages. This git clone command will create a directory→ **parental_control**.
12. Navigate to this folder by running cd command. You should see following files:
    a. dictionary.infoblox
    b. freeradius-server-3.0.9.tar
    c. index.html
    d. rad_msg.txt
13. Untar the freeradius-server-3.0.9.tar file by running **tar -xvf freeradius-server-3.0.9.tar**
14. Navigate to the freeradius-server-3.0.9 folder, by running **cd freeradius-server-3.0.9**
15. Copy the dictionary.infoblox file which we downloaded in step 12 to the ./share directory by running **cp ../dictionary.infoblox ./share/**
16. Run **./configure --with-openssl=no** to initiate the dependency test.
17. Run **make** command to start the build process.
18. Run **make install** command to finalize the installation.
19. Verify that Infoblox radius client is installed by running **radclient** at the command prompt, you should be able to view the different arguments:

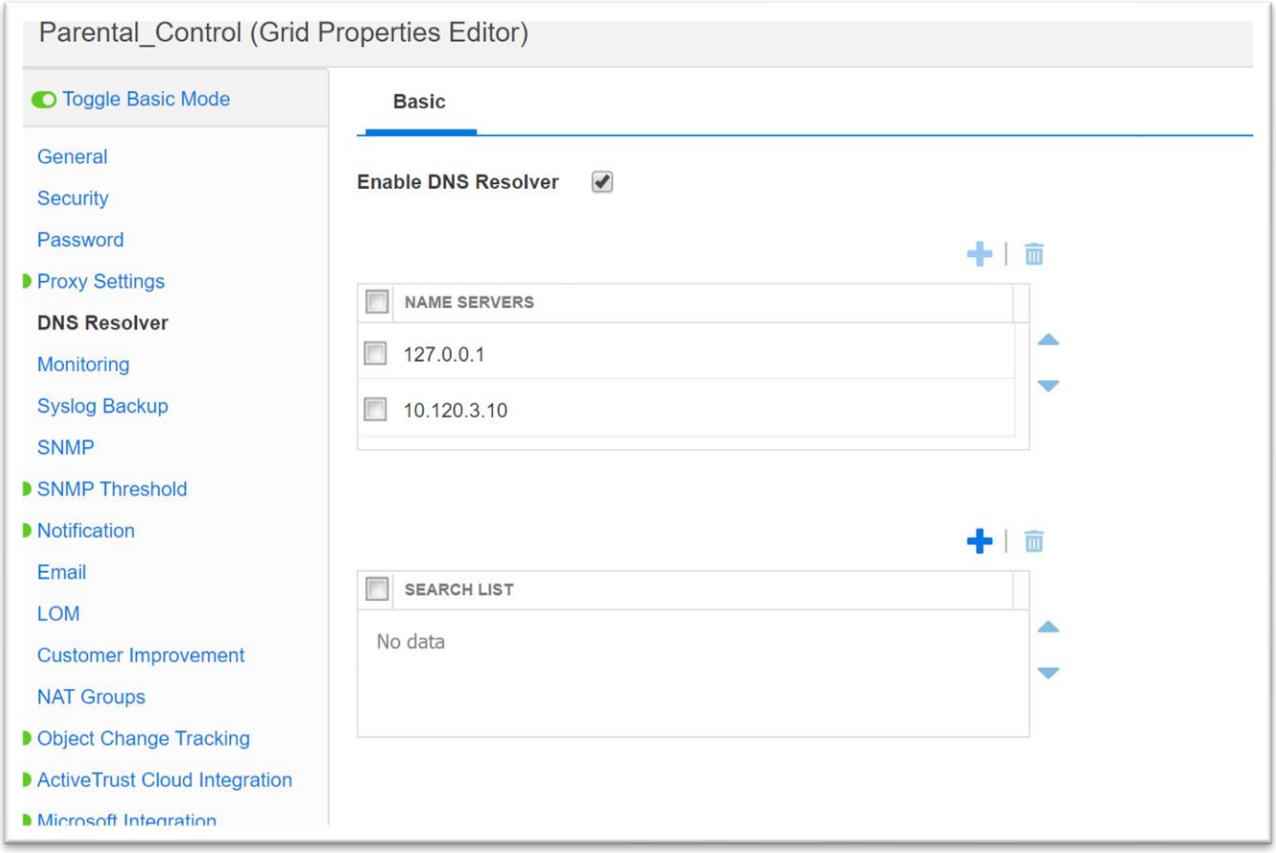
```
root@infoblox-virtual-machine:~/Infoblox-radius/parental_control# radclient
radclient: Insufficient arguments
Usage: radclient [options] server[:port] <command> [<secret>]
  <command>              One of auth, acct, status, coa, disconnect or auto.
  -4                     Use IPv4 address of server
  -6                     Use IPv6 address of server.
  -c <count>             Send each packet 'count' times.
  -d <raddb>             Set user dictionary directory (defaults to /etc/freerad
ius/3.0).
  -D <dictdir>           Set main dictionary directory (defaults to /usr/share/f
reeradius).
  -f <file>[:<file>]     Read packets from file, not stdin.
                         If a second file is provided, it will be used to verify
 responses
  -F                     Print the file name, packet number and reply code.
  -h                     Print usage help information.
  -i <id>                Set request id to 'id'.  Values may be 0..255
  -n <num>               Send N requests/s
  -p <num>               Send 'num' packets from a file in parallel.
  -q                     Do not print anything out.
  -r <retries>           If timeout, retry sending the packet 'retries' times.
  -s                     Print out summary information of auth results.
```

Configuring and enabling Parental Control

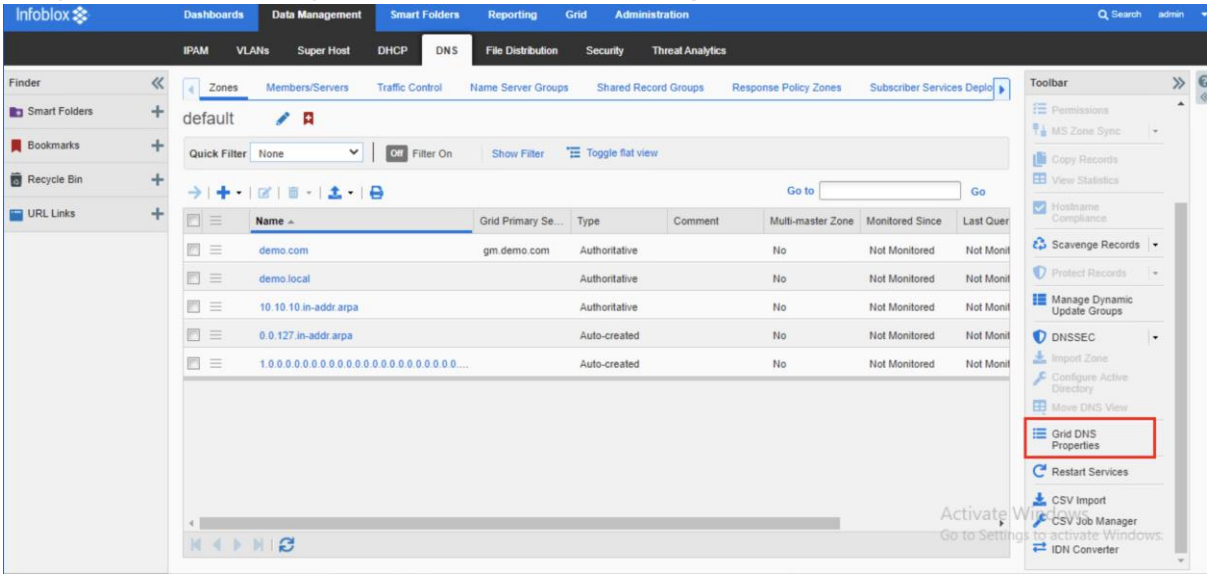
1. Login to the Infoblox grid and navigate to **Grid → Grid-Manager → Grid Properties →Edit**



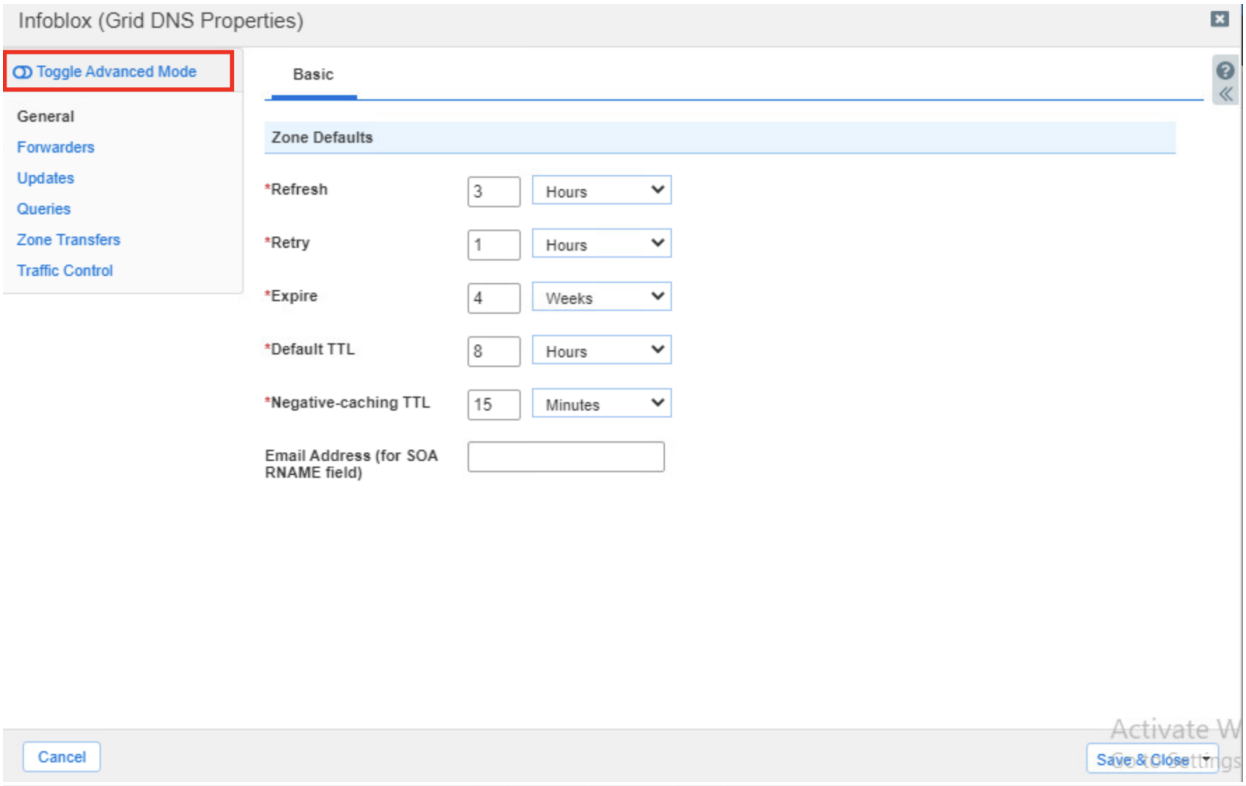
2. Navigate to the **DNS Resolver** option and click on + icon to enter the DNS resolvers. Please ensure that the first DNS resolver IP should be the loopback IPV4 address. Click on **Save & close**.

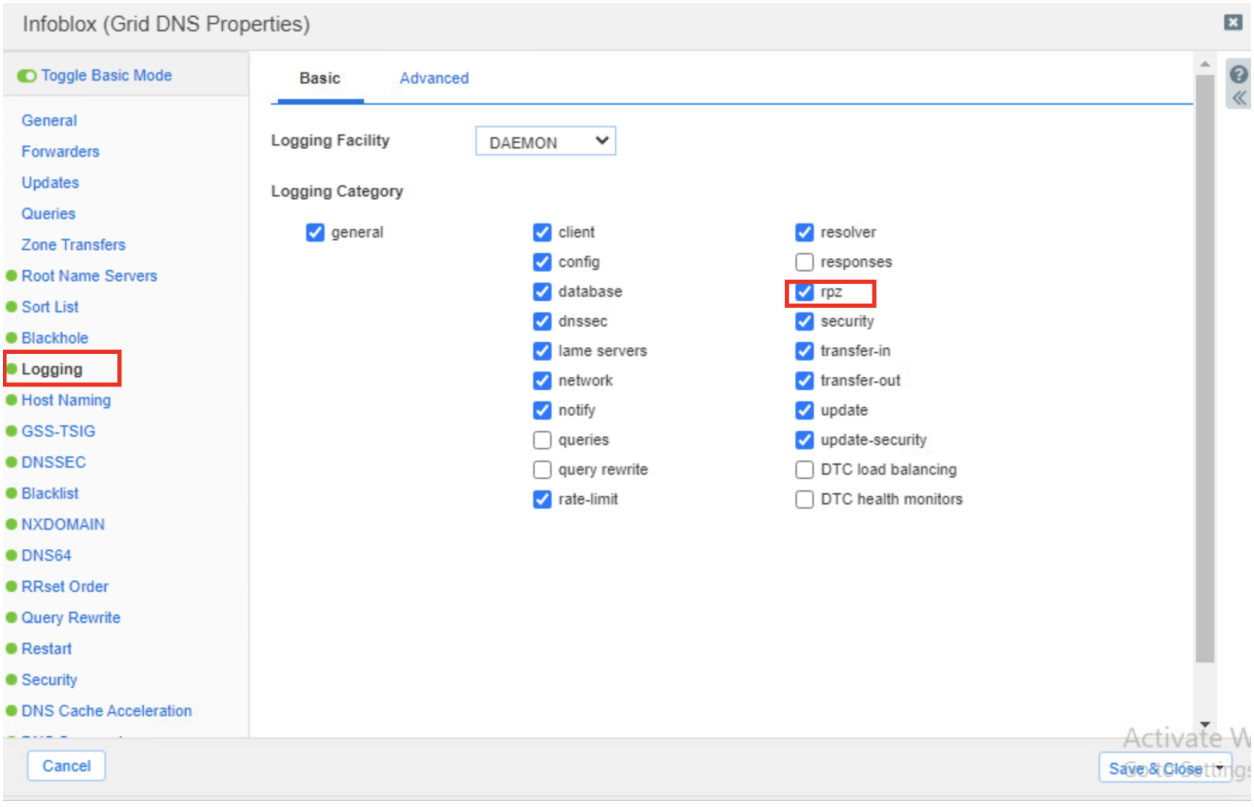


3. Navigate to the **Data Management → DNS → Grid DNS Properties.**

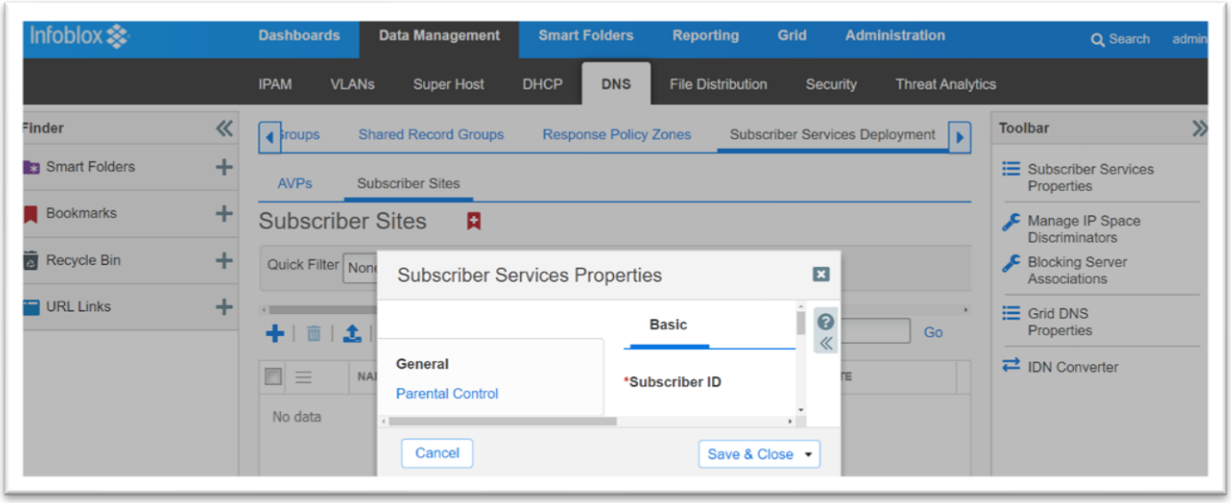


4. Click on **Toggle Advanced Mode** and then click on **Logging** and check **rpz** option to enable rpz logging.

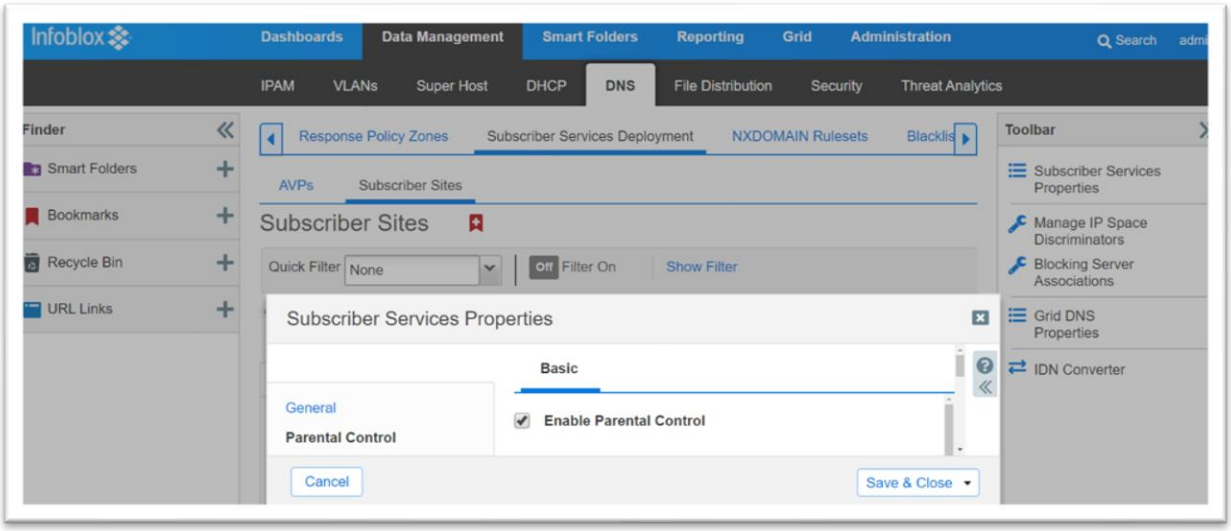

Infoblox (Grid DNS Properties)
Toggle Advanced Mode
General
Forwarders
Updates
Queries
Zone Transfers
Traffic Control
Basic
Zone Defaults
*Refresh
3
Hours
*Retry
1
Hours
*Expire
4
Weeks
*Default TTL
8
Hours
*Negative-caching TTL
15
Minutes
Email Address (for SOA RNAME field)
Cancel
Save & Close


Infoblox (Grid DNS Properties)
Toggle Basic Mode
General
Forwarders
Updates
Queries
Zone Transfers
Root Name Servers
Sort List
Blackhole
Logging
Host Naming
GSS-TSIG
DNSSEC
Blacklist
NXDOMAIN
DNS64
RRset Order
Query Rewrite
Restart
Security
DNS Cache Acceleration
Basic
Advanced
Logging Facility
DAEMON
Logging Category
general
client
config
database
dnssec
lame servers
network
notify
queries
query rewrite
rate-limit
resolver
responses
rpz
security
transfer-in
transfer-out
update
update-security
DTC load balancing
DTC health monitors
Cancel
Save & Close

5. Navigate to the **Data Management → DNS → Subscriber Services Deployment → Subscriber Sites → Subscriber Services Properties → Parental Control**

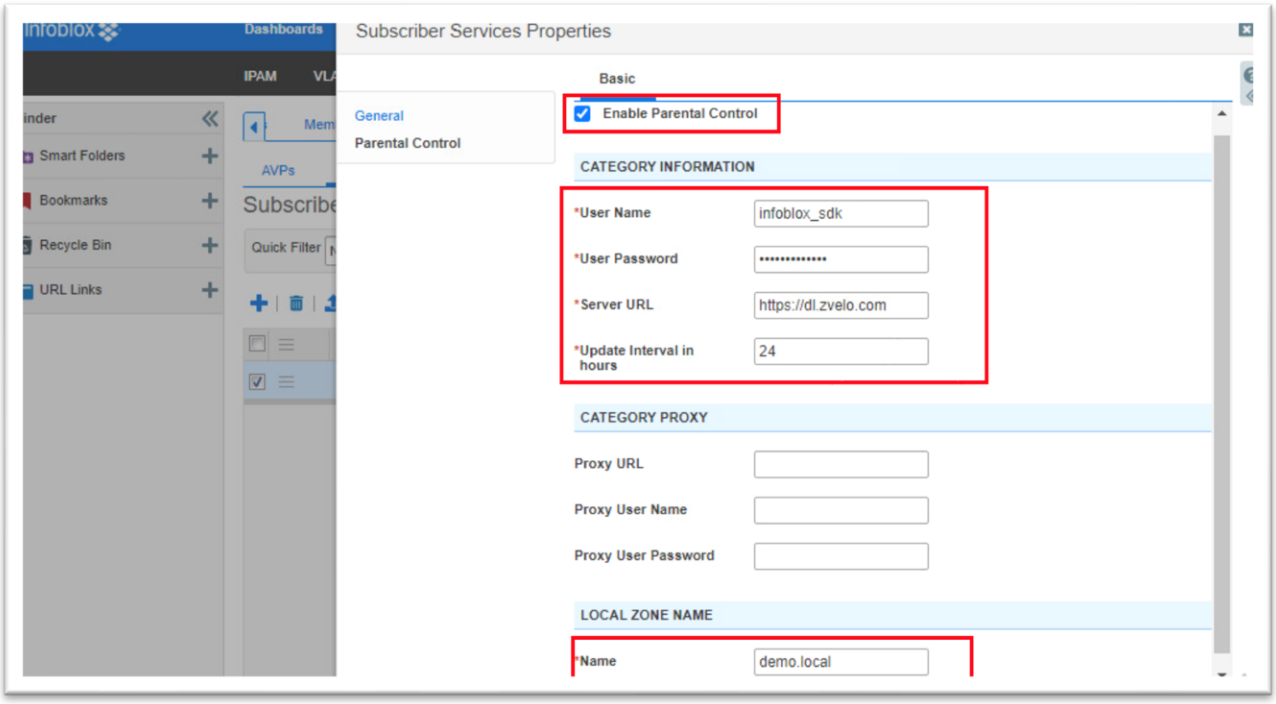


6. Navigate to the **Parental Control** option and check **Enable Parental Control** option.



7. Enter Content Categorization database credentials. These credentials can be obtained either from Infoblox accounts team or from a reseller.
8. Please ensure that **Server URL** is pointing ***https://dl.zvelo.com***
9. Enter a **LOCAL ZONE NAME.**

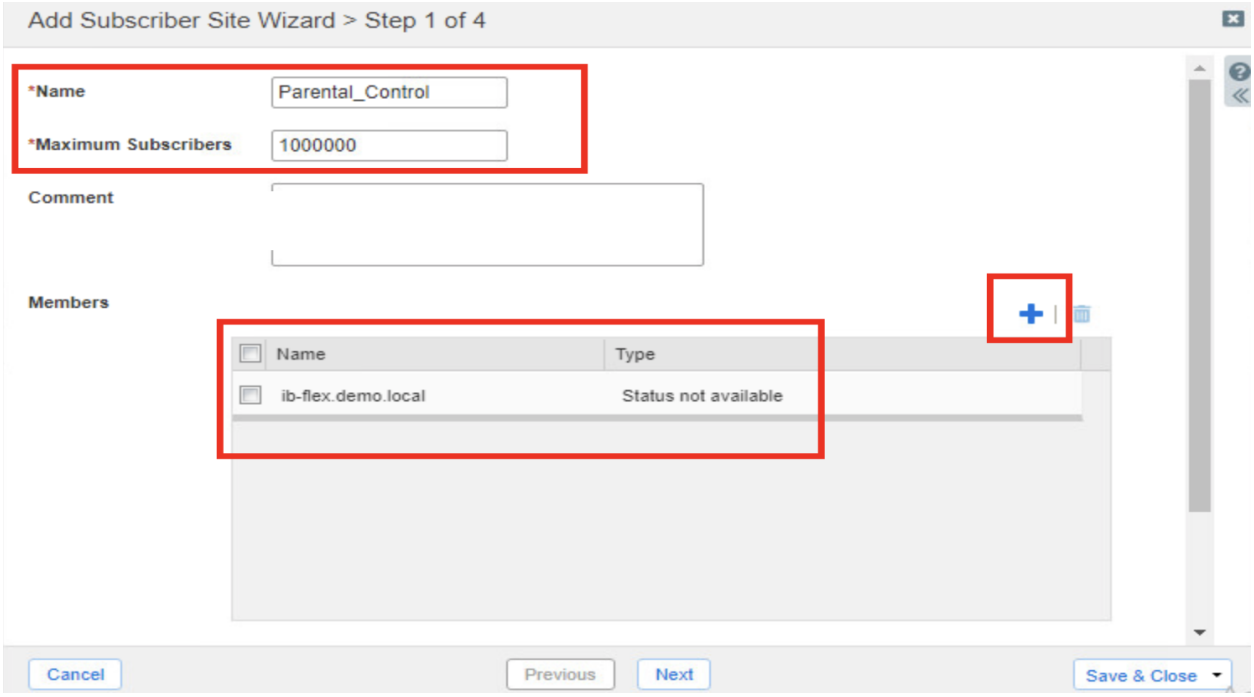
10. Click on **Save and close.**



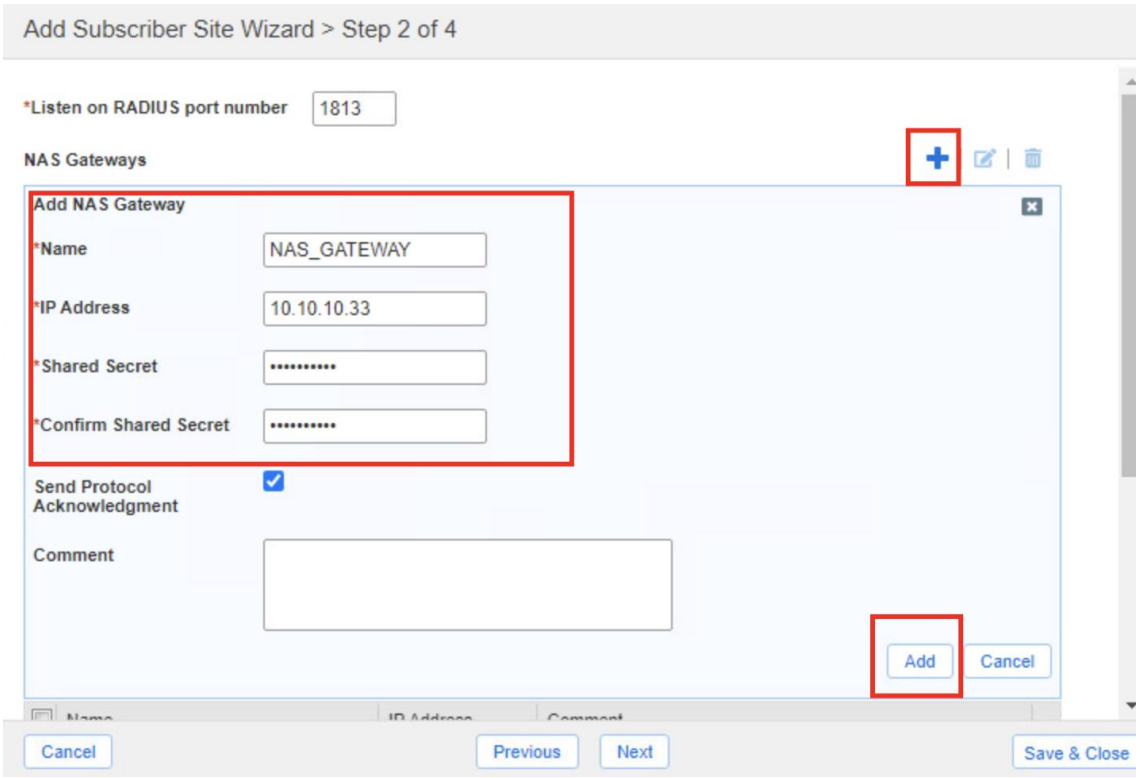
11. You will be prompted to click on restart, to implement the configuration change.

12. Navigate to **Data Management → DNS → Subscriber Services Deployment → Subscriber Sites** and click on **+** icon**.**

13. Enter Subscriber Site details like subscriber site **Name**, **Maximum Subscribers** and add grid members running DNS service.

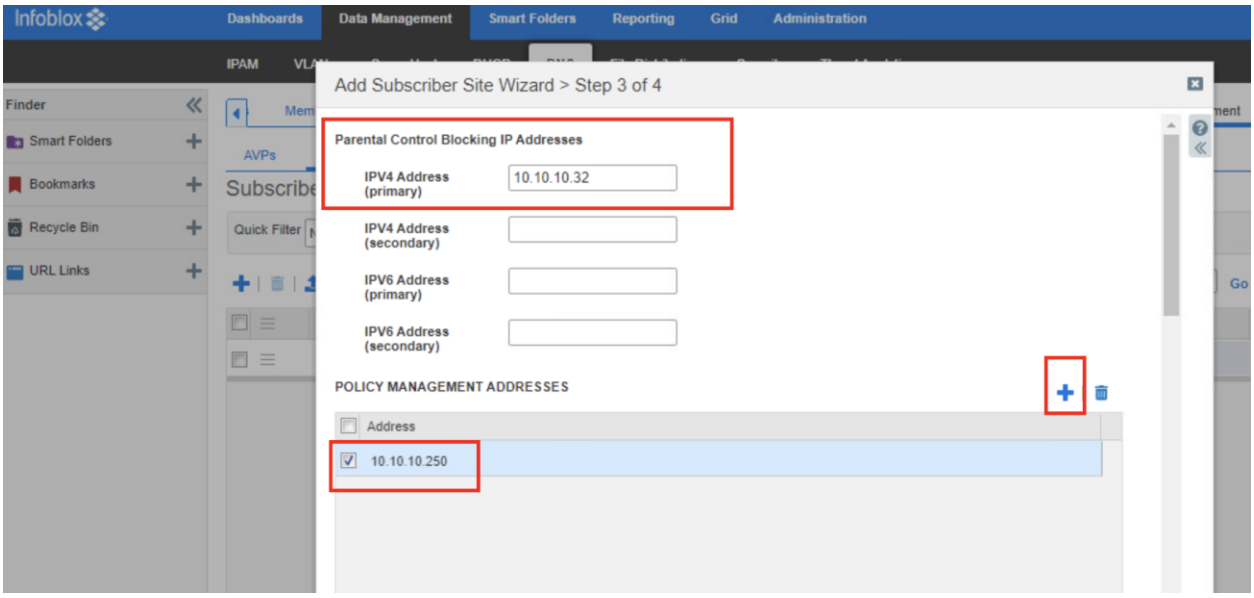


14. Enter the **IP address**, **Name** and the **shared secret (testing123)** for the Linux machine running Infoblox rad client and click on **Add.** Click on **Next**.

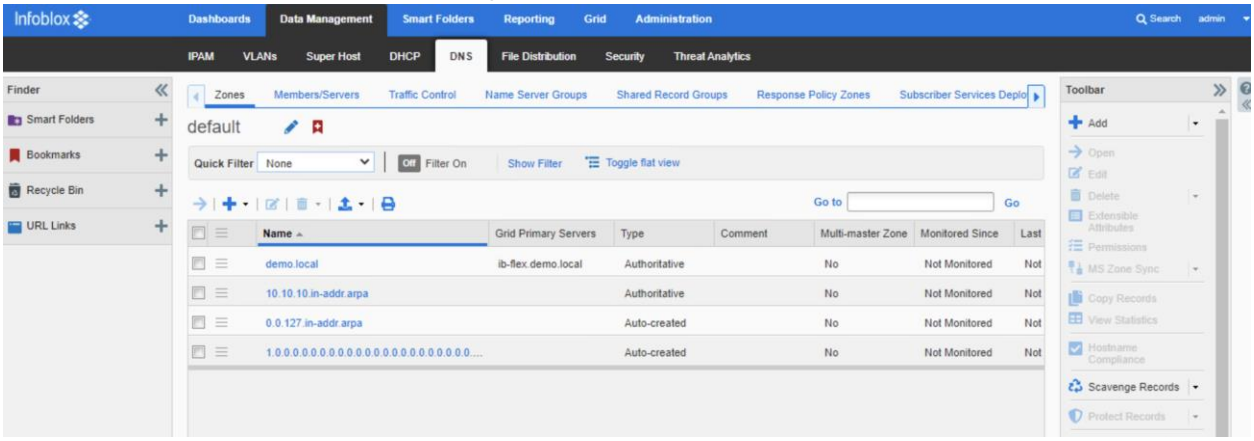


15. Under **Parental Control Blocking IP Addresses** option, enter the IP address of the Linux machine running webserver and hosting Blocking page. Under **Policy Management Addresses** option give a dummy IP. Under **Content Proxy Addresses** enter the same dummy IP. Click on **Save and Close**

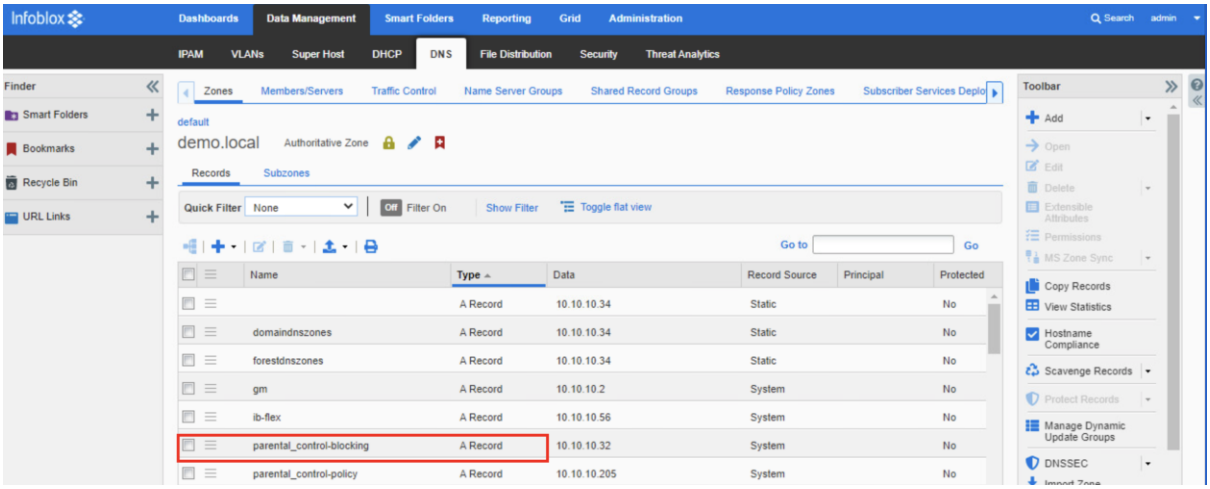
a. **Note**: *This deployment guide covers Parental control configuration without Multi Site Proxy (MSP) and hence dummy IPs are entered under Policy Management and Content Proxy Addresses.*



16. Navigate to **Data Management → DNS → Zones.** You will see a zone, with the name which we entered under **LOCAL ZONE NAME**, in step 9. Click on it to access the records.

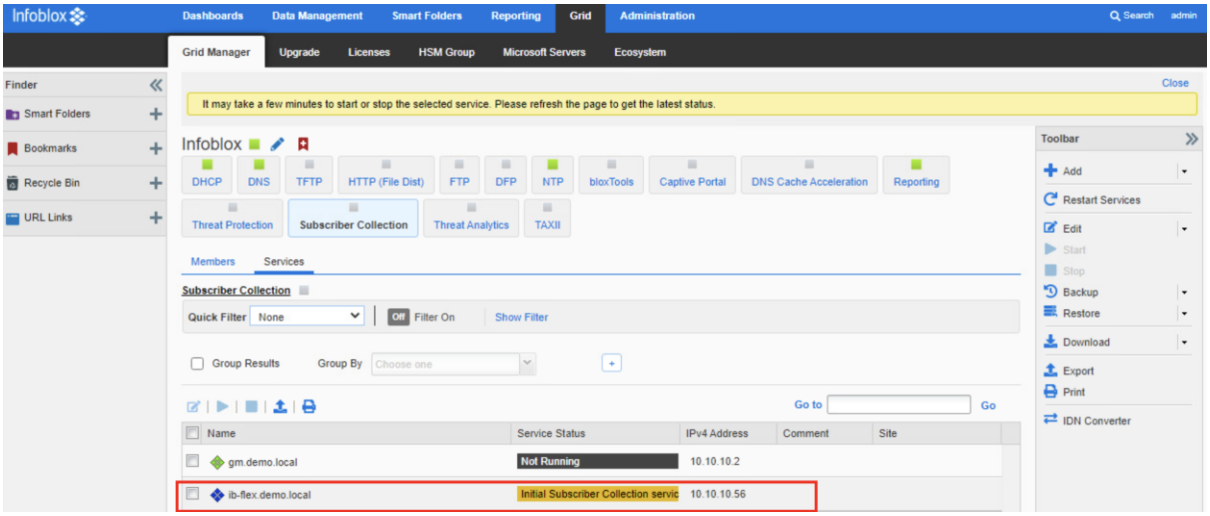


17. You will find a DNS A record for the **Blocking Server**. This record will be used to render the Blocking server webpage.

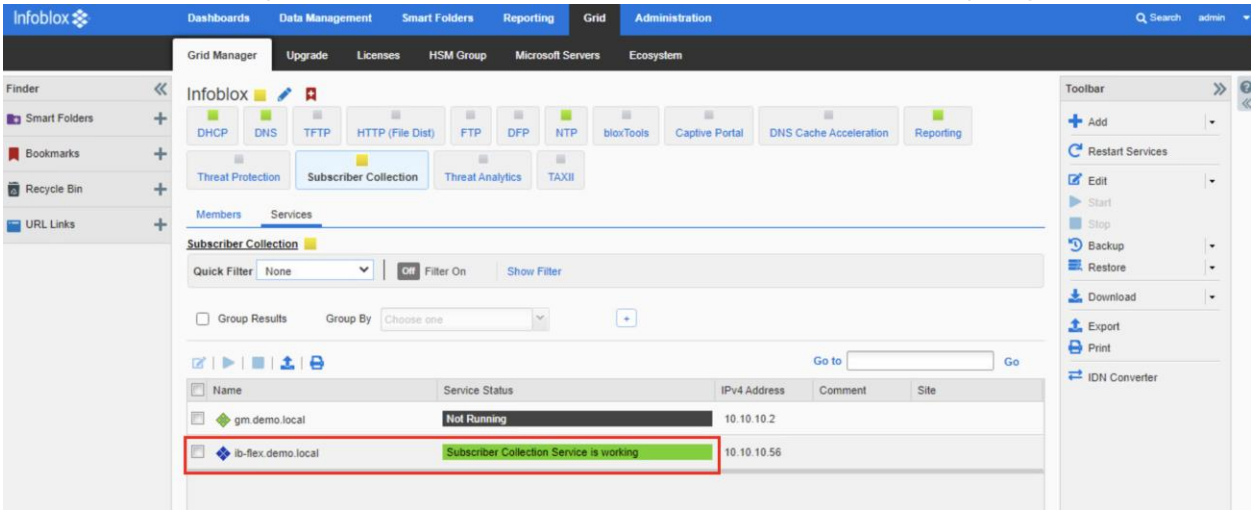


18. Navigate to **Grid → Grid Manager → Services → Subscriber Collection**. Check the members which are running DNS service and click on the Start button to start subscriber collection service.
19. You will be prompted to click on Restart to implement the configuration changes.

20. After clicking on restart, Subscriber collection will get started. Once started, Grid master starts downloading the Content Categorization database.
This database is close to 5.7 GB in size and takes about 4-5 hours to download.

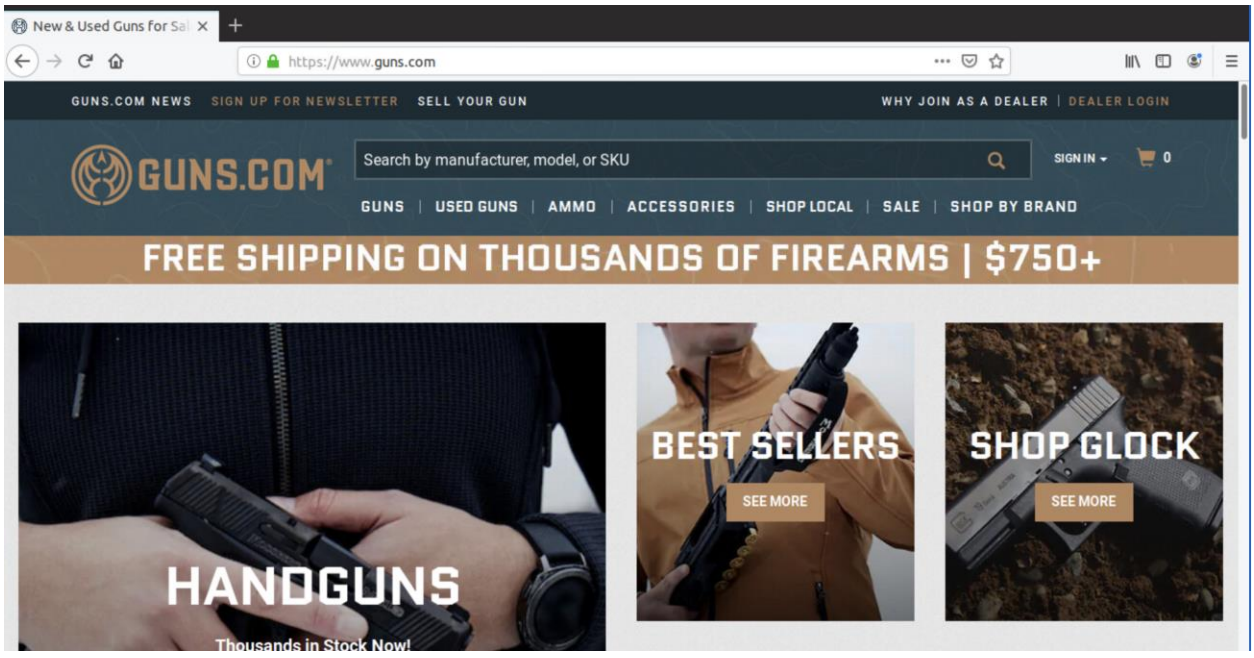


21. Once the Content Categorization database download is finished, members will show up as **green**.



Validating Parental Control functionality

1. Login to the client machine, open a web browser and go to the website www.guns.com , to make sure that you can open it.



2. Access the client machine via ssh and navigate to the **parental_control** folder present under **infoblox_radius** directory.
3. Open the rad_msg.txt file using your preferred editor (like vi) and add following AVPs Attribute Value Pairs) (Remove all the existing AVPs.

```
Packet-Type=4
Packet-Dst-Port=1813
Acct-Session-Id = "9999732d-34590e08"
Acct-Status-Type = Start
```

```
#Acct-Status-Type = INTERIM
#Acct-Status-Type = Stop
Acct-Authentic = RADIUS
NAS-Port = 1813
NAS-IP-Address = ip_address_of_the_radius_server
Called-Station-Id = 007
Calling-Station-Id = 007
Framed-IP-Address = ip_address_of_the_client_machine
NAS-Port-Type = Wireless-802.11
Connect-Info = "CONNECT 48Mbps 802.11b"
Acct-Session-Time = 45
Infoblox-Parental-Control-
Policy=0x00200000000000000000000000020000
```

```
root@infoblox-virtual-machine:~/Infoblox-radius/parental_control# cat rad_msg.t
xt
Packet-Type=4
Packet-Dst-Port=1813
Acct-Session-Id = "9999732d-34590e08"
Acct-Status-Type = Start
#Acct-Status-Type = INTERIM
#Acct-Status-Type = Stop
Acct-Authentic = RADIUS
NAS-Port = 1813
NAS-IP-Address = 10.10.10.33
Called-Station-Id = 007
Calling-Station-Id = 007
Framed-IP-Address = 10.10.10.33
NAS-Port-Type = Wireless-802.11
Connect-Info = "CONNECT 48Mbps 802.11b"
Acct-Session-Time = 45
Infoblox-Parental-Control-Policy = 0x00200000000000000000000000020000
```

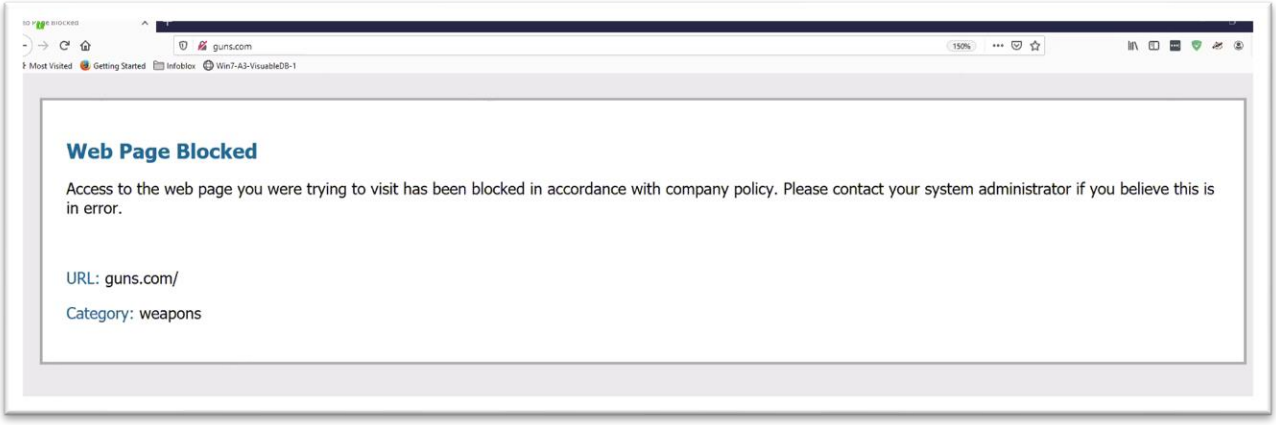
4. We will use **0x00200000000000000000000000020000** PCP bits to block guns category. To understand how this is derived, please refer to the section Parental control policy (PCP) bit for a category
5. Initiate the radius message from the client, using the following command:
   radclient *ip_address_of_infoblox_dns_appliance* **acct** *nas_shared_secret* -f rad_msg.txt

```
root@infoblox-virtual-machine:~/Infoblox-radius/parental_control# radclient 10.
10.10.56 acct testing123 -f rad_msg.txt
Sent Accounting-Request Id 227 from 0.0.0.0:43797 to 10.10.10.56:1813 length 13
9
Received Accounting-Response Id 227 from 10.10.10.56:1813 to 0.0.0.0:0 length 2
0
```

   (Note: In case the command doesn't work, check the contents of the dictionary.infoblox file and ensure that it has the required arguments. Always use the latest version of the Radclient)
6. Login to the console of the Infoblox DNS appliance and run following command to ensure subscriber information has been pushed to Infoblox DNS appliance.
   show subscriber_secure_data

```
Infoblox > show subscriber_secure_data
10.10.10.33/32¦LID:N/A¦IPS:N/A¦FLG:¦ACS:Acct-Session-Id=9999732d-34590e08;NAS:NA
S-PORT=1813;PCP:Parental-Control-Policy=0020000000000000000000000020000;PXP:PXY
_PRI=0a0a6401;PXS:PXY_SEC=0a0a6401;SUB:Calling-Station-Id=007;¦Thu Jan 28 07:23:
34 2021
```

7. Try to open guns.com website from the browser, a blocking page should pop up. This locking page is rendered by the blocking server.



8. Login to the rad client machine and open the **`rad_msg.txt`** file. Comment out the **`Acct-Status-Type = Start`** AVP and uncomment **`Acct-Status-Type = Stop`** AVP.

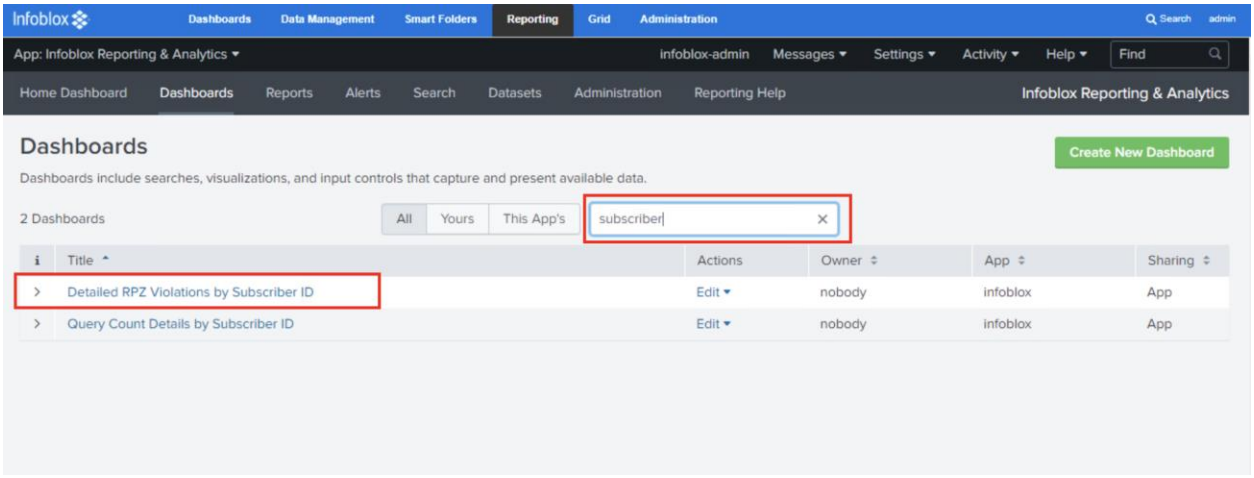
```
root@infoblox-virtual-machine:~/Infoblox-radius/parental_control# cat rad_msg.t
xt
Packet-Type=4
Packet-Dst-Port=1813
Acct-Session-Id = "9999732d-34590e08"
#Acct-Status-Type = Start
#Acct-Status-Type = INTERIM
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
NAS-Port = 1813
NAS-IP-Address = 10.10.10.33
Called-Station-Id = 007
Calling-Station-Id = 007
Framed-IP-Address = 10.10.10.33
NAS-Port-Type = Wireless-802.11
Connect-Info = "CONNECT 48Mbps 802.11b"
Acct-Session-Time = 45
Infoblox-Parental-Control-Policy = 0x0020000000000000000000000020000
```

9. Initiate the radius message from the client, by following step 5. Now you should be able to access the www.guns.com web page.

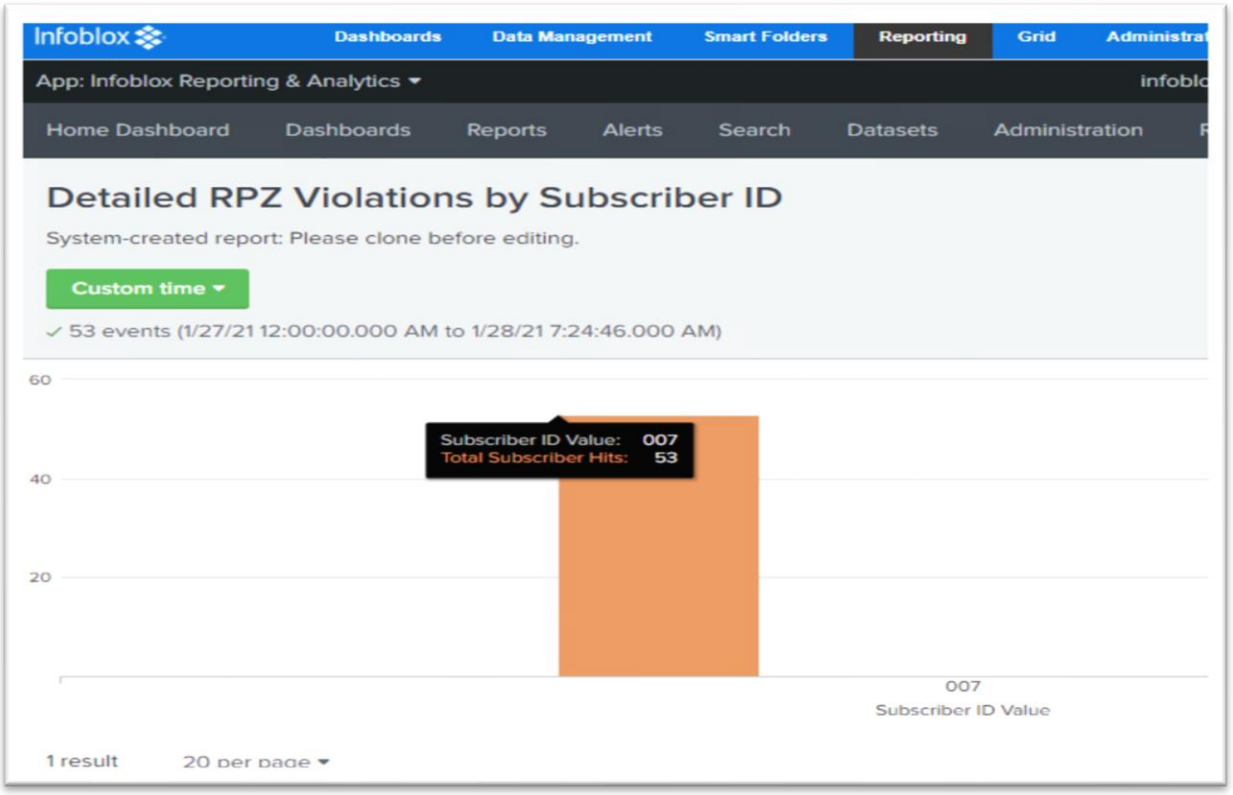
Reporting

With Subscriber security and Parental control, a new report has been introduced called the **Detailed RPZ Violations by Subscriber ID.** Purpose of this report is to display parental control policy violations based on client id or subscriber id.

1. Navigate to the **Reporting → Reports**, search for subscriber key word in the search bar and hit on return. **Detailed RPZ Violations with the subscriber ID** report will show up. Click on this report.



2. This report displays details like subscriber ID, accessed malicious domain and any other suspicious activity.



Some useful information

The Content Categorization database as of now supports the following categories:

Category bit number	Category
1	ALCOKI
2	ARTNUD
3	BIKINI

4	CGAMB
5	DRUG
6	GAMB
7	GAMBW
8	HATE
9	HSPCH
10	MATU
11	MIL
12	PCRIM
13	PERSW
14	PLACE
15	PLAG
16	POCCU
17	PORN
18	PORNW
19	PPERS
20	SUIC
21	SXED
22	TOBA
23	TOBAKI
24	VIOL
25	WEAP
26	WAMMO
27	WACCE
28	WGUNS
29	WKNIV
30	WMART
31	BULLY
32	GORE
33	NUDE
34	ADVI
35	ADVERT
36	ANON
37	AUTO
38	BACKUP
39	CAIC
40	ABOR
41	CCC1
42	CCC2
43	CCC3
44	CCC4
45	CDN
46	DYNAMI
47	DYNAMW
48	EDU
49	EMAIL
50	ENTER
51	FINAW
52	GAME
53	HEAL
54	HOST
55	KIDZ
56	LAW
57	MAIL
58	MOBE
59	MUSIC

60	NEWSW
61	PFINA
62	PGLAM
63	PHACK
64	PJOBS
65	ENTW
66	PNEWS
67	PORTAL
68	PROXYW
69	PSHOP
70	PSPOR
71	PTRAV
72	REF
73	SCI
74	SEHARM
75	SHARE
76	SPORTW
77	STREAM
78	TECH
79	TRAVW
80	VOIP
81	WEBAPP
82	CLOUD
83	REMOTE
84	SEARCH
85	PHISH
86	TRACK
87	ARTMUS
88	BLOG
89	BUSI
90	BUSIW
91	CHAT
92	CMC
93	ENERGY
94	FOOD
95	FORUM
96	GOV
97	NOPROF
98	PCULT
99	PEER
100	PETS
101	PHOTO
102	POLI
103	REALTY
104	RELI
105	WED
106	HOBBY
107	LING
108	BBFCB
109	BBFCW

Parental control policy (PCP) bit for a category

1. To find out Parental control policy (PCP) bit for a category, refer to the following example
    a. category bit number = 17.
    b. This is a PORN category. To find out PCP for PORN category we will start placing zeroes from LHS. First, we will place 17 zeroes and then place '1' after 17th zero

c. **i.e →100000000000000000**

d. Using Binary to Hexa Decimal converter link → (https://codebeautify.org/binary-hex-converter) we will convert '100000000000000000' to its hex value i.e '20000'

2. Since PCP is 32 bits, we will add 27 zeroes before 20000.
3. So, PCP bits for porn category will be 00000000000000000000000000020000
4. Always update and install the latest versions for all the applications used on the Linux machines.
5. Argument values should be checked for any typos and while copying verify if there are any unwanted characters added.

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com