BlueCat DNS Director v1.0.2

Installation & Configuration Guide

September 2014

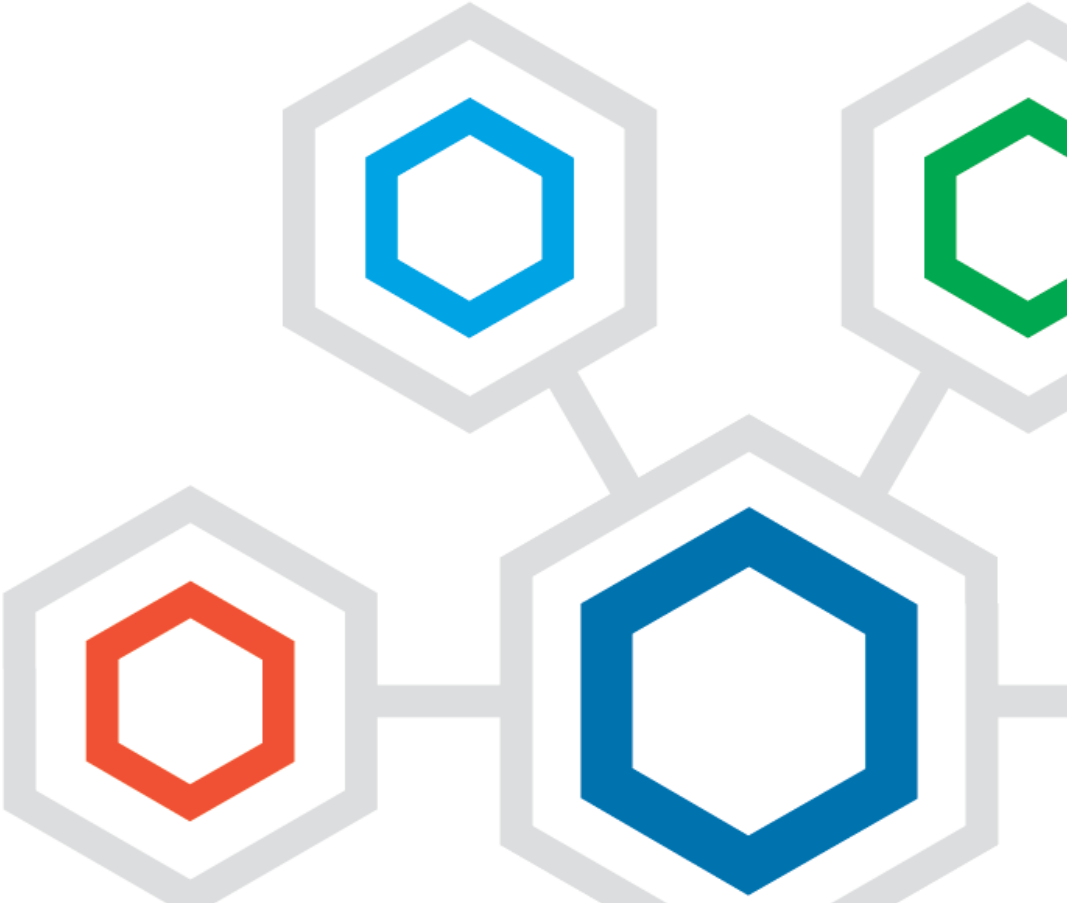


Table of Contents

FREE DNS DIRECTOR LICENSE AGREEMENT – VIRTUAL ("Agreement")

You and Licensor agree:

PARTIES: The Product is licensed to you by **BlueCat Networks, Inc.** if you are outside of the USA, or **BlueCat Networks (USA) Inc.**, if you are in the USA, (each a "Licensor"). In this Agreement, "You" means the entity downloading this software from the HP SDN App Store, and "Your" has a corresponding meaning.

EFFECTIVE DATE: The Agreement is effective from the time of the download, and downloading evidences Your acceptance of this Agreement.

USE/OWNERSHIP. Licensor licenses to you one (1) BlueCat SDN Director and standard end user manual (collectively "Product"), under a perpetual, non-exclusive, non-transferable, non-assignable object code license for your use at the site to which it was originally downloaded. Your license permits Product use only for end use purposes (and not for redistribution by You). No reviews may be published or provided to third parties without Licensor's prior written approval. All rights and ownership in the Product shall at all times remain solely with Licensor.

RESTRICTIONS. You may not: (a) copy, distribute, export, translate, disclose or make available to any third party for free or on a commercial basis, the Product, or any component thereof, or disclose how the Product works, except as expressly permitted for in this Agreement; or (b) reverse engineer, disassemble, decompile, or electronically transfer into another computer language, the Product or any component thereof.

CONFIDENTIAL AND PROPRIETARY INFORMATION ("C&PI"). You agree to keep confidential and use best efforts to prevent and protect the Products from unauthorized disclosure and use.

WARRANTY. THE PRODUCT IS PROVIDED "AS IS". LICENSOR MAKES NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCT, INCLUDING WITHOUT LIMITATION ANY WARRANTY AS TO TITLE, FITNESS FOR INTENDED PURPOSE, OR MERCHANTABILITY. IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DIRECT OR INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH OR ARISING OUT OF THE PRODUCT OR THIS AGREEMENT HOWEVER CAUSED AND REGARDLESS OF THE LEGAL THEORY OF LIABILITY. YOU ACKNOWLEDGE THAT AS LICENSOR IS MAKING THE LICENSE AND PRODUCT AVAILABLE WITH NO CHARGE TO YOU, THIS IS A FAIR ALLOCATION OF RISK.

SUPPORT. You acknowledge that You are not paying for, and Licensor is not required to provide, any implementation, training services or maintenance or technical support for the Product.

GENERAL. This is the entire agreement between the parties regarding the free license of the Product to You. Notwithstanding any agreement or understanding to the contrary between the Licensor and You, no other agreement governs the license of Product by Licensor to You. Ontario law applies, excepting its choice of law provisions and Toronto shall be the venue.

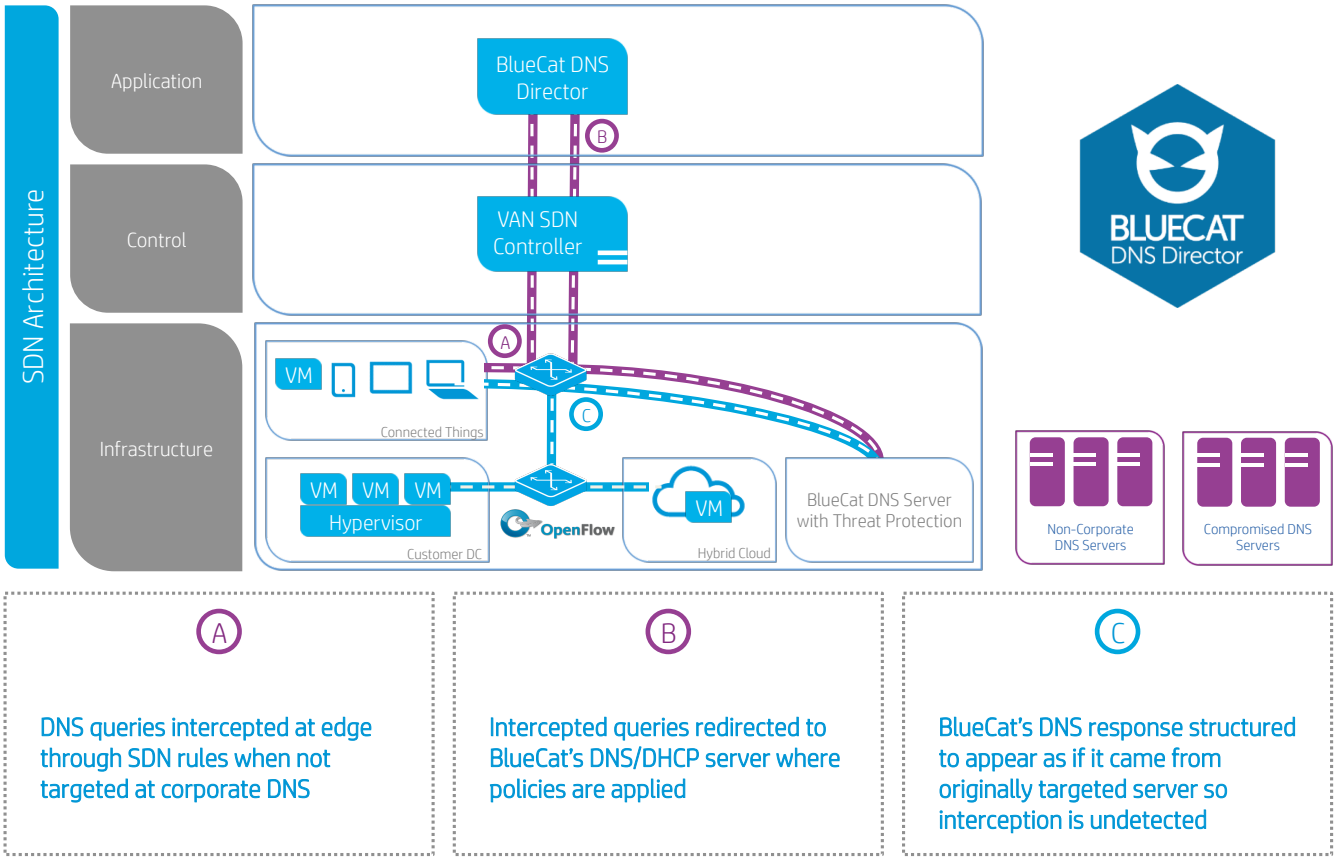
NOTE – YOU WILL NEED TO ACCEPT THE FREE DNS DIRECTOR LICENSE AGREEMENT FOR OPENFLOW FLOWS TO BE DEPLOYED TO YOUR SWITCHES. FOR DETAILS ON HOW TO ACCEPT THE EULA, PLEASE CONSULT: "Accessing the DNS Director User Interface".

Introduction

DNS Director is BlueCat's first SDN application for the HP Virtual Application Network (VAN) controller environment.

Domain Name System (DNS) is uniquely positioned in the network. DNS precedes nearly every Internet Protocol (IP) connection. As such, DNS queries expose a client's intent to connect, regardless of the device or application, thus providing you with extensive visibility.
Through its core function of translating a hostname to an IP address, DNS also provides you with tremendous control, allowing you to determine where devices and applications connect.

To ensure that all DNS traffic is subject to your DNS-driven policies, irrespective of the clients' configuration, BlueCat developed BlueCat DNS Director, an SDN App. for the HP VAN SDN Controller that deploys OpenFlow policies to the edge of the network to make sure that all DNS queries are processed by your DNS servers, including BlueCat DNS Servers augmented with Threat Protection:



Securing applications and devices through DNS does not require a network architectural shift. BlueCat Threat Protection can be added to existing BlueCat DNS servers quickly and easily, avoiding disruption or conflict with strategic investments in existing security technology or DNS infrastructure. BlueCat Threat Protection offers you an additional layer of protection to enhance your organization's existing defense in depth security capabilities

Bluecat's DNS Director, combined with the HP SDN Architecture, enables you to simplify end-to-end network security and increase the efficiency, agility and resilience of your network, providing you with central DNS security, globally delivered.

Compatibility Matrix

HP Virtual Application Networks SDN Controller

BlueCat DNS Director v1.0.2 is compatible with the HP VAN SDN Controller v2.3.5.6505, and newer versions.

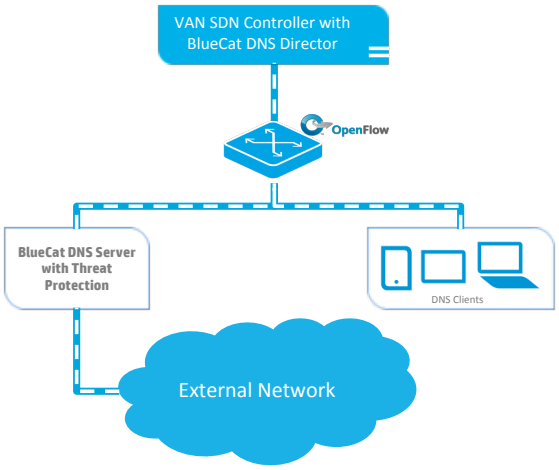
Switches

BlueCat DNS Director v1.0.2 was tested with the following HP Switch Models:

- HP 2920 Switch Series
- HP 3800 Switch Series
- HP 5500 Switch Series

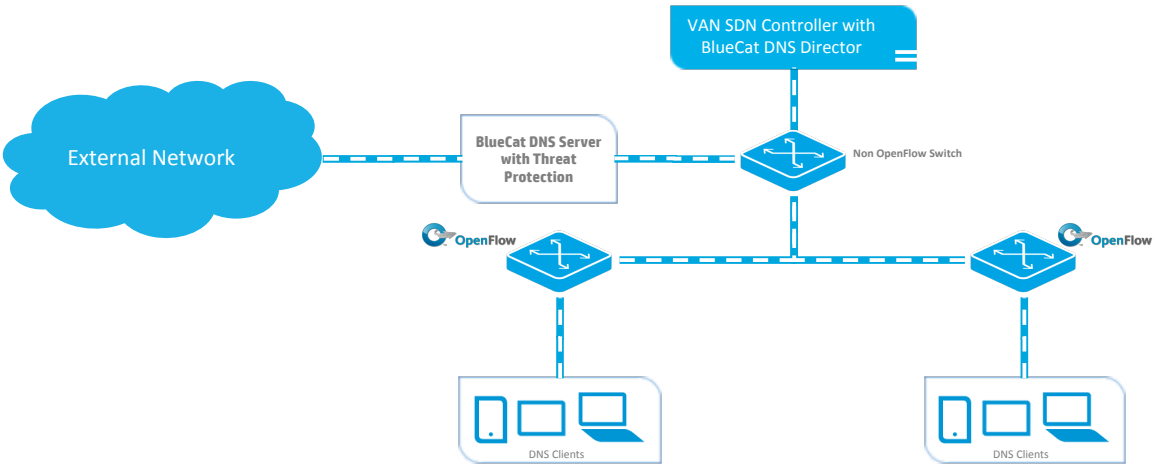
Network Topologies

Single OpenFlow Switch Configuration (Lab Example)



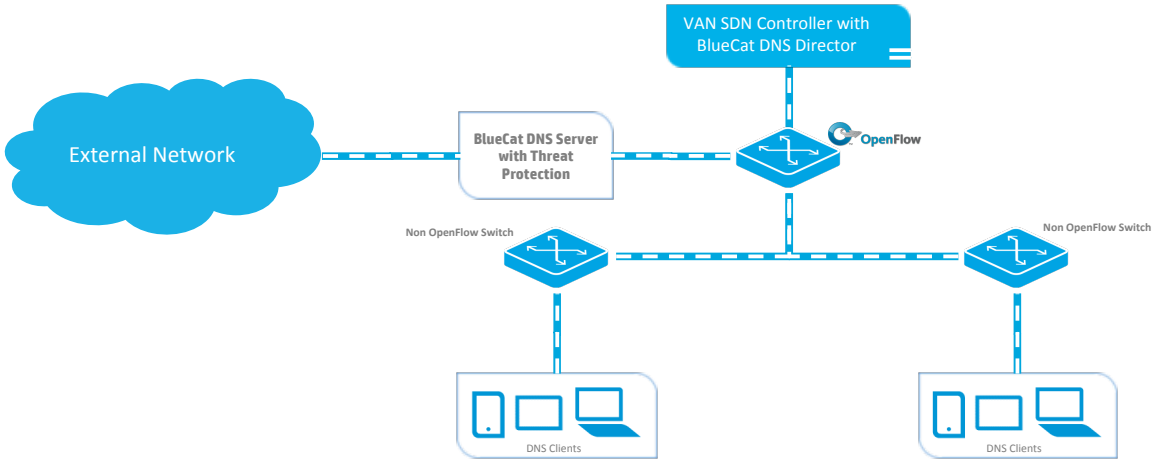
This scenario is intended to represent a basic lab scenario comprised of a single OpenFlow capable switch.

Two edge OpenFlow switches in a network of Switches



In this scenario, the OpenFlow enabled edge switches will allow DNS queries to be intercepted directly at the point of ingress, thus allowing policies to be enforced at the point that is closest to both devices and applications.

Central OpenFlow switch in a network of Switches



In this scenario, while the edge switches are not OpenFlow capable, DNS queries targeted at non-corporate servers will be intercepted by the distribution switches, still ensuring that DNS-enforced policies are applied across all devices, irrespective of their configuration.

Setup and Configuration

Installing BlueCat DNS Director on your HP VAN SDN Controller

Installing the BlueCat certificate on your HP VAN SDN Controller

NOTE – Prior to installing BlueCat DNS Director on your HP VAN SDN Controller, please make sure to install the BlueCat certificate included in the zip file per guidelines provided in the HP VAN SDN Controller documentation.

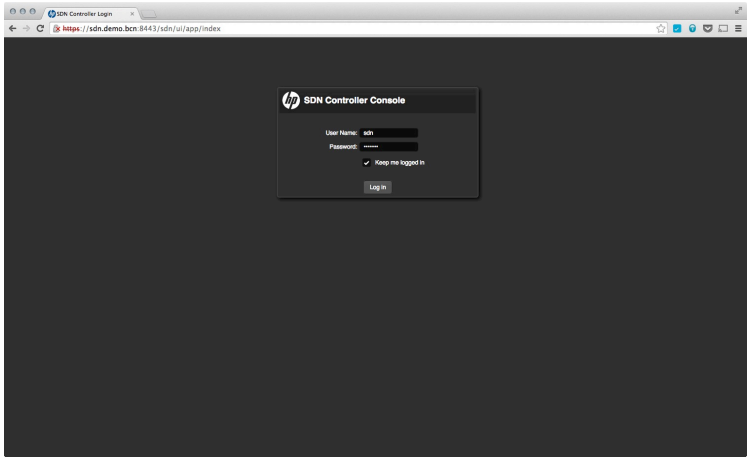
As a reminder, to install the BlueCat certificate included in the zip file, log into the HP VAN SDN Controller command line interface as an administrator, as this operation requires privileged access to the keystore.
Once logged in, please proceed with the following steps:

- Copy the bluecat-sdn.cer file included in the zip file to a directory on the controller
- Install the cert by typing:
  `keytool -keystore /opt/sdn/admin/sdnjar_trust.jks -importcert -file /<path>/bluecat-sdn.cer -alias bluecatsdncer` – When prompted enter the keytool password
- Verify the cert is present by typing:
  `keytool -keystore /opt/sdn/admin/sdnjar_trust.jks -list` – When prompted enter the keytool password

Installing BlueCat DNS Director on your HP VAN SDN Controller

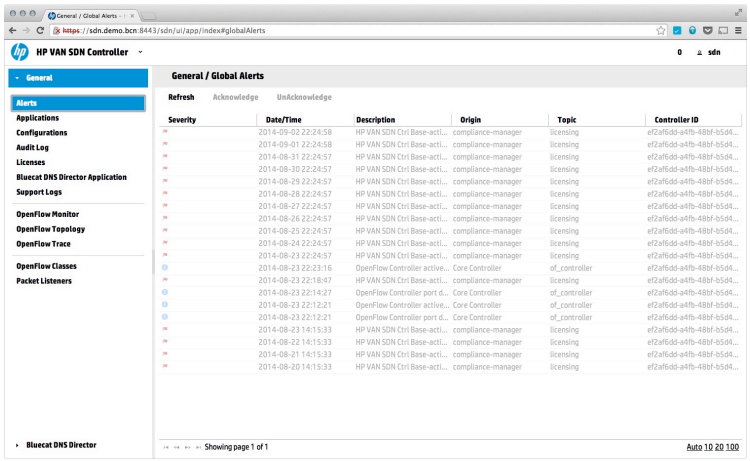
To install DNS Director on your SDN Controller, proceed according to the following steps:

1. Log-in to your SDN Controller (default username/password: sdn/skyline)

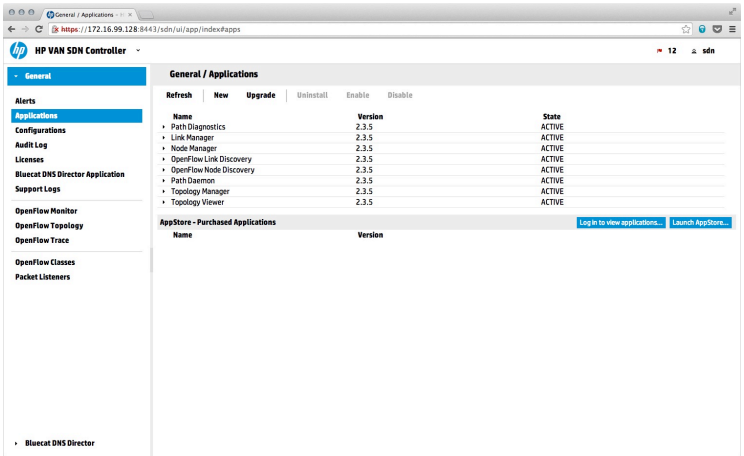


NOTE

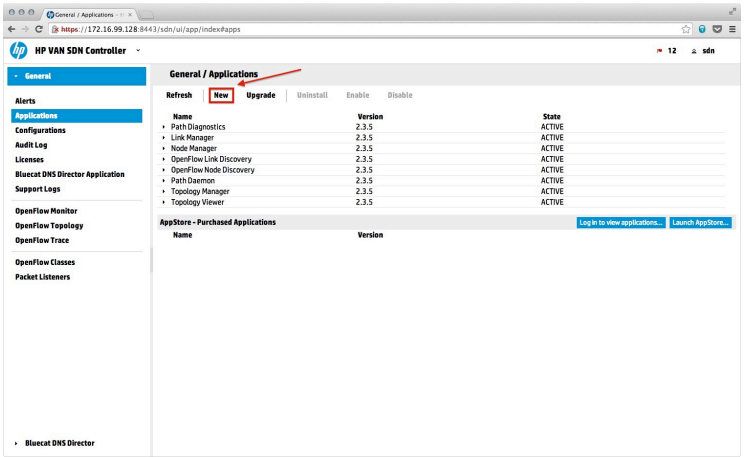
BlueCat DNS Director v1.0.2 can be deployed on the HP VAN SDN Controller v2.3.5.6505 and newer versions.



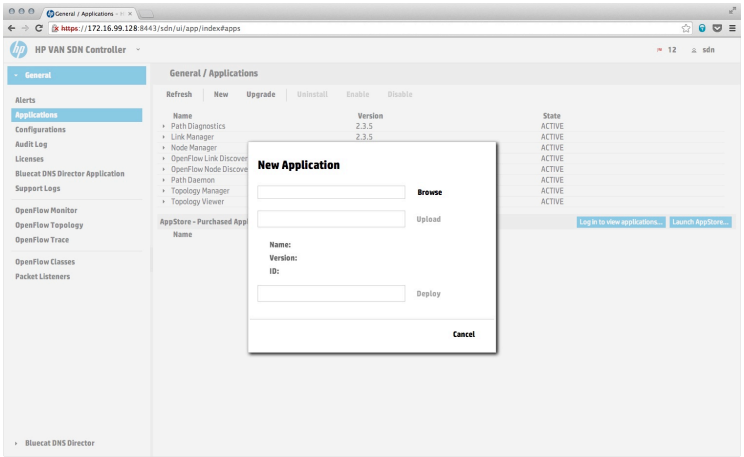
2. Select the "**Applications**" page



3. Click on "**New**"



4. Click on "**Browse**", then navigate to the application file on your local computer and select it



5. Click on "**Upload**"
6. Once the upload is completed, click on "**Deploy**"
7. DNS Director is now deploying on your controller.
8. Once the deployment is complete, your browser will display a list of Applications that includes DNS Director.
9. DNS Director is now installed on your HP VAN SDN Controller. Proceed to the next step – "Configuring DNS Director"

Configuring DNS Director

BlueCat DNS Director configuration parameters are defined and stored in the "**dnsdir.properties**" file located in **/etc/bluecat/**.
Sample Configuration File – /etc/bluecat/dnsdir.properties

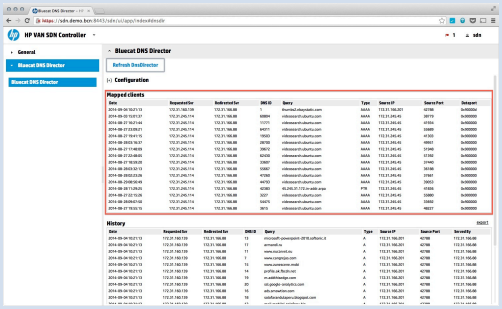
```
DataPathIds=00:00:00:00:00:00:00:01
#IpFlowTimeout=0
#HardTimeout=180
#PreferredAltitude=59999
PreferredDnsServer=1.2.3.4 <SET TO YOUR IP>
PreferredDnsPort=53000
#DnsFlowPriority=42201
#DnsCacheSize=100
#DnsHistorySize=1000
#DnsRequestTimeout=6000
Debug=0
```

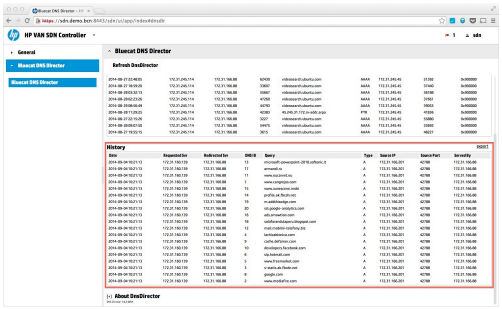
NOTE

If the "dnsdir.properties" file does not exist on your controller, you will need to create it using a text editor, such as vi.

NOTE

All commented values in this sample will be populated with their recommended default.

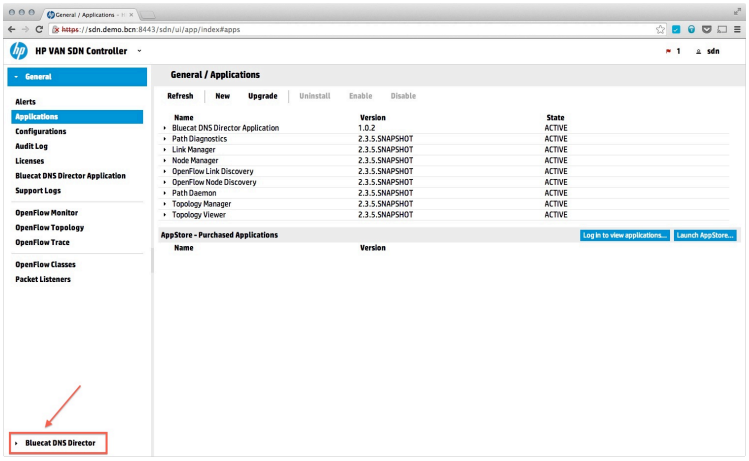
Parameter	Unit	Default Value	Description
Debug	N/A	0	Set to "**1**" for debug log output.
HardTimeout	Seconds	180	Flow timeout in seconds. Flows will be renewed every HardTimeout/2.
DataPathIds	N/A		Comma-separated list of switch IDs to be accepted. An empty list implies all switches. NOTE: Other switches will be ignored.
PreferredAltitude	N/A	59999	Preferred altitude can be changed if it conflicts with other applications.
IpFlowTimeout	Seconds	0	Idle timeout value in seconds (0 indicates no timeout).
PreferredDnsServer	IPv4 Addr.	N/A	DNS Server or Load Balancer to receive redirected DNS queries.
PreferredDnsPort	N/A	53000	UDP port to which redirected DNS queries are sent. **NOTE: The DNS server or Load Balancer must be configured to receive DNS queries on this port.**
DnsFlowPriority	N/A	42201	Base priority of the application flows. Value can be changed if it conflicts with other applications.
DnsCacheSize	N/A	100	Maximum size of the DNS cache in number of DNS queries. DNS queries still in cache will be displayed under "Mapped Client" in the BlueCat DNS Director user interface. 

Parameter	Unit	Default Value	Description
DnsHistorySize	N/A	1000	Maximum size of the DNS history list displayed in the BlueCat DNS Director user interface. Entries in the DNS history list are displayed under "**History**". 
DnsRequestTimeout	Seconds	6000	Timeout for un-responded queries to remain in the cache.

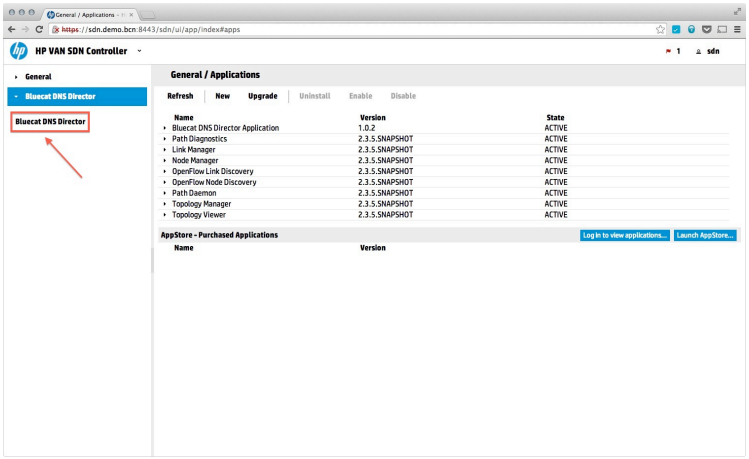
Accessing the DNS Director User Interface

To access the BlueCat DNS Director user interface, proceed according to the following steps:

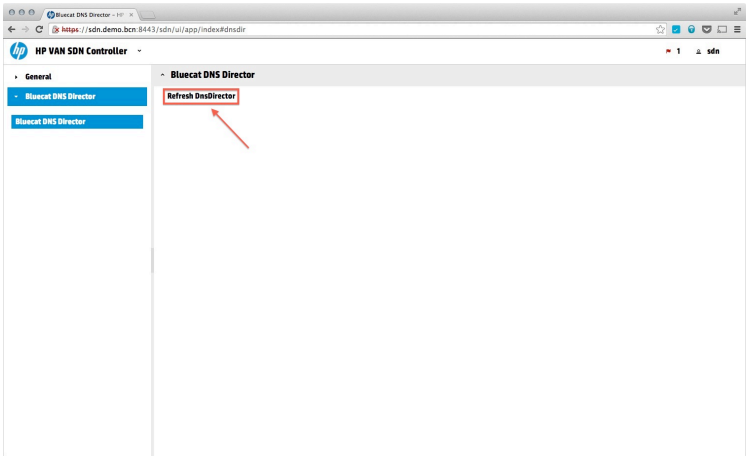
1. Locate and click on the "**BlueCat DNS Director**" label at the bottom of left panel
   NOTE – You may need to refresh your browser to see "**BlueCat DNS Director**"



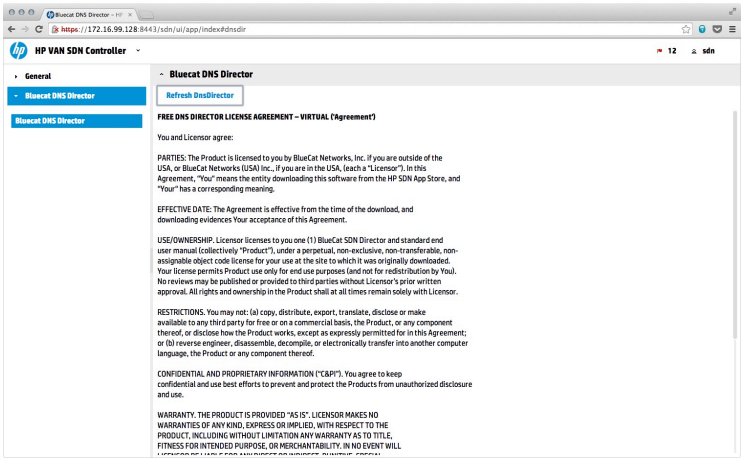
2. Click on the "**BlueCat DNS Director**" menu in the left panel



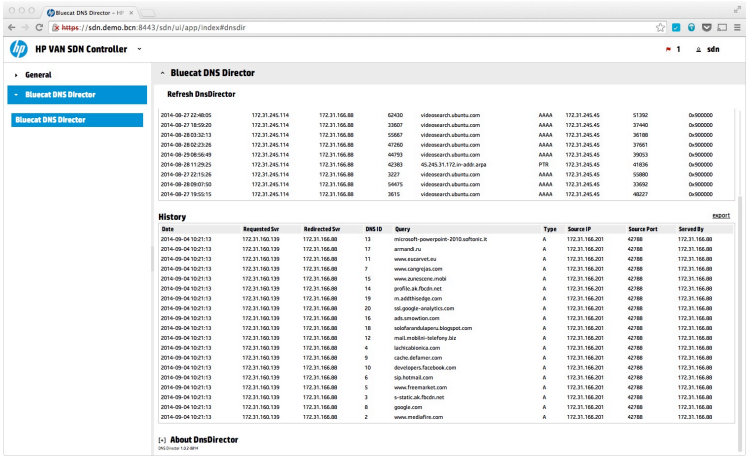
3. In the right-hand panel, click on "**Refresh DnsDirector**"



4. The first time DNS Director is run, please make sure to review and accept the EULA so flows can be deployed to your switches

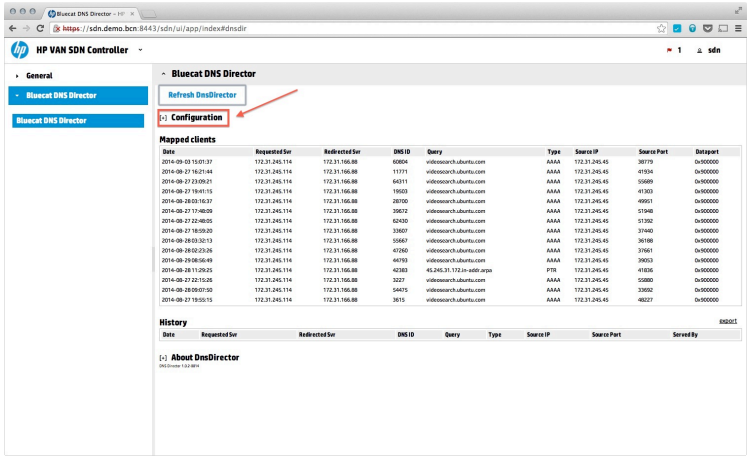


5. Once the EULA is accepted, the DNS Director flows are deployed to your switches, and DNS Director displays the list of outstanding and intercepted queries. For details on the information being displayed please refer to the "Interpreting DNS Director statistics" section.

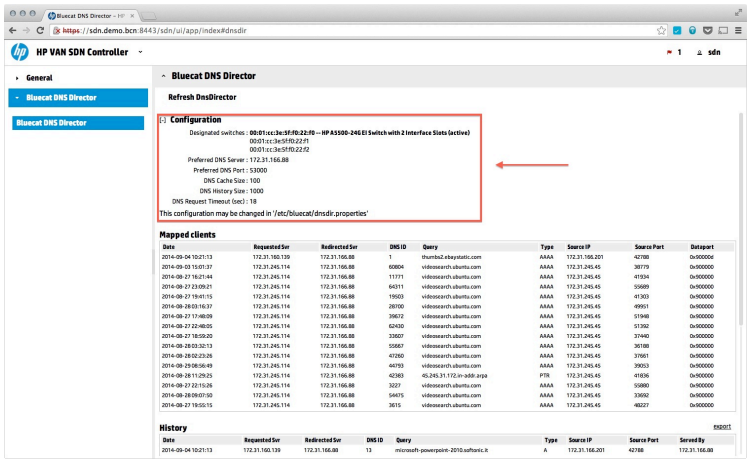


Vieweing DNS Director Active Configuration

1. Locate and click on the "**BlueCat DNS Director**" label at the bottom of left panel
2. Click on the "**BlueCat DNS Director**" menu in the left panel
3. In the right-hand panel, click on "**Refresh DnsDirector**"
4. Click on "**Configuration**"



5. The user interface now displays the currently active configuration for DNS Director, including the list of switches connected to BlueCat DNS Director. For details on how to change BlueCat DNS Director configuration, please consult "Configuring DNS Director"



Interpreting DNS Director statistics

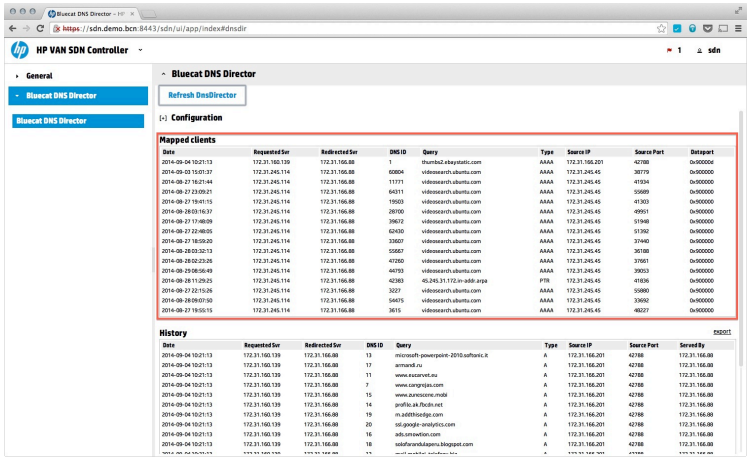
Mapped Clients

The Mapped Clients table shows the DNS requests that are in progress. DNS queries displayed include:

- All requests to a DNS server other than the preferred DNS server. Under normal operation, DNS queries are responded to within a few milli-seconds, however, the quality of the connection and/or performance of the Authoritative DNS servers queried may introduce unwanted delay. Information contained in the "**Mapped Clients**" table should therefore be transient. Upon receiving a response to the DNS query, DNS Director will automatically remove the entry from the "**Mapped Clients**" table.
- All requests to a DNS server other than the preferred DNS server that did not receive a response. This may occur when the Authoritative DNS server does not respond or the response does not come back to the SDN switch. These requests will remain in the Mapped Clients table until they expire and the table is full. Expiry timeout is configured via "DnsRequestTimeout". For more details on how to modify the DNS Request Timeout, please consult the "Configuring DNS Director" section.

Accessing the "Mapped Clients" table

1. Locate and click on the "**BlueCat DNS Director**" label at the bottom of left panel
2. Click on the "**BlueCat DNS Director**" menu in the left panel
3. In the right-hand panel, click on "**Refresh DnsDirector**"
4. The "**Mapped Clients**" table is now displayed in the right-hand panel



"Mapped Clients" table fields

Field	Description
Date	Date and Time the DNS query was received by DNS Director.
Requested Svr	IP address of the DNS server originally contacted by the client.
Redirected Svr	IP address of the DNS server to which the DNS query was redirected.
DNS ID	Unique identifier contained in the DNS query. The DNS ID is used to disambiguate similar requests.
Query	Host requested in the DNS entry.
Type	Type of Resource Record queried. Resource Record will typically be A (IPv4) or AAAA (IPv6), but can also be PTR, TXT, MX, SOA, etc.
Source IP	IP address of the client that initiated the DNS query.
Source Port	Port number from which the client initiated the DNS query.
Dataport	Network port on the switch that received the incoming packet from the client. Dataport is used to send the DNS response back to the client.

DNS Request History

The "**History**" table displays the list of DNS queries that were intercepted by DNS Director and redirected to the preferred DNS server defined in the DNS Director configuration.
For a DNS query to be displayed in the "**History**" table, one of 2 things must have occurred:

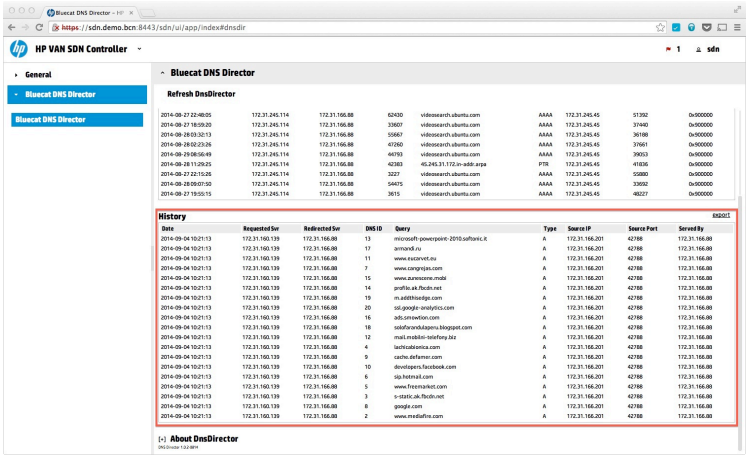
- A response was received from the Authoritative DNS server(s) via the preferred DNS server and the response was relayed to the DNS client.
- No response was received from the Authoritative DNS server(s) and the DNS query expired in the "**Mapped Clients**" cache. Such queries will be identified via the "**Served By**" field, which will be set to 0.0.0.0.

The maximum size of the table is limited by the "**DnsHistorySize**" configuration parameter.
For details on how to modify the "**DnsHistorySize**", please consult the "Configuring DNS Director" section.

NOTE
The table will always display the last 100 entries. To access the full history, simply export the history into a csv file using the instructions provided in the "Exporting the "History" table content" section.

Accessing the "History" table

1. Locate and click on the the "**BlueCat DNS Director**" label at the bottom of left panel
2. Click on the "**BlueCat DNS Director**" menu in the left panel
3. In the right-hand panel, click on "**Refresh DnsDirector**"
4. The "**History**" table is now displayed in the right-hand panel

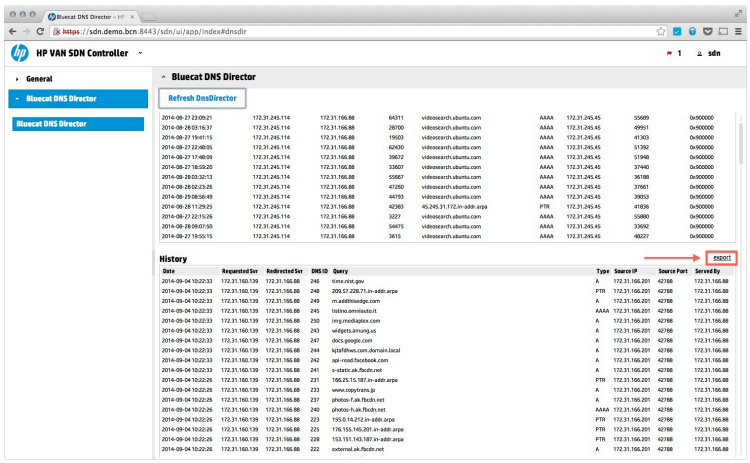


"History" table fields

Field	Description
Date	Date and Time the DNS query was received by DNS Director.
Requested Svr	IP address of the DNS server originally contacted by the client.
Redirected Svr	IP address of the DNS server to which the DNS query was redirected.
DNS ID	Unique identifier contained in the DNS query. The DNS ID is used to disambiguate similar requests.
Query	Host requested in the DNS entry.
Type	Type of Resource Record queried. Resource Record will typically be A (IPv4) or AAAA (IPv6), but can also be PTR, TXT, MX, SOA, etc.
Source IP	IP address of the client that initiated the DNS query.
Source Port	Port number from which the client initiated the DNS query.
Served By	IP address of the DNS server that responded to the DNS query. In case of no response, the entry will be 0.0.0.0

Exporting the "History" table content

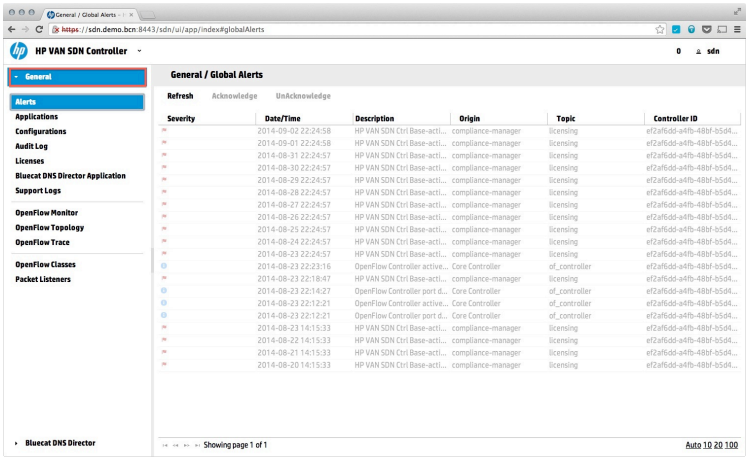
To export all the data in the "**History**" table in comma-separated value (csv) format, click on the "**export**" link.
This will allow you to save the data file on your local computer or view it in a spreadsheet application, such as Microsoft® Excel®.
Data exported in the comma-separated value file includes the number of entries defined in "**DnsHistorySize**".



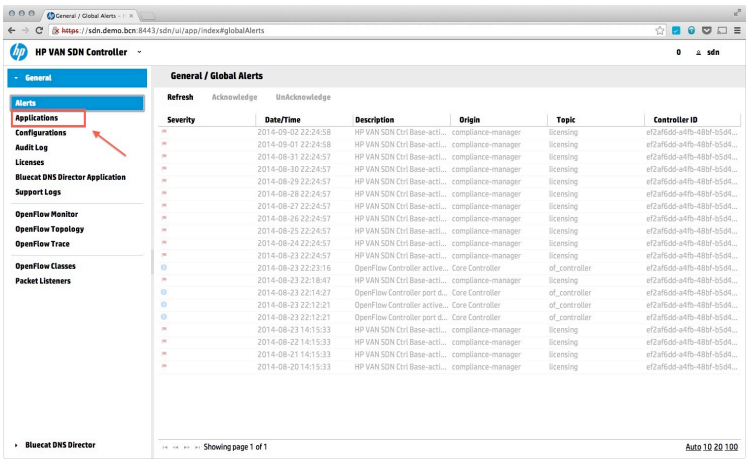
Troubleshooting

Verifying that BlueCat DNS Director was successfully installed on your controller

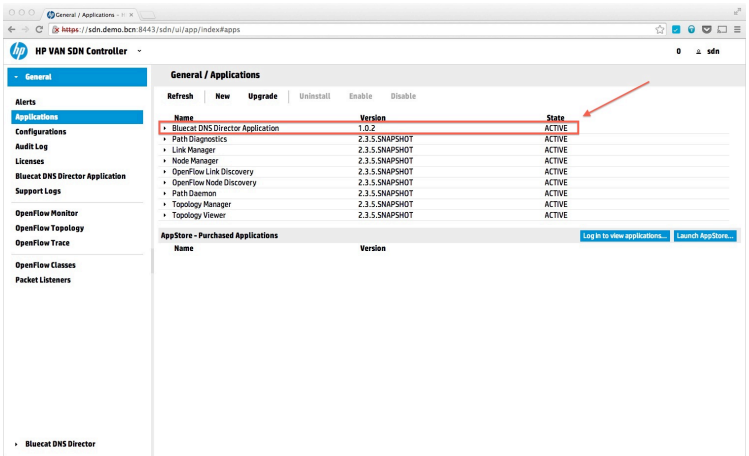
1. Log-in to your SDN Controller (default username/password: sdn/skyline)
2. Click on "**General**"



3. Click on "**Applications**"

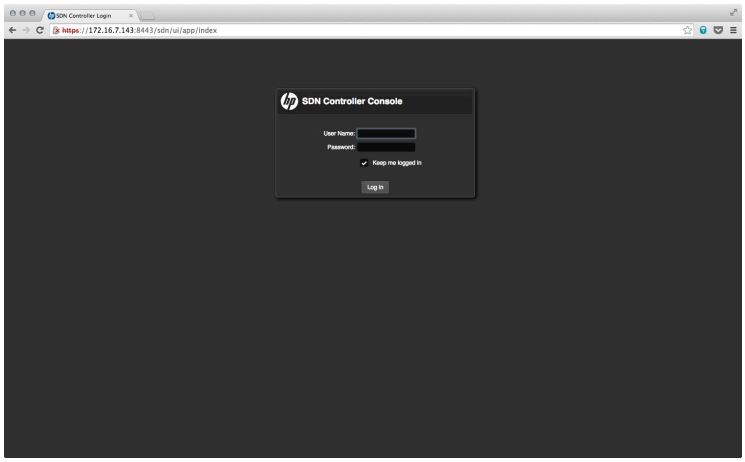


4. Verify that "**BlueCat DNS Director Application**" is listed in the right-hand panel and has a "**State**" of "**Active**"

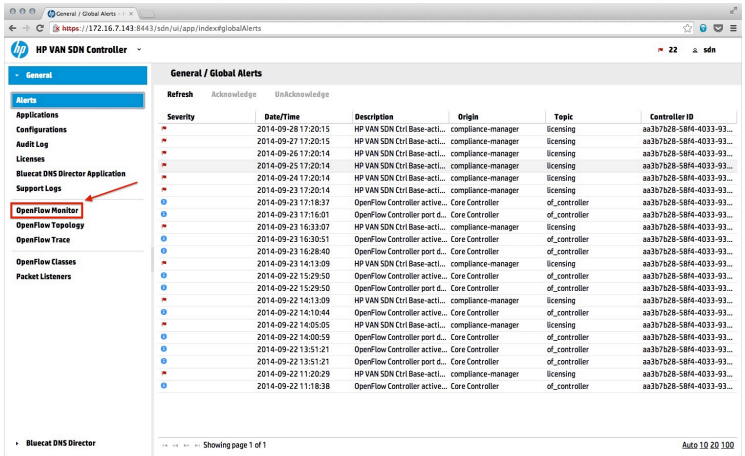


Verifying that BlueCat DNS Director flows are deployed on your OpenFlow switches

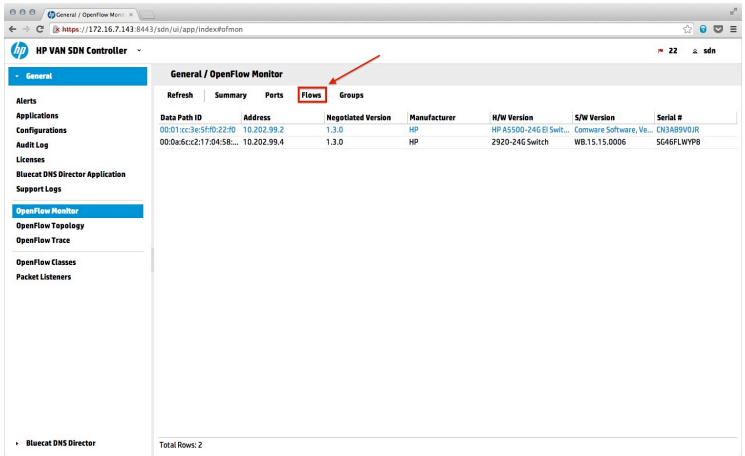
1. Log-in to your SDN Controller (default username/password: sdn/skyline)



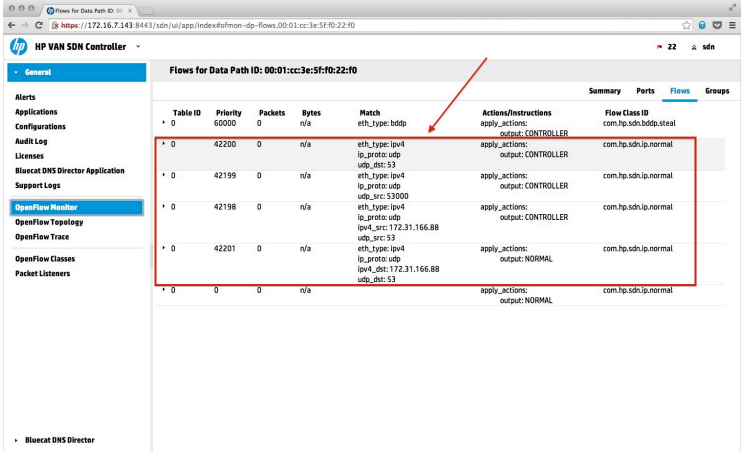
2. Click on "**OpenFlow Monitor**"



3. In the "**General/OpenFlow Monitor**" window, select one of the switch configured in DNS Director and click "**Flows**"



4. The highlighted flows are necessary for BlueCat DNS Director to operate.
    - If these flows are not present, please make sure you have accepted the BlueCat DNS Director EULA – For details, please consult: "Accessing the DNS Director User Interface".
    - If you have accepted the EULA, please consider restarting BlueCat DNS Director.



END OF DOCUMENT