Infoblox

DEPLOYMENT GUIDE

Advanced DNS Protection

Initial Deployment of PT (Physical) and Software ADP (Physical/Virtual) Appliances, Upgrade of Software ADP (Physical/Virtual) capable Appliances

NIOS 8.4

Table of Contents

Introduction

The Infoblox Advanced DNS Protection solution employs threat protection rules to detect, report upon, and stop DoS (Denial of Service), DDoS (Distributed Denial of Service) and other network attacks targeting DNS authoritative and recursive applications. Infoblox Advanced DNS Protection helps minimize “false positives” and ensures that your mission-critical DNS services continue to function even when under attack.

You can deploy the Advanced DNS Protection solution on hardware-accelerated appliances (physical appliances only) as well as software-based appliances (both physical and virtual) in the Grid. Depending on the appliances you deploy, you must install applicable hardware-based licenses, software subscription licenses or IB-FLEX capacity-based licensing.

This document is specifically for Software Based Advanced DNS Protection, though some recent NIOS features like profiles, and ruleset extensions also apply to hardware accelerated solutions.

Note: When referring to ADP, it should be implied the document is discussing appliances with Software ADP licenses, IB-FLEX, or Physical PT appliances.

Prerequisites for Grid Deployment

- A separate Infoblox Grid Master with Grid license.
- DNS, Threat Protection and Threat Protection Update licenses from Infoblox for the ADP appliance (Customer can use temp licenses for 60 days)
- Grid master should be able to access https://ts.infoblox.com (resolve and reach) for the Threat Protection rulesets.

Prerequisites for Standalone Deployment

- DNS, Threat Protection and Threat Protection Update licenses from Infoblox for the ADP appliance (Customer can use temp licenses for 60 days)
- The appliance should be able to access https://ts.infoblox.com (resolve and reach) for the Threat Protection rulesets.

Limitations and Cautions

- Grid Masters in Grid deployments cannot run the Threat Protection service. They are only responsible for updating rulesets.
- Standalone deployment does not support Infoblox HA (VRRP-based High Availability).
- Protected interfaces (LAN1 and LAN2) are limited to DNS and DHCP traffic, protocols in support of DNS anycast (BGP and OSPF) and the standard IP protocols such as ICMP, as well as connections to NTP servers.
- The MGMT interface is used for other traffic, such as Grid, SSH, SNMP, NTP, and it will not be protected by ADP.
- You cannot run other services, such as FTP, TFTP, and HTTP, on the advanced appliance.
    - The appliance terminates TCP connections for incoming DNS requests after handling the initial request through each TCP connection. The exception for this default Grid setting is for an SOA query sent by a client that is accepted in the allow-transfer ACL. In the case of an SOA query, the TCP connection remains open for subsequent DNS requests. This exception also covers the case in which an AXFR query follows the SOA query through the same TCP connection.

Cautions

Stateful Firewalls

Under volumetric (high PPS), stateful firewalls need to be sized appropriately. Some types of UDP DNS attacks may not have responses, which may lead to resource starvation in the firewall. Consider that 1GbE ~ 1.4 Mpps, and 10GbE ~ 14 Mpps. To prevent issues with firewalls, the LAN1/LAN2 interfaces of ADP servers should be in front of any stateful firewalls so that as ADP is not affected by these issues. This can also affect the recursion path.

Low performance network elements (PPS)

DNS is a UDP protocol whose typical query packet size is 80-90 bytes. When faced by a line-rate volumetric attack with these DNS packets, some firewalls/switches/routers are unable to cope and may reset or provide substandard performance.

Best Practices

When deploying ADP:

- ADP should not be deployed on the same Layer 2 as Clients, or where DHCP requests are broadcast. For example, in production, we're running our ADP in a /29, or /126 for IPv6
- Clients generate a lot of broadcast, especially port 5353, and other traffic which results in spurious/useless messages. DHCP broadcasts also create unnecessary noise.
- If you are running DHCP, then the expectation is that you use DHCP relay to the ADP.
- If you are not running DHCP, then the reason for the messages need to be understood and resolved. In a Lab environment, just disable the rules (set EPS to 0).
- In situations where a volumetric attack may be experienced against recursive servers, it is best to use LAN2 exclusively for recursion and to also make use of ANYcast.
- Make sure the Grid is using reliable NTP sources, a minimum of 3, and is fully synchronized.

Use of MGMT, LAN1, and LAN2

Whilst it is now possible (as of 8.1) to use LAN1 for management, it is considered a poor design choice since under volumetric attack, you may lose access to the ADP member, and the customer must accept any/all possible repercussions including loss of reporting data, logging data, disconnection from Grid, failure of Threat Protection Updates, failure to upgrade et al.

When you disable **Enable VPN on MGMT Port** setting, upon saving the following pop up is going to appear. This is a warning to be taken seriously.

ADP Profiles

It is a best practice, especially for PoC's, to utilize Profiles for all members. You can then leave the Grid version of the rules unaltered, and hence you can revert to the default rule settings for individual rules, or entire categories at any time. The only time you will need to change the Grid level rules is when you add custom rules.

ADP Rules

- With the exception of the DHCP system rules in general, and the TCP/UDP rules DNS query without Recursion Desired, all system rules should be enabled.
- When viewing the rulesets, sort by Order. The Order is the evaluation order of the rules which can prove useful for debugging and understanding rule deployment.
- Events Per Second (EPS) should either be 0 or 1 so as to reduce the chance of death by syslog. Values greater than 1 should only be used for short debug sessions. EPS limits the number of syslog entries per rule per client that can be generated.
- Setting EPS to 0 will prevent syslog messages, but the counts will still be available on the reporting server.
- Whitelisting should never be used, unless you have total and immediate control over the whitelisted client, and the reason is to give you a chance to formulate an appropriate remediation.
- Remember that like with a firewall ruleset, the last rule drops all. There must be an explicit pass somewhere (i.e. don't disable every rule).

Reporting

- It is recommended to have a Reporting member in the Grid.
- If you have not purchased a Reporting Member, you can consider deploying the free version.
- Remember to enable the security index.

System alerts

A Grid Master is able to generate SNMP and email alerts. Since these are real time, they should be configured for the categories that matter.

- System CPU/Memory/NIC usage
- Cache hit ratio
- NXDOMAIN hits
- Any issues with the status of services (DNS/DHCP/NTP/...)
- Notifications on threat protection dropped traffic and threat protection total traffic

SIEM

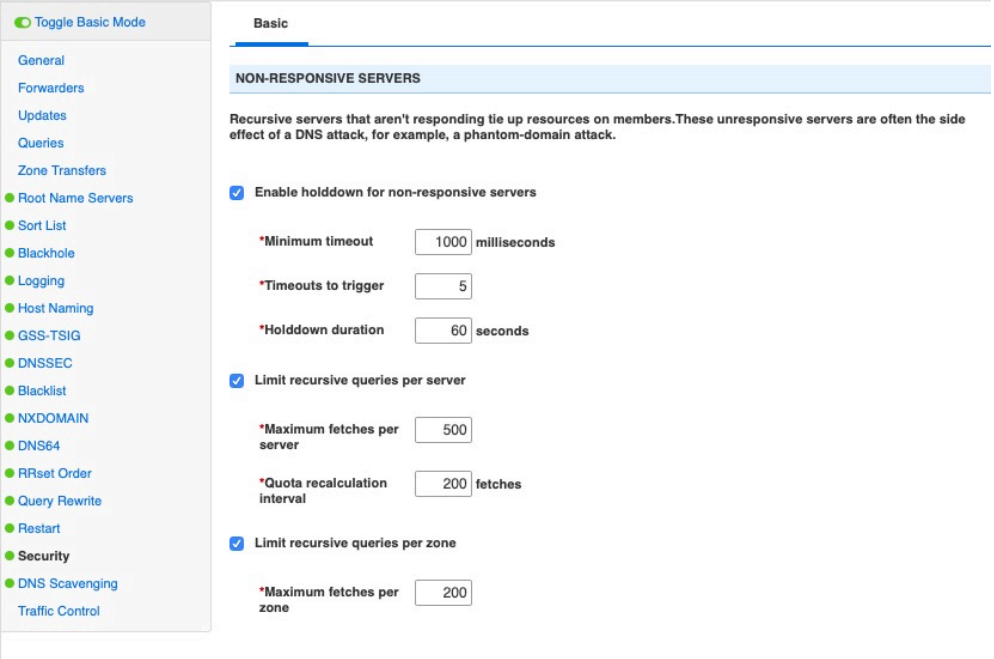
Use of any SIEM (Security Information and Event Management tool) is highly recommended since a great deal of Syslog information can be generated.

Unresponsive Servers

Recursive servers that aren't responding tie up resources on members.

In the **Security** tab in the **Grid DNS Properties**, it is recommended to turn on the following two options:

- Limit recursive queries per server
- Limit recursive queries per zone



ADP Appliances

PT Appliances

The Advanced DNS Protection Appliances are high performance Infoblox network appliances that support the Infoblox ADP solution. With valid licenses installed, these appliances provide a hardware-accelerated solution to DNS threats targeting DNS caching and authoritative applications.

Currently, Infoblox offers the IB-4030 physical appliance for Advanced DNS protection and DNS Cache Acceleration.

Infoblox supports PT-1405, PT-2205, PT-4000, and IB-4030-10G.

Software ADP Appliances

When deploying Advanced DNS Protection solution, you can now install software-based subscription licenses on supported appliances (physical and virtual), in addition to the hardware-based Advanced (PT) appliances.

The Threat Protection licenses for software ADP are currently limited to following virtual and physical appliances:

TE-815, TE-825, TE-1415, TE-1425, TE-2215, TE-2225, TE-4015, TE-4025
IB-V815, IB-V825, IB-V1415, IB-V1425, IB-V2215, IB-V2225, IB-V4015, IB-V4025, IB- FLEX

And we continue to support Threat Protection license for TE-1410, TE-1420, TE-2210, TE-2220 and TE-v1410, TE-v1420, TE-v2210, TE-v2220

Note: refer to the release notes for your version of NIOS for the most up to date information.

Licensing

- Threat Protection (Software add-on) - A new license feature, which enables the software add-on and is licensed on a per-appliance basis for appropriate Trinzic appliances.
- Supports the Threat Protection Update license for ADP rule feed.
- Threat Protection (Software add-on) licenses are subscription-based. If the license expires, the service will continue to work but a license expiry warning will be displayed.
- The following licenses are not supported if the Threat Protection (Software add-on) license is installed on the same member:
  - Multi-Grid Management
  - Microsoft Management
- For IB-FLEX appliances, the Threat Protection service and Threat Protection rule feed will be enabled via the Flex Grid Activation license but licensed via the appropriate SPLA ADP license. Please contact your Infoblox Sales Representative if you have any questions.

Supported Hypervisors

Software ADP appliances are supported for the following hypervisor environments:

- VMware ESXi 6.5 or later
- OpenStack (KVM) – check the NIOS release notes for the latest information of supported versions
- KVM – check the NIOS release notes for the latest information of supported versions

Deployment Architecture

Threat Protection appliances support standalone or grid member deployments. The Threat Protection feature is not supported on the Grid Master (GM) or Grid Master Candidate (GMC) servers. Threat Protection Appliances should always be deployed using out of band management and typically would use anycast for availability and redundancy. The intent is that any attack traffic should be contained to the network that the LAN1 interface is connected to.

If reporting is enabled, reporting traffic must be configured to use the management interface.

No extra configuration is needed if the ADP member’s management interface and Reporting member’s LAN1 interface share the same subnet. However, a route needs to be added in the ADP members network configuration to enable connectivity to the Reporting server if the two are on different subnets.

Deploying ADP

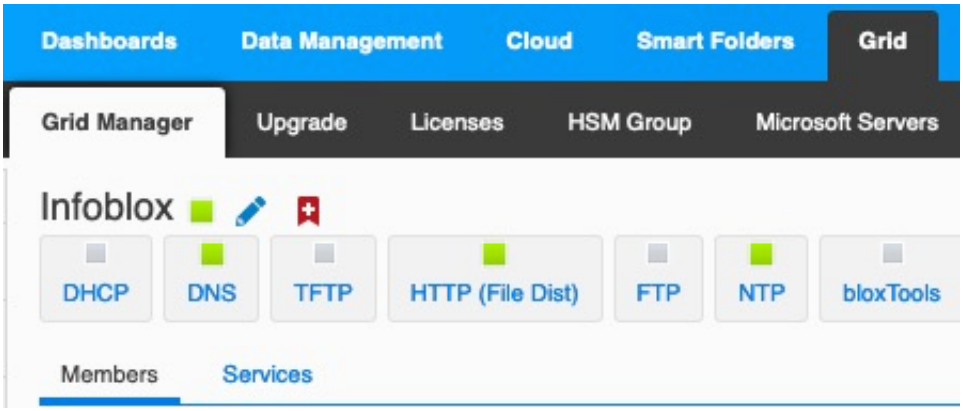
In this deployment guide we are using a Software ADP appliance. The ADP appliance is going to be configured so that it joins the Grid via its management interface as discussed in the deployment architecture section.

The following sections depict how to accomplish that:

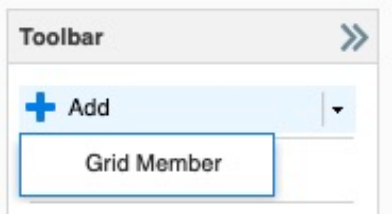
Adding member information in the Grid

Before joining the ADP appliance to the Grid we must add member information in the Grid using the Infoblox Web UI.
Log in to the Grid using super-user privileges.

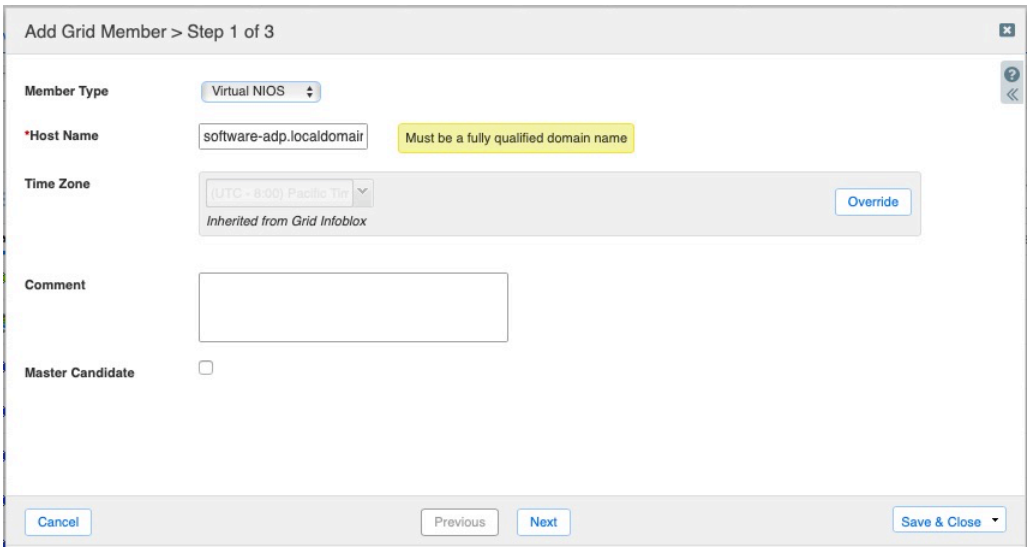
Go to **Grid** > **Grid Manager** > **Members** tab



Under **Toolbar**, Click **Add** > **Grid Member**

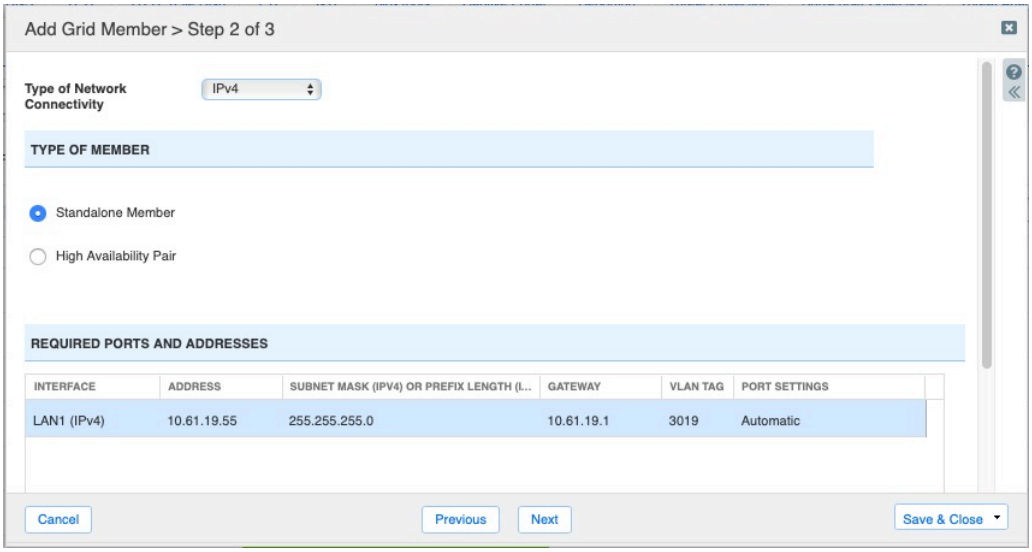


Pick the appropriate Member Type. In our example, it is virtual NIOS (select **Infoblox** for a physical appliance and **Virtual NIOS** for all virtual appliance types). In **Step 1 of 3** of the **Add Grid Member** wizard, select the correct **Member Type**. Type any name of your choice in **Host Name** field. In our example, it is **software-adp.localdomain**. Click **Next**.



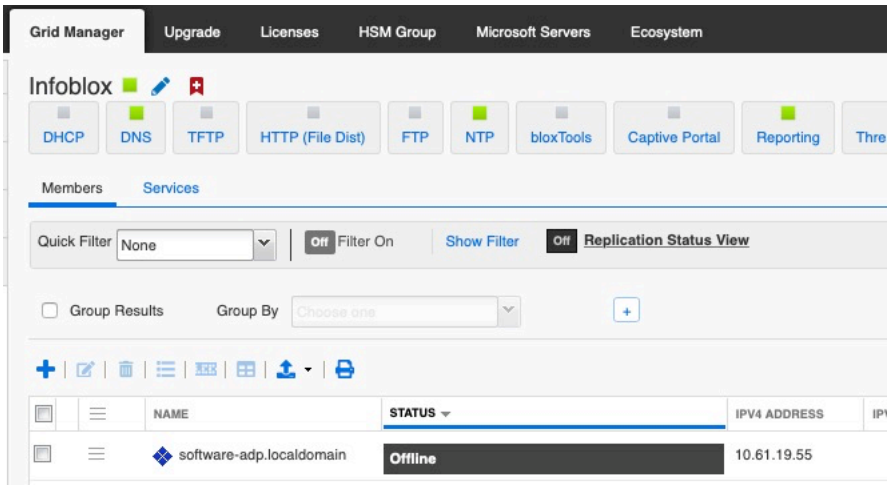
In **step 2 of 3**, keep the default value for **Type of Member** as **Standalone Member.**

Set the appropriate IP address, subnet mask and Gateway information for the member's LAN1 interface.

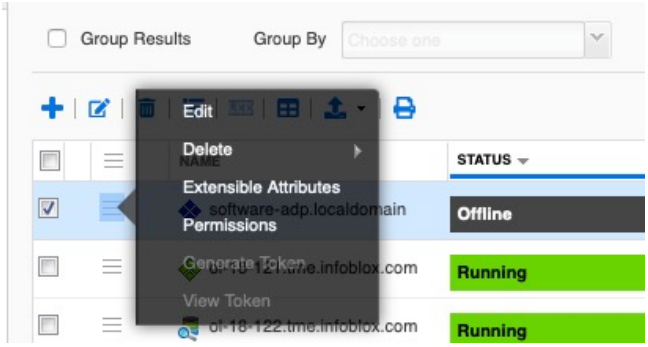


Click **Save & Close.**

Note: The newly added member will show as **offline** in the **Grid Manager** > **Members** Tab.

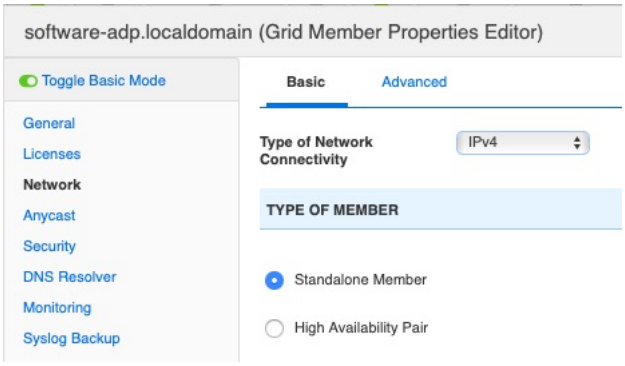


Click on the Properties icon next to the newly added member software-adp.localdomain.



Click **Edit**.

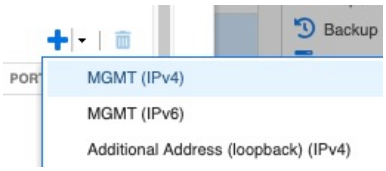
Click **Toggle Advanced Mode in not already selected.**



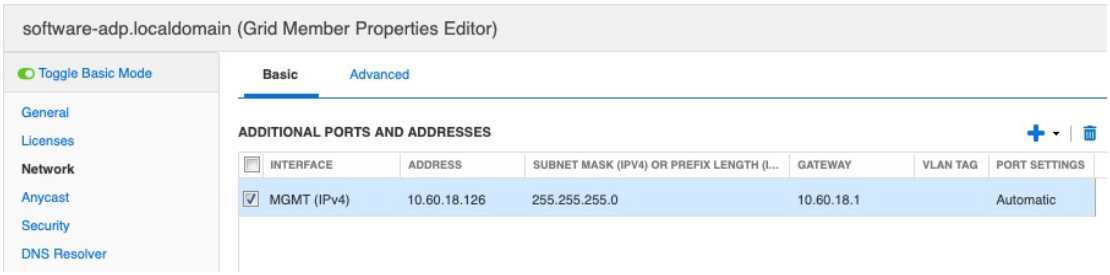
Go to the **Network** tab.

Scroll down in **Basic** Tab to **Additional Ports and Addresses** section.

Click **+** > **MGMT (IPV4)** (Please select the appropriate IP version- v4 or v6).

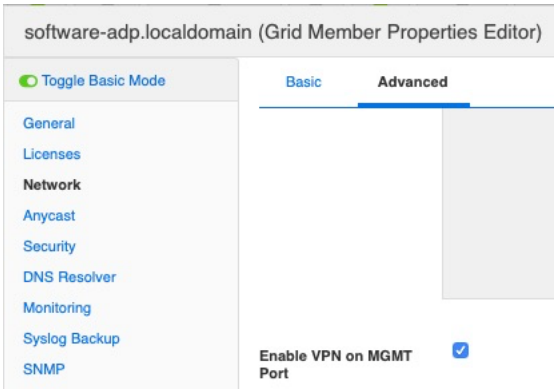


Set the appropriate IP Address, subnet mask and gateway information for the management interface of the software ADP member.



Switch to the **Network** -> **Advanced** tab.

Check the box next to **Enable VPN on MGMT Port**.

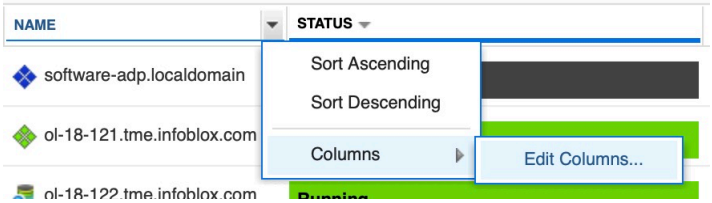


Click **Save & Close**.

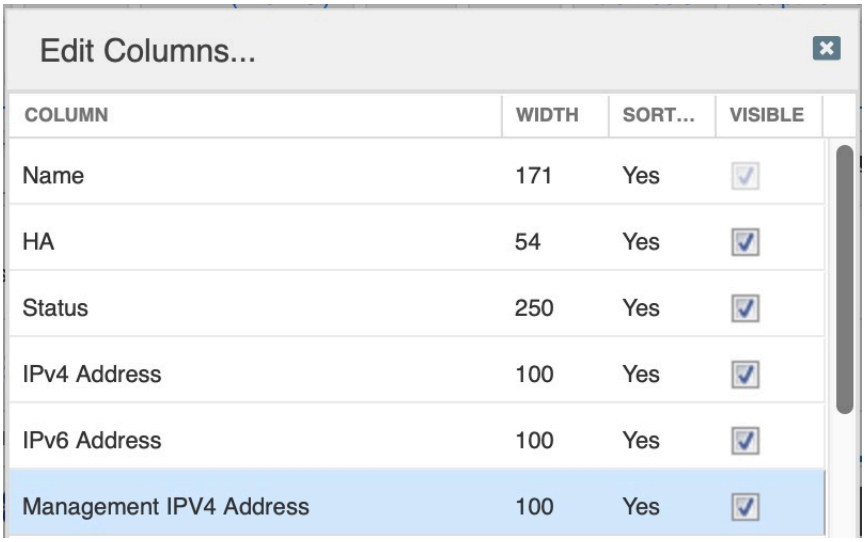
Click **Yes** to confirm at the warning message.

Enable Management IPv4 Address column in the Grid Manager GUI:

Hover over a button in the header row and click on the downwards facing arrow that appears. Expand the **Columns** menu item and select **Edit Columns**.

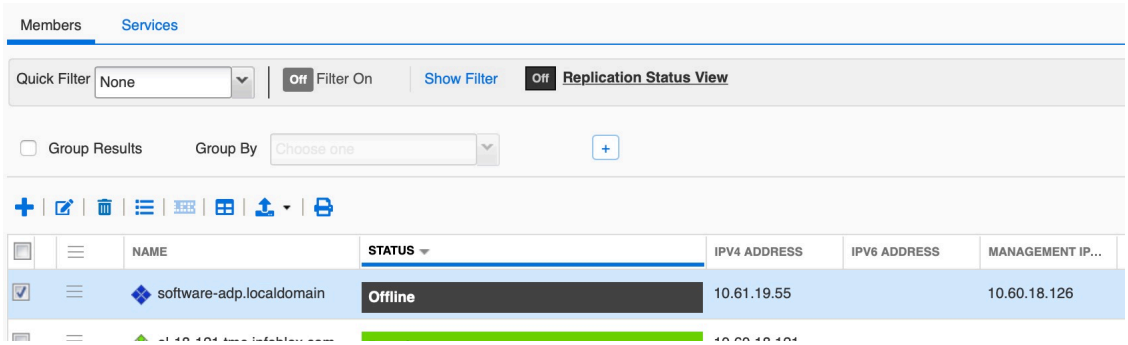


Check the box under the **Visible** column for **Management IPv4 Address.**



Click **Apply**.

You can now view the Management IP address for your server in the general display:



Making the member Join the Grid from Console

This section describes the steps to add mandatory licenses and networking information on the new Software ADP member through the use of its console and then making the member join the Grid.

Connect to the console of the new member.

Login using the default login (admin/infoblox)

Apply the appropriate license using either the **set license** or **set temp_license** command.

In this guide, we are using temporary licenses. Example:

set temp_license

```
                type 'help' for more information


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 Flex Grid Activation license
 17. Add Flex Grid Activation for Managed Services license

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

Select option **4**.

```
 14. Add Cloud Network Automation license
 15. Add Security Ecosystem license
 16. Add Flex Grid Activation license
 17. Add Flex Grid Activation for Managed Services 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: _
```

In our example we are deploying IB-V825. So, select option **4.**
Note: Please choose the option for the model you are going to deploy. For IB-FLEX, see https://docs.infoblox.com/display/nios84/About+IB-FLEX

The appliance will restart shortly after the NIOS license is applied. Once the server completes the restart process, add appropriate licenses using set license command. In our example here, we use the **set temp_licenses** command multiple times to apply the required licenses:

```
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 Threat Protection (Software add-on) license
 12. Add Threat Protection Update license
 13. Add Response Policy Zones license
 14. Add FireEye license
 15. Add DNS Traffic Control license
 16. Add Cloud Network Automation license
 17. Add Security Ecosystem license
 18. Add Flex Grid Activation license
 19. Add Flex Grid Activation for Managed Services license

Select license (1-19) or q to quit: _
```

Select option **5** (**DNS Server license).**

```
Select license (1-19) or q to quit: 5

This action will generate a temporary 60-day Add DNS Server license.
Are you sure you want to do this? (y or n): _
```

Select option 7 (**Add Grid license**).

```
Select license (1-19) or q to quit: 7

This action will generate a temporary 60-day Add Grid license.
Are you sure you want to do this? (y or n): _
```

Select option 11 (**Add Threat Protection (Software add-on) license**).

```
Select license (1-19) or q to quit: 11

Adding license(s) requires a product restart.


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

After Adding Threat Protection (Software add-on) License, the appliance will restart. Log back in once the restart completes.

Apply the appropriate license to enable the **threat protection** feature via the **set temp_license** command.

Select option **10** (**Add Threat Protection Update license**).

```
Select license (1-17) or q to quit: 10

This action will generate a temporary 60-day Threat Protection Update license.
Are you sure you want to do this? (y or n): y_
```

If not already configured, issue the following command to configure the LAN1 interface:

set network

Note: This IP address must match the IP address configured for the server in the grid that you will be joining it to. At the **Become grid member** prompt, enter 'n' at this time. You will join it to your Grid using the **set membership** command further down in the steps provided here.

```
Infoblox >
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: 10.61.19.55
Enter netmask [Default: 255.255.255.0]:
Enter gateway address [Default: 10.61.19.1]:
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:         10.61.19.55
  IPv4 Netmask:         255.255.255.0
  IPv4 Gateway address: 10.61.19.1
  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
        Are you sure? (y or n): _
```

The appliance will restart in order to reload its network interfaces. Once complete, log back in and configure the server's management interface by issuing the following command:

set interface mgmt

Enter **y** when asked to enable the management interface.

Then enter the appropriate IP address info for the management port (which again must match what has been set in the Grid which this server will be joining).

In our example we are not using IPv6 addressing. Hence we will not configure it.

Select **n** for the option **Configure Management IPv6 network settings?**

Select **n** for the option **Restrict Support and remote console access to MGMT port?**

Select **y** at the confirmation prompts. The management interface is now enabled.

```
Infoblox >
Infoblox >
Infoblox > set interface mgmt
Enable Management port? (y or n): y
Enter Management IP address: 10.60.18.126
Enter Management netmask [Default: 255.255.255.0]:
Enter Management gateway address [Default: 10.60.18.1]:
Configure Management IPv6 network settings? (y or n): n
Restrict Support and remote console access to MGMT port? (y or n): n
  Management IPv4 address:         10.60.18.126
  Management IPv4 netmask:         255.255.255.0
  Management IPv4 Gateway address: 10.60.18.1
  Restrict Support and remote console access to MGMT port: false
        Is this correct? (y or n):  y
        Are you sure? (y or n):  y
 The management port settings have been updated
Infoblox >
```

In this step, the server is joined to your Grid by executing the following command in the console:

Set membership

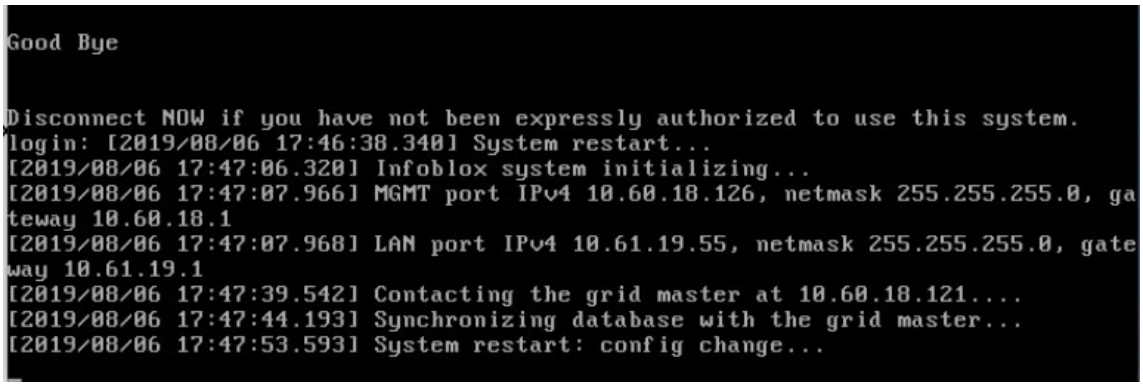
Enter the appropriate IP address of the Grid Master LAN1 interface, along with Grid name and Grid Shared Secret. By default, the Grid name is **Infoblox** and the shared secret is **test**. These are case sensitive.

When prompted for **Enable grid services on the Management port?**, select **y**. This will enable the server to join your Grid using its mgmt interface, instead of LAN1 as is done by default.
Enter **y** at the confirmation prompts.

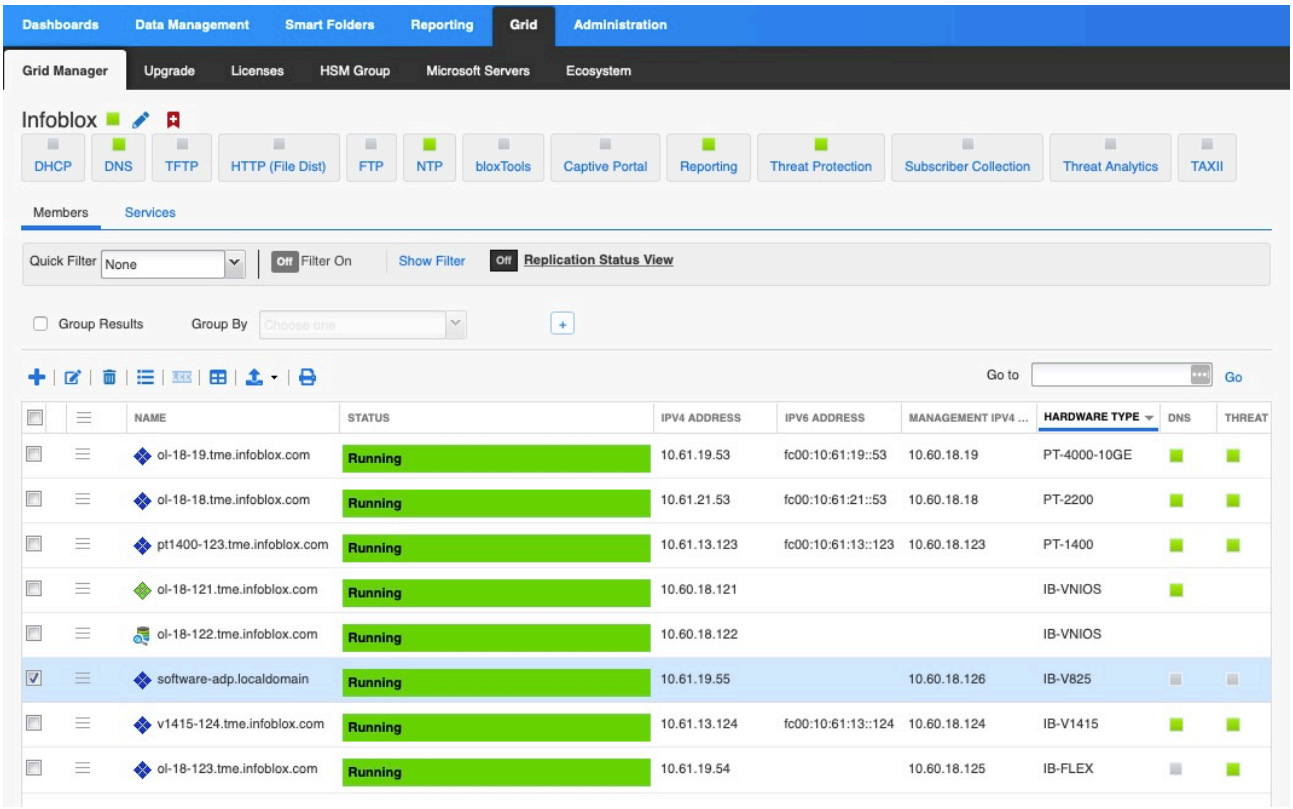
```
Infoblox >
Infoblox >
Infoblox > set membership
Join status: No previous attempt to join a grid.
 Enter New Grid Master VIP: 10.60.18.121
Enter Grid Name [Default Infoblox]:
Enter Grid Shared Secret: test
Enable grid services on the Management port? (y or n): y
  Join grid as member using the Managment port with attributes:
     Grid Master VIP:     10.60.18.121
     Grid Name:           Infoblox
     Grid Shared Secret:  test

WARNING: Joining a grid will replace all the data on this node!
        Is this correct? (y or n): y
```

The server will now attempt to contact Grid Master and synchronize database. Multiple restarts are expected during this process.



Once the server has completed the join process to your grid, it will show as online and running when viewing its status in your Grid Manager GUI.

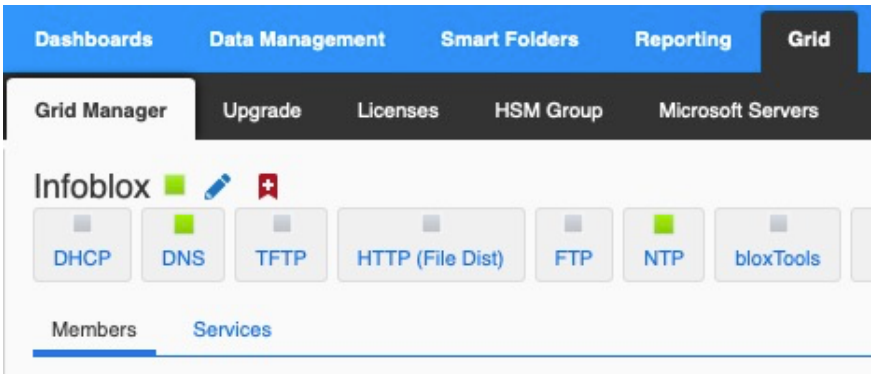


Enabling DNS resolver

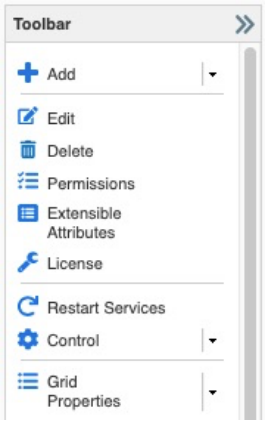
To add an appropriate DNS resolver to the Grid, if not already configured, please follow the steps listed below.

Note: If this ADP is part of a Subscriber Services Site, the DNS resolver should not be inherited from the Grid. Please review release notes and documentation on Subscriber Services

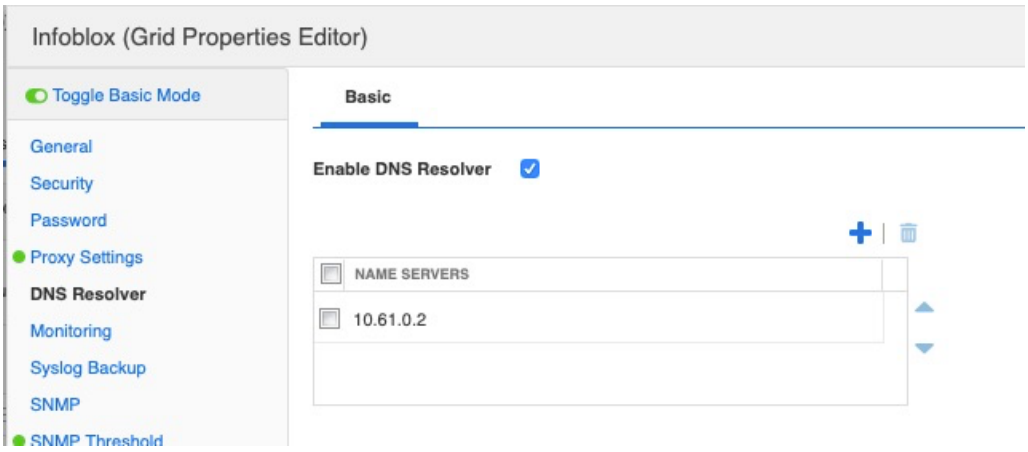
Go to **Grid** > **Grid Manager** > **Members**



From **Toolbar,** Click **Grid Properties**



Click **DNS Resolver** tab in **Grid Properties Editor**.
Click **Enable DNS Resolver**.
Click **+**
Add the IP address(es) to be used for the DNS resolver.



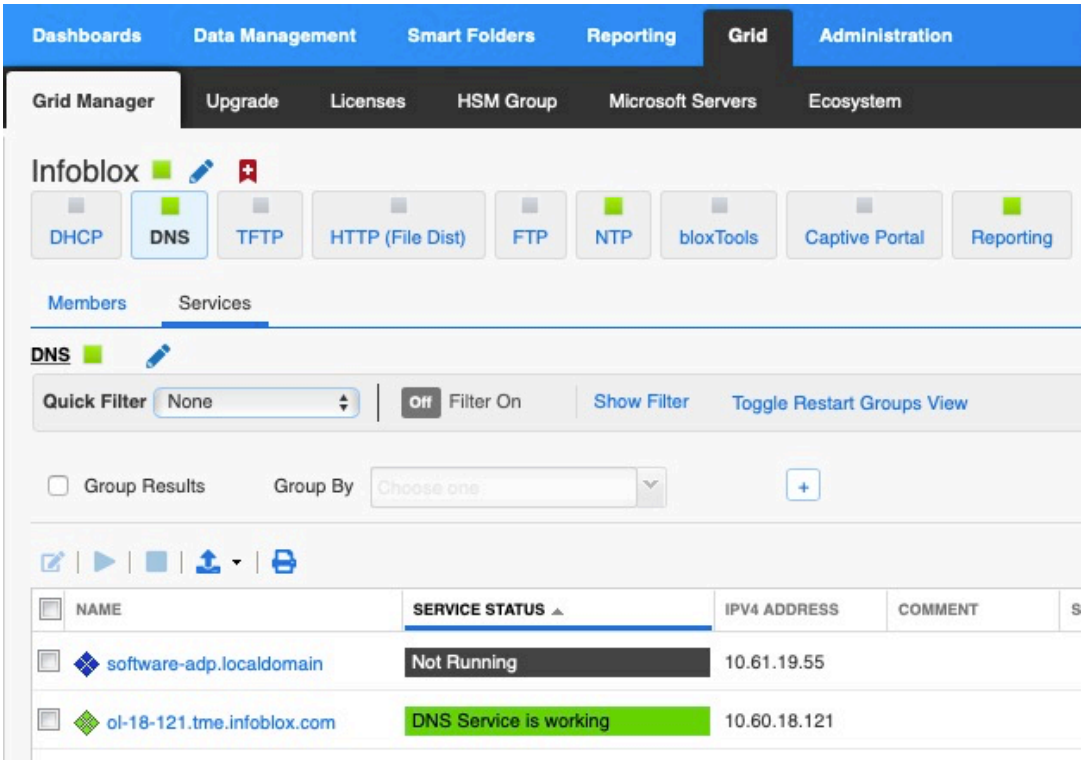
Click Save & Close.

Enabling Services on Software ADP appliance

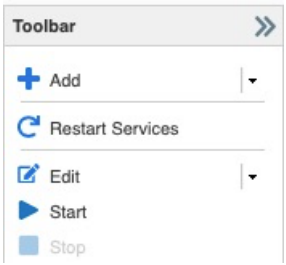
After the new server has joined the grid, it's time to start the DNS and Threat Protection services.

To start DNS Service, Go to the **Grid** > **Grid Manager** > **DNS** > **Services** tab.

Select the appropriate ADP member for which the DNS services need to be turned on.



Click **Start** from **Toolbar.**

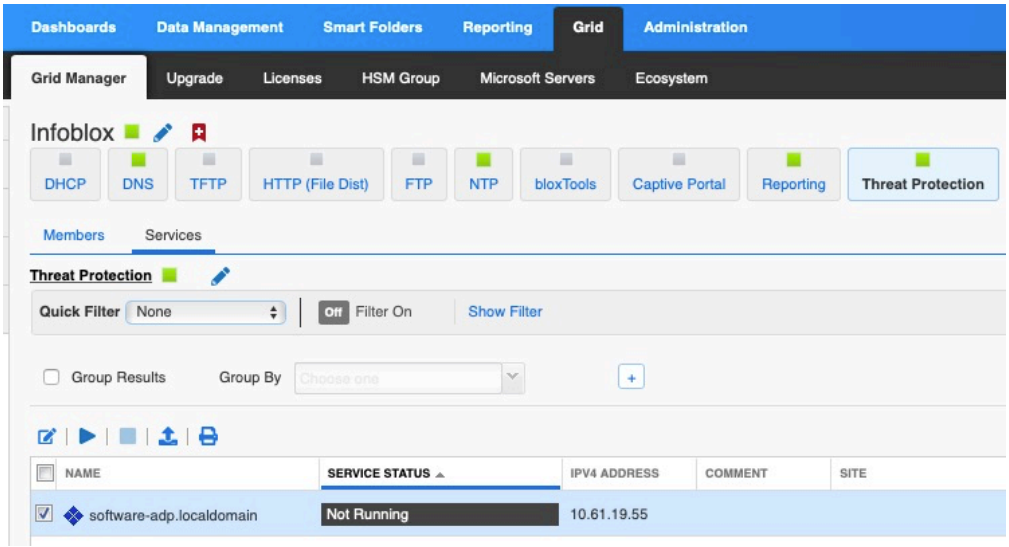


Click **Yes** when prompted for **Start Member DNS Service**.

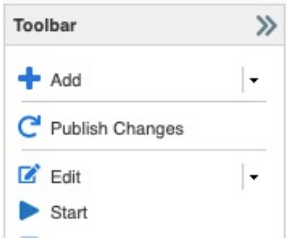
To verify if the DNS service started, check the **Services Status column.** It will report "**DNS Service is working**" once it has finished starting. Click on the Refresh button as necessary (the page does not automatically refresh).

To start Threat Protection Service, Go to the **Grid** > **Grid Manager** > **Threat Protection** > **Services** tab.

Select the appropriate ADP member for which the **Threat Protection** service needs to be turned on.



Click **Start** from **Toolbar**.



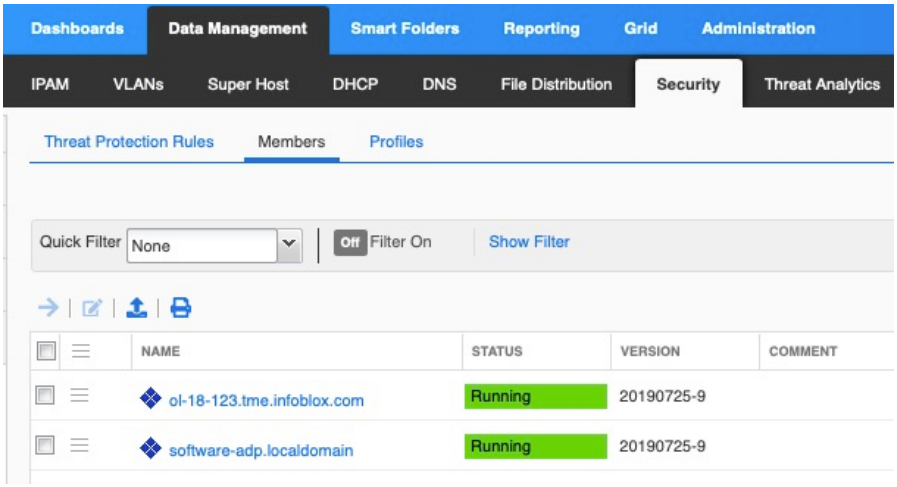
Click **Yes** at the **Start Member Threat Protection Service** prompt.

Click **Restart** (the prompt for Restart Services will appear twice).

To verify if the Threat Protection service started successfully, check the **Services Status column.** It must say, **"Threat Protection Service is working**". Click on the refresh button until this updates, as the page is not refreshed automatically.

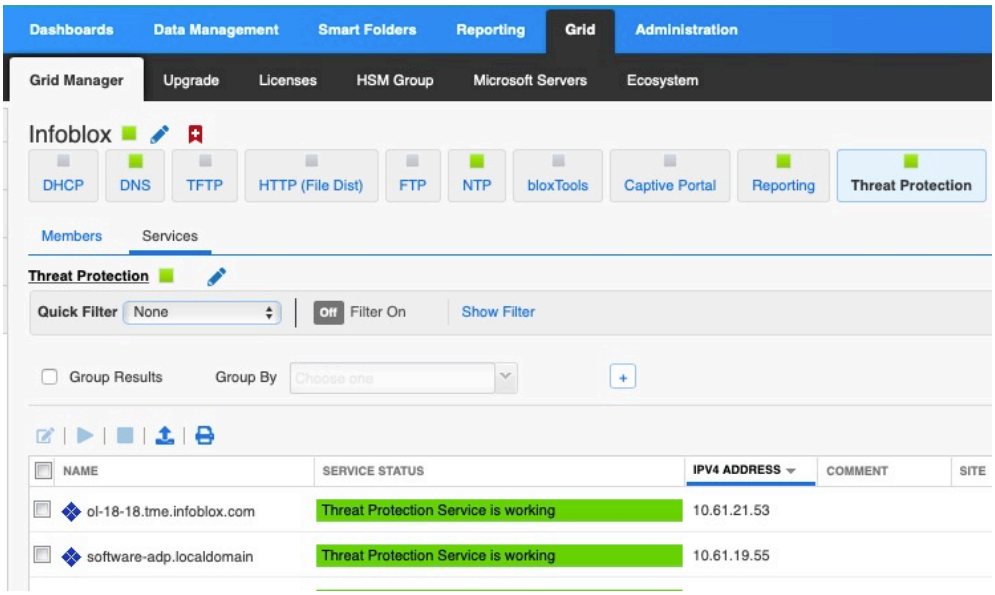
Viewing all Advanced DNS Protection appliances

All Infoblox Active DNS appliances that are part of a Grid can be viewed from a single location, by going to **Data Management** > **Security** > **Members**.



The other place where we can view only the ADP appliances under one location is by going to

Grid > **Grid Manager** > **Threat Protection** > **Services**.



Rules supported by Advanced DNS Protection

Infoblox ADP supports system rules, auto-generated rules, and custom rules. New system rules are added through rule updates.

System Rules

System rules are predefined threat protection rules that are built into ADP. You can enable an entire category of system rules, as well as individual rules. Although you cannot add or delete system rules, you can change some parameters, enable and disable. For most system rules, you can also modify the Action and Log Severity.

Auto Rules

Auto rules are firewall rules that are automatically defined by NIOS for blocking traffic for disabled services and ports. These rules can be grouped into different rule categories and are enabled or disabled automatically. You cannot enable or disable autogenerated rules, however, you may be able to set the log severity and control logging for some of these rules. Autogenerated rules are automatically enabled or disabled and are reconfigured based on the current running services and the configuration of the appliance.

Custom Rules

Based on your security needs, you can define custom rules using predefined rule templates. Custom rules are typically whitelisting and blacklisting rules that utilize rate limiting to detect suspicious UDP and TCP traffic. You can create up to 500 custom rules for each rule template offered by ADP. The appliance logs a syslog message if there are more than 500 rules for a specific rule category. You can remove some rules in order to create new ones for that category.

You can add or delete custom rules at the Grid level only. While you cannot add or delete custom rules for Grid Members and/or profiles, you can enable, disable, and modify some rule parameters at the appropriate place, which is recommended to be in Profiles.

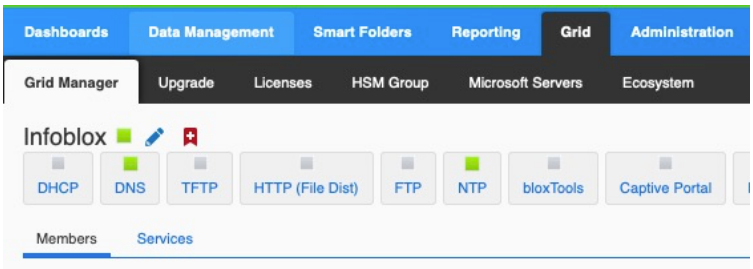
Adding Threat Protection Ruleset

The Threat Protection Ruleset can be added manually or automatically. In this guide, we demonstrate the automatic Ruleset deployment as it is considered a best practice to use automatic downloads for Threat Protection Rulesets.

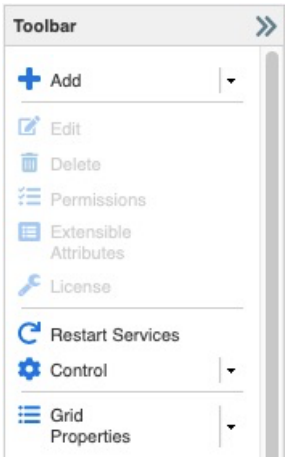
Proxy Setting on the Grid

Complete the following steps if you are using proxy server for web connections; otherwise skip this section and go to next section titled “Automatic Download”.

Go to **Grid** > **Grid Manager** > **Members**.

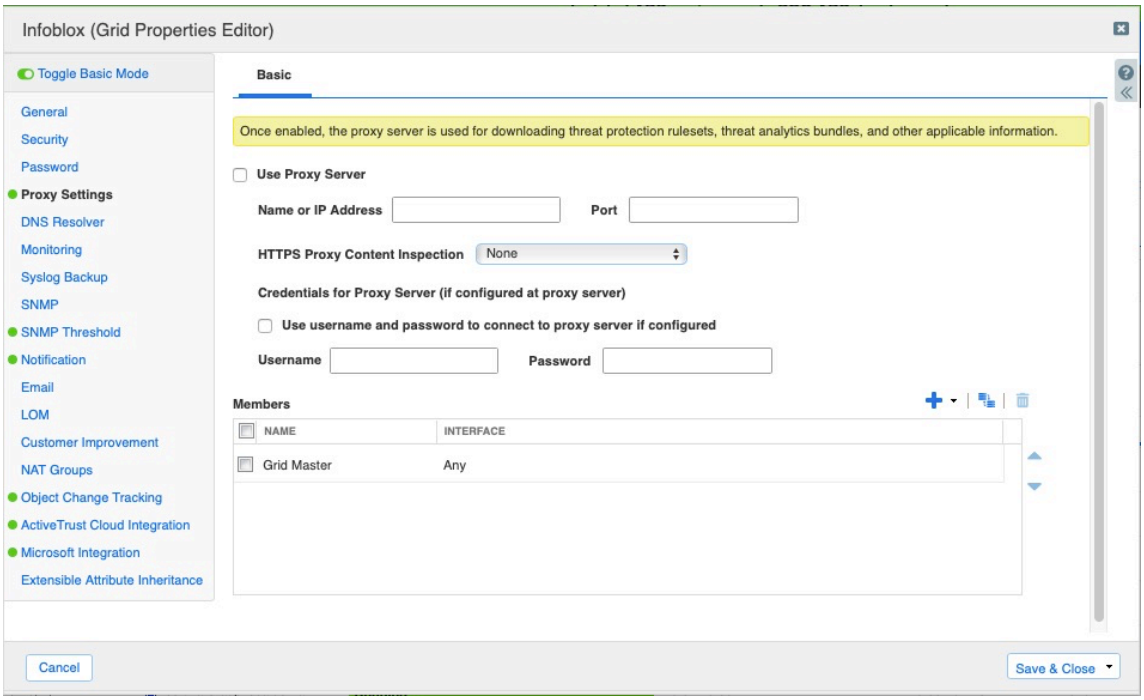


Click **Grid Properties** From **Toolbar**.



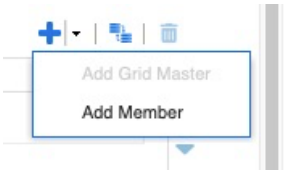
From Toggle Advanced Mode, click **Proxy Settings**.

Click **Use Proxy Server**.

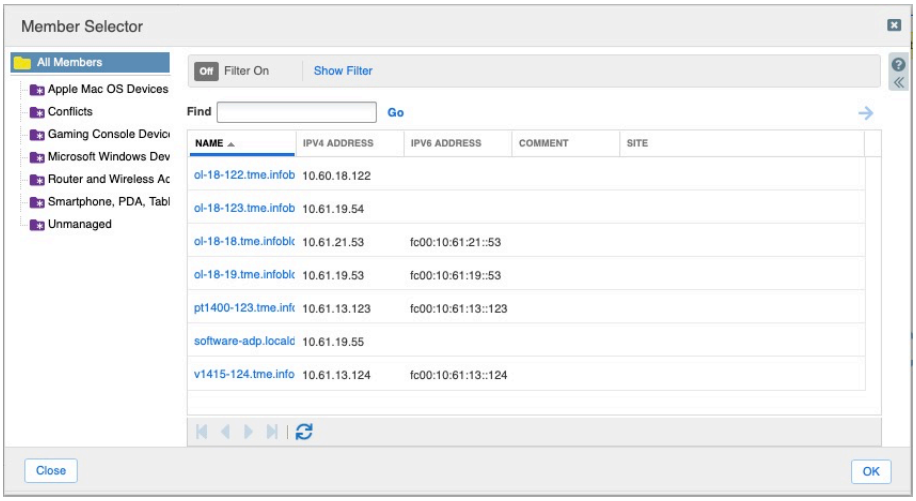


Add the appropriate Name or IP Address of the Proxy Server and the appropriate port number.

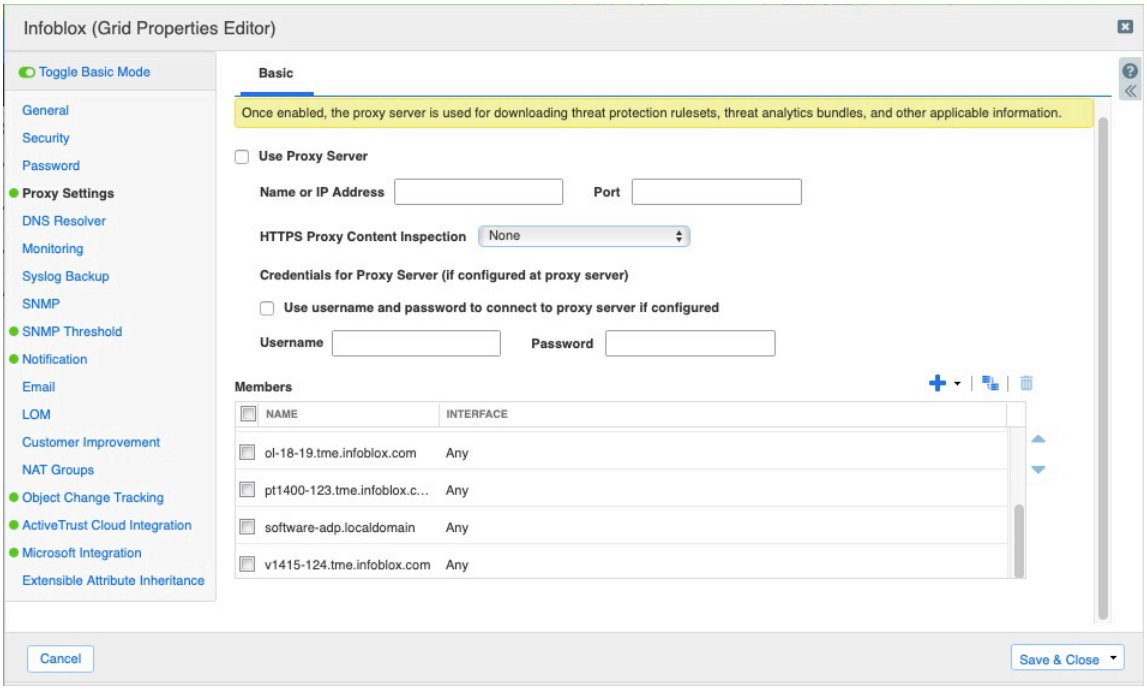
Add All Members in the Grid in Members Section by clicking **+** and then select **Add Member**.



Select all members in the Member Selector dialogue.



Click **OK**.

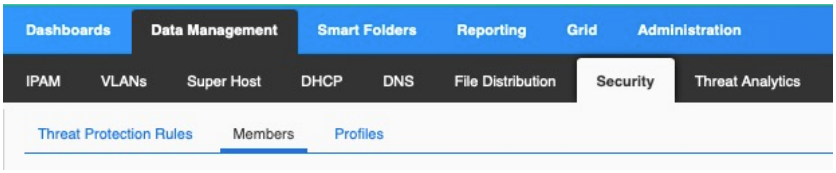


Click **Save & Close**.

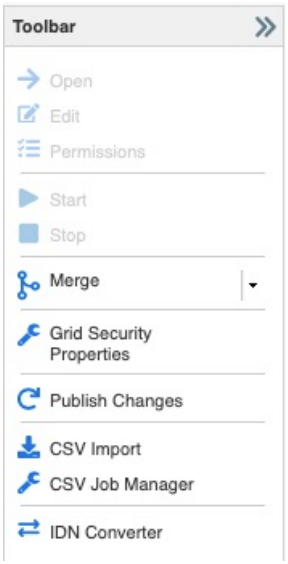
Automatic Download

This section describes the method to enable automatic download of the Threat Protection Ruleset.

Go to **Data Management** > **Security** > **Members**.

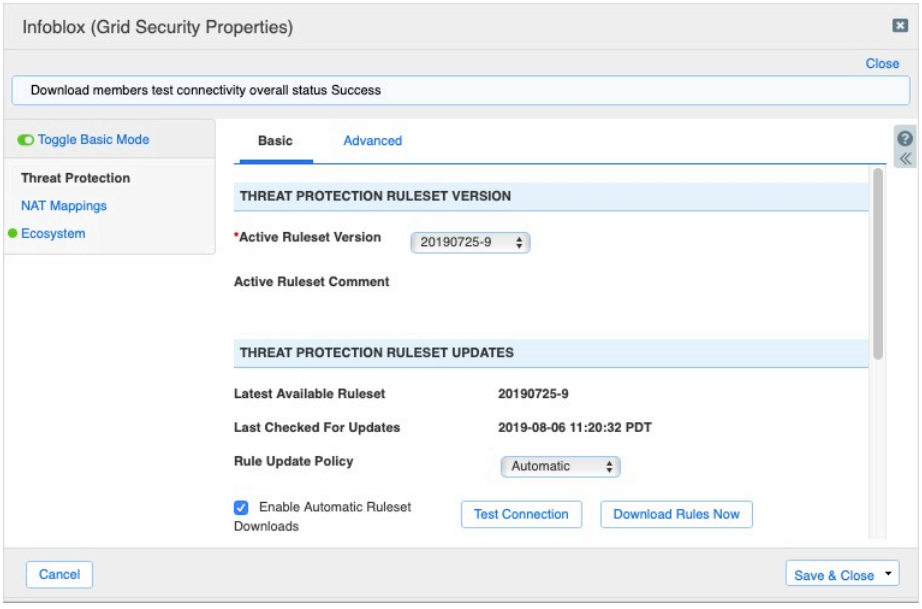


Click **Grid Security Properties** from **Toolbar**.



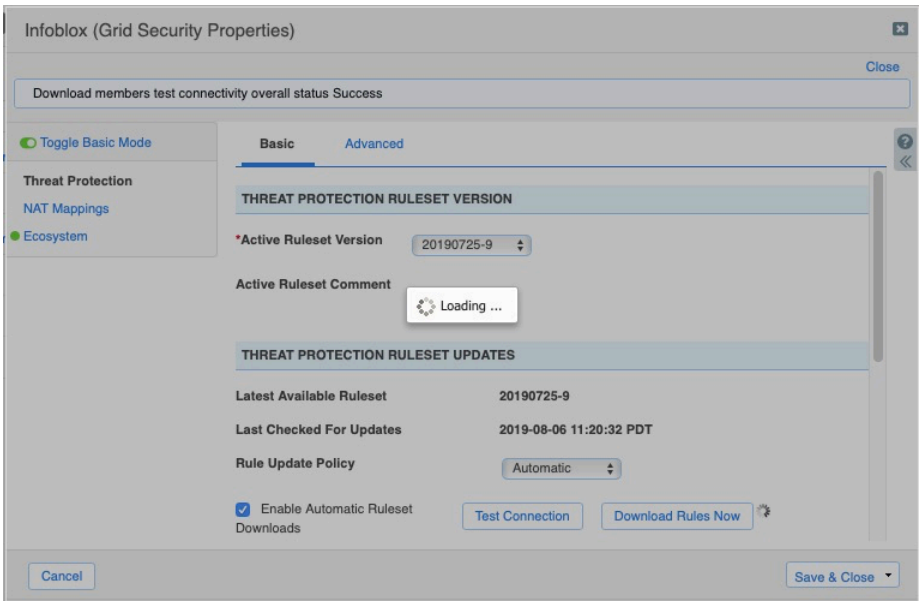
Select option **Enable Automatic Ruleset Downloads** and Click **Test Connection** to verify connectivity to the Ruleset portal.

Note: This will contact ts.infoblox.com directly from the Grid Master. If you need to use a proxy server for this connection, refer to the previous section titled "**Proxy Setting**".
A light blue banner displaying the message "**Download members test connectivity overall status Success**" will appear if this connection is successful.



Click **Download Rules Now**.

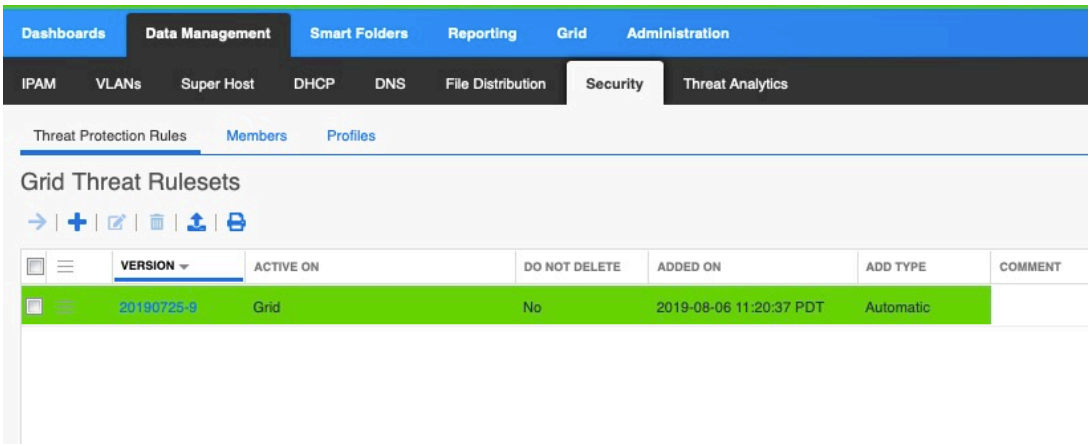
Wait for the download to complete.



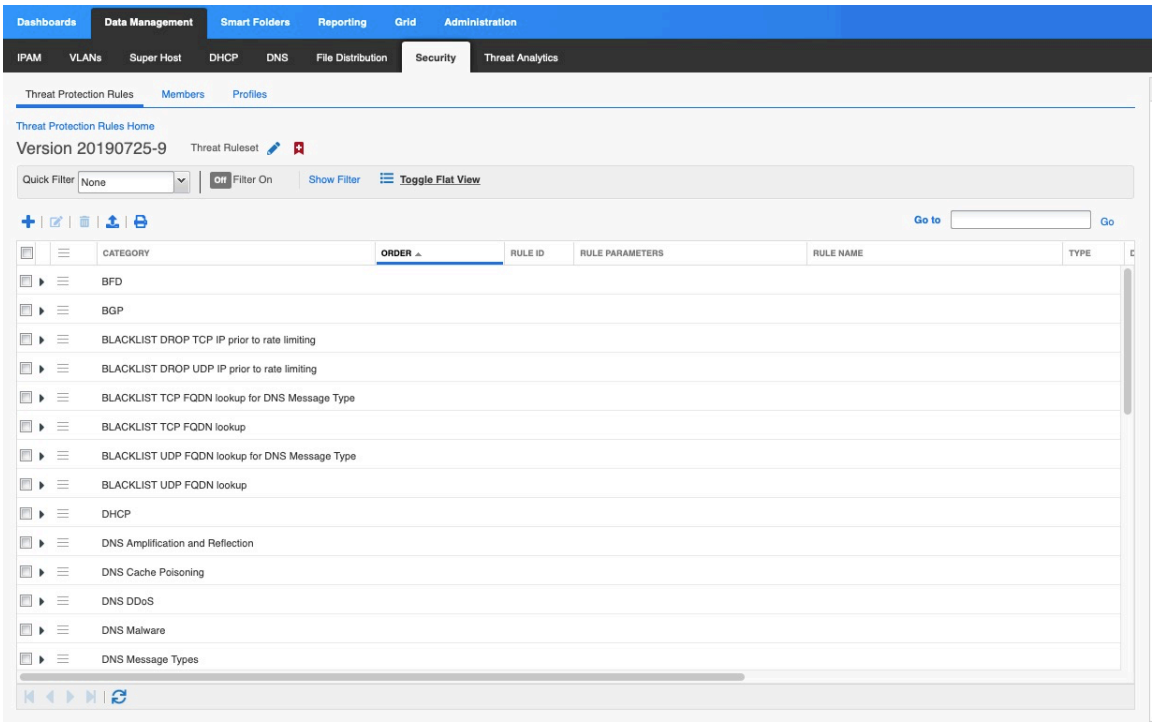
Click **Save & Close**.

Once the download is complete you are going to see the ruleset downloaded under;

Data Management > **Security** > **Threat Protection Rules**



Click on the ruleset to view its content,



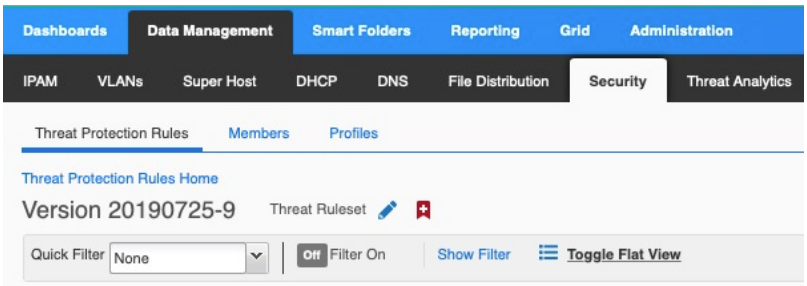
Creating Custom Ruleset

Infoblox Advanced DNS Protection supports a custom rule templates from which you create new custom rules. Note that when you use a specific rule template to create custom rules, the new rules reside in their respective rule categories.

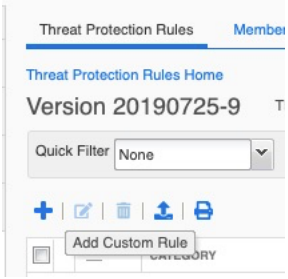
For each rule you create, you can define the Events per second value to determine the number of events per second that will be logged for the rule. In our example we are creating a custom rule that will block UDP DNS queries for domain foo.foo.foo.

To create this custom rule:

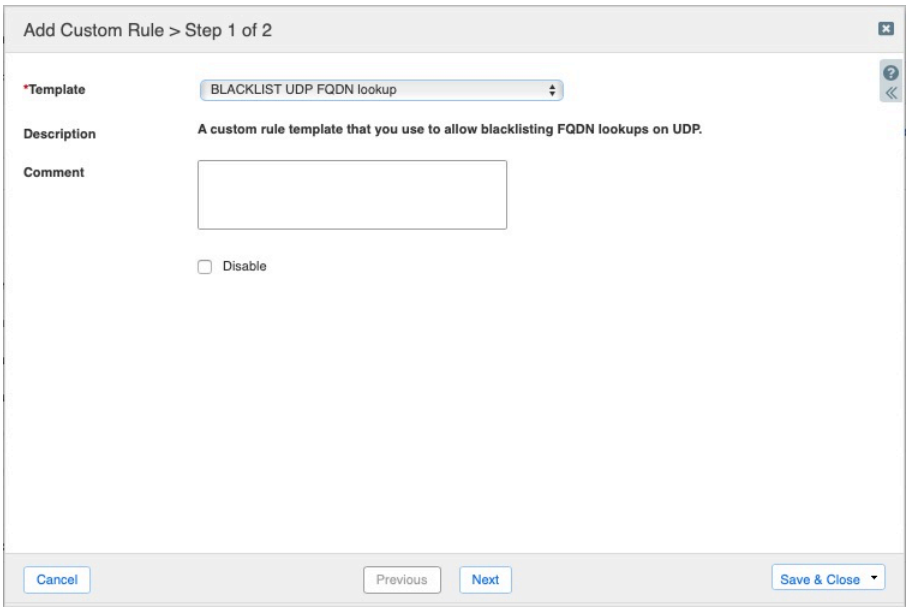
Go to **Data Management** > **Security** > **Threat Protection Rules** tab



Click **+**



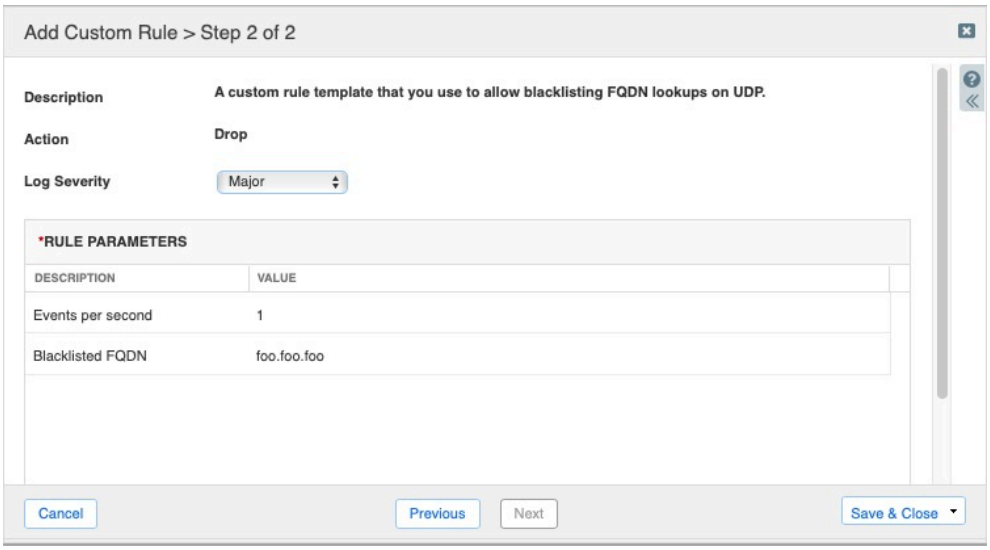
From the drop-down list, select the appropriate template. In our example we select **BLACKLIST UDP FQDN lookup**



Click **Next**

Select appropriate Log Severity. We leave it at default value, which is **Major.**

Add **foo.foo.foo** in the **Value** field for Blacklisted **FQDN**



Click **Save & Close**

Click **Publish** to bring up pop-up window

Click **Publish** to apply changes

To verify the custom rule configuration, send a DNS query (**dig @<LAN1-IP> foo.foo.foo**) to the LAN1 IP address of the ADP appliance. The query is not going to be resolved as expected and a log message confirms the query is dropped.

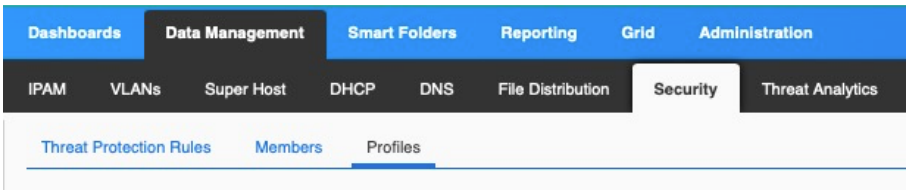
```
CEF:0|Infoblox|NIOS Threat|8.4.0-381062|120303001|Blacklist:foo.foo.foo|7|src=10.61.19.13 spt=58289 dst=10.61.19.55 dpt=53 act="DROP" cat="BLACKLIST UDP FQDN lookup" nat=0 nfpt=0 nlpt=0 fqdn=foo.foo.foo hit_count=1
```

Creating Profiles

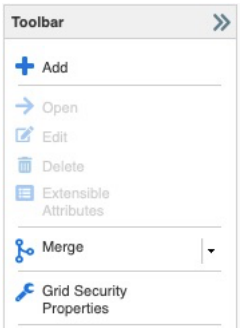
The ADP Profiles enables groups of members to have the same tuned ADP rulesets. Previously it was managed either as a Grid wide ruleset or every single member had to be individually managed. The cloning of profiles can be used to enable testing of ruleset tuning changes, which allow a rapid and accurate reversion, as well as implementing change control. Multiple profiles also allow you to match rulesets with customer profile. For example NATed Enterprise vs subscriber vs customer ISP.

To create a profile,

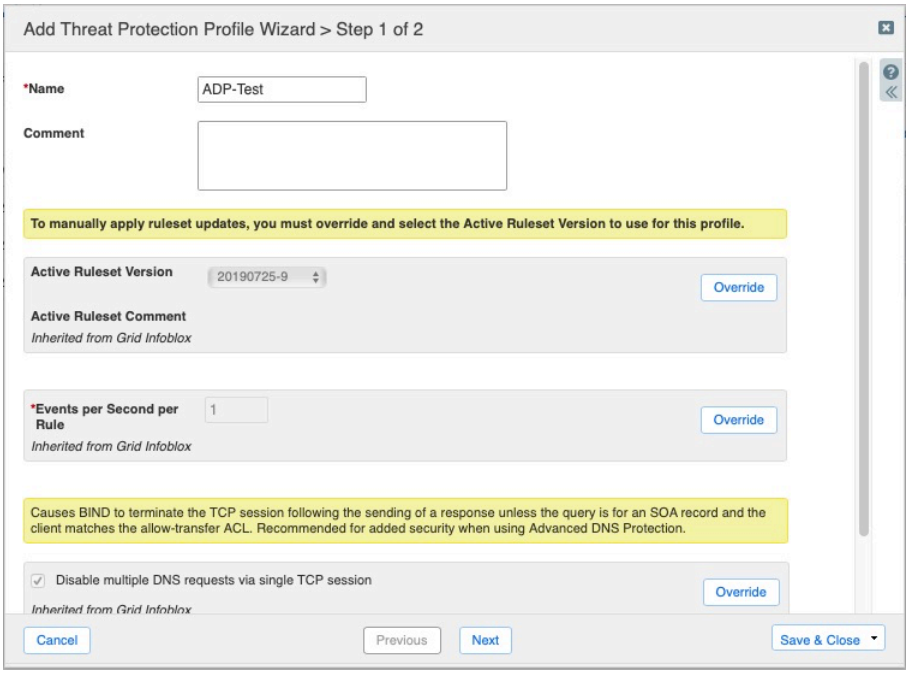
Go to **Data Management** > **Security** > **Profiles**



Click **Add** from **Toolbar**



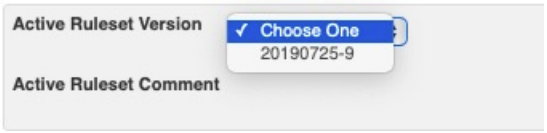
Enter an appropriate name for the profile.



Select a ruleset from **Active Ruleset Version** drop down menu

By default, this field has value inherited from the Grid setting.

To select a different ruleset, Click **Override**

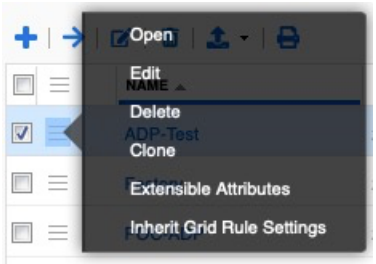


Select the appropriate ruleset from the list.

By default, **Events per Second per Rule** is set to **1**, to change this you can **Click Override** and configure the appropriate value.

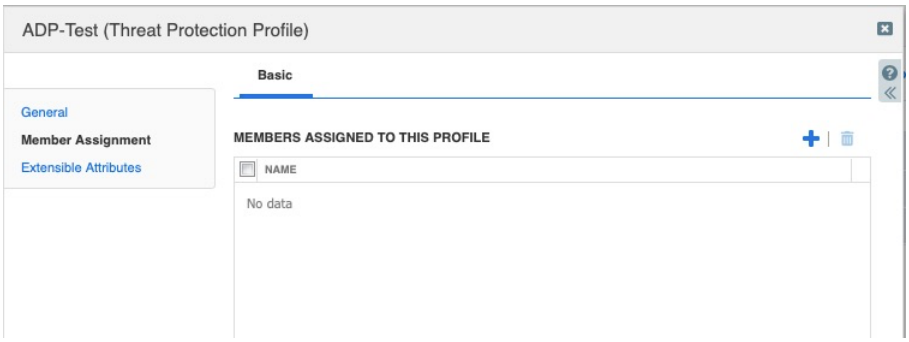
Click **Save & Close**

Click **Properties** icon next to the newly created profile in order to assign a member to it,

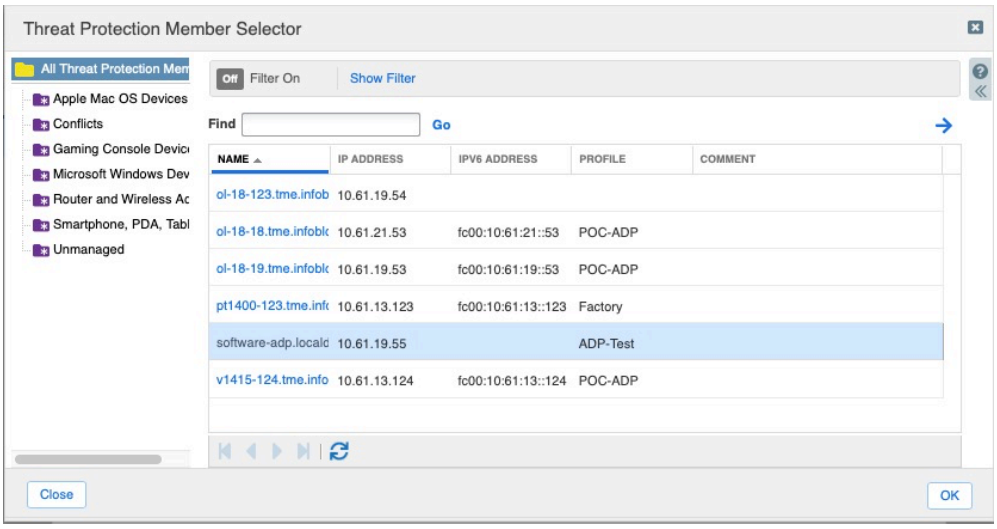


Click **Edit**

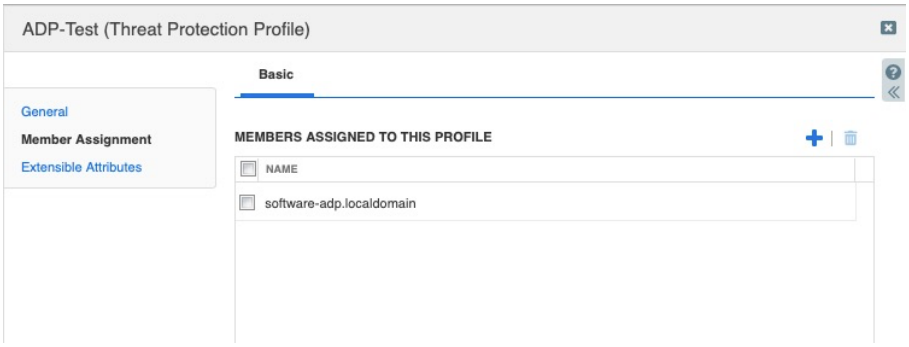
Click **Member Assignment**



Click **+**



Select the member you want to this profile be assigned to,



Click **Save & Close**

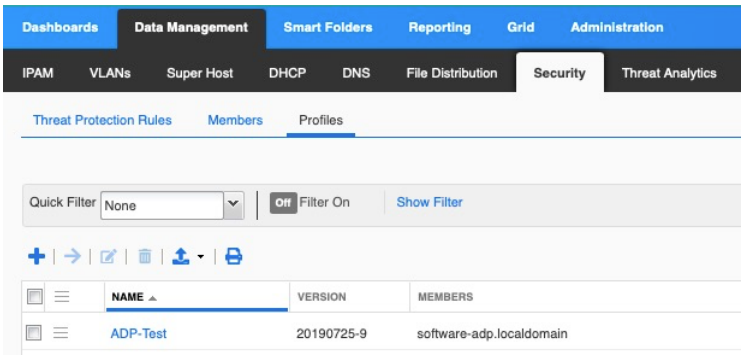
Click **Publish** to apply changes

Click **Publish**

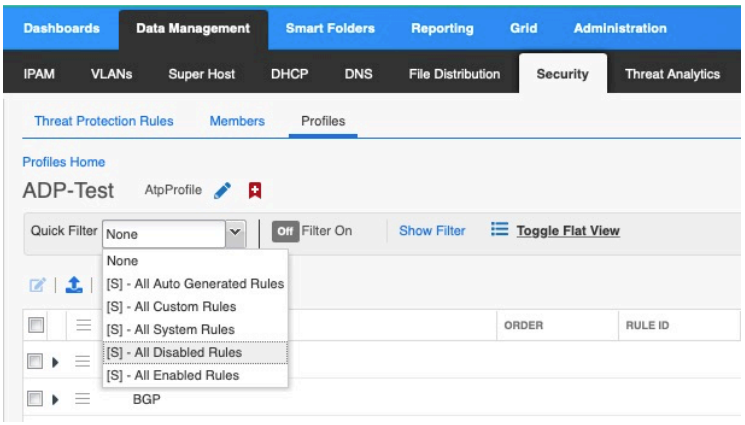
Making changes to rules in Profile

One advantage of Profile is to use it to tune rules. In this section we are going to enable a rule that is by default disabled on the Grid.

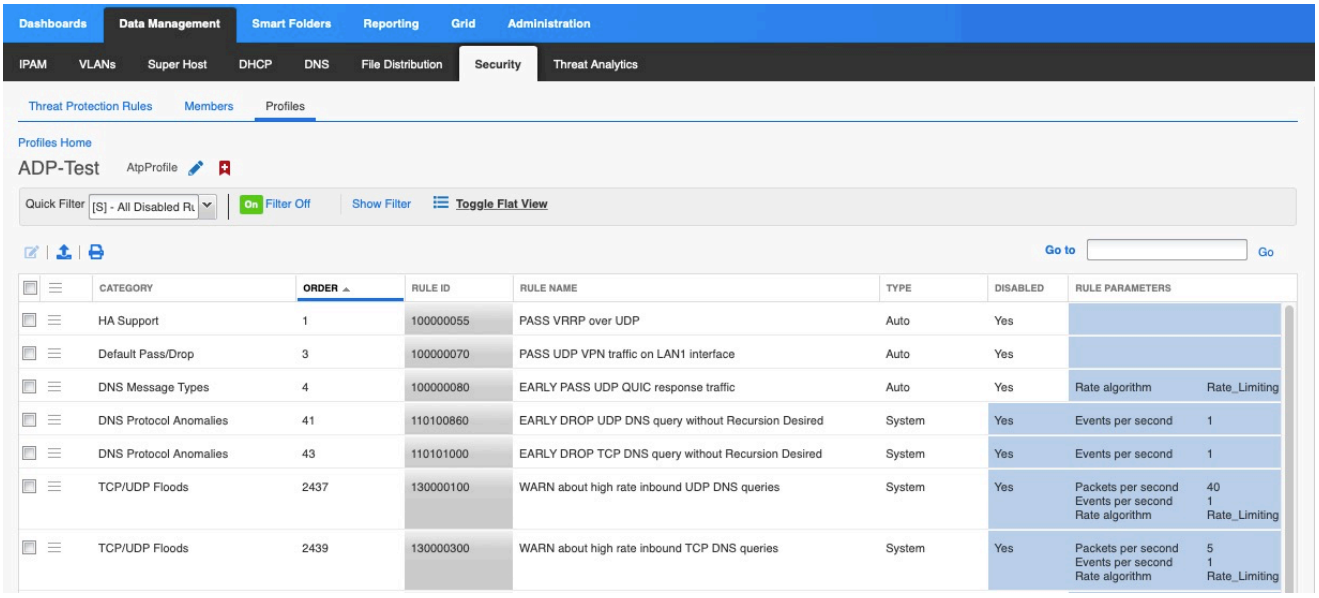
Click on the profile link under **Name** column



Click on **Quick Filter** drop down menu



Click on **All Disabled Rules**



Click on Properties icon next to category **TCP/UDP Floods**

The rule is disabled. Click **Disable** to enable it

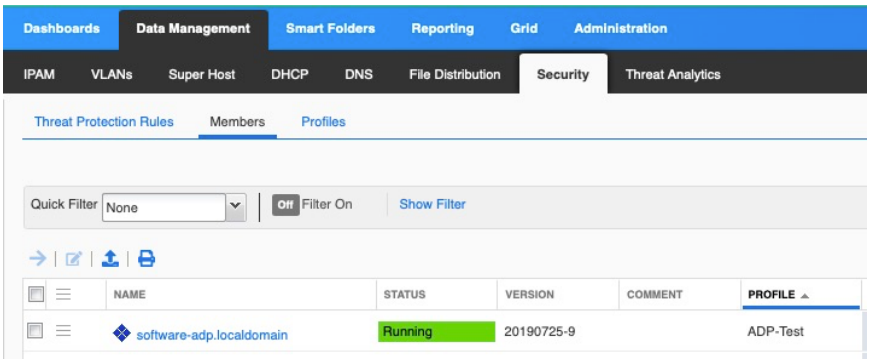
Click **Yes**

Click **Publish**

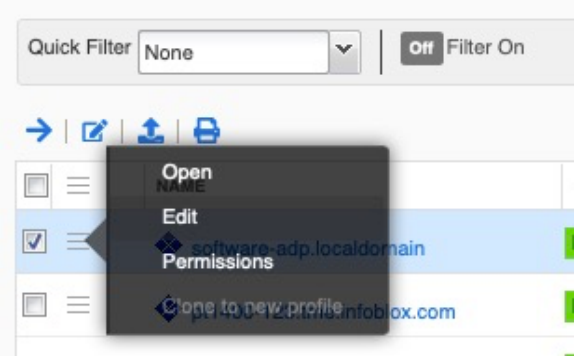
Switching between ADP Profiles

It is easy to move member assignments from one ADP profile to another ADP profile. In our example, the member is assigned to Profile named ADP-Test. If the need is to have member use a different ADP Profile, for example POC-ADP, then:

Go to **Data Management** > **Security** > **Members**

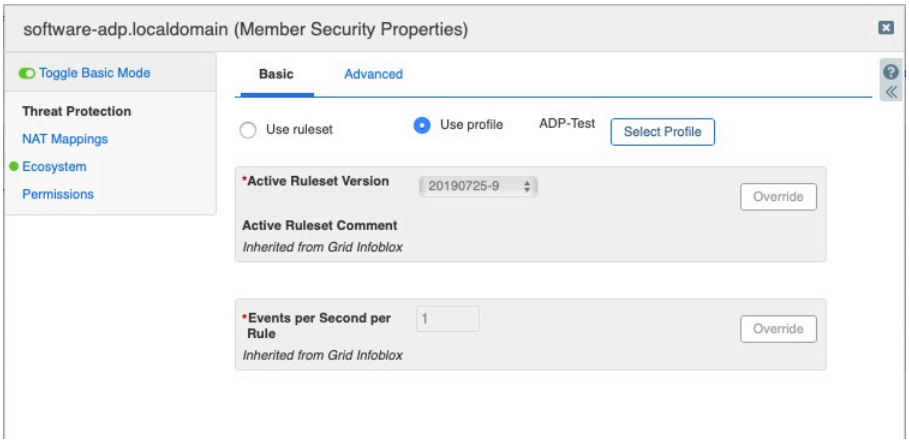


Click on Properties icon for the appropriate member,

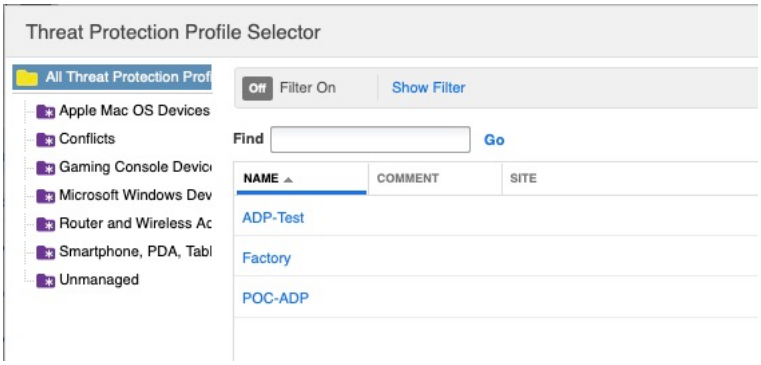


Click **Edit**

On **Basic** Tab under **Threat Protection**, you can select a specific ruleset or specific profile.



Click on **Select Profile**



Select the appropriate Profile from **Threat Protection Profile Selector**

Click **OK**, then **Save & Close**

Click **Publish**

Click **Publish** to apply changes

Click **Save & Close**

Verifying the Infoblox ADP appliance is working correctly

As a last step in the deployment, we can send a query to the ADP appliance to make sure it's configured as expected. Make sure rule 110100200 is not disabled. To do that, send the following query from a terminal that can reach the ADP appliance,

dig -t txt -c chaos VERSION.BIND @<LAN1-IP-Address>

The expected output is that the server is not going to be reached and the command is going to show the following output upon execution,

dig -t txt -c chaos VERSION.BIND @<LAN1-IP-Address>

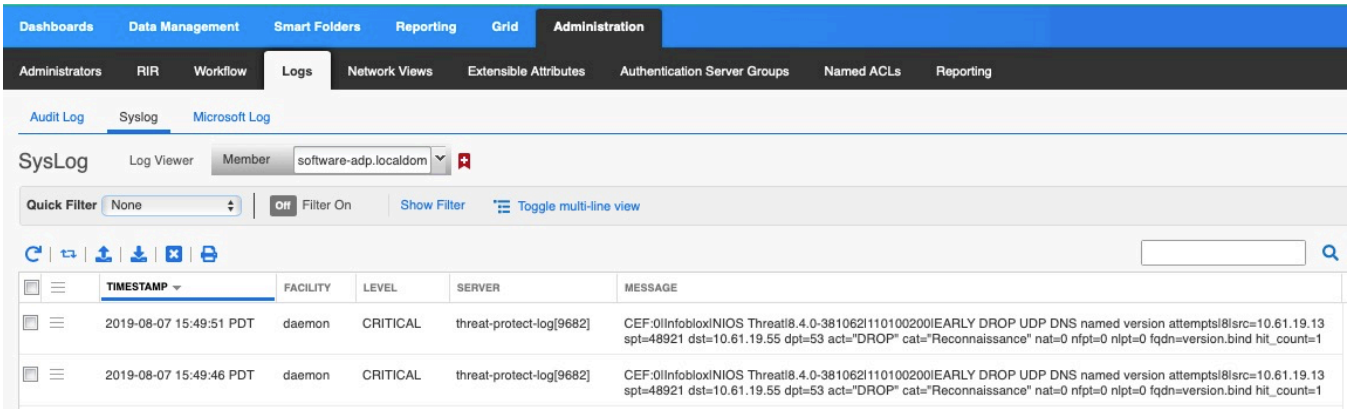
; <<>> DiG 9.8.3-P1 <<>> -t txt -c chaos VERSION.BIND @<LAN1-IP-Address>
;; global options: +cmd
;; connection timed out; no servers could be reached

If you are using nslookup instead of dig, then use the following command,

nslookup -q=txt -class=CHAOS version.bind. <LAN1-IP-Address>

Now go to the **Administration** > **Logs** > **Syslog**

Select the ADP appliance to which the query is sent in Member field.



The following log message confirms that query was received and dropped by design and it verified the correct configuration of the Infoblox ADP appliance. You can see it in context above, and the message details below.

CEF:0|Infoblox|NIOS Threat|8.4.0-381062|110100200|EARLY DROP UDP DNS named version attempts|8|src=10.61.19.13 spt=48921 dst=10.61.19.55 dpt=53 act="DROP" cat="Reconnaissance" nat=0 nfpt=0 nlpt=0 fqdn=version.bind hit_count=1

SNMP Support

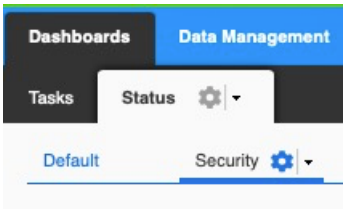
Software ADP supports:

- Existing SNMP threshold traps for software-based ADP platforms
  - Threat Protection Dropped Traffic
  - Threat Protection Total Traffic
  - Flood Threats
    - Alert Rate
    - Drop Rate
- SNMP trap for rule publish failure for software-based ADP platforms

Review the Security Dashboard for Threat Protection Information

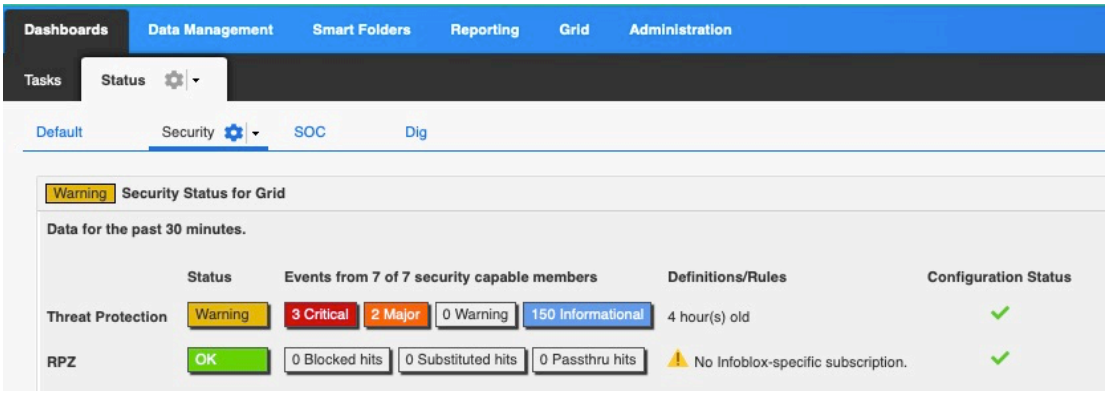
The Security Dashboard is appropriately populated whenever Threat Protection, RPZ, and Threat Analytics services are enabled. The dashboard shows data for last thirty minutes. If data more than 30 minutes is required then go to Reports for that. To review, and explore this dashboard,

Go to **Dashboards** > **Status** > **Security**



Security Status for Grid

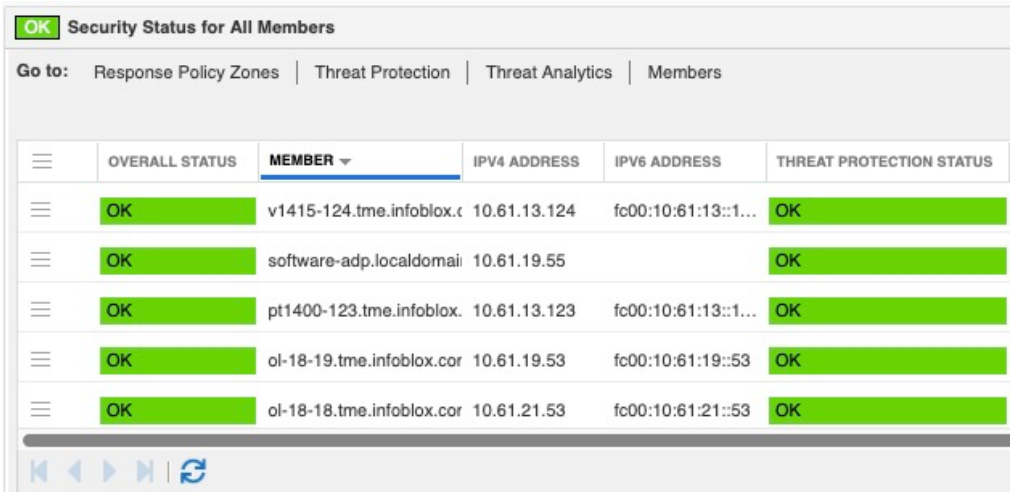
This widget displays the overall security status for the Grid. The **Security Status for Grid** widget shows the Critical, Major, Warning and Informational events for different security services enabled in the Grid, such as Threat Protection, RPZ and Threat Analytics. Grid manager displays this widget only when at least one member in the Grid has the Threat Protection, RPZ or Threat Analytics license installed.



Security Status for All Members

The widget Security Status for All Members shows the information about the status of all the Grid members that support ADP and Threat Analytics. At least one member in the Grid must have Threat Protection, RPZ or Threat Analytics licenses for this widget to be present. The green status means no security incident occurred for last 30 minutes.

Overall Status columns shows current overall Status of the members that support Infoblox ADP. The status can be **OK**, **Warning**, **Critical** or **Unknown**.

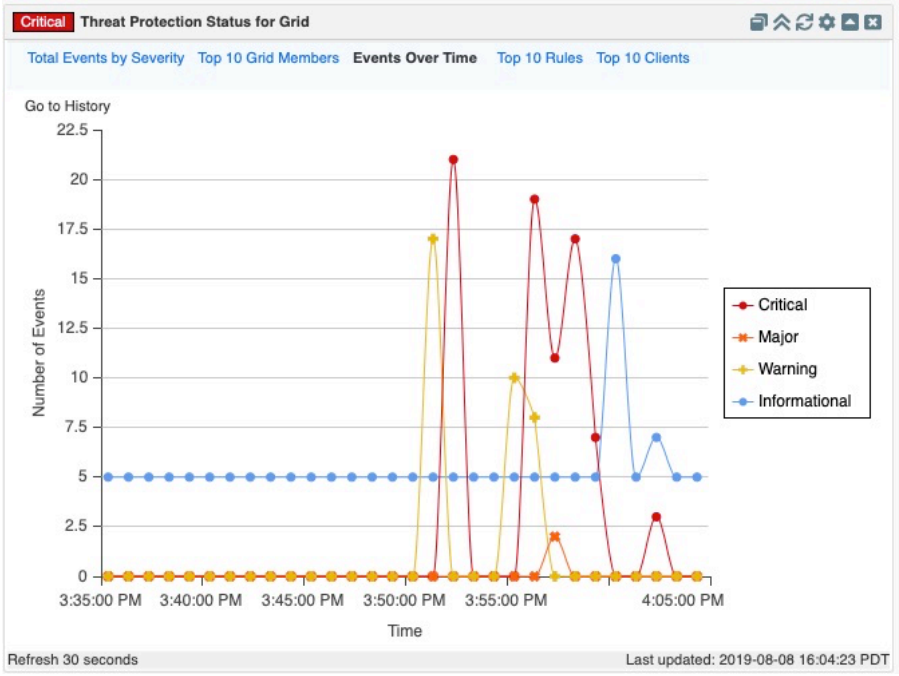


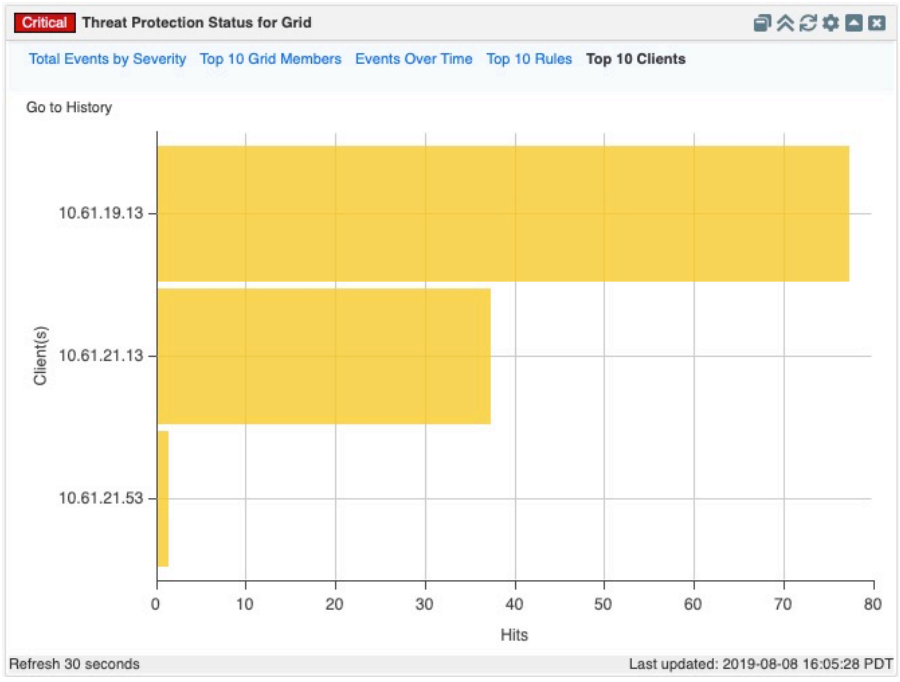
Threat Protection Status for Grid

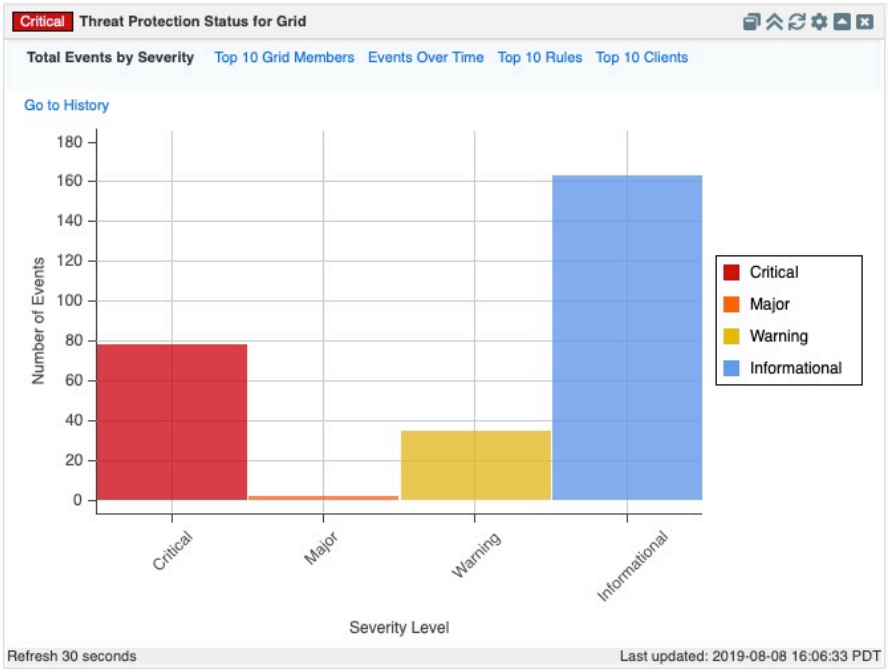
The Threat Protection Status for Grid widget displays the statistical information about the threat protection events triggered on all the members in the Grid that support ADP and Threat Analytics.
To see more detailed view of threat protection status, the **Threat Protection Status for Grid** widget is the place to go. It shows information such as,

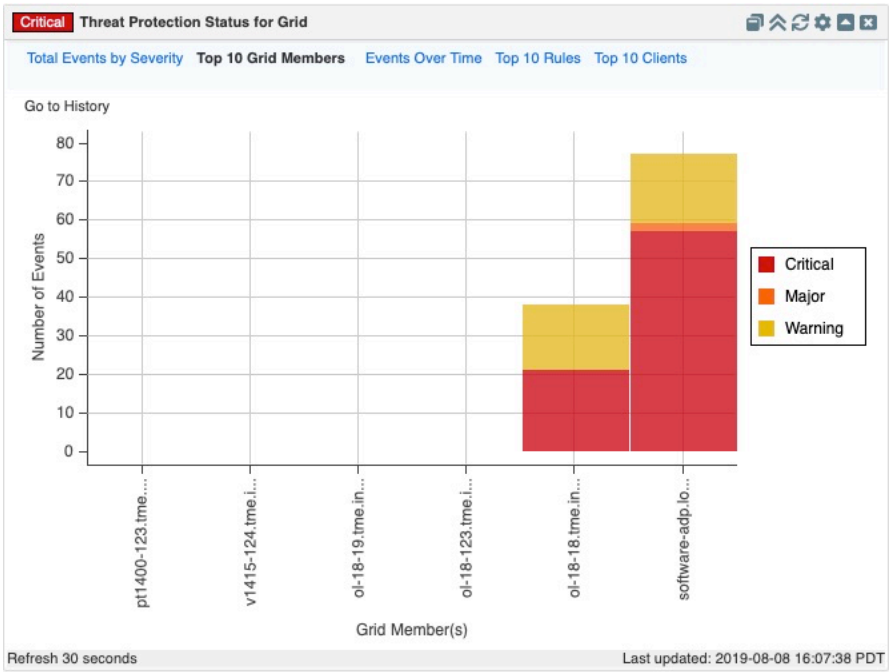
- Top 10 Rules hit.
- Top 10 attackers
- Number of events over time broken down to Critical, Major, Warning and Informational
- Top 10 Grid members reporting the events
- Total events by severity

The example screenshots are as follows:


Critical
Threat Protection Status for Grid
Total Events by Severity
Top 10 Grid Members
Events Over Time
Top 10 Rules
Top 10 Clients
Go to History
22.5
20
17.5
15
12.5
10
7.5
5
2.5
0
Number of Events
3:35:00 PM
3:40:00 PM
3:45:00 PM
3:50:00 PM
3:55:00 PM
4:05:00 PM
Time
Critical
Major
Warning
Informational
Refresh 30 seconds
Last updated: 2019-08-08 16:04:23 PDT

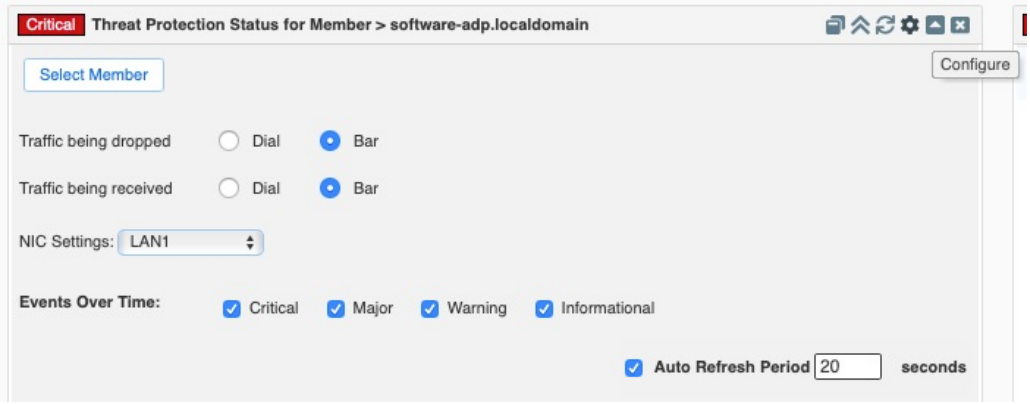

Critical
Threat Protection Status for Grid
Total Events by Severity
Top 10 Grid Members
Events Over Time
Top 10 Rules
Top 10 Clients
Go to History
10.61.19.13
10.61.21.13
10.61.21.53
Client(s)
0
10
20
30
40
50
60
70
80
Hits
Refresh 30 seconds
Last updated: 2019-08-08 16:05:28 PDT





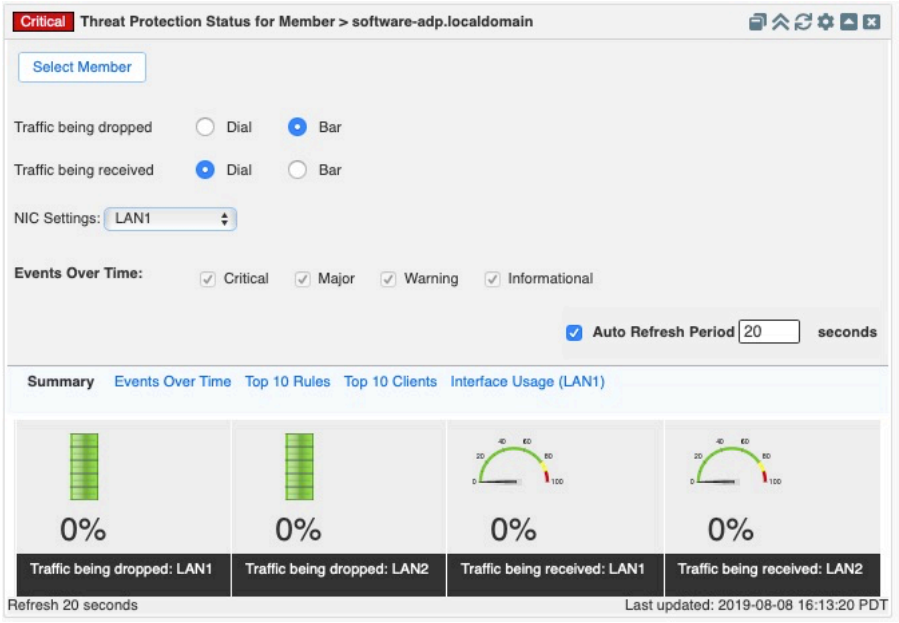
Threat Protection Status for Member

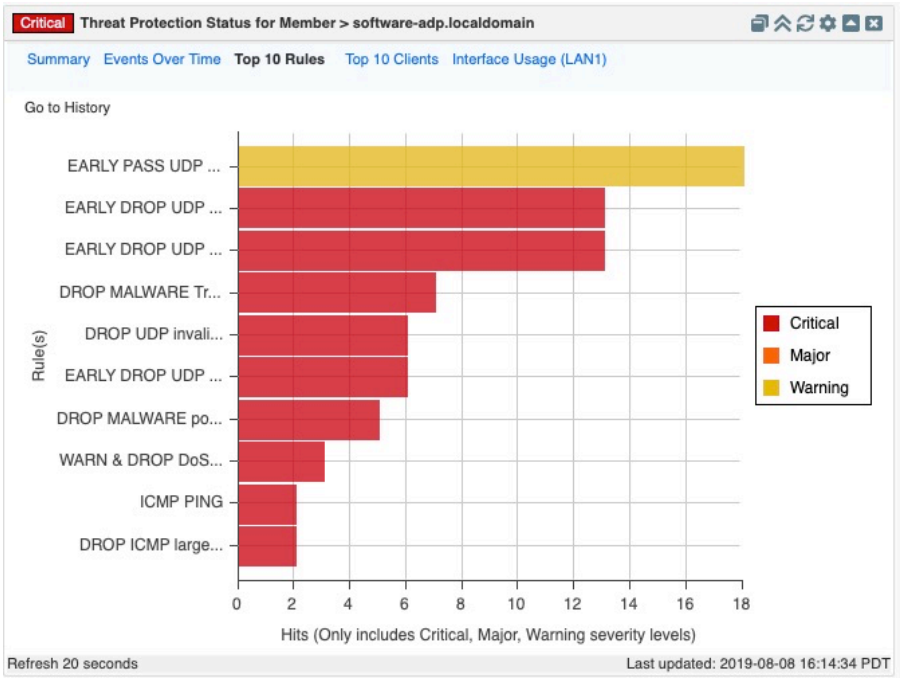
To view the Threat Protection Status for a particular member, go to the Widget **Threat Protection Status for Member.** You can select the Gear Icon, and edit the configuration, and select member.



Select the member for which you need status on.

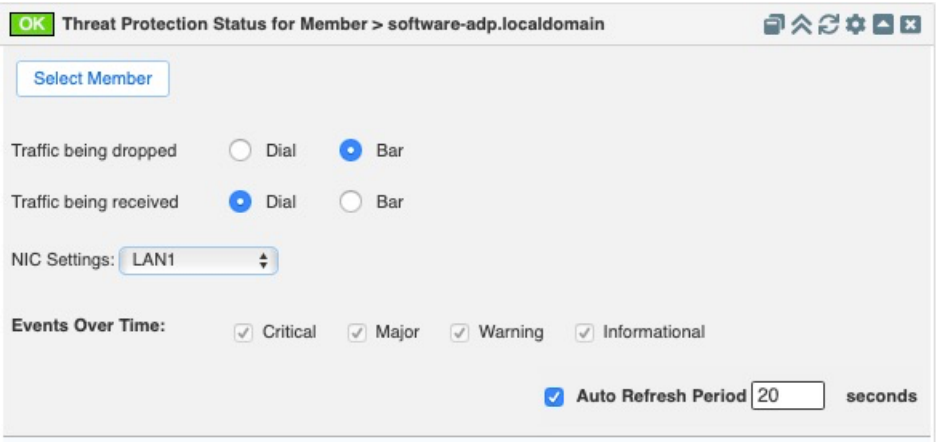
The widget now shows the percentage of traffic being received and dropped on LAN1 and LAN2 interfaces and interfaces usage. In addition, it also shows the Security events over time, top 10 rules being hit and the top 10 attackers handled by the appliance.





Auto Refresh

All widgets mentioned above support auto-refresh. Click the configure icon and select the **Auto Refresh Period** check box in the lower right corner. There you can specify the refresh period in seconds. The default auto refresh period is 30 seconds, the minimum is 5. Click the Configure icon again to hide the configuration panel.

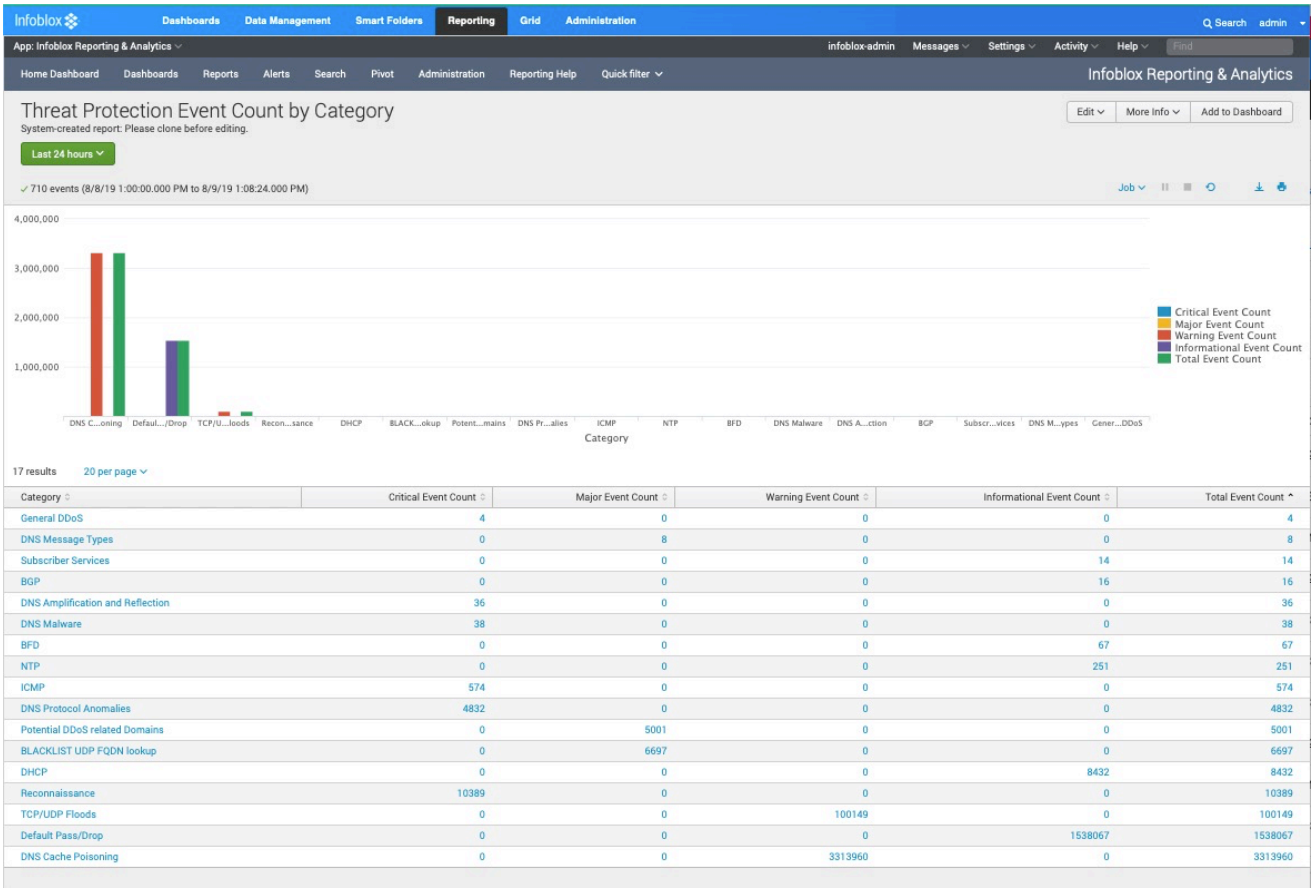


Viewing Reports

Various reports are available for Threat Protection service, examples below:

Threat Protection Event Count by Category

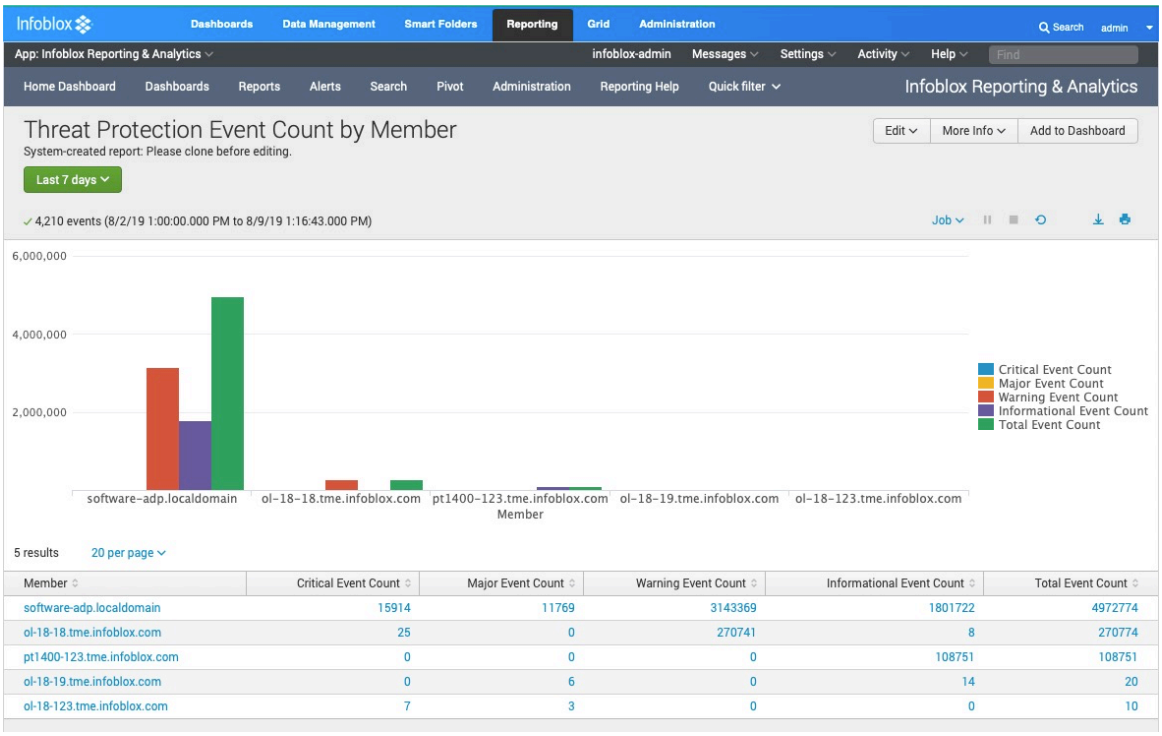
This report presents event counts based upon category for the selected time period.



Category	Critical Event Count	Major Event Count	Warning Event Count	Informational Event Count	Total Event Count
General DDoS	4	0	0	0	4
DNS Message Types	0	8	0	0	8
Subscriber Services	0	0	0	14	14
BGP	0	0	0	16	16
DNS Amplification and Reflection	36	0	0	0	36
DNS Malware	38	0	0	0	38
BFD	0	0	0	67	67
NTP	0	0	0	251	251
ICMP	574	0	0	0	574
DNS Protocol Anomalies	4832	0	0	0	4832
Potential DDoS related Domains	0	5001	0	0	5001
BLACKLIST UDP FQDN lookup	0	6697	0	0	6697
DHCP	0	0	0	8432	8432
Reconnaissance	10389	0	0	0	10389
TCP/UDP Floods	0	0	100149	0	100149
Default Pass/Drop	0	0	0	1538067	1538067
DNS Cache Poisoning	0	0	3313960	0	3313960

Threat Protection Event Count by Member

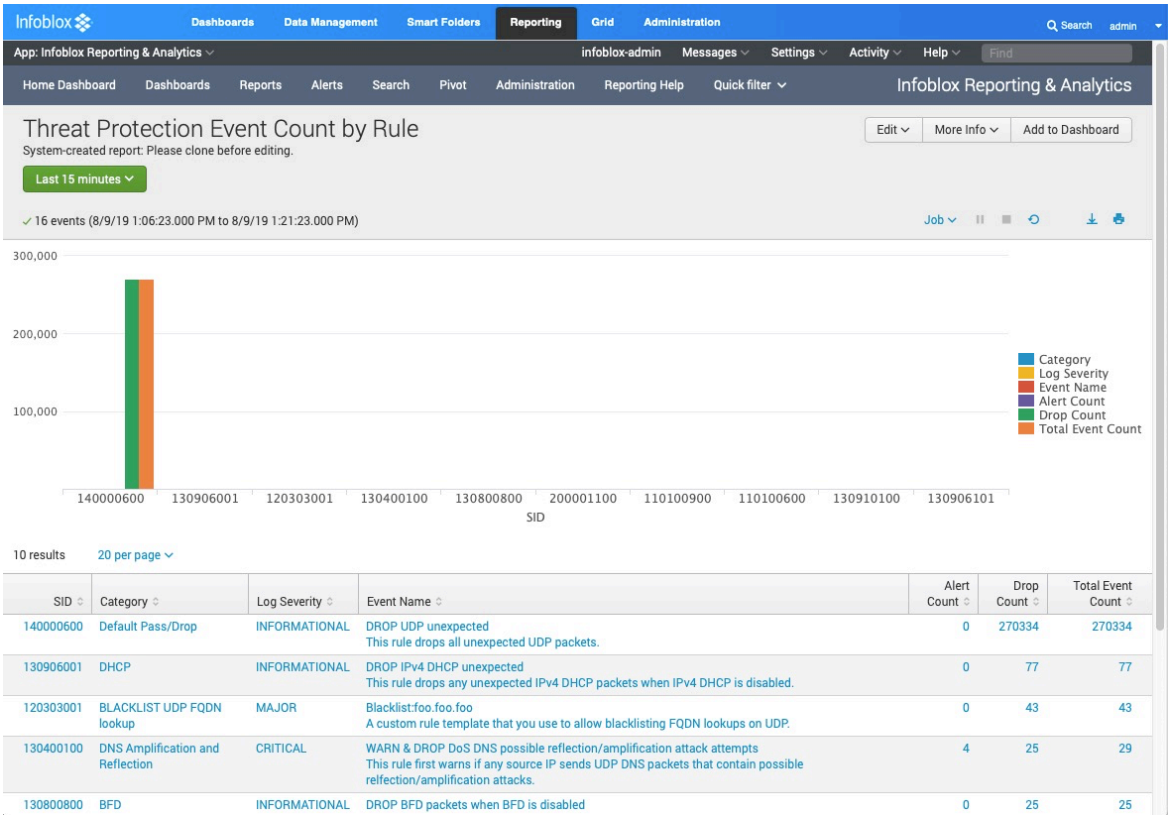
This report shows the event count by member based upon severity.



Member	Critical Event Count	Major Event Count	Warning Event Count	Informational Event Count	Total Event Count
software-adp.localdomain	15914	11769	3143369	1801722	4972774
ol-18-18.tme.infoblox.com	25	0	270741	8	270774
pt1400-123.tme.infoblox.com	0	0	0	108751	108751
ol-18-19.tme.infoblox.com	0	6	0	14	20
ol-18-123.tme.infoblox.com	7	3	0	0	10

Threat Protection Event Count by Rule

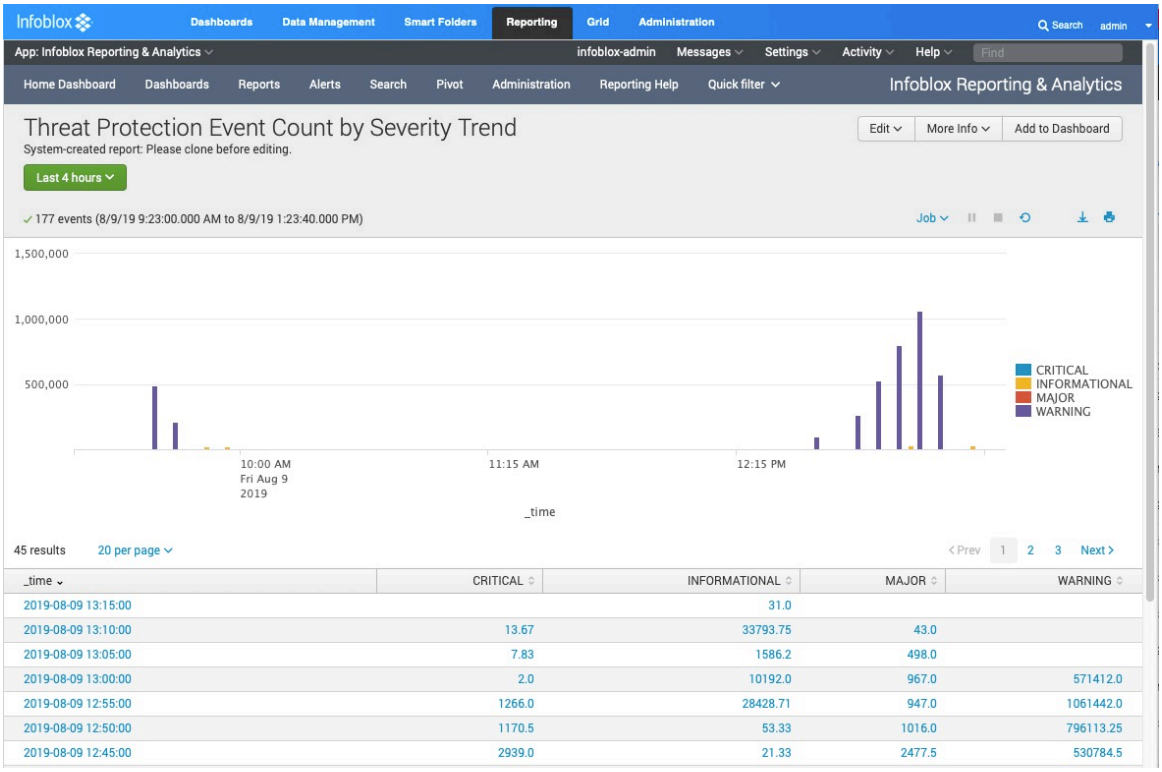
The report displays the event rule hits sorted by the total event count.



SID	Category	Log Severity	Event Name	Alert Count	Drop Count	Total Event Count
140000600	Default Pass/Drop	INFORMATIONAL	DROP UDP unexpected This rule drops all unexpected UDP packets.	0	270334	270334
130906001	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected This rule drops any unexpected IPv4 DHCP packets when IPv4 DHCP is disabled.	0	77	77
120303001	BLACKLIST UDP FQDN lookup	MAJOR	Blacklist:foo.foo.foo A custom rule template that you use to allow blacklisting FQDN lookups on UDP.	0	43	43
130400100	DNS Amplification and Reflection	CRITICAL	WARN & DROP DoS DNS possible reflection/amplification attack attempts This rule first warns if any source IP sends UDP DNS packets that contain possible reflection/amplification attacks.	4	25	29
130800800	BFD	INFORMATIONAL	DROP BFD packets when BFD is disabled	0	25	25

Threat Protection Event Count by Severity Trend

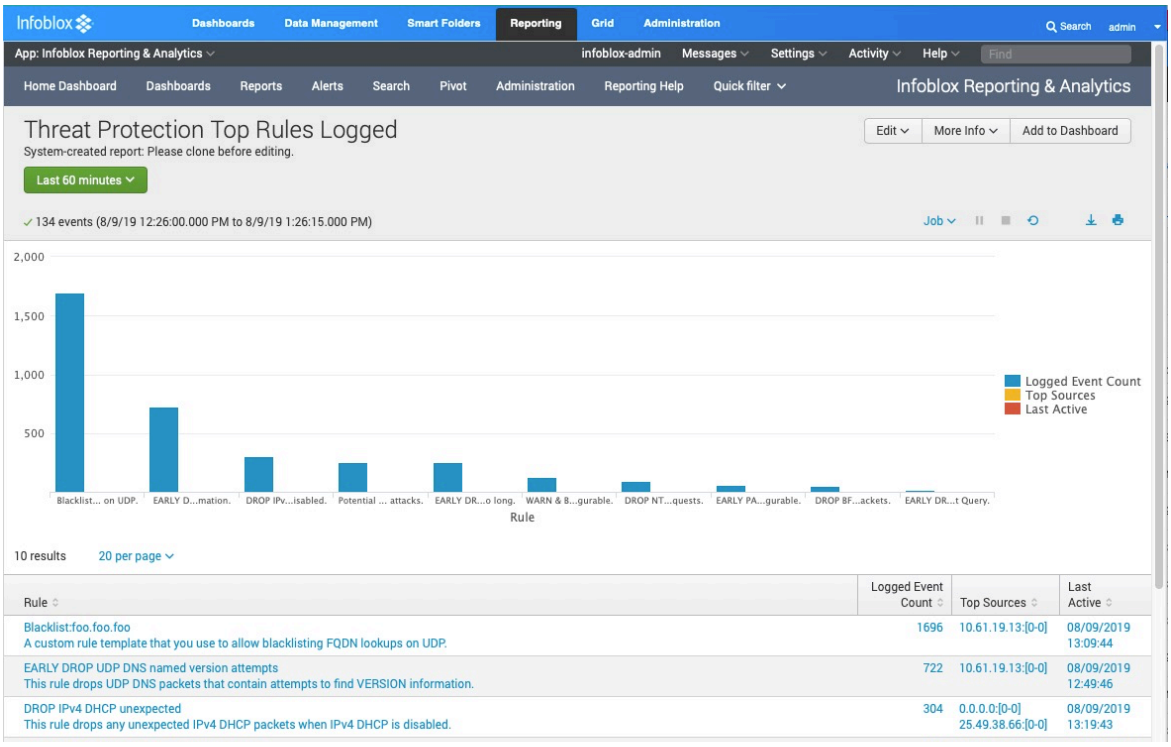
The report displays the number of threat protection events broken down by severity.



_time	CRITICAL	INFORMATIONAL	MAJOR	WARNING
2019-08-09 13:15:00		31.0		
2019-08-09 13:10:00	13.67	33793.75	43.0	
2019-08-09 13:05:00	7.83	1586.2	498.0	
2019-08-09 13:00:00	2.0	10192.0	967.0	571412.0
2019-08-09 12:55:00	1266.0	28428.71	947.0	1061442.0
2019-08-09 12:50:00	1170.5	53.33	1016.0	796113.25
2019-08-09 12:45:00	2939.0	21.33	2477.5	530784.5

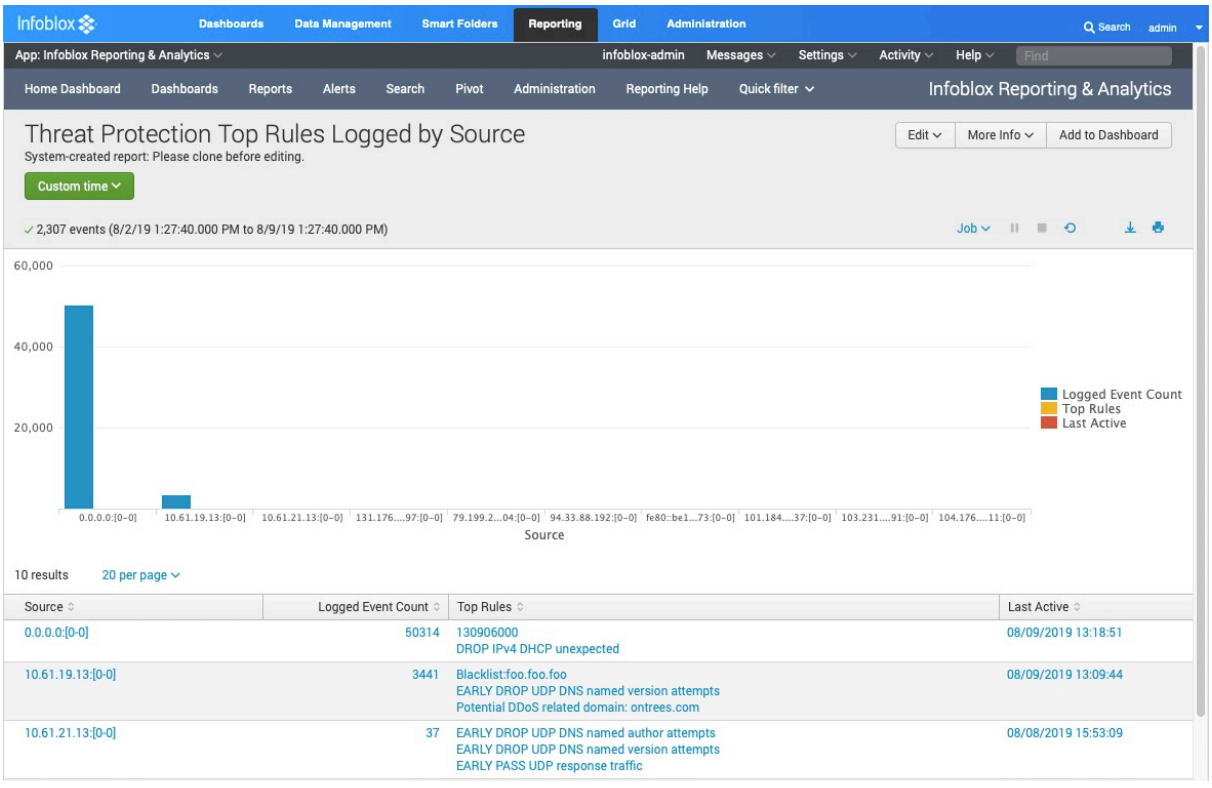
Threat Protection Top Rules Logged

The report is based on frequently hit rules and while displaying the top sources IP address.



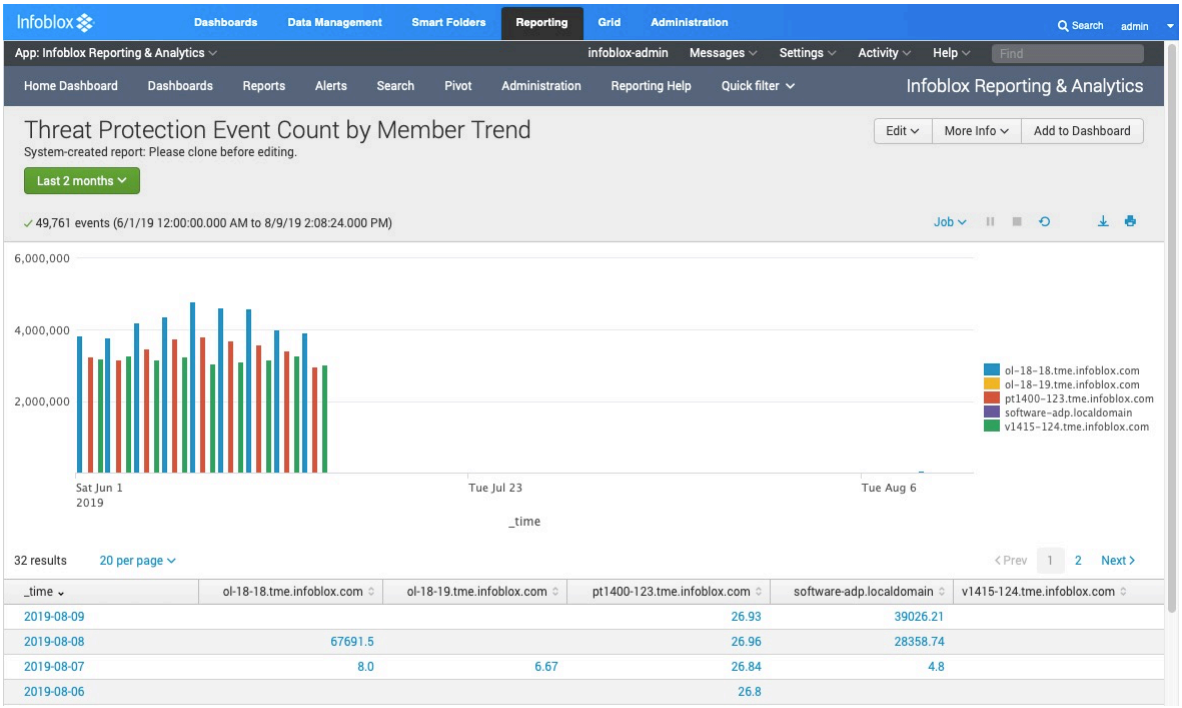
Threat Protection Top Rules Logged by Source

The source IP addresses with the highest logged event count are presented with the top rules that the address has hit.



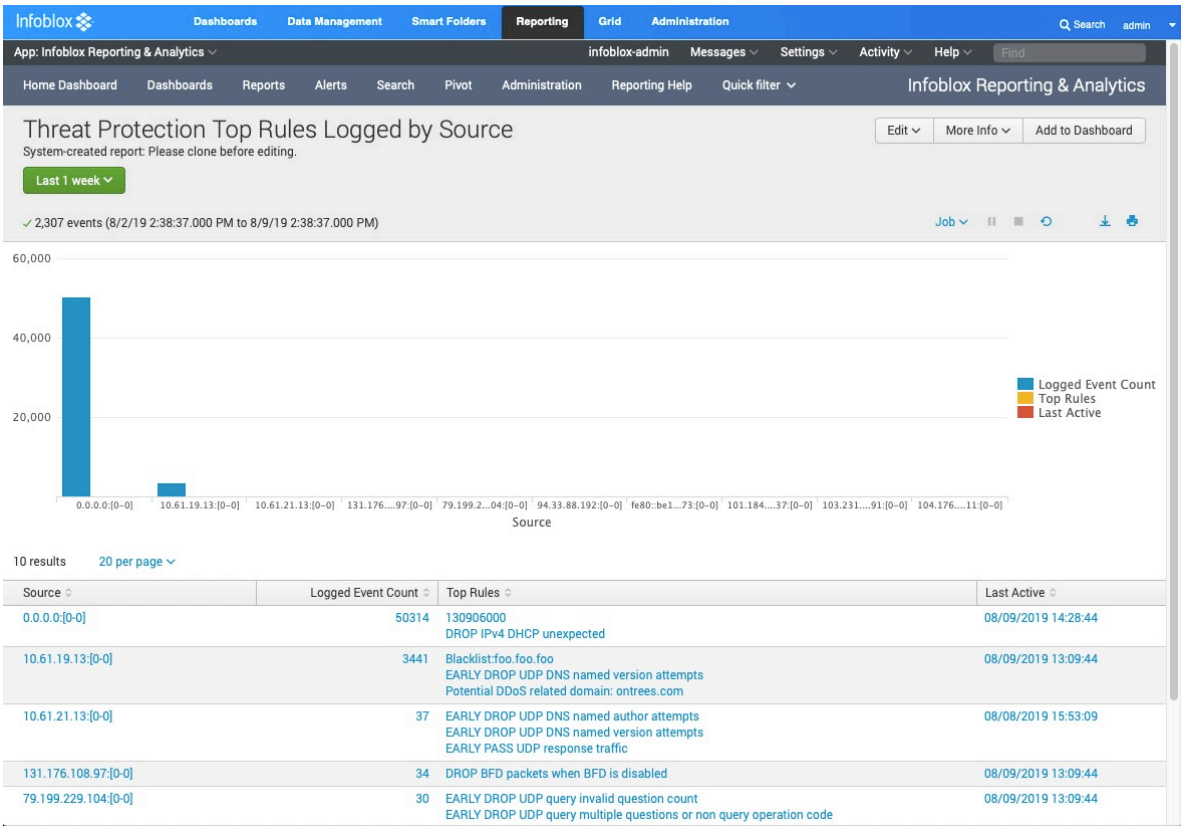
Threat Protection Event Count by Member Trend

This report displays number of threat protection events by each ADP member.



Threat Protection Top Rules Logged by Source

This shows the IP addresses that have the highest number of rule hits.



Logging

By default, when a DNS attack is detected against an enabled rule, the appliance generates a log message. These threat protection messages are displayed in CEF (Common Event Format).

The number of log messages generated is based on the 'Event per Second' setting in each rule. For example, if the setting is 5, the appliance generates maximum of five log messages of the same event per second per client when a rule is hit within the time duration. Following is a sample CEF log message for a ADP rule hit event,

2019-08-09 12:46:35 PDT daemon ERROR threat-protect-log[6524] CEF:0|Infoblox|NIOS Threat|8.4.4-386831|120601966|Potential DDoS related domain: ontrees.com|7|src=10.61.19.13 spt=51460 dst=10.61.19.55 dpt=53 act="DROP" cat="Potential DDoS related Domains" nat=0 nfpt=0 nlpt=0 fqdn=ontrees.com hit_count=4981

This log contains the following information:

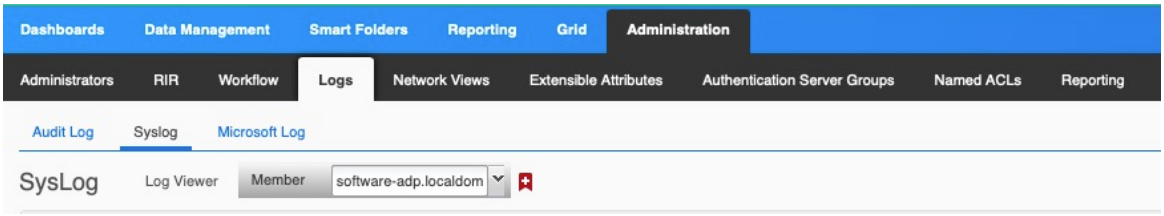
- The timestamp when the event happened in yyyy-mm-ddThh:mm:ss+00:00 format.
- Infoblox|NIOS Threat|x.x.x: Indicates the Infoblox product, and x.x.x represents the NIOS version.
- The number following the NIOS version is the rule ID. In this example, it is 120601966.
- Following the rule ID is the rule name specified in the rule. In this example it is “Potential DDoS related domain: ontrees.com”
- The number following the rule ID is the log severity. The following numbers indicate the severity levels:
    - 8 = Critical

    - 7 = Major
    - 6 = Warning
    - 4 = Informational
- src: Source IP address
- spt: Source port.
- dst: Destination IP address.
- dpt: Destination port.
- act: The rule action, which can be ALERT, DROP, or PASS, depending on the rule configuration.
- cat: The rule category to which the rule belongs. In this example, the rule category is “Potential DDoS related Domains
- nat: Indicates if the syslog event is logged for a NAT'ed client. In this example, nat=0 means that it's not a NAT’ed client.
- nfpt: Indicates the first port in the port block if syslog is for NAT’ed client.
- nlpt: Indicates the last port in the port block if syslog is for NAT’ed client.
- fqdn: Indicates the FQDN that was queried by the client
- hit_count: Indicates the number of rule hits

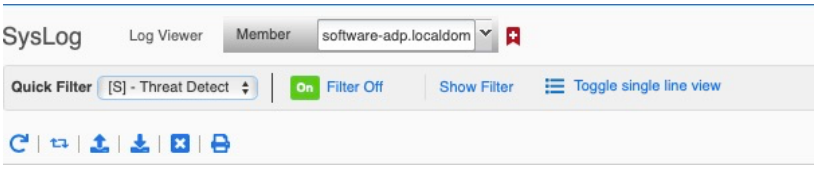
The logs for Infoblox Advanced DNS Protection appliance can be viewed by going to;

Administration > **Logs** > **Syslog**

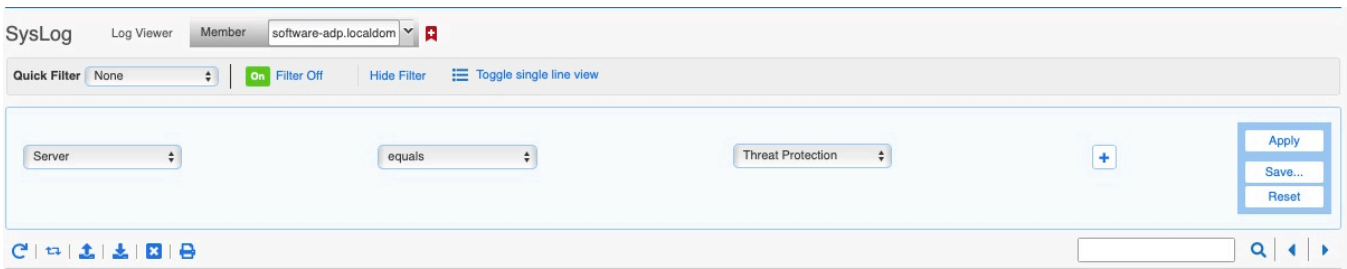
Select the appropriate member from the **Member** drop down menu.



To view Threat Protection logs, click on **Show filter**

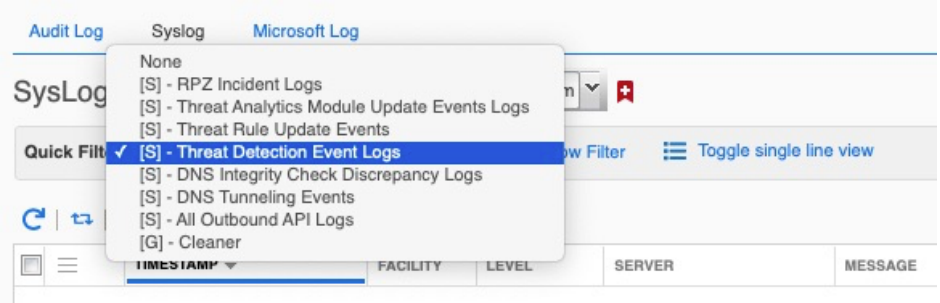


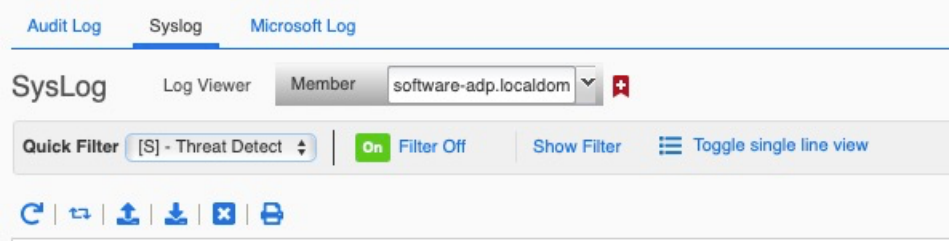
Select the values of the filter fields as “**Server equals Threat Protection**” shown in the screenshot below,



To only view CEF messages logged for Threat Protection Rules hit,

select **Threat Detection Event Logs** from Quick Filter drop down menu, after selecting the appropriate member in Syslog,





Click **Apply**

The filters can be used to view different levels of log messages, such as CRITICAL, ALERT, INFO etc.

The critical messages can be viewed by setting the filter settings as shown in the screenshot below,

A DNS amplification attack is a reflection-based distributed denial of service (DDoS) attack.

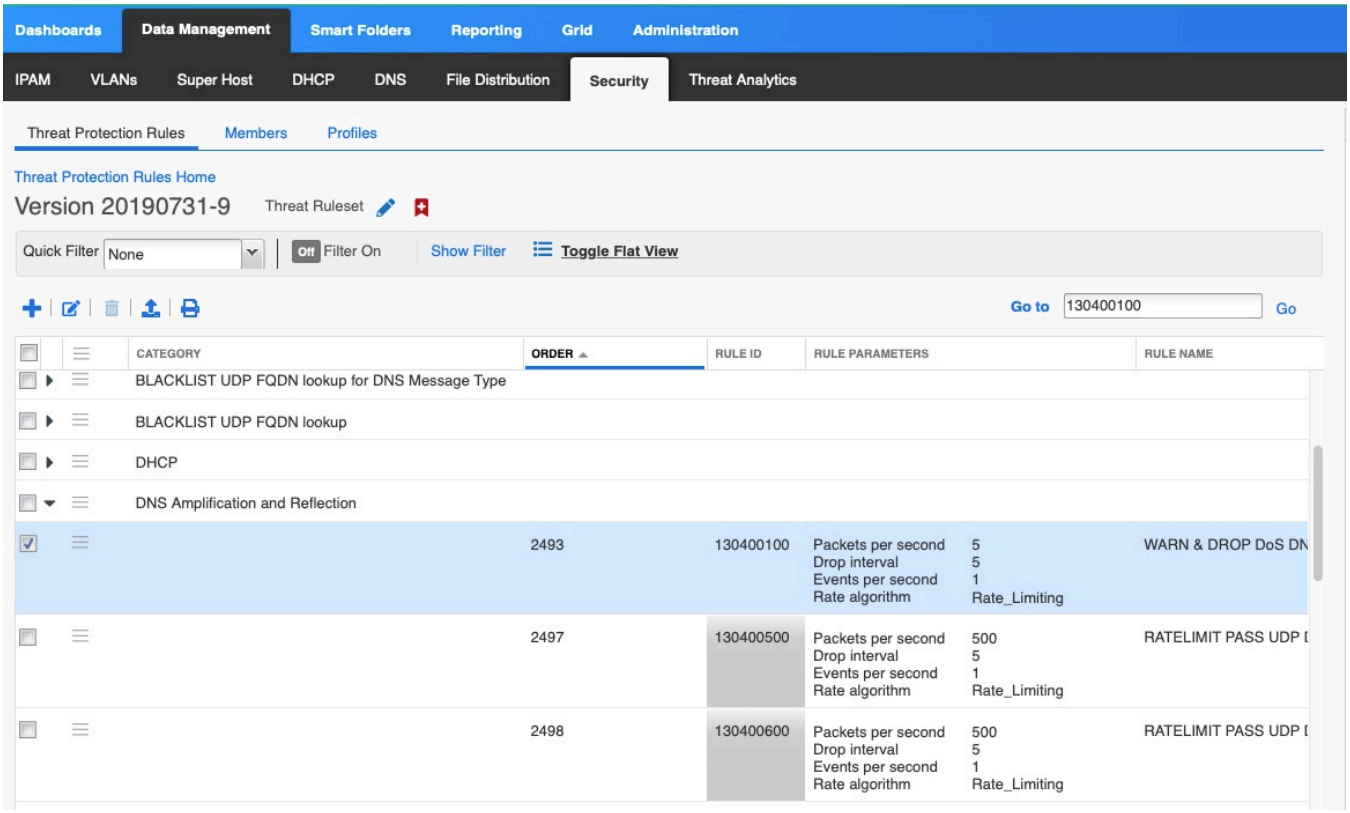
The attacker spoofs client requests to DNS servers to hide the true source of the attacker and direct the response to the client. Using various techniques, small DNS queries may be turned into a much larger payload directed at the target network. The following log message has rule id of 130400100. This rule first warns if any source IP sends UDP DNS packets that contain possible reflection/amplification attacks.

2019-08-09 15:05:45 PDT	daemon	CRITICAL	threat-protect-log[6524]	CEF:0|Infoblox|NIOS Threat|8.4.4-386831|130400100|WARN & DROP DoS DNS possible reflection/amplification attack attempts|8|src=10.61.19.13 spt=33921 dst=10.61.19.55 dpt=53 act="DROP" cat="DNS Amplification and Reflection" nat=0 nfpt=0 nlpt=0 fqdn=www.whitehouse.gov hit_count=33

In order to view the rule that is being hit to generate the above log message,

Go to **Data Management** > **Security** > **Threat Protection Rules**

Click on the Active ruleset for the Grid and in **Go to** field type the rule id **130400100**. Click **Go**



The following log message is generated when ADP receives large ICMP ping packet.

2019-08-09 09:39:00 PDT	daemon	CRITICAL	threat-protect-log[9682]	CEF:0|Infoblox|NIOS Threat|8.4.0-381062|130400200|DROP ICMP large packets|8|src=10.61.19.13 spt=8 dst=10.61.19.55 dpt=0 act="DROP" cat="ICMP" nat=0 nfpt=0 nlpt=0 fqdn=(null) hit_count=3

The following log message is generated when ADP receive drops request to a malicious domain.

2019-08-09 09:38:24 PDT	daemon	CRITICAL	threat-protect-log[9682]	CEF:0|Infoblox|NIOS Threat|8.4.0-381062|130300400|DROP MALWARE possible Hilotil|8|src=10.61.19.13 spt=60334 dst=10.61.19.55 dpt=53 act="DROP" cat="DNS Malware" nat=0 nfpt=0 nlpt=0 fqdn=9charname.cmd_exe hit_count=6

Troubleshooting & FAQ

Some common issues and their resolution are discussed in this section.

Unable to download Threat Protection Rules

You may encounter a situation where the ADP appliance is not able to download threat protection rules from ts.infoblox.com. The troubleshooting steps are as follows,

- Make sure the Grid can resolve the hostname ts.infoblox.com.
    - A Resolver must be configured for the Grid so that any member involved can resolve the hostname. (Please see **Enabling DNS resolver** section)
- Make sure the Grid can reach the server ts.infoblox.com.
    - Check to see if any firewall rule is blocking the path to https.
    - Check the proxy setting if applicable.

Trouble joining the Grid

If you are having trouble joining a member to the Grid, here are things to look at;

- Member type (Make sure the right member type is selected)
    - Infoblox - for physical PT Appliances, and TE Appliances for Software ADP.
    - Virtual NIOS - for Virtual TE-Appliances for Software ADP.
- **Enable VPN on MGMT Port** has been checked in **Grid Member Properties Editor** > **Network** > **Advanced**
- Make sure the member can ping the Grid Master and verify the firewall is not restricting any access. For reference, check the NIOS Administration Guide.
- Make sure that you have enable MGMT on the member to join and that MGMT IPs match on member local configuration & grid provisioned member configuration.

Different rulesets for different ADP appliances

Question

How can I create two rulesets in ADP? one for external ADP appliances and the other for internal ADP appliances? Both sets need to be tuned differently so I need to apply different tuning to different appliances.

Answer

Best practice is to use ADP Profiles.

Trouble Starting Threat Protection Service

- The Member cannot be a Grid-Master unless it is a Grid of one.
- The Threat Protection Service may not start.

Understanding a CEF Log message

Please see **Logging** section in this deployment guide to be able to read the contents of a CEF log message.

Outbound API

The Infoblox Outbound API can send outbound notifications to Syslog, DXL (Data Exchange Layer), and REST API endpoints. The ADP *event_type* can trigger on events like: Hits Count, Member IP, Member Name, Query FQDN, Rule Action, Rule Category, Rule Severity, SID, and Source IP. This will notify any solution that will accept indicators that can be acted upon.

These notifications can do a myriad number of things, like triggering client remediation with endpoint security solutions, integration with SOAR solutions, create SOC events, trigger DDoS mitigations, and even opening Service Now tickets. These notifications are vendor neutral.

To use the Outbound API, a Security Ecosystem License is required

Please defer to the NIOS 8.4 Documentation for details on the Infoblox Outbound API. At https://docs.infoblox.com, search for “Outbound Notification Overview”

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