Log Ingestion - Splunk Stream (DNS, DHCP)

Overview

https://www.splunk.com/pdfs/product-briefs/splunk-stream.pdf

https://docs.splunk.com/Documentation/StreamApp/8.1.1/DeployStreamApp/AboutSplunkStream

Purpose

Having customers complain about having to turn on DNS debug logging on their DCs? Similarly for DHCP? Fear not! Splunk Stream can accomplish the same result of ingesting DNS and DHCP (among many other protocols) **directly off the wire**, and ingest the events to Splunk! Splunk Stream contains pre-packaged NPCAP drivers (think of it as a behind the scenes `tcpdump`) for Windows, Linux, and Mac operating systems that are installed on target hosts and begin immediately capturing and ingesting data.

Pre-Requisites

- The KV Store **must** be enabled on the instance where Splunk App for Stream is installed for **active** Stream forwarder management (typically on the deployment server).

Installation/Configuration Procedure

Search Head

- Install Splunk App for Stream

> ℹ Splunk App for Stream is only used for the provided dashboards. Splunk documentation states to leverage Splunk Stream on the search head to manage stream forwarder configurations, however that would require customer hosts with stream configurations applied to phone home over TCP 8000 to the search head. Our current stance is to reduce public Internet traffic as much as possible; thus, `Splunk App for Stream` is installed on the nearest on-premise heavy forwarder for stream forwarder configuration. No stream forwarder configuration is performed on the search head, and can be safely ignored.

- Install Splunk Add-on for Stream Wire Data

Customer On-Prem HF

Base Installation/Configuration

This installation scenario implies that the On-Prem HF **is also** acting as a deployment server for universal forwarders.

If the Deployment server is separate from the heavy forwarder(s), install and configure Splunk App for Stream and Splunk Add-on for Stream Forwarders on the deployment server, and subsequently, install Splunk Add-on for Stream Wire Data on the heavy forwarder(s) that will be receiving traffic/events from the Universal Forwarder/Stream Forwarder.

- Install Splunk App for Stream

Splunk Web will prompt for a restart. Wait until all three apps are installed before restarting.

- Create indexes.conf within `$SPLUNK_HOME/etc/apps/splunk_app_stream/local` and specify the index for which the customer wishes to ingest, which maps to our Deepwatch Standard: Splunk Index Naming Convention. This will allow the selection of the appropriate index within Splunk Web for indexing data. No data will actually be indexed on the Heavy Forwarder.
  - Example indexes.conf entry for DNS data

```
[dns]
coldPath = $SPLUNK_DB/$_index_name/colddb
homePath = $SPLUNK_DB/$_index_name/db
thawedPath = $SPLUNK_DB/$_index_name/thaweddb
```

- Install Splunk Add-on for Stream Wire Data
- Install Splunk Add-on for Stream Forwarders

Splunk App for Stream **MUST** be installed prior to the installation of Splunk Add-on for Stream Forwarders. As long as the instructions are followed from top to bottom, this won't be an issue. Otherwise, Splunk will **NOT** create the necessary `inputs.conf` and `keystore.db` in `$SPLUNK_HOME/etc/apps/Splunk_TA_stream/local`

- Restart Splunkd on the HF

After the restart, Splunk will create an inputs.conf, keystore.db, and streamfwdlog.conf in `$SPLUNK_HOME/etc/apps/Splunk_TA_stream/local`

Deploy `Splunk_TA_Stream` to Forwarders

- **Move** (not copy) Splunk Add-on for Stream Forwarders (Splunk_TA_stream) to $SPLUNK_HOME/etc/deployment-apps. `Splunk_TA_stream` should **not** reside in $SPLUNK_HOME/etc/apps on the HF
- Change permissions of set_permissions.sh

```
cd $SPLUNK_HOME/etc/deployment-apps/Splunk_TA_stream
chmod +x ./set_permissions.sh
```

Do not execute the script. It is meant to be executed by the downstream UF that receives `Splunk_TA_stream`. Doing so will cause the TA to disappear from the Splunk Web Forwarder Management UI

- Configure ***$SPLUNK_HOME/etc/deployment-apps/Splunk_TA_stream/local/inputs.conf*** as follows (file should already exist):

```
[streamfwd://streamfwd]
splunk_stream_app_location = https://<ip> of HF>:8000/en-us/custom/splunk_app_stream/
stream_forwarder_id =
disabled = 0
```

Verify firewalld is configured to have port 8000/tcp open, and the downstream UF's have the capability to reach the HF over port 8000 (in addition to 9997 and 8089). Customer may have to add/modify a FW rule to allow this traffic (in addition to TCP 9997 and TCP 8089).

- On the deployment server, configure Forwarder Management to push Splunk_TA_stream to the desired hosts
  - Serverclass Name: `uf_stream`
  - Included apps: `Splunk_TA_Stream`

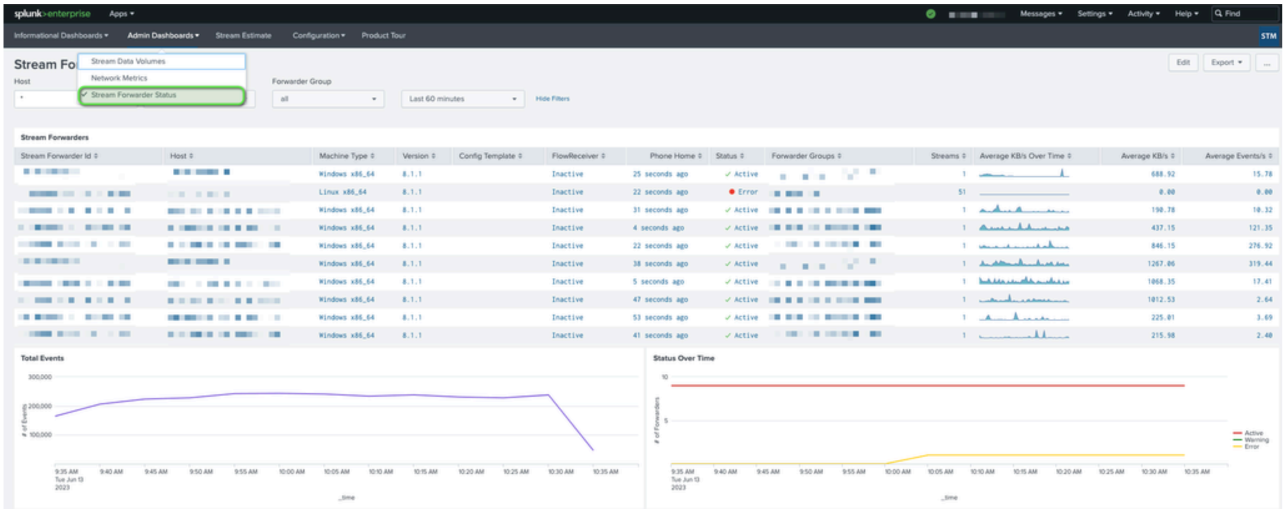
Ensure the app is configured to restart Splunkd on the UF, in addition to being enabled.

Splunk Stream dashboards and metrics WILL NOT POPULATE on the HF. The dashboards and metrics are populated by indexed data (which the HF cannot search). This is to avoid sending Splunk Stream management traffic across public address space to the search head (either Splunk Cloud or dwCloud).

- **From the search head** Access `splunk_app_stream`, and navigate to `Admin Dashboards` → `Stream Forwarder Status`. Information pertaining to the Stream forwarders you have pushed to UFs will begin to populate here. If the status of the Stream Forwarder is **NOT** active, run the following search to identify any issues:

```
index=_internal host IN (<uf1,uf2,etc>) sourcetype=stream*
```

The most common issue is the inability for the Stream Forwarder to communicate with the Stream Manager (HF) over port 8000.

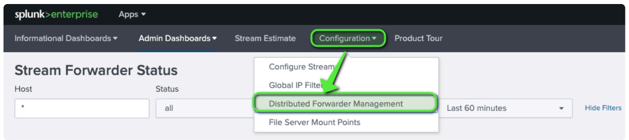


Stream Forwarders

Stream Forwarder Id	Host	Machine Type	Version	Config Template	FlowReceiver	Phone Home	Status	Forwarder Groups	Streams	Average KB/s Over Time	Average KB/s	Average Events/s
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	25 seconds ago	✓ Active	[redacted]	1		688.92	15.78
[redacted]	[redacted]	Linux x86_64	8.1.1		Inactive	22 seconds ago	● Error	[redacted]	51		0.00	0.00
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	31 seconds ago	✓ Active	[redacted]	1		190.78	10.32
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	4 seconds ago	✓ Active	[redacted]	1		437.15	121.35
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	22 seconds ago	✓ Active	[redacted]	1		846.15	276.92
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	38 seconds ago	✓ Active	[redacted]	1		1267.06	319.44
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	5 seconds ago	✓ Active	[redacted]	1		1068.35	17.41
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	47 seconds ago	✓ Active	[redacted]	1		1012.53	2.64
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	53 seconds ago	✓ Active	[redacted]	1		225.01	3.69
[redacted]	[redacted]	Windows x86_64	8.1.1		Inactive	41 seconds ago	✓ Active	[redacted]	1		215.98	2.40

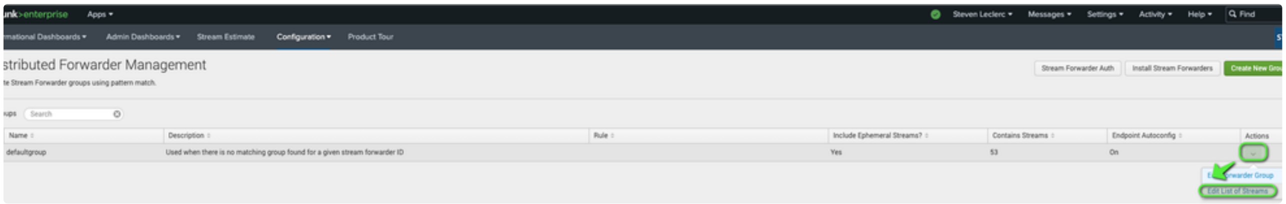
Distributed Forwarder Management Configuration

- On the DS, go to `splunk_app_stream` and navigate to `Configuration` → `Distributed Forwarder Management`



Distributed Forwarder Management

- Select the dropdown associated with `defaultgroup`, and select `Edit List of Streams`

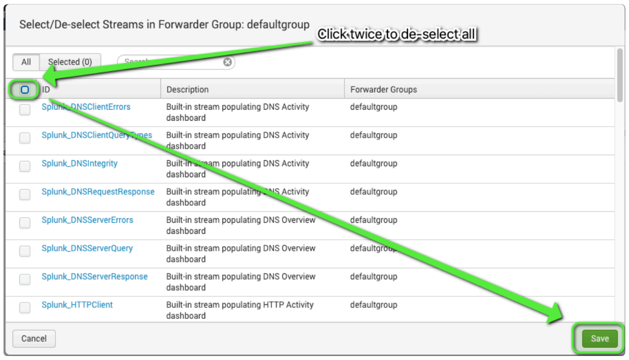


stributed Forwarder Management

te Stream Forwarder groups using pattern match.

Name	Description	Rule	Include Ephemeral Streams?	Contains Streams	Endpoint Autoconfig	Actions
defaultgroup	Used when there is no matching group found for a given stream forwarder ID		Yes	53	On	

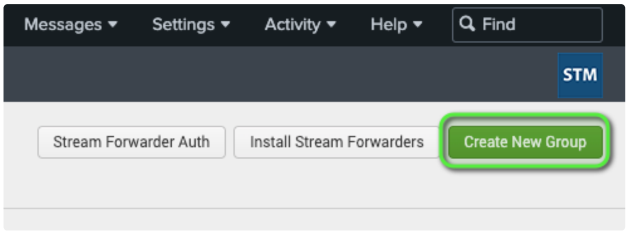
- Select the “global” selection checkbox twice, effectively disabling all streams associated with the `defaultgroup` Stream Forwarder group, and hit save



Select/De-select Streams in Forwarder Group: defaultgroup

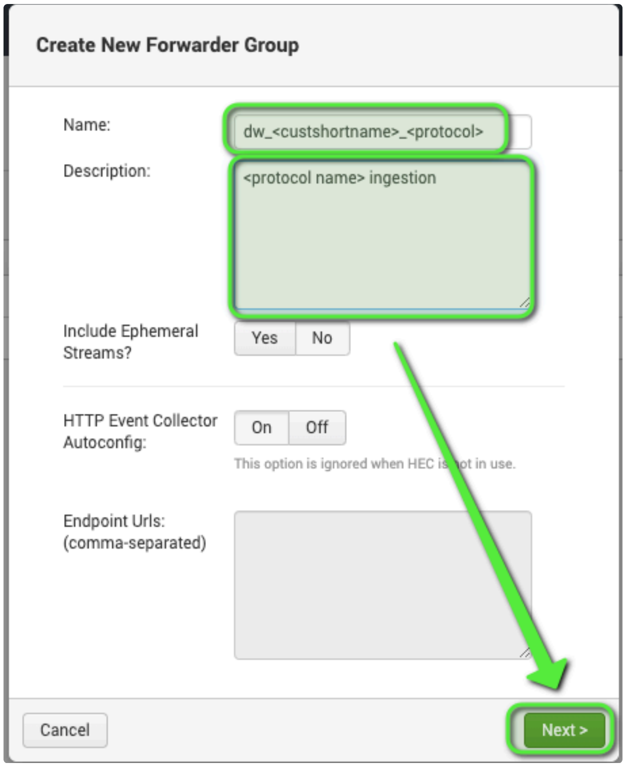
□	ID	Description	Forwarder Groups
□	Splunk_DNSClientErrors	Built-in stream populating DNS Activity dashboard	defaultgroup
□	Splunk_DNSClientQueryTypes	Built-in stream populating DNS Activity dashboard	defaultgroup
□	Splunk_DNSIntegrity	Built-in stream populating DNS Activity dashboard	defaultgroup
□	Splunk_DNSRequestResponse	Built-in stream populating DNS Activity dashboard	defaultgroup
□	Splunk_DNSServerErrors	Built-in stream populating DNS Overview dashboard	defaultgroup
□	Splunk_DNSServerQuery	Built-in stream populating DNS Overview dashboard	defaultgroup
□	Splunk_DNSServerResponse	Built-in stream populating DNS Overview dashboard	defaultgroup
□	Splunk_HTTPClient	Built-in stream populating HTTP Activity dashboard	defaultgroup

- Create a new Stream Forwarder group



- Follow the naming syntax to create a new Stream Forwarder group.

> ℹ If multiple protocols are required, create unique Stream Forwarder groups for each protocol.



Create New Forwarder Group

Name: dw_<custshortname>_<protocol>

Description: <protocol name> ingestion

Include Ephemeral Streams? Yes No

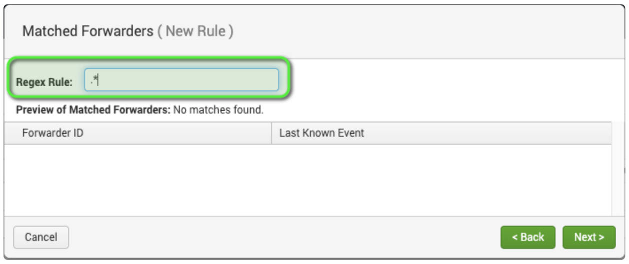
HTTP Event Collector Autoconfig: On Off

This option is ignored when HEC is not in use.

Endpoint Urls: (comma-separated)

- Create a regex rule to match the intended Stream Forwarders that were installed on the target UFs

Depending on the complexity of the intended targets, `.*` may not be acceptable for your use-case. If a more finite rule is required (e.g. to ingest DHCP events from a separate set of hosts compared to DNS events), run through the same procedure on the search head as a test bed. the `Matched Forwarders` section will populate on the search head, but **NOT** on the HF. From the search head, you can test/validate your regex rule matches the intended instances.



Matched Forwarders (New Rule)

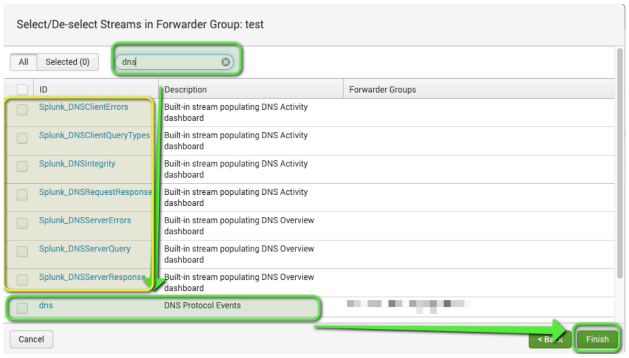
Regex Rule: .*

Preview of Matched Forwarders: No matches found.

Forwarder ID	Last Known Event

- Search for the protocol streams you wish to ingest, select the check box corresponding to each stream, and select next.

If Deepwatch and/or the Customer is interested in tuning opportunities, or is otherwise interested in the pre-built DNS activity dashboards provided by the `splunk_app_stream`, enable all of the corresponding `Splunk_DNS*` streams (highlighted in yellow). These dashboards provide an excellent way to identify said tuning opportunities.

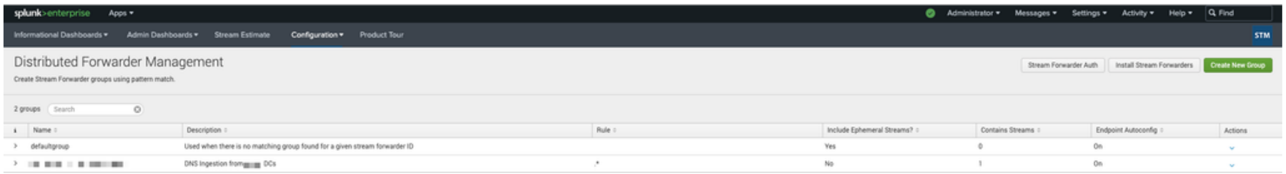


Select/De-select Streams in Forwarder Group: test

dns

□	ID	Description	Forwarder Groups
□	Splunk_DNSClientErrors	Built-in stream populating DNS Activity dashboard	
□	Splunk_DNSClientQueryTypes	Built-in stream populating DNS Activity dashboard	
□	Splunk_DNSIntegrity	Built-in stream populating DNS Activity dashboard	
□	Splunk_DNSRequestResponse	Built-in stream populating DNS Activity dashboard	
□	Splunk_DNSServerErrors	Built-in stream populating DNS Overview dashboard	
□	Splunk_DNSServerQuery	Built-in stream populating DNS Overview dashboard	
□	Splunk_DNSServerResponse	Built-in stream populating DNS Overview dashboard	
□	dns	DNS Protocol Events	[redacted]

- Your end result should look something similar to this



Distributed Forwarder Management

Create Stream Forwarder groups using pattern match.

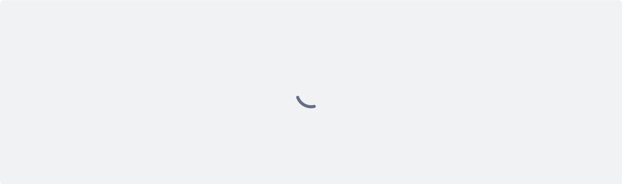
2 groups

Name	Description	Rule	Include Ephemeral Streams?	Contains Streams	Endpoint Autoconfig	Actions
defaultgroup	Used when there is no matching group found for a given stream forwarder ID		Yes	0	On	⌄
[redacted]	DNS Ingestion from [redacted] DCs	.*	No	1	On	⌄

End Result

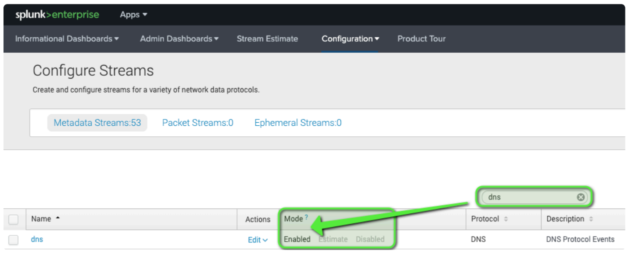
Configure Streams

- Also on the DS, Navigate to `Configuration` → `Configure Streams`



Configure Streams

- Edit the stream to modify the index destination by going into the Stream App and setting it in the UI.

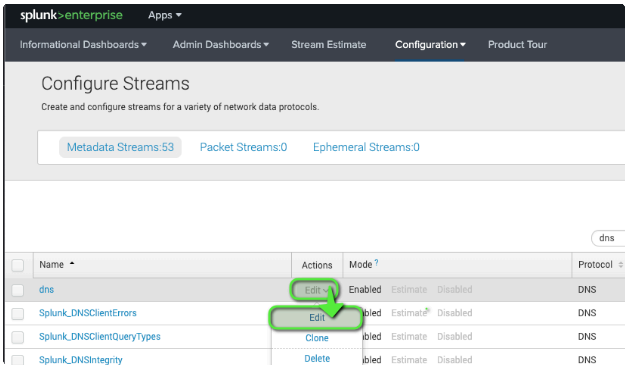


Configure Streams

Create and configure streams for a variety of network data protocols.

Name	Actions	Mode	Protocol	Description
dns	Edit ⌄	Enabled Estimate Disabled	DNS	DNS Protocol Events

- The index can be updated for each stream under Configuration → Configure Streams, clicking on the stream in question (I.E., “dns”) and updating the “index” field.



Configure Streams

Create and configure streams for a variety of network data protocols.

Name	Actions	Mode	Protocol
dns	Edit ⌄	Enabled Estimate Disabled	DNS
Splunk_DNSClientErrors		bled Estimate Disabled	DNS
Splunk_DNSClientQueryTypes		bled Estimate Disabled	DNS
Splunk_DNSIntegrity		bled Estimate Disabled	DNS

Fields Configuration

- Update the enabled fields to ensure only the necessary fields are selected. Refer to the following Confluence pages for more information on which fields to select
  - Splunk Stream: DNS Recommended Fields
  - Splunk Stream: DHCP Recommended Fields

Deepwatch currently does NOT have a “set” list of exact fields to select. As described in the above mentioned links, there are `must have`s, `nice to have`s, etc. It depends on how much the customer is concerned with their license usage (more fields, more license usage).