# ITSI Service Tree Automation

Hands-on Splunk ITSI Workshop


splunk>

# Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.



splunk>

# Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?


# Workshop Agenda

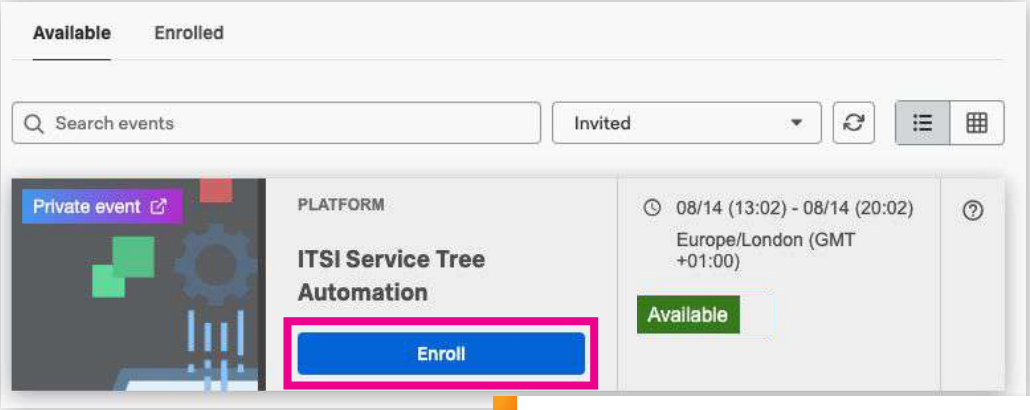
- Bulk import 500 entities
- Build a magic table
- Create 90 ITSI services at a time
- Check the result and discuss

# Enroll in Today's Workshop

## Tasks

1. Get a splunk.com account if you don't have one yet: https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event: https://show.splunk.com/event/<eventID>
3. Download a copy of today's slide deck: https://splk.it/ITSI-Automation-Attendee

## Goal

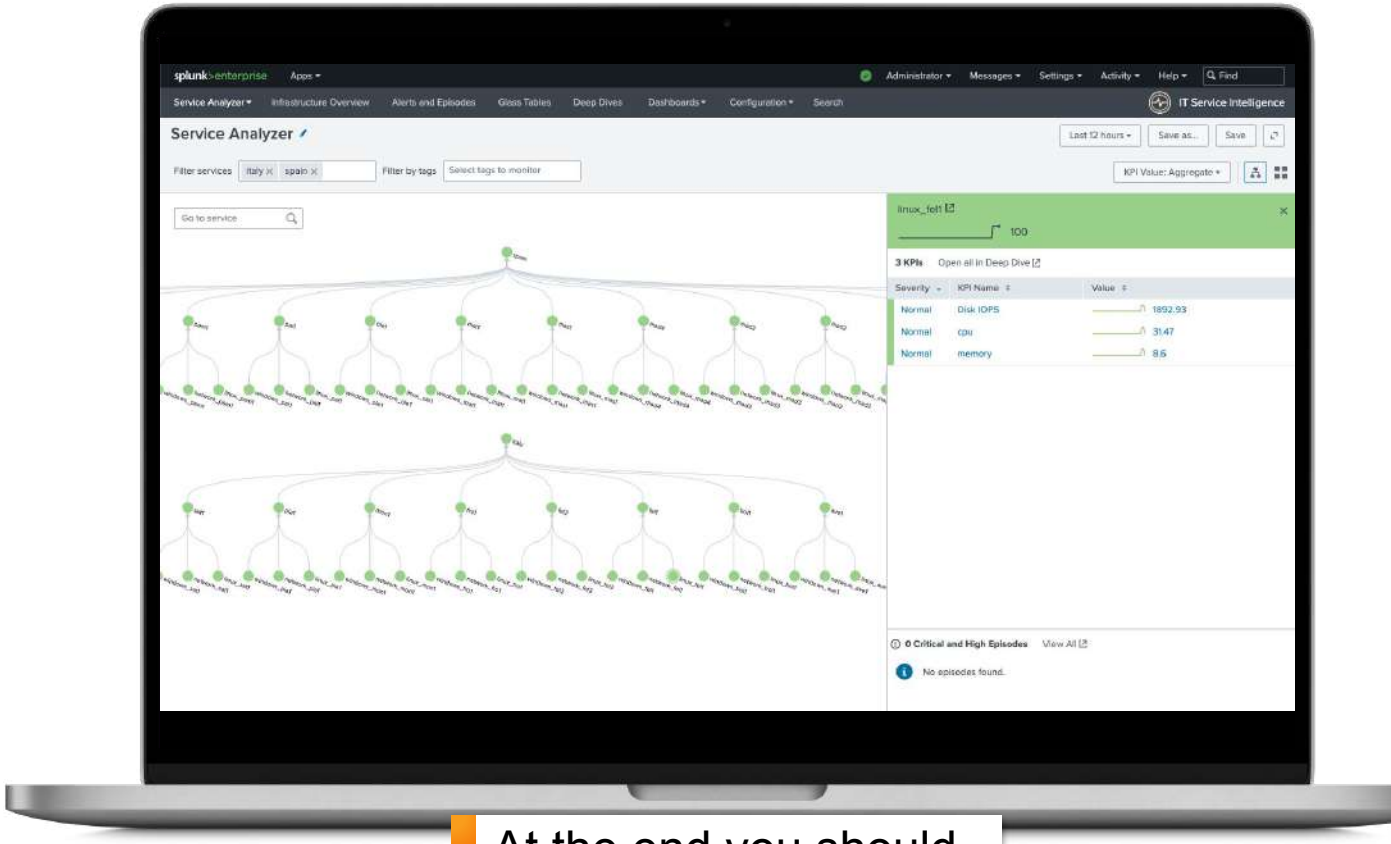



Enroll in today's event

# Objective for Today

Demonstrate advanced ITSI concepts to:

- ✓ Build a complex service tree from a single Splunk search
- ✓ Drastically reduce manual actions and limit build time
- ✓ Dynamically add and classify ITSI assets into a service tree




At the end you should have this!

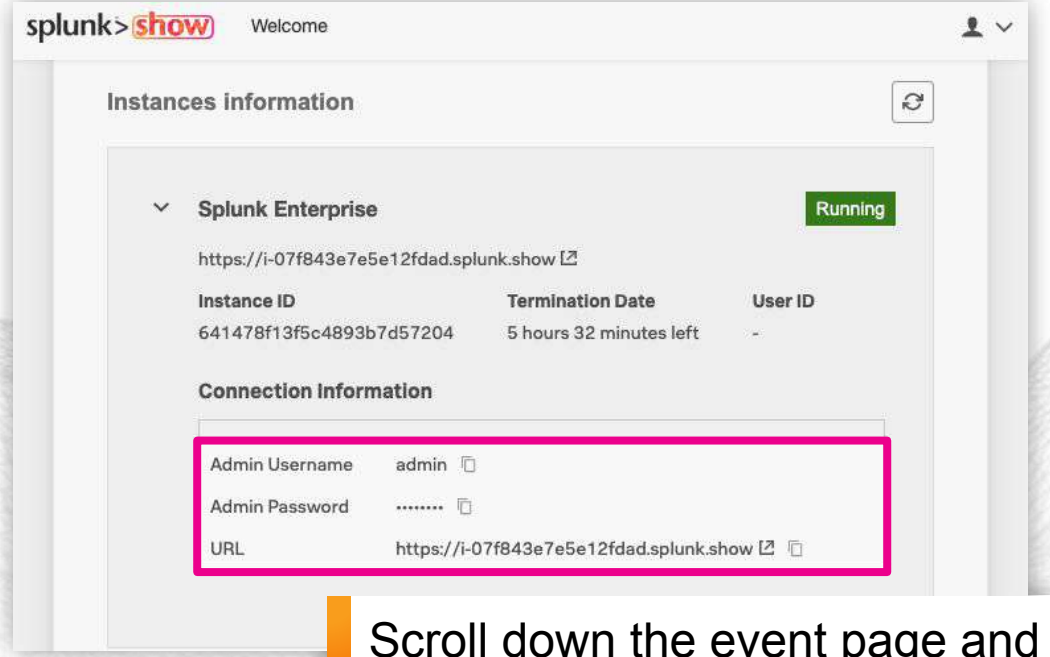
# Hands-On

Time to practice


splunk>

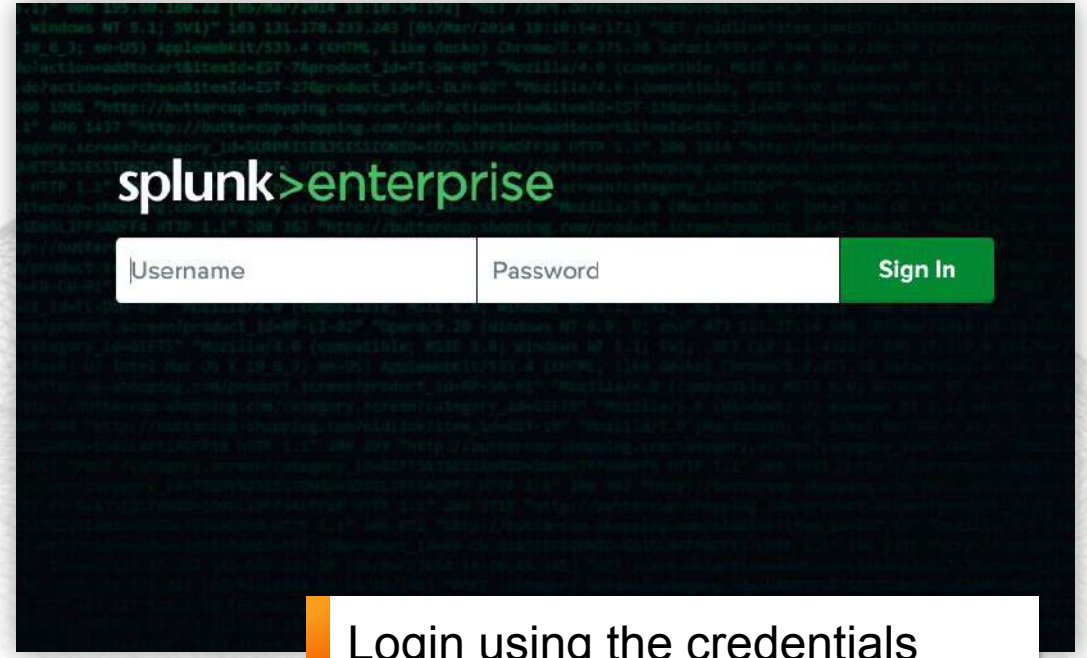
# Login to Splunk

Locate your instance URL and credentials in the Splunk Show event
https://show.splunk.com




Scroll down the event page and expand the **Splunk Enterprise** section to view your login details

Log in to your Splunk instance

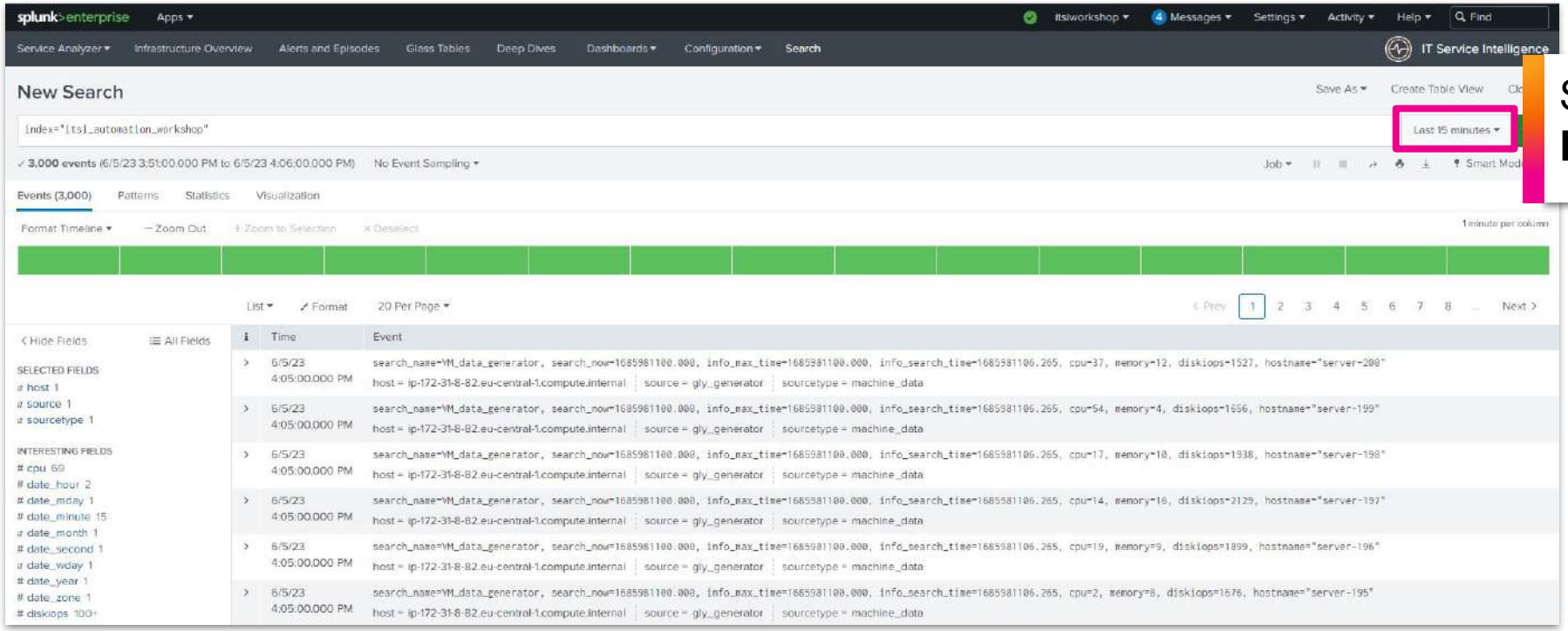



Login using the credentials provided by Splunk Show

# Check Live Data

First open **IT Service Intelligence** and check that there is some live data in the **itsi_automation_workshop** index

```
index="itsi_automation_workshop"
```




Search over the **Last 15 minutes**

splunk>

# Check Lookup

Check that 2 lookup files are present:

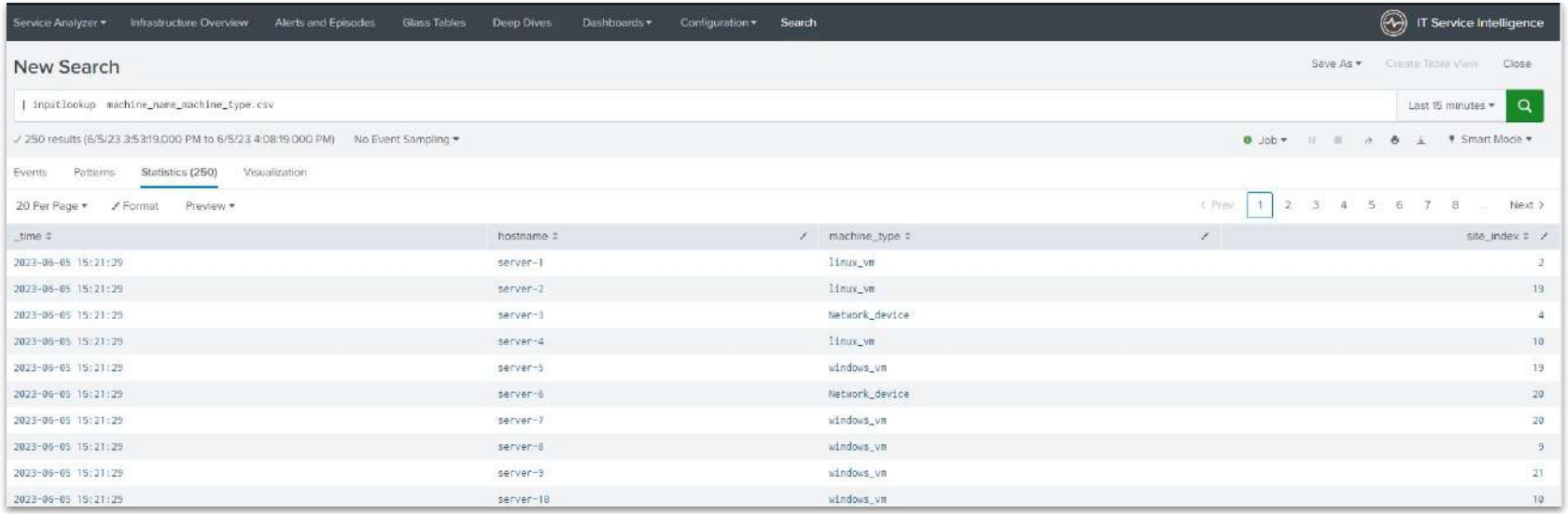
- **machine_name_machine_type.csv**
- **Geosite_machine_index.csv**

Search 1:

```
| inputlookup machine_name_machine_type.csv
```

Search 2:

```
| inputlookup Geosite_machine_index.csv
```




| _time | hostname | machine_type | site_index |
|---|---|---|---|
| 2023-06-05 15:21:29 | server-1 | linux_vm | 2 |
| 2023-06-05 15:21:29 | server-2 | linux_vm | 19 |
| 2023-06-05 15:21:29 | server-3 | Network_device | 4 |
| 2023-06-05 15:21:29 | server-4 | linux_vm | 10 |
| 2023-06-05 15:21:29 | server-5 | windows_vm | 19 |
| 2023-06-05 15:21:29 | server-6 | Network_device | 20 |
| 2023-06-05 15:21:29 | server-7 | windows_vm | 20 |
| 2023-06-05 15:21:29 | server-8 | windows_vm | 9 |
| 2023-06-05 15:21:29 | server-9 | windows_vm | 21 |
| 2023-06-05 15:21:29 | server-10 | windows_vm | 10 |

splunk>

# The Story

Time to practice

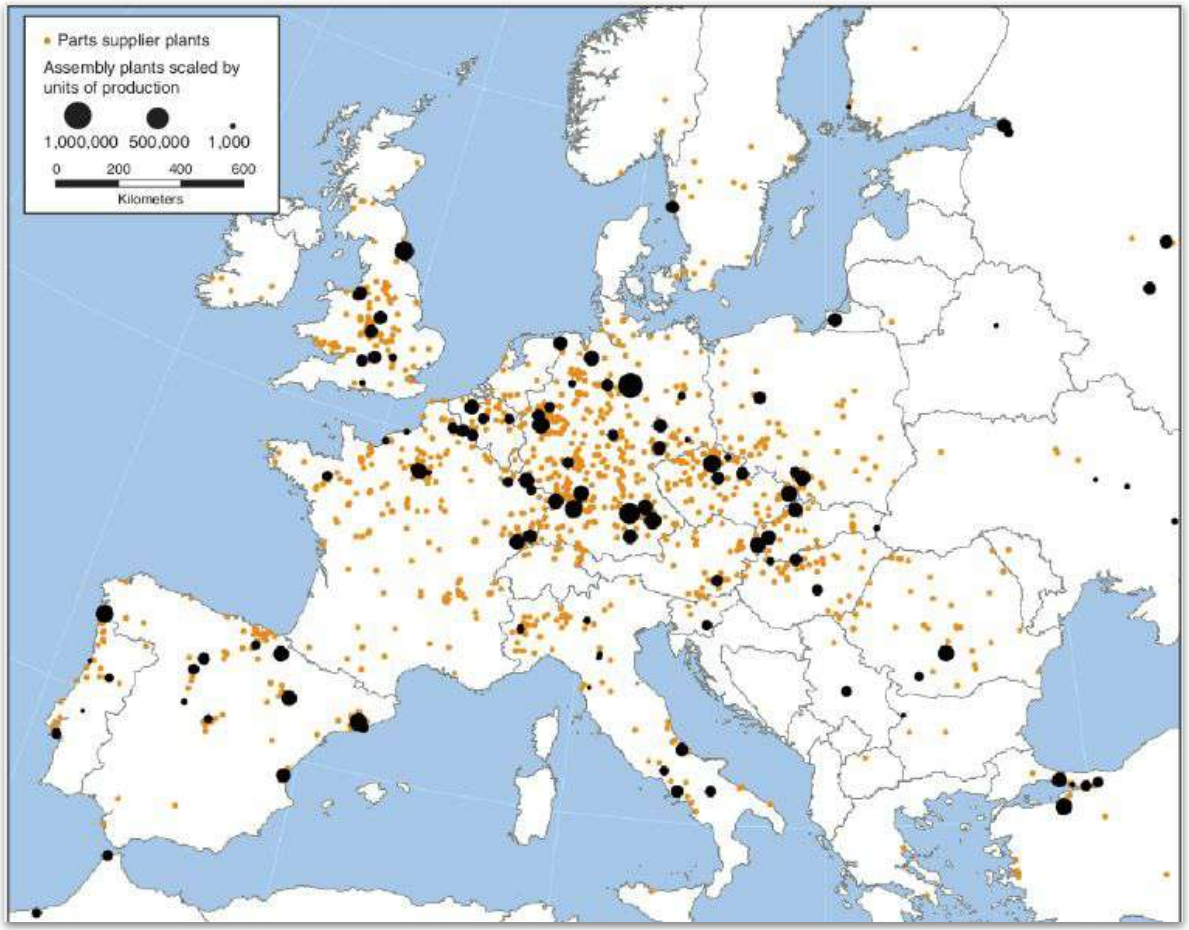

splunk>

# The Splunk T-Shirt Company

The Splunk T-Shirt Company has a large number of selling points and production sites across EMEA but is not able to easily monitor all of the remote IT.

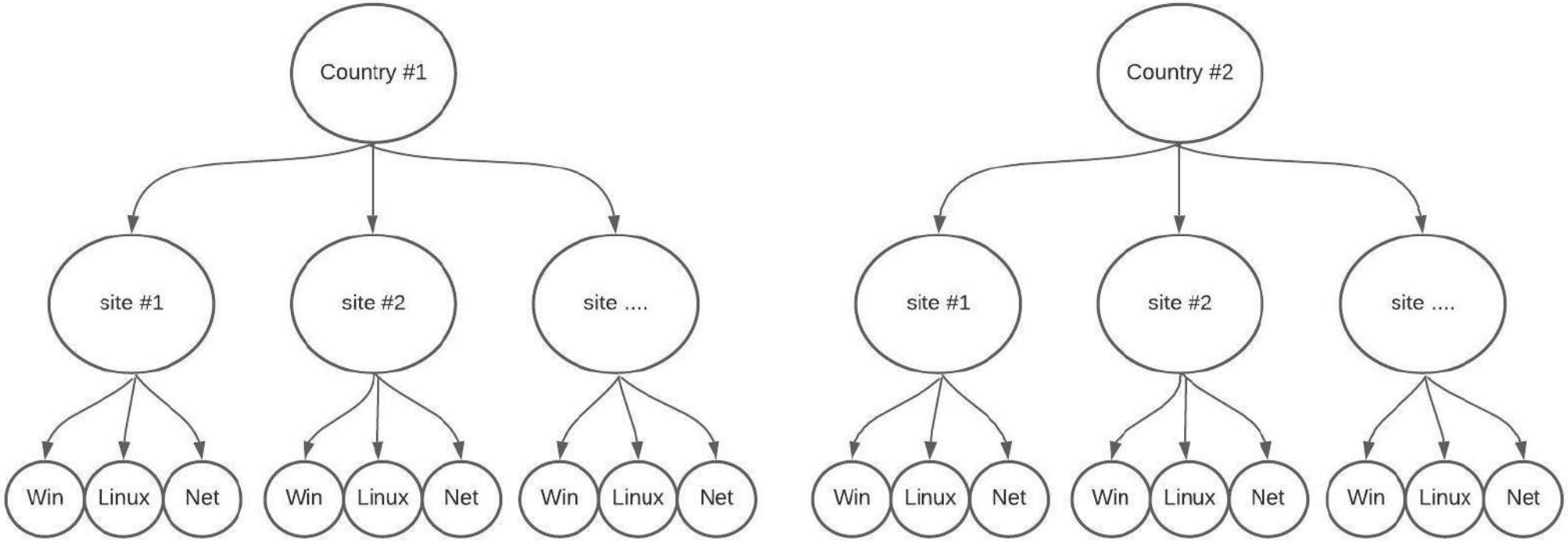
“Heckle the IT admin” has done a very good job when modeling a first Splunk T-Shirt Company production site in ITSI, but he needs “Jeckel - a more advanced ITSI user ” to find a way to reduce efforts needed to create and maintain the 50 production sites. And you are “Jeckel” :)

Heckle and Jeckel will focus first on Spanish and Italian production sites.

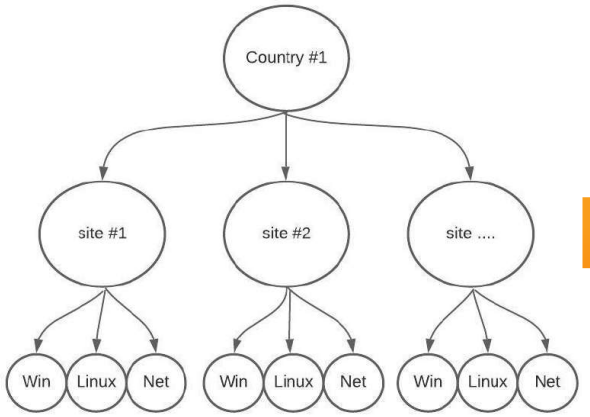


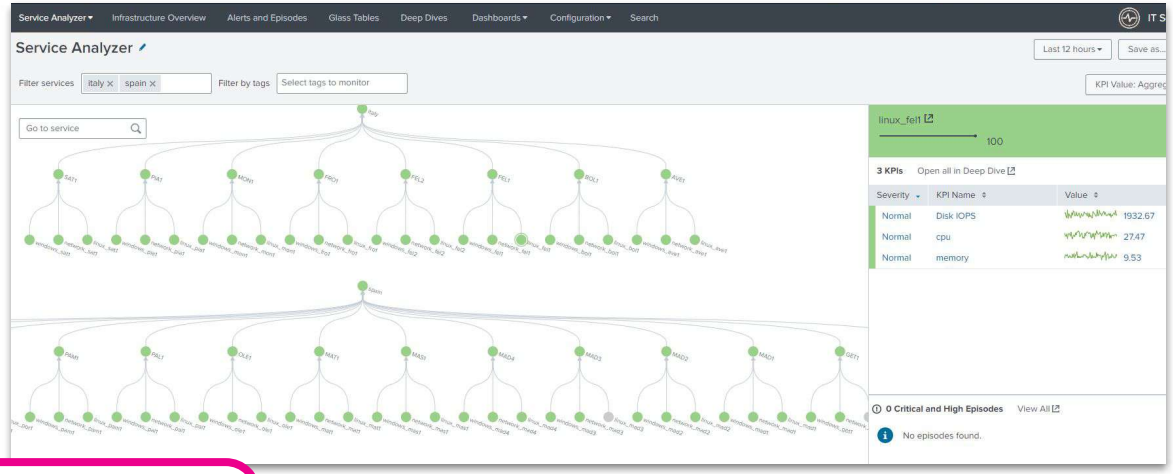
# Structure Sample / Service Decomposition Workshop

After a workshop Heckle and Jeckel decided with the CTO to focus on Linux, Windows and some standard network devices that are present in 99% of the remote sites (**90 sites and 500 entities**)



# Steps to go from paper to a working ITSI environment




**Live data**
`index=itsi_automation_workshop`

**Data enrichment**
machine_name_machine_type.csv
Geosite_machine_index.csv

**Service Template**
Entity filtering rules

1 SPL search

3 SPL search

**Create entities**
2

Entity Binding
5

**Create services**
4

1. Build a search that list all your assets
2. Create entities from the asset list
3. Build a search that list all services and dependencies
4. Create services from the search in step 3
5. Complete entities filtering rules

splunk>

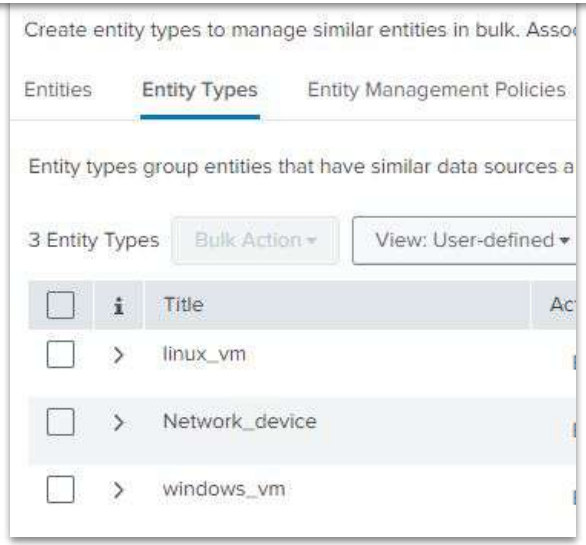
# Step 1: Add Your 500 ITSI Entities

To add entities you need to enrich your live data with an extract of the Splunk T-Shirt Company CMDB that provides:

- a list of assets
- ID of the production site
- machine type*

* The "**machine type**" field will be used to map one of the 3 "entity type" that have been already created

```
index="itsi_automation_workshop"
| dedup hostname
| lookup machine_name_machine_type.csv hostname
| table Geosite hostname machineAlias machine_type
site_index
```



# Step 1: Add Your 500 ITSI Entities

```
index="itsi_automation_workshop"
| dedup hostname
| lookup machine_name_machine_type.csv hostname
| table Geosite hostname machineAlias machine_type site_index
```

New Search

Save As ▾ Create Table View Close

```
index="itsi_automation_workshop" |dedup hostname |lookup machine_name_machine_type.csv hostname |table Geosite hostname
    machineAlias machine_type site_index
```

Last 24 hours

✓ **500 events** (6/25/23 11:00:00.000 AM to 6/26/23 11:32:46.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

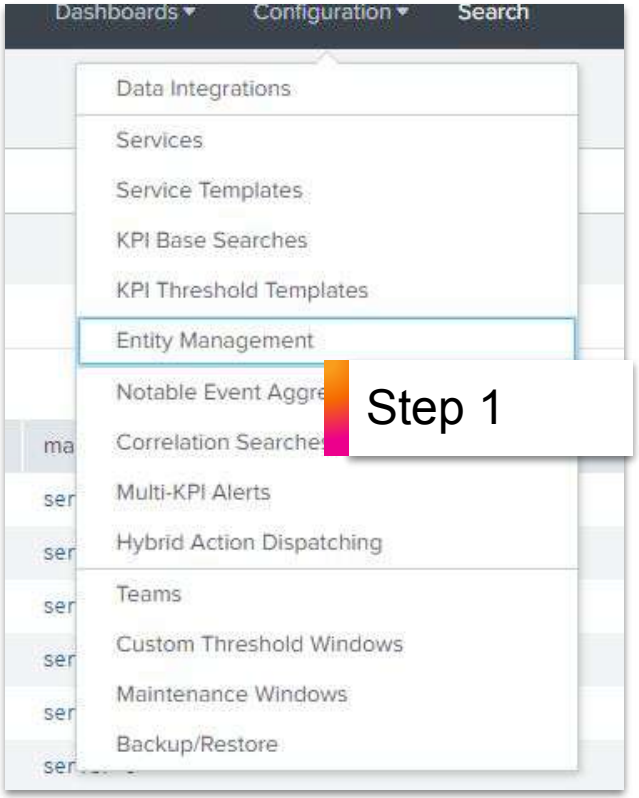
Events Patterns **Statistics (500)** Visualization

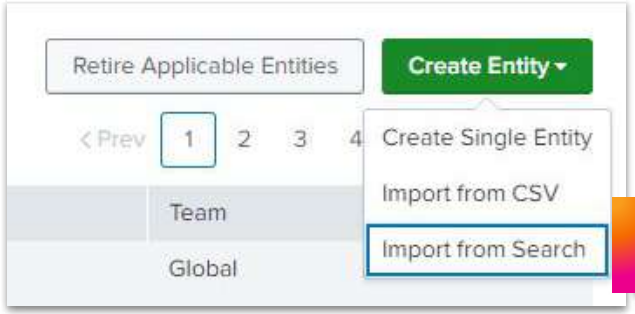
20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

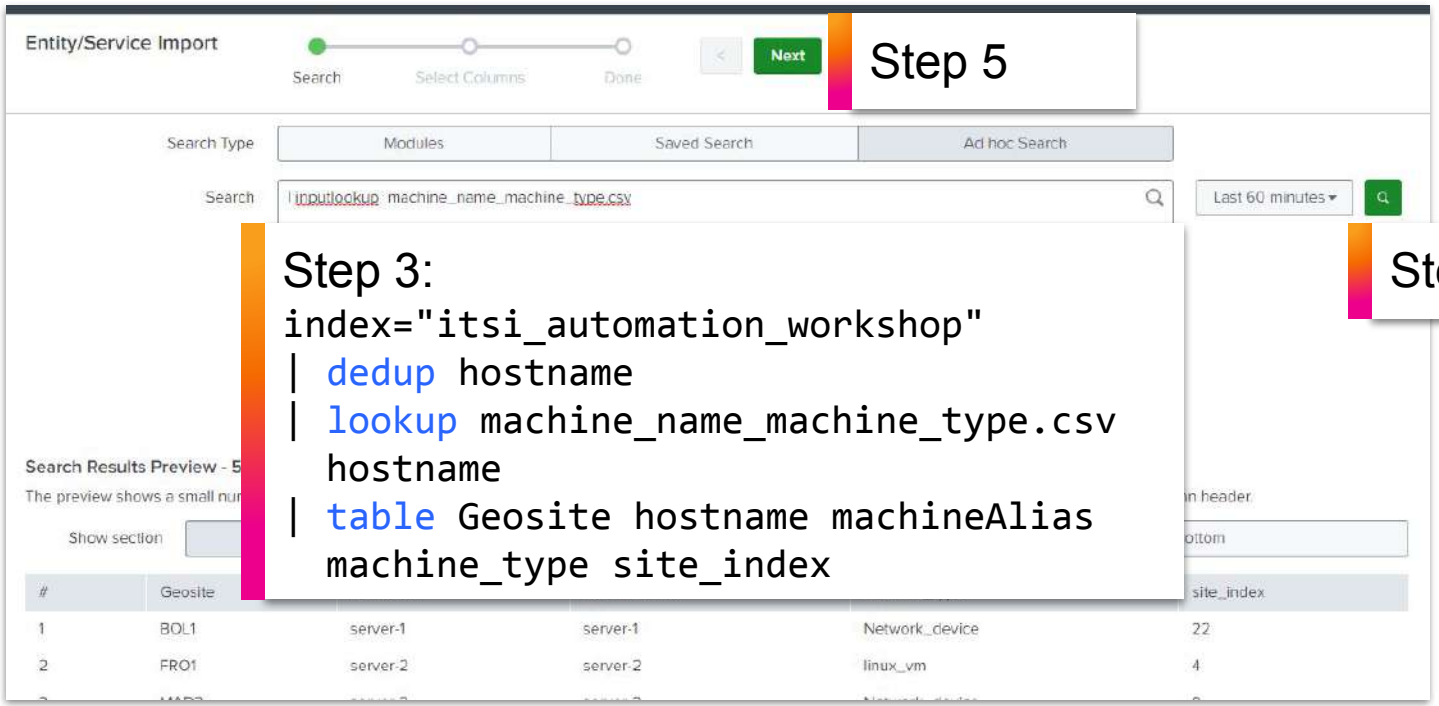
| Geosite | hostname | machineAlias | machine_type | site_index |
|---|---|---|---|---|
| SAR1 | server-500 | server-500 | windows_vm | 19 |
| MON1 | server-499 | server-499 | windows_vm | 13 |
| MAD1 | server-498 | server-498 | Network_device | 7 |
| PIA1 | server-497 | server-497 | linux_vm | 17 |
| MON1 | server-496 | server-496 | Network_device | 13 |
| MAS1 | server-495 | server-495 | Network_device | 11 |
| MAD4 | server-494 | server-494 | windows_vm | 10 |
| FEL1 | server-493 | server-493 | Network_device | 2 |
| MAS1 | server-492 | server-492 | Network_device | 11 |

splunk>

# Step 1: Add Your 500 ITSI Entities




Step 3:

```
index="itsi_automation_workshop"
| dedup hostname
| lookup machine_name_machine_type.csv
  hostname
| table Geosite hostname machineAlias
  machine_type site_index
```

splunk>

# Step 1: Add Your 500 ITSI Entities

Complete the **Import Column As** field as below and click on **Import**

Entity/Service Import

Search — Select Columns — Done

< Import

**Specify Columns**

Select the columns to import and how they should be converted to ITSI object data type (service or entity). If you are importing entities, you must specify one column as the Entity T
importing services, you must specify one column as the Service Title.

| Column Name | Import Column As | Sample Values From Search |
|---|---|---|
| Geosite | Entity Information Field | BOL1 |
| hostname | Entity Title | server-1 |
| machineAlias | Entity Alias | server-1 |
| machine_type | Entity Type | Network_device |
| site_index | Entity Information Field | 22 |

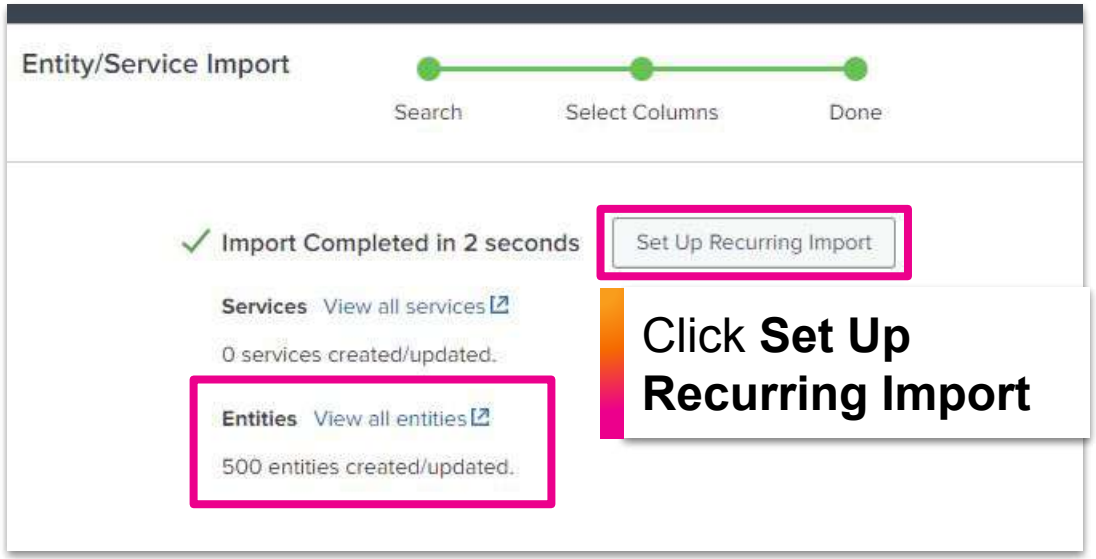
**Settings**

Conflict Resolution: Update Existing Entities

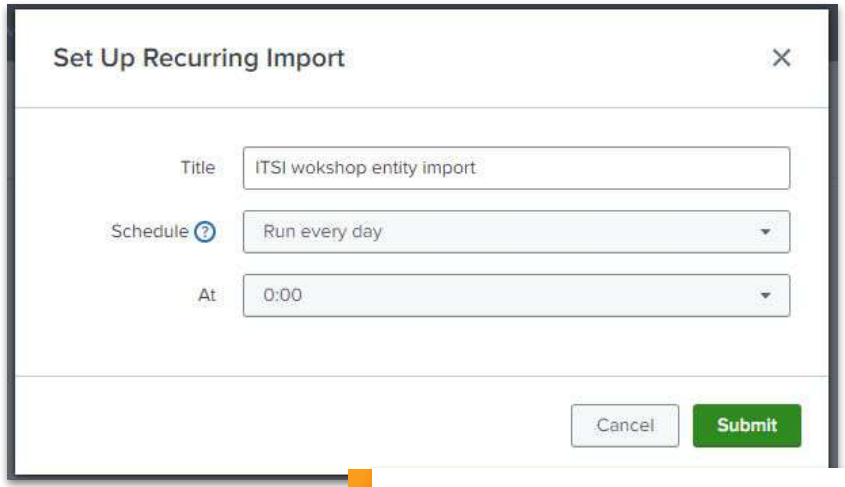
Conflict Resolution Field: hostname

splunk>

# Step 1: Add Your 500 ITSI Entities



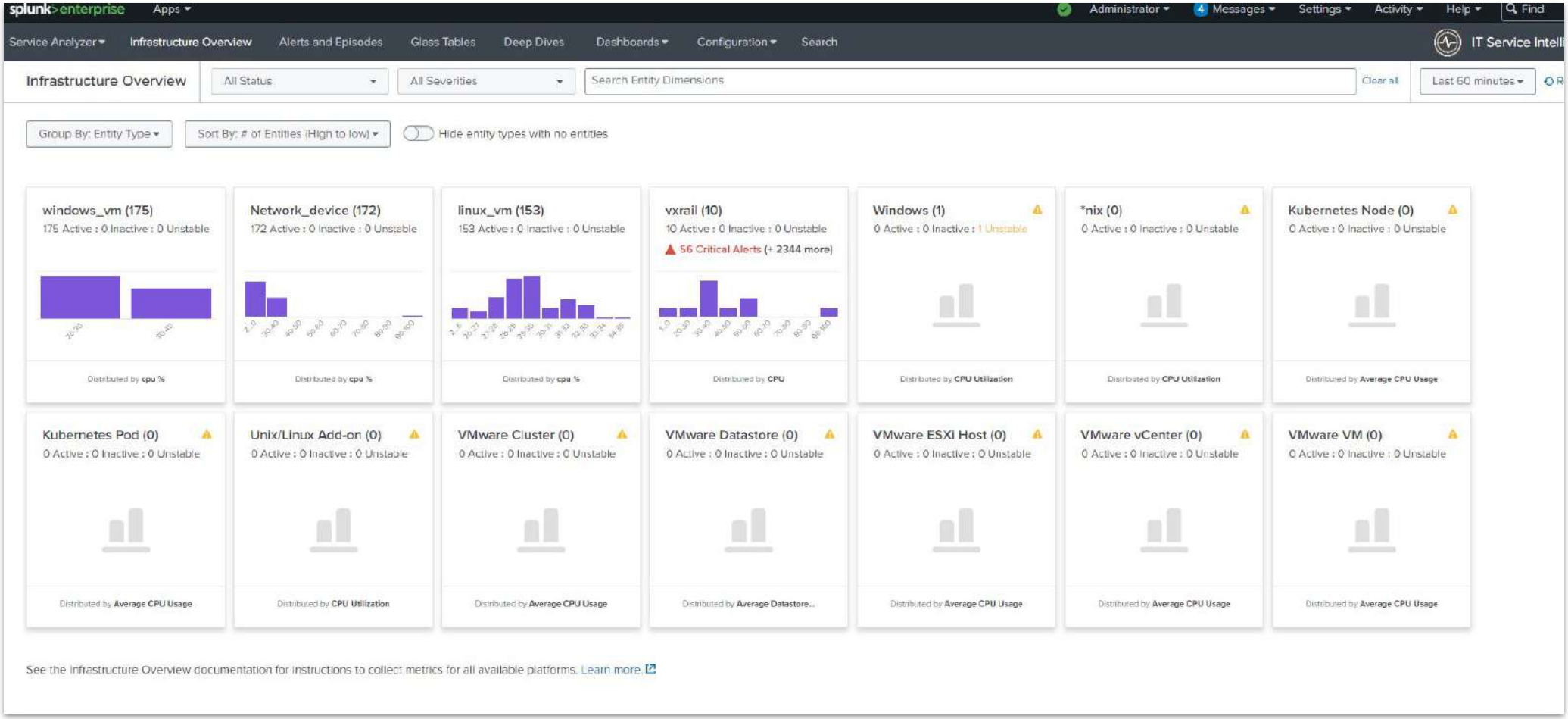

Click **Set Up Recurring Import**




Click **Submit** to schedule your recurring search

# Check Your Entities

Click on **Infrastructure Overview** and look for your new entities!




splunk>

# Check Your Entities

Drill into the **windows_vm** entity type to view the detail of the imported entities

splunk>enterprise Apps ▾ | Administrator ▾ | 4 Messages ▾ | Settings ▾ | Activity ▾ | Help ▾ | Find

Service Analyzer ▾ | Infrastructure Overview | Alerts and Episodes | Glass Tables | Deep Dives | Dashboards ▾ | Configuration ▾ | Search | IT Service Intelligenc

‹ Back | windows_vm | All Status | All Severities | Search Entity Dimensions | Clear all | Last 60 minutes ▾ | Refresh ▾

Entity Health

Current Entity Status Breakdown

cpu % 30

memory % 10

IOPS 1,954

Showing 175 entities with no alerts filter applied. 175 Active | 0 Unstable | 0 Inactive | 0 N/A

20 per page ▾ ‹ Prev 1 2 3 4 5 ... 9 Next ›

| Entity Name | Status | Last Updated | Dimensions | cpu % | memory % | IOPS |
|---|---|---|---|---|---|---|
| server-100 | Active | Wed, 14 Jun 2023 08:15:06 GMT | entity_name: server-100, hostname: server-100, machineAlias: server-100, Geosite: FEL1, site_index: 2 | 38 ↓ -17 | 14 ↑ 10 | 1899 ↓ -83 |
| server-102 | Active | Wed, 14 Jun 2023 08:15:06 GMT | entity_name: server-102, hostname: server-102, machineAlias: server-102, Geosite: MAS1, site_index: 11 | 51 ↑ 25 | 7 ↑ 1 | 1628 ↓ -623 |
| server-103 | Active | Wed, 14 Jun 2023 08:15:06 GMT | entity_name: server-103, hostname: server-103, machineAlias: server-103, Geosite: STA1, site_index: 21 | 39 ↑ 31 | 9 ↑ 4 | 1807 ↓ -436 |
| server-110 | Active | Wed, 14 Jun 2023 08:15:06 GMT | entity_name: server-110, hostname: server-110, machineAlias: server-110, Geosite: POR1, site_index: 18 | 21 ↓ -12 | 19 ↑ 8 | 1931 ↓ -44 |

splunk>

# Step 2: Automate Your Service Tree

## What ITSI expects when creating services

In order to automate a service tree in ITSI we need to create a Magic Table from SPL searches that fit with ITSI's expected fields:

| Service name | service dependency | service template | service tag 1 | service tag2 | service tag3 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

Seems to be too easy??

# Step 2: Automate Your Service Tree

## What ITSI expects when creating services

To get info about a production site we use a CMDB export with the following fields:

```
| inputlookup workshop_part1_site.csv
```

New Search

Save As ▾ Create Table View Close

|inputlookup workshop_part1_site.csv

Last 24 hours ▾

✓ 376 results (6/25/23 11:00:00.000 AM to 6/26/23 11:48:39.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns Statistics (376) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

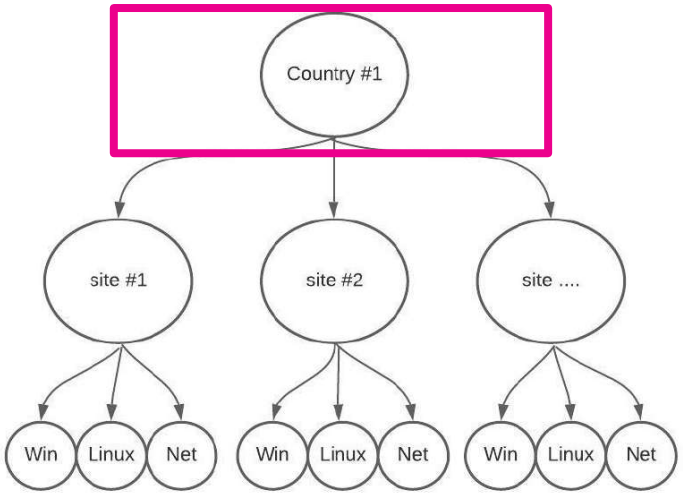
| City_Site | Continent | Country | Geosite | ITC_Code |
|---|---|---|---|---|
| Abbeville 1 | Europe | France | ABB1 | FR |
| Amiens 1 | Europe | France | AMI1 | FR |
| Amiens 2 | Europe | France | AMI2 | FR |
| Amsterdam 1 | Europe | Netherlands | AMS1 | NL |
| Angers 1 | Europe | France | ANG1 | FR |
| Angers 2 | Europe | France | ANG2 | FR |
| Annaka 1 | Asia | Japan | ANK1 | JP |

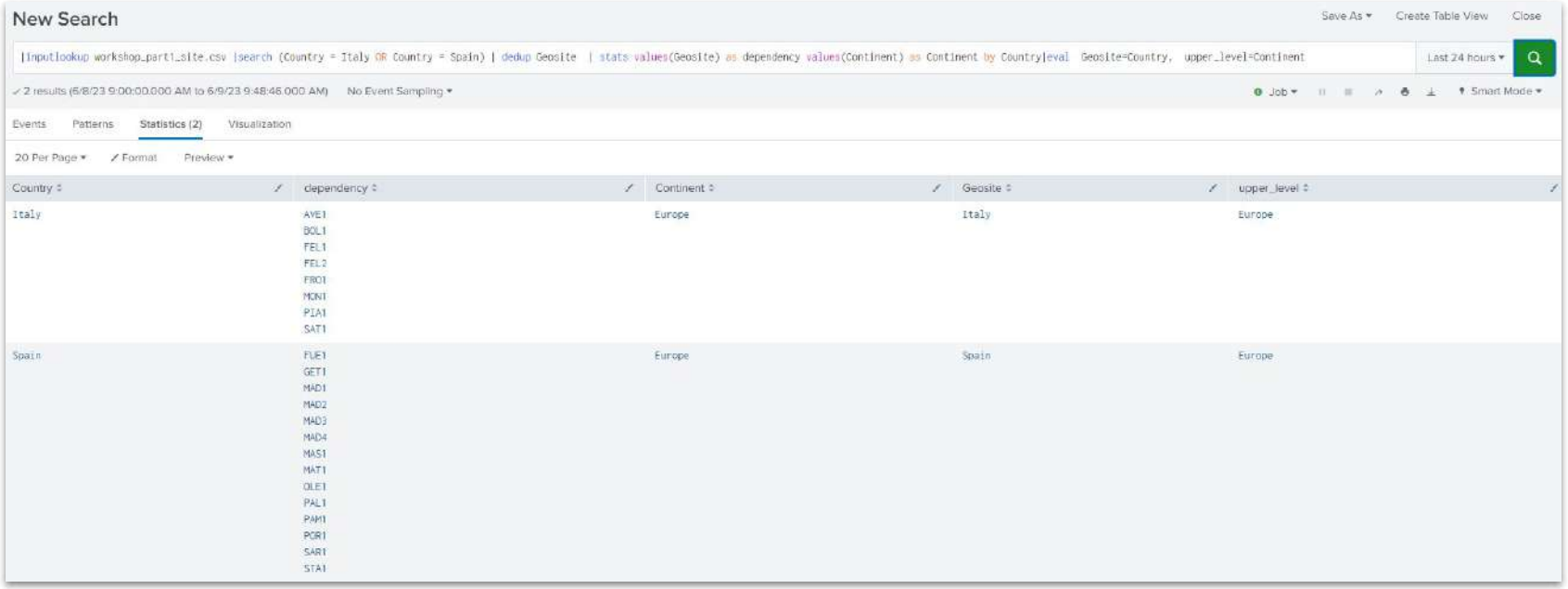
splunk>

# Step 2: Build Your Magic Table

## Service creation: Country

```
| inputlookup workshop_part1_site.csv
| search (Country=Italy OR Country=Spain)
| dedup Geosite
| stats values(Geosite) as dependency values(Continent) as Continent by Country
| eval  Geosite=Country,  upper_level=Continent
```



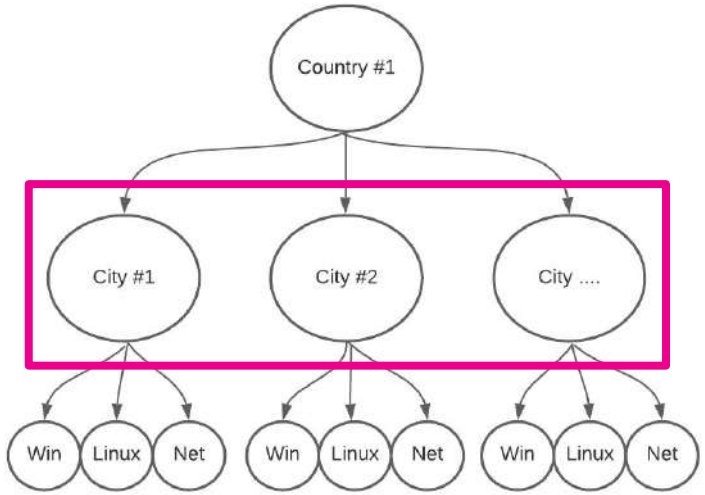



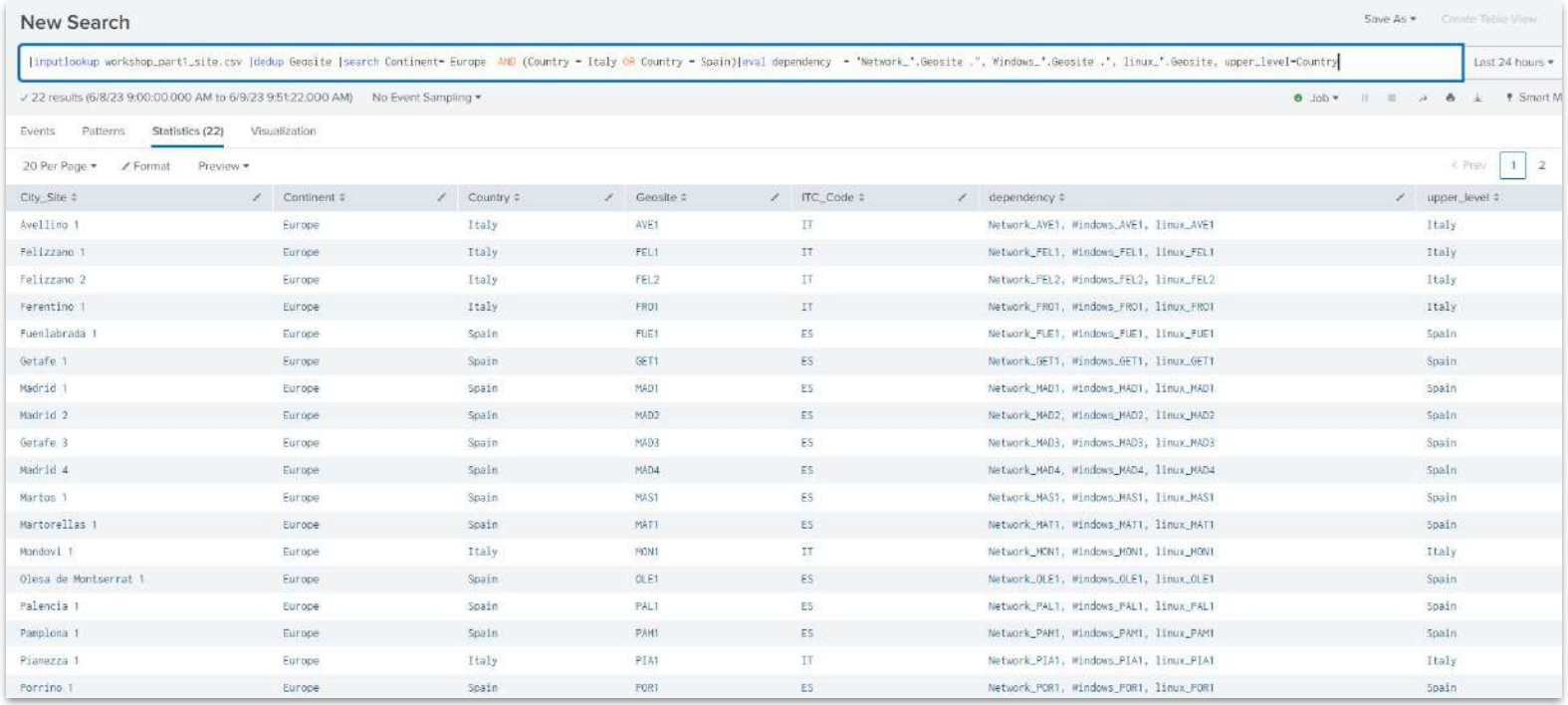

splunk>

# Step 2: Build Your Magic Table

## Service creation: City

```
| inputlookup workshop_part1_site.csv
| dedup Geosite
| search Continent=Europe AND (Country=Italy OR Country=Spain)
| eval dependency="Network_".Geosite ."., Windows_".Geosite ."., linux_".Geosite, upper_level=Country
```



New Search

Save As ▾ Create Table View

```
|inputlookup workshop_part1_site.csv |dedup Geosite |search Continent= Europe AND (Country = Italy OR Country = Spain)|eval dependency = "Network_".Geosite ."., Windows_".Geosite ."., linux_".Geosite, upper_level=Country
```

Last 24 hours ▾

✓ 22 results (6/8/23 9:00:00.000 AM to 6/9/23 9:51:22.000 AM) No Event Sampling ▾ Job ▾ Smart M

Events Patterns Statistics (22) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2

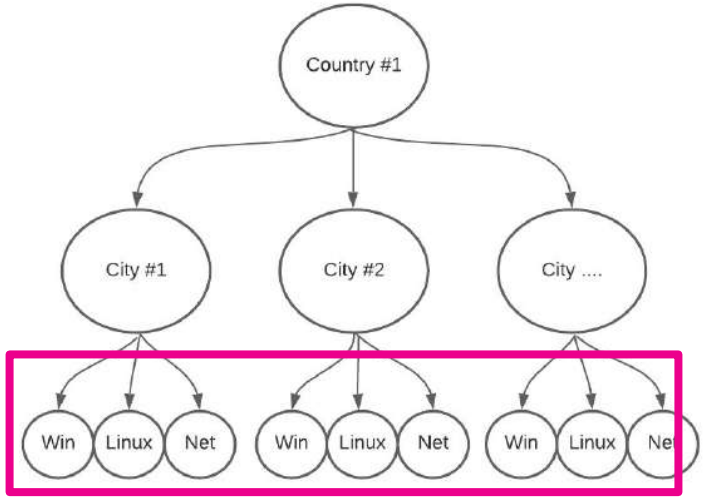
| City_Site | Continent | Country | Geosite | ITC_Code | dependency | upper_level |
|---|---|---|---|---|---|---|
| Avellino 1 | Europe | Italy | AVE1 | IT | Network_AVE1, Windows_AVE1, linux_AVE1 | Italy |
| Felizzano 1 | Europe | Italy | FEL1 | IT | Network_FEL1, Windows_FEL1, linux_FEL1 | Italy |
| Felizzano 2 | Europe | Italy | FEL2 | IT | Network_FEL2, Windows_FEL2, linux_FEL2 | Italy |
| Ferentino 1 | Europe | Italy | FRO1 | IT | Network_FRO1, Windows_FRO1, linux_FRO1 | Italy |
| Fuenlabrada 1 | Europe | Spain | FUE1 | ES | Network_FUE1, Windows_FUE1, linux_FUE1 | Spain |
| Getafe 1 | Europe | Spain | GET1 | ES | Network_GET1, Windows_GET1, linux_GET1 | Spain |
| Madrid 1 | Europe | Spain | MAD1 | ES | Network_MAD1, Windows_MAD1, linux_MAD1 | Spain |
| Madrid 2 | Europe | Spain | MAD2 | ES | Network_MAD2, Windows_MAD2, linux_MAD2 | Spain |
| Getafe 3 | Europe | Spain | MAD3 | ES | Network_MAD3, Windows_MAD3, linux_MAD3 | Spain |
| Madrid 4 | Europe | Spain | MAD4 | ES | Network_MAD4, Windows_MAD4, linux_MAD4 | Spain |
| Martos 1 | Europe | Spain | MAS1 | ES | Network_MAS1, Windows_MAS1, linux_MAS1 | Spain |
| Martorellas 1 | Europe | Spain | MAT1 | ES | Network_MAT1, Windows_MAT1, linux_MAT1 | Spain |
| Mondovi 1 | Europe | Italy | MON1 | IT | Network_MON1, Windows_MON1, linux_MON1 | Italy |
| Olesa de Montserrat 1 | Europe | Spain | OLE1 | ES | Network_OLE1, Windows_OLE1, linux_OLE1 | Spain |
| Palencia 1 | Europe | Spain | PAL1 | ES | Network_PAL1, Windows_PAL1, linux_PAL1 | Spain |
| Pamplona 1 | Europe | Spain | PAM1 | ES | Network_PAM1, Windows_PAM1, linux_PAM1 | Spain |
| Pianezza 1 | Europe | Italy | PIA1 | IT | Network_PIA1, Windows_PIA1, linux_PIA1 | Italy |
| Porrino 1 | Europe | Spain | POR1 | ES | Network_POR1, Windows_POR1, linux_POR1 | Spain |

splunk>

# Step 2: Build Your Magic Table

## Service creation: Technical service

```
| inputlookup workshop_part1_site.csv
| search (Country=Italy OR Country=Spain)
| eval upper_level=Geosite, Geosite="linux_".Geosite
| appendpipe [search | inputlookup workshop_part1_site.csv
  | search (Country=Italy OR Country=Spain) | eval upper_level=Geosite, Geosite="Windows_".Geosite]
  | appendpipe [search | inputlookup workshop_part1_site.csv
    | search (Country=Italy OR Country=Spain) | eval upper_level=Geosite, Geosite="Network_".Geosite]
```




Events (0) Patterns Statistics (44) Visualization

20 Per Page ▾ Format Preview ▾

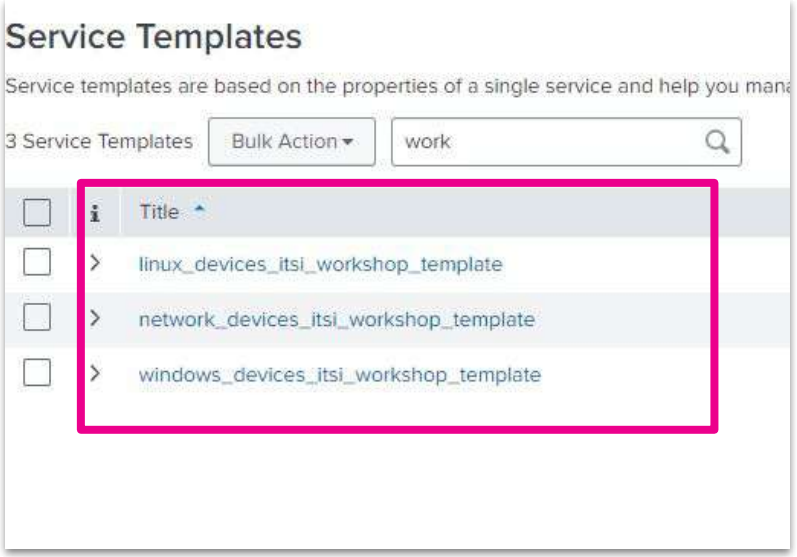
| City_Site | Continent | Country | Geosite | ITC_Code | upper_le |
|---|---|---|---|---|---|
| Santa Perpetua 1 | Europe | Spain | Windows_STA1 | ES | STA1 |
| Bologna 1 | Europe | Italy | Windows_BOL1 | IT | BOL1 |
| Avellino 1 | Europe | Italy | Network_AVE1 | IT | AVE1 |
| Felizzano 1 | Europe | Italy | Network_FEL1 | IT | FEL1 |
| Felizzano 2 | Europe | Italy | Network_FEL2 | IT | FEL2 |
| Ferentino 1 | Europe | Italy | Network_FRO1 | IT | FRO1 |
| Fuenlabrada 1 | Europe | Spain | Network_FUE1 | ES | FUE1 |
| Getafe 1 | Europe | Spain | Network_GET1 | ES | GET1 |
| Madrid 1 | Europe | Spain | Network_MAD1 | ES | MAD1 |
| Madrid 2 | Europe | Spain | Network_MAD2 | ES | MAD2 |

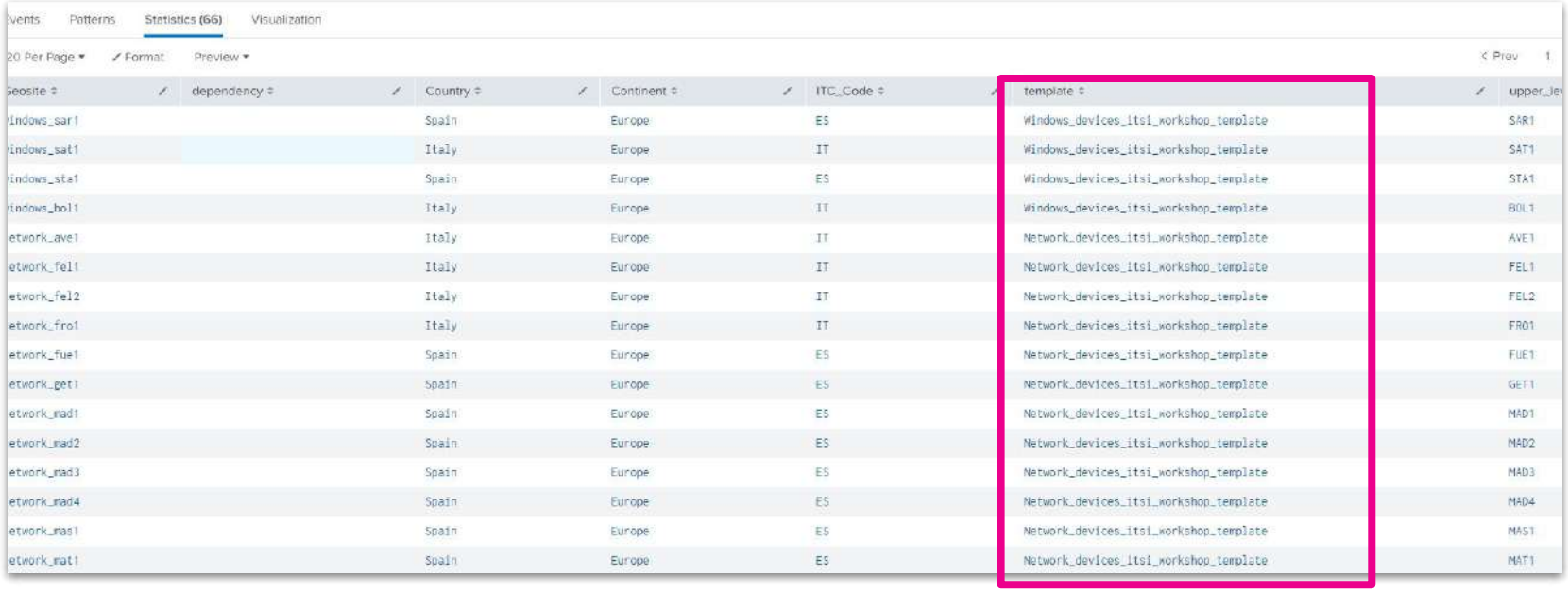
splunk>

# Step 2: Build Your Magic Table

## Service creation: Map your Template

```
| eval template=case(like(Geosite,"%linux%"), "linux_devices_itsi_workshop_template",
  like(Geosite,"%Windows%"),"Windows_devices_itsi_workshop_template",
  like(Geosite,"%Network%"),"Network_devices_itsi_workshop_template")
| eval Geosite=lower(Geosite)
| table Geosite dependency Country Continent ITC_Code template upper_level
```




| Geosite | dependency | Country | Continent | ITC_Code | template | upper_le |
|---|---|---|---|---|---|---|
| indows_sar1 | | Spain | Europe | ES | Windows_devices_itsi_workshop_template | SAR1 |
| indows_sat1 | | Italy | Europe | IT | Windows_devices_itsi_workshop_template | SAT1 |
| indows_sta1 | | Spain | Europe | ES | Windows_devices_itsi_workshop_template | STA1 |
| indows_bol1 | | Italy | Europe | IT | Windows_devices_itsi_workshop_template | BOL1 |
| etwork_ave1 | | Italy | Europe | IT | Network_devices_itsi_workshop_template | AVE1 |
| etwork_fel1 | | Italy | Europe | IT | Network_devices_itsi_workshop_template | FEL1 |
| etwork_fel2 | | Italy | Europe | IT | Network_devices_itsi_workshop_template | FEL2 |
| etwork_fro1 | | Italy | Europe | IT | Network_devices_itsi_workshop_template | FRO1 |
| etwork_fue1 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | FUE1 |
| etwork_get1 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | GET1 |
| etwork_mad1 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | MAD1 |
| etwork_mad2 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | MAD2 |
| etwork_mad3 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | MAD3 |
| etwork_mad4 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | MAD4 |
| etwork_mas1 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | MAS1 |
| etwork_mat1 | | Spain | Europe | ES | Network_devices_itsi_workshop_template | MAT1 |

splunk>

# Step 2: Build Your Magic Table

## Merge your searches

Merge your searches with appendpipe command

```
| inputlookup workshop_part1_site.csv | search (Country=Italy OR Country=Spain) | dedup Geosite
| stats values(Geosite) as dependency values(Continent) as Continent by Country
| eval  Geosite=Country, upper_level=Continent
| appendpipe [| inputlookup workshop_part1_site.csv
   | dedup Geosite | search Continent=Europe AND (Country=Italy OR Country=Spain)
   | eval dependency="Network_".Geosite ., Windows_".Geosite ., linux_".Geosite, upper_level=Country ]
| appendpipe [search | inputlookup workshop_part1_site.csv
   | search (Country=Italy OR Country=Spain) | eval upper_level=Geosite,  Geosite="linux_".Geosite]
| appendpipe [search | inputlookup workshop_part1_site.csv
   | search (Country=Italy OR Country=Spain) | eval upper_level=Geosite, Geosite="Windows_".Geosite]
| appendpipe [search | inputlookup workshop_part1_site.csv
   | search (Country=Italy OR Country=Spain) | eval upper_level=Geosite, Geosite="Network_".Geosite]
   | eval template=case(like(Geosite, "%linux%"), "linux_devices_itsi_workshop_template",
     like(Geosite, "%Windows%"), "Windows_devices_itsi_workshop_template",like(Geosite, "%Network%"),
     "Network_devices_itsi_workshop_template")
   | eval Geosite=lower(Geosite)
   | table Geosite dependency Country Continent ITC_Code template upper_level
```

splunk>

# Step 2: Build Your Magic Table

## Merge your searches

Here is your magic table with the three levels of dependencies!

New Search

Save As ▾ Create Table View

```
|inputlookup workshop_part1_site.csv |search (Country = Italy OR Country = Spain) | dedup Geosite  | stats values(Geosite) as dependency values(Continent) as Continent by Country|eval  Geosite=Country,  upper_level=Continent

| appendpipe [|inputlookup workshop_part1_site.csv |dedup Geosite |search Continent= Europe  AND (Country = Italy OR Country = Spain)|eval dependency  = "Network_".Geosite ., Windows_".Geosite ., linux_".Geosite, upper_level=Country ]

|appendpipe [search |inputlookup workshop_part1_site.csv |search (Country = Italy OR Country = Spain) |eval upper_level=Geosite,  Geosite = "linux_".Geosite]

| appendpipe [search |inputlookup workshop_part1_site.csv |search (Country = Italy OR Country = Spain) |eval upper_level=Geosite, Geosite = "Windows_".Geosite]

| appendpipe [search |inputlookup workshop_part1_site.csv |search (Country = Italy OR Country = Spain) |eval upper_level=Geosite, Geosite = "Network_".Geosite]

|eval  template= case(like(Geosite, "%linux%"), "linux_devices_itsi_workshop_template",like(Geosite, "%Windows%"), "Windows_devices_itsi_workshop_template",like(Geosite, "%Network%"),"Network_devices_itsi_workshop_template")|eval Geosite
    =lower(Geosite)|table Geosite dependency Country Continent ITC_Code template upper_level
```

Last 24 hours ▾

✓ 90 results (6/8/23 10:00:00.000 AM to 6/9/23 10:01:02.000 AM) No Event Sampling ▾ Job ▾ Smart M

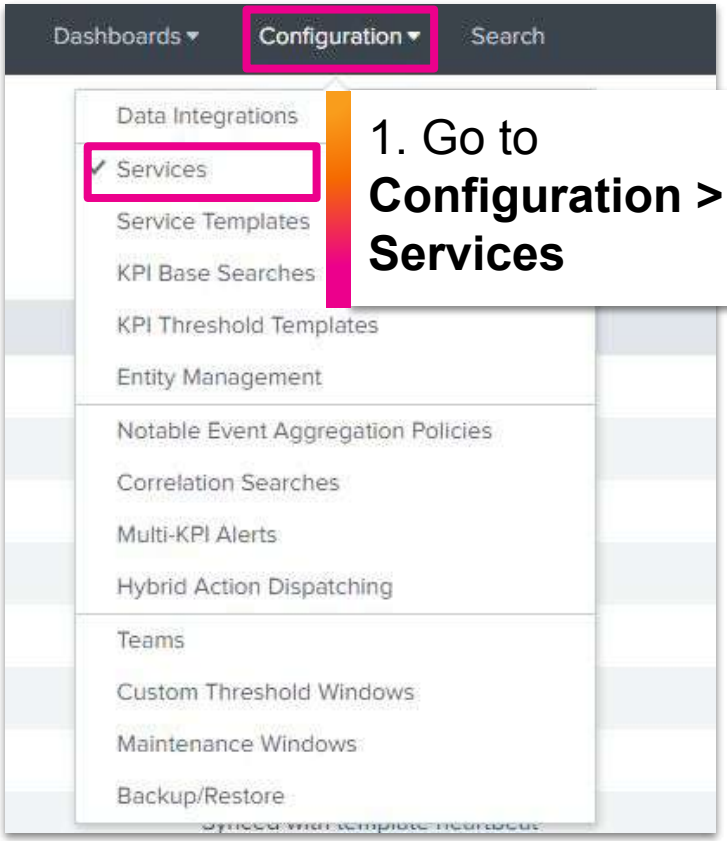
Events Patterns Statistics (90) Visualization

20 Per Page ▾ ✓ Format Preview ▾ ‹ Prev 1 2 3 4 5

| Geosite | dependency | Country | Continent | ITC_Code | template | upper_level |
|---|---|---|---|---|---|---|
| sar1 | Network_SAR1, Windows_SAR1, linux_SAR1 | Spain | Europe | ES | | Spain |
| sat1 | Network_SAT1, Windows_SAT1, linux_SAT1 | Italy | Europe | IT | | Italy |
| sta1 | Network_STA1, Windows_STA1, linux_STA1 | Spain | Europe | ES | | Spain |
| bol1 | Network_BOL1, Windows_BOL1, linux_BOL1 | Italy | Europe | IT | | Italy |
| linux_ave1 | | Italy | Europe | IT | linux_devices_itsi_workshop_template | AVE1 |
| linux_fel1 | | Italy | Europe | IT | linux_devices_itsi_workshop_template | FEL1 |
| linux_fel2 | | Italy | Europe | IT | linux_devices_itsi_workshop_template | FEL2 |
| linux_fro1 | | Italy | Europe | IT | linux_devices_itsi_workshop_template | FRO1 |
| linux_fue1 | | Spain | Europe | ES | linux_devices_itsi_workshop_template | FUE1 |
| linux_get1 | | Spain | Europe | ES | linux_devices_itsi_workshop_template | GET1 |
| linux_mad1 | | Spain | Europe | ES | linux_devices_itsi_workshop_template | MAD1 |
| linux_mad2 | | Spain | Europe | ES | linux_devices_itsi_workshop_template | MAD2 |
| linux_mad3 | | Spain | Europe | ES | linux_devices_itsi_workshop_template | MAD3 |

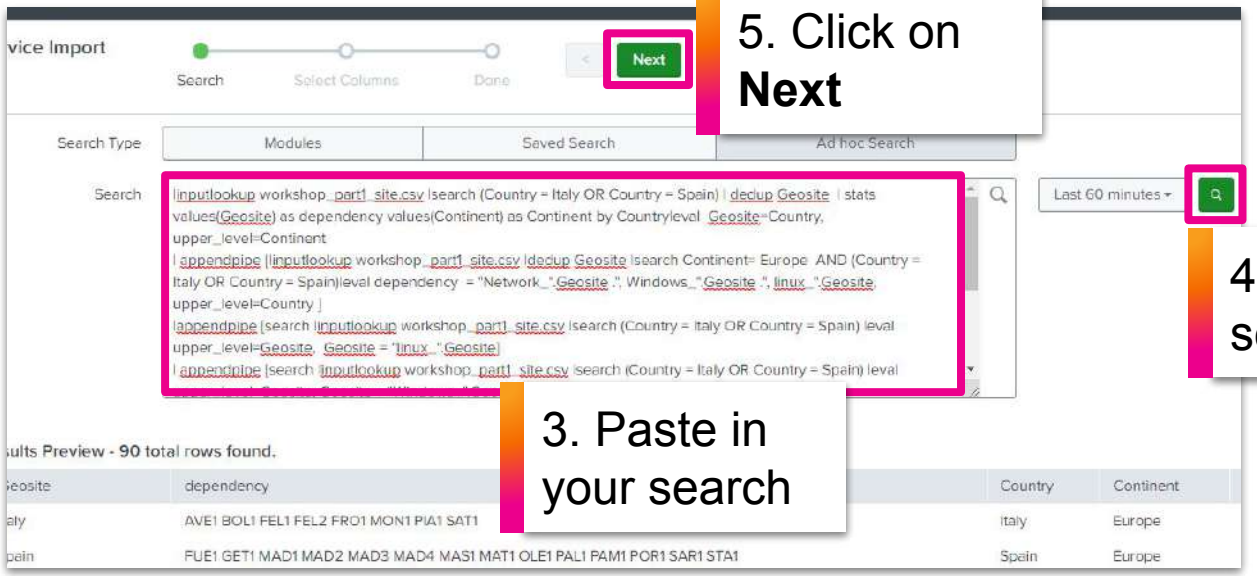
splunk>

# Step 3: Create Service Trees




1. Go to **Configuration > Services**


2. Go to **Create Service > Import from Search**




5. Click on **Next**

4. Run the search

3. Paste in your search

splunk>

# Step 3: Create Service Trees

## Service field mapping

Entity/Service Import

Search — Select Columns — Define Entity Rules — Done

< Next

**Specify Columns**

Select the columns to import and how they should be converted to ITSI object data type (service or entity). If you are importing entities, you must specify one column as the Entity Title. If you are importing ser

| Column Name | Import Column As | Sample Values From Search |
|---|---|---|
| Geosite | Service Title | italy |
| dependency | Dependent Services | AVE1 BOL1 FEL1 FEL2 FRO1 MON1 PI |
| Country | Service Tags | Italy |
| Continent | Service Tags | Europe |
| ITC_Code | Service Tags | |
| template | Service Template Link | |
| upper_level | Service Tags | Europe |

**Settings**

| | |
|---|---|
| Service Team | Global |
| Import Services As | Enabled |
| Enable 7 days of backfill for all service KPIs | Disabled |

Bind your magic table columns with the ITSI definitions as shown in the screenshot, then click on **Next**

splunk>

# Step 3: Create Service Trees

## Specify entity filtering rules

**Define Entity Rules**

Select a template to define the entity rules for its linked services.

3 Service Templates | Filter Service Templates

| Service Template Link | Services | Entity Rules Complete |
|---|---|---|
| Network_devices_itsi_workshop_template | 22 | Incomplete |
| Windows_devices_itsi_workshop_template | 22 | Incomplete |
| linux_devices_itsi_workshop_template | 22 | Incomplete |

Click on each template and complete the entity rules

**Complete Entity Rules for Network_devices_itsi_workshop_template**

The KPIs in the service template will be added to the linked services. The entity rule
entity rules in the template. For service template entity rules whose values need to
which to provide the value.

Entity Type matches Network_device

AND

Info Geosite matches Select a column

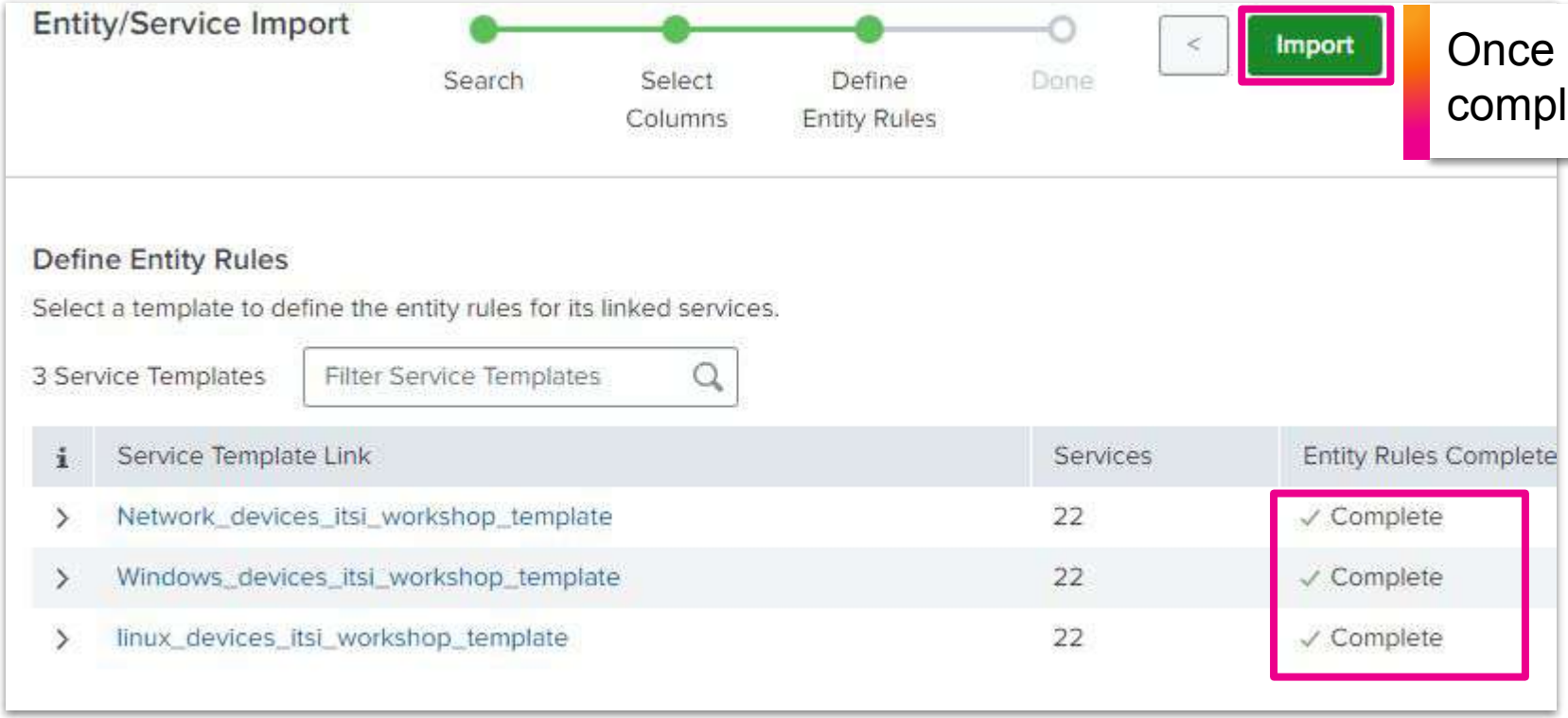
ITC_Code
dependency
template
upper_level
filter

Preview for Service network_ave1

**upper_level** contains the name of the production site. In this example we filter all entities of a specific production site and that have the Entity Type "**Network_device**"

# Step 3: Create Service Trees

## Specify entity filtering rules

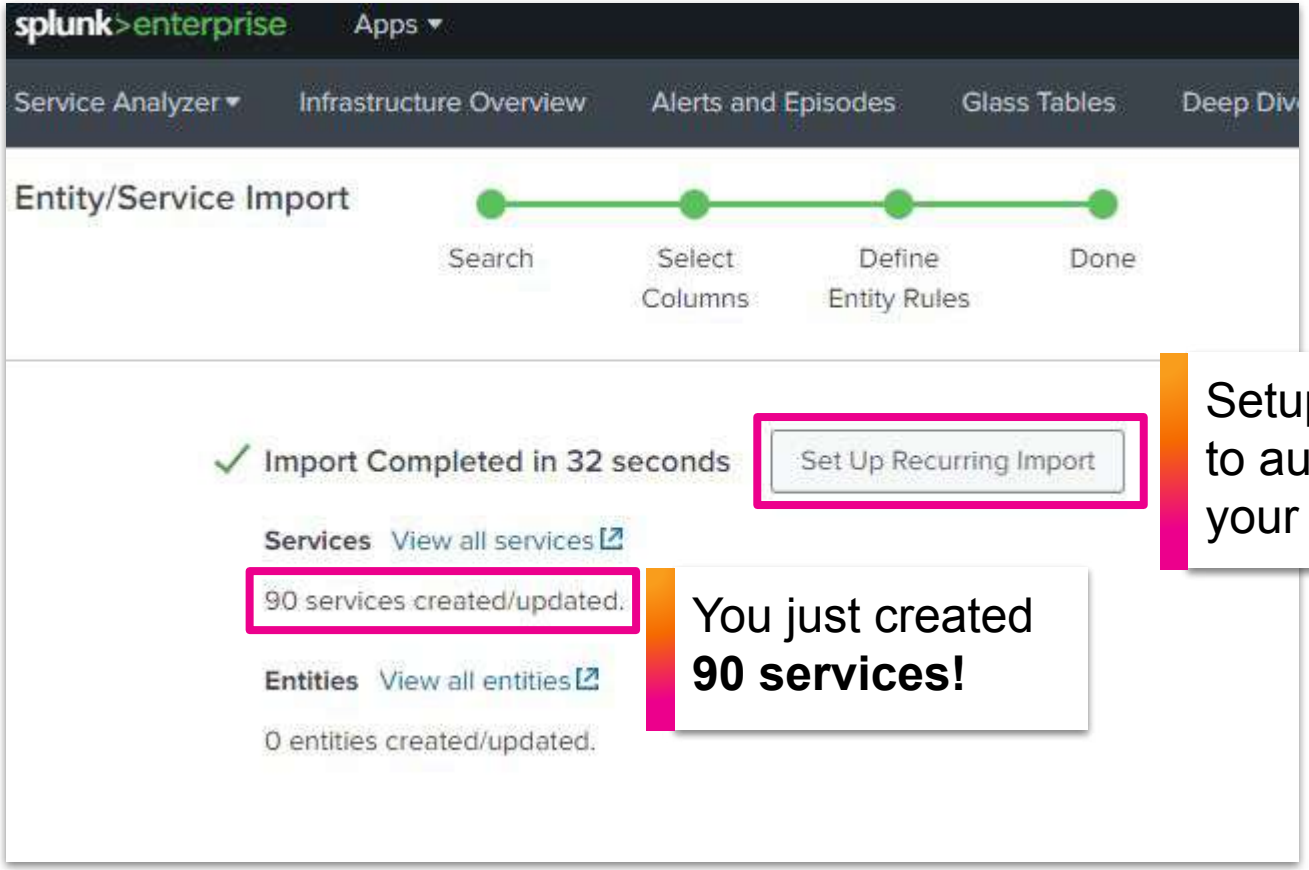



Once all your entity rules are completed, click on **Import**

# Step 3: Create Service Trees

## Specify entity filtering rules

Give your import time to run (it can take up to 1 minute)

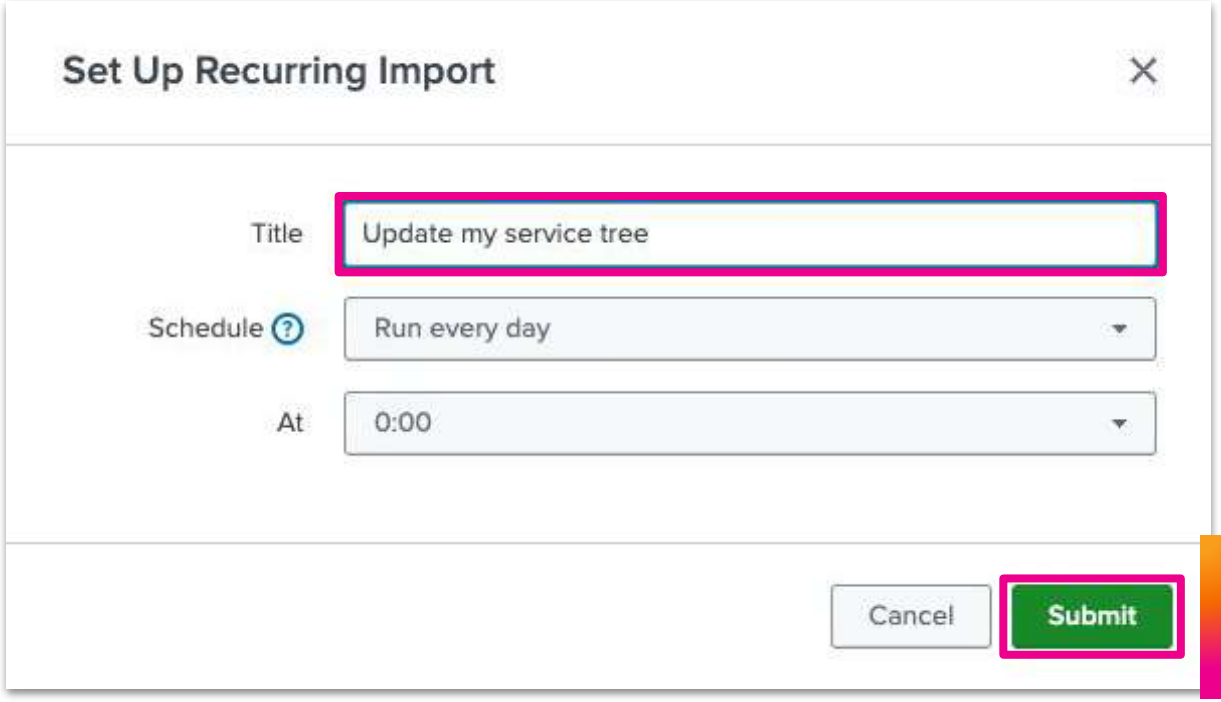



Setup a recurring import to automatically update your service tree!

You just created **90 services!**

# Step 3: Create Service Trees

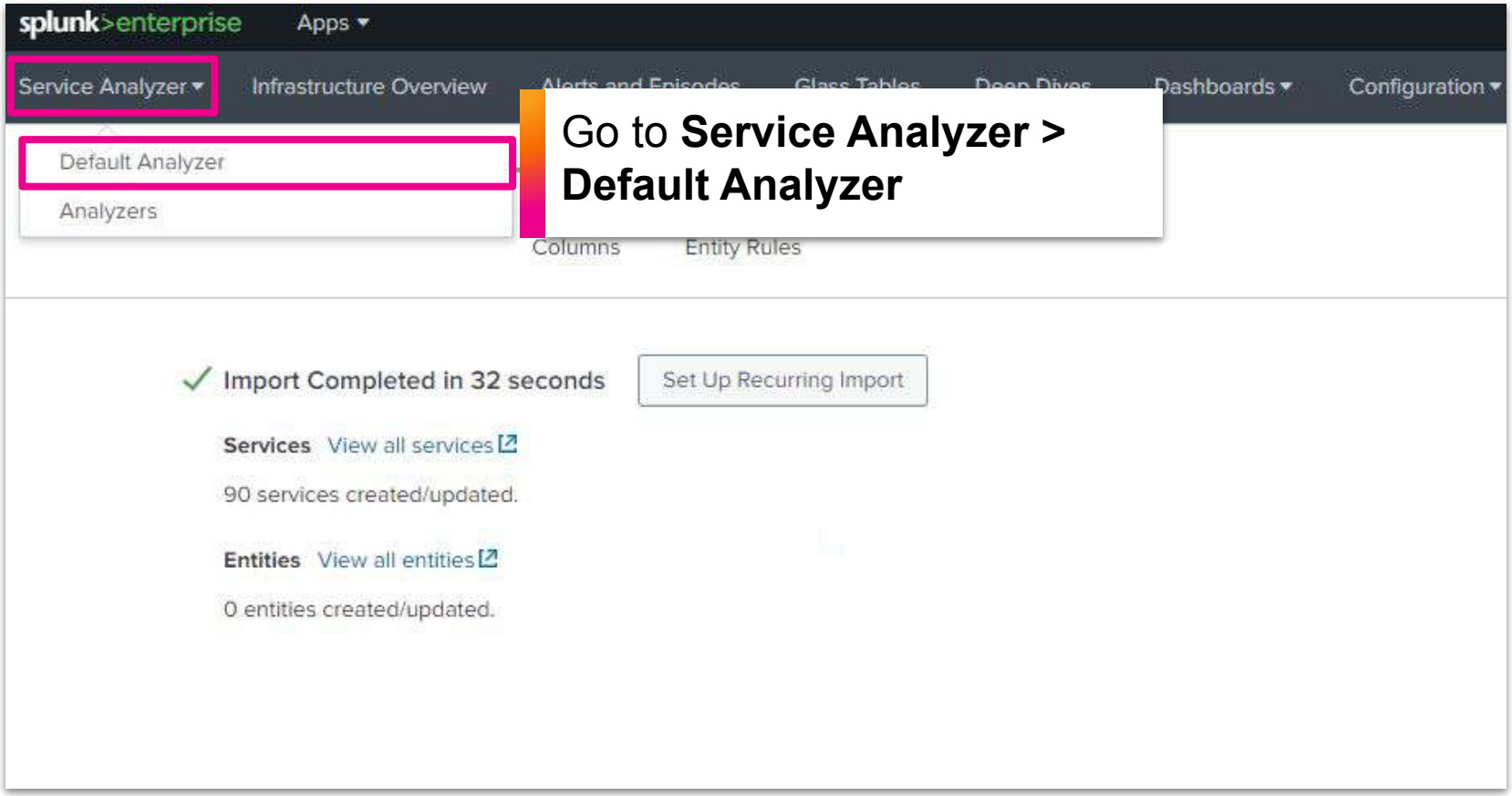
## Specify entity filtering rules




Add a name to the scheduled task and click on **Submit**

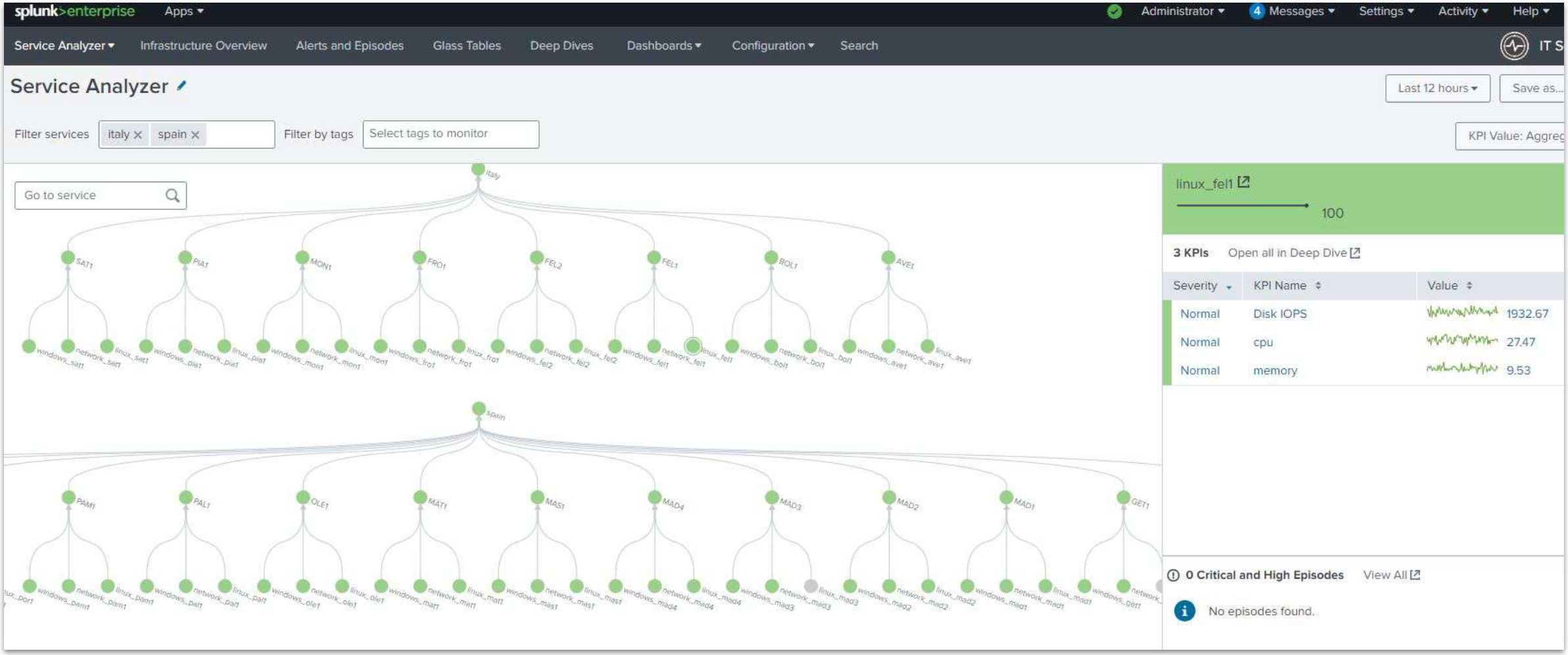
# You're All Done!

## Now time to check the Service Analyzer




Go to **Service Analyzer > Default Analyzer**

# Great Job! Now Let’s Discuss…



# Thank You!