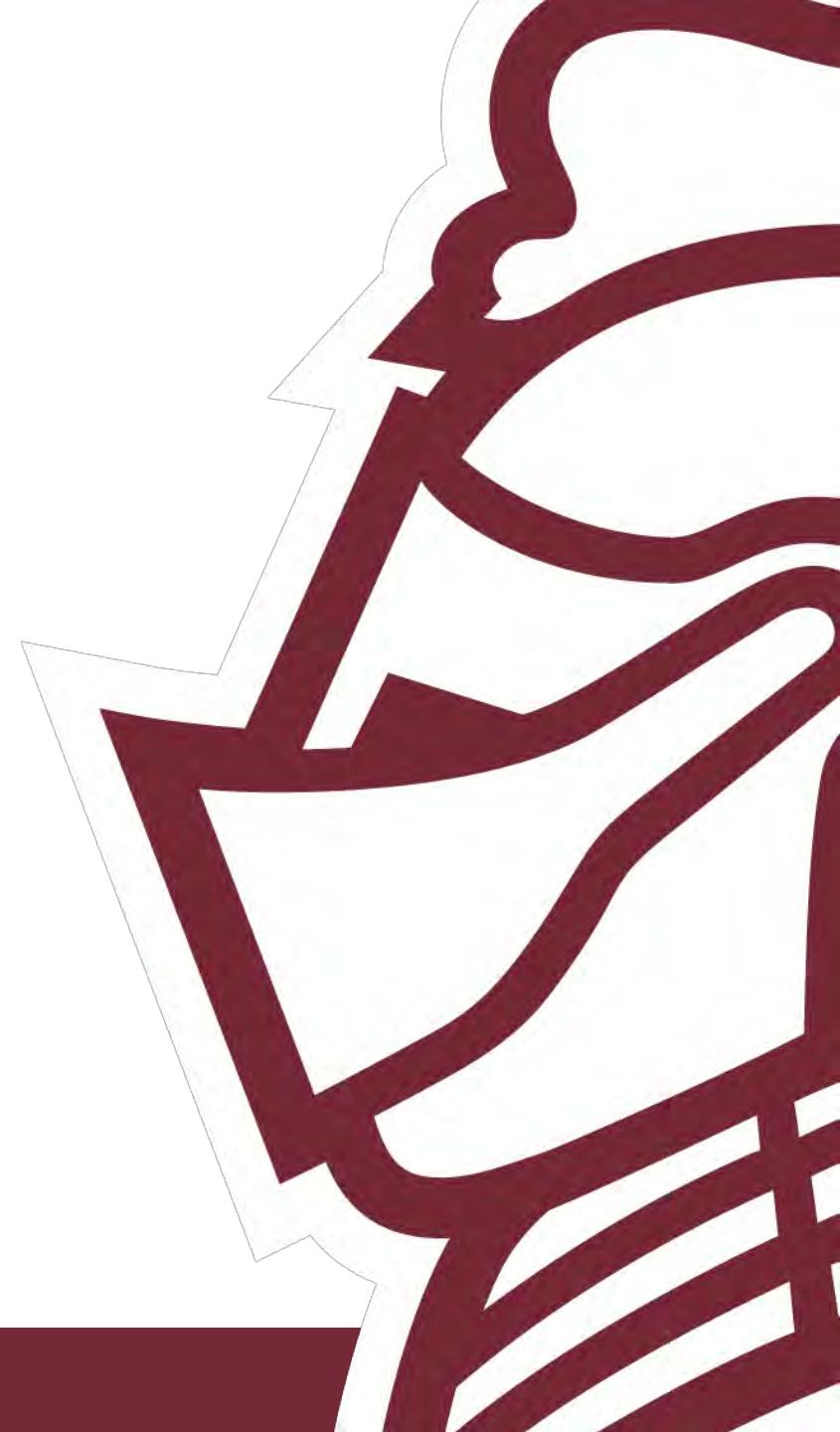


Building Your IT Toolbox



Who Am I?



- Tony Morrow
 - <https://lookanotherblog.com>
- Principal Solutions Architect @ Bellarmine University
- 16 years working at Bellarmine
- Focus
 - Networking
 - Wireless
 - Servers/Virtualization
 - Systems Integration
 - Problem Solving
 - PowerShell, PowerShell, PowerShell

Topics



- Who Am I?
- What is *Free*?
- Asset Inventory with Netbox
- System Monitoring with Zabbix
- Logging with Elastic
- Other tools

Disclaimer



- I am not a Microsoft MVP or Partner
- All technologies showcased are using free, trial, or paid licenses
- All the opinions here are my own

*Free (not that *free*, but also that *free*)*



- What do I mean by *free*?
 - Free to run the software however you want
 - Free to make changes to the software
 - Free to share the software and any changes
- It doesn't necessarily mean the software is \$0
- But also, yes, there is no cost to use the software
 - Because it is licensed under an open source license
 - Netbox: Apache 2.0 (<https://github.com/netbox-community/netbox?tab=Apache-2.0-1-ov-file#readme>)
 - Zabbix: AGPLv3 (<https://www.zabbix.com/license>)
 - Elastic*: AGPLv3/Elastic License 2.0 (<https://www.elastic.co/pricing/faq/licensing>) *it's complicated
 - Most developers provide compiled versions of the software making them easier to run

And also *Free*



- You are responsible for the
 - care
 - feeding
 - cleaning up the poop on the carpet

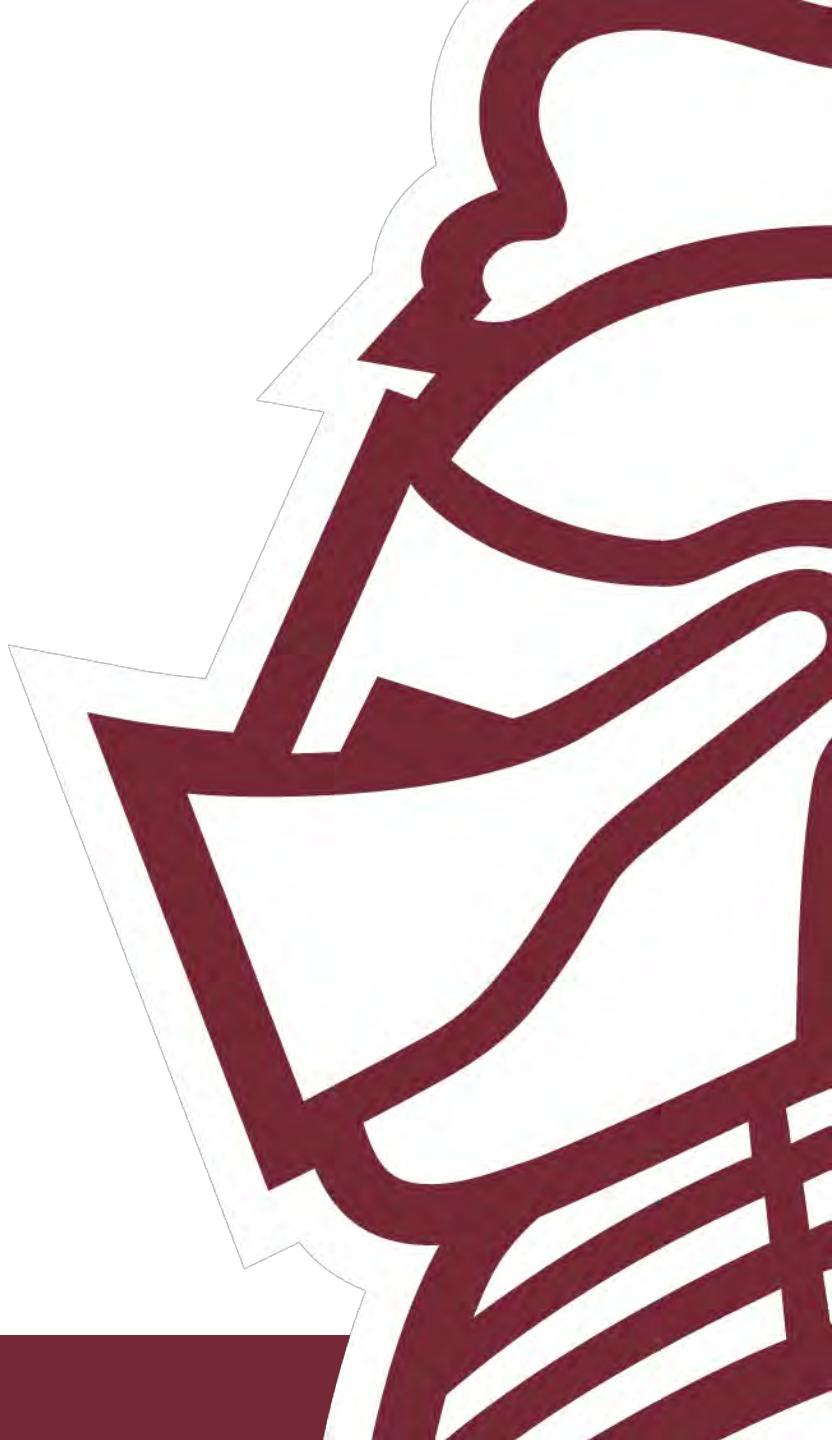


MakeAGIF.com

Asset Inventory with Netbox

Community Edition

<https://github.com/netbox-community/netbox>



Old Method: Spreadsheets



- Issues:
 - Multiple people couldn't edit at once
 - Didn't capture all the device information
 - Couldn't tell us what was connected to what

IP Addresses.xls - Read-Only - Compatibility Mode

Home Insert Draw Page Layout Formulas Data Review View Automate Help Power Pivot

Font Alignment Number Styles

Clipboard

Subnet Mask Default Gateway

Bellarmine University Computer Network Information

Address	Serial #	Equipment	Location	Sub_Location	H/W	F/W
1						
2	Master Node Cluster Project	Dr. Mahmood's Cluster Node (8307)	Pasteur Hall	P209 - Physics Lab		
3						
4	SG33FLZXXX	MSM760 Controller	BLA-17	Data Center	00:00:00:00:00:00	
5	GOLDBB	Virtual				
6	SG33FLZXXX	HP 2920-48G-POE+ Switch(J9729A)	Allen Hall	IDF, 2nd Floor, New Wing	00:00:00:00:00:00	
7	SG33FLZXXX	HP 2920-48G-POE+ Switch(J9729A)	Allen Hall	IDF, 3rd Floor, New Wing	00:00:00:00:00:00	
8	SG33FLZXXX	HP 2920-48G-POE+ Switch(J9729A)	Allen Hall	IDF, 4th Floor, New Wing	00:00:00:00:00:00	
9						
10						
11						
12						
13	GOLDTRANS	HP Proliant Server	Horigan Hall	CSGOLD, TRANSACTION Sever		
14	SG33FLZXXX	ProCurve Switch 2810-24G (J9021A)	BOB	1st Floor Switch Closet	N.11.06, ROM N.10.01	00:00:00:00:00:00
15						
16						
17						
18						
19						
20	diebold - follet	Diebold	Horigan Hall	Bookstore		
21	Crestron Docking Station	Creston Docking Station	Library	level 2 - Fraizer Board Room		
22	Crestron Control Processor	Crestron Control Processor	Library	level 2 - Fraizer Board Room		
23	Polycom Soundstructure DSP	Polycom Soundstructure DSP	Library	level 2 - Fraizer Board Room		
24	SG33FLZXXX	ProCurve Switch 2510-48 (J9020a)	Horigan Hall	Business Office, Ceiling	U.11.08, ROM R.10.06	00:00:00:00:00:00
25						
26	SG33FLZXXX	ProCurve 2610-24-PWR	Siena Quarto	Siena 2nd Floor, BDF in Boiler Room		
27	SG33FLZXXX	HP 2530-48G-PoEP Switch(J9772A)	SC-215	SC-215	YA.15.10.0003, ROM YA.15.00:00:00:00:00:00	
28						
29	SG33FLZXXX	ProCurve Switch 2610-24/12PWR (J9086A)	Newman Hall	Boiler Room	R.11.30, ROM R.10.06	
30						
31	Crestron Touch Panel	Creston Touch Panel	Library	level 2 - Fraizer Board Room		
32	Crestron Wireless Access Point	Creston Wireless AP	Library	level 2 - Fraizer Board Room		
33						
34	SG33FLZXXX	ProCurve Switch 2510-48 (J9020a)	IOS	BL-B20	U.11.08, ROM R.10.06	00:00:00:00:00:00
35						
36	SG33FLZXXX	ProCurve Switch 2610-24-PWR (J9087A)				
37						



New Method: Netbox

- What is Netbox? <https://netboxlabs.com/>
 - The “source of truth” for your infrastructure and datacenter
 - Device inventory
 - Hardware type
 - Serial number
 - Asset Tag
 - Components
 - IP Management
 - Prefixes
 - ASNs
 - VLANs
 - Connections
 - Patch panels
 - Cables
 - Connections between devices
 - Racks
 - Hardware U space

- What Netbox is not or doesn't do?

- Not a replacement for monitoring or logging
- Doesn't scan the network for devices*
- Doesn't automatically update device information or connections*

*Netbox Labs has announced new tools as part of their paid cloud offerings

Netbox Devices



Community

Organization

Racks

Devices

DEVICES

- Devices
- Modules
- Device Roles
- Platforms
- Virtual Chassis
- Virtual Device Contexts

DEVICE TYPES

- Device Types
- Module Types
- Module Type Profiles
- Manufacturers

DEVICE COMPONENTS

- Interfaces
- Front Ports
- Rear Ports
- Console Ports
- Console Server Ports
- Power Ports
- Power Outlets
- Module Bays

Search...

Devices 47 Filters 2

Role: Access Switch Manufacturer: Dell Clear all Save

Quick search

Showing 1-47 of 47 Per Page

ID	NAME	SERIAL NUMBER	ASSET TAG	STATUS	MAC ADDRESS	IP ADDRESS	SITE	LOCATION	RACK	ROLE	MANUFACTURER	TYPE	BATTERY CHANGE DATE
471	ALLN251-N2048P-01			Active		10.1.0.199/16	Allen Hall	ALLN251	—	Access Switch	Dell	PowerSwitch N2048P	—
473	ALLN353-N2048P-01			Active		10.1.0.239/16	Allen Hall	ALLN353	—	Access Switch	Dell	PowerSwitch N2048P	—
472	ALLN400D-04-N2048P			Active		10.1.0.237/16	Allen Hall	ALLN400D	—	Access Switch	Dell	PowerSwitch N2048P	—
163	Baseball-Pressbox-N2024P	—		Active		10.1.0.179/16	Baseball Press Box	—	—	Access Switch	Dell	PowerSwitch N2024P	—
347	CNCH067-Stack N2048P (01)			Active		10.1.0.17/16	Centro, McGowan Hall	CNMH067	—	Access Switch	Dell	PowerSwitch N2048P	—
348	CNCH067-Stack N2048P (02)			Active	—		Centro, McGowan Hall	CNMH067	—	Access Switch	Dell	PowerSwitch N2048P	—
345	CNCHBDF-01 N4032F			Active		10.1.0.15/16	Centro, McGowan Hall	BDF	—	Access Switch	Dell	PowerSwitch N4032F	—

+ Add Import Export

Netbox: Device Details



netbox Community

Search...

Devices / Allen Hall

ALLN251-N2048P-01

Created 2025-01-13 17:45 - Updated 2025-01-13 17:52

+ Add Components · Bookmarks · Subscribe · Clone · Edit · Delete

Organization · Racks · Devices

Devices · Modules · Device Roles · Platforms · Virtual Chassis · Virtual Device Contexts

Device Types · Device Types · Module Types · Module Type Profiles · Manufacturers

Device Components · Interfaces · Front Ports · Rear Ports · Console Ports · Console Server Ports · Power Ports · Power Outlets · Module Bays

Device · Interfaces · Console Ports · Power Ports · Config Context · Render Config · Contacts · Images · Journal · Changelog

Device

Region —

Site Allen Hall

Location ALLN251

Rack —

Position —

GPS Coordinates —

Tenant —

Device Type Dell PowerSwitch N2048P (1U)

Description —

Airflow Front to rear

Serial Number —

Asset Tag —

Config Template —

Custom Fields

Management

Mac Address ●

Purchasing

Purchase Date 2019-05-15

Tags

No tags assigned

Comments

No comments

Virtual Device Contexts

+ Create VDC

NAME	IDENTIFIER	STATUS	TENANT	IP ADDRESS
— No virtual device contexts found —				

Management

Status Active

Role Access Switch

Platform —

Primary IPv4 10.1.0.199

Primary IPv6 —

Out-of-band IP —

Application Services

+ Add an application service

NAME PARENT PROTOCOL PORTS DESCRIPTION

— No application services found —

Images

+ Attach an image

IMAGE OBJECT DESCRIPTION DIMENSIONS SIZE

— No image attachments found —

Dimensions

Height 1.0U

Weight —

dcim.device

amorozov@belarmine Admin

2026-01-07 19:57:50 UTC - netbox

netbox Community

Search...

Devices / Allen Hall

ALLN251-N2048P-01

Created 2025-01-13 17:45 Updated 2025-01-13 17:52

+ Add Components • Bookmark Subscribe Edit Delete

Organization

Racks

Devices

DEVICES

Devices

Modules

Device Roles

Platforms

Virtual Chassis

Virtual Device Contexts

DEVICE TYPES

Device Types

Module Types

Module Type Profiles

Manufacturers

DEVICE COMPONENTS

Interfaces

Front Ports

Rear Ports

Console Ports

Console Server Ports

Power Ports

Power Outlets

Module Bays

Device Interfaces (29) Console Ports (1) Power Ports (1) Config Context Render Config Contacts Images Journal Changelog

Quick search

Showing 1-52 of 52

Per Page

Name	Label	Enabled	Type	Parent	Lag	MTU	Mode	Description	IP Addresses	Cable	Connection	POE Type	Actions
Gi1/0/1		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/2		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/3		✓	1000BASE-T (IGE)	—	—	—	—	#1471 ALLN-2-AP02	> LAN1	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/4		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/5		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/6		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/7		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/8		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/9		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/10		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/11		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/12		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/13		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/14		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/15		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/16		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/17		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/18		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/19		✓	1000BASE-T (IGE)	—	—	—	—	#1472 ALLN-2-AP01	> LAN1	—	—	—	View Edit Details Clone Revert Delete
Gi1/0/20		✓	1000BASE-T (IGE)	—	—	—	—	—	—	—	—	—	View Edit Details Clone Revert Delete

Netbox: IP Management



netbox Community

Organization, Rocks, Devices, Connections, Wireless, IPAM, IP Addresses, IP Ranges, Prefixes, ASNs, ASN Ranges, ASNs, Aggregates, Aggregates, RIRs, VRFs, VRFs, Route Targets, VLANs.

Prefixes

Results 772 of 772

Quick search

Showing 1-72 of 72

Prefix	Gateway	Status	Children	Utilization	VLAN	Description
4.37.114.176/29	4.37.114.177/29	Active	0	33.3%	Lumen INET (106)	Lumen INET
10.1.0.16	10.1.0.254/16	Active	3	0.4%	Private (2)	—
10.1.0.0/24	—	Active	0	0.0%	—	Network Management
10.1.5.0.0/24	—	Active	0	0.0%	—	Printers: Departments
10.1.5.3.0/24	—	Active	0	20.3%	—	UPS
10.10.0.0/16	—	Active	2	0.2%	Public (3)	Public
10.10.50.0/24	—	Active	0	0.0%	—	Printers: Public
10.10.53.0/24	—	Active	0	20.3%	—	Nursing Simlab Hardware
10.20.0.0/16	10.20.0.254/16	Active	2	0.0%	Dorm (4)	Dorm
10.20.0.0/23	—	Active	0	36.2%	—	APs: Residence Halls
10.20.50.0/23	—	Active	0	71.1%	—	APs: Residence Halls Hospitality
10.30.0.0/16	10.30.0.254/16	Active	1	0.4%	Wireless (5)	—
10.30.0.0/23	—	Active	0	54.5%	—	APs: Campus
10.70.0.0/16	10.70.0.254/16	Active	0	0.0%	CARS (6)	—
10.90.0.0/16	10.90.0.254/16	Active	1	0.1%	Server (8)	Server
10.90.0.0/23	—	Active	0	14.7%	—	—
10.100.11.0/24	—	Active	0	3.1%	Replication (11)	—
10.100.13.0/24	—	Active	0	3.6%	iSCSI (13)	—
10.100.14.0/24	10.100.14.254/24	Active	0	20.1%	DC-Mgmt (14)	—
10.100.16.0/24	—	Active	0	14.2%	iSCSI (16)	—
10.100.17.224/30	10.100.17.224/30	Active	0	100.0%	CoLo-Tunnel (17)	—

netbox Community

Organization, Racks, Devices, Connections, Wireless, IPAM, IP Addresses, IP Ranges, Prefixes, Prefix & VLAN Roles, ASNs, ASN Ranges, ASNs, Aggregates, Aggregates, RIRs, VRFs, VRFs, Route Targets, VLANs.

Prefixes

10.1.0.0/24

Created 2025-01-30 15:02 - Updated 2025-01-30 15:02

Prefix Child Prefixes Child Ranges IP Addresses (172) Contacts Journal Changelog

Quick search

Showing 1-223 of 223

IP ADDRESS	VRF	STATUS	ASSIGNED	DNS NAME	DESCRIPTION	PARENT
2 IP available	Global	Available	—	—	—	—
1 IP available	Global	Available	—	—	—	SCCMS
10.1.0.3/16	Global	Active	✓	—	—	—
10.1.0.5/16	Global	Active	✓	—	—	BUGGOLDB
10.1.0.6/16	Global	Active	✓	—	—	Alien3-01-HP2920-48G-POE
10.1.0.7/16	Global	Active	✓	—	—	Alien3-01-HP2920-48G-POE
10.1.0.8/16	Global	Active	✓	—	—	Alien4-01-HP2920-48G-POE
10.1.0.9/16	Global	Active	✓	—	—	CNMH180-01-SG300-10MPP
1 IP available	Global	Available	—	—	—	—
10.1.0.11/16	Global	Active	✓	—	—	CNMH176-01-SG300-10PP
10.1.0.12/16	Global	Active	✓	—	—	CNMH170-01-SG300-10PP
10.1.0.13/16	Global	Active	✓	—	—	BUGGOLTRANS
10.1.0.14/16	Global	Active	✓	—	—	MDF-2810-24
10.1.0.15/16	Global	Active	✓	—	—	CNCHBDF-01-N4032F (A16817)
10.1.0.16/16	Global	Active	✓	—	—	CNCHBDF-02-N2048F (A16818)
10.1.0.17/16	Global	Active	✓	—	—	CNCHBDF-Stack N2048F (01) (A16819)
10.1.0.18/16	Global	Active	✓	—	—	CNTH225B-01-N2048F (A17587)
10.1.0.19/16	Global	Active	✓	—	—	CNMH163-Stack DellN2048F (01)
10.1.0.20/24	Global	Active	—	—	BookStore Prox Reader	—
10.1.0.21/16	Global	Active	✓	—	—	MDF-ISP-S5212F-ON (A20613)
10.1.0.22/24	Global	Active	✓	—	—	BDF-ISP-S5212F-ON (A20614)
10.1.0.23/16	Global	Active	✓	—	—	WallOfFire1-PA3440 (A20611)
10.1.0.24/16	Global	Active	✓	—	—	WallOfFire2-PA3440 (A20612)

Netbox: Racks

Community

Search...

Racks / Datacenter - Primary

Rack Server Rack 02

Created 2025-01-23 17:51 Updated 2025-01-23 17:51

dcim.rack.5

Server Rack 02 Bookmark Subscribe Clone Edit Delete

RACK TYPES

Rack Types

Devices

Connections

Wireless

IPAM

VPN

Virtualization

Circuits

Power

Provisioning

Customization

Operations

RACKS

Racks

Rack Roles

Reservations

Elevations

RACK TYPES

Rack Types

Devices

Connections

Wireless

IPAM

VPN

Virtualization

Circuits

Power

Provisioning

Customization

Operations

Front

Region

Site Datacenter - Primary

Location

Tenant

Status Active

Rack Type

Role

Description

Serial Number

Asset Tag

Airflow

Space Utilization 50%

Power Utilization 0.00

Dimensions

Form factor

Width 19 inches

Height 42U

Outer Width

Outer Height

Outer Depth

Mounting Depth

Numbering

Starting Unit 1

Descending Units X

Weight

Rack Weight

Maximum Weight

Total Weight 88.2 Kilograms (194.4 Pounds)

Related Objects

Devices

Front

42

41

40

39

38

37

36

35

34

33

32

31

30

29

28

27

26

25

24

23

22

21

20

19

18

17

16

15

14

13

12

11

10

9

8

7

6

5

4

3

2

1

Download SVG

Rear

42

41

40

39

38

37

36

35

34

33

32

31

30

29

28

27

26

25

24

23

22

21

20

19

18

17

16

15

14

13

12

11

10

9

8

7

6

5

4

3

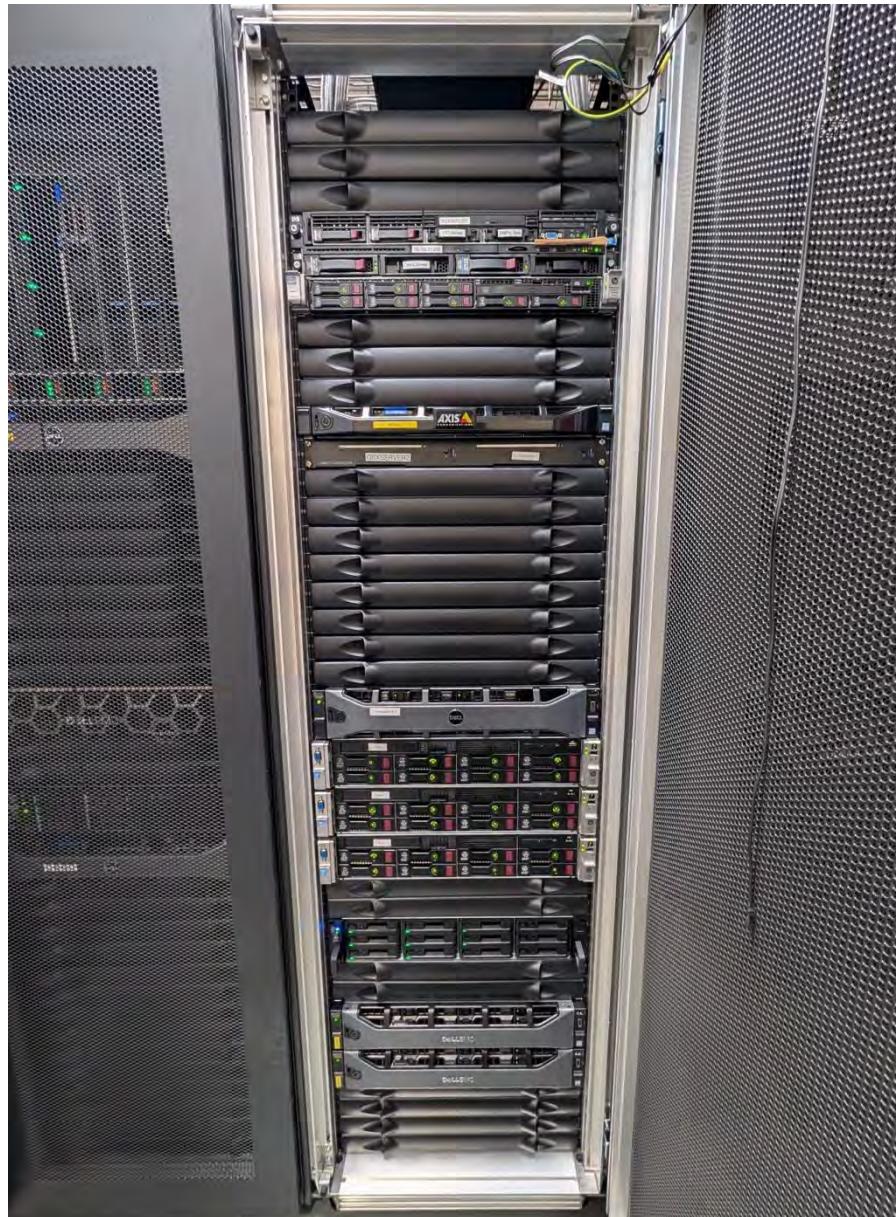
2

1

Download SVG

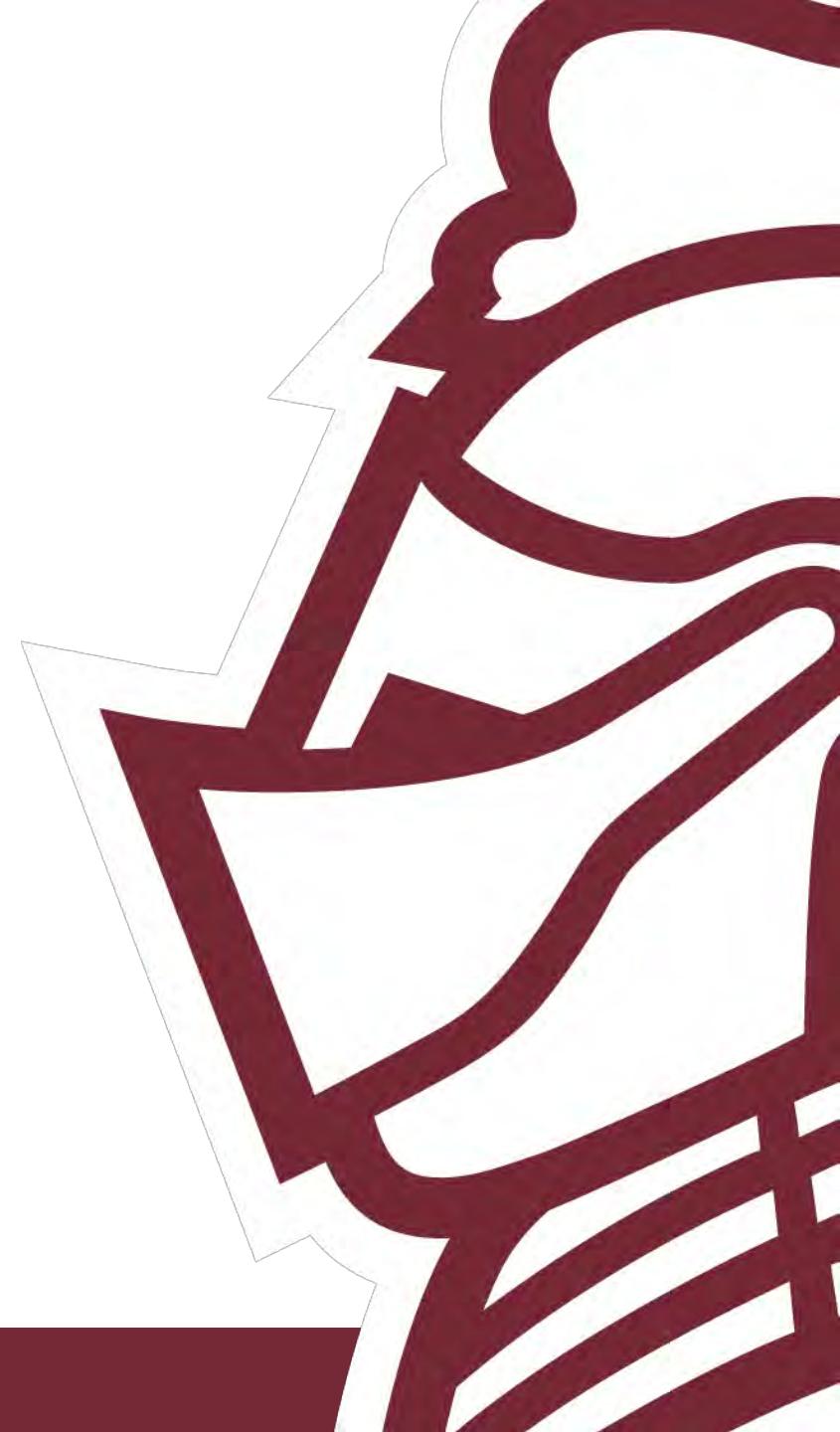
amorrow@bellarmine.edu Admin

2025-01-09 17:08:16 UTC netbox



Network/Service Monitoring with Zabbix

<https://www.zabbix.com/>



What is Zabbix?



- Monitoring and Alerting
- What can you monitor?
 - Network stuff
 - Server stuff
 - DB stuff
 - Cloud stuff
 - VM stuff
 - Application stuff

Zabbix Problems Monitoring



ZABBIX

zabbix

Dashboards

Monitoring

Problems

Hosts

Latest data

Maps

Discovery

Services

Inventory

Reports

Data collection

Alerts

Users

Problems

Export to CSV

Zoom out

Last 1 day

Time ▾

Severity

Recovery time

Status

Info

Host

Problem

Duration

Update

Actions

Tags

Time	Severity	Status	Info	Host	Problem	Duration	Update	Actions	Tags
11:09:11 AM	Warning	PROBLEM		dc-libr-mx740c-05-iDRAC	CPU2 Temp: Temperature is above warning threshold: >70	8m 2s	Update		[Application: Temperature]
11:00									
10:54:09 AM	Warning	PROBLEM		dc-libr-mx740c-02-iDRAC	CPU2 Temp: Temperature is above warning threshold: >70	23m 4s	Update		[Application: Temperature]
Today									
2026-01-24 09:54:08 AM	Warning	PROBLEM		DC Liebert	Device Status: Normal with Warning on DC Liebert	4d 1h 23m	Update		[Application: Status]
2026									
2025-12-13 09:14:50 PM	Warning	PROBLEM		SP106-02 2610-48-PWR	Interface 32(): In half-duplex mode	1M 15d 14h	Update		[Application: Interface 32()]
December									
2025-11-25 01:03:15 PM	Average	PROBLEM		DC-LIBR-Fortigate90G-01	FortiGate: Port 443 is unavailable	2M 3d 22h	Update		[class: network component: health component: network ...]
2025-11-14 03:06:37 AM	Warning	PROBLEM		VEEAMPROXY1	E:: Disk space is low (used > 85%)	2M 15d 8h	Update		[Application: Filesystem E::]
November									
2025-08-19 01:32:41 PM	Warning	PROBLEM		ST123-Stack-ICX8200	Interface ethernet 2/1/250(): In half-duplex mode	5M 11d 22h	Update		[Application: Interface ethernet 2/1/250]
August									
2025-07-20 01:17:11 AM	Warning	PROBLEM		Alien4-01-HP2920-48G-POEP	Interface 9(): In half-duplex mode	6M 12d 11h	Update		[Application: Interface 9()]

Displaying 8 of 8 found

Zabbix System Information



ZABBIX

zabbix

System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Zabbix server version	7.4.6	Up to date
Zabbix frontend version	7.4.6	Up to date
Software update last checked	2026-01-28	
Latest release	7.4.6	Release notes
Number of hosts (enabled/disabled)	1513	1182 / 331
Number of templates	254	
Number of items (enabled/disabled/not supported)	173155	108323 / 64646 / 186
Number of triggers (enabled/disabled [problem/ok])	89639	31495 / 58144 [16 / 31479]
Number of users (online)	9	2
Required server performance, new values per second	811.85	
Global scripts on Zabbix server	Disabled	
High availability cluster	Disabled	

Dashboards

Monitoring

Services

Inventory

Reports

System information

Scheduled reports

Availability report

Top 100 triggers

Audit log

Action log

Notifications

Zabbix Hosts Lists



ZABBIX

zabbix

Hosts

Host Wizard Create host Import Filter

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
3408Newburg-01 2610-48-PWR	531	Triggers 266	Graphs 52	Discovery 1	Web	10.1.0.125:10050		Bellarmino Network Generic Device SNMP (Bellarmino Interfaces SNMP, Generic SNMP)	Enabled	ZBX	SNMP	None	
3408Newburg-02 2620-48-PWR	531	Triggers 266	Graphs 52	Discovery 1	Web	10.1.0.189:10050		Bellarmino Network Generic Device SNMP (Bellarmino Interfaces SNMP, Generic SNMP)	Enabled	ZBX	SNMP	None	
3408Newburg-1-UPS1.bellarmino.edu	30	Triggers 8	Graphs 2	Discovery 4	Web	10.1.53.93:10050	ZabbixProxy1	Bellarmino Template Eaton UPS (Generic SNMP)	Enabled	ZBX	SNMP	None	
3408Newburg-1-UPS2.bellarmino.edu	30	Triggers 8	Graphs 2	Discovery 4	Web	10.1.53.94:10050	ZabbixProxy1	Bellarmino Template Eaton UPS (Generic SNMP)	Enabled	ZBX	SNMP	None	
3408NewburgTest 2610-48-PWR	531	Triggers 266	Graphs 52	Discovery 1	Web	10.1.0.105:10050		Bellarmino Network Generic Device SNMP (Bellarmino Interfaces SNMP, Generic SNMP)	Disabled	ZBX	SNMP	None	
ACMECHALLENGE	103	Triggers 72	Graphs 11	Discovery 4	Web	10.100.19.30:10050		Bellarmino Windows by Zabbix agent (Windows CPU by Zabbix agent, Windows filesystems by Zabbix agent, Windows generic by Zabbix agent, Windows memory by Zabbix agent, Windows network by Zabbix agent, Windows physical disks by Zabbix agent, Windows services by Zabbix agent, Zabbix agent)	Enabled	ZBX	PSK	None PSK CERT	
AL-109-01 2610-48PWR	541	Triggers 271	Graphs 53	Discovery 1	Web	10.1.0.194:10050		Bellarmino Network Generic Device SNMP (Bellarmino Interfaces SNMP, Generic SNMP)	Enabled	ZBX	SNMP	None	
ALERTUS	122	Triggers 85	Graphs 16	Discovery 4	Web	10.100.20.46:10050		Bellarmino Windows by Zabbix agent (Windows CPU by Zabbix agent, Windows filesystems by Zabbix agent, Windows generic by Zabbix agent, Windows memory by Zabbix agent, Windows network by Zabbix agent, Windows physical disks by Zabbix agent, Windows services by Zabbix agent, Zabbix agent)	Disabled	ZBX	PSK	None PSK CERT	
Allen-Bridge	3	Triggers 3	Graphs	Discovery	Web	10.30.0.253:10050		ICMP Ping	Enabled	ZBX	SNMP	None	
Allen2-01-HP2920-48G-POE	501	Triggers 251	Graphs 49	Discovery 1	Web	10.1.0.6:10050		Bellarmino Network Generic Device SNMP (Bellarmino Interfaces SNMP, Generic SNMP)	Enabled	ZBX	SNMP	None	
Allen3-01-HP2920-48G-POE	501	Triggers 251	Graphs 40	Discovery 1	Web	10.1.0.7:10050		Bellarmino Network Generic Device SNMP (Bellarmino Interfaces SNMP, Generic SNMP)	Enabled	ZBX	SNMP	None	
Allen4-01-HP2920-48G-POEP	501	Triggers 251	Graphs 49	Discovery 1	Web	10.1.0.8:10050		Bellarmino Network Generic Device SNMP (Bellarmino Interfaces SNMP, Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP01_old	11	Triggers 6	Graphs	Discovery	Web	10.30.1.182:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP02	11	Triggers 6	Graphs	Discovery	Web	10.30.1.183:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP03	11	Triggers 6	Graphs	Discovery	Web	10.30.1.184:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP04	11	Triggers 6	Graphs	Discovery	Web	10.30.1.185:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP05	11	Triggers 6	Graphs	Discovery	Web	10.30.1.186:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP06	11	Triggers 6	Graphs	Discovery	Web	10.30.1.187:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP07	11	Triggers 6	Graphs	Discovery	Web	10.30.1.188:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-AP08	11	Triggers 6	Graphs	Discovery	Web	10.30.1.189:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-1-UPS1.bellarmino.edu	30	Triggers 8	Graphs 2	Discovery 4	Web	10.1.53.104:10050	ZabbixProxy1	Bellarmino Template Eaton UPS (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-2-AP01	11	Triggers 6	Graphs	Discovery	Web	10.30.1.190:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	
ALLN-2-AP02	11	Triggers 6	Graphs	Discovery	Web	10.30.1.191:10050		Bellarmino Wireless Generic Device SNMP (Generic SNMP)	Enabled	ZBX	SNMP	None	

Templates (<https://www.zabbix.com/integrations>)



Screenshot of the Zabbix web interface showing the 'Templates' list page.

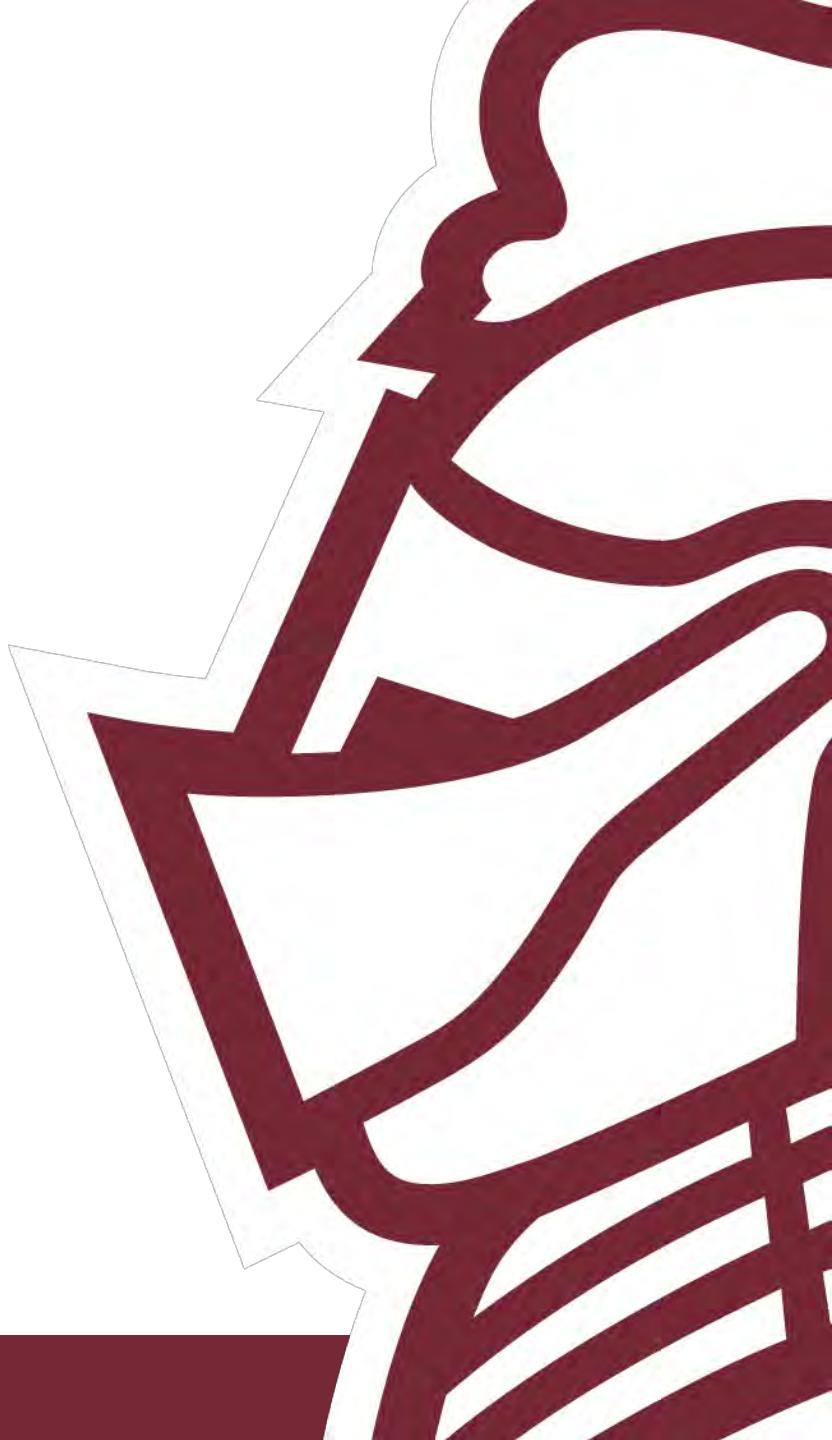
The left sidebar shows navigation links: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Template groups, Host groups, **Templates** (selected), Hosts, Maintenance, Event correlation, and Discovery.

The main content area is titled 'Templates' and displays a table of template entries. The columns are: Name, Hosts, Items, Triggers, Graphs, Dashboards, Discovery, Web, Vendor, Version, Linked templates, and Tags.

Name	Hosts	Items	Triggers	Graphs	Dashboards	Discovery	Web	Vendor	Version	Linked templates	Tags
AIX	Hosts	Items 43	Triggers 10	Graphs 4	Dashboards 1	Discovery 2	Web	Zabbix agent			
Alcatel Timetra TIMOS SNMP	Hosts	Items 18	Triggers 9	Graphs 3	Dashboards	Discovery 6	Web			EtherLike-MIB SNMP, Generic SNMP, Interfaces SNMP	
Apache ActiveMQ by JMX	Hosts	Items	Triggers	Graphs	Dashboards	Discovery 2	Web				
Apache by HTTP	Hosts	Items 22	Triggers 5	Graphs 3	Dashboards 1	Discovery 1	Web				
Apache by Zabbix agent	Hosts	Items 26	Triggers 6	Graphs 4	Dashboards 1	Discovery 1	Web				
Apache Cassandra by JMX	Hosts	Items 67	Triggers 6	Graphs 7	Dashboards	Discovery 1	Web				
Apache Kafka by JMX	Hosts	Items 62	Triggers 11	Graphs 9	Dashboards	Discovery 3	Web				
Apache Tomcat JMX	Hosts	Items 1	Triggers 1	Graphs	Dashboards	Discovery 4	Web				
APC Smart-UPS 2200 RM SNMP	Hosts	Items 25	Triggers 22	Graphs 3	Dashboards	Discovery 6	Web				
APC Smart-UPS 3000 XLM SNMP	Hosts	Items 25	Triggers 22	Graphs 3	Dashboards	Discovery 6	Web				
APC Smart-UPS RT 1000 RM XL SNMP	Hosts	Items 25	Triggers 22	Graphs 3	Dashboards	Discovery 6	Web				
APC Smart-UPS RT 1000 XL SNMP	Hosts	Items 25	Triggers 22	Graphs 3	Dashboards	Discovery 6	Web				
APC Smart-UPS SRT 5000 SNMP	Hosts	Items 25	Triggers 22	Graphs 3	Dashboards	Discovery 6	Web				
APC Smart-UPS SRT 5000 SNMP bkp	Hosts	Items 25	Triggers 22	Graphs 3	Dashboards	Discovery 6	Web				

Logging with Elastic Stack

<https://www.elastic.co>



What is Elastic Stack



- Centralized logging system for **EVERYTHING**
 - Syslog
 - File based logs
 - API based monitoring
 - Windows Event Logs
 - Audit monitoring
 - Metrics monitoring
- Data analytics and visualizations
- Act as a SIEM

Elastic Discovery Search



elastic

Find apps, content, and more.

Discover Network: Switch Logs

Untitled • +

Data view Logstash 8 Network

tags: switch NOT message: Ignore logs from Orion logons: Warning

Search field names 0

Selected fields 2

- host.ip
- message

Popular fields 2

- message
- host.ip

Available fields 21

- @timestamp
- @version
- component
- event.original
- filename
- host.ip
- line_number
- log.syslog.facility.code
- log.syslog.facility.name
- log.syslog.severity.code
- log.syslog.severity.name
- message

Auto interval No breakdown

February 27, 2025 05:15 05:30 05:45 06:00 06:15 06:30 06:45 07:00 07:15 07:30 08:00 08:15 08:30 08:45 09:00 09:15 09:30 09:45 10:00 10:15 10:30 10:45 11:00

Feb 27, 2025 @ 05:07:56.117 - Feb 27, 2025 @ 13:53:19.633 (Interval: Auto - 10 minutes)

Documents (8) Field statistics

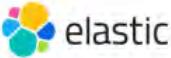
host.ip	message
10.1.0.29	<12> Feb 27 07:21:52 10.1.0.29 loop -protect: port 1 disabled - loop detected.
10.1.0.29	<14> Feb 27 07:21:52 10.1.0.29 ports: Loop Protect(64) has disabled port 1 for 300 seconds
10.1.0.29	<14> Feb 27 06:56:56 10.1.0.29 ports: Loop Protect(64) has disabled port 1 for 300 seconds
10.1.0.29	<12> Feb 27 06:56:56 10.1.0.29 loop -protect: port 1 disabled - loop detected.
10.1.0.29	<14> Feb 27 06:14:01 10.1.0.29 ports: Loop Protect(64) has disabled port 1 for 300 seconds



Elastic's Beats Data Shippers (<https://www.elastic.co/beat>)

+ New Forrester Wave Leader, Q2 2025 [Access report](#)

About us Partners Support ⚙ EN ⚙ Login

 Elasticsearch Solutions Enterprise Resources Docs Pricing

Search Start free trial Contact sales

All kinds of shippers for all kinds of data.

 Filebeat Lightweight shipper for logs and other data →	 Metricbeat Lightweight shipper for metric data →	 Packetbeat Lightweight shipper for network data →	 Winlogbeat Lightweight shipper for Windows event logs →
 Auditbeat Lightweight shipper for audit data →	 Heartbeat Lightweight shipper for uptime monitoring →		

Elastic Cluster Stats



Screenshot of the Elastic Stack interface showing cluster statistics for the ELK2 cluster.

Elasticsearch Overview:

- Health:** Healthy
- Version:** 9.2.4
- Uptime:** 5 days
- License:** Basic

Nodes: 3

- Disk Available:** 33.46% (13.6 TB / 40.6 TB)
- JVM Heap:** 41.60% (38.7 GB / 93.0 GB)

Indices: 880

- Documents:** 19,210,566,573
- Disk Usage:** 25.0 TB
- Primary Shards:** 880
- Replica Shards:** 880

Logs: No logs for Elasticsearch. Follow these directions to set up Elasticsearch.

Kibana Overview:

- Requests:** 3
- Max. Response Time:** 73 ms
- Rule Success Ratio:** 100.00%
- Queued Rules:** 4

Logstash Overview:

- Events Received:** 60.7k
- Events Emitted:** 40.4k

Logstash Nodes: 1

- Uptime:** 26 minutes
- JVM Heap:** 66.34% (679.4 MB / 1,024.0 MB)

Logstash Pipelines: 1

- With Memory Queues:** 1
- With Persistent Queues:** 0

Beats Overview:

- Total Events:** 5.8m
- Bytes Sent:** 1.5 GB

Beats: 6

- Filebeat:** 3
- Metricbeat:** 3



Other Tools

- NetDisco: <https://netdisco.org/>
 - Scan your network and find where and how devices are connected
- RANCID/Oxidized: <https://shrubbery.net/rancid/> <https://github.com/ytti/oxidized>
 - Backup your network hardware configurations
- LibreNMS: <https://www.librenms.org/>
 - Network monitoring system
- Nautobot: <https://docs.nautobot.com/projects/core/en/stable/>
 - Fork of Netbox that adds Ansible automation
- Uyuni: <https://www.uyuni-project.org/>
 - OS/package/patch/config management for Linux systems
- OpenSearch: <https://opensearch.org/>
 - Amazon's fork of Elastic (*it's complicated)