

NEW RELEASE



NetEye

16. Juni 2020 by Georg Kostner


- UNIFIED MONITORING - MONITORING – VISIBILITY - OBSERVABILITY

UNIFIED MONITORING
AVAILABILITY
SERVICE LEVEL MANAGEMENT



- ◆ Unified Monitoring
- ◆ Business Service Monitoring
- ◆ Distributed – IoT – IIoT Monitoring
- ◆ Datacenter Shutdown Module
- ◆ Asset Management
- ◆ Visual Synthetic Monitoring Alyvix
- ◆ Web Automation Monitoring

IT OPERATION ANALYTICS
APM
END2END




- ◆ Real User Experience
- ◆ User Experience
- ◆ IT Operation Analytics
- ◆ Application Performance Management
- ◆ Anomaly Detection
- ◆ Forecasting - Prediction
- ◆ Machine Learning

GDPR – SECURITY
LOG MGMT
SIEM



- ◆ Log Management
- ◆ Anomaly Detection
- ◆ SIEM
- ◆ Machine Learning

SERVICE & SUPPORT
SERVICE MANAGEMENT
TICKETING




- ◆ Jira Service Desk
- ◆ Confluence
- ◆ Ops Genie
- ◆ ITIL Consulting
- ◆ ServiceDesk


on premises – Hybrid – Cloud – Cloud SaaS

MONITORING – VISIBILITY - OBSERVABILITY

UNIFIED MONITORING
AVAILABILITY
SERVICE LEVEL MANAGEMENT




IT OPERATION ANALYTICS
APM
END2END



GDPR – SECURITY
LOG MANAGEMENT
SIEM



SERVICE & SUPPORT
SERVICE MANAGEMENT
TICKETING



strong technology partnership to drive innovation

New Feature

- New Login Picture for NetEye 4.12
- SLM report: show only related objects
- SLM Contracts should be multi tenant
- Elastic update to the latest version 7.6
- SIEM fully compatible with Elastic 7.6 X-Packs
- Improve GeoMap drilldown to host details
- Upgrade automation
- Integration of ntopng for network visibility
- Tornado Negation and String Operators
- Tornado GUI: Processing Tree Configuration
- Tornado GUI: Rule Configuration from Web
- Make Icingaweb2 Roles Tables searchable


Improvement

- Update VMWare Discovery to latest version
- Release Icinga2 2.11.3
- Add indexes to icinga tables to boost performances
- Add to the User Guide hints how to boost the performance of Elastic and NetEye 4
- Pass command name variable to scripted dashboards
- Update to latest CentOS Minor version 7.8.2003

Preview

- Problem View Filter [Technical PREVIEW]





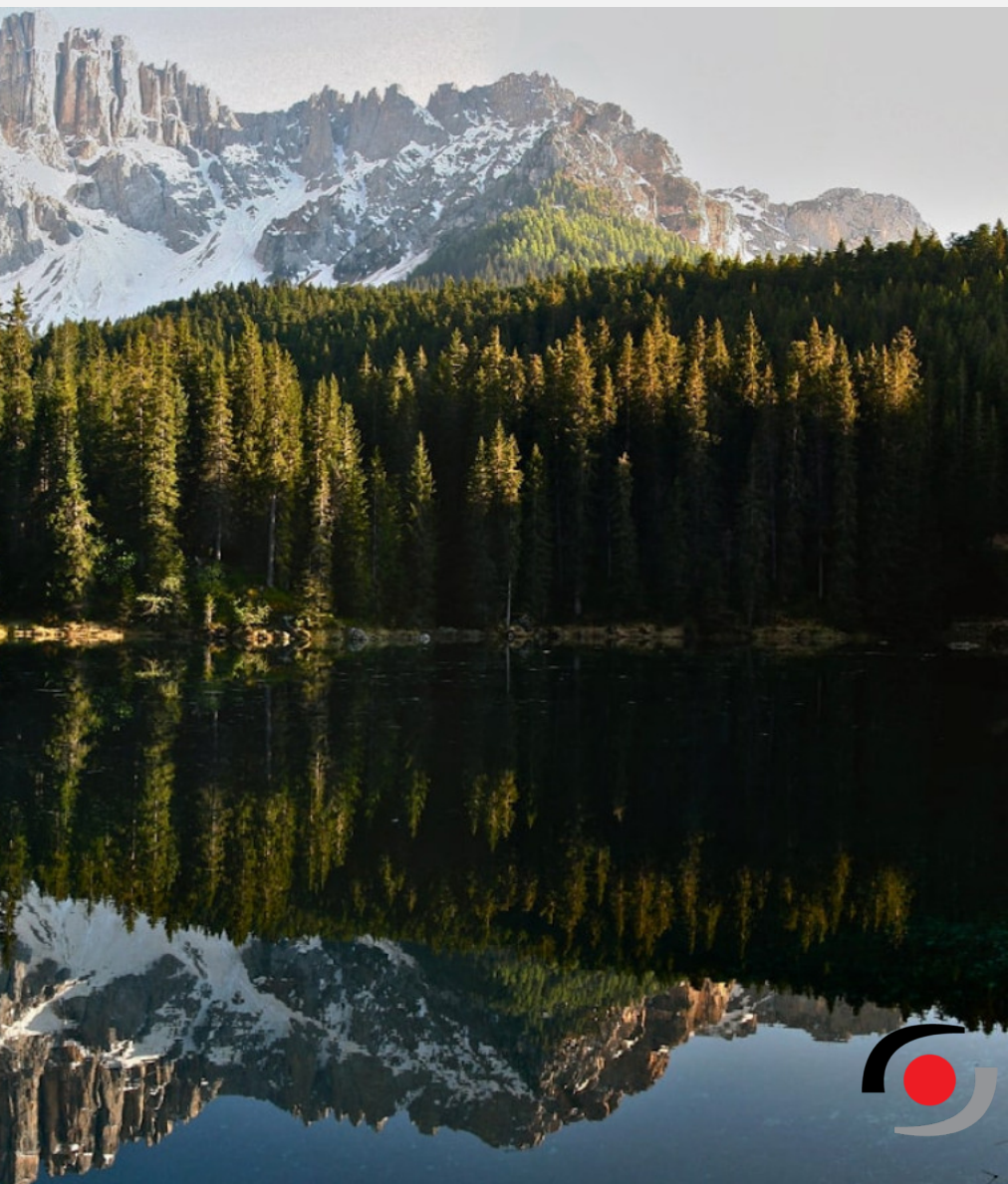
login

Username

●●●●

Password

Login





SERVICE LEVEL MANAGEMENT

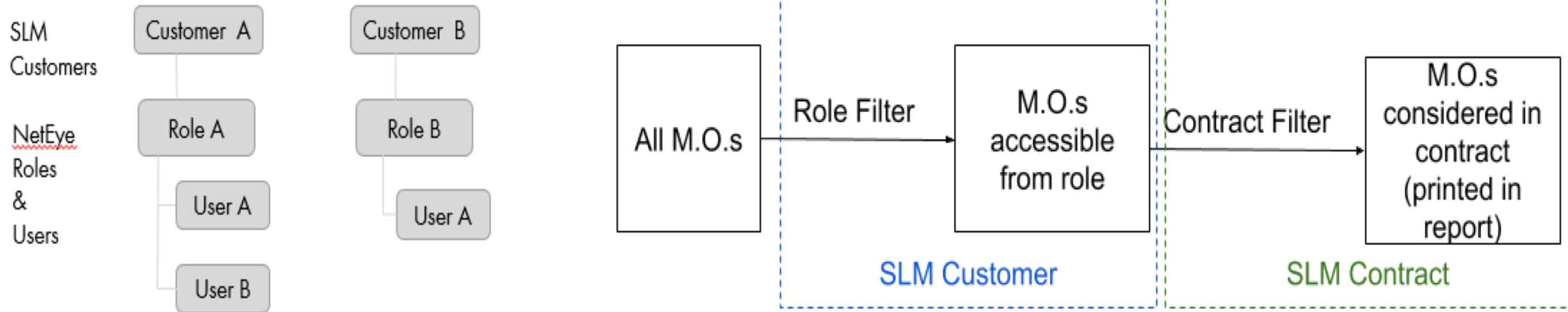


- Multi Tenancy
- SLM Report show related monitoring events

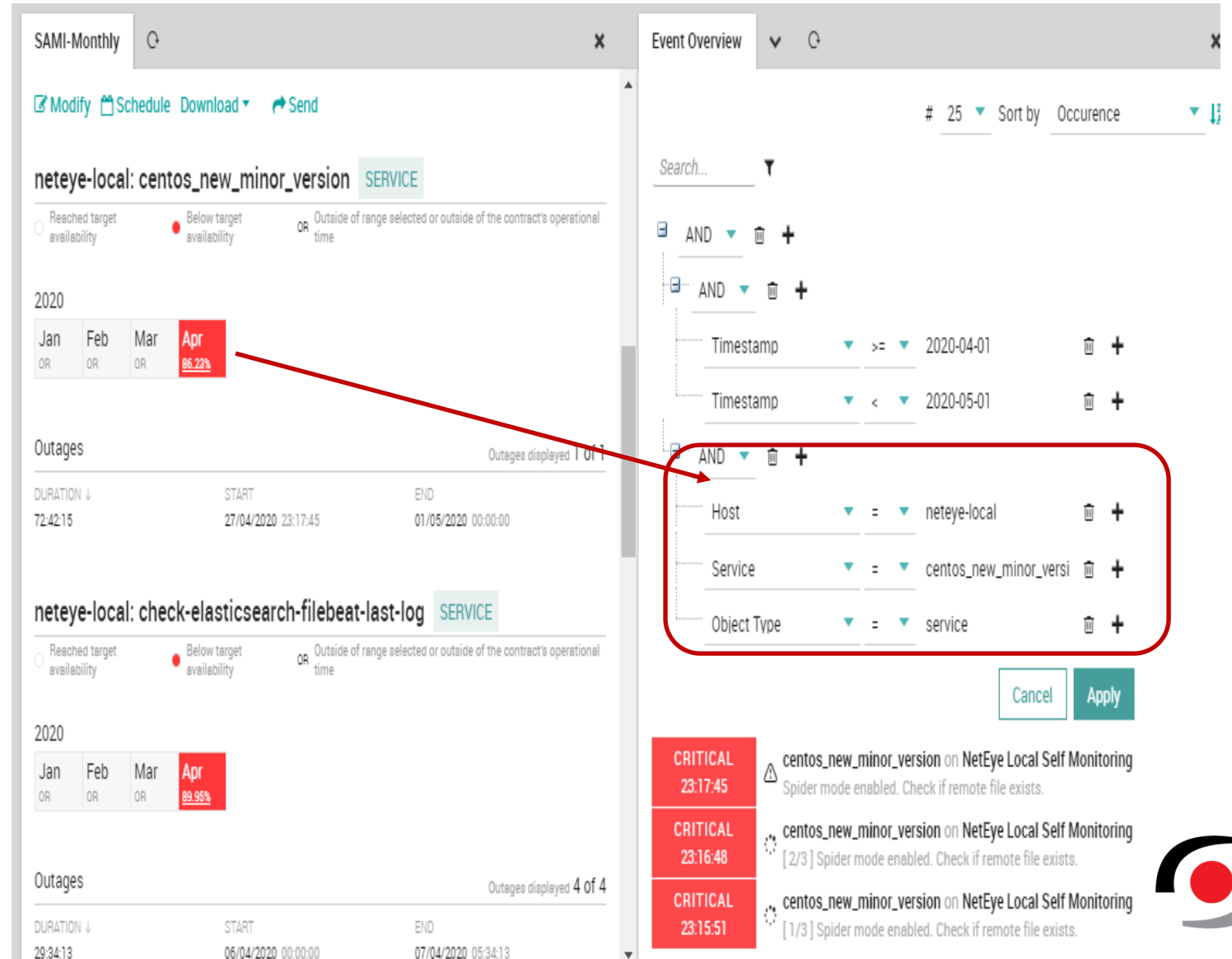


As an admin, I want that a NetEye user can see only the Monitoring Object and SLM configuration if his associated customer in SLM

- Introduced the role level restriction
 - SLM Users can view one or more SLM Customers/Contracts based on his associated roles.
 - Filtering the Monitoring Objects in Availability Contract according to the role inside the SLM.



- Show Host & Service which impacted the availability
- Help to understand the events which have generated the outage



The screenshot displays the NetEye SLM report interface. The left pane shows two availability charts for 'neteye-local: centos_new_minor_version' and 'neteye-local: check-elasticsearch-filebeat-last-log'. Both charts show a significant drop in availability in April 2020, with the first chart at 86.22% and the second at 89.95%. The right pane shows the 'Event Overview' for the first outage, with a search filter for 'Host = neteye-local', 'Service = centos_new_minor_versi', and 'Object Type = service'. A red box highlights this filter, and a red arrow points from the 'Apr' month in the chart to the filter. Below the filter, a list of critical events is shown, all related to 'Spider mode enabled' for the 'centos_new_minor_version' service.

Host	Service	Object Type
neteye-local	centos_new_minor_versi	service

CRITICAL	Event Description
23:17:45	centos_new_minor_version on NetEye Local Self Monitoring Spider mode enabled. Check if remote file exists.
23:16:48	centos_new_minor_version on NetEye Local Self Monitoring [2/3] Spider mode enabled. Check if remote file exists.
23:15:51	centos_new_minor_version on NetEye Local Self Monitoring [1/3] Spider mode enabled. Check if remote file exists.



A background image of a man in a white shirt and glasses, sitting at a desk and resting his head on his hand in a thoughtful or stressed pose. The image is overlaid with a large red diagonal shape that contains the main title.

ELASTIC STACK UPGRADE 7.6

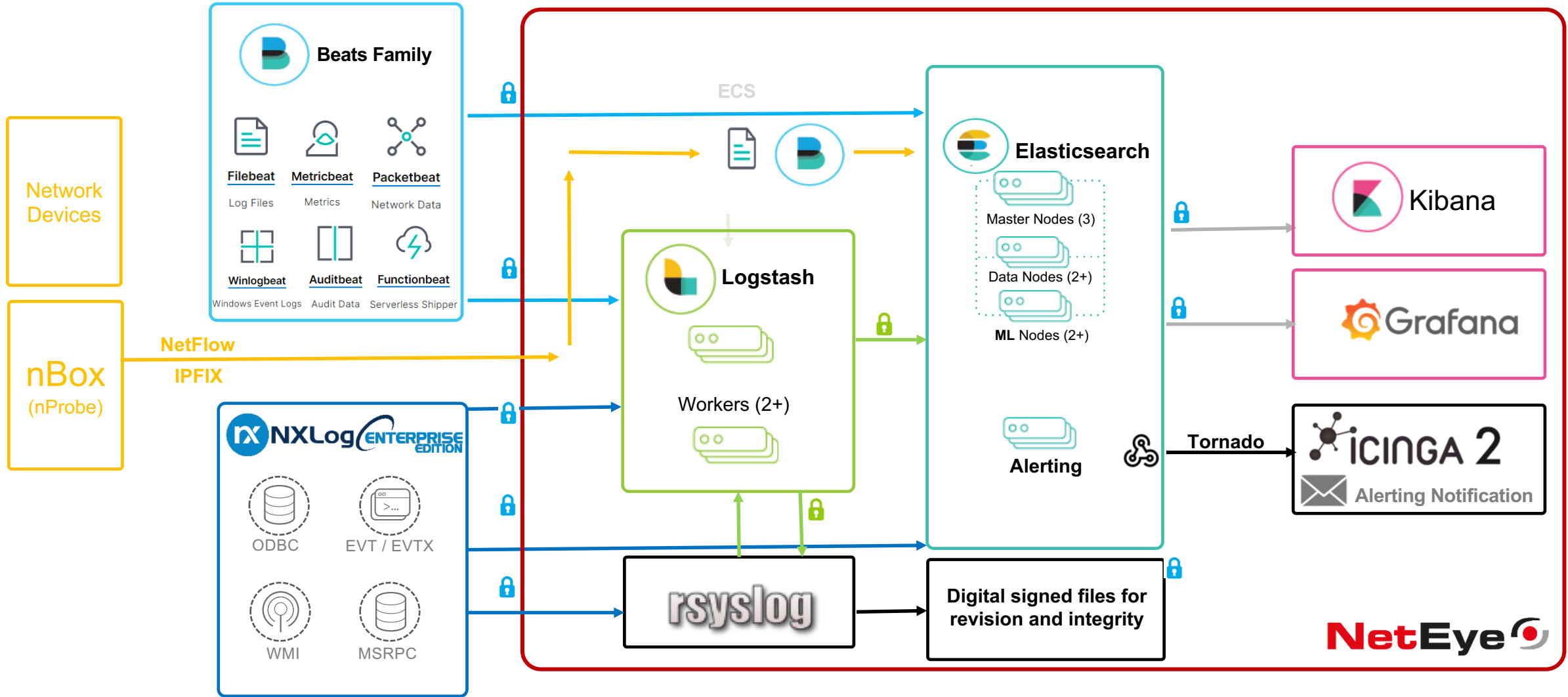


- Elastic Stack Features Platinum Subscription
- Security
- Kibana Spaces
- Kibana Reports
- Kibana Lens
- SIEM detections
- Elasticsearch data enrichment
- Elasticsearch performance improvements

Elastic Stack Features: <https://www.elastic.co/elastic-stack/features>

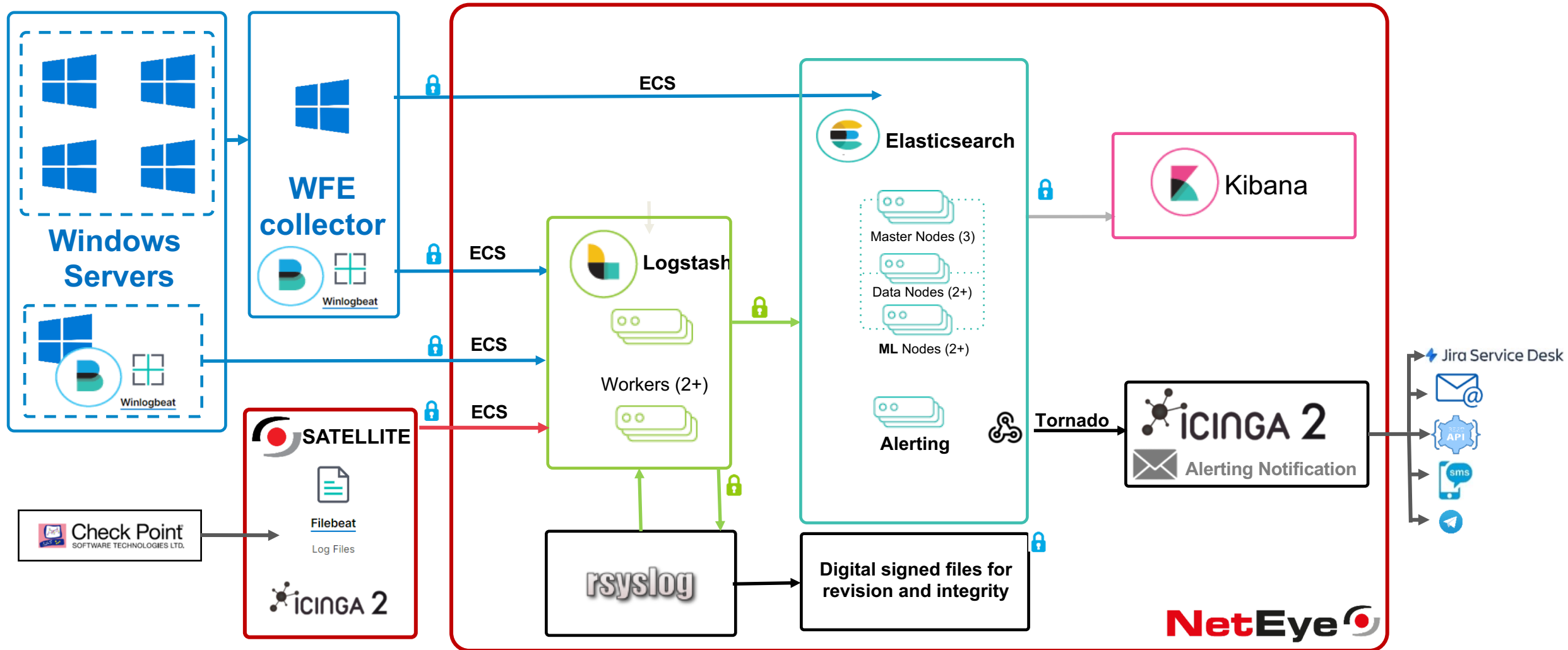


NETEYE: SIEM SOLUTION DESIGN



Agentless, with Agent (<https://nxlog.co/blog/agentless-vs-agent-based-log-collection>)

NETEYE: SIEM SOLUTION DESIGN WINDOWS ARCHITECTURE



NETEYE: SIEM SECURITY AND ELASTIC STACK FEATURES



- Encrypted Communication – Data integrity
- Role-based access control (RBAC)
- Attribute-based access control (ABAC)
- Field- and document-level security
- Audit logging
- IP filtering
- GDPR Compliance

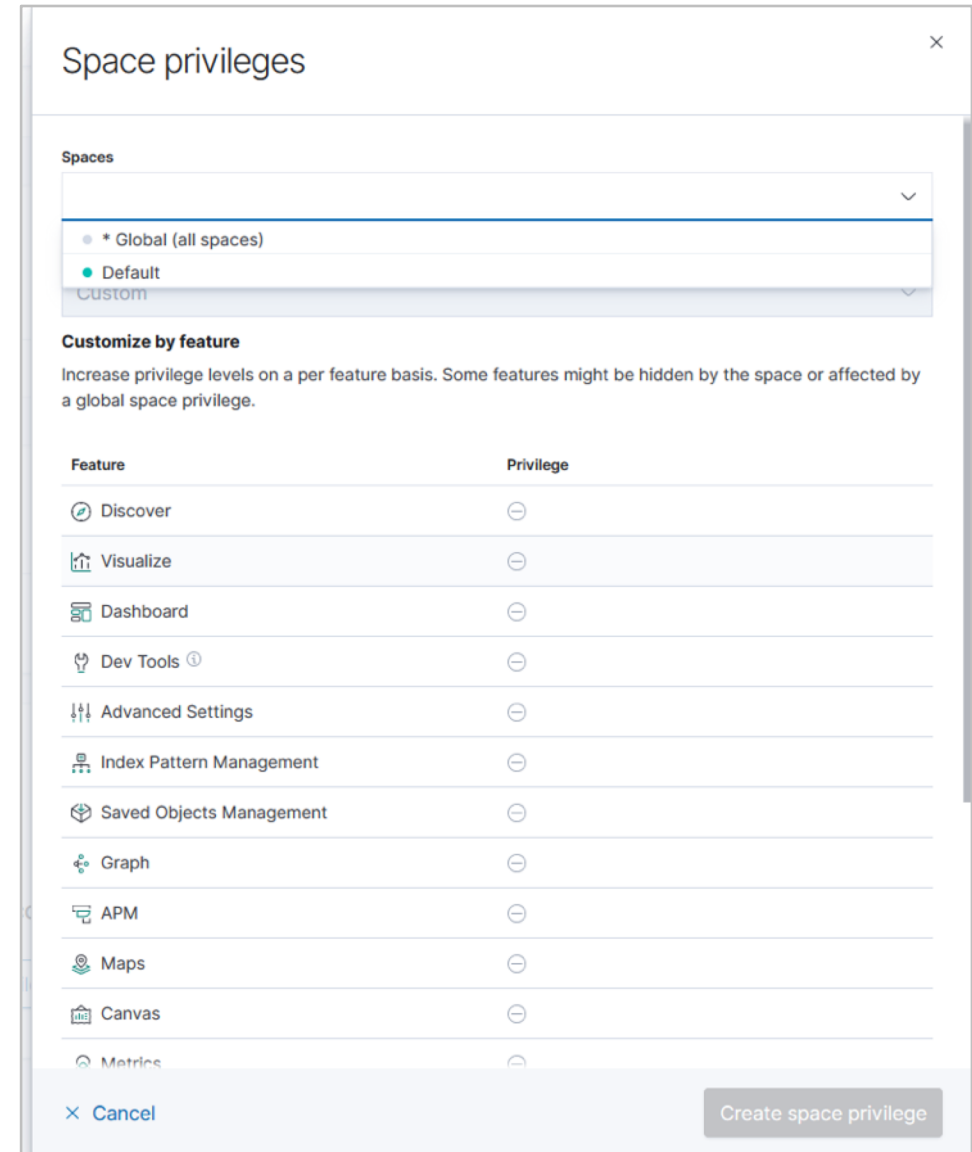
(See <https://www.elastic.co/pdf/white-paper-of-gdpr-compliance-with-elastic-and-the-elastic-stack.pdf>)

MANAGEMENT AND OPERATIONS			
SCALABILITY AND RESILIENCY	MANAGEMENT	STACK SECURITY	DEPLOYMENT
Clustering and high availability	Index lifecycle management	Secure settings	Download and install
Automatic node recovery	Hot-warm architecture	Encrypted communications	Elastic Cloud
Automatic data rebalancing	Frozen indices	Encryption at rest support	Elastic Cloud Enterprise
Horizontal scalability	Snapshot and restore	Role-based access control (RBAC)	Elastic Cloud on Kubernetes
Rack awareness	Source-only snapshots	Attribute-based access control (ABAC)	Helm Charts
Cross-cluster replication	Snapshot lifecycle management	Field- and document-level security	Docker containerization
Cross-datacenter replication	Data rollups	Audit logging	CLIENTS
	CLI tools	IP filtering	REST API
MONITORING	Upgrade Assistant UI	Security realms	Language clients
Full stack monitoring	Upgrade Assistant API	Single sign-on (SSO)	Console
Multi-stack monitoring	User and role management	Third-party security integration	Elasticsearch DSL
Configurable retention policy	Transforms	FIPS 140-2 mode	Elasticsearch SQL
Automatic alerts on stack issues		Section 508	JDBC client
	ALERTING	Standards (GDPR)	ODBC client
	Highly available, scalable alerting		
	Notifications via email, Slack, PagerDuty, or webhooks		
	Alerting UI		

Elastic Stack Features: <https://www.elastic.co/elastic-stack/features>



- Organize dashboards and other objects in categories
- Create a default space for users
- Control over which features are visible in each space
- Associate spaces to roles
- Create a custom landing page for users



Space privileges

Spaces

- * Global (all spaces)
- Default
- Custom

Customize by feature

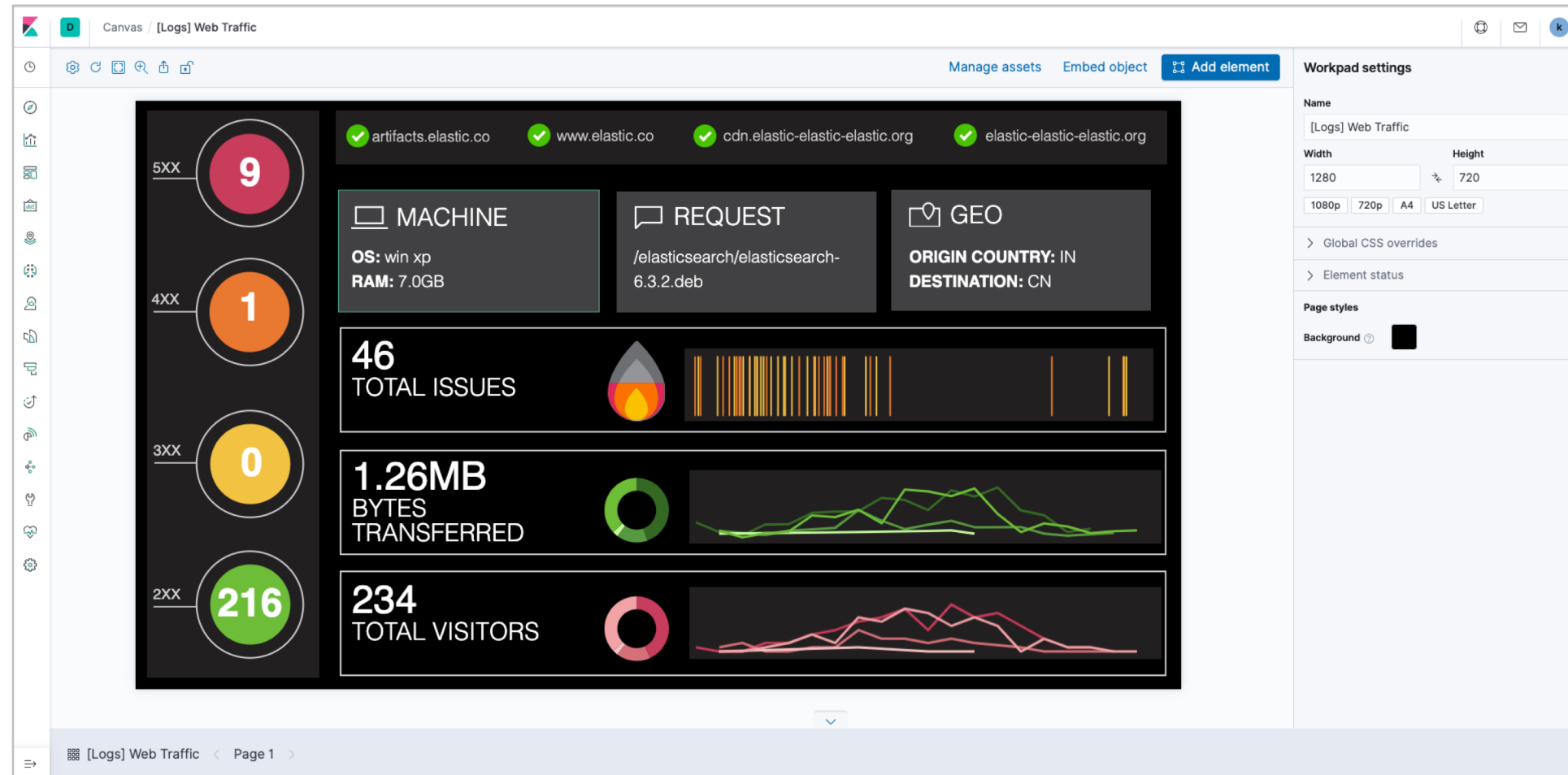
Increase privilege levels on a per feature basis. Some features might be hidden by the space or affected by a global space privilege.

Feature	Privilege
Discover	None
Visualize	None
Dashboard	None
Dev Tools	None
Advanced Settings	None
Index Pattern Management	None
Saved Objects Management	None
Graph	None
APM	None
Maps	None
Canvas	None
Metrics	None

× Cancel Create space privilege



- Personalize your workspace with colors, fonts and more
- Add text and images to visualizations
- Pull data directly from Elasticsearch
- Add filters



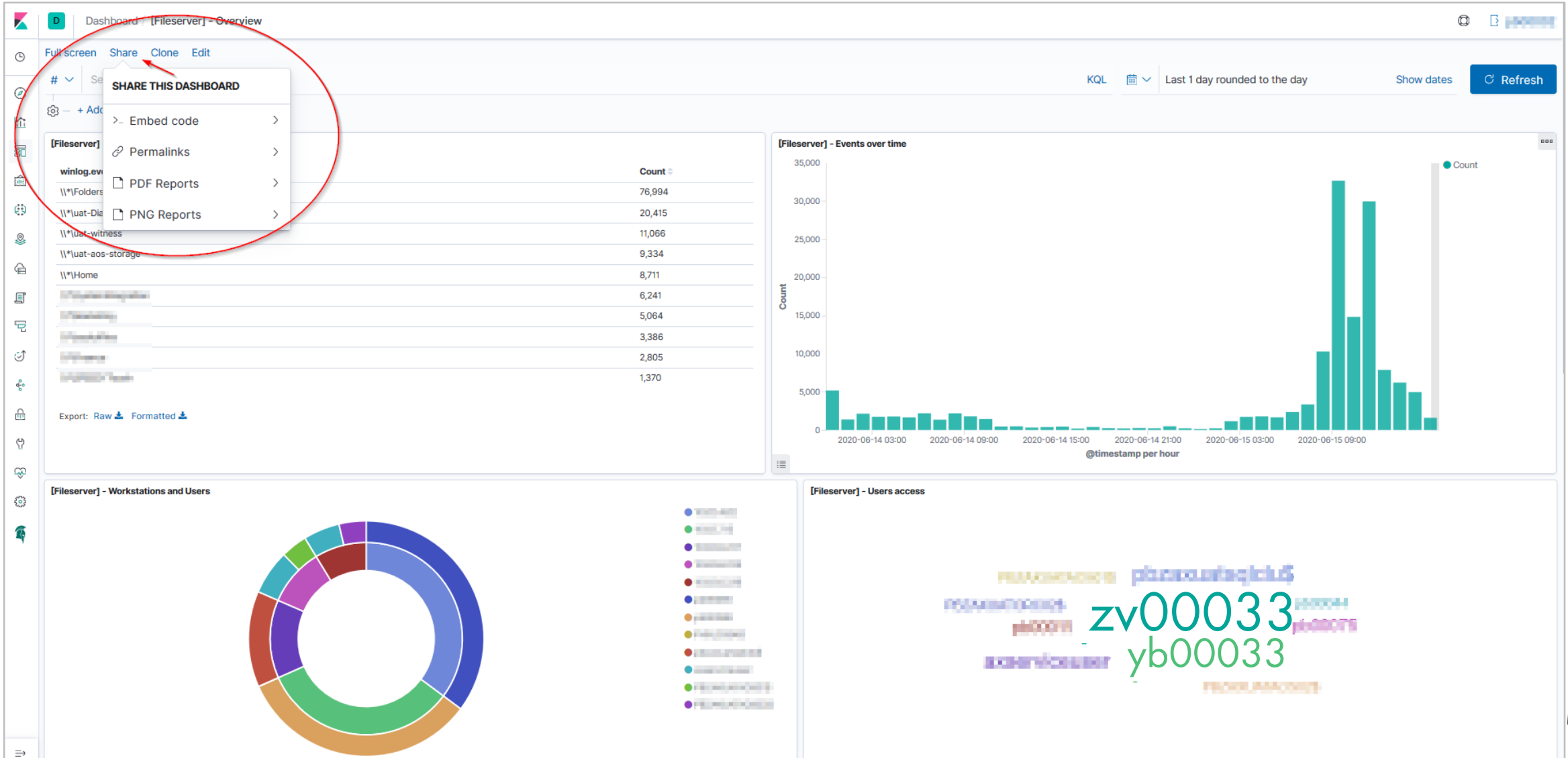
The screenshot displays the Kibana Canvas interface for a dashboard titled "[Logs] Web Traffic". The dashboard is composed of several widgets:

- 5XX:** A circular gauge showing 9 incidents.
- 4XX:** A circular gauge showing 1 incident.
- 3XX:** A circular gauge showing 0 incidents.
- 2XX:** A circular gauge showing 216 incidents.
- MACHINE:** A widget showing OS: win xp and RAM: 7.0GB.
- REQUEST:** A widget showing the path /elasticsearch/elasticsearch-6.3.2.deb.
- GEO:** A widget showing ORIGIN COUNTRY: IN and DESTINATION: CN.
- 46 TOTAL ISSUES:** A widget with a flame icon and a bar chart.
- 1.26MB BYTES TRANSFERRED:** A widget with a donut chart and a line graph.
- 234 TOTAL VISITORS:** A widget with a donut chart and a line graph.

At the top, there are four status indicators for domains: artifacts.elastic.co, www.elastic.co, cdn.elastic-elastic-elastic.org, and elastic-elastic-elastic.org, all marked with green checkmarks. The right sidebar shows "Workpad settings" for the dashboard, including Name, Width (1280), Height (720), and Page styles (Background).



NETEYE: KIBANA REPORTING



SHARE THIS DASHBOARD

- Embed code
- Permalinks
- PDF Reports
- PNG Reports

[Fileserver]	Count
winlog.ev	76,994
*\Folders	20,415
*\uat-Dia	11,066
*\uat-witness	9,334
*\uat-aos-storage	8,711
*\Home	6,241
*\uat-aos-storage	5,064
*\uat-aos-storage	3,386
*\uat-aos-storage	2,805
*\uat-aos-storage	1,370

Export: Raw Formatted

[Fileserver] - Events over time

Count

@timestamp per hour

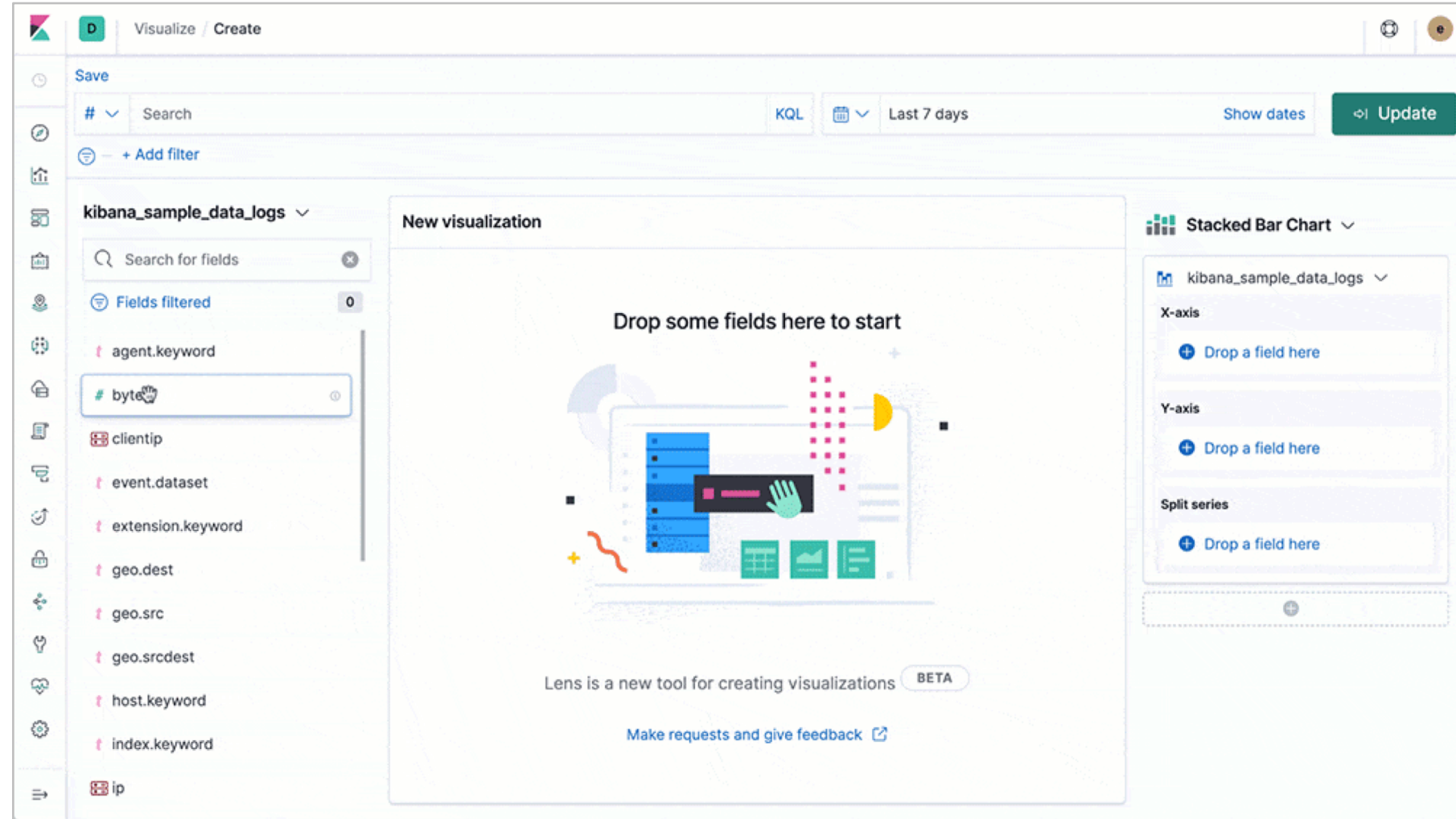
[Fileserver] - Workstations and Users

[Fileserver] - Users access

zv00033
yb00033

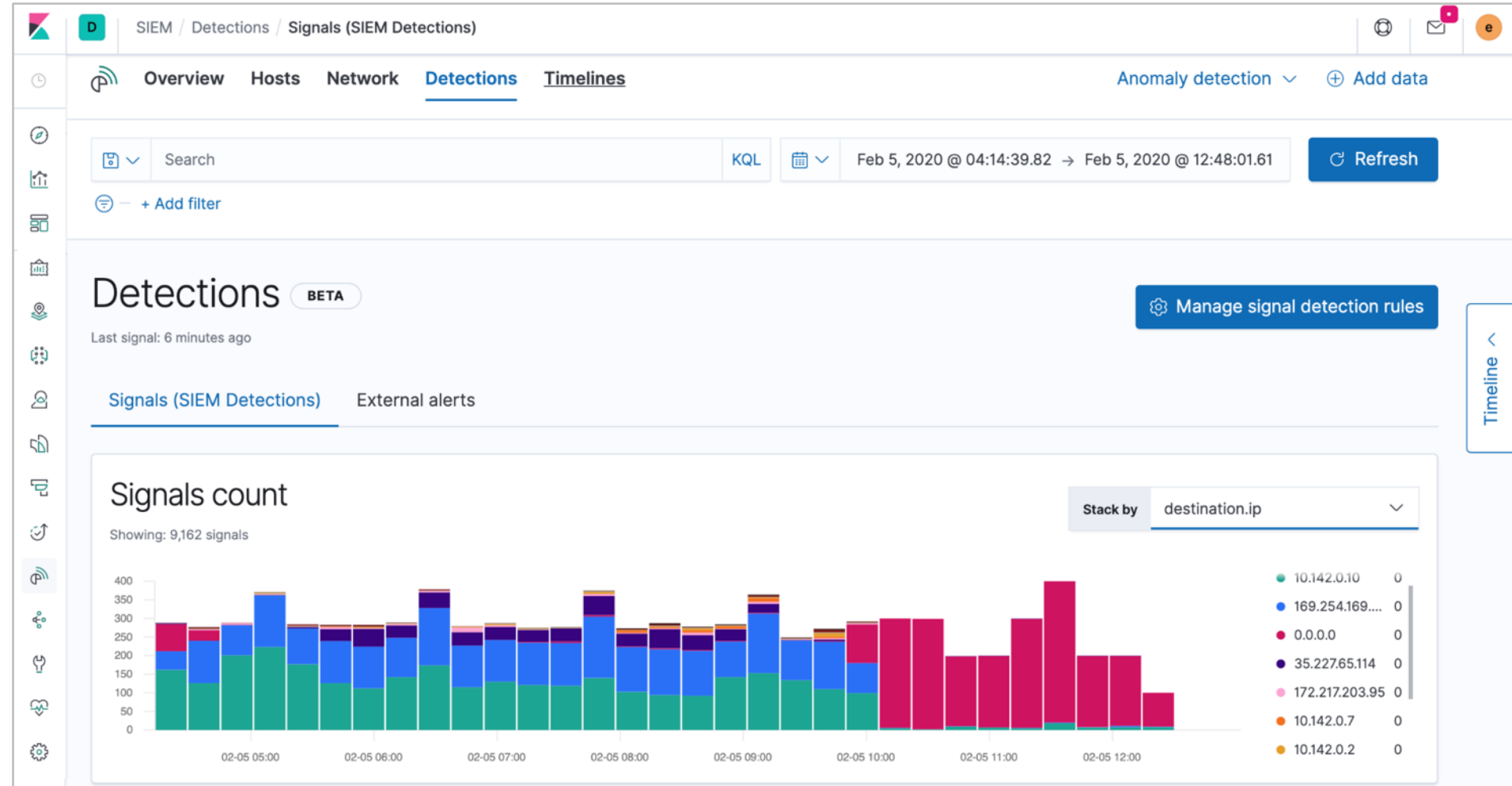


- Easily create visualizations
drag and drop from fields
- Data summaries
Preview of the data distribution
- Switch between visualization
types

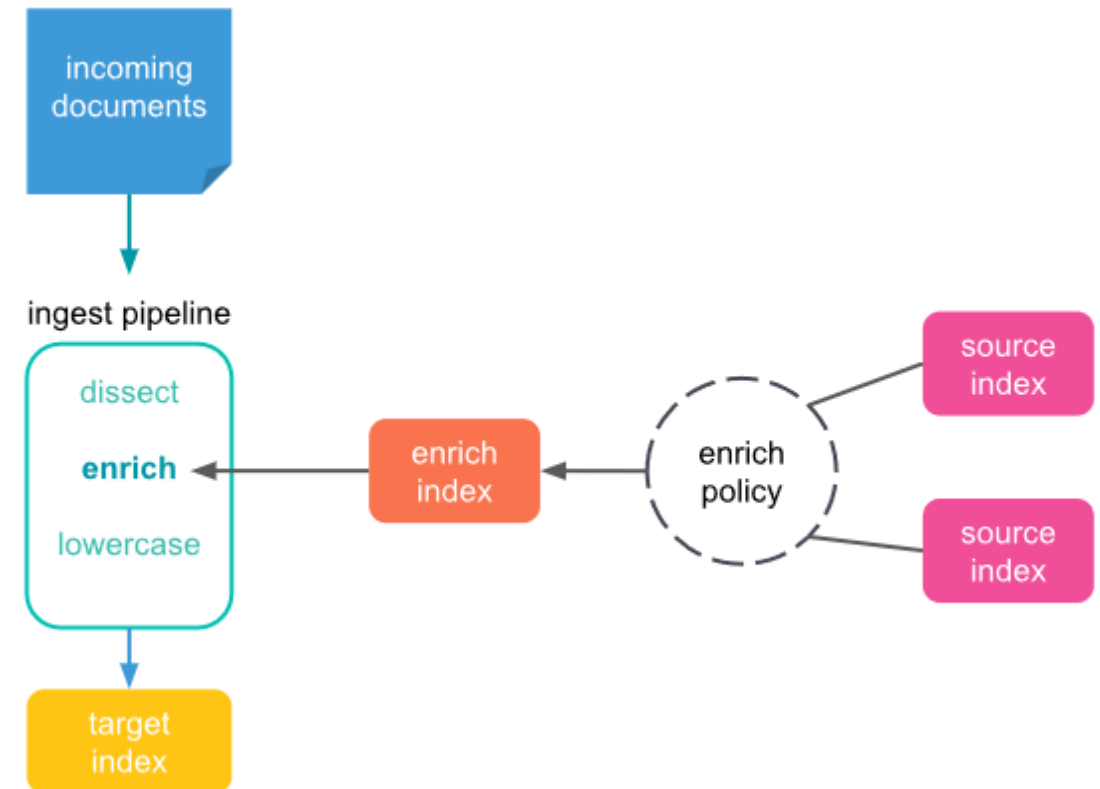


NETEYE: SIEM DETECTIONS

- The SIEM detection engine performs technique-based threat detection and alerts on high-value anomalies.
- Out-of-the-box rules developed by the Elastic security experts enable rapid adoption.
- Custom rules can be created for any data formatted for Elastic Common Schema (ECS).



- Identify web services or vendors based on known IP addresses
- Possibility to enrich data with information coming from Icinga (e.g. hostgroups, custom vars)
 - This allows to create roles that are based on this (multi-tenancy)

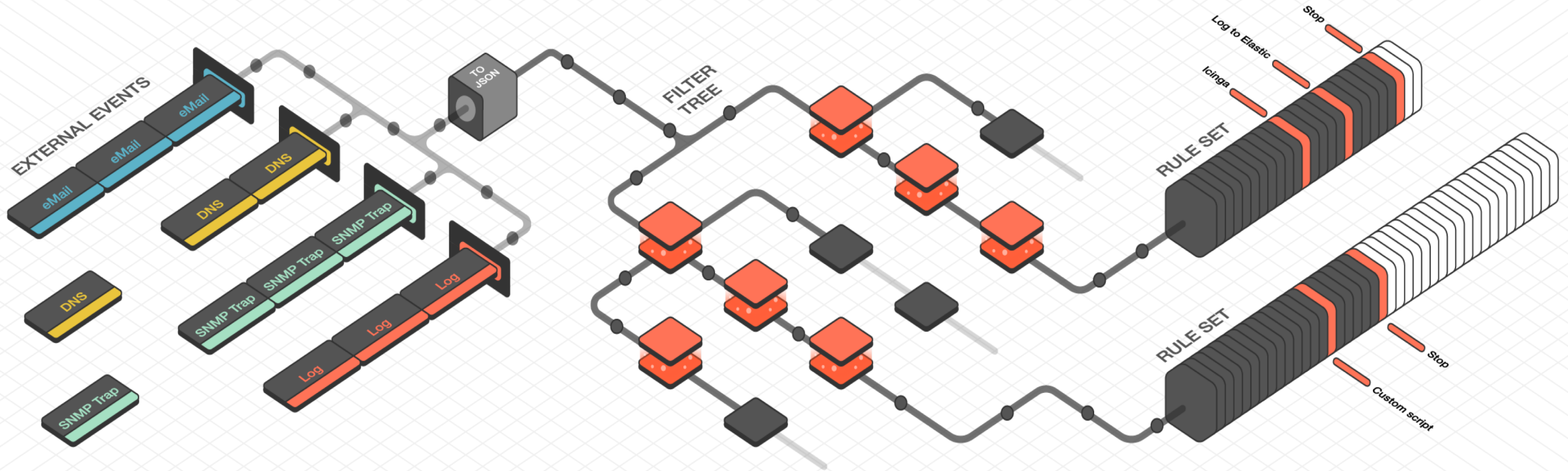




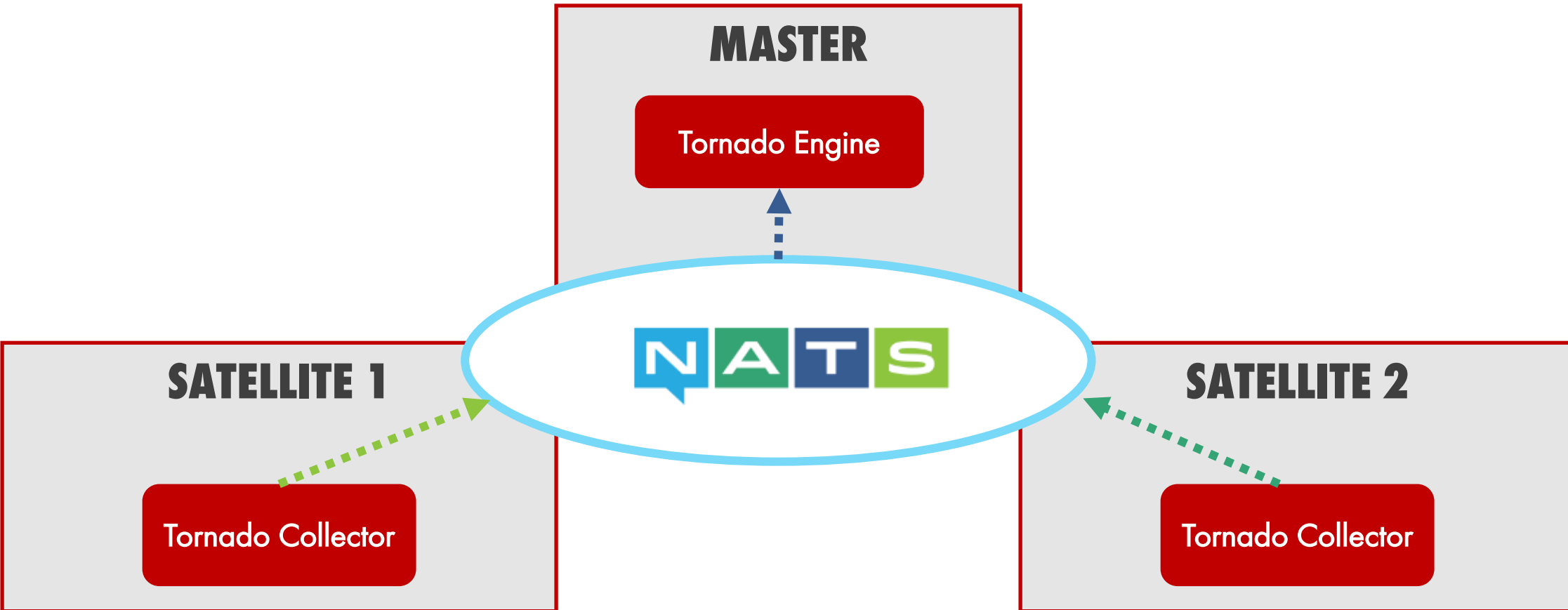
Tornado complex event processing



NETEYE: TORNAADO OVERVIEW



NETEYE: TORNADO DISTRIBUTED EVENT COLLECTIONS



All communications are via **TLS** to assure **security** and **confidentially**.

Nats.io is used as a communication layer



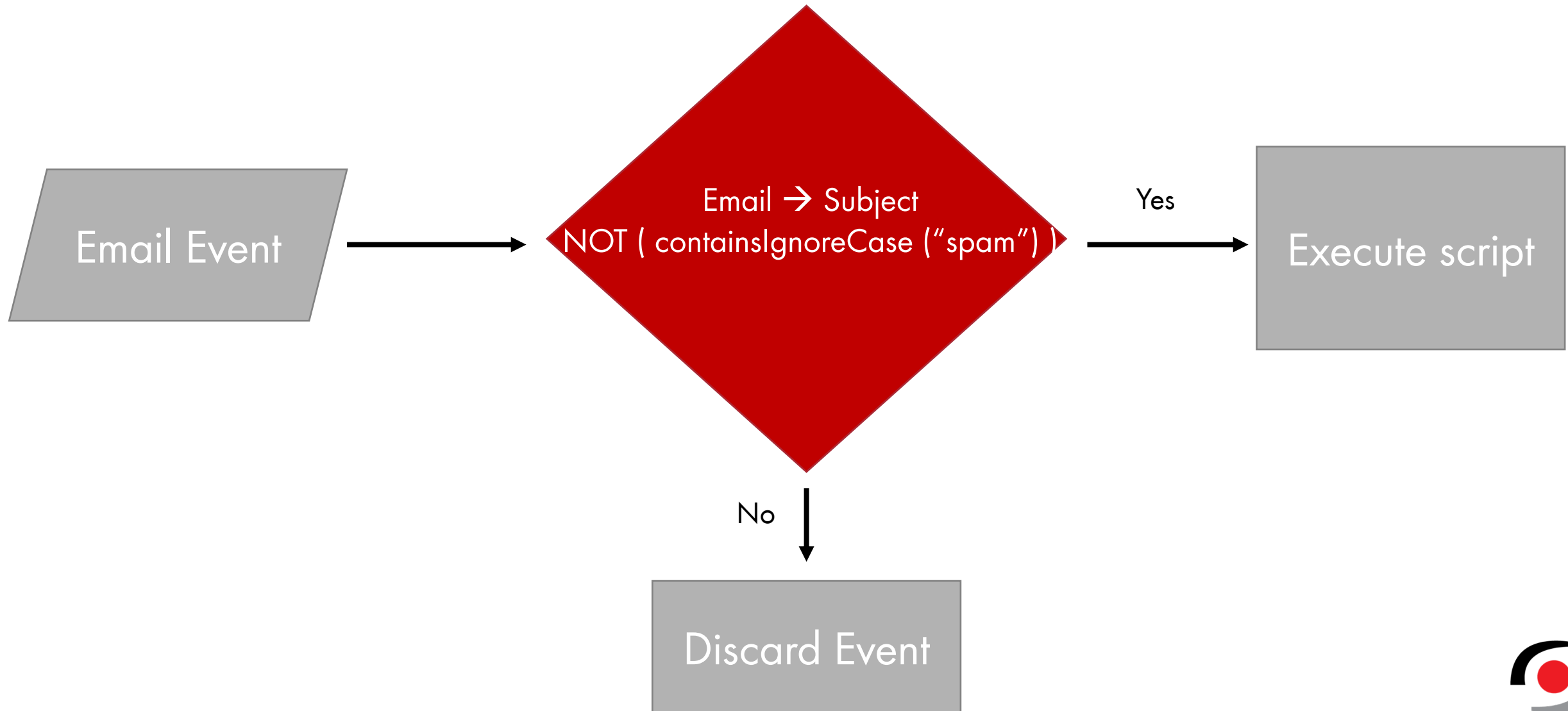
NETEYE 4.11

- equals
- contains
- AND
- OR
- regex
- gt, lt, ge, le

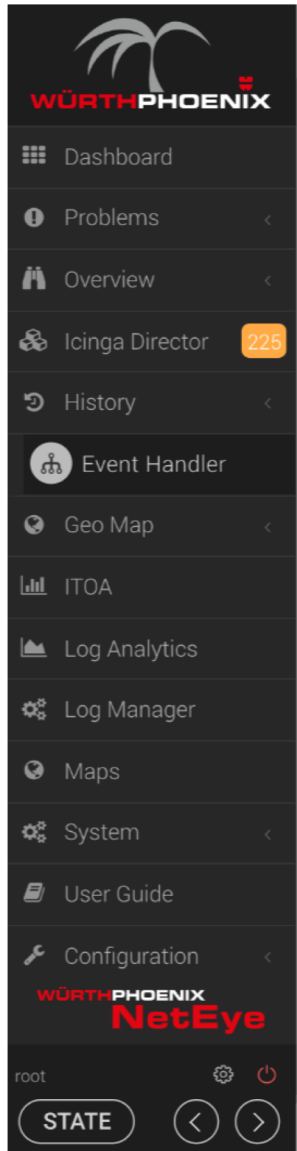
NETEYE 4.12 (NEW OPERATORS)

- NOT
- ne (notEquals)
- containsIgnoreCase
- equalsIgnoreCase





NETEYE: TORNADO CONFIGURATION



- Dashboard
- Problems
- Overview
- Icinga Director 225
- History
- Event Handler
- Geo Map
- ITOA
- Log Analytics
- Log Manager
- Maps
- System
- User Guide
- Configuration

WÜRTHPHOENIX NetEye

root

STATE

Search ...

Dashboard

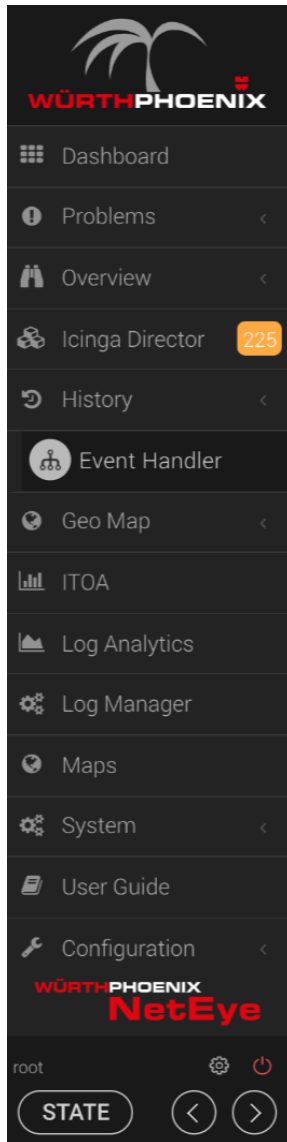
Processing tree

Edit mode **ON** Discard changes Commit changes

+ Add node

+ add node	Rome Configure events delivered from a received email. 120 rules	Bolzano Configure events delivered from a received email. Configure events. 120 rules	Paris Configure events delivered from a received email. 120 rules	Paris Configure events delivered from a received email. Configure events. 120 rules	Paris Configure events delivered from a received email. 120 rules	Turned off
+ add node	Email Configure events delivered from a received email. 120 rules	Trap Events from SNMP daemons in networked devices. 120 rules	SMS Administer events based on the reception of an SMS message. 120 rules	Log Manage events when system sends an alert. 120 rules	Turned off	
+ add node	Cisco Configure events delivered from a received email. Configure events. Rule set 120 rules	Ubiquity Configure events delivered from a received email. Configure events. Rule set 120 rules	Huawei Configure events delivered from a received email. Configure events. Rule set 120 rules	Samsung Configure events delivered from a received email. Configure events. Rule set 120 rules	Something 120 rules	





- Dashboard
- Problems
- Overview
- Icinga Director 225
- History
- Event Handler
- Geo Map
- ITOA
- Log Analytics
- Log Manager
- Maps
- System
- User Guide
- Configuration

WÜRTHPHOENIX NetEye

root

STATE

Search ...

Dashboard

Rules


































Processing tree > Bolzano > Email > Huawei

Open test window

Edit mode Discard changes ✓ Commit changes ↺ ↻

+ Add rule

Show only active rules OFF

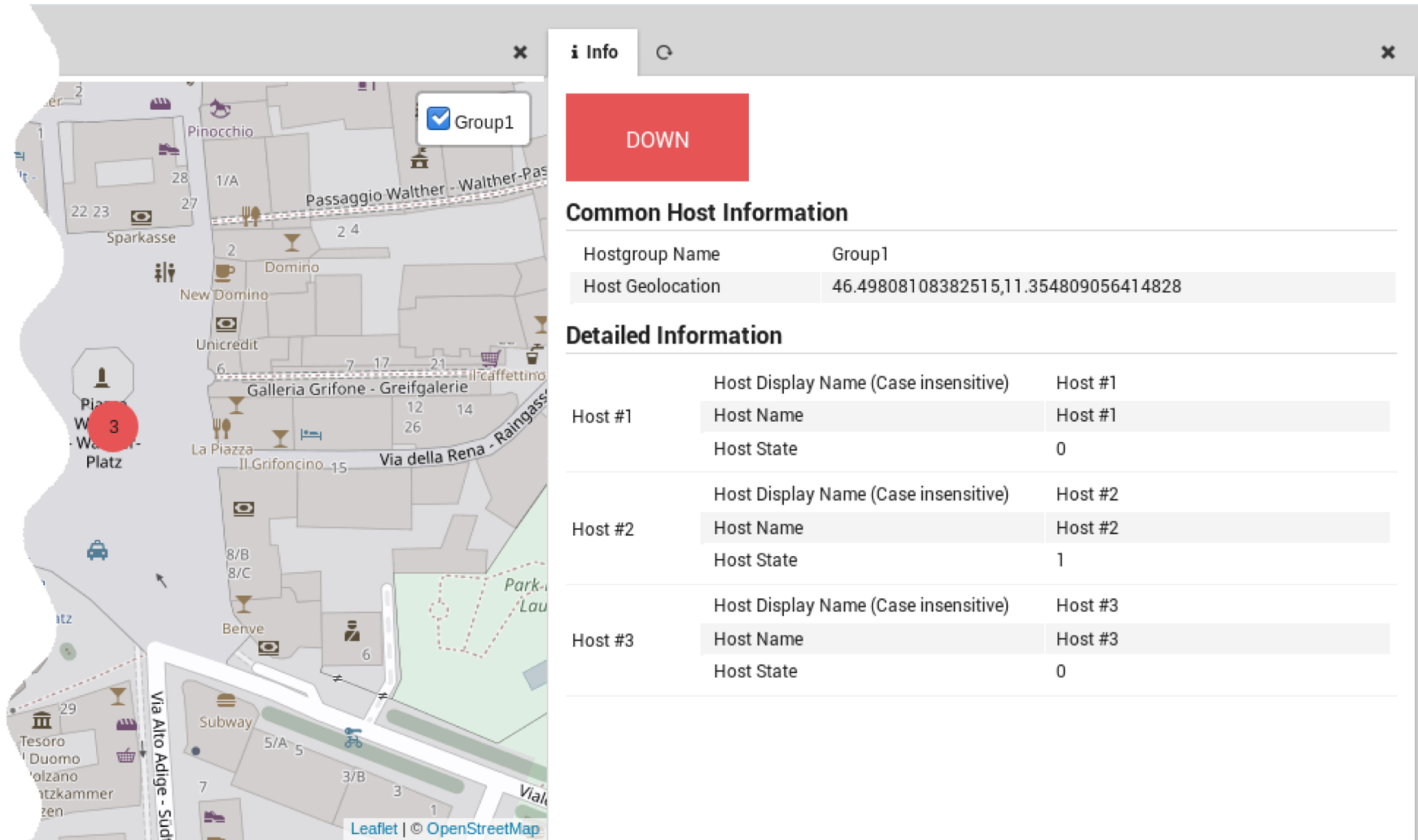
NAME	ACTIONS	DESCRIPTION	
Neactionlaunchpad	Icinga Continue Email Command	Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque quis lorem at	  
I'm also a rule	Icinga Email Command	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse eleifend mi sed	  
Sample rule name	Icinga Continue Email	Adipiscing elit. Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque	  
+ I'm also a rule	Icinga Continue Email Command	Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque quis lorem at	  
Neactionlaunchpad	Command	Adipiscing elit. Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque	  
Sample rule name	Icinga Continue Email	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse eleifend mi sed	  
Neactionlaunchpad	Continue	Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque quis lorem at	  
I'm also a rule	Icinga Continue Email Command	Adipiscing elit. Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque	  
Neactionlaunchpad	Continue Email	Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque quis lorem at	  
Sample rule name	Icinga Continue Command	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Suspendisse eleifend mi sed	  
Neactionlaunchpad	Icinga Continue Email Command	Suspendisse eleifend mi sed lorem pretium sagittis. Donec scelerisque quis lorem at	  

Drag to reorder



GeoMap





DOWN

Common Host Information

Hostgroup Name	Group1
Host Geolocation	46.49808108382515,11.354809056414828

Detailed Information

	Host Display Name (Case insensitive)	Host #1
Host #1	Host Name	Host #1
	Host State	0
Host #2	Host Display Name (Case insensitive)	Host #2
	Host Name	Host #2
	Host State	1
Host #3	Host Display Name (Case insensitive)	Host #3
	Host Name	Host #3
	Host State	0

Grouped
by host

More
readable

User
friendly

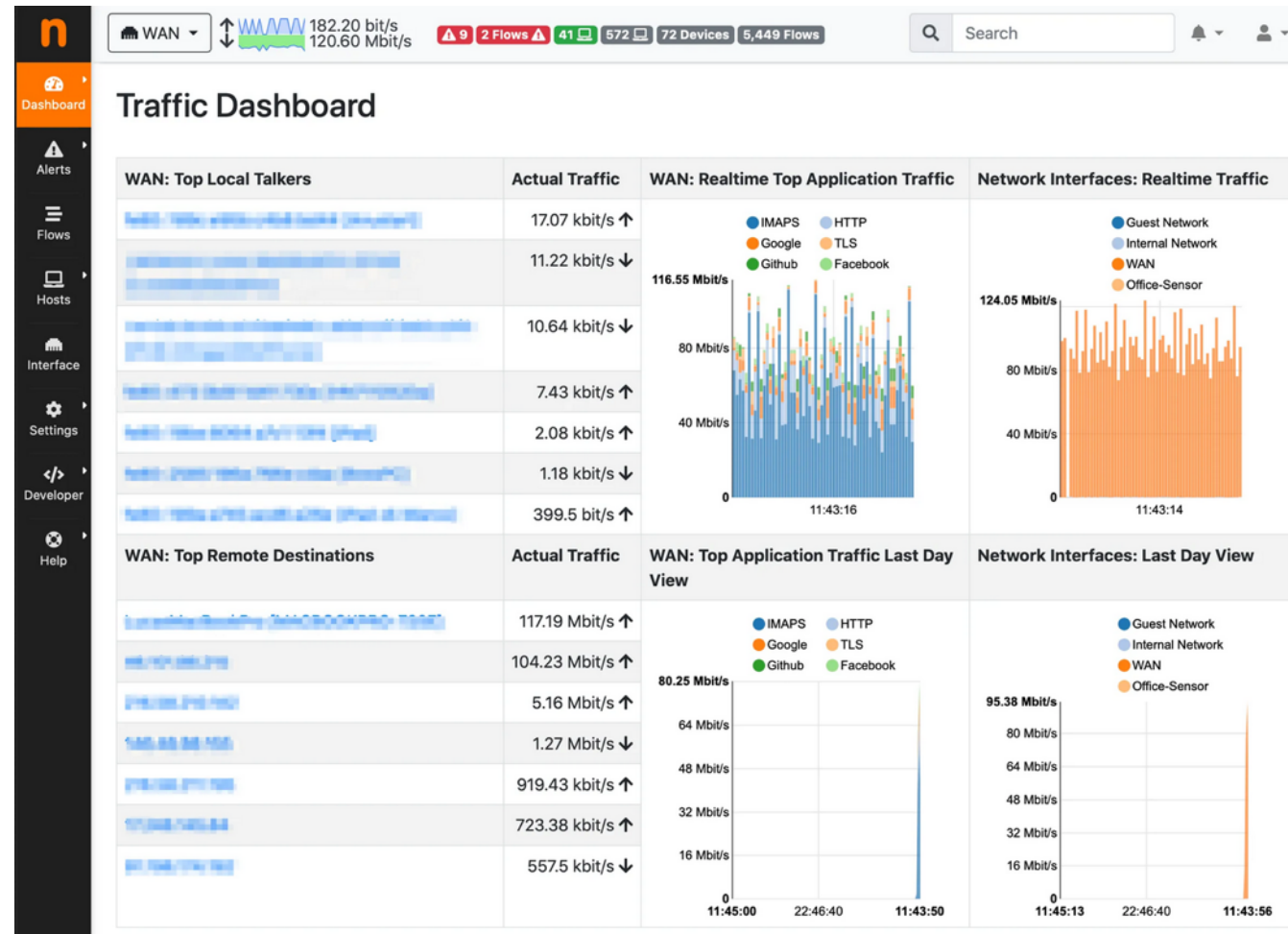


NETWORK VISIBILITY (NTOPNG)

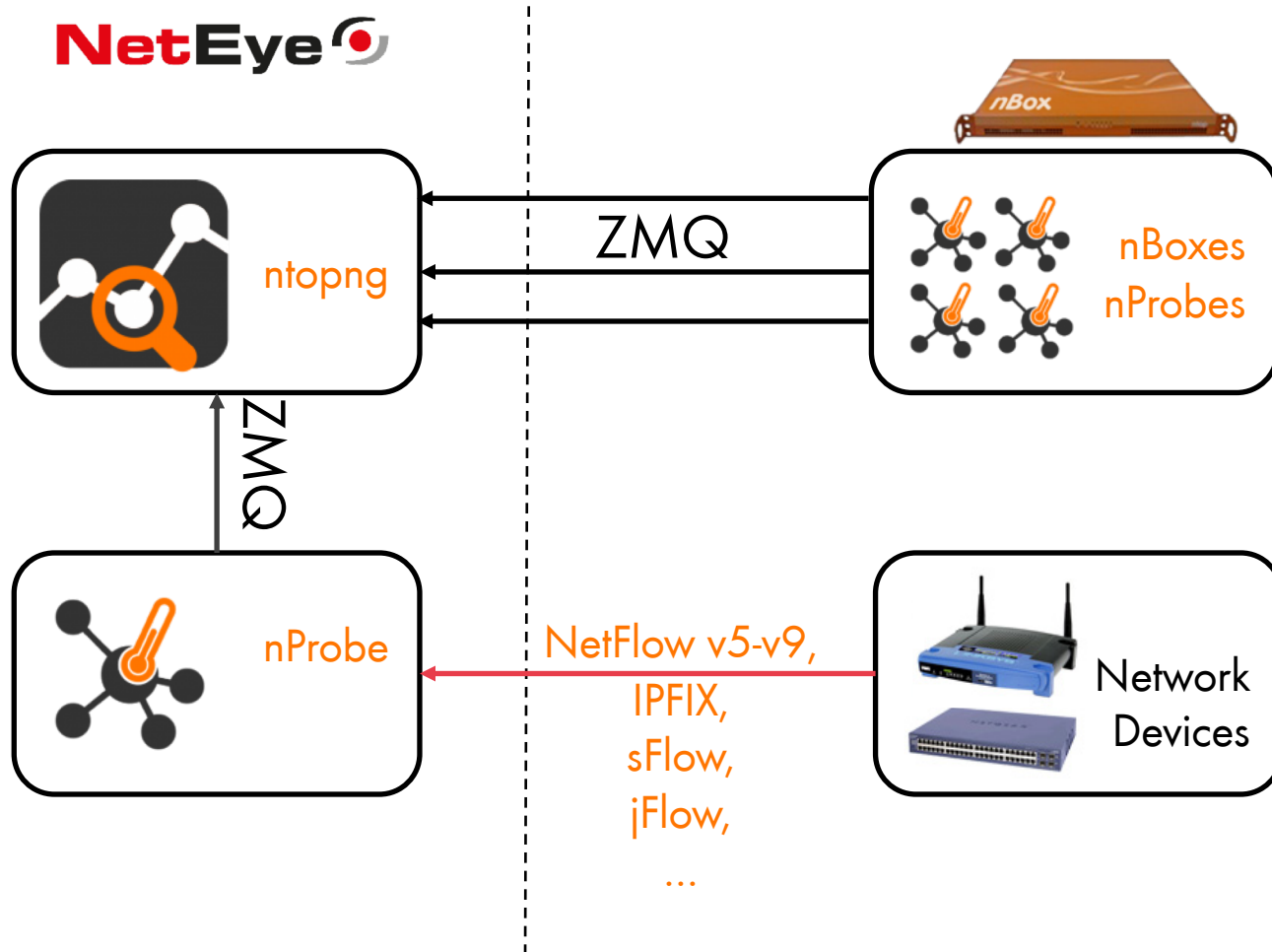


- High-Speed Traffic Analysis and Flow Collection

- New subscription: ntopng



NETEYE: NTOPNG ENTERPRISE INTEGRATION



- Running on NetEye:
 - ntopng
 - nProbe in Collector Mode
- nProbe listens for flows received from any capable Network Device
- ntopng listens for High Performance ZMQ Streams of flows, collected by nProbe Instances



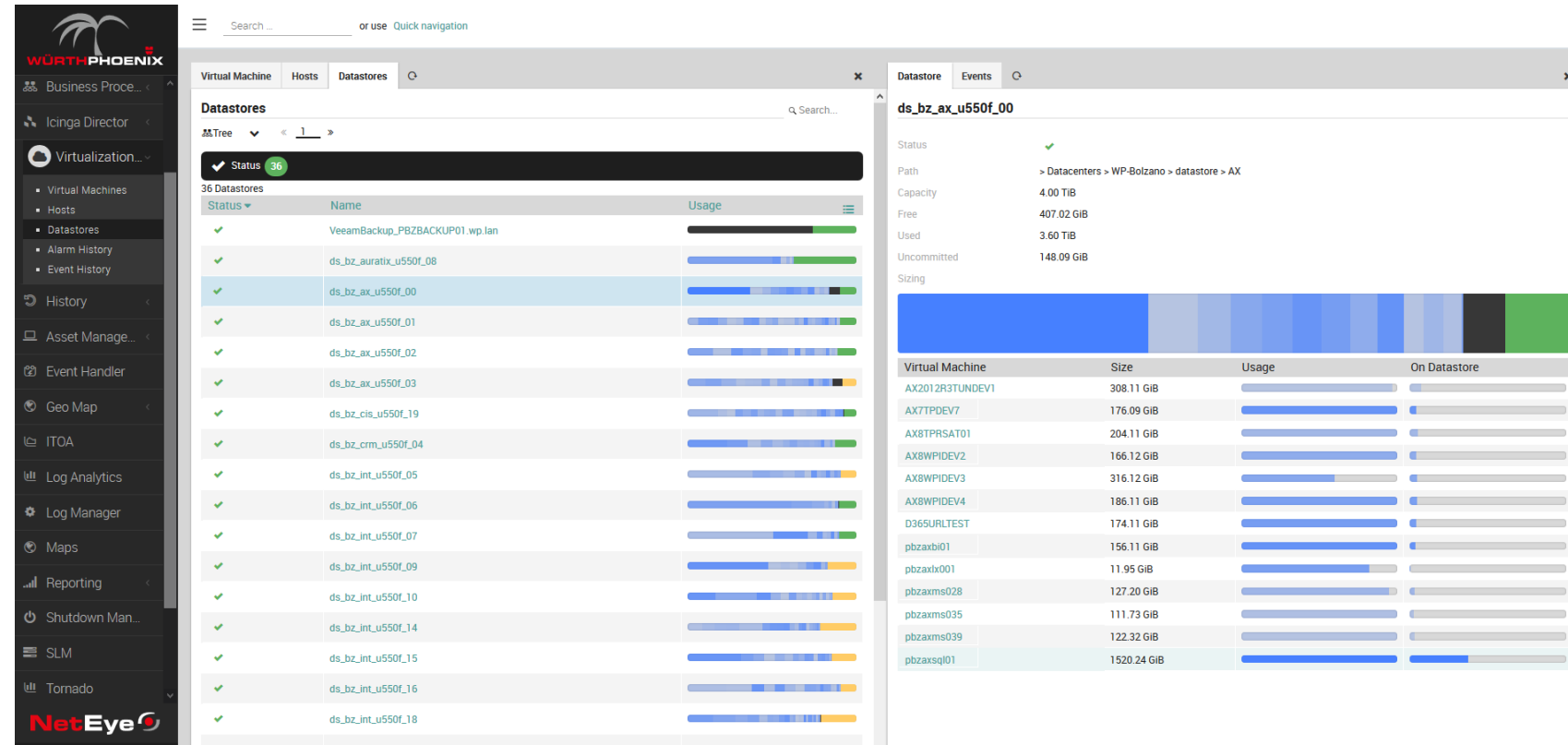


VMWARE DISCOVERY



NETEYE: VMD – VMWARE DISCOVERY

- New Version v1.1.0 of Icingaweb2 Module vSphereDB
- Dedicated Import Source for Icingaweb2 Module Director
- New “purge” Mechanism for logs
- Fixes problem of outdated Datastores



Virtual Machine	Size	Usage	On Datastore
AX2012R3TUNDEV1	308.11 GiB		
AX7TPDEV7	176.09 GiB		
AX8TPRSAT01	204.11 GiB		
AX8WPIDEV2	166.12 GiB		
AX8WPIDEV3	316.12 GiB		
AX8WPIDEV4	186.11 GiB		
D365URLTEST	174.11 GiB		
pbzaxbi01	156.11 GiB		
pbzaxix001	11.95 GiB		
pbzaxms028	127.20 GiB		
pbzaxms035	111.73 GiB		
pbzaxms039	122.32 GiB		
pbzaxsq01	1520.24 GiB		





UPGRADE PROCEDURE





CentOS 7.7.1908



CentOS 7.8.2003

Python 3 available by default
Many packages have got important updates

Further info:

<https://wiki.centos.org/Manuals/ReleaseNotes/CentOS7.2003>



```
/usr/sbin/neteye upgrade
```



It works for single instances and clusters

It checks prerequisites before upgrading:

- Health checks are successful
- Fencing is disabled (on clusters)
- Nodes are online (on clusters)
- Latest bug fixes are installed

It installs the new repo definitions

- The old procedure will not anymore work





WWW.WUERTH-PHOENIX.COM
WWW.NETEYE-BLOG.COM