



The bridge to possible

Next Generation ISE Telemetry

Monitoring and Custom Reporting

Emmanuel Cano, Security Consulting Engineer

 @EmmanuelCano

CISCO *Live!*



DEVNET-2035

9:30

26°



ALARMS



Insufficient Virtual M...

35

13 hrs 48 mins ...



No Configuration Bac...

14

17 hrs 40 mins ...



High Load Average

17

2 days ago



High Memory Utilizati...

11

7 days ago

05:27:24	PM	all	6.66	0.00	0.96	0.13	0.29	0.13	0.00	0.00	0.00	91.83
05:27:27	PM	all	1.47	0.00	1.72	0.04	0.25	0.17	0.00	0.00	0.00	96.34
05:27:30	PM	all	2.56	0.00	1.18	0.00	0.25	0.13	0.00	0.00	0.00	95.88



Agenda

- Why do we need next-gen Monitoring and reporting tools?
- Infrastructure Monitoring + Demo
- Log Analytics + Demo
- Data Connect + Demo
- Wrap-Up and Next Steps



Cisco Webex App

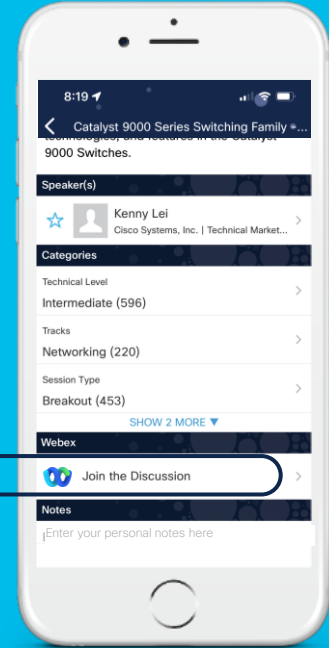
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2035>

For your Reference!



Slido: How do you
monitor your ISE
Hardware resources,
performance and
processes?

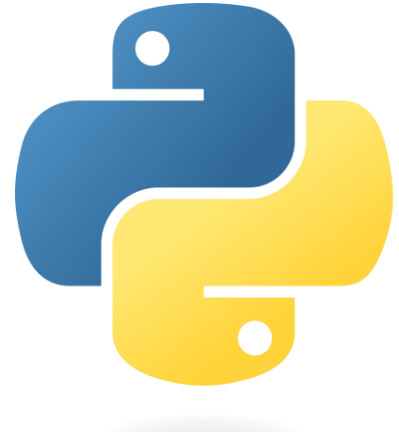


slido

- Join at
- Slido.com
- #3469 778



Do you recognize these logos?

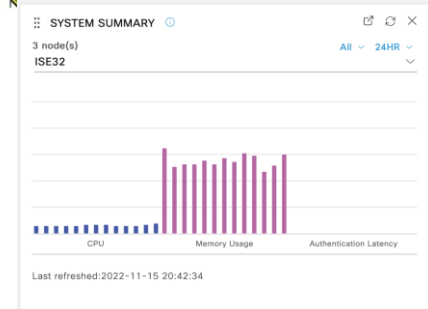


Why we need next-gen Monitoring and reporting tools?

Why Next-Generation Options

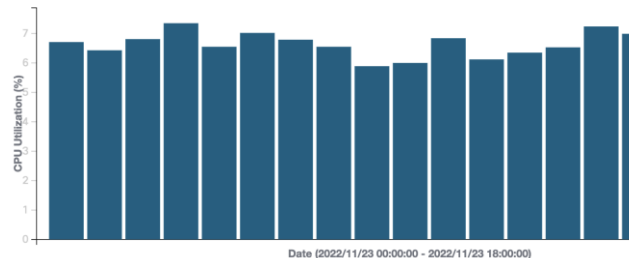
Hardware resources and processes Monitoring

Time	Date	Source	Description
12:15:03	05/25/18	10.1.100.6	est-server:Running
12:10:04	05/25/18	10.1.100.6	elasticsearch:Running
12:10:04	05/25/18	10.1.100.6	ca-server:Running
12:10:04	05/25/18	10.1.100.6	mint-processor:Running
12:10:04	05/25/18	10.1.100.6	mint-collector:Running
12:10:03	05/25/18	10.1.100.6	ad-connector:Running
12:10:03	05/25/18	10.1.100.6	redis-server:Running
12:10:03	05/25/18	10.1.100.6	rsyslog:Running
12:10:03	05/25/18	10.1.100.6	app-server:Running
12:07:37	05/25/18	10.1.100.6	Link Up
12:07:37	05/25/18	10.1.100.6	Link Up
12:07:37	05/25/18	10.1.100.6	Link Up
12:07:37	05/25/18	10.1.100.6	Link Up
12:07:37	05/25/18	10.1.100.6	Link Up
12:07:37	05/25/18	10.1.100.6	Link Up



- > show cpu usage
- > show memory
- > show app status ise
- > show disk

Chart: Time vs CPU Utilization



Why Next-Generation Options



Static
Reports.PDF

Authentications By Location

Location	Passed	Failed	Total
All Locations	101	0	101

Authentications By Device Name

Network Device Name	Passed	Failed	Total
EAP-TEST	101	0	101

Authentications By Allowed Protocol

Allowed Protocol	Passed	Failed	Total
Default Network Access	101	0	101

Logs and Reporting

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Click here to do wireless setup and visibility setup Do not show th

Misconfigured Supplicants 1 Misconfigured Network Devices 0 RADIUS Drops 13 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 24 hours

Refresh Reset Repeat Counts Export To

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...
Nov 20, 2019 02:25:04.871 AM	✓		0	GRAN ABuser1	D4:BE:D9:FA:96:13	Dell-Device	User_dot1x...	User_dot1x...
Nov 20, 2019 02:24:34.452 AM	✓			GRANDM jser1	D4:BE:D9:FA:96:13	Dell-Device	User_dot1x...	User_dot1x...
Nov 19, 2019 10:12:42.048 PM	✓			vpn	F0:18:98:77:5A:89	VPN >> Def...	VPN >> Def...	VPN >> VPN
Nov 19, 2019 10:12:03.856 PM	✓			vpn	F0:18:98:77:5A:89	VPN >> Def...	VPN >> Def...	VPN >> VPN
Nov 19, 2019 10:01:22.792 PM	✓			vpn	F0:18:98:77:5A:89	VPN >> Def...	VPN >> Def...	VPN >> VPN
Nov 19, 2019 10:01:12.838 PM	✓			vpn	F0:18:98:77:5A:89	VPN >> Def...	VPN >> Def...	VPN >> VPN
Nov 19, 2019 10:01:03.888 PM	✓			vpn	F0:18:98:77:5A:89	VPN >> Def...	VPN >> Def...	VPN >> VPN
Nov 19, 2019 05:58:04.955 PM	✓			GRANDMETRIC-LABuser1	D4:BE:D9:FA:96:13	Dell-Device	User_dot1x...	User_dot1x...

Why Next-Generation Options

Is this
Scalable/dynamic?

Customizable?

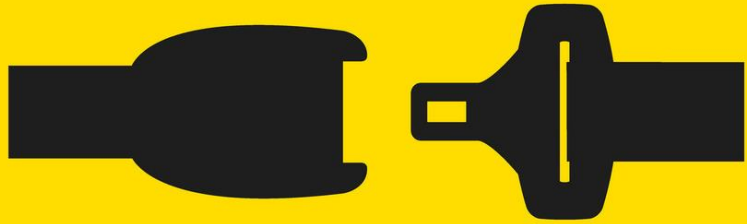
Do I need another
software?

Is this easy to
use/read?



Next Generation Monitoring and Custom Reporting

FASTEN YOUR



SEAT BELT



Infrastructure Monitoring

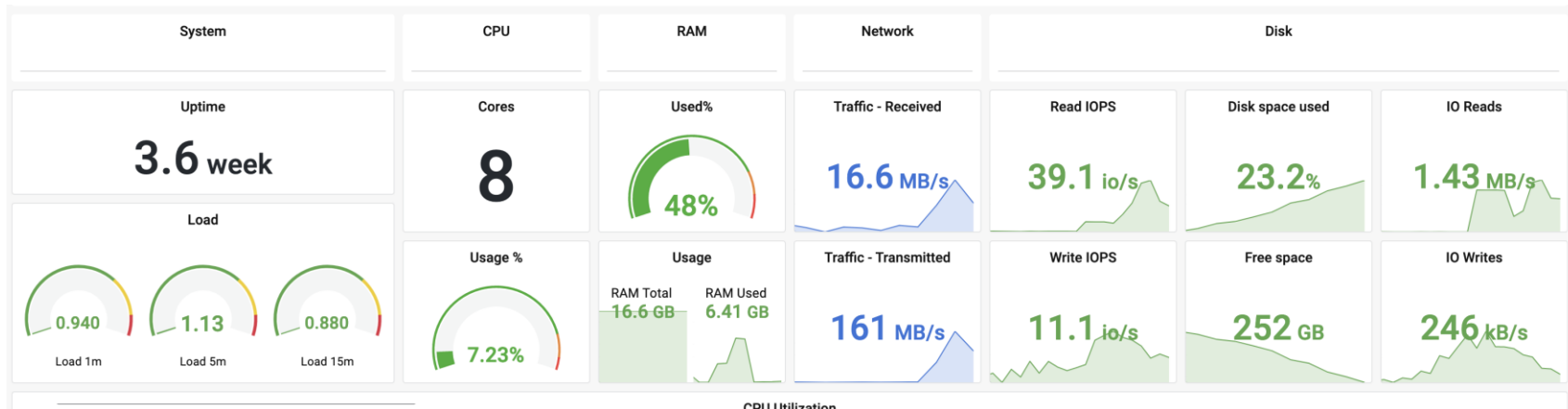
Infrastructure Monitoring – System 360



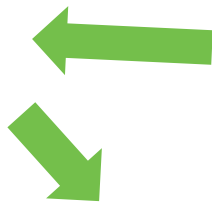
1. **CPU**: Overall CPU usage
2. **Diskstats**: HDD and SSD disk statistics
3. **Loadavg**: System load of the node for a defined period of time

1. **Meminfo**: RAM usage statistics
2. **Stat**: System kernel statistics
3. **Time**: System time

Infrastructure Monitoring



```
node_network_iface_tx
node_network_iface_link
node_network_iface_link_mode
node_network_info
node_network_mtu_bytes
node_network_name_assign_type
node_network_net_dev_group
node_network_protocol_type
node_network_receive_bytes_total
node_network_receive_compressed_total
node_network_receive_drop_total
node_network_receive_errs_total
node_network_receive_fifo_total
```



Explore Prometheus

A (Prometheus)

Metrics browser >

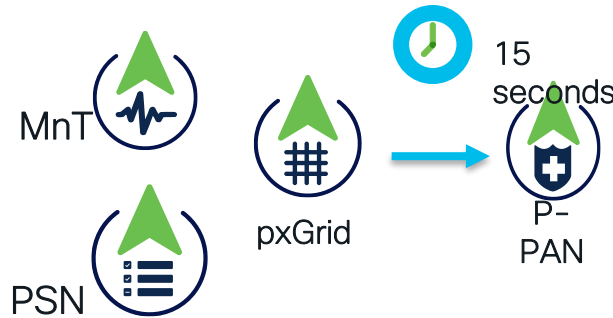
Query type: Range Instant Both Min step: auto Exemplars

[+ Add query](#) [Query history](#) [Inspector](#)

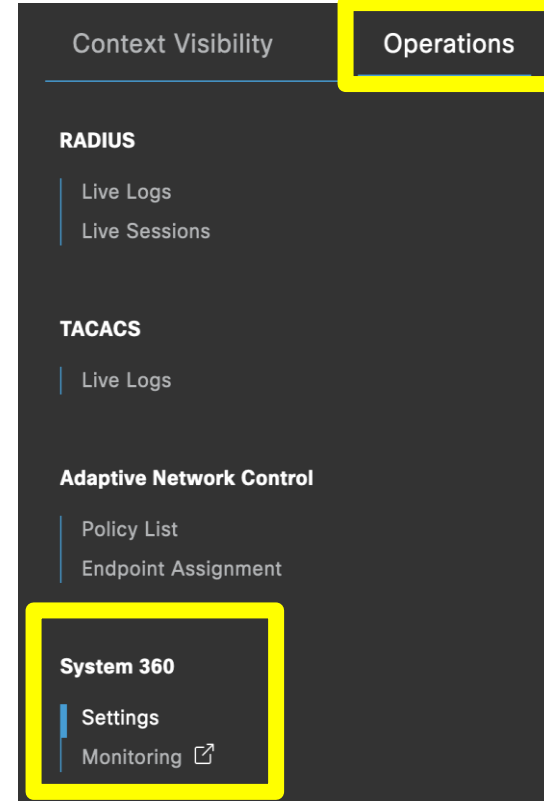
`node_network_info{job="node_ISE32"}`

Infrastructure Monitoring - Considerations

- The Monitoring service is enabled by default
- This data is accessed by Grafana to populate the dashboards.

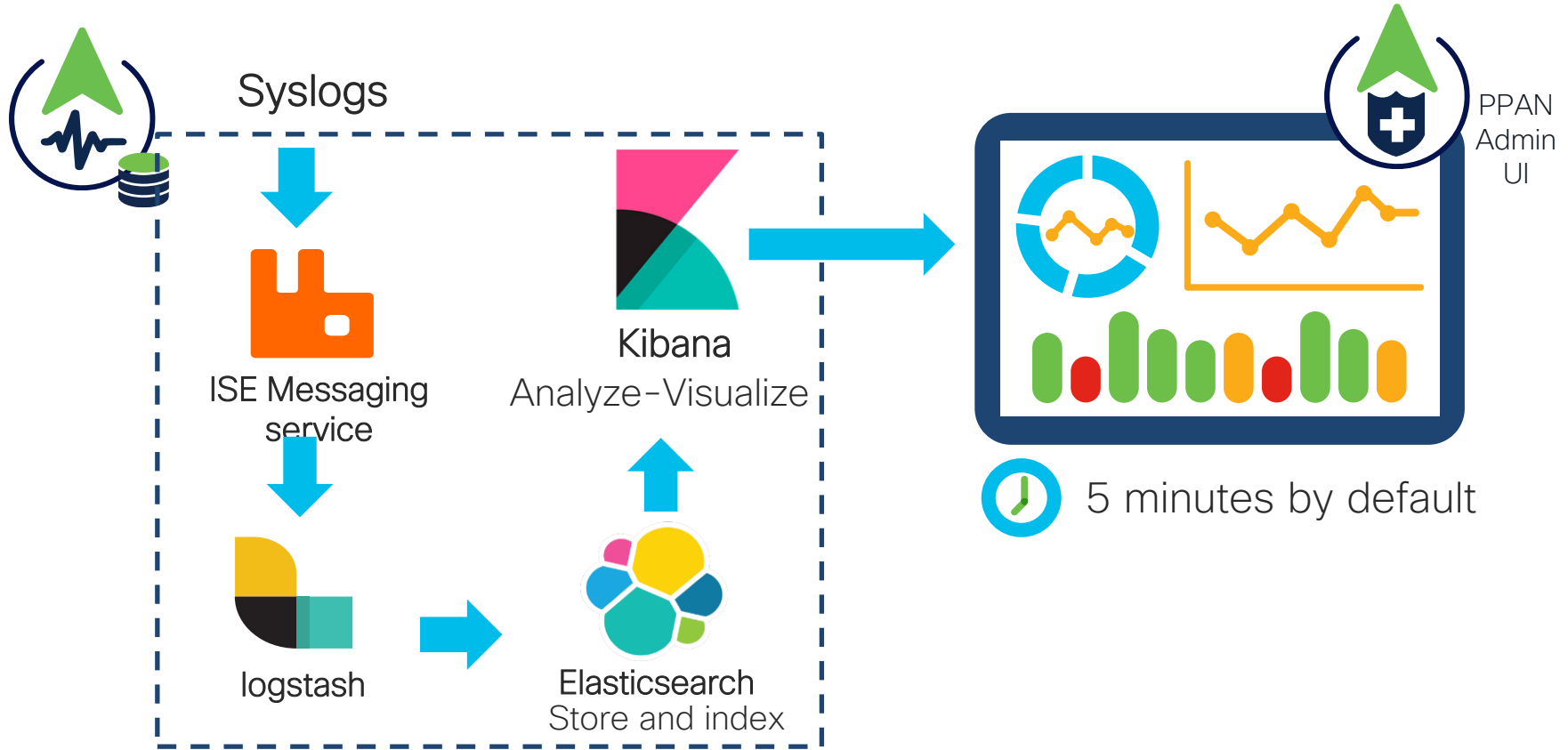


This data is retained in the Prometheus database for **7 days**.

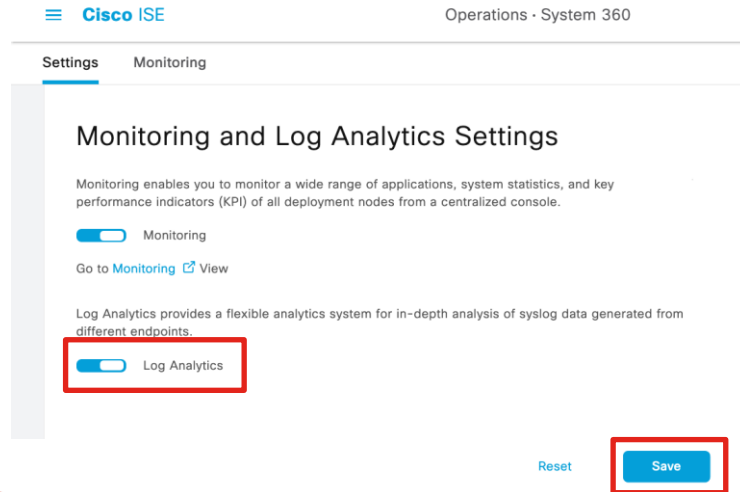
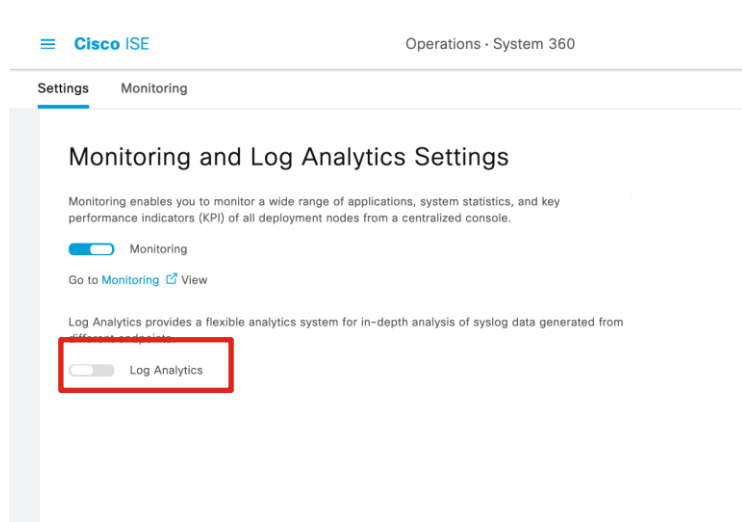


Log Analytics

Log Analytics – System 360



Log Analytics – System 360



Error

MnT doesn't have at least 8 CPU cores and at least 16GB memory.

OK

Log Analytics – Deployment Scenarios



Small Deployment



Medium Deployment



Large Deployment

Log Analytics and Infra Monitoring – Services Status



For your
Reference!

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	513862
Database Server	running	100 PROCESSES
Application Server	running	531252
Profiler Database	running	521678
ISE Indexing Engine	running	533133
AD Connector	running	534510
M&T Session Database	running	527746
M&T Log Processor	running	940202
Certificate Authority Service	running	534275
EST Service	running	577833
SXP Engine Service	disabled	
TC-NAC Service	disabled	
PassiveID WMI Service	disabled	
PassiveID Syslog Service	disabled	
PassiveID API Service	disabled	
PassiveID Agent Service	disabled	
PassiveID Endpoint Service	disabled	
PassiveID SPAN Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	517076
ISE API Gateway Database Service	running	520369
ISE API Gateway Service	running	526266
ISE pxGrid Direct Service	running	553719
Segmentation Policy Service	disabled	
REST Auth Service	disabled	
SSE Connector	disabled	
Hermes (pxGrid Cloud Agent)	disabled	
ISE Node Exporter	running	562260
ISE Prometheus Service	running	565973
ISE Grafana Service	running	561688
ISE MNT LogAnalytics Elasticsearch	running	663611
ISE Logstash Service	running	666082
ISE Kibana Service	running	667899

`show application status ise`

Infrastructure Monitoring

- ISE Node Exporter running 30774
- ISE Prometheus Service running 32862
- ISE Grafana Service running 36380

Log Analytics

- ISE MNT LogAnalytics Elasticsearch running 63388
- ISE Logstash Service running 68472
- ISE Kibana Service running

Demo: Infra Monitoring & Log Analytics

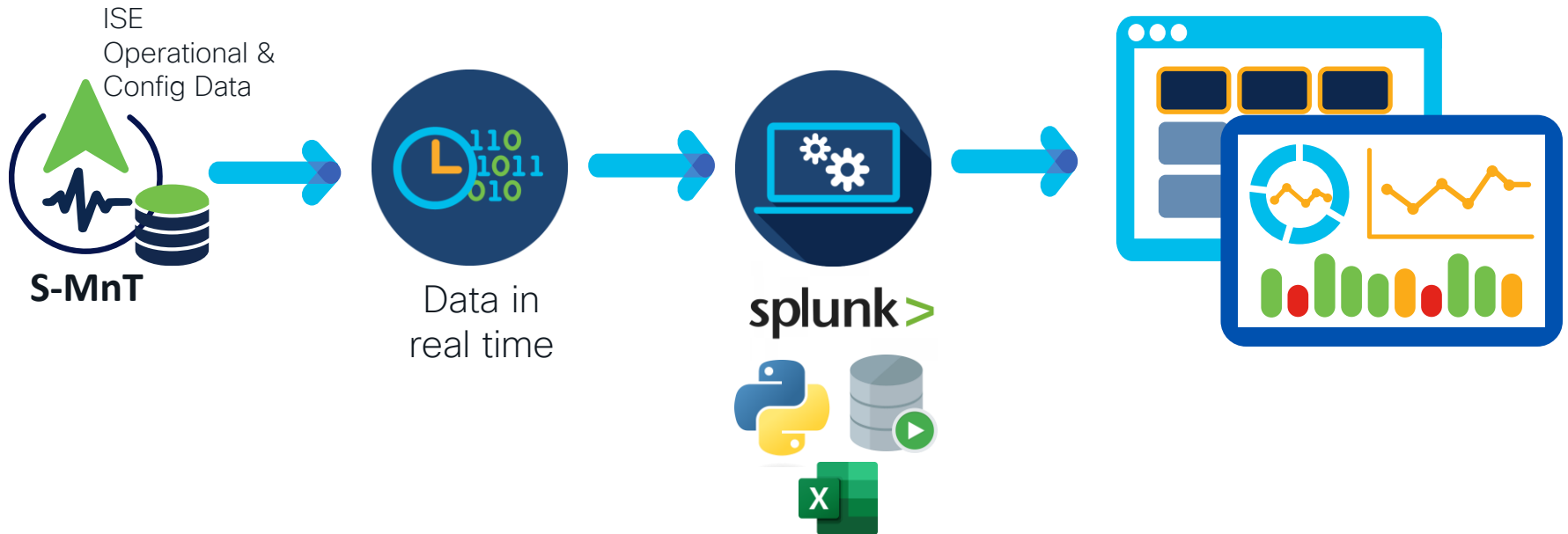
Well, this is great! But...still local...



Data Connect

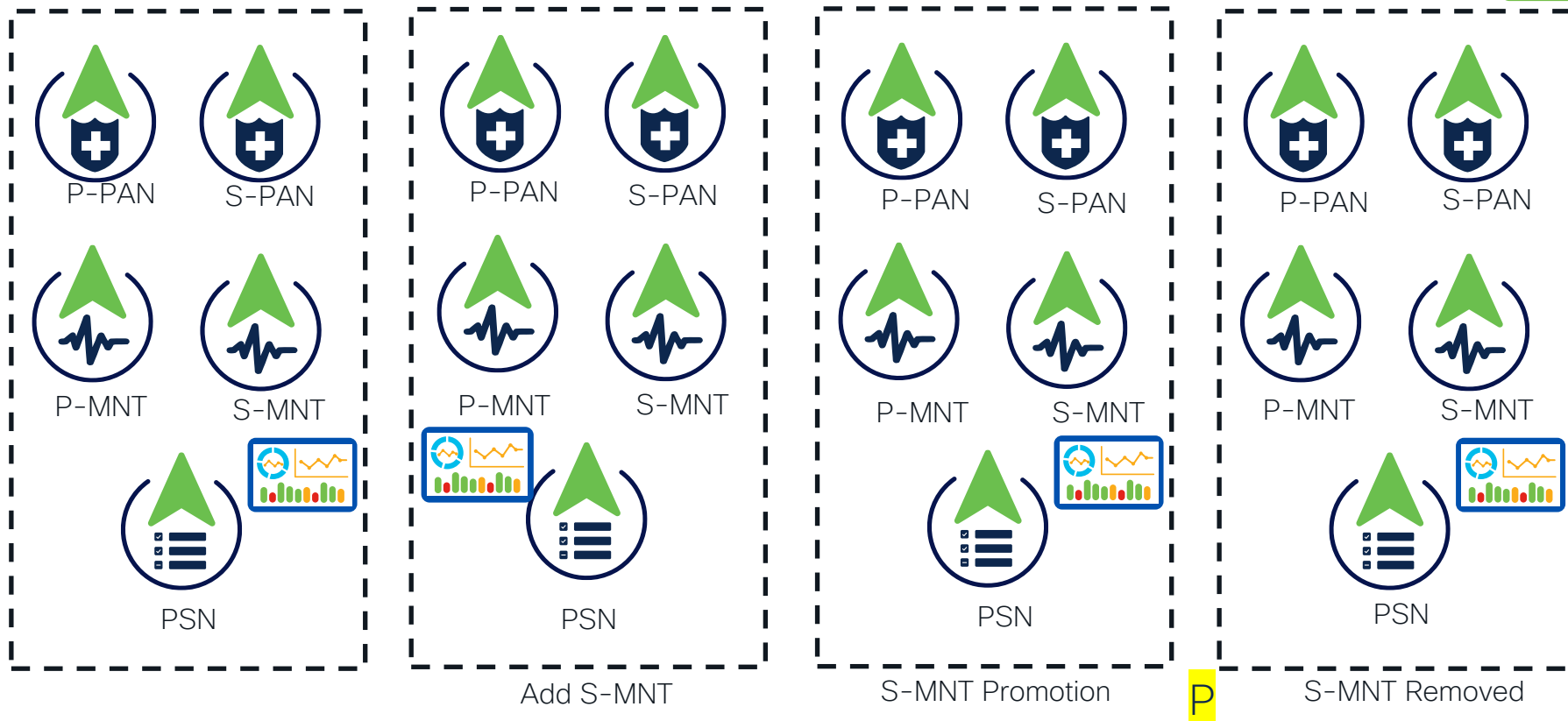
Data Connect – What you need WHEN you need it.

Extract any **configuration** or **operational** data

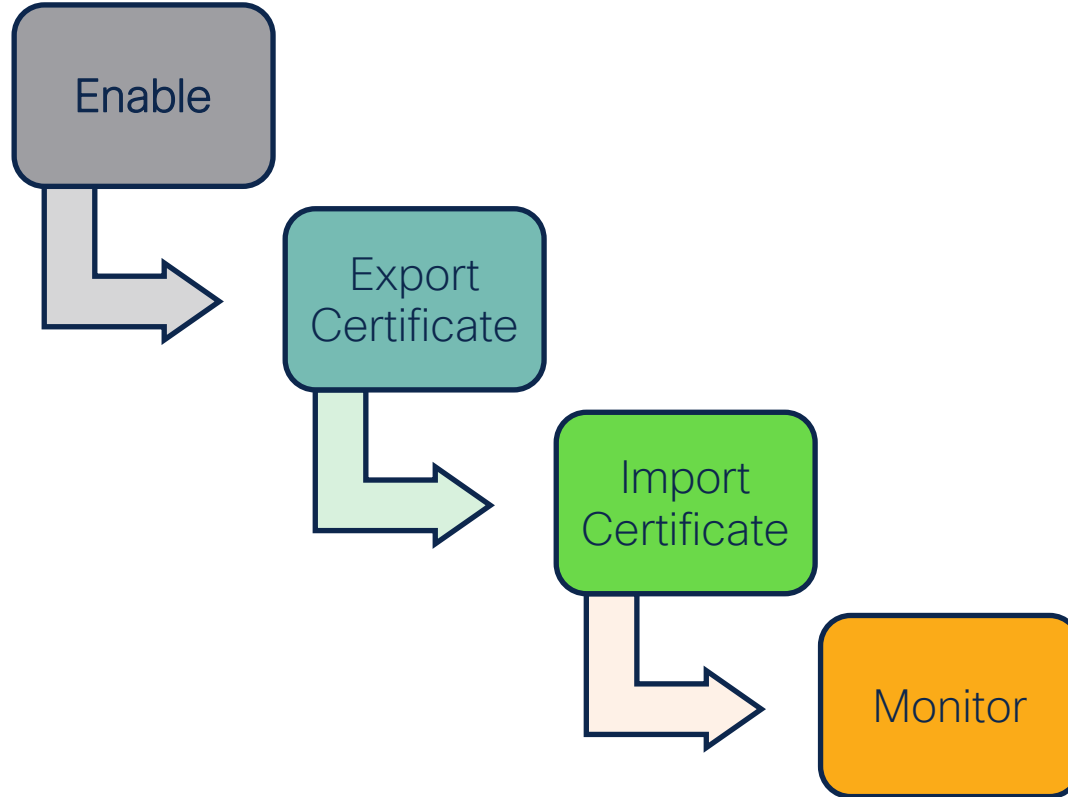


Data Connect – Deployment Scenarios

For your
Reference!



Data Connect - Steps



Data Connect – Enable.



• Essentials License

Administration > System > Settings > Data Connect

☒ Data Connect

User Name	dataconnect
Hostname/IP	ISEPANSEC.ciscoise.lab
Port	2484
Service Name	cpm10
Password Expires on	27 November 2023 at 21:43 UTC

Change Password

Password
.....

[View Password Criteria](#)

Confirm Password
.....

Password Expiry
365

Dataconnect Services

GET	/api/v1/mnt/data-connect/details	Retrieve the Dataconnect ODBC details.
GET	/api/v1/mnt/data-connect/settings	Retrieve the status of the Dataconnect feature
PUT	/api/v1/mnt/data-connect/settings/password	Update the Dataconnect user password.
PUT	/api/v1/mnt/data-connect/settings/password/expiry	Updates the number of days of Dataconnect password expiry.
PUT	/api/v1/mnt/data-connect/settings/status	Update the DataConnect feature status



<https://github.com/EmmanuelCano/DataConnect>

12 to 30 characters: (A-Z), (a-z), (0-9) -(#\$%&*+,-.:;=?^_~)

Data Connect – Export/Import Certificate

For your
Reference!



Trusted Certificates – Self-Signed Certificate

Certificate Hierarchy

Export

Import

ISE_ORACLE_ISEPANSEC.ciscoise.lab

ISE_ORACLE_ISEPANSEC.ciscoise.lab
Issued By : ISE_ORACLE_ISEPANSEC.ciscoise.lab
Expires : Wed, 8 Nov 2023 00:06:45 UTC

Certificate status is good

Details

Issued To

Common Name (CN) ISE_ORACLE_ISEPANSEC.ciscoise.lab

Organization Unit (OU)

Organization (O) Cisco Systems

City (L)

State (ST)

Country (C)

Serial Number 58:32:26:C2:C4:C2:FF:B7:1B:B3:79:68:BC:C2:A2:F9

keytool -import -alias CiscoLive -file
DataConnectCertificate.pem -storetype JKS -
keystore JKS



```
ECANOGUT-M-DY10:CiscoLive ecanogut$ keytool -import -alias CiscoLive -file Da
Enter keystore password:
Owner: CN=ISE_ORACLE_ISEPANSEC.ciscoise.lab, O=Cisco Systems
Issuer: CN=ISE_ORACLE_ISEPANSEC.ciscoise.lab, O=Cisco Systems
Serial number: 583226c2c4c2ffb71bb37968bcc2a2f9
Valid from: Tue Nov 08 01:06:45 CET 2022 until: Wed Nov 08 01:06:45 CET 2023
Certificate fingerprints:
    SHA1: B8:4A:18:11:9E:69:AB:8E:73:85:7F:BF:DF:83:41:F7:72:53:73:6F
    SHA256: B9:3A:97:4B:89:29:63:D5:4A:4E:E7:DE:23:8C:A0:53:D2:7E:4D:AC:
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```



Data Connect – Monitor



Data Connect alerts and alarms are generated in the following scenarios:

- **License Expiry:** If the Essentials license expires
- **Password Expiry:** If the Data Connect password expires
- **Certificate Expiry:** If the Data Connect certificate



Your Data Connect password expires in 3 days. Please update it. [Update password](#)

Demo: Data Connect

Wrap-Up - Monitoring and Reporting New Approach



Optimal resources utilization



Improve Visibility



Better Performance
and **Decision Making**



Proactive Actions

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer /
Meet the speaker meeting.



Attend any of the related sessions at the DevNet,
Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions
at ciscolive.com/on-demand.



Meet the Speaker:
Area 1
02/08/23 – 12:20pm

Security Technologies

Network Security

Learn about a broad range of solution and technologies which will help you better understand how to secure your network. You will find topics such as VPN, ISE, IPv6, DDoS, IoT....

START



Feb 5 | 19:00

LABSEC-2333

ISE integrations via pxGrid with FTD, WSA, StealthWatch



Feb 6 | 08:45

TECSEC-3781

Walking on solid ISE - Advanced Use Cases and Deployment Best Practices



Feb 7 | 08:45

BRKSEC-2445

The Art of ISE Posture, Configuration and Troubleshooting



Feb 7 | 11:30

BRKSEC-2037

Securing Starlink Internet Services



Feb 8 | 10:45

BRKSEC-2096

Securing Industrial Networks: Where do I start?



Feb 8 | 13:30

BRKSEC-2678

DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances



Feb 9 | 08:30

BRKSEC-2660

ISE Deployment Staging and Planning



Feb 9 | 10:30

BRKSEC-2101

Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis



Feb 9 | 15:45

BRKSEC-3058

Route based VPNs with Cisco Secure Firewall



Feb 9 | 15:45

BRKSEC-2044

Secure Operations for an IPv6 Network



Feb 10 | 09:00

BRKSEC-3019

Visibility, Detection and Response with Cisco Secure Network Analytics

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

CISCO *Live!*



Feb 10 | 09:00

LTRSEC-2381

Stronger Together: Uniting IT and
OT Security with Cyber Vision

Feb 10 | 09:00

BRKIPV-3134

IPv6 Security in the Local Area
with First Hop Security

Feb 10 | 11:00

FINISH

BRKSEC-2218

Cisco Secure Hybrid SWG -
Your First Step to Your SASE Journey

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

CISCO *Live!*



The bridge to possible

Thank you

CISCO *Live!*

References

More Resources

- Data Connect: <https://developer.cisco.com/docs/dataconnect/#!/introduction>
- Data Connect (Open API): <https://developer.cisco.com/docs/identity-services-engine/latest/#!/data-connect-openapi>
- ISE Public Bar: <https://eurl.io/#ryJFrhiBW>
- ISE Webinars and Training Videos: <https://learningnetwork.cisco.com/s/cisco-ise-training-videos>
- ISE Devnet: <https://developer.cisco.com/identity-services-engine/>
- Configure ISE 3.2 Data Connect Integration with Splunk:
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/218190-configure-ise-3-2-data-connect-integrati.html>
- GitHub Repository : <https://github.com/EmmanuelCano>

Appendix

Data Connect – Monitor

For your
Reference!



Logged At	Administrator	Server	Interface	Object Type	Object Name	Event	IP Address
Today ▾ ×	Administrator	Server		Object Type	Object Name		IP Address ▾
2022-12-05 23:15:22.216	admin	ISE32	GUI	DataconnectSetting	DataConnect	Changed configuration	10.209.222.192

The **Change Configuration Audit** logs are generated when the Data Connect feature is enabled or disabled by the admin, or as a result of a persona change.

Data Connect Logging

Additional logs for UI and Open API changes related to Data Connect will be available at **ise-psc.log**

object updated: Value=Dataconne...

object updated: Value=Dataconnect Setting has been enabled successfully

Infrastructure Monitoring – SOC VIEW!

For your
Reference!



Create Menu Access Permission

* Name Infra Monitorig

Description:

Menu Access Privileges

ISE Navigation Structure

- Operations
 - Adaptive Network Control
- Reports
 - System 360
- RADIUS
- Threat-Centric NAC Live Lo
- Troubleshoot
- TACACS
- Administration

Permissions for Menu Access

- ☒ Show
- ☐ Hide

Admin Group

* Name Monitoring

Description

Type ☐ External

Member Users

Users		
+ Add Delete		
<input type="checkbox"/>	Status	Email Username
<input type="checkbox"/>	Enabled	CiscoLive

Admin User

RBAC
Policy

☒ Monitor If Monitoring + then Infra Monitoring + [Actions](#)

Cisco ISE

Settings Monitoring

Monitoring and Log Analytics Settings

Monitoring enables you to monitor a wide range of applications, system statistics, and key performance indicators (KPI) of all deployment nodes from a centralized console.

☒ Monitoring

Go to [Monitoring](#) [View](#)

Log Analytics provides a flexible analytics system for in-depth analysis of syslog data generated from different endpoints.

☐ Log Analytics

After Log
in
Dashboard

Log Analytics – Patch 1 Known Limitations

For your
Reference!

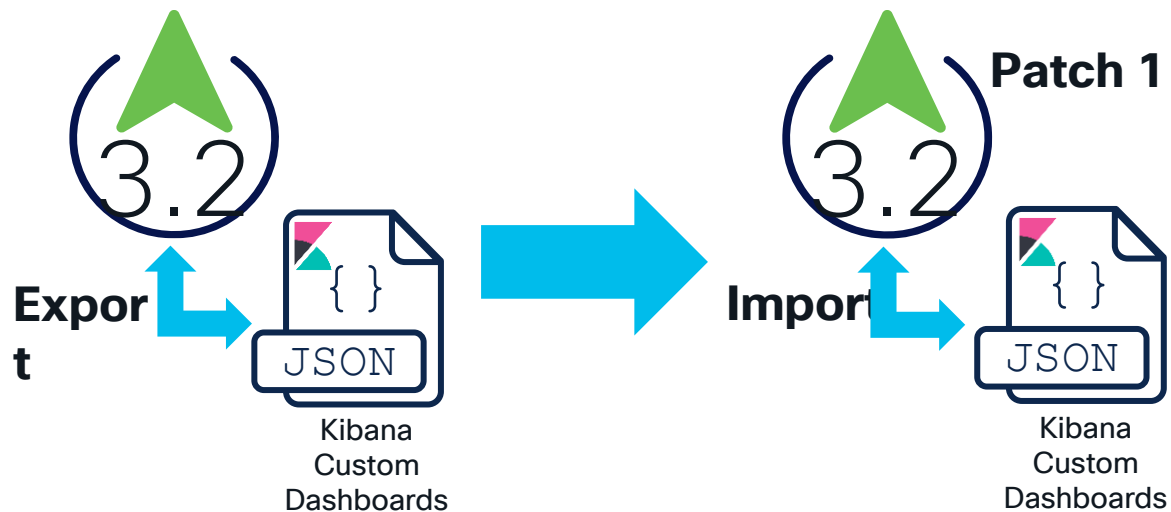


Limitation:

Custom Log Analytics dashboards that are created in ISE 3.2 are not displayed after you install **ISE 3.2 patch 1**

Solution:

Export the dashboards from Kibana and import them after patch install.





The bridge to possible

Thank you

CISCO *Live!*

