¿Qué hay de nuevo en ISE?

Nuevas funcionalidades, Versiones, Parches y Herramientas de monitoreo.

Comunidad de Cisco

Rubén De La Vega – Escalation Engineer Security TAC
Víctor Montes – Escalation Engineer Security TAC

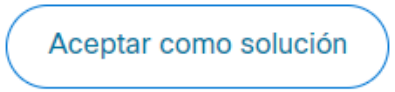
Martes 12 de Octubre de 2023

Conecte, Interactúe, ¡Colabore!

Soluciones

¡Acepte las soluciones correctas y felicite a quienes le ayudaron! Los foros de discusión tienen muchas entradas, de las cuales no todas cuentan con una respuesta correcta o válida.

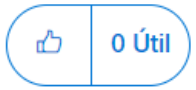
Ayude a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución”.

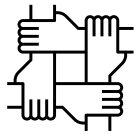


Agradecimientos

¡Resalte el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios además de ser una muestra valiosa de ¡nuestro reconocimiento!





Spotlight Awards

¡Nuevos ganadores cada periodo!

Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros. Los Premios Spotlight se otorgan mensualmente cada trimestre para destacar a los miembros más sobresalientes.

¡Ahora también puedes nominar a un candidato! Haga clic aquí

Community Spotlight awards

Rubén De La Vega

Escalation Engineer Security TAC

Ingeniero en Comunicaciones y Electrónica egresado del IPN; lleva cinco años en Cisco y empezó su recorrido en el equipo de TAC de Firewall, después de año y medio migró al equipo de ISE. Ahora tiene el rol de Ingeniero de Escalación enfocándose en casos críticos. Este año asistió al Cisco Live como Presentador obteniendo la presea de Presentador distinguido. Soy CCNA/DevNet Associate y SISE.

Víctor Montes

Escalation Engineer Security TAC

Egresado de la carrera de Ingeniería en Telecom por la UNAM en 2017. Forma parte de Cisco TAC desde 2018, desde entonces y hasta la fecha ha formado parte del equipo de AAA/ISE, donde actualmente tiene el rol de Escalation Engineer. Víctor cuenta con las certificaciones de CCNA Enterprise, DevNet Associate y también aprobó el examen Implementing and Configuring Cisco Identity Services Engine (SISE).

Descargue la presentación

https://bit.ly/CL2doc-oct23

slido

Join at

slido.com

#2507 190

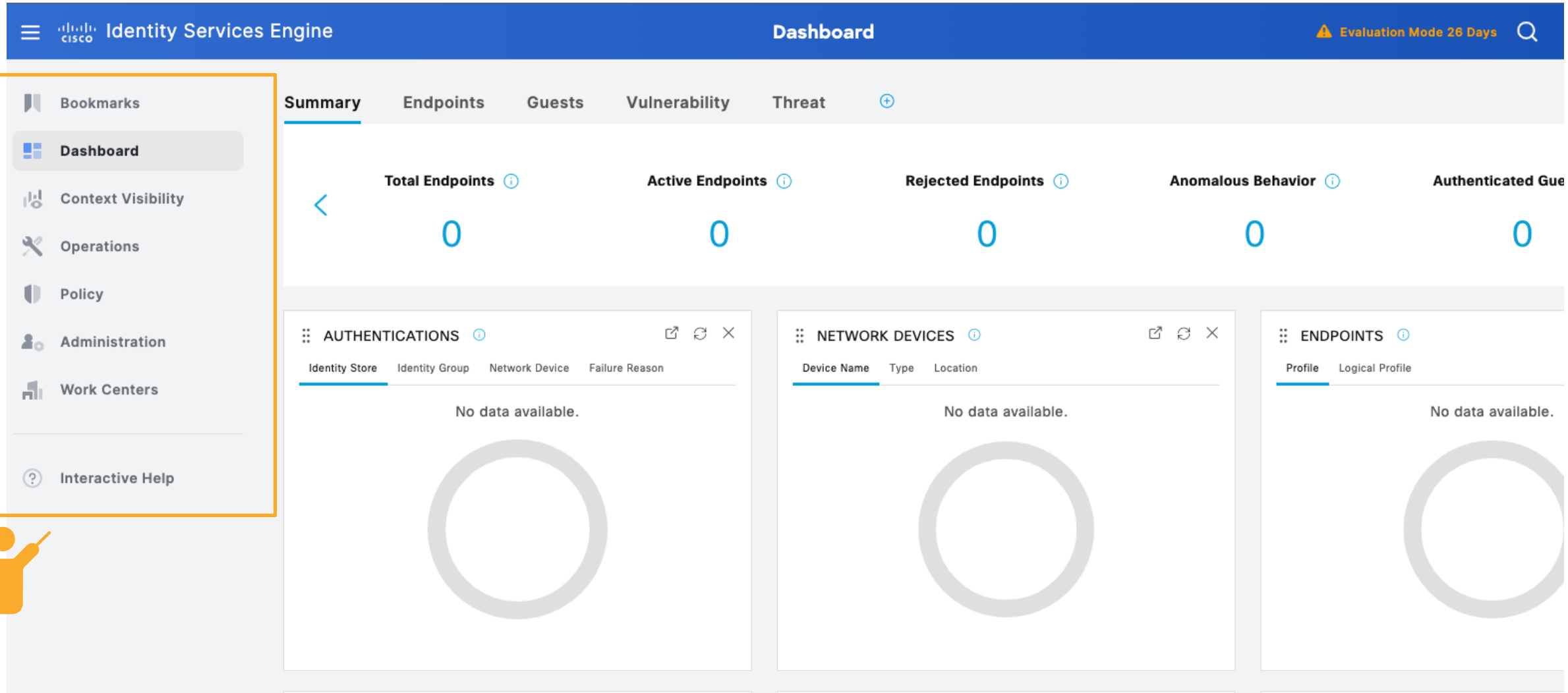
Passcode: **abdwyj**

Agenda

- ¿Qué es nuevo en ISE versión 3.3?
  - Nuevas funcionalidades
- Versiones de ISE y defectos destacables
  - Versiones End-Of-Life y End-Of-Support
  - Versión recomendada
  - Siguientes Parches para las versiones soportadas
  - Problemas actuales
- Monitoreando ISE por medio de System 360
  - Recorrido del System 360
  - Vistazo a Monitoring y Log Analytics

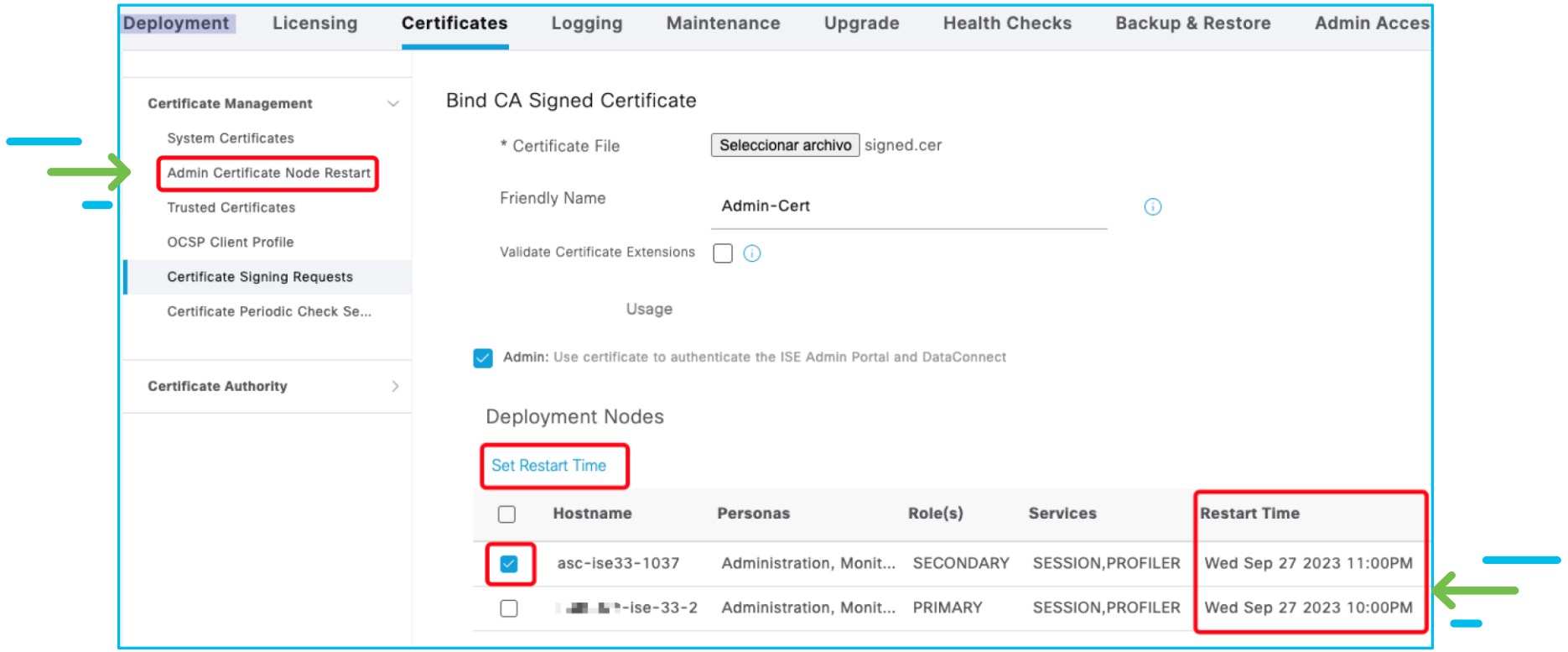
¿Qué es nuevo en ISE versión 3.3?

Cambio de la interface gráfica



Reinicio controlado de los nodos

- Cuando el certificado de Admin del PAN es cambiado, todos los nodos se reinician al aceptar el cambio del certificado
- 3.3 introduce una función donde se puede programar el reinicio de cada nodo
- Navega a **Administration > System > Certificates > Admin Certificate Node Restart**



Acceso a la Interfaz gráfica usando TLS 1.3

Opción para deshabilitar Ciphers específicos

- Navega a **Administration> System > Settings > Security Settings**

Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

☐ TLS 1.0 ☐ TLS 1.1 ☑ TLS 1.2 ☐ TLS 1.3

Manually Configure Cipher Settings

Enable the following setting to manually configure ciphers for communication with the following Cisco ISE components: admin UI, ERS, OpenAPI, secure ODBC, portals and pxGrid. A list of ciphers is displayed with allowed ciphers already selected. You can select and unselect ciphers as required.

☑ Manually configure ciphers list

☐	Name	TLS Version
☑	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS1.2
☑	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS1.2
☑	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS1.2

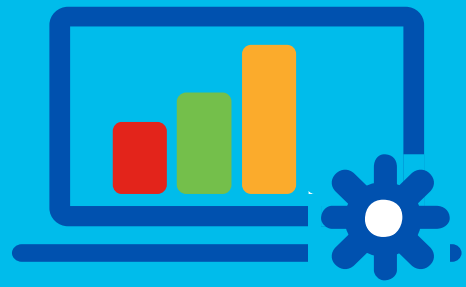
Soporte de IPv6 para Portales

Los portales soportados son:

- Sponsor Portal
- MyDevices Portal
- Certificate Provisioning Portal
- Hotspot Guest Portal
- Self-Registered Guest Portal

Soporte de IPv6 Agentless Posture

- Se soporta para Windows y MacOS



Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller

- Con esta feature se pueden obtener más atributos de los dispositivos Apple, Intel y Samsung
- Se pueden usar estos atributos para crear reglas de profiling.

DEVICE_INFO_DEVICE_FORM	PHONE
DEVICE_INFO_FIRMWARE_VERSION	WH6
DEVICE_INFO_MODEL_NUM	Samsung Galaxy S22+
DEVICE_INFO_OS_VERSION	Android 13
DEVICE_INFO_SALES_CODE	MXO
DEVICE_INFO_VENDOR_TYPE	SAMSUNG

Join at

slido.com

#2507 190

Passcode:

abdwyj

¿Cuál de las siguientes features es exclusiva de ISE 3.3?

A. IPV6 para Agentless Posture

0%

B. Agentless

0%

C. Posture para Windows 11

0%

Versiones de ISE y defectos destacables

End-of-life y End-of-Support

Software Maintenance:

A partir de esta fecha ya solo se trabaja en arreglar problemas por vulnerabilidades o defectos severos.

End of Support:

A partir de esta fecha, se deja de recibir soporte.

End of Life Notice:

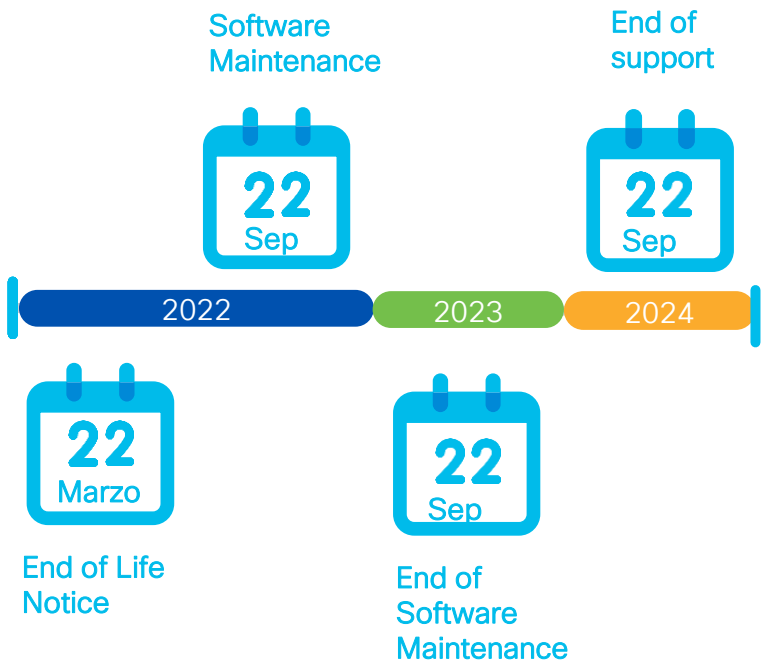
Fecha de publicación.

End of Software Maintenance:

El último día para que salga un parche de ISE, ya no se arregla ningún tipo de problema.

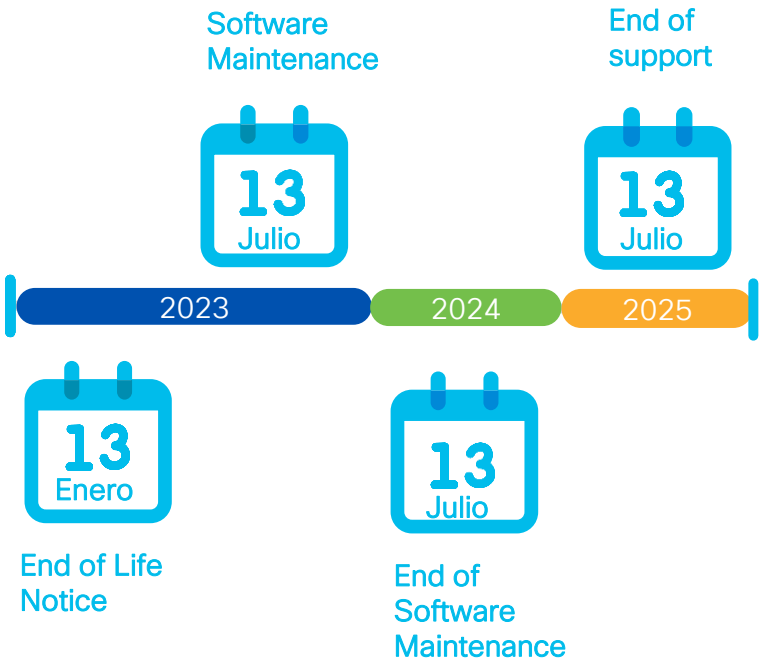
Time Line

ISE 2.7



- Último parche
  - ✓ Parche 10, 4 de Septiembre 2023

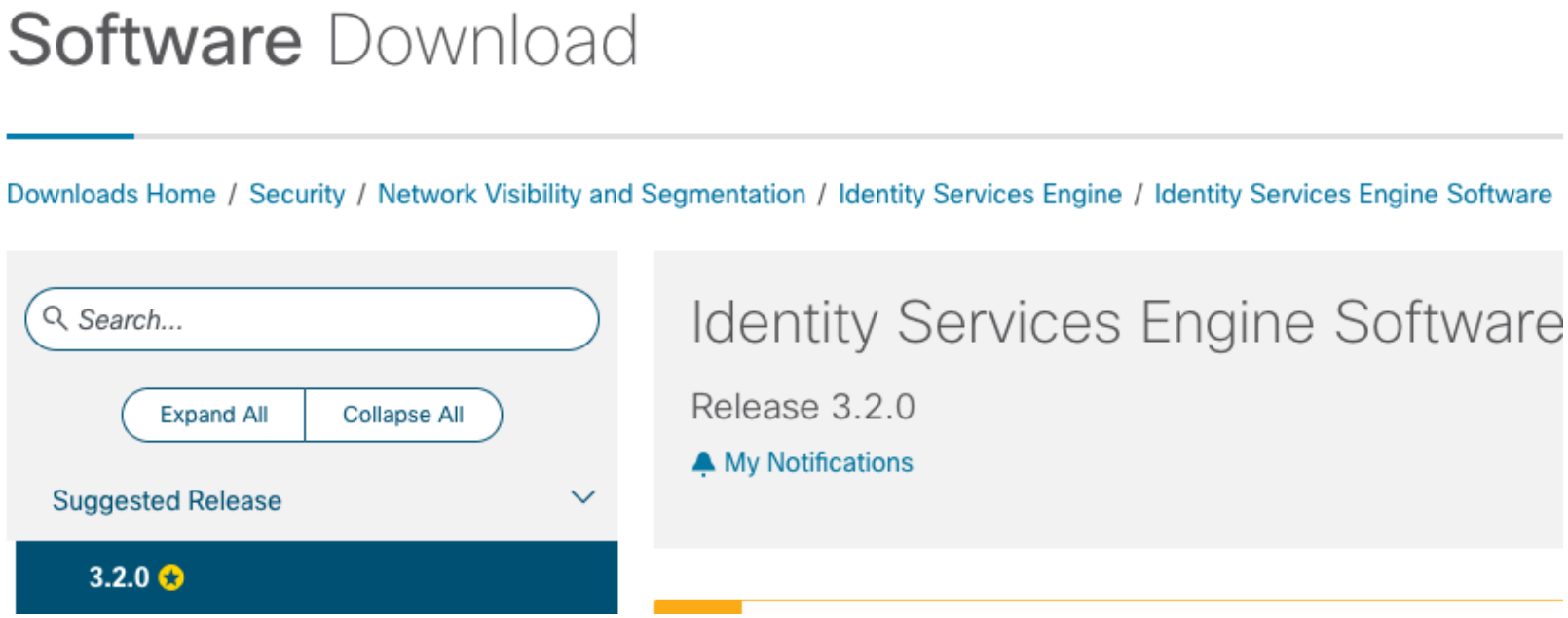
ISE 3.0



- Último parche por definir

Versión Recomendada

- En la página donde las versiones de ISE se encuentran, podemos encontrar una de ellas con una estrella dorada, eso quiere decir que es la versión recomendada por Cisco.
- Esta versión se vuelve recomendada una vez que el equipo de ingeniería analiza, prueba y confirma que es la mejor versión con base en la calidad del software, estabilidad y longevidad.
- Ejemplo:



Siguientes Parches

Versión	Parche	Fecha estimada
3.1	Parche 8	20 de Noviembre 2023
3.2	Parche 4	19 de Octubre 2023
3.3	Parche 1	20 de Diciembre 2023

Defectos

- **CSCwd45843 y CSCwd74531**

Problema
- Un error en el tamaño de un java heap introducido en ISE 2.7 Parche 2

Síntomas
- En general problemas de performance
- Memoria/CPU altos
- Tiempos de autenticación altos

Versiones reparadas
- 2.7 P8, 3.0 P7, 3.1 P5, 3.2 P1

Solución temporal:
- No existe
- Para este bug, se creó un HotFix universal que se encuentra en la página de descargas

Cuando se detecten estos síntomas, primero instalar el parche o el HotFix, si no lo soluciona, abrir un caso con TAC

File information

Cisco Identity Services Engine Software hot patch is to address CSCwc74531 (related to cached buffer cleanup) and CSCwd45843 (related to authentication step latency on multiple policy evaluation steps).

ise-apply-CSCwc74531_Universal_patchall-SPA.tar.gz

Advisories

Defectos

- **CSCwh08408-** ISE 3.3 Cannot Register New Nodes To Deployment Post Upgrade due to Node Exporter Password Not Found

Versiones afectadas
- 3.3

Síntomas
- Al registrar un nodo, la replicación fallará

Versiones reparadas
- 3.3 P1

Solución temporal:
- TAC debe implementar la solución entrando a Root

- **CSCwh28098-** ISE 3.2p3 CoA Disconnect is sent instead of CoA Push during Posture Assessment with RSD disabled

Versiones afectadas
- 3.2, 3.3

Síntomas
- Cuando el proceso de posture termina, ISE manda un COA Disconnect en lugar de COA Push

Versiones reparadas
- 3.2 P4, 3.3 P1

Solución temporal:
- Habilitar LSD/RSD

Defectos

- **CSCwh39008-** Not able to schedule or edit schedule for config backup

- Versiones afectadas
  - 3.1, 3.2, 3.3

- Síntomas
  - No se puede editar ni crear un nuevo backup programado

- Versiones reparadas
  - 3.1 P8, 3.2 P4, 3.3 P1

- Solución temporal:
  - Obtener un backup manual

- **CSCwh46669**- After admin certificate change, ISE is not restarting services if the Bond interface is configured

- Versiones afectadas
  - 3.2, 3.3

- Síntomas
  - El nodo Admin no se reinicia al cambiar el certificado de Admin si se cuenta con una interface Bond

- Versiones reparadas
  - 3.2 P4, 3.3 P1

- Solución temporal:
  - Reiniciar el equipo desde el CLI

Join at

slido.com

#2507 190

Passcode:

abdwyj

¿Cuándo debería de hacer upgrade?

A. Antes del End of Software Maintenance

0%

B. Después de la fecha de Out Of Support

0%

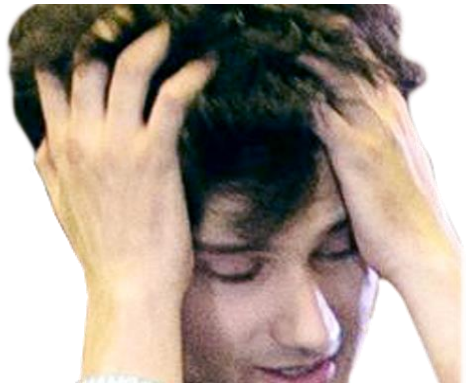
C. Cuando es publicado el documento de End Of Life

0%

Monitoreo de ISE por medio de System 360

Una problemática:

- Los administradores de ISE enfrentan gran dificultad al buscar tener una mejor visualización del rendimiento y métricas de la solución, pues los reportes que este es capaz de generar resultan complicados de leer y poco amigables.



- Dado que ISE carece de herramientas internas que permitan una visualización amigable de la información que este genera, se recurre al uso de herramientas externas para estos fines, lo cual conlleva costos y riesgos adicionales.

La Solución:

- A partir de la versión 3.2, ISE incorpora las funcionalidades de Monitoring y Log Analytics, herramientas internas que facilitan la visualización de métricas de rendimiento dentro de la solución, eliminando así la necesidad de recurrir a herramientas externas para estos fines.

- Este par de funcionalidades conforman lo que en ISE se conoce como **System 360. Al no recurrir a herramientas externas, también se reducen los riesgos potenciales que estas conllevan.**

System 360

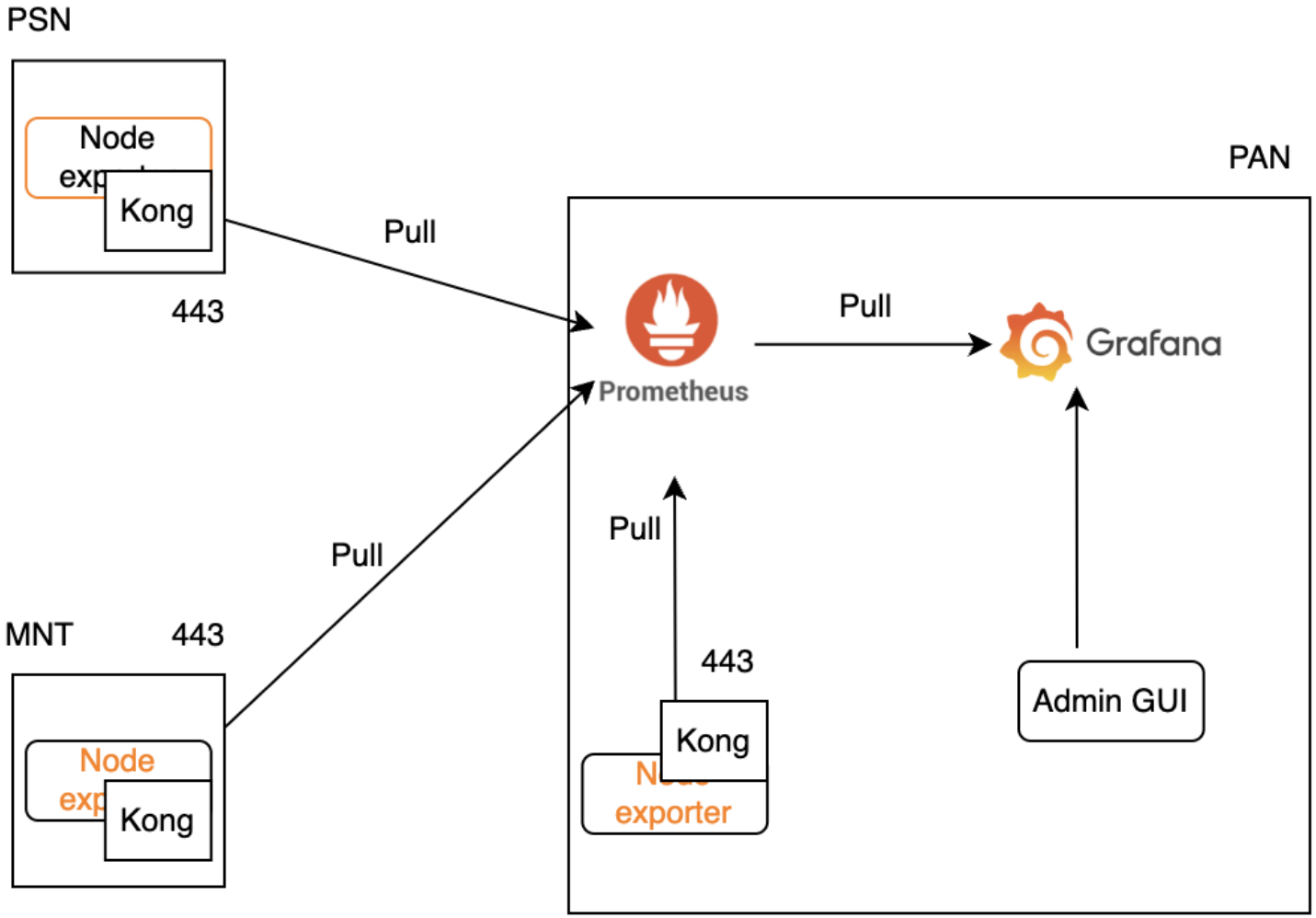
Monitoring

- Usa Grafana, una poderosa herramienta open-source para Monitoreo.
- Puede generar diversas representaciones gráficas usando como fuente información en tiempo real.

Log Analytics

- Emplea Kibana para su funcionamiento.
- Permite crear visualizaciones mucho más amigables a partir de mensajes de syslog e información no estructurada.

¿Cómo funciona Monitoring (Grafana) en ISE?



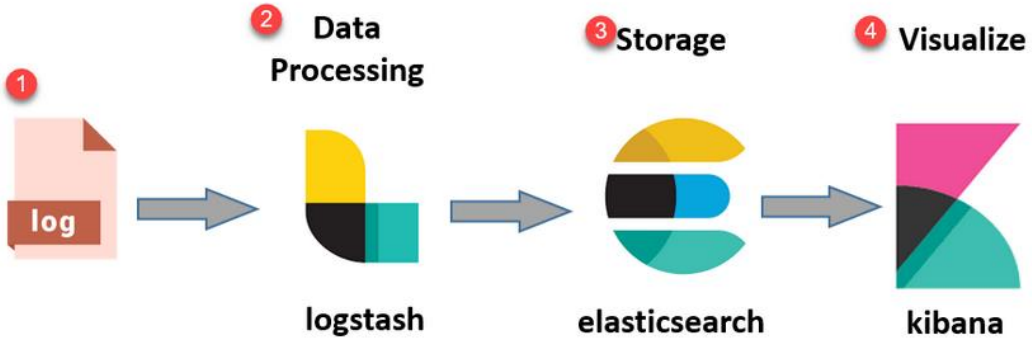
Puntos clave de Monitoring:

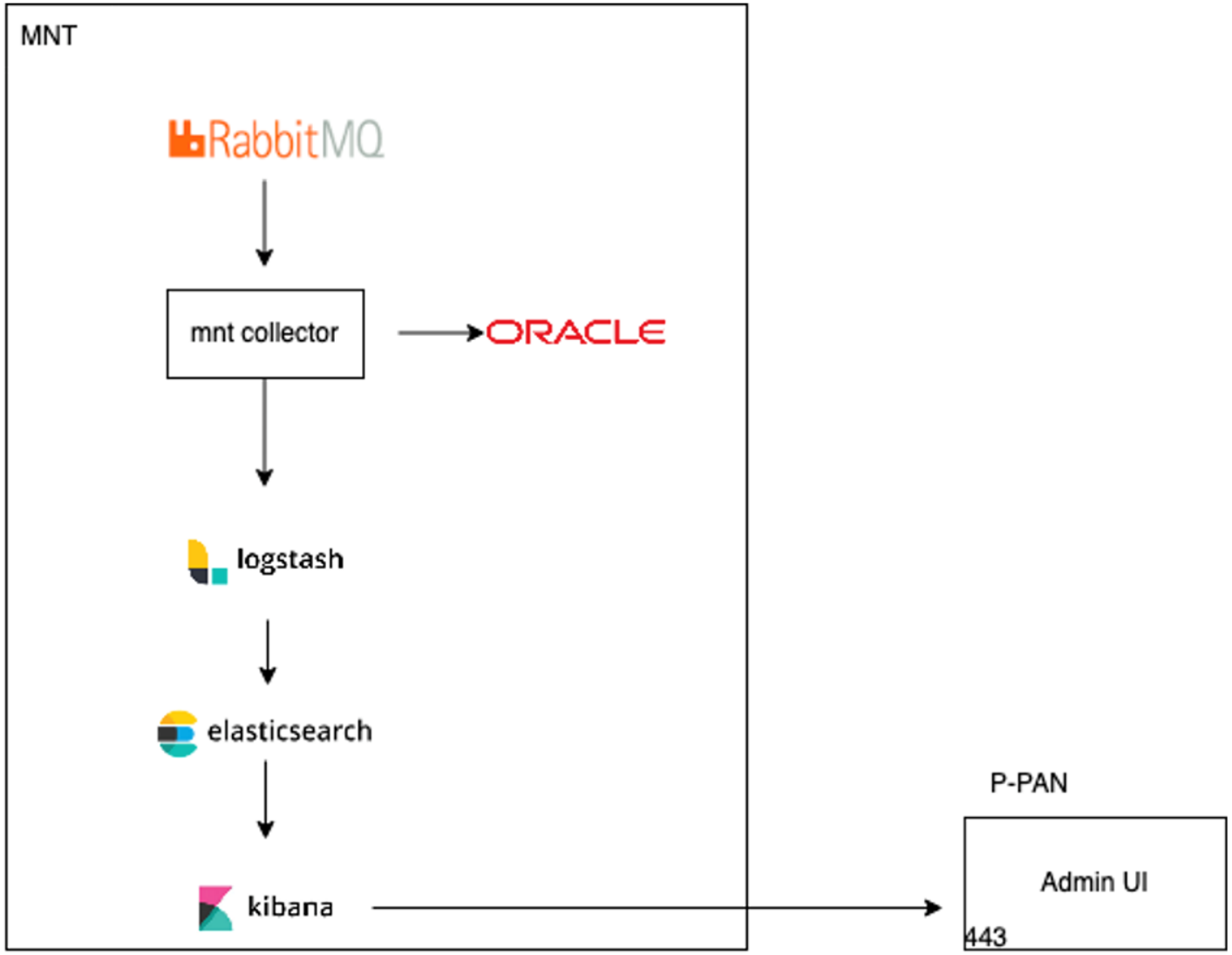
- ✓ Emplea 3 servicios para su funcionamiento:
  - ❖ ISE Node Exporter
  - ❖ ISE Prometheus Service
  - ❖ ISE Grafana Service
- ✓ Almacenamiento: Limitado a 7 días o 5GB de información. Al purgar, se empieza por la información más vieja. Por el momento, esta cantidad no es configurable.

Se requiere conectividad entre nodos a través del puerto 443.

ISE Monitoring			
Servicio	PAN	MNT	PSN
ISE Node Exporter	✓	✓	✓
ISE Prometheus Service	✓	✗	✗
ISE Grafana Service	✓	✗	✗

¿Cómo funciona Log Analytics (Kibana) en ISE?





Puntos clave de Monitoring:

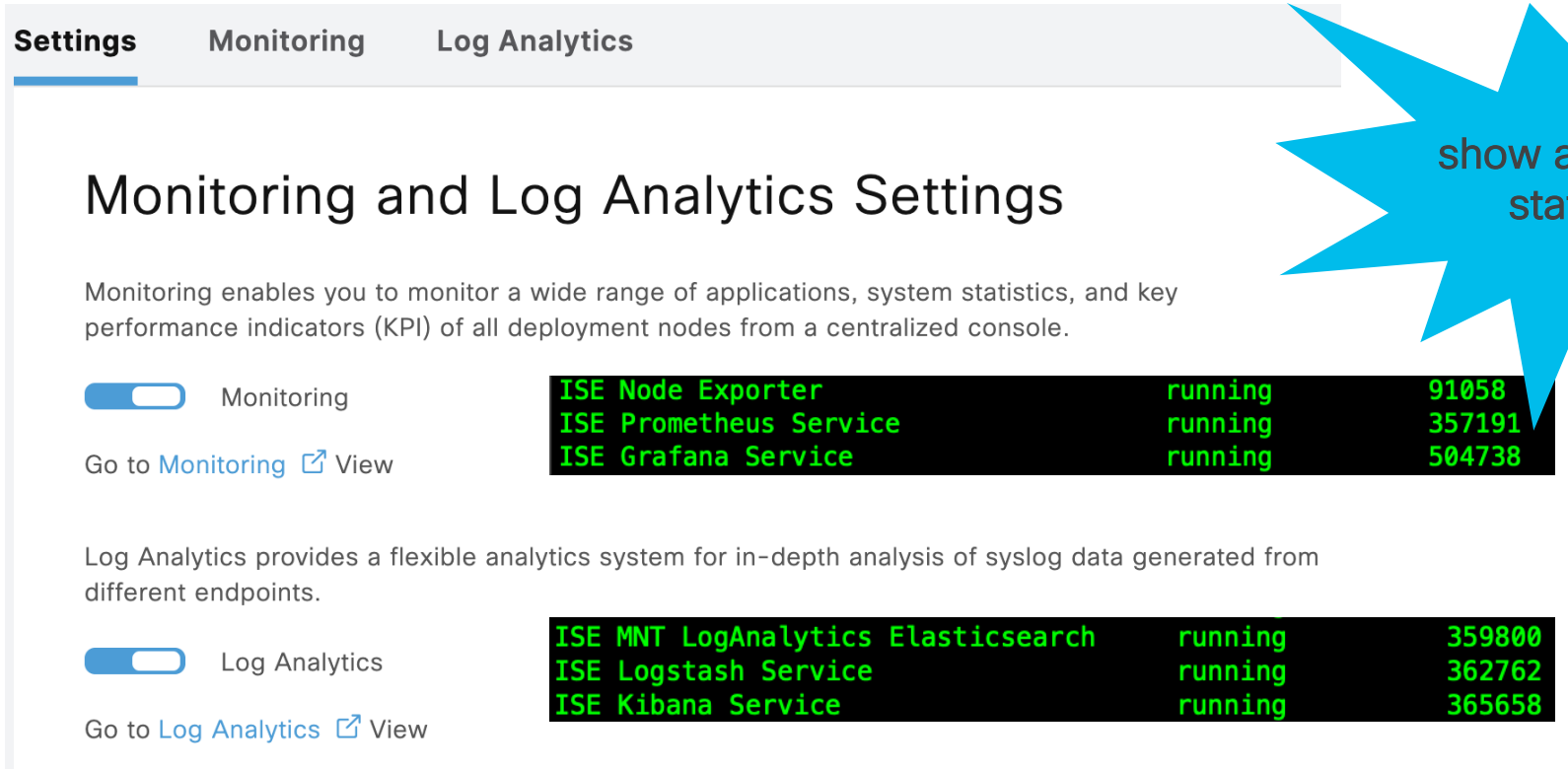
- ✓ Emplea 3 servicios para su funcionamiento:
  - ❖ ISE MnT LogAnalytics Elasticsearch
  - ❖ ISE Logstash Service
  - ❖ ISE Kibana Service
- ✓ Almacenamiento: Limitado a 7 días o 100GB de información. Al purgar, se empieza por la información más vieja.
- ✓ Esta purga de información no afecta a la almacenada en las bases de datas en Oracle.

Se requiere conectividad entre los nodos de Administración y Monitoreo a través del puerto 443.

ISE Log Analytics			
Servicio	PAN	MNT	PSN
ISE MNT Log Analytics Elasticsearch	✗	✓	✗
ISE Logstash Service	✗	✓	✗
ISE Kibana Service	✗	✓	✗

Habilitando las funcionalidades:

- Navegar al menú Operations > System 360 > Settings
- Desde este menú se puede habilitar cada funcionalidad de forma diferente.



show application status ise

```
ISE Node Exporter                   running          91058
ISE Prometheus Service              running          357191
ISE Grafana Service                 running          504738
```

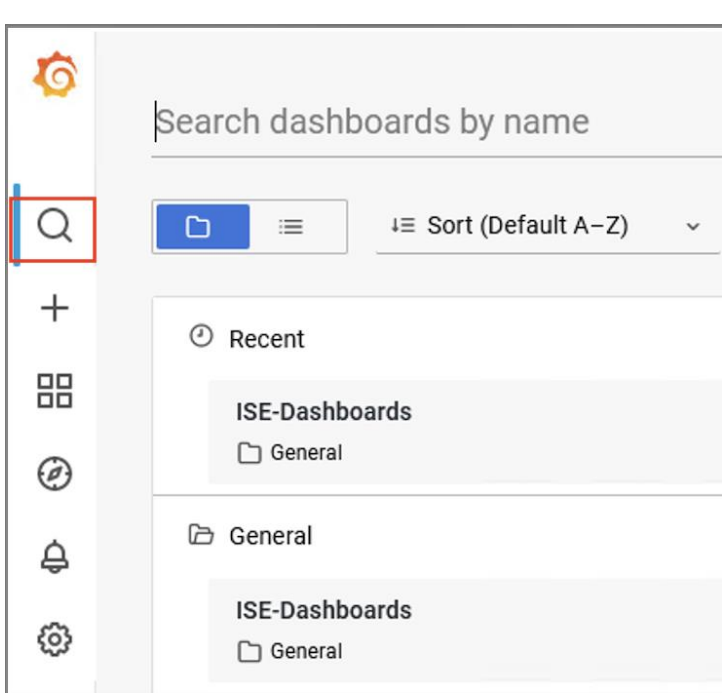
```
ISE MNT LogAnalytics Elasticsearch  running          359800
ISE Logstash Service                running          362762
ISE Kibana Service                  running          365658
```

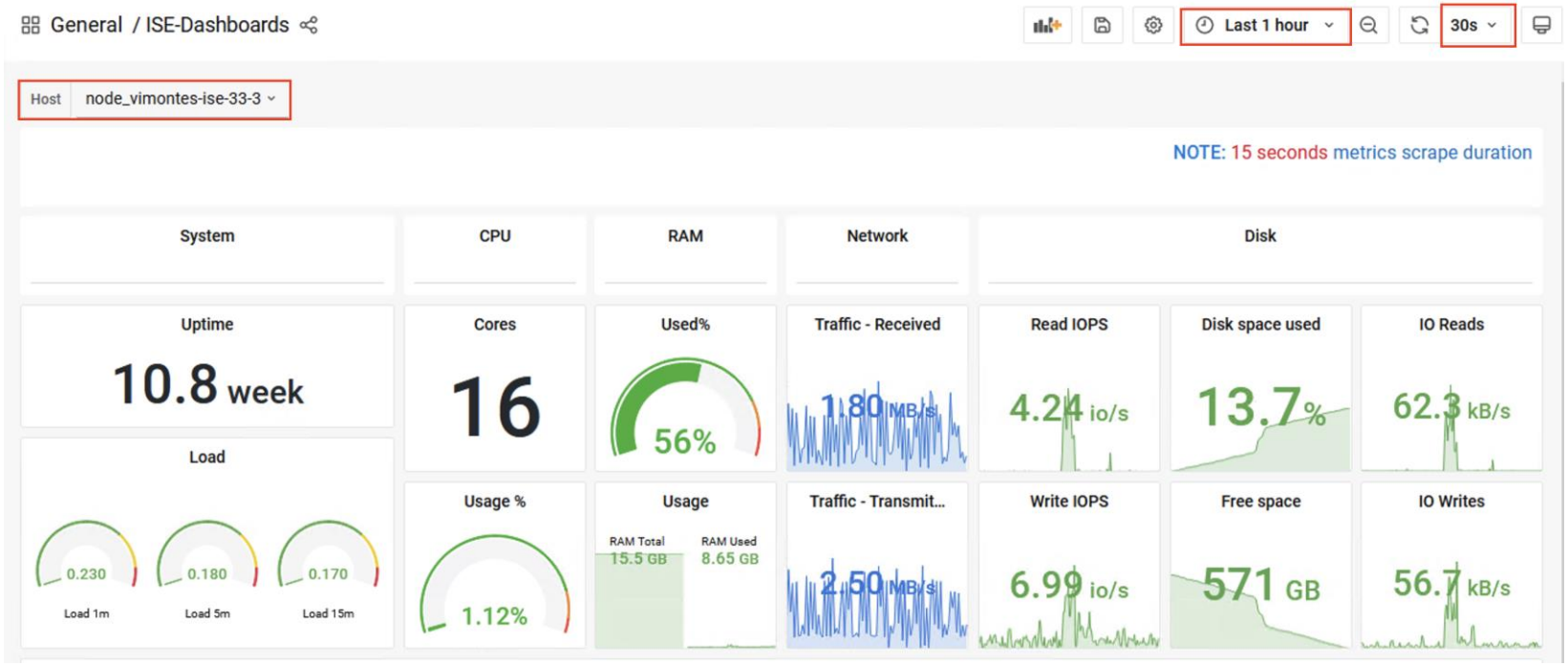
TIP

El estado de estos servicios depende de las personas habilitadas en el nodo que se revise

Dashboard por defecto – Monitoring

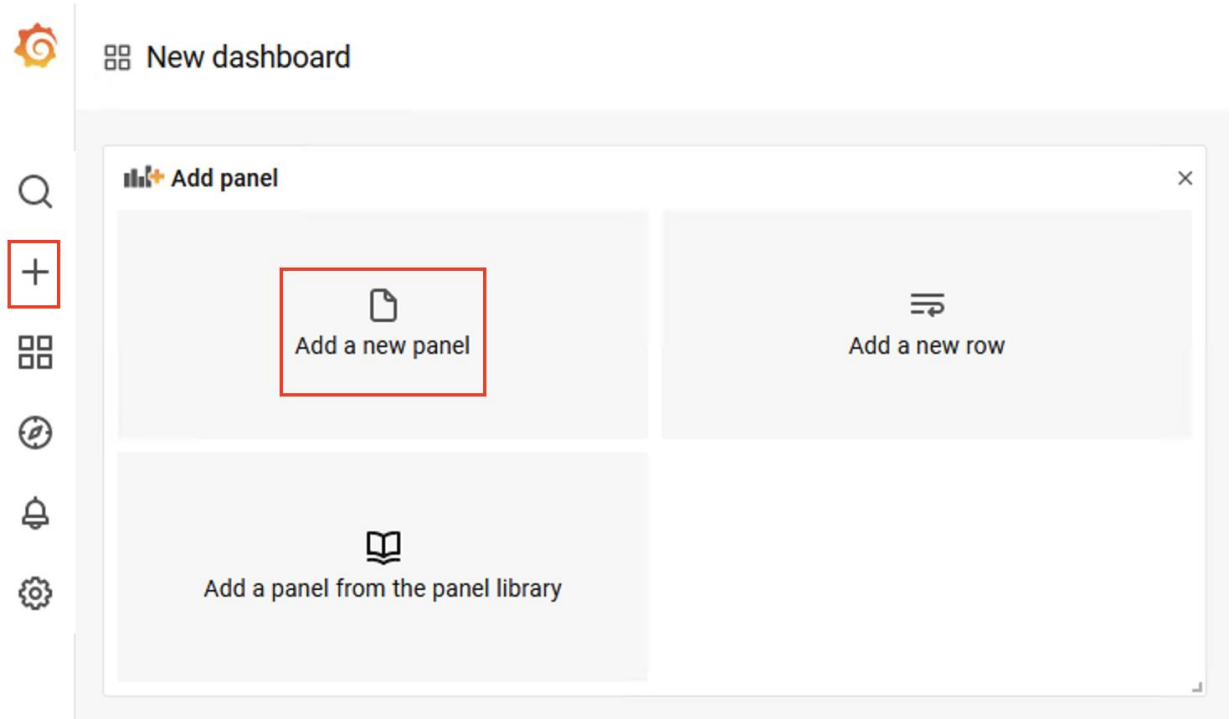
- ISE incluye por defecto un dashboard que puede mostrar las métricas de rendimiento en todos los nodos del deployment.
- Navegar al menú Operations > System 360 > Monitoring

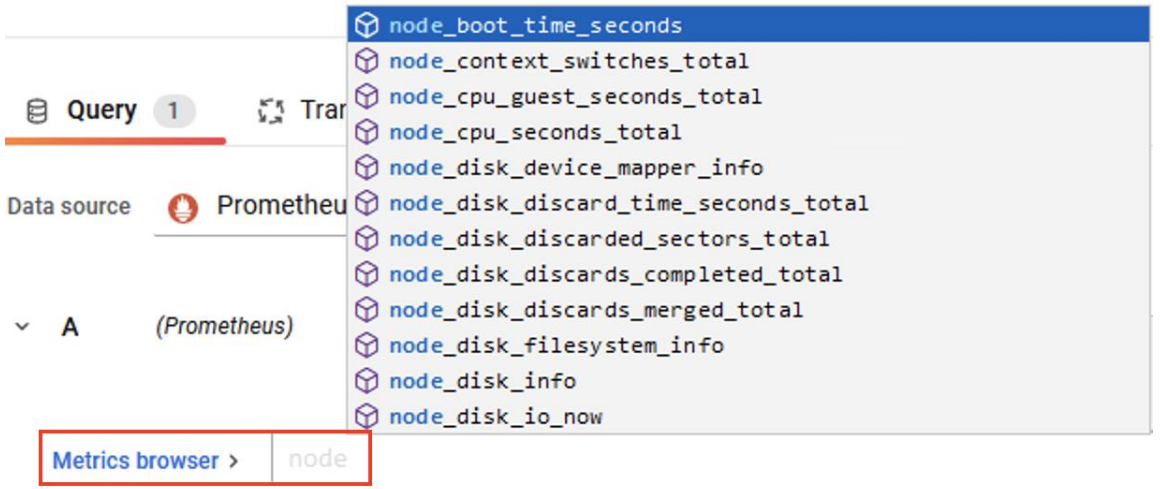




Dashboards Personalizados- Monitoring

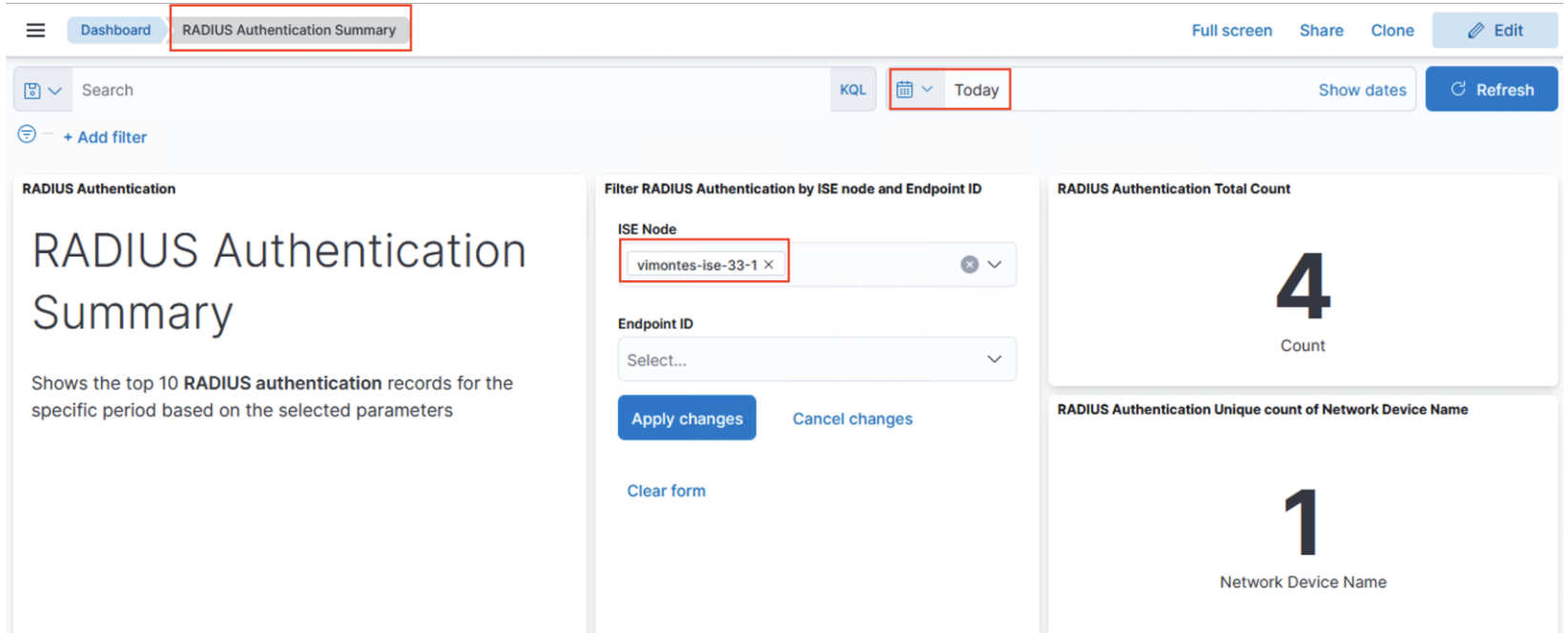
- Navegar a Operations > System 360 > Monitoring
- Dar clic en el “+” en el menú de lado izquierdo
- Seleccionar Add a new panel
- Dar clic en Metric-browser. Tras escribir “node” se desplegarán todas las métricas colectadas por el node exporter.

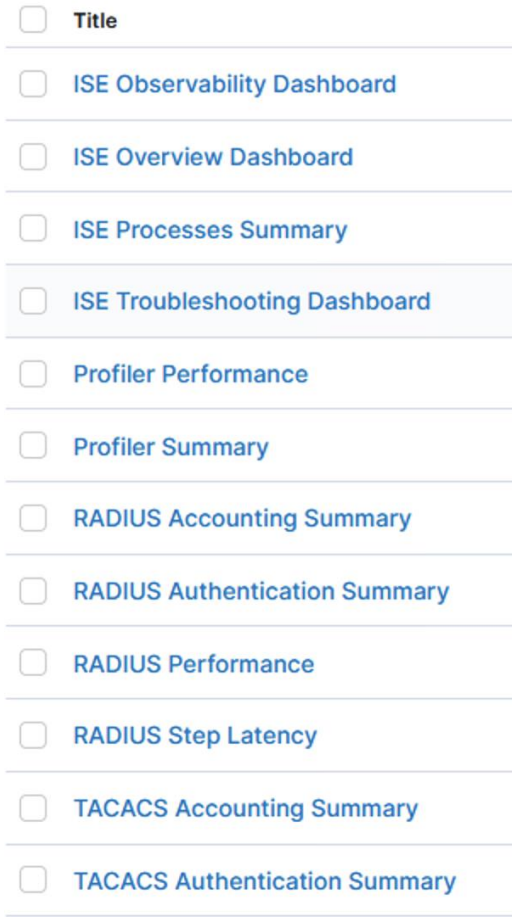




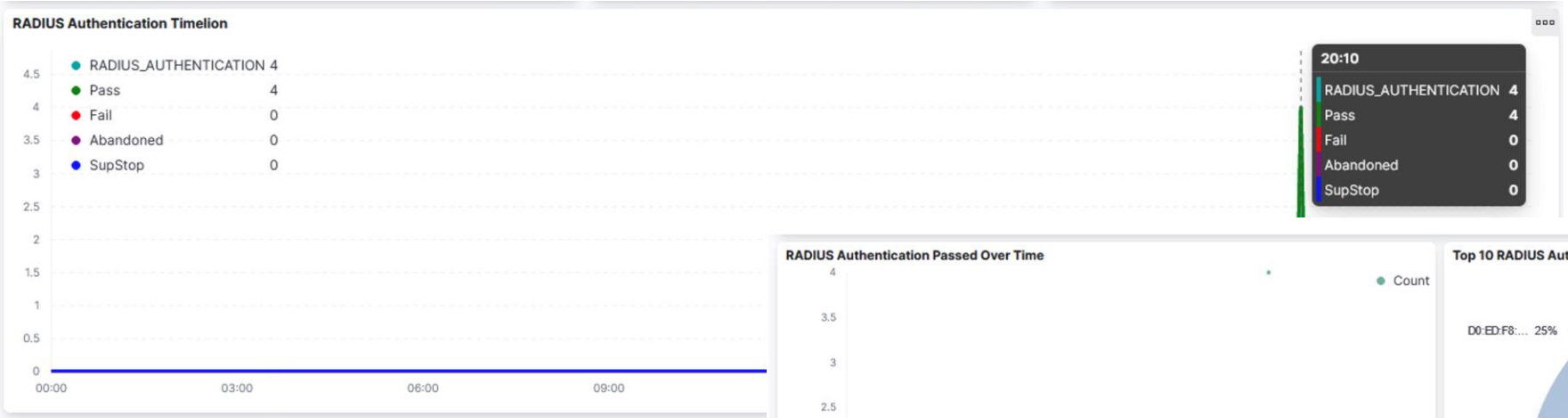
Dashboards por defecto – Log Analytics

- Al igual que con Monitoring, se incluyen dashboards por defecto, estos son referentes a información de RADIUS, TACACS y métricas del ISE.
- Para acceder, navegar a Operations > System 360 > Log Analytics



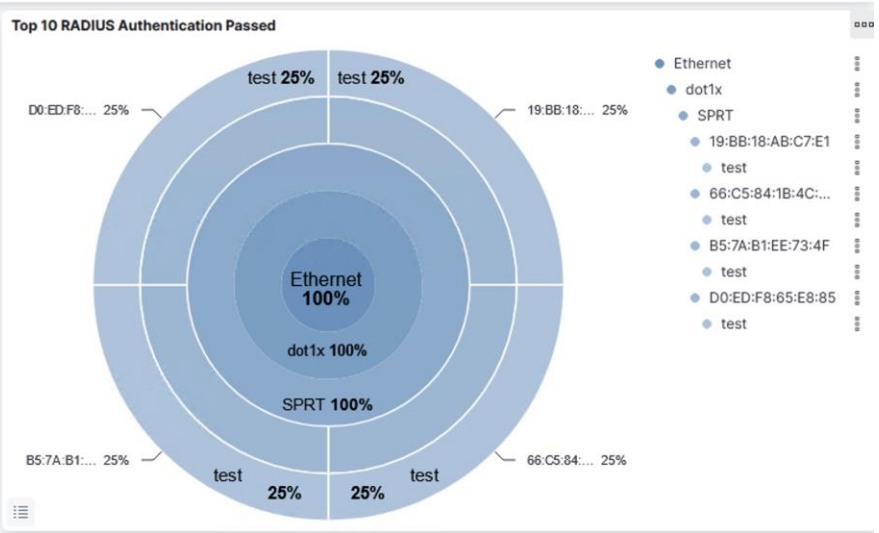


Dashboards por defecto – Log Analytics



RADIUS Authentications By Day Table

Date	Passed	Failed	Total count
2023-10-04	4	0	4



Top 10 RADIUS Authentication Passed by Date (More Info)

Date	ISE node	Endpoint ID	User Name	NAS PORT TYPE	Network Device ...	Authentication ...	Count
Oct 4, 2023 @ 20:11:16.855	vimontes-ise-33-1	19:BB:18:AB:C7:E1	test	Ethernet	SPRT	dot1x	1
Oct 4, 2023 @ 20:12:09.430	vimontes-ise-33-1	D0:ED:F8:65:E8:85	test	Ethernet	SPRT	dot1x	1
Oct 4, 2023 @ 20:12:39.251	vimontes-ise-33-1	B5:7A:B1:EE:73:4F	test	Ethernet	SPRT	dot1x	1
Oct 4, 2023 @ 20:12:40.473	vimontes-ise-33-1	66:C5:84:1B:4C:9D	test	Ethernet	SPRT	dot1x	1

Dashboards Personalizados – Log Analytics

- Al igual que los dashboard de Monitoring, también es posible configurar dashboards desde cero, este proceso se describe de forma muy detallada en el siguiente documento:

- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/220863-understand-log-analytics-elk-stack-on-ci.html#toc-hld--1976585706

Es posible modificar los dashboards incluidos por defecto y guardar los cambios, sin embargo, si se quisiera regresar al dashboard original, la única forma de lograrlo es el reinicio de fábrica de ISE por completo.

Join at

slido.com

#2507 190

Passcode:

abdwyj

¿Qué aplicación debo instalar para usar la herramienta de monitoreo en ISE?

A. Ninguna ya que la herramienta está instalada en ISE por defecto

0%

B. Graphana

0%

C. Instalar el último parche disponible

0%

Preguntas y respuestas

¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar ¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 20 de octubre de 2023

https://bit.ly/CL2ama-oct23

Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.

Nuestras Redes Sociales

LinkedIn

Cisco Community

Twitter

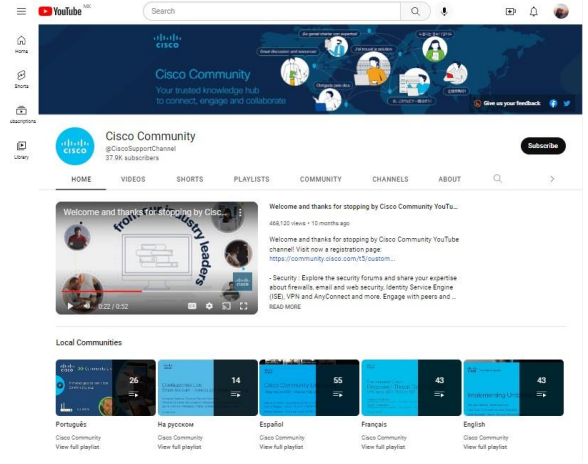
@CiscoCommunity

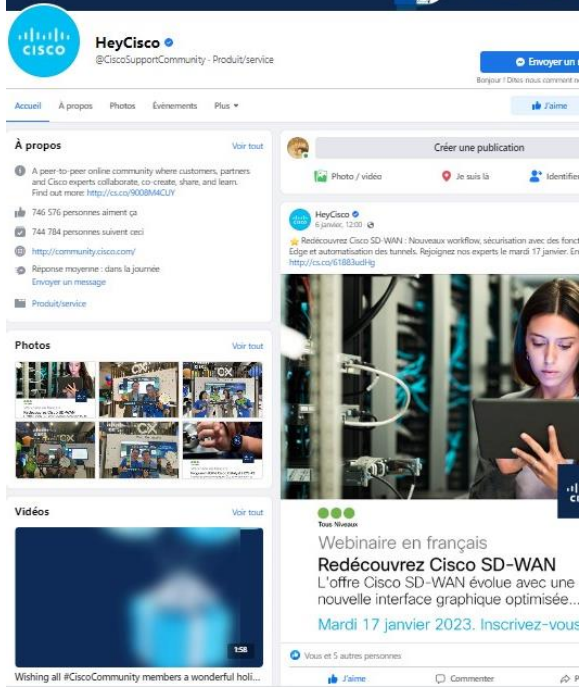
YouTube

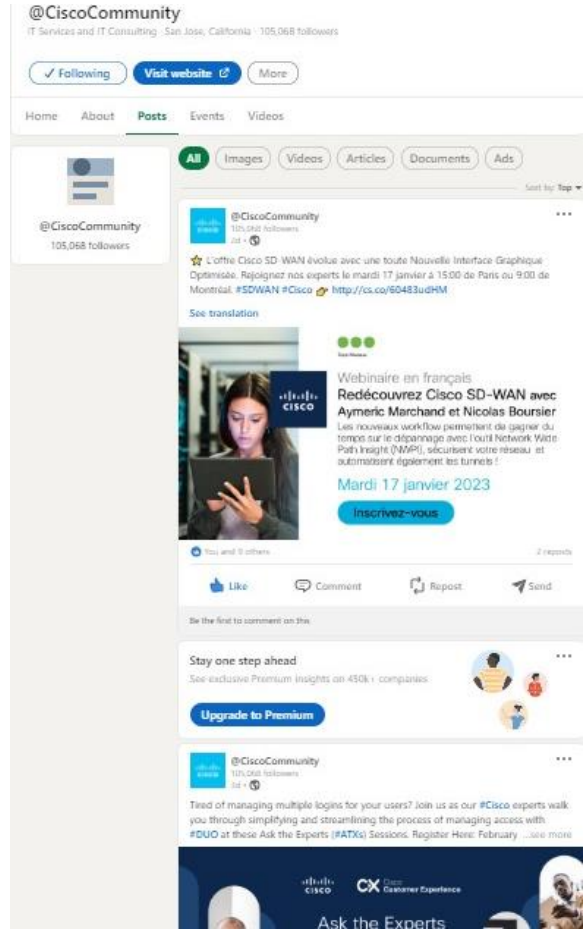
CiscoSupportChannel

Facebook

CiscoSupportCommunity







The bridge to possible