

SIEMENS
Ingenuity for life

V1.0 SP1

2020/02

SINEC NMS V1.0 SP1

Network Management System

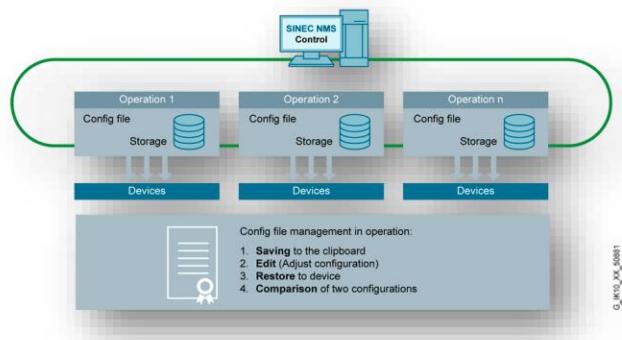
Restricted © Siemens 2020

siemens.com/sinec-nms

Update

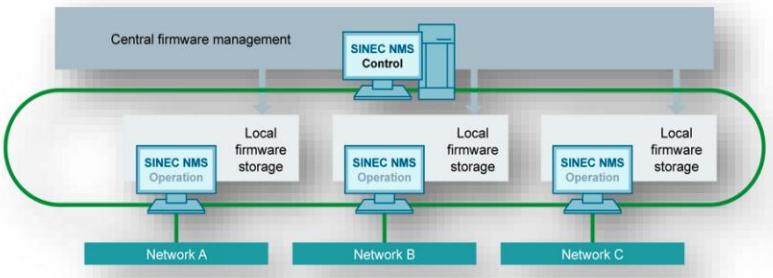
Valor añadido de SINEC NMS

Copias de seguridad programadas

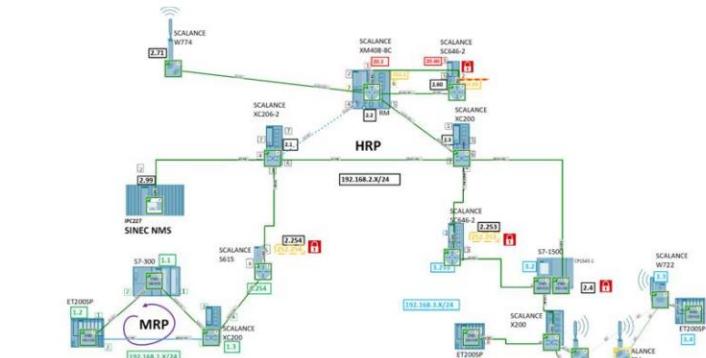
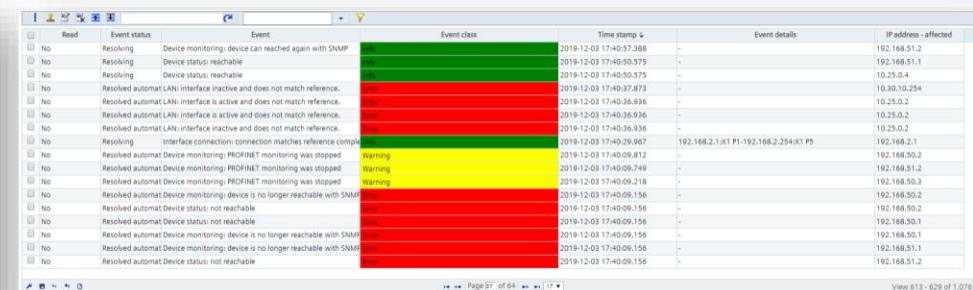
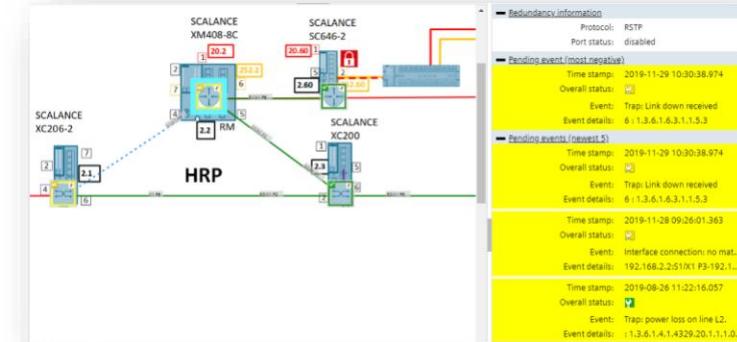


eventos de rojo

Actualizaciones de firmware masivas

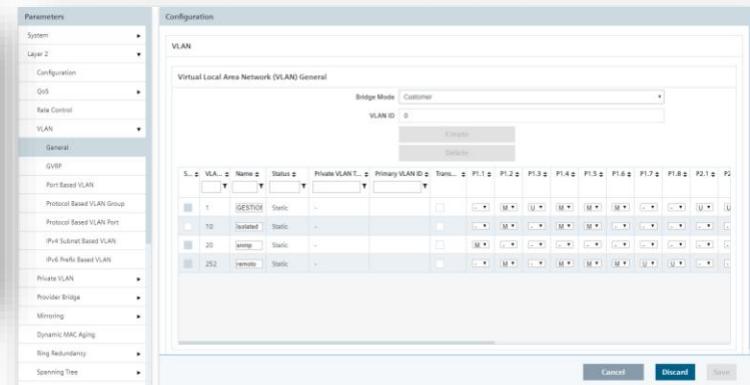


Informes del estado de red



Configuración

Políticas / copias de seguridad



SINEC NMS

Piedras angulares de un sistema de gestión de red

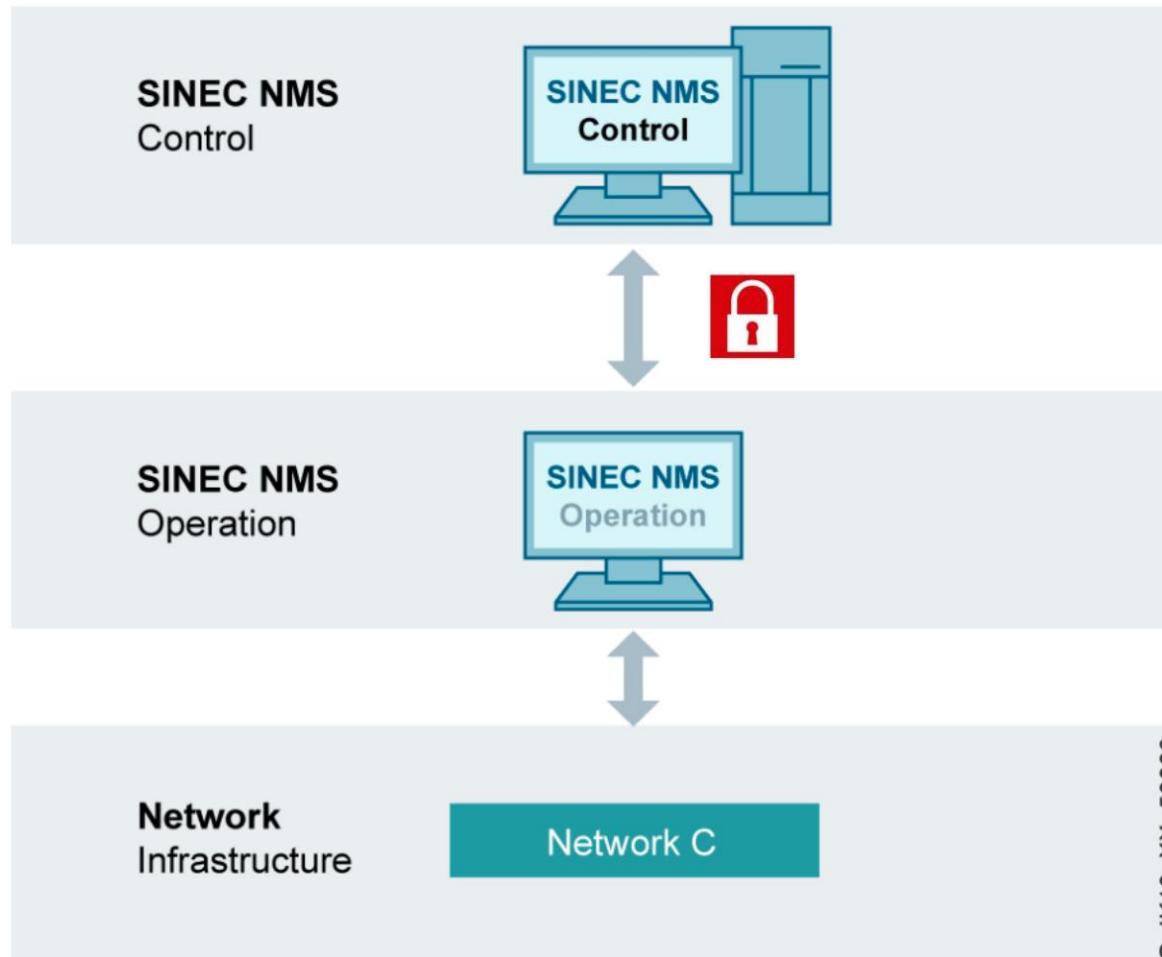
SIEMENS
Ingenuity for life



SINEC NMS

Sistema de gestión de red distribuida

SIEMENS
Ingenuity for life



Control SINEC NMS:

- Gestión de hasta 25 Operaciones SINEC NMS
- Resumen del estado general de las redes monitoreadas
- Lista de inventario central de todos los dispositivos en la red
- Gestión de archivos de firmware en la base de datos central
- Configuración basada en políticas en todas las operaciones
- Creación programada y automática de informes centrales (disponibilidad, inventario)

SINEC NMS Control / Operación:

- Las operaciones deben darse a conocer mediante certificado en el Control (fideicomiso relación)
- La comunicación de datos se realiza encriptada después de la inicialización del Operación en el Control
- Mín. Ancho de banda de red de 100 Mbps entre SINEC NMS Control y Operación SINEC NMS

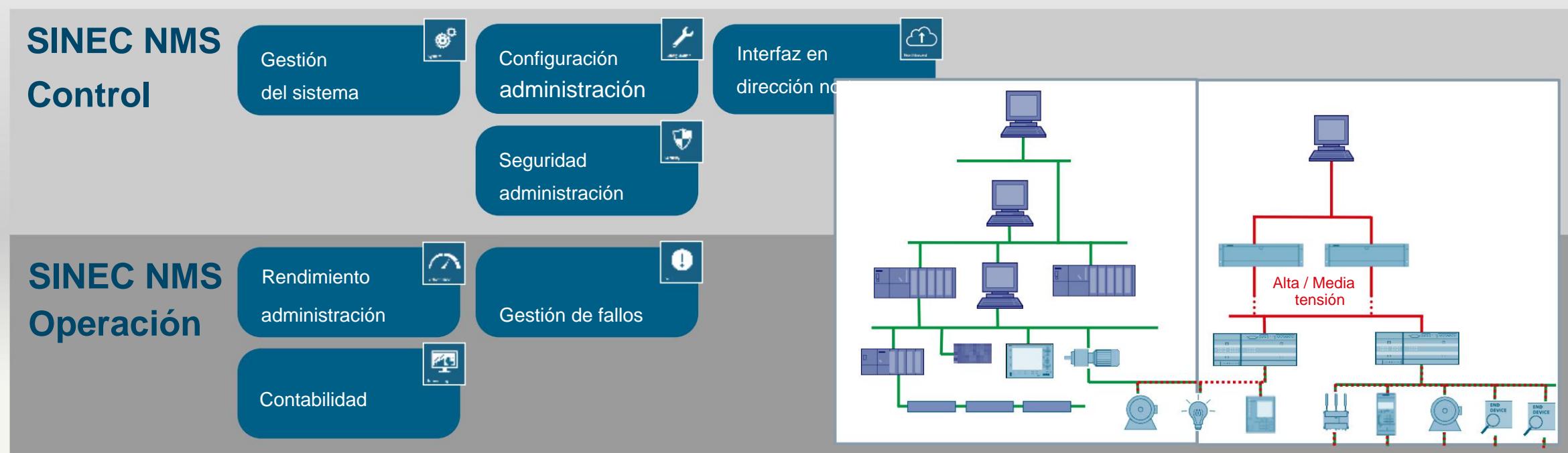
Operación SINEC NMS:

- Licencias para 50, 100, 250 o 500 dispositivos (se pueden agregar hasta un máximo de 500)
- Representación topológica de la infraestructura de red
- Configuración basada en políticas a nivel operativo
- Copia de seguridad/restauración/comparación y edición de configuraciones de dispositivos

SINEC NMS

Arquitectura – Entrada

SIEMENS
Ingenuity for life



SINCEC NMS

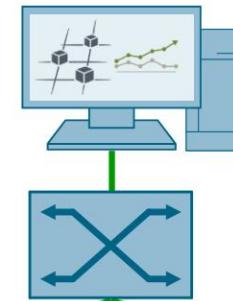
Escenarios de gestión

SIEMENS
Ingenuity for life

Escenarios de gestión

Nodo único

Control
y
Operación

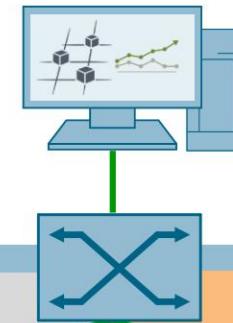


Nodo múltiple

Control

Operación A

Operación B



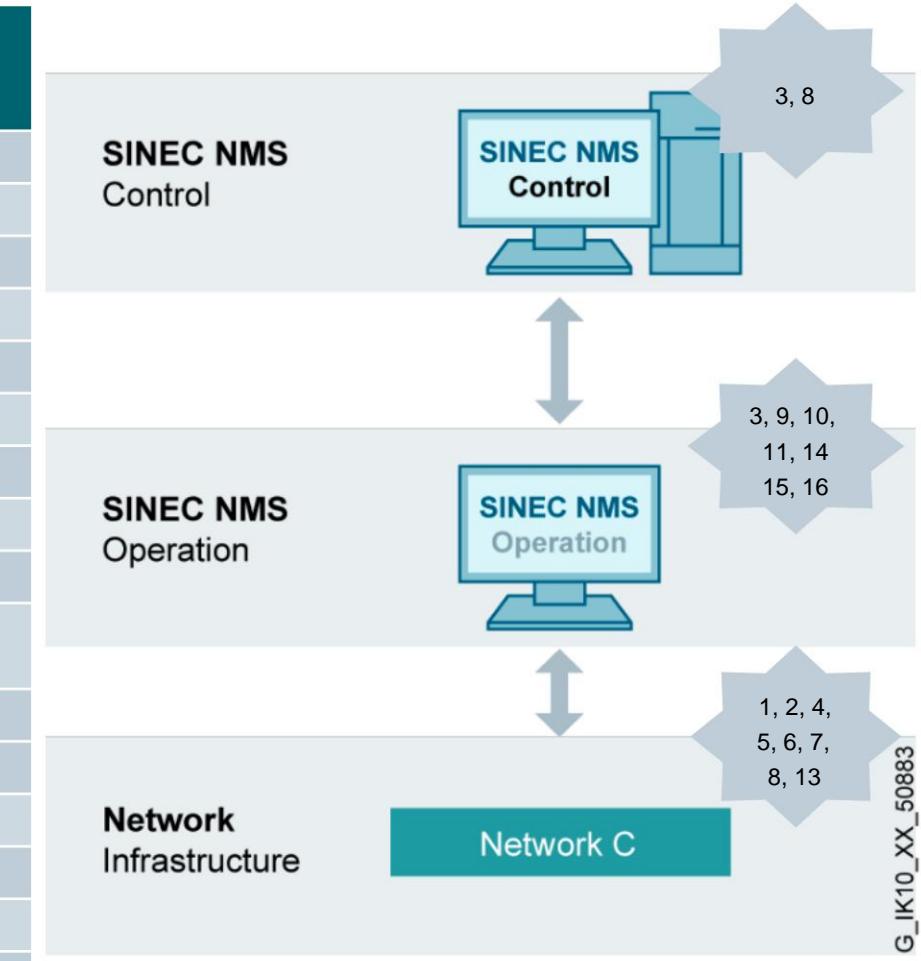
La gestión de red está instalada en una PC con Operación y Control.

La gestión de la red tiene un Control central y Operaciones dedicadas.

SINEC NMS

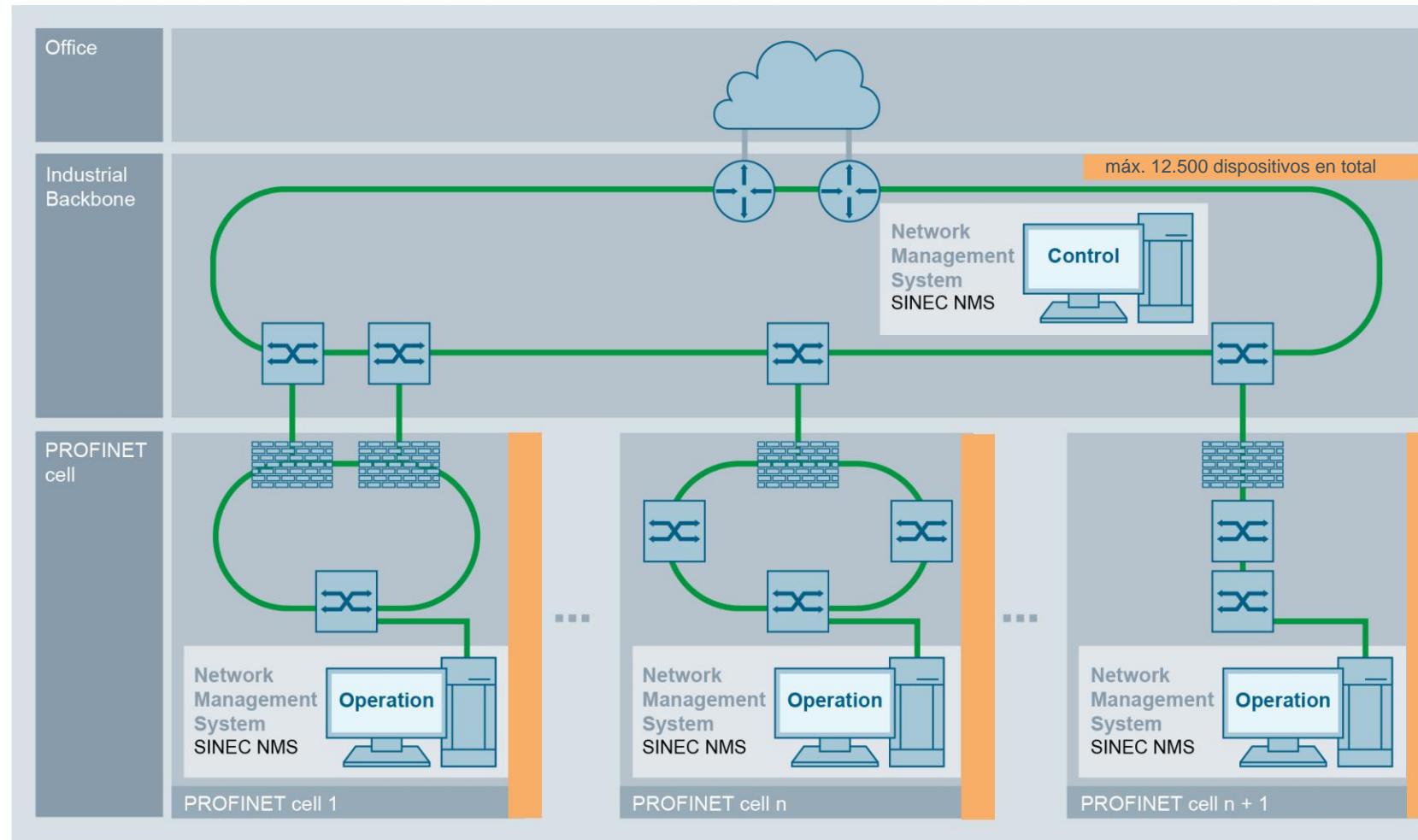
Descripción general de los puertos TCP relevantes

Puertos estándar de identificación	Descripción	Protocolo de transmisión relacionado	Configurabilidad
1 22	Shell seguro (SSH)	TCP	No
2 23	Telnet	TCP	No
3 25	SMTP	TCP	sí
4 69	TFTP	UDP	No
5 102	Comunicación SIMATIC S7	TCP	No
6 161	SNMP	UDP	No
7 162	Trampas SNMP	UDP	No
8 443	HTTPS (Servidor web SINEC NMS Control)	TCP	No
9 4841	Servidor OPCUA	TCP	sí
10 4897, 4998, 4999, 5671, 15671	Comunicación interna entre Control y Operación	TCP	No
11 5432, 5433	POSTGRESQL	TCP	No
12 8443	HTTPS (Servidor web SINEC NMS Operation) TCP		sí
13 34964, 49152-65535 PROFINET „leer registro“		UDP	No
14 49113	Latido del corazón	TCP	No
15 49131	FTP seguro	UDP	No
16 49132	Servicio de información de Internet (IIS)	TCP	No



Desafíos que necesitan ser resueltos de acuerdo a la Estándar de seguridad informática industrial IEC 62443

SIEMENS
Ingenuity for life



No se conocen todos los activos

Firmwares no actualizados

Sin endurecimiento del dispositivo (configuración de seguridad)

Sin estrategia de copia de seguridad y recuperación

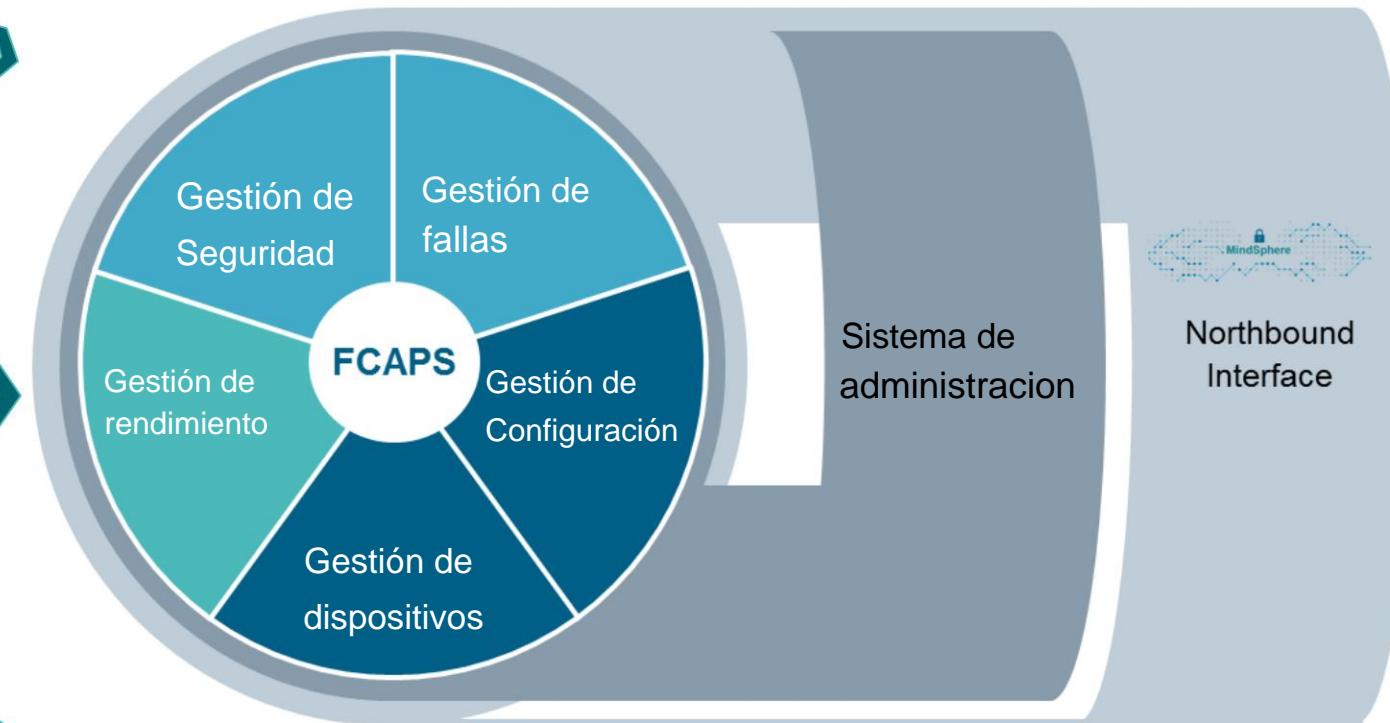
Configuración insegura se utilizan protocolos

Solo cuentas de usuario locales, sin políticas de contraseña

SINEC NMS

Pilares de un Sistema de Gestión de Red

SIEMENS
Ingenuity for life



Gestion de Fallos



Gestion de Fallos

Monitorización de la red

- Además de utilizar SNMP (Protocolo Simple de Gestión de Red), también es posible acceder directamente a los controladores SIMATIC (S7-300/S7-400) o acceder a los participantes de PROFINET a través de "read data record" (leer el registro del dato).
- SIMATIC S7-1200 y S7-1500 se detectan y leen principalmente a través de SNMP.
- Estadísticas puertos: opción de evaluación central de la red sobre la utilización de puertos individuales en los dispositivos: número de telegramas recibidos, enviados y rechazados.

Gestión de Diagnóstico

- Se utiliza una amplia gama de mecanismos (diagnósticos de DCP, ICMP, ARP, SNMP, PROFINET/SIMATIC) para recopilar y archivar centralmente el diagnóstico de los datos de todos los participantes de la red.
- Los estados de diagnóstico se informan como eventos, se asignan a los dispositivos correspondientes y se resaltan en color en la lista de dispositivos y en la topología. Esto permite detectar fallos.

topología

- La topología de planta se lee, representa y monitoriza automáticamente para detectar cambios (topología de referencia).
- El tipo de medio, redundancia y VLAN se representan gráficamente.
- Los cambios de topología (tool changers) se pueden monitorear sin alterar los mensajes de error. • Al estructurar la topología de red entera en vistas diferentes se puede crear jerarquías topológicas: para la conveniente localización.

SINEC NMS V1.0

Caso de uso: diagnóstico de red

Tarea

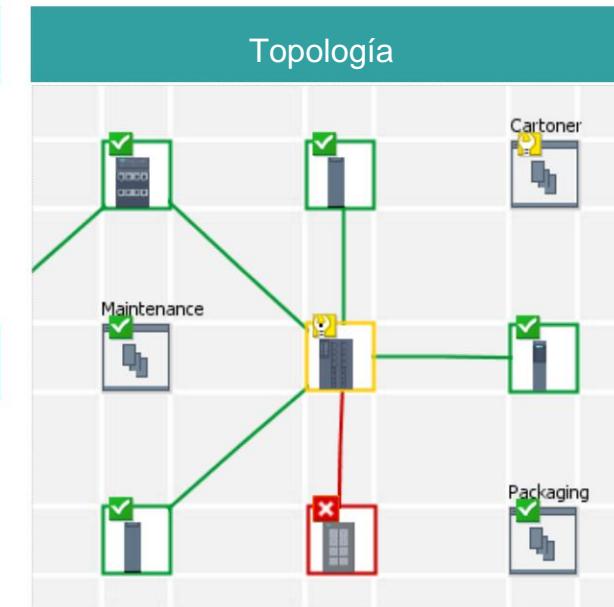
Los estados de diagnóstico actuales e históricos de los componentes monitoreados deben estar claramente representados.

Solución

Cada mensaje de diagnóstico determinado se representa rápidamente en la interfaz. El estado de diagnóstico puede así adquirirse y localizarse fácilmente.

Beneficios

Sólo una herramienta única y completa para el diagnóstico



Lista de eventos		
Ereigniszustand	Ereignis	Ereignisklasse
Auflösend	LAN: Schnittstelle ist aktiv und entspricht der Referenz.	Information
Automatisch aufg.	LAN: Schnittstelle ist inaktiv und entspricht nicht der Referenz.	Fehler
Anstehend	Geräteüberwachung: SIMATIC-Überwachung wurde gestoppt	Warnung
Auflösend	Schnittstellen-Auslastung: Normale Empfangsrate (Full-Duplex)	Information
Auflösend	Geräteüberwachung: SIMATIC-Überwachung wurde gestartet	Information

SINEC NMS

Información de vigilancia y seguimiento

SIEMENS
Ingenuity for life

Topología (LLDP, Puente)

Puertos LAN

incluido Estadísticas
(Utilización, Error, Descartado)

Port #	Status	Monitoring & Administrate	Port MAC address	Connection type	Speed in Mbps
fe-1-1	Down	Down	94:08:c5:12:a8:41	Unknown	100
fe-2-2	Down	Down	94:08:c5:12:a8:42	Unknown	100
fe-2-1	Down	Down	94:08:c5:12:a8:61	Unknown	100
fe-3-2	Down	Down	94:08:c5:12:a8:62	Unknown	100
fe-3-3	Up	Up	94:08:c5:12:a8:63	Unknown	100
fe-3-4	Down	Down	94:08:c5:12:a8:64	Unknown	100
fe-2-9	Down	Down	94:08:c5:12:a8:65	Unknown	100
fe-2-6	Down	Down	94:08:c5:12:a8:66	Unknown	100
fe-2-10	Up	Up	94:08:c5:12:a8:7d	Unknown	100
ge-1-1	Up	Up	94:08:c5:12:a8:21	Unknown	100
ge-1-2	Down	Down	94:08:c5:12:a8:22	Unknown	100

VLAN

(Incl. resaltado en Topología)

Basic data				
Max. possible VLANs	255	Currently used VLANs	2	
VLANs				
VLAN ID	Name	Status	Unagged ports	Tagged ports
1 switch_001	Static	-	-	-
2 switch_002	Static	-	-	-

Datos de I&M para la gestión de activos

Firmware	ROX 2.11.2 (2017-12-08 11:23)
Hardware version	rx1510
Vendor	Siemens AG
Serial number	30140102-0012-003A040017

Información de redundancia RSTP, MRP, HRP

(ruta redundante que se muestra en la topología)

Redundancy				
Port #	Protocol	Status	Additional information	Role
fe-2-1	RSTP	broken	enabled	-
fe-2-2	RSTP	broken	enabled	-
fe-3-1	RSTP	broken	enabled	-
fe-3-2	RSTP	broken	enabled	-
fe-3-3	RSTP	forwarding	enabled	-
fe-3-4	RSTP	broken	enabled	-

Gráficos de tendencia

Valores históricos (Disponibilidad, carga de trabajo, paquetes descartados...)

Protocolos



¿Cómo recibir información de los dispositivos SINEMA Server v14 / SINEC NMS?

<u>LLDP</u>	<u>ARP</u>	<u>ICMP</u>	<u>DCP</u>	<u>SNMP</u>
Enlace Capa Descubrimiento Protocolo	Habla a Resolución Protocolo	Internet Control Mensaje Protocolo	Descubrimiento Configuración Protocolo	Simple Red Gestión Protocolo
Topology	Inventory	Diagnostic	Diagnostic	Monitoring
			Inventory	

Servidor SINEMA V14 SP1 / SINEC NMS

Opciones de diagnóstico completo y de sistema completo



SNMP

- Diagnóstico estandarizado de redes
- Control y configuración remota
- Notificación de errores (traps)

PROFINET

- Estándar abierto de ethernet industrial del PI
- Evaluación de datos independientemente del fabricante
- Diagnósticos estandarizados

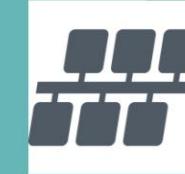
SIMATIC (S7-300, S7-400)

- Administración de SIMATIC eventos/alarmas internos
- Perfecta integración en el sistema de informes del

SNMP



PROFINET



SIMATIC



Gestion de Configuracion



Gestion de Configuracion

Configuración basada en políticas

- Ejecución automática de tareas regulares, tales como la realización de copias de seguridad de los componentes SCALANCE cada dos semanas.
- Configuración de la red a través de reglas basadas en funciones, por ejemplo: "set VLAN", "lock open ports".

Gestión de Firmware

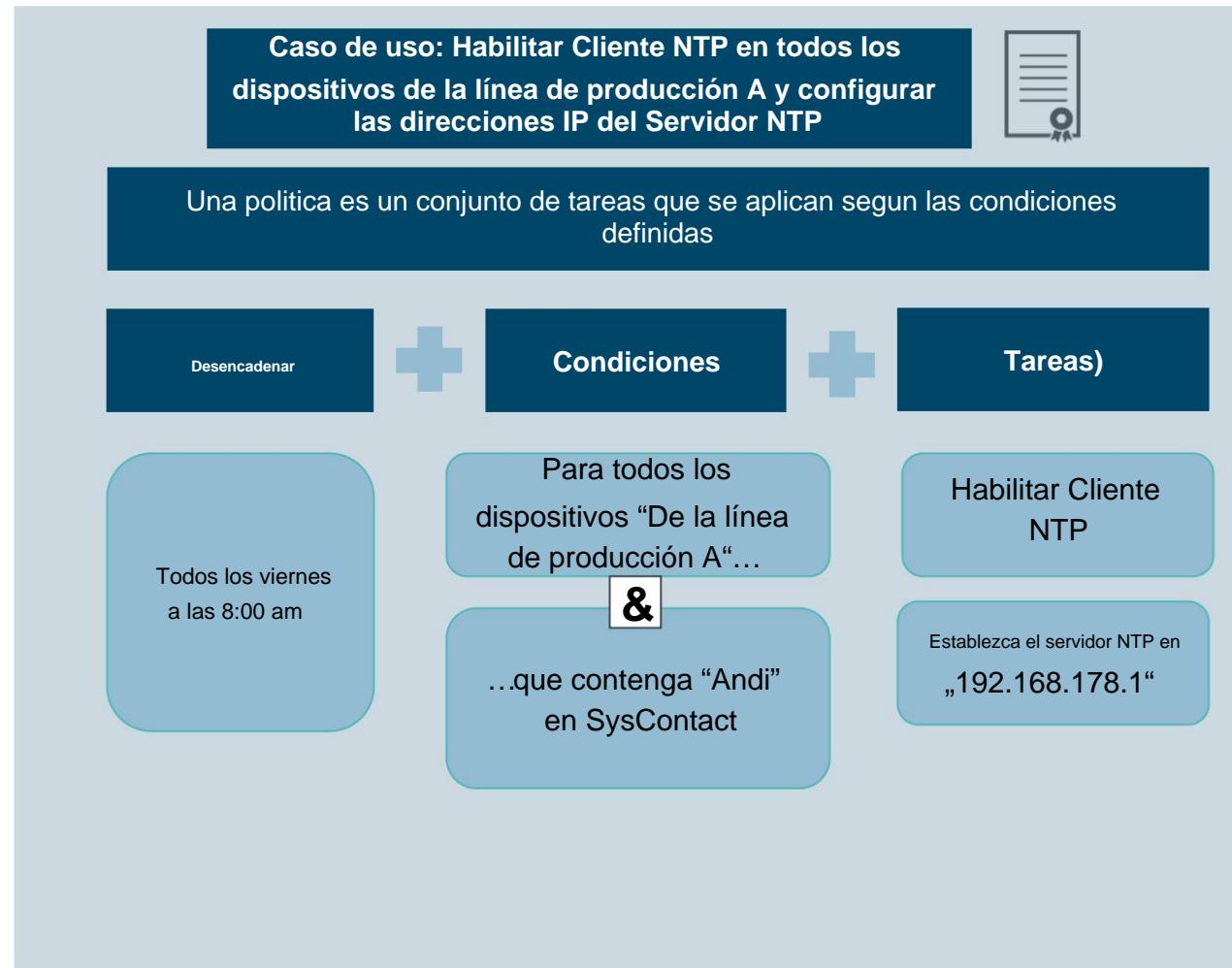
- Repositorio: Gestión central de las versiones de firmware de las diferentes familias de dispositivos (SCALANCE X, W, S, M).
- Función de actualización de firmware a un único o múltiples componentes SCALANCE (teniendo en cuenta la topología).

Gestión de configuración de dispositivos

- Copia de seguridad / restauración de la configuración de los dispositivos SCALANCE para un único o múltiples dispositivos.
- Función de comparación para detectar los cambios en la configuración de componentes SCALANCE.
- Definición de parámetros de red individuales para componentes SCALANCE únicos y múltiples.

SINEC NMS V1.0

Configuración basada en Políticas – Concepto y Método



- Sistema puede investigar las características del dispositivo para encontrar los dispositivos que se pueden configurar (basado en el **modelo de información**)
- Según las reglas / condiciones se puede definir el alcance de la aplicación
- Las políticas se pueden **programar o ejecutarse bajo demanda**
- Las políticas pueden **ejecutarse** para comprobar con qué valor están configurados y en qué dispositivos
- Los **registros ejecutados** se pueden archivar, y mediante reglas comprobar en cualquier momento los cambios producidos

SINEC NMS V1.0

Configuración de políticas– Ejemplos



Caso de uso: deshabilitar todos los puertos que tengan como estado “link down”



Una política es un conjunto de tareas que depende de unas condiciones definidas.

Desencadenar



Condiciones



Tareas)

Cada viernes
a las 8:00

Validar para “todos
los dispositivos” en la red



Cambiar el estado
del puerto a
“disabled”

...los cuales soportan la
función “standard port
setting”



...los cuales contienen
puertos con el estado
“down”

Caso de uso: deshabilitar todos los protocolos inseguros



Una política es un conjunto de tareas que depende de unas condiciones definidas.

Desencadenar



Condiciones



Tareas)

cada mes

Validar para “todos
los dispositivos” en la red



...los cuales soportan
las funciones
“HTTP,TELNET,DCP”

Cambiar
HTTP/HTTPS un
“Solo HTTPS”

Cambiar
“TELNET” a
“desactivar”

Cambiar DCP a
“Solo lectura”

Configuraciones

de dispositivos compatibles con **SINEC NMS** para V1.0



Grupo	Nombre de la tarea
SNMP	<p>1. Configurar el servidor SNMP 2. Configure la comunidad de lectura/escritura de SNMP v1/v2c 3. Configure la comunidad de lectura de SNMP v1/v2c 4. Configure el usuario de SNMP v3 5. Configure la contraseña de usuario de SNMP v3 6. Configure el trap de SNMP v1 7. Configure los eventos de trap de SNMP v1 8. Configure el SNMP Receptor de capturas v1 9. Eliminar el receptor de capturas SNMP v1</p>
registro del sistema	<p>1. Agregar servidor Syslog 2. Eliminar servidor Syslog 3. Establecer cliente Syslog 4. Establecer eventos Syslog</p>
Configuración del servidor	<p>1. Configurar el servidor DCP 2. Configurar el servidor Telnet 3. Configure el servidor SSH 4. Configure el modo HTTP</p>
NTP/SNTP	<p>1. Configurar cliente NTP 2. Configurar servidor para cliente NTP 3. Eliminar servidor para cliente NTP 4. Configurar cliente SNTP 5. Configurar el servidor para el cliente SNTP</p>
Punto de acceso de LAN inalámbrica Configuración	<p>1. Configure el modo de dispositivo WLAN 2. Configure el código de país WLAN 3. Configure las antenas WLAN 4. Configure WLAN 802.11 (compacto) 5. Configure habilitar radio 6. Configure la seguridad WLAN básica</p>

28 tareas

Tareas relevantes para la seguridad

!Se debe respetar el orden de las tareas WLAN!

Configuraciones

de dispositivos compatibles con **SINEC NMS** para V1.0



Grupo	Nombre de la tarea
Gestión de usuarios	<p>1. Establecer modo de autenticación de usuario 2. Establecer usuario local 3. Eliminar usuario local 4. Establecer función de usuario 5. Eliminar función de usuario</p> 
configuración de RADIO	<p>1. Establecer el servidor RADIUS 2. Establecer el modo de autorización RADIUS 3. Eliminar el servidor RADIUS</p> 
Cargar/Guardar archivo de configuración	<p>1. Guarde el archivo de configuración del dispositivo 2. Cargue el archivo de configuración en el dispositivo</p>
Gestión de FW	<p>1. Cargue el firmware en el dispositivo 2. Configure la activación del firmware</p>
Nombre del dispositivo/contacto/ubicación	1. Configure la información general del dispositivo
Configuración DHCP	<p>1. Configurar el cliente DHCP IPv4 2. Configurar el modo DHCP</p>
Diverso...	<p>1. Establecer el modo de configuración 2. Establecer los cambios de confirmación 3. Establecer la interfaz de configuración SINEMA habilitada 4. Establecer el contacto de señal 5. Establecer el reinicio del dispositivo 6. Establecer NFC 7. Establecer la configuración del botón de selección/establecimiento 8. Establecer el modo puente VLAN</p> 

21 tareas

Tareas relevantes para la seguridad

SINEC NMS

Configuraciones de interfaz soportadas para V1.0



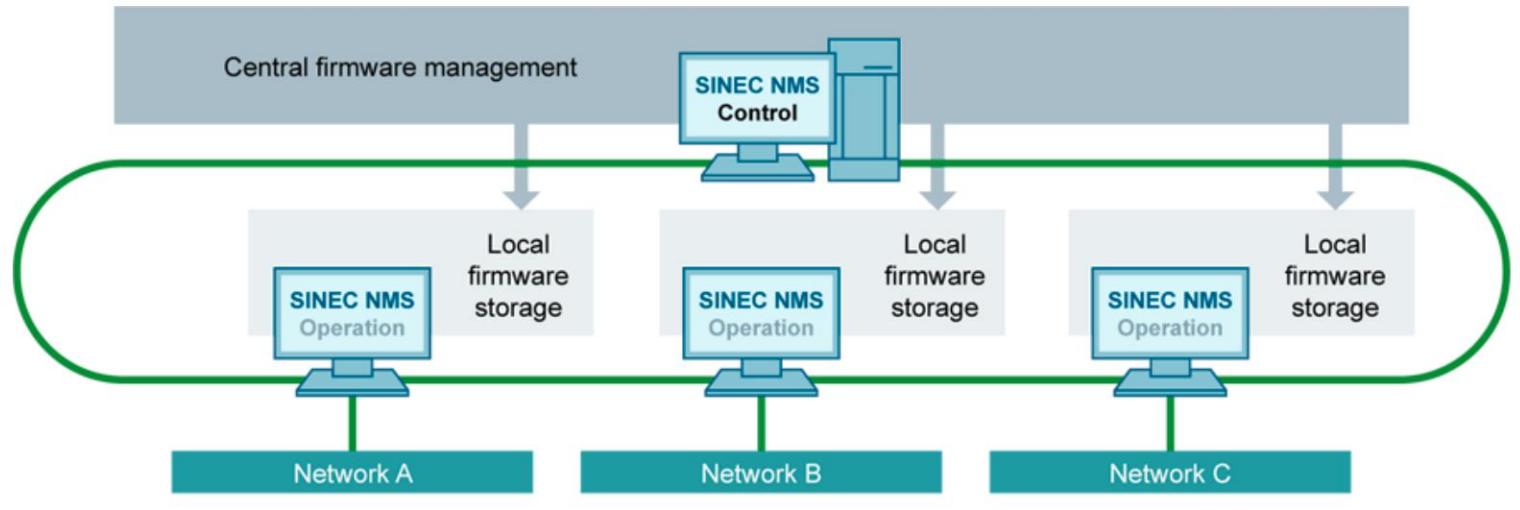
Grupo	Nombre de la tarea
Gestión portuaria	<p>1. Establecer la configuración general del puerto 2. Establecer la configuración mejorada del puerto</p> 
Configuración del puerto LLDP	<p>1. Establecer el estado del puerto LLDP</p>
Configuración de reenvío DCP	<p>1. Configurar el reenvío DCP</p>

4 tareas

SINEC NMS

Gestión de firmware: gestión central de los archivos de firmware

SIEMENS
Ingenuity for life



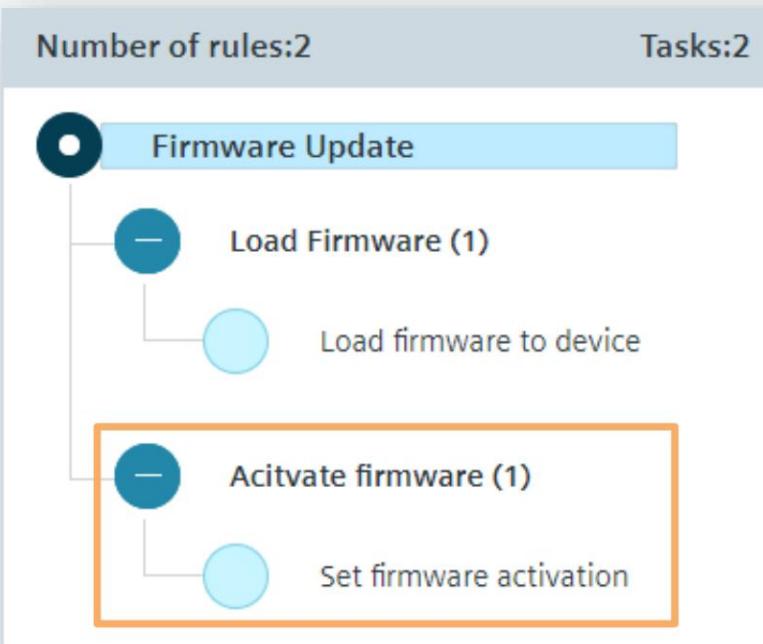
- El firmware se **administra** en **repositorio de firmware centralizado** en Control
 - El repositorio de firmware obtiene **sincronizado automáticamente** con todas las operaciones
 - El firmware se puede descargar en un dispositivo de forma **manual o programada** por una política
 - **Activación de firmware inteligente** (reinicio del dispositivo) basado en **conocimientos de topología** (basado en rutas)
- G_IK10_XX_50878

Ejemplo de mantenimiento:

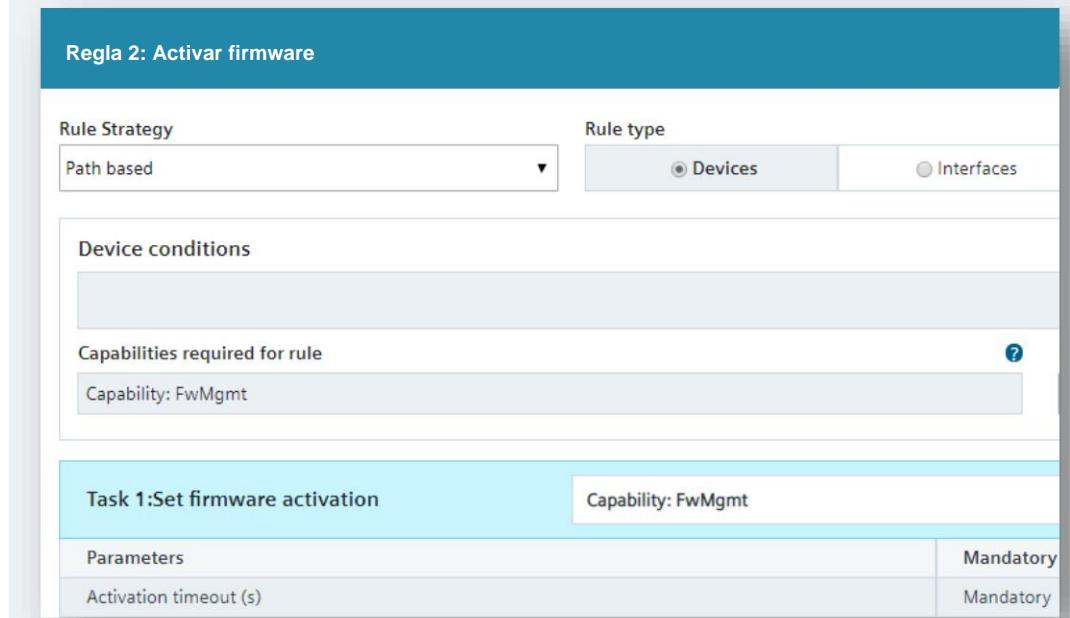
Aplique políticas predefinidas para implementar el firmware en toda su red OT



Seleccione políticas fácilmente arrastrando y soltando



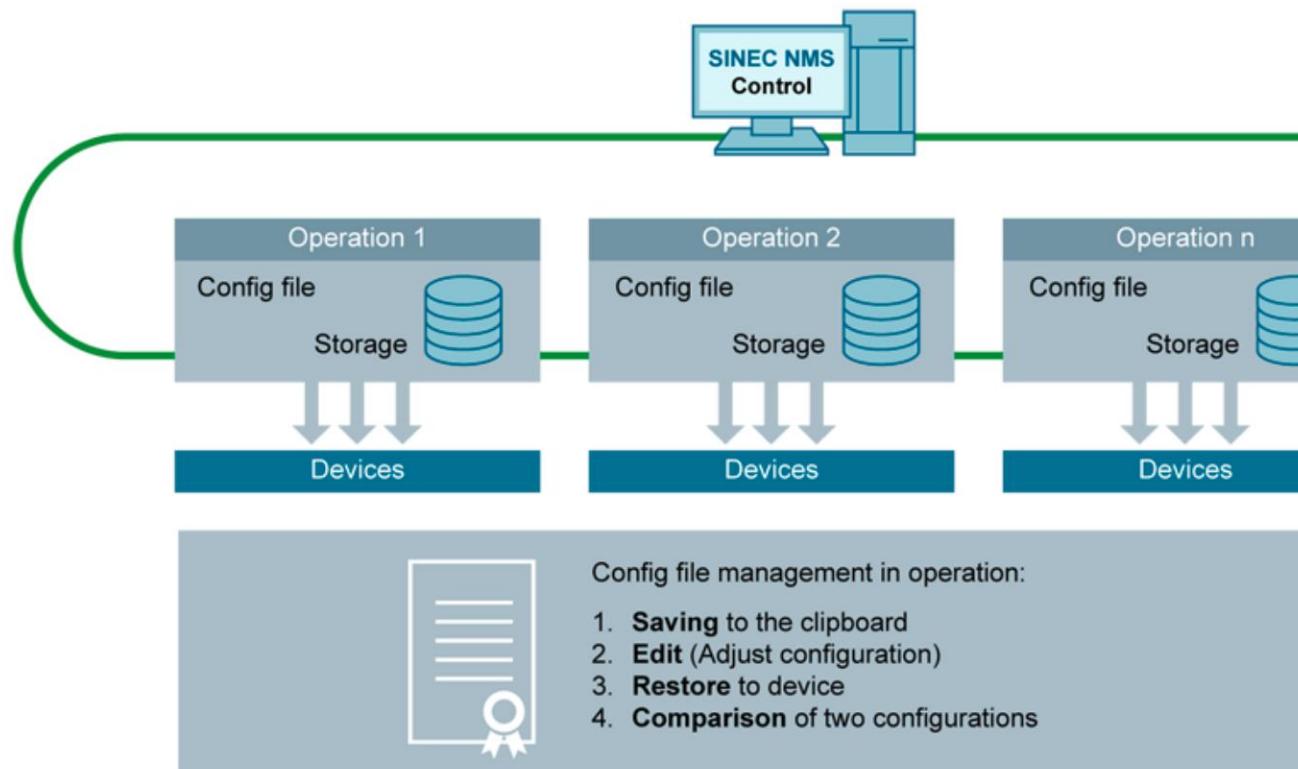
Despliegues inteligentes gracias a reglas y tareas



SINEC NMS

Guardar/restaurar/editar y comparar archivos de configuración

SIEMENS
Ingenuity for life



- Las copias de seguridad de la configuración del dispositivo se almacenan y **administran** a nivel de **operación**
- Las copias de seguridad se pueden **guardar manualmente** o **automáticamente** según la **política**
- Las copias de seguridad se pueden **comparar** (resumen) para detectar diferencias
- Las copias de seguridad se pueden **editar** y luego **restaurar**

G_IK10_XX_50881

SINEC NMS

Guardar/restaurar/editar y comparar archivos de configuración



Basics

- | | |
|---|---|
| 1. Device configuration repository <ul style="list-style-type: none">== contains all backups of the device configurationsBackups must be created via policies | ✓ |
| 2. For each device: <ul style="list-style-type: none">max. 10 device configurations are stored in a ring bufferSubsequent device configurations overwrite device configurations with the oldest time stamp | ✓ |
| 3. Device property " SINEMA Configuration Interface "* <ul style="list-style-type: none">device property must be enabled on the respective devicesUse the policy task „Set SINEMA Configuration Interface enabled“ | ✓ |

Comparar copia de seguridad

Comparar copia de seguridad

SIEMENS
Ingenuity for life

1.

Operación > Inicio > Administración de red > Repositorio de configuración de dispositivos

2.

3.

Compare

Lista de todas las diferencias

Configuration comparison					
Compared configurations					
No.	IP address	MAC address	Firmware version	System name	Time stamp
1	10.1.1.6/24	00:1b:1b:af:ea:00	V06.02.00		
Total differences:35 (first 35 shown)					
No.	Path	Field	Value configuration 1	Value configuration 2	
1	Layer 2 / Configuration	RSTP+		select	
2	Layer 2 / Configuration	MRP Interconnection	select		

Gestión de dispositivos



Gestión de dispositivos

inventario

- SINEMA Server detecta todos los dispositivos de la red y los representa ya sea como lista de dispositivos o lista de interfaces. Una actualización diaria completa la vista de todos los componentes instalados en la red, incluyendo sus propiedades esenciales producidas.

topología

- La topología se lee automáticamente, se representa y monitoriza los cambios.
- El tipo de medio (tales como WLAN, cobre, óptica), redundancia y VLANs son gráficamente representados.

validacion

- Los patrones de red configurables permiten que las propiedades esenciales de la red sean comprobadas reiterativas veces y documentos.
- El resultado de la validación se almacena junto a todos los datos subyacentes en un archivo PDF.

SINEC NMS V1.0

Caso de uso: inventario de red



Tarea

Creación de una representación actual de todos los componentes de la red y sus conexiones topológicas.

Solución

SINEC NMS detecta automáticamente los dispositivos PROFINET y Ethernet de la red mediante DCP, SNMP y PROFINET. La información se muestra de forma centralizada en una lista de dispositivos (inventario) y también se puede exportar en un formato estándar (CSV).

Beneficios

Una documentación de red siempre actualizada.

Lista central de dispositivos (inventario)									
SINEC NMS									
CONTROL									
Actions	Status	IP address	System name	Operation	Device type	Category	MAC address	Initial discovery	Article number
<input type="checkbox"/>	● Maintenance demanded	192.168.120.101/24	s-dpm3-x212-0d...	OpProduction	SCALANCE X212-2...	Switch	00:0E:8C:90:00:4D	3 Days ago	6GK5 212-2B800-2AA3
<input type="checkbox"/>	● OK	192.168.120.84/24	s-dps1-x308-95-35	OpProduction	SCALANCE X308-2...	Switch	00:1B:1B:3A:95:35	3 Days ago	6GK5 308-2GG00-2AA2
<input type="checkbox"/>	● OK	192.168.120.83/24	s-dps1-x308-5e-99	OpProduction	SCALANCE X308-2...	Switch	00:1B:1B:0E:5E:99	3 Days ago	6GK5 308-2GG00-2AA2
<input type="checkbox"/>	● OK	192.168.120.63/24	s-dp2-xf208-28...	OpProduction	SCALANCE X208-2...	Switch	00:1B:1B:A8:28:23	3 Days ago	6GK5 208-0B400-2AF2
<input type="checkbox"/>	● Maintenance demanded	192.168.120.72/24	s-dp2-xf204b-0...	OpProduction	SCALANCE X204-...	Switch	20:87:56:5C:92:1E	3 Days ago	6GK5 204-2AA00-2GF2
<input type="checkbox"/>	● OK	192.168.120.67/24	s-dp2-xc206-eb...	OpProduction	SCALANCE XC206-...	Switch	20:87:56:65:C8:C5	3 Days ago	6GK5 206-2B500-2AC2
<input type="checkbox"/>	● OK	192.168.120.71/24	s-dp2-xb208-a4...	OpProduction	SCALANCE XB208-...	Switch	20:87:56:64:A4:D8	3 Days ago	6GK5 208-0B400-2TB2
<input type="checkbox"/>	● OK	192.168.120.30/24	s-dp1-xf208-27...	OpOffice	SCALANCE X208-...	Switch	00:1B:1B:A8:27:AE	5 Days ago	6GK5 208-0B400-2AF2
<input type="checkbox"/>	● OK	192.168.120.27/24	s-dp1-x204-44...	OpOffice	SCALANCE X204R...	Switch	00:1B:1B:A8:44:B9	5 Days ago	6GK5 204-0B400-2BA3
<input type="checkbox"/>	● Error	192.168.120.26/24	s-dp1-x202-43...	OpOffice	SCALANCE X202-2...	Switch	00:1B:1B:A8:43:68	5 Days ago	6GK5 202-2B400-2BA3
<input type="checkbox"/>	● OK	192.168.120.82/24	w-dpk3-w784-A...	OpProduction	SCALANCE W784-1...	Access Point	00:1B:1B:37:A4:FC	3 Days ago	6GK5 784-1AA30-6AA0
<input type="checkbox"/>	● Maintenance demanded	192.168.120.81/24	w-dpk3-w747-1...	OpProduction	SCALANCE W747-1...	WLAN Client	00:1B:1B:37:A4:F9	3 Days ago	6GK5 747-1AA30-6AA0
<input type="checkbox"/>	● OK	192.168.120.29/24	sysName Not Set	OpOffice	SCALANCE W761-1...	Access Point	00:1B:1B:C9:7F:98	5 Days ago	6GK5 761-1FC00-0AA0
<input type="checkbox"/>	● OK	192.168.120.74/24	s-dp2-sc646-3B...	OpProduction	SCALANCE SC646 (...	Router	20:87:56:72:38:20	3 Days ago	6GK5 646-2G500-2AC2
<input type="checkbox"/>	● OK	192.168.101.1/24	n-rcx-x1510-a8-#	OpWarehouse	RUGGEDCOM_Mult...	Router	94:88:CS:12:A8:FF+	5 Days ago	

gestion de rendimiento



gestion de rendimiento

informe de gestion

- Se pueden mostrar y evaluar estadísticas para cualquier período de tiempo gracias a la base de datos del sistema.
Esto facilita estimar sucesos pasados:
 - Disponibilidad de dispositivos e interfaces •
 - Datos de rendimiento como el uso de interfaces •
 - Inventario y listas de fabricantes de dispositivos en la red. •
 - Clasificación de sucesos basada en el número de casos con estado “Error”, “Maintenance” o “OK”

Caso de uso SINEC

NMS V1.0 – Reducción de los tiempos de inactividad en redes industriales



Tarea

Identificar cambios en las redes industriales desde el principio y prevenir fallas, para garantizar la productividad de las plantas industriales y minimizar los tiempos de inactividad.

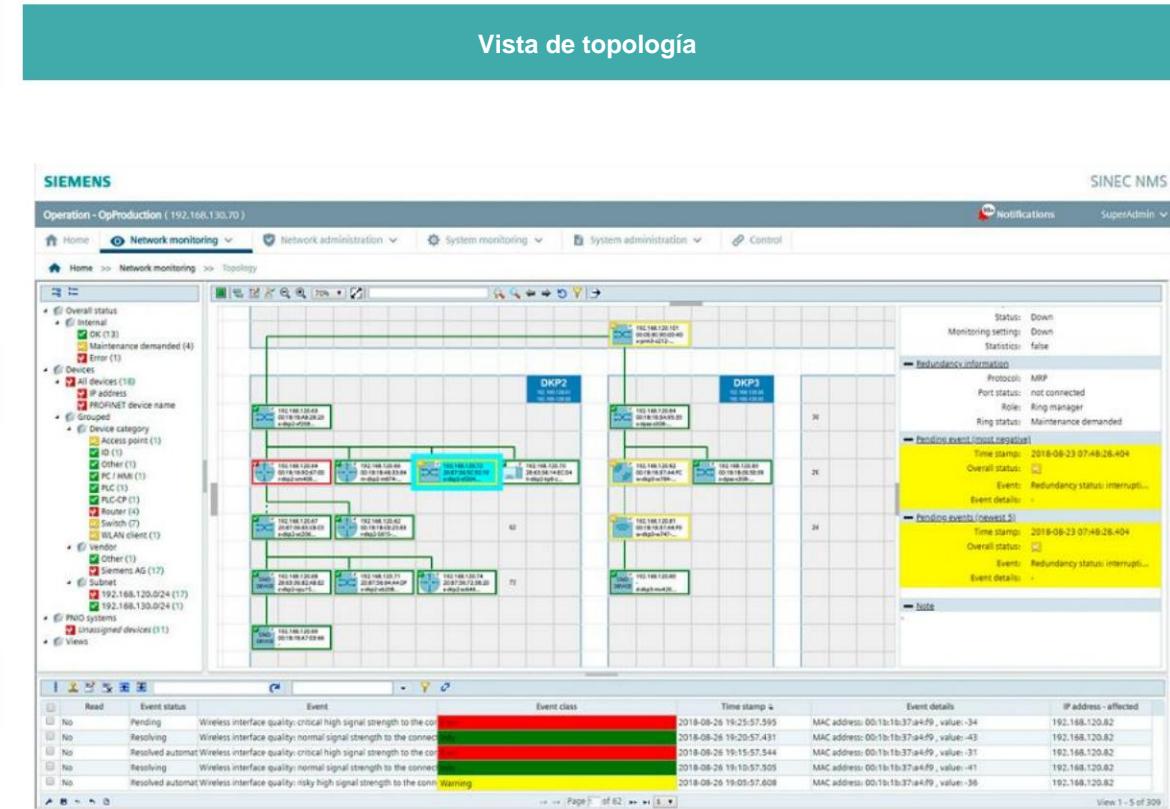
Solución

SINEC NMS supervisa constantemente la red, las 24 horas del día, los 7 días de la semana, y muestra en vivo los estados de diagnóstico de los dispositivos de la red. Además, se pueden mostrar y evaluar estadísticas de cualquier período de tiempo.

Beneficios

- Pantalla de diagnóstico a color para identificar fallas no deseadas desde el principio
- Notificación por correo electrónico para ser informado de inmediato sobre los cambios

Vista de topología



Gestion de la seguridad



Gestion de Seguridad

Según la norma
CEI 62443

Gestión accediendo
como usuario

- El acceso al sistema y el alcance de la funcionalidad para todas las personas autorizadas se pueden controlar con precisión a través de la administración del usuario.

seguridad del sistema

- Comunicación de datos cifrados (mediante certificados y contraseñas) entre las instancias de Control SINEC NMS y Operación SINEC NMS.
- La comunicación de datos entre SINEC NMS y los componentes de la infraestructura también pueden cifrarse (SNMP V3).

Interfaz en dirección norte



Interfaz en dirección norte

Notificaciones del sistema

- Las notificaciones de visualización centralizada informan al usuario de los problemas pendientes. A través de enlaces, el usuario puede ir directamente al lugar apropiado para solucionar el problema.

OPC UA

- La información del estado de la red se proporciona a otras aplicaciones OPC UA a través de la interfaz de servidor OPCUA.

Notificaciones vía

Correo electrónico

- Podemos usar el correo electrónico o cualquier aplicación de Windows para recibir avisos de eventos que puedan ocurrir.

Acceso vía URL

- Los sistemas HMI de alto nivel pueden acceder de forma cómoda y directa a la red monitorizada ya los datos de Diagnóstico mediante accesos URL.

SINEC NMS V1.0

Caso de uso: comunicación en dirección norte



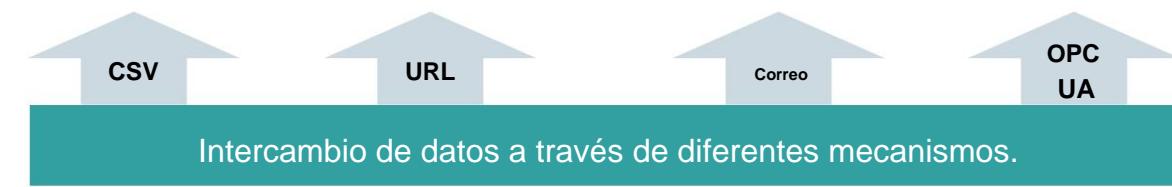
Tarea

Un departamento central quiere representar y monitorear el estado general de todas las redes.



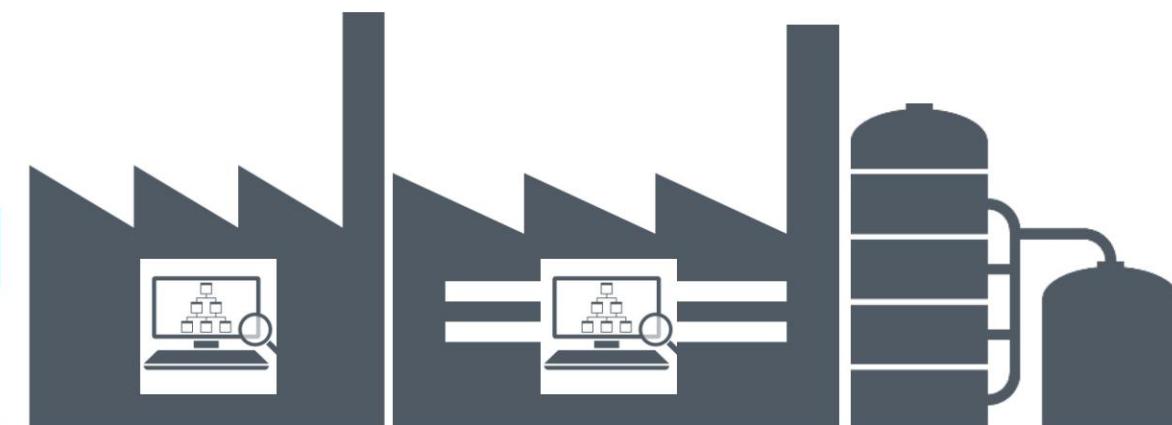
Solución

SINEC NMS está instalado en las áreas de producción y monitorea las redes locales allí. Utilizando una amplia gama de mecanismos, los datos locales se ponen a disposición de instancias de nivel superior o se enrutan hacia ellas. Con el protocolo OPC UA, los datos se pueden transferir directamente a sistemas basados en la nube, como MindSphere.



Beneficios

Representación en todo el sitio de todas las redes.



administración del sistema



administración del sistema

Gestión de las operaciones

- Podemos gestionar la puesta en marcha y la administración de las operaciones distribuidas del SINEC NMS en el Control SINEC NMS.

escalabilidad del sistema

- SINEC NMS es un sistema de gestión de redes distribuidas que se divide en SINEC NMS Control y SINEC NMS Operación.

Gestión de usuarios

- Los derechos de acceso pueden establecerse y gestionarse en la gestión de funciones y derechos.
- Podemos configurar y gestionar usuarios en la administración local de usuarios de SINEC NMS o mediante una conexión a una administración central de usuarios (por ejemplo, componente de gestión de usuarios [UMC] y directorio activo).

Acceso vía Web

- La apariencia y entorno de la Web junto con la propia personalización de la misma a gusto del usuario, (SSO (single sign-on)) permiten una navegación fácil en el sistema general.

SINEC NMS V1.0

Caso de uso: gestión central de usuarios/roles/derechos



Tarea

Gestión de usuarios y sus permisos desde una ubicación central para toda la red.

Solución

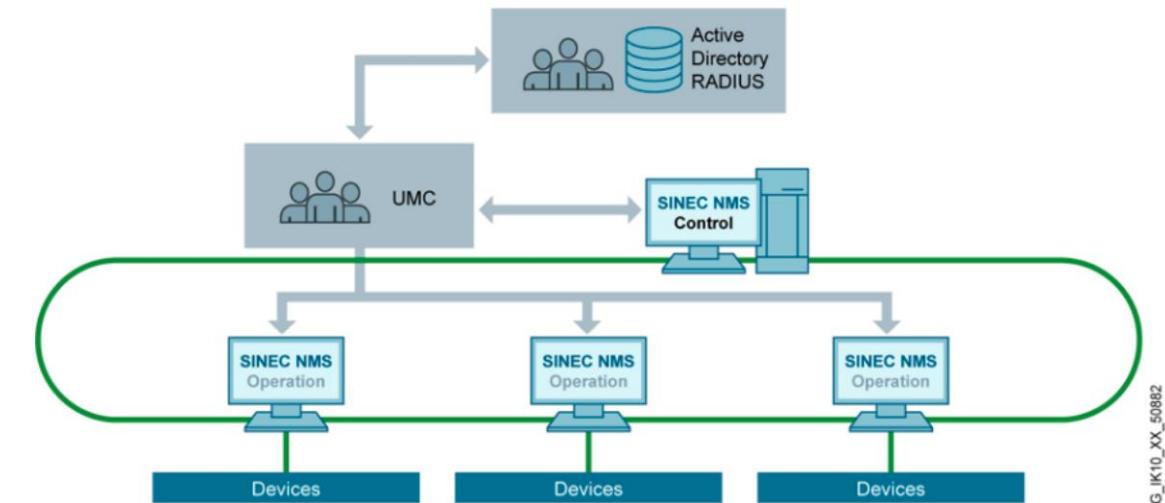
SINEC NMS ofrece dos opciones:

- Gestión central de usuarios con la gestión de usuarios - componente (UMC)
- Gestión local de usuarios en SINEC NMS

Beneficios

- La gestión de usuarios se realiza de forma centralizada
- Uso de usuarios existentes de RADIUS o directorio activo a través de UMC (según IEC 62443)

Gestión central de usuarios



G_IK10_XX_50882

Descripción general de las novedades de SINEC NMS V1.0 y V1.0 SP1



Gestión de cortafuegos

- NUEVO: Gestión de cortafuegos basada en relaciones de comunicación
- NUEVO: gestión de NAT basada en la comunicación relaciones
- NUEVO: Dispositivos compatibles con cortafuegos/NAT gestión: SCALANCE SC600, SCALANCE S615, RUGGEDCOM ROX2

Configuración de dispositivos basada en políticas

- NUEVO: Tarea para comandos CLI
- NUEVO: Tareas para la configuración de VLAN
- NUEVO: Tareas para la configuración de RSTP
- NUEVO: Tareas para la configuración de detección de LOOP
- NUEVO: Tareas para la configuración de WLAN AP/Client
- NUEVO: configuración de dispositivos basada en políticas que también es compatible con dispositivos RUGGEDCOM ROS
- NUEVO: configuración de dispositivos basada en políticas que también es compatible con dispositivos RUGGEDCOM ROX2

Registro de auditoría

- NUEVO: Registro de auditoría para la gestión de cortafuegos
- NUEVO: Registro de auditoría para la gestión de políticas
- NUEVO: registro de auditoría para dispositivos de confianza
- NUEVO: registro de auditoría en el contexto de eventos seguros

Gestión de certificados

- NUEVO: dispositivo de confianza automatizado basado en Certificados SSH/HTTP
- NUEVO: dispositivo manual de confianza/desconfianza
- NUEVO: Los certificados HTTP basados en SINEC NMS se pueden establecer en dispositivos de red (basados en políticas)

Gestión de credenciales de dispositivos

- UPG: Soporte de tareas de políticas para configurar contraseñas aleatorias en dispositivos (SSH, Web/SNMP)
- NUEVO: Compatibilidad con la gestión de credenciales Dispositivos ROS RUGGEDCOM
- NUEVO: Compatibilidad con la gestión de credenciales Dispositivos RUGGEDCOM ROX2

Centro de control de políticas

- NUEVO: las tareas se pueden usar varias veces dentro de la misma regla
- UPG: Reconocimiento de ruta mejorado
- UPG: Se mejoró la usabilidad en el contexto de la selección de parámetros.
- UPG: diseño de capacidad de dispositivo mejorado
- NUEVO: Progreso de aplicación de políticas (0%-100%)
- NUEVO: Pasos para la aplicación de políticas (Existente/Éxito/Error/Omitido)

Gestión de operaciones

- NUEVO: cambio de IP soportado para control y operación
- NUEVO: lista de restricciones de descubrimiento
- UPG: los perfiles de dispositivos se pueden exportar e importar
- NUEVO: se puede configurar el comportamiento de la interfaz DCP dentro de los perfiles de parámetros
- NUEVO: la información de licencia de las operaciones se puede ver en el monitor de operaciones

Descripción general de las novedades de SINEC NMS V1.0 y V1.0 SP1



Gestión de firmware

- NUEVO: manejo de firmware para RUGGEDCOM ROS dispositivos
- NUEVO: manejo de firmware para RUGGEDCOM ROX2 dispositivos
- UPG: descarga de firmware solo cuando el firmware aún no existe
- UPG: Comportamiento extendido en la definición de la referencia firmware

Gestión de archivos de configuración

- NUEVO: manejo de archivos de configuración para RUGGEDCOM ROS dispositivos
- NUEVO: manejo de archivos de configuración para RUGGEDCOM ROX2 dispositivos
- Nuevo: exportar archivos de configuración (ROS/ROX2) a HDD

Alarmas/ Notificaciones

- NUEVO: Alarmas en contexto de eventos seguros
- UPG: Mejora en enlaces dentro de notificaciones

Informes

- UPG: Las áreas de roles y dispositivos se consideran para la generación del informe

Supervisión

- NUEVO: dispositivos RUGGEDCOM ROS totalmente integrados en descubrimiento / monitoreo
- NUEVO: dispositivos RUGGEDCOM ROX2 totalmente integrados en descubrimiento / monitoreo
- NUEVO: se pueden recibir informes SNMP

Interfaces en dirección norte

- NUEVO: SYSLOG se puede utilizar para enviar todos los eventos / registros de auditoría a un servidor syslog
- NUEVO: Los datos de monitoreo se pueden leer desde la operación según la solicitud HTTPS (JSON/CSV)

Control de acceso basado en roles

- NUEVO: El tiempo de espera de la sesión se puede configurar por usuario papel

Sistema

- NUEVO: la integridad del sistema se puede validar
- UPG: el sistema ahora se puede escalar hasta 75 operaciones (500 dispositivos cada una)
- UPG: página de inicio de sesión combinada para inicio de sesión local y basado en UMC
- NUEVO: la recopilación de todos los archivos de registro se puede activar en control.
- UPG: actualización de UMC
- UPG: configuración de UMC extendida durante la configuración
- NUEVO: SINEC NMS se puede utilizar en el contexto de NAT (Operación dentro de la red NATed)
- UPG: el servicio Trap se habilita durante la configuración

Usabilidad/ UX

- NUEVO: el diseño de la cuadrícula se puede ajustar y se guarda automáticamente
- NUEVO: el diseño de la cuadrícula se puede restablecer
- NUEVO: los atajos de acción se pueden configurar
- UPG: Selección de filas (en cuadrículas) mejorada
- NUEVO: indicación de barra de bloqueo en las acciones del usuario
- NUEVO: Hipervínculos para acciones comunes del usuario

Vista general de las novedades de SINEC NMS V1.0 ÿ V1.0 SP1



SIEMENS

test2/s-dkp2-sc646-3B-20-MSPS 01/21/2019 07:43:54

Welcome admin Logout

Information System Layer 2 Layer 3 Security Users Passwords Certificates Firewall IPsec VPN

Internet Protocol (IP) Rules

General Predefined IPv4 IP Services ICMP Services IP Protocols IP Rules

IP Version: IPv4

Select	Protocol	Action	From	To	Source (Range)	Destination (Range)	Service	Log	Precedence
<input type="checkbox"/>	IPv4	Accept	vlan1 (INT)	vlan2 (EXT)	0.0.0.0/0	0.0.0.0/0	all	info	0
<input type="checkbox"/>	IPv4	Accept	vlan2 (EXT)	vlan1 (INT)	0.0.0.0/0	0.0.0.0/0	all	info	1
<input type="checkbox"/>	IPv4	Accept	vlan10	vlan1 (INT)	0.0.0.0/0	0.0.0.0/0	all	info	2
<input type="checkbox"/>	IPv4	Accept	vlan1 (INT)	vlan10	0.0.0.0/0	0.0.0.0/0	all	info	3
<input type="checkbox"/>	IPv4	Accept	Device	vlan2 (EXT)	0.0.0.0/0	0.0.0.0/0	all	info	4
<input type="checkbox"/>	IPv4	Accept	vlan2 (EXT)	Device	0.0.0.0/0	0.0.0.0/0	all	info	5
<input type="checkbox"/>	IPv4	Accept	vlan1 (INT)	Device	0.0.0.0/0	0.0.0.0/0	all	info	6
<input type="checkbox"/>	IPv4	Accept	Device	vlan1 (INT)	0.0.0.0/0	0.0.0.0/0	all	info	7

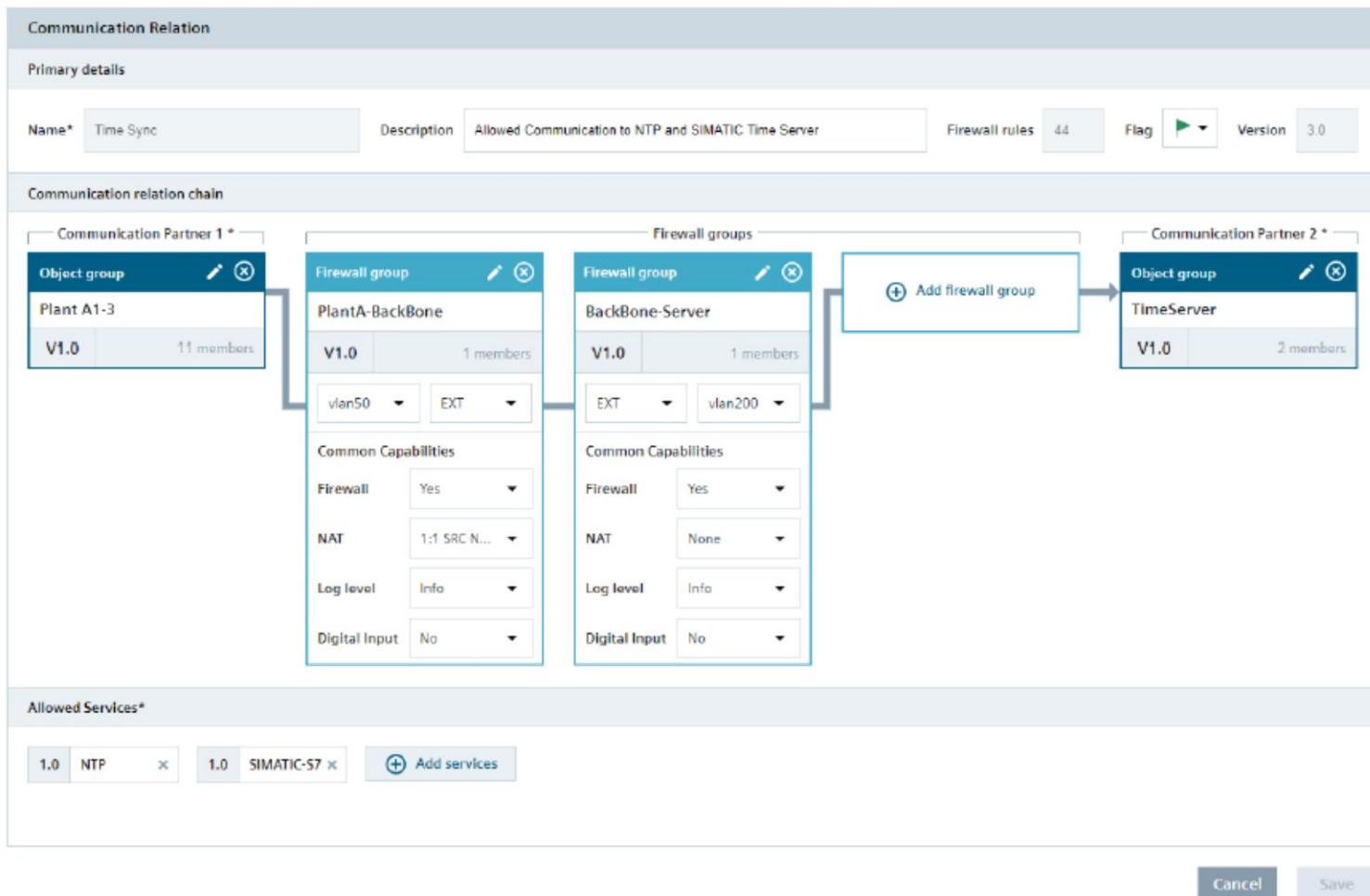
8 entries.

Create Delete Set Values Refresh

Vista general de las novedades de SINEC NMS V1.0 y V1.0 SP1

SIEMENS

Ingenuity for life



new

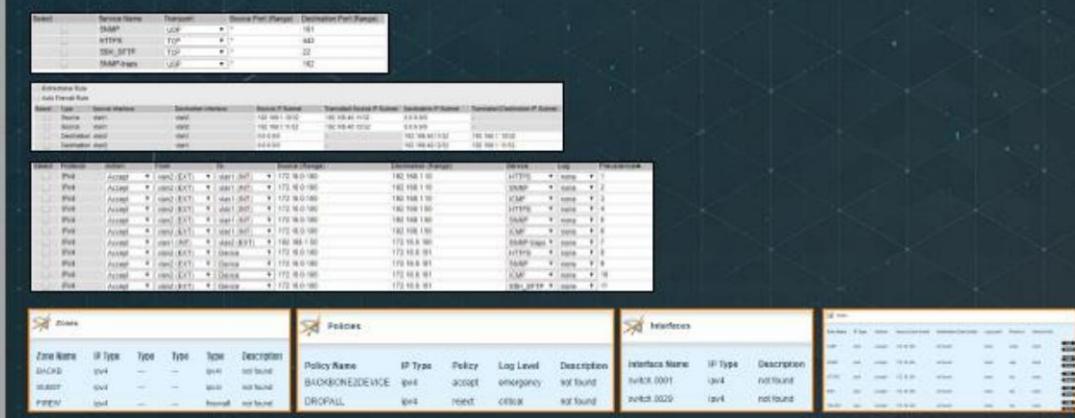
Vista general de las novedades de SINEC NMS V1.0 y V1.0 SP1



Manual Configuration

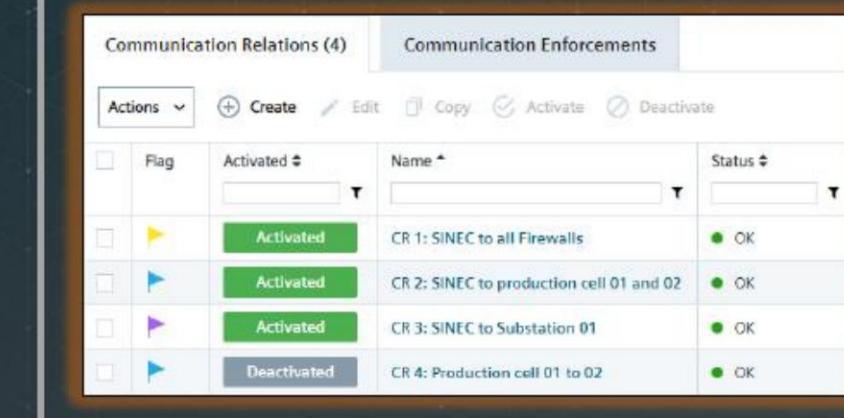
59 steps for 3 firewalls

- Firewall-/NAT router 1:
 - 16x IP-Rules; 4x NAT rules, 4x Services
- Firewall-/NAT router 2:
 - 16x IP-Rules; 4x NAT rules, 4x Services
- Firewall 3:
 - 3x Zones, 2x Interfaces, 2x Policies, 4x FW-Rules (incl. 4 rules + services)



SINEC NMS configuration

4x Communication Relation



SINEC NMS: Vista general de la configuración detallada del dispositivo para ESCALANCE/ RUGGEDCOM



Sistema operativo	Familia de dispositivos	Configuración basada en políticas (dependiendo de las capacidades del dispositivo)	Configurar copia de seguridad/restaurar/editar/comparar gestión de cortafuegos	
VxWorks		basado en CLI	-	-
MSPS	XR500 XM400	SMN 1.0	NMS 1.0 Actualización 1 (6.2.x) NMS 1.0 + SP1 (6.2.x)	-
MSPS	XB200 XC200 XP200 XR300WG XF200	SMN 1.0	NMS 1.0 + Actualización 1 (4.1.x) NMS 1.0 + SP1 (4.1.x)	-
MSPS	M800	SMN 1.0	NMS 1.0 + Actualización 1 (6.1.x) NMS 1.0 + SP1 (6.1.x, 6.2.x)	-
MSPS	S615	SMN 1.0	NMS 1.0 + Actualización 1 (6.1.x) NMS 1.0 + SP1 (6.1.x, 6.2.x)	NMS 1.0 SP1 (>=6.2.x)
MSPS	SC600	SMN 1.0	NMS 1.0 + Actualización 1 (2.0.x)	NMS 1.0 SP1 (>=2.0.x)
MSPS	W1700	SMN 1.0	NMS 1.0 + SP1 (2.0.x)	-
MSPS	W700	SMN 1.0	NMS 1.0 + SP1 + HSP (6.5.x) (6.5.x se lanzará en 2020)	-
RUGGEDCOM ROS		NMS 1.0 + SP1	NMS 1.0 + SP1 (5.3.x, 5.4.x)	
RUGGEDCOM ROX2		NMS 1.0 + SP1	NMS 1.0 + SP1 (2.13.2, 2.13.3)	NMS 1.0 + SP1 (>=2.13.2)



¡Gracias por su atención!

SIEMENS SA – Comunicaciones Industriales

<http://www.siemens.com/redes-industriales>

Solicitud de soporte de la línea directa de SIEMENS:

<https://www.siemens.com/supportrequest>