ANALISIS DE LOS PROCESOS DE SISTEMAS

Principios

- Una de las principales tareas de un ingeniero de sistemas es evaluar los datos de ingeniería y los artefactos creados durante el proceso de ingeniería de sistemas. Las evaluaciones están en el centro del análisis del sistema, proporcionando medios y técnicas:

- Definir criterios de evaluación basados en los requisitos del sistema.

- Evaluar las propiedades de diseño de cada solución candidata en comparación con estos criterios.

- Calificar las soluciones candidatas a nivel mundial y justificar las puntuaciones.

- Decidir la solución adecuada.

Proceso

- Es una ejecución concreta de un programa, con un camino determinado y un valor de sus variables determinados.
- La unidad mínima de expedición y de asignación de recursos es el proceso.

Identificación de los procesos

- los procesos tienen un identificador que les permite ser diferentes a cualquier otro

- cada proceso tiene su PID (Process IDentificator) que lo identifica frente a otros procesos.

- El PID no es más que un número, asignado por el sistema operativo, que le servirá a este para identificarlo, lanzarlo a ejecución, cancelarlo, detenerlo, reanudarlo, etc.

Identificación de los procesos

- Para cada proceso existe una estructura de datos denominada “bloque de control de proceso” (BCP) que identifica cada proceso y sirve para controlar su correcta ejecución.
- En esa estructura de datos se almacena información sobre el proceso, como:
  - El estado actual del proceso.
  - El identificador del proceso o PID.
  - La prioridad del proceso.
  - La ubicación en la memoria del proceso.
  - Los recursos utilizados por el proceso

Estados proceso

- **NUEVO:** Proceso que se acaba de crear, pero que aun no ha sido admitido por el sistema operativo en el grupo de procesos ejecutables.
- **LISTO:** Proceso que esta preparado para ejecutar, en cuanto se le de la oportunidad. puede pasar a bloqueado de inmediato si no cumple con todos los recursos necesarios para poder ser ejecutado.
- **BLOQUEADO:** proceso que no puede ejecutar hasta que se produzca cierto suceso, como la terminacion de otra operacion, etc.
- **BLOQUEADO A LISTO:** un proceso pasara al estado listo cuando se produzca el suceso que lo mantiene en bloqueado.
- **EJECUCION:** el proceso que esta actualmente en ejecución.
- **EJECUCION A LISTO:** la razón mas común de esta transicion es que el proceso que esta en ejecucion ha alcanzado el tiempo maximo permitido de ejecicion interrumpida.
- **TERMINADO:** un proceso que ha sido excluido por el sistema operativo del grupo de procesos ejecutables, bien porque se detuvo o porque fue abandonado por alguna razon.

Señales

- Las señales se utilizan en sistemas Unix y sirven para comunicar un evento a un proceso.
- Los procesos pueden capturar la señal y realizar una acción determinada o ignorarla, en ese caso se ejecutará la acción por defecto.
- Las señales pueden utilizarse por ejemplo para:
- Controlar un proceso desde un terminal (terminarlo, suspenderlo, etc.).
- El kernel puede enviar una señal cuando un proceso comete alguna infracción, como acceder ilegalmente a una zona de la memoria.
- Comunicar algo a un proceso desde otro.

Hilos /Threads

- Estado.
- Contexto del procesador.
  - Punto en el que estamos ejecutando, la instrucción concretamente en la que nos hallamos. Es útil a la hora de reanudar un hilo que fue interrumpido con anterioridad, puesto que al guardar el contexto, guardamos la ultima instrucción que ejecutamos, y así podemos conocer por donde tenemos que continuar la ejecución del hilo.
- Pila de ejecución
  - donde se irá metiendo y sacando instrucciones. (Lugar donde almacenaremos las instrucciones que van a ser ejecutadas).
- Espacio de almacenamiento estático
  - donde almacenará las variables.
- Acceso a los recursos de la tarea,
  - que son compartidos por todos los hilos de la tarea.

Algoritmos de planificación procesos

- **Tiempo de espera:** El tiempo que un proceso permanece en espera en la cola de ejecución.
- **Tiempo de retorno:** Tiempo que va desde que se lanza un proceso hasta que finaliza.
- **Tiempo de respuesta:** Por último éste se define a el tiempo que un proceso bloqueado tarda en entrar en ejecución.
- **Uso de CPU:** Porcentaje de tiempo que la CPU está ocupada.
- **Productividad:** Número de procesos realizados en una unidad de tiempo.

Algoritmos de planificación procesos

- **FCFS (*First-Come, First-Served*)**
- FCFS o también llamado FIFO (del inglés *First In, First Out*). Este algoritmo es muy sencillo y simple, pero también el que menos rendimiento ofrece, básicamente en este algoritmo el primer proceso que llega se ejecuta y una vez terminado se ejecuta el siguiente.

Algoritmos de planificación procesos

- **SJF (*Shortest Job First*).**
- Este algoritmo siempre prioriza los procesos más cortos primero independientemente de su llegada y en caso de que los procesos sean iguales utilizara el método FIFO anterior, es decir, el orden según entrada. Este sistema tiene el riesgo de poner siempre al final de la cola los procesos más largos por lo que nunca se ejecutarán, esto se conoce como **inanición**.
-

Algoritmos de planificación procesos

- **SRTF (*Short Remaining Time Next*).**
- Añadiendo la expulsión de procesos al algoritmo SJF obtenemos SRTF, éste será capaz de expulsar un proceso largo en ejecución para ejecutar otros más cortos. El problema que puede surgir es que un proceso largo puede llegar a expulsarse muchas veces y nunca terminar debido a la ejecución de otros mas cortos.

Algoritmos de planificación procesos

- ***Round Robin*.**
- este algoritmo de planificación es uno de los más complejos y difíciles de implementar, asigna a cada proceso un tiempo equitativo tratando a todos los procesos por igual y con la misma prioridad.
- Este algoritmo es circular, volviendo siempre al primer proceso una vez terminado con el último, para controlar este método a cada proceso se le asigna un intervalo de tiempo llamado *quantum* o cuanto (para definirlo se utiliza esta regla, el 80% de los procesos tienen que durar menos tiempo que el *quantum* definido).

Servicios

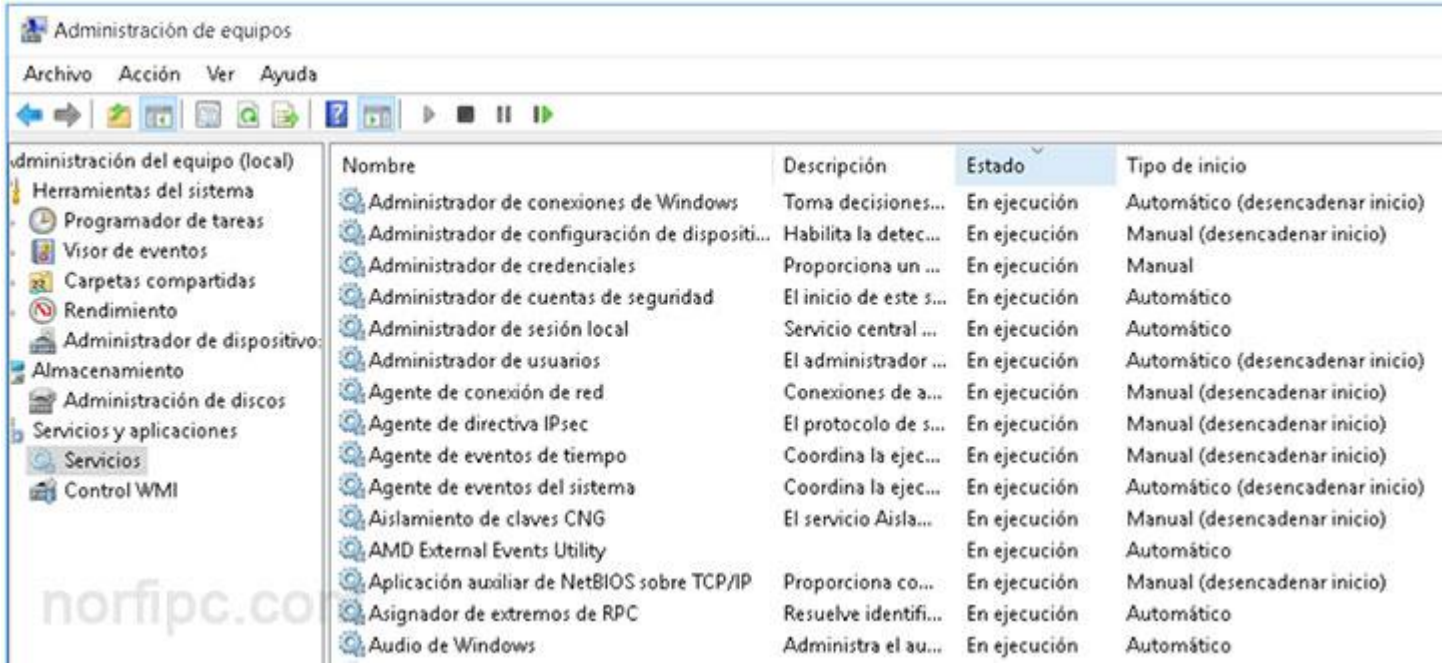
- Un servicio de Windows es un programa de ordenador que funciona en segundo plano.1 Es similar en concepto a un Daemon (informática). Un servicio de Windows debe ajustarse a las normas y protocolos de interfaz del Service Control Manager, el componente responsable de la gestión de servicios de Microsoft Windows.2

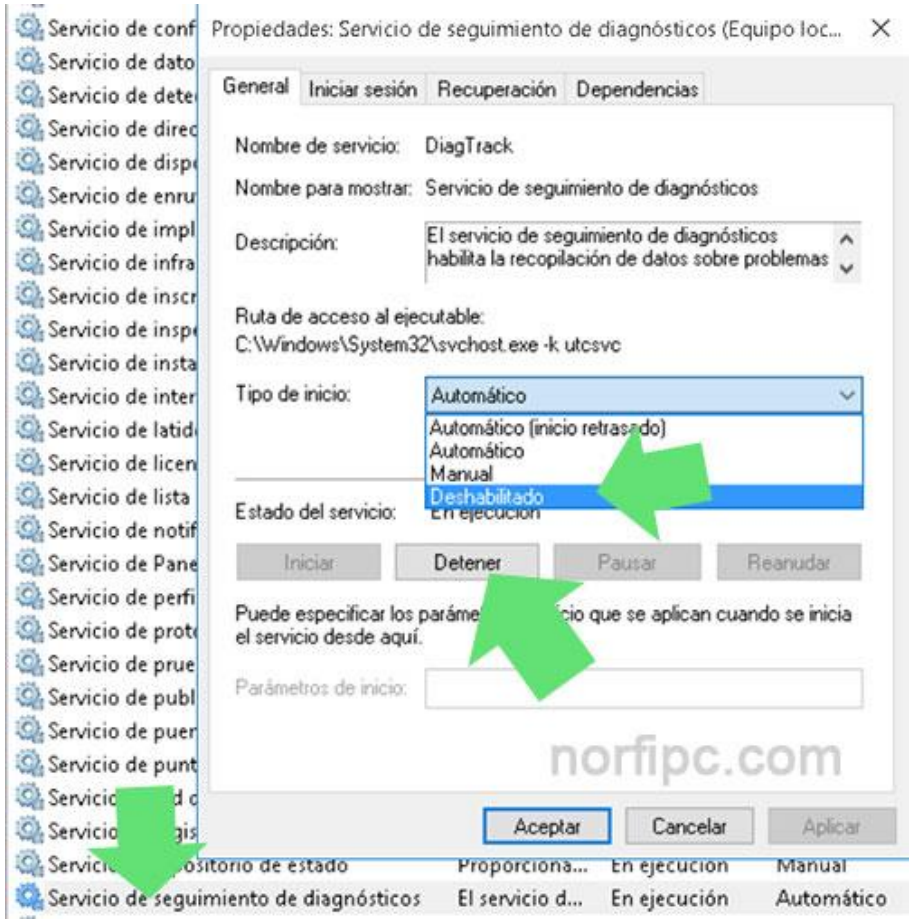
- Los servicios de Windows se pueden configurar para comenzar cuando se inicia el sistema operativo y ejecutarse en segundo plano mientras se ejecuta el sistema operativo. Alternativamente, se pueden iniciar manualmente o por un evento. Los sistemas operativos Windows incluyen numerosos servicios que se ejecutan en el contexto de tres cuentas de usuario: sistema, servicio de red y servicio local. Estos componentes de Windows a menudo se asocian con procesos de host para servicios de Windows. Debido a que los servicios de Windows funcionan en el contexto de sus propias cuentas de usuario dedicadas, pueden operar cuando un usuario no ha iniciado sesión.

- Los administradores de Windows pueden gestionar los servicios a través de:

- El complemento de Servicios (que se encuentra en Herramientas administrativas en el Panel de Control de Windows).
- Sc.exe
- Windows PowerShell

Servicios


Administración de equipos
Archivo Acción Ver Ayuda
Administración del equipo (local)
Herramientas del sistema
Programador de tareas
Visor de eventos
Carpetas compartidas
Rendimiento
Administrador de dispositivos
Almacenamiento
Administración de discos
Servicios y aplicaciones
Servicios
Control WMI
Nombre
Descripción
Estado
Tipo de inicio
Administrador de conexiones de Windows
Toma decisiones...
En ejecución
Automático (desencadenar inicio)
Administrador de configuración de dispositi...
Habilita la detec...
En ejecución
Manual (desencadenar inicio)
Administrador de credenciales
Proporciona un ...
En ejecución
Manual
Administrador de cuentas de seguridad
El inicio de este s...
En ejecución
Automático
Administrador de sesión local
Servicio central ...
En ejecución
Automático
Administrador de usuarios
El administrador ...
En ejecución
Automático (desencadenar inicio)
Agente de conexión de red
Conexiones de a...
En ejecución
Manual (desencadenar inicio)
Agente de directiva IPsec
El protocolo de s...
En ejecución
Manual (desencadenar inicio)
Agente de eventos de tiempo
Coordina la ejec...
En ejecución
Manual (desencadenar inicio)
Agente de eventos del sistema
Coordina la ejec...
En ejecución
Automático (desencadenar inicio)
Aislamiento de claves CNG
El servicio Aisla...
En ejecución
Manual (desencadenar inicio)
AMD External Events Utility
En ejecución
Automático
Aplicación auxiliar de NetBIOS sobre TCP/IP
Proporciona co...
En ejecución
Manual (desencadenar inicio)
Asignador de extremos de RPC
Resuelve identifi...
En ejecución
Automático
Audio de Windows
Administra el au...
En ejecución
Automático
norfipc.com


Propiedades: Servicio de seguimiento de diagnósticos (Equipo loc...
General
Iniciar sesión
Recuperación
Dependencias
Nombre de servicio: DiagTrack
Nombre para mostrar: Servicio de seguimiento de diagnósticos
Descripción: El servicio de seguimiento de diagnósticos habilita la recopilación de datos sobre problemas
Ruta de acceso al ejecutable:
C:\Windows\System32\svchost.exe -k utcsvc
Tipo de inicio: Automático
Automático (inicio retrasado)
Automático
Manual
Deshabilitado
Estado del servicio:
Iniciar
Detener
Pausar
Reanudar
Puede especificar los parámetros que se aplican cuando se inicia el servicio desde aquí.
Parámetros de inicio:
Aceptar
Cancelar
Aplicar
Servicio de seguimiento de diagnósticos
El servicio d...
En ejecución
Automático
norfipc.com

- - Administrador de mapas descargados (MapsBroker). Pueden Deshabilitarlo los que no usen la aplicación Mapas.
- - dmwappushservice (Servicio de enrutamiento de mensajes de inserción WAP). Deshabilitar para desactivar la Telemetría y recolección de datos por Microsoft.
- - GamesAppIntegrationService. Pueden detenerlo y deshabilitarlo los que no estén interesados en juegos.
- - IP Helper (Proporciona compatibilidad con la nueva tecnología IPv6). Pueden detenerlo y establecerlo en manual, los que su conexión a internet no soporta Ipv6.
- - Cola de impresión (Spooler). Pueden detenerlo y ponerlo en estado Manual los que no usen una impresora.
- - Geolocation Service (lfsvc). Pueden detenerlo y deshabilitarlo los que no usen servicios de geolocalización y los que desean mantener su privacidad a salvo.
- - Registro remoto (Permite modificar de forma remota desde otro equipo la configuración del Registro de Windows). Se puede deshabilitar por propósitos de seguridad.
- - Aplicación auxiliar de NetBIOS sobre TCP/IP (lmhosts). Pueden detenerlo y deshabitarlo los que no usen su equipo en una red local.

- - Security Center (Centro de seguridad). Monitorea constantemente el sistema, chequea diversos parámetros del antivirus, cortafuegos, Windows Update, control de usuarios y muestra notificaciones llamando a la acción.
- Lee mas información
- - Servicio Asistente para la compatibilidad de programas. Se puede detener y establecer como manual.
- - Servicio de seguimiento de diagnósticos. Se puede detener y deshabilitar para desactivar la Telemetría y recolección de datos por Microsoft.
- - Servicio de Panel de escritura a mano y teclado táctil. Pueden detenerlo y deshabilitarlo los que no posean un monitor táctil.
- - Servicio de Windows Defender. Pueden deshabilitarlo los que traten de usar un programa antivirus/antimalware adicional en el equipo y esto cause algún conflicto.
- - Servicio Informe de errores de Windows (WerSvc). Pueden Deshabilitar este servicio los que no les interese ni generar ni enviar informes a Microsoft sobre errores en programas o el sistema. De forma predeterminada está en estado manual y se inicia ante cualquier error.
- - Windows Update (Actualizaciones de Windows). Pueden detenerlo, los que experimenten conflictos por el excesivo consumo de internet del sistema en conexiones lentas y activarlo regularmente para comprobar la existencia de actualizaciones desde Microsoft y descargarlas.

Procesos linux

- top
- ps
- aux
- kill
- killall

Prioridades de procesos

- se puede determinar examinando la columna PRI del comando
  - ps -l o ps -efl.
- Dicha columna muestra la prioridad que tendrá el proceso en el sistema. Cuanto más alto sea el valor de esta columna, mayor prioridad tendrá el proceso.
- Un proceso con PRI de 100 tendrá máxima prioridad.
- También en este comando se puede observar la columna NI que muestra el nice number y que permite al sistema establecer la prioridad de un proceso.
- Su valor oscila entre −20 (más prioridad) y 20 (menos prioridad), siendo 0 su valor por defecto.

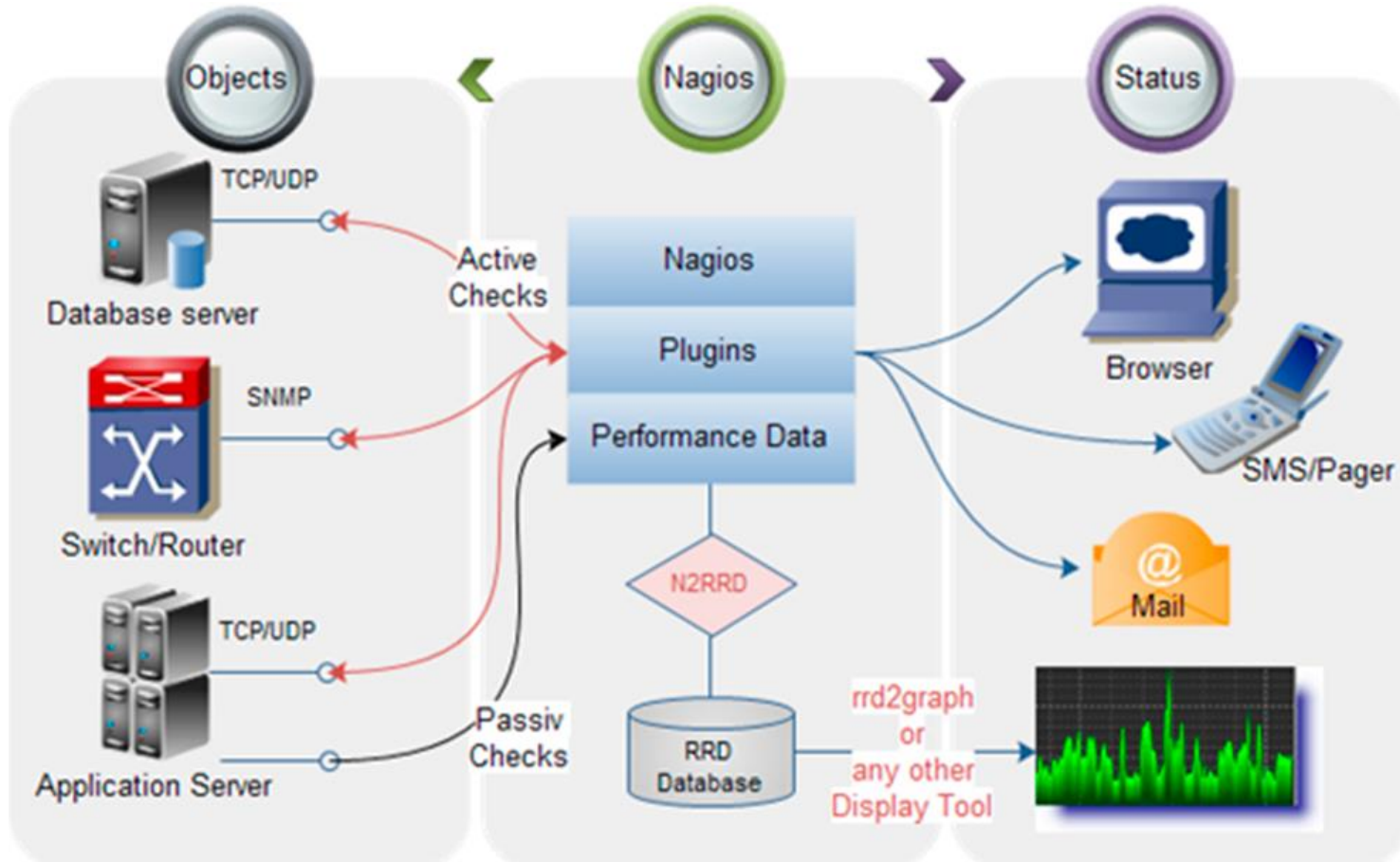
- El superusuario puede establecer la prioridad de los procesos a cualquier valor, mientras que cualquier otro usuario solamente podrá bajar la prioridad de sus procesos (por lo tanto, los usuarios solamente podrán especificar valores entre 1 y 20).
- Un ejemplo para establecer prioridades a los procesos puede ser el siguiente:
  - nice -n 20 top
- Se ejecutará el comando top con una prioridad baja (mínima prioridad), nice number=20.
  - nice -n -20 top
- Se ejecutará el comando top con una prioridad alta (máxima prioridad), nice number=-20

Herramientas de Monitorización

- Nagios
- Cacti
- …

NAGIOS

- Nagios es considerado como uno de los más populares, si no el más popular sistema de monitorización de red de código abierto disponible.
- Fue diseñado originalmente para ejecutarse en Linux, pero otras variantes de Unix son soportadas también. Nagios proporciona supervisión de los servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH) y recursos de host (carga del procesador, uso de disco, los registros del sistema), entre otros. El control remoto es manejado a través de túneles SSH o SSL cifrado.
- Nagios tiene un diseño simple que ofrece a los usuarios la libertad para desarrollar sus chequeos de servicio sin esfuerzo propio basado en las necesidades y mediante el uso de cualquiera de las herramientas de apoyo que guste. Para detectar y diferenciar entre hosts que están abajo y los que son inalcanzables, Nagios permite definir jerarquía de la red de acogida con los hosts "padre".
- Cuando los servicios o los problemas de acogida se plantean, la notificación será enviada a la persona que está a cargo de la red a través del correo electrónico, SMS, etc. http://nagios.org

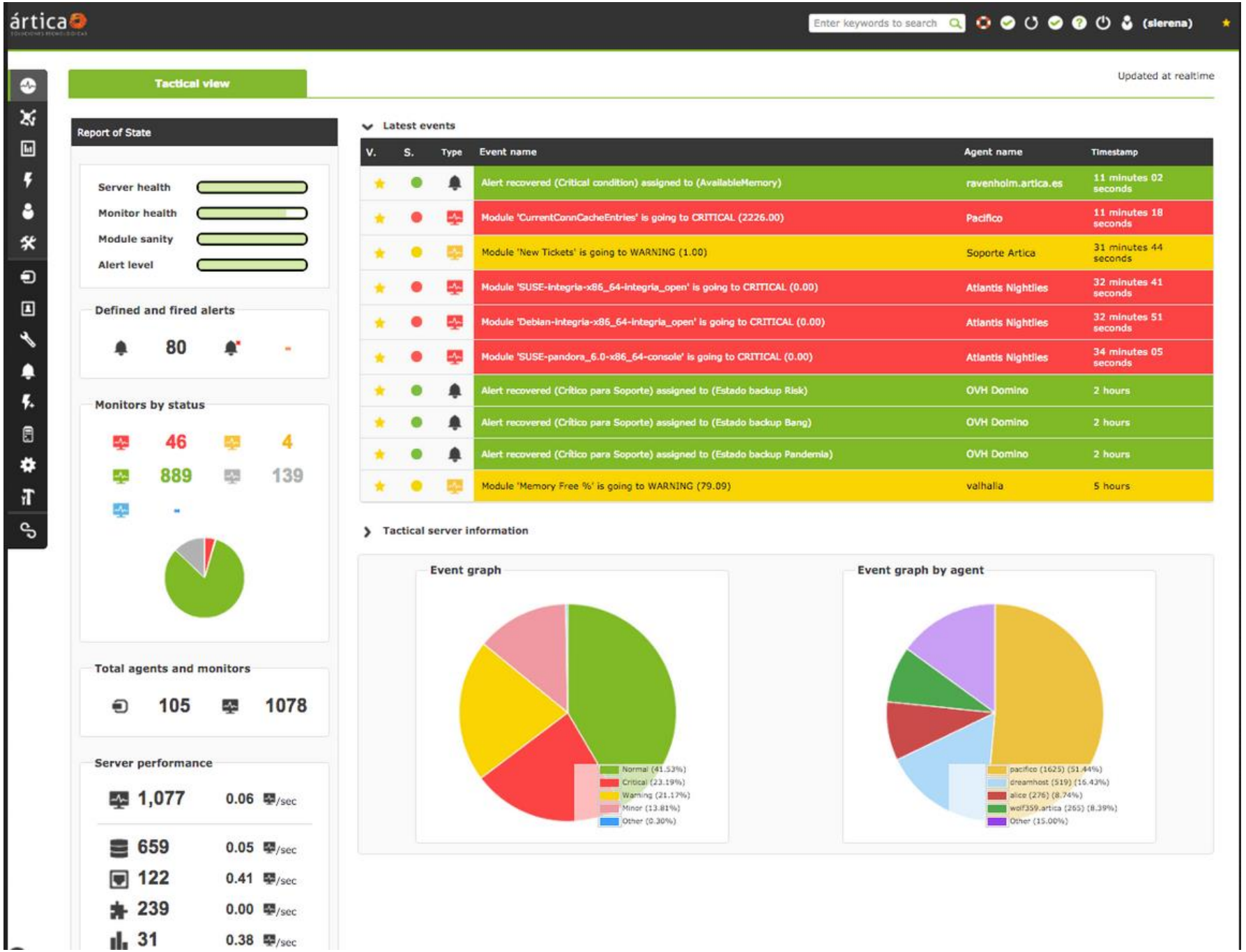

Objects
Nagios
Status
TCP/UDP
Database server
Active
Checks
Nagios
Plugins
Performance Data
Browser
SMS/Pager
SNMP
Switch/Router
N2RRD
Mail
TCP/UDP
Application Server
Passiv
Checks
RRD
Database
rrd2graph
or
any other
Display Tool

CACTI

- Cacti es una herramienta web de gráficas que está diseñada como una interfaz completa para almacenamiento de datos de RRDtool y la utilidad gráfica que permite a los usuarios monitorear y graficar la carga de la CPU, la utilización de ancho de banda de red, el tráfico de red, y mucho más.
- Puede ser utilizado para configurar la recopilación de datos en sí, lo que permite configuraciones particulares, a controlar sin ningún tipo de configuración manual de RRDtool. Cacti permite sondear los servicios en el período preestablecido y el gráfico de los datos resultantes.
- Se utiliza principalmente para representar gráficamente los datos de series temporales de parámetros tales como la carga de la CPU y la utilización de ancho de banda de red. Cacti se puede ampliar para controlar cualquier fuente a través de scripts de shell y ejecutables.
- También es compatible con arquitectura de plugins y tiene una comunidad grande y activa que se ha reunido en torno a los foros de Cacti para proporcionar scripts, plantillas y consejos sobre creación de plugins.
- http://www.cacti.net/

PANDORAFMS

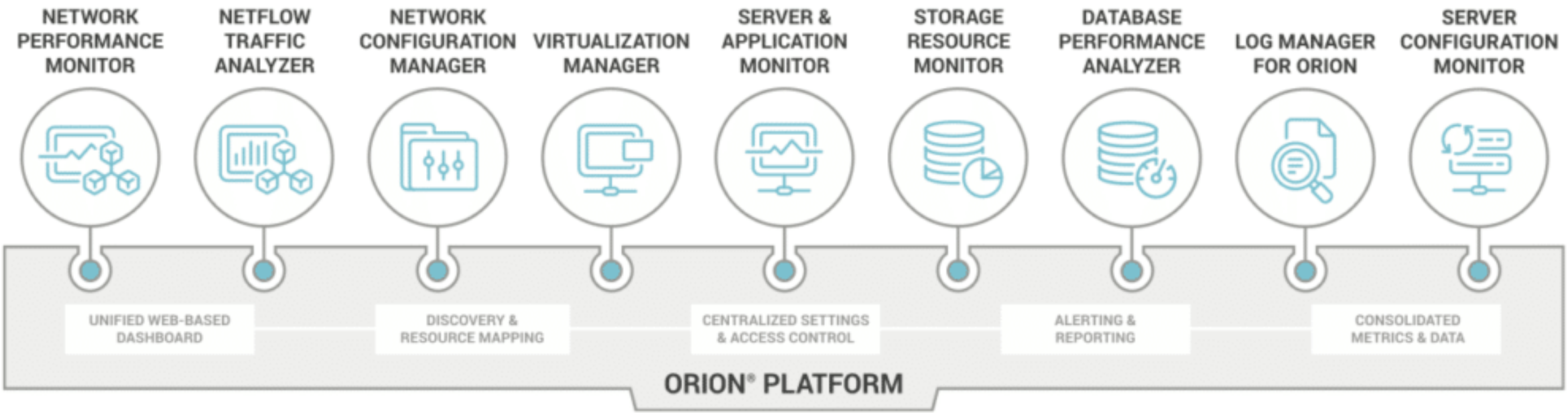
- Pandora FMS es el software de monitorización elegido por numerosas empresas de todo el mundo para gestionar su infraestructura IT. Además de garantizar un alto rendimiento y la máxima flexibilidad, cuenta con un gran número de funcionalidades que convierten a Pandora FMS en una de las herramientas más completas del mercado.
- Monitorización de red Autodescubra y monitorice su red al completo de una forma profesional y rápida. Soportamos todo tipo de tecnologías y topologías de red complejas y escalables.
- Monitorización MSP y SaaS Centralice y unifique en una única herramienta la gestión de su infraestructura y servicios, sean locales, remotos, físicos, virtuales o en la nube.
- Monitoreo de servidores Rendimiento, capacidad disponibilidad e inventario. Todo en uno, para todas las tecnologías de forma sencilla y centralizada.http://pandorafms.com/


ártica
Enter keywords to search
(slerena)
Tactical view
Updated at realtime
Report of State
Server health
Monitor health
Module sanity
Alert level
Defined and fired alerts
80
Monitors by status
46
4
889
139
Total agents and monitors
105
1078
Server performance
1,077
0.06 /sec
659
0.05 /sec
122
0.41 /sec
239
0.00 /sec
31
0.38 /sec
Latest events
V.
S.
Type
Event name
Agent name
Timestamp
Alert recovered (Critical condition) assigned to (AvailableMemory)
ravenholm.artica.es
11 minutes 02 seconds
Module 'CurrentConnCacheEntries' is going to CRITICAL (2226.00)
Pacifico
11 minutes 18 seconds
Module 'New Tickets' is going to WARNING (1.00)
Soporte Artica
31 minutes 44 seconds
Module 'SUSE-integria-x86_64-integria_open' is going to CRITICAL (0.00)
Atlantis Nightlies
32 minutes 41 seconds
Module 'Debian-integria-x86_64-integria_open' is going to CRITICAL (0.00)
Atlantis Nightlies
32 minutes 51 seconds
Module 'SUSE-pandora_6.0-x86_64-console' is going to CRITICAL (0.00)
Atlantis Nightlies
34 minutes 05 seconds
Alert recovered (Crítico para Soporte) assigned to (Estado backup Risk)
OVH Domino
2 hours
Alert recovered (Crítico para Soporte) assigned to (Estado backup Bang)
OVH Domino
2 hours
Alert recovered (Crítico para Soporte) assigned to (Estado backup Pandemia)
OVH Domino
2 hours
Module 'Memory Free %' is going to WARNING (79.09)
valhalla
5 hours
Tactical server information
Event graph
Normal (41.53%)
Critical (23.19%)
Warning (21.17%)
Minor (13.81%)
Other (0.30%)
Event graph by agent
pacifico (1625) (51.44%)
dreamhost (519) (16.43%)
alice (276) (8.74%)
wolf359.artica (265) (8.39%)
Other (15.00%)

Solarwinds

- Herramientas de administración de redes, desde configuración e inteligencia de tráfico a monitoreo del desempeño y mapeo de topologías, para ver, comprender y resolver problemas a tiempo. Un enfoque integrado de varios proveedores fácil de usar, extender y escalar a fin de optimizar las redes distribuidas.

- Desde sistemas, direcciones IP y máquinas virtuales hasta contenedores y servicios. Optimice el uso de recursos y reduzca la MTTR con capacidades potentes de monitoreo, detección, asignación de dependencias, alertas, informes y planificación de capacidades.


NETWORK PERFORMANCE MONITOR
NETFLOW TRAFFIC ANALYZER
NETWORK CONFIGURATION MANAGER
VIRTUALIZATION MANAGER
SERVER & APPLICATION MONITOR
STORAGE RESOURCE MONITOR
DATABASE PERFORMANCE ANALYZER
LOG MANAGER FOR ORION
SERVER CONFIGURATION MONITOR
UNIFIED WEB-BASED DASHBOARD
DISCOVERY & RESOURCE MAPPING
CENTRALIZED SETTINGS & ACCESS CONTROL
ALERTING & REPORTING
CONSOLIDATED METRICS & DATA
ORION® PLATFORM

Solarwinds


solarwinds
MY DASHBOARDS
ALERTS & ACTIVITY
REPORTS
SETTINGS
GUEST (LOGOUT)
HELP
NPM Summary
Friday, 09 October 2020 16:13:40
All Nodes managed by NPM
GROUPED BY VENDOR, STATUS
MANAGE NODES
HELP
American Power Conversion Corp.
Avaya Communication
Cisco
Up
Critical
NEWY-2811-WAN
Down
Warning
AUS-SUB-01
DEN-2960-1A
DEN-3750-SwitchStack
EAST-4506E-CORE
EAST-9300-1stFl
FIBRE-Tex-Mds9120
LON-3560-AS1.demo.lab
LON-3560-AS2.demo.lab
LOSA-2821-WAN
NX-7K-B-admin
SIN-3560-AS1.demo.lab
SIN-3560-AS2.demo.lab
WEST-3850-CORE
Dell Computer Corporation
F5 Networks, Inc.
H3C
IBM
InfoBlox Inc.
Juniper Networks, Inc.
Linux
Meraki Networks, Inc.
Netgear
Nutanix Inc.
Palo Alto Networks
SonicWALL, Inc.
MPLS Network
VIEW MODE
Cisco ACI Map
VIEW MODE
List of Switch Stacks
CAPTION
IP ADDRESS
MAC ADDRESS
MEMBER COUNT
STATUS
DATA RING STATUS
WEST-3850-CORE
10.129.0.1
DC:A5:F4:78:07:80
4
Warning
EAST-9300-1stFl
10.1.0.21
D4:AD:BD:70:F3:80
2
Up
DEN-3750-SwitchStack
10.1.120.23
00:25:46:6F:46:80
7
Up
Interfaces with High Percent Utilization
HELP
NODE
INTERFACE
RECEIVE
TRANSMIT
Nexus-2
port-channel31 - Po31
90%
60%
Nexus-1
Ethernet1/11 - Eth1/11
90%
30%
Nexus-2
mgmt0 - management0
30%
85%
Nexus-1
mgmt0 - management0
30%
85%
EAST-RP
eth0
86%
24%
Page 1 of 2
Items on page 5
Show all

Ataque a Solarwinds

- https://www.e-dea.co/ataque-solarwinds-orion#:~:text=Este%20ataque%20fue%20un%20ataque,los%20usuarios%20posteriores%20del%20software.