Área Tenerife 2030: Innovación, Educación, Cultura y Deportes.
Consejería con Delegación Especial en TIC y Sociedad de la Información
Servicio Técnico de Informática y Comunicaciones

CABILDO INSULAR DE TENERIFE

PROTOCOLO DE MONITORIZACIÓN

Calle Clavel, 2
38003 Santa Cruz de Tenerife
Tfno.: 922 239 999
Fax: 922 239 468
www.tenerife.es

Índice

1. Introducción

La infraestructura TI del Cabildo Insular de Tenerife debe ser monitorizada en horario de cobertura de 24x7x365 por personal especializado en este tipo de tareas.

Para dicha monitorización, se utilizan principalmente la plataforma basada en Nagios del propio Cabildo, aunque también se pueden realizan ciertas labores complementarias desde las plataformas del adjudicatario del CSU-ATIC.

Dichas labores complementarias deben incluir la monitorización de estos servicios:

- Operatividad de las URLs de tenerife.es:
  - Portal Web Corporativo
  - Extranet
  - Correo Web (OWA)
- Portal de Tramitación Electrónica
- Disponibilidad del dominio DNS cabtfe.es

2. Descripción del servicio

Los métodos de contacto con el servicio son:

2.1 Acuerdo de nivel de servicios ANS

Los establecidos para el servicio CSU-ATIC.

3. Protocolo de actuación

Ante la detección de una alerta el protocolo a seguir es el siguiente.

3.1 Notificación de Alerta

- Nagios notifica por correo electrónico la existencia de la nueva alerta:
  - A los técnicos definidos dentro de la lista de distribución establecida con este fin por el adjudicatario.
  - A la dirección csu@tenerife.es, para la creación automática de la incidencia dentro de Ca SD.
- Los servicios que notifican sus alertas por correo electrónico son aquellos que están configurados para ello dentro de Nagios/Centreon. Deberán estar activadas todas las comprobaciones posibles para lograr la mayor cobertura posible de los servicios en producción.
- De manera general, los servicios relacionados con **servidores de preproducción y desarrollo, tienen las notificaciones deshabilitadas**, así como algunos servicios asociados a servidores de producción (CPU, memoria y ancho de banda).
- Los servicios identificados por el Cabildo de Tenerife como “críticos” (aquellos que están dentro del grupo de servicios “**SERV_CRIT**” de Centreon), incluyen además en el asunto de la notificación la palabra "SERVICIO CRÍTICO" para una mejor identificación de la alerta y de la prioridad de la misma.

3.2 Creación de la incidencia en la herramienta de tiques

- Al enviarse una notificación a la dirección csu@tenerife.es, se crea automáticamente un ticket en el software de gestión de tiques, con la siguiente categorización:
  - Como “Solicitante”, aparecerá el usuario “Sistema Nagios”.
  - El tipo de ticket será “Incidente”.
  - El método informativo será “Monitorización”.
  - La categoría y el nombre de servicio afectado se asignarán en función del nombre del servicio que presenta la alarma en Nagios.
  - El grupo de resolución asignado será el grupo “N1 Monitorización”. En él, estará ubicado el personal que supervisará las incidencias de monitorización independientemente del horario.
  - La prioridad será alta para incidencias crítica y normal para el resto.

3.3 Confirmar alerta en Centreon

- Una vez se ha recibido la notificación y abierta la incidencia, el técnico de monitorización debe diagnosticar si se trata de una incidencia real o de un falso positivo. Dicha comprobación se realiza desde la consola web de Centreon lanzando una recomprobación manual y si es necesario realizando una verificación directa sobre el sistema afectado. Si transcurridos 5 minutos la alerta sigue presente en Centreon, consideramos que se trata de una alerta real. En caso contrario, es decir, si la alerta desaparece, consideramos que se trata de un falso positivo.
- En caso de que la alerta sea real, el técnico deberá reconocerla desde la consola de Centreon, evitando así que sigan llegando más alarmas y creándose nuevas incidencias:
    - Marcar la alerta seleccionando la casilla que aparece justo a la izquierda del nombre del host.
    - En el menú “Más acciones” seleccionar “Servicios: Aprobación”.
    - Marcar la opción “Sticky”, dejar el resto desmarcado.
    - Poner en el comentario el número de ticket creado en el que está siendo tratado el problema.
    - Pulsar el botón de “Acknowledge”.
    - Se deberá informar a través de correo electrónico la ocurrencia y confirmación de la alarma a los siguientes destinatarios:
        - cau@tenerife.es.
        - Listas del CSU-ATIC del personal involucrado en el tratamiento de la alarma.
        - Jefe de Servicio y responsables del STIC (lista de contactos en el siguiente apartado).

3.4 Cancelar o tratar la incidencia

- En caso de que se trata de un falso positivo, el técnico de monitorización deberá cancelar la incidencia.
- En caso de que la alerta sea real, el técnico debe comenzar a tratar la incidencia según lo indicado en los procedimientos de tratamiento en la MediaWiki.

3.5 Escalado

En caso de que no exista un procedimiento en la Wiki del ~~I3C~~ STIC para resolver la incidencia desde el primer nivel de atención (N1 Monitorización), se deberá proceder a escalar la incidencia, teniendo en cuenta lo siguiente:

1. Se realizará el escalado dentro de Service Desk.
2. En el caso de que se trate de una incidencia crítica se llamará por teléfono a uno de los técnicos que esté disponible en ese momento y se realizará una notificación por correo electrónico a los responsables del STIC (Jefe de Servicio y Responsables).

Los contactos por parte del STIC son los siguientes:

TÉCNICO	CARGO	TELÉFONO DE CONTACTO	CORREO ELECTRÓNICO

3.6 Seguimiento

Se aplicará el proceso de seguimiento establecido para el servicio actualmente:

Prioridad	Frecuencia de seguimiento	Protocolo de actuación
Critica	Cada 30 minutos	Llamada telefónica al técnico de Guardia Notificación manual en herramienta de tiques a responsables CSU y STIC Registro en el ticket
Alta	Cada 1 hora	Llamada telefónica al técnico de Guardia Notificación manual a responsables CSU y STIC Registro en el ticket

En cada revisión de los tickets generados por monitorización, deberá comprobarse si las alarmas que lo generaron siguen presentes en el sistema. De no ser así, el ticket correspondiente deberá ser cerrado (no se cancela dado que, al tener una duración suficiente, no se considera un falso positivo), pasándolo al estado “cerrado sin resolver”.

De manera general, al inicio del horario ampliado de servicio, los técnicos de N2 realizarán una revisión exhaustiva de los tickets de SD relacionados con alarmas de Monitorización Nagios.

3.7 Informe

Se entregará un **informe diario**, a primera hora de la mañana con los siguientes datos:

- Resumen de alarmas en el período (diario)
    - Número de alarmas generadas en el período (volumetría)
        - Acumulados agrupados por:
            - Estado por prioridad.
            - Grupos de hosts.
            - Grupos de servicios.
    - Alarmas activas a la finalización del período:
        - Acumulados agrupados por:
            - Estado: Reconocidas y no reconocidas.
            - Estado por prioridad.
            - Grupos de hosts.
            - Grupos de servicios.
        - Detalle de alarmas agrupadas por:
            - Estado: Reconocidas y no reconocidas
            - Estado por prioridad.
            - Grupos de hosts.
            - Grupos de servicios.

Por otro lado, los técnicos de N2 enviarán diariamente y antes de las 8:00h un correo electrónico informando del tratamiento que se está realizando de las alarmas de monitorización indicadas en el informe. También se indicarán las posibles causas de aparición de las alarmas que aparecieron en horario no presencial y que ya no están presentes.

El correo electrónico se enviará a los responsables del STIC (ver datos de contacto en apartado 3.5). Así mismo, se incluirá en copia a la lista de distribución de N1 CSU para que estén informados y puedan gestionar mejor las potenciales llamadas de los usuarios.

El **correo electrónico** a enviar seguirá este formato:

> *Las alarmas vigentes actualmente son las siguientes:*
>
> > *1. Alarma "x": se debe indicar el servicio TI afectado y las acciones que se están llevando a cabo para resolver el problema.*
> >
> > *2. (lo mismo para todas las alarmas presentes)*
>
> *Las alarmas aparecidas y que ya no están presentes en el sistema son las siguientes:*
>
> > *1. Alarma "y": se debe indicar:*
> >
> > > *a. La hora en la que se generó la alarma*
> > >
> > > *b. La hora en la que despareció*
> > >
> > > *c. La posible causa de su activación*
> > >
> > > *d. Una propuesta de solución a la misma*
> >
> > *2. (lo mismo para todas las alarmas no presentes)*