Resumen de Tablas - Cloud Pak for AIOps para IBM Cognos

Proyecto: Integración Cloud Pak for AIOps con IBM Cognos
Fecha: Octubre 2025

Introducción

Este documento describe las tablas exportadas por Cloud Pak for AIOps que se utilizan para crear dashboards y reportes en IBM Cognos. El esquema incluye tablas principales de estado (status) y tablas de auditoría para rastrear cambios históricos.

---

1. TABLAS DE ALERTAS

1.1 ALERTS_REPORTER_STATUS ⭐ MUY IMPORTANTE

Descripción: Tabla principal que contiene los datos actuales de todas las alertas en el sistema.

Campos Clave:

- `uuid` (PK): Identificador único de la alerta
- `tenantid`: Identificador del tenant/organización
- `id`: ID de la alerta
- `severity`: Nivel de severidad (0-6)
- `state`: Estado actual de la alerta
- `summary`: Resumen descriptivo de la alerta
- `owner`: Usuario propietario de la alerta
- `team`: Equipo asignado
- `businessCriticality`: Criticidad de negocio
- `firstOccurrenceTime`: Primera vez que ocurrió
- `lastOccurrenceTime`: Última vez que ocurrió
- `lastStateChangeTime`: Último cambio de estado
- `eventCount`: Contador de eventos
- `acknowledged`: Indicador de reconocimiento (0/1)

Campos Booleanos (0/1):

- `runbooks`: Tiene runbooks asociados
- `topology`: Tiene topología asociada
- `seasonal`: Es estacional
- `inIncident`: Está en un incidente
- `suppressed`: Está suprimida
- `anomalyInsights`: Tiene insights de anomalías
- `triggerAlert`: Es una alerta disparadora

Uso en Cognos: Esta es la tabla más importante para dashboards de alertas. Permite crear:

- Métricas de alertas activas por severidad
- Distribución por equipo y owner

- Alertas sin resolver
- Tendencias de eventos

1.2 ALERTS_SEVERITY_TYPES ⭐ IMPORTANTE

Descripción: Tabla de referencia estática con los tipos de severidad.

Valores:

- 0 = Clear
- 1 = Indeterminate
- 2 = Information
- 3 = Warning
- 4 = Minor
- 5 = Major
- 6 = Critical

Uso en Cognos: Tabla de lookup para convertir códigos numéricos de severidad en texto legible.

1.3 ALERTS_AUDIT_SEVERITY

Descripción: Tabla de auditoría que registra todos los cambios de severidad de las alertas a lo largo del tiempo.

Campos Clave:

- `uuid` (FK): Referencia a la alerta
- `lastStateChangeTime`: Timestamp del cambio
- `endDate`: Fecha de fin del período
- `severity`: Nivel de severidad en ese momento
- `state`: Estado (0=activo, 1=cerrado)

Uso en Cognos: Permite análisis histórico de escalamiento/desescalamiento de severidad.

1.4 ALERTS_AUDIT_ACK

Descripción: Registra el historial de reconocimientos (acknowledgements) de alertas.

Campos Clave:

- `uuid` (FK): Referencia a la alerta
- `acknowledged`: Valor del reconocimiento
- `lastStateChangeTime`: Timestamp del cambio
- `owner`: Usuario que reconoció
- `state`: Estado (0=activo, 1=cerrado)

Uso en Cognos: Métricas de tiempo de reconocimiento y responsabilidad.

1.5 ALERTS_AUDIT_OWNER

Descripción: Registra cambios en la propiedad/asignación de alertas.

Campos Clave:

- `oldOwner`: Propietario anterior
- `owner`: Nuevo propietario
- `lastStateChangeTime`: Timestamp del cambio

Uso en Cognos: Análisis de reasignaciones y carga de trabajo.

1.6 ALERTS_AUDIT_TEAM

Descripción: Registra cambios en la asignación de equipos.

Campos Clave:

- `oldTeam`: Equipo anterior
- `team`: Nuevo equipo
- `lastStateChangeTime`: Timestamp del cambio

Uso en Cognos: Análisis de redistribución de alertas entre equipos.

1.7 ALERTS_STATUS_VW ⭐ IMPORTANTE

Descripción: Vista consolidada que presenta las alertas con campos legibles para reportes.

Características:

- Convierte códigos de severidad a texto (usando ALERTS_SEVERITY_TYPES)
- Formatea timestamps para mejor legibilidad
- Convierte campos booleanos a "Yes"/"No"

Uso en Cognos: Vista ideal para reportes finales al usuario, ya que presenta datos en formato amigable.

1.8 ALERTS_AUDIT

Descripción: Vista unificada de todos los cambios de auditoría (severidad, acknowledgement, owner, team).

Uso en Cognos: Vista consolidada para reportes de historial de cambios y auditoría.

---

2. TABLAS DE INCIDENTES

2.1 INCIDENTS_REPORTER_STATUS ⭐ MUY IMPORTANTE

Descripción: Tabla principal que contiene los datos actuales de todos los incidentes en el sistema.

Campos Clave:

- `uuid` (PK): Identificador único del incidente
- `tenantid`: Identificador del tenant/organización
- `id`: ID del incidente
- `title`: Título del incidente

- `description`: Descripción detallada
- `priority`: Nivel de prioridad
- `state`: Estado actual del incidente
- `owner`: Usuario propietario
- `team`: Equipo asignado
- `createdTime`: Fecha de creación
- `createdBy`: Usuario creador
- `lastChangedTime`: Último cambio

Campos Numéricos de Relaciones:

- `alerts`: Número de alertas asociadas
- `similarIncidents`: Incidentes similares
- `splitIncidents`: Incidentes divididos
- `probableCauseAlerts`: Alertas de causa probable
- `tickets`: Tickets asociados
- `chatOpsIntegrations`: Integraciones de ChatOps

Uso en Cognos: Tabla más importante para dashboards de incidentes. Permite crear:

- Métricas de incidentes activos por prioridad
- Distribución por equipo y owner
- Tiempo de resolución
- Relación incidentes-alertas

2.2 INCIDENTS_AUDIT_PRIORITY

Descripción: Tabla de auditoría que registra cambios en la prioridad de incidentes.

Campos Clave:

- `uuid` (FK): Referencia al incidente
- `lastChangedTime`: Timestamp del cambio
- `priority`: Nivel de prioridad
- `complete`: Estado (0=activo, 1=cerrado)

Uso en Cognos: Análisis de escalamiento de prioridades y tendencias.

2.3 INCIDENTS_AUDIT_STATE

Descripción: Registra todos los cambios de estado del ciclo de vida de incidentes.

Campos Clave:

- `uuid` (FK): Referencia al incidente
- `state`: Estado del incidente
- `lastChangedTime`: Timestamp del cambio
- `owner`: Propietario en ese momento
- `complete`: Estado (0=activo, 1=cerrado)

Uso en Cognos: Análisis de flujo de trabajo y tiempo en cada estado.

2.4 INCIDENTS_AUDIT_OWNER

Descripción: Registra cambios en la propiedad/asignación de incidentes.

Campos Clave:

- `oldOwner`: Propietario anterior
- `owner`: Nuevo propietario
- `lastChangedTime`: Timestamp del cambio

Uso en Cognos: Análisis de reasignaciones y gestión de carga de trabajo.

2.5 INCIDENTS_AUDIT_TEAM

Descripción: Registra cambios en la asignación de equipos para incidentes.

Campos Clave:

- `oldTeam`: Equipo anterior
- `team`: Nuevo equipo
- `lastChangedTime`: Timestamp del cambio

Uso en Cognos: Análisis de redistribución de incidentes entre equipos.

2.6 INCIDENTS_STATUS_VW ⭐ IMPORTANTE

Descripción: Vista simplificada de incidentes para reportes.

Campos incluidos:

- priority, state, id, title
- alerts (conteo)
- createdTime (formateado)
- team, owner

Uso en Cognos: Vista ideal para dashboards ejecutivos con información consolidada.

2.7 INCIDENTS_AUDIT

Descripción: Vista unificada de todos los cambios de auditoría (estado, prioridad, owner, team).

Uso en Cognos: Vista consolidada para reportes de historial completo y compliance.

---

3. TABLAS MÁS IMPORTANTES PARA DASHBOARDING

🏆 Top 5 para Cognos:

1. **ALERTS_REPORTER_STATUS**
   - Dashboard operativo de alertas
   - KPIs en tiempo real

    - Distribución y análisis actual
2. **INCIDENTS_REPORTER_STATUS**
    - Dashboard operativo de incidentes
    - Estado actual de problemas
    - Métricas de gestión
3. **ALERTS_STATUS_VW**
    - Reportes ejecutivos de alertas
    - Presentación amigable al usuario
    - Datos formateados
4. **INCIDENTS_STATUS_VW**
    - Reportes ejecutivos de incidentes
    - Vista simplificada para management
    - Información de alto nivel
5. **ALERTS_SEVERITY_TYPES**
    - Lookup esencial para todos los reportes
    - Traducción de códigos a texto
    - Referencia constante

---

4. RELACIONES ENTRE TABLAS

Modelo de Alertas:

ALERTS_REPORTER_STATUS (principal)
├── ALERTS_AUDIT_SEVERITY (1:N)
├── ALERTS_AUDIT_ACK (1:N)
├── ALERTS_AUDIT_OWNER (1:N)
└── ALERTS_AUDIT_TEAM (1:N)

ALERTS_SEVERITY_TYPES (lookup)
└── Relacionada con severity en todas las tablas

Modelo de Incidentes:

INCIDENTS_REPORTER_STATUS (principal)
├── INCIDENTS_AUDIT_PRIORITY (1:N)
├── INCIDENTS_AUDIT_STATE (1:N)
├── INCIDENTS_AUDIT_OWNER (1:N)
└── INCIDENTS_AUDIT_TEAM (1:N)

---

5. RECOMENDACIONES PARA COGNOS

Dashboards Recomendados:

1. Dashboard Operativo - Alertas

- Tablas: ALERTS_REPORTER_STATUS, ALERTS_STATUS_VW
- Métricas: Alertas por severidad, por equipo, no reconocidas
- Gráficos: Distribución de severidad, tendencia temporal

2. Dashboard Operativo - Incidentes

- Tablas: INCIDENTS_REPORTER_STATUS, INCIDENTS_STATUS_VW
- Métricas: Incidentes por prioridad, por estado, por equipo
- Gráficos: Backlog, tiempo medio de resolución

3. Dashboard Ejecutivo

- Tablas: Vistas (ALERTS_STATUS_VW, INCIDENTS_STATUS_VW)
- Métricas: KPIs de alto nivel, SLA compliance
- Gráficos: Tendencias, comparativas

4. Dashboard de Auditoría

- Tablas: ALERTS_AUDIT, INCIDENTS_AUDIT
- Métricas: Cambios por período, reasignaciones
- Gráficos: Timeline de cambios, análisis de workflow

Campos Calculados Útiles:

1. **Tiempo de Respuesta (Alertas):**
   - `lastStateChangeTime - firstOccurrenceTime`
2. **Tiempo de Vida del Incidente:**
   - `lastChangedTime - createdTime`
3. **Tasa de Reconocimiento:**
   - `COUNT(acknowledged = 1) / COUNT(*)`
4. **Alertas por Incidente:**
   - Desde INCIDENTS_REPORTER_STATUS.alerts

Filtros Importantes:

- **tenantid**: Para ambientes multi-tenant
- **state**: Para filtrar alertas/incidentes activos
- **Rangos de fecha**: Para análisis temporal
- **team/owner**: Para vistas por responsable

---

6. NOTAS TÉCNICAS

Triggers y Automatización:

- Los scripts incluyen triggers que automáticamente populan las tablas de auditoría
- Los cambios en las tablas STATUS generan registros automáticos en las tablas AUDIT

Índices:

- Todas las tablas de auditoría tienen índices en `uuid` para optimizar joins
- Los índices mejoran el rendimiento de queries en Cognos

Integridad Referencial:

- Foreign keys con `ON DELETE CASCADE` aseguran limpieza automática
- Los registros de auditoría se eliminan cuando se elimina el registro principal

---

Conclusión

Para un dashboarding efectivo en Cognos, enfócate en:

1. **Tablas STATUS** para datos actuales y KPIs operativos
2. **Vistas (_VW)** para reportes ejecutivos con formato amigable
3. **Tablas AUDIT** para análisis históricos y compliance
4. **ALERTS_SEVERITY_TYPES** como tabla de referencia esencial

La combinación de estas tablas permite crear dashboards completos que cubren tanto aspectos operativos como estratégicos de la gestión de alertas e incidentes.