Artículo
Javier Lorenzo Mesa · 16 jul, 2021 Lectura de 5 min

DeepSee: Cómo configurar la seguridad - Parte 1 de 5

Tengo algunos modelos analíticos y numerosos paneles de control, y estoy listo para implementarlos en nuestros usuarios finales y administradores. ¿Cómo configurar DeepSee para que **los usuarios no alteren las áreas de los demás y se les restrinja** el uso de funciones específicas para los desarrolladores?

Ejecutar un sistema de *Business Intelligence* requiere, con frecuencia, configurar un modelo de seguridad. Este tutorial mostrará cómo configurar un modelo de seguridad sencillo para DeepSee.

El modelo de seguridad se basa en tres tipos de usuarios. Primero, crearemos un usuario sencillo para DeepSee que tenga acceso pero no pueda editar los paneles de control en DeepSee. El segundo tipo de usuario tendrá acceso a las tablas dinámicas en Analyzer y podrá visualizar, editar y crear paneles de control. Finalmente, los usuarios que son " Administradores " tendrán un control más amplio de la implementación, como el acceso a Architect.

También veremos cómo proteger y controlar la visibilidad de los elementos del modelo, como tablas dinámicas, paneles de control, modelos analíticos, etc. Esperamos que estos consejos para solucionar problemas faciliten la implementación de un modelo de seguridad.

Antes de empezar

En este artículo configuraremos un modelo de seguridad básico. Para ello, es necesario familiarizarse con esta página sobre Cómo configurar la seguridad para DeepSee. Si estás probando o creando una prueba de concepto, no utilices la base de datos o el namespace SAMPLES, ya que tiene una configuración especial. En vez de ello, trabaja en un namespace (por ejemplo, APP) con base(s) de datos dedicada(s) (por ejemplo, APP-DATA).

Para continuar con este tutorial, crea un namespace APP basado en una base de datos de APP-DATA en el Portal de administración de seguridad [SMP] > *Configuration* > *System Configuration* > *Namespaces*. Asigna un nuevo recurso %DBAPP-DATA a la base de datos recién creada. Asegúrate de que la aplicación web predeterminada para el namespace APP (/csp/app) está habilitada en DeepSee. Asumimos que tienes un servidor o una instalación personalizada, desde los que puedes iniciar sesión en Caché con un usuario que tiene los privilegios suficientes para ejecutar las operaciones de esta publicación.

Cómo conceder acceso de solo lectura a los paneles de control

En una implementación habitual, se permite que los usuarios finales utilicen Analytics, pero no pueden editar la implementación como tal. En esta sección definiremos un tipo de usuario que solo puede acceder pero no editar los paneles de control de DeepSee.

Cómo crear un rol DSUser

Según la documentación (mira la fila de la tarea "Viewing the User Portal apart from the Analyzer or the mini Analyzer with no ability to create dashboards" / " Ver el Portal de usuario de forma independiente a Analyzer o al mini Analyzer sin la capacidad de crear paneles " en la tabla), necesitamos permisos de USO para utilizar los recursos de %DeepSeePortal.

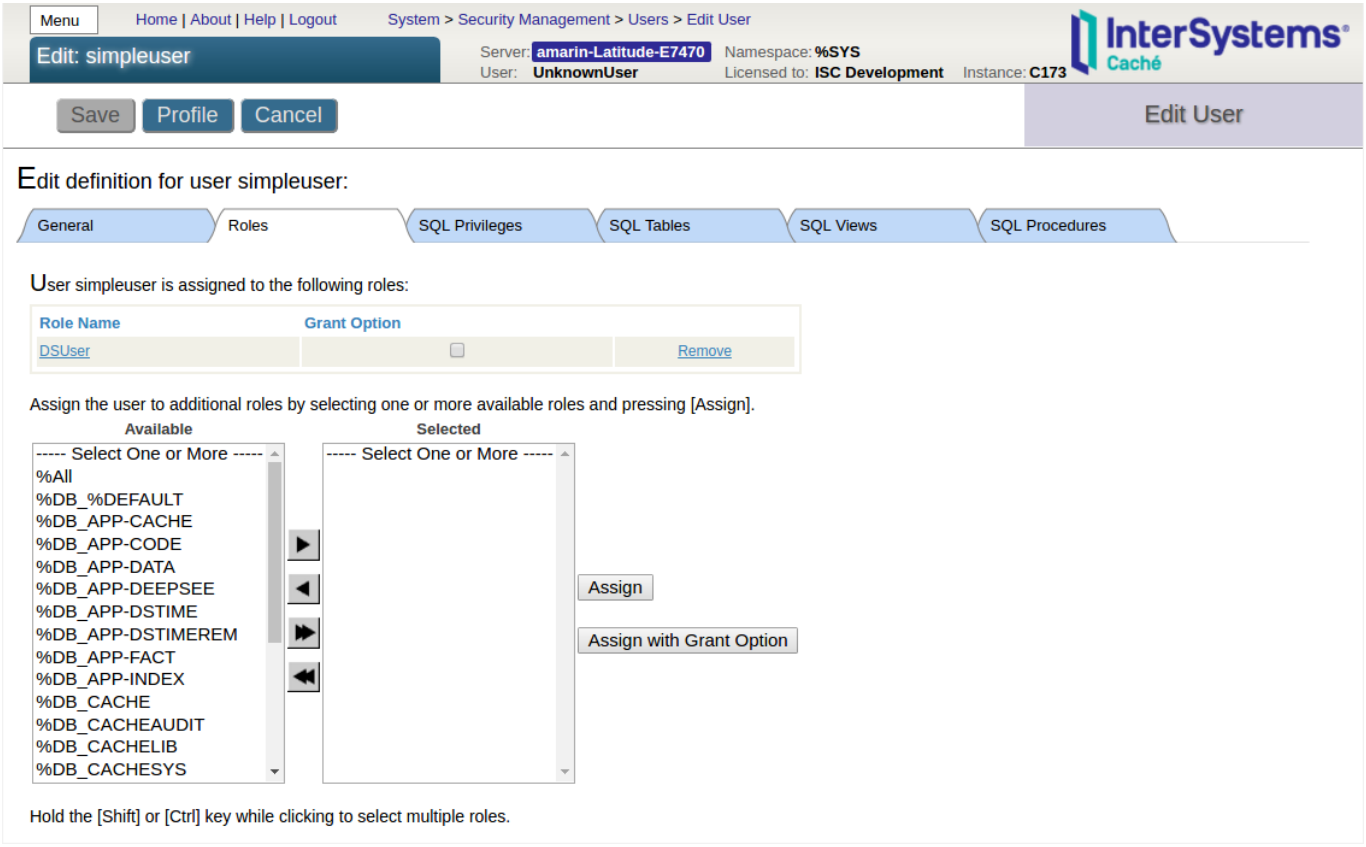
Crea un rol DSUser que incluya los siguientes recursos:

Recurso	Permiso
%DeepSeePortal	USE
%DBAPP-DATA	RW

Los permisos U y RW para el recurso que se encuentra en la tabla anterior deben configurarse automáticamente cuando asignes los roles. Dependiendo de tu namespace, base de datos y configuración de diagramas, necesitarás un permiso RW para proteger los recursos de las bases de datos. En nuestro ejemplo, %DBAPP-DATA es necesario para acceder a la base de datos predeterminada del namespace APP.

Cómo crear un simpleuser

En *Users page* > *Create new user* puedes crear un simpleuser con el rol DSUser asignado, como se muestra en esta captura de pantalla:



Cómo probar simpleuser

Abre una ventana de incógnito o privada en el navegador e inicia sesión como simpleuser. Desde el portal de administración, comprueba que las pestañas Architect y Analyzer en la sección DeepSee aparecen sombreadas en gris. Ve al *User Portal* / Portal de Usuario y confirma que simpleuser puede visualizar los paneles de control. También confirma que simpleuser no puede ver el botón *Save* en los paneles de control ni el icono " + " en el *User Portal* para crear elementos en la carpeta. Ten en cuenta que simpleuser puede visualizar tablas dinámicas en el *User Portal*, pero cuando intente ver una tabla dinámica debería mostrar que el usuario no está autorizado a ver la página. En esta sección de la parte 5, más adelante, veremos cómo ocultar las tablas dinámicas en el *User Portal*.

Consejo: utiliza dos ventanas del navegador. Una ventana se puede utilizar para iniciar sesión con un usuario administrador (por ejemplo, SYSTEM o SuperUser) que puede cambiar la configuración del sistema. En la otra ventana, utiliza un navegador en modo incógnito (Chrome) o privado (Firefox, Edge) e inicia sesión con un usuario de prueba. El modo incógnito/privado asegurará que el caché del navegador de la otra ventana no interfiere con tu trabajo y genere algún comportamiento inesperado.

Consejo: en el Portal de administración utiliza el botón *Menu* en la esquina superior izquierda para navegar rápidamente a las páginas de *Users* / Usuarios, *Roles* / Funciones, *Resources* / Recursos y *Web applications* / Aplicaciones web.

Cómo solucionar problemas: permisos públicos

Un problema habitual es encontrar que se permiten algunas funciones a pesar del modelo de seguridad. Como se explica de forma más amplia en la parte 5, una causa habitual de este comportamiento inesperado son los permisos públicos sobre los recursos. Por ejemplo, podrías ver que simpleuser es capaz de crear nuevos paneles de control en el *User Portal*. Si el recurso %DeepSee\PortalEdit todavía tiene asignados permisos públicos de USE, cualquier usuario podrá crear tablas dinámicas y paneles de control. Para resolver este problema, elimina los permisos públicos de USE en el recurso %DeepSee\PortalEdit.

En la parte 2 crearemos un segundo tipo de usuario que pueda editar y crear tablas dinámicas y paneles de

control en DeepSee.

#Principiante #Control de acceso #Seguridad #Control de acceso #InterSystems IRIS BI (DeepSee)

URL de fuente:https://es.community.intersystems.com/post/deepsee-c%C3%B3mo-configurar-la-seguridad-parte-1-de-5