Identity Console

Guía de administración

Septiembre de 2022

Información legal

Para obtener información acerca de la información legal, las marcas comerciales, las renuncias de responsabilidad, las garantías, la exportación y otras restricciones de uso, los derechos del gobierno estadounidense, la directiva de patentes y el cumplimiento de la norma FIPS, consulte el sitio https://www.netiq.com/es-es/company/legal.

Tabla de contenido

Acerca de este libro y la biblioteca

La *Guía de administración* presenta información conceptual sobre el producto NetIQ Identity Console (Identity Console). En este documento se define la terminología y se presentan escenarios de implementación.

Para obtener la versión más reciente de la *Guía de administración de NetIQ Identity Console*, consulte la versión en inglés de la documentación en el sitio de documentación en línea de NetIQ Identity Console.

A quién va dirigida

Esta guía está dirigida a administradores de red.

Otra información de la biblioteca

La biblioteca ofrece los siguientes recursos informativos:

Guía de instalación

Describe el procedimiento para instalar Identity Console. Este libro está dirigido a administradores de red.

Acerca de NetIQ Corporation

Somos una empresa mundial de software empresarial, centrada en resolver los tres principales desafíos de su entorno, a saber, cambios, complejidad y riesgo, y en cómo podemos ayudarle a controlarlos.

Nuestro punto de vista

La adaptación a los cambios y la gestión de la complejidad y los riesgos no son conceptos nuevos

De hecho, de todos los desafíos a los que se enfrenta, quizá sean estas las variables más destacadas que le deniegan el control necesario para poder medir, supervisar y gestionar de forma segura sus entornos físico, virtual y de cloud computing.

Activación de servicios esenciales para el negocio de forma más rápida y eficiente

Creemos que la única forma de hacer posible una prestación de servicios más puntual y económica es dotar a las organizaciones de TI del mayor control posible. La presión continua de los cambios y la complejidad seguirá aumentando a medida que las organizaciones sigan creciendo y las tecnologías necesarias para gestionarlas se hagan intrínsecamente más complejas.

Nuestra filosofía

Vender soluciones inteligentes, no solo software

Para poder ofrecer un control fiable, debemos entender primero los escenarios reales en los que —día a día— operan las organizaciones de TI como la suya. Esa es la única forma de desarrollar soluciones de TI prácticas e inteligentes que proporcionen resultados mensurables con una eficacia demostrada. Y eso es mucho más satisfactorio que vender simplemente software.

Fomentar su éxito es nuestra pasión

Ayudarle a alcanzar el éxito es el objetivo primordial de nuestro trabajo. Desde la concepción a la implantación, sabemos que usted necesita soluciones de TI que funcionen bien y se integren a la perfección con su inversión existente; necesita asistencia continua y formación posterior a la implantación; y, para variar, también necesita trabajar con alguien que le facilite las cosas. En definitiva, su éxito será también el nuestro.

Nuestras soluciones

- Control de identidad y acceso
- Gestión de acceso
- Gestión de la seguridad

- Gestión de sistemas y aplicaciones
- Gestión del trabajo
- Gestión de servicios

Cómo ponerse en contacto con la asistencia para ventas

Para cualquier pregunta sobre nuestros productos, precios y capacidades, póngase en contacto con su representante local. Si no puede contactar con su representante local, comuníquese con nuestro equipo de Asistencia para ventas.

Oficinas mundiales:	www.netiq.com/about_netiq/officelocations.asp
Estados Unidos y Canadá:	1-888-323-6768
Correo electrónico:	info@netiq.com
Sitio Web:	www.netiq.com

Cómo ponerse en contacto con el personal de asistencia técnica

Para obtener información sobre problemas con productos específicos, póngase en contacto con nuestro equipo de asistencia técnica.

Oficinas mundiales:	www.netiq.com/support/contactinfo.asp
Norteamérica y Sudamérica:	1-713-418-5555
Europa, Oriente Medio y África:	+353 (0) 91-782 677
Correo electrónico:	support@netiq.com
Sitio Web:	www.netiq.com/support

Cómo ponerse en contacto con la asistencia para documentación

Nuestro objetivo es proporcionar documentación que satisfaga sus necesidades. Si tiene sugerencias de mejoras, haga clic en **Add Comment** (Agregar comentario) en la parte de abajo de cualquier página de las versiones HTML de la documentación publicada en www.netiq.com/documentation. Si lo desea, también puede enviar un correo electrónico a Documentation-Feedback@netiq.com. Agradecemos sus comentarios y estamos deseando oír sus sugerencias.

Cómo ponerse en contacto con la comunidad de usuarios en línea

Qmunity, la comunidad de NetIQ en línea, es una red de colaboración que le pone en contacto con sus colegas y con otros expertos de NetIQ. Qmunity le ayuda a dominar los conocimientos que necesita para hacer realidad todo el potencial de su inversión en TI de la que depende, al proporcionarle información inmediata, enlaces útiles a recursos prácticos y acceso a los expertos de NetIQ. Para obtener más información, visite la página http://community.netiq.com.

1 ¿Qué es Identity Console?

Identity Console es una consola de administración basada en la Web de vanguardia que proporciona acceso virtual, seguro y personalizado a las utilidades de administración de red desde cualquier lugar a través de Internet y el navegador Web. Identity Console permite descentralizar de forma mucho más sencilla las tareas administrativas.

Funciones de Identity Console

Identity Console proporciona las siguientes funciones:

- Administración de objetos de eDirectory, usuarios, esquemas, particiones, réplicas, derechos, etc.
- Gestión de los controladores y los conjuntos de controladores de Identity Manager
- Gestionar y ver las estadísticas de rendimiento del controlador
- Inspección de objetos, visualización del flujo de datos del controlador, gestión de derechos, órdenes de trabajo, etc.
- Gestión del estado de sincronización de contraseñas y los ajustes de los controladores
- Gestión de las directivas de contraseñas y los métodos de entrada
- Gestión de certificados
- Administración de diversos recursos de red
- Medida de seguridad mejorada para proteger los datos
- Mayor capacidad de ampliación para gestionar objetos de eDirectory de mayor tamaño
- Entrada protegida al portal de Identity Console a través de One SSO Provider (OSP)
- Desarrollado con la tecnología de IU más reciente del sector
- Fácil instalación y configuración a través de contenedores de Docker

2 ¿Cómo se accede a Identity Console?

Puede acceder a Identity Console y a todas sus funciones desde cualquier navegador Web compatible. Aunque es posible que pueda acceder a Identity Console a través de un navegador Web que no se haya indicado, no se ofrece asistencia ni se garantiza una total funcionalidad si se utiliza un navegador distinto a los admitidos oficialmente.

Importante: Para obtener información sobre navegadores Web compatibles, consulte la *Identity Console Installation Guide* (Guía de instalación de Identity Console).

Acceder a Identity Console

Para acceder a la instancia de Identity Console basada en servidor, realice estos pasos:

1. Escriba el siguiente texto en el campo de dirección (URL) de un navegador Web compatible.

   Entrada segura: `https://<dirección-ip-servidor/nombrehost>:<puerto>/identityconsole/`

   En los ejemplos, la dirección IP de *<dirección-ip-servidor>* debe ser IPv4. El puerto por defecto que se utilizará es el 9000.
2. Entre a la sesión mediante su nombre completo de usuario y contraseña.
3. Especifique la dirección IP o el DNS del árbol de eDirectory con o sin puerto seguro LDAP.

Nota

- Al actualizar cualquier pestaña de Identity Console, se saldrá de la sesión del usuario por motivos de seguridad.
- Al abrir pestañas duplicadas de Identity Console en el navegador, se saldrá de la sesión del usuario por motivos de seguridad.
- El nombre completo debe especificarse con el formato `cn=admin,ou=sa,o=system`.
- Si eDirectory se ha configurado como puerto no por defecto, debe especificar el número de puerto.

---

3 Navegación por la interfaz de Identity Console

En esta sección, se describe cómo desplazarse por la interfaz Web de Identity Console.

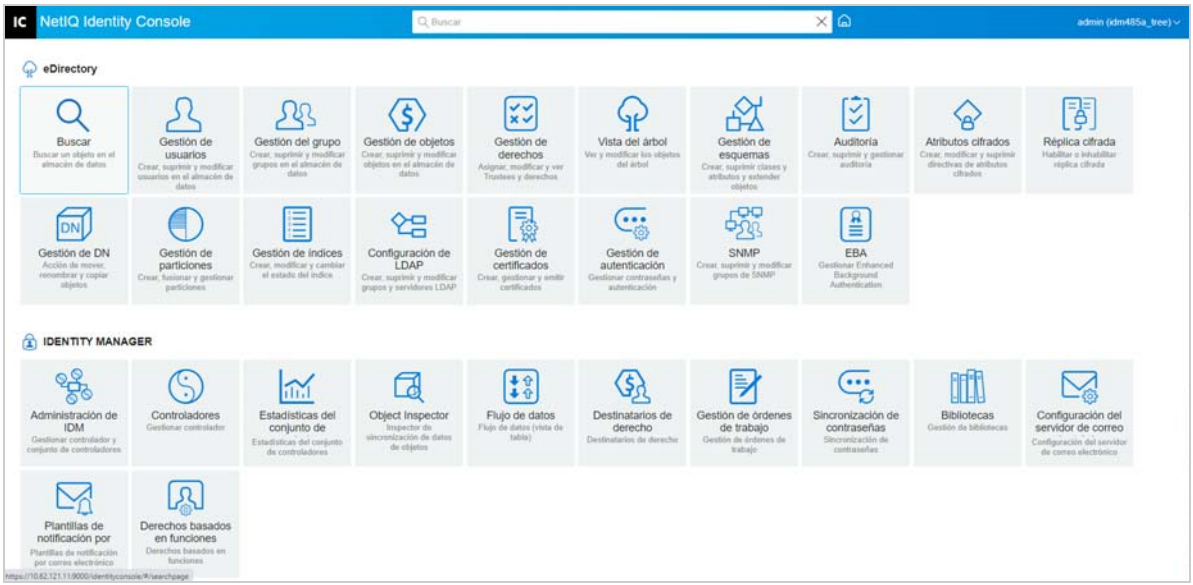
Buscar (versión preliminar de tecnología)

La función **Buscar (versión preliminar de tecnología)** ofrece un diseño introductorio de la funcionalidad de búsqueda. En esta vista preliminar, puede especificar palabras clave y el campo de búsqueda determina la fuente de información que se utilizará para buscar y mostrar los resultados coincidentes. Mediante esta opción, puede buscar un recurso y acceder a él con facilidad a través de cualquier página de la aplicación Identity Console.

Interface de Identity Console

La interfaz de Identity Console está compuesta por los módulos eDirectory e Identity Manager.

Figura 3-1 *Interface de Identity Console*



Importante: Varias animaciones GIF utilizadas en esta guía funcionan solo con la documentación en línea. Si decide cambiar al formato PDF, solo estarán visibles las capturas de pantalla.

Tabla 3-1 *Explicación de diversos módulos del portal Web de Identity Console*

Módulo	Descripción
Buscar	Busque un objeto en el almacén de datos.. Para obtener más información, consulte el Capítulo 4, “Realización de búsquedas”, en la página 25.
Gestión de usuarios	Cree, suprima y modifique usuarios en el almacén de datos.. Para obtener más información, consulte el Capítulo 5, “Gestión de usuarios”, en la página 29.
Gestión de grupos	Cree, suprima y modifique grupos en el almacén de datos. Para obtener más información, consulte Capítulo 6, “Gestión de grupos”, en la página 37.
Gestión de objetos	Cree, suprima y modifique objetos en el almacén de datos. Para obtener más información, consulte el Capítulo 7, “Gestión de objetos”, en la página 43.
Gestión de derechos	Asigne, modifique y visualice Trustees y derechos.. Para obtener más información, consulte el Capítulo 8, “Gestión de derechos”, en la página 51.
Vista Árbol	Visualice y modifique los objetos del árbol.. Para obtener más información, consulte el Capítulo 9, “Vista Árbol”, en la página 55.
Gestión de esquemas	Crea y suprima clases, clases auxiliares y atributos, y amplíe objetos.. Para obtener más información, consulte el Capítulo 10, “Gestión de esquemas”, en la página 59.
Auditoría	Habilite, inhabilite y gestione la auditoría de CEF.. Para obtener más información, consulte el Capítulo 11, “Gestión de eventos de auditoría”, en la página 67.
Atributos cifrados	Cree, modifique, suprima y visualice la directiva de atributos cifrados. Para obtener más información, consulte Capítulo 12, “Gestión de atributos cifrados”, en la página 73.
Réplica cifrada	Habilite, inhabilite y visualice la réplica cifrada.. Para obtener más información, consulte el Capítulo 13, “Gestión de réplica cifrada”, en la página 77.
Gestión de DN	Mueva, cambie de nombre y copie objetos.. Para obtener más información, consulte el Capítulo 7, “Gestión de objetos”, en la página 43.
Gestión de particiones	Cree, fusione y mueva particiones y réplicas. Para obtener más información, consulte Capítulo 14, “Gestión de particiones y réplicas”, en la página 79.
Gestión de índices	Cree, modifique y cambie el estado de los índices. Para obtener más información, consulte Capítulo 15, “Gestión de índices”, en la página 85.

Módulo	Descripción
Configuración de LDAP	Cree, suprima y modifique objetos LDAP. Para obtener más información, consulte Capítulo 16, “Configuración de objetos LDAP”, en la página 89.
Gestión de certificados	Cree y gestione certificados de servidor y CA. Para obtener más información, consulte Capítulo 17, “Gestión de certificados”, en la página 93.
Gestión de autenticación	Cree y gestione métodos y secuencias login.post-login. También puede gestionar las directivas de contraseñas y los conjuntos de preguntas desafío. Para obtener más información, consulte Capítulo 18, “Gestión del marco de autenticación”, en la página 111.
SNMP	Cree, suprima y modifique grupos de SNMP. Para obtener más información, consulte Capítulo 19, “Gestión de objetos Grupo de SNMP”, en la página 127.
EBA	Gestione Enhanced Background Authentication. Para obtener más información, consulte Capítulo 20, “Gestión de Enhanced Background Authentication”, en la página 131.
Administración de IDM	Gestione los controladores y los conjuntos de controladores de Identity Manager. Para obtener más información, consulte la Capítulo 21, “Gestión de controladores y conjuntos de controladores”, en la página 135. También puede gestionar las propiedades del conjunto de controladores mediante este módulo. Para obtener más información, consulte Capítulo 22, “Gestión de las propiedades del conjunto de controladores”, en la página 141.
Propiedades del controlador	Gestione las propiedades de diversos controladores. Para obtener más información, consulte Capítulo 23, “Gestión de las propiedades de los controladores”, en la página 155.
Estadísticas del conjunto de controladores	Gestione y consulte las estadísticas del conjunto de controladores. Para obtener más información, consulte Capítulo 24, “Gestión de las estadísticas del conjunto de controladores”, en la página 185.
Objeto Inspector	Gestione la asociación de objetos y la sincronización de datos. Para obtener más información, consulte Capítulo 25, “Inspección de objetos de Identity Manager”, en la página 187.
Flujo de datos	Gestione y consulte el flujo de datos de los controladores. Para obtener más información, consulte Capítulo 26, “Gestión del flujo de datos”, en la página 189.

Módulo	Descripción
Destinatarios de derecho	Gestione los destinatarios de derechos. Para obtener más información, consulte Capítulo 27, “Gestión de destinatarios de derechos”, en la página 191.
Gestión de órdenes de trabajo	Gestione las órdenes de trabajo. Para obtener más información, consulte Capítulo 28, “Gestión de órdenes de trabajo”, en la página 193.
Sincronización de contraseñas	Gestione la sincronización y el estado de las contraseñas. Para obtener más información, consulte Capítulo 29, “Gestión del estado y la sincronización de contraseñas”, en la página 197.
Gestión de bibliotecas	Gestione las bibliotecas. Para obtener más información, consulte Capítulo 30, “Gestión de bibliotecas”, en la página 201.
Configuración del servidor de correo electrónico	Gestione las opciones del servidor de correo electrónico. Para obtener más información, consulte Capítulo 31, “Gestión de las opciones del servidor de correo electrónico”, en la página 203.
Plantillas de notificación por correo electrónico	Gestione las plantillas de correo electrónico. Para obtener más información, consulte Capítulo 32, “Gestión de plantillas de correo electrónico”, en la página 205.

Gestión de eDirectory mediante Identity Console

En esta sección, se describen las distintas tareas que puede llevar a cabo para gestionar los servidores de eDirectory mediante el portal de Identity Console.

4 Realización de búsquedas

El mosaico Búsqueda le permite especificar la operación de búsqueda que desea realizar en el árbol de directorios y visualizar los resultados. Esta opción permite buscar diversos objetos, usuarios, grupos y otros elementos. Para realizar una operación de búsqueda de varios objetos del almacén de datos, siga los pasos que se indican a continuación:

1. Especifique el nombre del objeto para la búsqueda. Utilice el comodín asterisco para especificar un nombre parcial. Por ejemplo: `ldap*`, `*certificado`, `*servidor*`, etc. Si solo utiliza asteriscos en este campo, Identity Console devolverá todos los resultados de la búsqueda basados en el **Tipo** y el **Contexto** seleccionados.

   Nota: Mediante el Navegador de contexto, puede desplazarse por todo el árbol de eDirectory. Para ello, especifique un asterisco (*) en el campo de búsqueda. También puede filtrar los objetos en el Navegador de contexto mediante la búsqueda con comodines. Por ejemplo, `admin*`. Este comportamiento del Navegador de contexto se admite en varios módulos de Identity Console.

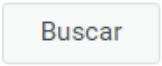
   ---

2. Seleccione el tipo de objeto para la búsqueda en el campo**Tipo**. Identity Console solo muestra los objetos del tipo especificado. El tipo **Usuario** se selecciona por defecto en este campo.

   Haga clic en el icono  para definir ajustes adicionales de búsqueda en el nivel de atributo. Para obtener más información, consulte “Configurar la búsqueda avanzada” en la página 26.

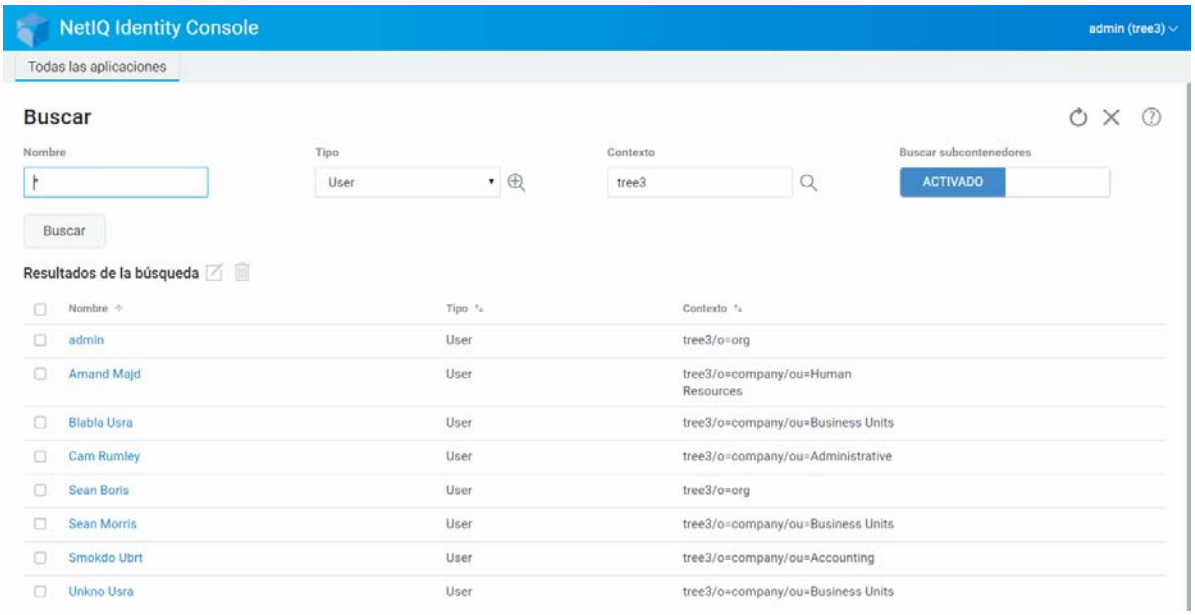
3. Especifique el contenedor inicial de la operación de búsqueda en el campo **Contexto**.

4. Si desea que la búsqueda incluya contenedores subordinados, seleccione **Activado** en la opción Buscar subcontenedores.

5. Haga clic en el botón 

.

Figura 4-1 *Realizar una operación de búsqueda*



Configurar la búsqueda avanzada

La Selección avanzada ofrece un entorno más configurable para buscar los objetos deseados en el directorio.

Tipo de objeto: Especifica la clase base del objeto que está buscando. Por ejemplo, Usuario.

Clases auxiliares: Haga clic en el icono + para especificar la clase auxiliar que desea incluir en la búsqueda.

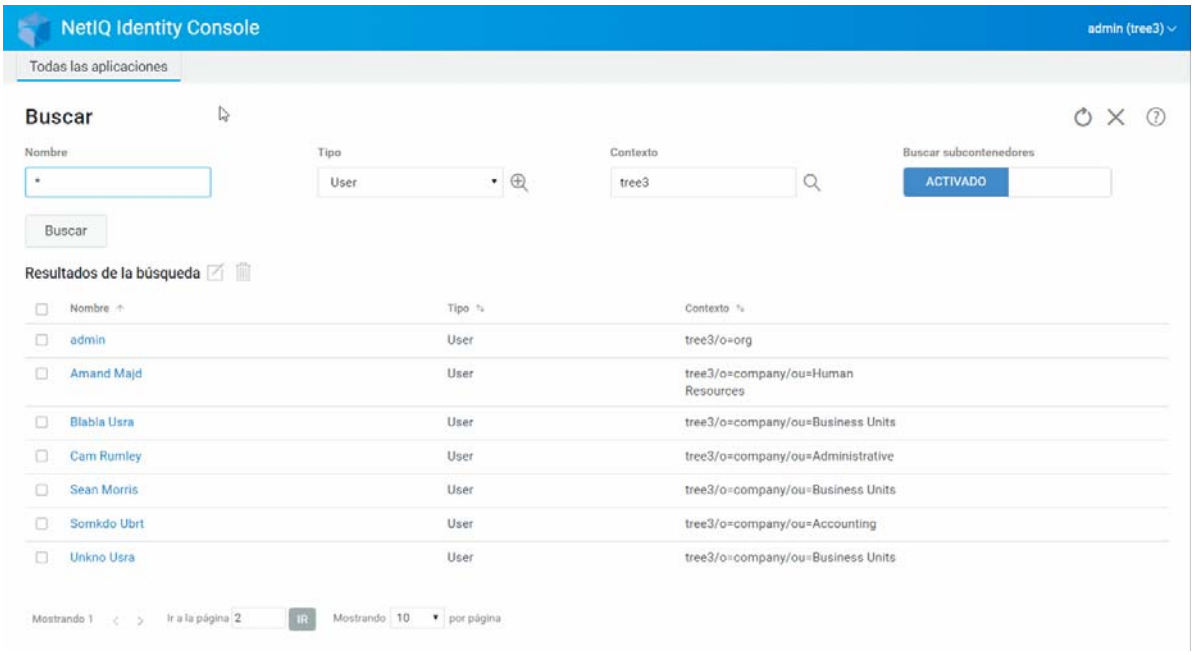
Atributo: Especifica un atributo (propiedad) que desea utilizar como parte del filtro.

Operador: Especifica el operador lógico que desea aplicar al filtro. Las opciones incluyen.

Valor: Especifica el valor de atributo que desea utilizar como filtro. El asterisco (*) se puede utilizar como comodín para indicar una parte de un valor. Por ejemplo, smi*, *th y *mit*.

Además, puede encadenar varios filtros de atributos para formar un grupo de filtros. Para ello, utilice el icono + Rule a fin de añadir un segundo atributo a la lista. Si utiliza varios filtros de atributo, enlácelos con un operador lógico AND u OR.

Figura 4-2 *Configurar la búsqueda avanzada*



5 Gestión de usuarios

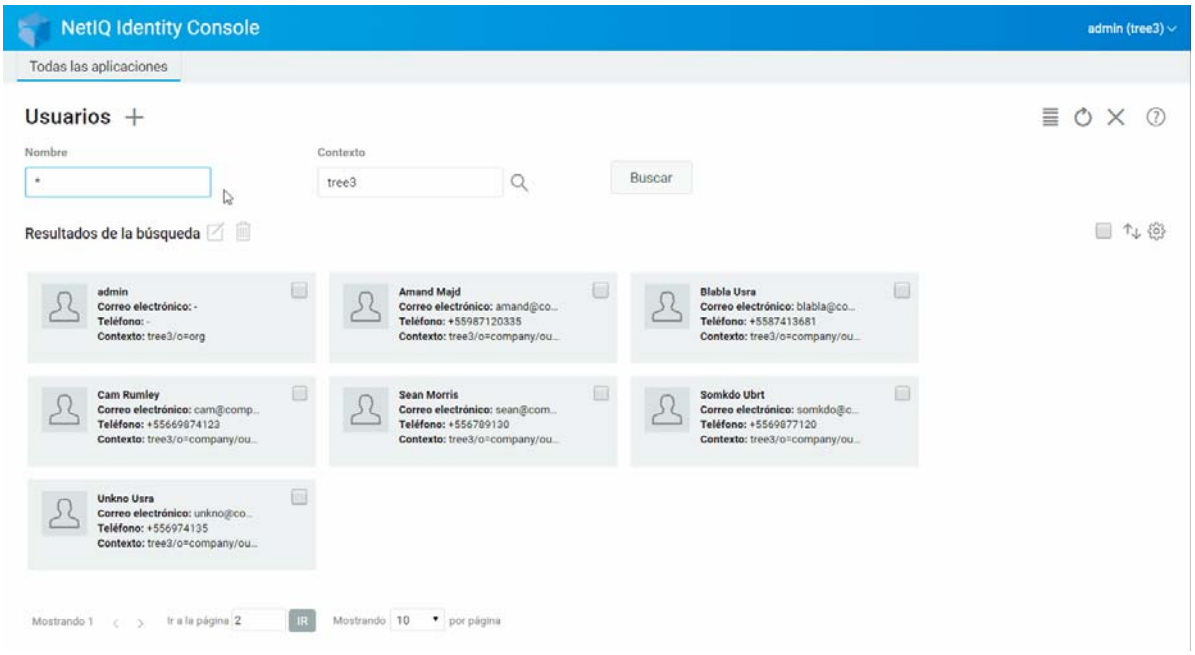
La gestión de usuarios y su acceso a la red es el objetivo central del almacén de datos. Mediante el portal Web de Identity Console, puede llevar a cabo las siguientes tareas relacionadas con los usuarios:

Crear un usuario

Para crear un objeto Usuario nuevo:

1. Haga clic en la opción **Gestión de usuarios** de la página de destino de Identity Console.
2. Haga clic en el icono +.
3. En la página Crear usuario, proporcione, como mínimo, la información relacionada con el usuario necesaria y haga clic en el botón Crear.
   - **Nombre de usuario**
   - **Contexto**
   - **Apellidos**
   - **Contraseña**
4. Aparece un mensaje de confirmación que indica que se ha creado el objeto Usuario.

Figura 5-1 *Crear usuarios*

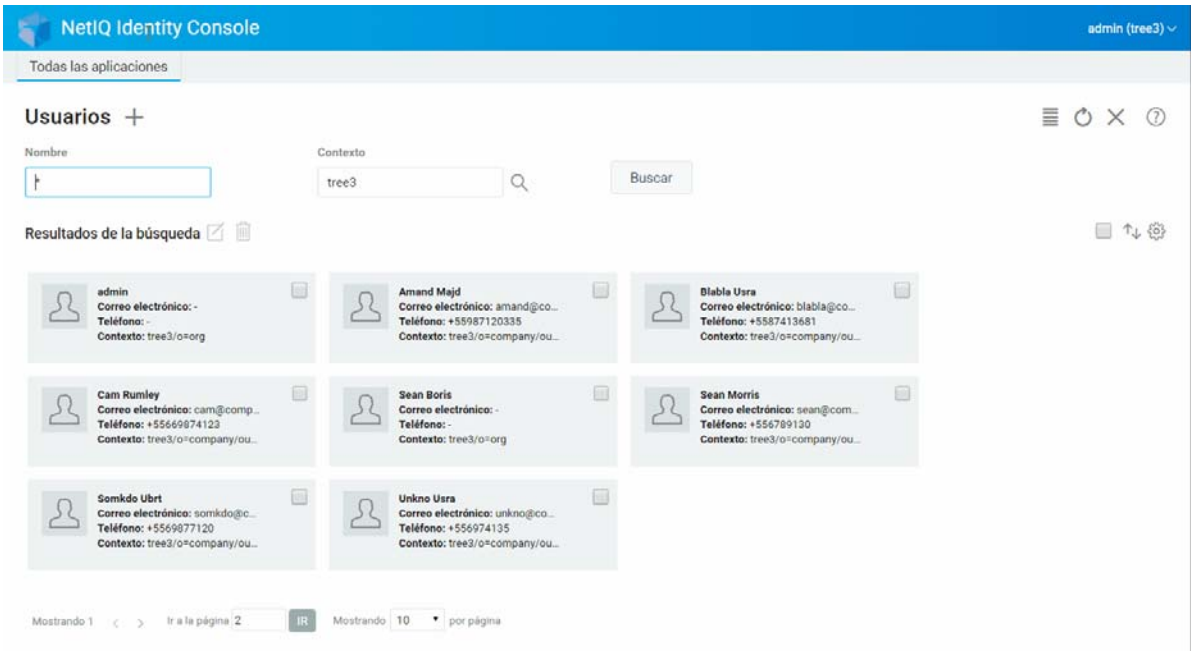


Suprimir un usuario

Para suprimir un objeto Usuario:

1. Haga clic en la opción **Gestión de usuarios** de la página de destino de Identity Console.
2. Especifique el nombre y el contexto del objeto, o utilice la función de búsqueda para buscarlo; a continuación, haga clic en el botón Buscar.
3. Seleccione el objeto Usuario en la lista de usuarios y haga clic en el icono 🗑.
4. Aparece un mensaje de confirmación que indica que se ha suprimido el objeto Usuario.

Figura 5-2 *Suprimir un usuario*

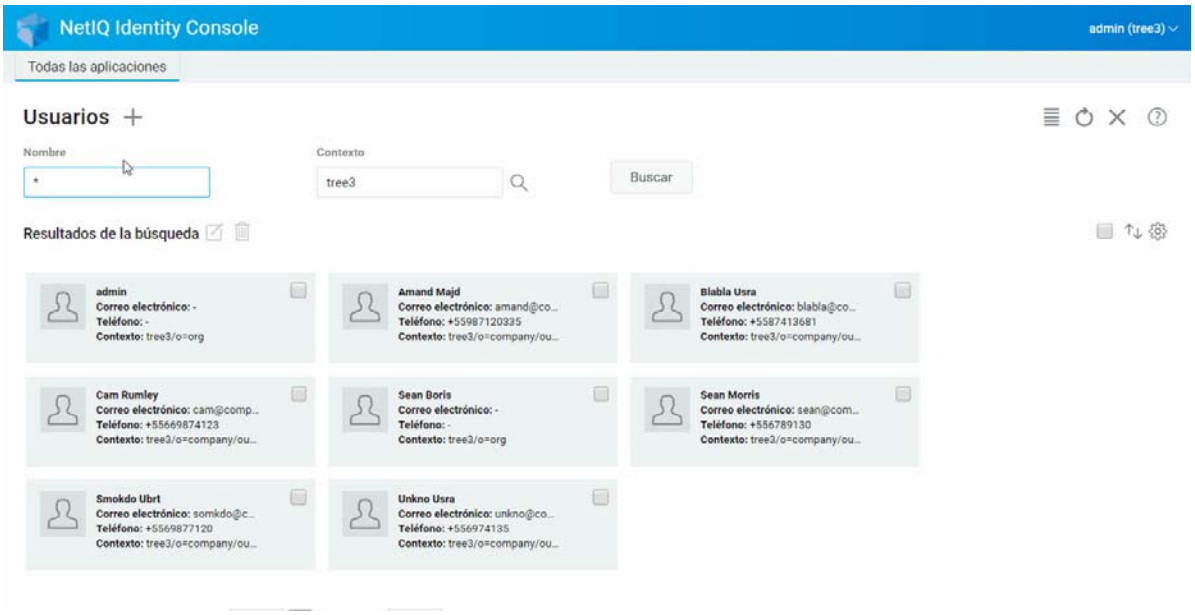


Modificar usuarios

Para modificar un objeto Usuario:

1. Haga clic en la opción **Gestión de usuarios** de la página de destino de Identity Console.
2. Especifique el nombre, el tipo y el contexto del objeto, o utilice la función de búsqueda para buscarlo; a continuación, haga clic en el botón Buscar.
3. Seleccione el objeto Usuario en la lista de usuarios y haga clic en el icono .
4. Realice los cambios y, a continuación, haga clic en el botón Guardar.
5. Aparece un mensaje de confirmación que indica que se ha modificado el objeto Usuario.

Figura 5-3 *Modificar un usuario*

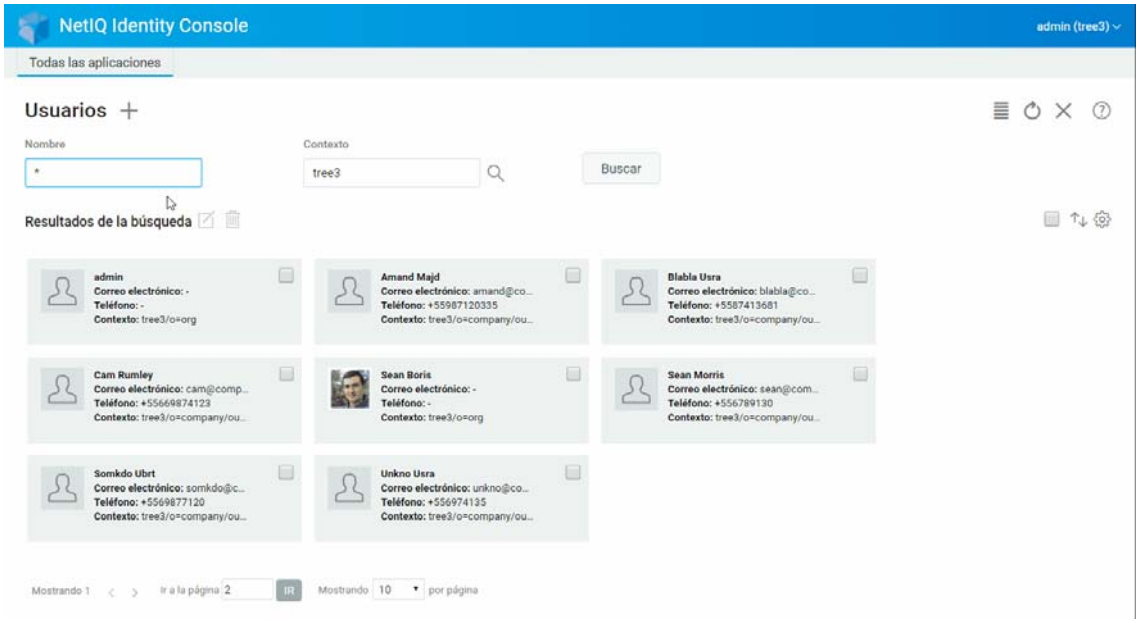


Buscar usuarios

Para buscar un objeto Usuario:

1. Haga clic en la opción **Gestión de usuarios** de la página de destino de Identity Console.
2. Puede buscar un usuario por nombre, o por nombre y contexto. Después de especificar la información necesaria, haga clic en el icono Buscar.

Figura 5-4 *Buscar un usuario*

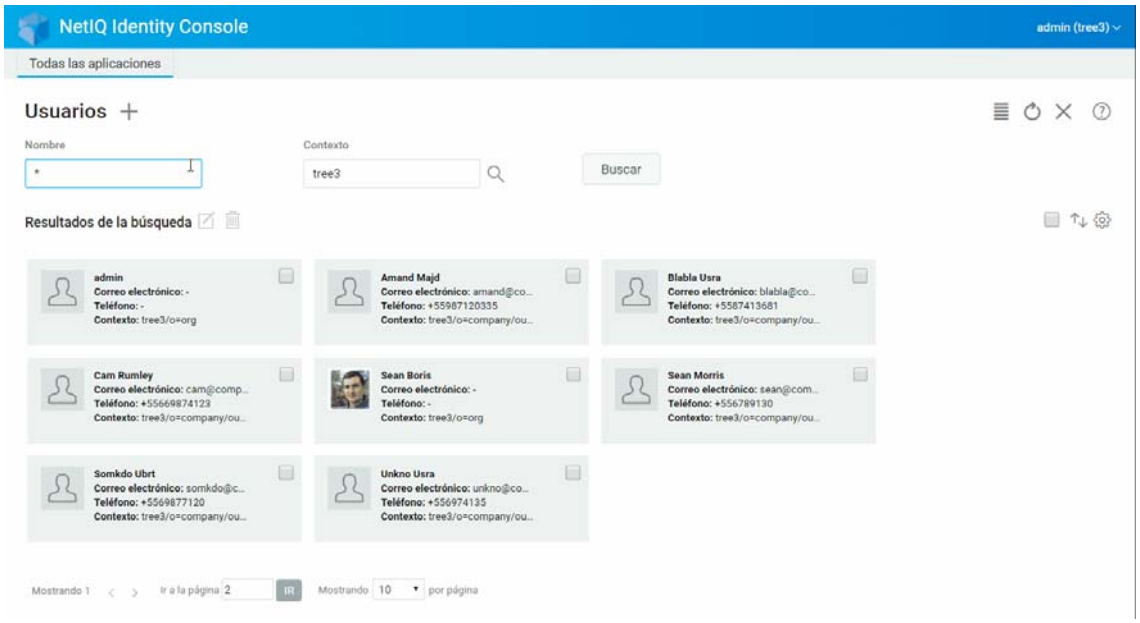


Definir restricciones de contraseña

Las restricciones de contraseña permiten realizar las siguientes acciones:

- Permite a los usuarios cambiar sus respectivas contraseñas.
- Aplique una contraseña para la entrada a la sesión.
- Especifique la seguridad de la contraseña.
- Aplique un cambio periódico de contraseña.
- Especifique la fecha de caducidad de la contraseña.
- Aplique la creación de contraseñas exclusivas.
- Especifique el periodo de entrada de gracia en caso de que la contraseña haya caducado.

Figura 5-5 *Restricciones de contraseña*

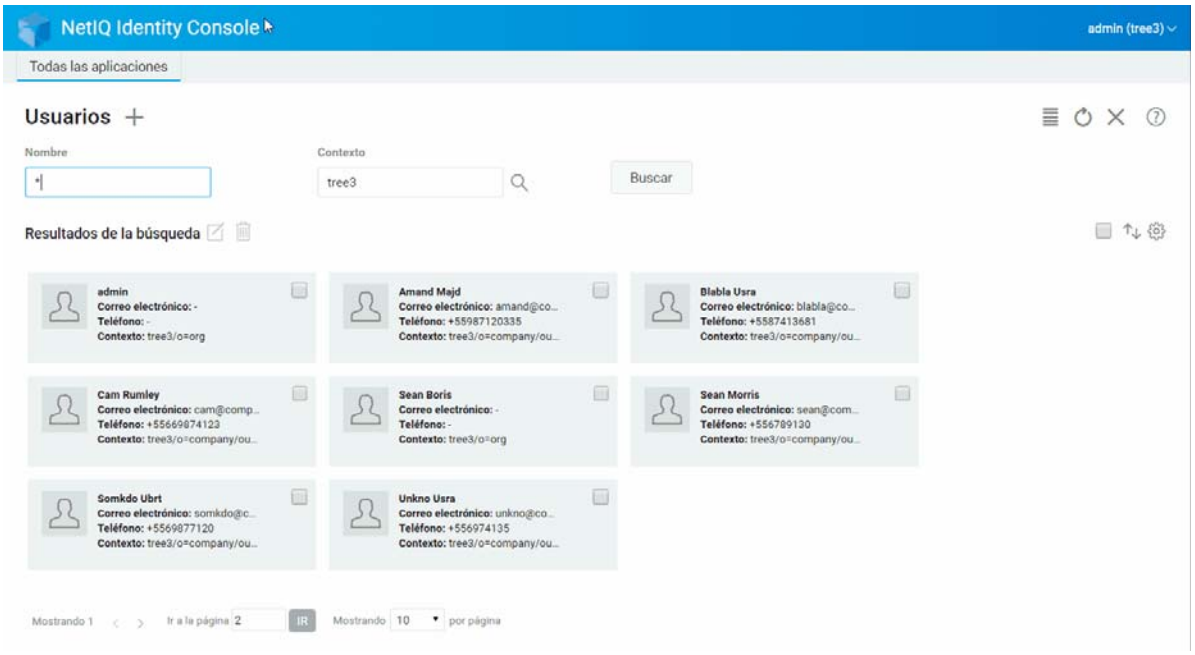


Inhabilitar y habilitar una cuenta de usuario

Para inhabilitar una cuenta de usuario, realice los siguientes pasos:

1. Seleccione el usuario cuya cuenta debe inhabilitarse y haga clic en el icono .
2. Haga clic en la pestaña **Restricciones** de la página **Modificar usuario**.
3. Expanda la pestaña **Restricciones de entrada** y seleccione la casilla de verificación **Cuenta inhabilitada**.
4. Haga clic en el icono Guardar.
5. Ahora la cuenta de usuario está inhabilitada. Para habilitar una cuenta de usuario inhabilitada, anule la selección de la casilla de verificación **Cuenta inhabilitada**.

Figura 5-6 *Inhabilitar y habilitar una cuenta de usuario*

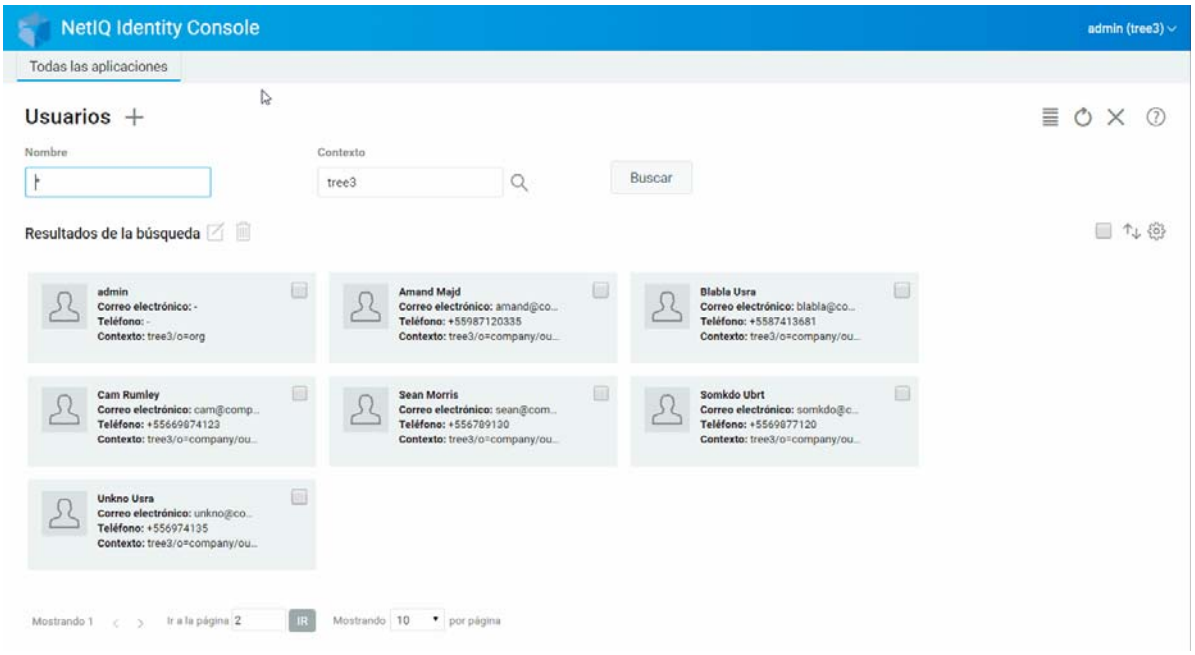


Definir la fecha de caducidad de la cuenta

Para definir la fecha de caducidad de una cuenta para los usuarios, realice los siguientes pasos:

1. Seleccione el usuario para el que se debe definir la fecha de caducidad de la cuenta y haga clic en el icono .
2. Haga clic en la pestaña **Restricciones** de la página **Modificar usuario**.
3. Expanda la pestaña **Restricciones de entrada** y seleccione la casilla de verificación **Cuenta con fecha de caducidad** y especifique la **Fecha de caducidad**.
4. Haga clic en el icono Guardar.

Figura 5-7 *Definir la fecha de caducidad de la cuenta*

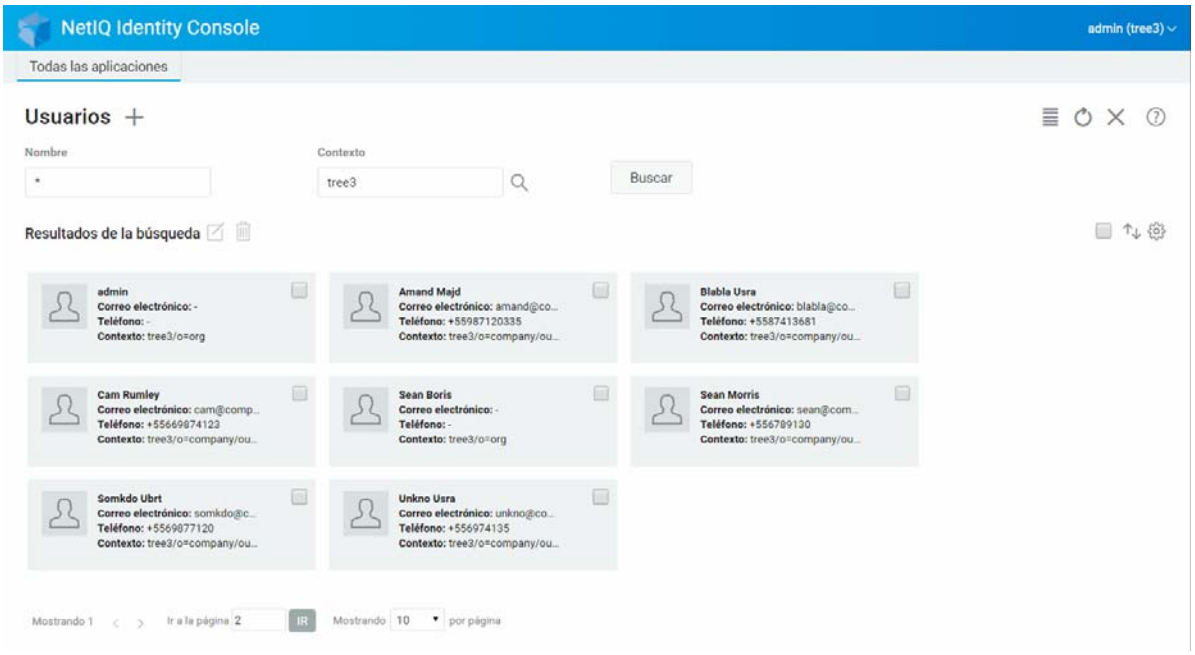


Comprobar y desactivar el bloqueo de intrusos

Puede ver los detalles del bloqueo de intrusos de cualquier cuenta de usuario mediante el portal Web de Identity Console. Para ver los detalles del bloqueo de intrusos:

1. Seleccione el usuario para el que se deben comprobar los detalles del bloqueo de intrusos y haga clic en el icono .
2. Haga clic en la pestaña **Restricciones** de la página **Modificar usuario**.
3. Expanda la pestaña **Bloqueo de intruso** y consulte los detalles del bloqueo de intrusos.
4. A continuación, seleccione la pestaña **Despejar bloqueo** y haga clic en el botón Despejar bloqueo.
5. Haga clic en el botón Guardar.

Figura 5-8 *Comprobar y desactivar el bloqueo de intrusos*



6 Gestión de grupos

Los grupos suelen contener diversos componentes. Cualquier usuario que cree un grupo se convertirá automáticamente en el propietario del mismo. Se pueden realizar las siguientes operaciones mediante la función de gestión de grupos:

Para obtener más información acerca de cómo utilizar y configurar objetos Grupo, consulte la *Guía de administración de NetIQ eDirectory 9.2* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Crear un grupo

Para crear un grupo:

1. Haga clic en **Gestión de grupos** en la página de destino de Identity Console.
2. Haga clic en el icono +.
3. En la página Crear grupo, introduzca la siguiente información:
   - Especifique el nombre del grupo.
   - Especifique el contexto.

   Seleccione **Grupo dinámico** para que el grupo nuevo sea dinámico, de la clase `dynamicGroup`. De lo contrario, el grupo se creará como un grupo estático.

   Seleccione **Grupo anidado** para convertir el nuevo grupo en un grupo anidado, de modo que se cree con la clase auxiliar `nestedGroupAux`.

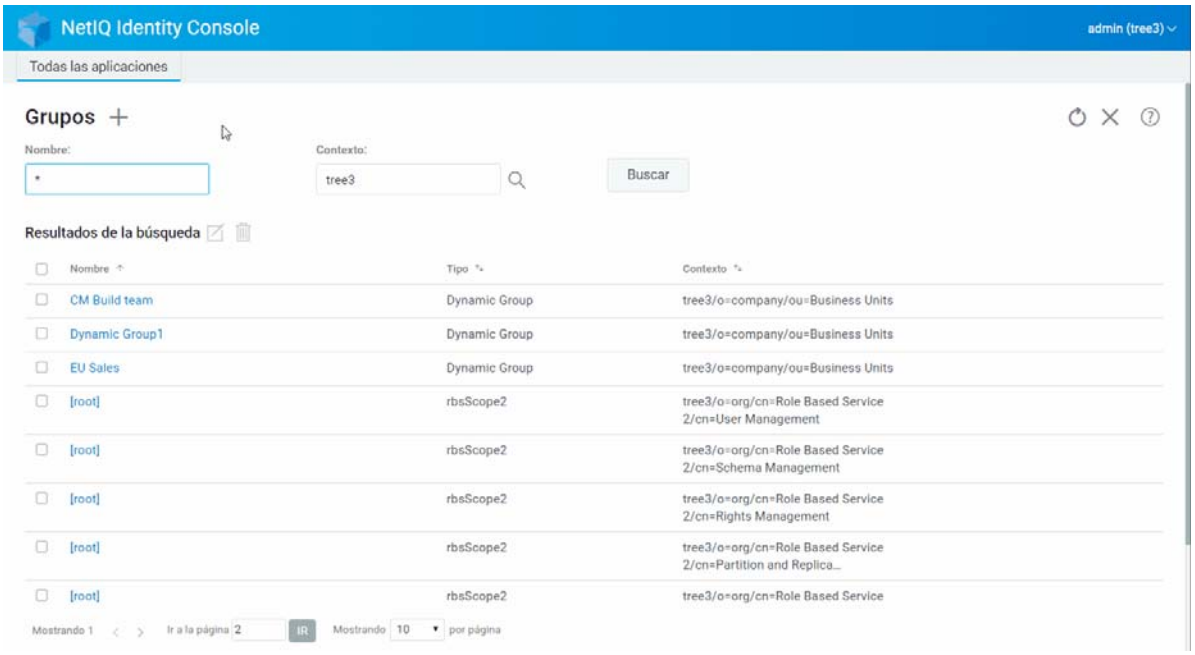
   Nota: Puede convertir un grupo estático en un grupo dinámico o anidado mediante el procedimiento indicado en Modificar objetos. Esto amplía el objeto Grupo seleccionado para que pertenezca a la clase `dynamicGroupAux` o `nestedGroupAux` respectivamente.

   Los grupos pueden ser anidados o dinámicos. No es posible crear un grupo que sea anidado y dinámico a la vez.

   ---

4. Después de especificar la información necesaria, haga clic en el botón Crear.
5. Aparece un mensaje de confirmación que indica que se ha creado el grupo.

Figura 6-1 *Crear un grupo*

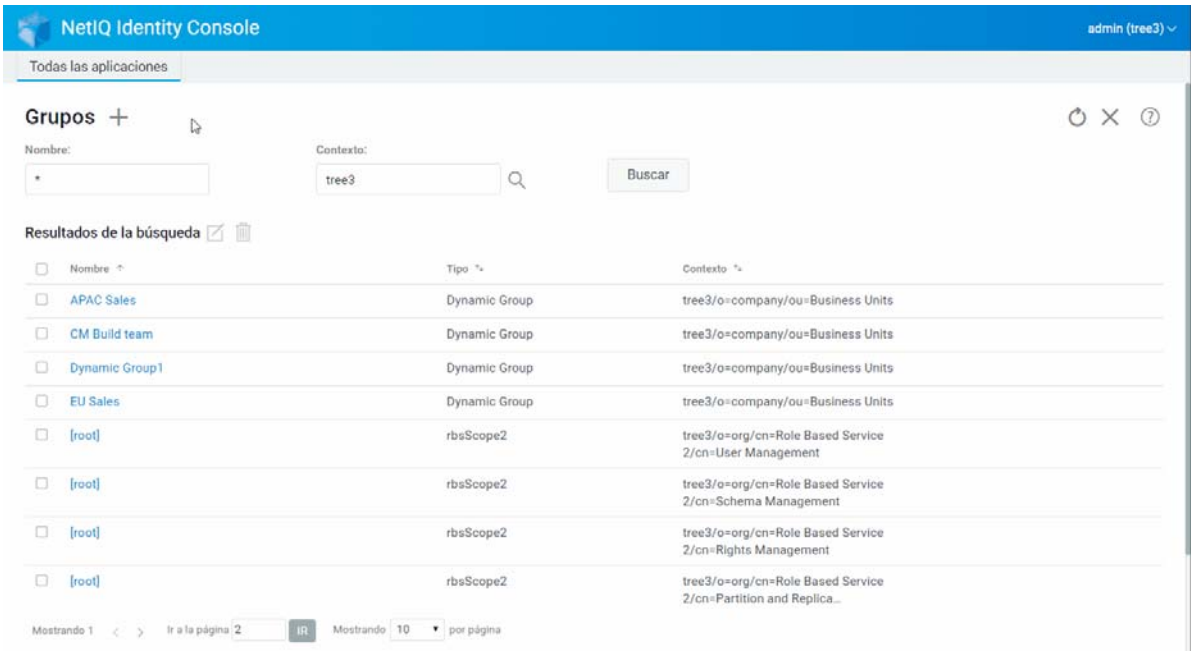


Suprimir grupos

Para suprimir grupos:

1. Haga clic en **Gestión de grupos** en la página de destino de Identity Console.
2. Especifique el nombre y el contexto del grupo, o utilice la función de búsqueda para buscarlo y, a continuación, haga clic en el botón Buscar.
3. Seleccione el grupo que debe suprimirse y haga clic en el icono 🗑.
4. Aparece un mensaje de confirmación que indica que se ha suprimido el grupo.

Figura 6-2 *Suprimir grupos*

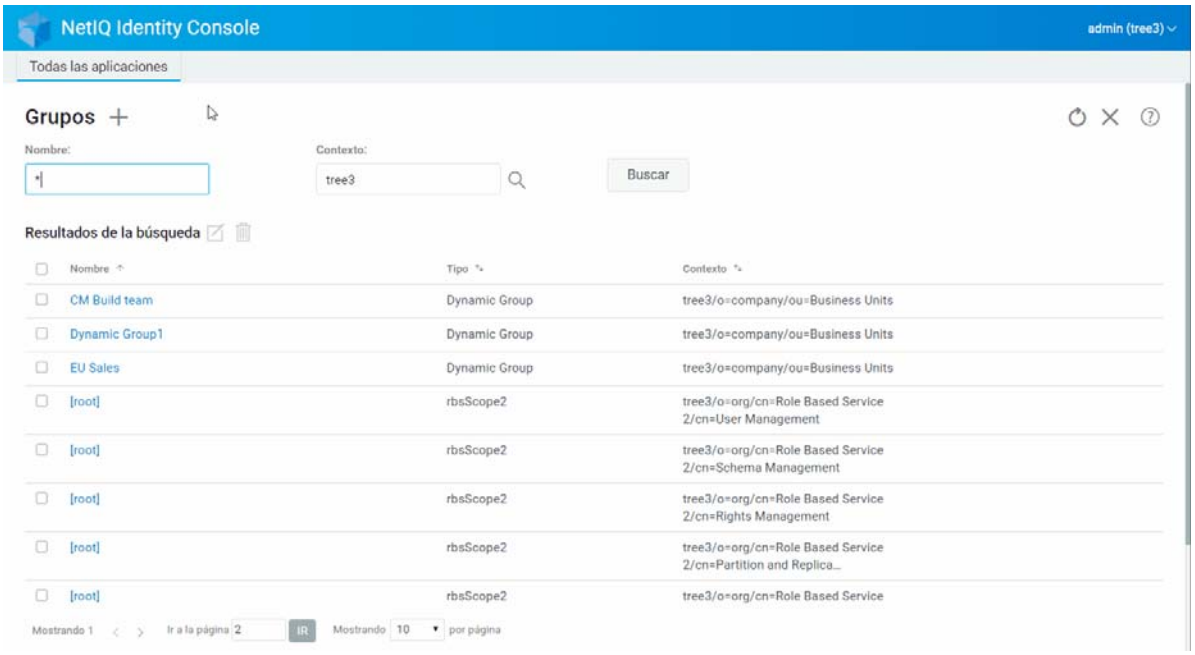


Modificar grupos

Para modificar grupos:

1. Haga clic en **Gestión de grupos** en la página de destino de Identity Console.
2. Especifique el nombre y el contexto del grupo y, a continuación, haga clic en el botón Buscar.
3. Seleccione el grupo que debe modificarse y haga clic en el icono .
4. Realice los cambios y, a continuación, haga clic en el botón Guardar.
5. Aparece un mensaje de confirmación que indica que se ha modificado el grupo.

Figura 6-3 *Modificar grupos*

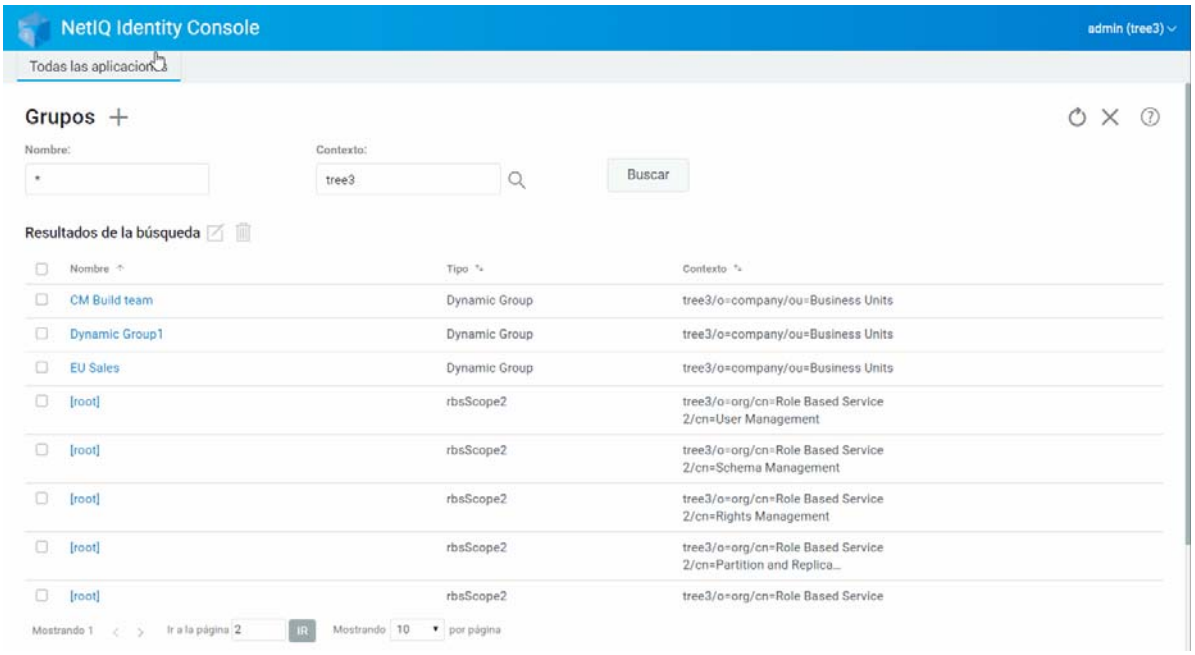


Añadir o modificar componentes de grupo

Para añadir o modificar componentes de grupo:

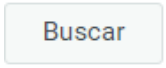
1. Haga clic en **Gestión de grupos** en la página de destino de Identity Console.
2. Especifique el nombre y el contexto del grupo y, a continuación, haga clic en el botón Buscar.
3. Seleccione el grupo y haga clic en el icono .
4. Haga clic en la pestaña **Componentes** de la página **Modificar grupo**.
5. Utilice el icono para añadir un nuevo componente al grupo. Si decide eliminar componentes del grupo, haga clic en el icono .
6. Después de realizar los cambios, haga clic en el botón Guardar.
7. Aparece un mensaje de confirmación que indica que se ha modificado el grupo.

Figura 6-4 *Añadir o modificar componentes de grupo*



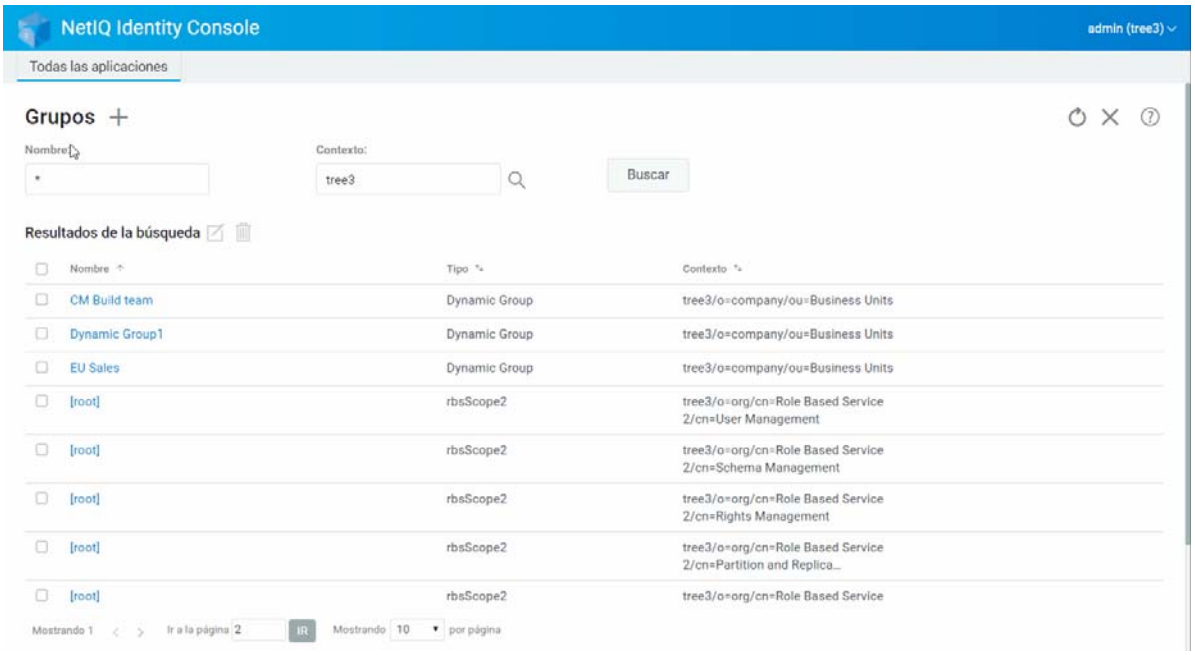
Buscar grupos

Para buscar grupos:

1. Haga clic en **Gestión de grupos** en la página de destino de Identity Console.
2. Puede buscar un grupo por nombre, o por nombre y contexto.
3. Después de especificar la información necesaria, haga clic en el icono 

.

Figura 6-5 *Buscar grupos*



7 Gestión de objetos

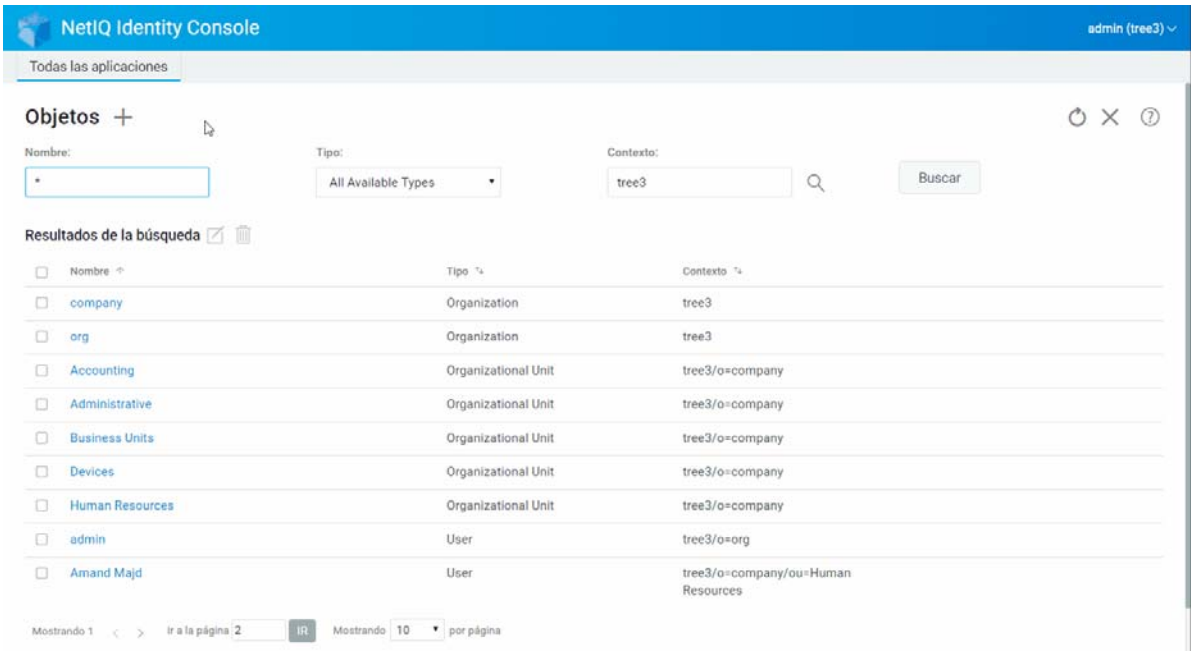
Identity Console permite gestionar diversos objetos del almacén de datos. Este módulo permite crear, modificar, suprimir y buscar objetos.

Crear un objeto

Para crear un nuevo objeto:

1. Haga clic en la opción **Gestión de objetos** de la página de destino de Identity Console.
2. Haga clic en el icono +.
3. En la página Crear objeto, introduzca la información siguiente:
   - Especifique un nombre de objeto.
   - Especifique el tipo.
   - Especifique el contexto.
4. Después de introducir toda la información necesaria, haga clic en **Siguiente** > **Crear**.
5. Aparece un mensaje de confirmación que indica que se ha creado el objeto.

Figura 7-1 *Crear un objeto*

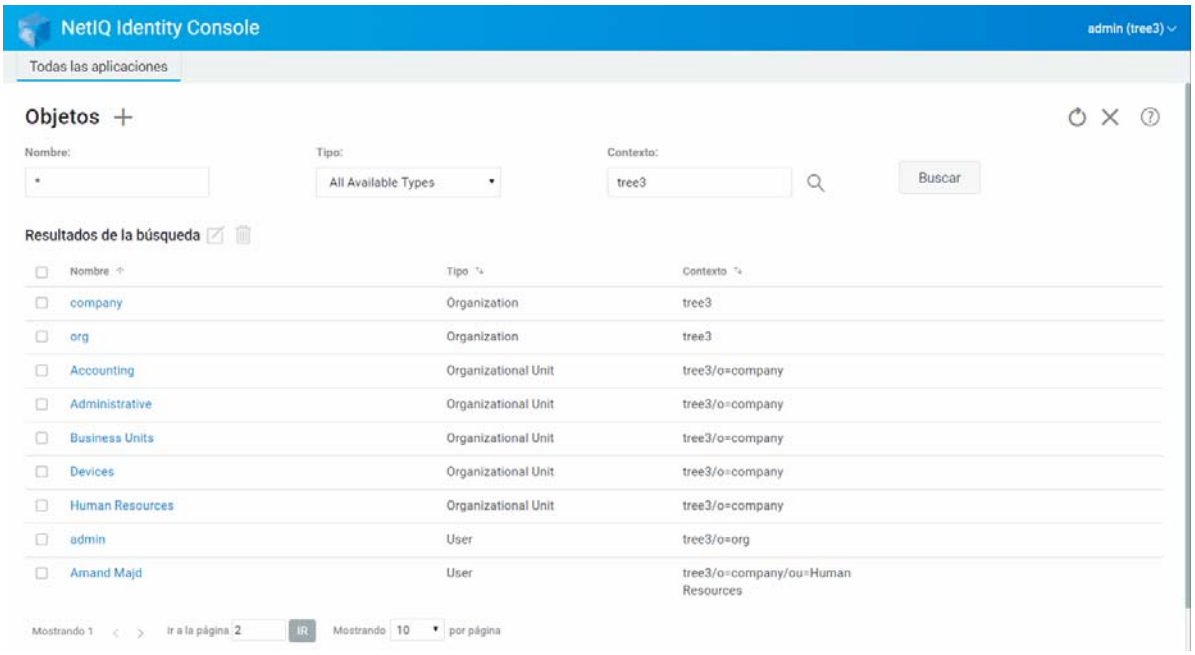


Suprimir objetos

Para suprimir objetos:

1. Haga clic en la opción **Gestión de objetos** de la página de destino de Identity Console.
2. Especifique el nombre, el tipo y el contexto del objeto o utilice la función de búsqueda para buscarlo y, a continuación, haga clic en el botón Buscar.
3. Seleccione el objeto en la lista de búsqueda y haga clic en el icono 🗑.
4. Aparece un mensaje de confirmación que indica que se ha suprimido el objeto.

Figura 7-2 *Suprimir objetos*

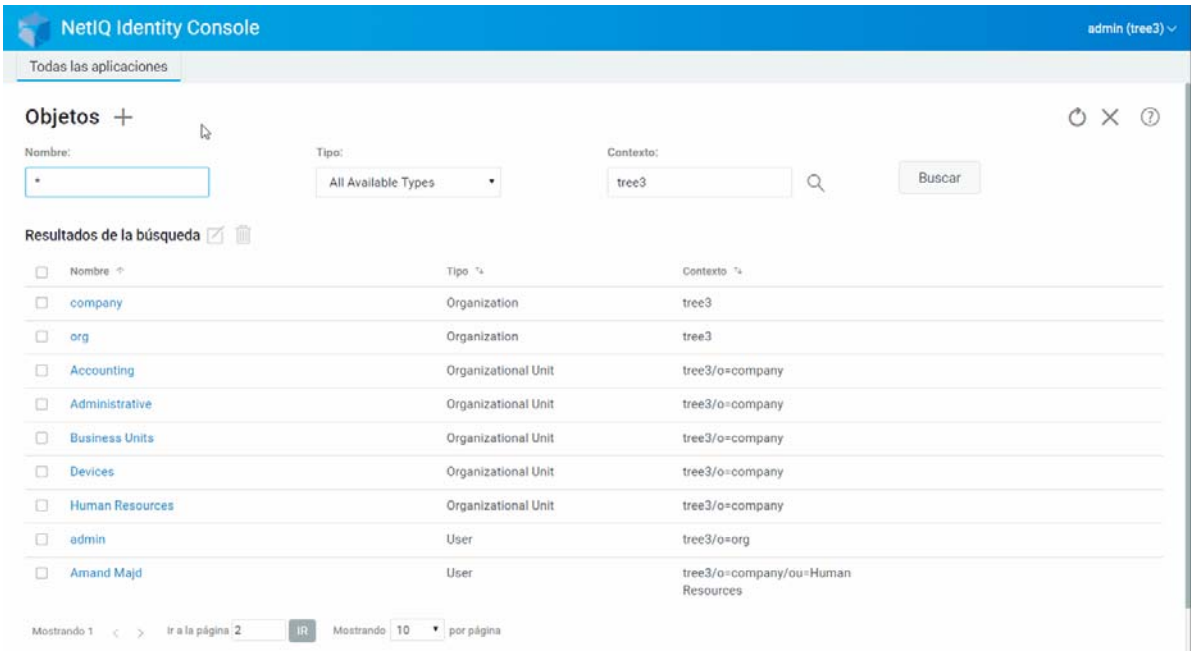


Modificar objetos

Para modificar objetos:

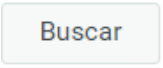
1. Haga clic en **Gestión de objetos** en la página de destino de Identity Console.
2. Especifique el nombre, el tipo y el contexto del objeto y, a continuación, haga clic en el botón Buscar.
3. Seleccione el objeto en la lista de búsqueda y haga clic en el icono .
4. Realice los cambios y, a continuación, haga clic en el botón Guardar.
5. Aparece un mensaje de confirmación que indica que se ha modificado el objeto.

Figura 7-3 *Modificar objetos*



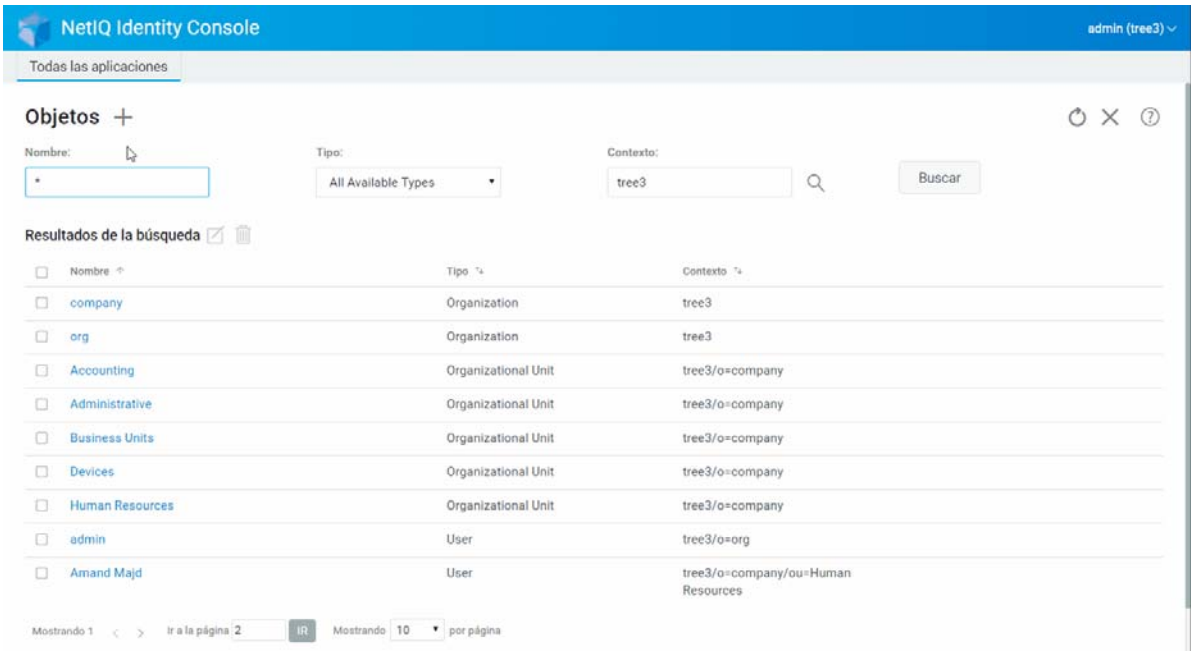
Buscar un objeto

Para buscar un objeto:

1. Haga clic en la opción **Gestión de objetos** de la página de destino de Identity Console.
2. Puede buscar un objeto por nombre, o por nombre, tipo y contexto.
3. Después de especificar la información necesaria, haga clic en el botón 

.

Figura 7-4 *Buscar un objeto*



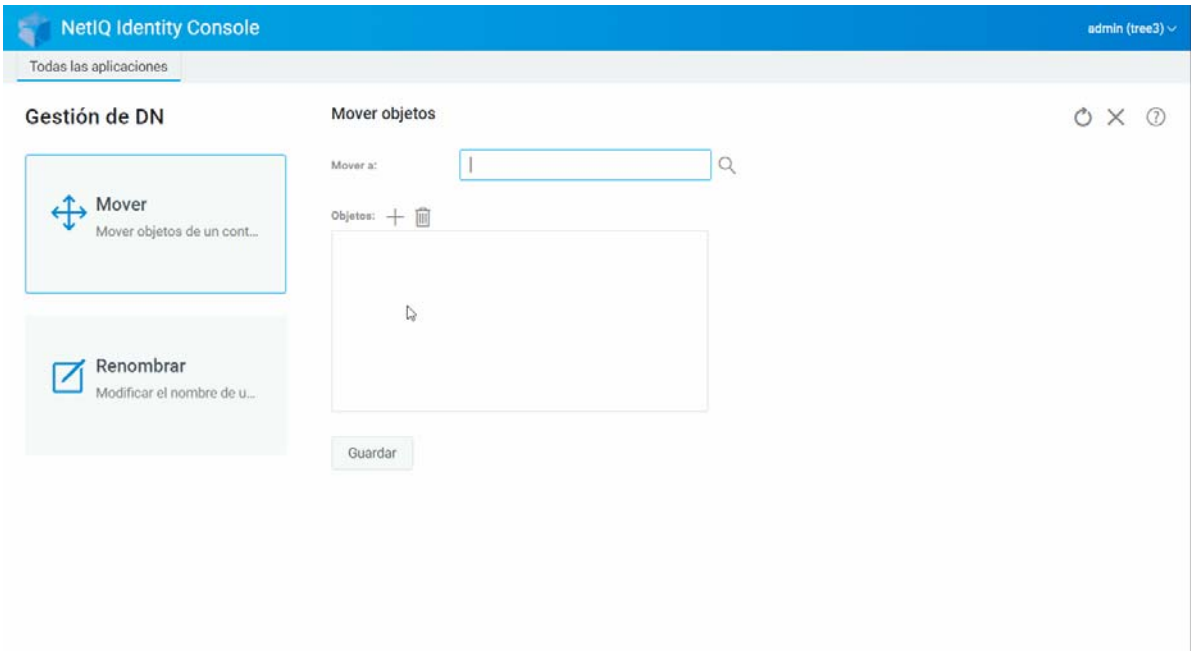
Mover un objeto

Para mover un objeto:

1. Haga clic en la opción **Gestión de DN** de la página de destino de Identity Console.
2. La opción **Mover objeto** se seleccionará por defecto.
3. En el campo **Mover a**, seleccione el contenedor al que desea mover el objeto.
4. Haga clic en el icono + para añadir el objeto que desea mover a un contenedor diferente.

   Si desea eliminar un objeto seleccionado, haga clic en el icono 🗑.
5. Haga clic en el botón Guardar.
6. Aparece un mensaje de confirmación que indica que la operación de mover el objeto se ha realizado correctamente.

Figura 7-5 *Mover un objeto*

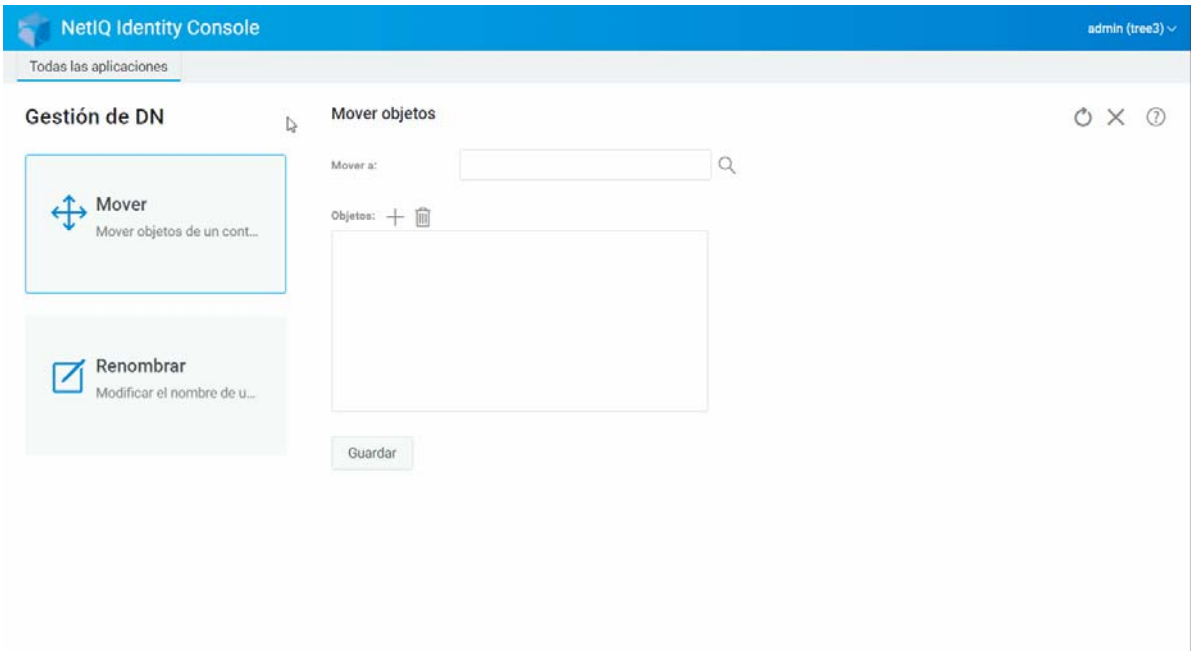


Renombrar un objeto

Para cambiar el nombre de un objeto:

1. Haga clic en la opción **Gestión de DN** de la página de destino de Identity Console.
2. Seleccione la opción **Renombrar objeto**.
3. Utilice la función de búsqueda para buscar el objeto cuyo nombre debe cambiar en el campo **Nombre del objeto**.
4. Especifique solo el nuevo nombre del objeto en el campo **Nuevo objeto**. No especifique el contexto.
5. Seleccione para guardar el nombre antiguo si lo desea.
6. Haga clic en el botón Guardar.
7. Aparece un mensaje de confirmación que indica que la operación de cambio de nombre del objeto se ha realizado correctamente.

Figura 7-6 *Renombrar un objeto*



8 Gestión de derechos

Derechos hace referencia a los derechos de Trustee y a los Trustees de eDirectory. Al crear un árbol, las asignaciones de derechos por defecto proporcionan acceso generalizado y seguridad a la red. Identity Console permite realizar las siguientes tareas relacionadas con los derechos:

- “Modificar el filtro de derechos heredados” en la página 51
- “Modificar los derechos de Trustee” en la página 52
- “Visualización de derechos vigentes” en la página 53

Para obtener más información acerca de los derechos de eDirectory, consulte la *Guía de administración de NetIQ eDirectory 9.2* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

Modificar el filtro de derechos heredados

eDirectory proporciona un mecanismo de filtro de derechos heredados (IRF, Inherited Rights Filter) para bloquear la herencia de derechos en elementos subordinados individuales.

Para obtener más información acerca de los filtros de derechos heredados, consulte la *Guía de administración de NetIQ eDirectory 9.2* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html).

1. Haga clic en la opción **Gestión de derechos** de la página de destino de Identity Console.
2. Seleccione **Filtro de derechos heredados**.

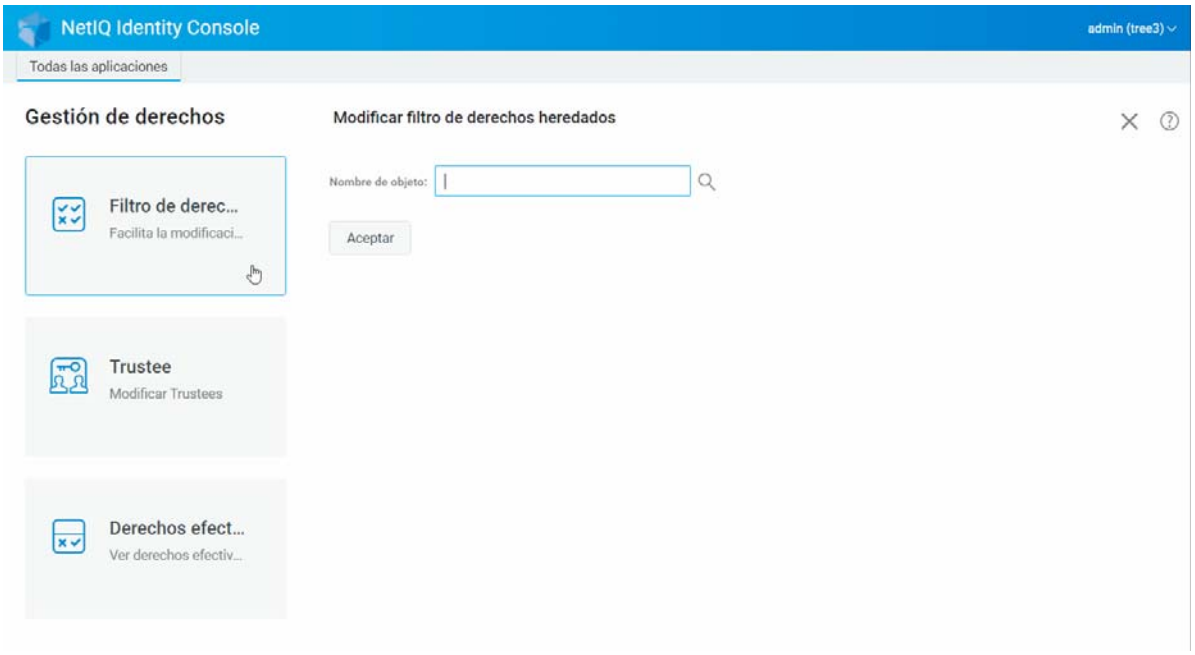
   Nota: El filtro de derechos heredados se selecciona por defecto.

3. Especifique el nombre completo del objeto cuyo filtro de derechos heredados desea modificar, o bien utilice el icono Selector de objetos para buscarlo y, a continuación, haga clic en **Aceptar**.

   Se muestra una lista de los filtros de derechos heredados definidos en el objeto.
4. En **Propiedades**, modifique la lista de filtros de derechos heredados según sea necesario y, a continuación, haga clic en **Aplicar**.

   Para editar la lista de filtros debe tener derechos de supervisión o de control de acceso a la propiedad ACL del objeto. Puede establecer filtros que bloqueen los derechos heredados en el objeto en conjunto, en todas las propiedades del objeto y en propiedades individuales.

Figura 8-1 *Modificar el filtro de derechos heredados*



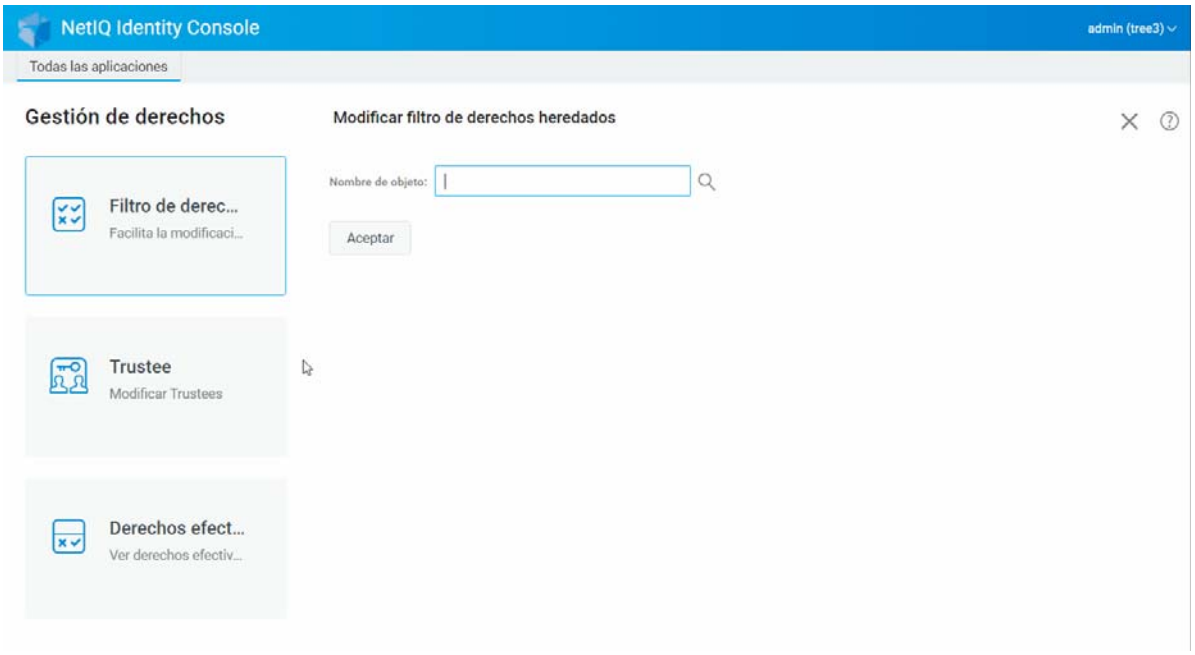
Modificar los derechos de Trustee

Un Trustee es un objeto al que se le han otorgado derechos explícitos en otro objeto del árbol de directorios. Para modificar la lista de Trustees de un objeto determinado:

1. Haga clic en la opción **Gestión de derechos** de la página de destino de Identity Console.
2. Seleccione **Trustee**.
3. Especifique el nombre del objeto cuya lista de Trustees desea ver, o bien utilice el icono Selector de objetos para buscarlo y, a continuación, haga clic en **Aceptar**.

   Así se abre una lista de los Trustees asignados al objeto.
4. Modifique la lista de Trustees si fuera necesario y haga clic en **Aceptar**.
   - Haga clic en el icono para añadir un Trustee.
   - Elimine un Trustee. Para ello, seleccione su casilla de verificación y haga clic en el icono .
   - Modifique la asignación de derechos de un Trustee seleccionando el enlace **Derechos asignados** de dicho Trustee.

Figura 8-2 *Modificar los derechos de Trustee*



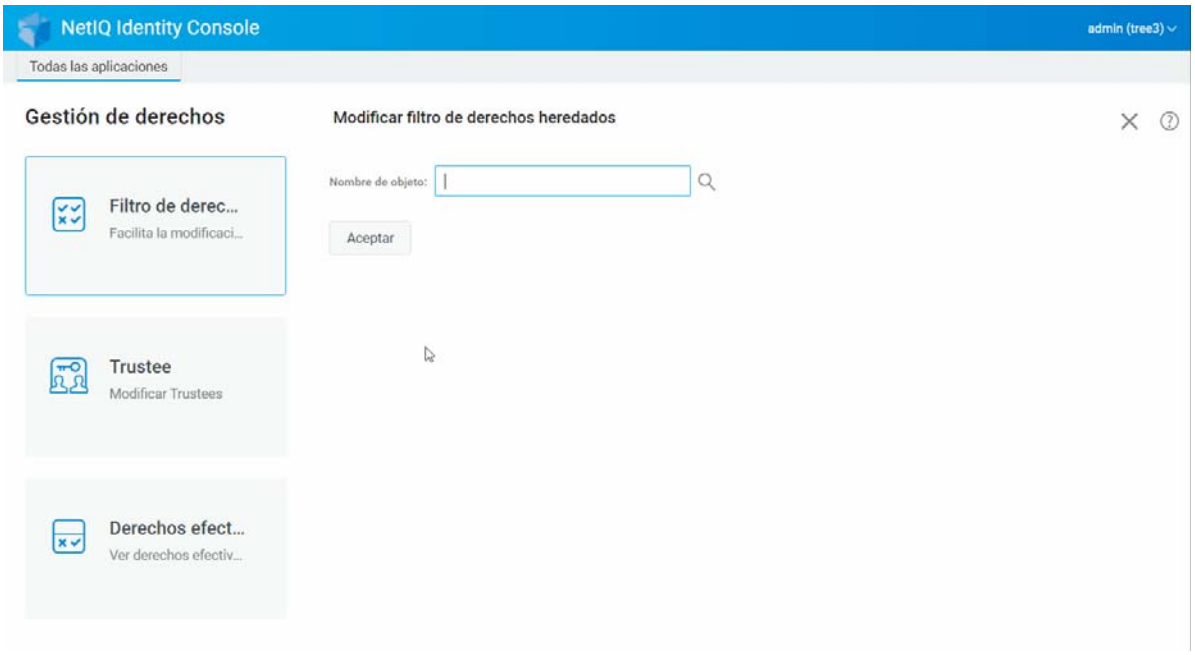
Visualización de derechos vigentes

Derechos efectivos es la combinación de derechos explícitos y heredados que tiene un objeto en cualquier punto del árbol de directorios. Para ver los derechos efectivos de un objeto sobre otro objeto:

1. Haga clic en la opción **Derechos** de la página de destino de Identity Console.
2. Seleccione **Derechos efectivos**.
3. Especifique el nombre del Trustee cuyos derechos desea ver, o bien utilice el icono Selector de objetos para buscarlo y, a continuación, haga clic en **Aceptar**.
4. En el campo Objeto, especifique el nombre del objeto para el que desea ver los derechos efectivos del Trustee.

   eDirectory calcula los derechos efectivos y los muestra en el campo **Derechos efectivos**.

Figura 8-3 *Visualizar los derechos vigentes*



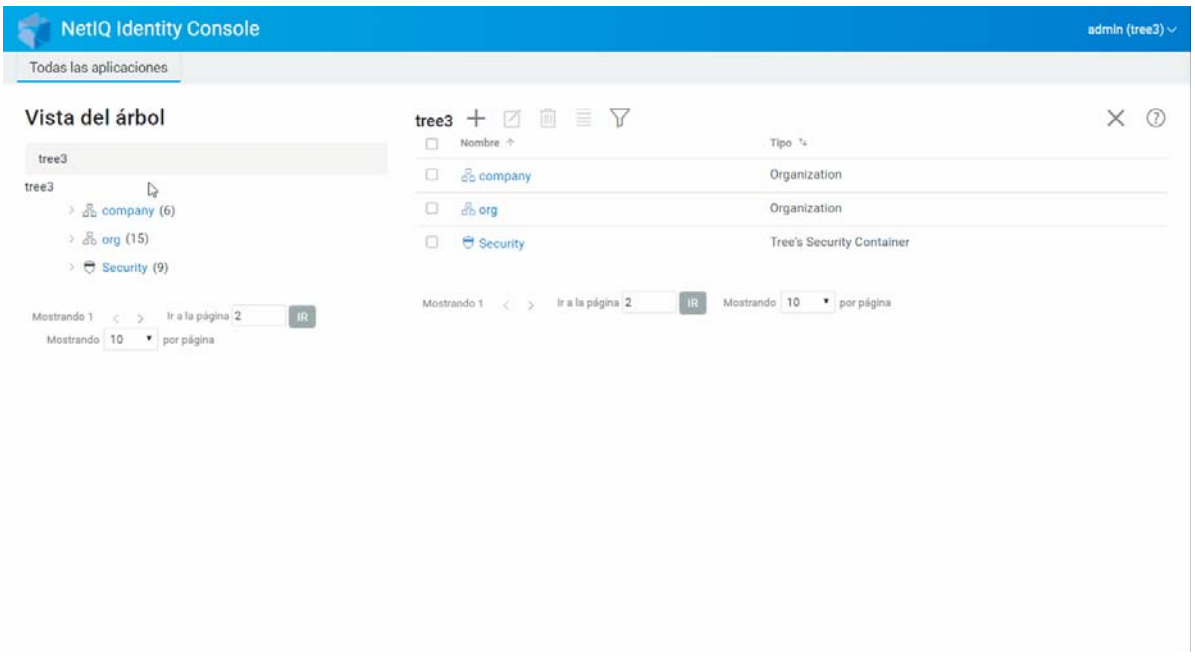
9 Vista Árbol

La vista Árbol permite examinar un árbol de directorios, y crear, suprimir o modificar varios objetos en ese árbol. La vista Árbol presenta un marco de navegación y otro de contenido.

Marco de navegación de la vista Árbol

En la vista de Árbol, el marco de navegación presenta la estructura de directorios. En el marco de navegación, se muestra el contenedor, incluidos el volumen (sistema de archivos), objetos, etc. Se puede hacer clic en todas las opciones que se muestran debajo del marco de navegación para ayudarle a examinar la estructura de directorios. En el marco de navegación, se muestran por defecto hasta 10 objetos subordinados por contenedor, pero puede cambiar este ajuste debajo del panel del marco de navegación en la vista Árbol.

Figura 9-1 *El marco de navegación en la vista del árbol*



Marco de contenido de la vista Árbol

Al seleccionar uno de los objetos Contenedor del marco de navegación, el marco de contenido muestra todos los objetos de dicho contenedor. El marco de contenido es el lugar en que realmente se visualizan y modifican los objetos de directorio. El marco de contenido incluye un encabezado que presenta varias acciones disponibles:

Barra de títulos: La barra de títulos del marco de contenido muestra el nombre del objeto Contenedor seleccionado.

Encabezado de la lista de objetos: El encabezado de la lista de objetos proporciona acceso a los siguientes elementos:

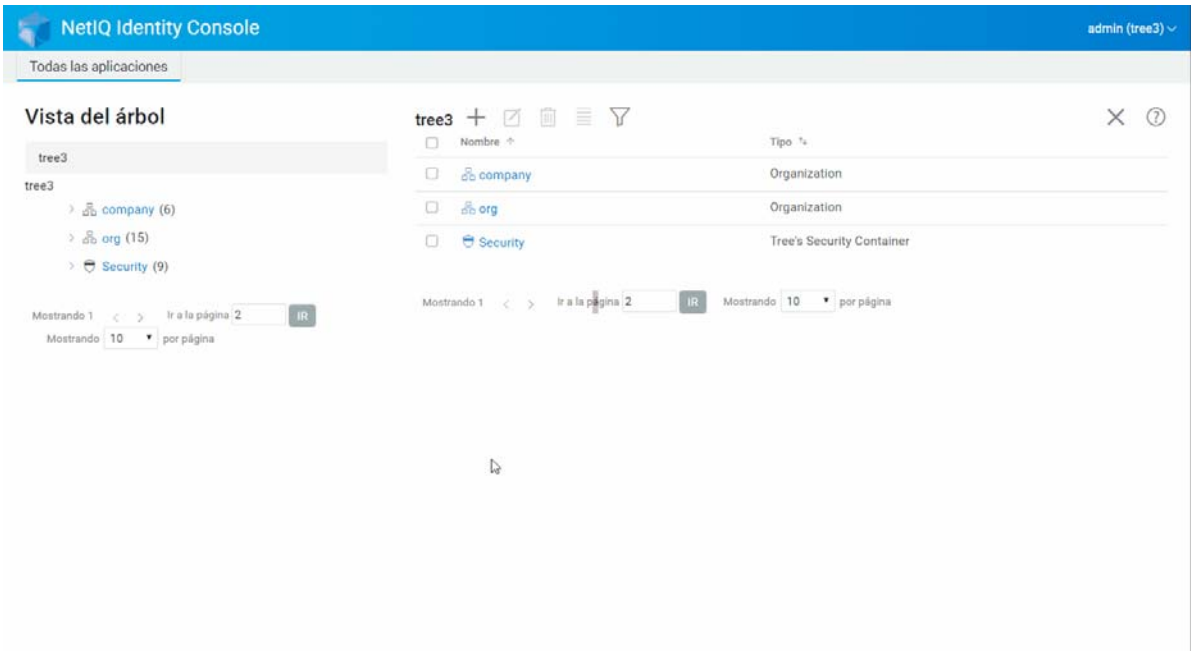
- **Añadir**: haga clic en el icono  para añadir un nuevo objeto.
- **Modificar**: seleccione un objeto y haga clic en el icono  para modificarlo. Esta acción abre el libro de propiedades del objeto seleccionado para que pueda modificar sus atributos. No se pueden modificar conjuntamente varios objetos.
- **Suprimir**: seleccione un objeto y haga clic en el icono  para suprimir los objetos seleccionados. Se pueden suprimir conjuntamente varios objetos. No se pueden suprimir los objetos No hoja.
- **Acciones**: seleccione un objeto y haga clic en el icono  para abrir un menú desplegable de tareas admitidas para los objetos seleccionados. Para realizar una tarea, selecciónela en el menú desplegable y proporcione la información requerida.
- **Recuento de objetos**: en la vista Árbol, se enumeran los objetos de la página actual en la parte inferior de la página. Por defecto, el marco de contenido muestra un máximo de 20 objetos subordinados por contenedor, pero puede cambiar este ajuste.
- **Seleccionar todo**: la casilla de verificación del encabezado permite seleccionar todos los objetos de la página actual.
- **Clasificar**: se pueden ordenar las columnas por **Nombre** y **Tipo**. Haga clic en cualquiera de ellos para conmutar la clasificación de objetos entre orden alfabético ascendente y descendente.
- **Filtro de búsqueda**: haga clic en el icono  . para abrir la ventana emergente del filtro. Mediante esta opción, puede crear un filtro que limite los objetos que se muestran en la lista de objetos. Puede filtrar un tipo y nombre de objeto según sea necesario.

  Seleccione la opción  para abrir el cuadro de diálogo Filtro avanzado, que le permite crear un filtro mediante casi cualquier atributo de objeto. Para obtener más información, consulte “Configurar la búsqueda avanzada” en la página 26.

Para realizar una acción en un objeto, seleccione la casilla de verificación y, a continuación, seleccione el icono de acción  en el encabezado Lista de objetos. Seleccione el objeto (en el nivel actual) para realizar una acción en el contenedor que está actualmente examinando. Mediante esta opción, se pueden realizar las siguientes acciones:

- “Modificar el filtro de derechos heredados” en la página 51
- “Modificar los derechos de Trustee” en la página 52
- “Ampliar un objeto” en la página 64
- “Renombrar un objeto” en la página 48
- Definir contraseña
- “Visualización de derechos vigentes” en la página 53

Figura 9-2 *Marco de contenido en la vista del árbol*



10 Gestión de esquemas

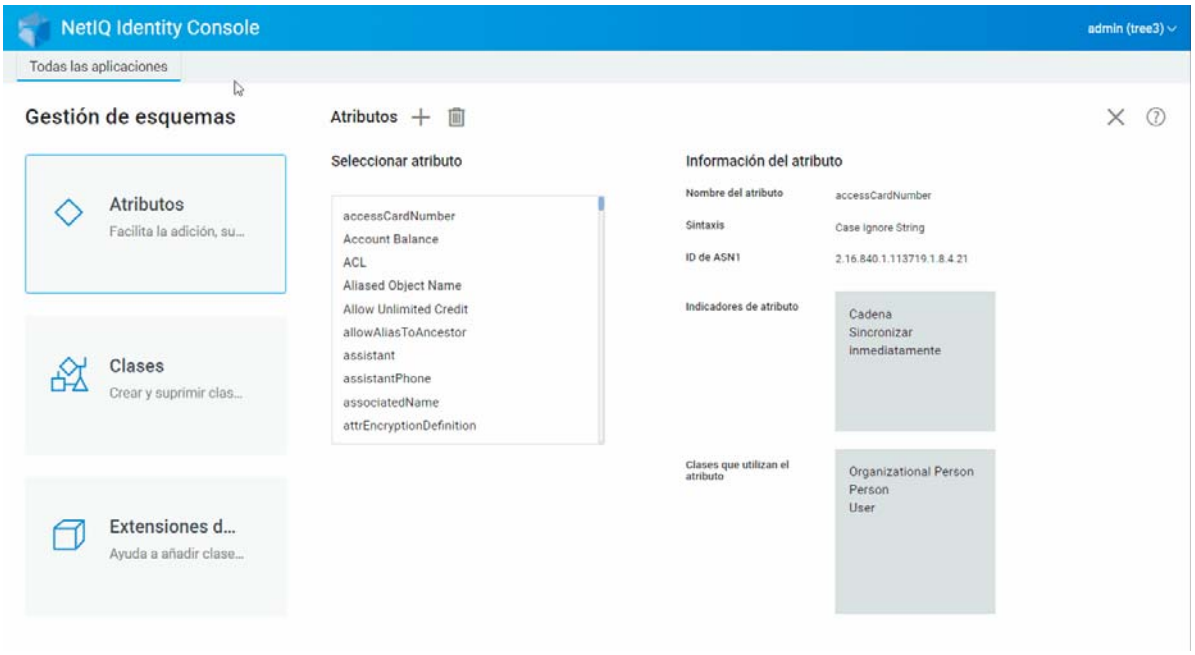
El esquema de directorio define los tipos de objetos que se pueden crear en el árbol (como usuarios, impresoras, grupos, etc.) y la información necesaria u opcional en el momento en que se crea el objeto. Identity Console proporciona las siguientes tareas relacionadas con los esquemas:

Crear un atributo

Puede definir sus propios tipos personalizados de atributos y añadirlos como atributos opcionales a las clases de objetos existentes. Sin embargo, no puede añadir atributos obligatorios a las clases existentes. Para crear un atributo:

1. Haga clic en la opción **Gestión de esquemas** de la página de destino de Identity Console.
2. Haga clic en el icono +.
3. En la página Crear atributo, introduzca la información siguiente:
   - Nombre de atributo
   - ID de ASN1 (opcional)
   - Sintaxis
   - Indicadores del atributo
4. Después de introducir toda la información necesaria, haga clic en el botón Crear.
5. Aparece un mensaje de confirmación que indica que se ha creado el atributo.

Figura 10-1 *Crear un atributo*



Crear una clase

Mediante la opción **Gestión de esquemas**, puede definir sus propias clases. A continuación, puede ampliar objetos individuales con las propiedades definidas en las clases. Para crear una clase:

1. Haga clic en la opción **Gestión de esquemas** de la página de destino de Identity Console y seleccione **Clases**.
2. Haga clic en el icono +.
3. En la página Crear atributo, introduzca la información siguiente:
   - Nombre de clase
   - ID de ASN1 (opcional)
   - Indicadores de clase: seleccione uno de los siguientes indicadores de clase:
     - **Clase efectiva:** Defina este indicador si desea crear una clase efectiva que pueda utilizarse para crear objetos.
     - **Clase no efectiva:** Se utiliza como espacio reservado para un grupo de atributos. Una clase no efectiva no puede utilizarse para crear objetos, pero puede especificarse como una clase de la que otras pueden heredar atributos. Por ejemplo, la clase Persona es una clase no efectiva que contiene atributos heredados por la clase Usuario.
     - **Clase auxiliar:** Recopilación de atributos que solo pueden asociarse a objetos individuales, no a clases enteras.
     - **Clase contenedor:** Defina este indicador si desea que sea una clase contenedor. Si se utiliza para crear objetos, éstos pasan a ser objetos contenedor (como OU). No defina este indicador para una clase de objeto hoja.

Nota: Si selecciona clases efectivas y no efectivas, debe especificar también valores para la superclase. Si seleccione la clase auxiliar, la superclase será opcional.

4 Después de introducir todos los detalles de la directiva, haga clic en **Siguiente**.

5 En la pantalla siguiente, seleccione los atributos opcionales, obligatorios y de denominación, y haga clic en **Aceptar**.

6 Aparece un mensaje de confirmación que indica que se ha creado la clase.

Asignar atributos a una clase

Puede añadir atributos opcionales a las clases existentes si las necesidades de información de su organización cambian o si se está preparando para fusionar árboles. Para añadir un atributo a una clase existente:

Nota: Los atributos obligatorios sólo se pueden definir durante la creación de una clase. Un atributo obligatorio es aquel que debe completarse cuando se va a crear un objeto.

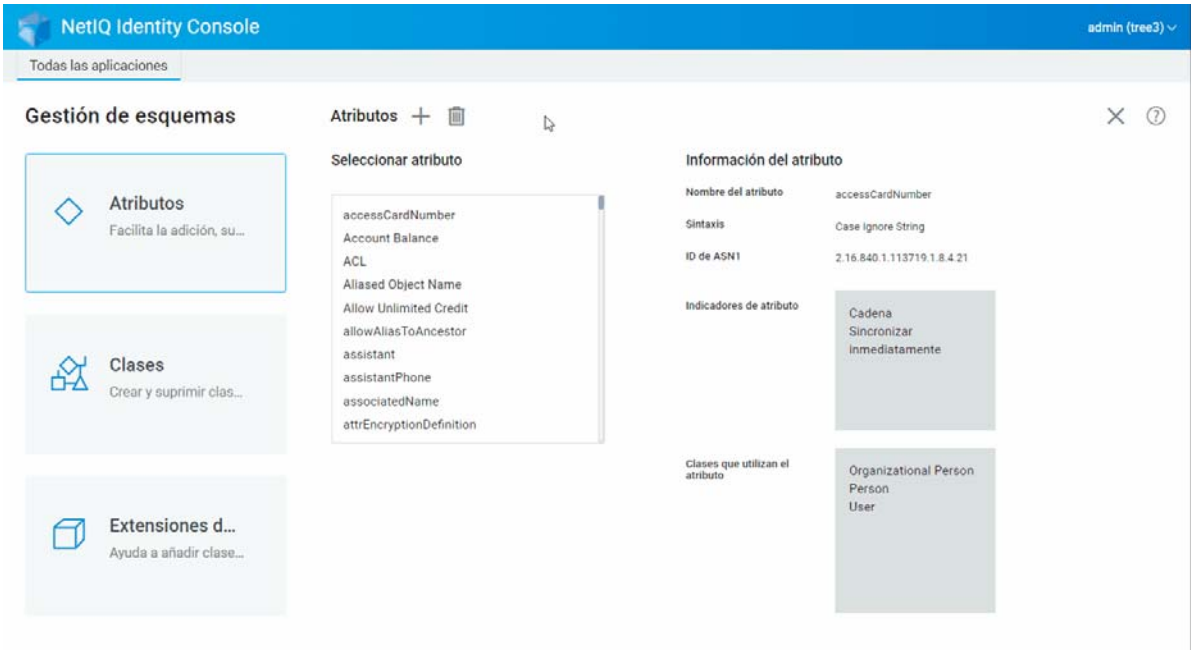
1 Haga clic en la opción **Gestión de esquemas** de la página de destino de Identity Console y seleccione **Clases**.

2 Haga clic en cualquier clase enumerada en **Seleccionar clase**.

3 La información de la clase correspondiente se mostrará en el lado derecho de la pantalla.

4 Haga clic en el botón + ubicado junto a la opción **Atributos** y seleccione los atributos que desee añadir. A continuación, haga clic en **Añadir** > **Guardar**.

Figura 10-2 *Asignar atributos a una clase*

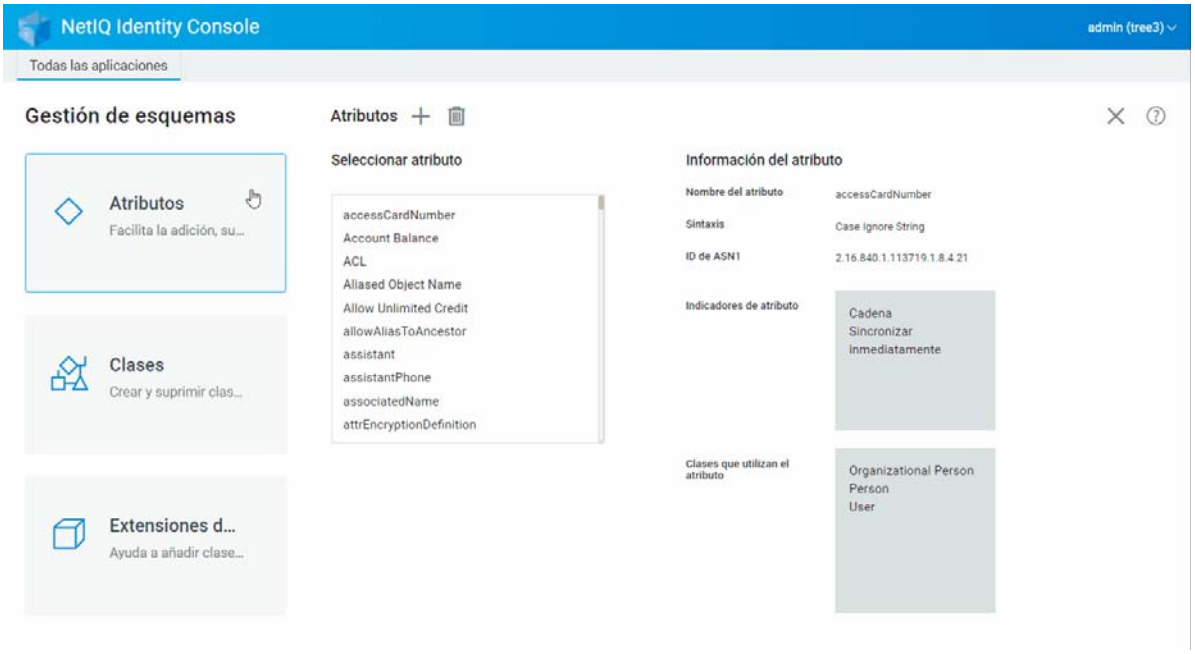


Ver información de los atributos

Puede ver los detalles estructurales de un atributo, como por ejemplo, la sintaxis, los indicadores y las clases que utilizan el atributo. Para ver la información de un atributo:

1. Haga clic en la opción **Gestión de esquemas** de la página de destino de Identity Console y seleccione **Atributos**.
2. Haga clic en cualquier atributo enumerado en **Seleccionar atributo**.
3. La información del atributo correspondiente se mostrará en el lado derecho de la pantalla.

Figura 10-3 *Ver información de los atributos*



Suprimir un atributo

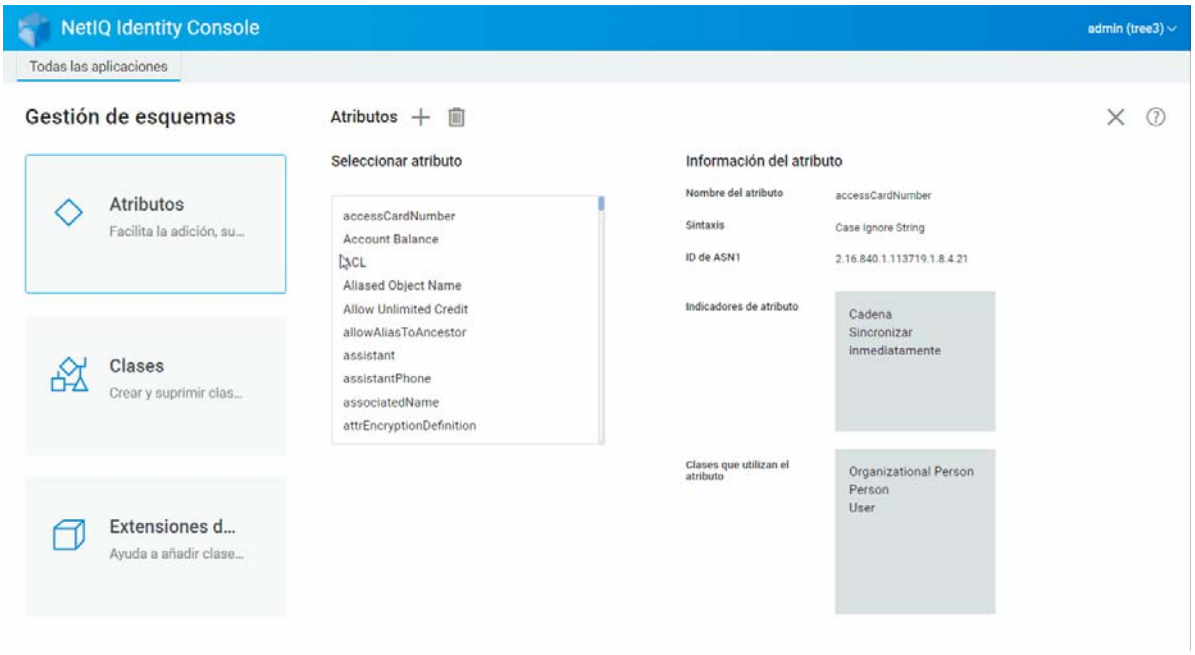
Puede suprimir los atributos no utilizados que no formen parte del esquema base del árbol de eDirectory. Esto puede resultar muy útil después de fusionar dos árboles de directorios o si un atributo se ha quedado obsoleto con el paso del tiempo. Para suprimir un atributo:

1. Haga clic en la opción **Gestión de esquemas** de la página de destino de Identity Console y seleccione **Atributos**.
2. Seleccione el atributo que desee suprimir en la lista **Seleccionar atributo** y haga clic en el icono .

   Nota: El icono solo se habilitará cuando seleccione un atributo que pueda suprimirse.

3. Haga clic en **Aceptar** para confirmar la supresión.

Figura 10-4 *Suprimir un atributo*



Suprimir una clase

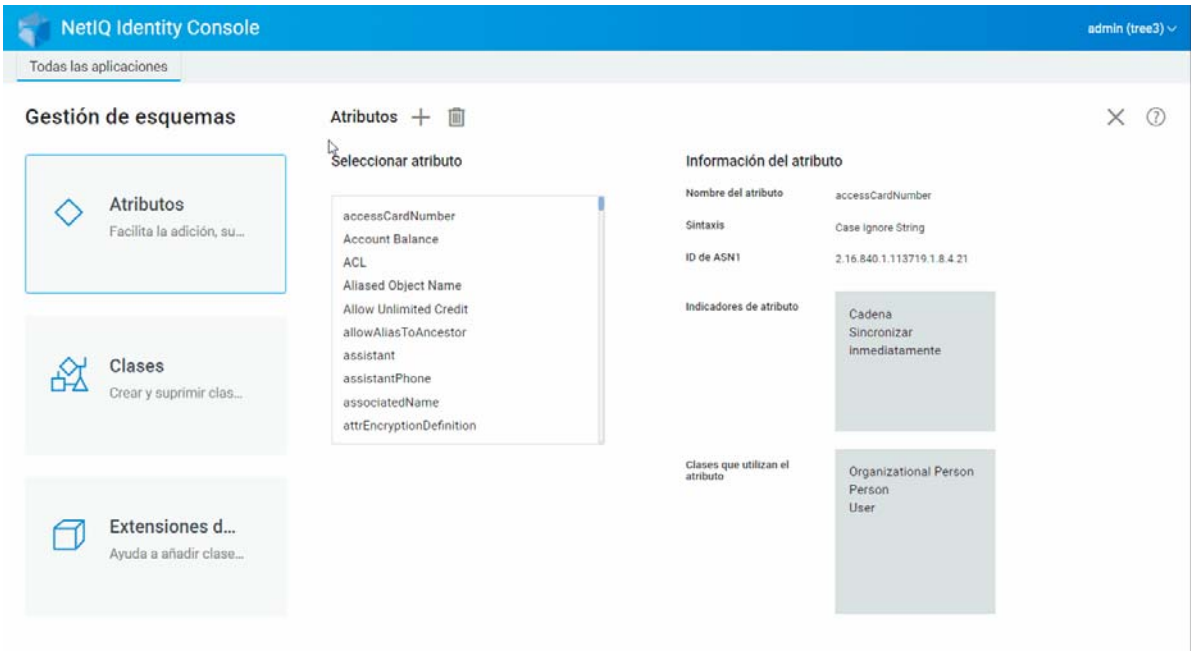
Puede suprimir las clases no utilizadas que no formen parte del esquema base del árbol de eDirectory. Identity Console no permite suprimir clases que se estén utilizando en particiones duplicadas localmente. Para suprimir una clase:

1. Haga clic en la opción **Gestión de esquemas** de la página de destino de Identity Console y seleccione **Clases**.
2. Seleccione la clase que desee suprimir en la lista **Seleccionar clase** y haga clic en el icono .

   Nota: El icono solo se habilitará cuando seleccione una clase que pueda suprimirse.

3. Haga clic en **Aceptar** para confirmar la supresión.

Figura 10-5 *Suprimir una clase*



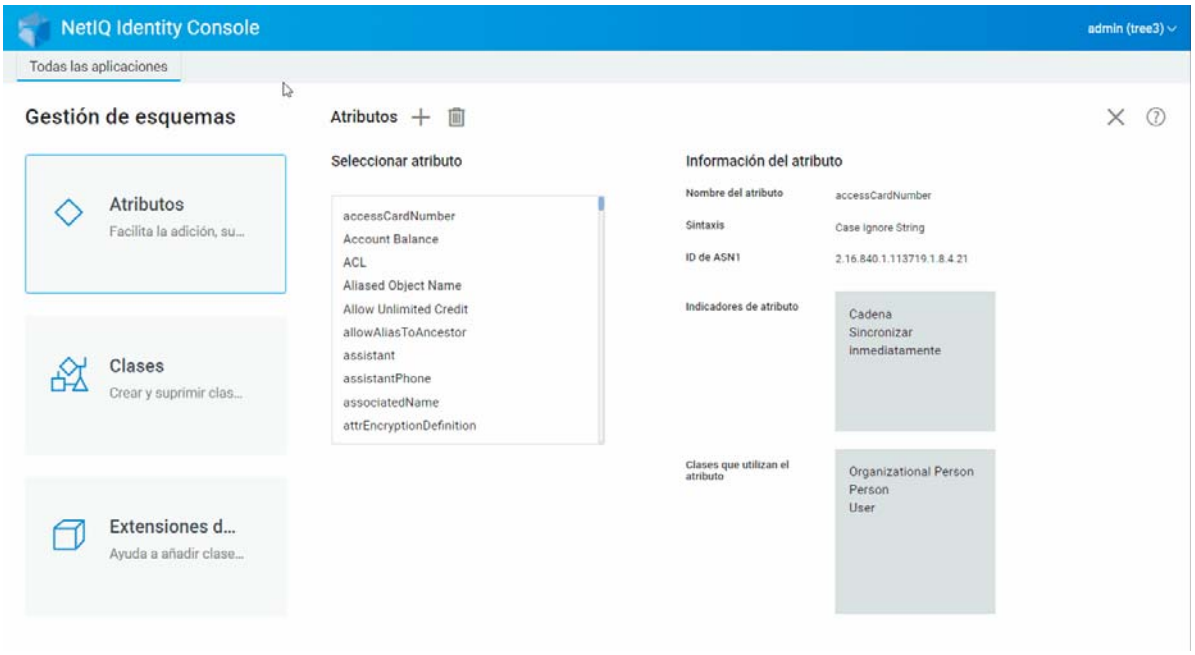
Ampliar un objeto

Realice los pasos siguientes para ampliar un objeto:

1. Haga clic en la opción **Gestión de esquemas** de la página de destino de Identity Console y seleccione **Extensión del objeto**.
2. Especifique el nombre del objeto o utilice el selector de objetos para elegir el objeto que desea ampliar y haga clic en el icono .
3. Haga clic en el icono y seleccione la clase auxiliar; a continuación, haga clic en **Aceptar**.

   Nota: Si se adjunta un atributo obligatorio a la clase auxiliar seleccionada, se le solicitará que introduzca los valores necesarios en la ventana emergente **Atributos obligatorios**.
4. Aparecerá un mensaje de confirmación que indica que la clase auxiliar se ha añadido al objeto.
5. Para eliminar una clase auxiliar existente del objeto, seleccione la clase y haga clic en el icono .

Figura 10-6 *Ampliar un objeto*



11 Gestión de eventos de auditoría

En este capítulo, se explica cómo gestionar distintos eventos de auditoría mediante Identity Console. Esta función permite habilitar o inhabilitar eventos de auditoría para el servidor NCP.

Configurar los eventos de auditoría de CEF

1. Entre a la sesión de Identity Console mediante su nombre de usuario y contraseña.
2. Seleccione **Auditoría**.
3. Seleccione el servidor NCP que desea importar y haga clic en **Aceptar**.

   Nota: Después de habilitar por primera vez los eventos de CEF para cualquier servidor NCP, algunos se seleccionarán por defecto.

4. Configure los eventos de auditoría de CEF:
   - **Configuración de eventos:** Habilite o inhabilite los siguientes eventos en función de la auditoría necesaria para su entorno:

Nota: Las categorías de eventos individuales de la sección de configuración de eventos se contraerán por defecto. Puede expandir cada categoría para seleccionar eventos individuales.

Opciones	Descripción
Eventos de seguridad	Seleccione los eventos de seguridad para los que desea registrar eventos. Puede registrar eventos para añadir o suprimir un componente, detectar un intruso, cambiar una contraseña o autenticar usuarios, etc.
Eventos de objeto	Seleccione los eventos de objeto para los que desea registrar eventos. Puede registrar eventos para crear, suprimir, renombrar, mover y buscar objetos.
Eventos de atributos	Seleccione los eventos de atributos para los que desea registrar eventos. Puede registrar eventos para leer y suprimir atributos y para añadir, suprimir y comparar valores de atributo.
Eventos de LDAP	Seleccione los eventos LDAP para los que desea registrar eventos.

- **Ajustes avanzados:** Mediante los ajustes avanzados, puede realizar las siguientes acciones.
  - **Global:** Puede seleccionar o borrar los ajustes globales de entradas duplicadas.
    - **No enviar eventos replicados:** Seleccione esta opción para dejar de recibir eventos duplicados procedentes de réplicas de otros servidores.
  - **Registrar valores del evento:** Los eventos se registran en un archivo de texto. Los valores de eventos cuyo tamaño supera los 768 bytes se consideran "valores grandes". Es posible registrar eventos de cualquier tamaño.
    - **Registrar valores elevados:** Seleccione esta opción para registrar eventos cuyo tamaño supere los 768 bytes.
    - **Registrar valores de atributos:** Seleccione esta opción para visualizar los valores de atributos. Esto se aplica solo a los eventos **Añadir valor** y **Suprimir valor**.
    - **Registrar valores de atributos cifrados:** Seleccione esta opción para visualizar los valores de atributos cifrados. Esto se aplica solo a los eventos **Añadir valor** y **Suprimir valor**.

    Nota: Si el tamaño del evento es superior a 768 bytes, el valor del evento se trunca y se guarda en el archivo de registro.

Descripción de los tipos de eventos de CEF

Puede configurar CEF para que registre eventos en las siguientes categorías:

- Seguridad
- Objetos

- Atributos
- LDAP

Puede auditar el siguiente conjunto de tipos de eventos por defecto:

Categoría	Tipo de evento
Seguridad	◆ ACL cambiada ◆ Añadir componente ◆ Suprimir componente ◆ Intruso detectado ◆ Entrada inhabilitada ◆ Entrada habilitada ◆ Entrada ◆ Cambiar equivalencias de seguridad ◆ Config. de auditoría ◆ Cambiar contraseña ◆ Desbloqueo de cuenta ◆ Salir ◆ Conexión ◆ Suplantar ◆ Authenticate ◆ Verificar contraseña ◆ Cambiar configuración de entrada ◆ Consultar credenciales
Objetos	◆ Crear un objeto ◆ Suprimir el objeto ◆ Renombrar objeto ◆ Mover el objeto ◆ Lectura DSA ◆ Buscar
Atributos	◆ Leer atributo ◆ Suprimir el atributo ◆ Añadir valor ◆ Suprimir el valor ◆ Comparar valor de atributos

Categoría	Tipo de evento
LDAP	◆ Asociación LDAP ◆ Respuesta de asociación LDAP ◆ Desasociación LDAP ◆ Conexión LDAP ◆ Búsqueda LDAP ◆ Respuesta de búsqueda LDAP ◆ Respuesta de entrada de búsqueda LDAP ◆ Adición de LDAP ◆ Respuesta de adición de LDAP ◆ Comparación de LDAP ◆ Respuesta de comparación de LDAP ◆ Modificación de LDAP ◆ Modificación de la respuesta LDAP ◆ Eliminación de LDAP ◆ Respuesta de supresión de LDAP ◆ Modificación de nombre completo de LDAP ◆ Respuesta de modificación de nombre completo de LDAP ◆ Abandono de LDAP ◆ Operación extendida de LDAP ◆ Operación extendida del sistema LDAP ◆ Respuesta de operación extendida de LDAP ◆ Modificar configuración del servidor LDAP ◆ Operación desconocida de LDAP ◆ Modificación de contraseña LDAP

Configurar el filtrado de auditoría de CEF

Mediante los filtros y las notificaciones de eventos, CEF es capaz de generar informes cuando se produce o no un tipo de evento específico. También puede filtrar eventos de uno o varios atributos o clases de objeto específicos en función del tipo de evento. CEF evalúa todos los eventos generados a partir de los filtros configurados en el servidor de eDirectory y registra solo los eventos que coinciden con los filtros.

En esta sección, se proporciona la información necesaria para configurar los filtros y las notificaciones del sistema.

- “Filtrar eventos de eDirectory con filtro de exclusión” en la página 71
- “Filtrar eventos de objetos de CEF” en la página 71
- “Filtrar eventos de atributos de CEF” en la página 72

Filtrar eventos de eDirectory con filtro de exclusión

Haga clic en el enlace **Filtro de exclusión** para configurar el filtrado de esos atributos y clases de objetos para que los que no desea que se genere un evento. Puede seleccionar atributos y clases de objetos.

Para configurar el filtrado de eventos de eDirectory no deseados:

1. En Identity Console, seleccione **Auditoría** en la página principal.
2. Seleccione el servidor NCP que desea importar y haga clic en **Aceptar**.
3. A continuación, vaya a **Ajustes avanzados** y haga clic en **Filtro de exclusión** en **Filtros**.

   Aparece la ventana Filtrado de exclusiones de CEF.
4. En la lista **Clases Objeto disponibles**, seleccione las clases de objeto para las que no desea recopilar eventos y, a continuación, haga clic en la flecha derecha para moverlas a la lista **Clases Objeto seleccionadas**.
5. En la lista **Atributos disponibles**, seleccione los atributos que desee. Seleccione el atributo y haga clic en la flecha derecha para añadir el atributo a la lista de atributos seleccionados.
6. Haga clic en **Aceptar.**

Mediante el filtro configurado, el módulo de auditoría de CEF deja de generar eventos para todos los atributos y las clases de objetos seleccionados.

Filtrar eventos de objetos de CEF

Puede configurar el filtrado de objetos para buscar solo un evento o eventos específicos. Por ejemplo, si desea recibir una notificación cuando alguien cree una cuenta de usuario en eDirectory, puede crear un filtro mediante la selección de la clase de objeto Usuario a fin de registrar eventos de creación de un nuevo objeto Usuario.

Para configurar el filtrado de cuentas, haga clic en el enlace Eventos de objeto, seleccione la clase y, a continuación, haga clic en **Aceptar** para salir de la aplicación.

Para configurar filtros para los eventos de gestión de cuentas:

1. En Identity Console, seleccione **Auditoría** en la página principal.
2. Seleccione el servidor NCP que desea importar y haga clic en **Aceptar**.
3. A continuación, vaya a **Ajustes avanzados** y haga clic en **Eventos de objeto** en **Filtros**.

   Aparece la ventana Filtrado de objetos de CEF.
4. En la lista **Clases Objeto disponibles**, seleccione la clase de objeto que desee y, a continuación, haga clic en la flecha derecha para moverla a la lista **Clases Objeto seleccionadas**. A continuación, haga clic en **Aceptar**.

Mediante el filtro configurado, el módulo de auditoría de CEF comprueba todos los eventos generados para las clases de objeto seleccionadas y registra esos eventos.

Filtrar eventos de atributos de CEF

Haga clic en el enlace **Eventos de atributos** para configurar el filtrado de eventos de atributos. Por ejemplo, si desea recibir una notificación cuando alguien añada un nuevo valor de atributo en eDirectory, puede crear un filtro para registrar eventos de adición de un nuevo valor.

Para configurar el filtrado de eventos de atributos:

1. En Identity Console, seleccione **Auditoría** en la página principal.
2. Seleccione el servidor NCP que desea importar y haga clic en **Aceptar**.
3. A continuación, vaya a **Ajustes avanzados** y haga clic en **Eventos de atributos** en **Filtros**.

   Aparece la ventana **Filtrado de configuración de atributos**.
4. En la lista **Clases Objeto disponibles**, seleccione las clases de objeto para las que desea recopilar eventos y, a continuación, haga clic en la flecha derecha para moverlas a la lista **Clases Objeto seleccionadas**.
5. En la lista **Atributos seleccionados**, seleccione los atributos que desee para las clases de objeto seleccionadas. Seleccione el atributo y haga clic en la flecha derecha para añadir el atributo a la lista de atributos seleccionados.

   Nota: Si selecciona una clase de objeto, se seleccionan todos los eventos de todos los atributos de esa clase de objeto. En este caso, obtendrá todos los eventos de todos los atributos de las clases de objeto seleccionadas.

   ---
6. Haga clic en **Aceptar**.

Con el filtro configurado, el módulo de auditoría de CEF comprueba los eventos generados para buscar todos los atributos y las clases de objetos seleccionados y los registra.

12 Gestión de atributos cifrados

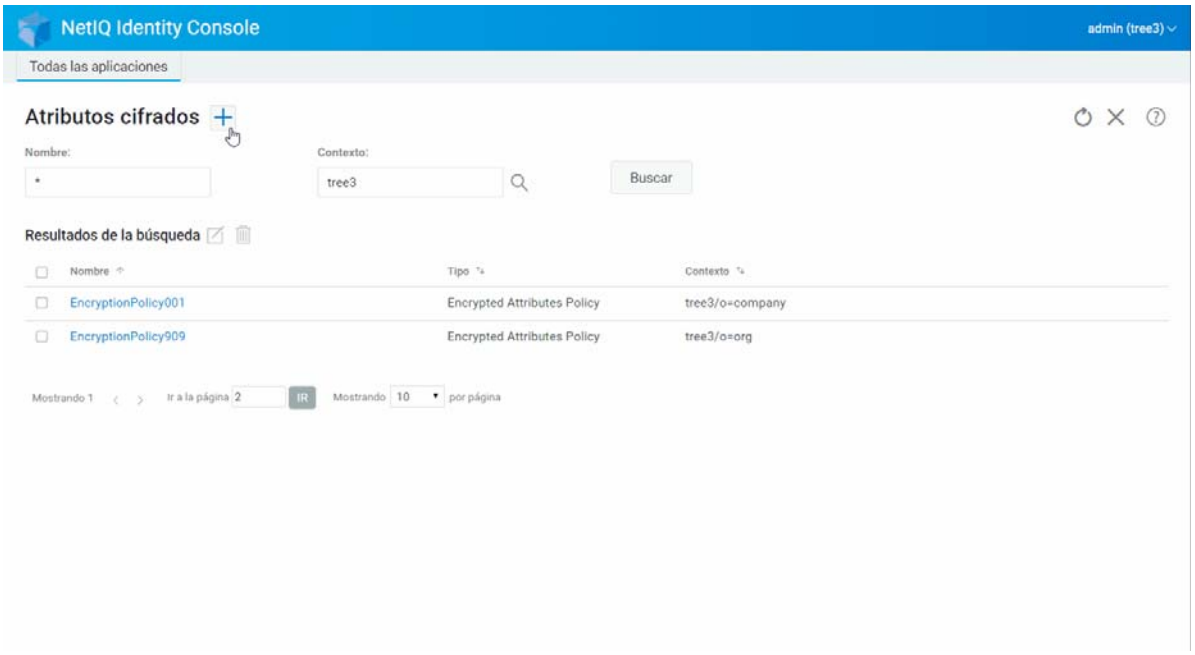
Identity Console puede leer de forma segura los atributos cifrados del directorio de eDirectory. Mediante Identity Console, puede crear, modificar o suprimir varias directivas para estos atributos cifrados.

Crear una directiva de atributos cifrados

Para crear una nueva directiva de contraseña:

1. Haga clic en la opción **Atributos cifrados** de la página de destino de Identity Console.
2. Haga clic en el icono +.
3. En la página Crear directiva de atributos cifrados, introduzca la siguiente información:
   - Especifique el nombre de la directiva.
   - Introduzca o seleccione el contexto.
   - Seleccione el servidor NCP.
   - Seleccione atributos.
4. Después de especificar la información necesaria, haga clic en **Finalizar**.
5. Aparecerá un mensaje de confirmación que indica que se ha creado la directiva.

Figura 12-1 *Crear una directiva de atributos cifrados*

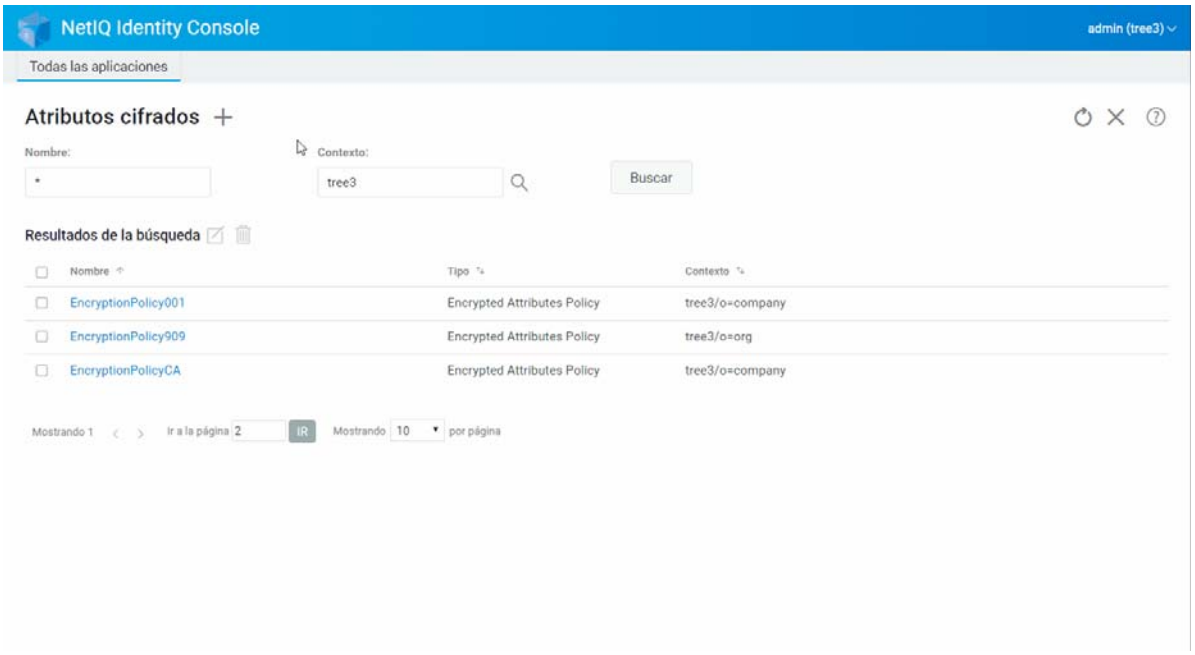


Suprimir una directiva de atributos cifrados

Para suprimir una directiva de atributos cifrados:

1. Haga clic en la opción **Atributos cifrados** de la página de destino de Identity Console.
2. Especifique el nombre y el contexto del atributo, o utilice la función de búsqueda para buscarlo; a continuación, haga clic en el botón Buscar.
3. Seleccione los atributos en la lista y haga clic en el icono 🗑.
4. Aparece un mensaje de confirmación que indica que se ha suprimido la directiva.

Figura 12-2 *Suprimir una directiva de atributos cifrados*

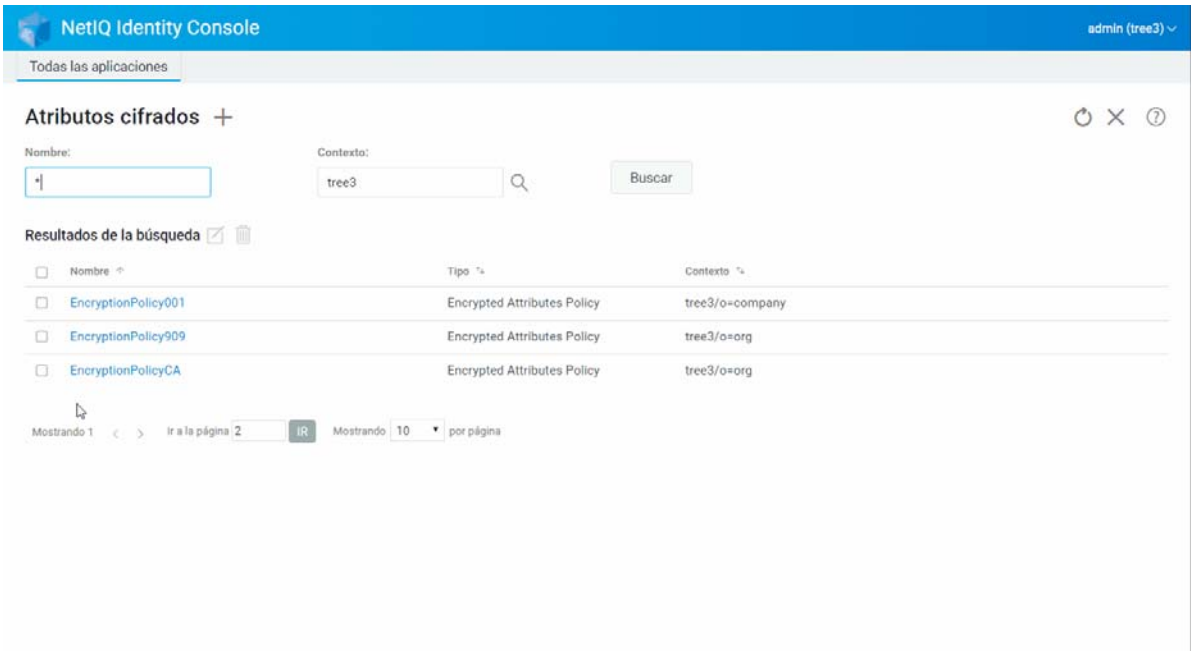


Modificar una directiva de atributos cifrados

Para modificar una directiva de atributos cifrados:

1. Haga clic en la opción **Atributos cifrados** de la página de destino de Identity Console.
2. Especifique el nombre y el contexto del objeto y, a continuación, haga clic en el botón Buscar.
3. Seleccione el atributo en la lista de objetos y haga clic en el icono .
4. Realice los cambios y, a continuación, haga clic en el botón Guardar.
5. Aparecerá un mensaje de confirmación que indica que se ha modificado la directiva.

Figura 12-3 *Modificar una directiva de atributos cifrados*



13 Gestión de réplica cifrada

Para habilitar la réplica cifrada, debe configurar la partición para esta función. Los ajustes de configuración se almacenan en el objeto raíz de la partición. Solo puede optar por habilitar la réplica cifrada en un nivel de partición. Al habilitar la réplica cifrada en un nivel de partición, se cifra la réplica entre todas las réplicas que alojan la partición. Por ejemplo, supongamos que la partición P1 tiene las réplicas R1, R2, R3 y R4. Puede cifrar la réplica entre todas las réplicas.

- "Habilitar la réplica cifrada para las particiones" en la página 77

Habilitar la réplica cifrada para las particiones

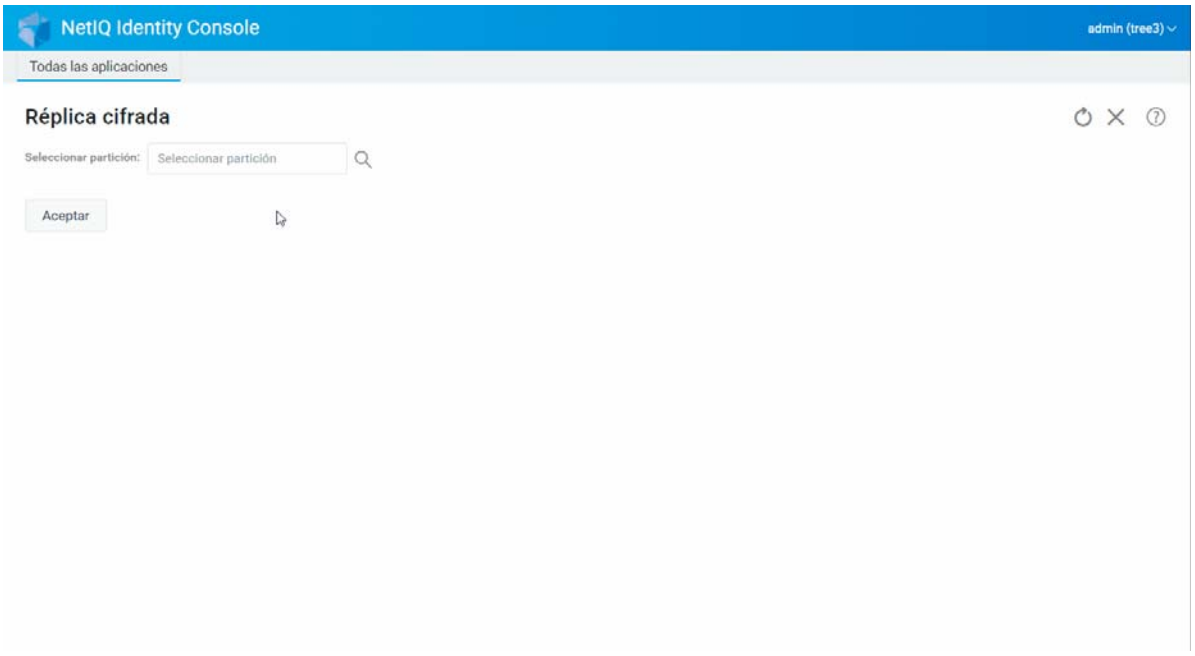
Para habilitar la réplica cifrada para las particiones:

Nota: Para habilitar una partición para la réplica cifrada, todos los servidores que alojen la partición deben ser servidores de eDirectory 9.2 o versiones posteriores.

---

1. Haga clic en la opción **Réplica cifrada** de la página de destino de Identity Console.
2. Especifique la partición para la que desea habilitar la réplica cifrada o desplácese a ella.
3. Asegúrese de seleccionar la opción **Habilitar réplica cifrada**. Si inhabilita la réplica cifrada para una partición, anule la selección de esta opción.
4. Haga clic en **Finalizar**.
5. Aparece un mensaje de confirmación que indica que se ha habilitado la réplica cifrada.

Figura 13-1 *Habilitar la réplica cifrada para las particiones*



14 Gestión de particiones y réplicas

Las operaciones de partición y réplica permiten gestionar el diseño físico de eDirectory y su distribución entre los servidores de directorio.

Las particiones crean divisiones lógicas del árbol de eDirectory. Por ejemplo, si elige una unidad administrativa y la crea como una partición nueva, dividirá dicha unidad administrativa y todos sus objetos subordinados de su partición padre. La unidad administrativa que elija se convierte en la raíz de una partición nueva. Las réplicas de la nueva partición existen en los mismos servidores que las réplicas del padre y los objetos de la nueva partición pertenecen al objeto raíz de la nueva partición.

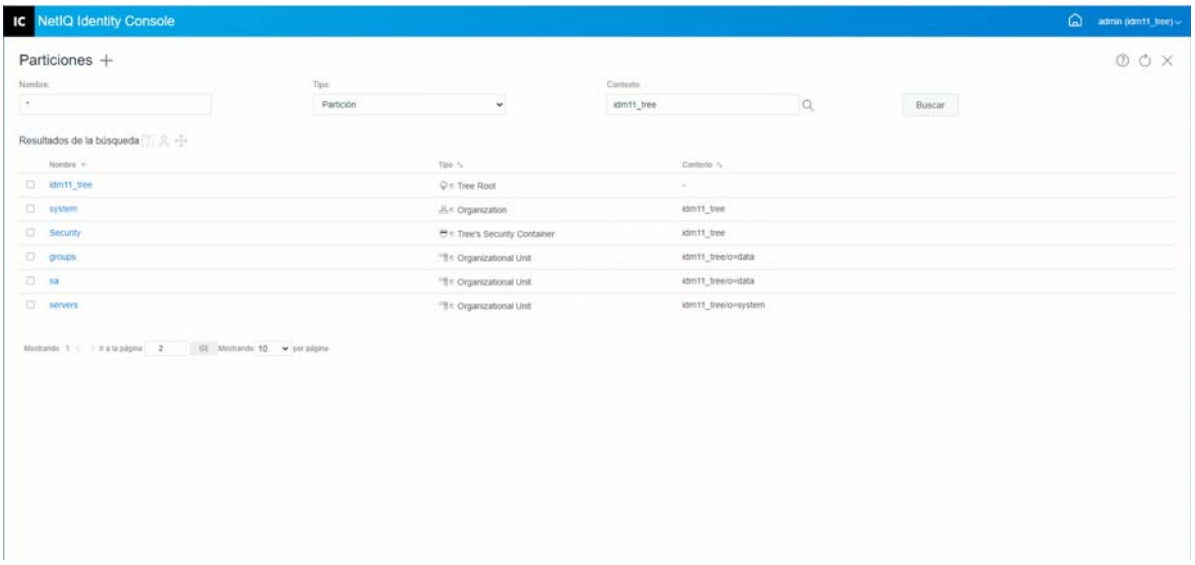
Mediante el módulo Partición, se pueden realizar las siguientes tareas:

Creación de particiones

Para crear una nueva partición:

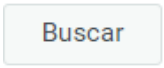
1. Haga clic en la opción **Gestión de particiones** de la página de destino de Identity Console.
2. Haga clic en el icono  .
3. En la página Crear partición, especifique el contenedor que desea utilizar como raíz de la nueva partición o utilice el icono  para buscarlo. A continuación, haga clic en **Crear**.
4. Aparece un mensaje de confirmación que indica que se ha creado la partición.

Figura 14-1 *Creación de una partición nueva*



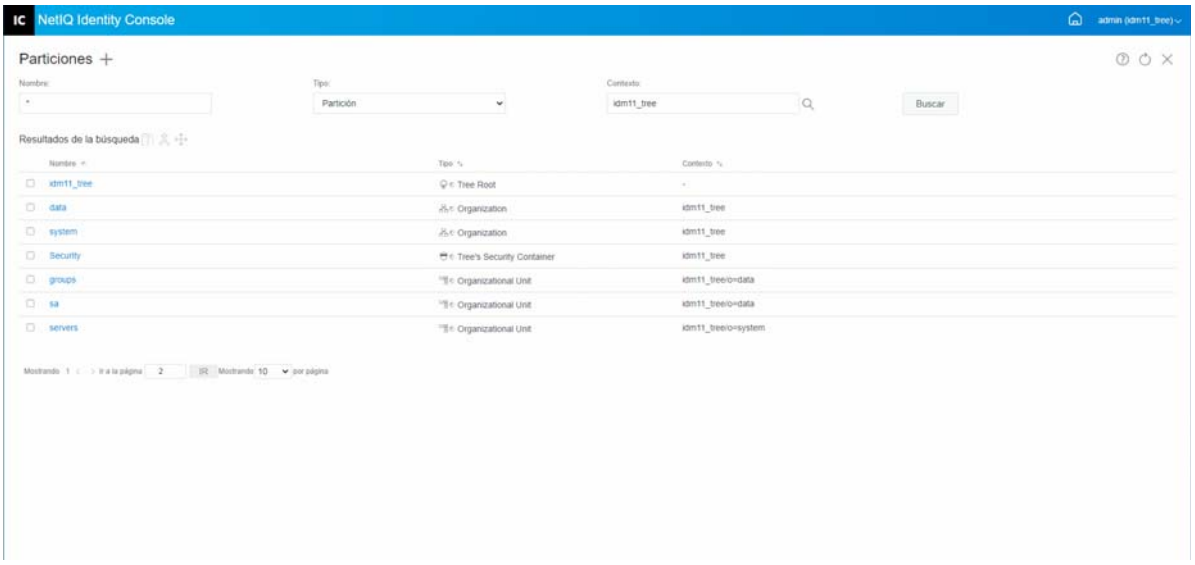
Fusionar particiones

Para fusionar particiones con su partición padre:

1. Haga clic en la opción **Gestión de particiones** de la página de destino de Identity Console.
2. Especifique el nombre, el tipo y el contexto de la partición o utilice la función de búsqueda para buscarla y, a continuación, haga clic en el botón 

.
3. Seleccione la partición en la lista de búsqueda, haga clic en el icono  y, a continuación, haga clic en **Aceptar**.
4. Aparece un mensaje de confirmación que indica que se ha fusionado la partición.

Figura 14-2 *Fusión de particiones*



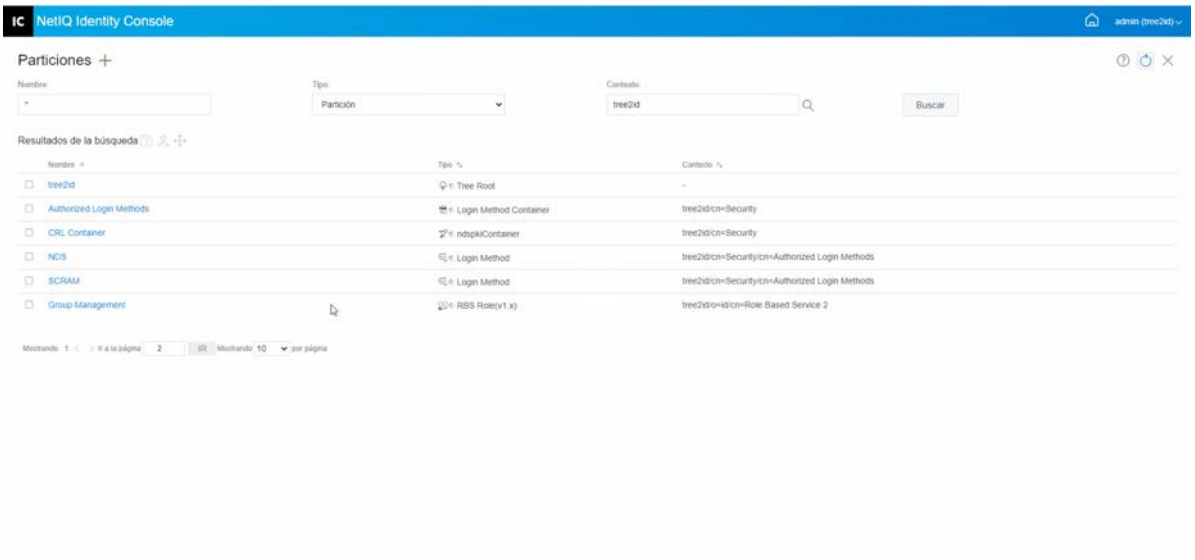
Modificación de particiones

Para modificar particiones:

1. Haga clic en la opción **Gestión de particiones** de la página de destino de Identity Console.
2. Especifique el nombre, el tipo y el contexto de la partición y, a continuación, haga clic en el botón Buscar.
3. Seleccione la partición en la lista de búsqueda y haga clic en el icono .
4. Haga clic en la opción **Editar** en **Filtro** para cambiar los filtros de réplica y sus correspondientes clases y atributos; a continuación, haga clic en **Aceptar**.

   Si se ha seleccionado **Servidor** en el campo **Tipo**, aparecerá una lista con todos los servidores. Al hacer clic en cada servidor, se mostrará una lista de todas las particiones del servidor.
5. Aparece un mensaje de confirmación que indica que se ha modificado la partición.

Figura 14-3 *Modificación de particiones*



Mover una partición

Mover una partición le permite mover un subárbol del árbol del directorio. Esto también se conoce como una operación de recortar e insertar. Sólo se pueden mover aquellas particiones que no tengan particiones subordinadas. Si existen particiones subordinadas, en primer lugar, debe fusionarlas antes de realizar la operación de movimiento.

Al mover una partición, eDirectory cambia todas las referencias al objeto Raíz de la partición. Aunque el nombre común del objeto no cambia, sí lo hace el nombre completo del contenedor (y el de todos sus subordinados).

Nota: Al mover una partición, hay que seguir las reglas de contención de eDirectory. Por ejemplo, no se puede mover una unidad administrativa directamente debajo de la raíz del árbol de directorios, ya que las reglas de contención de la raíz sólo permiten objetos de la localidad, del país o de la organización, pero no los de la unidad administrativa.

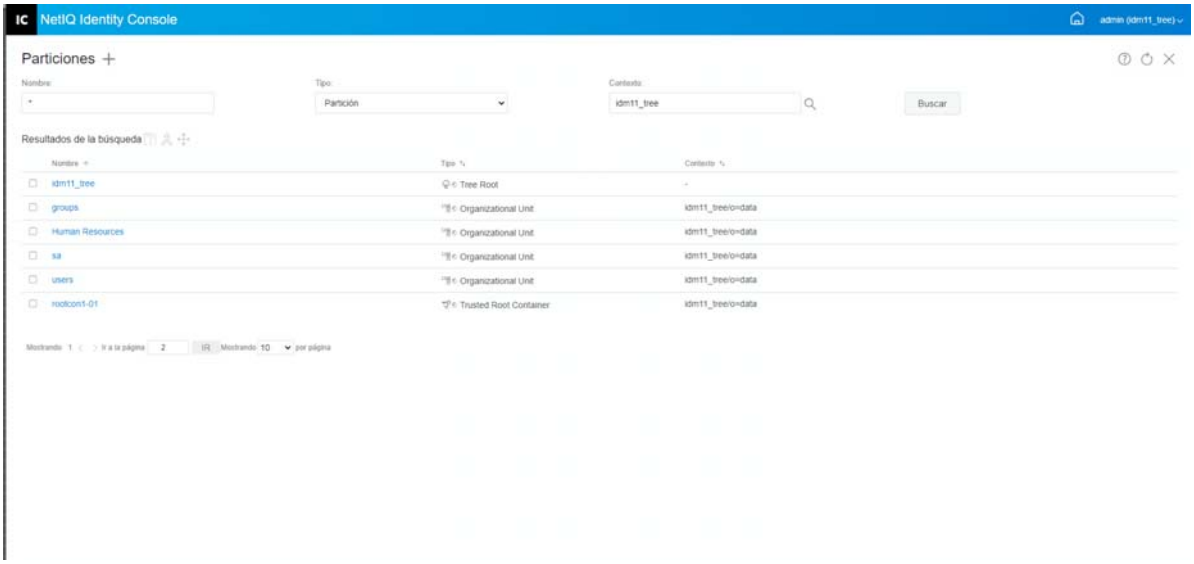
Para mover una partición:

1. Haga clic en la opción **Gestión de particiones** de la página de destino de Identity Console.
2. Especifique el nombre, el tipo y el contexto de la partición y, a continuación, haga clic en el botón Buscar.
3. Seleccione la partición en la lista de búsqueda y haga clic en el icono ✣.
4. Seleccione el objeto Contenedor de destino al que desea mover la partición especificada y haga clic en **Aceptar**.

Nota: La opción **Crear un alias en lugar de la partición movida** crea un puntero a la nueva ubicación de la partición. Esto permite que todas las operaciones que dependen de la ubicación anterior no se interrumpan hasta que se puedan actualizar para que reflejen la ubicación nueva. Los usuarios pueden seguir entrando a la red y buscar objetos en la ubicación original del directorio.

5 Aparece un mensaje de confirmación que indica que la operación de desplazamiento de la partición se ha realizado correctamente.

Figura 14-4 *Mover una partición*



15 Gestión de índices

Index Manager es un atributo del objeto Servidor que permite gestionar índices de la base de datos. eDirectory utiliza estos índices para mejorar significativamente los resultados de las consultas.

NetIQ eDirectory incluye un conjunto de índices que proporcionan funciones básicas de consulta. Estos índices por defecto son para los atributos siguientes.

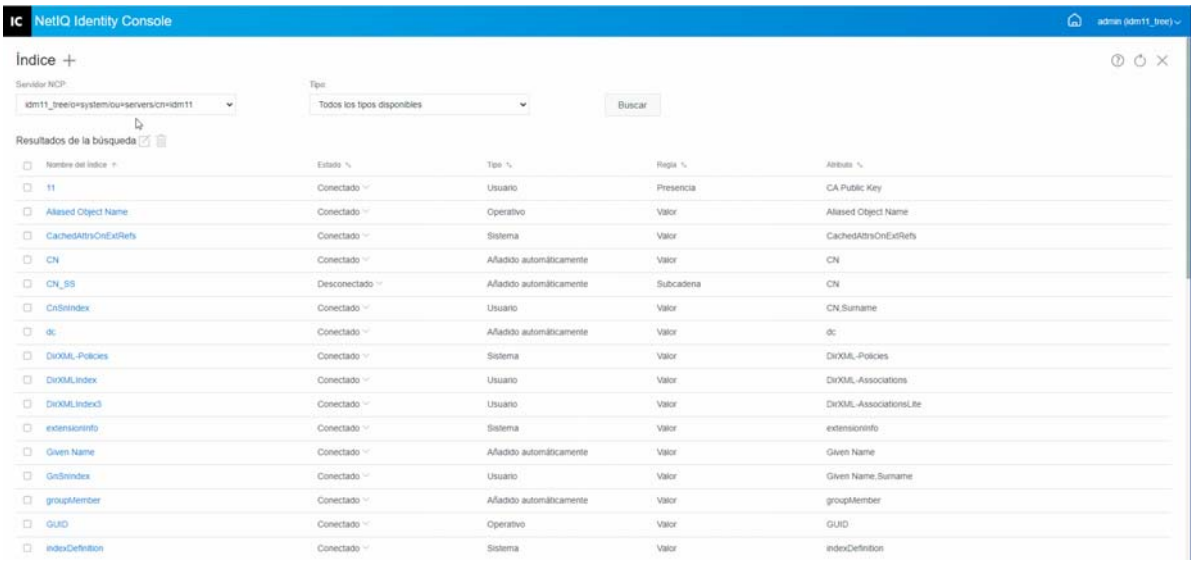
Las siguientes tareas se pueden realizar mediante el módulo Índice:

Creación de un índice

Para crear un nuevo índice:

1. Haga clic en la opción **Gestión de índices** de la página de destino de Identity Console.
2. Haga clic en el icono +.
3. Introduzca el nombre del índice.
4. Seleccione los servidores en la lista de servidores NCP disponibles.
5. Seleccione los atributos necesarios.
6. Seleccione la regla de índice:
   - 6a **Subcadena:** coincide con un subconjunto de la cadena de valores del atributo. Por ejemplo, una consulta para buscar un Apellido con "der" devolverá concordancias con Derington, Anderson y Lauder. La creación y el mantenimiento de un índice de subcadenas son las tareas que consumen más recursos del sistema.
   - 6b **Presencia:** requiere únicamente la presencia de un atributo en lugar de valores de atributo específicos. Una consulta para buscar todas las entradas con el atributo Guion de entrada utilizará un índice de presencia.
   - 6c **Valor:** coincide con todo el valor o con la primera parte del valor de un atributo. Por ejemplo, el valor de concordancia puede utilizarse para buscar entradas con el Apellido igual a "Jensen" y entradas que comiencen por "Jen".
7. Haga clic en el botón Crear.
8. Aparece un mensaje de confirmación que indica que se ha creado el índice.

Figura 15-1 *Creación de un índice nuevo*

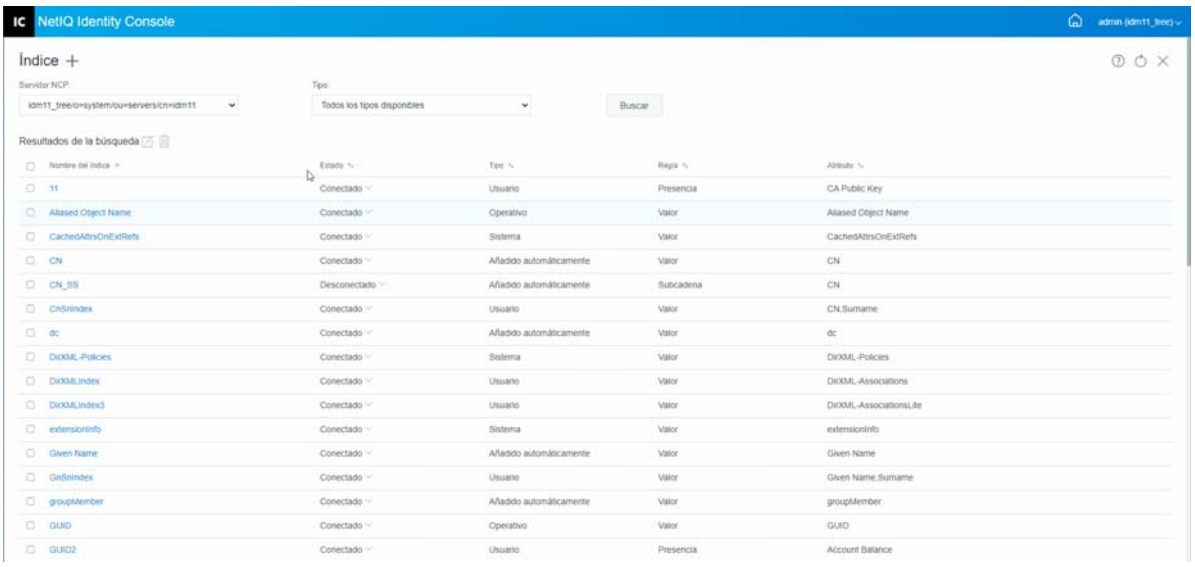


Supresión de un índice

Para suprimir un índice:

1. Haga clic en la opción **Gestión de índices** de la página de destino de Identity Console.
2. Seleccione el servidor NCP y el tipo de índice y, a continuación, haga clic en el botón Buscar.
3. Seleccione el índice en la lista de búsqueda y haga clic en el icono 🗑.
4. Aparece un mensaje de confirmación que indica que se ha suprimido el índice.

Figura 15-2 *Supresión de un índice*



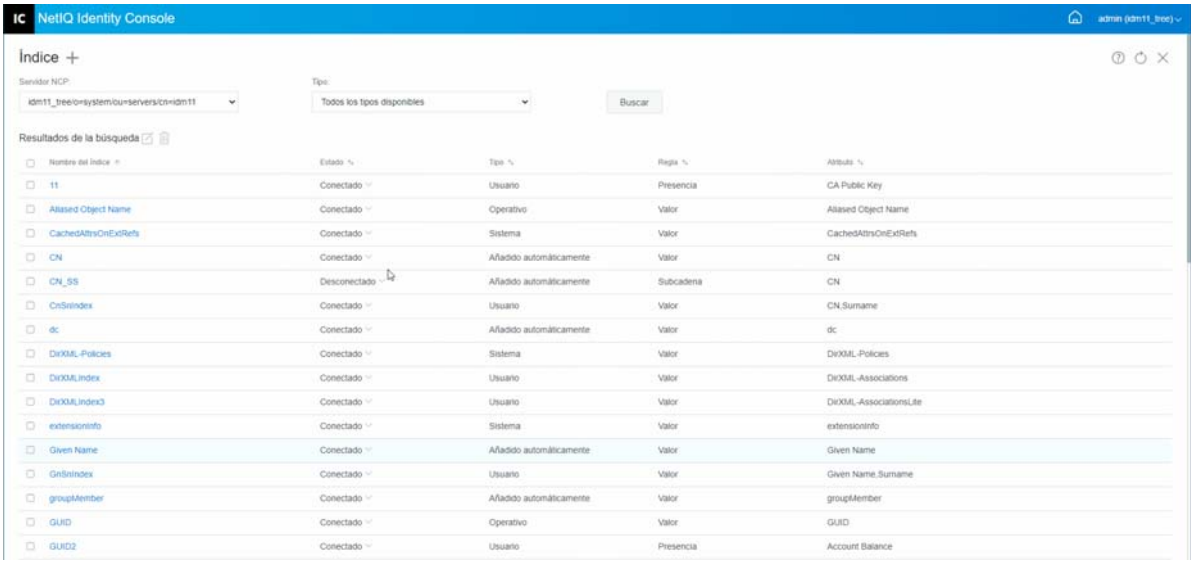
Copiar un índice

Si ha descubierto que un índice específico es útil en un servidor y cree que puede necesitar este índice en otro servidor, puede copiar la definición de índice de un servidor a otro. Al revisar los datos del predicado, también puede encontrar el caso contrario: un índice que satisfacía una necesidad de varios servidores ya no es útil en uno de estos servidores. En ese caso, podría suprimir el índice del servidor que no se beneficia del índice.

Para copiar un índice:

1. Haga clic en la opción **Gestión de índices** de la página de destino de Identity Console.
2. Seleccione el servidor NCP y el tipo de índice y, a continuación, haga clic en el botón Buscar.
3. Seleccione el índice en la lista de búsqueda y haga clic en el icono .
4. Seleccione los servidores NCP en los que desea copiar el índice y haga clic en el botón Guardar.
5. Aparece un mensaje de confirmación que indica que se ha modificado el índice.

Figura 15-3 *Copiar un índice*



Cambio del estado de un índice

Durante las horas de mayor actividad, puede que desee desconectar temporalmente los índices para ajustar el rendimiento. Por ejemplo, para conseguir una velocidad de carga masiva adicional, es posible que desee suspender todos los índices definidos por el usuario. Como cada adición o

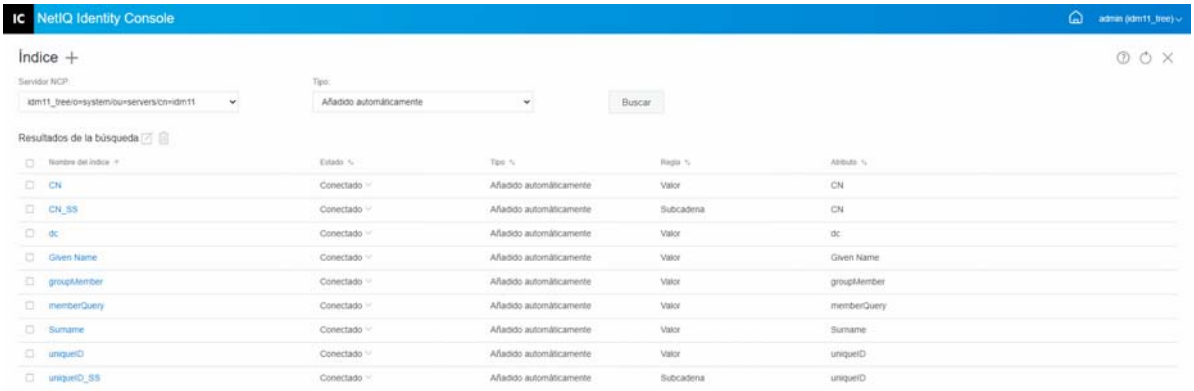
modificación de objetos requiere la actualización de índices definidos, tener todos los índices activos puede ralentizar la carga masiva de datos. Una vez completada la carga masiva, los índices se pueden volver a establecer en línea.

Para desconectar un índice:

1. Haga clic en la opción **Gestión de índices** de la página de destino de Identity Console.
2. Seleccione el servidor NCP y el tipo de índice y, a continuación, haga clic en el botón Buscar.
3. Haga clic en la lista desplegable de **Estado** de la lista de índices. Un índice puede tener los siguientes estados:
   - **En línea:** en ejecución.
   - **Desconectado:** suspendido. El índice se puede volver a iniciar.

Nota: No se pueden cambiar los índices de tipo Sistema y Operativo. Estos índices tampoco se pueden suprimir.

Figura 15-4 *Desconexión de un índice*



16 Configuración de objetos LDAP

La instalación de eDirectory crea un objeto Servidor LDAP y un objeto Grupo LDAP. La configuración por defecto de los servicios LDAP se encuentra en el directorio de estos dos objetos. Puede modificar la configuración por defecto mediante la tarea Gestión de LDAP de Identity Console.

El objeto Servidor LDAP representa los datos de configuración específicos del servidor. Sin embargo, el objeto Grupo LDAP contiene información de configuración que puede compartirse cómodamente entre varios servidores LDAP. Este objeto proporciona datos de configuración comunes y representa un grupo de servidores LDAP. Los servidores tienen datos comunes.

Puede asociar varios objetos Servidor LDAP a un objeto Grupo LDAP. A continuación, todos los servidores LDAP asociados obtienen la configuración específica del servidor del objeto Servidor LDAP, aunque obtienen información común o compartida del objeto Grupo LDAP.

Mediante el módulo LDAP, se pueden realizar las siguientes tareas:

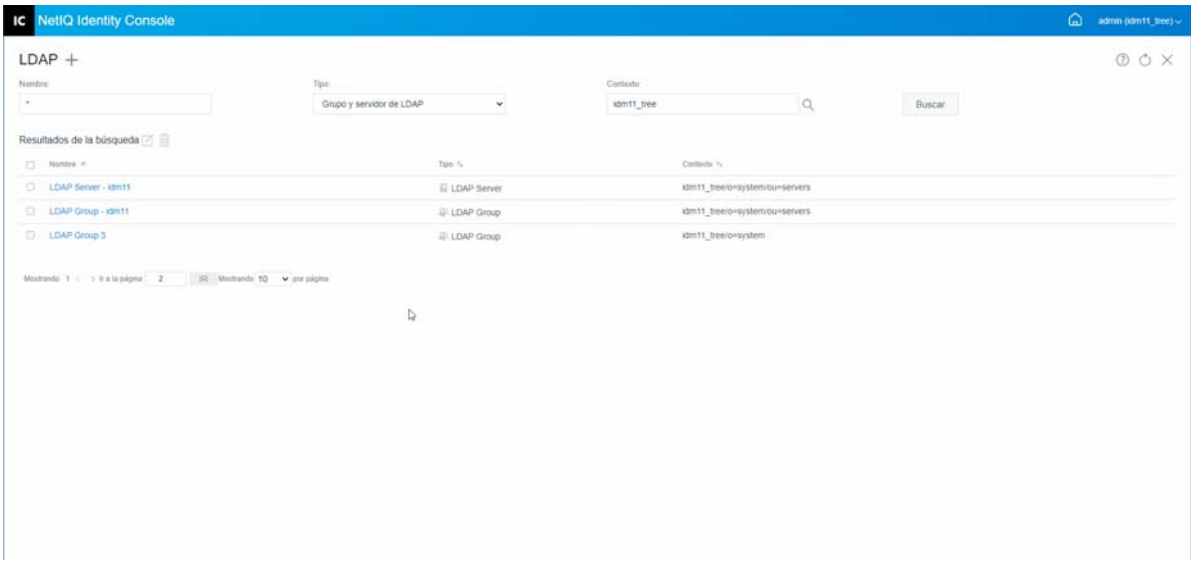
- "Creación de objetos LDAP" en la página 89
- "Supresión de objetos LDAP" en la página 90
- "Modificación de objetos LDAP" en la página 91

Creación de objetos LDAP

Para crear un nuevo objeto LDAP:

1. Haga clic en la opción **Configuración de LDAP** de la página de destino de Identity Console.
2. Haga clic en el icono  .
3. En la página Crear objeto LDAP, especifique el nombre, el tipo y el contexto, o bien utilice el icono  de contexto de búsqueda y, a continuación, haga clic en **Crear**.
4. Aparece un mensaje de confirmación que indica que se ha creado el objeto LDAP.

Figura 16-1 *Creación de un nuevo objeto LDAP*

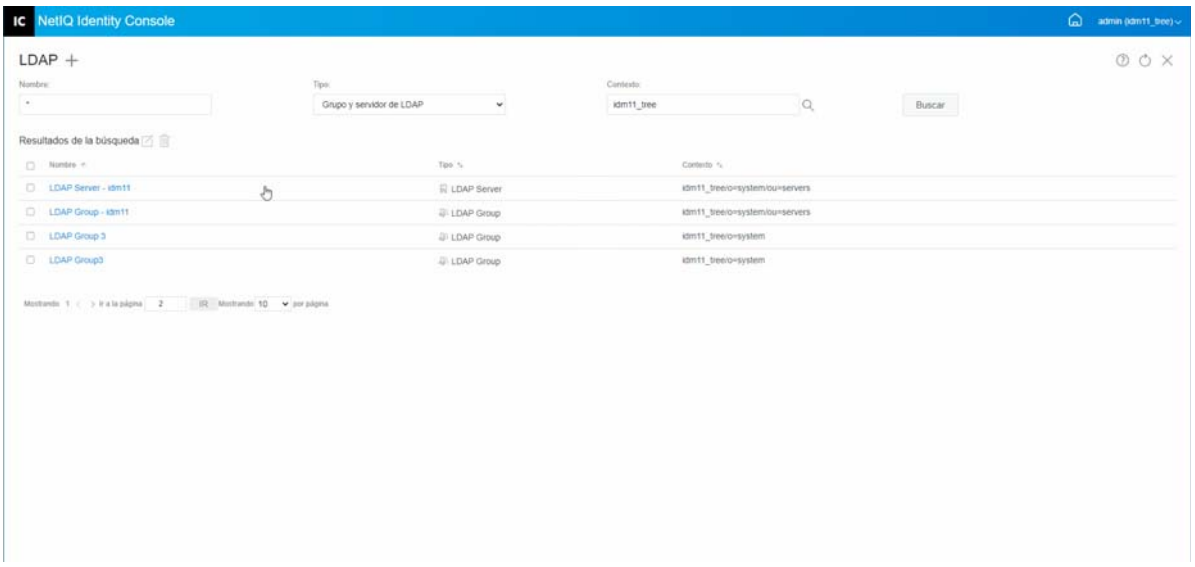


Supresión de objetos LDAP

Para suprimir objetos LDAP:

1. Haga clic en la opción **Configuración de LDAP** de la página de destino de Identity Console.
2. Especifique el nombre, el tipo y el contexto del objeto LDAP y, a continuación, haga clic en el botón Buscar.
3. Seleccione los objetos LDAP en la lista de búsqueda y haga clic en el icono 🗑.
4. Aparece un mensaje de confirmación que indica que se han modificado los objetos LDAP.

Figura 16-2 *Supresión de objetos LDAP*

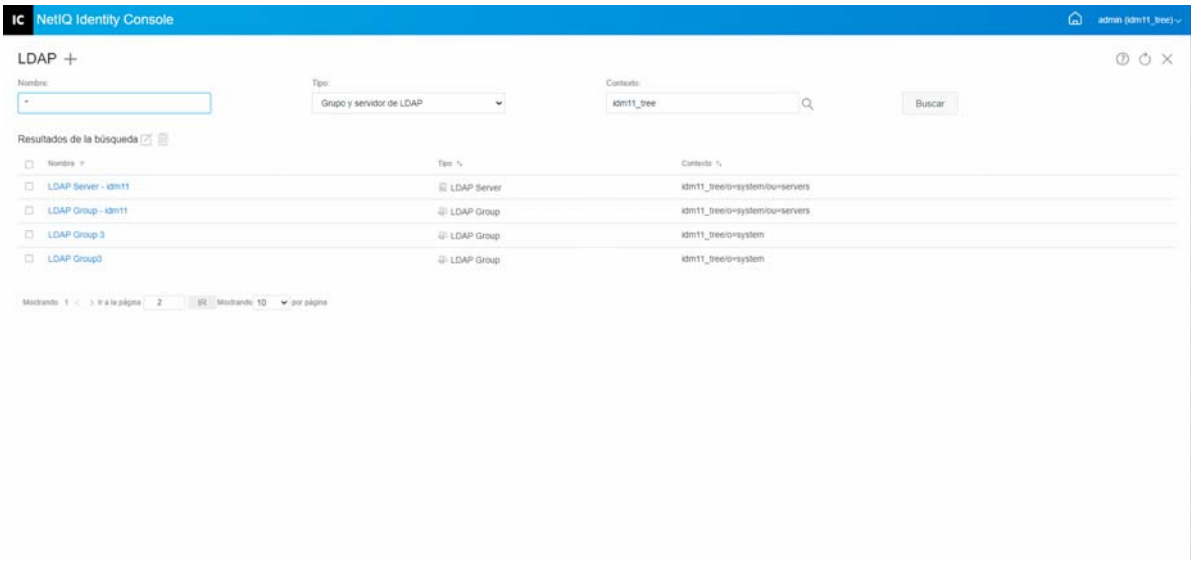


Modificación de objetos LDAP

Para modificar objetos LDAP:

1. Haga clic en la opción **Configuración de LDAP** de la página de destino de Identity Console.
2. Escriba el nombre, el tipo y el contexto del objeto LDAP y, a continuación, haga clic en el botón Buscar.
3. Seleccione el objeto LDAP en la lista de búsqueda y haga clic en el icono .
4. Modifique los atributos y la información del objeto LDAP específico según sea necesario y haga clic en el botón Guardar. Para obtener más información sobre los atributos de los objetos LDAP, consulte Configuring LDAP Server and LDAP Group Objects on Linux (Configuración de los objetos Servidor LDAP y Grupo LDAP en Linux) de *NetIQ eDirectory Administration Guide* (Guía de administración de NetIQ eDirectory).
5. Aparece un mensaje de confirmación que indica que se ha modificado el objeto LDAP.

Figura 16-3 *Modificación de objetos LDAP*



17 Gestión de certificados

El Servidor de certificados de NetIQ se instala automáticamente al instalar eDirectory. El Servidor de certificados de ofrece servicios de cifrado de clave pública, integrados originalmente en eDirectory, que permiten elaborar, emitir y gestionar tanto certificados de servidor como de usuario. Estos servicios permiten la protección de transmisiones de datos confidenciales por canales de comunicaciones públicos como el Internet.

Nota: Si desea utilizar el módulo Gestión de certificados con Identity Console, debe actualizar el servidor de eDirectory a 9.2.4 HF2.

Identity Console proporciona las siguientes tareas de gestión de certificados:

- "Gestión de la autoridad certificadora" en la página 93
- "Gestión de certificados de servidor" en la página 97
- "Gestión de certificados de usuario" en la página 100
- "Gestión de contenedores raíz de confianza" en la página 102
- "Creación de objetos Certificado de servidor por defecto" en la página 104
- "Emisión de un certificado de clave pública" en la página 106
- "Gestión de un objeto SAS Service" en la página 109

Gestión de la autoridad certificadora

Por defecto, el proceso de instalación del Servidor de certificados de NetIQ crea automáticamente la autoridad certificadora (CA) administrativa. Se le pedirá que especifique un nombre de CA administrativa. Al hacer clic en Finalizar, se crea la CA administrativa con los parámetros por defecto y se incluye en el contenedor Seguridad. Si desea tener más control sobre la creación de la CA administrativa, puede crearla manualmente mediante el portal de Identity Console. Además, si suprime la CA administrativa, deberá volver a crearla.

Mediante el módulo Autoridad certificadora, puede realizar las siguientes tareas:

- "Creación de un objeto CA administrativa" en la página 94
- "Copia de seguridad de certificados de CA administrativa" en la página 94
- "Restauración de una CA administrativa" en la página 95
- "Validación de certificados de la CA administrativa" en la página 95
- "Sustitución de los certificados de la CA administrativa" en la página 96
- "Revocación de certificados de la CA administrativa" en la página 96

Creación de un objeto CA administrativa

Para crear un objeto CA administrativa, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de CA** de la página de destino de Identity Console.
2. Si no existe ningún objeto Autoridad certificadora administrativa, se abrirá el recuadro de diálogo Crear un objeto Autoridad certificadora administrativa y el asistente correspondiente que crea el objeto. Siga las indicaciones para crear el objeto.

   Nota: Asegúrese de que la vía del archivo CRL que se especifique aquí hace referencia a la vía de instalación de eDirectory.
3. Cuando haya terminado de crear la autoridad certificadora, es recomendable realizar una copia de seguridad del par de claves pública/privada de la CA y almacenarla en un lugar seguro. Para obtener más información, consulte "Copia de seguridad de certificados de CA administrativa" en la página 94.

Copia de seguridad de certificados de CA administrativa

Es recomendable realizar una copia de seguridad de los certificados y la clave privada de la CA administrativa por si el servidor host de la CA administrativa presenta un error irrecuperable. Si se produce un fallo, puede utilizar el archivo de copia de seguridad para restaurar la CA administrativa en cualquier servidor del árbol.

Nota: La capacidad de realizar una copia de seguridad de una CA administrativa solo está disponible para las CA administrativas creadas a partir de la versión 9.0 del Servidor de certificados. En versiones anteriores del Servidor de certificados, la clave privada de la CA administrativa se creaba de forma que era imposible exportarla.

El archivo de copia de seguridad contiene la clave privada de la CA, el certificado autofirmado, el certificado de clave pública y otros certificados necesarios para que funcione. Esta información se almacena en formato PKCS #12 (también conocido como PFX).

Se debe realizar una copia de seguridad de la CA administrativa cuando funcione correctamente.

Para realizar una copia de seguridad de la CA administrativa, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de CA** de la página de destino de Identity Console.
2. Haga clic en la pestaña **Certificados**.
3. Seleccione **Self Signed Certificate** (Certificado autofirmado) o **Public Key Certificate** (Certificado de clave pública). Ambos certificados se escriben en el archivo durante la operación de copia de seguridad. Es recomendable que seleccione por separado el certificado autofirmado para los certificados RSA y ECDSA.
4. Haga clic en el icono  .

5 Opte por exportar la clave privada, especifique una contraseña con seis o más caracteres alfanuméricos para utilizarla en el cifrado del archivo PFX y seleccione PKCS12 como formato de exportación. A continuación, haga clic en **Aceptar**.

6 El archivo de copia de seguridad cifrado se escribe en la ubicación especificada. Ya está listo para almacenarse en una ubicación segura a fin de utilizarlo en caso de emergencia.

Restauración de una CA administrativa

Si el objeto CA administrativa se ha suprimido o está dañado o si el servidor host de la CA administrativa ha sufrido un error irrecuperable, la CA administrativa se puede restaurar para que presente un funcionamiento completo mediante el archivo de copia de seguridad, como se describe en "Copia de seguridad de certificados de CA administrativa" en la página 94.

Para restaurar la CA administrativa, realice los siguientes pasos:

1 Haga clic en las opciones **Gestión de certificados** > **Gestión de CA** de la página de destino de Identity Console.

2 Haga clic en ↑↓ en la parte superior de la pantalla (junto a **Gestión de la autoridad certificadora**) para suprimir la CA administrativa existente.

3 A continuación, se le solicitará que configure una nueva CA administrativa. Se abrirán el recuadro de diálogo Crear un objeto Autoridad certificadora administrativa y el asistente correspondiente que crea el objeto.

4 En el recuadro de diálogo de creación, especifique el servidor que debe alojar la CA administrativa y el nombre del objeto CA administrativa.

5 Seleccione **Importar**.

6 Seleccione los certificados RSA y ECDSA. El Servidor de certificados requiere que ambos certificados tengan el mismo nombre de sujeto. Sin embargo, el Servidor de certificados no admite la importación de certificados de CA autofirmados externos. No obstante, permite importar certificados de CA subordinados.

7 En las pantallas siguientes, busque y seleccione el nombre del archivo para RSA y ECDSA.

8 Introduzca la contraseña utilizada para cifrar el archivo cuando se realizó la copia de seguridad y haga clic en **Aceptar**.

9 Ya se han restaurado la clave privada y los certificados de la CA administrativa, que está completamente funcional. El archivo se puede volver a almacenar ahora para utilizarlo en el futuro.

Validación de certificados de la CA administrativa

Si sospecha que existe un problema con un certificado o cree que ya no es válido, puede validarlo fácilmente mediante Identity Console. Se puede validar cualquier certificado del árbol de eDirectory, incluidos los certificados emitidos por CA externas.

El proceso de validación de certificados incluye varias comprobaciones de los datos del certificado, así como de los datos de la cadena de certificados. Una cadena de certificados está formada por un certificado de CA raíz y, de forma opcional, por los certificados de una o varias CA intermedias.

Para validar un certificado:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de CA** de la página de destino de Identity Console.
2. Haga clic en la pestaña **Certificados**.
3. Seleccione **Self Signed Certificate** (Certificado autofirmado) o **Public Key Certificate** (Certificado de clave pública).
4. Haga clic en  para validar los certificados de CA seleccionados.

Sustitución de los certificados de la CA administrativa

Si los certificados están dañados o no son válidos por algún motivo o si solo desea sustituir los certificados existentes, realice los siguientes pasos:

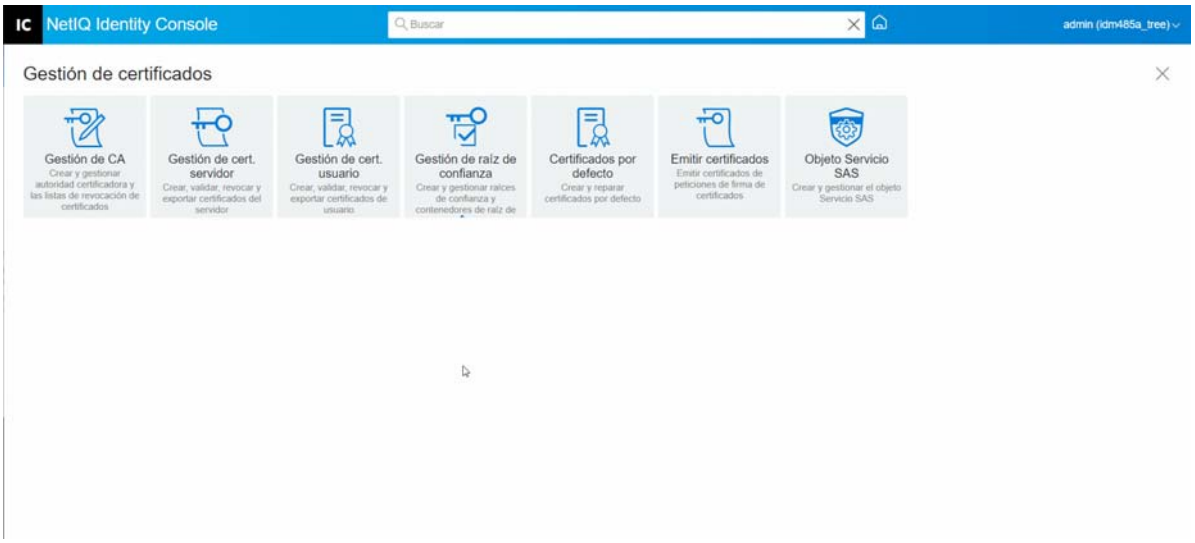
1. Haga clic en las opciones **Gestión de certificados** > **Gestión de CA** de la página de destino de Identity Console.
2. Haga clic en la pestaña **Certificados**.
3. Seleccione **Self Signed Certificate** (Certificado autofirmado) o **Public Key Certificate** (Certificado de clave pública).
4. Haga clic en  para reemplazar el certificado de CA seleccionado.
5. Importe un certificado de CA con el formato `.pfx` o `.p12` y especifique una contraseña para cifrar la clave privada.
6. Haga clic en **Aceptar**.

Revocación de certificados de la CA administrativa

Para revocar un certificado:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de CA** de la página de destino de Identity Console.
2. Haga clic en la pestaña **Certificados**.
3. Seleccione **Self Signed Certificate** (Certificado autofirmado) o **Public Key Certificate** (Certificado de clave pública).
4. Haga clic en el icono  .
5. Lea y entienda el riesgo que implica revocar certificados de servidor.
6. Seleccione un motivo válido para la revocación en la lista desplegable, elija la fecha de invalidez y especifique cualquier otro comentario.
7. Haga clic en **Aceptar** para finalizar la revocación.

Figura 17-1 *Gestión de la autoridad certificadora*



Gestión de certificados de servidor

Mediante el módulo Gestión de cert. servidor, el administrador puede realizar las siguientes tareas:

- "Creación de objetos Certificado de servidor" en la página 97
- "Exportación de objetos Certificado de servidor" en la página 98
- "Validación de objetos Certificado de servidor" en la página 98
- "Sustitución de un objeto Certificado de servidor" en la página 98
- "Revocación de objetos Certificado de servidor" en la página 99
- "Supresión de objetos Certificado de servidor" en la página 99

Creación de objetos Certificado de servidor

Para crear un objeto Certificado de servidor, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. servidor** de la página de destino de Identity Console.
2. Haga clic en el icono +.
3. En la página **Crear certificado de servidor**, especifique un **apodo** y un servidor; a continuación, seleccione una de las siguientes opciones:
   - **Estándar (parámetros por defecto):** permite crear un objeto Certificado de servidor por defecto de tipo RSA o ECDSA.
   - **Personalizado (El usuario especifica los parámetros):** permite especificar los parámetros personalizados del objeto Certificado de servidor.
   - **Importar (permite que un archivo PKCS12 proporcione las claves y certificados):** permite importar un archivo PKCS12 con el formato `.pfx` o `.p12`.

4 Después de especificar los parámetros, haga clic en **Siguiente** para revisar el resumen del certificado.

5 En la pantalla **Resumen**, haga clic en **Aceptar** para crear un objeto Certificado de servidor.

Exportación de objetos Certificado de servidor

Para exportar objetos Certificado de servidor, realice los siguientes pasos:

1 Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. servidor** de la página de destino de Identity Console.

2 Seleccione el servidor adecuado en la lista desplegable.

3 Seleccione el certificado de servidor adecuado en la lista y haga clic en el icono  .

4 En la siguiente pantalla, seleccione la casilla de verificación **Exportar clave privada** y especifique una contraseña para proteger la clave privada. Confirme la contraseña y seleccione el formato de exportación.

Nota: Los certificados de servidor solo se pueden exportar con el formato PKCS12.

---

5 Haga clic en **Aceptar** para exportar el objeto Certificado de servidor.

Validación de objetos Certificado de servidor

Para validar un objeto Certificado de servidor, realice los siguientes pasos:

1 Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. servidor** de la página de destino de Identity Console.

2 Seleccione el servidor adecuado en la lista desplegable.

3 Seleccione el certificado de servidor adecuado en la lista y haga clic en el icono  .

4 Aparece un mensaje de confirmación que indica que la validación del objeto Certificado de servidor se ha realizado correctamente.

Sustitución de un objeto Certificado de servidor

Si los certificados de servidor están dañados o no son válidos por algún motivo o si solo desea sustituir los certificados por defecto existentes, realice los siguientes pasos:

1 Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. servidor** de la página de destino de Identity Console.

2 Seleccione el servidor adecuado en la lista desplegable.

3 Seleccione el certificado de servidor adecuado en la lista y haga clic en el icono  .

4 Lea y entienda el riesgo que implica la sustitución de certificados de servidor y haga clic en **Aceptar**.

5 En la pantalla siguiente, busque y seleccione el nuevo certificado de servidor con formato `.pfx` o `.p12` y especifique una contraseña.

6 Haga clic en **Aceptar** para sustituir el certificado de servidor.

Revocación de objetos Certificado de servidor

Para revocar un objeto Certificado de servidor, realice los siguientes pasos:

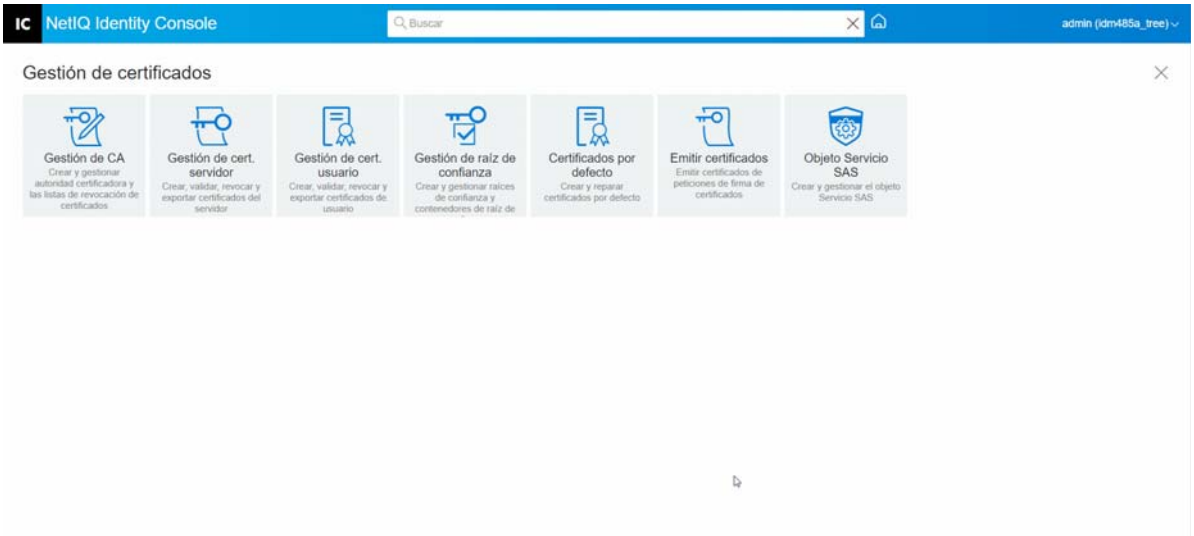
1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. servidor** de la página de destino de Identity Console.
2. Seleccione el servidor adecuado en la lista desplegable.
3. Seleccione el certificado de servidor adecuado en la lista y haga clic en el icono ⊘.
4. Lea y entienda el riesgo que implica revocar certificados de servidor y haga clic en **Aceptar**.
5. En la siguiente pantalla, seleccione un motivo válido para la revocación en la lista desplegable, elija la fecha de invalidez y especifique cualquier otro comentario.
6. Haga clic en **Aceptar** para finalizar la revocación.

Supresión de objetos Certificado de servidor

Para eliminar objetos Certificado de servidor, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. servidor** de la página de destino de Identity Console.
2. Seleccione el servidor adecuado en la lista desplegable.
3. Seleccione el certificado de servidor adecuado en la lista y haga clic en el icono 🗑.
4. En la siguiente pantalla, haga clic en **Aceptar**.
5. Aparece un mensaje de confirmación que indica que el objeto Certificado de servidor se ha suprimido correctamente.

Figura 17-2 *Gestión de certificados de servidor*



Gestión de certificados de usuario

Mediante el módulo Gestión de certificados de usuario, puede realizar la siguiente tarea:

Creación de objetos Certificado de usuario

Para crear un objeto Certificado de usuario, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. usuario** de la página de destino de Identity Console.
2. Haga clic en el icono +.
3. En la página **Crear certificado de usuario**, especifique un **apodo** y un servidor; a continuación, seleccione una de las siguientes opciones:
   - **Estándar (parámetros por defecto):** permite crear un objeto Certificado de usuario por defecto de tipo RSA o ECDSA.
   - **Personalizado (El usuario especifica los parámetros):** permite especificar los parámetros personalizados del objeto Certificado de usuario.
   - **Importar:** permite importar un archivo de certificado con el formato CERT o PKCS12.
4. Después de especificar los parámetros, haga clic en **Siguiente** para revisar el resumen del certificado.
5. En la pantalla **Resumen**, haga clic en **Aceptar** para crear un objeto Certificado de usuario.

Exportación de objetos Certificado de usuario

Para exportar objetos Certificado de usuario, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. usuario** de la página de destino de Identity Console.
2. Seleccione el servidor adecuado en la lista desplegable.
3. Seleccione el certificado de usuario adecuado en la lista y haga clic en el icono .
4. En la siguiente pantalla, seleccione la casilla de verificación **Exportar clave privada** y especifique una contraseña para proteger la clave privada. Confirme la contraseña y seleccione el formato de exportación.

   Nota: Los certificados de usuario solo se pueden exportar con el formato PKCS12.

5. Haga clic en **Aceptar** para exportar el objeto Certificado de usuario.

Validación de objetos Certificado de usuario

Para validar un objeto Certificado de usuario, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. usuario** de la página de destino de Identity Console.
2. Seleccione el servidor adecuado en la lista desplegable.
3. Seleccione el certificado de usuario adecuado en la lista y haga clic en el icono .
4. Aparece un mensaje de confirmación que indica que la validación del objeto Certificado de usuario se ha realizado correctamente.

Revocación de objetos Certificado de usuario

Para revocar un objeto Certificado de usuario, realice los siguientes pasos:

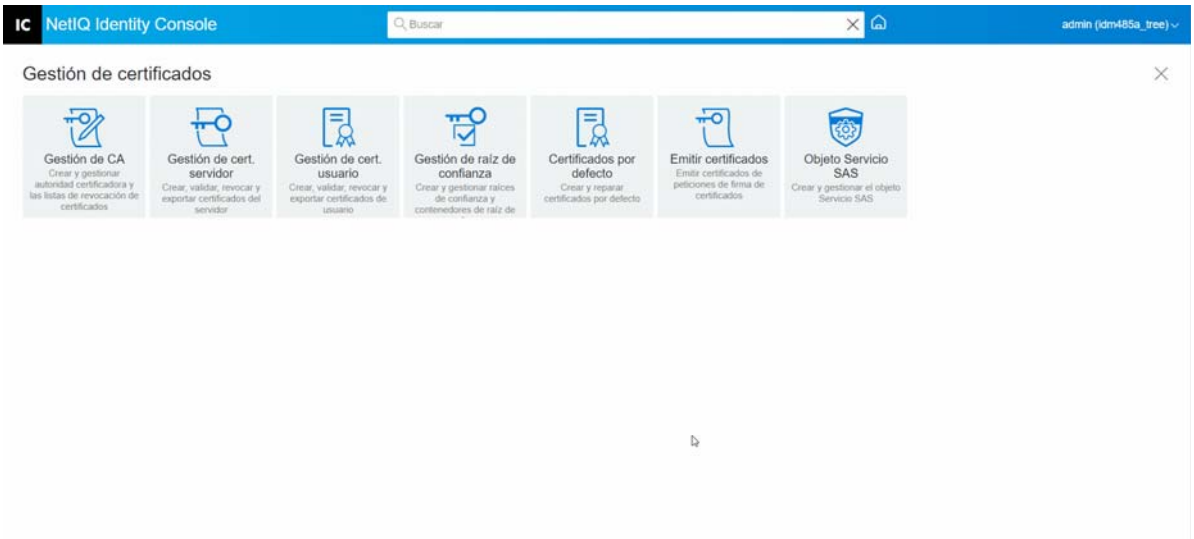
1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. usuario** de la página de destino de Identity Console.
2. Seleccione el servidor adecuado en la lista desplegable.
3. Seleccione el certificado de usuario adecuado en la lista y haga clic en el icono .
4. Lea y entienda el riesgo que implica revocar certificados de usuario.
5. Seleccione un motivo válido para la revocación en la lista desplegable, elija la fecha de invalidez y especifique cualquier otro comentario.
6. Haga clic en **Aceptar** para finalizar la revocación.

Supresión de objetos Certificado de usuario

Para eliminar objetos Certificado de usuario, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de cert. usuario** de la página de destino de Identity Console.
2. Seleccione el servidor adecuado en la lista desplegable.
3. Seleccione el certificado de usuario adecuado en la lista y haga clic en el icono .
4. En la siguiente pantalla, haga clic en **Aceptar**.
5. Aparece un mensaje de confirmación que indica que el objeto Certificado de usuario se ha eliminado correctamente.

Figura 17-3 *Gestión de certificados de usuario*



Gestión de contenedores raíz de confianza

Una raíz de confianza proporciona la base para confiar en el cifrado de clave pública. Las raíces de confianza permiten validar certificados firmados por otras CA. Las raíces de confianza ofrecen seguridad para SSL, correo electrónico seguro y autenticación basada en certificados.

Mediante el módulo Gestión de raíz de confianza, puede realizar las siguientes tareas:

- “Creación de un contenedor raíz de confianza” en la página 102
- “Creación de un objeto Certificado raíz de confianza” en la página 103
- “Exportación de objetos Certificado raíz de confianza” en la página 103
- “Validación de objetos Certificado raíz de confianza” en la página 103
- “Supresión de objetos Certificado raíz de confianza” en la página 104
- “Supresión de contenedores raíz de confianza” en la página 104

Creación de un contenedor raíz de confianza

Para crear un contenedor raíz de confianza, realice las siguientes tareas:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de raíz de confianza** de la página de destino de Identity Console. La casilla de verificación **Contenedor raíz de confianza** se seleccionará por defecto.
2. Haga clic en el icono + para crear un nuevo contenedor raíz de confianza.
3. Especifique un nombre para el contenedor raíz de confianza.
4. Utilice el selector de objetos para buscar el contenedor adecuado.
5. Haga clic en el botón **Aceptar**.
6. Aparece un mensaje de confirmación que indica que el contenedor raíz de confianza se ha creado correctamente.

Creación de un objeto Certificado raíz de confianza

Para crear un objeto Raíz de confianza, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de raíz de confianza** de la página de destino de Identity Console. La casilla de verificación **Contenedor raíz de confianza** se seleccionará por defecto. Seleccione la casilla de verificación **Raíz de confianza**.
2. Haga clic en el icono + para crear un nuevo objeto Raíz de confianza.
3. Especifique un nombre para el objeto Raíz de confianza.
4. Seleccione el contenedor raíz de confianza adecuado en la lista desplegable.
5. Busque y seleccione el archivo de certificado adecuado con el formato `.der` o `.b64`.

   Nota: Cualquier tipo de certificado se puede almacenar en un objeto Raíz de confianza (certificados de CA, certificados de CA intermedia o certificados de usuario).
6. Haga clic en el botón **Aceptar**.
7. Aparece un mensaje de confirmación que indica que el objeto Raíz de confianza se ha creado correctamente.

Exportación de objetos Certificado raíz de confianza

Para exportar objetos Certificado raíz de confianza, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de raíz de confianza** de la página de destino de Identity Console. La casilla de verificación **Contenedor raíz de confianza** se seleccionará por defecto. Seleccione la casilla de verificación **Raíz de confianza**.
2. Seleccione el certificado raíz de confianza adecuado en la lista y haga clic en el icono .
3. En la siguiente pantalla, seleccione la casilla de verificación **Exportar clave privada** y especifique una contraseña para proteger la clave privada. Confirme la contraseña y seleccione el formato de exportación.

   Nota: Los certificados raíz de confianza solo se pueden exportar con los formatos DER o BASE64.
4. Haga clic en **Aceptar** para exportar el objeto Certificado raíz de confianza.

Validación de objetos Certificado raíz de confianza

Para validar los objetos Certificado raíz de confianza, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de raíz de confianza** de la página de destino de Identity Console. La casilla de verificación **Contenedor raíz de confianza** se seleccionará por defecto. Seleccione la casilla de verificación **Raíz de confianza**.
2. Seleccione el certificado raíz de confianza adecuado en la lista y haga clic en el icono .
3. Aparece un mensaje de confirmación que indica que la validación del objeto Certificado raíz de confianza se ha realizado correctamente.

Supresión de objetos Certificado raíz de confianza

Para eliminar objetos Certificado raíz de confianza, realice los siguientes pasos:

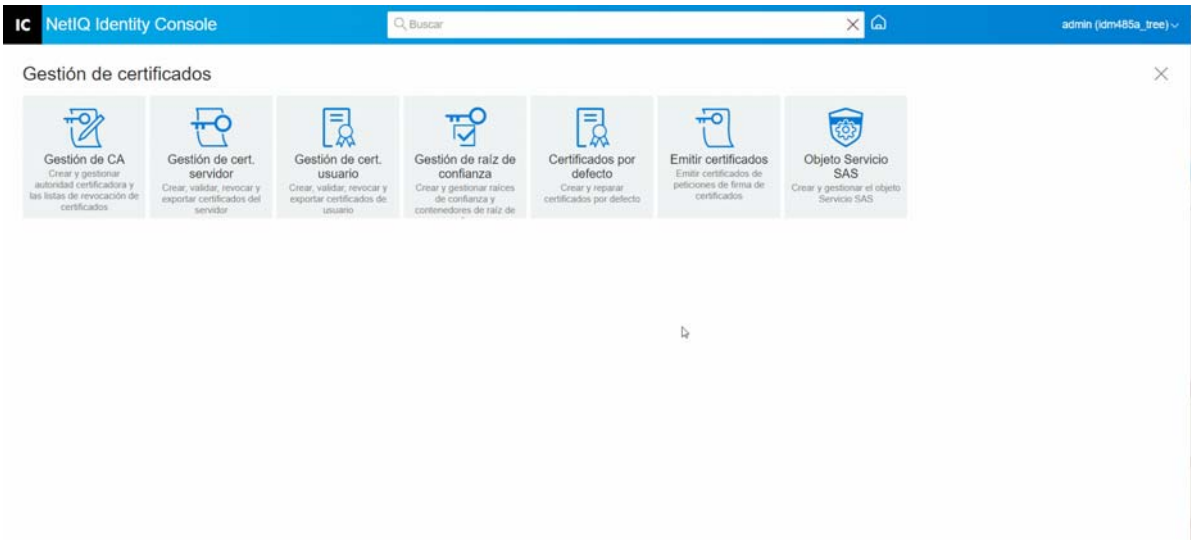
1. Haga clic en las opciones **Gestión de certificados** > **Gestión de raíz de confianza** de la página de destino de Identity Console. La casilla de verificación **Contenedor raíz de confianza** se seleccionará por defecto. Seleccione la casilla de verificación **Raíz de confianza**.
2. Seleccione el certificado raíz de confianza adecuado en la lista y haga clic en el icono .
3. Haga clic en **Aceptar** en la ventana de advertencia.
4. Aparece un mensaje de confirmación que indica que el objeto Certificado raíz de confianza se ha eliminado correctamente.

Supresión de contenedores raíz de confianza

Para eliminar un contenedor raíz de confianza, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Gestión de raíz de confianza** de la página de destino de Identity Console. La casilla de verificación **Contenedor raíz de confianza** se seleccionará por defecto.
2. Seleccione el contenedor raíz de confianza adecuado en la lista y haga clic en el icono .
3. Haga clic en **Aceptar** en la ventana de advertencia.
4. Aparece un mensaje de confirmación que indica que el objeto Contenedor raíz de confianza se ha eliminado correctamente.

Figura 17-4 *Gestión de contenedores raíz de confianza*



Creación de objetos Certificado de servidor por defecto

La instalación del Servidor de certificados crea objetos Certificado de servidor por defecto.

- SSL CertificateDNS - *nombre_del_servidor*

- Un certificado para cada dirección IP configurada en el servidor (IPAG*xxx.xxx.xxx.xxx* - *nombre_del_servidor*)
- Un certificado para cada nombre DNS configurado en el servidor (DNSAG*www.example.com* - *nombre_del_servidor*)

Nota: eDirectory no crea automáticamente SSL CertificateIP. El DNS del certificado SSL contiene todas las direcciones IP del nombre alternativo del sujeto. Cuando intenta crear o reparar los certificados por defecto mediante Identity Console, el certificado SSL CertificateIP no se crea o se repara por defecto. Sin embargo, la interfaz del módulo auxiliar proporciona una casilla de verificación que puede seleccionar para anular el comportamiento por defecto y forzar la creación o la reparación del certificado SSL CertificateIP.

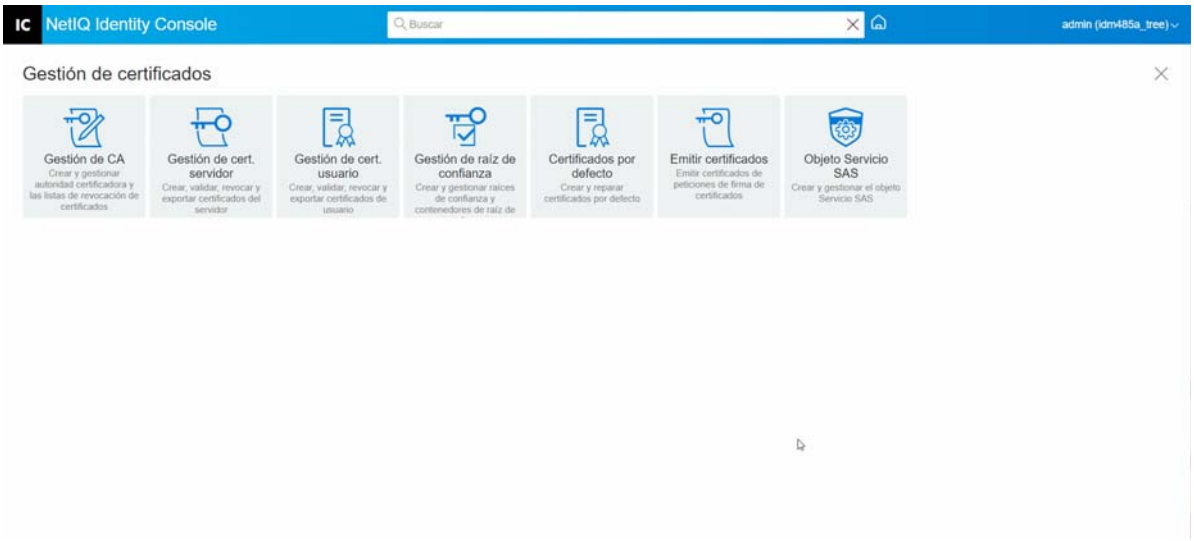
La versión eDirectory 9.0 y superiores crean automáticamente certificados ECDSA si la CA de la organización dispone de un certificado ECDSA.

Si estos certificados están dañados o no son válidos por algún motivo o si solo desea sustituir los certificados por defecto existentes, puede utilizar el Asistente para crear certificados de servidor por defecto, como se describe en el siguiente procedimiento:

1. Haga clic en las opciones **Gestión de certificados** > **Certificados por defecto** de la página de destino de Identity Console.
2. Seleccione el servidor o los servidores para los que desee crear certificados por defecto y, a continuación, haga clic en **Siguiente**.
3. Seleccione Sí si desea sobrescribir los certificados de servidor por defecto existentes o No si desea sobrescribir los certificados de servidor por defecto existentes solo si no son válidos.
4. (Solo para un único servidor) Si desea utilizar la dirección DNS existente, seleccione esa opción. Si desea utilizar una dirección DNS diferente, seleccione esa opción y especifique la nueva dirección DNS.
5. (Solo para un único servidor) Si desea utilizar la dirección IP por defecto existente, seleccione esa opción. Si desea utilizar una dirección IP diferente, seleccione esa opción y especifique la nueva dirección IP.
6. Haga clic en **Siguiente.**.
7. Revise la página de resumen y haga clic en **Finalizar**.

Si desea tener más control sobre la creación del objeto Certificado de servidor, puede crearlo manualmente. Para obtener más información, consulte “Creación de objetos Certificado de servidor” en la página 97.

Figura 17-5 *Creación de objetos Certificado de servidor por defecto*



Emisión de un certificado de clave pública

La CA administrativa funciona del mismo modo que una CA externa. Es decir, puede emitir certificados desde peticiones de firma de certificados (CSR). Puede emitir certificados mediante la CA administrativa cuando un usuario le envíe una CSR para firmar. A continuación, el usuario que solicita el certificado puede utilizar el certificado emitido e importarlo directamente en la aplicación habilitada para el cifrado.

Esta tarea permite generar certificados para aplicaciones habilitadas para el cifrado que no reconocen objetos Certificado de servidor.

Para emitir un certificado, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Emitir certificados** de la página de destino de Identity Console.
2. Busque y seleccione un archivo CSR.
3. Seleccione el tipo de clave adecuado y el uso de clave correspondiente en Especificaciones de uso clave. Las opciones siguientes le permiten seleccionar un tipo de clave. Cada tipo de clave tiene valores del uso de la clave predefinidos y asociados:
   - 3a **Sin especificar:** esta opción está seleccionada por defecto y no activa ningún uso de clave en el certificado.
   - 3b **Autoridad certificadora:** esta opción activa los usos de clave Firma de CRL y Firma de certificado.
   - 3c **Cifrado:** Esta opción activa el uso de claves Cifrado de clave.
   - 3d **Firma:** Esta opción activa el uso de claves Firma digital.
   - 3e **SSL o TSL:** Esta opción configura la clave para que se pueda utilizar en transacciones SSL o TLS.

3f **Personalizado:** esta opción permite seleccionar manualmente alguna o todas las opciones de uso de clave.

3g **Ajustar la extensión de uso de claves como crítica:** Todos los tipos de clave seleccionados, salvo No especificado, permiten marcar la extensión de uso de clave como crítica. Para que el certificado se pueda usar con algún fin, el software receptor debe entender las extensiones críticas. Por tanto, marcar una extensión como crítica supone cierto riesgo, ya que no todas las aplicaciones pueden utilizar el certificado. Sin embargo, en el caso de las extensiones conocidas, como el uso de la clave, el riesgo es mínimo. En general, si se especifica el uso de la clave, la extensión se debe marcar como crítica.

4 Puede optar por codificar una extensión **Uso mejorado de clave** en el certificado. Para activar esta función, seleccione **Habilitar uso mejorado de clave**:

4a **Servidor:** esta opción activa el uso mejorado de clave Autenticación del servidor.

4b **Usuario:** esta opción activa los usos mejorados de clave Autenticación de usuario y Protección de correo electrónico.

4c **Personalizado:** esta opción permite seleccionar cualquiera de los usos mejorados de clave o todos ellos.

4d **Cualquiera:** Permite utilizar la clave para cualquier uso de la clave extendida.

4e **Defina la extensión de uso mejorado de clave como crítica:** Para que el certificado se pueda usar con algún fin, el software receptor debe entender las extensiones críticas. Por tanto, marcar una extensión como crítica supone cierto riesgo, ya que no todas las aplicaciones pueden utilizar el certificado. Como muchas aplicaciones no entienden la extensión del uso de la clave extendida, la marca de esta extensión como crítica supone el gran riesgo de que una aplicación dada no acepte el certificado; por consiguiente, sólo se debe definir como crítica cuando sea necesario.

5 Seleccione las **restricciones básicas** adecuadas:

5a **Tipo de certificado:**

5a1 **Sin especificar:** Seleccione esta opción si no desea añadir ninguna extensión de límite básico al certificado.

5a2 **Autoridad certificadora:** Seleccione esta opción para añadir al certificado una extensión de límite básico de la Autoridad certificadora. Si el certificado es para una Autoridad certificadora, debe seleccionar esta opción.

5a3 **Entidad final:** Seleccione esta opción para añadir una extensión de límite básico al certificado que especifique que éste es un certificado de Entidad final (que no es una Autoridad certificadora). Nota: si un certificado es del tipo Entidad final, la longitud de la vía se debe establecer en No especificado.

5b **Longitud de vía:**

5b1 **Sin especificar:** Seleccione esta opción si no desea especificar el número de niveles de CA subordinadas que se pueden crear bajo esta CA.

Nota: Si un certificado es del tipo Entidad final, la longitud de la vía sólo se debe establecer en No especificado.

5b2 **Específicas:** Seleccione esta opción si desea especificar el número de niveles de CA subordinadas que se pueden crear bajo esta CA. Para especificar la longitud de la vía, haga clic en las flechas arriba y abajo.

Nota: Si el certificado que se va a crear es una CA subordinada, la longitud de la vía debe ser coherente con la CA superior. Por ejemplo, si la longitud de vía de la CA superior es 3, la de la subordinada debe ser 2 o menos. Si la CA superior tiene una longitud de vía no especificada, la subordinada también puede tener una longitud de vía no especificada o cualquier longitud de vía concreta deseada.

5c **Definir la extensión de las restricciones básicas como crítica:** En general, la extensión de las restricciones básicas se debe definir como crítica para los certificados de CA. Para que el certificado se pueda usar con algún fin, el software receptor debe entender las extensiones críticas. Por tanto, marcar una extensión como crítica supone cierto riesgo, ya que no todas las aplicaciones pueden utilizar el certificado. Sin embargo, en el caso de las extensiones conocidas, como las restricciones básicas, el riesgo es mínimo.

6 Especifique los siguientes parámetros de certificado:

6a **Nombre de sujeto:** muestra el nombre completo del árbol de eDirectory.

6b **Nombre de sujeto:** muestra el nombre completo del árbol de eDirectory.

6c **Período de validez:** Utilice la lista desplegable para especificar el período de validez del certificado. El rango va de seis meses al máximo, el año 2036 (una limitación de tiempo basada en un valor de tiempo de 32 bits). Si selecciona la opción Especificar fechas, puede editar los campos Entrada en vigor y Caducidad para crear un período de validez personalizado. La fecha máxima seleccionada debe encontrarse dentro de la fecha de validez de la CA.

6c1 **Fecha efectiva:** Permite mostrar o editar la fecha y hora en las que el certificado adquiere validez.

6c2 **Fecha de caducidad:** Permite mostrar o editar la fecha y hora en las que el certificado deja de ser válido.

6d **Extensiones personalizadas:** Permite que el Servidor de certificados admita todas las extensiones estándar o personalizadas que desee incluir al crear certificados. Las extensiones se deben haber creado y almacenado previamente en un archivo (una extensión por archivo). Todas las extensiones deben tener la codificación ASN.1, tal como se define en la sección 4.2 de IETF RFC 2459/3280.

Si desea incluir una o varias extensiones en el certificado que va a crear, haga clic en Nuevo, busque un archivo que contenga la extensión personalizada y añádalo al certificado. Para añadir varias extensiones, repita este proceso.

Para suprimir un archivo de extensiones personalizadas, selecciónelo y haga clic en el icono  .

7 Seleccione el formato de certificado adecuado entre las opciones siguientes:

7a **Archivo en formato DER binario:** esta opción permite guardar o exportar un certificado a un archivo que se muestra en el campo Nombre de archivo. Por defecto, el archivo de certificado se exporta con una extensión .DER en la raíz de la unidad C: de una estación de trabajo de Identity Console basada en Windows y en el directorio personal de una estación de trabajo de Identity Console basada en Linux.

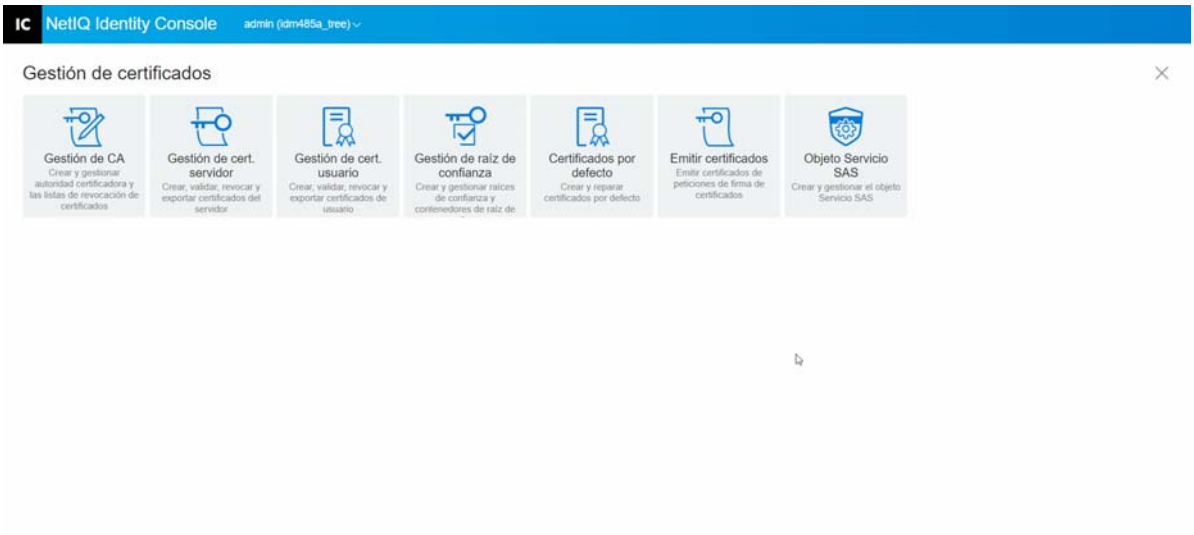
7b **Archivo en formato Base64:** esta opción permite guardar un archivo CSR o exportar un certificado a un archivo que se muestra en el campo Nombre de archivo. Por defecto, los archivos de certificado y CSR se exportan con una extensión .B64 en la raíz de la unidad C: de una estación de trabajo de Identity Console basada en Windows y en el directorio personal de una estación de trabajo de Identity Console basada en Linux.

7c **Archivo en formato CER:** esta opción permite guardar un archivo CSR o exportar un certificado a un archivo que se muestra en el campo Nombre de archivo. Por defecto, los archivos de certificado y CSR se exportan con una extensión .CER en la raíz de la unidad C: de una estación de trabajo de Identity Console basada en Windows y en el directorio personal de una estación de trabajo de Identity Console basada en Linux.

8 Revise el resumen del certificado en la pantalla siguiente y haga clic en **Aceptar**.

9 Aparece un mensaje de confirmación que indica que el certificado se ha emitido correctamente.

Figura 17-6 *Emisión de un certificado de clave pública*



Gestión de un objeto SAS Service

El objeto SAS Service facilita la comunicación entre un servidor y sus certificados de servidor. Si quita un servidor de un árbol de eDirectory, también deberá quitar el objeto SAS Service asociado a dicho servidor. Si desea volver a colocar el servidor en el árbol, deberá crear el objeto SAS Service que acompañe a ese servidor. De lo contrario, no podrá crear nuevos certificados de servidor.

El objeto SAS Service se crea automáticamente como parte de la comprobación de estado del servidor. No debería ser necesario crearlo manualmente.

Puede crear un objeto SAS Service nuevo si no hay un objeto SAS Service con el nombre adecuado en el mismo contenedor que el objeto Servidor. Por ejemplo, para un servidor denominado WAKE, tendrá un objeto SAS Service denominado SAS Service - WAKE. La utilidad añade los punteros DS del objeto Servidor al objeto SAS y del objeto SAS al objeto Servidor y configura las entradas ACL correctas en el objeto SAS Service.

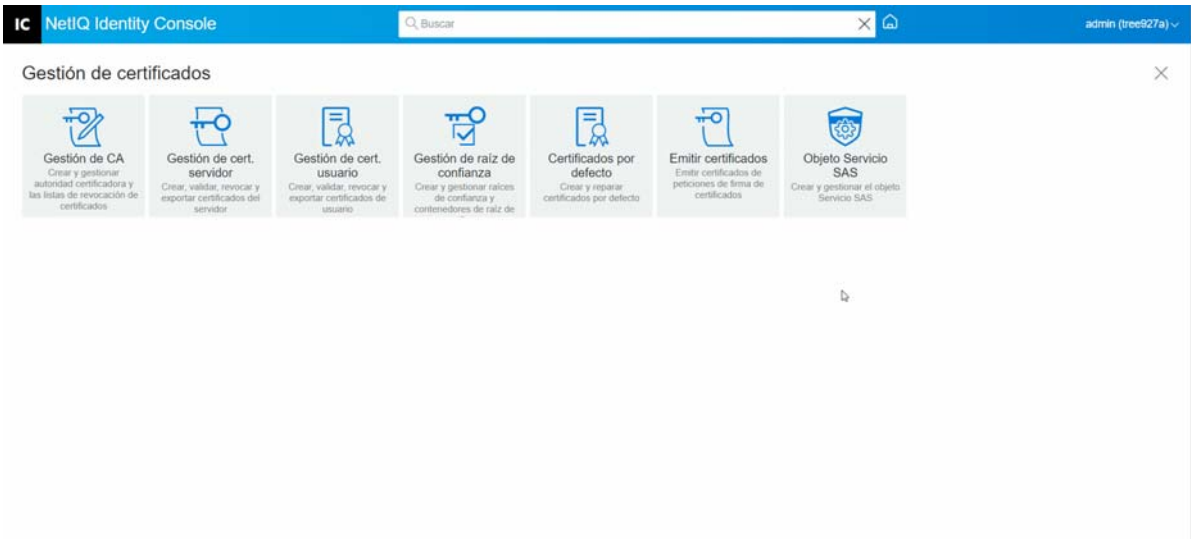
Si ya existe un objeto SAS Service con el nombre adecuado, no puede crear uno nuevo. Es posible que los punteros DS del objeto SAS Service anterior sean erróneos o no existan o que las ACL no sean correctas. En ese caso, puede suprimir el objeto SAS Service dañado y utilizar el portal de Identity Console para crear uno nuevo.

Creación o supresión de un objeto SAS Service

Para crear o suprimir un objeto SAS Service, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de certificados** > **Objeto SAS Service** de la página de destino de Identity Console.
2. Si no se ha creado ningún objeto SAS Service para un servidor existente, haga clic en el icono + para crear uno nuevo.
3. Aparece un mensaje de confirmación que indica que se ha creado correctamente un objeto SAS Service.
4. Para eliminar un objeto SAS Service, haga clic en el icono 🗑.
5. Haga clic en **Aceptar** en la pantalla de confirmación para eliminar correctamente un objeto SAS Service.

Figura 17-7 *Gestión de objetos SAS Service*



18 Gestión del marco de autenticación

Mediante el módulo Autenticación, puede realizar las siguientes tareas:

Gestión de secuencias y métodos de entrada y posteriores a la entrada

NMAS incluye compatibilidad con varios métodos de entrada y posteriores a la entrada de NetIQ y de desarrolladores de autenticación de terceros. Algunos métodos requieren hardware y software adicionales. Asegúrese de que cuenta con todos los componentes de hardware y software necesarios para los métodos que va a utilizar.

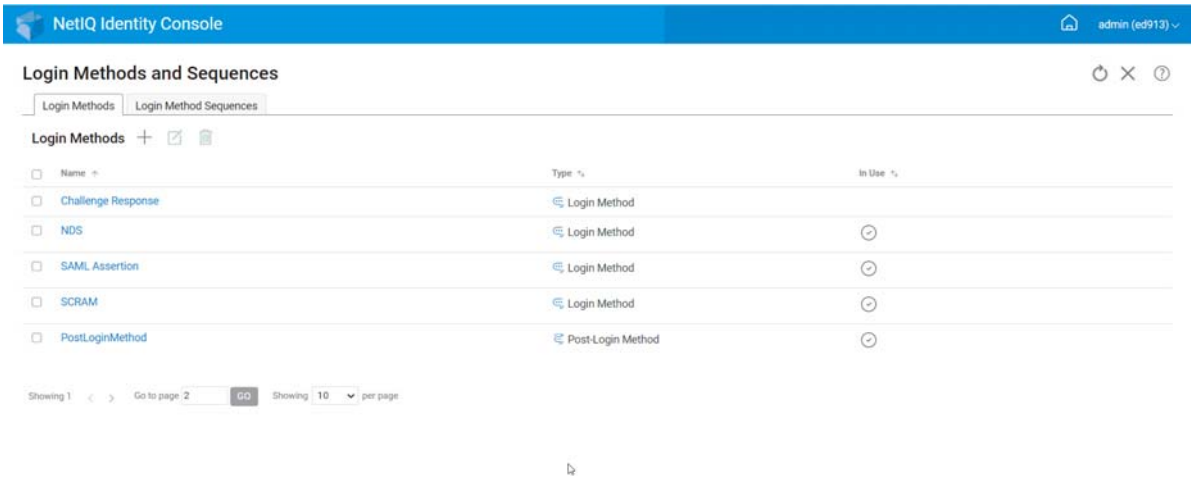
En esta sección, se describe cómo instalar y configurar métodos y secuencias de entrada y posteriores a la entrada para NMAS.

Instalación de un método de entrada o posterior a la entrada

Para instalar un método de entrada, realice las siguientes tareas:

1. Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.
2. Haga clic en el icono + para instalar un nuevo método de entrada.
3. Busque y seleccione el archivo de método de entrada (.zip) que desea instalar y, a continuación, haga clic en **Siguiente**.
4. Siga el asistente de instalación para completar el proceso de instalación del método de entrada.

Figura 18-1 *Instalación de un nuevo método de entrada*

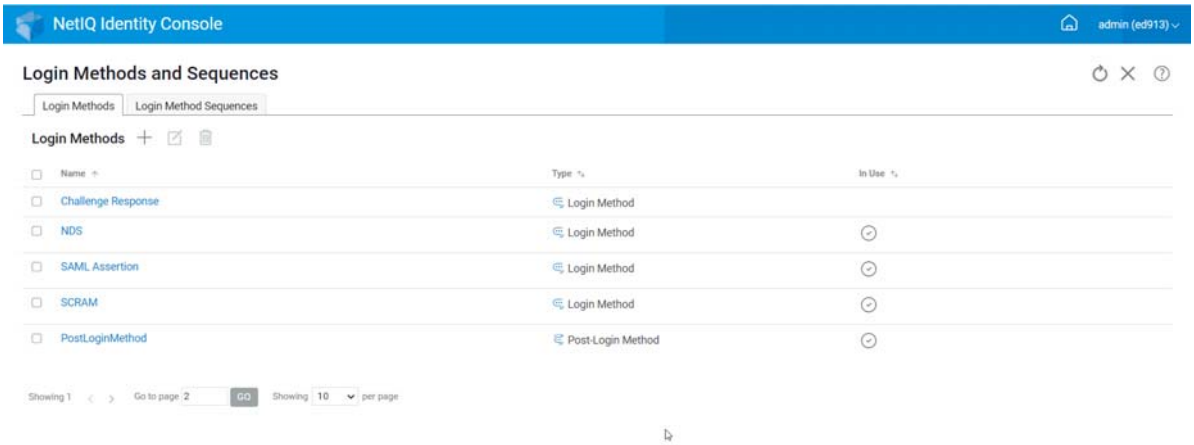


Actualización de un método de entrada o posterior a la entrada existente

Para actualizar un método de entrada existente, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.
2. Seleccione el método de entrada que desea actualizar en la lista y haga clic en el icono .
3. Busque y seleccione el archivo de método de entrada (.zip) que desea actualizar y, a continuación, haga clic en **Siguiente**.
4. Siga el asistente de actualización para completar la actualización del método de entrada.

Figura 18-2 *Actualización de un método de entrada existente*

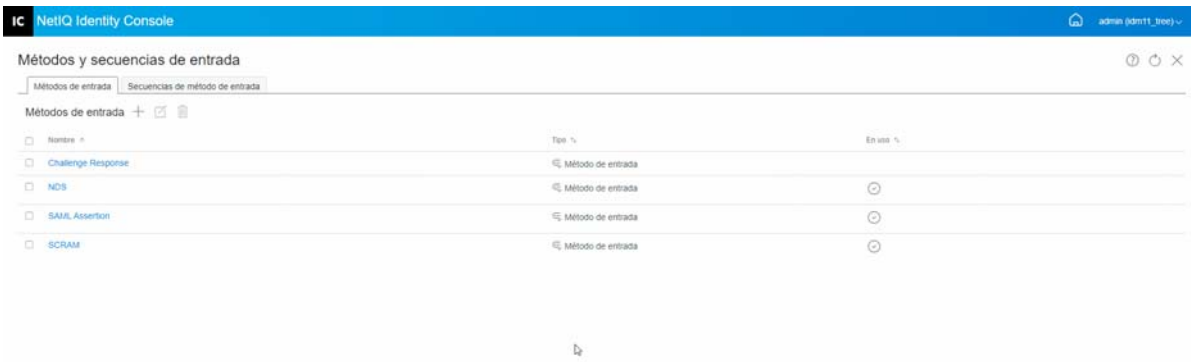


Desinstalación de métodos de entrada o posteriores a la entrada

Para desinstalar métodos de entrada o posteriores a la entrada, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.
2. Seleccione los métodos de entrada que desea desinstalar en la lista y haga clic en el icono .
3. En la siguiente pantalla, haga clic en **Aceptar**.
4. Aparece un mensaje de confirmación que indica que se han desinstalado los métodos de entrada.

Figura 18-3 *Desinstalación de un método de entrada*



Creación de una nueva secuencia de método de entrada

Una vez que haya creado varios métodos de entrada para su entorno, puede decidir el orden en el que deben utilizarse. Para crear una nueva secuencia de método de entrada, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.
2. Seleccione la pestaña **Secuencias de método de entrada**.
3. Haga clic en el icono + para crear una nueva secuencia de método de entrada.
4. Especifique un **nombre** y seleccione el **tipo de secuencia**.
5. Seleccione los métodos de entrada y posteriores a la entrada necesarios en la lista de métodos disponibles.

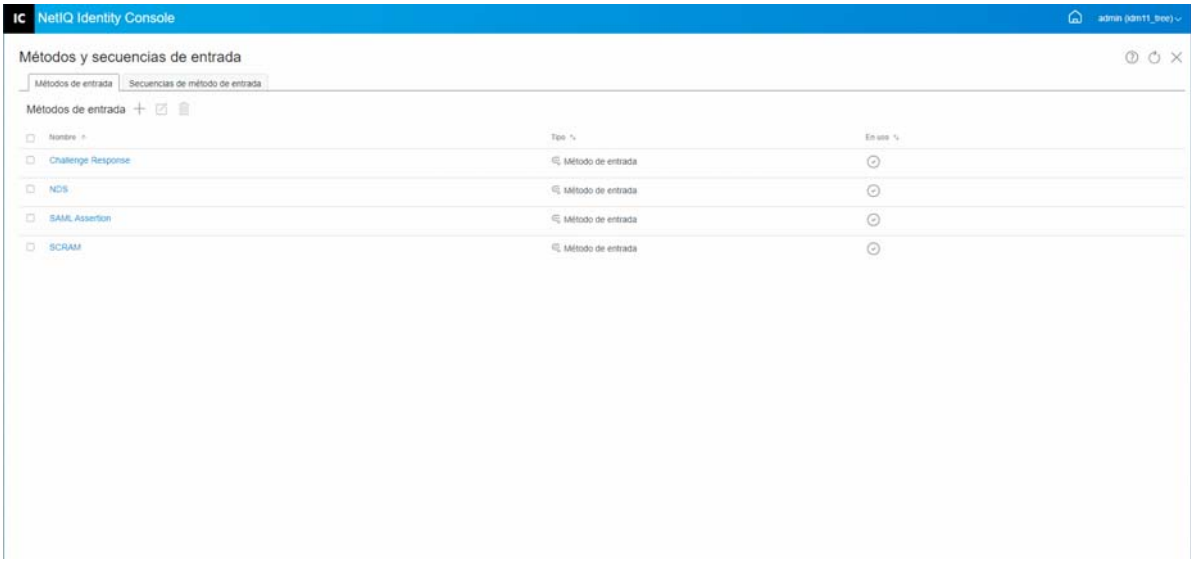
Nota: Puede decidir el orden de los métodos de entrada. Para ello, haga clic en las flechas arriba y abajo que aparecen en los objetos Método de entrada.

---

6 Haga clic en el botón **Crear**.

7 Aparece un mensaje de confirmación que indica que se ha creado correctamente una nueva secuencia de métodos de entrada.

Figura 18-4 *Creación de una secuencia de método de entrada*



Modificación de una secuencia de método de entrada

Para modificar una secuencia de método de entrada existente, realice los siguientes pasos:

1 Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.

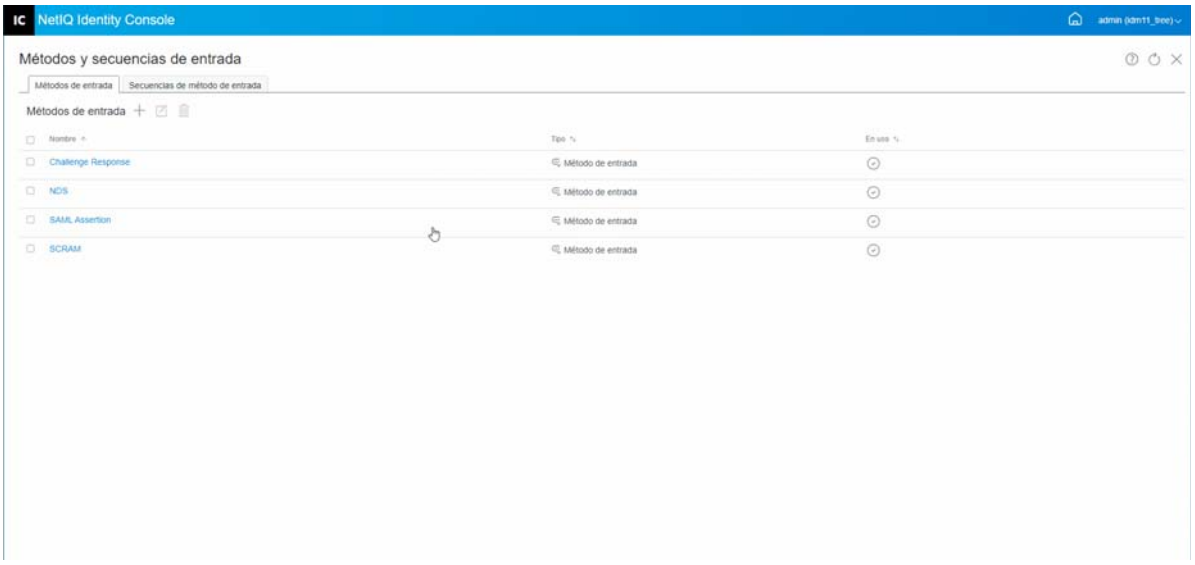
2 Seleccione la pestaña **Secuencias de método de entrada**.

3 Haga clic en el icono ☑ para modificar una secuencia de método de entrada existente.

4 Realice los cambios necesarios en la página **Modificar secuencia del método de entrada** y haga clic en **Guardar**.

5 Aparece un mensaje de confirmación que indica que la secuencia de método de entrada se ha modificado correctamente.

Figura 18-5 *Modificación de una secuencia de método de entrada*

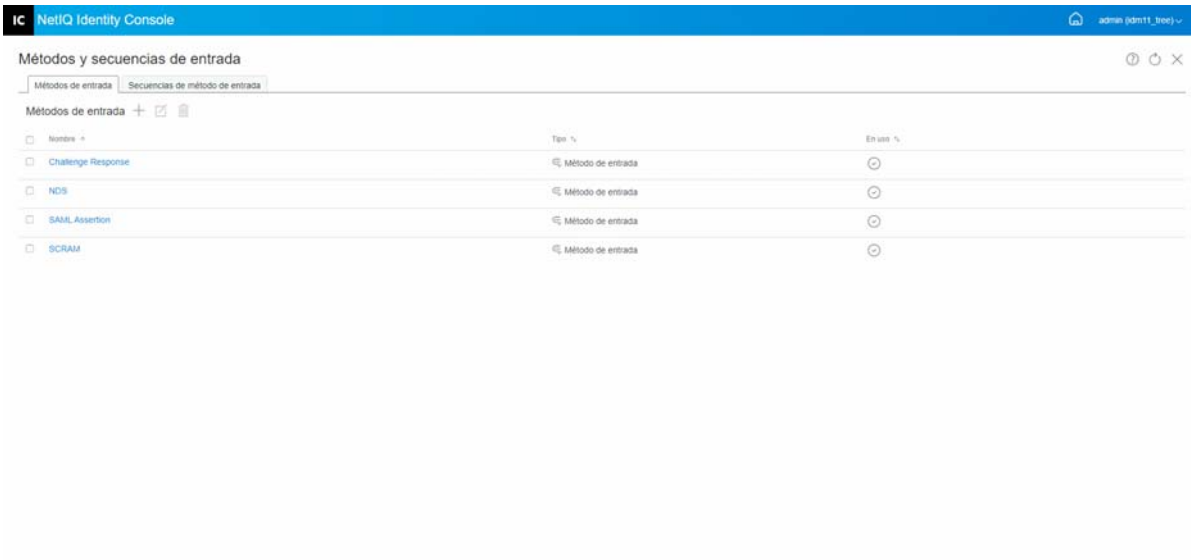


Autorización o desautorización de una secuencia de método de entrada

Una secuencia de método de entrada se debe autorizar y definir como por defecto para asociarla a usuarios, contenedores y particiones. Para autorizar una secuencia de método de entrada, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.
2. Seleccione la pestaña **Secuencias de método de entrada**.
3. Seleccione la secuencia de método de entrada adecuada en la lista y haga clic en el icono ⓥ.
4. Para desautorizar una secuencia de método de entrada, selecciónela y haga clic en el icono ⓧ.
5. También puede autorizar o desautorizar una secuencia de método de entrada desde el menú desplegable situado bajo la columna **Autorizado** de la lista Secuencias de método de entrada.

Figura 18-6 *Autorización o desautorización de una secuencia de método de entrada*

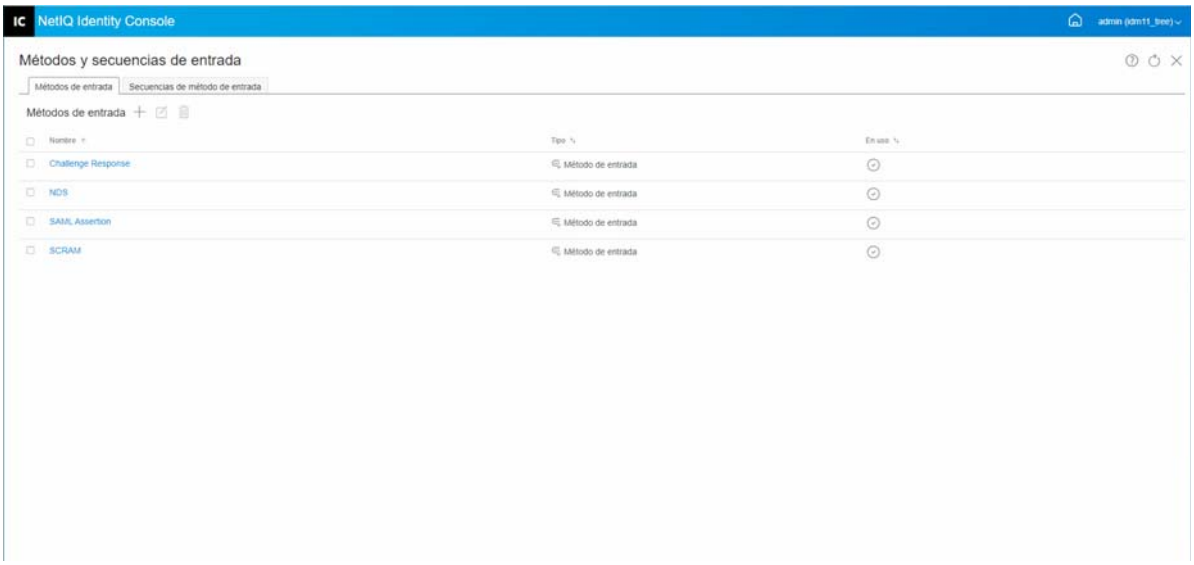


Definición de una secuencia de método de entrada por defecto

Para definir una secuencia de entrada por defecto de modo que los usuarios no tengan que especificar una secuencia de entrada al iniciar sesión:

1. Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.
2. Seleccione la pestaña **Secuencias de método de entrada**.
3. Habilite el icono para definir una secuencia de método de entrada autorizada como por defecto.

Figura 18-7 *Definición de una secuencia de método de entrada por defecto*

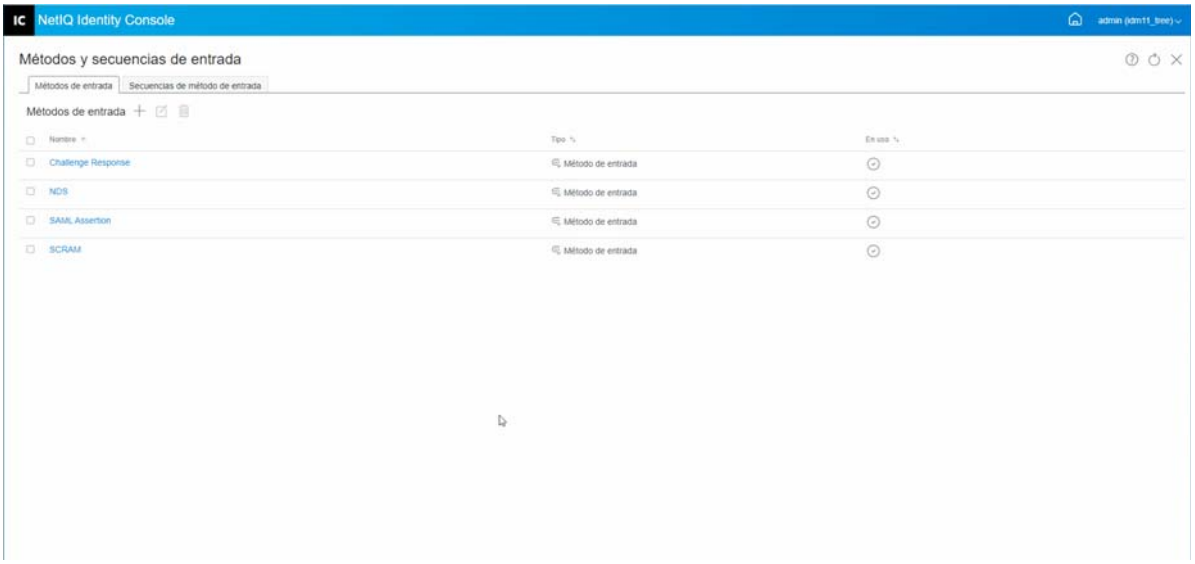


Supresión de secuencias de método de entrada

Para suprimir una secuencia de método de entrada:

1. Haga clic en las opciones **Gestión de autenticación** > **Métodos y secuencias de entrada** de la página de destino de Identity Console.
2. Seleccione la pestaña **Secuencias de método de entrada**.
3. Seleccione la secuencia de método de entrada adecuada en la lista y haga clic en el icono .
4. Haga clic en **Aceptar** en la siguiente pantalla de confirmación.

Figura 18-8 *Supresión de una secuencia de método de entrada*



Gestión de las directivas de contraseñas

Una directiva de contraseñas es un conjunto de reglas definidas por el administrador que especifican los criterios de creación y sustitución de contraseñas de usuario final. NMAS le permite aplicar las directivas de contraseñas que asigne a los usuarios en eDirectory. Estas directivas también pueden incluir funciones de autoservicio de Contraseña olvidada para reducir las llamadas al servicio de asistencia técnica para recuperar contraseñas. Otra función de autoservicio es Restablecer contraseña, que permite a los usuarios cambiar las contraseñas mientras visualizan las reglas que el administrador ha especificado en la directiva de contraseñas. Los usuarios pueden acceder a estas funciones a través de Identity Console o la aplicación de usuario de Identity Manager.

Mediante el módulo Directivas de contraseñas, puede realizar las siguientes tareas:

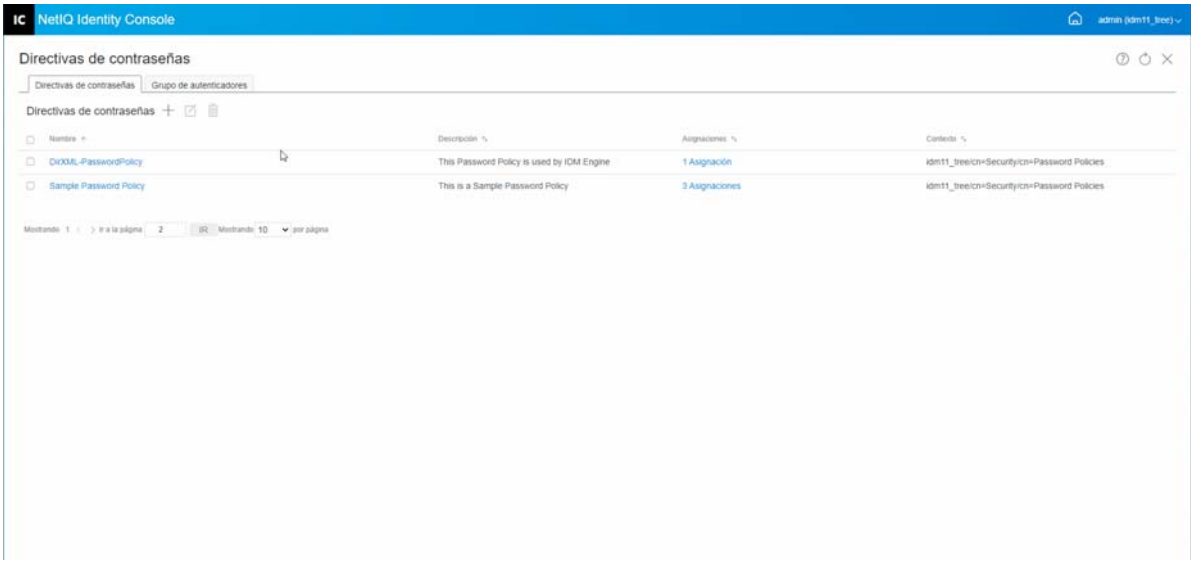
- “Creación de una directiva de contraseñas con parámetros por defecto” en la página 118
- “Creación de una directiva de contraseñas con parámetros personalizados” en la página 118
- “Modificación de una directiva de contraseñas” en la página 122
- “Supresión de directivas de contraseña” en la página 122

Creación de una directiva de contraseñas con parámetros por defecto

Para crear una nueva directiva de contraseñas, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Directivas de contraseñas** de la página de destino de Identity Console.
2. Haga clic en el icono + para crear una nueva directiva de contraseñas.
3. Especifique el nombre, el contexto, la descripción y un mensaje de cambio de contraseña en la pantalla siguiente.
4. Si desea crear una directiva de contraseñas con la configuración por defecto, marque la casilla **Crear una nueva directiva de contraseñas basada en los ajustes por defecto** y haga clic en **Siguiente** para ver la página **Resumen**.
5. Compruebe los detalles en la página **Resumen** y haga clic en **Crear**.
6. Aparece un mensaje de confirmación que indica que la directiva de contraseñas se ha creado correctamente.

Figura 18-9 *Creación de una directiva de contraseñas con parámetros por defecto*



Creación de una directiva de contraseñas con parámetros personalizados

Para crear una directiva de contraseñas con parámetros personalizados, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Directivas de contraseñas** de la página de destino de Identity Console.
2. Haga clic en el icono + para crear una nueva directiva de contraseñas.
3. Especifique el nombre, el contexto, la descripción y un mensaje de cambio de contraseña en la pantalla siguiente.

4 Si desea crear una directiva de contraseñas con los parámetros personalizados, haga clic en **Siguiente**.

5 Realice las siguientes acciones en la página **Configuración**:

5a **Habilitar Contraseña Universal:** al habilitar la contraseña universal para una directiva, puede utilizar las opciones de la función Directivas de contraseñas. Sin embargo, para poder habilitar la contraseña universal en una directiva, debe cumplir los requisitos previos de la contraseña universal en el entorno.

5b **Habilitar las reglas avanzadas para contraseñas:** esta opción habilita las reglas para contraseñas que se encuentran en la pestaña Reglas avanzadas para contraseñas. Estas reglas le ayudan a proteger su entorno al proporcionarle control sobre diversos criterios, como la duración de una contraseña y el contenido de una contraseña como, por ejemplo, una combinación de letras, números, letras mayúsculas o minúsculas y caracteres especiales. Puede excluir aquellas contraseñas que no considere seguras, como el nombre de la empresa.

5c **Sincronización de contraseñas:** estas opciones determinan la forma en que la contraseña universal se sincroniza en eDirectory con otros tipos de contraseñas del repositorio seguro de identidades. La función Sincronización de contraseñas incluye las siguientes opciones:

5c1 **Eliminar la contraseña de NDS al definir la contraseña:** si esta opción está seleccionada, la contraseña de NDS se inhabilita al definir la contraseña universal. Los usuarios no podrán usar métodos o utilidades anteriores que entren a la sesión con la contraseña de DNS en lugar de comunicarse con NMAS. Si se establece esta opción, la siguiente opción **Sincronizar la contraseña de NDS al definir la contraseña** se inhabilitará por defecto.

5c2 **Sincronizar la contraseña de NDS al definir la contraseña:** si selecciona esta opción, al definir la contraseña universal en aplicaciones como Identity Console, también se cambia la contraseña de NDS.

5c3 **Sincronizar la contraseña simple al definir la contraseña:** esta opción proporciona compatibilidad con NetIQ y clientes de terceros que utilizan la contraseña simple y la provisión de usuarios.

5c4 **Sincronizar la contraseña de distribución al definir la contraseña:** esta opción determina si el motor de metadirectorio puede recuperar o definir la contraseña universal de un usuario en eDirectory.

5d **Recuperación de la contraseña universal:** Están disponibles las siguientes opciones:

5d1 **Permitir al usuario recuperar la contraseña:** permite al agente de usuario recuperar la contraseña. Esta opción determina si la función Autoservicio de contraseña olvidada puede recuperar una contraseña en nombre de un usuario, con el fin de que se le pueda enviar por correo electrónico. Si no selecciona esta opción, la función correspondiente aparece atenuada en la pestaña Contraseña olvidada de la directiva de contraseñas.

5d2 **Permitir que el administrador recupere contraseñas:** marque esta casilla si tiene un servicio específico que necesita esta opción. Identity Manager no necesita que los administradores recuperen contraseñas. Sin embargo, algunos servicios de terceros pueden aprovechar esta opción.

5d3 **Permitir lo siguiente para recuperar contraseñas:** seleccione el usuario adecuado que debe recuperar la contraseña. Para ello, haga clic en el icono +.

5e Autenticación:

5e1 Verificar si las contraseñas existentes cumplen la directiva de contraseñas (la verificación se produce al entrar a la sesión): esta opción es útil si va a instalar una directiva de contraseñas nueva o a cambiar las reglas avanzadas para las contraseñas de una directiva existente y desea confirmar que las contraseñas existentes cumplen las reglas nuevas o modificadas.

Si selecciona esta opción, cuando los usuarios entren a la sesión, se analizarán las contraseñas existentes para asegurarse de que cumplan las reglas avanzadas para contraseñas de la directiva de contraseñas nueva o modificada. Si alguna contraseña no las cumple, el usuario debe cambiarla.

Una vez que haya terminado, haga clic en **Siguiente**.

6 La función **Reglas avanzadas para contraseñas** le ayudan a proteger el entorno al ofrecerle control sobre la información de contraseñas como, por ejemplo, la duración de una contraseña, su frecuencia de cambio y su contenido.

Los caracteres especiales son los caracteres que no son numéricos (0-9) ni alfabéticos.

Realice las siguientes acciones en la página Reglas avanzadas para contraseñas:

6a Puede gestionar los ajustes de sintaxis de contraseña mediante la sintaxis de la directiva de complejidad de Microsoft (anterior a Microsoft Windows Server 2008), la directiva de contraseñas de Microsoft Server 2008 o la sintaxis de Novell.

6b Especifique las opciones necesarias para Cambiar contraseña, Duración de la contraseña, Longitud y composición de la contraseña y Exclusiones de contraseñas en el asistente y haga clic en **Siguiente**.

7 Puede reducir el coste del servicio de asistencia técnica habilitando el autoservicio de **Contraseña olvidada**para los usuarios que no recuerden su contraseña. Estas funciones de autoservicio están disponibles para los usuarios a través del portal de Identity Console. Realice las siguientes acciones en la página Contraseña olvidada:

Nota: Si habilita Contraseña olvidada, también debe especificar si se requiere un conjunto de preguntas desafío para ayudar al usuario a entrar a la sesión.

7a Conjuntos de preguntas desafío: si utiliza la opción Conjuntos de preguntas desafío, los usuarios no podrán utilizar el autoservicio de Contraseña olvidada hasta que respondan a las preguntas del conjunto de preguntas desafío. Para asegurarse de que se solicita a los usuarios que introduzcan esta información a través del portal de Identity Console, seleccione la opción **Requerir grupo de preguntas desafío**.

7b Acción: las opciones disponibles de esta pestaña permiten al usuario restablecer la contraseña mediante conjuntos de preguntas desafío y la contraseña universal, habilitar el envío de la contraseña actual o la sugerencia de contraseña por correo electrónico y visualizar la opción de sugerencia de contraseña.

7c Autenticar: seleccione **Forzar al usuario a configurar preguntas de seguridad o sugerencias sobre la autenticación** para garantizar que a los usuarios se les solicite que especifiquen los conjuntos de preguntas desafío o la sugerencia de contraseña.

Una vez que haya terminado, haga clic en **Siguiente**.

8 Una directiva no es efectiva hasta que se asigna a uno o varios objetos. Para simplificar la administración, es recomendable que asigne directivas en la parte más elevada posible del árbol. Se puede asignar una directiva de contraseñas a los siguientes objetos:

8a **Objeto Directiva de entrada:** es recomendable crear una directiva de contraseñas por defecto para todos los usuarios del árbol y asignarla al objeto Directiva de entrada que se encuentra en el contenedor Seguridad.

8b **Un contenedor que es una raíz de partición:** si asigna una directiva a un contenedor que es la raíz de una partición, todos los usuarios de esa partición, incluidos los usuarios de subcontenedores, heredarán la asignación de directiva.

8c **Un contenedor que no es una raíz de partición:** si asigna una directiva a un contenedor que no es la raíz de una partición, solo los usuarios incluidos en ese contenedor específico heredarán la asignación de directiva. Los usuarios incluidos en subcontenedores no heredará la directiva.

Para aplicar la directiva a todos los usuarios de un contenedor que no sea una raíz de partición, asigne la directiva a cada subcontenedor individualmente.

8d **Un usuario:** puede asignar una directiva a uno o varios usuarios.

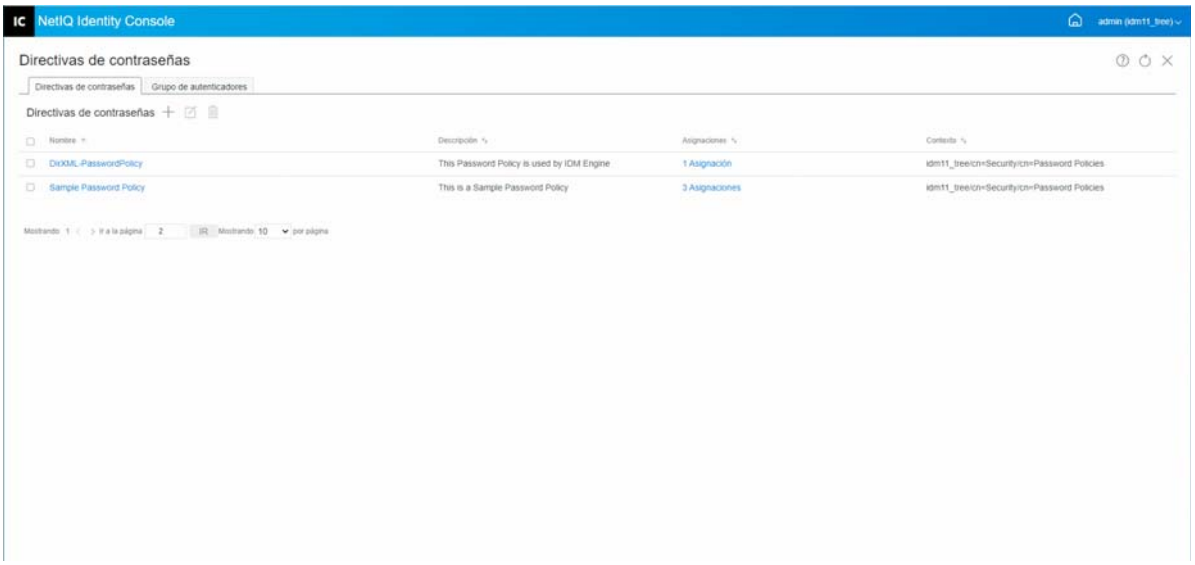
Para asignar una directiva, haga clic en el icono +. A continuación, busque y seleccione el objeto adecuado para asignar una directiva de contraseñas.

En caso de que desee eliminar una asociación de directiva, seleccione la directiva en la lista y haga clic en el icono 🗑.

9 Compruebe los detalles en la página **Resumen** y haga clic en **Crear**.

10 Aparece un mensaje de confirmación que indica que la directiva de contraseñas se ha creado correctamente.

Figura 18-10 *Creación de una directiva de contraseñas con parámetros personalizados*

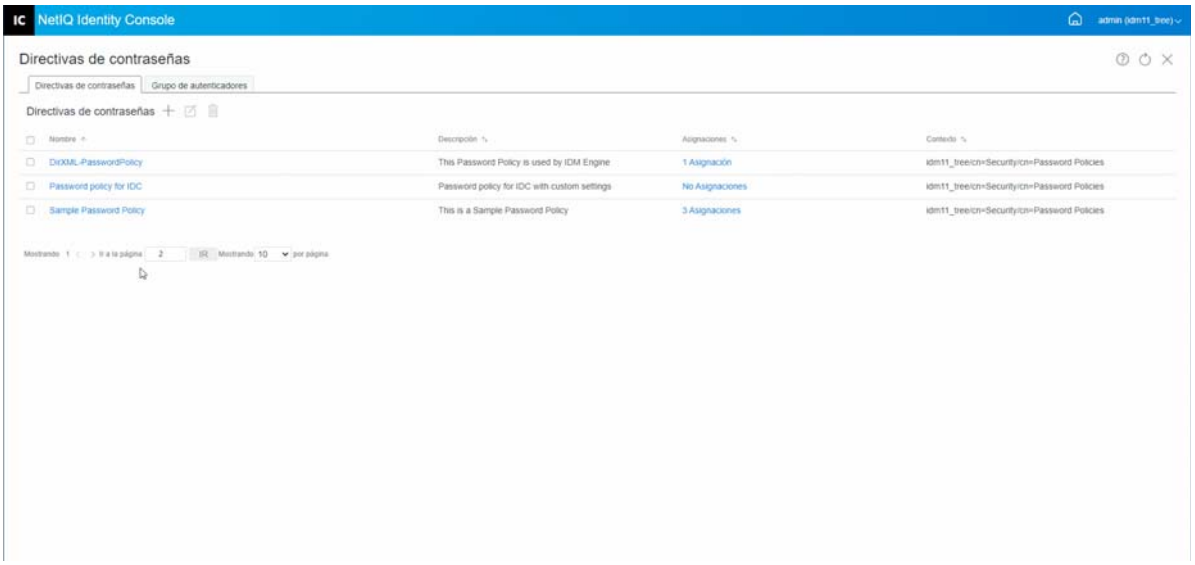


Modificación de una directiva de contraseñas

Para modificar una directiva de contraseñas existente, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Directivas de contraseñas** de la página de destino de Identity Console.
2. Seleccione la directiva de contraseñas adecuada en la lista y haga clic en el icono .
3. Realice los cambios necesarios en la página **Modificar directiva de contraseña** y haga clic en **Guardar**.

Figura 18-11 *Modificación de una directiva de contraseñas*

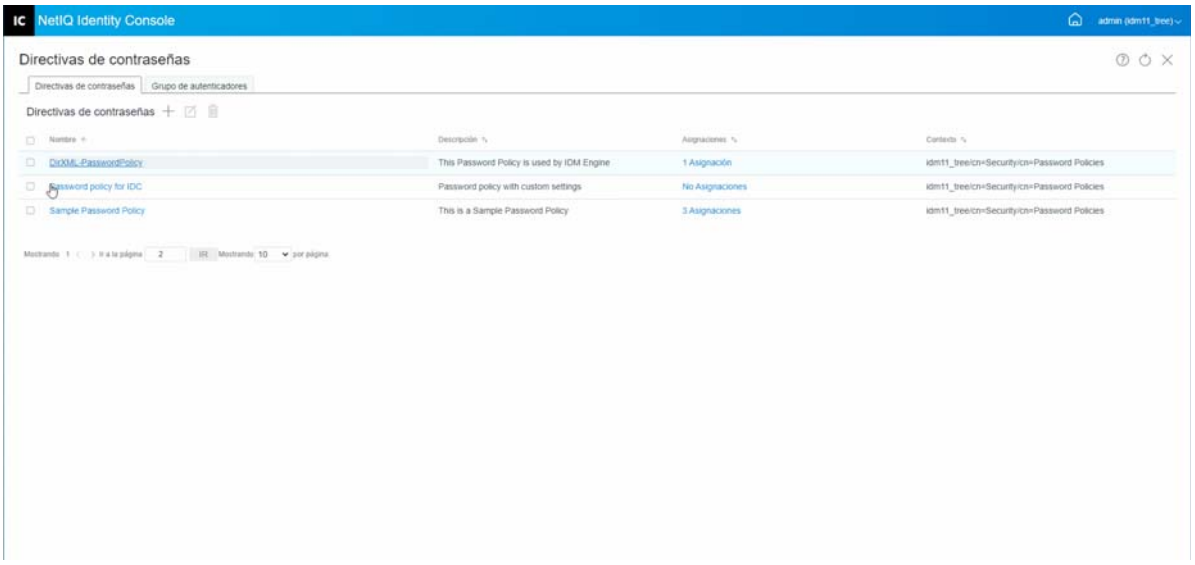


Supresión de directivas de contraseña

Para suprimir directivas de contraseña, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Directivas de contraseñas** de la página de destino de Identity Console.
2. Seleccione las directivas de contraseñas adecuadas en la lista y haga clic en el icono .
3. En la siguiente pantalla de advertencia, haga clic en **Aceptar**.
4. Aparece un mensaje de confirmación que indica que se han suprimido las directivas de contraseñas.

Figura 18-12 *Supresión de directivas de contraseñas*



Gestión de conjuntos de preguntas desafío

Un conjunto de preguntas desafío hace referencia a una o varias preguntas a las que el usuario debe responder para validar su identidad. Esta función forma parte del autoservicio de contraseña.

Si un usuario tiene problemas al recordar o utilizar la contraseña, puede utilizar el autoservicio de contraseña en lugar de llamar al servicio de asistencia técnica. Un conjunto de preguntas desafío permite al usuario validar la identidad y, a continuación, recibir una sugerencia o una contraseña en un mensaje de correo electrónico o restablecer una contraseña mediante un navegador Web.

Puede permitir que los usuarios creen sus propias preguntas y respondan a ellas, o bien solicitar a los usuarios que respondan a las preguntas que cree.

La página Conjuntos de preguntas desafío permite buscar y editar conjuntos de preguntas desafío existentes y crear nuevos.

- “Creación de un nuevo conjunto de preguntas desafío” en la página 123
- “Modificación de un conjunto de preguntas desafío” en la página 124
- “Supresión de conjuntos de preguntas desafío” en la página 125

Creación de un nuevo conjunto de preguntas desafío

Para crear un nuevo conjunto de preguntas desafío, realice los siguientes pasos:

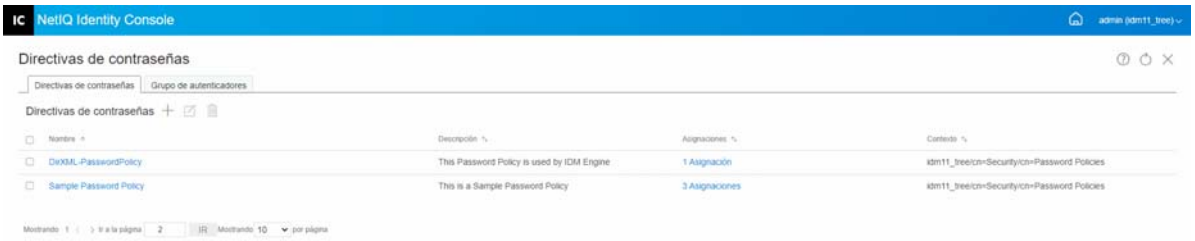
1. Haga clic en las opciones **Gestión de autenticación** > **Directivas de contraseñas** > **Conjuntos de preguntas desafío** de la página de destino de Identity Console.
2. Haga clic en el icono + para crear un nuevo conjunto de preguntas desafío.
3. Especifique un nombre para el objeto Conjunto de preguntas desafío y seleccione el contenedor o el subcontenedor en el que debe crearse el conjunto de preguntas desafío.

4 Cree un nuevo conjunto de preguntas que se realizarán para recuperar la contraseña del usuario. También puede seleccionar preguntas en el conjunto existente de preguntas aleatorias.

5 Defina el número de preguntas que se deben realizar y, a continuación, haga clic en **Crear**.

6 Aparece un mensaje de confirmación que indica que el conjunto de preguntas desafío se ha creado correctamente.

Figura 18-13 *Creación de un conjunto de preguntas desafío*



Modificación de un conjunto de preguntas desafío

Para modificar un conjunto de preguntas desafío existente, realice los siguientes pasos:

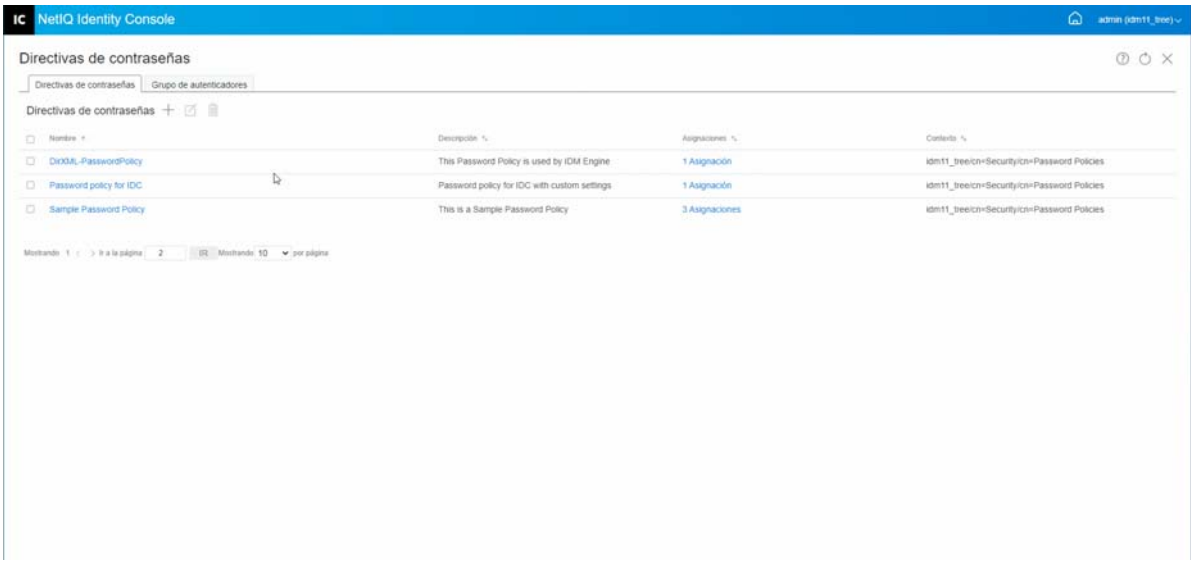
1 Haga clic en las opciones **Gestión de autenticación** > **Directivas de contraseñas** > **Conjuntos de preguntas desafío** de la página de destino de Identity Console.

2 Seleccione el conjunto de preguntas desafío adecuado en la lista y haga clic en el icono ☑.

3 Realice los cambios necesarios en la página Modificar conjunto de preguntas desafío y, a continuación, haga clic en **Guardar**.

4 Aparece un mensaje de confirmación que indica que el conjunto de preguntas desafío se ha modificado correctamente.

Figura 18-14 *Modificación de un conjunto de preguntas desafío*

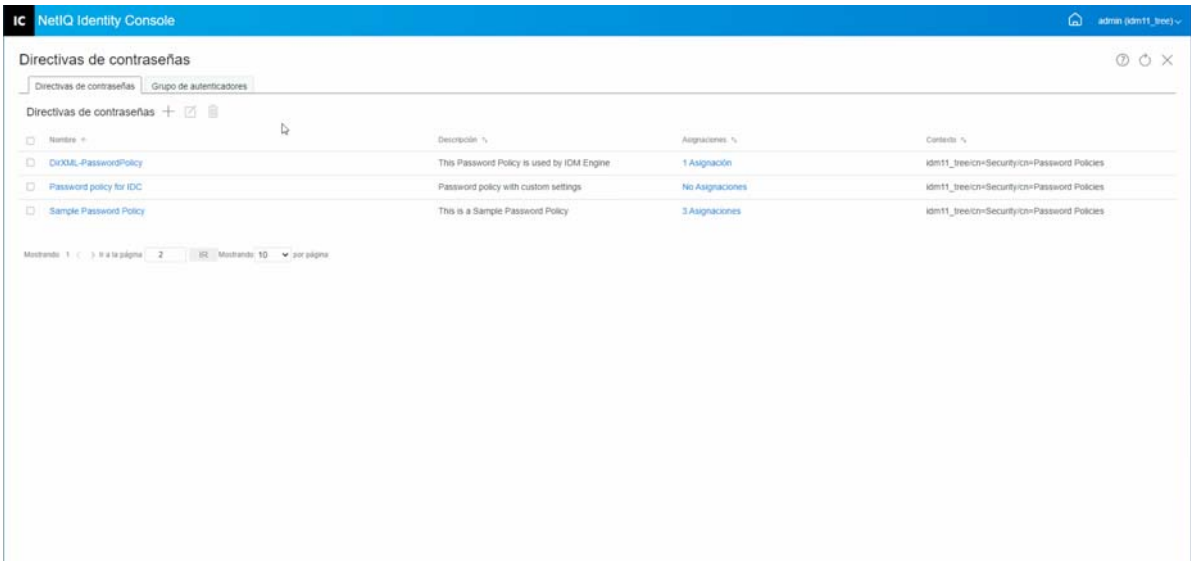


Supresión de conjuntos de preguntas desafío

Para suprimir conjuntos de preguntas desafío, realice los siguientes pasos:

1. Haga clic en las opciones **Gestión de autenticación** > **Directivas de contraseñas** > **Conjuntos de preguntas desafío** de la página de destino de Identity Console.
2. Seleccione el conjunto de preguntas desafío correspondiente en la lista y haga clic en el icono .
3. Haga clic en **Aceptar** en la pantalla de confirmación.
4. Aparece un mensaje de confirmación que indica que el conjunto de preguntas desafío se ha suprimido correctamente.

Figura 18-15 *Supresión de un conjunto de preguntas desafío*



19 Gestión de objetos Grupo de SNMP

El Protocolo simple de administración de redes (SNMP) es el protocolo estándar de operaciones y mantenimiento de Internet para el intercambio de información de gestión entre las aplicaciones de la consola de gestión y los dispositivos gestionados.

Mediante el módulo SNMP, puede realizar las siguientes tareas:

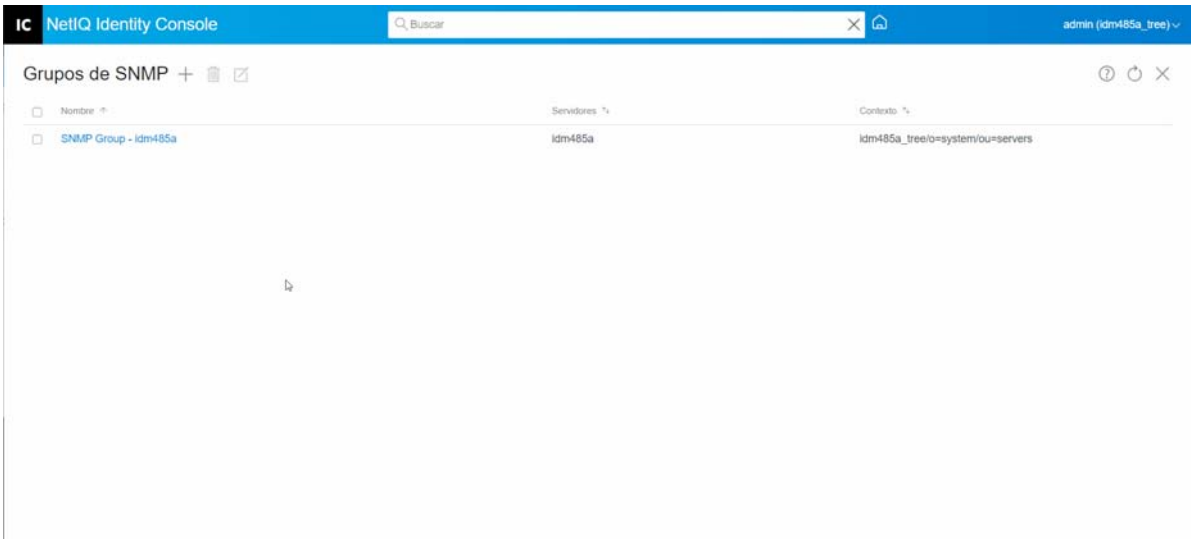
- “Creación de objetos Grupo de SNMP” en la página 127
- “Modificación de objetos Grupo de SNMP” en la página 128
- “Supresión de objetos Grupo de SNMP” en la página 128

Creación de objetos Grupo de SNMP

Para crear objetos Grupo de SNMP, realice los siguientes pasos:

1. Haga clic en el módulo **SNMP** de la página de destino de Identity Console.
2. Haga clic en el icono + para crear un nuevo objeto Grupo de SNMP.
3. Especifique el nombre y seleccione el contexto para crear un nuevo objeto Grupo de SNMP.
4. Haga clic en el botón **Crear**.
5. Aparece un mensaje en la pantalla que confirma que el objeto Grupo de SNMP se ha creado correctamente.

Figura 19-1 *Creación de objetos Grupo de SNMP*

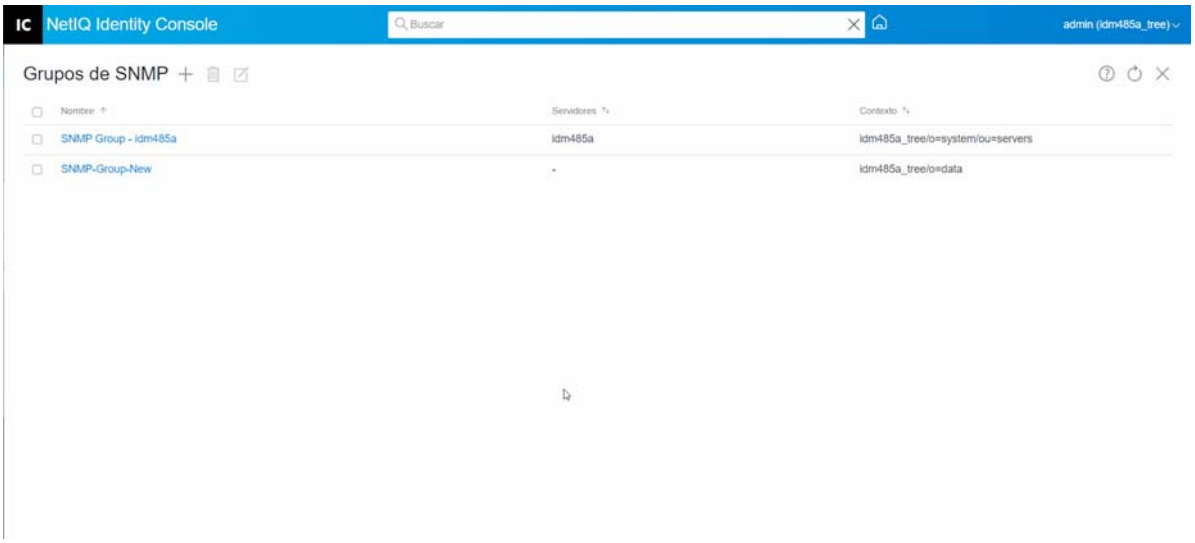


Modificación de objetos Grupo de SNMP

Para modificar objetos Grupo de SNMP, realice los siguientes pasos:

1. Haga clic en el módulo **SNMP** de la página de destino de Identity Console.
2. Seleccione el objeto Grupo de SNMP que desee modificar y haga clic en el icono .
3. Modifique los parámetros configurables en la página **General**/**Alertas**.
4. Cuando haya terminado, haga clic en el botón **Guardar**.
5. Aparece un mensaje en la pantalla que confirma que el objeto Grupo de SNMP se ha modificado correctamente.

Figura 19-2 *Modificación de objetos Grupo de SNMP*

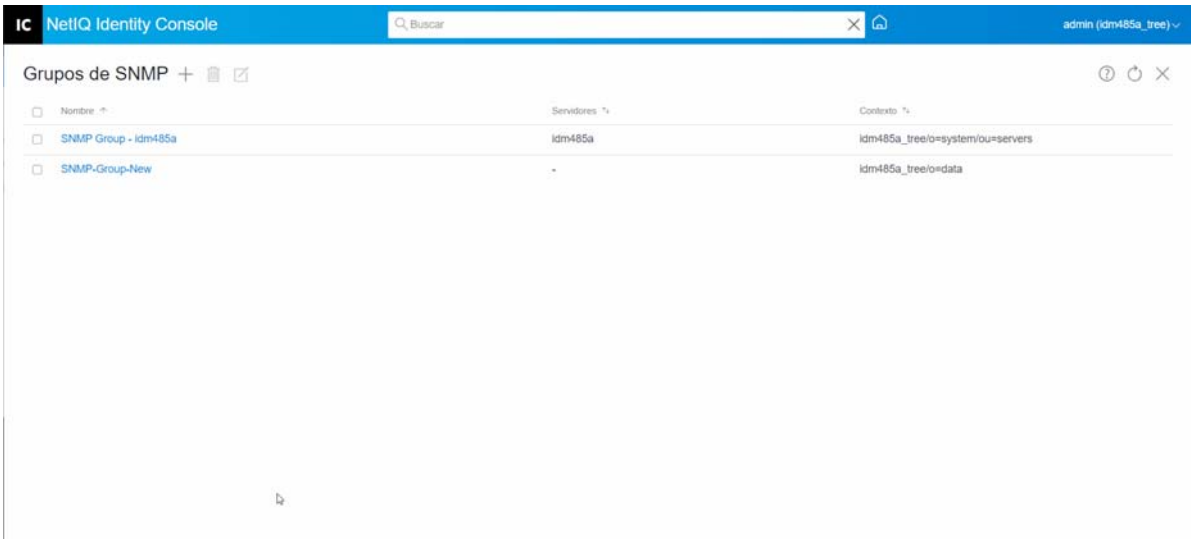


Supresión de objetos Grupo de SNMP

Para suprimir objetos Grupo de SNMP, realice los siguientes pasos:

1. Haga clic en el módulo **SNMP** de la página de destino de Identity Console.
2. Seleccione el objeto Grupo de SNMP que desee modificar y haga clic en el icono .
3. Haga clic en **Aceptar** en la siguiente pantalla.
4. Aparece un mensaje en la pantalla que confirma que el objeto Grupo de SNMP se ha suprimido correctamente.

Figura 19-3 *Supresión de objetos Grupo de SNMP*



20 Gestión de Enhanced Background Authentication

Para acceder a eDirectory desde el módulo auxiliar EBA de Identity Console, debe tener un servidor habilitado para EBA en el árbol con un archivo eba.p12 válido. Para obtener más información sobre cómo habilitar EBA en el árbol de eDirectory, consulte Enabling EBA on an eDirectory Tree (Habilitar EBA en un árbol de eDirectory) de *NetIQ eDirectory Administration Guide* (Guía de administración de NetIQ eDirectory).

Nota: Si desea utilizar el módulo EBA con Identity Console, debe actualizar el servidor de eDirectory a 9.2.4 HF2.

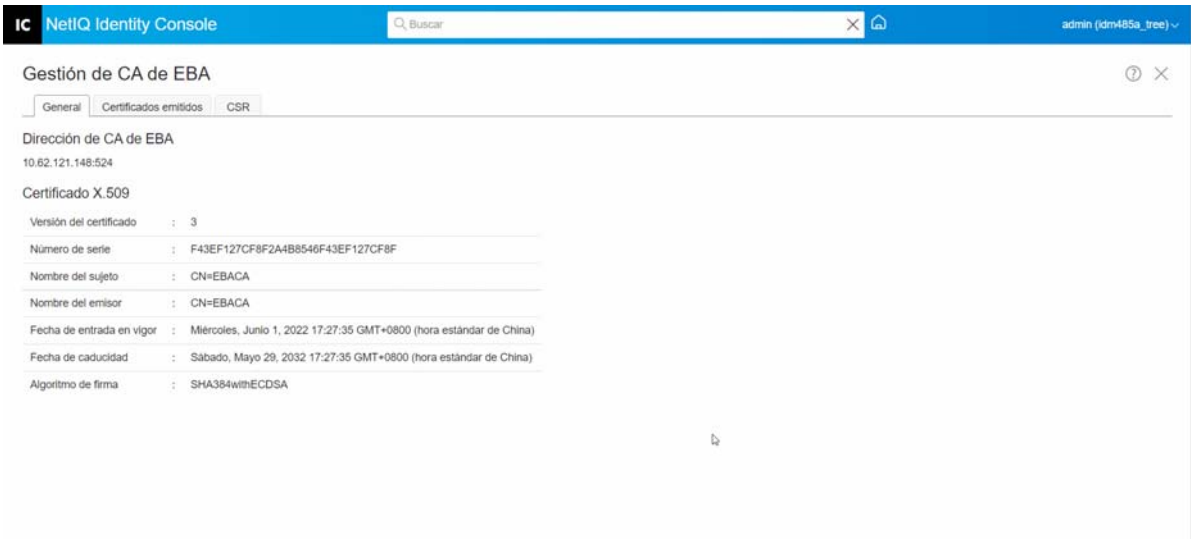
Para abrir la página Gestión de CA de EBA, entre en el portal de Identity Console y haga clic en el módulo **EBA**.

La página Gestión de CA de EBA incluye las siguientes pestañas para gestionar distintos aspectos de la CA de EBA:

- **General:** Muestra la dirección IP de la autoridad certificadora de EBA y su certificado.
- **Certificados emitidos:** Muestra los certificados de la autoridad certificadora de NCP junto con su dirección IP y puerto.

  Para revocar un certificado, seleccione el certificado y haga clic en  . Utilice esta opción solo en situaciones extremas, ya que el servidor que posee el certificado de CA de NCP dejará de estar operativo cuando revoque su certificado. Por lo general, la revocación del certificado es necesaria cuando la seguridad del servidor se ve comprometida.
- **CSR:** Muestra las peticiones de firma de certificados pendientes para la aprobación del administrador. Para aprobar una petición de firma de certificado, selecciónela en la lista y haga clic **Aprobar**.

Figura 20-1 *Gestión de Enhanced Background Authentication*



II Gestión de Identity Manager mediante Identity Console

En esta sección, se describen las distintas tareas que puede llevar a cabo para gestionar los servidores de Identity Manager mediante el portal de Identity Console.

21 Gestión de controladores y conjuntos de controladores

Un conjunto de controladores es un contenedor que contiene controladores de Identity Manager. Solo un conjunto de controladores puede estar activo en un servidor cada vez. Por lo tanto, todos los controladores activos deben agruparse en el mismo conjunto de controladores. El conjunto de controladores se puede crear mediante la herramienta Designer. Para obtener más información, consulte Configuring Driver Sets (Configuración de conjuntos de controladores) en la *NetIQ Designer for Identity Manager Administration Guide* (Guía de administración de NetIQ Designer para Identity Manager).

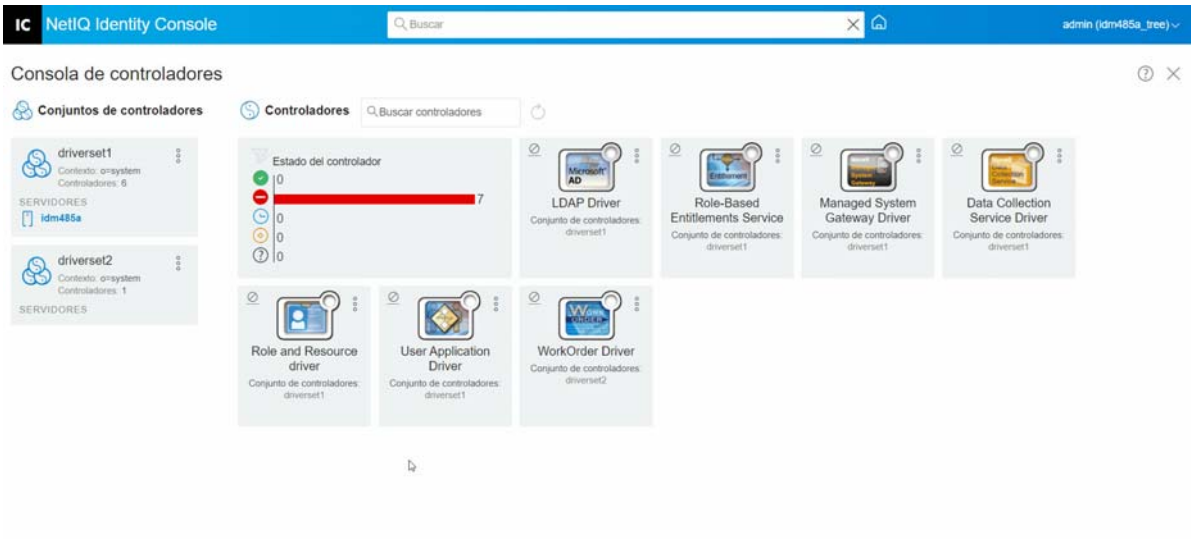
Añadir o suprimir servidores

Un conjunto de controladores se puede asociar a uno o varios servidores cada vez. Sin embargo, en función de sus requisitos, puede asociar un objeto Conjunto de controladores diferente al servidor disponible.

Para añadir un nuevo servidor, haga clic en el icono del objeto Conjunto de controladores específico > seleccione **Añadir servidores** y elija el servidor adecuado en el Navegador de contexto.

Para suprimir un servidor existente, seleccione la opción **Eliminar servidor**.

Figura 21-1 *Añadir servidor a un conjunto de controladores*



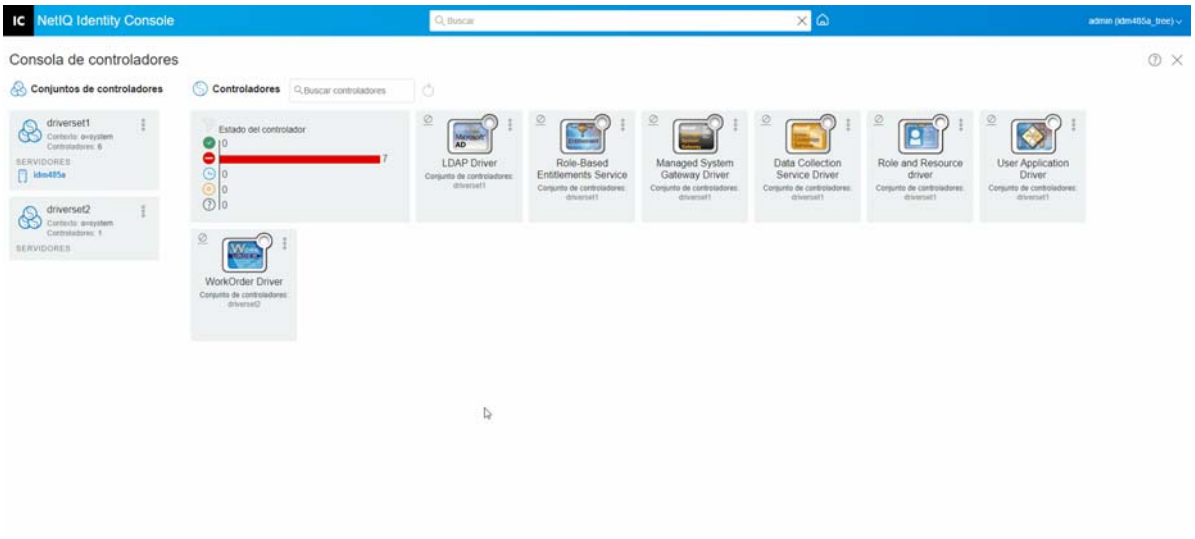
Activación de los conjuntos de controladores mediante la clave de activación del producto

Antes de utilizar un conjunto de controladores y los controladores incluidos en él, debe activarlo mediante el código de activación recibido en su ID de correo electrónico. Después de adquirir una licencia, recibirá la clave de activación de NetIQ. Lleve a cabo los pasos siguientes para activar el conjunto de controladores mediante la clave de activación:

1. Haga clic en la pestaña **Administración de IDM** en la pantalla de inicio de Identity Console.
2. Haga clic en el icono Acciones del recuadro del conjunto de controladores específico que desea activar y, a continuación, haga clic en **Instalación de activación**.

   Al aplicar la activación, en cada pestaña del conjunto de controladores en el mosaico Administración de IDM, se muestra la información de activación de todos los servidores asociados a ese conjunto de controladores. Esta información ayuda a identificar cuándo caducará la activación.
3. Si ha descargado el archivo de activación en el equipo, marque la casilla de verificación **Seleccione un archivo que incluya credenciales**.
4. Busque y seleccione el archivo de activación y haga clic en **Enviar**.
5. También puede activar el conjunto de controladores mediante el contenido del archivo de activación. Marque la casilla de verificación **Introduzca las credenciales**.
   - **5a** Abra el archivo de certificación de activación de productos y copie su contenido en el portapapeles.
   - **5b** Si ha decidido copiar el contenido, no incluya líneas ni espacios adicionales. Debe empezar a copiar desde el primer guion (-) de la certificación (----INICIO DE LA CERTIFICACIÓN DE ACTIVACIÓN DE PRODUCTOS) hasta el último guion (FINAL DE LA CERTIFICACIÓN DE ACTIVACIÓN DE PRODUCTOS-----). A continuación, haga clic en **Finalizar**.
6. Aparece un mensaje de confirmación que indica que el conjunto de controladores se ha activado correctamente.

Figura 21-2 *Activación de conjuntos de controladores*

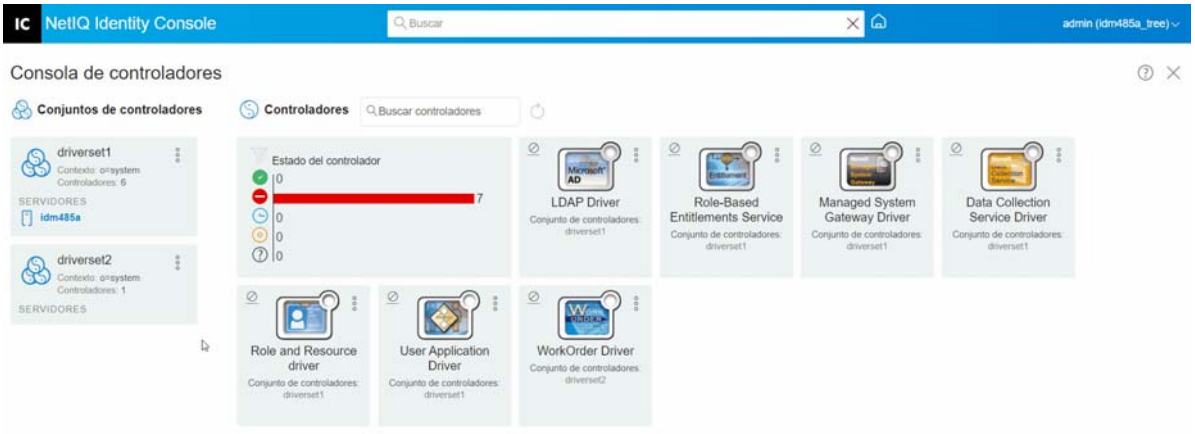


Visualización de la información de activación de conjuntos de controladores

Después de activar el conjunto de controladores, debe comprobar que este se haya activado correctamente. Para verificarlo, realice los siguientes pasos:

1. Haga clic en la pestaña **Administración de IDM** en la pantalla de inicio de Identity Console.
2. Haga clic en el icono Acciones ⋮ del objeto Conjunto de controladores específico para el que desea verificar la información de activación y haga clic en **Info. de activación**.
3. Aparecerá la ventana emergente de información relacionada con la activación en el equipo. En esta página, puede verificar los detalles de activación del conjunto de controladores específico.

Figura 21-3 *Visualización de la información de activación de conjuntos de controladores*

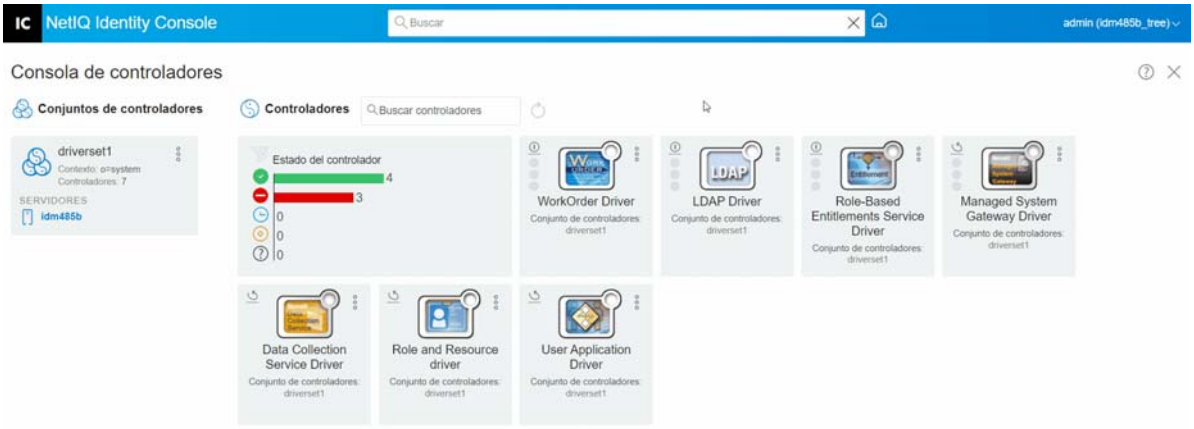


Inicio y detención de controladores

Cuando se crea un controlador, este está detenido por defecto. Para que el controlador funcione, debe iniciarlo. Identity Manager es un sistema basado en eventos, por lo que después de iniciar el controlador, este permanecerá inactivo hasta que se produzca un evento. Realice los siguientes pasos para iniciar o detener los controladores.

1. Haga clic en la pestaña **Administración de IDM** en la pantalla de inicio de Identity Console.
2. Haga clic en el objeto Conjunto de controladores específico en el lado derecho de la pantalla del equipo para visualizar todos los controladores asociados a él.
3. Haga clic en el icono Acciones del controlador específico y seleccione **Iniciar controlador**.
4. Para detener un objeto Controlador, haga clic en el icono Acciones del controlador específico y seleccione **Detener controlador**.
5. (Opcional) También puede iniciar o detener todos los controladores que residen simultáneamente en el mismo objeto Conjunto de controladores. Haga clic en el icono Acciones del objeto Conjunto de controladores y seleccione **Iniciar todos los controladores** o **Detener todos los controladores**.

Figura 21-4 *Inicio y detención de controladores*



Búsqueda de controladores

Identity Console proporciona la opción de buscar un controlador específico en el servidor. Para buscar un controlador, realice los siguientes pasos:

1. Haga clic en la pestaña **Administración de IDM** en la pantalla de inicio de Identity Console.
2. Especifique el nombre del controlador en el recuadro **Buscar**. El objeto Controlador específico aparecerá en la pantalla del equipo. También puede actualizar la lista de controladores. Para ello, haga clic en el icono .

Figura 21-5 *Búsqueda de controladores*

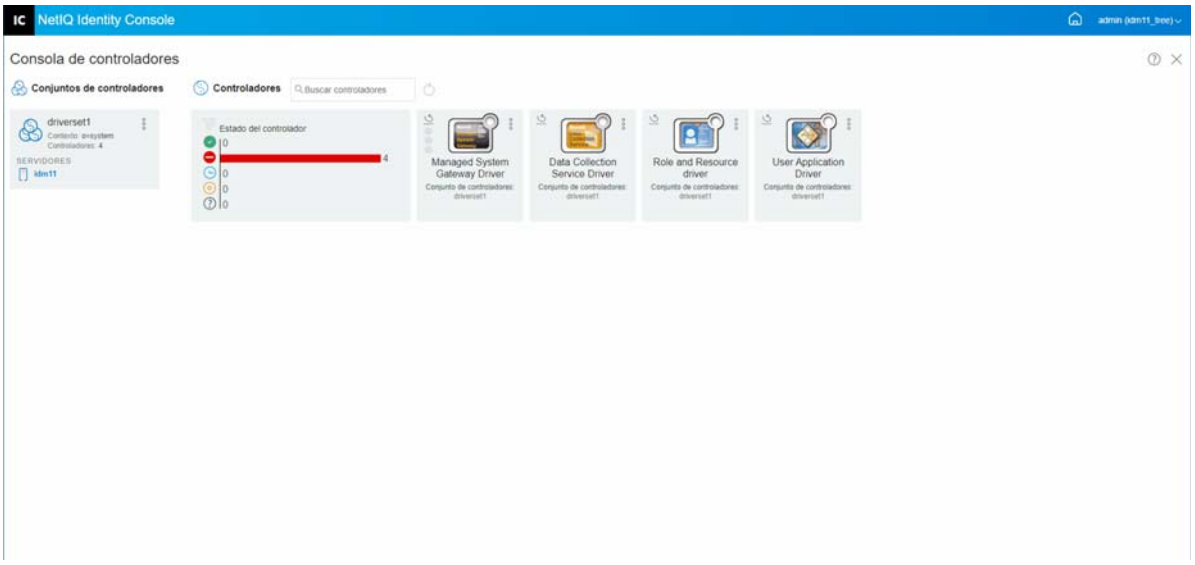
Filtrado de controladores y conjuntos de controladores

Los controladores se pueden filtrar en función de su estado desde la página **Administración de IDM**. Para filtrar controladores:

1. Haga clic en la pestaña **Administración de IDM** en la pantalla de inicio de Identity Console.
2. Haga clic en los siguientes iconos del mosaico **Estado del controlador** para filtrar los controladores en función de su estado:
   - Haga clic en el icono para filtrar todos los controladores en ejecución del servidor.
   - Haga clic en el icono para filtrar todos los controladores detenidos del servidor.
   - Haga clic en el icono para filtrar todos los controladores que se están iniciando.
   - Haga clic en el icono para filtrar todos los controladores que se están deteniendo.
   - Haga clic en el icono para filtrar los controladores que no tengan un estado asociado. Cuando un conjunto de controladores no tiene un servidor asociado, los controladores que residen en ese conjunto presentarán el estado **Desconocido**.

   Para borrar todos los filtros que se hayan aplicado a los controladores, haga clic en el icono que aparece en el mosaico **Estado del controlador**.
3. Los conjuntos de controladores también se pueden filtrar mediante el portal de Identity Console. Por defecto, en el portal de Identity Console, se mostrarán todos los controladores asociados a todos los conjuntos de controladores del servidor. Si desea ver los controladores de un conjunto de controladores específico, debe seleccionar el conjunto de controladores adecuado en la lista de conjuntos de controladores situada a la izquierda del portal de Identity Console. Para borrar la selección del conjunto de controladores, haga clic una vez más en el conjunto de controladores seleccionado.

Figura 21-6 *Filtrado de controladores y conjuntos de controladores*



Suprimir el conjunto de controladores

Para suprimir un conjunto de controladores, realice los siguientes pasos:

1. Haga clic en la pestaña **Administración de IDM** en la pantalla de inicio de Identity Console.
2. Haga clic en el botón de acciones ⋮ en el conjunto de controladores adecuado que desee suprimir.
3. Seleccione **Suprimir**.

Acciones del controlador

Se admiten las siguientes acciones al hacer clic en el icono de acciones ⋮ del mosaico de un control individual:

- **Iniciar controlador**: para iniciar un controlador.
- **Detener controlador**: para detener un controlador.
- **Reiniciar controlador**: para reiniciar un controlador detenido.
- **Suprimir controlador**: para suprimir un controlador.
- **Estadísticas**: para ver las estadísticas de rendimiento del controlador.
- **Copiar datos**: para copiar los datos del controlador de un servidor a otro. Esta opción solo está disponible en un entorno de varios servidores.

22 Gestión de las propiedades del conjunto de controladores

En esta sección, se proporciona información acerca de las propiedades comunes a todos los conjuntos de controladores. Esto incluye todas las propiedades (Contraseña con nombre, Nivel de registro, Inspector del conjunto de controladores, etc.).

Esta sección se divide en las siguientes categorías:

Configuración de conjuntos de controladores

Para modificar la configuración del conjunto de controladores, realice los siguientes pasos:

1. Haga clic en **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores**.
2. Por defecto, aparece la página **Configuración del conjunto de controladores**. Las opciones de configuración del conjunto de controladores se dividen en las siguientes categorías:

Contraseña con nombre

Identity Manager permite almacenar de forma segura varias contraseñas para un conjunto de controladores. Esta función se conoce como contraseñas con nombre. A cada contraseña diferente se accede mediante una clave o un nombre.

Puede añadir contraseñas con nombre a un conjunto de controladores o a controladores individuales. Las contraseñas con nombre de un conjunto de controladores están disponibles para todos los controladores del conjunto.

Para utilizar una contraseña con nombre en una directiva de controlador, debe hacer referencia a ella por el nombre de la contraseña en lugar de utilizar la contraseña real; el motor de Identity Manager envía la contraseña al controlador. El método descrito en esta sección para almacenar y recuperar contraseñas con nombre se puede utilizar con cualquier controlador sin necesidad de realizar cambios en el shim del controlador.

Para acceder a la contraseña con nombre, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Contraseña con nombre** en **Configuración del conjunto de controladores**.

Para añadir una contraseña con nombre nueva, haga clic en el icono  . Para eliminar una contraseña con nombre existente, seleccione la contraseña adecuada y haga clic en el icono  .

Valores de configuración global

Muestra una lista ordenada de objetos Configuración global. Los objetos contienen definiciones de extensión de GCV para el controlador que carga Identity Manager cuando se inicia el controlador. Puede añadir o eliminar los objetos Configuración global y cambiar el orden en el que se ejecutan.

Haga clic en el icono  para guardar los GCV. Para actualizar la lista de GCV, haga clic en el icono  .

Configuración de los parámetros de entorno de Java

Para configurar los parámetros de entorno de Java, realice los siguientes pasos:

1. En Identity Console, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores**.
2. Haga clic en **Parámetros del entorno Java** en **Configuración del conjunto de controladores** para visualizar la página de propiedades que contiene los parámetros de entorno de Java.
3. Modifique los siguientes ajustes según sea necesario:

   Adiciones de vía de clase: especifique vías adicionales para que la JVM busque archivos de paquetes (`.jar`) y clases (`.class`). El uso de este parámetro es igual a utilizar el comando `java -classpath`. Cuando introduzca varias vías de clase, sepárelas con un punto y coma (;) para una JVM de Windows y dos puntos (:) para una JVM de UNIX o Linux.

   Opciones de JVM: especifique las opciones adicionales que se utilizarán con JVM. Consulte la documentación de JVM para obtener información sobre las opciones válidas.

   `DHOST_JVM_OPTIONS` es la variable de entorno correspondiente. Especifica los argumentos de JVM 1.2. Por ejemplo:

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Cada cadena de opción está separada por un espacio en blanco. Si una cadena de opción contiene un espacio en blanco, debe ir entre comillas dobles.

   La opción de atributo del conjunto de controladores tiene prioridad sobre la variable de entorno `DHOST_JVM_OPTIONS`. Esta variable de entorno se incluye al final de la opción de atributo del conjunto de controladores.

Tamaño de montón inicial: especifique el tamaño inicial (mínimo) del montón disponible para la JVM. El aumento del tamaño inicial del montón puede mejorar el tiempo de inicio y el rendimiento general. Utilice un valor numérico seguido de G, M o K. Si no se especifica ningún tamaño de letra, el valor por defecto es bytes. El uso de este parámetro es igual a utilizar el comando `java -Xms`.

`DHOST_JVM_INITIAL_HEAP` es la variable de entorno correspondiente. Especifica el tamaño inicial del montón de JVM mediante un número decimal de bytes. Tiene prioridad sobre la opción de atributo del conjunto de controladores.

Consulte la documentación de JVM para obtener información acerca del tamaño de montón inicial por defecto de JVM.

Tamaño máximo del montón: especifique el tamaño máximo del montón disponible para la JVM. Utilice un valor numérico seguido de G, M o K. Si no se especifica ningún tamaño de letra, el valor por defecto es bytes. El uso de este parámetro es igual a utilizar el comando `java -Xmx`.

`DHOST_JVM_MAX_HEAP` es la variable de entorno correspondiente. Especifica el tamaño máximo del montón de JVM mediante un número decimal de bytes. Tiene prioridad sobre la opción de atributo del conjunto de controladores.

Consulte la documentación de JVM para obtener información acerca del tamaño máximo del montón por defecto de JVM.

4 Haga clic en (Aceptar) para guardar los cambios.

5 Reinicie el repositorio seguro de identidades para aplicar los cambios.

Gestión de una lista de atributos con valor

Para añadir atributos a la lista de atributos con valor de un conjunto de controladores específicos, realice los siguientes pasos:

1 En Identity Console, seleccione el módulo **Gestión de objetos**.

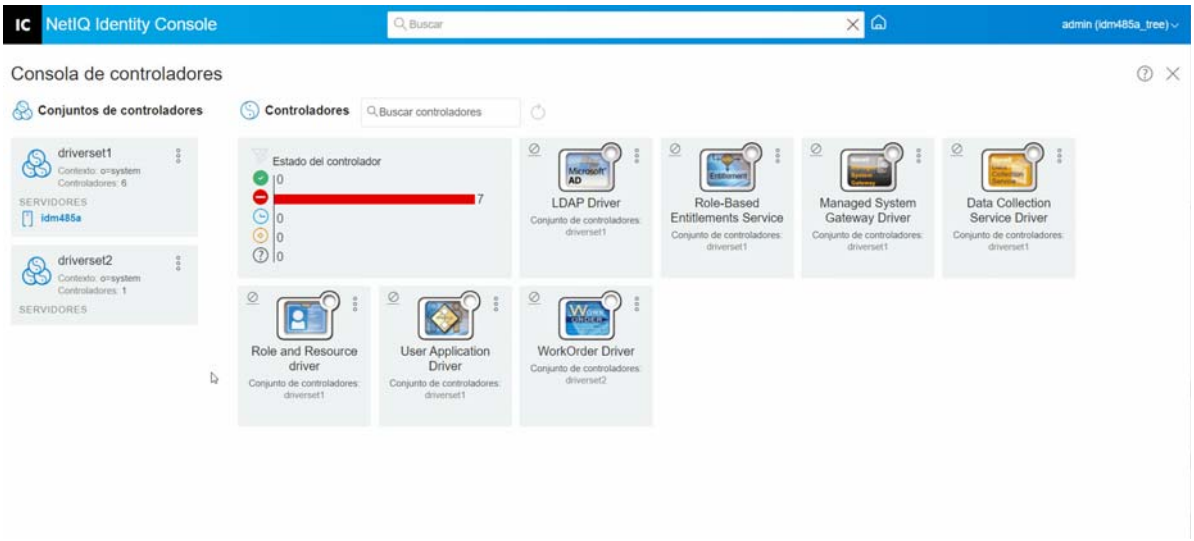
2 Seleccione el tipo **DirXML-DriverSet** en la lista desplegable y haga clic en el botón Buscar.

3 Haga clic en el conjunto de controladores adecuado en la lista de búsqueda.

4 Para añadir atributos sin valor a la lista de atributos con valor, haga clic en el icono junto a **Atributos con valor** y seleccione los atributos sin valor adecuados en la lista.

5 Una vez que haya terminado, haga clic en **Aceptar**.

Figura 22-1 *Gestión de los parámetros de configuración del conjunto de controladores*



Gestión de tareas para conjuntos de controladores

Identity Console permite programar eventos mediante la opción Tareas para todos los controladores que residan en el conjunto de controladores correspondiente.

La página Programador de tareas contiene el nombre y la descripción de la tarea, si la tarea está habilitada o inhabilitada y cuándo está programada para ejecutarse. Haga clic en el nombre de la tarea para abrir la página Tareas. Haga clic en el icono Habilitar/inhabilitar ubicado debajo de la columna Habilitado para habilitar o inhabilitar la tarea. Haga clic en la descripción de la tarea para verla por completo.

Para acceder a la página Tareas, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > pestaña **Avanzado** en la página principal de Identity Console. La pestaña Tareas contiene una tabla en la que se muestran los objetos de tarea existentes del controlador seleccionado, que aparece con su nombre completo en la entrada del controlador.

La página Programador de tareas permite realizar las siguientes tareas:

- **Crear la tarea**: haga clic en el icono + para crear una nueva tarea.

  En la ventana emergente **Nueva tarea**, realice los siguientes pasos para crear una nueva tarea:

  1. Especifique el nombre de la tarea.
  2. Seleccione el tipo de tarea.
  3. Haga clic en el icono y seleccione el servidor en el que desea ejecutar la tarea en la lista de servidores disponibles. De lo contrario, especifique un nombre de servidor y, a continuación, seleccione el servidor.
  4. Haga clic en el botón **Crear**.

- **Iniciar la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono ▷.

- **Detener la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono  .
- **Habilitar la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono  .
- **Inhabilitar la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono  .
- **Obtener estado**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono  .
- **Suprimir la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono  .

Haga clic en una tarea para acceder a la página **Job Property** (Propiedad de tarea). Aquí puede configurar cómo desea que se ejecute la tarea.

General: muestra el nombre de clase de Java de la tarea. Utilice esta página para habilitar o inhabilitar la tarea, suprimir la tarea después de que se ejecute, seleccionar el servidor o los servidores en los que debe ejecutarse esta tarea, especificar el servidor de correo electrónico, y asignar a la tarea un nombre de visualización y una descripción diferentes.

Programa: le permite definir cuándo desea ejecutar la tarea. Especifique un valor en "Iniciar tarea a las" para definir la hora y establecer si la tarea se ejecutará con periodicidad diaria, semanal, mensual o anual. También puede personalizar cuándo desea ejecutar la tarea, o bien habilitar el conmutador para que la tarea se ejecute manualmente.

Ámbito: permite definir los objetos a los que se aplica esta tarea. Un objeto puede ser un contenedor, un grupo dinámico, un grupo o una hoja. Haga clic en Añadir para seleccionar el objeto al que desea aplicar esta tarea. Puede utilizar el botón Examinar para seleccionar un objeto y, a continuación, hacer clic en Aceptar. Para eliminar un objeto de la lista Ámbito, seleccione un objeto Ámbito. Para ello, haga clic en el recuadro situado a la izquierda del objeto DN y, a continuación, haga clic en Eliminar.

Una vez que se haya añadido el objeto, selecciónelo para visualizar más opciones. Si selecciona un objeto Grupo, tiene la opción de aplicar la tarea a los componentes del grupo o solo al grupo. Si selecciona un objeto Contenedor, tiene la opción de aplicar la tarea a todos los descendientes de ese contenedor, a todos los hijos del contenedor o solo al contenedor.

Parámetros: permite añadir parámetros adicionales a la tarea y ver los parámetros tal y como están configurados actualmente. Estos parámetros cambian en función del tipo de tarea seleccionada.

Resultados: permite definir lo que se desea hacer con los resultados de la tarea. La página Resultados se divide en dos partes, Resultado intermedio y Resultado final, con los siguientes resultados permitidos: Correcto, Advertencia, Error y Cancelado. A la derecha de la columna Resultados, se encuentra la columna Acción. Al hacer clic en la columna Acción, puede definir el modo en que desea que se le notifique cada resultado. Entre las acciones, se incluyen el envío de resultados de una auditoría o el envío de un mensaje de correo electrónico cuando se complete el resultado. Si no se selecciona ninguna opción, no se realizará ninguna acción para el resultado.

En la pestaña **Seguimiento**, puede configurar el seguimiento de un controlador específico. Para obtener más información, consulte “Configuración del nivel de seguimiento” en la página 174.

Gestión de bibliotecas para un conjunto de controladores específico

Los objetos de biblioteca almacenan varias directivas y otros recursos compartidos por uno o varios controladores. Se puede crear un objeto de biblioteca en un objeto Conjunto de controladores o en cualquier contenedor de eDirectory. Pueden existir varias bibliotecas en un árbol de eDirectory. Los controladores pueden hacer referencia a cualquier biblioteca del árbol siempre que el servidor en el que se ejecute el controlador contenga una réplica de lectura/escritura o principal del objeto de biblioteca.

Las hojas de estilo, las directivas, las reglas y otros objetos de recursos se pueden almacenar en una biblioteca y se puede hacer referencia a ellos mediante uno o varios controladores.

Mediante el módulo Gestión de bibliotecas, puede realizar las siguientes tareas:

- “Visualización y supresión de una biblioteca existente” en la página 146
- “Visualización y supresión de objetos de la biblioteca” en la página 146

Visualización y supresión de una biblioteca existente

Para ver y suprimir una biblioteca existente, realice los siguientes pasos:

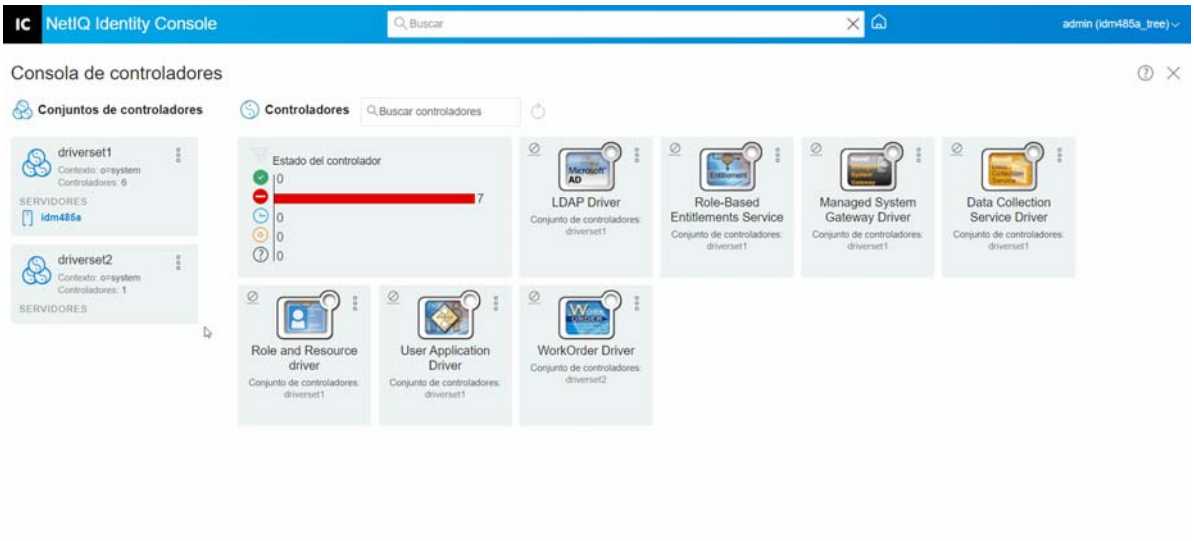
1. En Identity Console, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Avanzado** > **Bibliotecas**.
2. Seleccione la biblioteca adecuada en la lista.
3. Haga clic en el icono  . Haga clic en **Aceptar** para confirmar.

Visualización y supresión de objetos de la biblioteca

Puede ver y suprimir directivas y tablas de asignación de objetos de biblioteca. Para suprimir objetos, realice los siguientes pasos:

1. En Identity Console, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Avanzado** > **Bibliotecas**.
2. Haga clic en la biblioteca adecuada en la lista.
3. Para suprimir directivas, seleccione la pestaña **Directivas**.
4. Seleccione la directiva adecuada en la lista y haga clic en el icono  .
5. Para suprimir tablas de asignación, seleccione la pestaña **Tablas de asignación**.
6. Seleccione la tabla de asignación adecuada en la lista y haga clic en el icono  .
7. Haga clic en **Aceptar** para confirmar.

Figura 22-2 *Gestión de tareas y bibliotecas para los conjuntos de controladores*



Configuración de los niveles de registro y seguimiento de los conjuntos de controladores

Para configurar el registro y el seguimiento de los conjuntos de controladores, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > pestaña **Configuración de registro y seguimiento** de la página principal de Identity Console. Esta sección se divide en las siguientes categorías:

- “Configuración del nivel de registro” en la página 147
- “Configuración del nivel de seguimiento” en la página 148
- “Seguimiento del guion DirXML” en la página 149

Configuración del nivel de registro

Cada conjunto de controladores tiene un campo de nivel de registro en el que puede definir el nivel de errores del que debería realizarse un seguimiento. El nivel que indique aquí determina qué mensajes habrá disponibles en los registros. Por defecto, el nivel de registro se define para realizar un seguimiento de los mensajes de error. (Esto también incluye los mensajes irrecuperables). Para realizar un seguimiento de los tipos de mensajes adicionales, cambie el nivel de registro. Para configurar el nivel de registro, seleccione En Identity Console y elija **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Configuración de registro y seguimiento** > **Nivel de registro**. En la tabla siguiente, se describen los ajustes del nivel de registro:

Opción	Descripción
Desactive el registro en los registros de conjunto de controladores, suscriptor y editor	Desactiva todos los registros de todos los controladores del objeto Conjunto de controladores, y los canales de suscriptor y editor.

Opción	Descripción
Número máximo de entradas en el registro (50-500)	Número de entradas en el registro. El valor por defecto es 50.
Niveles de registro	Se pueden seleccionar los siguientes niveles de registro: ◆ **Registrar errores**: registra solo errores. ◆ Registrar errores y advertencias: registra errores y advertencias. ◆ **Registrar eventos específicos**: registra los eventos seleccionados. Si se selecciona esta opción, se habilitará la siguiente lista de eventos: ◆ **Eventos del motor de metadirectorio** ◆ **Eventos de estado** ◆ **Eventos de operación** ◆ **Eventos de transformación** ◆ **Eventos de provisión de credenciales** ◆ **Actualizar solo la última hora de registro**: actualiza la última hora de registro. ◆ **Desactivar registro**: desactiva el registro del controlador.

Configuración del nivel de seguimiento

Puede configurar el seguimiento de un conjunto de controladores específico. En función del nivel de seguimiento especificado para un conjunto de controladores, el seguimiento muestra los eventos relacionados con los controladores cuando el motor procesa los eventos. El nivel de seguimiento del controlador solo afecta al controlador o al conjunto de controladores en los que se ha definido el seguimiento. Si utiliza el cargador remoto, el archivo de seguimiento del cargador remoto se define directamente en el cargador remoto y solo contiene el seguimiento de shim del controlador.

Para configurar el seguimiento para un conjunto de controladores, seleccione **Seguimiento de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Configuración de registro y seguimiento** > pestaña **Seguimiento**. En la tabla siguiente, se describen los ajustes de seguimiento:

Parámetro	Controlador
Nivel de seguimiento	A medida que aumenta el nivel de seguimiento del controlador, aumenta la cantidad de información que aparece en el seguimiento. El nivel uno de seguimiento muestra errores, pero no su causa. Si desea ver la información de sincronización de contraseñas, defina el nivel de seguimiento en cinco. Si selecciona **Usar el ajuste del conjunto de controladores**, el valor se obtiene del conjunto de controladores.

Parámetro	Controlador
Nivel de seguimiento XSL	El seguimiento muestra eventos XSL. Defina este nivel de seguimiento solo al resolver problemas con hojas de estilo XSL. Si no desea ver la información de XSL, defina el nivel en cero.
Puerto de depuración de Java	Permite a los desarrolladores conectar un depurador de Java. Reinicie el repositorio seguro de identidades después de conectar el depurador de Java.
Archivo de seguimiento	Especifique el nombre de archivo y la ubicación en la que se escribirá la información de Identity Manager para el controlador seleccionado. Si selecciona **Usar el ajuste del conjunto de controladores**, el valor se obtiene del conjunto de controladores.
Codificación de archivos de seguimiento	El archivo de seguimiento utiliza la codificación por defecto del sistema. Si lo desea, puede especificar otra codificación. Si selecciona **Usar el ajuste del conjunto de controladores**, el valor se obtiene del conjunto de controladores.
Límite de tamaño de archivo de seguimiento	Permite definir un límite para el archivo de seguimiento de Java. Si define el tamaño de archivo como ilimitado, el archivo aumentará de tamaño hasta que no quede espacio en el disco. **Nota:** Si se especifica el límite de tamaño de archivo, el archivo de seguimiento se crea en varios archivos. Identity Manager divide automáticamente el tamaño máximo de archivo por diez y crea diez archivos independientes. El tamaño combinado de estos archivos es igual al tamaño máximo del archivo de seguimiento. Si selecciona **Usar el ajuste del conjunto de controladores**, el valor se obtiene del conjunto de controladores.

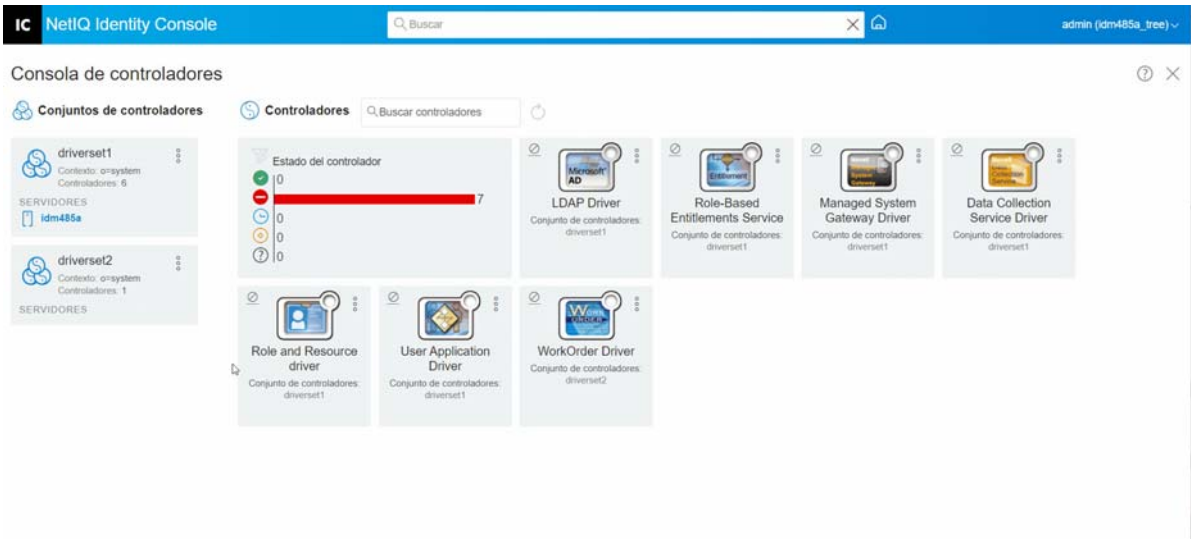
Seguimiento del guion DirXML

La opción Seguimiento del guion DirXML permite seleccionar un nivel de seguimiento para un conjunto de controladores. La selección se aplica a todas las directivas del conjunto de controladores. Se pueden seleccionar las siguientes opciones de seguimiento del guion DirXML:

- Todo el seguimiento de guiones DirXML habilitado
- Todo el seguimiento de guiones DirXML inhabilitado
- Seguimiento activado de regla de guion DirXML
- Seguimiento desactivado de regla de guion DirXML

Haga clic en (Aceptar) para guardar los cambios.

Figura 22-3 *Gestión de los niveles de registro y seguimiento de los conjuntos de controladores*



Gestión del Inspector y las estadísticas del conjunto de controladores

Puede utilizar el Inspector del conjunto de controladores para ver información detallada acerca de los objetos asociados a un conjunto de controladores. Esta sección se divide en las siguientes categorías:

- "Visualización de estadísticas del conjunto de controladores" en la página 150
- "Visualización de información de versión" en la página 151
- "Visualización de estadísticas de asociación" en la página 152

Visualización de estadísticas del conjunto de controladores

Puede utilizar el portal de Identity Console para ver diversas estadísticas de un único controlador o de un conjunto de controladores completo. Entre las estadísticas, se incluyen el tamaño del archivo de caché, el tamaño de las transacciones sin procesar del archivo de caché, las transacciones más antiguas y más recientes y el número total de transacciones sin procesar por categoría (adición, eliminación, modificación, etc.). Para ver las estadísticas del conjunto de controladores:

1. En Identity Console, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Inspector y estadísticas** > **Estadísticas**.
2. Seleccione el servidor adecuado en la lista desplegable.

   Aparecerá una página que permite ver las estadísticas de todos los controladores incluidos en el conjunto de controladores.

   - Para actualizar las estadísticas, haga clic en el icono .
   - Para cerrar las estadísticas de un controlador, haga clic en el botón situado en la esquina superior derecha de la ventana de estadísticas del controlador.

- Para visualizar las estadísticas de todos los controladores, haga clic en **Acciones** > **Mostrar todo**.
- Para contraer la lista de transacciones sin procesar de un controlador, haga clic en el botón ^ situado encima de la lista. Para contraer la lista de transacciones sin procesar de todos los controladores, haga clic en **Acciones** > **Contraer todas las transacciones**.
- Para expandir la lista de transacciones, haga clic en el botón v. Para expandir la lista de transacciones sin procesar de todos los controladores, haga clic en **Acciones** > **Expandir todas las transacciones**.
- Para cerrar la consola de estadísticas de los controladores inhabilitados, haga clic en **Acciones** y seleccione **Cerrar controladores inhabilitados**.

Visualización de información de versión

El motor de Identity Manager, los shims del controlador y los archivos de configuración del controlador contienen un número de versión independiente. La opción Descubrimiento de versiones de Identity Console le ayuda a encontrar las versiones del motor de Identity Manager y de shims del controlador. Los archivos de configuración del controlador contienen sus propias convenciones de denominación. Para ver la información de versión:

1. En Identity Console, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Inspector y estadísticas** > **Descubrimiento de versiones**.
2. Ver una visualización de nivel superior de la información de versiones:
   - El árbol de eDirectory en el que se ha autenticado.

     Nota: Se hace referencia a eDirectory como el repositorio seguro de identidades en el entorno de Identity Manager.

   - El conjunto de controladores que ha seleccionado.
   - Los servidores asociados al conjunto de controladores.

     Si el conjunto de controladores está asociado a dos o más servidores, puede ver la información de Identity Manager en cada servidor.
   - Controladores
3. Haga clic en el icono **Ver** para visualizar una representación textual de la misma información incluida en la vista de nivel superior.
4. Haga clic en el botón Exportar para exportar y guardar el texto en un archivo de la unidad local o de red.

Visualización de estadísticas de asociación

Mediante la función Estadísticas de asociación de Identity Manager, puede encontrar los detalles de asociación de las identidades gestionadas por Identity Manager. Identity Manager utiliza las estadísticas de asociación para obtener el recuento de asociaciones de los controladores de esta solución.

Para obtener objetos activos, inactivos y gestionados del sistema de un controlador, ejecute la tarea de estadísticas de asociación. Puede programar la tarea de estadísticas de asociación con periodicidad diaria, semanal, mensual o anual. Por defecto, la tarea está programada para ejecutarse todas las semanas.

En la consola Estadísticas de asociación, se muestra los detalles de la asociación. También puede ver los detalles mediante la exportación de las asociaciones a un archivo.

Nota

- El número de asociaciones de los controladores es por servidor. Si un objeto está asociado a más de un controlador, el recuento de asociaciones se calcula de forma exclusiva para cada controlador.
- Si tiene más de 200 000 asociaciones, es recomendable definir el tamaño máximo del montón para el controlador en 2 GB o más. Para obtener información acerca de cómo definir el tamaño del montón, consulte "Configuración de los parámetros de entorno de Java" en la página 142.

Para ver las estadísticas de asociación:

1. En Identity Console, seleccione **Administración de IDM** > **haga clic en el menú contextual (tres puntos) del conjunto de controladores adecuado** > **Propiedades del conjunto de controladores** > **Inspector y estadísticas** > **Estadísticas de asociación**.
2. Seleccione el servidor para el que desea ejecutar las estadísticas de asociación.
3. El recuento de asociaciones muestra los resultados calculados anteriormente.

   Identity Console muestra el recuento de asociaciones de los objetos activos, inactivos y gestionados del sistema de todos los controladores asociados al conjunto de controladores.

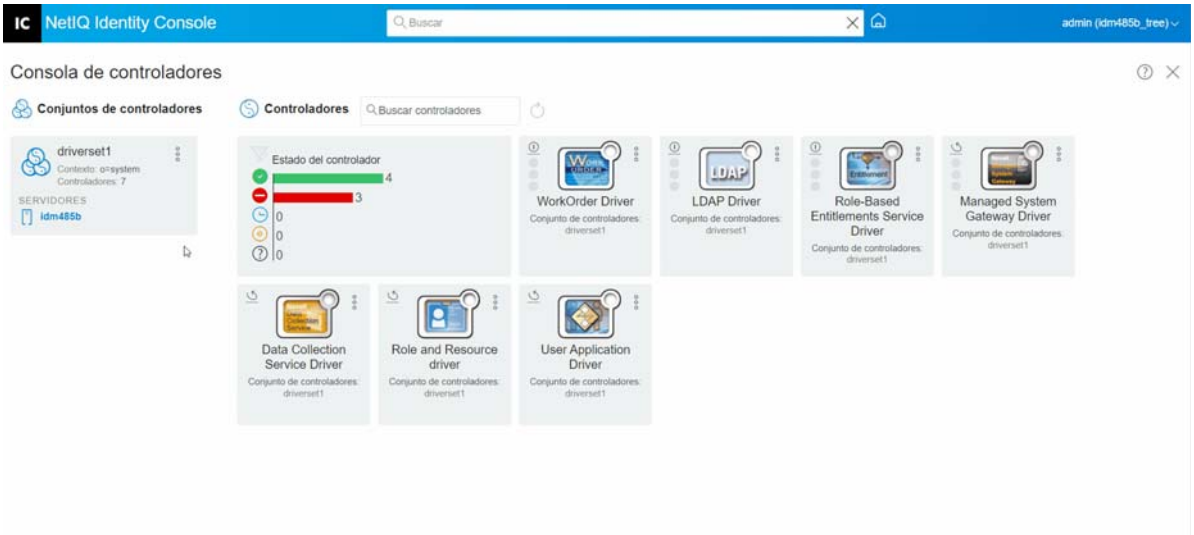
   Identity Console considera los grupos y las unidades organizativas como objetos gestionados del sistema. Identity Console considera un objeto como inactivo si el atributo `Entrada inhabilitada` del objeto se ha definido en verdadero y el objeto no se ha modificado en los últimos 120 días. Todos los objetos restantes se consideran objetos gestionados activos.
4. Haga clic en el icono para obtener los resultados actualizados.

   Cuando un controlador está inhabilitado en el servidor, Identity Console no lo muestra en la consola.
5. Haga clic en el icono para exportar los detalles del sistema y el recuento de asociaciones de los controladores asociados al servidor.
6. Para exportar los objetos asociados a un controlador específico, haga clic en junto a los objetos necesarios y guarde el archivo.

Nota: En el caso de los controladores de dispersión, solo se exportan objetos exclusivos. Si un objeto está asociado a varias instancias de un controlador de dispersión, Identity Console muestra todos los recuentos de asociaciones en la consola. Sin embargo, si decide exportar los objetos de un archivo, Identity Console solo exporta los objetos exclusivos.

7 Haga clic en **Acciones**y seleccione la opción necesaria para organizar el panel de recuento de asociaciones.

Figura 22-4 *Gestión de las estadísticas del conjunto de controladores*



23 Gestión de las propiedades de los controladores

En esta sección, se proporciona información acerca de las propiedades comunes a todos los controladores. Esto incluye todas las propiedades (Contraseña con nombre, Valores de control del motor, Nivel de registro, etc.).

Se muestra la información de activación de un controlador, que le recuerda una acción para activar el controlador de caducidad.

Para modificar la configuración del controlador, realice los siguientes pasos:

1. Haga clic en la pestaña **Controladores** de la pantalla de inicio de Identity Console.
2. Haga clic en el mosaico del controlador correspondiente para ver la página de configuración del controlador.

   Por defecto, aparece la página **Parámetros de conexión**. Las opciones de configuración del controlador se dividen en las siguientes categorías:

Parámetros de conexión

Los parámetros de conexión controlan si el controlador debe ejecutarse de forma local o remota.

- **Java:** utilice esta opción para especificar el nombre de la clase de Java para la que se va a crear una instancia para el componente shim del controlador. Esta clase se encuentra en el directorio de clases como un archivo de clases o en el directorio `lib` como un archivo `.jar`. Seleccione esta opción para ejecutar el controlador localmente. También debe especificar la contraseña del objeto Controlador y el límite de caché del controlador. Puede definir una nueva contraseña. Para ello, haga clic en el enlace **Definir contraseña**.

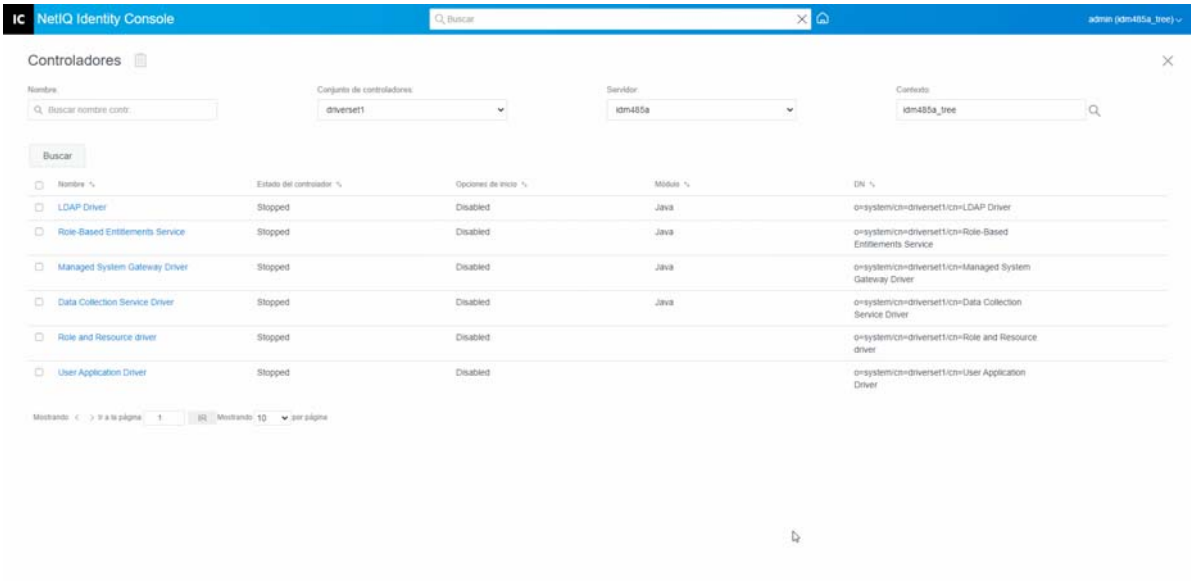
  Por ejemplo, `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`
- **Nativo:** esta opción se utiliza para especificar el nombre del archivo `.dll` que se ha desarrollado en el lenguaje nativo (como, por ejemplo, C++) para el controlador. También debe especificar la contraseña del objeto Controlador y el límite de caché del controlador. Puede definir una nueva contraseña. Para ello, haga clic en el enlace **Definir contraseña**.

  Por ejemplo, `addriver.dll`.

- **Conectar al cargador remoto:** esta opción se utiliza cuando el controlador se conecta de forma remota al sistema conectado. Si esta opción está seleccionada, debe especificar las siguientes subopciones:
  - **Parámetros de conexión del conector remoto**: incluye información del entorno del cargador remoto como, por ejemplo, el nombre de host, el puerto de conexión, etc.
  - **Contraseña del cargador remoto**: la contraseña del cargador remoto.
  - **Contraseña del objeto Controlador**: permite especificar una contraseña para el objeto Controlador. Si utiliza el cargador remoto, debe introducir una contraseña en esta página. El cargador remoto utiliza esta contraseña para autenticarse en el shim del controlador remoto.
- **Autenticación**: los parámetros de autenticación se utilizan para autenticar los servidores del motor de Identity Manager y el cargador remoto. Especifique los parámetros siguientes:
  - **ID de autenticación**: especifique un ID de aplicación de usuario. Este ID se utiliza para transferir la información de suscripción del repositorio seguro de identidades a la aplicación.
  - **Contexto de autenticación**: especifique el nombre o la dirección IP del servidor con el que debe comunicarse el shim de la aplicación.
  - **Contraseña de la aplicación**: la opción para definir la contraseña de autenticación de la aplicación.

Cuando haya terminado, haga clic en el icono para guardar la configuración.

Figura 23-1 *Gestión de parámetros de conexión*



Configuración del controlador

En la sección de configuración del controlador, puede configurar los parámetros específicos del controlador, los valores de control del motor, los valores de configuración global, etc. Al cambiar los parámetros del controlador, se ajusta el comportamiento del controlador para que se adapte al entorno de red. Esta sección se divide en las siguientes categorías:

Parámetros del controlador

Los parámetros del controlador se dividen en Ajustes del controlador, Ajustes de suscriptor y Ajustes del editor. Estos parámetros se rellenarán en función de la configuración del controlador. Para obtener más información sobre los parámetros del controlador, consulte la guía específica del controlador en la documentación de controladores de Identity Manager.

Una vez que haya terminado, puede hacer clic en  para guardar los parámetros. Si desea definir los parámetros con su valor por defecto, haga clic en el icono  . Para modificar la configuración del controlador mediante el archivo xml, haga clic en el icono  .

Valores de configuración global

Muestra una lista ordenada de objetos Configuración global. Los objetos contienen definiciones de extensión de GCV para el controlador que carga Identity Manager durante el inicio del controlador. Puede ver o modificar los objetos de la pestaña **Valores de configuración global** mediante el editor XML. Haga clic en el icono  para guardar los GCV. Para actualizar la lista de GCV, haga clic en el icono  . Para suprimir GCV, seleccione el objeto GCV adecuado y haga clic en el icono  .

Valores de control del motor

Los valores de control del motor permiten cambiar determinados comportamientos por defecto del motor de Identity Manager. Solo se puede acceder a los valores si un servidor está asociado al objeto Conjunto de controladores.

Opción	Descripción
Intervalo de reintento del canal de suscriptor en segundos	El intervalo de reintento del canal de suscriptor controla la frecuencia con la que el motor de Identity Manager vuelve a intentar el procesamiento de una transacción almacenada en caché después de que el objeto Suscriptor del shim de la aplicación devuelva un estado de reintento.
Formato completo de los valores de atributos de sintaxis de DN	La especificación completa para los valores de atributos de sintaxis de DN controla si los valores de los valores de atributo de sintaxis de DN se presentan en forma de barra inclinada de forma completa o incompleta. Un ajuste de verdadero indica que los valores se presentan de forma completa.
Formato completo de eventos de cambio de nombre	El formato completo de eventos de cambio de nombre controla si la parte del nuevo nombre de los eventos procedentes del repositorio seguro de identidades se presenta al canal de suscriptor con calificadores de tipos. Por ejemplo, CN=. Un ajuste de verdadero indica que los nombres se presentan de forma completa.
Tiempo máximo de espera de replicación de eDirectory en segundos	Este ajuste controla el tiempo máximo que el motor de Identity Manager espera a que un cambio específico se repita entre la réplica local y una remota. Esto solo afecta a las operaciones en las que el motor de Identity Manager debe ponerse en contacto con un servidor remoto de eDirectory del mismo árbol para realizar una operación y puede que tenga que esperar hasta que se haya replicado algún cambio en el servidor remoto o desde él antes de que pueda completarse la operación (por ejemplo, el objeto se mueve cuando el servidor de Identity Manager no contiene la réplica principal del objeto movido; operaciones de derechos del sistema de archivos para usuarios creados a partir de una plantilla).
Utilizar un modo de compatibilidad con versiones anteriores no conforme para XSLT	Este control define el procesador XSLT utilizado por el motor de Identity Manager en un modo compatible con versiones anteriores. El modo de compatibilidad con versiones anteriores permite que el procesador XSLT utilice uno o varios comportamientos no conformes a XPath 1.0 ni XSLT 1.0. Esto se realiza para garantizar la compatibilidad con las hojas de estilo de DirXML existentes que dependen de los comportamientos no estándar. Por ejemplo, el comportamiento de XPath "!=" cuando un operando es un conjunto de nodos y el otro operando no es un conjunto de nodos es incorrecto en las versiones de DirXML hasta Identity Manager 2.0, inclusive. Este comportamiento se ha corregido. Sin embargo, el comportamiento corregido está inhabilitado por defecto mediante este control a favor de la compatibilidad de versiones anteriores con las hojas de estilo de DirXML existentes.
Número máximo de objetos de aplicación que se deben migrar al mismo tiempo	Este control se utiliza para limitar el número de objetos de aplicación que el motor de Identity Manager solicita desde una aplicación durante una única consulta que se realiza como parte de una operación de migración de objetos desde la aplicación. Si se detectan errores de tipo java.lang.OutOfMemoryError durante una operación de migración desde la aplicación, este número debe ser inferior al valor por defecto. El puerto por defecto es el 50. **Nota:** Este control no limita el número de objetos de aplicación que se pueden migrar; simplemente limita el tamaño del lote.

Opción	Descripción
Definir creatorsName en objetos creados en el repositorio seguro de identidades	Este control lo utiliza el motor de Identity Manager para determinar si el atributo creatorsName debe definirse en el DN de este controlador en todos los objetos creados en el repositorio seguro de identidades por este controlador. La definición del atributo creatorsName permite identificar fácilmente los objetos creados por este controlador, pero también conlleva una reducción del rendimiento. Si no se define, el atributo creatorsName utiliza por defecto el DN del objeto Servidor NCP que aloja el controlador.
Escribir asociaciones pendientes	Este control determina si el motor de Identity Manager escribe una asociación pendiente en un objeto durante el procesamiento del canal de suscriptor. La escritura de una asociación pendiente no tiene muy pocas ventajas o ninguna y puede reducir el rendimiento. No obstante, existe la opción de activarla para garantizar la compatibilidad con versiones anteriores.
Usar valores de eventos de contraseña	Este control determina el origen del valor notificado del atributo nspmDistributionPassword para los eventos de adición y modificación del canal de suscriptor. Al definir este control como falso, se obtiene el valor actual de nspmDistributionPassword y se notifica como el valor del evento de atributo. Esto significa que solo está disponible el valor de contraseña actual. Este es el comportamiento por defecto. Si se define como verdadero, el valor registrado con el evento de eDirectory se descifra y se notifica como el valor del evento de atributo. Esto significa que tanto el valor de contraseña anterior (si existe) como el valor de contraseña de sustitución en el momento del evento están disponibles. Esto resulta útil para sincronizar contraseñas con determinadas aplicaciones que requieren la contraseña anterior para habilitar la definición de una contraseña nueva.
Reintentar eventos fuera de banda	Este control determina si se deben intentar realizar de nuevo o no los eventos de sincronización fuera de banda si se recibe el estado de **reintento** del evento de sincronización fuera de banda. Si el control se define como falso, no se intenta realizar de nuevo la sincronización fuera de banda. Si se define en verdadero, se intenta realizar de nuevo la sincronización fuera de banda hasta que se complete correctamente.
Utilizar el motor ECMAScript de Rhino	Determina si el motor de Identity Manager utiliza el motor ECMAScript de Rhino. El motor utiliza Rhino como motor ECMAScript por defecto. Este control es **verdadero** por defecto, si se establece en **falso**, el motor utiliza el guion Nashorm.

Opción	Descripción
Habilitar canal de servicio de suscriptor	Determina si el motor de Identity Manager procesa las consultas fuera de banda en el canal del servicio de suscriptor del controlador. Algunos ejemplos habituales de estas consultas son la actualización de asignación de código, la recopilación de datos y las consultas activadas desde dxcmd. Si este control se define en verdadero, el canal procesa por separado estas consultas sin interrumpir el procesamiento normal de los eventos. Actualmente, este control solo está disponible para su uso con el controlador de dispersión JDBC (habilitado por defecto).
Habilitar informes de estado de sincronización de contraseñas	Este control determina si el motor de Identity Manager informa del estado de los eventos de cambio de contraseña del canal de suscriptor. Si se informa del estado de los eventos de cambio de contraseña del canal de suscriptor, aplicaciones como la aplicación de usuario de Identity Manager pueden supervisar el progreso de sincronización de un cambio de contraseña que debe sincronizarse con la aplicación conectada.
Combinar valores del objeto de plantilla con los de la operación de adición	Este valor determina si el motor de Identity Manager combina valores, como los de una plantilla de creación y una operación de adición, al realizar la operación de adición. Si se define el valor en verdadero, se utilizarán los valores de atributo multivalente de la plantilla, además de los valores del mismo atributo especificados en la operación de adición. Si se define el valor en falso, se omitirán los valores de la plantilla si hay valores para el mismo atributo especificado en la operación de adición.
Permitir retorno de bucle de eventos del canal de editor al de suscriptor	Este valor determina si el motor de Identity Manager permite que un evento pase en bucle desde el canal de editor del controlador al canal de suscriptor. Si se define en falso, el motor de Identity Manager no permita que los eventos se repitan en bucle. Si se define en verdadero, el motor de Identity Manager permite que los eventos pasen en bucle del canal de editor al de suscriptor.
Revertir al comportamiento de valores de pertenencia a grupos calculados	Este valor determina el método utilizado por el motor de Identity Manager al realizar acciones de lectura y búsqueda relacionadas con la pertenencia a grupos. Si se establece este valor en falso (el ajuste por defecto), el motor de Identity Manager, al leer o buscar los atributos Miembro y Miembro de grupo de los objetos del repositorio seguro de identidades, devolverá solo aquellos valores que sean "estáticos". Los valores estáticos son objetos que han recibido la pertenencia al grupo por asignación directa al grupo en lugar de por la asignación heredada a través de un grupo anidado. Si se define este valor en verdadero, el motor de Identity Manager vuelve al método utilizado antes de Identity Manager 3.6. En estas versiones anteriores, la búsqueda del motor de Identity Manager de los atributos Miembro y Miembro de grupo recuperaba todos los valores "calculados". Los valores calculados incluyen objetos que son 1) miembros asignados estáticamente o 2) miembros asignados dinámicamente en virtud de los cálculos de jerarquía de grupos anidados utilizados por eDirectory. Una búsqueda del atributo Componente de grupo devuelve todos los objetos que se han asignado directamente al grupo o a los que se ha asignado la pertenencia a través de un grupo anidado.

Opción	Descripción
Tiempo máximo de espera para el apagado del controlador en segundos	Este ajuste controla el tiempo máximo que el motor de Identity Manager espera a que se apague el canal de editor del controlador. Si el controlador no se apaga en el intervalo de tiempo especificado, el motor de Identity Manager lo finalizará.
Metacaracteres de escape de expresión regular	Este control determina los metacaracteres que se utilizarán con un carácter de escape mientras se expande la variable local cuando se utilice en un contexto de expresión regular. Todos los caracteres con carácter de escape deben añadirse como una lista separada por comas para este valor de control. Si un metacarácter no está presente en el valor de control, no se utilizará con un carácter de escape durante la expansión de variables locales que contengan una expresión regular. Al utilizar, asegúrese de lo siguiente: ◆ El valor no se ha dejado vacío. Por defecto, se rellena con ***$***. Este carácter es necesario para la expansión de variables locales. ◆ El valor debe ser una lista válida separada por comas (,); de lo contrario, se producirán errores durante la evaluación de la directiva. ◆ Para utilizar un carácter de escape para todos los metacaracteres, especifique "\,$,^,.,?,*,+,[,],(,),|" como valor. ◆ Si no es necesario utilizar un carácter de escape para un metacarácter, elimine este carácter del valor. ◆ Para usar un carácter de escape con un metacarácter, especifique el metacarácter con una barra diagonal inversa (\).
Omitir cambios de derechos de otros controladores	Este control determina si el motor de Identity Manager omite o procesa los cambios de derechos de otros controladores. El valor por defecto es Verdadero. Esto significa que el controlador omite automáticamente los cambios de derechos de otros controladores. Si este control se define en falso, este controlador almacenará en caché los cambios de derechos de otros controladores y los procesará.
Permitir retorno de bucle de eventos de derechos de cprs al canal de suscriptor	Este control determina si el motor de Identity Manager permite un retorno de bucle de un evento de derecho generado por una asignación CPRS al canal de suscriptor del controlador. El valor por defecto es Falso. Esto significa que el evento no regresa en bucle al canal de suscriptor. Si este control se define como verdadero, el evento pasará al canal de suscriptor del controlador.

Opciones de inicio

Las opciones de inicio permiten definir el estado del controlador cuando se inicia el servidor de Identity Manager.

- **Inicio automático**: el controlador se inicia cada vez que se arranca el servidor de Identity Manager.

- **Manual**: el controlador no se inicia durante el arranque del servidor de Identity Manager. El controlador debe iniciarse mediante el portal de Identity Console.
- **Inhabilitado**: el controlador tiene un archivo de caché que almacena todos los eventos. Si el controlador se define como Inhabilitado, este archivo se suprimirá y no se almacenará ningún evento nuevo en el archivo hasta que el estado del controlador cambie a Manual o Inicio automático.

Después de configurar la opción de inicio preferida, haga clic en el icono  para guardarla. Para restablecer la opción de inicio, haga clic en el icono  .

Contraseña con nombre

Identity Manager permite almacenar de forma segura varias contraseñas para un controlador. Esta función se conoce como contraseñas con nombre. A cada contraseña diferente se accede mediante una clave o un nombre.

Puede añadir contraseñas con nombre a un conjunto de controladores o a controladores individuales. Las contraseñas con nombre de un conjunto de controladores están disponibles para todos los controladores del conjunto. Las contraseñas con nombre de un controlador individual solo están disponibles para ese controlador.

Para utilizar una contraseña con nombre en una directiva de controlador, debe hacer referencia a ella por el nombre de la contraseña en lugar de utilizar la contraseña real; el motor de Identity Manager envía la contraseña al controlador. El método descrito en esta sección para almacenar y recuperar contraseñas con nombre se puede utilizar con cualquier controlador sin necesidad de realizar cambios en el shim del controlador.

Para añadir una contraseña con nombre nueva, haga clic en el icono  . Para eliminar una contraseña con nombre existente, haga clic en el icono  . Para guardar la lista, haga clic en el icono  .

Equivalentes de seguridad

Utilice la página Equivalencias de seguridad para ver o cambiar la lista de objetos a los que el controlador es explícitamente equivalente en seguridad. Este objeto tiene realmente todos los derechos de los objetos enumerados.

Puede añadir un nuevo objeto en la lista de equivalencias de seguridad. Para ello, haga clic en el icono  . Si añade o suprime un objeto de la lista, el sistema añade o suprime automáticamente este objeto en la propiedad "Seguridad igual a mí" de ese objeto. No es necesario añadir el Trustee (público) ni los contenedores padre de este objeto a la lista, ya que este objeto ya tiene los mismos valores de seguridad de forma implícita.

Para eliminar un objeto existente de esta lista, haga clic en el icono  . Para guardar la lista, haga clic en el icono .

Objetos excluidos

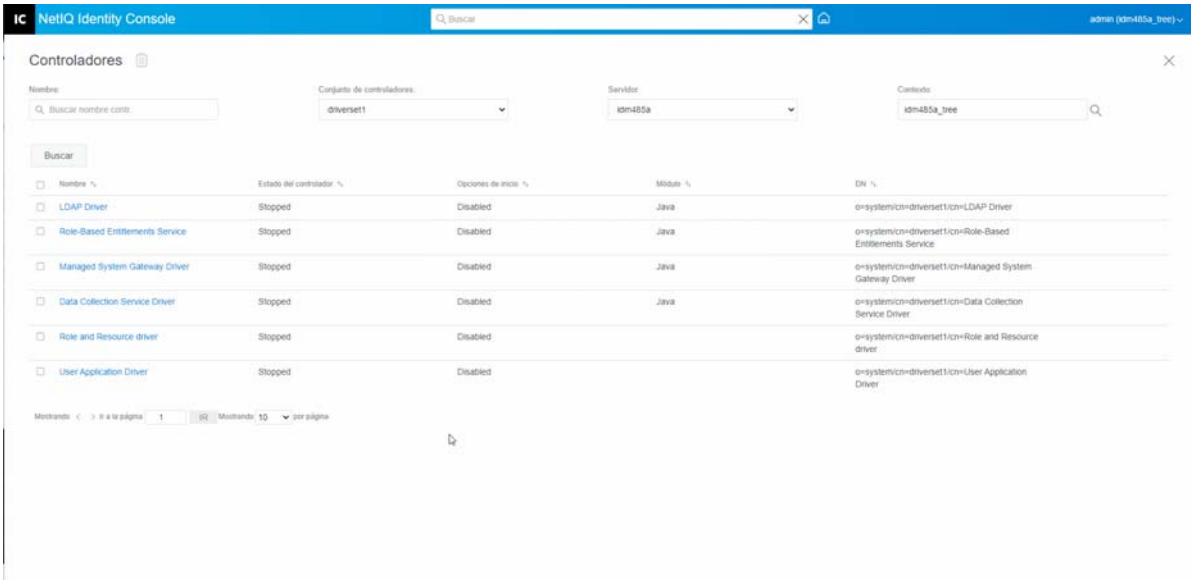
Utilice esta opción para crear una lista de objetos que no se replicarán en la aplicación. Es recomendable añadir todos los objetos que representen una función administrativa (por ejemplo, el objeto ADMIN) a esta lista. Puede añadir un objeto nuevo a esta lista. Para ello, haga clic en el icono +. Para eliminar un objeto existente de esta lista, haga clic en el icono 🗑. Para guardar la lista, haga clic en el icono ⬇.

Gestión de una lista de atributos con valor

Para añadir atributos a la lista de atributos con valor de un controlador específico, realice los siguientes pasos:

1. En Identity Console, seleccione el módulo **Gestión de objetos**.
2. Seleccione el tipo **Dir-XML-Driver** en la lista desplegable y haga clic en el botón Buscar.
3. Haga clic en el controlador adecuado en la lista de búsqueda.
4. Para añadir atributos sin valor a la lista de atributos con valor, haga clic en el icono + junto a **Atributos con valor** y seleccione los atributos sin valor adecuados en la lista.
5. Una vez que haya terminado, haga clic en **Aceptar**.

Figura 23-2 *Gestión de la configuración de los controladores*



Transformación y sincronización de datos

Esta sección se divide en las siguientes categorías:

- “Vista de sincronización de datos” en la página 164
- “Filtros de atributo de clase” en la página 166

- "Guion de ECMA" en la página 167
- "Asignación de atributo recíproco" en la página 167

Vista de sincronización de datos

La página de descripción general del controlador se divide en las siguientes categorías:

- "Filtro" en la página 164
- "Todas las directivas" en la página 164
- "Migrar datos en el repositorio seguro de identidades" en la página 165
- "Migrar datos del repositorio seguro de identidades" en la página 165
- "Sincronizar objetos" en la página 165
- "Seguimiento del guion DirXML" en la página 165

Filtro

Los filtros existentes en el controlador permiten especificar las clases y los atributos que una aplicación puede enviar y recibir en el repositorio seguro de identidades. Si desea que una clase específica se transfiera para que el motor del metadirectorio la procese, debe añadir la clase al filtro en el canal correspondiente. También puede filtrar los objetos según el valor de atributo específico que defina.

Para añadir las clases y los atributos que desea incluir para la sincronización y modificar el filtro del controlador, haga clic en **Filtro** en el canal Editor o Suscriptor.

Nota: En la representación gráfica de la descripción general, se muestran dos objetos independientes para el filtro de controladores en los canales Editor y Suscriptor. Aunque se muestran dos objetos, se utiliza el mismo filtro para ambos canales.

Todas las directivas

Por defecto, se muestra la página Todas las directivas. Puede importar una directiva existente en el contenedor. Para ello, haga clic en el icono . También puede eliminar cualquier directiva que no sea necesaria. Para seleccionar un nivel de seguimiento para el controlador, haga clic en el icono . Puede mover las directivas hacia arriba y hacia abajo en la lista mediante los iconos y .

Nota: Identity Console no admite la adición ni la distribución de nuevas directivas para controladores. Es recomendable utilizar iManager e Identity Designer para añadir e implantar directivas nuevas.

Migrar datos en el repositorio seguro de identidades

Esta tarea permite definir los criterios que utiliza Identity Manager para migrar objetos de una aplicación al repositorio seguro de identidades. Cuando se migra un objeto, el motor de metadirectorio aplica al objeto todas las directivas de concordancia, colocación y creación, así como el filtro de editor. Los objetos se migran al repositorio seguro de identidades en el orden especificado en la lista Clase. Puede llevar a cabo las siguientes tareas mediante esta opción:

1. **Añadir clases y atributos**: para añadir o eliminar las clases y los atributos que desea migrar, haga clic en el icono . A continuación, seleccione la clase y los atributos respectivos que desee añadir. Después de seleccionar la clase y los atributos, haga clic en **Añadir** para guardar los cambios.
2. **Editar valor de atributo**: para cambiar el valor del atributo de migración que especificó al editar la lista, haga clic en el icono Editar atributo .
3. **Reordenar la lista de clases**: utilice los botones y para cambiar el orden de las clases de la lista. Los objetos se migran al repositorio seguro de identidades en el orden especificado en la lista Clase.
4. **Actualizar:** haga clic en el icono para actualizar la lista.

Migrar datos del repositorio seguro de identidades

Mediante la pestaña **Exportar**, puede seleccionar los contenedores o los objetos que desea migrar desde el repositorio seguro de identidades a una aplicación. Cuando se migra un objeto, el motor de metadirectorio aplica al objeto todas las directivas de concordancia, creación y colocación, así como el filtro de suscriptor.

Para migrar objetos o contenedores del repositorio seguro de identidades a otra aplicación, haga clic en el icono . Busque y seleccione el objeto que desea migrar y haga clic en **Aceptar** para añadir el objeto a la lista de migración. Para eliminar objetos de la lista de migración, haga clic en el icono .

Cuando haya terminado de seleccionar los objetos que desea migrar, haga clic en para iniciar la migración. El progreso de migración se mostrará en la pantalla. Si desea detener la migración, haga clic en el botón .

Sincronizar objetos

La operación de sincronización busca objetos que se han modificado y los sincroniza. Puede seleccionar **Examine todos los objetos** para iniciar la sincronización al instante. También puede definir una fecha/hora para iniciar la sincronización.

Seguimiento del guion DirXML

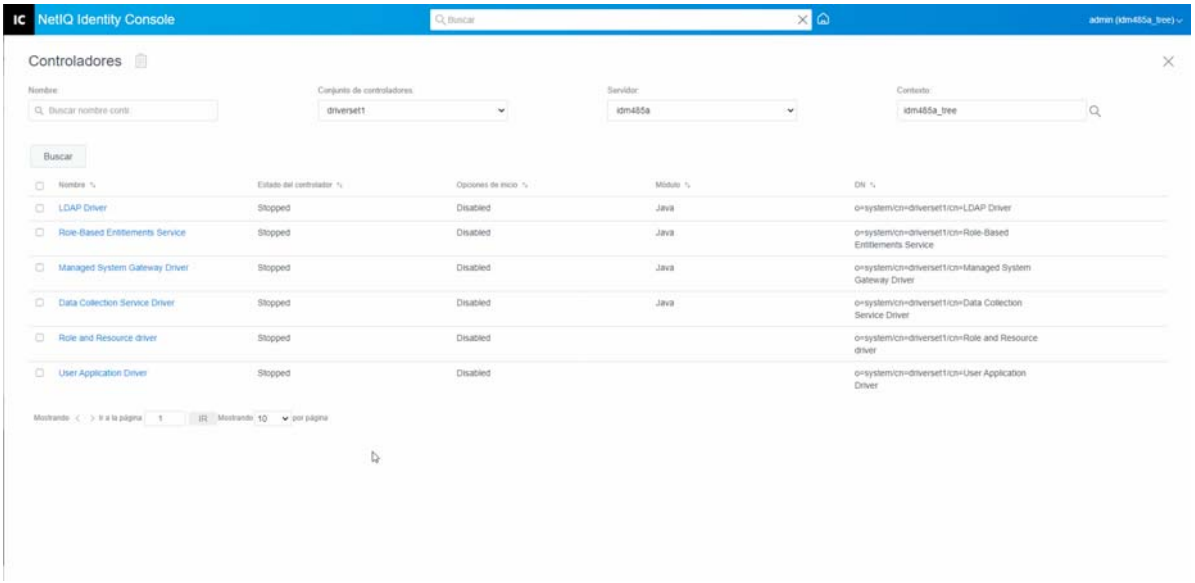
La opción Seguimiento del guion DirXML permite seleccionar un nivel de seguimiento para un controlador. También aplica ajustes de seguimiento a todos los canales de editor y suscriptor. Se pueden seleccionar las siguientes opciones de seguimiento del guion DirXML:

- Todo el seguimiento de guiones DirXML habilitado

- Todo el seguimiento de guiones DirXML inhabilitado
- Seguimiento activado de regla de guion DirXML
- Seguimiento desactivado de regla de guion DirXML

Haga clic en (Aceptar) para guardar los cambios.

Figura 23-3 *Gestión de la sincronización de datos de los controladores*



Filtros de atributo de clase

Los filtros de atributo de clase permiten especificar las clases y los atributos que una aplicación puede enviar y recibir en el repositorio seguro de identidades. Si desea que una clase específica se transfiera para que el motor del metadirectorio la procese, debe añadir la clase al filtro en el canal correspondiente. También puede filtrar objetos según un valor de atributo específico que defina. Mediante esta opción, puede realizar las siguientes acciones:

- **Definir plantilla**: utilice esta opción para establecer las opciones por defecto de todos los atributos que se han añadido al filtro. Haga clic en el icono situado junto a la etiqueta Filtro de atributo de clase.
- **Añadir una nueva clase**: haga clic en el icono para añadir una nueva clase.
- **Añadir un nuevo atributo**: haga clic en el icono para añadir un nuevo atributo.
- **Copiar filtro de**: esta opción permite copiar un filtro desde otro controlador. Haga clic en el icono para copiar el filtro.
- **Editar XML**: edite la configuración del filtro de clase y atributo mediante el icono Editar archivo XML .
- **Suprimir clase o atributos**: suprima cualquier clase o atributo. Para ello, haga clic en el icono situado junto a la clase o el atributo correspondientes.

Puede definir las siguientes opciones para un valor de clase y atributo en los canales de editor y suscriptor:

- Sincronizar
- Ignorar
- Notificar
- Reset

Autoridad de fusión

Si no se está sincronizando un atributo en ninguno de los dos canales, no se realiza ninguna fusión.

Si un atributo se está sincronizando en un canal y no en el otro, todos los valores existentes en el destino de ese canal se eliminarán y se sustituirán por los valores del origen de ese canal. Si el origen tiene varios valores y el destino solo puede incluir un valor, se utilizará únicamente uno de los valores en el lado de destino.

Si se está sincronizando un atributo en ambos canales y estos solo pueden incluir un valor, la aplicación conectada adquiere los valores almacenados en el repositorio seguro de identidades a menos que no haya ningún valor en él. En ese caso, el repositorio seguro de identidades adquiere los valores de la aplicación conectada.

Si un atributo se está sincronizando en ambos canales y solo un lado puede incluir varios valores, el valor del canal de un solo valor se añade al canal multivalente si aún no se encuentra en él. Si no hay ningún valor en un solo lado, puede elegir el valor que desea añadir al lado único. Puede definir las siguientes opciones para Autoridad de fusión:

- Por defecto
- Repositorio seguro de identidades
- Aplicación
- Ninguno

Haga clic en (Aceptar) para guardar los cambios.

Guion de ECMA

Muestra una lista ordenada de archivos de recursos ECMAScript. Los archivos contienen las funciones de extensión del controlador que Identity Manager carga en el momento de iniciarse. Puede importar archivos adicionales haciendo clic en , eliminar archivos existentes haciendo clic en o cambiar el orden de los archivos que se ejecutan. También puede subir o bajar los guiones en la lista. Para guardar la lista de guiones de ECMA, haga clic en el icono .

Asignación de atributo recíproco

Las asignaciones de atributo recíproco permiten crear y gestionar los enlaces en segundo plano o las referencias entre objetos. Por ejemplo, el objeto Grupo incluye un atributo Miembros que hace referencia a todos los objetos Usuario que pertenecen a ese grupo. Del mismo modo, cada objeto Usuario incluye un atributo Pertenencia a grupo que hace referencia a los objetos Grupo de los que

es miembro ese usuario. Para que el motor de metadirectorio mantenga "Group object" (objeto Grupo) > "Members attribute synchronized with the User object" (atributo Miembros sincronizado con el objeto Usuario) > "Group Membership attribute for all Group objects and User objects" (atributo Pertenencia a grupo de todos los objetos Grupo y los objetos Usuario" del repositorio seguro de identidades, estos atributos deben enlazarse. Los enlaces entre atributos de objeto se conocen como asignaciones de atributo recíproco.

Mediante este módulo, puede realizar las siguientes acciones:

Creación de asignaciones de atributo recíproco personalizadas

Esta sección solo es aplicable si la página Asignación de atributo recíproco muestra el mensaje **El controlador no contiene asignaciones de atributo recíproco personalizadas. Haga clic en el icono '+' arriba para crear asignaciones de atributo recíproco básicas**.

1. Haga clic en el icono + para crear una nueva lista de asignaciones de atributo recíproco personalizadas.
2. Se muestran las asignaciones de atributo por defecto del controlador. Ahora puede añadir asignaciones, modificar las existentes o suprimirlas.

Adición de una nueva asignación de atributo recíproco

Al crear una asignación de atributo, debe añadir primero uno de los atributos a la lista de asignaciones de atributo recíproco.

1. Haga clic en el icono + situado junto al menú desplegable Acciones.
2. En la nueva entrada de atributo, seleccione el atributo deseado en la lista desplegable.
3. Especifique los detalles de la asignación de atributo recíproco:
   - 3a **Clase de origen**: permite especificar el nombre de la clase a la que está asociado el atributo en la lista de asignaciones. Por ejemplo, si coloca el atributo Pertenencia a grupo en la lista de asignaciones de atributo recíproco, la clase de origen asociada será Usuario.
   - 3b **Clase de destino**: permite especificar el nombre de la clase asociada al atributo para el que desea crear una asignación de atributo recíproco. Por ejemplo, si ha colocado el atributo Pertenencia a grupo en la lista de asignaciones de atributo recíproco, la clase de destino asociada será Grupo.
   - 3c **Atributo recíproco**: permite especificar el nombre del atributo para el que desea crear una asignación de atributo recíproco.

4 Si desea asignar el atributo a otro atributo recíproco, haga clic en el icono + situado a la derecha del nombre del atributo.

   Al final de la lista del atributo, se añade una nueva sección para el atributo. Seleccione la clase de origen y la de destino, así como el atributo recíproco.

Eliminación de una asignación de atributo recíproco

Para eliminar una asignación de atributo recíproco:

1 Marque la casilla de verificación de la asignación de atributo recíproco que desea eliminar situada delante de **Clase de origen**.

2 Haga clic en el icono situado junto a la lista desplegable de atributos.

Eliminación de un atributo de la lista de asignaciones de atributo recíproco

Para eliminar un atributo de la lista de asignaciones de atributo recíproco:

1 Seleccione el atributo que desea eliminar. Para ello, marque la casilla de verificación que se encuentra delante del atributo.

2 Haga clic en el icono situado junto a la lista desplegable **Acciones**.

Reordenación de los atributos asignados

Las asignaciones de atributos se utilizan en el orden mostrado, de arriba a abajo. Puede mover los atributos asignados hacia arriba o hacia abajo en la lista para asegurarse de que se resuelven en el orden correcto. Por lo general, se deben mostrar primero las asignaciones específicas seguidas de las más generales. Por ejemplo, una asignación del atributo Miembro de un objeto Grupo debe aparecer antes de la asignación del atributo Miembro de cualquier objeto (la opción <Cualquier clase>).

Marque la casilla de verificación situada delante del atributo asignado que desee mover y, a continuación, haga clic en ↑ para mover el atributo hacia arriba o en ↓ para moverlo hacia abajo.

Eliminación de la asignación de atributo recíproco personalizada

Puede suprimir las asignaciones de atributos personalizadas que ha creado. Esto provoca que el motor de metadirectorio utilice las asignaciones de atributos por defecto para el controlador.

Para eliminar una asignación de atributo recíproco personalizada, haga clic en el icono situado en la parte superior de la pantalla.

Edición de XML de atributo recíproco

Si lo desea, puede editar directamente el archivo XML de un atributo recíproco. Para ello, haga clic en el icono Editar XML  de la página Asignaciones de atributo recíproco personalizadas. Se abrirá un editor XML básico que le permitirá modificar el archivo XML. Cuando haya terminado, haga clic en Aceptar o Cancelar para cerrar el editor XML.

Valores avanzados

Los ajustes avanzados se dividen en las siguientes categorías:

- "Gestión de derechos" en la página 170
- "Gestión de la tabla de asignación de objetos" en la página 170
- "Gestión de tareas para controladores" en la página 171

Gestión de derechos

La página Derechos contiene una tabla en la que se muestran todos los derechos definidos actualmente en el controlador seleccionado (enumerados con su nombre completo). En esta página, se pueden realizar las siguientes acciones:

- **Editar en XML**: para editar derechos en el archivo XML, seleccione el derecho en la lista y haga clic en el icono  . A continuación, marque la casilla **Habilitar edición de XML**.
- **Suprimir**: para suprimir un derecho, haga clic en la casilla situada a la izquierda del nombre del derecho y, a continuación, haga clic en el icono  . Aparecerá un mensaje que indica que la operación no se puede deshacer y se le preguntará si está seguro de que desea suprimir el derecho seleccionado. Haga clic en **Aceptar** para suprimir el derecho o en **Cancelar** para detener la operación. Puede hacer clic en más de una casilla para suprimir varios derechos o en la casilla superior izquierda para suprimir todos los derechos.

Gestión de la tabla de asignación de objetos

Las directivas de Identity Manager utilizan tablas de asignación para asignar un conjunto de valores a otro. Al instalar el paquete de derechos, las directivas de ese paquete se añaden al conjunto de directivas de inicio del controlador. El controlador ejecuta estas directivas solo una vez cuando se inicia el controlador. Para obtener más información, consulte Mapping Table Objects (Asignación de objetos de tabla) en la *NetIQ Identity Manager Driver Administration Guide* (Guía de administración de controladores de NetIQ Identity Manager).

Mediante la tabla de asignación de objetos, puede realizar las siguientes acciones:

- **Modificar una asignación existente:** para modificar una tabla de asignación de objetos existente, haga clic en la asignación en la lista y realice estas acciones en la pantalla siguiente:
  - Añada una nueva columna.

    Especifique un valor para la columna y, a continuación, seleccione si el valor distingue o no entre mayúsculas y minúsculas o si es numérico.

- Añada una fila nueva y especifique un valor para ella.
- Haga clic en el icono .

- **Suprimir asignación**: para eliminar una asignación de la lista, seleccione la asignación correspondiente en la lista y haga clic en el icono .
- **Editar en XML**: para editar una asignación en un archivo XML, haga clic en la asignación en la lista y seleccione el icono . A continuación, marque la casilla **Habilitar edición de XML**.

Gestión de tareas para controladores

Identity Console permite programar eventos mediante la opción Tareas para todos los controladores individuales.

La página Programador de tareas contiene el nombre y la descripción de la tarea, si la tarea está habilitada o inhabilitada y cuándo está programada para ejecutarse. Haga clic en el nombre de la tarea para abrir la página Tarea. Haga clic en el icono Habilitar/inhabilitar ubicado debajo de la columna Habilitado para habilitar o inhabilitar la tarea. Haga clic en la descripción de la tarea para verla por completo.

La pestaña Tareas contiene una tabla en la que se muestran los objetos de tarea existentes del controlador seleccionado, que aparece con su nombre completo en la entrada del controlador.

La página Programador de tareas permite realizar las siguientes tareas:

- **Crear la tarea**: haga clic en el icono para crear una nueva tarea.

  En la ventana emergente **Nueva tarea**, realice los siguientes pasos para crear una nueva tarea:

  1. Especifique el nombre de la tarea.
  2. Seleccione el tipo de tarea.
  3. Haga clic en el icono y seleccione el servidor en el que desea ejecutar la tarea en la lista de servidores disponibles. De lo contrario, especifique un nombre de servidor y, a continuación, seleccione el servidor.
  4. Haga clic en el botón **Crear**.
- **Iniciar la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono .
- **Detener la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono .
- **Habilitar la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono .
- **Inhabilitar la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono .

- **Obtener estado**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono ⓘ.
- **Suprimir la tarea**: seleccione una tarea. Para ello, haga clic en la casilla situada a la izquierda de la tarea y, a continuación, haga clic en el icono 🗑.

Haga clic en una tarea para acceder a la página **Job Property** (Propiedad de tarea). Aquí puede configurar cómo desea que se ejecute la tarea.

General: muestra el nombre de clase de Java de la tarea. Utilice esta página para habilitar o inhabilitar la tarea, suprimir la tarea después de que se ejecute, seleccionar el servidor o los servidores en los que debe ejecutarse esta tarea, especificar el servidor de correo electrónico, y asignar a la tarea un nombre de visualización y una descripción diferentes.

Programa: le permite definir cuándo desea ejecutar la tarea. Especifique un valor en "Iniciar tarea a las" para definir la hora y establecer si la tarea se ejecutará con periodicidad diaria, semanal, mensual o anual. También puede personalizar cuándo desea ejecutar la tarea, o bien habilitar el conmutador para que la tarea se ejecute manualmente.

Ámbito: permite definir los objetos a los que se aplica esta tarea. Un objeto puede ser un contenedor, un grupo dinámico, un grupo o una hoja. Haga clic en Añadir para seleccionar el objeto al que desea aplicar esta tarea. Puede utilizar el botón Examinar para seleccionar un objeto y, a continuación, hacer clic en Aceptar. Para eliminar un objeto de la lista Ámbito, seleccione un objeto Ámbito. Para ello, haga clic en el recuadro situado a la izquierda del objeto DN y, a continuación, haga clic en Eliminar.

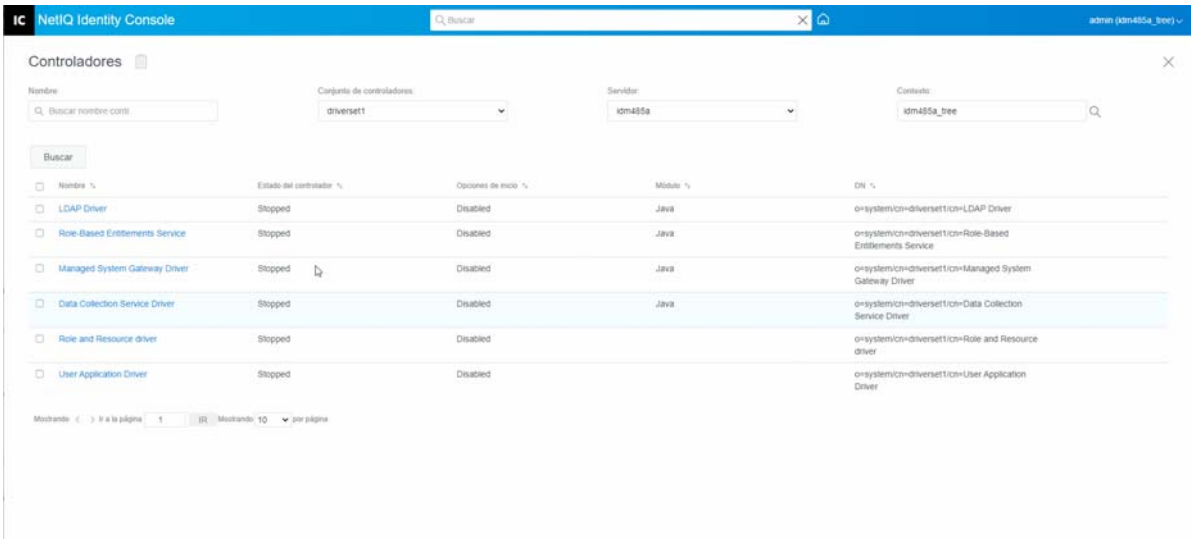
Una vez que se haya añadido el objeto, selecciónelo para visualizar más opciones. Si selecciona un objeto Grupo, tiene la opción de aplicar la tarea a los componentes del grupo o solo al grupo. Si selecciona un objeto Contenedor, tiene la opción de aplicar la tarea a todos los descendientes de ese contenedor, a todos los hijos del contenedor o solo al contenedor.

Parámetros: permite añadir parámetros adicionales a la tarea y ver los parámetros tal y como están configurados actualmente. Estos parámetros cambian en función del tipo de tarea seleccionada.

Resultados: permite definir lo que se desea hacer con los resultados de la tarea. La página Resultados se divide en dos partes, Resultado intermedio y Resultado final, con los siguientes resultados permitidos: Correcto, Advertencia, Error y Cancelado. A la derecha de la columna Resultados, se encuentra la columna Acción. Al hacer clic en la columna Acción, puede definir el modo en que desea que se le notifique cada resultado. Entre las acciones, se incluyen el envío de resultados de una auditoría o el envío de un mensaje de correo electrónico cuando se complete el resultado. Si no se selecciona ninguna opción, no se realizará ninguna acción para el resultado.

En la pestaña **Seguimiento**, puede configurar el seguimiento de un controlador específico. Para obtener más información, consulte “Configuración del nivel de seguimiento” en la página 174.

Figura 23-4 *Gestión de la configuración avanzada*



Configuración de los niveles de registro y seguimiento de los controladores

Para configurar el registro y el seguimiento para los controladores, seleccione la pestaña **Controladores** > **Configuración de registro y seguimiento** en la página principal de Identity Console. Esta sección se divide en las siguientes categorías:

- "Configuración del nivel de registro" en la página 173
- "Configuración del nivel de seguimiento" en la página 174

Configuración del nivel de registro

Cada controlador tiene un campo de nivel de registro en el que puede definir el nivel de errores del que debería realizarse un seguimiento. El nivel que indique aquí determina qué mensajes habrá disponibles en los registros. Por defecto, el nivel de registro se define para realizar un seguimiento de los mensajes de error. (Esto también incluye los mensajes irrecuperables). Para realizar un seguimiento de los tipos de mensajes adicionales, cambie el nivel de registro. Para configurar el nivel de registro, seleccione la pestaña **Configuración de registro y seguimiento**> **Nivel de registro**. En la tabla siguiente, se describen los ajustes del nivel de registro:

Opción	Descripción
Usar ajustes del registro del conjunto de controladores	Si se selecciona esta opción, el controlador registra eventos en función de los ajustes de registro del objeto Conjunto de controladores.
Desactive el registro en los registros de conjunto de controladores, suscriptor y editor	Desactiva todo el registro de este controlador en el objeto Conjunto de controladores, y el canal de suscriptor y el de editor.

Opción	Descripción
Número máximo de entradas en el registro (50-500)	Número de entradas en el registro. El valor por defecto es 50.
Niveles de registro	Se pueden seleccionar los siguientes niveles de registro: ◆ **Registrar errores**: registra solo errores. ◆ Registrar errores y advertencias: registra errores y advertencias. ◆ **Registrar eventos específicos**: registra los eventos seleccionados. Si se selecciona esta opción, se habilitará la siguiente lista de eventos: ◆ **Eventos del motor de metadirectorio** ◆ **Eventos de estado** ◆ **Eventos de operación** ◆ **Eventos de transformación** ◆ **Eventos de provisión de credenciales** ◆ **Actualizar solo la última hora de registro**: actualiza la última hora de registro. ◆ **Desactivar registro**: desactiva el registro del controlador.

Configuración del nivel de seguimiento

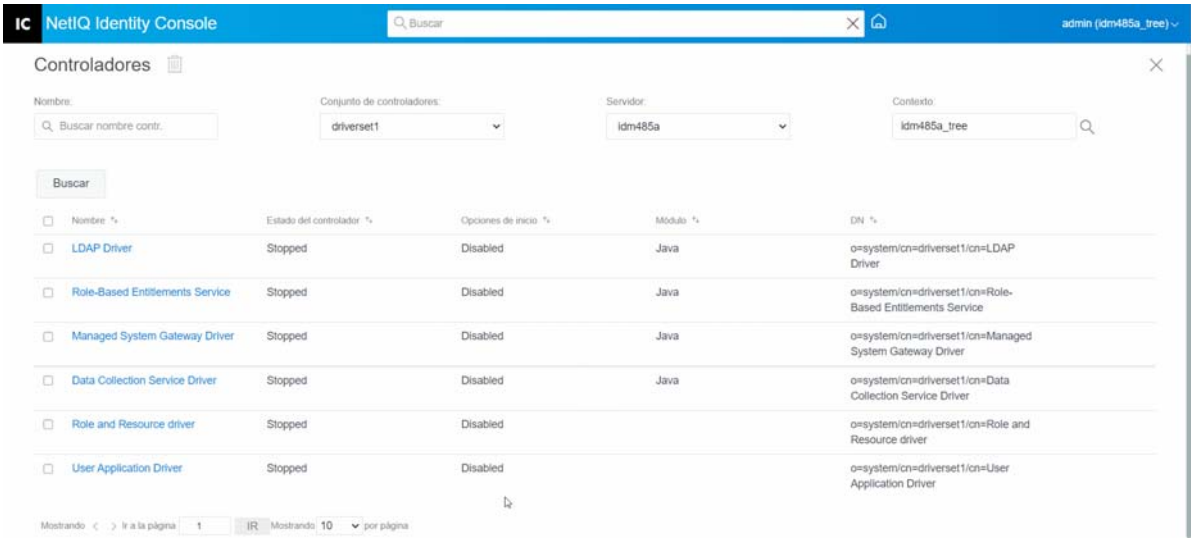
Puede configurar el seguimiento de un controlador específico. En función del nivel de seguimiento especificado para un controlador, el seguimiento muestra los eventos relacionados con los controladores cuando el motor procesa los eventos. El nivel de seguimiento del controlador solo afecta al controlador o al conjunto de controladores en los que se ha definido el seguimiento. Si utiliza el cargador remoto, el archivo de seguimiento del cargador remoto se define directamente en el cargador remoto y solo contiene el seguimiento de shim del controlador.

Para configurar el seguimiento de un controlador, seleccione la pestaña **Configuración de registro y seguimiento** > **Seguimiento**. En la tabla siguiente, se describen los ajustes de seguimiento:

Parámetro	Controlador
Nivel de seguimiento	A medida que aumenta el nivel de seguimiento del controlador, aumenta la cantidad de información que aparece en el seguimiento. El nivel uno de seguimiento muestra errores, pero no su causa. Si desea ver la información de sincronización de contraseñas, defina el nivel de seguimiento en cinco. Si selecciona **Usar el ajuste del conjunto de controladores**, el valor se obtiene del conjunto de controladores.

Parámetro	Controlador
Archivo de seguimiento	Especifique el nombre de archivo y la ubicación en la que se escribirá la información de Identity Manager para el controlador seleccionado. Si selecciona **Usar el ajuste del conjunto de controladores**, el valor se obtiene del conjunto de controladores.
Nombre de seguimiento	Los mensajes de seguimiento del controlador se introducen previamente con el valor especificado en lugar del nombre del controlador. Utilice esta opción si el nombre del controlador es demasiado largo.
Codificación de archivos de seguimiento	El archivo de seguimiento utiliza la codificación por defecto del sistema. Si lo desea, puede especificar otra codificación.
Límite de tamaño de archivo de seguimiento	Permite definir un límite para el archivo de seguimiento de Java. Si define el tamaño de archivo como ilimitado, el archivo aumentará de tamaño hasta que no quede espacio en el disco. **Nota:** Si se especifica el límite de tamaño de archivo, el archivo de seguimiento se crea en varios archivos. Identity Manager divide automáticamente el tamaño máximo de archivo por diez y crea diez archivos independientes. El tamaño combinado de estos archivos es igual al tamaño máximo del archivo de seguimiento. Si selecciona **Usar el ajuste del conjunto de controladores**, el valor se obtiene del conjunto de controladores.

Figura 23-5 *Gestión de los niveles de registro y seguimiento de los controladores*



Inspección de controladores

Puede utilizar el Inspector de controladores para ver información detallada acerca de los objetos asociados a un controlador. Esta sección se divide en las siguientes categorías:

Inspector de controladores

Para ver los objetos asociados a un controlador:

1. En Identity Console, seleccione **Controladores** > **Inspector** > pestaña **Inspector de controladores**.
2. En el campo **Controlador**, especifique el nombre completo del controlador que desea inspeccionar o haga clic en el icono Examinar para buscar y seleccionar el controlador que desee.
3. Cuando haya seleccionado el controlador que desea inspeccionar, haga clic en **Aceptar** para visualizar la página Inspector de controladores.

   En la página, se muestra información acerca de los objetos asociados al controlador seleccionado. Puede llevar a cabo cualquiera de las siguientes acciones:

   - **Suprimir:** elimina la asociación entre el controlador y un objeto. Marque la casilla de verificación situada delante del objeto que ya no desea asociar al controlador, haga clic en el icono  y, a continuación, haga clic en **Aceptar** para confirmar la supresión.
   - **Actualizar:** seleccione el icono Actualizar  para volver a leer todos los objetos asociados al controlador y actualizar la información.
   - **Mostrar:** seleccione el número de asociaciones que se mostrarán por página. Puede seleccionar un número predefinido (25, 50 o 100) o especificar otro número de su elección. El valor por defecto es 10 asociaciones por página. Si hay más asociaciones que el número mostrado, puede utilizar los botones de flecha para visualizar las páginas de asociaciones siguientes y anteriores.
   - **Acciones:** lleve a cabo acciones en los objetos asociados al controlador. Haga clic en **Acciones** y, a continuación, seleccione una de las siguientes opciones:
     - **Mostrar todas las asociaciones:** muestra todos los objetos asociados al controlador.
     - **Filtrar para asociaciones 'Inhabilitadas':** muestra todos los objetos asociados al controlador que presentan el estado Inhabilitado.
     - **Filtrar para asociaciones 'Manuales':** muestra todos los objetos asociados al controlador que presentan el estado Manual.
     - **Filtrar para asociaciones 'Migrar':** muestra todos los objetos asociados al controlador que presentan el estado Migrar.
     - **Filtrar para asociaciones 'Pendientes':** muestra todos los objetos asociados al controlador que presentan el estado Pendiente.

- **Filtrar para asociaciones 'Procesadas':** muestra todos los objetos asociados al controlador que presentan el estado Procesado.
- **Filtrar para asociaciones 'Sin definir':** muestra todos los objetos asociados al controlador que presentan el estado Sin definir.
- **Resumen de asociaciones:** muestra el estado de todos los objetos asociados al controlador.

- **DN de objeto:** muestra el DN de los objetos asociados.
- **Estado:** muestra el estado de asociación del objeto.
- **ID de objeto:** muestra el valor de la asociación.

Inspector del caché de controladores

Puede ver las transacciones de un archivo de caché del controlador mediante Identity Console. El **Inspector del caché de controladores** muestra información sobre el archivo de caché, incluida una lista de los eventos que procesará el controlador.

1. En Identity Console, seleccione **Controladores** > **Inspector** > pestaña **Inspector del caché de controladores**.
2. En el campo **Controlador**, especifique el nombre completo del controlador cuyo caché desea inspeccionar o haga clic en el icono Examinar para buscar y seleccionar el controlador deseado y, a continuación, haga clic en **Aceptar** para visualizar la página del Inspector de caché de controladores.

   Un archivo de caché del controlador solo puede leerse cuando el controlador no se está ejecutando. Si se detiene el controlador, la página Inspección del caché de controladores mostrará el caché. Si el controlador se está ejecutando, en la página, se muestra la nota `El controlador no se ha detenido; no se puede leer el caché` en lugar de las entradas de caché. Para detener el controlador, haga clic en el botón  ; a continuación, se leerá y se mostrará el caché.

   - **Caché del controlador en el servidor:** muestra el servidor que contiene esta instancia del archivo de caché. Si el controlador se ejecuta en varios servidores, puede seleccionar otro servidor en la lista para ver el archivo de caché del controlador para ese servidor.
   - **Iconos de Iniciar/Detener controlador:** muestra el estado actual del controlador y permite iniciarlo o detenerlo. El caché solo puede leerse mientras el controlador está detenido.
   - **Suprimir:** seleccione las entradas del caché y, a continuación, haga clic en  para eliminarlas del archivo de caché.
   - **Acciones:** permite realizar acciones en las entradas del archivo de caché. Haga clic en **Acciones** para expandir el menú y, a continuación, seleccione una de las siguientes opciones:
     - **Borrar todos los eventos en caché:** permite borrar todos los eventos almacenados en caché.
     - **Resumen de caché:** resume todos los eventos almacenados en el archivo de caché.

Visualización de la información de sistemas conectados de los controladores

Para ver la información de sistemas conectados de un controlador específico, realice las siguientes acciones:

1. En Identity Console, haga clic en el módulo **Object Inspector**.
2. Busque y seleccione el objeto Controlador específico para el que desea que se muestren los sistemas conectados.
3. Toda la información de sistemas conectados del objeto Controlador seleccionado se mostrará en el equipo.

Inspector de caché de sincronización fuera de banda

Para ver eventos en el caché de sincronización fuera de banda:

1. En Identity Console, seleccione **Controladores** > **Inspector** > pestaña **Inspector de caché de sincronización fuera de banda**.
2. En el campo **Controlador**, especifique el nombre completo del controlador cuyo caché desea inspeccionar o haga clic en el icono Examinar para buscar y seleccionar el controlador que desee. A continuación, haga clic en **Aceptar**.

   Un archivo de caché del controlador solo puede leerse cuando el controlador no se está ejecutando. Si se detiene el controlador, la página Inspección del caché de controladores mostrará el caché. Si el controlador se está ejecutando, en la página, se muestra la nota `El controlador no se ha detenido; no se puede leer el caché` en lugar de las entradas de caché. Para detener el controlador, haga clic en el botón  ; a continuación, se leerá y se mostrará el caché.

   - **Nombre de archivo de caché:** muestra el nombre de archivo del caché.
   - **Caché del controlador en el servidor:** muestra el servidor que contiene esta instancia del archivo de caché. Si el controlador se ejecuta en varios servidores, puede seleccionar otro servidor en la lista para ver el archivo de caché del controlador para ese servidor.
   - **Iconos de Iniciar/Detener controlador:** muestra el estado actual del controlador y permite iniciarlo o detenerlo. El caché solo puede leerse mientras el controlador está detenido.
   - **Suprimir:** seleccione las entradas del caché y, a continuación, haga clic en  para eliminarlas del archivo de caché.
   - **Acciones:** permite realizar acciones en las entradas del archivo de caché. Haga clic en **Acciones** para expandir el menú y, a continuación, seleccione una de las siguientes opciones:
     - **Resumen de caché:** resume todos los eventos almacenados en el archivo de caché.
     - **Borrar todos los eventos en caché:** permite borrar todos los eventos almacenados en caché.

Inventario de controladores

El inventario de controladores presenta información del controlador. Indica lo que admite el controlador e incluye algunos ajustes de configuración. El inventario de controladores debe proporcionarlo el desarrollador del controlador. Por lo general, un administrador de red no necesita editar el inventario de controladores. Si el administrador desea editar el inventario de controladores, debe seleccionar **Controladores** > **Inspector** > **Inventario de controladores** > **Habilitar edición de XML**.

Supervisión de actividad del controlador

La supervisión de actividad del controlador permite ver el estado de actividad actual de un controlador como verde, amarillo o rojo y definir las acciones que se realizarán en función de cada uno de estos estados.

Puede crear las condiciones (criterios) que determinan cada uno de los estados de actividad y también definir las acciones que se realizan cada vez que cambia el estado de actividad del controlador. Por ejemplo, si la actividad del controlador cambia de un estado verde a amarillo, puede llevar a cabo acciones como reiniciar el controlador o apagarlo y enviar un mensaje de correo electrónico a la persona designada para resolver los problemas con el controlador.

Mediante este módulo, puede realizar las siguientes acciones:

- "Modificación de las condiciones de actividad del controlador" en la página 179
- "Modificación de las acciones de actividad del controlador" en la página 182
- "Creación de un estado personalizado" en la página 183
- "Modificación de un estado personalizado" en la página 184

Modificación de las condiciones de actividad del controlador

Puede controlar las condiciones que determinan cada estado de actividad. El estado verde debe representar un controlador con actividad correcta y un estado rojo, un controlador con actividad incorrecta.

Las condiciones del estado verde se evalúan primero. Si el controlador no cumple las condiciones del estado verde, se evalúan las condiciones del estado amarillo. Si el controlador no cumple las condiciones del estado amarillo, se le asigna automáticamente un estado de actividad rojo.

Para modificar las condiciones de un estado:

1. En Identity Console, abra la página Configuración de actividad de controladores de un controlador cuyas condiciones desee modificar:
   - **1a** Abra la página principal de Identity Console.
   - **1b** Seleccione **Controladores** > **haga clic en el controlador adecuado en la lista** > **Inspector** > **Configuración de actividad de controladores**.
2. Haga clic en la pestaña del estado (verde o amarillo) que desee modificar.

   En la pestaña, se muestran las condiciones actuales del estado de actividad. Las condiciones se organizan en grupo y se utilizan operadores lógicos, AND u OR, para combinar cada condición y cada grupo. Tenga en cuenta el siguiente ejemplo del estado verde:

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

En el ejemplo, al controlador se le asigna un estado verde si las condiciones de GROUP1 o GROUP2 se evalúan como verdaderas. Si ninguno de los dos grupos de condiciones es verdadero, se evalúan las condiciones del estado amarillo.

Las condiciones que se pueden evaluar son las siguientes:

- **Estado del controlador:** en ejecución, detenido, en inicio, no en ejecución o en proceso de cierre. Por ejemplo, una de las condiciones por defecto del estado de actividad verde es que el controlador se está ejecutando.
- **Desbordamiento de controladores en caché:** el estado del caché utilizado para conservar transacciones del controlador. Si el controlador presenta un desbordamiento de caché, se ha utilizado todo el caché disponible. Por ejemplo, la condición por defecto del estado de actividad verde es que la condición Desbordamiento de controladores en caché es falsa y la condición por defecto del estado de actividad amarillo es que esta condición es falsa.
- **Más reciente:** la antigüedad de la transacción más reciente del caché.
- **Más antigua:** la antigüedad de la transacción más antigua del caché.
- **Tamaño total:** el tamaño del caché.
- **Tamaño sin procesar:** el tamaño de todas las transacciones sin procesar del caché.
- **Transacciones sin procesar:** el número de transacciones sin procesar del caché. Puede especificar todos los tipos de transacciones o tipos específicos (como, por ejemplo, adiciones, eliminaciones o cambios de nombre).
- **Historial de transacciones:** el número de transacciones procesadas en varios puntos del canal de suscriptor o de editor durante un periodo determinado. Esta condición utiliza varios elementos con el siguiente formato:

  <*tipo de transacción*> <*ubicación y periodo de la transacción* > <*operador relacional*> <*número de transacciones*>.

  - <*tipo de transacción*>: especifica el tipo de transacción que se está evaluando. Puede tratarse de todas las transacciones, adiciones, eliminaciones, cambios de nombre, etc.
  - <*ubicación y periodo de la transacción*>: especifica la ubicación del canal del suscriptor o del editor y el periodo que se está evaluando. Por ejemplo, puede evaluar el número total de transacciones procesadas como eventos notificados del editor en las últimas 48 horas. Por defecto, los datos del historial de transacciones se conservan durante dos semanas, lo que implica que no es posible especificar un periodo superior a este a menos que cambie el ajuste por defecto de Duración de los datos de la transacción.
  - <*operador relacional*>: indica que las transacciones identificadas deben ser igual a, no ser igual a, ser menor que, ser menor o igual que, ser mayor que o ser mayor o igual que el <número de transacciones>.
  - <*número de transacciones*>: especifica el número de transacciones que se utilizan en la evaluación.

A continuación, se proporciona un ejemplo de condición Historial de transacciones:

```
<número de adiciones> <como comandos del editor> <en los últimos
10 minutos> <es menor que> <1000>
```

- **Historial disponible:** la cantidad de datos del historial de transacciones que están disponibles para su evaluación. El objetivo principal de esta condición es asegurarse de que una condición Historial de transacciones no provoca el fallo del estado actual porque no tiene suficientes datos de historial de transacciones recopilados durante el periodo de evaluación.

  Por ejemplo, supongamos que desea utilizar la condición Historial de transacciones para evaluar el número de adiciones como comandos de editor durante las últimas 48 horas (el ejemplo mostrado en la sección Historial de transacciones anterior). Sin embargo, no desea que la condición falle si aún no hay 48 horas de datos, como puede ser después de la configuración inicial de la actividad del controlador o si el servidor del controlador se reinicia (ya que los datos del historial de transacciones se guardan en la memoria). Por lo tanto, puede crear grupos de condiciones similares a los siguientes:

  ```
  Historial disponible de Group1 <es menor que> <48 horas> o Historial
  disponible de Group2 <es mayor o igual que> <48 horas> e Historial
  de transacciones <número de adiciones> <como comandos del editor>
  <en las últimas 48 horas> <es menor que> <1000>
  ```

  El estado se evalúa como verdadero si cualquiera de los dos grupos de condiciones es verdadero, lo que significa que a) hay menos de 48 horas de datos o b) hay al menos 48 horas de datos y el número de adiciones como comandos del editor durante las últimas 48 horas es inferior a 1000.

  El estado se evalúa como falso si ambas condiciones se evalúan como falsas, lo que significa que a) hay al menos 48 horas de datos y b) el número de adiciones como comandos del editor durante las últimas 48 horas es superior a 1000.

3 Modifique los criterios según sea necesario.

- Para añadir un nuevo grupo, haga clic en el icono + situado junto a los **Grupos de condiciones**.
- Para añadir una condición, haga clic en el icono + situado junto a los operadores lógicos (AND/OR). También puede hacer clic en el enlace **Añadir nueva condición**.
- Para reordenar grupos de condiciones o condiciones individuales, marque la casilla de verificación situada junto al grupo o la condición que desee mover y, a continuación, haga clic en los botones de flecha para subir o bajar. También puede utilizar los botones de flecha para mover una condición de un grupo a otro.

4 Cuando haya terminado, guarde los cambios. Para ello, haga clic en el botón **Guardar**.

5 Si desea cambiar las acciones asociadas a las condiciones que ha definido, continúe con "Modificación de las acciones de actividad del controlador" en la página 182.

Modificación de las acciones de actividad del controlador

Puede determinar las acciones que desea llevar a cabo cuando cambie el estado del controlador. Por ejemplo, si el estado cambia de verde a amarillo, puede apagar o reiniciar el controlador, generar un evento o iniciar un flujo de trabajo. O bien, si el estado cambia de amarillo a verde, se llevarán a cabo las acciones asociadas al estado verde.

Las acciones de un estado de actividad solo se llevan a cabo una vez cuando se cumplen las condiciones; mientras el estado sea verdadero, las acciones no se repetirán. Si el estado cambia porque ya no se cumplen sus condiciones, las acciones se volverán a realizar la próxima vez que se cumplan.

1. En Identity Console, abra la página Configuración de actividad de controladores de un controlador cuyas acciones desee modificar:
   1a. Abra la página principal de Identity Console.
   1b. Seleccione **Controladores** > **haga clic en el controlador adecuado en la lista** > **Inspector** > **Configuración de actividad de controladores**.
2. Haga clic en la pestaña **Verde**, **Amarillo** o **Rojo** del estado cuyas acciones desee modificar.
3. Haga clic en el icono más (+) situado junto al encabezado **Acciones** para añadir una acción y, a continuación, seleccione el tipo de acción que desee:
   - **Iniciar controlador:** inicia el controlador.
   - **Detener controlador:** detiene el controlador.
   - **Reiniciar controlador:** detiene y, a continuación, inicia el controlador.
   - **Borrar caché del controlador:** elimina todas las transacciones, incluidas las transacciones sin procesar, del caché.
   - **Enviar mensaje de correo electrónico:** envía un mensaje de correo electrónico a uno o varios destinatarios. La plantilla que desea utilizar en el cuerpo del mensaje de correo electrónico debe existir. Para incluir el nombre del controlador, el nombre del servidor y la información de estado de actividad actual en el mensaje de correo electrónico, añada los testigos `$Driver$`, `$Server$` y `$HealthState$` a la plantilla de correo electrónico y, a continuación, incluya los testigos en el texto del mensaje. Por ejemplo:

     ```
     The current health state of the $Driver$ driver running on $Server$
     is $HealthState$.
     ```

     Importante: Para enviar mensajes de correo electrónico a varios usuarios, separe cada dirección solo con una coma (,). No utilice punto y coma en lugar de coma.
   - **Escribir mensaje de seguimiento:** escribe un mensaje en el archivo de registro de la tarea Actividad de controladores o en el archivo de registro del conjunto de controladores si el archivo de seguimiento no se ha configurado en la tarea Actividad de controladores.
   - **Generar evento:** genera un evento que pueden utilizar Audit y Sentinel.
   - **Ejecutar ECMAScript:** ejecuta un ECMAScript existente.

     Para obtener información sobre cómo crear guiones ECMA, consulte Using ECMAScript in Policies (Uso de ECMAScript en directivas) en *NetIQ Identity Manager - Using Designer to Create Policies* (NetIQ Identity Manager: uso de Designer para crear directivas).
   - **Iniciar un flujo de trabajo:** inicia un flujo de trabajo de provisión.

- **Al producirse un error:** si falla una acción, indica lo que se debe hacer con las acciones restantes, el estado de actividad actual y la tarea Actividad de controladores.
  - **Aplicar a acciones por:** puede seguir ejecutando las acciones restantes o detenerlas, o bien establecer el valor actual como por defecto. El ajuste actual solo se aplica si tiene varias acciones Al producirse un error y define la opción Aplicar acciones por en una de las acciones Al producirse un error anteriores.
  - **Aplicar a estado por:** puede guardar o rechazar el estado actual, o bien establecer el valor actual como por defecto. Si guarda el estado, las condiciones del estado se seguirán evaluando como verdaderas. Al rechazar el estado, las condiciones del estado se evaluarán como falsas. El ajuste actual solo se aplica si tiene varias acciones Al producirse un error y define la opción Aplicar a estado por en una de las acciones Al producirse un error anteriores.
  - **Aplicar a tarea de estado del controlador por:** puede continuar con la ejecución de la tarea, abortarla e inhabilitarla o establecer el valor actual como por defecto. Si se sigue ejecutando la tarea, esta terminará de evaluar las condiciones para determinar el estado de actividad del controlador y realizará cualquier acción asociada al estado. Al abortar e inhabilitar la tarea, se detiene su actividad actual y se cierra; la tarea no se volverá a ejecutar hasta que la habilite. El ajuste actual solo se aplica si tiene varias acciones Al producirse un error y define la opción Aplicar a tarea de estado del controlador por en una de las acciones Al producirse un error anteriores.

4 Cuando haya terminado, guarde los cambios. Para ello, haga clic en el botón **Guardar**.

Creación de un estado personalizado

Puede crear uno o varios estados personalizados para realizar acciones independientemente del estado de actividad actual del controlador (verde, amarillo o rojo). Si se cumplen las condiciones de un estado personalizado, sus acciones se llevan a cabo independientemente del estado de actividad actual.

Al igual que con los estados verde, amarillo y rojo, las acciones de un estado personalizado se llevan a cabo solo una vez cuando se cumplen las condiciones; mientras el estado sea verdadero, las acciones no se repetirán. Si el estado cambia porque ya no se cumplen sus condiciones, las acciones se volverán a realizar la próxima vez que se cumplan.

1 En Identity Console, abra la página Configuración de actividad de controladores del controlador para el que desee crear un estado personalizado:

  1a Abra la página principal de Identity Console.

  1b Seleccione **Controladores** > **haga clic en el controlador adecuado en la lista** > **Inspector** > **Configuración de actividad de controladores**.

2 Haga clic en el icono + situado junto a los iconos de estado de actividad del controlador (verde, amarillo y rojo).

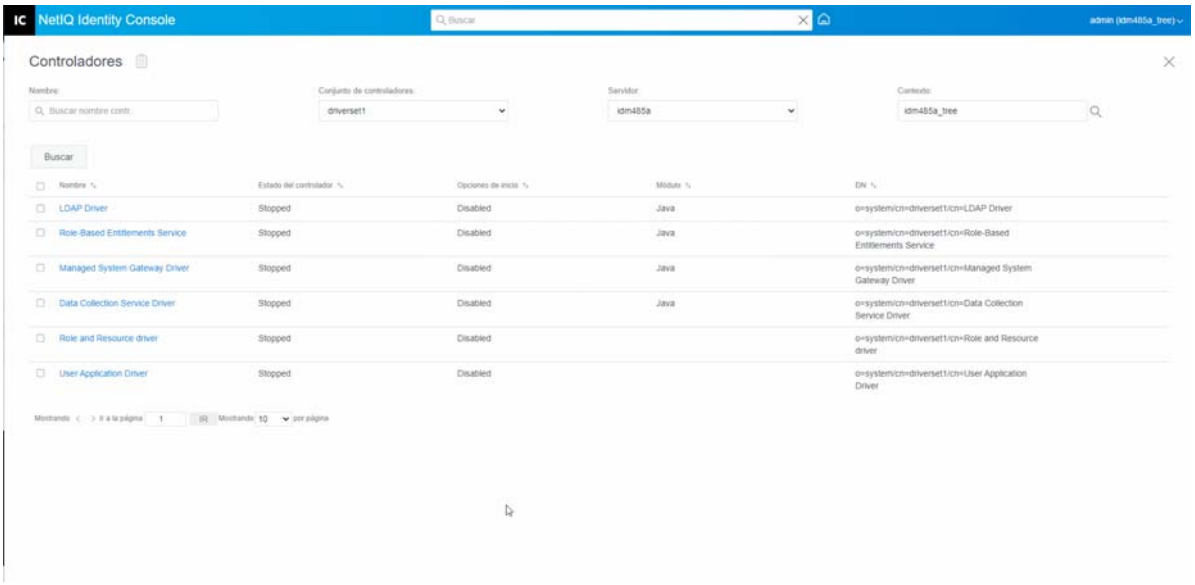
3 Siga las instrucciones indicadas en "Modificación de las condiciones de actividad del controlador" en la página 179 y "Modificación de las acciones de actividad del controlador" en la página 182 para definir las condiciones y las acciones del estado personalizado.

Modificación de un estado personalizado

Para modificar estados personalizados, realice los siguientes pasos:

1. En Identity Console, abra la página Configuración de actividad de controladores del controlador para el que desee crear un estado personalizado:
   - **1a** Abra la página principal de Identity Console.
   - **1b** Seleccione **Controladores** > **haga clic en el controlador adecuado en la lista** > **Inspector** > **Configuración de actividad de controladores**.
2. Haga clic en el icono situado junto a los iconos de estado de actividad del controlador (verde, amarillo y rojo).
3. Siga las instrucciones indicadas en "Modificación de las condiciones de actividad del controlador" en la página 179 y "Modificación de las acciones de actividad del controlador" en la página 182 para definir las condiciones y las acciones del estado personalizado.

Figura 23-6 *Gestión de los inspectores de controladores*



24 Gestión de las estadísticas del conjunto de controladores

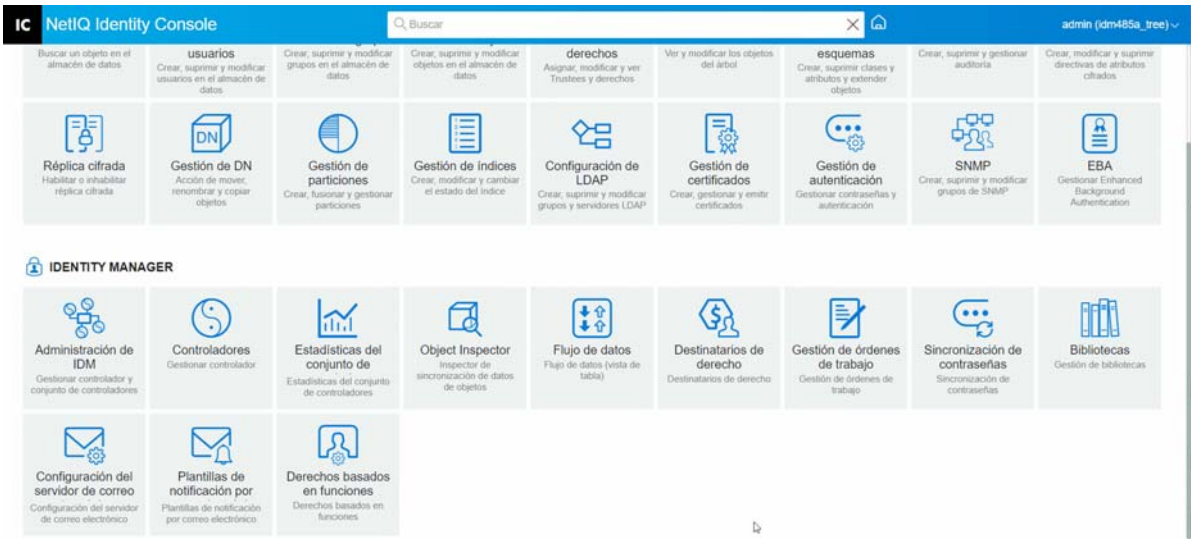
Puede utilizar el portal de Identity Console para ver diversas estadísticas de un único controlador o de un conjunto de controladores completo. Entre las estadísticas, se incluyen el tamaño del archivo de caché, el tamaño de las transacciones sin procesar del archivo de caché, las transacciones más antiguas y más recientes y el número total de transacciones sin procesar por categoría (adición, eliminación, modificación, etc.). Para ver las estadísticas del conjunto de controladores:

1. En Identity Console, abra la página **Estadísticas del conjunto de controladores**.
2. Seleccione el servidor adecuado en la lista desplegable.

   Aparecerá una página que permite ver las estadísticas de todos los controladores incluidos en el conjunto de controladores.

   - Para actualizar las estadísticas, haga clic en el icono .
   - Para cerrar las estadísticas de un controlador, haga clic en el botón situado en la esquina superior derecha de la ventana de estadísticas del controlador.
   - Para visualizar las estadísticas de todos los controladores, haga clic en **Acciones** > **Mostrar todo**.
   - Para contraer la lista de transacciones sin procesar de un controlador, haga clic en el botón situado encima de la lista. Para contraer la lista de transacciones sin procesar de todos los controladores, haga clic en **Acciones** > **Contraer todas las transacciones**.
   - Para expandir la lista de transacciones, haga clic en el botón . Para expandir la lista de transacciones sin procesar de todos los controladores, haga clic en **Acciones** > **Expandir todas las transacciones**.
   - Para cerrar la consola de estadísticas de los controladores inhabilitados, haga clic en **Acciones** y seleccione **Cerrar controladores inhabilitados**.

Figura 24-1 *Gestión de las estadísticas del conjunto de controladores*



25 Inspección de objetos de Identity Manager

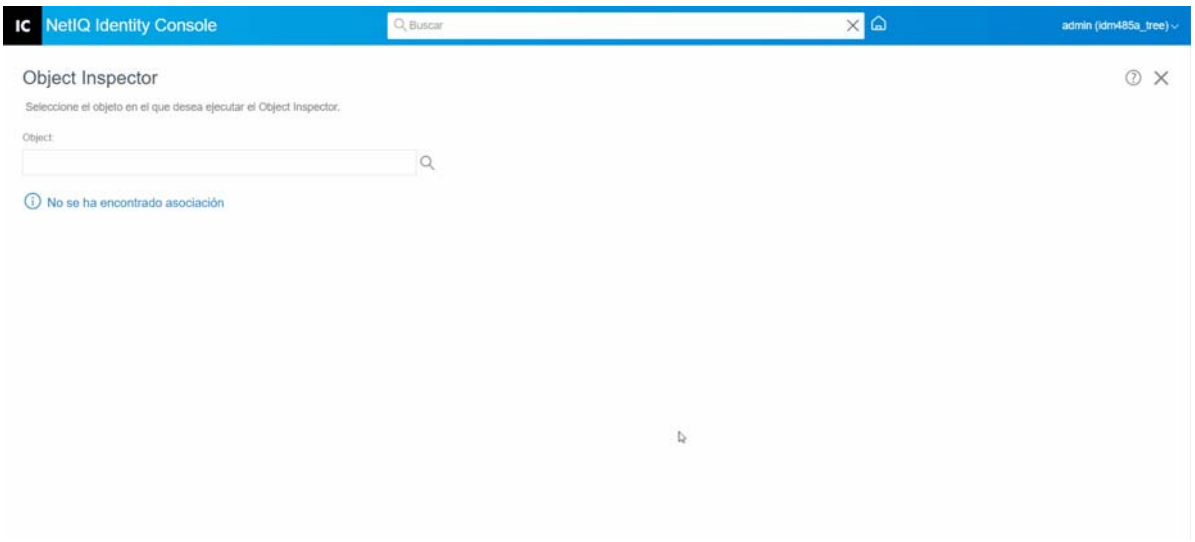
Puede utilizar Object Inspector para ver información detallada acerca de cómo participa un objeto en las relaciones de Identity Manager. Entre estas relaciones, se incluyen los sistemas conectados asociados al objeto, cómo fluyen los datos entre el repositorio seguro de identidades y los sistemas conectados, los valores de atributos que están almacenados actualmente en el repositorio seguro de identidades y en los sistemas conectados, las configuraciones del controlador del sistema conectado, etc.

Para inspeccionar los objetos de Identity Manager, haga clic en la opción **Object Inspector** de la página principal de Identity Console. Especifique el nombre completo del objeto que desea inspeccionar o haga clic en el icono Examinar para buscar y seleccionar el objeto que desee.

En la sección Sistemas conectados, se muestra cada uno de los sistemas conectados a los que está asociado el objeto. Mediante la página **Object Inspector**, puede realizar las siguientes acciones:

- **Adición de una asociación**: para añadir una nueva asociación a un sistema conectado, haga clic en el icono +. Busque y seleccione el **Objeto Controlador de integración** y especifique el **ID de objeto asociado**.
- **Supresión de una asociación**: para suprimir una asociación a un sistema conectado, marque la casilla de verificación situada a la izquierda de la asociación y haga clic en el icono 🗑. Para suprimir todas las asociaciones, marque la casilla de verificación situada debajo de la columna Suprimir y haga clic en el icono 🗑.

Figura 25-1 *Inspección de objetos de Identity Manager*



26 Gestión del flujo de datos

El flujo de datos muestra los canales de editor y de suscriptor de varios controladores en una sola vista. Esta opción permite ver y actualizar la propiedad de los datos de todos los controladores.

Para acceder a la vista de tabla del flujo de datos, haga clic en el módulo **Flujo de datos (vista de tabla)** de la página principal de Identity Console. A continuación, examine y seleccione el contenedor adecuado para visualizar la lista de controladores.

Para gestionar la propiedad de los datos de controladores individuales, realice los siguientes pasos:

1 Cada controlador tiene dos botones para gestionar el flujo de datos a través de los canales de editor y suscriptor. El botón de la parte izquierda gestiona el flujo de datos del canal de editor y el botón de la derecha gestiona el flujo de datos del canal de suscriptor.

   1a **Sincronizar**: seleccione esta opción para sincronizar el atributo específico. El icono cambiará a ↑ en el canal de editor y a ↓ en el canal de suscriptor después de seleccionar esta opción.

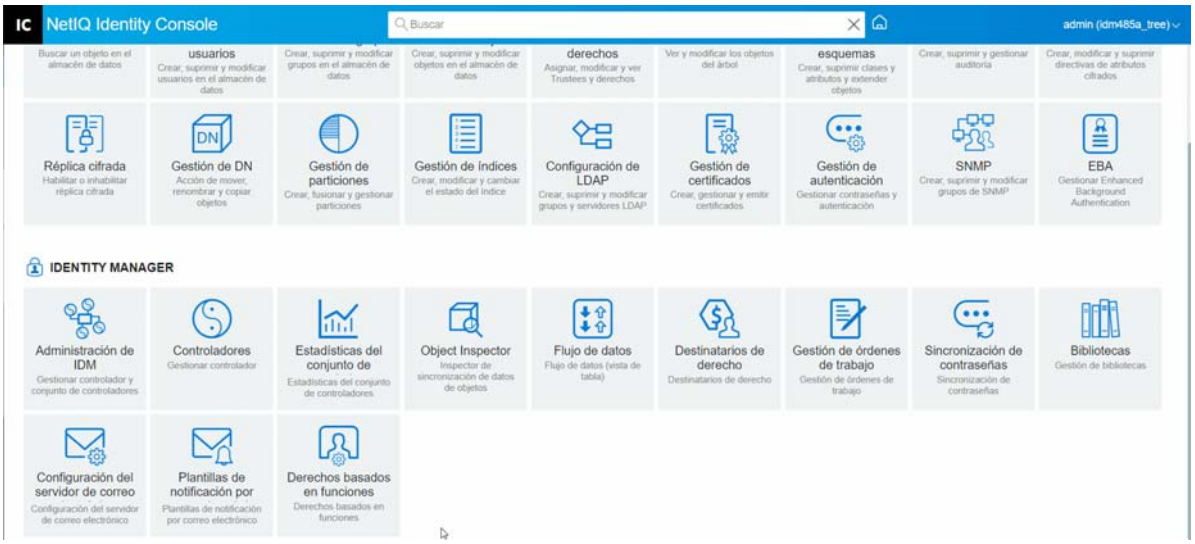
   1b **Ignorar**: seleccione esta opción para detener la sincronización del atributo específico. El icono cambiará a ⊘ después de seleccionar esta opción.

   1c **Notificar**: seleccione esta opción para que se le notifique cualquier cambio realizado en un atributo específico. No obstante, el cambio no se sincronizará automáticamente. El icono cambiará a 🔔 después de seleccionar esta opción.

   1d **Restaurar**: seleccione esta opción para restablecer el valor del atributo al valor especificado por el otro canal. El icono cambiará a ↻ después de seleccionar esta opción.

   Nota: Puede definir este valor en el canal de editor o de suscriptor. No puede definir este valor en ambos canales de forma simultánea.

Figura 26-1 *Gestión del flujo de datos*



27 Gestión de destinatarios de derechos

Las referencias de derechos y los resultados se conservan en los objetos que tienen un derecho otorgado o revocado. Las referencias de derechos y los resultados contienen información sobre si el derecho se ha otorgado o revocado actualmente en ese objeto. Los destinatarios del derecho son todos los objetos que contengan referencias a un derecho.

Referencias a derechos

Para ver las referencias a derechos y los resultados, haga clic en la opción **Destinatarios de derecho** de la página principal de Identity Console y seleccione Referencia a derechos. A continuación, especifique el nombre completo del objeto que es un `DirXML-EntitlementRecipient`. Puede hacer clic en el botón Selector de objetos  para seleccionar el objeto.

Resultados de derechos

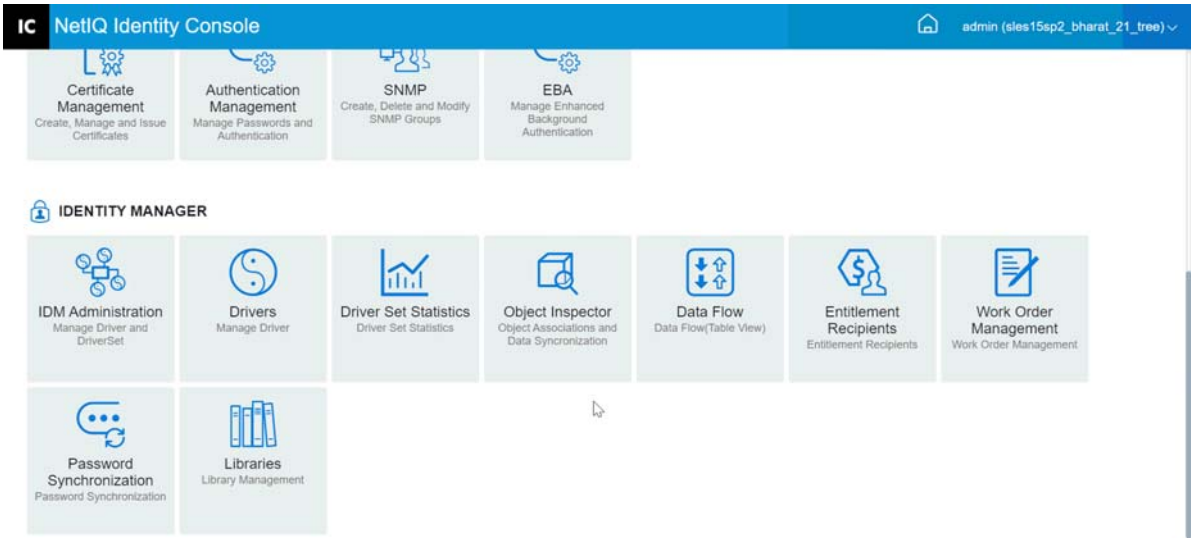
En la tabla Resultados de derechos de Identity Console, se muestran los resultados de derechos asociados al objeto seleccionado. Para ver el derecho asociado, seleccione el DN del derecho. Para ver los resultados del derecho en formato XML, seleccione el ID de resultado correspondiente.

- **Encabezados de columna de resultados de derechos**: los encabezados de columna incluyen el nombre completo del derecho, su estado actual de concesión o revocación, la procedencia de los resultados (origen), el estado del resultado, todos los mensajes que hayan llegado con el resultado, y la marca horaria y la identificación del resultado.
  - **DN con derecho**: haga clic en el nombre completo del derecho del objeto para que aparezca la página Modificar objeto. Esta página permite ver cómo se han asignado los atributos de eDirectory al objeto. También puede utilizar esta página para modificar los atributos del objeto. El número de categorías mostradas en la página Modificar objeto depende del objeto seleccionado.
  - **Estado:** muestra si el derecho se ha otorgado o revocado. Si el módulo auxiliar encuentra otro valor en el flujo XML, se muestra ese valor directamente.
  - **Mensaje**: cualquier mensaje del shim de DirXML asociado con el estado de los resultados. La información que se almacena en la parte <msg></msg> del archivo de resultados XML. Haga clic en la entrada ID de resultados para ver todos los detalles del resultado en una página del visor XML.

- **Marca horaria**: la hora a la que el motor de derechos procesó y escribió el resultado. Haga clic en la entrada ID de resultados para ver todos los detalles del resultado en una página del visor XML.
- **ID de resultado**: haga clic en la entrada ID de resultados para ver todos los detalles del resultado en una página del visor XML. Cuando termine de ver los resultados, haga clic en Cerrar.

Para suprimir una entrada de resultados de derechos, haga clic en la casilla de verificación situada a la izquierda de la entrada de resultados de derechos y seleccione **Suprimir**.

Figura 27-1 *Gestión de destinatarios de derechos*



28 Gestión de órdenes de trabajo

Los controladores de Identity Manager pueden crear órdenes de trabajo como resultado de eventos procesados por los controladores. Por ejemplo, si utiliza un controlador de Recursos Humanos (SAP HR, PeopleSoft, etc.), puede conseguir que el controlador genere una orden de trabajo cada vez que se añada un nuevo usuario.

Puede utilizar Identity Console para crear y gestionar órdenes de trabajo creadas para distintos controladores compatibles con esta funcionalidad específica.

Creación de una nueva orden de trabajo

Para crear una nueva orden de trabajo, realice los siguientes pasos:

1. Haga clic en la opción **Orden de trabajo** de la página de destino de Identity Console.
2. Haga clic en el icono + para crear una nueva orden de trabajo.
3. Especifique un nombre para la orden de trabajo y, a continuación, haga clic en **Aceptar**.

   El nombre se utiliza para el nombre del objeto WorkOrder del repositorio seguro de identidades.
4. Cumplimente los siguientes campos:

   Estado: una nueva orden de trabajo puede presentar el siguiente estado:**Pendiente** o **Retenido**. Por lo general, la orden de trabajo presenta el estado **Pendiente**. Para detener una orden de trabajo, seleccione **Retenido**. Una vez que se haya procesado una orden de trabajo, aparecerá el estado resultante de la orden de trabajo en este campo.

   Fecha límite: puede optar por conseguir que el controlador procese la orden de trabajo al instante o programar la orden de trabajo. Para programar una fecha límite, haga clic en el icono del calendario. Utilice el calendario para elegir la fecha. Utilice las flechas para seleccionar el mes, el año y la hora.

   Repetir orden de trabajo: seleccione esta opción para que la orden de trabajo se procese varias veces. Especifique el intervalo de tiempo mediante la selección del número de semanas, días, horas o minutos antes de que se repita la orden de trabajo. La orden de trabajo deja de repetirse en la fecha de supresión a menos que se suprima o se edite manualmente o el controlador envíe un mensaje de error.

   Fecha de supresión: utilice el control de calendario para seleccionar una fecha en la que suprimir las órdenes de trabajo configuradas. Las órdenes de trabajo con estado de error no se eliminan a menos que seleccione **Suprimir la orden de trabajo incluso cuando tenga un error**.

Órdenes de trabajo dependientes: al crear una nueva orden de trabajo, puede establecerla como dependiente de una o varias órdenes de trabajo. Haga clic en  para buscar y seleccionar órdenes de trabajo dependientes. Para eliminar una orden de trabajo en la lista, seleccione una orden de trabajo y, a continuación, haga clic en  .

Tipo: utilice este campo para especificar un tipo de orden de trabajo. El controlador no cambia este atributo. El atributo se pasa al objeto WorkToDo cuando se procesa la orden de trabajo.

Número de orden de trabajo: un número de orden de trabajo exclusivo. Este valor se puede asignar a un sistema corporativo de órdenes de trabajo que no sea NetIQ eDirectory, como una base de datos de órdenes de trabajo.

Información de contacto: información de contacto de la persona responsable de la orden de trabajo.

Registro de procesamiento de órdenes de trabajo: después de procesar una orden de trabajo, el controlador registra en este campo sus resultados, incluido el estado. Esto le permite comprobar el estado actual de la orden de trabajo e identificar los problemas que se han encontrado en el controlador al intentar configurarla.

El atributo de estado de la orden de trabajo permanece pendiente hasta que esta se procese. La orden de trabajo se procesa cuando ha vencido la fecha límite. El controlador notifica los resultados del proceso mediante la definición del atributo de estado como Configurado, Advertencia o Error. Si la orden de trabajo presenta el estado Retenido, se omitirá.

- **Pendiente:** el controlador está esperando a la fecha límite para completar la orden de trabajo.
- **Configurado:** la orden de trabajo se ha procesado correctamente.
- **Error:** el controlador no ha podido realizar la orden de trabajo.
- **Advertencia:** hay una advertencia relacionada con la orden de trabajo. Por ejemplo, si la orden de trabajo tiene un orden de trabajo dependiente con una fecha de límite posterior, el controlador enviará una advertencia.

Descripción: la descripción de la orden de trabajo.

Contenido de la orden de trabajo: los datos de este campo los utilizan las reglas del controlador para procesar la orden de trabajo. Por ejemplo, puede ser el XML que la transformación de comandos utiliza para procesar la orden de trabajo.

Supresión de una orden de trabajo existente

Para suprimir una orden de trabajo existente, realice los siguientes pasos:

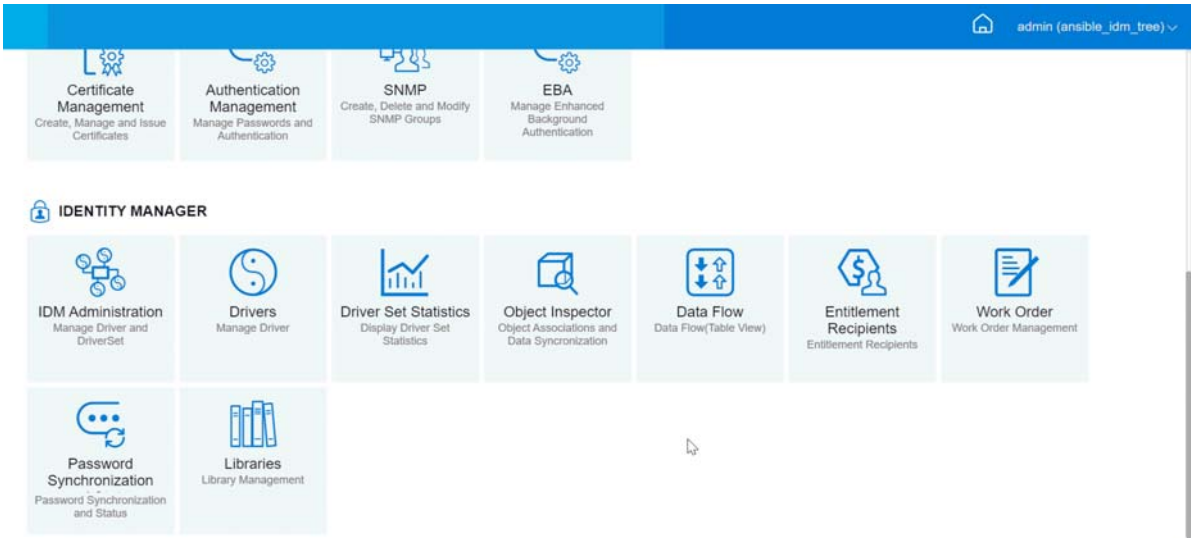
1. Haga clic en la opción **Orden de trabajo** de la página de destino de Identity Console.
2. Seleccione la orden de trabajo que desee eliminar.
3. Haga clic en el icono  .

Filtrado de la lista de órdenes de trabajo

Para filtrar la lista de órdenes de trabajo, realice los siguientes pasos:

1. Haga clic en la opción **Orden de trabajo** de la página de destino de Identity Console.
2. Haga clic en **Acciones** en Gestión de órdenes de trabajo.
3. En el menú desplegable, seleccione el tipo de filtro:
   - **Mostrar todo:** se muestran todas las órdenes de trabajo asociadas al controlador.
   - **Configurado:** solo se muestran las órdenes de trabajo configuradas asociadas al controlador.
   - **Error:** solo se muestran las órdenes de trabajo con estado de error.
   - **Retenido:** se muestran las órdenes de trabajo que se han retenido manualmente.
   - **Pendiente:** se muestran las órdenes de trabajo que aún no han vencido.

Figura 28-1 *Gestión de órdenes de trabajo*



29 Gestión del estado y la sincronización de contraseñas

Puede comprobar la sincronización y el estado de las contraseñas de controladores individuales mediante el portal de Identity Console. Para verificar esto, seleccione el módulo **Sincronización de contraseñas** en la página principal de Identity Console.

Puede llevar a cabo las siguientes acciones mediante este módulo:

Comprobación del estado de sincronización de contraseñas

Puede determinar si la contraseña de distribución de un usuario específico es la misma que la del sistema conectado. Lleve a cabo los pasos siguientes para comprobar el estado de sincronización de contraseñas:

1. En la Identity Console, seleccione **Sincronización de contraseñas** > **Estado de contraseña**.
2. Busque y seleccione un usuario para el que desee comprobar el estado de la contraseña.
3. Se pueden ver los siguientes estados de contraseña:
   - Se sincronizan las contraseñas.
   - NO se sincronizan las contraseñas.
   - El estado de la contraseña es desconocido, ya que no se puede establecer contacto con el sistema conectado para solicitar una comprobación de contraseña.
   - Se ha producido un error.

Nota: Para obtener más información sobre cada uno de los estados anteriores, debe colocar el puntero sobre el estado que aparece en la columna **Estado de contraseña**.

La tarea Estado de contraseña provoca que el controlador realice una acción Verificación de contraseña de objetos. No todos los controladores admiten la comprobación de contraseñas. Los que sí lo hacen deberán contener una función de comprobación de contraseñas en el inventario del controlador. Identity Console no permite que se envíen operaciones de comprobación de contraseñas a controladores que no contengan esta función en el inventario.

La acción Verificar contraseña de objetos comprueba la contraseña de distribución. Si la contraseña de distribución no se está actualizando, es posible que Verificar contraseña de objetos informe de que las contraseñas no están sincronizadas.

La contraseña de distribución no se actualiza si se produce una de las siguientes situaciones:

- Está utilizando el método de sincronización mediante la contraseña de NDS o universal que se va a sincronizar. Para obtener más información, consulte “Creación de una directiva de contraseñas con parámetros personalizados” en la página 118.

Nota: La acción Estado de contraseña comprueba la contraseña de NDS en lugar de la contraseña universal en el repositorio seguro de identidades. Por lo tanto, si la directiva de contraseñas del usuario no especifica que se sincronice la contraseña de NDS con la contraseña universal, las contraseñas siempre se notifican como no sincronizadas. De hecho, es posible que la contraseña de distribución y la del sistema conectado estén sincronizadas, pero la comprobación de estado de contraseñas no será precisa a menos que la contraseña de NDS y la de distribución estén sincronizadas con la contraseña universal.

Verificación de los ajustes de sincronización de contraseñas

La función Sincronización de contraseñas permite sincronizar contraseñas entre sistemas conectados mediante Identity Manager. Para ver los ajustes de Sincronización de contraseñas de los sistemas conectados, seleccione el conjunto de controladores adecuado en el menú desplegable.

Mediante la Sincronización de contraseñas, puede configurar sistemas conectados para realizar lo siguiente:

- Publicar contraseñas en Identity Manager.
- Suscribirse a contraseñas de Identity Manager u otros sistemas conectados.
- Aplicar directivas de contraseñas en los sistemas conectados.
- Enviar mensajes de correo electrónico de notificación.

Lleve a cabo los pasos siguientes para comprobar los parámetros de sincronización de contraseñas:

1. En Identity Console, seleccione **Sincronización de contraseñas** > **Sincronización de contraseñas** desde la página principal.
2. Seleccione el conjunto de controladores que contiene el controlador cuyos ajustes desea comprobar.
3. Haga clic en el nombre del controlador en la lista.

   Nota: Los ajustes habilitados e inhabilitados varían en función del controlador. Solo están disponibles los ajustes para las funciones compatibles con el controlador.

   ---

4. Compruebe que los ajustes se hayan configurados correctamente.

   Identity Manager acepta contraseñas (canal de editor): si esta opción está habilitada, Identity Manager permite que las contraseñas fluyan desde el sistema conectado al repositorio seguro de identidades. Si se inhabilita esta opción, no se permite el flujo de elementos `<contraseña>` al Identity Manager. Se quitan del archivo XML mediante una directiva de sincronización de contraseñas en el canal de editor.

   Este ajuste se aplica a las contraseñas de usuario proporcionadas por el propio sistema conectado y a los valores de contraseña creados por una directiva en el canal de editor.

Si esta opción está habilitada, pero la opción Contraseña de distribución que aparece debajo de ella está inhabilitada, un valor de <contraseña> procedente del sistema conectado se escribe directamente en la contraseña universal del repositorio seguro de identidades. Si la directiva de contraseñas del usuario no habilita la contraseña universal, la contraseña se escribirá en la contraseña de NDS.

Usar la contraseña de distribución para la sincronización de contraseñas: este parámetro solo está disponible si el ajuste **Identity Manager acepta contraseñas (canal de editor)** está activado.

Si esta opción está habilitada, se escribe un valor de contraseña procedente del sistema conectado en la contraseña de distribución. La contraseña de distribución es reversible, lo que significa que se puede recuperar del almacén de datos del repositorio seguro de identidades para la sincronización de contraseñas. Identity Manager la utiliza para la sincronización bidireccional de contraseñas con sistemas conectados. Para que Identity Manager distribuya contraseñas de este sistema a otros, esta opción debe estar habilitada.

Aceptar la contraseña solo si cumple la directiva de contraseñas del usuario: este parámetro solo está disponible si el ajuste **Usar la contraseña de distribución para la sincronización de contraseñas** está habilitado.

Si se selecciona esta opción, Identity Manager no escribe una contraseña de este sistema conectado en la contraseña de distribución del repositorio seguro de identidades ni la publica en los sistemas conectados a menos que la contraseña cumpla con la directiva de contraseñas del usuario.

Si una contraseña no la cumple, habilite el ajuste **Restablecer la contraseña del usuario a la contraseña de distribución** para restablecer la contraseña del usuario en el sistema conectado. Esto le permite aplicar la directiva de contraseñas en el sistema conectado y en el repositorio seguro de identidades. Si no selecciona esta opción, es posible que las contraseñas de usuario no estén sincronizadas en los sistemas conectados. Sin embargo, debe tener en cuenta las directivas de contraseñas del sistema conectado a la hora de decidir si desea utilizar esta opción. Es posible que algunos sistemas conectados no permitan el restablecimiento porque no admiten la repetición de contraseñas.

Al utilizar el ajuste **Notificar al usuario el error de sincronización de la contraseña por correo electrónico**, puede informar a los usuarios cuando falle la configuración o el restablecimiento de una contraseña. La notificación es especialmente útil para esta opción. Si el usuario cambia a una contraseña permitida por el sistema conectado, pero rechazada por Identity Manager debido a la directiva de contraseñas, el usuario no sabrá que la contraseña se ha restablecido hasta que reciba una notificación o intente entrar al sistema conectado con la contraseña antigua.

Aceptar siempre contraseña; ignorar las directivas de contraseñas: este parámetro solo está disponible si el ajuste **Usar la contraseña de distribución para la sincronización de contraseñas** está habilitado.

Si selecciona esta opción, Identity Manager no aplica la directiva de contraseñas del usuario en este sistema conectado. Identity Manager escribe la contraseña de este sistema conectado en la contraseña de distribución del repositorio seguro de identidades y la distribuye a otros sistemas conectados independientemente del cumplimiento de las directivas de contraseñas.

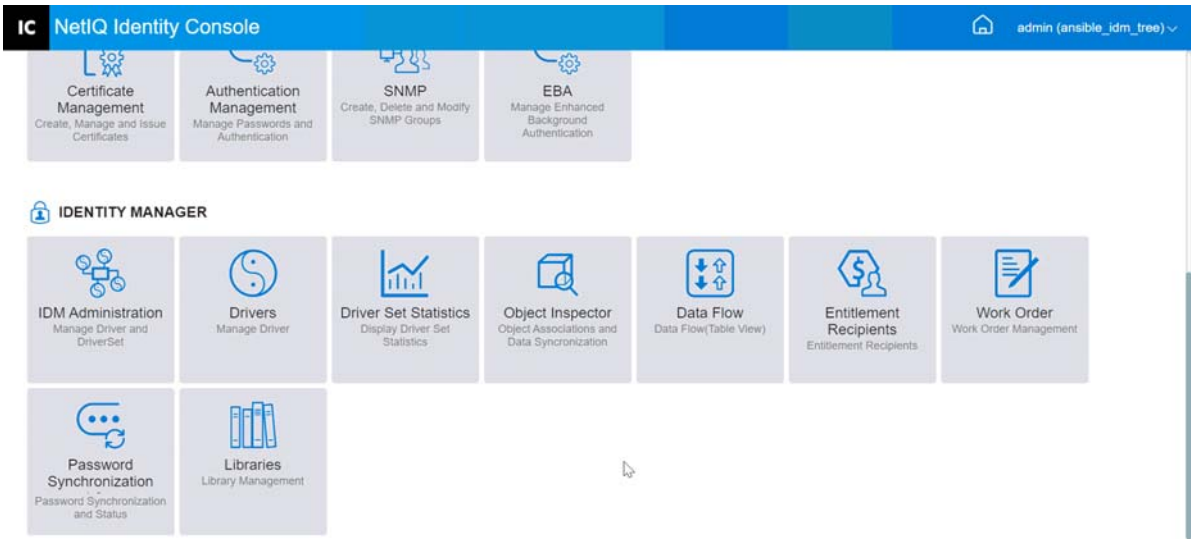
La aplicación acepta contraseñas (canal de suscriptor): si habilita esta opción, el controlador envía contraseñas desde el repositorio seguro de identidades a este sistema conectado. Esto también significa que si un usuario cambia la contraseña en un sistema conectado diferente que publica contraseñas en la contraseña de distribución del repositorio seguro de identidades, la contraseña se cambiará en este sistema conectado.

Por defecto, la contraseña de distribución es la misma que la contraseña universal del repositorio seguro de identidades, por lo que los cambios realizados en la contraseña universal del repositorio seguro de identidades también se envían al sistema conectado.

Notificar al usuario el error de sincronización de la contraseña por correo electrónico: si habilita esta opción, se enviará un mensaje de correo electrónico al usuario en caso de que no se sincronice, se defina o se restablezca una contraseña. El mensaje de correo electrónico enviado al usuario se basa en una plantilla de correo electrónico. Esta plantilla la proporciona la aplicación Sincronización de contraseñas. Sin embargo, para que funcione la plantilla, debe personalizarla y especificar un servidor de correo electrónico para enviar los mensajes de notificación. Para obtener instrucciones, consulte Configuring E-Mail Notification (Configuración de la notificación por correo electrónico) en *NetIQ Identity Manager Password Management Guide*.(Guía de gestión de contraseñas de NetIQ Identity Manager).

5 Cuando haya terminado, haga clic en **Guardar** para guardar los cambios. Los ajustes se guardan como Valores de configuración global.

Figura 29-1 *Gestión de la sincronización de contraseñas*



30 Gestión de bibliotecas

Los objetos de biblioteca almacenan varias directivas y otros recursos compartidos por uno o varios controladores. Se puede crear un objeto de biblioteca en un objeto Conjunto de controladores o en cualquier contenedor de eDirectory. Pueden existir varias bibliotecas en un árbol de eDirectory. Los controladores pueden hacer referencia a cualquier biblioteca del árbol siempre que el servidor en el que se ejecute el controlador contenga una réplica de lectura/escritura o principal del objeto de biblioteca.

Las hojas de estilo, las directivas, las reglas y otros objetos de recursos se pueden almacenar en una biblioteca y se puede hacer referencia a ellos mediante uno o varios controladores.

Mediante el módulo Gestión de bibliotecas, puede realizar las siguientes tareas:

- "Visualización y supresión de una biblioteca existente" en la página 201
- "Visualización y supresión de objetos de la biblioteca" en la página 201

Visualización y supresión de una biblioteca existente

Para ver y suprimir una biblioteca existente, realice los siguientes pasos:

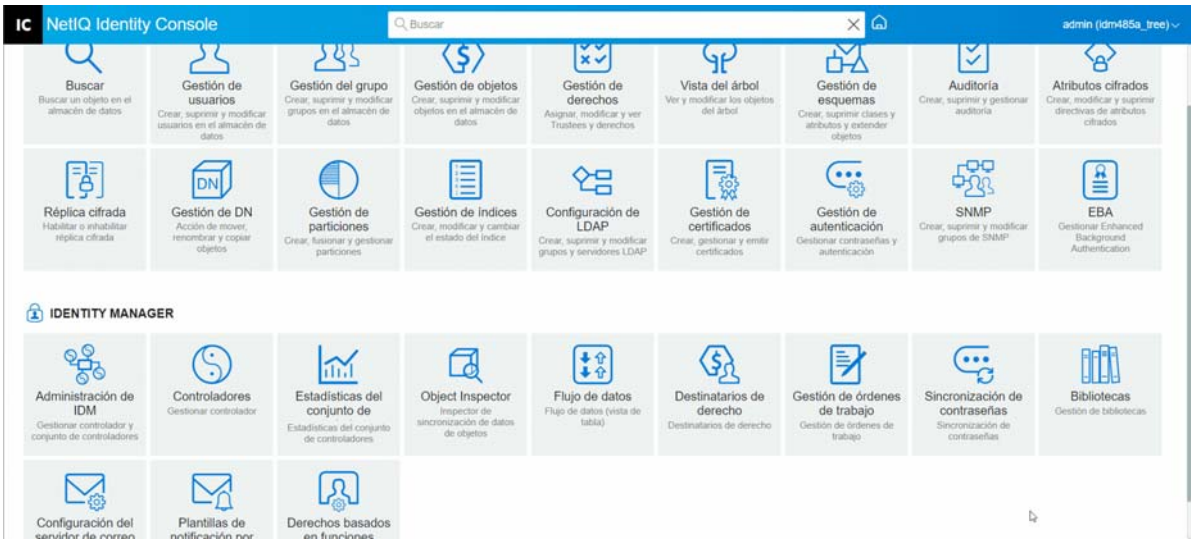
1. En Identity Console, seleccione la opción **Bibliotecas** de la página principal.
2. Seleccione la biblioteca adecuada en la lista.
3. Haga clic en el icono  . Haga clic en **Aceptar** para confirmar.

Visualización y supresión de objetos de la biblioteca

Puede ver y suprimir directivas y tablas de asignación de objetos de biblioteca. Para suprimir objetos, realice los siguientes pasos:

1. En Identity Console, seleccione la opción **Bibliotecas** de la página principal.
2. Haga clic en la biblioteca adecuada en la lista.
3. Para suprimir directivas, seleccione la pestaña **Directivas**.
4. Seleccione la directiva adecuada en la lista y haga clic en el icono  .
5. Para suprimir tablas de asignación, seleccione la pestaña **Tablas de asignación**.
6. Seleccione la tabla de asignación adecuada en la lista y haga clic en el icono  .
7. Haga clic en **Aceptar** para confirmar.

Figura 30-1 *Gestión de bibliotecas*



31 Gestión de las opciones del servidor de correo electrónico

Puede utilizar las opciones del servidor de correo electrónico para especificar la configuración del servidor de correo electrónico SMTP.

Nombre del host

El nombre de host de su servidor de correo electrónico SMTP. También puede ser una dirección IP. También puede especificar un puerto personalizado seguido del nombre de host o la dirección IP.

Importante: Utilice dos puntos (:) como separador entre el nombre de host o la dirección IP y el puerto.

De

Puede especificar una dirección de correo electrónico válida que se mostrará como el campo De del encabezado del mensaje de correo electrónico.

Valor de tiempo límite

La opción de tiempo límite permite definir el límite de tiempo (en segundos) para enviar mensajes de correo electrónico de notificación.

Habilitar SSL

Si es necesario, puede habilitar la opción SSL.

Autenticarse en un servidor empleando credenciales

Se utiliza para los servidores SMTP seguros. Si su servidor requiere autenticación antes de enviar correo electrónico, especifique aquí el nombre de usuario y la contraseña.

Aunque la información de la autenticación se especifica aquí, es posible que también haya que especificarla por separado para la aplicación que va a enviar los correos electrónicos de notificación.

Por ejemplo, puede utilizar la información de autenticación que especifique aquí para enviar notificaciones por correo electrónico de Contraseña olvidada. Sin embargo, la sincronización de contraseñas de Identity Manager utiliza la directiva de controlador para enviar mensajes de correo electrónico de notificación. Es posible que también tenga que proporcionar la información de autenticación en esa directiva de controlador.

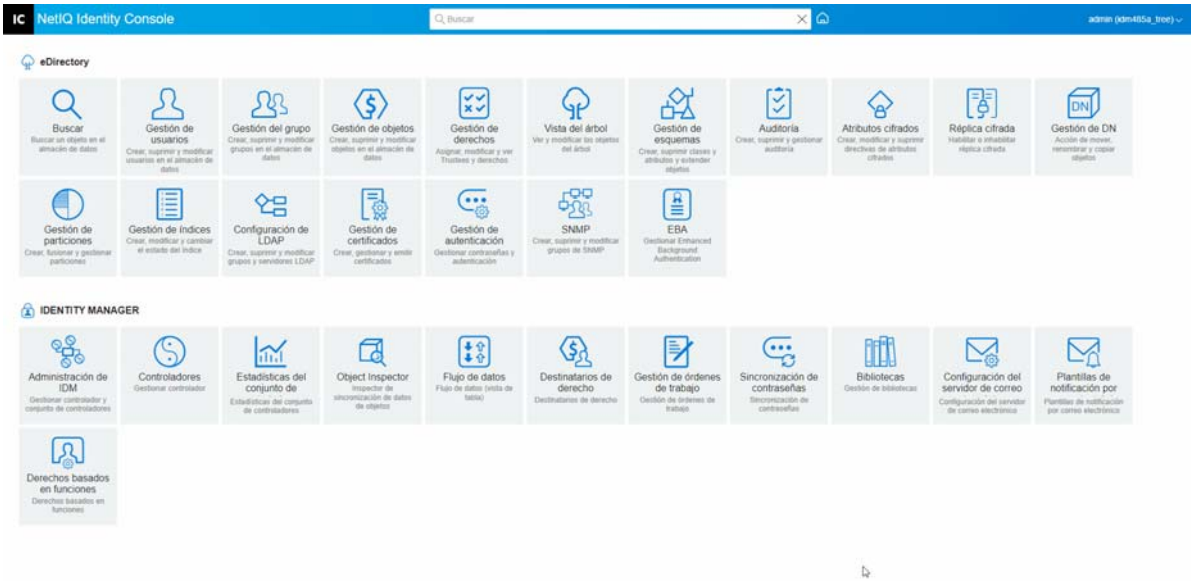
Para realizar la autenticación en el servidor, realice los siguientes pasos:

1. Seleccione la opción **Autentíquese en el servidor mediante sus credenciales**.
2. Especifique el **nombre de usuario** y la **contraseña**.
3. Haga clic en **Probar conexión del servidor** para verificar la conectividad.

4. Haga clic en **Guardar**.

Nota: Después de guardar la información de credenciales, la opción **Probar conexión del servidor** se inhabilita.

Figura 31-1 *Configuración del servidor de correo electrónico*



32 Gestión de plantillas de correo electrónico

En esta lista, se muestran las plantillas de notificación disponibles. Utilice estas plantillas para enviar un mensaje de correo electrónico a los usuarios de este árbol. Dichas plantillas se pueden personalizar con texto propio.

Algunas aplicaciones proporcionan sus propias plantillas. Estos objetos Plantilla se encuentran en el Contenedor de seguridad, que normalmente se encuentra en la raíz del árbol.

La lista se puede ordenar por nombre, fecha o asunto.

Asunto

El texto que un usuario ve en el encabezado Asunto de un mensaje de correo electrónico. Para editar una plantilla, haga clic en el encabezado Asunto de la plantilla. Mediante la interfaz de Editar plantilla de notificación por correo electrónico, puede modificar la plantilla y sus detalles.

Nombre de plantilla

Cada plantilla tiene un nombre exclusivo. La aplicación que envía el mensaje de correo electrónico hace referencia a este nombre.

Última modificación

La fecha y la hora en las que se modificó por última vez la plantilla.

Nuevo

Permite crear una plantilla de correo electrónico nueva.

1. Haga clic en el icono +.
2. Especifique un nombre para la nueva plantilla (por ejemplo, Aprobación) y haga clic en **Aceptar**.

Si ha inhabilitado las ventanas emergentes, volverá a la ventana emergente Editar plantilla de notificación por correo electrónico. El nuevo nombre de plantilla aparece en la columna Nombre, pero se muestra [No Subject] (Sin asunto) en la columna del encabezado Asunto. En este caso, haga clic en [No Subject] (Sin asunto) para poder proporcionar detalles en la nueva plantilla.

Editar plantilla de notificación por correo electrónico

La página Editar plantilla de notificación por correo electrónico permite modificar la plantilla de correo electrónico. La plantilla se puede personalizar con texto propio.

Nombre de plantilla

Muestra el nombre de la plantilla.

Tema

El texto que un usuario ve en el encabezado Asunto de un mensaje de correo electrónico. Puede cambiar el texto de la línea del asunto. El nombre real de la plantilla sigue siendo el mismo.

Enviar como

El formato que utiliza el servidor SMTP para enviar el mensaje de correo electrónico: Texto o HTML.

Testigos o etiquetas de sustitución

Las etiquetas de sustitución ayudan a personalizar el mensaje para el usuario. Puede copiar etiquetas de sustitución de la lista de etiquetas disponibles y pegarlas en el mensaje.

Cada plantilla incluye testigos o etiquetas de sustitución por defecto, que son variables necesarias para personalizar el correo electrónico del usuario. Por ejemplo, la plantilla de correo electrónico Contraseña olvidada para enviar una contraseña al usuario incluye el testigo o la etiqueta de sustitución por defecto llamada "$CurrentPassword".

Añadir: puede definir otros testigos o etiquetas de sustitución para utilizarlos en el cuerpo del mensaje.

Para añadir un testigo o una etiqueta de sustitución, realice los siguientes pasos:

1. Haga clic en el icono  .
2. Especifique el **nombre** y la **descripción** en la ventana **Añadir etiqueta de sustitución**.
3. Haga clic en **Aceptar**.
4. El nuevo testigo o etiqueta de sustitución aparece en la columna Etiquetas de sustitución.

Copiar etiqueta: haga clic en  para copiar la etiqueta seleccionada en el buffer del sistema y, a continuación, puede hacer clic con el ratón para pegarla y utilizarla en la línea de asunto o en el cuerpo del mensaje.

Suprimir: seleccione un testigo o una etiqueta de sustitución en la lista y haga clic en  para suprimir la etiqueta de la lista. Asegúrese de que no elimina ninguna etiqueta que sea necesaria para el cuerpo del mensaje.

Cuerpo del mensaje

El texto del mensaje de correo electrónico.

Haga clic en **Actualizar** después de especificar todas las modificaciones de la plantilla de notificación por correo electrónico.

Suprimir

Elimina (del depósito de identidades) las plantillas que ha creado. No se pueden suprimir las plantillas por defecto que se incluyen con aplicaciones como, por ejemplo, Identity Manager.

1. Seleccione la plantilla que desea suprimir.

   Si hace clic en el encabezado Asunto de la plantilla, Identity Console proporciona el recuadro de diálogo "Edit Email Templates" (Editar plantillas de correo electrónico).

2. Haga clic en el icono Suprimir.
3. Haga clic en **Aceptar**.

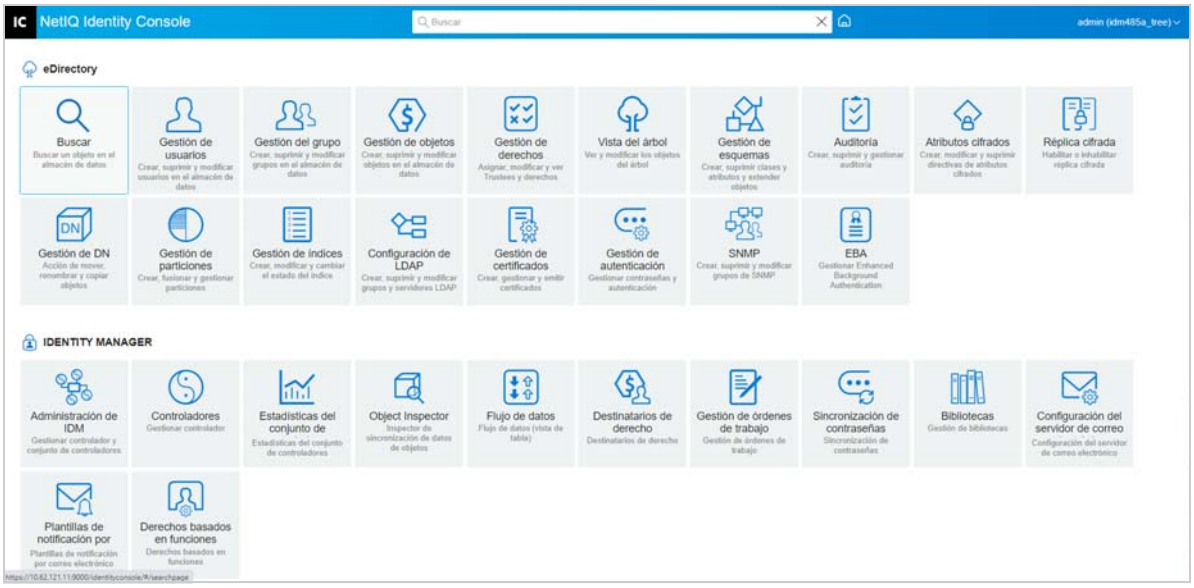
Filtrar plantillas

Permite filtrar la plantilla de correo electrónico que se desea mostrar. Solo se mostrarán las plantillas seleccionadas. La opción "Filter by all" (Filtrar por todo) muestra todas las plantillas.

Actualizar plantillas

Haga clic en el icono para actualizar y eliminar las plantillas de filtro aplicadas.

Figura 32-1 *Plantillas de notificación por correo electrónico*



33 Gestión de derechos basados en funciones

El derecho basado en funciones permite otorgar derechos en sistemas conectados a un grupo de usuarios de NetIQ® Identity Console. Mediante las directivas de derechos basados en funciones, puede agilizar la gestión de directivas empresariales y reducir la necesidad de configurar los controladores de Identity Manager.

El módulo Derecho basado en funciones incluye lo siguiente:

Derecho basado en funciones

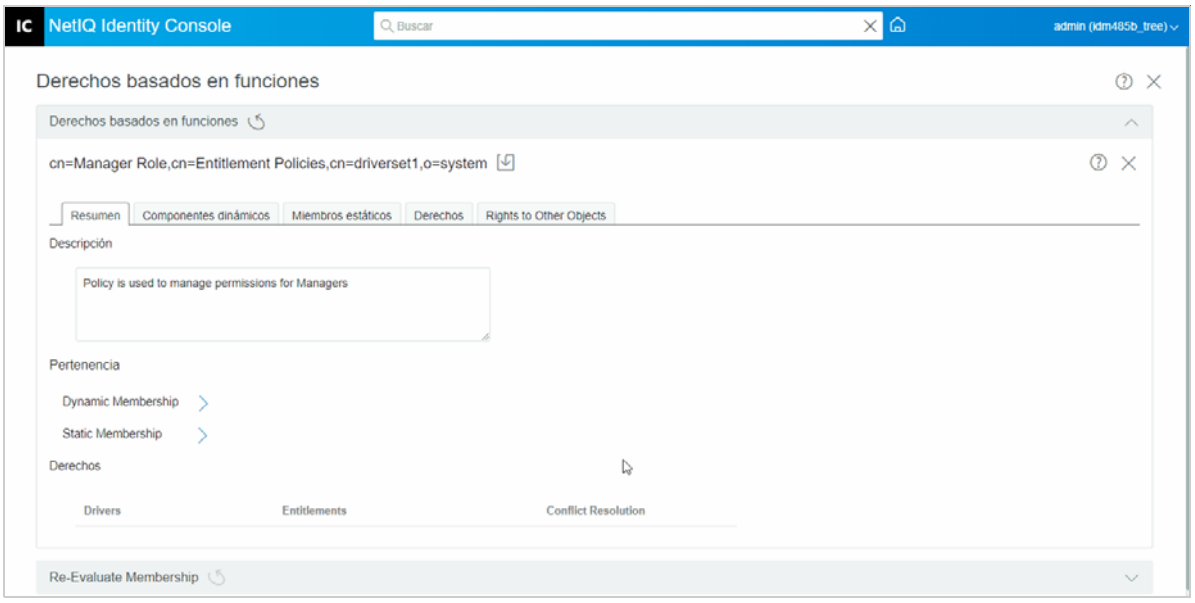
Una directiva de derechos basados en funciones es un objeto Grupo dinámico de Identity Console con funciones adicionales que permiten otorgar derechos basados en funciones en los sistemas conectados. Al crear una directiva de derechos basados en funciones, puede definir la pertenencia de la directiva y los derechos que deben otorgarse a los miembros de la directiva de derechos basados en funciones. Cada directiva de derechos basados en funciones está asociada a un único objeto Conjunto de controladores asignado a un servidor específico. Al igual que un controlador de Identity Manager, cada directiva de derechos solo puede gestionar objetos que se encuentran en una réplica principal o de lectura/escritura en el servidor al que se ha asignado.

En las secciones siguientes, se describen detalladamente los derechos basados en funciones:

Resumen

Esta página proporciona información general de los criterios de pertenencia y los derechos de la directiva de derechos.

Figura 33-1 *Página de resumen*



Pertenencia:

Los criterios especificados para la pertenencia dinámica se muestran con la sintaxis de un filtro LDAP. Identidad de búsqueda indica los derechos del objeto que se utilizan al consultar la pertenencia dinámica, y DN base y Ámbito indican la parte del árbol que se incluye en la consulta.

Para ver las inclusiones y las exclusiones de la pertenencia estática, marque la casilla de verificación.

La lista combinada de todos los miembros no se muestra en la página Resumen porque puede ser larga. Para ver una lista combinada de todos los miembros de la directiva de derechos, tanto dinámicos como estáticos, utilice la pestaña Pertenencia > Ver pertenencia.

Derechos:

Los derechos en los sistemas conectados que se otorgan a los miembros de la directiva de derechos. Tenga en cuenta que los derechos basados en funciones son poco coherentes con los sistemas conectados. Esto significa que el estado de un derecho en un sistema conectado no se muestra en la interfaz de la directiva de derechos. Si otorga un derecho a una directiva de derechos y, más tarde, ese derecho ya no está disponible en el sistema conectado, el derecho seguirá figurando en la directiva de derechos hasta que lo elimine manualmente de la lista.

Resolución de conflictos:

En los derechos basados en funciones que tienen valores, estos métodos se utilizan para determinar los valores otorgados a un usuario si dos o más directivas de derechos basados en funciones conceden diferentes valores a ese usuario. Un ejemplo de derecho que tiene valores es la pertenencia a listas de distribución de correo electrónico, donde los valores son los nombres de las listas de distribución.

El método de resolución de conflictos se define por separado para cada derecho individual en cada objeto Controlador. Si se utiliza un derecho en varias directivas de derechos basados en funciones, el método de resolución de conflictos es el mismo en todas esas directivas. Para cambiar el método de resolución de conflictos de un derecho, cambie el valor de ese derecho en el inventario de controladores de ese controlador.

- **No reconocido:** la directiva de derechos basados en funciones no se ha completado en el asistente o la configuración se ha escrito incorrectamente en el inventario de controladores.
- **Fusionar:** la opción por defecto es Fusionar (`union` en el inventario de controladores). Esto significa que a un usuario se le conceden todos los valores de este derecho desde todas las directivas de derechos basados en funciones de las que sea miembro.

  Cuando se utiliza la opción por defecto Fusionar, el orden de prioridad de la lista de directivas no es importante para este derecho específico.

  Por ejemplo, a un usuario se le otorga la pertenencia a las listas de distribución de correo electrónico del controlador A de GroupWise® mediante dos directivas de derechos basados en funciones diferentes, la directiva de gestores y la directiva de miembros del equipo. En la directiva 1, al usuario se le otorga la pertenencia a la lista de distribución de correo electrónico de los gestores y, en la directiva 2, al usuario se le otorga la pertenencia a la lista de distribución de correo electrónico de los miembros del equipo. Con la opción Fusionar, se otorga al usuario la pertenencia a ambas listas de distribución de correo electrónico.
- **Prioridad:** con esta opción, si varias directivas de derechos basados en funciones otorgan a un usuario diferentes valores para el mismo derecho del mismo objeto Controlador, al usuario solo se le conceden los valores especificados en la directiva que esté más alta en la lista.

  Cuando se utiliza la opción Prioridad, el orden de prioridad de la lista de directivas es importante para este derecho específico.

  Por ejemplo, a un usuario se le otorga la pertenencia a las listas de distribución de correo electrónico del controlador A de GroupWise mediante dos directivas de derechos basados en funciones diferentes, la directiva de gestores y la directiva de miembros del equipo. En la directiva de gestores, al usuario se le concede la pertenencia a la lista de distribución de correo electrónico de los gestores y, en la directiva de miembros del equipo, al usuario se le otorga la pertenencia a la lista de distribución de correo electrónico de los miembros del equipo. La directiva de gestores aparece más arriba en la lista de directivas que la de miembros del equipo. Con la opción Prioridad, el usuario solo puede ser miembro de la lista de distribución de correo electrónico de los gestores.

  El uso de la prioridad para la resolución de conflictos puede resultar útil, por ejemplo, si un atributo en un sistema conectado solo permite un valor. Si dos directivas de derechos basados en funciones diferentes conceden un valor para ese atributo al mismo usuario, este recibe el valor otorgado por la directiva que esté más alta en la lista.

Nota: No se proporciona una opción de resolución de conflictos para los derechos que no tienen valores, como una cuenta. Los derechos que no tienen valores se conceden siempre a los miembros de la directiva de derechos basados en funciones, independientemente de la prioridad de las directivas en la lista.

Componentes dinámicos

Los criterios especificados para la pertenencia dinámica se muestran con la sintaxis de un filtro LDAP. Identidad de búsqueda indica los derechos del objeto que se utilizan al consultar la pertenencia dinámica, y DN base y Ámbito indican la parte del árbol que se incluye en la consulta.

Filtro de pertenencia

Puede definir criterios de pertenencia como, por ejemplo, la ubicación en el árbol y los atributos del objeto. Por ejemplo, la pertenencia puede depender de si el usuario se encuentra en el contenedor Activo o de si el cargo incluye la palabra Gestor. Los usuarios que cumplen los criterios son automáticamente miembros de la directiva de derechos basados en funciones, sin necesidad de añadir específicamente a cada usuario a la directiva. La pertenencia dinámica funciona de la misma manera que un objeto Grupo dinámico.

Si un objeto cambia y deja de cumplir los criterios de pertenencia dinámica, los derechos se revocarán automáticamente la próxima vez que reevalúe al usuario.

Definir parámetros de búsqueda

Especifique la ubicación de los usuarios que desea que gestione la directiva de derechos. Elija el contenedor que contiene los usuarios (DN base) y la profundidad de búsqueda desde ese contenedor (Ámbito de búsqueda). Para que la directiva de derechos gestione usuarios en los contenedores especificados, los usuarios deben encontrarse en una réplica principal o de lectura/escritura en el servidor.

Se proporcionan las siguientes opciones para Ámbito de búsqueda:

- Este contenedor y subcontenedores: los usuarios situados bajo este contenedor del árbol serán miembros de la directiva de derechos si cumplen los criterios especificados para la pertenencia dinámica. Los usuarios incluidos en los subcontenedores también serán miembros si cumplen los criterios.
- Solo este contenedor: los usuarios incluidos en este contenedor solo son miembros si cumplen los criterios especificados para la pertenencia dinámica. Los usuarios que se encuentran en subcontenedores bajo este contenedor no serán miembros, aunque cumplan los criterios.

Definir criterios de filtro

Especifique las características que determinan los usuarios que son miembros de la directiva de derechos.

En la página Resumen de una directiva de derechos, los criterios de pertenencia dinámica especificados se muestran con la sintaxis de un filtro LDAP.

Por defecto, la pertenencia dinámica se configura para incluir todos los objetos Clase de usuario (y los objetos de clases derivados de la clase de usuario) en el ámbito de búsqueda como miembros de la directiva de derechos.

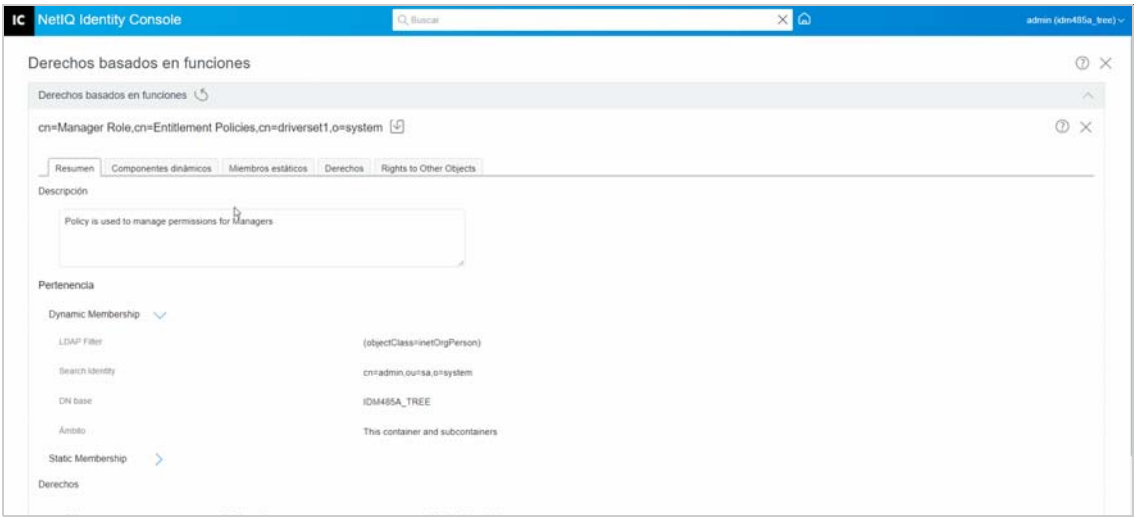
Nota: Si crea una nueva clase de objeto que se deriva del usuario, una directiva de derechos existente no la reconocerá hasta que realice una modificación en la directiva de derechos. Esto evita que los usuarios de una nueva clase reciban derechos accidentalmente. Cuando se realiza una modificación en la directiva de derechos, se actualiza la lista de clases derivadas de usuario para esa directiva.

Creación de pertenencia dinámica

En la pestaña Miembros dinámicos, realice lo siguiente:

1. Haga clic en la pestaña **Miembros dinámicos**.
2. Utilice los filtros **Identidad de búsqueda**, **Empezar a buscar en** y **Ámbito de búsqueda** según sus necesidades.
3. Haga clic en la opción **Crear grupo** específica para crear una nueva condición o una fila y, a continuación, proporcione la condición o los criterios de búsqueda necesarios.

Figura 33-2 *Componentes dinámicos*



Ámbito de búsqueda: el ámbito de búsqueda indica el conjunto de entradas en el DN base de búsqueda (o debajo de él) que pueden considerarse posibles coincidencias en una operación de búsqueda.

Criterios de búsqueda: puede limitar una búsqueda para ayudarle a localizar un registro específico o un grupo de registros de un gran número de registros.

DN base: un DN base es el punto desde el que un servidor buscará usuarios.

Grupo LDAP: se trata de una organización jerárquica de usuarios, grupos y unidades administrativas que son contenedores de usuarios y grupos.

Nota: El usuario puede crear uno o varios grupos con condiciones. Las condiciones están formadas por atributos, operadores y valores. Por defecto, se utiliza **Clase de objeto** > **es igual a** > **Usuario**.

Componentes estáticos

Los componentes estáticos son una clase de componentes que se declaran mediante palabras clave estáticas. Un componente estático presenta determinados accesos limitados.

En la pestaña Componentes estáticos, se pueden realizar las siguientes operaciones:

Componentes incluidos:

Añada componentes de forma estática que se hayan incluido mediante el filtro de pertenencia dinámica.

Componentes excluidos:

Excluya los componentes que cumplan los criterios del filtro, pero que no se deben incluir en la directiva de derechos.

Derechos

Los derechos basados en funciones permiten conceder derechos en los sistemas conectados y derechos en Identity Manager. Los derechos pueden ser cualquiera de los siguientes:

- Cuentas en sistemas conectados.
- Pertenencia a listas de distribución de correo electrónico en sistemas conectados.
- Pertenencia a grupo en sistemas conectados.
- Atributos de los objetos correspondientes en los sistemas conectados, rellenados con los valores que especifique.

Nota: La funcionalidad Derechos forma parte de Identity Manager, por lo que debe tener instalados y configurados los controladores de Identity Manager para admitir los derechos antes de poder otorgarlos en los sistemas conectados.

Crear derecho

En la pestaña Derechos, realice lo siguiente:

1. Haga clic en la pestaña **Derecho**.
2. Haga clic en + para **añadir controladores** y proporcionar derechos en los sistemas conectados.

   Aparece la pantalla **Añadir controlador**.
3. Seleccione el controlador en el menú desplegable.
4. Haga clic en **Añadir**.

   Aparece la pantalla **Añadir derechos**.
5. En el menú desplegable, **seleccione un grupo de derechos** que desee añadir.
6. Seleccione el **tipo de consulta**:
   - **En caché:** si las consultas se han ejecutado anteriormente.
   - **Consulta externa:** si las consultas son nuevas.

Aparece la pantalla **Añadir derecho de grupo**.

7 Seleccione el derecho de grupo en el menú desplegable y, a continuación, haga clic en **Seleccionar**.

"Rights to other Objects" (Derechos a otros objetos)

Utilice esta página para otorgar derechos de un Trustee de directiva de derechos a un objeto de eDirectory. Cada miembro de la directiva de derechos se convierte en un Trustee del objeto.

Además de asignar derechos a todos los atributos, puede hacer clic en Añadir propiedad para asignar derechos a propiedades específicas.

La casilla de verificación Heredar determina si los derechos fluyen hacia abajo en el árbol. Por ejemplo, si va a asignar derechos a un objeto Contenedor y desea que la directiva de derechos tenga los mismos derechos sobre los objetos y los subcontenedores que se encuentran por debajo de ese contenedor, marque la casilla de verificación Heredar.

Los derechos de los objetos de eDirectory se otorgan a los miembros de la directiva de derechos después de que se completen los cambios en esta página. Por el contrario, los derechos de los sistemas conectados se otorgarán a cada miembro de la directiva de derechos la próxima vez que se modifique un atributo utilizado para la pertenencia dinámica de ese usuario, o bien se desplace un usuario o se cambie su nombre. (Lo mismo ocurre cuando se revocan derechos). Utilice la tarea Reevaluar pertenencia para forzar una actualización.

Crear derechos para otros objetos

Para crear derechos:

1 Haga clic en la pestaña **Derechos a otros objetos**

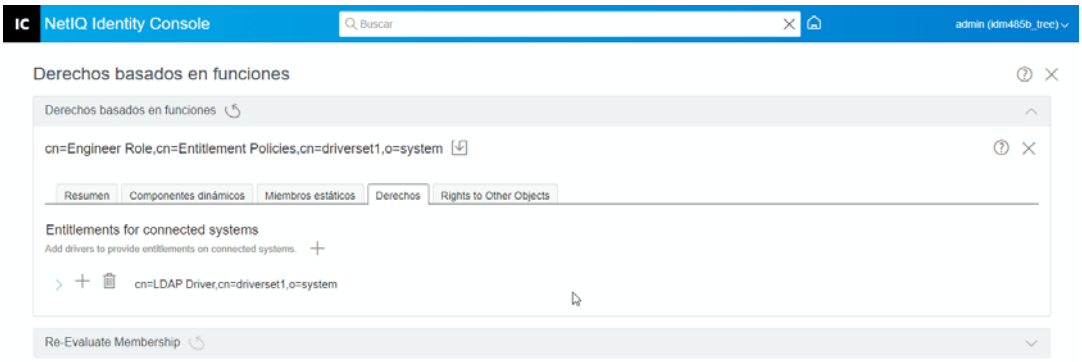
Aquí puede añadir un objeto nuevo y buscar los objetos para los que desea que esta directiva de derechos sea un Trustee.

1a Para añadir un objeto, haga clic en el botón  .

Aparece la página **NAVEGADOR DE CONTEXTO**. La página consta de `objetos`.

1b Expanda los `objetos` y seleccione grupos o usuarios individuales según sus necesidades y asígneles derechos.

Figura 33-3 *"Rights to other Objects" (Derechos a otros objetos)*

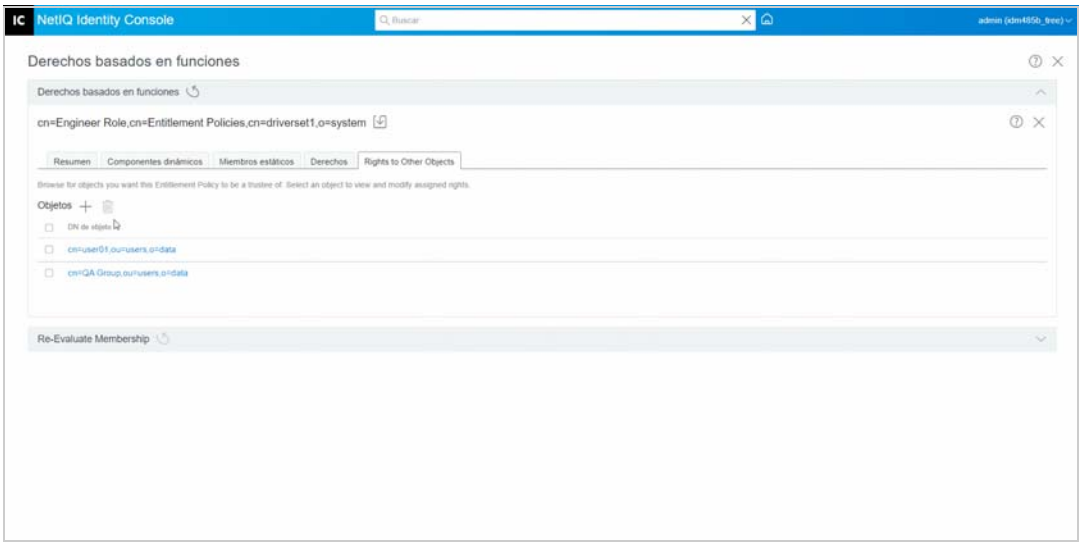


1c Para añadir más propiedades, haga clic en +.

Aparece la página **SELECCIONAR PROPIEDADES**. Esta página contiene la lista de propiedades que puede tener un objeto.

1d Haga clic en **Terminado**.

Figura 33-4 *Seleccione Propiedades*



2 (Opcional) Con las flechas **Arriba** y **Abajo** ↑ ↓, se organizan las directivas de derechos basados en funciones por orden de prioridad.

La organización por orden de prioridad permite resolver conflictos entre varias directivas. La directiva más importante tiene la máxima prioridad. Para obtener más información, consulte "Organizar las directivas de derechos basados en funciones por orden de prioridad" en la página 217.

Organizar las directivas de derechos basados en funciones por orden de prioridad

Al crear directivas de derechos basados en funciones, es posible que entren en conflicto las directivas que afectan a un determinado usuario.

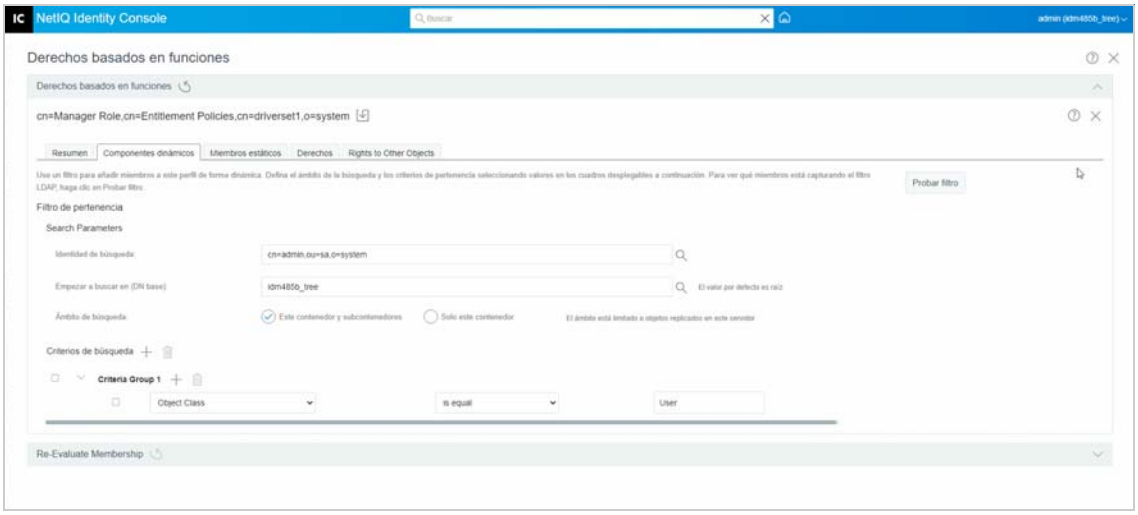
El orden de las directivas de derechos basados en funciones de la lista representa la prioridad. Puede cambiar el orden de la lista mediante los botones de flecha arriba y flecha abajo.

- Este parámetro puede ser útil si, por ejemplo, un atributo del sistema conectado solo permite un único valor. Si dos directivas de derechos basados en funciones diferentes conceden un valor para ese atributo al mismo usuario, este recibe el valor otorgado por la directiva que esté más alta en la lista. Otro ejemplo es que quizás haya configurado su entorno para que utilice derechos a fin de incluir usuarios en una estructura jerárquica de otro sistema. Le gustaría que el usuario se incluyera en una ubicación u otra, no en dos lugares al mismo tiempo.
- Tenga en cuenta que el parámetro es independiente para cada derecho que ofrece cada controlador.
- Como norma general, debería incluir las directivas de administradores o gestores en una posición más elevada en la lista que las directivas de usuarios finales o colaboradores individuales. Debe incluir los grupos con un número más reducido de miembros en una posición más elevada que los grupos con un número mayor de miembros.

Para organizar las directivas de derechos basados en funciones por orden de prioridad:

1. Seleccione la directiva de derechos que desea subir o bajar en la lista.
2. Utilice la flecha **Arriba** o **Abajo** para organizar las directivas de derechos basados en funciones por orden de prioridad.

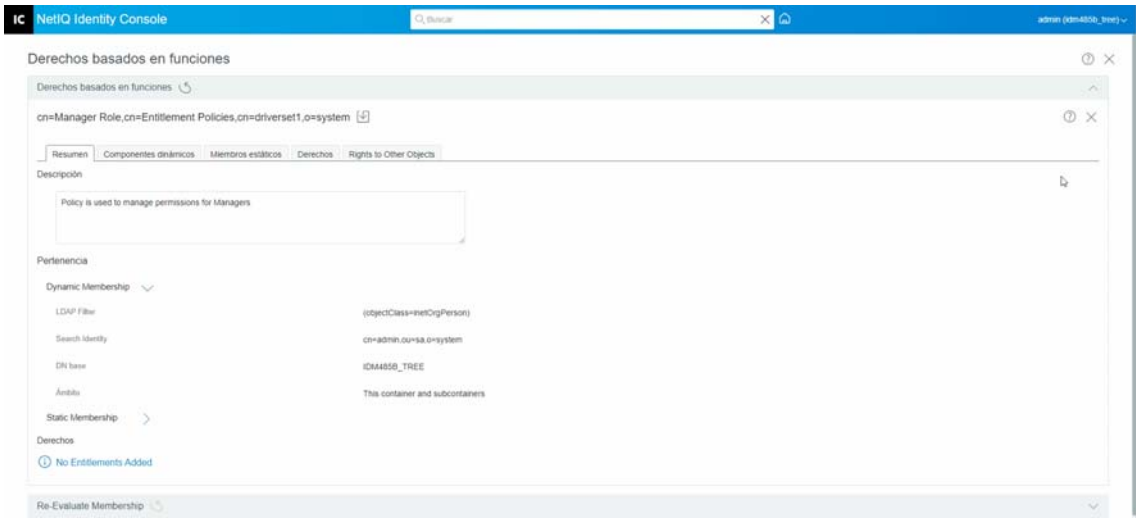
   Figura 33-5 *Organización de las directivas por orden de prioridad*



3. Haga clic en el botón Guardar .

   El resumen de los detalles de pertenencia de la directiva se muestra en la pestaña **Resumen**.
4. Reinicie el controlador.

Figura 33-6 *Cerrar y reiniciar*



Nota: Debe reiniciar el controlador para que se apliquen los cambios.

Reevaluar pertenencia

La característica **Derechos basados en funciones** le permite otorgar derechos en sistemas conectados a un grupo de usuarios.

Al crear o editar una directiva de derechos basados en funciones, la pertenencia de cada usuario se debe reevaluar para determinar si es necesario otorgar, cambiar o revocar los derechos en los sistemas conectados. Por defecto, la reevaluación tiene lugar para los usuarios de forma individual, la próxima vez que se modifique un atributo que afecte a la pertenencia para cada usuario, o cuando se desplace un usuario o se cambie su nombre. Este comportamiento por defecto minimiza el uso de los recursos del sistema, pero significa que puede haber un retraso significativo entre el momento en que se modifica la directiva de derechos basados en funciones y el momento en que se conceden, se cambian o se revocan los derechos de un usuario específico.

Puede asegurarse de que los derechos de los usuarios se actualicen todos al mismo tiempo mediante la tarea "Reevaluar directivas de derechos basados en funciones" en la página 219 para especificar los usuarios que se deben reevaluar al instante. Es recomendable realizar esta tarea cada vez que cree o modifique una directiva de derechos basados en funciones.

Antes de Identity Manager 3.6, la reevaluación de la pertenencia se realizaba para todas las directivas de derechos basados en funciones de un conjunto de controladores, no para una directiva de derechos individual. Sin embargo, Identity Manager 3.6 permite **evaluar** una directiva de derechos basados en funciones y **añadir** sus miembros a la lista de **objetos** seleccionados. Si ha definido una directiva de derechos y ha creado una lista de pertenencia, aparecerá el encabezamiento **Evalúe una directiva de derechos para añadir sus miembros a la lista** junto a la entrada de objetos seleccionada. Seleccione la directiva y, a continuación, haga clic en el icono + para añadir los miembros de la directiva a la **lista de objetos**. Puede añadir o eliminar miembros u objetos en la **lista de objetos** seleccionados.

Para aprovechar al máximo los recursos del sistema, debería realizar todos los cambios en las directivas de derechos basados en funciones de un conjunto de controladores específico antes de utilizar “Reevaluar directivas de derechos basados en funciones” en la página 219.

Nota: Solo es necesario reevaluar los derechos en los sistemas conectados. Cuando se modifican los derechos de Identity Console para una directiva de derechos basados en funciones, los cambios se aplican al instante para cada usuario. El controlador del servicio de derechos debe estar ejecutándose para poder realizar las reevaluaciones de pertenencia.

Reevaluar directivas de derechos basados en funciones

Para reevaluar la pertenencia:

1. Haga clic en **Reevaluar pertenencia** > **Seleccionar conjunto de controladores**.

   Aparece una lista de directivas creadas.

2. Seleccione la directiva que se va a evaluar y haga clic en **Evaluar** Evaluate.

   En la pestaña **Objetos**, aparecerán los usuarios que forman parte del grupo.

3. (Opcional) Para añadir un usuario específico, haga clic en +.

   Solo podrá utilizar la función **Añadir** + cuando falten usuarios en la lista y desee añadir usuarios específicos.

4. (Opcional) Para eliminar un usuario específico, haga clic en 🗑.

   Solo podrá utilizar la función **Suprimir** 🗑 cuando se necesite eliminar usuarios de la lista.

5. Haga clic en el botón Reevaluar pertenencia ▷.

Figura 33-7 *Reevaluar pertenencia*