
Directory and Resource Administrator Guía del usuario

Septiembre de 2018

Información legal

© Copyright 2007-2018 Micro Focus o uno de sus afiliados.

Las únicas garantías de los productos y servicios de Micro Focus y sus afiliados y licenciantes ("Micro Focus") se establecen en las declaraciones de garantía expresas que acompañan a dichos productos y servicios. Nada de lo establecido en este documento debe interpretarse como una garantía adicional. Micro Focus no se responsabiliza de los errores técnicos o editoriales, ni de las omisiones que se incluyan en este documento. La información contenida en este documento está sujeta a cambios sin previo aviso.

Acerca de esta guía **5**

1 Primeros pasos **7**

- 1.1 ¿Qué es Directory and Resource Administrator? 7
- 1.2 Descripción de los componentes de Directory and Resource Administrator 8
 - 1.2.1 Servidor de administración de DRA. 8
 - 1.2.2 Consola de gestión de cuentas y recursos 9
 - 1.2.3 Consola Web 9
 - 1.2.4 Componentes de elaboración de informes 9
 - 1.2.5 Motor de flujo de trabajo 10
 - 1.2.6 Arquitectura del producto. 11

2 Cómo trabajar con las interfaces de usuario **13**

- 2.1 Consola Web 13
 - 2.1.1 Inicio de la consola Web 13
 - 2.1.2 Configuración de la consola Web 14
 - 2.1.3 Personalización de la consola Web. 17
 - 2.1.4 Historial de cambios unificado. 20
 - 2.1.5 Acceso al historial de cambios de un usuario 21
 - 2.1.6 Flujo de trabajo automatizado 22
- 2.2 Consola de gestión de cuentas y recursos 22
 - 2.2.1 Conexión a un servidor de administración o un dominio gestionado. 23
 - 2.2.2 Modificación del título de la consola 24
 - 2.2.3 Personalización de columnas de lista 24
 - 2.2.4 Ejecución de consultas avanzadas guardadas 24
 - 2.2.5 Restauración de la configuración de la consola 25
 - 2.2.6 Uso de caracteres especiales 25
 - 2.2.7 Uso de caracteres comodín. 26
 - 2.2.8 Visualización de las funciones y los poderes asignados 27
 - 2.2.9 Visualización del número de versión del producto y las revisiones instaladas 27
 - 2.2.10 Visualización de la licencia actual 28
 - 2.2.11 Recuperación de la contraseña de BitLocker 28
- 2.3 Módulo de elaboración de informes de DRA 29
 - 2.3.1 Descripción del módulo de elaboración de informes de DRA 30
 - 2.3.2 Cómo DRA utiliza los archivos de registro. 31
 - 2.3.3 Descripción de las fechas y las horas 32
 - 2.3.4 Tareas del módulo de elaboración de informes de DRA 32

3 Gestión de cuentas de usuario, grupos y contactos **35**

- 3.1 Gestión de cuentas de usuario 35
 - 3.1.1 Cuentas de usuario de dominios de confianza 35
 - 3.1.2 Tareas de gestión de cuentas de usuario 35
 - 3.1.3 Transformación de cuentas de usuario 38
- 3.2 Gestión de grupos 41
 - 3.2.1 Tareas de gestión de grupos 41
 - 3.2.2 Asignaciones temporales de grupos 43
- 3.3 Gestión de grupos dinámicos de distribución. 44
- 3.4 Gestión de grupos dinámicos. 46
- 3.5 Gestión de contactos 48

4 Gestión de los buzones de Exchange y las carpetas públicas **51**

- 4.1 Gestión de tareas de buzones de usuario 51
- 4.2 Tareas de gestión de buzones de Office 365. 53

4.3	Tareas de gestión de buzones de recursos	54
4.4	Tareas de gestión de buzones compartidos	55
4.5	Tareas de gestión de buzones vinculados	56
4.6	Tareas de gestión de carpetas públicas	57
5	Gestión de recursos	59
5.1	Gestión de unidades administrativas	59
5.2	Gestión de equipos	60
5.3	Gestión de servicios	61
5.4	Gestión de impresoras y tareas de impresión	62
5.4.1	Tareas de gestión de impresoras	62
5.4.2	Gestión de tareas de impresión	63
5.4.3	Tareas de gestión de impresoras publicadas	64
5.4.4	Gestión de tareas de impresión de impresoras publicadas	64
5.5	Gestión de recursos compartidos	65
5.6	Gestión de usuarios conectados	66
5.7	Gestión de dispositivos	66
5.8	Gestión de registros de eventos	67
5.8.1	Tipos de registros de eventos	67
5.8.2	Tareas de gestión del registro de eventos	67
5.9	Gestión de archivos abiertos	68
6	Gestión de consultas avanzadas	69
7	Gestionar la Papelera	71
A	Uso de la consola Web heredada	73
A.1	Inicio de la consola Web heredada	73
A.2	Uso del inicio rápido para resolver problemas	73
A.3	Personalización de la consola Web heredada	73

Acerca de esta guía

La *Guía del usuario* proporciona información conceptual sobre el producto Directory and Resource Administrator. En este documento se define la terminología y se presentan escenarios de implementación.

A quién va dirigida

Este manual proporciona información para las personas responsables de comprender los conceptos de administración y de implementar un modelo de administración seguro y distribuido.

Documentación adicional

Esta guía forma parte del conjunto de documentación de Directory and Resource Administrator. Para obtener una lista completa de las publicaciones de esta versión, visite el [sitio Web de documentación \(https://www.netiq.com/documentation/directory-and-resource-administrator-92/\)](https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

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 para mejorar la documentación, haga clic en **comment this topic** (comentar sobre este tema) en la parte inferior de cualquier página de la versión HTML de la documentación. 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

NetIQ Communities, 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. NetIQ Communities 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 Primeros pasos

Antes de comenzar a gestionar objetos de Active Directory empleando Directory and Resource Administrator™ (DRA), debe comprender los conceptos básicos de lo que DRA puede hacer por su empresa y la función de los componentes de DRA en la arquitectura del producto.

1.1 ¿Qué es Directory and Resource Administrator?

Directory and Resource Administrator proporciona una administración segura y eficaz de identidades con privilegios de Microsoft Active Directory (AD). DRA realiza una delegación granular de "privilegios mínimos" para que los administradores y los usuarios reciban solo los permisos necesarios para completar las tareas específicas acordes a su función. DRA también impone el cumplimiento de directivas, proporciona auditorías e informes de actividades detalladas y simplifica la realización de tareas repetitivas con la automatización de procesos de TI. Cada una de estas funciones contribuye a la protección de los entornos de AD y Exchange de los clientes frente al riesgo de derivación de privilegios, errores, actividad malintencionada e incumplimiento normativo, al mismo tiempo que reduce la carga de trabajo de los administradores al ofrecer funciones de autoservicio a usuarios, directores empresariales y personal del servicio de Ayuda técnica.

Exchange Administrator amplía las potentes funciones de DRA para proporcionar una administración transparente de Microsoft Exchange. A través de una única interfaz de usuario común, Exchange Administrator ofrece administración basada en directivas para la gestión de buzones, carpetas públicas y listas de distribución en el entorno de Microsoft Exchange.

DRA proporciona las soluciones que necesita para controlar y gestionar los entornos de Active Directory, Microsoft Windows, Microsoft Exchange y Microsoft Office 365.

- ♦ **Compatibilidad con Active Directory, Office 365, Exchange y Skype Empresarial:** ofrece una gestión administrativa de Active Directory, Exchange Server en las instalaciones, Skype Empresarial en las instalaciones, Exchange Online y Skype Empresarial Online.
- ♦ **Controles granulares de acceso de privilegios administrativos y de usuario:** la tecnología patentada ActiveView delega solo los privilegios necesarios para completar tareas específicas y ofrece protección frente a la derivación de privilegios.
- ♦ **Consola Web personalizable:** el enfoque intuitivo permite al personal no técnico llevar a cabo tareas administrativas de forma fácil y segura a través de funciones y acceso limitados (y asignados).
- ♦ **Auditorías e informes exhaustivos de actividad:** proporciona un registro de auditoría completo de todas las actividades realizadas con el producto. Almacena de forma segura los datos a largo plazo y demuestra a los auditores (por ejemplo, PCI DSS, FISMA, HIPAA y NERC CIP) que se han implementado procesos para controlar el acceso a AD.
- ♦ **Automatización del proceso de TI:** automatiza los flujos de trabajo para diversas tareas, como la provisión y el desaprovisionamiento, las acciones de usuarios y buzones, la aplicación de directivas y las tareas de autoservicio controladas; aumenta la eficacia empresarial y reduce los esfuerzos administrativos manuales y repetitivos.
- ♦ **Integridad operativa:** impide que se realicen cambios malintencionados o incorrectos que afecten el rendimiento y la disponibilidad de los sistemas y servicios al proporcionar control de acceso granular para los administradores y gestionar el acceso a los sistemas y los recursos.

- ♦ **Aplicación de procesos:** mantiene la integridad de los procesos clave de gestión de cambios, lo que le ayudará a mejorar la productividad, reducir los errores, ahorrar tiempo y aumentar la eficacia de la administración.
- ♦ **Integración con Change Guardian:** mejora de la auditoría de eventos generados en Active Directory fuera de la automatización de DRA y flujos de trabajo.

1.2 Descripción de los componentes de Directory and Resource Administrator

Entre los componentes de DRA que utilizará sistemáticamente para gestionar el acceso con privilegios, se incluyen servidores principales y secundarios, consolas de administrador, componentes de elaboración de informes y el motor de flujo de trabajo que permite automatizar los procesos de flujo de trabajo.

En la siguiente tabla, se indican las interfaces de usuario típicas y los servidores de administración utilizados por cada tipo de usuario de DRA:

Tipo de usuario de DRA	Interfaces de usuario	Servidor de administración
Administrador de DRA	Consola de delegación y configuración	Servidor principal
(La persona encargada del mantenimiento de la configuración del producto)	Módulo de elaboración de informes de DRA CLI Proveedor ADSI de DRA	Servidor secundario
Administrador ocasional del servicio de Ayuda técnica	Consola de gestión de cuentas y recursos Consola Web	Servidor secundario

1.2.1 Servidor de administración de DRA

El servidor de administración de DRA almacena datos de configuración (entorno, acceso delegado y directivas), ejecuta tareas de automatización y de operador, y audita todas las actividades del sistema. Aunque admite varios clientes de nivel de consola y API, el servidor se ha diseñado para proporcionar una alta disponibilidad tanto para la redundancia como para el aislamiento geográfico a través de un modelo de ampliación horizontal de conjunto de varios maestros (MMS, Multi-Master Set). En este modelo, cada entorno de DRA requerirá un servidor de administración de DRA principal que se sincronizará con varios servidores de administración de DRA secundarios adicionales.

Es recomendable que no instale los servidores de administración en controladores de dominio de Active Directory. En cada dominio que gestiona DRA, asegúrese de que haya al menos un controlador de dominio en el mismo emplazamiento que el servidor de administración. Por defecto, el servidor de administración accede al controlador de dominio más cercano para todas las operaciones de lectura y escritura; al realizar tareas específicas del sitio, como el restablecimiento de contraseñas, puede especificar un controlador de dominio específico del sitio para procesar la operación. Como práctica recomendable, considere la posibilidad de utilizar de forma específica un servidor de administración secundario para la elaboración de informes, el procesamiento por lotes y las cargas de trabajo automatizadas.

1.2.2 Consola de gestión de cuentas y recursos

La consola de gestión de cuentas y recursos es una interfaz de usuario que se puede instalar y permite que los administradores asistentes de DRA puedan ver y administrar los objetos delegados de los dominios y los servicios conectados.

1.2.3 Consola Web

La consola Web es una interfaz de usuario basada en la Web que proporciona acceso rápido y fácil a los administradores asistentes de DRA para ver y administrar los objetos delegados de los dominios y los servicios conectados.

Los administradores pueden personalizar el aspecto y el uso de la consola Web para incluir marcas empresariales y propiedades de objetos personalizados, así como configurar la integración con los servidores de Change Guardian para habilitar la auditoría de cambios que se producen fuera de DRA.

El administrador de DRA también puede crear y modificar formularios de flujo de trabajo automatizados para ejecutar tareas automáticas rutinarias cuando se activen.

El Historial de cambios unificado es otra función de la consola Web que permite la integración con los servidores de Historial de cambios para auditar los cambios realizados en los objetos de AD fuera de DRA. Entre las opciones de informe de Historial de cambios, se incluyen las siguientes:

- ♦ Cambios realizados en...
- ♦ Cambios realizados por...
- ♦ Buzón creado por...
- ♦ Usuario, grupo y dirección de correo electrónico de contacto creados por...
- ♦ Usuario, grupo y dirección de correo electrónico de contacto suprimidos por...
- ♦ Atributo virtual creado por...
- ♦ Objetos movidos por...

1.2.4 Componentes de elaboración de informes

El módulo de elaboración de informes de DRA proporciona plantillas integradas y personalizables para la administración de DRA e información sobre los dominios y los sistemas gestionados de DRA:

- ♦ Informes de recursos para objetos de AD
- ♦ Informes de datos de objetos de AD
- ♦ Informes de resumen de AD
- ♦ Informes de configuración de DRA
- ♦ Informes de configuración de Exchange
- ♦ Informes de Office 365 Exchange Online
- ♦ Informes detallados de tendencia de actividad (por mes, dominio y pico)
- ♦ Informes resumidos de actividad de DRA

Los informes de DRA se pueden programar y publicar a través de SQL Server Reporting Services para distribuirlos de forma cómoda entre las partes interesadas.

1.2.5 Motor de flujo de trabajo

DRA se integra con el motor de flujo de trabajo para automatizar las tareas de flujo de trabajo a través de la consola Web donde los administradores asistentes pueden configurar el servidor de flujo de trabajo y ejecutar formularios de automatización del flujo de trabajo personalizados y ver a continuación su estado. Para obtener más información sobre el motor de flujo de trabajo, consulte la documentación de la Automatización del flujo de trabajo en el [sitio de documentación de DRA](#).

1.2.6 Arquitectura del producto



2 Cómo trabajar con las interfaces de usuario

Las interfaces de usuario de DRA satisfacen diversas necesidades de administración. Estas interfaces incluyen:

Consola Web

Permite realizar tareas comunes de administración de cuentas y recursos a través de una interfaz basada en Web. Puede acceder a la consola Web desde cualquier equipo que ejecute Internet Explorer, Chrome o Firefox.

Consola de gestión de cuentas y recursos

Permite administrar los objetos de cualquier dominio gestionado. A través de la consola de gestión de cuentas y recursos (ARM, Account and Resource Management), puede ver y modificar cuentas, recursos, asignaciones temporales de grupos y buzones de Microsoft Exchange. Esta interfaz responde a las necesidades de gestión empresarial, desde la administración básica hasta los problemas avanzados del servicio de Ayuda técnica.

PowerShell

El módulo PowerShell permite a los clientes que no son de DRA solicitar operaciones de DRA mediante cmdlets de PowerShell.

Consola de NetIQ Reporting Center

Permite ver e implementar informes de gestión para que pueda auditar la seguridad de su empresa y realizar un seguimiento de las actividades de administración. Entre los informes de gestión, se incluyen informes de actividad, configuración y resumen. Muchos de estos informes se pueden ver en forma de representación gráfica.

2.1 Consola Web

La consola Web es una interfaz de usuario basada en Web que proporciona acceso rápido y fácil a muchas tareas de cuentas de usuario, grupos, equipos, recursos y buzones de Microsoft Exchange. Puede personalizar las propiedades de objeto para aumentar la eficacia de las tareas rutinarias. También puede gestionar las propiedades generales de su propia cuenta de usuario, como la dirección o el número de teléfono móvil.

En la consola Web, solo se muestra una tarea si tiene el poder para realizarla.

2.1.1 Inicio de la consola Web

Puede iniciar la consola Web desde cualquier equipo que ejecute Internet Explorer. Para iniciar la consola Web, especifique la dirección URL correspondiente en el campo de dirección del navegador Web. Por ejemplo, si ha instalado el componente Web en el equipo HOUserver, escriba `https://HOUserver.entDomain.com/draclient` en el campo de dirección del navegador Web.

Nota: Para visualizar la información más actual de la cuenta y Microsoft Exchange en la consola Web, configure el navegador Web para que busque las versiones más recientes de las páginas almacenadas en caché en cada visita.

2.1.2 Configuración de la consola Web

Con los poderes adecuados, puede configurar todas las integraciones y las conexiones de servidor necesarias, el comportamiento de salida automática de la sesión y la función Advanced Authentication en la consola Web.

Salir automáticamente

Puede definir un incremento de tiempo para que la consola Web salga automáticamente de la sesión después de un periodo de inactividad o establecerla para que nunca cierre la sesión automáticamente.

Para configurar la salida automática de la sesión en la consola Web, desplácese a **Administración > Configuración > Salir automáticamente**.

Conexión del servidor DRA

Puede configurar una de las tres opciones en la consola Web para definir las opciones de conexión del servidor DRA al entrar a la sesión.

- ♦ Utilizar siempre la ubicación por defecto del servidor DRA (**Siempre**).
- ♦ No utilizar nunca la ubicación por defecto del servidor DRA (**Nunca**).
- ♦ Utilizar solo la ubicación por defecto del servidor DRA si se selecciona (**Solo si está seleccionado**).

A continuación, se describe el comportamiento de cada opción al entrar a la sesión:

Configuración de la conexión	Pantalla de entrada - Opciones	Descripción de la opción de conexión
Siempre	Ninguno	Se inhabilita la configuración de las opciones.
Nunca	Usar descubrimiento automático	Busca automáticamente un servidor DRA; no hay disponible ninguna opción de configuración.
	Conectar a un servidor DRA específico	El usuario configura el servidor y el puerto.
	Conectarse a un servidor DRA que gestiona un dominio específico	El usuario especifica un dominio gestionado y elige una opción de conexión: <ul style="list-style-type: none">♦ Usar descubrimiento automático (en el dominio especificado)♦ Servidor principal de este dominio♦ Buscar un servidor DRA (en el dominio especificado)
Solo si está seleccionado	Usar descubrimiento automático	Busca automáticamente un servidor DRA; no hay disponible ninguna opción de configuración.

Configuración de la conexión	Pantalla de entrada - Opciones	Descripción de la opción de conexión
	Conectar al servidor DRA por defecto	Se selecciona el servidor por defecto y se inhabilita la configuración del servidor DRA.
	Conectar a un servidor DRA específico	El usuario configura el servidor y el puerto.
	Conectarse a un servidor DRA que gestiona un dominio específico	El usuario especifica un dominio gestionado y elige una opción de conexión: <ul style="list-style-type: none"> ◆ Usar descubrimiento automático (en el dominio especificado) ◆ Servidor principal de este dominio ◆ Buscar un servidor DRA (en el dominio especificado)

Para configurar la conexión del servidor DRA en la consola Web, desplácese a [Administración > Configuración > Conexión del servidor DRA](#).

Conexión del servidor REST

La configuración de la conexión del servicio REST incluye la configuración de una ubicación de servidor por defecto y un tiempo límite de conexión expresado en segundos. Puede configurar una de las tres opciones en la consola Web para definir las opciones de conexión del servicio REST al entrar a la sesión.

- ◆ Utilizar siempre la ubicación por defecto del servicio REST (**Siempre**).
- ◆ No utilizar nunca la ubicación por defecto del servicio REST (**Nunca**).
- ◆ Utilizar solo la ubicación por defecto del servicio REST si se selecciona (**Solo si está seleccionado**).

A continuación, se describe el comportamiento de cada opción al entrar a la sesión:

Configuración de la conexión	Pantalla de entrada - Opciones	Descripción de la opción de conexión
Siempre	Ninguno	Se inhabilita la configuración de las opciones.
Nunca	Usar descubrimiento automático	Busca automáticamente un servidor REST; no hay disponible ninguna opción de configuración.
	Conectar a un servidor REST específico	El usuario configura el servidor y el puerto.
	Conectar a un servidor REST de un dominio específico	El usuario especifica un dominio gestionado y elige una opción de conexión: <ul style="list-style-type: none"> ◆ Usar descubrimiento automático (en el dominio especificado) ◆ Buscar un servidor REST (en el dominio especificado)
Solo si está seleccionado	Usar descubrimiento automático	Busca automáticamente un servidor REST; no hay disponible ninguna opción de configuración.

Configuración de la conexión	Pantalla de entrada - Opciones	Descripción de la opción de conexión
	Conectar al servidor REST por defecto	Se selecciona el servidor REST por defecto y se inhabilita la configuración del servidor REST.
	Conectar a un servidor REST específico	El usuario configura el servidor y el puerto.
	Conectar a un servidor REST de un dominio específico	El usuario especifica un dominio gestionado y elige una opción de conexión: <ul style="list-style-type: none"> ♦ Usar descubrimiento automático (en el dominio especificado) ♦ Buscar un servidor REST (en el dominio especificado)

Para configurar la conexión del servicio REST en la consola Web, desplácese a [Administración > Configuración > Conexión del servicio REST](#).

Advanced Authentication

Advanced Authentication permite ir más allá del uso de un nombre de usuario y una contraseña sencillos a una forma más segura de proteger la información confidencial mediante el uso de la autenticación multifactor. La autenticación multifactor es un método de control de acceso al equipo que requiere más de un método de autenticación a partir de categorías independientes de credenciales para verificar la identidad de un usuario.

Una vez que el administrador de DRA configure las cadenas y los eventos, si dispone de los poderes necesarios, puede entrar en la consola Web y habilitar Advanced Authentication. Una vez habilitada la autenticación, todos los usuarios deberán autenticarse mediante Advanced Authentication para que se les conceda acceso a la consola Web.

Para habilitar Advanced Authentication, entre a la consola Web y desplácese a [Administración > Configuración > Advanced Authentication](#). Active la casilla de verificación **Habilitado** y configure el formulario en función de las instrucciones proporcionadas para cada campo.

Para obtener más información sobre Advanced Authentication, consulte la sección [“Autenticación”](#) de la *Guía del administrador de Directory and Resource Administrator*.

Servidores de integración

DRA se integra con un servidor de Automatización del flujo de trabajo y los servidores de Change Guardian para proporcionar acceso a formularios de flujo de trabajo automatizados e informes del Historial de cambios unificado (UCH, Unified Change History) respectivamente. Con los poderes necesarios, puede configurar la conexión con el servidor de Automatización del flujo de trabajo y uno o varios servidores de Change Guardian.

Configuración del servidor de Automatización del flujo de trabajo

Para utilizar la Automatización del flujo de trabajo en DRA, el motor de flujo de trabajo debe instalarse en la instancia de Windows Server en la que se crean los flujos de trabajo automatizados. La integración de DRA con el servidor de Automatización del flujo de trabajo se configura en la consola Web.

Para configurar el servidor de Automatización del flujo de trabajo, entre a la consola Web y acceda a **Administración > Integraciones > Automatización del flujo de trabajo**.

Configuración de los servidores de Historial de cambios unificado

Para configurar servidores de UCH:

- 1 Lance la consola Web y entre a la sesión con credenciales de administrador asistente.
- 2 Vaya a **Administración > Integraciones > Unified Change History (Historial de cambios unificado)** y haga clic en el icono **Añadir**.
- 3 Especifique el nombre o la dirección IP del servidor de UCH, el número de puerto, el tipo de servidor y la información de la cuenta de acceso en la configuración del Historial de cambios unificado.
- 4 Pruebe la conexión del servidor y haga clic en **Aceptar** para guardar la configuración.
- 5 Añada servidores adicionales según sea necesario.

2.1.3 Personalización de la consola Web

En la consola Web, puede personalizar las propiedades de objeto y la marca de la interfaz de usuario. Si se implementan correctamente, las personalizaciones de propiedades ayudarán a automatizar tareas con gestión de objetos.

Personalización de las páginas de propiedades

Puede personalizar los formularios de propiedades de objeto que utiliza en la función de gestión de Active Directory por tipo de objeto. Esto incluye la creación y la personalización de nuevas páginas de objetos que se basan en tipos de objetos que ya se han integrado en DRA. También puede modificar las propiedades de los tipos de objetos integrados.

Los objetos de propiedades se definen claramente en la lista Páginas de propiedad de la consola Web para que pueda identificar fácilmente las páginas de objetos que se han integrado, las páginas integradas que se han personalizado y las páginas que no se han integrado y que creó el administrador.

Personalización de una página de propiedades de objeto

Puede personalizar formularios de propiedades de objeto mediante la adición o la eliminación de páginas, la modificación de páginas y campos existentes, y la creación de gestores para los atributos de propiedades. Al crear gestores personalizados, estos se ejecutan automáticamente cuando cambia un campo de propiedad o cuando un administrador responde a una solicitud para ejecutar una consulta en función de cómo se haya configurado el gestor personalizado.

La lista de objetos de las páginas de propiedades ofrecen dos tipos de operaciones para cada tipo de objeto: Crear objeto y Editar propiedades. Estas son las principales operaciones que puede realizar en el cliente Web; las personalizaciones pueden aumentar la eficacia y la experiencia al gestionar los objetos de Active Directory en DRA.

Para personalizar una página de propiedades de objeto en la consola Web:

- 1 Acceda a **Personalización > Páginas de propiedad**.
- 2 Seleccione un tipo de objeto y un tipo de operación (crear o editar) en la lista Páginas de propiedad.
- 3 Haga clic en el botón **Editar** .
- 4 Personalice el formulario de propiedades de objeto. Para ello, realice una o varias de las siguientes tareas y, a continuación, aplique los cambios:
 - ♦ Añada una nueva página de propiedades: **Añadir página**
 - ♦ Seleccione una página de propiedades y personalícela:
 - ♦ Vuelva a ordenar los campos de configuración de la página:  
 - ♦ Edite los campos o los subcampos: 
 - ♦ Añada uno o varios campos: **+** o **Añadir campo**
 - ♦ Elimine uno o varios campos: **x**
 - ♦ Cree gestores personalizados para las propiedades mediante guiones, cuadros de mensajes o consultas (LDAP, DRA o REST).

Para obtener más información sobre cómo utilizar gestores personalizados, consulte [Adición de gestores personalizados](#).

Adición de gestores personalizados

Los gestores personalizados se utilizan en DRA para que los atributos de propiedades interactúen entre sí a fin de realizar una tarea de flujo de trabajo. Algunos ejemplos de gestores personalizados de propiedades incluyen la consulta del valor de otros campos, la actualización de valores, la activación o la desactivación del estado de solo lectura de un campo y la visualización o la ocultación de campos en función de variables configuradas.

DRA también simplifica la creación de gestores personalizados con varias macros de JavaScript (JS) seleccionables que puede elegir durante el proceso de creación y validación del gestor personalizado.

Pasos básicos para la creación de un gestor personalizado:

Los pasos siguientes comienzan desde una página de gestor personalizado preseleccionada. Para llegar hasta ese punto, puede acceder a los gestores personalizados de propiedades de objeto mediante el botón **Editar**  de un campo de propiedades.

- 1 Haga clic en la pestaña **Gestores personalizados** y habilite la página .
- 2 Elija un gestor personalizado en el menú desplegable y seleccione el momento en que se ejecutará. Por lo general, debe utilizar la segunda o la tercera opción de **Tiempo de ejecución**.

Nota: Normalmente solo necesitará un único gestor personalizado, pero puede utilizar más de uno mediante la configuración de los controles de flujo en el guión para vincular gestores.

- 3 Deberá configurar  cada gestor personalizado que añada a la página. Las opciones de configuración varían según el tipo de gestor, pero todos los gestores se ejecutan desde JavaScript.

Puede crear sus propias entradas de Vanilla JavaScript o utilizar las macros integradas.

♦ **Gestores de consultas LDAP o REST:**

1. Si desea que la consulta se base en valores estáticos, defina **Información de conexión** y **Parámetros de consulta**.

Si desea que la consulta sea dinámica, introduzca el texto de espacio reservado en los campos obligatorios. Esto es necesario para que se ejecute el guión. El guión anulará los valores falsos.

Nota: También puede configurar Encabezados y Cookies para la consulta REST.

2. En Acción anterior a consulta, seleccione un tipo de macro: **Global**, **Consulta** o **Campo de formulario**.
3. Seleccione una macro en la lista desplegable e insértela (</> **Insertar macro**).
4. Inserte otras macros según sea necesario y, a continuación, proporcione los valores que desee para completar el guión.

Como ejemplo, en Acción anterior a consulta, utilizaremos un guión para validar que el nombre de grupo especificado por un usuario no existe en Active Directory al enviar el formulario.

Es necesario crear una consulta LDAP mediante el nombre introducido por el usuario. Utilizaremos la macro `Field()` para tener acceso al valor del campo de nombre y crear la cadena de consulta que estableceremos como el filtro de consulta mediante la macro `Filter()`.

```
Filter() = '(&(objectCategory=group)(objectClass=group)(name=' +  
Field(name) + '))';
```

5. Siguiendo con el ejemplo anterior, en la Acción posterior a consulta, comprobaremos los resultados devueltos por la consulta. Los resultados se devuelven como una matriz de objetos que coinciden con la consulta, por lo que solo tenemos que comprobar si la longitud de la matriz es superior a 0.

Si se encuentra un grupo coincidente, utilizaremos la macro `Cancel()` para cancelar el envío del formulario, transfiriendo a la macro un mensaje opcional que debe mostrarse al usuario.

```
if (QueryResults().length > 0) { Cancel('Ya existe un grupo con ese  
nombre; introduzca un nombre exclusivo.');
```

- ♦ **Guión:** introduzca el código JavaScript personalizado o utilice las macros para generar el guión.
 - ♦ **Consulta de DRA:** en Parámetros de consulta, defina una carga con el formato JSON. A continuación, utilice las macros de manera similar a la descrita anteriormente para las consultas LDAP y REST.
 - ♦ **Gestores de cuadro de mensajes:** después de definir las propiedades del cuadro de mensajes, utilice las macros de manera similar a la descrita anteriormente para las consultas LDAP y REST, pero en lugar de las acciones anterior y posterior a consulta, redacte los guiones de la macro para las acciones anterior a mostrar y posterior al cierre.
- 4 Haga clic en **Probar gestores** para validar el guión antes de guardar el formulario.

Esto generará un Resumen de resultados de prueba donde se pueden ver los resultados de la ejecución.

Nota: Si el gestor depende del estado actual del formulario (por ejemplo, el campo tiene un valor), no se ejecutará correctamente, ya que no se cargan datos al editar un formulario. En esos casos, el gestor deberá probarse fuera del editor de formularios. Para ello, guarde la personalización, desplácese al formulario correspondiente y proporcione los datos necesarios.

Creación de una nueva página de propiedades de objeto

Para crear una nueva página de propiedades de objeto:

- 1 Entre a la consola Web y desplácese a **Personalización > Páginas de propiedad**.
- 2 En Tareas, haga clic en **Crear nueva acción**.
- 3 Cree el formulario inicial de propiedades de objeto. Para ello, defina su nombre, icono, tipo de objeto y configuración de la operación.
- 4 Personalice el formulario según sea necesario. Consulte la [Personalización de una página de propiedades de objeto](#).

Personalización de la marca de la interfaz de usuario

Puede personalizar la barra de título de la consola Web de DRA con un su propio título e imagen de logotipo. Se coloca directamente a la derecha del nombre de producto de DRA. Dado que esta ubicación también se utiliza para la navegación de nivel superior, la ocultan los enlaces de navegación de DRA de nivel superior después de entrar a la sesión. Sin embargo, la pestaña del navegador sigue mostrando el título personalizado.

Para personalizar la marca de título en DRA:

- 1 Entre a la consola Web y desplácese a **Personalización > Marca**.
- 2 Si va a añadir un logotipo de la empresa, guarde la imagen de logotipo en la ubicación `components\lib\img` del servidor Web.
- 3 Añada la información necesaria, según corresponda, en los tres campos de la página de personalización de marca y guarde los cambios.

2.1.4 Historial de cambios unificado.

Para obtener información acerca de cómo configurar servidores de UCH, consulte [Configuración de los servidores de Historial de cambios unificado](#).

Búsqueda y generación de informes de Historial de cambios unificado

Puede realizar búsquedas en todos los informes del Historial de cambios unificados o limitar la búsqueda mediante las opciones disponibles. Solo se pueden ver informes de UCH desde la consola Web. Si desea realizar búsquedas sin parámetros, se muestran todos los informes de UCH. Si se añaden parámetros de búsqueda, se filtrarán los informes que devuelve la búsqueda.

Importante: Para generar informes UCH, debe disponer del poder **Generar informes de IU**.

Para buscar y generar informes de Historial de cambios unificado:

- 1 Lance la consola Web.
- 2 Vaya a **Gestión > Buscar**.

- 3 Ejecute la búsqueda con o sin criterios de nombre, ubicación o contenedor secundario.
Si no se utiliza ningún criterio, los resultados de la búsqueda devolverán todos los objetos. Para restringir los resultados, incluya criterios de búsqueda.
- 4 Haga clic en el icono **Buscar** para visualizar los resultados de la búsqueda.
- 5 Seleccione los objetos para los que desea generar informes.
- 6 Haga clic en el icono **Ver informes del historial de cambios**.
En **Criterios de informe del historial de cambios**, puede editar y generar el informe mediante criterios, como, por ejemplo, los tipos de informes, los objetos de destino, la fecha de inicio y finalización, el número máximo de filas o los servidores (servidor DRA o de Change Guardian).
- 7 Haga clic en **Generar** para obtener datos de auditoría y generar un informe de UCH.
- 8 Puede ordenar y exportar el informe en un formato compatible, como CSV o HTML.

Visualización de las propiedades del Historial de cambios unificado

Para ver las propiedades de un servidor de UCH configurado, desplácese a **Administración > Integraciones > Unified Change History** (Historial de cambios unificado), seleccione el servidor configurado y, a continuación, haga clic en el menú **Opciones** para realizar cualquiera de las siguientes acciones:

- ♦ **Propiedades:** Vea y actualice las propiedades de UCH.
- ♦ **Probar conexión:** Compruebe la conexión del servidor.
- ♦ **Suprimir:** Suprima el servidor de UCH configurado.

2.1.5 Acceso al historial de cambios de un usuario

Puede utilizar la consola Web para ver un historial de los cambios realizados en un usuario o por un usuario. Puede ver los siguientes tipos de cambios:

- ♦ Cambios realizados por el usuario.
- ♦ Cambios realizados en el usuario.
- ♦ Buzones de usuario creados por el usuario.
- ♦ Buzones de usuario suprimidos por el usuario.
- ♦ Direcciones de correo electrónico de contacto y grupo establecidas por el usuario.
- ♦ Direcciones de correo electrónico de contacto y grupo suprimidas por el usuario.
- ♦ Atributos virtuales creados o inhabilitados por el usuario.
- ♦ Objetos desplazados por el usuario.

Para ver o generar el informe de Historial de cambios:

- 1 Lance la consola Web.
- 2 Busque el objeto cuyo historial desea ver.
- 3 Haga clic en el icono **Ver informes del historial de cambios**.
- 4 Para cambiar los criterios de generación de informes, haga clic en **Modificar**.
Puede cambiar las fechas de inicio o finalización, el objeto del que se está realizando un seguimiento, el tipo de informe y otros criterios.
- 5 Para crear un archivo CSV del informe, haga clic en **Generar**.

2.1.6 Flujo de trabajo automatizado

Mediante la Automatización del flujo de trabajo, puede automatizar los procesos de TI a través del lanzamiento de formularios de flujo de trabajo que se activan al ejecutar un flujo de trabajo o al desencadenarse un evento de flujo de trabajo con nombre que se crea en el servidor de Automatización del flujo de trabajo.

Al crear o modificar formularios de flujo de trabajo, estos se guardan en el servidor Web. Al entrar a la consola Web de este servidor, tendrá acceso a los formularios en función de los poderes delegados y el modo en que se hayan configurado los formularios. Por lo general, los formularios están disponibles para todos los usuarios con credenciales de servidor Web. Para poder enviar el formulario, se necesitan los poderes adecuados.

Lanzamiento de un formulario de flujo de trabajo: los flujos de trabajo se crean en el servidor de Automatización del flujo de trabajo, que deben estar integrados en DRA a través de la consola Web. Para guardar un nuevo formulario, se debe configurar la opción **Iniciar flujo de trabajo específico** o **Activar flujo de trabajo por evento** en las propiedades del formulario. A continuación, se proporciona más información sobre estas opciones:

- ♦ **Iniciar flujo de trabajo específico:** esta opción enumera todos los flujos de trabajo que se encuentran en producción en el servidor de flujo de trabajo de DRA. Para que esta lista se rellene con los flujos de trabajo, estos deben crearse en la carpeta `DRA_Workflows` del servidor de Automatización del flujo de trabajo.
- ♦ **Activar flujo de trabajo por evento:** esta opción se utiliza para ejecutar flujos de trabajo con activadores predefinidos. Los flujos de trabajo con activadores también se crean en el servidor de Automatización del flujo de trabajo.

Nota: Solo los formularios de flujo de trabajo configurados con Iniciar flujo de trabajo específico tendrán un historial de ejecución que se puede consultar en el panel de búsqueda principal, en [Administración > Peticiones](#).

Puede encontrar más información sobre la automatización de flujos de trabajo en la *Guía del administrador de Directory and Resource Administrator*.

2.2 Consola de gestión de cuentas y recursos

La consola de gestión de cuentas y recursos proporciona acceso a la mayoría de las tareas del administrador asistente de DRA y satisface las necesidades de gestión empresarial, desde la administración básica hasta los problemas avanzados del servicio de Ayuda técnica. Mediante esta consola, puede llevar a cabo tareas de gestión de cuentas y recursos, y administrar los buzones de Microsoft Exchange.

La consola de gestión de cuentas y recursos contiene los siguientes nodos:

Todos mis objetos gestionados

Permite administrar objetos, como cuentas de usuario, grupos, contactos, recursos, grupos dinámicos, grupos dinámicos de distribución, buzones de recursos y carpetas públicas para cada dominio en el que disponga de poderes.

Asignaciones temporales de grupos

Permite gestionar la pertenencia a un grupo para usuarios que solo la necesitan durante un periodo específico.

Consultas de búsqueda avanzadas

Permite gestionar las consultas avanzadas disponibles en el servidor de administración.

Papelera

Permite gestionar las cuentas de usuario, los grupos, los contactos y los recursos suprimidos de cualquier dominio de Microsoft Windows en el que se haya habilitado la Papelera.

Para iniciar la interfaz de la consola de gestión de cuentas y recursos, haga clic en **Gestión de cuentas y recursos** en la carpeta del programa Directory and Resource Administrator.

Al iniciar la consola de gestión de cuentas y recursos, se conecta inicialmente al mejor servidor de administración disponible en el dominio local. El mejor servidor de administración disponible es el más cercano, que suele ser un servidor en el sitio de red. Al buscar el mejor servidor de administración disponible, DRA proporciona una conexión más rápida y un mayor rendimiento.

Puede llevar a cabo las siguientes tareas de interfaz de usuario habituales en la consola de gestión de cuentas y recursos:

2.2.1 Conexión a un servidor de administración o un dominio gestionado

Por defecto, DRA se conecta al mejor servidor de administración disponible para un equipo o un dominio gestionados. El mejor servidor de administración disponible es el más cercano, que suele ser un servidor en el sitio de red. Si el sitio no incluye un servidor de administración, DRA se conecta al siguiente servidor disponible en el dominio o el subárbol gestionados. También puede especificar el servidor de administración o el dominio al que desea conectarse.

Al iniciar por primera vez las interfaces de usuario, DRA se conecta inicialmente al dominio de la cuenta de entrada a la sesión. Si ha entrado a la sesión en un dominio que no gestiona un servidor de administración o si DRA no puede conectarse al servidor de administración de ese dominio, es posible que DRA muestre un mensaje de error. Asegúrese de que el servidor de administración esté disponible e inténtelo de nuevo.

Para conectarse a un servidor de administración:

- 1 En el menú Archivo, haga clic en **Connect to DRA server** (Conectarse al servidor DRA).
- 2 Haga clic en **Connect to this DRA server** (Conectarse a este servidor DRA).
- 3 Escriba el nombre del servidor de administración con el formato siguiente: *nombre_equipo*.
- 4 Haga clic en **Aceptar**.

Para conectarse a un equipo o un dominio gestionados:

- 1 En el menú Archivo, haga clic en **Connect to DRA server** (Conectarse al servidor DRA).
- 2 Seleccione la opción adecuada y, a continuación, escriba el nombre del equipo o el dominio gestionados.
- 3 Por ejemplo, para conectarse al dominio HOULAB, haga clic en **Connect to a DRA server that manages this domain** (Conectarse a un servidor DRA que gestione este dominio) y, a continuación, escriba HOULAB.
- 4 Para especificar un servidor de administración para el equipo o el dominio gestionados, haga clic en **Advanced** (Opciones avanzadas) y, a continuación, seleccione la opción adecuada.
- 5 Haga clic en **Aceptar**.

2.2.2 Modificación del título de la consola

Puede modificar la información que aparece en la barra de título de la consola de gestión de cuentas y recursos. Para mayor comodidad y claridad, puede añadir el nombre de usuario con el que se ha lanzado la consola y el servidor de administración al que se ha conectado la consola. En entornos complejos en los que necesita conectarse a varios servidores de administración con diferentes credenciales, esta función le ayuda a discernir rápidamente la consola que debe usar.

Para modificar la barra de título de la consola:

- 1 Inicie la consola de gestión de cuentas y recursos.
- 2 Haga clic en **Ver > Opciones**.
- 3 Seleccione la pestaña "Window Title" (Título de la ventana).
- 4 Especifique las opciones adecuadas y haga clic en **Aceptar**.

2.2.3 Personalización de columnas de lista

Puede seleccionar las propiedades del objeto que DRA muestra en columnas de lista. Esta función flexible le permite personalizar la interfaz de usuario, como las listas de resultados de la búsqueda, para satisfacer mejor las demandas específicas de administración de su empresa. Por ejemplo, puede configurar columnas para que muestren el nombre de entrada a la sesión del usuario o el tipo de grupo, lo que permite buscar y ordenar de forma rápida y eficaz los datos que necesita.

Para personalizar las columnas de lista:

- 1 Seleccione el nodo adecuado. Por ejemplo, para elegir las columnas que aparecen al ver los resultados de la búsqueda en objetos gestionados, seleccione **Todos mis objetos gestionados**.
- 2 En el menú Ver, haga clic en **Choose columns** (Elegir columnas).
- 3 En la lista de las propiedades disponibles para este nodo, seleccione las propiedades del objeto que desea visualizar.
- 4 Para cambiar el orden de las columnas, seleccione una columna y, a continuación, haga clic en **Mover arriba** o **Mover abajo**.
- 5 Para especificar el ancho de la columna, seleccione una columna y, a continuación, especifique el número adecuado de píxeles en el campo correspondiente.
- 6 Haga clic en **Aceptar**.

2.2.4 Ejecución de consultas avanzadas guardadas

Mediante las consultas avanzadas, puede buscar usuarios, contactos, grupos, equipos, impresoras, unidades administrativas y cualquier otro objeto compatible con DRA. Si dispone del poder para ejecutar consultas avanzadas guardadas, puede ejecutar las consultas avanzadas disponibles en la lista **Consultas guardadas** de cualquier contenedor en el nodo Gestión de cuentas y recursos. Para obtener más información sobre los poderes asignados, consulte [Visualización de las funciones y los poderes asignados](#).

Para ejecutar consultas avanzadas guardadas:

- 1 Expanda **Gestión de cuentas y recursos > Todos mis objetos gestionados**.
- 2 Seleccione el contenedor adecuado. Por ejemplo, si desea que DRA busque información de cuentas de usuario, seleccione **Usuarios**.
- 3 Para ver el panel de búsqueda avanzada, haga clic en **Búsqueda avanzada**.

- 4 En el panel de búsqueda avanzada, seleccione una consulta avanzada en la lista **Consultas guardadas**.
- 5 Haga clic en **Cargar consultay**, a continuación, haga clic en **Buscar ahora**.

2.2.5 Restauración de la configuración de la consola

DRA permite cambiar el tamaño de las ventanas y conservar posteriormente ese tamaño. DRA también conserva muchas otras configuraciones, incluido el último servidor de administración al que se conecta, las columnas que añade o elimina de los resultados de la lista y los anchos de columna. Si desea restaurar esta configuración a los valores originales con los que se instaló DRA, puede utilizar la opción Restore Default Settings (Restaurar configuración por defecto).

Para restaurar la configuración por defecto de la consola:

- 1 Haga clic en **Ver > Opciones**.
- 2 Seleccione la pestaña **Saved Settings** (Configuración guardada).
- 3 Revise la información proporcionada en la ventana y, a continuación, haga clic en **Restore Default Settings** (Restaurar configuración por defecto).

2.2.6 Uso de caracteres especiales

No puede utilizar los siguientes caracteres especiales al asignar un nombre a cuentas de usuario, grupos, contactos, unidades administrativas, equipos, ActiveViews, grupos de AA, funciones, directivas o activadores de automatización. Estas restricciones de nomenclatura son aplicables al nombre del objeto, así como al nombre de la regla que define el objeto.

Asignación de nombres a cuentas de usuario, grupos y equipos

Al especificar un nombre anterior a Windows 2000, no puede utilizar los siguientes caracteres especiales:

Barra inversa	\
Dos puntos	:
Coma	,
Comillas dobles	"
Signo igual	=
Barra inclinada	/
Mayor que	>
Corchete izquierdo	[
Menor que	<
Signo más	+
Corchete derecho]
Punto y coma	;
Barra vertical	

Importante: En la administración de carpetas públicas, no se admite el carácter de barra inclinada invertida ("\").

Al asignar nombres a las cuentas de usuario, grupos y equipos en los dominios de Microsoft Windows, puede utilizar cualquier carácter especial.

Asignación de nombres a contactos y unidades administrativas

Al asignar nombres a contactos y unidades organizativas, puede utilizar cualquier carácter especial.

Asignación de nombres a ActiveViews, grupos de administradores asistentes y funciones

Al asignar nombres a ActiveViews, grupos de administradores asistentes y funciones, no puede utilizar una barra diagonal inversa (\).

Asignación de nombres a directivas y activadores de automatización

Al asignar nombres a directivas y activadores de automatización, no puede utilizar la barra diagonal inversa (\).

Caracteres no válidos en los buzones de Office 365

Los caracteres no válidos provocarán que no se realice correctamente la sincronización entre Office 365 y el directorio en sus instalaciones. Consulte el subtema sobre [preparación de atributos y objetos de directorio](#) en el sitio Web de asistencia de Microsoft Office para obtener más información acerca de estos caracteres no válidos.

Para asegurarse de que estos caracteres no se utilicen en las propiedades del buzón en línea, vaya a la consola de gestión de directivas y automatización, y haga clic en **Configure Exchange Policies** (Configurar directivas de Exchange). Haga clic en **Office 365 Rules** (Reglas de Office 365), **Enforce online mailbox policies for invalid characters and character length** (Aplicar directivas de buzones en línea para caracteres no válidos y la longitud de caracteres) y, a continuación, en **Aceptar**.

2.2.7 Uso de caracteres comodín

DRA admite caracteres comodín en muchos campos de las consolas de DRA y en los comandos de la CLI. Los caracteres comodín permiten definir reglas que hacen coincidir varios objetos con una condición o una norma específicas, como una convención de nomenclatura. Puede utilizar caracteres comodín en lugar de expresiones regulares para restringir o ampliar el ámbito de la regla. La búsqueda con caracteres comodín no distingue entre mayúsculas y minúsculas. También puede utilizar los caracteres comodín de signo de interrogación (?), asterisco (*) o signo de número (#) como caracteres normales. Para ello, incluya una barra diagonal inversa (\) delante del carácter comodín específico. Por ejemplo, para buscar `abc*`, escriba el texto de búsqueda `abc*`.

DRA admite los siguientes caracteres comodín. No se pueden utilizar caracteres comodín en los nombres.

Elemento de coincidencia	Carácter	Definición
Cualquier carácter	Signo de interrogación de cierre ?	Puede sustituir a cualquier carácter.
Cualquier dígito	Signo de número #	Puede sustituir a un dígito.
Cualquier carácter, 0 o más coincidencias.	Asterisco *	Puede sustituir a varios caracteres o a ninguno.

En la siguiente tabla, se proporcionan ejemplos de especificaciones de caracteres comodín que ofrecen coincidencias o no.

Ejemplo	Coincide	No coincide
Den???	Denton y Dennis	Denison
El ?????o	El Campo y El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA no admite especificaciones de caracteres comodín que contengan operaciones lógicas.

2.2.8 Visualización de las funciones y los poderes asignados

Los poderes y las funciones definen el modo en que se gestionan los objetos. Una función es un conjunto de poderes que ofrece los permisos necesarios para realizar una tarea de administración específica, como crear una cuenta de usuario o desplazar directorios compartidos.

El administrador de DRA asigna funciones, añade usuarios a grupos de administradores asistentes específicos y asocia usuarios con ActiveViews (conjuntos de objetos de dominio que se pueden gestionar). Puede ver estas asignaciones mediante la consola de gestión de cuentas y recursos. No necesita poderes auxiliares para ver las funciones y los poderes que se le han asignado.

Para ver las funciones y los poderes asignados:

- 1 En el menú Archivo, haga clic en **Propiedades de DRA**.
- 2 Haga clic en **Poderes**.
- 3 Seleccione la vista adecuada. Por ejemplo, haga clic en **Flat View** (Vista sin formato) para ver una tabla de la pertenencia a grupos de administradores asistentes, las funciones y los poderes asignados, y las ActiveViews asociadas.
- 4 Expanda el elemento correspondiente. Por ejemplo, en la columna **Tiene poder**, expanda **Funciones y poderes** para ver las funciones o los poderes que se le han asignado.
- 5 Haga clic en **Aceptar**.

2.2.9 Visualización del número de versión del producto y las revisiones instaladas

Puede ver el número de versión del producto y las revisiones instaladas en la ventana Propiedades de DRA. Esta ventana proporciona números de versión y listas de revisiones instaladas en relación con el servidor de administración y el equipo cliente de DRA.

Para ver el número de versión del producto y las revisiones instaladas:

- 1 En el menú Archivo, haga clic en **Propiedades de DRA**.
- 2 Haga clic en **General**.
- 3 Consulte la información que necesite.
- 4 Haga clic en **Aceptar**.

2.2.10 Visualización de la licencia actual

DRA requiere un archivo de clave de licencia. Puede ver la licencia del producto desde cualquier equipo del servidor de administración. No se necesitan poderes auxiliares para ver la licencia del producto.

Para ver su licencia:

- 1 En el menú Archivo, haga clic en **Propiedades de DRA**.
- 2 Haga clic en **Licencia**.
- 3 Revise las propiedades de la licencia y, a continuación, haga clic en **Aceptar**.

2.2.11 Recuperación de la contraseña de BitLocker

Microsoft BitLocker almacena las contraseñas de recuperación en Active Directory. Con los poderes necesarios, puede usar la función de recuperación de BitLocker de DRA para buscar y recuperar las contraseñas de BitLocker perdidas para los usuarios finales.

Importante: Antes de utilizar la función Contraseña de recuperación de BitLocker, asegúrese de que el equipo se haya asignado a un dominio y BitLocker esté activado.

Visualización y copia de una contraseña de recuperación de BitLocker

Si se pierde la contraseña de BitLocker de un equipo, se puede restablecer mediante la clave de contraseña de recuperación de las propiedades del equipo en Active Directory. Copie la clave de contraseña y proporciónese la al usuario final.

Para ver y copiar la contraseña de recuperación:

- 1 Lance la consola de gestión de cuentas y recursos, y desplácese a **Todos mis objetos gestionados > Dominio > Equipos**.
- 2 En la lista de equipos, haga clic con el botón derecho en el equipo correspondiente y seleccione **Propiedades > Contraseña de recuperación de BitLocker**.
- 3 Haga clic con el botón derecho y copie la contraseña de recuperación de BitLocker; a continuación, pegue el texto de la contraseña en un archivo de texto.

Búsqueda de una contraseña de recuperación

Si se ha cambiado el nombre de un equipo, se debe buscar la contraseña de recuperación en el dominio mediante los primeros ocho caracteres del ID de contraseña.

Para buscar una contraseña de recuperación mediante un ID de contraseña:

- 1 Lance la consola de **Gestión de cuentas y recursos** y desplácese a **Todos mis objetos administrados**.
- 2 Haga clic con el botón derecho en **Dominio gestionado** y, a continuación, haga clic en **Buscar contraseña de recuperación de BitLocker**.

Para buscar los primeros ocho caracteres de la contraseña de recuperación, consulte [Visualización y copia de una contraseña de recuperación de BitLocker](#).

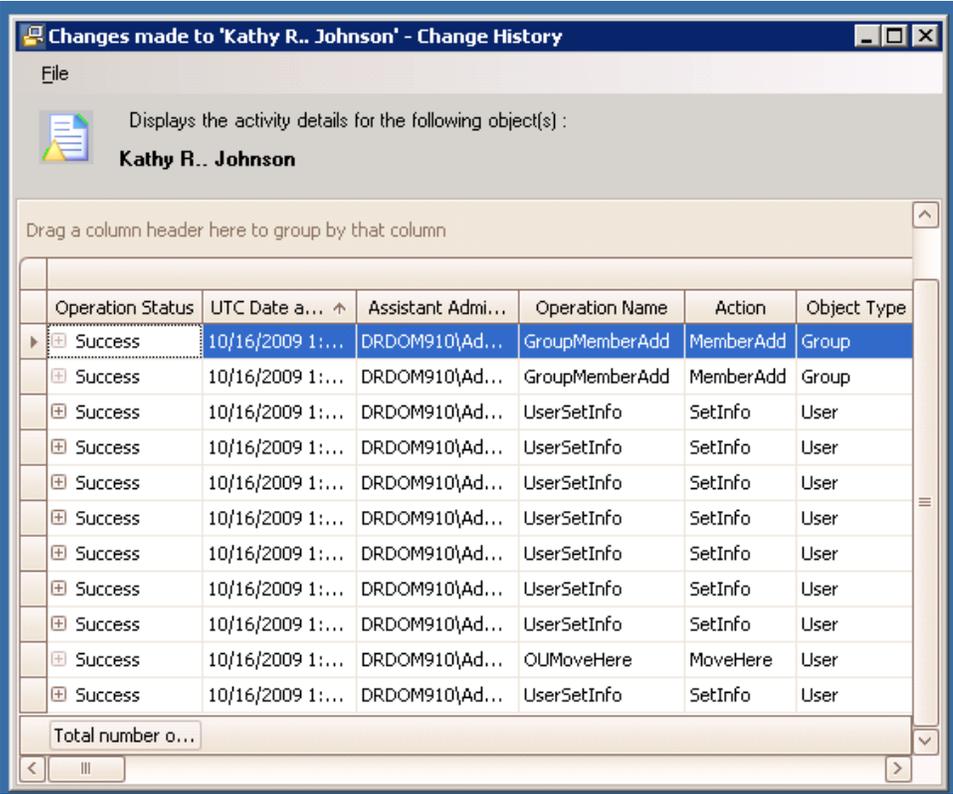
- 3 En la página [Buscar contraseña de recuperación de BitLocker](#), pegue los caracteres copiados en el campo de búsqueda y, a continuación, haga clic en **Buscar**.

2.3 Módulo de elaboración de informes de DRA

El módulo de elaboración de informes de DRA proporciona informes integrados listos para usar que permiten realizar rápidamente un seguimiento de las cuentas duplicadas, las últimas entradas a la cuenta, la información del buzón de Microsoft Exchange y mucho más. El módulo de elaboración de informes proporciona también información en tiempo real de los cambios realizados en su entorno, incluidos los valores anteriores y posteriores a la modificación de las propiedades. Puede exportar, imprimir o ver informes, o publicarlos en SQL Server Reporting Services.

DRA proporciona dos métodos para generar informes que permiten recopilar y revisar las definiciones de cuentas, grupos y recursos de usuarios del dominio. **Informes de detalles de actividad:** se pueden visualizar mediante la consola de delegación y configuración, y proporcionan información de cambios en tiempo real en relación con los objetos del dominio. Por ejemplo, puede ver una lista de los cambios realizados en o por un objeto durante un periodo especificado mediante los informes de detalles de actividad.

En la siguiente ilustración, se muestra un informe de detalles de actividad:



Operation Status	UTC Date a...	Assistant Admi...	Operation Name	Action	Object Type
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	GroupMemberAdd	MemberAdd	Group
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User
Success	10/16/2009 1:...	DRDOM910\Ad...	OLMoveHere	MoveHere	User
Success	10/16/2009 1:...	DRDOM910\Ad...	UserSetInfo	SetInfo	User

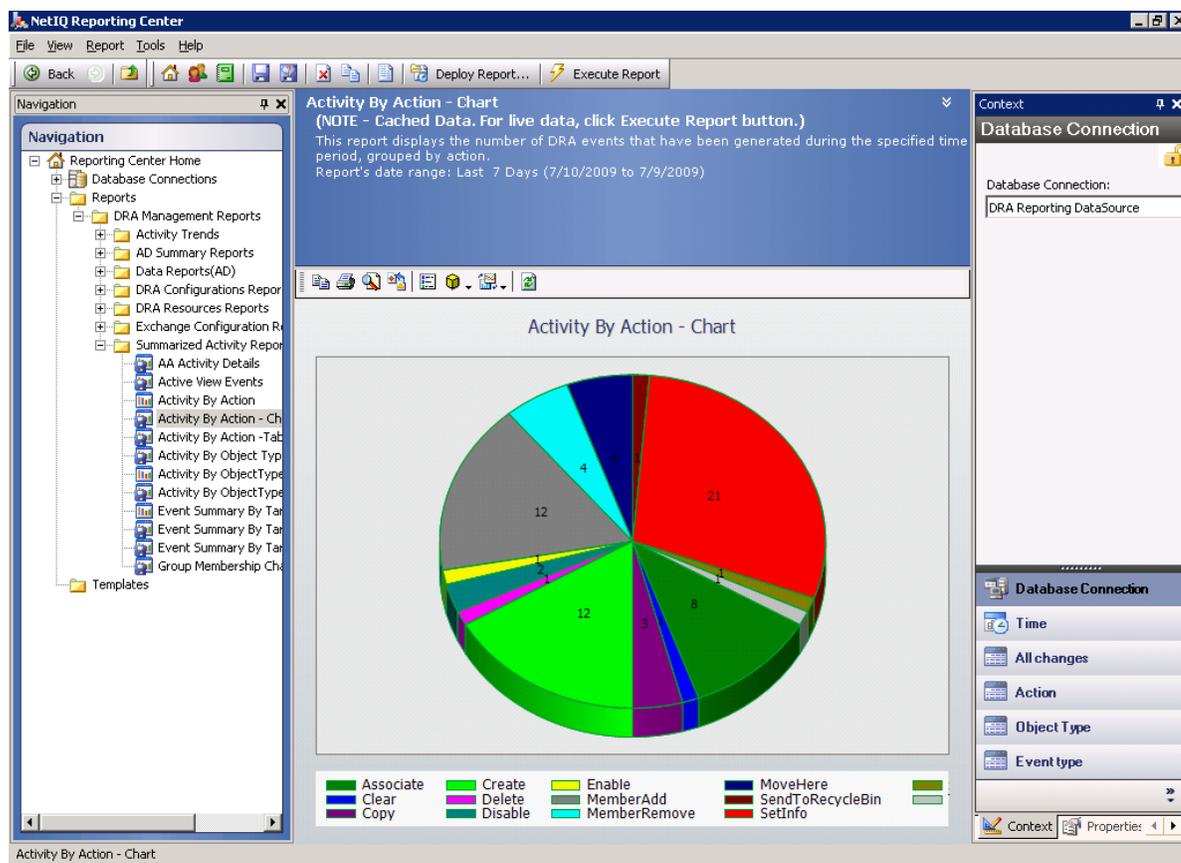
Informes de gestión de DRA: se pueden visualizar a través de NetIQ Reporting Center (Reporting Center) y proporcionan información de actividad, configuración y resumen sobre los eventos de los dominios gestionados. Algunos informes de gestión están disponibles como representaciones gráficas de los datos. Estos informes integrados también pueden personalizarse para que le proporcionen exactamente la información que necesita.

Por ejemplo, puede ver un gráfico que muestre la cantidad de eventos en cada dominio gestionado durante un periodo específico mediante informes de gestión. El módulo de elaboración de informes permite ver información sobre el modelo de seguridad de DRA, como definiciones de grupo de administradores asistentes y ActiveView.

Debe instalar y configurar primero los informes de gestión opcionales para poder verlos. Para obtener más información sobre la instalación de componentes de elaboración de informes, consulte la *Guía de instalación*. Para obtener más información sobre el módulo de elaboración de informes de DRA, consulte “[Módulo de elaboración de informes de DRA](#)” en la [página 29](#).

Lance la consola de Reporting Center en el grupo de programas NetIQ > Reporting Center.

En la siguiente ilustración, se muestra la interfaz de Reporting Center con informes de gestión de DRA seleccionados.



2.3.1 Descripción del módulo de elaboración de informes de DRA

El módulo de elaboración de informes de DRA proporciona dos métodos para generar informes que permiten ver los cambios más recientes realizados en el entorno, y recopilar y ver las definiciones de cuentas de usuario, grupos y recursos del dominio.

Informes de detalles de actividad

Se accede a ellos mediante la consola de gestión de cuentas y recursos, y proporcionan información de cambios en tiempo real en relación con los objetos del dominio.

Informes de gestión de DRA

Se accede a ellos a través de NetIQ Reporting Center (Reporting Center) y proporcionan información de actividad, configuración y resumen sobre los eventos de los dominios gestionados. Algunos informes están disponibles como representaciones gráficas de los datos.

Por ejemplo, puede ver una lista de los cambios realizados en o por un objeto durante un periodo especificado mediante los informes de detalles de actividad. También puede ver un gráfico que muestre la cantidad de eventos en cada dominio gestionado durante un periodo específico mediante informes de gestión. El módulo de elaboración de informes también permite ver información sobre el modelo de seguridad de DRA, como definiciones de grupo de AA y ActiveView.

DRA inhabilita las funciones y los informes que no admite su licencia. También debe disponer de los poderes adecuados para ejecutar y ver informes. Por lo tanto, es posible que no tenga acceso a algunos informes.

Los informes de detalles de actividad están disponibles en cuanto se instala DRA a través de la consola de gestión de cuentas y recursos y la consola de delegación y configuración para proporcionar la información más reciente sobre los cambios realizados en la red.

Los informes de gestión de DRA se pueden instalar y configurar como una función opcional y se pueden visualizar en Reporting Center. Al habilitar y configurar la recopilación de datos, DRA recopila información acerca de los eventos sometidos a auditoría y la exporta a una base de datos de SQL Server con la programación que se defina. Al conectarse a esta base de datos en Reporting Center, tendrá acceso a más de 60 informes integrados:

- ♦ Informes de actividad que muestran quién hizo qué y cuándo.
- ♦ Informes de configuración que muestran el estado de AD o DRA en un momento específico.
- ♦ Informes de resumen que muestran el volumen de actividad.

Para obtener más información acerca de la configuración de la recopilación de datos para los informes de gestión, consulte la *Guía del administrador*.

2.3.2 Cómo DRA utiliza los archivos de registro

Para revisar y notificar las acciones del administrador asistente, DRA registra todas las operaciones de usuarios en el archivo de registro, en el equipo del servidor de administración. Entre las operaciones de los usuarios, se incluyen todos los intentos de cambiar definiciones, como actualizar cuentas de usuario, suprimir grupos o definir de nuevo ActiveViews. DRA también registra operaciones internas específicas, como la inicialización del servidor de administración y la información del servidor relacionada. Además de registrar estos eventos de auditoría, DRA registra los valores anteriores y posteriores al evento para que pueda ver exactamente qué ha cambiado.

DRA utiliza una carpeta, **NetIQLogArchiveData**, denominada **archivo de registro** para almacenar de forma segura los datos de registro archivados. DRA archiva los registros a lo largo del tiempo y borra posteriormente los datos más antiguos para dejar espacio para los datos más recientes mediante un proceso denominado limpieza.

DRA utiliza los eventos de auditoría almacenados en los archivos incluidos en el archivo de registro para mostrar informes de detalles de actividad como, por ejemplo, los cambios realizados en un objeto durante un periodo específico. También puede configurar DRA para exportar información de estos archivos incluidos en el archivo de registro a una base de datos de SQL Server que NetIQ Reporting Center utilizará para mostrar informes de gestión.

DRA siempre escribe eventos de auditoría en el archivo de registro. También puede habilitar o inhabilitar la función de escritura de eventos de DRA en los registros de eventos de Windows.

Para obtener más información sobre la auditoría de DRA, consulte la *Guía del administrador*.

2.3.3 Descripción de las fechas y las horas

DRA utiliza el **estilo de fecha corta** y el **estilo de hora** especificados en la aplicación de configuración regional del Panel de control para que se muestren en los informes. En los informes de DRA, se muestran la fecha y la hora UTC como fecha y hora locales para los eventos. Los informes de DRA admiten los siguientes formatos de fecha:

- ♦ m/d/aa
- ♦ m-d-aa
- ♦ m/d/aaaa
- ♦ m-d-aaaa
- ♦ mm/dd/aa
- ♦ mm-dd-aa
- ♦ mm/dd/aaaa
- ♦ mm-dd-aaaa
- ♦ dd/mm/aa
- ♦ dd-mm-aa
- ♦ dd/mm/aaaa
- ♦ dd-mm-aaaa

2.3.4 Tareas del módulo de elaboración de informes de DRA

Para generar informes de gestión de DRA, instale Reporting Center y habilite la recopilación de datos en DRA. Para obtener más información sobre cómo habilitar la recopilación de datos, consulte la *Guía del administrador*. Para generar informes de detalles de actividad, haga clic con el botón derecho en cualquier objeto y, a continuación, haga clic en **Reporting** (Informes) si quiere ver las opciones disponibles para los informes en ese objeto. Las siguientes secciones le guiarán a través de las distintas tareas de elaboración de informes.

Visualización de informes de detalles de actividad

Los informes de detalles de actividad muestran información sobre los cambios realizados en el entorno. Puede ver o imprimir un informe, así como guardar un informe en formato Excel, CSV o TXT. Para ver o imprimir informes, debe estar asociado a la función de administración de informes.

Al visualizar informes, escriba los criterios para especificar el periodo sobre el que desea que se muestre información. También puede optar por ver un informe limitado a los cambios realizados en servidores DRA específicos, y puede restringir el número de filas que se incluirán en el informe. Si el tamaño del informe supera uno de los siguientes límites, DRA muestra un mensaje que indica que no se ha completado el informe:

- ♦ El tamaño supera los 500 MB.
- ♦ El tiempo necesario para consultar todos los servidores DRA supera los 5 minutos.
- ♦ El número de filas que se mostrarán supera las 1000.

Tiene la opción de ver el informe que contiene solo la información recuperada antes de alcanzar uno de estos límites o puede cambiar los criterios del informe para ver uno que cumpla con estos límites.

Para ver un informe:

- 1 En el panel izquierdo, expanda **Todos mis objetos gestionados**.

- 2 Para especificar el objeto sobre el que desea ver un informe, realice los pasos siguientes:
 - 2a **Si conoce la ubicación del objeto**, seleccione el dominio y la unidad administrativa que contiene ese objeto.
 - 2b En el panel de búsqueda, especifique los atributos de objeto y, a continuación, haga clic en **Find Now** (Buscar ahora).
- 3 En el panel de lista, haga clic en el objeto y haga clic en **Reporting** (Informes).
- 4 Seleccione el tipo de informe como **Cambios realizados en nombreObjeto** o **Cambios realizados por nombreObjeto**. Los informes disponibles varían en función del tipo de objeto seleccionado.
- 5 Seleccione las fechas de inicio y finalización para especificar los cambios que desee ver.
- 6 **Si desea cambiar el número de filas que se mostrarán**, escriba un número para sustituir el valor por defecto 250.

Nota: El número de filas mostradas se aplica a cada servidor de administración del entorno. Si incluye tres servidores de administración en el informe y utiliza el valor por defecto de 250 filas para mostrar, el informe puede presentar hasta 750 filas.

- 7 **Si desea incluir solo servidores de administración específicos en el informe**, seleccione **Restringir consulta a estos servidores DRA** y escriba el nombre o los nombres de servidor que desea que incluya el informe. Separe varios nombres de servidor con comas.
- 8 Haga clic en **Aceptar**.

Nota: Es posible que DRA tarde hasta 5 segundos en mostrar los cambios recientes en los informes. Por lo tanto, espere al menos 5 segundos después de realizar un cambio y antes de intentar ver un informe que contenga el cambio.

Exportación de informes de detalles de actividad

Puede exportar los informes de detalles de actividad con los formatos siguientes: XLS, CSV y TXT. El formato por defecto es el de Microsoft Excel.

Para exportar informes de detalles de actividad:

- 1 En la ventana de informes, en el menú Archivo, haga clic en **Preview and Export** (Obtener vista previa y exportar).
- 2 En el menú Archivo de la ventana de vista previa, haga clic en **Export Document** (Exportar documento) > **Excel File** (Archivo de Excel).
- 3 Seleccione las opciones de exportación y haga clic en **Aceptar**.
- 4 En la ventana Guardar como, especifique un nombre para el archivo y haga clic en **Guardar**.

Impresión de los informes de detalles de actividad

Para imprimir informes, debe estar asociado a la función de administración de informes. Puede ver o imprimir informes de detalles de actividad, así como guardar un informe en varios formatos.

Para imprimir informes de detalles de actividad:

- 1 En la ventana de informes, en el menú Archivo, haga clic en **Preview and Export** (Obtener vista previa y exportar).
- 2 En el menú Archivo de la ventana de vista previa, haga clic en **Imprimir**.

Visualización de informes de gestión

Debe instalar el módulo de elaboración de informes de DRA y configurar los recopiladores de datos de DRA para poder ver los informes de gestión en Reporting Center. Para obtener más información sobre la instalación del módulo de elaboración de informes de DRA y la configuración de los recopiladores de DRA, consulte la *Guía del administrador*.

Al entrar a Reporting Center, el servicio Web utiliza IIS para validar las credenciales de la cuenta de acuerdo con la forma en que configuró el servicio Web durante la instalación.

Para ver informes de gestión:

- 1 Entre al equipo que ejecuta Reporting Center Console.
- 2 Inicie **Reporting Center Console** en el grupo de programas NetIQ > Reporting Center.
- 3 Proporcione la información necesaria en el recuadro de diálogo de entrada y haga clic en **Logon** (Entrar a la sesión).
- 4 En el panel de navegación, expanda **Reports (Informes)** > **DRA Management Reports (Informes de gestión de DRA)**.
- 5 Expanda las categorías de informes hasta que encuentre un informe que desee ver.
- 6 Haga clic en el nombre del informe en el panel de navegación; el informe se cargará en el panel de resultados del centro, mostrando los datos almacenados en caché.
- 7 **Si desea ver el informe con los datos más recientes**, haga clic en **Execute Report** (Ejecutar informe) en el panel de resultados.

Puede cambiar la configuración de contexto por defecto para que se muestren diferentes resultados de informes. Para obtener más información acerca de la configuración de contexto en Reporting Center, consulte la *Guía del administrador*.

Personalización de los informes de gestión

En DRA, se incluyen más de 60 informes de gestión. Reporting Center le proporciona la flexibilidad de personalizar e implantar estos informes de muchas formas. Para obtener más información acerca de la personalización y distribución de los informes de gestión en Reporting Center, consulte la *Guía del administrador*.

Para personalizar un informe de gestión:

- 1 Vea un informe que sea similar al que desea crear. Para obtener más información, consulte [Visualización de informes de gestión](#).
- 2 Personalice el informe. Para ello, cambie la configuración de contexto y las propiedades del informe para que se muestre la información que desea.
- 3 Haga clic en **Execute Report** (Ejecutar informe).
- 4 En el menú Report (Informe), haga clic en **Save Report As** (Guardar informe como) y especifique un título para el informe y la ubicación en la que se guardará.
- 5 Haga clic en **Guardar**.

Para obtener más información acerca de cómo trabajar con informes de gestión en Reporting Center, consulte la *Guía del administrador*.

3

Gestión de cuentas de usuario, grupos y contactos

Este capítulo contiene información conceptual y de procedimientos para gestionar cuentas de usuario, grupos, grupos dinámicos, grupos dinámicos de distribución y contactos tanto en la consola de gestión de cuentas y recursos como en la consola Web. La información de cuentas de usuario proporciona información más completa sobre cómo gestionar de forma general los objetos en ambas aplicaciones cliente.

3.1 Gestión de cuentas de usuario

Microsoft Windows utiliza el tipo de cuenta de usuario para determinar los poderes de acceso para la cuenta de usuario asociada. Una cuenta de usuario puede ser global o local. DRA admite también los objetos InetOrgPerson, pero los reconoce como usuarios normales.

Cuenta de usuario global

Una cuenta de usuario que puede utilizarse en cualquier dominio que confíe en el dominio en el que se ha creado la cuenta de usuario. Puede otorgar poderes específicos a una cuenta de usuario. También puede establecer una cuenta de usuario como miembro de un grupo y, a continuación, asignar los poderes a ese grupo. La agrupación de cuentas de usuario ayuda a simplificar el proceso de gestión de poderes de red para muchas cuentas de usuario.

Cuenta de usuario local

Una cuenta de usuario local es igual a la cuenta que utiliza para entrar al sistema operativo Windows. Le permite acceder a los recursos del sistema en su propio espacio de usuario.

3.1.1 Cuentas de usuario de dominios de confianza

Microsoft Windows almacena la cuenta de usuario y las definiciones de grupo en el directorio del dominio gestionado. Por lo tanto, un servidor de administración no puede modificar la información del directorio de un dominio de confianza a menos que DRA también gestione ese dominio.

Por ejemplo, en la consola administración de cuentas y recursos, puede ver cuentas de usuario y grupos que no se pueden modificar. Estas cuentas de usuario y grupos se definen en dominios en los que confía uno de los dominios gestionados. Sin embargo, puede añadir cuentas y grupos de un dominio de confianza a otros grupos en el dominio gestionado.

3.1.2 Tareas de gestión de cuentas de usuario

En esta sección, se le guía por el proceso de gestión de cuentas de usuario en la consola de gestión de cuentas y recursos, y en la consola Web. Con los poderes adecuados, puede realizar varias tareas de administración de cuentas de usuario, como crear y suprimir cuentas. Si selecciona varias cuentas de usuario, puede realizar las tareas seleccionadas en una única operación, como mover o añadir usuarios a un grupo, o suprimirlos de este. Para obtener más información sobre los poderes asignados, consulte [Visualización de las funciones y los poderes asignados](#).

Nota: Solo se puede copiar una cuenta de usuario en otra ActiveView desde la consola de gestión de cuentas y recursos.

Tareas de cuenta de usuario en la consola de gestión de cuentas y recursos

Puede ejecutar todas las tareas pertinentes debajo del menú **Tareas** o desde el menú contextual. Por lo general, debe seleccionar el nodo **Todos mis objetos gestionados** y ejecutar la operación **Buscar ahora** para localizar y seleccionar el objeto de usuario que desee. Si crea un nuevo usuario, debe seleccionar el dominio o la unidad administrativa donde desea crearlo. El menú Tareas indica las tareas que puede llevar a cabo al seleccionar una o varias cuentas de usuario.

Tareas de cuenta de usuario en la consola Web

Puede ejecutar la mayoría de las siguientes tareas desde **Gestión** > pestaña **Buscar** en la consola Web. Por lo general, debe ejecutar una operación de búsqueda para localizar y seleccionar el objeto de usuario que desee. Una vez que seleccione uno o varios objetos en la lista, se activarán los botones de la barra de herramientas. Coloque el puntero del ratón sobre los botones para visualizar sus funciones.



Nota: Solo se puede copiar una cuenta de usuario en otra ActiveView desde la consola de gestión de cuentas y recursos.

Crear una cuenta de usuario

Puede crear cuentas de usuario en el dominio o el subárbol gestionados. También puede modificar las propiedades, crear un buzón, habilitar el correo electrónico y especificar la pertenencia a grupos para la nueva cuenta.

Nota

- ♦ Es posible que en su empresa se aplique una convención de nomenclatura mediante una directiva que determina el nombre que puede asignar a la nueva cuenta de usuario.
 - ♦ Por defecto, DRA coloca la nueva cuenta de usuario en la unidad administrativa Usuarios del dominio gestionado.
 - ♦ No se pueden crear objetos InetOrgPerson en DRA.
-

Clonar una cuenta de usuario

Al clonar una cuenta de usuario, los grupos de los que el usuario es miembro se añaden automáticamente a la nueva cuenta de usuario, lo que le permite ahorrar tiempo en la configuración de la nueva cuenta. Puede añadir o eliminar grupos en la nueva cuenta, habilitar el correo electrónico y realizar cualquier otra configuración de propiedades como lo haría con cualquier cuenta nueva.

Nota: Al clonar un objeto InetOrgPerson, puede crear una cuenta de usuario.

Modificar las propiedades de las cuentas de usuario

Puede gestionar las propiedades de las cuentas de usuario en el dominio o el subárbol gestionados. Los poderes de los que disponga determinarán las propiedades que puede modificar para una cuenta de usuario. Si ha instalado Exchange y ha habilitado la compatibilidad con Microsoft Exchange, puede modificar las propiedades del buzón asociadas mientras gestiona las cuentas de usuario.

Nota: Si se han habilitado las directivas del directorio personal, DRA modifica automáticamente el directorio personal de una cuenta de usuario al gestionar esa cuenta. Por ejemplo, si cambia la ubicación del directorio personal, DRA intenta crear el directorio personal especificado y transfiere el contenido del directorio personal anterior a la nueva ubicación. DRA también aplica las ACL asignadas del directorio anterior al nuevo.

Gestionar su propia cuenta

Puede gestionar su propia cuenta mediante la modificación de las propiedades generales, como su número de teléfono. Antes de gestionar su cuenta, asegúrese de que dispone del poder adecuado.

Cambiar el nombre de una cuenta de usuario

Puede cambiar el nombre de las cuentas de usuario en el dominio o el subárbol gestionados. Al cambiar el nombre de entrada a la sesión del usuario, también se modifica el buzón asociado a la cuenta de usuario.

Habilitar una cuenta de usuario

Puede habilitar una cuenta de usuario en el dominio o el subárbol gestionados. Si gestiona una cuenta de Microsoft Windows, puede especificar el controlador de dominio en el que DRA aplica este cambio.

Al aplicar este cambio a un controlador de dominio específico, DRA también lo aplica en el controlador de dominio por defecto para este dominio gestionado. Para verificar el controlador de dominio por defecto que está utilizando DRA, consulte las propiedades del dominio.

Inhabilitar una cuenta de usuario

Puede inhabilitar una cuenta de usuario en el dominio gestionado. Si gestiona una cuenta de Microsoft Windows, puede especificar el controlador de dominio en el que DRA aplica este cambio.

Al aplicar este cambio a un controlador de dominio específico, DRA también lo aplica en el controlador de dominio por defecto para este dominio gestionado. Para verificar el controlador de dominio por defecto que está utilizando DRA, consulte las propiedades del dominio.

Desbloquear una cuenta de usuario

Puede desbloquear una cuenta de usuario en el dominio o el subárbol gestionados.

Como DRA recupera el estado de la cuenta de usuario de la memoria caché de cuentas, la interfaz de usuario puede indicar que la cuenta seleccionada está desbloqueada cuando realmente está bloqueada. DRA permite desbloquear una cuenta de usuario, incluso aunque el estado de la cuenta indique que se encuentra bloqueada. También puede especificar un controlador de dominio al desbloquear una cuenta de usuario mediante la consola de DRA sin necesidad de restablecer la contraseña de la cuenta de usuario.

Restablecer la contraseña de una cuenta de usuario

Puede restablecer la contraseña de una cuenta en el dominio o el subárbol gestionados. Los poderes de los que disponga determinarán los campos que puede modificar en esa cuenta de usuario.

Al restablecer la contraseña de una cuenta de usuario, DRA desbloquea automáticamente la cuenta. Puede seleccionar si DRA genera una nueva contraseña para la cuenta de usuario. También puede modificar varias opciones relacionadas con la contraseña de la cuenta. Si gestiona una cuenta de Microsoft Windows, puede especificar el controlador de dominio en el que DRA aplica estos cambios.

Nota: Al aplicar este cambio a un controlador de dominio específico, DRA también lo aplica en el controlador de dominio por defecto para este dominio gestionado. Para verificar el controlador de dominio por defecto que está utilizando DRA, consulte las propiedades del dominio.

Copiar una cuenta de usuario a otra ActiveView

Puede copiar una cuenta de usuario en otra ActiveView. Esta acción recibe el nombre de transferencia de una cuenta de usuario. Para copiar una cuenta de usuario en otra ActiveView, necesita disponer del poder para copiar un usuario en otra ActiveView tanto en la ActiveView de origen como en la de destino. Al transferir una cuenta de usuario a otra ActiveView, no se elimina la cuenta de usuario de la ActiveView de origen.

Mover una cuenta de usuario a otro contenedor

Puede mover una cuenta de usuario a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Suprimir una cuenta de usuario

Puede suprimir una cuenta de usuario en el dominio o el subárbol gestionados. Si se ha inhabilitado la Papelera para ese dominio, al suprimir una cuenta de usuario, esta se elimina de forma permanente de Active Directory. Si se ha habilitado la Papelera para ese dominio, al suprimir una cuenta de usuario, esta se transfiere a la Papelera.

Advertencia: Al crear una cuenta de usuario, Microsoft Windows asigna un identificador de seguridad (SID) a esa cuenta. El SID no se genera a partir del nombre de la cuenta. Microsoft Windows utiliza los SID para registrar privilegios en listas de control de acceso (ACL) para cada recurso. Si suprime una cuenta de usuario, no puede devolver las funciones de acceso de esa cuenta mediante la creación de una nueva cuenta de usuario con el mismo nombre.

Especificar la pertenencia a grupos de las cuentas de usuario

Puede añadir o eliminar cuentas de usuario en un grupo específico del dominio o el subárbol gestionados. También puede ver o modificar las propiedades de los grupos existentes a los que pertenece esa cuenta.

3.1.3 Transformación de cuentas de usuario

DRA permite transformar de forma rápida y eficaz las cuentas de usuario. Cuando el individuo asociado a una cuenta de usuario adquiere nuevas responsabilidades laborales, puede utilizar las funciones de transformación de DRA. Mediante las plantillas de funciones de trabajo, puede añadir, eliminar o actualizar rápidamente las pertenencias a grupos asociadas a una cuenta. Ya sea para indicar el ascenso de una persona, los cambios realizados en el departamento o la salida de la empresa, la capacidad de transformar una cuenta de usuario le ahorrará tiempo, dinero y conjeturas.

Descripción del proceso de transformación

Puede usar las funciones de transformación de la cuenta de usuario para satisfacer cualquiera de las siguientes necesidades:

- ♦ Eliminar la pertenencia a un grupo de una cuenta de usuario.

- ♦ Añadir pertenencias a grupos a una cuenta de usuario.
- ♦ Cambiar las propiedades de usuario.
- ♦ Eliminar pertenencias a grupos específicas, al mismo tiempo que se añaden otras a una cuenta de usuario.

Tenga en cuenta el siguiente proceso antes de intentar transformar una cuenta de usuario:

- 1 Decida si desea añadir, eliminar (o realizar ambas acciones) y eliminar las pertenencias a grupos.
- 2 Revise las plantillas de sustracción y aditivas actuales para asegurarse de que dispone de las cuentas de usuario de plantilla necesarias.
- 3 Si es necesario, cree todas las cuentas de plantilla necesarias.
- 4 Complete el Asistente para transformar usuarios.

A medida que DRA transforma un usuario, las pertenencias a grupos designadas por la plantilla de sustracción se eliminan de la cuenta de usuario, mientras que las pertenencias designadas por la plantilla de adición se asignan a la cuenta de usuario. DRA deja intactas las pertenencias que se encuentran fuera de las plantillas de sustracción o adición. Por ejemplo, una persona de su departamento de venta externo se transfiere del equipo de ventas de EE. UU. al de Europa. Dentro de su organización, hay grupos de distribución y grupos de seguridad que son exclusivos para estos equipos de ventas y otros que comparten todos los equipos de ventas. El equipo de ventas de EE. UU. cuenta con los grupos de distribución "LD zonas activas EE. UU." y "LD gestión ventas EE. UU.", mientras que el equipo de ventas europeo tiene los grupos de distribución "Zonas activas Europa" y "Gestión ventas Europa". Ambos equipos son miembros del grupo de seguridad "Seguridad global ventas", pero disponen de grupos de seguridad específicos del emplazamiento.

La plantilla de sustracción denominada "Plantilla ventas EE. UU." se asignaría a las siguientes pertenencias a grupos:

- ♦ LD zonas activas EE. UU.
- ♦ LD gestión ventas EE. UU.
- ♦ Seguridad global ventas
- ♦ Seguridad EE. UU.

La plantilla de adición denominada "Ventas Europa" se asignaría a las siguientes pertenencias a grupos:

- ♦ LD zonas activas Europa
- ♦ LD gestión ventas Europa
- ♦ Seguridad global ventas
- ♦ Seguridad Europa

Durante el proceso de transformación, la cuenta de usuario del vendedor transferido se elimina primero de todas las pertenencias a grupos designadas por la plantilla "Plantilla ventas EE. UU." y, a continuación, se añade a todas las pertenencias a grupos designadas por la plantilla "Plantilla ventas Europa". Si esta persona también era miembro del grupo de distribución "Jugadores póquer", la pertenencia a ese grupo no se modifica.

Los siguientes poderes permiten a un administrador asistente modificar de forma adicional una cuenta de usuario durante el proceso de transformación:

- ♦ Modificar las propiedades de dirección durante la transformación de una cuenta de usuario.
- ♦ Modificar la descripción durante la transformación de una cuenta de usuario.

- ♦ Modificar la oficina durante la transformación de una cuenta de usuario.
- ♦ Modificar las propiedades de teléfono durante la transformación de una cuenta de usuario.

También puede restringir la capacidad de añadir o eliminar pertenencias a grupos mediante la concesión a un administrador asistente solo uno de los siguientes poderes:

- ♦ Añadir un usuario a los grupos encontrados en una plantilla.
- ♦ Eliminar un usuario de los grupos encontrados en una plantilla.

Puede utilizar cualquiera de estas opciones de limitación basadas en poderes para crear un nivel de seguridad dentro de su organización. Al otorgar a determinadas personas la capacidad de eliminar solo los grupos encontrados en una plantilla, puede crear cuentas de usuario provisionales. Estas cuentas provisionales se pueden revisar antes de que un administrador asistente distinto utilice una cuenta de plantilla de adición para otorgar las nuevas pertenencias a grupos.

Creación de plantillas de transformación de usuarios

La transformación de cuentas de usuario está directamente vinculada a las funciones y la jerarquía de puestos de su organización. Considere la posibilidad de crear una plantilla para cada función o cargo en su empresa. DRA no hace distinción entre una plantilla de cuenta de usuario utilizada como de sustracción o de adición. Cree una única cuenta de usuario de plantilla para cada función dentro de su organización. Durante la transformación, seleccione la plantilla como de sustracción o adición. La selección de una plantilla como de sustracción no impide que la misma plantilla se utilice como de adición en una transformación futura.

Para crear una plantilla de transformación de usuario, debe tener los poderes para crear una cuenta de usuario y asignarla a los grupos adecuados. Estos poderes se pueden obtener al asociar su cuenta con las funciones Crear y suprimir cuentas de usuario y Administración de grupos en las ActiveViews adecuadas o mediante la asignación de poderes individuales.

Transformación de cuentas de usuario

La transformación de una cuenta de usuario le permite añadir o eliminar (o realizar ambas acciones) pertenencias a grupos de cuentas de usuario. Utilice este flujo de trabajo como ayuda cuando las personas cambien de un cargo a otro dentro de su organización. Debe disponer de la función Transformar un usuario o una función que contenga los poderes adecuados para transformar cuentas de usuario. Esta función solo puede realizarse desde la consola de gestión de cuentas y recursos.

Para transformar una cuenta de usuario:

- 1 En el panel izquierdo, expanda **Todos mis objetos gestionados**.
- 2 Para especificar la cuenta de usuario que desea gestionar, ejecute la operación **Buscar ahora** para localizar el objeto y, a continuación, selecciónelo.
- 3 Haga clic en **Tareas > Transformar**.
- 4 Revise la ventana de bienvenida y, a continuación, haga clic en **Siguiente**.
- 5 En la ventana Seleccionar plantilla de usuario, utilice **Examinar** para seleccionar el usuario de plantilla de sustracción adecuado.
- 6 Si desea revisar las propiedades de la cuenta de usuario de plantilla de sustracción, haga clic en **Ver**.
- 7 Utilice **Examinar** para seleccionar el usuario de plantilla de adición adecuado.
- 8 Si desea revisar las propiedades de la cuenta de usuario de plantilla de adición, haga clic en **Ver**.

- 9 Si dispone de los poderes adecuados, puede marcar la opción **Change other properties of the user** (Cambiar otras propiedades del usuario) y seleccionar las propiedades que desea modificar. Haga clic en **Siguiente** para desplazarse por las propiedades disponibles.
- 10 Haga clic en **Siguiente**.
- 11 Revise la ventana de resumen y haga clic en **Finalizar**.

3.2 Gestión de grupos

Como administrador asistente, puede utilizar DRA para gestionar grupos y modificar sus propiedades. Los grupos permiten conceder permisos específicos a un conjunto definido de cuentas de usuario. Los grupos permiten controlar a qué datos y recursos puede acceder una cuenta de usuario en cualquier dominio.

Puede gestionar grupos de cualquier tipo y ámbito. Por ejemplo, puede anidar grupos, lo que permite que un grupo pueda heredar permisos de otros grupos. También puede controlar de forma eficaz las pertenencias a grupos en dominios mediante la adición de grupos de dominios de confianza a otros grupos en el dominio gestionado y la administración de asignaciones de grupos temporales.

3.2.1 Tareas de gestión de grupos

En esta sección, se le guiará por el proceso de administración de grupos en la consola de gestión de cuentas y recursos. Con los poderes adecuados, puede realizar varias tareas de administración de grupos, como modificar las pertenencias a grupos. Si selecciona varios grupos, puede realizar las tareas seleccionadas en una única operación, como mover o añadir miembros a un grupo, o suprimirlos de este. El menú Tareas indica las tareas que puede llevar a cabo al seleccionar una o varios grupos.

Añadir cuentas a grupos

Puede añadir cuentas de usuario, contactos y equipos a un grupo gestionado.

Nota: Esta tarea añade varias cuentas al grupo seleccionado. Puede añadir una única cuenta a un grupo. Para ello, seleccione la cuenta adecuada y, a continuación, haga clic en Añadir a grupos en el menú Tareas.

Si la adición de una cuenta a otro grupo aumenta sus poderes en la cuenta, DRA no le permitirá añadirla.

Añadir grupos a otros grupos

Puede anidar grupos mediante la adición de un grupo a otro grupo gestionado. Si un grupo se ha anidado en otro grupo, el grupo secundario puede heredar permisos del grupo principal.

Nota: Si la adición de un grupo a otro aumenta sus poderes en el grupo de origen, DRA no le permitirá añadirlo.

Modificar las propiedades de los grupos

Puede modificar las propiedades de los grupos locales y globales. Los poderes de los que disponga determinarán las propiedades que puede modificar para un grupo en el dominio o el subárbol gestionados. Si ha instalado Exchange y ha habilitado la compatibilidad con Microsoft Exchange, puede modificar las propiedades de la lista de distribución mientras gestiona grupos.

Crear un grupo

Puede crear un grupo en el dominio o el subárbol gestionados. También puede modificar las propiedades del nuevo grupo como, por ejemplo, los miembros del grupo.

Nota

- ♦ Es posible que en su empresa se aplique una convención de nomenclatura mediante una directiva que determina el nombre que puede asignar al nuevo grupo.
 - ♦ Por defecto, DRA coloca el nuevo grupo en la unidad administrativa Usuarios del dominio gestionado.
-

Especificar los miembros del grupo

Puede añadir o eliminar cuentas de usuario, contactos, equipos u otros grupos en el grupo gestionado. DRA solo permite eliminar entidades de seguridad externas. También puede ver o modificar las propiedades de los miembros de grupo existentes, excepto las entidades de seguridad externas.

Al eliminar miembros de un grupo, DRA no suprime los objetos. Al añadir miembros a un grupo, debe disponer del poder para modificar los objetos que desea añadir.

Nota: No puede añadir cuentas de usuario o grupos a ninguno de los grupos especiales de Windows (Administradores, Operadores de cuentas, Operadores de copia de seguridad u Operadores de servidor) a menos que sea un administrador de Windows o un miembro de ese grupo especial específico.

Especificar la pertenencia a grupos

Puede añadir o eliminar un grupo en otros grupos en el dominio o el subárbol gestionados. También puede ver o modificar las propiedades de los grupos existentes a los que pertenece este grupo.

Configurar permisos de seguridad de pertenencia a grupo

Puede definir permisos de seguridad de Active Directory para las pertenencias a grupos. Estos permisos especifican quién puede ver (leer) y modificar (escribir) las pertenencias a grupos mediante Microsoft Outlook. Esta configuración permite proteger de forma más eficaz listas de distribución y grupos de seguridad en el entorno. No se pueden modificar los permisos de seguridad heredados.

Nota: Al gestionar la seguridad de la pertenencia a grupo, los permisos inhabilitados pueden indicar permisos heredados.

Configurar la propiedad del grupo

Puede definir la propiedad de cualquier grupo de distribución o seguridad de Microsoft Windows. Puede otorgar el permiso de propiedad del grupo a una cuenta de usuario, un grupo o un contacto. Al otorgar la propiedad del grupo, la cuenta de usuario, el grupo o el contacto especificados modifican la pertenencia a ese grupo.

Nota: DRA inhabilita la casilla de verificación **Manager can update membership list** (El gestor puede actualizar la lista de miembros) cuando la pertenencia al grupo está oculta para el servidor de Microsoft Exchange. Para habilitar esta casilla de verificación, haga clic en **Expose Group Membership** (Mostrar pertenencia a grupo) en la pestaña Exchange de la ventana Group Properties (Propiedades del grupo).

Clonar un grupo

Puede clonar grupos tanto locales como globales en los dominios gestionados. La clonación de grupos crea nuevos grupos del mismo tipo y con los mismos atributos que el grupo original. DRA también intenta añadir todos los miembros del grupo original al nuevo grupo.

Al clonar un grupo, puede crear rápidamente grupos basados en otros con propiedades similares. Al clonar un grupo, DRA incluye los valores del grupo seleccionado en el Asistente para clonar grupos. También puede modificar las propiedades del nuevo grupo.

Nota

- ♦ Es posible que en su empresa se aplique una convención de nomenclatura mediante una directiva que determina el nombre que puede asignar al nuevo grupo.
 - ♦ Por defecto, DRA coloca el nuevo grupo en la unidad administrativa Usuarios del dominio gestionado.
-

Suprimir un grupo

Puede suprimir grupos locales y globales en el dominio o el subárbol gestionados. Si se ha inhabilitado la Papelera para ese dominio, al suprimir un grupo, este se elimina de forma permanente de Active Directory. Si la Papelera se ha habilitado para ese dominio, al suprimir un grupo, este se transfiere a la Papelera y se desactivan las propiedades del grupo.

Para obtener más información sobre la Papelera, consulte [Gestionar la Papelera](#).

Advertencia: Al crear un grupo, Microsoft Windows asigna un identificador de seguridad (SID) a ese grupo. El SID no se genera a partir del nombre del grupo. Microsoft Windows utiliza los SID para registrar privilegios en listas de control de acceso (ACL) para cada recurso. Si suprime un grupo, no puede devolver las funciones de acceso de ese grupo mediante la creación de un nuevo grupo con el mismo nombre.

Mover un grupo a otro contenedor

Puede mover un grupo a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Mostrar las pertenencias a grupos en listas de distribución

Puede visualizar las pertenencias a grupos en listas de distribución de los grupos en el dominio o el subárbol gestionados.

Ocultar las pertenencias a grupos en listas de distribución

Puede ocultar las pertenencias a grupos en listas de distribución de los grupos en el dominio o el subárbol gestionados.

3.2.2 Asignaciones temporales de grupos

Las asignaciones temporales de grupos permiten gestionar la pertenencia a un grupo para usuarios que solo la necesitan durante un periodo específico. En esta sección, se le guiará por el proceso de administración de asignaciones temporales de grupos en la consola de gestión de cuentas y recursos. Con los poderes adecuados, puede realizar tareas, como crear nuevas asignaciones temporales de grupos o eliminar las asignaciones temporales de grupos caducadas. Solo puede llevar a cabo estas tareas en el servidor de administración principal. El menú Tareas indica las tareas que puede llevar a cabo al seleccionar una o varias asignaciones temporales de grupos.

Gestionar las propiedades de las asignaciones temporales de grupos

Solo puede gestionar las propiedades de las asignaciones temporales de grupo o las propiedades temporales de grupos caducadas guardadas en el servidor de administración principal. Los poderes de los que disponga determinarán las propiedades que puede modificar para una asignación temporal de grupos.

Crear una nueva asignación temporal de grupos

Solo puede crear una asignación temporal de grupos en el servidor de administración principal. También puede modificar las propiedades como, por ejemplo, programaciones, para la nueva asignación temporal de grupos.

Gestionar cuentas de usuario de una asignación temporal de grupos

Puede añadir o eliminar cuentas de usuario de asignaciones temporales de grupos en el servidor de administración principal.

Nota: Solo puede gestionar cuentas de usuario para asignaciones temporales de grupos que aún no estén activas.

Reprogramar una asignación temporal de grupos

Solo puede reprogramar asignaciones temporales de grupos en el servidor de administración principal. También puede reprogramar una asignación temporal de grupos caducada que se haya guardado.

Nota: Cuando caduca una asignación temporal de grupos, DRA la elimina automáticamente, a menos que la haya guardado para utilizarla en el futuro.

Suprimir una asignación temporal de grupos

Puede suprimir cualquier asignación temporal de grupos en el servidor de administración principal.

3.3 Gestión de grupos dinámicos de distribución

Un grupo dinámico de distribución es un objeto de grupo de Active Directory habilitado para correo que puede crear para agilizar el envío masivo de mensajes de correo electrónico y otra información.

La lista de miembros de un grupo dinámico de distribución se calcula cada vez que se envía un mensaje al grupo en función de los filtros y las condiciones que defina. Esto difiere de un grupo de distribución normal, que contiene un conjunto definido de miembros. Cuando se envía un mensaje de correo electrónico a un grupo dinámico de distribución, se entrega a todos los destinatarios de la organización que coincidan con los criterios definidos para ese grupo.

DRA admite las siguientes funciones:

- ♦ Auditoría e informes de la interfaz de usuario
- ♦ Compatibilidad con la enumeración de grupos dinámicos de distribución
- ♦ Informes de NetIQ Reporting Center (NRC) para grupos dinámicos de distribución
- ♦ Compatibilidad de las operaciones de activadores con los grupos dinámicos de distribución
- ♦ Compatibilidad de la extensión de interfaz de usuario con los grupos dinámicos de distribución

Tareas de los grupos dinámicos de distribución:

Crear un grupo dinámico de distribución

Puede crear un grupo dinámico de distribución en el dominio o el subárbol gestionados. También puede modificar las propiedades del nuevo grupo dinámico de distribución como, por ejemplo, los miembros del grupo.

Nota

- ♦ Es posible que en su empresa se aplique una convención de nomenclatura mediante una directiva que determina el nombre que puede asignar al nuevo grupo dinámico de distribución.
 - ♦ Por defecto, DRA coloca el nuevo grupo dinámico de distribución en la unidad administrativa Usuarios del dominio gestionado.
-

Clonar un grupo dinámico de distribución

Puede clonar grupos dinámicos de distribución tanto locales como globales en los dominios gestionados. La clonación de grupos dinámicos de distribución crea nuevos grupos dinámicos de distribución del mismo tipo y con los mismos atributos que el grupo dinámico de distribución original.

Al clonar un grupo dinámico de distribución, puede crear rápidamente grupos dinámicos de distribución basados en otros con propiedades similares. Al clonar un grupo dinámico de distribución, DRA incluye los valores del grupo dinámico de distribución seleccionado en el Asistente para clonar grupos dinámicos de distribución. También puede modificar las propiedades del nuevo grupo dinámico de distribución.

Mover un grupo dinámico de distribución a otro contenedor

Puede mover un grupo dinámico de distribución a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Suprimir un grupo dinámico de distribución

Puede suprimir grupos dinámicos de distribución locales y globales en el dominio o el subárbol gestionados. Si se ha inhabilitado la Papelera para ese dominio, al suprimir un grupo dinámico de distribución, este se elimina de forma permanente de Active Directory. Si la Papelera se ha habilitado para ese dominio, al suprimir un grupo dinámico de distribución, este se transfiere a la Papelera y se desactivan las propiedades del grupo dinámico de distribución.

Para obtener más información sobre la Papelera, consulte [Gestionar la Papelera](#).

Advertencia: Al crear un grupo dinámico de distribución, Microsoft Windows asigna un identificador de seguridad (SID) a ese grupo dinámico de distribución. El SID no se genera a partir del nombre del grupo dinámico de distribución. Microsoft Windows utiliza los SID para registrar privilegios en listas de control de acceso (ACL) para cada recurso. Si suprime un grupo dinámico de distribución, no puede devolver las funciones de acceso de ese grupo dinámico de distribución mediante la creación de un nuevo grupo dinámico de distribución con el mismo nombre.

Modificar las propiedades de grupos dinámicos de distribución

Puede modificar las propiedades de los grupos dinámicos de distribución locales y globales. Los poderes de los que disponga determinarán las propiedades que puede modificar para un grupo en el dominio o el subárbol gestionados.

Especificar un filtro

La pertenencia de una lista de distribución dinámica se determina mediante su filtro, que puede definir.

Especificar condiciones

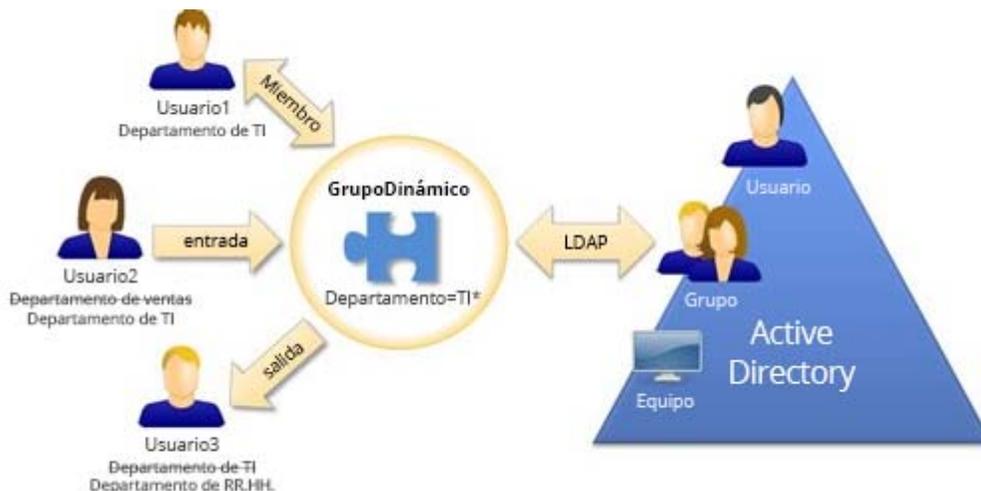
Las condiciones definen los criterios que un objeto debe cumplir para ser miembro del grupo dinámico de distribución.

3.4 Gestión de grupos dinámicos

Un grupo dinámico es uno cuya pertenencia cambia en función de un conjunto definido de criterios. Hasta ahora, los grupos dinámicos solo eran posibles en el entorno de Exchange, pero ahora también se pueden crear en la configuración de Active Directory.

En el gráfico mostrado a continuación, se describe un uso típico de un grupo dinámico de Active Directory. Hay tres grupos dinámicos en el gráfico. Cada grupo dispone de un conjunto de criterios que determina quién puede añadirse al grupo y quién no. Cada grupo controla el acceso a un conjunto específico de archivos, carpetas y aplicaciones.

Sugerencia: Puede crear una *lista de miembros estáticos* que contenga miembros permanentes del grupo dinámico; también puede crear una *lista de miembros excluidos* que deniegue la pertenencia al grupo dinámico a esos usuarios.



El Usuario2 se ha unido recientemente al departamento de TI. Cuando se actualice el grupo dinámico del departamento de TI, se añadirá al grupo. Cuando se actualice el grupo dinámico del departamento de ventas, el Usuario2 se eliminará de su lista de miembros.

Sugerencia: Puede actualizar la lista de miembros de un grupo dinámico. Para ello, haga clic con el botón derecho en ella y seleccione **Actualizar miembros**.

El Usuario3 que ha dejado el departamento de TI para pasar al de RR.HH. se eliminará del grupo dinámico del departamento de TI y se añadirá al grupo dinámico del departamento de RR.HH.

Crear un grupo dinámico

Puede crear un grupo dinámico en el dominio o el subárbol gestionados. También puede modificar las propiedades del nuevo grupo dinámico como, por ejemplo, los miembros del grupo.

Nota

- ♦ Es posible que en su empresa se aplique una convención de nomenclatura mediante una directiva que determina el nombre que puede asignar al nuevo grupo dinámico.
 - ♦ Por defecto, DRA coloca el nuevo grupo dinámico en la unidad administrativa Usuarios del dominio gestionado.
-

Crear un filtro

El grupo dinámico utiliza el filtro para añadir o eliminar usuarios en la lista de miembros cada vez que se actualiza el grupo.

Gestionar la lista de miembros estáticos

Los usuarios incluidos en una lista de miembros estáticos de un grupo dinámico se convierten en miembros permanentes del grupo hasta que se les elimina manualmente.

Al eliminar miembros de un grupo dinámico, DRA no suprime los objetos. Al añadir miembros a un grupo dinámico, debe disponer del poder para modificar los objetos que desea añadir.

Gestionar la lista de miembros excluidos

Los usuarios incluidos en la lista de miembros excluidos de un grupo dinámico no se podrán unir al grupo hasta que se eliminen manualmente de la lista.

Actualizar la lista de miembros

Puede actualizar los miembros de un grupo dinámico mediante la acción [Actualizar miembros](#).

Clonar un grupo dinámico

Puede clonar grupos dinámicos tanto locales como globales en los dominios gestionados. La clonación de grupos dinámicos crea nuevos grupos dinámicos de distribución del mismo tipo y con los mismos atributos que el grupo dinámico original.

Al clonar un grupo dinámico, puede crear rápidamente grupos dinámicos basados en otros con propiedades similares. Al clonar un grupo dinámico, DRA incluye los valores del grupo dinámico seleccionado en el Asistente para clonar grupos dinámicos. También puede modificar las propiedades del nuevo grupo dinámico.

Mover un grupo dinámico a otro contenedor

Puede mover un grupo dinámico a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Suprimir un grupo dinámico

Puede suprimir grupos dinámicos locales y globales en el dominio o el subárbol gestionados. Si se ha inhabilitado la Papelera para ese dominio, al suprimir un grupo dinámico, este se elimina de forma permanente de Active Directory. Si la Papelera se ha habilitado para ese dominio, al suprimir un grupo dinámico, este se transfiere a la Papelera y se desactivan las propiedades del grupo dinámico.

Para obtener más información sobre la Papelera, consulte [Gestionar la Papelera](#).

Advertencia: Al crear un grupo dinámico, Microsoft Windows asigna un identificador de seguridad (SID) a ese grupo dinámico. El SID no se genera a partir del nombre del grupo dinámico. Microsoft Windows utiliza los SID para registrar privilegios en listas de control de acceso (ACL) para cada recurso. Si suprime un grupo dinámico, no puede devolver las funciones de acceso de ese grupo dinámico mediante la creación de un nuevo grupo dinámico con el mismo nombre.

Modificar las propiedades de grupos dinámicos

Puede modificar las propiedades de los grupos dinámicos locales y globales. Los poderes de los que disponga determinarán las propiedades que puede modificar para un grupo en el dominio o el subárbol gestionados.

Añadir grupos dinámicos a otros grupos dinámicos

Puede anidar grupos dinámicos mediante la adición de un grupo dinámico a otro grupo dinámico gestionado. Si un grupo dinámico se ha anidado en otro, el grupo dinámico secundario puede heredar permisos del grupo dinámico principal.

Nota: Si la adición de un grupo dinámico a otro aumenta sus poderes en el grupo dinámico de origen, DRA no le permitirá añadirlo.

Configurar permisos de seguridad de pertenencia a grupo

Puede definir permisos de seguridad de Active Directory para las pertenencias a grupos dinámicos. Estos permisos especifican quién puede ver (leer) y modificar (escribir) las pertenencias a grupos dinámicos mediante Microsoft Outlook. Esta configuración permite proteger de forma más eficaz listas de distribución y grupos dinámicos de seguridad en el entorno. No se pueden modificar los permisos de seguridad heredados.

Nota: Al gestionar la seguridad de la pertenencia a un grupo dinámico, los permisos inhabilitados pueden indicar permisos heredados.

Configurar la propiedad del grupo dinámico

Puede otorgar el permiso de propiedad del grupo dinámico a una cuenta de usuario, un grupo o un contacto. Al otorgar la propiedad del grupo dinámico, la cuenta de usuario, el grupo o el contacto especificados modifican la pertenencia a este grupo dinámico.

Mostrar las pertenencias a grupos dinámicos en listas de distribución

Puede visualizar las pertenencias a grupos dinámicos en listas de distribución para grupos en el dominio o el subárbol gestionados.

Ocultar las pertenencias a grupos dinámicos en listas de distribución

Puede ocultar las pertenencias a grupos dinámicos en listas de distribución de grupos en el dominio o el subárbol gestionados.

Nota: La opción **Hide Group Membership** (Ocultar pertenencia a grupo) está inhabilitada en las listas de distribución de Microsoft Exchange 2007.

3.5 Gestión de contactos

DRA permite gestionar muchos objetos de red, incluidos los contactos y las direcciones de correo electrónico asociadas. Los contactos solo están disponibles en dominios de Microsoft Windows en modo mixto o nativo. Los contactos no disponen de un identificador de seguridad (SID), a diferencia de las cuentas de usuario y los grupos. Utilice contactos para añadir miembros a listas de distribución o grupos sin otorgarles acceso a los servicios de red.

Puede añadir contactos a grupos de seguridad o distribución en dominios en modo mixto y nativo. Dado que los grupos de seguridad se pueden utilizar como listas de distribución de Microsoft Windows, es posible que desee añadir contactos a estos grupos. Tener un contacto en un grupo de seguridad global no impide que el grupo se convierta en un grupo de seguridad universal al migrar a un dominio de Microsoft Windows en modo nativo.

Modificar las propiedades de los contactos

Puede modificar las propiedades de los contactos. Los poderes de los que disponga determinarán las propiedades que puede modificar para un contacto en el dominio o el subárbol gestionados. Si ha instalado Exchange y ha habilitado la compatibilidad con Exchange, puede modificar las propiedades de la dirección de correo electrónico mientras gestiona los contactos.

Crear un contacto

Puede crear contactos en el dominio o el subárbol gestionados. También puede modificar las propiedades, habilitar el correo electrónico, y especificar direcciones de correo electrónico y pertenencias a grupos para el nuevo contacto.

Clonar un contacto

Al clonar un contacto, puede crear rápidamente contactos basados en otros con propiedades similares. Al clonar un contacto, DRA incluye los valores del contacto seleccionado en el Asistente para clonar contactos. También puede modificar las propiedades, habilitar el correo electrónico, y especificar direcciones de correo electrónico y pertenencias a grupos para el nuevo contacto.

Gestionar las pertenencias a grupos de los contactos

Puede añadir o eliminar contactos en un grupo específico del dominio o el subárbol gestionados. También puede ver o modificar las propiedades de los grupos existentes a los que pertenece este contacto.

Mover un contacto a otra unidad administrativa

Puede mover un contacto a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Suprimir un contacto

Puede suprimir un contacto en el dominio o el subárbol gestionados. Si se ha inhabilitado la Papelera para ese dominio, al suprimir un contacto, este se elimina de forma permanente de Active Directory. Si se ha habilitado la Papelera para ese dominio, al suprimir un contacto, este se transfiere a la Papelera.

Para obtener más información sobre la Papelera, consulte [Gestionar la Papelera](#).

4 Gestión de los buzones de Exchange y las carpetas públicas

Con DRA, puede gestionar los buzones de Microsoft Exchange como una extensión de las propiedades de la cuenta de usuario. Esta integración permite simplificar los flujos de trabajo de administración para que pueda administrar de forma eficaz las propiedades de Exchange. También puede vincular buzones desde cuentas de usuario y bosques de cuentas de Exchange, y gestionar buzones de recursos, buzones compartidos y carpetas públicas.

Gestión de tareas de buzones en la consola de gestión de cuentas y recursos

Al usar la consola de gestión de cuentas y recursos, puede ejecutar las tareas de buzones correspondientes desde la pestaña **Exchange Tasks** (Tareas de Exchange) en las propiedades del objeto, a las que también se puede acceder desde **Tareas** o el menú contextual del objeto seleccionado. Por lo general, debe seleccionar el nodo **Todos mis objetos gestionados** y ejecutar la operación **Buscar ahora** para localizar y seleccionar el objeto que desee.

Gestión de tareas de buzones en la consola Web

Al utilizar la consola Web, puede ejecutar las tareas de buzones correspondientes en **Gestión** > pestaña **Buscar**. Por lo general, debe ejecutar una operación de búsqueda para localizar y seleccionar el objeto de buzón que desee. Una vez que seleccione uno o varios objetos en la lista, se activarán los botones de la barra de herramientas. Coloque el puntero del ratón sobre los botones para visualizar sus funciones. Todas las opciones relacionadas con el correo se encuentran en la parte derecha de la barra de herramientas.



4.1 Gestión de tareas de buzones de usuario

Puede gestionar los buzones de Microsoft Exchange de las cuentas de usuario en el dominio o en el subárbol gestionados. Todos los aspectos de la gestión de los buzones de Microsoft Exchange requieren poderes diferentes. Los poderes de los que dispone controlan las propiedades del buzón que puede modificar, o si puede crear, clonar, ver o suprimir buzones de Microsoft Exchange. También puede gestionar los derechos y los permisos de los buzones asociados a una cuenta de usuario, lo que le permite controlar la seguridad de los entornos de Microsoft Exchange. Si no dispone de los poderes necesarios para modificar una pestaña o un campo del buzón seleccionado, DRA inhabilita las pestañas y los campos que no puede modificar.

Además de las tareas definidas a continuación, las cuentas de usuario pueden tener opciones habilitadas en las propiedades del objeto por el administrador de DRA para configurar los ajustes de Skype y Skype Online. Skype se puede configurar desde cuentas de usuario tanto en la consola de gestión de cuentas y recursos como en la consola Web. Skype Online solo se puede configurar desde la consola Web.

Crear un buzón

Puede crear un buzón de Microsoft Exchange para una cuenta de usuario existente. También puede modificar las propiedades del nuevo buzón.

Nota: Al crear un buzón, Exchange genera las cadenas de apoderado necesarias en función de la configuración de directivas de Exchange. Microsoft Exchange también genera las cadenas de apoderado por defecto. Como resultado, al visualizar las propiedades del buzón recién creado, podrá ver los dos tipos de cadenas de apoderado.

Clonar una cuenta de usuario

Al clonar una cuenta de usuario, los grupos de los que el usuario es miembro se añaden automáticamente a la nueva cuenta de usuario, lo que le permite ahorrar tiempo en la configuración de la nueva cuenta. Puede añadir o eliminar grupos en la nueva cuenta, habilitar el correo electrónico y realizar cualquier otra configuración de propiedades como lo haría con cualquier cuenta nueva.

Nota: Al clonar un objeto InetOrgPerson, puede crear una cuenta de usuario.

Mover un buzón

Puede mover un buzón de Microsoft Exchange de una cuenta de usuario a otro almacén de buzones o servidor de Microsoft Exchange.

Modificar las propiedades de los buzones

Puede modificar las propiedades de los buzones de Microsoft Exchange a medida que gestiona las cuentas de usuario asociadas. Los poderes de los que dispone determinan las propiedades del buzón que puede modificar.

Nota: No puede modificar las propiedades del buzón de las cuentas de usuario gestionadas en los servidores miembros.

Configurar los permisos de seguridad del buzón

Puede especificar las cuentas de usuario, los grupos o los equipos a los que desee otorgar o denegar la capacidad de enviar y recibir correo electrónico con un buzón específico de Microsoft Exchange. Estos ajustes permiten proteger de forma más eficaz el entorno de Exchange. No se pueden modificar los permisos de seguridad heredados.

Nota: Al gestionar la seguridad del buzón, los permisos inhabilitados pueden indicar permisos heredados.

Eliminar los permisos de seguridad del buzón

Puede eliminar los permisos de seguridad del buzón de una cuenta de usuario, un grupo o un equipo asociados a un buzón de Microsoft Exchange. La eliminación de los permisos de seguridad del buzón impide que la cuenta de usuario, el grupo o la cuenta del equipo envíen y reciban correo electrónico a través del buzón especificado. No se pueden eliminar los permisos de seguridad heredados.

Configurar los derechos del buzón

Puede otorgar o denegar derechos de otras cuentas de usuario, grupos o equipos a un buzón específico de Microsoft Exchange. Estos ajustes permiten proteger de forma más eficaz el entorno de Exchange. No se pueden modificar los derechos de buzón heredados.

Nota: Al gestionar los derechos del buzón, los permisos inhabilitados pueden indicar permisos heredados.

Eliminar los derechos del buzón

Puede eliminar derechos del buzón de cuentas de usuario, grupos o equipos asociados a un buzón específico de Microsoft Exchange. La eliminación de los derechos del buzón impide que la cuenta de usuario, el grupo o la cuenta del equipo utilicen el buzón especificado. No se pueden eliminar los derechos de buzón heredados.

Suprimir un buzón

Puede suprimir un buzón asociado a una cuenta de usuario en el dominio o el subárbol gestionados. Al suprimir un buzón, también se eliminan todos los mensajes incluidos en él.

Añadir o modificar una dirección de correo electrónico

Puede especificar direcciones de correo electrónico para buzones asociados a cuentas de usuario en el dominio o el subárbol gestionados. También puede asignar direcciones de correo electrónico a las cuentas de usuario que aún no dispongan de buzones. Al gestionar los buzones de Microsoft Exchange, solo puede añadir los tipos de dirección de correo electrónico definidos por sus directivas de generación de apoderado.

Especificar una dirección de respuesta

Puede definir direcciones de respuesta para un buzón asociado a una cuenta de usuario en el dominio o el subárbol gestionados. Puede definir varias direcciones de respuesta para un buzón. Sin embargo, no puede definir más de un tipo de dirección de correo electrónico como una dirección de respuesta. Por ejemplo, no se puede especificar más de una dirección de Internet como una dirección de respuesta.

Suprimir una dirección de correo electrónico

Puede suprimir una dirección de correo electrónico mediante la eliminación de la dirección del buzón.

Especificar las opciones de entrega

Puede especificar los buzones que puede utilizar el usuario para enviar mensajes, definir opciones de reenvío y especificar límites de destinatarios.

Especificar restricciones de entrega

Al definir restricciones de entrega, puede limitar el tamaño de los mensajes entrantes y salientes, y la aceptación de los mensajes entrantes en un buzón específico.

Especificar límites de almacenamiento

Puede especificar límites de almacenamiento como, por ejemplo, advertencias en función del tamaño de un buzón. También puede especificar el tiempo de retención de los elementos suprimidos.

Comprobar el estado de los desplazamientos de buzones

Puede comprobar el estado de los desplazamientos de buzones y realizar acciones en ellos, como borrar el estado, cancelar un desplazamiento y reanudar un desplazamiento interrumpido.

4.2 Tareas de gestión de buzones de Office 365

Esta sección contiene información para gestionar los buzones de Microsoft Office 365 en la consola de administración de cuentas y recursos, y la consola Web. Con los poderes adecuados, puede realizar varias tareas de gestión de cuentas de usuario, como establecer retenciones por juicio y configurar el reenvío de correo electrónico.

Establecer una retención por juicio

Puede ser necesaria una retención por juicio cuando existe una expectativa razonable de una demanda. Las organizaciones deben conservar la información almacenada electrónicamente, incluido el correo electrónico, que sea pertinente para el caso.

Establezca una retención por juicio en un buzón para conservar todo su contenido, incluidos los elementos suprimidos y las versiones originales de los elementos modificados. Al establecer un buzón en retención por juicio, también se conserva el contenido, si existe, en el buzón de archivo del usuario. La retención puede durar un periodo especificado o hasta que se elimine la retención por juicio del buzón.

Debe disponer de una licencia de Exchange Online Enterprise E3 para establecer una retención por juicio. Puede configurar la función mediante la pestaña **Litigation Hold** (Retención por juicio) de las propiedades del objeto de usuario.

Delegar los permisos del buzón

Puede delegar los permisos del buzón de Office 365 a través de la pestaña Delegación de buzón de las propiedades del objeto de usuario. Existen tres tipos de permisos entre los que puede delegar: enviar como, enviar en nombre de y acceso completo. Los tipos de permisos que pueden delegarse dependen del tipo de objeto receptor.

Configurar el reenvío de correo electrónico

Puede habilitar el reenvío para cuentas de usuario mediante la opción Flujo de correo de las propiedades del objeto de usuario.

4.3 Tareas de gestión de buzones de recursos

La función de buzón de recursos de Microsoft Exchange le permite crear un buzón que representa un recurso, como una sala de conferencias, para que pueda reservarlo mediante el envío de una invitación a la reunión, como lo haría con una persona. DRA contiene un conjunto de funciones, poderes y directivas que permiten gestionar de forma eficaz los buzones de recursos.

DRA dispone de compatibilidad de extensión de IU con los buzones de recursos, además de permitir la creación de informes de auditoría o IU. DRA también incluye compatibilidad con los guiones de ADSI.

Crear un buzón de recursos

Puede crear buzones de recursos en el dominio o el subárbol gestionados.

Mover un buzón de recursos a otro contenedor

Puede mover un buzón de recursos a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Mover un buzón de recursos a otro almacenamiento de buzones u otra instancia de Exchange Server

Puede mover un buzón de recursos a otro almacenamiento de buzones u otra instancia de Microsoft Exchange Server.

Clonar un buzón de recursos

Al clonar un buzón de recursos, puede crear rápidamente otros con propiedades similares. Al clonar un buzón de recursos, DRA incluye los valores del recurso seleccionado en el Asistente para clonar buzones de recursos.

Cambiar el nombre de un buzón de recursos

Puede cambiar el nombre de buzones de recursos en el dominio o el subárbol gestionados. Al cambiar el nombre de entrada a la sesión del usuario, también se modifica el buzón asociado a la cuenta de usuario.

Añadir un buzón de recursos a un grupo

Puede añadir buzones de recursos a un grupo específico del dominio o el subárbol gestionados.

Suprimir un buzón de recursos de un contenedor

Puede suprimir un buzón de recursos de un dominio o un subárbol gestionados. Si se ha inhabilitado la Papelera para ese dominio, al suprimir un buzón de recursos, este se elimina de forma permanente de Active Directory. Si se ha habilitado la Papelera para ese dominio, al suprimir un buzón de recursos, este se transfiere a la Papelera.

Suprimir un buzón de recursos

Puede suprimir un buzón de recursos en el dominio o el subárbol gestionados. Al suprimir un buzón de recursos, también se eliminan todos los mensajes incluidos en él.

Restaurar un buzón de recursos suprimido

Puede restaurar un buzón de recursos suprimido si se ha habilitado la Papelera de ese dominio.

Modificar las propiedades del buzón de recursos

Puede gestionar las propiedades de los buzones de recursos en el dominio o el subárbol gestionados. Los poderes de los que dispone determinan las propiedades que puede modificar.

4.4 Tareas de gestión de buzones compartidos

Los buzones compartidos son útiles para los administradores del servicio de Ayuda técnica y el personal del servicio de asistencia técnica, ya que todas las respuestas se pueden configurar para que se introduzcan en un único buzón al que puedan acceder varios usuarios. El buzón debe encontrarse en un dominio gestionado por DRA con la directiva de Exchange habilitada y debe disponer de poderes delegados para gestionar buzones compartidos.

Al crear un buzón compartido, hay dos tipos de permisos que puede delegar a los usuarios: Enviar como y Acceso completo. Enviar como proporciona permisos para leer y enviar mensajes de correo electrónico. Puede delegar permisos a objetos de usuario y grupo. También puede especificar las restricciones y las opciones de entrega, los límites de almacenamiento, los permisos de carpeta y varias opciones adicionales en las propiedades del objeto.

La gestión de buzones compartidos solo se admite en la consola Web.

Crear un buzón compartido

Puede crear buzones compartidos en el dominio o el subárbol gestionados.

Mover un buzón compartido a otro contenedor

Puede mover un buzón compartido a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Mover un buzón compartido a otro almacenamiento de buzones

Puede mover un buzón compartido a otro almacenamiento de buzones.

Clonar un buzón compartido

Al clonar un buzón compartido, puede crear rápidamente otros con propiedades similares.

Cambiar el nombre de un buzón compartido

Puede cambiar el nombre de buzones compartidos en el dominio o el subárbol gestionados. Al cambiar el nombre de entrada a la sesión del usuario, también se modifica el buzón asociado a la cuenta de usuario.

Suprimir un buzón compartido de un contenedor

Puede suprimir un buzón compartido de un dominio o un subárbol gestionados. Si se ha inhabilitado la Papelera para ese dominio, al suprimir un buzón compartido, este se elimina de forma permanente de Active Directory. Si se ha habilitado la Papelera para ese dominio, al suprimir un buzón compartido, este se transfiere a la Papelera.

Suprimir un buzón compartido

Puede suprimir un buzón compartido en el dominio o el subárbol gestionados. Al suprimir un buzón compartido, también se eliminan todos los mensajes incluidos en él.

Restaurar un buzón compartido suprimido

Puede restaurar un buzón compartido que se haya suprimido si se ha habilitado la Papelera de ese dominio.

Crear un buzón compartido de archivo

Puede crear buzones compartidos archivados en el dominio o el subárbol gestionados.

Eliminar un buzón compartido de archivo

Puede suprimir buzones compartidos archivados en el dominio o el subárbol gestionados.

Modificar las propiedades del buzón compartido

Puede modificar las propiedades de los buzones compartidos en el dominio o el subárbol gestionados. Los poderes de los que dispone determinan las propiedades que puede modificar.

4.5 Tareas de gestión de buzones vinculados

Los buzones vinculados son útiles para los grandes cambios organizativos que se producen durante las fusiones, las adquisiciones y las divisiones de la empresa, cuando es habitual la migración de buzones. Esta función permite vincular buzones de diferentes bosques de Exchange para impedir la interrupción del correo electrónico del usuario. Los buzones deben encontrarse en dominios gestionados por DRA con la directiva de Exchange habilitada y debe disponer de poderes delegados para gestionar buzones vinculados. Al crear un buzón vinculado, se añade la pestaña **Buzón vinculado** a las propiedades del objeto de usuario.

La gestión de buzones vinculados solo se admite en la consola Web. Puede crear un buzón vinculado desde la barra de herramientas de la cuenta de usuario seleccionada. Esta opción solo está habilitada cuando el dominio del usuario seleccionado dispone de confianza de bosque externa con otros dominios gestionados en DRA. Solo las cuentas de usuario inhabilitadas aparecerán en la lista cuando se busque una cuenta para vincular en otro dominio gestionado por DRA.

Crear un buzón vinculado

Puede crear un buzón vinculado desde dos cuentas de usuario seleccionadas en diferentes bosques de Exchange gestionados.

Suprimir un buzón vinculado

Puede suprimir un buzón vinculado de la barra de herramientas de un usuario seleccionado que tenga un buzón vinculado.

Modificar las propiedades del buzón vinculado

Puede modificar las propiedades de un buzón vinculado desde la pestaña **Buzón vinculado** en las propiedades del usuario seleccionado.

Crear un buzón de archivo vinculado

Puede crear un buzón de archivo vinculado a partir de un usuario seleccionado que tenga un buzón vinculado.

Suprimir un buzón de archivo vinculado

Puede suprimir un buzón de archivo vinculado de la barra de herramientas de un usuario seleccionado que tenga un buzón de archivo vinculado.

Restaurar un buzón vinculado suprimido

Puede restaurar un buzón vinculado que se haya suprimido si se ha habilitado la Papelera de ese dominio.

4.6 Tareas de gestión de carpetas públicas

Si el administrador de DRA ha creado bosques de carpetas públicas en la empresa gestionada por DRA y le ha otorgado poderes para gestionar las carpetas públicas en DRA, podrá crear carpetas públicas, modificar sus propiedades y generar informes de historial de cambios. La creación y la modificación de carpetas públicas solo se pueden realizar en la consola Web. Puede ejecutar las tareas de Carpeta pública en **Gestión** > pestaña **Carpetas públicas**.

Crear una carpeta pública

Puede crear nuevas carpetas públicas en los dominios, los subárboles y los buzones de Carpeta pública mediante la consola Web. Puede utilizar el buzón por defecto del dominio seleccionado o elegir uno.

Habilitar el correo electrónico para una carpeta pública

Puede habilitar el correo electrónico para una carpeta pública mediante la opción **Habilitar correo** de la barra de herramientas de lista. Esto le permite asociar direcciones de correo electrónico a la carpeta pública y modificar las propiedades de la carpeta pública.

Inhabilitar el correo electrónico para una carpeta pública

Puede inhabilitar el correo electrónico para una carpeta pública mediante la opción **Inhabilitar correo** de la barra de herramientas de lista.

Modificar las propiedades de las carpetas públicas

Después de habilitar el correo en una carpeta pública existente, puede ver las estadísticas de la carpeta y modificar las propiedades de esa carpeta pública. En estas propiedades, puede especificar opciones de entrega y restricciones para el usuario, límites de tamaño y avisos de cuotas, propiedades de correo, límites de antigüedad del almacenamiento, inclusión de moderadores para aprobar correo y atributos personalizados.

Nota: También puede actualizar algunas propiedades para varias carpetas públicas cuando se selecciona más de una, como las cuotas de almacenamiento.

Suprimir una carpeta pública

Puede suprimir las carpetas públicas si no tienen ninguna subcarpeta y la opción de correo electrónico está inhabilitada.

5 Gestión de recursos

DRA le permite administrar recursos, entre los que se incluyen equipos, impresoras y otros dispositivos, así como procesos asociados a estos recursos. Por ejemplo, si necesita iniciar un servicio específico en un equipo gestionado, puede buscar ese objeto de equipo en DRA, acceder a sus servicios a través de las propiedades del objeto y, a continuación, reiniciar un servicio específico en ese equipo desde DRA sin tener que acceder de forma remota a ese equipo.

5.1 Gestión de unidades administrativas

En esta sección, se le guiará por el proceso de gestión de unidades administrativas en la consola de gestión de cuentas y recursos. Con los poderes adecuados, puede realizar diversas tareas de gestión de unidades administrativas, como desplazar una unidad administrativa a otro contenedor.

Modificación de las propiedades de las unidades administrativas

Puede modificar las propiedades de las unidades administrativas. Los poderes de los que disponga determinarán las propiedades que puede modificar para una unidad administrativa en el dominio o el subárbol gestionados.

Creación de unidades administrativas

Puede crear unidades administrativas en el dominio o el subárbol gestionados. También puede modificar las propiedades generales como, por ejemplo, la descripción de la unidad administrativa.

Clonación de unidades administrativas

Puede crear una nueva unidad administrativa mediante la clonación de una existente desde el dominio o el subárbol gestionados. También puede modificar las propiedades generales de una unidad administrativa como, por ejemplo, su descripción. Al clonar una unidad administrativa, no se clonan los objetos incluidos en ella.

Apertura del árbol de Active Directory en una ubicación de una unidad administrativa

Puede abrir de forma rápida y fácil el árbol de Active Directory en la ubicación de una unidad administrativa específica en el dominio o el subárbol gestionados.

Desplazamiento de una unidad administrativa a otro contenedor

Puede desplazar una unidad administrativa a un contenedor diferente del dominio gestionado. Al gestionar un subárbol de un dominio, puede desplazar las unidades administrativas incluidas en la jerarquía de ese subárbol.

Nota

- ♦ Si el desplazamiento de una unidad administrativa a otro contenedor aumenta sus poderes en esa unidad, DRA no le permitirá moverla.
 - ♦ También puede arrastrar una unidad administrativa a la nueva ubicación para desplazarla.
-

Supresión de unidades administrativas

Puede suprimir unidades administrativas en el dominio o el subárbol gestionados. Solo se pueden suprimir unidades administrativas vacías. Si una unidad administrativa contiene objetos, no se puede suprimir. Para suprimir una unidad administrativa que contenga objetos, suprima primero todos los objetos y, a continuación, elimine la unidad administrativa.

5.2 Gestión de equipos

DRA permite administrar equipos en el dominio o el subárbol gestionados. Por ejemplo, puede añadir o eliminar cuentas de equipo en los dominios gestionados, así como administrar los recursos de cada equipo. Al añadir un equipo a un dominio, DRA crea una cuenta de equipo en ese dominio para ese equipo. A continuación, puede conectar el equipo en ese dominio y configurarlo para que utilice esa cuenta de equipo. También puede ver y modificar las propiedades de las cuentas de equipo. DRA también permite apagar un equipo y sincronizar los controladores de dominio de un dominio gestionado.

Nota: No se pueden gestionar los controladores de dominio ocultos. La memoria caché de dominio no incluye los controladores de dominio ocultos. Por lo tanto, DRA no muestra equipos de dominio ocultos en listas o ventanas de propiedades.

Especificar la pertenencia a grupo de los equipos

Puede añadir o eliminar equipos en un grupo específico del dominio o el subárbol gestionados. También puede ver o modificar las propiedades de los grupos existentes a los que pertenece este equipo.

Gestionar las propiedades de la cuenta de equipo

Puede gestionar las propiedades de la cuenta de equipo. Los poderes de los que disponga determinarán las propiedades que puede modificar para un equipo en el dominio o el subárbol gestionados.

Añadir un equipo a un dominio

Puede añadir un equipo a un dominio o un subárbol gestionados mediante la creación de una nueva cuenta de equipo.

Eliminar un equipo de un dominio

Puede eliminar un equipo de un dominio o un subárbol gestionados mediante la eliminación de la cuenta de equipo.

Mover un equipo

Puede mover un equipo a otro contenedor, como una unidad administrativa, en el dominio o el subárbol gestionados.

Apagar o reiniciar un equipo

Puede apagar y reiniciar el equipo inmediatamente o en la fecha y hora definidas.

Restablecer la contraseña de la cuenta de administrador

Para restablecer la contraseña de la cuenta de administrador de un equipo, debe disponer del poder para restablecer una contraseña para el administrador local o estar asociado a una función que contenga este poder. Puede restablecer la contraseña de administrador de los servidores miembros en el dominio o el subárbol gestionados. No se puede restablecer la contraseña de administrador de un controlador de dominio.

Restablecer la cuenta de equipo

Puede restablecer la cuenta de equipo de los servidores miembros en el dominio o el subárbol gestionados. No se puede restablecer la cuenta de equipo de un controlador de dominio.

Suprimir una cuenta de equipo

Puede suprimir una cuenta de equipo en el dominio o el subárbol gestionados. Si va a administrar un dominio de Microsoft Windows, puede suprimir las cuentas de equipo que contengan otros objetos como, por ejemplo, un recurso compartido. Si se ha inhabilitado la Papelera para ese dominio, al suprimir una cuenta de equipo, esta se elimina de forma permanente de Active Directory. Si se ha habilitado la Papelera para ese dominio, al suprimir una cuenta de equipo, esta se transfiere a la Papelera.

Nota: No se pueden eliminar las cuentas de equipo de los servidores miembros en el dominio o el subárbol gestionados.

Inhabilitar una cuenta de equipo

Puede inhabilitar una cuenta de equipo en el dominio o el subárbol gestionados. Al inhabilitar una cuenta de equipo, se impide que los usuarios entren a la sesión en cualquier dominio.

Habilitar una cuenta de equipo

Puede habilitar una cuenta de equipo en el dominio o el subárbol gestionados. Al habilitar una cuenta de equipo, los usuarios pueden entrar a la sesión en cualquier dominio.

Gestionar los recursos de equipo

En cada cuenta de equipo del dominio o el subárbol gestionados, puede gestionar los recursos asociados, como servicios, recursos compartidos, dispositivos, impresoras y tareas de impresión.

5.3 Gestión de servicios

Un servicio es un tipo de aplicación que recibe un tratamiento especial en el sistema operativo Windows. Los servicios se pueden ejecutar, incluso aunque ningún usuario haya entrado a la sesión en un equipo. DRA habilita a los administradores asistentes (AA) con los poderes adecuados para gestionar servicios a través de la consola de gestión de cuentas y recursos.

Gestionar las propiedades de los servicios

Puede gestionar las propiedades de los servicios que se ejecutan en equipos del dominio o el subárbol gestionados. Puede gestionar los servicios mientras se administran otros recursos de ese equipo.

Iniciar un servicio

Puede iniciar un servicio en cualquier equipo del dominio o el subárbol gestionados.

Iniciar un servicio con parámetros

Al iniciar servicios que aceptan parámetros, puede especificar estos parámetros durante el inicio. Puede iniciar servicios en los equipos del dominio o el subárbol gestionados.

Especificar un tipo de inicio de servicio

Puede cambiar el tipo de inicio de un servicio como, por ejemplo, solicitar un inicio manual.

Especificar una cuenta de entrada a la sesión del servicio

Puede cambiar la cuenta de entrada a la sesión del servicio a una cuenta distinta a la cuenta del sistema actual. Puede especificar las cuentas de entrada a la sesión de servicios que se ejecuten en equipos del dominio o el subárbol gestionados. Puede especificar la cuenta del sistema local o una cuenta de usuario específica.

Reiniciar un servicio

Puede reiniciar un servicio que se ejecute en un equipo del dominio o el subárbol gestionados.

Para reiniciar un servicio, debe tener los poderes para detener o iniciar un servicio o estar asociado a un función que contenga estos poderes como, por ejemplo, la función Iniciar y detener servicio.

Detener un servicio

Puede detener un servicio que se ejecute en un equipo del dominio o el subárbol gestionados.

Pausar un servicio

Puede pausar un servicio que se ejecute en un equipo del dominio o el subárbol gestionados. La capacidad de pausar o no un servicio depende del tipo de servicio. Por ejemplo, es posible que no pueda pausar un servicio que tenga servicios dependientes.

Reanudar un servicio en pausa

Puede reanudar un servicio que se haya pausado en un equipo del dominio o el subárbol gestionados.

5.4 Gestión de impresoras y tareas de impresión

Para gestionar impresoras, administre las colas de impresión que dan servicio a esas impresoras. DRA permite pausar o reanudar, iniciar, modificar, detener y ver impresoras de recursos y publicadas. DRA también le permite modificar las propiedades y las prioridades de las tareas de impresión. Para añadir o suprimir una impresora, utilice las herramientas nativas de Windows.

Un servidor de impresión es un equipo en el que se instalan una o varias impresoras lógicas. Una impresora lógica se define en el equipo que contiene el controlador de dispositivo de la impresora. Una impresora lógica incluye el controlador de impresión, la cola de impresión y los puertos para una impresora. El servidor de impresión asocia impresoras lógicas a dispositivos de impresora.

Una impresora conectada se define en los equipos en los que seleccionan los documentos para imprimirse. Una impresora conectada es una conexión a un recurso compartido de impresión en la red. Por lo tanto, puede gestionar impresoras y tareas de impresión a través de los equipos asociados.

Una impresora publicada es una impresora que se ha publicado en Active Directory. Una impresora publicada puede ser una impresora de red que no esté conectada directamente a un servidor o una impresora alojada por un servidor de clúster.

5.4.1 Tareas de gestión de impresoras

Puede gestionar impresoras asociadas a equipos del dominio o el subárbol gestionados. DRA permite gestionar impresoras mientras se administran otros recursos de ese equipo.

En esta sección, se le guiará por el proceso de administración de impresoras en la consola de gestión de cuentas y recursos. Con los poderes adecuados, puede realizar varias tareas de administración de impresoras, como detener una impresora.

Gestionar las propiedades de las impresoras

Puede gestionar las propiedades de las impresoras en el dominio o el subárbol gestionados. DRA permite gestionar impresoras mientras se administran otros recursos de ese equipo.

Pausar una impresora

Puede pausar una impresora asociada a un equipo del dominio o el subárbol gestionados. DRA permite gestionar impresoras mientras se administran otros recursos de ese equipo.

Reanudar una impresora

Puede reanudar una impresora asociada a un equipo del dominio o el subárbol gestionados. DRA permite gestionar impresoras mientras se administran otros recursos de ese equipo.

5.4.2 Gestión de tareas de impresión

Puede gestionar las tareas de impresión asociadas a las impresoras del dominio o el subárbol gestionados. Como las tareas de impresión están asociadas a una impresora, puede gestionarlas mientras administra la impresora.

En esta sección, se le guiará por el proceso de gestión de tareas de impresión en la consola de gestión de cuentas y recursos. Con los poderes adecuados, puede realizar diversas tareas de gestión de tareas de impresión, como cancelar una tarea de impresión.

Gestionar las propiedades de las tareas de impresión

Puede modificar las propiedades de las tareas de impresión como parte del flujo de trabajo de gestión de la impresora. Debido a que las tareas de impresión están asociadas a impresoras, puede modificarlas mientras gestiona la impresora correspondiente. Las propiedades de tareas de impresión que puede modificar dependen del tipo de poder del que disponga. Para modificar las propiedades de las tareas de impresión, debe poder acceder a la impresora y el equipo correspondientes.

Pausar una tarea de impresión

Puede pausar una tarea de impresión en una impresora del dominio o el subárbol gestionados. Para pausar una tarea de impresión, debe poder acceder a la impresora y el equipo correspondientes. Al pausar una tarea de impresión, esta no se suprime de la cola de impresión.

Reanudar una tarea de impresión

Puede reanudar una tarea de impresión que se haya pausado. Para reanudar una tarea de impresión, debe poder acceder a la impresora y el equipo correspondientes.

Reiniciar una tarea de impresión

Puede iniciar una tarea de impresión que se haya detenido. Para reiniciar una tarea de impresión, debe poder acceder a la impresora y el equipo correspondientes.

Cancelar una tarea de impresión

Puede cancelar una tarea de impresión que se encuentre en la cola de impresión. Al cancelar una tarea de impresión, DRA la suprime de forma permanente de la cola de la impresora. Para cancelar una tarea de impresión, debe poder acceder a la impresora y el equipo correspondientes.

5.4.3 Tareas de gestión de impresoras publicadas

Puede gestionar las impresoras publicadas en el dominio o el subárbol gestionados. Puede añadir o buscar cualquier impresora que se haya publicado en Active Directory o impresoras que se hayan alojado en un servidor de clúster.

En esta sección, se le guiará por el proceso de administración de impresoras publicadas en la consola de gestión de cuentas y recursos. Con los poderes adecuados, puede realizar varias tareas de administración de impresoras, como detener una impresora.

Gestionar las propiedades de las impresoras publicadas

Puede gestionar las propiedades de las impresoras publicadas en el dominio o el subárbol gestionados. DRA permite gestionar impresoras publicadas mientras se administran otros recursos.

Actualizar la información de la impresora publicada

Puede actualizar la información de la impresora publicada en el dominio o el subárbol gestionados. DRA permite gestionar impresoras publicadas mientras se administran otros recursos.

Pausar una impresora publicada

Puede pausar una impresora publicada en el dominio o el subárbol gestionados. DRA permite gestionar impresoras publicadas mientras se administran otros recursos.

Reanudar una impresora publicada

Puede reanudar una impresora publicada que se haya pausado en el dominio o el subárbol gestionados. DRA permite gestionar impresoras publicadas mientras se administran otros recursos.

Mover una impresora publicada

Puede mover una impresora publicada disponible en un contenedor del dominio gestionado a otro contenedor del mismo dominio. DRA permite gestionar impresoras publicadas mientras se administran otros recursos.

Cambiar el nombre de una impresora publicada

Puede cambiar el nombre de una impresora publicada compartida en Active Directory. DRA permite gestionar impresoras publicadas mientras se administran otros recursos.

Nota: Al cambiar el nombre de una impresora publicada en Active Directory, no se cambia el nombre del recurso compartido de la impresora de recursos ni se propaga el cambio de nombre a la impresora de recursos que desea gestionar. Por ejemplo, si el nombre de la impresora de recursos es Esmeralda y cambia el nombre de la impresora a Rubí en Active Directory, otros usuarios verán el nombre de la impresora como Rubí, pero el nombre de la impresora de recursos seguirá siendo Esmeralda.

5.4.4 Gestión de tareas de impresión de impresoras publicadas

Puede gestionar las tareas de impresora asociadas a las impresoras publicadas del dominio o el subárbol gestionados. Como las tareas de impresión están asociadas a una impresora, puede gestionarlas mientras administra la impresora publicada.

En esta sección, se le guiará por el proceso de administración de impresoras publicadas en la consola de gestión de cuentas y recursos. Con los poderes adecuados, puede realizar diversas tareas de gestión de tareas de impresión, como cancelar una tarea de impresión.

Gestionar las propiedades de las tareas de impresión

Puede modificar las propiedades de las tareas de impresión como parte del flujo de trabajo de gestión de la impresora publicada. Debido a que las tareas de impresión están asociadas a impresoras, puede modificarlas mientras gestiona la impresora publicada correspondiente. Las propiedades de tareas de impresión que puede modificar dependen del tipo de poder del que disponga. Para modificar las propiedades de las tareas de impresión, debe poder acceder a la impresora publicada correspondiente.

Pausar una tarea de impresión

Puede pausar una tarea de impresión en una impresora publicada del dominio o el subárbol gestionados. Para pausar una tarea de impresión, debe poder acceder a la impresora publicada correspondiente. Al pausar una tarea de impresión, esta no se suprime de la cola de impresión.

Reanudar una tarea de impresión

Puede reanudar una tarea de impresión que se haya pausado en un dominio o un subárbol gestionados. Para reanudar una tarea de impresión, debe poder acceder a la impresora publicada correspondiente.

Reiniciar una tarea de impresión

Puede reiniciar una tarea de impresión que se haya detenido en un dominio o un subárbol gestionados. Para reiniciar una tarea de impresión, debe poder acceder a la impresora publicada correspondiente.

Cancelar una tarea de impresión

Puede cancelar una tarea de impresión que se encuentre en la cola de impresión en un dominio o un subárbol gestionado. Al cancelar una tarea de impresión, DRA la suprime de forma permanente de la cola de la impresora. Para cancelar una tarea de impresión, debe poder acceder a la impresora publicada correspondiente.

5.5 Gestión de recursos compartidos

Un recurso compartido permite facilitar recursos como, por ejemplo, archivos o impresoras, a otros usuarios en la red. Cada recurso compartido presenta un nombre que hace referencia a una carpeta compartida en el servidor. DRA gestiona los recursos compartidos solo en los equipos de los dominios gestionados. Para gestionar correctamente los recursos compartidos, la cuenta de acceso debe tener permisos de administrador, como ser miembro del grupo de administradores locales, en todos los equipos en los que desee gestionar recursos. Para asignar estos permisos, añada la cuenta de acceso al grupo de administradores de dominio en modo nativo del dominio del equipo.

Gestionar las propiedades de los recursos compartidos

Puede gestionar las propiedades de los recursos compartidos en el dominio o el subárbol gestionados. DRA permite gestionar recursos compartidos mientras se administran otros recursos de ese equipo.

Crear un recurso compartido

Puede crear un recurso compartido para un equipo del dominio o el subárbol gestionados. También puede modificar las propiedades de ese recurso compartido.

Clonar un recurso compartido

Puede clonar un recurso compartido para un equipo del dominio o el subárbol gestionados. Al clonar un recurso compartido, puede crear rápidamente recursos compartidos basados en otros con propiedades similares. Esta flexibilidad permite aplicar una configuración coherente a todos los recursos compartidos que cree en un determinado dominio.

Al clonar un recurso compartido, DRA incluye los valores del recurso compartido seleccionado en el Asistente para clonar recursos compartidos. También puede modificar las propiedades del nuevo recurso compartido.

Suprimir un recurso compartido

Puede suprimir recursos compartidos de los equipos del dominio o el subárbol gestionados.

5.6 Gestión de usuarios conectados

Se establece una sesión cada vez que un usuario se conecta a un recurso específico en un equipo remoto. Un usuario conectado es un usuario que se ha conectado a un recurso compartido en la red.

DRA gestiona los usuarios conectados solo en los equipos de los dominios gestionados. La cuenta de acceso debe tener permisos de administrador, como ser miembro del grupo de administradores locales, en todos los equipos en los que desee gestionar usuarios conectados. Para asignar estos permisos, añada la cuenta de acceso al grupo de administradores de dominio en modo nativo del dominio del equipo.

Desconectar un usuario

Puede desconectar un usuario conectado desde un equipo del dominio o el subárbol gestionados. Debe poder acceder al equipo y a la sesión abierta. La desconexión de un usuario conectado finaliza la sesión abierta.

Actualizar la lista de usuarios conectados

Para asegurarse de que está viendo la información más reciente sobre las sesiones abiertas en un equipo, actualice manualmente la lista de usuarios conectados. Debe poder acceder al equipo y a la sesión abierta.

5.7 Gestión de dispositivos

Un dispositivo es cualquier equipo conectado a una red, como un equipo informático, una impresora, un módem o cualquier otro dispositivo periférico.

Aunque es posible que haya un dispositivo instalado en el equipo, Windows no podrá reconocer el dispositivo hasta que instale y configure el controlador adecuado. Un controlador de dispositivo habilita una parte del hardware para comunicarse con el sistema operativo.

DRA solo permite configurar y gestionar los dispositivos en los equipos de los dominios gestionados. La cuenta de acceso debe tener permisos de administrador, como ser miembro del grupo de administradores locales, en todos los equipos en los que desee gestionar dispositivos. Para asignar estos permisos, añada la cuenta de acceso al grupo de administradores de dominio en modo nativo del dominio del equipo.

Gestionar las propiedades de un dispositivo

Puede modificar las propiedades de un dispositivo en un equipo específico. La modificación de las propiedades de un dispositivo permite cambiar el tipo de inicio de un dispositivo.

Iniciar un dispositivo

Puede iniciar un dispositivo en un equipo específico del dominio o el subárbol gestionados.

Detener un dispositivo

Puede detener un dispositivo en un equipo específico del dominio o el subárbol gestionados.

5.8 Gestión de registros de eventos

Un evento es un suceso importante de un sistema o una aplicación. El sistema operativo Windows registra información sobre eventos en archivos de registro de eventos. Puede haber varios registros de eventos almacenados en cada equipo. Utilice el visor de eventos nativo de Windows para ver los registros de eventos. DRA gestiona los registros de eventos solo en los equipos de los dominios gestionados.

DRA incluye las operaciones iniciadas por el usuario en el archivo de registro, un repositorio seguro. Tiene la opción de conseguir que DRA incluya también las operaciones iniciadas por el usuario en el registro de eventos de Windows, además de incluir la información en el archivo de registro de DRA. Para obtener más información, consulte [Descripción de las fechas y las horas](#).

5.8.1 Tipos de registros de eventos

Los equipos con Microsoft Windows incluyen información adicional en diversos registros. Los registros se describen brevemente a continuación:

Tipo de registro	Descripción
ADAM	Registra los eventos registrados por el repositorio de ADAM.
Aplicación	Registra los eventos registrados por una aplicación en el equipo, como el inicio o un error de un servicio. Por ejemplo, DRA almacena eventos en el registro de la aplicación.
Servicio de directorio	Registra eventos relacionados con los controladores de dominio que mantienen la base de datos de seguridad.
Servicio de réplica de archivos	Registra eventos relacionados con los servicios de réplica de archivos proporcionados por el sistema operativo.
Seguridad	Registra eventos que incluyen intentos de entrada a la sesión, acceso a archivos y directorios, y cambios en la directiva de seguridad que se basan en las opciones de la directiva de auditoría.
Sistema	Registra los eventos registrados por los componentes del sistema de Windows, como el error de un controlador o servicios que se inician y se detienen.

5.8.2 Tareas de gestión del registro de eventos

Puede especificar el tamaño máximo de un archivo de registro de eventos y lo que sucede con un registro de eventos cuando se llena. En la ventana de propiedades, también se muestra el nombre del registro, la vía del archivo de registro y el nombre del archivo, cuándo se creó el registro, cuándo

se modificó por última vez y cuándo se accedió a él por última vez. Si opta por realizar una copia de seguridad del archivo de registro, DRA guarda el registro de eventos con un nombre de archivo exclusivo en una ubicación estándar del equipo seleccionado.

DRA permite gestionar los registros de eventos mientras se administran otros recursos de ese equipo. Con los poderes adecuados, puede realizar diversas tareas de gestión de recursos compartidos, como cambiar las propiedades del registro de eventos.

Habilitar e inhabilitar la auditoría del registro de eventos de Windows para DRA

Al instalar DRA, los eventos de auditoría no se registran por defecto en el registro de eventos de Windows. Puede habilitar este tipo de registro mediante la modificación de una clave de registro.

Advertencia: Tenga cuidado al editar el Registro de Windows. Si se produce un error en el Registro, es posible que el equipo deje de funcionar. Si se produce un error, puede restaurar el Registro al estado que presentaba la última vez que inició correctamente el equipo. Para obtener más información, consulte la ayuda del editor del Registro de Windows.

Gestionar las propiedades del registro de eventos

Puede modificar las propiedades del registro de eventos para un equipo específico.

Visualizar las entradas del registro de eventos

Puede ver las entradas de un registro de eventos específico para un equipo del dominio o el subárbol gestionados. Al ver un registro de eventos, DRA lanzará el visor de eventos nativo de Windows.

Borrar el registro de eventos

Puede borrar las entradas de un registro de eventos específico para un equipo del dominio o el subárbol gestionados. También puede guardar las entradas del registro de eventos antes de borrarlo.

5.9 Gestión de archivos abiertos

Un archivo abierto es una conexión a recursos compartidos, como archivos o conductos. Un conducto es un mecanismo de comunicación entre procesos que permite que un proceso se comunique con otro proceso local o remoto.

DRA gestiona los archivos abiertos solo en los equipos del dominio y el subárbol gestionados. Como los archivos abiertos están asociados a un equipo, puede gestionarlos mientras administra otros recursos de ese equipo. Por ejemplo, es posible que desee cerrar los archivos abiertos al cerrar un sistema, o instalar un nuevo dispositivo o servicio. También puede supervisar los archivos a los que acceden los usuarios con más frecuencia, lo que le ayudará a evaluar de forma más eficaz la seguridad.

Cerrar un archivo

Puede cerrar archivos abiertos desde recursos de la red. Es recomendable enviar una notificación a los usuarios cuando se tenga intención de cerrar archivos abiertos. Es posible que necesiten tiempo para guardar los datos. Para cerrar un archivo abierto, debe poder acceder al equipo correspondiente.

Actualizar la lista de archivos abiertos

Para asegurarse de que está viendo la información más reciente sobre las sesiones abiertas en un equipo, actualice manualmente la lista de usuarios conectados. Para actualizar la lista de archivos abiertos, debe poder acceder al equipo correspondiente.

6 Gestión de consultas avanzadas

La función de búsqueda normal de DRA permite buscar atributos de objetos en Active Directory, como usuarios, equipos, impresoras, grupos y unidades administrativas. También permite especificar búsquedas con caracteres comodín. Sin embargo, no puede utilizar la función de búsqueda de DRA para buscar atributos personalizados, como el estado de bloqueo o caducidad de la cuenta. Las consultas de búsqueda avanzadas permiten realizar búsquedas mediante atributos personalizados que no están disponibles en la función de búsqueda de DRA. DRA utiliza LDAP para admitir la función de consultas avanzadas. Puede utilizar consultas avanzadas para buscar usuarios, contactos, grupos, equipos, impresoras, unidades administrativas y cualquier otro objeto compatible con DRA.

Crear una nueva consulta avanzada

Puede crear una consulta avanzada en el servidor de administración principal o secundario. También puede modificar las propiedades de la nueva consulta avanzada como, por ejemplo, la cadena de consulta.

Modificar una consulta avanzada

Solo puede cambiar determinadas propiedades de una consulta avanzada guardada en Consultas públicas si dispone de los permisos necesarios para modificar consultas avanzadas compartidas. Puede modificar las propiedades de todas las consultas que guarde en Mis consultas.

Copiar una consulta avanzada

Puede copiar consultas avanzadas entre Consultas públicas y Mis consultas. Al copiar una consulta avanzada en Consultas públicas, los administradores asistentes que dispongan de los poderes necesarios podrán modificar y ejecutar la consulta avanzada.

Personalizar los resultados de la consulta avanzada

DRA proporciona un conjunto por defecto de columnas en la lista de resultados de la búsqueda. Para personalizar los resultados de la búsqueda, puede añadir o eliminar columnas en la lista de resultados de la búsqueda. Puede personalizar los resultados de la búsqueda al crear una nueva consulta avanzada o modificar una existente.

Importar una consulta avanzada

Puede importar las consultas avanzadas que cree en ADUC en lugar de crear de nuevo estas consultas mediante DRA. Solo se pueden importar consultas avanzadas que presenten el formato XML.

Exportar una consulta avanzada

Puede exportar las consultas avanzadas que cree en DRA en lugar de crear de nuevo estas consultas mediante ADUC.

Suprimir una consulta avanzada

Solo puede suprimir las consultas avanzadas de Consultas públicas si dispone de los permisos necesarios para suprimir consultas avanzadas compartidas. Puede suprimir cualquier consulta avanzada que se encuentre en Mis consultas.

7 Gestionar la Papelera

La Papelera proporciona una red de seguridad, ya que permite suprimir de forma temporal cuentas, grupos, contactos y cuentas de equipo. Puede restaurar a continuación esos objetos como, por ejemplo, SID, ACL y pertenencias a grupos, a su estado original con todos los datos intactos o eliminarlos de forma permanente. Esta flexibilidad proporciona un método más seguro de gestionar cuentas de usuario, grupos, contactos y cuentas de equipo.

Restaurar un objeto de la Papelera

Puede restaurar objetos eliminados para devolverlos a los contenedores desde los que se han suprimido. DRA restaura estos objetos a su estado original con todos los datos intactos, como SID, ACL y pertenencias a grupos. Un objeto puede ser una cuenta de usuario, un grupo, un contacto, un grupo dinámico, un buzón de recursos, un grupo dinámico de distribución o una cuenta de equipo.

Restaurar todos los objetos

Puede restaurar todos los objetos de la Papelera de un dominio gestionado. Puede restaurar los objetos de la Papelera en un dominio específico o en todos los dominios gestionados. Para restaurar objetos de una Papelera de un dominio específico, esta debe habilitarse para ese dominio.

Suprimir un objeto de la Papelera

Puede eliminar de forma permanente los objetos de la Papelera de un dominio gestionado. Una vez suprimido un objeto de la Papelera, este no se puede restaurar. Un objeto puede ser una cuenta de usuario, un grupo, un contacto, un grupo dinámico, un buzón de recursos, un grupo dinámico de distribución o una cuenta de equipo.

Vaciar la Papelera

Puede vaciar la Papelera de un dominio gestionado. Al vaciar la Papelera, se suprimen de forma permanente todos los objetos incluidos en ella. Puede vaciar la Papelera en un dominio específico o en todos los dominios gestionados. Para vaciar una Papelera de un dominio específico, esta debe habilitarse para ese dominio. Una vez vaciada la Papelera, no se pueden restaurar los objetos suprimidos.

A

Uso de la consola Web heredada

La consola Web heredada, que se ha sustituido por una consola Web más reciente con el lanzamiento de DRA 9.0.1, aún se puede utilizar. Consulte la sección [Instalar el servidor de administración de DRA](#) de la *Guía del administrador de Directory and Resource Administrator* para obtener información sobre cómo instalar esta versión de la consola Web.

La consola Web heredada es una interfaz de usuario basada en Web que proporciona acceso rápido y fácil a muchas tareas de cuentas de usuario, grupos, equipos, recursos y buzones de Microsoft Exchange. También puede gestionar las propiedades generales de su propia cuenta de usuario, como la dirección o el número de teléfono móvil.

El uso de la consola Web heredada es sencillo y fácil de aprender, lo que la convierte en una excelente herramienta para administradores ocasionales o principiantes. La consola Web proporciona ayuda paso a paso que le guiará a través de cada tarea. Al completar una tarea, se muestran enlaces a otras tareas relacionadas para que pueda llevar a cabo rápidamente un flujo de trabajo completo. En la consola Web, solo se muestra una tarea si tiene el poder para realizarla.

A.1 Inicio de la consola Web heredada

Puede iniciar la consola Web desde cualquier equipo que ejecute Internet Explorer. Para iniciar la consola Web, especifique la dirección URL adecuada en el campo de dirección del navegador Web o utilice el enlace proporcionado en la consola de cuentas y recursos. Por ejemplo, si ha instalado el componente Web en el equipo HOUserver, escriba `http://HOUserver/dra` en el campo de dirección del navegador Web.

Nota: Para visualizar la información más actual de la cuenta y Microsoft Exchange en la consola Web, configure el navegador Web para que busque las versiones más recientes de las páginas almacenadas en caché en cada visita.

A.2 Uso del inicio rápido para resolver problemas

El inicio rápido le permite resolver rápida y fácilmente los problemas de la cuenta. Puede ver las propiedades y las estadísticas vitales de una cuenta de usuario, un equipo o un grupo específicos. A continuación, puede utilizar un enlace a la tarea adecuada como, por ejemplo, restablecer la contraseña de una cuenta de usuario, lo que soluciona el problema.

A.3 Personalización de la consola Web heredada

Puede personalizar de forma rápida y fácil la consola Web de las siguientes formas:

Modificar las tareas proporcionadas

Por ejemplo, puede modificar la tarea de actualización de las propiedades del usuario para incluir un nuevo campo que gestione un ajuste de propietario. Puede ocultar tareas específicas que no desea que los administradores asistentes (AA) utilicen independientemente de los poderes delegados de los que dispongan. También puede publicar informes generados desde el módulo de elaboración de informes de directorios y recursos.

Desarrollar nuevas tareas

Por ejemplo, puede desarrollar una nueva tarea de actualización de propiedades del usuario que satisfaga sus necesidades de administración exclusivas. Puede sustituir las tareas proporcionadas por tareas personalizadas sin perder las funciones integradas.

Modificar flujos de trabajo

Por ejemplo, puede cambiar el marco de la consola Web y la navegación por ella mediante la modificación de la forma en que los administradores asistentes se desplazan por una tarea específica. Esta flexibilidad le permite añadir, eliminar o mover pasos para crear la solución exacta que necesita.

Implantar varias aplicaciones de la consola Web

Puede instalar y configurar varias aplicaciones de la consola Web. Por ejemplo, puede implantar una aplicación personalizada de la consola Web para las instalaciones de Houston y otra para las instalaciones de Atlanta. Cada aplicación puede admitir un conjunto exclusivo de tareas que satisfagan las necesidades específicas de sus instalaciones. Para obtener más información, consulte "Deploying DRA" (Implantación de DRA) en "Unique Environments Technical Reference" (Referencia técnica de entornos exclusivos). Para obtener más información acerca de la personalización de la consola Web, consulte Resource Administrator Software Development Kit (Kit para desarrolladores de software de Directory and Resource Administrator).