
Directory and Resource Administrator

Guía del administrador

Julio 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	7
----------------------------	----------

1 Primeros pasos	9
-------------------------	----------

1.1 ¿Qué es Directory and Resource Administrator?	9
1.2 Descripción de los componentes de Directory and Resource Administrator	10
1.2.1 Servidor de administración de DRA	10
1.2.2 Consola de delegación y configuración	11
1.2.3 Consola de gestión de cuentas y recursos	11
1.2.4 Consola Web	11
1.2.5 Componentes de elaboración de informes	12
1.2.6 Motor de flujo de trabajo	12
1.2.7 Arquitectura del producto	13

2 Instalación y actualización del producto	15
---	-----------

2.1 Planificación de la implantación	15
2.1.1 Recomendaciones de recursos probadas	15
2.1.2 Provisión de recursos del entorno virtual	15
2.1.3 Puertos y protocolos necesarios	16
2.1.4 Plataformas compatibles	19
2.1.5 Requisitos del servidor de administración de DRA	20
2.1.6 Requisitos de la consola Web y las extensiones de DRA	24
2.1.7 Requisitos de elaboración de informes	25
2.1.8 Requisitos de licencias	26
2.2 Instalación del producto	26
2.2.1 Instalación del servidor de administración de DRA	27
2.2.2 Instalar clientes de DRA	28
2.2.3 Instalar las extensiones REST de DRA	29
2.2.4 Instalación del servidor de flujo de trabajo	30
2.2.5 Instalación del módulo de elaboración de informes de DRA	30
2.3 Actualización del producto	31
2.3.1 Planificación de una actualización de DRA	31
2.3.2 Tareas previas a la actualización	32
2.3.3 Actualización del servidor de administración de DRA	35
2.3.4 Actualizar las extensiones REST de DRA	38
2.3.5 Actualizar el módulo de elaboración de informes	39

3 Configuración de los componentes y el proceso	41
--	-----------

3.1 Configuración inicial	41
3.1.1 Lista de verificación de configuración	41
3.1.2 Instalación o actualización de licencias	41
3.1.3 Configurar los servidores y las funciones de DRA	42
3.1.4 Configurar el cliente de delegación y configuración	57
3.1.5 Configurar el cliente Web	57
3.2 Conexión de sistemas gestionados	66
3.2.1 Gestión de dominios de Active Directory	66
3.2.2 Conexión de carpetas públicas	69
3.2.3 Habilitación de la compatibilidad con Microsoft Exchange	71
3.2.4 Habilitación de Exchange Online y Skype Empresarial Online	72
3.2.5 Adición de un inquilino de Office 365	72

4 Modelo de delegación	75
-------------------------------	-----------

4.1 Descripción del modelo de delegación dinámica	75
4.1.1 Controles del modelo de delegación	75
4.1.2 Cómo procesa DRA las peticiones	76

4.1.3	Ejemplos de cómo DRA procesa las asignaciones de delegación	76
4.2	ActiveViews	79
4.2.1	ActiveViews integradas	80
4.2.2	Implementación de una ActiveView personalizada	81
4.3	Funciones	83
4.3.1	Funciones integradas	83
4.3.2	Creación de funciones personalizadas	91
4.4	Poderes	92
4.4.1	Poderes integrados	92
4.4.2	Implementación de poderes personalizados	92
4.4.3	Ampliación de poderes	93
4.5	Asignaciones de delegación	94

5 Automatización de directivas y procesos **95**

5.1	Descripción de la directiva de DRA	95
5.1.1	Cómo aplica las directivas el servidor de administración	95
5.1.2	Directiva integrada	96
5.1.3	Implementación de directivas personalizadas	99
5.1.4	Restricción de grupos de seguridad integrados nativos	100
5.1.5	Gestión de directivas	102
5.1.6	Directiva del cliente de delegación y configuración	112
5.2	Automatización de los activadores anteriores y posteriores a las tareas	114
5.2.1	Cómo automatiza los procesos el servidor de administración	115
5.2.2	Implementación de un activador de automatización	115
5.3	Flujo de trabajo automatizado	116

6 Auditoría y elaboración de informes **119**

6.1	Auditoría de actividad	119
6.1.1	Registro de eventos de Windows nativo	119
6.1.2	Descripción de los archivos de registro	121
6.2	Elaboración de informes	123
6.2.1	Gestión de la recopilación de datos para la elaboración de informes	124
6.2.2	Informes integrados	125

7 Funciones adicionales **129**

7.1	Asignaciones temporales de grupos	129
7.2	Grupos dinámicos de DRA	130
7.3	Funcionamiento de la adición de marcas a eventos	130
7.3.1	El evento de DS AD	131
7.3.2	Operaciones admitidas	131
7.4	Contraseña de recuperación de BitLocker	132
7.4.1	Visualización y copia de una contraseña de recuperación de BitLocker	132
7.4.2	Búsqueda de una contraseña de recuperación	133
7.5	Analizador de ActiveView	133
7.5.1	Inicio de una recopilación de datos de ActiveView	133
7.5.2	Generación de un informe del analizador	134
7.5.3	Limpieza de los datos analizados	134
7.6	Papelera	134
7.6.1	Asignación de poderes de la Papelera	135
7.6.2	Uso de la Papelera	135

8 Personalización de clientes **137**

8.1	Cientes de delegación y configuración, y de gestión de cuentas y recursos	137
-----	---	-----

8.1.1	Personalización de las páginas de propiedades	137
8.1.2	Herramientas personalizadas	144
8.1.3	Personalización de la interfaz de usuario	146
8.2	Cliente Web	147
8.2.1	Personalización de las páginas de propiedades	147
8.2.2	Personalización de formularios de flujo de trabajo	149
8.2.3	Personalización de la marca de la interfaz de usuario	151

9 Herramientas y utilidades 153

9.1	Utilidad de diagnóstico	153
9.2	Utilidad Objetos suprimidos	153
9.2.1	Permisos necesarios para la utilidad Objetos suprimidos	154
9.2.2	Sintaxis de la utilidad Objetos suprimidos	154
9.2.3	Opciones de la utilidad Objetos suprimidos.	154
9.2.4	Ejemplos de la utilidad Objetos suprimidos.	155
9.3	Utilidad de comprobación de estado	155
9.4	Utilidad Papelera	156
9.4.1	Permisos necesarios para la utilidad Papelera	157
9.4.2	Sintaxis de la utilidad Papelera	157
9.4.3	Opciones de la utilidad Papelera	157
9.4.4	Ejemplos de la utilidad Papelera	157

Acerca de esta guía

La *Guía del administrador* proporciona información conceptual sobre el producto Directory and Resource Administrator (DRA). Este manual define la terminología y diversos conceptos relacionados. También proporciona una guía paso a paso para un gran número de tareas de configuración y operativas.

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 instalar y configurar todos los componentes de 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 el catálogo de productos.

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 atención técnica.

DRA también amplía las potentes funciones de Microsoft Exchange para proporcionar una gestión sin problemas de objetos de Exchange. A través de una única interfaz de usuario común, DRA 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 de Aegis para 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)	Configuración de Reporting Center de DRA (NRC) CLI (<i>opcional</i>) Proveedor ADSI de DRA (<i>opcional</i>)	Servidor secundario
Administrador ocasional del servicio de Ayuda técnica	Consola de gestión de cuentas y recursos	Servidor secundario
Administrador ocasional del servicio de Ayuda técnica	Consola Web	Cualquier servidor de DRA con el servicio REST de DRA instalado

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 delegación y configuración

La consola de delegación y configuración es una interfaz de usuario que se puede instalar y que proporciona a los administradores del sistema acceso a las funciones de configuración y administración de DRA.

- ♦ **Gestión de delegación:** permite especificar y asignar de forma granular el acceso a las tareas y los recursos gestionados a los administradores asistentes.
- ♦ **Gestión de directivas y automatización:** permite definir y aplicar directivas para garantizar el cumplimiento de las normas y las convenciones del entorno.
- ♦ **Gestión de configuraciones:** permite actualizar la configuración y las opciones del sistema DRA, añadir personalizaciones y configurar servicios gestionados (Active Directory, Exchange, Office 365, etc.).

1.2.3 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.

1.2.4 Consola Web

La consola Web es una interfaz de usuario basada en Web que proporciona acceso rápido y fácil a los administradores asistentes 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 objeto personalizadas.

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...

1.2.5 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.

1.2.6 Motor de flujo de trabajo

DRA se integra con el motor de flujo de trabajo de Aegis 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 de flujo de trabajo personalizados y ver a continuación su estado. Para obtener más información sobre el motor de flujo de trabajo, consulte el [sitio de documentación de DRA \(https://www.netiq.com/documentation/directory-and-resource-administrator-92/\)](https://www.netiq.com/documentation/directory-and-resource-administrator-92/).

1.2.7 Arquitectura del producto



2 Instalación y actualización del producto

En este capítulo, se describen los requisitos recomendados de hardware, software y cuenta necesarios para Directory and Resource Administrator. A continuación, se le guiará por el proceso de instalación con una lista de comprobación para cada componente de la instalación.

2.1 Planificación de la implantación

Al planificar la implantación de Directory and Resource Administrator, utilice esta sección para evaluar la compatibilidad del hardware y el entorno, y anotar los puertos y los protocolos necesarios que deberá configurar para la implantación.

2.1.1 Recomendaciones de recursos probadas

En esta sección, se proporciona información de ajuste de tamaño para la recomendación básica de recursos. Los resultados pueden variar según el hardware disponible, el entorno específico, el tipo concreto de datos procesados y otros factores. Es probable que otras configuraciones de hardware de mayor dimensión y potencia puedan manejar una carga mayor. Si tiene alguna pregunta, póngase en contacto con los servicios de consultoría de NetIQ.

Se ejecuta en un entorno con aproximadamente un millón de objetos de Active Directory:

Componente	CPU	Memoria	Almacenamiento
Servidor de administración de DRA	4 CPU (x64)/núcleos a 2,0 GHz	16 GB	100 GB
Consola Web de DRA	2 CPU (x64)/núcleos a 2,0 GHz	8 GB	100 GB
Módulo de elaboración de informes de DRA	4 CPU (x64)/núcleos a 2,0 GHz	16 GB	100 GB
Servidor de flujo de trabajo de DRA	4 CPU (x64)/núcleos a 2,0 GHz	16 GB	100 GB

2.1.2 Provisión de recursos del entorno virtual

DRA mantiene activos grandes segmentos de memoria durante periodos prolongados. Durante la provisión de recursos para un entorno virtual, se deben tener en cuenta las siguientes recomendaciones:

- ♦ Asigne el almacenamiento como "Provisión pesada".
- ♦ Establezca la reserva de memoria en "Reserve All Guest Memory(All Locked)".
- ♦ Asegúrese de que el archivo de paginación sea lo suficientemente grande como para cubrir la posible reasignación de la memoria inflada en la capa virtual.

2.1.3 Puertos y protocolos necesarios

En esta sección, se indican los puertos y los protocolos de comunicación de DRA.

- ♦ Los puertos que se pueden configurar se indican con un asterisco (*).
- ♦ Los puertos que requieren un certificado se indican con dos asteriscos (**).

Servidores de administración de DRA

Protocolo y puerto	Dirección	Destino	Uso
TCP 135	Bidireccional	Servidores de administración de DRA	Asignador de puesto final, un requisito básico para la comunicación de DRA; permite que los servidores de administración se localicen entre sí en MMS.
TCP 445	Bidireccional	Servidores de administración de DRA	Réplica del modelo de delegación; réplica basada en archivos durante la sincronización MMS (SMB).
Intervalo de puertos TCP dinámicos*	Bidireccional	Controladores de dominio de Microsoft Active Directory	Por defecto, DRA asigna puertos de forma dinámica a partir del intervalo de puertos TCP 1024 a 65535. Sin embargo, puede configurar este intervalo mediante servicios de componentes. Para obtener más información, consulte la sección Uso de COM distribuido con el cortafuegos (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM).
TCP 50000 *	Bidireccional	Servidores de administración de DRA	Réplica de atributos y comunicación del servidor de DRA con ADAM. (LDAP)
TCP 50001 *	Bidireccional	Servidores de administración de DRA	Réplica de atributos SSL (ADAM).
TCP/UDP 389	Saliente	Controladores de dominio de Microsoft Active Directory	Gestión de objetos de Active Directory (LDAP).
	Saliente	Microsoft Exchange Server	Gestión de buzones (LDAP).
TCP/UDP 53	Saliente	Controladores de dominio de Microsoft Active Directory	Resolución de nombres
TCP/UDP 88	Saliente	Controladores de dominio de Microsoft Active Directory	Permite la autenticación desde el servidor de DRA en los controladores de dominio (Kerberos).
TCP 80	Saliente	Microsoft Exchange Server	Necesario para las versiones de Exchange server de 2010 a 2013 instaladas localmente (HTTP).
	Saliente	Microsoft Office 365	Acceso remoto a PowerShell (HTTP).
TCP 443	Saliente	Microsoft Office 365 y Change Guardian	Acceso de API gráfica e integración de Change Guardian (HTTPS).

Protocolo y puerto	Dirección	Destino	Uso
TCP 443, 5986 y 5985	Saliente	Microsoft PowerShell	cmdlets nativos de PowerShell (HTTPS) y acceso remoto a PowerShell.
TCP 8092 * **	Saliente	Servidor de flujo de trabajo	Activación y estado de flujo de trabajo (HTTPS).
TCP 50101 *	Entrante	Cliente de DRA	Haga clic con el botón derecho en el informe Historial de cambios para obtener un informe de auditoría de IU. Se puede configurar durante la instalación.
TCP 8989	Host local	Servicio de archivo de registro	Comunicación con el archivo de registro (no es necesario abrirlo a través del cortafuegos).
TCP 50102	Bidireccional	Servicio del núcleo de DRA	Servicio de archivo de registro
TCP 50103	Host local	Servicio de caché de DRA	Comunicación del servicio de caché en el servidor DRA (no necesita abrirlo a través del cortafuegos).
TCP 1433	Saliente	Microsoft SQL Server	Recopilación de datos de informes.
UDP 1434	Saliente	Microsoft SQL Server	El servicio de navegador de SQL Server utiliza este puerto para identificar el puerto de la instancia con nombre.
TCP 8443	Bidireccional	Servidor de Change Guardian	Historial de cambios unificado.

Servidor REST de DRA

Protocolo y puerto	Dirección	Destino	Uso
TCP 8755 * **	Entrante	Servidor IIS, cmdlets de PowerShell de DRA.	Ejecute las actividades de flujo de trabajo basadas en REST de DRA (ActivityBroker).
TCP 11192 * **	Saliente	Servicio de host de DRA	Para la comunicación entre el servicio REST de DRA y el servicio de administración de DRA.
TCP 135	Saliente	Controladores de dominio de Microsoft Active Directory	Detección automática mediante el punto de conexión de servicio (SCP).
TCP 443	Saliente	Controladores de dominio de Microsoft AD	Detección automática mediante el punto de conexión de servicio (SCP).

Consola Web (IIS)

Protocolo y puerto	Dirección	Destino	Uso
TCP 8755 * **	Saliente	Servicio REST de DRA	Para la comunicación entre la consola Web, PowerShell y el servicio de host de DRA.
TCP 443	Entrante	Navegador de cliente	Apertura del sitio Web de DRA.
TCP 443 **	Saliente	Servidor de Advanced Authentication	Advanced Authentication

Consola de delegación y administración de DRA

Protocolo y puerto	Dirección	Destino	Uso
TCP 135	Saliente	Controladores de dominio de Microsoft Active Directory	Detección automática mediante SCP.
Intervalo de puertos TCP dinámicos*	Saliente	Servidores de administración de DRA	Actividades de flujo de trabajo del adaptador de DRA. Por defecto, DCOM asigna puertos de forma dinámica a partir del intervalo de puertos TCP 1024 a 65535. Sin embargo, puede configurar este intervalo mediante servicios de componentes. Para obtener más información, consulte la sección Uso de COM distribuido con el cortafuegos (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM).
TCP 50102	Saliente	Servicio del núcleo de DRA	Creación de informes Historial de cambios.

Servidor de flujo de trabajo

Protocolo y puerto	Dirección	Destino	Uso
TCP 8755	Saliente	Servidores de administración de DRA	Ejecute las actividades de flujo de trabajo basadas en REST de DRA (ActivityBroker).
Intervalo de puertos TCP dinámicos*	Saliente	Servidores de administración de DRA	Actividades de flujo de trabajo del adaptador de DRA. Por defecto, DCOM asigna puertos de forma dinámica a partir del intervalo de puertos TCP 1024 a 65535. Sin embargo, puede configurar este intervalo mediante servicios de componentes. Para obtener más información, consulte la sección Uso de COM distribuido con el cortafuegos (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM).

Protocolo y puerto	Dirección	Destino	Uso
TCP 1433	Saliente	Microsoft SQL Server	Almacenamiento de datos de flujo de trabajo.
TCP 8091	Entrante	Consola de operaciones y consola de configuración.	API de BSL de flujo de trabajo (TCP).
TCP 8092 **	Entrante	Servidores de administración de DRA	API de BSL de flujo de trabajo (HTTP y HTTPS)
TCP 2219	Host local	Proveedor de espacio de nombres	Utilizado por el proveedor de espacio de nombres para ejecutar adaptadores.
TCP 9900	Host local	Correlation Engine	Utilizado por el motor de correlación para comunicarse con el motor de flujo de trabajo y el proveedor del espacio de nombres.
TCP 10117	Host local	Proveedor de espacio de nombres de gestión de recursos	Utilizado por el proveedor de espacio de nombres de gestión de recursos.

2.1.4 Plataformas compatibles

Para obtener la información más reciente acerca de las plataformas de software admitidas, consulte la página de Directory and Resource Administrator en el sitio Web de NetIQ: <https://www.netiq.com/support>

Sistema gestionado	Requisitos previos
Active Directory	<ul style="list-style-type: none"> ◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	<ul style="list-style-type: none"> ◆ Microsoft Exchange 2010 SP3 (excepto las carpetas públicas) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online
Microsoft Office 365	<ul style="list-style-type: none"> ◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ Módulo Windows Azure Active Directory para Windows PowerShell https://docs.microsoft.com/es-es/office365/enterprise/powershell/connect-to-office-365-powershell ◆ Skype Empresarial Online y Módulo de Windows PowerShell https://www.microsoft.com/es-es/download/details.aspx?id=39366
Skype Empresarial	<ul style="list-style-type: none"> ◆ Microsoft Skype Empresarial 2015
Historial de cambios	<ul style="list-style-type: none"> ◆ Change Guardian 5.0 y 5.1

Sistema gestionado	Requisitos previos
Navegadores Web	<ul style="list-style-type: none"> ◆ Microsoft Internet Explorer 11 y Microsoft Edge ◆ Google Chrome ◆ Mozilla Firefox
Automatización de flujos de trabajo	<ul style="list-style-type: none"> ◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2

2.1.5 Requisitos del servidor de administración de DRA

DRA presenta los siguientes requisitos del servidor para el software y las cuentas:

Requisitos de software

Componente	Requisitos previos
Destino de instalación	Sistema operativo de NetIQ Administration Server:
Sistema operativo	<ul style="list-style-type: none"> ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 2008 R2 se admite solo para la actualización. <p>Nota: El servidor también debe ser un miembro de un dominio nativo de Microsoft Windows Server admitido.</p> <p>Interfaces de DRA de Windows:</p> <ul style="list-style-type: none"> ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 8.1 (x86 y x64) y 10 (x86 y x64)
Instalador	<ul style="list-style-type: none"> ◆ Microsoft .NET Framework 4.5.2 y posterior

Componente	Requisitos previos
Servidor de administración	<p>Directory and Resource Administrator:</p> <ul style="list-style-type: none"> ◆ Microsoft .NET Framework 4.5.2 y posterior ◆ Uno de los siguientes: <ul style="list-style-type: none"> ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Packages (x64 y x86) ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages (x64 y x86) ◆ Microsoft Message Queuing ◆ Funciones de Active Directory Lightweight Directory Services de Microsoft ◆ Servicio de Registro remoto iniciado <p>Administración de Microsoft Office 365/Exchange Online:</p> <ul style="list-style-type: none"> ◆ Módulo Windows Azure Active Directory para Windows PowerShell ◆ Microsoft Online Services - Ayudante para el inicio de sesión para profesionales de TI ◆ Skype Empresarial Online y Módulo de Windows PowerShell <p>Para obtener más información, consulte Plataformas compatibles.</p>
Componentes Web heredados	<p>Servidor Web:</p> <ul style="list-style-type: none"> ◆ Versiones 8.0, 8.5 y 10 de Microsoft Internet Information Services (IIS) <p>Componentes de Microsoft IIS:</p> <ul style="list-style-type: none"> ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Servicio de funciones de seguridad de Microsoft IIS <p>Interfaces de DRA de Windows:</p> <ul style="list-style-type: none"> ◆ Microsoft .NET Framework 4.5.2 ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x86)

Requisitos de la cuenta

Cuenta	Descripción	Permisos
Grupo de AD LDS	La cuenta de servicio de DRA debe añadirse a este grupo para acceder a AD LDS.	◆ Grupo de seguridad local de dominio

Cuenta	Descripción	Permisos
Cuenta de servicio de DRA	Los permisos necesarios para ejecutar el servicio de administración de NetIQ.	<ul style="list-style-type: none"> ◆ Permisos de "Usuarios COM distribuidos". ◆ Miembro del grupo de administradores de AD LDS. ◆ Grupo de operadores de cuentas. ◆ Grupos de archivos de registro (OnePointOp ConfigAdms y OnePointOp). <p>Nota: Para obtener más información sobre cómo configurar las cuentas de acceso de dominio con privilegios mínimos, consulte: Cuentas de acceso de DRA con privilegios mínimos.</p>
Administrador de DRA	Cuenta de usuario o grupo configurada para la función integrada de administradores de DRA.	<ul style="list-style-type: none"> ◆ Grupo de seguridad local de dominio o cuenta de usuario de dominio. ◆ Miembro del dominio gestionado o un dominio de confianza. <ul style="list-style-type: none"> ◆ Si especifica una cuenta desde un dominio de confianza, asegúrese de que el equipo del servidor de administración pueda autenticar esta cuenta.
Cuentas de administrador asistente de DRA	Cuentas con competencias delegadas a través de DRA.	<ul style="list-style-type: none"> ◆ Añada todas las cuentas de administrador asistente de DRA al grupo "Usuarios COM distribuidos" para que puedan conectarse al servidor de DRA desde clientes remotos. <p>Nota: Se puede configurar DRA para gestionar esto durante la instalación.</p>

Cuentas de acceso de DRA con privilegios mínimos

A continuación, se muestran los permisos y los privilegios necesarios para las cuentas especificadas y los comandos de configuración que debe ejecutar.

Cuenta de acceso al dominio: Asigne los siguientes permisos de Active Directory a la cuenta de acceso al dominio:

- ◆ Control TOTAL de los objetos de dominio integrados
- ◆ Control TOTAL de los objetos de equipo
- ◆ Control TOTAL de los objetos de contacto
- ◆ Control TOTAL de los objetos de contenedor
- ◆ Control TOTAL de los grupos de distribución dinámica
- ◆ Control TOTAL de los objetos de grupo
- ◆ Control TOTAL de los objetos de Inetorgperson
- ◆ Control TOTAL de los objetos de MsExchSystemObjectContainer

- ♦ Control TOTAL de los objetos de unidad organizativa
- ♦ Control TOTAL de los objetos de impresora
- ♦ Control TOTAL de las carpetas públicas
- ♦ Control TOTAL de los objetos de usuario

Especifique los siguientes privilegios con un ámbito de "Este objeto y todos los objetos secundarios" en la cuenta de acceso al dominio:

- ♦ Permitir creación de objetos de equipo.
- ♦ Permitir creación de objetos de contacto.
- ♦ Permitir creación de contenedor.
- ♦ Permitir creación de objetos de grupo.
- ♦ Permitir creación de MsExchDynamicDistiributionList.
- ♦ Permitir creación de objetos de unidad organizativa.
- ♦ Permitir creación de carpetas públicas.
- ♦ Permitir creación de punto de conexión de servicio.
- ♦ Permitir creación de objetos de usuario.
- ♦ Permitir supresión de objetos de equipo.
- ♦ Permitir supresión de objetos de contacto.
- ♦ Permite supresión de contenedor.
- ♦ Permitir supresión de objetos de grupo.
- ♦ Permitir supresión de objetos de InetOrgPerson.
- ♦ Permitir supresión de MsExchDynamicDistiributionList.
- ♦ Permitir supresión de objetos de unidad organizativa.
- ♦ Permitir supresión de carpetas públicas.
- ♦ Permitir supresión de punto de conexión de servicio.
- ♦ Permitir supresión de objetos de usuario.

Cuenta de acceso de inquilino a Office 365: asigne los siguientes permisos de Active Directory a la cuenta de acceso de inquilino a Office 365:

- ♦ Administrador de gestión de usuarios de Office 365
- ♦ Gestión de destinatarios de Exchange Online

Cuenta de acceso a Exchange: asigne la función **Administración de organización** a la cuenta de acceso a Exchange para gestionar Exchange 2010.

Cuenta de acceso a Skype: asegúrese de que esta cuenta sea un usuario habilitado para Skype y que sea miembro de al menos una de las siguientes funciones:

- ♦ Función de CSAdministrator
- ♦ Funciones de CSUserAdministrator y CSArchiving

Cuenta de acceso a las carpetas públicas: asigne los siguientes permisos de Active Directory a la cuenta de acceso a las carpetas públicas:

- ♦ Gestión de carpetas públicas
- ♦ Carpetas públicas habilitadas para correo

Después de la instalación de DRA:

- ♦ Ejecute el siguiente comando para delegar permisos al "Contenedor Objetos eliminados" de la carpeta de instalación de DRA (Nota: un administrador de dominio debe ejecutar el comando):

```
DraDelObjsUtil.exe /domain:<NombreDominioNetbios> /delegate:<Nombre de cuenta>
```

- ♦ Ejecute el siguiente comando para delegar el permiso a "NetIQReceyleBin OU" desde la carpeta de instalación (Nota: esta acción solo puede realizarse después de añadir los dominios respectivos para que DRA los gestione):

```
DraRecycleBinUtil.exe /domain:<NombreDominioNetbios> /delegate:<Nombre de la cuenta>
```

- ♦ Añada la cuenta de anulación de privilegios mínimos al grupo "Administradores locales" en cada equipo que gestionará DRA como, por ejemplo, impresoras, servicios, registro de eventos, dispositivos, etc.
- ♦ Conceda la cuenta de anulación de privilegios mínimos "Permiso completo" en las carpetas compartidas o las carpetas DFS donde se aprovisionan los directorios principales.
- ♦ Añada la cuenta de anulación de privilegios mínimos a la función "Administración de organización" para gestionar los objetos de Exchange.

2.1.6 Requisitos de la consola Web y las extensiones de DRA

Entre los requisitos de la consola Web y las extensiones REST, se incluyen los siguientes:

Requisitos de software

Componente	Requisitos previos
Destino de instalación	Sistema operativo: <ul style="list-style-type: none">♦ Microsoft Windows Server 2016 y Microsoft Windows 10 con Microsoft IIS 10♦ Microsoft Windows Server 2012 y 2012 R2 con Microsoft IIS 8.0, 8.5
Servicio de host de DRA	<ul style="list-style-type: none">♦ Microsoft .NET Framework 4.5.2♦ Servidor de administración de DRA
Servicio y puesto final REST de DRA	<ul style="list-style-type: none">♦ Microsoft .NET Framework 4.5.2
Extensiones de PowerShell	<ul style="list-style-type: none">♦ Microsoft .NET Framework 4.5.2♦ PowerShell 4.0

Componente	Requisitos previos
Consola Web de DRA	<p>Servidor Web:</p> <ul style="list-style-type: none"> ◆ Microsoft Internet Information Server 8.0, 8.5 y 10 ◆ Microsoft Internet Information Services WCF (activación) <p>Componentes de Microsoft IIS:</p> <ul style="list-style-type: none"> ◆ Servidor Web <ul style="list-style-type: none"> ◆ Características HTTP comunes <ul style="list-style-type: none"> ◆ Contenido estático ◆ Documento por defecto ◆ Navegador de directorios ◆ Errores HTTP ◆ Desarrollo de aplicaciones <ul style="list-style-type: none"> ◆ ASP ◆ Estado y diagnóstico <ul style="list-style-type: none"> ◆ Registro HTTP ◆ Monitor de petición ◆ Seguridad <ul style="list-style-type: none"> ◆ Autenticación básica ◆ Rendimiento <ul style="list-style-type: none"> ◆ Compresión de contenido estático ◆ Herramientas de gestión del servidor Web

2.1.7 Requisitos de elaboración de informes

Entre los requisitos del módulo de elaboración de informes de DRA, se incluyen los siguientes:

Requisitos de software

Componente	Requisitos previos
Destino de instalación	<p>Sistema operativo:</p> <ul style="list-style-type: none"> ◆ Microsoft Windows Server 2012, 2012 R2, 2016

Componente	Requisitos previos
NetIQ Reporting Center (v3.2)	<p>Base de datos:</p> <ul style="list-style-type: none"> ◆ Microsoft SQL Server 2012, 2014 y 2016 ◆ Servicios de informes de Microsoft SQL Server <p>Servidor Web:</p> <ul style="list-style-type: none"> ◆ Microsoft Internet Information Server 8.0, 8.5 y 10 ◆ Componentes de Microsoft IIS: <ul style="list-style-type: none"> ◆ ASP .NET 4.0 <p>Microsoft .NET Framework 3.5:</p> <p>Todos los servidores de administración de DRA que se conectan al módulo de elaboración de informes de DRA también requieren .NET Framework 3.5.</p> <p>Nota: Al instalar NetIQ Reporting Center (NRC) en un equipo con SQL Server, es posible que sea necesario instalar manualmente .NET Framework 3.5 antes de instalar NRC.</p>
Módulo de elaboración de informes de DRA	<p>Base de datos:</p> <ul style="list-style-type: none"> ◆ Microsoft SQL Server Integration Services ◆ Agente Microsoft SQL Server

2.1.8 Requisitos de licencias

La licencia determina los productos y las funciones que puede utilizar. DRA requiere una clave de licencia instalada con el servidor de administración.

Después de instalar el servidor de administración, puede utilizar la utilidad de comprobación de estado para instalar una clave de licencia de prueba (TrialLicense.lic) que le permita gestionar un número ilimitado de cuentas de usuario y buzones durante 30 días.

Consulte el Acuerdo de licencia de usuario final (EULA) para obtener información sobre la definición y las restricciones de licencia.

2.2 Instalación del producto

En este capítulo se le guiará por el proceso de instalación de Directory and Resource Administrator. Para obtener más información acerca de la planificación de la instalación o actualización, consulte [Planificación de la implantación](#).

- ◆ [Sección 2.2.1, “Instalación del servidor de administración de DRA”, en la página 27](#)
- ◆ [Sección 2.2.2, “Instalar clientes de DRA”, en la página 28](#)
- ◆ [Sección 2.2.3, “Instalar las extensiones REST de DRA”, en la página 29](#)
- ◆ [Sección 2.2.4, “Instalación del servidor de flujo de trabajo”, en la página 30](#)
- ◆ [Sección 2.2.5, “Instalación del módulo de elaboración de informes de DRA”, en la página 30](#)

2.2.1 Instalación del servidor de administración de DRA

Puede instalar el servidor de administración de DRA como un nodo principal o secundario en su entorno. Los servidores de administración principal y secundario comparten los mismos requisitos. Sin embargo, cada implantación de DRA debe incluir un servidor de administración principal.

Lista de verificación de instalación interactiva

Paso	Detalles
Entrar en el servidor de destino	Entre en el servidor de Microsoft Windows de destino para realizar la instalación con una cuenta que disponga de privilegios administrativos locales.
Copiar y ejecutar el kit de instalación de administrador de NetIQ	Ejecute el kit de instalación de DRA (NetIQAdminInstallationKit.msi) para extraer los medios de instalación de DRA en el sistema de archivos local. Nota: El kit de instalación instalará .NET Framework en el servidor de destino, si es necesario.
Ejecutar la instalación de DRA	Lance la instalación de DRA. Nota: Para ejecutar la instalación más adelante, acceda a la ubicación en la que se han extraído los medios y ejecute Setup.exe.
Seleccionar el componente NetIQ Administration Server y el destino de instalación	Seleccione los componentes que desea instalar y acepte la ubicación de instalación por defecto C:\Archivos de programa (x86)\NetIQ\DRA o especifique una ubicación alternativa para la instalación. Opciones de componentes: NetIQ Administration Server <ul style="list-style-type: none">◆ Kit de recursos del archivo de registro◆ SDK de DRA de NetIQ Componente Web heredado Interfaces de usuario <ul style="list-style-type: none">◆ Gestión de cuentas y recursos◆ Proveedor ADSI de DRA◆ Interfaz de línea de comandos◆ Delegación y configuración
Comprobar los requisitos previos	En el cuadro de diálogo Requisitos previos , se mostrará la lista de software necesario en función de los componentes seleccionados para la instalación. El instalador le guiará por la instalación de los requisitos previos que faltan para que la instalación se complete correctamente.
Aceptar el acuerdo de licencia (EULA)	Acepte los términos del acuerdo de licencia de usuario final.
Seleccionar el modo de funcionamiento del servidor	Seleccione Principal para instalar el primer servidor de administración de DRA en un conjunto de varios maestros (solo habrá un servidor principal en una implantación) o Secundario para unir un nuevo servidor de administración de DRA a un servidor existente. Para obtener información sobre el conjunto de varios maestros, consulte Configuración del conjunto de varios maestros .

Paso	Detalles
Especificar las cuentas y las credenciales de instalación	<ul style="list-style-type: none"> ◆ Cuenta de servicio de DRA ◆ Grupo de AD LDS ◆ Administrador de DRA <p>Para obtener más información, consulte: Requisitos del servidor de administración de DRA.</p>
Configurar los permisos de DCOM	Habilite DRA para configurar el acceso de "COM distribuido" para los usuarios autenticados.
Configurar los puertos	Para obtener más información sobre los puertos por defecto, consulte Puertos y protocolos necesarios .
Especificar la ubicación de almacenamiento	Especifique la ubicación del archivo local que utilizará DRA para almacenar datos de auditoría y caché.
Comprobar la configuración de la instalación	Puede comprobar la configuración en la página de resumen de instalación antes de hacer clic en Instalar para continuar con la instalación.
Comprobación posterior a la instalación	Una vez que la instalación se haya completado, la utilidad comprobación de estado se ejecutará para verificar la instalación y actualizar la licencia del producto.

2.2.2 Instalar clientes de DRA

Puede instalar consolas y clientes de línea de comandos de DRA específicos. Para ello, ejecute DRAInstaller.msi con el correspondiente paquete .mst en el destino de la instalación:

NetIQDRAUserConsole.mst	Instala la consola de gestión de cuentas y recursos.
NetIQDRACLI.mst	Instala la interfaz de línea de comandos.
NetIQDRAADSI.mst	Instala al proveedor ADSI de DRA.
NetIQDRAClients.mst	Instala todas las interfaces de usuario de DRA.

Para implantar clientes de DRA específicos en varios equipos de toda su empresa, configure un objeto de directiva de grupo para instalar el paquete .MST específico.

- 1 Inicie Usuarios y equipos de Active Directory y cree un objeto de directiva de grupo.
- 2 Añada el paquete DRAInstaller.msi a este objeto de directiva de grupo.
- 3 Asegúrese de que este objeto de directiva de grupo tenga una de las siguientes propiedades:
 - ◆ Cada cuenta de usuario del grupo tiene permisos de Usuario avanzado para el equipo adecuado.
 - ◆ Habilite la opción de directiva Instalar siempre con privilegios elevados.
- 4 Añada el archivo .mst de interfaz de usuario como, por ejemplo, NetIQDRAUserConsole.mst, a este objeto de directiva de grupo.
- 5 Distribuya la directiva de grupo.

Nota: Para obtener más información sobre la directiva de grupo, consulte la Ayuda de Microsoft Windows. Para probar e implantar de forma fácil y segura la directiva de grupo en toda la empresa, utilice *Administrador de directiva de grupo*.

2.2.3 Instalar las extensiones REST de DRA

El paquete de extensiones REST de DRA incluye cuatro funciones:

- ♦ **Servicio de host de DRA de NetIQ:** gateway que se utiliza para comunicarse con el servicio de administración de DRA. Este servicio se debe ejecutar en un equipo con el servicio de administración de DRA instalado.
- ♦ **Servicio y puestos finales REST de DRA:** proporciona las interfaces RESTful que permiten que la consola Web de DRA y los clientes que no son de DRA soliciten operaciones de DRA. Este servicio debe ejecutarse en un equipo con una consola de DRA o el servicio de administración de DRA instalado.
- ♦ **Extensiones de PowerShell:** proporciona un módulo PowerShell que permite a los clientes que no son de DRA solicitar operaciones de DRA mediante cmdlets de PowerShell.
- ♦ **Consola Web de DRA:** la interfaz del cliente Web utilizada principalmente por los administradores asistentes, que también incluye opciones de personalización.

Paso	Detalles
Entrar en el servidor de destino	Entre en el servidor de Microsoft Windows de destino para realizar la instalación con una cuenta que disponga de privilegios administrativos locales.
Instalar el certificado SSL	Si aún no se ha instalado en el servidor de Windows, deberá instalarse un certificado SSL antes de ejecutar la instalación.
Copiar y ejecutar el kit de instalación de administrador de NetIQ	Copie el paquete de instalación de DRA <code>NetIQAdminINstallationKit.msi</code> en el servidor de destino y ejecútelo. Para ello, haga doble clic en el archivo o llámelo desde la línea de comandos. El kit de instalación extraerá los medios de instalación de DRA en una ubicación del sistema de archivos local que se puede personalizar.
Ejecutar el instalador de extensiones REST de DRA	Después de que el kit de instalación de DRA termine de extraer los medios de instalación, se le solicitará que inicie la instalación de DRA. Desplácese a la ubicación en la que se han extraído los medios de instalación, haga clic con el botón derecho en el archivo <code>DRARESTExtensionsInstaller.exe</code> y seleccione Ejecutar como administrador .
Aceptar el acuerdo de licencia (EULA)	Acepte los términos del acuerdo de licencia de usuario final.
Seleccionar los componentes y especificar la ubicación de destino de la instalación	En el cuadro de diálogo Seleccionar componentes de la instalación, instale todas las opciones: servicio de host de DRA, servicio y puestos finales REST de DRA, extensiones de PowerShell y consola Web de DRA. Acepte la ubicación de instalación por defecto <code>C:\Archivos de programa (x86)\NetIQ\DRA Extensions</code> o especifique una ubicación para la instalación.
Comprobar los requisitos previos	En el cuadro de diálogo Requisitos previos , se mostrará la lista de software necesario en función de los componentes seleccionados para la instalación. El instalador le guiará por la instalación de los requisitos previos que faltan para que la instalación se complete correctamente.

Paso	Detalles
Especificar la cuenta de servicio que se utilizará para la ejecución	Se muestra por defecto la cuenta de servicio existente del servidor de DRA. Especifique la contraseña de la cuenta de servicio. Para obtener más información sobre cómo configurar una cuenta de servicio para el servidor de administración de DRA, consulte Requisitos del servidor de administración de DRA .
Especificar el certificado SSL del servicio REST	Seleccione el certificado SSL que utilizará para el servicio REST y especifique los puertos de servicio de host y REST.
Especificar el certificado SSL de la consola Web	Especifique el certificado SSL que utilizará para el enlace HTTPS.
Comprobar la configuración de la instalación	Puede comprobar la configuración en la página de resumen de instalación antes de hacer clic en Instalar para continuar con la instalación.

2.2.4 Instalación del servidor de flujo de trabajo

Para obtener información sobre cómo instalar el servidor de flujo de trabajo, consulte [Workflow Automation Administrator Guide](#) (Guía del administrador de Automatización del flujo de trabajo).

2.2.5 Instalación del módulo de elaboración de informes de DRA

El módulo de elaboración de informes de DRA requiere que instale dos archivos ejecutables del kit de instalación de DRA de NetIQ: `NRCSetup.exe` y `DRAReportingSetup.exe`.

Pasos	Detalles
Entrar en el servidor de destino	Entre en el servidor de Microsoft Windows de destino para realizar la instalación con una cuenta que disponga de privilegios administrativos locales. Asegúrese de que esta cuenta tenga privilegios administrativos locales y de dominio, así como privilegios de administrador del sistema en SQL Server.
Copiar y ejecutar el kit de instalación de administrador de NetIQ	Copie el paquete de instalación de DRA <code>NetIQAdminInstallationKit.msi</code> en el servidor de destino y ejecútelo. Para ello, haga doble clic en el archivo o llámelo desde la línea de comandos. El kit de instalación extraerá los medios de instalación de DRA en una ubicación del sistema de archivos local que se puede personalizar. Además, el kit de instalación instalará .NET Framework en el servidor de destino si es necesario para satisfacer el requisito previo del instalador del producto DRA.
Ejecutar la instalación de NetIQ Reporting Center (NRC)	Después de que el kit de instalación de DRA termine de extraer los medios de instalación, desplácese a la ubicación en la que se han extraído los medios de instalación y ejecute <code>NRCSetup.exe</code> .
Seleccionar el componente NetIQ Reporting Center	En el cuadro de diálogo Seleccionar componentes de la instalación, utilice el componente "NetIQ Reporting Center" por defecto para instalar los cuatro componentes de NRC.
Especificar la ubicación de destino de la instalación	Acepte la ubicación de instalación por defecto <code>C:\Archivos de programa (x86)\NetIQ\Reporting Center</code> o especifique una ubicación para la instalación.

Pasos	Detalles
Comprobar los requisitos previos de instalación	En el cuadro de diálogo Requisitos previos , se mostrará la lista de software necesario en función de los componentes seleccionados para la instalación. El instalador le guiará por la instalación de los requisitos previos que faltan para que la instalación se complete correctamente. Importante: .NET Framework 3.5 debe instalarse manualmente en el servidor de elaboración de informes antes de instalar NRC.
Aceptar el acuerdo de licencia (EULA)	Acepte los términos del acuerdo de licencia de usuario final.
Instalar la base de datos de configuración	Utilice los valores por defecto del cuadro de diálogo Instalación de la base de datos de configuración - Entrada en SQL Server o proporcione la autenticación SQL para completar la instalación de NRC. Si ha utilizado la instancia por defecto para la instalación de SQL Server, el campo Instancia debe permanecer en blanco.
Ejecutar la instalación del módulo de elaboración de informes de DRA	Desplácese a la ubicación en la que se han extraído los medios de instalación y ejecute <code>DRAReportingSetup.exe</code> para instalar el componente de gestión para la integración del módulo de elaboración de informes de DRA.
Aceptar el acuerdo de licencia (EULA)	Acepte los términos del acuerdo de licencia de usuario final para completar la ejecución de la instalación.

2.3 Actualización del producto

En este capítulo, se proporciona un proceso que ayuda a actualizar o migrar un entorno distribuido en fases controladas.

En este capítulo, se presupone que el entorno contiene varios servidores de administración, con algunos de ellos ubicados en sitios remotos. Esta configuración recibe el nombre de conjunto de varios maestros (MMS, Multi-Master Set). Un MMS está formado por un servidor de administración principal y uno o varios servidores de administración secundarios asociados. Para obtener más información sobre el funcionamiento de un MMS, consulte [Configuración del conjunto de varios maestros](#).

- ♦ [Sección 2.3.1, “Planificación de una actualización de DRA”, en la página 31](#)
- ♦ [Sección 2.3.2, “Tareas previas a la actualización”, en la página 32](#)
- ♦ [Sección 2.3.3, “Actualización del servidor de administración de DRA”, en la página 35](#)
- ♦ [Sección 2.3.4, “Actualizar las extensiones REST de DRA”, en la página 38](#)
- ♦ [Sección 2.3.5, “Actualizar el módulo de elaboración de informes”, en la página 39](#)

2.3.1 Planificación de una actualización de DRA

Ejecute el archivo `NetIQAdminInstallationKit.msi` para extraer los medios de instalación e instalar y ejecutar la utilidad de comprobación de estado.

Asegúrese de planificar la implantación de DRA antes de iniciar el proceso de actualización. Al planificar la implantación, tenga en cuenta las directrices siguientes:

- ♦ Pruebe el proceso de actualización en su entorno de laboratorio antes de llevar la actualización a su entorno de producción. Las pruebas le permiten identificar y resolver cualquier problema inesperado sin que esto afecte a las tareas administrativas diarias.

- ◆ Consulte [Puertos y protocolos necesarios](#).
- ◆ Determine cuántos AA dependen de cada MMS. Si la mayoría de los AA dependen de servidores o conjuntos de servidores específicos, actualice primero esos servidores durante las horas de menor actividad.
- ◆ Determine los AA que necesitan la consola de delegación y configuración. Puede obtener esta información de una de las siguientes formas:
 - ◆ Consulte los AA asociados a los grupos de AA integrados.
 - ◆ Consulte los AA asociados a las ActiveViews integradas.
 - ◆ Utilice el componente de elaboración de informes de Directory and Resource Administrator para generar informes de modelo de seguridad como, por ejemplo, informes de información de administradores asistentes de ActiveView y grupos de administradores asistentes.

Informe a estos AA acerca de sus planes de actualización de las interfaces de usuario.

- ◆ Determine los AA que deben conectarse al servidor de administración principal. Estos AA deben actualizar los equipos cliente una vez que actualice el servidor de administración principal.

Informe a estos AA acerca de sus planes para actualizar los servidores de administración e interfaces de usuario.

- ◆ Determine si necesita implementar los cambios de delegación, configuración o directivas que se hayan realizado antes de iniciar el proceso de actualización. En función del entorno, se puede realizar esta decisión de un sitio a otro.
- ◆ Coordine la actualización de los equipos cliente y los servidores de administración para garantizar un tiempo de inactividad mínimo. Tenga en cuenta que DRA no admite la ejecución de versiones anteriores de DRA con la versión actual de DRA en el mismo servidor de administración o equipo cliente.

2.3.2 Tareas previas a la actualización

Antes de comenzar las instalaciones de actualización, siga los pasos previos a la actualización indicados a continuación para preparar cada conjunto de servidores para la actualización.

Pasos	Detalles
Copia de seguridad de la instancia de AD LDS	Abra la utilidad de comprobación de estado de DRA y ejecute la comprobación de copia de seguridad de la instancia de AD LDS para crear una copia de seguridad de la instancia actual de AD LDS.
Realizar un plan de implantación	Realice un plan de implantación para actualizar los servidores de administración y las interfaces de usuario (equipos cliente AA). Para obtener más información, consulte Planificación de una actualización de DRA .
Reservar un servidor secundario para la ejecución de una versión anterior de DRA	<i>Opcional:</i> reserve un servidor de administración secundario para que ejecute una versión de DRA mientras actualiza un sitio.
Realizar los cambios necesarios para este MMS	Realice los cambios necesarios en los ajustes de delegación, configuración o directiva de este MMS. Utilice el servidor de administración principal para modificar estos ajustes.
Sincronizar el MMS	Sincronice los conjuntos de servidores para que cada servidor de administración contenga la configuración y los ajustes de seguridad más recientes.

Pasos	Detalles
Realizar una copia de seguridad del registro del servidor principal	Realice una copia de seguridad del registro del servidor de administración principal. Disponer de una copia de seguridad de la configuración anterior del registro le permite recuperar fácilmente la configuración anterior y los ajustes de seguridad.

Nota: Si necesita restaurar la copia de seguridad de la instancia de AD LDS, realice lo siguiente:

- 1 Detenga la instancia actual de AD LDS en Administración de equipos > Servicios. Esta presentará un título diferente: `NetIQDRASecureStoragexxxxx`.
- 2 Sustituya el archivo **actual** `adamnts.dit` por el archivo de **copia de seguridad** `adamnts.dit`, como se indica a continuación:
 - ◆ Ubicación del archivo actual: `%ProgramData%/NetIQ/DRA/<NombreInstanciaDRA>/data/`
 - ◆ Ubicación del archivo de copia de seguridad: `%ProgramData%/NetIQ/ADLDS/`
- 3 Reinicie la instancia de AD LDS.

Reserva de un servidor de administración local para la ejecución de una versión anterior de DRA

Reservar uno o varios servidores de administración secundarios para que ejecuten de forma local una versión anterior de DRA en un sitio durante la actualización puede ayudar a minimizar el tiempo de inactividad y las costosas conexiones a sitios remotos. Este paso es opcional y permite a los AA utilizar una versión anterior de DRA durante todo el proceso de actualización hasta que esté satisfecho con la implantación completada.

Considere esta opción si necesita cumplir uno o más de los siguientes requisitos de actualización:

- ◆ El tiempo de inactividad debe ser mínimo o no debe haber ninguno.
- ◆ Debe admitir un gran número de AA y no puede actualizar al instante todos los equipos cliente.
- ◆ Desea seguir proporcionando acceso a una versión anterior de DRA después de actualizar el servidor de administración principal.
- ◆ El entorno incluye un MMS que abarca varios sitios.

Puede instalar un nuevo servidor secundario de administración o designar un servidor secundario existente para que ejecute una versión anterior de DRA. Si tiene intención de actualizar este servidor, este debe ser el último servidor que se actualice. De lo contrario, desinstale por completo DRA en este servidor cuando se haya completado correctamente la actualización.

Configuración de un nuevo servidor secundario

La instalación de un nuevo servidor de administración secundario en un sitio local puede ayudarle a evitar costosas conexiones a sitios remotos y garantiza que los AA puedan seguir utilizando una versión anterior de DRA sin interrupciones. Si el entorno incluye un MMS que abarca varios sitios, debe considerar la posibilidad de usar esta opción. Por ejemplo, si el MMS consta de un servidor de administración principal en el sitio de Londres y un servidor de administración secundario en el sitio de Tokio, considere la posibilidad de instalar un servidor secundario en el sitio de Londres y añadirlo al MMS correspondiente. Este servidor adicional permitirá que los AA del sitio de Londres utilicen una versión anterior de DRA hasta que se haya completado la actualización.

Uso de un servidor secundario existente

Puede utilizar un servidor de administración secundario existente como servidor reservado para la ejecución de una versión anterior de DRA. Si no tiene intención de actualizar un servidor de administrador secundario en un determinado sitio, debe considerar la posibilidad de usar esta opción. Si no puede reservar un servidor secundario existente, considere la posibilidad de instalar un nuevo servidor de administración para este fin. Reservar uno o varios servidores secundarios para que ejecuten una versión anterior de DRA permite a los AA seguir utilizando una versión anterior de DRA sin interrupciones hasta que se complete la actualización. Esta opción funciona mejor en entornos de mayor tamaño que utilizan un modelo de administración centralizada.

Sincronización del conjunto de servidores con la versión anterior de DRA

Antes de realizar una copia de seguridad del registro de la versión anterior de DRA o iniciar el proceso de actualización, asegúrese de sincronizar los conjuntos de servidores para que cada servidor de administración contenga la configuración y los ajustes de seguridad más recientes.

Nota: Asegúrese de que haya realizado todos los cambios necesarios en los ajustes de delegación, configuración o directiva de este MMS. Utilice el servidor de administración principal para modificar estos ajustes. Una vez actualizado el servidor de administración principal, no podrá sincronizar los ajustes de delegación, configuración o directiva en ningún servidor de administración que ejecute versiones anteriores de DRA.

Para sincronizar el conjunto de servidores existente:

- 1 Entre en el servidor de administración principal como administrador integrado.
- 2 Inicie la interfaz de MMC.
- 3 En el panel de la izquierda, haga clic en **Gestión de configuraciones**.
- 4 Haga clic en **Servidores de administración**.
- 5 En el panel de la derecha, seleccione el servidor de administración principal adecuado para este conjunto de servidores.
- 6 Haga clic en **Propiedades**.
- 7 En la pestaña Programación de sincronización, haga clic en **Actualizar ahora**.
- 8 Compruebe que la sincronización se realice correctamente y que todos los servidores de administración secundarios estén disponibles.

Copia de seguridad del registro del servidor de administración

Una copia de seguridad del registro del servidor de administración garantiza que puede restablecer las configuraciones anteriores. Por ejemplo, si debe desinstalar por completo la versión actual de DRA y utilizar la versión anterior, disponer de una copia de seguridad de la configuración anterior del registro le permitirá recuperar fácilmente la configuración y los ajustes de seguridad anteriores.

Sin embargo, tenga cuidado al editar el registro. Si se produce un error en el registro, es posible que el servidor de administración no presente el funcionamiento esperado. Si se produce un error durante el proceso de actualización, puede utilizar la copia de seguridad de la configuración del registro para restaurar el registro. Para obtener más información, consulte la *Ayuda del Editor del registro*.

Importante: La versión del servidor de DRA, el nombre del sistema operativo Windows y la configuración del dominio gestionado deben ser exactamente iguales al restaurar el registro.

Importante: Antes de actualizar, realice copias de seguridad del sistema operativo Windows del equipo que aloja DRA o cree una captura de máquina virtual del equipo.

Para realizar copias de seguridad del registro del servidor de administración:

- 1 Ejecute `regedit.exe`.
- 2 Haga clic con el botón derecho en el nodo
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint` y seleccione **Exportar**.
- 3 Especifique el nombre y la ubicación del archivo para guardar la clave de registro y haga clic en **Guardar**.

2.3.3 Actualización del servidor de administración de DRA

La siguiente lista de verificación le guiará por todo el proceso de actualización. Utilice este proceso para actualizar cada uno de los conjuntos de servidores del entorno. Si aún no lo ha hecho, use la utilidad de comprobación de estado para crear una copia de seguridad de la instancia actual de AD LDS.

Puede distribuir este proceso de actualización en varias fases mediante la actualización de un MMS cada vez. Este proceso de actualización también le permite incluir temporalmente servidores secundarios que ejecuten una versión anterior de DRA y servidores secundarios que ejecuten la versión actual de DRA en el mismo MMS. DRA admite la sincronización entre los servidores de administración que ejecutan una versión anterior de DRA y los servidores que ejecutan la versión actual de DRA. Sin embargo, tenga en cuenta que DRA no admite la ejecución de una versión anterior de DRA con la versión actual de DRA en el mismo servidor de administración o equipo cliente.

En DRA 9.2 o versiones posteriores, la configuración del servidor de Automatización del flujo de trabajo se almacena en AD LDS en lugar del registro. Al actualizar desde DRA 9.1 o versiones anteriores a DRA 9.2 o versiones posteriores, la configuración del registro se transfiere automáticamente a AD LDS y se replica en todos los servidores secundarios.

Advertencia: No actualice los servidores de administración secundarios hasta que haya actualizado el servidor de administración principal de ese MMS.

Pasos	Detalles
Ejecutar la utilidad de comprobación de estado	Instale la utilidad de comprobación de estado de DRA independiente y ejecútela mediante una cuenta de servicio. Solucione los problemas existentes.
Realizar una actualización de prueba	Realice una actualización de prueba en el entorno de laboratorio para identificar posibles problemas y minimizar el tiempo de inactividad de la producción.
Determinar el orden de actualización	Determine el orden en el que desea actualizar los conjuntos de servidores.
Preparar cada MMS para la actualización	Prepare cada MMS para la actualización. Para obtener más información, consulte Tareas previas a la actualización .
Actualizar el servidor principal	Actualice el servidor de administración principal del MMS adecuado.
Instalar un nuevo servidor secundario	<i>(Opcional)</i> Para minimizar el tiempo de inactividad en sitios remotos, instale un servidor de administración secundario local que ejecute la versión más reciente de DRA.
Implantar las interfaces de usuario	Implante las interfaces de usuario en los administradores asistentes.
Actualizar los servidores secundarios	Actualice los servidores de administración secundarios del MMS.
Actualizar el módulo de elaboración de informes de DRA	Actualice el módulo de elaboración de informes de DRA.
Actualizar las extensiones REST	Ejecute el instalador de extensiones REST de DRA.
Ejecutar la utilidad de comprobación de estado	Ejecute la utilidad de comprobación de estado que se ha instalado como parte de la actualización. Solucione los problemas existentes.

Actualización del servidor de administración principal

Después de preparar correctamente el MMS, actualice el servidor de administración principal. No actualice las interfaces de usuario en los equipos cliente AA hasta que se haya completado la actualización del servidor de administración principal. Para obtener más información, consulte [Implantación de las interfaces de usuario de DRA](#).

Nota: Para obtener instrucciones e información de actualización más detallados, consulte las *Notas de la versión de Directory and Resource Administrator*.

Antes de actualizar, informe a los AA de cuándo tiene intención de iniciar este proceso. Si ha reservado un servidor de administración secundario para que ejecute una versión anterior de DRA, identifique también este servidor para que los AA puedan seguir utilizando la versión anterior de DRA durante la actualización.

Nota: Una vez actualizado el servidor de administración principal, no podrá sincronizar los ajustes de delegación, configuración o directiva de este servidor en los servidores de administración secundarios que ejecuten una versión anterior de DRA.

Instalación de un servidor de administración secundario local para la versión actual de DRA

La instalación de un nuevo servidor de administración secundario para que ejecute la versión actual de DRA en un sitio local puede ayudarle a minimizar conexiones costosas a sitios remotos, a la vez que reduce el tiempo de inactividad general y permite una implantación más rápida de las interfaces de usuario. Este paso es opcional y permite a los AA utilizar una versión actual y una versión anterior de DRA durante todo el proceso de actualización hasta que esté satisfecho con la implantación completada.

Considere esta opción si necesita cumplir uno o más de los siguientes requisitos de actualización:

- ♦ El tiempo de inactividad debe ser mínimo o no debe haber ninguno.
- ♦ Debe admitir un gran número de AA y no puede actualizar al instante todos los equipos cliente.
- ♦ Desea seguir proporcionando acceso a una versión anterior de DRA después de actualizar el servidor de administración principal.
- ♦ El entorno incluye un MMS que abarca varios sitios.

Por ejemplo, si el MMS consta de un servidor de administración principal en el sitio de Londres y un servidor de administración secundario en el sitio de Tokio, considere la posibilidad de instalar un servidor secundario en el sitio de Tokio y añadirlo al MMS correspondiente. Este servidor adicional equilibra mejor la carga de administración diaria en el sitio de Tokio y permite a los AA de cualquiera de los sitios utilizar una versión anterior de DRA, así como la versión actual de DRA hasta que se complete la actualización. Además, los AA no experimentarán ningún tiempo de inactividad porque puede implantar al instante las interfaces de usuario de DRA actuales. Para obtener más información acerca de la actualización de las interfaces de usuario, consulte [Implantación de las interfaces de usuario de DRA](#).

Implantación de las interfaces de usuario de DRA

Por lo general, debe implantar las interfaces de usuario de DRA actuales después de actualizar el servidor de administración principal y un servidor de administración secundario. Sin embargo, para los AA que deben utilizar el servidor de administración principal, asegúrese de actualizar primero los equipos cliente mediante la instalación de la consola de delegación y configuración. Para obtener más información, consulte [Planificación de una actualización de DRA](#).

Si lleva a cabo a menudo un procesamiento por lotes a través de la CLI o el proveedor ADSI, o genera informes con frecuencia, considere la posibilidad de instalar estas interfaces de usuario en un servidor de administración secundario reservado para mantener un equilibrio de carga adecuado en todo el MMS.

Puede permitir que los AA instalen las interfaces de usuario de DRA o las implanten a través de la directiva de grupo. También puede implantar de forma fácil y rápida la consola Web en varios AA.

Nota: No puede ejecutar varias versiones de componentes de DRA en paralelo en el mismo servidor de DRA. Si tiene intención de actualizar gradualmente los equipos cliente AA, considere la posibilidad de implantar la consola Web para garantizar el acceso instantáneo a un servidor de administración que ejecute la versión actual de DRA.

Actualización de los servidores de administración secundarios

Al actualizar los servidores de administración secundarios, puede actualizar cada servidor según sea necesario, según los requisitos de administración. Además, tenga en cuenta cómo desea actualizar e implantar las interfaces de usuario de DRA. Para obtener más información, consulte [Implantación de las interfaces de usuario de DRA](#).

Por ejemplo, una vía de actualización típica puede incluir los siguientes pasos:

- 1 Actualice un servidor de administración secundario.
- 2 Indique a los AA que utilicen este servidor para instalar las interfaces de usuario adecuadas, como la consola de gestión de cuentas y recursos.
- 3 Repita los pasos 1 y 2 anteriores hasta que actualice por completo el MMS.

Antes de actualizar, informe a los AA de cuándo tiene intención de iniciar este proceso. Si ha reservado un servidor de administración secundario para que ejecute una versión anterior de DRA, identifique también este servidor para que los AA puedan seguir utilizando la versión anterior de DRA durante la actualización. Cuando haya completado el proceso de actualización de este MMS, y todos los equipos cliente AA ejecuten interfaces de usuario actualizadas, desconecte todos los servidores restantes con la versión anterior de DRA.

2.3.4 Actualizar las extensiones REST de DRA

Para actualizar la consola Web y las extensiones REST en Directory and Resource Administrator 9.2, debe utilizar DRA 9.0.1 o una versión posterior. Para obtener información sobre los requisitos, consulte [Requisitos de la consola Web y las extensiones de DRA](#).

Para actualizar la consola Web y las extensiones de DRA:

- 1 Después de descargar el kit de instalación de DRA, desplácese a la ubicación en la que se han extraído los medios de instalación, haga clic con el botón derecho en el archivo `DRARESTExtensionsInstaller.exe` y seleccione **Ejecutar como administrador**.
- 2 Siga las instrucciones del asistente de instalación hasta que se complete la instalación y haga clic en **Finalizar**.

Para obtener más información acerca de los pasos descritos en el asistente de instalación, consulte los pasos necesarios para realizar una nueva instalación: [Instalar las extensiones REST de DRA](#).

Actualización del contenido personalizado

Al actualizar a una versión más reciente de DRA, desea conservar todas las personalizaciones que haya realizado en la consola Web del servidor Web. Para facilitar esta tarea, DRA dispone de una utilidad de actualización de personalización integrada en el instalador de extensiones REST de DRA. Esta utilidad se ejecuta automáticamente al ejecutar `DRARESTExtensionsInstaller.exe` para actualizar las extensiones REST en el servidor Web. También puede volver a ejecutar la utilidad manualmente desde el directorio de instalación fuera de la instalación.

Parte del proceso de la utilidad de actualización de personalización consiste en realizar una copia de seguridad de las personalizaciones antes de que se inicie la actualización. Durante el proceso de actualización, la utilidad crea un archivo de registro de todos los cambios realizados debido a la actualización y también incluye una advertencia en relación con los elementos de personalización que no se pueden actualizar automáticamente.

Como práctica recomendada, es recomendable que consulte el registro después de realizar la actualización. Si es necesario, puede deshacer las personalizaciones previas a la actualización. Para ello, cópielas desde la carpeta de copia de seguridad. Puede definir la vía de carpeta para las personalizaciones actualizadas cuando se abra la utilidad de actualización de personalización, o bien puede utilizar la vía por defecto que se rellena automáticamente.

A continuación, se indican las vías por defecto para las personalizaciones actualizadas y la copia de seguridad de las personalizaciones:

- ♦ Vía a la carpeta personalizada por defecto
C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom
- ♦ Vía a la copia de seguridad por defecto:
\$CustomFolderPath\custom_upgrade_\$VERSIONFROM_to_\$VERSIONTO_backup

2.3.5 Actualizar el módulo de elaboración de informes

Antes de actualizar el módulo de elaboración de informes de DRA, asegúrese de que su entorno cumpla con los requisitos mínimos para NRC 3.2. Para obtener más información sobre los requisitos de instalación y las consideraciones de actualización, consulte la *Guía de informes del Centro de informes de NetIQ*.

Pasos	Detalles
Inhabilitar la compatibilidad con el módulo de elaboración de informes de DRA	Para asegurarse de que los compiladores de elaboración de informes no se ejecuten durante el proceso de actualización, desactive la compatibilidad con el módulo de elaboración de informes DRA en la ventana Configuración del servicio de elaboración de informes de la consola de delegación y configuración.
Entrar en la instancia de SQL Server con las credenciales pertinentes	Entre en la instancia de Microsoft Windows Server en el que se haya instalado la instancia de SQL para las bases de datos de informes con una cuenta de administrador. Asegúrese de que esta cuenta tenga privilegios administrativos locales, así como privilegios de administrador del sistema en SQL Server.
Ejecutar la instalación del módulo de elaboración de informes de DRA	Ejecute DRAReportingSetup.exe desde el kit de instalación y siga las instrucciones del asistente de instalación.
Ejecutar la instalación de NRC	<i>Condicional:</i> si el servicio Web NRC se ha instalado en un equipo diferente, entre en el equipo en el que se haya instalado el servicio Web y ejecute NRCSetup.exe para actualizar el servicio Web NRC. Nota: Si se ha instalado la base de datos de configuración en un servidor distinto, esta deberá actualizarse primero.
Ejecutar la instalación de NRC en equipos cliente	Ejecute NRCSetup.exe en todos los equipos cliente NRC.
Habilitar la compatibilidad con el módulo de elaboración de informes de DRA	En el servidor de administración principal, habilite el módulo de elaboración de informes en la consola de delegación y configuración.

Si el entorno utiliza la integración con SSRS, deberá implantar de nuevo los informes. Para obtener más información acerca de cómo volver a distribuir informes, consulte [Reporting Center Guide](#) (Guía de Reporting Center) en el sitio Web de documentación.

3 Configuración de los componentes y el proceso

Este capítulo proporciona información para configurar DRA por primera vez, incluidos servidores y sus personalizaciones, consolas y sus personalizaciones, Office 365, administración de carpetas públicas y conexión a servidores.

3.1 Configuración inicial

En esta sección, se describen los pasos de configuración necesarios si va a instalar por primera vez Directory and Resource Administrator.

3.1.1 Lista de verificación de configuración

La siguiente lista de verificación le guiará por el proceso de configuración de DRA para utilizar el producto por primera vez.

Pasos	Detalles
Instalar una licencia de DRA	Utilice la utilidad de comprobación de estado para aplicar una licencia de DRA. Para obtener más información sobre las licencias de DRA, consulte Requisitos de licencias .
Configurar los servidores y las funciones de DRA	Configure el MMS, las excepciones de clonación, la réplica de archivos, la adición de marcas a eventos, el almacenamiento en caché, los AD LDS, los grupos dinámicos, la Papelera, los informes, el Historial de cambios unificado y el servidor de flujo de trabajo.
Configurar el cliente de delegación y configuración	Configure cómo se accede a los elementos y cómo se muestran en el cliente de configuración y delegación.
Configurar el cliente Web	Configure la salida automática de la sesión, los certificados, las conexiones del servidor y los componentes de autenticación.

3.1.2 Instalación o actualización de licencias

DRA requiere un archivo de clave de licencia. Este archivo contiene la información de su licencia y se ha instalado en el servidor de administración. Después de instalar el servidor de administración, use la utilidad de comprobación de estado para instalar el archivo de clave de licencia de prueba (`TrialLicense.lic`) proporcionado por NetIQ Corporation.

Para actualizar una licencia existente o de prueba, abra la consola de delegación y configuración y desplácese a **Gestión de configuraciones > Actualizar licencia**. Al actualizar la licencia, actualice el archivo de licencia en cada servidor de administración.

Puede ver la licencia del producto mediante la consola de delegación y configuración o la consola de gestión de cuentas y recursos. Para ver la licencia del producto, desplácese al menú **Archivo > Propiedades de DRA > Licencia**.

3.1.3 Configurar los servidores y las funciones de DRA

Para administrar el acceso con privilegios mínimos para las tareas de Active Directory que utilizan DRA, deben configurarse muchos componentes y procesos. Entre ellos, se incluyen las configuraciones de componentes de cliente y generales. En esta sección, se proporciona información sobre los componentes y los procesos generales que deben configurarse para DRA.

Configuración del conjunto de varios maestros

Un entorno de conjunto de varios maestros (MMS, Multi-Master Set) utiliza varios servidores de administración para gestionar el mismo conjunto de dominios y servidores miembros. Un MMS está formado por un servidor de administración principal y varios servidores de administración secundarios asociados.

El modo por defecto del servidor de administración es Principal. A medida que añade servidores secundarios al entorno MMS, tenga en cuenta que un servidor de administración secundario solo puede pertenecer a un único conjunto de servidores.

Para asegurarse de que cada servidor del conjunto gestione los mismos datos, sincronice periódicamente los servidores secundarios con el servidor de administración principal. Para reducir el mantenimiento, utilice la misma cuenta de servicio para todos los servidores de administración en el bosque de dominios.

Importante

- ♦ Al instalar el servidor secundario, seleccione **Servidor de administración secundario** en el instalador.
- ♦ La versión de DRA del nuevo servidor secundario debe ser igual a la del servidor principal de DRA para que todas las funciones del servidor principal estén disponibles en el secundario.

Adición de un servidor de administración secundario

Puede añadir un servidor de administración secundario a un MMS existente en el cliente de delegación y configuración. Para añadir un servidor secundario, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Nota: Para añadir correctamente un nuevo servidor secundario, debe instalar primero el producto Directory and Resource Administrator en el equipo del servidor de administración. Para obtener más información, consulte [Instalación del servidor de administración de DRA](#).

Para añadir un servidor de administración secundario, haga clic con el botón derecho en **Administration Server** (Servidor de administración) en el nodo "Configuration Management" (Gestión de configuraciones) y seleccione **Add Secondary Server** (Añadir servidor secundario).

Subir de nivel un servidor de administración secundario

Puede subir de nivel un servidor de administración secundario a uno principal. Al subir de nivel un servidor de administración secundario a uno principal, el servidor de administración principal existente se convierte en el secundario en el conjunto de servidores. Para subir de nivel un servidor

de administración secundario, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios. Antes de subir de nivel un servidor de administración secundario, sincronice el MMS para que presente la configuración más reciente.

Para obtener información acerca de cómo sincronizar el MMS, consulte [Programación de la sincronización](#).

Nota: Un servidor primario que se acaba de subir de nivel solo puede conectarse a servidores secundarios que estuviesen disponibles durante el proceso de subida de nivel. Si un servidor secundario deja de estar disponible durante el proceso de subida de nivel, póngase en contacto con el servicio de asistencia técnica.

Para subir de nivel un servidor de administración secundario:

- 1 Desplácese al nodo **Configuration Management** (Gestión de configuraciones) > **Administration Servers** (Servidores de administración).
- 2 En el panel derecho, seleccione el servidor de administración secundario que desea subir de nivel.
- 3 En el menú Tareas, haga clic en **Advanced (Opciones avanzadas)** > **Promote Server** (Subir de nivel servidor).

Importante: Si la cuenta de servicio del servidor secundario es diferente a la del servidor principal o el servidor secundario se ha instalado en un dominio diferente al del servidor principal (dominios de confianza/que no son de confianza) y sube de nivel el servidor secundario, asegúrese de delegar las siguientes funciones antes de realizar el proceso de subida de nivel: **Auditar todos los objetos**, **Configurar servidores y dominios** y **Generar informes de IU**. A continuación, compruebe que las sincronizaciones de MMS se hayan realizado correctamente.

Bajar de nivel un servidor de administración principal

Puede bajar de nivel un servidor de administración principal a uno secundario. Para bajar de nivel un servidor de administración principal, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Para bajar de nivel un servidor de administración principal:

- 1 Desplácese al nodo **Configuration Management** (Gestión de configuraciones) > **Administration Servers** (Servidores de administración).
- 2 En el panel derecho, seleccione el servidor de administración principal que desea bajar de nivel.
- 3 En el menú Tareas, haga clic en **Advanced (Opciones avanzadas)** > **Demote Server** (Bajar de nivel servidor).
- 4 Especifique el equipo que desea designar como el nuevo servidor de administración principal y haga clic en **Aceptar**.

Programación de la sincronización

La sincronización garantiza que todos los servidores de administración del MMS utilicen los mismos datos de configuración. Aunque se pueden sincronizar manualmente los servidores en cualquier momento, la programación por defecto determina la sincronización del MMS cada 4 horas. Modifique esta programación para adaptarla a sus necesidades empresariales.

Para modificar la programación de sincronización o para sincronizar manualmente los servidores MMS, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Para acceder a la programación de sincronización o realizar sincronizaciones manuales, desplácese a **Configuration Management** (Gestión de configuraciones) > **Administration Servers** (Servidores de administración) y utilice el menú **Tareas** o haga clic con el botón derecho en las opciones del servidor seleccionado. La programación de sincronización se encuentra en las propiedades del servidor seleccionado.

Descripción de las opciones de sincronización

Existen básicamente cuatro opciones diferentes para sincronizar servidores MMS:

- ♦ Seleccione el servidor principal y sincronice todos los servidores secundarios, "Synchronize All Servers" (Sincronizar todos los servidores).
- ♦ Seleccione un servidor secundario y sincronice solo ese servidor.
- ♦ Configure la programación de sincronización de los servidores principal y secundarios de forma independiente.
- ♦ Configure la programación de sincronización de todos los servidores. Esta opción está habilitada si se ha seleccionado el siguiente ajuste en la programación de sincronización del servidor principal:

Configure secondary Administration servers when refreshing the primary Administration server (Configurar los servidores de administración secundarios al actualizar el servidor de administración principal)

Nota: Si desactiva esta opción, los archivos de configuración se copian en los servidores secundarios de la programación principal, pero no se cargarán en ese momento en la programación secundaria; se cargarán en función de la programación configurada en el servidor secundario. Esto es útil si los servidores se encuentran en distintas zonas horarias. Por ejemplo, puede configurar todos los servidores para que se actualice la configuración en mitad de la noche, aunque haya diferencias de hora debido a las distintas zonas horarias.

Gestión de excepciones de clonación

Las excepciones de clonación permiten definir propiedades de usuarios, grupos, contactos y equipos que no se copiarán cuando se clone uno de estos objetos.

Puede gestionar las excepciones de clonación con los poderes adecuados. La función Gestionar excepciones de clonación otorga poderes para ver, crear y suprimir excepciones de clonación.

Para ver o suprimir una excepción de clonación existente, o crear una nueva, desplácese a **Configuration Management** (Gestión de configuraciones) > **Clone Exceptions** (Excepciones de clonación) > **Tareas**, o bien haga clic con el botón derecho en el menú.

Réplica de archivos

Al crear herramientas personalizadas, es posible que deba instalar los archivos de compatibilidad utilizados por la herramienta personalizada en el equipo cliente de DRA antes de poder ejecutar la herramienta personalizada. Puede utilizar las funciones de réplica de archivos de DRA para replicar de forma fácil y rápida los archivos de compatibilidad de herramientas personalizadas desde el

servidor de administración principal en los servidores de administración secundarios del MMS, así como en los equipos cliente de DRA. La réplica de archivos también permite replicar guiones de activador de servidores principales en secundarios.

Puede utilizar de forma conjunta las herramientas personalizadas y la réplica de archivos para asegurarse de que los equipos cliente de DRA puedan acceder a los archivos de herramientas personalizadas. DRA replica los archivos de herramientas personalizadas en los servidores de administración secundarios para garantizar que los equipos cliente de DRA que se conectan a los servidores de administración secundarios puedan acceder a las herramientas personalizadas.

DRA replica los archivos de herramientas personalizadas en el servidor de administración principal en los servidores de administración secundarios durante el proceso de sincronización de MMS. DRA descarga los archivos de herramientas personalizadas en los equipos cliente de DRA cuando estos se conectan a los servidores de administración.

Nota: DRA descarga los archivos de herramientas personalizadas en la siguiente ubicación de los equipos cliente de DRA:

```
{DirInstalDRA}\{ID de MMS}\Download
```

El ID de MMS es la identificación del conjunto de varios maestros desde el que DRA descarga los archivos de herramientas personalizadas.

Carga de archivos de herramientas personalizadas para la réplica

Al cargar archivos en el servidor de administración principal, especifique los archivos que desea cargar y replicar entre el servidor de administración primario y todos los servidores de administración secundarios del conjunto MMS. DRA permite cargar archivos de biblioteca, guión y ejecutables.

La función Replicar archivos le permite replicar archivos del servidor de administración principal en los servidores de administración secundarios del MMS, así como en los equipos clientes de DRA. La función Replicar archivos contiene los siguientes poderes:

- ♦ **Suprimir archivos del servidor:** este poder permite a DRA suprimir archivos que ya no existen en los servidores de administración principal y secundarios, y los equipos cliente de DRA.
- ♦ **Definir información del archivo:** este poder permite a DRA actualizar la información de los archivos en los servidores de administración secundarios.
- ♦ **Cargar archivos en el servidor:** este poder permita a DRA cargar archivos del equipo cliente de DRA en el servidor de administración principal.

Nota: Solo puede cargar un archivo para la réplica cada vez mediante la interfaz de usuario de réplica de archivos de la consola de delegación y configuración.

Para cargar un archivo de herramienta personalizada en el servidor de administración principal:

- 1 Desplácese a **Configuration Management** (Gestión de configuraciones) > **File Replication** (Réplica de archivos).
- 2 En el menú Tareas, haga clic en **Upload file** (Cargar archivo).
- 3 Para buscar y seleccionar el archivo que desea cargar, haga clic en **Examinar**.
- 4 *Si desea descargar el archivo seleccionado en todos los equipos cliente de DRA*, seleccione la casilla de verificación **Download to all client computers** (Descargar en todos los equipos cliente).
- 5 *Si desea registrar una biblioteca COM*, seleccione la casilla de verificación **Register COM library** (Registrar biblioteca COM).

6 Haga clic en **Aceptar**.

Nota

- ♦ DRA carga en la carpeta `{DirInstalDRA}\FileTransfer\Replicate` del servidor de administración principal el archivo de guión o los archivos de compatibilidad que deben replicarse en otros servidores de administración secundarios. La carpeta `{DirInstalDRA}\FileTransfer\Replicate` también recibe el nombre de `{Vía_archivos_replicados_DRA}`.
 - ♦ DRA carga el archivo de guión o los archivos de compatibilidad que deben replicarse en los equipos cliente de DRA, en la carpeta `{DirInstalDRA}\FileTransfer\Replicate` del servidor de administración principal.
 - ♦ El archivo de herramienta personalizada cargado en el servidor de administración principal se distribuirá a los servidores de administración secundarios durante la próxima sincronización programada o mediante sincronización manual.
-

Réplica de varios archivos entre servidores de administración

Si tiene varios archivos que desea cargar y replicar entre el servidor de administración principal y los servidores de administración secundarios en el MMS, puede cargarlos manualmente para la réplica. Para ello, copie los archivos en el directorio de réplica del servidor de administración principal, que se encuentra en la siguiente ubicación:

```
{DRAInstallDir}\FileTransfer\Replicate
```

El directorio de réplica se crea durante la instalación de DRA.

El servidor de administración identifica automáticamente los archivos en el directorio de réplica y replica los archivos entre los servidores de administración durante la próxima sincronización programada. Después de la sincronización, DRA muestra los archivos cargados en la ventana Réplica de archivos de la consola de delegación y configuración.

Nota: Si desea replicar archivos que contienen bibliotecas COM que deben registrarse, no puede copiar manualmente los archivos en el directorio de réplica del servidor de administración. Debe utilizar la consola de delegación y configuración para cargar cada archivo y registrar la biblioteca COM.

Réplica de varios archivos en los equipos cliente de DRA

Si tiene varios archivos que desea replicar entre el servidor de administración principal y los equipos cliente de DRA, puede copiar los archivos en el directorio de réplica del cliente del servidor de administración principal, que se encuentra en la siguiente ubicación:

```
{DRAInstallDir}\FileTransfer\Download
```

El directorio de réplica del cliente se crea durante la instalación de DRA.

El servidor de administración identifica automáticamente los archivos en la carpeta `Download` y replica los archivos en los servidores de administración secundarios durante la próxima sincronización programada. Después de la sincronización, DRA muestra los archivos cargados en la ventana Réplica de archivos de la consola de delegación y configuración. DRA descarga los archivos replicados en los equipos cliente de DRA la primera vez que estos se conectan a los servidores de administración tras la réplica.

Nota: Si desea replicar archivos que contienen bibliotecas COM que deben registrarse, no puede copiar los archivos en el directorio de descarga del servidor de administración. Debe utilizar la consola de delegación y configuración para cargar cada archivo y registrar la biblioteca COM.

Adición de marcas a eventos

Cuando se habilita la auditoría de los servicios de dominio de AD, los eventos de DRA se registran como generados por la cuenta de servicio de DRA o la cuenta de acceso al dominio, si se ha configurado. La adición de marcas a eventos lleva esta función un paso más allá al generar un evento de AD DS adicional que identifica al administrador asistente que realizó la operación.

Para que se generen estos eventos, debe configurar la auditoría de AD DS y habilitar la función de adición de marcas a eventos en el servidor de administración de DRA. Si se ha habilitado la adición de marcas a eventos, podrá ver los cambios que los administradores asistentes realizan en los informes de eventos de Change Guardian.

- ♦ Para configurar la auditoría de AD DS, consulte [Auditoría de AD DS \(https://technet.microsoft.com/en-us/library/cc731607\(v=ws.10\).aspx\)](https://technet.microsoft.com/en-us/library/cc731607(v=ws.10).aspx).
- ♦ Para configurar la integración de Change Guardian, consulte [Configuración de los servidores del Historial de cambios unificado](#).
- ♦ Para habilitar la adición de marcas a eventos, abra la consola de delegación y configuración como administrador de DRA y realice lo siguiente:
 1. Acceda a **Configuration Management** (Gestión de configuraciones) > **Update Administration Server Options** (Actualizar opciones del servidor de administración) > **Event Stamping** (Adición de marcas a eventos).
 2. Seleccione un tipo de objeto y haga clic en **Actualizar**.
 3. Seleccione el atributo que desea utilizar para la adición de marcas a eventos para ese tipo de objeto.

DRA admite actualmente la adición de marcas a eventos para usuarios, grupos, contactos, equipos y unidades administrativas.

DRA también requiere que los atributos existan en el esquema de AD para cada uno de los dominios gestionados. Debe tener esto en cuenta si añade dominios gestionados después de configurar la adición de marcas a eventos. Si añadiese un dominio gestionado que no incluyese el atributo seleccionado, las operaciones de ese dominio no se auditarían con los datos de adición de marcas a eventos.

DRA modificará esos atributos, por lo que debe seleccionar los atributos que DRA o cualquier otra aplicación del entorno no utilicen.

Para obtener más información sobre la adición de marcas a eventos, consulte [Funcionamiento de la adición de marcas a eventos](#).

Habilitación de varios administradores de grupos

Al habilitar la compatibilidad con la gestión de un grupo por varios administradores, se utiliza uno de los dos atributos por defecto para almacenar los administradores del grupo. El atributo al ejecutar Microsoft Exchange es `msExchCoManagedByLink`. El atributo por defecto al no ejecutar Microsoft Exchange es `nonSecurityMember`. Esta última opción se puede modificar. Sin embargo, es recomendable que se ponga en contacto con el servicio de asistencia técnica para determinar el atributo adecuado si necesita cambiar esta configuración.

Para habilitar la compatibilidad de varios administradores con los grupos:

- 1 En el panel izquierdo, haga clic en **Configuration Management** (Gestión de configuraciones).
- 2 En "Common Tasks" (Tareas comunes), en el panel derecho, haga clic en **Update Administration Server Options** (Actualizar opciones del servidor de administración).
- 3 En la pestaña "Enable Support for Group Multiple Managers" (Habilitar compatibilidad con varios administradores de grupos), seleccione la casilla de verificación **Enable support for group's multiple managers** (Habilitar compatibilidad con varios administradores del grupo).

Comunicaciones cifradas

Esta función permite habilitar o inhabilitar el uso de la comunicación cifrada entre el servidor de administración y los clientes de delegación y configuración y los de gestión de cuentas y recursos. Por defecto, DRA cifra las contraseñas de las cuentas. Esta función no cifra las comunicaciones del cliente Web o de PowerShell, que se gestiona por separado mediante certificados del servidor.

El uso de comunicaciones cifradas puede afectar al rendimiento. La comunicación cifrada está inhabilitada por defecto. Si habilita esta opción, los datos se cifran durante la comunicación entre las interfaces de usuario y el servidor de administración. DRA utiliza el cifrado estándar de Microsoft para la llamada a procedimiento remoto (RPC).

Para habilitar las comunicaciones cifradas, desplácese a **Configuration Management** (Gestión de configuraciones) > **Update Administration Server Options** (Actualizar las opciones del servidor de administración) > pestaña **General** y seleccione la casilla de verificación **Encrypted Communications** (Comunicaciones cifradas).

Nota: Para cifrar todas las comunicaciones entre el servidor de administración y las interfaces de usuario, debe disponer de los poderes adecuados, como los de la función integrada Configurar servidores y dominios.

Definición de atributos virtuales

Con los atributos virtuales, puede crear nuevas propiedades y asociarlas a usuarios, grupos, grupos dinámicos de distribución, contactos, equipos y unidades administrativas. Los atributos virtuales le permiten crear nuevas propiedades sin necesidad de ampliar el esquema de Active Directory.

Mediante atributos virtuales, puede añadir nuevas propiedades a objetos en Active Directory. Solo puede crear, habilitar, inhabilitar y asociar atributos virtuales, además de anular su asociación, en el servidor de administración principal. DRA almacenará los atributos virtuales que cree en AD LDS. DRA replica los atributos virtuales del servidor de administración principal en los servidores de administración secundarios durante el proceso de sincronización de MMS.

Puede gestionar los atributos virtuales con los poderes adecuados. La función Gestionar atributos virtuales otorga poderes para crear, habilitar, asociar, inhabilitar y ver atributos virtuales, así como anular su asociación.

Creación de atributos virtuales

Necesita disponer del poder *Crear atributos virtuales* para crearlos y del poder *Ver atributos virtuales* para visualizarlos.

Para crear un atributo virtual, desplácese a **Configuration Management** (Gestión de configuraciones) > **Virtual Attributes** (Atributos virtuales) > nodo **Managed Attributes** (Atributos gestionados) y haga clic en **New Virtual Attribute** (Nuevo atributo virtual) en el menú Tareas.

Asociación de atributos virtuales a objetos

Solo puede asociar atributos virtuales habilitados a objetos de Active Directory. Una vez que asocia un atributo virtual a un objeto, el atributo virtual está disponible como parte de las propiedades del objeto.

Para que los atributos virtuales se muestren a través de las interfaces de usuario de DRA, debe crear una página de propiedades personalizada.

Para asociar un atributo virtual a un objeto, desplácese a **Configuration Management** (Gestión de configuraciones) > **Virtual Attributes** (Atributos virtuales) > nodo **Managed Attributes** (Atributos gestionados) y seleccione **Associate** (Asociar) > (tipo de objeto).

Nota

- ♦ Solo puede asociar atributos virtuales a usuarios, grupos, grupos dinámicos de distribución, equipos, contactos y unidades administrativas.
 - ♦ Al asociar un atributo virtual a un objeto, DRA crea automáticamente dos poderes personalizados por defecto. Los administradores asistentes deben disponer de estos poderes personalizados para gestionar el atributo virtual.
-

Anulación de la asociación de atributos virtuales

Se puede anular la asociación de atributos virtuales de los objetos de Active Directory. Cualquier objeto nuevo que cree no mostrará el atributo virtual cuya asociación se ha anulado como parte de las propiedades del objeto.

Para anular la asociación de un atributo virtual de un objeto de Active Directory, desplácese a **Configuration Management** (Gestión de configuraciones) > **Virtual Attributes** (Atributos virtuales) > **Managed Classes** (Clases gestionadas) > nodo (tipo de objeto). Haga clic en el atributo virtual y seleccione **Disassociate** (Anular asociación).

Inhabilitación de los atributos virtuales

Puede inhabilitar los atributos virtuales si no se han asociado a un objeto de Active Directory. Al inhabilitar un atributo virtual, los administradores no pueden ver el atributo virtual ni asociarlo a un objeto.

Para inhabilitar un atributo virtual, desplácese a **Configuration Management** (Gestión de configuraciones) > **Managed Attributes** (Atributos gestionados). Haga clic en el atributo correspondiente en el panel de lista y seleccione **Inhabilitar**.

Configuración del almacenamiento en caché

El servidor de administración se encarga de la creación y el mantenimiento de la **memoria caché de cuentas** que contiene partes de Active Directory para los dominios gestionados. DRA utiliza la memoria caché de cuentas para mejorar el rendimiento al gestionar cuentas de usuario, grupos, contactos y cuentas de equipo.

Para programar el periodo de actualización de la memoria caché o ver su estado, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Nota: Para realizar actualizaciones incrementales de la memoria caché de cuentas en dominios que contienen subárboles gestionados, asegúrese de que la cuenta de servicio tenga acceso de lectura al contenedor Objetos suprimidos, así como a todos los objetos del dominio del subárbol. Puede usar la utilidad Objetos suprimidos para comprobar y delegar los poderes adecuados.

Actualizaciones completas o incrementales

Una actualización incremental de la memoria caché de cuentas solo actualiza los datos que han cambiado desde la última actualización. La actualización incremental le proporciona un método simplificado de mantenerse al día con los cambios de Active Directory. Utilice la actualización incremental para actualizar rápidamente la memoria caché de cuentas con el mínimo efecto en la actividad de su empresa.

Importante: Microsoft Server limita el número de usuarios simultáneos conectados a la sesión de WinRM/WinRS a cinco y el número de shells por usuario a cinco, así que asegúrese de que la misma cuenta de usuario esté limitada a cinco shells para los servidores secundarios de DRA.

Una actualización incremental actualiza los siguientes datos:

- ♦ Objetos nuevos y clonados
- ♦ Objetos suprimidos y movidos
- ♦ Pertenencias a grupos
- ♦ Todas las propiedades almacenadas en caché de los objetos modificados

Una actualización completa de la memoria caché de cuentas reconstruye la memoria caché de cuentas de DRA para el dominio especificado.

Nota: Al ejecutar una actualización completa de la memoria caché de cuentas, el dominio no estará disponible para los usuarios de DRA.

Actualización completa de la memoria caché de cuentas

Para actualizar la memoria caché de cuentas, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada "Configurar servidores y dominios".

Para llevar a cabo al instante una actualización completa de la memoria caché de cuentas:

- 1 Desplácese a **Configuration Management** (Gestión de configuraciones) > **Managed Domains** (Dominios gestionados).
- 2 Haga clic con el botón derecho en el dominio que desee y seleccione **Propiedades**.
- 3 Haga clic en **Actualizar ahora** en la pestaña **Full refresh** (Actualización completa).

Periodos programados por defecto

La frecuencia con la que debe actualizar la memoria caché de cuentas dependerá de la frecuencia con la que cambie su empresa. Utilice la actualización incremental para actualizar la memoria caché de cuentas con frecuencia, lo que garantiza que DRA disponga de la información más actualizada sobre Active Directory.

Por defecto, el servidor de administración lleva a cabo una actualización incremental de la memoria caché de cuentas con las siguientes frecuencias:

Tipo de dominio	Periodo de actualización programado por defecto
Dominios gestionados	Cada 5 minutos
Dominios de confianza	Cada hora

No se puede programar una actualización completa de la memoria caché de cuentas (FACR). Sin embargo, DRA ejecuta una FACR en las siguientes circunstancias:

- ◆ Después de configurar un dominio gestionado por primera vez.
- ◆ Después de actualizar DRA a una nueva versión completa desde una versión anterior.
- ◆ Después de instalar un paquete de servicios de DRA.

Las actualizaciones completas de la memoria caché de cuentas tardan varios minutos en completarse.

Observaciones

Debe actualizar periódicamente la memoria caché de cuentas para asegurarse de que DRA disponga de la información más reciente. Antes de realizar o programar una actualización de la memoria caché de cuentas, tenga en cuenta lo siguiente:

- ◆ Para realizar una actualización incremental de la memoria caché de cuentas, las cuentas de acceso o servicio del servidor de administración deben tener permiso para acceder a los objetos suprimidos en la instancia de Active Directory del dominio gestionado o de confianza.
- ◆ Si DRA realiza una actualización de la memoria caché de cuentas, el servidor de administración no incluirá los grupos de seguridad locales de los dominios de confianza. Como la memoria caché no contiene estos grupos, DRA no le permitirá añadir un grupo de seguridad local de dominio desde el dominio de confianza a un grupo local en el servidor miembro gestionado.
- ◆ Si omite un dominio de confianza de una actualización de la memoria caché de cuentas, el servidor de administración también omitirá ese dominio de la actualización de configuración del dominio.
- ◆ Si incluye un dominio de confianza omitido anteriormente en la actualización de la memoria caché de cuentas, realice una actualización completa de la memoria caché de cuentas para el dominio gestionado. Esto garantiza que la memoria caché de cuentas incluida en el servidor de administración del dominio gestionado refleje correctamente los datos de pertenencia a grupo en los dominios gestionados y de confianza.
- ◆ Si define el intervalo de actualización incremental de la memoria caché de cuentas en **Nunca**, el servidor de administración solo realizará actualizaciones completas de la memoria caché de cuentas. Una actualización completa de la memoria caché de cuentas puede tardar algún tiempo en completarse. Durante ese proceso, no se pueden gestionar los objetos de ese dominio.

- ♦ DRA no puede determinar automáticamente cuándo se realizan cambios mediante otras herramientas, como los Servicios de directorio de Microsoft. Las operaciones realizadas fuera de DRA pueden afectar a la precisión de la información almacenada en caché. Por ejemplo, si utiliza otra herramienta para añadir un buzón a una cuenta de usuario, no puede usar Exchange para gestionar ese buzón hasta que actualice la memoria caché de cuentas.
- ♦ Al realizar una actualización completa de la memoria caché de cuentas, las estadísticas de las últimas entradas a la sesión se conservan en la memoria caché. A continuación, el servidor de administración recopila la información más reciente de entrada a la sesión desde todos los controladores de dominio.

Habilitación de la recopilación de impresoras de Active Directory

La recopilación de impresoras de AD está inhabilitada por defecto. Para habilitarla, desplácese a **Configuration Management** (Gestión de configuraciones) > **Update Administration Server Options** (Actualizar opciones del servidor de administración) > pestaña **General** y seleccione la casilla de verificación **Collect Printers** (Recopilar impresoras).

AD LDS

Puede configurar la actualización de limpieza de AD LDS para que se ejecute según una programación para dominios específicos. La configuración por defecto es no actualizar "Nunca". También puede ver el estado de limpieza e información específica relacionada con la configuración de AD LDS (ADAM).

Para configurar la programación de limpieza de AD LDS o ver su estado, haga clic con el botón derecho en el nodo **Account and Resource Management** (Gestión de cuentas y recursos) > **Todos mis recursos gestionados** y seleccione **Propiedades** > **Adlds Cleanup Refresh Schedule** (Programación de la actualización de limpieza de AD LDS) o **Adlds Cleanup status** (Estado de la limpieza de AD LDS) respectivamente.

Para ver información de configuración de AD LDS (ADAM), desplácese a **Configuration Management** (Gestión de configuraciones) > **Update Server Options** (Actualizar opciones del servidor) > **ADAM Configuration** (Configuración de ADAM).

Grupo dinámico

Un grupo dinámico es aquel cuya pertenencia a grupo cambia según un conjunto definido de criterios que puede configurar en las propiedades del grupo. En las propiedades del dominio, puede configurar la actualización del grupo dinámico para que se ejecute según una programación de dominios específicos. La configuración por defecto es no actualizar "Nunca". También puede ver el estado de la actualización.

Para configurar la programación o ver el estado de actualización del grupo dinámico, haga clic con el botón derecho en el dominio que desee del nodo **Gestión de cuentas y recursos** > **Todos mis objetos gestionados** y seleccione **Propiedades** > **Dynamic group refresh** (Actualización del grupo dinámico) o **Dynamic group status** (Estado del grupo dinámico) respectivamente.

Para obtener más información sobre grupos dinámicos, consulte [Grupos dinámicos de DRA](#).

Configuración de la Papelera

Puede habilitar o inhabilitar la Papelera para cada dominio u objeto de Microsoft Windows dentro de cada dominio, y configurar cuándo y cómo desea que se realice la limpieza de la Papelera.

Para obtener información detallada sobre el uso de la Papelera, consulte [Papelera](#).

Habilitación de la Papelera

Puede habilitar la Papelera para dominios específicos de Microsoft Windows y para objetos dentro de esos dominios. Por defecto, DRA habilita la Papelera para cada dominio que gestiona y todos los objetos del dominio. Debe ser miembro del grupo de admin. de DRA o de administradores asistentes de configuración de DRA para habilitar la Papelera.

Si su entorno incluye la siguiente configuración, utilice la utilidad Papelera para habilitar esta función:

- ♦ DRA gestiona un subárbol de este dominio.
- ♦ Las cuentas de acceso o servicio del servidor de administración no tienen permiso para crear el contenedor de la Papelera, desplazar las cuentas a ese contenedor ni modificar las cuentas incluidas en él.

También puede usar la utilidad Papelera para comprobar los permisos de las cuentas de acceso o servicio del servidor de administración en el contenedor de la Papelera.

Para habilitar la Papelera, haga clic con el botón derecho en el dominio que desee en el nodo **Papelera** y seleccione **Disable Recycle Bin** (Habilitar la Papelera).

Inhabilitación de la Papelera

Puede inhabilitar la Papelera para dominios específicos de Microsoft Windows y para objetos dentro de esos dominios. Si una Papelera inhabilitada contiene cuentas, no podrá ver, suprimir permanentemente ni restaurar esas cuentas.

Debe ser miembro del grupo de admin. de DRA o de administradores asistentes de admin. de configuración de DRA para inhabilitar la Papelera.

Para inhabilitar la Papelera, haga clic con el botón derecho en el dominio que desee en el nodo **Papelera** y seleccione **Enable Recycle Bin** (Inhabilitar la Papelera).

Configuración de los objetos y la limpieza de la Papelera

La configuración por defecto de limpieza de la Papelera es diariamente. Puede cambiar esta configuración para que la limpieza de la Papelera se realice cada x días. Durante la limpieza programada, la Papelera suprime los objetos que tienen una antigüedad superior a la cantidad de días que ha configurado para cada tipo de objeto. La configuración por defecto para cada tipo consiste en suprimir objetos con más de 1 día. Puede personalizar el comportamiento de la limpieza de la Papelera. Para ello, inhabilite, vuelva a habilitar y defina la antigüedad de los objetos que se suprimirán para cada tipo de objeto.

Para configurar la limpieza de la Papelera, seleccione el dominio que desee en la consola de delegación y configuración y desplácese a **Tareas > Propiedades > pestaña Papelera**.

Configuración de informes

En las siguientes secciones, se proporciona información conceptual sobre los informes de gestión de DRA y los recopiladores de informes que puede habilitar. Para acceder al asistente que le permitirá configurar los recopiladores, desplácese a **Configuration Management** (Gestión de configuraciones) > **Update Reporting Service Configuration** (Actualizar la configuración del servicio de elaboración de informes).

Configuración del recopilador de Active Directory

El recopilador de Active Directory recopila un conjunto específico de atributos de Active Directory para cada usuario, grupo, contacto, equipo, unidad administrativa y grupo dinámico de distribución gestionados en DRA. Estos atributos se almacenan en la base de datos de informes y se utilizan para generar informes en la consola de elaboración de informes.

Puede configurar el recopilador de Active Directory para especificar los atributos que se recopilarán y almacenarán en la base de datos de informes. También puede configurar el servidor de administración de DRA en el que se ejecutará el recopilador.

Configuración del recopilador de DRA

El recopilador de DRA recopila información sobre la configuración de DRA y la almacena en la base de datos de informes, que se utiliza para generar informes en la consola de elaboración de informes.

Para habilitar el recopilador de DRA, debe especificar el servidor de administración de DRA en el que se ejecutará el recopilador. Como práctica recomendada, debe programar el recopilador de DRA para que se ejecute después de que se ejecute correctamente el recopilador de Active Directory y en los momentos en que el servidor tenga una menor carga o fuera del horario laboral habitual.

Configuración del recopilador de inquilinos de Office 365

El recopilador de inquilinos de Office 365 recopila información sobre los usuarios gestionados que se sincronizan con Office 365 y la almacena en la base de datos de informes, que se utiliza para generar informes en la consola de elaboración de informes.

Para habilitar el recopilador de Office 365, debe especificar el servidor de administración de DRA en el que se ejecutará el recopilador.

Nota: El inquilino de Office 365 solo puede ejecutar una recopilación satisfactoria después de que el recopilador de Active Directory del dominio correspondiente ejecute correctamente una recopilación.

Configuración del recopilador de informes de gestión

El recopilador de informes de gestión recopila información de auditoría de DRA y la almacena en la base de datos de informes, que se utiliza para generar informes en la consola de elaboración de informes. Al habilitar el recopilador, puede configurar la frecuencia con la que se actualizan los datos en la base de datos para las consultas que se ejecutan en la herramienta de elaboración de informes de DRA.

Esta configuración requiere que la cuenta de servicio de DRA disponga del permiso **sysadmin** en la instancia de SQL Server del servidor de elaboración de informes. A continuación, se indican las opciones que se pueden configurar:

- ♦ **Audit Export Data Interval** (Intervalo de exportación de datos de auditoría): se trata del intervalo en el que se exportan los datos de auditoría del registro de seguimiento de DRA (LAS) en la base de datos "SMCubeDepot" de SQL Server.
- ♦ **Management Report Summarization Interval** (Intervalo de resumen de informes de gestión): se trata del intervalo en el que los datos de auditoría de la base de datos de SMCubeDepot se transfieren a la base de datos de informes de DRA donde pueden consultarse con la herramienta de elaboración de informes de DRA.

Recopilación de las estadísticas de las últimas entradas a la sesión

Puede configurar DRA para que recopile las estadísticas de las últimas entradas a la sesión de todos los controladores de dominio del dominio gestionado. Para habilitar y programar la recopilación de las estadísticas de las últimas entradas a la sesión, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

La función de recopilación de las estadísticas de las últimas entradas a la sesión está inhabilitadas por defecto. Si desea recopilar los datos de las estadísticas de las últimas entradas a la sesión, debe habilitar esta función. Una vez que habilite la recopilación de estadísticas de las últimas entrada a la sesión, podrá ver estas estadísticas para un usuario específico o mostrar el estado de la recopilación de estadísticas de las últimas entradas a la sesión.

Para recopilar las estadísticas de las últimas entradas a la sesión:

- 1 Desplácese a **Configuration Management** (Gestión de configuraciones) > **Managed Domains** (Dominios gestionados).
- 2 Haga clic con el botón derecho en el dominio que desee y seleccione **Propiedades**.
- 3 Haga clic en la pestaña **Last logon schedule** (Programación de últimas entradas a la sesión) para configurar la recopilación de estadísticas de las últimas entradas a la sesión.

Historial de cambios unificado

Por defecto, la función de Historial de cambios unificado (UCH, Unified Change History) permite generar informes de los cambios realizados por DRA.

Delegación de poderes del Historial de cambios unificado

Para gestionar el Historial de cambios unificado, asigne la función de administración del servidor del Historial de cambios unificado o los poderes correspondientes mostrados a continuación a los administradores asistentes:

- ♦ Eliminar la configuración del servidor del Historial de cambios unificado.
- ♦ Definir la información de configuración del Historial de cambios unificado.
- ♦ Ver la información de configuración del Historial de cambios unificado.

Para delegar los poderes de UCH:

- 1 Haga clic en **Poderes** en el nodo de gestión de delegación y utilice la función de búsqueda de objetos para buscar y seleccionar los objetos de UCH que desee.
- 2 Haga clic en una de los poderes de UCH seleccionados y seleccione **Delegate Roles and Powers** (Delegar funciones y poderes).
- 3 Busque el usuario específico, el grupo o el grupo de administradores asistentes al que desea delegar poderes.
- 4 Utilice el **Selector de objetos** para buscar y añadir los objetos que desee y, a continuación, haga clic en **Roles and Powers** (Funciones y poderes) en el **Asistente**.
- 5 Haga clic en **ActiveViews** y utilice el **Selector de objetos** para buscar y añadir los objetos que desee.
- 6 Haga clic en **Siguiente** y, a continuación, en **Finalizar** para completar el proceso de asignación de delegación.

Configuración de los servidores del Historial de cambios unificado

Para configurar los servidores UCH:

- 1 Lance la consola Web y entre a la sesión con las 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 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 proceda.

Servidor de flujo de trabajo

Para utilizar la Automatización del flujo de trabajo en DRA, debe instalar el Motor de flujo de trabajo en una instancia de Windows Server y configurar el servidor de Automatización del flujo de trabajo mediante 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**.

Para obtener información acerca de cómo instalar el Motor de flujo de trabajo, consulte [Workflow Automation Administrator Guide](#) (Guía del administrador de Automatización del flujo de trabajo).

3.1.4 Configurar el cliente de delegación y configuración

El cliente de delegación y configuración proporciona acceso a las tareas de configuración y delegación, y satisface las necesidades de gestión empresarial, desde la administración distribuida hasta la aplicación de directivas. Mediante la consola de delegación y configuración, puede definir el modelo de seguridad y las configuraciones de servidor que necesita para gestionar su empresa de forma eficaz.

Para configurar el cliente de delegación y configuración:

- 1 Lance el cliente de delegación y configuración, y desplácese a **Configuration Management** (Gestión de configuraciones) > **Update Administration Server Options** (Actualizar opciones del servidor de administración).
- 2 Haga clic en la pestaña **Client Options** (Opciones de cliente) y defina los valores que prefiera en las opciones de configuración que se muestran:
 - ♦ "Allow users to search by ActiveView" (Permitir a los usuarios buscar por ActiveView)
 - ♦ "Hide source-only objects from console lists" (Ocultar los objetos solo de origen de las listas de consolas)
 - ♦ "Show advanced Active Directory objects" (Mostrar objetos avanzados de Active Directory)
 - ♦ "Show Security command" (Mostrar el comando de seguridad)
 - ♦ "Show resource and shared mailboxes when searching for users" (Mostrar recurso y buzones compartidos al buscar usuarios)
 - ♦ "Default user UPN suffix to current domain" (Sufijo de UPN de usuario por defecto en el dominio actual)
 - ♦ "Maximum items editable at a time (Multi-select)" (Número máximo de elementos que se pueden editar cada vez, selección múltiple)
 - ♦ Opciones de búsqueda
 - ♦ "Carriage Return Option" (Opción de retorno de carro)
 - ♦ "Exchange Mailbox Storage Limits Units" (Unidades de los límites de almacenamiento de los buzones de Exchange)

3.1.5 Configurar el cliente Web

Puede configurar la consola Web para realizar la autenticación con tarjetas inteligentes o mediante la autenticación multifactor y personalizar también la marca con su propio logotipo y título de la aplicación.

Inicio de la consola Web

Puede iniciar la consola Web desde cualquier equipo, o dispositivo iOS o Android que ejecute un navegador Web. Para iniciar la consola, especifique la dirección URL adecuada en el campo de dirección del navegador Web. Por ejemplo, si ha instalado el componente Web en el equipo HOUser, escriba `https://HOUser/draclient` en el campo de dirección del navegador Web.

Nota: Para que se muestre la información más reciente de la cuenta y de Microsoft Exchange en la consola Web, configure el navegador Web para que compruebe si hay versiones más recientes de las páginas en caché en cada visita.

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. Una vez establecida, la configuración de conexión es la misma tanto para los administradores como para los administradores asistentes en el panel desplegable **Opciones** al entrar a la consola Web.

- ♦ 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 a la sesión - Opciones	Descripciones de las opciones de conexión
Siempre	Ninguno	Se inhabilitan las configuraciones de la opción.
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.
	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.

Configuración de la conexión	Pantalla de entrada a la sesión - Opciones	Descripciones de las opciones de conexión
	Conectarse a un servidor DRA que gestiona un dominio específico	<p>El usuario especifica un dominio gestionado y elige una opción de conexión:</p> <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. Una vez establecida, la configuración de conexión es la misma tanto para los administradores como para los administradores asistentes en el panel desplegable **Opciones** al entrar a la consola Web.

- ◆ 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 a la sesión - Opciones	Descripciones de las opciones de conexión
Siempre	Ninguno	Se inhabilitan las configuraciones de la opción.
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	<p>El usuario especifica un dominio gestionado y elige una opción de conexión:</p> <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.
	Conectar al servidor REST por defecto	Se selecciona el servidor REST por defecto y se inhabilita la configuración del servidor REST.

Configuración de la conexión	Pantalla de entrada a la sesión - Opciones	Descripciones de las opciones de conexión
	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](#).

Autenticación

Esta sección contiene información para configurar la autenticación con tarjeta inteligente, la autenticación de Windows y la autenticación multifactor mediante la integración de Advanced Authentication.

Autenticación de tarjeta inteligente

Para configurar la consola Web para que acepte a un usuario en función de las credenciales del cliente de la tarjeta inteligente, debe configurar Internet Information Services (IIS) y el archivo de configuración de los servicios REST.

Importante: Asegúrese de que los certificados de la tarjeta inteligente se hayan instalado también en el almacén de certificados raíz del servidor Web debido a que IIS debe poder encontrar certificados que coincidan con los que se incluyen en la tarjeta.

- 1 Instale los componentes de autenticación en el servidor Web.
 - 1a Inicie el gestor del servidor.
 - 1b Haga clic en [Servidor Web \(IIS\)](#).
 - 1c Acceda a la sección Role Services (Servicios de función) y haga clic en [Add Role Services](#) (Añadir servicios de función).
 - 1d Vaya al nodo de servicios de función de seguridad y seleccione [Windows Authentication](#) (Autenticación de Windows) y [Client Certificate Mapping Authentication](#) (Autenticación de asignaciones de certificado de cliente).
- 2 Habilite la autenticación en el servidor Web.
 - 2a Inicie el [Administrador de IIS](#).
 - 2b Seleccione el servidor Web.
 - 2c Busque el icono de [Autenticación](#) que aparece debajo de la sección de IIS y haga doble clic en él.
 - 2d Habilite "Active Directory Client Certificate Authentication" (Autenticación de asignaciones de certificado de cliente) y "Windows Authentication" (Autenticación de Windows).

- 3 Configure el cliente de DRA.
 - 3a Seleccione el cliente de DRA.
 - 3b Busque el icono de **Autenticación** que aparece debajo de la sección de IIS y haga doble clic en él.
 - 3c Habilite "Windows Authentication" (Autenticación de Windows) y desactive "Anonymous Authentication" (Autenticación anónima).
- 4 Habilite los certificados SSL y de cliente en el cliente de DRA.
 - 4a Busque el icono de **Servicios SSL** que aparece debajo de la sección de IIS y haga doble clic en él.
 - 4b Seleccione **Require SSL** (Requerir SSL) y, a continuación, **Require** (Requerir) en "Client certificates" (Certificados de cliente).

Sugerencia: Si la opción está disponible, seleccione **Require 128-bit SSL** (Requerir SSL de 128 bits).

- 5 Configure la aplicación Web de los servicios REST.
 - 5a Seleccione la aplicación Web de los servicios REST.
 - 5b Busque el icono de **Autenticación** que aparece debajo de la sección de IIS y haga doble clic en él.
 - 5c Habilite "Windows Authentication" (Autenticación de Windows) y desactive "Anonymous Authentication" (Autenticación anónima).
- 6 Habilite los certificados SSL y de cliente en la aplicación Web de los servicios REST.
 - 6a Busque el icono de **Servicios SSL** que aparece debajo de la sección de IIS y haga doble clic en él.
 - 6b Seleccione **Require SSL** (Requerir SSL) y, a continuación, **Require** (Requerir) en "Client certificates" (Certificados de cliente).

Sugerencia: Si la opción está disponible, seleccione **Require 128-bit SSL** (Requerir SSL de 128 bits).

- 7 Configure el archivo del servicio Web WCF.
 - 7a Seleccione la aplicación Web de los servicios REST y cambia a la vista de contenido.
 - 7b Busque el archivo `.svc` y haga clic con el botón derecho en él.
 - 7c Seleccione **Switch to Features View** (Cambiar a la vista de funciones).
 - 7d Busque el icono de **Autenticación** que aparece debajo de la sección de IIS y haga doble clic en él.
 - 7e Habilite "Anonymous Authentication" (Autenticación anónima) e inhabilite todos los demás métodos de autenticación.
- 8 Edite el archivo de configuración de servicios REST.
 - 8a Utilice un editor de texto para abrir el archivo
C:\inetpub\wwwroot\DRAClient\rest\web.config.
 - 8b Busque la línea `<authentication mode="None" />` y suprimala.
 - 8c Añada las líneas mostradas a continuación debajo de la línea `<system.serviceModel>`:

```
<services> <service name="NetIQ.DRA.DRARestProxy.RestProxy"> <endpoint address=""  
binding="webHttpBinding" bindingConfiguration="webHttpEndpointBinding"  
name="webHttpEndpoint" contract="NetIQ.DRA.DRARestProxy.IRestProxy" /> </service> </  
services>
```

8d Añada las siguientes líneas debajo de la línea `<serviceDebug includeExceptionDetailInFaults="false"/>`:

```
<serviceAuthorization impersonateCallerForAllOperations="true" /> <serviceCredentials>
<clientCertificate> <authentication mapClientCertificateToWindowsAccount="true" /> </
clientCertificate> </serviceCredentials>
```

8e Añada las siguientes líneas **encima** de la línea `<serviceHostingEnvironment multipleSiteBindingsEnabled="true" />`:

```
<bindings> <webHttpBinding> <binding name="webHttpEndpointBinding"> <security
mode="Transport"> <transport clientCredentialType="Certificate" /> </security> </binding> </
webHttpBinding> </bindings>
```

9 Guarde el archivo y reinicie el servidor IIS.

Autenticación de Windows

Para habilitar la autenticación de Windows en la consola Web, debe configurar Internet Information Services (IIS) y el archivo de configuración de los servicios REST.

- 1 Abra Gestor IIS.
- 2 En el panel Conexiones, localice la aplicación Web de servicios REST y selecciónela.
- 3 En el panel derecho, vaya a la sección IIS y haga doble clic en **Autenticación**.
- 4 Habilite **Windows Authentication** (Autenticación de Windows) e inhabilite todos los demás métodos de autenticación.
- 5 Utilice un editor de texto para abrir el archivo `C:\inetpub\wwwroot\DRAClient\rest\web.config` y busque la línea `<authentication mode="None" />`.
- 6 Cambie "None" por "Windows" y guarde el archivo.
- 7 Reinicie el servidor IIS.

Autenticación multifactor con Advanced Authentication

Advanced Authentication Framework (AAF) es nuestro paquete de software principal que 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.

Advanced Authentication admite los siguientes protocolos de comunicación para la seguridad:

- ♦ TLS 1.2 (valor por defecto), TLS 1.1 y TLS 1.0
- ♦ SSL 3.0

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.

Existen tres tipos de categorías de autenticación o factores:

- ♦ *Conocimientos*. Esta categoría requiere que conozca información específica, como una contraseña o un código de activación.
- ♦ *Posesión*. Esta categoría requiere que tenga un dispositivo de autenticación, como una tarjeta o un teléfono inteligentes.
- ♦ *Cuerpo*. Esta categoría requiere que utilice una parte de su anatomía, como su huella dactilar, como método de verificación.

Cada factor de autenticación contiene al menos un método de autenticación. Un método de autenticación es una técnica específica que puede utilizar para establecer la identidad de un usuario, por ejemplo, mediante el uso de una huella digital o la solicitud de una contraseña.

Puede considerar un proceso de autenticación como seguro si utiliza más de un tipo de método de autenticación; por ejemplo, si requiere una contraseña y una huella digital.

Advanced Authentication admite los siguientes métodos de autenticación:

- ♦ Contraseña de LDAP
- ♦ Servicio de autenticación remota telefónica de usuario (RADIUS, Remote Authentication Dial-In User Service)
- ♦ Teléfono inteligente

Sugerencia: El método de teléfono inteligente requiere que el usuario descargue una aplicación para iOS o Android. Para obtener más información, consulte *Advanced Authentication - Smartphone Applications User Guide* (Advanced Authentication: guía del usuario de las aplicaciones para teléfonos inteligentes) en el [sitio Web de documentación de NetIQ](#).

Utilice la información de las siguientes secciones para configurar la consola Web a fin de utilizar la autenticación multifactor.

Importante: Aunque algunos de los pasos descritos en las siguientes secciones se realizan dentro de la consola Web, la mayoría del proceso de configuración de autenticación multifactor requiere acceso a AAF. En estos procedimientos, se presupone que ha instalado AAF y tiene acceso a la documentación de ayuda de AAF.

Adición de repositorios a Advanced Authentication Framework

El primer paso para configurar la consola Web para utilizar la autenticación multifactor consiste en añadir todos los dominios de Active Directory que contienen los administradores de DRA y los administradores asistentes gestionados por DRA a AAF. Estos dominios se denominan repositorios y contienen los atributos de identidad de los usuarios y grupos que desea autenticar.

- 1 Entre al portal de administración de AAF con un nombre de usuario y contraseña de nivel de administrador.
- 2 Vaya al panel izquierdo y haga clic en **Repositories** (Repositorios).
- 3 Haga clic en **Añadir**.
- 4 Complete el formulario.

Sugerencia: El **tipo de LDAP** es **AD**.

Sugerencia: Escriba un nombre de usuario y una contraseña de nivel de administrador en los campos correspondientes.

- 5 Haga clic en **Add Server** (Añadir servidor).
- 6 Escriba la dirección IP del servidor LDAP en el campo **Address** (Dirección).
- 7 Haga clic en **Save** (Guardar).
- 8 Repita los pasos 3 a 7 para todos los demás repositorios de AD gestionados por DRA.
- 9 En cada repositorio que aparezca en la página "Repositories" (Repositorios), haga clic en **Sync now** (Sincronizar ahora) para sincronizarlo con el servidor AAF.

Creación de cadenas de autenticación

Una cadena de autenticación contiene al menos un método de autenticación. Se llamará a los métodos de la cadena en el orden en el que se añadieron a esta. Para que un usuario logre autenticarse, debe superar todos los métodos de la cadena. Por ejemplo, puede crear una cadena que contenga el método de contraseña LDAP y el método SMS. Cuando un usuario intenta autenticarse con esta cadena, debe autenticarse primero con su contraseña LDAP; a continuación, se le enviará un mensaje de texto a su teléfono móvil con una contraseña de un solo uso. Después de que introduzca la contraseña, todos los métodos de la cadena se habrán cumplido y la autenticación se completará satisfactoriamente. Se puede asignar una cadena de autenticación a un usuario o un grupo específicos.

Para crear una cadena de autenticación:

- 1 Entre al portal de administración de AAF con un nombre de usuario y contraseña de nivel de administrador.
- 2 Vaya al panel izquierdo y haga clic en **Chains** (Cadenas). En el panel derecho, se muestra una lista de las cadenas disponibles.
- 3 Haga clic en **Añadir**.
- 4 Complete el formulario. Todos los campos son obligatorios.

Importante: Añada los métodos de autenticación en el orden en que deben llamarse, es decir, si desea que el usuario introduzca primero una contraseña LDAP, añádala primero.

Importante: Asegúrese de que el conmutador **Apply if used by endpoint owner** (Aplicar si se utiliza por el propietario del puesto final) se haya establecido en OFF (desactivado).

- 5 Cambie **Is enabled** (Está habilitado) a ON (activado).
- 6 Escriba los nombres de las funciones o grupos que se someterán a la solicitud de autenticación en el campo **Roles & Groups** (Funciones y grupos).

Sugerencia: Si desea que la cadena se aplique a todos los usuarios, escriba `all users` (todos los usuarios) en el campo **Roles & Groups** (Funciones y grupos) y seleccione **All Users** (Todos los usuarios) en la lista desplegable resultante.

Todos los usuarios o los grupos que seleccione se añadirán debajo del campo **Roles & Groups** (Funciones y grupos).

- 7 Haga clic en **Save** (Guardar).

Creación de eventos de autenticación

Un evento de autenticación lo activa una aplicación (en ese caso, la consola Web) que desea que se autentique un usuario. Se debe asignar al menos una cadena de autenticación al evento para que, cuando se active el evento, se llame a los métodos de la cadena asociada con el evento para autenticar al usuario.

Un puesto final es el dispositivo real, como un equipo o un teléfono inteligente, que ejecuta el software que activa el evento de autenticación. DRA registrará el puesto final en AAF después de crear el evento.

Puede utilizar el recuadro de lista blanca de puestos finales para restringir el acceso a un evento a puestos finales específicos, o bien puede permitir que todos los puestos finales accedan al evento.

Para crear un evento de autenticación:

- 1 Entre al portal de administración de AAF con un nombre de usuario y contraseña de nivel de administrador.
- 2 Vaya al panel izquierdo y haga clic en **Events** (Eventos). En el panel derecho, se muestra una lista de los eventos disponibles.
- 3 Haga clic en **Añadir**.
- 4 Complete el formulario. Todos los campos son obligatorios.

Importante: Asegúrese de que el conmutador **Is enabled** (Está habilitado) se haya establecido en ON (activado).

- 5 Si desea restringir el acceso a puestos finales específicos, vaya a la sección de la lista blanca de puestos finales y desplace los puestos finales seleccionados de la lista *Available* (Disponibles) a la lista *Used* (Usados).

Sugerencia: Si no hay ningún puesto final en la lista *Used* (Usados), el evento estará disponible para todos los puestos finales.

Habilitación de la consola Web

Después de configurar cadenas y eventos, puede entrar a la consola Web como administrador y habilitar Advanced Authentication.

Una vez habilitada la autenticación, todos los usuarios deberán autenticarse mediante AAF para que se les conceda acceso a la consola Web.

Importante: Antes de habilitar la consola Web, debe haberse inscrito en los métodos de autenticación que la consola Web utilizará para la autenticación de usuarios. Consulte *Advanced Authentication Framework User Guide* (Guía del usuario de Advanced Authentication Framework) para obtener información sobre cómo inscribirse en los métodos de autenticación.

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.

Sugerencia: Después de guardar la configuración, se creará el puesto final en AAF. Para verlo o editarlo, entre al portal de administración de AAF con un nombre de usuario y una contraseña de nivel de administrador y haga clic en **Endpoints** (Puestos finales) en el panel izquierdo.

Pasos finales

- 1 Entre al portal de administración de AAF con un nombre de usuario y una contraseña de nivel de administrador y haga clic en **Events** (Eventos) en el panel izquierdo.
- 2 Edite cada uno de los eventos de la consola Web:
 - 2a Abra el evento para editarlo.
 - 2b Vaya a la sección de la lista blanca de puestos finales y desplace el puesto final que creó al configurar la consola Web de la lista **Available** (Disponibles) a la lista **Used** (Usados). Esto garantizará que solo la consola Web pueda utilizar estos eventos.
- 3 Haga clic en **Save** (Guardar).

3.2 Conexión de sistemas gestionados

En esta sección, se proporciona información para conectar y configurar sistemas gestionados relacionados con los dominios y los componentes de Microsoft Exchange, entre los que se incluyen Carpetas públicas, Exchange, Office 365 y Skype Empresarial Online.

3.2.1 Gestión de dominios de Active Directory

Puede añadir nuevos dominios y equipos gestionados mediante el cliente de delegación y configuración después de instalar el servidor de administración. También puede añadir subárboles y dominios de confianza, y configurar cuentas de acceso al dominio y de Exchange para ellos. Para añadir dominios y equipos gestionados, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Nota: Cuando termine de añadir dominios gestionados, asegúrese de que se hayan establecido correctamente las programaciones de actualización de caché de cuentas de esos dominios.

Para añadir dominios y equipos gestionados:

- 1 Desplácese a **Configuration Management** (Gestión de configuraciones) > **New Managed Domain** (Nuevo dominio gestionado).
- 2 Especifique el nombre del dominio o el equipo que desea gestionar y, a continuación, haga clic en **Siguiente**.
- 3 En la pestaña "Access account" (Cuenta de acceso), especifique las credenciales de la cuenta que desea que utilice DRA para acceder a este dominio o equipo. Por defecto, DRA utiliza la cuenta de servicio del servidor de administración.
- 4 Revise el resumen y haga clic en **Finalizar**.
- 5 Para comenzar a gestionar objetos desde este dominio o equipo, actualice la configuración del dominio.

Especificar cuentas de acceso al dominio

En cada dominio o subárbol gestionados, puede especificar la cuenta que se utilizará en lugar de la cuenta de servicio del servidor de administración para acceder a ese dominio. Esta cuenta alternativa se denomina cuenta de acceso. Para configurar una cuenta de acceso, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Para especificar una cuenta de acceso para un servidor miembro, debe tener permiso para gestionar el dominio en el que se encuentra el miembro del dominio. Solo puede gestionar miembros del dominio si existen en un dominio gestionado al que puede acceder a través del servidor de administración.

Para especificar una cuenta de acceso:

- 1 Desplácese al nodo **Configuration Management** (Gestión de configuraciones) > **Managed Domains** (Dominios gestionados).
- 2 Haga clic con el botón derecho en el dominio o subárbol para el que desea especificar una cuenta de acceso y haga clic en **Propiedades**.
- 3 En la pestaña "Domain access account" (Cuenta de acceso al dominio), haga clic en **Use the following account to access this domain** (Utilizar la siguiente cuenta para acceder al dominio).
- 4 Especifique y confirme las credenciales para la cuenta y haga clic en **Aceptar**.

Para obtener información sobre la configuración de esta cuenta con privilegios mínimos, consulte [Cuentas de acceso de DRA con privilegios mínimos](#).

Especificar cuentas de acceso a Exchange

En cada dominio de DRA, puede gestionar objetos de Exchange mediante la cuenta de acceso al dominio de DRA o una cuenta de acceso a Exchange independiente. Para configurar una cuenta de acceso a Exchange, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Importante: Microsoft Server limita el número de usuarios simultáneos conectados a la sesión de WinRM/WinRS a cinco y el número de shells por usuario a cinco, así que asegúrese de que la misma cuenta de usuario esté limitada a cinco shells para los servidores secundarios de DRA.

Para especificar una cuenta de acceso a Exchange:

- 1 Desplácese al nodo **Configuration Management** (Gestión de configuraciones) > **Managed Domains** (Dominios gestionados).
- 2 Haga clic con el botón derecho en el dominio o subárbol para el que desea especificar una cuenta de acceso y haga clic en **Propiedades**.
- 3 En la pestaña "Exchange access account" (Cuenta de acceso a Exchange), haga clic en **Use the following account to access all Exchange servers** (Utilizar la siguiente cuenta para acceder a todos los servidores de Exchange).
- 4 Especifique y confirme las credenciales para la cuenta y haga clic en **Aceptar**.

Para obtener información sobre la configuración de esta cuenta con privilegios mínimos, consulte [Cuentas de acceso de DRA con privilegios mínimos](#).

Adición de un subárbol gestionado

Puede añadir subárboles gestionados y ausentes de dominios específicos de Microsoft Windows después de instalar el servidor de administración. Para añadir un subárbol gestionado, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios.

Para obtener información sobre las versiones compatibles de Microsoft Windows, consulte [Requisitos del servidor de administración de DRA](#).

Al gestionar un subárbol de un dominio de Windows, puede utilizar DRA para proteger un departamento o una división dentro de un dominio corporativo de mayor tamaño.

Por ejemplo, puede especificar el subárbol Houston en el dominio `SOUTHWEST`, lo que permite a DRA gestionar de forma segura solo esos objetos incluidos en la unidad administrativa de Houston y sus unidades administrativas secundarias. Esta flexibilidad permite gestionar uno o varios subárboles sin que sea necesario disponer de permisos administrativos para todo el dominio.

Nota

- ♦ Para garantizar que la cuenta especificada tenga permisos para gestionar este subárbol y realizar actualizaciones incrementales de la memoria caché de cuentas, utilice la herramienta Objetos suprimidos para comprobar y delegar los permisos correspondientes.
 - ♦ Cuando termine de añadir subárboles gestionados, asegúrese de que se hayan establecido correctamente las programaciones de actualización de caché de cuentas de los dominios correspondientes.
-

Para añadir un subárbol gestionado:

- 1 Desplácese a **Configuration Management** (Gestión de configuraciones) > **New Manage Domain** (Gestionar nuevo dominio).
- 2 En la pestaña "Domain or server" (Dominio o servidor), haga clic en **Manage a domain** (Gestionar un dominio) y especifique el dominio del subárbol del que desea gestionar.
- 3 Especifique el dominio del subárbol que desea gestionar.
- 4 Seleccione **Manage a subtree of this domain** (Gestionar un subárbol de este dominio) y, a continuación, haga clic en **Siguiente**.
- 5 En la pestaña "Subtrees" (Subárboles), haga clic en **Añadir** para especificar el subárbol que desea gestionar. Puede especificar varios subárboles.
- 6 En la pestaña "Access account" (Cuenta de acceso), especifique las credenciales de la cuenta que desea que utilice DRA para acceder a este subárbol. Por defecto, DRA utiliza la cuenta de servicio del servidor de administración.
- 7 Revise el resumen y haga clic en **Finalizar**.
- 8 Para empezar a gestionar objetos de este subárbol, actualice la configuración del dominio.

Adición de un dominio de confianza

Los dominios de confianza permiten la autenticación de usuarios en sistemas gestionados de todo el entorno administrado. Una vez que haya añadido un dominio de confianza, puede especificar las cuentas de dominio y de acceso a Exchange, programar actualizaciones de la memoria caché y realizar otras acciones en las propiedades del dominio, al igual que en un dominio gestionado.

Para añadir un dominio de confianza:

- 1 En el nodo **Configuration Management** (Gestión de configuraciones) > **Managed Domains** (Dominios gestionados), seleccione el dominio gestionado que tiene un dominio de confianza asociado.
- 2 Haga clic en **Trusted domains** (Dominios de confianza) en el panel de detalles. El panel de detalles debe activarse en el menú Ver.
- 3 Haga clic con el botón derecho en el dominio de confianza y seleccione **Propiedades**.
- 4 Desactive la casilla **Ignore this trusted domain** (Omitir este dominio de confianza) y aplique los cambios.

Nota: Al añadir un dominio de confianza, se iniciará una actualización completa de la memoria caché de cuentas, aunque se le notificará de esta acción mediante un mensaje de confirmación cuando haga clic en **Aplicar**.

3.2.2 Conexión de carpetas públicas

DRA permite gestionar las carpetas públicas de Microsoft Exchange. Puede gestionar algunas de las propiedades de las carpetas públicas con DRA mediante la configuración de los dominios del bosque de carpetas públicas y la concesión de poderes a los administradores asistentes.

Importante: Para gestionar la administración de carpetas públicas, debe habilitar la compatibilidad con Microsoft Exchange en DRA y disponer de los poderes correspondientes.

- ♦ Para obtener información sobre cómo habilitar Microsoft Exchange, consulte [Habilitación de la compatibilidad con Microsoft Exchange](#).
- ♦ Para obtener información sobre los permisos de cuenta, consulte [Cuentas de acceso de DRA con privilegios mínimos](#).

Para configurar la compatibilidad con las carpetas públicas de Exchange:

- 1 Haga clic con el botón derecho en **Managed Public Folder Forests** (Bosque de carpetas públicas gestionadas) en el nodo "Configuration and Management" (Configuración y gestión), y haga clic en **New Public Folder Forest** (Nuevo bosque de carpetas públicas).
- 2 Haga clic en **Forest Domain** (Dominio del bosque), especifique el bosque de directorios activos en el que se encuentran los objetos de carpeta pública y, a continuación, haga clic en **Siguiente**.
- 3 En **Domain access** (Acceso al dominio), especifique la cuenta de acceso:
 - ♦ **"Use the Directory and Resource Administrator service account" (Utilizar la cuenta de servicio de Directory and Resource Administrator):** si desea utilizar la cuenta de servicio de DRA.
 - ♦ **"Use the following account to access this domain" (Utilizar la siguiente cuenta para acceder a este dominio):** si desea utilizar la cuenta de acceso al dominio.

Importante: Si utiliza el servidor secundario, estará disponible la opción **Use the Primary Administration Server domain access account** (Utilizar la cuenta de acceso al dominio del servidor de administración principal).

- 4 En **Exchange access** (Acceso a Exchange), especifique la cuenta que desea que utilice DRA para el acceso seguro a los servidores de Exchange:
 - ♦ **"Use the Domain access account for all Exchange servers" (Utilizar la cuenta de acceso al dominio para todos los servidores de Exchange):** si desea utilizar la cuenta de acceso al dominio.
 - ♦ **"Use the following account to access all Exchange servers" (Utilizar la siguiente cuenta para acceder a todos los servidores de Exchange):** si desea utilizar la cuenta de acceso a Exchange.

Importante: Si utiliza el servidor secundario, estará disponible la opción **Use the Primary Administration Server Exchange access account** (Utilizar la cuenta de acceso a Exchange del servidor de administración principal).

- 5 En **Servidor Exchange**, seleccione la instancia de Exchange Server que desea que utilice DRA para gestionar las carpetas públicas.
- 6 En **Summary** (Resumen), revise la información de la cuenta y los detalles de Exchange Server y, a continuación, haga clic en **Finalizar** para completar el proceso.

El servidor DRA ejecuta una actualización completa de la memoria caché de cuentas en la carpeta pública. El nuevo bosque de carpetas públicas aparecerá en la consola después de que se complete la actualización de la memoria caché, lo que puede tardar unos minutos.

Nota: Puede eliminar un dominio del bosque público seleccionado en **Tareas** o el menú contextual.

Visualización y modificación de las propiedades del dominio de carpetas públicas

Para ver o modificar las propiedades del dominio de carpetas públicas:

- 1 Haga clic en **Managed Public Folder Forests** (Gestionar bosques de carpetas públicas gestionadas) en el nodo "Configuration Management" (Gestión de configuraciones) para ver las carpetas públicas.
- 2 Haga clic con el botón derecho en la cuenta de carpeta pública que desee ver y seleccione **Propiedades**.
- 3 En las propiedades del **bosque de carpetas públicas**, puede llevar a cabo las siguientes acciones:
 - ♦ **General:** consulte la información de la cuenta de carpeta pública y actualice el campo **Servidor Exchange**, que utiliza el servidor DRA para realizar la actividad de Exchange en el servidor de carpetas públicas.
 - ♦ **Estadísticas:** consulte el número de carpetas públicas y de carpetas públicas habilitadas para correo.
 - ♦ **"Incremental Status" (Estado incremental):** consulte o actualice el estado de la memoria caché de cuentas incremental.
 - ♦ **"Incremental schedule" (Programación incremental):** consulte la programación incremental de la actualización de la memoria caché y vuelva a programar la actualización.
 - ♦ **"Full status" (Estado completo):** consulte el estado de la actualización completa de la memoria caché de cuentas.
 - ♦ **"Full refresh" (Actualización completa):** realice al instante una actualización completa de la memoria caché de cuentas.
NetIQ recomienda que solo realice una **actualización completa** si se han dañado los datos de la memoria caché de las carpetas públicas.
 - ♦ **"Domain access" (Acceso al dominio):** consulte la información de la cuenta de servicio o sustituya las cuentas de acceso.
 - ♦ **"Exchange access" (Acceso a Exchange):** consulte o actualice el acceso seguro a los servidores de Exchange.

Delegación de poderes de carpetas públicas

Utilice ActiveViews para definir poderes y gestionar la delegación de carpetas públicas. Puede especificar reglas para añadir objetos gestionados, elegir dominios y asignar poderes, y delegar a continuación esos poderes de carpetas públicas a los administradores asistentes.

Para crear una ActiveView y delegar los poderes de carpetas públicas:

- 1 En el nodo **Delegation Management** (Gestión de delegación), haga clic en **ActiveViews**.
- 2 Haga clic en **Siguiente** en el **Asistente para crear > ActiveViews**, seleccione la regla necesaria en la lista desplegable **Añadir** y elija **Carpetas públicas** como tipo de objeto. Por ejemplo, para crear una regla de coincidencia de objetos: seleccione **Objects that match a rule** (Objetos que coinciden con una regla) y elija **Carpetas públicas** como tipo de objeto.
- 3 Especifique la regla de ActiveView que desea añadir a la carpeta pública y, a continuación, haga clic en **Siguiente**.

- 4 Especifique un nombre para la ActiveView y, a continuación, haga clic en **Finalizar**.
- 5 Haga clic con el botón derecho en **ActiveViews** y vaya a **Delegate Administration** (Delegar administración) > **Administradores asistentes** y especifique el tipo de administrador en la lista desplegable **Añadir del Asistente**.
- 6 Busque el usuario específico, el grupo o el grupo de administradores asistentes al que desea delegar poderes.
- 7 Utilice el **Selector de objetos** para buscar y añadir los objetos que desee y, a continuación, haga clic en **Roles and Powers** (Funciones y poderes) en el **Asistente**.
- 8 Seleccione **Funciones** en la lista desplegable **Añadir** y, a continuación, busque y añada la función Administración de carpetas públicas.
- 9 Seleccione Poderes en la lista desplegable **Añadir** y, a continuación, busque y añada cualquier poder adicional que desee asignar a los administradores asistentes que no formen parte de la función Administración de carpetas públicas.
- 10 Haga clic en **Siguiente** y, a continuación, en **Finalizar** para completar el proceso de asignación de delegación.

Una vez finalizada la delegación completa de poderes de carpetas públicas, los usuarios autorizados podrán realizar operaciones de creación, lectura, actualización y supresión en las propiedades de las carpetas públicas de dominios configurados mediante la consola Web.

3.2.3 **Habilitación de la compatibilidad con Microsoft Exchange**

Al habilitar la compatibilidad con Microsoft Exchange, puede aprovechar las funciones de Exchange, como las directivas de Microsoft Exchange, el buzón integrado y la gestión de objetos habilitados para correo. Puede habilitar o inhabilitar la compatibilidad con Microsoft Exchange para cada servidor de administración en las siguientes plataformas: Microsoft Exchange Server 2010, y Microsoft Exchange Server 2013 y versiones posteriores.

Para habilitar la compatibilidad con Microsoft Exchange, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización, y su licencia debe admitir el producto Exchange. Para obtener más información acerca de los requisitos de Microsoft Exchange, consulte [Plataformas compatibles](#).

Para habilitar la compatibilidad con Microsoft Exchange:

- 1 Acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Exchange Policies** (Configurar las directivas de Exchange).
- 2 Seleccione **Enable Exchange Policy** (Habilitar la directiva de Exchange) y haga clic en **Aplicar**.
DRA comprueba las versiones de las herramientas de gestión de Exchange que se han instalado en el servidor de administración y habilita las opciones que permiten seleccionar la compatibilidad con Exchange para las versiones adecuadas.
- 3 *Si ya se ha seleccionado "Enable Exchange Policy" (Habilitar la directiva de Exchange) y no se han habilitado las opciones que le permiten seleccionar la compatibilidad con Exchange, haga clic en **Actualizar** para que DRA compruebe las versiones de las herramientas de administración de Exchange que se han instalado en el servidor de administración.*
- 4 Para habilitar la compatibilidad con la administración de Exchange, seleccione las opciones para habilitar la compatibilidad con las versiones de Exchange que tenga intención de gestionar con este servidor de administración.
- 5 Haga clic en **Aceptar**.

3.2.4 Habilitación de Exchange Online y Skype Empresarial Online

Para habilitar el buzón de Exchange Online y Skype Empresarial Online en Office 365, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización. La licencia debe admitir también el producto Microsoft Exchange.

Importante: Microsoft Server limita el número de usuarios simultáneos conectados a la sesión de WinRM/WinRS a cinco y el número de shells por usuario a cinco, así que asegúrese de que la misma cuenta de usuario esté limitada a cinco shells para los servidores secundarios de DRA.

Para habilitar la compatibilidad con Exchange Online y Skype Empresarial Online:

- 1 Si aún no los ha hecho, instale los componentes de Microsoft indicados a continuación:
 - ♦ PowerShell 5.0+
 - ♦ Microsoft Online Services - Ayudante para el inicio de sesión para profesionales de TI RTW
<https://www.microsoft.com/es-es/download/details.aspx?id=41950>
 - ♦ Skype Empresarial Online y Módulo de Windows PowerShell
<https://www.microsoft.com/es-es/download/details.aspx?id=39366>
 - ♦ Abra PowerShell y ejecute `Install-Module MSOnline`.

Para obtener más información, consulte <https://docs.microsoft.com/es-es/office365/enterprise/powershell/connect-to-office-365-powershell>.
- 2 Abra la consola de gestión de equipos y reinicie el **servicio de administración de NetIQ**.
- 3 En el panel izquierdo, haga clic en **Policy and Automation Management** (Gestión de directivas y automatización).
- 4 Desplácese a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Office 365 Policies** (Configuración de las directivas de Office 365) y haga clic en **Enable Exchange Online Administration support** (Habilitar la compatibilidad con la administración de Exchange Online).

3.2.5 Adición de un inquilino de Office 365

Para gestionar Exchange Online y Skype Empresarial Online, debe administrar uno o varios inquilinos de Office 365. Antes de poder gestionar los inquilinos de Office 365, debe habilitar la compatibilidad con Exchange Online o Skype Empresarial Online.

Importante: Microsoft Server limita el número de usuarios simultáneos conectados a la sesión de WinRM/WinRS a cinco y el número de shells por usuario a cinco, así que asegúrese de que la misma cuenta de usuario esté limitada a cinco shells para los servidores secundarios de DRA.

Para obtener información sobre cómo habilitar Exchange Online o Skype Empresarial Online, consulte:

- ♦ [Habilitación de la compatibilidad con Microsoft Exchange](#)
- ♦ [Habilitación de Exchange Online y Skype Empresarial Online](#)

Antes de configurar DRA para gestionar los inquilinos de Exchange Online, debe crear una cuenta en el portal de Office 365 que tenga los siguientes permisos:

DRA utilizará esta cuenta para realizar todas las tareas de gestión de Exchange Online.

- ♦ Administrador de gestión de usuarios de Office 365
- ♦ Gestión de destinatarios de Exchange Online

Nota: Esta cuenta se puede sincronizar con el entorno de Active Directory o alojarse en la nube de Microsoft Office 365. DRA no requiere que esta cuenta se encuentre en Active Directory para realizar tareas de gestión.

Para obtener más información sobre los permisos de cuenta, consulte [Cuentas de acceso de DRA con privilegios mínimos](#).

Gestión de un inquilino de Office 365 y creación de una entidad de servicio

Una vez que haya habilitado la directiva en línea de DRA, puede acceder a un nuevo nodo en "Configuration Management" (Gestión de configuraciones) denominado **Office 365 Tenants** (Inquilinos de Office 365) donde puede gestionar nuevos inquilinos de Office 365.

Para añadir un inquilino de Office 365, vaya a **Configuration Management** (Gestión de configuraciones) > **Office 365 Tenants** (Inquilinos de Office 365) y siga las instrucciones del asistente, entre las que se incluye la adición de una cuenta de acceso al inquilino de Office 365 y la configuración de las programaciones de actualización.

DRA requiere una entidad de servicio con permisos de lectores de directorio para poder recopilar datos sobre los objetos del inquilino.

Para crear la entidad de servicio, puede proporcionar a DRA las credenciales de una cuenta de usuario con la función Administrador de la empresa en Office 365; DRA creará automáticamente la entidad de servicio o puede crearla sin conexión.

Nota

- ♦ DRA no almacena las credenciales de Administrador de la empresa proporcionadas para crear la entidad de servicio.
- ♦ Si crea la entidad de servicio sin conexión, debe proporcionar el identificador y la contraseña de la entidad de servicio en el Asistente.

La adición de un inquilino de Office 365 puede tardar varios minutos en completarse. Una vez que se haya añadido correctamente el inquilino, DRA realizará una actualización completa de la memoria caché de cuentas (FACR, Full Accounts Cache Refresh) para el inquilino. Una vez completada la actualización de la memoria caché, puede comenzar a gestionar las licencias y los buzones de Office 365 para el inquilino.

4 Modelo de delegación

DRA permite a los administradores implementar un esquema de permisos de "privilegios mínimos" al proporcionar un conjunto flexible de controles para otorgar poderes granulares a objetos gestionados específicos de la empresa. Mediante estas delegaciones, los administradores pueden garantizar que los administradores asistentes reciban solo los permisos necesarios para completar sus funciones y responsabilidades específicas.

4.1 Descripción del modelo de delegación dinámica

DRA permite gestionar el acceso administrativo a la empresa en el contexto de un modelo de delegación. El modelo de delegación permite configurar el acceso de "privilegios mínimos" para los administradores asistentes a través de un conjunto dinámico de controles que pueden adaptarse a medida que la empresa cambia y evoluciona. El modelo de delegación proporciona un control de acceso administrativo que representa mejor cómo funciona la empresa:

- ♦ Con las reglas de ámbito flexibles, los administradores pueden asignar de forma precisa los permisos a objetos gestionados específicos en función de las necesidades del negocio en lugar de la estructura de la empresa.
- ♦ La delegación basada en funciones garantiza que los permisos se otorguen de manera coherente y simplifica la provisión.
- ♦ La asignación de privilegios puede administrarse entre dominios, inquilinos en la nube y aplicaciones gestionadas desde una única ubicación.
- ♦ Los poderes granulares permiten adaptar el acceso específico otorgado a los administradores asistentes.

4.1.1 Controles del modelo de delegación

Los administradores utilizan los siguientes controles para proporcionar acceso a través del modelo de delegación:

- ♦ **Delegación:** los administradores proporcionan acceso a usuarios y grupos mediante la asignación de una función, que tiene permisos específicos en el contexto de una ActiveView que proporciona el ámbito.
- ♦ **ActiveViews:** una ActiveView representa un ámbito específico de objetos gestionados que definen una o varias reglas. Los objetos gestionados identificados por cada regla en una ActiveView se añaden de forma conjunta a un ámbito unificado.
- ♦ **Regla de ActiveView:** las reglas se definen mediante expresiones que coinciden con un conjunto de objetos gestionados en función de una serie de condiciones, como el tipo de objeto, la ubicación, el nombre, etc.
- ♦ **Funciones:** una función representa un conjunto específico de poderes (permisos) necesarios para realizar una función de administración específica. DRA proporciona una serie de funciones integradas para las actividades comerciales habituales y puede definir las funciones personalizadas que mejor se adapten a las necesidades de su organización.
- ♦ **Poderes:** un poder define un permiso específico para realizar tareas admitidas por el objeto gestionado, como ver, modificar, crear, eliminar, etc. Los permisos en torno a la modificación de un objeto gestionado se pueden desglosar en función de las propiedades específicas que se

pueden cambiar. DRA proporciona una lista extensa de poderes integrados para los objetos gestionados admitidos y puede definir poderes personalizados para ampliar lo que se puede proporcionar mediante el modelo de delegación.

4.1.2 Cómo procesa DRA las peticiones

Cuando el servidor de administración recibe una petición de acción, como cambiar la contraseña de un usuario, utiliza el siguiente proceso:

1. Busque ActiveViews que se hayan configurado para gestionar el objeto de destino de la operación.
2. Valide los poderes asignados a la cuenta que solicita la acción.
 - a. Evalúe todas las asignaciones de ActiveViews que contienen el administrador asistente que solicita la operación.
 - b. Una vez completada la lista, cree una lista de todas las ActiveViews que contengan tanto el objeto de destino como el administrador asistente.
 - c. Compare los poderes con los que se necesitan para la operación de petición.
3. *Si la cuenta dispone del poder correcto*, el servidor de administración permite realizar la acción. *Si la cuenta no dispone del poder correcto*, el servidor de administración devuelve un error.
4. Actualización de Active Directory.

4.1.3 Ejemplos de cómo DRA procesa las asignaciones de delegación

En los siguientes ejemplos, se describen las situaciones habituales que surgen en cuanto al modo en que DRA evalúa el modelo de delegación cuando se procesa una petición:

Ejemplo 1: cambio de la contraseña de un usuario

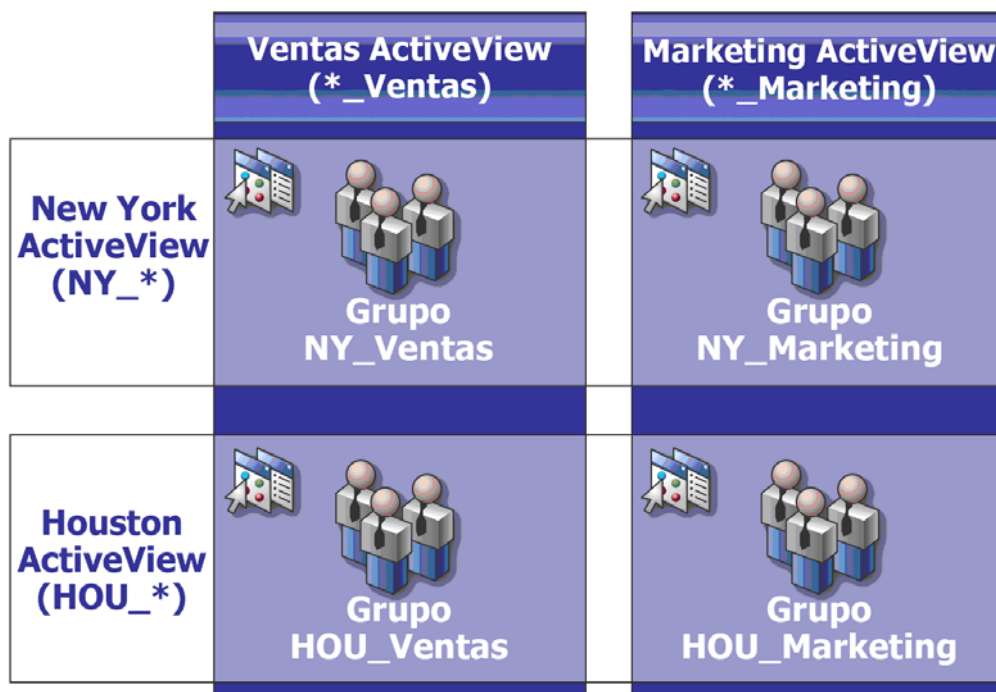
Cuando un administrador asistente intenta definir una nueva contraseña para la cuenta de usuario JSmith, el servidor de administración busca todas las ActiveViews que incluyan JSmith. Esta búsqueda devuelve todas las ActiveViews que especifican directamente JSmith mediante una regla de caracteres comodín o una pertenencia a grupo. Si una ActiveView incluye otras ActiveViews, el servidor de administración también busca esas ActiveViews adicionales. El servidor de administración determina si el administrador asistente tiene el poder *Restablecer la contraseña de la cuenta de usuario* en cualquiera de estas ActiveViews. Si el administrador del asistente dispone del poder *Restablecer la contraseña de la cuenta de usuario*, el servidor de administración restablece la contraseña para JSmith. Si no dispone de ese poder, el servidor de administración rechaza la petición.

Ejemplo 2: superposición de ActiveViews

Un poder define las propiedades de un objeto que un administrador asistente puede ver, modificar o crear en el dominio o el subárbol gestionados. Varias ActiveViews pueden incluir el mismo objeto. Esta configuración se denomina **superposición de ActiveViews**.

Si se solapan las ActiveViews, puede acumular un conjunto de distintos poderes para los mismos objetos. Por ejemplo, si una ActiveView permite añadir una cuenta de usuario a un dominio y otra ActiveView permite suprimir una cuenta de usuario del mismo dominio, puede añadir o suprimir cuentas de usuario en ese dominio. De esta forma, los poderes de los que disponga para un determinado objeto serán acumulativos.

Es importante entender cómo las ActiveViews pueden superponerse y puede disponer de más poderes para los objetos incluidos en ellas. Tenga en cuenta la configuración de ActiveView que se muestra en la siguiente ilustración.



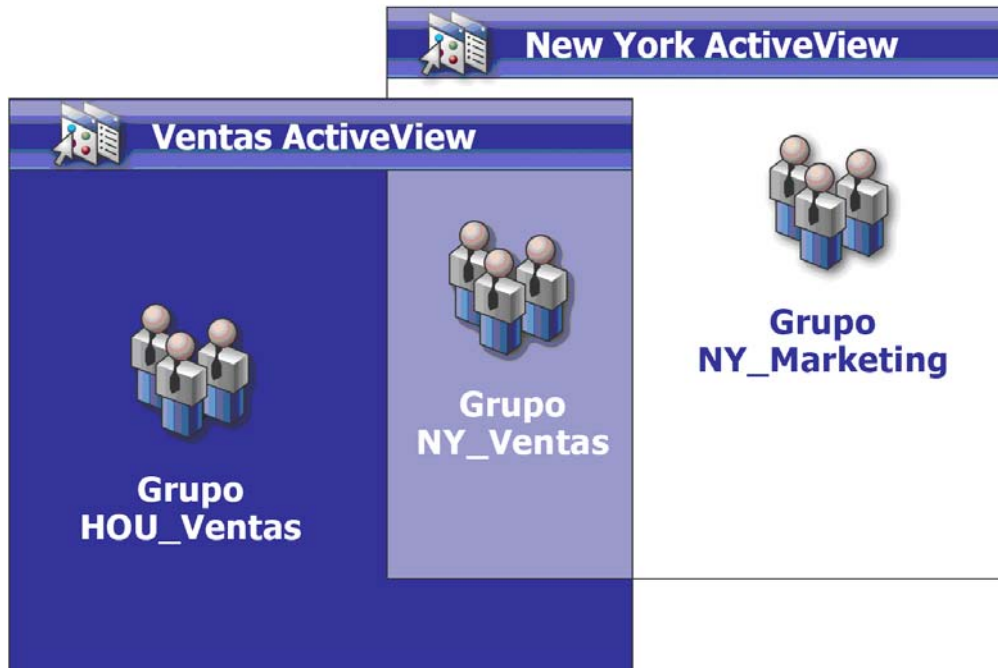
Las pestañas blancas identifican ActiveViews por ubicación, *Nueva York* y *Houston*. Las pestañas negras identifican ActiveViews por su función administrativa, *Ventas* y *Marketing*. Las celdas muestran los grupos incluidos en cada ActiveView.

Los grupos "NY_Ventas" y "HOU_Ventas" se representan ambos en la ActiveView Ventas. Si dispone de poderes en la ActiveView Ventas, puede gestionar cualquier miembro de los grupos "NY_Ventas" y "HOU_Ventas". Si también dispone de poderes en la ActiveView Nueva York, estos poderes adicionales se aplican al grupo "NY_Marketing". De esta forma, se acumulan los poderes a medida que se superponen las ActiveViews.

La superposición de ActiveViews puede proporcionar un modelo de delegación eficaz y flexible. Sin embargo, esta función también puede tener consecuencias no deseadas. Planifique cuidadosamente las ActiveViews para asegurarse de que cada administrador asistente disponga solo de los poderes que desea para cada cuenta de usuario, grupo, unidad administrativa, contacto o recurso.

Grupos en varias ActiveViews

En este ejemplo, el grupo "NY_Ventas" se representa en más de una ActiveView. Los miembros del grupo "NY_Ventas" están representados en la ActiveView Nueva York debido a que el nombre del grupo coincide con la regla de ActiveView `NY_*`. El grupo también se encuentra en la ActiveView Ventas debido a que el nombre de grupo coincide con la regla de ActiveView `*_ventas`. Al incluir el mismo grupo en varias ActiveViews, puede permitir que distintos administradores asistentes gestionen los mismos objetos de forma diferente.






Uso de poderes en varias ActiveViews

Supongamos que hay un administrador asistente, JSmith, que tiene el poder *Modificar las propiedades generales del usuario* en la ActiveView Nueva York. Este primer poder permite a JSmith editar todas las propiedades en la pestaña General de una ventana de propiedades de usuario.

JSmith dispone del poder *Modificar las propiedades del perfil de usuario* en la ActiveView Ventas. Este segundo poder permite a JSmith editar todas las propiedades en la pestaña Perfil de una ventana de propiedades de usuario.

En la siguiente ilustración, se indican los poderes que JSmith tiene para cada grupo.

	Ventas ActiveView (*_Ventas)	Marketing ActiveView (*_Marketing)
New York ActiveView (NY_*)	 !Propiedades generales !Propiedades del perfil Grupo NY_Ventas	 !Propiedades generales Grupo NY_Marketing
Houston ActiveView (HOU_*)	 !Propiedades del perfil Grupo HOU_Ventas	 !Sin permisos Grupo HOU_Marketing

JSmith dispone de los siguientes poderes:

- ♦ Propiedades generales en la ActiveView NY_*
- ♦ Propiedades del perfil en la ActiveView *_Ventas

La delegación de poderes en estas ActiveViews superpuestas permite a JSmith modificar las propiedades generales y de perfil del grupo NY_Ventas. Por lo tanto, JSmith dispone de todos los poderes concedidos en las ActiveViews que representan al grupo NY_Ventas.

4.2 ActiveViews

Las ActiveViews permiten implementar un modelo de delegación con las siguientes características:

- ♦ Es independiente de la estructura de Active Directory.
- ♦ Permite asignar poderes y definir directivas que se correlacionan con los flujos de trabajo existentes.
- ♦ Proporciona automatización que le ayudará a integrar y personalizar de forma adicional su empresa.
- ♦ Responde de forma dinámica a los cambios.

Una ActiveView representa un conjunto de objetos en uno o varios dominios gestionados. Puede incluir un objeto en más de una ActiveView. También puede incluir un gran número de objetos de varios dominios o unidades administrativas.

4.2.1 ActiveViews integradas

Las ActiveViews integradas son las ActiveViews por defecto proporcionadas por DRA. Estas ActiveViews representan todos los objetos actuales y la configuración de seguridad. Por lo tanto, las ActiveViews integradas proporcionan acceso inmediato a todos los objetos y ajustes, así como al modelo de delegación por defecto. Puede utilizar estas ActiveViews para gestionar objetos, como cuentas de usuario y recursos, o aplicar el modelo de delegación por defecto a la configuración empresarial actual.

DRA proporciona varias ActiveViews integradas que pueden representar el modelo de delegación. El nodo de ActiveViews integradas contiene las siguientes ActiveViews:

Todos los objetos

Incluye todos los objetos de todos los dominios gestionados. A través de este ActiveView, puede gestionar cualquier aspecto de su empresa. Asigne esta ActiveView al administrador o a un administrador asistente que necesite poderes de auditoría en toda la empresa.

Objetos que el usuario actual gestiona como Administrador de Windows

Incluye los objetos del dominio gestionado actual. A través de esta ActiveView, puede gestionar cuentas de usuario, grupos, contactos, unidades administrativas y recursos. Asigne esta ActiveView a los administradores nativos que sean responsables de los objetos de cuenta y recurso en el dominio gestionado.

Servidores de administración y dominios gestionados

Incluye los equipos del servidor de administración y los dominios gestionados. Mediante esta ActiveView, puede gestionar el mantenimiento diario de los servidores de administración. Asigne esta ActiveView a los administradores asistentes cuyas obligaciones incluyan la supervisión del estado de sincronización o la actualización de la memoria caché.

Directivas de DRA y activadores de automatización

Incluye todos los objetos de directiva y activador de automatización de todos los dominios gestionados. Mediante esta ActiveView, puede gestionar las propiedades y el ámbito de la directiva, así como las propiedades de activación de la automatización. Asigne esta ActiveView a los administradores asistentes responsables de la creación y el mantenimiento de las directivas de la empresa.

Objetos de seguridad de DRA

Incluye todos los objetos de seguridad. Mediante esta ActiveView, puede gestionar ActiveViews, grupos de administradores asistentes y funciones. Asigne esta ActiveView a los administradores asistentes responsables de la creación y la gestión del modelo de seguridad.

Usuarios de SPA de todos los dominios gestionados y de confianza

Incluye todas las cuentas de usuario de dominios gestionados y de confianza. Mediante esta ActiveView, puede gestionar las contraseñas de los usuarios a través de Secure Password Administrator (SPA).

Acceso a las ActiveViews integradas

Acceda a las ActiveViews integradas para auditar el modelo de delegación por defecto o gestione su propia configuración de seguridad.

Para acceder a las ActiveViews integradas:

- 1 Desplácese a **Delegation Management** (Gestión de delegación) > **Manage ActiveViews** (Gestionar ActiveViews).

- 2 Asegúrese de que el campo de búsqueda esté en blanco y haga clic en **Find Now** (Buscar ahora) en el panel **List items that match my criteria** (Mostrar elementos que coincidan con los criterios).
- 3 Seleccione la ActiveView adecuada.

Uso de las ActiveViews integradas

No se pueden suprimir, clonar o modificar las ActiveViews integradas. Sin embargo, puede incorporar estas ActiveViews en el modelo de delegación existente o utilizar estas ActiveViews para diseñar su propio modelo.

Puede utilizar ActiveViews integradas de las siguientes formas:

- ♦ Asigne las ActiveViews integradas individuales a los grupos de administradores asistentes adecuados. Esta asociación permite a los miembros del grupo de administradores asistentes gestionar el conjunto correspondiente de objetos con los poderes adecuados.
- ♦ Consulte las reglas y las asociaciones de ActiveView integradas como directrices para diseñar e implementar el modelo de delegación.

Para obtener más información sobre el diseño de un modelo de delegación dinámico, consulte [Descripción del modelo de delegación dinámica](#).

4.2.2 Implementación de una ActiveView personalizada

Una ActiveView proporciona acceso en tiempo real a objetos específicos dentro de uno o varios dominios o unidades administrativas. Puede añadir o eliminar objetos de una ActiveView sin cambiar la estructura subyacente del dominio o la unidad administrativa.

Puede considerar una ActiveView como un dominio o una unidad administrativa virtuales o el resultado de una vista de base de datos o declaración seleccionadas de una base de datos relacional. Las ActiveViews pueden incluir o excluir cualquier conjunto de objetos, contener otras ActiveViews y tener contenidos superpuestos. Las ActiveViews pueden contener objetos de diferentes dominios, árboles y bosques. Puede configurar ActiveViews para satisfacer cualquier necesidad de gestión de la empresa.

Las ActiveViews pueden incluir los siguientes tipos de objetos:

Cuentas:

- ♦ Usuarios
- ♦ Grupos
- ♦ PCs
- ♦ Contactos
- ♦ Grupos dinámicos de distribución
- ♦ Impresoras publicadas
- ♦ Tareas de impresión de impresoras publicadas
- ♦ Buzones de recursos
- ♦ Buzones compartidos
- ♦ Carpetas públicas

Objetos de directorio:

- ♦ Unidades administrativas

- ♦ Dominios
- ♦ Servidores miembros

Objetos de delegación:

- ♦ ActiveViews
- ♦ Autoadministración
- ♦ Informes directos
- ♦ Grupos gestionados

Recursos:

- ♦ Usuarios conectados
- ♦ Dispositivos
- ♦ Registros de eventos
- ♦ Archivos abiertos
- ♦ Impresoras
- ♦ Tareas de impresión
- ♦ Servicios
- ♦ Recursos compartidos

A medida que cambie o crezca su empresa, las ActiveViews cambiarán para incluir o excluir los nuevos objetos. Por lo tanto, puede utilizar ActiveViews para reducir la complejidad del modelo, proporcionarle la seguridad que necesita y ofrecerle mucha más flexibilidad que otras herramientas de organización empresarial.

Reglas de ActiveViews

Una ActiveView puede constar de reglas que incluyen o excluyen objetos, como cuentas de usuario, grupos, unidades administrativas, contactos, recursos, equipos, buzones de recursos, buzones compartidos, grupos dinámicos de distribución y ActiveViews. Esta flexibilidad convierte a las ActiveViews en componentes dinámicos.

Estas coincidencias se denominan **caracteres comodín**. Por ejemplo, puede definir una regla que incluya todos los equipos con nombres que coincidan con `DOM*`. Esta especificación de caracteres comodín buscará cualquier cuenta de equipo cuyo nombre comience con la cadena de caracteres `DOM`. La coincidencia de caracteres comodín permite que la administración sea dinámica, ya que las cuentas se incluyen automáticamente cuando coinciden con la regla. Por lo tanto, al utilizar caracteres comodín, no necesita configurar de nuevo las ActiveViews a medida que cambie su organización.

Otro ejemplo consiste en definir ActiveViews en función de la pertenencia a grupo. Puede definir una regla que incluya todos los miembros de los grupos que empiecen por las letras `NY`. A continuación, a medida que los miembros se añadan a cualquier grupo que coincida con esta regla, estos miembros se incluirán automáticamente en esta ActiveView. A medida que cambie o crezca su empresa, DRA volverá a aplicar las reglas para incluir o excluir los nuevos objetos en las ActiveViews adecuadas.

4.3 Funciones

Esta sección incluye una lista con descripciones de las funciones integradas en DRA, cómo utilizarlas e información sobre cómo crear y administrar funciones personalizadas.

Para obtener una descripción general de las funciones y su uso, consulte [Controles del modelo de delegación](#).

4.3.1 Funciones integradas

Las funciones integradas de administradores asistentes proporcionan acceso al instante a un conjunto de poderes utilizados habitualmente. Puede ampliar la configuración de seguridad actual mediante estas funciones por defecto para delegar poderes a cuentas de usuario específicas u otros grupos.

Estas funciones contienen los poderes necesarios para realizar tareas de administración habituales. Por ejemplo, la función Administración de DRA contiene todos los poderes necesarios para gestionar objetos. Sin embargo, para utilizar esos poderes, la función debe estar asociada a una cuenta de usuario o a un grupo de administradores asistentes y la ActiveView gestionada.

Como las funciones integradas forman parte del modelo de delegación por defecto, puede utilizarlas para delegar rápidamente poderes e implementar la seguridad. Estas funciones integradas abordan tareas habituales que puede realizar mediante las interfaces de usuario de DRA. En la siguiente lista, se describe cada función integrada y se resumen los poderes asociadas a esa función.

Administración de servidores de aplicación

Proporciona los poderes necesarios para configurar, ver y suprimir las configuraciones del servidor de aplicaciones.

Auditar todos los objetos

Proporciona todos los poderes necesarios para ver las propiedades de los objetos, las directivas y las configuraciones en toda la empresa. Esta función no permite que un administrador asistente modifique las propiedades. Asigne este rol a los administradores asistentes responsables de las acciones de auditoría de la empresa. Permite a los administradores asistentes ver todos los nodos, excepto el nodo Herramientas personalizadas.

Auditar propiedades limitadas de cuentas y recursos

Proporciona poderes para todas las propiedades de objetos.

Auditar recursos

Proporciona todos los poderes necesarios para ver las propiedades de los recursos gestionados. Asigne esta función a los administradores asistentes responsables de auditar los objetos de recurso.

Auditar usuarios y grupos

Proporciona todos los poderes necesarios para ver las propiedades de cuentas de usuario y grupos, pero no el poder para modificarlas. Asigne esta función a los administradores asistentes responsables de auditar propiedades de cuentas.

Programador integrado (solo para uso interno)

Proporciona poderes para realizar una programación cuando DRA actualice la memoria caché.

Clonar usuario con buzón

Proporciona todos los poderes necesarios para clonar una cuenta de usuario existente junto con su buzón. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de usuario.

Nota: Para permitir que el administrador asistente añada la nueva cuenta de usuario a un grupo durante la tarea de clonación, asigne también la función Gestionar pertenencias a grupos.

Administración de equipos

Proporciona todos los poderes necesarios para modificar las propiedades de los equipos. Esta función permite que los administradores asistentes añadan, supriman y apaguen equipos, además de permitir la sincronización de controladores de dominio. Asigne esta función a los administradores asistentes responsables de gestionar equipos en la ActiveView.

Configurar servidores y dominios

Proporciona todos los poderes necesarios para modificar las opciones del servidor de administración y los dominios gestionados. También proporciona poderes para configurar y gestionar los inquilinos de Office 365. Asigne esta función a los administradores asistentes responsables de la supervisión y el mantenimiento de los servidores de administración.

Ponerse en contacto con la administración

Proporciona todos los poderes necesarios para crear un nuevo contacto, modificar sus propiedades o eliminar un contacto. Asigne esta función a los administradores asistentes responsables de gestionar contactos.

Crear y suprimir cuentas de equipo

Proporciona todos los poderes necesarios para crear y suprimir una cuenta de equipo. Asigne esta función a los administradores asistentes responsables de gestionar equipos.

Crear y suprimir grupos

Proporciona todos los poderes necesarios para crear y suprimir un grupo. Asigne esta función a los administradores asistentes responsables de gestionar grupos.

Crear y suprimir un buzón de recursos

Proporciona todos los poderes necesarios para crear y suprimir un buzón. Asigne esta función a los administradores asistentes responsables de gestionar buzones.

Crear y suprimir recursos

Proporciona todos los poderes necesarios para crear y suprimir recursos compartidos y cuentas de equipo, y borrar registros de eventos. Asigne esta función a los administradores asistentes responsables de gestionar objetos de recurso y registros de eventos.

Crear y modificar cuentas de usuario

Proporciona todos los poderes necesarios para crear y suprimir una cuenta de usuario. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de usuario.

Administración de DRA

Proporciona todos los poderes a un administrador asistente. Esta función le otorga a un usuario los permisos para realizar todas las tareas de administración en DRA. Esta función es equivalente a los permisos de un administrador. Un administrador asistente asociado a la función Administración de DRA puede acceder a todos los nodos de Directory and Resource Administrator.

Administración de grupos dinámicos

Proporciona todos los poderes necesarios para gestionar los grupos dinámicos de Active Directory.

Ejecutar consultas avanzadas

Proporciona todos los poderes necesarios para ejecutar las consultas avanzadas guardadas. Asigne esta función a los administradores asistentes responsables de ejecutar consultas avanzadas.

Administración de grupos

Proporciona todos los poderes necesarios para gestionar grupos y pertenencias a grupos, y ver las propiedades de usuario correspondientes. Asigne esta función a los administradores asistentes responsables de gestionar grupos u objetos de cuenta y recurso que se gestionan mediante grupos.

Administración de la Ayuda técnica

Proporciona todos los poderes necesarios para ver las propiedades de las cuentas de usuario, y cambiar las contraseñas y las propiedades relacionadas con ellas. Esta función también permite a los administradores asistentes inhabilitar, habilitar y desbloquear cuentas de usuario. Asigne esta función a los administradores asistentes responsables de las tareas de la Ayuda técnica asociadas con garantizar que los usuarios tengan acceso adecuado a sus cuentas.

Administración de buzones

Proporciona todos los poderes necesarios para gestionar las propiedades de los buzones de Microsoft Exchange. Si utiliza Microsoft Exchange, asigne esta función a los administradores asistentes responsables de gestionar los buzones de Microsoft Exchange.

Gestionar los recopiladores de Active Directory, DRA e informes de gestión

Proporciona todos los poderes necesarios para gestionar los recopiladores de Active Directory, DRA, inquilinos de Office 365 e informes de gestión para la recopilación de datos. Asigne esta función a los administradores asistentes responsables de gestionar la configuración de elaboración de informes.

Gestionar recopiladores de Active Directory, DRA e informes de gestión, y la configuración de base de datos

Proporciona todos los poderes necesarios para gestionar los recopiladores de Active Directory, DRA e informes de gestión, y la configuración de base de datos para la recopilación de datos. Asigne esta función a los administradores asistentes responsables de gestionar la configuración de elaboración de informes y base de datos.

Gestionar consultas avanzadas

Proporciona todos los poderes necesarios para crear, gestionar y ejecutar consultas avanzadas. Asigne esta función a los administradores asistentes responsables de gestionar consultas avanzadas.

Gestionar y ejecutar herramientas personalizadas

Proporciona todos los poderes necesarios para crear, gestionar y ejecutar herramientas personalizadas. Asigne esta función a los administradores asistentes responsables de gestionar herramientas personalizadas.

Gestionar excepciones de clonación

Proporciona todos los poderes necesarios para crear y gestionar excepciones de clonación.

Gestionar las propiedades del equipo

Proporciona todos los poderes necesarios para gestionar todas las propiedades de una cuenta de equipo. Asigne esta función a los administradores asistentes responsables de gestionar equipos.

Gestionar la configuración de base de datos

Proporciona todos los poderes necesarios para gestionar la configuración de base de datos para los informes de gestión. Asigne esta función a los administradores asistentes responsables de gestionar la configuración de base de datos de elaboración de informes.

Gestionar grupos dinámicos de distribución

Proporciona todos los poderes necesarios para gestionar los grupos dinámicos de distribución de Microsoft Exchange.

Gestionar los derechos de los buzones de Exchange

Proporciona todos los poderes necesarios para gestionar la seguridad y los derechos de los buzones de Microsoft Exchange. Si utiliza Microsoft Exchange, asigne esta función a los administradores asistentes responsables de gestionar los permisos de los buzones de Microsoft Exchange.

Gestionar el correo electrónico del grupo

Proporciona todos los poderes necesarios para ver, habilitar o inhabilitar la dirección de correo electrónico de un grupo. Asigne esta función a los administradores asistentes responsables de gestionar grupos o direcciones de correo electrónico de los objetos de cuenta.

Gestionar la seguridad de la pertenencia a grupo

Proporciona todos los poderes necesarios para designar quién puede ver y modificar las pertenencias a grupos de Microsoft Windows mediante Microsoft Outlook.

Gestionar pertenencias a grupos

Proporciona todos los poderes necesarios para añadir y eliminar cuentas de usuario o grupos de un grupo existente y ver el grupo principal de una cuenta de usuario o equipo. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de usuario o grupos.

Gestionar las propiedades del grupo

Proporciona todos los poderes necesarios para gestionar todas las propiedades de un grupo. Asigne esta función a los administradores asistentes responsables de gestionar grupos.

Gestionar las peticiones de desplazamiento de buzones

Proporciona todos los poderes necesarios para gestionar las peticiones de desplazamiento de buzones.

Gestionar directivas y activadores de automatización

Proporciona todos los poderes necesarios para definir directivas y activadores de automatización. Asigne esta función a los administradores asistentes responsables del mantenimiento de las directivas de la empresa y los flujos de trabajo de automatización.

Gestionar impresoras y tareas de impresión

Proporciona todos los poderes necesarios para gestionar impresoras, además de colas y tareas de impresión. Para gestionar las tareas de impresión asociadas a una cuenta de usuario, la tarea de impresión y la cuenta de usuario deben incluirse en la misma ActiveView. Asigne esta función a los administradores asistentes responsables del mantenimiento de las impresoras y la gestión de las tareas de impresión.

Gestionar las propiedades del buzón de recursos

Proporciona todos los poderes necesarios para gestionar todas las propiedades de un buzón. Asigne esta función a los administradores asistentes responsables de gestionar buzones.

Gestionar los recursos de los usuarios gestionados

Proporciona todos los poderes necesarios para gestionar los recursos asociados a cuentas de usuario específicas. El administrador asistente y las cuentas de usuario deben incluirse en la misma ActiveView. Asigne esta función a los administradores asistentes responsables de gestionar objetos de recurso.

Gestionar el modelo de seguridad

Proporciona todos los poderes necesarios para definir las reglas de administración, incluidos administradores asistentes, ActiveViews y funciones. Asigne esta función a los administradores asistentes responsables de la implementación y el mantenimiento del modelo de seguridad.

Gestionar servicios

Proporciona todos los poderes necesarios para gestionar servicios. Asigne esta función a los administradores asistentes responsables de gestionar servicios.

Gestionar carpetas compartidas

Proporciona todos los poderes necesarios para gestionar carpetas compartidas. Asigne esta función a los administradores asistentes responsables de gestionar carpetas compartidas.

Gestionar asignaciones temporales de grupos

Proporciona todos los poderes necesarios para crear y gestionar asignaciones temporales de grupos. Asigne esta función a los administradores asistentes responsables de gestionar grupos.

Gestionar el módulo de elaboración de informes de la interfaz de usuario

Proporciona todos los poderes necesarios para generar y exportar informes de detalles de actividad para usuarios, grupos, contactos, equipos, unidades administrativas, poderes, funciones, ActiveViews, contenedores, impresoras publicadas y administradores asistentes. Asigne esta función a los administradores asistentes responsables de generar informes.

Gestionar las propiedades de marcado de los usuarios

Proporciona todos los poderes necesarios para modificar las propiedades de marcado de las cuentas de usuario. Asigne esta función a los administradores asistentes responsables de gestionar las cuentas de usuario que tienen acceso remoto a la empresa.

Gestionar el correo electrónico del usuario

Proporciona todos los poderes necesarios para ver, habilitar o inhabilitar la dirección de correo electrónico de una cuenta de usuario. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de usuario o direcciones de correo electrónico de los objetos de cuenta.

Gestionar la contraseña de usuario y desbloquear la cuenta

Proporciona todos los poderes necesarios para restablecer la contraseña, especificar la configuración de contraseña y desbloquear una cuenta de usuario. Asigne esta función a los administradores asistentes responsables del mantenimiento del acceso a las cuentas de usuario.

Gestionar las propiedades del usuario

Proporciona todos los poderes necesarios para gestionar todas las propiedades de una cuenta de usuario, incluidas las propiedades del buzón de Microsoft Exchange. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de usuario.

Gestionar atributos virtuales

Proporciona todos los poderes necesarios para crear y gestionar atributos virtuales. Asigne esta función a los administradores asistentes responsables de gestionar atributos virtuales.

Gestionar las propiedades de entorno de WTS

Proporciona todos los poderes necesarios para cambiar las propiedades de entorno de WTS para una cuenta de usuario. Asigne esta función a los administradores asistentes responsables del mantenimiento del entorno de WTS y la gestión de cuentas de usuario.

Gestionar las propiedades de control remoto de WTS

Proporciona todos los poderes necesarios para cambiar las propiedades de control remoto de WTS para una cuenta de usuario. Asigne esta función a los administradores asistentes responsables del mantenimiento del acceso a WTS y la gestión de cuentas de usuario.

Gestionar las propiedades de sesión de WTS

Proporciona todos los poderes necesarios para cambiar las propiedades de sesión de WTS para una cuenta de usuario. Asigne esta función a los administradores asistentes responsables del mantenimiento de las sesiones de WTS y la gestión de cuentas de usuario.

Gestionar las propiedades de terminal de WTS

Proporciona todos los poderes necesarios para cambiar las propiedades de terminal de WTS para una cuenta de usuario. Asigne esta función a los administradores asistentes responsables del mantenimiento de las propiedades de terminal de WTS y la gestión de cuentas de usuario.

Gestión de unidades administrativas

Proporciona todos los poderes necesarios para gestionar unidades administrativas. Asigne esta función a los administradores asistentes responsables de gestionar la estructura de Active Directory.

Administración de carpetas públicas

Proporciona los poderes para crear, modificar, suprimir, habilitar o inhabilitar carpetas y ver las propiedades de la carpeta pública. Puede asignar esta función a todos los administradores asistentes responsables de gestionar la carpeta pública.

Cambiar el nombre del grupo y modificar la descripción

Proporciona todos los poderes necesarios para modificar el nombre y la descripción de un grupo. Asigne esta función a los administradores asistentes responsables de gestionar grupos.

Cambiar el nombre del usuario y modificar la descripción

Proporciona todos los poderes necesarios para modificar el nombre y la descripción de una cuenta de usuario. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de usuario.

Replicar archivos

Proporciona todos los poderes necesarios para cargar, suprimir y modificar la información de archivo. Asigne esta función a los administradores asistentes responsables de replicar los archivos del servidor de administración principal en otros servidores de administración de los equipos cliente de DRA y MMS.

Restablecer la contraseña del administrador local

Proporciona todos los poderes para restablecer la contraseña de la cuenta de administrador local y ver el nombre del administrador del equipo. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de administrador.

Restablecer contraseña

Proporciona todos los poderes necesarios para restablecer y modificar contraseñas. Asigne esta función a los administradores asistentes responsables de la gestión de contraseñas.

Restablecer contraseña y desbloquear la cuenta mediante SPA

Proporciona todos los poderes necesarios para utilizar Secure Password Administrator para restablecer las contraseñas y desbloquear las cuentas de usuario.

Restablecer las propiedades del PIN de mensajería unificada

Proporciona todos los poderes necesarios para restablecer las propiedades del PIN de mensajería unificada para las cuentas de usuario.

Administración de recursos

Proporciona todos los poderes necesarios para modificar las propiedades de los recursos gestionados, incluidos los recursos asociados a cualquier cuenta de usuario. Asigne esta función a los administradores asistentes responsables de gestionar objetos de recurso.

Administración de buzones de recursos

Proporciona todos los poderes necesarios para gestionar buzones de recursos.

Autoadministración

Proporciona todos los poderes necesarios para modificar las propiedades básicas, como números de teléfono, de su propia cuenta de usuario. Asigne esta función a los administradores asistentes para permitirles gestionar su propia información personal.

Administración de buzones compartidos

Proporciona todos los poderes necesarios para crear, modificar, suprimir y ver las propiedades de los buzones compartidos. Asigne esta función a todos los administradores asistentes responsables de gestionar buzones compartidos.

Recursos de inicio y parada

Proporciona todos los poderes necesarios para pausar, iniciar, reanudar o detener un servicio, iniciar o detener un dispositivo o impresora, apagar un equipo o sincronizar los controladores de dominio. También proporciona todos los poderes necesarios para pausar, reanudar e iniciar servicios, detener dispositivos o colas de impresión y apagar equipos. Asigne esta función a los administradores asistentes responsables de gestionar objetos de recurso.

Transformar un usuario

Proporciona todos los poderes necesarios para añadir un usuario o eliminar un usuario en los grupos que se encuentran en una cuenta de plantilla, incluida la capacidad de modificar las propiedades del usuario mientras se transforma.

Administración del servidor del Historial de cambios unificado

Proporciona los poderes necesarios para configurar, ver y suprimir las configuraciones del servidor del Historial de cambios unificado.

Administración de usuarios

Proporciona todos los poderes necesarios para gestionar cuentas de usuario, buzones de correo de Microsoft Exchange asociados y pertenencias a grupos. Asigne esta función a los administradores asistentes responsables de gestionar cuentas de usuario.

Ver la información de los recopiladores de Active Directory, DRA e informes de gestión, y la configuración de base de datos

Proporciona todos los poderes necesarios para ver la información de los recopiladores de AD, DRA e informes de gestión, y la configuración de base de datos.

Ver todas las propiedades del equipo

Proporciona todos los poderes necesarios para ver las propiedades de una cuenta de equipo. Asigne esta función a los administradores asistentes responsables de auditar equipos.

Ver todas las propiedades del grupo

Proporciona todos los poderes necesarios para ver las propiedades de un grupo. Asigne esta función a los administradores asistentes responsables de auditar grupos.

Ver todas las propiedades del buzón de recursos

Proporciona todos los poderes necesarios para ver las propiedades de un buzón de recursos. Asigne esta función a los administradores asistentes responsables de auditar buzones de recursos.

Ver todas las propiedades de usuario

Proporciona todos los poderes necesarios para ver las propiedades de una cuenta de usuario. Asigne esta función a los administradores asistentes responsables de auditar cuentas de usuario.

Administración del servidor de Automatización del flujo de trabajo

Proporciona los poderes necesarios para configurar, ver y suprimir las configuraciones del servidor de Automatización del flujo de trabajo.

Administración de WTS

Proporciona todos los poderes necesarios para gestionar las propiedades de Windows Terminal Server (WTS) para las cuentas de usuario de la ActiveView. Si utiliza WTS, asigne esta función a los administradores asistentes responsables del mantenimiento de las propiedades de WTS de las cuentas de usuario.

Acceso a las funciones integradas

Acceda a las funciones integradas para auditar el modelo de delegación por defecto o gestione su propia configuración de seguridad.

Para acceder a las funciones integradas:

- 1 Desplácese a **Delegation Management** (Gestión de delegación) > **Manage Roles** (Gestionar funciones).
- 2 Asegúrese de que el campo de búsqueda esté en blanco y haga clic en **Find Now** (Buscar ahora) en el panel **List items that match my criteria** (Mostrar elementos que coincidan con los criterios).
- 3 Seleccione la función adecuada.

Uso de funciones integradas

No se pueden suprimir ni modificar las funciones integradas. Sin embargo, puede incorporar las funciones integradas en el modelo de delegación existente o utilizar estas funciones para diseñar e implementar su propio modelo.

Puede utilizar las funciones integradas de las siguientes formas:

- ♦ Asocie una función integrada a una cuenta de usuario o a un grupo de administradores asistentes. Esta asociación proporciona al usuario o miembros del grupo de administradores asistentes los poderes adecuados para la tarea.
- ♦ Clone una función integrada y utilice ese clon como base para una función personalizada. Puede añadir otras funciones o poderes a esa nueva función y eliminar los poderes incluidos originalmente en la función integrada.

Para obtener más información sobre el diseño de un modelo de delegación dinámico, consulte [Descripción del modelo de delegación dinámica](#).

4.3.2 Creación de funciones personalizadas

Al crear una función, puede delegar rápida y fácilmente un conjunto de poderes que representa una tarea administrativa o un flujo de trabajo. Puede crear y gestionar funciones desde **Delegation Management** (Gestión de delegación) > nodo **Funciones** de la consola de delegación y configuración. En este nodo, puede realizar las siguientes acciones:

- ♦ Crear nuevas funciones.
- ♦ Clonar funciones existentes.
- ♦ Modificar las propiedades de la función.
- ♦ Suprimir funciones.
- ♦ Gestionar asignaciones de funciones.
 - ♦ Delegar una nueva asignación.
 - ♦ Eliminar una asignación existente.
 - ♦ Ver las propiedades de un administrador asistente asignado.
 - ♦ Ver las propiedades de una ActiveView asignada.
- ♦ Gestionar las funciones y los poderes de una función (las funciones se pueden anidar).
- ♦ Generar informes de cambio de funciones.

Para ejecutar cualquiera de las acciones identificadas en esta sección, por lo general, debe seleccionar el nodo **Funciones** y realizar una de las siguientes acciones:

- ♦ Utilice el menú **Tareas** o el menú contextual para abrir el asistente o el cuadro de diálogo correspondientes para continuar con la acción necesaria.
- ♦ Busque el objeto de función en el panel **List items that match my criteria** (Mostrar los elementos que coincidan con los criterios) y utilice el menú **Tareas** o el menú contextual para seleccionar y abrir el asistente o el cuadro de diálogo correspondientes para seguir adelante con la acción necesaria.

Para llevar a cabo cualquiera de las acciones anteriores, debe disponer de los poderes adecuados, como los que se incluyen en la función Gestionar el modelo de seguridad.

4.4 Poderes

Los poderes son los pilares iniciales de la administración de "privilegios mínimos". La asignación de poderes a los usuarios le ayuda en la implementación y el mantenimiento del modelo de seguridad dinámico. Puede realizar estos procedimientos en la consola de delegación y configuración.

4.4.1 Poderes integrados

Hay más de 390 poderes integrados para gestionar objetos y realizar tareas administrativas habituales con las que puede trabajar al definir funciones y realizar asignaciones de delegación. Los poderes integrados no se pueden suprimir, pero puede clonarlos para convertirlos en poderes personalizados. A continuación, se incluyen algunos ejemplos de poderes integrados:

Crear un grupo y modificar todas sus propiedades

Proporciona el poder para crear grupos y especificar todas las propiedades durante la creación de grupos.

Eliminar una cuenta de usuario

Si la Papelera está habilitada, proporciona el poder para transferir cuentas de usuario a la Papelera. Si la Papelera está inhabilitada, proporciona el poder para suprimir de forma permanente cuentas de usuario.

Modificar todas las propiedades del equipo

Proporciona el poder para modificar todas las propiedades de las cuentas de equipo.

4.4.2 Implementación de poderes personalizados

Para crear un poder personalizado, puede crear un nuevo poder o clonar uno existente. Puede utilizar un poder existente como plantilla para las nuevas delegaciones de poderes. Un poder define las propiedades de un objeto que un administrador asistente puede ver, modificar o crear en el dominio o el subárbol gestionados. Los poderes personalizados pueden incluir acceso a varias propiedades como, por ejemplo, el poder *Ver todas las propiedades de usuario*.

Nota: No se pueden clonar todos los poderes integrados.

Puede implementar los poderes integrados desde **Delegation Management** (Gestión de delegación) > nodo **Poderes** de la consola de delegación y configuración. En este nodo, puede realizar las siguientes acciones:

- ♦ Ver todas las propiedades de los poderes.
- ♦ Crear nuevos poderes.
- ♦ Clonar poderes existentes.
- ♦ Modificar los poderes personalizados
- ♦ Generar informes de cambio de poderes.

Para llevar a cabo estas acciones, debe disponer de los poderes adecuados, como los que se incluyen en la función Gestionar el modelo de seguridad.

Tenga en cuenta el siguiente proceso antes de intentar crear un nuevo poder.

1. Revise los poderes proporcionados con DRA.

2. Decida si necesita un poder personalizado. Si es pertinente, puede clonar un poder personalizado existente.
3. Realice los procedimientos adecuados del Asistente. Por ejemplo, complete el Asistente para crear nuevos poderes.
4. Consulte el nuevo poder.
5. Modifique el nuevo poder si es necesario.

Para ejecutar cualquiera de las acciones identificadas en esta sección, por lo general, debe seleccionar el nodo **Poderes** y realizar una de las siguientes acciones:

- ♦ Utilice el menú **Tareas** o el menú contextual para abrir el asistente o el cuadro de diálogo correspondientes para continuar con la acción necesaria.
- ♦ Busque el objeto de poder en el panel **List items that match my criteria** (Mostrar los elementos que coincidan con los criterios) y utilice el menú **Tareas** o el menú contextual para seleccionar y abrir el asistente o el cuadro de diálogo correspondientes para seguir adelante con la acción necesaria.

4.4.3 Ampliación de poderes

Puede añadir permisos o funciones a un poder para ampliarlo.

Por ejemplo, para permitir que un administrador asistente cree una cuenta de usuario, puede asignar el poder *Crear usuarios y modificar todas sus propiedades* o *Crear usuarios y modificar las propiedades limitadas*. Si asigna también el poder *Añadir un nuevo usuario al grupo*, el administrador asistente puede añadir esa nueva cuenta de usuario a un grupo mientras se utiliza el Asistente para crear usuarios. En este caso, el poder *Añadir un nuevo usuario al grupo* proporciona una función adicional al Asistente. El poder *Añadir un nuevo usuario al grupo* es el **poder de ampliación**.

Los poderes de ampliación no pueden añadir permisos ni funciones por sí mismos. Para delegar correctamente una tarea que incluya un poder de ampliación, debe asignar el poder de ampliación junto con el poder que desea ampliar.

Nota

- ♦ Para crear correctamente un grupo e incluir el nuevo grupo en una *ActiveView*, debe disponer del poder *Añadir un nuevo grupo a ActiveView* en la *ActiveView* especificada. La *ActiveView* especificada debe incluir también la unidad administrativa o el contenedor integrado que incluirá el nuevo grupo.
 - ♦ Para clonar correctamente un grupo e incluir el nuevo grupo en una *ActiveView*, debe disponer del poder *Añadir un grupo clonado a una ActiveView* en la *ActiveView* especificada. La *ActiveView* especificada también debe incluir el grupo de origen, así como la unidad administrativa o el contenedor integrado que incluirá el nuevo grupo.
-

En la tabla siguiente, se muestran algunos ejemplos de acciones que se pueden configurar al crear un nuevo poder o modificar las propiedades de un poder existente:

Para delegar esta tarea	Asigne este poder	Y este poder de ampliación
Clonar un grupo e incluir el nuevo grupo en la <i>ActiveView</i> especificada	Clonar un grupo y modificar todas sus propiedades	Añadir un grupo clonado a una <i>ActiveView</i>
Crear un grupo e incluir el nuevo grupo en la <i>ActiveView</i> especificada	Crear un grupo y modificar todas sus propiedades	Añadir un nuevo grupo a <i>ActiveView</i>

Para delegar esta tarea	Asigne este poder	Y este poder de ampliación
Crear un contacto habilitado para correo	Crear un contacto y modificar todas sus propiedades Crear un contacto y modificar las propiedades limitadas	Habilitar el correo electrónico del nuevo contacto
Crear un grupo habilitado para correo	Crear un grupo y modificar todas sus propiedades	Habilitar el correo electrónico para el nuevo grupo
Crear una cuenta de usuario habilitada para correo	Crear usuarios y modificar todas sus propiedades Crear usuarios y modificar las propiedades limitadas	Habilitar el correo electrónico para el nuevo usuario
Crear una cuenta de usuario y añadir la nueva cuenta a grupos específicos	Crear usuarios y modificar todas sus propiedades Crear usuarios y modificar las propiedades limitadas	Añadir un nuevo usuario al grupo

4.5 Asignaciones de delegación

Puede gestionar asignaciones de delegación desde **Delegation Management** (Gestión de delegación) > nodo **Administrador asistente** en la consola de delegación y configuración. En este nodo, puede ver las funciones y los poderes asignados a los administradores asistentes y gestionar las asignaciones de funciones y ActiveViews. También puede realizar lo siguiente con los grupos de administradores asistentes:

- ♦ Añadir miembros de grupos.
- ♦ Crear grupos.
- ♦ Clonar grupos.
- ♦ Suprimir grupos.
- ♦ Modificar las propiedades del grupo

Para ver y gestionar las asignaciones y realizar cambios en los grupos de administradores asistentes, debe disponer de los poderes adecuados, como los que se incluyen en la función Gestionar el modelo de seguridad.

Para ejecutar cualquiera de las acciones identificadas en esta sección, por lo general, debe seleccionar el nodo **Administradores asistentes** y realizar una de las siguientes acciones:

- ♦ Utilice el menú Tareas o el menú contextual para abrir el asistente o el cuadro de diálogo correspondientes para continuar con la acción necesaria.
- ♦ Busque el grupo o el administrador asistente en el panel **List items that match my criteria** (Mostrar los elementos que coincidan con los criterios) y utilice el menú **Tareas** o el menú contextual para seleccionar y abrir el asistente o el cuadro de diálogo correspondientes para seguir adelante con la acción necesaria.

5 Automatización de directivas y procesos

Este capítulo proporciona información que le ayudará a entender cómo funcionan las directivas en el entorno de DRA y qué son las opciones de directiva. También explica cómo se utilizan los activadores y el flujo de trabajo automatizado para automatizar los procesos al trabajar con objetos en Active Directory.

5.1 Descripción de la directiva de DRA

DRA le permite configurar varias directivas que le ayudarán a proteger su empresa y evitar que se dañen los datos. Estas directivas funcionan dentro del contexto del modelo de seguridad dinámico, lo que garantiza que la aplicación de directivas esté automáticamente al día en relación con los cambios de la empresa. El establecimiento de directivas, como las convenciones de denominación, los límites de uso del disco y la validación de propiedades, le permite aplicar reglas que ayudarán a mantener la integridad de los datos de su empresa.

En DRA, puede definir rápidamente reglas de directiva para estas áreas de gestión empresarial:

- ♦ Microsoft Exchange
- ♦ Office 365
- ♦ Directorio personal.
- ♦ Generación de contraseñas

DRA también proporciona directivas integradas para grupos, cuentas de usuario y equipos.

Para administrar o definir directivas, debe disponer de los poderes adecuados, como los que se incluyen en las funciones Administradores de DRA o Gestionar directivas y activadores de automatización. Para ayudarle a gestionar las directivas, DRA proporciona el informe de información de directiva. Este informe proporciona la siguiente información:

- ♦ Indica si se ha habilitado la directiva.
- ♦ Muestra las operaciones asociadas.
- ♦ Muestra los objetos que se rigen por esta directiva.
- ♦ Proporciona información sobre el ámbito de la directiva.

Puede utilizar este informe para asegurarse de que se hayan definido correctamente las directivas. También puede utilizar este informe para comparar las propiedades de las directivas, detectar conflictos y aplicar de forma más eficaz las directivas en su empresa.

5.1.1 Cómo aplica las directivas el servidor de administración

Puede asociar cada tarea u operación de administración a una o varias directivas. Al realizar una operación asociada a una directiva, el servidor de administrador ejecuta la directiva y aplica las reglas especificadas. Si el servidor detecta una infracción de la directiva, devuelve un mensaje de

error. Si el servidor no detecta ninguna infracción de la directiva, completa la operación. Puede limitar el ámbito de una directiva al asociarla a determinados grupos de administradores asistentes o ActiveViews.

Si se ha asociado una operación a varias directivas, el servidor de administración las aplica en orden alfabético. Es decir, la directiva A se aplicará antes que la directiva B, independientemente de las reglas especificadas.

Para asegurarse de que las directivas no entren en conflicto entre sí, siga las siguientes directrices:

- ♦ Asigne un nombre a las directivas para que se ejecuten en el orden correcto.
- ♦ Compruebe que cada directiva no interfiera con las validaciones o las acciones realizadas por otras directivas.
- ♦ Pruebe de forma exhaustiva las directivas personalizadas antes de implementarlas en el entorno de producción

El servidor de administración introduce el estado de la directiva en el registro de auditoría cada vez que se ejecuta una directiva. Estas entradas de registro incluyen el código de devolución, las operaciones asociadas, los objetos en los que se han realizado acciones y si la directiva personalizada se ha aplicado correctamente.

Advertencia: Las directivas se ejecutan mediante la cuenta de servicio de administración. Como la cuenta de servicio dispone de permisos de administrador, las directivas tienen acceso completo a todos los datos de la empresa. Por lo tanto, los administradores asistentes asociados a la función integrada Gestionar directivas y activadores de automatización podrían obtener más poderes de los que tenía intención de otorgar.

5.1.2 Directiva integrada

Las directivas integradas se implementan al instalar el servidor de administración. Al trabajar con estas directivas, es posible que aparezcan los siguientes términos:

Ámbito de la directiva

Define los objetos o las propiedades a los que DRA aplica la directiva. Por ejemplo, algunas directivas permiten aplicar una directiva a determinados administradores asistentes en ActiveViews específicas. Algunas directivas permiten elegir entre diferentes clases de objetos, como cuentas de usuario o grupos.

Directivas globales

Aplique las reglas de directiva en todos los objetos de la clase o tipo especificados en los dominios gestionados. Las directivas globales no le permiten limitar el alcance de los objetos a los que se aplica la directiva.

Relación de directivas

Define si la directiva se aplica de forma conjunta o por sí misma. Para establecer una relación de directivas, defina dos o más reglas que se apliquen a la misma acción y elija el miembro de una opción de grupo de directivas. Si la propiedad o los parámetros de la operación coinciden con cualquiera de las reglas, la operación se realizará correctamente.

Descripción de las directivas integradas

Las directivas integradas proporcionan reglas de negocios para abordar problemas habituales de seguridad e integridad de los datos. Estas directivas forman parte del modelo de seguridad por defecto, lo que le permite integrar las funciones de seguridad de DRA en la configuración empresarial existente.

DRA proporciona dos formas de aplicar directivas. Puede crear directivas personalizadas o elegir entre varias directivas integradas. Las directivas integradas facilitan la aplicación de directivas sin necesidad de desarrollar guiones personalizados. Si necesita implementar una directiva personalizada, puede adaptar una directiva existente para que se ajuste a sus necesidades. La mayoría de las directivas le permiten modificar el texto del mensaje de error, cambiar el nombre de la directiva, añadir una descripción y especificar cómo se aplica.

Al instalar DRA, están habilitadas diversas directivas integradas. Las siguientes directivas se implementan por defecto. Si no desea aplicar estas directivas, puede inhabilitarlas o suprimirlas.

Nombre de directiva	Valor por defecto	Descripción
\$ComputerNameLengthPolicy	64 15 (anterior a Windows 2000)	Limita el número de caracteres en el nombre de equipo actual o anterior a Windows 2000.
\$GroupNameLengthPolicy	64 20 (anterior a Windows 2000)	Limita el número de caracteres en el nombre de grupo actual o anterior a Windows 2000.
\$GroupSizePolicy	5000	Limita el número de miembros de un grupo.
\$NameUniquenessPolicy	Ninguno	Garantiza que los nombres de CN actuales y anteriores a Windows 2000 sean exclusivos en todos los dominios gestionados.
\$SpecialGroupsPolicy	Ninguno	Impide una derivación no comprobada de poderes en el entorno.
\$UCPowerConflictPolicy	Ninguno	Impide la derivación de poderes al establecer los poderes para crear y clonar usuarios se excluyan mutuamente.
\$UPNUniquenessPolicy	Ninguno	Garantiza que los nombres de UPN sean exclusivos en todos los dominios gestionados.
\$UserNameLengthPolicy	64 20 (nombre de entrada a la sesión de nivel inferior)	Limita el número de caracteres en el nombre de entrada a la sesión del usuario o inferior.

Directivas disponibles

DRA proporciona varias directivas que puede personalizar para el modelo de seguridad.

Nota: Puede crear una directiva que requiera una entrada para una propiedad que no esté disponible actualmente en las interfaces de usuario de DRA. Si la directiva requiere una entrada y la interfaz de usuario no proporciona un campo para introducir el valor, como un departamento para una nueva cuenta de usuario, no podrá crear ni gestionar el objeto. Para evitar este problema, configure las directivas que requieran que solo se pueda acceder a esas propiedades desde las interfaces de usuario.

Crear una directiva personalizada

Permite vincular un guión o un archivo ejecutable a una operación de DRA o Exchange. Las directivas personalizadas permiten validar cualquier operación que elija.

Aplicar una longitud máxima de nombre

Permite aplicar globalmente la longitud máxima de nombre para cuentas de usuario, grupos, unidades administrativas, contactos o equipos.

La directiva comprueba el contenedor de nombres (nombre común o `cn`) o el nombre anterior a Windows 2000 (nombre de entrada a la sesión del usuario).

Aplicar un número máximo de miembros de grupo

Permite aplicar globalmente el límite de miembros de un grupo.

Aplicar nombres exclusivos de cuenta anteriores a Windows 2000

Comprueba que un nombre anterior a Windows 2000 sea exclusivo en todos los dominios gestionados. En los dominios de Microsoft Windows, los nombres anteriores a Windows 2000 deben ser exclusivos dentro de un dominio. Esta directiva global aplica esta regla en todos los dominios gestionados.

Aplicar nombres principales de usuario exclusivos

Comprueba que un nombre principal de usuario (UPN, User Principal Name) sea exclusivo en todos los dominios gestionados. En los dominios de Microsoft Windows, los UPN deben ser exclusivos dentro de un dominio. Esta directiva aplica esta regla en todos los dominios gestionados. Como se trata de una directiva global, DRA proporciona el nombre, la descripción y la relación de directivas.

Limitar las acciones que se realizan en miembros de grupos especiales

Impide gestionar miembros de un grupo de administradores a menos que sea miembro de ese grupo. Esta directiva global está habilitada por defecto.

Al limitar las acciones de los miembros de los grupos de administradores, el Asistente para crear directivas no requiere información adicional. Puede especificar un mensaje de error personalizado. Como se trata de una directiva global, DRA proporciona el nombre, la descripción y la relación de directivas.

Evitar que los administradores asistentes creen y clonen usuarios en la misma AV

Impide una posible derivación de poderes. Cuando esta directiva está habilitada, puede crear o clonar cuentas de usuario, pero no puede disponer de ambos poderes. Esta directiva global garantiza que no se puedan crear y clonar cuentas de usuario en la misma ActiveView.

Esta directiva no requiere información adicional.

Definir la directiva de convención de denominación

Permite establecer convenciones de denominación que se aplican a administradores asistentes, ActiveViews y clases de objetos específicos, como cuentas de usuario o grupos.

También puede especificar los nombres exactos supervisados por esta directiva.

Crear una directiva para validar una propiedad específica

Permite crear una directiva para validar cualquier propiedad de una unidad administrativa o un objeto de cuenta. Puede especificar un valor por defecto, una máscara de formato de propiedad, y los valores y los rangos válidos.

Utilice esta directiva para aplicar la integridad de los datos mediante la validación de campos de entrada específicos al crear, clonar o modificar propiedades de determinados objetos. Esta directiva proporciona una gran flexibilidad y eficacia para validar entradas, proporcionar entradas por defecto y limitar las opciones de entrada para diversos campos de propiedad. Con esta directiva, puede solicitar que se realice una entrada correcta antes de que se complete la tarea, lo que permite mantener la integridad de los datos en los dominios gestionados.

Por ejemplo, suponga que tiene tres departamentos: Fabricación, Ventas y Administración. Puede limitar las entradas que DRA aceptará solo para estos tres valores. También puede utilizar esta directiva para aplicar formatos de números de teléfono adecuados, proporcionar un rango de datos válidos o requerir una entrada para el campo de dirección de correo electrónico. Para especificar varias máscaras de formato para un número de teléfono como, por ejemplo, (123)456 7890, así como 456 7890, defina la máscara de formato de la propiedad como (###)### ####,### ####.

Crear una directiva para aplicar las licencias de Office 365

Permite crear una directiva para asignar licencias de Office 365 en función de la pertenencia al grupo de Active Directory. Esta directiva también aplica la eliminación de las licencias de Office 365 al suprimir un miembro del grupo de Active Directory correspondiente.

Si un usuario que no se haya sincronizado con la nube se añade al grupo de Active Directory, este se sincronizará antes de que se asigne una licencia de Office 365 al usuario.

Durante la creación de la directiva, puede especificar varias propiedades y configuraciones, como el nombre de la directiva y la redacción del mensaje de error que aparece cuando un administrador asistente intenta realizar una acción que infringe esta directiva.

Por defecto, las directivas que cree para aplicar las licencias de Office 365 no se implementarán cuando se realicen cambios fuera de DRA, a menos que también habilite la programación de actualización de licencias en la página de propiedades del inquilino.

Uso de directivas integradas

Como las directivas integradas forman parte del modelo de seguridad por defecto, puede utilizar estas directivas para aplicar el modelo de seguridad actual o modificarlas para satisfacer mejor sus necesidades. Puede cambiar el nombre, la configuración de las reglas, el ámbito, la relación de directivas y el mensaje de error de varias directivas integradas. Puede habilitar o inhabilitar cada directiva integrada.

También puede crear fácilmente nuevas directivas.

5.1.3 Implementación de directivas personalizadas

Las directivas personalizadas permiten aprovechar por completo la eficacia y la flexibilidad del modelo de seguridad por defecto. Mediante el uso de directivas personalizadas, puede integrar DRA en componentes empresariales existentes al mismo tiempo que garantiza que se cumplan las reglas patentadas. Puede utilizar la función de directivas personalizadas para ampliar las directivas de su empresa.

Puede crear y aplicar directivas personalizadas mediante la asociación de un archivo ejecutable o un guión a una operación de administración. Por ejemplo, un guión de directiva asociado con la operación `UserCreate` puede comprobar la base de datos de RR.HH. para comprobar si existe el

empleado especificado. Si el empleado existe en la base de datos de RR.HH. y no tiene una cuenta existente, el guión recupera el ID, el nombre y el apellido del empleado de la base de datos. La operación se completa correctamente y llena la ventana de propiedades de la cuenta de usuario con la información adecuada. Sin embargo, si el empleado ya dispone de una cuenta, se produce un error en la operación.

Los guiones le proporcionan una enorme cantidad de flexibilidad y eficacia. Para crear sus propios guiones de directivas, puede utilizar el proveedor ADSI de Directory and Resource Administrator (proveedor ADSI), el kit de desarrollo de software (SDK) y cmdlets de PowerShell. Para obtener más información sobre cómo crear sus propios guiones de directivas, consulte la sección de referencia en el sitio de [documentación de DRA](#).

5.1.4 Restricción de grupos de seguridad integrados nativos

Para proporcionar un entorno más seguro, DRA permite limitar los poderes otorgados a los grupos de seguridad integrados de Microsoft Windows. La capacidad de modificar la pertenencia a grupo, las propiedades integradas del grupo de seguridad o las propiedades de los miembros del grupo puede tener importantes implicaciones de seguridad. Por ejemplo, si puede cambiar la contraseña de un usuario del grupo Operadores de servidores, puede entrar a la sesión como ese usuario y disponer de los poderes delegados a este grupo de seguridad integrado.

DRA impide que se produzca este problema de seguridad al proporcionar una directiva que comprueba los poderes que tiene para un grupo de seguridad integrado nativo y sus miembros. Esta validación garantiza que las acciones solicitadas no amplíen estos poderes. Después de habilitar esta directiva, un administrador asistente que sea miembro de un grupo de seguridad integrado, como el grupo Operadores de servidores, solo puede gestionar otros miembros del mismo grupo.

Grupos de seguridad integrados nativos que puede restringir

Puede restringir los poderes de los siguientes grupos de seguridad integrados de Microsoft Windows mediante las directivas de DRA:

- ♦ Operadores de cuentas
- ♦ Administradores
- ♦ Operadores de copia de seguridad
- ♦ Editores de CERT
- ♦ Administradores de DNS
- ♦ Administradores de dominio
- ♦ Administradores de empresa
- ♦ Propietarios del creador de directivas de grupo
- ♦ Operadores de impresión
- ♦ Administradores de esquema

Nota: DRA hace referencia a los grupos de seguridad integrados por sus identificadores internos. Por lo tanto, DRA admitirá estos grupos, incluso aunque se cambie su nombre. Esta función garantiza que DRA admita grupos de seguridad integrados con nombres diferentes en distintos países. Por ejemplo, DRA hace referencia a los grupos Administradores y *Administratoren* con el mismo identificador interno.

Restringir las acciones realizadas en grupos de seguridad integrados nativos

DRA utiliza la directiva para limitar los poderes que pueden utilizar los grupos de seguridad integrados nativos y sus miembros. Esta directiva, denominada `$SpecialGroupsPolicy`, restringe las acciones que un miembro de un grupo de seguridad integrado nativo puede realizar en otros miembros u otros grupos de seguridad integrados nativos. DRA habilita esta directiva por defecto. Si no desea restringir las acciones realizadas en los grupos de seguridad integrados nativos y sus miembros, puede inhabilitar esta directiva.

Si se ha habilitado esta directiva, DRA utiliza las siguientes pruebas de validación para determinar si se permite una acción en un grupo de seguridad integrado nativo o sus miembros:

- ♦ Si es un administrador de Microsoft Windows, puede realizar acciones en grupos de seguridad integrados nativos y sus miembros que dispongan de los poderes adecuados.
- ♦ Si es miembro de un grupo de seguridad integrado, puede realizar acciones en el mismo grupo de seguridad integrado y sus miembros, siempre que disponga de los poderes adecuados.
- ♦ Si no es miembro de un grupo de seguridad integrado, no podrá modificar un grupo de seguridad integrado ni sus miembros.

Por ejemplo, si es miembro de los grupos Operadores de servidores y Operadores de cuentas, y dispone de los poderes adecuados, puede realizar acciones en los miembros de un grupo, otro o ambos. Sin embargo, no puede realizar acciones en una cuenta de usuario que sea miembro de los grupos Operadores de impresión y Operadores de cuentas.

DRA le impide realizar las siguientes acciones en los grupos de seguridad integrados nativos:

- ♦ Clonación de un grupo.
- ♦ Creación de un grupo
- ♦ Supresión de un grupo
- ♦ Adición de un miembro a un grupo
- ♦ Eliminación de un miembro de un grupo.
- ♦ Traslado de un grupo a una unidad administrativa.
- ♦ Modificación de las propiedades de un grupo
- ♦ Copia de un buzón.
- ♦ Eliminación de un buzón.
- ♦ Clonación de una cuenta de usuario
- ♦ Creación de una cuenta de usuario
- ♦ Supresión de una cuenta de usuario
- ♦ Traslado de una cuenta de usuario a una unidad administrativa.
- ♦ Modificación de las propiedades de la cuenta de usuario

DRA también restringe las acciones para garantizar que no obtenga poderes para un objeto. Por ejemplo, al añadir una cuenta de usuario a un grupo, DRA comprueba que no obtenga poderes adicionales en la cuenta de usuario porque sea miembro de ese grupo. Esta validación ayuda a la protección frente a una derivación de poderes.

5.1.5 Gestión de directivas

Mediante el nodo "Policy and Automation Management" (Gestión de directivas y automatización), puede acceder a las directivas de Microsoft Exchange y el directorio personal, así como a las directivas integradas y personalizadas. Utilice las siguientes tareas habituales para mejorar la seguridad de su empresa y la integridad de los datos.

Configurar las directivas de Exchange

Permite definir las reglas de configuración de Microsoft Exchange, directiva de buzón, denominación automática y generación de apoderado. Estas reglas pueden definir cómo se gestionan los buzones cuando un administrador asistente crea, modifica o suprime una cuenta de usuario.

Configurar las directivas de Office 365

Permite aplicar directivas de caracteres no válidos y longitud de caracteres para evitar errores en la sincronización de directorios.

Las reglas de Office 365 permiten especificar cómo Exchange Online gestiona los buzones de Office 365 al crear o suprimir cuentas de usuario.

Configurar las directivas del directorio personal

Permite crear, renombrar o suprimir automáticamente directorios y recursos compartidos personales cuando un administrador asistente crea o suprime una cuenta de usuario, o cambia su nombre. La directiva de directorio personal también permite habilitar o inhabilitar la compatibilidad con cuotas de disco para directorios personales en servidores de Microsoft Windows, así como en servidores que no sean de Windows.

Configurar las directivas de generación de contraseñas

Permite definir los requisitos para las contraseñas generadas por DRA.

Directiva de Microsoft Exchange

Exchange proporciona varias directivas para ayudarle a gestionar de forma más eficaz los objetos de Microsoft Exchange. La directiva de Microsoft Exchange permite automatizar la gestión de buzones, aplicar convenciones de denominación para alias y almacenes de buzones, y generar automáticamente direcciones de correo electrónico.

Estas directivas pueden ayudarle a simplificar los flujos de trabajo y mantener la integridad de los datos. Por ejemplo, puede especificar cómo Exchange gestiona los buzones al crear, modificar o suprimir cuentas de usuario. Para definir y gestionar las directivas de Microsoft Exchange, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización.

Especificar una directiva de dirección de correo electrónico por defecto

Para especificar una directiva de dirección de correo electrónico por defecto, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización, y su licencia debe admitir el producto Exchange.

Para especificar una directiva de dirección de correo electrónico por defecto:

- 1 Acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Exchange Policies** (Configurar las directivas de Exchange) > **Proxy Generation** (Generación de apoderado).

- 2 Especifique el dominio del servidor de Microsoft Exchange.
 - 2a Haga clic en **Examinar**.
 - 2b Especifique los criterios de búsqueda adicionales según sea necesario y, a continuación, haga clic en **Find Now** (Buscar ahora).
 - 2c Seleccione el dominio que desea configurar y, a continuación, haga clic en **Aceptar**.
- 3 Especifique las reglas de generación de apoderado para el dominio seleccionado.
 - 3a Haga clic en **Añadir**.
 - 3b Seleccione un tipo de apoderado. Por ejemplo, haga clic en **Dirección de Internet**.
 - 3c Acepte el valor por defecto o escriba una nueva regla de generación de apoderado y, a continuación, haga clic en **Aceptar**.

Para obtener más información acerca de las cadenas de sustitución admitidas para las reglas de generación de apoderado, consulte [Directiva del cliente de delegación y configuración](#).
- 4 Haga clic en **Atributos personalizados** para editar el nombre personalizado de las propiedades de buzón personalizadas.
 - 4a Seleccione el atributo y haga clic en el botón **Editar**.
 - 4b En la ventana Attribute Properties (Propiedades de atributo), introduzca el nombre del atributo en el campo **Custom name** (Nombre personalizado) y haga clic en **Aceptar**.
- 5 Haga clic en **Aceptar**.

Nota: Los administradores de directivas de DRA deben disponer del poder *Gestionar herramientas personalizadas* para modificar atributos personalizados de la directiva de Microsoft Exchange.

Reglas de buzón

Las reglas de buzón permiten especificar cómo Exchange gestiona los buzones cuando los administradores asistentes crean, clonan, modifican o suprimen cuentas de usuario. Las reglas de buzón gestionan automáticamente los buzones de Microsoft Exchange en función de la forma en que los administradores asistentes gestionan las cuentas de usuario asociadas.

Nota: Si se habilita **Do not allow Assistant Admins to create a user account without a mailbox** (No permitir que los administradores asistentes creen una nueva cuenta de usuario sin un buzón) en los dominios de Microsoft Windows, asegúrese de que el administrador asistente tenga poder para clonar o crear una cuenta de usuario. Al habilitar esta opción, los administradores asistentes deben crear cuentas de usuario con un buzón.

Para especificar las reglas de buzón de Microsoft Exchange, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización, y su licencia debe admitir el producto Exchange.

Para especificar las reglas de buzón de Exchange:

- 1 Acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Exchange Policies** (Configurar las directivas de Exchange) > **Mailbox Rule** (Reglas de buzón).
- 2 Seleccione las directivas de buzón que desea que Exchange aplique cuando cree o modifique cuentas de usuario.
- 3 Haga clic en **Aceptar**.

Directiva de Office 365

Para definir y gestionar las directivas de buzón de Office 365, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización. La licencia debe admitir también el producto Microsoft Exchange.

Para restringir los caracteres no válidos y las longitudes de caracteres con propiedades que se sincronizan con Office 365, haga clic en **Office 365 Rules** (Reglas de Office 365) y seleccione la casilla de verificación **Enforce online mailbox policies for invalid characters and character lengths** (Aplicar directivas de buzón en línea para caracteres no válidos y longitudes de caracteres).

Permitir que DRA gestione las licencias de Office 365 (opcional)

Si desea permitir que DRA gestione sus licencias de Office 365, debe realizar lo siguiente:

- ♦ Crear una directiva de aplicación de licencia.
- ♦ Habilite **License update schedule** (Programación de actualización de licencias) en la página de propiedades del inquilino.

Creación de una directiva para aplicar las licencias de Office 365

Para crear una directiva a fin de aplicar las licencias de Office 365, haga clic en el nodo **Policy and Automation Management** (Gestión de directivas y automatización) en la consola de delegación y configuración y seleccione **New Policy > Create New Policy to Enforce Office 365 Licenses** (Nueva directiva > Crear nueva directiva para aplicar las licencias de Office 365).

Cuando se aplica la directiva y se añade un usuario a Active Directory, DRA utiliza la pertenencia a grupo para asignar automáticamente la licencia de Office 365 al usuario.

Programación de actualización de licencias de Office 365

Las directivas que cree para aplicar las licencias de Office 365 no se aplicarán cuando se realicen cambios fuera de DRA, a menos que también habilite **License update schedule** (Programación de actualización de licencias) en la página de propiedades del inquilino. La tarea de actualización de licencias garantiza que las licencias de Office 365 asignadas a los usuarios coincidan con las directivas de licencia de Office 365.

La tarea de actualización de licencias y las directivas de licencia de Office 365 trabajan de forma conjunta para garantizar que a todos los usuarios gestionados se les asignen solo las licencias de Office 365 que se supone que deben tener.

Nota

- ♦ DRA no gestiona las licencias de Office 365 para cuentas de usuario solo en línea. Para que DRA gestione los usuarios con licencias de Office 365, estos deben sincronizarse con Active Directory.
 - ♦ Si opta por utilizar DRA para gestionar las licencias de Office 365, DRA anulará todos los cambios manuales realizados en Office 365 que se hayan aplicado fuera de DRA la próxima vez que se ejecute la tarea de actualización de licencias.
 - ♦ Si habilita la tarea de actualización de licencias de Office 365 antes de asegurarse de que se hayan configurado correctamente las directivas de licencia de Office 365, las licencias asignadas pueden ser incorrectas después de que se ejecute esa tarea.
-

Creación e implementación de la directiva de directorio personal

Al gestionar una gran cantidad de cuentas de usuario, la creación y el mantenimiento de estos directorios y recursos compartidos pueden requerir mucho tiempo y convertirse en una fuente de errores de seguridad. Es posible que se necesite mantenimiento adicional cada vez que se cree, cambie de nombre o suprima un usuario. Las directivas de directorio personal le ayudarán a gestionar el mantenimiento del directorio personal y los recursos compartidos personales.

DRA permite automatizar la creación y el mantenimiento de los directorios personales del usuario. Por ejemplo, puede configurar fácilmente DRA para que el servidor de administración cree un directorio personal cuando cree una cuenta de usuario. En este caso, si especifica una vía del directorio personal al crear la cuenta de usuario, el servidor crea automáticamente el directorio personal según la vía especificada. Si no especifica una vía, el servidor no creará el directorio personal.

DRA es compatible con las vías del Sistema de archivos distribuido (DFS, Distributed File System) durante la creación de los directorios personales de usuario o la configuración de las directivas de directorio personal para los usuarios en las vías principales permitidas. Puede crear, cambiar de nombre y suprimir directorios personales en vías o particiones de archivadores NetApp y DFS.

Configuración de las directivas de directorio personal

Para configurar las directivas de directorio, los recursos compartidos y las cuotas de disco de volúmenes personales, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización. Cada directiva gestiona automáticamente los directorios, los recursos compartidos y las cuotas de disco de volúmenes personales en función de cómo administre las cuentas de usuario asociadas.

Para configurar las directivas de directorio personal, desplácese a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Home Directory Policies** (Configurar directivas de directorio personal) >

- ♦ Directorio personal.
- ♦ "Home share" (Recurso compartido personal)
- ♦ "Home Volume Disk Quota" (Cuota de disco de volúmenes personales)

Requisitos del servidor de administración de

En cada equipo en el que necesite crear un recurso compartido personal, se deben utilizar una cuenta de servicio o de acceso del servidor de administración con función de administrador en ese equipo o de miembro del grupo de administradores en el dominio correspondiente.

Debe haber un recurso compartido de administración como, por ejemplo, C\$ o D\$, en cada unidad en la que DRA gestione o almacene directorios personales. DRA utiliza los recursos compartidos de administración para realizar algunas tareas de automatización del directorio y los recursos compartidos personales. Si no existen estos recursos compartidos, DRA no podrá proporcionar la automatización de directorios y recursos compartidos personales.

Configuración de las vías permitidas del directorio personal para archivadores NetApp

Para configurar las vías principales permitidas para un archivador NetApp:

- 1 Acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Home Directory Policies** (Configurar las directivas de directorio personal).

- 2 En el recuadro de texto **Allowable parent paths** (Vías principales permitidas), introduzca una de las vías permitidas de la siguiente tabla:

Tipo de recurso compartido	Vía permitida
Windows	(\\nombreArchivo\recursoCompartidoAdmin:\víaRaízVolumen\víaDirectorio)
No Windows	(\\no Windows\recurso compartido)

- 3 Haga clic en **Añadir**.
- 4 Repita los pasos 1 a 3 para cada vía principal permitida cada vez que desee aplicar las directivas de directorio personal.

Descripción de la directiva de directorio personal

Para mantener la coherencia con las directivas de seguridad de Microsoft Windows adecuadas, DRA crea restricciones de control de acceso solo en el nivel de directorio. Al establecer restricciones de control de acceso tanto en el nivel de nombre de recurso compartido como en el nivel de objeto de archivo o directorio, a menudo se obtiene un esquema de acceso confuso para administradores y usuarios.

Al cambiar una restricción de control de acceso para un recurso compartido personal, DRA no cambia la seguridad existente para ese directorio. En este caso, deberá asegurarse de que las cuentas de usuario dispongan de acceso adecuado a sus propios directorios personales.

Reglas y automatización del directorio personal

DRA automatiza las tareas de mantenimiento del directorio personal al gestionar directorios personales cuando se modifica una cuenta de usuario. DRA puede realizar diferentes acciones cuando se crea, clona, modifica, cambia de nombre o suprime una cuenta de usuario.

Para aplicar correctamente la directiva de directorio personal, tenga en cuenta las directrices siguientes:

- ◆ Asegúrese de que la vía especificada utilice el formato correcto.
 - ◆ Para especificar una vía para un único directorio personal, utilice una de las plantillas de la tabla siguiente:

Tipo de recurso compartido	Plantilla de vía
Windows	\\equipo\recurso compartido\ Por ejemplo, si desea que DRA cree automáticamente un directorio personal en la carpeta Home Share del equipo "server01", escriba \\server01\Home Share\ No Windows
No Windows	\\no windows\recurso compartido

- ◆ Para estandarizar la administración del directorio personal en el directorio raíz del recurso personal correspondiente, utilice la sintaxis de la convención de denominación universal, como \\nombre del servidor\C:\vía al directorio raíz.
- ◆ Para especificar una vía para los directorios personales anidados, utilice una de las plantillas de la tabla siguiente:

Tipo de recurso compartido	Plantilla de vía
Windows	<pre>\\equipo\recurso compartido\primer directorio\segundo directorio\</pre> <p>Por ejemplo, si desea que DRA cree automáticamente un directorio personal en el directorio JSmith\Home existente de la carpeta "Home Share" del equipo "server01", escriba \\server01\Home Share\JSmith\Home.</p>
No Windows	<pre>\\no Windows\recurso compartido\primer directorio\segundo directorio\</pre>

Nota: DRA también admite los siguientes formatos: `\\equipo\recurso compartido\nombre de usuario` y `\\equipo\recurso compartido\%username%`. En cada caso, DRA crea automáticamente un directorio personal para la cuenta de usuario asociada.

- ♦ Al definir una directiva o un activador de automatización para gestionar directorios personales en un archivador NetApp, deberá utilizar un formato diferente para especificar el directorio.
 - ♦ Si se utiliza archivadores NetApp, especifique el directorio principal con el siguiente formato: `\\nombreArchivador\recursoCompartidoAdmin:\viaRaízVolumen\viaDirectorio`
 - ♦ La variable "recursoCompartidoAdmin" hace referencia al recurso compartido oculto que se asigna al volumen raíz en el archivador NetApp, como c\$. Por ejemplo, si la vía local del recurso compartido en un archivador NetApp, denominado usfiler, es `c$\vol\vol0\mydirectory`, puede especificar una vía raíz `\\usfiler\c:\vol\vol0\mydirectory` para el archivador NetApp.
- ♦ Para especificar una vía DFS al crear directorios personales de usuario o configurar directivas de directorio personal para los usuarios, utilice `\\servidor\raíz\formato <enlace>`, donde "raíz" puede ser el dominio gestionado o un directorio raíz independiente con el siguiente formato: `\\nombreArchivador\recursoCompartidoAdmin:\viaRaízVolumen\viaDirectorio`.
- ♦ Cree un directorio compartido para almacenar el directorio personal para esta cuenta de usuario.
- ♦ Asegúrese de que DRA pueda acceder al equipo o el recurso compartido a los que se hace referencia en la vía.

Crear un directorio personal al crear una cuenta de usuario

Esta regla permite a DRA crear automáticamente los directorios personales respectivos para nuevas cuentas de usuario. Cuando DRA crea un directorio personal, el servidor de administración utiliza la vía especificada en los campos **Directorio personal** del Asistente para crear usuarios. Posteriormente, puede modificar esta vía a través de la pestaña Perfil de la ventana de propiedades de usuario y DRA trasladará el directorio personal a la nueva ubicación. Si no especifica valores para estos campos, DRA no creará un directorio personal para esa cuenta de usuario.

DRA establece la seguridad para el nuevo directorio según las opciones seleccionadas de **Home directory permissions** (Permisos del directorio personal). Estas opciones permiten controlar el acceso general para todos los directorios personales.

Por ejemplo, puede especificar que los miembros del grupo Administradores tengan control total y los miembros del grupo Ayuda técnica tengan acceso de lectura al recurso compartido en el que se crean los directorios personales de usuario. A continuación, cuando DRA cree un directorio personal del usuario, el directorio personal nuevo podrá heredar estos derechos del

directorío principal. Por lo tanto, los miembros del grupo Administradores tienen control total de todos los directorios personales de usuario y los miembros del grupo Ayuda técnica tienen acceso de lectura a todos los directorios personales de usuario.

Si el directorío personal especificado ya existe, DRA no lo creará ni modificará los permisos del directorío existente.

Cambiar el nombre del directorío personal al cambiar el nombre de la cuenta de usuario

Esta regla permite a DRA realizar las siguientes acciones:

- ♦ Crear un directorío personal al especificar una vía del directorío personal nuevo.
- ♦ Mover el contenido del directorío personal al cambiar la vía del directorío personal.
- ♦ Cambiar el nombre de un directorío personal al cambiar el nombre de la cuenta de usuario.

Al cambiar el nombre una cuenta de usuario, DRA cambia el nombre del directorío personal existente en función del nuevo nombre de cuenta. Si se está utilizando el directorío personal existente, DRA crea un nuevo directorío personal con el nuevo nombre y no cambia el directorío personal existente.

Puede cambiar el nombre del directorío personal si el nombre y la ubicación anteriores del directorío personal son iguales a los nuevos. Sin embargo, si se produce un error en el cambio de nombre del directorío, DRA crea un nuevo directorío personal, transfiere el contenido del directorío personal anterior al nuevo y suprime el directorío personal existente.

Si cambia la vía del directorío personal, DRA intenta crear el directorío personal especificado y transfiere el contenido del directorío personal anterior a la nueva ubicación. También puede configurar la directiva de directorío personal para crear un directorío personal sin transferir el contenido del directorío personal existente. DRA también aplica la ACL asignada desde el directorío anterior al nuevo. Si el directorío personal especificado ya existe, DRA no crea este nuevo directorío ni modifica los permisos de directorío existentes. Si no se ha bloqueado el directorío personal anterior, DRA lo suprime.

Si DRA no puede cambiar el nombre del directorío personal, DRA intentará crear un nuevo directorío personal con un nuevo nombre y copiará el contenido del directorío personal anterior en el nuevo. A continuación, DRA intentará suprimir el directorío personal anterior. Puede configurar DRA para que no copie el contenido del directorío personal anterior en el nuevo y transfiera manualmente el contenido del directorío personal anterior al nuevo para evitar problemas, como la copia de archivos abiertos.

Al suprimir el directorío personal anterior, DRA requiere un permiso explícito para suprimir los subdirectoríos y los archivos de solo lectura del directorío personal anterior. Puede proporcionar a DRA el permiso para suprimir explícitamente los subdirectoríos y los archivos de solo lectura del directorío personal anterior.

Permitir un directorío o una vía principales para un recurso compartido personal

DRA permite especificar los directoríos o las vías principales autorizadas para los recursos compartidos personales de los servidores de archivos. Si dispone de muchas vías de directorío o servidor de archivos que especificar, puede exportarlas a un archivo CSV y añadir las vías desde el archivo CSV a DRA mediante la consola de DRA. DRA utiliza la información introducida en el campo **Allowable parent paths** (Vías principales admitidas) para asegurarse de lo siguiente:

- ♦ DRA no elimina el directorío principal en el servidor de archivos cuando los administradores asistentes suprimen una cuenta de usuario y el directorío principal de la cuenta de usuario.
- ♦ DRA mueve el directorío personal a un directorío o una vía principales válidos en el servidor de archivos cuando cambia el nombre de una cuenta de usuario o cambia la vía del directorío principal de una cuenta de usuario.

Suprimir el directorio personal al suprimir la cuenta de usuario

Esta regla permite a DRA suprimir automáticamente un directorio personal cuando se suprime la cuenta de usuario asociada. Si se habilita la Papelera, DRA no suprimirá el directorio personal hasta que se elimine la cuenta de usuario desde la Papelera. Al suprimir el directorio personal, DRA requiere un permiso explícito para suprimir los subdirectorios y los archivos de solo lectura del directorio personal anterior. Puede proporcionar a DRA el permiso para suprimir explícitamente los subdirectorios y los archivos de solo lectura del directorio personal anterior.

Automatización y reglas de los recursos compartidos personales

DRA automatiza las tareas de mantenimiento de los recursos compartidos personales mediante la gestión de estos recursos cuando se modifica una cuenta de usuario o se gestionan directorios personales. DRA puede realizar diferentes acciones cuando se crea, clona, modifica, cambia de nombre o suprime una cuenta de usuario.

Para mantener la coherencia con las directivas de seguridad de Microsoft Windows adecuadas, DRA no establece restricciones de control de acceso en el nivel de nombre de recurso compartido. En su lugar, DRA establece restricciones de control de acceso solo en el nivel del directorio. Al establecer restricciones de control de acceso tanto en el nivel de nombre de recurso compartido como en el nivel de objeto de archivo o directorio, a menudo se obtiene un esquema de acceso confuso para administradores y usuarios.

Nota: La ubicación especificada debe tener un recurso compartido personal común, como `HOMEDIRS`, en un nivel superior a los directorios personales.

Por ejemplo, la siguiente vía es válida: `\\HOUSEV1\HOMEDIRS\%username%`

La siguiente vía no es válida: `\\HOUSEV1\%username%`

Especificar nombres de recursos compartidos personales

Al definir las reglas de automatización de recursos compartidos personales, puede especificar un prefijo y un sufijo para cada recurso compartido personal creado de forma automática. Mediante la especificación de un prefijo o un sufijo, se puede aplicar una convención de denominación para los recursos compartidos personales.

Por ejemplo, puede habilitar las reglas de automatización Crear directorio personal y Crear recurso compartido personal. Para el recurso compartido personal, especifique un prefijo de carácter de subrayado y un sufijo de signo de dólar. Si se crea un usuario denominado TomS, se debe asignar el nuevo directorio a la unidad U y especificar `\\HOUSEV1\HOMEDIRS\%username%` como la vía de directorio. En este ejemplo, DRA crea un recurso compartido de red denominado `_TomS$` que señala al directorio `\\HOUSEV1\HOMEDIRS\TomS`.

Creación de recursos compartidos personales para nuevas cuentas de usuario

Cuando DRA crea un recurso compartido personal, el servidor de administración utiliza la vía especificada en los campos **Directorio personal** del Asistente para crear usuarios. Puede modificar posteriormente esta vía a través de la pestaña Perfil de la ventana de propiedades de usuario.

DRA crea el nombre del recurso compartido mediante la adición del prefijo y el sufijo especificados, si hay, al nombre de usuario. Si utiliza nombres de cuenta de usuario largos, es posible que DRA no pueda añadir el prefijo y el sufijo del recurso compartido personal especificados. El prefijo y el sufijo, así como el número de conexiones permitidas, se basan en las opciones de creación de recursos compartidos personales que seleccione.

Creación de recursos compartidos personales para cuentas de usuario clonadas

Si ya existe el nombre del recurso compartido personal generado a partir del nombre de cuenta de usuario recién creada, DRA suprime el recurso compartido existente y crea un nuevo recurso compartido en el directorio principal especificado.

Al clonar una cuenta de usuario, el nombre compartido de la cuenta de usuario actual debe existir actualmente. Al clonar una cuenta de usuario, DRA clona también la información del directorio personal y la personaliza para el nuevo usuario.

Modificación de las propiedades del recurso compartido personal

Al cambiar la ubicación del directorio personal, DRA elimina el recurso compartido existente y crea un nuevo recurso compartido en el nuevo directorio personal. Si el directorio personal original está vacío, DRA suprime el directorio original.

Cambio de nombre de recursos compartidos personales para las cuentas de usuario renombradas

Al cambiar el nombre de una cuenta de usuario, DRA suprime el recurso compartido personal existente y crea uno nuevo basado en el nuevo nombre de cuenta. El nuevo recurso compartido señala al directorio personal existente.

Supresión de recursos compartidos personales para cuentas de usuario suprimidas

Al suprimir de forma permanente una cuenta de usuario, DRA suprime el recurso compartido personal.

Reglas de gestión de cuotas de disco de volúmenes personales

DRA permite gestionar cuotas de disco de volúmenes personales. Puede implementar esta directiva en dominios nativos en los que el directorio personal resida en un equipo con Microsoft Windows. Al implementar esta directiva, debe especificar una cuota de disco de al menos 25 MB para permitir un amplio espacio.

Habilitación de generación de contraseñas

Esta función le permite especificar la configuración de directivas para las contraseñas que genera DRA. DRA no aplica esta configuración en las contraseñas que crean los usuarios. Al configurar las propiedades de la directiva de contraseñas, la longitud de la contraseña no debe ser inferior a 6 caracteres ni superior a 127 caracteres. Todos los valores pueden definirse en cero, excepto la longitud de contraseña.

Para configurar las directivas de generación de contraseñas, acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Password Generation Policies** (Configurar directivas de generación de contraseñas) y seleccione la casilla de verificación **Enable Password Policy** (Habilitar directiva de contraseñas). Haga clic en **Password Settings** (Configuración de contraseñas) y configure las propiedades de la directiva de contraseñas.

Tareas de directiva

Para suprimir, habilitar e inhabilitar directivas, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización.

Para llevar a cabo una de estas acciones, desplácese a **Policy and Automation Management** (Gestión de directivas y automatización) > **Policy** (Directiva). Haga clic con el botón derecho en la directiva que desea suprimir, habilitar o inhabilitar en el panel derecho y seleccione la acción deseada.

Implementación de directivas integradas

Para implementar directivas integradas, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización. Para obtener más información acerca de las directivas integradas, consulte [Descripción de las directivas integradas](#).

Nota: Antes de asociar la directiva integrada a un administrador asistente y una ActiveView, compruebe primero que el administrador asistente se haya asignado a esa ActiveView.

Para implementar directivas integradas:

- 1 Desplácese a **Policy and Automation Management** (Gestión de directivas y automatización) > **Policy** (Directiva).
- 2 En el menú Tareas, haga clic en **New Policy** (Nueva directiva) y, a continuación, seleccione el tipo de directiva integrada que desea crear.
- 3 En cada ventana del asistente, especifique los valores adecuados y, a continuación, haga clic en **Siguiente**. Por ejemplo, puede asociar esta nueva directiva a una ActiveView específica, lo que permite que DRA aplique esta directiva en los objetos incluidos en esa ActiveView.
- 4 Revise el resumen y haga clic en **Finalizar**.

Implementación de directivas personalizadas

Para implementar una directiva personalizada, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización.

Para implementar correctamente una directiva personalizada, debe escribir un guión que se ejecute durante una operación (tarea administrativa) específica. En el guión de la directiva personalizada, puede definir mensajes de error para que se muestren siempre que una acción infrinja la directiva. También puede especificar un mensaje de error por defecto mediante el Asistente para crear directivas.

Para obtener más información acerca de cómo escribir directivas personalizadas, ver una lista de las operaciones de administración o utilizar matrices de argumentos, consulte el SDK. Para obtener más información, consulte [Escritura de archivos ejecutables o guiones de directivas personalizadas](#).

Nota

- ♦ Antes de asociar la directiva personalizada a un administrador asistente y una ActiveView, asegúrese primero de que el administrador asistente se haya asignado a esa ActiveView.
- ♦ Si la vía del archivo ejecutable o el guión de la directiva personalizada contiene espacios, escriba la vía entre comillas ("").

Para implementar una directiva personalizada:

- 1 Escriba un archivo ejecutable o un guión de directiva.
- 2 Entre en un equipo cliente de DRA con una cuenta a la que se le haya asignado la función integrada Gestionar directivas y activadores de automatización en el dominio gestionado.
- 3 Inicie la consola de delegación y configuración.
- 4 Conéctese al servidor de administración principal.
- 5 En el panel izquierdo, expanda **Policy and Automation Management** (Gestión de directivas y automatización).

- 6 Haga clic en **Policy** (Directiva).
- 7 En el menú Tareas, haga clic en **New Policy > Create a Custom Policy** (Nueva directiva > Crear una directiva personalizada).
- 8 En cada ventana del asistente, especifique los valores adecuados y, a continuación, haga clic en **Siguiente**. Por ejemplo, puede asociar esta nueva directiva a una ActiveView específica, lo que permite que DRA aplique esta directiva en los objetos incluidos en esa ActiveView.
- 9 Revise el resumen y haga clic en **Finalizar**.

Modificación de las propiedades de directiva

Para modificar todas las propiedades de una directiva, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización.

Para modificar las propiedades de directiva:

- 1 Desplácese a **Policy and Automation Management** (Gestión de directivas y automatización) > **Policy** (Directiva).
- 2 Haga clic en la directiva que desee modificar y seleccione **Propiedades**.
- 3 Modifique las propiedades y los ajustes adecuados para esta directiva.

Escritura de archivos ejecutables o guiones de directivas personalizadas

Para obtener más información acerca de cómo escribir archivos ejecutables o guiones de directivas personalizadas, consulte el SDK.

Para acceder al SDK:

- 1 Asegúrese de que haya instalado el SDK en el equipo. El programa de instalación crea un acceso directo al SDK en el grupo de programas de Directory and Resource Administrator. Para obtener más información, consulte la lista de verificación de instalación en [Instalación del servidor de administración de DRA](#).
- 2 Haga clic en el acceso directo al SDK en el grupo de programas de Directory and Resource Administrator.

Para obtener más información sobre el SDK, consulte "DRA REST Services Guide" (Guía de servicios REST de DRA) en el sitio de [documentación de DRA](#).

5.1.6 Directiva del cliente de delegación y configuración

La directiva de denominación automática incluye tres configuraciones de directivas de Exchange que son exclusivas del cliente de delegación y configuración, lo que significa que se trata de una directiva del cliente.

La directiva de denominación automática permite especificar reglas de denominación automatizada para propiedades específicas de un buzón. Estas opciones permiten establecer convenciones de denominación y generar rápidamente valores estándar para las propiedades de nombre de visualización, nombre de directorio y alias. Exchange permite especificar cadenas de sustitución como, por ejemplo %First y %Last, para varias opciones de denominación automatizada.

Cuando Exchange genera un alias o un nombre de directorio, comprueba si el valor generado es exclusivo. Si el valor generado no es exclusivo, Exchange añade un guión (-) y un número de dos dígitos, empezando por -01, para conseguir que el valor sea exclusivo. Si Exchange genera un nombre de visualización, no comprueba si el valor es exclusivo.

Exchange admite las siguientes cadenas de sustitución para las directivas de generación de apoderado y denominación automática:

%First	Indica el valor de la propiedad Nombre de la cuenta de usuario asociada.
%Last	Indica el valor de la propiedad Apellidos de la cuenta de usuario asociada.
%Initials	Indica el valor de la propiedad Iniciales de la cuenta de usuario asociada.
%Alias	Indica el valor de la propiedad de buzón Alias.
%DirNam	Indica el valor de la propiedad buzón Nombre de directorio. Al generar direcciones de correo electrónico para buzones de Microsoft Exchange, Exchange no admite cadenas de generación de apoderado que especifiquen la variable %DirName.
%UserName	Indica el valor de la propiedad de nombre de usuario de la cuenta de usuario asociada.

También puede especificar un número entre el signo de porcentaje (%) y el nombre de la cadena de sustitución para indicar el número de caracteres que se incluirán de ese valor. Por ejemplo, %2First indica los dos primeros caracteres de la propiedad **Nombre** name de la cuenta de usuario.

Cada directiva de generación de apoderado y regla de denominación automática puede contener una o varias cadenas de sustitución. También puede especificar caracteres en cada regla como un prefijo o un sufijo para una cadena de sustitución específica, como un punto y un espacio(.) después de la cadena de sustitución %Initials. Si la propiedad de la cadena de sustitución está en blanco, Exchange no incluirá el sufijo de esa propiedad.

Por ejemplo, tenga en cuenta la siguiente regla de denominación automática para la propiedad **Nombre de visualización**:

```
%First %1Initials. %Last
```

Si la propiedad **Nombre** es Susan, la propiedad **Iniciales** es May y la propiedad **Apellidos** es Smith, Exchange define la propiedad **Nombre de visualización** name en Susan M. Smith.

Si la propiedad **Nombre** es Michael, la propiedad **Iniciales** está en blanco y la propiedad **Apellidos** es Jones, Exchange define la propiedad **Nombre de visualización** en Michael Jones.

Especificar una directiva de denominación automatizada de buzones

Para especificar las opciones de denominación automatizada de buzones, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización, y su licencia debe admitir el producto Exchange.

Para especificar una directiva de denominación automatizada de buzones:

- 1 Acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Exchange Policies** (Configurar las directivas de Exchange) > **Alias naming** (Denominación de alias).
- 2 Especifique la información de generación de nombres adecuada.
- 3 Seleccione **Enforce alias naming rules during mailbox updates** (Aplicar reglas de denominación de alias durante las actualizaciones de buzones).
- 4 Haga clic en **Aceptar**.

Especificar una directiva de denominación de recursos

Para especificar las opciones de denominación de recursos, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización, y su licencia debe admitir el producto Exchange.

Para especificar una directiva de denominación de recursos:

- 1 Acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Exchange Policies** (Configurar las directivas de Exchange) > **Resource naming** (Denominación de recursos).
- 2 Especifique la información de generación de nombres de recursos adecuada.
- 3 Seleccione **Enforce resource naming rules during mailbox updates** (Aplicar reglas de denominación de recursos durante las actualizaciones de buzones).
- 4 Haga clic en **Aceptar**.

Especificar una directiva de denominación de archivos de reserva

Para especificar las opciones de denominación de archivos de reserva, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización, y su licencia debe admitir el producto Exchange.

Para especificar un archivo de denominación de archivos de reserva:

- 1 Acceda a **Policy and Automation Management** (Gestión de directivas y automatización) > **Configure Exchange Policies** (Configurar las directivas de Exchange) > **Archive naming** (Denominación de archivos de reserva).
- 2 Especifique la información de generación de nombres de archivos de reserva adecuada para las cuentas de usuario.
- 3 Seleccione **Enforce archive naming rules during mailbox updates** (Aplicar reglas de denominación de archivos de reserva durante las actualizaciones de buzones).
- 4 Haga clic en **Aceptar**.

5.2 Automatización de los activadores anteriores y posteriores a las tareas

Un activador de automatización es una regla que asocia un guión o un archivo ejecutable a una o varias operaciones. Mediante el guión o el archivo ejecutable, puede automatizar un flujo de trabajo existente y establecer un puente de información entre DRA y otros repositorios de datos. Los activadores de automatización permiten ampliar las funciones y la seguridad que ofrece DRA.

Al definir un activador de automatización, define los parámetros de la regla, las operaciones que deben asociarse con el activador, el archivo ejecutable o el guión que se van a ejecutar y, si corresponde, las ActiveViews o los administradores asistentes que deben asociarse a este activador. Estas reglas determinan cómo aplica el servidor de administración el activador.

También puede especificar un guión o un archivo ejecutable para deshacer una acción para el activador. Un **guión para deshacer** permite deshacer los cambios si la operación no se realiza correctamente.

DRA admite los guiones VBScript y PowerShell.

5.2.1 Cómo automatiza los procesos el servidor de administración

Además de la administración basada en reglas de ActiveView, DRA permite automatizar los flujos de trabajo existentes y ejecutar automáticamente las tareas relacionadas mediante activadores de automatización. La automatización de los flujos de trabajo existentes puede ayudarle a optimizar su empresa a la vez que proporciona servicios más eficaces y rápidos.

Cuando el servidor de administración ejecuta la operación asociada con el activador de automatización, el servidor también ejecuta el guión o el archivo ejecutable del activador. Si su activador es un activador anterior a la tarea, el servidor ejecuta el guión o el archivo ejecutable antes de ejecutar la operación. Si su activador es un activador posterior a la tarea, el servidor ejecuta el guión o el archivo ejecutable antes de ejecutar la operación. Este proceso se denomina transacción. Una **transacción** representa el ciclo completo de implementación de cada tarea u operación que realiza el servidor de administración. Una transacción incluye las acciones necesarias para completar una operación junto con las acciones para deshacer que el servidor de administración debe realizar si la operación no se realiza correctamente.

El servidor de administración introduce el estado de activación en el registro de auditoría cada vez que se ejecuta un activador de automatización. Estas entradas de registro incluyen el código de devolución, las operaciones asociadas, los objetos en los que se han realizado acciones y si el guión del activador se ha ejecutado correctamente.

Advertencia: Los activadores de automatización se ejecutan mediante la cuenta de servicio del servidor de administración. Como la cuenta de servicio dispone de permisos de administrador, las directivas y los activadores de automatización tienen acceso completo a todos los datos de la empresa. Para definir activadores de automatización, debe disponer de los poderes adecuados, como los que se incluyen en la función integrada Gestionar directivas y activadores de automatización. Estos activadores de automatización se ejecutarán en el contexto de seguridad de la cuenta de servicio. Por lo tanto, los administradores asistentes asociados a la función integrada Gestionar directivas y activadores de automatización podrían obtener más poderes de los que tenía intención de otorgar.

5.2.2 Implementación de un activador de automatización

Para implementar los activadores de automatización, debe escribir primero los guiones o los archivos ejecutables del activador y disponer de los poderes adecuados, como los que se incluyen en la función Gestionar directivas y activadores de automatización.

Para implementar correctamente un activador personalizado, debe escribir un guión que se ejecute durante una operación (tarea administrativa) específica. Puede especificar si DRA aplica el activador antes (anterior a la tarea) o después (posterior a la tarea) de que se ejecute una operación. En el guión del activador, puede definir mensajes de error para que se muestren cada vez que se produzca un error en el activador. También puede especificar un mensaje de error por defecto mediante el Asistente para crear activadores de automatización.

Para obtener más información acerca de cómo escribir activadores personalizados, ver una lista de las operaciones de administración o utilizar matrices de argumentos, consulte el *SDK*.

Nota

- ♦ Antes de asociar el activador personalizado a un administrador asistente y una ActiveView, asegúrese primero de que el administrador asistente se haya asignado a esa ActiveView.
 - ♦ Si la vía del archivo ejecutable o el guión de la directiva personalizada contiene espacios, escriba la vía entre comillas ("").
-

Para implementar un activador de automatización:

- 1 Escriba un archivo ejecutable o un guión de activador.
- 2 Entre en un equipo cliente de DRA con una cuenta a la que se le haya asignado la función integrada **Gestionar directivas y activadores de automatización** en el dominio gestionado.
- 3 Inicie la consola de delegación y configuración.
- 4 Conéctese al servidor de administración principal.
- 5 En el panel izquierdo, expanda **Policy and Automation Management** (Gestión de directivas y automatización).
- 6 Haga clic en **Automation Triggers** (Activadores de automatización).
- 7 En el menú Tareas, haga clic en **New Trigger** (Nuevo activador).
- 8 En cada ventana del asistente, especifique los valores adecuados y, a continuación, haga clic en **Siguiente**. Por ejemplo, puede asociar este nuevo activador a una ActiveView específica, lo que permite que DRA aplique este activador cuando los administradores asistentes gestionen objetos incluido en esa ActiveView.
- 9 Revise el resumen y haga clic en **Finalizar**.

5.3 Flujo de trabajo automatizado

Mediante la Automatización del flujo de trabajo, puede automatizar los procesos de TI a través de la creación 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 un formulario de flujo de trabajo, puede definir los grupos de admin. que pueden ver el formulario. El envío del formulario o la ejecución del proceso de trabajo dependen de los poderes delegados al grupo o los grupos incluidos al crear el formulario de flujo de trabajo.

Al crear o modificar formularios de flujo de trabajo, estos se guardan en el servidor Web. Los administradores asistentes que entran a la consola Web de este servidor tendrán acceso a los formularios en función de cómo configuren el formulario. Por lo general, los formularios están disponibles para todos los usuarios con credenciales de servidor Web. Para limitar el acceso a un formulario específico, añada grupos de administradores asistentes y, a continuación, oculte el formulario a otros usuarios. Para enviar el formulario, se necesitan uno de los siguientes poderes:

- ♦ Crear un evento de flujo de trabajo y modificar todas sus propiedades
- ♦ Iniciar un flujo de trabajo

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 modificar un formulario existente o crear uno nuevo. Para crear un formulario de flujo de trabajo nuevo o modificar uno existente, desplácese a **Personalización > Flujo de trabajo**.

Al crear un nuevo formulario, debe seguir estos pasos básicos:

1. Configure el formulario para ejecutar el *flujo de trabajo especificado* cuando se envíe el formulario o para que se ejecute cuando lo active un *evento con nombre* predefinido.
2. Elija el grupo o los grupos de administradores asistentes que se incluyen en el proceso de flujo de trabajo y habilite la opción **El formulario está oculto** de la pestaña General para restringir el acceso al formulario a estos usuarios.
3. Añada los campos de propiedades necesarios o páginas de propiedades adicionales al formulario.
4. Si corresponde, cree gestores personalizados para definir de forma más eficaz el proceso de flujo de trabajo y cómo se ejecuta.

Nota: Las opciones del gestor personalizado no se muestran para un nuevo formulario de flujo de trabajo hasta que este se guarde inicialmente. Puede crear y modificar gestores personalizados, y acceder a ellos, en **Propiedades del formulario**.

Para obtener información sobre cómo personalizar los formularios de flujo de trabajo, consulte [Personalización de formularios de flujo de trabajo](#).

6 Auditoría y elaboración de informes

Auditar las acciones de los usuarios es uno de los aspectos más importantes de una implementación de seguridad eficaz. Para permitir la revisión y la notificación de las acciones del administrador asistente (AA), DRA registra todas las operaciones de usuarios en el archivo de registro, en el equipo del servidor de administración. DRA proporciona informes claros y completos que incluyen valores antes y después de los eventos auditados para que pueda ver exactamente qué ha cambiado.

6.1 Auditoría de actividad

La auditoría de la actividad en los registros de eventos puede ayudarle a aislar, diagnosticar y resolver problemas en su entorno. Esta sección proporciona información que le ayudará a habilitar y comprender el registro de eventos y cómo trabajar con los archivos de registro.

6.1.1 Registro de eventos de Windows nativo

Para permitir la revisión y la notificación de 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.

Habilitación e inhabilitación de 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.

Para habilitar la auditoría de eventos:

- 1 Haga clic en **Inicio > Ejecutar**.
- 2 Escriba `regedit` en el campo **Abrir** y haga clic en **Aceptar**.
- 3 Expanda la siguiente clave del Registro: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
- 4 Haga clic en **Editar > Nuevo > Valor DWORD**.
- 5 Introduzca `IsNTAuditEnabled` como nombre de clave.
- 6 Haga clic en **Editar > Modificar**.
- 7 Introduzca `1` en el campo **Información del valor** y haga clic en **Aceptar**.
- 8 Cierre el editor del Registro.

Para inhabilitar la auditoría de eventos:

- 1 Haga clic en **Inicio > Ejecutar**.
- 2 Escriba `regedit` en el campo **Abrir** y haga clic en **Aceptar**.
- 3 Expanda la siguiente clave del Registro: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\`.
- 4 Seleccione la clave `IsNTAuditEnabled`.
- 5 Haga clic en **Editar > Modificar**.
- 6 Introduzca `0` en el campo **Información del valor** y haga clic en **Aceptar**.
- 7 Cierre el editor del Registro.

Garantizar la integridad de la auditoría

Para garantizar que se auditen todas las acciones de los usuarios, DRA proporciona métodos de registro alternativos cuando el producto no puede verificar la actividad del registro. Al instalar DRA, la clave y la vía de `AuditFailsFilePath` se añaden al Registro para garantizar las siguientes acciones:

- ♦ Si DRA detecta que los eventos de auditoría ya no se registran en un archivo de registro, DRA incluirá los eventos de auditoría en un archivo local del servidor de administración.
- ♦ Si DRA no puede escribir eventos de auditoría en un archivo local, DRA incluirá los eventos de auditoría en el registro de eventos de Windows.
- ♦ Si DRA no puede escribir eventos de auditoría en el registro de eventos de Windows, el producto incluirá eventos de auditoría en el registro de DRA.
- ♦ Si DRA detecta que no se están registrando los eventos de auditoría, bloqueará otras operaciones del usuario.

Para habilitar las operaciones de escritura cuando el archivo de registro no está disponible, también debe definir un valor de clave de registro para la clave `AllowOperationsOnAuditFailure`.

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.

Para habilitar las operaciones de escritura:

- 1 Haga clic en **Inicio > Ejecutar**.
- 2 Escriba `regedit` en el campo **Abrir** y haga clic en **Aceptar**.
- 3 Expanda la siguiente clave del Registro: `HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\`.
- 4 Haga clic en **Editar > Nuevo > Valor DWORD**.
- 5 Introduzca `AllowOperationsOnAuditFailure` como nombre de clave.
- 6 Haga clic en **Editar > Modificar**.
- 7 Introduzca `736458265` en el campo **Información del valor**.
- 8 Seleccione **Decimal** en el campo **Base** y haga clic en **Aceptar**.
- 9 Cierre el editor del Registro.

6.1.2 Descripción de los archivos de registro

DRA registra los datos de actividad del usuario en archivos de registro, en el servidor de administración. DRA crea particiones diarias de archivo de registro para almacenar los datos recopilados y normalizados ese día. DRA usa la fecha en hora local en el servidor de administración (AAAAMMDD) como convención de denominación para las particiones diarias de archivo de registro.

Si ha habilitado el recopilador de informes de gestión, DRA exporta los datos del archivo de registro a una base de datos de SQL Server como origen de los informes de gestión de DRA.

Inicialmente, DRA mantiene por defecto indefinidamente datos del registro en el archivo de registro. El tamaño del archivo de registro puede alcanzar un tamaño máximo que se determina durante la instalación en función del espacio disponible en la unidad de disco duro. Cuando el archivo de registro supera este tamaño máximo, no se almacenan nuevos eventos de auditoría. Puede definir un límite de tiempo para la conservación de datos; DRA elimina los datos más antiguos a fin de dejar espacio para los datos más recientes a través de un proceso denominado limpieza. Asegúrese de que dispone de una estrategia de copia de seguridad antes de habilitar la limpieza. Puede configurar el periodo de conservación del archivo de registro mediante la utilidad Configuración del archivo de registro. Para obtener más información, consulte [Modificación de la configuración de limpieza del archivo de registro](#).

Uso de la utilidad Visor del archivo de registro

Use la utilidad Visor del archivo de registro para ver los datos almacenados en los archivos incluidos en el archivo de registro. NetIQ DRA Log Archive Resource Kit (LARK), que puede optar por instalar con DRA, proporciona la utilidad Visor del archivo de registro. Para obtener más información, consulte [NetIQ DRA Log Archive Resource Kit Technical Reference](#) (Referencia técnica de NetIQ DRA Log Archive Resource Kit).

Copia de seguridad de los archivos incluidos en el archivo de registro

Un **archivo incluido en el archivo de registro** es un conjunto de bloques de registro. Como los archivos incluidos en el archivo de registro son archivos binarios comprimidos que se encuentran fuera de una base de datos física, no es necesario usar Microsoft SQL Server Management Studio para realizar una copia de seguridad de los archivos de registro. Si dispone de un sistema automatizado de copia de seguridad de archivos, los archivos incluidos en el archivo de registro se guardan automáticamente como cualquier otro archivo.

Tenga en cuenta las siguientes prácticas recomendadas al planificar la estrategia de copia de seguridad:

- ♦ Se crea una única partición cada día que contiene datos de eventos para ese día. Al habilitar la limpieza, el servicio de archivo de registro limpiará por defecto los datos de estas particiones automáticamente cada 90 días. La estrategia de copia de seguridad debe tener en cuenta la programación de limpieza para determinar la frecuencia de las copias de seguridad. Al limpiar las particiones de archivo de registro, DRA suprime los archivos binarios. No se pueden recuperar los datos limpiados. Estos se deben restaurar a partir de una copia de seguridad. Para obtener más información, consulte [Modificación de la configuración de limpieza del archivo de registro](#).
- ♦ Solo debería realizar una copia de seguridad de las particiones después de que se hayan cerrado. En condiciones normales, se cierra una partición en un plazo de 2 horas a partir de la medianoche del día siguiente.
- ♦ Realice una copia de seguridad de las carpetas de particiones y todas sus subcarpetas como una unidad y restáurelas. Realice una copia de seguridad del archivo `VolumeInfo.xml` como parte del proceso de copia de seguridad de particiones.
- ♦ Si desea restaurar las particiones de archivo de registro para los informes, asegúrese de que los archivos de registro de copia de seguridad se conserven o se puedan restaurar a su formato original.
- ♦ Al configurar el proceso de copia de seguridad de los archivos incluidos en el archivo de registro, NetIQ recomienda que excluya las subcarpetas `index_data` y `CubeExport` ubicadas en la carpeta principal del archivo de registro. Estas subcarpetas contienen datos temporales y no se debe realizar una copia de seguridad de ellos.

Modificación de la configuración de limpieza del archivo de registro

Al instalar DRA, la limpieza del archivo de registro está inhabilitada por defecto. Al establecer procedimientos de copia de seguridad regulares para los archivos incluidos en el archivo de registro, debe habilitar la limpieza del archivo de registro para ahorrar espacio en el disco. Puede modificar el número de días antes de que se limpien las particiones de archivo de registro mediante la utilidad Configuración del archivo de registro.

Para cambiar el número de días antes de que se limpien las particiones del archivo de registro:

- 1 Entre en el servidor de administración mediante una cuenta que sea miembro del grupo de administradores locales.
- 2 Inicie **Log Archive Configuration** (Configuración del archivo de registro) en el grupo de programas NetIQ Security Manager > Configuration (Configuración).
- 3 Haga clic en **Configuración del servidor de archivo de registro**.
- 4 *Si desea habilitar la limpieza de particiones*, defina el valor del campo **Partition Grooming Enabled** (Limpieza de particiones) en True (Verdadero).

- 5 Escriba el número de días que desea conservar las particiones del archivo de registro antes de la limpieza en el campo **Number of Days before Grooming** (Número de días antes de la limpieza).
- 6 Haga clic en **Aplicar**.
- 7 Haga clic en **Sí**.
- 8 Haga clic en **Cerrar**.
- 9 Localice la carpeta *<vía a LogArchiveData> \ <nombre de la partición>* y, a continuación:

Si el valor

Se ha activado

Haga clic en **Sí** en el mensaje de confirmación para reiniciar el servicio de archivo de registro de NetIQ Security Manager.

Nota: Si modifica cualquier ajuste del archivo de registro, debe reiniciar el servicio de archivo de registro para que se aplique el cambio.

No se ha activado

Haga clic en **No** en el mensaje de confirmación. Consulte [Para habilitar el servidor de archivo del registro de DRA a fin de limpiar los datos no archivados:](#).

Si no se ha activado el atributo "File is ready for archiving" (El archivo está listo para archivarse) de las carpetas o los archivos incluidos en las particiones especificadas, debe editar el archivo CONFIG para habilitar la limpieza del archivo de registro. Para comprender por qué es posible que se haya activado o no este atributo, consulte la sección **Additional Information** (Información adicional) del artículo de la base de conocimientos [How do you configure the data retention period for DRA Logarchival Data?](#) (¿Cómo se configura el periodo de conservación de datos para los datos del archivo de registro de DRA?).

Para habilitar el servidor de archivo del registro de DRA a fin de limpiar los datos no archivados:

- 1 Entre localmente a cada consola de servidor de DRA de Windows como miembro del grupo de administradores locales.
- 2 Utilice un editor de texto para abrir el archivo `C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config` y busque la línea `<Property name="GroomUnarchivedData" value="false" />`.
- 3 Cambie "false" (falso) a "true" (verdadero) y guarde el archivo.
- 4 Reinicie el servicio de archivo de registro de DRA de NetIQ.

Nota: Si modifica cualquier ajuste del archivo de registro, debe reiniciar el servicio de archivo de registro para que se aplique el cambio.

6.2 Elaboración de informes

Esta sección proporciona información para comprender y habilitar los informes de DRA, la recopilación de datos de informes, la recopilación y los informes del Analizador de ActiveView y para acceder a los informes integrados.

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.

- ♦ [Sección 6.2.1, “Gestión de la recopilación de datos para la elaboración de informes”, en la página 124](#)
- ♦ [Sección 6.2.2, “Informes integrados”, en la página 125](#)

6.2.1 Gestión de la recopilación de datos para la elaboración de informes

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 a través de la consola de gestión de cuentas y recursos y la consola de delegación y configuración; estos informes 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.

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 [Configuración de informes](#).

Visualización del estado de los recopiladores

Puede ver información de cada recopilador de datos en la pestaña "Collectors Status" (Estado de los recopiladores).

Para ver el estado de los recopiladores:

- 1 Expanda **Configuration Management** (Gestión de configuraciones) y, a continuación, haga clic en **Update Reporting Service Configuration** (Actualizar la configuración del servicio de elaboración de informes).

- 2 En la pestaña "Collectors Status" (Estado de los recopiladores), haga clic en cada entrada para ver información adicional sobre la recopilación de datos, por ejemplo, cuándo se recopilaron los últimos datos y si la última recopilación de datos se ha realizado correctamente.
- 3 Si no aparecen datos en la lista de servidores, haga clic en **Actualizar**.

Habilitación de elaboración de informes y recopilación de datos

Después de instalar los componentes del módulo de elaboración de informes de DRA, habilite y configure la recopilación de datos de informes para acceder a los informes de Reporting Center.

Para habilitar la recopilación de datos y la elaboración de informes:

- 1 Desplácese a **Configuration Management** (Gestión de configuraciones) > **Update Reporting Service Configuration** (Actualizar la configuración del servicio de elaboración de informes).
- 2 En la pestaña SQL Server, seleccione **Enable DRA Reporting support** (Habilitar la compatibilidad con el módulo de elaboración de informes de DRA).
- 3 Haga clic en **Examinar** el campo Nombre del servidor y seleccione el equipo en el que se ha instalado SQL Server.
- 4 En la pestaña "Credentials" (Credenciales), especifique las credenciales adecuadas que se utilizarán en las interacciones de SQL Server.
- 5 Si se trata de la misma cuenta que se puede utilizar para crear la base de datos e inicializar el esquema, seleccione la casilla de verificación "Use the above credentials for creating a database and initializing the database schema" (Utilizar las credenciales anteriores para crear una base de datos e inicializar el esquema de base de datos).
- 6 Si desea especificar una cuenta diferente para crear una base de datos, en la pestaña "Admin Credentials" (Credenciales de admin.), especifique esa cuenta de usuario y contraseña.
- 7 Haga clic en **Aceptar**.

Para obtener información acerca de cómo configurar recopiladores específicos, consulte [Configuración de informes](#).

6.2.2 Informes integrados

Los informes integrados permiten generar informes sobre cambios realizados en los objetos, listas de objetos e información sobre los objetos. Para obtener información sobre cómo acceder a estos informes, consulte los temas de esta sección.

Informes sobre los cambios realizados en los objetos

Puede ver información en tiempo real sobre los cambios realizados en los objetos de los dominios mediante la generación de informes de detalles de actividad. Por ejemplo, puede ver una lista de los cambios realizados en o por un objeto durante un periodo especificado. También puede exportar e imprimir informes de detalles de actividad.

Para elaborar informes sobre los cambios realizados en los objetos:

- 1 Buscar los objetos que coincidan con los criterios.
- 2 Haga clic con el botón derecho en **Reporting > Changes made to objectName** (Informes > Cambios realizados en nombreObjeto) o **Reporting > Changes made by objectName** (Informes > Cambios realizados por nombreObjeto).
- 3 Seleccione las fechas de inicio y finalización para especificar los cambios que desee ver.

- 4 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.

- 5 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.
- 6 Haga clic en **Aceptar**.

Informes sobre listas de objetos

Puede exportar o imprimir los datos de las listas de objetos. Con esta función, puede elaborar informes de forma rápida y fácil sobre detalles generales sobre los objetos gestionados, además de distribuirlos.

Al exportar una lista de objetos, puede especificar la ubicación, el nombre y el formato de archivo. DRA admite los formatos HTML, CSV y XML, por lo que puede exportar esta información en las aplicaciones de base de datos o publicar los resultados de la lista en una página Web.

Nota: También puede seleccionar varios elementos de una lista y, a continuación, copiarlos en una aplicación de texto, como el Bloc de notas.

Para elaborar informes sobre listas de objetos:

- 1 Buscar los objetos que coincidan con los criterios.
- 2 Para exportar esta lista de objetos, haga clic en **Export List** (Exportar lista) en el menú Archivo.
- 3 Para imprimir esta lista de objetos, haga clic en **Print List** (Imprimir lista) en el menú Archivo.
- 4 Especifique la información adecuada para guardar o imprimir la lista.

Elaboración de informes sobre detalles de objetos

Puede exportar o imprimir datos desde pestañas de detalles que enumeran atributos de objetos, como pertenencias a grupos. Con esta función, puede elaborar informes de forma rápida y fácil acerca de la información sobre objetos específicos que se necesita con frecuencia, además de distribuirlos.

Al exportar una pestaña de detalles de objetos, puede especificar la ubicación, el nombre y el formato de archivo. DRA admite los formatos HTML, CSV y XML, por lo que puede exportar esta información en las aplicaciones de base de datos o publicar los resultados de la lista en una página Web.

Para elaborar informes sobre detalles de objetos:

- 1 Busque el objeto que coincida con los criterios.
- 2 En el menú Ver, haga clic en **Detalles**.
- 3 En el panel de detalles, seleccione la pestaña adecuada.
- 4 Para exportar estos detalles del objeto, haga clic en **Export Details** (Exportar detalles) en el menú Archivo.

- 5 Para imprimir estos detalles del objeto, haga clic en **Print Details** (Imprimir detalles) en el menú Archivo.
- 6 Especifique la información adecuada para guardar o imprimir la lista.

7 Funciones adicionales

Las asignaciones temporales de grupos, los grupos dinámicos, la adición de marcas a eventos y la contraseña de recuperación de BitLocker son funciones adicionales de DRA que puede utilizar en su entorno empresarial.

7.1 Asignaciones temporales de grupos

DRA permite crear asignaciones temporales de grupos que proporcionan a los usuarios autorizados acceso temporal a los recursos. Los administradores asistentes pueden utilizar asignaciones temporales de grupos para asignar usuarios a un grupo de destino durante un periodo específico. Al final del periodo, DRA elimina automáticamente los usuarios del grupo.

La función Gestionar asignaciones temporales de grupos otorga poderes a los administradores asistentes para crear y gestionar asignaciones temporales de grupos.

Utilice los siguientes poderes para delegar la creación y la gestión de asignaciones temporales de grupos:

- ♦ Crear asignaciones temporales de grupos
- ♦ Ver asignaciones temporales de grupos
- ♦ Suprimir/modificar asignaciones temporales de grupos
- ♦ Añadir un objeto a un grupo
- ♦ Eliminar un objeto de un grupo

El grupo y los usuarios de destino deben encontrarse también en la misma ActiveView.

Nota

- ♦ Los administradores asistentes solo pueden crear, modificar y suprimir asignaciones temporales de grupos en el servidor de administración principal. No pueden gestionar asignaciones temporales de grupos en los servidores de administración secundarios.
- ♦ DRA replica las asignaciones temporales de grupos del servidor de administración principal en los servidores de administración secundarios durante la réplica de MMS.
- ♦ No se puede crear una asignación temporal de grupos para un usuario que ya sea miembro del grupo de destino. Si intenta crear una asignación temporal de grupos para un usuario que ya sea miembro del grupo de destino, DRA mostrará un mensaje de advertencia y no le permitirá crear una asignación temporal de grupos para el usuario.
- ♦ Si crea una asignación temporal de grupos para un usuario que no sea miembro del grupo de destino, DRA eliminará al usuario del grupo cuando caduque la asignación temporal de grupos.

Para obtener más información sobre la creación y el uso de asignaciones temporales de grupos, consulte la *Guía del usuario*.

7.2 Grupos dinámicos de DRA

Un grupo dinámico es aquel cuya pertenencia a grupo cambia según un conjunto definido de criterios que puede configurar en las propiedades del grupo. Puede convertir cualquier grupo en dinámico o eliminar el filtro dinámico de cualquier grupo para el que se haya configurado. Esta función permite también añadir miembros de un grupo a una lista de miembros estáticos o excluidos. Los miembros del grupo incluidos en estas listas no se verán afectados por los criterios dinámicos.

Si restablece un grupo dinámico a un grupo normal, todos los miembros de la lista de miembros estáticos se añadirán a la pertenencia a grupo, y se omitirán los filtros dinámicos y los miembros excluidos. Puede establecer los grupos existentes como dinámicos o crear un nuevo grupo dinámico tanto en la consola de delegación y configuración como en la consola Web.

Para convertir un grupo en dinámico:

- 1 Localice el grupo en la consola correspondiente.
 - ♦ Delegación y configuración: vaya a **Todos mis objetos gestionados** > **Find Now** (Buscar ahora).

Nota: Para habilitar el generador de consultas, haga clic en **Examinar** y seleccione un dominio, un contenedor o una unidad administrativa.

- ♦ Consola Web: vaya a **Gestión** > **Buscar**.
- 2 Abra las propiedades del grupo y seleccione **Convertir grupo en dinámico** en la pestaña Filtro de miembros dinámicos.
 - 3 Añada los atributos virtuales y de LDAP que desee para filtrar la pertenencia a grupo.
 - 4 Añada todos los miembros estáticos o excluidos que desee al grupo dinámico y aplique los cambios.

Para crear un nuevo grupo dinámico:

- ♦ **Delegación y configuración:** haga clic en con el botón derecho en el dominio o el nodo secundario en Todos mis objetos gestionados y seleccione **Nuevo** > **Grupo dinámico**.
- ♦ **Consola Web:** vaya a **Gestión** > **Crear** > **Nuevo grupo dinámico**.

7.3 Funcionamiento de la adición de marcas a eventos

Cuando configura un atributo para un tipo de objeto, y DRA realiza una de las operaciones admitidas, ese atributo se actualizará (marcará) con información específica de DRA, incluido quién realizó la operación. Esto provoca que AD genere un evento de auditoría para ese cambio de atributo.

Por ejemplo, imagine que ha seleccionado el atributo `extensionAttribute1` como atributo de usuario y ha configurado la auditoría de AD DS. Cada vez que un administrador asistente actualiza un usuario, DRA actualizará el atributo `extensionAttribute1` con datos de adición de marcas a eventos. Esto significa que junto con los eventos de AD DS para cada atributo que el administrador asistente ha actualizado (por ejemplo, descripción, nombre, etc.) habrá un evento de AD DS adicional para el atributo `extensionAttribute1`.

Cada uno de estos eventos contiene un ID de correlación, que es el mismo para cada atributo modificado que se ha cambiado al actualizar el usuario. Así es como las aplicaciones pueden asociar los datos de adición de marcas a eventos con los demás atributos que se actualizaron.

7.3.1 El evento de DS AD

Aparecerá un evento como, por ejemplo, un registro de eventos de seguridad de Windows cada vez que DRA ejecute una operación admitida.

Nombre de visualización de LDAP:	<code>extensionAttribute1</code>
Sintaxis (OID): 2.5.5.12	2.5.5.12
Valor:	<pre><dra-event user="DRDOM300\drauseradmin" sid="S-1-5-21-53918190-1560392134-2889063332-1914" tid="E0E257E6B4D24744A9B0FE3F86EC7038" SubjectUserSid="S-1-5-21-4224976940-2944197837-1672139851-500" ObjectDN="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/>+a+02ROO+bJbhyPbR4leJpKWCGTp/KXdqI7S3EBhVyniE7iXvxIT6eB6ldcXQ5StkblAHJgKzLN5FCOM5fZclTxyAPLW hbstaA7ZA0VbVC9MGIVlaAcjl3z7mpF9GKXsfDogbSeNImHliXvH5KpOX3/29AKMPj/zvf6Yuczoos=</pre>

El valor de evento consta de dos partes. La primera es una cadena XML que contiene los datos de adición de marcas a eventos. El segundo es una firma de los datos que puede utilizarse para validar los datos que ha generado realmente DRA. Para validar la firma, una aplicación debe disponer de la clave pública de la firma.

La cadena XML consta de la siguiente información:

User	El administrador del asistente que ha realizado la operación.
Sid	El SID del administrador asistente que ha realizado la operación.
Tid	El ID de la transacción de auditoría de DRA para garantizar que cada evento sea exclusivo.
SubjectUserSid	El SID de la cuenta de servicio o acceso de DRA que AD ha actualizado realmente.
ObjectDN	El nombre completo del objeto que se ha modificado

7.3.2 Operaciones admitidas

Usuario	<ul style="list-style-type: none">♦ Crear♦ Renombrar♦ Modificar♦ Clonar
Grupo	<ul style="list-style-type: none">♦ Crear♦ Renombrar♦ Modificar♦ Clonar

Contacto	<ul style="list-style-type: none"> ◆ Crear ◆ Renombrar ◆ Modificar ◆ Clonar
Equipo	<ul style="list-style-type: none"> ◆ Crear ◆ Habilitar ◆ Inhabilitar ◆ Renombrar ◆ Modificar
Unidad administrativa	<ul style="list-style-type: none"> ◆ Crear ◆ Renombrar ◆ Clonar

7.4 Contraseña de recuperación de BitLocker

Microsoft BitLocker almacena las contraseñas de recuperación en Active Directory. Mediante la función de recuperación de BitLocker de DRA, puede delegar poderes a los administradores asistentes para buscar y recuperar las contraseñas perdidas de BitLocker 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.

7.4.1 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 proporciónesela al usuario final.

Para ver y copiar la contraseña de recuperación:

- 1 Lance la consola de **delegación y configuración** y expanda la estructura de vista en árbol.
- 2 En el nodo **Account and Resource Management** (Gestión de cuentas y recursos), desplácese a **Todos mis objetos gestionados > Dominio > Equipos**.
- 3 En la lista de equipos, haga clic con el botón derecho en el equipo correspondiente y seleccione **Propiedades**.
- 4 Haga clic en la pestaña **Contraseña de recuperación de BitLocker** para ver la contraseña de recuperación de BitLocker.
- 5 Haga clic con el botón derecho en la contraseña de recuperación de BitLocker, haga clic en **Copiar** y, a continuación, pegue el texto en el archivo de texto o la hoja de cálculo correspondientes.

7.4.2 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 **delegación y configuración** y expanda la estructura de vista en árbol.
- 2 En el nodo **Account and Resource Management** (Gestión de cuentas y recursos), desplácese a **All My Managed Objects** (Todos mis objetos gestionados), 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**.

7.5 Analizador de ActiveView

El Analizador de ActiveView le ayuda a diagnosticar problemas de ActiveView. Por ejemplo, puede buscar anomalías relacionadas con el procesamiento de ActiveViews, incluido el tiempo de procesamiento prolongado o el procesamiento de ActiveViews no utilizado cuando se realiza una operación. El Analizador de ActiveView también simplifica la búsqueda de ActiveViews duplicadas.

Después de ejecutar una recopilación de datos y ver un informe, es posible que considere necesario modificar las reglas de ActiveView.

7.5.1 Inicio de una recopilación de datos de ActiveView

Con el Analizador de ActiveView, puede recopilar datos en ActiveViews de acciones realizadas por los administradores asistentes (AA). A continuación, estos datos pueden visualizarse en el informe del Analizador. Para recopilar los datos, debe especificar el administrador asistente para la recopilación de datos y, a continuación, iniciar una recopilación de ActiveView.

Nota: El administrador asistente en el que desea recopilar datos debe estar conectado al mismo servidor DRA en el que se ejecuta el Analizador.

Para iniciar una recopilación de ActiveView:

- 1 Lance la consola Web y entre a la sesión con las credenciales de administrador.
- 2 Desplácese a **Administrador > Analizador ActiveView**.
- 3 En la página Analizador ActiveView, especifique lo siguiente:
 - 3a **Administrador asistente:** utilice la función de búsqueda para buscar y añadir un administrador asistente en el que desee recopilar datos.
 - 3b **Ver propiedades:** (opcional) utilice la función Ver propiedades para ver o modificar las propiedades del administrador asistente antes de iniciar la recopilación.
 - 3c **Duración de la recopilación:** especifique el número total de horas necesarias para recopilar los datos del analizador. Una vez que se supere el tiempo especificado, la recopilación de datos se detendrá y se creará un índice en la base de datos de Mongo.
- 4 Haga clic en **Iniciar recopilación** para recopilar datos de ActiveView.

- 5 (Opcional) Haga clic en **Detener recopilación** para detener el registro de las operaciones del administrador asistente en las ActiveViews. Se creará un índice en la base de datos de Mongo. Puede detener la recopilación de datos manualmente antes de que finalice la duración programada; aún podrá generar un informe.

Importante: Si detiene la recopilación y cambia el administrador asistente o reinicia una recopilación de datos para el mismo administrador asistente, el Analizador de ActiveView borrará los datos existentes de la base de datos de Mongo. Solo puede tener datos del Analizador de un administrador asistente en la base de datos cada vez.

7.5.2 Generación de un informe del analizador

Antes de generar un informe del Analizador, asegúrese de haber detenido la recopilación de datos y de que haya un índice disponible en la base de datos de Mongo.

Para generar un informe del Analizador:

- 1 Desplácese a **Administrador > Analizador ActiveView**.
- 2 En la página Analizador ActiveView, se muestra la lista de operaciones realizadas por el administrador asistente y puede elegir entre las siguientes opciones:
 - ♦ **"Operations Performed" (Operaciones realizadas):** seleccione la operación para la que desea recopilar datos del Analizador.
 - ♦ **"Top Longest Operation" (Operación de mayor duración):** seleccione cuántas operaciones de mayor duración desea ver.
- 3 Haga clic en **Generar informe** para generar un informe de análisis con los detalles de la operación de ActiveView a fin de incluir elementos coincidentes, elementos no coincidentes y duración.

Al utilizar el informe, puede analizar las reglas que tardan más tiempo en realizar operaciones y, a continuación, decidir si alguna de ellas debe modificarse o suprimirse de sus respectivas ActiveViews.

7.5.3 Limpieza de los datos analizados

La acción Limpiar le ayuda a liberar espacio en la base de datos de Mongo al suprimir datos duplicados y no utilizados.

Para borrar todos los datos analizados de ActiveView existentes de la base de datos de Mongo, haga clic en **Limpiar datos**.

7.6 Papelera

Puede habilitar o inhabilitar la Papelera para cada dominio u objeto de Microsoft Windows dentro de esos dominios, lo que le permitirá controlar la gestión de cuentas en toda su empresa. Si habilita la Papelera y, a continuación, suprime una cuenta de usuario, un grupo, un grupo dinámico de distribución, un grupo dinámico, un buzón de recursos, un contacto o una cuenta de equipo, el servidor de administración inhabilita la cuenta seleccionada y la transfiere al contenedor de la Papelera. Una vez que DRA transfiere la cuenta a la Papelera, esta no se mostrará en las ActiveViews a las que pertenecía. Si suprime una cuenta de usuario, un grupo, un contacto o una cuenta de equipo cuando la Papelera está inhabilitada, el servidor de administración suprimirá de

forma permanente la cuenta seleccionada. Puede inhabilitar la Papelera que contiene las cuentas suprimidas anteriormente. Sin embargo, una vez que la Papelera está inhabilitada, estas cuentas ya no estarán disponibles en el nodo Papelera.

7.6.1 Asignación de poderes de la Papelera

Para permitir que un administrador asistente elimine de forma permanente las cuentas del nodo Todos mis objetos gestionados, así como de la Papelera, asigne el poder correspondiente de la siguiente lista:

- ◆ Suprimir de forma permanente una cuenta de usuario
- ◆ Suprimir de forma permanente un grupo
- ◆ Suprimir de forma permanente un equipo
- ◆ Suprimir de forma permanente un contacto
- ◆ Suprimir de forma permanente un grupo dinámico de distribución
- ◆ Suprimir de forma permanente un grupo dinámico
- ◆ Suprimir de forma permanente un buzón de recursos

Si varios servidores de administración gestionan diferentes subárboles en el mismo dominio de Microsoft Windows, puede utilizar la Papelera para ver cualquier cuenta eliminada de ese dominio, independientemente del servidor de administración que gestione esa cuenta.

7.6.2 Uso de la Papelera

Utilice la Papelera para eliminar de forma permanente o restaurar cuentas, o ver las propiedades de las cuentas suprimidas. También puede buscar cuentas específicas y realizar un seguimiento de cuántos días ha permanecido una cuenta suprimida en la Papelera. También se incluye la pestaña Papelera en la ventana Propiedades para un dominio seleccionado. En esta pestaña, puede habilitar o inhabilitar la Papelera para todo el dominio o para objetos específicos, así como programar una limpieza de la Papelera.

Utilice las opciones **Restore All** (Restaurar todo) o **Empty Recycle Bin** (Vaciar la Papelera) para restaurar de forma fácil y rápida elementos o suprimir estas cuentas.

Al restaurar una cuenta, DRA la restablece, incluidos todos los permisos, las delegaciones de poderes, las asignaciones de directivas, las pertenencias a grupos y las suscripciones a ActiveView. Si suprime de forma permanente una cuenta, DRA elimina esa cuenta de Active Directory.

Para garantizar la supresión segura de cuentas, solo los administradores asistentes que dispongan de los siguientes poderes pueden eliminar de forma permanente las cuentas de la Papelera:

- ◆ Suprimir de forma permanente una cuenta de usuario
- ◆ Suprimir usuario de la Papelera
- ◆ Suprimir de forma permanente una cuenta de grupo
- ◆ Suprimir grupo de la Papelera
- ◆ Suprimir de forma permanente una cuenta de equipo
- ◆ Suprimir equipo de la Papelera
- ◆ Suprimir de forma permanente una cuenta de contacto
- ◆ Suprimir contacto de la Papelera
- ◆ Suprimir de forma permanente un grupo dinámico de distribución

- ♦ Suprimir grupo dinámico de distribución de la Papelera
- ♦ Suprimir de forma permanente un grupo dinámico
- ♦ Suprimir grupo dinámico de la Papelera
- ♦ Suprimir de forma permanente un buzón de recursos
- ♦ Suprimir buzón de recursos de la Papelera
- ♦ Ver todos los objetos de la Papelera

Para restaurar una cuenta desde la Papelera, los administradores asistentes deben disponer de los siguientes poderes en la unidad administrativa que contiene la cuenta:

- ♦ Restaurar usuario desde la Papelera
- ♦ Restaurar grupo desde la Papelera
- ♦ Restaurar grupo dinámico de distribución desde la Papelera
- ♦ Restaurar grupo dinámico desde la Papelera
- ♦ Restaurar buzón de recursos desde la Papelera
- ♦ Restaurar equipo desde la Papelera
- ♦ Restaurar contacto desde la Papelera
- ♦ Ver todos los objetos de la Papelera

Nota

- ♦ Si suprime una cuenta de administrador asistente en la Papelera, DRA continúa mostrando las asignaciones de ActiveView y funciones de esa cuenta. En lugar de mostrar el nombre de la cuenta de administrador asistente suprimida, DRA muestra el identificador de seguridad (SID). Puede eliminar estas asignaciones antes de suprimir de forma permanente la cuenta de administrador asistente.
 - ♦ DRA suprime el directorio personal después de eliminar la cuenta de usuario de la Papelera.
 - ♦ Si suprime un usuario que tiene una licencia de Office 365, esta pasará a la Papelera y se eliminará la licencia. Si más adelante se restaura la cuenta de usuario, también se restaurará la licencia de Office 365.
-

8

Personalización de clientes

Puede personalizar los clientes de delegación y configuración, y de gestión de cuentas y recursos, y la consola Web. Los primeros requieren acceso físico o remoto y las credenciales de la cuenta. La última requiere la dirección URL del servidor y las credenciales de cuenta para entrar a la sesión desde un navegador Web.

8.1 Clientes de delegación y configuración, y de gestión de cuentas y recursos

Esta sección incluye información para ayudarle a personalizar los clientes de delegación y configuración, y de gestión de cuentas y recursos, lo que incluye comprender cómo crear páginas de propiedades personalizadas, cómo crear herramientas personalizadas en DRA que puedan ejecutarse en equipos cliente y de servidor en la red, y cómo personalizar la configuración de la interfaz de usuario.

8.1.1 Personalización de las páginas de propiedades

Puede personalizar y ampliar las consolas de delegación y configuración, y gestión de cuentas y recursos mediante la implementación de propiedades personalizadas. Las propiedades personalizadas permiten añadir propiedades patentadas de cuenta y unidad administrativa, como extensiones de esquema de Active Directory y atributos virtuales, a ventanas de propiedades y asistentes específicos. Estas ampliaciones permiten personalizar DRA para satisfacer sus requisitos específicos. Con el Asistente para crear nuevas páginas personalizadas de la consola de delegación y configuración, puede crear de forma fácil y rápida una página personalizada para ampliar la interfaz de usuario adecuada.

Si los administradores asistentes requieren poderes exclusivos para gestionar de forma segura la página personalizada, también puede crear y delegar poderes personalizados. Por ejemplo, es posible que desee limitar la gestión de cuentas de usuario a las propiedades incluidas solo en la página personalizada. Para obtener más información, consulte [Implementación de poderes personalizados](#).

Cómo funcionan las páginas de propiedades personalizadas

Las ampliaciones de la interfaz de usuario son páginas personalizadas que DRA muestra en las ventanas de propiedades y el asistente adecuados. Puede configurar páginas personalizadas para visualizar los atributos de Active Directory, las extensiones de esquema y los atributos virtuales en la consola de delegación y configuración y en la consola de gestión de cuentas y recursos.

Al seleccionar un atributo admitido de Active Directory, una extensión de esquema o un atributo virtual, puede utilizar páginas personalizadas de las siguientes maneras:

- ♦ Limite los administradores asistentes para que gestionen un conjunto bien definido y controlado de propiedades. Este conjunto de propiedades puede incluir *propiedades estándar* y extensiones de esquema. Las propiedades estándar son atributos de Active Directory que se muestran por defecto a través de la consola de gestión de cuentas y recursos.

- ♦ Visualice los atributos de Active Directory distintos a las propiedades estándar gestionadas por DRA.
- ♦ Amplíe la consola de gestión de cuentas y recursos, y la consola de delegación y configuración para incluir propiedades patentadas.

También puede configurar el modo en que DRA muestra y aplica a estas propiedades. Por ejemplo, puede definir controles de la interfaz de usuario con los valores de propiedades por defecto.

DRA aplica las páginas personalizadas a todos los objetos gestionados pertinentes de su empresa. Por ejemplo, si crea una página personalizada para añadir extensiones de esquema de Active Directory a la ventana Propiedades de grupo, DRA aplicará las propiedades de esta página a cada grupo gestionado en un dominio que admita las extensiones de esquema especificadas. Cada página personalizada requiere un conjunto exclusivo de propiedades. No se puede añadir un atributo de Active Directory a más de una página personalizada.

No se pueden inhabilitar ventanas o pestañas individuales en la interfaz de usuario existente. Un administrador asistente puede seleccionar un valor de propiedad mediante la interfaz de usuario por defecto o una página personalizada. DRA aplica el valor seleccionado más recientemente a una propiedad.

DRA proporciona un seguimiento de auditoría completo para las propiedades personalizadas. DRA registra los datos siguientes en el registro de eventos de aplicaciones:

- ♦ Cambios realizados en las páginas personalizadas.

Importante: Debe configurar manualmente la auditoría del registro de aplicaciones de Windows. Consulte "[How do I re-enable DRA to write events to the Application Event log in DRA 8.5 and later?](#)" (¿Cómo se habilita de nuevo DRA para que escriba eventos en el registro de eventos de aplicaciones en DRA 8.5 y versiones posteriores?).

- ♦ Creación y supresión de páginas personalizadas
- ♦ La extensión de esquema, los atributos de Active Directory y los atributos virtuales mostrados se incluyen en las páginas personalizadas.

También puede ejecutar informes de actividad de cambios para supervisar los cambios de configuración de las propiedades personalizadas.

Implemente y modifique las páginas personalizadas desde el servidor de administración principal. Durante la sincronización, DRA replica las configuraciones de páginas personalizadas en el conjunto de varios maestros. Para obtener más información, consulte [Configuración del conjunto de varios maestros](#).

Páginas personalizadas admitidas

Cada página personalizada que cree le permitirá seleccionar un conjunto de propiedades de Active Directory, extensiones de esquema o atributos virtuales y visualizar esas propiedades como una pestaña personalizada. Puede crear los siguientes tipos de páginas personalizadas:

Página personalizada de usuario

Permite visualizar las pestañas personalizadas en las siguientes ventanas:

- ♦ Ventana Propiedades de usuario
- ♦ Asistente para crear usuarios
- ♦ Asistente para clonar usuarios

Página personalizada de grupo

Permite visualizar las pestañas personalizadas en las siguientes ventanas:

- ♦ Ventana Propiedades de grupo
- ♦ Asistente para crear grupos
- ♦ Asistente para clonar grupos

Página personalizada de equipo

Permite visualizar las pestañas personalizadas en las siguientes ventanas:

- ♦ Ventana Propiedades de equipo
- ♦ Asistente para crear equipos

Página personalizada de contacto

Permite visualizar las pestañas personalizadas en las siguientes ventanas:

- ♦ Ventana Propiedades de contacto
- ♦ Asistente para crear contactos
- ♦ Asistente para clonar contactos

Página personalizada de unidad administrativa

Permite visualizar las pestañas personalizadas en las siguientes ventanas:

- ♦ Ventana Propiedades de unidad administrativa
- ♦ Asistente para crear unidades administrativas
- ♦ Asistente para clonar unidades administrativas

Página personalizada de buzón de recursos

Permite visualizar las pestañas personalizadas en las siguientes ventanas:

- ♦ Ventana Propiedades de buzón de recursos
- ♦ Asistente para crear buzones de recursos
- ♦ Asistente para clonar buzones de recursos

Página personalizada de grupo dinámico de distribución

Permite visualizar las pestañas personalizadas en las siguientes ventanas:

- ♦ Ventana Propiedades de grupo dinámico de distribución
- ♦ Asistente para crear grupos dinámicos de distribución
- ♦ Asistente para clonar grupos dinámicos de distribución

Controles de propiedades personalizadas compatibles

Al añadir un atributo de Active Directory, una extensión de esquema o un atributo virtual a una página personalizada, también configura el control de la interfaz de usuario con el que un administrador asistente introduce el valor de la propiedad. Por ejemplo, puede especificar valores de propiedades de las siguientes formas:

- ♦ Defina los rangos de valores específicos.
- ♦ Defina los valores de propiedades por defecto.
- ♦ Indique si se necesita una propiedad.

También puede configurar el control de la interfaz de usuario para visualizar instrucciones o información patentada. Por ejemplo, si define un rango específico para un número de identificación de empleado, puede configurar la etiqueta de control del recuadro de texto para que muestre **Especifique el número de identificación de empleado (001 a 100)**.

Cada control de interfaz de usuario proporciona compatibilidad con un único atributo de Active Directory, una extensión de esquema o un atributo virtual. Configure los siguientes controles de interfaz de usuario en función del tipo de propiedad:

Tipo de atributo de Active Directory	Controles de la interfaz de usuario compatibles
Booleano	Casilla de verificación
Fecha	Control de calendario
Número entero	Recuadro de texto (por defecto) Lista de selección
Cadena	Recuadro de texto (por defecto) Lista de selección Selector de objetos
Cadena con varios valores	Lista de selección

Trabajo con páginas personalizadas

Puede crear páginas personalizadas desde el nodo "User Interface Extensions" (Ampliaciones de la interfaz de usuario). Una vez que se crea una página, puede añadir o eliminar las propiedades del atributo AD, e inhabilitar o suprimir la página. Para cada personalización que desee configurar, cree una página personalizada y asigne la función o el poder adecuados al administrador asistente. Tenga en cuenta las prácticas recomendadas mostradas a continuación al empezar a trabajar con páginas personalizadas:

1. Para asegurarse de que DRA reconoce los atributos de Active Directory, los atributos de extensión de esquema o los atributos virtuales, reinicie el servicio de administración de NetIQ en cada servidor de administración.
2. Identifique el tipo de página personalizada que desea crear y las propiedades que desea que los administradores asistentes gestionen con esta página personalizada. Puede seleccionar cualquier atributo de Active Directory, incluidos los atributos de extensión de esquema y los atributos de los asistentes de DRA existentes y las ventanas de propiedades o cualquier atributo virtual que cree. Sin embargo, cada página personalizada requiere un conjunto exclusivo de propiedades. No se puede añadir un atributo de Active Directory a más de una página personalizada.

Las páginas personalizadas no sustituyen a la interfaz de usuario existente. Para obtener más información, consulte la [Cómo funcionan las páginas de propiedades personalizadas](#) y la [Páginas personalizadas admitidas](#).

3. Determine cómo desea que los administradores asistentes especifiquen estas propiedades. Por ejemplo, es posible que desee limitar una propiedad específica a tres posibles valores. Puede definir un control de interfaz de usuario adecuado para cada propiedad. Para obtener más información, consulte [Controles de propiedades personalizadas compatibles](#).

4. Determine si los administradores asistentes necesitan instrucciones o información patentada para gestionar correctamente estas propiedades. Por ejemplo, determine si Active Directory requiere una sintaxis para el valor de la propiedad, como un nombre completo (DN) o una vía LDAP.
5. Identifique el orden en el que estas propiedades deben mostrarse en la página personalizada. Puede cambiar el orden de visualización en cualquier momento.
6. Determine cómo DRA debe utilizar esta página personalizada. Por ejemplo, puede añadir una página personalizada de usuario al Asistente para nuevos usuarios y la ventana Propiedades de usuario.
7. Utilice la pestaña Asignaciones en el panel de detalles de los administradores asistentes para comprobar que estos dispongan de los poderes adecuados para el conjunto de objetos correcto. Si ha creado poderes personalizados para esta página personalizada, delegue esos poderes a los administradores asistentes correspondientes.
8. Determine si los administradores asistentes necesitan un poder personalizado para gestionar las propiedades de esta página. Por ejemplo, si añade una página personalizada a la ventana Propiedades de usuario, delegando el poder *Modificar todas las propiedades de usuario*, puede otorgarle a un administrador asistente demasiados poderes. Cree todos los poderes personalizados necesarios para implementar la página personalizada. Para obtener más información, consulte [Implementación de poderes personalizados](#).
9. Con las respuestas de pasos anteriores, cree las páginas personalizadas adecuadas.
10. Distribuya información sobre las páginas de propiedades personalizadas que ha implementado en los administradores asistentes adecuados como, por ejemplo, la Ayuda técnica.

Para implementar la personalización de propiedades, debe disponer de los poderes incluidos en la función Administración de DRA. Para obtener más información acerca de las páginas personalizadas, consulte [Cómo funcionan las páginas de propiedades personalizadas](#).

Creación de páginas de propiedades personalizadas

Puede crear diferentes propiedades personalizadas mediante la creación de distintas páginas personalizadas. Por defecto, se habilitan las nuevas páginas personalizadas.

Al crear una página personalizada, puede inhabilitarla. Si se inhabilita una página personalizada, se oculta de la interfaz de usuario. Si va a crear varias páginas personalizadas, es posible que desee inhabilitar las páginas hasta que sus personalizaciones se hayan probado y completado.

Nota: Las cuentas de equipo heredan los atributos de Active Directory de las cuentas de usuario. Si amplía el esquema de Active Directory para incluir atributos adicionales para las cuentas de usuario, puede seleccionar estos atributos cuando cree una página personalizada a fin de gestionar las cuentas de equipo.

Para crear páginas de propiedades personalizadas:

- 1 Desplácese al nodo **Configuration Management** (Gestión de configuraciones) > **User Interface Extensions** (Ampliaciones de la interfaz de usuario).
- 2 En el menú Tareas, haga clic en **Nuevo** y, a continuación, haga clic en el elemento de menú adecuado para la página personalizada que desea crear.
- 3 En la pestaña General, escriba el nombre de esta página personalizada y, a continuación, haga clic en **Aceptar**. Si desea inhabilitar esta página, desactive la casilla de verificación **Habilitado**.

- 4 Para cada propiedad que desee incluir en esta página personalizada, siga los siguientes pasos:
 - 4a En la pestaña Propiedades, haga clic en **Añadir**.
 - 4b Para seleccionar una propiedad, haga clic en **Examinar**.
 - 4c En el campo **Control label** (Etiqueta de control), escriba el nombre de propiedad que debe utilizar DRA como etiqueta del control de la interfaz de usuario. Asegúrese de que la etiqueta de control sea fácil de usar y muy descriptiva. También puede incluir instrucciones, rangos de valores válidos y ejemplos de sintaxis.
 - 4d Seleccione el control de la interfaz de usuario adecuado en el menú **Control type** (Tipo de control).
 - 4e Seleccione en qué parte de la consola de gestión de cuentas y recursos desea que DRA muestre esta página personalizada.
 - 4f Para especificar los atributos adicionales, como la longitud mínima o valores por defecto, haga clic en **Advanced** (Opciones avanzadas).
 - 4g Haga clic en **Aceptar**.
- 5 Para cambiar el orden en que DRA muestra estas propiedades en la página personalizada, seleccione la propiedad adecuada y, a continuación, haga clic en **Mover arriba** o **Mover abajo**.
- 6 Haga clic en **Aceptar**.

Modificación de las propiedades personalizadas

Puede cambiar una página personalizada mediante la modificación de las propiedades personalizadas.

Para modificar las propiedades personalizadas:

- 1 Desplácese al nodo **Configuration Management** (Gestión de configuraciones) > **User Interface Extensions** (Ampliaciones de la interfaz de usuario).
- 2 En el panel de lista, seleccione la página personalizada que desee.
- 3 En el menú Tareas, haga clic en **Propiedades**.
- 4 Modifique las propiedades y los ajustes adecuados para esta página personalizada.
- 5 Haga clic en **Aceptar**.

Identificación de atributos de Active Directory gestionados con páginas personalizadas

Puede identificar rápidamente las propiedades de Active Directory, las extensiones de esquema o los atributos virtuales que se gestionan mediante una página personalizada específica.

Para identificar las propiedades de Active Directory gestionadas mediante páginas personalizadas:

- 1 Desplácese al nodo **Configuration Management** (Gestión de configuraciones) > **User Interface Extensions** (Ampliaciones de la interfaz de usuario).
- 2 En el panel de lista, seleccione la página personalizada que desee.
- 3 En el panel de detalles, haga clic en la pestaña **Propiedades**. Para ver el panel de detalles, haga clic en **Detalles** en el menú Ver.
- 4 Para comprobar cómo DRA muestra y aplica una propiedad, seleccione el atributo de Active Directory, la extensión de esquema o el atributo virtual adecuados en la lista y, a continuación, haga clic en el icono **Propiedades**.

Habilitación, inhabilitación y supresión de las páginas personalizadas

Al habilitar una página personalizada, DRA la añade a las ventanas y los asistentes asociados. Para especificar las ventanas y los asistentes que muestran una página personalizada, defina las propiedades de la página personalizada.

Nota: Para garantizar que cada página personalizada muestre un conjunto exclusivo de propiedades, DRA no habilita las páginas personalizadas que contienen propiedades mostradas en otras páginas personalizadas.

Al inhabilitar una página personalizada, DRA la elimina de las ventanas y los asistentes asociados. DRA suprime la página personalizada. Para garantizar que una página personalizada nunca se muestre en la interfaz de usuario, suprimala.

Al suprimir una página personalizada, DRA la elimina de las ventanas y los asistentes asociados. No se puede restaurar una página personalizada suprimida. Para eliminar temporalmente una página personalizada de la interfaz de usuario, inhabilite la página personalizada.

Para habilitar, inhabilitar, o suprimir una página personalizada, vaya al nodo **Configuration Management** (Gestión de configuraciones) > **User Interface Extensions** (Ampliaciones de la interfaz de usuario) y seleccione la acción deseada en el menú Tareas o el menú contextual.

Interfaz de línea de comandos

La CLI permite acceder a eficaces funciones del producto de administración y aplicarlas mediante comandos y archivos por lotes. Con la CLI, puede emitir un comando para implementar los cambios realizados en varios objetos.

Por ejemplo, si necesita cambiar de ubicación los directorios personales de 200 empleados a un nuevo servidor, con la CLI, puede introducir el siguiente comando individual para cambiar las 200 cuentas de usuario:

```
EA USER @GroupUsers(HOU_VENTAS),@GroupUsers(HOU_VARIOS) UPDATE  
HOMEDIR: \\HOU2\USERS\@Target()
```

Este comando le indica a DRA que cambie el campo del directorio personal de cada una de las 200 cuentas de usuario en los grupos HOU_VENTAS y HOU_VARIOS en \\HOU2\USERS\id_usuario. Para realizar esta tarea con las herramientas de administración nativas de Microsoft Windows, deberá realizar un mínimo de 200 acciones independientes.

Nota: La herramienta CLI quedará obsoleta en versiones futuras, a medida que se añadan más funciones a PowerShell.

8.1.2 Herramientas personalizadas

Se pueden utilizar herramientas personalizadas para llamar a cualquier aplicación que se ejecute en equipos cliente y de servidor en la red mediante la selección de una cuenta de Active Directory que se gestione en DRA.

DRA admite dos tipos de herramientas personalizadas:

- ♦ Herramientas personalizadas que lancen utilidades de escritorio comunes, como Microsoft Office.
- ♦ Herramientas personalizadas que cree y distribuya en cada equipo cliente DRA.

Puede crear una herramienta personalizada que inicie un análisis antivirus desde todos los equipos en los que se haya instalado DRA. También puede crear una herramienta personalizada que inicie una aplicación externa o una herramienta que requiera que DRA actualice un guión periódicamente. Estas actualizaciones periódicas pueden ser cambios en la configuración o en la regla de negocios. Por lo tanto, después de las actualizaciones periódicas, DRA replica las herramientas personalizadas del servidor de administración principal en los servidores de administración secundarios y los equipos cliente de DRA.

Para comprender cómo se replican las herramientas personalizadas en el conjunto de varios maestros del servidor, consulte [Réplica de archivos](#).

Creación de herramientas personalizadas

Puede crear herramientas personalizadas en el servidor principal de DRA al asociar un objeto de Active Directory seleccionado o a todos los objetos de Active Directory que se muestren en ese Asistente para crear herramientas personalizadas. Se replicarán las mismas herramientas en los servidores secundarios del MMS y los clientes de DRA mediante la réplica de archivos.

Una nueva herramienta personalizada creará un menú y un submenú, si es necesario, para llamar a la operación que se realizará en los objetos de Active Directory asociados en DRA.

Puede delegar poderes a administradores asistentes para crear y ejecutar herramientas personalizadas, y acceder a la aplicación y ejecutarla.

Al crear una herramienta personalizada, deberá introducir los parámetros, como se indica a continuación:

General (pestaña)

1. **Nombre:** cualquier nombre de cliente necesario para la herramienta.
2. **Menú y submenú:** para crear un elemento de menú para una nueva herramienta personalizada, escriba el título del menú en el campo **Menu and Submenu Structure** (Estructura de menús y submenús). Al crear una herramienta personalizada y seleccionar el objeto, DRA muestra el elemento de menú de herramientas personalizadas mediante la estructura de menús y submenús que especifique en el menú Tareas, el menú de acceso directo y la barra de herramientas de DRA.

Ejemplo de estructura de menús y submenús: escriba el nombre del elemento de menú, un carácter de barra diagonal inversa (\) y, a continuación, el nombre del elemento de submenú.

Para tener una tecla de acceso directo: escriba un carácter de Y comercial (&) delante del nombre del elemento de menú.

- a. **Ejemplo:** `EnviarCorreoElectrónico\AprobarAcción` ---- `EnviarCorreoElectrónico` es el menú y `AprobarAcción` es el submenú y la primera letra ("A") de `AprobarAcción` es la tecla de acceso directo habilitada.

3. **Habilitado:** marque esta casilla para activar la herramienta personalizada.
4. **Descripción:** puede añadir cualquier valor de descripción necesario.
5. **Comentario:** puede añadir los comentarios necesarios en la herramienta personalizada.

Pestaña Objetos admitidos

Seleccione el objeto de AD necesario o todos los objetos de AD a los que se asociará la herramienta personalizada creada.

Entre las opciones de herramientas personalizadas admitidas, se incluyen: Dominio gestionado, Contenedores, Usuarios, Contactos, Grupos, Equipos, Unidad administrativa e Impresoras publicadas.

Nota: Otros objetos introducidos recientemente como Buzón de recursos, Grupo dinámico y Grupo dinámico de Exchange no son compatibles con las herramientas personalizadas.

Pestaña Ajustes de la aplicación

Ubicación de la aplicación: es necesario proporcionar la vía o la ubicación en las que se ha instalado la aplicación. Para ello, copie o pegue la vía exacta de la aplicación o utilice la opción **Insertar**.

También puede usar variables de DRA, variables de entorno y valores de registro para especificar la ubicación de la aplicación externa en el campo "Location of the application" (Ubicación de la aplicación). Para utilizar estas variables, haga clic en **Insertar** y seleccione la variable que desee utilizar.

Después de insertar la variable, escriba un carácter de barra invertida (\) y, a continuación, especifique el resto de la vía de la aplicación, incluido el nombre del archivo ejecutable de la aplicación.

Ejemplos:

- ♦ *Ejemplo 1:* para especificar la ubicación de una aplicación externa que ejecutará la herramienta personalizada, seleccione la variable de entorno `{%PROGRAMFILES%}` y, a continuación, especifique el resto de la vía de la aplicación en el campo "Location of the application" (Ubicación de la aplicación): `{%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe`

Nota: DRA proporciona el valor de Registro del directorio de instalación de Office como ejemplo. Para especificar una clave del Registro que contenga una vía como valor, utilice la siguiente sintaxis: `{HKEY_LOCAL_MACHINE\SOFTWARE\MiProducto\Clave\ (Por defecto)}`

- ♦ *Ejemplo 2:* para especificar la ubicación de un archivo de guión personalizado que utilizará la herramienta personalizada, seleccione la variable de DRA `{Vía_archivos_replicados_DRA}` y, a continuación, especifique el resto de la vía del archivo de guión en el campo "Location of the application" (Ubicación de la aplicación): `{Vía_archivos_replicados_DRA}\cscript.vbs ;` donde `{Vía_archivos_replicados_DRA}` es la vía a los archivos replicados o la carpeta `{DirInstalDRA}\FileTransfer\Replicate` del servidor de administración.

Nota: Antes de crear la herramienta personalizada, cargue el archivo de guión en el servidor de administración principal mediante la función de réplica de archivos. La función de réplica de archivos carga el archivo de guión en la carpeta `{DirInstalDRA}\FileTransfer\Replicate` del servidor de administración principal.

- ♦ *Ejemplo 3:* para especificar la ubicación de una utilidad de DRA que ejecutará la herramienta personalizada, seleccione la variable de DRA {Vía_aplicación_DRA} y, a continuación, especifique el resto de la vía de la utilidad en el campo "Location of the application" (Ubicación de la aplicación): {Vía_aplicación_DRA}\DRADiagnosticUtil.exe, donde {Vía_aplicación_DRA} es la ubicación en la que se ha instalado DRA.
- ♦ *Ejemplo 4:* simplemente copie y pegue la ubicación de la aplicación junto con el nombre del archivo de la aplicación con la extensión.

Parámetros que se transferirán a la aplicación: para definir un parámetro que se transferirá a una aplicación externa, copie y pegue, o escriba uno o más parámetros en el campo "Parameters to pass to the application" (Parámetros que se transferirán a la aplicación). DRA proporciona parámetros que puede utilizar en el campo "Parameters to pass to the application" (Parámetros que se transferirán a la aplicación). Para utilizar estos parámetros, haga clic en Insertar y seleccione el parámetro o los parámetros que desea usar. Al proporcionar las propiedades del objeto como un parámetro, asegúrese de que el administrador asistente disponga de los permisos de lectura necesarios en la propiedad de objeto, junto con el poder *Ejecutar herramientas personalizadas* para ejecutar la herramienta personalizada.

Ejemplos:

- ♦ *Ejemplo 1:* para transferir el nombre de grupo y de dominio como parámetros a una aplicación o guión externos, seleccione los parámetros Nombre de la propiedad de objeto y Nombre de la propiedad de dominio y especifique los nombres de los parámetros en el campo "Parameters to pass to the application" (Parámetros que se transferirán a la aplicación): "{Object.Name}" "{Domain.\$McsName}"
- ♦ *Ejemplo 2:* para transferir el parámetro "ipconfig" de la aplicación "C:\Windows\SysWOW64\cmd.exe", simplemente escriba "{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}" en ese campo.

Directorio en el que se ejecutará la aplicación: esta es la ubicación en la que debe ejecutarse la aplicación en el equipo cliente o del servidor. Debe transferir la vía en la que se debe ejecutar la aplicación. También puede utilizar la opción "Insertar" de la misma manera que se transfiere el parámetro en el campo "Location of the application" (Ubicación de la aplicación). Otros parámetros de esta pestaña explican de forma implícita su uso.

8.1.3 Personalización de la interfaz de usuario

Hay varias opciones para personalizar la configuración de la consola de delegación y configuración. La mayoría de estas opciones permiten ocultar, visualizar o volver a configurar funciones en los diferentes paneles de funciones de la aplicación. También puede ocultar o visualizar la barra de herramientas, personalizar el título de la aplicación y añadir, eliminar o reordenar columnas. Todas estas opciones de personalización se encuentran en el menú **Ver**.

Modificación del título de la consola

Puede modificar la información que se muestra en la barra de título de la consola de delegación y configuración, y 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 delegación y configuración.

- 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**. Para obtener más información, haga clic en el icono ?.

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**.

8.2 Cliente Web

En el cliente Web, puede personalizar las propiedades de objeto, los formularios de Automatización del flujo de trabajo y la marca de la interfaz de usuario. Si se han implementado correctamente, las personalizaciones de propiedades y flujos de trabajo ayudarán a automatizar las tareas del administrador asistente mediante la gestión de objetos y los envíos de flujos de trabajo automatizados.

8.2.1 Personalización de las páginas de propiedades

Puede personalizar los formularios de propiedades de objetos que los administradores asistentes utilizan en sus funciones 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 realiza el administrador asistente en el cliente Web; las personalizaciones pueden aumentar la eficacia y la experiencia del administrador al gestionar los objetos de Active Directory en DRA.

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

- 1 Entrada a la consola Web como administrador de DRA.
- 2 Desplácese a **Personalización > Páginas de propiedad**.
- 3 Seleccione un tipo de objeto y un tipo de operación (crear o editar) en la lista Páginas de propiedad.
- 4 Haga clic en el botón **Editar** .
- 5 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](#).

Creación de una nueva página de propiedades de objeto

Para crear una nueva página de propiedades de objeto:

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

8.2.2 Personalización de formularios de flujo de trabajo

Al crear o modificar formularios de flujo de trabajo, estos se guardan en el servidor Web y se accede a ellos desde la página [Personalización > Flujo de trabajo](#) de la consola Web. Estos formularios se utilizan para enviar flujos de trabajo automatizados que se crean en el servidor de Automatización del flujo de trabajo. Puede personalizar los formularios para automatizar y mejorar aún más la capacidad de uso de los administradores asistentes cuando utilizan formularios para realizar tareas de gestión de objetos.

Puede añadir y modificar las propiedades de formularios existentes y los gestores personalizados. El comportamiento de la interfaz para añadir y personalizar propiedades es el mismo en un formulario de Automatización del flujo de trabajo que al personalizar propiedades de objetos. Consulte los temas mostrados a continuación para obtener más información sobre cómo añadir y modificar propiedades, añadir gestores personalizados, y para comprender la Automatización del flujo de trabajo.

- ♦ [Personalización de las páginas de propiedades](#) (Cliente Web)
- ♦ [Adición de gestores personalizados](#)
- ♦ [Flujo de trabajo automatizado](#)

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 y para las personalizaciones de carga y envío en un formulario de creación, propiedad o 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.

Los gestores de carga de formularios permiten a los usuarios personalizar formularios al realizar normalmente una inicialización de controles. Los gestores de envío de formularios permiten a los usuarios realizar una validación y, posiblemente, cancelar el envío si se produce un problema.


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. Puede acceder a los gestores de carga y envío de formularios desde Propiedades del formulario en un formulario de flujo de trabajo o una página de creación de objetos.

- 1 Haga clic en la pestaña de gestores personalizados correspondiente y habilite la página 
 - ♦ Gestores personalizados
 - ♦ Gestores de carga de formularios
 - ♦ Gestores de envío de formularios
- 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.

8.2.3 Personalización de la marca de la interfaz de usuario

Puede personalizar la barra de título de la consola Web de DRA con 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 Entrada a la consola Web como administrador de DRA.
- 2 Desplácese a **Personalización > Marca**.
- 3 Si va a añadir un logotipo de la empresa, guarde la imagen de logotipo en la ubicación `components\lib\img` del servidor Web.
- 4 Añada la información necesaria, según corresponda, en los tres campos de la página de personalización de marca y guarde los cambios.

9 Herramientas y utilidades

En estas secciones, se abordan las utilidades de diagnóstico, Objetos suprimidos, comprobación de estado y Papelera proporcionadas con DRA.

9.1 Utilidad de diagnóstico

La utilidad de diagnóstico recopila información del servidor de administración para ayudar a diagnosticar problemas con DRA. Use esta utilidad para proporcionar archivos de registro a su representante de asistencia técnica. La utilidad de diagnóstico proporciona una interfaz de asistente que le guía a través de la configuración de niveles de registro y la recopilación de información de diagnóstico.

Puede acceder a la utilidad de diagnóstico desde cualquier equipo del servidor de administración. Sin embargo, debe ejecutar la utilidad de diagnóstico en el servidor de administración en el que está experimentando el problema.

Para acceder a la utilidad de diagnóstico, entre a la sesión del equipo del servidor de administración mediante la cuenta de administrador de DRA y ejecute `DRADiagnosticUtil.exe` en la carpeta Archivos de programa (x86)\NetIQ\DRA.

Para obtener más información acerca del uso de esta utilidad, póngase en contacto con el [servicio de asistencia técnica](#).

9.2 Utilidad Objetos suprimidos

Esta utilidad le permite habilitar la compatibilidad con la actualización incremental de la memoria caché de cuentas para un dominio específico cuando la cuenta de acceso al dominio no es un administrador. Si la cuenta de acceso al dominio no tiene permisos de lectura en el contenedor Objetos suprimidos del dominio, DRA no puede realizar una actualización incremental de la memoria caché de cuentas.

Puede usar esta utilidad para realizar las siguientes tareas:

- ♦ Compruebe que la cuenta de usuario o el grupo especificados disponen de permisos de lectura en el contenedor Objetos suprimidos del dominio especificado.
- ♦ Delege o elimine permisos de lectura en una cuenta de usuario o grupo específicos.
- ♦ Delege o elimine el derecho de usuario Sincronizar los datos del servicio de directorio en una cuenta de usuario.
- ♦ Visualice la configuración de seguridad del contenedor Objetos suprimidos.

Puede ejecutar el archivo de la utilidad Objetos suprimidos (`DraDelObjsUtil.exe`) desde la carpeta Archivos de programa (x86)\NetIQ\DRA del servidor de administración.

9.2.1 Permisos necesarios para la utilidad Objetos suprimidos

Para usar esta utilidad, debe disponer de los permisos siguientes:

Si desea ...	Si necesita este permiso...
Verificar los permisos de cuenta	Permisos de lectura en el contenedor Objetos suprimidos
Delegar permisos de lectura en el contenedor Objetos suprimidos	Permisos de administrador en el dominio en el que se encuentra el contenedor Objetos suprimidos
Delegar el derecho de usuario Sincronizar datos del servicio de directorio	Permisos de administrador en el dominio en el que se encuentra el contenedor Objetos suprimidos
Eliminar los permisos delegados anteriormente	Permisos de administrador en el dominio en el que se encuentra el contenedor Objetos suprimidos
Visualice la configuración de seguridad del contenedor Objetos suprimidos.	Permisos de lectura en el contenedor Objetos suprimidos

9.2.2 Sintaxis de la utilidad Objetos suprimidos

```
DRADELOBJSUTIL /DOMAIN:NOMBREDOMINIO [/DC:NOMBREEQUIPO] {/  
DELEGATE:NOMBRECuenta | /VERIFY:NOMBRECuenta | /REMOVE:NOMBRECuenta | /  
DISPLAY [/RIGHT]}
```

9.2.3 Opciones de la utilidad Objetos suprimidos

Puede especificar las siguientes opciones:

<i>/DOMAIN: dominio</i>	Especifica el nombre de NETBIOS o DNS del dominio donde se encuentra el contenedor Objetos suprimidos.
<i>/SERVER: nombre_equipo</i>	Especifica el nombre o la dirección IP del controlador de dominio del dominio especificado.
<i>/DELEGATE: nombre_de_cuenta</i>	Delega los permisos a la cuenta de usuario o el grupo especificados.
<i>/REMOVE: nombre_de_cuenta</i>	Elimina los permisos delegados anteriormente en la cuenta de usuario o el grupo especificados.
<i>/VERIFY: nombre_de_cuenta</i>	Compruebe los permisos de la cuenta de usuario o el grupo especificados.
<i>/DISPLAY</i>	Muestra la configuración de seguridad del contenedor Objetos suprimidos en el dominio especificado.
<i>/RIGHT</i>	Garantiza que la cuenta de usuario o el grupo especificados dispongan del derecho de usuario Sincronizar datos del servicio de directorio. Puede utilizar esta opción para delegar o verificar este derecho. El derecho de usuario Sincronizar datos del servicio de directorio permite que la cuenta lea todos los objetos y las propiedades de Active Directory.

Nota

- ♦ Si el nombre de la cuenta de usuario o el grupo que desea especificar contiene un espacio, escriba el nombre de la cuenta entre comillas. Por ejemplo, si desea especificar el grupo de TI de Houston, escriba "Houston TI".
 - ♦ Al especificar un grupo, utilice el nombre anterior a Windows 2000 para ese grupo.
-

9.2.4 Ejemplos de la utilidad Objetos suprimidos

A continuación, se muestran ejemplos de comandos en situaciones habituales.

Ejemplo 1

Para comprobar que la cuenta de usuario MYCOMPANY\JSmith disponga de permisos de lectura en el contenedor Objetos suprimidos del dominio hou.mycompany.com, introduzca:

```
DRADELOBSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Ejemplo 2

Para delegar permisos de lectura en el contenedor Objetos suprimidos del dominio MYCOMPANY en el grupo MYCOMPANY\DraAdmins, introduzca:

```
DRADELOBSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Ejemplo 3

Para delegar permisos de lectura en el contenedor Objetos suprimidos y el derecho de usuario Sincronizar datos del servicio de directorio del dominio MYCOMPANY en la cuenta de usuario MYCOMPANY\JSmith, introduzca:

```
DRADELOBSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

Ejemplo 4

Para visualizar la configuración de seguridad del contenedor Objetos suprimidos del dominio hou.mycompany.com mediante el controlador de dominio HQDC, introduzca:

```
DRADELOBSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

Ejemplo 5

Para eliminar los permisos de lectura en el contenedor Objetos suprimidos del dominio MYCOMPANY del grupo MYCOMPANY\DraAdmins, introduzca:

```
DRADELOBSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

9.3 Utilidad de comprobación de estado

La utilidad de comprobación de estado de DRA es una aplicación independiente que se incluye con el kit de instalación de DRA. Puede usar esta utilidad después de la instalación, y antes y después de la actualización para verificar, validar y notificar el estado de los componentes y procesos del

servidor DRA, y el sitio Web y los clientes de DRA. También puede utilizarla para instalar o actualizar una licencia de producto, realizar una copia de seguridad de la instancia de AD LDS antes de aplicar una actualización del producto, ver descripciones de las comprobaciones y corregir problemas o identificar acciones que deben realizarse para solucionar problemas y validarlos de nuevo a continuación.

Se puede acceder a la utilidad de comprobación de estado desde la carpeta del programa DRA después de ejecutar el instalador `NetIQAdminInstallationKit.msi`.

Puede ejecutar la utilidad de comprobación de estado en cualquier momento. Para ello, ejecute el archivo `NetIQ.DRA.HealthCheckUI.exe`. Cuando se abre la aplicación, puede optar por realizar una operación específica, o ejecutar comprobaciones en determinados componentes o en todos ellos. Consulte a continuación las funciones eficaces que puede usar con la utilidad de comprobación de estado:

Función	Acciones de usuario
Seleccionar todo o anular la selección de todo	Utilice las opciones de la barra de herramientas o del menú Archivo para seleccionar o anular la selección de todos los elementos de comprobación o seleccione casillas de verificación individuales para ejecutar comprobaciones específicas.
Ejecutar las comprobaciones seleccionadas	Utilice esta opción de la barra de herramientas o el menú Archivo para ejecutar las comprobaciones seleccionadas (todas o específicas).
Guardar o escribir resultados	Utilice esta opción de la barra de herramientas o el menú Archivo para crear y guardar un informe detallado de las comprobaciones que se ejecutan.
Ejecutar esta comprobación	<p>Seleccione el título de un elemento para ver una descripción de la comprobación y, a continuación, haga clic en este icono de la barra de herramientas para ejecutar la comprobación. Por ejemplo, para ejecutar una de las operaciones siguientes:</p> <ul style="list-style-type: none"> ◆ Instalar o actualizar una licencia de producto (Validación de la licencia). ◆ Realizar una copia de seguridad de la instancia de AD LDS (Copia de seguridad de la instancia de AD LDS).
Solucionar este problema	Seleccione el título de un elemento y, a continuación, utilice esta opción de la barra de herramientas si se ha producido un error en una comprobación. Si ejecutar de nuevo la comprobación no soluciona el problema, la descripción debe incluir información o acciones que puede realizar para resolver el problema.

9.4 Utilidad Papelera

Esta utilidad permite habilitar la compatibilidad con la Papelera cuando se está gestionando un subárbol de un dominio. Si la cuenta de acceso al dominio no tiene permisos en el contenedor `NetIQRecycleBin` oculto del dominio especificado, DRA no podrá transferir las cuentas suprimidas a la Papelera.

Nota: Después de utilizar esta utilidad para habilitar la Papelera, realice una actualización completa de la memoria caché de cuentas para asegurarse de que el servidor de administración aplique este cambio.

Puede usar esta utilidad para realizar las siguientes tareas:

- ♦ Compruebe que la cuenta especificada dispone de permisos de lectura en el contenedor NetIQRecycleBin del dominio especificado.
- ♦ Delege permisos de lectura a la cuenta especificada.
- ♦ Visualice la configuración de seguridad del contenedor NetIQRecycleBin.
- ♦ [Sección 9.4.1, “Permisos necesarios para la utilidad Papelera”, en la página 157](#)
- ♦ [Sección 9.4.2, “Sintaxis de la utilidad Papelera”, en la página 157](#)
- ♦ [Sección 9.4.3, “Opciones de la utilidad Papelera”, en la página 157](#)
- ♦ [Sección 9.4.4, “Ejemplos de la utilidad Papelera”, en la página 157](#)

9.4.1 Permisos necesarios para la utilidad Papelera

Para usar esta utilidad, debe disponer de los permisos siguientes:

Si desea ...	Si necesita este permiso...
Verificar los permisos de cuenta	Permisos de lectura en el contenedor NetIQRecycleBin
Delegar permisos de lectura en el contenedor NetIQRecycleBin	Permisos de administrador en el dominio especificado
Visualizar la configuración de seguridad del contenedor NetIQRecycleBin	Permisos de lectura en el contenedor NetIQRecycleBin

9.4.2 Sintaxis de la utilidad Papelera

```
DRARECYCLEBINUTIL /DOMAIN:NOMBREDOMINIO [/DC:NOMBREEQUIPO] {/  
DELEGATE:NOMBRECuenta | /VERIFY:NOMBRECuenta | /DISPLAY}
```

9.4.3 Opciones de la utilidad Papelera

Las siguientes opciones permiten configurar la utilidad Papelera:

<code>/DOMAIN: <i>dominio</i></code>	Especifica el nombre de NETBIOS o DNS del dominio donde se encuentra la Papelera.
<code>/SERVER: <i>nombre_equipo</i></code>	Especifica el nombre o la dirección IP del controlador de dominio del dominio especificado.
<code>/DELEGATE: <i>nombre_de_cuenta</i></code>	Delega permisos en la cuenta especificada.
<code>/VERIFY: <i>nombre_de_cuenta</i></code>	Comprueba los permisos de la cuenta especificada.
<code>/DISPLAY</code>	Muestra la configuración de seguridad del contenedor NetIQRecycleBin en el dominio especificado.

9.4.4 Ejemplos de la utilidad Papelera

A continuación, se muestran ejemplos de comandos en situaciones habituales.

Ejemplo 1

Para comprobar que la cuenta de usuario `MYCOMPANY\JSmith` disponga de permisos de lectura en el contenedor `NetIQRecycleBin` del dominio `hou.mycompany.com`, introduzca:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

Ejemplo 2

Para delegar permisos de lectura en el contenedor `NetIQRecycleBin` del dominio `MYCOMPANY` en el grupo `MYCOMPANY\DraAdmins`, introduzca:

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

Ejemplo 3

Para visualizar la configuración de seguridad del contenedor `NetIQRecycleBin` del dominio `hou.mycompany.com` mediante el controlador de dominio `HQDC`, introduzca:

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```