Directory and Resource Administrator

Guía de instalación

Julio de 2018

Información legal

Acerca de esta guía

La *Guía de instalación* proporciona información sobre la planificación, la instalación, las licencias y la configuración para Directory and Resource Administrator (DRA) y sus componentes integrados.

Esta manual le guiará por el proceso de instalación y le ayudará a tomar las decisiones correctas para instalar y configurar DRA.

A quién va dirigida

Esta guía proporciona información para cualquier usuario que instale DRA.

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/).

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.

¿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.

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

De forma conjunta, DRA y ExA proporcionan 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.

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 (La persona encargada del mantenimiento de la configuración del producto)	Consola de delegación y configuración	Servidor principal
	Configuración de Reporting Center de DRA (NRC) CLI *(opcional)* Proveedor ADSI de DRA *(opcional)*	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

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.

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.).

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.

Consola Web

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

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

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

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

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

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.

Motor de flujo de trabajo

DRA se integra con el motor de flujo de trabajo 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/).

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.

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.

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

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.

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 y clientes de DRA	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).
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.

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	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3 (excepto las carpetas públicas) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online
Microsoft Office 365	◆ 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	◆ Microsoft Skype Empresarial 2015
Historial de cambios	◆ Change Guardian 5.0 y 5.1

Sistema gestionado	Requisitos previos
Navegadores Web	◆ Microsoft Internet Explorer 11 y Microsoft Edge ◆ Google Chrome ◆ Mozilla Firefox

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	◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 2008 R2 se admite solo para la actualización. **Nota:** El servidor también debe ser un miembro de un dominio nativo de Microsoft Windows Server admitido. **Interfaces de DRA de Windows:** ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 8.1 (x86 y x64) y 10 (x86 y x64)
Instalador	◆ Microsoft .NET Framework 4.5.2 y posterior
Servidor de administración	**Directory and Resource Administrator:** ◆ Microsoft .NET Framework 4.5.2 y posterior ◆ Uno de los siguientes: ◆ 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 **Administración de Microsoft Office 365/Exchange Online:** ◆ 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 Para obtener más información, consulte Plataformas compatibles.

Componente	Requisitos previos
Componentes Web heredados	**Servidor Web:** ◆ Versiones 8.0, 8.5 y 10 de Microsoft Internet Information Services (IIS) **Componentes de Microsoft IIS:** ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Servicio de funciones de seguridad de Microsoft IIS **Interfaces de DRA de Windows:** ◆ 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 de servicio de DRA	Los permisos necesarios para ejecutar el servicio de administración de NetIQ.	◆ Permisos de "Usuarios COM distribuidos". ◆ Miembro del grupo de administradores de AD LDS. ◆ Grupo de operadores de cuentas. ◆ Grupos de archivos de registro (OnePointOp ConfgAdms y OnePointOp). **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.
Administrador de DRA	Cuenta de usuario o grupo configurada para la función integrada de administradores de DRA.	◆ Grupo de seguridad local de dominio o cuenta de usuario de dominio. ◆ Miembro del dominio gestionado o un dominio de confianza. ◆ Si especifica una cuenta desde un dominio de confianza, asegúrese de que el equipo del servidor de administración pueda autenticar esta cuenta.

Cuenta	Descripción	Permisos
Cuentas de administrador asistente de DRA	Cuentas con competencias delegadas a través de DRA.	◆ 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. **Nota:** Se puede configurar DRA para gestionar esto durante la instalación.

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 usuario
- Control TOTAL de los objetos de equipo
- Control TOTAL de los objetos de grupo
- Control TOTAL de los objetos de contacto
- Control TOTAL de los objetos de unidad organizativa
- Control TOTAL de los objetos de Inetorgperson
- Control TOTAL de los objetos de impresora
- Control TOTAL de los objetos de dominio integrados
- Control TOTAL de los objetos de contenedor
- Control TOTAL de los objetos de MsExchSystemObjectContainer
- Control TOTAL de los grupos de distribución dinámica
- Control TOTAL de las carpetas públicas

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

- Permitir creación de objetos de equipo.
- Permitir supresión de objetos de equipo.
- Permitir creación de objetos de contacto.
- Permitir supresión de objetos de contacto.
- Permitir creación de objetos de grupo.
- Permitir supresión de objetos de grupo.
- Permitir supresión de objetos de InetOrgPerson.
- Permitir creación de objetos de unidad organizativa.
- Permitir supresión de objetos de unidad organizativa.
- Permitir creación de objetos de usuario.
- Permitir supresión de objetos de usuario.
- Permitir creación de grupos de distribución dinámica.

- Permitir supresión de grupos de distribución dinámica.
- Permitir creación de punto de conexión de servicio.
- Permitir supresión de punto de conexión de servicio.
- Permitir creación de contenedor.
- Permite supresión de contenedor.
- Permitir creación de carpetas públicas.
- Permitir supresión de carpetas públicas.

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.

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:** ◆ 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	◆ Microsoft .NET Framework 4.5.2 ◆ Servidor de administración de DRA
Servicio y puesto final REST de DRA	◆ Microsoft .NET Framework 4.5.2
Extensiones de PowerShell	◆ Microsoft .NET Framework 4.5.2 ◆ PowerShell 4.0
Consola Web de DRA	**Servidor Web:** ◆ Microsoft Internet Information Server 8.0, 8.5 y 10 ◆ Microsoft Internet Information Services WCF (activación) **Componentes de Microsoft IIS:** ◆ Servidor Web ◆ Características HTTP comunes ◆ Contenido estático ◆ Documento por defecto ◆ Navegador de directorios ◆ Errores HTTP ◆ Desarrollo de aplicaciones ◆ ASP ◆ Estado y diagnóstico ◆ Registro HTTP ◆ Monitor de petición ◆ Seguridad ◆ Autenticación básica ◆ Rendimiento ◆ Compresión de contenido estático ◆ Herramientas de gestión del servidor Web

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	**Sistema operativo:** ◆ Microsoft Windows Server 2012, 2012 R2, 2016
NetIQ Reporting Center (v3.2)	**Base de datos:** ◆ Microsoft SQL Server 2012, 2014 y 2016 ◆ Servicios de informes de Microsoft SQL Server **Servidor Web:** ◆ Microsoft Internet Information Server 8.0, 8.5 y 10 ◆ Componentes de Microsoft IIS: ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** Todos los servidores de administración de DRA que se conectan al módulo de elaboración de informes de DRA también requieren .NET Framework 3.5. **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.
Módulo de elaboración de informes de DRA	**Base de datos:** ◆ Microsoft SQL Server Integration Services ◆ Agente Microsoft SQL Server

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 (License1.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.

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.

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** ◆ Kit de recursos del archivo de registro ◆ SDK de DRA de NetIQ **Componente Web heredado** **Interfaces de usuario** ◆ 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.

Paso	Detalles
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 “Configuring the Multi-Master Set?” (¿Qué es un conjunto de varios maestros?) en *Directory and Resource Administrator Administrator Guide* (Guía del administrador de Directory and Resource Administrator).
Especificar las cuentas y las credenciales de instalación	◆ Cuenta de servicio de DRA ◆ Grupo de AD LDS ◆ Administrador de DRA Para obtener más información, consulte: Requisitos del servidor de administración de DRA.
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.

Instalación de 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*.

Instalación de 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 `NetIQAdminINstallationKit.msi` 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 `DRARESTExtensionsInstaller.exe` y seleccione **Ejecutar como administrador**.
Aceptar el acuerdo de licencia (EULA)	Acepte los términos del acuerdo de licencia de usuario final.

Paso	Detalles
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 `C:\Archivos de programa (x86)\NetIQ\DRA Extensions` 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.
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.

Instalación del servidor de flujo de trabajo

Para obtener información sobre cómo instalar el servidor de flujo de trabajo, consulte Aegis Administrator Guide (Guía del administrador de Aegis).

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 `NetIQAdminINstallationKit.msi` 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 `NRCSetup.exe`.

Pasos	Detalles
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 `C:\Archivos de programa (x86)\NetIQ\Reporting Center` o especifique una ubicación para la instalación.
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 `DRAReportingSetup.exe` 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.

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 “Configuring the Multi-Master Set” (Configuración del conjunto de varios maestros) en *Directory and Resource Administrator Administrator Guide* (Guía del administrador de Directory and Resource Administrator).

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.

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	*Opcional:* 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 tiene un motivo para 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**.

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	*(Opcional)* 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.

Actualización de los componentes del módulo de elaboración de informes de DRA

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 *Reporting Center Guide* (Guía de Reporting Center) en el sitio de documentación de DRA.

Pasos	Detalles
Inhabilitar la compatibilidad con el módulo de elaboración de informes de DRA	Para asegurarse de que los recopiladores 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	*Condicional:* 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.

Pasos	Detalles
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 *NetIQ Reporting Center Reporting Guide* (Guía de informes de NetIQ Reporting Center) en el sitio de documentación de DRA.

Actualización de 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 versiones posteriores. 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: Instalación de 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 de DRA 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`

3 Configuración del producto

En este capítulo, se describen los pasos y los procedimientos de configuración necesarios si va a instalar por primera vez Directory and Resource Administrator.

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
Aplicar 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.
Abrir la consola de delegación y configuración	Con la cuenta de servicio de DRA, entre en un equipo en el que se haya instalado la consola de delegación y configuración. Abra la consola.
Añadir el primer dominio gestionado a DRA	Añada el primer dominio gestionado a DRA. **Nota:** Puede iniciar las funciones de delegación una vez completada la actualización completa inicial de la cuenta.
Añadir subárboles y dominios gestionados	*Opcional:* añada subárboles y dominios gestionados adicionales a DRA. Para obtener más información sobre los dominios gestionados, consulte Adición de dominios gestionados.
Configurar los ajustes de DCOM	*Opcional:* configure los ajustes de DCOM. Para obtener más información sobre los ajustes de DCOM, consulte Configuración de los ajustes de DCOM.

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.

Adición de dominios gestionados

Puede añadir servidores, estaciones de trabajo o dominios gestionados después de instalar el servidor de administración. Al añadir el primer dominio administrado, debe entrar a la sesión mediante la cuenta de servicio de DRA en un equipo en el que se haya instalado la consola de delegación y configuración. También debe tener derechos administrativos dentro del dominio, como

los derechos concedidos al grupo Administradores de dominio. Para añadir equipos y dominios gestionados después de instalar el primer dominio gestionado, debe tener los permisos 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 obtener más información sobre cómo modificar la programación de actualización de caché de cuentas, consulte “Configuring Caching” (Configuración del almacenamiento en caché) en *Directory and Resource Administrator Administrator Guide* (Guía del administrador de Directory and Resource Administrator).

Adición de subárboles gestionados

Puede añadir subárboles gestionados de dominios específicos de Microsoft Windows después de instalar el servidor de administración. Puede añadir los subárboles que falten y que desee gestionar mediante el nodo Configuración avanzada de la consola de delegación y configuración. Para añadir subárboles gestionados después de instalar el servidor de administración, debe tener los permisos adecuados, como los que se incluyen en la función integrada Configurar servidores y dominios. Para garantizar que la cuenta de acceso especificada tenga permisos para gestionar este subárbol y realizar actualizaciones incrementales de caché de cuentas, utilice la herramienta Objetos eliminados para comprobar y delegar los permisos correspondientes.

Para obtener más información sobre el uso de esta utilidad, consulte “Deleted Objects Utility” (Utilidad Objetos eliminados) en *Directory and Resource Administrator Administrator Guide* (Guía del administrador de Directory and Resource Administrator).

Para obtener más información sobre la configuración de la cuenta de acceso, consulte “Specifying Domain Access Accounts” (Especificar cuentas de acceso al dominio) en *Directory and Resource Administrator Administrator Guide* (Guía del administrador de Directory and Resource Administrator).

Nota: 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 obtener más información sobre cómo modificar la programación de actualización de caché de cuentas, consulte “Configure Caching” (Configurar el almacenamiento en caché) en *Directory and Resource Administrator Administrator Guide* (Guía del administrador de Directory and Resource Administrator).

Configuración de los ajustes de DCOM

Configure los ajustes de DCOM en el servidor de administración principal si no ha permitido que el programa de instalación configurara automáticamente DCOM.

Configuración del grupo Usuarios COM distribuidos

Si ha optado por no configurar el componente COM distribuido durante el proceso de instalación de DRA, debe actualizar la suscripción al grupo Usuarios COM distribuidos para incluir todas las cuentas de usuario que utilicen DRA. Esta suscripción debe incluir la cuenta de servicio de DRA y todos los administradores asistentes.

Para configurar el grupo Usuarios COM distribuidos:

1. Entre en un equipo cliente de DRA como un administrador de DRA.
2. Inicie la consola de delegación y configuración. Si la consola no se conecta automáticamente al servidor de administración, establezca la conexión manualmente.

   Nota: Es posible que no pueda conectarse al servidor de administración si el grupo de Usuarios COM distribuidos no contiene ninguna cuenta de administrador asistente. Si este es el caso, configure el grupo Usuarios COM distribuidos mediante el módulo integrable Usuarios y equipos de Active Directory. Para obtener más información sobre el módulo integrable Usuarios y equipos de Active Directory, consulte el sitio Web de Microsoft.

   ---
3. En el panel de la izquierda, expanda **Gestión de cuentas y recursos**.
4. Expanda **Todos mis objetos gestionados**.
5. Expanda el nodo de cada dominio en el que haya un controlador de dominio.
6. Haga clic en el contenedor **Incorporado**.
7. Busque el grupo Usuarios COM distribuidos.
8. En la lista de resultados de búsqueda, haga clic en el grupo **Usuarios COM distribuidos**.
9. Haga clic en **Miembros** en el panel inferior y, a continuación, haga clic en **Añadir miembros**.
10. Añada usuarios y grupos que utilizarán DRA. Asegúrese de añadir la cuenta de servicio de DRA a este grupo.
11. Haga clic en **Aceptar**.

Configuración del controlador de dominio y el servidor de administración

Después de configurar el equipo cliente que ejecuta la consola de delegación y configuración, debe configurar cada controlador de dominio y servidor de administración.

Para configurar el controlador de dominio y el servidor de administración:

1. En el menú Inicio, vaya a **Configuración > Sistema y seguridad > Panel de control**.
2. Abra Herramientas administrativas y, a continuación, Servicios de componentes.
3. Expanda **Servicios de componentes > Equipos > Mi PC > Configuración DCOM**.
4. Seleccione **MCS OnePoint Administration Service** en el servidor de administración.
5. En el menú Acción, haga clic en **Propiedades**.
6. En la pestaña General del área Nivel de autenticación, seleccione **Paquete**.
7. En la pestaña Seguridad del área Permisos de acceso, seleccione **Personalizar** y, a continuación, haga clic en **Editar**.
8. Asegúrese de que el grupo Usuarios COM distribuidos esté disponible. Si no está disponible, añádalo. Si el grupo Todos está disponible, elimínelo.

9. Asegúrese de que el grupo Usuarios COM distribuidos tenga permisos de acceso local y remoto.
10. En la pestaña Seguridad del área Permisos de inicio y activación, seleccione **Personalizar** y, a continuación, haga clic en **Editar**.
11. Asegúrese de que el grupo Usuarios COM distribuidos esté disponible. Si no está disponible, añádalo. Si el grupo Todos está disponible, elimínelo.
12. Asegúrese de que el grupo Usuarios COM distribuidos tenga los siguientes permisos:
    - Ejecución local
    - Ejecución remota
    - Activación local
    - Activación remota
13. Aplique los cambios.